The ISC Int'l Journal of Information Security
ISeCure

January 2018, Volume 10, Number 1 (pp. 3–14)
http://www.isecure-journal.org

Impossible Differential Cryptanalysis of Reduced-Round Midori64 Block Cipher☆

Aein Rezaei Shahmirzadi [1], Seyyed Arash Azimi [1], Mahmoud Salmasizadeh [2,*], Javad Mohajeri [2], and Mohammad Reza Aref [3]

[1] *Department of Electrical Engineering, Sharif University of Technology, Tehran, Iran*
[2] *Electronics Research Institute, Sharif University of Technology, Tehran, Iran*
[3] *Information Systems and Security Lab (ISSL), Department of Electrical Engineering, Sharif University of Technology, Tehran, Iran*

ARTICLE INFO.

Article history:
Received: 14 September 2017
Accepted: 24 January 2018
Published Online: 30 January 2018

Keywords:
Midori, Block Cipher, Impossible Differential Attack.

Abstract

Impossible differential attack is a well-known mean to examine robustness of block ciphers. Using impossible differential cryptanalysis, we analyze security of a family of lightweight block ciphers, named Midori, that are designed considering low energy consumption. Midori state size can be either 64 bits for Midori64 or 128 bits for Midori128; however, both versions have key size equal to 128 bits. In this paper, we mainly study security of Midori64. To this end, we use various techniques such as early-abort, memory reallocation, miss-in-the-middle and turning to account the inadequate key schedule algorithm of Midori64. We first show two new 7-round impossible differential characteristics which are, to the best of our knowledge, the longest impossible differential characteristics found for Midori64. Based on the new characteristics, we mount three impossible differential attacks on 10, 11, and 12 rounds on Midori64 with $2^{87.7}$, $2^{90.63}$, and $2^{90.51}$ time complexity, respectively, to retrieve the master-key.

1 Introduction

Since early twenty-first century, lightweight cryptography has become an inevitable domain which focuses on designing cryptographic algorithms and modes specialized for highly constrained devices, including RFID tags, IoT devices, sensor networks, etc. providing confidentiality and integrity of the aforementioned systems.

☆ This article is an extended version of an ISCISC'2017 paper.

* Corresponding author.
Email addresses: rezaeishahmirzadi@ee.sharif.edu (A. Rezaei Shahmirzadi), arash_azimi@ee.sharif.edu (S. A. Azimi), salmasi@sharif.edu (M. Salmasizadeh), mohajer@sharif.edu (J. Mohajeri), aref@sharif.edu (M. R. Aref)

ISSN: 2008-2045

In design rationale of lightweight block ciphers, there are quite a few constraints that diversify the block cipher applications. For instance, area restriction and low latency are mainly considered in PRESENT [2], PRINTCipher [3], TWINE [4],PRINCE [5], LBlock [6], CLEFIA [7] , KATAN and KTANTAN [8]. In Asiacrypt'15, Midori [9] was presented as a lightweight block cipher considering energy consumption as a constraint that had not theretofore attracted much attention. There are two variants of Midori block cipher: Midori64 and Midori128, which have 64 and 128 bits of block length, respectively. Moreover, they both take 128 bits as a key input.

Despite the fact that Midori is recently presented, it has faced a number of attacks evaluating its security. In weak-key setting, Guo *et al.* [10] analyzed the cipher using invariant subspace attack and found 2^{32} weak keys for Midori64. In addition, Todo *et al.* [11] found 2^{64} weak keys using nonlinear invariant attack. In related-key setting, Dong and Shen [12] could retrieve the master-key by applying related-key differential attack to 14 rounds of Midori64. Furthermore, Gérault *et al.* [13] gave a related-key differential attack for full-round of Midori64. In single-key setting, Chen and Wang [14] applied impossible differential attack to 10 rounds of Midori64. Furthermore, Lin and Wu [15] gave three meet-in-the-middle attacks mounted on 10, 11 and 12 rounds of Midori64.

Impossible differential attack is a powerful method of cryptanalysis which has been applied to plenty of lightweight block ciphers to analyze their security [16–20]. In this paper, we use the attack to evaluate Midori64 security. We introduce two new 7-round impossible differential characteristics which are the first 7-round impossible differential trails to the best of our knowledge.

Utilizing new impossible differential characteristics, we present three impossible differential attacks mounted on 10, 11, and 12 rounds of Midori64. Table 1 summarizes results of the attacks applied to Midori64. Note that the attack [10] and [11] in weak-key setting could only recover the master-key if it belongs to the weak-key sets, which have a cardinality of 2^{32} and 2^{64}, respectively. Therefore, the attacks are not capable of recovering master-key if it has been selected from the complement set containing the other $(2^{128} - 2^{32})$ and $(2^{128} - 2^{64})$ possible keys, respectively, which are approximately equal to the whole 2^{128} key space. Moreover, comparing related-key model with single-key model is inequitable since in related-key model the attacker requires more than one cipher having related secret keys which seems to be non-viable.

The 10-round version of our attacks includes both pre and post whitening keys and has less time complexity comparing to [15], while in comparison to [14], which excludes pre whitening key, needs less data but more computations to retrieve the master-key. Although 11-round and 12-round attacks, respectively, exclude post whitening key and both whitening keys, they are, to the best of our knowledge, fastest attacks against 11-round and 12-round Midori64 in single-key model, respectively. Moreover, by creating two lists and reallocating memory, we could significantly decrease memory complexity of our attacks. Consequently, all our attacks need 2^{41} 64-bit blocks, while in contrast to $2^{92.7}$, $2^{89.2}$ and 2^{106} [15], and $2^{62.4}$ [14], our attacks have minimum memory complexity among all known attacks in single-key model.

The rest of paper is organized as follows. In Section 2 we discuss preliminaries including brief description of Midori64 and impossible differential cryptanalysis with some notations that is used in this paper. Section 3 instantiates the new IDCs. In Section 4 we present three impossible differential attacks applied to Midori64. Finally, Section 5 concludes the paper.

2 Preliminaries

2.1 Brief Description of Midori

Midori is a family of lightweight block ciphers that is based on the Substitution Permutation Network (SPN). There are two versions of Midori: Midori64 and Midori128, both have 128-bit key size. The total round number of Midori64 is 16, while in Midori128 it is 20 rounds. The block size of Midori64 and Midori128 are equal to 64 and 128 bits, respectively. In this paper, we specifically exhaust the security of Midori64. Following 4×4 array represents data expression in each state of Midori64. In matrix S, s_i denotes nibble i^{th} of the state.

$$S = \begin{pmatrix} s_0 & s_4 & s_8 & s_{12} \\ s_1 & s_5 & s_9 & s_{13} \\ s_2 & s_6 & s_{10} & s_{14} \\ s_3 & s_7 & s_{11} & s_{15} \end{pmatrix}$$

Each round of Midori consists of four steps: *SubCell*, *ShuffleCell*, *MixColumn* and *KeyAdd*. One should observe that among the mentioned steps, the execution time of *SubCell* overcomes the other three operations. As a result, the running time of each round in Midori64 is approximately equal to performing *SubCell* operation.

SubCell

A non-linear substitution step where each nibble is replaced with another nibble by a bijective 4-bit S-box.

ShuffleCell

Each nibble of the state is permuted as follows:

$$\begin{pmatrix} s_0 & s_4 & s_8 & s_{12} \\ s_1 & s_5 & s_9 & s_{13} \\ s_2 & s_6 & s_{10} & s_{14} \\ s_3 & s_7 & s_{11} & s_{15} \end{pmatrix} \rightarrow \begin{pmatrix} s_0 & s_{14} & s_9 & s_7 \\ s_{10} & s_4 & s_3 & s_{13} \\ s_5 & s_{11} & s_{12} & s_2 \\ s_{15} & s_1 & s_{16} & s_8 \end{pmatrix}$$

In fact, each column is spread to all four rows.

MixColumn

This step consists of a mixing operation which operates on each columns of the state by applying the following matrix:

Table 1. Midori64 Key Recovery Attacks in Single-Key Model

Attack	Pre/Post WK	#	Time	Data (CP)	Memory (64-bit)	Ref
Single-key setting (full-key space)						
MITM	Pre & Post	10	$2^{99.5}$	$2^{59.5}$	$2^{92.7}$	[15]
MITM	Pre & Post	11	2^{122}	2^{53}	$2^{89.2}$	[15]
MITM	Pre & Post	12	$2^{125.5}$	$2^{55.5}$	2^{106}	[15]
IDC	Post	10	$2^{80.81}$	$2^{62.4}$	$2^{65.13}$	[14]
IDC	Pre & Post	10	$2^{87.71}$	$2^{61.97}$	2^{41}	This Paper
IDC	Pre	11	$2^{90.63}$	$2^{61.87}$	2^{41}	
IDC	None	12	$2^{90.51}$	$2^{61.87}$	2^{41}	
Related-key setting (full-key space)						
RKDA	Pre & Post	14	2^{116}	2^{59}	2^{112}	[12]
RKDA	Pre & Post	full	$2^{35.8}$	$2^{23.75}$	–	[13]
Weak-key setting (2^{32} and 2^{64} weak key space, respectively)						
ISA	Pre & Post	full	2^{16}	2	–	[10]
NISA	Pre & Post	full	2^{16}	2	–	[11]

WK: Whitening Key, #: Rounds, Ref: Reference, Time: Time Complexity, CP: Chosen Plain-text

MITM: Meet-In-The-Middle, IDC: Impossible Differential Cryptanalysis

Table 2. 4-bit bijective S-box in hexadecimal form

x	Sb(x)	x	Sb(x)	x	Sb(x)	x	Sb(x)
0	c	4	e	8	8	c	0
1	a	5	b	8	9	d	2
2	d	6	f	8	1	e	4
3	3	7	7	8	5	f	6

$$M = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

It must be noted here that the operations are performed over $GF(2^m)$.

KeyAdd

In this step, the sub-key is added by combining each nibble of the state with the corresponding nibble of the sub-key using bit-wise XOR.

Note that in the last round of Midori, *ShuffleCell* and *MixColumn* are omitted and in the first round, one additional *KeyAdd* operation are applied. Overview of Midori64 is shown in Figure 1 [9].

Key schedule

In Midori64, the first half and the second half of master-key are named k_0 and k_1, respectively; in other words, $K = k_0 \| k_1$. The round keys for $i = 0, \cdots, 14$ are $RK_i = K_{(i+1)(mod\ 2)} \oplus \alpha_i$ where each α_i is a known constant. The whitening key $WK = k_0 \oplus k_1$ is used as sub-key in the first and the last *KeyAdd* operations (i.e. RK_{-1} and RK_{15}, respectively). Due to the fact that we can compute each sub-key for even rounds from k_0 and odd rounds from k_1, we do not consider the constants for sub-keys and refer to them as k_0 and k_1.

2.2 Brief explanation of impossible differential cryptanalysis

Impossible differential cryptanalysis is a special kind of differential cryptanalysis for block ciphers. Differential attack [21] traces differences through the cipher that exhibits non-random behavior while impossible differential cryptanalysis uses differentials that is impossible to occur (zero probability) in order to discard wrong keys and find the correct key.

Knudsen uses this attack in [22] for the first time. Later, in the same year, Biham et al. introduced the name "impossible differential" and applied this technique to IDEA, Khufu and Skipjack block ciphers [23, 24]. After that, this attack is used to analyze the security of many block ciphers like AES [25],

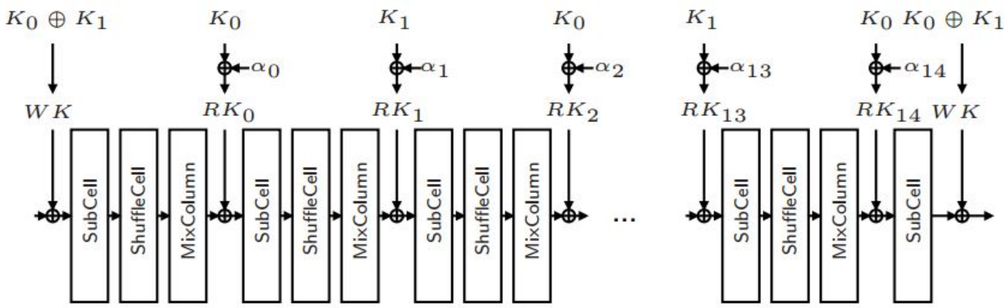


Figure 1. The block cipher Midori64 [9]

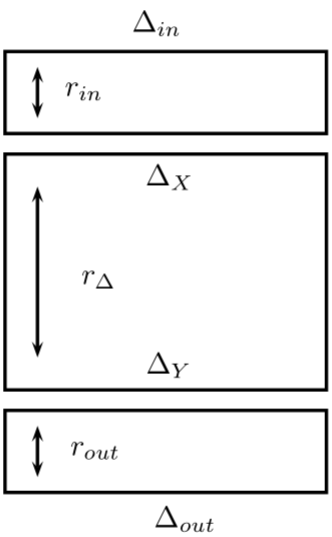


Figure 2. ΔX, ΔY: input and output difference of the impossible differential.
r_Δ: number of rounds of the impossible differential.
Δ_{in}, Δ_{out}: set of all possible input and output differences of the cipher.
r_{in}: number of rounds of the differential path (ΔX, Δ_{in}).
r_{out}: number of rounds of the differential path (ΔY, Δ_{out}). [17]

CRYPTON [26], Camellia [27] and SPARX [28]. The best results in terms of number of rounds and time complexity are reached by using this technique to the best of our knowledge in this block ciphers [29–32].

Impossible differential attack can be divided into two main steps. The first step is to find an appropriate impossible differential characteristic which has maximum number of rounds. In second step, the characteristic is extended in both directions and the incorrect keys are removed from the candidate master-keys (see Figure 2).

2.2.1 Discovering Impossible Differential Characteristic

In this step, we should find an input difference ΔX and an output difference ΔY in a way that if ΔX propagates through certain number of rounds (r_Δ), the probability of occurrence of ΔY will be equal to zero. Any path that has this property is called an impossible differential characteristic.

Initially, impossible differential characteristics are found via ad-hoc methods and the attacker should search within many cases to find a contradiction. After that, many researches and studies have been conducted and many algorithms proposed to find it automatically [33–36].

2.2.2 Key Sieving

After finding maximum-length characteristic, first we choose some plain-text pairs that their differences are equal to Δ_{in} (see Figure 2). Then, for each plain-text, we ask for their corresponding cipher-texts and keep those cipher-text pairs that have Δ_{out} differences. Subsequently, we partially encrypt plain-texts (decrypt cipher-tests) to reach characteristic with guessed key and discard those pairs that do not satisfy special property that derived from impossible differential characteristic. Finally, we remove the guessed key from the key space if at least one plain-text pair and its corresponding cipher-text pair remains after sieving process. We repeat the above procedure to eliminate wrong keys. For the remaining candidate keys, we examine them using one or more plain-text/cipher-text to find the correct master-key. Indeed, we find the correct key by discarding all the wrong guesses. This part of attack is highly technical and many parameters should be taken into consideration to calculate time and data complexity correctly.

There are many methods to reduce time complexity. one of the most powerful methods is called early abort [37]. We can reduce computational workload by using this technique. Furthermore, we may apply the attack to include more rounds of the corresponding block cipher. The general approach is to guess all relevant sub-keys to partially encrypt/decrypt each pair and then check the differences generated by plain-text pairs with an expected difference (or check the differences produced by its corresponding cipher-text pairs with an expected difference). However, we can check the conditions step by step by guessing only a small fraction of the round sub-key bits instead of the whole relevant sub-key. In this way, we can perform the attack more efficiently in terms of time complexity. Moreover, a pair can be sieved using the intermediate value differences to alleviate the total computations. We extensively used this technique in this paper to reduce time complexity.

2.3 Notations

The notations in this paper are summarized in Table 3.

Table 3. Notations

Symbol	Definition
$\oplus$	bit-wise XOR;
$A\|B$	concatenation of A and B;
WK	whitening key;
K	master-key;
k_0	the first half of the master-key;
k_1	the second half of the master-key;
$k[j]$	the j^{th} nibble of k;
X_i	the data after *KeyAdd* operation at round i;
Y_i	the data after *SubCell* operation at round i;
Z_i	the data after *ShuffleCell* operation at round i;
V_i	the data after *MixColumn* operation at round i;
a,b	known non-zero difference;
$*$	unknown non-zero difference;
?	uncertain difference;
MC(u)	*MixColumn* of u;
ΔX_i	the difference of X , X' at round i, i.e. $\Delta X = X \oplus X'$.

3 7-round Impossible Differential Characteristics for Midori64 and Midori128

This section is devoted to our new 7-round impossible differential characteristics. Each of the characteristics begins with two equal non-zero differences and ends with three equal non-zero differences.

Among these characteristics, we try to find the best trail considering the time complexity. Taking that into account, we choose impossible differential characteristic used for the 10-round impossible differential attack mounted on Midori64 as shown in Figure 3. Figure 4 indicates another impossible differential characteristic that is leveraged in 11-round

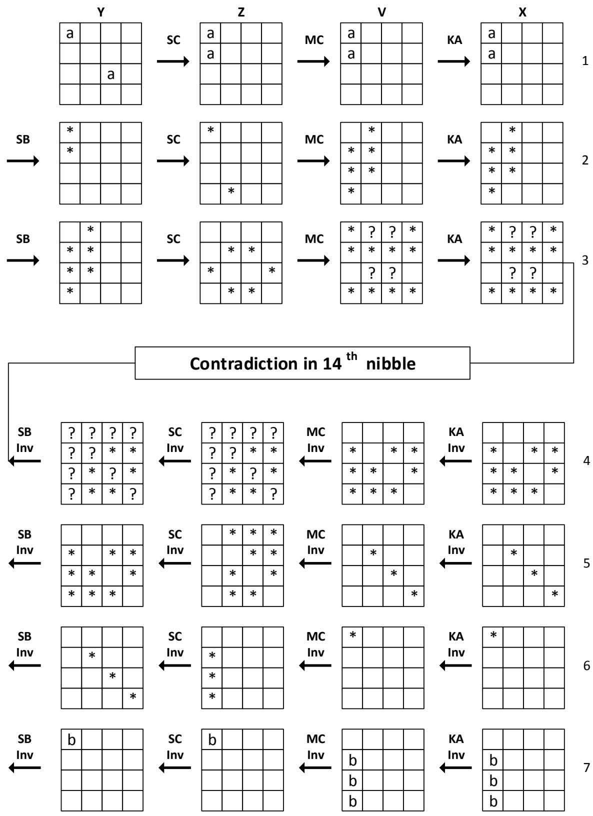


Figure 3. 7-round IDC used for 10-round impossible differential attack.

and 12-round versions of impossible differential attack proposed in this paper. Note that in this paper "a","*", "?" and blank cell represent known non-zero difference, unknown zero-difference, zero difference and uncertain difference, respectively.

4 Impossible Differential Cryptanalysis of Midori64

In this section we present three impossible differential attacks mounted on 10, 11 and 12 rounds of Midori64 block cipher, all in single-key model. For each case, impossible differential characteristics have been selected to minimize time complexity of the attacks.

Note that in view of memory complexity, for each structure we save all plain-texts and all cipher-texts in two 64-bit list. We also devote a table that each row stands for a pair and the content of the row is a 1-bit flag showing whether the corresponding pair is sieved or not.

4.1 Impossible Differential Cryptanalysis of 10-round Midori64

Figure 5 shows overview of the attack. The series of steps of the attack are:

(1) Consider 2^{24} plain-texts that take all possible

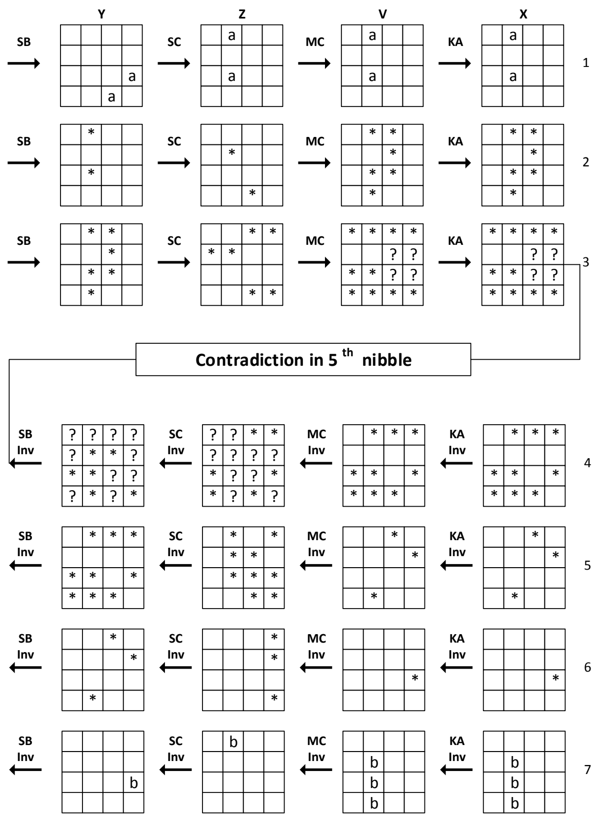


Figure 4. 7-round IDC used for 11 and 12-round impossible differential attacks.

values in positions (3, 5, 6, 9, 10, 15) and have fixed values in other nibbles. That is called a structure. The number of pairs that can be formed by one structure is about $2^{24} \times 2^{23} = 2^{47}$. We take 2^n structures, therefore we have 2^{n+24} plain-texts and 2^{n+47} pairs.

(2) Guess $WK[3,5,6,9,10,15] = (k_0 \oplus k_1)[3,5,6,9,10,15]$ and compute Y_1 for all 2^{n+24} data. Keep only pairs that have $\Delta Y_1[5] = \Delta Y_1[10] = \Delta Y_1[15]$ as well as $\Delta Y_1[3] = \Delta Y_1[6] = \Delta Y_1[9]$. The probability of this event is about $2^{-8\times 2} = 2^{-16}$, hence $2^{n+47-16} = 2^{n+31}$ pairs remain at the end of this step.

(3) Guess $k_0[0,10]$ and compute Y_2. Keep only pairs that have same values in $\Delta Y_2[0] = \Delta Y_2[10]$. Consequently, the number of remaining pairs is approximately $2^{n+31-4} = 2^{n+27}$.

(4) Consider all remaining plain-texts and ask for corresponding cipher-texts. Keep those pairs that their cipher-texts have zero differences in nibbles $(0,1,2,3,7,9,14)$. Therefore, the number of remaining pairs is about $2^{n+27-28} = 2^{n-1}$. Since the values of $WK[5,6,10,15]$ are known from stage 2, only guess values of $WK[4,8,11,12,13] = (k_0 \oplus k_1)[4,8,11,12,13]$ to compute $Y_{10}[4,5,6,8,10,11,12,13,15]$. Then, find $MC^{-1}(X_{10})[4,5,6,8,10,11,12,13,15]$ and for each pair compare the non-zero differences in second column and keep those pairs that have same values for the three non-zero differences. Perform the same procedure for third and forth columns, too. The probability that a pair will be held is about 2^{-24}, thus the expected number of remaining pairs is about 2^{n-25}. This step is dominant term in execution time, so we use early-abort technique to reduce time complexity. Early-abort is a technique that reduces time complexity without any side effects. Regarding this technique, we will explain how to calculate time complexity for this step in more detail.

As mentioned before, the number of remaining pairs is about 2^{n-1}; hence, there are $2\times 2^{n-1}$ plain-texts. Six and two nibbles of the master key are guessed in second and third step, respectively, thus the term $2^{24} \times 2^8$ will be appeared in time complexity of this part. Consider second column of the whitening key in the last round and as mentioned previously, $WK[5]$ and $WK[6]$ are known. The early-abort technique is utilized as follows. First, calculate $X_9[5,6]$. After that, if $\Delta X_9[5]$ and $\Delta X_9[6]$ are the same, guess $WK[4]$ and afterwards, calculate $X_9[4]$. The probability that $\Delta X_9[5]$ and $\Delta X_9[6]$ are identical is 2^{-4}, hence $X_9[4]$ can be calculated with probability of 2^{-4}. If $\Delta X_9[4]$, $\Delta X_9[5]$ and $\Delta X_9[6]$ are the same, by taking into account the known $WK[10]$, compute $X_9[10]$. After that, guess $WK[11]$ and compute $X_9[11]$. The probability that $\Delta X_9[4]$, $\Delta X_9[5]$ and $\Delta X_9[6]$ are equal is 2^{-8}, as a deduction $X_9[10]$ and $X_9[11]$ are computed with probability of 2^{-8}. Next, guess $WK[8]$ and calculate $X_9[8]$ if $\Delta X_9[10]$ and $\Delta X_9[11]$ are the same values and $\Delta X_9[4]$, $\Delta X_9[5]$ and $\Delta X_9[6]$ are equal. Thus, $X_9[8]$ is calculated with probability of 2^{-12} . If $\Delta X_9[4] = \Delta X_9[5] = \Delta X_9[6]$ and $\Delta X_9[4] = \Delta X_9[5] = \Delta X_9[6]$, compute $X_9[15]$ using $WK[15]$ that is known from stage 2. Thereupon, guess $WK[13]$ and calculate $X_9[13]$. The probability that the differences in nibbles $[4,5,6]$ and $[8,10,11]$ of X_9 are the same is 2^{-16}; therefore, with the same probability, $X_9[13]$ and $X_9[15]$ can be computed. Finally, if $X_9[13]$ and $X_9[15]$ are equal, guess $WK[12]$ and calculate $X_9[12]$.

(5) For each remaining pairs, guess $u_0[7,9,14]$ (note that $MC(u_0) = k_0$) and compute $Z_9[7,9,14]$ and $X_8[1,2,3]$. Find those pairs that each has equal values in $\Delta X_8[1]$, $\Delta X_8[2]$ and $\Delta X_8[3]$. If at least one pair remains, calculate the and discard corresponding master-key

Complexity analysis

In step 2, 3, 4 and 5 we guessed 24, 8, 20, 12 key bits, respectively. Hence, the expected number of the remaining wrong keys is $N = 2^{64} \times (1 - 2^{-8})^{2^{n-25}}$. If we want to have small time complexity, we set $n = 37.97$ thus data complexity is $2^{61.97}$ chosen plain-texts. The total time complexity is about $2^{87.71}$ 10-round encryptions and memory complexity is 2^{41} 64-bit blocks. Table 4 summarizes the procedure of the attack. Note that the last row of Table 4 indicates the time complexity of examining the remaining keys via one plain-text/cipher-text pair to find the correct key. In the last step, the probability of equality of $\Delta X_8[1]$, $\Delta X_8[2]$ and $\Delta X_8[3]$ is 2^{-8}, thus the probability of remaining a wrong key for each pair is $1 - 2^{-8}$. The number of remaining pairs is 2^{n-25}, on average. Therefore, the probability of remaining a wrong key is about $(1 - 2^{-8})^{2^{n-25}}$ and the number of 10-round encryption that must be done for finding a correct key is $2^{128} \times (1 - 2^{-8})^{2^{n-25}}$ that is called ERK (Examining the Remaining Keys) in Table 4.

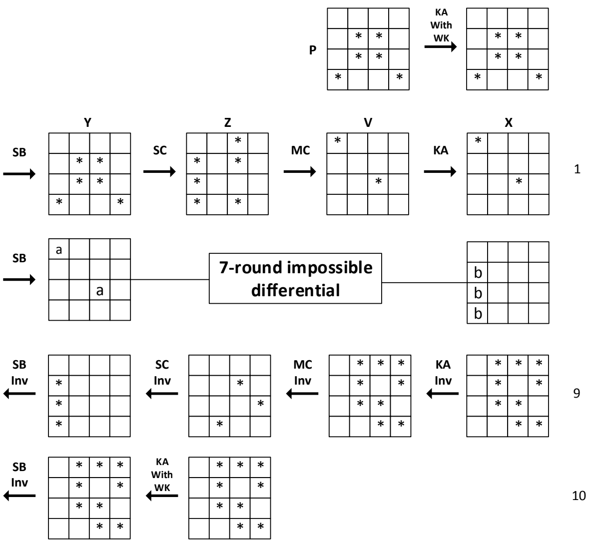


Figure 5. Impossible differential cryptanalysis of 10-round Midori64.

4.2 Impossible Differential Cryptanalysis of 11-round Midori64

In this subsection we explain an impossible differential attack on 11-round Midori64 including pre-whitening key shown in Figure 6. The attack on 11-round Midori64 is:

(1) Choose a group of 2^{24} plain-texts which have fixed values in all nibbles, except positions $(3, 7, 8, 9, 12, 13)$, which is named a structure. A structure forms approximately $2^{24} \times 2^{23} = 2^{47}$

Table 4. Time Complexity of 10-Round Attack on Midori64

Step	Time Complexity in One Round Encryption
2	$2^{n+24} \times 2^{24} \times \frac{6}{16} = 2^{n+46.58}$
3	$2^{n+24} \times 2^{24} \times 2^{8} \times \frac{2}{16} = 2^{n+53} 2 \times 2^{n-1} \times 2^{24} \times 2^{8} \times \frac{1}{16} \times [2 + 2^{-4} \times 2^{4} + 2^{-8} \times 2^{4} + 2^{-8} \times 2^{8}$
4	$+2^{-12} \times 2^{12} + 2^{-16} \times 2^{12} + 2^{-16} \times 2^{16} + 2^{-20} \times 2^{20} = 2^{n+30.83}$
5	$2 \times 2^{12} \times 2^{52} \times \frac{3}{16} \times [1 + (1-2^{-8}) + \cdots + (1-2^{-8})^{2^{n-25}}]$
ERK	$10 \times 2^{128} \times (1 - 2^{-8})^{2^{n-25}}$

*ERK: Examining the Remaining Keys by using one pair of plain-text/cipher-text.

pairs. Taking 2^n structure, there will be 2^{n+24} plain-texts and 2^{n+47} pairs.

(2) Guess $WK[3, 7, 8, 9, 12, 13] = (k_0 \oplus k_1)[3, 7, 8, 9, 12, 13]$ and calculate Z_1. Afterwards, hold only pairs that have $\Delta Z_1[8] = \Delta Z_1[9] = \Delta Z_1[10]$ as well as $\Delta Z_1[12] = \Delta Z_1[13] = \Delta Z_1[15]$. Because probability of the event is 2^{-16}, the remaining pairs are about $2^{n+47-16} = 2^{n+31}$.

(3) Guess $k_0[11, 14]$ and compute $Y_2[11, 14]$. Keep only pairs that have same values in $\Delta Y_2[11] = \Delta Y_2[14]$. Hence, after this step $2^{n+31-4} = 2^{n+27}$ pairs exist, on average.

(4) Ask for corresponding cipher-texts for each remaining plain-texts. For round 9 and 10, swap the *MixColumn* and *KeyAdd* operations and consider the equivalent sub-key

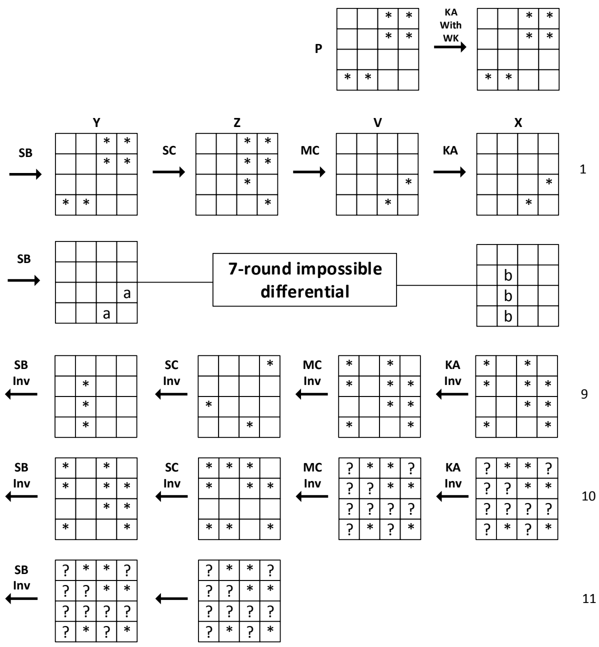


Figure 6. Impossible differential cryptanalysis of 11-round Midori64.

$u_i = MC^{-1}(k_i)$. Compute $MC^{-1}(X_{10})$, excluding *KeyAdd* operation. Consequently, guess $u_1[0,1,3,4,7,8,9,13,15]$ and calculate Z_{10}. Hold only those pairs that have zero differences in positions $(2,5,6,10,11,12,14)$. Hence, the number of remaining pairs is about $2^{n+27-28} = 2^{n-1}$. Afterwards, compare the non-zero differences in first column of X_9 and keep those pairs that have same values for the three non-zero differences. Perform the same procedure for third and forth columns, too. The probability for that to occur is about $2^{-8\times 3} = 2^{-24}$, therefore, the expected number of remaining pairs is $2^{n-1-24} = 2^{n-25}$, averagely. To reduce time complexity we use early-abort technique in this step. There are 2^{n+24} plain-texts in the first part of this section and in stage 2 and 3, 24 and 8 bits of the master key are guessed, respectively. The time complexity of this step is $2^{n+24} \times 2^{24} \times 2^{8}$. The second part contains the dominant term of time complexity and using early-abort is so beneficial in this part. At first, guess $u_1[0,7]$ and calculate $X_9[0,1]$. If $\Delta X_9[0]$ and $\Delta X_9[1]$ are the same, guess $u_1[9]$ and compute $X_9[3]$. The probability of $\Delta X_9[0] = \Delta X_9[1]$ is 2^{-4} and with the same probability, the value of $X_{10}[3]$ can be found. Guess $u_1[1]$ and $u_1[8]$ and calculate $X_9[10]$ if $\Delta X_9[0]$, $\Delta X_9[1]$ and $\Delta X_9[3]$ are the same and then compute $X_9[9]$. Hence, $X_9[10]$ and $X_9[9]$ are computed with probability of 2^{-8}. Guess $u_1[15]$ and calculate $X_9[8]$ whenever $\Delta X_9[10]$ and $\Delta X_9[9]$ are equal. The nibble $X_9[8]$ is calculated in case that $\Delta X_9[10]$ and $\Delta X_9[9]$ are equal. Moreover, $\Delta X_9[0]$, $\Delta X_9[1]$ and $\Delta X_9[3]$ must be equal, so the probability of calculating $X_9[8]$ is 2^{-12}. Afterwards, guess $u_1[3,4]$ and calculate $X_9[14,15]$ and if $\Delta X_9[14]$ and $\Delta X_9[15]$ have same values, guess $u_1[13]$ and calculate $X_9[13]$.

(5) For each remaining pairs, guess $u_0[2,11,12]$ and compute $Z_9[2,11,12]$ and $X_8[5,6,7]$. Find those pairs that the values of $\Delta X_9[5]$, $\Delta X_8[6]$ and $\Delta X_8[7]$ are equal. If at least one pair conforms to the condition, determine master-key from corresponding sub-key and discard the master-key.

Complexity analysis

In step 2, 3, 4 and 5 we guessed 24, 8, 36, 12 key bits, respectively. Hence, the expected number of the remaining wrong keys is $N = 2^{80} \times (1-2^{-8})^{2^{n-25}}$. If we want to have small time complexity, we set $n = 37.87$. Thus, the data complexity is equal to $2^{61.87}$ chosen plain-texts. Moreover, the time complexity is about $2^{90.63}$ 11-round encryptions and memory complexity is 2^{41} 64-bit blocks. Table 5 summarizes the time complexity of each step in the attack.

4.3 Impossible Differential Cryptanalysis of 12-round Midori64

In this subsection we describe the impossible differential attack mounted on 12-round Midori64. The impossible differential characteristic that we use in this attack is as the same as Section 4.2. Figure 7 shows overview of the attack.

(1) Consider a structure of 2^{24} data in state V_1

Table 5. Time Complexity of 11-Round Attack on Midori64

Step	Time Complexity in One-Round Encryption
2	$2^{n+24} \times 2^{24} \times \frac{6}{16} = 2^{n+46.58}$
3	$2^{n+24} \times 2^{24} \times 2^{8} \times \frac{2}{16} =$ $2^{n+53} 2^{n+24} \times 2^{24} \times 2^{8} + 2 \times 2^{n-1} \times 2^{24} \times 2^{8} \times 2^{8} \times \frac{1}{16} \times$
4	$[2 + 2^{-4} \times 2^{4} + 2^{-8} \times 2^{8} + 2^{-8} \times 2^{12} + 2^{-12} \times 2^{16} + 2^{-16} \times 2^{20} + 2^{-16} \times 2^{24} + 2^{-20} \times 2^{28}] = 2^{n+56} + 2^{n+45.13}$
5	$2 \times 2^{12} \times 2^{68} \times \frac{3}{16} \times [1 + (1-2^{-8}) + \cdots + (1-2^{-8})^{2^{n-25}}]$
ERK	$11 \times 2^{128} \times (1-2^{-8})^{2^{n-25}}$

*ERK: Examining the Remaining Keys by using one pair of plain-text/cipher-text.

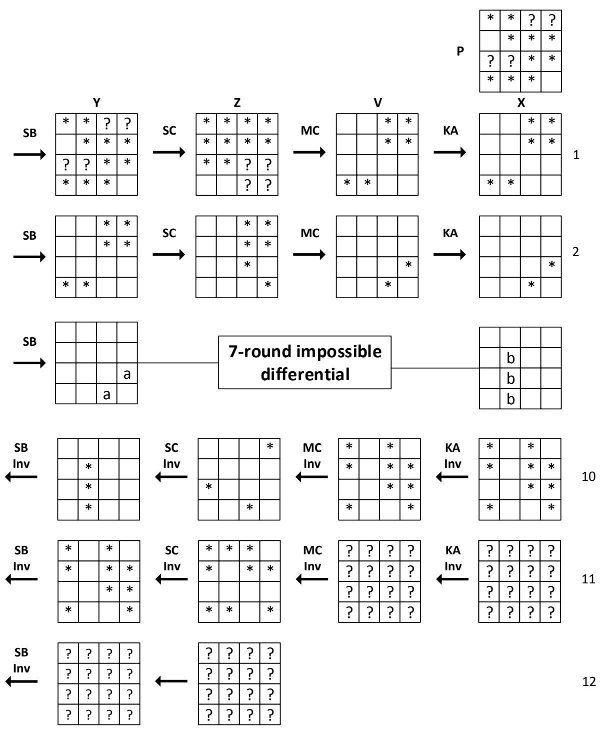


Figure 7. Impossible differential cryptanalysis of 12-round Midori64.

which have different value in (3, 7, 8, 9, 12, 13) positions and have fixed values in other nibbles. Each structure consists of about $2^{24} \times 2^{23} = 2^{47}$ pairs. Taking 2^n structure, there will be 2^{n+24} data and 2^{n+47} pairs.

(2) Find P using V_1 to reach aforementioned plain-texts.

(3) Guess $k_0[3,7,8,9,12,13]$ and compute Z_2. Keep only pairs that the value of $\Delta Z_2[8] = \Delta Z_2[9] = \Delta Z_2[10]$ and $\Delta Z_2[12] = \Delta Z_2[13] = \Delta Z_2[15]$ are equal. Thus, the remaining pairs are about $2^{n+47-16} = 2^{n+31}$.

(4) Guess $k_1[11,14]$ and calculate $Y_3[11,14]$. Hold only pairs that $\Delta Y_3[11] = \Delta Y_3[14]$, leading to $2^{n+31-4} = 2^{n+27}$ pairs, on average.

(5) Ask for corresponding cipher-text for remaining plain-text and find X_{11} and $Z_{11} = MC^{-1}(X_{11})$. Keep only pairs that have zero value in $\Delta Z_{11}[2,5,6,10,11,12,14]$. The probability of such event is 2^{-28}; thus, the number of remaining pairs is about $2^{n+27-28} = 2^{n-1}$.

(6) Guess $u_0[0,1,3,4,7,8,13,15]$, and compute X_{10} (note that $u_0[9] = u_0[8] \oplus k_0[8] \oplus k_0[9]$). Find only pairs that satisfy $\Delta X_{10}[0] = \Delta X_{10}[1] = \Delta X_{10}[3]$, $\Delta X_{10}[8] = \Delta X_{10}[9] = \Delta X_{10}[10]$ and $\Delta X_{10}[13] = \Delta X_{10}[14] = \Delta X_{10}[15]$. Hence the number of remaining pairs is about 2^{n-25}. In this step, we use early-abort technique to reduce time complexity. Details of using this technique is as follows. Guess $u_0[1,8]$ and calculate $X_{10}[9,10]$. If $\Delta X_{10}[10]$ and $\Delta X_{10}[9]$ are identical, guess $u_0[15]$ and then compute $X_{10}[8]$. In the case that $\Delta X_{10}[10]$, $\Delta X_{10}[9]$ and $\Delta X_{10}[8]$ are the same, guess $u_0[0]$ and compute $X_{10}[0]$. Considering the known $k_0[8]$ and $k_0[9]$ which are guessed in stage 3 and the known $u_0[8]$, calculate $u_0[9]$ and then $X_{10}[3]$. Guess $u_0[7]$ and then find $X_{10}[1]$ if $\Delta X_{10}[0]$ and $\Delta X_{10}[3]$ are equal. Afterwards, guess $u_0[3,4]$ and compute $X_{10}[14,15]$. If $\Delta X_{10}[14]$ and $\Delta X_{10}[15]$ are the same, guess $u_0[13]$ and calculate $X_{10}[13]$.

(7) For desired remaining pairs, guess $u_1[2,11,12]$ and compute X_9. If the condition $\Delta X_9[5] = \Delta X_9[6] = \Delta X_9[7]$ is satisfied, calculate the master-key from the corresponding sub-key and discard the master-key.

Complexity analysis

In step 3, 4, 6 and 7 we guessed 24, 8, 32, 12 bits of key, respectively. Hence, the expected number of the remaining wrong keys is $N = 2^{76} \times (1-2^{-8})^{2^{n-25}}$. We set $n = 37.87$ to reach small time complexity, thus data complexity is $2^{61.87}$ chosen plain-texts. The total time complexity is about $2^{90.51}$ 12-round encryptions, requiring 2^{41} 64-bit blocks of memory.

Table 6 summarizes the procedure of the attack.

Table 6. Time Complexity of 12-Round Attack on Midori64

Step	Time Complexity in One Round Encryption
2	2^{n+24}
3	$2^{n+24} \times 2^{24} \times \frac{6}{16} = 2^{n+46.58}$
4	$2^{n+24} \times 2^{24} \times 2^8 \times \frac{2}{16} = 2^{n+53}$
5	$2^{n+24} \times 2^{24} \times 2^8 =$ $2^{n+56} 2 \times 2^{n-1} \times 2^{24} \times 2^8 \times 2^8 \times \frac{1}{16} \times$
6	$[2 + 2^{-4} \times 2^4 + 2^{-8} \times 2^8 + 2^{-8} \times 2^8 + 2^{-12} \times 2^{12} + 2^{-16} \times 2^{16} + 2^{-16} \times 2^{20} + 2^{-20} \times 2^{24}] = 2^{n+41.29}$
7	$2 \times 2^{12} \times 2^{64} \times \frac{3}{16} \times [1+(1-2^{-8})+\cdots+(1-2^{-8})^{2^{n-25}}]$
ERK	$12 \times 2^{128} \times (1-2^{-8})^{2^{n-25}}$

*ERK: Examining the Remaining Keys by using one pair of plain-text/cipher-text.

5 Conclusion

In this paper, we presented two new 7-round impossible differential paths of Midori64 and Midori128. Based on these paths, we mounted an attack to 10-round Midori64, covering pre and post whitening keys, with data complexity of $2^{64.97}$ chosen plain-texts and time complexity of $2^{87.71}$ 10-round encryptions. Next, we showed 11-round attack, containing pre whitening key, with time complexity of $2^{90.63}$ 11-round encryptions and data complexity of $2^{61.87}$ chosen plain-texts. Finally, we mounted impossible differential attack on 12-round Midori64 which requires $2^{61.87}$ chosen plain-texts and with $2^{90.51}$ time complexity of 12-round encryptions.

Acknowledgment

The authors would like to thank INSF and Professor Farokh Marvasti for their partial support.

References

[1] Aein Rezaei Shahmirzadi, Seyyed Arash Azimi, Mahmoud Salmasizadeh, Javad Mohajeri, and Mohammad Reza Aref. Impossible differential cryptanalysis of reduced-round midori64 block cipher. In *Information Security and Cryptology (ISCISC), 2017 14th International ISC Conference on*. IEEE, 2017.

[2] Andrey Bogdanov, Lars R Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew JB Robshaw, Yannick Seurin, and Charlotte Vikkelsoe. Present: An ultra-lightweight block cipher. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 450–466. Springer, 2007.

[3] Lars Knudsen, Gregor Leander, Axel Poschmann, and Matthew JB Robshaw. Printcipher: a block

cipher for ic-printing. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 16–32. Springer, 2010.

[4] Tomoyasu Suzaki, Kazuhiko Minematsu, Sumio Morioka, and Eita Kobayashi. Twine: A lightweight, versatile block cipher. In *ECRYPT Workshop on Lightweight Cryptography*, volume 2011, 2011.

[5] Julia Borghoff, Anne Canteaut, Tim Güneysu, Elif Bilge Kavun, Miroslav Knezevic, Lars R Knudsen, Gregor Leander, Ventzislav Nikov, Christof Paar, Christian Rechberger, et al. Prince–a low-latency block cipher for pervasive computing applications. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 208–225. Springer, 2012.

[6] Wenling Wu and Lei Zhang. Lblock: a lightweight block cipher. In *International Conference on Applied Cryptography and Network Security*, pages 327–344. Springer, 2011.

[7] Taizo Shirai, Kyoji Shibutani, Toru Akishita, Shiho Moriai, and Tetsu Iwata. The 128-bit blockcipher clefia. In *FSE*, volume 4593, pages 181–195. Springer, 2007.

[8] Christophe De Canniere, Orr Dunkelman, and Miroslav Knežević. Katan and ktantanâĂŤa family of small and efficient hardware-oriented block ciphers. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 272–288. Springer, 2009.

[9] Subhadeep Banik, Andrey Bogdanov, Takanori Isobe, Kyoji Shibutani, Harunaga Hiwatari, Toru Akishita, and Francesco Regazzoni. Midori: a block cipher for low energy. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 411–436. Springer, 2015.

[10] Jian Guo, Jérémy Jean, Ivica Nikolic, Kexin Qiao, Yu Sasaki, and Siang Meng Sim. Invariant subspace attack against full midori64. *IACR Cryptology ePrint Archive*, 2015:1189, 2015.

[11] Yosuke Todo, Gregor Leander, and Yu Sasaki. Nonlinear invariant attack: Practical attack on full scream, i scream, and midori 64. In *Advances in Cryptology–ASIACRYPT 2016: 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part II 22*, pages 3–33. Springer, 2016.

[12] Xiaoyang Dong and Yanzhao Shen. Cryptanalysis of reduced-round midori64 block cipher. Technical report, Cryptology ePrint Archive, Report 2016/676, 2016.

[13] David Gérault and Pascal Lafourcade. Related-key cryptanalysis of midori. In *Progress in Cryptology–INDOCRYPT 2016: 17th International Conference on Cryptology in India, Kolkata, India, December 11-14, 2016, Proceedings 17*, pages 287–304. Springer, 2016.

[14] Zhan Chen and Xiaoyun Wang. Impossible differential cryptanalysis of midori. *IACR Cryptology ePrint Archive*, 2016:535, 2016.

[15] Li Lin and Wenling Wu. Meet-in-the-middle attacks on reduced-round midori64. *IACR Transactions on Symmetric Cryptology*, 2017(1):215–239, 2017.

[16] Seyyed Arash Azimi, Zahra Ahmadian, Javad Mohajeri, and Mohammad Reza Aref. Impossible differential cryptanalysis of piccolo lightweight block cipher. In *Information Security and Cryptology (ISCISC), 2014 11th International ISC Conference on*, pages 89–94. IEEE, 2014.

[17] Christina Boura, María Naya-Plasencia, and Valentin Suder. Scrutinizing and improving impossible differential attacks: Applications to clefia, camellia, lblock and simon. *ASIACRYPT (1)*, 8873:179–199, 2014.

[18] Masroor Hajari, Seyyed Arash Azimi, Poorya Aghdaie, Mahmoud Salmasizadeh, and Mohammad Reza Aref. Impossible differential cryptanalysis of reduced-round tea and xtea. In *Information Security and Cryptology (ISCISC), 2015 12th International Iranian Society of Cryptology Conference on*, pages 58–63. IEEE, 2015.

[19] Hamid Mala, Mohammad Dakhilalian, and Mohsen Shakiba. Impossible differential attacks on 13-round clefia-128. *Journal of Computer Science and Technology*, 26(4):744–750, 2011.

[20] Seyyed Arash Azimi, Siavash Ahmadi, Zahra Ahmadian, Javad Mohajeri, and Mohammad Reza Aref. Improved impossible differential and biclique cryptanalysis of hight. *International Journal of Communication Systems*, 31(1), 2018.

[21] Eli Biham and Adi Shamir. Differential cryptanalysis of des-like cryptosystems. In *Advances in Cryptology-CRYPTO*, volume 90, pages 2–21. Springer, 1991.

[22] Lars R Knudsen. Deal a 128-bit cipher. Technical report, Technical Report, Department of Informatics, University of Bergen, Norway, 1998.

[23] Eli Biham, Alex Biryukov, and Adi Shamir. Miss in the middle attacks on idea and khufu. In *FSE*, volume 1636, pages 124–138. Springer, 1999.

[24] Eli Biham, Alex Biryukov, and Adi Shamir. Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 12–23. Springer, 1999.

[25] Joan Daemen and Vincent Rijmen. *The design of Rijndael: AES-the advanced encryption standard.*

Springer Science & Business Media, 2013.

[26] Chae Hoon Lim. Crypton: A new 128-bit block cipher. *NIsT AEs Proposal*, 1998.

[27] Kazumaro Aoki, Tetsuya Ichikawa, Masayuki Kanda, Mitsuru Matsui, Shiho Moriai, Junko Nakajima, and Toshio Tokita. Camellia: A 128-bit block cipher suitable for multiple platforms-design and analysis. In *Selected Areas in Cryptography*, volume 2012, pages 39–56. Springer, 2000.

[28] Daniel Dinu, Léo Perrin, Aleksei Udovenko, Vesselin Velichkov, Johann Großschädl, and Alex Biryukov. Design strategies for arx with provable bounds: Sparx and lax. In *Advances in Cryptology–ASIACRYPT 2016: 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part I 22*, pages 484–513. Springer, 2016.

[29] Jiqiang Lu, Orr Dunkelman, Nathan Keller, and Jongsung Kim. New impossible differential attacks on aes. In *Indocrypt*, volume 8, pages 279–293. Springer, 2008.

[30] Jung Hee Cheon, MunJu Kim, Kwangjo Kim, Lee Jung-Yeun, and SungWoo Kang. Improved impossible differential cryptanalysis of rijndael and crypton. In *International Conference on Information Security and Cryptology*, pages 39–49. Springer, 2001.

[31] Céline Blondeau. Impossible differential attack on 13-round camellia-192. *Information Processing Letters*, 115(9):660–666, 2015.

[32] Ahmed Abdelkhalek, Mohamed Tolba, and Amr M Youssef. Impossible differential attack on reduced round sparx-64/128. In *AFRICACRYPT*, pages 135–146, 2017.

[33] Yu Sasaki and Yosuke Todo. New impossible differential search tool from design and cryptanalysis aspects. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 185–215. Springer, 2017.

[34] Charles Bouillaguet, Orr Dunkelman, Pierre-Alain Fouque, and Gaëtan Leurent. New insights on impossible differential cryptanalysis. In *Selected Areas in Cryptography*, volume 7118, pages 243–259. Springer, 2011.

[35] Jongsung Kim, Seokhie Hong, and Jongin Lim. Impossible differential cryptanalysis using matrix method. *Discrete Mathematics*, 310(5):988–1002, 2010.

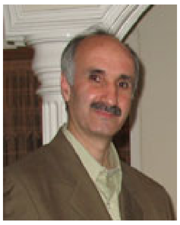
[36] Jongsung Kim, Seokhie Hong, Jaechul Sung, Sangjin Lee, Jongin Lim, and Soohak Sung. Impossible differential cryptanalysis for block cipher structures. In *International Conference on Cryptology in India*, pages 82–96. Springer, 2003.

[37] Jiqiang Lu, Jongsung Kim, Nathan Keller, and Orr Dunkelman. Improving the efficiency of impossible differential cryptanalysis of reduced camellia and misty1. In *CT-RSA*, volume 4964, pages 370–386. Springer, 2008.

Aein Rezaei Shahmirzadi received his B.S. in electrical engineering from Sharif University of Technology, Tehran, Iran, in 2016. He is currently working toward his M.S. degree at electrical engineering department of Sharif University of Technology. His research interests include machine learning, signal processing and cryptography.

Arash Azimi is a Ph.D. candidate in communication systems at Sharif University of Technology, Tehran, Iran. He previously received the B.S. and M.S. degrees in electrical engineering from Sharif University of Technology, Tehran, Iran. His current research interests include symmetric cryptography, mostly focusing on cryptanalysis.

Mahmoud Salmasizadeh received the B.S. and M.S. degrees in electrical engineering from Sharif University of Technology, Tehran, Iran, in 1972 and 1989, respectively. He also received the Ph.D. degree in information technology from Queensland University of Technology, Australia, in 1997. Currently, he is an associate professor in the Electronics Research Institute and adjunct associate professor in the Electrical Engineering Department, Sharif University of Technology. His research interests include design and cryptanalysis of cryptographic algorithms and protocols, e-commerce security, and information theoretic secrecy. He is a founding member of Iranian Society of Cryptology.



Javad Mohajeri received the B.S. degree from Isfahan University in 1986 and the M.S. degree from Sharif University of Technology in 1989, both in mathematics. He has been a faculty member at Electronics Research Institute of Sharif University of Technology since 1990. His research interests include cryptography and data security. He is the author/co-author of over 60 research articles in refereed Journals/ Conferences.

Mohammad Reza Aref was born in city of Yazd in Iran in 1951. He received his B.S. in 1975 from University of Tehran, his M.S. and Ph.D. in 1976 and 1980, respectively, from Stanford University, all in Electrical Engineering. He returned to Iran in 1980 and was actively engaged in academic and political affairs. He was a faculty member of Isfahan University of Technology from 1982 to 1995. He has been a Professor of Electrical Engineering at Sharif University of Technology since 1995 and has published more than 260 technical research papers in communication and information theory and cryptography in international journals and conference proceedings. His current research interests include areas of communication theory, information theory, and cryptography with special emphasis on network information theory and security for multiuser wireless communications. During his academic activities, he has been involved concomitantly in political positions. First Vice President of I. R. Iran, Vice President of I. R. Iran and Head of Management and Planning Organization, Minister of ICT of I. R. Iran, and Chancellor of University of Tehran, are the most recent ones.