Executive Summary

Background:

Ciphers like AES, DES are known for their huge footprint, high power dissipation and higher gate counts. It is practically impossible to use these ciphers to provide security for small scale embedded systems. Small scale embedded systems work on 4-bit/8-bit processors. These processors have a very small memory size and cannot afford the applications which dissipate huge power. Devices like RFID tags have a total of 10,000 GEs (Gate Equivalents) available for hardware implementation. Out of these only 300-2100 GEs would be available for security aspects. These constraints result in the emergence of a new field, Lightweight Cryptography. Lightweight cryptography endorses those ciphers that have a robust design, smaller footprint, low power dissipation and GEs less than 2100. Recently, many lightweight ciphers have been designed with robust architecture to make fields like IoT and pervasive computing feasible. Ciphers like PRESENT, HUMMINGBIRD-2, SIMON, SPECK, PICCOLO and RECTANGLE have a compact design and need smaller GEs which are the key parameters in the field of lightweight cryptography. The newly designed cipher like PRESENT has a weak S box according to lemmas but has a strong permutation layer. PRESENT is designed by keeping in mind compactness while the RECTANGLE cipher is designed with strong cryptanalysis properties. The RECTANGLE cipher has a strong S-box. In recent years, ciphers like SIMON, SPECK, TWINE are considered as being the most compact ciphers and have a good performance on both hardware and software platforms.

Problem statement and objective

To design, analyze and build a lightweight hardware and software design which can be implemented for security in applications like IoT, pervasive computing and small scale embedded systems. The design should have a small footprint, low power dissipation and a low gate count.

Abstract

Pervasive computing is an emerging field that needs devices that have low power consumption and low memory requirements, specifically devices like RFID tags and wireless sensor nodes. Privacy is of great concern in applications like Internet of Things (IoT), where
each device has intelligence and has the ability to communicate with other devices. The total Gate Equivalents (GEs) required to build an RFID tag circuit is approximately 10000. In that design for providing security, the GEs should not be more than 2000-2200. For such applications, the ciphers like AES, DES are not suitable for deploying security, as they need 2400-3500 GEs. This has led to the emergence of the field of lightweight cryptography. In this field, new ciphers are needed which have lower GEs and have lower RAM and Flash requirements. In recent years, many lightweight ciphers have been designed. These lightweight ciphers are either block ciphers or stream ciphers. In block ciphers, the ciphers are divided either as Feistel structures or as SP-networks. Stream ciphers are compact in nature, which results in smaller hardware implementation and faster throughput. However, by using reused key attacks, stream ciphers can be broken; while block ciphers are versatile structures and they have made their mark in the cryptographic environment as structures that are difficult to break. KLEIN, PRESENT, LED, mCrypton and ZORRO are SP-network block ciphers, while CLEFIA, PICCOLO, TWINE, TEA, XTEA, SIMON and SPECK are Feistel networks. These Feistel networks have classifications as Generalized Feistel structures (GFS) and classical Feistel structures. In GFS, a block size is divided into more than or equal to 3 sub blocks. CLEFIA is the example of GFS developed by SONY. But, the GFS has the disadvantage of requiring more number of rounds to provide optimum security.

The work in this thesis is aimed at providing an ultra lightweight cipher design which has a robust design and should result in a lower footprint, lower power dissipation, and lower GEs. The designed ciphers should thwart all possible types of attacks. Block ciphers are known as workhorses in the cryptographic environment. In this thesis, we aimed at designing block ciphers of both SP-network and Feistel based designs. These cipher designs should perform efficiently both on hardware as well as on software platforms. The cipher designs proposed and presented in this thesis are competitive as compared to the existing lightweight ciphers in terms of memory requirement, GEs, throughput and power consumption.

**Scope of Present Work**

It is necessary to design a lightweight cipher which has a rich encryption standard but consumes lesser power and need a smaller footprint for its hardware implementation. All the standardized existing cryptographic algorithms have a huge footprint and a complex process which makes them infeasible for small scale embedded systems where memory is the constraint. The software implementation of cryptographic algorithms consumes more power
as compared to its hardware implementation. It is necessary to design a hardware implementation of cryptographic algorithm which accelerates the sorting and permutation process in encryption. Standard algorithm decryption will consume more power than encryption, as in the case of AES-128, decryption consumes 30% more power than encryption. Measures should be taken to dissipate lesser energy while securing an environment. Hardware architecture accelerates cryptography but lacks flexibility while software versions have high flexibility but consume more power. Hence, the need to have a balance between hardware and software design in securing an embedded system environment.

While designing a lightweight cipher, the metrics like throughput, execution time and number of CPU cycles needed for encryption should also be considered. The first aim in designing a cipher should be its robust architecture. The cipher should thwart all possible types of attacks. A lightweight cipher should show good resistance against linear and differential cryptanalysis. These techniques are the basic cryptanalysis techniques to find the robustness of a cipher. Other advanced techniques like Biclique attack, Zero correlation attack, Avalanche test decide the robustness of a lightweight cipher. The lightweight cipher should be tested for all these cryptanalysis techniques and the cipher design should thwart these attacks. But, at the same time, the lightweight cipher should also have a small footprint, lower GEs and lower power consumption. Thus, each stage in the lightweight cipher should be designed carefully in order to address all these constraints effectively.

**Methodology and Methods**

1) All the lightweight ciphers are implemented in embedded C on ARM platform. Flash memory size and RAM memory size are calculated through the KEIL uVision 4.0 Simulator. Verilog is used for the hardware implementation and power is calculated through the Xilinx Xpower tool analyzer.

2) Different Cryptanalysis methods are studied and implemented. To mount a linear and differential attack we wrote algorithms to find and evaluate Linear Approximation Table, (LAT) and Difference Distribution Table, (DDT). We wrote algorithms also to find linear and differential trails with a minimum number of active S-boxes.

3) One of the most important parameters in cipher design is its non-linear layer popularly known as S-box. Designing of a good S-box can result in robust architecture and also
indicates strong Linear and Differential properties. The Computer based algorithm is designed to find good 4-bit S-boxes. Different S-boxes of existing ciphers are compared with S-boxes designed and proposed in this paper. S-boxes proposed in this paper have better linear and differential cryptanalysis as compared to other lightweight ciphers.

4) GRP, known as group operations, is known for good cryptographic properties. In this thesis, with the help of GRP, a hybrid cipher is designed which results in a robust architecture.

5) Advance attacks like Biclique attack, Zero correlation attack, Meet In The Middle attacks (MITM) are also studied, analyzed and mounted on the proposed lightweight ciphers in this thesis. Other attacks like Avalanche Test, Algebraic attacks are also mounted on all these lightweight variants.

6) Other important parameters like throughput, execution time and numbers of cycles needed are also considered while designing the lightweight cipher.

**Results and Discussions:**

In this thesis, we have presented a work which revolves around designing a robust lightweight cipher. Security of ciphers is of the utmost concern along with other important parameters like GEs, power dissipation, footprint and throughput. The motivation of the work presented in this thesis is to design a lightweight cipher which is robust in design and competitive in all other parameters like footprint, GEs, power consumption and throughput.

The first design proposed in this paper is a hybrid structure which is a fusion of a GRP based permutation layer and an S-box of the PRESENT cipher. GRP instructions are known for complex operations which are useful in the cryptographic environment. With the GRP instructions we have designed a robust permutation layer which thwarts linear and differential attacks. Similarly, we have used the S-box of the PRESENT cipher and SPECK cipher key scheduling to make the design compact and competitive in parameters like footprint and GEs.

The other important designs presented in this paper are the lightweight ciphers which are BORON, MANTRA, GRANULE and PICO. All these proposed cipher designs are innovative in nature and robust in design. All lightweight ciphers proposed in this paper resist all possible types of attacks as discussed in previous chapters. These ciphers perform more efficiently based on the required applications as compared to the existing ciphers.
The BORON cipher aims for throughput; BORON has maximum throughput as compared to the existing lightweight SP-network ciphers. MANTRA cipher has a very small footprint and it is the smallest as compared to other lightweight variants. GRANULE is designed to have less GE’s and it is competitive with respect to existing ultra lightweight ciphers. The last design proposed in this paper, PICO, has lesser power dissipation and consumes even lesser power than the PRESENT cipher. All these ciphers thwart basic as well as advance attacks as discussed and presented in this thesis. We have also done some study on S-box properties and their design. We have presented and proposed a few S-boxes which have better properties and can be considered while designing a lightweight cipher.

**Conclusion**

In this thesis, we have proposed a few light variants that are robust in design and need lesser memory space for its software implementation. For hardware implementation of these ciphers, we need 1400-1900 GEs which is a competitive figure with respect to implementation of existing ciphers.

We have designed one hybrid cipher with the help of GRP (Group operations). We have presented in this thesis both SP-network ciphers as well as Feistel based networks. GRANULE and MANTRA are Feistel based networks while PICO and BORON are SP-network ciphers. All these ciphers show good cryptanalysis and resist all possible types of attacks. Advance attacks like Biclique and Zero correlation attacks are also mounted on these ciphers and all our designs resist these types of attacks. These ciphers also have a small footprint and very low power dissipation which makes them suitable for applications like pervasive computing. Power consumption is one of the important aspects in lightweight cipher design. Very few lightweight ciphers have shown this aspect. Even if the footprint is small, it does not imply that its power consumption will also be low. In this thesis, we have presented in detail analysis about power consumption and all the proposed lightweight ciphers consume lesser power as compared to existing lightweight ciphers. We have made designs in such a way that it should have a strong architecture and it should also result in lower power consumption, lower Flash memory size and higher throughput. All designs are innovative and suited for applications where footprint size and power consumption are major constraints.