Title: Side-Channel Leakage Quantification and Efficient Post-Quantum Architectures on Emerging Platforms: Next Generation Challenges in Hardware Security

Speaker: Dr. Debapriya Basu Roy, Technical University of Munich.

Date and Time: June 21, 2021 (Mon), 11:00 AM

Venue: Zoom

Abstract:

The domain of hardware security has gone under a significant transformation in last few years due to the advancement in side-channel analysis and quantum computing. A side-channel adversary observes physical information like time, power, or electromagnetic radiation of cryptographic algorithm implementation and obtains the secret key from classical-cryptanalysis secure cryptographic algorithms like AES or elliptic curve cryptography (ECC). Due to this, every cryptographic implementation should be properly evaluated for detection and quantification of side-channel leakages. Recent progress in quantum computing hardware, on the other hand, would make the public key algorithms like RSA and ECC vulnerable, and therefore search for post-quantum secure public-key algorithms along with their efficient implementation are of paramount importance. In this talk, we are going to focus on these two advanced research problems.

Testing for side-channel leakages can be done in two distinct ways: evaluation style and validation style. Evaluation style testing computes the actual success rate (SR) of side-channel attacks, but is quite slow and often dependent upon the expertise of the evaluator. Validation style testing uses "Test Vector Leakage Assessment" (TVLA) to detect the presence of side-channel leakages and has the advantage of being fast and analytical. However, it cannot quantify the leakage in terms of SR, thus cannot be used for leakage quantification. In this first half of the presentation, we extend the TVLA testing to derive a concrete relationship between TVLA and signal-to-noise ratio (SNR) of side-channel traces. The linking of the two metrics allows direct computation of success rate (SR) from TVLA for a given choice of intermediate variable and leakage model in an automated analytical manner. Thus the proposed testing methodology unifies these two side-channel detection (TVLA) and evaluation (SR) metrics.

In the second part of the talk, we would focus on the integration of a post-quantum secure public-key algorithm "Supersingular Isogeny based Key Exchange" (SIKE) with advanced microcontrollers like ARM Cortex A9 and RISC-V processor. In this context, we show the advantage of a tightly coupled accelerator that can be developed for RISC-V processors, compared to a loosely coupled accelerator applicable on ARM processors. The design of the SIKE is based on novel redundant number system architecture which reduces the clock cycle requirement significantly. We will conclude the talk with an overview of future research directions in the domain of side-channel analysis and post-quantum cryptography implementation.

Bio:

Debapriya Basu Roy did his Ph.D. at the Indian Institute of Technology Kharagpur under the supervision of Dr. Debdeep Mukhopadhyay. in the field of hardware security. He is currently working as a postdoctoral research fellow at the chair of security in information technology in the Technical University of Munich. His broad research areas are efficient cryptographic implementations, side-channel security, and advanced hardware security primitives. He is currently focusing on secure implementations of post-quantum cryptography and advanced side-channel attacks.