Advanced Lightweight Data Encryption Technique

Meera Saifi¹, Nadiya Habeeb²
M.Tech Scholar in VLSI and Embedded Systems¹, Associate Professor²
Department of ECE
Musaliair College of Engineering and Technology, Kerala, India

Abstract:
Cryptosystem is one of the most discussed area in today’s digital world. The increasing use of pervasive devices in the field of electronics has raised the concerns about security. In embedded applications, implementing a full-fledged cryptographic environment would not be practical because of the constraints like security, power dissipation, area and cost. Due to these constraints, the focus is on using lightweight cryptography that needs as less memory space as possible. The standard algorithm like AES, DES have huge memory requirement and would not be feasible to be implemented for embedded system design. Lightweight cryptography is an interesting field which provides security, higher throughput, low power consumption and compactness. Several algorithms like PRESENT, CLEFIA, SEA, TEA, Hummingbird and KANTAN have made the mark to be used as lightweight algorithms. In this paper, we present the design of lightweight encryption system based on bit permutation instruction GRP (group operation). This design has resulted in most compact implementation in terms of memory requirement. They provide good resistance against most of the attacks because of confusion and diffusion property. GRP properties are very helpful to attain the compact implementation in hardware. The design is coded using VHDL language and the code is synthesized and simulated using XILINX ISE and ModelSim respectively.

Key Words: Lightweight cryptography, PRESENT, GRP, Encryption, Bit permutation.

I. INTRODUCTION
It is widely recognized that data security will play a central role in THE UPCOMING ERA of pervasive computing. In embedded applications, implementing a full-fledged cryptographic environment would not be practical because of the constraints like power dissipation, area and cost. Due to these constraints, the focus is on using lightweight cryptography that needs as less memory space as possible. The main criterion for the lightweight cipher is to have less memory space and that which would result into a less Gate Equivalent (GEs) count for an efficient hardware implementation without compromising the requirement of strong security.
In response, security solutions are being developed to provide robustness, protection from attacks, and recovery capabilities. In order to secure the devices, below form of security are deployed.
- Data transfer in an encrypted format.
- Securing the read only memory of the system.
- Creation of a secure digital signature.
- Creation of digital certificates.
- Creation of encrypted keys to send and accept data.

Security has been the subject of intensive research in the context of general purpose computing and communications systems. However, security is often misconstrued by embedded system designers as the addition of features, such as specific cryptographic algorithms and security protocols, to the system. In reality, it is a new dimension that designers should consider throughout the design process, along with other metrics such as cost, performance, security and power. The challenges unique to embedded systems require new approaches to security covering all aspects of embedded system design from architecture to implementation.

The implementation of cryptographic systems presents several requirements and challenges. First, the performance of the algorithms is often crucial. One needs encryption algorithms to run at the transmission rates of the communication links. Slow running cryptographic algorithms translate into consumer dissatisfaction and inconvenience. On the other hand, fast running encryption might mean high product costs since traditionally, higher speeds were achieved through custom hardware devices. Previous designs are focused on the performance and their configuration rules are usually complex. However, they may be difficult to meet the cost of resource-constrained systems. A new biometric algorithm has been developed and is Lightweight cryptography. Algorithm is an interesting field that strikes the perfect balance in providing security, higher throughput, low-power consumption, and compactness. Bit permutations are popularly known to be used in permutation block known as diffusion property. We have carefully studied the properties and security aspects of bit permutation instructions like GRP.

II. RELATED WORK
The increasing use of pervasive devices in the field of electronics has raised the concerns about security. In embedded applications, implementing a full-fledged cryptographic environment would not be practical because of the constraints like security, power dissipation, area and cost. Due to these constraints, the focus is on using lightweight cryptography. Cryptography is a method that has been developed for transferring data securely.

Cryptography now plays an increasingly important role in modern society, and it is essential to solve problems that involve secrecy, authentication, integrity, and dishonest entities. In digital communications, the data is sent through the wires or air and thus it is not from eavesdropping. Therefore, confidentiality of the transferring...
data is of extreme importance. Encryption is a process which transforms the data that is aimed to be sent to encrypted data using a key. The encryption process is not confidential but the key is only known to the sender and receiver of data. The receiver transforms the received data using the decryption process to obtain the original data. A modern information theory concept was first published by Claude Elwood Shannon in 1948. There are two basic types of encryption, symmetric and asymmetric encryption:

- Asymmetric encryption uses public key and symmetric encryption uses shared private key. Asymmetric ciphers have two keys, a public (shared) key, and a mathematical related private key.
- Symmetric key cryptography, which uses a shared key in both ends for encryption and decryption, has been utilized for secure communications for long period of time. Figure 2.1 shows the symmetric key cryptography.

Fig 2.1: Symmetric key cryptography

Symmetric key cryptography comprises two different methods for encryption and decryption. In the first method which is denoted as stream cipher, the bits of data are encrypted/decrypted one at a time. Transmission error in one cipher text block have effect on other block and difficult to implement correctly. However, in the second method which is called block cipher, blocks of the input data which consist of a number of bits are encrypted/decrypted. Transmission errors in one cipher text block have no effect on other block and easier to implement. Figure 2.2 shows the block cipher structure. It provides integrity, confidentiality and authentication. The Data Encryption Standard (DES), triple DES (3DES) and the Advanced Encryption Standard (AES) are examples for the block cipher symmetric key cryptography.

Fig 2.2: Block cipher structure

PRESENT

PRESENT is a substitution and permutation network with 64-bit iterated block cipher. PRESENT was designed to allow fast and compact implementation in hardware and software. PRESENT structure is Substitution and Permutation (SP) design which consists of S and P layer and consists of 31 rounds. S-box of PRESENT is resistant to brute force attack. PRESENT, like any other SPN, comprises three stages: a key-mixing step, a substitution layer, and a permutation layer. For the key mixing, choose a simple XOR because this operation can be implemented efficiently in both hardware and software. The key is 128 bit. The substitution layer comprises 30 S-boxes with 128 bit input and 128 bit output. Through the careful selection of s-box, its possible to achieve high security level. The permutation layer (P-layer) is a very regular and group instruction operation is performed. The output from P-layer is xored with key and given to s-box as the input.

III. SYSTEM ANALYSIS

3.1 PROPOSED SYSTEM

As we discussed above, this study is based on cryptography, we provide suitable modifications to those designs, to make the proposed system. Here, S-box of PRESENT algorithm is removed and provide GRP permutation mechanism. Algorithm focused is to implement lightweight design to avoid high power dissipation and large memory requirement. To provide a high security and low cost, there is need to have a lightweight crypto algorithm whose coverage area would be less. The standard algorithm like AES, DES have huge memory requirement and would not be feasible to be implemented for embedded system design. Many lightweight algorithms have been designed in the past and various attacks have been proven on them. PRESENT algorithm is ISO/IEC standardized. The aim of this work is to provide adequate security for the digital systems. The lightweight cryptography is a biometric algorithm combination of PRESENT algorithm with group instruction permutation. The developed algorithm is highly secured and need only less area when compared with Advanced Encryption Standard.

3.2 PROPOSED ENCRYPTION AND DECRYPTION SYSTEM

Fig 3.2, 128 bit encryption using GRP

In this section, the detail of the proposed encryption system is provided. Figure above illustrates the general block diagram of the proposed system which is comprised of PLayer where GRP permutation is performed. The general block diagram of the proposed system comprises of two main modules:

1. Player – Basically where GRP permutation is performed
2. Key register-where key is generated for each round is stored

3.3 OVERVIEW OF THE GRP: A BIT PERMUTATION INSTRUCTION

GRP is one of the most complicated bit permutation instructions that make it an obvious choice to be used in cryptographic environment. GRP performs a bit permutation with \( \log_2(n) \) steps while other instructions take \( O(n) \) steps. The basic idea of the GRP instruction is to divide the bits in
the source R1 into two groups according to the bits in R2. For each bit in R1, we check the corresponding bit in R2. If the bit in R2 is 0, we put this bit in R1 into the first group. Otherwise we put this bit in R1 into the second group. During this process we do not change the relative positions of bits in the same group. Finally, putting the first group to the left of the second group, we get the result value in R3. From the position of two groups, we call the first the left group, and the second the right group. Figure 3.3 shows how the GRP instruction works on 8-bit systems.

IV. METHODOLOGY

In this section, a detailed description of the hardware architecture of the proposed encryption system is provided. Fig.4.4.1 illustrates the general block diagram of the proposed system that is comprised of two main modules: P-LAYER and KEY REGISTER.

4.1 PLAYER

In P-layer group instruction operation (GRP) is performed. GRP algorithm can generate different values from a given integer sequence. In this project, 128 bit encryption and decryption is designed and P-layer operation is performed based on bit permutation instruction.

Fig. 3.3 GRP instruction on 8-bit systems

Fig 3.3: Movement of bit S(i) to P(i)

The figure 4.1.2 shows the group instruction operation of a 8 bit in P-layer. It is a universal design which generates code words for n integers.
Fig 5.1: Simulation result of lightweight encryption algorithm

5.2 LIGHTWEIGHT DECRYPTION ALGORITHM
The operation is same as encryption. Here the input will be given as the value obtained from the encryption and the key value is same as used in the encryption algorithm since its a symmetric key cryptography. The plain text of 128 bit value is obtained. Figure 7.5 shows the simulation result of lightweight decryption algorithm.

Fig 5.2: Simulation result of lightweight decryption algorithm

5.3 GATE COUNT RESULT OF LIGHTWEIGHT ALGORITHM
The total gate utilized in Lightweight algorithm is shown in Figure 7.6.

VII. CONCLUSION
In this work, the design and implementation of a high security, less area and low cost is achieved. The increasing use of electronic device has raised concerns about security. The bit permutation is the process of generating values at different rounds from given integer sequence. This fusion structure results into a novel approach by introducing a compact hybrid system in terms of security and memory requirements that is best suited for lightweight cryptographic design. The comparative study of AES and Lightweight cryptographic algorithm proves lightweight cryptography more suitable for security based embedded applications. Bit permutation instructions increases strength of a block cipher by allowing them to perform any arbitrary permutations efficiently with ‘log(n)’ steps as compared to ‘n’. It performs fast bit permutation and uses subword sorter that makes the operation faster and can increase the throughput in applications like scanning an image, performing bubble sort and in the permutations layer in block ciphers. GRP generates the control words faster, that which helps in increasing the performance of many embedded systems. Block ciphers like RC5, RC6 use DDR instructions which make them vulnerable to differential attacks. This further increases the number of rounds and memory requirements. But, by replacing DDR with GRP not only adds cryptographic strength to the cipher, but also reduces the memory requirements and the power consumption. GRPs have better differential and linear cryptanalysis properties. Though they cannot completely replace DDR, but they add strength to the block cipher by removing the weaknesses of DDR. GRP have all these good properties that provide strength in cryptographic environment. Key generation is also achieved through GRP. For designing a lightweight secure cipher, a confusion property is a must and it should be well mapped with the diffusion property. The proposed system was suitable for implementation using an FPGA and can be used as a part of an ASIC. In the current implementation, FPGA was the simple and available way of the proof of concept. The aim of this project was to achieve the objectives. high security, less area and low cost This paper proposes a novel approach by introducing compact hybrid system in terms of memory requirements that is best suited for lightweight cryptographic design.

VII. REFERENCES


