ISBN 978-981-14-1684-2
Proceedings of 2019 the 9th International Workshop on Computer Science and Engineering
(WCSE 2019 SUMMER)
Hong Kong, 15-17 June, 2019, pp. 734-737
doi: 10.18178/wcse.2019.06.109

How to Obtain the Missing Terms of Reduced-Round DES

Lei Zhang [1+], Zhaohui Liu [1], Weihua Hu [1], Juan Li [1]and Lei Shi [1]

[1] China Information Technology Security Evaluation Center, CNITSEC, Beijing, China

Abstract. In this paper, we obtain the missing IV terms of round function of DES, so that we can obtain the distinguishers of reduced-round DES. We apply the IV representation to reduced-round DES, so that the missing terms can be obtained. The missing IV terms can be exploited as the integral distinguishers because sum over any missing IV term is zero. This is the first time to construct integral distinguishers on reduced round DES.

Keywords: Missing Terms, IV representation, Integral Distinguisher, DES, Block Cipher.

1. Introduction

Cryptography is of vital importance due to the fact that encryption is the basic procedure to guarantee the information security. Cryptanalysis of ciphers can help to design more secure ciphers. The cryptanalysis of ciphers include key recovery attack, distinguishing attack and collision attack. Collision attack is majored applied for cryptanalysis of Hash functions.

Block ciphers play an important part in data encryption due to the high performance and the application in block transactions such as the IP services. Most block ciphers have an iterative structure, improving a weaker round function. DES [1], designed by IBM, was the first accepted encryption standard. It applies a Feistel structure, which may have a good pseudorandom property. In addition, this structure can guarantee that the decryption is the same as the encryption.

Since it was accepted by NIST, a variety of cryptanalysis techniques were proposed to attack DES and its reduced round versions. In 1991, Biham and Shamir proposed differential analysis [2] to attack full round DES [3,4]. Since then, differential cryptanalysis has been the standard technique to cryptanalysis the block ciphers and even the stream ciphers. Matsui proposed the linear cryptanalysis method [5] and showed the attack on DES. The differential and linear cryptanalysis method relies on the probability that is determined by the data complexity.

Integral property was exploited to distinguisher a keyed cipher and a random permutation. The traditional method to construct an integral distinguisher is to search or to convert an impossible differential property as an integral distinguisher. Cube attack and cube tester are important techniques [6,7] to test the nonrandom property including integral property. Cube tester is often used to construct distinguishers in order to attack ciphers, combined with other key recovery technique. For example, Dinur et al. proposed dynamic cube attack to break Grain-128 [8], where the nonrandom property was obtained by cube tester. In addition, the integral property performs when the integral is zero while it is sum over a 'cube' is zero. So it is connected with cube property, which can be obtained by cube tester technique.

However, the cube tester is of high complexity when the cube is of high dimension, i.e. the cube complexity is 2^d when the cube dimension is d. When there is no low-dimensional nonrandom property, it is hard to obtain the nonrandom property with restrict to our computational ability. In [9], Fu et al. proposed a series of methods

+ Corresponding author. Tel: 18701363097
E-mail address: zhangwj8998@126.com.

to obtain the integral property, including nullification technique, polynomial reduction technique and IV representation. It is the IV representation, using computation but not testing, that helps to obtain the missing IV terms, which can be applied as the integral distinguisher or cube distinguisher.

In this paper, we determine the missing IV terms and construct integral properties for reduced round DES. This is the first time to construct integral distinguishers using IV representation for block ciphers. Our contribution include 1) IV representation is applied to cryptanalysis of block ciphers; 2) The deterministic missing IV terms of DES are obtained; 3) The integral distinguishers can be constructed.

The rest of the paper is as follows. In Section 2, some preliminaries will be introduced, including the introduction to DES and some basic concepts. In Section 3, it will be introduced how to obtain the missing IV terms. Section 4 concludes this paper.

2. Preliminaries

In this section, DES and some basic techniques will be introduced.

2.1. Introduction to DES

DES is an iterative block cipher with a 64-bit block and 56-bit valid key. On each round, the state updates with a new 64-bit. There is an initial permutation (IP) and a final inverse permutation (IP^{-1}). Denote (L_r, R_r) as the left half and right half part of the state at round r. The iterative update follows the following formula

$$\begin{cases} L_{r+1} = R_r \\ R_{r+1} = L_r \oplus f(R_r + E(k)), \end{cases} \tag{1}$$

where the $f(\cdot)$ is denoted as the round function (F function) and $E(k)$ is the expansion function of key. F function is eight parallel (six bits to four bits) S boxes. For more details about DES, you can refer to [5].

2.2. Algebraic Normal Form

The output bits of symmetric cryptosystems can be illustrated as an algebraic normal form (ANF) over n-bit public variables and m-bit private variables, i.e.

$$z = \sum_{I,J} \prod_{I,i\in I} v_i \prod_{J,j\in J} k_j,$$

where $I \subseteq \{1, 2, \ldots, n\}$ and $J \subseteq \{1, 2, \ldots, m\}$. For stream ciphers, the public variables are initial vector (IV) while they are plaintexts for block ciphers. For certain I and J, $\prod_{I,i\in I} v_i \prod_{J,j\in J} k_j$ is a term and $\prod_{I,i\in I} v_i$ is the corresponding IV term. For example, let $z = v_1v_2k_1 + v_1k_2 + v_1k_1k_3 + v_3 + k_3$ be an ANF over 3 public variables v_1, v_2, v_3 and 3 private variables k_1, k_2, k_3.

2.3. IV Representation

Replacing the term with its corresponding IV term and removing the repeated IV terms is denoted as IV representation [8]. For the forehead example in Section 2.2, the IV representation of z is $v_1v_2 + v_1 + v_3$, i.e., all the IV terms are v_1v_2, v_1 and v_3.

In [9], two important algorithms were proposed to obtain some specific missing IV terms. The first is the repeated IV term removing algorithm (Algorithm 1), which can be used to remove the repeated IV terms. The second is the covered IV term removing algorithm (Algorithm 2), which can be used to obtain the IV terms of highest degree.

2.4. Integral Distinguishers and Missing IV Terms

A missing IV term means that sum over this cube is zero, which can be a transfer as an equivalent integral distinguisher, i.e., integral on this term is zero.

Take the instance in Section 2.2 as an example. The missing IV terms include v_2 of dimension 1 and v_1v_3, v_2v_3 of dimension 2. The IV term $v_1v_2v_3$ is not used regularly because it is trial. Then sum over these missing IV terms is always zero. These missing IV terms can be obtained by cube tester [7] or IV representation [8]. The results obtained by cube tester is probabilistic and are deterministic by IV representation.

3. Obtain the Missing IV Terms

In this section, the missing IV terms of reduced round DES will be obtained, so that the integral distinguishers can be constructed. In this paper, we just consider the integral distinguishers for R_r at round **r** for that $L_r = R_{r-1}$ with Feistel structure.

3.1. The Boolean Functions for Sbox of DES

The IV representation relies on the view of Boolean function. For block ciphers, there is no natural Boolean function because Sbox is often used. We need to transfer an Sboxes to Boolean functions, that is we need to obtain the ANF of Sbox.

From the true value tables, we can obtain the ANF of the S boxes using Mobius transformation. Let x_i $(0 \le i \le 5)$ and y_j $(0 \le j \le 3)$ denote input and output bits separately, where x_5 and y_3 is the most significant bit and x_0 and y_0 is the least significant bit of input and output. The Boolean functions of the eight tables can be obtained by Mobius Transformation.

3.2. IV Representation for Sboxes of DES

To obtain the missing highest degree IV terms, we use IV representation, combined with Algorithm 2. Let a $\approx$ b denote that the IV representation of a is b, then the results of IV representation for eight S boxes can be obtained.

In fact, x_i indicates the input bit of the S box, which is equal to the exclusive-or (XOR) of the corresponding bit of right half state and key bit. The key bits are constant, which can be treated as 1 by IV representation, so that it will disappear using Algorithm 2. Hence, x_i can be treated as the corresponding bit of the right half. Using IV representation, the number of terms processed drops off dramatically.

Based on the IV representation, we can construct integral distinguishers by determining the missing IV terms.

3.3. Integral Distinguishers for Sboxes of DES

The integral distinguishers for one-round DES can be obtained directly by the IV representation in Section 3.2. We use the first bit of R_1 to construct integral distinguishers. Let $P = (v_0, v_1, \ldots, v_{63}) = (L_0, R_0)$ denote the plaintexts.

3.3.1 Integral Distinguishers Using L_0

The first bit of R_1, denotes as R_1^3, can be illustrated as $R_1^3 = L_0^3 \oplus f(.)$, where $f(.)$ is a function over R_0. So the integral over any two-dimensional v_0v_t $(1 \le t \le 63)$ is zero. As there are no other bits in L_0 are involved in generating R_1^3, so integral over v_t $(1 \le t \le 31)$ is zero, which can be an integral distinguisher.

3.3.2 Integral Distinguishers Using R_0

3.3.2.1 Integral Distinguishers Using the IV representation in Section 3.2

To generate R_1^3, totally six bits are involved. The integral distinguishers can be obtained using the missing IV terms. The missing IV terms of dimension 4 are $x_0x_1x_2x_3$ and $x_0x_1x_3x_4$ and the missing IV terms of dimension 5 are $x_0x_1x_3x_4x_5$, $x_0x_1x_2x_3x_5$ and $x_0x_1x_2x_3x_4$. The missing IV terms can be used as integral distinguishers. The x_0, x_1, x_2, x_3, x_4 and x_5 corresponds to v_{36}, v_{35}, v_{34}, v_{33}, v_{32} and v_{63} separately. So the integral distinguishers are shown in the following table.

Dimension	Distinguishers
4	$v_{33}v_{34}v_{35}v_{36}$ $v_{32}v_{33}v_{35}v_{36}$
5	$v_{33}v_{34}v_{35}v_{36}v_{63}$ $v_{32}v_{33}v_{35}v_{36}v_{63}$ $v_{32}v_{33}v_{34}v_{35}v_{36}$

Table 1 Integral Distinguishers for One-Round DES Using IV Representation

3.3.2.2 Integral Distinguishers Using the Other Bits of R_0

The other bits of R_0 are not involved in generating R_1^3, so one-dimensional integral on one of these bits is zero, so that one-dimensional integral distinguishers can be obtained.

3.4. Integral Distinguishers for Two-round DES

In Section 3.3, three types of integral distinguishers can be obtained. But for two round DES, it is hard to obtain the direct integral distinguishers without any reduction technique or IV representation.

Let us consider R_2^3, which can be illustrated by $R_2^3 = L_1^3 \oplus f(.)$, where $f(.)$ is a function over R_1. We just consider the IV terms of highest degree, L_1^3 can be discarded for that degree of L_1^3 is 1 since $L_1^3 = R_0^3$. Then we use IV representation and remove the covered terms, i.e., $R_2^3 \simeq x_0x_1x_3x_5 + x_0x_1x_2x_4x_5 + x_0x_2x_3x_4x_5 + x_1x_2x_3x_4x_5$, where x_0, x_1, x_2, x_3, x_4 and x_5 corresponds to R_1^{31}, R_1^0, R_1^1, R_1^2, R_1^3 and R_1^4 separately. The degree of x_0, x_1, x_2, x_3, x_4 and x_5 are 5.

Then we substitute R_1^{31}, R_1^0, R_1^1, R_1^2, R_1^3 and R_1^4 with the form of IV representation in Section 3.2 as follows.

$$R_1^{31} \simeq v_{32}v_{60}v_{62}v_{63} + v_{32}v_{59}v_{61}v_{63} + v_{32}v_{59}v_{60}v_{63} + v_{32}v_{59}v_{60}v_{61}v_{62} + v_{59}v_{60}v_{61}v_{62}v_{63}$$

$$R_1^0 \simeq v_{32}v_{35}v_{36} + v_{34}v_{35}v_{36}v_{63} + v_{33}v_{35}v_{36}v_{63} + v_{32}v_{33}v_{34}v_{36}v_{63} + v_{32}v_{33}v_{34}v_{35}v_{63}$$

$$R_1^1 \simeq v_{32}v_{34}v_{35}v_{36}v_{63} + v_{32}v_{33}v_{35}v_{36}v_{63} + v_{32}v_{33}v_{34}v_{36}v_{63} + v_{32}v_{33}v_{34}v_{35}v_{63}$$

$$R_1^2 \simeq v_{32}v_{34}v_{35}v_{36}v_{63} + v_{32}v_{33}v_{35}v_{36}v_{63} + v_{32}v_{33}v_{34}v_{36}v_{63} + v_{32}v_{33}v_{34}v_{35}v_{63}$$

$$R_1^3 \simeq v_{33}v_{35}v_{36}v_{63} + v_{32}v_{34}v_{35}v_{36}v_{63} + v_{32}v_{33}v_{34}v_{36}v_{63} + v_{32}v_{33}v_{34}v_{35}v_{63}$$

$$R_1^4 \simeq v_{35}v_{36}v_{38}v_{40} + v_{35}v_{36}v_{37}v_{39}v_{40} + v_{35}v_{36}v_{37}v_{38}$$

$$R_2^3 \simeq v_{32}v_{33}v_{34}v_{35}v_{36}v_{59}v_{60}v_{61}v_{62}v_{63}(v_{37}v_{38} + v_{38}v_{40} + v_{37}v_{39}v_{40})$$

So the degree of R_2^3 is 13 and only one term of degree 13 exists. The other IV terms of degree 13 are missing, so that they can be serve as the integral distinguishers.

4. Conclusion

In this paper, we show a new method to obtain deterministic integral distinguisher of block cipher DES, combined with Algorithm 2. This is the first time to obtain the deterministic integral distinguisher of reduced round DES. In fact, we can obtain integral distinguishers of lower degree, combined with Algorithm 1. The complexity may be much higher, which will be our future work.

5. References

[1] Standard, Data Encryption. "Federal information processing standards publication 46." National Bureau of Standards, US Department of Commerce(1977).

[2] E. Biham and A. Shamir, "Differential Cryptanalysis of FEAL and N-Hash," *Advances in Cryptology-EUROCRYPT'91*, Lecture Notes in Computer Science, Vol.547, pp. 1–16, (1991)..

[3] E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems," Journal of Cryptology, Vol.4, pp.3–72, (1991).

[4] E. Biham and A. Shamir, "Differential Cryptanalysis of the full 16-round DES,"CRYPTO'92 Extended Abstracts, pp.12-1–12-5, (1992)..

[5] Matsui M. Linear cryptanalysis method for DES cipher[C]. EUROCRYPT'93. Springer Berlin/Heidelberg, 1994: 386-397.

[6] Dinur, Itai, and Adi Shamir. "Cube Attacks on Tweakable Black Box Polynomials." Eurocrypt. Vol. 5479. 2009..

[7] Aumasson, Jean-Philippe, et al. "Cube Testers and Key Recovery Attacks on Reduced-Round MD6 and Trivium." FSE. Vol. 5665. 2009.

[8] Dinur, Itai, and Adi Shamir. "Breaking Grain-128 with Dynamic Cube Attacks." FSE. Vol. 6733. 2011.

[9] Fu, Ximing, Xiaoyun Wang, and Jiazhe Chen. "Determining the Nonexistent Terms of Non-linear Multivariate Polynomials: How to Break Grain-128 More Efficiently." IACR Cryptology ePrint Archive 2017 (2017): 412.