To Cryptanalyse PRESENT Lightweight Block Cipher using Zero Correlation Linear Cryptanalysis

[1]Mehak Khurana, [2]Meena Kumari
[1]Assistant Professor, [2]Professor,
[1,2]Dept of Computer Science and Engineering
The NorthCap University, Gurgaon, Haryana, India

***Abstract*— Block cipher is in vogue due to its requirement for integrity, confidentiality and authentication. With the rapid advances in small devices, such as Sensors, RFID tags, sensor nodes, medical devices are being deployed at a fast pace. These devices are being used in various applications which lead to requirement of providing security. Resource-limited devices and its implementation cost should be kept in mind when designing a algorithm. In order to satisfy these need, secure and efficient encryption and authentication schemes have to be developed. Symmetric-key algorithms are still used to provide confidentiality in the above mentioned applications. In this paper, the need of lightweight block cipher has been discussed and what all primitives are required to maintain balance between security, size, cost and other factors are illustrated. In this paper study of security and weakness are discussed. It also shows how this Zero correlation linear cryptanalytic technique can be applied to PRESENT Lightweight Block Cipher. For this, the code has been implemented which uses miss in middle technique and finds all the paths with zero correlation with fixed input and output where no other path exist with other exist for same input and output.**

***Index Terms*— Lightweight block cipher, PRESENT, Zero correlation, cryptanalysis**

I. INTRODUCTION (HEADING 1)

Cryptography is the ways to protect and secure the information with confidentiality, integrity and authentication. Cryptography has been associated with high performance computing. But devices that stores and transmits information bring a security challenge as they have high level resource constraint according to the needs of earlier cryptographic primitives [1]. Nowadays the main aim and focus of the designer is on the designing new cryptographic algorithms or primitives that are well suited according to the resource available with some constrains. This research area is termed as lightweight cryptography. This paper summarizes the latest design requirements in lightweight block ciphers [2]. It also discusses the latest designed lightweight block ciphers. This paper demonstrates various criteria that are required for evaluation of lightweight cryptography. The main aim is to analyse and crypt-analyse the security of the lightweight block cipher and what all characteristics of the round function put an impact on the security of these cipher. It focuses on recently designed ciphers e.g. PRESENT. This paper shows how many no. of rounds that can be attacked by Zero Correlation linear cryptanalysis which uses miss in middle technique [3-4]. It shows the middle point of the PRESENT block cipher which can be extended to attack these many number of rounds. Paper also presents various properties and analyse the structure of other lightweight ciphers. The goals of the paper are summarized below into three main objectives:

1. Study the designing techniques of lightweight block cipher.
2. Cryptanalysis of lightweight block cipher's structure and to implement Zero Correlation Linear attack [4-7]
3. To propose the solution to prevent the cipher from the attack.

The goal is to achieve these objectives by using analytical and practical methods mainly through python programming.

1.1 Scope of Paper

In paper first part focuses on the designing principles of the lightweight block ciphers. It discusses the different design strategies that have been employed for designing a lightweight block cipher. It also highlights issues in designing lightweight cryptographic algorithm.

The second part of the paper explains the crypt-analysis of the PRESENT block cipher. The main focus here is to find weakness in various recently proposed lightweight ciphers. The latest variant of Linear Cryptanalysis called Zero Correlation Linear Cryptanalysis [8-14] has been implemented on Lightweight block cipher to find the breakpoint and number of rounds the cipher can be attacked. Success in breaking these ciphers has not been obtained, but there are some properties of the cipher and the key schedule which can be and have been used to attack the cipher. This paper includes the finding of these properties.

II. LIGHTWEIGHT BLOCK CIPHER

2.1 NEED FOR LIGHTWEIGHT CRYPTOGRAPHY

Devices, such as RFIDs and sensor nodes contain sensitive and confidential information. But these small devices are resource constrained so it becomes impossible for these small devices to run these security algorithms that require large amount of memory and high processing power [1]. The other parts that should be in mind before designing a block cipher are the purpose of the device and cost of security. But the question arises that each and every designer have to address the amount of security is required

and how much of security is a good security because as factors that increases the security will also increase the cost. So, if mechanism deployed is not fully utilized to its capability, then it leads to the wastage of resource. For example, Advanced Encryption Standard (AES) has widely being analysed for its security and many attacks have been tried on this cipher. So AES can be deployed in all the devices. But size of the AES stops it from doing so. It also requires large no. of resource which again stops it from using it in small devices. We need to check the requirement of the user in its device. The aim here is to use a cipher in these devices which maintains the balance between security and resources. Hence the need is to design such a algorithm to suit the resource constraints for small devices with having primitives which provide adequate security to the user. These major reasons have lead to the development of lightweight block ciphers.

2.2 The Design Principles of Lightweight Block Ciphers

Block size, ciphertext size, key size, round function of the cipher has to be chosen as it is required for the security and for deployment purpose in device. A block cipher design can be divided in Feistel and SPN design [15]. These both designs are used in today's era. Similar design principles have been employed in lightweight block ciphers also. But amount of freedom is not same as in earlier cryptographic technique. For the block and for the size of the state, designer chooses multiple of word size. For ciphers plaintext generally size selected is 64 bits. Advantages and disadvantages are there for the both Fiestel and SPN design. The decryption is almost free in fiestel cipher. But the no. of rounds are more in it due to which throughput of the cipher reduces whereas there are less no. of rounds in SPN design as it has complex round function. But some decisions are same for the both designs. Since there is restriction of memory and data paths so the smaller block size is chosen. Generally block size is 64 bit and key size varies from 64-128 bits. The round function needs to be simple for the implementation in the hardware so that it takes less space. The confusion and diffusion layer is introduced in round function to increase security. For confusion S-Box of 4 x 4 bit is compact in size.. For any n x n bit S-box we need 2n x 2^{2n} bits of memory to store S-box. So smaller the S-box, compact is the implementation. For diffusion layer permutation of bits is used which provide security.

III. PRESENT LIGHTWEIGHT BLOCK CIPHER AND CRYPTANALYSIS

3.1 PRESENT Lightweight Block Cipher

Bogdanov et al. proposed a lightweight block cipher based on SPN structure called PRESENT cipher for restricted applications such as RFID, sensor networks etc. The structure of PRESENT consists of 64bit block, 80 or 128 bit key length and 31 rounds. Each round has 3 layers i.e. addRoundKey, sboxLayer and pLayer as shown in figure 1. The complete structure is shown in figure 2.

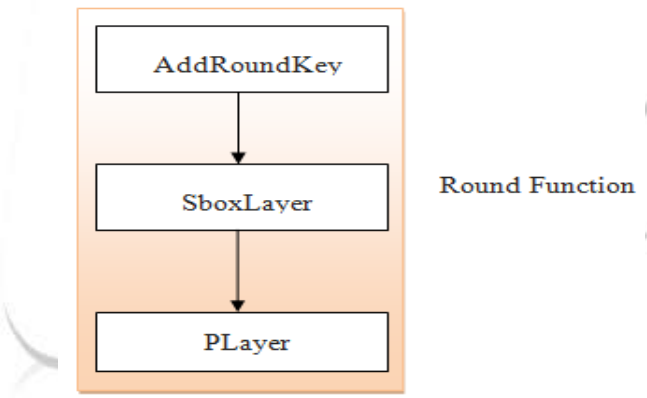


Figure 1: Round Function of PRESENT Block Cipher

In each round addRoundKey XOR's 64 bit of key with 64 bit of data. In sboxLayer, confusion is introduces using SBox of 4x4 which has nonlinear bijective mapping $\boldsymbol{S}: \boldsymbol{GF(2)^4} \rightarrow \boldsymbol{GF(2)^4}$ and is used 16 times in parallel in each round to substitute 4 bit of value. In pLayer bit by bit permutation is done $\boldsymbol{P}: \boldsymbol{GF(2)^{64}} \rightarrow \boldsymbol{GF(2)^{64}}$.

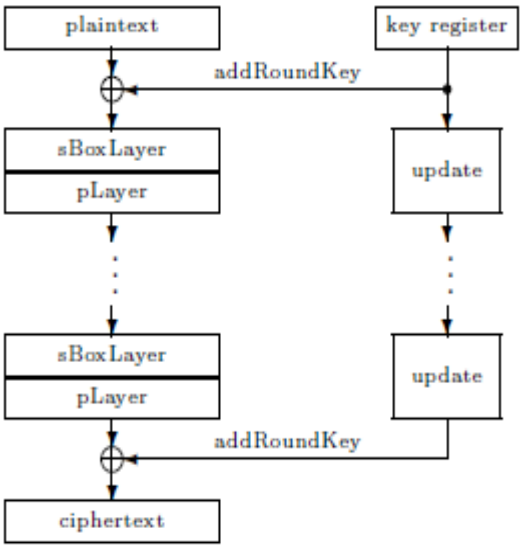


Figure 2: PRESENT Cipher Structure

In Key Schedule algorithm, initial 64 bit key is derived for each round from 80 bit master key. PRESENT is easy to implement in hardware with 1570 gate equivalents. The choice of diffusion layer as permutation of bits is suitable for small devices as it can be easily achieved.

3.2 PRESENT cipher Linear Cryptanalysis

Linear hull stands for the collection of all linear relations (across a certain number of rounds) that have the same (fixed) input and output bitmasks, but involves different sets of round subkeys according to different linear trails [17-18].

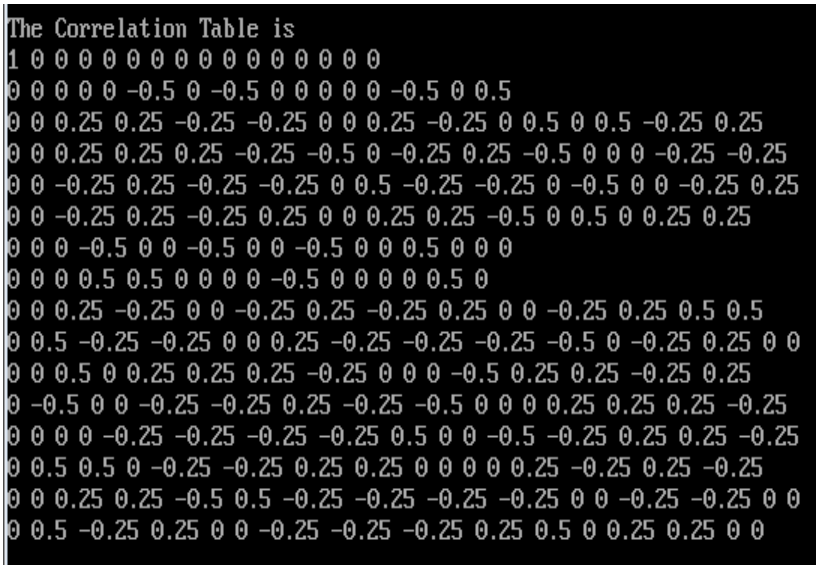
The Linear Approximation Table shown in table 1 of its 4 × 4 S-box has been generated for PRESENT block cipher in python, the entries for non-zero masks are either 0, 2, −2, 4 or −4, this shows that the S-box is linearly 4-uniform. Thus, the largest entry corresponds to a bias of $4/16 = 2^{-2}$, which is exploited to apply linear cryptanalysis. With the condition of plaintext with some fixed part of it to be constant, the Collard et al. presented that attack recovers the key of 24 round variant with 2^{57} chosen texts and 2^{57} time complexity. Jorge Nakahara et al presented the attack on 25-round PRESENT with the whole code book, $2^{96.68}$ 25-round PRESENT encryptions, 2^{40} blocks of memory.

Table 1: Linear Approximation for PRESENT Cipher

8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	−4	0	−4	0	0	0	0	0	−4	0	4
0	0	2	2	−2	−2	0	0	2	−2	0	4	0	4	−2	2
0	0	2	2	2	−2	−4	0	−2	2	−4	0	0	0	−2	−2
0	0	−2	2	−2	−2	0	4	−2	−2	0	−4	0	0	−2	2
0	0	−2	2	−2	2	0	0	2	2	−4	0	4	0	2	2
0	0	0	−4	0	0	−4	0	0	−4	0	0	4	0	0	0
0	0	0	4	4	0	0	0	0	−4	0	0	0	0	4	0
0	0	2	−2	0	0	−2	2	−2	2	0	0	−2	2	4	4
0	4	−2	−2	0	0	2	−2	−2	−2	−4	0	−2	2	0	0
0	0	4	0	2	2	2	−2	0	0	0	−4	2	2	−2	2
0	−4	0	0	−2	−2	2	−2	−4	0	0	0	2	2	2	−2
0	0	0	0	−2	−2	−2	−2	4	0	0	−4	−2	2	2	−2
0	4	4	0	−2	−2	2	2	0	0	0	0	2	−2	2	−2
0	0	2	2	−4	4	−2	−2	−2	−2	0	0	−2	−2	0	0
0	4	−2	2	0	0	−2	−2	−2	2	4	0	2	2	0	0

In this paper, the attack has been applied for various trails to reduce error probability. These properties shoen in correlation table have been exploited and attacked this cipher. The attack on 25 rounds of cipher has been seen by implementing the code in python by using multiple trails

Table 2: Correlation Table for PRESENT Cipher



IV. CONCLUSION

Cryptographers have been applying the latest attacks to already published or newly designed crypto algorithm. This paper includes the designing principles and need of lightweight ciphers. The papers summarise that design of cipher should maintain the balance between performance, resources and security. The weakness of the PRESENT block cipher has been analysed. The large no. of rounds includes much higher complexity of attack. Zero correlation attack which is a variant of linear cryptanalysis and is based on the concept of Miss in Middle technique has been tried on PRESENT lightweight block cipher. The code has been implemented to find correlation table. The code has been implemented using correlation table to find the break point of the cipher where the bits do not match in the middle, so to find the number of rounds that can be attacked.

EFERENCES

[1] Mehak Khurana, Meena Kumari, "Security Primitives: Block and Stream Ciphers", International Journal of Innovations & Advancement in Computer Science (IJIACS), ISSN 2347 – 8616, Vol. 4, March 2015.

[2] Kumar, M.; Pal, SK and Panigrahi, A., "Some Results on Design Parameters of Lightweight Block Ciphers" In Bilingual International Conference on Information Technology: Yesterday, Today, and Tomorrow, pp. 81-85, DESIDOC, 2015

[3] Bogdanov and V. Rijmen, "Linear hulls with correlation zero and linear cryptanalysis of block ciphers," Designs, Codes and Cryptography, vol. 70 , no. 3, pp. 369-383, March 2014 .

[4] Howard M. Heys, A Tutorial on Linear and Differential Cryptanalysis pp 1-11.

[5] Mehak Khurana, Meena Kumari, "Variants of Differential and Linear Cryptanalysis", International Journal of Computer Applications (0975 – 8887) Volume 131 – No.18, PP 20-28, December 2015

[6] H. Soleimany and K. Nyberg. Zero-Correlation Linear Cryptanalysis of Reduced round LBlock. Des. Codes Cryptography, 73(2):683-698, 2014.

[7] Mehak Khurana, Meena Kumari, "An Approach of Zero Correlation Linear Cryptanalysis" in International Journal of Computer Science and Engineering Technology, (IJCSET), ISSN : 2229-3345, Vol. 7, No. 05, pp 228-232, May 2016

[8] A.Bogdanov, V.Rijmen, Linear Hulls with Correlation Zero and Linear Cryptanalysis of Block Ciphers. Designs, Codes and Cryptography, Springer, US, 2012, pp. 1–15.

[9] Bogdanov, V. Rijmen: Zero Correlation Linear Cryptanalysis of Block Ciphers, IACR Eprint Archive Report 2011/123, March 2011.

[10] Andrey Bogdanov, Huizheng Geng, Meiqin Wang, Long Wen, and Baudoin Collard. Zero-Correlation Linear Cryptanalysis with FFT and Improved Attacks on ISO Standards Camellia and CLEFIA. In Selected Areas in Cryptography - SAC 2013, LNCS 8282, pages 306-323, 2013.

[11] Andrey Bogdanov, Gregor Leander, Kaisa Nyberg, and Meiqin Wang. Integral and Multidimensional Linear Distinguishers with Correlation Zero. In ASIACRYPT, in Lect. Notes Computer Science, vol. 7658, Springer, Heidelberg, pages 244-261, 2012.

[12] Boura, M. Naya-Plasencia, and V. Suder. Scrutinizing and Improving Impossible Differential attacks: Applications to CLEFIA, Camellia, LBlock and Simon. In ASIACRYPT 2014, LNCS 8873, pages 179-199, 2014.

[13] A. Bogdanov, M. Wang: Zero Correlation Linear Cryptanalysis with Reduced Data Complexity, FSE'12, LNCS, Anne Canteaut (ed.), Springer-Verlag, 2012.

[14] L. Wen, M. Wang, and A. Bogdanov. Multidimensional Zero-Correlation Linear Cryptanalysis of E2. In AFRICACRYPT'14, LNCS 8469, Springer-Verlag, pages 147-164, 2014.

[15] Wentan Yi and Shaozhen Chen, Multidimensional Zero-Correlation Linear Cryptanalysis of the Block Cipher KASUMI, [cs.CR] 14 Oct 2014
[16] Bogdanov, A. and Shibutani., K, "Generalized Feistel networks revisited", Designs, Codes and Cryptography, Vol. 66, Issue 1-3, pp. 75-97, Springer 2013
[17] Wentan Yi and Shaozhen Chen, Improved Integral and Zero-correlation Linear Cryptanalysis of Reduced-round CLEFIA Block Cipher, Cryptology ePrint Archive, Report 2016/149, http://eprint.iacr.org/, 2016
[18] J. Chen, M.Wang, B. Preneel: Impossible Differential Cryptanalysis of Lightweight Block Ciphers TEA, XTEA and HIGHT. IACR Eprint Archive Report 2011/616, 2011.

Mehak Khurana is currently working as assistant professor in The NorthCap University in CSE & IT and has around 6 years of experience. She completed her M.Tech from USIT, GGSIPU in 2011 and B.Tech from GTBIT, GGSIPU in 2009. Her key areas of interest are Cryptography, Information Security and Cyber Security. She is lifetime member of Cryptology Research Society