DESIGNING A CRYPTOGRAPHIC ALGORITHMS FOR ENCRYPTING & DECRYPTING THE DATA

S.HASMA SHRUTHI[1], R.DEEPAK[2] A.SINDHU[3], PRASANTH[4],

[1]*Department of Electronics and communication Engineering, Assistant professor, ,SNS College of Technology, Autonomous, Coimbatore, India.*
E-mail: shruthiji06@gmail.com.
[2]*Department of Electrical & Electronics Engineering, SNS College of Technology, Autonomous, Coimbatore, India,*
E-mail: deepakramesh006@gmail.com
[3]*Department of Electronics and communication Engineering, Assistant professor, ,SNS College of Technology, Autonomous, Coimbatore, India.*
E-mail: sindhuaruchamy@gmail.com.
[4]*Department of Electronics and communication Engineerin, ,SNS College of Technology, Autonomous, Coimbatore, India.*
E-mail: ursfriendprasanth@gmail.com

Abstract

Lightweight encryption is an interesting field that strikes the perfect balance in providing security, low-power consumption, and compactness. In this paper, we present the design of a lightweight encryption based on the grouping permutation(GRP).In the s-box we have added the confusion property for GRP.The existing S boxes with DESXL, CLEFIA, and AES algorithms are compared and a new lightweight encryption system is proposed in this paper that provides compact results which reduces gates and memory size.GRP not only adds strength to the cipher it also reduces the power consumption and memeory requirements.By using the S box of PRESENT the gate complexity is reduced.A lightweight S box that can be mapped into the GRP to have efficient cryptographic structure and to strengthen the security.

Keywords—***Lightweight cryptography, PRESENT, GRP,embedded security, encryption, bit permutation.***

I. INTRODUCTION

The use of pervasive devices in the field of electronics has raised the concerns about security. The main criterion for the lightweight cipher is to have less memory space and that which would result into a less Gate Equivalent count. In the security environment, there are two types of instructions, one is the "SP-network" Substitution Permutation network like AES, PRESENT, etc. and other is the"Feistel network". Feistel structure with a substitution box. The disadvantage of generalized Feistel structure is that it requires larger number of rounds to make the cipher secure. In the GRP the results of a design of a cipher with adequate security for applications like pervasive computing. Block ciphers should be limited to less GEs in order to fit in lightweight applications.

Ciphers like AES [3], DES [4] would result in high GEs that make them infeasible for small scale real time applications. Light variants of DES such as DESL [6] have been proposed by slightly modifying the algorithms, by reducing the S-boxes and by using key whitening to increase security levels.Alternative to this approach of modifying an existing block cipher and to have an efficient hardware model, is an entirely new structure that has been designed called "PRESENT." PRESENT is a Substitution Permutation network based on 80 bit or 128 bit key size and 64 bit block size.

PRESENT [8] is a block cipher with 31 rounds and its various variants need 2520 to 3010 GEs to provide adequate security levels. CLEFIA [9], [10] is one more compact algorithm GEs and has two confusion and two diffusion properties that results in a higher memory requirement. In the cryptographic environment, there are two types of instructions, one is the "SP-network" (Substitution Permutation network) like AES, PRESENT, etc. and other is the "Feistel network" like TEA, XTEA, etc. In this paper, we have focused on SP-network only, as they provide good resistance against most of the attacks. Stream ciphers are also widely studied in the cryptographic environment because of its faster execution, but they are susceptible to attacks compared to SP network block ciphers. CLEFIA [9], is a generalized Feistel structure with a substitution box.

The aim of this paper is to describe the results of a design of a compact cipher with adequate security for applications like pervasive computing. They are complex in nature which gives them an edge in cryptographic environment. Bit permutations are popularly known to be used in permutation block known as diffusion property. Among all bit permutation instruction GRP proved to be an efficient instruction in terms of cryptographic properties, memory size and total number of gate counts. Bit permutation instructions are widely studied and currently supported by all word oriented processors. GRP is an extensively researched instruction set, its cryptanalysis is well known, and many attacks have been tried in the past on bit permutation instructions. GRP is known for fast bit permutation. GRP is complex in nature that makes it more suitable for cryptographic environment as compared to operations like shifting, multiply or addition. GRP is suitable specifically for encryption in an application like remote sensor continuously encrypting data and sending it to a server location [9]. Moreover, GRP has good differential properties because the paths of data bits totally depends on control bits applied to the structure. Change of even a single control bit will cause all the data bits to change at the output [5]. This property helps to achieve desired avalanche effect and makes design more robust against attacks.

Algorithms like DES [4], [5], SERPENT [14] and TWO FISH [9] use bit permutation instructions in their operations which helps to resist against linear and differential cryptanalysis. Bit permutation instructions lack confusion property that is an S-box. According to Shannon having only the diffusion property is not sufficient to provide a secure cipher [2]. GRP uses sub word permutation that not only does permutation efficiently but also accelerates the software cryptography [6].

The rest of the paper is organized as follows. Section II discusses about GRP Algorithm which is a universal design which generates code word for n integers. Section III discusses about Lightweight Cryptography in which GRP key generation, inputs is given by user, and based on that GRP generates a sequence of 0's and 1's which serve as key to the encryption and decryption process. Section IV discusses about GRP: A New Hybrid Lightweight Design Bit permutation instructions increases strength of a block cipher.

It performs fast bit permutation and uses sub word sorter that makes the operation faster and can increase the throughput .Section V. Result And Discussion for 128 bit permutation and finally encrypted the data. Finally the conclusion is drawn in Section VI.

II.GRP ALGORITHM

By providing integer sequence GRP algorithm generates the different keys at different rounds where the user has to give an 128 bit input and GRP performs the exact same operations for 128 bits which is performed for an 8 bit encryption the basic GRP encryption operations in terms of AND, OR and NOT gates. key register generates the key according to GRP algorithm that is based on the user defined integer sequence and that key is applied as code word to each of the permutations to do the encryption.

The algorithm and the steps involved while deigning permutation box by using GRP .In a scenario, let us assume that the input is a plain text with a bit length w = 128 that needs to be permuted with the help of GRP. To permute 128 bits, the operation needs total 7 stages as 2^7 = 128 bits. 7 stages means GRP 128 will perform up to 7 rounds as 27 = 128.Similarly, for 64 bit and 8 bit permutations, we need total of 6 and 3 stages ,respectively. w indicates word length and n indicates number of stages, where 2n = w.P = w/2 indicates pairing bits in which if word length is 128 bits then P value will be 64 which depicts in the first stage of permuting 128 bits, first group is the 0th bit and 64th bit second will be 1st and 65th bit, third group will be 2nd and 66th bit and similarly last will be 63rd and 127th bit.

C represents combination of pairing bits. For example, for P = 64, C value will be 1, for second stage where P = 32, C value will be 2 and for last stage P = 1, C value will be 64 which means we will be having 64 combinations of single pair.

By providing integer sequence GRP algorithm generates the different keys at different rounds . Key generation for respective integer sequence is illustrated with an example in paper [8]. where the user provides an 128 bit inputs and Grouping permutation performs the same operations for 128 bits which is performed for an 8 bitin Fig. 1. It is a universal design which generates code word for n integers. Fig. 1 indicates the basic GRP encryption operations in terms of AND, OR and NOT gates.In Fig. 1, key register generates the key according to GRP algorithm [6], that is based on the user defined integer sequence The algorithm and the steps involved while deigning permutation box by using GRP are outlined in Fig. 1.

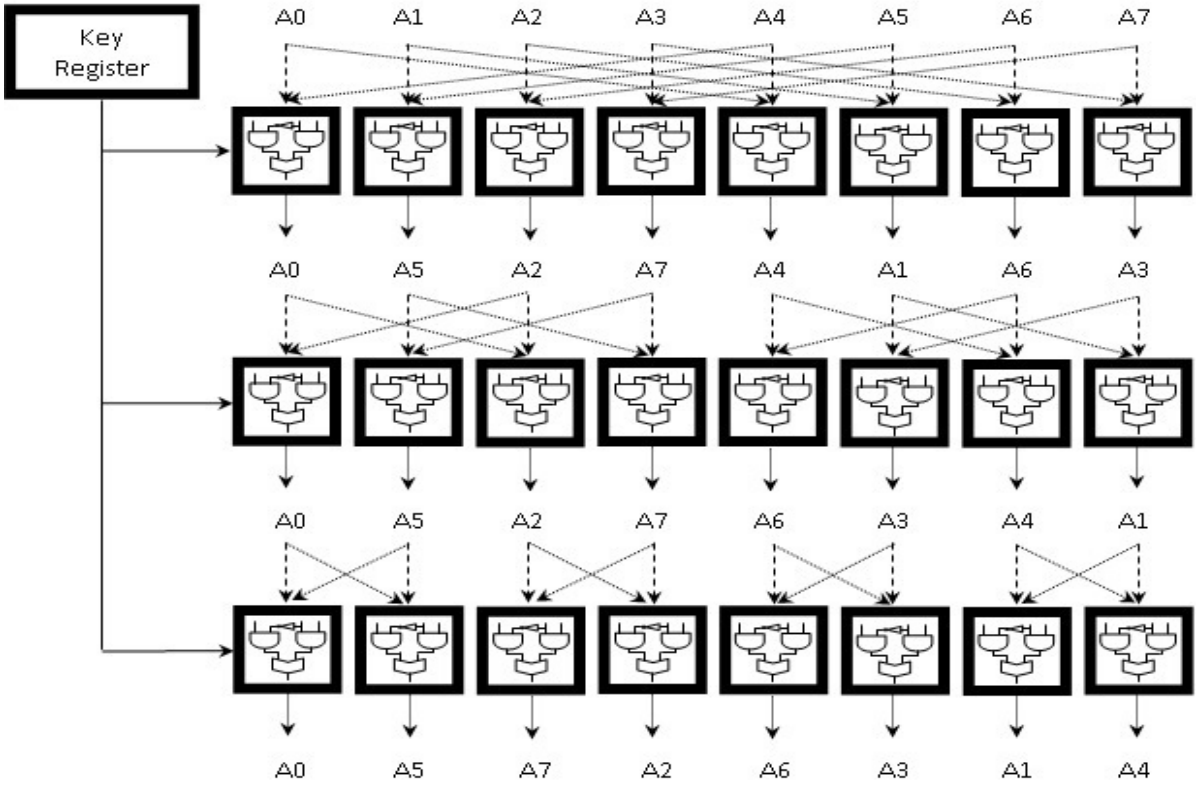


Fig. 1. GRP implementing encryption for 8 bi

III. LIGHTWEIGHT CRYPTOGRAPHY

Internet of things (IOT) is one of the most discussed topics today in the digital world.Focus area of researchers is to implement lightweight design to avoid high power dissipation and large memory requirement.

RFID tag is one of the fast growing technologies that would be useful for IOT [1], [3]. To provide a security at RFID level, there is need to have a lightweight crypto algorithm whose coverage area would be nearly 2100 GE. The standard algorithm like AES [3], DES [4], [5] 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.

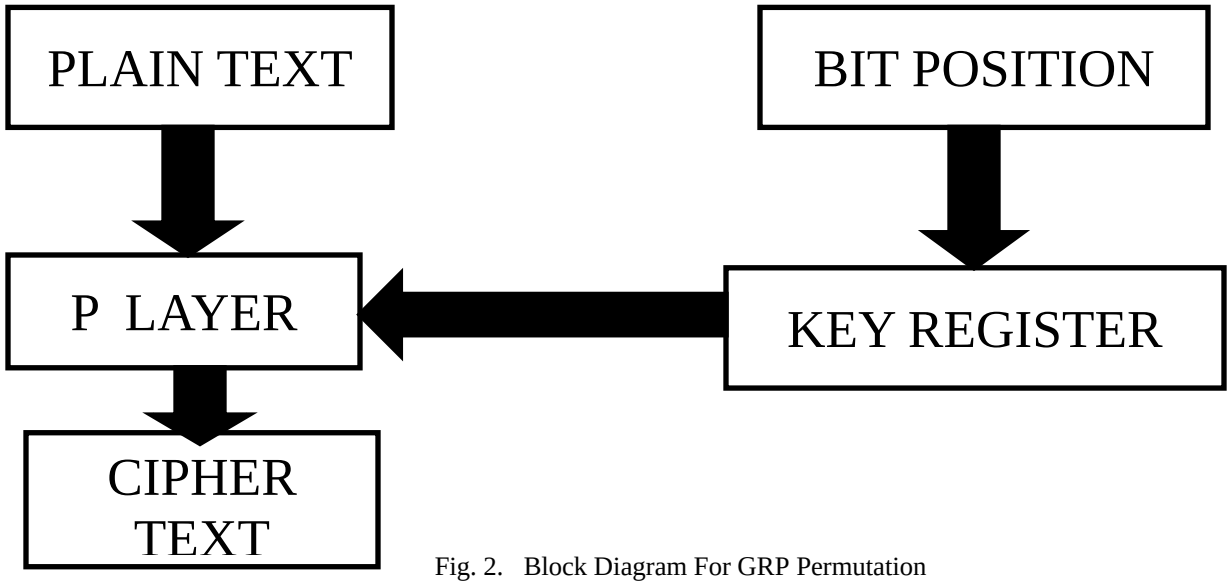


Fig. 2. Block Diagram For GRP Permutation

In GRP module, 64 bit/128 bit blocks were passed through the S-box of PRESENT and after mapping according to PRESENT, the output was passed to the permutation layer which performed encryption based on GRP algorithms. Keys at each stage were applied based on key generation method of GRP. In GRP key generation, inputs will be the bit positions given by user, and based on that

GRP generates a sequence of 0's and 1's which serve as key to the encryption and decryption process. Grouping permutation has very robust mechanism for generation of key which is the necessity in cryptographic environment. GRP does the key generation as well as encryption with fast bit permutations.

IV.PRESENT-GRP: A NEW HYBRID LIGHTWEIGHT DESIGN

The hybrid structure of PRESENT-GRP has very less memory requirement as compared to the other algorithms. Bit permutation instructions increases strength of a block cipher.

It performs fast bit permutation and uses sub word 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. GRP have all these good properties that provide strength in security environment. But, it lacks S-box which is necessary to provide a more secure design.

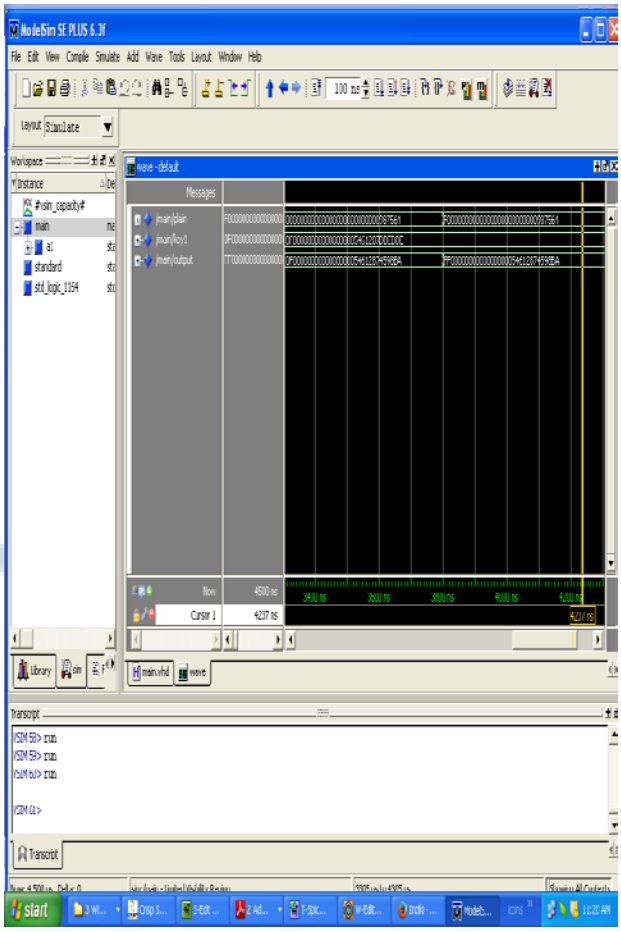
This shifted our focus to find a light weighted S-box that can be mapped onto GRP to get a secure and efficient hybrid crypto structure.

In order to achieve a very compact implementation of cipher, we have carefully designed the permutation box that has resulted in a much lower gate count. key generation by GRP achieving tremendous speed because most of the permutation instructions exist in this block. 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.

Moreover, GRP properties are very helpful to have less memory Space. In the GRP the results of a design of a compact cipher with adequate security for applications like pervasive computing.

GRP have all these good properties that provide strength in security environment

V.RESULT AND DISCUSSION



VI. CONCLUSION

Bit permutation instructions increases strength of a block cipher. GRP not only adds cryptographic strength to the cipher, but also reduces the memory requirements and the power consumption. Other ciphers like hash functions and stream ciphers may get benefited by one introducing the bit permutation instructions in them. GRP have all these good properties that provide strength in cryptographic environment. But, it lacks S-box which is necessary to provide a more secure design. This shifted our focus to find a light weighted S-box that can be mapped onto GRP to get a secure and efficient hybrid crypto structure.

VII.REFERENCES

[1] K. Finkenzeller, RFID Handbook: Fundamentals and Applications inContactless Smart Cards and Identification. Hoboken, NJ, USA: Wiley,2003.

[2] A. Juels and S. A. Weis, "Authenticating pervasive devices with human protocols," in Advances in Cryptology. Berlin Germany: Springer-Verlag,2005, pp. 293–308.

[3] National Institute of Standards and Technology (NIST). (Nov. 26, 2001).Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197. [Online]. Available: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[4] National Institute of Standards and Technology (NIST).(Dec. 30, 1993). Data Encryption Standard (DES), FederalInformation Processing Standards Publication 46-2. [Online]. Available:

[5] National Institute of Standards and Technology (NIST). (October25, 1999). Data Encryption Standard (DES), Federal InformationProcessing Standards Publication 46-3.

[6] A. Poschmann, G. Leander, K. Schramm, and C. Paar, "New light-weight crypto algorithms for RFID," in Proc. IEEE Int. Symp. Circuits Syst.(ISCAS), May 2007, pp. 1843–1846.

[7] T. Eisenbarth and S. Kumar, "A survey of lightweight-cryptography implementations," IEEE Des. Test. Comput., vol. 24, no. 6, pp. 522–533, Nov./Dec. 2007.

[8] A. Bogdanov et al., "PRESENT—An ultra-lightweight block cipher,"in Cryptographic Hardware and Embedded Systems (Lecture Notes in Computer Science), vol. 4727, P. Paillier and I. Verbauwhede, Eds.Berlin, Germany: Springer-Verlag, 2007, pp. 450–466.

[9] T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata, "The 128 bit in Fast Software Encryption (Lecture Notes in Computer Science), vol. 4593, A. Biryukov, Ed. Berlin, Germany: Springer-Verlag, 2007, pp. 181–195.

[10] The 128 Bit Blockcipher CLEFIA: Algorithm Specification, Sony Corporation, Tokyo, Japan, 2007.

[11] D. Hong et al., "HIGHT: A new block cipher suitable for low-resource device," in Cryptographic Hardware and Embedded Systems (Lecture Notes in Computer Science), vol. 4249, L. Goubin and M. Matsui, Eds.Berlin, Germany: Springer-Verlag, 2006, pp. 46–59.

[12] L. Brown, J. Pieprzyk, and J. Seberry, "LOKI—A cryptographic primitive for authentication and secrecy applications," in Advances in Cryptology (Lecture Notes in Computer Science), vol. 453,J. Pieprzyk and J. Seberry, Eds. Berlin, Germany: Springer-Verlag, 1990,pp. 229–236.

[13] F.-X. Standaert, G. Piret, N. Gershenfeld, and J.-J. Quisquater, "SEA: A scalable encryption algorithm for small embedded applications," in Smart Card Research and Applications (Lecture Notes in ComputerScience), vol. 3928, J. Domingo-Ferrer, J. Posegga, and D. Schreckling,Eds. Berlin, Germany: Springer-Verlag, 2006, pp. 222–236.

[14] D. J. Wheeler and R. M. Needham, "TEA, a tiny encryption algorithm,"in Fast Software Encryption (Lecture Notes in Computer Science),vol. 1008, B. Preneel, Ed. Berlin, Germany: Springer-Verlag, 1994,pp. 363–366.

[15] F.-X. Standaert, G. Piret, G. Rouvroy, J.-J. Quisquater, and J.-D. Legat,"ICEBERG : An involutional cipher efficient for block encryption in reconfigurable hardware," in Fast Software Encryption, B. Roy and W. Meier, Eds. Berlin, Germany: Springer-Verlag, 2004.