VERSITA

TATRA MOUNTAINS
Mathematical Publications

DOI: 10.2478/tmmp-2013-0034
Tatra Mt. Math. Publ. **57** (2013), 35–43

LOW DATA COMPLEXITY DIFFERENTIAL-ALGEBRAIC ATTACK ON REDUCED ROUND DES

Arkadiusz Gąsecki

ABSTRACT. At IMA 2007 Courtois and Bard presented low-data complexity attacks on up to 6 rounds of DES by software algebraic attack methods and SAT solvers. With current methods it appears that 8 rounds of DES should be able to resist such attacks [Courtois, N. T.—Gawinecki, A.—Song, G.: *Contradiction immunity and guess-then-determine attacks on GOST,* Tatra Mt. Math. Publ. **53** (2012), 65–79]. An explicit challenge with a price was proposed: break 8 rounds of DES in less than a week on one PC with maximum 2 gigabytes of RAM and given at most 16 chosen plaintexts.

In this paper we propose a new attack which is trying to achieve this objective as much as possible. Presented method combines two, already known techniques, namely differential cryptanalysis and algebraic attacks. More specifically, it shows how to use relations arising from differential chracteristics to speed up and improve key-recovery algebraic attacks against reduced block cipher DES.

1. Introduction

The idea of mixing two, already known cryptanalysis techniques, has been shown in [1] as well as in [2] and [7]. The aim of this article is to verify, whether this type of attack can be applied to DES cipher [4], reduced to eight rounds. An extra assumption is that we do not have knowledge about bits of the key used to encryption. Section 2 describes idea of differential cryptanalysis and summarizes already known algebraic and combined attacks on DES. Section 3 presents the algorithm of attack performed, introduces differential characteristics used to implement it and shows experimental results. Finally, Section 4 summarizes the main conclusions of this paper and presents an outlook for future work.

Keywords: cryptology, cryptanalysis, block cipher, differential cryptanalysis, algebraic attack, SAT solver.

2. Known attacks on DES

This section presents idea of the attacks, performed on DES, which were then used to apply attack described in this article.

2.1. Differential cryptanalysis of DES

The idea of differential cryptanalysis was presented by E. Biham and A. Shamir in [3]. This type of attack is based on studying differences between plaintexts and corresponding ciphertexts, created using the same key. In the simplest case we have two plaintexts – P and P^*– and two corresponding ciphertexts – C and C^*. Finding the key bits is based on difference Ω_P between plaintext and difference Ω_C between ciphertexts, as shown on Fig. 1.

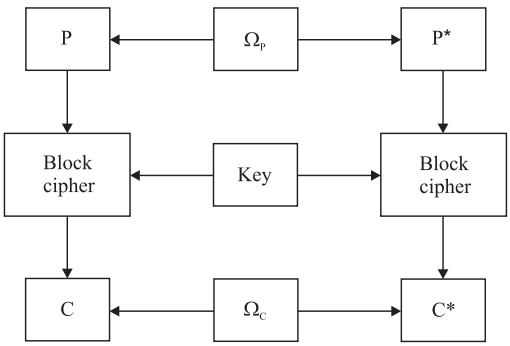

FIGURE 1. The idea of differential cryptanalysis.

Differential cryptanalysis is usually chosen plaintext attack. The best known attack of this type against full round DES needs 2^{47} chosen plaintexts and it was presented in [11]. Selected differential characteristics, described in [3] were used to apply attack described in this article and will be introduced in following section.

2.2. Algebraic and combined attacks on DES

The basic principle of algebraic attacks is to model a cryptographic primitive by a set of algebraic equations. The system of equations is constructed in such a way as to have a correspondence between the solutions of this system, and a secret information of the cryptographic primitive (for instance, the secret key of a block cipher).

Algebraic cryptanalysis of block cipher DES was applied by N. Courtois and G. V. Bard and described in [5]. To solve sets of equations they used fact that this NP-hard problem is equivalent to another one, namely boolean satisfiability problem (called SAT). Then, they have used MiniSAT tool to find a solution. These sets of equations, describing different variants of DES cipher,

were given in [6]. The authors attacked successfully 6 rounds of DES assuming, that they know any 20 bits of the key.

The equations, specified in [6], were also used by authors of the attack, described in [2]. Method, presented there, shows improvements given by combination of algebraic attack and differential cryptanalysis. Using both techniques, authors applied successful attack against four and six rounds of DES.

A method of algebraic-differential cryptanalysis and its applications against reduced block cipher DES was also presented in [7]. The authors published their results of attacks on $6, 7$ and 8 rounds of DES, respectively. With 6 rounds they considered 3-rounds characteristics proposed in [3]. With 8 rounds they combine their attack with exhaustive search of eight bits of the key. Table 1, taken from [7], presents comparisons between different types of attacks and their results.

TABLE 1. Comparison between different attacks on DES.

No. of rounds	Method of cryptanalysis	No. of ciphertexts	Time (in seconds)
6	Differential ([3])	240 (chosen)	< 1
	Differential ([8])	46 (chosen)	< 10
	Algebraic ([5])	1 (known)	2^{25}
	Diff+Alg ([7])	32 (chosen)	3000
	Diff+Alg ([7])	22 (chosen)	< 3600
7	Diff+Alg ([7])	2000 (chosen)	10000
8	Differential ([3])	50000 (chosen)	100
	Linear ([9])	2^{20} (known)	40
	Diff+Alg ([7])	11500 (chosen)	2^{25}

3. Description of the attack and its results

3.1. General overview

First step is to enhance algebraic attack by using more than one pair plaintext––ciphertext. Given two equation systems F and F^* for two plaintext—ciphertext pairs (P, C) and (P^*, C^*) under the same encryption key K, we can combine these equation systems to form a new set $\overline{F} = F \cup F^*$. Such set has twice as many equations as the original systems, however it provides many new variables. Next step is to take advantage of probabilistic dependencies given from differential cryptanalysis. This leads us to new kind of the attack.

Let assume that attack is applied on cipher having Feistel structure where round function consists of permutations and non-linear transformations implemented as S-boxes. Moreover, assume that for such cipher we have differential characteristic for fixed number of rounds $\Omega = (\delta_0, \delta_1, \ldots, \delta_r)$ where specific difference in ith round occurs with a probability p_i. Then, probability of a characteristic Ω is equal to $p = \Pi p_i$.

Each one-round difference gives rise to equations relating the input and output pairs for active S-Boxes. Let $X_{i,j}$ and $X^*_{i,j}$ denote the jth bit of the input to the S-box layer in ith round for systems F and F^*, respectively. Similarly, let $Y_{i,j}$ and $Y^*_{i,j}$ denote the correspondence output bits. Hence, we are given following expressions

$$X_{i,j} + X^*_{i,j} = \Delta X_{i,j} \rightarrow \Delta Y_{i,j} = Y_{i,j} + Y^*_{i,j}.$$

Values $\Delta X_{i,j}$ and $\Delta Y_{i,j}$ are given from differential characteristic. Similarly, for non-active S-boxes we have the expression

$$X_{i,j} + X^*_{i,j} = 0 = Y_{i,j} + Y^*_{i,j}.$$

If we consider the equation system $\overline{F} = F \cup F^*$, we can combine it with additional equations given from differential characteristic. It leads to the new equation system $\overline{F}^+$which holds with probability p. We can also perform this attack in a chosen plaintext scenario and use such pair which already satisfies differential characteristic used. Advantage of this solution against differential cryptanalysis is that in this scenario we need only one “right pair" which satisfies a set of differences at every round. We also expect system $\overline{F}^+$to be easier to solve than original system while many linear constrains were added without adding any new variables.

A major difficulty in the differential part of our attacks is to find a “right pair" which satisfies a set of differences at every round. In order to find such a pair we first select pairs which satisfy differences at input and at the output, and expect that with high probability they also satisfy additional differences.

This makes a difference between typical differential cryptanalysis, where attacker cares only about distinguishers on observable properties, and presented attack, where we are taking advantage on all the relations arising in the middle of encryption.

Next step of increasing efficiency of presented method is to concatenate sets of equations which are describing more than two pairs: plaintext–ciphertext. Such sets do not share most of the state variables however they still share key variables. Result set is expected to be solved faster than both sets separately while it involves many new variables.

3.2. Description of differential characteristics

The attack, described in this paper, uses two differential characteristics. First one, called iterative characteristic, is two-round characteristic, shown on Fig. 2. Its output is the same as input so it can be concatenated multiple times. However, such operations, lowers its probability, for instance application of it to the attack against DES, reduced to eight rounds, makes its probability equal

$$(1/234)^{-4} \approx 2^{-33}$$

.

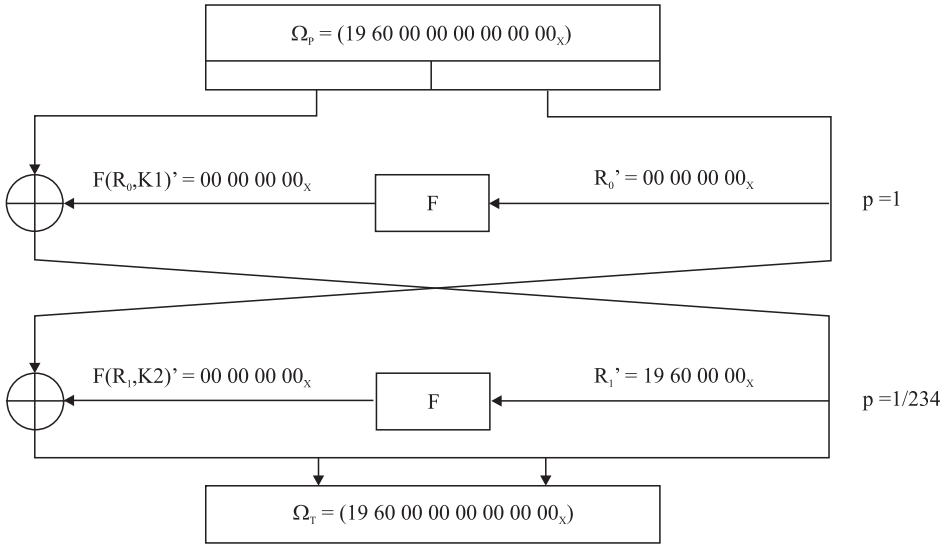

FIGURE 2. Two-round iterative characteristic of DES algorithm.

The second characteristic is five-round characteristic for which the plaintext XOR is $\Omega_p = 40\ 5C\ 00\ 00\ 04\ 00\ 00\ 00_X$. It is shown on Fig. 3 and it has probability $25/2^{18} \approx 1/10485$. For successful attack against eight-round DES we have to assume that output XOR after 5^{th} round will be equal to $\Omega_5 = 40\ 5C\ 00\ 00\ 04\ 00\ 00\ 00_X$. To find such pair we will have to solve the set of equations for every pair satisfying input XOR. If there is no solution, then it means that such pair is wrong. This approach causes the data complexity to be about $25/2^{18} \approx 2^{13.356}$ chosen plaintexts.

The characteristics mentioned above were chosen from those described in [3]. The two-round differential characteristic was chosen, while it can be easily adopted to perform attack on eight rounds. Basics to use five-round characteristic are that it was originally used to implement attack on eight rounds of DES cipher.

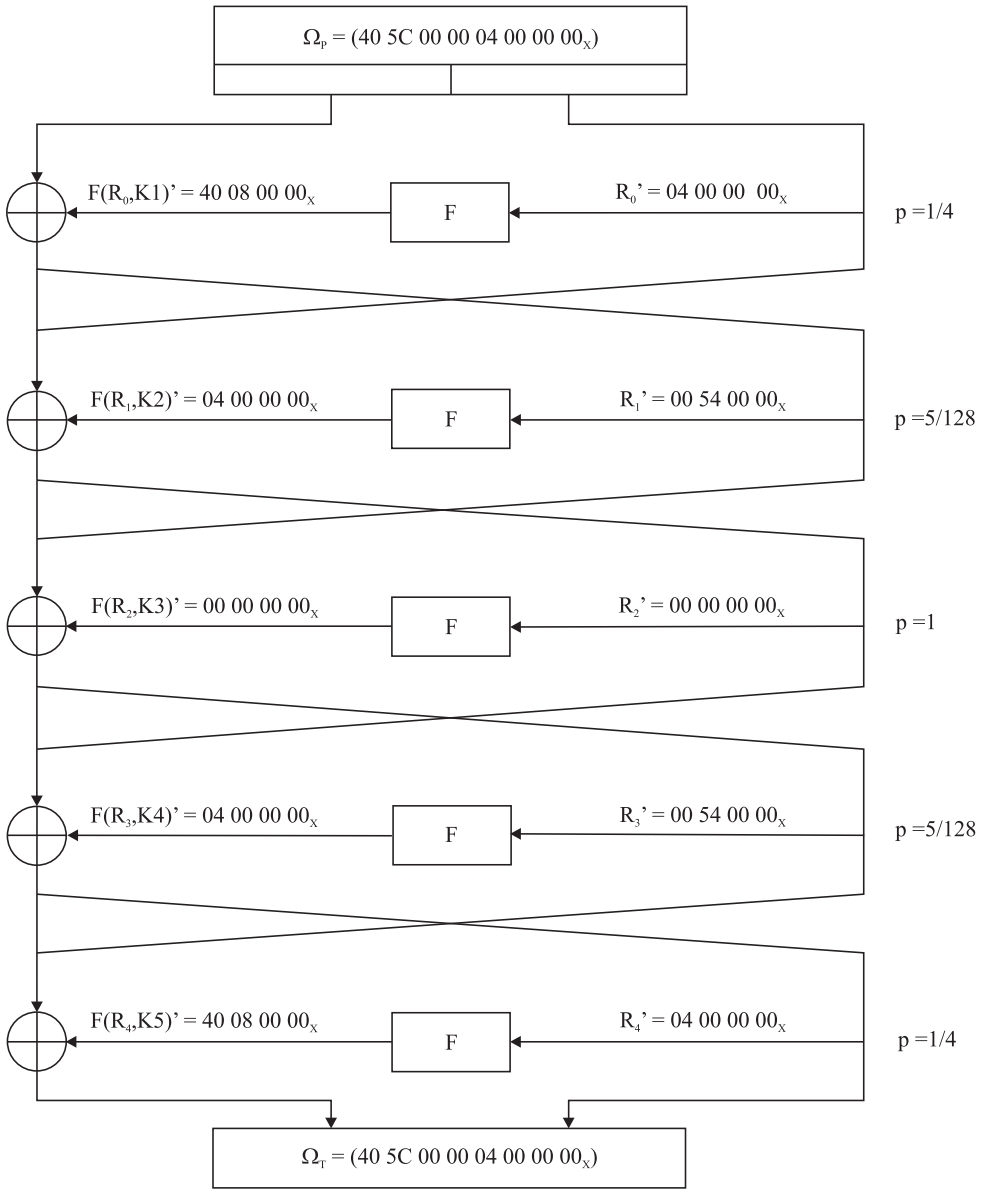

FIGURE 3. Five-round characteristic.

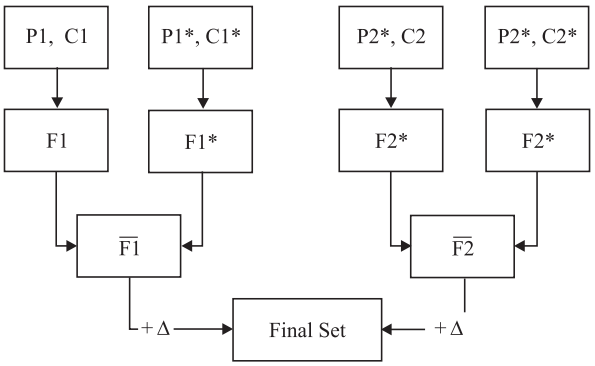

FIGURE 4. General scheme of the attack.

3.3. Performance of the attack and its results

Attack was performed as follows. Two pairs, satisfying a defined characteristic were found. It means we had four plaintexts, P_1, P_1^*, P_2, P_2^*, and four corresponding ciphertexts, namely C_1, C_1^*, C_2, C_2^*. For every pair plaintext—ciphertext, a set of equations, describing the way of encryption, was built. Then all sets were merged to a one set sharing the key variables. The next step was to enhance the final set with equations derived from differential characteristics. This was possible because of the fact that both pairs $(P_1, P_1^*)-(C_1, C_1^*)$ and $(P_2, P_2^*)-(C_2, C_2^*)$ were the right pairs, which means, they satisfied a specific differential characteristic as it was mentioned before. The idea of the attack is presented on Fig. 4.

Finally, all the equations were converted to a form possible to be solved by a selected SAT-solver, which in this case was MiniSat version 1.14 available to download at `http://www.minisat.se/MiniSat.html`. This technique was also applied for more than four plaintexts. Attack was performed on a PC computer equipped with 1.73 Ghz dual core processor and 2 gigabytes of RAM. MiniSat program was run under Linux Ubuntu operational system. Table 2 shows best results of the attack performed on equation systems created from almost 400 chosen plaintexts encrypted with six different, randomly chosen keys.

TABLE 2. Results of combined attack on 8-round DES.

Characteristic used	Right pairs needed	Data complexity	Time (in second)
2-round iterative characteristic (Fig. 2)	2	2^{34}	98007
5-round characteristic (Fig. 3)	3	≈ 32000	15
5-round characteristic (Fig. 3)	4	≈ 42600	25

The second column describes number of "right pairs", namely these which satisfy characteristic given and which were used to build and solve sets of equations. Fourth column shows time needed to solve these sets. Third column describes data complexity, namely chosen plaintexts needed to find "right pair". This complexity is product of right pairs needed and probability of the characteristic.

Time needed to solve the equation with contradiction (created from "wrong pairs") is 0.375 second. For 32000 plaintexts to examine it gives 12000 seconds. Still it is much less time than needed for solution of set built using 2-round iterative characteristic.

4. Conclusion

The attack shown in this paper proved that 8 rounds of DES can be broken without having knowledge of key bits. Differential-algebraic attack is also better than techniques used separately. Although data complexity is worse than it was presented in [7] nevertheless time needed to find the solution is better. Moreover, this attack was performed without exhaustive search over part of bits of the key. This is a work in progress. In particular, we are planning to adapt other ANF to CNF conversion techniques as well as to examine correlation between number of pairs used to attack and the time of solution sets of equations.

REFERENCES

[1] ALBRECHT, M.—CID, C.: *Algebraic techniques in differential cryptanalysis,* IACR Cryptology ePrint Archive, Report 2008/177.

[2] GĄSECKI, A.— MISZTAL, M.: *Application of algebraic techniques in differential cryptanalysis aganst block cipher DES,* MUT Bulletin, Warsaw, 2011.

[3] BIHAM, E.—SHAMIR, A.: *Differential cryptanalysis of DES-like cryptosystems,* in: Advances in Cryptology—CRYPTO '90 (A. Menezes et al., eds.), Santa Barbara, USA, 1990, Lecture Notes in Comput. Sci., Vol. 537, Springer-Verlag, Berlin, 1990, pp. 2–21.

[4] NATIANAL INSTITUTE OF STANDARDS AND TECHNOLOGY: *Data Encryption Standard,* FIPS PUB 46–3, 1999.

[5] COURTOIS, N. T.—BARD, G. V.: *Algebraic cryptanalysis of the data encryption standard,* IACR Cryptology ePrint Archive, Report 2006/402.

[6] COURTOIS, N. T.: *Examples of equations generated for experiments with algebraic cryptanalysis of DES,* `http://www.cryptosystem.net/aes/toyciphers.html`.

[7] FAUGERE, J.-C.—PERRET, L.—SPAENLEHAUER, P.-J.: *Algebraic-differential cryptanalysis of DES,* in: Western European Workshop on Research in Crypt.—WEWoRC '09 (C. Rechberger, ed.), Graz, Austria, 2009, Lecture Notes in Comput. Sci., Vol. 6429, Springer-Verlag, Berlin, 2009, pp. 1–5.

[8] KNUDSEN, L. R.: *Truncated and higher order differentials,* in: Fast Software Encryption, 2nd Internat. Workshop (B. Preneel, ed.), Leuven, Belgium, 1994, Lecture Notes in Comput. Sci., Vol. 1008, Springer-Verlag, Berlin, 1995, pp. 196–211.

[9] MATSUI, M.: *Linear cryptanalysis method for DES cipher,* in: Advances in Cryptology––Eurocrypt '93 (T. Helleseth, ed.), Lofthus, Norway, 1993, Lecture Notes in Comput. Sci., Vol. 765, Springer-Verlag, Berlin, 1993, pp. 386–397.

[10] COURTOIS, N. T.—GAWINECKI, A.—SONG, G.: *Contradiction immunity and guess-then-determine attacks on GOST,* Tatra Mt. Math. Publ. **53** (2012), 65–79.

[11] BIHAM, E.—SHAMIR, A.: *Differential cryptanalysis of the full 16-round DES,* in: Advances in Cryptology—CRYPTO '92 (E. Brickell, ed.), 12th Annual Internat. Cryptology Conf., Santa Barbara, CA, USA, 1992, Lecture Notes in Comput. Sci., Vol. 740, Springer, Berlin, 1993, pp. 487–496.

Received July, 5,2013

Military University of Technology
Cybernetics Faculty
Institut of Mathematics and Cryptology
Kaliskiego St. 2
PL–00-908 Warsaw
POLAND
E-mail: agasecki@wat.edu.pl