An Efficient One-Bit Model for Differential Fault Analysis on Simon Family

Juan Grados [1]   Fábio Borges [2]   Renato Portugal [1]   Pedro Lara [3]

[1]National Laboratory for Scientific Computing

[2]Technische Universität Darmstadt, CASED – Telecooperation Lab

[3]CEFET-RJ

juancgv@lncc.br, fabio.borges@cased.de, portugal@lncc.br and pedro.lara@cefet-rj.br

September 13, 2015
FDTC 2015

Overview

Introduction

SIMON Family

- Simon is a family of lightweight block ciphers based upon Feistel structure.
- This family was designed by the National Security Agency (NSA).
- Its design provides optimal performance on resource-constrained devices.
- Simon supports 5 block sizes of 32, 48, 64, 96, 128 bits and up to 3 key sizes for each block size.

Differential Fault Attack

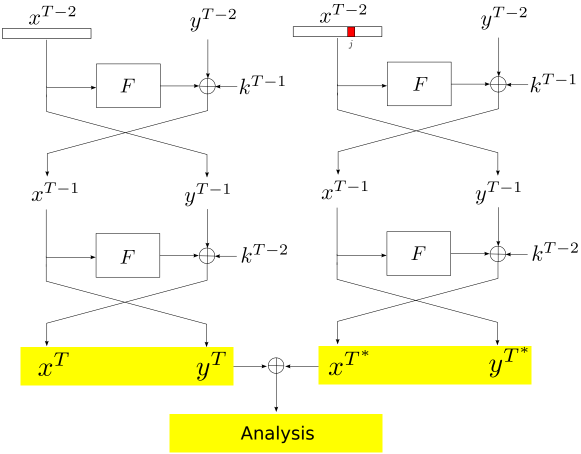


Figure: Differential Fault Attack.

Notation

- T: total number of rounds in the cipher.
- $\left(L^{i-1}, R^{i-1}\right)$: $2n$-bit input of the i^{th} round of the cipher, $i \in \{0, \cdots, T-1\}$.
- $\left(L^{i+1}, R^{i+1}\right)$: $2n$-bit output of the i^{th} round of the cipher, $i \in \{0, \cdots, T-1\}$.
- $L^{(i-1)^*}$,$R^{(i-1)^*}$ wrong left half input and wrong right half input respectively of the i^{th}.
- P: plaintext, C: ciphertext, C^*: faulty ciphertext.
- K^i: n-bit round-key used in the i^{th} round of the cipher, $i \in \{0 \cdots T-1\}$.
- $x <<< a$: circular left rotation of x by a bits.
- x_l: l^{th} bit of the bit string x.
- $\oplus$: logical operator xor.
- $\odot$: logical operator and.
- $a\%b$: $a \mod b$

Background

SIMON Family

The Simon Family Cipher

cipher	Block size $2n$	Key words m	Key size mn	Rounds T	Index to z j
Simon32/64	32	4	64	32	0
Simon48/72	48	3	72	36	0
Simon48/96	48	4	96	36	1
Simon64/96	64	3	96	42	2
Simon64/128	64	4	128	44	3
Simon96/92	96	2	92	52	2
Simon96/144	96	3	144	54	3
Simon128/128	128	2	128	68	2
Simon128/192	128	3	192	69	3
Simon128/256	128	4	256	72	4

Table: Members of the SIMON family with their parameters

Round of SIMON

The design of SIMON is a classical Feistel scheme.

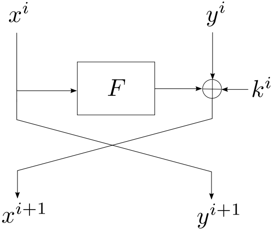


Figure: SIMON round.

$$F(x) = ((x <<< 8) \odot (x <<< 1)) \oplus (x <<< 2) \tag{1}$$

Key Schedule

$$
\begin{aligned}
m = 2\colon K^i &= K^{i-2} \oplus \left(K^{i-1} >\!>\!> 3\right) \\
&\quad \oplus \left(K^{i-1} >\!>\!> 4\right) \oplus c \oplus (z_j)_{i-m} \\
m = 3\colon K^i &= K^{i-3} \oplus \left(K^{i-1} >\!>\!> 3\right) \\
&\quad \oplus \left(K^{i-1} >\!>\!> 4\right) \oplus c \oplus (z_j)_{i-m} \\
m = 4\colon K^i &= \left(K^{i-4} \oplus K^{i-3}\right) \oplus \left(K^{i-1} >\!>\!> 3\right) \\
&\quad \oplus \left(\left(K^{i-3} \oplus \left(K^{i-1} >\!>\!> 3\right)\right) >\!>\!> 1\right) \\
&\quad \oplus c \oplus (z_j)_{i-m}
\end{aligned} \tag{2}
$$

where $c = (2^n - 1) \oplus 3$ is a constant value, $(z_j)_{i-m}$ denotes the i^{th} bit of z_j, and $i - m$ is taken module 62.

The z_j vectors

j	z_j
0	11111010001001010110000111001101111101000100101011000011100110
1	10001110111110010011000010110101000111011111001001100001011010
2	10101111011100000011010010011000101000010001111110010110110011
3	11011011101011000110010111100000010010001010011100110100001111
4	11010001111001101011011000100000010111000011001010010011101111

Table: The z_j vectors used in the SIMON key schedule.

Previous DFA Models

Previous DFA Models

- H. Tupsamudre, S. Bisht, and D. Mukhopadhyay, Differential fault analysis on the families of simon and speck ciphers, in Fault Diagnosis and Tolerance in Cryptography (FDTC), 2014 Workshop on, Sept 2014, pp. 4048
- J. Takahashi and T. Fukunaga, Fault Analysis on SIMON Family of Lightweight Block Ciphers, in Information Security and Cryptology - ICISC 2014,

The One-Bit-Flip and One-Byte Models

One bit affects three bits

$$
\begin{aligned}
F\left(L^{i-1}\right)_{(j+1)\%n} &= \left(L^{i-1}_{j\%n} \odot L^{i-1}_{(j-7)\%n}\right) \oplus L^{i-1}_{(j-1)\%n} \\
F\left(L^{i-1}\right)_{(j+2)\%n} &= \left(L^{i-1}_{(j+1)\%n} \odot L^{i-1}_{(j-6)\%n}\right) \oplus L^{i-1}_{j\%n} \\
F\left(L^{i-1}\right)_{(j+8)\%n} &= \left(L^{i-1}_{(j+7)\%n} \odot L^{i-1}_{j\%n}\right) \oplus L^{i-1}_{(j+6)\%n}
\end{aligned} \tag{3}
$$

Equation of the Last Round

Let (L^T, R^T) be the output of the cipher. Then

$$K^{T-1} = L^{T-2} \oplus F(R^T) \oplus L^T \quad (4)$$

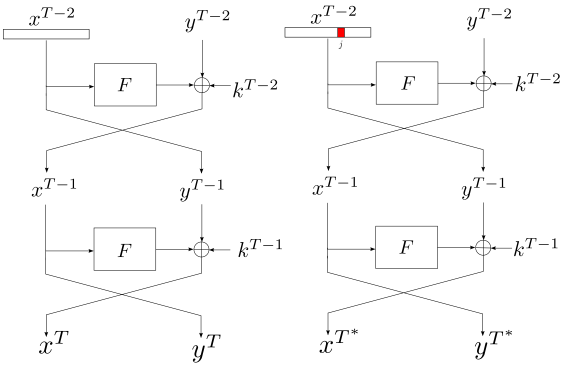
Determining the Fault Position and Value

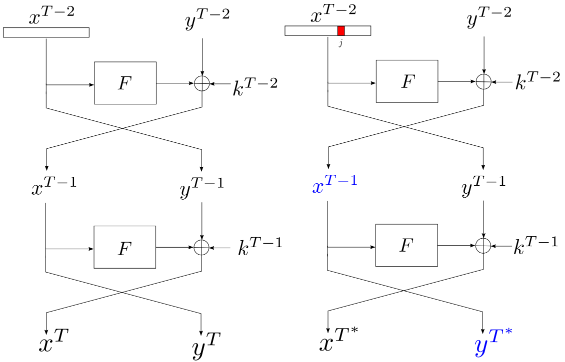
Let be (L^{T^*}, R^{T^*}) the faulty ciphertext when an error occurred in the intermediate result L^{T-2}. Then

$$e = L^T \oplus L^{T^*} \oplus F(R^T) \oplus F(R^{T^*}).$$

One-Bit-Flip Model

One-Bit-Flip Fault Attack on SIMON

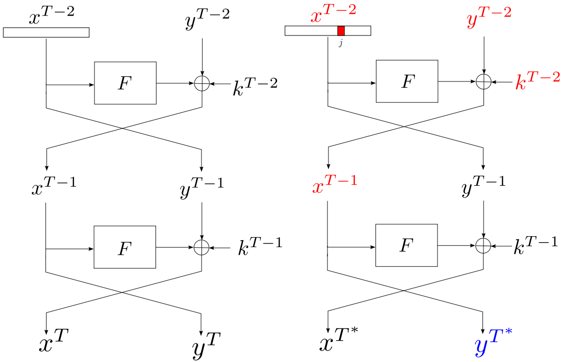




$$R^T = L^{T-1}$$

$$R^{T^*} = L^{T-1^*}$$

One-Bit-Flip Fault Attack on SIMON



$$R^T = L^{T-1} = R^{T-2} \oplus F(L^{T-2}) \oplus K^{T-2}$$

$$R^{T^*} = L^{T-1^*} = R^{T-2} \oplus F(L^{T-2^*}) \oplus K^{T-2}$$

One-Bit-Flip Fault Attack on SIMON

$$R^{T^*} = R^{T-2} \oplus F(L^{T-2^*}) \oplus K^{T-2}$$
$$R^{T} = R^{T-2} \oplus F(L^{T-2}) \oplus K^{T-2}$$

One-Bit-Flip Fault Attack on SIMON

$$
\begin{aligned}
R^{T^*} &= R^{T-2} \oplus F(L^{T-2^*}) \oplus K^{T-2} \\
R^{T} &= R^{T-2} \oplus F(L^{T-2}) \oplus K^{T-2} \\
R^{T} \oplus R^{T^*} &= F(L^{T-2}) \oplus F(L^{(T-2)^*})
\end{aligned}
$$

$$
\begin{aligned}
(R^{T} \oplus R^{T^*})_{(j+1)\%n} &= (L_j^{T-2} \odot L_{(j-7)\%n}^{T-2}) \oplus (L_{(j-7)\%n}^{T-2} \odot (L_j^{T-2} \oplus 1) \\
(R^{T} \oplus R^{T^*})_{(j+8)\%n} &= (L_j^{T-2} \odot L_{(j+7)\%n}^{T-2}) \oplus (L_{(j+7)\%n}^{T-2} \odot (L_j^{T-2} \oplus 1)) \\
(R^{T} \oplus R^{T^*})_{(j+2)\%n} &= L_j^{T-2} \oplus L_j^{T-2} \oplus 1 = 1
\end{aligned}
$$

One-Bit-Flip Fault Attack on SIMON

$$(R^T \oplus R^{T^*})_{(j+1)\%n} = (L_j^{T-2} \odot L_{(j-7)\%n}^{T-2}) \oplus (L_{(j-7)\%n}^{T-2} \odot (L_j^{T-2} \oplus 1)$$

L_j^{T-2}	$L_j^{T-2} \oplus 1$	$L_{(j-7)\%n}^{T-2}$	$(R^T \oplus R^{T^*})_{(j+1)\%n}$
0	1	0	0
1	0	0	0
0	1	1	1
1	0	1	1

One-Bit-Flip Fault Attack on SIMON

$$(R^T \oplus R^{T^*})_{(j+8)\%n} = (L_j^{T-2} \odot L_{(j+7)\%n}^{T-2}) \oplus (L_{(j+7)\%n}^{T-2} \odot (L_j^{T-2} \oplus 1)$$

L_j^{T-2}	$L_j^{T-2} \oplus 1$	$L_{j+7\%n}^{T-2}$	$(R^T \oplus R^{T^*})_{(j+8)\%n}$
0	1	0	0
1	0	0	0
0	1	1	1
1	0	1	1

One-Bit-Flip Fault Attack on SIMON

With the values of the bits $L^{T-2}_{j-7\%n}$, $L^{T-2}_{j+7\%n}$, and

$$K^{T-1} = L^{T-2} \oplus F(R^T) \oplus L^T$$

it is possible retrieve the corresponding bits of K^{T-1}.

$$K^{T-1}_{(j-7)\%n} = L^{T-2}_{(j-7)\%n} \oplus F(R^T)_{(j-7)\%n} \oplus L^T_{(j-7)\%n}$$
$$K^{T-1}_{(j+7)\%n} = L^{T-2}_{(j+7)\%n} \oplus F(R^T)_{(j+7)\%n} \oplus L^T_{(j+7)\%n}$$

The One-Byte Model

The One-Byte Model

- In this model one byte of L^{T-2} is affected.
- It uses the same working principle of the one-bit-flip model to retrieve K^{T-1}.
- Except for two cases.

The One-Byte Model

- In this model one byte of L^{T-2} is affected.
- It uses the same working principle of the one-bit-flip model to retrieve K^{T-1}.
- Except for two cases.
  1. the least and most significant bits of the induced byte fault are one.
  2. a byte fault flips two adjacent bits.

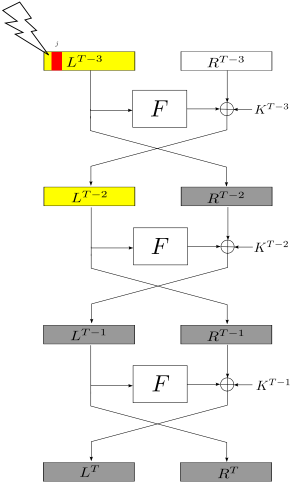
The n-bit Model

The n-bit Model

- Similar to the last two models, the authors analyzed the input and output differences in the AND operation when applying random fault injections on n bits.
- They have precisely calculated the average number of fault injections to obtain a round key by examining the relationships between the bits obtained through multiple fault injections.
- Their analysis reduce significantly the average number of fault injections to retrieve L^{T-2}.

One-Bit-Flip Fault Attack on Simon at round $T - 3$

One-Bit-Flip Fault Attack on Simon at round $T - 3$

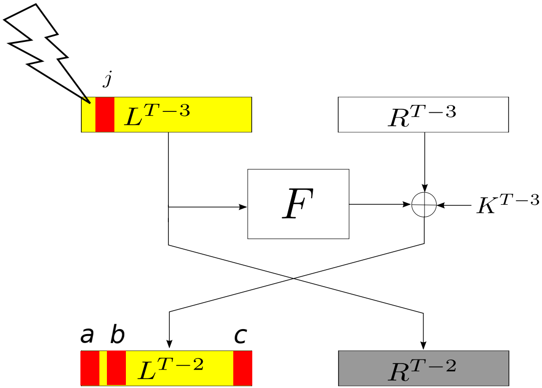


Deducing j

Deducing j

Similarly, for our modification we cannot perform our attack if we do not know the position of the flipped bit in the left half input L^{T-3}, and the positions of flipped bits in L^{T-2} affected by $F\left(L^{(T-3)^*}\right)$.

Deducing j



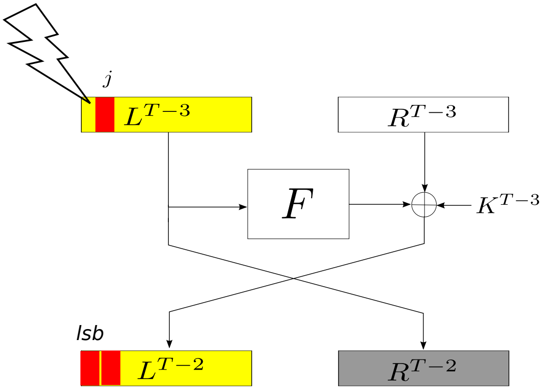
Deducing *j*

Algorithm 1 Deducing j

Input: bit string e' of size n
Output: deducing j

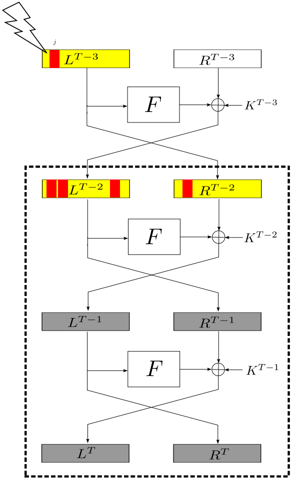
```
lsb ← LSB (e')
msb ← MSB (e')
j ← −1
if wt (e') = 3 then
    for i = 0 to n − 1 do
        if e'[i%n] = 1 and e'[(i + 1) %n] = 1 then
            j ← i − 1
        end if
    end for
end if
if wt (e') = 2 then
    d ← abs (lsb − msb)
    if d > 1 then
        if d = 7 then
            j ← (lsb − 1) %n
        end if
        if d = 6 then
            j ← (lsb − 2) %n
        end if
        if d = n − 7 + 1 then
            j ← (msb − 2) %n
        end if
        if d = n − 7 then
            j ← (msb − 1) %n
        end if
        if d = n − 1 then
            j ← n − 2
        end if
    else
        for i = 0 to n − 1 do
            if e'[i%n] = 1 and e'[(i + 1) %n] = 1 then
                j ← i − 1
            end if
        end for
    end if
end if
return j%n
```

For example



Retrieving L^{T-2} and K^{T-1}

Retrieving L^{T-2} and K^{T-1}



New Formulas

A flip in $L^{T-2}_{(j+1)\%n}$ affects 3 bits:

$$\left(R^{T} \oplus R^{T^*}\right)_{(j+2)\%n} = \left(L^{T-2}_{(j+1)\%n} \odot L^{T-2}_{(j-6)\%n}\right) \oplus \left(\left(L^{T-2}_{(j+1)\%n} \oplus 1\right) \odot L^{T-2}_{(j-6)\%n}\right) \oplus \tilde{R}^{T-2}_{(j+2)\%n}$$

$$\left(R^{T} \oplus R^{T^*}\right)_{(j+3)\%n} = \begin{cases} \left(L^{T-2}_{(j+2)\%n} \odot L^{T-2}_{(j-5)\%n}\right) \oplus \left(\left(L^{T-2}_{(j+2)\%n} \oplus 1\right) \odot L^{T-2}_{(j-5)\%n}\right) \oplus 1 \oplus \tilde{R}^{T-2}_{(j+3)\%n} \\ \text{if } L_{(j+2)\%n} \text{ was affected} \\ 1 \oplus \tilde{R}^{T-2}_{(j+3)\%n} \\ \text{if otherwise} \end{cases}$$

$$\left(R^{T} \oplus R^{T^*}\right)_{(j+9)\%n} = \begin{cases} \left(L^{T-2}_{(j+8)\%n} \odot L^{T-2}_{(j+1)\%n}\right) \oplus \left(\left(L^{T-2}_{(j+8)\%n} \oplus 1\right) \odot \left(L^{T-2}_{(j+1)\%n} \oplus 1\right)\right) \oplus \tilde{R}^{T-2}_{(j+9)\%n} \\ \text{if } L_{(j+8)\%n} \text{ was affected} \\ \left(L^{T-2}_{(j+8)\%n} \odot L^{T-2}_{(j+1)\%n}\right) \oplus \left(\left(L^{T-2}_{(j+8)\%n}\right) \odot \left(L^{T-2}_{(j+1)\%n} \oplus 1\right)\right) \oplus \tilde{R}^{T-2}_{(j+9)\%n} \\ \text{if otherwise} \end{cases}$$

New Formulas

A flip in $L^{T-2}_{(j+2)\%n}$ affects 3 bits:

$$\left(R^T \oplus R^{T^*}\right)_{(j+3)\%n} = \begin{cases} \left(L^{T-2}_{(j+2)\%n} \odot L^{T-2}_{(j-5)\%n}\right) \oplus \left(\left(L^{T-2}_{(j+2)\%n} \oplus 1\right) \odot L^{T-2}_{(j-5)\%n}\right) \oplus 1 \oplus \tilde{R}^{T-2}_{(j+3)\%n} \\ \text{if } L_{(j+1)\%n} \text{ was affected} \\ \left(L^{T-2}_{(j+2)\%n} \odot L^{T-2}_{(j-5)\%n}\right) \oplus \left(\left(L^{T-2}_{(j+2)\%n} \oplus 1\right) \odot L^{T-2}_{(j-5)\%n}\right) \oplus \tilde{R}^{T-2}_{(j+3)\%n} \\ \text{if otherwise} \end{cases}$$

$$\left(R^T \oplus R^{T^*}\right)_{(j+4)\%n} = L^{T-2}_{(j+2)\%n} \oplus (L^{T-2}_{(j+2)\%n} \oplus 1) \oplus \tilde{R}^{T-2}_{(j+4)\%n} = 1 \oplus \tilde{E}^{T-2}_{(j+4)\%n}$$

$$\left(R^T \oplus R^{T^*}\right)_{(j+10)\%n} = \begin{cases} \left(L^{T-2}_{(j+9)\%n} \odot L^{T-2}_{(j+2)\%n}\right) \oplus \left(L^{T-2}_{(j+9)\%n} \odot \left(L^{T-2}_{(j+2)\%n} \oplus 1\right)\right) \oplus 1 \oplus \tilde{R}^{T-2}_{(j+10)\%n} \\ \text{if } L_{(j+8)\%n} \text{ was affected} \\ \left(L^{T-2}_{(j+9)\%n} \odot L^{T-2}_{(j+2)\%n}\right) \oplus \left(L^{T-2}_{(j+9)\%n} \odot \left(L^{T-2}_{(j+2)\%n} \oplus 1\right)\right) \oplus \tilde{R}^{T-2}_{(j+10)\%n} \\ \text{if otherwise} \end{cases}$$

New Formulas

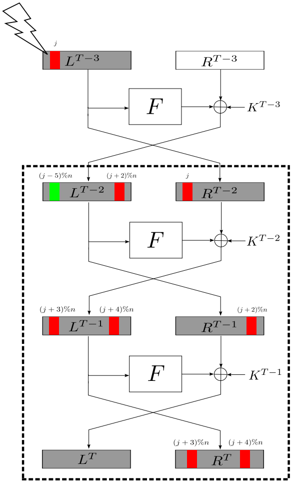
A flip in $L^{T-2}_{(j+8)\%n}$ affects 3 bits:

$$\left(R^T \oplus R^{T^*}\right)_{(j+9)\%n} = \begin{cases} \neg\left(L^{T-2}_{(j+8)\%n} \oplus L^{T-2}_{(j+1)\%n}\right) \oplus \tilde{R}^{T-2}_{(j+9)\%n} \\ \text{if } L_{(j+1)\%n} \text{ was affected} \\ \left(L^{T-2}_{(j+8)\%n} \odot L^{T-2}_{(j+1)\%n}\right) \oplus \left(L^{T-2}_{(j+1)\%n} \odot \left(L^{T-2}_{(j+8)\%n} \oplus 1\right)\right) \oplus \tilde{R}^{T-2}_{(j+9)\%n} \\ \text{if otherwise} \end{cases}$$

$$\left(R^T \oplus R^{T^*}\right)_{(j+10)\%n} = \begin{cases} \left(L^{T-2}_{(j+9)\%n} \odot L^{T-2}_{(j+2)\%n}\right) \oplus \left(L^{T-2}_{(j+9)\%n} \odot \left(L^{T-2}_{(j+2)\%n} \oplus 1\right)\right) \oplus \tilde{R}^{T-2}_{(j+10)\%n} \\ \text{if } L_{(j+2)\%n} \text{ was affected} \\ 1 \\ \text{if otherwise} \end{cases}$$

$$\left(R^T \oplus R^{T^*}\right)_{(j+16)\%n} = \left(L^{T-2}_{(j+15)\%n} \odot L^{T-2}_{(j+8)\%n}\right) \oplus \left(L^{T-2}_{(j+15)\%n} \odot \left(L^{T-2}_{(j+8)\%n} \oplus 1\right)\right) \oplus \tilde{R}^{T-2}_{(j+16)\%n}$$

Deducing bit of L^{T-2}



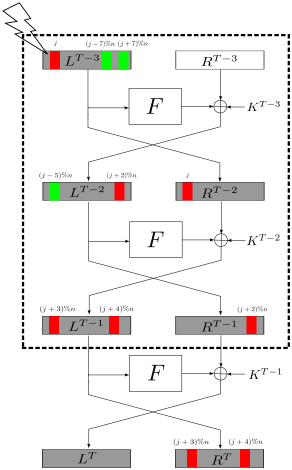
affected bits by L^{T-2}_{j+1}	conditions	deduce value
$\left(R^T \oplus R^{T^*}\right)_{(j+2)\%n}$		$L^{T-2}_{(j-6)\%n}$
$\left(R^T \oplus R^{T^*}\right)_{(j+3)\%n}$	$\tilde{L}^{T-2}_{(j+2)\%n} = 1$	$L^{T-2}_{(j-5)\%n}$
	$\tilde{L}^{T-2}_{(j+2)\%n} = 0$	
$\left(R^T \oplus R^{T^*}\right)_{(j+9)\%n}$	$\tilde{L}^{T-2}_{(j+8)\%n} = 1$	
	$\tilde{L}^{T-2}_{(j+8)\%n} = 0$	$L^{T-2}_{(j+8)\%n}$
affected bits by L^{T-2}_{j+2}	conditions	deduce value
$\left(R^T \oplus R^{T^*}\right)_{(j+3)\%n}$	$\tilde{L}^{T-2}_{(j+1)\%n} = 1$	$L^{T-2}_{(j-5)\%n}$
	$\tilde{L}^{T-2}_{(j+1)\%n} = 0$	$L^{T-2}_{(j-5)\%n}$
$\left(R^T \oplus R^{T^*}\right)_{(j+4)\%n}$		
$\left(R^T \oplus R^{T^*}\right)_{(j+10)\%n}$	$\tilde{L}^{T-2}_{(j+8)\%n} = 1$	$L^{T-2}_{(j+9)\%n}$
	$\tilde{L}^{T-2}_{(j+8)\%n} = 0$	$L^{T-2}_{(j+9)\%n}$
affected bits by L^{T-2}_{j+8}	conditions	deduce value
$\left(R^T \oplus R^{T^*}\right)_{(j+9)\%n}$	$\tilde{L}^{T-2}_{(j+1)\%n} = 1$	
	$\tilde{L}^{T-2}_{(j+1)\%n} = 0$	$L^{T-2}_{(j+1)\%n}$
$\left(R^T \oplus R^{T^*}\right)_{(j+10)\%n}$	$\tilde{L}^{T-2}_{(j+2)\%n} = 1$	$L^{T-2}_{(j+9)\%n}$
	$\tilde{L}^{T-2}_{(j+2)\%n} = 0$	
$\left(R^T \oplus R^{T^*}\right)_{(j+16)\%n}$		$L^{T-2}_{(j+15)\%n}$

Deducing bit of L^{T-2}

$$\left(R^{T} \oplus R^{T^*}\right)_{(j+3)\%n} = \left(L^{T-2}_{(j+2)\%n} \odot L^{T-2}_{(j-5)\%n}\right) \oplus \left(\left(L^{T-2}_{(j+2)\%n} \oplus 1\right) \odot L^{T-2}_{(j-5)\%n}\right) \oplus \tilde{R}^{T-2}_{(j+3)\%n}. \tag{5}$$

Retrieving L^{T-3} and K^{T-2}

Retrieving L^{T-3} and K^{T-2}



affected bits by L^{T-2}_{j+1}	conditions	deduce value
$\left(R^T \oplus R^{T^*}\right)_{(j+2)\%n}$		$L^{T-2}_{(j-6)\%n}$
$\left(R^T \oplus R^{T^*}\right)_{(j+3)\%n}$	$\tilde{L}^{T-2}_{(j+2)\%n} = 1$	$L^{T-2}_{(j-5)\%n}$
	$\tilde{L}^{T-2}_{(j+2)\%n} = 0$	
$\left(R^T \oplus R^{T^*}\right)_{(j+9)\%n}$	$\tilde{L}^{T-2}_{(j+8)\%n} = 1$	
	$\tilde{L}^{T-2}_{(j+8)\%n} = 0$	$L^{T-2}_{(j+8)\%n}$
affected bits by L^{T-2}_{j+2}	conditions	deduce value
$\left(R^T \oplus R^{T^*}\right)_{(j+3)\%n}$	$\tilde{L}^{T-2}_{(j+1)\%n} = 1$	$L^{T-2}_{(j-5)\%n}$
	$\tilde{L}^{T-2}_{(j+1)\%n} = 0$	$L^{T-2}_{(j-5)\%n}$
$\left(R^T \oplus R^{T^*}\right)_{(j+4)\%n}$		
$\left(R^T \oplus R^{T^*}\right)_{(j+10)\%n}$	$\tilde{L}^{T-2}_{(j+8)\%n} = 1$	$L^{T-2}_{(j+9)\%n}$
	$\tilde{L}^{T-2}_{(j+8)\%n} = 0$	$L^{T-2}_{(j+9)\%n}$
affected bits by L^{T-2}_{j+8}	conditions	deduce value
$\left(R^T \oplus R^{T^*}\right)_{(j+9)\%n}$	$\tilde{L}^{T-2}_{(j+1)\%n} = 1$	
	$\tilde{L}^{T-2}_{(j+1)\%n} = 0$	$L^{T-2}_{(j+1)\%n}$
$\left(R^T \oplus R^{T^*}\right)_{(j+10)\%n}$	$\tilde{L}^{T-2}_{(j+2)\%n} = 1$	$L^{T-2}_{(j+9)\%n}$
	$\tilde{L}^{T-2}_{(j+2)\%n} = 0$	
$\left(R^T \oplus R^{T^*}\right)_{(j+16)\%n}$		$L^{T-2}_{(j+15)\%n}$

Comparison of results of DFA on Simon family.

Comparison of results of DFA on Simon family.

Table: Comparison of results of DFA on Simon family.

Block Size	Key Size	Key Words(m)	Fault Location	Avg. One-byte	Avg. One-bit-flip	Avg. n-bit	Fault Location	Avg. One-bit-flip
32	64	4	$L^{27}, L^{28}, L^{29}, L^{30}$	24	101.72	12.20	L^{27}, L^{29}	50.85
48	72	3	L^{32}, L^{33}, L^{34}	27	130.78	9.91	L^{32}, L^{33}	87.19
48	96	4	$L^{31}, L^{32}, L^{33}, L^{34}$	36	174.37	13.22	L^{31}, L^{33}	87.19
64	96	3	L^{38}, L^{39}, L^{40}	39	189.44	10.45	L^{38}, L^{39}	126.29
64	128	4	$L^{39}, L^{40}, L^{41}, L^{42}$	52	252.58	13.93	L^{39}, L^{41}	126.29
96	96	2	L^{49}, L^{50}	42	210.24	7.46	L^{49}	105.12
96	144	3	L^{50}, L^{51}, L^{52}	63	315.36	11.19	L^{50}, L^{51}	210.24
128	128	2	L^{65}, L^{66}	60	299.68	7.82	L^{65}	149.84
128	192	3	L^{65}, L^{66}, L^{67}	90	449.52	11.73	L^{65}, L^{66}	299.68
128	256	4	$L^{67}, L^{68}, L^{69}, L^{70}$	120	599.36	15.64	L^{67}, L^{69}	299.68

Conclusion

Conclusion

- We have described a DFA on Simon family inspired on the ideas of Tupsamudre *et al*.
- As we show, besides using the information leaked by the AND operation, we exploit the pseudo invertibility of the round function F when a single fault injection happens in its input.
- We believe that this pseudo invertibility contributes to the study of Fault Analysis on other cryptographic primitives. For example SPECK.
- In the future, we will investigate if it is possible to extend our method using random-byte fault model or the n-bit model.

Thanks!