SECURITY AWARE ARCHITECTURAL EXPLORATION OF PUBLIC KEY ALGORITHMS

Debapriya Basu Roy

Abstract

Public key cryptography is a major component in a secure communication network as it ensures authentication and confidentiality of different interacting parties. The recent bloom of Internet-of-Things enhances the importance of implementation of public key cryptography in embedded devices. The front runners of public key cryptography are RSA crypto-system and elliptic curve cryptography (ECC), out of which ECC suits more the purpose of embedded device security for its wonderful property of providing more security per key bit than its counterpart RSA. Depending upon the implementation requirement, in some cases, a lightweight implementation of ECC will be desired (for example home security system). Similarly, in applications like autonomous car systems, a fast implementation of ECC will be required. Moreover, with the recent advances in quantum computing, public key cryptography is going to undergo major changes as traditional cryptosystems like ECC and RSA will not remain secure anymore. National Institute of Standards and Technology (NIST) has already identified this threat and currently, the process of standardizing post quantum secure public key algorithm is being carried out. Developing efficient implementations of such post quantum secure public key algorithms is therefore an absolute necessity.

In this thesis, we have developed three different types of ECC implementations. The first one is directed for resource constrained devices suitable for IoT applications. The objective of the second ECC implementation is to meet the speed requirement of applications like autonomous cars on any generic elliptic curve. Finally, in this thesis, we will also propose an efficient implementation of supersingular isogeny based key exchange algorithm (SIKE) which is a potential candidate in the NIST post quantum public key algorithm standardization program.

Apart from traditional cryptanalysis, a cryptographic algorithm can be vulnerable to side channel cryptanalysis where an adversary observes physical information like power, time, electromagnetic radiation to retrieve the secret key. Therefore, a proper testing methodology to quantify the side channel vulnerability

is imperative. Existing methodologies for side channel vulnerability testing are complex to quantify leakage or easy, but can only detect leakage. In this thesis, we will propose an efficient hybrid side channel testing methodology which can quantify side channel leakage using a completely analytical approach.

Keywords: Elliptic Curve Cryptography, FPGA, Lightweight, Generic, SIKE, Side Channel, Leakage Quantification