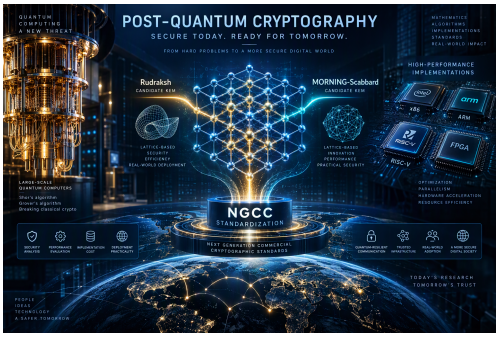
Optimizing Future Post-Quantum Encryption Standards



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

Post-quantum cryptography (PQC) aims to ensure the long-term security and integrity of digital communications against adversaries equipped with large-scale quantum computers. To facilitate the adoption of quantum-resistant cryptographic standards, the Chinese Institute of Commercial Cryptography Standards (ICCS) launched the Next Generation Commercial Cryptographic (NGCC) algorithms project, an open standardization effort focused on identifying and evaluating suitable post-quantum cryptographic primitives for commercial deployment. It has recently announced its first-round candidates for digital signature, key encapsulation, and key exchange algorithms [1].

Two key encapsulation mechanisms (KEMs) developed by our research team, Rudraksh [2] and MORNING-Scabbard [3], have been selected as first-round candidates in the NGCC standardization process. The objective of this thesis is to investigate the practical efficiency of these two emerging PQC schemes and evaluate their suitability for real-world deployment. The student will analyze the computational bottlenecks of existing implementations and develop optimized software and/or hardware realizations of algorithms of one or both schemes. 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 outcomes of this thesis will provide valuable insights into the implementation efficiency of two promising PQC candidates and may contribute directly to their ongoing evaluation within international post-quantum cryptography 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/1HynPuJ7s-qgL6RV5Szd9OUE0aPpzkt_1/view
[3] https://drive.google.com/file/d/1RMrZoasaDLyDb12eVZgaWd_Yhb6wnAFz/view

 © 2026 – 2027 COSIC