VERSITA

TATRA MOUNTAINS
Mathematical Publications

DOI: 10.2478/v10127-011-0036-y
Tatra Mt. Math. Publ. **50** (2011), 51–61

LINEAR AND DIFFERENTIAL CRYPTANALYSIS OF REDUCED-ROUND AES

Lucia Lacko-Bartošová

ABSTRACT. The subject of this paper is linear and differential cryptanalysis of two rounds of the Advanced Encryption Standard (AES) with estimation of complexity for three-round AES attack. Presented linear attack is based on finding highly probable linear expressions and presented differential attack is based on finding specific bitwise differences. Data complexity of described linear and differential attack is 2^{28} and 2^{27}, respectively, where 8 bits of subkey are recovered. Minimal complexity of linear attack on three-round AES is bigger than $d \times 2^{60}$, where d is a small constant.

1. Introduction

The Advanced Encryption Standard (AES) was designed by J o a n D a e m e n and V i n c e n t R i j m e n and became a standard announced by National Institute of Standards and Technology in 2002 [3]. Several recent papers have dealt with provable security against linear and differential cryptanalysis of the AES, but to the best knowledge of the author no paper have dealt with linear and differential attacks on the AES.

Linear cryptanalysis was introduced at Eurocrypt conference in 1993 by M. M a t s u i as a theoretical attack on the Data Encryption Standard (DES) [9] and later successfully used in the practical cryptanalysis of DES [8]. Linear cryptanalysis works on the principle of finding "high probability occurrences of linear expressions involving plaintext bits, ciphertext bits (actually we shall use bits from the 2nd last round output), and subkey bits" [4]. It is a known plaintext attack in which a large number of plaintext-ciphertext pairs are used to determine the value of key bits [4].

2010 M a t h e m a t i c s S u b j e c t C l a s s i f i c a t i o n: 94A60, 68P25.
K e y w o r d s: AES, SPN, linear cryptanalysis, differential cryptanalysis, linear and differential probability, MELP.
Supported by the Grant VEGA 2/0206/10.

Differential cryptanalysis was first presented at Crypto conference in 1990 by E. Biham and A. Shamir as an attack on DES [2]. Heys [4] describes the main principle: "Differential cryptanalysis exploits the high probability of certain occurrences of plaintext differences and differences into the last round of the cipher". It is a chosen plaintext attack, that means plaintext can be selected and output subsequently calculated in order to derive the key.

The paper is organized as follows. In Section 2 the AES cipher is described and the basic definitions for linear and differential cryptanalysis are given. In Section 3 the main results are described. The linear and differential probability of the AES S-box is given, analysis of complexity of attacks is done, main results of linear and differential cryptanalysis of two-round AES are listed and estimation of complexity for three-round AES attack is carried out. Conclusions are presented in Section 4.

2. Preliminaries

2.1. The advanced encryption standard

The AES is a substitution-permutation network (SPN) with the block length of 128 bits, and supports key lengths of 128, 192 and 256 bits [3]. The numbers of rounds are 10, 12 or 14 according to key lengths. Each round consists of round transformation, which is a sequence of four transformations, called steps:

1. SubBytes,
2. ShiftRows,
3. MixColumns,
4. AddRoundKey.

In the final round, step MixColumns is removed. The round transformation and its steps operate on an intermediate result, called the state [3]. 128 bit plaintext $p_0p_1p_2\dots p_{15}$ is arranged into the 4×4 matrix of bytes depicted in Table 1.

Table 1. State layout for 128 bit plaintext and 128 bit intermediate state.

p_0	p_4	p_8	p_{12}
p_1	p_5	p_9	p_{13}
p_2	p_6	p_{10}	p_{14}
p_3	p_7	p_{11}	p_{15}

$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$

SubBytes. The SubBytes step is the only non-linear transformation of the cipher. It consists of an 8×8 S-box applied to the bytes of the state. S-box operates on $\mathrm{GF}(2^8)$ and can be described as

$$S[x] = L(x^{-1}) + q,$$

where x^{-1} denotes the multiplicative inverse of x in GF(2^8), extended with 0 being mapped to 0. Multiplication is done modulo the irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$. L is a linear transformation over GF(2) and q is a constant [3].

ShiftRows. The ShiftRows transformation consists of 4 steps:

1. no shift of the first row of the state array,
2. cyclic shift of the second row by one byte to the left,
3. cyclic shift of the third row by two bytes to the left,
4. cyclic shift of the last row by three bytes to the left.

MixColumns. The MixColumns step operates on the state column, that means on 32 bits. State columns are understood as polynomials over $GF(2^8)$ and multiplied modulo $(x^4 + 1)$ with polynomial

$$c(x) = 0x03 \cdot x^3 + 0x01 \cdot x^2 + 0x01 \cdot x + 0x02.$$

This polynomial is coprime to $x^4 + 1$ and therefore invertible. Modular multiplication can be written as a matrix multiplication. Let $b(x) = c(x) \cdot a(x) \bmod (x^4 + 1)$. Then

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}.$$

AddRoundKey. The key addition is a transformation, where the state is modified by combining it with a round key with the bitwise XOR operation.

For more detailed information, we refer to [3].

2.2. Linear and differential probability

In this subsection linear and differential probability and expected linear and differential probability are defined.

Definition 1 ([5]). Let $B\colon \{0,1\}^d \to \{0,1\}^d$, and let $\mathbf{a}, \mathbf{b}, \mathbf{\Delta x}, \mathbf{\Delta y} \in \{0,1\}^d$ be fixed. If $\mathbf{X} \in \{0,1\}^d$ is a uniformly distributed random variable, then the linear probability $LP(\mathbf{a}, \mathbf{b})$ and the differential probability $DP(\mathbf{\Delta x}, \mathbf{\Delta y})$ are defined as

$$LP(\mathbf{a}, \mathbf{b}) = \Big(2 \cdot \mathrm{Prob}_{\mathbf{X}}\big\{\mathbf{a} \bullet \mathbf{X} = \mathbf{b} \bullet B(\mathbf{X})\big\} - 1\Big)^2, \tag{1}$$

$$DP(\mathbf{\Delta x}, \mathbf{\Delta y}) = \mathrm{Prob}_{\mathbf{X}}\big\{B(\mathbf{X}) \oplus B(\mathbf{X} \oplus \mathbf{\Delta x}) = \mathbf{\Delta y}\big\}. \tag{2}$$

where " $\bullet$ " is an inner product in $GF(2)$ ($a \bullet b = \oplus_{i=0}^{n-1} a_i b_i$).

If B is parameterized by a key, $\mathbf{k}$, we write $\mathrm{LP}(\mathbf{a}, \mathbf{b}; \mathbf{k})$ and $\mathrm{DP}(\boldsymbol{\Delta}\mathbf{x}, \boldsymbol{\Delta}\mathbf{y}; \mathbf{k})$, respectively, and we define the expected linear probability $\mathrm{ELP}(\mathbf{a}, \mathbf{b})$ and expected differential probability $\mathrm{EDP}(\boldsymbol{\Delta}\mathbf{x}, \boldsymbol{\Delta}\mathbf{y})$ as

$$\mathrm{ELP}(\mathbf{a}, \mathbf{b}) = E_{\mathbf{K}}\big[\mathrm{LP}(\mathbf{a}, \mathbf{b}; \mathbf{K})\big], \tag{3}$$

$$\mathrm{EDP}(\boldsymbol{\Delta}\mathbf{x}, \boldsymbol{\Delta}\mathbf{y}) = \mathrm{E}_{\mathbf{K}}\big[\mathrm{DP}(\boldsymbol{\Delta}\mathbf{x}, \boldsymbol{\Delta}\mathbf{y}; \mathbf{K})\big], \tag{4}$$

where $\mathbf{K}$ is a random variable uniformly distributed over the space of keys.

The values $\mathbf{a}, \mathbf{b}$ are called input and output masks, and the values $\boldsymbol{\Delta}\mathbf{x}, \boldsymbol{\Delta}\mathbf{y}$ are called input and output differences [5]. LP, ELP, DP, EDP values are viewed as entries in a $2^d \times 2^d$ table. For our purposes, the mapping B in Definition 1 will be bijective and the AES S-box.

For $T \geq 2$ core cipher rounds, the critical value for linear cryptanalysis is the maximum expected linear probability (MELP) and for differential cryptanalysis is the maximum expected differential probability (MEDP) [6]:

$$\mathrm{MELP} = \max_{\mathbf{a},\mathbf{b} \in \{0,1\}^N \setminus \mathbf{0}} \mathrm{ELP}^{[1\ldots T]}(\mathbf{a}, \mathbf{b}), \tag{5}$$

$$\mathrm{MEDP} = \max_{\triangle\mathbf{x},\triangle\mathbf{y} \in \{0,1\}^N \setminus \mathbf{0}} \mathrm{EDP}^{[1\ldots T]}(\triangle\mathbf{x}, \triangle\mathbf{y}). \tag{6}$$

For linear/differential cryptanalysis the data complexity of an attack with a given probability of success is proportional to the inverse of MELP/MEDP [5].

2.3. Linearly and differentially active S-box

In this subsection we define active S-box. First, linear and differential characteristic has to be defined.

Definition 2 ([5]). A linear/differential characteristic for rounds $1 \ldots T$ is a $(T+1)$-tuple of N-bit masks/differences, $\Omega = \langle \mathbf{a^1}, \mathbf{a^2}, \ldots, \mathbf{a^T}, \mathbf{a^{T+1}} \rangle / \Omega = \langle \triangle\mathbf{x^1}, \triangle\mathbf{x^2}, \ldots, \triangle\mathbf{x^T}, \triangle\mathbf{x^{T+1}} \rangle$; we view $\mathbf{a^t}/\triangle\mathbf{x^t}$ and $\mathbf{a^{t+1}}/\triangle\mathbf{x^{t+1}}$ as input and output masks/differences, respectively, for round t $(1 \leq t \leq T)$.

Next, consistent linear and differential characteristic is defined.

Definition 3 ([5]). Let Ω be a T-round linear/differential characteristic for rounds $1 \ldots T$. Then Ω is called consistent if, for each S-box in rounds $1 \ldots T$, the input and output masks/differences determined by Ω for that S-box are either both zero or both nonzero.

Now, the active S-box is defined.

Definition 4 ([1]). Given a consistent linear/differential characteristic, any S-box for which the resulting input and output masks/differences are nonzero is called linearly/differentially active (or just active when the context is clear).

In two consecutive rounds, the minimum number of linearly/differentially active S-boxes is indicated by the linear/differential branch number of AES transformation MixColumns, and is five [3].

3. Main results

3.1. Distribution of LP and DP values

First the smallest nonlinear part of the cipher—the AES S-box—was investigated. The LP/DP values from Definition 1 were calculated and they are given in Table 2 and Table 3, respectively. It can be seen that all the nontrivial rows and columns of the LP/DP table for the AES S-box have the same distribution of values.

TABLE 2. Distribution of LP values for the AES S-box.

Value	$\left(\frac{8}{64}\right)^2$	$\left(\frac{7}{64}\right)^2$	$\left(\frac{6}{64}\right)^2$	$\left(\frac{5}{64}\right)^2$	$\left(\frac{4}{64}\right)^2$	$\left(\frac{3}{64}\right)^2$	$\left(\frac{2}{64}\right)^2$	$\left(\frac{1}{64}\right)^2$	0
Frequency	5	16	36	24	34	40	36	48	17

From Table 2 results that in every row and every column of the LP table, five input and output masks can be found, that will give the highest value of linear probability, exactly $\left(\frac{8}{64}\right)^2 = 2^{-6}$.

TABLE 3. Distribution of DP values for the AES S-box.

Value	$\frac{4}{256}$	$\frac{2}{256}$	0
Frequency	1	126	129

Table 3 shows that in every row and every column of the DP table can be found exactly one input and output difference, that will give the highest value of differential probability, exactly $4/256 = 2^{-6}$.

According to the LP/DP values in Table 2 and Table 3 we are able to count the highly probable linear expression for the linear attack and specific bitwise difference for the differential attack of two rounds of the AES.

3.2. Linear cryptanalysis

In this subsection successful two-round AES linear cryptanalysis is described and complexity estimation of three-round AES linear cryptanalysis attack is provided. First, the complexity of a two-round attack is estimated.

3.2.1. Analysis of complexity of two-round AES linear cryptanalysis

In Table 4 total complexity of two-round AES linear cryptanalysis is estimated. $\mathcal{N}_L$ is the data complexity of the attack and is derived from LP values of S-box. Based on different numbers of active S-boxes in the first and the second round, 8 to 32 bits of subkey can be recovered.

The lowest complexity is reached in the last scenario, where four S-boxes are active in the first round and one S-box is active in the second round. Data complexity is $c \times 2^{26}$, where c is a small constant. Because one S-box is active in the second round, 8 bits of subkey can be recovered. In order to derive the right key, 2^8 subkeys have to be tested. That makes total complexity $c \times 2^{34}$.

TABLE 4. Total complexity of two-round AES linear cryptanalysis.

Number of active S-boxes		$\mathcal{N}_L$	Number of target partial subkeys	Total complexity
1. round	2. round			
1	4	$c \times 2^8$	2^{32}	$c \times 2^{40}$
2	3	$c \times 2^{14}$	2^{24}	$c \times 2^{38}$
3	2	$c \times 2^{20}$	2^{16}	$c \times 2^{36}$
4	1	$c \times 2^{26}$	2^8	$c \times 2^{34}$

In order to conduct an attack, input and output masks for the last scenario have to be calculated.

3.2.2. Input and output masks

Calculated input mask to the first round that is used for the attack is

$$\mathbf{a} = (0x32000000002c000000002c0000000003). \tag{7}$$

Calculated output mask into the second round of the AES is

$$\mathbf{b} = (0x00000035000000000000000000000000). \tag{8}$$

3.2.3. Results of linear cryptanalysis of two-round AES

Program in C++ language was implemented and executed on a notebook (Intel Core 2, 1.66 GHz, 1 GB RAM). Table 5 contains results.

The attack, where $c = 2$ was not successful. Right key was not determined.

The fastest successful attack with the lowest complexity was accomplished when $c = 4$. 8 bits of subkey were obtained.

Constant c = 4. Calculation lasted 44 minutes and right key was determined. Output of the program lists first five maximum probability values and pertaining keys. Counted Bias (derived from LP value) for pertaining input and output masks (Eq. 7, 8), is $2^{-13} \approx 0.000122$.

```
Linear cryptanalysis
Output (c=4):
Bias: 0.000172 Key: 79          Bias: 0.000089 Key: 25
Bias: 0.000115 Key: ff          Bias of right key: 0.000172 Key: 79
Bias: 0.000098 Key: 47          Estimated time: 2612.140 s
Bias: 0.000091 Key: b4
```

TABLE 5. Execution time of two-round AES linear cryptanalysis.

c	2	4	8	16
$\mathcal{N}_L$	2^{27}	2^{28}	2^{29}	2^{30}
Number of target partial subkeys	2^8	2^8	2^8	2^8
Total complexity	2^{35}	2^{36}	2^{37}	2^{38}
Execution time	22 min. *not successful	44 min.	86 min.	171 min.

On Figure 1 there is depicted Bias for all targeted subkeys depending on number of plaintext/ciphertext pairs $\mathcal{N}_L$. Right key $0x79$ is gaining throughout the calculation significantly bigger probability than other keys and is separating after the second third of calculation.

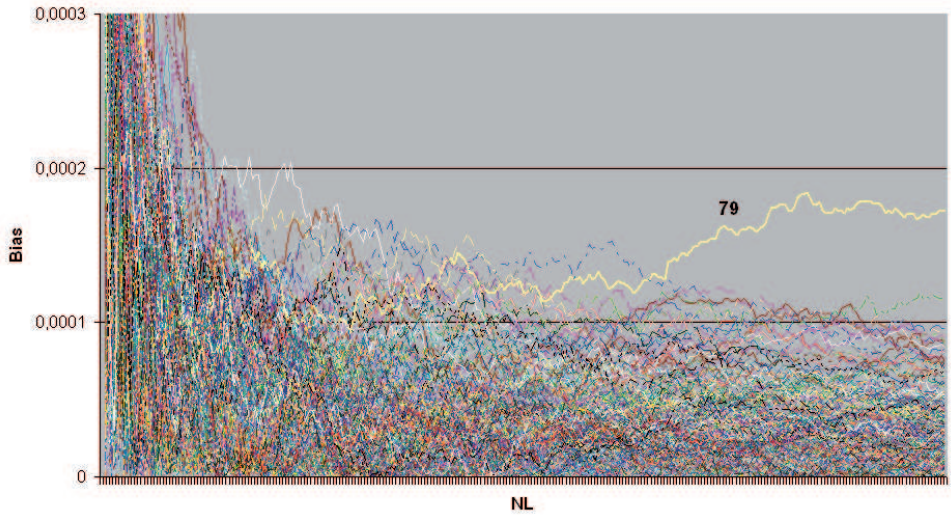

FIGURE 1. Linear cryptanalysis of two-round AES, c=4.

3.2.4. Estimation of complexity for three-round AES linear attack

In order to estimate the complexity of three-round AES linear cryptanalysis we have to know the MELP for two-round AES. K e l i h e r and S u i [6] calculated the exact maximum expected linear probability for two-round AES and it is equal to $109953193/2^{54} \approx 1.638 \times 2^{-28}$. This value is only valid for input/output masks listed in Table 3 in [6], for 1 S-box active in the first round and 4 S-boxes active in the second round.

In Table 6 complexity is estimated. Minimal total complexity is obtained when four S-boxes are active in the first round, one S-box is active in the second round and four S-boxes are active in the third round. The ELP has to be smaller than 1.638×2^{-28} which implies that data complexity $\mathcal{N}_L$ has to be bigger than $d \times 2^{28}$, where d is a small constant. In order to derive the right key we would have to try 2^{32} subkeys. That makes total complexity bigger than $d \times 2^{60}$. This complexity is over our computing power.

TABLE 6. Total complexity estimation of three-round AES linear cryptanalysis.

Number of active S–boxes			$\mathcal{N}_L$	Number of target partial subkeys	Total complexity
1. round	2. round	3. round			
1	4	16	$d \times 2^{28}$	2^{128}	$d \times 2^{156}$
2	3	12	$> d \times 2^{28}$	2^{96}	$> d \times 2^{124}$
3	2	8	$> d \times 2^{28}$	2^{64}	$> d \times 2^{92}$
4	1	4	$> d \times 2^{28}$	2^{32}	$> d \times 2^{60}$

3.3. Differential cryptanalysis

In this subsection successful two-round differential cryptanalysis of AES is described.

3.3.1. Analysis of complexity of two-round AES differential cryptanalysis

In order to conduct differential attack, analysis of complexity is made and provided in Table 7. The lowest complexity is in the last scenario, where four S-boxes are active in the first round and one S-box is active in the second round. Data complexity is calculated from DP values of S-boxes. In order to derive the right key, 2^8 subkeys have to be tested. That makes total complexity $c \times 2^{32}$.

The last scenario is chosen and input and output differences are calculated.

TABLE 7. Total complexity of two-round AES differential.

Number of active S-boxes		Data	Number	Total
1. round	2. round	complexity	of target subkeys	complexity
1	4	$c \times 2^6$	2^{32}	$c \times 2^{38}$
2	3	$c \times 2^{12}$	2^{24}	$c \times 2^{36}$
3	2	$c \times 2^{18}$	2^{16}	$c \times 2^{34}$
4	1	$c \times 2^{24}$	2^8	$c \times 2^{32}$

3.3.2. Input and output difference

Calculated input difference to the first round that is used for the attack is

$$\mathbf{\Delta x} = (0xd8000000090000000004000000000e5). \tag{9}$$

Calculated output difference into the second round of the AES is:

$$\mathbf{\Delta y} = (0xd1000000000000000000000000000000). \tag{10}$$

3.3.3. Results of differential cryptanalysis of two-round AES

Program in C++ language was implemented and executed on the notebook (Intel Core 2, 1.66 GHz, 1 GB RAM). Results are in Table 8. Fastest attack with lowest complexity was accomplished when $c = 8$. 8 bits of subkey were obtained.

TABLE 8. Execution time of two-round AES differential cryptanalysis.

c	8	16	32	64
Data complexity	2^{27}	2^{28}	2^{29}	2^{30}
Number of target subkeys	2^8	2^8	2^8	2^8
Total complexity	2^{35}	2^{36}	2^{37}	2^{38}
Execution time	6.5 min.	13 min.	26 min.	53 min.

Constant c = 8. Calculation lasted 6.5 minutes and right key was determined. Output of the program lists first five maximum probability values and pertaining keys. Counted probability p_D for pertaining input and output difference (Eq. 9, 10), is $2^{-24} \approx 5.96 \times 10^{-8}$.

```
Differential cryptanalysis
Output (c=8):
pD: 5.960464e-008 Key: ac        pD: 7.450581e-009 Key: 11
pD: 1.490116e-008 Key: 43        pD right key: 5.960464e-008 Key: ac
pD: 1.490116e-008 Key: 58        Estimated time: 398.656 s
pD: 1.490116e-008 Key: 8e
```

On Figure 2 is depicted probability p_D for all targeted subkeys depending on number of plainext/ciphertext pairs $\mathcal{N}_D$. Right key $0xac$ is gaining throughout the calculation significantly bigger probability than other keys and is separating after the first quarter of calculation. Most of the keys have zero probability during whole calculation.

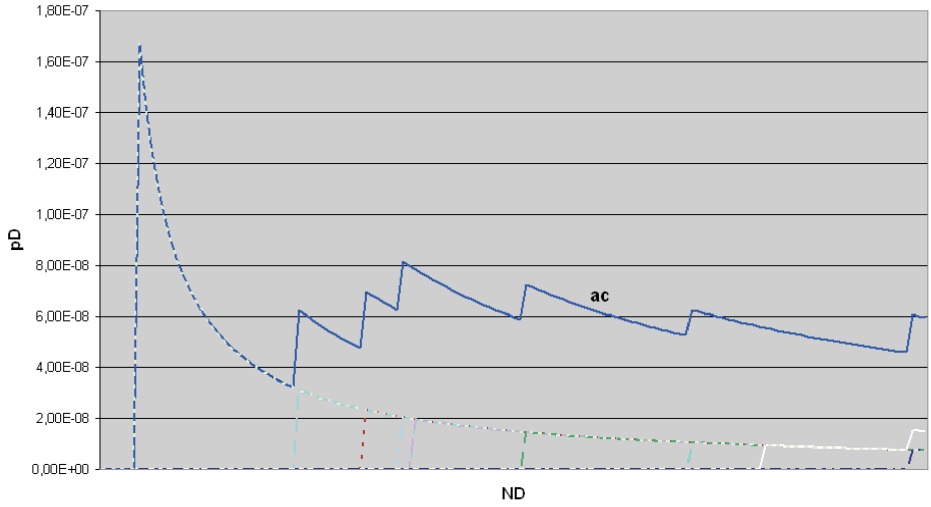

FIGURE 2. Differential cryptanalysis of two-round AES, c=8.

4. Conclusion

In the paper successful linear and differential attack on two-round AES is presented. For realization of linear attack it was necessary to calculate linear probability of S-box, determine appropriate input and output mask and analyze complexity. Data complexity of successful attack that recovers 8 subkey bits is 2^{28} and on standard laptop takes 44 minutes. Analysis of linear attack on three-round AES showed that minimal complexity of this attack is bigger than $d \times 2^{60}$, where d is a small constant. This attack would recover 32 subkey bits. For this estimation *maximum expected linear probability* (first calculated by [6], recalculated by [7]), was used.

For successful realization of differential attack it was necessary to calculate differential probability of S-box, determine appropriate input and output differences and analyze complexity. Data complexity of successful attack that recovers 8 subkey bits is 2^{27} and on standard laptop takes 6.5 minutes.

REFERENCES

[1] BIHAM, E.: *On Matsui's linear cryptanalysis,* in: Advances in Cryptology–EUROCRYPT '94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, 1994 (A. De Santis, ed.), Lecture Notes in Comput. Sci., Vol. 950, Springer-Verlag, Berlin, 1995, pp. 341–355.

[2] BIHAM, E.—SHAMIR, A.: *Differential cryptanalysis of DES-like cryptosystems,* in: Advances in Cryptology—CRYPTO '90, Conf. on the Theory and Application of Cryptography, Santa Barbara, USA, 1990 (A. Menezes, ed.), Lecture Notes in Comput. Sci., Vol. 537, Springer-Verlag, Berlin, 1991, pp. 2–21.

[3] DAEMEN, J.—RIJMEN, V.: *The Design of Rijndael: AES—The Advanced Encryption Standard.* Springer-Verlag, Berlin, 2002.

[4] HEYS, H. M.: *A tutorial on linear and differential cryptanalysis,* Technical Report CORR 2001-17, Centre for Applied Cryptographic Research, Department of Combinatorics and Optimization, University of Waterloo, March 2001.

[5] KELIHER, L.: *Refined analysis of bounds related to linear and differential and linear cryptanalysis for the AES*, in: Advanced Encryption Standard—AES '04, 4th Internat. Conf. (H. Dobbertin et al., eds.), Bonn, Germany, 2004, Lecture Notes in Comput. Sci., Vol. 3373, Springer-Verlag, Berlin, 2005, pp. 42–57.

[6] KELIHER, L.—SUI, J.: *Exact maximum expected differential and linear probability for two-round Advanced Encryption Standard,* IET Information Security **1** (2007), 53–57.

[7] LACKO-BARTOŠOVÁ, L.: *Útoky na zmenšené verzie AES.* Master Thesis, Faculty of Electrical Engineering and Information Technology, Slovak University of Technology, Bratislava, SK, 2009.

[8] MATSUI, M.: *The first experimental cryptanalysis of the Data Encryption Standard,* in: Advances in Cryptology—CRYPTO '94, 14th Annual Internat. Cryptology Conf., Santa Barbara, CA, USA, 1994 (Y. G. Desmedt, ed.), Lecture Notes in Comput. Sci., Vol. 839, Springer-Verlag, Berlin, 1994, pp. 1–11.

[9] MATSUI, M.: *Linear cryptanalysis method for DES cipher,* in: Advances in Cryptology––EUROCRYPT '93, Workshop on the Theory and Application of Cryptographic Techniques, Lofthus, Norway, 1993 (T. Helleseth, ed.), Lecture Notes in Comput. Sci., Vol. 765, Springer-Verlag, Berlin, 1994, pp. 386–397.

Received August 16, 2011

Mathematical Institute
Slovak Academy of Sciences
Štefánikova 49
SK–814-73 Bratislava
SLOVAKIA
E-mail: lucia.lacko-bartosova@mat.savba.sk