A First DFA on PRIDE: from Theory to Practice

Works presentation at CRiSIS 2016

Benjamin Lac[1,5], Marc Beunardeau[2,6], Anne Canteaut[3], Jacques J.A. Fournier[1], Renaud Sirdey[4]

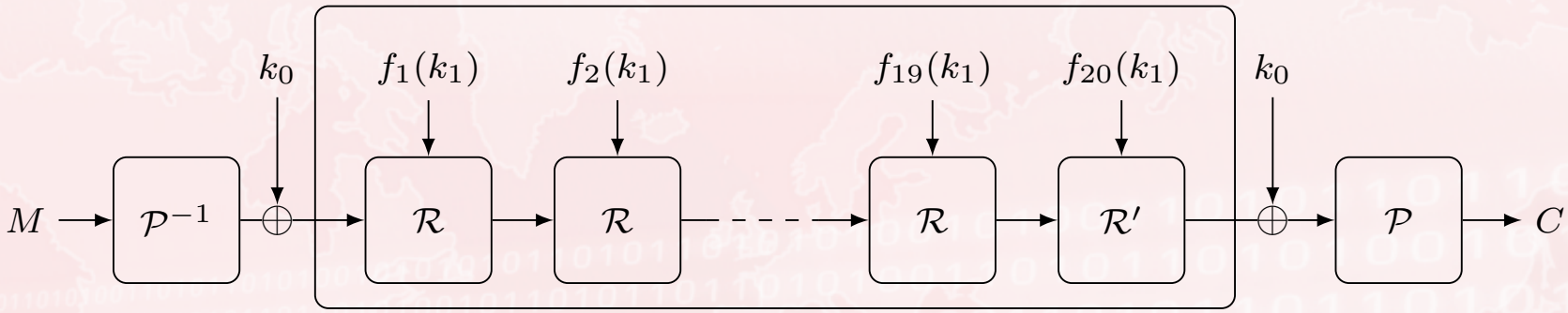
1 CEATech/DPACA, Gardanne, France,
2 Ingenico Labs, Paris, France,
3 Inria, Paris, France,
4 CEATech/LIST, Saclay, France
5 ENSM-SE, Saint-Étienne, France,
6 ENS, Paris, France,
{benjamin.lac, jacques.fournier, renaud.sirdey}@cea.fr,
marc.beunardeau@ingenico.com, anne.canteaut@inria.fr

September 7th, 2016

The PRIDE block cipher

The structure of PRIDE

Iterative block cipher composed of 20 rounds and introduced by Albrecht & al. in 2014.
It takes as input a 64-bit block and uses a 128-bit key $k = k_0||k_1$.



The key scheduling

We denote k_{1_i} the i-th byte of k_1 then

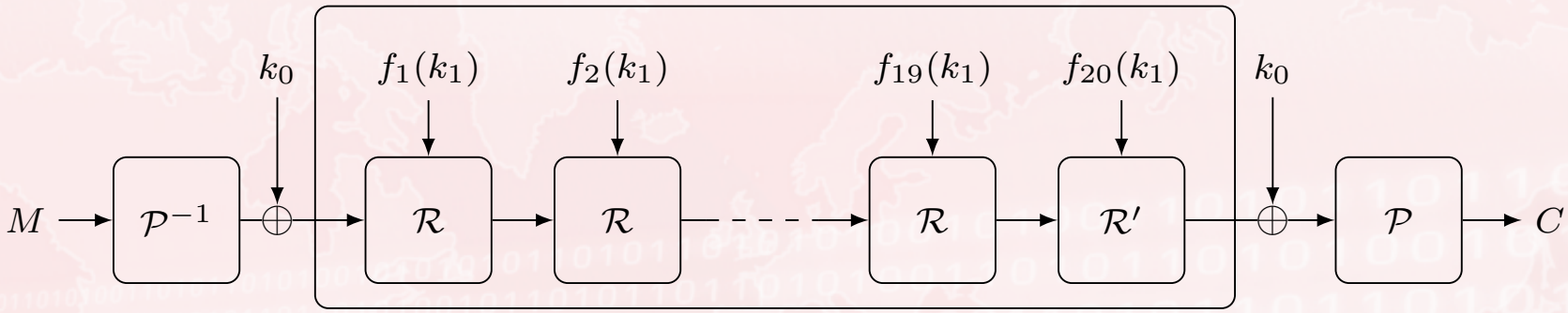
$$f_r(k_1) = k_{1_0}||g_r^{(0)}(k_{1_1})||k_{1_2}||g_r^{(1)}(k_{1_3})||k_{1_4}||g_r^{(2)}(k_{1_5})||k_{1_6}||g_r^{(3)}(k_{1_7})$$

for round r with

$$g_r^{(i)}(x) = (x + C_i r) \mod 256 \text{ where } C_i \text{ is a constant.}$$

The structure of PRIDE

Iterative block cipher composed of 20 rounds and introduced by Albrecht & al. in 2014.
It takes as input a 64-bit block and uses a 128-bit key $k = k_0||k_1$.



The key scheduling

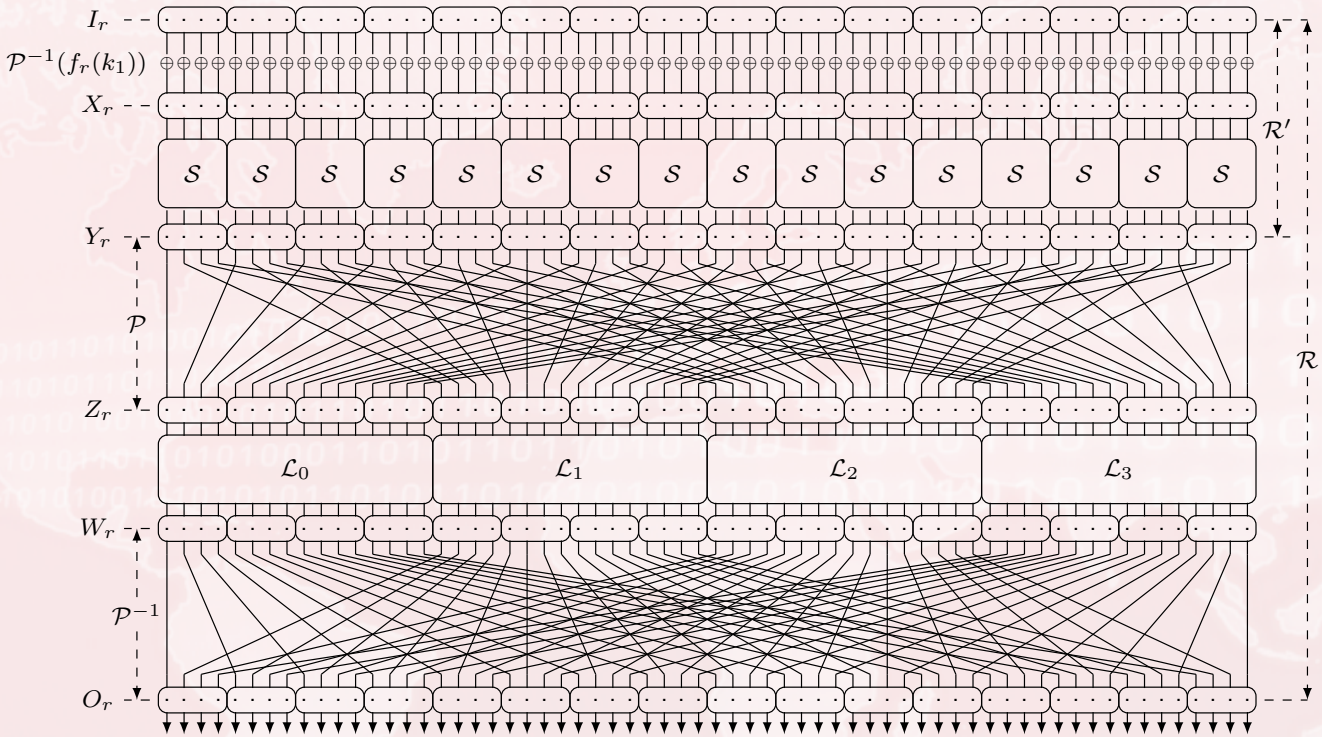
We denote k_{1_i} the i-th byte of k_1 then

$$f_r(k_1) = k_{1_0}||g_r^{(0)}(k_{1_1})||k_{1_2}||g_r^{(1)}(k_{1_3})||k_{1_4}||g_r^{(2)}(k_{1_5})||k_{1_6}||g_r^{(3)}(k_{1_7})$$

for round r with

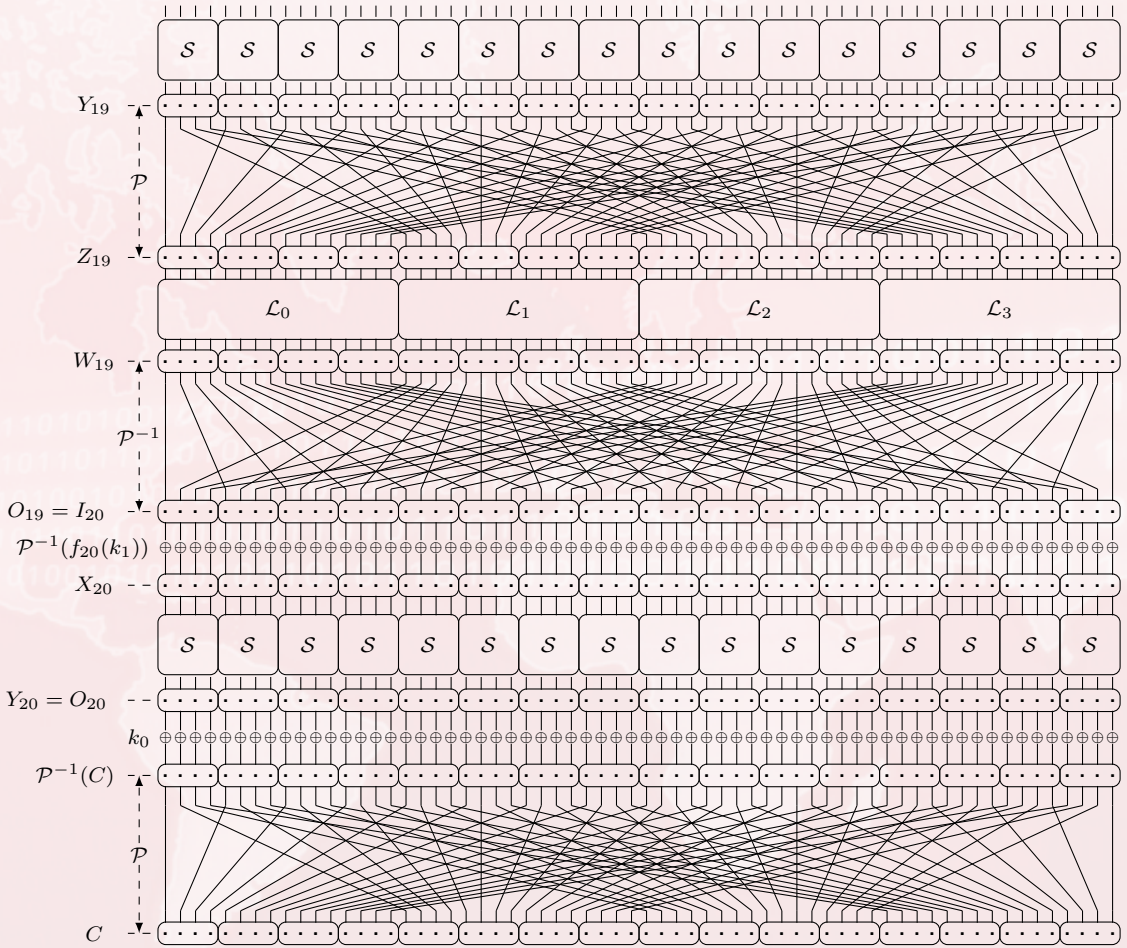
$$g_r^{(i)}(x) = (x + C_i r) \mod 256 \text{ where } C_i \text{ is a constant.}$$

The PRIDE round function

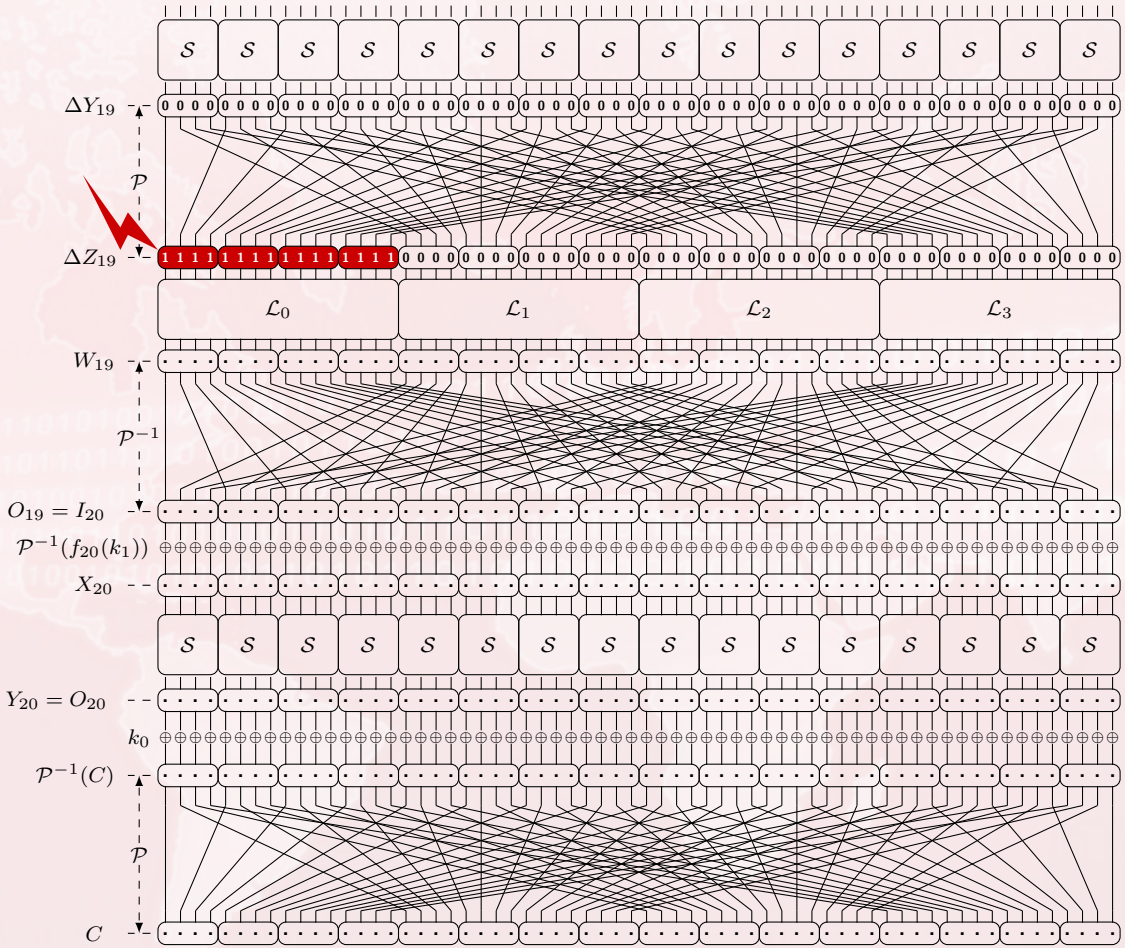


Differential Fault Analysis of PRIDE

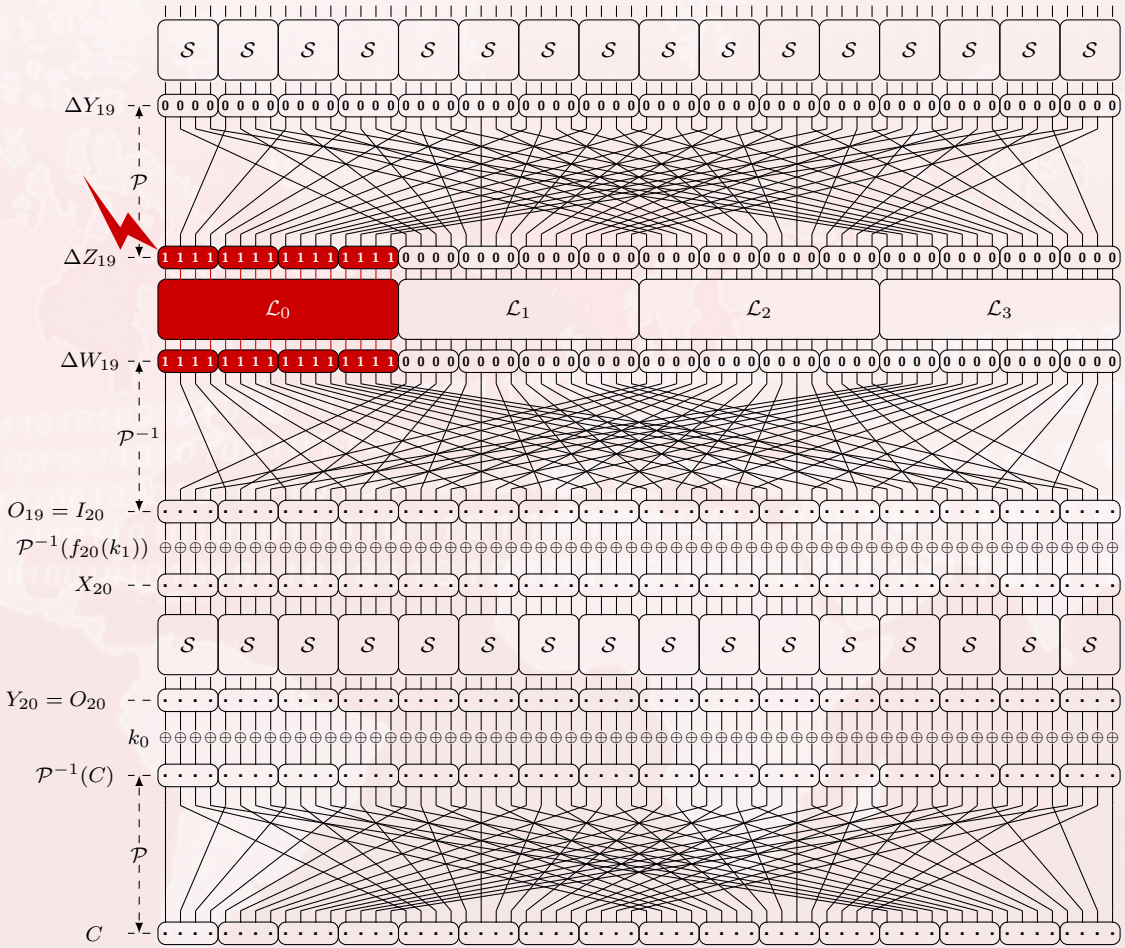
- **Injecting faults on Z_{19}**



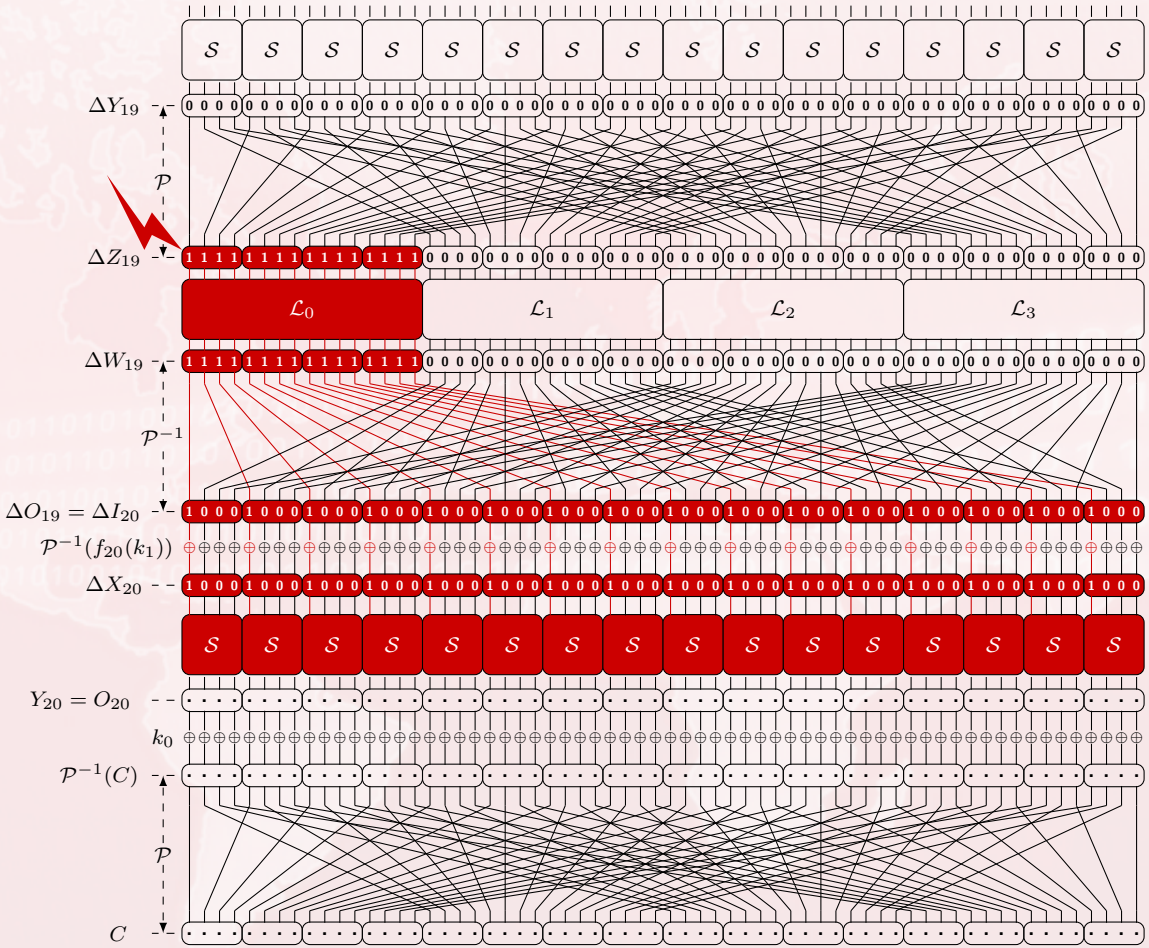
Injecting faults on Z_{19}



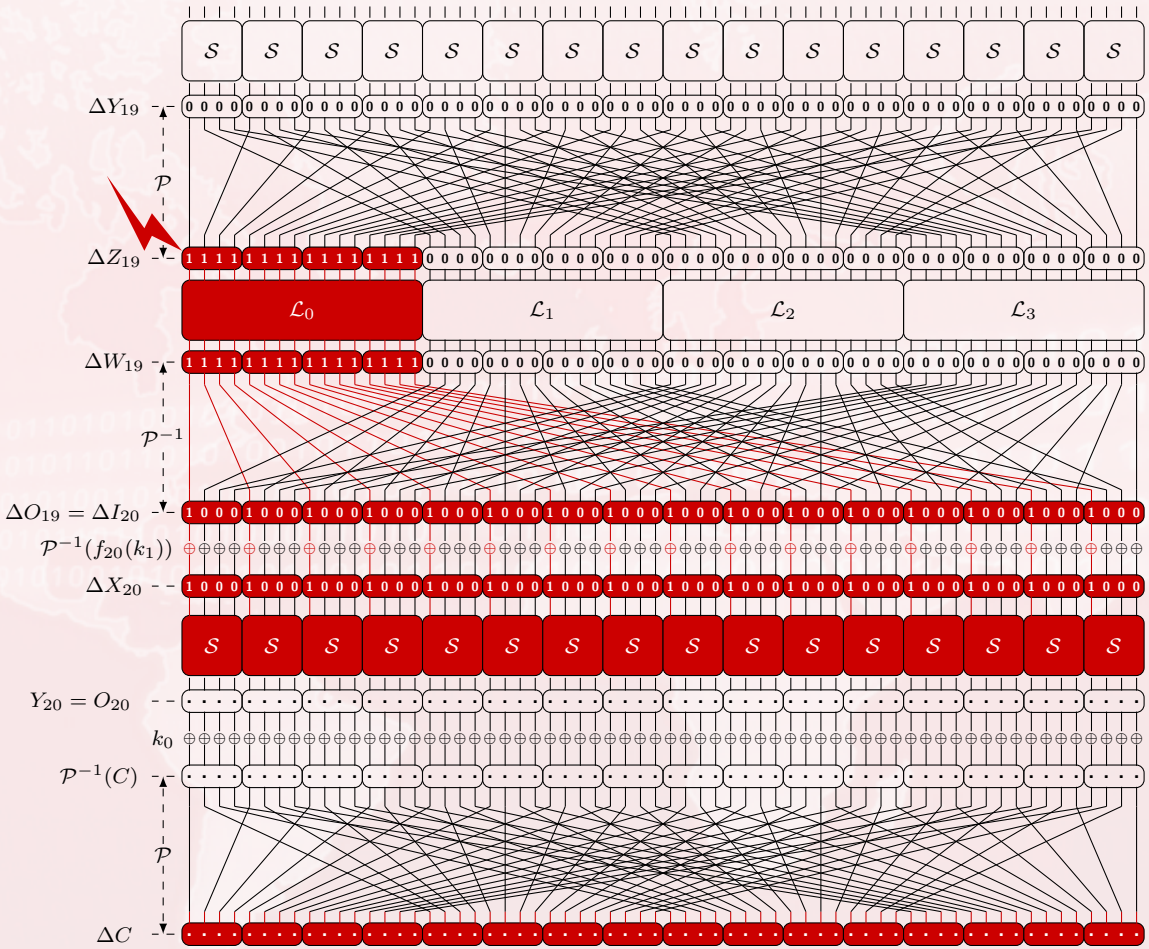
Injecting faults on Z_{19}



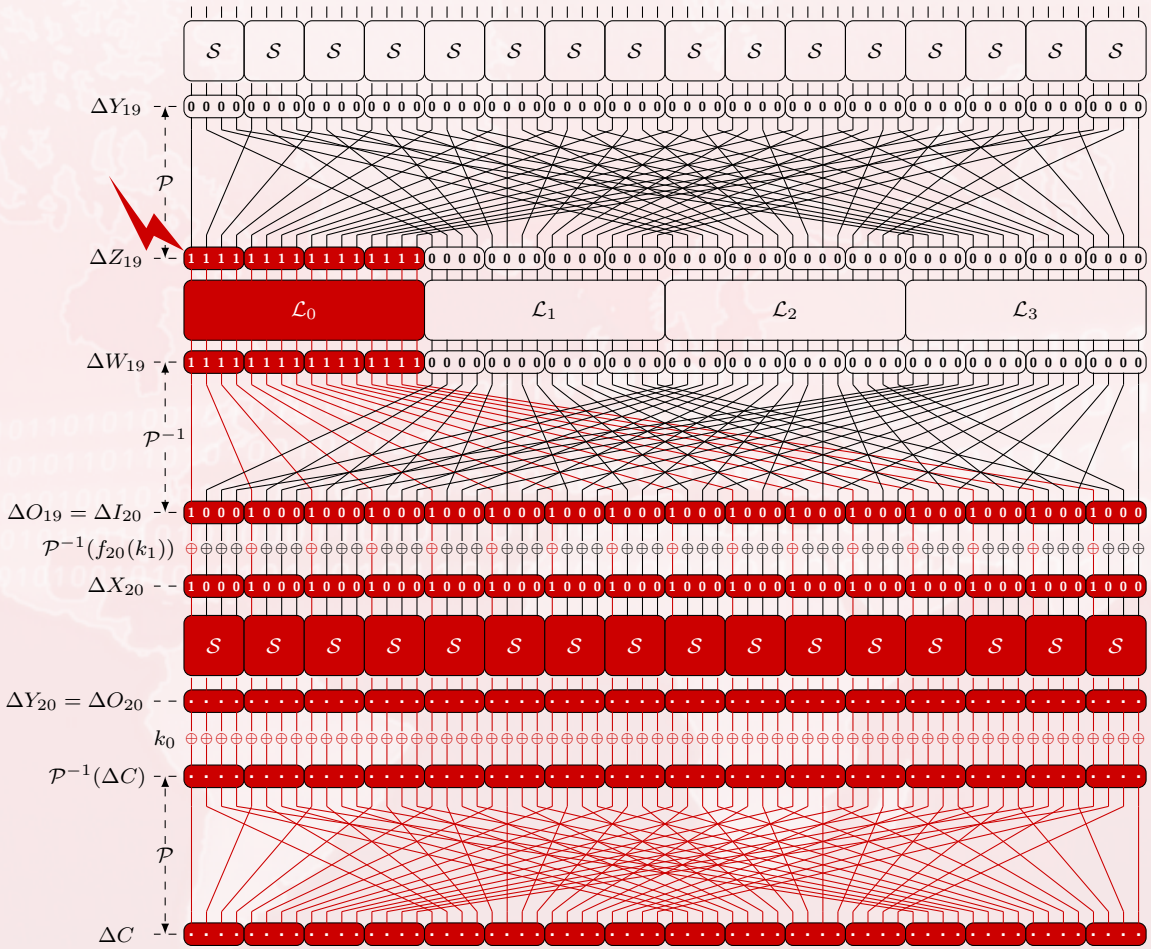
Injecting faults on Z_{19}



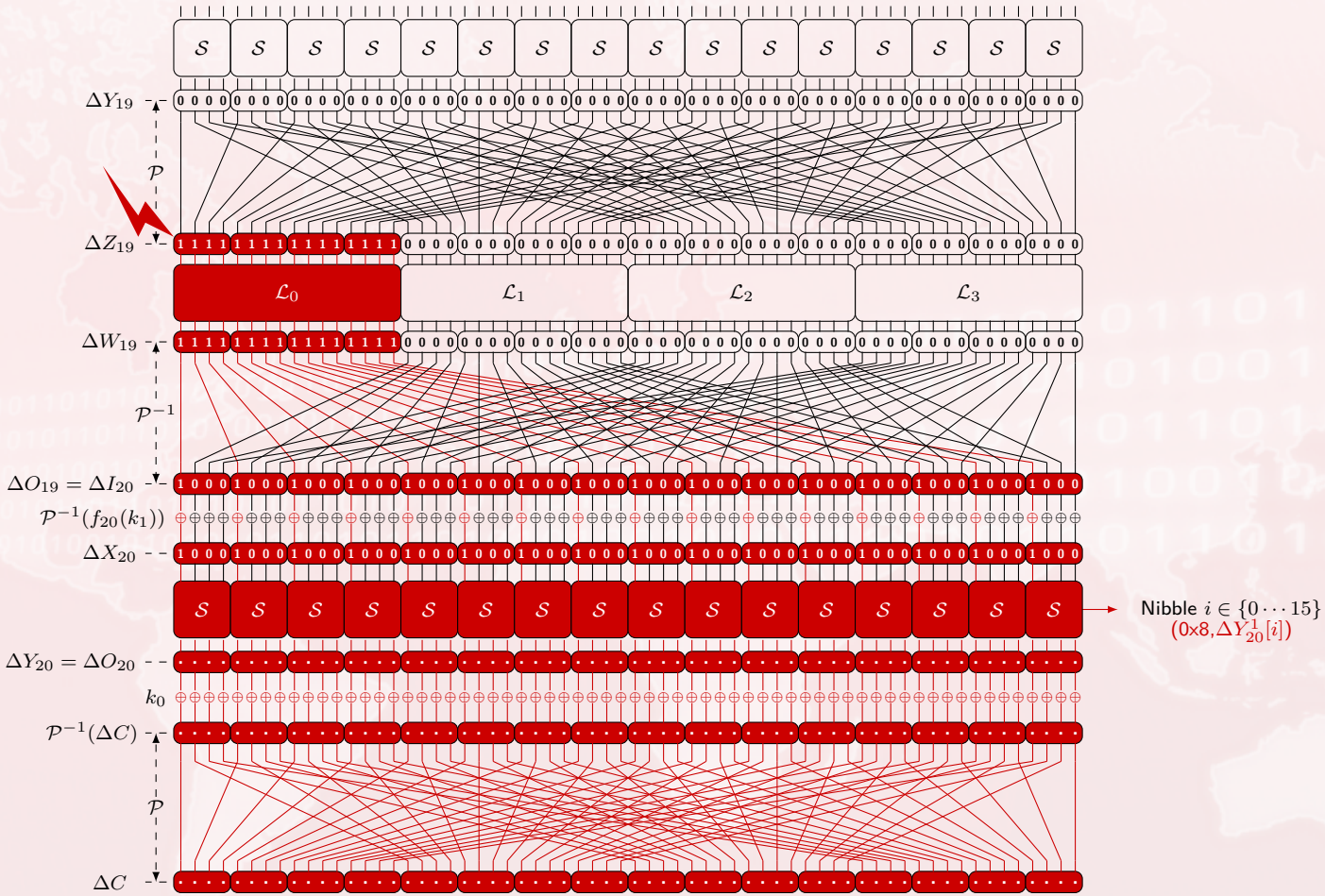
- **Injecting faults on Z_{19}**



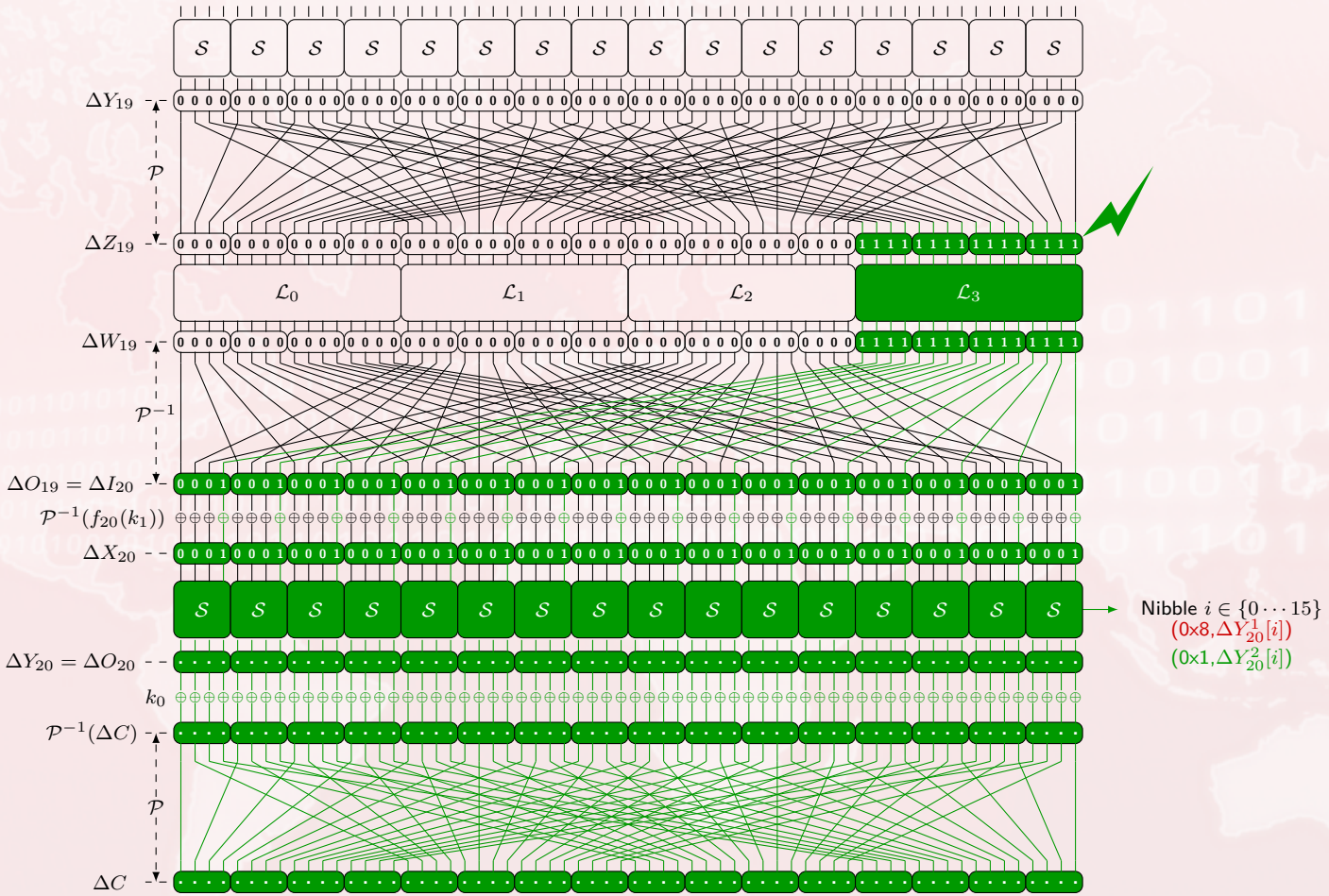
- **Injecting faults on Z_{19}**



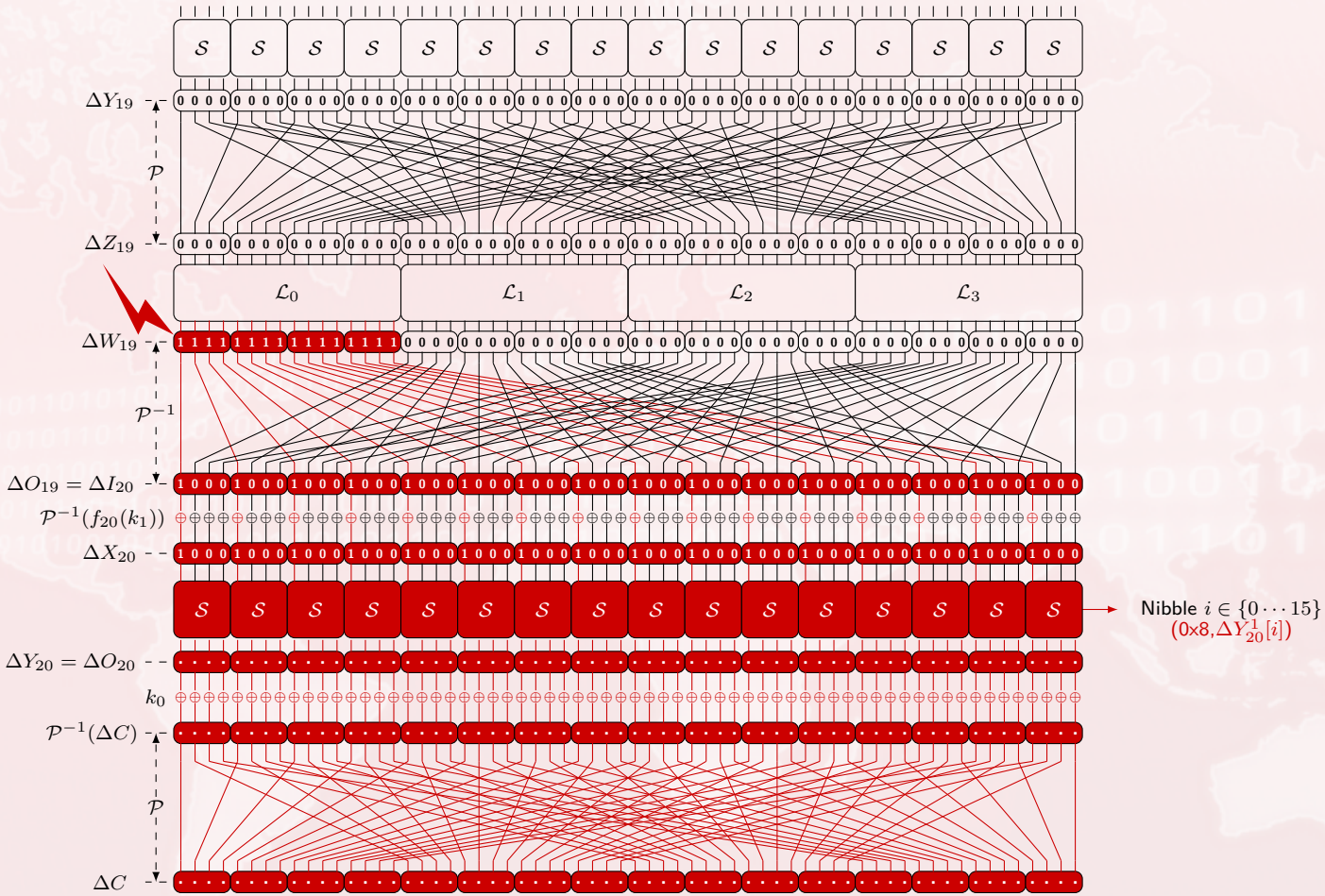
- **Injecting faults on Z_{19}**



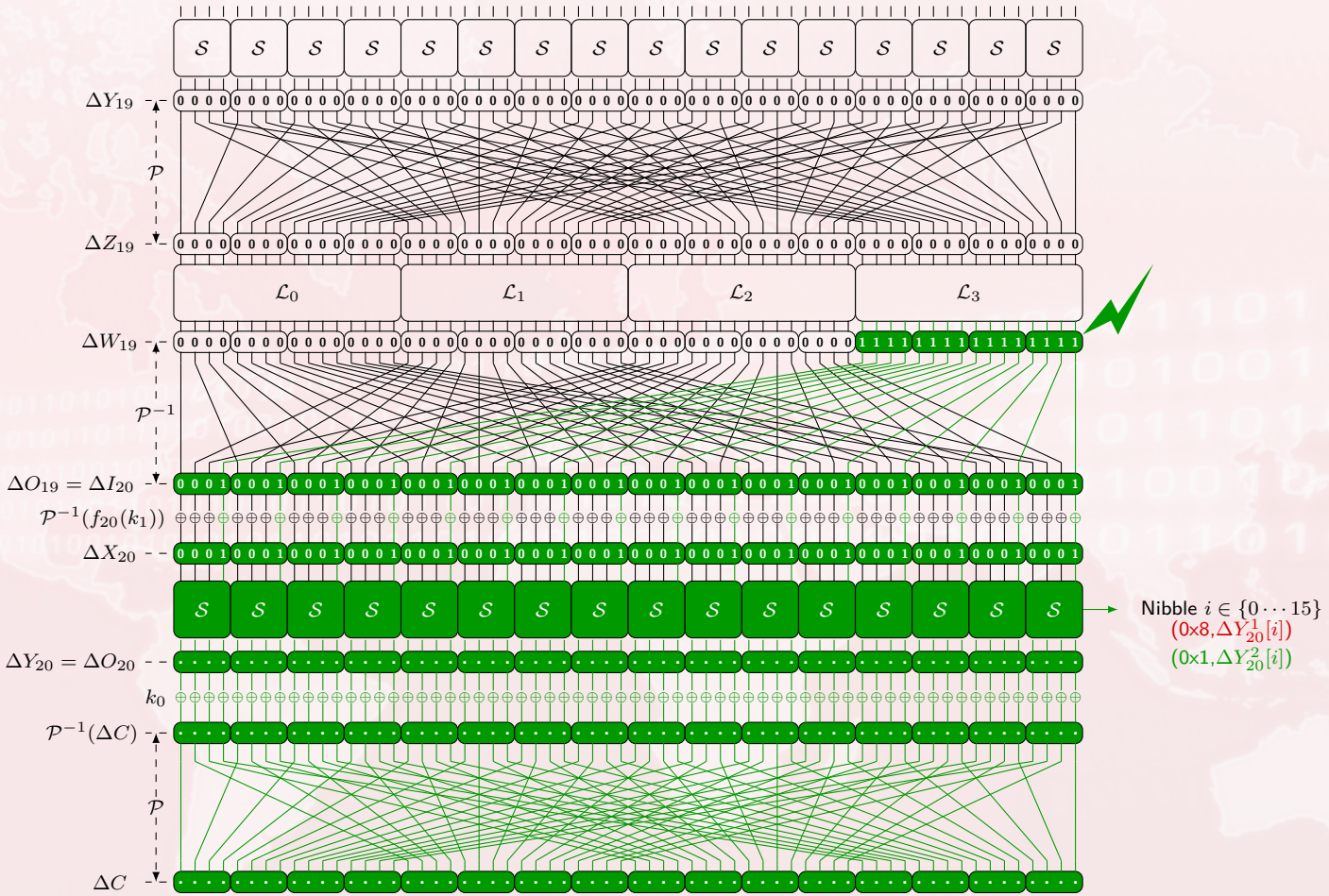
Injecting faults on Z_{19}



- **Injecting faults on W_{19}**



Injecting faults on W_{19}



Proposition

Let $\mathcal{S}$ be an n-bit S-box with differential uniformity 4. Let (a_1, b_1) and (a_2, b_2) be two differentials with $a_1 \neq a_2$ such that the system of two equations

$$\mathcal{S}(x \oplus a_1) \oplus \mathcal{S}(x) = b_1 \quad (1)$$
$$\mathcal{S}(x \oplus a_2) \oplus \mathcal{S}(x) = b_2 \quad (2)$$

has at least two solutions. Then, each of the three equations (1), (2) and

$$\mathcal{S}(x \oplus a_1 \oplus a_2) \oplus \mathcal{S}(x) = b_1 \oplus b_2 \quad (3)$$

has at least four solutions.

Mathematical exploited relations

For all i in $\{0, \cdots, 15\}$

$$\Delta X_{20}[i] = \mathcal{S}^{-1}(\mathcal{P}^{-1}(C)[i] \oplus k_0[i]) \oplus \mathcal{S}^{-1}(\mathcal{P}^{-1}(C^*)[i] \oplus k_0[i])$$

Let

$$x = \mathcal{P}^{-1}(C)[i] \oplus k_0[i]$$
$$a_1 = \mathcal{P}^{-1}(C)[i] \oplus \mathcal{P}^{-1}(C^*)[i] = \Delta Y_{20}[i]$$
$$b_1 = \Delta X_{20}[i]$$

Proposition

Let $\mathcal{S}$ be an n-bit S-box with differential uniformity 4. Let (a_1, b_1) and (a_2, b_2) be two differentials with $a_1 \neq a_2$ such that the system of two equations

$$\mathcal{S}(x \oplus a_1) \oplus \mathcal{S}(x) = b_1 \quad (1)$$
$$\mathcal{S}(x \oplus a_2) \oplus \mathcal{S}(x) = b_2 \quad (2)$$

has at least two solutions. Then, each of the three equations (1), (2) and

$$\mathcal{S}(x \oplus a_1 \oplus a_2) \oplus \mathcal{S}(x) = b_1 \oplus b_2 \quad (3)$$

has at least four solutions.

Mathematical exploited relations

For all i in $\{0, \cdots, 15\}$

$$\Delta X_{20}[i] = \mathcal{S}^{-1}(\mathcal{P}^{-1}(C)[i] \oplus k_0[i]) \oplus \mathcal{S}^{-1}(\mathcal{P}^{-1}(C^*)[i] \oplus k_0[i])$$

Let

$$x = \mathcal{P}^{-1}(C)[i] \oplus k_0[i]$$
$$a_1 = \mathcal{P}^{-1}(C)[i] \oplus \mathcal{P}^{-1}(C^*)[i] = \Delta Y_{20}[i]$$
$$b_1 = \Delta X_{20}[i]$$

Proposition

Let $\mathcal{S}$ be an n-bit S-box with differential uniformity 4. Let (a_1, b_1) and (a_2, b_2) be two differentials with $a_1 \neq a_2$ such that the system of two equations

$$\mathcal{S}(x \oplus a_1) \oplus \mathcal{S}(x) = b_1 \quad (1)$$
$$\mathcal{S}(x \oplus a_2) \oplus \mathcal{S}(x) = b_2 \quad (2)$$

has at least two solutions. Then, each of the three equations (1), (2) and

$$\mathcal{S}(x \oplus a_1 \oplus a_2) \oplus \mathcal{S}(x) = b_1 \oplus b_2 \quad (3)$$

has at least four solutions.

Mathematical exploited relations

For all i in $\{0, \cdots, 15\}$

$$\Delta X_{20}[i] = \mathcal{S}^{-1}(\mathcal{P}^{-1}(C)[i] \oplus k_0[i]) \oplus \mathcal{S}^{-1}(\mathcal{P}^{-1}(C^*)[i] \oplus k_0[i])$$

Let

$$x = \mathcal{P}^{-1}(C)[i] \oplus k_0[i]$$
$$a_1 = \mathcal{P}^{-1}(C)[i] \oplus \mathcal{P}^{-1}(C^*)[i] = \Delta Y_{20}[i]$$
$$b_1 = \Delta X_{20}[i]$$

Proposition

Let $\mathcal{S}$ be an n-bit S-box with differential uniformity 4. Let (a_1, b_1) and (a_2, b_2) be two differentials with $a_1 \neq a_2$ such that the system of two equations

$$\mathcal{S}(x \oplus a_1) \oplus \mathcal{S}(x) = b_1 \quad (1)$$
$$\mathcal{S}(x \oplus a_2) \oplus \mathcal{S}(x) = b_2 \quad (2)$$

has at least two solutions. Then, each of the three equations (1), (2) and

$$\mathcal{S}(x \oplus a_1 \oplus a_2) \oplus \mathcal{S}(x) = b_1 \oplus b_2 \quad (3)$$

has at least four solutions.

Mathematical exploited relations

For all i in $\{0, \cdots, 15\}$

$$\Delta X_{20}[i] = \mathcal{S}^{-1}(\mathcal{P}^{-1}(C)[i] \oplus k_0[i]) \oplus \mathcal{S}^{-1}(\mathcal{P}^{-1}(C^*)[i] \oplus k_0[i])$$

Let

$$x = \mathcal{P}^{-1}(C)[i] \oplus k_0[i]$$
$$a_1 = \mathcal{P}^{-1}(C)[i] \oplus \mathcal{P}^{-1}(C^*)[i] = \Delta Y_{20}[i]$$
$$b_1 = \Delta X_{20}[i]$$

Proposition

Let $\mathcal{S}$ be an n-bit S-box with differential uniformity 4. Let (a_1, b_1) and (a_2, b_2) be two differentials with $a_1 \neq a_2$ such that the system of two equations

$$\mathcal{S}(x \oplus a_1) \oplus \mathcal{S}(x) = b_1 \quad (1)$$
$$\mathcal{S}(x \oplus a_2) \oplus \mathcal{S}(x) = b_2 \quad (2)$$

has at least two solutions. Then, each of the three equations (1), (2) and

$$\mathcal{S}(x \oplus a_1 \oplus a_2) \oplus \mathcal{S}(x) = b_1 \oplus b_2 \quad (3)$$

has at least four solutions.

Mathematical exploited relations

For all i in $\{0, \cdots, 15\}$

$$\Delta X_{20}[i] = \mathcal{S}^{-1}(\mathcal{P}^{-1}(C)[i] \oplus k_0[i]) \oplus \mathcal{S}^{-1}(\mathcal{P}^{-1}(C^*)[i] \oplus k_0[i])$$

Let

$$x = \mathcal{P}^{-1}(C)[i] \oplus k_0[i]$$
$$a_1 = \mathcal{P}^{-1}(C)[i] \oplus \mathcal{P}^{-1}(C^*)[i] = \Delta Y_{20}[i]$$
$$b_1 = \Delta X_{20}[i]$$

Obtained differences

From injecting faults on Z_{19} or on W_{19}

$(a_1, 0x1), (a_2, 0x8)$

Difference distribution table of the PRIDE S-box

T	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf
0x0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0x1	0	0	0	0	4	4	4	4	0	0	0	0	0	0	0	0
0x2	0	0	0	0	0	0	0	0	4	0	0	4	2	2	2	2
0x3	0	0	0	0	0	0	0	0	4	0	0	4	2	2	2	2
0x4	0	4	0	0	0	0	4	0	0	2	2	0	2	0	0	2
0x5	0	4	0	0	0	0	4	0	0	2	2	0	2	0	0	2
0x6	0	4	0	0	4	0	0	0	0	2	2	0	0	2	2	0
0x7	0	4	0	0	0	0	0	4	0	2	2	0	0	2	2	0
0x8	0	0	4	4	0	0	0	0	4	0	4	0	0	0	0	0
0x9	0	0	0	0	2	2	2	2	0	0	0	0	2	2	2	2
0xa	0	0	0	0	2	2	2	2	4	0	4	0	0	0	0	0
0xb	0	0	4	4	0	0	0	0	0	0	0	0	2	2	2	2
0xc	0	0	2	2	2	2	0	0	0	2	0	2	2	0	2	0
0xd	0	0	2	2	0	0	2	2	0	2	0	2	0	2	0	2
0xe	0	0	2	2	0	0	2	2	0	2	0	2	2	0	2	0
0xf	0	0	2	2	2	2	0	0	0	2	0	2	0	2	0	2

Obtained differences

From injecting faults on Z_{19} or on W_{19}

$$(a_1, 0x1), (a_2, 0x8)$$

Difference distribution table of the PRIDE S-box

T	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf
0x0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0x1	0	0	0	0	4	4	4	4	0	0	0	0	0	0	0	0
0x2	0	0	0	0	0	0	0	0	4	0	0	4	2	2	2	2
0x3	0	0	0	0	0	0	0	0	4	0	0	4	2	2	2	2
0x4	0	4	0	0	0	0	4	0	0	2	2	0	2	0	0	2
0x5	0	4	0	0	0	4	0	0	0	2	2	0	2	0	0	2
0x6	0	4	0	0	4	0	0	0	0	2	2	0	0	2	2	0
0x7	0	4	0	0	0	0	0	4	0	2	2	0	0	2	2	0
0x8	0	0	4	4	0	0	0	0	4	0	4	0	0	0	0	0
0x9	0	0	0	0	2	2	2	2	0	0	0	0	2	2	2	2
0xa	0	0	0	0	2	2	2	2	4	0	4	0	0	0	0	0
0xb	0	0	4	4	0	0	0	0	0	0	0	0	2	2	2	2
0xc	0	0	2	2	2	2	0	0	0	2	0	2	2	0	2	0
0xd	0	0	2	2	0	0	2	2	0	2	0	2	0	2	0	2
0xe	0	0	2	2	0	0	2	2	0	2	0	2	2	0	2	0
0xf	0	0	2	2	2	2	0	0	0	2	0	2	0	2	0	2

Obtained differences

From injecting faults on Z_{19} or on W_{19}

$$(a_1, 0x1), (a_2, 0x8)$$

Difference distribution table of the PRIDE S-box

T	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf
0x0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0x1	0	0	0	0	4	4	4	4	0	0	0	0	0	0	0	0
0x2	0	0	0	0	0	0	0	0	4	0	0	4	2	2	2	2
0x3	0	0	0	0	0	0	0	0	4	0	0	4	2	2	2	2
0x4	0	4	0	0	0	0	4	0	0	2	2	0	2	0	0	2
0x5	0	4	0	0	0	4	0	0	0	2	2	0	2	0	0	2
0x6	0	4	0	0	4	0	0	0	0	2	2	0	0	2	2	0
0x7	0	4	0	0	0	0	0	4	0	2	2	0	0	2	2	0
0x8	0	0	4	4	0	0	0	0	4	0	4	0	0	0	0	0
0x9	0	0	0	0	2	2	2	2	0	0	0	0	2	2	2	2
0xa	0	0	0	0	2	2	2	2	4	0	4	0	0	0	0	0
0xb	0	0	4	4	0	0	0	0	0	0	0	0	2	2	2	2
0xc	0	0	2	2	2	2	0	0	0	2	0	2	2	0	2	0
0xd	0	0	2	2	0	0	2	2	0	2	0	2	0	2	0	2
0xe	0	0	2	2	0	0	2	2	0	2	0	2	2	0	2	0
0xf	0	0	2	2	2	2	0	0	0	2	0	2	0	2	0	2

Obtained differences

From injecting faults on Z_{19} or on W_{19}

$$(a_1, 0x1), (a_2, 0x8)$$

Difference distribution table of the PRIDE S-box

T	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf
0x0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0x1	0	0	0	0	4	4	4	4	0	0	0	0	0	0	0	0
0x2	0	0	0	0	0	0	0	0	4	0	0	4	2	2	2	2
0x3	0	0	0	0	0	0	0	0	4	0	0	4	2	2	2	2
0x4	0	4	0	0	0	0	4	0	0	2	2	0	2	0	0	2
0x5	0	4	0	0	0	4	0	0	0	2	2	0	2	0	0	2
0x6	0	4	0	0	4	0	0	0	0	2	2	0	0	2	2	0
0x7	0	4	0	0	0	0	0	4	0	2	2	0	0	2	2	0
0x8	0	0	4	4	0	0	0	0	4	0	4	0	0	0	0	0
0x9	0	0	0	0	2	2	2	2	0	0	0	0	2	2	2	2
0xa	0	0	0	0	2	2	2	2	4	0	4	0	0	0	0	0
0xb	0	0	4	4	0	0	0	0	0	0	0	0	2	2	2	2
0xc	0	0	2	2	2	2	0	0	0	2	0	2	2	0	2	0
0xd	0	0	2	2	0	0	2	2	0	2	0	2	0	2	0	2
0xe	0	0	2	2	0	0	2	2	0	2	0	2	2	0	2	0
0xf	0	0	2	2	2	2	0	0	0	2	0	2	0	2	0	2

Obtained differences

From injecting faults on Z_{19} or on W_{19}

$$(a_1, 0x1), (a_2, 0x8)$$

Difference distribution table of the PRIDE S-box

T	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf
0x0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0x1	0	0	0	0	4	4	4	4	0	0	0	0	0	0	0	0
0x2	0	0	0	0	0	0	0	0	4	0	0	4	2	2	2	2
0x3	0	0	0	0	0	0	0	0	4	0	0	4	2	2	2	2
0x4	0	4	0	0	0	0	4	0	0	2	2	0	2	0	0	2
0x5	0	4	0	0	0	4	0	0	0	2	2	0	2	0	0	2
0x6	0	4	0	0	4	0	0	0	0	2	2	0	0	2	2	0
0x7	0	4	0	0	0	0	0	4	0	2	2	0	0	2	2	0
0x8	0	0	4	4	0	0	0	0	4	0	4	0	0	0	0	0
0x9	0	0	0	0	2	2	2	2	0	0	0	0	2	2	2	2
0xa	0	0	0	0	2	2	2	2	4	0	4	0	0	0	0	0
0xb	0	0	4	4	0	0	0	0	0	0	0	0	2	2	2	2
0xc	0	0	2	2	2	2	0	0	0	2	0	2	2	0	2	0
0xd	0	0	2	2	0	0	2	2	0	2	0	2	0	2	0	2
0xe	0	0	2	2	0	0	2	2	0	2	0	2	2	0	2	0
0xf	0	0	2	2	2	2	0	0	0	2	0	2	0	2	0	2

Obtained differences

From injecting faults on Z_{19} or on W_{19}

$$(a_1, 0x1), (a_2, 0x8)$$

Difference distribution table of the PRIDE S-box

T	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf
0x0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0x1	0	0	0	0	4	4	4	4	0	0	0	0	0	0	0	0
0x2	0	0	0	0	0	0	0	0	4	0	0	4	2	2	2	2
0x3	0	0	0	0	0	0	0	0	4	0	0	4	2	2	2	2
0x4	0	4	0	0	0	0	4	0	0	2	2	0	2	0	0	2
0x5	0	4	0	0	0	4	0	0	0	2	2	0	2	0	0	2
0x6	0	4	0	0	4	0	0	0	0	2	2	0	0	2	2	0
0x7	0	4	0	0	0	0	0	4	0	2	2	0	0	2	2	0
0x8	0	0	4	4	0	0	0	0	4	0	4	0	0	0	0	0
0x9	0	0	0	0	2	2	2	2	0	0	0	0	2	2	2	2
0xa	0	0	0	0	2	2	2	2	4	0	4	0	0	0	0	0
0xb	0	0	4	4	0	0	0	0	0	0	0	0	2	2	2	2
0xc	0	0	2	2	2	2	0	0	0	2	0	2	2	0	2	0
0xd	0	0	2	2	0	0	2	2	0	2	0	2	0	2	0	2
0xe	0	0	2	2	0	0	2	2	0	2	0	2	2	0	2	0
0xf	0	0	2	2	2	2	0	0	0	2	0	2	0	2	0	2

- **The design of the linear layer**
  - Flip the 16-bit output of one matrix after the $\mathcal{L}$-layer activates all S-boxes in the next round.

  Use this property on the penultimate round allows the attacker to recover information on all nibbles of k_0.

  The number of remaining candidates is at most 4^{16}, where 4 is the differential-uniformity of the PRIDE S-box.

- **The differential properties of the S-box**

  The number of inputs which satisfy two valid differentials simultaneously is usually reduced to a single element.

  It is the case in each nibble for the presented strategies.

- **The design of the linear layer**
  - Flip the 16-bit output of one matrix after the $\mathcal{L}$-layer activates all S-boxes in the next round.
  - Use this property on the penultimate round allows the attacker to recover information on all nibbles of k_0.

The number of remaining candidates is at most 4^{16}, where 4 is the differential-uniformity of the PRIDE S-box.

The differential properties of the S-box

The number of inputs which satisfy two valid differentials simultaneously is usually reduced to a single element.

It is the case in each nibble for the presented strategies.

- **The design of the linear layer**
  - Flip the 16-bit output of one matrix after the $\mathcal{L}$-layer activates all S-boxes in the next round.
  - Use this property on the penultimate round allows the attacker to recover information on all nibbles of k_0.
  - The number of remaining candidates is at most 4^{16}, where 4 is the differential-uniformity of the PRIDE S-box.

- **The differential properties of the S-box**

  The number of inputs which satisfy two valid differentials simultaneously is usually reduced to a single element.

  It is the case in each nibble for the presented strategies.

- **The design of the linear layer**
  - Flip the 16-bit output of one matrix after the $\mathcal{L}$-layer activates all S-boxes in the next round.
  - Use this property on the penultimate round allows the attacker to recover information on all nibbles of k_0.
  - The number of remaining candidates is at most 4^{16}, where 4 is the differential-uniformity of the PRIDE S-box.
- **The differential properties of the S-box**
  - The number of inputs which satisfy two valid differentials simultaneously is usually reduced to a single element.

    It is the case in each nibble for the presented strategies.

- **The design of the linear layer**
  - Flip the 16-bit output of one matrix after the $\mathcal{L}$-layer activates all S-boxes in the next round.
  - Use this property on the penultimate round allows the attacker to recover information on all nibbles of k_0.
  - The number of remaining candidates is at most 4^{16}, where 4 is the differential-uniformity of the PRIDE S-box.
- **The differential properties of the S-box**
  - The number of inputs which satisfy two valid differentials simultaneously is usually reduced to a single element.
  - It is the case in each nibble for the presented strategies.

Practical implementation of the DFA on PRIDE

The chip used and our PRIDE implementation

- We have implemented PRIDE on a chip embedding an Cortex-M3 micro-controller. It is quite representative of the devices used for IoT applications.

In order to take advantage of the 32-bit architecture of the micro-controller, we have implemented PRIDE in ARM assembly language.

The faults injection device

We used electromagnetic pulses to disrupt PRIDE execution. This approach requires no decapsulation of the chip and allows to precisely target a given time.

We used a simple EM analysis to identify in time the 18-th and 19-th rounds.

- **The chip used and our PRIDE implementation**
  - We have implemented PRIDE on a chip embedding an Cortex-M3 micro-controller. It is quite representative of the devices used for IoT applications.
  - In order to take advantage of the 32-bit architecture of the micro-controller, we have implemented PRIDE in ARM assembly language.

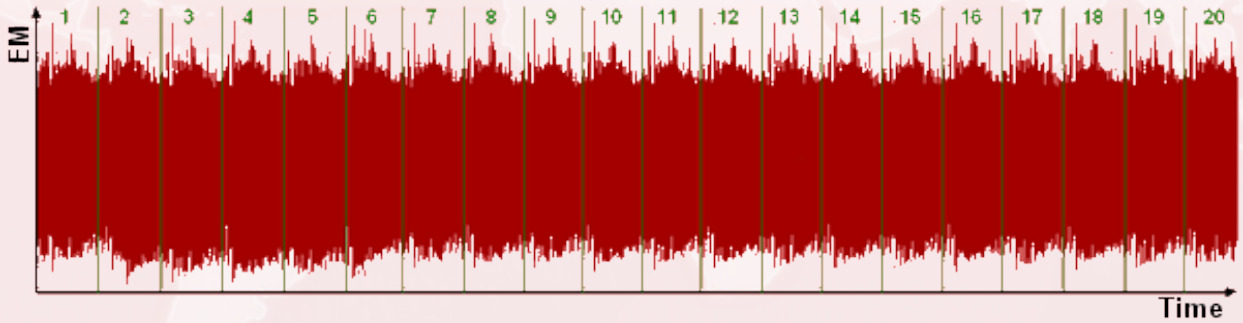
The faults injection device

We used electromagnetic pulses to disrupt PRIDE execution. This approach requires no decapsulation of the chip and allows to precisely target a given time.

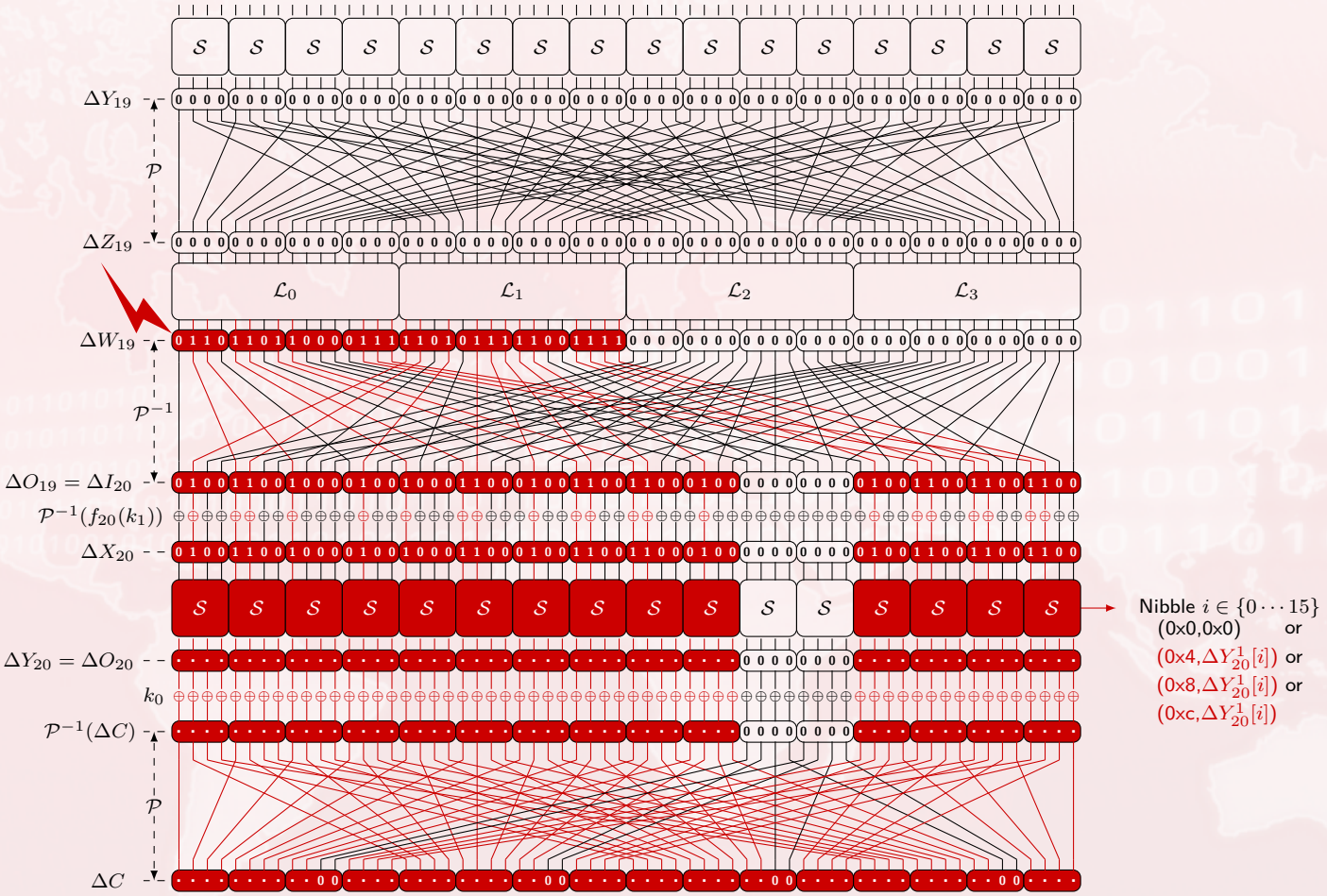
We used a simple EM analysis to identify in time the 18-th and 19-th rounds.

- **The chip used and our PRIDE implementation**
  - We have implemented PRIDE on a chip embedding an Cortex-M3 micro-controller. It is quite representative of the devices used for IoT applications.
  - In order to take advantage of the 32-bit architecture of the micro-controller, we have implemented PRIDE in ARM assembly language.
- **The faults injection device**
  - We used electromagnetic pulses to disrupt PRIDE execution. This approach requires no decapsulation of the chip and allows to precisely target a given time.
  - We used a simple EM analysis to identify in time the 18-th and 19-th rounds.

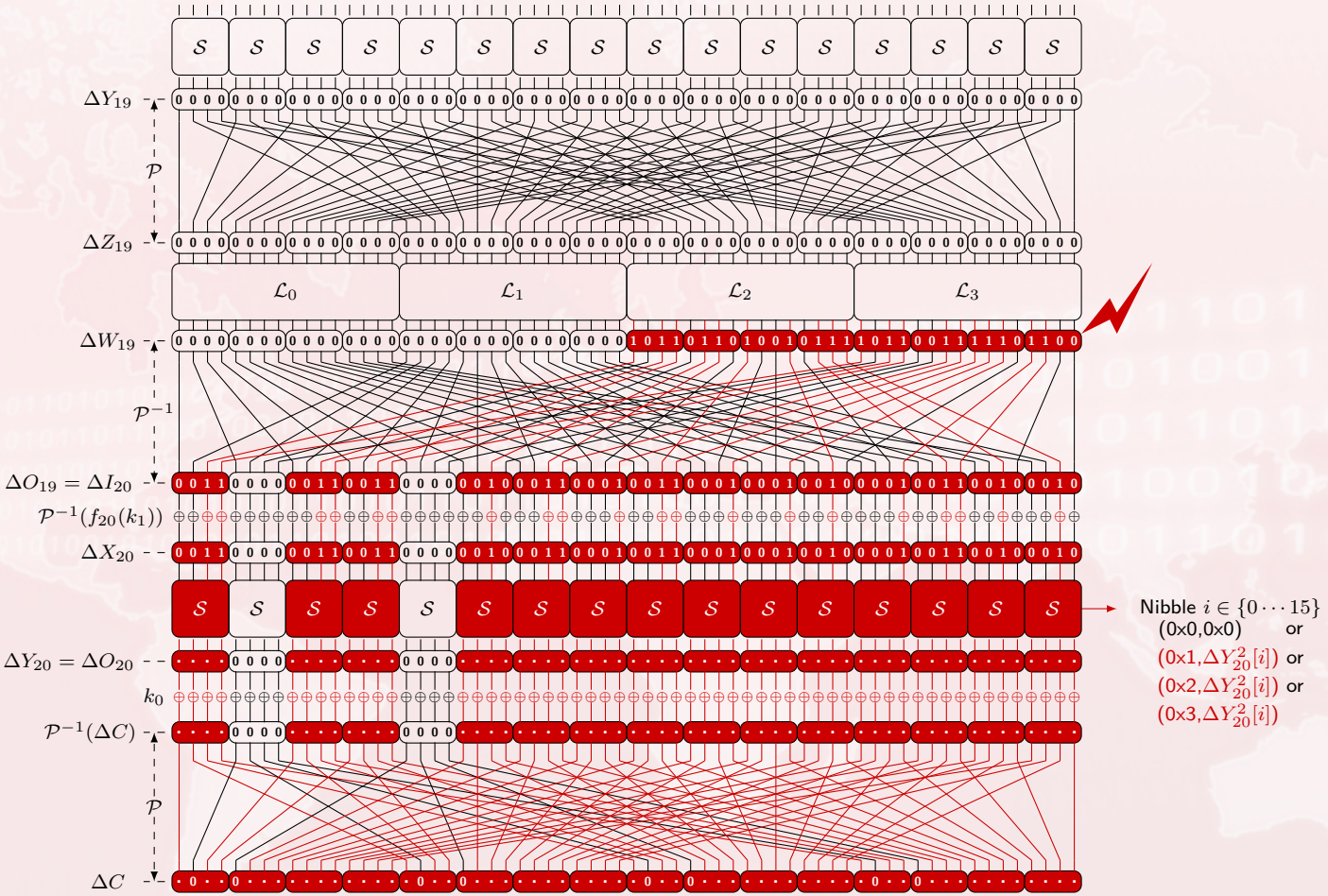
- **The chip used and our PRIDE implementation**
  - We have implemented PRIDE on a chip embedding an Cortex-M3 micro-controller. It is quite representative of the devices used for IoT applications.
  - In order to take advantage of the 32-bit architecture of the micro-controller, we have implemented PRIDE in ARM assembly language.
- **The faults injection device**
  - We used electromagnetic pulses to disrupt PRIDE execution. This approach requires no decapsulation of the chip and allows to precisely target a given time.
  - We used a simple EM analysis to identify in time the 18-th and 19-th rounds.



32-bit random faults on W_{19}



32-bit random faults on W_{19}



The parameter values

- We used a key $k = k_0||k_1$ where

$$k_0 = \text{0xf3f721cb1c882658 and } k_1 = \text{0xe417d148e239ca5d}$$

The plaintext used for all executions was 0x0132546798badcfe and the correct ciphertext was 0x9aecb37ea45a6c89. We denote respectively by θ, β, γ, δ the possible pair of values (0x2,0x3), (0x4,0x8), (0x4,0xc), (0x8,0xc).

The obtained faults on the 19-th round

No.	Faulty ciphertext	Value of the fault on W_{19}	Value of ΔY_{20}	Value of ΔX_{20}
1	0x1aad3b972c92ec09	0x00000000804108e8	0xf00060007e40600c	0xθ0001000$1\theta$101000θ
2	0x7b4c93dea55a6d89	0x00000000e1a0a0a0	0x88c0000bc0c00000	0x$\theta\theta\theta$0000$\theta\theta$0θ00000
3	0x1b6c733e255aadc9	0x0000000081804040	0xf500000b85000000	0xθ100000$\theta\theta$1000000
4	0x71ecd27ee55a6d89	0x00000000eb00e900	0x8ec0808f00000000	0x$\theta\theta\theta$0θ0$\theta\theta$00000000
5	0x9aecb324a4426cdb	0x000000000000005a	0x0000000005076050	0x0000000001011010
6	0x9a57b33fa4626cf1	0x0000000000bb005a	0x0000000085bbb08c	0x00000000θ1$\theta\theta\theta$0$\theta\theta$
7	0x9a57b365a4606cb9	0x0000000000bb0000	0x0000000080bfe0ec	0x00000000θ0$\theta\theta\theta$0$\theta\theta$
8	0x77aa24313111ed8c	0x00000000ed461f4d	0xf8868e4f0e006de7	0x$\theta\theta\theta$1$\theta\theta$1θ0θ001$\theta\theta$1
9	0x9ae8b37ac15a6989	0x6500040400000000	0x0220030300000c00	0x0$\delta\delta$00δ0δ00000γ00
10	0x8aecb27e415abc89	0xe400d10000000000	0x3329020600000000	0x$\delta\delta\delta\gamma$0δ0400000000
11	0xa3e692ed909ee688	0x355fab9300000000	0x10ea921c620482c5	0x40c$\beta\gamma\delta$4γ4δ0c8$\delta\gamma$c
12	0x05ecb27e565a7289	0xf3001f0000000000	0xa22b99bc00000000	0x$\beta\delta\delta$c$\gamma\gamma$cγ00000000

- **The parameter values**
  - We used a key $k = k_0||k_1$ where

$$k_0 = \text{0xf3f721cb1c882658 and } k_1 = \text{0xe417d148e239ca5d}$$

  - The plaintext used for all executions was 0x0132546798badcfe and the correct ciphertext was 0x9aecb37ea45a6c89. We denote respectively by θ, β, γ, δ the possible pair of values (0x2,0x3), (0x4,0x8), (0x4,0xc), (0x8,0xc).

The obtained faults on the 19-th round

No.	Faulty ciphertext	Value of the fault on W_{19}	Value of ΔY_{20}	Value of ΔX_{20}
1	0x1aad3b972c92ec09	0x00000000804108e8	0xf00060007e40600c	0xθ0001000$1\theta$101000θ
2	0x7b4c93dea55a6d89	0x00000000e1a0a0a0	0x88c0000bc0c00000	0x$\theta\theta\theta$0000$\theta\theta$0θ00000
3	0x1b6c733e255aadc9	0x0000000081804040	0xf500000b85000000	0xθ100000$\theta\theta$1000000
4	0x71ecd27ee55a6d89	0x00000000eb00e900	0x8ec0808f00000000	0x$\theta\theta\theta$0θ0$\theta\theta$00000000
5	0x9aecb324a4426cdb	0x000000000000005a	0x0000000005076050	0x0000000001011010
6	0x9a57b33fa4626cf1	0x0000000000bb005a	0x0000000085bbb08c	0x00000000θ1$\theta\theta\theta$0$\theta\theta$
7	0x9a57b365a4606cb9	0x0000000000bb0000	0x0000000080bfe0ec	0x00000000θ0$\theta\theta\theta$0$\theta\theta$
8	0x77aa24313111ed8c	0x00000000ed461f4d	0xf8868e4f0e006de7	0x$\theta\theta\theta$1$\theta\theta$1θ0θ001$\theta\theta$1
9	0x9ae8b37ac15a6989	0x6500040400000000	0x0220030300000c00	0x0$\delta\delta$00δ0δ00000γ00
10	0x8aecb27e415abc89	0xe400d10000000000	0x3329020600000000	0x$\delta\delta\delta\gamma$0δ0400000000
11	0xa3e692ed909ee688	0x355fab9300000000	0x10ea921c620482c5	0x40c$\beta\gamma\delta$4γ4δ0c8$\delta\gamma$c
12	0x05ecb27e565a7289	0xf3001f0000000000	0xa22b99bc00000000	0x$\beta\delta\delta$c$\gamma\gamma$cγ00000000

The parameter values

- We used a key $k = k_0||k_1$ where

$$k_0 = \text{0xf3f721cb1c882658 and } k_1 = \text{0xe417d148e239ca5d}$$

- The plaintext used for all executions was 0x0132546798badcfe and the correct ciphertext was 0x9aecb37ea45a6c89. We denote respectively by θ, β, γ, δ the possible pair of values (0x2,0x3), (0x4,0x8), (0x4,0xc), (0x8,0xc).

The obtained faults on the 19-th round

No.	Faulty ciphertext	Value of the fault on W_{19}	Value of ΔY_{20}	Value of ΔX_{20}
1	0x1aad3b972c92ec09	0x00000000804108e8	0xf00060007e40600c	0xθ0001000$1\theta$10100θ
2	0x7b4c93dea55a6d89	0x00000000e1a0a0a0	0x88c0000bc0c00000	0x$\theta\theta\theta$0000$\theta\theta$0θ00000
3	0x1b6c733e255aadc9	0x0000000081804040	0xf500000b85000000	0xθ100000$\theta\theta$1000000
4	0x71ecd27ee55a6d89	0x00000000eb00e900	0x8ec0808f00000000	0x$\theta\theta\theta$0θ0$\theta\theta$00000000
5	0x9aecb324a4426cdb	0x000000000000005a	0x0000000005076050	0x0000000001011010
6	0x9a57b33fa4626cf1	0x0000000000bb005a	0x0000000085bbb08c	0x0000000θ1$\theta\theta\theta$0$\theta\theta$
7	0x9a57b365a4606cb9	0x0000000000bb0000	0x0000000080bfe0ec	0x0000000θ0$\theta\theta\theta$0$\theta\theta$
8	0x77aa24313111ed8c	0x00000000ed461f4d	0xf8868e4f0e006de7	0x$\theta\theta\theta$1$\theta\theta$1θ0θ001$\theta\theta$1
9	0x9ae8b37ac15a6989	0x6500040400000000	0x0220030300000c00	0x0$\delta\delta$00δ0δ00000γ00
10	0x8aecb27e415abc89	0xe400d10000000000	0x3329020600000000	0x$\delta\delta\delta\gamma$0δ0400000000
11	0xa3e692ed909ee688	0x355fab9300000000	0x10ea921c620482c5	0x40c$\beta\gamma\delta$4γ4δ0c8$\delta\gamma$c
12	0x05ecb27e565a7289	0xf3001f0000000000	0xa22b99bc00000000	0x$\beta\delta\delta$c$\gamma\gamma$cγ00000000

Exploitation of the faults to retrieve k_0

No.	$k_0[0]$	$k_0[1]$	$k_0[2]$	$k_0[3]$	$k_0[4]$	$k_0[5]$	$k_0[6]$	$k_0[7]$	$k_0[8]$	$k_0[9]$	$k_0[10]$	$k_0[11]$	$k_0[12]$	$k_0[13]$	$k_0[14]$	$k_0[15]$
1	0x0 0x1 0xe 0xf	∅	∅	∅	0x2 0x3 0x4 0x5	∅	∅	∅	0x0 0x1 0x6 0x7	0x2 0x3 0xc 0xd	0x8 0x9 0xc 0xd	∅	0x2 0x3 0x4 0x5	∅	∅	0x4 0x5 0x8 0x9
3	0x0 0x1 0xe 0xf	0x2 0x3 0x6 0x7	∅	∅	∅	∅	∅	0x0 0x1 0x2 0x3 0x8 0x9 0xa 0xb	0x0 0x1 0x2 0x3 0x8 0x9 0xa 0xb	0x8 0x9 0xc 0xd	∅	∅	∅	∅	∅	∅
6	∅	∅	∅	∅	∅	∅	∅	∅	0x0 0x1 0x2 0x3 0x8 0x9 0xa 0xb	0x8 0x9 0xc 0xd	0x0 0x1 0x2 0x3 0x8 0x9 0xa 0xb	0x0 0x1 0x2 0x3 0x8 0x9 0xa 0xb	0x0 0x1 0x2 0x3 0x8 0x9 0xa 0xb	∅	0x4 0x5 0x6 0x7 0xc 0xd 0xe 0xf	0x4 0x5 0x8 0x9
8	0x0 0x1 0xe 0xf	0x0 0x1 0x2 0x3 0x8 0x9 0xa 0xb	0x4 0x5 0x6 0x7 0xc 0xd 0xe 0xf	0x0 0x1 0x6 0x7	0x0 0x1 0x2 0x3 0x8 0x9 0xa 0xb	0x0 0x1 0xe 0xf	0x8 0x9 0xc 0xd	0x4 0x5 0xa 0xb	∅	0x2 0x3 0xc 0xd	∅	∅	0x2 0x3 0x4 0x5	0x6 0x7 0xa 0xb	0x4 0x5 0xa 0xb	0x8 0x9 0xe 0xf
11	0xa 0xb 0xe 0xf	∅	0x1 0xf	0x1 0x5 0x7 0xb 0xd 0xf	0x2 0x4 0xb 0xd	0x1 0x3 0x4 0x6 0x9 0xb	0x8 0x9 0xc 0xd	0x2 0x7 0xb 0xe	0x0 0x1 0x6 0x7	0x4 0x6 0x9 0xb 0xc 0xe	∅	0x8 0xc	0x1 0x2 0x9 0xa	0x4 0x6 0x9 0xb 0xc 0xe	0x0 0x5 0x9 0xc	0x8 0xd
12	0x3 0x5 0x7 0x9 0xd 0xf	0x1 0x3 0x4 0x6 0x9 0xb	0x0 0x2 0x5 0x7 0xd 0xf	0x7 0xc	0x2 0x4 0xb 0xd	0x1 0x7 0x8 0xe	0x7 0xc	0x2 0x7 0xb 0xe	∅	∅	∅	∅	∅	∅	∅	∅
∩	0xf	0x3	0xf	0x7	0x2	0x1	0xc	0xb	0x0 0x1	0xc	0x8 0x9	0x8	0x2	0x6	0x5	0x8

- **Reducing the remaining candidates for k_0 from faults obtained on the 18-th round**
  - From the faulty ciphertext 0xf24690de8df8cc89 obtained from a fault on W_{18}, we obtain the 4 following values for ΔY_{19} for each possible value of k_0

k_0	ΔY_{19}
f3f721cb0c882658	0xc000009022000000
f3f721cb0c982658	0xe000009022220000
f3f721cb1c882658	0xc00000b000000000
f3f721cb1c982658	0xe00000b000220000

and since we know that we injected faults on the last 32 bits of W_{18}, we know that each nibble of ΔX_{19} is either 0x0, 0x1, 0x2 or 0x3.

From the difference distribution table of the S-box, we see that an input difference equal to 0x1, 0x2 or 0x3 can lead to an output difference only in

{0x4, 0x5, 0x6, 0x7, 0x8, 0xb, 0xc, 0xd, 0xe, 0xf}

- **Reducing the remaining candidates for k_0 from faults obtained on the 18-th round**
  - From the faulty ciphertext 0xf24690de8df8cc89 obtained from a fault on W_{18}, we obtain the 4 following values for ΔY_{19} for each possible value of k_0

k_0	ΔY_{19}
f3f721cb0c882658	0xc000009022000000
f3f721cb0c982658	0xe000009022220000
f3f721cb1c882658	0xc00000b000000000
f3f721cb1c982658	0xe00000b000220000

and since we know that we injected faults on the last 32 bits of W_{18}, we know that each nibble of ΔX_{19} is either 0x0, 0x1, 0x2 or 0x3.

From the difference distribution table of the S-box, we see that an input difference equal to 0x1, 0x2 or 0x3 can lead to an output difference only in

$$\{0x4, 0x5, 0x6, 0x7, 0x8, 0xb, 0xc, 0xd, 0xe, 0xf\}$$

- **Reducing the remaining candidates for k_0 from faults obtained on the 18-th round**
  - From the faulty ciphertext 0xf24690de8df8cc89 obtained from a fault on W_{18}, we obtain the 4 following values for ΔY_{19} for each possible value of k_0

k_0	ΔY_{19}
f3f721cb0c882658	0xc000009022000000
f3f721cb0c982658	0xe000009022220000
f3f721cb1c882658	0xc00000b000000000
f3f721cb1c982658	0xe00000b000220000

and since we know that we injected faults on the last 32 bits of W_{18}, we know that each nibble of ΔX_{19} is either 0x0, 0x1, 0x2 or 0x3.

From the difference distribution table of the S-box, we see that an input difference equal to 0x1, 0x2 or 0x3 can lead to an output difference only in

{0x4, 0x5, 0x6, 0x7, 0x8, 0xb, 0xc, 0xd, 0xe, 0xf}

- **Reducing the remaining candidates for k_0 from faults obtained on the 18-th round**
  - From the faulty ciphertext 0xf24690de8df8cc89 obtained from a fault on W_{18}, we obtain the 4 following values for ΔY_{19} for each possible value of k_0

k_0	ΔY_{19}
f3f721cb0c882658	0xc000009022000000
f3f721cb0c982658	0xe000009022220000
f3f721cb1c882658	0xc00000b000000000
f3f721cb1c982658	0xe00000b000220000

and since we know that we injected faults on the last 32 bits of W_{18}, we know that each nibble of ΔX_{19} is either 0x0, 0x1, 0x2 or 0x3.

  - From the difference distribution table of the S-box, we see that an input difference equal to 0x1, 0x2 or 0x3 can lead to an output difference only in

$$\{0x4, 0x5, 0x6, 0x7, 0x8, 0xb, 0xc, 0xd, 0xe, 0xf\}$$

- **Reducing the remaining candidates for k_0 from faults obtained on the 18-th round**
  - From the faulty ciphertext 0xf24690de8df8cc89 obtained from a fault on W_{18}, we obtain the 4 following values for ΔY_{19} for each possible value of k_0

k_0	ΔY_{19}
f3f721cb0c882658	0xc000009022000000
f3f721cb0c982658	0xe000009022220000
f3f721cb1c882658	0xc00000b000000000
f3f721cb1c982658	0xe00000b000220000

and since we know that we injected faults on the last 32 bits of W_{18}, we know that each nibble of ΔX_{19} is either 0x0, 0x1, 0x2 or 0x3.

  - From the difference distribution table of the S-box, we see that an input difference equal to 0x1, 0x2 or 0x3 can lead to an output difference only in

$$\{0x4, 0x5, 0x6, 0x7, 0x8, 0xb, 0xc, 0xd, 0xe, 0xf\}$$

- **Reducing the remaining candidates for k_0 from faults obtained on the 18-th round**
  - From the faulty ciphertext 0xf24690de8df8cc89 obtained from a fault on W_{18}, we obtain the 4 following values for ΔY_{19} for each possible value of k_0

k_0	ΔY_{19}
f3f721cb0c882658	0xc000009022000000
f3f721cb0c982658	0xe000009022220000
f3f721cb1c882658	0xc00000b000000000
f3f721cb1c982658	0xe00000b000220000

and since we know that we injected faults on the last 32 bits of W_{18}, we know that each nibble of ΔX_{19} is either 0x0, 0x1, 0x2 or 0x3.

  - From the difference distribution table of the S-box, we see that an input difference equal to 0x1, 0x2 or 0x3 can lead to an output difference only in

$$\{0x4, 0x5, 0x6, 0x7, 0x8, 0xb, 0xc, 0xd, 0xe, 0xf\}$$

The obtained faults on the 18-th round

No.	Faulty ciphertext	Value of the fault on W_{18}	Value of ΔY_{19}	Value of ΔX_{19}
13	0xf24690de8df8cc89	0x0000000082000000	0xc00000b000000000	0xθ0000θ000000000
14	0x2df93aebf5935009	0x0000000041c0d0d0	0x7807000bd8050000	0x1θ01000$\theta\theta\theta$010000
15	0xa9a4a34f84604dde	0x0000000003010707	0x000004cd0000065c	0x00001$\theta\theta$00000011θ
16	0x52c367c49a9b8786	0x0000000000b55858	0x05077000b6d84808	0x01011000θ1$\theta\theta$1θ0θ
17	0x00632c247f18e99e	0x0000000058580000	0x0e0bb0000d0ef000	0x0θ0$\theta\theta$0000θ0$\theta\theta$000
18	0xecbc98d50864ad3a	0x00000000a7a70000	0xc0f008bbb0d00888	0xθ0θ00$\theta\theta\theta\theta$0θ00$\theta\theta\theta$
19	0x43b733ec34c1ec11	0x0093000000000000	0x00000000300a0022	0x00000000δ00β00$\delta\delta$
20	0xcabdf870ee423736	0x75e5575700000000	0x0c8c0b123baf049e	0x0γ8γ0c4$\delta\delta$cβ40cγc
21	0x46eb59132610ef55	0x01e0c60100000000	0x6f0001133aa00006	0x4400044$\delta\delta\beta\beta$00004
22	0x9d13b57cf2211618	0x13974cd400000000	0x0f036133290c0422	0x040δ44$\delta\delta\delta\gamma$0γ0c$\delta\delta$
23	0x1247352b2400c0ed	0x0000006700000000	0x0000000009900c96	0x000000000$\gamma\gamma$00$\gamma\gamma$4
24	0x770a084c5528c599	0x6363000000000000	0x0a8000330aa00022	0x0β8000$\delta\delta$0$\beta\beta$000$\delta\delta$
25	0xc80ca16eb67b9711	0x3600a90000000000	0x6043623a00000000	0x40cδ4$\delta\delta\beta$00000000

We first retrieved each nibble Nib_i of $\mathcal{L}^{-1}(\mathcal{S}(\mathcal{P}^{-1}(C) \oplus k_0) \oplus \mathcal{P}^{-1}(f_{20}(k_1)))$.

Exploitation of the faults to retrieve $\mathcal{L}^{-1}(\mathcal{S}(\mathcal{P}^{-1}(C) \oplus k_0) \oplus \mathcal{P}^{-1}(f_{20}(k_1)))$

No.	Nib_0	Nib_1	Nib_2	Nib_3	Nib_4	Nib_5	Nib_6	Nib_7	Nib_8	Nib_9	Nib_{10}	Nib_{11}	Nib_{12}	Nib_{13}	Nib_{14}	Nib_{15}
16	∅	0x2 0x3 0x6 0x7	∅	0x8 0x9 0xe 0xf	0x8 0x9 0xe 0xf	∅	∅	∅	0x4 0x5 0x6 0x7 0xc 0xd 0xe 0xf	0xa 0xb 0xc 0xd	0x6 0x7 0xa 0xb	0x0 0x1 0x2 0x3 0x8 0x9 0xa 0xb	0x0 0x1 0x4 0x5	0x0 0x1 0x2 0x3 0x8 0x9 0xa 0xb	∅	0x0 0x1 0x2 0x3 0x8 0x9 0xa 0xb
17	∅	0x2 0x3 0xa 0xb	∅	0x4 0x5 0x6 0x7 0xc 0xd 0xe 0xf	0x4 0x5 0x6 0x7 0xc 0xd 0xe 0xf	∅	∅	∅	∅	0x6 0x7 0xa 0xb	∅	0x2 0x3 0xa 0xb	0x0 0x1 0xe 0xf	∅	∅	∅
18	0x4 0x5 0x8 0x9	∅	0x0 0x1 0xe 0xf	∅	∅	0x0 0x1 0x2 0x3 0x8 0x9 0xa 0xb	0x4 0x5 0x6 0x7 0xc 0xd 0xe 0xf	0x4 0x5 0x6 0x7 0xc 0xd 0xe 0xf	0x4 0x5 0x6 0x7 0xc 0xd 0xe 0xf	∅	0x6 0x7 0xa 0xb	∅	∅	0x0 0x1 0x2 0x3 0x8 0x9 0xa 0xb	0x0 0x1 0x2 0x3 0x8 0x9 0xa 0xb	0x0 0x1 0x2 0x3 0x8 0x9 0xa 0xb
20	∅	0x3 0x6 0xa 0xf	0x5 0x6 0xd 0xe	0x3 0x6 0xa 0xf	∅	0x0 0xb	0x0 0x1 0x4 0x5	0x0 0x2 0x5 0x7 0x8 0xa	0x1 0x2 0x4 0x7 0xc 0xf	0x0 0xb	0x1 0x3 0x7 0x9 0xb 0xd	0x3 0xc	∅	0xa 0xe	0x2 0x4 0xb 0xd	0x6 0x8
22	∅	0x3 0xc	∅	0x1 0x2 0x4 0x7 0xc 0xf	0x8 0x9 0xe 0xf	0x0 0x1 0x4 0x5	0x1 0x2 0x4 0x7 0xc 0xf	0x1 0x2 0x4 0x7 0xc 0xf	0x0 0x2 0x5 0x7 0x8 0xa	0x2 0x4 0xb 0xd	∅	0x3 0x6 0xa 0xf	∅	0xa 0xe	0x0 0x2 0x5 0x7 0x8 0xa	0x0 0x2 0x5 0x7 0x8 0xa
23	∅	∅	∅	∅	∅	∅	∅	∅	∅	0x2 0x4 0xb 0xd	0x2 0x4 0xb 0xd	∅	∅	0x3 0x6 0xa 0xf	0x2 0x4 0xb 0xd	0x8 0x9 0xe 0xf
25	0x8 0x9 0xe 0xf	∅	0xa 0xe	0x1 0x2 0x4 0x7 0xc 0xf	0x8 0x9 0xe 0xf	0x0 0x2 0x5 0x7 0x8 0xa	0x1 0x2 0x4 0x7 0xc 0xf	0x1 0x3 0x7 0x9 0xb 0xd	∅	∅	∅	∅	∅	∅	∅	∅
∩	0x8 0x9	0x3	0xe	0xf	0xe 0xf	0x0	0x4	0x7	0x7	0xb	0xb	0x3	0x0 0x1	0xa	0x2	0x8

- **Calculating the value of k**
  - By intersecting sets for each nibble, we got 8 candidates for

$$\mathcal{L}^{-1}(\mathcal{S}(\mathcal{P}^{-1}(C) \oplus k_0) \oplus \mathcal{P}^{-1}(f_{20}(k_1)))$$

Then, we calculated the 8 possible $\mathcal{S}(\mathcal{P}^{-1}(C) \oplus k_0) \oplus \mathcal{P}^{-1}(f_{20}(k_1))$, and from

$$\mathcal{S}(\mathcal{P}^{-1}(C) \oplus k_0) = \text{0x128bb20f824eda39},$$

we deduced 8 candidates for $\mathcal{P}^{-1}(f_{20}(k_1))$.

Finally we got 8 values for $f_{20}(k_1)$ and so for k_1.

We eventually obtained, by testing all possible k_1, the secret key

$$k = \text{0xf3f721cb1c882658e417d148e239ca5d}$$

from a few number of faults.

- **Calculating the value of k**
  - By intersecting sets for each nibble, we got 8 candidates for

$$\mathcal{L}^{-1}(\mathcal{S}(\mathcal{P}^{-1}(C) \oplus k_0) \oplus \mathcal{P}^{-1}(f_{20}(k_1)))$$

  - Then, we calculated the 8 possible $\mathcal{S}(\mathcal{P}^{-1}(C) \oplus k_0) \oplus \mathcal{P}^{-1}(f_{20}(k_1))$, and from

$$\mathcal{S}(\mathcal{P}^{-1}(C) \oplus k_0) = \text{0x128bb20f824eda39},$$

we deduced 8 candidates for $\mathcal{P}^{-1}(f_{20}(k_1))$.

Finally we got 8 values for $f_{20}(k_1)$ and so for k_1.

We eventually obtained, by testing all possible k_1, the secret key

$$k = \text{0xf3f721cb1c882658e417d148e239ca5d}$$

from a few number of faults.

- **Calculating the value of k**
  - By intersecting sets for each nibble, we got 8 candidates for

$$\mathcal{L}^{-1}(\mathcal{S}(\mathcal{P}^{-1}(C) \oplus k_0) \oplus \mathcal{P}^{-1}(f_{20}(k_1)))$$

  - Then, we calculated the 8 possible $\mathcal{S}(\mathcal{P}^{-1}(C) \oplus k_0) \oplus \mathcal{P}^{-1}(f_{20}(k_1))$, and from

$$\mathcal{S}(\mathcal{P}^{-1}(C) \oplus k_0) = \text{0x128bb20f824eda39},$$

  we deduced 8 candidates for $\mathcal{P}^{-1}(f_{20}(k_1))$.
  - Finally we got 8 values for $f_{20}(k_1)$ and so for k_1.

We eventually obtained, by testing all possible k_1, the secret key

$$k = \text{0xf3f721cb1c882658e417d148e239ca5d}$$

from a few number of faults.

- **Calculating the value of k**
  - By intersecting sets for each nibble, we got 8 candidates for

$$\mathcal{L}^{-1}(\mathcal{S}(\mathcal{P}^{-1}(C) \oplus k_0) \oplus \mathcal{P}^{-1}(f_{20}(k_1)))$$

  - Then, we calculated the 8 possible $\mathcal{S}(\mathcal{P}^{-1}(C) \oplus k_0) \oplus \mathcal{P}^{-1}(f_{20}(k_1))$, and from

$$\mathcal{S}(\mathcal{P}^{-1}(C) \oplus k_0) = \text{0x128bb20f824eda39},$$

  we deduced 8 candidates for $\mathcal{P}^{-1}(f_{20}(k_1))$.
  - Finally we got 8 values for $f_{20}(k_1)$ and so for k_1.
  - We eventually obtained, by testing all possible k_1, the secret key

$$k = \text{0xf3f721cb1c882658e417d148e239ca5d}$$

  from a few number of faults.

Countermeasures

Description

$W_{17} \xrightarrow{\text{enc.}} O_{20}$

$W_{17} \xrightarrow{\text{enc.}} O'_{20}$

$W_{17} \xrightarrow{\text{enc.}} O''_{20}$

$O_{20} = O'_{20}\,?$ — True → O'_{20} ; False → O_{20}

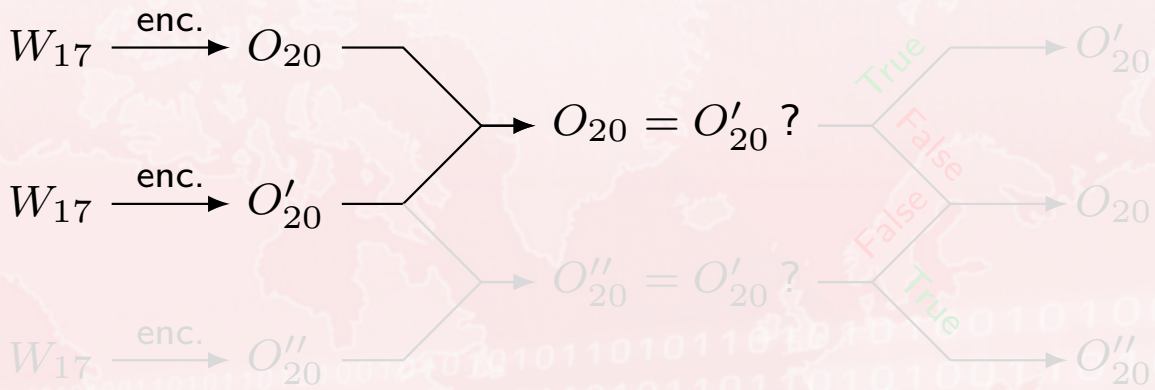
$O''_{20} = O'_{20}\,?$ — False → O_{20} ; True → O''_{20}

Cost per duplication

- 2 matrix layers
- 3 substitution layers
- 3 subkey updates
- 3 subkey additions

Total $< 15\%$ of PRIDE enc./dec.

Description

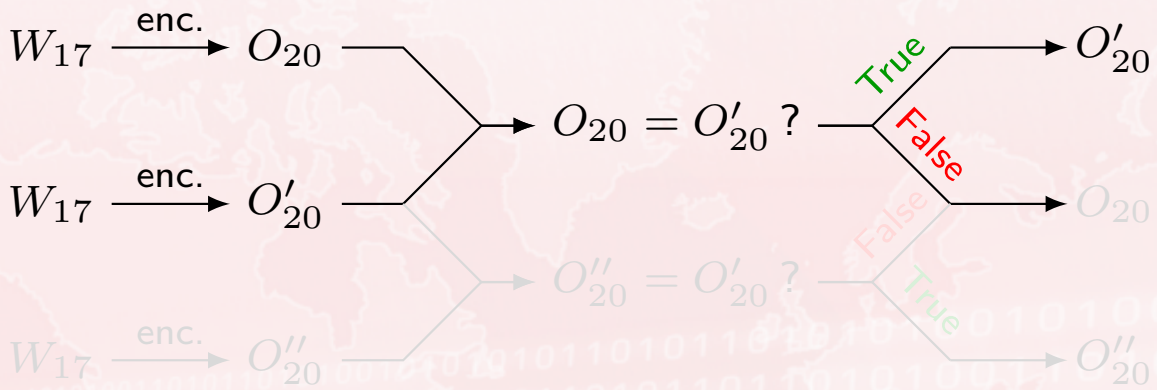


Cost per duplication

- 2 matrix layers
- 3 substitution layers
- 3 subkey updates
- 3 subkey additions

Total $< 15\%$ of PRIDE enc./dec.

Description

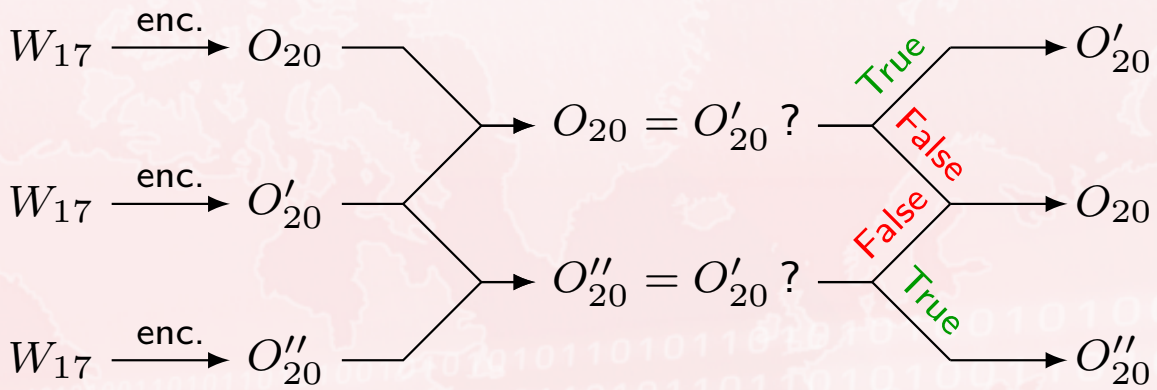


Cost per duplication

- 2 matrix layers
- 3 substitution layers
- 3 subkey updates
- 3 subkey additions

Total $<$ 15% of PRIDE enc./dec.

Description

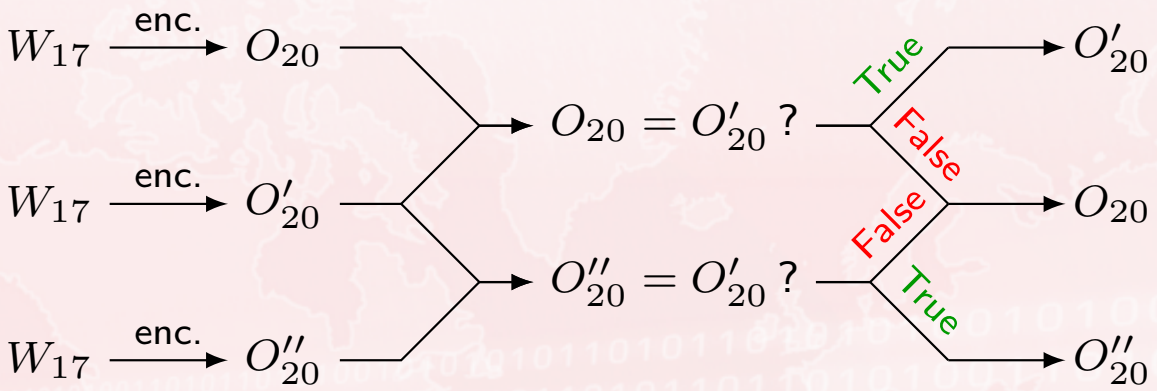


Cost per duplication

- 2 matrix layers
- 3 substitution layers
- 3 subkey updates
- 3 subkey additions

Total $< 15\%$ of PRIDE enc./dec.

Description

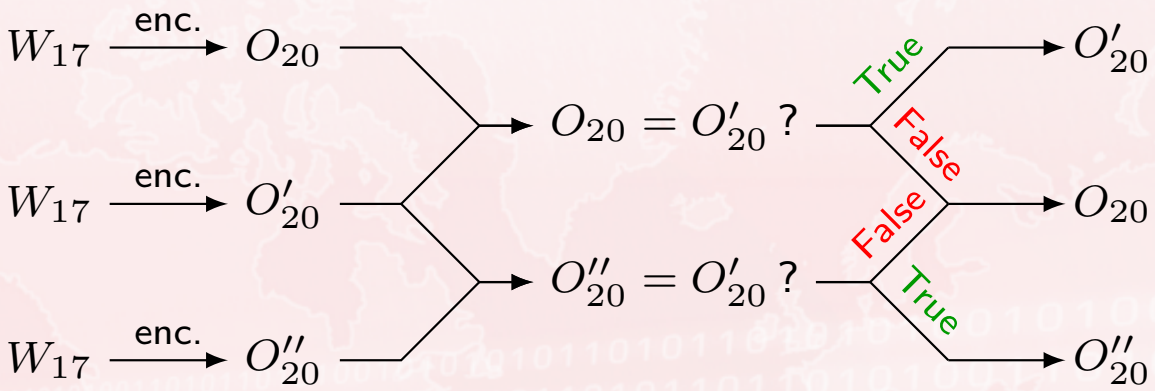


Cost per duplication

- 2 matrix layers
- 3 substitution layers
- 3 subkey updates
- 3 subkey additions

Total < 15% of PRIDE enc./dec.

Description

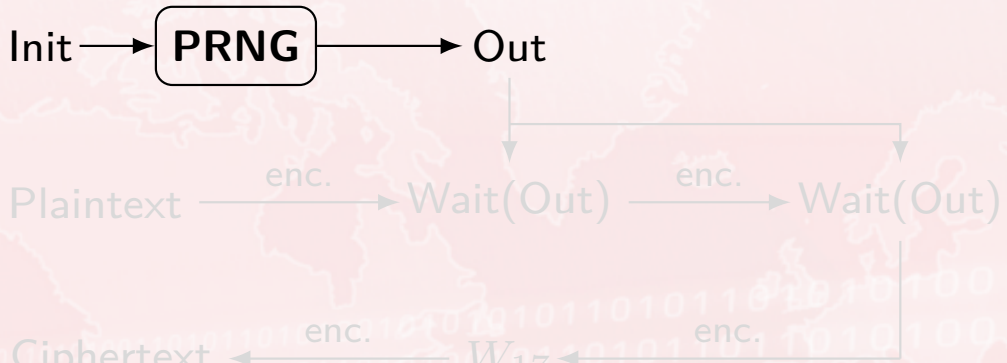


Cost per duplication

- 2 matrix layers
- 3 substitution layers
- 3 subkey updates
- 3 subkey additions

Total $<$ 15% of PRIDE enc./dec.

Description



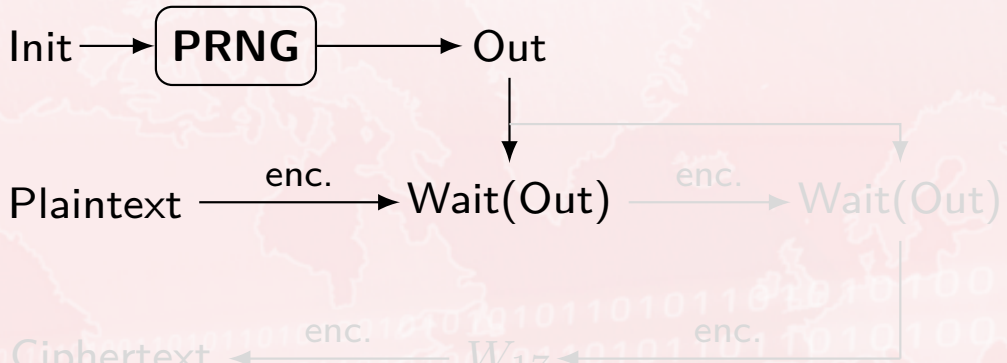
Cost

Generation of the PRNG's output

Access to the PRNG's output

Duration of the 'random delay'

Description



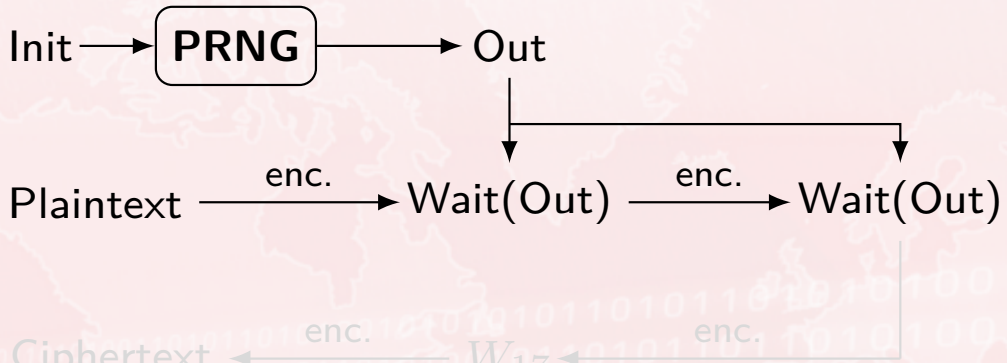
Cost

Generation of the PRNG's output

Access to the PRNG's output

Duration of the 'random delay'

Description



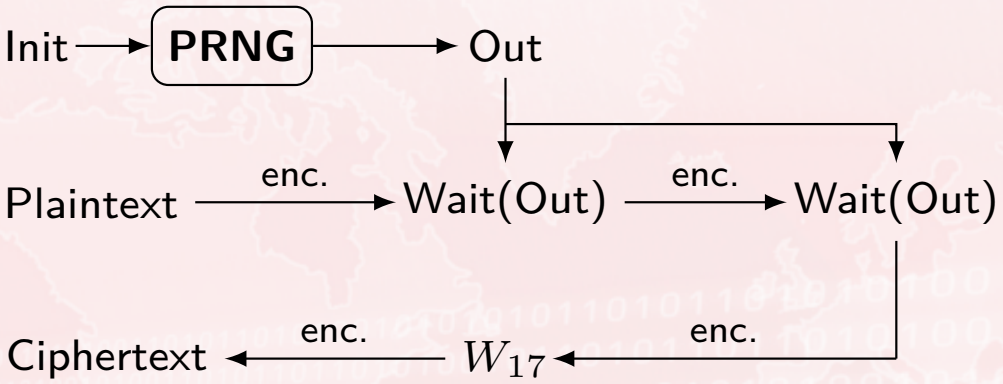
Cost

Generation of the PRNG's output

Access to the PRNG's output

Duration of the 'random delay'

Description



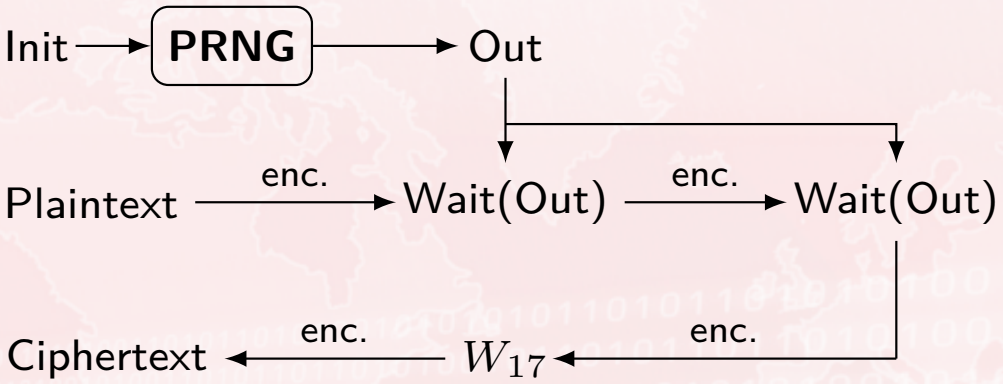
Cost

Generation of the PRNG's output

Access to the PRNG's output

Duration of the 'random delay'

Description



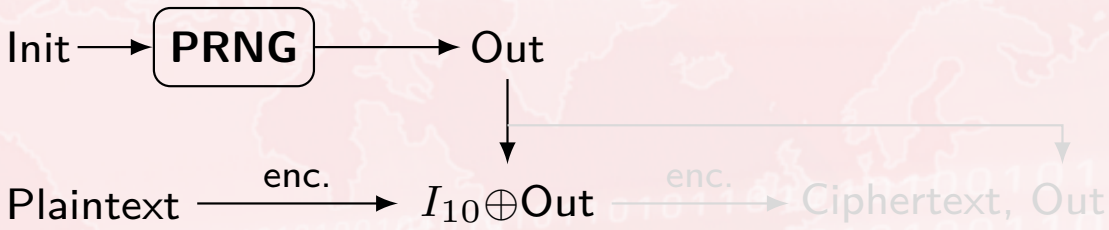
Cost

- Generation of the PRNG's output
- Access to the PRNG's output
- Duration of the 'random delay'

- **Description**

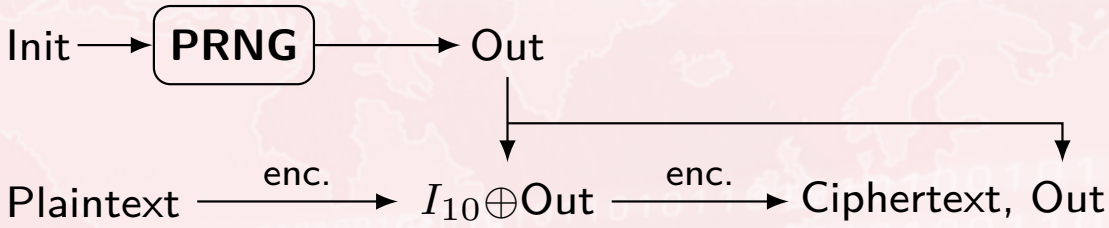
- **Cost**
  - Generation of the PRNG's output
  - Access to the PRNG's output

- **Description**



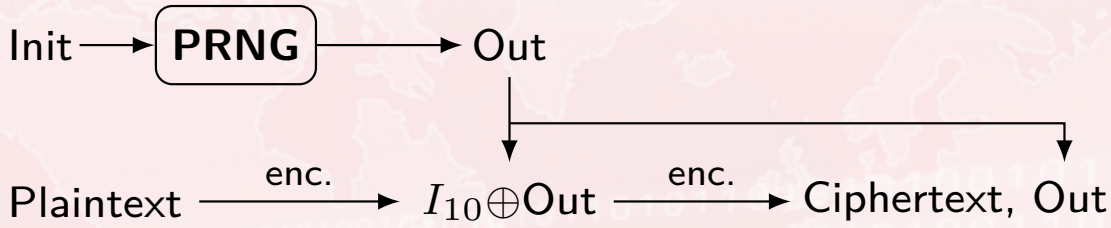
- Cost
  - Generation of the PRNG's output
  - Access to the PRNG's output

- **Description**



- Cost
  - Generation of the PRNG's output
  - Access to the PRNG's output

- **Description**



- **Cost**
  - Generation of the PRNG's output
  - Access to the PRNG's output

Conclusion and perspectives

Conclusion

- First DFA on PRIDE with 4 faults only to retrieve the full secret key.

  Practical implementation from 32-bit random faults obtained with electromagnetic injection, which is a low-cost means of injection.

  Resistance against DFA is important for a cipher like PRIDE, which will be dedicated to low-end devices thanks to its lightness.

  Some countermeasures which leave the cipher still efficient for IoT devices.

Perspectives

Optimize countermeasures to make them less costly and keep the light side of PRIDE : be careful that the protections do not open doors to further attacks.

Apply our attack to SPN-based block ciphers with a linear layer similar to the one used in PRIDE like the LS-Designs family : will be studied in a future work.

Conclusion

- First DFA on PRIDE with 4 faults only to retrieve the full secret key.
- Practical implementation from 32-bit random faults obtained with electromagnetic injection, which is a low-cost means of injection.

Resistance against DFA is important for a cipher like PRIDE, which will be dedicated to low-end devices thanks to its lightness.

Some countermeasures which leave the cipher still efficient for IoT devices.

Perspectives

Optimize countermeasures to make them less costly and keep the light side of PRIDE : be careful that the protections do not open doors to further attacks.

Apply our attack to SPN-based block ciphers with a linear layer similar to the one used in PRIDE like the LS-Designs family : will be studied in a future work.

Conclusion

- First DFA on PRIDE with 4 faults only to retrieve the full secret key.
- Practical implementation from 32-bit random faults obtained with electromagnetic injection, which is a low-cost means of injection.
- Resistance against DFA is important for a cipher like PRIDE, which will be dedicated to low-end devices thanks to its lightness.

Some countermeasures which leave the cipher still efficient for IoT devices.

Perspectives

Optimize countermeasures to make them less costly and keep the light side of PRIDE : be careful that the protections do not open doors to further attacks.

Apply our attack to SPN-based block ciphers with a linear layer similar to the one used in PRIDE like the LS-Designs family : will be studied in a future work.

Conclusion

- First DFA on PRIDE with 4 faults only to retrieve the full secret key.
- Practical implementation from 32-bit random faults obtained with electromagnetic injection, which is a low-cost means of injection.
- Resistance against DFA is important for a cipher like PRIDE, which will be dedicated to low-end devices thanks to its lightness.
- Some countermeasures which leave the cipher still efficient for IoT devices.

Perspectives

Optimize countermeasures to make them less costly and keep the light side of PRIDE : be careful that the protections do not open doors to further attacks.

Apply our attack to SPN-based block ciphers with a linear layer similar to the one used in PRIDE like the LS-Designs family : will be studied in a future work.

Conclusion

- First DFA on PRIDE with 4 faults only to retrieve the full secret key.
- Practical implementation from 32-bit random faults obtained with electromagnetic injection, which is a low-cost means of injection.
- Resistance against DFA is important for a cipher like PRIDE, which will be dedicated to low-end devices thanks to its lightness.
- Some countermeasures which leave the cipher still efficient for IoT devices.

Perspectives

- Optimize countermeasures to make them less costly and keep the light side of PRIDE : be careful that the protections do not open doors to further attacks.
- Apply our attack to SPN-based block ciphers with a linear layer similar to the one used in PRIDE like the LS-Designs family : will be studied in a future work.

Conclusion

- First DFA on PRIDE with 4 faults only to retrieve the full secret key.
- Practical implementation from 32-bit random faults obtained with electromagnetic injection, which is a low-cost means of injection.
- Resistance against DFA is important for a cipher like PRIDE, which will be dedicated to low-end devices thanks to its lightness.
- Some countermeasures which leave the cipher still efficient for IoT devices.

Perspectives

- Optimize countermeasures to make them less costly and keep the light side of PRIDE : be careful that the protections do not open doors to further attacks.
- Apply our attack to SPN-based block ciphers with a linear layer similar to the one used in PRIDE like the LS-Designs family : will be studied in a future work.

DE LA RECHERCHE À L'INDUSTRIE

THANKS FOR YOUR ATTENTION

Commissariat à l'énergie atomique et aux énergies alternatives

Benjamin Lac | DRT/CEATech/DPACA/LSAS

Public Industrial and Commercial Establishment | RCS Paris B 775 685 019