Cryptographic Hardware Acceleration for Emerging Security Applications

Hardware security has emerged as a major concern with the advent of the Internet of Things which consists of large networks of wireless-connected embedded devices. Although the growth of such networks has enabled novel applications, they have also become attractive targets for cyber attackers. Securing these resource-constrained embedded systems involves circuits, architectures and algorithms with low computation and storage overheads as well as countermeasures against physical attacks. The threat of quantum adversaries has led to the development of quantum-safe cryptography with unique implementation requirements and challenges. A widely adopted approach is the design of efficient cryptographic hardware accelerators for IoT applications. This talk will summarize recent results and emerging research directions in the implementation aspects of post-quantum cryptography algorithms, including design considerations, custom hardware architectures, software-hardware co-design, system-level integration and end-to-end security protocols.