Differential Attacks on LILLIPUT cipher

Valérie Nachef[1], Nicolas Marrière[1], and Emmanuel Volte[1]

Department of Mathematics, University of Cergy-Pontoise, CNRS UMR 8088
2 avenue Adolphe Chauvin, 95011 Cergy-Pontoise Cedex, France
valerie.nachef@u-cergy.fr
nicolas.marriere@u-cergy.fr
emmanuel.volte@u-cergy.fr

Abstract. In SAC 2013, Berger et al. defined Extended Generalized Feistel Networks (EGFN) and analyzed their security. Later, they proposed a cipher based on this structure: *LILLIPUT*. Impossible differential attacks and integral attacks have been mounted on *LILLIPUT*. We propose a tool which has found some classical, impossible and improbable differential attacks by using the variance method. It has highlighted unusual differential conditions which lead to efficient attacks by the complexity. Moreover, it is the first time we apply the generic variance method to a concrete cipher.

Key words: Differential cryptanalysis, Improbable differential cryptanalysis, Automated research of attacks

1 Introduction

Lightweight cryptography has become an important field of research with the development of IoT. As a solution, a lot of symmetric block ciphers have been built. Some of them are SPN ciphers like SERPENT [5], PRESENT [9] or more recently SKINNY [2]. Others are Feistel ciphers like SIMON [1], CLEFIA [18] or PICCOLO [17]. In this context, a new variant of generalized Feistel network has been designed: the Extended Generalized Feistel Network [4] (EGFN). It is based on a matrix representation and provides an efficient diffusion. In comparison to the generalized Feistel networks, the distinctive feature in the EGFN is a linear layer after the confusion step. Moreover, an efficient differential analysis method remains unknown [15] because of this linear layer. A cipher based on the EGFN structure called *LILLIPUT* [3] has been designed. It is a 30 rounds block cipher. Several kinds of attacks on *LILLIPUT* have been provided as shown in Table 1.

Differential attacks [7] consist in putting a specific difference in inputs and looking how it propagates through the cipher into the outputs in order to highlight a bias. Differential cryptanalysis is an efficient statistical attack and some attacks are derived from it: truncated differential ones [11], boomerang ones [22] or impossible differential ones [6] for example. A differential analysis based on the variance method [13] has been made on the EGFN [12]. In this article, we have applied this method to *LILLIPUT*.

Our contribution. In this paper, we provide some differential cryptanalysis attacks on *LILLIPUT*. Indeed, we provide some differential distinguishers. These attacks are

Table 1. Best Attacks on *LILLIPUT*.

Variety	Distinguisher	Key recovery	Source
Impossible differential	9 rounds	N/A	[16]
Division property	13 rounds	17 rounds	[15]
Differential	8 rounds	12 rounds	Section 4

NCPA (Non-Adaptive Chosen Plaintext Attack) ones. These are based on the variance method [13] that was already used on the EGFN and on some generalized Feistel network [14, 21]. For the first time, we apply this generic method to a concrete cipher. These differential attacks do not rely on the key schedule, the structure of *LILLIPUT* is the only way used. One can see in [15] that there are 15 active sboxes for *LILLIPUT* reduced to 8 rounds. The involved sboxes work on 4-bits words. Since the differential probability of an active sbox is at most 2^{-3}, then the differential probability is at most 2^{-45}. In this paper, we will see an implemented differential attack with complexity of 2^{-25}. This is why this method is interesting. Moreover, we have made a tool in Python to process an automated research of differential attacks. There are generic tools devoted to different kinds of attacks: meet-in-the-middle and impossible differential attacks in [10], or only for impossible differential attacks in [16], in [23] or in [24] for example. Contrary to others generic tools, our program is designed to apply the variance method to a concrete cipher. It can be used on some block ciphers and allows to get differential attacks, impossible differential attacks and improbable differential attacks. Indeed, we have found empirically some improbable differential attacks [20, 19] and we provide explanations of how it works. Improbable differential cryptanalysis is a statistical cryptanalytic technique for which some attacks have been invalidated [8] when built from an impossible distinguisher. In the theory, an improbable differential attack is like a classical differential attack but the expected differences occur less for a permutation generated by the studied cipher than for a random permutation. In this paper, the attacks we describe work in practice and we provide simulations of them.

This paper is organized as follow: In Section 2, we will describe *LILLIPUT*. Then in Section 3 we will detail the general structure of our attacks and describe the tool that allows to find attacks. Section 4 is devoted to the presentation of distinguishing attacks up to 8 rounds. Conclusion is given in Section 5.

2 LILLIPUT

The input is denoted by 16 nibbles of 4-bits: $I = [I_{16}, I_{15}, \cdots, I_1]$. Similarly, the output is denoted by: $S = [S_{16}, S_{15}, \cdots, S_1]$. We describe one round of *LILLIPUT* in the figure 1.

We can see there are three steps in a round:

- *NonLinearLayer* step with the sbox. There is only one 4-bits sbox in *LILLIPUT* and it is descibred in the table 2.
- *LinearLayer* step: this is a step with some xor operations between the left side branches and the right side.

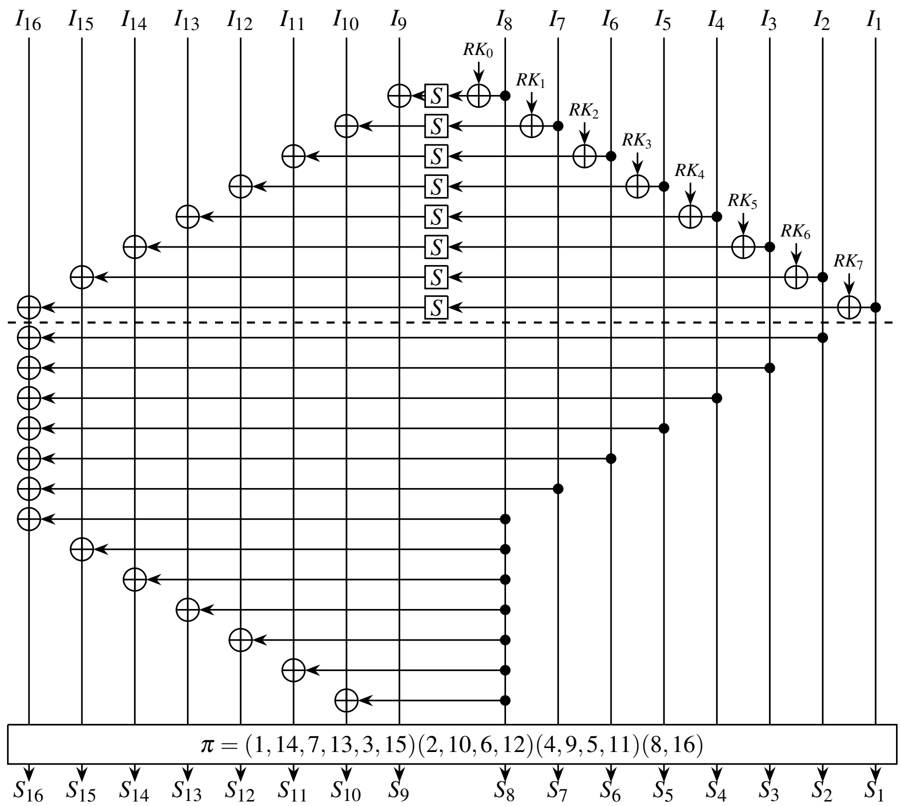

Fig. 1. One round of *LILLIPUT*.

– *PermutationLayer*: there is a permutation step and we have described the modification of the different branches in the table 3.

One can notice that there are two sides and the left side branches go to the right side through the permutation step and vice versa.

Table 2. Sbox of *LILLIPUT*.

Input branch	0	1	2	3	4	5	6	7	8	9	*A*	*B*	*C*	*D*	*E*	*F*
Ouput branch	4	8	7	1	9	3	2	*E*	0	*B*	6	*F*	*A*	5	*D*	*C*

LILLIPUT is an instance of Extended Generalized Feistel Network, a generic family of Feistel schemes. Because of the *LinearLayer*, there are no efficient known methods to make a differential study of this scheme.

Table 3. Permutation of *LILLIPUT*.

Input	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Output	14	10	15	9	11	12	13	16	5	6	4	2	3	7	1	8

As previously said, differential attacks on EGFN have already been proposed. These attacks are based on the variance method [13] that we will use on *LILLIPUT* as well. However, we can not use the same differential trails or use the same kind of relations between inputs and outputs because in *LILLIPUT* the sbox is a bijection. In order to find a solution, we have made a tool in Python which has tested many kinds of differential relations and it has highlighted a specific and unusual sort of conditions which are not intuitive.

3 Structure of the attacks

3.1 Variance method

Our attacks are based on variance method [13]. With this method, we can make a further analysis than a classical differential attack. The aim of the attack is to distinguish a permutation obtained with *LILLIPUT* from a random permutation. Just like the authors of the variance method, we will generate a lot of pairs of messages and count how many of them satisfy specific differential relations between inputs and outputs. The number of such pairs is denoted by $\mathcal{N}_{perm}$ for a random permutation and by $\mathcal{N}_L$ for a *LILLIPUT* permutation.

Then, the attack is a success if $\mathcal{N}_{perm}$ is significantly different from $\mathcal{N}_L$. If it is smaller, we obtain an impossible or an improbable differential attack and if it is greater, we have a classical differential one. But if $\mathcal{N}_L$ and $\mathcal{N}_{perm}$ have the same order, then the attack can be successful thanks to the expectation and standard deviation functions if $|\mathbb{E}(\mathcal{N}_L) - \mathbb{E}(\mathcal{N}_{perm})| > \max(\sigma(\mathcal{N}_{perm}), \sigma(\mathcal{N}_L))$, where $\mathbb{E}$ stands for the expectation function and σ for the standard deviation function. In that case, the attacks work thanks to the Chebychev formula, which states that for any random variable X, and any $\alpha > 0$, we have $\mathbb{P}\left(|X - \mathbb{E}(X)| \geq \alpha\sigma(x)\right) \leq \frac{1}{\alpha^2}$. Using this formula, it is then possible to construct a prediction interval for $\mathcal{N}_L$ for example, in which future computations will fall, with a good probability. It is important to notice that for our attacks, it is enough to compute $\mathbb{E}(\mathcal{N}_{perm})$, $\mathbb{E}(\mathcal{N}_L)$ and $\sigma(\mathcal{N}_{perm})$. For more details about the variance method see [13], Chapter 5 for example.

Moreover, for all attacks we will see, the condition on the outputs is an equality on 4 bits. So, it is easy to check that if m is the number of messages for a given attack, then for a random permutation: $\mathbb{E}(\mathcal{N}_{perm}) \simeq \frac{m\cdot(m-1)}{2} \times \frac{1}{2^4}$ and $\sigma(\mathcal{N}_{perm}) \simeq \sqrt{\mathbb{E}(\mathcal{N}_{perm})}$.

3.2 Conditions on the inputs and the outputs

There are 16 branches in *LILLIPUT*. Our attacks are differential ones, so we look for differential trails. Due to the structure of *LILLIPUT*, we look for attacks by putting conditions to the left side $[I_{16}, \cdots, I_9]$ of the inputs and looking some conditions on the left side $[S_{16},\cdots,S_9]$ of the outputs. Indeed, one can check that, if we found an interesting distinguisher which uses the right side of the output, it leads to a distinguisher which uses the left side of the output and reaches one more round. It is because in a round the right side goes to the left side with probability 1 without changes.

We have found by hand distinguishers up to 4 rounds and for more rounds with the tool. Most attacks are based on a common structure. Each pair (m_1, m_2) of messages that we study has to verify that: m_1 and m_2 are equal on all branches but some on the left side. Moreover, on the branches involved, the non-zero differences have to be equal. For example, this condition on branch number 9 will be written $I_9(m_1) \oplus I_9(m_2) = \Delta$ or if more simply $\Delta I_9 = \Delta$.

On the outputs, if $c_1 = LILLIPUT(m_1)$ and $c_2 = LILLIPUT(m_2)$ we will look at the xor between some branches of $c = c_1 \oplus c_2$. For example, if we are interested in the branches S_{12} and S_{10}, we will compute $S_{12} \oplus S_{10}$ on c and it is denoted by $\Delta S_{12} \oplus \Delta S_{10}$. One can notice that if one is interested in only one branch, it leads to a classical differential attack.

3.3 Complexity

In our differential attacks we use structures of messages. Let (m_1, m_2) be a pair of messages. As we have said earlier, there are 2 properties the pairs have to follow. First, m_1 and m_2 are equal on all branches but some on the left side. Then, for the non zero branches of $m_1 \oplus m_2$, the difference has to be the same. Thus, a structure is based on a message m that is randomly chosen. As we want the same difference on some branches, it leads to 15 more messages. Indeed, the non zero difference can be $\Delta \in [1 \cdots 15]$ because branches have 4 bits. So, a structure has 16 messages, and it leads to $16 \times 15/2 = 120$ pairs.

For example, if we are interested in the branches I_{10} and I_{13}, a pair will be (m_1, m_2) such that: $m_1 \oplus m_2 = [0,0,0,\Delta,0,0,\Delta,0,0,0,0,0,0,0,0,0]$. There are exactly $2^{4\times 14}$ of such structures.

The main drawback of our attacks is the data complexity. Indeed for a given attack which requires 2^7 messages, the number of pairs is $\frac{2^7\times(2^7-1)}{2} = 8{,}128$. With our kinds of attacks, because we need the same Δ difference on several branches, we need 68 structures of 120 pairs ($68 \times 120 = 8{,}160$ pairs) and it corresponds to $68 \times 16 = 1{,}088$ messages instead of 2^7. But, thanks to these new conditions, one can see special relations between internal variables which can be used to build a differential attack.

3.4 Automated research of attacks

To extend this kind of attacks, we have implemented a tool[1] in Python to process an exhaustive research of such conditions. We describe it in the algorithm 1.

In order to optimise this algorithm, we test on a small number of samples and if we found an interesting result, then we test again in a more meaningful number of samples. It appears that the most efficient attacks are based on having 2 branches involved on the

[1] Our tool is available on the Internet at this anonymous link: github.com/anon159753/Lilliput_analysis.

Algorithm 1 Automated research of attacks

for all inputCondition=Combination of branches in the left side of inputs: **do**
  Generate a sample of pairs which verify the condition on the input: Equal on all branches but the inputCondition.
  for all outputCondition=Combination of branches in the left side of outputs: **do**
    Count how many pairs verify the outputCondition: the xor between some branches of the difference of the outputs equals to 0.
    if this result is significantly different than the one expected for a random permutation. **then**
      We have found a distinguisher.
    end if
  end for
end for

inputs and 2 branches involved on the ouput. We detail the best attacks we have found in Section 4.

4 Distinguishing attacks

In this Section, we will describe the different distinguishers we have found by hand or thanks to the tool. We have made simulations of these attacks. Input is denoted by: $I_{16},\cdots,I_1$. After the first *NonLinearLayer* and *LinearLayer* steps and before the permutation, the output is: $X_8^1,X_7^1,X_6^1,X_5^1,X_4^1,X_3^1,X_2^1,X_1^1,I_8,I_7,I_6,I_5,I_4,I_3,I_2,I_1$. Here $X_1^1,\ldots,X_8^1$ denote the internal variable that appear at round 1. More generally, X_j^i, $1 \leq j \leq 16$ represent the internal variable that are introduced at round i. In the sequel, to simplify the notation, we always denote by f the round functions. But the even though we always use the same bijective sbox, since the entry is xored with a sub-key, for the same round we note that $f(X_j^i) = f(X_k^i)$ does not mean that $X_j^i = X_k^i$.

4.1 First rounds

In the first rounds, we can mount differential attacks with probability 1 on *LILLIPUT* with only 1 or 2 messages. So let (m_1,m_2) be a couple of messages. We will note $c_1 = LILLIPUT(m_1)$, $c_2 = LILLIPUT(m_2)$ and $c = c_1 \oplus c_2$.

Attack on one round. After one round, the output is given by:
$[I_8,I_3,I_1,I_7,I_6,I_5,I_2,I_4,X_8^1,X_6^1,X_2^1,X_1^1,X_3^1,X_5^1,X_4^1,X_7^1]$ with

$$\begin{aligned}
X_1^1 &= I_9 \oplus f(I_8),\\
X_2^1 &= I_{10} \oplus I_8 \oplus f(I_7),\\
X_3^1 &= I_{11} \oplus I_8 \oplus f(I_6),\\
X_4^1 &= I_{12} \oplus I_8 \oplus f(I_5),\\
X_5^1 &= I_{13} \oplus I_8 \oplus f(I_4),\\
X_6^1 &= I_{14} \oplus I_8 \oplus f(I_3),
\end{aligned}$$

$$X_7^1 = I_{15} \oplus I_8 \oplus f(I_2),$$
$$X_8^1 = I_{16} \oplus I_8 \oplus I_2 \oplus I_3 \oplus I_4 \oplus I_5 \oplus I_6 \oplus I_7 \oplus f(I_1).$$

So there is an attack with one message: one has to encrypt one message and check if S_{16} is equal to I_8. This is done with probability 1 for *LILLIPUT* and with probability $\frac{1}{2^4}$ for a random permutation because it is an equality on 4 bits.

Attack on two rounds. After two rounds, the output is given by: $[X_8^1, X_5^1, X_7^1, X_6^1, X_2^1, X_1^1, X_4^1, X_3^1, X_8^2, X_6^2, X_2^2, X_1^2, X_3^2, X_5^2, X_4^2, X_7^2]$ with

$$X_1^2 = I_4 \oplus f(X_8^1),$$
$$X_2^2 = I_2 \oplus X_8^1 \oplus f(X_6^1),$$
$$X_3^2 = I_5 \oplus X_8^1 \oplus f(X_2^1),$$
$$X_4^2 = I_6 \oplus X_8^1 \oplus f(X_1^1),$$
$$X_5^2 = I_7 \oplus X_8^1 \oplus f(X_3^1),$$
$$X_6^2 = I_1 \oplus X_8^1 \oplus f(X_5^1),$$
$$X_7^2 = I_3 \oplus X_8^1 \oplus f(X_4^1),$$
$$X_8^2 = I_8 \oplus X_1^1 \oplus X_2^1 \oplus X_3^1 \oplus X_4^1 \oplus X_5^1 \oplus X_6^1 \oplus X_8^1 \oplus f(X_7^1).$$

So there is an NCPA attack with 2 messages. As input condition, we have $I_8(m_1) = I_8(m_2)$. Then, one has to check if $S_{11}(c) = I_9(m_1) \oplus I_9(m_2)$. This is done with probability 1 for *LILLIPUT* and with probability $\frac{1}{2^4}$ for a random permutation because it is an equality on 4 bits.

Property 1 *After r rounds ($r \geq 3$), the output is:* $[X_8^{r-1}, X_5^{r-1}, X_7^{r-1}, X_6^{r-1}, X_2^{r-1}, X_1^{r-1}, X_4^{r-1}, X_3^{r-1}, X_8^r, X_6^r, X_2^r, X_1^r, X_3^r, X_5^r, X_4^r, X_7^r]$. *We have the following formulas:*

$$X_1^r = X_3^{r-2} \oplus f(X_8^{r-1}),$$
$$X_2^r = X_4^{r-2} \oplus X_8^{r-1} \oplus f(X_6^{r-1}),$$
$$X_3^r = X_1^{r-2} \oplus X_8^{r-1} \oplus f(X_2^{r-1}),$$
$$X_4^r = X_2^{r-2} \oplus X_8^{r-1} \oplus f(X_1^{r-1}),$$
$$X_5^r = X_6^{r-2} \oplus X_8^{r-1} \oplus f(X_3^{r-1}),$$
$$X_6^r = X_7^{r-2} \oplus X_8^{r-1} \oplus f(X_5^{r-1}),$$
$$X_7^r = X_5^{r-2} \oplus X_8^{r-1} \oplus f(X_4^{r-1}),$$
$$X_8^r = X_8^{r-2} \oplus X_8^{r-1} \oplus X_6^{r-1} \oplus X_5^{r-1} \oplus X_4^{r-1} \oplus X_3^{r-1} \oplus X_2^{r-1} \oplus X_1^{r-1} \oplus f(X_7^{r-1}).$$

Attack on three rounds. After three rounds, there is an NCPA attack with 2 messages. Thanks to Property 1, one can see that $S_{11} = X_1^2 = I_4 \oplus f(X_8^1)$. Thus, we put as input conditions: $I_i(m_1) = I_i(m_2)$, $\forall i \in \{1, \cdots, 8, 16\}$. Then, one has to check if $S_{11}(c) = 0$. This is done with probability 1 for *LILLIPUT* and with probability $\frac{1}{2^4}$ for a random permutation because it is an equality on 4 bits.

Attack on four rounds. After four rounds, there is an NCPA attack that needs only 2 messages. As input condition we have $I_i(m_1) \neq I_i(m_2)$ only for $i = 15$. Then, one has to check if $S_{13}(c) \oplus S_9(c) = I_{15}(m_1) \oplus I_{15}(m_2)$. We now show that this is done with probability 1 for *LILLIPUT* and with probability $\frac{1}{2^4}$ for a random permutation because we have an equality on 4 bits.
Here we have: $S_{13} = X_6^3$ and $S_9 = X_3^3$. According to Property 1, we obtain:

$$\begin{aligned} S_{13} \oplus S_9 &= X_3^3 \oplus X_6^3 \\ &= X_1^1 \oplus X_7^1 \oplus f(X_5^2) \oplus f(X_2^2) \\ &= I_9 \oplus f(I_8) \oplus I_{15} \oplus I_8 \oplus f(I_2) \oplus f(I_7 \oplus X_8^1 \oplus f(X_3^1)) \oplus f(I_2 \oplus X_8^1 \oplus f(X_6^1)). \end{aligned}$$

Using the input conditions, we obtain:

$$\Delta S_9 \oplus \Delta S_{13} = \Delta I_{15} \oplus \Delta f(I_7 \oplus X_8^1 \oplus f(X_3^1)) \oplus \Delta f(I_2 \oplus X_8^1 \oplus f(X_6^1)).$$

But, we have:

$$\begin{aligned} X_3^1 &= I_{11} \oplus I_8 \oplus f(I_6) \, \text{and} \, \Delta X_3^1 = 0, \\ X_6^1 &= I_{14} \oplus I_8 \oplus f(I_3) \, \text{and} \, \Delta X_6^1 = 0, \\ X_8^1 &= I_{16} \oplus I_2 \oplus I_3 \oplus I_4 \oplus I_5 \oplus I_6 \oplus I_7 \oplus I_8 \oplus f(I_1) \, \text{and} \, X_8^1 = 0. \end{aligned}$$

since the input conditions are $I_i(m_1) \oplus I_i(m_2) = 0$, $\forall i \in \{1, \cdots, 14, 16\}$. Finally we obtain, $\Delta S_{13} \oplus \Delta S_9 = \Delta I_{15}$ with probability 1.

Attack on five rounds. After five rounds, there is an NCPA attack that needs only 2 messages. As input condition we have $I_i(m_1) \neq I_i(m_2)$ only for $i \in \{9, 10\}$. Moreover, we set $I_9(m_1) \oplus I_9(m_2) = I_{10}(m_1) \oplus I_{10}(m_2)$. Then, one has to check if $S_9(i) \oplus S_9(j) \oplus S_{10}(i) \oplus S_{10}(j) = 0$. This is satisfied with probability $\frac{1}{2^4}$ for a random permutation. We now explain why this is true with probability 1 for a permutation obtained with *LILLIPUT*.
According to Property 1:
$S_9 = X_3^4 = X_1^2 \oplus X_8^3 \oplus f(X_2^3)$ and $S_{10} = X_4^4 = X_2^2 \oplus X_8^3 \oplus f(X_1^3)$.

$$\begin{aligned} X_1^2 &= I_{14} \oplus f(X_8^1), \\ X_2^3 &= X_4^1 \oplus X_8^2 \oplus f(X_6^2), \\ X_2^2 &= I_2 \oplus X_8^1 \oplus f(X_6^1), \\ X_1^3 &= X_3^1 \oplus f(X_8^2). \end{aligned}$$

Using the input conditions, we obtain $\Delta X_8^1 = 0, \Delta X_1^2 = 0, \Delta X_6^1$ and $\Delta X_2^2 = 0$. This gives $\Delta S_9 \oplus \Delta_{10} = \Delta f(X_2^3) \oplus \Delta f(X_1^3)$. Moreover, $\Delta X_3^1 = 0$ and $\Delta X_8^2 = \Delta X_1^1 \oplus \Delta X_2^1 = I_9 \oplus \Delta I_{10} = 0$. This implies that $\Delta f(X_1^3) = 0$. It is easy to check that we also have $\Delta f(X_2^3) = 0$. This shows that we have $\Delta S_9 \oplus \Delta S_{10} = 0$ with probability 1.

We have found 26 of such attacks.[2]

[2] See appendix C.

4.2 Further attacks

As we have said in Section 3, our attacks are based on a specific structure: for each pair we have equalities on all but some branches and this non zero difference is the same on the different branches. So, we will detail for each attack, the input branches involved. Similarly, we have said that the output condition is the xor between some branches of $c = c_1 \oplus c_2$. So, we will precise which output branches are involved. In order to obtain $\mathbb{E}(\mathscr{N}_L)$, we will use the mean value obtained from some samples. Thus, we will also detail the number of samples, the number of pairs for each sample and the results we have obtained.

6 rounds. The tool has found a lot of attacks on 6 rounds.[3] We present here the most efficient of these. With only one structure (so 120 pairs of messages, this corresponds to 2^4 messages since if m is the number of messages, then we have $\frac{m(m-1)}{2}$ pairs of distinct messages) we will see that we can distinguish *LILLIPUT* from a random permutation. The output condition is $\Delta S_9 \oplus \Delta S_{15} = 0$. It is an equality on 4 bits, so for a random permutation, the mean value is expected to be $\mathbb{E}(\mathscr{N}_{perm}) = \frac{m(m-1)}{2 \cdot 2^4} = 7.5$. The results we have obtained are shown in Table 4. We notice that the number of pairs of message satisfying the conditions is 32. This provides a distinguishing attack.

Moreover, this attack is still valid with only 4 messages: the last version of our tool works with structures of messages so the minimal number is 2^4 but, one can reduce this attack to 4 messages. Indeed, the mean value of pairs which satisfy the output condition for a random permutation is then expected to be $\mathbb{E}(\mathscr{N}_{perm}) = 0.375$ and we have obtained by simulation:[4] $\mathbb{E}(\mathscr{N}_L) = 1.7128$. We now explain how the structure of *LILLIPUT* leads to this result.

Table 4. Attack on 6 rounds.

Input branches	Output branches	#Sample	#Pairs in a sample	#Pairs in average
I_{10}, I_{14}	S_9, S_{15}	100	120	32

At the end of round 6 (see Property 1) we have: $S_{15} = X_5^5$ and $S_9 = X_3^5$ and

$$
\begin{aligned}
X_5^5 &= X_6^3 \oplus X_8^4 \oplus f(X_3^4), & X_3^5 &= X_1^3 \oplus X_8^4 \oplus f(X_2^4),\\
X_6^3 &= X_7^1 \oplus X_8^2 \oplus f(X_5^2), & X_1^3 &= X_3^1 \oplus f(X_8^2),\\
X_7^1 &= I_{15} \oplus I_8 \oplus f(I_2), & X_3^1 &= I_{11} \oplus I_8 \oplus f(I_6),\\
X_5^2 &= I_7 \oplus X_8^1 \oplus f(X_3^1). & &
\end{aligned}
$$

So we have: $\Delta X_7^1 = 0$, $\Delta X_3^1 = 0$, $\Delta X_5^2 = 0$. Or, $\Delta X_8^2 = \Delta I_{10} \oplus \Delta I_{14} = 0$. So, $\Delta X_1^3 = 0$ and $\Delta X_6^3 = 0$. Thus $\Delta S_9 \oplus \Delta S_{15} = \Delta f(X_2^4) \oplus \Delta f(X_3^4)$.

[3] See appendix C.

[4] Mean value obtained in simulation with 5000 samples of 4 messages.

$$X_2^4 = X_4^2 \oplus X_8^3 \oplus f(X_6^3), \qquad X_3^4 = X_1^2 \oplus X_8^3 \oplus f(X_2^3),$$
$$X_4^2 = I_6 \oplus X_8^1 \oplus f(X_1^1), \qquad X_1^2 = I_4 \oplus f(X_8^1),$$
$$X_1^1 = I_9 \oplus f(I_8), \qquad X_2^3 = X_4^1 \oplus X_8^2 \oplus f(X_6^2).$$

So $\Delta X_1^1 = 0$, $\Delta X_4^2 = 0$, $\Delta X_2^3 = 0$, $\Delta X_1^2 = 0$. So $\Delta f(X_2^3) = 0$, $\Delta X_3^4 = \Delta X_2^4 = \Delta X_8^3$. Or, we have:

$$\begin{aligned}\Delta X_8^3 &= \Delta X_2^2 \oplus \Delta X_3^2 \\ &= \Delta f(X_6^1) \oplus \Delta f(X_2^1) \\ &= f(X_6^1) \oplus f(X_6^1 \oplus \Delta I_{14}) \oplus f(X_2^1) \oplus f(X_2^1 \oplus \Delta I_{10}).\end{aligned}$$

So we have: $\Delta S_9 \oplus \Delta S_{15} = f(X_2^4) \oplus f(X_2^4 \oplus \Delta X_8^3) \oplus f(X_3^4) \oplus f(X_3^4 \oplus \Delta X_8^3)$.

The bias is obtained if $f(X_2^4) = f(X_3^4)$ note that the round key is not the same for these two values so it does not lead to $X_2^4 = X_3^4$. We can also follow the differential trail if $X_8^3 = 0$. This happens at random or if $f(X_6^1) = f(X_2^1)$ and, similarly, it does not mean $X_6^1 = X_2^1$. Thus we are able to distinguish a random permutation from a *LILLIPUT* permutation. We can also turn this attack into a related key attack with probability 1.[5]

7 rounds. Just like the attacks for 6 rounds, our program has found some attacks[6] and we will describe the most efficient of them. The tool found an improbable differential attack on *LILLIPUT* reduced to 7 rounds. For this attack, we use samples of 8,160 pairs, so 68 structures of 120 pairs of messages each. This corresponds to about 2^7 messages, but with this kind of attack, about 2^{10} messages are needed (see Subsection 3.3). The output condition is an equality on 4 bits: $\Delta S_{10} \oplus \Delta S_{12} = 0$. Thus, for a random permutation, the number of pairs verifying this condition is expected to be 510 in average, since we have $\mathbb{E}(\mathcal{N}_{perm}) \simeq \frac{m(m-1)}{2.\cdot 2^4}$ and we obtain that $\sigma(\mathcal{N}_{perm}) \simeq \sqrt{\mathbb{E}(\mathcal{N}_{perm})}$ is about 22.58. If we look at the values we have obtained and that are given in Table 5, we see that $|\mathbb{E}(\mathcal{N}_L) - \mathbb{E}(\mathcal{N}_{perm})| > \sigma(\mathcal{N}_{perm})$. This shows that, as explained in Section 3.1, the attack is successful. Moreover, since $\mathbb{E}(\mathcal{N}_L) < \mathbb{E}(\mathcal{N}_{perm})$, we have an improbable attack.

Table 5. Attack simulation on 7 rounds.

Input branches	Output branches	#Sample	#Pairs in a sample	#Pairs in average
I_{10}, I_{12}	S_{10}, S_{12}	500	8,160	477

We describe now the details of the equations and explain why it leads to an improbable differential attack. At the end of round 6 (see Property 1) we have: $S_{10} = X_4^6$ and $S_{12} = X_2^6$.

[5] See appendix B.
[6] See appendix C.

$$
\begin{aligned}
X_4^6 &= X_2^4 \oplus X_8^5 \oplus f(X_1^5), & X_2^6 &= X_4^4 \oplus X_8^5 \oplus f(X_6^5),\\
X_2^4 &= X_4^2 \oplus X_8^3 \oplus f(X_6^3), & X_4^4 &= X_2^2 \oplus X_8^3 \oplus f(X_1^3),\\
X_4^2 &= I_6 \oplus X_8^1 \oplus f(X_1^1), & X_2^2 &= I_2 \oplus X_8^1 \oplus f(X_6^1),\\
X_1^1 &= I_9 \oplus f(I_8), & X_6^1 &= I_{14} \oplus I_8 \oplus f(I_3),\\
X_6^3 &= X_7^1 \oplus X_8^2 \oplus f(X_5^2), & X_1^3 &= X_3^1 \oplus f(X_8^2),\\
X_7^1 &= I_{15} \oplus I_8 \oplus f(I_2), & X_3^1 &= I_{11} \oplus I_8 \oplus f(I_6).
\end{aligned}
$$

So, $\Delta X_3^1 = 0$, $\Delta X_1^3 = 0$, $\Delta X_6^1 = 0$, $\Delta X_2^2 = 0$. Similarly, $\Delta X_7^1 = 0$, $\Delta X_6^3 = 0$, $\Delta X_1^1 = 0$ and $\Delta X_4^2 = 0$. So, $\Delta X_4^6 \oplus \Delta X_2^6 = \Delta f(X_6^5) \oplus \Delta f(X_1^5)$. Moreover we have: $\Delta X_6^5 = \Delta X_3^3 \oplus \Delta f(X_8^4)$ and $\Delta X_6^5 = \Delta_8^4 \oplus \Delta f(X_3^3)$ It is easy to check that $\Delta X_3^3 = 0$ and $\Delta X_5^4 = \Delta X_6^2 \oplus \Delta X_8^3 \oplus \Delta f(X_3^3) = \Delta X_8^3$. We also have $\Delta X_8^4 = \Delta X_8^3 \oplus \Delta X_5^3$. This gives:

$$
\begin{aligned}
\Delta S_{10} \oplus \Delta S_{12} = f(X_1^5) \oplus f\left(X_1^5 \oplus f(X_8^4) \oplus f(X_8^4 \oplus \Delta X_8^4)\right)&\\
\oplus\ f(X_6^5) \oplus f\left(X_6^5 \oplus \Delta X_8^4 \oplus f(X_5^4) \oplus f(X_5^4 \oplus \Delta X_8^3)\right)&.
\end{aligned}
$$

Suppose that $\Delta X_8^3 = \Delta X_5^3$. This implies that $\Delta X_8^4 = 0$ and we have: $\Delta S_{10} \oplus \Delta S_{12} = f(X_6^5) \oplus f\left(X_6^5 \oplus f(X_5^4) \oplus f(X_5^4 \oplus \Delta X_8^3)\right)$. Since f is bijective, we obtain:

$$
\Delta S_{10} \oplus \Delta S_{12} = 0 \Leftrightarrow f(X_5^4) \oplus f(X_5^4 \oplus \Delta X_8^3) = 0 \Leftrightarrow \Delta X_8^3 = 0.
$$

This also gives $\Delta X_5^3 = 0$. But $\Delta X_5^3 = 0 \Leftrightarrow \Delta X_3^2 = 0 \Leftrightarrow \Delta I_{10} = 0$ which is not possible. We now compute the probabilities. We have:

$$
\begin{aligned}
\mathbb{P}\left[\Delta S_{10} \oplus \Delta S_{12} = 0\right] = \mathbb{P}\left[\Delta S_{10} \oplus \Delta S_{12} = 0 / \Delta X_5^3 \neq \Delta X_8^3\right] \mathbb{P}\left[\Delta X_5^3 \neq \Delta X_8^3\right]&\\
+\ \mathbb{P}\left[\Delta S_{10} \oplus \Delta S_{12} = 0 / \Delta X_5^3 = \Delta X_8^3\right] \mathbb{P}\left[\Delta X_5^3 = \Delta X_8^3\right]&.
\end{aligned}
$$

The previous computations show that: $\mathbb{P}\left[\Delta S_{10} \oplus \Delta S_{12} = 0 / \Delta X_5^3 = \Delta X_8^3\right] = 0$. Thus we obtain, if m is the number of messages.

$$
\begin{aligned}
\mathbb{P}\left[\Delta S_{10} \oplus \Delta S_{10} = 0\right] &= \mathbb{P}\left[\Delta S_{10} \oplus \Delta S_{10} = 0 / \Delta X_5^3 \neq \Delta X_8^3\right] \mathbb{P}\left[\Delta X_5^3 \neq \Delta X_8^3\right]\\
&= \frac{m(m-1)}{2 \cdot 2^4}\left(1 - \frac{1}{2^4}\right).
\end{aligned}
$$

With $m = 2^7$, this is the value given in Table 5. This shows that we have here an improbable attack.

8 rounds. The tool have found a differential attack on *LILLIPUT* reduced to 8 rounds. For this attack, we use samples of 301,977,600 pairs, so 2,516,480 structures. This corresponds to about 1.5×2^{14} messages, but with this kind of attack, about 2^{25} messages are needed (see Subsection 3.3). The output condition is an equality on 4 bits:

$\Delta S_{12} \oplus \Delta S_{14} = 0$. For a random permutation, the number of pairs verifying this condition is expected to be 18,873,600 in average, i.e. $\mathbb{E}(\mathcal{N}_{perm}) \simeq \frac{m(m-1)}{2 \cdot 2^4}$, and the standard deviation is about the square root of the mean value which gives: 4344. Since the mean value obtained for a *LILLIPUT* permutation is 18,882,219.56, we can see that $|\mathbb{E}(\mathcal{N}_L) - \mathbb{E}(\mathcal{N}_{perm})| > \sigma(\mathcal{N}_{perm})$. This shows that, as explained in Section 3.1, the attack is successful. The simulations described in Table 6 have taken 65.6 hours of computation on a virtual machine with a E8500 as processor and 4Go of RAM.

Table 6. Attack simulation on 8 rounds.

Input branches	Output branches	#Sample	#Pairs in a sample	#Pairs in average
I_9, I_{10}	S_{12}, S_{14}	50	301,977,600	18,882,219.56

Here are the details of the equations: $S_{12} = X_2^7$ and $S_{14} = X_7^7$.

$$\begin{aligned}
X_2^7 &= X_4^5 \oplus X_8^6 \oplus f(X_6^6), & X_7^7 &= X_5^5 \oplus X_8^6 \oplus f(X_4^6),\\
X_4^5 &= X_2^3 \oplus X_8^4 \oplus f(X_1^4), & X_5^5 &= X_6^3 \oplus X_8^4 \oplus f(X_3^4),\\
X_2^3 &= X_4^1 \oplus X_8^2 \oplus f(X_6^2), & X_6^3 &= X_7^1 \oplus X_8^2 \oplus f(X_5^2),\\
X_4^1 &= I_{12} \oplus I_8 \oplus f(I_5), & X_4^1 &= I_{12} \oplus I_8 \oplus f(I_5),\\
\Delta X_4^1 &= 0, & \Delta X_7^1 &= 0.
\end{aligned}$$

Or $\Delta f(X_5^2) = 0$ and $\Delta f(X_6^2) = 0$. So $\Delta S_{12} \oplus \Delta S_{14} = \Delta f(X_6^6) \oplus \Delta f(X_4^6) \oplus \Delta f(X_1^4) \oplus \Delta f(X_3^4)$. We can observe that the condition $\Delta S_{12} \oplus \Delta S_{14} = 0$ can be satisfied if for example: $f(X_1^4) = f(X_3^4), f(X_1^4 \oplus \Delta X_1^4) = f(X_3^4 \oplus \Delta X_3^4), f(X_4^6) = f(X_6^6)$, and $f(X_4^6 \oplus \Delta X_4^6) = f(X_6^6 \oplus \Delta X_6^6)$. But other equalities are also possible.

5 Conclusion

We have seen some differential attacks on *LILLIPUT*. These attacks were found by a tool we have made and are based on the variance method. This is the first time this method is applied to a concrete cipher. The tool has highlighted unusual differential conditions for which *LILLIPUT* is sensitive. We can see our distinguishers do not reach more rounds than the previous analysis. But, contrary to these attacks, we have found our results empirically and since the last attack require 2^{25} messages, one can see that it is far from the maximum and from the complexity of 2^{45} based on the number of active sboxes. Thus, we can look for distinguishers which reach more rounds with a devoted equipment. We have described how the key recovery works with our attacks in the appendix A. Finally, we have also seen improbable differential attacks which work well in simulations. This scheme can be an efficient support to study this kind of attacks thanks to the complexity of relations between internal variables in *LILLIPUT* due to the *LinearLayer* step.

References

1. R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, and al. The SIMON and SPECK Families of Lightweight Block Ciphers. *Cryptology ePrint archive: 2013/404: Listing for 2013*.
2. C. Beierle, J. Jean, S. Kölbl, and al. The SKINNY Family of Block Ciphers and its Low-Latency Variant MANTIS. *Cryptology ePrint archive: 2016/660: Listing for 2016*.
3. T. P. Berger, J. Francq, M. Minier, and G. Thomas. Extended generalized feistel networks using matrix representation to propose a new lightweight block cipher: Lilliput. *IEEE Transactions on Computers*, 65(7):2074–2089, July 2016.
4. T.P. Berger, M. Minier, and G. Thomas. *Extended Generalized Feistel Networks Using Matrix Representation*, pages 289–305. Springer Berlin Heidelberg, Berlin, Heidelberg, 2014.
5. E. Biham, R.J. Anderson, and L.R. Knudsen. Serpent: A new block cipher proposal. In *Proceedings of the 5th International Workshop on Fast Software Encryption*, FSE '98, pages 222–238, London, UK, UK, 1998. Springer-Verlag.
6. E. Biham, A. Biryukov, and A. Shamir. Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials. In J. Stern, editor, *Advances in Cryptology – EUROCRYPT 99*, volume 1592 of *Lecture Notes in Computer Science*, pages 12–23. Springer-Verlag, 1999.
7. E. Biham and A. Shamir. Differential Cryptanalysis of DES-like Cryptosystems. *J. Cryptology*, 4(1):3–72, 1991.
8. C. Blondeau. *Improbable Differential from Impossible Differential: On the Validity of the Model*, pages 149–160. Springer International Publishing, Cham, 2013.
9. A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin, and C. Vikkelsoe. *PRESENT: An Ultra-Lightweight Block Cipher*, pages 450–466. Springer Berlin Heidelberg, Berlin, Heidelberg, 2007.
10. Patrick Derbez and Pierre-Alain Fouque. *Automatic Search of Meet-in-the-Middle and Impossible Differential Attacks*, pages 157–184. Springer Berlin Heidelberg, Berlin, Heidelberg, 2016.
11. L.R. Knudsen. Truncated and higher order differentials. In B. Preneel, editor, *Fast Software Encrytion – FSE '94*, volume 1008 of *Lecture Notes in Computer Science*, pages 291–311. Springer-Verlag, 1994.
12. V. Nachef, N. Marrière, and E. Volte. *Improved Attacks on Extended Generalized Feistel Networks*, pages 562–572. Springer International Publishing, Cham, 2016.
13. V. Nachef, J. Patarin, and E. Volte. *Feistel Ciphers*. Springer International Publishing, 2017.
14. V. Nachef, E. Volte, and J. Patarin. Differential Attacks on Generalized Feistel schemes. In M. Abdalla, C. Nita-Rotaru, and R. Dahab, editors, *CANS 2013*, volume 8257 of *Lecture Notes in Computer Science*, pages 1–19. Springer-Verlag, 2013.
15. Y. Sasaki and Y. Todo. New differential bounds and division property of lilliput: Block cipher with extended generalized feistel network. In *Selected Areas in Cryptography – SAC 2016*. Springer, 2016.
16. Y. Sasaki and Y. Todo. New impossible differential search tool from design and cryptanalysis aspects - revealing structural properties of several ciphers. In *EUROCRYPT (3)*, pages 185–215. Springer, 2017.
17. K. Shibutani, T. Isobe, H. Hiwatari, A. Mitsuda, T. Akishita, and T. Shirai. *Piccolo: An Ultra-Lightweight Blockcipher*, pages 342–357. Springer Berlin Heidelberg, Berlin, Heidelberg, 2011.
18. T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata. *The 128-Bit Blockcipher CLEFIA (Extended Abstract)*, pages 181–195. Springer Berlin Heidelberg, Berlin, Heidelberg, 2007.
19. C. Tezcan. Truncated, impossible, and improbable differential analysis of ascon. *Cryptology ePrint archive: 2016/490: Listing for 2016*.

20. C. Tezcan. *The Improbable Differential Attack: Cryptanalysis of Reduced Round CLEFIA*, pages 197–209. Springer Berlin Heidelberg, Berlin, Heidelberg, 2010.
21. E. Volte, V. Nachef, and N. Marrière. Automatic Expectation and Variance Computing for Attacks on Feistel Schemes. *Cryptology ePrint archive: 2016/136: Listing for 2016*.
22. D. Wagner. The boomerang attack. In *Proceedings of the 6th International Workshop on Fast Software Encryption*, FSE '99, pages 156–170, London, UK, UK, 1999. Springer-Verlag.
23. Shengbao Wu and Mingsheng Wang. *Automatic Search of Truncated Impossible Differentials for Word-Oriented Block Ciphers*, pages 283–302. Springer Berlin Heidelberg, Berlin, Heidelberg, 2012.
24. Y. Luoand Z. Wu, X. Lai, and G. Gong. A Unified Method for Finding Impossible Differentials of Block Cipher Structures. 2009. http://eprint.iacr.org/.

A Key recovery

In this appendix, we describe how the key recovery works in order to show what we can do. We process the key recovery on *LILLIPUT* reduced to 7 and 8 rounds. We have used the distinguishing attack on 6 rounds to attack 7 then 8 rounds in order to do simulations because the distinguishing attack on 8 rounds require 2^{25} messages to be processed. Nevertheless, it will work similarly for this distinguishing attack.

A.1 Key schedule description

LILLIPUT uses a 80-bit master key. The key schedule is managed by an internal state denoted by 20 nibbles (4-bit words): $Y_{19},\dots,Y_0$. It is initialized with the master key and is processed by the algorithm 2 in order to build the round keys $RK^0,\dots,RK^{29}$. The *ExtractRoundKey* function is described in the algorithm 3. Note that the Sbox S used in the *ExtractRoundKey* function is the same as the one in *LILLIPUT*. The functions L_0, L_1, L_2 and L_3 are generalized Feistel schemes with 5 branches and a bit size of 4. They are described in Fig 2, Fig 3, Fig 4 and Fig 5 respectively.

Algorithm 2 LILLIPUT key schedule

$Y_{19},\dots,Y_0 = MasterKey$
$RK^0 = ExtractRoundKey(Y_{19},\dots,Y_0)$
for i in $1,\dots,29$ **do**
  $(Y_4,\dots,Y_0) = L_0(Y_4,\dots,Y_0)$
  $(Y_9,\dots,Y_5) = L_1(Y_9,\dots,Y_5)$
  $(Y_{14},\dots,Y_{10}) = L_2(Y_{14},\dots,Y_{10})$
  $(Y_{19},\dots,Y_{15}) = L_3(Y_{19},\dots,Y_{15})$
  $RK^i = ExtractRoundKey(Y_{19},\dots,Y_0)$
end for

Algorithm 3 *ExtractRoundKey* function for RK^i

Let Z, a 32-bit word such that: $Z = Y_{18}Y_{16}Y_{13}Y_{10}Y_9Y_6Y_3Y_1$
The bits of Z are denoted by: $Z_{31}, \ldots, Z_0$
$RK^0 = ExtractRoundKey(Y_{19}, \ldots, Y_0)$
for j in $0, \ldots, 7$ **do**
  $RK^i_j = S(Z_j || Z_{8+j} || Z_{16+j} || Z_{24+j})$
end for
$RK^i = RK^i \oplus (i||0)$

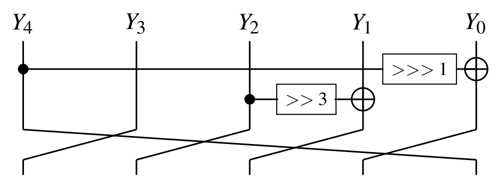

Fig. 2. L_0

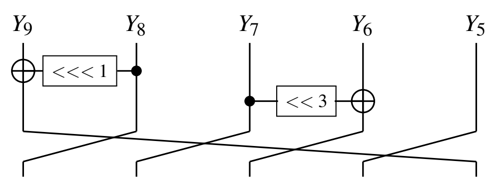

Fig. 3. L_1

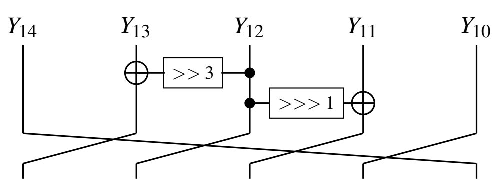

Fig. 4. L_2

A.2 Key recovery analysis on 7 rounds

This attack is based on some distinguishing attacks on 6 rounds. As usual, a plaintext structure contains 16 messages (thus 120 different pairs) which are different only on 2 branches. Moreover, the difference has to be the same on these branches.

On *LILLIPUT* reduced to 6 rounds, there are some differential attacks based on our attacks. The involved input branches are I_9 and I_{10}. On the outputs, the conditions can be: $\Delta S_9 \oplus \Delta S_{10} = 0$ or $\Delta S_9 \oplus \Delta S_{14} = 0$ or $\Delta S_{10} \oplus \Delta S_{14} = 0$. Based on one of these attacks, one can mount a key recovery attack on 7 rounds with the algorithm 4.

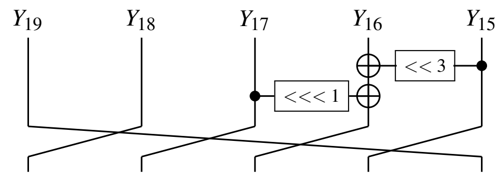

Fig. 5. L_3

Algorithm 4 Key recovery on 7 rounds.

Encrypt some samples of 68 structures on 7 rounds.
for all guess of RK_0^6, RK_1^6 **do**
  Decrypt one round with the guess.
  r =Count how many pairs verify $\Delta S_9 \oplus \Delta S_{10} = 0$.
  if $r > 550$ **then**
    The guess is possible, one has to stock it.
  end if
end for

This algorithm allows to get a list of possible RK_0^6, RK_1^6. There are 2^8 possibilities for the guess. In simulations, one can find directly the correct guess (list of one element) with 5 or 10 samples. But with less samples, one get a list of several possibilities. With the knowledge of RK_0^6, RK_1^6, one get the following bits of the corresponding Z: $Z_0Z_1Z_8Z_9Z_{16}Z_{17}Z_{24}Z_{25}$. Even if there are several RK_0^6, RK_1^6, the cost of the brute-force attack is reduced from 2^{80} to about 2^{74}. Of course, one can optimize this algorithm.

Indeed, one can use several attacks in order to get a better attack. It is described in the algorithm 5. In simulations, we have always get the correct guess RK_0^6, RK_1^6 and RK_5^6. As we do not test all the possibilities for the second and third attack but only the ones which work from the previous, the number of possibilities is lower than 3×2^8.

With the algorithm 5, one has the knowledge of RK_0^6, RK_1^6 and RK_5^6. It corresponds to the following bits of Z: $Z_0Z_1Z_5Z_8Z_9Z_{13}Z_{16}Z_{17}Z_{21}Z_{24}Z_{25}Z_{29}$. Then, the cost of the brute-force attack is reduced from 2^{80} to 2^{68}.

We can also improve the algorithm 5 by using the following improbable differential attacks: $\Delta S_9 \oplus \Delta S_{15} = 0$, $\Delta S_{10} \oplus \Delta S_{15} = 0$ and $\Delta S_{14} \oplus \Delta S_{15} = 0$. There are 2^4 possibilities for RK_6^6, the corresponding round key for S_{15}, and we test only with the possible RK_0^6, RK_1^6 and RK_5^6. Thus, the cost of the brute-force attack is reduced from 2^{80} to 2^{64}.

Starting from these attack, one can get additional details by using distinguishing attacks on *LILLIPUT* reduced to 5 rounds. Indeed, based on the same input conditions, there are the following attacks on 5 rounds: $\Delta S_{13} \oplus \Delta S_{15} = 0$, $\Delta S_{13} \oplus \Delta S_{14} = 0$ and $\Delta S_{14} \oplus \Delta S_{15} = 0$. These attacks require the previous guess RK_0^6, RK_1^6 and RK_6^6. One can use the same method from the algorithm 5 to get RK_4^5, RK_5^5 and RK_6^5. Thus, the corresponding bits of Z for the round 5 are: $Z_4Z_5Z_6Z_{12}Z_{13}Z_{14}Z_{20}Z_{21}Z_{22}Z_{28}Z_{29}Z_{30}$. In the key schedule, these bits correspond to Y_3, Y_9, Y_{13} and Y_{18}. Then, for the round 6, they shift to: Y_4, Y_5, Y_{14} and Y_{19}. For this step, the number of possibilities is lower than 3×2^8.

Algorithm 5 Key recovery on 7 rounds.

Encrypt some samples of 68 structures on 7 rounds.
for all guess of RK_0^6, RK_1^6 **do**
  Decrypt one round with the guess.
  r =Count how many pairs verify $\Delta S_9 \oplus \Delta S_{10} = 0$.
  if $r > 550$ **then**
    The guess is possible, one has to stock it in $List_0$.
  end if
end for
for all possible RK_0^6 in $List_0$ **do**
  for all guess of RK_5^6 **do**
    Decrypt one round of the ciphertexts after 7 rounds with the guess RK_0^6 and RK_5^6.
    r =Count how many pairs verify $\Delta S_9 \oplus \Delta S_{14} = 0$.
    if $r > 550$ **then**
      The guess is possible, one has to stock it in $List_1$.
    end if
  end for
end for
for all possible RK_1^6 in $List_0$ **do**
  for all possible RK_5^6 in $List_1$ **do**
    Decrypt one round of the ciphertexts after 7 rounds with the guess RK_1^6 and RK_5^6.
    r =Count how many pairs verify $\Delta S_{10} \oplus \Delta S_{14} = 0$.
    if $r > 550$ **then**
      The guess is possible, one has to stock it.
    end if
  end for
end for
Deduce the possible correct guess RK_0^6, RK_1^6, RK_5^6.

There is a efficient attack with the same input condition on *LILLIPUT* reduced to 5 rounds and we can exploit it in our key recovery attack. The output condition is $\Delta S_9 \oplus \Delta S_{10} = 0$. This condition is always verified, so we can test it on smaller samples in order to decrease the global complexity. One can look which round keys are involved from the end of round 7: RK_0^5, RK_1^5, RK_4^6 and RK_7^6. The number of possibilities is 2^{16}.

Table 7. Round key recover at the end of round 6.

Round key	Corresponding bits on Z	Corresponding Y
RK_0^6	Z_0, Z_8, Z_{16}, Z_{24}	Y_1, Y_6, Y_{10}, Y_{16}
RK_1^6	Z_1, Z_9, Z_{17}, Z_{25}	Y_1, Y_6, Y_{10}, Y_{16}
RK_4^6	$Z_4, Z_{12}, Z_{20}, Z_{28}$	Y_3, Y_9, Y_{13}, Y_{18}
RK_5^6	$Z_5, Z_{13}, Z_{21}, Z_{29}$	Y_3, Y_9, Y_{13}, Y_{18}
RK_6^6	$Z_6, Z_{14}, Z_{22}, Z_{30}$	Y_3, Y_9, Y_{13}, Y_{18}
RK_7^6	$Z_7, Z_{15}, Z_{23}, Z_{31}$	Y_3, Y_9, Y_{13}, Y_{18}

Table 8. Round key recover at the end of round 5.

Round key	Corresponding bits on Z	Corresponding Y
RK_0^5	Z_0, Z_8, Z_{16}, Z_{24}	Y_1, Y_6, Y_{10}, Y_{16}
RK_1^5	Z_1, Z_9, Z_{17}, Z_{25}	Y_1, Y_6, Y_{10}, Y_{16}
RK_4^5	$Z_4, Z_{12}, Z_{20}, Z_{28}$	Y_3, Y_9, Y_{13}, Y_{18}
RK_5^5	$Z_5, Z_{13}, Z_{21}, Z_{29}$	Y_3, Y_9, Y_{13}, Y_{18}
RK_6^5	$Z_6, Z_{14}, Z_{22}, Z_{30}$	Y_3, Y_9, Y_{13}, Y_{18}

Finally, we have attacked *LILLIPUT* reduced to 7 rounds using distinguishing attacks on 6 and 5 rounds. One can see the round keys recovered in the table 7 and table 8. Here is the state[7] at the end of round 6: $Y_1 =??||$, $Y_3 = ||||$, $Y_6 =??||$, $Y_9 = ||||$, $Y_{10} =??||$, $Y_{13} = ||||$, $Y_{16} =??||$, $Y_{18} = ||||$. At the end of the round 5, it is similar, we have the knowledge of: $Y_1 =??||$, $Y_3 =?|||$, $Y_6 =??||$, $Y_9 =?|||$, $Y_{10} =??||$, $Y_{13} =?|||$, $Y_{16} =??||$, $Y_{18} =?|||$. But, these bits shift for the round 6. Thus, at the end of round 6, we also have more details described in table 9. We can see in this table that we have recovered 44 bits of the internal state. Thus, the cost of the brute-force is reduced from 2^{80} to 2^{36}. The cost for all guess is less than: $c = 2^{16} + 6 * 2^8 + 2^4$. We can continue to use the previous rounds with more distinguishing attacks in order to reduce the complexity.

Table 9. Internal state at round 6.

Parts of Y	State of the nibble
Y_0, Y_8, Y_{12}, Y_{15}	????
$Y_1, Y_2, Y_6, Y_7, Y_{10}, Y_{11}, Y_{16}, Y_{17}$	??||
Y_4, Y_5, Y_{14}, Y_{19}	?|||
Y_3, Y_9, Y_{13}, Y_{18}	||||

A.3 Key recovery analysis on 8 rounds

We have seen how the key recovery works based on our attacks. Now, we will see how it can be extend. In this subsection, we will see how it works on *LILLIPUT* reduced to 8 rounds.

First, we want to use our distinguishing attack on 6 rounds: $\Delta S_9 \oplus \Delta S_{10} = 0$. If we look the branches involved until 8 rounds, we can see which round key we have to guess. We summarize the analysis in the table 10. To mount a key recovery attack on *LILLIPUT* reduced to 8 rounds, one can use the algorithm 6. As is it described in the table 10, if one wants to exploit $\Delta S_9 \oplus \Delta S_{10} = 0$, the round key to guess will be: RK_0^6, RK_1^6, RK_7^7 and RK_4^7. Thus the number of possibilities is 2^{16}. We can use more distinguishing attacks in order to get more round keys: $\Delta S_9 \oplus \Delta S_{10} = 0$ and $\Delta S_9 \oplus$

[7] '?' means unknown bit and '|' means known bit

Table 10. Round key involved for key recovery on 8 rounds.

Branch involved	Round key and involved branches	Round key for internal variables
X_3^5	RK_0^6, X_8^6	RK_7^7
X_4^5	RK_1^6, X_6^6	RK_4^7
X_7^5	RK_5^6, X_5^6	RK_6^7
X_5^5	RK_6^6, X_4^6	RK_1^7

$\Delta S_{10} = 0$ for example. Moreover, there are the same improbable differential attacks as in the Section A.2: $\Delta S_9 \oplus \Delta S_{15} = 0$, $\Delta S_{10} \oplus \Delta S_{15} = 0$ and $\Delta S_{14} \oplus \Delta S_{15} = 0$.

Algorithm 6 Key recovery on 8 rounds.

```
Encrypt some samples of 68 structures on 8 rounds.
for all guess of RK^7_7, RK^7_4 do
    Decrypt one round with the guess.
    for all guess of RK^6_0, RK^6_1 do
        r =Count how many pairs verify ΔS_9 ⊕ ΔS_10 = 0.
        if r > 550 then
            The guess is possible, one has to stock it.
        end if
    end for
end for
```

We can use the same method as the algorithm 5. Thanks to this algorithm, we have recovered 24 bits of data as described in the table 11 and table 12. Then we will see how much is the cost of the brute-force attack without using previous rounds method.

Table 11. Round key recover at the end of round 6.

Round key	Corresponding bits on Z	Corresponding Y
RK_0^6	Z_0, Z_8, Z_{16}, Z_{24}	Y_1, Y_6, Y_{10}, Y_{16}
RK_1^6	Z_1, Z_9, Z_{17}, Z_{25}	Y_1, Y_6, Y_{10}, Y_{16}
RK_5^6	$Z_4, Z_{12}, Z_{20}, Z_{28}$	Y_3, Y_9, Y_{13}, Y_{18}

As we can see in the Section A.1, the information recovered at the end of round 7 can be go up at the end of round 6 without any condition. Thus, with an algorithm similar to the algorithm 5, we have recovered 24 bits of data for the internal state at the end of round 6 and not only split on two rounds. It is described in the table 13. The cost of the brute-force attack is reduced from 2^{80} to 2^{56}.

Table 12. Round key recover at the end of round 7.

Round key	Corresponding bits on Z	Corresponding Y
RK_4^7	$Z_4, Z_{12}, Z_{20}, Z_{28}$	Y_3, Y_9, Y_{13}, Y_{18}
RK_6^7	$Z_6, Z_{14}, Z_{22}, Z_{30}$	Y_3, Y_9, Y_{13}, Y_{18}
RK_7^7	$Z_7, Z_{15}, Z_{23}, Z_{31}$	Y_3, Y_9, Y_{13}, Y_{18}

Table 13. Internal state at round 6.

Parts of Y	State of the nibble
$Y_0,Y_4,Y_5,Y_7,Y_{11},Y_{14},Y_{15}Y_{19}$	????
Y_3,Y_9,Y_{13},Y_{18}	??|?
Y_1,Y_6,Y_{10},Y_{16}	??||
Y_2,Y_8,Y_{12},Y_{17}	||?|

A.4 Key recovery analysis on more rounds

We have seen how to attack 2 rounds more than the distinguisher. In order to attack more rounds, we need the internal variable on the branch I_{16}. Thus we will need to guess all the round keys for this round. So, it costs 2^{32}. Similarly, if we want to attack 4 rounds more than the distinguisher attack, it will cost 2^{64}. It is possible to reduce enough the complexity to do that but we can not process one more round with this method. Based on the distinguisher on 8 rounds, it is then possible to attack 12 rounds.

B Related key attack on 6 rounds

In this appendix, we describe the related key attack on *LILLIPUT* reduce to 6 rounds. To recall the attack, the input branches involved are I_{10} and I_{14}. If $c = c_1 \oplus c_2$, the ouput condition is $S_9(c) \oplus S_{15}(c) = 0$.

If $I_{10} = I_{14}$ and $RK_1^1 = RK_5^1$ and $RK_1^2 = RK_2^2$, the differential trail is verified with probability 1. This attack was verified in practice.

The aim of the attack is to make $\Delta X_8^3 = 0$.

We have seen that $\Delta X_8^3 = f(X_6^1) \oplus f(X_6^1 \oplus \Delta I_{14}) \oplus f(X_2^1) \oplus f(X_2^1 \oplus \Delta I_{10})$. Moreover, we know that $\Delta I_{14} = \Delta I_{10}$.

But, it is important to notice that $f(X_6^1) = sbox(X_6^1 \oplus RK_1^1)$. Similarly, $f(X_2^1) = sbox(X_2^1 \oplus RK_2^1)$. So, $\Delta X_8^3 = 0$ if and only if $sbox(X_2^1 \oplus RK_2^1) = sbox(X_6^1 \oplus RK_1^1)$. It can happens at random but if we have the condition on the key $RK_1^1 = RK_2^1$, then $(X_6^1 = X_2^1) \Rightarrow \Delta X_8^3 = 0$.

Then, we have $X_6^1 \oplus X_2^1 = I_{14} \oplus I_{10} \oplus sbox(I_3 \oplus RK_5^0) \oplus sbox(I_7 \oplus RK_1^0)$. So if $I_{10} = I_{14}$, then $(X_6^1 \oplus X_2^1 = 0$ if and only if $I_3 \oplus RK_5^0 = I_7 \oplus RK_1^0)$.

Now we will see what kind of conditions on the master key we have.

The key state is denoted by 20 nibbles of 4 bits: $Y = [Y_{19}, \cdots, Y_0]$ Each round there is a 32-bit round key extract by the extraction function.

First, we have $Z = [Y_{18}, Y_{16}, Y_{13}, Y_{10}, Y_9, Y_6, Y_3, Y_1]$. Let $Z = Z_{31}, \cdots, Z_0$ the bits of Z. Then, we have:

$$\begin{aligned}
RK_1^1 &= sbox([Z_1, Z_9, Z_{17}, Z_{25}]),\\
RK_5^1 &= sbox([Z_5, Z_{13}, Z_{21}, Z_{29}]),\\
RK_1^2 &= sbox([Z_1, Z_9, Z_{17}, Z_{25}]) \oplus 1,\\
RK_2^2 &= sbox([Z_2, Z_{10}, Z_{18}, Z_{26}]) \oplus 1.
\end{aligned}$$

Note that the xor with 1 is processed to flip the bit at the left. $RK_1^1 = RK_5^1$ if and only if $sbox([Z_1, Z_9, Z_{17}, Z_{25}]) = sbox([Z_5, Z_{13}, Z_{21}, Z_{29}])$. So $RK_1^1 = RK_5^1$ if and only if $[Z_1, Z_9, Z_{17}, Z_{25}] = [Z_5, Z_{13}, Z_{21}, Z_{29}]$.

So $RK_1^1 = RK_5^1$ if $Z_1 = Z_5$, $Z_9 = Z_{13}$, $Z_{17} = Z_{21}$ and $Z_{25} = Z_{29}$. If $K = K_{79}, \cdots, K_0$ is the master key, these conditions lead to: $K_5 = K_{13}$, $K_{25} = K_{38}$, $K_{41} = K_{53}$ and $K_{65} = K_{73}$

Similarly $RK_1^2 = RK_2^2$ if $Z_1 = Z_2$, $Z_9 = Z_{10}$, $Z_{17} = Z_{18}$ and $Z_{25} = Z_{26}$. Note that it is the Z of the second round, so the Z_9 is not the same. It leads to these conditions on the master key: $K_1 \oplus K_{18} = K_2 \oplus K_{19}$, $K_{21} = K_{22}$, $K_{58} = K_{57}$ and $K_{61} = K_{62}$. With these 8 conditions on 1 bit on the master key, we have the attack with probability 1 on *LILLIPUT* reduced to 6 rounds.

C Attacks on 5, 6 and 7 rounds

In this appendix, we describe some attacks on *LILLIPUT* reduced to 5, 6 and 7 rounds. These attacks are based on 500 samples of 8,160 couples of messages. This corresponds to 2^7 messages. We count how many couples verify a property. The average result for a random permutation is $\frac{8160}{2^4} = 510$ because it is an equality on 4 bits. The results obtained with the attacks we described below are significantly greater or significantly smaller than this value. In fact, in order to obtain an attack, the difference between these values is expected to be $\frac{8160}{2^8} = 32$. As said in Section 4, these attacks are based on an non zero difference put on two input branches. We detail these branches involved, the differential condition on the ouput and the average result obtained.

The attacks described below from the table 14 to the table 25 use only two branches in input and two branches in output. The tool also found a lot of attacks for all combination $i \in \{1, \cdots, 8\}$ branches in input and $j \in \{1, \cdots, 8\}$ branches in output but $i = 2$ and $j = 2$ leads to the most relevant attacks. Note that the attacks on 7 rounds are not based on 2^7 messages but 2^{11}.

Table 14. Differential attacks which require only 2 messages.

Inputs	Condition	Result
I_9, I_{10}	$\Delta S_9 \oplus \Delta S_{10} = 0$	8,160.0
I_9, I_{11}	$\Delta S_9 \oplus \Delta S_{13} = 0$	8,160.0
I_9, I_{12}	$\Delta S_{10} \oplus \Delta S_{14} = 0$	8,160.0
I_9, I_{13}	$\Delta S_{10} \oplus \Delta S_{13} = 0$	8,160.0
I_9, I_{13}	$\Delta S_{10} \oplus \Delta S_{14} = 0$	8,160.0
I_9, I_{13}	$\Delta S_{13} \oplus \Delta S_{14} = 0$	8,160.0
I_9, I_{14}	$\Delta S_9 \oplus \Delta S_{14} = 0$	8,160.0
I_{10}, I_{11}	$\Delta S_9 \oplus \Delta S_{15} = 0$	8,160.0
I_{10}, I_{12}	$\Delta S_{10} \oplus \Delta S_{12} = 0$	8,160.0
I_{10}, I_{12}	$\Delta S_{10} \oplus \Delta S_{15} = 0$	8,160.0
I_{10}, I_{12}	$\Delta S_{12} \oplus \Delta S_{15} = 0$	8,160.0
I_{10}, I_{13}	$\Delta S_{10} \oplus \Delta S_{12} = 0$	8,160.0
I_{10}, I_{14}	$\Delta S_9 \oplus \Delta S_{12} = 0$	8,160.0
I_{12}, I_{13}	$\Delta S_{10} \oplus \Delta S_{12} = 0$	8,160.0
I_{12}, I_{13}	$\Delta S_{10} \oplus \Delta S_{14} = 0$	8,160.0
I_{12}, I_{13}	$\Delta S_{12} \oplus \Delta S_{14} = 0$	8,160.0
I_{12}, I_{14}	$\Delta S_{12} \oplus \Delta S_{14} = 0$	8,160.0
I_{13}, I_{14}	$\Delta S_{12} \oplus \Delta S_{14} = 0$	8,160.0

Table 15. Impossible differential attacks on 5 rounds.

Inputs	Condition	Result
I_9, I_{10}	$\Delta S_9 \oplus \Delta S_{12} = 0$	0.0
I_9, I_{10}	$\Delta S_9 \oplus \Delta S_{13} = 0$	0.0
I_9, I_{10}	$\Delta S_9 \oplus \Delta S_{14} = 0$	0.0
I_9, I_{10}	$\Delta S_9 \oplus \Delta S_{15} = 0$	0.0
I_9, I_{10}	$\Delta S_{10} \oplus \Delta S_{12} = 0$	0.0
I_9, I_{10}	$\Delta S_{10} \oplus \Delta S_{13} = 0$	0.0
I_9, I_{10}	$\Delta S_{10} \oplus \Delta S_{14} = 0$	0.0
I_9, I_{10}	$\Delta S_{10} \oplus \Delta S_{15} = 0$	0.0
I_9, I_{11}	$\Delta S_9 \oplus \Delta S_{10} = 0$	0.0
I_9, I_{11}	$\Delta S_9 \oplus \Delta S_{14} = 0$	0.0
I_9, I_{11}	$\Delta S_9 \oplus \Delta S_{15} = 0$	0.0
I_9, I_{11}	$\Delta S_{10} \oplus \Delta S_{13} = 0$	0.0
I_9, I_{11}	$\Delta S_{13} \oplus \Delta S_{14} = 0$	0.0
I_9, I_{11}	$\Delta S_{13} \oplus \Delta S_{15} = 0$	0.0
I_9, I_{12}	$\Delta S_9 \oplus \Delta S_{10} = 0$	0.0
I_9, I_{12}	$\Delta S_9 \oplus \Delta S_{14} = 0$	0.0
I_9, I_{12}	$\Delta S_{10} \oplus \Delta S_{12} = 0$	0.0
I_9, I_{12}	$\Delta S_{10} \oplus \Delta S_{13} = 0$	0.0
I_9, I_{12}	$\Delta S_{10} \oplus \Delta S_{15} = 0$	0.0
I_9, I_{12}	$\Delta S_{10} \oplus \Delta S_{16} = 0$	0.0
I_9, I_{12}	$\Delta S_{12} \oplus \Delta S_{14} = 0$	0.0
I_9, I_{12}	$\Delta S_{13} \oplus \Delta S_{14} = 0$	0.0
I_9, I_{12}	$\Delta S_{14} \oplus \Delta S_{15} = 0$	0.0
I_9, I_{12}	$\Delta S_{14} \oplus \Delta S_{16} = 0$	0.0
I_9, I_{13}	$\Delta S_9 \oplus \Delta S_{10} = 0$	0.0
I_9, I_{13}	$\Delta S_9 \oplus \Delta S_{13} = 0$	0.0
I_9, I_{13}	$\Delta S_9 \oplus \Delta S_{14} = 0$	0.0
I_9, I_{13}	$\Delta S_{10} \oplus \Delta S_{12} = 0$	0.0
I_9, I_{13}	$\Delta S_{12} \oplus \Delta S_{13} = 0$	0.0
I_9, I_{13}	$\Delta S_{12} \oplus \Delta S_{14} = 0$	0.0
I_9, I_{14}	$\Delta S_9 \oplus \Delta S_{10} = 0$	0.0
I_9, I_{14}	$\Delta S_9 \oplus \Delta S_{12} = 0$	0.0
I_9, I_{14}	$\Delta S_9 \oplus \Delta S_{13} = 0$	0.0
I_9, I_{14}	$\Delta S_{10} \oplus \Delta S_{14} = 0$	0.0
I_9, I_{14}	$\Delta S_{12} \oplus \Delta S_{14} = 0$	0.0
I_9, I_{14}	$\Delta S_{13} \oplus \Delta S_{14} = 0$	0.0
I_9, I_{16}	$\Delta S_{10} \oplus \Delta S_{13} = 0$	0.0
I_9, I_{16}	$\Delta S_{10} \oplus \Delta S_{14} = 0$	0.0
I_{10}, I_{11}	$\Delta S_9 \oplus \Delta S_{10} = 0$	0.0
I_{10}, I_{11}	$\Delta S_9 \oplus \Delta S_{12} = 0$	0.0
I_{10}, I_{11}	$\Delta S_9 \oplus \Delta S_{13} = 0$	0.0
I_{10}, I_{11}	$\Delta S_{10} \oplus \Delta S_{15} = 0$	0.0

Inputs	Condition	Result
I_{10}, I_{11}	$\Delta S_{12} \oplus \Delta S_{15} = 0$	0.0
I_{10}, I_{11}	$\Delta S_{13} \oplus \Delta S_{15} = 0$	0.0
I_{10}, I_{12}	$\Delta S_9 \oplus \Delta S_{10} = 0$	0.0
I_{10}, I_{12}	$\Delta S_9 \oplus \Delta S_{12} = 0$	0.0
I_{10}, I_{12}	$\Delta S_9 \oplus \Delta S_{15} = 0$	0.0
I_{10}, I_{12}	$\Delta S_{10} \oplus \Delta S_{14} = 0$	0.0
I_{10}, I_{12}	$\Delta S_{10} \oplus \Delta S_{16} = 0$	0.0
I_{10}, I_{12}	$\Delta S_{12} \oplus \Delta S_{14} = 0$	0.0
I_{10}, I_{12}	$\Delta S_{12} \oplus \Delta S_{16} = 0$	0.0
I_{10}, I_{12}	$\Delta S_{14} \oplus \Delta S_{15} = 0$	0.0
I_{10}, I_{12}	$\Delta S_{15} \oplus \Delta S_{16} = 0$	0.0
I_{10}, I_{13}	$\Delta S_9 \oplus \Delta S_{10} = 0$	0.0
I_{10}, I_{13}	$\Delta S_9 \oplus \Delta S_{12} = 0$	0.0
I_{10}, I_{13}	$\Delta S_{10} \oplus \Delta S_{13} = 0$	0.0
I_{10}, I_{13}	$\Delta S_{10} \oplus \Delta S_{14} = 0$	0.0
I_{10}, I_{13}	$\Delta S_{10} \oplus \Delta S_{15} = 0$	0.0
I_{10}, I_{13}	$\Delta S_{12} \oplus \Delta S_{13} = 0$	0.0
I_{10}, I_{13}	$\Delta S_{12} \oplus \Delta S_{14} = 0$	0.0
I_{10}, I_{13}	$\Delta S_{12} \oplus \Delta S_{15} = 0$	0.0
I_{10}, I_{14}	$\Delta S_9 \oplus \Delta S_{10} = 0$	0.0
I_{10}, I_{14}	$\Delta S_9 \oplus \Delta S_{14} = 0$	0.0
I_{10}, I_{14}	$\Delta S_9 \oplus \Delta S_{15} = 0$	0.0
I_{10}, I_{14}	$\Delta S_{10} \oplus \Delta S_{12} = 0$	0.0
I_{10}, I_{14}	$\Delta S_{12} \oplus \Delta S_{14} = 0$	0.0
I_{10}, I_{14}	$\Delta S_{12} \oplus \Delta S_{15} = 0$	0.0
I_{10}, I_{16}	$\Delta S_{10} \oplus \Delta S_{12} = 0$	0.0
I_{10}, I_{16}	$\Delta S_{10} \oplus \Delta S_{15} = 0$	0.0
I_{11}, I_{12}	$\Delta S_9 \oplus \Delta S_{15} = 0$	0.0
I_{11}, I_{12}	$\Delta S_{10} \oplus \Delta S_{15} = 0$	0.0
I_{11}, I_{12}	$\Delta S_{12} \oplus \Delta S_{15} = 0$	0.0
I_{11}, I_{12}	$\Delta S_{13} \oplus \Delta S_{15} = 0$	0.0
I_{11}, I_{12}	$\Delta S_{14} \oplus \Delta S_{15} = 0$	0.0
I_{11}, I_{12}	$\Delta S_{15} \oplus \Delta S_{16} = 0$	0.0
I_{11}, I_{13}	$\Delta S_9 \oplus \Delta S_{13} = 0$	0.0
I_{11}, I_{13}	$\Delta S_{10} \oplus \Delta S_{13} = 0$	0.0
I_{11}, I_{13}	$\Delta S_{12} \oplus \Delta S_{13} = 0$	0.0
I_{11}, I_{13}	$\Delta S_{13} \oplus \Delta S_{14} = 0$	0.0
I_{11}, I_{13}	$\Delta S_{13} \oplus \Delta S_{15} = 0$	0.0
I_{11}, I_{14}	$\Delta S_9 \oplus \Delta S_{12} = 0$	0.0
I_{11}, I_{14}	$\Delta S_9 \oplus \Delta S_{13} = 0$	0.0
I_{11}, I_{14}	$\Delta S_9 \oplus \Delta S_{14} = 0$	0.0
I_{11}, I_{14}	$\Delta S_9 \oplus \Delta S_{15} = 0$	0.0

Table 16. Impossible differential attacks on 5 rounds.

Inputs	Condition	Result
I_{12}, I_{13}	$\Delta S_{10} \oplus \Delta S_{13} = 0$	0.0
I_{12}, I_{13}	$\Delta S_{10} \oplus \Delta S_{15} = 0$	0.0
I_{12}, I_{13}	$\Delta S_{12} \oplus \Delta S_{13} = 0$	0.0
I_{12}, I_{13}	$\Delta S_{12} \oplus \Delta S_{15} = 0$	0.0
I_{12}, I_{13}	$\Delta S_{13} \oplus \Delta S_{14} = 0$	0.0
I_{12}, I_{13}	$\Delta S_{14} \oplus \Delta S_{15} = 0$	0.0
I_{12}, I_{14}	$\Delta S_{9} \oplus \Delta S_{12} = 0$	0.0
I_{12}, I_{14}	$\Delta S_{9} \oplus \Delta S_{14} = 0$	0.0
I_{12}, I_{14}	$\Delta S_{10} \oplus \Delta S_{12} = 0$	0.0
I_{12}, I_{14}	$\Delta S_{10} \oplus \Delta S_{14} = 0$	0.0
I_{12}, I_{14}	$\Delta S_{12} \oplus \Delta S_{15} = 0$	0.0
I_{12}, I_{14}	$\Delta S_{12} \oplus \Delta S_{16} = 0$	0.0
I_{12}, I_{14}	$\Delta S_{14} \oplus \Delta S_{15} = 0$	0.0
I_{12}, I_{14}	$\Delta S_{14} \oplus \Delta S_{16} = 0$	0.0
I_{12}, I_{16}	$\Delta S_{10} \oplus \Delta S_{12} = 0$	0.0
I_{12}, I_{16}	$\Delta S_{10} \oplus \Delta S_{14} = 0$	0.0
I_{12}, I_{16}	$\Delta S_{10} \oplus \Delta S_{15} = 0$	0.0
I_{13}, I_{14}	$\Delta S_{9} \oplus \Delta S_{12} = 0$	0.0
I_{13}, I_{14}	$\Delta S_{9} \oplus \Delta S_{14} = 0$	0.0
I_{13}, I_{14}	$\Delta S_{10} \oplus \Delta S_{12} = 0$	0.0
I_{13}, I_{14}	$\Delta S_{10} \oplus \Delta S_{14} = 0$	0.0
I_{13}, I_{14}	$\Delta S_{12} \oplus \Delta S_{13} = 0$	0.0
I_{13}, I_{14}	$\Delta S_{13} \oplus \Delta S_{14} = 0$	0.0
I_{13}, I_{16}	$\Delta S_{10} \oplus \Delta S_{12} = 0$	0.0
I_{13}, I_{16}	$\Delta S_{10} \oplus \Delta S_{13} = 0$	0.0
I_{13}, I_{16}	$\Delta S_{10} \oplus \Delta S_{14} = 0$	0.0

Table 17. Differential attacks on 5 rounds.

Inputs	Condition	Result
I_9, I_{10}	$\Delta S_9 \oplus \Delta S_{16} = 0$	542.59
I_9, I_{10}	$\Delta S_{10} \oplus \Delta S_{16} = 0$	542.59
I_9, I_{10}	$\Delta S_{11} \oplus \Delta S_{12} = 0$	1,284.936
I_9, I_{10}	$\Delta S_{11} \oplus \Delta S_{14} = 0$	615.462
I_9, I_{10}	$\Delta S_{11} \oplus \Delta S_{15} = 0$	616.796
I_9, I_{10}	$\Delta S_{12} \oplus \Delta S_{13} = 0$	550.578
I_9, I_{10}	$\Delta S_{12} \oplus \Delta S_{14} = 0$	1,276.944
I_9, I_{10}	$\Delta S_{12} \oplus \Delta S_{15} = 0$	1,284.72
I_9, I_{10}	$\Delta S_{13} \oplus \Delta S_{14} = 0$	550.61
I_9, I_{10}	$\Delta S_{13} \oplus \Delta S_{15} = 0$	551.39
I_9, I_{10}	$\Delta S_{14} \oplus \Delta S_{15} = 0$	1,282.128
I_9, I_{11}	$\Delta S_9 \oplus \Delta S_{11} = 0$	1,743.32
I_9, I_{11}	$\Delta S_9 \oplus \Delta S_{12} = 0$	550.684
I_9, I_{11}	$\Delta S_9 \oplus \Delta S_{16} = 0$	543.678
I_9, I_{11}	$\Delta S_{10} \oplus \Delta S_{14} = 0$	1,278.672
I_9, I_{11}	$\Delta S_{10} \oplus \Delta S_{15} = 0$	1,252.536
I_9, I_{11}	$\Delta S_{11} \oplus \Delta S_{13} = 0$	1,743.32
I_9, I_{11}	$\Delta S_{12} \oplus \Delta S_{13} = 0$	550.684
I_9, I_{11}	$\Delta S_{13} \oplus \Delta S_{16} = 0$	543.678
I_9, I_{11}	$\Delta S_{14} \oplus \Delta S_{15} = 0$	1,282.344
I_9, I_{12}	$\Delta S_9 \oplus \Delta S_{12} = 0$	1,271.76
I_9, I_{12}	$\Delta S_9 \oplus \Delta S_{13} = 0$	1,252.968
I_9, I_{12}	$\Delta S_9 \oplus \Delta S_{15} = 0$	1,278.024
I_9, I_{12}	$\Delta S_9 \oplus \Delta S_{16} = 0$	550.794
I_9, I_{12}	$\Delta S_{10} \oplus \Delta S_{11} = 0$	1,053.244
I_9, I_{12}	$\Delta S_{11} \oplus \Delta S_{14} = 0$	1,053.244
I_9, I_{12}	$\Delta S_{12} \oplus \Delta S_{13} = 0$	1,260.96
I_9, I_{12}	$\Delta S_{12} \oplus \Delta S_{15} = 0$	1,271.76
I_9, I_{12}	$\Delta S_{12} \oplus \Delta S_{16} = 0$	595.752
I_9, I_{12}	$\Delta S_{13} \oplus \Delta S_{15} = 0$	1,281.696
I_9, I_{12}	$\Delta S_{13} \oplus \Delta S_{16} = 0$	550.948
I_9, I_{12}	$\Delta S_{15} \oplus \Delta S_{16} = 0$	551.776
I_9, I_{13}	$\Delta S_9 \oplus \Delta S_{12} = 0$	549.68
I_9, I_{13}	$\Delta S_{10} \oplus \Delta S_{11} = 0$	1,744.92
I_9, I_{13}	$\Delta S_{10} \oplus \Delta S_{15} = 0$	1,270.464
I_9, I_{13}	$\Delta S_{11} \oplus \Delta S_{13} = 0$	1,744.92
I_9, I_{13}	$\Delta S_{11} \oplus \Delta S_{14} = 0$	1,744.92
I_9, I_{13}	$\Delta S_{11} \oplus \Delta S_{15} = 0$	610.29
I_9, I_{13}	$\Delta S_{13} \oplus \Delta S_{15} = 0$	1,270.464
I_9, I_{13}	$\Delta S_{14} \oplus \Delta S_{15} = 0$	1,270.464

Inputs	Condition	Result
I_9, I_{14}	$\Delta S_9 \oplus \Delta S_{11} = 0$	1,734.96
I_9, I_{14}	$\Delta S_9 \oplus \Delta S_{15} = 0$	594.91
I_9, I_{14}	$\Delta S_9 \oplus \Delta S_{16} = 0$	543.972
I_9, I_{14}	$\Delta S_{10} \oplus \Delta S_{12} = 0$	1,273.272
I_9, I_{14}	$\Delta S_{10} \oplus \Delta S_{13} = 0$	1,286.664
I_9, I_{14}	$\Delta S_{11} \oplus \Delta S_{14} = 0$	1,734.96
I_9, I_{14}	$\Delta S_{12} \oplus \Delta S_{13} = 0$	1,256.856
I_9, I_{14}	$\Delta S_{14} \oplus \Delta S_{15} = 0$	594.91
I_9, I_{14}	$\Delta S_{14} \oplus \Delta S_{16} = 0$	543.972
I_9, I_{15}	$\Delta S_9 \oplus \Delta S_{10} = 0$	1,057.336
I_9, I_{15}	$\Delta S_9 \oplus \Delta S_{12} = 0$	666.698
I_9, I_{15}	$\Delta S_9 \oplus \Delta S_{13} = 0$	1,728.196
I_9, I_{15}	$\Delta S_9 \oplus \Delta S_{14} = 0$	1,738.81
I_9, I_{15}	$\Delta S_{10} \oplus \Delta S_{12} = 0$	562.01
I_9, I_{15}	$\Delta S_{10} \oplus \Delta S_{13} = 0$	1,055.428
I_9, I_{15}	$\Delta S_{10} \oplus \Delta S_{14} = 0$	1,056.176
I_9, I_{15}	$\Delta S_{12} \oplus \Delta S_{13} = 0$	667.754
I_9, I_{15}	$\Delta S_{12} \oplus \Delta S_{14} = 0$	666.358
I_9, I_{15}	$\Delta S_{13} \oplus \Delta S_{14} = 0$	1,738.462
I_9, I_{16}	$\Delta S_{10} \oplus \Delta S_{11} = 0$	902.446
I_9, I_{16}	$\Delta S_{10} \oplus \Delta S_{15} = 0$	544.0
I_9, I_{16}	$\Delta S_{13} \oplus \Delta S_{14} = 0$	543.22
I_{10}, I_{11}	$\Delta S_9 \oplus \Delta S_{14} = 0$	1,268.304
I_{10}, I_{11}	$\Delta S_9 \oplus \Delta S_{16} = 0$	611.888
I_{10}, I_{11}	$\Delta S_{10} \oplus \Delta S_{11} = 0$	611.288
I_{10}, I_{11}	$\Delta S_{10} \oplus \Delta S_{12} = 0$	551.35
I_{10}, I_{11}	$\Delta S_{10} \oplus \Delta S_{13} = 0$	550.92
I_{10}, I_{11}	$\Delta S_{12} \oplus \Delta S_{13} = 0$	551.252
I_{10}, I_{11}	$\Delta S_{14} \oplus \Delta S_{15} = 0$	1,268.304
I_{10}, I_{11}	$\Delta S_{15} \oplus \Delta S_{16} = 0$	611.888
I_{10}, I_{12}	$\Delta S_9 \oplus \Delta S_{11} = 0$	565.622
I_{10}, I_{12}	$\Delta S_9 \oplus \Delta S_{14} = 0$	1,279.536
I_{10}, I_{12}	$\Delta S_{10} \oplus \Delta S_{13} = 0$	550.596
I_{10}, I_{12}	$\Delta S_{11} \oplus \Delta S_{14} = 0$	563.856
I_{10}, I_{12}	$\Delta S_{12} \oplus \Delta S_{13} = 0$	550.596
I_{10}, I_{12}	$\Delta S_{13} \oplus \Delta S_{15} = 0$	550.596
I_{10}, I_{13}	$\Delta S_9 \oplus \Delta S_{13} = 0$	550.608
I_{10}, I_{13}	$\Delta S_9 \oplus \Delta S_{14} = 0$	550.912
I_{10}, I_{13}	$\Delta S_9 \oplus \Delta S_{15} = 0$	596.804
I_{10}, I_{13}	$\Delta S_{11} \oplus \Delta S_{14} = 0$	610.154

Table 18. Differential attacks on 5 rounds.

Inputs	Condition	Result
I_{10}, I_{13}	$\Delta S_{11} \oplus \Delta S_{15} = 0$	1,270.896
I_{10}, I_{13}	$\Delta S_{13} \oplus \Delta S_{14} = 0$	550.548
I_{10}, I_{13}	$\Delta S_{13} \oplus \Delta S_{15} = 0$	550.54
I_{10}, I_{13}	$\Delta S_{14} \oplus \Delta S_{15} = 0$	1,265.928
I_{10}, I_{14}	$\Delta S_{9} \oplus \Delta S_{13} = 0$	594.642
I_{10}, I_{14}	$\Delta S_{9} \oplus \Delta S_{16} = 0$	611.952
I_{10}, I_{14}	$\Delta S_{10} \oplus \Delta S_{11} = 0$	1,283.208
I_{10}, I_{14}	$\Delta S_{10} \oplus \Delta S_{14} = 0$	1,267.224
I_{10}, I_{14}	$\Delta S_{10} \oplus \Delta S_{15} = 0$	593.402
I_{10}, I_{14}	$\Delta S_{11} \oplus \Delta S_{14} = 0$	613.168
I_{10}, I_{14}	$\Delta S_{12} \oplus \Delta S_{13} = 0$	594.642
I_{10}, I_{14}	$\Delta S_{12} \oplus \Delta S_{16} = 0$	611.952
I_{10}, I_{14}	$\Delta S_{14} \oplus \Delta S_{15} = 0$	552.278
I_{10}, I_{15}	$\Delta S_{9} \oplus \Delta S_{10} = 0$	1,054.44
I_{10}, I_{15}	$\Delta S_{9} \oplus \Delta S_{15} = 0$	1,741.32
I_{10}, I_{15}	$\Delta S_{10} \oplus \Delta S_{15} = 0$	1,056.38
I_{10}, I_{15}	$\Delta S_{11} \oplus \Delta S_{16} = 0$	566.092
I_{10}, I_{15}	$\Delta S_{12} \oplus \Delta S_{14} = 0$	1,279.32
I_{10}, I_{16}	$\Delta S_{10} \oplus \Delta S_{13} = 0$	544.0
I_{10}, I_{16}	$\Delta S_{10} \oplus \Delta S_{14} = 0$	596.114
I_{10}, I_{16}	$\Delta S_{12} \oplus \Delta S_{15} = 0$	613.966
I_{11}, I_{12}	$\Delta S_{9} \oplus \Delta S_{10} = 0$	1,266.36
I_{11}, I_{12}	$\Delta S_{9} \oplus \Delta S_{12} = 0$	551.74
I_{11}, I_{12}	$\Delta S_{9} \oplus \Delta S_{13} = 0$	1,268.304
I_{11}, I_{12}	$\Delta S_{9} \oplus \Delta S_{14} = 0$	1,273.704
I_{11}, I_{12}	$\Delta S_{10} \oplus \Delta S_{12} = 0$	550.054
I_{11}, I_{12}	$\Delta S_{10} \oplus \Delta S_{13} = 0$	1,282.56
I_{11}, I_{12}	$\Delta S_{10} \oplus \Delta S_{14} = 0$	1,280.616
I_{11}, I_{12}	$\Delta S_{11} \oplus \Delta S_{15} = 0$	1,051.468
I_{11}, I_{12}	$\Delta S_{12} \oplus \Delta S_{13} = 0$	548.646
I_{11}, I_{12}	$\Delta S_{12} \oplus \Delta S_{14} = 0$	595.28
I_{11}, I_{12}	$\Delta S_{12} \oplus \Delta S_{16} = 0$	544.0
I_{11}, I_{12}	$\Delta S_{13} \oplus \Delta S_{14} = 0$	1,248.648
I_{11}, I_{12}	$\Delta S_{14} \oplus \Delta S_{16} = 0$	544.0
I_{11}, I_{13}	$\Delta S_{9} \oplus \Delta S_{10} = 0$	550.208
I_{11}, I_{13}	$\Delta S_{9} \oplus \Delta S_{12} = 0$	549.644
I_{11}, I_{13}	$\Delta S_{9} \oplus \Delta S_{14} = 0$	550.648
I_{11}, I_{13}	$\Delta S_{9} \oplus \Delta S_{15} = 0$	595.88
I_{11}, I_{13}	$\Delta S_{10} \oplus \Delta S_{12} = 0$	550.288
I_{11}, I_{13}	$\Delta S_{10} \oplus \Delta S_{14} = 0$	1,266.144

Inputs	Condition	Result
I_{11}, I_{13}	$\Delta S_{10} \oplus \Delta S_{15} = 0$	1,265.496
I_{11}, I_{13}	$\Delta S_{11} \oplus \Delta S_{13} = 0$	1,719.88
I_{11}, I_{13}	$\Delta S_{12} \oplus \Delta S_{14} = 0$	593.428
I_{11}, I_{13}	$\Delta S_{12} \oplus \Delta S_{15} = 0$	550.316
I_{11}, I_{13}	$\Delta S_{14} \oplus \Delta S_{15} = 0$	1,262.472
I_{11}, I_{14}	$\Delta S_{9} \oplus \Delta S_{10} = 0$	1,285.8
I_{11}, I_{14}	$\Delta S_{9} \oplus \Delta S_{11} = 0$	1,725.328
I_{11}, I_{14}	$\Delta S_{9} \oplus \Delta S_{16} = 0$	610.24
I_{11}, I_{14}	$\Delta S_{10} \oplus \Delta S_{11} = 0$	617.944
I_{11}, I_{14}	$\Delta S_{11} \oplus \Delta S_{16} = 0$	612.464
I_{11}, I_{14}	$\Delta S_{12} \oplus \Delta S_{13} = 0$	551.284
I_{11}, I_{14}	$\Delta S_{12} \oplus \Delta S_{14} = 0$	595.708
I_{11}, I_{14}	$\Delta S_{12} \oplus \Delta S_{15} = 0$	551.876
I_{11}, I_{14}	$\Delta S_{13} \oplus \Delta S_{14} = 0$	1,285.8
I_{11}, I_{14}	$\Delta S_{13} \oplus \Delta S_{15} = 0$	550.746
I_{11}, I_{14}	$\Delta S_{14} \oplus \Delta S_{15} = 0$	550.956
I_{11}, I_{15}	$\Delta S_{9} \oplus \Delta S_{13} = 0$	1,744.06
I_{11}, I_{15}	$\Delta S_{9} \oplus \Delta S_{15} = 0$	1,730.04
I_{11}, I_{15}	$\Delta S_{10} \oplus \Delta S_{14} = 0$	567.802
I_{11}, I_{15}	$\Delta S_{13} \oplus \Delta S_{15} = 0$	1,723.052
I_{11}, I_{16}	$\Delta S_{13} \oplus \Delta S_{15} = 0$	616.944
I_{12}, I_{13}	$\Delta S_{9} \oplus \Delta S_{10} = 0$	593.886
I_{12}, I_{13}	$\Delta S_{9} \oplus \Delta S_{12} = 0$	593.886
I_{12}, I_{13}	$\Delta S_{9} \oplus \Delta S_{14} = 0$	593.886
I_{12}, I_{13}	$\Delta S_{10} \oplus \Delta S_{11} = 0$	1,051.278
I_{12}, I_{13}	$\Delta S_{11} \oplus \Delta S_{12} = 0$	1,051.278
I_{12}, I_{13}	$\Delta S_{11} \oplus \Delta S_{14} = 0$	1,051.278
I_{12}, I_{13}	$\Delta S_{13} \oplus \Delta S_{15} = 0$	1,262.904
I_{12}, I_{13}	$\Delta S_{15} \oplus \Delta S_{16} = 0$	575.986
I_{12}, I_{14}	$\Delta S_{9} \oplus \Delta S_{10} = 0$	1,255.56
I_{12}, I_{14}	$\Delta S_{9} \oplus \Delta S_{15} = 0$	550.276
I_{12}, I_{14}	$\Delta S_{10} \oplus \Delta S_{15} = 0$	592.83
I_{12}, I_{14}	$\Delta S_{10} \oplus \Delta S_{16} = 0$	544.0
I_{12}, I_{14}	$\Delta S_{11} \oplus \Delta S_{12} = 0$	1,052.232
I_{12}, I_{14}	$\Delta S_{11} \oplus \Delta S_{13} = 0$	564.396
I_{12}, I_{14}	$\Delta S_{11} \oplus \Delta S_{14} = 0$	1,052.232
I_{12}, I_{14}	$\Delta S_{12} \oplus \Delta S_{13} = 0$	1,274.568
I_{12}, I_{14}	$\Delta S_{13} \oplus \Delta S_{14} = 0$	1,274.568
I_{12}, I_{14}	$\Delta S_{15} \oplus \Delta S_{16} = 0$	544.0
I_{12}, I_{15}	$\Delta S_{9} \oplus \Delta S_{12} = 0$	1,262.904

Table 19. Differential attacks on 5 rounds.

Inputs	Condition	Result
I_{12}, I_{15}	$\Delta S_9 \oplus \Delta S_{13} = 0$	665.692
I_{12}, I_{15}	$\Delta S_{10} \oplus \Delta S_{14} = 0$	1,053.13
I_{12}, I_{15}	$\Delta S_{10} \oplus \Delta S_{15} = 0$	1,055.476
I_{12}, I_{15}	$\Delta S_{10} \oplus \Delta S_{16} = 0$	972.51
I_{12}, I_{15}	$\Delta S_{11} \oplus \Delta S_{16} = 0$	559.624
I_{12}, I_{15}	$\Delta S_{12} \oplus \Delta S_{13} = 0$	666.406
I_{12}, I_{15}	$\Delta S_{14} \oplus \Delta S_{15} = 0$	1,735.592
I_{12}, I_{15}	$\Delta S_{14} \oplus \Delta S_{16} = 0$	900.544
I_{12}, I_{15}	$\Delta S_{15} \oplus \Delta S_{16} = 0$	900.472
I_{12}, I_{16}	$\Delta S_9 \oplus \Delta S_{10} = 0$	561.768
I_{12}, I_{16}	$\Delta S_{10} \oplus \Delta S_{11} = 0$	963.714
I_{12}, I_{16}	$\Delta S_{12} \oplus \Delta S_{14} = 0$	542.272
I_{12}, I_{16}	$\Delta S_{12} \oplus \Delta S_{15} = 0$	613.964
I_{12}, I_{16}	$\Delta S_{14} \oplus \Delta S_{15} = 0$	544.13
I_{13}, I_{14}	$\Delta S_9 \oplus \Delta S_{10} = 0$	550.194
I_{13}, I_{14}	$\Delta S_9 \oplus \Delta S_{13} = 0$	550.898
I_{13}, I_{14}	$\Delta S_{10} \oplus \Delta S_{13} = 0$	1,281.48
I_{13}, I_{14}	$\Delta S_{11} \oplus \Delta S_{12} = 0$	1,740.224
I_{13}, I_{14}	$\Delta S_{11} \oplus \Delta S_{14} = 0$	1,740.224
I_{13}, I_{14}	$\Delta S_{12} \oplus \Delta S_{15} = 0$	550.844
I_{13}, I_{14}	$\Delta S_{14} \oplus \Delta S_{15} = 0$	550.844
I_{13}, I_{15}	$\Delta S_{10} \oplus \Delta S_{13} = 0$	1,054.164
I_{13}, I_{15}	$\Delta S_{10} \oplus \Delta S_{14} = 0$	1,052.654
I_{13}, I_{15}	$\Delta S_{12} \oplus \Delta S_{15} = 0$	664.048
I_{13}, I_{15}	$\Delta S_{13} \oplus \Delta S_{14} = 0$	1,713.588
I_{13}, I_{16}	$\Delta S_9 \oplus \Delta S_{10} = 0$	565.006
I_{13}, I_{16}	$\Delta S_{10} \oplus \Delta S_{11} = 0$	900.286
I_{13}, I_{16}	$\Delta S_{12} \oplus \Delta S_{13} = 0$	614.604
I_{13}, I_{16}	$\Delta S_{12} \oplus \Delta S_{14} = 0$	543.066
I_{13}, I_{16}	$\Delta S_{13} \oplus \Delta S_{14} = 0$	542.57
I_{14}, I_{15}	$\Delta S_9 \oplus \Delta S_{14} = 0$	1,744.13
I_{14}, I_{15}	$\Delta S_{10} \oplus \Delta S_{12} = 0$	561.934
I_{14}, I_{15}	$\Delta S_{10} \oplus \Delta S_{13} = 0$	564.562
I_{14}, I_{15}	$\Delta S_{12} \oplus \Delta S_{13} = 0$	1,275.216
I_{14}, I_{16}	$\Delta S_{10} \oplus \Delta S_{14} = 0$	550.886
I_{14}, I_{16}	$\Delta S_{12} \oplus \Delta S_{14} = 0$	543.868
I_{14}, I_{16}	$\Delta S_{13} \oplus \Delta S_{15} = 0$	558.836
I_{15}, I_{16}	$\Delta S_{10} \oplus \Delta S_{11} = 0$	562.682
I_{15}, I_{16}	$\Delta S_{11} \oplus \Delta S_{12} = 0$	564.098
I_{15}, I_{16}	$\Delta S_{13} \oplus \Delta S_{15} = 0$	626.906

Table 20. Improbable differential attacks on 5 rounds.

Inputs	Condition	Result
I_9, I_{10}	$\Delta S_9 \oplus \Delta S_{11} = 0$	456.406
I_9, I_{10}	$\Delta S_{10} \oplus \Delta S_{11} = 0$	456.406
I_9, I_{11}	$\Delta S_{10} \oplus \Delta S_{11} = 0$	427.664
I_9, I_{11}	$\Delta S_{10} \oplus \Delta S_{12} = 0$	459.68
I_9, I_{11}	$\Delta S_{11} \oplus \Delta S_{14} = 0$	455.106
I_9, I_{11}	$\Delta S_{11} \oplus \Delta S_{15} = 0$	428.986
I_9, I_{11}	$\Delta S_{12} \oplus \Delta S_{14} = 0$	456.43
I_9, I_{11}	$\Delta S_{12} \oplus \Delta S_{15} = 0$	460.224
I_9, I_{12}	$\Delta S_9 \oplus \Delta S_{11} = 0$	477.28
I_9, I_{12}	$\Delta S_{11} \oplus \Delta S_{13} = 0$	470.25
I_9, I_{12}	$\Delta S_{11} \oplus \Delta S_{15} = 0$	476.564
I_9, I_{12}	$\Delta S_{11} \oplus \Delta S_{16} = 0$	473.812
I_9, I_{13}	$\Delta S_9 \oplus \Delta S_{11} = 0$	426.94
I_9, I_{13}	$\Delta S_9 \oplus \Delta S_{15} = 0$	454.32
I_9, I_{13}	$\Delta S_{11} \oplus \Delta S_{12} = 0$	455.378
I_9, I_{13}	$\Delta S_{12} \oplus \Delta S_{15} = 0$	382.816
I_9, I_{14}	$\Delta S_{10} \oplus \Delta S_{11} = 0$	457.022
I_9, I_{14}	$\Delta S_{10} \oplus \Delta S_{15} = 0$	458.88
I_9, I_{14}	$\Delta S_{11} \oplus \Delta S_{12} = 0$	457.022
I_9, I_{14}	$\Delta S_{11} \oplus \Delta S_{13} = 0$	429.452
I_9, I_{14}	$\Delta S_{12} \oplus \Delta S_{15} = 0$	456.974
I_9, I_{14}	$\Delta S_{13} \oplus \Delta S_{15} = 0$	457.692
I_9, I_{15}	$\Delta S_9 \oplus \Delta S_{15} = 0$	453.836
I_9, I_{15}	$\Delta S_{12} \oplus \Delta S_{15} = 0$	455.466
I_9, I_{15}	$\Delta S_{13} \oplus \Delta S_{15} = 0$	452.946
I_9, I_{15}	$\Delta S_{14} \oplus \Delta S_{15} = 0$	453.876
I_{10}, I_{11}	$\Delta S_9 \oplus \Delta S_{11} = 0$	456.658
I_{10}, I_{11}	$\Delta S_{10} \oplus \Delta S_{14} = 0$	383.872
I_{10}, I_{11}	$\Delta S_{11} \oplus \Delta S_{14} = 0$	453.642
I_{10}, I_{11}	$\Delta S_{11} \oplus \Delta S_{15} = 0$	456.658
I_{10}, I_{11}	$\Delta S_{11} \oplus \Delta S_{16} = 0$	475.422
I_{10}, I_{11}	$\Delta S_{12} \oplus \Delta S_{14} = 0$	455.266
I_{10}, I_{11}	$\Delta S_{13} \oplus \Delta S_{14} = 0$	460.764
I_{10}, I_{12}	$\Delta S_9 \oplus \Delta S_{13} = 0$	459.58
I_{10}, I_{12}	$\Delta S_{13} \oplus \Delta S_{14} = 0$	458.946
I_{10}, I_{13}	$\Delta S_{10} \oplus \Delta S_{11} = 0$	456.836
I_{10}, I_{13}	$\Delta S_{11} \oplus \Delta S_{12} = 0$	456.836
I_{10}, I_{14}	$\Delta S_9 \oplus \Delta S_{11} = 0$	457.08
I_{10}, I_{14}	$\Delta S_{10} \oplus \Delta S_{13} = 0$	456.904
I_{10}, I_{14}	$\Delta S_{11} \oplus \Delta S_{12} = 0$	457.08
I_{10}, I_{14}	$\Delta S_{11} \oplus \Delta S_{16} = 0$	474.526
I_{10}, I_{14}	$\Delta S_{13} \oplus \Delta S_{14} = 0$	457.626
I_{10}, I_{15}	$\Delta S_9 \oplus \Delta S_{12} = 0$	453.456
I_{10}, I_{15}	$\Delta S_9 \oplus \Delta S_{13} = 0$	427.922
I_{10}, I_{15}	$\Delta S_9 \oplus \Delta S_{14} = 0$	452.084
I_{10}, I_{15}	$\Delta S_{10} \oplus \Delta S_{11} = 0$	473.66
I_{10}, I_{15}	$\Delta S_{10} \oplus \Delta S_{13} = 0$	474.326
I_{10}, I_{15}	$\Delta S_{12} \oplus \Delta S_{15} = 0$	452.492
I_{10}, I_{15}	$\Delta S_{13} \oplus \Delta S_{15} = 0$	426.356
I_{10}, I_{15}	$\Delta S_{14} \oplus \Delta S_{15} = 0$	452.268
I_{10}, I_{16}	$\Delta S_{10} \oplus \Delta S_{11} = 0$	431.544
I_{11}, I_{12}	$\Delta S_9 \oplus \Delta S_{11} = 0$	476.908
I_{11}, I_{12}	$\Delta S_{10} \oplus \Delta S_{11} = 0$	474.896
I_{11}, I_{12}	$\Delta S_{11} \oplus \Delta S_{12} = 0$	474.328
I_{11}, I_{12}	$\Delta S_{11} \oplus \Delta S_{13} = 0$	470.094
I_{11}, I_{13}	$\Delta S_9 \oplus \Delta S_{11} = 0$	430.764
I_{11}, I_{13}	$\Delta S_{10} \oplus \Delta S_{11} = 0$	429.96
I_{11}, I_{13}	$\Delta S_{11} \oplus \Delta S_{12} = 0$	429.842
I_{11}, I_{13}	$\Delta S_{11} \oplus \Delta S_{14} = 0$	458.144
I_{11}, I_{13}	$\Delta S_{11} \oplus \Delta S_{15} = 0$	458.144
I_{11}, I_{14}	$\Delta S_{10} \oplus \Delta S_{12} = 0$	459.376
I_{11}, I_{14}	$\Delta S_{10} \oplus \Delta S_{13} = 0$	381.808
I_{11}, I_{14}	$\Delta S_{10} \oplus \Delta S_{14} = 0$	380.128
I_{11}, I_{14}	$\Delta S_{10} \oplus \Delta S_{15} = 0$	453.502
I_{11}, I_{14}	$\Delta S_{11} \oplus \Delta S_{12} = 0$	428.66
I_{11}, I_{14}	$\Delta S_{11} \oplus \Delta S_{13} = 0$	429.124
I_{11}, I_{14}	$\Delta S_{11} \oplus \Delta S_{14} = 0$	457.298
I_{11}, I_{14}	$\Delta S_{11} \oplus \Delta S_{15} = 0$	429.524
I_{11}, I_{15}	$\Delta S_9 \oplus \Delta S_{10} = 0$	468.954
I_{11}, I_{15}	$\Delta S_9 \oplus \Delta S_{14} = 0$	432.018
I_{11}, I_{15}	$\Delta S_{10} \oplus \Delta S_{13} = 0$	468.918
I_{11}, I_{15}	$\Delta S_{10} \oplus \Delta S_{15} = 0$	468.61
I_{11}, I_{15}	$\Delta S_{13} \oplus \Delta S_{14} = 0$	429.128
I_{11}, I_{15}	$\Delta S_{14} \oplus \Delta S_{15} = 0$	428.412
I_{11}, I_{16}	$\Delta S_{10} \oplus \Delta S_{11} = 0$	470.666
I_{11}, I_{16}	$\Delta S_{10} \oplus \Delta S_{14} = 0$	461.568
I_{12}, I_{13}	$\Delta S_9 \oplus \Delta S_{13} = 0$	455.984
I_{12}, I_{13}	$\Delta S_9 \oplus \Delta S_{15} = 0$	461.136
I_{12}, I_{13}	$\Delta S_{11} \oplus \Delta S_{13} = 0$	471.014
I_{12}, I_{14}	$\Delta S_9 \oplus \Delta S_{11} = 0$	476.81

Table 21. Improbable differential attacks on 5 rounds.

Inputs	Condition	Result
I_{12}, I_{14}	$\Delta S_9 \oplus \Delta S_{13} = 0$	383.504
I_{12}, I_{14}	$\Delta S_{10} \oplus \Delta S_{13} = 0$	383.68
I_{12}, I_{14}	$\Delta S_{11} \oplus \Delta S_{15} = 0$	473.448
I_{12}, I_{14}	$\Delta S_{13} \oplus \Delta S_{15} = 0$	460.536
I_{12}, I_{14}	$\Delta S_{13} \oplus \Delta S_{16} = 0$	458.422
I_{12}, I_{15}	$\Delta S_9 \oplus \Delta S_{11} = 0$	477.23
I_{12}, I_{15}	$\Delta S_9 \oplus \Delta S_{14} = 0$	451.714
I_{12}, I_{15}	$\Delta S_9 \oplus \Delta S_{15} = 0$	452.648
I_{12}, I_{15}	$\Delta S_9 \oplus \Delta S_{16} = 0$	431.954
I_{12}, I_{15}	$\Delta S_{10} \oplus \Delta S_{13} = 0$	474.572
I_{12}, I_{15}	$\Delta S_{11} \oplus \Delta S_{12} = 0$	476.134
I_{12}, I_{15}	$\Delta S_{12} \oplus \Delta S_{14} = 0$	453.04
I_{12}, I_{15}	$\Delta S_{12} \oplus \Delta S_{15} = 0$	452.112
I_{12}, I_{15}	$\Delta S_{12} \oplus \Delta S_{16} = 0$	432.952
I_{12}, I_{15}	$\Delta S_{13} \oplus \Delta S_{14} = 0$	428.988
I_{12}, I_{15}	$\Delta S_{13} \oplus \Delta S_{15} = 0$	427.398
I_{12}, I_{15}	$\Delta S_{13} \oplus \Delta S_{16} = 0$	471.12
I_{13}, I_{14}	$\Delta S_9 \oplus \Delta S_{11} = 0$	426.906
I_{13}, I_{14}	$\Delta S_{10} \oplus \Delta S_{11} = 0$	457.886
I_{13}, I_{14}	$\Delta S_{10} \oplus \Delta S_{15} = 0$	453.848
I_{13}, I_{14}	$\Delta S_{11} \oplus \Delta S_{13} = 0$	428.98
I_{13}, I_{14}	$\Delta S_{13} \oplus \Delta S_{15} = 0$	459.242
I_{13}, I_{15}	$\Delta S_9 \oplus \Delta S_{10} = 0$	472.576
I_{13}, I_{15}	$\Delta S_9 \oplus \Delta S_{13} = 0$	426.866
I_{13}, I_{15}	$\Delta S_9 \oplus \Delta S_{14} = 0$	427.7
I_{13}, I_{15}	$\Delta S_{10} \oplus \Delta S_{15} = 0$	473.606
I_{13}, I_{15}	$\Delta S_{12} \oplus \Delta S_{13} = 0$	451.614
I_{13}, I_{15}	$\Delta S_{12} \oplus \Delta S_{14} = 0$	452.74
I_{13}, I_{15}	$\Delta S_{13} \oplus \Delta S_{15} = 0$	430.478
I_{13}, I_{15}	$\Delta S_{14} \oplus \Delta S_{15} = 0$	429.422
I_{14}, I_{15}	$\Delta S_9 \oplus \Delta S_{10} = 0$	473.934
I_{14}, I_{15}	$\Delta S_9 \oplus \Delta S_{12} = 0$	452.584
I_{14}, I_{15}	$\Delta S_9 \oplus \Delta S_{13} = 0$	452.326
I_{14}, I_{15}	$\Delta S_9 \oplus \Delta S_{15} = 0$	425.86
I_{14}, I_{15}	$\Delta S_{10} \oplus \Delta S_{11} = 0$	472.896
I_{14}, I_{15}	$\Delta S_{10} \oplus \Delta S_{14} = 0$	473.216
I_{14}, I_{15}	$\Delta S_{12} \oplus \Delta S_{14} = 0$	453.174
I_{14}, I_{15}	$\Delta S_{13} \oplus \Delta S_{14} = 0$	452.394
I_{14}, I_{15}	$\Delta S_{14} \oplus \Delta S_{15} = 0$	425.856
I_{14}, I_{16}	$\Delta S_{10} \oplus \Delta S_{11} = 0$	432.282
I_{14}, I_{16}	$\Delta S_{10} \oplus \Delta S_{13} = 0$	455.698
I_{15}, I_{16}	$\Delta S_{10} \oplus \Delta S_{14} = 0$	472.974

Table 22. Differential attacks on 6 rounds.

Inputs	Condition	Result
I_9, I_{10}	$\Delta S_9 \oplus \Delta S_{10} = 0$	587.834
I_9, I_{10}	$\Delta S_9 \oplus \Delta S_{14} = 0$	590.538
I_9, I_{10}	$\Delta S_{10} \oplus \Delta S_{14} = 0$	637.662
I_9, I_{11}	$\Delta S_{10} \oplus \Delta S_{12} = 0$	1,744.584
I_9, I_{12}	$\Delta S_9 \oplus \Delta S_{12} = 0$	584.23
I_9, I_{12}	$\Delta S_9 \oplus \Delta S_{15} = 0$	587.71
I_9, I_{12}	$\Delta S_{12} \oplus \Delta S_{15} = 0$	625.994
I_9, I_{13}	$\Delta S_9 \oplus \Delta S_{10} = 0$	588.014
I_9, I_{13}	$\Delta S_{12} \oplus \Delta S_{14} = 0$	2,336.416
I_9, I_{14}	$\Delta S_9 \oplus \Delta S_{12} = 0$	588.802
I_9, I_{14}	$\Delta S_{10} \oplus \Delta S_{15} = 0$	1,731.616
I_9, I_{15}	$\Delta S_{12} \oplus \Delta S_{14} = 0$	565.276
I_{10}, I_{11}	$\Delta S_{10} \oplus \Delta S_{15} = 0$	623.274
I_{10}, I_{11}	$\Delta S_{11} \oplus \Delta S_{13} = 0$	679.866
I_{10}, I_{12}	$\Delta S_9 \oplus \Delta S_{13} = 0$	1,722.962
I_{10}, I_{13}	$\Delta S_9 \oplus \Delta S_{10} = 0$	625.052
I_{10}, I_{13}	$\Delta S_9 \oplus \Delta S_{11} = 0$	561.728
I_{10}, I_{14}	$\Delta S_9 \oplus \Delta S_{15} = 0$	2,364.232
I_{11}, I_{12}	$\Delta S_{12} \oplus \Delta S_{14} = 0$	625.882
I_{11}, I_{13}	$\Delta S_{11} \oplus \Delta S_{12} = 0$	562.106
I_{11}, I_{14}	$\Delta S_{11} \oplus \Delta S_{15} = 0$	638.076
I_{11}, I_{15}	$\Delta S_{12} \oplus \Delta S_{13} = 0$	671.91
I_{12}, I_{13}	$\Delta S_9 \oplus \Delta S_{14} = 0$	1,736.72
I_{12}, I_{13}	$\Delta S_{10} \oplus \Delta S_{13} = 0$	556.906
I_{12}, I_{13}	$\Delta S_{10} \oplus \Delta S_{15} = 0$	559.664
I_{12}, I_{14}	$\Delta S_9 \oplus \Delta S_{12} = 0$	633.65
I_{12}, I_{15}	$\Delta S_{13} \oplus \Delta S_{14} = 0$	565.65
I_{13}, I_{15}	$\Delta S_{12} \oplus \Delta S_{14} = 0$	566.012

Table 23. Improbable differential attacks on 6 rounds.

Inputs	Condition	Result
I_9, I_{10}	$\Delta S_9 \oplus \Delta S_{15} = 0$	413.818
I_9, I_{10}	$\Delta S_{10} \oplus \Delta S_{15} = 0$	431.676
I_9, I_{10}	$\Delta S_{14} \oplus \Delta S_{15} = 0$	392.032
I_9, I_{11}	$\Delta S_{10} \oplus \Delta S_{14} = 0$	432.738
I_9, I_{11}	$\Delta S_{10} \oplus \Delta S_{15} = 0$	429.832
I_9, I_{11}	$\Delta S_{12} \oplus \Delta S_{14} = 0$	389.782
I_9, I_{11}	$\Delta S_{12} \oplus \Delta S_{15} = 0$	388.614
I_9, I_{12}	$\Delta S_9 \oplus \Delta S_{14} = 0$	458.15
I_9, I_{12}	$\Delta S_{10} \oplus \Delta S_{14} = 0$	472.758
I_9, I_{12}	$\Delta S_{12} \oplus \Delta S_{14} = 0$	431.422
I_9, I_{12}	$\Delta S_{14} \oplus \Delta S_{15} = 0$	432.224
I_9, I_{13}	$\Delta S_9 \oplus \Delta S_{12} = 0$	413.908
I_9, I_{13}	$\Delta S_9 \oplus \Delta S_{14} = 0$	413.084
I_9, I_{13}	$\Delta S_{10} \oplus \Delta S_{12} = 0$	431.656
I_9, I_{13}	$\Delta S_{10} \oplus \Delta S_{14} = 0$	431.802
I_9, I_{13}	$\Delta S_{12} \oplus \Delta S_{15} = 0$	387.35
I_9, I_{13}	$\Delta S_{14} \oplus \Delta S_{15} = 0$	388.41
I_9, I_{14}	$\Delta S_9 \oplus \Delta S_{10} = 0$	460.36
I_9, I_{14}	$\Delta S_9 \oplus \Delta S_{15} = 0$	414.122
I_9, I_{14}	$\Delta S_{10} \oplus \Delta S_{12} = 0$	434.114
I_9, I_{14}	$\Delta S_{12} \oplus \Delta S_{15} = 0$	391.38
I_{10}, I_{11}	$\Delta S_{10} \oplus \Delta S_{13} = 0$	431.58
I_{10}, I_{11}	$\Delta S_{13} \oplus \Delta S_{15} = 0$	391.014
I_{10}, I_{12}	$\Delta S_9 \oplus \Delta S_{14} = 0$	435.314
I_{10}, I_{12}	$\Delta S_9 \oplus \Delta S_{15} = 0$	430.81
I_{10}, I_{12}	$\Delta S_{13} \oplus \Delta S_{14} = 0$	432.612

Inputs	Condition	Result
I_{10}, I_{12}	$\Delta S_{13} \oplus \Delta S_{15} = 0$	431.518
I_{10}, I_{13}	$\Delta S_9 \oplus \Delta S_{14} = 0$	391.92
I_{10}, I_{13}	$\Delta S_9 \oplus \Delta S_{15} = 0$	388.426
I_{10}, I_{14}	$\Delta S_9 \oplus \Delta S_{10} = 0$	430.186
I_{10}, I_{14}	$\Delta S_9 \oplus \Delta S_{13} = 0$	386.47
I_{10}, I_{14}	$\Delta S_{10} \oplus \Delta S_{15} = 0$	430.984
I_{10}, I_{14}	$\Delta S_{13} \oplus \Delta S_{15} = 0$	386.146
I_{11}, I_{12}	$\Delta S_9 \oplus \Delta S_{10} = 0$	473.87
I_{11}, I_{12}	$\Delta S_{10} \oplus \Delta S_{13} = 0$	473.644
I_{11}, I_{12}	$\Delta S_{12} \oplus \Delta S_{13} = 0$	431.702
I_{11}, I_{12}	$\Delta S_{13} \oplus \Delta S_{14} = 0$	432.164
I_{11}, I_{13}	$\Delta S_{10} \oplus \Delta S_{12} = 0$	432.768
I_{11}, I_{13}	$\Delta S_{12} \oplus \Delta S_{14} = 0$	391.322
I_{11}, I_{14}	$\Delta S_{10} \oplus \Delta S_{12} = 0$	434.188
I_{11}, I_{14}	$\Delta S_{10} \oplus \Delta S_{13} = 0$	430.098
I_{11}, I_{14}	$\Delta S_{10} \oplus \Delta S_{15} = 0$	433.2
I_{12}, I_{13}	$\Delta S_9 \oplus \Delta S_{12} = 0$	432.092
I_{12}, I_{13}	$\Delta S_{12} \oplus \Delta S_{14} = 0$	432.376
I_{12}, I_{14}	$\Delta S_9 \oplus \Delta S_{10} = 0$	473.888
I_{12}, I_{14}	$\Delta S_9 \oplus \Delta S_{13} = 0$	426.554
I_{12}, I_{14}	$\Delta S_9 \oplus \Delta S_{15} = 0$	431.738
I_{12}, I_{15}	$\Delta S_{10} \oplus \Delta S_{15} = 0$	474.674
I_{13}, I_{14}	$\Delta S_9 \oplus \Delta S_{10} = 0$	430.32
I_{13}, I_{14}	$\Delta S_9 \oplus \Delta S_{12} = 0$	391.266
I_{13}, I_{14}	$\Delta S_9 \oplus \Delta S_{15} = 0$	387.298
I_{14}, I_{15}	$\Delta S_{14} \oplus \Delta S_{15} = 0$	474.544

Table 24. Differential attacks on 7 rounds.

Inputs	Condition	Result
I_9, I_{11}	$\Delta S_9 \oplus \Delta S_{13} = 0$	131,738.9
I_9, I_{13}	$\Delta S_9 \oplus \Delta S_{10} = 0$	133,707.05
I_9, I_{13}	$\Delta S_9 \oplus \Delta S_{12} = 0$	131,796.3
I_9, I_{14}	$\Delta S_{13} \oplus \Delta S_{14} = 0$	131,893.75
I_{10}, I_{13}	$\Delta S_{10} \oplus \Delta S_{12} = 0$	132,552.95
I_{10}, I_{14}	$\Delta S_9 \oplus \Delta S_{15} = 0$	132,127.9
I_{11}, I_{12}	$\Delta S_{12} \oplus \Delta S_{14} = 0$	133,870.55
I_{11}, I_{13}	$\Delta S_9 \oplus \Delta S_{14} = 0$	132,262.4
I_{11}, I_{15}	$\Delta S_{10} \oplus \Delta S_{11} = 0$	131,637.65
I_{11}, I_{15}	$\Delta S_{10} \oplus \Delta S_{15} = 0$	131,621.1
I_{12}, I_{13}	$\Delta S_9 \oplus \Delta S_{15} = 0$	131,560.6
I_{12}, I_{13}	$\Delta S_{10} \oplus \Delta S_{12} = 0$	131,683.85
I_{12}, I_{13}	$\Delta S_{12} \oplus \Delta S_{13} = 0$	131,538.65
I_{12}, I_{14}	$\Delta S_9 \oplus \Delta S_{15} = 0$	133,746.8
I_{13}, I_{14}	$\Delta S_9 \oplus \Delta S_{15} = 0$	132,071.85
I_{13}, I_{15}	$\Delta S_{10} \oplus \Delta S_{12} = 0$	131,978.15

Table 25. Improbable differential attacks on 7 rounds.

Inputs	Condition	Result
I_9 I_{11}	$\Delta S_9 \oplus \Delta S_{14} = 0$	127,667.15
I_9 I_{13}	$\Delta S_9 \oplus \Delta S_{13} = 0$	127,620.15
I_9 I_{13}	$\Delta S_9 \oplus \Delta S_{14} = 0$	130,417.3
I_9 I_{13}	$\Delta S_9 \oplus \Delta S_{15} = 0$	127,600.45
I_9 I_{13}	$\Delta S_{10} \oplus \Delta S_{15} = 0$	130,096.95
I_9 I_{14}	$\Delta S_9 \oplus \Delta S_{13} = 0$	127,740.7
I_{10} I_{12}	$\Delta S_{10} \oplus \Delta S_{12} = 0$	123,372.9
I_{10} I_{13}	$\Delta S_{10} \oplus \Delta S_{15} = 0$	130,042.35
I_{10} I_{14}	$\Delta S_{12} \oplus \Delta S_{13} = 0$	130,258.05
I_{10} I_{14}	$\Delta S_{13} \oplus \Delta S_{15} = 0$	130,438.75
I_{11} I_{13}	$\Delta S_9 \oplus \Delta S_{10} = 0$	129,541.15
I_{11} I_{13}	$\Delta S_9 \oplus \Delta S_{12} = 0$	130,483.15
I_{11} I_{14}	$\Delta S_{10} \oplus \Delta S_{14} = 0$	130,240.5
I_{12} I_{13}	$\Delta S_9 \oplus \Delta S_{10} = 0$	130,304.7
I_{12} I_{15}	$\Delta S_{13} \oplus \Delta S_{14} = 0$	130,761.2