Abstract

Physically Unclonable Functions (PUFs) promise to be a critical hardware primitive to provide unique identities to billions of connected devices in Internet of Things (IoTs). In traditional authentication protocols, a user presents a set of credentials with an accompanying proof such as password or digital certificate. However, IoTs need more evolved methods as these classical techniques suffer from the pressing problems of password dependency and inability to bind access requests to the “things” from which they originate. The primary goal of the thesis is to design PUF based authentication protocols for IoT framework.

In this thesis, an identity-based authentication, key generation and secure communication protocol has been proposed that deploys PUFs to produce the public identity of a device. Next, we provide a theoretical analysis of delay constraints in the delay-based PUFs that can be exploited by the adversary to generate a larger set of challenge-response pairs (CRPs) from a smaller set, thus aiding to machine learning tool based attacks on PUFs. Next we propose a framework where the verifier can authenticate a prover with an embedded PUF instance without having access to raw CRPs. We then integrate our proposed framework with OpenSSL and shown that it can be used in Transport Layer Security (TLS) protocols with less message exchange overhead. We also investigate remote integrity verification of sensor data and propose a family of authenticated sensing protocols leveraging the unreliability property of the PUFs to provide a trustworthy proof of the data across environmental factors variations.
Apart from the traditional prover-verifier model of PUF based authentication where the identity of the prover is tagged with its CRP database, we also propose an anonymous authentication protocol where the PUF instance will be private to the prover; still it will be able to authenticate itself to the verifier without violating the principle of anonymity.

Keywords: Physically Unclonable Functions, Authentication, Key management, Cryptographic protocols, Anonymity, Internet-of-Things.