Side-channel analysis of cryptographic implementations: Lessons learned and future directions

Lejla Batina

Radboud University, The Netherlands

Side-channel analysis has changed the field of cryptography and it became the most common cause of real-world security applications failing today. It has also shaped the way crypto competitions are run such as recently finished NIST Post-quantum and Lightweight crypto standardization processes. In this talk we give an overview of side-channel attacks on implementations of cryptography and countermeasures. We also discuss the ways in which Machine learning and AI changed the side-channel analysis landscape and attackers' capabilities in particular. We survey several examples of AI assisting with leakage evaluation and discuss the impact of it on the field and security evaluations. Finally, we also describe the way side-channel analysis threatens AI implementations e.g. neural nets architectures that are commonly used in practice. In the end, we identify some avenues for future research.