International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 05 | May 2018 www.irjet.net p-ISSN: 2395-0072

LIGHTWEIGHT CRYPTOGRAPHY: A SURVEY

Shweta V. Pawar[1], T.R. Pattanshetti[2]

[1]*Student, Dept. of Computer engineering, College of Engineering Pune, Maharashtra, India*
[2] *Professor, Dept. of Computer engineering, College of Engineering Pune, Maharashtra, India*

Abstract - *The main purpose of lightweight cryptography is to provide security for devices with limited resources. These devices with limited resources implement lightweight ciphers which are reliable and require low power and low computations. The lightweight cipher should be designed with fast encryption speed and minimal use of resources. This paper states overview of the current state of the art encryption technique in the area of lightweight cryptography, the comparison of block ciphers viz., PRESENT, QTL, BORON, LiCi, NUX on the basis of parameters such as input size, output size, structure used, key size, number of rounds, gate equivalents, vulnerable attacks etc. This paper presents brief overview of security analysis of recent block ciphers*.

Key Words: **Lightweight cryptography, block cipher, gate equivalents**

1. INTRODUCTION

As world is growing digitally new devices are also getting invented which are having battery and high performance, limited resources, execution time. New attacks are also happened on such devices. So there is a necessity to provide some kind security. Pre-existing algorithms available in market provide high security but consume more battery power. Thus, there is a need of developing new encryption method such that it should take low battery power with identical security as current state of art ciphers. Numerous applications will process biometric information or sensitive health-monitoring data, the interest for cryptographic segments that can be actualized effectively is solid and developing. For such usage, and for ciphers that are particularly suited for this reason, we refer the term lightweight cryptography in this paper. All makers of lightweight cryptography must spotlight on the balance between security, cost, and performance. It's by and large simple to accomplish any two of the three outline objectives - security and cost, security and execution, or cost and execution; notwithstanding, it is too difficult to enhance every one of the three plan objectives at once. For instance, a protected and superior equipment execution can be accomplished by a pipelined, side-channel-channel resistance architecture, bringing about a high zone prerequisite of area, and consequently high cost. Then again, it's possible to design a low-cost, secure hardware implementation but lacks performance.

In this paper, we are presenting the survey on selection of recent lightweight block ciphers and compare their performances. Section 2 describes the basic components in design of block ciphers. Section 3 describes the Criteria of performance measurement. Section 4 gives brief description of lightweight block ciphers. Section 5 compares them with respect to input size, output size, structure used, key size, number of rounds, gate equivalents, vulnerable attacks etc.

2. DESIGN BASICS OF BLOCK CIPHERS (Cryptographic Primitives)

2.1.1 S Box (Substitution Box)

In lightweight block ciphers, the input to s box is structure is usually 4 bits block which results into 4 bits output from substitution function. The 8*8 s-box increases the computation and processing time, thus 4-bit s-boxes are used in lightweight ciphers. This output can be calculated by using k-map techniques or fixed function which should have high confusion and diffusion. For decryption, the input and outputs get reverted. A robust S-box should follow the avalanche effect property i.e. change in single input bit should modify at least 50% of the bits in the output. If the encryption contains large number of active S-boxes, the security is high. Active S-boxes are calculated using two approaches,

1. Matusi's branch and bound algorithm [8]
2. Mixed-integer programming technique [9].

2.1.2 P Box (Permutation- Box)

P-box is a shuffling of the input bits or blocks to some other bits or blocks. The P-Box takes input from the outputs of the S-boxes of single round, changes order of bits, and gives input to S-boxes of the next round. If P-box has the good design then the output bits of any S-box are d to as many S-box inputs as possible.

2.1.3 Rounds

Every Encryption and decryption algorithm carries operations in multiple rounds. For each round different sub-keys are used. These sub-keys are built using key generation algorithm.

2.1.4 SP Network

Substitution – permutation network (SP Network) structure consists of mathematical operation. The s-box and p-box operations are carried out on plaintext and key to output the cipher text block. The input for SP network is divided into small multiple blocks to pass them to s-box or p-box. The operation which are hardware-efficient need to be performed for ex. Bitwise rotation or XOR. The Round keys are used in each round.

2.1.5 Feistel Cipher

Feistel structure is a design model which has symmetric structure and used in design of many block ciphers. In Feistel Cipher input is divided into two blocks which are swapped

iteratively before passing it to next rounds. The Right block is passed to a cryptographic function before swapping. The structure is as shown in fig.1 [7].

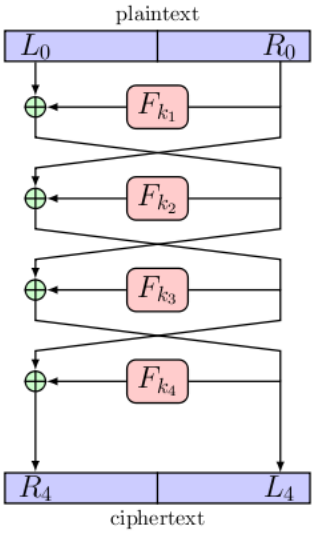

Fig.1 Feistel Structure

3. CRITERIA OF PERFORMANCE MEASUREMENT

The measurement of performance of lightweight ciphers is of great importance to reduce cost and increases security and efficiency of the encryption. The cryptography which is traditionally used only focuses on high security by ignoring the other requirement of low power and low processor devices. This devices developed in recent years has changed focus and researches are growing in this field for providing high security in low processing power, low computation, low cost hardware. The listed performance parameters are considered for high performance [10].

1. Clock Cycle Speed

Clock cycle per block and time required are important metrics to define lightweight block cipher. It is measured as number of clock cycles divided by operating frequency. The operating frequency should be identical in order to measure clock cycle speed accurately.

2. Gate Equivalent

A GE is equal to area needed by 2- input NAND gate. It is a standard measure referred as unit area. It represents measure of complexity of computations of lightweight block ciphers. Device generally having gate equivalents less than 2000 are considered as lightweight

.

3. Power

The good lightweight cipher design exhibits the property of low power consumption. Currently low power CMOS gate technology is available to decrease power consumption of cipher. Energy required per bit is calculated to measure power.

4. Memory Size

The memory size requires calculation of RAM or ROM used by the block cipher for encryption. Flash Memory is used to store look up table and program code. During program execution the dynamic access is provided by SRAM. If the encryption algorithm processes less data for performing operations the more lightweight it is.

4. LIGHTWEIGHT BLOCK CIPHERS

4.1. PRESENT

PRESENT is one of type of SP-network block cipher and has total 31 rounds. 64 The 64 bits input block is provided and uses two keys of 80 bits and 128 bits in length. It provides sufficient security level for low-security applications typically required for constrained devices. Each round of total 31 rounds performs XOR operation to produce a round key K_j for $1 < j < 32$, and K_{32} is used for a linear bitwise permutation, post-whitening, and a non-linear substitution layer. The S-box of 4-bits is used by the non-linear layer which is executed in each round 16 times in parallel manner. The pseudo-code for this cipher is as follows:

```
GenerateRoundKeys ( )
For j = 1 to 31 do following
AddRoundKeyFunction(state, Kj)
S-Box-Layer (state)
PLayerBlock (state)
End for
AddRoundKeyFunction (state, K32)
```

One major drawback of this block cipher is that it is vulnerable to side-channel and an invasive hardware attack which is the drawback of PRESENT light weight block cipher [1].

4.2 QTL

This light weight cipher is developed by L. Li et al to support optimal performance for low-power devices such as RFID devices. The input accepted is 64 bits block along with support of two different key length i.e. 64-bit and 128-bit keys.

QTL lightweight block cipher makes use of Feistel-type structures and improves security as compared to PRESENT block cipher. While performing encryption task it has many active S-boxes. To minimize the power consumption in hardware structure of the cipher, the QTL does not require key scheduling. QTL is vulnerable to the standard statistical attacks on block ciphers [3].

Structure of F-Function in QTL contains following steps:

1. Add Constants operation
2. Add Round Key operation
3. S-box operation
4. Permutation-layer operation
5. S-box layer operation

Structure of QTL:

```
Keyscheduling ( )
F (key, plaintext)
Shuffle blocks ( )
RoundTransposing (plaintext)
F (key, plaintext)
Ciphertext=Shuffle blocks ( )
```

4.3 BORON

BORON created by utilizing SPN, which underpins 64-bit block of plain text content alongside a key length of 128/80 bits. BORON requires 1626 Gate Equivalent (GEs) for a 80-bit key and 1939 GEs for a 128-bit key. It incorporates round permutation layers, shift operators, and XOR activities. Its diverse structure can produce S-boxes by utilizing rounds, which battles against the linear and differential attacks. BORON has the ideal execution on both programming and hardware platforms. It picks low power utilization when contrasted with LED and has higher throughput when contrasted with SP networks. BORON functions admirably for applications where both the security and low power concerns are present [4].The pseudo-code for this cipher is as follows:

```
M=m63 m62 ... m0
Round Keys ( )
For j=0 to 24 do
Add_round_key-Operation (M, Pj)
S_Box_Layer-Operation(M)
Block_Shuffle (M)
Round_Permutation-Operation(M)
XOR_Operation (M)
End for
Add_round_key -Operation(M, P25)
```

4.4 LiCi

The LiCi utilizes Feistel based network system which works by using 64-bits plain text content along with 128 bits key length. It creates 64 bits cipher message as an output. Its outline demonstrates best execution both on equipment and in addition on software. When contrasted with the current ciphers it requires less power consumption that necessities just 1153 GE's (Gate Equivalents) and has less memory measure prerequisites. LiCi opts the most minimal memory size and it is just 1944 bytes of Flash memory. It likewise takes just 30mW which is less power when contrasted with the other existing ciphers. The security investigation of the LiCi demonstrates that the LiCi opposes the direct, differential attack, Biclique and Zero correlation assaults [5]. Pseudo code is given as:

```
Plaintext = Plaintext_MOSIBI + Plaintext_LISIBI
For j =0 to 30 do
Plaintext _ MOSIBI (j+1) = S[Plaintext_ MOSIBI (j)]
Plaintext _ LISIBI (j+1) = ((Plaintext_ LISIBI (j) xor
Plaintext_ MOSIBI (j+1) xorRoundKey_j1)<<< 3)
Plaintext_MSB (j+1) = ((Plaintext_ MOSIBI (j+1)
xorPlaintext_ MOSIBI (j+1) xorRoundkey_j2)>>> 7)
Update Round Key ( )
Ciphertext_ MOSIBI (j) = Plaintext_ LISIBI (j+1)
Ciphertext_ LISIBI (j) = Plaintext_ MOSIBI (j+1)
Plaintext_ MOSIBI (j+1) = Ciphertext_ MOSIBI (j)
Plaintext_ LISIBI (j+1) = Ciphertext_LSB (j)
End for
Ciphertext = Ciphertext_ MOSIBI + Ciphertext_ LISIBI
```

4.5 NUX

NUX is a summed up with Feistel based network structure cipher, which has most noteworthy information complexity i.e. 2^24 and for less rounds brings about most noteworthy number of active S-boxes. It requires just 1022 GEs for 128-bit key length which is less when contrasted with all current lightweight ciphers. NUX cipher configuration is hearty and is most appropriate for applications where footprint areas, GE's are in requirements. With this cipher outline, it is conceivable to accomplish less GEs and focused memory space. It fights well against fundamentals assaults as well as MITM and Biclique Attacks. It is also used in IoT devices for low power consumption along with competitive security.

5. COMPARISON OF BLOCK CIPHERS

Table -1: Comparison1 of ciphers

Name of the block cipher	Implemented on software or hardware platform	Security Against Attacks	Vulnerable to Attacks	Active S-Boxes in Differential Analysis
LiCi	Both	Linear, Differential, Biclique, Zero Correlation	Differential Cryptanalysis on 16 rounds	1, 2, 6, 12 for first 4 rounds
QTL	Hardware	Linear, Differential, Related Key	Differential Cryptanalysis on 15 rounds , Standard Statistical Attacks	2, 4, 10, 14 for first 4 rounds
PRESENT	Hardware	Linear, Differential, Key Collision, Key Scheduling	Differential Cryptanalysis on 26 rounds, Biclique Attack	3, 7, 11, 17 for first 4 rounds
Boron	Both	Linear, Differential, Key Collision, Key Scheduling	Zero Correlation, Algebraic	1, 3, 8, 18 for first 4 rounds
NUX	Software	Linear, Differential, Biclique, MITM	Zero Correlation, Algebraic	0, 1, 2, 5 for first 4 rounds

Table -2: Comparison2 of ciphers

Name of the block cipher	Input block size	Key size	No. of rounds	Algorithm Design Pattern	GE
LiCi	64	128	31	Feistel	1153
QTL	64	80/128	25/31	Feistel	1025/1206
PRESENT	64	80/128	31	SPN	1339
Boron	64	80/128	16	SPN	1626/1939
NUX	64	80/128	31	Feistel	1022

6. CONCLUSION

In this paper, we have gone through the latest light weight block ciphers. Their algorithms and the security level of all these light weight block ciphers. It is also shown that which of the cipher uses which of the structure to develop itself i.e. Feistel network or SPN network. It is also compared that which of the cipher provides security against which attacks and susceptible to which attacks. The number of GEs required for particular light weight block cipher is also a crucial factor to consider. The study also proved that which of the cipher is best if number of GEs is main goal to design the block cipher. Among these light weight block cipher NUX is the latest one for constrained devices such as RFID and sensor network. The attacks which are possible and which are not possible also studied and best cipher is defined well in the study.

7. REFERENCES

[1] Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J., Seurin, Y. and Vikkelsoe, C., 2007, September. PRESENT: An ultra-lightweight block cipher. In International Workshop on Cryptographic Hardware and Embedded Systems (pp. 450-466). Springer, Berlin, Heidelberg.

[2] L. Li, Liu, B. and Wang, H., 2016. QTL: a new ultra-lightweight block cipher. Microprocessors and Microsystems, 45, pp.45-55.

[3] Sadeghi, S., Bagheri, N. and Abdelraheem, M.A., 2017. Cryptanalysis of reduced QTL block cipher. Microprocessors and Microsystems, 52, pp.34-48.
[4] Bansod, Gaurav, Narayan Pisharoty, and Abhijit Patil. "BORON: an ultra-lightweight and low power encryption design for pervasive computing." Frontiers of Information Technology & Electronic Engineering 18, no. 3 (2017): 317-331.
[5] Patil, J., Bansod, G. and Kant, K.S., 2017, February. LiCi: A new ultra-lightweight block cipher. In Emerging Trends & Innovation in ICT (ICEI), 2017 International Conference on (pp. 40-45). IEEE.
[6] BANSOD, G., SUTAR, S., PATIL, A. and PATIL, J.," NUX: A New Lightweight Block Cipher for Security at Wireless Sensor Node Level".
[7] http://barrywatson.se/crypto_feistel_cipher.html
[8] Matsui, M., 1994. On correlation between the order of S-boxes.
[9] A.Sun, S., Hu, L., Wang, M., et al., 2014a. Towards finding the best characteristics of some bit-oriented block ciphers and automatic enumeration of (related-key) differential and linear characteristics with predefined properties. Cryptology ePrint Archive, 2014/747.
[10] S. Kotel, F. Sbiaa, M. Zeghid, M. Machhout, A. Baganne and R. Tourki, "Performance evaluation and design considerations of lightweight block cipher for low-cost embedded devices," *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications,(AICCSA)*,Agadir,2016,pp.1-7.