Abstract

In resource-constrained networks like IoT and CPS systems, security is a crucial aspect that needs to be well-studied. These networks have limited resources designated for performing cryptographic operations to provide security. At the same time, these low-end devices are easily accessible by adversaries. Therefore, secure communication and computation protocols should be proposed that are lightweight in nature while providing robust security. Hardware intrinsic primitives like physically unclonable functions (PUFs) act as device-level fingerprints. They eliminate the requirement of secure storage of private keys on resource-constrained devices, which are prone to key-stealing attacks. However, existing solutions, still have limitations like, the requirement of secure storage, trusted third parties and physical transfer of the hardware primitive from one party to the other. The primary goal of the thesis is to design PUF and PReF-based authentication, bit commitment and oblivious transfer protocols that eliminate the limitations of existing PUF-based solutions.

In this thesis, an operationally asymmetric PUF-based authenticated key exchange protocol is proposed for the smart metering test bed, to eliminate secure storage of challenge-response pairs on the server and secret key on the meter. Next, we propose a novel concept called the physically related functions (PReF) and build a suite of PReF-based protocols, without requiring a trusted third party for secure authentication and key exchange between resource-constrained nodes. Then, we propose a throughput enhanced PUF-architecture and use it to build authenticated key exchange between nodes, without requiring asymmetric cryptographic operations like elliptic curve scalar multiplication. In the next part of the thesis, we explore the XOR composition of PReFs and new security properties to prove the security of PReF-based secure two-party computation protocols. We propose a statistically hiding and computationally binding XOR_PReF-based bit commitment protocol. Finally, we propose two oblivious transfer protocols based on XOR_PReFs in the malicious receiver setting.

Keywords: Hardware Intrinsic Primitives, Physically Unclonable Functions, Physically Related Functions, Authenticated Key Exchange, Forward Secrecy, Bit Commitment, Oblivious Transfer.