ABSTRACT

Modern security systems such as smart cards and Radio Frequency Identification (RFID) tags use cryptographic algorithms to provide confidentiality, integrity and authenticity of data. Breaking a cryptographic algorithm typically means finding the secret key. In the real world, an adversary has access to the cryptographic device and can tamper with it or monitor some physical leakages that emanate from the chip. These are classified as side-channel attacks which target the cryptographic device itself. The proposed research targets power analysis attacks as they are one of the most powerful and common type of side channel attacks.

The main objective of this research is to investigate both power analysis attacks and their countermeasures on cryptographic devices. In the initial phase of the research, a novel method for improving the success rate in machine learning based power analysis attack is proposed using minimal data set. In the second phase, different countermeasures are proposed both at the circuit level and gate level to resist the power analysis attacks in cryptographic devices.

In the initial phase, machine learning based power analysis attack is proposed to improve the key guessing ratio and simultaneously reduce the number of power supply current traces. In this proposed methodology, power supply current traces are pre-processed by using wavelet transform, data normalization, and principal component analysis. Then, the pre-processed power supply current traces are used to train the

Probabilistic Neural Network. The trained network is used to classify the power supply current traces of the actual device to which the attack is mounted and the correct key is guessed. In the proposed methodology, the attacker can determine the secret key with one measured power trace from the device to be attacked which is more advantageous when compared to the bit-by-bit guessing of the secret key in earlier methods.

In the second phase, an energy efficient and power analysis attack resistant cryptographic hardware implementation is proposed. The XOR logic plays an important role in Galois Field arithmetic operations which are used in most of the cryptographic algorithms. This research focuses on the implementation of XOR logic operation and the proposed structure uses adiabatic 2N-2N2P pull-up which improves the energy efficiency. In addition, charge sharing mechanism is also employed to achieve constant current consumption independent of the inputs. Hence, the proposed XOR gate can be used to implement an energy efficient and secure hardware resistant against power analysis attacks.

In the third phase, cryptographic algorithms such as Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) are designed using reversible logic gates. It has been proved in literature that for a logically reversible system, the energy dissipation theoretically approaches zero under ideal physical circumstances. This shows that reversible logic gates are the ideal candidates to design cryptographic algorithms to make them resilient against power analysis attacks. The major transformations of AES algorithm such as SubBytes, MixColumns, ShiftRows, AddRoundKey and Key scheduler are deduced to logical operations using Galois Field arithmetic. The deduced logical operations are synthesized by using Toffoli family of reversible logic gates and they are reused wherever possible to achieve optimum results.

The important performance metrics considered for optimization in the proposed designs are the number of ancilla inputs, garbage outputs, gate count, quantum cost and delay.

In addition, two new hardware architectures are proposed to perform Montgomery multiplication in prime field GF(p) and binary field GF(2^m). The proposed structures are optimized by removing redundant gates thereby saving hardware cost and reducing quantum cost by efficient design in reversible logic. Both prime field and binary field multiplier architectures can be used to perform scalar point multiplication operations in Elliptic curve cryptography. For example, binary field multiplier structure has been used to implement scalar multiplication operation of ECC in this research. Standard projective coordinates are used to represent elliptic curve points which avoid expensive inverse operations.

The physical implementation of reversible logic gates is still an active area of research. A novel adiabatic implementation of reversible logic gates is proposed to provide resistance against power analysis attacks by using charge sharing mechanisms. Hence, any secure hardware systems can be implemented by using the proposed adiabatic reversible gates which gives protection against power analysis attacks.

In this research, a novel method is proposed to perform power analysis attacks on cryptographic devices based on machine learning method. In order to safeguard the secure system against power analysis attacks, two different countermeasures are proposed in this research at different levels of abstraction such as circuit level and gate level. The proposed countermeasures can be used to design secure hardware in low-energy applications, such as smart cards, RFID tags, wireless sensors and biomedical devices.