IOSR Journal of Computer Engineering (IOSRJCE)
ISSN: 2278-0661, ISBN: 2278-8727 Volume 5, Issue 5 (Sep-Oct. 2012), PP 01-04
www.iosrjournals.org

Performance Analysis of New Light Weight Cryptographic Algorithms

Jacob John
(Sinhgad Institute of Technology, Pune, India)

Abstract: *Humming Bird-2 and PRESENT are two recently proposed Light weight cryptographic algorithms specifically made for implementation in resource constrained devices like wireless sensor nodes, smart cards and RFID systems. Performance analyses of these two efficient algorithms are done in this paper. Results of hardware implementations of these algorithms are also discussed. An analysis also done on the results of implementation of the Humming bird-2 and PRESENT on low cost FPGA devices.*

Keywords: *Light weight cryptography, resource constrained devices, FPGA devices, Humming bird-2, PRESENT.*

I. INTRODUCTION

Since traditional cryptographic algorithms were not suitable for implementation in low resource devices like wireless sensor nodes, smart cards and RFID tags, there was a need to develop specifically designed cryptographic algorithms for these resource constrained devices. This led to the development of a new branch of cryptography called Light weight cryptography. The algorithms already developed in this category are Humming bird-2[1], PRESENT[2], HIGHT[3], DESL[4], light weight version of AES[5] etc .

Humming bird-2 does not come under the category of block cipher or stream cipher, but is having the properties of both. 16 bit blocks are operated on humming bird-2 which is suitable for RFID devices or wireless sensors which handles only small messages. Humming bird-2 optionally produces an authentication tag for each message processed. Hardware implementation of this can be done in RFID tags and wireless sensors, which gives performance and cost advantages. PRESENT is a hardware optimized block cipher which is designed to meet the area and power constraints. At the same time PRESENT is resistant to different types of security attacks. The architecture of PRESENT is an example of SP network which contains 31 rounds. The block size of PRESENT is 64 bit and key size is 80 bit. PRESENT has implementation requirements similar to many compact stream ciphers. Performance analysis of these two efficient algorithms are done in this paper.

The algorithms are described briefly in section 2. Security analysis of these algorithms are discussed in section 3. Section 4 explains the hardware implementations and FPGA implementation results are discussed in section 5.Then the paper is concluded in Section 6.

II. ALGORITHMS

2.1 Humming bird-2

The Humming bird-2 has key K of size 128 bit and it has 128 bit internal state R which is initialized using 64 bit Initialization Vector IV. Accessing of these variables are done as vectors of 16 bit words. The operations in Humming bird-2 are exclusive OR, addition modulo 65536 and non linear mixing function f(x) which are performed on 16 bit words.

The nonlinear mixing function f(x) is computed from the following operations.

$S(x) = S_1(x_0) \mid S_2(x_1) \mid S_3(x_2) \mid S_4(x_3)$

$L(x) = x \oplus (x <<< 6) \oplus (x <<< 10)$

$f(x) = L(S(x))$.

where S(x) denote computation of four S- Boxes and L(x) is the linear transformation.

A 16-bit keyed permutation WD16 can be found out using the following expression

$WD16(x, a, b, c, d) = f(f(f(f(x \oplus a) \oplus b) \oplus c) \oplus d)$

A four round procedure is used for initialization of internal state of Humming bird-2.

$R^{(0)} = (IV_1, IV_2, IV_3, IV_4, IV_1, IV_2, IV_3, IV_4)$

then iteration is done for i=0,1,2,3 to find t_1, t_2, t_3, t_4. These are used to update four state registers R_1, R_2, R_3, R_4.

Four invocations of WD16 is required to encrypt a single word of plain text to cipher text. After encryption or decryption of each word state update is done. Authenticated Encryption with Associated Data is a method in Humming bird -2 which authenticates any associated data that travels with cipher text. Processing of associated data happens only after entire encrypted payload has been processed. It is better to communicate data which are less than 16 bits in size without message expansion. If m is a short message with size 15 bits or less the cipher text message is derived from the n least significant bits of m $\oplus$ E(0).For message integrity the state is further updated by E(m).

2.2 PRESENT

The block length of PRESENT is 64 bits and the key sizes are 80 or 128 bits. There are 32 rounds in PRESENT. 31 rounds consists of XOR operation to form a round key and the 32nd round is used for post whitening. Each of the 31 rounds consists of a non linear substitution layer and a linear permutation layer. The main module of the cipher is given below.

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

addRoundKey performs the following operation

$$b_j \longrightarrow b_j \oplus k_j^i$$

where j varies from 0 to 63 and I varies from 1 to 32. sBoxlayer performs a conversion from 4 bit to 4 bit. This is more compact than an 8-bit S Box which gives more hardware efficiency. pLayer performs the movement of bit i to a bit position P(i). The key given by the user is stored in key register K. $K_i= K_{63}K_{62}K_{61}\ldots K_1K_0$ contains left most 64 bits of K. Thus at round i, $K_i=K_{63}K_{62}K_{61}\ldots K_0=K_{79}K_{78}\ldots\ldots K_{16.}$ Then the key register is updated as follows.

$K_{79}K_{78}\ldots.K_1K_0=K_{18}K_{17}\ldots K_{20}K_{19}$
$K_{79}K_{78}K_{77}K_{76}=S[K_{79}K_{78}K_{77}K_{76}]$
$K_{19}K_{18}K_{17}K_{16}K_{15}= K_{19}K_{18}K_{17}K_{16}K_{15} \oplus$ round_counter

The key is rotated by 61 bit positions to the left , left most 4 bits are passed through the S Box and the round counter value i is XORed with bits $K_{19}K_{18}K_{17}K_{16}K_{15}$ of K with the least significant bit of round counter on the right.

III. SECURITY ANALYSIS

Humming bird-2 can resists security attacks like Differential Cryptanalysis[6] and Linear Cryptanalysis[7]. From the security analysis it is found that Humming bird-2 is resistant against linear cryptanalysis up to 12 rounds of *f*. The four rotations in the initialization phase makes a good resistance against related key attacks. The algebraic degree and branch number of S-Boxes thwart different forms of algebraic distinguishing attacks.

The sBoxLayer and pBoxLayer in PRESENT provide good defensive mechanism against differential cryptanalysis and linear cryptanalysis. Linear cryptanalysis of PRESENT require more than 2^{84} plain text/cipher texts. Such data requirements are impossible to achieve. PRESENT is also resistant to related key attacks[8] and slide attacks[9]. Round – dependant keys are used in PRESENT so that the sub key sets cannot be slid and a non linear operation is used to mix the contents of the key register. The bitwise operations in PRESENT resist structural attacks like integral attacks[10] and bottleneck attacks[11].

IV. HARDWARE IMPLEMENTATION

Performances of two different hardware implementations of Humming bird-2 are analyzed. The high performance design HB2-ee4c with 4 clock implementation requires 3220 GEs. The low area and power design HB2-ee20c with 20 clocks per word requires comparatively less power and less area requirement of 2159 GEs. The hardware implementation of PRESENT requires power consumption of 5µw and area requirement of 1570 GEs and 32 clock cycles to encrypt a 64 bit plain text with an 80 bit key. A comparative analysis of these hardware implementations are given in the following table.

.

Table 1 Comparison of Hardware Implementations of Cryptographic Algorithms

Profile	frequency	clocks per round	Peak power(µw)	GE
HB2-ee4c	100KHz	4	1.93	3220
HB2-ee20c	100 KHz	20	1.73	2159
PRESENT	100 KHz	32	5	1570

Throughputs of various cryptographic algorithms under the operating frequency 80 MHz is given in the following table. Throughput indicates the processing speed of a cipher, that is how fast it converts the plain text to cipher text. Throughput of Humming bird-2 is higher than the throughputs of other algorithms, which shows the processing speed of Humming bird-2 is faster than the other algorithms.

Table 2 Performance Comparison of Light Weight Cryptographic Algorithms

Cipher	Block length	Cycles per block	Key size	Throughput (at 80 MHz) in Mbps
Humming bird-2	16	4	128	320
PRESENT	64	32	80	160
HIGHT	64	34	128	150.6
DESXL	64	144	184	35.6
AES	128	1032	128	9.9

Throughputs various ciphers under the same conditions are compared in the following figure. It is found that Humming bird-2 is having the highest throughput.

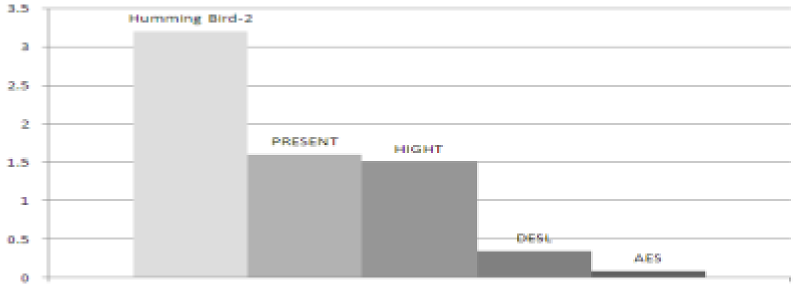

Fig 1 Comparison of throughputs of various ciphers under the operating frequency 80 MHz.

V. FPGA IMPLEMENTATION

A performance comparison of FPGA implementations of Humming bird-2 and PRESENT are done with low cost FPGA devices. The FPGA devices used are Spartan-3 XC 35200 and Spartan-3 XC 35400. A summary of the implementation results are shown in the table where area requirement (slices), maximum frequency, throughput and efficiency are given. The results show that PRESENT is more efficient than humming bird-2.

Table 3 Performance Comparison of FPGA Implementations of Cryptographic Algorithms[12]

Cipher	Key size	Block Size	FPGA device	Max frequency	Throughput	Slices	Efficiency
Humming bird-2	128	16	Spartan-3 XC 35200	40.1	160.4	273	0.59
PRESENT	80	64	Spartan-3 XC 35400	258	516	176	2.93
PRESENT	128	64	Spartan-3 XC 35400	254	508	202	2.51

VI. CONCLUSION

In this paper results of implementations of light weight cryptographic algorithms Humming bird-2 and PRESENT are analyzed. It is found from security analysis that both the algorithms provide adequate security. The hardware implementation of PRESENT requires comparatively less area. PRESENT is more efficient in FPGA implementation. But the power consumption of Humming bird-2 is comparatively less in hardware implementation. The throughput of Humming bird-2 is higher than other algorithms. So it is found from the analysis that Humming bird-2 is more suitable as cryptographic algorithm for resource constrained devices.

REFERENCES

[1] Daniel Engels, Marakku-Juhani O. Saarinen, Peter Schweitzer, Eric M. Smith "The Hummingbird-2 Light weight Authenticated Encryption Algorithm" RFID Sec 2011.The 7th workshop on RFID Security and Privacy, Amherst, Massachusets , USA June 2011.

[2] A. Bogdanov et al., "PRESENT: An ultra-lightweight block cipher," in CHES 2007, ser. LNCS, vol. 4727. Springer, 2007, pp. 450–466.

[3] Hong, J. Sung, S. Hong, J. Lim, S. Lee, B.-S; Koo, C. Lee, D. Chang, J. Lee, K. Jeong, H. Kim, J. Kim, and S. Chee. "HIGHT: A New Block Cipher Suitable for Low-Resource Device," In L. Goubin and M. Matsui, editors, Proceedings of CHES 2006.

[4] G. Leander, C Paar, A. Poschmann, and K Schramm "A Family of Lightweight Block Ciphers Based on DES Suited for RFID Applications". In A. Biryukov, editor,Proceedings of FSE 2007, LNCS, Springer-Verlag.

[5] M. Feldhofer, S. Dominikus, and J.Wolkerstorfer."Strong Authentication for RFIDSystems Using the AES algorithm". In M. Joye and J.-J. Quisquater, editors, Proceedings of CHES 2004, LNCS, volume 3156, pages 357–370, Springer Verlag, 2004.

[6] E. Biham, A. Shamir. "Differential Cryptanalysis of the Data Encryption Standard," Springer-Verlag,1993.

[7] M. Matsui, “Linear Cryptanalysis Method for DES Cipher," Advances in Cryptology - EUROCRYPT'93, T. Helleseth, Ed., LNCS 765, Springer-Verlag, pp. 386-397, 1994.

[8] E.Biham. “ New Types of Cryptanalytic Attacks Using Related Keys”. In T.Helleseth, editor, Proceedings of Eurocrypt ’93, LNCS, volume 765, pages 398-409, Springer-Verlag , 1994.

[9] A. Biryukov and D Wagner. “Advanced Slide Attacks”. In B . Preneel , editor, Proceedings of Eurocrypt 2000, LNCS, volume 1807, pages 589-606, Springer – Verlag 2000.

[10] L R Kundsen and D Wagner , “Integral Cryptanalysis”. In J.Daemen and V.Rijmen, editors, Proceedings of FSE 2002, LNCS , volume 2365, pages 112-137, Springer – Verlag 2002.

[11] H. Gilbert and M. Minier. “A Collision Attack on 7 Rounds of Rijndael”. In Proceedings of Third Advanced encryption Standard Conference, National Institutes of Standards and Technology, 230-241, 2000.

[12] Xinxin Fan, Guang Gong, K. Lauffenburger, T. Hicks “ FPGA Implementations of the Hummingbird Cryptographic Algorithm” Hardware Oriented Security and Trust (HOST) 2010 IEEE International Symposium.