**Far East Journal of Electronics and Communications**
*Proceedings of SHANNON* 100 - 3*rd Int. Conf. Comp. Sci.*, 2016

http://dx.doi.org/10.17654/ECSV3PI16169
Special Volume 3, Part I, 2016, Pages 169-176 **ISSN: 0973-7006**

# ON THE COMPLEXITY OF ALGORITHMS AFFECTING THE SECURITY OF TEA AND XTEA

**Amandeep and G. Geetha**

School of Computer Applications
Lovely Professional University
Punjab, India

## Abstract

Ciphers are vulnerable to different types of attacks which exploit them for their weaknesses. Since security is a vital and fundamental requirement in the current era of information system and communication process, even a little compromise can be detrimental. Whenever a security system is made, cryptanalysts over the world check it for robustness by opting different methods. Focusing on security of block ciphers, this paper mainly aims to discuss various types of attacks. This paper dwells on the complexity of Bitsum Algorithm but also classifies and compares different attacks based on their complexities. Five popular and strong algorithms were analyzed under Bitsum algorithm. FEAL, Blowfish, and AES were able to withstand Bitsum Attack whereas TEA and XTEA could not. This comparison has shown that the complexity of the Bitsum attack is least on Reduced TEA, TEA and XTEA.

## 1. Introduction

With proliferation of technology and networking becoming an integral part of life these days, network security assumes utmost importance. Vast

Conference held during April 8-9, 2016 at Lovely Professional University, Punjab, India.
Guest Editor: G. Geetha; Division of Research and Development, Lovely Professional University, Punjab, India.

amount of data is being communicated daily through the internet. The rapid expansion in the field information technology and secure transmission of confidential data has fetched the great deal of attention of the cryptologists all around the world. The conventional security mechanisms can only maintain the data security. Information could be accessed by any unauthorized user for malicious purpose. Therefore, it is necessary to update the security systems and their robustness. Cryptanalysis is the method adopted for the improvement of the cryptographic techniques. Development of the Bitsum algorithm is an initiative in this direction. Implications of this algorithm were checked on XOR [1] with good results. Based on this research, this algorithm was implemented on some other block ciphers to check its applicability. This paper discusses the results of the experimentation done on the selective block ciphers. Complexity of the Bitsum algorithm is also discussed in this paper. A comparative study of the cryptanalytic ciphers is also done in the last section of this paper.

## 2. Bitsum Algorithm

Bitsum is the sum of number of 1's in the given binary number. This Bitsum is used to design an algorithm to explore the possibility of having correlation between the Bitsum of Plaintext, Key, and Ciphertext in an encryption scheme.

A chosen Plaintext attack, "Bitsum algorithm" is formulated and implemented on some of the symmetric ciphers. The ciphers under study were analyzed to find the weaknesses in them. The algorithm steps are given below:

**Explanation of the algorithm**

(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 the message that yields the best correlation between Bitsums of ciphertext and key.

(d) Conclusions will be drawn on the basis of the obtained result.

Let us consider a cipher to be studied. Suppose key length is 64 bits. The brute force attack is the worst scenario which would test all $2^{64}$ keys. Now Bitsum of the key (Sum of the number of 1's) has to be calculated to reduce the keyspace. The worst case scenario here would be 32 ones, for which we would have ${}^{64}C_{32}$ (64 choose 32) possible keys.

It is proposed to investigate a chosen plaintext attack with the hope that there could be a specific message for which the Bitsum of the ciphertext would correlate with the Bitsum of the key. It is likely that the correlation may not be perfect, so a suggested range of values for the Bitsum of the key may be produced. Still, this would be a great savings over brute force. This has been the basis of our algorithm that was used to investigate the strength of symmetric ciphers.

## 3. Performance of TEA, XTEA, FEAL, BLOWFISH and AES (128, 192 & 256) based on Correlation Test

This section focuses on the comparative analysis of implementation of Bitsum Algorithm on selective block ciphers. These ciphers are TEA [2], XTEA [3], FEAL [4], BLOWFISH [5] and AES (128, 192 & 256) [6]. SPSS is used to do this analysis.

**Table 1.** Analysis of confusion and diffusion property of selective ciphers

| Algorithm | Significance Value of Bitsum of Plaintext – Ciphertext relation | Significance Value of Bitsum of Ciphertext – Key relation |
|---|---|---|
| **TEA/XTEA** | .000 | .000 |
| **FEAL** | .701 | .059 |
| **BLOWFISH** | .956 | .181 |
| **AES – 128** | .471 | .739 |

| | | |
|---|---|---|
| **AES – 192** | .229 | .446 |
| **AES – 256** | .929 | .239 |

Table 1 shows the significance values of the correlation test performed on the values of Bitsum of Plaintext, Bitsum of Ciphertext and Bitsum of Key. The second column of the table gives the significance value of relation between Bitsum of Plaintext and Bitsum of the Ciphertext which indicate the diffusion property of the respective algorithm.

Significance values of the relation between Bitsum of Ciphertext and Bitsum of Key are listed in the third column of the Table 1. This column indicates the confusion property of the ciphers.

We have used the .05 level of significance. Whereever the significance value of the test (for Bitsum of Ciphertext and Bitsum of Key) is > .05, this means that there is no correlation between the Bitsums of the keys and the cipher texts i.e. FEAL, BLOWFISH, AES - 128, AES - 192 and AES - 256 holds the confusion property.

In the similar way, whereever the significance value of the test (for Bitsum of Plaintext and Bitsum of Ciphertext) is > .05, this means that there is no correlation between the Bitsums of the keys and the cipher texts i.e. of FEAL, BLOWFISH, AES - 128, AES - 192 and AES - 256 holds the diffusion property.

The noticeable values are for TEA and XTEA, where the significance values are .000 in both the cases. That means these ciphers do not hold confusion or diffusion property. As a result, Bitsum algorithm poses a threat on TEA and XTEA.

## 4. Complexity of an Algorithm

To analyze an algorithm, it is important to study its complexity. This will give us an opportunity to compare its performance with other algorithms. To estimate the complexity of an algorithm, we must consider the least time it takes, the storage requirements, and the data it needs to be executed.

**The Big O Notation**

In order to be able to define the complexity of an algorithm, we must understand the 'O' notation. The O is known as the *Order* on which the rate of growth of a function is dependent. To explain this concept take the example of an equation, $T(n)$,

$T(n) = 6n^2 + 5n - 3$

$T(n) = O(n^2)$, which means that $T(n)$ grows at the rate of $n^2$.

**Formal Definition.** $f(n) = O(g(n))$ means there are positive constants $c$ and $k$, such that $0 \leq f(n) \leq cg(n)$ for all $n \geq k$. The values of $c$ and $k$ must be fixed for the function $f$ and must not depend on $n$ [7].

There are some common notations which are used for representing the complexity of the algorithms. Some of the common notations are given below:

**Table 2.** Common notations used for representing the complexity of the algorithms

| Notation | Name |
|---|---|
| $O(1)$ | Constant |
| $O(\log(n))$ | Logarithmic |
| $O(n)$ | Linear |
| $O(n^2)$ | Quadratic |
| $O(n^c)$ | Polynomial |
| $O(c^n)$ | Exponential |

**The Time and Space Complexity of Bitsum Algorithm**

The time and space complexity of Bitsum algorithm is in the order of **O(n),** which states that the order of growth of Bitsum algorithm is linear.

## 5. Applicability of Various Cryptanalytic Algorithms

In the security world, symmetric ciphers have been ruling since so many

years. So we have decided to implement this algorithm on some famous and strong symmetric ciphers to check its applicability. For this the selected algorithm were XOR, TEA, XTEA, FEAL, Blowfish and AES. The first algorithm to be implemented and analyzed against Bitsum Algorithm was XOR cipher. Taking motivation from DES, security of reduced key Tiny Encryption Algorithm has been analyzed. TEA and XTEA, FEAL, BLOWFISH and AES are also analyzed through Bitsum algorithm.

This section is devoted to the study of attacks implemented on the algorithms under consideration i.e. TEA, XTEA, FEAL, Blowfish and AES. In Table 4 we have summarized this analysis.

**Table 3.** Cryptanalytic attacks on the ciphers under study

| **Cryptanalytic Algorithms** | **TEA** | **XTEA** | **FEAL** | **BLOWFISH** | **AES** |
|---|---|---|---|---|---|
| Exhaustive search | **Yes** | **Yes** | **Yes** | **Yes** | **Yes** |
| Zero correlation [8] | **Yes** | **Yes** | No | No | No |
| Related Key [9] | **Yes** | **Yes** | No | No | **Yes** |
| Slide Attack [10] | No | No | No | **Yes** | No |
| Reflection Attack [11] | No | No | No | **Yes** | No |
| Bit Sum [12] | **Yes** | **Yes** | No | No | No |

From Table 3 summarizes the cryptanalysis of TEA, XTEA, FEAL, BLOWFISH and AES. Exhaustive search can be done on all the ciphers. Zero correlation attack is applicable on TEA and XTEA. Related key attack is pertinent on TEA, XTEA and AES. Slide attack is applicable on Blowfish. Reflection attack is applicable on Blowfish. Bitsum algorithm is able to cryptanalyze TEA and XTEA.

It can be observed from Table 3, that for comparing the performance of Bitsum algorithm, four algorithms/attacks can be considered. These four techniques are Exhaustive search, Zero correlation, related key and Bitsum algorithm. The comparison of these algorithms is done on the basis of their complexity.

The choice of the algorithms in Table 4 for the comparison is due to the

reason that all the three algorithms are used for the cryptanalysis of TEA and XTEA. Hence the Table 4 draws comparison for them only.

**Table 4.** Comparison of complexities of various algorithms

| **Cryptanalytic Algorithms** | **TEA** | **XTEA** | **Reduced Tiny Encryption Algorithm** [13] |
|---|---|---|---|
| Exhaustive search | $2^{128}$ | $2^{128}$ | $2^{64}$ |
| Zero Correlation | $2^{119.64}$ | $2^{120.71}$ | - |
| Related Key attack | $2^{32}$( with a condition of having $2^{23}$ chosen plaintexts) | $2^{104.33}$ | - |
| Bitsum | $2^{64}$ | $2^{64}$ | $2^{32}$ |

From the comparison table we can conclude that performance of the Bitsum algorithm is better than the other algorithms. Although complexity of related key attack is lesser, but it comes with a condition of having $2^{23}$ chosen plaintexts.

## 6. Conclusion

The idea behind this study was to find out the correlation between Bitsum of Ciphertext with Bitsum of Key or the Plaintext. On the basis of the results and analysis thereof, we sum up our findings as follows:

Blowfish and FEAL are secure algorithms as they have confusion and diffusion properties to hold. They maintain the requirements of good cipher.

TEA and XTEA have their own disadvantages as they have neither confusion nor diffusion property and therefore they are considered to be weak ciphers.

All the show confusion and diffusion property, so they are strong enough to provide security.

## References

[1] A. Bagga and G. Geetha, Implications of bitsum attack on XOR, Proc. 2nd National Conf. Emerging Trends in Comp. Appl., Chennai, 2012.

[2] D. Needham and R. Wheeler, TEA a tiny encryption algorithm, Proc. FSE, 1994.

[3] R. Needham and D. Wheeler, XTEA,
Available: https://en.wikipedia.org/wiki/XTEA. [Accessed 9 January 2016].

[4] A. Shimuzu and S. Miyaguchi, Fast data encipherment algorithm FEAL, Advances in Cryptology, Eurocrypt, 1987.

[5] B. Schneier, Description of a new variable-length key, 64-bit Block Cipher (Blowfish), in Springer-Verlag, Fast Software Encryption: Second International Workshop, Leuven, Belgium, 1994.

[6] V. Rijmen and J. Deamon, The design of rijndael: AES - the advanced encryption standard, 2002.

[7] P. E. Black, Big-O Notation, 31 August 2012.
Available: http://www.nist.gov/dads/HTML/bigOnotation.html.
[Accessed 4 February 2016].

[8] A. Bogdanov and M. Wang, Zero correlation linear cryptanalysis with reduced data complexity, Lecture Notes in Computer Science , 7549 (2012), pp. 29-48.

[9] J. Kelsey, D. Wagner and B. Schneier, Related-key cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X, NewDES, RC2, and TEA, First Intern. Conf. on Infor. and Commun. Security ICICS'97, London, 1997.

[10] D. Wagner and A. Biryukov, Slide attacks, International Workshop on Fast Software Encryption, Springer, Heidelberg, 1999.

[11] O. Kara and C. Manap, A New Class of Weak Keys for Blowfish, 14th International Workshop, FSE 2007, Luxembourg, March 26-28, Luxembourg, 2007.

[12] Amandeep and G. Geetha, Implications of bitsum attack on tiny encryption algorithm and XTEA, Journal of Computer Science, 10(6) (2014), 1077-1083.

[13] Amandeep and G. Geetha, On the security of reduced key tiny encryption algorithm, Inter. Conf. Comp. Sci. (ICCS), 2012 , Phagwara, 2012.