A New Kind of Integral Cryptanalysis for the Round-reduced AES

Tongfei Xia
Anhui Jiyuan Software Co. Ltd,SGITG
Hefei, China

Ziyan Zhao
State Grid Information & Telecommunication Branch
Beijing, China

Wei Li
State Grid Jiangsu Electric Power Co.Ltd.
Nanjing, China

Hengshan Fan
Anhui Jiyuan Software Co. Ltd,SGITG
Hefei, China

Can Cao
Anhui Jiyuan Software Co. Ltd,SGITG
Hefei, China

***Abstract*—AES is the mostly used block cipher nowadays. At CRYPTO 2016, Sun et al. proposed the first 5-round distinguisher of the AES [19]. However, it is somewhat closely related with the keys and hardly be used to mount a key recovery attack. Later in FSE 2016 [12] and EUROCRYPT 2017 [13], the distinguisher was improved. In this paper, by combining the techniques proposed by Sun et al. at CRYPTO 2016, we find a new 3-round integral distinguisher of AES which is closely related with the round keys. Then, based on the new distinguisher, we develop new techniques and give a new integral cryptanalysis for the round-reduced AES. We believe this may give new insight on the security of the AES.**

Keywords—integral cryptanalysis, AES, symmetric key cryptology

I. INTRODUCTION

A. The State-of-the-Art Cryptanalysis of AES

Block ciphers play a fundamental role in the field of symmetric-key cryptography. For example, we can build stream ciphers, hash functions and message authenticate codes (MAC) based on a known block cipher. Among the instances of block ciphers, perhaps the Advanced Encryption Standard (AES) [7] is the most widely used one nowadays. After its being proposal, the AES has attracted many attentions from the cryptographic community, and there have already been many developments in the cryptanalysis of AES.

Firstly, the designers of AES show a 6-round attack against the AES-128 by the square attack based on a 3-round distinguisher, the data and time complexities of this attack are 2^{32} and 2^{72}, respectively [7]. This attack has been improved by the partial sum technique and the workload has been reduced to 2^{44} in [10]. In 2000, Gilbert and Minier found a collision property of 3-round Rijndeal [11] based on which 7 rounds of AES-192 and AES-256 can be broken using 2^{32} chosen plaintexts with the complexity being 2^{140} encryptions. This attack was then improved by Dunkelman et al. at ASIACRYPT 2010 [9] and Derbez et al. at EUROCRYPT 2013 [8]. Until now, the meet-in-the-middle attack give the best attack against round-reduced version of the AES with respect to the trade-offs between the data complexity, the time complexity and the memory. Many literatures have studied the security of the AES against the impossible differential cryptanalysis, such [15], [17], [18], [22]. However, it seems that the key recovery attack can achieve at most 7 rounds with respect to the 128-bit key version. Boomerang attack is applied by Biryukov [1] for the 5 and 6 rounds of the cipher. It breaks 5 rounds of AES-128 using 2^{46} adaptive chosen plaintexts in 2^{46} steps of analysis, whereas the 6-round attack needs 2^{78} chosen plaintexts, 2^{78} steps of analysis, and 2^{36} bytes of memory. A class of algebraic attacks on AES were examined in [5], where the S-box of the AES is written as a system of implicit quadratic equations, resulting the conversion of the cryptanalysis to solving a huge system of quadratic equations. The algebraic cryptanalysis was once considered as the most powerful method against the AES. However, there is little progress against the security of the AES. Besides the single-key model, Biryukov et al. shown that the related-key model can break some full version of the AES [2], [3]. However, the related-key setting may not be accepted by all the cryptographic community.

Among all the attacks, a distinguisher of the round-reduced AES is of vital importance. We always try to find a distinguisher that covers as many rounds as possible. Before 2016, all the distinguishers of the AES-128 cover at most 4-rounds. Then, at EUROCRYPT 2016, Sun et al. proved that without the details of the S-box, an impossible differential of the AES cannot cover 5 or more rounds [20]. At CRYPTO 2016, Sun et al. proposed the first 5-round distinguisher of the AES [19] which was later improved by Grassi et al. [12], [13] to cover 5 rounds. However, these distinguishers seem hardly to be used to mount a key recovery attack against the AES.

B. Intergral Cryptanalysis

At FSE 2002, Knudsen et al. proposed the Integral Cryptanalysis [14] which becomes one of the most effective cryptanalytic methods since then. Integrals have many interesting features and they are especially well-suited in analyzing ciphers with primarily bijective components. Moreover, they exploit the simultaneous relationship between many encryptions, in contrast to differential cryptanalysis where only pairs of encryptions are considered. Consequently, integrals apply to a lot of ciphers which are not vulnerable to differential and linear cryptanalysis. For example, it has been proved that the 4-round AES does not have an effective differential characteristic while there exist many 4-round integrals. These features have made integral an increasingly popular tool in recent cryptanalysis work. In fact, integral cryptanalysis is a more generalization of Square attack [6], Saturation attack [16] and Multiset attack [4] proposed by Daemen et al., Lucks, and Biryukov et al., respectively. And the newly proposed division property [21]

gives a novel way to construct the integral distinguisher of a cipher.

Let V be a subset of F_{2^n}, and $E_k(x)$ be a cipher defined over F_{2^n}. An integral of F_{2^n} over V is defined as the sum of all values of $E_k(x)$ on V. In other words, the integral of $E_k(x)$ over V is

$$\int(E_k, V) = \sum_{x \in V} E_k(x)$$

It should be emphasized here that most of the integral distinguishers are independent with the specific value of the key k. That is, no matter which k the cipher adopts, $\int(E_k, V)$ is always a constant.

C. Our Contributions

Actually, the distinguisher proposed by Sun et al. can be considered as a key-related one. To be exact, if the difference of the inputs equals the differences of the corresponding round keys, then the sum of the corresponding ciphertexts is zero. Due to the large amount of the palintexts, even though we believe it is correct, we cannot verify the distinguisher practically and use it to mount a key recovery attack. In this paper, we are going to propose a new kind of integral distinguisher of the 3-round AES which has a practical data complexity and we can also use it to mount a key recovery attack against the 4-round AES practically. The steps of the attack are as following:

Step 1. Find a key-related distinguisher of the round-reduced cipher;

Step 2. Guess a value for the round-keys related to the distinguisher, say k, and denote the key candidates pool correspondence to k by K_k;

Step 3. Apply the traditional integral cryptanalysis to recover the key;

Step 4. Distinguish the right key from the wrong ones:

(1)If $K_k = \varnothing$, it indicates that k is a wrong value for the key related to the distinguisher;

(2) If there is only one element in K_k, then k may be the right value for the key related to the distinguisher, and element in K_k is the right value for other round-keys.

This paper is organized as following: the description of the AES is shown in Sec.II. In Sec.III, some new key-related 3-round integral distinguishers of AES are given, and the correspondence key-recovery attack are also discussed in this section; Sec. IV gives the key recovery attack against 4-round AES. Then, Sec.V concludes this paper.

II. Data Encryption Process Of AES

The AES [7] is designed by Deamem and Rijmen, which is the winner of the AES project. Perhaps it is the mostly used block ciphers nowadays. The block size of the AES is 128- bit, and during the encryption process, both the plaintext and the round-keys are considered as matrices in $F_{2^8}^{4\times4}$, and the entries of the matrix are represented as an element of F_{2^8} (a byte). Let $A^{(r)} = (a_{ij}^{(r)})_{4\times4}$ and $K^{(r)} = (k_{ij}^{(r)})_{4\times4}$ be the state and roundkey of the r-th round. Then each round function, except the final one, consists of the following 4 transformations:

AddRoundkey (**ARK**): the state is XORed with the 128-bit round key:

$$A^{(r)} \oplus K^{(r)} = (a_{ij}^{(r)} \oplus k_{ij}^{(r)})_{4\times4}$$

ByteSubstitute (**BS**): Each entry of state is passed through a nonlinear substitution layer(S-box):

$$BS(A^{(r)}) = (\text{S-box}(a_{ij}^{(r)}))_{4\times4}$$

ShiftRows (**SR**): Rows are shifted to the left by 0, 1, 2, and 3 bytes, from the first row to the last;

MixColumns (**MC**): This operation provides efficient confusion on columns of the matrix:

$$MC(A^{(r)}) = (M(a_{ij}^{(r)}))_{4\times4}$$

where M is an MDS matrix multiplication over $F_{2^8}^{4\times4}$. The MDS matrix used in AES is

$$M = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix}$$

Each round, except the last one, applies AddRoundKey, ByteSubstitute, ShiftRow and MixColumn consequently. Note in the last round, the MixColumn is replaced by another AddRoundkey. The round keys are generated through the key schedule. The round number nr of AES with 128-/192-/256-bit key is 10/12/14, respectively.

III. A New Integral Distinguisher Of The 3-Round AES

In this section, some new distinguishers of 3-round AES will be given and new attacks against 4-round AES will be proposed.

Firstly, let's recall the well-known 3-round integral distinguisher:

Let the inputs of AES be $\begin{pmatrix} x & c_{0,1} & c_{0,2} & c_{0,3} \\ c_{1,0} & c_{1,1} & c_{1,2} & c_{1,3} \\ c_{2,0} & c_{2,1} & c_{2,2} & c_{2,3} \\ c_{3,0} & c_{3,1} & c_{3,2} & c_{3,3} \end{pmatrix}$ where $c_{i,j}$'s are fixed to some constants in F_{2^8}. Then each byte of the output of the third round is balanced.

This distinguisher was discovered by the designer and have been improved to cover 4 rounds then [10]. And most of the known integral attacks are based on the 4-round

distinguisher.

As we known, combining different cryptanalytic methods may sometimes be more powerful. For example, the differential-linear cryptanalysis is actually linear cryptanalysis with the inputs being fixed to some given difference. However, as two powerful methods, we haven't seen the combination of differential and integral cryptanalysis. In the following, we are going to consider these two methods together.

THEOREM. Let the inputs to the AES be

$$\begin{pmatrix} x & c_{0,1} & c_{0,2} & c_{0,3} \\ c_{1,0} & x \oplus \delta & c_{1,2} & c_{1,3} \\ c_{2,0} & c_{2,1} & c_{2,2} & c_{2,3} \\ c_{3,0} & c_{3,1} & c_{3,2} & c_{3,3} \end{pmatrix}$$

where $c_{i,j}$'s are fixed to some constants in F_{2^8}. If

$$\delta = K_{0,0}^{(0)} \oplus K_{1,1}^{(0)},$$

then each byte of the output of the 3-rd round is balanced.

Proof. If the input is

$$\begin{pmatrix} x & c_{0,1} & c_{0,2} & c_{0,3} \\ c_{1,0} & x \oplus \delta & c_{1,2} & c_{1,3} \\ c_{2,0} & c_{2,1} & c_{2,2} & c_{2,3} \\ c_{3,0} & c_{3,1} & c_{3,2} & c_{3,3} \end{pmatrix}$$

where $\delta = K_{0,0}^{(0)} \oplus K_{1,1}^{(0)}$ and $c_{i,j}$'s are constants, the output of the first round is:

$$\begin{pmatrix} f_0(x) & d_{0,1} & d_{0,2} & d_{0,3} \\ f_1(x) & d_{1,1} & d_{1,2} & d_{1,3} \\ d_{2,0} & d_{2,1} & d_{2,2} & d_{2,3} \\ f_2(x) & d_{3,1} & d_{3,2} & d_{3,3} \end{pmatrix}$$

where $f_i(x)$'s are permutation polynomials over $F_{2^8}[x]$ and $d_{i,j}$'s are constants.

Consequently, we can compute that each byte of the output of the third round is of the form

$$q_1(x) \oplus q_2(x) \oplus q_3(x)$$

where $q_i(x)$'s ($i = 1,2,3$) are permutation polynomials over $F_{2^8}[x]$, thus they are balanced.

Actually, we can construct many other distinguishers with the same form using the same techniques above, and we leave the details to the readers.

IV. Integral Attack Against The 4-Round AES-128

In this subsection, we briefly give a new key-recovery attack against 4-round AES based on the distinguisher constructed in the last section.

Step 1: Choose plaintexts of the following form where s are constants:

$$P(x,\delta) = \begin{pmatrix} x & c_{0,1} & c_{0,2} & c_{0,3} \\ c_{1,0} & x \oplus \delta & c_{1,2} & c_{1,3} \\ c_{2,0} & c_{2,1} & c_{2,2} & c_{2,3} \\ c_{3,0} & c_{3,1} & c_{3,2} & c_{3,3} \end{pmatrix}$$

and for all possible x and δ, encrypt these plaintexts. The ciphertext correspondence to $P(x,\delta)$ is denoted by $C(x,\delta)$.

Step 2: For each $\delta \in F_{2^8}$, denote the pool for the key candidates of $K_{0,0}^{(4)}$ as $K(\delta)$, and randomly choose a value from $K(\delta)$, say k, compute

$$s_k = \sum_{x \in F_{2^8}} S^{-1}(C(x,\delta)_{0,0} \oplus k)$$

If $s_k \neq 0$, delete k from $K(\delta)$.

Step 3: If necessary, repeat Step 1 and Step 2 until there is an element, say δ_0 such that $|K(\delta_0)| = 1$, and for other $\delta \neq \delta_0$, $K(\delta_0) = \varnothing$. Thus δ_0 is the right value for $K_{0,0}^{(0)} \oplus K_{1,1}^{(0)}$, and the single element in $K(\delta_0)$ is the right value for $K_{0,0}^{(4)}$.

For each δ, the probability that $s_k = 0$ is 2^{-8}. Thus on average, for each δ, we can use at most two structures to determine whether $K(\delta) = \varnothing$ or $|K(\delta)| = 1$. This tells that the complexity of this attack is 2^{16} chosen plaintexts, and the time complexity is about 2^{24} encryptions.

We have implemented the 4-round attack using personal computer, and the round keys can be recovered in less than a second.

We have also tried to give a 5-round key recovery attack. However, compared with the traditional integral attack, this new distinguisher contains more active bytes, thus more key bytes are needed to do a partial key recovery attack.

V. Conclusion

Integral cryptanalysis is among the popular methods to evaluate the security of a block cipher. This paper combined the differential cryptanalysis and integral cryptanalysis together to show a new type of integral distinguisher of the 3-round AES, based on which we can also mount a key-recovery attack against 4-round AES. The newly proposed distinguisher and key-recovery attack may give us new insight to the security of the AES. In the future, we are going to study the possibility of extending the length of the distinguisher so that we may get better result about the security analysis of the cipher.

REFERENCES

[1] Biryukov, A.: The boomerang attack on 5 and 6-round reduced AES. In: Advanced Encryption Standard - AES, 4th International Conference, AES 2004, Bonn, Germany, May 10-12, 2004, Revised Selected and Invited Papers. (2004) 11–15

[2] Biryukov, A., Khovratovich, D.: Related-key cryptanalysis of the full AES-192 and AES-256. In: Advances in Cryptology – ASIACRYPT 2009, 15th International Conference on the Theory and Application of Cryptology and Information Security, Tokyo, Japan, December 6-10, 2009. Proceedings. (2009) 1–18

[3] Biryukov, A., Khovratovich, D., Nikolic, I.: Distinguisher and related key attack on the full AES-256. In: Advances in Cryptology – CRYPTO 2009, 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2009. Proceedings. (2009) 231–249

[4] Biryukov, A., Shamir, A.: Structural cryptanalysis of SASAS. In: Advances in Cryptology - EUROCRYPT 2001, International Conference on the Theory and Application of Cryptographic Techniques, Innsbruck, Austria, May 6-10, 2001, Proceeding. (2001) 394–405

[5] Courtois, N., Pieprzyk, J.: Cryptanalysis of block ciphers with overdefined systems of equations. In: Advances in Cryptology - ASIACRYPT 2002, 8th International Conference on the Theory and Application of Cryptology and Information Security, Queenstown, New Zealand, December 1-5, 2002, Proceedings. (2002) 267–287

[6] Daemen, J., Knudsen, L.R., Rijmen, V.: The block cipher square. In: Fast Software Encryption, 4th International Workshop, FSE '97, Haifa, Israel, January 20-22, 1997, Proceedings. (1997) 149–165

[7] Daemen, J., Rijmen, V.: The Design of Rijndael: AES - The Advanced Encryption Standard. Information Security and Cryptography. Springer (2002)

[8] Derbez, P., Fouque, P., Jean, J.: Improved key recovery attacks on reducedround AES in the single-key setting. In: Advances in Cryptology -EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings. (2013) 371–387

[9] Dunkelman, O., Keller, N., Shamir, A.: Improved single-key attacks on 8-round AES-192 and AES-256. In: Advances in Cryptology – ASIACRYPT 2010 - 16th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 5-9, 2010. Proceedings. (2010) 158–176

[10] Ferguson, N., Kelsey, J., Lucks, S., Schneier, B., Stay, M., Wagner, D.A., Whiting, D.: Improved cryptanalysis of rijndael. In: Fast Software Encryption, 7th International Workshop, FSE 2000, New York, NY, USA, April 10-12, 2000, Proceedings. (2000) 213–230

[11] Gilbert, H., Minier, M.: A collision attack on 7 rounds of rijndael. In: AES Candidate Conference. (2000) 230–241

[12] Grassi, L., Rechberger, C., Rønjom, S.: Subspace trail cryptanalysis and its applications to AES. IACR Trans. Symmetric Cryptol. 2016(2) (2016) 192–225

[13] Grassi, L., Rechberger, C., Rønjom, S.: A new structural-differential property of 5-round AES. In: Advances in Cryptology – EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part II. (2017) 289–317

[14] Knudsen, L.R., Wagner, D.A.: Integral cryptanalysis. In: Fast Software Encryption, 9th International Workshop, FSE 2002, Leuven, Belgium, February 4-6, 2002, Revised Papers. (2002) 112–127

[15] Lu, J., Dunkelman, O., Keller, N., Kim, J.: New impossible differential attacks on AES. In Chowdhury, D.R., Rijmen, V., Das, A., eds.: Progress in Cryptology - INDOCRYPT 2008, 9th International Conference on Cryptology in India, Kharagpur, India, December 14-17, 2008. Proceedings. Volume 5365 of LNCS., Springer (2008) 279–293

[16] Lucks, S.: The saturation attack - A bait for twofish. In Matsui, M., ed.: Fast Software Encryption, 8th International Workshop, FSE 2001 Yokohama, Japan, April 2-4, 2001, Revised Papers. Volume 2355 of LNCS., Springer (2001) 1–15

[17] Mala, H., Dakhilalian, M., Rijmen, V., Modarres-Hashemi, M.: Improved impossible differential cryptanalysis of 7-round AES-128. In Gong, G., Gupta, K.C., eds.: Progress in Cryptology - INDOCRYPT 2010 -11th International Conference on Cryptology in India, Hyderabad, India, December 12-15, 2010. Proceedings. Volume 6498 of LNCS., Springer (2010) 282–291

[18] Phan, R.C.: Impossible differential cryptanalysis of 7-round advanced encryption standard (AES). Inf. Process. Lett. 91(1) (2004) 33–38

[19] Sun, B., Liu, M., Guo, J., Qu, L., Rijmen, V.: New insights on aes-like SPN ciphers. In: Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part I. (2016) 605–624

[20] Sun, B., Liu, M., Guo, J., Rijmen, V., Li, R.: Provable security evaluation of structures against impossible differential and zero correlation linear cryptanalysis. In: Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part I. (2016) 196–213

[21] Todo, Y.: Structural evaluation by generalized integral property. In: Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I. (2015) 287–314

[22] Zhang,W.,Wu,W., Zhang, L., Feng, D.: Improved related-key impossible differential attacks on reduced-round AES-192. In: Selected Areas in Cryptography, 13th International Workshop, SAC 2006, Montreal, Canada, August 17-18, 2006 Revised Selected Papers. (2006) 15–27