Better, Faster, Stronger! Optimizing Post-Quantum Cryptography in Hardware



This image was generated using OpenAI's DALL·E AI image generator.

Haven't you heard? Advances in quantum computing are making waves across the world. While this opens up incredible possibilities, there is a major downside: quantum computers have the potential to break current asymmetric cryptographic standards, which protect billions of devices globally. This has created an urgent need for new cryptographic algorithms resistant to quantum attacks, which is the focus of post-quantum cryptography. To select quantum-resistant standards, the National Institute of Standards and Technology (NIST) initiated a public process, including a call for additional digital signature (DS) schemes[1].

In order to diversify the portfolio of future PQC standards, NIST has selected schemes from multiple families, each based on different mathematical hard problems. One family in particular, isogeny-based cryptography, is particularly interesting as it offers significantly smaller key material and signatures compared to other candidates. However, these schemes suffer from a large computational overhead making them unsuitable for real-world deployment in their current state.

In this thesis, the student will dive into this exciting area by implementing an isogeny-based DS scheme, involved in the ongoing NIST competition. Starting with the reference software implementation, the student investigates how to efficiently map the scheme onto hardware. Given that several of these schemes are relatively new and there is minimal time for the community to explore, significant opportunities for optimization exist. The goal of this project is to showcase the practical potential of these new PQC DS schemes, helping to demonstrate their real-world feasibility. By optimizing their implementation, your work could play a pivotal role in advancing these schemes in the NIST competition and directly contribute to the development of quantum-resistant cryptography. As a prerequisite, the student should have taken the Design of Digital Platforms (DDP) course (and earned a passing grade) and be familiar with the PYNQ FPGA development board.

Practicalities

Promoter:	Ingrid Verbauwhede		
Daily supervisor:	Emre Koçer	emre.kocer@esat.kuleuven.be	office 01.16
	Suparna Kundu	suparna.kundu@esat.kuleuven.be	office 01.20
	Quinten Norga	quinten.norga@esat.kuleuven.be	office 01.16
Nature of the work:	20% literature, 20% theoretical work, 60% implementation		
Number of students:	1		

[1] https://csrc.nist.gov/Projects/pqc-dig-sig/round-2-additional-signatures