Title: Post-Quantum Cryptography: From the Point of View of Hardware Security

Abstract: In the present day, it is not an 'if' on whether quantum computers will be a reality, but rather when. It is well known, that such power of computing can break well known public key cryptosystems, necessitating the development and standardization of quantum-resilient cryptography. In this talk, we provide an overview on Post Quantum Cryptography (PQC), discussing the multiple hard-problems which seem to be resilient against Quantum Computers. However, PQC involves complex arithmetic, obviating the need of hardware acceleration for real time requirements in the present world of digital transactions. In this context, we make a quick look into the NIST standardization, and delve into the important protocol of Transport-Layer-Security (TLS) and identify key NIST-certified PQC algorithms based on lattices which are necessary for achieving a post-quantum TLS. In this talk, we make a deeper look into how the specifications of the KEM-algorithm, namely Kyber, and signature scheme, Delithium can be manoeuvred to realize a common datapath for NTT Number-Theoretic-Transform) multiplier, one of the crucial arithmetic blocks. We propose a sketch of an agile co-processor for the Post-quantum-TLS (KGP-PQC-TLS) which has the ability to not only support varying security levels, but also can be used in the future to support other post-quantum algorithms based on lattices. Finally, we conclude with some comments on side channel vulnerabilities of such hardware instances.