Impossible Differential Cryptanalysis of Reduced Round SIMON

Zhan Chen[1], Ning Wang[2,3], and Xiaoyun Wang[2,3,4*]

[1] Department of Computer Science and Technology,
Tsinghua University, Beijing 100084, China
z-chen14@mails.tsinghua.edu.cn
[2] Key Laboratory of Cryptologic Technology and Information Security,
Ministry of Education, Shandong University, Jinan 250100, China
[3] School of Mathematics, Shandong University, Jinan 250100, China
wangning_2014@hotmail.com
[4] Institute of Advanced Study, Tsinghua University, Beijing 100084, China
xiaoyunwang@mail.tsinghua.edu.cn

Abstract

Impossible differential is a useful method for cryptanalysis. SIMON is a light weight block cipher that has attracted lots of attention ever since its publication in 2013. In this paper we propose impossible differential attack on five versions of SIMON, using bit conditions to minimize key bits guessed. We calculate keybits and give the exact attack results.

Keywords: SIMON, impossible differential, bit condition

1 Introduction

SIMON [1] is a family of block ciphers designed by the U.S. National Security Agency (NSA) in 2013. It is designed to have excellent performance on both hardware and software [2]. It has a feistel structure and 5 different block sizes with different key lengths. Ever since its publication, SIMON has attracted much cryptanalysis such as differential analysis [3] [4] [5] [6], linear cryptananlysis [7] [8], impossible differential and zero-correlation linear hull cryptanalysis [7] [9].

Impossible differential attacks were independently introduced by Knudsen [10] and Biham et al. [11], the aim of impossible differential cryptanalysis is to use differentials that never occur to eliminate wrong key candidates that result in such a differential.

This paper is organized as follows. We give a brief description of SIMON and some notations in section 2. In section 3, we express a useful property of SIMON concerning bit conditions

*Corresponding author

which is used in our attack. In section 4 we give a 19-round impossible differential attack on SIMON32. In section 5 we mount 20-round impossible differential attack on SIMON48/72. Section 6 concludes the paper.

2 A brief description of Simon

SIMON is a feistel structure block cipher with block size $2n$ where $n \in \{16, 24, 32, 48, 64\}$, and key size mn where $m \in \{2, 3, 4\}$, usually denoted as SIMON$2n/mn$. We list some notations as follows:

- $X_i[n, \ldots, 2n-1, 0, \ldots, n-1]$: the input of the i-th round
- $L_i[n, \ldots, 2n-1]$: the left half of the i-th round input
- $R_i[0, \ldots, n-1]$: the right half of the i-th round input
- $\triangle X_i$: the difference of two inputs X_i and X_i'
- $k_i[0, \ldots, n-1]$: the subkey of the i-th round
- $X \lll r$: the left rotation of X by r bits
- $\oplus$: bitwise exclusive OR
- $\cap$: bitwise AND
- $\%$: modular operation

All versions of SIMON with corresponding numbers of rounds are listed in Table 1.

Table 1: The 10 versions of SIMON

Block size ($2n$)	Key size (mn)	Number of rounds
32	64	32
48	72	36
	96	36
64	96	42
	128	44
96	96	52
	144	54
128	128	68
	192	69
	256	72

Simon uses a simple round function $F(x) = (x \lll 1) \cap (x \lll 8) \oplus (x \lll 2)$. The plaintext is (L_0, R_0). After round i, (L_i, R_i) are updated to (L_{i+1}, R_{i+1}) as follows:

$$L_{i+1} = F(L_i) \oplus R_i \oplus k_i$$
$$R_{i+1} = L_i$$

The output of the last round (L_{N_r}, R_{N_r}) yields the ciphertext.

The key schedules generate a sequence of N_r subkeys $\{k_0, \ldots, k_{N_r-1}\}$. The procedure differs, depending on the value m. The first m subkeys are initialized by the master key. For $i = m, \ldots, N_{r-1}$,

$$k_i = c \oplus (z_j)_{i-m} \oplus k_{i-m} \oplus Y_{i-m} \oplus (Y_{i-m} \lll 1),$$

where

$$Y_{i-m} = \begin{cases} k_{i-m+1} \lll 3, & \text{if } m = 2, \\ k_{i-m+2} \lll 3, & \text{if } m = 3, \\ k_{i-m+3} \lll 3 \oplus k_{i-m+1}, & \text{if } m = 4. \end{cases}$$

Here $c = 2^n - 4$ and z_j is a version-dependent constant sequence. For more details refer to [2].

3 Some Observations of Bit Property

Observation 1 (from [12]) Let $\triangle x = x \oplus x'$, $\triangle y = y \oplus y'$, then

$$\begin{aligned} (x \cap y) \oplus (x' \cap y) &= \triangle x \cap y \\ (x \cap y) \oplus (x \cap y') &= x \cap \triangle y \\ (x \cap y) \oplus (x' \cap y') &= (x \cap \triangle y) \oplus (\triangle x \cap y) \oplus (\triangle x \cap \triangle y) \end{aligned}$$

Observation 2 (from [3]) Given two inputs X_i and X_i' of the i-th round, the difference of output $\triangle X_{i+1}$ can be computed without any information of subkeys. Each bit of the difference $\triangle X_{i+2}$ can be computed with no more than one key bits, depending on two bits of $\triangle X_{i+1}$.

We know from the round function that

$$X_{i+1}[j+n] = X_i[(j+1)\%n+n] \cap X_i[(j+8)\%n+n] \oplus X_i[(j+2)\%n+n] \oplus X_i[j] \oplus K_i[j],$$

so

$$\begin{aligned} \triangle X_{i+1}[j+n] =& (\triangle X_i[(j+1)\%n+n] \cap X_i[(j+8)\%n+n]) \\ & \oplus (X_i[(j+1)\%n+n] \cap \triangle X_i[(j+8)\%n+n]) \\ & \oplus (\triangle X_i[(j+1)\%n+n] \cap \triangle X_i[(j+8)\%n+n]) \\ & \oplus \triangle X_i[(j+2)\%n+n] \oplus \triangle X_i[j]. \end{aligned}$$

When computing $\triangle X_{i+2}[j+n]$ we need the value $(\triangle X_{i+1}[(j+1)\%n+n]), \triangle X_{i+1}[(j+8)\%n+n])$.

If $(\triangle X_{i+1}[(j+1)\%n+n], \triangle X_{i+1}[(j+8)\%n+n]) = (0,0)$, then $\triangle X_{i+2}[j+n]$ can be computed without any keybits.

If $(\triangle X_{i+1}[(j+1)\%n+n], \triangle X_{i+1}[(j+8)\%n+n]) = (0,1)$, then only $X_{i+1}[(j+1)\%n+n]$ is needed, we only have to guess $k_{i+1}[(j+1)\%n]$.

If $(\triangle X_{i+1}[(j+1)\%n+n], \triangle X_{i+1}[(j+8)\%n+n]) = (1,0)$, then only $X_{i+1}[(j+8)\%n+n]$ is needed, we only have to guess $k_{i+1}[(j+8)\%n]$.

If $(\triangle X_{i+1}[(j+1)\%n+n], \triangle X_{i+1}[(j+8)\%n+n]) = (1,1)$, then we only have to guess $k_{i+1}[(j+1)\%n] \oplus k_{i+1}[(j+8)\%n]$.

This bit condition reduces the key bits guessed greatly. We will use this property in our attack.

4 Impossible Differential Attack on SIMON32/64

We use a impossible differential characteristic of 11 rounds. This path is that, given input difference $\triangle X = [0000, 0000, 0000, 0000, 0000, 0000, 0000, 0001]$, after 11 SIMON32/64 rounds, the output difference cannot be like this: $[0000, 0000, 1000, 0000, 0000, 0000, 0000, 0000]$ or this: $[0000, 0010, 0000, 0000, 0000, 0000, 0000, 0000]$. Here we should note that, the input difference or output difference must have at least one non-zero bit. Since only zero difference propagates into zero difference, and the plaintext pairs or ciphertext pairs we use all have non-zero difference. Using a potential zero input difference or output difference may result in better attack than it should be.

We add four rounds on top and four rounds at the bottom of the first impossible differential path, and present attack on 19 rounds SIMON32/64. The state of each round is listed in Table 2 :

Table 2: States of SIMON32/64

$\triangle L_0 = (\mathbf{000}?, ??\mathbf{0}?, \mathbf{01}??, ???\mathbf{0})$	$\triangle R_0 = (\mathbf{0}???, ???\mathbf{1}, ????, ??\mathbf{0}?)$
$\triangle L_1 = (0\mathbf{000}, \mathbf{0}??0, \mathbf{0001}, ??0?)$	$\triangle R_1 = (000?, ??0?, 01??, ???0)$
$\triangle L_2 = (000\mathbf{0}, \mathbf{00}0?, 00\mathbf{00}, \mathbf{01}?0)$	$\triangle R_2 = (0000, 0??0, 0001, ??0?)$
$\triangle L_3 = (0000, 0\mathbf{00}0, 0000, \mathbf{000}\mathbf{1})$	$\triangle R_3 = (0000, 000?, 0000, 01?0)$
$\triangle L_4 = (0000, 000\mathbf{0}, 0000, 00\mathbf{0}0)$	$\triangle R_4 = (0000, 0000, 0000, 0001)$
$\triangle L_{15} = (0000, 0000, 1000, 0000)$	$\triangle R_{15} = (\mathbf{0}000, 000\mathbf{0}, 0000, 0000)$
$\triangle L_{16} = (?000, 001?, 0000, 0000)$	$\triangle R_{16} = (0000, 0\mathbf{00}0, \mathbf{1}000, 00\mathbf{00})$
$\triangle L_{17} = (0000, 1??0, ?000, 00??)$	$\triangle R_{17} = (?00\mathbf{0}, \mathbf{001}?, 0000, \mathbf{000}0)$
$\triangle L_{18} = (?01?, ????, 0000, ???0)$	$\triangle R_{18} = (0\mathbf{000}, \mathbf{1}??0, ?0\mathbf{00}, \mathbf{00}??)$
$\triangle L_{19} = (\mathbf{1}???, ???\mathbf{0}, ?\mathbf{0}??, ????)$	$\triangle R_{19} = (?\mathbf{01}?, ????, \mathbf{0000}, ???\mathbf{0})$

4.1 Procedure of the attack

Step 1 We build structures as follows: there are 10 necessary conditions on the plaintext, we divide all the 2^{32} plaintexts into 2^{10} parts, with 10 bits $X_0[0, 7, 14, 16, 17, 18, 22, 24, 25, 31]$ fixed for each part and other 22 bits traversing. Because $\triangle X_1$ can be computed without any key bits, we can use this property for data collection. There are 11 conditions on $\triangle X_1$, only 8 of them need to be considered. The other 3 are certain to hold. By round function definition, we build 8 equations $X_1[j+n] = X_0[(j+1)\%n+n] \cap X_0[(j+8)\%n+n] \oplus X_0[(j+2)\%n+n] \oplus X_0[j]$ for $X_1[17, 18, 19, 20, 24, 25, 26, 27]$ and solve the equation system. So for each of the 2^{10} parts, we obtain 2^8 structures with 10 bits of X_0 and 8 bits of X_1 fixed and other 14 bits traversing. In total we get 2^{18} structures.

Step 2 Two structures with three different bits $X_0[25, 7], X_1[27]$ can form 2^{28} pairs. The 2^{32} plaintexts can form 2^{17+1} structures which is $2^{17+28} = 2^{45}$ pairs. Encrypt these pairs and choose pairs whose ciphertexts have zero difference at $\triangle X_{19}[23, 25, 1, 8, 9, 10, 11, 15]$ and non-zero difference at $\triangle X_{19}[16, 2]$, the expected number of pairs left is $2^{45-10} = 2^{35}$.

Step 3 Compute 8 bits difference $\triangle X_{18}[1, 2, 3, 4, 10, 11, 12, 13]$ for the remaining pairs, and select the pairs that satisfy the required difference. The expected number of pairs left is

$2^{35} \times 2^{-8} = 2^{27}$.

Step 4 We want $\triangle L_2 = (000\mathbf{0}, \mathbf{00}0?, 00\mathbf{00}, \mathbf{01}?0)$.

1, From property 2, $0 = \triangle X_2[19] = X_1[20] \oplus \triangle X_1[21] \oplus \triangle X_1[3]$, where $X_1[20] = X_0[21] \cap X_0[28] \oplus X_0[22] \oplus X_0[4] \oplus k_0[4]$. So $k_0[4]$ has one value.

2, From property 2, $\triangle X_2[20] = (X_1[21] \cap \triangle X_1[28]) \oplus (\triangle X_1[21] \cap X_1[28]) \oplus (\triangle X_1[21] \cap \triangle X_1[28]) \oplus \triangle X_1[22] \oplus \triangle X_1[4]$.

If $(\triangle X_1[21], \triangle X_1[28]) = (0, 0)$, and if $\triangle X_1[22] \oplus \triangle X_1[4] = 1$ then these discard these pairs. If $\triangle X_1[22] \oplus \triangle X_1[4] = 0$, then $k_0[5, 12]$ has 4 values.

If $(\triangle X_1[21], \triangle X_1[28]) = (0, 1)$ then $\triangle X_2[20] = X_1[21] \oplus \triangle X_1[22] \oplus \triangle X_1[4]$ where $X_1[21] = X_0[22] \cap X_0[29] \oplus X_0[23] \oplus X_0[5] \oplus k_0[5]$, then $k_0[5]$ has 1 value.

If $(\triangle X_1[21], \triangle X_1[28]) = (1, 0)$, then $\triangle X_2[20] = X_1[28] \oplus \triangle X_1[22] \oplus \triangle X_1[4]$ where $X_1[28] = X_0[29] \cap X_0[20] \oplus X_0[30] \oplus X_0[12] \oplus k_0[12]$, then $k_0[12]$ has 1 value.

If $(\triangle X_1[21], \triangle X_1[28]) = (1, 1)$, then $\triangle X_2[20] = X_1[21] \oplus X_1[28] \oplus 1 \oplus \triangle X_1[22] \oplus \triangle X_1[4]$, so $k_0[5] \oplus k_0[12]$ has 1 value.

For all the above circumstances, discard the pairs that do not meet requirement, there are $2^{27} \times (1 - \frac{1}{8})$left. $k_0[5, 12]$ has $\frac{16}{7}$ values.

3, From property 2, $\triangle X_2[21] = (X_1[22] \cap \triangle X_1[29]) \oplus (\triangle X_1[22] \cap X_1[29]) \oplus (\triangle X_1[22] \cap \triangle X_1[29]) \oplus \triangle X_1[23] \oplus \triangle X_1[5]$

Similarly, discard unnecessary pairs there are $2^{27} \times (1 - \frac{1}{8})^2$ left. $k_0[6, 13]$ has $\frac{16}{7}$ values.

4, From property 2, $\triangle X_2[26] = X_1[18] \oplus \triangle X_1[28] \oplus \triangle X_1[10] = X_1[18]$. And $X_1[18] = X_0[19] \cap X_0[26] \oplus X_0[20] \oplus X_0[2] \oplus k_0[2]$. So $k_0[2]$ has 1 value.

5, From property 2, if $\triangle X_1[28] = 1$ then $\triangle X_2[27] = X_1[19] \oplus \triangle X_1[29] \oplus \triangle X_1[11]$, $k_0[3]$ has 1 value.

If $\triangle X_1[28] = 0$ then $\triangle X_2[27] = \triangle X_1[29] \oplus \triangle X_1[11]$. If $\triangle X_1[29] \oplus \triangle X_1[11] = 1$ then discard these pairs. If $\triangle X_1[29] \oplus \triangle X_1[11] = 0$ then $k_0[3]$ has 2 values.

After discarding unnecessary pairs there are $2^{27} \times (1 - \frac{1}{8})^2 \times (1 - \frac{1}{4})$ left. $k_0[3]$ has $\frac{4}{3}$values.

6, Similarly about $\triangle X_2[28]$, after discarding unnecessary pairs there are $2^{27} \times (1 - \frac{1}{8})^2 \times (1 - \frac{1}{4})^2$ left. $k_0[3]$ has $\frac{4}{3}$ values.

7, Similarly about $\triangle X_2[29]$, after discarding unnecessary pairs there are $2^{27} \times (1 - \frac{1}{8})^2 \times (1 - \frac{1}{4})^3 = 2^{25.37}$ left. $k_0[14]$ has $\frac{4}{3}$ values.

In this step, 8 key bits have in total $1 \times \frac{16}{7} \times \frac{16}{7} \times 1 \times \frac{4}{3} \times \frac{4}{3} = \frac{4049}{441}$ values.

Step 5 We want $\triangle R_{17} = (?00\mathbf{0}, \mathbf{001}?, 0000, \mathbf{000}0)$.

As is done in step 4, we discard pairs that do not help in our attack, and calculate keybits. There are $2^{25.37} \times (1 - \frac{1}{4})^3 \times (1 - \frac{1}{8})^2 = 2^{24.15}$ pairs left and 8 key bits have in total $1 \times \frac{4}{3} \times \frac{4}{3} \times \frac{4}{3} \times 1 \times \frac{16}{7} \times \frac{16}{7} = \frac{16384}{1323}$ values.

Step 6 As for $\triangle L_3 = (0000, 0\mathbf{00}0, 0000, \mathbf{00}0\mathbf{1})$, there are $2^{24.15} \times (1 - \frac{1}{8}) \times (1 - \frac{1}{4})^2 = 2^{23.127}$ pairs left and the 10 key bits have in total $3 \times \frac{36}{7} \times 1 \times \frac{4}{3} \times \frac{8}{3} = \frac{384}{7}$ values.

Step 7 As for $R_{16} = (0000, 0\mathbf{00}0, \mathbf{1}000, 00\mathbf{00})$, there are $2^x \times (1 - \frac{1}{4})^2 \times (1 - \frac{1}{8})$ pairs left and the 10 key bits have in total $2 \times \frac{4}{3} \times \frac{16}{3} \times 2 \times \frac{16}{7} = \frac{4096}{63}$ values.

Step 8 As for $R_{15} = (\mathbf{0}000, 000\mathbf{0}, 0000, 0000)$, 6 key bits have in total 32 possible values.

Step 9 As for $\triangle L_4 = (0000, 000\mathbf{0}, 0000, 00\mathbf{0}0)$, 6 key bits have in total 32 possible values.

Step 10 In the end we have $2^{27} \times (1 - \frac{1}{4})^{10} \times (1 - \frac{1}{8})^6 = 2^{21.693}$ pairs left. The 49 key bits have in total $\frac{4096}{441} \times \frac{16384}{1323} \times \frac{384}{7} \times \frac{4096}{63} \times 32 \times 32 = 2^{28.646}$ possible values.

That is to say each pair can sieve out $2^{28.646}$ wrong key bits. There remains $2^{49} \times (1 - \frac{2^{28.646}}{2^{49}})^{2^{21.693}} = 2^{49} \times 2^{-3.65} = 2^{45.35}$ key candidates.

Step 11 Above is the sieving results of the first impossible differential path. We add four rounds on top and bottom of the second impossible differential path. The number of key bits involved is also 49. 44 of them appeared for the first path. So the $2^{45.35}$ 44-bit keys together with the other 5-bit keys of the second path is the remaining key candidates.

Similarly we sieve the key candidates using the second path, in the end, the number of remaining keys is $2^{45.35+5} \times (1 - \frac{2^{28.646}}{2^{45.35+5}})^{2^{21.693}} = 2^{50.35-1.431} = 2^{48.919}$. That is to say, the total 54-bit keys are left with $2^{48.919}$.

The right key is definitely included in the remaining keys. We have guessed 54 bits, only have to traverse 10 bit equivalent bits to compute the master key, and test on 2 pairs of plaintexts.

4.2 Complexity analysis

The data complexity is 2^{32} known plaintexts. The memory complexity is the storing of remaining key candidates in step 11, which is $2^{48.919} \times 54/32 = 2^{49.674}$ states. The time complexity is also dominated by Step 11. In step 11, the time complexity is $2^{48.919} \times 2^{10} = 2^{58.919}$ 19-round SIMON32.

5 Impossible Differential Attacks on SIMON48/72

The 12-round impossible differential path we use is that, given input difference $[(0000, 0000, 0000, 0000, 0000, 0000), (1000, 0000, 0000, 0000, 0000, 0000)]$, after 12 round SIMON48 the output difference cannot be: $[(0100, 0000, 0000, 0000, 0000, 0000), (0000, 0000, 0000, 0000, 0000, 0000)]$.

We add four rounds on top and four rounds at the bottom, and present attack on 20-round SIMON48/72. The state of each round is listed in the following Table 3:

5.1 Procedure of the attack

Step 1 Same as done for SIMON32/64, we build 2^{32} structures and form 2^{63} pairs. Choose pairs that satisfy the differences of $\triangle X_{20}$ and $\triangle X_{19}$, there remains 2^{31} pairs.

Table 3: States of SIMON48/72

$\triangle L_0 = (?000, 00??, 0000, ???0, ?01?, ??0?)$	$\triangle R_0 = (1000, ???0, ?0??, ????, ????, ????)$
$\triangle L_1 = (?000, \mathbf{000}0, ?0\mathbf{00}, \mathbf{00}??, \mathbf{0000}, \mathbf{1}??\mathbf{0})$	$\triangle R_1 = (?000, 00??, 0000, ???0, ?01?, ??0?)$
$\triangle L_2 = (\mathbf{0}000, 00\mathbf{00}, 0000, \mathbf{000}0, ?00\mathbf{0}, \mathbf{00}1?)$	$\triangle R_2 = (1000, 0000, ?000, 00??, 0000, 1??0)$
$\triangle L_3 = (1000, 0000, \mathbf{0}000, 00\mathbf{00}, 0000, 0\mathbf{00}0)$	$\triangle R_3 = (0000, 0000, 0000, 0000, ?000, 001?)$
$\triangle L_4 = (0000, 0000, 0000, 0000, \mathbf{0}000, 000\mathbf{0})$	$\triangle R_4 = (1000, 0000, 0000, 0000, 0000, 0000)$
$\triangle L_{16} = (0100, 0000, 0000, 0000, 0000, 0000)$	$\triangle R_{16} = (\mathbf{0}000, 0000, 0000, 0000, 0\mathbf{00}0, 0000)$
$\triangle L_{17} = (?000, 0000, 0000, 0000, 0?00, 0001)$	$\triangle R_{17} = (0100, 0000, 0\mathbf{00}0, 000\mathbf{0}, \mathbf{0}000, 00\mathbf{00})$
$\triangle L_{18} = (0100, 0000, 0?00, 000?, ?000, 01??)$	$\triangle R_{18} = (?\mathbf{0}00, 000\mathbf{0}, \mathbf{0}000, 0\mathbf{000}, 0?00, \mathbf{000}1)$
$\triangle L_{19} = (??00, 000?, ?000, 0???, 0?01, ???0)$	$\triangle R_{19} = (\mathbf{0}100, 0\mathbf{000}, 0?0\mathbf{0}, \mathbf{000}?, ?\mathbf{000}, \mathbf{01}??)$
$\triangle L_{20} = (?100, 0???, 0?0?, ????, ????, ????)$	$\triangle R_{20} = (??00, 000?, ?000, 0???, 0?01, ???0)$

Step 2 For $\triangle X_2, \triangle X_3, \triangle X_4$ and $\triangle X_{18}, \triangle X_{17}, X_{16}$, discard pairs that are helpful to the attack, and compute average key bits solved for each pair. In the end we get $2^{31} \times (1 - \frac{1}{4})^{14} \times (1 - \frac{1}{8})^6 = 2^{24.034}$ pairs left. The 64-bit key has on average $2^{38.966}$ values.

That is, each pair can sieve out $2^{38.966}$ wrong keys. There remains $2^{64} \times (1 - \frac{2^{38.966}}{2^{64}})^{2^{24.034}} = 2^{63.278}$ keys. Sadly we cannot use a second impossible differential path to sieve out more wrong keys because a cumulation of involved key bits of two paths will exceed 72 bits.

Step 3 The right key is definitely included in the remaining keys. We have guessed 64 bits, and have to traverse 8 equivalent key bits to compute master key and test on two pairs of plaintexts.

5.2 Complexity analysis

The data complexity is 2^{48} known plaintexts. The memory complexity is the storing of remaining key candidates in step 2, which is $2^{63.278} \times 64/48 = 2^{63.393}$ states. The time complexity is $2^{63.278} \times 2^8 = 2^{71.278}$ 20-round SIMON48.

6 Conclusion

For SIMON48/96, SIMON64/96 and SIMON64/128, only one impossible differential path can be used for the attack. We present impossible differential attacks on SIMON32, SIMON48 AND SIMON96 with bit-wise precision in this paper. Table 4 is a comparison of previous results and our new results. We have done a detailed calculation of key bits involved, this means no better attack can be obtained other than this.

References

[1] Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., Wingers, L. (2012). Performance of the SIMON and SPECK families of lightweight block ciphers. http://iauth. org/wp-content/uploads/2013/01/SimonSpeckPerformance1. pdf.

Table 4: Summary of impossible differential attacks on SIMON

Cipher	Full rounds	Attacked rounds	Complexity			Source
			Time	Data	Memory	
SIMON32/64	32	13	$2^{50.1}$	2^{30}	2^{20}	[4]
		14	$2^{44.183}$	$2^{33.291}$	$2^{29.203}$	[13]
		18	$2^{61.14}$	2^{32}	$2^{47.67}$	[9]
		19	$2^{62.56}$	2^{32}	2^{44}	[14]
		19	$2^{58.919}$	2^{32}	$2^{49.674}$	Subsect 4.2
SIMON48/72	36	15	$2^{69.079}$	$2^{50.262}$	$2^{45.618}$	[13]
		18	$2^{61.87}$	2^{48}	$2^{42.12}$	[9]
		20	$2^{71.278}$	2^{48}	$2^{63.393}$	Subsect 5.1.2
		20	$2^{70.69}$	2^{48}	2^{58}	[14]
SIMON48/96	36	15	2^{53}	2^{38}	$2^{20.6}$	[4]
		15	$2^{69.079}$	$2^{50.262}$	$2^{45.618}$	[13]
		19	$2^{85.82}$	2^{48}	$2^{66.68}$	[9]
		21	$2^{94.73}$	2^{48}	2^{70}	[14]
		21	$2^{94.556}$	2^{48}	$2^{86.447}$	Subsect 5.2.2
SIMON64/96	42	16	$2^{91.986}$	$2^{65.248}$	$2^{60.203}$	[13]
		21	$2^{95.279}$	2^{64}	$2^{72.469}$	Subsect 6.1.2
		21	$2^{94.56}$	2^{64}	2^{60}	[14]
SIMON64/128	44	16	$2^{91.986}$	$2^{65.248}$	$2^{60.203}$	[13]
		22	$2^{126.56}$	2^{64}	2^{75}	[14]
		22	$2^{125.115}$	2^{64}	$2^{98.773}$	Subsect 6.2.2

[2] Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., Wingers, L. (2013). The SIMON and SPECK Families of Lightweight Block Ciphers. IACR Cryptology ePrint Archive, 2013, 404.

[3] Ning Wang, Xiaoyun Wang, KetingJia, and Jingyuan Zhao. Differential Attacks on Reduced SIMON Versions with Dynamic Key-Guessing Techniques. Technical report, Cryptology ePrint Archive, Report 2014/448, 2014.

[4] Abed, F., List, E., Lucks, S., Wenzel, J. (2013). Differential and linear cryptanalysis of reduced-round SIMON. Cryptology ePrint Archive, Report 2013/526.

[5] Biryukov, A., Roy, A., Velichkov, V. (2014). Differential analysis of block ciphers SIMON and SPECK. In International Workshop on Fast Software Encryption-FSE.

[6] Sun, S., Hu, L., Wang, P., Qiao, K., Ma, X., Song, L. (2014). Automatic security evaluation and (related-key) differential characteristic search: Application to SIMON, PRESENT, LBlock, DES (L) and other bit-oriented block ciphers. In Advances in Cryptology-ASIACRYPT 2014 (pp. 158-178). Springer Berlin Heidelberg.

[7] Alizadeh, J., Alkhzaimi, H. A., Aref, M. R., Bagheri, N., Gauravaram, P., Kumar, A., Lauridsen, M. M., and Sanadhya, S. K. (2014). Cryptanalysis of Simon variants with Connections.

In Radio Frequency Identification: Security and Privacy Issues (pp. 90-107). Springer International Publishing.

[8] Alizadeh, J., Alkhzaimi, H. A., Aref, M. R., Bagheri, N., Gauravaram, P., Lauridsen, M. M. Improved linear cryptanalysis of round reduced SIMON. IACR Cryptology ePrint Archive, Reprot 2014/681, 2014. http://eprint. iacr. org/2014/681. pdf.

[9] Wang, Q., Liu, Z., Varıcı, K., Sasaki, Y., Rijmen, V., Todo, Y. (2014). Cryptanalysis of Reduced-round SIMON32 and SIMON48. In Progress in Cryptology–INDOCRYPT 2014 (pp. 143-160). Springer International Publishing.

[10] Knudsen, L. (1998). DEAL-a 128-bit block cipher. complexity, 258(2).

[11] Biham, E., Biryukov, A., Shamir, A. (1999, January). Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials. In Advances in Cryptology-Eurocrypt'99 (pp. 12-23). Springer Berlin Heidelberg.

[12] Kühn, U. (2002, January). Improved cryptanalysis of MISTY1. In Fast Software Encryption (pp. 61-75). Springer Berlin Heidelberg.

[13] AlKhzaimi, H., Lauridsen, M. M. (2013). Cryptanalysis of the SIMON Family of Block Ciphers. IACR Cryptology ePrint Archive, 2013, 543.

[14] Boura, C., Naya-Plasencia, M., Suder, V. (2014). Scrutinizing and improving impossible differential attacks: Applications to clefia, camellia, lblock and simon. In Advances in Cryptology-ASIACRYPT 2014 (pp. 179-199). Springer Berlin Heidelberg.