Lightweight Block Ciphers: a Comparative Study

Sufyan Salim Mahmood AlDabbagh [1,a], Imad Al Shaikhli [2,b]

[1]Department of information systems, International Islamic University of Malaysia, Malaysia
[2]Department of Computer, International Islamic University of Malaysia, Malaysia
[a] sufyansalim_77@yahoo.com, [b] imadf@iium.edu.my

Article Info

Received: 7th July 2012
Accepted: 3rd September 2012
Published online: 15th November 2012

ISSN: 2231-8275

ABSTRACT

Although the AES is an excellent and preferred choice for almost all block cipher applications, it is not suitable for extremely constrained environments such as RFID (Radio-Frequency IDentification) tags and sensor networks. Therefore lightweight cryptography has become very vital and a strong demand. This paper meant to be a reference (for the cryptographic designers) on the lightweight block ciphers. It starts by doing a survey to collect the latest proposed ciphers, then to study them in terms of their algorithms specifications, hardware implementation and attacks. Finally, after the explanation and comparison, this research can be the basement for starting point to improve the lightweight block cipher in many directions like number of clock cycle, size of memory, number of Chosen Plaintext, Gate equivalence (GE), throughput and attacks.

***Keyword:* Lightweight block ciphers, RFID, RFID tag and AES**

1. Introduction

The pervasive computing like smart cards, RFID tags and sensor nodes that are used for public transport, smart electricity meters and anti-counterfeiting is become the main point for wireless communication and embedded systems. So, the choice of security algorithms of resource-limited devices should be very careful by consideration of the implementation costs, amount of power and Symmetric-key algorithms especially block ciphers still play an important role for the security of the embedded systems. For security and performance concerns, typically sensors are equipped with hardware implementation of AES-128. But for resource-constrained devices, AES could be too expensive despite the various approaches that have been proposed to reduce the costs of AES hardware and software implementations. So a compact hardware and software efficient block cipher could be the most promising candidate for security in such those devices. Therefore we introduce new branch of cryptography called lightweight cryptography. The main idea of lightweight cryptography is finding a compromise between low resource requirements, performance and strength of cryptographic primitives. In this paper, we present a selection of recently published lightweight-cryptography implementations and compare them to state-of-the-art results in their field(Knudsen, et al., 2011)(Yue-chao, et. al., 2010)(Paar, et.al., 2010).

2. Lightweight algorithms

This research will explore four published work on lightweight algorithms through discussion work on algorithms, hardware requirements and attacks as the following:

2.1hight

It was proposed by Hong et al. in 2006. It is lightweight block cipher which has high security and light weight with 64-bit block length and 128-bit key length which is suitable for low-cost, low-power, and ultra-light implementation. HIGHT has a 32-round iterative structure which is a variant of generalized Feistel network. The prominent feature of HIGHT is that it consists of simple operations such as XOR, addition mod 2^8 and left bitwise rotation as shown in Figure 1. So, it is hardware-oriented rather than software-oriented. HIGHT can be implemented with 3048 gates on 0.25µm (Hong, et al., 2006)(Anjali Arora, et al., 2012).

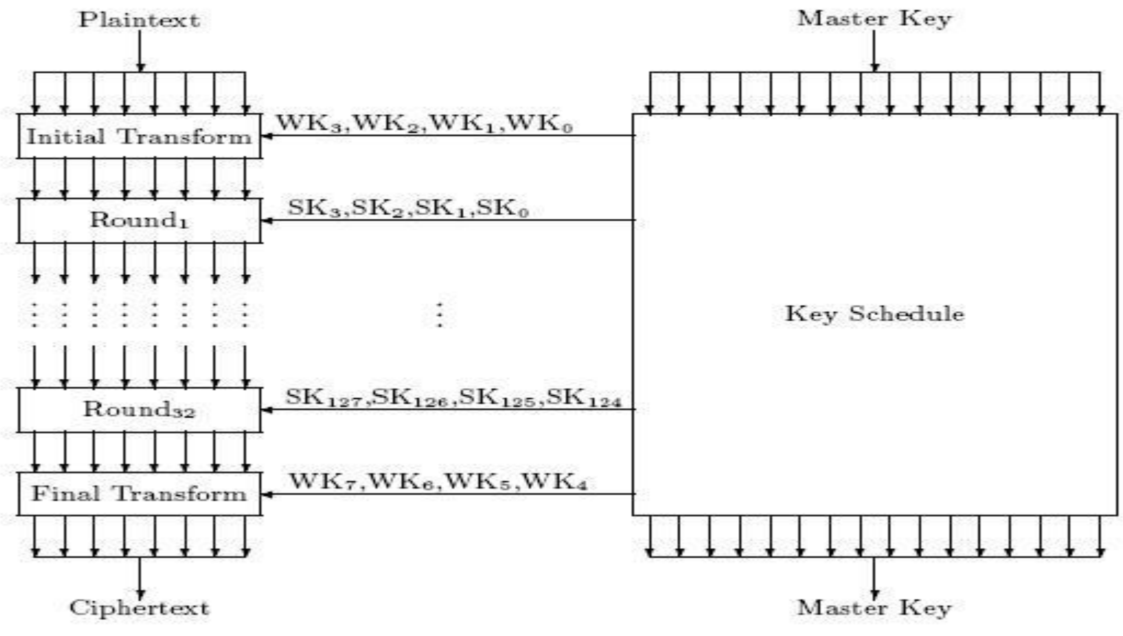


Fig 1. HIGHT encryption

2.2 Present

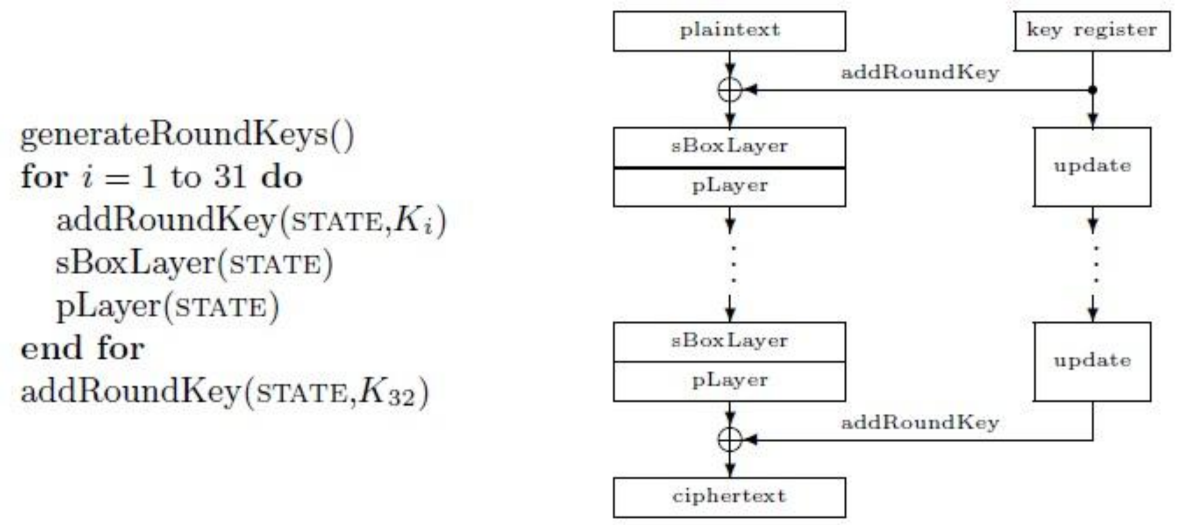
It was designed by Bogdanov et al. in 2007. It is an example of an SP-network and consists of 31 rounds. The block length is 64 bits and two key lengths of 80 and 128 bits are supported. Each of 31 rounds consists of XOR operation to introduce a round key Ki for 1≤ i <32, where K32 is used for post-whitening, a linear bitwise permutation and a non-linear substitution layer. The non-linear layer uses a single 4-bit S-box which is applied 16 times in parallel in each round as shown in Figure2 (Bogdanov, et al., 2007) (Anjali Arora, et al., 2012).

2.3 mCrypton

It was designed in 2005 by Lim and Korkishko. It has a block size of 64-bit and offers three different key sizes: 64 bits, 96 bits and 128 bits. Each of the 12 rounds consists of a substitution layer, a column-wise permutation layer, a column-to-row transposition layer and a key addition layer (Lim, et al., 2006).

2.4 Clefia

It was developed jointly by Sony, the University of Nagoya and Shirai et al. in 2007. It is Similar to the AES it has a block length of 128 Bits and offers three different key lengths: 128, 192 and 256 bits. CLEFIA uses a 4-branch and an 8-branch Type-2 generalized Feistel network and depending on the key length it takes 18 (128 bits), 22 (192 bits), or 26 (256 bits) rounds to encrypt one block of data. (Shirai, et al., 2007)



```
generateRoundKeys()
for $i = 1$ to 31 do
    addRoundKey(STATE,$K_i$)
    sBoxLayer(STATE)
    pLayer(STATE)
end for
addRoundKey(STATE,$K_{32}$)
```

Fig. 2. Top level of PRESENT

3. Comparison between lightweight blocks cipher

First of all, the comparison among the above explained algorithms will be based on the algorithm specifications (key size, block size and round), hardware implementation (clock cycles, throughput and area GE gate equivalent) and cryptanalysis (attack type, round number, data and memory).

3.1 Algorithm specifications

For key size, the CLEFIA and HIGHT have fixed key size 128-bit while the PRESENT has two keys 80,128 bit. Also, mCrypton has three keys 64, 96 and 128 bit. About the block size, the PRESENT, HEIGHT and mCrypton have fixed block size 64-bit while CLEFIA has three block sizes 128, 192 and 256. For round number, the CLEFIA has three numbers of rounds 18, 22 and 26. The PRESENT has 31 rounds while HIGHT has 32 rounds and mCrypton has 12 rounds as shown in table 1.

Table 1: Algorithm specifications for lightweight block ciphers

Block cipher	Key size (bit)	Block size (bit)	Round No.
CLEFIA	128-bit	128,192,256	18,22,26
PRESENT	80,128	64-bit	31
HIGHT	128-bit	64-bit	32
mCrypton	64,96,128	64-bit	12

3.2 Hardware implementation

The comparison results between lightweight block ciphers will show depend on: clock cycles, throughput and area GE. For clock cycle, the CLEFIA$_{128,\ 192,\ 256}$ have 18, 22 and 26 clock cycle respectively (Shirai, et al., 2007). The mCrypton$_{64,\ 96,\ 128}$ have the same clock cycle (Lim, et al., 2006) while the PRESENT$_{80,\ 128}$ have the same clock cycle (Bogdanov, et al., 2007) (Axel,2009) and the HIGHT has 34 clocks cycle (Özen, et al., 2009). About the throughput, the block ciphers that they have different clocks cycle they have different throughput while the block ciphers that they have same clocks cycle they have same throughput. For area GE, every block cipher has different GE as shown in table 2.

Table 2: Hardware implementation for lightweight block ciphers

Block cipher	Clock cycles	Area GE	Throughput Kbps
CLEFIA128	18	5,979	711.11
CLEFIA192	22	8,536	581.8
CLEFIA256	26	8,482	492.3
HIGHT	34	2,608	188.2
mCrypton64	13	3,473	492.3
mCrypton96	13	3,789	492.3
mCrypton128	13	4,108	492.3
PRESENT80	32	1,570	200
PRESENT128	32	1,884	200

3.3 Cryptanalysis

There are many attacks against lightweight block ciphers, such as: Impossible Differential and related- Key Rectangle. For Impossible Differential attack, it needs $2^{101.7}$ CP (chosen plaintext), $2^{103.5}$CP, 2^{111}CP, $2^{111.8}$CP, $2^{112.3}$CP and 2^{32}, 2^{121}, 2^{81}, 2^{112}, 2^{113} blocks of memory respectively(Shirai, et al., 2007) (Tsujihara,et al.,2008) to attacks from 10 to 14 rounds CLEFIA (Tsujihara,et al.,2008) while this attack needs $2^{46.4}$CP and 2^{60}CP and not specified memory to attacks 18 and 22 rounds of HIGHT respectively(Hong, et al.,2006) (Lu,2007). Also, this attack needs 2^{61}CP and 2^{109} byte to attacks 26 rounds of HIGHT as shown in the table3 (Özen, et al., 2009).

The result of Related Key Rectangle attack against PRESENT, mCrypton and HIGHT is shown in table 4. It attacks 17 rounds of PRESENT_{128}, 26 rounds of HIGHT and 8 rounds of mCrypton_{128}. It needs 2^{63}CP in PRESENT_{128}, $2^{51.2}$ CP in HIGHT and 2^{46}CP in mCrypton_{128}. About the memory, it needs 2^{53} byte in PRESENT_{128}, 5*2^{48} byte in mCrypton128 and not specified in HIGHT (Özen, et al., 2009) (Lu,2007) (Park,2009).

Table 3: Result of Impossible Differential attack

Block cipher	**Round No.**	**Data**	**Memory**
$\text{CLEFIA}_{128,192,256}$	10	$2^{101.7}$CP	2^{32}blocks
$\text{CLEFIA}_{192,256}$	11	$2^{103.5}$CP	2^{121}blocks
$\text{CLEFIA}_{128,192,256}$	12	2^{111}CP	2^{81}blocks
$\text{CLEFIA}_{192,256}$	13	$2^{111.8}$CP	2^{112}blocks
CLEFIA_{256}	14	$2^{112.3}$CP	2^{113}blocks
HIGHT	18	$2^{46.8}$CP	Not specified
HIGHT	25	2^{60}CP	Not specified
HIGHT	26	2^{61}CP	2^{109} byte

Table 4: Result of Related Key Rectangle

Block cipher	**Round No.**	**Data**	**Memory**
PRESENT_{128}	17	2^{63}CP	2^{53} byte
HIGHT	26	$2^{51.2}$ CP	Not specified
mCrypton_{128}	8	2^{46}CP	5*2^{48} byte

4. Discussion

From the results shown in the previous section we want to highlights some points. Firstly the hardware implementation, the mCrypton has the lowest clock cycle 13 while the GE and throughput are in the middle. The PRESENT80 has the lowest GE 1570 but the clock cycle is high and the throughput is approximately low. Third, CLEFIA128 has the highest throughput 711.11 but the GE is approximately is high and the clock cycle is approximately low.

Secondly the attacks, for Impossible Differential attack, the lowest memory blocks and CP in $\text{CLEFIA}_{128, 192, 256}$ are 2^{32} and $2^{101.7}$ respectively and the number of rounds that attack is 10 rounds only. To attack more rounds the value of CP and memory blocks will change. So, to attack 14 rounds of CLEFIA_{256} it needs $2^{111.3}$ CP and 2^{113} blocks memory. In the HIGHT the lowest CP is $2^{46.8}$CP and memory is not specified to attack 18 rounds of HIGHT while it needs 2^{61}CP and 2^{109} memory to attack 26 rounds of HIGHT. As a result, the Impossible Differential attacks 26 rounds out of 32 rounds of HIGHT but in CLEFIA it attacks 14 rounds out of 26 rounds. So this attack is well done in HIGHT rather than CLEFIA. For Related-Key Rectangle attack, it attacks only 17 out of 31 rounds of PRESENT_{128} and it needs 2^{63}CP with 2^{53} byte memory. So this number of attacked rounds is low when it compare with HIGHT and mCrypton. In HIGHT the number of attacked rounds is 26 out of 32 and it needs 2^{46}CP with not specified memory. While in the mCrypton the number of attacked rounds is 8 out of 12 and it needs 2^{46}CP with $5*2^{48}$ byte. As a result, this attack is bettter done in mCrypton rather than PRESENT and HIGHT.

5. Conclusion

The comparative study is done among lightweight block ciphers based on three criteria: algorithm specifications, hardware implementation and attacks. This paper shows that the mCrypton has the least clock cycle 13 while the PRESENT_{80} has the least area GE (1570) and the CLEFIA_{128} has the largest throughput (711.11). This paper shows that Impossible Differential attack was done successfully on HIGHT better than CLEFIA, while Related Key Rectangle was better when applied on mCrypton than on HIGHT and PRESENT. Finally, after the explanation and comparison, this research can be the starting point to improve the lightweight block cipher in many directions like number of clock cycle, size of memory, number of Chosen Plaintext, GE, throughput and attacks, which is our under going research.

Reference

Anjali Arora, P., & Pal, S. K. (2012). A Survey of Cryptanalytic Attacks on Lightweight Block Ciphers. *International Journal of Computer Science and Information Technology & Security (IJCSITS), Vol. 2,* pp.472-481.

Axel Poschmann. (2009).Lightweight Cryptography - Cryptographic Engineering for a Pervasive World. Number 8 in IT Security, Europaischer niversi atsverlag. Published: Ph.D. Thesis, Ruhr University Bochum.

Bogdanov, A., Knudsen, L., Leander, G., Paar, C., Poschmann, A., Robshaw, M., Seurin, Y., & Vikkelsoe, C. (2007). PRESENT: An Ultra-Lightweight Block Cipher Cryptographic Hardware and Embedded Systems - CHES 2007. In P. Paillier & I. Verbauwhede (Eds.), (Vol. 4727, pp. 450-466): Springer Berlin / Heidelberg.

Hong, D., Sung, J., Hong, S., Lim, J., Lee, S., Koo, B.-S., Lee, C., Chang, D., Lee, J., Jeong, K., Kim, H., Kim, J., & Chee, S. (2006). HIGHT: A New Block Cipher Suitable for Low-Resource Device Cryptographic Hardware and Embedded Systems - CHES 2006. In L. Goubin & M. Matsui (Eds.), (Vol. 4249, pp. 46-59): Springer Berlin / Heidelberg.

Knudsen, L. R., & Robshaw, M. J. B. (2011). The Block Cipher Companion: Springer Berlin Heidelberg.

Lim, C., & Korkishko, T. (2006). mCrypton – A Lightweight Block Cipher for Security of Low-Cost RFID Tags and Sensors Information Security Applications. In J.-S. Song, T. Kwon & M. Yung (Eds.), (Vol. 3786, pp. 243-258): Springer Berlin / Heidelberg.

Lu, J. (2007). Cryptanalysis of Reduced Versions of the HIGHT Block Cipher from CHES 2006. Information Security and Cryptology - ICISC 2007. In K.-H. Nam & G. Rhee (Eds.), (Vol. 4817, pp. 11-26): Springer Berlin / Heidelberg.

Ozen, O., Varıcı, K., Tezcan, C., & Kocair, Ç. (2009). Lightweight Block Ciphers Revisited: Cryptanalysis of Reduced Round PRESENT and HIGHT Information Security and Privacy. In C. Boyd & J. González Nieto (Eds.), (Vol. 5594, pp. 90-107): Springer Berlin / Heidelberg.

Park, J. H. (2009) .Security analysis of mcrypton proper to low-cost ubiquitous computing devices and applications. International Journal of Communication Systems, pp.959- 969.

Paar, C., & Pelzl, J. (2010). The Advanced Encryption Standard (AES) Understanding Cryptography (pp. 87-121): Springer Berlin Heidelberg.

Shirai, T., Shibutani, K., Akishita, T., Moriai, S., & Iwata, T. (2007). The 128-Bit Blockcipher CLEFIA Fast Software Encryption. In A. Biryukov (Ed.), (Vol. 4593, pp. 181-195): Springer Berlin / Heidelberg.

Tsujihara, E., Shigeri, M., Suzaki, T., Kawabata, T. and Tsunoo, Y.(2008).New Impossible Differential of CLEFIA. InIEICE Technical Report - ISEC2008-3.

Yue-chao, H., & Yi-ming, W. (2010, 17-19 June 2010). *Secure RFID system based on lightweight block cipher algorithm of optimized S-box.* Paper presented at the RFID-Technology and Applications (RFID-TA), 2010 IEEE International Conference on.