KU LEUVEN

ARENBERG DOCTORAL SCHOOL
Faculty of Engineering Science

Secure and Privacy-Preserving Biometric Systems

Christina-Angeliki Toli

Supervisor:
Prof. dr. ir. Bart Preneel

Dissertation presented in partial fulfillment of the requirements for the degree of Doctor of Engineering Science (PhD): Electrical Engineering

November 2018

Secure and Privacy-Preserving Biometric Systems

Christina-Angeliki TOLI

Examination committee:
Prof. dr. Adhemar Bultheel, chair
Prof. dr. ir. Bart Preneel, supervisor
Prof. dr. ir. Frank Piessens
Prof. dr. Maria Claudia Diaz Martinez
Dr. Enrique Argones Rúa
Prof. dr. Aikaterini Mitrokotsa
(Chalmers University of Technology)

Dissertation presented in partial fulfillment of the requirements for the degree of Doctor of Engineering Science (PhD): Electrical Engineering

November 2018

Acknowledgements

"Whether you think you can or whether you think you can't, you're right."
Henry Ford

This thesis is only the written result of a long journey. The note of acknowledgements is the finishing touch on a personal quest. An accomplishment that would not have had the same value without the help of some people who deserve my gratitude.

I want to express my deep and sincere appreciation to my supervisor Prof. Bart Preneel for giving me the opportunity to pursue the PhD Degree in COSIC. I am grateful for what I have learned and for the flexibility to work on such an exciting research topic. My stay at COSIC was more rewarding than I could have imagined. Thank you for your patience, guidance and constructive recommendations which helped me to improve not only the quality of this work, but also my perseverance as a research engineer. My gratitude also extends to my supervisory committee member Prof. Claudia Diaz. Thank you for adopting me into the privacy group and for our conversations. I greatly appreciated your encouragement. In addition, I would like to thank my supervisory committee member Prof. Frank Piessens for his valuable remarks throughout my PhD. Special thanks to my jury member Prof. Katerina Mitrokotsa for her time and effort invested in this dissertation. Katerina, I feel very fortunate to have met you and I am grateful for your advice on my professional career. I will always remember your moral support. I hope that our paths will cross again. I couldn't forget Enrique Argones Rúa for being an additional member of the jury, an immensely encouraging co-author and a friend. Thank you for your candid attitude, the proofreading of my work and your good ideas that helped me to grow into the field of biometrics. I am also happy that Prof. Adhemar Bultheel was a jury member. Thank you for chairing and organizing the examination procedure.

The KU Leuven has many talented researchers, a fact that stood as inspiration.

I would like to thank all my former and current colleagues for making my time in COSIC an interesting professional experience. I notably want to thank my co-authors for our fruitful research discussions that gave us the opportunity to combine our topics and work on papers together. A big thanks goes to my very good friend Pagona Tsormpatzoudi who I met during this PhD adventure. Thank you for the all the insightful chats regarding the legal framework of biometric applications, for believing in me and for being always present! I would like to express my very great appreciation to Aysajan Abidin for our collaboration and the comments that I received throughout these years. I enjoyed a lot working with you and I learned many things through your serenity and kindness. A special mention goes to all those who have been a part of my getting here: Sara Cleemput, Iraklis Symeonidis, Eleftheria Makri, Charlotte Bonte and Fatemeh Shirazi. I am lucky to have your friendship and your sympathetic ear that means a lot to me. Thank you all for the shared moments of deep anxiety and big excitement.

This thesis would not be the same without the careful title and abstract Dutch translation that have been made by Sara and Charlotte. Thanks to my colleague Eduard Marín Fàbregas, I managed to fix the LaTeX errors on this dissertation's template. Danny De Cock helped me to get started into the topic of biometrics security during my first year at COSIC. Thank you for your advices and your feedback on my thesis. The assistance of Péla Noë, Wim Devroye and Saartje Verheyen is highly acknowledged. Thank you for being so nice to deal with the practicalities of working in a research group and for making my days smoother. COSIC wouldn't be the same without your helping hands.

No acknowledgment part would be complete without some last words for the persons who influenced us on a personal level. I have always believed that people born with personality. However, we are made up of thousands of others. Everyone who has ever done a good deed for us, has played a special role into the make-up of our character, being an additional success factor into our life path. From my closest friends to my teachers and athletic coaches, you know well who you are. Even though it is extremely difficult to mention you all in this text, because the list would be absurdly long, I want to say a warm thanks for your thoughts and your ways to brighten my daily routine. Most importantly, I am exceptionally grateful to my family members for offering me the necessary background to develop my spirit. I am forever indebted to you for teaching me to chase my dreams with the virtues of freedom and braveness.

Christina-Angeliki Toli
Leuven, Winter 2018

Abstract

This thesis focuses on the analysis and design of secure and privacy-preserving biometric deployments. The widespread use of biometric-based architectures for the identification and authentication of individuals poses many concerns due to the collection of personal data. Privacy principles and security recommendations recognize biometrics as highly sensitive information that can be abused and thus must be protected. The approaches that have been proposed depend on the type and the number of the underlying biometric features, such as face, fingerprint or iris, multi-factor or multibiometric schemes. Additionally, the targeted use-cases, for instance government or financial services and the infrastructure of the applications (local or online models) play an important role in the effectiveness of a proposed mechanism. This is a challenging task for the evaluation of practical, accurate and reliable countermeasures to address the security and privacy issues in biometric architectures.

Firstly, we analyze why the designs with multiple biometric modalities have attracted attention in high security-demanding schemes. We discuss whether multimodal recognition can overcome the limitations of traditional unimodal and multi-factor techniques. We analyze the increase of user identification precision and reliability by extending the space of biometric features. We address the concept of biometric integration and we describe the difficulties in selecting a convenient fusion model. We also investigate the impact of performance metrics on the robustness of fusion strategies.

Secondly, we describe the risks of the extraction, storage and processing of biometric data. We analyze why biometrics have been seen intrinsically as privacy's foe. We define the terms of privacy and security for biometric schemes. We study the current cryptographic approaches, clarifying to which extent they can be characterized as Privacy Enhancing Technologies. Additionally, we compare and evaluate their advantages and limitations in relation to the existing security regulations and privacy principles of the legal biometric data protection framework applicable in the European Union.

Thirdly, we carry out an analysis on the vulnerabilities of biometric features to attacks. Mainly driven by government services and the biometric electronic passports that are currently used in many countries, we emphasize data-identity fraud, mostly known as spoofing. We identify the cryptographic tools to enhance the security of biometric data used in ePassport identification documents. Motivated by the functionality of eGates at immigration checkpoints in arrival halls of airports, we design a bimodal biometric anti-spoofing verification system. Our architecture leverages the technique of crypto-biometrics for the secure storage of biometric data in the chip of the ePassport and a liveness detection method as a countermeasure to detect and avert spoofing attempts during automated checking processes.

Fourthly, we investigate the security and privacy concerns of biometric authentication schemes in services of the financial sector. We assess the feasibility of the technique of pseudonymous biometric identities as a privacy-preserving approach. Several advantages are demonstrated and some limitations are derived. Subsequently, we design a biometric authentication model for mobile electronic financial applications. We evaluate how the privacy requirements and the security recommendations for the processing of biometric data can be met in our scenario. Moreover, we identify the ways of developing privacy-by-design biometric-based eFinance architectures.

Finally, we investigate the necessity for highly accessible, scalable and secure biometric deployments. In addition to the popularity of mobile devices, we study whether the remote computation environment of a cloud can provide improved biometric identity management possibilities. We introduce a secure architecture for multimodal user authentication designed to function as an expert system, using stored unimodal biometrics held by cloud-based identity providers. We present a complete analysis of privacy threats associated with this infrastructure. For user multimodal recognition, we exploit a user-specific weighted score level fusion method. We also propose, implement and evaluate decentralized privacy-preserving protocols. In contrast to the existing literature and to the best of our knowledge, we are the first to design a novel, less invasive approach for multimodal authentication, avoiding an auxiliary enrollment of the user and preventing any storage of private information. It is assessed as a convenient solution that restricts misuses of sensitive data, and it is characterized by dynamic functionality and adaptability.

To conclude, biometric systems gain ground globally. Achieving effective and privacy-aware means of authentication has been a long-recognized issue of biometric security. In this thesis, we provide a comprehensive analysis and a critical evaluation of countermeasures and present solutions that can serve as a framework for future applications.

Beknopte Samenvatting

Deze thesis concentreert zich op het analyseren en ontwerpen van veilige en privacybeschermende biometrische implementaties. Het wijdverbreide gebruik van architecturen voor identificatie en authenticatie van personen, gebaseerd op biometrische kenmerken, leidt tot bezorgdheden over de verzameling van persoonlijke gegevens. Privacyregulatie en beveiligingsaanbevelingen erkennen biometrische kenmerken als zeer gevoelige informatie die misbruikt kan worden en bijgevolg beschermd moet worden. De voorgestelde technieken hangen af van het aantal en type van de onderliggende biometrische kenmerken, bv. gezicht, vingerafdruk, iris, multifactorauthenticatie of multibiometrische concepten. Bovendien spelen het beoogde scenario en doelpubliek, bv. overheid of financiële diensten, en de infrastructuur van de toepassingen (lokale en online modellen) een belangrijke rol in de effectiviteit van de voorgestelde mechanismen. Dit is een uitdagende taak voor het evalueren van praktische, accurate en betrouwbare tegenmaatregelen die zich richten op de beveiligingsproblemen in biometrische architecturen.

Eerst analyseren we waarom ontwerpen rond verschillende biometrische modaliteiten zoveel aandacht krijgen binnen scenario's met hoge veiligheidsvereisten. We bekijken of multimodale herkenning de beperkingen van traditionele unimodale en multifactortechnieken overstijgt. We analyseren de toename in identificatieprecisie en betrouwbaarheid door de biometrische kenmerkruimte uit te breiden. We bespreken het concept van biometrische integratie en beschrijven de moeilijkheden in het selecteren van een geschikt fusiemodel. Ten slotte onderzoeken we de impact van performante metrieken op de robuustheid van de fusiestrategieën.

Ten tweede beschrijven we de risico's verbonden aan de extractie, opslag en verwerking van biometrische gegevens. We onderzoeken waarom biometrische kenmerken inherent als de vijand van privacy gezien worden. We definiëren de privacy- en beveiligingsvoorwaarden voor biometrische concepten. We bestuderen de huidige cryptografische methoden en verduidelijken in welke

mate ze als privacybevorderende technologieën gekarakteriseerd kunnen worden. Bovendien vergelijken en evalueren we hun voordelen en beperkingen ten opzichte van de bestaande beveiligingsregels en de privacyprincipes van het wettelijke kader rond de bescherming van biometrische gegevens die in de Europese Unie gelden.

Vervolgens analyseren we de kwetsbaarheid van biometrische systemen voor aanvallen. We leggen de nadruk op identiteitsfraude (spoofing) gedreven door overheidsdiensten en het biometrische elektronische paspoort dat momenteel in veel landen gebruikt wordt. We identificeren cryptografische tools om de veiligheid van biometrische gegevens in elektronische paspoorten te verhogen. Gemotiveerd door de elektronische toegangspoortjes (eGates) aan de douanecheckpoints in de aankomsthal van luchthavens, ontwerpen we een bimodaal biometrisch anti-spoofing verificatiesysteem. Onze architectuur maakt gebruik van crypto-biometrie voor de opslag van biometrische gegevens in de chip van het elektronisch paspoort en van een methode voor de detectie van leven om pogingen tot spoofing tijdens het automatisch controleproces te detecteren en af te wenden.

Daarnaast onderzoeken we de beveiligings- en privacybezorgdheden van biometrische authenticatieconcepten in de financiële sector. We beoordelen de haalbaarheid van pseudonieme biometrische identiteiten als privacybeschermende aanpak. We tonen verschillende voordelen aan en leiden enkele beperkingen af. Vervolgens ontwerpen we een biometrisch authenticatiemodel voor mobiele elektronische financiële toepassingen. We evalueren hoe aan de privacyvereisten en de beveiligingsaanbevelingen voor het verwerken van biometrische gegevens voldaan kan worden in ons scenario. Vervolgens identificeren we manieren om biometrische privacy-by-designgebaseerde eFinanceimplementaties te ontwerpen.

Tot slot onderzoeken we de nood aan zeer toegankelijke, schaalbare en veilige biometrische implementaties. In aanvulling op de populariteit van mobiele toestellen onderzoeken we of de externe rekenomgeving van een cloud betere biometrische identiteitsmanagementmogelijkheden verschaffen. We introduceren een veilige architectuur voor multimodale gebruikersauthenticatie, ontworpen om als expertsysteem te functioneren en gebruik te maken van biometrische kenmerken die bijgehouden worden door cloudgebaseerd identiteitsproviders. We presenteren een volledige analyse van de privacybedreigingen geassocieerd met deze infrastructuur. Voor multimodale herkenning van gebruikers, maken we gebruik van een gebruikersspecifieke gewogen-scorefusiemethode. We stellen ook gedecentraliseerde privacybeschermende protocollen voor en implementeren en evalueren ze. In tegenstelling tot de bestaande literatuur, en voor zover wij weten, zijn we de eersten om een nieuwe minder invasieve aanpak voor multimodale authenticatie te ontwerpen waarbij een registratie van de gebruiker waarin biometrische gegevens opgeslagen worden, vermeden wordt zodat er geen

gevoelige gegevens opgeslagen worden. Dit is een geschikte oplossing die misbruik van gevoelige gegevens beperkt en gekarakteriseerd wordt door dynamische functionaliteit en ingebruikname.

We concluderen dat biometrische systemen globaal terrein winnen. Het bereiken van effectieve en privacybewuste authenticatiemiddelen is reeds lang erkend als een probleem binnen de biometrische beveiliging. In deze thesis voorzien we een uitgebreide analyse en een kritische evaluatie van tegenmaatregelen en bestaande oplossingen die als raamwerk kan dienen voor voorzienbare toepassingen.

Contents

List of Figures

List of Tables

Abbreviations

AaaS	Authentication as a Service
AD	Auxiliary Data
BaaS	Biometrics as a Service
CBDB	Centralized Biometric Database
DB	Database
EER	Equal Error Rate
FAR	False Acceptance Rate
FRR	False Rejection Rate
GDPR	General Data Protection Regulation
HD	Helper Data
ICAO	International Civil Aviation Organization
IdMaaS	Identity Management as a Service
ISO	International Organization for Standardization
MIP	Multimodal Identity Provider
MPC	Multi-Party Computation
PETs	Privacy Enhancing Technologies
PI	Pseudonymous Biometric Identity
PIN	Personal Identification Number
RFID	Radio Frequency Identification
ROC	Receiver Operating Characteristic
SP	Service Provider
UA	Unimodal Authenticator

Part I

Security and Privacy in Biometric Schemes

Chapter 1

Introduction

Biometry is the science of establishing the identity of a person based on human physical or behavioral attributes, Li and Jain [122]. The first systematic capture of biometric data for identification purposes was done by William Herschel in 1858. In 1870, Alphonse Bertillon developed a method for the recognition of criminals based on body measurements, such as height or surface's marks, for instance scares and tattoos, Ross et al. [182]. With the passage of time, a complete methodology was developed where biometrics stored and separated into categories for retrieval and matching procedures in applications for law enforcement. From the late 19th to the early 20th century, fingerprint identification was introduced and widely used by police agencies, Maltoni et al. [131]. Over the years, shortcomings and weaknesses of these measurements and techniques were identified. This knowledge increased the need for more accurate features and led to the development of new technologies that have been successfully deployed, Jain et al. [102].

Biometric systems rely on who a person is, or what someone does, contrary to other authentication approaches and credential types, such as passwords, Personal Identification Number (PIN) codes, tokens or cards that can be forgotten, guessed, transferred, copied, lost or stolen as explained by Podio in [166]. Moreover, in today's electronically connected society means people are asked to remember a multitude of personal identification numbers for computer accounts, bank automated teller machines (ATMs), e-mails, wireless phones, web sites and so forth, Tistarelli and Nixon [205]. Although biometric characteristics are mainly introduced for applications useful in forensic science and the government sector, due to the fast-paced digital revolution, the automatic biometric-based recognition of a person's identity becomes constantly more

popular and sometimes compulsive since it is considered to be fundamental for reliable day-to-day transactions, di Vimercati et al. [63], Shoniregun and Crosier [191]. Examples of these applications include several commercial and civilian services, such as the physical access control for facilities, the logical access control to log into biometrically-enabled devices, to secure electronic banking and online transactions and to improve border security among others, Campisi [39]. While the use of biometrics is a part of the daily routine, the proliferation of mobile and web-based technologies have further accentuated the need for improved identity management solutions that can accommodate a large number of users, Ashbourn [15], Menezes et al. [142], Simoens et al. [195].

According to a recent study of Acuity [5], all smartphone devices will have at least some kind of an embedded biometric technology by 2019, while by 2020 the technology will be applicable to wearable tech and tablets. In the age of the Internet, the need for highly accessible, scalable and secure biometric deployments moves the existing biometric technology to the cloud. Furthermore, Acuity [5] estimates that users' biometric data will be outsourced to the cloud and more than 5.5 billion biometrically-enabled devices will create a global platform by 2022. A governance cloud-based Biometrics as a Service (BaaS) framework can leverage the cloud infrastructures, allowing for component developers to outsource the tools for biometric authentication and identification purposes as described by Talreja et al. [202], Zareen et al. [230] and Zhu et al. [232]. It is expected that the usability of the cloud computing services will be increased and Service Providers (SPs) will be capable of authenticating more than one trillion transactions annually while the revenue of markets will rise rapidly.

Thanks to the imaginative and flattering depiction of biometric systems in movies and television shows, the general perception is that the biometric technology is foolproof, Burge and Bowyer [37]. However, its increasing usage has proven the weaknesses and has given rise to additional security and privacy concerns as analyzed by Jain and Kumar [99]. Although biometrics as an authentication mechanism are intended primarily to enhance security, biometric data are unique physical properties that people carry on; a fact that renders them sensitive by nature, Ngo et al. [151] and Yang et al. [227]. Furthermore, the biometric applications require the collection and storage of datasets for matching purposes and their transmission and processing across third parties could be compromised, Pagnin and Mitrokotsa [158]. Biometrics can also be used as identifiers to link the users' information across different applications for profiling or to trace their whereabouts and in that way they may reveal more personal information than necessary, Bhattasali et al. [21]. These elements emphasize the fact that there are numerous challenges that need to be addressed in order to broaden the reach of biometric technology.

A biometric scheme is a pattern recognition system that compares the extracted

features of a user with the stored template of biometric datasets from a prior enrollment process. Biometric recognition systems that use one biometric trait of the individual for identification and verification purposes are called unimodal designs, Li and Jain [122]. However, unimodal traits might not be compatible with certain groups of population and although the biometric traits are expected to exist among every individual, there could be some exceptions where a user is unable to provide a particular feature, Jain et al. [98]. Unimodal biometric systems are quite vulnerable to spoofing attacks where the data can be imitated, Hadid et al. [82]. These limitations and vulnerabilities of unimodal models have increased the necessity for more robust architectures, Rathgeb and Busch [172]. In the literature, there are several approaches for authentication mechanisms based on multi-factor schemes that combine a single biometric modality and a password, a PIN code or a token. Multi-factor authentication systems provide an additional layer of security and make it harder for attackers to gain access to a person's information. Consequently, they are used on a daily basis in government, health-care, financial and business applications, Wazid et al. [223]. Moreover, since every human possesses more than one forms of recognition, multimodalities can be used to enhance the efficiency of the currently used models, Peng et al. [164]. When adopting a biometric technology for recognition applications, the most crucial pre-deployment question is whether to choose a unimodal, multi-factor or multimodal biometric architecture. A recent report of 2018 presented by IndustryARC [91] concludes that multimodal models that integrate the multiple biometrics of a user have proven to be more secure and reliable, managing to supersede the unimodal and multi-factor authentication designs due to their effectiveness and robustness while it addresses their applicability in the next generation biometric systems.

Cavoukian and Stoianov discussed that the aim of using cryptography in biometrics is to protect these pieces of data that are used for the recognition of a claimed identity [47]. Although the task may sound simple, there are several constraints and complications such as these presented by Bringer et al. in [35] and Kanade et al. in [109]. Biometric characteristics are anthropometrics and thus, their extraction, representation and matching imply classification problems, Menezes et al. [142] and Ross et al. [181]. A stored template hardly ever is exactly the same as a newly captured trait, even if both are processed by the same type of sensor. Secondly, the accuracy of biometric schemes is dependent on False Acceptance Rates (FAR) and False Rejection Rates (FRR), known as performance rates, Nandakumar and Jain [149]. Additionally, the utility of a biometric feature in real-world applications is determined by certain properties, such as uniqueness, measurability and spoofability among others as analytically presented in the International Organization for Standardization (ISO) [96]. In 2003, the International Civil Aviation Organization (ICAO) initiated a study for quantifying the compatibility of biometric data according to their properties

for their adoption in machine readable travel documents such as electronic passports. Facial, fingerprint and iris biometrics stated as globally interoperable and they are widely used in a variety of applications, Bharadwaj et al. [20].

Although biometrics were initially introduced as a means to overcome the security limitations of the traditional authentication approaches, they are tied with the identity of the user, Jain and Kumar [99]. Hence, if biometric data are not efficiently protected, they can be compromised and reveal more information than necessary, violating the user privacy, Nandakumar and Jain [149]. *Security* for biometric architectures is related to the technical characteristics of the system and its overall robustness. In this direction, literature offers several approaches that have been proposed to hide the biometric data and to prevent the linking of personal information, always maintaining the ability to accurately verify a person's identity. Schemes, such as cancelable biometrics and biometric cryptosystems among others, can offer advantageous solutions, Bolle et al. [30], Kanade et al. [108] and Sutcu et al. [201]. *Privacy* is defined here as the control of the users over their own data and it plays an important role in public acceptance of biometric designs, Kindt [115]. For biometric technology, security and privacy have been treated as two factors that should be developed cooperatively. Specifically, privacy cannot be preserved and achieved independently without the enhancement of security. The balance between privacy and security and the optimum trade-off lies on the system context, the targeted use-cases and the risk assessments regarding the attackers' capabilities, Prabhakar et al. [167]. Cavoukian in [45] and Kindt in [115] analytically explained that the deployment and practical implementation of biometric schemes require compliance with the evaluation criteria and the privacy principles as addressed by the legal framework for the protection of biometric data. Finally, the ISO Standards for the biometric principles and framework [93] underlines that the effectiveness of cryptographic methods for different modalities and their combinations need to be resolved according to the relevant privacy principles and security requirements that are important to be addressed since they define their applicability.

Academia, industry, the military and security agencies invest in the research for the development of provably secure and privacy-aware biometric technologies. Even though over a decade of extensive analysis has brought many novel biometric protection proposals, there is still a discrepancy between security requirements and privacy demands in this relatively young discipline, Campisi et al. [40]. Kindt analyzed that the existing efforts to protect the privacy of the users may be proven insufficient, while the growth of information-analysis technology has profound consequences, both good and bad [116]. The legal rules that are currently developed to cope with these developments will determine the limits of our freedom and privacy, Solve [198]. Through the prism of the new European General Data Protection Regulation (GDPR) [66] and the European

Regulatory Technical Standards for Strong Customer Authentication [183], biometric technology is forced to revise the infrastructure and the evaluation activities. The main objective in this direction is the design and implementation of biometric architectures that prioritize the privacy awareness to address the security issues against vulnerabilities and potential infringements.

1.1 Contributions of the Thesis

The aim of this thesis is to advance the understanding of security and privacy in biometric systems. We mainly contributed to this field in two ways. Firstly, by analyzing the security and privacy of several schemes in widely used biometric-based applications. Secondly, by proposing practical and efficient solutions to address the weaknesses we have identified and to make the biometric designs more secure and privacy-friendly. To facilitate the evaluation of our work, we map the contributions of our papers in Table 1.1.

Table 1.1: Contributions of our work.

Publication's Title	**Contributions**					
	1	2	3	4	5	6
A Survey on Multimodal Biometrics and the Protection of their Templates[1] [210]	✓		✓			
A Bimodal Verification Cryptosystem as a Framework against Spoofing Attacks [211]	✓		✓	✓	✓	
A Privacy-Preserving Model for Biometric Fusion [208]	✓		✓			✓
Privacy-Preserving Biometric Authentication Model for eFinance Applications [213]	✓	✓				✓
Secure and Privacy-Friendly Multimodal Authentication using Cloud-based Providers [207]			✓	✓		✓

We made the following contributions that can be summarized as follows:

1) Study the feasibility of using cryptography in biometric schemes. A biometric system is a pattern recognition scheme that extracts and compares the tested features of a user with the stored ones, from the process of a prior enrollment. However, the existing biometric template protection techniques, applied to enhance the secrecy of the stored data, can reduce the recognition efficiency, Kanade et al. [109] and Simoens [193]. We conducted studies on

[1]This work is presented in the background of Part I and it is not included in the selected publications of Part II.

whether cryptography can be used in unimodal, multi-factor and multibiometric schemes without reducing the performance accuracy. Moreover, in this context, we identified the types of biometrics that present fewer drawbacks and offer the necessary amount of information for user recognition. Finally, we analyzed the optimal applicability of several cryptographic methodologies in order to improve both the robustness and the performance reliability in biometric designs.

2) Privacy analysis of cryptographic mechanisms for the protection of biometric data. It is a common belief that even when a biometric recognition procedure is securely performed by a legal authority, sensitive information about the users could be gathered and shared for other than the initially defined purposes, without any official approval, Bertino [19]. Thus, during the last decade, there is a rapid progress of development for regulations and recommendations regarding the secure transmission and handling of user's data in biometric schemes. We identified and mapped the privacy principles and the security properties that should be addressed in real-world biometric deployments. We presented a complete analysis of the existing cryptographic approaches in the context of privacy-preserving measures to assess their adequacy. We provided a comparative study of the security and privacy advantages and weaknesses of each technique following the currently used recommendations as addressed in the ISO Standards for biometric information protection [92] and [96] and the new European GDPR [66]. Finally, our work addressed the importance of privacy-by-design solutions in biometric schemes.

3) Analysis of the performance accuracy and security evaluation of multimodal designs. The consolidation of biometric information for the design of secure multibiometric systems is an active research area with numerous applications, Ross et al. [182]. Fusion constitutes a way to enhance the recognition reliability of a system. However, the concept of multimodal integration and the selection of a convenient model is a challenging task as discussed by Meva and Kumbharana [143]. An important part of our work based on studying and analyzing the matching accuracy and the security of multimodal schemes. We studied the impact of performance rates in different fusion strategies and we analyzed the efficiency of the existing cryptographic approaches in multimodal models. Finally, we identified the practical difficulties of designing secure multimodal systems, while we proposed several methodologies for enhancing security and privacy in different multimodal recognition architectures.

4) Attacks on biometric architectures. We analyzed passive and active attacks against unimodal and multimodal biometric designs. We identified the feasibility of these attacks and the information that an intruder can gain, compromising the authorized user privacy. We elaborated on possible ways to overcome some of these challenges and we discussed the role of cryptographic mechanisms in facing different kinds of vulnerabilities related to

the communication, templates' storage, and computations on biometric data.

5) Framework of anti-spoofing measures. Spoofing attacks take place directly at the biometric sensor of a recognition system by using artificial biometric samples. An active adversary tries to claim a different identity and deceive the matching result. State-of-the-art research has shown that none of the cryptographic schemes is completely spoof-proof, Marcel et al. [136]. We analyzed the anti-spoofing methodologies and we studied the current mechanisms in realistic scenarios. We identified their advantages and limitations and we proposed potential improvements. Liveness-detection requires the cooperation between the user and the function itself and tests if the biometric being captured is an actual measurement from the authorized, alive person who is present at the time of the capture procedure. According to our findings, this approach can recognize and prevent a significant number of spoofing attacks in unimodal systems. Finally, motivated by the growth of illegal immigration that may increase fraud, cloning and identity thefts with numerous social, economic and political consequences, Rebera et al. [176], we proposed a bimodal architecture that combines two modalities for automated border control able to detect spoofing attacks. To reduce the risk of the exposure of the stored templates, we used an encryption scheme based on the technique of crypto-biometrics. Additionally, in our design we involved a liveness-detection module to increase the security robustness, without compromising the matching accuracy.

6) Design of a secure and privacy-preserving system for biometric authentication. The targeted use-cases, for example commercial, government or financial applications and the infrastructure of an architecture play an important role in the applicability of a proposed cryptographic approach.

- We proposed a biometric authentication model for eFinance applications. The system allows remote monitoring of the user's account, using his mobile device with an embedded fingerprint sensor. To reduce the privacy risks and increase the security, we implemented a multi-factor scheme based on minimal extracted data (minutiae features of a fingerprint) and a PIN code as inputs to a Pseudonymous Biometric Identity (PI) recoder. Through the use of the PI technique, there is no storage of sensitive biometric data and user's references. According to the ISO Standards for the security framework in financial services [94] and the evaluation methods as presented in ISO Standards [95], we discussed the ways that privacy could be addressed under the given scenario and how the security recommendations were satisfied during the design process.

- Furthermore, biometric designs have attracted attention in online services. However, even if cryptography is used, the context information of these communications could lead to the leak of private data about users across

the network, Butt et al. [38]. Even though several proposals on multimodal fusion, performance rates and secure mechanisms for the protection of biometric data can be found in the literature, the combination of these fields is a challenging task. We proposed a design that incorporates the performance rates in a multimodal fusion strategy. We designed a model for authentication and identification purposes. Finally, we discussed the usability and the advantages of our approach and we analyzed what cryptography can offer to reduce the privacy and security threats.

- Our final work was motivated by the fact that the storage of biometric data in Centralized Biometric Databases (CBDBs) seriously increases risks for the privacy of the users according to the analysis presented by Jain and Kumar in [99]. Hence, there are extensive efforts to discourage additional and auxiliary Databases (DBs) with biometric templates. Moreover, the adoption of biometric technologies for various applications has grown exponentially over the last decade. Due to the increasing demand for authentication solutions, cloud computing can serve as a means to deliver biometric services over the Internet offering numerous benefits, such as reduced cost, increased storage capacity, parallel processing capabilities and flexibility, Ashbourn [15]. Thus, cloud can offer improved next generation biometric technologies while it has an enormous potential market value. We proposed a novel Biometrics as a Service (BaaS) scheme and a less invasive, distributed approach for multimodal biometric Authentication as a Service (AaaS) in the cloud. Our system performs authentication, exploiting prior stored unimodal templates being collected by Authentication as a Service (AaaS) and distinct untrusted Identity Management as a Service (IdMaaS) providers. To obtain a multimodal result, we used Hamming Distance algorithms and a user-specific weighted score level fusion method. We performed an extensive threat and risk analysis. Taking into account the severity of the security and privacy concerns that may limit the design and implementation we used Multi-Party Computation (MPC) techniques to build our privacy-preserving protocols, allowing mutually distrusting parties to jointly compute the matching score without revealing any private data. The extracted biometric features, the stored templates, the fusion results or any derived information from them are not exposed towards the parties involved in the computation. We simulated the functionality, practicality and efficiency of our approach.

1.2 Structure of this Thesis

This thesis is based on publications and consists of two parts. Part I provides an introduction to the field of biometrics and defines the objectives and the

motivation behind this work. We analyze why it is necessary to enhance the security of biometric data, while preserving user privacy. We present an overview of our contributions and formulate some open problems with potential directions for future research. In Part II, we present a selection of our publications.

Chapter 1 stands as introduction and sets the scene for this work. We present our research goals and the outline of this thesis. In Chapter 2 we give an overview of the basic concepts of biometrics and some terminology. We discuss the concept of multibiometric information fusion and the role of recognition performance metrics. In Chapter 3, we address why the protection of biometric data is not a trivial task, in order to contextualize the thesis. Additionally, we describe and discuss the state-of-the-art in methodologies and techniques for the design of secure and privacy-preserving biometric schemes, including our analysis of the existing approaches. Finally, Chapter 4 summarizes the concluding remarks of this thesis and presents research directions for future work.

Part II bundles a selection of our publications. Firstly, we present a full list of our publications and then we reproduce each of the selected works in their respective chapter as follows:

1. We analyze the existing spoofing countermeasures and we present a bimodal framework for user authentication using an ePassport for secure automated border control applications. Our design uses the cryptographic technique of crypto-biometrics to enhance the protection of biometric data and a liveness detection mechanism able to detect and prevent spoofing attacks during access control at eGates, Toli and Preneel [211].

2. We give an overview of the guidelines on how to use performance metrics into a biometric fusion model. We present a model for multimodal identification and authentication purposes and we analyze the the security and privacy challenges related to its functionality, Toli et al. [208].

3. We present a privacy-preserving multi-factor biometric authentication model, specially designed for eFinance applications. We provide a critical evaluation of its advantages and weaknesses in the context of the currently issued legal frameworks for the security and privacy of biometric data in applications in the financial sector, Toli and Preneel [213].

4. We present a secure and privacy-friendly multimodal biometric authentication system using remote distrusting cloud-based identity providers. We analyze the threat model and we present the security and privacy analysis of our decentralized protocols. Furthermore, we discuss the results of our experimentations in terms of complexity, efficiency and overall accuracy. Finally, we evaluate the usability and applicability of our approach, Toli et al. [207].

Chapter 2

Biometrics

This chapter stands as an introduction to the field of biometrics. It is important to present the concepts and primitives of performance metrics due to their impact on secure biometric schemes. Moreover, we give an overview of the multibiometric systems while we discuss the levels of information fusion. Finally, we address the issues that determine the accuracy and security which are related to the applicability of multimodal designs in real-world deployments.

2.1 Biometric Modalities

In the era of technological evolution, automatic recognition of individuals has become fast and easy. The popularity and acceptability of biometric technologies is proved by the local fingerprint authentication which is a part of the daily routine for millions of smartphone users, enhancing their experience and convenience. According to the results from a recent survey commissioned by VISA [220], biometrics win the favor of users and the day when biometric implementations completely substitute passwords is drawing nearer than expected by the biometric markets. Biometrics present certain advantages that cannot be provided by other authentication mechanisms, Prabhakar et al. [167]. They are recognition forms that set a strong link between a person and his identity due to the fact that biometric features cannot be easily lost, or duplicated. Thus, biometrics are considered to be more resistant to attacks than the other methods of recognition, Furnell [68]. One of their major advantages is that they can offer a negative recognition functionality. In this way, the system establishes whether the person is who he implicitly or explicitly denies

to be and it guarantees whether a certain user is indeed enrolled in a system although the individual's claims might. Additionally, biometric systems require the presence of the user at the time of authentication, preventing the individuals from making false repudiation claims as presented in ISO Standards [96]. Both of these terms are especially critical in security-demanding applications, where impostors may attempt to claim different identities and gain benefits. Besides enhancing security, biometric systems also offer improved user convenience by alleviating the need to design passwords and tokens, Vasiu [218].

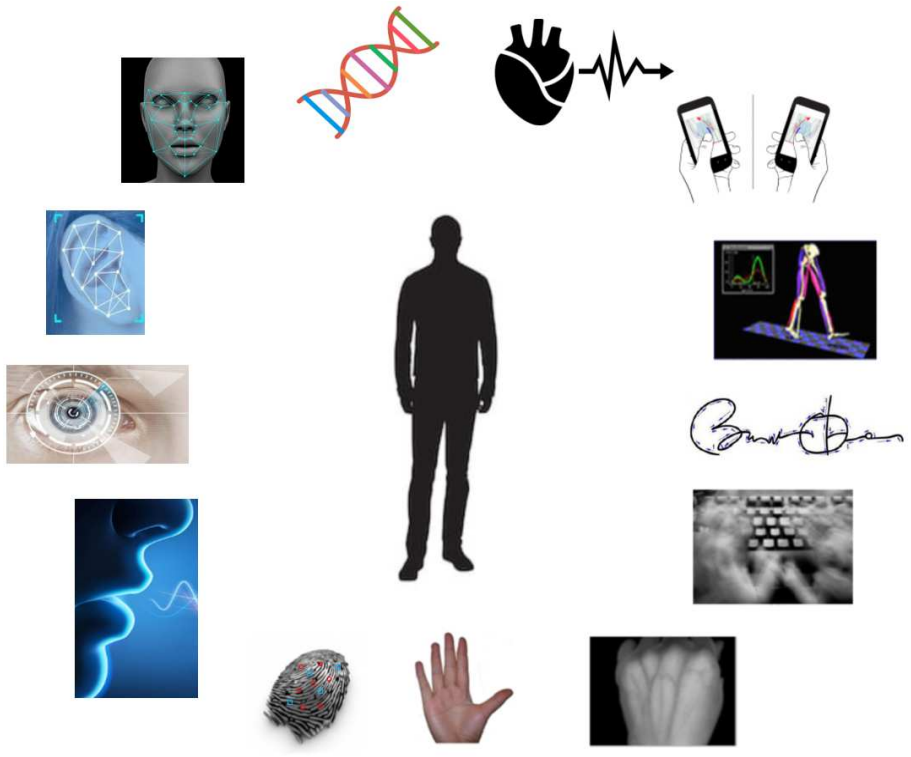

Figure 2.1: Physical and behavioral biometric features.

Biometric systems use a variety of physical or behavioral characteristics. Figure 2.1 illustrates some examples of biometric traits that can be used for authenticating a user. They include face, ear, iris, retinal scans, voice, fingerprint, palmprint, hand/finger geometry, vein patterns, heartbeat or even DNA, Abaza et al. [1], Burge and Bowyer [37]. Behavioral characteristics define how the person behaves or something unique regarding what he does or knows, such as gait, signature analysis, keystroke dynamics/typing rhythm, computer's mouse

use and device holding characteristics among others. Moreover, soft biometrics, which belong to both categories, include the skin, eye and hair color, presence of beard, height, weight, tattoos and accessories among others, are widely used for lawful surveillance purposes, Othman and Ross [156]. Devices, such as cameras from super markets to public places and roads, can identify the people passing through. The new systems are carefully designed so that can reduce the misidentification errors. A recent study presented by Connor and Ross [54] concludes that it is expected that the next generation systems can further reduce the misidentification errors by detecting the conditions that weaken any external factor that could affect the effectiveness of a biometric-based device.

2.2 Properties for Biometric Modalities

The main properties that need to be considered before a modality can be characterized as suitable for its applicability in a biometric recognition system include: universality, uniqueness, permanence, collectability, measurability, performance, acceptability and circumvention, ISO Standards Biometrics Vocabulary [96], Jain et al. in "Handbook of Biometrics" [98] and Podio in "Biometric Technologies and Security-International Biometric Standards Development Activities" [166]. They are briefly discussed as follows:

Universality. Every individual accessing the biometric application should possess a specific modality. A large majority of people should have this characteristic such as everybody or at least the most individuals have at least one fingerprint, eye or ear that they can use to identify themselves.

Uniqueness. The given characteristic should be sufficiently different across users comprising the population. For example a fingerprint or an iris are unique even between identical twins. Unique characteristics can be used to prevent unauthorized access to a biometric system, preventing attacks. Although the uniqueness is seen as an advantage, it does not prevent the threat of tracing individuals across different applications. It remains possible for an attacker to trace operations done by an individual who uses the same biometric modality through the logging of authentication sessions. This the reason for the importance of this property which reflects the need for security and privacy in biometric designs.

Permanence. The biometric characteristic of an individual should be sufficiently invariant over a period of time with respect to the applicable matching algorithm of the system. This means that the trait should not change significantly over a time period because otherwise it cannot be considered as

a useful biometric. The ridge structures on the palm are the most well-known biometric features that do not change much as the person ages.

Collectability. The term is referred to the easiness of obtaining the biometric data. It should be possible to acquire and digitize the biometric features using suitable devices with embedded sensors that do not cause undue inconvenience to the user. In that way, we can achieve a successful extraction and representation of the datasets in biometric templates.

Measurability. The biometric datasets should be suitable in order to use statistical analysis to determine the matching result. The complexity of the applicable algorithms, the computation time and the cost of the scheme's components should be evaluated in order to determine the efficiency of a system in real-world applications.

Performance. This measurement is used to address system's accuracy in order to allow the access to only authorized users and reject impostors. It also includes the constraints imposed by the application, such as the used resources and the environmental factors that may affect the recognition accuracy.

Acceptability. This property is referred to how people react to a biometric system, how familiar they are with biometric technologies and the use of applications (habituation) and which is their willingness to provide their biometric data. The cooperation of the individuals is necessary and they should feel comfortable and both legally and technically protected using this form of recognition for their personal security.

Reliability. This concept refers to the quality of the biometric characteristic. It should be not easy to be forged and the delivery of the characteristic should not be apt to fooling the system. In the same context, the property of **circumvention/spoofability** is used to define that we should be able to assess potential spoofing attacks and measure how easily a biometric trait of a user can be imitated using artifacts, such as create gelatin genetic clones of fingerprints, contact lens with a copy of iris or retinal scans, artificial replicas of faces, facial samples in the form of photographs, a video or a 3D mask, Chingovska et al. [51] and Rebera et al. [176]. It refers to the effort of an attacker to fraudulently alter and bypass the biometric system in order to gain unauthorized access.

2.3 Operating Modes of Biometric Systems

Depending on the context of application, a biometric system may operate for *authentication/verification* or *identification* purposes. When it is necessary to avoid this distinction, we are referred to the term of *recognition*, Jain et

al. [98]. Figure 2.2 depicts the main modules of a typical biometric recognition architecture.

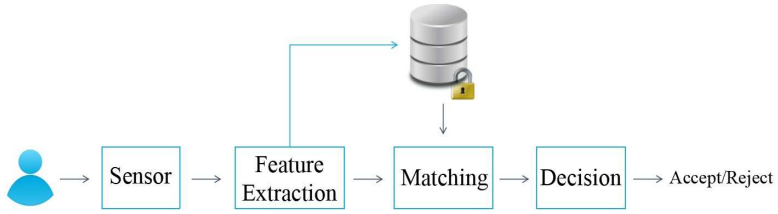

Figure 2.2: Stages of enrollment and recognition in biometric schemes.

During the enrollment process, the user presents his fresh biometric features at a sensor that is a biometric scanner device. For example, optical fingerprint sensors are used by the administrative authorities to collect citizens fingerprints for civilian applications, such as electronic identity cards, Ross et al. [182]. This module is part of the human machine interface. The feature extraction module is involved to compute the quality of biometric samples that is assessed in order to determine their suitability for the next processing stages. Furthermore, the acquired data are subjected to signal enhancement algorithms in order to remove noise and improve their quality. The feature sets compose the new template and along with the user's biographic information, such as name, address, etc. , they are securely transmitted and stored in an encrypted biometric repository such as a smart card issued to the user, or a DB, Yang et al. [227]. The protection mechanisms for the secure storage of biometric information are extensively discussed in Chapter 3.

For authentication purposes, a user who claims an identity presents a username or a passcode and his biometric features at the sensor of the system. After the feature extraction, the scheme conducts a one-to-one comparison, where the created template is compared to the stored template. In the matching module, an algorithm computes the *similarity* or the *distance* between the two templates to determine a matching result. For instance, in a fingerprint-based biometric model, the number of matching minutiae between the two templates is computed and a match score is reported. Finally, the module of decision is used to compare the matching score to the system's threshold in order to validate a claimed identity.

In identification applications, the scheme follows the same stages as in the authentication mode. However, the user does not present his credentials and the system tries to identify him by searching the templates of all the enrolled individuals in the DB for one-to-many comparison. The process fails if the subject has not been successfully enrolled, and therefore his templates are not included in the system's DB. Identification is a critical component in recognition

applications and it can only be established through biometric features and not by other recognition methods, Cavoukian and Stoianov [48]. It is the only way to prevent a person from using multiple identities while the scheme establishes the true identity of the person in spite of who he claims or denies to be.

2.4 Performance Metrics and Recognition Accuracy

The selection of a particular biometric for an application and the confidence in the functionality of a biometric scheme are determined by specific measures that are used to evaluate the recognition accuracy and effectiveness as addressed in ISO Standards [93]. During the matching process, the generated score, after the comparison of the new and stored templates, can be analyzed on the basis of a predefined threshold, Tao and Veldhuis [203]. In biometric designs that use an algorithm that computes the similarity between a new and a stored template, the decision result is represented as 0 which means that the template is not matching and the authentication is rejected. The closer the score is to 1 the more certain is the system that the new and the stored templates come from the same user. A threshold τ lying in the interval $[0, 1]$ is defined to decide if a user does or does not correspond to a claimed identity. If the matching score is less than the system's threshold τ then the authentication is rejected. Biometric data are anthropometrics and thus, they are noisy, resulting high error rates in biometric designs, Li and Jain [122], Ross et al. [181]. Hence, schemes hardly ever encounters a user's fresh biometric trait and a stored template that result in a 100% match. The statistical calculation of thresholds is related to the extraction and validation of performance rates, Malik et al. [130].

The most important measures that are used to evaluate the performance of a biometric recognition scheme are the False Acceptance Rate (FAR) and the False Rejection Rate (FRR), Golfarelli et al. [75]. Figure 2.3 illustrates the computation of the performance metrics for a given threshold τ, Maltoni et al. [131]. FAR indicates the probability that the system incorrectly authorizes a non-authorized person, due to falsely matching the biometric input with a template. Moreover, FRR is the percentage of times when an individual is not matched to his own stored template. In other words, FRR is the percentage of the genuine scores which are lower than the decision threshold and they are incorrectly rejected.

Figure 2.4 shows the Equal Error Rate (EER) that denotes the rate at a threshold τ for which both FAR and FRR are equal, where genuine and impostor error rates are closest to zero. Although in practice the EER is not useful in assessing

the actual system's performance, it is an important operating indicator for the selection of the threshold and consequently the recognition accuracy of the biometric architecture, Li and Jain [122].

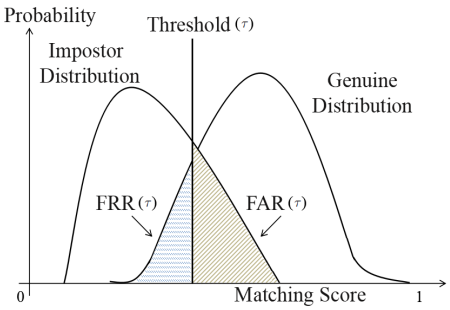

Figure 2.3: Performance metrics over genuine and impostor distributions.

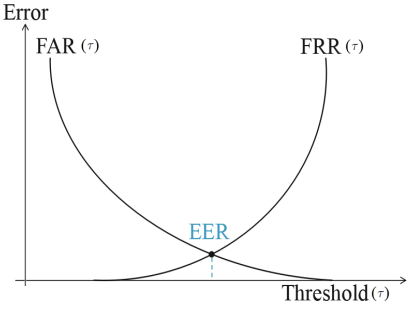

Figure 2.4: EER corresponding point on FAR(τ) and FRR(τ) curves.

In biometric schemes, the performance of tests on biometric data is an essential technique in order to achieve an acceptable value of FAR, or select an optimum FRR for the purposes of the recognition schemes, Tao and Veldhuis [203]. This can be achieved by training the applicable algorithms for examining how the system behaves under different values of threshold. Tuning the system's threshold is a mechanism to study the performance accuracy under a given procedure. This process always affects not only the corresponding rates of the system, but also the final decision, Malik et al. [130], Prabhakar et al. [167] and Ross et al. [182]. In unimodal designs, these rates cannot be reduced simultaneously by adjusting the threshold. Although, a lower threshold makes the system more tolerant to input variations and noise, it increases the corresponding FAR. For that reason, the system's overall accuracy is associated with the ability of the system designers to perform tests on biometric datasets in order to handle the problems of high performance rates or select an optimum EER according to the demands of recognition applications. In that way, systems with high requirements in terms of robustness (e.g., border control, law enforcement and surveillance applications) demand a low FAR, selecting a higher threshold for enhancing security, Jain and Kumar [99] and Li et al. [123]. On the contrary, in architectures for forensic applications the output should indicate the set of possible matching identities sorted in decreasing order of confidence and therefore a higher FRR is more convenient, Cavoukian and Stoianov [47]. For commercial applications, it is necessary to select an optimal solution in order to avoid an extensive number of FAR and to reduce the need for human intervention. Figure 2.5 presents the Receiver Operating Characteristic (ROC) curve of the recognition accuracy trade-off that is preferred in several types of applications,

adapted from Maltoni et al. [131].

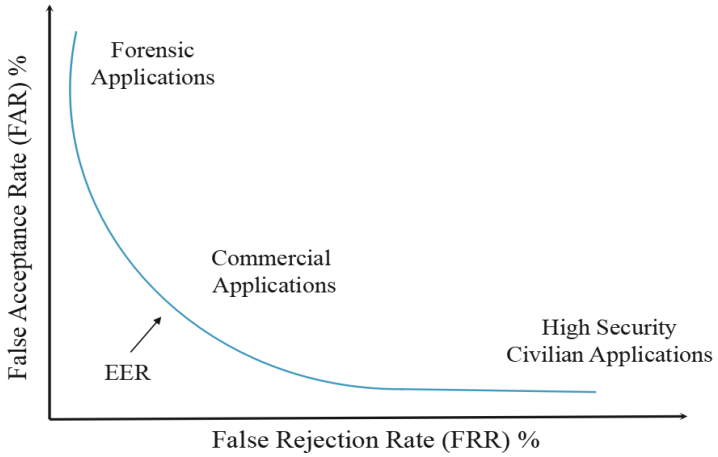

Figure 2.5: ROC curve of accuracy and operating points in biometric applications.

2.5 Multibiometric Systems

The biometric properties, such as non-universality, and the operational factors, for instance noisy input data, can restrict the availability of specific modalities for a part of the users' population. Thus, a fine tuning of the system's parameters cannot be expected to provide continuous performance improvement, ISO Standards for Biometric Performance Testing and Reporting [93]. Therefore, the accuracy of a biometric system employing a single unimodal trait is constrained by intrinsic factors. According to the findings of Ross et al. in [181], there is not a single biometric modality that can be considered sufficiently accurate for robust real-world applications, while it is demanded from designers to produce efficiently secure systems with low error rates. These limitations can be alleviated by fusing the information presented by multiple sources, Manasa et al. [132]. This increases the number of the users that can be effectively enrolled in a recognition system while improves the reliability, as explained below. A system that consolidates the evidences presented by multiple biometric sources is known as a *multibiometric scheme*, Nair et al. [147].

Multibiometrics present several advantages over traditional unimodal deployments. They address the issue of insufficient population coverage, since they improve the flexibility of a design where people can be enrolled using different

features, Lee et al. [118]. Moreover, they can offer substantial improvement in the matching accuracy, depending on the information being combined and the applied fusion methodology. Hence, both the FAR and FAR can be reduced simultaneously, Sasidhar et al. [188]. Taking the quality assessment into consideration, they can effectively address the problem of poor data by selecting only the used features that can be accurately measured. Finally, they present resistance against certain types of attacks such as spoofing attacks, where it becomes increasingly difficult for an impostor to spoof multiple biometric modalities of an authorized user, Akhtar et al. [9]. A multibiometric design is as a fault tolerant mechanism that continues to operate even when some of the biometric traits are unreliable, Jain et al. [98].

There are different sources that can be used in order to obtain multiple pieces of biometric evidence from the same user, Ross et al. [182]. In multi-sensor designs, a unimodal biometric is extracted by multiple sensors. For multi-algorithm models, the same unimodal is processed by multiple extraction algorithms. This approach has been mainly introduced as an effective solution to reduce the cost of the multi-sensor deployments, Kelkboom et al. [112]. Moreover, multi-instance and multi-sample schemes use the same biometric trait captured by different angles or at multiple times such as the irises of the left and right eyes of a user and their representations during the eye movement. Finally, multimodal designs combine the evidences presented by different body parts of the user to establish his identity. In the biometric technology markets, vendors have already deployed systems that use two or three patterns of face, fingerprint or/and iris for the same user, providing reliable recognition in many commercial applications, Omotosho et al. [154]. Hybrid systems that implement both multimodal and multi-algorithm approaches are also designed as an attempt to extract as much information as possible from the various biometric characteristics of the user. However, due to their complexity and cost, they are considered ineffective for commercial applications, Li and Jain [122].

2.5.1 Information Fusion in Multibiometric Schemes

The concept of multibiometric integration and the selection of a convenient fusion model is a challenging task, Meva and Kumbharana [143]. The design of a multibiometric system is governed by several factors including the selected sources of information, the acquisition and processing sequences, the types of combined information and mostly the fusion strategy to be employed, Ross and Jain in “Information fusion in biometrics” [180]. Data fusion in multimodal systems is an active research area with numerous applications. Fusion for multimodal architectures constitutes a way to solve the disadvantages of unimodalities and to enhance the matching accuracy of the system without

requiring additional measurements or techniques, but only using the biometric features, Sasidhar et al. [188]. The different approaches for the fusion of biometric information in multibiometric designs are presented below.

Sensor Level Fusion. Fusion at this level involves the consolidation of user's biometric data presented by multiple sources before the fresh traits are subjected to the feature extraction algorithm. This technique can benefit multi-instance and multi-sample systems that capture multiple forms of the same biometric feature, Ross and Jain [180]. For this procedure, the sensor interface is designed in a way that can avoid rotational offsets between the slices in order to reduce the complexity. This means that it is possible to construct a 3D face texture by combining the evidence presented by 2D texture or 3D range images. According to the experimental analysis of Ross et al. [182], the novelty of this approach is the generation of a spherical projection that is efficient when there is a head motion in both the horizontal and vertical directions. Thus, the matching computation is more accurate in comparison to the unimodal facial schemes that use a single template image.

Feature Level Fusion. Information fusion at feature level consolidates the data extracted and presented by the biometric feature sets of the user. If the datasets belong to the same characteristic and originate from the same extraction algorithm then the feature level fusion can be used to update the template. However, the combination of feature sets that are products of dissimilar biometrics and follow different extraction algorithms is not a trivial task, Xi et al. [224]. The incompatibility of non-homogenous measures demands the applicability of a normalization technique in order to handle the fixed length feature vectors and to perform computations on modalities that result in a different range. The augmentation of the vectors arising from the extractors is also included in the process while the final step is subjecting the vector to a transformation algorithm. The correlation between the main inputs has to be examined, in order to evaluate the improvements in matching performance, Hamad et al. [85]. In spite of its complexity, this method is applicable in multimodalities and it is effective for multi-algorithm and multi-sensor schemes.

Score Level Fusion. In this level of fusion, matching scores are returned by each individual subsystem and the obtained output results are combined. However, it is necessary to use specific normalization techniques in order to achieve uniform matching scores from distinct sensors, uncorrelated unimodal data and different extraction, representation algorithms. State-of-the-art research presents a large number of normalization mechanisms. Score level techniques are classified into three main subcategories: density-based, transformation-based and classifier-based schemes, Ross and Jain [180]. The performance of each scheme depends on the quantity and quality of the available information. Score level fusion, also known as fusion at measurement

or confidence level is a popular and widely used technique in current multimodal biometric architectures due to its reliability, Ross et al. [182]. It provides an improved recognition performance in comparison to other methods, while it allows an easy integration for modalities extracted by disparate sensors, Jain et al. [101]. Recently, Tiwari and Gupta introduced a score level fusion scheme and tested it for different biometric datasets [206]. Their experimental evaluation presents a strong authentication accuracy with low error rates in comparison to the performance of the unimodal subsystems.

Decision Level Fusion. This level of information fusion is termed as such because it depends on the final acceptance or rejection decisions. This type of fusion strongly depends on the application and the functionality of the involved subsystems. Gathering the information by the independent components of the scheme, and fusing the results, constitutes an approach to increase the overall precision, supporting the idea of universality in multimodal architectures, Podio [166]. However, this fusion method presents several inconveniences that reduce its applicability in multimodal applications. Techniques proposed in the literature include the Daugman rules, majority voting conditions, Bayesian decision, the Dempster-Shafer theory of evidence and behavior knowledge space that present high values of FAR and FRR, resulting a lower accuracy according to the findings of Rathgeb and Busch [172], Tao and Veldhuis [203]. The research in this area is still immature, while recent works study the approaches for fusion at the decision level for the incorporation of multiple soft biometric characteristics into a multimodal system for its applicability to biometric identification systems, Cavoukian and Stoianov [48] and Guo et al. [80].

Figure 2.6 illustrates the levels of information fusion and the recognition stages in multibiometric designs. The evaluation of a system that incorporates multiple biometric features is complex and requires the user's cooperation. Compact multibiometric templates need to be generated, offering in this way enough information of high quality for the recognition of the user. In the literature, there are many approaches for fusion of biometric data in multimodal recognition schemes and the majority of them are still on a theoretical level. The most important limitation for the evaluation and consequently the applicability of fusion techniques in real-world schemes is the lack of available for examination datasets. This problem is especially pronounced in the case of a biometric system operating in the identification mode with a large number of enrolled users. Moreover, the European Regulatory Technical Standards for Strong Customer Authentication [183], following the new European GDPR [66] underlines the necessity to address the concerns for user privacy when his multimodal data are stored in Centralized Biometric Databases (CBDBs). Finally, the precision of the multimodal model distributions and the evaluation of the overall accuracy are still intricate issues, Lejbølle et al. [119].

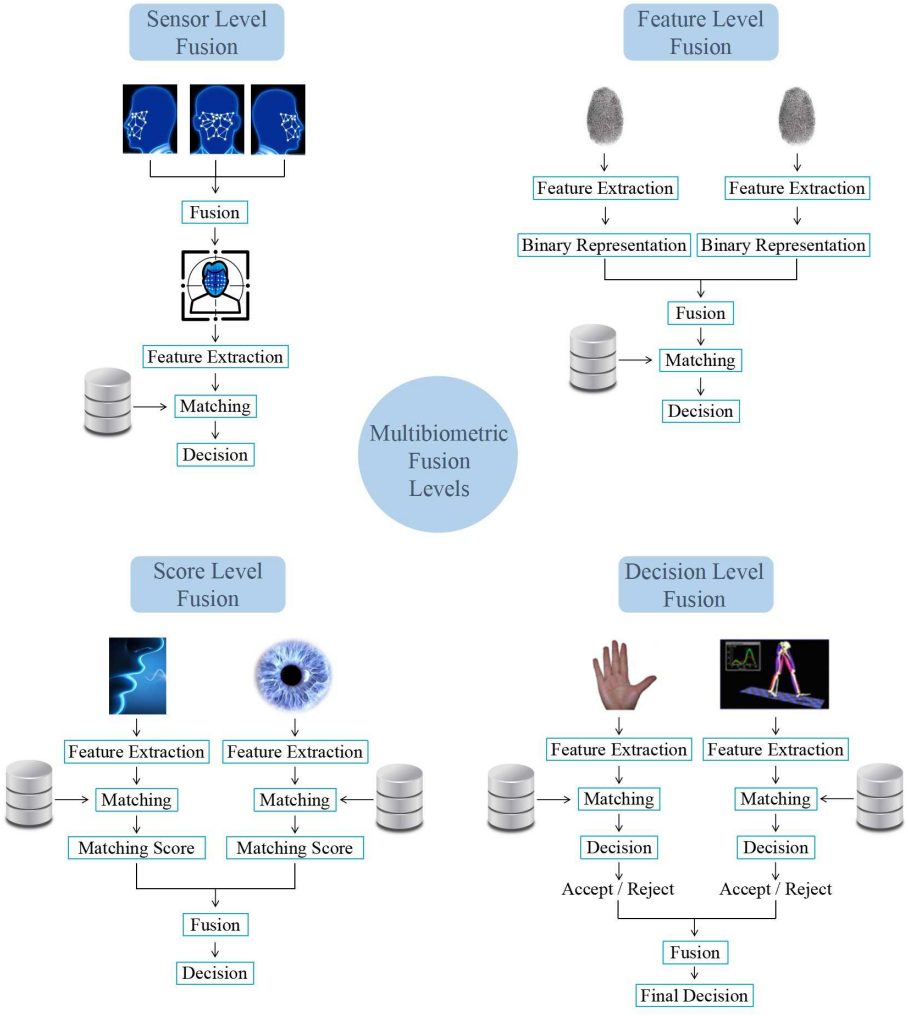

Figure 2.6: Levels of information fusion in multibiometric designs.

2.6 Evaluation of Biometric Systems

From an engineering perspective, the evaluation of biometric schemes is a challenging task. In order to gain a thorough understanding of the performance accuracy of a biometric system, we need to consider the effectiveness of the data extraction, representation and matching techniques, Jain et al. [98], Maltoni

et al. [131] and Ross et al. [182]. Additionally, we need to assess the risks regarding the privacy of the users and examine the robustness of the currently used cryptographic methods in the application domain where the scheme is about to be embedded, di Vimercati et al. [63]. In this way, we will be able to provide the tools for privacy-by-design approaches in biometric recognition that follow the legal framework for the protection of private data, Kindt [115]. Campisi et al. [40], Kindt [116] and Phillips et al. [165] underline that there is no evaluation framework to study these issues in a systematic manner. However, in concrete terms we need to address the following questions:

- What is the optimum matching algorithm and how efficient can it be applied to encrypted biometric data?
- What is the impact of specific complications such as the sample population and data collection environment on the performance accuracy and the scalability of the design, during the experimental studies on representative standardized biometric DBs?
- What is the accuracy of the technical performance of the biometric system in a given application?
- What is the user acceptability of the system? How does the architecture address the human factor issues such as user habituation?
- What level of security does the biometric system provide to the application in which it is embedded? How effective is the applied cryptographic technique to protect the biometric data?
- What are the security limitations of the biometric system? How we can perform a complete risk assessment and map the vulnerabilities under realistic scenarios?
- How does the system address the privacy concerns of its users regarding their personal information?
- What are the technical and practical constraints to preserve privacy with respect to the recommendations of the legal framework for the protection of biometric data?
- What is the availability and maintainability of the system?
- What is the cost and throughput of the biometric system and what tangible benefits can be derived from its deployment as a return on investment?

Our contribution. In this thesis, we are mainly focused on multimodal designs due to their efficiency, practicality and applicability in the next generation high security biometric systems. However, our research included approaches for user authentication based on unimodal biometrics and multi-factor schemes. It is noted that the number of methodologies for the data extraction, collection, representation and the available in the literature matching algorithms is

quasi endless. Studies on how pattern recognition techniques can improve the performance reliability fall outside the scope of this thesis.

Performance rates are important indicators for a biometric design while they define its accuracy. Moreover, fusion of biometric modalities is a challenging task for the functionality of a secure multimodal design. In a fusion model, the performance rates can be applied in such a way that different weights are assigned to the various modalities on a user-by-user basis, Ross et al. [181]. In our works [208] and [209], we showed how these rates can be applied in fusion strategies to increase the performance accuracy of multimodal designs. In these studies, presented also in Part II, we exploited score level fusion approaches and we analytically presented their advantages related to the performance improvement and the security targets of our proposed recognition schemes. Finally, we introduced in [207] a system for remote multimodal authentication. Hamming Distance techniques and a user-specific weighted score level fusion method were used in order to incorporate unimodal datasets of three biometric modalities (face, fingerprint, iris) into a final fused result for user recognition. Our experimental analysis justified our selection of this fusion approach in terms of computation efficiency, cost and reliability.

Chapter 3

Methodologies for the Protection of Biometric Data

In this chapter, we present an overview of the mechanisms for securing biometric architectures. Security issues are defined while we also discuss how spoofing attacks in biometric recognition schemes differ from other vulnerabilities. Additionally, we address the topic of biometric data protection from a privacy perspective discussing the privacy principles and requirements. We analyze the cryptographic approaches that have been developed to prevent impersonation and the exposure of biometric information with respect to security and privacy while we also present our conducted research and contributions.

3.1 Vulnerabilities of Biometric Systems

In 2001, the main security concerns related to biometric-based recognition designs were highlighted, Ratha et al. [171]. Since then, a complete collection of targeted attacks has been presented and it has been shown that a system can be vulnerable either due to an intrinsic failure or because of intentional attacks, Linnartz and Tuyls [125], Rathgeb and Uhl [174].

For the vulnerabilities related to the intrinsic failures, accuracy and robustness are the main performance metrics of a biometric architecture, as explained in Section 2.4. This means that a system that is characterized by a high FAR is very prone to be breached since it is likely to accept an attacker with an arbitrary biometric feature. Performance metrics are usually related to intrinsic

failures or referred to as zero-effort attacks, Jain et al. [100]. However, this fact depends on the quality of the biometric modality and the applied extraction, representation and matching algorithms. This justifies the selection of specific types of biometrics, such as face, fingerprint and iris data due to their properties and reliability for security demanding applications in order to avoid as much as possible potential intrinsic failures.

Secondly, Figure 3.1 illustrates the most common intentional attacks that can take place against the building blocks of a biometric authentication scheme, adapted from Campisi [39].

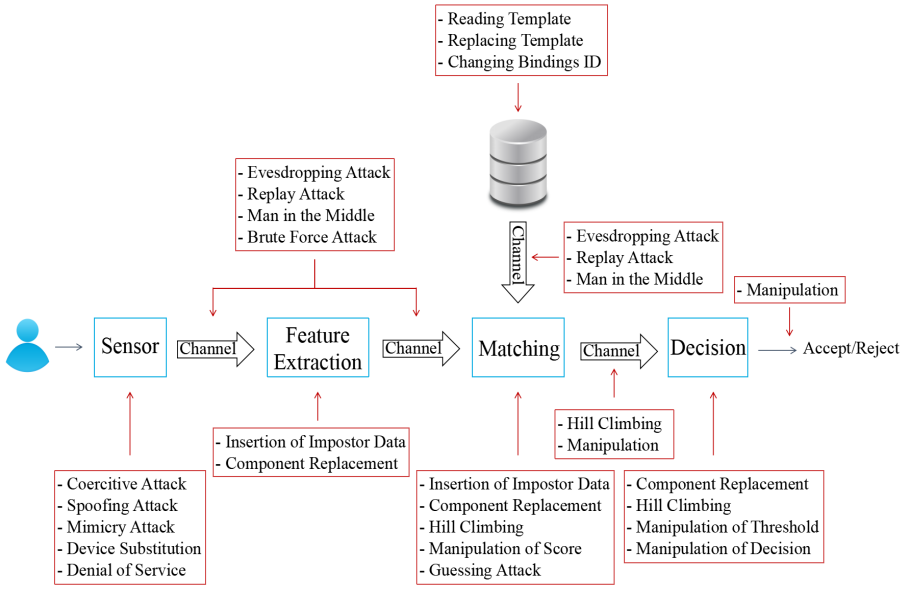

Figure 3.1: Attacks in biometric authentication schemes.

- **Sensor**: Attacks aimed directly towards the biometric sensor are usually referred to as *direct attacks*, Martinez-Diaz et al. [139]. A *coercitive attack* may happen when a true biometric is presented by an impostor who forces a legitimate user to grant him access to the system. *Spoofing* and *mimicry attacks* are related to the reproduction of the biometric features of an enrolled user by means of different strategies that are presented as inputs by an impostor in order to fool the system. *Device substitution* is referred to the substitution of a legitimate biometric device with a modified or replacement capture unit. Finally, *denial of service* is another mode of attack in which an impostor overwhelms the biometric system with massive requests.

Consequently, a system can be loaded with so many access requests, to a point that may cause its failure while all the involved computation subsystems can no longer handle valid users.

- **Feature extraction**: This process can be forced by an attacker to produce preselected biometric features by an *insertion of impostor data* or a *component replacement* which is referred to the substitution of either the software or hardware components of the system in order to control its behavior and produce specific feature sets.
- **Database**: The stored templates can be either local or remote. The data might be distributed over several servers. At this level, an attacker may try to *read the templates*, *replace/modify* one or more stored records in the DB or *change the links* between the biometric data and the users' personal credentials such as name. These may cause the acceptance of an intruder as an authorized user or the denial of the service to the enrolled persons associated with the corrupted templates. Attacks on biometric DBs are seen as very serious as they are related to the user privacy, Yang et al. [227]. As presented in Section 3.3, several mechanisms can be found in the literature as a primary goal to enhance the security of stored biometric templates.
- **Matching process**: The matcher can be attacked or corrupted in order to produce preselected scores. This can be achieved by *inserting impostor data*, *replacing a component* or *manipulating the match score*, where an intruder inserts or changes the values of the score by manipulating the computational result or by substituting the software/hardware components of the system before the final decision. *Guessing attack* and *hill-climbing* are referred to as iterative attacks that can be performed when an intruder, given an input, constantly tries to modify the score in order to surpass the decision threshold, Maltoni et al. [131]. State-of-the-art research present numerous approaches for enhancing the security of unimodal and multimodal biometric authentication schemes against hill-climbing attacks, Higo et al. [87] and Maiorana et al. [129].
- **Channels**: Channels interconnecting the sensor and the feature extractor or located between the feature extractor and the matcher can be intercepted and controlled by an attacker. In an *eavesdropping attack* an intruder listens to the transmission of the biometric data. In a *replay attack*, a recorded signal is replayed to the system, bypassing the sensor. In a *man in the middle* attack, an attacker is able to manipulate the feature sets exchanged between two parties without the parties knowing that the link has been compromised. In local authentication designs the two stages of feature extraction and matching are inseparable and this attack is considered to be extremely difficult, Bhattasali et al. [21]. However, if the data are transmitted to a remote matcher this mode of attack can be a serious threat to the biometric system, Peer et al. [163] and Uludag et al. [217]. Moreover, a *brute force*

attack is an exhaustive search over the space of biometric inputs in order to find those that match with the user's biometric data. The channel between the stored templates and the matcher can be attacked when the biometric templates are sent to the matcher through a communication channel that it is subject to interception or modification. Finally, the channel between the matcher and the final stage of decision may be attacked through a *manipulation of the match score* by capturing or changing the value of the matcher, or by performing a hill-climbing attack to achieve an optimum match score before the final decision.

- **Decision**: Overriding the final decision can take place by an attacker who performs *manipulation of the decision score* at the final level of a biometric verification scheme. Even if the actual pattern recognition framework presents an excellent level of accuracy, it may be rendered useless by this type of attacks, Li and Jain [122].

3.1.1 Spoofing Attacks and Countermeasures

The indirect attacks are performed inside the system and they can be prevented by firewalls, anti-virus software, intrusion detection and encryption mechanisms that are presented in Section 3.3. However, direct attacks at the user interface level are outside the digital limits of a biometric deployment and therefore, no digital protection mechanisms can preclude it, Marcel et al. [136]. Spoofing at the level of the stored templates are the most dangerous type of attacks, Podio [166]. Unlike the DB, a sensor can be attacked without advanced programming techniques, posing serious threats to the security and the privacy of the enrolled individuals, Cavoukian and Stoianov [47]. A spoofing attack occurs when an impostor tries to masquerade as a valid user by presenting a stolen, replicated or copied forged biometric feature to the sensor. Systems using face, fingerprint, or iris patterns (the modalities adopted by ICAO) can be spoofed relatively simply using, for example, three-dimensional shaped models or falsification of facial characteristics using make-up or plastic surgery, silicon gummy fingerprints and contact lenses, Chen et al. [50], Hadid et al. [82] and Matsumoto [140]. The increasing popularity of social media where the photographs of the users are publicly available presents an advantage to the cheaters who can gain access to high-resolution photos; this helps them to fool a great variety of the most robust biometric devices, Pereira et al. [60]. Finally, speech and voice modalities and soft biometrics including gait and handwriting have been found prone to spoofing attacks, Chingovska et al. [51] and Hadid et al. [83].

Identity theft and fraud are widespread problems with serious consequences related to the ethical, legal or policy standards and the acceptability of biometric applications, Rebera et al. [176]. Since biometrics affect millions

of users, anti-spoofing technologies need a thorough study. However, spoofing is a difficult problem to address since the major objective is not only to detect and prevent these attacks, but also to establish countermeasures that can ensure the protection of user's information and guarantee the trustworthiness of the design, Marasco et al. [135]. Multimodal recognition is one of the approaches that has been experimentally proven more secure against spoofing attacks, contrary to the designs that implement a unimodal biometric or multi-factor combinations, Biggio et al. [22]. However, according to the the analyses of Akhtar et al. in [9] and Rodrigues et al. in [179] the lack of robustness can be the major drawback of multimodal systems. This depends on the selection of a fusion model and the applied matching algorithms to compute a final multimodal result. The issue is still an open research question, while recent studies focus on the multimodal combinations and new score level fusion rules to enhance the security of multimodal recognition designs, Jomaa et al. [105] and Luckyanets et al. [127].

Furthermore, *liveness-detection* is the most common technique to detect physiological signs of life and recognize whether a biometric feature presented at the sensor belongs to a living subject, discriminating a real human trait from an artifact, Marcel et al. [136]. Several passive and active approaches have been proposed in the literature, including the use of additional hardware means to acquire temperature, pulse detection, blood pressure etc., and software means to provide high-resolution images of the extracted biometric data, to detect liveness information inherent to the obtained feature and to analyze multiple captured instances of the same trait, Li and Jain [122]. In the last few years, *challenge-response* active methods have been added to the research agenda. In this approach the user is asked to interact with the system, i.e., to move his head or to roll a finger across the sensor among others, Beham et al. [16], Chugh et al. [53], Okereafor et al. [153] and Singh and Arora [196]. Liveness active and passive analysis based on spoofing detection can offer promising results although they have not yet been extensively studied on large-scale datasets, Akhtar et al. [10]. Their practical disadvantages include an additional cost of the hardware scanner, a time-consuming authentication process, and an increase of the FRR percentage where genuine users may be rejected as impostors, Sohankar et al. [197]. These facts may affect applicability of liveness-detection techniques in commercial designs in a negative way.

Our contribution. We investigated the vulnerability of fingerprint-based schemes against several attacks including fingerprint obfuscation and impersonation. Based on datasets of spoofed samples, which are publicly available for research purposes, we analyzed the system's performance in terms of accuracy and we addressed how security can be preserved under realistic scenarios. Additionally, we focused on a bimodal system, consisting of fingerprint and

facial biometrics, to study the robustness of a typical multimodal design against spoofing attacks. Our analysis presented in [212] showed that multimodal schemes can be affected by attacks against a single biometric trait, while the FAR probability mainly depends on the applied fusion technique. For this reason, fusion plays an important role to attain an optimum trade-off between performance and robustness.

Furthermore, we analyzed why an anti-spoofing method should not be designed to operate as a stand-alone procedure. We mainly examined challenge-response approaches on unimodal and multimodal architectures and we conducted a theoretical analysis on how they could be applied in real-world use cases. We concluded that in order to improve the robustness of multimodal systems, it might be necessary to integrate the user's match score with the scores provided by the liveness detectors. Finally, in the context of the FIDELITY Project [67], we examined the effectiveness of challenge-response methods for secure automated border control applications. The infrastructure of the ePassport identification documents requires secure data transmission, encrypted information storage and high accuracy rates. We analyzed the robustness against identity theft if additional security measures are implemented. In [211] presented in Part II, we summarized our findings and we proposed a multimodal authentication framework for ePassports based on our theoretical analyses and motivated by the functionality of eGates at the immigration checkpoints in arrival halls of airports. Our model was designed to combine two modalities using a score level fusion; it used a Radio Frequency Identification (RFID) subsystem and a liveness detection function to offer increased security.

3.2 Security and Privacy in Biometric Designs

From fingerprint scanners, embedded in smartphones, to border control infrastructures, the use of biometric technologies has increased security and privacy concerns. The major security and privacy threats related to biometrics have been described extensively in the literature, Kindt [116] and Prabhakar et al. [167] among others. However, security and privacy in biometric schemes are seen as two different, yet complementary fields, Campisi [39]. Cryptography has become a powerful tool to address the potential vulnerabilities of biometric recognition schemes, enhancing their robustness, Menezes et al. [142]. However, a central question is whether a biometric trait can keep its source secret. The use of biometrics can raise cultural, religious as well as ethnicity related concerns, Li and Jain [122]. To some extent, biometrics are related to the loss of anonymity, while it is a common belief that even when a biometric-based recognition procedure is performed by a legislative authority, the collection and use of

such a personal data unjustifiably violates the human rights to freedom and autonomy, Podio [166]. This debate has been occurring for many years and will continue until the public is completely satisfied with how the implementations of biometric systems protect their interests and to what extent they affect their private lives, Kindt [115]. Over the last years, there is an increased awareness in the need for security and privacy requirements for the protection of biometric data both in civilian and commercial applications. Through legislation, national and international organizations emphasize the importance of *privacy-by-design* in biometric deployments. The concept refers to the approaches that combine encryption techniques in accordance with both the security recommendations and the privacy principles from the early stage of the design, Cavoukian [45]. Requirements as described below have been developed for privacy-friendly biometric systems. For a detailed analysis, we refer the reader to Breebaart et al. [34] and the ISO Standards for the protection of biometric information [92] and [96].

3.2.1 Security Requirements

Security for biometric architectures is related to the technical characteristics of the system and its overall robustness against the vulnerabilities presented in Section 3.1. We first introduce some terminology. A *biometric reference* is the template that includes the binary representation of the biometric data belonging to a user that can be used to recognize him in biometric applications. An *identity reference* are the user's credentials such as name, address etc. A user may have several non-biometric identity references as a combination of attributes that uniquely identifies the entity in a particular system context. The security of a biometric design revolves around several fundamental requirements that are presented below.

Availability. The requirement is referred to the security mechanisms and controls that should be established in order to guarantee that every part of the system is available when this is necessary in order to protect the system from accidental failures and physical or network attacks.

Entity Authenticity. This requirement ensures that all the entities involved in the processing are the ones they claim to be.

Data Authenticity. This requirement includes the authenticity of the *data origin* and the *data integrity* as explained by Menezes et al. in [142]. Data origin ensures the genuineness and the originality of biometrics. Data integrity is the condition that guarantees that the data are consistent, accurate and correct. Security measures offering integrity can also ensure that modifications

are detectable at all the software and hardware components involved in the biometric system.

Confidentiality. It ensures the secrecy of user data. No information when biometrics are captured, templates are generated, transferred and stored should be revealed to unauthorized parties. This also means that the templates should be protected from any illegal access. The challenging issue is that the computational parties involved in the matching process need access to the biometric references.

Non-repudiation. This requirement guarantees that the involved parties in a biometric system, including the user, cannot deny that they have performed a certain action. It also provides evidence for the entities and components that took place in an action and for the messages that have been sent. As described below, it is related to many privacy principles in order to ensure the trustworthiness of the recognition procedure and the biometric architecture.

Non-invertibility/Irreversibility. The property refers to the application of one-way functions to create a secure template with the user's biometric references such that knowledge of the transformed biometrics cannot be used to obtain any information on the original biometric input, Ngo et al. [151].

Unlinkability. This property indicates that multiple biometric references (transformed templates) from the same user cannot be linked to each other or to the user from which they were derived. It is also related to the entities involved in the matching process. This means that in an unlinkable biometric system, it should not be possible to derive any further information on the relation between the parties, Simoens et al. [194].

Permanence. It determines the validity period that correspond to a set of stored templates and protected identity references.

Cancelability/Revocability. In case the security measures detect attack(s) in the biometric system, the risk of compromised templates can be mitigated by providing methods to cancel a biometric template in order to prevent future successful verification of a specific biometric reference for a given user's identity.

Renewability. It guarantees the creation of new multiple, independent transformed biometric references derived from one or more biometric samples from the same user. It permits their use to recognize the individual without revealing information about the original biometric input or the already stored templates. From a practical perspective, this security requirement is considered very challenging as it is related to revocability, indicating the necessity for several biometric references to allow an automated user's re-enrollment in biometric systems. In this way, the presence of the user for the re-enrollment procedure can be avoided. The property also ensures the users' data update after a time period

and offers a certain security level when the user utilizes the same biometric features to access several applications.

3.2.2 Privacy Principles

Security requirements are not considered to be a solution in and of itself, Gerber and Zimmermann [74]. For every given technology, the legal framework establishes the criteria for the configuration of a process, tool or system, Bertino [19]. Given that the processing of each individual's private information is an essential criterion for the applicability of a biometric scheme, the system needs to address the protection of biometric data. Additionally, a common toolkit specifies the privacy metrics to avoid any misunderstanding among developers and users. For biometric designs, Data Protection Authorities specify the following information: the formats for the interchange of biometric information, the platform independence, the program interfaces, the application profiles, the calculations and the methods for evaluation, Cavoukian [45]. Hence, the architecture is neutral, without being in favor of any particular vendor or biometric modality. Even if it is difficult to categorize the properties as security requirements or privacy principles, the concept of privacy for biometric architectures is defined as the ability of the user to control by whom and how his personal data is collected and used, Kindt [115]. In practical terms, user privacy in biometric application is determined by specific requirements knows as *privacy principles for biometric schemes*. In Europe, as described by the ISO Standards in [92] and [96] and addressed by the recent GDPR [66], the main objectives of the privacy principles for biometric architectures are the following:

Consent, choice and respect to the application context. The legal framework defines that the biometric data must be only used for the predefined purposes of the biometric application. Moreover, the choice whether the system performs identification or authentication functionalities requires an explicit legal guideline. This is also depended on the sector (government civilian applications or commercial applications) in which the biometrics are applied. This sector determines the responsible authority for the legal extraction, processing and storage of biometric references. The concept of consent is based on the fact that the user holds the biometric data and he is well informed about their processing and the scope of the biometric applications. Privacy principles recommend that the storage of biometric data in CBDB should be avoided since it implies additional privacy threats, Yang et al. [227]. However, if this process is considered to be necessary, the biometric scheme should exclusively perform authentication, being compliant with the recommendations of the European Regulatory Technical Standards for Strong Customer Authentication [183].

Transparency and Accountability. The privacy principle of transparency provides the users with meaningful notices about how the organizations responsible for the biometric extraction, transmission and storage intend to use the biometric technology in the specific application. Additionally, the users must be informed about the encryption mechanisms that will be applied to prevent the exposure of biometric data and the accuracy of the system related to the error rates that may lead to its failure. Accountability is referred to the reasonable steps that should be taken to ensure that all the parties involved in the computation adhere to the principles presented above, Campisi [39].

Discriminability. Biometric references that disclose physiological or pathological medical conditions, such as the retina patterns of the human eye that can reveal health information and behavioral biometrics which are related to neurological diseases, must not be used for unintended functional or application scopes without the permission of the user who wishes to be recognized, Campisi et al. [40]. This principle implies that the new GDPR [66] guarantees the user's control over his private data by prohibiting any covert identification procedure such as surveillance applications based on soft biometrics for individual identification in a crowd. It has also an international impact since organizations established outside the EU are subject to the GDPR [66] when they process personal data of EU citizens.

Accuracy and Rectification. These principles require that the personal data must be accurate and they should be kept up to date. They are related to the security recommendations of revocability and renewability which should be established to ensure that every reasonable step has be taken to guarantee that biometric data which are no more accurate or considered to be incomplete are erased, canceled or rectified.

Minimization and Limitation. Minimization determines both the amount of the biometric data and the scope of the biometric applications. Data usage should be limited to what is necessary while biometrics must be collected for specified, explicit and legitimate purposes. The biometric references should be adequate, relevant and limited to what is necessary. For example, the use of images for facial recognition and the use of templates, even if they are encrypted, which include complete fingerprint information instead of minutiae points (minimal data) are prohibited, Gray [79], Palanichamy and Marimuthu [161]. The principle of limitation prohibits processing for the purpose of uniquely identifying a natural person if consent has not been given explicitly. However, this procedure is allowed in the field of employment, social security, social protection law and for reasons of public interest in the area of public health if the principle of minimization is preserved. This means that if consent is not feasible for a group of users, then additional steps are taken to address the concept of minimization either by minimizing the use and impact of the examined biometric technology

or if this not possible by using minimal data as biometric references for user recognition.

Anonymity. To reduce the privacy issues of linking transactions or identity references across DBs or applications, the legal framework determines the principle of anonymity. Anonymity can be achieved in practice by combining the security recommendations of non-invertibility, unlinkability, cancelability and renewability. Regarding the user, anonymity stands for the fact that he should be indistinguishable within a set of subjects or a particular group of individuals. The term also refers to the parties and recipients of biometric and identity references involved in a biometric system to jointly compute a matching process. It characterizes an unknown authorship, lacking distinction or recognizability within the anonymity set by reducing the likelihood to be identified as an originator, Breebaart et al. [33].

To conclude, it is underlined that the term of privacy for biometric designs is characterized by the effectiveness of the users' control over their own personal data. This fact is related to the properties of biometric data and to both the security requirements and the privacy principles and how these are addressed in a biometric architecture. Although a complete evaluation framework is still not available, our analysis in Section 2.6 can be used as a guidance tool.

3.3 Cryptographic Mechanisms for Biometric Designs

This section presents the cryptographic approaches that have been proposed to enhance the security of biometric designs. The objective of the applied cryptography in biometric architectures is to protect pieces of personal data. This biometric reference has to be used for comparison with another similar yet different template which includes the binary form of the extracted user's information created after the enrollment procedure, Hao et al. [86] and Menezes et al. [142]. However, at the matching process it should be possible to compare unprotected with encrypted data. This fuzziness of biometric features renders the traditional data protection techniques ineffective for biometric computations, Kanade et al. [109] and Tuyls et al. [216]. Recent reports evaluate the applicability, usability and security issues of widely used approaches (e.g., implicit authentication protocols) and they discuss why they are considered impractical for high security and privacy-preserving biometric recognition systems, Bringer et al. [35], Kaur and Khanna [111], Khan et al. [114], Pagnin et al. [157], Safa et al. [184] and Saraswat et al. [185]. Biometric data protection is a well covered topic in the literature. Below, we present a compact survey

on cryptographic mechanisms for secure unimodal and multimodal biometric deployments. The overview is by no means exhaustive but it is important to provide the reader with the background that is necessary for the remaining of this thesis.

3.3.1 Basic Protection Techniques for Unimodal Schemes

It is noted that many authors adopt the term *biometric template protection* to describe all the methodologies that can be used to protect the templates of biometric information. However, we believe that this classification is not exclusive since a method can draw upon more than one approach (*hybrid protection model*) in order to comply with the security requirements and privacy principles discussed in Section 3.2. In this thesis, we use the term *cryptographic mechanisms* to categorize the state-of-the-art research on secure biometric technologies according to their functionality and purposes to effectively address the vulnerabilities presented in Section 3.1. Figure 3.2 illustrates the basic techniques to protect the biometric references. These approaches were initially introduced for the protection of unimodal biometric templates. We proceed to analyze their functionality and discuss their applicability in multimodal architectures.

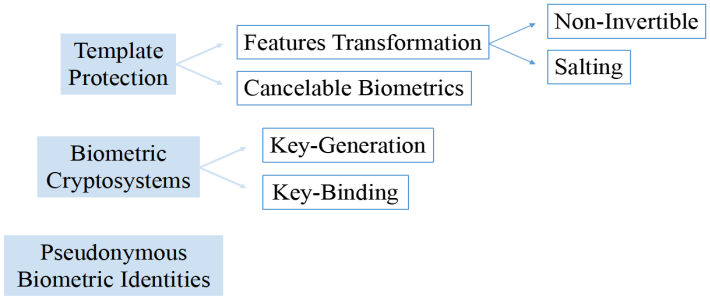

Figure 3.2: Categories of the approaches for the encryption of biometrics.

Features Transformation. *Biometric template protection* refers to the encryption of biometric templates including the user's biometric references to preclude attacks at the level of the DB, Jain et al. [100] and Ngo et al. [151]. During the enrollment phase, an algorithm transforms the data extracted from the captured biometric features before their transfer and storage. The transformation may have different characteristics and use secret parameters such as auxiliary data (AD) (e.g., key, password or PIN code). Thus, the template stored in the DB is strongly protected in order to make it infeasible to

retrieve the genuine biometric feature from the template, Campisi [39]. For user authentication, the new template is also transformed in the same way as the stored template and the matching process occurs in the transformed domain. Depending on the characteristics of the transformation, the approaches can be further divided into *non-invertible* and *salting* methods, Choudhury et al. [52]. The first category applies a one-way function to the unprotected data such that it is computationally hard to recover the initial user's biometric data. This is also true even if some of the parameters of the transformation function would be revealed, Lim et al. [124]. Salting transforms combine a user-specific key with the biometrics such that the protected template cannot be obtained without the knowledge of the key. This implies that identical biometric data sets may lead to multiple templates. Salting methods are multi-factor approaches by definition and the literature offers several works that aim to reduce the security issues of a potential compromise of the AD, Karabat and Topcu [110].

Cancelable Biometrics. The security requirement of cancelability in biometric systems, is related to the privacy of the user, while it implies that the biometric architecture should provide a mechanism for authentication even when the biometric template is compromised or stolen, Kindt [115]. Cancelable or revocable biometrics were introduced as the first privacy-preserving mechanism for biometric schemes that respect several properties for the protection of user privacy, Ratha et al. [171]. The philosophy is more or less the same as the non-invertible approaches of the features transformation technique. The original biometric features are distorted intentionally and a deformed version of the template is stored in the DB. In contrast to features transformation, the mechanism of cancelable biometrics allows the generation of multiple transformed biometric templates, offering higher security levels and addressing the practical issues and concerns related to linking users across different applications as analyzed by Bhattasali et al. in [21], Cavoukian et al. [46] and Rathgeb and Uhl [174].

Biometric Cryptosystems. Biometric cryptosystems or crypto-biometrics belong to the second category of privacy-preserving techniques for the protection of biometric information. The two main models are named after their role as *key-generation* and *key-binding* schemes, Uludag et al. [217]. In both approaches, some public information known as helper data (HD) is transmitted and stored to set up not only a protected storage of the templates but the complete process of extraction and transmission. HD consist of a key bounded to a biometric template and some supplementary information. HD are not always required to be secret since it is computationally hard to derive any private information about the user's biometrics. However, their authenticity has to be protected, Adamovic et al. [6]. For key-generation schemes, biometric features are used to directly create a digital secret. In this approach, HD are derived from the

extracted biometric feature set and the cryptographic key is generated from both the HD and the biometric template. The generated keys are shared with the involved entities and they are used to secure all the communication channels. The state-of-the-art presents a variety of approaches under the names of as fuzzy extractors, Dodis et al. [65] and secure sketches, Linnartz and Tuyls [125] and Sutcu et al. [201]. Key-binding cryptosystems allow only the transmission and storage of information coming from the combination of biometric data with randomly independent external keys. In this case, the keys are non-biometric elements, such as a PIN, a password or a credential with certified attributes. Crypto-biometrics rely heavily on the use of error-correcting codes to correct errors from noise and intra-class variations, Li et al. [121]. Further analysis is outside the scope of this thesis and we refer the interested readers to the works of Davida et al. in [59], Sarier in [186] and Simoens et al. in [195]. It is noted that research into this direction has offered promising results regarding security and overall performance. Key-binding approaches appear in the literature as fuzzy commitment schemes, Ignatenko and Willems [89], fuzzy vault designs, Juels and Sudan [107] and shielding functions, Li and Jain [122].

Pseudonymous Biometric Identities (PIs). In 2008, the partners of TURBINE European Project [215] proposed the technique of Pseudonymous Biometric Identities (PIs). The mechanism has been considered as a privacy-by-design cryptographic approaches for biometric designs, Breebaart et al. [33]. It utilizes non-invertible functions, to create PIs from the user's extracted biometric data. For higher levels of security, the scheme requires the presence of a password or a credential that are used as supplementary auxiliary data (AD). Figure 3.3 presents the architecture of the extraction of the PIs from biometric data and how the security requirements of renewability is addressed, adapted from Delvaux et al. [62].

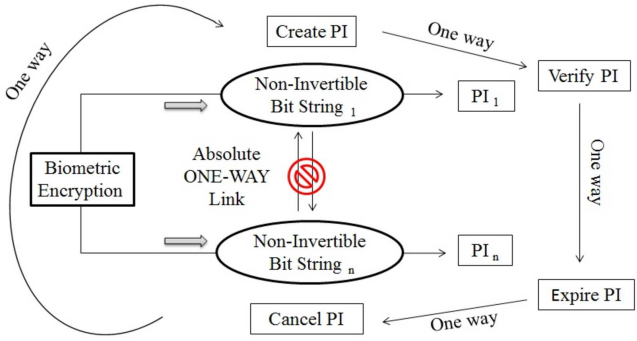

Figure 3.3: Pseudonymous biometric identities derived from biometric samples.

During the enrollment phase, a biometric device captures the user's biometric

features while the user provides a password. Subsequently, an encoder generates the PI and creates additional non-biometric helper data (HD), using as an input only the user's AD. This process is inspired by the functionality of crypto-biometrics. The initial biometric information and AD are destroyed. The design involves the parameters for the separation and individualization of the elements, preventing impersonation and improving the security of users with very similar characteristics, Ngo et al. [122]. HD and PI references are securely stored as different templates in the encrypted domain, such as a DB, card or token. During the authentication procedure, the PI expires, while the scheme can create a new PI for a second recognition. The authentication process can be divided into two different approaches, Gafurov et al. [69]. The scheme can proceed to a direct verification of the PI. The user presents his biometrics at the sensor and enters the password that was presented during the enrollment phase. Given the stored templates of the HD and the PI, a verifier defines the decision result that is communicated to the parties involved in the application. After a successful authentication, user's fresh biometrics and the AD are destroyed. According to the second approach, the user presents his biometric data and provides AD. This information and the stored template of HD are transmitted to a PI recoder, allowing the generation of a new PI. The user's biometric data and the given AD are destroyed. The generated PI and the stored template of the initially created PI are both provided to the application's PI comparator. The final decision is determined by the comparison of the two PIs and the result is communicated to the involved parties. The complete technical analysis can be found on page 100.

3.3.2 Basic Techniques in Multibiometric Schemes

As described in Section 2.5, multimodal biometrics improve the reliability of the recognition systems and offer improved levels of security; this enhances user confidence and increases public acceptance of biometric technologies. However, the protection of multibiometric templates and the complete evaluation of multimodal schemes in terms of user security and privacy is a challenging task, Sasidhar et al. [188]. The applied fusion models and the embedded cryptographic techniques affect the performance accuracy which renders the systems vulnerable to attacks and may lead to further security and privacy threats, Ross et al. [182]. Focusing on the basic approaches for the encryption of unimodal templates, Rathgeb and Busch evaluated the incorporation of multimodal biometrics to template protection and biometric cryptosystems techniques analyzing the advantages and limitations of the proposed strategies [172].

Furthermore, when a user presents his biometric characteristics on a biometric sensor, the scanned template might be distorted and misaligned. Depending on the fusion strategy and the matching algorithm, the biometric system

should ensure that the generated templates are properly aligned. An alignment correction algorithm can be applied before or after the feature extraction procedure and prior to the selection of the cryptographic technique, Li and Jain [122] and Theodorakis [204]. State-of-the-art presents studies focused on the alignment issues in order to effectively address the multimodal template generation and representation, evaluated on different fusion levels and combinations of biometric data, Kelkboom et al. [112] and Sutcu et al. [200] among others. Bolle et al. [30] described how cancelable biometrics can be used as a protection mechanism for multibiometric references taking into account the error ratio, Stoianov [199]. Nandakumar and Jain [148] and Yang et al. [226] proposed novel protection schemes based on the technique of biometric cryptosystems, using alignment methods to increase their applicability in multimodal templates. Sutcu et al. in [201] emphasized the complexity of the crypto-biometric algorithms, proposing solutions to decrease the computation time in order to make multimodal solutions more practical for real-world deployments. To conclude, experimental analyses that have been carried out in different combinations of biometric samples using several cryptographic approaches report a significant improvement of the reliability of multimodal designs, Rathgeb and Busch [173]. However, the practicality of secure and privacy-aware multibiometric schemes is still seen as an open research problem, Wang et al. [221]. This is mainly due to the selection of the optimal fusion rules and the overall performance setting in order to allow secure multimodal recognition, Peng et al. [164] and Islam et al. [170].

Currently, research is focused on the possibilities to establish a cryptographic technique that can offer the security requirements of non-invertibility, unlinkability, and cancelability, Natgunanathan et al. [150]. However, basic protection approaches for multimodal templates have not managed to completely address the properties of renewable biometric templates from multimodal data, Nandakumar and Jain [149]. The design of a generalized encryption framework applied on multibiometric data could be the first step towards this direction, Jagadeesan and Duraiswamy [97]. Several ideas of using a set of multiple biometric features within protection schemes have been proposed. Figure 3.4 summarizes the objectives of these efforts, illustrating a framework for multimodal recognition architectures, adapted from Rathgeb and Busch [172].

The major goal of the design is to effectively address the performance and to apply cryptographic mechanisms that will not be affected by the embedded biometric extraction algorithms, representation techniques and the selected fusion approaches. Additionally, the scheme should allow the extraction of multiple references to maintain unlinkability while offering the advantages of revocability and renewability. One of the limitations that the current design presents is the selection of the fusion strategy. The existing research concludes

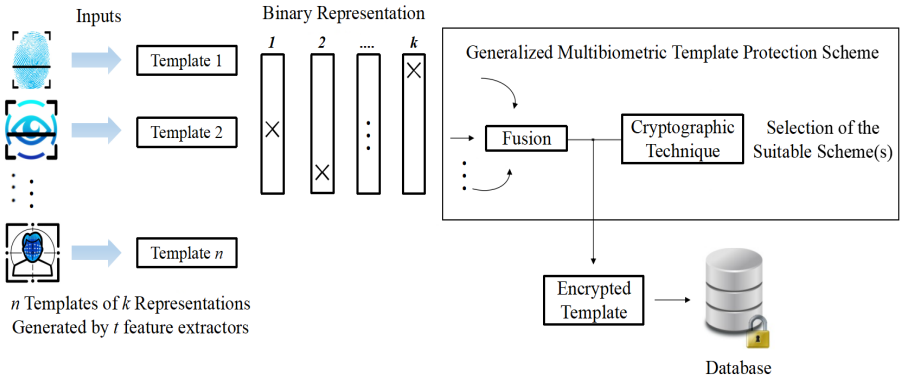

Figure 3.4: A generalized protection scheme for multimodal designs.

that fusion at the feature level, as presented in Section 2.5.1, is the most suitable approach, Rathgeb et al. [175]. In this way, the system is capable of incorporating n templates, addressing the necessity to follow complex fusion rules and a normalization technique for the template generation, where k different binary representations of the biometric feature sets may be involved. After the features extraction and representation the fusion process continues with an applicable fusion algorithm and the selection of a basic or hybrid cryptographic technique. The protection model can be based on template protection and crypto-biometric schemes that are applied to the final fused biometric feature sets and generate the encrypted multimodal templates.

Our contribution. In our work [210], we presented a detailed study on the protection mechanisms for multimodal recognition designs. We discussed the efficiency of the proposed approaches and addressed the security and privacy issues that may arise. We focused on the advantages and limitations of template protection and crypto-biometric techniques, discussing their functionality and practical implementation to multimodal systems. As [210] is not included in Part II of this thesis, we proceed to summarize our findings. Fusion techniques and rules are important factors that affect the performance accuracy and consequently the robustness of a multimodal system. Hence, their selection should be thoroughly evaluated before applying the cryptographic mechanism. The alignment of the multimodal templates is also a non-trivial task. The use of algorithms to improve the alignment of the biometric templates requires some additional primitives. However, the exposure of the parameters of these primitives may compromise the biometric references. Any approach to handle this issue should be carefully selected in order to avoid any information loss and to preserve the protection of biometric data. Moreover, error-correction codes

play a crucial role in multimodal representation and the selected error-correction algorithm should be evaluated to avoid an increase of the FRR that may render the system more vulnerable to attacks at the levels of the matching and decision. Even if a unified protection scheme for multimodal schemes would be valuable, its practicality is still under evaluation. Feature fusion offers adequate performance accuracy. However, it fails to address the address the issue of availability for a certain type of modalities. Additionally, due to its complexity, it is considered ineffective for high security real-world multimodal applications. Finally, we analyzed the security advantages of an approach based on fusion at the decision level, combined with the cryptographic technique of biometric cryptosystems. We discussed the importance of the security requirement for renewability and the directions to address it in multimodal architectures. Our work has offered a tool to address open research questions and it has contributed to the development of privacy-preserving, practical solutions for multimodal recognition systems.

3.3.3 Security and Privacy Analysis of the Basic Techniques

The number of publications on the analysis side of the cryptographic mechanisms and the design of new protection schemes and their applications to different modalities has been increasing in the last years. Research presents numerous approaches and tools to handle the vulnerabilities of biometric encryption techniques. Moreover, empirical evaluations have led to the proposal of new solutions. These approaches have been implemented in minimal data (minutiae fingerprints), multi-factor and multibiometric designs. In [211], we presented a theoretical evaluation of biometric cryptosystems in secure multimodal architectures. We described how privacy can be addressed and we discussed the security advantages of this approach against the attacks at the level of the sensor. Furthermore, our work in [213] discussed to what extent biometric designs can be characterized as Privacy Enhancing Technologies (PETs). We analyzed and compared the existing approaches that address security and privacy in biometric designs. Below, we summarize our findings.

The technique of features transformation offers a minimum level of security. However, it is seen as the basis for the template protection technique of cancelable biometrics. The mechanism can be applied in unibiometric templates and minimal data, while for multibiometric designs that require the selection of a fusion strategy, non-invertible can be efficiently applied. However, salting approaches for multimodal schemes are not considered as an efficient solution due to the complexity and the reduction of the overall accuracy. The experimental analysis of Nandakumar and Jain [149] concluded that complex transformations may reduce the authentication performance. This is a common problem for

transformation approaches that is mainly caused by the information loss and the difficulty in the alignment of the templates.

Cancelable biometrics present several advantages as they can be applied to unimodal and minimal data. The main advantage of this technique is that it provides a larger number of protected templates from the same biometric data and it prevents the use of the same references across multiple applications. Msgna et al. evaluated in [146] the practicality of this method. Their experiments focused on a possible change of human characteristics due to time or injury and they analyzed how these factors lead to intrinsic failures. According to their findings, even if the requirements of non-invertibility, unlinkability and cancelability are preserved, cancelable template protection approaches fail to address the principle of renewability. This requires an non-automated re-issuance of the biometric templates after an attack, while the applicable alignment algorithms may affect performance.

The technique of biometric cryptosystems suffers from security–performance trade-off issues. However, during the last decade, fuzzy commitment schemes have attracted much attention, Schaller et al. [189]. Nowadays, they are considered a widely used cryptographic method, being one of the most suitable approaches for commercial applications that demand large-scale DBs for the storage of biometric information and high robustness against multiple attacks, Li and Jain [122]. Hence, these hybrid privacy-aware approaches have been broadly used in biometric unimodal and minimal data deployments with high complexity, Riccio et al. [177]. For multimodal designs, the presented intra-class variations and the required error-correcting codes may reduce the reliability of the technique. Hence, it is not a mechanism that can be characterized by high flexibility due to the computational complexity. However, research into this direction is continued where recent works evaluated the applicability of cryptosystems in biometric recognition systems, identifying their weaknesses in both authentication and identification schemes, suggesting promising measures to improve their efficiency, Adamovic et al. [6] and Lafkih et al. in [117].

Finally, our work in [213] focused on the technique of Pseudonymous Biometric Identities (PIs) from biometric data. We have analyzed the challenges of privacy-by-design biometric architectures. PIs preserve the privacy principles of ISO standards as addressed in [92] while they also respect the GDPR [66] principles for data protection. The mechanism involves individualized comparison parameters to optimize the performance, offering cancelability, renewability and allowing the automated re-issuance of the templates after an attack. It also allows the creation and communication of multiple PIs for the same user in distributed environments, for instance cloud-based designs that demand high flexibility. The security requirements of confidentiality and the privacy principle of anonymity are also satisfied. Hence, it is an approach that can overcome the limitations

of the other basic mechanisms, Ngo et al. [151]. However, the integration of multimodal data and the optimum trade-off between the performance of the fusion methods and the overall robustness are currently studied by the research community. The interoperability of the method between a variety of applications and the integration of minimal data as an input (e.g., minutiae fingerprints) is still evaluated for several threat scenarios. To facilitate the reader, we map the advantages and disadvantages of the basic cryptographic techniques in Table 3.1.

Table 3.1: Comparison of the basic cryptographic techniques.

Technique	Advantages	Disadvantages
Features Transformation	• Non-invertibility • Applicable to minimal data	• Non-automated permanence • Non-preserved unlinkability • Non-preserved cancelability • Non-preserved renewability • Complexity affects performance
Cancelable Biometrics	• Non-invertibility • Unlinkability • Cancelability • Minimal & multimodals	• Non-preserved renewability • Alignment causes information loss • Alignment affects performance • Non-automated permanence • Non-preserved renewability
Biometric Cryptosystems	• Non-invertibility • Unlinkability • Cancelability • Confidentiality • Minimal & multimodals • Widely used • Used in large-scale DBs	• Present intra-class variations • Require error-correcting codes • Complexity affects flexibility • Non-automated permanence • Non-automated renewability
Pseudonymous Biometric Identities	• Cancelability & Renewability • Automated permanence • Confidentiality • Security requirements • Anonymity, EU GDPR [66]	• Multimodals under study • Minimal data under evaluation • Interoperability is evaluated

3.3.4 Alternative Approaches for Unimodal and Multibiometric Designs

Several works in the literature have proposed solutions as an alternative to the basic cryptographic approaches. They mainly rely on the distribution of

data and functionalities over different parties according to the requirements of the application environment. As mentioned in Section 3.1, a biometric recognition system consists of a number of logical subsystems such as the sensor, the communication channels and the storage area. In some applications these entities are physically separated from each other and there are numerous security and privacy concerns that we need to consider in order to effectively address the exposure of private information. To this end, many protocols have been developed that rely on particular cryptographic primitives for the protection of biometric data, allowing user authentication (e.g., by verifying that the key extracted from the new template of the biometric data matches the key that was generated after the enrollment of the user). The most well known solutions use hybrid approaches of the basic protection models combined with Homomorphic Encryption schemes or Multi-Party Computation (MPC) techniques that can be used in centralized and distributed biometric authentication domains.

Akdogan et al. proposed in [8] a secure key agreement protocol based on Hamming Distance matching techniques and cancelable biometrics to enhance the security of a fingerprint biometric scheme against brute force, replay and impersonation attacks. The work of Inamdar and Dandawate [90] introduced a multimodal system which combines a technique for fusion at the feature level with an Euclidean Distance matching algorithm. The data are encrypted using the mechanism of crypto-biometrics where the keys are generated by the feature extraction parameters and the computation primitives. Jin et al. [103] proposed a hybrid cryptographic method focused on fuzzy commitment mechanisms in order to address not only on the security requirements of non-invertibility, revocability and renewability, but also the privacy principle of minimization. Several works have presented similar approaches for unimodal and multimodal schemes, Mai et al. [128] and Yang et al. [228], among others.

The purpose of Homomorphic Encryption is to perform computations on encrypted data in untrusted environments, Rivest et al. [178]. The development of Fully Homomorphic Encryption that supports arbitrary computations has greatly extended the scope of applications that demand processing over encrypted data homomorphically, Gentry [73]. Such schemes enable the generation of encrypted inputs for any given functionality, producing an encryption of the result that can be used by untrusted parties within a computation domain (e.g., cloud computing), without exposing private data, Armknecht et al. [14]. The work of Torres et al. [214] is not the first that attempts to evaluate the effectiveness of Fully Homomorphic Encryption schemes to preserve user privacy in biometric models. Although the protocols in the literature offer promising security results and manage to address the properties of non-invertibility, cancelability and renewability, they are very computationally intensive. Their major limitation is the trade-off between computations in the

encrypted domain and the time for matching execution along with the size of the DB and the key length that significantly slows the computational speed. However, literature has analyzed the field in depth, proposing different protocols trying to make them more secure and privacy-preserving, improving the efficiency of Homomorphic Encryption schemes and rendering them practical for several biometric-based applications, such as cloud computing and electronic voting schemes, Barrero et al. [77]. An important problem that arises for distributed approaches (i.e., when the computation is outsourced to an untrusted domain) is the correctness of the computations performed by the web-based environment that may affect the confidentiality of the outsourced data, Abidin [2], Abidin and Mitrokotsa [3]. Thus, the design of privacy-preserving models is necessary in order to guarantee the protection of biometric data towards malicious parties who aim to learn information on the computation parameters and to modify the process which can lead to leakage of user data, Mandal et al. [133]. To conclude, it is noted that the state-of-the-art is mature in the field of Homomorphic Encryption schemes, presenting many promising results and any further analysis falls outside the scope of this thesis.

Blanton and Aliasgari applied MPC techniques to achieve security and privacy in biometric schemes [25]. They designed a framework for outsourced computation for iris matching that can be implemented in a cloud setting. Other unimodal architectures include the model of Xiang et al. in [225] who introduced a privacy-preserving protocol for face recognition with outsourced computation and the cloud-based design of Zhu et al. in [232] that provides an efficient model for privacy-preserving unimodal identification. Finally, Sarier [187] introduced the first protocol resistant to hill-climbing attacks for multimodal biometric authentication in the cloud, working with Euclidean Distance for the matching procedures on encrypted stored templates.

Our contribution. In [208], we described how MPC can be used in biometric recognition technologies. We analyzed the privacy benefits of this approach and we studied the security concerns that may occur during the calculation phases of recognition, from the interactions between untrusted parties. Motivated by the outcomes of this research, we proposed in [207] a complete privacy-by-design model for multimodal user authentication. Specifically, the verification setup was designed to function as an expert system, using previously stored biometric templates that are held by distinct cloud-based identity providers. Our protocols were based on MPC techniques in order to allow mutually distrusting parties to jointly compute the matching score without revealing any private information, maintaining the authenticity and confidentiality of users' data. In contrast to the existing state-of-the-art in cloud-based biometric identity management architectures that use Homomorphic Encryption or MPC techniques, our design provided multimodal authentication without having

to re-enroll the users, preventing any additional biometric extraction and storage of private information. Finally, to obtain a multimodal fused result, we utilized Hamming Distance algorithms and a user-specific weighted score level fusion method. According to our security and privacy analysis, our decentralized approach leverages the advantages of multimodal biometrics and the efficiency of the underlying primitives, characterized by dynamic functionality and flexibility in terms of computation and communication efficiency.

Chapter 4

Conclusion and Future Work

In this chapter, we present the main contributions and conclusions of this thesis and we discuss some directions for future research.

4.1 Conclusion

In this work, we focused on the integration of multiple biometrics. In collaboration with colleagues from the Biometric System Laboratory of the University of Bologna we identified the types of biometrics that can be consolidated into a fusion model. We implemented minutiae-based fingerprints and we compared different cryptographic algorithms and mechanisms to study the system's behavior under realistic scenarios. Furthermore, we analyzed the recognition performance for different approaches and we described why the accuracy of fusion strategies is the key asset in the design of multimodal architectures. Motivated by our findings, we investigated the impact of the performance metrics on the selection and the applicability of fusion approaches. We observed how these elements can increase the complexity of cryptographic methodologies. Our finding showed that multimodalities can increase the user's recognition precision and reliability. However, it is necessary to select the appropriate cryptographic technique in order to prevent the degradation of the scheme's overall accuracy. Fortunately, the last few years, there has been a steady improvement that offers deeper insights into this problem.

Additionally, we studied several cryptographic techniques for the secure transmission and storage of biometric data. We described the privacy principles,

the security recommendations and the properties for the implementation of biometric designs in privacy-preserving applications. We extensively analyzed the advantages and limitations of each strategy in the context of the existing ISO Standards for the protection of biometric information [92] and [96]. Furthermore, we investigated how the new security recommendations could be fulfilled as addressed in the European GDPR [66] and the European Regulatory Technical Standards for Strong Customer Authentication [183]. Our analysis showed that each protection approach has its strengths and weaknesses. Although for biometric developments, international standards and regulations legally specify the formats for the secure handling of user's data, the number of modalities, the platform, the software interface and the functionality of the final application determined our selection for a particular cryptographic mechanism. Our aim was to address these shortcomings and our work pointed out that security and privacy in biometrics should not be seen as two different fields, hindering each other. Internationally and in the European Union, with the proliferation of technological changes, the legal frameworks for the protection of biometric data are increased. However, we believe that there is need for future work in order to evaluate whether the biometric designs serve their primary objectives and respect the privacy policies, especially for the scenarios where impersonation and biometric disclosure are crucial.

An important part of this thesis focused on the techniques to enhance the secrecy and privacy of biometric data for their implementation in ePassports and identity cards. We presented a concrete analysis of cryptographic schemes and evaluated how these could limit the security gaps. In collaboration with colleagues from FIDELITY Project [67], we concluded that although research in pattern recognition and biometric protection areas matures, the existing approaches suffer from vulnerabilities. The encryption of biometric data cannot sufficiently protect against all types of attacks, for example, spoofing attacks, Marcel et al. [136]. Specifically, we analyzed the need of anti-spoofing techniques for preventing this kind of attacks. Motivated by rapid progress of adversaries' actions, we addressed the vulnerabilities of unimodal and multi-factor schemes under realistic scenarios. An interesting finding when carrying out this analysis was that challenge-response approaches can work effectively towards the spoofing attacks in unimodal schemes while the applicability of these mechanisms in multimodal architectures renders them more robust. Consequently, we proposed a biometric authentication framework, that combined two modalities and a liveness detection technique to increase the security levels. Additionally, our approach involved the secure storage of biometric data in the chip of the ePassport leveraging the technique of biometric cryptosystems, key-generation approach to ensure both security and user privacy. We believe that this work will help to appraise the impact of spoofing attacks and contribute to the ongoing attempts for the public acceptance of government biometric-based deployments.

Moreover, remote biometric authentication has become popular in eFinance and ePayment applications, increasing the privacy concerns. We showed that the mechanism of pseudonymous biometric identities results in privacy-enhanced designs. The technique was initially introduced in the context of biometric development projects funded by the European Union, such as TURBINE [215] and FIDELITY [67]. In our work, we implemented this method in an eFinance model based on the findings of these projects. We evaluated our design according to the existing privacy principles and security recommendations for biometric protection as addressed by the ISO Standards [92] and the new GDPR [66]. The results showed that our model can follow the ISO recommendations for the security framework in financial services [94]. Finally, we analyzed how the privacy requirements and concepts, presented in ISO Standards [95], could be satisfied during the technical implementation. We hope that the results of our research can contribute to the toolkits for secure and privacy-preserving biometric-based identity management solutions in financial services.

Nowadays, the amount of biometric data for recognition purposes has been increased rapidly, while requires enormous processing and storage capacity. We analyzed how we can manage these challenges in cloud and we pointed out the privacy risks to maintain confidentiality and integrity of user's biometric data. Moreover, we introduced a distributed approach for secure and privacy-preserving multimodal Authentication as a Service (AaaS) in an environment with malicious adversaries. We avoided an additional re-enrollment phase and any auxiliary temporary or permanent storage of user's biometrics in a Centralized Biometric Database (CBDB) in order to decrease any inappropriate use of personal information that can lead to users' identity tracking and monitoring. The design served the criteria that should be addressed from the early stage of the design, characterizing the architecture, and thus determining the user acceptance, as addressed in ISO Standards for biometric technologies [96]. Our approach was designed for authentication applications and it could also operate in identification mode with slight differences. Nonetheless, there were some limitations, such as the selected biometric modalities, the matching technique and the fusion strategy that might affect the complexity and efficiency. Our detailed analysis showed that other options presented weaknesses and their implementation was inefficient. Finally, our decentralized privacy-preserving protocols may be easily extended to update the parameters and adjust different biometrics, classifiers, matching methods and fusion rules. They are characterized by dynamic functionality and flexibility in terms of computation and communication efficiency. Due to the potential market value, our approach can offer a cost-effective business model and serve as a framework for future applications, platforms and systems in which existing biometric datasets need to be leveraged.

Our main conclusion is that the field of security and privacy in biometric

schemes for authentication and identification purposes has received significant attention over the last years. There has been substantial progress and the field of cryptographic techniques for biometric protection is maturing, presenting mechanisms that can preserve the user's rights to privacy. However, there is still room for improvements. An important observation to make is that the biometric protection involves more than just applying cryptographic primitives and the practical implementation of privacy-by-design approaches is a challenging task. In the age of the Internet of Things, we hope that the results of this thesis will inspire other researchers to properly design more robust biometric architectures.

4.2 Open Problems and Directions for Future Work

Because biometric designs in day-to-day life applications belong to a relatively young discipline, they offer new research opportunities. There are many open problems and unanswered questions that deserve a deeper evaluation based on the findings of this thesis. In this section, we formulate potential directions for future work on the security and privacy of biometric designs.

- **Evaluation of the encryption mechanisms for the protection of biometric data.** Biometric template protection mechanisms that allow matching over the encrypted stored biometric data without causing the degradation of recognition accuracy are a major challenge. Confidence in the security of an algorithm or a protocol can only be established if they have been subject to a thorough examination of the research community. This implies not only using well-scrutinized cryptographic primitives, but also finding possible ways to appropriately manage the FAR and FRR parameters, and to protect the biometric systems against physical attacks. More models and evaluation methods should be developed to analyze the optimal trade-off between performance and security. Additionally, the desired security properties depend on the type of biometrics, the targeted use-cases and the applications for which a method is implemented. Therefore, the evaluation criteria should be related to a particular biometric modality, the biometric protection strategies, the operational environment and other assumptions, such as the user privacy objectives.
- **Privacy analysis of cryptographic techniques in biometric schemes.** ISO Standards and legal frameworks specify the privacy principles and the security requirements for the interoperability of biometric deployments. Nonetheless, there is a function creep where the technical measures cannot always address the organizational criteria for the protection of user privacy. This triggers the question whether

we can adequately keep secret the source of a biometric trait and if we can come up with privacy-by-design engineering solutions to solve this issue. In this thesis, we presented some steps towards the understanding of user privacy in biometric schemes. Future research should define the criteria and identify the constraints, considering not only technical, but also nonfunctional requirements, from the initial phases of the system's design and development. A complete threat analysis and risk assessment should be conducted to evaluate the efficiency of encryption techniques. Guidelines and specific measures should be developed in order to address the privacy of the users in critical identity management schemes. Finally, there is still work to be done on the implementation of privacy-aware approaches in biometric architectures that need to preserve the property of anonymity, as defined by Campisi in [39] and addressed by the ISO Standards for the protection of biometric information [92].

- **Providing methodologies for robust multibiometric deployments.** A multimodal design can increase the recognition reliability of the system in which it is embedded. The fusion of multiple modalities has a critical role to play in biometric architectures. The fusion strategies work differently for every combination and thus deserve further analysis in order to examine the optimum selection of data, algorithms, levels of fusion, rules and techniques. The reliability of a fusion approach should be assessed over the range of the retrieval FAR and FRR. Additionally, the advantages of multimodal deployments have shifted the efforts to the combination of cryptology and multibiometrics, Kanade et al. [109]. The incorporation of multiple biometrics in template protection and biometric cryptosystems techniques can offer new security advantages. Multimodal encrypted schemes, such as fingerprint-face-iris, can provide better security levels than their unimodal components, Tiwari and Gupta [206]. An intriguing question is whether it is possible to design the tools and set the criteria for the evaluation of the cryptographic mechanisms applied in multimodal architectures. The design of a generalized encryption framework for multibiometric data, which will not be affected by the used biometric extraction algorithms, representation techniques and the selected fusion approaches could be the first step towards this direction. To efficiently address the accuracy and scalability, a multimodal system should be tested on a large representative database (DB), obtained from a diverse population of individuals. The absence of legal multimodal DBs limits the research margins. This issue should be addressed in order to study and evaluate the security of multimodal models. Although these processes will be costly, time and effort consuming, the benefits that will be derived can lead to the design of robust multimodal biometric schemes in high security systems, building and maintaining authentic public trust.

- **Developing anti-spoofing tools for secure biometric deployments.** The art of attacking biometric systems has gained sophistication over the past years, Marasco and Ross [135]. In this direction, anti-spoofing methods can used to improve the robustness of biometrics. Multimodal schemes are one of the proposed approaches for the design of anti-spoofing technologies, Marcel et al. [136]. The research area has received great attention presenting promising results in facial recognition biometric deployments, mainly used in civilian applications of the government sector, Beham and Roomi [16] and Juels et al. [106]. However, not all of the existing techniques are commercially available, due to their cost and the lack of evaluation measures. Multibiometric anti-spoofing is currently an open problem in this field, Biggio et al. [22]. It is important to understand whether and to what extent the fusion rules are vulnerable to spoofing attacks, and under what circumstances the rules may be more secure than others. We suggest future work on targeted attacks on different combinations of biometrics to address the security of multimodal recognition systems. Finally, there is a need for designing generalized countermeasures and testing their stability and resistance under various spoofing algorithms. To increase the effectiveness, practicality and consequently the applicability, simple yet effective defenses towards more realistic models are required, both at the hardware and software level of biometric schemes, while managing complexity and cost.

- **Security and privacy analysis of new biometric-based schemes in cloud applications.** The growing adoption rate of biometric designs in the web-enabled world has paved the way to a challenging research agenda for practically secure mechanisms. We identified several directions for future work on BaaS. The protection of user's information remains the biggest challenge for the migration of biometrics to a web interface. It is important to conduct a risk assessment for outsourcing the stored biometric data in the cloud. A complete threat analysis is necessary in order to study how it is possible to avoid the correlation of helper data originating from different DBs that can reveal the identity of the user and link his identity to other applications. Moreover, cloud-based IdMaaS and AaaS providers may use different security primitives and privacy regulations which may limit the flexibility of multimodal AaaS. Hence, research in this direction for the design of a framework with unified protection techniques and evaluation criteria would be valuable. For multimodal AaaS architectures, future work should be focused on the impact of matching algorithms, normalization techniques, fusion approaches and applied cryptographic mechanisms on the system's overall accuracy. For identification purposes, the size of the DBs should be taken into account, for the evaluation of scalability in terms of computation and complexity.

Part II

Publications

List of publications

International Journals

1. Christina-Angeliki Toli, Aysajan Abidin, Abdelrahaman Aly, Enrique Argones Rúa and Bart Preneel, "Secure and Privacy-Friendly Multimodal Biometric Authentication using Cloud-based Identity Providers," (Currently under review in Computers & Security Journal, Elsevier), 28 pages, 2018.

2. Christina-Angeliki Toli and Bart Preneel, "A Bimodal Verification Cryptosystem as a Framework against Spoofing Attacks," International Journal of Intelligent Computing Research (IJICR), Infonomics Society, Volume 6-Issue 2, pp. 540 - 549, 2015.

International Conferences

1. Christina-Angeliki Toli and Bart Preneel, "Privacy-Preserving Biometric Authentication Model for eFinance Applications," In Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP), SciTePress, pp. 353 - 360, 2018.

2. Christina-Angeliki Toli, Abdelrahaman Aly and Bart Preneel, "A Privacy-Preserving Model for Biometric Fusion," In Proceedings of the 15th International Conference on Cryptology and Network Security (CANS), Lecture Notes in Computer Science, pp. 743 - 748, 2016.

3. Christina-Angeliki Toli and Bart Preneel, "Provoking Security: Spoofing Attacks against Crypto-Biometrics," In Proceedings of the World Congress on Internet Security (WorldCIS), IEEE, pp. 67 - 72, 2015.

4. Christina-Angeliki Toli and Bart Preneel, "A Survey on Multimodal Biometrics and the Protection of their Templates," In Revised Selected Papers of the IFIP Advances in Information and Communication Technology, volume 457, 9th International Summer School on Privacy and Identity Management for the Future Internet in the Age of Globalisation, Springer, pp. 169 - 184, 2014.

Scientific Conferences without Proceedings

1. Christina-Angeliki Toli and Bart Preneel, "Biometric Solutions as Privacy Enhancing Technologies (PETs)," Amsterdam Privacy Conference (APC), Amsterdam, The Netherlands, 16 pages, 2015.

Posters

1. Christina-Angeliki Toli, "Privacy Evaluation of Cryptographic Techniques in Biometric Applications," Training School on Secure and Trustworthy Computing, University Politechnica of Bucharest and System Security Lab at TU Darmstadt, Bucharest, Romania, 2015.
2. Christina-Angeliki Toli, "Construction and Evaluation of Privacy-Preserving Crypto-Biometric Systems," 12th International Training School on Advanced Studies on Biometrics for Secure Authentication: Biometrics in Forensics, Security and Mobile Applications, Alghero, Italy, 2015.

Internal Reports

1. Christina-Angeliki Toli, Aysajan Abidin, Enrique Argones Rúa, Roel Peeters and Bart Preneel, "A Privacy-Preserving Two-Factor Authentication Protocol for Secure Access Control," COSIC Internal Report, 8 pages, 2016.
2. Christina-Angeliki Toli, "Crypto-biometric Systems in the ePassport Life Cycle," COSIC Internal Report, 13 pages, 2013.

External Reports

1. Christina-Angeliki Toli, Abdelrahaman Aly and Bart Preneel, "Privacy-Preserving Multibiometric Authentication in Cloud with Untrusted Database Providers," IACR Cryptology ePrint Archive 2018(359), 18 pages, 2018.

Miscellaneous

1. Andreas Pashalidis, Roel Peeters and Christina-Angeliki Toli, "Privacy-Friendly Access Management for ePassports," FIDELITY Project Deliverable, WP 8: Biometric Data Protection, 2013.

2. Jens Hermans, Roel Peeters and Christina-Angeliki Toli, "Multibiometric Template Protection to Enhance the Privacy of Personal Data for their Implementation in ePassports," FIDELITY Project Deliverable, WP 8: Biometric Data Protection, 2014.

3. Jens Hermans, Roel Peeters and Christina-Angeliki Toli, "Specialized Crypto-Biometric Solutions for Identity Cards and ePassports," FIDELITY Project Deliverable, WP 8: Biometric Data Protection, 2014.

Publication

A Bimodal Verification Cryptosystem as a Framework against Spoofing Attacks

Publication Data

Christina-Angeliki Toli and Bart Preneel, "A Bimodal Verification Cryptosystem as a Framework against Spoofing Attacks."

In International Journal of Intelligent Computing Research (IJICR), Infonomics Society Volume 6-Issue 2, 10 pages, 2015.

The paper contains 40% of new additional material, being the extended version of the work "Provoking Security: Spoofing Attacks against Crypto-Biometrics," Christina-Angeliki Toli and Bart Preneel, In Proceedings of the World Congress on Internet Security (WorldCIS), IEEE, Dublin, Ireland, 6 pages, 2015, [212].

Contributions

- Principal author. The proposed design is the result of discussions with co-author. We also acknowledge for their ideas the colleagues from the Biometric System Laboratory of the University of Bologna, the University of Sassari, Michigan State University and the University of Halmstad.

A Bimodal Verification Cryptosystem as a Framework against Spoofing Attacks

Christina-Angeliki Toli and Bart Preneel

Department of Electrical Engineering ESAT/COSIC, KU Leuven & iMinds
Kasteelpark Arenberg 10, bus 2452, Leuven-Heverlee B-3001, Belgium

Abstract. The exponential growth of immigration crisis and the recent terrorism cases revealed the increase of fraud occurrences, cloning and identity theft with numerous social, economic and political consequences. The trustworthiness of biometrics during verification processes has been compromised by spoofing attackers sprang up to exploit the security gaps. Additionally, the cryptography's role in the area is highly important as it may promote fair assessment procedures and foster public trust by serving the demands for proportionality, reducing the concerns about national surveillance. Literature efforts are devoted to studying model threats and problems raised by targeted malicious actions for biometric techniques. However, attacks against multimodal crypto-biometric systems have not received much attention. This paper presents cryptosystems, intrusions and countermeasures for single, multiple modalities and complicated schemes. Finally, a novel bimodal privacy-friendly cryptosystem is suggested, able to reject such kind of attacks, presenting an anti-spoofing behavior under the cooperation between user and the function. The aim of this multidisciplinary work is to organize the current performances on how to develop security, contributing to the research in privacy-by-design able to address real-world use-cases and pinpoint the potentiality for improvements.

Keywords: Biometrics · Cryptography · Cryptosystems · Template Protection · Spoofing · Deception · Prevention Techniques · ePassport

1 Introduction

Until relatively recently, biometric enabled systems have replaced the traditional forms of individuals' recognition of his/her presence, access to facilities or log in to an account as their traits can be very discriminative yet less easily lost or stolen. Automated identity management, using face, hand or fingerprints, has become an experience in everyday life, mainly due to their diffusion in technologies, such as electronic passports or IDs. From border control, to log on computers, mailing and eBanking services, biometrics constitute a unique and integral part of the user, to whom are associated with, and this is a serious tangible reason for being vulnerable to activities that threat to compromise not only the reliability of the application, but also the security and privacy rights of the person [191].

A closer look at the explanation for any extensive attack to fields related to biometrics will lead to the nature of the data, the personal non-biometric information that may be stored and correlated or other private facts, such as the medical condition of the user that may be enclosed and revealed on occasions where someone's identity is not appropriately protected. In terms of spoofing, a non-colluding honest entity tries to fake somebody else's identity by presenting samples of that person's traits, or tries to gain benefit from the "leakage" of stored biometric information in a DB or an electronic chip. Considering the special assumption when a biometric trait is compromised, then it cannot be canceled and renewed, hence moreover, it seems critical that may be used to create gelatin genetic clones of fingerprints, contact lens with a copy of iris or retinal scans, artificial replicas of faces, facial samples in the form of photographs, a video or a 3D mask. Voice or even gait can be recorded, inducing a system to falsely infer a presence under another's identity. A behavioral biometric, such as signature, handwriting are not stolen, under the classical term, but can be easily mimicked and used to a certain degree for illegal means. These concerns have given space to public debates on the pressing matter of confidence in authorized, biometry compulsive systems and therefore, societal, ethical themes.

As an address to the challenges of strengthened privacy for human characteristics, a range of standards and security methodologies have been suggested. Standard conventional cryptographic algorithms have been characterized, simply, as not enough, as a result of not allowing and supporting comparison between template and fresh sample caught on sensor, thus making the system possibly to be cheated. In this philosophy, biometric template protection schemes have been deployed. The paramount idea is the secured form of the stored template, making it unusable without authorization, but still capable for recognition its true energetic owner. The approaches try to follow the requirements of accuracy, irreversibility, diversity, unlinkability, revocability. In the direction of

enhancing security, privacy information and overcome drawbacks in both areas, the combinations of biometrics with cryptography techniques were born [109]. Crypto-biometric systems or biometric cryptosystems, as they are denoted in this paper, respect the previously referred compulsions and additionally can obtain cryptographic/crypto-bio keys strongly linked to the user's identity.

Although crypto-biometrics propose alternative solutions, biometric recognition systems are still suffering and sometimes defeated by intruders. Vulnerabilities primarily include direct and indirect attacks performed at the sensor level, or correspondingly, inside the parts of the system, such as communication channels, storage domain, feature and matcher extractions. Direct operations happen when an attacker tries to masquerade as a valid and authorized user by changing his/her biometric characteristics, claiming a different identity posing himself/herself or presenting false traits. Surprisingly, multibiometric systems, based on their sources, separated to multi- sensors, recorded samples, algorithmics, units and modals, are constitute a more difficult, but not impossible target. Ideally, several mechanisms have been tried for the defense of security for the involved items in a system, with controversial results. From a realistic point of research, academic and industrial trials on detection, encryption and anti-spoofing measures have been proposed to deal, in some extent, with these threats.

In addition to these, admittedly, there has never been a proposed model on how best biometrics applications can be secured, especially those ones that are related to governmental and organizational purposes [191]. The proposals for CBDBs including information for national ID cards or passports bring about a feeling of discomfort, reinforcing the assertions wherein biometrics have seen intrinsically as privacy's foe. Conversely, keeping pace with technological changes, biometric schemes as a modern and sometimes mandatory key to validate transactions must also be given the capacity and the resources to deal with millions of expected requests, always respecting their primary objectives of data minimization, accuracy, transparency, confidentiality etc. Template protection models should prevent the re-generation of the original template from the initial and the laws should strictly be followed to ensure their acceptance from citizens.

This study is motivated by recent advances in the scientific field of biometric system security, and protected templates to ensure the secrecy of person's identity. Its target is to present and add new information to the studies against fraud processes to biometric based verification technologies, something that since 2012 is indicated as well, from the increasing number of projects aim to suggest ideas for preventing risks, directly applicable to special issues, such as border control. Our essential objective here is to clarify the role of cryptology in biometrics, and examine how honest is the statement for a safe and reliable

biometric application environment, when this is constantly exposed to human mind's contrivances. The remainder of the article is organized as follows: In the next two sections, a thorough summarized review on research articles is analyzed, particularly on the development of standard metrics, protocols and datasets for the appraisal of the progress, introducing readers to enlightenment. The fourth part is devoted to single and/or multibiometric cryptosystems, spoofing attacks, and resistance processes. Fifth section aims to present the design of an innovative multimodal model. It is a suggestion capable of being used in electronic passport applications based on liveness detection and RFID access control as combined mechanisms for reinforcement the cryptographic bearing against spoofing. The privacy standards and principals are also discussed while a standard evaluation methodology which is needed to assess the influence of countermeasures on biometric system performance is indicated. As a conclusion, comprehensive remarks together with some directions for future approaches are listed, providing food for thought.

2 Preliminaries on Cryptography for Biometrics

2.1 Biometric Cryptosystems and Protocols

Approaches towards security of biometric technologies are briefly presented in this section. The variety of the concepts are divided to schemes that aspire to transform the aforementioned data, reducing the possibilities for generation of the initial trait used during the enrollment phase, and to cryptosystems that combine known cryptographic functions to derive cryptographic keys from biometric data. A uniform classification of the various techniques according to their functionality is described diagrammatically in Figure 1. In the first division, encryption, hashing, transformation and other cryptographic techniques produce one-bit verification for biometric systems. Next in order, data are used to obtain keys that further will be used as an extra secured method. Ordinary biometric systems requires prior a DB which contains stored biometric or non-biometric references to the data for further comparison causes. The lack of revocability for each of these pieces and the very existence of a place from where information could be leaked, leading to numerous concerns.

For this reason and following the lines of the diagram, classical encryption of biometric data, such as the Advanced Encryption Standard (AES) technique, the trait collaborates with one, or more secrets, similar to passwords that can be stored also in a token or smart card, preserving diversity. Cancelable biometrics category has been studied extensively and inspired various designs for other proposed methodologies. The fundamental ideology can be found in the

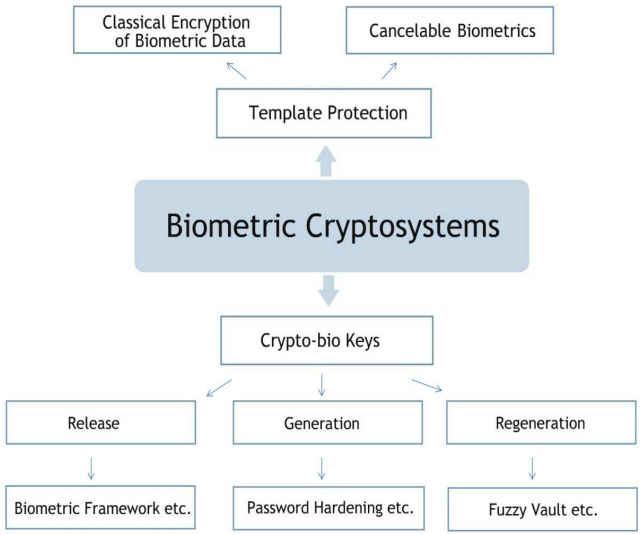

Figure 1: Categories of biometric cryptosystems.

one-way function re/irreversible feature transformations, where there is luxury for multiple transformed templates and their uses across applications, under the same identity. At the second cryptosystems' family, the creation and re-issuance of keys from biometric data constitute a remarkable and template-free concept. There is a cryptographic framework that is used to securely store just a key born after enrollment and released only over successful verification. This key can be irrelevant or stable bit-string directly extracted from biometrics and in binding approaches can be regenerated, as it is combined with the biometric data using cryptography and it is possible to be later retrieved [23].

Protocols for re-generation crypto-biometrics in systems are come to address the specific ways on how to share the keys between the untrusted parties of an authorized user/client and an intended server's principle, and as a field lacks of research progress. Symmetric-key cryptography is fast but too risky, on the grounds that several cryptanalytic attacks can occur in the event of using a single key for a large-scale application. Public key suggestions are vulnerable to other kinds of attacks and initially they do not include the verification of authenticity to each entity. To overcome the limitations, protocols designs help to share the crypto-bio keys or create secure authenticated sessions based on biometrics [109].

Taking the advantage of this collective knowledge on the core technologies of both biometrics and cryptography, pseudo-identities (PIs) based mostly on

fingerprint characteristics have been carefully chosen during the initial design phase to accomplish a workable trustworthy and friendly scheme that serves principals of user's privacy [33]. The typical architecture of a related ecosystem is based on the independent generation of references coming directly from live biometric samples or already stored biometric templates which after their use as parameters to the embed and non-invertible, one-way, yet unique, functions are finally fully deleted/destroyed. The encoder verifies the identity and builds additional AD. These information may serve the purposes of interoperability. The methodology is considered to be successful when the final non-biometric data can provide multiple renewable and protected templates, independent PIs for the same individual within an application able to be used across other systems to prevent DB cross matching and linking, preventing impersonation and providing data separation for people with similar features and ability to handle a duplicate enrollment check scenario.

Back to the process, at the second phase, some AD like knowledge-based secrets to be entered by the enrollee, such as passwords, signature, secrets are used as an input to the PI encoder and their string is not stored. During verification process, re-creation of a PI or directly verification a previously stored PI based on a provided recognition sample is performed. The transformation of information and the provided data are also used and of course the same AD from the user. The comparator compares both elements or identities to check if originally coming from the first subject. Validity checks and expiration can be controlled especially for characteristics that can change with the passing of the years. Revocation is also available, in case of deleting the PI from a DB, and/or removing the authorization, then the re-enrollment may result in a new protected template. Figure 2 presents the creation and verification of the PIs [33].

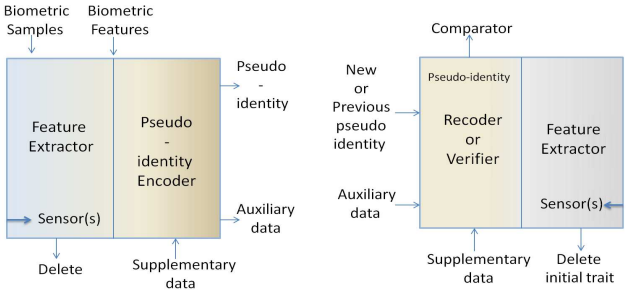

Figure 2: Protection mechanism of biometric pseudo-identities.

Indubitably, in every scenario, the verification performance and the evaluation of the overall function of the crypto-biometric systems largely depend and based

on the baseline of its system. The error correcting codes algorithms are used to improve the degrades and analyze any perspectives able to change, in a better level, each approach. The important factors are the adoption of multibiometrics as an emerging development, understanding that obtaining high entropy keys is still a challenging, but encouraging issue. The use of passwords, tokens, electronic documents or smart cards can secure user's privacy, the appropriate secured sharing of the keys based on totally untrusted involved sides on a system and the ability to combine basic elements from each category suffice to design new complete hybrid systems.

2.2 Attack Points in Biometric Systems

The security breaches directly or indirectly, as described above, may aim towards different parts in system modules. Eights categories are used for notice the points for possible threats, such as the generic scheme in Figure 3 portrays. The frame symbolizes the inner aura and attacks that can take place in that are further divided into three groups [174]. Threats at the communication channels between different parts of the system, attacks to the feature and matcher extractors, those ones that could take place under the assumption of the DB of information is compromised. The direct, also known as spoofing attacks are substantially described at the next subsection and here indicated as the first spot at the level of sensor.

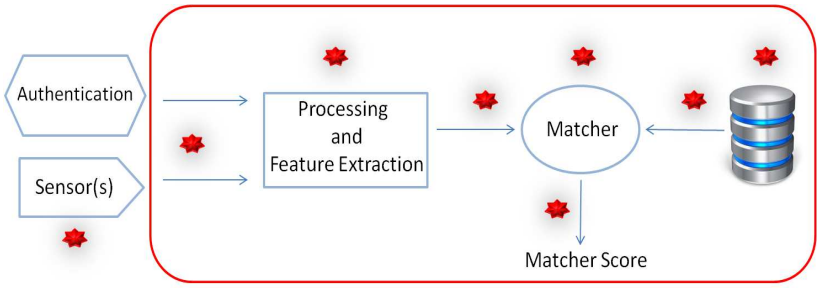

Figure 3: Areas of attacks on a typical biometric scheme.

An analytical outlook to indirect attacks involves a deviant and the communication tunnel between user and the valid end system's controller. The attacker must mainly know specific information about the process of the whole application, the template format, the scores, communications protocol, the data transmission elements and can perform an access to all its stages. In this way, the intruder can gain the extraction, changing, deleting, adding of

important data on identities. Specifically, the communication channels across consecutive parts of the system can be intercepted by an eavesdropper who changes surreptitiously the messages in the link, manipulates the scores, decisions and results or makes brute force attacks by exhaustively trying to find the input that can unlock the region of interest. During the pre-processing and feature extraction progresses, insertion of impostor data and component replacement can happen while the same could take place as well at the matcher level with the hill-climbing algorithms, consisting on iteratively changing some synthetically generated templates until the right one is found. Lastly, the DB's region is characterized as imperatively dangerous and involves malicious tampering at the templates from reading to modifications of the links between biometric data, increasing privacy concerns.

3 Comprehensive Literature Review

3.1 Spoofing Attacks

In the case of spoofing attacks that may take place directly towards the initial level of sensor, a zero-effort or active impostor tries to positively claim a different identity deceiving the acquisition system. The means of this kind attack are highly depended on the type and quality of design and application. For the first mentioned, an unauthorized person uses his/her own trait that by mistake can be matched to a template. This cascade effect happens due to dysfunctional false acceptance rates of a system that make it vulnerable. Obfuscation intents are carried out without the requirement of advanced technical skills, by presenting a counterfeited stolen, copied, replicated biometric and the range includes gummy fingerprints, photos, three dimensional-3D shaped models or falsification of facial characteristics using make-up, plastic surgery, imitations or short video clips for gait, signature or handwriting, recorded speech modality and voice conversion, high resolution pictures of iris or even ears. To sum up, sophisticated cheaters have constantly managed to artistically fool the most smart computer devices simply by taking the advantage of the increasing popularity of social network websites where photographs are available, such as facebook, instagram, youtube etc.

Research has proved that none scheme is completely spoof-proof, since almost all commercial devices by private security firms are defeated after this kind of attack. However, the issue is not about the hacked systems but people and this is a particular challenge, not only in criminal, but also in civil matters. The implications are gradually increased across different devices and public services. Depending on the position of the attack, recently published works have

managed to categorize and evaluate them with regards to the scores of rates that a system can demonstrate when it is threaten. Insufficient, sub-optimal, optimal and super-optimal attacks constitute the terminology for spoofing acts [51].

From an ethical perspective, a deceiver can claim an identity and gain access to private data or parallel information that may lead him/her to someone's car, mobile, computer, house, electronic passport, totally ruining a personality in society. A decade ago, all these would be heard like a myth or seen as a movie scenario, nevertheless, nowadays persons may well consider such information intimate and part of a broadly acceptable status quo, and hence demand a vigilance attitude from companies and authorities, with skeptical position against any alarming behavior could threaten their interests. Undoubtedly, it remains really hard for nonspecialists to assess the security-low-level parts of a system and perfectly compose their plan, but still there is the belief about those who if they are motivated will find an idea on how to get around any barriers used to protect the targeted system [136]. To overcome these arguments, applications should be designed following the security level needed according to its potential purpose, the scale of the data and concurrently follow privacy by design rules, covering the ISO Standards, respecting legal provisions.

3.2 Anti-Spoofing Measures

Up to this point, in research community different methods have been suggested for facing this long-neglected problem against many biometric modes, referred as anti-spoofing, spoof detection or presentation attack detection. By definition, their role is to confer a highly positive characterization about system's trustworthiness [176]. In this way, the major objective is to ensure the protected environment of an application which can recognize only genuine users and not detect and prevent spoofing attacks, as is mistakenly believed. Having this in mind, the questions about the huge chasm between research results and real-world applications can be answered [60]. Minding the gap, the technology of a biometric verification system should contain by design the incorporation of mechanisms that reject spoofing attacks and are under alliance with the parts of the final system considerations and characterize its overall susceptibility.

One the most familiar and user-comfort technique that is used for increasing the awkwardness to spoof a system are passwords or smart cards, offering the opportunity for supervising the verification process. Although the way has been successfully, at some percentage, practiced on transactions, other recognition applications that require communication between services and enrolled person, such as travelers' checks, need other anti-spoofing methods, involving the combination of multimodal biometrics for one identity and liveness detection.

Human physiologic information do not indicate that the person who is present at the time of capture is actually alive. Liveness detection tests some data inherent to the biometric or additional processing of information captured by reader to extract contextual, discriminating features or extra hardware. On the same wavelength, pulse oximetry, electrocardiogram, palm vein, keystroke, typing rhythm, gait, ear acoustic properties, finger/hand temperature sensing, facial thermograms as continuous authentication mechanisms and challenge/response actions describe the cooperation of the user who provides unintentionally or must do something, a blink, pupil, lip or head movement, allowing the system to understand his/her real presence.

Algorithms, recently proposed countermeasures, standards, protocols and recorded DBs for further analysis have received upsurge attention, with varying degrees of spoofing vulnerability, covering a range of attack scenarios and acquisition conditions [168]. Methods are classified in three categories, firstly, a real living body possess color, texture, elasticity and supplementary intrinsic properties, which can be used to check the validity, human expressions, reflex and involuntary signals are secondly grouped. Finally, coming from traditional forensic environments, the collected trait is examined for spotting clues of forgery of friction ridge skin clarity. Academic and industrial projects choose the baseline, plot the licit/normal scenarios and the error rates criteria for the experiments, conducting on freely datasets, available for offline work, containing samples for different modalities. Among the most "overused" evaluated biometrics are fingerprints, iris and face, due to their widely accepted distinctiveness [136].

Respectively, face presentation potential can be handled by subject-specific 3D facial masks which analyze local binary patterns based measures. A powerful way to eliminate similar threats are the background motion correlation and texture of the surrounding facial region quality measurements, something that could be useful especially to more realistic scenarios [81]. For fingerprints, algorithms that can perform an analysis about the capture of multiple samples of a biometric instance in a short time frame are combined with those that allow live detection and segmentation of the finger, including defenses against gelatin, gummy and silicon samples and others that offer processing of the photo with graphical operations, enabling a convenient thought about how to capture multiple views of modality from different fingers of one subject. The results prove well-promising rates, even though the existence of a purely incapable of being deceived climate system is simply a utopia, under the current circumstances. A novel multi-spectral approach to manage these challenges is to use the proposed cascade structures as a part of a larger anti-spoofing solution that involves multiple modalities from the user, his/her movements to justify the presence, algorithms that overcome the noises, simulate light reflections, determine the scene motion, fixations, speed, acceleration, or even anticipate video replay

attacks. The developments may be evaluated through test protocols, applied to more comprehensive DBs, and meanwhile the techniques should to be based on specific frameworks, supporting larger scales of datasets and each generalization need to be carefully controlled.

4 Mutlibiometric Cryptosystems

4.1 Attacks

The technologies of multi or single biometric cryptosystems have been encountered to infiltrate systems, preventing from some malicious performances, while remain exposed to classic spoofing ones. Briefly, it is pointed out that a skillful adversary has to know additional transform parameters or secret keys to defeat the area with previously enrolled samples, since both categories used to cooperate with helper data or are bound to cryptographic techniques and tokens. In such a condition, reconstruction of the original template, and consequently its raw usage or the synthesization of fake physical biometrics, is greatly complicated. The multimodalities for one identity offer the advantage of extremely low false acceptance attacks in a tampering hypothesis. On the contrary, if a single trait is compromised then the whole template can be recovered, when a blended replacement attack take place, where subject and attacker's template and distinct parts of larger sets are merged into one [9].

Cancelable approaches transform non-invertibly can unlock the genuine user's biometric or some elements of it respectively, as described in [120]. Fuzzy commitment schemes and vaults, which are related to entropy rates and wittily hiding the biometric (for instance minutiae and chaff points for fingerprints), are vulnerable if the algorithms are poor. Helper data and key-re-generation schemes extracting short keys or suffering from improper accuracy present high tolerance, making achievable the composition of an approximation of the initial biometric from its hashes. Coercitive, device substitution intrusions and any possible combination of serial venomous acts could be applied sufficiently, compounding a worst possible scenario, but rather unrealistic in everyday contexts.

Since it still remains necessary to test the robustness of multimodal biometric systems, especially for combinations, such as face-fingerprint or/and face-iris, under various realistic hypotheses, recent studies such as the work in [9] conducted some experiments. This analysis may allow figuring out to what extent each balanced countermeasure is representative of the performance. The relevant endeavor was based on established state-of-the-art authentication technologies for each modality and different combinations of attacking story

lines using datasets of spoofed templates or traits. The final comments led us to the denouement that multimodal schemes suffer from lack of unsuitable strong protection for their template, as the design of optimized fusion rules is currently under research. At the very least, attacking assumptions are too pessimistic and result in a significant overestimation of the false acceptance rates, a case that turned out to be positively reassuring, but certainly non-effective for more advanced and elaborate intrusions.

4.2 Resistance

Response-focused methodology on the basis of possibility to integrate liveness detection or the mentioned anti-spoofing methods include experimental investigations to verify whether and to what extent multimodal verification systems could be assessed as securely protected. Until now, studies on spoofing underline that using multibiometrics, the recognition performance is higher but unfortunately unimodal approaches handle better external attacks [76, 137]. To reduce the risk of exposure of the combined template, if a single trait revealed, the selection of other biometrics, akin to hand-fingerprint, face-iris, instead of multiple fingerprint samples, for example, is recommended, based on empirical evidences. For increasing robustness, the design of stronger fusion rules (score or feature level are recommended) between samples is mandatory. Additionally, cryptosystems and especially crypto-bio keys ideas for multimodalities are not only more efficient than unimodal ones, but simultaneously privacy-friendly. These suggestions pretend to bring some insight into the difficult problem of evaluation through the effective countermeasures that can minimize the effects of threats by taking into consideration the techniques of fusion, the serial or parallel modes, the type of cryptographic algorithms, complexion of the application according to the hardware and its interconnects [9]. Finally, we emphasize that any protection mechanism should respect design principles and keep the overall balance of the system, without underestimating that extra efforts can bring about the cost of sharply reduction of verification performance.

5 Bimodal Biometric Verification System

People from dozens of nations have already acquired their new electronic passport equipped with contactless chip that stores personal data. The expansion of illegal occurrences in this area increases the lack of public trust with numerous privacy, physical safety, and psychological comfort consequences [136, 176]. As a counterweight for the theoretical analysis of the previous sections, Figure 4 introduces a bimodal biometric model for person identification made up of

face and fingerprint, or face and iris matchers. The framework is a bold initiative in the deployment of three technologies: crypto-biometrics, spoofing countermeasures and Radio Frequency Identification (RFID). This ePassport idea is inspired by previous works on spoofing for biometrics [51] and designs to defeat attacks through implementations of RFID authentication protocols and data encryption, increasing the complexity and therefore robustness [104] while cryptographically advocating the secrecy requirements for biometric data, which is mandatory for identity documents schemes [106, 191].

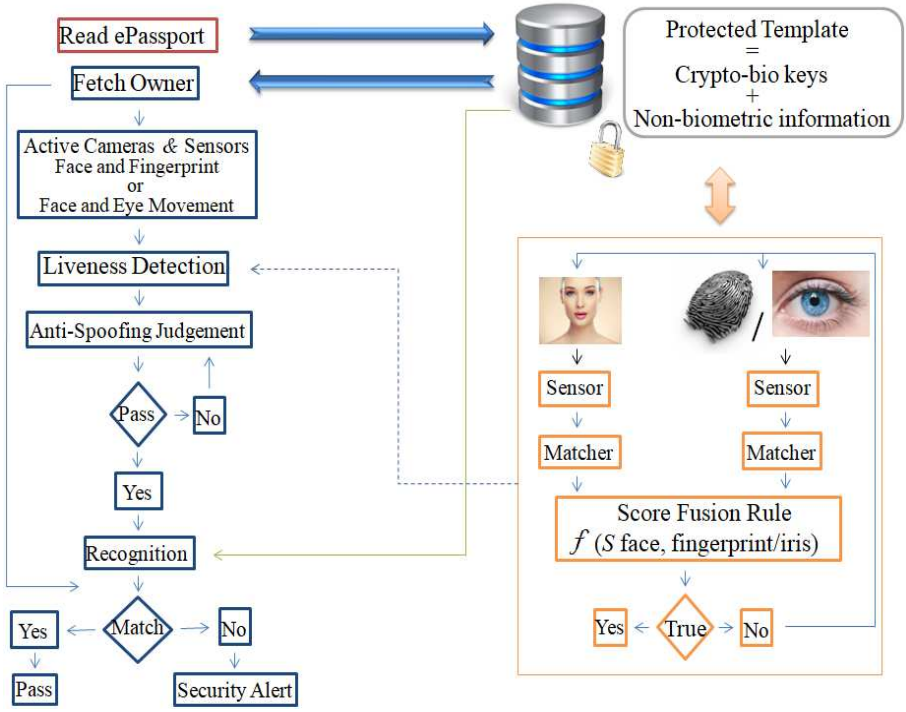

Figure 4: Flowchart of the bimodal system.

5.1 Functionality and Design

During the enrollment phase a pair of datasets is collected. To preserve the principals for the protection of user's privacy, the created template consists of transformed minimal elements of the initial biometrics binded together under a cryptographic algorithm which uses them to create keys. The extended version of this deployment can be understood as this part was explained previously

in Section 2. The scheme involves AD delivered from the involved hardware, authority etc. The supplementary data in our design comes from the liveness detection process. The final non-biometric information stored on ePassport's chip are the crypto-bio key, which can be "unlocked" only when both biometrics are matched, traveler's personal details and document's type, digital number, etc.

The description of the anti-spoofing verification system involves liveness detection method combined with the current RFID access control process. When a user approaches to an E-Gate for automatic passport checking, video sequences are captured by its cameras. Then the system requires the cooperation of person who has to turn left or right the head and provide his/her fingerprint to a sensor (or move eye to an iris movement tracker). The three dimensional facial object as a result helps system to separate an alive human from a photo. The matching parameters are scored under a fusion rule which its optimal threshold depends on both of them, as a mechanism against multibiometric template threats [9]. After judgment, the recognition procedure demands the use of final fusion score to extract from the DB (chip) the cryptographic key and thus the informative content.

5.2 Usability and Advantages

Exploring the privacy and security usability of this method, authors respected the needs of such an impending worldwide next-generation authentication technology, as those were determined in admissible experiments [106]. The framework preserves data confidentiality as the initial biometric used for enrollment and verification or authentication is minimal and can be only available for the creation of a protected template. The final chip does not store fresh biometric information and it is additionally transformed using one-way bit functions. The re-generation or revocation of the pseudo-references as a privacy-preserving mechanism for biometric protection may be an answer to lost identity documents or compromised identities. This approach as a biometric template mechanism could be also useful for many other applications. For example using only identity cards or ePassports, if someone travels from one country to another, for gaining access at his/her bank account [191]. The supporting architecture of RFID protection mechanisms provides extra security for sensitive information, such as birth date or nationality that are carried on passports.

Liveness detection as an anti-spoofing measure is nowadays among the most acceptable ways against spoofing of identity documents, during border control checks. The process can ensure the presence of the passport's owner. Furthermore, analyzing the result of sensor on a three subject-specific 3D facial trait with

local binary patterns and those data delivered after the cooperation of person, iris movement tracking or presenting his/her fingerprints, the system can be smart enough to understand a genuine user or not.

The design requires the matching of many parameters that are scored under fusion rules, as a more tested method for better results in modalities like those used in our scheme. The optimal threshold depends on both of the strings "unlocked" under the presence of its biometric characteristic, something that can overcome the threat of exposure the whole template in multibiometric template combinations [9]. The overall strings are cryptographically secured to proof that the judgment during the recognition procedure will minimize the false acceptance rates

Summarizing, this deployment definitely deserves a better analysis as it is just the first step of spoofing against next-generation identification systems. The encouraging part is the fact that this thought underlies on previously researches that emphasize how important is to combine all the current knowledge in cryptography to protect the biometric systems and the human rights to privacy. The anti-spoofing methods based on the cooperation of machine-user add a new layer to secure authentication, and relevant deployments after test and evaluation can benefit the needs of citizens, government and industry.

5.3 Vulnerabilities and Limitations

The vulnerabilities of this framework found on false acceptance percentages for an impostor's recognition and ingenious spoofing actions, under police presence and could be considered as worst-case assumptions. ICAO and ISO standards through documents that unequivocally identify their bearers were assumed to guarantee the protection from the document forgery. RFID access control processes and other impacts on security issues in ePassports, even though they are a charming field, are outside the scope of this paper.

As limitations of the design could be characterized the poor quality of the cryptographic methodologies used in producing the template or/and score fusion rules results. The function is time consuming, regarding that it performs different steps to provide a final result. This is a significant drawback considering that it should be used as a method for border control with millions visitors daily. The facial recognition as the first and immutable part of this system is weak during liveness detection performances as the result may vary if the user moves the head fast, increasing the error rates. The fingerprints present shortcomings, as well, due to the fact that are affected by age. Finally, the use of PIs in such a scheme instead of crypto-biometric approaches has been

implemented in applications only for fingerprints and it remains untested their performance in other biometric traits.

Research about the function of the suggested model is currently aimed on tests on the cryptographic mechanisms for other samples. Secondly, the selection of fusion rules will be carefully selected according to the need of the scheme, as those were underlined above. The final experiments will be conducted on datasets of real and spoofed biometric elements. The overall accuracy and privacy evaluation will be determinant for the acceptance of the methods.

6 Conclusion

The paper represents an attempt to acknowledge and account the biometric schemes using combination of cryptography with biometric characteristics and how this could play an increasing role in electronic documents and transactions for identifying a person, limiting security risks. Current methods and their design suffer from vulnerabilities, and here is where measures become crucial in order to protect schemes and the overall efficiency of government and commercial applications. Spoofing attacks at the sensor level of a system used for automatic recognition of people from their biometric characteristics have been tackled by independent and/or collaborated to initial design and application, anti-spoofing attempts [135]. To appraise data protection problems, multimodalities, current research developments on suggestions against invasive actions and a prototype face-fingerprint/iris cryptosystem have been presented. Create an all-inclusive view, we believe that this project will help to better evaluate the impact of spoofing attacks from a security and privacy engineering aspect, contributing to ongoing and expected attempts in pattern recognition area.

In outcome's atmosphere, the application of biometrics in different services requires high accuracy rates, secure personal information storage and reliable generation of data while the whole process of transfer is proof. Identity thief might exploit in occasion of low protection levels. Even so, some modalities are more robust than others, however, this should not be interpreted as meaning they are more reliable [82]. Spoofing and countermeasure assessments are a complex part for each study as it is mandatory to think all the involved possibilities and design generic frameworks with a manageable impact of usability. Challenge-response approaches seem to be supplementary to the traditional ones and more effective for risky applications. The standard evaluation methodology during the phases of the architecture can lead to better independent networks and fused countermeasures as a valuable strategy.

For some conditions, even if anti-spoofing measures could adequately assessed, the rapid progress of adversaries' actions at the initial steps of verification purposes throw up wider concerns on public narratives of privacy and frequent monitoring of individuals. The advancement of theory on secured access control and practical design implementations of the provided valuable experience on technologies will improve their robustness.

7 Future Research

Directions for further research and open issues may be focused on anti-spoofing techniques for biometric multimodalities and their combinations, seeking to reduce the different degrees of deception/lying while enhancing the proper function of the system. An anti-spoofing method is not constructed to operate as a stand-alone procedure but together with the biometric recognition system. During the design process the error recognition rates should be taken into consideration. Cryptography can offer significant, but inadequate solutions in this emerging technology, and thus next steps on encryption schemes may promote the security strength against intrusive attacks. Multibiometric systems can be easily cracked by spoofing at least only one trait and future works should flatly investigate how to bring robust results on score level fusion rules and provide protocols for provable secure authentication based on template protection schemes.

From another angle, state-of-the-art suggests the use of DBs for spoofing and anti-spoofing analysis but still lacks to cover all the possible scenarios and certainly the implementation in real-world applications. The problem of generalization should be addressed as well, due to the fact that current findings may cover individual occasions for some biometric traits, leaving gaps to varying areas of a system that verifies or identifies biometrically the users. Concurrently, the missing pieces of the puzzle for better approaches may lie at the combination of different anti-spoofing algorithms. Liveness detection efforts, and challenge approaches with the cooperation of user, could be tested to offer advantages versus tricks that can fool existing systems.

Apart from the design ideas and open research questions on the protected operation of the system, the major themes of human privacy and rights to anonymization, facing the obstacles of societal suspicions over surveillance, and other specified and legitimate services should be covered. Decisively, the starting setup is vital for the entire field. Human biometrics may be collected and processed under detailed protocols, compatible and related to the scope of the authority involved in the transaction. The procedure should respect

proportionality and serve the forensic experts thoughts on the prevention of spoofing, where we may profit more from a careful appraisal of the processes, supporting the structure of the biometric system.

Acknowledgements. This research is a part of KU Leuven contribution as a Partner in EU Project FIDELITY (Fast and trustworthy Identity Delivery and check with ePassports leveraging Traveler privacy), which is funded by the European Commission, under the security theme of the Seventh Framework Programme (Grant agreement no: 284862). Authors would like to thank colleagues from KU Leuven, University of Sassari, Michigan State University and University of Halmstad, for their ideas. The attention, support, comments, and contribution of anonymous reviewers regarding improvements of this work, is gratefully acknowledged.

Publication

A Privacy-Preserving Model for Biometric Fusion

Publication Data

Christina-Angeliki Toli, Abdelrahaman Aly and Bart Preneel, "A Privacy-Preserving Model for Biometric Fusion."

In Proceedings of the 15th International Conference on Cryptology and Network Security (CANS), Lecture Notes in Computer Science, Milan, Italy, 6 pages, 2016.

Contributions

- Principal author. The guidelines on how to use performance metrics into a fusion scheme is the result of several discussions with co-authors. Responsible for the design of the proposed model for multimodal identification and verification purposes, except for the overview of using MPC techniques in the design.

A Privacy-Preserving Model for Biometric Fusion

Christina-Angeliki Toli, Abdelrahaman Aly, and Bart Preneel

Department of Electrical Engineering, KU Leuven-ESAT/COSIC & iMinds
Kasteelpark Arenberg 10, bus 2452, B-3001 Leuven-Heverlee, Belgium

Abstract. Biometric designs have attracted attention in practical technological schemes with high requirements in terms of accuracy, security and privacy. Nevertheless, multimodalities have been approached with skepticism, as fusion deployments are affected by performance metrics. In this paper, we introduce a basic fusion model blueprint for a privacy-preserving cloud-based user verification/authentication. We consider the case of three modalities, permanently located in different DBs of semi-honest providers, being combined according to their strength performance parameters, in a user-specific weighted score level fusion. Secure multiparty computation techniques are utilized for protecting confidentiality and privacy among the parties.

Keywords: Biometrics · Multimodalities · Fusion · Performance Metrics · Identity Authentication · Reliability · Cloud Computing · Secure Multi-Party Computation · Applied Cryptography · Privacy

1 Introduction

Over the last decade, biometric-based systems have been part of the daily routine for identity verification. This is specially true for online services. Moving the existing technology to cloud-based platforms could be proven effective for many access control or surveillance applications with millions of users. Nevertheless, with all eyes on security, privacy challenges encountered in the transmission of personal data across the parties could be characterized as extremely serious. The reader could take into account the following attacking scenarios [21, 64]. Additionally, to store several biometric templates under the same user's identity in one DB could not only be a difficult feat, considering the restricted access on templates from competing biometric suppliers, but

also discouraged or illegal [116]. Multibiometrics were originally introduced to alleviate the inherent limitations of single biometric modalities that render them unable to correspond at the high security requirements. Furthermore, the confidence on the functionality of a biometric scheme is determined by some specific metrics: False Acceptance Rate (FAR) shows if a system incorrectly recognizes an intruder while False Rejection Rate (FRR), the percentage of valid inputs which are incorrectly rejected for an authorized person. Being inspired by biometric applications on cloud we introduce a model for a verification protocol based on fusion and designed to operate in a cloud environment for privacy-preserving biometric recognition and identification purposes.

To reduce privacy threats, we employ secure Multi-Party Computation (MPC), thus avoiding any centralized repository and using the stored templates by the service providers in a decentralized manner. That way we can authenticate an individual based on his/her biometric characteristics, searching, matching and combining the results, and return a reliable decision guaranteeing the secrecy of the new (fresh/raw) and old (stored) biometric templates. Applications include a cloud-based border control system that integrates stored unimodal biometrics by a set of different recognition services, evaluating them accordingly to their FAR to prevent access to unauthorized individuals. Contrary, a cloud-based surveillance solution, operating to automatically screen the crowd in order to identify a person sets up a FRR respective fusion mechanism. We refer the reader to [17, 49, 58, 141] for a more detailed treatment on MPC.

Contribution: We provide a view of a decentralized cloud based mechanism for multimodal user verification, using distrustful DB providers. The service is provided under strong privacy-preserving constraints, where the only thing the involved entity learns is the final output.

Our main **contribution** includes the following:

- The design uses previously stored unimodals, providing the advantage of handling information without extra unnecessarily storage of fused data.
- We incorporate FAR and FRR rates of uncorrelated biometrics in a user-specific transformation-based score level fusion. Weights are assigned to each trait according to its strength performance.
- Since biometric data transmitted across the network and design involves various distrustful service providers, MPC is considered to be a suitable mechanism for the execution of our protocols. In this way, no information related to the raw, stored or the final output is revealed to the cloud parties.

Motivation: Even though several proposals on multimodal fusion, performance rates and secure cloud-based biometric applications can be found in the literature, the combination of these results seems to be a challenging task. Given that utilizing more than two biometrics offers improved identification efficiency [180], we make use of the three most popular and robust biometric body traits (face, iris and fingerprint) for our model. However, the concept of integration is considered as an open problem [182], and it is an undeniable admission since that we assume a cloud-based setting induces many privacy risks. Thus, it is necessary to enhance security between the non-trust parties, protecting intermediate computations and user's information. The novelty of our model lies on bridging the gaps of cloud-based multimodal biometric verification or identification, ensuring the privacy between the involved entities and the user, whenever data transmitted across the network.

2 Environment and Settings

The scenario is as follows: an involved entity provides the fresh biometric templates to three unimodal cloud biometric service providers that store old templates of faces, irises and fingerprints, separately. The involved entity needs to verify/authenticate a user's identity with better accuracy than when operating with single modal module. The verification process takes place in the cloud and has to guarantee the privacy of the user's data (fresh and old templates). Figure 1 illustrates the generic form of the proposed biometric authentication access control system.

Parties and Roles: Parties involved in our protocol fulfill at least one or more of the following roles during the verification process:

- **Dealers:** Any subset of parties that provide the private inputs for the computation in shared/encrypted to the parties responsible of the computation (computational parties). In our case, an involved entity delivers the fresh extracted features, and the service providers are the owners of the stored templates. Both have also to provide other metrics, the proportions, thresholds and rates in shared form as well.
- **Computational Parties:** Any subset of parties in charge of the computation. They are also in charge of communicating the necessary results of the computation to the output parties in shared form. Typically, the computational parties are distrustful parties with competing interests, in the case at hand they could be represented by the service providers or any coalition composed by control agencies, service providers and civil entities.

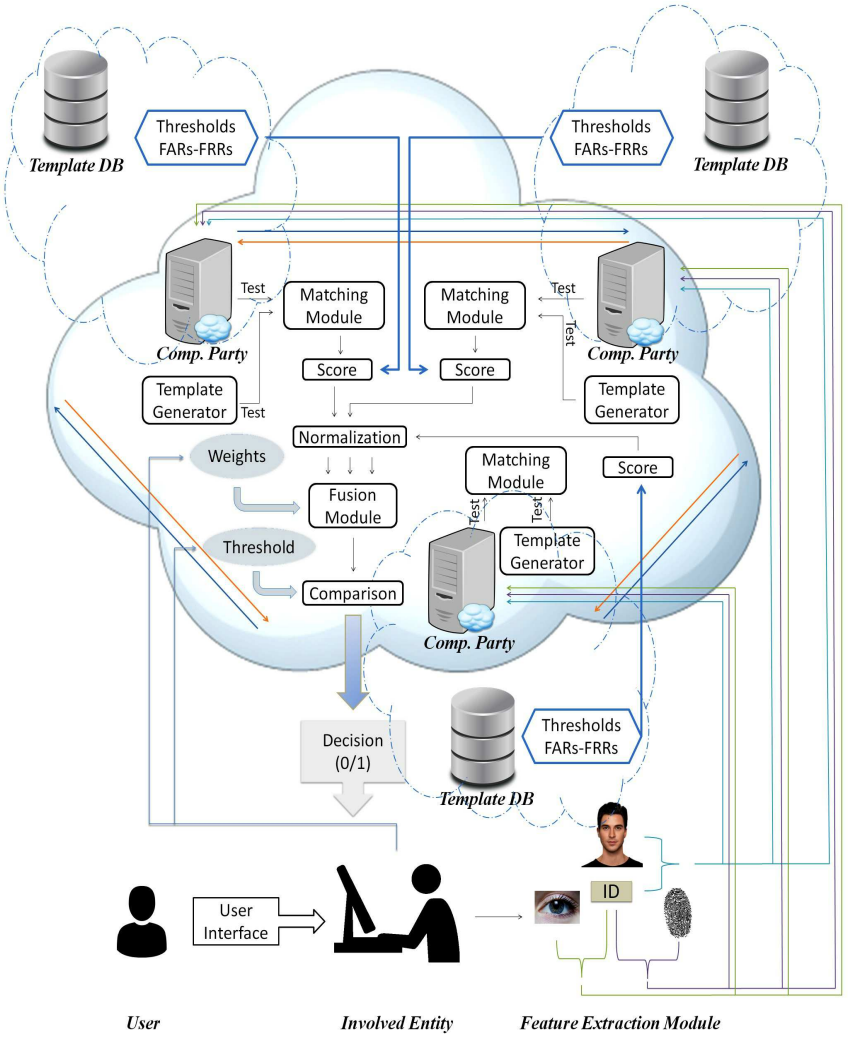

Figure 1: Proposed model of fusion for multimodal verification.

- **Output Parties:** Any subset of parties in charge of the reconstruction the output. These parties are the only ones who learn the output and what can be inferred from it. In our setting, this role is occupied by the involved entity.

On privacy and security: it follows from the underlying MPC primitives used

(for instance perfect security with BGW [17]), and the oblivious nature of the future protocol.

3 System Outline

1. The involved entity needs to verify a user's identity based obligingly on three biometric inputs. It obtains the user's data (a physical presentation of an identification document). Features are acquired sequentially and processed in a cascade mode.

2. The three new biometric templates and the identity references are transmitted across the network. Service providers then use this information to extract and secretly share the old templates, or return a dummy instead.

3. During the next phase, a feature matching algorithm, such as Hamming Distance algorithms, or similarity measurement methods are used to give a degree of comparison between the new and old templates.

4. Next, service providers choose the specified value of the reference thresholds. These calculations on unibiometric features come from the service providers. The process can be improved from genuine and impostor training samples distributions available from the enrolled users in monomodal verification/identification functions of their systems. Note that this undertaking is out of the scope of the current work.

5. On the basis of the selected thresholds, where monomodal system performs better in a such a way that the corresponding FAR is as low as possible and respecting the requirements of the application that operates in verification/authentication mode, the matching score that mostly reflects the similarity between the new and one of the old stored template set is selected from the generated vector for each modality, respectively.

6. The matching module output by three non-homogeneous biometrics and consequently scores have to be transformed into a common domain, before combination. The application has to normalize the results in the cloud by placing the three obtained matching scores in the same numerical range varied over $\{0, .., 1\}$. Fractional representation can be utilized for its MPC adaptation.

7. Weights are selected by the involved entity (according to the FAR, FRR that each service provider considers to be permissible). These weights, assigned to the three modalities, are in the range of $\{0, ..., 1\}$ for the user u as $w_{face,u}$, $w_{iris,u}$ and $w_{fingerprint,u}$, such that the constraint

$w_{face,u} + w_{iris,u} + w_{fingerprint,u} = 1$ is satisfied. As before, fractional representation can be used during our MPC adaptation.

8. Normalized matching scores are fused in ideally to output one from three. A user-specific weighted sum rule is then applied in order to determine the final result of the score level fusion for multimodal identity verification.

9. Finally, the involved entity determines a threshold $\perp$ and communicates it to the computational parties. The final acceptance happens in case of an individual has been authenticated as a previously successfully enrolled user. Regarding rejection, this simply means that the system failed to surpass the threshold $\perp$, not leaking whether the user is enrolled or not on any or all the DBs.

4 Usability and Limitations

Usability: The generic verification model introduced by this paper incorporates three popular and well-studied modalities into a fusion method, operating in cloud. Note that the system could operate in identification mode, without requesting the presence of a credential by the user, where the biometric templates are contrasted against the hole DB. Thus, the proposal could be used in identity management applications and surveillance oriented models. The authentication accuracy is based on utilizing physically uncorrelated biometrics that can present significant improvements at performance, even when the quality of the samples is sub-optimal.

Limitations: One clear limitation of our model is related to interoperability issues, regarding the matching sensors of the involved service providers. This is due to the fact that biometric data is usually matched by sensors produced by different manufactures, this proposal is restricted in its ability to fuse templates originating from disparate sensors. For that reason, one of the major challenges in the biometrics recognition domain is the use of similar types of sensors, establishing a common technological behavior, something that reflects effort and cost ineffectiveness. Moreover, the system might be affected by the restrictions put in place by the use of MPC, for instance, a viable protocol might prefer the use of Hamming distance for simplicity and avoid the use of floating point arithmetic.

5 Conclusion and Discussion

We present a model for privacy-preserving fusion in a non-traditional, but reality representative distrustful environment. We incorporate multiple biometric traits, for cloud-based identity authentication, and make use of MPC techniques to offer privacy. Moreover, multimodal fusion gives better results than using a single matching module in the context of security and reliability. In general, it is indisputable that biometrics fusion has a critical role to play in identification systems and different fusion mechanisms work differently for every combination of data, rules and tools, while optimality is conflicting with regard to the retrieval performance rates. Furthermore, identity-purposed biometric DBs for online authentication mechanisms, seriously enhance risks from different perspectives and for each assessment separately. MPC restricts the misuses of private biometric information at the levels required by realistic applications. Future solutions for these major issues can support the feasibility of large-scale privacy-enhancing biometric identity management technologies.

Acknowledgements. This work was supported in part by the Research Council KU Leuven: C16/15/058. In addition, it will contribute to ICT programme under contract FP7-ICT-2013-10-SEP-210076296 PRACTICE of the European Commission through the Horizon 2020 research and innovation programme.

Publication

Privacy-Preserving Biometric Authentication Model for eFinance Applications

Publication Data

Christina-Angeliki Toli and Bart Preneel, "Privacy-Preserving Biometric Authentication Model for eFinance Applications."

In Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP), SciTePress, Funchal-Madeira, Portugal, 8 pages, 2018.

Contributions

- Principal author. Responsible for the design of the model and its analysis, based on security and privacy requirements. The idea for the proposed model is the result of discussions with co-author and COSIC colleagues.

Privacy-Preserving Biometric Authentication Model for eFinance Applications

Christina-Angeliki Toli and Bart Preneel

imec-COSIC KU Leuven, Leuven, Belgium

Abstract. Widespread use of biometric architectures implies the need to secure highly sensitive data to respect the privacy rights of the users. In this paper, we discuss the following question: To what extent can biometric designs be characterized as Privacy Enhancing Technologies? The terms of privacy and security for biometric schemes are defined while current regulations for the protection of biometric information are presented. Additionally, we analyze and compare cryptographic techniques for secure biometric designs. Finally, we introduce a privacy-preserving approach for biometric authentication in mobile electronic financial applications. Our model utilizes the mechanism of pseudonymous biometric identities for secure user registration and authentication. We discuss how the privacy requirements for the processing of biometric data can be met in our scenario. This work attempts to contribute to the development of privacy-by-design biometric technologies.

Keywords: Biometrics · Cryptography · Security · Privacy Enhancing Technologies · Privacy Metrics · Access Control

1 Introduction

Systems that automatically recognize a user's identity based on his biometric characteristics are becoming increasingly prevalent or even compulsive. From fingerprint scanners, embedded in smart mobile phones, to border control infrastructures, the extensive use of biometric authentication applications has increased the security and privacy concerns [167]. Specifically, security and privacy are two different complementary fields [39]. Biometrics were initially introduced as a technology that overcomes the security limitations of the traditional authentication approaches, such as passwords or tokens [68]. However, biometric recognition relies on who a person is, or what someone does [99]. Hence, biometric data may reveal more information about the user than necessary [122].

State-of-the-art in cryptographic techniques presents concrete mechanisms that enhance the security of biometric designs [39]. The research focus on testing the approaches towards malicious adversaries, and evaluating the implementation in realistic scenarios [149]. Furthermore, the users' fundamental right to privacy has been internationally established and legally supported [115]. Security frameworks standardize the developments while privacy principles confirm biometric data sources, ensuring that they are accurate and consistent [166]. However, adopting the procedures and implementing these requirements are challenging tasks [63]. Cryptography has offered privacy-aware approaches, addressing the practical difficulties on the design of biometric schemes [99, 144]. In 2016, the European General Data Protection Regulation (GDPR) [66] has set new recommendations for the processing of biometric information. The criteria should be addressed from the early stage of the design, characterizing the architecture, and thus determining the user acceptance, as these are addressed in ISO [96].

Achieving effective and privacy-aware means of authentication has been a long-recognized issue of biometric security [45]. While passwords are still dominant, current implementations exhibit a much greater diversity of architectures, particularly in relation to those used on mobile devices [146]. Nowadays, secret-based schemes that combine PIN codes and biometrics are widely implemented in electronic financial applications, achieving great public acceptance [19]. This paper addresses the very recent privacy regulations for biometric data and the advances in the field of cryptography for secure biometric designs. We define the terms of privacy and security for biometric designs and discuss the current legal framework. Additionally, we analyze the security measures and privacy-preserving cryptographic techniques found in the literature. Finally, due to the rapid deployment of biometric-based access control systems for electronic financial and payment purposes, we introduce a privacy-preserving biometric authentication model for eFinance applications.

Our **contribution** is as follows:

- We analyze the advantages and limitations of privacy-preserving cryptographic techniques according to the current ISO privacy principles for biometric information protection [92] and the new security recommendations of the new European GDPR [66].
- We present a biometric authentication model for eFinance applications, based on the privacy-preserving cryptographic technique of pseudonymous biometric identities.
- We evaluate our proposal following the ISO security framework for financial services [94]. We discuss how the privacy requirements, presented in ISO [95] can be satisfied during the technical implementation.

This work is the first to introduce a privacy-preserving eFinance model, based on the findings of biometric development projects funded by the European Union, such as TURBINE [215] and FIDELITY [67].

2 Definitions

2.1 Privacy

In the age of the Internet of Things, the growing utility of biometric technologies in cloud applications has enabled the aggregation of personal data from multiple sources [19]. This has resulted in a constant criticism, influencing negatively the public opinion [99]. Users are skeptical, especially when they cannot prevent the biometric registration in an access control scheme. For instance, government designs, such as border control systems that demand the collection of biometric data without the permission of their users [99]. This information can be gathered and shared for ambiguous and unintended purposes, without any official approval [115]. It is a common belief that even when a procedure is performed by a legislative authority, the collection of such a personal data unjustifiably violates the human rights [39]. Privacy for biometrics is a basic user's right in a society where anonymity is considered as an inalienable privilege [99]. Thus, during the last decade, there is an accelerated pace of regulations development for the legal transmission of biometric data in government and industrial schemes [45]. Through legislation, European and International organizations emphasize the importance of privacy for biometric systems [166]. These activities are analytically discussed in Section 3.

2.2 Security

The concept of security for biometric architectures refers to the technical characteristics of the system and it is related to its overall robustness [39]. The protection mechanisms are classified based on the vulnerable points, where direct and indirect attacks on a biometric recognition scheme may occur [171]. After 2001, complete collections of targeted attacks and possible security measures have been presented [139,151,212]. Although the legislation to protect biometric data has been strengthened, the current legal regime is believed to be insufficient to preserve privacy [99]. As a supplementary response to that call, cryptographic techniques have managed to decrease the security limitations of biometric schemes through biometric template protection mechanisms [166]. Architectures that are more complex based on the combinations of multibiometrics and

passwords or tokens have been introduced while extra attention has been paid to anti-spoofing measures [176]. A privacy-by-design approach that combines cryptography and respects the privacy principles is considered to be the optimal option for enhancing both security and user's privacy in biometric schemes [115]. Sections 4 and 5 present the most recent privacy-preserving cryptographic tools.

3 Privacy Principles and Security Regulations

For every given technology, international and national standards establish the criteria for the configuration of a process, tool or system [115]. In this way, the applicability is resolved according to the requirements that define the security for user's personal data. To such a degree, a common toolkit specifies the privacy metrics to avoid any misunderstanding among developers and users. For biometric designs, standards specify the formats for the interchange of private data, the platform independence, program interfaces, application profiles, calculations and tests for the results [45, 99]. Hence, the architecture is neutral, without being in favor of any particular vendor or modality [66, 96].

In terms of security, ISO standards set the general guidelines for systems, tokens, smart cards, authentication employments, identity management designs and cyber-security architectures [19]. In the context of privacy for biometric data, they define the principles of *limitation*, *minimization*, *accuracy*, *completeness*, *transparency* and *rectification* that regulate the process of personal data and provide suitable formats for the development of the procedures [96]. The security requirements of *confidentiality*, *integrity*, *authenticity*, *availability* and *non-repudiation* should be met for every system that is linked to the network [96,151]. Supplementary security recommendations for biometric applications report the properties of *anonymity*, *unobservability*, *revocability*, *cancelability*, *non-invertibility*, *unlinkability* and *discriminability* [39]. They referred mainly to the data transmission and distribution and the prohibitions towards the parties [92].

Recently, the term of *renewability* [96] has been added to the ISO security recommendations for privacy-preserving biometric designs [66]. It is considered the most challenging regulation as it indicates the necessity of a user's re-enrollment in a system for updating his data. *Permanence* is also included in the new recommendations. It determines the validity period of the stored data while it guarantees the uniqueness of an attribute. The new regulation is focused on the importance of privacy-by-design, underlining that as biometric technology matures, the interaction increases among users, markets, and the technology itself [66].

4 Literature Review

In this section, we present the existing cryptographic approaches that have been proposed for enhancing the security of biometric designs and preserving the privacy of user's sensitive data. The literature analyzes the privacy weaknesses in biometric schemes and suggests ways to secure the implementation process [6,144, 149]. The approaches include: ***Template Protection Schemes***, ***Biometric Cryptosystems*** and ***Pseudonymous Biometric Identities*** [39]. The first category includes ***Features Transformation Mechanisms*** and ***Cancelable Biometrics***.

4.1 Features Transformation

Biometric template protection as a term refers to the techniques where data is transformed to prevent a possible leakage [151]. The mechanism transforms the template data extracted from the freshly captured biometric before storing it. Thus, the template stored in the DB is strongly protected with a goal that it would be almost impossible to retrieve the genuine biometric feature from the template [39]. In case of attacks, it is computationally hard for an intruder to find the function that was initially applied to the biometric data [124]. Although the technique offers reliable security, a recent analysis concludes that complex transformations may reduce the performance [149]. The mechanism can be utilized in unibiometric and multibiometric templates. However, multibiometric designs demand more complex parameters and it is not possible to apply one-way functions with a high cryptographic security level. Consequently, it is very challenging to make this approach compliant with the privacy recommendations of *non-invertibility* and *discriminability*.

4.2 Cancelable Biometrics

Inducing the privacy recommendations of *cancelability* and *revocability* in biometric systems [96], being presented in Section 3, the purpose is the user's data protection, under a threat scenario, by composing quotation to biometric templates [39, 139]. The method of cancelable or revocable biometrics is introduced as the first privacy-preserving mechanism for biometric schemes that respects these privacy properties for biometric information [171]. The mechanism allows multiple transformed biometric templates, offering higher security levels. One of the basic objectives is the diversity that provides a larger number of protected templates from the same features and it prevents the use of the same references across the variety of applications. The recommendations of

non-invertibility and *revocability* are covered, since this approach demands the re-issuance of biometrics after an attack [111]. However, the privacy recommendation of *renewability* introduced in [66] is not preserved. Human characteristics may change during time or due to other interferences, such as an injury. In this scenario, the biometric scheme presents high False Rejection Rates (FRR) and system's performance is decreased, being vulnerable to intruders [146].

4.3 Biometric Cryptosystems

Biometric cryptosystems or shortly crypto-biometrics belong to the second category of privacy-preserving techniques for the protection of biometric data. They combine cryptographic encryption and decryption functions to derive keys from biometric data [39]. Mainly, there are two schemes that named after their role as key-generation and key-binding schemes [6]. For the first group of the classification, biometric feature directly creates the generated keys and their products are shared to the involved entities to secure all the communication pipelines and tunnels. Key-binding approaches allow only the storage of information coming from the combination of biometric data with randomly generated keys. In this case, the keys are non-biometric elements, such as a PIN, password or credential with certified container of attributes. Both schemes are fuzzy, since the demanded samples are slightly different each time, unlike the encryption keys in the traditional cryptography [151]. Crypto-biometrics are currently a popular technique, being one of the most suitable fields for applications that demand large-scale DBs for the storage of biometric information and high robustness against multiple attacks, such as government or banking services [122]. It is a privacy-aware cryptographic method that respects the privacy recommendation of *unlinkability*. It can be used in access control mechanisms with high *complexity* [177]. However, this can affect the *flexibility* of the technique. Recent works report that its applicability is ineffective for anonymous DB models [6].

5 Background

5.1 Pseudonymous Biometric Identities

Pseudonymous identities from biometric samples are the newest interface in the domain of privacy-preserving cryptographic approaches for biometrics [33]. Figure 1 presents the complete architecture of renewable pseudo-identities (PIs)

in a typical biometric application [62]. The mechanism utilizes non-invertible functions, to create PIs based on the references of biometric data. After the user's registration, the created PI is securely stored. After the authentication procedure, the PI expires while for a second recognition, the scheme can create a new PI. For higher levels of security, the scheme requires the presence of a password or credential that are used as supplementary/auxiliary data (AD).

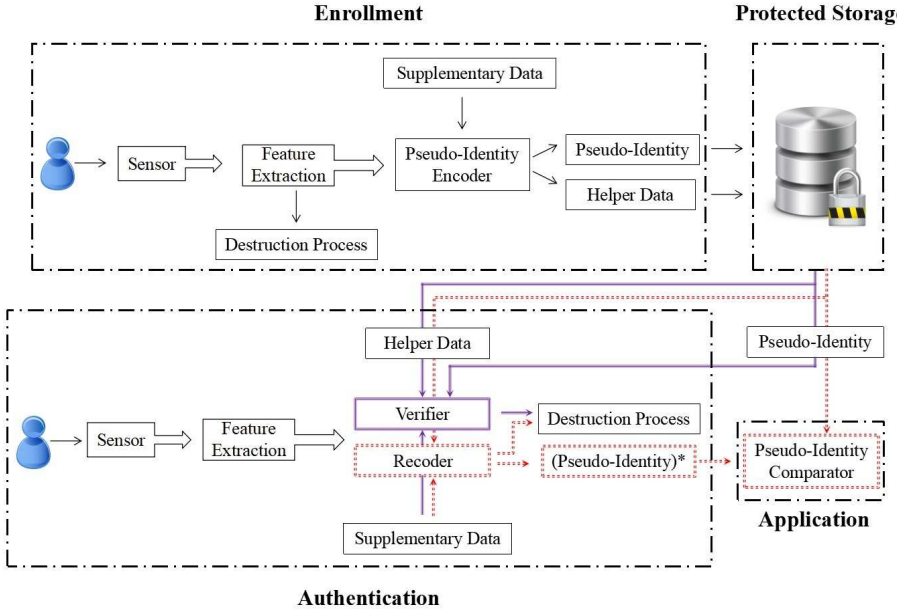

Figure 1: Architecture for renewable biometric pseudo-identities.

During the enrollment phase, a biometric device captures the biometric templates from user's fresh features while the user provides a password. Subsequently, an encoder generates the PI and creates additional non-biometric HD, using as an input only the user's AD. The initial biometric information and AD are destroyed. The design involves the parameters for the separation and individualization of the elements, preventing impersonation, bringing obstacles for users that have very similar characteristics [122]. Helper data and PI references are securely stored as different templates in an encrypted domain, such as a DB, card or token.

The authentication process is divided in two different approaches [33]. The scheme can proceed to a direct and simple verification of the PI. The user presents his biometrics at the system's sensors and provides the password that was presented during the enrollment phase. Given the stored templates of the

helper data and the PI, a verifier provides and communicates the decision result to the application's parties. After a successful authentication, user's fresh biometrics and the password are destroyed. According to the second authentication method, the new captured biometric features, the AD and the template of the HD are provided to a PI recoder, allowing the generation of a new (pseudo-identity)*. It follows the destruction process for the biometric and supplementary data, while the new PI is provided to the application's comparator. The authentication decision is determined by the comparison of the new created (pseudo-identity)* with the template of the stored pseudo-identity.

The technique can combine passwords and biometric data, presenting high levels of security [62]. It preserves the privacy principles of ISO standards in [92] while it also respects the properties in [66]. The embedded one-way functions are subject to the recommendation of *non-invertibility*. The mechanism offers individualized comparison parameters to optimize the performance, offering *renewability*, *cancelability* and *revocability*. It allows the creation and communication of multiple PIs for the same user in several non-local architectures, for instance cloud-based designs that demand high *flexibility*. The security requirements of *confidentiality* and *anonymity* are satisfied. Hence, it overcomes the limitations of the other mechanisms [151]. However, the recommendations of *interoperability* and *integrity* are evaluated for different threat scenarios. The integration of minimal data as a user's input such as minutiae features of fingerprints is examined, testing the overall accuracy of the implementation in realistic use-cases. Table 1 compares and summarizes the presented approaches.

6 Privacy-Preserving Authentication Model

In this section, we introduce an authentication model based on the privacy-preserving cryptographic mechanism of pseudo-identities. Due to their advantages and high security results, the PIs are the ideal technique for our model that is specially designed for eFinance applications. Following the ISO framework for privacy and security in services of the financial sector [94], we present the practical issues in technically addressing the privacy principles and security regulations introduced in [66, 92, 95].

6.1 Related Work

Literature offers a variety of proposals for secure biometric authentication in mobile devices [146]. Moreover, privacy-preserving approaches that combine passwords and biometrics in electronic financial architectures, present reliable

Table 1: Privacy-preserving cryptographic approaches.

Technique	Advantages	Disadvantages
Features Transformation	• Applicable to multibiometrics • Meets privacy principles [92]	• Complexity affects performance • Non-preserved non-invertibility • Non-satisfied discriminability
Cancelable Biometrics	• High flexibility, interoperability • Meets privacy principles [92] • Non-invertibility • Cancelability/Revocability	• Renewability affects performance • Non-satisfied discriminability • Non-preserved anonymity
Crypto-Biometrics	• High security, flexibility • Meets privacy principles [92] • Non-invertibility, renewability • Confidentiality, unlinkability	• Complexity affects flexibility • Non-satisfied interoperability • Non-preserved anonymity
Pseudo-Identities	• High security, flexibility • Meets privacy principles [92] • Meets properties [66] • Cancelability/Revocability • Renewability, unlinkability • Confidentiality, anonymity	• Minimization affects flexibility • Interoperability is evaluated

security levels [32, 145]. The cryptographic technique of PIs is characterized as the optimum mechanism for commercial applications [33, 62]. In terms of security and privacy, although its promising results, state-of-the-art offers only theoretical works that lack of applicability [69]. We exploit and analyze the mechanism in an eFinance service scenario.

6.2 Scenario, Parties and Roles

Figure 2 presents the registration and authentication processes. For higher levels of security, our model utilizes the second approach of authentication that involves a PI recoder as it is presented in Section 5. The design involves a user, a bank and the user's mobile device with an embedded fingerprint sensor. The bank, through the application running on the device controlled by the user, offers to the clients the service of the online financial checking. The user creates an electronic bank account and gains the eFinance service access.

The architecture of PIs presents a classification of systems according to the choices for storage and comparison [33]. The models for cloud-based applications

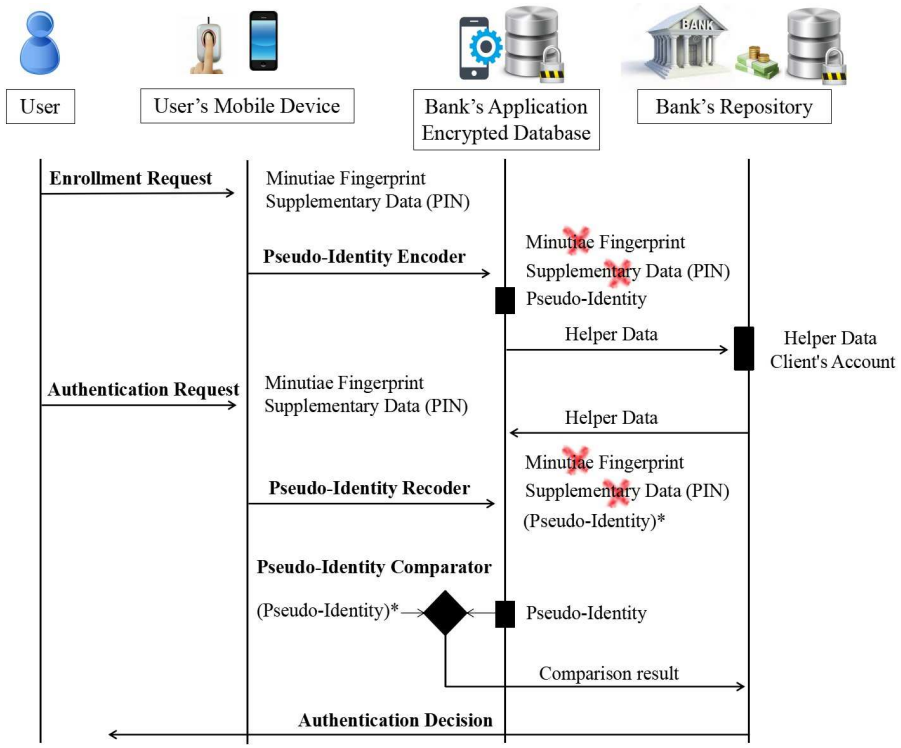

Figure 2: Biometric pseudo-identities model in an eFinance application.

are more accurate when they distribute the templates of comparison, according to the evaluation introduced in [215]. We select this approach in order to reduce the parameter of tampering attacks and prevent a malicious user from registering, using another person's name and getting access to his account. The signal processing subsystems of the PI encoder and recoder are local. Our model stores the information distributed on user's mobile device and on server. The results are transmitted through decision subsystems while bank's application handles the comparison procedures that take place on server.

6.3 Registration and Authentication

For the user's enrollment procedure, the client utilizes the bank's application, requesting the creation of his account. The biometric sensors capture and extract minimal minutiae data of his fingerprint while the application demands the

presence of a PIN code that is used as AD. The device's encoder uses this information to generate the PI and create additional helper non-biometric data, using as an input only client's PIN code. The PI is encrypted and locally stored at the device, the helper data template is securely transmitted at the bank. It is stored and associated with the client's account information. Biometrics and PIN code are erased.

During the authentication, the client requests access at his account, using the bank's application and presenting his fingerprints and the PIN code. For the comparison procedure, the bank securely transmits to the bank's application the encrypted helper data for the given user's PIN code. The decision is not determined only by the helper data, since the subsystem of a PI recoder creates a new (pseudo-identity)* based on the new biometric features that the client presents. At this phase, there is no storage of private biometrics and their related references. The PI comparator of the bank's application communicates to the bank the result of the comparison between the new created (pseudo-identity)* and the initial stored pseudo-identity while PIN code and biometric minimal data is destroyed. The authentication decision is provided to the client.

6.4 Security and Privacy Requirements

The **security requirements** of *confidentiality*, *cancelability* and *revocability* [96] can be met through the utilization of the pseudo-identities approach. The new recommendation of *renewability* introduced in [66] is also covered. According to the security regulations for financial services [94, 95] the property of *permanence* is critical for privacy-aware schemes. Our model preserves the recommendation, since the PIs expire and can be re-created. Finally, our design is based on two levels of security, combining passwords and biometrics. Thus, it offers higher robustness, as this is suggested in [95]

The **privacy requirements** of *non-invertibility* and *unlinkability* [92] are preserved. It is noted that the term of *unlinkability* is not referred to the bank. This party is considered semi-honest, and the privacy regulations are related to the malicious third parties. In case of an attack, the PIs are canceled and the compromised templates become incompatible with the user's original ones, respecting client's privacy [215]. Though the one-way functions, the model prevents the use of biometric data for any other purpose than the one originally intended [94]. In that way, further processing of additional data across applications and other DBs is avoided. The original biometric feature cannot be recovered and the system offers *confidentiality* against access by an unauthorized intruder. For the online environment of the bank's application, it is challenging

to study the implementation of minimal data for preserving *data minimization* and offer user's control over his data [95].

7 Conclusion

Biometric authentication for eFinance and ePayment purposes gains ground globally, increasing the privacy concerns in financial sector. In the light of the foregoing critique, research on the field of cryptography for biometrics offers mechanisms that their practical implementation brings new privacy-enhanced designs. In this paper, we discussed the current security approaches and privacy practices that can offer protection of user's biometric information, respecting his privacy rights. We presented a privacy-preserving biometric authentication model for eFinance applications, based on the recent cryptographic technique of pseudonymous biometric identities. In compliance with the data protection regulations, we discussed the ways that privacy can be addressed and how the security requirements could be satisfied during the design process. Authors' future direction is the design of the protocols and the technical implementation of the model. The proposed approach can lead to the toolkits for secure and privacy-aware identity management in financial services.

Acknowledgements. This work was supported in part by the Research Council KU Leuven: C16/15/058. Authors would like to thank, for his ideas on this research, Professor Arun Ross of the Department of Computer Science and Engineering, Michigan State University. The comments of anonymous reviewers are gratefully acknowledged.

Publication

Secure and Privacy-Friendly Multimodal Biometric Authentication using Cloud-based Identity Providers

Publication Data

Christina-Angeliki Toli, Aysajan Abidin, Abdelrahaman Aly, Enrique Argones Rúa and Bart Preneel, "Secure and Privacy-Friendly Multimodal Biometric Authentication using Cloud-based Identity Providers."

Currently under review in Computers & Security Journal, Elsevier, 2018.

This paper introduces an integrated secure system and uses a part of the insights presented in "Privacy-Preserving Multibiometric Authentication in Cloud with Untrusted Database Providers," Christina-Angeliki Toli, Abdelrahaman Aly and Bart Preneel, IACR Cryptology ePrint Archive 2018(359), 18 pages, 2018, [209].

Contributions

- Principal author, except for the design of MPC protocols and the evaluation of the computational efficiency. The analysis of security and privacy is the result of joint work with co-authors.

Secure and Privacy-Friendly Multimodal Biometric Authentication using Cloud-based Identity Providers

Christina-Angeliki Toli, Aysajan Abidin, Abdelrahaman Aly, Enrique Argones Rúa, and Bart Preneel

imec-COSIC KU Leuven, Belgium

Abstract. Biometric authentication is part of the daily routine for millions of users, enhancing their experience and convenience. Additionally, the adoption of biometric technologies for various applications has grown exponentially over the last decade. Due to the increasing demand for authentication solutions, cloud computing can serve as a means to deliver biometric services over the Internet offering numerous benefits, such as reduced cost, increased storage capacity, unlimited data processing, efficiency and flexibility. However, with the proliferation of cloud-based biometric authentication deployments, security and privacy concerns become more relevant than ever. Although biometrics provide strong guarantees in verifying users' identity, privacy regulations recognize biometric data as sensitive information. Over the last few years, numerous cloud-based biometric authentication architectures have been proposed in the literature. However, the majority, if not all, of them are unimodal and multi-factor models. Multibiometric designs have attracted attention in high security schemes as they offer improved reliability and accuracy. In this work, we propose a distributed approach for multimodal user authentication that allows incorporation of already existing biometric datasets in a secure and privacy-preserving manner. Specifically, the verification setup is designed to function as an expert system, using previously stored biometric templates that are held by distinct mutually untrusted cloud-based identity providers. We focus on biometric integration by exploiting a user-specific weighted score level fusion method that provides an optimum trade-off between accuracy and robustness. Our system uses Multi-Party Computation techniques to allow mutually distrusting parties to jointly compute the matching score without revealing any private data. The final fused score is only communicated to a single party. In contrast to the existing state-of-the-art in cloud-based biometric identity management architectures, our system provides multimodal authentication without having to re-enroll the users

by collecting their biometric samples, preventing any additional biometric extraction and storage of users' private information. The proposed design is analyzed to demonstrate its usability, security, privacy, computational efficiency and applicability.

Keywords: Biometrics · Score Level Fusion · Distributed Identity Management · Secret Sharing, Multi-Party Computation · Secure Distributed Systems · Cloud Security · Cryptography · Privacy

1 Introduction

In the era of technological evolution, automatic recognition of users has become fast and easy. A major issue with traditional user authentication techniques, such as passwords, is the existence of too many password-account pairs for the same username across several services [31]. Moreover, tokens, smart cards and digital signatures can be forgotten or lost, resulting in increased security threats and privacy concerns [116]. Initially, biometric authentication has primarily been used in forensic science and the military, and it is seen as an accurate method of recognizing individuals from their unique anatomical, physiological or behavioral characteristics [122]. Nowadays, authentication technologies based on unimodal biometrics and multi-factor schemes (e.g., single biometric modality and password) are considered more convenient by the users of the smartphones while they are used on a daily basis in government, health-care, financial and business applications, Wazid et al. [223]. Moreover, multimodal designs that integrate multiple biometrics have proven to be more secure and reliable, managing to supersede the unimodal and multi-factor authentication approaches due to their effectiveness [39, 182]. A recent report of 2018 presented by IndustryARC [91] concludes that multimodal models are practical and robust while it addresses their applicability in the next generation biometric systems. Finally, according to the results from a recent survey commissioned by VISA in 2018 [220], biometrics win the favor of users and the day when biometric implementations completely substitute the other traditional recognition technologies is drawing nearer.

Over the last years, the biometric verification of a claimed identity in online services is growing rapidly [15]. According to the study of Acuity 2018 [5], all smartphone devices will have at least some kind of an embedded biometric technology by 2019, while by 2020 the technology will be applicable to wearable tech and tablets. Such expectations induce an enormous increase of the amount of biometric data, requiring sufficient storage capacity and a significant processing power [163]. In the age of the Internet, the need for highly accessible, scalable

and secure biometric deployments leads to the move of the existing biometric technology to the cloud [15]. This is mainly due to the cloud computing promising benefits of unbounded resources, parallel processing capabilities, better flexibility and cost reduction [11]. In addition to the widespread use of mobile devices, the cloud provides an accessible entry point for various services for mobile consumers [202]. Thus, the remote computation environment in the cloud is capable of addressing operational issues on large-scale datasets originated from various platforms and handling efficiently the challenges related to the next generation of biometrics [99]. Finally, it enables advanced applications including smart spaces, access control schemes, ePayment architectures and ambient intelligence systems, among others.

Furthermore, Acuity [5] estimates that biometric data will be outsourced to the cloud and more than 5.5 billion biometrically-enabled devices will create a global platform by 2022. It is expected that the cloud computing services will become even easier to use and service providers will be capable of authenticating more than one trillion transactions annually while the market volume will rise rapidly. A governance cloud-based Biometrics-as-a-Service (BaaS) framework leverages the cloud computing infrastructure, allowing for component developers to outsource custom tools for biometric recognition to the cloud [11]. Similarly to the Single Sign-On designs, BaaS offers identity management services via cloud-based Identity-Management-as-a-Service (IdMaaS) providers. Acuity [5] predicts that during the next years, many services will rely heavily on IdMaaS vendors that develop and outsource biometric extraction methods and matching algorithms for multiple biometric modalities, allowing for convenient and secure user authentication. Therefore, Authentication-as-a-Service (AaaS) is being studied as a new cloud service model that provides ubiquitous network access for performing on-demand authentication processes [202]. Although biometric local processing is usually seen as more convenient for the privacy of the users, there are numerous use cases, including these of the government and financial sectors, which can be benefit from the existing biometric datasets. For these scenarios motivated by law enforcement (e.g., fighting identity fraud and money laundering), the access and usage of large-scale information in the cloud are essential.

However, the protection of user's data remains the biggest challenge for the migration of biometrics to the cloud, preventing service providers and organizations from trusting the cloud and taking advantage of its computing resources [11]. Biometric data are sensitive personal information by nature and their storage, transmission and processing across third parties could result in compromise [96, 99]. Thus, the European Regulatory Technical Standards for Strong Customer Authentication [183], following the European General Data Protection Regulation (GDPR) [66] define the privacy principles and

the security requirements for cloud schemes that support different security objectives for the storage of biometrics. The regulatory compliance requires the incorporation of cryptographic techniques for the security of biometrics in order to address the threats to the privacy of the user when his data are stored in a Centralized Biometric Database (CBDB). Additionally, cloud providers that perform IdMaaS and AaaS tasks must use encryption schemes to protect data and must offer to the users the control over their own data in accordance with the security recommendations of the legal framework [27]. Traditional encryption does not allow processing of encrypted data and therefore it cannot preserve the privacy of biometric information processed in the cloud. Current secure cloud storage schemes rely on different cryptographic primitives, such as homomorphic encryption and template protection mechanisms as privacy-friendly approaches in an environment with untrusted parties [109]. Nevertheless, users' profiles including information such as access patterns and cloud connections may still remain available to the parties involved in the computation, thus disclosing information that affects the users' rights to privacy [39]. The rise of BaaS schemes in a variety of applications has led to the necessity for more secure practices, taking into account data leakage and attacks [202].

Currently used commercial BaaS offers unimodal biometric AaaS as described by IndustryARC [91]. Figure 1 illustrates a typical architecture. 1) The user requests the registration to a service. The service provider (SP) authenticates the user based on biometric data. However, it does not have the authorization or expertise to process the biometric features. For that reason, the SP redirects the user to the cloud-based BaaS third-party provider that performs the biometric authentication. 2) During the enrollment phase, through the use of a mobile-enabled web application of the SP and the embedded camera on his smartphone, the user provides identity credentials and presents his facial biometric to the cloud computing infrastructure. The interface involves a unimodal IdMaaS provider that establishes the list of user identities while it manages authorization and maintains user permissions. Additionally, this provider is in charge of extracting the biometric features and securely storing the biometric data while it outsources the algorithms for the template generation which includes the binary representation of the extracted samples. Hence, it can offer AaaS services. It is noted that the IdMaaS developers may follow and outsource different methods to determine a matching result. 3) The third stage of the enrollment involves the secure transmission of the user's biometric information that are placed in the encrypted DB of the IdMaaS which includes the stored templates of the enrolled users. 4) During the authentication process, the user who wants to login to the service, is redirected by the SP to the IdMaaS. 5) The user presents his fresh biometrics. 6) In the computing infrastructure through the tools of the IdMaaS provider, the biometric data are securely extracted and the new template is created. 7) During the matching operation or module, which is

the term used in the area of pattern recognition [122], the new and the stored templates are securely transmitted and compared. 8) The decision module involves the comparison of the matching score with a predefined threshold. 9) The SP communicates the result of this final module that determines the access of the user.

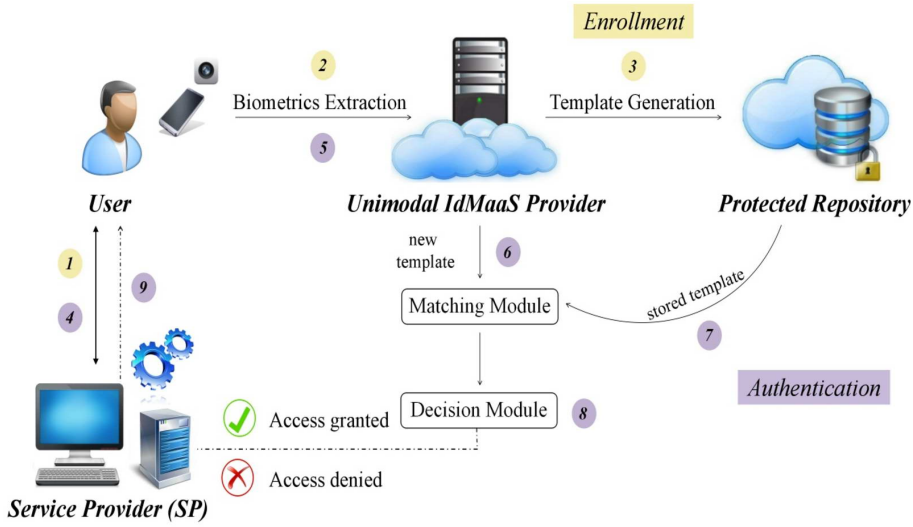

Figure 1: Unimodal biometric recognition as a cloud-based service.

Biometrics in cloud-based services and user authentication using remote IdMaaS providers have an enormous market potential and present important research challenges [5, 11, 15]. However, the available literature on multimodalities in BaaS is still scarce. Motivated by biometric recognition services adopting cloud computing, we introduce a less invasive, secure and privacy-preserving system for multimodal biometric authentication in the cloud. Similar to the previous example, the SP that requires the biometric authentication of the user redirects him to a cloud-based multimodal AaaS computation environment. The purpose of our approach is to reduce the privacy risks of an additional re-enrollment phase such as the collection and access to more individual's data and their possible misuses. In this way, we avoid an auxiliary temporary or permanent storage of user's biometrics in a CBDB, in order to decrease any further inappropriate use of personal information that can lead to users' identity tracking and monitoring. The main **contributions** of our work are:

- We introduce a protocol for biometric authentication that exploits prior stored unimodal templates collected in distinct DBs by AaaS providers that we call unimodal authenticators (UAs).

- To obtain a multimodal result, the matching scores of the distinct unimodal subsystems of the UAs are combined to determine a final fusion score. We use Hamming Distance matching algorithms and a user-specific weighted score level fusion method for the integration of unimodal matching scores into a final fused score.
- Our distributed approach involves a multimodal identity provider (MIP) that is responsible for the cooperation of the UAs and their communication between the SP and consequently the user. The MIP performs the IdMaaS tasks for the transmission of the user's new templates to the UAs while it receives the fused score, sets the system's final decision threshold and communicates the authentication result to the SP.
- Taking into account the strict privacy concerns that may limit the design and implementation we use Multi-Party Computation (MPC) techniques to utilize the stored templates in a privacy-preserving decentralized manner and to achieve secure multimodal fusion.
- Using a virtualized computation environment, no sensitive privately held data are exposed to any untrusted third party involved in the computation. The MIP and the UAs do not learn the freshly acquired biometric data, the stored templates, the unimodal matching scores, the fusion score or any derived information from them. There is no leakage of data towards the SP except of the unique output for the acceptance or rejection of the user.

The remainder of this paper is organized as follows. Section 2 discusses the related work. Section 3 presents design preliminaries on multimodal authentication and on the MPC techniques used for building the security protocol. Section 4 elaborates the proposed system, which is followed by a security and privacy analysis in Section 5, and a performance evaluation in Section 6. Finally, Section 7 outlines the potential advantages and limitations of our approach while Section 8 concludes this paper and describes future work.

2 Related Work

During the last years, research has been focused on biometric authentication schemes as a secure method to access cloud services [99]. There are several studies, such as the works in [160, 163] that address the advantages that cloud can offer to biometric schemes, while the work in [21] underlines the security and privacy threats of this integration to an untrusted infrastructure. In the context of unimodal user authentication, the authors of [134] proposed an iris recognition system implemented in the cloud to speed up the matching process of biometric traits. Similarly, Blanton and Aliasgari in [25] designed a secure framework

for outsourced computation for iris matching that can be implemented in a cloud setting. Additional unimodal architectures include the model of Zhu et al. in [231] performed a voice-based authentication using homomorphic encryption to secure the matching phase in the cloud. The work of Xiang et al. in [225] introduced a privacy-preserving protocol for face recognition with outsourced computation. Moreover, Omri et al. in [155] proposed a cloud-based design for handwriting recognition using classifier algorithms to handle the degradation of the recognition accuracy, while the authors in [230] presented a complete analysis on the biometrics extraction, storage and matching for a cloud-based mobile signature authentication.

Wang et al. in [222] presented a remote privacy-preserving biometric identification based on fingerprints placed in an outsourced domain. The protocol is built on a prototype encryption model for distance-computation. However, the authors of [162] showed that the security assumptions for the scheme of Wang et al. were not realistic and failed to take into consideration possible privacy issues created by the information collection and distribution over several SPs. Based on these findings, the work in [84] showed a practical attack that enrolls fake fingerprint data and then manipulates them to recover the encrypted identification request. The authors also addressed the fact of the performance degradation of the approach of Wang et al. while they suggested several solutions for improvements. Zhu et al. in [232] focused on the encryption scheme that provides an efficient model for privacy-preserving unimodal identification in the cloud, while Talreja et al. in [202] designed a generic AaaS framework for remote user-specific unimodal authentication, providing a selection on matching algorithms to achieve an ecosystem that benefits both SPs and users.

Furthermore, Sarier [187] introduced the first protocol resistant to hill-climbing attacks for multimodal biometric authentication in the cloud, working with Euclidean Distance for the matching procedures on encrypted stored templates. However, the recognition is performed on unimodal templates of fingerprints or stored multimodal biometrics, where data recollection and transmission may violate the privacy regulations as described in [183]. In the context of the MPC techniques for BaaS purposes, the authors of [88] proposed a unimodal matching on fingerprints using MPC to enhance privacy during the calculation stages of authentication. Finally, Blanton and Saraph in [26] described a secure framework for unimodal matching that can be applied in a cloud. The design avoids the storage of biometrics and the usage of MPC helps to protect the results from the untrusted parties.

Unlike the related works, our system offers AaaS using distinct cloud-based providers, without an additional enrollment phase and the presence of an additional CBDB. It performs multimodal fusion on already stored unimodal sets through Hamming Distance matching algorithms and MPC techniques,

and thus it avoids the loss of recognition accuracy and functionality. There is no storage of multimodal templates while the stored unimodal biometrics, the matching scores and the fused result are unaccessible by the remote providers. The studies presented in [208, 209] described a new fusion model, an overview of how MPC can be combined with biometrics and an attempt to focus on the privacy violation concerns that may occur during the calculation phases of recognition, from the interactions between untrusted parties. In this paper, we use part of their insights and present an integrated secure system. Moreover, we take into consideration the work of Bringer et al. in [36] on the impact of MPC techniques on identification schemes in terms of accuracy, security and privacy. To the best of our knowledge, our work is the first to present such configuration in a detailed fashion, providing an efficient secure and privacy-preserving system that follows a less invasive process for multimodal biometric AaaS and addresses the recommendations of the new European GDPR [66].

3 Preliminaries

This section includes the concepts and terms for our system related to the feature recognition, matching and fusion. Additionally, the assumptions and requirements used in the design of our secure protocol are detailed.

3.1 Background on Multimodal Authentication

Unimodal Biometric Recognition

Biometrics are based on pattern recognition techniques applied to the statistically unique parts of biometric modalities in order to allow recognition [99]. For the use-case scenario of our multimodal AaaS system introduced in Section 4, we selected face, fingerprint and iris biometrics. These biometric features have gained considerable attention leading to their broader acceptance and trust in schemes that integrate these features; they are currently preferred over other modalities, as indicated in [20]. Below, recent state-of-the-art approaches for face, fingerprint and iris recognition are summarily presented; their extensive analysis is outside the scope of this paper. According to the findings that are presented in [36, 122, 229] the technique of Hamming Distance for biometrics recognition is widely used in current commercial deployments, presenting reliable results in terms of accuracy. For that reason, our system performs the matching process of unimodal sets based on Hamming Distance algorithms. It is noted that the authentication protocol can be adapted to support different (or even

more than three) biometrics and recognition methods that can be calculated over an arithmetic or Boolean circuit, as presented in [25, 26].

Face Recognition Euclidean Distance and facial texture features are the newest techniques in the field of face recognition that can offer an improved accuracy in face recognition. In the literature, there are several approaches that take advantage of statistical facial characteristics that are robust to noise. Ahdid et al. in [7] introduced a notable face recognition scheme that outperforms the classical Euclidean Distance approaches, as proposed in [70]. However, the Hamming Distance technique is considered to be an easily applicable and efficient way to perform matching in various infrastructures as underlined in [15].

Fingerprint Recognition Fingerprint recognition is a challenging task since a varying number of minutia features and ridges from fingerprint characteristics need to be matched. Recently, the technique suggested by Palanichamy and Marimuthu in [161] shows that matching based on distance algorithms can offer promising recognition accuracy. Although their work contributes to the field of fingerprint recognition, the performance of their proposed image alignment and the minutia matching algorithms are still under evaluation. The mixed model of Martin and Cao in [138] is based on a Hamming Distance algorithm. The authors experimentally analyzed the applicability of their method and presented the performance improvements, showing reliable results. Therefore, nowadays their approach is considered to be the basis for the next generation of highly secure fingerprint-based schemes.

Iris Recognition Hamming Distance algorithms are popular and widely used in iris recognition methods. Rai and Yadav [169] proposed a technique that correlates the area of iris for the extraction of the feature, capturing only a small part of the biometric pattern. The method of minimal data is used in order to protect user privacy. To expand the recognition level, their technique involves vector machine models and a Hamming Distance approach. Finally, filters are used for feature extraction to improve the authentication performance. The work of Dehkordi and Abu-Bakar in [61] introduced a Hamming Distance technique applied on subsets with an adaptive length. Their results provide a significant increase in accuracy of iris matching.

Thresholds and Performance Rates

The confidence in the functionality of a biometric scheme is determined by specific measures that are used to evaluate the accuracy and effectiveness [182].

Thresholds are defined to decide if a user does or does not correspond to a claimed identity. In multimodal recognition schemes there are two categories of metrics, named *Reference Thresholds* ϑ_i for the unimodal recognition of the modality i and *Decision Thresholds* τ for the multimodal scheme respectively. During the comparison in the matching process based on Hamming Distance algorithms, the generated matching score s_i, after the comparison of the new and stored templates, can be analyzed on the basis of a predefined threshold ϑ_i. In biometric designs, the decision result is represented as 0 which means that the template is not matching and the authentication is rejected; and 1 that corresponds to an acceptable match for the user recognition. For recognition systems that follow a matching algorithm that is based on the calculation of distances between the new and the stored templates, the decision result is represented as:

$$\begin{aligned} s_i \leq \vartheta_i \quad & \text{Accept} \\ s_i > \vartheta_i \quad & \text{Reject}\,. \end{aligned} \tag{1}$$

Similarly, for multimodal recognition approaches that perform matching using algorithms that compute the dissimilarity of the templates, the fused score sf, given the system's τ is compared as follows:

$$\begin{aligned} sf \leq \tau \quad & \text{Accept} \\ sf > \tau \quad & \text{Reject}\,. \end{aligned} \tag{2}$$

Based on Hamming Distance algorithms, the comparison between the new and stored templates and consequently the s_i and ϑ_i reflect a genuine/authentic person, or an impostor/intruder score if there is an inadmissible distance. However, biometric data are inherently noisy and thus unimodal and multimodal biometric recognition suffer from error rates [122]. Hence, schemes hardly ever encounters a user's fresh biometric trait and a stored template that result in a 100% match. According to the analysis of Malik et al. in [130], the statistical calculation of ϑ_i is related to the biometric system's performance rates. The most important rates that are used to evaluate the performance of a biometric recognition scheme are the False Acceptance Rate (FAR) and the False Rejection Rate (FRR). For each unimodal biometric feature i given a ϑ_i, for a matching score s_i, the $p(s_i \mid \text{genuine})$ represents the probability of distance values for a given matching score s_i, between the new and stored templates, under the genuine conditions. Correspondingly $p(s_i \mid \text{impostor})$ indicates the probability for the impostor conditions. Figure 2 illustrates the distribution of matching scores and its relation to FAR and FRR [182].

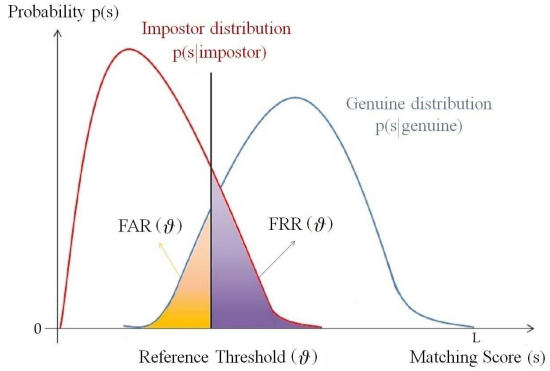

Figure 2: The genuine and impostor distributions.

In the literature, for impostor and genuine users, the performance rates are usually represented as integrals [182]. In practice for our protocol, working on Hamming Distance algorithms and binary templates, for an impostor who is not enrolled in the unimodal scheme based on the modality i, for a threshold ϑ_i and a given length L of the experimental unimodal templates, the matching score $s_i = 0$ means that two templates match perfectly, while a matching score $s_i = L$ reflects the condition where the templates present an inadmissible distance. In this way, the FAR_i is calculated as follows:

$$\mathrm{FAR}_i(\vartheta_i) = \sum_{s_i=0}^{s_i=\vartheta_i} p(s_i \mid \text{impostor})\,. \tag{3}$$

Accordingly, the FRR_i is given by:

$$\mathrm{FRR}_i(\vartheta_i) = \sum_{s_i=\vartheta_i+1}^{s_i=L} p(s_i \mid \text{genuine})\,. \tag{4}$$

The accuracy of the unimodal biometric scheme is given by:

$$\mathrm{Accuracy}_i(\%) = 100 - \frac{\mathrm{FAR}_i(\%) + \mathrm{FRR}_i(\%)}{2}\,. \tag{5}$$

Training Datasets

The distributions of Figure 2 and Equation (5) illustrate the effect of ϑ on FAR and FRR on the biometric scheme's accuracy. For unimodal designs, the

performance of tests on the biometric data is an essential technique in order to achieve an acceptable value of FAR, or select an optimum FRR for the purposes of the recognition schemes [203]. This can be achieved by training the applicable algorithms for examining how the system behaves under different values of ϑ. Tuning the system's threshold is a technique to study the performance accuracy under a given procedure; this process always effects not only on the decision module represented in (1), but also the corresponding rates of the system, as underlined in [130, 182]. In real-world deployments, training is not always adequate, as a result of the time, effort, cost and the privacy regulations for the collection of biometric information [116, 122].

The technique plays an important role in fusion methods that integrate the results of multiple biometrics to obtain a final multimodal score [182]. In multimodal designs, each contributing biometric modality i provides a user-specific FAR_i and FRR_i, given a ϑ_i. It is noted that these rates cannot be reduced simultaneously by adjusting the ϑ_i. For instance, working with Hamming Distance matching algorithms, a lower threshold decreases the FAR and it is used for enhancing security, while a higher threshold increases the user's convenience [182]. In that way, systems with high requirements in terms of robustness and security may set a user-specific FAR approach to determine the final fused result. On the contrary, a higher FRR is considered to be more convenient in order to increase the number of matching results, expanding the recognition range for identification applications such as government services that perform investigations for missing persons. However, in practice it is necessary to select an optimal solution in order to avoid an extensive number of false acceptances and to reduce the need for human intervention. Section 3.1 analytically presents how these rates can be used in fusion strategies to increase the accuracy. We emphasize that the purpose of our system is to avoid a re-enrollment procedure. The user is already enrolled in the remote UAs of the cloud and thus the ϑ_i, FAR_i and FRR_i are parameters that these parties in the cloud hold and tune. It is assumed that the training procedures on the unimodal datasets are carried out by third parties and any related specific computations are outside the scope of this work.

Score Level Fusion

The works in [180, 182] have shown that unimodal biometric designs suffer from several issues, for instance noise and spoofing attacks. Multibiometrics can solve these limitations and surpass even multi-factor authentication schemes by extending the feature space to increase security and identification reliability [99]. However, the concept of multimodal integration and the selection of a convenient fusion model is still a challenging task [143]. In a multimodal recognition system,

biometric fusion represents an active area with numerous approaches; it can be accomplished at several levels and by several strategies using the biometric data prior to matching, at the decision or after the matching stages. Furthermore, multimodal deployments are governed by the type of biometric data and sources, the acquisition, the processing stages and the final application.

Given the purposes of our multimodal AaaS system, user authentication takes place in a distributed environment where the matching scores of the distinct subsystems of the UAs are combined to determine a final score. In this work, we use the term *fusion* to describe the consolidation of matched unimodal templates in a single score that is called *multimodal result*, as described in *"Handbook of Multibiometrics"* [182]. For the functionality of our proposed system, the selection of biometric consolidation at the decision level was discarded because of the inconvenience that current fusion methods may cause in practical architectures. Techniques such as Daugman rules, conditions in majority voting, Bayesian decision, Dempster-Shafer theory and behavior knowledge space, present high values of FAR and FRR, resulting a lower accuracy; even if they have been used in some commercial multimodal biometric systems, they are considered inefficient for high security applications, according to the results presented in [182, 203]. Thus, a fusion technique after the matching process is the preferred option, following the study in [206].

Match score level fusion, also known as fusion at measurement or confidence level is a widely used fusion approach in current biometric architectures due to its reliability. Jain et al. in [101] showed that this technique provides an improved performance in comparison to other methods, while it allows an easy integration of modalities extracted by diverse sensors. Recently, Tiwari and Gupta in [206] introduced a score level fusion scheme and tested it on several biometric datasets. Their experimental evaluation shows a strong authentication accuracy with low error rates in comparison to the performance of the unimodal subsystems.

User-Specific Weighted Score Fusion Predicting the performance of a multimodal scheme following a particular score level fusion method is almost impossible. Ross et al. in [182] noted that the performance can only be evaluated based on empirical results. However, as presented in Section 3.1, every user exhibits different performance rates in biometric schemes, and thus it is possible to further enhance the accuracy of a multimodal design by using user-specific score fusion techniques. According to the findings in [181], in a fusion model performance rates can be applied in such a way that they can assign different degrees (weights) of importance to the various modalities on a user-by-user basis. This means that a set of different weights, representing the user's FAR

function (3), FRR function (4) or even the overall accuracy, given by Equation (5) of the unimodal recognition subsystems, were applied to determine the fusion result. Recent experimental studies such as the works presented in [4, 192, 219] have exploited it in order to test it or even suggest complementary measures for fusion methodologies, presenting important improvements in the performance of multimodal deployments from uncorrelated unimodal biometrics.

In this work, we utilize a user-specific weighted score level fusion method to incorporate the unimodal scores of the cloud-based UAs to achieve a final fused multimodal result for authentication purposes. In real-world deployments, the matching scores obtained from the biometric matchers are non-homogenous measures with different scales, where $\{-1, +1\}$ is typically used for faces, a unit interval $\{0, 1\}$ for irises, and $\{0, 100\}$ is the range for fingerprints. Therefore, a normalization technique is usually followed prior to the fusion phase [101]. However, as presented in [182], setting a sum rule in a user-specific weighted fusion to determine the final fused result, the normalization process can be omitted due to the linear weighting coefficients. In a system with M modalities, where modality i has weight w_i, and the unimodal matching score is equal to s_i, the final fused score is computed as follows:

$$sf = \sum_{i=1}^{M} w_i s_i \,. \tag{6}$$

According to the findings in [4, 85] the sum rule in a user-specific weighted fusion improves the performance of the scheme. Figure 3 summarizes our experimental analysis on their findings based on face and fingerprint biometrics of NIST [152], and iris datasets found in CASIA [43] public available research DBs. The Receiver Operating Characteristic (ROC) curve of fusion, following Equation (6), combines the three unimodal biometrics and presents the quality of the recognition performance. Moreover, the authors in [182] discussed the effects of the equal and user-specific weights on the overall accuracy of the fusion model. Based on the study of Verma and Singh in [219] and the experiments of Manasa et al. in [132], Figure 4 illustrates our analysis on the improvement of the performance on a multimodal scheme of fingerprint on NIST [152], palmprint and iris on CASIA [43] datasets respectively. When user-specific different weights are applied according to the FAR of each user, a significantly better ROC curve is obtained than when equal weights are used for the three biometric traits.

From the figures and the analysis of Tao and Veldhuis in [203], we can assess the importance of the final *Decision Thresholds* and the training datasets for the overall performance and robustness of a weighted score level fusion model. It is noted that the biometric matching algorithms and the size of the

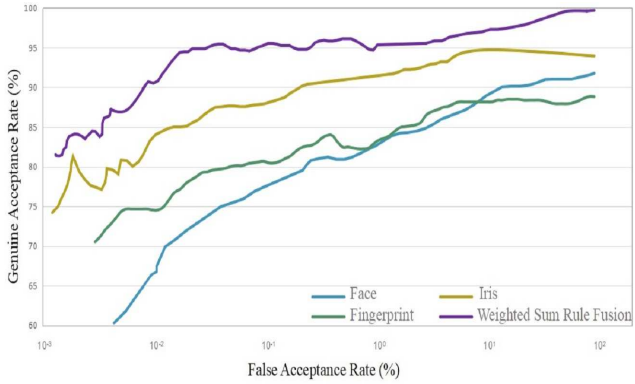

Figure 3: Comparison of unimodals and weighted sum rule fusion.

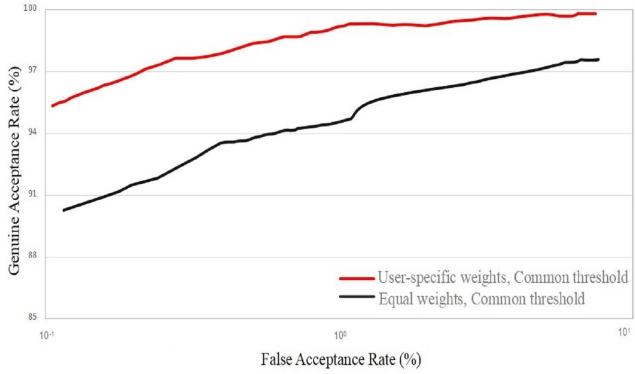

Figure 4: Comparison of recognition performance for weighted scores.

datasets in the DBs have great impact on the outcome of an evaluation [24]. A user-specific weighted fusion with a sum rule is considered to be a beneficial approach in multimodal designs where unimodal information is provided by different subsystems and the performance varies across the population. Finally, in our scenario for a multimodal AaaS system, we choose to follow this fusion technique to incorporate face, fingerprint and iris for user recognition. However, it is underlined that specific calculations on thresholds and performance rates for the selection of user-specific weights are outside the scope of this paper.

3.2 Achievable Security with MPC

To handle the privacy concerns, which may limit the design and implementation of our system for multimodal authentication in the cloud, we use secure Multi-Party Computation (MPC). This collection of techniques allows any set of parties to compute a publicly available function without requiring the parties to reveal their private inputs. Additionally, depending on the model, the security offered can vary from computational to information theoretic or perfect security [17]. The field was at first regarded as purely theoretical, but recently interest has grown by the emergence of practical Virtual Ideal Functionality Framework (VIFF) as a tool that implements functionalities for general MPC on asynchronous networks [71]. The commercial implementations, such as the Sharemind framework [28], have also led to an increased research attention for improvements. Recently, protocols such as SPDZ [56, 58] and BDOZ [18] have been added to the mix, providing robust security properties, such as passive and active security in the presence of dishonest majorities. In our work, MPC is used to build a protocol that can ensure the secrecy of biometric templates and protect private information during the authentication stages.

Security under MPC addresses the confidentiality of the private inputs with respect to the parties involved in any computation stage of the protocol. MPC is used for security reasons against typical privacy adversarial models, such as honest but curious and malicious adversaries, offering various security levels, from statistical to perfect security [17, 58]. We define security under MPC as follows:

Definition 1. *(**Security**): Consider $I = P_1, ..., P_n$ the parties that want to compute a function $y = f(x_1, ..., x_n)$, where x_i is the secret input of P_i. Then, any protocol π that computes y is secure if the parties do not learn anything but the output y and what can be inferred from y.*

This definition implies that no party P_i should learn any information from the private inputs of P_j, $\forall j \in I$, where $i \neq j$, except what can be inferred from the output. Note that in our authentication system, the SP knows the credentials of the user. Finally, access patterns towards the protocol could also be statistically hidden, as explained in the following sections. To ease security analysis and the protocol description, we use the following arithmetic black-box as an abstraction that idealizes access to a certain secure functionality.

Arithmetic Black-Box

We use and extend the arithmetic black-box in [57] based on a composable efficient MPC from threshold homomorphic encryption. The original arithmetic

black box was built under the composability hybrid model presented by Canetti in [41] and proved secure against passive and active adversaries. This makes simulation proofs straightforward, where the simulated view of any P_i is the same as the adversary's view, reducing the complexity of our security analysis. The black box in [57] could be seen as a virtualized entity capable to store field elements over $\mathbb{F}_p$, where p is any sufficiently large prime number or RSA modulus. It also provides secure addition and multiplication with a scalar and between secretly stored values. The basic functionality of our arithmetic black-box $\mathcal{F}_{ABB}$ can be achieved by well-known protocols for homomorphic encryption, such as the cryptosystem in [159], or linear secret sharing schemes [190]. The addition and multiplication provided by the $\mathcal{F}_{ABB}$ use well-known MPC protocols, based on the properties of the cryptographic sharing primitive selected. These categories include the BGW protocol in [17], BDOZ in [18], SPDZ in [58], MASCOT in [113] and the highly specialized three-party protocols in [13].

Arithmetic Black-Box Extension

Following the work presented by Lipmaa and Toft in [126], we proceed to extend our black box, in order to have inequality tests for our protocol. Arithmetic circuits and protocols for ***secure comparison*** have been introduced in [44,55], among others. Inequality tests can be found in [126], where the authors use the same $\mathcal{F}_{ABB}$ conceptualization. In the context of our $\mathcal{F}_{ABB}$ extension, the following operations are provided:

$$[z] \leftarrow [x] \overset{?}{=} [y] \mid [z] \in \{0,1\}\,. \tag{7}$$

$$[z] \leftarrow [x] \overset{?}{<} [y] \mid [z] \in \{0,1\}\,. \tag{8}$$

3.3 Assumptions

We assume that the embedded biometric sensors are tamper-proof devices. A Public Key Infrastructure (PKI) is available in order to establish a secure channel for the transmission of the newly extracted biometric samples from the user to the multimodal AaaS system. To protect the privacy of the user towards the cloud-based providers, the new and stored templates are distributed in the cloud using a secret sharing key scheme. The reference thresholds ϑ_i that determine the unimodal authentication are held and tuned by the cloud-based UAs and they secretly share them during the execution of the protocol. Regarding the training procedures and the user-specific weighted score level fusion, we assume that UAs hold and calculate the performance rates FAR_i,

FRR_i and the parameters for the accuracy. We make the assumption that they carry out the training of the matching algorithms on their unimodal datasets by regulating the ϑ_i while they also utilize established techniques to manage the user-specific error rates. As mentioned previously, the calculation of these rates and any related actions on the computing of such metrics are outside the scope of this paper. Finally, the UAs are considered to be untrusted computational parties. However, due to their conflicting and competing interests, UAs do not collude.

3.4 Notation

We assume that all inputs and intermediate values are elements of a finite field bounded by p ($\mathbb{F}_p$), such that $x \ll p$, for any value x in $\mathbb{F}_p$, in order to avoid overflows. We assume that the underlying cryptographic primitive is secret sharing. Additionally, we use the notation introduced in [57], where $[x]$ represents the secretly shared value of x. To express operations provided by the $\mathcal{F}_{ABB}$, we use the infix representation $[z] \leftarrow [x] + [y]$. In reality, the operations (addition, multiplication gates) are provided by the underlying protocols, as referred to Section 3.2. Our protocol is as secure as the underlying MPC functionality that is implemented. Negative numbers are represented in the typical way, where the lower half of the $\mathbb{F}_p$ field represents the positives and the other half the negatives.

Under the $\mathcal{F}_{ABB}$ model, the complexity is measured by the number of the non-concurrent black-box operations that are executed. MPC protocols based on linear secret sharing schemes can offer addition of shares and scalar multiplication, approximately at the same cost of similar *"plaintext"* operations. However, multiplications require information exchange between the computational parties since common MPC protocols work on linear secret sharing schemes and the non-linear operations require additional information that is hold by different parties [58].

Concurrent operations that require information exchange between parties is referred to as a communication round. Comparisons are by themselves arithmetic circuits, composed of addition and multiplication gates. Their computation and communication cost is much higher than for a multiplication, and thus is in the interest of the algorithm designer to minimize their use.

4 Proposed Multimodal Authentication System

This section describes our novel multimodal authentication system using cloud-based providers. Prior to the detailed description, we first give an overview of the scheme which is depicted in Figure 5. The user requests the login to a service. The SP wants to authenticate the user based on biometric information. In our indicative scenario, the SP requires a multimodal authentication result based on three modalities (face, fingerprint, iris). However, the SP does not have the authorization, expertise or intention to be involved in the biometric feature recognition. For that reason, the SP redirects the user to the multimodal AaaS system. The computing infrastructure involves third parties that operate as unimodal AaaS providers with their unimodal DBs outsourced to the cloud. It is assumed that the user has already been enrolled in the remote unimodal subsystems of these providers to be authenticated for several applications and services that require unimodal recognition. The architecture includes the transmission of the user credentials, such as his name, from the SP and the presence of his fresh biometric samples from the user. According to the purposes of the service, the preferences and the requirements of the SP, the user's biometrics can be submitted locally to the SP's sensors, or on any other device with embedded sensors that corresponds to the web application of the SP. The credentials and the new template of the extracted biometrics are encrypted and securely transmitted to the multimodal AaaS system. The third parties search to their cloud-based DBs for the corresponding stored templates and securely perform unimodal authentication and multimodal fusion. Given the application and the recommendations of the SP, the AaaS system sets the decision threshold of the overall authentication procedure, and communicates the output to the SP. The user learns from the SP whether his access is granted or denied.

4.1 Parties and Roles

For an in-depth examination of the infrastructure and functionality of the multimodal AaaS system, Figure 6 illustrates the distributed cloud-based providers and presents the interaction diagram of the parties in our design.

User: This entity wants to access various services provided by the SP and requests the login to the service. The user may also carry a personal device that he uses to authenticate himself while he performs the authentication-related action by presenting his fresh biometric features.

Service Provider: Party that is interested in the authentication of the user. SP knows and holds the credentials of the user and transmits them to the multimodal AaaS system. The SP may hold a device with embedded sensors

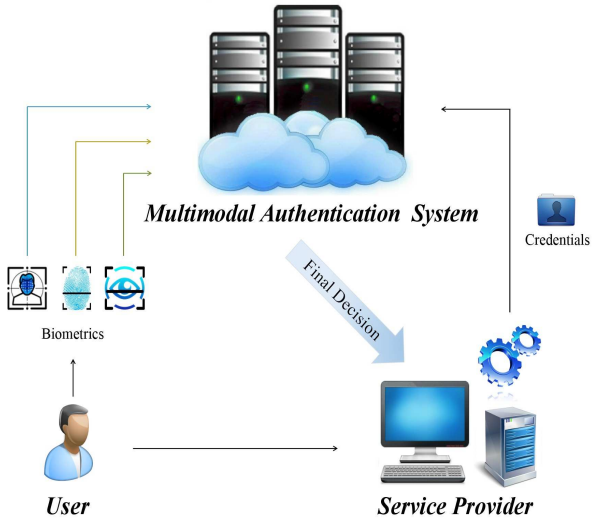

Figure 5: An overview of the proposed multimodal authentication system.

and request the submission of user's biometrics locally. The entity does not actively participate in the computation. It is informed only of the final decision of the multimodal result.

Unimodal Authenticators: These parties operate as unimodal AaaS providers. They also can be considered as IdMaaS developers that establish the users' identities and outsource their tools for BaaS purposes. They hold their respective unimodal templates stored in distinct unimodal DBs and they are in charge of adjusting the reference thresholds ϑ_i of their unimodal subsystems. Moreover, they also use training techniques to manage the $\mathrm{FAR}_i(\vartheta_i)$ and $\mathrm{FRR}_i(\vartheta_i)$ parameters in order to select the user-specific weights w_i. We consider the maintenance of the templates to be an orthogonal problem. If the stored unimodal templates have to be updated in the DB of each UA, this can be directly managed by the authorized UAs that can adjust the biometric data of the user and recalculate the performance metrics, thresholds and weights of their schemes.

Multimodal Identity Provider: In our system, for clarity purposes this party is the product of the cooperation of the UAs. It is considered to be an IdMaaS intermediary provider that is responsible for the communication of the user and the SP with the cloud-based UAs in the computation environment. Towards the UAs third parties, MIP performs the tasks of the communication of the credentials of the user and the secure transmission of the encrypted

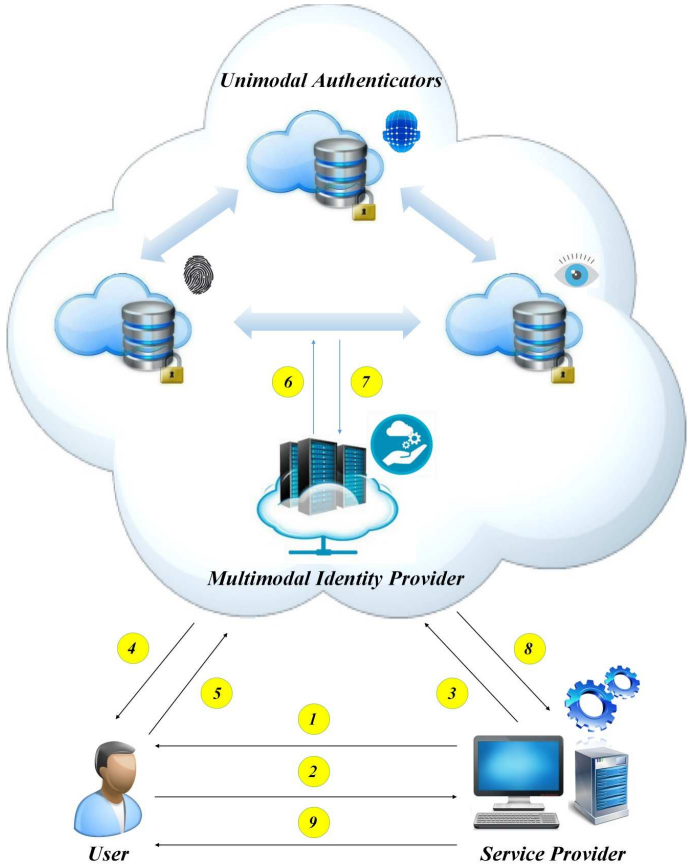

Figure 6: The multi-recipient architecture used in the design of the multimodal authentication system.

new templates that are generated from the sensors after the feature extraction module. Additionally, the MIP sets the final decision threshold τ and securely communicates the authentication result to the SP.

Input data: All the input data of the parties are considered to be private. In our privacy-preserving protocol, biometric information is represented in binary form; the data are measured and converted by the sensor and sent to the MIP and the UAs computational parties using secure private channels. We assume that input data are integers that can be represented as elements of the finite field $\mathbb{F}_p$. For fixed point precision, the data can be multiplied by a sufficiently large decimal constant. This procedure takes place to avoid complex decimal

arithmetic with arithmetic circuits.

Dealers: They have to provide inputs to the protocol for the computation in a shared form. In our case, the user provides the biometric data extracted by the sensors. Additionally, MIP receives the new templates and transmits the secret shares of the new templates to the UAs. The cloud-based UAs receive the secret shares of the new templates and transmit the secret shares of the stored templates. Finally, UAs communicate the parametrization.

Computational parties: They are the set of servers in charge of executing the protocol. They receive the shares from the dealers and execute the computation. The role of these parties can be executed by the UAs and partly by the MIP that sets the decision threshold. Note that there is no upper bound on the number of the involved computational parties.

Output parties: The parties that learn the final output. In our case, the SP and the MIP play this role while no other party, including the UAs, learns any auxiliary information besides their original inputs.

4.2 Threat Model

The users are considered malicious. A user might actively try to collect and alter the extracted new templates and/or stored and exchanged information within the multimodal AaaS system, in an attempt to gain access to the data or the service which he does not have the permission to access. *The SP is an active adversary.* It may try to learn information about the users. We consider that its aim might be to gain access to the computation environment, collect or modify the data in an attempt to disrupt and extract confidential information about users, other competitive SPs and the multimodal AaaS system iteself. The devices with the embedded biometric sensors can either by owned by the users or by the SP. In the first case, they *are trusted (tamper-evident).* We assume that these devices support cryptographic operations and the security mechanisms in order to provide access control and protection against malware. In the second case, according to the preferences and requirements of the SP, if the devices with the biometric sensors are held by the SP, then both the SP and the devices are considered honest-but-curious entities. The case that the SP gains access to the fresh biometric features and tries to learn the private data of the user is not included in the scenario. Within the distributed domain, *the MIP is an honest-but-curious entity.* It follows the mutimodal authentication specifications and it performs the protocol honestly, but it might try to collect the exchanged data, learn the calculation results within the computation environment and extract unauthorized private information about the users. *The UAs are malicious.* Although they do not collude due to

their competing interests, the data they calculate and forward to the MIP and consequently to the SP might be corrupted.

4.3 Authentication Phases

Following the interaction diagram of Figure 6, the next phases for the authentication of the user using our multimodal AaaS system are executed:

1. The SP that wants to authenticate the user requests an identification document or personal credentials.
2. The user transmits this information to the SP.
3. The SP communicates the credentials of the user to the cloud-based MIP.
4. The MIP requests the user to provide his biometric samples. For our scenario, the authentication is performed on face, fingerprint and iris samples.
5. The user presents his biometrics to the sensors of a device that is best suited to the operational requirements of the SP and it is compatible with the web application of the SP. During the feature extraction operation, the acquired fresh biometrics are securely extracted and their binary representation as new templates are transmitted to the MIP.
6. The MIP transmits secret shares of these new templates to the remote UAs. Figure 7 illustrates the authentication modules using a weighted score level fusion and represents the flowchart that takes place in the cloud. The UAs receive the secret shares of the encrypted new templates. According to the given user credentials, they subsequently transmit secret shares of their relative unimodal stored templates.

   For the unimodal matching score generation module, the computation domain uses the technique of Hamming Distance algorithms to match the biometric templates. Given the matching score of the user and according to the conditions of (1), each UA holds the reference threshold ϑ_i for its unimodal subsystem and it can compute the user's performance rates. During the weights selection operation, based on the results of FAR from Equation (3), FRR from Equation (4) or the overall accuracy given by Equation (5), the UAs define the weights on a user-by-user basis. It is noted that the ϑ and the performance rates of the user are considered to be private data and they are not transmitted in the interactive computation environment. Hence, the technical expertise of each UA for the calculation of weights is not accessible to the cloud-based parties. Additionally, since the weights are arithmetic metrics they cannot disclose any sensitive information about the

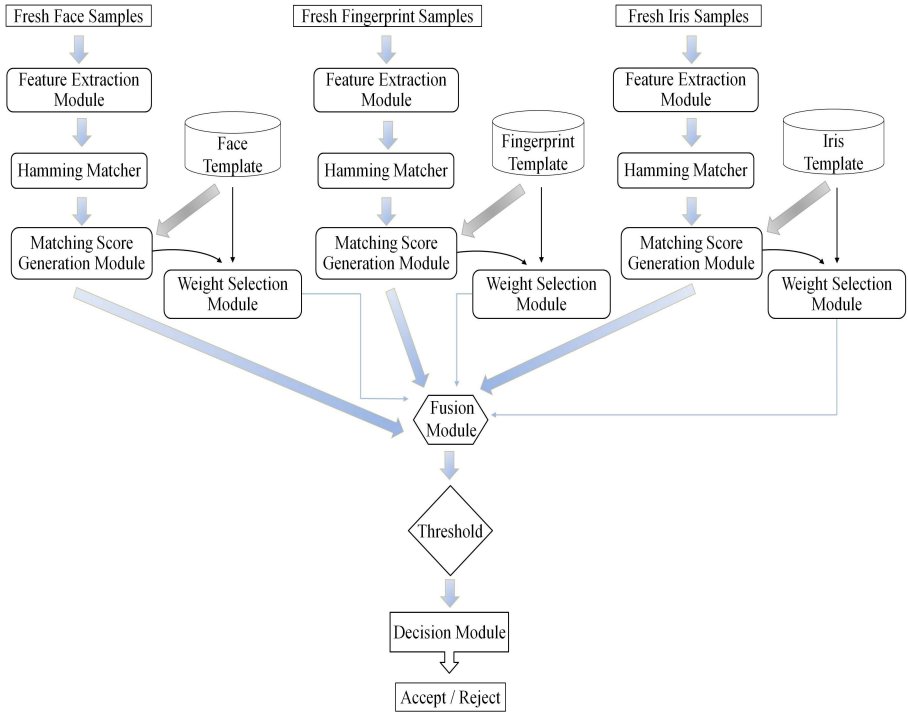

Figure 7: Flowchart of the multimodal authentication operations under user-specific weighted score level fusion.

user's identity and thus they are public and they are provided by the UAs to the AaaS system.

In the fusion module, according to our analysis in Section 3.1, the weights are used to assign different degrees of importance to the user's modalities. The proposed multimodal AaaS system incorporates the unimodal matching scores and the weights of the UAs by applying a user-specific weighted sum rule, given by Equation (6). Additional details regarding the selection of the user-specific weights based on the performance rates for score level fusion models can be found in [209].

7. The computation environment of the UAs secretly shares the result of the fusion module to the MIP. According to the purpose of the service application and the preferences of the SP, the MIP sets the decision threshold τ and compares the final fused score (6) following the conditions of (2). The output of the decision module is binary represented as 1 that means that the authentication is accepted, or 0 that corresponds to a failed user recognition.

The user is rejected when the system fails to correspond the new templates to the stored data in the DBs of the UAs, for instance when the user is not registered in one or more unimodal subsystems of the UAs and his biometric data are not stored in the unimodal DBs of these providers. It can also happen when the matching scores are poor, resulting a final fusion score that failed to surpass the threshold of decision.

8. The MIP communicates the binary output of the decision module to the SP.

9. The SP informs the user for his successful or failed authentication.

4.4 Distributed Calculation of Multimodal Authentication with MPC

In this section, we give a detailed treatment of our secure distributed protocol for the biometric authentication mechanism and analyze its complexity, security and privacy. To facilitate readability, we divide the process into the modules presented in Figure 7. In the context of the MPC, this is no more than a conceptual division rather than a tangible task separation. It is important to stress that they together form a unique and uninterrupted arithmetic circuit, with a single output point. The protocol does not suffer from the typical composability related security weaknesses presented by Canetti in [42]. Instead, our protocol is designed following the composable hybrid model for MPC introduced in [41]. To maintain privacy and adhere to the security definition, the modules are adapted such that any leakage of information is avoided, commonly referred to as data-obliviousness [44].

MPC Protocols

1. ***New template transmission:*** The MIP receives from the user the fresh templates. Note that the new templates represent the raw acquired biometrics and they are of a publicly known fixed size N^m for each $m \in M$ modality. They are encrypted either with the public keys of the servers or a distributed shared key. The MIP transmits the new templates in secret shared form, using an underlying sharing mechanism, such as the secret sharing scheme presented in [190], towards the computational parties. These parties could then learn their bit representation of the inputs as follows: $T_i = t_1, ..., t_N$ where $t_j \in \{0, 1\}$ for all $j \in \{1, ..., N\}$, by using mechanisms, such as the ones outlined in [55].

2. ***Stored template transmission:*** The service providers send the binary templates in shared form and the FAR and FRR for the given template to

the computational parties. We call the set of stored templates of a given modality O^M, and O_i is the i^{th} binary template where $i \in O^M$.

3. ***Calculate matching scores:*** The computational parties proceed to compute the scores between the new and the stored templates of modality M. The scores can be obtained obliviously, by utilizing the Hamming Distance algorithm to calculate distances between the new and stored template without any information leakage. As shown by Protocol 1, this can be achieved by performing N^M multiplications, where N^M is the size of the template of the M modality. The result of this phase is the vector of Hamming Distance scores H^M, where $[h]_i^M$ is new template score T versus the stored O^j, for all j delivered by the SP.

Protocol 1: Hamming Distance Protocol.

Input: Vector $[T]$ of, Vector $[O]$ where $[T]$ and $[O]$ are of size N.
Output: Hamming Distance $[h]$

for $i \leftarrow 1$ **to** N^M **do**
  $[\nu]_i^h \leftarrow [T]_i + [O]_i - 2 \cdot ([T]_i \cdot [O]_i)$;
$[h] \leftarrow \sum_{i=1}^{N^M} [\nu]_i^h$;

4. ***Select matching scores:*** The protocol selects the best suitable score from vector H^M for every modality M. This unique value per modality is the one that corresponds to the higher/lower score in each vector H^M. We call the vector, composed of the higher/lower scores of each modality S^M, where $[s]_i^M$ represents the score of a biometric in the set of all modalities M in the i^{th} position of the vector S^M. To identify such values and to construct the vector S^M in an oblivious fashion, it suffices to follow Protocol 2.

Protocol 2: Match Score Selection Protocol.

Input:
Output: Vector S^M

for $i \leftarrow 1$ **to** M **do**
  $[\delta] \leftarrow \tau$; **for** $j \leftarrow 1$ **to** $|H_i^M|$ **do**
    $[c] \leftarrow [\delta] \overset{?}{<} [h_{ij}^M]$;
    $[\delta] \leftarrow ([h_{ij}^M] - [\delta]) \cdot [c] + [\delta]$;
  $[s]_i^M = [\delta]$;

5. ***Fusion proportions:*** To perform fusion, a set of weights is provided to the mechanism by the MIP and applied to the normalized matching scores.

Normalization is not needed, given that the size and weights are in the public domain. In other words, normalization coefficients could be applied to them. In our setting, weights represent normalized performance rates for each user of the unimodal cloud-based schemes. To reduce the processing times, the proportions are presented in fractional form such that a weight w is represented by the tuple $\{n_w, d_w\}$, where n_w is its numerator and d_w is its denominator.

6. ***Fusion aggregation:*** Once the proportions are applied to the score vector S^M, they are aggregated. The result is also represented by a tuple $([n], [d])^{\mathtt{out}}$. Given that each normalized S^M score is represented by a similar fraction, in order to be able to aggregate them, it suffices to calculate the following equations:

$$[n^{\mathtt{out}}] \leftarrow [d]_{s_2^M} \cdot [d]_{s_3^M} \cdot [n]_{s_1^M} + [d]_{s_1^M} \cdot [d]_{s_3^M} \cdot [n]_{s_2^M} + [d]_{s_1^M} \cdot [d]_{s_2^M} \cdot [n]_{s_3^M} \tag{9}$$

$$[d^{\mathtt{out}}] \leftarrow [d]_{S_2^M} \cdot [d]_{S_3^M} \cdot [d]_{S_1^M} \tag{10}$$

7. ***Result delivery:*** The secret shares of the fusion result are transmitted by the UAs computational parties towards the MIP. The combination of the shares is performed by the MIP. This process is not computationally demanding, since additive secret sharing requires the addition of n field elements, where n in the number of parties (Lagrange polynomial interpolation). The MIP is the only one that accesses the final result. The MIP performs the fractional division to obtain a value $\in \{0, 1\}$.

8. ***Concealing fusion score:*** Note that the MIP is an honest-but-curious entity. For security purposes, if the application requires the score of fusion to be concealed; this can be achieved as follows: the MIP transmits, in shared form, the threshold of decision $[\tau]$ in fractional representation to the computational parties. The parties will be in charge of performing the comparison by cross-multiplying numerators, denominators and calling to the comparison functionality of our $\mathcal{F}_{ABB}$. The resulting shares are transmitted towards the system operator (through the MIP), for their interpolation, yielding only $\{0, 1\}$ values.

5 Security and Privacy Analysis

Our protocol offers perfect security against active adversaries under the information-theoretic model, including unbounded adversary and assuming secure channels and synchronous network. We proceed to show how our protocol provides the achievable security under MPC described in Section 3.2, *Definition* 1. The *matching and fusion* are designed in a data-oblivious fashion, from the perspective of the computational parties and dealers. In other words, there is no information leakage at any stage of the protocol. From an engineering perspective, the creation of a model than can be manipulated to decide how a system works in a real world application is considered necessary for testing whether a system meets the performance standards. During this procedure or *simulation* as referred by scientists who design complex systems, the model for a realistic scenario is developed and compared against an ideal functionality [78]. For our protocol, simulation provides conclusions and ideas on how to improve our design while executing the modules needed to make the model into a functioning design laboratory. In this way, if a UA cloud-based party would be corrupted, it would not receive the protocol output, nor the available intermediate values for any operation performed by our $\mathcal{F}_{ABB}$, making, in this case, the simulation trivial. This also holds for the case of a corrupted dealer. Given that our protocol can be assembled as a unitary arithmetic circuit, made of addition and multiplication gates, the simulation is achieved by invoking the simulation of the gates in the predefined order by the arithmetic circuit. During the execution of our protocol π, the view of an adversary (the information that the adversary has access to) does not compromise any private input from the honest parties, as long as the security properties of the underlying MPC primitives hold. Consequently, we can compose the properties of the combination of an ideal and real functionality (hybrid model) as described in [41]. Given that no other information is made available to any involved party, besides their corresponding private inputs and the binary output to the SP and the user, we fulfill *Definition* 1. Practically, the security depends exclusively on the MPC primitives that implement the $\mathcal{F}_{ABB}$ functionality. We mention the perfect security against passive and active adversaries of completeness theorems [17], adhering to the corresponding set of assumptions such as private channels. This is also true for our MPC protocol that is secure under composition.

6 Evaluation

6.1 Complexity

The complexity of MPC protocol is measured in communication rounds, that is defined as a message exchange step between the computational parties. A multiplication protocol can be implemented such that it requires one computational round [72]. The same holds for sharing or reconstructing a value. On the other hand, additions have no communication cost associated and in the context of this work can be executed for "free". Similar to the work of Catrina and de Hoogh [44], comparisons can be implemented in constant time. However, they are more expensive than multiplications since they need several multiplications that can be parallelized for each round but in absolute terms, they typically grow with the size of the input.

The *Feature collection* takes place during the first two stages, it requires a constant round complexity $\mathcal{O}(1)$. We do not consider the case in which a decryption of the ciphertexts takes place. If such an approach is implemented, the complexity of this step would vary depending on the distributed public key decryption mechanism used. The *Matching* uses Protocols 1 and 2; both present linear asymptotic complexities on the sides of their respective inputs: $\mathcal{O}(N^M)$ for the former, where N^M is the size of the template, and $\mathcal{O}(|H|^M)$, where $|H|^M$ is the size of the vector of Hamming Distance scores, for each modality M. In addition to that, the *Fusion* stages have constant time complexity $\mathcal{O}(1)$ because the number of biometric modalities is fixed. In our protocol, accompanying constants are in single digits and inequality tests are only used when it is strictly necessary; they can be executed in constant rounds, as described in [44], but they are more expensive in practice.

6.2 Computational Efficiency

The asymptotic complexity of our protocol is relatively low, as a result of the linear complexity in the templates' size. However, in realistic scenarios, factors such as the cryptographic primitives and the execution environment play an important role. As previously stated, a multiplication requires a communication round, whereas a comparison requires ~ 4 rounds, even when its computation is parallelized [44]. We have compatibilized the number of multiplications that are needed in total for a fixed standard template size. We measured the average execution time for the number of multiplications and the necessary comparisons. We use a custom implementation of the BGW protocol, taking into consideration the improvements on network flow problems presented in [12].

Environment Setting

We use a RAM memory $\approx$ 500 KB per instance, where each party instance takes two separate computational threads in order to manage communication and cryptographic tasks separately. On the cryptographic MPC background and adversarial model, we use the secret sharing model of Shamir [190], linear addition, and BGW for multiplication, [17, 72]. Comparisons were implemented according to the results introduced in [44]. We consider input sizes of 32 bits.

Execution environment: We have run our computational evaluations using a 64-bit server equipped with $2 \times 2 \times 10$ cores Intel Xeon E5-2687 at 3.1 GHz.

Parties: We assume the same scenario for the mechanism put forward by this paper, considering three computational parties, under the theoretic information model (private channels). All our tests were executed on the same server; hence network latency was not considered.

Templates' sizes: We used for our experiments: **i)** Face: 1024 bits, **ii)** Iris: 2048 bits and **iii)** Fingerprint: 4096 bits [122]. For our experimental analysis, we have indicatively chosen five templates per modality with a relatively high sizes to be able to easily adjust the protocol to realistic biometric deployments.

Computation Results

Following the results presented in Section 4.4, we accounted for the total number of operations that require communication rounds, specifically, multiplications and comparisons used by our protocol, (addition, is a linear operation and it is well established that the cost is negligible [12, 17, 29, 58]. Table 1 shows the number of operations per activity, where σ_{M} is equal to the templates' size in bits, and γ_{M} is the number of the available templates for the analysis.

Table 1: Total atomic operations

Stage	**Multiplications**	**Inequality Tests**
Feature Collection	$\sum_{i=1}^{M} \sigma_i \cdot \gamma_i = 35,840$	$\sigma \cdot \gamma = 15$
Fusion	1	0
Total:	35,841	15

Given that our protocol uses an arithmetic circuit approach, our tests had to account for the cost of each arithmetic gate. Table 2 shows the CPU times for the atomic MPC operations. The results reflect the average CPU time of $_{+}2 \times 10^7$ multiplications and 1.6×10^6 inequality tests. Given the limited number of equality tests, for instance 2, the impact of the difference in performance

between a comparison and an equality test is negligible. Table 3 presents the details of the amortized computational time for our circuit size. Table 4 shows the total communication cost per party in bits and in megabytes. A comparison actually accounts for 121 multiplication operations and each share is 63 bits.

Table 2: CPU time for atomic operations

Operation	**CPU Time in Secs**
Multiplications	2.08×10^{-5}
Inequality test	2.5×10^{-3}

Table 3: Overall CPU time

Operation	**CPU Time in Secs**
Multiplications	0.745
Inequality tests	0.038
Total:	0.8

Table 4: Total communication cost per party

Operation	**Bits Sent**	**MB**
Multiplications	$4,515,966$	0.538345098
Inequality tests	$228,690$	0.027261972
Total:	$4,744,656$	0.565607071

The overall execution time of the protocol for multimodal user authentication is less than a second. Note that the number and/or the size of the templates might differ depending on the application.

7 Discussion

The use of cloud technologies for providing biometric services requires biometric data outsourcing, which implies security and privacy risks for the users' information. However, due to the increased fraud occurrences and malicious attacks, BaaS has been a competitive arena for more advanced and complex cryptographic techniques to ensure security of the private data. Our multimodal AaaS architecture leverages the large-scale computing resources in the cloud while it offers flexibility, mobility, scalability, and cost reduction in terms of data storage and processing power to enhance the performance of user recognition. The system can securely share data with remote UAs with biometric DBs over

the network while MPC techniques make the stored templates, matching and fusion scores inaccessible to all parties. There is no biometric data disclosure towards the MIP and consequently the UAs that can only learn the fact that a query for a given user was made, and they do not gain access to the result of computation.

Furthermore, our approach implements multimodal biometrics providing better identification reliability, which is a common requirement for high security services [122]. Using the multimodal AaaS system, the SP acquires recognition capabilities without additional costs for the infrastructure to deal with the feature extraction, matching, fusion and decision modules. In that way, the SP confirms identities via a network connection to the cloud-based MIP and subsequently to the UAs while it avoids to handle time and cost consuming enrollment procedures, invest in necessary storage capacity and worry about the legal requirements regarding the security of sensitive information in a CBDB. This significantly reduces startup, running and policy costs for both the MIPs and SPs. As a result of being able to quickly search, compare and accurately fuse, the MIP can help the SP to combat fraud and to offer an improved user-service interface. Additionally, since IdMaaS enables the developers of authentication technology to set their statistical and mathematical methods to match biometrics in the cloud, the UAs can securely provision and release the shared resources with minimal MIP interaction and management effort. Finally, our approach guarantees to the users that the rendered services are only accessible to authorized parties. Thus, instead of being enrolled and presenting the same biometric traits across different remote providers, he can trust the storage and processing of his biometrics in an AaaS scheme that applies the necessary controls and is consistent with legal requirements for privacy and security by design. Hence, we assess that our proposed solution for identity management can offer a cost-effective, flexible business model for unimodal, bimodal or multimodal user authentication. It presents greater accountability with biometric logins because it connects an individual to a particular action and it is ready to deploy in realistic scenarios that fit to the government and financial sectors for access control applications where user higher authentication precision and security without compromising privacy are important [91, 183].

Although, the system has been designed for authentication purposes, it can also operate for identification with slight differences, without requesting and transmitting user credentials to the cloud. One foreseen application could be a lawful surveillance oriented scheme for government services, operating to automatically screen and match the crowd (facial and gait recognition) in order to identify missing persons. However, computation time would drastically increase for identification use cases. The size of the unimodal repositories has an impact on the overall procedure and our architecture may be proven an

unpractical approach for large-scale biometric DBs. Furthermore, regarding fusion, the final fused matching score is computed from stored unimodal templates originated from disparate sensors of the UAs. Thus, interoperability issues may reduce the multimodal authentication performance and consequently our system's accuracy and robustness. Finally, we assess that a clear limitation is the requirements and restrictions put in place by our research methodology. We selected three uncorrelated modalities to perform the matching procedure working with Hamming Distance algorithms and a user-specific weighted score level fusion with an applicable sum rule. Although the authentication protocol is flexible and can easily permit different unimodal biometrics, matching and fusion techniques, the use of more complex metrics and processes may affect the complexity and efficiency due to a higher cost for biometrics extraction and user multimodal recognition.

8 Conclusion and Future Work

Nowadays, the amount of biometric data for authentication purposes is increasing rapidly, while it requires large processing and storage capacity. Cloud computing is an innovative infrastructure allowing SPs to manage these challenges efficiently and offer improved AaaS technologies. In this work, we presented a distributed approach for secure and privacy-preserving multimodal AaaS in a domain with mutually distrustful parties. To avoid an auxiliary temporary or permanent CBDB, we exploited already stored unimodal templates held by distinct UAs, being used in AaaS designs based on single modalities. To obtain a multimodal fused result, we utilized Hamming Distance algorithms and a user-specific weighted score level fusion method. Finally, MPC techniques are used in order to build our protocol that obtains security and privacy in a decentralized manner without information disclosure in order to maintain the confidentiality and integrity of users' data. The stored biometric information, the data transmission, the authentication calculations and the final output are protected from the untrusted cloud parties. In this way, the proposed system leverages the advantages of multimodal biometrics and the efficiency of the underlying primitives with computation and communication overhead.

To the best of our knowledge, our work is the first one to propose a privacy-by-design approach for multimodal biometric authentication using cloud-based providers. Our system performs authentication including several biometric features (in our studied scenario have been selected three) while avoiding a new enrollment process for the users and without requesting any additional storage of private data. It offers a convenient solution for precision and reliability while restricting misuses of sensitive information, characterized by dynamic functionality and flexibility in terms of computation and communication

efficiency. Moreover, the protocol may be easily extended to update the parameters and adjust different biometrics, classifiers, matching methods and fusion rules. Through the prism of the new European GDPR [66] and the European Regulatory Technical Standards for Strong Customer Authentication RTS-SCA [183], biometric markets are forced to revise their infrastructure, taking into account the privacy rights of their users in order to be benefit from utility of the cloud. Thus, our architecture can serve as a framework for future applications, platforms and systems in which existing biometric datasets need to be leveraged.

We identified five directions for future work on multimodal authentication as BaaS using cloud-based IdMaaS and AaaS providers. First, the system's effectiveness depends on the weighted score level fusion model, where weights are products of the training procedures that are followed by the UAs subsystems. Although this is a time-consuming process and the available for research biometric data sources are limited, it should be explored how the combination of a variety of thresholds over the range of performance rates affects the overall accuracy and the usability of the user-specific fusion methods. Second, in the context of the MPC, to preserve confidentiality, unobservability and unlinkability, the query patterns can be statistically anonymized in order to hide the user's identity and real authentication queries count from the remote UAs. This would require protocol changes, where trade-offs between security and efficiency should be assessed. Third, the size of the templates' repositories of the UAs should be taken into account for any extension of the protocol to perform in identification mode, evaluating the practicality of the system in terms of computation and communication, complexity. Fourth, regarding the privacy and security frameworks, there are legal regulations that allow the migration of users' biometric data to a web interface. However, they prevent personal information transfers outside the organizations' national operating framework [183]. This fact may limit the flexibility of the UAs that may not comply with the same privacy regulations and constraints, and consequently the scalability of multimodal AaaS. Fifth and last, a critical aspect for AaaS is to integrate an anti-spoofing module, such as a challenge-response user interaction approach for liveness detection, to test stability and resistance against sophisticated fraud attacks.

Acknowledgements. This research was supported in part by the Research Council KU Leuven: C16/15/058. In addition, it was supported by imec through ICON BoSs, and by FWO through SBO SPITE S002417N. The work was also supported by the European Commission through H2020-DS-2014-653497 PANORAMIX.

Bibliography

[1] A. Abaza, A. Ross, C. Hebert, M. A. F. Harrison, and M. S. Nixon. A Survey on Ear Biometrics. *ACM Comput. Surv.*, 45(2):22:1–22:35, 2013.

[2] A. Abidin. On Privacy-Preserving Biometric Authentication. In *Information Security and Cryptology - 12th International Conference, Inscrypt 2016, Beijing, China, November 4-6, 2016, Revised Selected Papers*, pages 169–186, 2016.

[3] A. Abidin and A. Mitrokotsa. Security Aspects of Privacy-Preserving Biometric Authentication based on Ideal Lattices and Ring-LWE. In *2014 IEEE International Workshop on Information Forensics and Security, WIFS 2014, Atlanta, GA, USA, December 3-5, 2014*, pages 60–65, 2014.

[4] A. Aboshosha, K. A. E. Dahshan, E. A. Karam, and E. A. Ebeid. Score Level Fusion for Fingerprint, Iris and Face Biometrics. *International Journal of Computer Applications*, 111(4):47–55, February 2015.

[5] Acuity. Market Intelligence: An emerging technology strategy and research consultancy with a proven record of accurately anticipating biometric and electronic identity (eID) market trends., 2018. Accessed June 2018.

[6] S. Adamovic, M. M. Milosavljevic, M. D. Veinovic, M. Sarac, and A. Jevremovic. Fuzzy Commitment Scheme for Generation of Cryptographic Keys based on Iris Biometrics. *IET Biometrics*, 6(2):89–96, 2017.

[7] R. Ahdid, S. Safi, and B. Manaut. Euclidean and Geodesic Distance between a Facial Feature Points in Two-Dimensional Face Recognition System. *International Arab Conference on Information Technology (ACIT'2016)*, 14(4A):565–571, 2017.

[8] D. Akdogan, D. K. Altop, L. Eskandarian, and A. Levi. Secure Key Agreement Protocols: Pure Biometrics and Cancelable Biometrics. *Computer Networks*, 142:33–48, 2018.

[9] Z. Akhtar, B. Biggio, G. Fumera, and G. L. Marcialis. Robustness of Multi-Modal Biometric Systems under Realistic Spoof Attacks against All Traits. In *IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications, BIOMS 2011, Milan, Italy, September 28, 2011*, pages 1–6, 2011.

[10] Z. Akhtar, C. Micheloni, and G. L. Foresti. Biometric Liveness Detection: Challenges and Research Opportunities. *IEEE Security & Privacy*, 13(5):63–72, 2015.

[11] A. A. Albahdal and T. E. Boult. Problems and Promises of Using the Cloud and Biometrics. In *11th International Conference on Information Technology: New Generations, ITNG 2014, Las Vegas, NV, USA, April 7-9, 2014*, pages 293–300, 2014.

[12] A. Aly. *Network Flow Problems with Secure Multiparty Computation.* PhD thesis, Université Catholique de Louvain, IMMAQ, 2015.

[13] T. Araki, J. Furukawa, Y. Lindell, A. Nof, and K. Ohara. High-Throughput Semi-Honest Secure Three-Party Computation with an Honest Majority. In E. R. Weippl, S. Katzenbeisser, C. Kruegel, A. C. Myers, and S. Halevi, editors, *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 24-28, 2016*, pages 805–817. ACM, 2016.

[14] F. Armknecht, C. Boyd, C. Carr, K. Gjøsteen, A. Jäschke, C. A. Reuter, and M. Strand. A Guide to Fully Homomorphic Encryption. *IACR Cryptology ePrint Archive*, 2015, 2015.

[15] J. Ashbourn. *Biometrics in the New World - The Cloud, Mobile Technology and Pervasive Identity.* Springer, 2014.

[16] M. P. Beham and S. M. M. Roomi. Anti-Spoofing Enabled Face Recognition based on Aggregated Local Weighted Gradient Orientation. *Signal, Image and Video Processing*, 12(3):531–538, 2018.

[17] M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation (Extended Abstract). In J. Simon, editor, *Proceedings of the 20th Annual ACM Symposium on Theory of Computing, May 2-4, 1988, Chicago, Illinois, USA*, pages 1–10. ACM, 1988.

[18] R. Bendlin, I. Damgård, C. Orlandi, and S. Zakarias. Semi-Homomorphic Encryption and Multiparty Computation. In K. G. Paterson, editor, *Advances in Cryptology - EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques,*

Tallinn, Estonia, May 15-19, 2011. Proceedings, volume 6632 of *Lecture Notes in Computer Science*, pages 169–188. Springer, 2011.

[19] E. Bertino. Data Security and Privacy in the IoT. In *Proceedings of the 19th International Conference on Extending Database Technology, EDBT, Bordeaux, France, March, 2016, Bordeaux, France.*, pages 1–3, 2016.

[20] S. Bharadwaj, M. Vatsa, and R. Singh. Biometric Quality: A Review of Fingerprint, Iris, and Face. *EURASIP Journal on Image and Video Processing*, 2014:34, 2014.

[21] T. Bhattasali, K. Saeed, N. Chaki, and R. Chaki. A Survey of Security and Privacy Issues for Biometrics based Remote Authentication in Cloud. In *Computer Information Systems and Industrial Management - 13th IFIP TC8 International Conference, CISIM 2014, Ho Chi Minh City, Vietnam, November 5-7, 2014. Proceedings*, pages 112–121, 2014.

[22] B. Biggio, Z. Akhtar, G. Fumera, G. L. Marcialis, and F. Roli. Robustness of Multi-Modal Biometric Verification Systems under Realistic Spoofing Attacks. In *2011 IEEE International Joint Conference on Biometrics, IJCB 2011, Washington, DC, USA, October 11-13, 2011*, pages 1–6, 2011.

[23] D. Bissessar, C. Adams, and D. Liu. Using Biometric Key Commitments to Prevent Unauthorized Lending of Cryptographic Credentials. In *2014 Twelfth Annual International Conference on Privacy, Security and Trust, Toronto, ON, Canada, July 23-24, 2014*, pages 75–83, 2014.

[24] BIT. Biometrics Ideal Test, (BIT) : Website for biometric database sharing and algorithms evaluation, 2018. Accessed April 2018.

[25] M. Blanton and M. Aliasgari. Secure Outsourced Computation of Iris Matching. *Journal of Computer Security*, 20(2-3):259–305, 2012.

[26] M. Blanton and S. Saraph. Oblivious Maximum Bipartite Matching Size Algorithm with Applications to Secure Fingerprint Identification. In G. Pernul, P. Y. A. Ryan, and E. R. Weippl, editors, *Computer Security - ESORICS 2015 - 20th European Symposium on Research in Computer Security, Vienna, Austria, September 21-25, 2015, Proceedings, Part I*, volume 9326 of *Lecture Notes in Computer Science*, pages 384–406. Springer, 2015.

[27] Bloomberg. Delivering business and financial information, and connecting decision makers around the world to a dynamic network of news and ideas, featuring stories from Businessweek and Bloomberg News: In Europe They are Giving Users Control of Their Online Data, 2018. Accessed May 2018.

[28] D. Bogdanov, S. Laur, and J. Willemson. Sharemind: A Framework for Fast Privacy-Preserving Computations. In S. Jajodia and J. López, editors, *Computer Security - ESORICS 2008, 13th European Symposium on Research in Computer Security, Málaga, Spain, October 6-8, 2008. Proceedings*, volume 5283 of *Lecture Notes in Computer Science*, pages 192–206. Springer, 2008.

[29] P. Bogetoft, D. L. Christensen, I. Damgård, M. Geisler, T. P. Jakobsen, M. Krøigaard, J. D. Nielsen, J. B. Nielsen, K. Nielsen, J. Pagter, M. I. Schwartzbach, and T. Toft. Secure Multiparty Computation Goes Live. In R. Dingledine and P. Golle, editors, *Financial Cryptography and Data Security, 13th International Conference, FC 2009, Accra Beach, Barbados, February 23-26, 2009. Revised Selected Papers*, volume 5628 of *Lecture Notes in Computer Science*, pages 325–343. Springer, 2009.

[30] R. M. Bolle, S. S. Chikkerur, J. H. Connell, and N. K. Ratha. Methods and Apparatus for Generation of Cancelable Fingerprint Template, 2013. US Patent 8,538,096.

[31] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano. Passwords and the Evolution of Imperfect Authentication. *Commun. ACM*, 58(7):78–87, June 2015.

[32] J. Breebaart, I. Buhan, K. de Groot, and E. Kelkboom. Evaluation of a Template Protection Approach to Integrate Fingerprint Biometrics in a PIN-based Payment Infrastructure. *Electronic Commerce Research and Applications*, 10(6):605–614, 2011.

[33] J. Breebaart, C. Busch, J. Grave, and E. Kindt. A Reference Architecture for Biometric Template Protection based on Pseudo-Identities. In *BIOSIG 2008 - Proceedings of the Special Interest Group on Biometrics and Electronic Signatures, 11.-12. September 2008 in Darmstadt, Germany*, pages 25–38, 2008.

[34] J. Breebaart, B. Yang, I. Buhan-Dulman, and C. Busch. Biometric Template Protection - The Need for Open Standards. *Datenschutz und Datensicherheit*, 33(5):299–304, 2009.

[35] J. Bringer, H. Chabanne, and B. Kindarji. Identification with Encrypted Biometric Data. *Security and Communication Networks*, 4(5):548–562, 2011.

[36] J. Bringer, H. Chabanne, and A. Patey. Privacy-Preserving Biometric Identification Using Secure Multiparty Computation: An Overview and Recent Trends. *IEEE Signal Process. Mag.*, 30(2):42–52, 2013.

[37] M. J. Burge and K. W. Bowyer, editors. *Handbook of Iris Recognition.* Advances in Computer Vision and Pattern Recognition. Springer, 2013.

[38] M. Butt, O. Henniger, A. Nouak, and A. Kuijper. Privacy Protection of Biometric Templates. In *HCI International 2014 - Posters' Extended Abstracts - International Conference, HCI International 2014, Heraklion, Crete, Greece, June 22-27, 2014. Proceedings, Part I*, pages 153–158, 2014.

[39] P. Campisi, editor. *Security and Privacy in Biometrics.* Springer, 2013.

[40] P. Campisi, E. Maiorana, and A. Neri. Privacy Enhancing Technologies in Biometrics. In *Handbook of Research on Computational Forensics, Digital Crime, and Investigation: Methods and Solutions*, pages 1–22. IGI Global, 2010.

[41] R. Canetti. Security and Composition of Multiparty Cryptographic Protocols. *Journal of Cryptology*, 13(1):143–202, 2000.

[42] R. Canetti. Universally Composable Security: A New Paradigm for Cryptographic Protocols. In *42nd Annual Symposium on Foundations of Computer Science, FOCS 2001, 14-17 October 2001, Las Vegas, Nevada, USA*, pages 136–145. IEEE Computer Society, 2001.

[43] CASIA. Casia Iris Image Database (CASIA-IRIS) Version 4.0 and CASIA Palmprint Image Database (CASIA-Palmprint), 2010. Accessed April 2018.

[44] O. Catrina and S. de Hoogh. Improved Primitives for Secure Multiparty Integer Computation. In J. A. Garay and R. D. Prisco, editors, *Security and Cryptography for Networks, 7th International Conference, SCN 2010, Amalfi, Italy, September 13-15, 2010. Proceedings*, volume 6280 of *Lecture Notes in Computer Science*, pages 182–199. Springer, 2010.

[45] A. Cavoukian. Privacy-by-Design: Leadership, Methods and Results. In *European Data Protection: Coming of Age*, pages 175–202. Springer, 2013.

[46] A. Cavoukian, M. Snijder, A. Stoianov, and M. Chibba. Privacy and Biometrics for Authentication Purposes: A Discussion of Untraceable Biometrics and Biometric Encryption. In *Ethics and Policy of Biometrics - Third International Conference on Ethics and Policy of Biometrics and International Data Sharing, ICEB 2010, Hong Kong, January 4-5, 2010. Revised Papers*, pages 14–22, 2010.

[47] A. Cavoukian and A. Stoianov. Biometric Encryption. In *Encyclopedia of Cryptography and Security, 2nd Ed.*, pages 90–98. Springer, 2011.

[48] A. Cavoukian and A. Stoianov. Privacy-by-Design Solutions for Biometric One-to-Many Identification Systems. *IPC Technical Report*, pages 1–37, 2014.

[49] D. Chaum, C. Crépeau, and I. Damgård. Multiparty Unconditionally Secure Protocols (Extended Abstract). In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing, May 2-4, 1988, Chicago, Illinois, USA*, pages 11–19, 1988.

[50] C. Chen, A. Dantcheva, T. Swearingen, and A. Ross. Spoofing Faces using Makeup: An Investigative Study. In *IEEE International Conference on Identity, Security and Behavior Analysis, ISBA 2017, New Delhi, India, February 22-24, 2017*, pages 1–8, 2017.

[51] I. Chingovska, A. R. dos Anjos, and S. Marcel. Biometrics Evaluation Under Spoofing Attacks. *IEEE Trans. Information Forensics and Security*, 9(12):2264–2276, 2014.

[52] B. Choudhury, P. T. Greene, B. Issac, V. Raman, and M. K. Haldar. A Survey on Biometrics and Cancelable Biometrics Systems. *Int. J. Image Graphics*, 18(1):1–39, 2018.

[53] T. Chugh, K. Cao, and A. K. Jain. Fingerprint Spoof Buster: Use of Minutiae-Centered Patches. *IEEE Trans. Information Forensics and Security*, 13(9):2190–2202, 2018.

[54] P. Connor and A. Ross. Biometric Recognition by Gait: A Survey of Modalities and Features. *Computer Vision and Image Understanding*, 167:1–27, 2018.

[55] I. Damgård, M. Fitzi, E. Kiltz, J. B. Nielsen, and T. Toft. Unconditionally Secure Constant-Rounds Multiparty Computation for Equality, Comparison, Bits and Exponentiation. In S. Halevi and T. Rabin, editors, *Theory of Cryptography, Third Theory of Cryptography Conference, TCC 2006, New York, NY, USA, March 4-7, 2006, Proceedings*, volume 3876 of *Lecture Notes in Computer Science*, pages 285–304. Springer, 2006.

[56] I. Damgård, M. Keller, E. Larraia, V. Pastro, P. Scholl, and N. P. Smart. Practical Covertly Secure MPC for Dishonest Majority - Or: Breaking the SPDZ Limits. In *Computer Security - ESORICS 2013 - 18th European Symposium on Research in Computer Security, Egham, UK, September 9-13, 2013. Proceedings*, pages 1–18, 2013.

[57] I. Damgård and J. B. Nielsen. Universally Composable Efficient Multiparty Computation from Threshold Homomorphic Encryption.

In D. Boneh, editor, *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings*, volume 2729 of *Lecture Notes in Computer Science*, pages 247–264. Springer, 2003.

[58] I. Damgård, V. Pastro, N. P. Smart, and S. Zakarias. Multiparty Computation from Somewhat Homomorphic Encryption. In R. Safavi-Naini and R. Canetti, editors, *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*, volume 7417 of *Lecture Notes in Computer Science*, pages 643–662. Springer, 2012.

[59] G. I. Davida, Y. Frankel, B. J. Matt, and R. Peralta. On the Relation of Error-Correction and Cryptography to an Off-Line Biometric based Identification Scheme. In *Workshop on Coding and Cryptography*, pages 129–138, 1999.

[60] T. de Freitas Pereira, A. Anjos, J. M. D. Martino, and S. Marcel. Can Face Anti-Spoofing Countermeasures Work in a Real World Scenario? In *International Conference on Biometrics, ICB 2013, 4-7 June, 2013, Madrid, Spain*, pages 1–8, 2013.

[61] A. B. Dehkordi and S. A. R. Abu-Bakar. Iris Code Matching using Adaptive Hamming Distance. In *2015 IEEE International Conference on Signal and Image Processing Applications, ICSIPA 2015, Kuala Lumpur, Malaysia, October 19-21, 2015*, pages 404–408, 2015.

[62] N. Delvaux, H. Chabanne, J. Bringer, B. Kindarji, P. Lindeberg, J. Midgren, J. Breebaart, T. H. Akkermans, M. van der Veen, R. N. J. Veldhuis, E. Kindt, K. Simoens, C. Busch, P. Bours, D. Gafurov, B. Yang, J. Stern, C. Rust, B. Cucinelli, and D. Skepastianos. Pseudo-Identities Based on Fingerprint Characteristics. In *4th International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2008), Harbin, China, August 2008, Proceedings*, pages 1063–1068, 2008.

[63] S. D. C. di Vimercati, S. Foresti, G. Livraga, S. Paraboschi, and P. Samarati. Privacy in Pervasive Systems: Social and Legal Aspects and Technical Solutions. In *Data Management in Pervasive Systems*, pages 43–65. Springer, 2015.

[64] S. D. C. di Vimercati, S. Foresti, and P. Samarati. Data Security Issues in Cloud Scenarios. In *Information Systems Security - 11th International Conference, ICISS 2015, Kolkata, India, December 16-20, 2015, Proceedings*, pages 3–10, 2015.

[65] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. D. Smith. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. *SIAM J. Comput.*, 38(1):97–139, 2008.

[66] EU. European General Data Protection Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. *Official Journal of the European Union*, 2016. Accessed November 2017.

[67] Fidelity. European Project Fidelity: Fast and trustworthy Identity Delivery and Check with ePassports leveraging Traveler privacy, http://fidelity-project.eu/, 2015.

[68] S. Furnell. From Passwords to Biometrics - In Pursuit of a Panacea. In O. Camp, E. Weippl, C. Bidan, and E. Aïmeur, editors, *Information Systems Security and Privacy*, pages 3–15. Springer International Publishing, 2015.

[69] D. Gafurov, P. Bours, B. Yang, and C. Busch. Independent Performance Evaluation of Pseudonymous Identifier Fingerprint Verification Algorithms. In *Image Analysis and Recognition - 10th International Conference, ICIAR 2013, Póvoa do Varzim, Portugal, June, 2013. Proceedings*, pages 63–71, 2013.

[70] Q. Gao, F. Gao, H. Zhang, X. Hao, and X. Wang. Two-Dimensional Maximum Local Variation based on Image Euclidean Distance for Face Recognition. *IEEE Trans. Image Processing*, 22(10):3807–3817, 2013.

[71] M. Geisler. *Cryptographic Protocols: Theory and Implementation.* PhD thesis, Aarhus University Denmark, Department of Computer Science, 2010.

[72] R. Gennaro, M. O. Rabin, and T. Rabin. Simplified VSS and Fast-track Multiparty Computations with Applications to Threshold Cryptography. In *Proceedings of the Seventeenth Annual ACM Symposium on Principles of Distributed Computing*, PODC '98, pages 101–111, New York, NY, USA, 1998. ACM.

[73] C. Gentry. *A Fully Homomorphic Encryption Scheme.* PhD thesis, Stanford University, 2009. https://crypto.stanford.edu/craig/craig-thesis.pdf.

[74] N. Gerber and V. Zimmermann. Security vs. Privacy? User Preferences Regarding Text Passwords and Biometric Authentication. In *Mensch und Computer 2017 - Workshopband, Regensburg, Germany, September 10-13, 2017.*, 2017.

[75] M. Golfarelli, D. Maio, and D. Maltoni. On the Error-Reject Trade-Off in Biometric Verification Systems. *IEEE Trans. Pattern Anal. Mach. Intell.*, 19(7):786–796, 1997.

[76] M. Gomez-Barrero, J. Galbally, and J. Fiérrez. Efficient Software Attack to Multimodal Biometric Systems and its Application to Face and Iris Fusion. *Pattern Recognition Letters*, 36:243 – 253, 2014.

[77] M. Gomez-Barrero, E. Maiorana, J. Galbally, P. Campisi, and J. Fiérrez. Multi-Biometric Template Protection based on Homomorphic Encryption. *Pattern Recognition*, 67:149–163, 2017.

[78] R. J. Gran. *Creating Simulations. Numerical Computing with Simulink, vol. 1.* Society of Industrial and Applied Mathematics (SIAM), 2007.

[79] S. Gray. Future of Privacy Forum: A Discussion Document in Privacy Principles for Facial Recognition Technology, 2015. Accessed July 2018.

[80] B. H. Guo, M. S. Nixon, and J. N. Carter. Fusion Analysis of Soft Biometrics for Recognition at a Distance. In *IEEE 4th International Conference on Identity, Security, and Behavior Analysis, ISBA 2018, Singapore, January 11-12, 2018*, pages 1–8, 2018.

[81] A. Hadid. Face Biometrics Under Spoofing Attacks: Vulnerabilities, Countermeasures, Open Issues, and Research Directions. In *IEEE Conference on Computer Vision and Pattern Recognition, CVPR Workshops 2014, Columbus, OH, USA, June 23-28, 2014*, pages 113–118, 2014.

[82] A. Hadid, N. W. D. Evans, S. Marcel, and J. Fiérrez. Biometrics Systems Under Spoofing Attack: An Evaluation Methodology and Lessons Learned. *IEEE Signal Process. Mag.*, 32(5):20–30, 2015.

[83] A. Hadid, M. Ghahramani, V. Kellokumpu, X. Feng, J. D. Bustard, and M. S. Nixon. Gait Biometrics under Spoofing Attacks: An Experimental Investigation. *J. Electronic Imaging*, 24(6):063022, 2015.

[84] C. Hahn, H. Shin, and J. Hur. Cloud-based Biometrics Processing for Privacy-Preserving Identification. In *Ninth International Conference on Ubiquitous and Future Networks, ICUFN 2017, Milan, Italy, July 4-7, 2017*, pages 595–600, 2017.

[85] A. M. Hamad, R. S. Elhadary, and A. O. Elkhateeb. Multimodal Biometric Identification Using Fingerprint, Face and Iris Recognition. *International Journal of Information Science and Intelligent System*, 3(4):53–60, 2014.

[86] F. Hao, R. J. Anderson, and J. Daugman. Combining Crypto with Biometrics Effectively. *IEEE Trans. Computers*, 55(9):1081–1088, 2006.

[87] H. Higo, T. Isshiki, K. Mori, and S. Obana. Privacy-Preserving Fingerprint Authentication Resistant to Hill-Climbing Attacks. *IEICE Transactions*, 101-A(1):138–148, 2018.

[88] Y. Huang, L. Malka, D. Evans, and J. Katz. Efficient Privacy-Preserving Biometric Identification. In *Proceedings of the Network and Distributed System Security Symposium, NDSS 2011, San Diego, California, USA, 6th February - 9th February 2011*. The Internet Society, 2011.

[89] T. Ignatenko and F. M. J. Willems. Information Leakage in Fuzzy Commitment Schemes. *IEEE Trans. Information Forensics and Security*, 5(2):337–348, 2010.

[90] S. R. Inamdar and Y. H. Dandawate. Multimodal Biometric Cryptosystem based on Fusion of Wavelet and Curvelet Features in Robust Security Application. *IJBM*, 8(1):33–51, 2016.

[91] IndustryARC. Report for the Next Generation Biometrics Market: By Type of Authentication (Single Factor, Multi-Factor, Others); By End User (Banking, Government, Consumer Electronics, Others); By Geography - Forecast (2018-2023), 2018. Accessed July 2018.

[92] ISO/IEC 24745:2011, Information Technology - Security Techniques - Biometric Information Protection, 2011.

[93] ISO/IEC 19795-1:2006, Information Ttechnology - Biometric Performance Testing and Reporting - Part 1: Principles and Framework, 2006.

[94] ISO/IEC 19092:2008, Financial Services - Biometrics - Security Framework, 2008.

[95] ISO 13491-1:2016, Financial Services - Secure Cryptographic Devices - Part 1: Concepts, Requirements and Evaluation Methods, 2016.

[96] ISO2017. ISO/IEC 2382-37/2017, Information Technology - Vocabulary - Part 37: Biometrics, 2017.

[97] A. Jagadeesan and K. Duraiswamy. Secured Cryptographic Key Generation From Multimodal Biometrics Feature Level Fusion Of Fingerprint And Iris. *CoRR*, abs/1002.2527, 2010.

[98] A. K. Jain, P. Flynn, and A. A. Ross. *Handbook of Biometrics*. Springer Publishing Company, Incorporated, 1st edition, 2010.

[99] A. K. Jain and A. Kumar. Biometric Recognition: An Overview. In E. Mordini and D. Tzovaras, editors, *Second Generation Biometrics: The Ethical, Legal and Social Context*, pages 49–79. Springer, 2012.

[100] A. K. Jain, K. Nandakumar, and A. Nagar. Biometric Template Security. *EURASIP Journal on Advances in Signal Processing*, 2008, 2008.

[101] A. K. Jain, K. Nandakumar, and A. Ross. Score Normalization in Multimodal Biometric Systems. *Pattern Recognition*, 38(12):2270–2285, 2005.

[102] A. K. Jain, K. Nandakumar, and A. Ross. 50 years of Biometric Research: Accomplishments, Challenges, and Opportunities. *Pattern Recognition Letters*, 79:80–105, 2016.

[103] Z. Jin, A. B. J. Teoh, B. Goi, and Y. H. Tay. Biometric Cryptosystems: A New Biometric Key Binding and its Implementation for Fingerprint Minutiae-based Representation. *Pattern Recognition*, 56:50–62, 2016.

[104] B.-Z. Jing, P. P. K. Chan, W. W. Y. Ng, and D. S. Yeung. Anti-Spoofing System for RFID Access Control Combining with Face Recogntion. In *International Conference on Machine Learning and Cybernetics*, volume 2, pages 698–703, 2010.

[105] R. M. Jomaa, M. S. Islam, and H. Mathkour. Improved Sequential Fusion of Heart-Signal and Fingerprint for Anti-Spoofing. In *IEEE 4th International Conference on Identity, Security, and Behavior Analysis, ISBA 2018, Singapore, January 11-12, 2018*, pages 1–7, 2018.

[106] A. Juels, D. Molnar, and D. A. Wagner. Security and Privacy Issues in ePassports. In *First International Conference on Security and Privacy for Emerging Areas in Communications Networks, SecureComm 2005, Athens, Greece, 5-9 September, 2005*, pages 74–88, 2005.

[107] A. Juels and M. Sudan. A Fuzzy Vault Scheme. *Des. Codes Cryptography*, 38(2):237–257, 2006.

[108] S. G. Kanade, D. Petrovska-Delacrétaz, and B. Dorizzi. Cancelable Biometrics for Better Security and Privacy in Biometric Systems. In *Advances in Computing and Communications - First International Conference, ACC 2011, Kochi, India, July 22-24, 2011, Proceedings, Part III*, pages 20–34, 2011.

[109] S. G. Kanade, D. Petrovska-Delacrétaz, and B. Dorizzi. *Enhancing Information Security and Privacy by Combining Biometrics with Cryptography*. Synthesis Lectures on Information Security, Privacy, and Trust. Morgan & Claypool Publishers, 2012.

[110] C. Karabat and B. Topcu. How to Assess Privacy Preservation Capability of Biohashing Methods?: Privacy Metrics. In *2014 22nd Signal Processing and Communications Applications Conference (SIU), Trabzon, Turkey, April 23-25, 2014*, pages 2217–2220, 2014.

[111] H. Kaur and P. Khanna. Biometric Template Protection using Cancelable Biometrics and Visual Cryptography Techniques. *Multimedia Tools Appl.*, 75(23):16333–16361, 2016.

[112] E. J. C. Kelkboom, X. Zhou, J. Breebaart, R. N. J. Veldhuis, and C. Busch. Multi-Algorithm Fusion with Template Protection. In *IEEE 3rd International Conference on Biometrics: Theory, Applications, and Systems*, pages 1–8, 2009.

[113] M. Keller, E. Orsini, and P. Scholl. MASCOT: Faster Malicious Arithmetic Secure Computation with Oblivious Transfer. In E. R. Weippl, S. Katzenbeisser, C. Kruegel, A. C. Myers, and S. Halevi, editors, *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 24-28, 2016*, pages 830–842. ACM, 2016.

[114] H. Khan, U. Hengartner, and D. Vogel. Usability and Security Perceptions of Implicit Authentication: Convenient, Secure, Sometimes Annoying. In *Eleventh Symposium On Usable Privacy and Security, SOUPS 2015, Ottawa, Canada, July 22-24, 2015.*, pages 225–239, 2015.

[115] E. Kindt. The Use of Privacy Enhancing Technologies for Biometric Systems Analysed from a Legal Perspective. In *Privacy and Identity Management for Life - 5th IFIP WG 9.2, 9.6/11.4, 11.6, 11.7/PrimeLife International Summer School, Nice, France, September 7-11, 2009, Revised Selected Papers*, pages 134–145, 2009.

[116] E. J. Kindt. *Privacy and Data Protection Issues of Biometric Applications-A Comparative Legal Analysis*. Springer Netherlands, 2013.

[117] M. Lafkih, M. Mikram, S. Ghouzali, M. E. Haziti, and D. Aboutajdine. Biometric Cryptosystems based Fuzzy Commitment Scheme: A Security Evaluation. *Int. Arab J. Inf. Technol.*, 13(4):443–449, 2016.

[118] D. Lee, S. Hussain, G. Roussos, and Y. Zhang. Editorial: Special Issue on Security and Multimodality in Pervasive Environments. *Wireless Personal Communications*, 55(1):1–4, 2010.

[119] A. R. Lejbølle, K. Nasrollahi, and T. B. Moeslund. Enhancing Person Re-Identification by Late Fusion of Low-, Mid- and High-Level Features. *IET Biometrics*, 7(2):125–135, 2018.

[120] C. Li and J. Hu. Attacks via Record Multiplicity on Cancelable Biometrics Templates. *Concurrency and Computation: Practice and Experience*, 26(8):1593–1605, 2014.

[121] P. Li, X. Yang, H. Qiao, K. Cao, E. Liu, and J. Tian. An Effective Biometric Cryptosystem Combining Fingerprints with Error Correction Codes. *Expert Syst. Appl.*, 39(7):6562–6574, 2012.

[122] S. Z. Li and A. K. Jain, editors. *Encyclopedia of Biometrics, Second Edition*. Springer US, 2015.

[123] X. Li, Y. Yin, Y. Ning, G. Yang, and L. Pan. A Hybrid Biometric Identification Framework for High Security Applications. *Frontiers Comput. Sci.*, 9(3):392–401, 2015.

[124] M. Lim, A. B. J. Teoh, and J. Kim. Biometric Feature-Type Transformation: Making Templates Compatible for Secret Protection. *IEEE Signal Process. Mag.*, 32(5):77–87, 2015.

[125] J. M. G. Linnartz and P. Tuyls. New Shielding Functions to Enhance Privacy and Prevent Misuse of Biometric Templates. In *Audio-and Video-based Biometrie Person Authentication, 4th International Conference, AVBPA 2003, Guildford, UK, June 9-11, 2003 Proceedings*, pages 393–402, 2003.

[126] H. Lipmaa and T. Toft. Secure Equality and Greater-Than Tests with Sublinear Online Complexity. In F. V. Fomin, R. Freivalds, M. Z. Kwiatkowska, and D. Peleg, editors, *Automata, Languages, and Programming - 40th International Colloquium, ICALP 2013, Riga, Latvia, July 8-12, 2013, Proceedings, Part II*, volume 7966 of *Lecture Notes in Computer Science*, pages 645–656. Springer, 2013.

[127] E. Luckyanets, A. Melnikov, O. Kudashev, S. Novoselov, and G. Lavrentyeva. Bimodal Anti-Spoofing System for Mobile Security. In *Speech and Computer - 19th International Conference, SPECOM 2017, Hatfield, UK, September 12-16, 2017, Proceedings*, pages 211–220, 2017.

[128] G. Mai, M. Lim, and P. C. Yuen. Fusing Binary Templates for Multi-Biometric Cryptosystems. In *IEEE 7th International Conference on Biometrics Theory, Applications and Systems, BTAS 2015, Arlington, VA, USA, September 8-11, 2015*, pages 1–8, 2015.

[129] E. Maiorana, G. E. Hine, and P. Campisi. Hill-Climbing Attacks on Multibiometrics Recognition Systems. *IEEE Trans. Information Forensics and Security*, 10(5):900–915, 2015.

[130] J. Malik, D. Girdhar, R. Dahiya, and G. Sainarayanan. Reference Threshold Calculation for Biometric Authentication. *International Journal of Image, Graphics and Signal Processing*, 2:46–53, 2014.

[131] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar. *Handbook of Fingerprint Recognition*. Springer Publishing Company, Incorporated, 2nd edition, 2009.

[132] N. L. Manasa, A. Govardhan, and C. Satyanarayana. Fusion of Multiple Biometric Traits: Fingerprint, Palmprint and Iris. In *Bio-inspiring Cyber Security and Cloud Services: Trends and Innovations*, pages 287–320. Springer, 2014.

[133] A. Mandal, A. Roy, and M. Yasuda. Comprehensive and Improved Secure Biometric System Using Homomorphic Encryption. In *Data Privacy Management, and Security Assurance - 10th International Workshop, DPM 2015, and 4th International Workshop, QASA 2015, Vienna, Austria, September 21-22, 2015. Revised Selected Papers*, pages 183–198, 2015.

[134] S. Mangla and N. S. Raghava. Iris Recognition on Hadoop: A Biometrics System Implementation on Cloud Computing. In *2011 IEEE International Conference on Cloud Computing and Intelligence Systems, CCIS 2011, Beijing, China, September 15-17, 2011*, pages 482–485, 2011.

[135] E. Marasco and A. Ross. A Survey on Anti-spoofing Schemes for Fingerprint Recognition Systems. *ACM Comput. Surv.*, 47(2):28:1–28:36, 2014.

[136] S. Marcel, M. S. Nixon, and S. Z. Li, editors. *Handbook of Biometric Anti-Spoofing - Trusted Biometrics under Spoofing Attacks*. Advances in Computer Vision and Pattern Recognition. Springer, 2014.

[137] G. L. Marcialis, P. Coli, and F. Roli. Fingerprint Liveness Detection based on Fake Finger Characteristics. *IJDCF*, 4(3):1–19, 2012.

[138] E. Martin and E. Cao. Euclidean Chemical Spaces from Molecular Fingerprints: Hamming Distance and Hempel's Ravens. *Journal of Computer-Aided Molecular Design*, 29(5):387–395, 2015.

[139] M. Martinez-Diaz, J. Fiérrez, J. Galbally, and J. Ortega-Garcia. An Evaluation of Indirect Attacks and Countermeasures in Fingerprint Verification Systems. *Pattern Recognition Letters*, 32(12):1643–1651, 2011.

[140] T. Matsumoto. Gummy and Conductive Silicone Rubber Fingers. In *Advances in Cryptology - ASIACRYPT 2002, 8th International Conference*

on the Theory and Application of Cryptology and Information Security, Queenstown, New Zealand, December 1-5, 2002, Proceedings, pages 574–576, 2002.

[141] U. M. Maurer. Secure Multi-Party Computation Made Simple. *Discrete Applied Mathematics*, 154(2):370–381, 2006.

[142] A. Menezes, P. C. van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.

[143] D. T. Meva and C. K. Kumbharana. Comparative Study of Different Fusion Techniques in Multimodal Biometric Authentication. *International Journal of Computer Applications*, 66(19):16–19, 2013.

[144] C. L. Miltgen, A. Popovic, and T. Oliveira. Determinants of End-User Acceptance of Biometrics: Integrating the "Big 3" of Technology Acceptance with Privacy Context. *Decision Support Systems*, 56:103–114, 2013.

[145] M. Mrdaković and S. Adamović. Privacy Friendly Biometrics. *Synthesis 2015 - International Scientific Conference of IT and Business-Related Research, Singidunum University, Belgrade, Serbia*, 2015.

[146] M. G. Msgna, H. Ferradi, R. N. Akram, and K. Markantonakis. Secure Application Execution in Mobile Devices. In *The New Codebreakers - Essays Dedicated to David Kahn on the Occasion of His 85th Birthday*, pages 417–438, 2016.

[147] S. K. R. Nair, B. Bhanu, S. Ghosh, and N. S. Thakoor. Predictive Models for Multibiometric Systems. *Pattern Recognition*, 47(12):3779–3792, 2014.

[148] K. Nandakumar and A. K. Jain. Multibiometric Template Security using Fuzzy Vault. In *Biometrics: Theory, Applications and Systems, 2008. BTAS 2008. 2nd IEEE International Conference on*, pages 1–6. IEEE, 2008.

[149] K. Nandakumar and A. K. Jain. Biometric Template Protection: Bridging the Performance Gap between Theory and Practice. *IEEE Signal Process. Mag.*, 32(5):88–100, 2015.

[150] I. Natgunanathan, A. Mehmood, Y. Xiang, G. Hua, G. Li, and S. Bangay. An Overview of Protection of Privacy in Multibiometrics. *Multimedia Tools Appl.*, 77(6):6753–6773, 2018.

[151] D. C. L. Ngo, A. B. J. Teoh, and J. Hu. *Biometric Security*. Cambridge Scholars Publisher, 2015.

[152] NIST. National Instiute of Standards and Technology (NIST) NBIS Fingerprint and Facial Biometric Special Research Databases, 2012. Accessed April 2018.

[153] K. Okereafor, C. Onime, and O. Osuagwu. Enhancing Biometric Liveness Detection Using Trait Randomization Technique. In *UKSim-AMSS 19th International Conference on Computer Modelling & Simulation, UKSim 2017, Cambridge, UK, April 5-7, 2017*, pages 28–33, 2017.

[154] A. Omotosho, O. Adegbola, B. Adelakin, A. Adelakun, and J. Emuoyibofarhe. Exploiting Multimodal Biometrics in ePrivacy Scheme for Electronic Health Records. *CoRR*, abs/1502.01233, 2015.

[155] F. Omri, S. Foufou, R. Hamila, and M. Jarraya. Cloud-based Mobile System for Biometrics Authentication. In *13th International Conference on ITS Telecommunications, ITST 2013, Tampere, Finland, November 5-7, 2013*, pages 325–330, 2013.

[156] A. A. Othman and A. Ross. Privacy of Facial Soft Biometrics: Suppressing Gender but Retaining Identity. In *Computer Vision - ECCV 2014 Workshops - Zurich, Switzerland, September 6-7 and 12, 2014, Proceedings, Part II*, pages 682–696, 2014.

[157] E. Pagnin, C. Dimitrakakis, A. Abidin, and A. Mitrokotsa. On the Leakage of Information in Biometric Authentication. In *Progress in Cryptology - INDOCRYPT 2014 - 15th International Conference on Cryptology in India, New Delhi, India, December 14-17, 2014, Proceedings*, pages 265–280, 2014.

[158] E. Pagnin and A. Mitrokotsa. Privacy-Preserving Biometric Authentication: Challenges and Directions. *Security and Communication Networks*, 2017:7129505:1–7129505:9, 2017.

[159] P. Paillier. Public-Key Cryptosystems based on Composite Degree Residuosity Classes. In J. Stern, editor, *Advances in Cryptology - EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May 2-6, 1999, Proceeding*, volume 1592 of *Lecture Notes in Computer Science*, pages 223–238. Springer, 1999.

[160] D. Pal, P. Khethavath, T. Chen, and Y. Zhang. Mobile Payments in Global Markets using Biometrics and Cloud. *Int. J. Communication Systems*, 30(14), 2017.

[161] J. Palanichamy and R. Marimuthu. A Novel Image Alignment and a Fast Efficient Localized Euclidean Distance Minutia Matching Algorithm

for Fingerprint Recognition System. *International Arab Journal of Information Technology*, 13(3):313–319, 2016.

[162] S. Pan, S. Yan, and W. T. Zhu. Security Analysis on Privacy-Preserving Cloud Aided Biometric Identification Schemes. In J. K. Liu and R. Steinfeld, editors, *Information Security and Privacy - 21st Australasian Conference, ACISP 2016, Melbourne, VIC, Australia, July 4-6, 2016, Proceedings, Part II*, volume 9723 of *Lecture Notes in Computer Science*, pages 446–453. Springer, 2016.

[163] P. Peer, J. Bule, J. Zganec-Gros, and V. Struc. Building Cloud-based Biometric Services. *Informatica (Slovenia)*, 37(2):115–122, 2013.

[164] J. Peng, Q. Li, A. A. A. El-Latif, and X. Niu. Finger Multibiometric Cryptosystems: Fusion Strategy and Template Security. *J. Electronic Imaging*, 23(2):023001, 2014.

[165] P. J. Phillips, A. F. Martin, C. L. Wilson, and M. A. Przybocki. An Introduction to Evaluating Biometric Systems. *IEEE Computer*, 33(2):56–63, 2000.

[166] F. L. Podio. Biometric Technologies and Security - International Biometric Standards Development Activities. In *Encyclopedia of Cryptography and Security, 2nd Edition*, pages 124–130. Springer US, 2011.

[167] S. Prabhakar, S. Pankanti, and A. K. Jain. Biometric Recognition: Security and Privacy Concerns. *IEEE Security & Privacy*, 1(2):33–42, 2003.

[168] R. Raghavendra and C. Busch. Presentation Attack Detection Algorithm for Face and Iris Biometrics. In *22nd European Signal Processing Conference, EUSIPCO 2014, Lisbon, Portugal, September 1-5, 2014*, pages 1387–1391, 2014.

[169] H. Rai and A. Yadav. Iris Recognition using Combined Support Vector Machine and Hamming Distance Approach. *Expert Systems with Applications*, 41(2):588–593, 2014.

[170] S. S. Rajibul Islam and A. Samraj. Multimodality to Improve Security and Privacy in Fingerprint Authentication System. In *International Conference on Intelligent and Advanced Systems ICIAS*, pages 753–757. IEEE, 2007.

[171] N. K. Ratha, J. H. Connell, and R. M. Bolle. Enhancing Security and Privacy in Biometrics-Based Authentication Systems. *IBM Systems Journal*, 40(3):614–634, 2001.

[172] C. Rathgeb and C. Busch. Multi-Biometric Template Protection: Issues and Challenges. *New Trends and Developments in Biometrics*, pages 173–190, 2012.

[173] C. Rathgeb and C. Busch. Cancelable Multi-Biometrics: Mixing Iris-Codes based on Adaptive Bloom Filters. *Computers & Security*, 42:1–12, 2014.

[174] C. Rathgeb and A. Uhl. A Survey on Biometric Cryptosystems and Cancelable Biometrics. *EURASIP J. Information Security*, 2011:3, 2011.

[175] C. Rathgeb, A. Uhl, and P. Wild. Reliability-Balanced Feature Level Fusion for Fuzzy Commitment Scheme. In *2011 IEEE International Joint Conference on Biometrics, IJCB 2011, Washington, DC, USA, October 11-13, 2011*, pages 1–7, 2011.

[176] A. P. Rebera, M. E. Bonfanti, and S. Venier. Societal and Ethical Implications of Anti-Spoofing Technologies in Biometrics. *Science and Engineering Ethics*, 20(1):155–169, 2014.

[177] D. Riccio, C. Galdi, and R. Manzo. Biometric Cryptographic Keys Binding based on Function Minimization. In *12th International Conference on Signal-Image Technology & Internet-based Systems, Naples, Italy, December, 2016*, pages 144–150, 2016.

[178] R. L. Rivest, L. Adleman, and M. L. Dertouzos. On Data Banks and Privacy Homomorphisms. *Foundations of Secure Computation, Academia Press*, pages 169–179, 1978.

[179] R. N. Rodrigues, N. Kamat, and V. Govindaraju. Evaluation of Biometric Spoofing in a Multimodal System. In *Fourth IEEE International Conference on Biometrics: Theory Applications and Systems, BTAS 2010, Washington, DC, USA, 27-29 September, 2010*, pages 1–5, 2010.

[180] A. Ross and A. K. Jain. Information Fusion in Biometrics. *Pattern Recognition Letters*, 24(13):2115–2125, 2003.

[181] A. Ross, A. Rattani, and M. Tistarelli. Exploiting the "Doddington Zoo" Effect in Biometric Fusion. In *IEEE 3rd International Conference on Biometrics: Theory, Applications, and Systems*, BTAS'09, pages 264–270, 2009.

[182] A. A. Ross, K. Nandakumar, and A. K. Jain. *Handbook of Multibiometrics (International Series on Biometrics)*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2006.

[183] RTS-SCA. Regulatory Technical Standards (RTS)- Strong Customer Authentication (SCA) European Commission Delegated Regulation (EU) 2018/389 of the supplementing Directive 2015/2366 of the European Parliament and of the Council with regard to common and secure open standards of communication, 2018. Accessed May 2018.

[184] N. A. Safa, R. Safavi-Naini, and S. F. Shahandashti. Privacy-Preserving Implicit Authentication. In *ICT Systems Security and Privacy Protection - 29th IFIP TC 11 International Conference, SEC 2014, Marrakech, Morocco, June 2-4, 2014. Proceedings*, pages 471–484, 2014.

[185] D. Saraswat, D. S. Sofat, and M. Kaur. Template and Database Security in Biometrics Systems: A Challenging Task. *International Journal of Computer Applications*, 4(5):1–5, July 2010. Published By Foundation of Computer Science.

[186] N. D. Sarier. *Biometric Cryptosystems: Authentication, Encryption and Signature for Biometric Identities.* PhD thesis, University of Bonn, 2011.

[187] N. D. Sarier. Privacy Preserving Multimodal Biometric Authentication in the Cloud. In *Green, Pervasive, and Cloud Computing - 12th International Conference, GPC 2017, Cetara, Italy, May 11-14, 2017, Proceedings*, pages 90–104, 2017.

[188] K. Sasidhar, V. L. Kakulapati, R. Kolikipogu, and K. KailasaRao. Multimodal Biometric Systems - Study to Improve Accuracy and Performance. *CoRR*, abs/1011.6220, 2010.

[189] A. Schaller, T. Stanko, B. Skoric, and S. Katzenbeisser. Eliminating Leakage in Reverse Fuzzy Extractors. *IEEE Trans. Information Forensics and Security*, 13(4):954–964, 2018.

[190] A. Shamir. How to Share a Secret. *Commun. ACM*, 22(11):612–613, 1979.

[191] C. A. Shoniregun and S. Crosier, editors. *Securing Biometrics Applications.* Springer US, 2008.

[192] H. M. Sim, H. Asmuni, R. Hassan, and R. M. Othman. Multimodal Biometrics: Weighted Score Level Fusion based on Non-Ideal Iris and Face Images. *Expert Systems with Applications*, 41(11):5390–5404, 2014.

[193] K. Simoens. *Analysis of Fuzzy Encryption Schemes for the Protection of Biometric Data (Analyse van Fuzzy Encryptieschema's voor het Afschermen van Biometrische Gegevens).* PhD thesis, KU Leuven, Belgium, 2012.

[194] K. Simoens, J. Bringer, H. Chabanne, and S. Seys. A Framework for Analyzing Template Security and Privacy in Biometric Authentication Systems. *IEEE Trans. Information Forensics and Security*, 7(2):833–841, 2012.

[195] K. Simoens, P. Tuyls, and B. Preneel. Privacy Weaknesses in Biometric Sketches. In *30th IEEE Symposium on Security and Privacy (S&P 2009), 17-20 May 2009, Oakland, California, USA*, pages 188–203, 2009.

[196] M. Singh and A. S. Arora. A Novel Face Liveness Detection Algorithm with Multiple Liveness Indicators. *Wireless Personal Communications*, 100(4):1677–1687, 2018.

[197] J. Sohankar, K. Sadeghi, A. Banerjee, and S. K. S. Gupta. Systematic Analysis of Liveness Detection Methods in Biometric Security Systems. In *2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation, SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI 2017, San Francisco, CA, USA, August 4-8, 2017*, pages 1–6, 2017.

[198] D. J. Solove. The Chronicle Review of Higer Education: Dizzied by Data, https://www.chronicle.com/article/dizzied-by-data/124125, 2010.

[199] A. Stoianov. Security of Error Correcting Code for Biometric Encryption. In *Eighth Annual Conference on Privacy, Security and Trust, PST 2010, August 17-19, 2010, Ottawa, Ontario, Canada*, pages 231–235, 2010.

[200] Y. Sutcu, Q. Li, and N. D. Memon. Secure Biometric Templates from Fingerprint-Face Features. In *2007 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR 2007), 18-23 June 2007, Minneapolis, Minnesota, USA*, 2007.

[201] Y. Sutcu, Q. Li, and N. D. Memon. Secure Sketches for Protecting Biometric Templates. In *Security and Privacy in Biometrics*, pages 69–104. Springer, 2013.

[202] V. Talreja, T. Ferrett, M. C. Valenti, and A. Ross. Biometrics-as-a-Service: A Framework to Promote Innovative Biometric Recognition in the Cloud. In *IEEE International Conference on Consumer Electronics, ICCE 2018, Las Vegas, NV, USA, January 12-14, 2018*, pages 1–6, 2018.

[203] Q. Tao and R. N. J. Veldhuis. Threshold-Optimized Decision-Level Fusion and its Application to Biometrics. *Pattern Recognition*, 42(5):823–836, 2009.

[204] N. Theodorakis. Secure and Privacy-Preserving User Authentication Using Biometrics. Master's thesis, KU Leuven & University of Piraeus, 2017. Enrique Argones Rua and Bart Preneel and Christina-Angeliki Toli (promotors).

[205] M. Tistarelli and M. S. Nixon, editors. *Advances in Biometrics, Third International Conference, ICB 2009, Alghero, Italy, June 2-5, 2009. Proceedings*, volume 5558 of *Lecture Notes in Computer Science*. Springer, 2009.

[206] K. Tiwari and P. Gupta. An Adaptive Score Level Fusion Scheme for Multimodal Biometric Systems. In *Adaptive Biometric Systems: Recent Advances and Challenges*, pages 119–131. Springer, 2015.

[207] C.-A. Toli, A. Abidin, A. Aly, E. A. Rúa, and B. Preneel. Secure and Privacy-Friendly Multimodal Biometric Authentication using Cloud-based Identity Providers. *Computers & Security, Elsevier (under review)*, 2018.

[208] C.-A. Toli, A. Aly, and B. Preneel. A Privacy-Preserving Model for Biometric Fusion. In S. Foresti and G. Persiano, editors, *Cryptology and Network Security - 15th International Conference, CANS 2016, Milan, Italy, November 14-16, 2016, Proceedings*, volume 10052 of *Lecture Notes in Computer Science*, pages 743–748, 2016.

[209] C.-A. Toli, A. Aly, and B. Preneel. Privacy-Preserving Multibiometric Authentication in Cloud with Untrusted Database Providers. *IACR Cryptology ePrint Archive*, 2018, 2018.

[210] C.-A. Toli and B. Preneel. A Survey on Multimodal Biometrics and the Protection of Their Templates. In *Privacy and Identity Management for the Future Internet in the Age of Globalisation - 9th IFIP WG 9.2, 9.5, 9.6/11.7, 11.4, 11.6/SIG 9.2.2 International Summer School, Patras, Greece, September 7-12, 2014, Revised Selected Papers*, pages 169–184, 2014.

[211] C.-A. Toli and B. Preneel. A Bimodal Verification Cryptosystem as a Framework against Spoofing Attacks. *International Journal of Intelligent Computing Research (IJICR)*, 6(2):548 – 557, 2015.

[212] C.-A. Toli and B. Preneel. Provoking Security: Spoofing Attacks against Crypto-Biometric Systems. In *2015 World Congress on Internet Security WorldCIS, Dublin, Ireland, October, 2015*, pages 67–72, 2015.

[213] C.-A. Toli and B. Preneel. Privacy-Preserving Biometric Authentication Model for eFinance Applications. In *Proceedings of the 4th International Conference on Information Systems Security and Privacy, ICISSP 2018, Funchal, Madeira - Portugal, January 22-24, 2018.*, pages 353–360, 2018.

[214] W. A. A. Torres, N. Bhattacharjee, and B. Srinivasan. Effectiveness of Fully Homomorphic Encryption to Preserve the Privacy of Biometric Data. In *Proceedings of the 16th International Conference on Information Integration and Web-based Applications & Services, Hanoi, Vietnam, December 4-6, 2014*, pages 152–158, 2014.

[215] Turbine. European Project Turbine: TrUsted Revocable Biometric IdeNtitiEs, http://cordis.europa. eu/project/rcn/85447.html, 2011.

[216] P. Tuyls, A. H. M. Akkermans, T. A. M. Kevenaar, G. J. Schrijen, A. M. Bazen, and R. N. J. Veldhuis. Practical Biometric Authentication with Template Protection. In *Audio- and Video-based Biometric Person Authentication, 5th International Conference, AVBPA 2005, Hilton Rye Town, NY, USA, July 20-22, 2005, Proceedings*, pages 436–446, 2005.

[217] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain. Biometric Cryptosystems: Issues and Challenges. *Proceedings of the IEEE*, 92(6):948–960, 2004.

[218] L. Vasiu. Biometric Recognition - Security and Privacy Concerns. In *ICETE 2004, 1st International Conference on E-Business and Telecommunication Networks, Setúbal, Portugal, August 24-28, 2004, Proceedings*, page 3, 2004.

[219] S. Verma and D. R. K. Singh. Multimodal Biometrics Information Fusion for Efficient Recognition using Weighted Method. *Inter. Journal of Engineering Research and General Science*, 2:582–588, 2014.

[220] VISA. Consumers ready to switch from passwords to biometrics, study shows. Research conducted by AYTM Market Research, among adult consumers who use at least one credit card, debit card, and/or mobile pay., 2018. Accessed May 2018.

[221] N. Wang, Q. Li, A. A. A. El-Latif, J. Peng, X. Yan, and X. Niu. A Novel Template Protection Scheme for Multibiometrics based on Fuzzy Commitment and Chaotic System. *Signal, Image and Video Processing*, 9(Supplement-1):99–109, 2015.

[222] Q. Wang, S. Hu, K. Ren, M. He, M. Du, and Z. Wang. CloudBI: Practical Privacy-Preserving Outsourcing of Biometric Identification in the Cloud. In G. Pernul, P. Y. A. Ryan, and E. R. Weippl, editors, *Computer Security - ESORICS 2015 - 20th European Symposium on Research in Computer Security, Proceedings, Part II*, volume 9327 of *Lecture Notes in Computer Science*, pages 186–205. Springer, 2015.

[223] M. Wazid, A. K. Das, S. Kumari, X. Li, and F. Wu. Provably Secure Biometric-based User Authentication and Key Agreement Scheme in Cloud Computing. *Security and Communication Networks*, 9(17):4103–4119, 2016.

[224] X. Xi, M. Tang, and Z. Luo. Feature-Level Fusion of Surface Electromyography for Activity Monitoring. *Sensors*, 18(2):614, 2018.

[225] C. Xiang, C. Tang, Y. Cai, and Q. Xu. Privacy-Preserving Face Recognition with Outsourced Computation. *Soft Comput.*, 20(9):3735–3744, 2016.

[226] B. Yang, D. Hartung, K. Simoens, and C. Busch. Dynamic Random Projection for Biometric Template Protection. In *Fourth IEEE International Conference on Biometrics: Theory Applications and Systems, BTAS 2010, Washington, DC, USA, 27-29 September, 2010*, pages 1–7, 2010.

[227] B. Yang, L. Rajbhandari, C. Busch, and X. Zhou. Privacy Implications of Identity References in Biometrics Databases. In *Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIH-MSP 2012, Piraeus-Athens, Greece, July 18-20, 2012*, pages 25–30, 2012.

[228] W. Yang, S. Wang, J. Hu, G. Zheng, J. A. Chaudhry, E. Adi, and C. Valli. Securing Mobile Healthcare Data: A Smart Card based Cancelable Finger-Vein Bio-Cryptosystem. *IEEE Access*, 6:36939–36947, 2018.

[229] M. Yasuda. Secure Hamming Distance Computation for Biometrics using Ideal-Lattice and Ring-LWE Homomorphic Encryption. *Information Security Journal: A Global Perspective*, 26(2):85–103, 2017.

[230] F. J. Zareen, K. A. Shakil, M. Alam, and S. Jabin. A Cloud based Mobile Biometric Authentication Framework. *CoRR*, abs/1601.02781, 2016.

[231] H. Zhu, Q. He, H. Tang, and W. Cao. Voiceprint-Biometric Template Design and Authentication based on Cloud Computing Security. In *2011 International Conference on Cloud and Service Computing, CSC 2011, Hong Kong, December 12-14, 2011*, pages 302–308, 2011.

[232] L. Zhu, C. Zhang, C. Xu, X. Liu, and C. Huang. An Efficient and Privacy-Preserving Biometric Identification Scheme in Cloud Computing. *IEEE Open Access*, 6:19025–19033, 2018.

Curriculum Vitae

Christina-Angeliki Toli was born in Thessaloniki, Greece. She received the B.Sc. degree in Electrical and Computer Engineering, Specialization on Electronics & Computers from Aristotle University of Thessaloniki (ECE AUTH), Greece. In November 2011, she obtained the M.Sc. degree in Computer Engineering from the same university ECE AUTH, Greece. She was member of the Information Processing and Computing Laboratory and the Multimedia Understanding Group. Her Master's thesis based on the topics of Computational Intelligence (Data Integration, Management and Representation, Data Mining, Machine Learning, Description logics, Semantic Web), was entitled "*Design and Implementation of an Ontology as a Tool for the Organization of the Undergraduate Studies Program of the ECE AUTH*". Since then, she is member of the Stanford University-Protégé Community Platform for the evaluation of the Protégé tool for ontologies design. Since March 2012, she is member of the National Association of Electrical and Computers Engineering Organization of the Technical Chamber of Greece. In October 2012, she joined Computer Security and Industrial Cryptography (COSIC) research group of the Department of Electrical Engineering (ESAT) at KU Leuven, Belgium. She started her PhD under the supervision of Professor Bart Preneel. Her research was financially supported by the European Project FIDELITY (Fast and trustworthy Identity Delivery and Check with ePassports leveraging Traveler privacy) and a grant of the KU Leuven Research Council (C16/15/058). Her main research interests are biometrics, template protection schemes, secure access control and identity management, privacy-preserving authentication, and privacy-by-design for secure biometric applications.

FACULTY OF ENGINEERING SCIENCE
DEPARTMENT OF ELECTRICAL ENGINEERING
COSIC
Kasteelpark Arenberg 10, bus 2452
B-3001 Leuven
christina-angeliki.toli@esat.kuleuven.be
https://securewww.esat.kuleuven.be/cosic/