IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. XII (Mar-Apr. 2014), PP 91-95
www.iosrjournals.org

BEST-1: A Light Weight Block Cipher

Jacob John
(Sinhgad Institute of Business Administration and Computer Application, Lonavala, Pune, India)

Abstract: *The demand for applications involving Wireless Sensor Network (WSN) or RFID systems is increasing. The sensor in a WSN and RFID tag/reader in a RFID system are called resource constrained devices because these devices have limited processing power, memory size and energy supply. The information transmitted among these low resource devices must be protected from unauthorized access using specifically made cryptographic algorithms. In this paper a new block cipher BEST-1 (Better Encryption Security Technique-1) is proposed with 64 bit block length and 128 bit key length. It is specifically designed for the above mentioned low resource devices. It provides good security and better processing speed as a cryptographic algorithm.*

Keywords: *Light weight, block cipher, cryptography, low resource, resource constrained devices.*

I. Introduction

Radio frequency identification (RFID) tags and WSN nodes are few examples of ubiquitous computing, which are used in applications like supply chain management, access control, inventory management, automated electronic toll systems etc. There are security concerns about the confidentiality and privacy of radio frequency communication between reader and the tag in a RFID system. A wireless sensor network is a network composed of a large number of sensors that are physically small, communicate wirelessly among each other. Sensor node senses surrounding environment, gather data, transmit them through network. Sensor devices and RFID systems have critical resource constraints such as processing power, memory size and energy supply. Due to wireless nature of the sensor network and constrained nature of resources, there are number of security threats. Since the security and privacy of collected data are important, secure communication channel must be established between nodes. In order to obtain a high level of security in the above said low resource devices, it is necessary to use strong cryptographic algorithms.

The traditional cryptographic algorithms are not suitable for the light weight platforms of sensor network and RFID systems. The algorithms already developed for this particular environment are Hummingbird-2[1, 2], PRESENT [3,4], HIGHT [3,5], DESXL [6], low resource version of AES [7], etc. To meet the demands of the future, there is a need to design and develop a new light weight cryptographic algorithm with better security and faster processing speed.

In this paper a new block cipher BEST-1 (Better Encryption Security Technique-1) is proposed, which is specifically designed for low cost, low power and ultra light implementation. BEST-1 is designed to suit the requirements of 8 bit oriented CPUs of sensor nodes in sensor networking system or RFID system.

The paper is organized as follows. In section II, the specifications of BEST-1 are presented. The design principles of BEST-1 and the hardware implementation are described in section III. Security analysis is discussed in Section IV. In section V, the performances of various block ciphers are analysed. Then the paper is concluded in section VI.

II. Proposed Block Cipher BEST-1

The block length of BEST-1 is 64 bit and key length is 128 bit. The key schedule algorithm of BEST-1 generates transformation keys and sub keys. Sub keys are generated in the fly during encryption and decryption process. It also keeps the value of the Master key in both these processes. The operations performed in BEST-1 are XOR, addition mod 2^8 , subtraction mod 2^8 and bitwise shift.

The notations used for the operations in BEST-1 are given as below.

$\oplus$: XOR (exclusive OR) $\boxplus$: addition mod 2^8

$\boxminus$: subtraction mod 2^8 $X^{<<<a}$: a-bit left rotation of a 8 bit value X

The 64 bit plain text and cipher text are considered as concatenations of 8 bytes and denoted by $P=P_0||P_1||..P_7$ and $C=C_0||C_1||$ .. C_7 respectively. The 64 bit intermediate values are represented as $X_i=X_{i,0}||X_{i,1}||..X_{i,7}$ where i=0,..,11.The 128 bit master key is considered as concatenation of 16 bytes and denoted by $MK=MK_0||MK_1||..MK_{15}$.

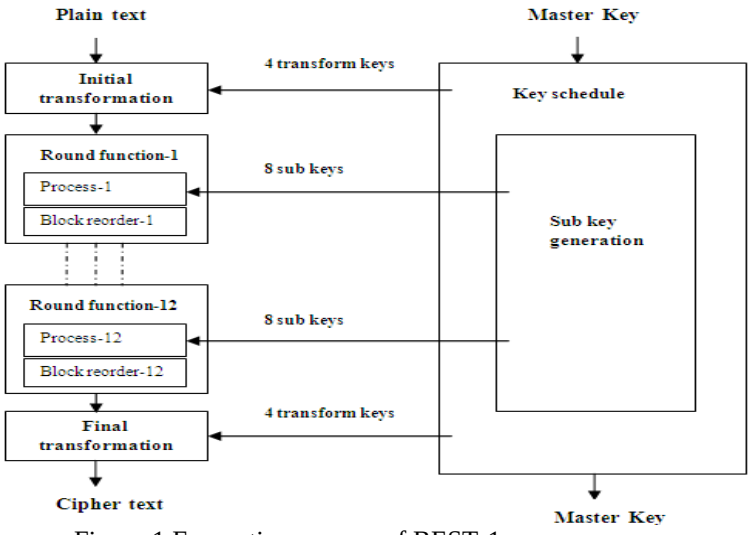

Figure-1 Encryption process of BEST-1

The encryption process of BEST-1, BESTEncryption consists of key schedule, initial transformation, round function and final transformation. The main algorithm BESTEncryption is given below.

```
BESTEncryption(P,MK){
KeySchedule(MK,TK,SK);
BEncryption(P,TK,SK){
InitialTransformation(P, X0 , TK3 , TK2 , TK1 , TK0 );
for i=0 to 11
{
RoundFunction(){
Process( );
BlockReorder();
} }
FinalTransformation(C, X11 , TK7 , TK6 , TK5 , TK4 );
}}
```

TK and SK stands for Transformation keys and Sub keys.

2.1. Key Schedule

The algorithm KeySchedule consists of two sub algorithms TransformationKeyGeneration which generates 8 transformation keys TK_0 ..TK_7 and SubKey Generation which generates 96 sub keys SK_0...SK_{95}.

```
KeySchedule(MK,,TK,SK){
TransformationKeyGeneration(MK,TK);
SubKeyGeneration(MK,SK);
}
```

2.1.1 TransformationKeyGeneration( )

TransformationKeyGeneration generates 8 transformation keys which are used in initial and final transformations. The algorithm TransformationKey Generation is given below.

```
TransformationKeyGeneration {
for i=0 to 7
{
If  0≤ i ≤ 3    then  TKi ← MKi+12 ;
                else  TKi ← MKi-4 ;
}}
```

2.1.2 SubKeyGeneration( )

SubKeyGeneration algorithm generates 96 sub keys. In round function 8 sub keys are processed per round. The algorithm SubKeyGeneration uses sub algorithm ConstantGeneration to generate 96 constants d_0..d_{95}, then use these constants to generate sub keys SK_0..SK_{95}.

The value of d_0 is fixed. The algorithm ConstantGeneration uses LFSR to generate d_1.. d_{95} from d_0 as follows.

ConstantGeneration {
$S_0 \leftarrow 0$; $S_1 \leftarrow 1$; $S_2 \leftarrow 0$;
$S_3 \leftarrow 1$; $S_4 \leftarrow 1$; $S_5 \leftarrow 0$;
$S_6 \leftarrow 1$; $S_7 \leftarrow 0$;
$d_0 \leftarrow S_7 \| S_6 \| S_5 \| S_4 \| S_3 \| S_2 \| S_1 \| S_0$
for i=1 to 95 {
$S_{i+7} \leftarrow S_{i+2} \oplus S_{i-1}$
$d_i \leftarrow S_{i+7} \| S_{i+6} \| S_{i+5} \| S_{i+4} \| S_{i+3} \| S_{i+2} \| S_{i+1} \| S_{i+0}$
}

The algorithm SubKeyGeneration generates the sub keys as follows.

SubKeyGeneration (MK , SK){
Run ConstantGeneration
For i=0 to 7 {
For j=o to 5{
$SK_{16.i+j} \leftarrow MK_j \boxplus d_{16.i+j}$;
}
For j=0 to 5 {
$SK_{16.i+j+8} \leftarrow MK_{j+8} \boxplus d_{16.i+j+8}$;
} }

2.2. Initial Transformation

The plain text P is transformed into the input of Round Function $X_0 = X_{0,0} \| X_{0,1} \| .. \| X_{0,7}$ through InitialTransformation using four transformation key bytes TK_0 , TK_1 , TK_2, TK_3.

InitialTransformation(P, X_0 , TK_3 , TK_2 , TK_1 , TK_0){
$X_{0,0} \leftarrow P_0 \boxplus TK_0$; $X_{0,1} \leftarrow P_1$;
$X_{0,2} \leftarrow P_2 \oplus TK_1$; $X_{0,3} \leftarrow P_3$;
$X_{0,4} \leftarrow P_4 \boxplus TK_2$; $X_{0,5} \leftarrow P_5$;
$X_{0,6} \leftarrow P_6 \oplus TK_3$; $X_{0,7} \leftarrow P_7$;
}

2.3.Round Function

The sub algorithm RoundFunction() is given below.

RoundFunction()
{
Process( );
BlockReorder();
}

There are two sub algorithms inside RoundFunction() . They are Process() and BlockReorder().

2.3.1 Process( )

Four sub functions are used in process. They are F_1 , F_3 , F_4 and F_6 which are given as follows.

$F_1 = X^{<<<1}$ $F_3 = X^{<<<3}$
$F_4 = X^{<<<4}$ $F_6 = X^{<<<6}$

For i=0,..,11 Process( ) transforms $X_i=X_{i,0}\|X_{i,1}\|..X_{i,7}$ into $X_{i+1}=X_{i+1,0}\|X_{i+1,1}\|..X_{i+1,7}$ as follows.

Process (X_i , X_{i+1} , $SK_{8.i+0}$, $SK_{8.i+1}$, $SK_{8.i+2}$, $SK_{8.i+3}$, $SK_{8.i+4}$, $SK_{8.i+5}$, $SK_{8.i+6}$, $SK_{8.i+7}$) {
$X_{i+1,0} \leftarrow SK_{8.i+0} \oplus X_{i,0}$
$X_{i+1,1} \leftarrow SK_{8.i+1} \boxplus X_{i,1}$
$X_{i+1,2} \leftarrow SK_{8.i+2} \oplus F_1(X_{i,2})$
$X_{i+1,3} \leftarrow SK_{8.i+3} \boxplus F_3(X_{i,3})$
$X_{i+1,4} \leftarrow SK_{8.i+4} \oplus X_{i,4}$
$X_{i+1,5} \leftarrow SK_{8.i+5} \boxplus X_{i,5}$
$X_{i+1,6} \leftarrow SK_{8.i+6} \oplus F_4(X_{i,6})$
$X_{i+1,7} \leftarrow SK_{8.i+7} \boxplus F_6(X_{i,7})$

}

2.3.2 BlockReorder( )

BlockReorder() reorders the block after the execution of process( ) function in each and every round. In the next round process( ) will be applied on the reordered block. The BlockReorder() algorithm is given as follows.

BlockReorder(X_j , X_k , j,k) {
j←0; k ← 7;
While (j<k)
{
swap(X_j , X_k); j ← j+1; k ← k-1;
}}

2.4.Final Transformation

Final transformation transforms $X_{11} = X_{11,0} \| X_{11,1} \| .. \| X_{11,7}$ to cipher text C using four transformation key bytes TK_4 , TK_5 , TK_6, TK_7 . The sub algorithm FinalTransformation is given below.

FinalTransformation(C, X_{11} , TK_7 , TK_6 , TK_5 , TK_4) {

$C_0 \leftarrow X_{11,0} \boxplus TK_4$; $C_1 \leftarrow X_{11,1}$; $C_2 \leftarrow X_{11,2} \oplus TK_5$; $C_3 \leftarrow X_{11,3}$;

$C_4 \leftarrow X_{11,4} \boxplus TK_6$; $C_5 \leftarrow X_{11,5}$; $C_6 \leftarrow X_{11,6} \oplus TK_7$; $C_7 \leftarrow X_{11,7}$;

}

2.5.Decryption Process

Decryption is done as a sequence of steps after inverting the BEST-1Encryption(). During decryption, in the round function $\boxminus$ is done instead of $\boxplus$ and bitwise shifting is performed in the reverse direction.

III. Design Principles Of Best-1

Encryptions of a large amount of data are not expected in applications involving low resource devices. The block length of BEST-1 is 64 bit. If the block length is increased it will decrease the speed of processing. CPUs associated with the sensors in WSN are based on 8 bit processor. So every operation in BEST-1 must be 8 bit oriented. Since encryption is simply converted into decryption process, implementation of circuit supporting both encryption and decryption does not require much more cost than encryption only circuit. Key length of BEST-1 is 128 bit, it provides adequate security. If length of key is increased more it will affect the speed of processing. The combination of XOR and addition mod 2^8 plays an important role for resistance against existing attacks. The inner functions F_1 , F_3 , F_4 , F_6 of round function provides BEST-1 bitwise diffusion. The sequence d_0 ... d_{95} generated by linear feedback shift register enhances the randomness of sub keys. Many security attacks will be resisted by these process. The function BlockReorder( ) included in the round function increases the security.

The algorithm BEST-1 can be implemented in a hardware circuit. The main parts of the circuit are Key schedule, Round function and Control logic. The resource requirements for the hardware implementation will be approximately around 2200 GEs.

IV. Security Analysis

The security of BEST-1 is analysed against various attacks. It is found from the results of analysis that BEST-1 is secure enough for cryptographic applications. The differential cryptanalysis [8] uses paths from the plain text difference to the cipher text difference for attacking the ciphers. The round function with block reorder function and final transformation make a good defensive mechanism against differential cryptanalysis. Linear cryptanalysis [9] uses relations of plain text, cipher text and master key. In the case of BEST-1, such attack requires more than 2^{58} plain texts to get some success rate. Truncated differential cryptanalysis [10] is a path from a partial difference of the input to partial difference of the output.

The probabilities of truncated differential characteristics are too low to be applied for attack. Boomerang attack [11] use two differential characteristics with relatively high probabilities. The improved form of Boomerang attack is amplified Boomerang attack [12] and rectangle attacks [13,14]. The block reorder function and final transformation can resist such attacks. The weakness of the key schedule is exploited by the slide [15] and related key attacks [16]. The sub key generation algorithm is strong enough to prevent such attacks. Different sub keys are processed in each round of the round function. Different constants are used to make those sub keys. This is a good resistance against slide attack. Related key attack is done by finding the relation between two master keys. The combination of key schedule and round function will resist such attacks

V. Performance Analysis

A comparative analysis of the performances of various block ciphers are shown in the below given table.

Table -1 Performance Analysis of Various Block Ciphers

	Block length	Cycles per block	Key size	Throughput (at 80 MHz) in Mbps
BEST-1	64	14	128	365.7
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

VI. Conclusion

A new block cipher BEST-1 with 64 bit block length and 128 bit key length is proposed. It is designed for implementation in resource constrained devices such as RFID systems or wireless sensor networks. It is found from security analysis that it has adequate security. The throughput of BEST-1 is 365.7 Mbps under the operating frequency 80 MHz, which shows it has faster processing speed.

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] 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.

[3] P Yalla , Jens-Peter Kaps "Light Weight Cryptography for FPGAs " IEEE International Conference on Reconfigurable Computing and FPGAs 2009 IEEE Computer Society Press.

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

[5] D. 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.

[6] 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.

[7] 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.

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

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

[10] L. R. Knudsen, "Truncated and Higher Order Differential," FSE 94, LNCS 1008, Springer-Verlag, pp. 229-236, 1995.

[11] D. Wagner,"The Boomerang Attack," FSE'99, LNCS 1636, Springer-Verlag, pp.156-170, 1999.

[12] J. Kelsey, T. Kohno, B. Schneier, " Amplified Boomerang Attacks Against Reduced-Round MARS and Serpent," FSE 2000, LNCS 1978, Springer-Verlag, pp. 75-93,2001.

[13] E. Biham, O. Dunkelman, N. Keller, "The Rectangle Attack- Rectangling theSerpent," Advances in Cryptology - EUROCRYPT 2001, LNCS 2045, Springer-Verlag, pp. 340-357, 2001.

[14] E. Biham, O. Dunkelman, N. Keller, "New Results on Boomerang and Rectangle Attacks," FSE 2002, LNCS 2365, Springer-Verlag, pp. 1-16, 2002.

[15] A. Biryukov, D.Wagner, "Slide Attacks," Advances in Cryptology - FSE'99, LNCS1687, Springer-Verlag, pp. 244-257, 1999.

[16] E. Biham," New Types of Cryptanalytic Attack Using Related Keys," Journal of Cryptology, Volume 7, Number 4, pp. 156-171,1994.