NEW EXPERIMENTAL RESULTS IN DIFFERENTIAL – LINEAR CRYPTANALYSIS OF REDUCED VARIANTS OF DES[1]

ANNA GÓRSKA[1], KAROL GÓRSKI[1], ZBIGNIEW KOTULSKI[2], ANDRZEJ PASZKIEWICZ[3], JANUSZ SZCZEPAŃSKI[2]

[1]ENIGMA Information Security Systems Sp. z o.o., Cryptography Dept., ul. Cietrzewia 8, 02-492 Warsaw, POLAND, ph./fax: (+48 22) 863 62 65, email: {ania, karol}@enigma.com.pl

[2]Institute of Fundamental Technological Research, Polish Academy of Sciences, ul. Świętokrzyska 21, 00-049 Warsaw, POLAND, ph.:fax: (+48 22) 826 12 81, (+48 22) 826 98 15, email: {zkotulsk, jszczepa}@ippt.gov.pl

[3]Institute of Telecommunications, Warsaw University of Technology, ul. Nowowiejska 15/19, 00-665 Warsaw, POLAND, ph.: (+48 22) 660 78 35, fax: (+48 22) 825 49 50, email: anpa@tele.pw.edu.pl

Abstract: At the beginning of the paper we give an overview of linear and differential cryptanalysis of block ciphers. We describe two extensions of linear cryptanalysis (analysis with multiple expressions [7] and differential-linear cryptanalysis [10]) which form the basis of the conducted experiments. Then we describe the functioning of truncated differentials [1],[8] and the usage of differential structures ([1],[2] and [3]).

In the second part of the article we present experimental results of implementation of differential-linear cryptanalysis with multiple expressions applied to reduced DES variants. In an attack on DES reduced to 8 rounds we obtained a significant reduction in the number of needed chosen pairs of texts – reduction by a factor greater than 4.

Key words: cryptology, linear cryptanalysis, differential cryptanalysis, multiple expressions, differential structures

[1] This work has been supported by grant No 8 T11D 020 19 of the Polish Scientific Research Committee.

1. INTRODUCTION

Symmetric block ciphers are one of the fundamental tools in modern cryptography. Their popularity requires a high level of trust in their security. Unfortunately there are neither known constructions of block ciphers, which offer unconditional security nor practical constructions, which offer provable computational security. So in practice evaluations of the security of these ciphers is heuristic. The effectiveness of an attack is measured by a comparison of its complexity (time and memory) with the exhaustive search attack. During this evaluation only those attacks are taken into account, which are known at the time. One of the most important attacks considered is linear cryptanalysis. In 1993 it was successfully used by Matsui to analyse DES [11]. It needed 2^{43} known plaintext/ciphertext pairs to derive 26 bits of the key.

Since 1993 several extensions of linear cryptanalysis appeared (from the use of multiple expressions [7], through non-linear approximations in outer rounds [9], probabilistic counting [15] and Shimoyama's extension [16] to differential-linear cryptanalysis [10]). In our previous paper [20] we have suggested that the complete evaluation of the resistance of a block cipher to linear cryptanalysis should consider combining the extensions mentioned above.

The purpose of this paper is to describe recent experimental results of combining the extensions of linear cryptanalysis. We have added multiple expressions to the differential-linear analysis, which results in a decrease of the amount of analysed texts in an attack on DES reduced to 8 rounds by a factor greater than 4.

1.1 NOTATION AND DEFINITIONS

Throughout this paper we use Matsui's numbering of DES bits. The input bits, key bits and output bits of F-functions, S-boxes, etc. are numbered from right to left starting from 0. We also use Matsui's notation in which $A[i]$ denotes i-th bit of vector A, while $A[i_1, i_2, \ldots i_n]$ denotes exclusive or of the bits of vector A located in positions $i_1, i_2, \ldots i_n$. We also use the notation of Harpes [6] in which $A \bullet \Gamma A$ denotes scalar multiplication of two binary vectors over GF(2), which is equivalent to an exclusive or of the bits of A chosen by binary vector ΓA (e.g. A = 1011, ΓA = 0001, then $A \bullet \Gamma A = 0 \oplus 0 \oplus 0 \oplus 1 = A[i_4]$).

Let P, C, K denote plaintext, ciphertext and key. We assume that plaintexts, ciphertexts and keys are uniformly distributed in appropriate spaces. We also assume that round keys are independent.

By r we denote the number of rounds, while by C_i we denote the ciphertext after round i, which means that $P = C_0$ and $C = C_r$. N denotes the number of analysed pairs of texts.

A linear approximation is a linear dependence between bits of the round input block, bits of the round output block and bits of the round subkey. A linear expression is a linear dependence between bits of the cipher input, cipher output and bits of all the subkeys. An effective linear expression is an expression which holds with probability different from 1/2.

Probability of the linear approximation (p) is defined in the probabilistic space with:

- a set of elementary events Ω, which is a Cartesian product of the set of all input blocks to the round and all subkey blocks,
- σ - field which is the set of all subsets of Ω,
- probability distribution on the elementary events assigning to each of them equal probability.

There is a random variable defined in this space, which assigns to each elementary event the value 0 or 1, dependent on whether the approximation holds or not. Event X is defined as a sum of the elementary events for which the random variable is equal to 0. Probability of a linear approximation is equal to the probability of event X in this probabilistic space.

1.2 LINEAR CRYPTANALYSIS

The basic idea of linear cryptanalysis is to find an effective linear expression for an analysed block cipher, s.t.:

$$(P \bullet \Gamma P) \oplus (C \bullet \Gamma C) = \Sigma_z (K_z \bullet \Gamma K_z). \qquad (1)$$

with a certain probability p, measured over all choices of plaintext P and key K.

In the case of iterative block ciphers, finding the linear expression has 2 steps. At first we linearise one round, looking for effective approximations of non-linear elements, then we

combine them to derive round approximation of the following form:

$$(C_{i-1} \bullet \Gamma C_{i-1}) \oplus (C_i \bullet \Gamma C_i) = K_i \bullet \Gamma K_i \qquad (2)$$

where C_{i-1} is the input vector to round i, C_i is the output vector from round i and K_i is the key used in round i. A linear expression is obtained by combining linear approximations in such a way, that only bits of plaintext, ciphertext and subkeys appear in the final expression. For a few rounds of a cipher and for ciphers with a simple structure (e.g. RC5) this process can be done manually, but in most cases it is easier to use a computer. The algorithms for finding linear expressions for DES can be found in [13], [14], [17], the comparison of their effectiveness can be found in [17] and discussion of the potential mistakes can be found in [4].

With an effective linear expression we can start a so-called 0R attack (algorithm 1), based on the maximum likelihood method. This attack determines with required probability whether the right side of equation 1 is equal to 0 or 1. The success rate of the attack increases with the number of analysed texts and with the bias |p - 1/2|.

Algorithm 1 (attack 0R) [11]
Input:
N known pairs of plaintext and ciphertext,
effective linear expression with probability p
Step 1:
For each pair count the value of left side of equation 1. Let N_0 be the number of pairs for which the left side of the equation is equal to 0.
Step 2:
If $N_0 > N/2$ then
set $\Sigma_z(K_z \bullet \Gamma K_z) = 0$, if $p>1/2$ and 1 if $p<1/2$,
else
set $\Sigma_z(K_z \bullet \Gamma K_z) = 1$, if $p>1/2$ and 0 if $p<1/2$.
Output:
the value of $\Sigma_z(K_z \bullet \Gamma K_z)$ (correct with probability dependent on N and $|p - 1/2|$).

In practical attacks with similar complexity we can obtain more subkey bits. For this purpose attacks with round reduction are used (1R and 2R). The first uses an effective linear expression for r-1 rounds and computes the inverse of the last round of the cipher for each candidate for the last round subkey. For each candidate we count the difference between the number of times when the left side of the linear expression is equal to 0 and when it is equal to 1. For the correct subkey the difference between this value and $N/2$ (relative to N) will be close to the expected bias for the expression in use. For incorrect keys it will be close to 0. In this way we can determine with the required probability the subkey bits in the last round and the value of the modulo 2 sum of the subkey bits appearing in the linear expression. The idea of this attack is based on a hypothesis described by Harpes [6] that the choice of an incorrect key in the last round is equivalent to adding an additional round to the cipher, which decreases the effectiveness of the linear expression in use. In practice checking all the possible values of the subkey in the last round is too complex (requires too much memory). The solution is to check only a subset of the bits of the last round subkey.

In a similar way the 1R attack can be used for the reduction of the first round of the cipher.

Algorithm 2 (attack 1R) [11]
Input:
N known pairs of plaintext and ciphertext,
effective subset of last round subkey bits being searched
effective linear expression for r-1 rounds with probability p, which uses only these bits of C_{r-1} which can by computed from the effective subset of subkey bits
Step 1:
For value of K^i_r effective bits of subkey K_r, let N_0^i denote the number of pairs of texts for which the left side of the (r-1) - round linear expression is equal to 0.
Step 2:
Let $N_{0max} = \max_i (N_0^i)$ and $N_{0min} = \min_i (N_0^i)$.
Step 3:
If $|N_{0max} - N/2| > |N_{0min} - N/2|$ then
set the value of effective subkey bits K^i_r corresponding to N_{0max},
set $\Sigma_z(K_z \bullet \Gamma K_z) = 0$, if $p>1/2$ and 1 if $p<1/2$,
If $|N_{0max} - N/2| < |N_{0min} - N/2|$ then
set the value of effective subkey bits K^i_r corresponding to N_{0min},
set $\Sigma_z(K_z \bullet \Gamma K_z) = 1$, if $p>1/2$ and 0 if $p<1/2$,
Output:
effective subkey bits in last round,
the value of $\Sigma_z(K_z \bullet \Gamma K_z)$ for rounds 1 to r-1,
both results returned with probability dependent on N and $|p-1/2|$.

The 2R attack allows further increase of the effectiveness of the analysis. The idea is similar to the 1R attack: we use an expression for *r*-2 rounds of the cipher and invert the first and the last round.

2. PROBABILISTIC FUNDAMENTALS OF LINEAR CRYPTANALYSIS

In this section we sketch the probabilistic tools which form the basis of linear cryptanalysis. Among these tools we should list first the piling-up lemma (used to calculate the linear expression probability from probabilities of linear approximations and to calculate the success rate), the Moivre-Laplace theorem and the formula for total probability (which are fundamental for the construction of the algorithms for 0R, 1R and 2R attacks).

Lemma 1 (Piling-Up) [11]

Let $Appr_i$ $(1 \le i \le r)$ be independent, random variables, which are equal to 0 with probability p_i and are equal to 1 with probability $1 - p_i$. Then the probability that

$$Appr_1 \oplus Appr_2 \oplus ... \oplus Appr_r = 0 \qquad (3)$$

is equal to:

$$1/2 + 2^{r-1} \prod_{i=1}^{r} (p_i - 1/2). \qquad (4)$$

Theorem 1 (Moivre-Laplace) [5]

Let random variable *Appr* realise some event (called success) with probability p, and opposite event with probability $q = 1 - p$. By S_N denote a random variable which represents the number of successes in N independent trials of variable *Appr*. We define a standardised random variable S_N':

$$S_N' = \frac{\frac{S_N}{N} - p}{\sqrt{\frac{pq}{N}}} \qquad (5)$$

Then, if $0 < p < 1$:

$$\lim_{N\to\infty} \Pr(\{a < S_N' < b\}) = \frac{1}{\sqrt{2\pi}} \int_a^b e^{-t^2/2} dt, \qquad (6)$$

where $a, b \in R$.

According to this theorem, for large enough N, the distribution of S_N' converges to the standardised normal distribution (N(0;1)).

2.1 Probabilistic fundamentals of the 0R attack

From the probabilistic point of view a (random) choice of N plaintext blocks and evaluation of the left side of equation (1) can be treated as N independent trials, where by success we mean obtaining zero (with probability p), and by failure obtaining one (with probability $q = 1 - p$).

Let $p > 1/2$. The probability of correct decision is equal to the probability that the number of successes N_0 in the Bernoulli scheme is greater than $N/2$. In this case N_0 describes the random variable S_N in theorem 1 formulated above. We get a sequence of equivalences:

$$N_0 > N/2 \Leftrightarrow S_N > N/2 \Leftrightarrow S_N/N > 1/2 \Leftrightarrow$$

$$\Leftrightarrow \frac{S_N}{N} - p > \frac{1}{2} - p \Leftrightarrow \frac{\frac{S_N}{N} - p}{\sqrt{\frac{pq}{N}}} > \frac{\frac{1}{2} - p}{\sqrt{\frac{pq}{N}}}. \qquad (7)$$

Therefore:

$$\Pr(N_0 > N/2) = \Pr(S_N > N/2) = \Pr(S_N/N > 1/2) =$$

$$= \Pr\left(\frac{\frac{S_N}{N} - p}{\sqrt{\frac{pq}{N}}} > \left(\frac{\frac{1}{2} - p}{\sqrt{\frac{pq}{N}}}\right)\right) = \Pr\left(S_N > \frac{\frac{1}{2} - p}{\sqrt{\frac{pq}{N}}}\right). \qquad (8)$$

In practical ciphers probability p (and also q) should be close to 1/2, so we obtain that $\sqrt{pq} \approx 1/2$ and in consequence an approximation of (8):

$$\Pr(N_0 > N/2) = \Pr(S_N > -2\sqrt{N}\,(p-1/2)). \qquad (9)$$

For large enough N from theorem 1 we obtain:

$$\Pr(N_0 > N/2) = \frac{1}{\sqrt{2\pi}} \int_{-2\sqrt{N}(p-1/2)}^{\infty} e^{-t^2/2} dt. \qquad (10)$$

This equation describes the success rate (Table 1) for some probability p of a linear expression. This probability increases when the number of analysed texts increases and when bias $|p\text{-}1/2|$ increases.

N	$1/4\|p\text{-}1/2\|^{-2}$	$1/2\|p\text{-}1/2\|^{-2}$	$\|p\text{-}1/2\|^{-2}$	$2\|p\text{-}1/2\|^{-2}$
SR	84,1%	92,1%	97,7%	99,8%

Table 1. Success rate of 0R attack

2.2 Probabilistic fundamentals of 1R attack

We assume that the following equations hold with probability q_i:

$$F_r(C_r, k_r) \bullet IC_{r-1} = F_r(C_r, K^i_r) \bullet IC_{r-1}, \qquad (11)$$

where C_r are randomly chosen, k_r is the real value of last round subkey, K^i_r are the candidates for the subkey value. F_r is the last round function with one of the arguments reduced to the length of effective subkey bits. The F_r value for each candidate K^i_r is substituted in place of C_{r-1} used in the linear expression for r-1 rounds.

Assume for simplicity $|N_{0max} - N/2| > |N_{0min} - N/2|$. Then the probability of the correct choice of subkey bits is:

$$\Pr(K^i_{r\,max} = k_r) = \frac{1}{\sqrt{2\pi}} \int_{-2\sqrt{N}(p-1/2)}^{\infty} te^{-x^2/2} dx,$$

where

$$t = \prod_{K^i_r \neq k_r} \int_{-x-4\sqrt{N}(p-1/2)q^i}^{x+4\sqrt{N}(p-1/2)(1-q^i)} \frac{1}{\sqrt{2\pi}} e^{-y^2/2} dy$$

The above equation describes the success rate (Table 2) of the 1R attack.

N	$2\|p\text{-}1/2\|^{-2}$	$4\|p\text{-}1/2\|^{-2}$	$8\|p\text{-}1/2\|^{-2}$	$16\|p\text{-}1/2\|^{-2}$
SR	48,6%	78,5%	96,7%	99,9%

Table 2. Success rate of 1R attack

3. DIFFERENTIAL CRYPTANALYSIS

Differential cryptanalysis is a method which analyses the effect of the differences of plaintext pairs on differences of ciphertext pairs. These differences are used to assign probabilities to keys and to determine the most probable key. In the case of DES the used difference is a modulo 2 sum (XOR) of a pair of plaintexts. The XOR operation of two texts is invariant for most of the DES elements (expansion E, permutation P, xor with subkey and xor with left half of the text). Only in the case of S boxes knowledge of the input XOR does not guarantee the knowledge of the output XOR, but the input XOR of an S box suggests a probabilistic distribution of output XORs (table containing probabilities for all possible input XORs and all possible output XORs is called the differential profile of an S box). There are entries in the differential profile table which have 0 or near 0 probability, and there are entries which have high probability e.g. 16/64. This property can be used to identify key bits. If we have the output XOR of the F function in the last round and we know the pair of resultant ciphertexts, we can calculate the input XOR to the F function in the last round, and then input and output XOR to each S box in the last round. So it is possible to check in the differential profile table how many input pairs can lead to the entry determined by the input and output XOR of an S box. If there are k input pairs, which lead to the entry, exactly k values of the corresponding six bit key are possible. Most subkey values are suggested by only a few pairs, but the real value is suggested by all the pairs and this makes it possible to recognise it.

Let us give an example [3], XOR of two plaintexts, denoted by P* = 00808200 60000000_x results in the same difference of ciphertexts after three rounds of DES C* = 00808200 60000000_x with probability $p = (14/64)^2 \approx 0.05$. Above 3-round characteristic can be used to analyse 6-round DES (in so-called attack with round reduction) by deciphering a part of ciphertexts to determine when the characteristic occurs, in which case it is possible to derive some bits of the subkey. The attack is possible, because the partial deciphering of ciphertexts after round 6, which tells us when the characteristic occurs depends on a small subset of subkey bits, possible to

search exhaustively. Further details of the differential attack can be found in [3].

In [8] Knudsen introduced the concept of truncated differential, which is used in differential-linear cryptanalysis. Just to sketch the concept, truncated differential is a set of differential characteristics, which have a defined input XOR, and which have a defined output XOR truncated to some bits (the rest of the output XOR bits remains unknown).

Differential attack usually requires a large amount of chosen texts. To reduce the number of texts needed to be analysed Biham and Shamir [3],[1] proposed the use of differential structures (these structures are of interest to us, because they also let us reduce the number of analysed texts in differential-linear analysis [10]). The basic idea is the following: whenever it is possible to use a set of characteristics we can analyse a structure of plaintexts instead of only one pair, and this allows to get more pairs with particular differential from the same amount of plaintexts. Let us assume, that we need in an attack pairs of texts, which have all possible differences on the two youngest bits of the first byte of the plaintext. The construction is as follows: for a randomly chosen plaintext P we construct 4-tuple of plaintexts: P, P $\oplus$ 0100000000000000_x, P $\oplus$ 0200000000000000_x, P $\oplus$ 0300000000000000_x and denote them by P, P_1, P_2 and P_3. Using them we can obtain two pairs of plaintexts of characteristic with input difference 0100000000000000_x (P $\oplus$ P_1, P_2 $\oplus$ P_3), two pairs of plaintexts of characteristic with input difference 0200000000000000_x (P $\oplus$ P_2, P_1 $\oplus$ P_3), and two pairs of plaintexts of characteristic with input difference 0300000000000000_x (P $\oplus$ P_3, P_1 $\oplus$ P_2). So after encryption of only four texts we receive six pairs of plaintexts, satisfying the input difference.

4. EXTENSIONS OF LINEAR CRYPTANALYSIS

Several extensions to linear cryptanalysis were proposed, which improve the effectiveness of the attack, e.g. use of non-linear approximations in outer rounds reduces the number of analysed texts by a factor of $1/\sqrt{2}$.

Differential-linear cryptanalysis is a very powerful attack on DES with a reduced number of rounds. In comparison to linear cryptanalysis of DES reduced to 8 rounds which needs to analyse 500,000 of known plaintexts and to differential cryptanalysis which needs to analyse 5,000 chosen plaintexts, a differential-linear attack uses only 512 chosen plaintexts to obtain the same success probability.

Multiple expression[2] attack reduces the number of analysed texts by a factor of

$$\frac{p-1/2}{\sqrt{\sum_i (p_i-1/2)^2}},$$

where p is the probability of the best linear expression in use, and p_i are the probabilities of each of the expressions.

The latest extension proposed by Shimoyama reduces the number of plaintexts by the factor 25/34.

The extension proposed by Sakurai and Furuya [15], which uses probabilistic counting in reduction of rounds was originally applied to LOKI. The major advantage of this extension was the increase of the flexibility of an attack, by allowing to determine in the reduced rounds a number of bits, which is not a multiple of the number of S-box inputs. The use of this extension in an attack on DES can be found in [21].

In this section we sketch the use of multiple expression and differential-linear attack.

4.1 Differential-linear cryptanalysis

Differential-linear cryptanalysis was proposed by Langford and Hellman [10]. They noticed that three round differential characteristics [2], [3], which hold with probability 1 can be effectively used in linear cryptanalysis.

The main idea of the attack is the observation that complementing two bits (which after expansion are the middle bits of an input to an S-box) in one of the analysed texts leaves many bits of C_3 unchanged.

Among these bits are input bits to Matsui's best 3-round linear expression (bits number 57, 46, 40, 35 and 17). Because the parity of these bits never changes, the parity of output bits from the linear expression is unchanged with probability $p' = p^2 \oplus (1-p)^2 = 0.576$, where

[2] called multiple approximation in the original paper [7].

$p = 0.695$ is the probability of Matsui's linear expression. (This result comes directly from the Piling-Up Lemma.)

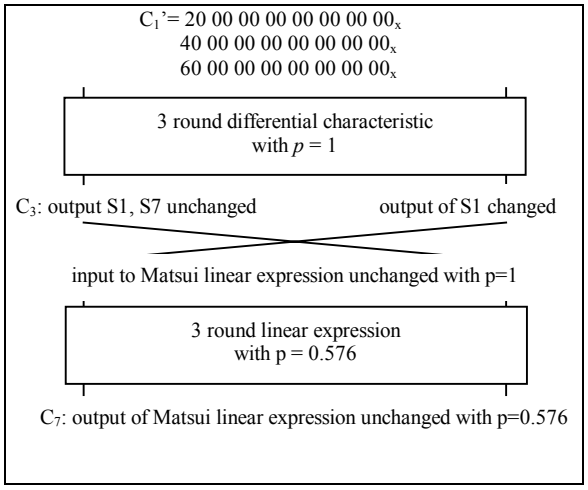

Figure 1. Differential-linear attack on DES reduced to 8 rounds

To attack DES the cryptanalyst for each pair of plaintexts inverts the first round and is looking for a key (denote by i) which toggles bits 2 and/or 3 in the input to the second round and for each pair of ciphertexts inverts the last round, computes the parity for both inverted ciphertexts and, if the parity is equal increases N_0^{ij} where j is the index of the analysed candidate for the last round subkey. The largest N_0^{ij} indicates the correct subkeys with a probability depending on the probability of the linear expression in use and the number of analysed pairs.

Further improvement of this attack can be achieved by using differential structures mentioned above, proposed by [1], [3] for packing the analysed plaintexts.

4.2 Multiple expressions

The extension proposed by Kaliski and Robshaw [7] was based on the observation that during the attack, the cryptanalyst differentiates between the distribution with an expected value equal to p and variance p^2 and the distribution with an expected value equal to 1-p and variance p^2. Use of multiple expressions decreases the variance of the distributions.

Modified equation 1 assumes the following form:

$$(P \bullet \Gamma P^j) \oplus (C \bullet \Gamma C^j) = \Sigma_z (K_z \bullet \Gamma K_z), \quad (12)$$

where ΓP^j, ΓC^j denote binary masking vectors of plaintext and ciphertext used in linear expression number j ($1 \le j \le J$).

Instead of N_0 in algorithm 1, Kaliski proposed to use a statistic of the following form:

$$U = \sum_{j=1}^{J} a_j N_0^j \quad (13)$$

where $a_1, a_2, ..., a_J$, are positive and s.t.

$$\sum_{j=1}^{J} a_j = 1 .$$

For simplicity we assume that p_j-1/2 > 0.

Algorithm 3 (attack 0R with multiple expressions) [7]
Input:
N known pairs of texts,
effective linear expressions with probability p_j.
Step 1:
For each linear expression let N_0^j be the number of pairs for which the left side of equation 12 was equal to 0.
Step 2:
Count the value $U = \sum_{j=1}^{J} a_j N_0^j$.
Step 3:
If $U > N/2$ then
set $\Sigma_z(K_z \bullet \Gamma K_z) = 0$, if $p>1/2$ and 1 if $p<1/2$,
else
set $\Sigma_z(K_z \bullet \Gamma K_z) = 1$, if $p>1/2$ and 0 if $p<1/2$.
Output:
the value of $\Sigma_z(K_z \bullet \Gamma K_z)$ (correct with probability dependent on N and $|p - 1/2|$ and weights a_j.)

Kaliski noticed that the distribution of statistic U can be modelled using a normal distribution. He calculated the expected values and the variance. He also indicated that when the weights a_j are proportional to the biases (p_j-1/2) of linear expressions, the distance between $N/2$ and E[U] is maximised. He calculated the success rate of the modified algorithm, which is equal to:

$$\Phi(2\sqrt{N}\sqrt{\frac{\sum_{j=1}^{n}(p_j-1/2)^2}{1-4\sum_{j=1}^{n}(p_j-1/2)^2}}), \qquad (14)$$

where $\Phi(.)$ denotes the normal cumulative distribution function. When $\sum_{j=1}^{J}(p_j-1/2)$ is small, the success rate can be approximated as $\Phi(2\sqrt{N}\sqrt{\sum_{j=1}^{n}(p_j-1/2)^2})$, while the success rate of Matsui's algorithm is equal to $\Phi(2\sqrt{N}(p-1/2))$.

Algorithm 3 can be easily extended to 1R and 2R attacks.

5. EXPERIMENTS

We have extended our work already presented in [20]. We propose the differential-linear cryptanalysis with multiple expressions and list decoding [12] as a tool, which enables a further decrease in the number of texts in an attack on DES. We improved the result obtained by Langford [10] for analysis of 8 round DES (they achieved probability of success 80% after analysing 512 chosen plaintexts), getting a success rate improved by a factor larger than 4.
We obtained the best results by using differential 3=round characteristic proposed by Langford (ch_L) which holds with probability 1 (presented above) and the following linear expressions: Matsui's best 3-round linear expression (e_M) and:
$C_4[39,50,56,15] \oplus C_7[39,50,56,15] = 0$,
denoted by e_1, which holds with probability $p_1 = 1/2 + 0.78 / 16$,
$C_4[37,43,49,59,1] \oplus C_7[37,43,49,59,1] = 0$,
denoted by e_2, which holds with probability $p_2 = 1/2 + 0.76 / 8$,
$C_4[34,40,48,58,23] \oplus C_7[34,40,48,58,23] = 0$,
denoted by e_3, which holds with probability $p_3 = 1/2 + 0.56 / 8$, and
$C_4[34,40,58,23] \oplus C_7[34,40,58,23] = 0$,
denoted by e_4, which holds with probability $p_4 = 1/2 + 0.78 / 16$.

We have obtained the following success rate function for the basic differential-linear attack:

N	192	384	512	704
SR	0,33	0,67	0,81	0,92

Table 3. Success rate of differential linear cryptanalysis (linear expression e_M, differential characteristic ch_L)

and the following success rate function for the proposed differential linear attack with multiple expressions and list decoding (which basically means checking the candidates for the last round subkey, ordered by decreasing number of counts instead of checking only the best candidate). A list of candidates in our experiments has a length of 100.

N	128	192	384	512
SR	0,86	0,97	1	1

Table 4. Success rate of differential linear cryptanalysis with multiple expressions and list decoding(linear expressions e_M, e_0, e_2, e_3, e_4, differential characteristic ch_L).

6. CONCLUSIONS AND FURTHER RESEARCH

We have presented the experimental results of differential-linear cryptanalysis with multiple linear expressions and list decoding method. We have achieved an improvement over previous results by decreasing the number of chosen texts by a factor greater than 4. So, the first conclusion is that to evaluate the real security of a cipher, the combinations of extensions of the basic attack have to be taken into account.

Presented attack can be effectively extended up to 11 DES rounds. which is a slight improvement in comparison to previous experiments [20], but it still cannot be extended further. So, we conclude that differential-linear cryptanalysis even extended, still remains only a theoretical attack for DES.

Our further research will concentrate on combining extensions of linear cryptanalysis with higher order differentials [8] and impossible differentials [3], [1]. Also our attention will be concentrated on combining the extensions of linear cryptanalysis with Shimoyama's attack.

REFERENCES

[1] E. Biham, "Differential Cryptanalysis and its Extensions", Proceedings of V National

Conference on Applications of Cryptography ENIGMA'2001, ISBN 83-911317-7-7.
[2] E. Biham, A. Shamir, "Differential Cryptanalysis of DES-like cryptosystems", Journal of Cryptology, 4(1):3-72, 1991.
[3] E. Biham, A. Shamir, "Differential Cryptanalysis of Data Encryption Standard", Springer Verlag, 1993.
[4] U. Blöcher, M. Dichtl, „Problems with the Linear Cryptanalysis of DES Using more than one Active S-Box per Round", Fast Software Encryption, Springer Verlag 1994, ISBN 3-540-60590-8.
[5] W. Feller, „Introduction to the probability theory", PWN 1977.
[6] C. Harpes, G.G. Kramer, J. L. Massey, „A Generalization of Linear Cryptanalysis and Applicability of Matsui's piling-up Lemma", Advances in Cryptology Eurocrypt'95, Springer Verlag 1995, ISBN 3-540-59409-4.
[7] B. S. Kaliski Jr., M.J.B Robshaw, „Linear Cryptanalysis Using Multiple Approximations", Advances in Cryptology Crypto'94, Springer Verlag 1994, ISBN 3-540-58333-5.
[8] L.R. Knudsen, "Truncated and Higher Order Differentials", Second International Workshop on Fast Software Encryption, Lueven, Belgium, 1994, pp. 196-211.
[9] L.R. Knudsen, M.J.B. Robshaw, „Non-Linear Approximations in Linear Cryptanalysis, Advances in Cryptology Eurocrypt'96, Springer Verlag 1996, ISBN 3-540-61186-X.
[10] S. Langford, M.E. Hellman, „Differential-linear Cryptanalysis", Advances in Cryptology Crypto'94, Springer Verlag 1994, ISBN 3-540-58333-5.
[11] M. Matsui, „Linear Cryptanalysis Method for DES Cipher", Advances in Cryptology Eurocrypt'93.
[12] M. Matsui, „On Correlation Between the Order of S-boxes and the Strength of DES", Advances in Cryptology Eurocrypt'94, Springer Verlag 1994, ISBN 3-540-60176-7.
[13] M. Matsui, „The First Experimental cryptanalysis of Data Encryption Standard", Advances in Cryptology Crypto'94, Springer Verlag 1994, ISBN 3-540-58333-5.
[14] K. Ohta, S. Morai, K. Aoki, „Improving the Search Algorithm for Best Linear Expression", Advances in Cryptology Crypto'95, Springer Verlag 1995, ISBN 3-540-60221-6.
[15] K. Sakurai, S. Furuya, "Improving linear cryptanalysis of LOKI91 by probabilistic counting method", Fast Software Encryption Workshop (FSE4), Haifa, Israel, 1997.
[16] T. Shimoyama, T. Kaneko, "Quadratic Relation of S-Box and Its Application to the Linear Attack of Full Round DES", Advances in Cryptology, Crypto'98. ISBN 3-540-64892-5.
[17] A. Zugaj, "The linear expression search algorithms", Proceedings of IV National Conference on Applications of Cryptography ENIGMA'2000, ISBN 83-911317-3-4.
[18] A. Zugaj, K. Górski, Z. Kotulski, A. Paszkiewicz, J. Szczepański, S. Trznadel, "Linear cryptanalysis of DES algorithm", (in Polish), seminar notes Institute of Telecommunications, Warsaw University of Technology, April 1998.
[19] A. Zugaj, K. Górski, Z. Kotulski, A. Paszkiewicz, J. Szczepański, S. Trznadel, „Linear cryptanalysis", (in Polish) PWT, December 1998.
[20] A.Zugaj, K. Górski, Z. Kotulski, J. Szczepański, A. Paszkiewicz, "Extending linear cryptanalysis – theory and experiments", Regional Conference on Military Communication and Information Systems, RCMCIS'99, October 6-8, 1999.
[21] A.Zugaj, K. Górski, Z. Kotulski, A. Paszkiewicz, J. Szczepański, "New constructions in linear cryptanalysis of block ciphers", ACS'2000, October 2000.