Accelerating the Next Generation of Post-Quantum Digital Signatures



This image was generated using Microsoft Copilot (AI image generation).

The emergence of large-scale quantum computers threatens the security of currently deployed public-key cryptographic systems. Post-quantum cryptography (PQC) aims to develop secure alternatives that remain resistant to both classical and quantum adversaries. As part of this global effort, the Chinese Institute of Commercial Cryptography Standards (ICCS) launched the Next Generation Commercial Cryptographic (NGCC) project to identify and standardize next-generation cryptographic algorithms for commercial applications. It has recently announced its first-round candidates for digital signature, key encapsulation, and key exchange algorithms [1].

MORNING-ATLAS [2] is a post-quantum digital signature designed by our research group, and has been selected as a first-round candidate in the NGCC standardization process. The objective of this thesis is to investigate the practical efficiency of this digital signature scheme and evaluate its suitability for real-world deployment. The student will analyze the computational bottlenecks in existing implementations and develop optimized software and/or hardware implementations of the MORNING-ATLAS scheme's algorithms. Depending on the student's interests, the optimization effort may target modern processor architectures such as x86, ARM, or RISC-V, leveraging architecture-specific features such as vector instructions, parallelism, and memory optimization techniques. Alternatively, the thesis may explore hardware acceleration using FPGA-based platforms. The results of this thesis will offer critical insights into the implementation efficiency of these promising post-quantum cryptography (PQC) candidates, potentially contributing to their ongoing assessment within international standardization efforts.

Practicalities

Promoter:	Prof. Dr. Ingrid Verbauwhede		
Daily supervisor:	Suparna Kundu	Suparna.Kundu@esat.kuleuven.be	office 01.20
	Emre Koçer	emre.kocer@esat.kuleuven.be	office 01.16
	Quinten Norga	quinten.norga@esat.kuleuven.be	office 01.16
Nature of the work:	20% literature, 30% theoretical work, 50% Implementation		
Number of students:	1 or 2		

[1] https://www.niccs.org.cn/niccs/Notice/pc/content/content_2100875480644800512.html
[2] https://drive.google.com/file/d/10JxDlTKhTsYA5F5kmm1Pr91J7SCfZPY4/view?usp=sharing

 © 2026 – 2027 COSIC