Commun.Fac.Sci.Univ.Ank.Séries A2-A3
Volume 58, Number 1, Pages 1-15 (2016)
DOI: 10.1501/commua1-2_0000000090
ISSN 1303-6009

ON THE SUCCESS PROBABILITIES OF DIFFERENTIAL ATTACKS ON PRESENT

Fatih SULAK and Okan ŞEKER

Fatih Sulak, Mathematics Department, Atılım University, 06836 Ankara, Turkey
E-mail: fatih.sulak@atilim.edu.tr
Okan Şeker, Institute of Applied Mathematics, Middle East Technical University, 06800 Ankara, Turkey
E-mail : okan.seker@metu.edu.tr

(Received: December 19, 2015; Accepted: February 29, 2016)

ABSTRACT

Advanced growth in ubiquitous devices leads to increasing popularity of lightweight cryptography and as a result, various block ciphers are designed. The analysis of these algorithms has become popular and as a result, underlying theory of analysis tools including success probabilities has widely been studied recently. In this work, we focus on Present, a lightweight block cipher introduced by Bogdanov et al. and the analysis of this algorithm.
We give a detailed information of differential cryptanalysis and multiple differential cryptanalysis on Present. Also, the underlying theory of statistical cryptanalysis are presented. As an important part of cryptanalysis, success probability is examined and expressed by the formulas given by Selçuk and Blondeau et al. The main aim of this work is to contribute to the theory of statistical cryptanalysis. Therefore, we give a general framework of statistical cryptanalysis and success probabilities. The details of success probabilities are given with experimental results. Also, we apply the *sieving phase* to decrease the cost of the attacks.

KEYWORDS: Present, Differential cryptanalysis, Multiple differential cryptanalysis, Success probability

1. INTRODUCTION

Lightweight cryptography becomes one of the most vital topics in recent years because of the needs in computing devices which have limited sources. Due to the power consumptions, most of the current cryptographic primitives are not suitable to run on these devices. In order to fill the gap, many lightweight ciphers are designed like CGEN [16], Hight [9], Katan&Ktantan [7], mCrypton [17], Present [6], Tea [23] and the like.

Present is an ultra-lightweight block cipher proposed by Bogdanov et al. [6]. It is a 31-round substitution-permutation network with 64-bit block length and it consists of two layers; the non-linear substitution layer and the linear permutation layer. Moreover, Present is selected as international standard [10] due to its good hardware-software performance, secure and simple structure.

Differential cryptanalysis is introduced by Biham and Shamir in 1990 [2]. It is a statistical cryptanalysis method and it uses plaintext-ciphertext pairs with input and output differences such that, for an input difference, a specific output difference is observed with high probability. The first application is the cryptanalysis of the data encryption standard (DES).

Differential cryptanalysis is considered as an effective analysis method for evaluating the security level of block ciphers. Various extensions are introduced in the following years such as impossible differential cryptanalysis [11], truncated differential cryptanalysis [12] and improbable differential cryptanalysis [20]. In 2011 multiple differential cryptanalysis is stated by Blondeau et al. [4]. Unlike the original version of differential cryptanalysis in which one input-output difference is used, in multiple differential cryptanalysis several input differences are used with a set of corresponding output differences.

Differential cryptanalysis is widely used in security analysis, however underlying theory, including estimating the success probability is focused recently. In their work, Biham and Shamir [3] define signal-to-noise ratio as the ratio between the number of right pairs and the average count in a counting scheme. That is, let p be the probability of differential characteristics and p_r be the average probability of wrong keys being suggested by random pairs then signal-to-noise ratio S_N is defined as p / p_r. Also they show the relation between success probability and signal-to-noise ratio. Later, analytic calculations of success probability are presented by Selçuk [19]. Moreover, the term success is generalized by defining advantage. A key recovery attack on m-bit key gets an advantage of a-bit over exhaustive search if the correct key is listed within the top 2^{m-a} key candidates.

In this work, we focus on attacks on Present and the success probabilities of the attacks, in particular differential and multiple differential cryptanalysis. Also we give the experimental results of both attacks including success probabilities.

The contributions are summarized as follows. Our main aim is to contribute to understanding the underlying theory of statistical cryptanalysis

and give a general framework of it by using differential cryptanalysis and multiple differential cryptanalysis. Also, we simulate these attacks for reduced rounds of Present and SmallPresent. The details of success probability calculations are also given. Experiments results show the validation of these attacks and success probabilities. In our experiments we use a *sieving phase* in order to decrease the cost of attacks. Finally, this work is considered as a starting point of success probability of statistical cryptanalysis methods.

The rest of the work is formed as follows. In Section 2 the preliminaries are given. First, we briefly describe the infrastructure of Present. Then, we introduce the notation that is used through the paper and finally we explain the framework of the statistical cryptanalysis which is a generalization of some cryptanalysis methods like differential cryptanalysis. Also success probabilities of these attacks are stated. In Section 3 both differential and multiple differential cryptanalysis of Present are explained. In Subsection 3.1

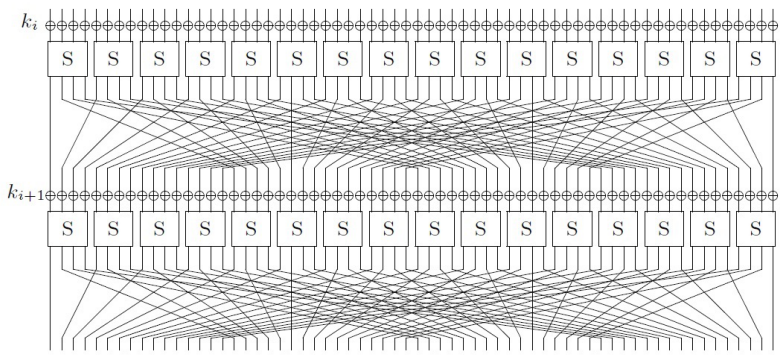

Figure 1 Encryption scheme of Present

the experimental setup is explained. Furthermore, validations of the probabilities of differential characteristics are shown. Finally in Section 4 we summarize our results.

2. PRELIMINARIES

2.1 Description of Present

Present is introduced in the conference CHES 2007 [6]. It is a substitution permutation network with 31-rounds and it has 16 identical 4x4

S-boxes. One round of Present consists of three phases as seen in Figure 1. In the first phase, addRoundKey is the bitwise XOR of the key and state. That is, let s_i be the current state and k_i^j be the j^{th} round key where $0 \leq i \leq 63$. Then the state after addRoundKey is $s_i = s_i \oplus k_i^j \; 0 \leq i \leq 63$.

In the second phase, 16 identical 4x4 S-boxes are applied to the state. The S-box is given in Table I. In the pLayer phase, bit permutation is applied to the state and i^{th} bit is moved to $P(i)^{th}$ position and permutation $P(i)$ is stated in Equation 1 [15].

$$P(i) = \begin{cases} 16 \times i \; mod(63), & 0 \leq x < 63 \\ 63 \quad , & x \geq 0 \end{cases} \qquad (1)$$

Table 1 S-BOX OF PRESENT

$\boldsymbol{i}$	0	1	2	3	4	5	6	7
$\boldsymbol{S(i)}$	C	5	6	B	9	0	A	D
$\boldsymbol{i}$	8	9	A	B	C	D	E	F
$\boldsymbol{S(i)}$	3	E	F	8	4	7	1	2

Two different size of keys can be used in Present; either 80-bit or 128-bit. In this work we briefly state the 80-bit key schedule and 128-bit case is presented in a similar way. Let $K = k_{79}k_{78} \dots k_0$ be the user-supplied key and K_i be the i^{th} round key. In this notation k denotes the key-register's bits and κ denotes the round key bits. Then;

$$K_i = \kappa_{63}\kappa_{62} \dots \kappa_0 = k_{79}k_{78} \dots k_{16}$$

To find the next-round key, the updated register is found in the following way;

- $k_{79}k_{78} \dots k_0 = k_{18}k_{17} \dots k_{20}k_{19}$
- $k_{79}k_{78}k_{77}k_{76} = S(k_{79}k_{78}k_{77}k_{76})$
- $k_{19}k_{18}k_{17}k_{16} = k_{19}k_{18}k_{17}k_{16} \oplus round\_counter$

where `round_counter` denotes the round number with least significant bit on the right.

2.2 Notation

In this section, we introduce the notations and then we give the framework of differential cryptanalysis (DC) and multiple differential cryptanalysis (MDC).

Let *m* be the block size of a block cipher, *x* and *y* be the plaintext and ciphertext, respectively. Throughout the paper, we denote a block cipher using the key *K* as;

$$E_K: \mathbb{F}_2^m \to \mathbb{F}_2^m$$
$$x \to y$$

An *r*-round encryption is defined as: $E_K(x) = F_{K_r} \circ \cdots F_{K_1} = F_K^R$ where F_{k_i} is the round function with round key k_i which is generated by master key *K* [5]. Also an *r*-round differential characteristics of a block cipher we use the following notation [14]. Let $(\delta_0, \delta_r) \in \mathbb{F}_2^m \times \mathbb{F}_2^m$ then,

$$P_r[\delta_0 \to \delta_r] = \Pr[E_K(X) \oplus E_K(X \oplus \delta_0) = \delta_r].$$

In the setting of DC, the attacker deals with a single differential pair (δ_0, δ_r) with high probability. However, we need a collection of differential to state the MDC. The collection of differentials is denoted by Δ [4]. To describe the set Δ, first the set of all input differences included in Δ is defined.

$$\Delta_0 = \{\delta_0 | \exists \delta_r, (\delta_0, \delta_r) \in \Delta\}.$$

In a similar way, the set of output differences Δ_r^i is defined for a fixed input difference δ_0^i as follows:

$$\Delta_r^i = \{\delta_r | (\delta_0^i, \delta_r) \in \Delta\}.$$

Hence, the set of all differentials which the attacker aims to exploit is defined as follows;

$$\Delta = \left\{ (\delta_0^i, \delta_i^{i,j}) \middle| i = 1, \dots, |\Delta_0| \text{ and } j = 1, \dots |\Delta_r^i| \right\}$$

2.3. FRAMEWORK OF STATISTICAL CRYPTANALYSIS

The purpose of DC and MDC is to recover a partial encryption key k_* with an effort less then exhaustive search. Both DC and MDC are parts of statistical cryptanalysis and therefore, they consist of three steps.

- *Distillation:* For N plaintext-ciphertext pairs, ciphertexts are partially decrypted by using each candidate key and the number of occurrences of differential characteristics are counted. Therefore, for each candidate key, the information is obtained.
- *Analysis:* Using the information that obtained in the first step, the list L of the best candidates of k_* is generated according to the counters.
- *Search:* In the last step, all master keys corresponding to the candidate keys are tested until the correct one is found.

Also, the success probability P_S of these attacks are defined as the probability of correct sub-key being in the list L of candidates, in other words $P_S = \Pr[k_* \in L]$. Other features on which the efficiency of the attack depends are data complexity, time complexity and memory complexity. The sufficient number of plaintext-ciphertext pairs (N) to successfully recover the subkey is defined as data complexity. Also the time complexity and the memory complexity is highly influenced by the size of the candidate key list L. Furthermore, the success probability depends on the data complexity since increasing N means increasing P_S and also there is a tradeoff between the data and the time complexity.

Statistical cryptanalysis mostly deals with last-round attacks. More generally, the statistical characteristics is defined as the behavior of $F_{K_{r-1}} \circ \ldots \circ F_{K_1}$. The idea is to partially decipher the ciphertexts using candidates k which are a part of round key K_r. For instance, in DC or MDC the attacker partially decrypts N ciphertexts with all possible last round sub-keys k and counts the number of occurrences of differential δ_{r-1} or the number of occurrences of differentials in the set Δ, respectively. Moreover, if sufficient number of sample is available, the statistical characteristics corresponding to $F_K^{-1} \circ F_K^r$ should be observed by using the correct key candidates. The assumption which statistical cryptanalysis relies on, is the sets F_K^{r-1} and $F_K^{-1} \circ$

F_K^r should be distinguishable. That is, $F_K^{-1} \circ F_K^r$ acts as a random mapping as stated by the following Wrong Key Randomization Hypothesis [8].

Hypothesis 1 (Wrong Key Randomization): The sets $F_K^{-1} \circ F_K^r$ formed by partially encryption of N ciphertexts with wrong key candidates k are indistinguishable from random mapping.

To define the success probabilities of DC and MDC we use the theorems stated by Selçuk [19] and Blondeau et. al [4] respectively and the theorems are stated in Sect 2.4.

2.4 Success Probability

Understanding the underlying theory of statistical attacks is important to achieve a strong analysis and success probability is an important part of the theory also it is introduced as a requirement of an efficient analysis.

The term of success probability in differential cryptanalysis is defined as follows. After observing a differential characteristic, a sufficient number of plaintext-ciphertext pairs are collected with a specific input difference. Using the phases stated in Section 2.3 each pair suggests a set of candidates for last round key. Let S_i be the candidate key set formed by i^{th} pair. If a pair satisfies the differential characteristics (called as *right pair)* then the right key k_* is always in the set S_i. If a pair is *wrong pair*, it suggests a set of random keys. And the right k_* doesn't have to be in this set. At the end of the attack, candidate list L is formed by counting the keys that are suggested by pairs. The counting list L plays an important role to introduce the success of the attack because, the term *success* is defined as observing the right key k_* within the top 2^{m-a} candidates list L where m is the block size and a is the advantage [19]. We know that exhaustive search space is 2^m, therefore success probability with the term advantage states the relation between the cryptanalysis and exhaustive search.

Statistical cryptanalysis is based on the Hypothesis 1. The idea of it is basically distinguishing $F_K^{-1} \circ F_K^r$ from a random mapping. While using incorrect key, the probability of observing the differential is stated as $\frac{1}{2^{m-1}}$ since we actually randomly pick the bits. Using Hypothesis 1 the following equation is introduced to differential cryptanalysis and it is the adaptation of Hypothesis 1 to differential cryptanalysis.

$$P_{r_x}\left[F_k^{-1}\left(E_{K_*}(X)\right) \oplus F_k^{-1}\left(E_{K_*}\left(X \oplus \delta_0^i\right)\right) = \delta^{i,j}\right] \quad (2)$$
$$= \begin{cases} p_*^{i,j} & \text{if } k = k_* \\ p^{i,j} = \dfrac{1}{2^m - 1} & \text{if } k \neq k_* \end{cases}$$

To present the success probability of a differential attack we use the formulas stated by Selçuk [19].

Theorem 1: [19] Let P_S be the probability that a differential attack using N plaintext-ciphertext pairs, on a k-bit key, with a characteristic of probability $P_r[\delta_0 \rightarrow \delta_r] = p$ and signal to noise ratio S_N and an a-bit or higher advantage. Assuming that Hypothesis 1 holds then we have, for sufficiently large m and N, and μ denoting pN,

$$P_S = \Phi\left(\frac{\sqrt{\mu S_N} - \Phi^{-1}(1 - 2^{-a})}{\sqrt{S_N + 1}}\right)$$

Where $S_N = p/p_r$ is the signal to noise ratio.

In a multiple differential attack, the list L is formed by counting the suggested keys by pairs which satisfy a set of differential characteristics. Also, the success probability of a MDC is stated by Blondeau et al. [4].

Theorem 2:

$$P_S \approx 1 - G_*\left[G^{-1}\left(1 - \frac{l-1}{2^{n_k - 2}}\right) - 1\right]$$

where $G_*(x)$ and $G(x)$ are the estimation of the cumulative distribution

function of the counters defined in [4] Proposition 1.

3. DIFFERENTIAL AND MULTIPLE DIFFERENTIAL ATTACKS ON PRESENT

The analysis of Present has drawn a special attention from many researchers due to its simple design and good performance. In 2008 Wang [21] state a differential attack on 16-rounds of Present. Another differential attack is stated by Albrecht et al [1] using algebraic techniques and corrected

comment: Initialze a table D for key candidates
for each $\delta_0^{(i)} \in \Delta_0$
do {
  for each *plaintext pair* (x_a, x_b) *with* $x_b = x_a \oplus \delta_0^{(i)}$
  do {
    if $y_a \oplus y_b \in \Delta_{r+1}^{(i)}$
    then for each *key candidate* k
    do {
      $\delta = F_k^{-1}(y_a) \oplus F_k^{-1}(y_b)$
      if $\delta \in \Delta_r^{(i)}$
      then $D[k] \leftarrow D[k] + 1$
comment: The list L is formed by using the highest counters
for each $k \in L$
do {
  for each master key K corresponding to k
  do {
    if $E_k(x) = y = E_{k_*}(x)$
    then return (K)

Algorithm 1 DIFFERENTIAL CRYPTANALYSIS ($(x_i;y_i)$; K)

version of this attack is showed by Preneel et al [22]. Also, related key cryptanalysis of Present introduced by Kocair et al [18] and in 2011 multiple differential attack is presented by Blondeau et al. [4].

3.1 EXPERIMENTAL SETUP

In this section we apply differential and multiple differential attacks on Present. In our experiments, we use *sieving phase* to decrease the cost. In this phase some pairs for which the *r* round difference after encrypting *r+1* rounds cannot be δ_r (or cannot be in the set Δ_r^i) are discarded. To generate the sieve, an off-line computation is done by finding all $\delta_{r+1} \in \mathbb{F}_2^m$ such that there exists a difference $\delta_r^{i,j}$ with the probability $\Pr[\delta_r^{i,j} \rightarrow \delta_{r+1}] \neq 0$.

The general framework of differential cryptanalysis is stated in Algorithm 1 and we use this framework in our experiments. An important remark is that in differential cryptanalysis, δ_0^i and Δ_r^i consist of one elements, that is, we exploit only one differential characteristics.

The first experiment is applied to validate Wang's [21] differential attacks on Present. In the paper Wang proposed a differential attack on 16-rounds of Present which requires 2^{64} chosen plaintext, 2^{32} 6-bit counters and 2^{24} hash cells with time complexity approximately 2^{65}.

Knudsen's method iterative characteristics [13] is used in the Wang's paper for finding differential characteristics. The maximum number of

difference occurrences in difference distribution table (DDT) are 4. Therefore, maximum number of S-boxes of round-2 is 4, round-3 is 7 and round-4 is 9. We calculate the probability of differential characteristics using the values in DDT. Hence, 4-round iterative characteristics with probability 2^{-18} is found. The iterative characteristics is stated in Table 2.

Table 2 4-ROUND ITERATIVE DIFFERENTIAL OF PRESENT [21]

ROUND DIFFERENCE $\boldsymbol{\delta_i}$	*DIFFERENCES*		$\boldsymbol{Pr(\delta_i \rightarrow \delta_{i+1})}$
$\boldsymbol{\delta_0}$	x_0 =0x4	x_3 =0x4	2^{-4}
$\boldsymbol{\delta_1}$	x_0 =0x9	x_8 =0x9	2^{-4}
$\boldsymbol{\delta_2}$	x_8 =0x1	x_{10} =0x1	2^{-4}
$\boldsymbol{\delta_3}$	x_2 =0x5	x_{14} =0x5	2^{-4}
$\boldsymbol{\delta_4}$	x_0 =0x4	x_3 =0x4	2^{-6}

To find the success probability of the attack, signal to noise ratio should be found first. And it is determined in the following way. Let m be the number of pairs, k be the number of key bits which are targeted. α be the average count per counted pair and β be the ratio of counted pairs to all pairs. Then signal to noise ratio is found by the following equation.

$$S_N = \frac{m \cdot p}{m \cdot \alpha \cdot \beta / 2^k} = \frac{2^k \cdot p}{\alpha \cdot \beta}$$

Using this characteristics, Wang found differential characteristics for 11 to 15 rounds [21]. Also, differential probability of Wang's 16-round differential attack is 2^{-62}. We use 4-round differential characteristics of Present stated in Table 2. Signal to noise ratio of this attack is;

$$S_N = \frac{2^k \cdot p}{\alpha \cdot \beta} = \frac{2^{-62} \cdot 2^{32}}{2^{33.18-17.25} \cdot 2^{17.25-67.32}} = 17.63$$

In our experiments, we add sieving phase to increase the efficiency of the attack. The sieve contains possible differentials consists of 2^{32} differences. That is, each element in the set of difference outputs Δ_{r+1} should be of the form 0x000?000?000?000?. Also, our aim is to recover the some bits of the 5th round key. The set of candidate key corresponds to S-boxes with non-zero difference which are seen in the sieve set. Therefore, the list L consist of 2^{32} key candidates.

The success probability of the experiment P_S is found by the following formula where $\mu = p \cdot N = 2^{-18} \cdot 2^{23}$ and N is the number of plaintext-ciphertext pairs. Moreover, we achieve an advantage of 8-bit. Experimental results on success probability are observed by performing the differential attack 100 times.

$$P_S = \Phi\left(\frac{\sqrt{\mu S_N} - \Phi^{-1}(1-2^{-a})}{\sqrt{S_N+1}}\right) = 0.998$$

In the second part of our experiments, we use multiple differential characteristics stated by Blondeau et al. [4]. The attack proposed by Blondeau et al. targets the 18 rounds of Present. The data complexity and the time complexity of the attack are 2^{64}, 2^{79} [4] respectively with the success probability of 98%.

In this experiment we work on the reduced version of Present named as SmallPresent-[n], as the attack on Present is rely on the framework which is represented on SmallPresent-[8]. The structure of SmallPresent-[8] is slightly different than Present and the details of the algorithm is found in [15].

Table 3 Differential characteristics for SmallPresent-[8]

δ_0	0X3	0X5	0X7	0XF	0XD	0XB
δ_r	0x40400000	0x40400000	0x40400000	0x40400000	0x05050000	0x40400000
	0x04040000	0x04040000	0x04040000	0x04040000	0x40400000	0x04040000
	0x50500000	0x50500000	0x50500000	0x50500000	0x04040000	0x50500000
	0x05050000	0x10100000	0x10100000	0x05050000	0x10100000	0x05050000
	0x10100000	0x05050000	0x05050000	0x80800000	0x50500000	0x08080000
	0x01010000	0x01010000	0x01010000	0x08080000	0x01010000	0x80800000
	0x80800000	0x08080000	0x0a0a0000	0x10100000	0x0a0a0000	0x10100000
	0x08080000	0x80800000	0x80800000	0x01010000	0x80800000	0x01010000
	0x0a0a0000	0x0a0a0000	0x08080000	0x0a0a0000	0x00110000	0x0a0a0000
		0x40500000				

Contrary to the previous experiment we use a set of input differences $\Delta_0 = \{0x3, 0x5, 0x7, 0xB, 0xD, 0xF\}$ on x_0. Corresponding output set Δ_r consists of elements of the form 0x????0000. To mount the analysis 55 differential characteristics are used and the list of differentials is stated in Table 3.

The set of candidate keys corresponds to active 4 S-boxes and our sieve set consists of elements of the form 0x?0?0?0?. As a result, the candidates list L of keys consists of 2^{16} elements.

Using differential characteristics set stated in Table 3 and Algorithm 1, we simulate the multiple differential cryptanalysis on SmallPresent-[8]. Total probability of the differential characteristics is approximately 2^{-12}. Using

this analysis we able to recover 16 bits of the 5^{th} round key. Using different number of pairs between 2^{13} and 2^{22} we achieve different advantages. The success probabilities stated in the paper are between 0.47 and 0.92, in our experiments we produce these probabilities with an advantage of 8-bit. Experimental results on success probability are observed by performing the multiple differential attack 100 times.

4. CONCLUSION

Design and analysis of lightweight block ciphers have gain popularity due to the needs in ubiquitous devices' industry. Also understanding the underlying tools of analysis methods becomes important.

In this work, we focus on Present which is one of the most analyzed algorithms using different types of attacks in recent years. Also, differential and multiple differential attacks are proposed as two powerful methods. Therefore, our aim is to analyze the differential attacks on Present.

We give a brief framework of differential cryptanalysis and multiple differential cryptanalysis which is seen as a generalization of the former one. Both attacks are considered as a statistical cryptanalysis method. We give a framework of statistical cryptanalysis and the underlying theory of it including success probabilities. Also calculations and experimental results on Present and SmallPresent are given. Simulation results are provided to validate theoretical results. Also we use a use *sieving phase* to decrease the cost. Both differential attacks are not considered as the best attack on Present. However multiple differential cryptanalysis has advantages and promising results over classical differential cryptanalysis.

Our main idea is to contribute to understanding the underlying theory of statistical cryptanalysis and give a general framework of it by using differential cryptanalysis and multiple differential cryptanalysis. Also, we simulate these attacks for reduced rounds of Present and SmallPresent. The details of success probability calculations are also given. Experiments results show the validation of these attacks and success probabilities. Although these attacks are proposed on more rounds of Present, our results provide a starting point of success probability of statistical cryptanalysis methods and underlying theory of multiple differential cryptanalysis and other differential cryptanalysis methods are still open research area.

REFERENCES

[1] Martin Albrecht and Carlos Cid, *Algebraic techniques in differential cryptanalysis*. Cryptology ePrint Archive, Report 2008/177, 2008. http://eprint.iacr.org/.

[2] Eli Biham and Adi Shamir, *Differential cryptanalysis of des-like cryptosystems*, In Proceedings of the 10th Annual International Cryptology Conference on Advances in Cryptology, CRYPTO '90, pages 2–21, London, UK, UK, 1991. Springer-Verlag.

[3] Eli Biham and Adi Shamir, *Differential Cryptanalysis of DES-like cryptosystems*, Journal of Cryptology, 4(1):3–72, 1991.

[4] Celine Blondeau and Benot Grard, *Multiple differential cryptanalysis: Theory and practice*, In Antoine Joux, editor, Fast Software Encryption, volume 6733 of Lecture Notes in Computer Science, pages 35–54. Springer Berlin Heidelberg, 2011.

[5] Celine Blondeau, Benot Grard, and Kaisa Nyberg, *Multiple differential cryptanalysis using LLR and χ2 statistics*, In Ivan Visconti and Roberto De Prisco, editors, Security and Cryptography for Networks, volume 7485 of Lecture Notes in Computer Science, pages 343–360. Springer Berlin Heidelberg, 2012.

[6] A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin, and C. Vikkelsoe, *Present: An ultralightweight block cipher*, In Pascal Paillier and Ingrid Verbauwhede, editors, Cryptographic Hardware and Embedded Systems - CHES 2007, volume 4727 of Lecture Notes in Computer Science, pages 450–466. Springer Berlin Heidelberg, 2007.

[7] Christophe Canniere, Orr Dunkelman, and Miroslav Knezevic, *Katan and Ktantan – a family of small and efficient hardware-oriented block ciphers*, In Proceedings of the 11th International Workshop on Cryptographic Hardware and Embedded Systems, CHES '09, pages 272–288, Berlin, Heidelberg, 2009. Springer-Verlag.

[8] Carlo Harpes, Gerhard G. Kramer, and James L. Massey, *A generalization of linear cryptanalysis and the applicability of matsui's piling-up lemma*, In Proceedings of the 14th Annual International Conference on Theory and Application of Cryptographic Techniques, EUROCRYPT'95, pages 24–38, Berlin, Heidelberg, 1995. Springer-Verlag.

[9] Deukjo Hong, Jaechul Sung, Seokhie Hong, Jongin Lim, Sangjin Lee, Bon-Seok Koo, Changhoon Lee, Donghoon Chang, Jesang Lee, Kitae Jeong, Hyun Kim, Jongsung Kim, and Seongtaek Chee, *Hight: A new block cipher suitable for low-resource device*, In Louis Goubin and Mitsuru Matsui, editors, Cryptographic Hardware and Embedded Systems - CHES 2006, volume 4249 of Lecture Notes in Computer Science, pages 46–59. Springer Berlin Heidelberg, 2006.

[10] ISO. Information technology – Security techniques – Lightweight cryptography – Part 2: Block ciphers. Technical Report ISO/IEC 29192-2:2012, International Organization for Standardization, Geneva, Switzerland, 2012.

[11] Lars Knudsen, *Deal - a 128-bit block cipher*, In NIST AES Proposal, 1998.

[12] Lars R. Knudsen, *Truncated and higher order differentials*, In Fast Software Encryption: Second International Workshop. Leuven, Belgium, 14-16 December 1994, Proceedings, pages 196–211, 1994.

[13] Lars Ramkilde Knudsen, *Iterative characteristics of DES and s^2-DES*, In Ernest F. Brickell, editor, Advances in Cryptology CRYPTO 92, volume 740 of Lecture Notes in Computer Science, pages 497–511. Springer Berlin Heidelberg, 1993.

[14] Xuejia Lai, JamesL. Massey, and Sean Murphy, *Markov ciphers and differential cryptanalysis*, In DonaldW. Davies, editor, Advances in Cryptology EUROCRYPT 91, volume 547 of Lecture Notes in Computer Science, pages 17–38. Springer Berlin Heidelberg, 1991.

[15] Gregor Leander, *Small scale variants of the block cipher PRESENT*, IACR Cryptology ePrint Archive, 2010:143, 2010.

[16] Gregor Leander, Christof Paar, Axel Poschmann, and Kai Schramm, *New lightweight des variants*, In Fast Software Encryption, 14th International Workshop, FSE 2007, Luxembourg, Luxembourg, March 26-28, 2007, Revised Selected Papers, volume 4593 of Lecture Notes in Computer Science, pages 196–210. Springer, 2007.

[17] Chae Hoon Lim and Tymur Korkishko, *mCrypton a lightweight block cipher for security of low-cost rfid tags and sensors*, In Joo-Seok Song, Taekyoung Kwon, and Moti Yung, editors, Information Security Applications, volume 3786 of Lecture Notes in Computer Science, pages 243–258. Springer Berlin Heidelberg, 2006.

[18] Onur Özen, Kerem Varıcı, Cihangir Tezcan, and Çelebi Kocair, *Lightweight block ciphers revisited: Cryptanalysis of reduced round present and hight*, In Colin Boyd and Juan Gonzlez Nieto, editors,

Information Security and Privacy, volume 5594 of Lecture Notes in Computer Science, pages 90–107. Springer Berlin Heidelberg, 2009.

[19] Ali Aydın Selçuk, *On probability of success in linear and differential cryptanalysis*, Journal of Cryptology, 21(1):131–147, 2008.

[20] Cihangir Tezcan, *Improbable differential cryptanalysis*, In Proceedings of the 6th International Conference on Security of Information and Networks, SIN '13, pages 457–457, New York, NY, USA, 2013. ACM.

[21] Meiqin Wang, *Differential cryptanalysis of reduced-round present*, In Serge Vaudenay, editor, Progress in Cryptology AFRICACRYPT 2008, volume 5023 of Lecture Notes in Computer Science, pages 40–49. Springer Berlin Heidelberg, 2008.

[22] Meiqin Wang, Yue Sun, Nicky Mouha, and Bart Preneel, *Algebraic techniques in differential cryptanalysis revisited*, In Udaya Parampalli and Philip Hawkes, editors, Information Security and Privacy, volume 6812 of Lecture Notes in Computer Science, pages 120–141. Springer Berlin Heidelberg, 2011.

[23] David Wheeler and Roger Needham, *Tea, a tiny encryption algorithm*, pages 97–110. Springer-Verlag, 1995.