A Modified XTEA

Niladree De, JaydebBhaumik

Abstract*—This paper presentsa modified Extended Tiny Encryption Algorithm (XTEA). A nonlinear Boolean function called Nmix is used to replace addition modulo 2^{32}.Proposed design has been implemented on a FPGA platform. Simulation result shows that it requires a reasonable hardware and provides an acceptable throughput. It is shown that proposed design requires less hardware compared to XTEA.

Index Terms*— Extended Tiny Encryption Algorithm (XTEA), Nonlinear Mixing Function, VLSI Implementation.

I. INTRODUCTION

Security of information has become a main issue in the ever evolving world of small mobile devices such as personal digital assistants (PDAs) and cell phones. Cryptographic algorithms and protocols constitute the central component of systems that protect network transmissions and stored data.In such small devices, the fight over high performance and low power consumption, besides security are primary targets. A great deal of assistance in creating low-power and high-speed cores, comes from the simplicity of the selected algorithm for embedding as a hardware component.

In cryptography, a block cipher is a bijective mapping from $\{0,1\}^n$ to $\{0,1\}^n$, parameterized by a key $\{0,1\}^k$. Typically block sizes are n €{64,128,256} and key size k € {128,192,256}. During encryption it takes a block of plaintext as input, and produces a block of corresponding ciphertext. The decryption algorithm takes a block of ciphertext together with the secret key, and yields the original block of plaintext.Many encryption algorithms are now available in the market and the selection of a specific one is dependent on the relatively tight constraints in small devices. The selected algorithm should be small, relatively secure, with a proven history of overcoming possible well known attacks on it.

Advanced Encryption Standard [14] is the most popular block cipher which is used everywhere for encryption. It is mainly designed for software implementation. So it is not suitable for extremely constrained environments like Radio-frequency identification (RFID) tags and sensor networks.The Tiny Encryption Algorithm (TEA) [1] for such type of application has been proposed by Wheeler and Needham.Its successor the Extended-TEA or XTEA has been introduced in [8].Several attacks against XTEA have been reported in [3, 4, 5, 6, 9].

Manuscript received on April 26, 2012.

Niladree De, Department of Electronics and Communication Engineering, Haldia Institute of Technology, Purba Medinipur, India (e-mail: mtech.niladri.10@gmail.com).

JaydebBhaumik, Department of Electronics and Communication Engineering, Haldia Institute of Technology, PurbaMedinipur, India (e-mail: bhaumik.jaydeb@gmail.com).

A nonlinear Boolean function Nmix and its inverse I-Nmix have been introduced in [13]. In this paper a modified XTEA was proposed. Here a new nonlinear Boolean Nmixfunction has been used during encryption and I-Nmix is used in decryption. Whereas in original XTEA, additionmodulo 232is used during encryption and subtraction modulo 232is employed during decryption.

The rest of the paper is organized as follows: Next section provides a brief overview of Extended Tiny Encryption Algorithm (XTEA). Existing attacks on block cipher XTEA introduced in section 3. Modified XTEA is introduced in section 4. VLSI implementation result of proposed architecture is presented in section 5 andfinally the paperis concluded in section6.

II. BRIEF OVERVIEW OF XTEA

The Extended Tiny Encryption Algorithm (XTEA) is a block cipher that uses a cryptographic key of 128 bits to encrypt or decrypt data in blocks of 64 bits. Each input block is split into two halves Ln andRnwhich are then applied to a routine similar to a Feistel network for N rounds, where N is typically 32. Most Feistel networks apply the result of a mixing function to one half of the data using XOR as a reversible function. On the other hand,XTEA uses integer addition modulo 232 during encryption and subtraction modulo 232during decryption.Operations used in XTEA are just exclusive-or, additions and shifts for encryption.

In case of XTEA 64 bit input is divided into two 32 bits variables (Ln, Rn). The variables Ln,Rnand sub-key, have a length of 32 bits. All additions and subtractions within XTEA are modulo 232. Logical left shifts of Rn by 4 bits are denoted as Rn<< 4 and logical right shift by 5 bits as Rn>> 5. The symbol'⊕' denotes the bitwise XOR operation.The constant δ has value of 9e3779b9x and (Ln,Rn) are the inputsof the n-th round, for 1≤n≤64. The corresponding output of the n-th round is (Ln+1,Rn+1), where Ln+1 = Rn and Rn+1is computed using following equations:

For each i (1≤ i ≤32),

If n = 2i – 1

$$R_{n+1} = L_n \boxplus (((R_n \ll 4 \oplus R_n \gg 5) \boxplus R_n) \oplus ((i-1).\delta \boxplus K((i-1).\delta \gg 11) \& 3)$$

And if n = 2i,

$$R_{n+1} = L_n \boxplus (((R_n \ll 4 \oplus R_n \gg 5) \boxplus R_n) \oplus (i.\delta \boxplus K(i.\delta \gg 11) \& 3)$$

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

XTEA has a very simple key schedule: the 128-bit master key K is split into four 32-bit blocks K0, K1, K2 and K3. Then, for r = 1, · · ·, 64, the round keys $K_r$are derived from the following equation:

$$K_r = K_{(\frac{r-1}{2}.\delta \gg 11)\&3}\,, if\ r\ is\ odd;$$

$$K_r = K_{(\frac{r}{2}.\delta \gg 11)\&3}\,, if\ r\ is\ even;$$

As shown in Fig. 1, XTEA has a very simple round function.

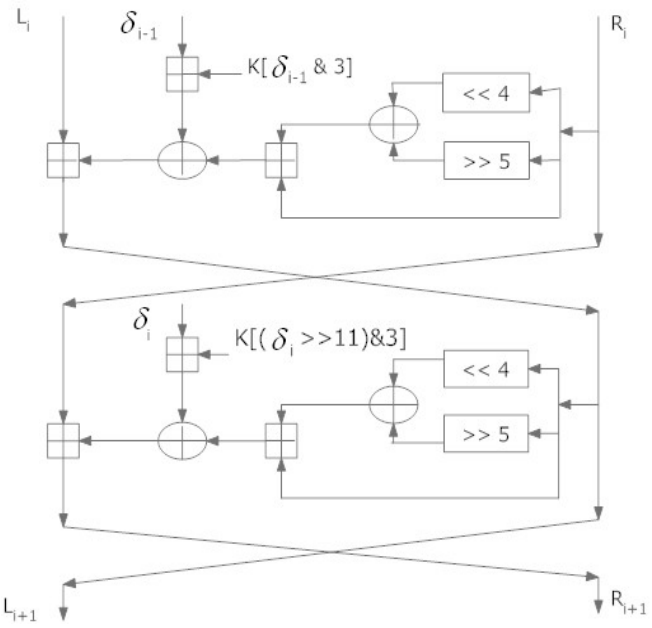

Fig.-1:Two Feistel rounds (one cycle) of XTEA

III. EXISTING ATTACKS ON XTEA

There exist various adversary models that are classifiedwith respect to the operations on the inputs and outputs of the cipher (i.e. plaintext, ciphertext and key) the adversary is allowed to perform. Normally, one distinguishes between such operations as reading access (known values), writing access (chosen values) and adaptive writing access (adaptively chosen values). In this section, different existing attacks on XTEA have been discussed.

Chosen plaintext attacks: The adversary can choose plaintexts to be encrypted by the cipher prior to the attack and has reading access to the corresponding ciphertexts during the attack. The most known attack of this kind is differential cryptanalysis.Biham'et al. [8] developed differential cryptanalysis method to attack block ciphers. This attack is the general method of attacking cryptographic algorithms. It has exposed the weakness in many algorithms. It looks specifically at ciphertext pairs: pairs of ciphertexts whose plaintexts have particular differences and analyzes the evolution of these differences as the plaintexts propagate through the rounds of the encryption algorithm when they are encrypted with the same key. The two plaintexts (with a fixed difference) can be chosen at random as long as they satisfy particular differences. Then, using the differences in the resulting ciphertexts, assign different probabilities to different keys. As we analyze more and more ciphertexts, one key will emerge as the most probable or correct key.Differential cryptanalysis on TEA and XTEA has been reported in [5].

A 12-round impossible differential characteristic of XTEA:

Moon et al. presented animpossibledifferential cryptanalysis on reduced round XTEA in [4]. For sake of completeness a construction of a 12-round impossible differential characteristic of XTEAis discussed here. Let an input difference be

$(A_x a_1 a_2 10\ 0_x0_x0_x0_x0_x0_x \,||\, b_1000\ 0_x0_x0_x0_x0_x0_x0_x)\ldots$ (1)

Then the difference after round 6 must be of the form

$(N_xO_xP_xQ_xR_xS_xf_1f_210\ 0_x \,||\, T_xU_xV_xW_xX_xY_xZ_xg_1g_2g_31)\ldots$ (2)

On the other hand, we can predict the difference after round 6 from the outputdifference of round 12, i.e., to consider the differentials in the backward direction. Similarly to the 6-round differential characteristic with probability 1, there is a backward 6-round differential characteristic with probability 1. It has the difference

$(a_1000\ 0_x0_x0_x0_x0_x0_x0_x \,||\, A_x\ b_1b_210\ 0_x0_x0_x0_x0_x0_x)\ldots$ (3)

After round 12, and then it is clear that the difference after round 6 must be ofthe form

$(T_xU_xV_xW_xX_xY_xZ_xg_1g_2g_31 \,||\, N_xO_xP_xQ_xR_xS_xf_1f_210\ 0_x)\ldots$ (4)

Combining these two differential characteristics, it can be conclude that any pair with input difference (1) before round 1 and output difference (3) after round 12 must have differences of the form (2) = (4) after round 6. But this event never occurs.Therefore, this characteristic is a 12-round impossible characteristic of XTEA.

8-Round Related Key Truncated Differential Characteristic:

An 8-round truncated differential characteristic in order to attack 23 rounds of XTEA has been reported in [6]. Here, an 8-round related key truncated differential characteristic is constructed. Let Ψ be our 8-round related key truncated differential characteristic described.

The following section describes the proposed modified XTEA.

IV. MODIFIED XTEA

In this section we discuss about modified XTEA. The basic operators like left shift (<<), right shift (>>), xoroperation (⊕) are same as previous version of XTEA. But, here we replaced the modulo addition and subtraction 2^{32} by a functionNmixand I-Nmix during encryption and decryption respectively.In Figure 2, the $F_{l\rightarrow r}$ and $F_{l\leftarrow r}$ function are the Nmixfunction operating from most significant bit to least significant bit and least significant bit to most significant bit respectively.

Proposed Architecture:

Here two inputs plaintext are Y_i and Z_i both are 32 bits, but for the Nmixand I-Nmix we used four 8 bit parallel operations. i.e, for both LSB and MSB operation we used bitwise operation.

Nmix: The function Nmix operates on two n-bit variables $X=(x_{n-1}\ x_n\ldots.\ x_0)$ and $K=(k_{n-1}k_{n-2}\ldots..\ k_0)$ and produces an n-bit output variable $Y=(y_{n-1}y_{n-2}\ldots.\ y_0)$, where Y=F(X,K) and F is the Nmix function. Each output bit of Nmixis related to the input bits by the following relationship

$$Y_i = x_i \oplus k_i \oplus c_{i-1}$$

$$c_i = \oplus_{j=0}^{i} x_j k \oplus x_{i-1}.x_i \oplus k_{i-1}.k_i$$

Where $0 \le i \le n-1$, $c_{-1} = 0$, $x_{-1} = 0$, $k_{-1} = 0$ and c_i is the carry term propagating form i-th bit position to (i+1)-th bit position. Each output bit Y_i is balanced for all i, where $0 \le i \le n-1$.

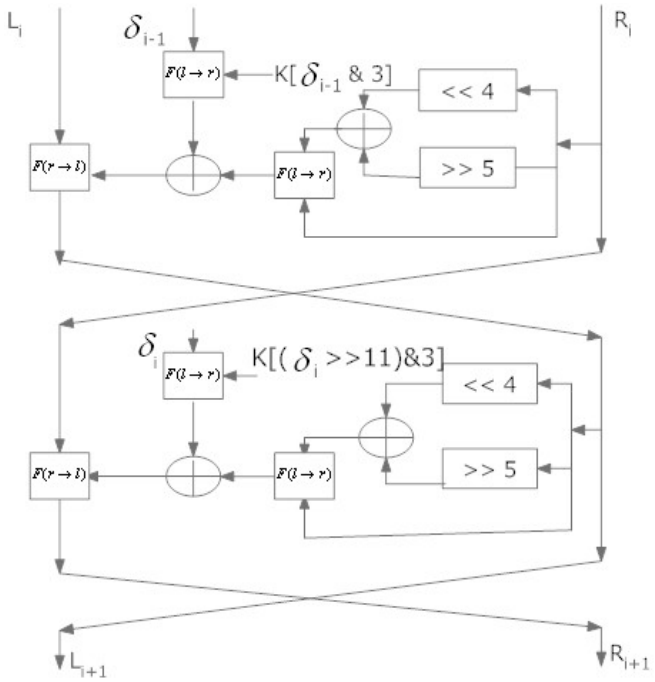

Fig.-2: Modified XTEA One Round Architecture

I-Nmix :- In inverse mixing the mixer takes two n-bits variables $Y=(y_{n-1}y_{n-2}\ldots\ldots y_0)$ and $K=(k_{n-1}k_{n-2}\ldots\ldots k_0)$ as input and produces an n-bit output $X=(x_{n-1}\ x_{n-2}\ \ldots\ldots\ x_0)$, where X=G(Y,K) and G is the I-Nmixfunction . Inverse mixing function is defined as follows.

$$X_i = y_i \oplus k_i \oplus d_{i-1}$$

$$d_i = \oplus_{j=0}^{i} y_j.k_j \oplus y_{i-1}.y_i \oplus k_{i-1}.k_i$$

Where $0 \le i \le n-1$, $d_{-1}= 0$, $x_{-1} = 0$, $k_{-1} = 0$ and d_i is the carry term propagating form i-th bit position to (i+1)-th bit position. Function G is the inverse function of the function F.

Key Schedule: In ModifiedXTEA we used same key schedule algorithm as on. The 128 bit master key K is split into four 32 bits blocks K_0 ,K_1 ,K_2 ,K_3 .Then for r = 1,2,….,64, the round keys $K_r$are derived from the following equation :

$$K_r = K_{(\frac{r-1}{2}.\delta \gg 11)\&3}, if\ r\ is\ odd;$$

$$K_r = K_{(\frac{r}{2}.\delta \gg 11)\&3}, if\ r\ is\ even;$$

Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Key	K_0	K_3	K_1	K_2	K_2	K_1	K_3	K_0	K_0	K_0	K_1	K_3	K_2	K_2	K_3	K_1
Round	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Key	K_0	K_0	K_1	K_0	K_2	K_3	K_3	K_2	K_0	K_1	K_1	K_1	K_2	K_0	K_3	K_3
Round	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
Key	K_0	K_2	K_1	K_1	K_2	K_1	K_3	K_0	K_0	K_3	K_1	K_2	K_2	K_1	K_3	K_1
Round	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
Key	K_0	K_0	K_1	K_3	K_2	K_2	K_3	K_2	K_0	K_1	K_1	K_0	K_2	K_3	K_3	K_2

Fig.-3: Key Schedule of ModifiedXTEA

V.IMPLEMENTATION RESULTS ANDCOMPARISON

Every architectural module has been implemented in Verilog and simulated using Model Sim XE III 6.0a. The design has been synthesized by Xilinx ISE 7.1i tool and the target FPGA device was Spartan3 XC3S5000 which provides Low-cost, high-performance logic solution for high-volume, consumer-oriented applications, is used as target device.It produces a maximum frequency of 67.37 MHz and using 1% of slices and input LUTs. Among compact architectures this described design is one of the smallest and better performance architecture. The following table shows performance characteristics of different model of XTEA.

Design	Minimum period (ns)	Clock Cycles	Area (slices)	Frequency (MHz)	Throughput (Mbps)	Throughput/ area (Mbps/slice)
Modified XTEA	14.84	33	238	67.37	130.66	0.55
XTEA	23.21	33	320	43.08	83.55	0.26
Tiny XTEA-1	13.87	240	266	71.25	19	0.07
Tiny XTEA-3	15.97	112	254	66.5	36	0.14
AES 8-bit	14.93	3900	264	60.93	2	0.01

Fig.-4: Results for half-round Modified XTEA compared to different block ciphers

Proposed design gives an acceptable tradeoff between area and the throughput. The modified XTEA gives better throughput of 130.66 Mbps and requires 238 Slices.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

VI. CONCLUSIONS

The Modified XTEAarchitecture iswell suited for devices in which low cost and low power consumption are desired.The proposed folded architecture achievesgood performance and occupies less area than XTEA. Thiscompact design was developed by thorough examination of each of the components of the Modified XTEA algorithm. The proposed implementation can be accommodated in a very inexpensive Xilinx Spartan-3FPGAXCS5000. The encryption speed, functionality, and costmake this solution perfectly applicable for resource constrained applicationspassive RFIDandwireless sensor networks.

REFERENCES

1. D. Wheeler, R. Needham, “TEA, a Tiny Encryption Algorithm,” FSE 1994, LNCS, Springer-Verlag, vol. 1008, 1995, pp. 97-110.
2. J.P. Kaps, “Chai-tea, cryptographic hardware implementations of XTEA,”INDOCRYPT2008, LNCS, vol. 5365, HeidelbergSpringer, 2008, pp. 363-375.
3. L. Jiqiang ,"Related-key rectangle attack on 36 rounds of the XTEA block cipher," *International Journal of Information Security*, vol. 8 , no.1, 2009, pp. 1-11.
4. D. Moon, K. Hwang, W. Lee, S. Lee, and J. Lim, “Impossible Differential Cryptanalysis of Reduced Round XTEA and TEA”, Fast Software Encryption ’02, LNCS, Springer-Verlag,vol. 2365, 2002, pp. 49-60.
5. S.Hong,D. Hong,Y.Ko, D.Chang, W. Lee, S. Lee,“Differential cryptanalysis of TEA and XTEA,”ICISC 2003, vol. 2971, Springer Heidelberg,2004, pp. 402–417.
6. Y.Ko, S. Hong, W.Lee, S.Lee, Kang, and J. Lim, "Related key differential attacks on 27 rounds of XTEA and full rounds of GOST," *FSE '04*, LNCS, vol. 3017,2004,pp. 299-316.
7. E. Biham and A. Shamir, “Differential Cryptanalysis of the DES-like Cryptosytems,” CRYPTO 1990,LNCS, Springer-Verlag,vol. 537, 1990**,** pp.187-195
8. R. Needham and D. Wheeler, “eXtended Tiny Encryption Algorithm, ”Technical Report, Cambridge University,England, Oct. 1997.
9. J. Cesar, H. Castro and P. I. Vinuela, “New results on the genetic cryptanalysis of TEAand reduced-round versions of XTEA,” Journal of New Generation Computing, vol. 23, no. 3, 2005, pp. 233-243.
10. C. H. Lim and T. Korkishko,“mCrypton - A Lightweight Block Cipher for Security of Low-Cost RFIDTags and Sensors,” WISA, LNCS, Springer, vol. 3786,2005**,** pp. 243–258.
11. D.Wagner, “The boomerang attack,” Fast SoftwareEncryption Workshop, LNCS, Springer Heidelberg, vol. 1636, 1999**,** pp. 156–170.
12. E. Lee, D. Hong, D. Chang, S.Hong, J. Lim “ A weakkey class of XTEA for a related-key rectangle attack,” VIETCRYPT, LNCS, vol. 4341, 2006, pp. 286-297.
13. J. Bhaumik, and D. Roy Chowdhury, “Nmix: An Ideal Candidate For Key Mixing,” Proc. of Int. Conf. on Security and Cryptography (Secrypt), Milan, Italy, July 2009, pp. 285-288.
14. J.Daemen and V.Rijmen. “The Design of Rijndael - AES The Advanced Encryption Standard, “ Springer-Verlag, 2002.

AUTHORS PROFILE

Niladree De isa M. Tech. student in the Department of Electronics and Communication Engineering, Haldia Institute of Technology, Haldia, PurbaMedinipur, India. He received his B. Tech. degree inElectronics and Instrumentation Engineering from West Bengal University of Technology in the year 2010. His research interests include Digital VLSI Design and Cryptography.

Jaydeb Bhaumikis currently working as an Associate Professor in the Department of Electronics and Communication Engineering, HaldiaInstitute of Technology, Haldia, India. He obtained his PhD degreefrom G. S. Sanyal School of Telecommunications, Indian Institute ofTechnology Kharagpur, India in 2010. He received his B. Tech. and M.Tech. degrees in Radio Physics and Electronics from University ofCalcutta in 1999 and 2001 respectively. His research interests includeCryptography, Cellular Automata, Error Correcting Codes, and DigitalVLSI Design. He is a member of IEEE and Cryptology Research Society ofIndia.