DESIGN AND IMPLEMENTATION OF "PRESENT BLOCK CIPHER ALGORITHM"

*1 Anil G. Sawant, 2 Dr. Anupama Deshpande, 3 Madhuri Daunde, 4 Komal Ghadage, 5 Rasika Pilane
*1 Research Scholar (Asst. Professor) , 2 Professor, 3 Student, 4 Student, 5 Student
*1 JJT University, Rajasthan, India (Trinity College of Engineering and Research, Pune), 2 JJT University, Rajasthan, India, 3 Trinity College of Engineering and Research, Pune 4 Trinity College of Engineering and Research, Pune 5 Trinity College of Engineering and Research, Pune.
Email: * anilsawant.22@gmail.com, madhuridaunde73@gmail.com, ghadagekomal1997@gmail.com, pilanerasika11@gmail.com

Abstract **-** Due to the vast development of information technology, it is very necessary to protect the sensitive information via encryption and decryption which is becoming more and more important in daily life. Cryptographic operation in devices which use little memory and a low power processor causes system overhead. Thereby implementing cryptographic operation is necessary nowadays. Today increases any wireless communication security is crucial during data transmission. for encryption and decryption of data we use "PRESENT BLOCK CIPHER ALGORITHM "algorithm to enhance the security in FPGA by creating a module dedicated for encrypting the data transmitted by FPGA. Once the connection is established between two machines then the encrypted message is sent from the transmitter to receiver and output is observed. The algorithm "PRESENT" is a block cipher lightweight algorithm of reduced size and execution It uses substitution and permutation blocks of only 4 bits also the key size is small as compared to other algorithms. It uses a block size of 64 bits and the key size is 80 bits or 128 bits. In total, the number of rounds for a PRESENT block cipher is 31.The project presents a security which can be used by ATM, Smart TV ,WiFi, smart phone. Now days security is very important so we design present algorithm.The project presents a security which can be PRESENT is a block cipher algorithm lightweight type highly used since it has easy implementation in both hardware and software . Its implementation in hardware can be done in some of the smallest FPGA's on the market.

Keywords- Cryptography, Block Cipher, Lightweight Algorithm.

INTRODUCTION:

In today's communication network, data is required to travel safely giving a minimum throughput. For this purpose, the algori thm must have efficient hardware and software implementation[1]. Because of this reason, a versatile encryption algorithm is applied which is flexible with low use of resources and which is easy to implement regarding hardware and software. PRESENT is a lightweight algorithm[2]. The algorithm "PRESENT" is a block cipher lightweight algorithm of reduced size and execution[3]. It uses substitution and permutation blocks of only 4 bits also the key size is small as compared to other algorithms[4]. It uses a block size of 64 bits and the key size is 80 bits or 128 bits. In total, the number of rounds for a PRESENT block cipher is 32.Cryptography can be described as a set of techniques to encode information[5]. The main purpose of encryption is to protect the information contained in a document and it becomes unreadable after this process. To revert the information contained in the document, a reverse process called decrypt is required. Encryption techniques may be described by algorithms, which makes it feasible implementation by computers[6]. Over time, several different methods have been developed in order to make it difficult to decode encrypted files. Currently there are some methods that require a password to retrieve information, such as asymmetric key algorithms, for example. Other methods, such as hash functions, do not allow the decryption of once encrypted content, serving as digital signature of files. The new evolution of cryptography can be explained by the development of computing. Most of the widespread in modern world, computing has become ubiquitous and is present in the daily lives of most people. A simple example of the importance of encryption in the world today is the growing use of smart phones for banking transactions. If their was no safe ways to protect the information entered on banking applications, invasions to accounts of thousands of people would be easily seen.

Cryptographic algorithms like RSA, ECC and AES are not suitable for all currently devices[7]. Most of their operation based on battery, which requires a low consumption by the algorithm[9]. Others have a low capacity and may not support keys over 128 bits, as is common in most asymmetric algorithms. Different approach necessary for these devices the use of lightweight cryptographic algorithms[10]. The basic features for a lightweight cryptographic algorithm is to meet the limitations of the devices for which it was designed, without losing the security focus[11]. There are limitations in relation to classic algorithms, the lightweight cryptography must match the classical in terms of functionality and safety[12].

METHODOLOGY:

Block Cipher: In this type of encryption, the information is organized in blocks of fixed size, performing operations that try to eliminate the possible relationships between the encrypted text and the original message[1]. In all of the block ciphers a combination of operations is generated by: ByteSub, ShiftRow, MixColum and AddRoundKey; these combinations are called round. The complexity of the algorithm depends upon the combination of these operations and rounds performed along with the size of the key used.

Present block cipher algorithm:

To protect our information, it is necessary to choose a scheme in which how the information will be a cipher, how the secret key is shared and which type of cryptography scheme is used? There are two types of cryptography scheme such as symmetric cryptography and asymmetric cryptography. In this algorithm, we have chosen symmetric cryptography scheme in which only one key called "secret key" is used known by sender and receiver. In this type of encryption, the information is organized in the blocks of fixed size, regardless of the place, it occupies in the binary chain so that all the bits of the block are coded together and performing operations that try to eliminate the possible relationships between encrypted text and the original message[2].

PRESENT ALGORITHM STRUCTURE:

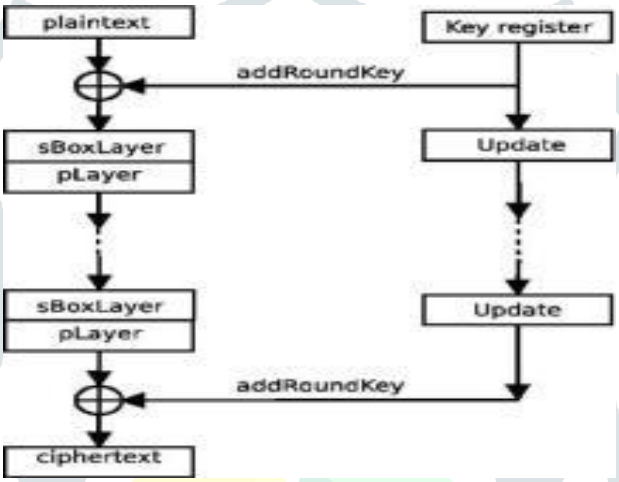

Figure 1 : Structure of Present Algorithm

The operation of each of the layers of the algorithm is:

Add Round Key:

The Add Round Key operation is a simple EXOR operation between the State and the Round Key. The Round Key is defined from the Cipher key by means of the key schedule. The State and Round Key are of the same size and to obtain the next State an EXOR operation is done per element:

$$s(I, J) = x(I, J) \text{ xor } w(I, J)$$

where s is the current State, s the next State and w the round key.

Byte substitution layer: It consists of a non-linear substitution that is applied independently to each nibble of the state matrix. Thissubstitution block is applied to 16 nibbles that complete 64 bits of information, which is the standard size of the cipher blocks.

Table 2: s box

Y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S(Y)	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

Bit Permutation (p Layer): It is a layer that mixes by means of a bitwise substitution block of information of 64 bits, where the "I"bit of the round is moved to the position P(I).

Table 1: P layer substitution table.

I	P(i)	I	P(i)	I	P(i)	I	P(i)
0	0	16	4	32	8	48	12
1	16	17	20	33	24	49	28
2	32	18	36	34	40	50	44
3	48	19	52	35	56	51	60
4	1	20	5	36	9	52	13
5	17	21	21	37	25	53	29
6	33	22	37	38	41	54	45
7	49	23	53	39	57	55	61
8	2	24	6	40	10	56	14
9	18	25	22	41	20	57	30
10	34	26	38	42	42	58	46
11	50	27	54	43	58	59	62
12	3	28	7	44	11	60	15
13	19	29	23	45	27	61	31
14	35	30	39	46	43	62	47
15	51	31	55	47	59	63	63

Key expansion function (add Round Key):

PRESENT can have keys of 80 or 128 bits in length, but for this design and implementation only a key of 80 bits will be taken into the account, which will be stored in a K register of that size and will be listed K_{79} K_{78} .... K_{0}. But in each round, only the 64 most significant bits of the new calculated key will be mixed up after applying the key expansion function.

Technical Background:

Two categories of cryptographic algorithms are the block cipher and stream cipher. The former groups the information to be encrypted into blocks from 8 to 16 bytes before the encryption process and then encrypts the whole block. The latter encrypts text one bit at time by using the logical xor operation between the input and the key. A key is a unique string that is used to encrypt and/or decrypt a file.symmetric and asymmetric are the two classes of algorithms with respect to the key. Symmetric algorithms use only one key for encryption and decryption of the input, which is a private key that must be distributed among all parties involved in the communication. Public and Private are the two keys in the asymmetric cryptography. Where as one is used to encrypt, other is able to restore the information and vice-versa. A lightweight encryption application is its possible use in Radio Frequency Identification (RFID) technology, an automatic identification method using radio signals. RFID tags generally have high limitations of computational resources, such as those listed by Saarinen and Engels in The total integrated circuit area available for implementing the entire device's logic, including the security, is reduced. The power depends on the device's clock frequency. Thus, security implementations need to reduce the use of clock cycles. The lightweight cryptography is noted by Katagi and Moriai lightweight cryptographic algorithms meet precisely the restrictions lifted by Saarinen and Engels [4]. Especially algorithms designed to hardware fit this case: low power consumption and small footprint, which leads to interest in implementing such algorithms in VHDL.

SECURITY DISCUSSION:

The cryptanalysis is useful factor for the security of the algorithm. As it was mentioned before ,the S-box is an important part and the heart of the algorithm. To measure the security of algorithm, this is done by using the cryptanalysis. Most of then attacks are linear and differential cryptanalysis. These attacks are the basic of all other attacks. In the proposed algorithm, in each round there is adifferent S-box and it chooses one S-box by XORING between all elements of key. We will analyse the proposed algorithm against differential and linear cryptanalysis.Each S-box has 16 values and to know which value is used, there are 16 (24) possibilities. For the PRESENT lightweight algorithm, the total possibilities for all S-boxes in each round are 24*16=24*24=28. While the total possibilities for all S-boxes of the proposed algorithm in each round are 28*16=28*24=212. We therefore, can conclude that the attackers need more time to recover the key for the proposed algorithm comparing with the PRESENT algorithm.

CONCLUSION:

PRESENT- block cipher is an ultra-lightweight algorithm with one of the confused encryption methods. Because of these characteristics, it is used in applications of low power consumption. It's performance on different lavels was studied, with the intention of finding ideal conditions for high performance applications. In this paper we implement the new block cipher present. Our target is an ultra-lightweight cipher that offers a level of security commensurate with a 64-bit block size and an 80-bit key.

REFERENCES:

[1] T. Eisenbarth and S. Kumar, "A Survey of Lightweight-Cryptography Implementations," IEEE Des Test Compute, vol. 24, no. 6, pp. 522–533, 2007

[2] J. Pospiil and M. Novotny, "Evaluating Cryptanalytical Strength of Lightweight Cipher PRESENT on Reconfigurable Hardware," in Digital System Design (DSD), 2012 15th Euromicro Conference on, 2012, pp. 560–567.

[3] Bogdanov et al., "PRESENT : An Ultra- Lightweight Block Cipher," Springer Berlin Heidelb., pp. 450–466, 2007 J.

[4] Attrite, "An Overview of Hardware Security Modules," SANS Institute, InfoSec Read. Room, vol. 1, no. 1, pp. 1–10, 2002.[5] Daniel, D.; Le Corre, Y.; Khovratovich, D.; Perrin, L.; Grobschadl, J.; Biryukov, A. Triathlon of Lightweight

[6] Bansod, G.; Raval, N.; Pisharoty, N. Implementation of a new lightweight encryption design for embedded security. IEEE Trans. Inf. Forensics Secur. 2015, 10, 142–151

[7] J. Pospiil and M. Novotny, Evaluating cryptanalytical strength of lightweight cipher PRESENT on reconfigurable hardware, 2012 15th Euromicro Conference on Digital System Design (DSD), (2012), 560–567. https://doi.org/10.1109/dsd.2012.53

[8] N. Pineda and N. Velásquez, Diseño e Implementación de un Prototipo Criptoprocesador AES-Rijndael en FPGA, Universidad de los Llanos, Colombia, (2007).

[9] J. Attridge, An overview of hardware security modules, SANS Institute InfoSec Read Room, 1 (2002), 1–10.

[10] Aysu, E. Gulcan, P. Schaumont, SIMON says: Break area records of block ciphers on FPGAs, IEEE Embed Syst Lett., 6 (2014), 37–40. https://doi.org/10.1109/les.2014.2314961

[11] Delgadillo, M. Guerrero and N. Pena, Diseno de un criptosistema para redes de sensores inalambricos WSN basado en MPSOC, Universidad de los Andes, (2008).

[12] F. M. Qatan and I. W. Damaj, "High-speed KATAN ciphers on-a-chip," in Computer Systems and Industrial Informatics (ICCSII), 2012 International Conference on, 2012, pp. 1–6.

[13] W. Wu and L. Zhang, "LBlock: A Lightweight Block Cipher Applied Cryptography and Network Security." G. Leander and A. Poschmann, "On the Classification of 4 Bit S-Boxes Arithmetic of Finite Fields.

[14] B. Liu, Z. Gong, W. Qiu, and D. Zheng, "On theSecurity of 4-Bit Involutive S-Boxes for LightweightDesigns Information Security Practice and Experience." vol. 6672, F. Bao and J. Weng, Eds., ed:Springer Berlin / Heidelberg, 2011, pp. 247-256.