Krzysztof CHMIEL
POZNAŃ UNIVERSITY OF TECHNOLOGY

Rough evaluation of block ciphers

PhD Eng. Krzysztof CHMIEL

Assistant professor at Poznań University of Technology, Poland. His research and scientific interests focus on data security in information systems and cryptology, especially methods of designing and cryptanalysis of cryptographic algorithms. He is the author of a number of publications on differential and linear approximation of block ciphers and their component functions.

e-mail: krzysztof.chmiel@put.poznan.pl

Abstract

In the paper a rough evaluation of block ciphers method is presented. As a criterion of quality, effectiveness of the best nonzero linear approximation is taken. The main idea of the method is to evaluate the best nonzero linear approximation of a cipher by a composition of the best nonzero linear approximation of a single iteration. A block cipher quality is compared to quality of a comparative algorithm, with the same block length. The method is applied to a *DES*-like cipher and to the PP-1 cipher which is a scalable SPN.

Keywords: cryptanalysis, linear approximation, block cipher.

Zgrubna ocena szyfrów blokowych

Streszczenie

W artykule przedstawiono zgrubną metodę oceny szyfrów blokowych. Jako kryterium jakości przyjęto efektywność najlepszej niezerowej liniowej aproksymacji. Główna idea prezentowanej metody polega na ocenie najlepszej niezerowej liniowej aproksymacji szyfru przez złożenie najlepszej niezerowej liniowej aproksymacji pojedynczej iteracji. Jakość szyfru porównywana jest z jakością algorytmu porównawczego o tej samej długości bloku. Rozpatrzono własności aproksymacji szyfru blokowego istotne dla oceny. Metoda zgrubna zapewnia górne ograniczenie efektywności najlepszej niezerowej aproksymacji szyfru o właściwie skonstruowanej funkcji iteracji *h*. Dla funkcji *h* wprowadzono S-blok zastępczy klasy q_a o *s* bitach wejściowych. Sformułowano następnie twierdzenie, które dla znanych parametrów S-bloku zastępczego określa liczbę iteracji *r*, wymaganych dla szyfru blokowego by dorównał jakością algorytmowi porównawczemu. Z twierdzenia tego wynika między innymi, że realizacja szyfru o bloku 256-bitowym i większych dla $q_a = 4$ nawet przy $s = 16$ wymaga większej liczby iteracji niż 16. Metodę zgrubną zastosowano do szyfru typu *DES* rozumianego jako szyfr o strukturze Feistela z dowolną funkcją *f* i do szyfru PP-1, który jest skalowalną siecią podstawieniowo-permutacyjną (SPN). W szczególności pokazano, że zgodnie z metodą zgrubną 64-bitowy wariant szyfru PP-1 o 11 rundach ma znacznie lepszą jakość niż 64-rundowy algorytm *DES*, który osiąga jakość algorytmu porównawczego dopiero po poprawieniu S-bloków *S1*, *S5* i *S7* do klasy jakości 4.

Słowa kluczowe: kryptoanaliza, liniowa aproksymacja, szyfr blokowy.

1. Introduction

Well constructed block cipher should be resistant to any kinds of cryptographic attacks. To the most important general methods of cryptanalysis belong to differential cryptanalysis [1, 2] and linear cryptanalysis [2, 5, 6]. Both methods were successfully applied to the Data Encryption Standard, where S-boxes with six input bits are used. In paper [2] it is shown, that with increase of the number of bits, the linear approximation becomes more effective than the differential one. Therefore, the presented evaluation of block ciphers is restricted to the linear approximation.

We distinguish the following three methods of block cipher evaluation. In the first, *exact* method, the best nonzero linear approximation of a cipher is determined [6]. In the second, *rough* method, the best nonzero linear approximation of a cipher is assumed to be a composition of the best nonzero linear approximation of a single iteration. In the third, *intermediate* method, we find the best zero-nonzero approximation of a cipher, that fulfils approximation conditions [3, 4]. The first method should be applied to existing ciphers. The remaining methods, that omit the details of a cipher, are useful at the stage of construction.

The basic idea of linear cryptanalysis is to describe a given cipher algorithm by a linear approximate expression, so-called linear approximation. In general, the *linear approximation* of function $y = f(x)$: $\{0, 1\}^n \to \{0, 1\}^m$ is defined as an arbitrary equation of the form:

$$\bigoplus_{i \in y'} y_i = \bigoplus_{j \in x'} x_j, \tag{1}$$

which is fulfilled with approximation probability $p = N(x', y') / 2^n$, where $x' \subseteq \{1, 2, ..., n\}$, $y' \subseteq \{1, 2, ..., m\}$ and $N(x', y')$ denotes the number of pairs (x, y) with $y = f(x)$ for which the equation holds. For simplicity the above equation is written in the following form:

$$y[y'] = x[x']. \tag{2}$$

The sets of indexes x', y' are called input and output *mask* respectively and the function $N(x', y')$ is called the *counting function* of the approximation. Masks x', y' are often denoted by numbers, corresponding to the zero-one representation of sets. Among approximations we distinguish the *zero-approximation*, for which $x' = y' = \Phi$. Probability p of the zero-approximation is equal to 1 for arbitrary function *f*.

The *effectiveness* of the linear approximation of function *f* is represented by magnitude of $|\Delta p| = |p - 1/2|$. Approximations with positive value of the effectiveness measure are said to be effective. Effectiveness of the zero-approximation $|\Delta p^0| = 1/2$. For effectiveness of nonzero approximation it holds $|\Delta p^+| \le 1/2$.

By *composition* of approximations $y_1[y_1'] = x_1[x_1']$ and $y_2[y_2'] = x_2[x_2']$ we mean approximation $y_1[y_1'] \oplus y_2[y_2'] = x_1[x_1'] \oplus x_2[x_2']$.

Definition 1

We say, that a given S-box is of *quality class q*, if for effectiveness of nonzero approximation of its function *f* the following holds:

$$|\Delta p^+| \le q/2^{\lfloor n/2 \rfloor + 1}. \tag{3}$$

2. Comparative algorithm

The comparative algorithm (Fig. 1) is a block cipher with a single round, which encrypts *n*-bit plaintext *m* into *n*-bit ciphertext *c* under *n*-bit key *k*, in the following way:

$$c = S_p(m \oplus k). \tag{4}$$

Decryption performed by comparative algorithm is as follows:

$$m = S_p^{-1}(c) \oplus k. \tag{5}$$

Quality of the comparative algorithm depends on quality of S-box S_p. Assuming that S-box S_p is of quality class q_p, we have:

$$|\Delta p_p^+| \le q_p/2^{\lfloor n/2 \rfloor + 1}. \tag{6}$$

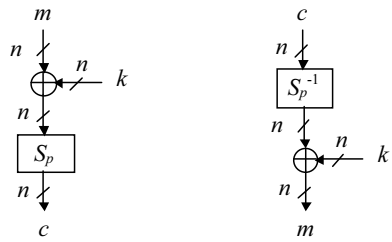

Fig. 1. Encryption and decryption performed by comparative algorithm
Rys. 1. Szyfrowanie i deszyfrowanie algorytmem porównawczym

3. Properties of a block cipher approximation

Let us consider, important for the evaluation method, properties of the linear approximation A of a block cipher with r iterations shown in Figure 2.

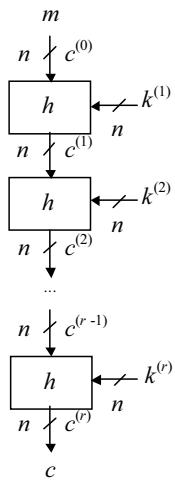

Fig. 2. General structure of a block cipher
Rys. 2. Ogólna struktura szyfru blokowego

Approximation A is a composition of approximations A_j of iteration function h where $j = 1, 2, ..., r$. Probability p_a of A approximation can be calculated by formula:

$$\Delta p_a = 2^{r-1} \prod_{j=1}^{r} \Delta p_j, \tag{7}$$

where p_j is the probability of A_j approximation.

In the following, the zero approximation of a cipher is denoted by A^0, a nonzero approximation by A^+ and nonzero approximation with the zero input mask is denoted by A^{+0}. Similar notation is used to other approximations in particular to A_j approximations.

Property 1

Cipher approximation A is effective if and only if all iteration approximations A_j are effective, i.e. it holds:

$$\Delta p_a \neq 0 \Leftrightarrow \Delta p_j \neq 0 \text{ for all } 1 \leq j \leq r. \tag{8}$$

Property 2

Cipher approximation A is the zero approximation if and only if all iteration approximations A_j are the zero approximations, i.e. it holds:

$$A = A^0 \Leftrightarrow A_j = Aj^0 \text{ for all } 1 \leq j \leq r. \tag{9}$$

Property 3

The only effective cipher approximation A with the zero output mask is the zero approximation A^0, moreover it holds:

$$\Delta p_a \neq 0 \text{ and } c' = \Phi \Leftrightarrow A = A^0. \tag{10}$$

Definition 2

Function $y = h(x, k)$: $\{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$ is said to be *properly constructed*, if the only effective approximation of function h with the zero input mask x' is the zero approximation.

Property 4

The only effective cipher approximation A with the zero input mask is the zero approximation A^0 if and only if the iteration function h is properly constructed, moreover it holds:

$$(\Delta p_a \neq 0 \text{ and } m' = \Phi \Leftrightarrow A = A^0) \Leftrightarrow$$
$$\Leftrightarrow h \text{ is properly constructed.} \tag{11}$$

If function h is not properly constructed then there exists an effective nonzero cipher approximation with the zero input mask A^{+0} which is a composition of the zero approximations A_j^0 of all iterations apart from the last one and a nonzero approximation of the last iteration with the zero input mask A_r^{+0}. Then, from formula (4), we obtain:

$$\Delta p_a^{+0} = 2^{r-1} \prod_{j=1}^{r-1} (1/2) \cdot \Delta p_r^{+0} = \Delta p_r^{+0}. \tag{12}$$

Effectiveness of such an approximation A^{+0} is not dependent on the number r of rounds and is equal to the effectiveness of the last iteration approximation A_r^{+0}.

For properly constructed iteration function h, each effective nonzero cipher approximation A^+ is a composition of r nonzero iteration approximations A_j^+. Then, it holds:

$$\Delta p_a^+ = 2^{r-1} \prod_{j=1}^{r} \Delta p_j^+. \tag{13}$$

Taking into account formula (13), the rough method assures the upper bound on effectiveness of the best nonzero approximation of a cipher with properly constructed iteration function h.

4. The rough method

A block cipher quality should not be worse than quality of the comparative algorithm, with the same block length. For a given quality of the round function h of a cipher, evaluation of the cipher quality reduces in fact to verification, whether sufficient number r of rounds is applied.

Definition 3

By the substitute S-box for function h we mean an S-box of quality class q_a with s input bits, such that:

$$|\Delta p_h^+| \leq q_a / 2^{\lfloor s/2 \rfloor + 1}. \tag{14}$$

Assume that for all nonzero approximations A_j^+ of iteration function h, where $j = 1, 2, ..., r$, formula (14) holds. This assumption means, that effectiveness $|\Delta p_j^+|$ of approximation A_j^+ is not greater than effectiveness of the best nonzero approximation of the substitute S-box. Then, from formula (13), we obtain:

$$|\Delta p_a^+| \leq (1/2) \cdot (q_a / 2^{\lfloor s/2 \rfloor})^r. \tag{15}$$

In Table 1 is shown maximum effectiveness $|\Delta p_a^+|$, calculated by formula (15) for some chosen values of s and r, assuming $q_a = 4$. For the substitute S-box with the number of input bits $s = 4$, we obtain $|\Delta p_a^+| = 1/2$ for any number r of iterations. Function h is too weak to construct a cipher. By comparison with formula (6) assuming $q_p = 1$, we obtain that quality of the comparative algorithm with block length n equal to 32 and 64 bits is reached for $s = 6$ in the case of $r = 16$ and $r = 32$ respectively . For $s = 8$, realization of a cipher with block length of 32, 64 and 128 bits requires respectively of 8, 16 and 32 iterations.

Tab. 1. Maximum effectiveness $|\Delta p_a^+|$ of a cipher approximation ($q_a = 4$)
Tab. 1. Maksymalna efektywność $|\Delta p_a^+|$ aproksymacji szyfru ($q_a = 4$)

s	r					
	8	**16**	**24**	**32**	**40**	**48**
4	1/2	1/2	1/2	1/2	1/2	1/2
6	$1/2^{9}$	$1/2^{17}$	$1/2^{25}$	$1/2^{33}$	$1/2^{41}$	$1/2^{49}$
8	$1/2^{17}$	$1/2^{33}$	$1/2^{49}$	$1/2^{65}$	$1/2^{81}$	$1/2^{97}$
10	$1/2^{25}$	$1/2^{49}$	$1/2^{73}$	$1/2^{97}$	$1/2^{121}$	$1/2^{145}$
12	$1/2^{33}$	$1/2^{65}$	$1/2^{97}$	$1/2^{129}$	$1/2^{161}$	$1/2^{193}$
14	$1/2^{41}$	$1/2^{81}$	$1/2^{121}$	$1/2^{161}$	$1/2^{201}$	$1/2^{241}$
16	$1/2^{49}$	$1/2^{97}$	$1/2^{145}$	$1/2^{193}$	$1/2^{241}$	$1/2^{289}$

Theorem 1

The number r of iterations, required by a block cipher to reach the quality of the comparative algorithm is expressed by the following formula:

$$r \geq (\lfloor n/2 \rfloor - \lg q_p) / (\lfloor s/2 \rfloor - \lg q_a), \tag{16}$$

where n and q_p are parameters of the comparative algorithm, s and q_a are parameters of the substitute S-box for iteration function h and lg denotes the binary logarithm.

Proof

A block cipher reaches quality of the comparative algorithm if for the best nonzero approximations of the cipher and the algorithm holds:

$$|\Delta p_a^+| \leq |\Delta p_p^+|. \tag{17}$$

For the upper bounds on effectiveness, $|\Delta p_a^+|$ from formula (15) and $|\Delta p_p^+|$ from formula (6), of the best nonzero approximations of the cipher and algorithm we have:

$$(q_a / 2^{\lfloor s/2 \rfloor})^r \leq q_p / 2^{\lfloor n/2 \rfloor}. \tag{18}$$

After calculation of r we obtain formula (16).

■

The minimal values of r, assuming $q_a = 4$ and $q_p = 1$, are presented in Table 2. It follows from the table that realization of a cipher with block length of 256 bits or greater, even for $s = 16$, requires more than 16 iterations. To realize a cipher with 16 iterations and block length at least of 256 bits, it is necessary to strengthen the iteration function h so that the number of the input bits of the substitute S-box was greater than 16.

Tab. 2. The minimal number r of iterations for a block cipher ($q_a = 4$, $q_p = 1$)
Tab. 2. Minimalna liczba r iteracji dla szyfru blokowego ($q_a = 4$, $q_p = 1$)

s	n					
	32	**64**	**128**	**256**	**512**	**1024**
4	∞	∞	∞	∞	∞	∞
6	16	32	64	128	256	512
8	8	16	32	64	128	256
10	5.3	10.7	21.3	42.7	85.3	170.6
12	4	8	16	32	64	128
14	3.2	6.4	12.8	25.6	51.2	102.4
16	2.7	5.3	10.7	21.3	42.7	85.3

5. Rough evaluation of a *DES*-like cipher

By a *DES*-like cipher we mean the Feistel structure with r rounds and an arbitrary function f. Let h_1 be the round function. It can easily be shown that for the best approximation A_{h1}^+ it holds $\Delta p_{h1}^+ = \Delta p_f^0 = 1/2$. For composition of r best approximations A_{h1}^+ we obtain:

$$\Delta p_a^+ = 2^{r-1} \prod_{j=1}^{r} (1/2) = 1/2. \tag{19}$$

The rough method applied to a *DES*-like cipher leads to the trivial evaluation of the cipher quality. Let us extend the method to function h_2 composed of two rounds, shown in Figure 3.

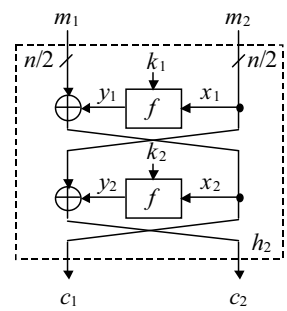

Fig. 3. Iteration function h_2 of a *DES*-like cipher
Rys. 3. Funkcja iteracji h_2 szyfru typu *DES*

The general form of the linear approximation of function $c_1||c_2 = h_2(m_1||m_2, k_1, k_2)$ is:

$$c_1[c_1'] \oplus c_2[c_2'] = m_1[m_1'] \oplus m_2[m_2'] \oplus k_1[k_1'] \oplus k_2[k_2']. \tag{20}$$

Theorem 2

For masks of the general form (20) of the linear approximation of function h_2 it holds:

$$m_1' = y_1', m_2' = y_2' \oplus x_1', \tag{21}$$

$$c_1' = y_1' \oplus x_2', c_2' = y_2', \tag{22}$$

where x_1', y_1', x_2', y_2' are masks of the first and second function f approximations.

Proof

To compute the linear approximation of function h_2, for given linear approximations of both functions f, the following set of equations can be written, that describe the linear approximations of functions f and *XOR* of consecutive rounds:

$$y_1[y_1'] = x_1[x_1'] \oplus k_1[k_1'], \tag{23}$$

$$x_2[y_1'] = y_1[y_1'] \oplus m_1[y_1'], \tag{24}$$

$$y_2[y_2'] = x_2[x_2'] \oplus k_2[k_2'], \tag{25}$$

$$c_2[y_2'] = y_2[y_2'] \oplus x_1[y_2']. \tag{26}$$

After addition of the above equations modulo 2, we obtain:

$$x_2[y_1'] \oplus x_2[x_2'] \oplus c_2[y_2'] = m_1[y_1'] \oplus$$

$$\oplus x_1[y_2'] \oplus x_1[x_1'] \oplus k_1[k_1'] \oplus k_2[k_2']. \tag{27}$$

Considering that $x_2 = c_1$ and $x_1 = m_2$, we have:

$$c_1[y_1' \oplus x_2'] \oplus c_2[y_2'] = m_1[y_1'] \oplus$$

$$\oplus m_2[y_2' \oplus x_1'] \oplus k_1[k_1'] \oplus k_2[k_2']. \tag{28}$$

■

From theorem 2 it follows that for the zero approximation of both functions f is obtained the zero approximation of function h_2. For the best approximation A_{h2}^{+} it holds: $\Delta p_{h2}^{+} = 2\Delta p_f{}^{0}\Delta p_f{}^{+} = \Delta p_f{}^{+}$. For composition of $r/2$ best approximations A_{h2}^{+} we obtain:

$$\Delta p_a{}^{+} = 2^{r/2-1}\prod_{j=1}^{r/2}\Delta p_f{}^{+}. \tag{29}$$

The extended rough method applied to a *DES*-like cipher with an even number r of rounds leads to evaluation of the cipher quality based on composition of $r/2$ best nonzero approximations of function f.

Assume that the worst S-box *S5* of *DES* is the substitute S-box for properly constructed iteration function h_2 of the cipher, i.e. $q_a = 5$ and $s = 6$. In Table 3 is shown comparison of a *DES*-like cipher with the comparative algorithm. The block length n is a multiple of 64 bits. The number r of iterations was determined by formula (16) for $q_a = 4$ and $q_p = 1$.

Tab. 3. Quality of a *DES*-like cipher and of the comparative algorithm ($s = 6$)
Tab. 3. Jakość szyfru typu *DES* i algorytmu porównawczego ($s = 6$)

n	64	128	192	256
r	64	128	192	256
$\lvert\Delta p_a^{+}\rvert$ for $q_a = 5$	$1.23/2^{23}$	$1.52/2^{45}$	$1.87/2^{67}$	$1.15/2^{88}$
$\lvert\Delta p_p^{+}\rvert$ for $q_p = 1$	$1/2^{33}$	$1/2^{65}$	$1/2^{97}$	$1/2^{129}$
$\lvert\Delta p_a^{+}\rvert$ for $q_a = 4$	$1/2^{33}$	$1/2^{65}$	$1/2^{97}$	$1/2^{129}$

From Table 3 it follows that the quality of a *DES*-like cipher with block length n is significantly worse than the quality of the comparative algorithm. The cipher is not worse than the comparative algorithm in the case of improvement of the substitute S-box to quality class $q_a = 4$. In particular, the 64-bit *DES* cipher reaches the quality of the comparative algorithm for the number of rounds $r = 64$ after improvement of S-boxes *S1*, *S5* and *S7* to quality class $q = 4$.

6. Rough evaluation of PP-1 cipher

Block length n of the PP-1 cipher is a multiple of 64 bits and S-box S of dimension 8×8 bits is of quality class $q = 2.25$. Assume that S-box S is the substitute S-box for properly constructed iteration function h of the cipher, i.e. $q_a = q$ and $s = 8$. In Table 4 is shown comparison of the PP-1 cipher with the comparative algorithm. The number r of iterations was determined by formula (16) for $q_a = q \approx 2$ and $q_p = 1$.

Tab. 4. Quality of the PP-1 cipher and of the comparative algorithm ($s = 8$)
Tab. 4. Jakość szyfru PP-1 i algorytmu porównawczego ($s = 8$)

n	64	128	192	256
r	11	22	32	43
$\lvert\Delta p_a^{+}\rvert$ for $q_a = 2.25$	$1.83/2^{33}$	$1.67/2^{64}$	$1.35/2^{92}$	$1.24/2^{123}$
$\lvert\Delta p_p^{+}\rvert$ for $q_p = 1$	$1/2^{33}$	$1/2^{65}$	$1/2^{97}$	$1/2^{129}$
$\lvert\Delta p_a^{+}\rvert$ for $q_a = 2$	$1/2^{34}$	$1/2^{67}$	$1/2^{97}$	$1/2^{130}$

From Table 4 it follows that the quality of the PP-1 cipher with block length n is slightly worse than the quality of the comparative algorithm. The PP-1 cipher is not worse than the comparative algorithm in the case of improvement of S-box S to quality class $q = 2$.

7. Conclusion

The presented in the paper rough evaluation method of block ciphers gives an upper bound to effectiveness of the best, i.e. most effective, nonzero linear approximation of the cipher. The upper bound should not be greater than upper bound obtained for the comparative algorithm with the same block length. For a given quality of the round function, evaluation of the cipher quality reduces in fact to verification, whether sufficient number of rounds is applied. According to the rough method, the 64-bit variant of the PP-1 cipher with 11 rounds is of much better quality than 64-round *DES*, which reaches the quality of the comparative algorithm only after improvement of S-boxes *S*1, *S*5 and *S*7 to quality class 4.

8. References

[1] Biham E., Shamir A.: Differential Cryptanalysis of the Data Encryption Standard, Springer-Verlag, Berlin Heidelberg New York 1993.

[2] Chmiel K.: On Differential and Linear Approximation of S-box Functions, In Saeed K., Pejaś, J., Mosdorf R. (Eds) Biometrics, Computer Security Systems and Artificial Intelligence Applications, Springer, pp. 111-120, New York 2006.

[3] Chmiel K.: Intermediate Evaluation of Block Ciphers, Proceedings of the 13-th International Multi-Conference on Advanced Computer Systems ACS'2006, vol. 1, pp. 331-342, Szczecin 2006.

[4] Chmiel K., Intermediate Evaluation of DES-like Cryptosystems, Proceedings of Military CIS Conference, MCC 2007, (Bonn, Sept. 25-26), ISBN 978-3-934401-16-7, pp. 1-7, Bonn 2007.

[5] Chmiel K., Grocholewska-Czuryło A., Stokłosa J., Involutional Block Cipher for Limited Resources, Proceedings of IEEE GLOBECOM Conference, (Nov. 30 - Dec. 4), pp. 1-5, New Orleans 2008.

[6] Matsui M.: Linear Cryptanalysis Method for DES Cipher, In Helleseth, T. (ed.) Advances in Cryptology Eurocrypt'93, Springer, pp. 386-397, New York 1994.

Artykuł recenzowany