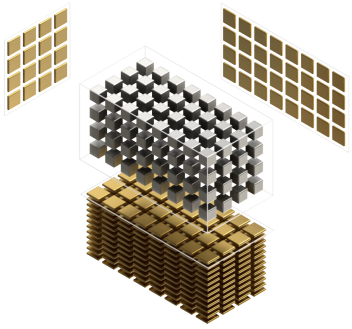
Leveraging Machine-Learning Accelerators for High-Performance Post-Quantum Cryptography



Source: https://developer.nvidia.com/blog/programming-tensor-cores-cuda-9/

Advances in quantum computing are making waves across the world, paving the way for potential breakthroughs in several scientific disciplines. However, 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 that are resistant to quantum attacks, which is the focus of post-quantum cryptography (PQC). To select quantum-resistant standards, the National Institute of Standards and Technology (NIST) published a call for additional digital signature (DS) schemes[1]. However, these newly proposed schemes suffer from a large computational overhead - in part due to large matrix-vector arithmetic - making them less suitable for real-world deployment in their current state.

Similarly, the latest AI technologies are requiring an ever-increasing demand for computational power, leading to significant breakthroughs in machine learning (ML) accelerators. Naturally, the question arises if this hardware can be leveraged to accelerate cryptographic workloads, enabling cryptography to benefit from the advances in the field of AI hardware development.

In this thesis, the student will implement a novel and promising DS scheme, involved in the ongoing NIST competition, and optimize it for ML accelerators. More specifically, through a combination of algorithmic analysis (e.g. optimal mappings of cryptographic operations to GPU kernels) and an in-depth analysis of ML accelerators, the goal is to showcase the practical potential of these new PQC DS schemes by demonstrating significant speed-ups compared to SOTA implementations on other platforms. Through this thesis, the student 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. Experience with the CUDA language (or similar) are a bonus.

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 ESAT 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