ANONYMITY CONTROLLED ELECTRONIC PAYMENT SYSTEMS

Joris Claessens*, Bart Preneel†, Joos Vandewalle

Katholieke Universiteit Leuven, ESAT-SISTA/COSIC
Kardinaal Mercierlaan 94, B-3001 Heverlee, Belgium
joris.claessens@esat.kuleuven.ac.be

Today’s most used electronic payment systems offer no anonymity at all to their users. Electronic payment systems exist that provide unconditional anonymity. In this article electronic payment systems are described in which anonymity can be controlled. The requirements of such systems are discussed, and two types of tracing mechanisms are defined. An overview of the proposed anonymity controlled systems is given. We analyze to what extent these systems offer the defined tracing mechanisms. The importance of anonymous communication is stressed.

INTRODUCTION

The importance of electronic payment systems is increasing rapidly as electronic commerce is becoming part of our ordinary daily life. In order to make electronic payment systems acceptable to the general public, some degree of anonymity has to be offered. Just as with physical cash, the privacy of the users can be protected, so that the ability to link a buyer with a purchase is reduced. On the other hand, the anonymity of electronic money can be misused by criminals for money laundering, blackmailing and illegal purchases. In order to make anonymous electronic cash systems acceptable to governments and banks, mechanisms for revoking anonymity under certain conditions have been introduced. Such anonymity revocation must be possible only for a trusted third party, named trustee or judge.

In this article we discuss a number of electronic payment systems, ranging from today’s frequently used systems which offer no anonymity, to systems which offer unconditional anonymity. In between these two are the systems which offer

* Funded by a research grant of the Flemish Institute for the Promotion of Industrial Scientific and Technological Research (IWT).
† F.W.O. postdoctoral researcher, sponsored by the Fund for Scientific Research – Flanders

©1999 IEEE
some kind of controlled anonymity. We will discuss the different tracing models which can be present in an anonymity controlled electronic payment system, as well as the currently proposed systems that provide anonymity control according to these tracing models. Finally, we will address the need of anonymous communication in all these systems. Moreover, methods to obtain anonymous communication can be integrated with electronic payment systems that are far less complex, while still providing anonymity control properties.

NO PRIVACY VERSUS UNCONDITIONAL ANONYMITY

Today’s electronic commerce is almost totally based on electronic credit card transactions on the World Wide Web (WWW). The security of this system relies on the security provided by the protocols used to secure the WWW [9]. The standard SET [16] provides a lot of advanced security features, but is not yet commonly used on the Internet. These systems do not protect the user’s privacy, as the bank knows every purchase the user makes, via the user’s credit card number. However, anonymity is probably not wanted by banks, as the value of credit card payments can be rather high.

The Belgian electronic wallet Proton [19] is an electronic payment system designed for small purchases. It is based on symmetric key cryptography and uses smart card technology. The system can already be used on the Internet, and is gaining international interest. The user’s privacy is not protected. This should however be a necessary condition in order to fully emulate a wallet with physical coins.

Ecash [22] is an electronic cash system developed by (the late) DigiCash. The system uses blind signatures [8]. A blind signature scheme allows the user to get a message signed by a signer, without disclosing the contents of the message to the signer. In the ecash system coins are basically random strings signed by the bank. As the bank signs a blinded version of the random string, the bank cannot link the identity of the user (known during withdrawal of the coin) to the finally obtained coin (and thus to the payment in which that coin will be involved). To prevent double-spending of coins, the bank just keeps a list with all spent coins, and verifies whether a coin is already on that list. Therefore payment and deposit is done at the same time, which classifies the payment system as an on-line system.

More advanced electronic cash systems that offer unconditional anonymity, use restrictive blind signatures (e.g., the CAFE payment system is based on [2]).

Appeared in Proceedings of the 20th Symposium on Information Theory in the Benelux
©1999 IEEE
The bank still signs a blinded string, but the identity of the user is encoded in this string. The encoding is done in this way, that the identity of the user is revealed when the coin is double-spent. The payment can be performed off-line (i.e., deposit can be done afterwards). More information about off-line electronic cash systems can be found in [20].

**CONTROLLED ANONYMITY**

Systems exist that provide unconditional anonymity and a mechanism to protect against double-spending. However, other crimes are possible [26], in which coins are not double-spent, such as money laundering and blackmailing. In order for an electronic payment system to be acceptable for both users, banks and government, some kind of anonymity control has to be provided. In these kind of systems, it is possible to trace the owner of a coin or to trace the coins originating from a specific withdrawal. This will only be possible in cooperation with a trusted third party (or more than one) which has additional information that can be used to link coins and users. The trusted third party (also called ‘trustee’) will only reveal information if e.g. the bank obtained an approval by a judge.

According to [10], generally the following requirements are necessary for anonymity control of electronic money:

1. Electronic money should be anonymous and unlinkable to legitimate users.
2. Anonymity should be revocable, but only by a trustee or judge and when necessary.
3. The trustee should not have any power other than tracing.
4. The bank should not be able to impersonate users (even in collaboration with the trustee or the shop).
5. The anonymity is revocable only for the transaction for which a trustee’s order is given.
6. A trustee must be involved only when revocation is required, remaining off-line otherwise.
7. Anonymity revocation should not motivate crimes more serious than those it protects against.

Two types of anonymity control models are also discussed in [10], more specifically two types of tracing mechanisms: An owner tracing protocol exposes the identity of the owner of a specific coin. In this kind of protocol the bank gives to the trustee the information it received during the deposit protocol. The trustee...
then returns information which can be used to identify the owners. Owner tracing prevents money laundering and making illegal purchases, as it allows the authorities to identify the involved users. This is also called ‘after-the-purchase’ tracing. A coin tracing protocol traces the coin that originated from a specific withdrawal. In this kind of protocol the bank gives to the trustee the information about a specific withdrawal. The trustee returns information that will appear when the coin is spent. Coin tracing allows the authorities to find the destination of suspicious withdrawals. It can thus be used to identify the seller of illegal goods, and prevents the blackmailing problem. This is also called ‘before-the-purchase’ tracing. Note that an anonymity controlled system must include both means of tracing in order to satisfy selectivity (requirement 5).

**ANONYMITY CONTROLLED PAYMENT SCHEMES**

This section describes the different types of schemes that implement anonymity control.

**An efficient fair payment system.** With a fair payment system, anonymous payments are still possible, but the anonymity can be removed with the help of a trusted party, which need not be involved in the transaction itself. The efficient fair payment system by Camenisch, Piveteau and Stadler [6] is an online system (payment and deposit at the same time) in which users have two types of accounts, personal and anonymous. An anonymous payment is a transaction from an anonymous account to a shop’s account. The clue of the system consists of an efficient method for transferring money from a personal account to an anonymous account without revealing the correspondence between them (except to the judge).

The system is realized using electronic coins that can be paid only into a single account (therefore double-spending of coins can be prevented by a single counter, instead of a large database with spent coins). Perfect unlinkability of personal and anonymous accounts is realized by using a blind signature scheme. To achieve fairness, the judge knows the correspondence between the two accounts, and coins withdrawn from a personal account can only be deposit into the corresponding anonymous account.

Although the customer’s identity is not revealed, the bank can still link different transactions when the same anonymous account is used for different payments. However, the customer can use different accounts for transactions that should not
be linked. This system provides owner tracing as the judge can at any time find the origin of a transfer given the anonymous account number, and coin tracing as the judge can find the destination of a transfer, given the personal account number.

**Trustee-based tracing extensions.** Brickell, Gemmell and Kravitz [3] add anonymity control as an extension to existing electronic cash systems – in particular [2] and [12] – but still provably protect user anonymity. It is interesting that two trustees are involved in these schemes. Only if the two agree and work together, owner/coin tracing can be performed.

These two proposals require the trustees to be on-line during withdrawal, which is not as efficient as stated in requirement 6 above.

**Fair blind signatures.** Stadler, Piveteau and Camenisch [5] proposed fair blind signatures, a new type of blind signature schemes, with the additional property that, with the help of a trusted entity, it is possible to link a message-signature pair and the corresponding protocol view of the signer.

Two different types can be defined. Type I fair blind signatures allow a judge to find the message-signature pair, given the signer’s view of the protocol (which is in fact coin tracing). Type II fair blind signatures allow a judge to identify the sender, given a specific message-signature pair (i.e. owner tracing).

In anonymity controlled payment systems based on this scheme, the trustees are again on-line. Note that [25] points out some weaknesses and vulnerabilities in one of the fair blind signature schemes proposed in [5].

**Advanced schemes.** In the literature, more advanced schemes have appeared. In [13] an on-line electronic cash was proposed using blind weak signatures. A stronger tracing model, which survives the ‘bank robbery’ attack, was proposed in [15]. Owner and coin tracing with off-line trustees were proposed in [4] and [11]. A scheme with trustees distributed over the Internet can be found in [18].

**ANONYMOUS COMMUNICATION**

Although this is not always specifically mentioned in the papers, anonymous communication between the different parties is necessary, in order to have real anonymous cash. A solution for anonymous communication, called ‘mixes’, was already introduced in [7]. Mixes are applied in [24] for anonymous communication on the WWW. A very simple solution, but with not so strong properties, is the...
Anonymizer [1]. Another interesting solution, with stronger properties, can be found in [21].

One can also specifically rely on anonymous communication during the design of an anonymous cash protocol. In this way, much simpler systems can be obtained. For example, in [23] anonymity is provided by just using one-way functions. In the following sections, two anonymity controlled payment systems are described, which specifically rely on anonymous communication or techniques used for this purpose.

Mix-based payments. In [14], Jakobsson and M’Raïhi present an electronic payment system in which anonymity and anonymity control are solely based on the use of a mix network. A payment order is of the form \( o = m|a|s \) in which \( m \) is a hash of the contract, \( a \) account number merchant, and \( s \) serial number. The payer encrypts a set of orders \( o_1 \ldots o_n \) to \( \tilde{o}_1 \ldots \tilde{o}_n \) using the public key. The corresponding secret key is known only to the transaction center, and is kept in a distributed manner so that any quorum of mix servers can calculate it. The values of the transactions are described in \( d \). The payer signs \( \tilde{o}_1 \ldots \tilde{o}_n \) and \( d \), resulting in \( \sigma \). The transaction center verifies \( \sigma \). It adds each valid \( \tilde{o}_i \) to an internal list (one such list for each denomination) and debits the payer’s account. It signs each \( \tilde{o}_i \) (different public keys for different denominations) and sends \( \sigma_1 \ldots \sigma_n \) to the payer. The payer sends \( \tilde{o}_i, \sigma_i \) to the merchant, which verifies \( \sigma_i \). At given intervals, the transaction center decrypts all payment orders: the input is a list of encrypted messages, the output is a permuted list of the corresponding decrypted messages. The items of these lists indicate what accounts are to be credited, and by how much. The two tracing operations are based on the mix en/de-cryption scheme. A payment order of a specific payer can be traced (coin tracing) by simply decrypting the encrypted payment order \( \tilde{o} \) in question. The payer of a specific payment order can be traced (owner tracing) by reversing the encryption of \( o \) to \( \tilde{o} \) step by step (how this must be done, depends on what type of mix network is used).

NetCash. NetCash [17] is an on-line electronic cash system developed at the University of Southern California. There are three parties involved: ‘Clients’, ‘Merchants’ (including Banks) and ‘Currency Servers’ (CS). Currency Servers have to obtain a certificate for minting currency from the ‘Federal Insurance Corporation’ (FIC): \( \{\text{Certif}.id, CS\_name, K_{CS}, \text{issue\_date}, \text{exp\_date}\}K_{FIC}^{-1} \). An electronic coin is represented as: \( \{CS\_name, s\_addr, exp\_date, serial\_num, coin\_val\}K_{CS}^{-1}, \text{Certif}.id \).

Appeared in Proceedings of the 20th Symposium on Information Theory in the Benelux
©1999 IEEE
Both Clients and Merchants can perform an exchange protocol with a CS in order to verify coins, exchange coins for untraceability, purchase coins and cash in coins. A simple payer-payee exchange exists in which the Client receives a kind of ticket in exchange for coins, that can be used to get the service for which the Client has paid. Double-spending is either detected at the time the recipient verifies or exchanges coins with a CS, or the coins can only be spent by the recipient during an initial time window, allowing the recipient to cash them in before they can be double-spent. The anonymity provided by NetCash is weaker than the unconditional anonymity. It is possible for a CS to record which coins have been issued. It is expected that CSs will not do so. Clients can choose their own CS, and will choose one that they feel they can trust. If CSs can be seen as trustees, recording all information, but revealing information only when asked for by a judge, then the NetCash system can be classified as an anonymity controlled electronic cash system.

**CONCLUSION**

Today’s currently used electronic payment systems do not provide privacy to the users. However, payment schemes exist that provide unconditional anonymity. These electronic payment systems are not used on a large scale, as they are not accepted by governments and banks.

In this article, the current state of the art of anonymity control in electronic payment systems has been discussed. We have seen the requirements for a good anonymity controlled payment system, as well as the two tracing models that have to be implemented in order to fulfill one of these requirements. We have discussed different proposed anonymity controlled electronic payment systems.

Finally, we have addressed the need for anonymous communication. Moreover, anonymity control in electronic payment systems can be implemented relying on the anonymous communication mechanisms.

**REFERENCES**


