Journal of Computer Science 10 (6): 1077-1083, 2014
ISSN: 1549-3636

doi:10.3844/jcssp.2014.1077.1083 Published Online 10 (6) 2014 (http://www.thescipub.com/jcs.toc)

IMPLICATIONS OF BITSUM ATTACK ON TINY ENCRYPTION ALGORITHM AND XTEA

Amandeep and G. Geetha

School of Computer Applications, Lovely Professional University, Phagwara, India

Received 2013-12-07; Revised 2014-01-05; Accepted 2014-02-03

ABSTRACT

TEA and XTEA are block ciphers that uses Fiestal structure. We enciphered a fixed message with different keys using TEA and XTEA cryptographic algorithms. Our interest was to find the correlation of the bitsum of the ciphertext with the bitsums of the corresponding keys. In our attempt, we found that for specific patterns of keys, whatever be the plaintext, the bitsum of the key is in perfect correlation with bitsum of the ciphertext.

Keywords: TEA, XTEA, Cryptanalysis, Bitsum

1. INTRODUCTION

Wheeler and Needham (1994) proposed Tiny Encryption Algorithm, a Fiestal cipher that is using many iterations rather than complicated coding (Wheeler and Needham, 1994). A single bit change in the plain text can make up to 32 bits change in the Cipher Text. TEA performs very efficiently on modern computers and hand held devices.

The easy implementation of TEA has made it a very popular and is being used in electronic product development, PDA data encryption, smart card encryption, embedded systems.

David Wagner has informed the developers of TEA that TEA has two minor weaknesses Needham and Wheeler (1997) through an e-mail. To overcome those weaknesses, Needham and Wheeler (1997) presented XTEA, which is a block cipher with 64-bit block size and 128 bit key. XTEA is retaining the simplicity and efficiency of TEA. It has some rearrangements of XORs and shifts and it has a more complex key schedule.

2. CRYPTANALYSIS

Cryptanalysis is the science of breaking the cryptographic ciphers. We have some Ciphertext produced by some algorithm and we try to produce plaintext or, better, the KEY. Schneier (1996) there are four general types of cryptanalytic attacks. All these attacks assume that the cryptanalyst has complete knowledge of the encryption algorithm used.

2.1. Ciphertext-Only Attack

In this type of attack, the cryptanalyst has the Ciphertext of a number of messages, all of these messages are encrypted with same encryption algorithm. The job of the cryptanalyst is to recover the plaintext from all available Ciphertext or as many as possible.

2.2. Known-Plaintext Attack

In such kind of attack, the cryptanalyst has the Ciphertext of numerous messages as well as their plaintext also. So his job now is to deduce the key used to encrypt the messages or algorithm, so that any other messages encrypted with the same key can also be decrypted.

2.3. Chosen-Plaintext Attack

In this type of attack, the cryptanalyst has access to the Ciphertext and their associated plaintext for a number of messages, but also he chooses the plaintext which gets encrypted.

Corresponding Author: Amandeep, School of Computer Applications, Lovely Professional University, Phagwara, India

2.4. Adaptive-Chosen-Plaintext Attack

This type of attack is a special case of chosen-plaintext attack. In such kind of attack, the cryptanalyst can choose the plaintext that is being encrypted and he can also amend his choice based on the outcomes of the previous encryption.

3. CRYPTANALYSIS OF TEA

Some of the attacks on TEA are mentioned below:

- Moon *et al*. (2002) showed impossible differential cryptanalysis of TEA on reduced rounds. They exploited the design simplicity of TEA and XTEA on the reduced rounds
- Saarinen (1998) did cryptanalysis of Block TEA. This attack was characterized as a differential attack
- Andem (2003) Reddy found some of the weaknesses of TEA. But encryption with more than six rounds shows resistance against cryptanalytic attacks and his research also concludes that TEA is a best fit algorithm for small devices
- Hernandez and Isasi (2004) had shown that TEA with less than five rounds is not robust against the proposed distinguisher and should not be used for cryptographic purposes
- Mirza (1998) presented a report in which he presented the design and cryptanalysis of variants of TEA
- Shoeb and Gupta (2013) proposed study on TEA for random number generator tests

4. CRYPTANALYSIS OF XTEA

- Lu (2009) presented Related-key rectangle attack on 36 rounds of the XTEA block cipher
- Moon *et al*. (2002) presented Impossible Differential Cryptanalysis of Reduced Round XTEA and TEA.
- Sekar *et al*. (2011) presented meet in the middle attack on reduced rounds of XTEA
- Lee *et al*. (2006) gave a class of weak keys for which makes 34 round XTEA vulnerable to the related key rectangle attack
- Hong *et al*. (2003) has presented differential and truncated differential attacks on TEA and XTEA
- Youngdai *et al*. (2004) had presented related key truncated differential attack on 27 rounds of XTEA

5. PROPOSED METHOD

We presented a novel bit sum attack Geetha and Bagga (2011) and is same is reproduced here for the better understanding of the paper:

a. Choose a cipher to be investigated.
b. Loop
    i. For cipher under investigation, we will encipher a fixed message M with N different keys
    ii. Calculate the correlation of the bitsums of the cipher texts produced with the bitsums of the corresponding keys.

    End Loop
c. We will keep track of which message yields the best correlation between bitsums of ciphertext and key.
d. Conclusions will be drawn on the basis of this record.

We applied the above Bitsum attack on XOR cipher Bagga and Geetha (2012). The results we obtained encouraged us to proceed further. We applied to TEA of key size 64 bits and the results were amazing. We concluded in Amandeep and Geetha (2012) that, if bit sum of the key is less than 14 or greater than 50, then there is strong correlation between the bitsum of the ciphertext and the bitsum of the key.

In same lines we continued to attack TEA with 128 bit key size. The results we obtained are presented are in this study.

6. IMPLEMENTATION

TEA is the Cipher to be investigated. We enciphered at around 10000 messages and around 50000 records were generated to be analysed. The random key was generated to encipher the message. We tried to find the correlation between the BitSum of the cipher Text and BitSum of the Key. We got the values of correlation coefficient for each and every message.

While doing the analysis of the data, we realized that there is a pattern of the key, for which value of the BitSum of the Ciphertext remains constant for every plaintext. Then to find the fact we kept the key constant and changed the plaintext several times. It was seen that result is true for some specific patterns of the key.

Table 1. TEA values for analaysis

Key (k) from the Set (K)	BitSum of the Plain Text	Bitsum of the Key	Bitsum of the Ciphertext
00000000000000000000000	14	16	37
00000000000000000000000			
00000000000000000000000			
00000000000000000000000			
00000000000000011111111111111			
00000000000000000000	16	16	37
00000000000000000000000			
00000000000000000000000			
00000000000000000000000			
00000000011111111111111			
00000000000000000000	19	16	37
00000000000000000000000			
00000000000000000000000			
00000000000000000000000			
00000000000000011111111111111			
00000000000000000000	23	16	37
00000000000000000000000			
00000000000000000000000			
00000000000000000000000			
00000000000000011111111111111			

In this research, we deduced a set of keys:

K = {0000....1, 0000....11, 0000....111, 0000....1111, 0000....11111 and so on upto 01111....1,
1000....0, 1100....0, 1110....0, 11110....0 and so on upto 11111.....10 and
00..010..00, 00..0110..00, 00..111..00, 00..1111..00 and so on upto 0111..1110}

For any key out of this set, the Bitsum of the Ciphertext is constant, no matter what is the plaintext.

For example, let's say the key:

k Є K is
00000000000000000000……00000000000000000
000000111111111111111

The resulting values are listed in the **Table 1**.

From the above example we can see that, when we have a constant value of the bitsum of the Ciphertext, then we can guess the pattern of the key. It may belong to the set of the keys which we deduced.

Values of XTEA are listed in the **Table 2**.

7. RESULTS

We got specific patterns of the key for which Bitsum of the Ciphertext remains constant. Those patterns of the keys are shown below:

M1, M2……Mn are the messages to be encrypted. K1, k2…..Kn are the keys. C1, C2,…Cn are going to be the BitSum of the Ciphertext.

Case 1:

Key pattern K1: The set of randomly generated messages are encrypted with TEA encryption routine. When all these messages were encrypted using K1, then we found that Bitsum of the Ciphertext produced C1 was constant. This result is depicted in the **Fig. 1** below.

Case 2:

To analyse the results further we took another key of the same type. Then again the messages were generated randomly and were encrypted with K2 (the next key pattern). Again we got same kind of results i.e., the bitsum of the Ciphertext (C2) was constant. Results are depicted in the **Fig. 2**.

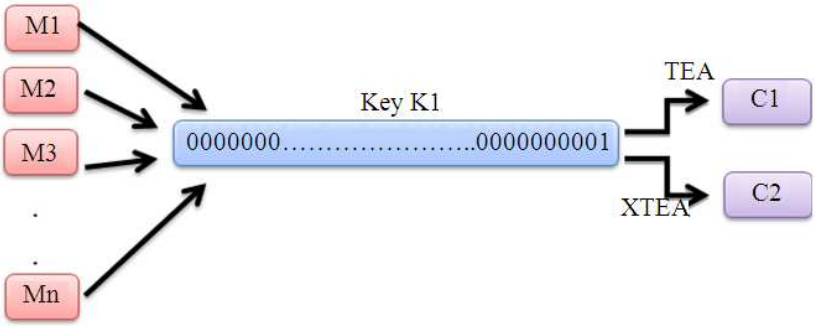

Fig. 1. Result 1

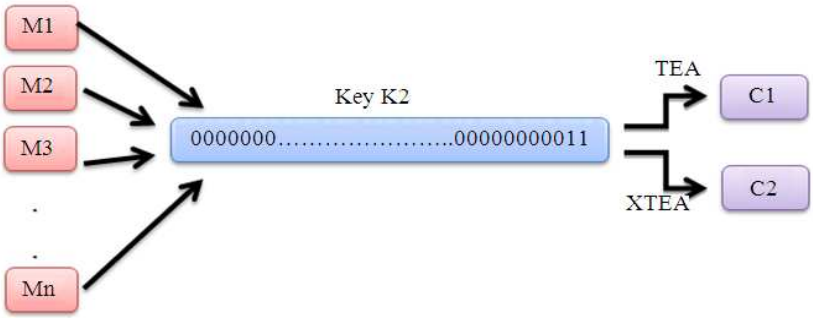

Fig. 2. Result 2

Case n:

We analysed all such patterns of the key and got same kind of results. The **Fig. 3** below is showing the results for Key pattern Kn.

After doing this experimentation, we tried on the keys having such a pattern in the reverse order. By reversing the order of placing of all the 1's, the results of this experiment remained same. We are showing these results in the following diagrams.

Case 1:

We again generated the random messages and encrypted those messages with the Key pattern K1. Results are shown in the diagram below **Fig. 4**.

Case 2:

Same kind of experiment was done with Key pattern K2 and results are shown in the diagram below **Fig. 5**.

Case n:

This experiment was also conducted for all such patterns of the keys and we found similar results for all such keys. Now at the end, the results for Key pattern Kn are shown below **Fig. 6**.

Whenever we get a pattern of the key where we get some number of 1s together and all other bits are 0s, then also we get constant bitsum of the Ciphertext.

For example, M1, M2……Mn are the messages to be encrypted and C is a constant, which is representing bitsum of the Ciphertext.

Then encrypt all such messages with the Key of such a pattern, the bitsum of the Ciphertext remain same. This is also depicted in the **Fig. 7** below.

We know that for a symmetric encryption, Equation:

$$C \leftarrow ENC(m,k)$$
$$m \leftarrow DEC(c,\ k)$$

Where:
C = The Ciphertext
ENC = The encryption algorithm
DEC = The decryption algorithm
m = The plaintext/message to be encrypted
k = The key

7.1. The Key Pattern Theorem on TEA and XTEA

Key Pattern theorem on TEA and XTEA:

K = {0000....1, 0000....11, 0000....111, 0000....1111, 0000....11111 and so on upto 01111....1,
1000....0, 1100....0, 1110....0, 11110....0 and so on upto 11111.....10 and
00..010..00, 00..0110..00, 00..111..00, 00..1111..00 and so on upto 0111..1110}
M = { m1, m2, m3,……m_n} where n represents 2^{64}.

Considering k Є K and m_i Є M and computing:

C = $ALG_e(m_i, k)$
m_i = $ALG_d(C,k)$
C_{BS} = $ALG_e(m_i, k)$ is constant for constant Bitsum of Key for whatever value of m_i

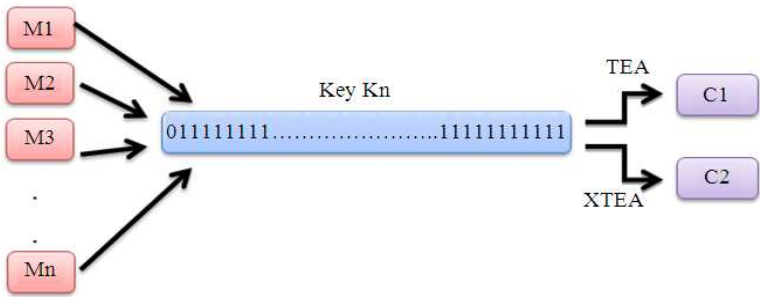

Fig. 3. Result 3

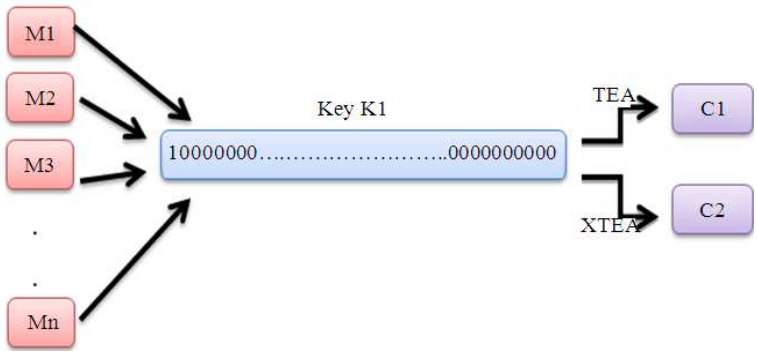

Fig. 4. Result 4

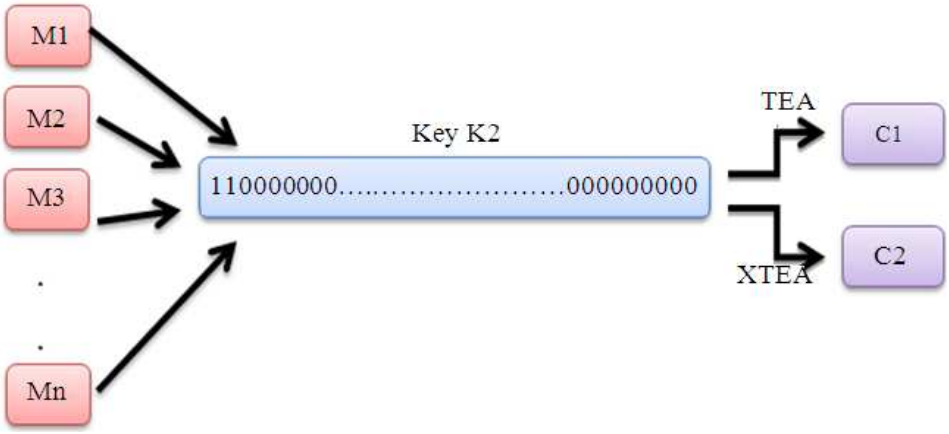

Fig. 5. Result 5

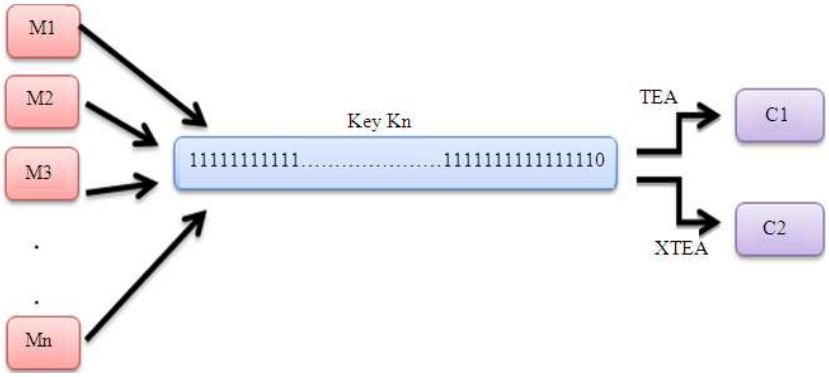

Fig. 6. Result 6

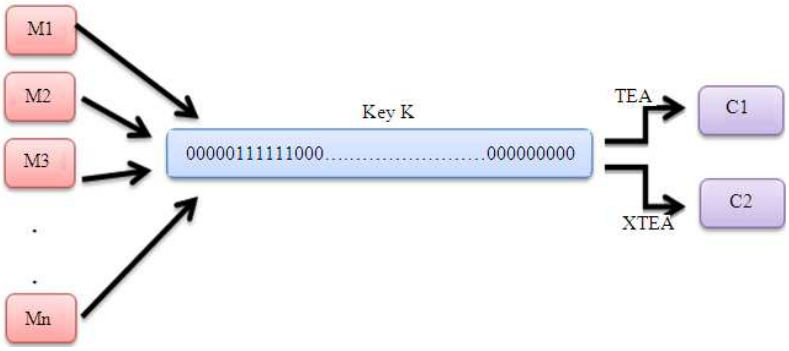

Fig. 7. Result 7

Table 2. XTEA values for analysis

Key (k) from the Set(K)	BitSum of the Plain Text	Bitsum of the Key	Bitsum of the Ciphertext
00000000000000000000000000000000	14	16	31
00000000000000000000000000000000			
00000000000000000000000000000000			
00000000000000000000000000000000			
00000000000000111111111111111			
00000000000000000000000000000000	16	16	31
00000000000000000000000000000000			
00000000000000000000000000000000			
00000000000000000000000000000000			
00000000000000111111111111111			
00000000000000000000000000000000	19	16	31
00000000000000000000000000000000			
00000000000000000000000000000000			
00000000000000000000000000000000			
00000000000000000000000000000000			
00111111111111111			
00000000000000000000000000000000	23	16	31
00000000000000000000000000000000			
00000000000000000000000000000000			
00000000000000000000000000000000			
00000000000000000000000000000000			
00000111111111111111			

Where:
ALG_e = Encryption routine of TEA or XTEA
ALG_d = The decryption routine of TEA
C_{BS} = The Bitsum of the CipherText

8. CONCLUSION

We presented Bitsum Attack on TEA and XTEA. Results were found based on the bitsum of the ciphertext and bitsum of key. There is a strong correlation between bitsum of the key with a particular pattern and bitsum of the corresponding ciphertext. Our experiment had shown that a set of keys in TEA and XTEA is not secure under Bitsum Attack. In future we will experiment this attack on other block ciphers, preferably which are using XOR in their functioning.

9. REFERENCES

Amandeep, A. and G. Geetha, 2012. On the security of reduced Key Tiny encryption algorithm. Proceedings of the International Conference on Computing Sciences, Punjab, Sept. 14-15, IEEE Xplore Press, Phagwara, pp: 323-326. DOI: 10.1109/ICCS.2012.51

Andem, V., 2003. A cryptanalysis of the tiny encryption algorithm. The Msc Thesis, Department of Computer Science, University of Alabama, Tuscaloosa.

Bagga, A. and G. Geetha, 2012. Implications of bitsum attack on XOR. Proceedings of the 2nd National Conference on Emerging Trends in Computer Application, Chennai, pp: 47-50.

Geetha, G. and A. Bagga, 2011. Bit sum attack. Security J., 35: 21-22.

Hernandez, J.C. and P. Isasi, 2004. Finding efficient distinguishers for cryptographic mappings, with an application to the block cipher TEA. Compuat. Intell., 20: 517-525. DOI: 10.1111/j.0824-7935.2004.00250.x

Hong, S., D. Hong, Y. Ko, D. Chang and W. Lee, 2003. Differential cryptanalysis of TEA and XTEA. Proceedings of the 6th International Conference Information Security and Cryptology, (SC' 03), Springer Berlin Heidelberg, pp: 402-417. 10.1007/978-3-540-24691-6_30

Lee, E., D. Hong, D. Chang, S. Hong and J. Lim, 2006. A weak key class of XTEA for a related-key rectangle attack. Progress Cryptol., 4341: 286-297. DOI: 10.1007/11958239_19

Lu, J., 2009. Related-key rectangle attack on 36 rounds of the XTEA block cipher. Int. J. Inform. Sec., 8: 1-11. DOI: 10.1007/s10207-008-0059-9

Mirza, F., 1998. Block Ciphers and Cryptanalysis. Royal Holloway University of London, Department of Mathematics, England.

Moon, D., H. Kpngdeok, W. Lee, S. Lee, 2002. Impossible differential cryptanalysis of reduced round XTEA and TEA. Proceedings of the 9th International Workshop Fast Software Encryption, Feb. 4-6, Springer Berlin Heidelberg, Belgium, Springer, pp: 49-60. DOI: 49-60. 10.1007/3-540-45661-9_4

Needham, R.M. and D.J Wheeler, 1997. TEA extensions. Technical report, the Computer Laboratory, University of Archive.

Saarinen, M.J., 1998. Cryptanalysis of block TEA, unpublished manuscript.

Schneier, B., 1996. Applied Cryptography. 2nd Edn., John Wiley and Sons, ISBN-10: 0471117099, pp: 758.

Sekar, G., N. Mouha, V. Velichkov and B. Preneel, 2011. Meet-in-the-middle attacks on reduced-round XTEA. Topics Cryptol., 6558: 250-267. DOI: 10.1007/978-3-642-19074-2_17

Shoeb, M. and V.K. Gupta, 2013. a crypt analysis of the tiny encryption algorithm in key generation. Int. J. Commun. Comput. Technol., 1: 123-128.

Wheeler, D.J. and R.J. Needham, 1994. TEA, a tiny encryption algorithm. Proceedings of the 2nd International Workshop on Fast Software Encryption, (WFSE' 94).

Youngdai, K., S. Hong, W. Lee, S. Lee and J.S. Kang, 2004. Related key differential attacks on 27 rounds of XTEA and full-round GOST. Fast Software Encrypt., 3017: 299-316. DOI: 10.1007/978-3-540-25937-4_19