Post-Quantum Cryptography Meets Approximate Computing: Challenges and Opportunities

Emanuele Valea
CEA Greonble

11/06/2025, session 2, orateur 2

Résumé

Approximate Computing (AxC) is an emerging paradigm that trades algorithmic accuracy for reduced implementation costs, such as lower power consumption or silicon area. While AxC is widely used in error-resilient applications like AI, its application in cryptography has been controversial, as cryptographic schemes are typically intolerant to computational errors. However, Post-Quantum Cryptography (PQC), designed to withstand quantum-enabled attacks, is founded on a new class of cryptographic schemes based on hard learning problems. Notable examples include Learning with Errors (LWE) and its variant, Module-LWE (M-LWE). Since these cryptographic schemes inherently incorporate probabilistic functions and controlled noise generation, it opens new opportunities for AxC-driven hardware optimizations. This talk will explore existing and novel approaches for applying AxC to PQC, leveraging both digital approximate circuits and electrical-level approximations. Finally, it will highlight future research challenges and opportunities at the intersection of AxC and PQC.