Oberthur Technologies

Differential Fault Analysis on DES Middle Rounds

Matthieu Rivain

Speaker: Christophe Giraud

Oberthur Technologies

Agenda

1. Introduction
   - Data Encryption Standard
   - DFA on DES Last & Middle Rounds
2. Our Attack
   - Principle
   - Fault Models
   - Attack Simulations
3. Conclusion

Outline

1. Introduction
   - Data Encryption Standard
   - DFA on DES Last & Middle Rounds
2. Our Attack
   - Principle
   - Fault Models
   - Attack Simulations
3. Conclusion

Data Encryption Standard (DES)

- 64-bit block cipher using a 56-bit key K

Data Encryption Standard (DES)

- 64-bit block cipher using a 56-bit key K
- Iterative structure: 16 times the same round transformation F
- Surrounded by bit-permutations IP and FP

Data Encryption Standard (DES)

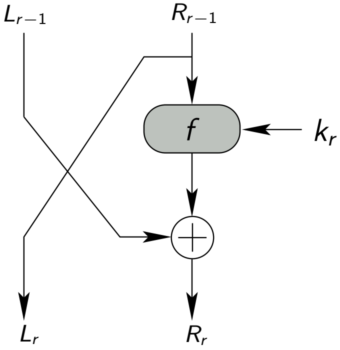
- 64-bit block cipher using a 56-bit key K
- Iterative structure: 16 times the same round transformation F
- Surrounded by bit-permutations IP and FP
- A ciphertext C is computed from a plaintext P as:

$$C = \mathsf{FP} \circ \left(\bigcirc_{r=1}^{16} \mathsf{F}_{k_r} \right) \circ \mathsf{IP}(P) \ .$$

where k_r is a 48-bit round key derived from K.

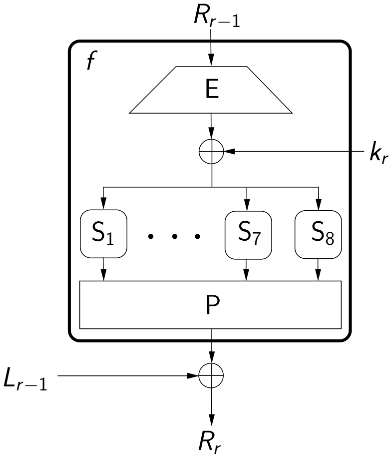
Data Encryption Standard (DES)

- F follows a Feistel scheme:



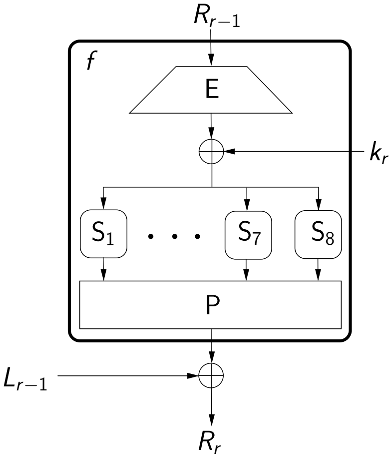
Data Encryption Standard (DES)

- Function f:

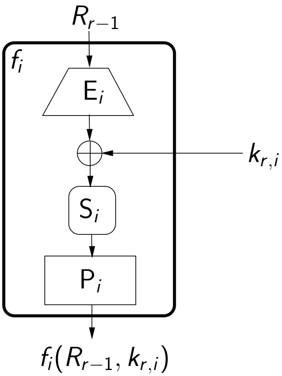


Data Encryption Standard (DES)

- Function f:



- Can be decomposed Sbox per Sbox:



Introduction to Fault Analysis

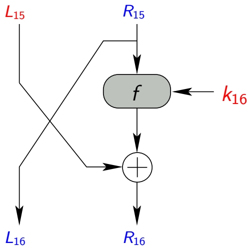
- Fault Attacks introduced in 1996 [BonehDeMilloLipton96]
- Applied to Asymmetric Cryptosystems : RSA, Rabin, Fiat-Shamir and Schnorr

Introduction to Fault Analysis

- Fault Attacks introduced in 1996 [BonehDeMilloLipton96]
- Applied to Asymmetric Cryptosystems : RSA, Rabin, Fiat-Shamir and Schnorr
- Followed by a dozen of notes on this subject over the next few weeks:
  - Improved attack on CRT RSA [Lenstra96]
  - Attacks on several signatures schemes (ElGamal, DSA) [BaoDengHanJengNarasimhaluNgair96]
  - A New Cryptanalytic Attack on DES [BihamShamir96]
    - Differential Fault Analysis (DFA)
  - ...

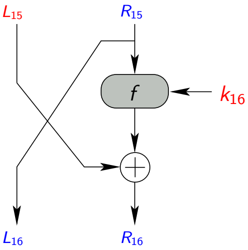
DFA on DES Last Round

- The last round:

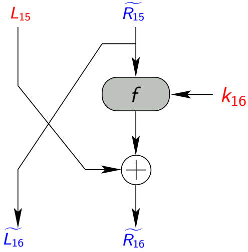


DFA on DES Last Round

- The last round:

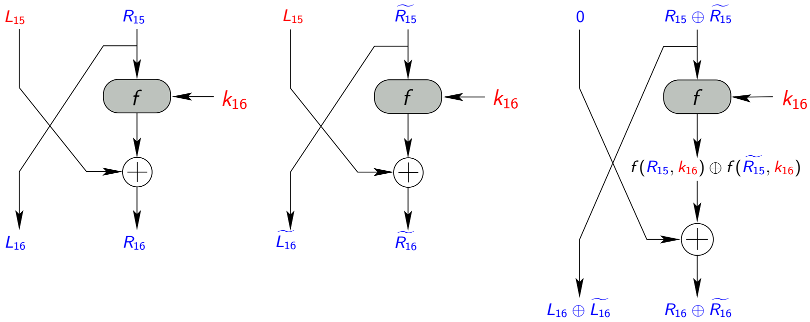


- If a fault is induced on R_{15}:



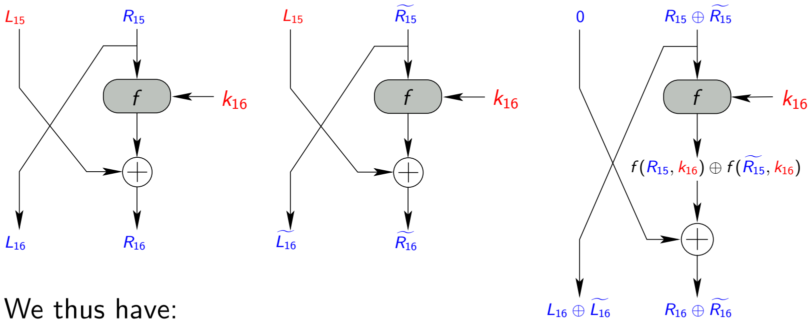
DFA on DES Last Round

- The last round:
- If a fault is induced on R_{15}:
- The corresponding differential:



DFA on DES Last Round

- The last round:
- If a fault is induced on R_{15}:
- The corresponding differential:

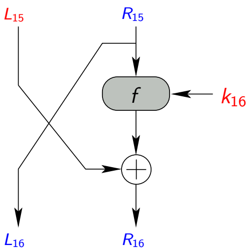


- We thus have:

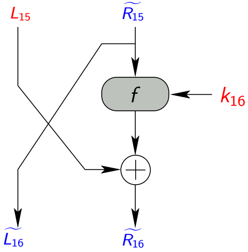
$$f(R_{15}, k_{16}) \oplus f(\widetilde{R_{15}}, k_{16}) = (R_{16} \oplus \widetilde{R_{16}})$$

DFA on DES Last Round

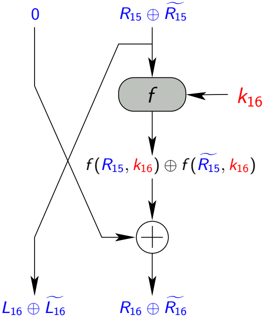
- The last round:



- If a fault is induced on R_{15}:



- The corresponding differential:



- We thus have:

$$f(R_{15}, k_{16}) \oplus f(\widetilde{R_{15}}, k_{16}) = (R_{16} \oplus \widetilde{R_{16}})$$

- This relation holds for each SBox independently :

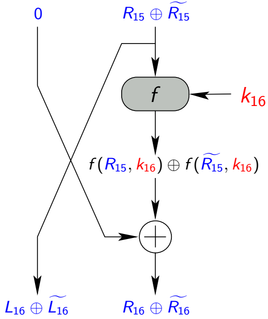
$$f_i(R_{15}, k_{16,i}) \oplus f_i(\widetilde{R_{15}}, k_{16,i}) = (R_{16} \oplus \widetilde{R_{16}})_i$$

DFA on DES Last Round

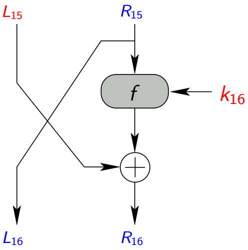
- The attack:
  - For each $i \in \{1, \cdots, 8\}$, guess $k_{16,i} \in \{0,1\}^6$ and test if

$$f_i(R_{15}, k_{16,i}) \oplus f_i(\widetilde{R_{15}}, k_{16,i}) = (R_{16} \oplus \widetilde{R_{16}})_i$$

  - If no, then discard $k_{16,i}$
- By using several faulty ciphertexts, only one candidate remain.

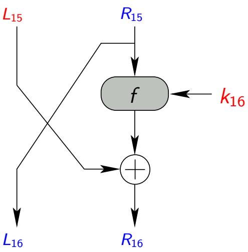


- The last round:

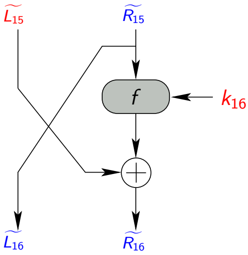


DFA on DES Last Rounds

- The last round:

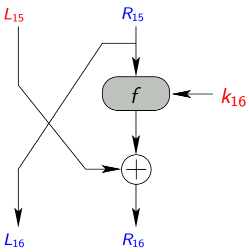


- Fault before Round 16:

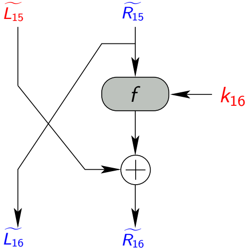


DFA on DES Last Rounds

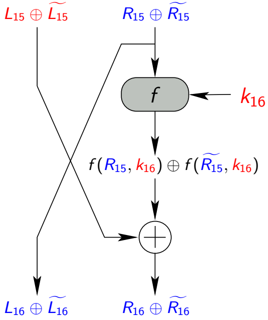
- The last round:



- Fault before Round 16:

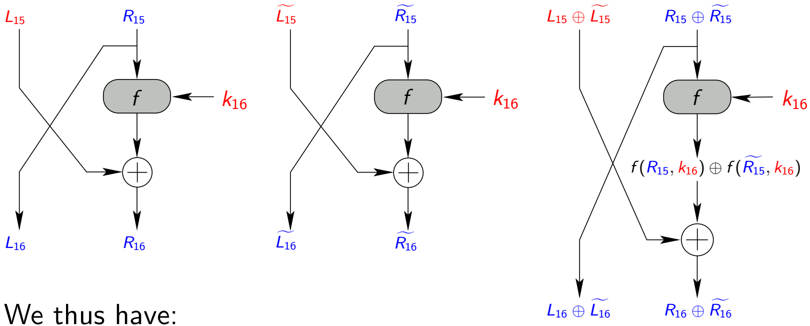


- The corresponding differential:



DFA on DES Last Rounds

- The last round:
- Fault before Round 16:
- The corresponding differential:



- We thus have:

$$f_i(R_{15}, k_{16,i}) \oplus f_i(\widetilde{R_{15}}, k_{16,i}) = (R_{16} \oplus \widetilde{R_{16}})_i \oplus (L_{15} \oplus \widetilde{L_{15}})_i$$

- **Problem:** $L_{15} \oplus \widetilde{L_{15}}$ is unknown

DFA on DES Last Rounds

- **Solutions:**
  - Bit fault attack on rounds 14 and 15 [BihamShamir96]:
    - From $C \oplus \widetilde{C}$, they obtain information on $(L_{15} \oplus \widetilde{L_{15}})_i$

DFA on DES Last Rounds

- **Solutions:**
  - Bit fault attack on rounds 14 and 15 [BihamShamir96]:
    - From $C \oplus \widetilde{C}$, they obtain information on $(L_{15} \oplus \widetilde{L_{15}})_i$
  - Known Value Fault Attack on round 13 [Akkar04]:
    - Corrupting L_{13} only, we have

$$L_{15} \oplus \widetilde{L_{15}} = L_{13} \oplus \widetilde{L_{13}}$$

DFA on DES Middle Rounds

- Motivation:
  - DFA usually targets few last rounds of DES
  - Usual countermeasure: double the few last rounds
  - Question: can we mount an effective DFA by disturbing rounds 12, 11, 10, . . . ?

DFA on DES Middle Rounds

- Motivation:
  - DFA usually targets few last rounds of DES
  - Usual countermeasure: double the few last rounds
  - Question: can we mount an effective DFA by disturbing rounds 12, 11, 10, . . . ?
- Previous work [Akkar04]:
  - Strong adversary model:
    - the attacker can choose the differential $(L_r, R_r) \oplus (\widetilde{L_r}, \widetilde{R_r})$
    - hypothesis relaxed but most usual fault models not considered
  - Suboptimal distinguisher:
    - based on a counting strategy
    - does not exploit the whole available information

Oberthur Technologies

DFA on DES Middle Rounds

- Motivation:
  - DFA usually targets few last rounds of DES
  - Usual countermeasure: double the few last rounds
  - Question: can we mount an effective DFA by disturbing rounds 12, 11, 10, . . . ?
- Previous work [Akkar04]:
  - Strong adversary model:
    - the attacker can choose the differential $(L_r, R_r) \oplus (\widetilde{L_r}, \widetilde{R_r})$
    - hypothesis relaxed but most usual fault models not considered
  - Suboptimal distinguisher:
    - based on a counting strategy
    - does not exploit the whole available information
- Our work:
  - Generalization and improvement of [Akkar04]
  - Study under various realistic fault models

Outline

1 Introduction
- Data Encryption Standard
- DFA on DES Last & Middle Rounds

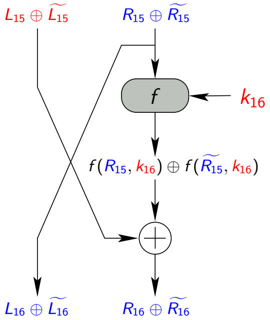
2 Our Attack
- Principle
- Fault Models
- Attack Simulations

3 Conclusion

Principle

- The guess function:

$$g_i(k) = f_i(R_{15}, k) \oplus f_i(\widetilde{R_{15}}, k) \oplus (R_{16} \oplus \widetilde{R_{16}})_i$$

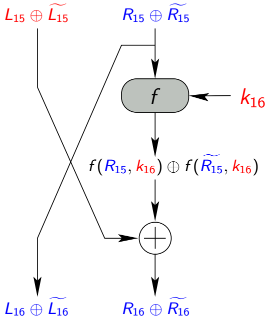


Principle

- The guess function:

  $$g_i(k) = f_i(R_{15}, k) \oplus f_i(\widetilde{R_{15}}, k) \oplus (R_{16} \oplus \widetilde{R_{16}})_i$$

- **Principle:**
  - For $k = k_{16,i}$: $g_i(k) = (L_{15} \oplus \widetilde{L_{15}})_i$
  - For $k \neq k_{16,i}$: $g_i(k) \sim \mathcal{U}(\{0,1\}^4)$

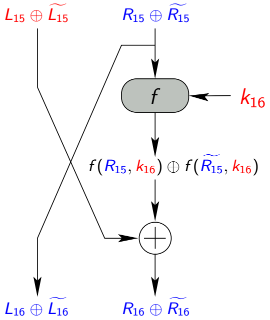


Principle

- The guess function:

  $g_i(k) = f_i(R_{15}, k) \oplus f_i(\widetilde{R_{15}}, k) \oplus (R_{16} \oplus \widetilde{R_{16}})_i$

- **Principle:**
  - For $k = k_{16,i}$: $g_i(k) = (L_{15} \oplus \widetilde{L_{15}})_i$
  - For $k \neq k_{16,i}$: $g_i(k) \sim \mathcal{U}(\{0,1\}^4)$
  - If the distribution of $(L_{15} \oplus \widetilde{L_{15}})_i$ is biased then we have a **wrong-key distinguisher**

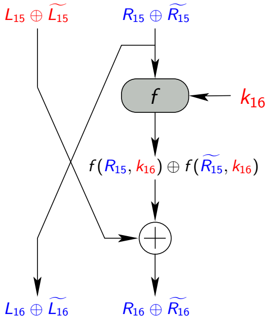


Principle

- The guess function:

  $g_i(k) = f_i(R_{15}, k) \oplus f_i(\widetilde{R_{15}}, k) \oplus (R_{16} \oplus \widetilde{R_{16}})_i$

- **Principle:**
  - For $k = k_{16,i}$: $g_i(k) = (L_{15} \oplus \widetilde{L_{15}})_i$
  - For $k \neq k_{16,i}$: $g_i(k) \sim \mathcal{U}(\{0,1\}^4)$
  - If the distribution of $(L_{15} \oplus \widetilde{L_{15}})_i$ is biased then we have a **wrong-key distinguisher**



- **Description:**
  - Collect on several pairs of correct-faulty ciphertexts $(C_j, \widetilde{C}_j)$
  - For each pair $(C_j, \widetilde{C}_j)$, compute $g_i^{(j)}(k)$
  - By assumption the sample $< g_i^{(j)}(k) >_j$ is
    - biased if $k = k_{16,i}$
    - close to uniformity if $k \neq k_{16,i}$

Two Wrong-Key Distinguishers

- If the fault model is known:
  - The distribution of $(L_{15} \oplus \widetilde{L_{15}})_i$ can be estimated before the attack:

$$\forall \delta \in \{0,1\}^4, \quad p_i(\delta) = \widehat{\Pr}\left[(L_{15} \oplus \widetilde{L_{15}})_i = \delta\right]$$

Two Wrong-Key Distinguishers

- If the fault model is known:
  - The distribution of $(L_{15} \oplus \widetilde{L_{15}})_i$ can be estimated before the attack:

$$\forall \delta \in \{0,1\}^4, \quad p_i(\delta) = \widehat{\Pr}\left[(L_{15} \oplus \widetilde{L_{15}})_i = \delta\right]$$

  - A **maximum likelihood approach** can then be used:

$$d(k) = \sum_{j=1}^{N} \log\left(p_i\left(g_i^{(j)}(k)\right)\right) .$$

Two Wrong-Key Distinguishers

- If the fault model is known:
  - The distribution of $(L_{15} \oplus \widetilde{L_{15}})_i$ can be estimated before the attack:

$$\forall \delta \in \{0,1\}^4, \quad p_i(\delta) = \widehat{\Pr}\left[(L_{15} \oplus \widetilde{L_{15}})_i = \delta\right]$$

  - A **maximum likelihood approach** can then be used:

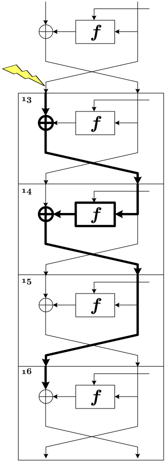
$$d(k) = \sum_{j=1}^{N} \log\left(p_i\left(g_i^{(j)}(k)\right)\right) .$$

- Otherwise, look for the strongest biais by using the **squared Euclidean imbalance** ($\equiv$ square Euclidean distance to the uniform distribution):

$$d(k) = \sum_{\delta=0}^{15} \left(\frac{\#\{g_i^{(j)}(k) = \delta\}}{N} - \frac{1}{16}\right)^2 .$$

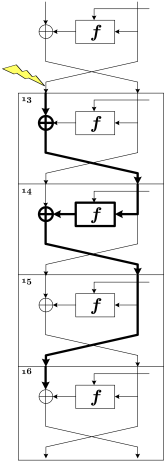
Fault Models: A First Remark

- Where inducing a fault in a round to have the smallest impact on $(L_{15} \oplus \widetilde{L_{15}})$?



Fault Models: A First Remark

- Where inducing a fault in a round to have the smallest impact on $(L_{15} \oplus \widetilde{L_{15}})$?



The attacker must inject a fault in the **left part** of DES internal value at the end of round r:

$$L_r \mapsto \widetilde{L_r} = L_r \oplus \varepsilon$$

Fault Models

- Kind of fault:
  - Bit error:

$$\varepsilon = \begin{cases} (1,0,0,\ldots,0) \\ (0,1,0,\ldots,0) \\ \textit{etc.} \end{cases}$$

  - Byte error:

$$\varepsilon = \begin{cases} (0\mathrm{xXX}, 0\mathrm{x}00, 0\mathrm{x}00, 0\mathrm{x}00) \\ (0\mathrm{x}00, 0\mathrm{xXX}, 0\mathrm{x}00, 0\mathrm{x}00) \\ \textit{etc.} \end{cases}$$

where $0\mathrm{xXX} \sim \mathcal{U}(\{0,1\}^8)$.

Fault Models

- Kind of fault:
  - Bit error:

$$\varepsilon = \begin{cases} (1,0,0,\ldots,0) \\ (0,1,0,\ldots,0) \\ \textit{etc.} \end{cases}$$

  - Byte error:

$$\varepsilon = \begin{cases} (\mathrm{0xXX}, \mathrm{0x00}, \mathrm{0x00}, \mathrm{0x00}) \\ (\mathrm{0x00}, \mathrm{0xXX}, \mathrm{0x00}, \mathrm{0x00}) \\ \textit{etc.} \end{cases}$$

    where $\mathrm{0xXX} \sim \mathcal{U}(\{0,1\}^8)$.
- Fault position:
  - Chosen
  - or random

    among the 32 bit-positions or the 4 byte-positions.

Fault Models

- Kind of fault:
  - Bit error:

$$\varepsilon = \begin{cases} (1, 0, 0, \dots, 0) \\ (0, 1, 0, \dots, 0) \\ \textit{etc.} \end{cases}$$

  - Byte error:

$$\varepsilon = \begin{cases} (\mathrm{0xXX}, \mathrm{0x00}, \mathrm{0x00}, \mathrm{0x00}) \\ (\mathrm{0x00}, \mathrm{0xXX}, \mathrm{0x00}, \mathrm{0x00}) \\ \textit{etc.} \end{cases}$$

    where $\mathrm{0xXX} \sim \mathcal{U}(\{0, 1\}^8)$.
- Fault position:
  - Chosen
  - or random

    among the 32 bit-positions or the 4 byte-positions.

$\Rightarrow$ We have 4 models: {chosen,random} position {bit,byte}-error

Attack Simulations

Table: Number of faults to recover the 16-th round key with a 99% success rate.

Round	Distinguisher	Bit error: chosen pos.	Bit error: random pos.	Byte error: chosen pos.	Byte error: random pos.
12	Likelihood	7	11	9	17
	SEI	14	12	17	21

Attack Simulations

Table: Number of faults to recover the 16-th round key with a 99% success rate.

Round	Distinguisher	Bit error chosen pos.	Bit error random pos.	Byte error chosen pos.	Byte error random pos.
12	Likelihood	7	11	9	17
	SEI	14	12	17	21
11	Likelihood	11	44	210	460
	SEI	30	71	500	820

Attack Simulations

Table: Number of faults to recover the 16-th round key with a 99% success rate.

Round	Distinguisher	Bit error: chosen pos.	Bit error: random pos.	Byte error: chosen pos.	Byte error: random pos.
12	Likelihood	7	11	9	17
	SEI	14	12	17	21
11	Likelihood	11	44	210	460
	SEI	30	71	500	820
10	Likelihood	290	1500	13400	18500
	SEI	940	2700	26400	23400

Attack Simulations

Table: Number of faults to recover the 16-th round key with a 99% success rate.

Round	Distinguisher	Bit error chosen pos.	Bit error random pos.	Byte error chosen pos.	Byte error random pos.
12	Likelihood	7	11	9	17
	SEI	14	12	17	21
11	Likelihood	11	44	210	460
	SEI	30	71	500	820
10	Likelihood	290	1500	13400	18500
	SEI	940	2700	26400	23400
9	Likelihood	$3.4 \cdot 10^5$	$2.2 \cdot 10^7$	$> 10^8$	$> 10^8$
	SEI	$1.4 \cdot 10^6$	$> 10^8$	$> 10^8$	$> 10^8$

Outline

1 Introduction
- Data Encryption Standard
- DFA on DES Last & Middle Rounds

2 Our Attack
- Principle
- Fault Models
- Attack Simulations

3 Conclusion

Conclusion

- Extension of DFA on DES on rounds 12, 11, 10 and 9.
- Very efficient even in the byte fault model:
  - $\approx$ 20 faults on the 12$^{\text{th}}$ round
  - $\approx$ 800 faults on the 11$^{\text{th}}$ round
- Depending on the adversary, the last 7 or 8 rounds must now be protected against FA

Questions ?

or contact M. Rivain at m.rivain@oberthur.com