International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 04 | Apr -2017 www.irjet.net p-ISSN: 2395-0072

IMPOSSIBLE DIFFERENTIAL CRYPTANALYSIS ON REDUCED ROUND OF TINY AES

Mehak Khurana[1], Meena Kumari[2]

[1]Assistant Prof, Dept of Computer Science, The NorthCap Univerity, Gurugram, India
[2]Prof, Dept of Computer Science, The NorthCap Univerity, Gurugram, India

---

Abstract - *The emerging need of the secure ciphers has lead to the designing and analysis of many lightweight block ciphers. In this respect, many lightweight block ciphers have been designed, of which is simple AES, one of the popular proposed secure block ciphers is used in ubiquitous systems. In this paper, we evaluate the security of reduced round of simple AES (Tiny AES) against impossible differential cryptanalysis. Firstly the analysis of Tiny AES has been introduced. Secondly the impossible cryptanalysis on 5 rounds of Tiny AES has been analyzed which requires data complexity 2^{110} approximately and 2^{40}.memory accesses to recover the secret key which is better than exhaustive search.*

Key Words: Symmetric key ciphers, block ciphers, Tiny AES, Impossible differential cryptanalysis

1. INTRODUCTION

During the recent decade, it has become a challenge to design cryptographic primitives [1] to provide security with efficiency when limited hardware resources are available. Many lightweight block ciphers were designed to be used in devices used for storing and transmitting information securely. Some of the block cipher [2-3] having a structure derived from that of the AES are KLEIN, LED, Midori, Mysterion, SKINNY, Zorro. Some of the fiestel block ciphers are Hight, LEA, XTEA, Simon and Speck. Some block ciphers which have bit sliced S-Boxes are PRIDE, Rectangle, Noekeon. Some SPN structured ciphers are PRESENT, PRINCE, mCrypton. Some other two branched block ciphers are DESLX, MISTY, Lblock, KASUMI, SEA, and some Generalized Feistel Networks (GFN) ciphers are CLEFIA, Piccolo, TWINE.

Advanced Encryption Standard (AES) is an iterated block cipher that was selected in 2000 by NIST as an replacement of Data Encryption standard (DES) after a three year competition. It was declares as a national and international standard and was and still being used in many applications such as online banking, File transfer, voice calls etc. The AES has three versions called AES-128, AES-192, and AES- 256 where each version differ from another on the basis of the key length i.e. 128, 192, and 256 bits and have 10, 12, and 14 rounds respectively. Encryption of data through rounds is same in all three versions but the key generation process to generate number of subkeys differs in each version. NSA analyzed security of all three variants of AES thoroughly and declared that none version has any known vulnerability and can be used in protecting the storage and transmission of highly secret digital data.

Later on the situation started to change, different authors [4-5] started attacking on AES by recovering key with less complexity than brute force attack. All the attacks were similar attacks and fell in one category of mainly related key and subkey attack which had similar concept of key characteristic cancelation. This attack was launch on 192 and 256 version of AES. Further many other attacks were launched by finding the trails in AES.

2. Block cipher:

1.2 The AES Block Cipher

In 2001, AES block cipher was introduced by Joan Daemen, Vincent Rijmen.The AES (*Rijndael)* has 3 versions which have been standardized by the NIST, and Versions are AES-128, AES-192 and AES-256 where the number corresponds to the key size. The 128 bits AES in the encryption standard version which is also large enough to prevent any exhaustive key search. An encryption algorithm performs following operations and stores the state of 128 bits in 4x4 matrix a_{ij} of 16 bytes

$$\begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{bmatrix}$$

It consists of subbyte, shiftrow, mix column and add round key.

1. SubBytes: In parallel each byte in $GF(2^8)$ of a 4x4 matrix state is substituted by its corresponding byte in its defined 8 bit invertible S-box. The S-box is $S(a) = M(a^{-1}) \oplus C$ where a^{-1} represents multiplicative inverse, M represents matrix and C represents constant and a^{-1} is calculated in $GF(2^8)$ and is used because of it is highly non-linear.

2. ShiftRows: Each row is shifted to the left by its own row no-1. i.e first row of matrix is shifted by zero

towards left which means it is left untouched, second row is shifted by 1 to the left, third by 2 and those in the fourth by 3. This is to ensure diffusion between columns. The new a_{ij} state generated is

$$\begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{11} & a_{12} & a_{13} & a_{11} \\ a_{22} & a_{23} & a_{20} & a_{21} \\ a_{33} & a_{30} & a_{31} & a_{32} \end{bmatrix}$$

3. MixColumns: Each column is multiplied by an invertible MDS constant 4x4 matrix over $GF(2^8)$ field to ensure diffusion between the rows. Last round does not include column mixing to improve efficiency in decryption.

4. AddRoundKey: Key schedule algorithm generates succession of 128 bits keys using original key. The 128 bits for m^{th} round key k_m is placed into 4x4 matrix $k_{m_{ij}}$ each of 16 bytes. The each byte of $k_{m_{ij}}$ of subkey is XORed with current state a_{ij} i.e. $k_{m_{ij}} \oplus a_{ij}$.

It offers good hardware and software performance and is more efficient and secure than many other known block ciphers. For cryptographer, if an attacker can attack a cipher in fewer computations and faster than a brute force attack then it is a cryptographic break. Thus computations required against 128 bit key of AES are less than 2^{128} then it is considered a break of cipher, even though it takes 2^{112} computations which takes much longer time to be computed. Basic security analysis of AES has been done which shows resistance against attacks such as linear, differential and their variants. In order to speed up the algorithm we want as few rounds of encryption as possible but there are a minimum number of rounds required to assure the security level.

3. Impossible Differential Attacks

Most known and powerful attacks on block ciphers are differential cryptanalysis (DC) [6-9] and linear cryptanalysis (LC) [10]. These cryptanalytic techniques have attacked many block ciphers. So as to design a block cipher, every designer keeps the DC and LC attacks in mind to make it secure against these attacks. But now a days to secure a block cipher only against DC and LC is not sufficient. There are many other cryptanalysis techniques [11] which can attack block ciphers

Biham et.al. in 1998 developed variant of a truncated differential cryptanalysis called impossible differential cryptanalysis [12-16] by formulating distinguisher based on the fact that certain differentials never occur (i.e. the differentials with zero probability). It can be applied to the cipher, whose non-linear round function is bijective.

3.1 Generalized Impossible Differential Attack

To apply impossible differential attack, we need to find impossible differential pair ($\boldsymbol{\alpha} \nrightarrow \boldsymbol{\delta}$) which can be used as distinguisher. The difference $\boldsymbol{\alpha}$ after $\mathbf{r_i}$ rounds produces the output difference $\boldsymbol{\delta}$. An impossible differential with miss in middle technique works as a distinguisher to rule out the incorrect keys, where miss in middle technique uses combination of two differentials both of which hold with probability one and do not meet in middle i.e. for $\boldsymbol{r_1}$ rounds of partial encryption $\boldsymbol{\alpha}$ becomes $\boldsymbol{\beta}$ and for partial decryption of $\boldsymbol{r_2}$ rounds $\boldsymbol{\delta}$ becomes $\boldsymbol{\gamma}$. If $\boldsymbol{\beta \neq \gamma}$ the difference $\boldsymbol{\alpha \nrightarrow \delta}$ after $\boldsymbol{r_1 + r_2}$ rounds of encryption is impossible because $\boldsymbol{\alpha \rightarrow \beta \neq \gamma \leftarrow \delta}$ and $(\boldsymbol{\alpha},\boldsymbol{\delta})$ is called impossible differential pair. We eliminate or discard keys for which impossible differential characteristic $\boldsymbol{\beta \neq \gamma}$ holds for the subkey of that key.

Finding the Distinguisher, to obtain impossible differentials ($\boldsymbol{\alpha \nrightarrow \delta}$) and filtering and Key Elimination

1. Let the defined structure of set of $2^{8xz_f^p}$ plaintext with input differential $\boldsymbol{\alpha}$ and where z_f^p is represented as active bytes of chosen plaintexts, which means it has all fixed values except z_f^p bytes.
2. Some set of t structures are selected randomly, encrypt $2^{16xz_f^p-1}$ plaintext pairs by $\boldsymbol{r_i}$ rounds to obtain //differential $\boldsymbol{\beta}$ of the outputs for $\boldsymbol{Pr(\alpha \rightarrow \beta) = 1}$
3. In those t structures, select only those plaintext ciphertext PC pairs for those, whose ciphertext pairs have same bytes in the appointed positions with zero difference except for z_f^c fixed bytes of ciphertext, discard the rest of the pairs.
4. Create a table T of remaining ciphertexts pairs.
5. For active bytes in the last jth round $\boldsymbol{r_j}$, guess the subkeys $\boldsymbol{K_i}$ and store in table $\boldsymbol{T_1}$. Partially decrypt all ciphertext pairs from table T through last round $\boldsymbol{r_j}$ using these guessed key bytes. Select only those ciphertext pairs which after partially decryption through $\boldsymbol{r_{j-1}}$ round give output difference of non-zero bytes only in the guessed key positions in obtained ciphertext pair.
6. For each of the remaining ciphertext pairs in table T, compute their corresponding plaintext pair and Check $\boldsymbol{\beta \neq \gamma}$ then subkey is invalid.
7. Eliminate the invalid keys from table $\boldsymbol{T_1}$ that lead to the input difference of the impossible differential in the input of the 1st round. If a guess for these bytes remains, guess all the remaining key bytes to obtain original key with exhaustive search by checking over PC pairs and check the guess using trial encryption, else try above steps for all remaining guessed keys in $\boldsymbol{T_1}$.

8. Rejecting the invalid keys, the total key space is reduced.

3.2 Probability and Complexity Evaluation

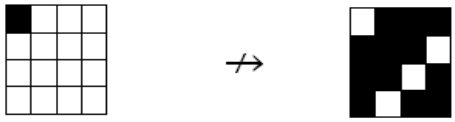
In step 1, Let $2^{8xz_f^p}$ plaintext set in a structure and in each structure, there are about $2^{16xz_f^p-1}$ plaintext pairs. In step 2, for t structure $t \times 2^{16xz_f^p-1-8xz_f^p}$ are the expected pairs. In step 4, $t \times 2^{16xz_f^p-1-8xz_f^p} \times P^{r_i} \times P^{r_{i-1}} \dots P^{r_1}$ are expected remaining pairs after decryption and P^{r_i} denotes probability for i^{th} decryption round. In step 6, $2^{m-8xz_f^p}$ output difference pairs which meet impossible differential property. In previous papers the data complexity of AES-128 is $2^{11.5}$ and 2^{119} time complexity for its 7-rounds which says it almost near to entire codebook and time complexity is nearly to exhaustive key search attack [15-16].
In our paper impossible differential path decides the time complexity for the algorithm and explained in section 3.4

3.3 Impossible Differential Attacks on AES

This section introduces impossible differential attack on 5-rounds of Tiny AES which utilize 4-round impossible differential characteristics. For impossible differential attack on 5-rounds of Tiny AES, use of similar characteristic of 4 rounds as in [19] which enables to attack 5-round of Tiny AES with a lower complexity. All known impossible differential attacks on the AES, are based on the following 4-round impossible differential property of AES. Impossible differential property for any 4 consecutive rounds holds if input difference Δa_i to round $r_i$has one non zero byte and output difference after shift row operation Δa_{i+3}^{SR} of 3 rounds r_{i+3}, considering last round has no mix column operation has zero difference for column i for atleast one of bytes in 4 columns.
A data collection is processed for the generation of necessary plaintext-ciphertext PC pairs. Then, to guarantee the impossible differential characteristic, PC pairs are filtered by checking meet in middle conditions at each intermediate round. Impossible differential attack uses differential which holds probability 1. Guessed keys for miss in middle PC pairs for differentials of 1 probability are collected and at the end those keys are eliminated because it satisfies the impossible differential characteristic and we are left with right keys.

3.4 Example of Impossible Differential Attack on AES-128

4-round impossible differential $\alpha \nrightarrow \delta$ for AES is



(X,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)$\nrightarrow$ (0, x1, X2, X3, X4, X5, X6, 0, X8, X9, 0, X11, X12, 0, X14, X15) is the impossible difference $\alpha \nrightarrow \delta$ for 4 rounds where it is assumed that mix column operation does not exist in last round. Non-zero difference in bytes is denoted by black background and zero difference in bytes is denoted by white.
Code has been implemented where T-AES has been executed in Python which generates 13440 plaintext pairs and goes through a path by following steps given in 3.1 and filters out 120 plaintext ciphertext pairs which help in finding out the exact key. The complexity calculated through this algorithm is around 2^{110} and memory required is 2^{40} bytes for 5 rounds of AES which is less than the other techniques.

4. Conclusion

Important design principles of lightweight ciphers are an efficient hardware implementation, a good performance and a moderate security level. Usually there is a trade-off between the performance and the security level. The Tiny AES block cipher is popular example of a lightweight cipher. We have evaluated and analysed the security of reduced round of T-AES against impossible differential cryptanalysis. The impossible cryptanalysis on 5 rounds of Tiny AES has been analyzed which requires 2^{110} data complexity and 2^{40} memory complexity approximately to recover the secret key which is better than exhaustive search.

REFERENCES

[1] Mehak Khurana, Meena Kumari, "Security Primitives: Block and Stream Ciphers", International Journal of Innovations & Advancement in Computer Science (IJIACS), ISSN 2347 – 8616, Vol. 4, March 2015.
[2] Kumar, M.; Pal, SK and Panigrahi, A., "Some Results on Design Parameters of Lightweight Block Ciphers" In Bilingual International Conference on Information Technology: Yesterday, Today, and Tomorrow, pp. 81-85, DESIDOC, 2015

[3] Bogdanov, A. and Shibutani., K, "Generalized Feistel networks revisited", Designs, Codes and Cryptography, Vol. 66, Issue 1-3, pp. 75-97, Springer 2013
[4] A.Biryukov and D. Khovratovich. Related-key cryptanalysis of full AES-192 and AES-256, in M.Matsui(Ed.): Asiacrypt 2009, LNCS 5912, PP.1-18,2009.
[5] A. Biryukov, O.Dunkelman, N. Keller, D. Khovratovich and A.Shamir. Key Recovery Attacks of practical Complexity on AES variants with up to 10 Rounds available at hhtp://eprint.iacr.org/2009/374.pdf
[6] E. Biham, A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems," Journal of Cryptology, Vols. 4, no.1, pp. 3-72, 1991.
[7] E. Biham, A. Shamir, Differential Cryptanalysis of the Data Encryption Standard, Springer Verlag, 1993.
[8] Biham, E. and Shamir, A., "Differential cryptanalysis of DES-like cryptosystems". In Advances in Cryptology CRYPTO 1990, Vol. 537, LNCS, pp. 2-21, Springer, 1990
[9] Zhang, L. and Wu, W., "Differential Cryptanalysis of Extended Generalized Feistel Networks", Information Processing Letters, Vol. 114, Issue 12, pp. 723-727, Elsevier, 2014
[10] A. Bogdanov and V. Rijmen,"Linear hulls with correlation zero and linear cryptanalysis of block ciphers," Designs, Codes and Cryptography, vol. 70 , no. 3, pp. 369-383, March 2014 .

[11] Mehak Khurana, Meena Kumari, "Variants of Differential and Linear Cryptanalysis", International Journal of Computer Applications (0975 – 8887) Volume 131 – No.18, PP 20-28, December 2015
[12] Mehak Khurana, Meena Kumari, "An Approach of Zero Correlation Linear Cryptanalysis" in International Journal of Computer Science and Engineering Technology, (IJCSET), ISSN : 2229-3345, Vol. 7, No. 05, pp 228-232, May 2016
[13] Biham, E.; Biryukov, A. and Shamir, A., "Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials". In Advances in Cryptology EUROCRYPT 1999, Vol. 1592, LNCS, pp. 12-23, Springer, 1999
[14] R. Li1, B. Sun1 and C. Li, "Impossible Differential Cryptanalysis of SPN Ciphers," https://eprint.iacr.org/2010/307.pdf, 2010.
[15] Y. Liu, D. Gu, Z. Liu, Wei Li, "Impossible Differential Attacks on Reduced Round LBlock," in ISPEC 2012, LNCS 7232, pp. 97–108, 2012, Springer-Verlag Berlin Heidelberg 2012, 2012.
[16] C. Boura, M. Naya-Plasencia, V. Suder, "Scrutinizing and Improving Impossible Differential Attacks: Applications to CLEFIA, Camellia, LBlock and Simon" Asiacrypt 2014, LNCS Volume 8873, 2014, pp 179-199, Springer-Verlg. 1999

BIOGRAPHIES

Mehak Khurana is currently working as assistant professor in The NorthCap University in CSE & IT and has around 6 years of experience. She completed her M.Tech from USIT, GGSIPU in 2011 and B.Tech from GTBIT, GGSIPU in 2009. Her key areas of interest are Cryptography, Information Security and Cyber Security. She is lifetime member of Cryptology Research Society of India (CRSI).

Meena Kumari, has worked as a professor, Dept of CSE&IT at The NorthCap University. She has also worked as Scientist 'G' at DRDO (Defence Research & Development Organization) and has 37 years of research experience in cryptology.