Destroying Fault Invariant with Randomization -A Countermeasure for AES against Differential Fault Attacks

Harshal Tupsamudre, Shikha Bisht, Debdeep Mukhopadhyay
(IIT KHARAGPUR)

CHES 2014

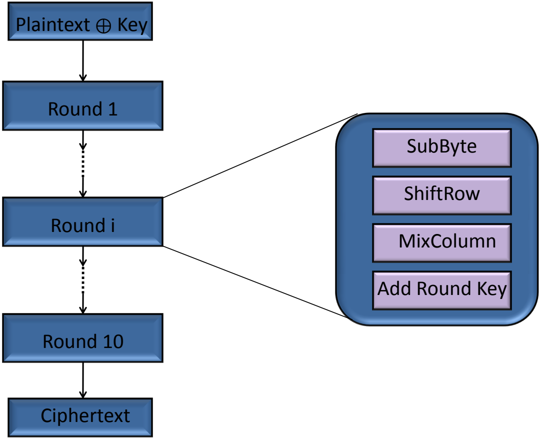
South Korea, Busan

September 24, 2014

Outline

Preliminaries

AES128


Plaintext ⊕ Key
Round 1
Round i
Round 10
Ciphertext
SubByte
ShiftRow
MixColumn
Add Round Key

AES128: Round Function

$$\begin{pmatrix} I_0 & I_4 & I_8 & I_{12} \\ I_1 & I_5 & I_9 & I_{13} \\ I_2 & I_6 & I_{10} & I_{14} \\ I_3 & I_7 & I_{11} & I_{15} \end{pmatrix}$$

AES128: Round Function

$$\begin{pmatrix} I_0 & I_4 & I_8 & I_{12} \\ I_1 & I_5 & I_9 & I_{13} \\ I_2 & I_6 & I_{10} & I_{14} \\ I_3 & I_7 & I_{11} & I_{15} \end{pmatrix} \text{—S—} \begin{pmatrix} S[I_0] & S[I_4] & S[I_8] & S[I_{12}] \\ S[I_1] & S[I_5] & S[I_9] & S[I_{13}] \\ S[I_2] & S[I_6] & S[I_{10}] & S[I_{14}] \\ S[I_3] & S[I_7] & S[I_{11}] & S[I_{15}] \end{pmatrix}$$

AES128: Round Function

$$\begin{pmatrix} I_0 & I_4 & I_8 & I_{12} \\ I_1 & I_5 & I_9 & I_{13} \\ I_2 & I_6 & I_{10} & I_{14} \\ I_3 & I_7 & I_{11} & I_{15} \end{pmatrix} \text{—S—} \begin{pmatrix} S[I_0] & S[I_4] & S[I_8] & S[I_{12}] \\ S[I_1] & S[I_5] & S[I_9] & S[I_{13}] \\ S[I_2] & S[I_6] & S[I_{10}] & S[I_{14}] \\ S[I_3] & S[I_7] & S[I_{11}] & S[I_{15}] \end{pmatrix} \text{—SR—} \begin{pmatrix} S[I_0] & S[I_4] & S[I_8] & S[I_{12}] \\ S[I_5] & S[I_9] & S[I_{13}] & S[I_1] \\ S[I_{10}] & S[I_{14}] & S[I_2] & S[I_6] \\ S[I_{15}] & S[I_3] & S[I_7] & S[I_{11}] \end{pmatrix}$$

AES128: Round Function

$$\begin{pmatrix} I_0 & I_4 & I_8 & I_{12} \\ I_1 & I_5 & I_9 & I_{13} \\ I_2 & I_6 & I_{10} & I_{14} \\ I_3 & I_7 & I_{11} & I_{15} \end{pmatrix} \text{—S—} \begin{pmatrix} S[I_0] & S[I_4] & S[I_8] & S[I_{12}] \\ S[I_1] & S[I_5] & S[I_9] & S[I_{13}] \\ S[I_2] & S[I_6] & S[I_{10}] & S[I_{14}] \\ S[I_3] & S[I_7] & S[I_{11}] & S[I_{15}] \end{pmatrix} \text{—SR—} \begin{pmatrix} S[I_0] & S[I_4] & S[I_8] & S[I_{12}] \\ S[I_5] & S[I_9] & S[I_{13}] & S[I_1] \\ S[I_{10}] & S[I_{14}] & S[I_2] & S[I_6] \\ S[I_{15}] & S[I_3] & S[I_7] & S[I_{11}] \end{pmatrix}$$

$$\text{—MC—} \begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix} \begin{pmatrix} S[I_0] & S[I_4] & S[I_8] & S[I_{12}] \\ S[I_5] & S[I_9] & S[I_{13}] & S[I_1] \\ S[I_{10}] & S[I_{14}] & S[I_2] & S[I_6] \\ S[I_{15}] & S[I_3] & S[I_7] & S[I_{11}] \end{pmatrix}$$

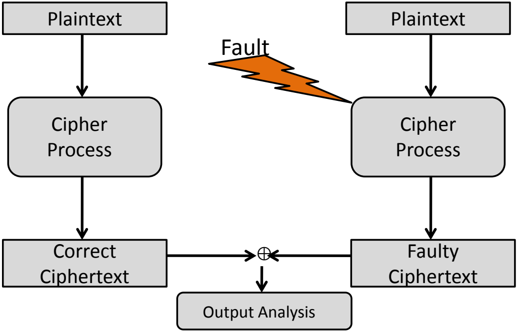
AES128: Round Function

$$\begin{pmatrix} I_0 & I_4 & I_8 & I_{12} \\ I_1 & I_5 & I_9 & I_{13} \\ I_2 & I_6 & I_{10} & I_{14} \\ I_3 & I_7 & I_{11} & I_{15} \end{pmatrix} \text{—S—} \begin{pmatrix} S[I_0] & S[I_4] & S[I_8] & S[I_{12}] \\ S[I_1] & S[I_5] & S[I_9] & S[I_{13}] \\ S[I_2] & S[I_6] & S[I_{10}] & S[I_{14}] \\ S[I_3] & S[I_7] & S[I_{11}] & S[I_{15}] \end{pmatrix} \text{—SR—} \begin{pmatrix} S[I_0] & S[I_4] & S[I_8] & S[I_{12}] \\ S[I_5] & S[I_9] & S[I_{13}] & S[I_1] \\ S[I_{10}] & S[I_{14}] & S[I_2] & S[I_6] \\ S[I_{15}] & S[I_3] & S[I_7] & S[I_{11}] \end{pmatrix}$$

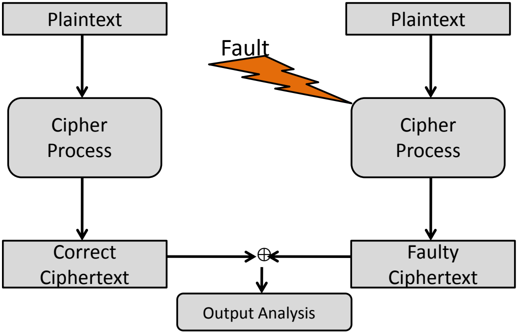
$$\text{—MC—} \begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix} \begin{pmatrix} S[I_0] & S[I_4] & S[I_8] & S[I_{12}] \\ S[I_5] & S[I_9] & S[I_{13}] & S[I_1] \\ S[I_{10}] & S[I_{14}] & S[I_2] & S[I_6] \\ S[I_{15}] & S[I_3] & S[I_7] & S[I_{11}] \end{pmatrix}$$

$$\text{—Add key—} \begin{pmatrix} I_0' \oplus k_0 & I_4' \oplus k_4 & I_8' \oplus k_8 & I_{12}' \oplus k_{12} \\ I_1' \oplus k_1 & I_5' \oplus k_5 & I_9' \oplus k_9 & I_{13}' \oplus k_{13} \\ I_2' \oplus k_2 & I_6' \oplus k_6 & I_{10}' \oplus k_{10} & I_{14}' \oplus k_{14} \\ I_3' \oplus k_3 & I_7' \oplus k_7 & I_{11}' \oplus k_{11} & I_{15}' \oplus k_{15} \end{pmatrix}$$

Fault Attack



Fault Attack



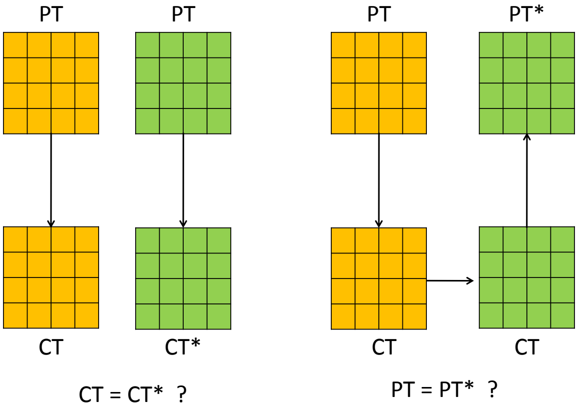
Only one fault sufficient to retrieve the entire secret key of AES.

Fault Attack

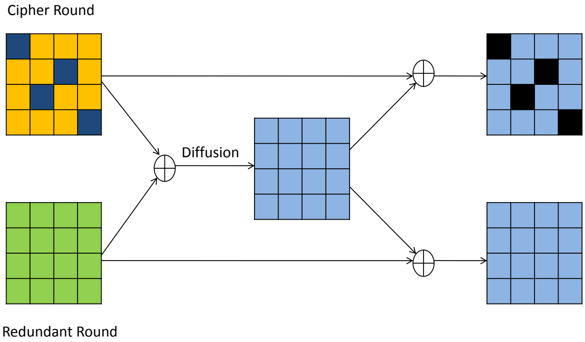
1. Fault models to model the strength of adversary
    1. Bit flip Fault Model : Affects a bit of the intermediate result
    2. Constant Byte Fault Model : Requires control over fault value and position
    3. Random Byte Fault Model : No control over fault value and position
2. Attacks that require both the correct and faulty ciphertext are known as differential fault attacks

Countermeasures Against Fault Attacks

Detection Countermeasure



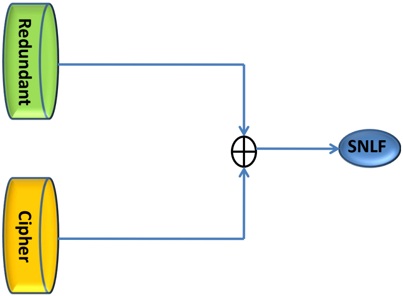
Infection Countermeasure



LatinCrypt 2012 Infection Countermeasure

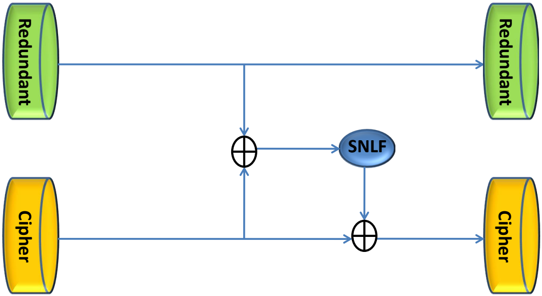
LatinCrypt 2012 Infection Countermeasure

SNLF operates on a byte and $\text{SNLF}(0) = 0$



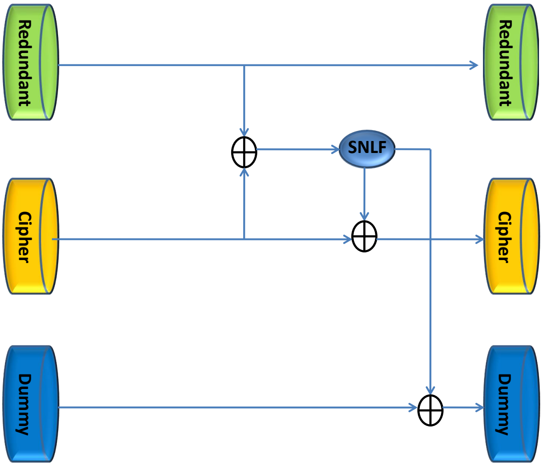
LatinCrypt 2012 Infection Countermeasure

SNLF operates on a byte and SNLF(0) $= 0$



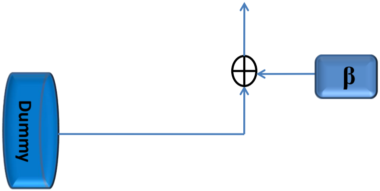
LatinCrypt 2012 Infection Countermeasure

Dummy rounds occur randomly



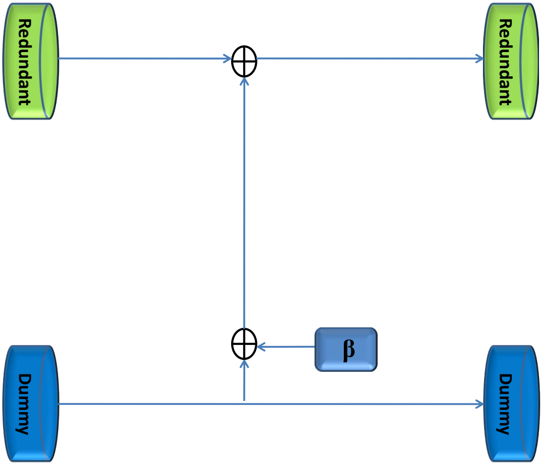
LatinCrypt 2012 Infection Countermeasure

$RoundFunction(\beta,\ k^0) = \beta$



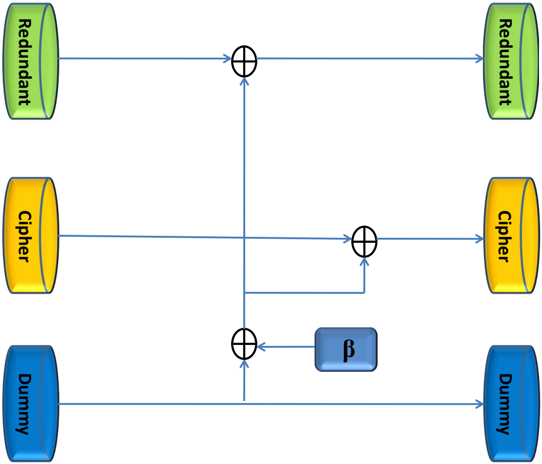
LatinCrypt 2012 Infection Countermeasure

$RoundFunction(\beta,\ k^0) = \beta$



LatinCrypt 2012 Infection Countermeasure

$RoundFunction(\beta,\ k^0) = \beta$



FDTC 2013 Attack

FDTC 2013 Attack

FDTC 2013 Attack

- Fault f in I_1^{10}, *i.e.*, first byte of the second row in the input of 10^{th} *cipher round* of AES128

FDTC 2013 Attack

- Fault f in I_1^{10}, *i.e.*, first byte of the second row in the input of 10^{th} *cipher round* of AES128
- Countermeasure infects the faulty computation twice

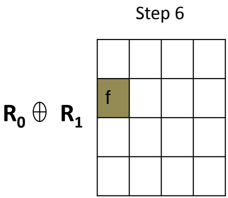
FDTC 2013 Attack

- Fault f in I_1^{10}, *i.e.*, first byte of the second row in the input of 10^{th} *cipher round* of AES128
- Countermeasure infects the faulty computation twice
  - After the execution of 10^{th} cipher round

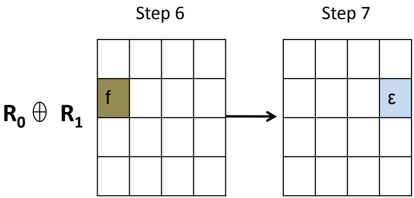
FDTC 2013 Attack

- Fault f in I_1^{10}, *i.e.*, first byte of the second row in the input of 10^{th} *cipher round* of AES128
- Countermeasure infects the faulty computation twice
  - After the execution of 10^{th} cipher round
  - After the execution of compulsory dummy round

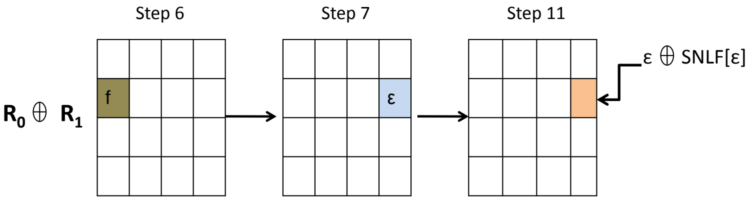
FDTC 2013 Attack

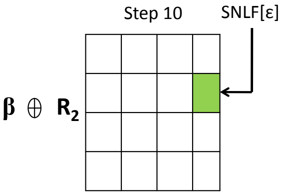


FDTC 2013 Attack

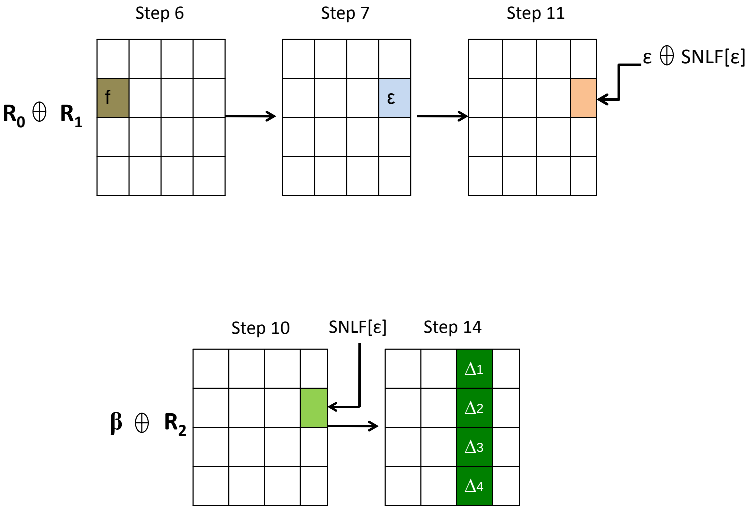


FDTC 2013 Attack

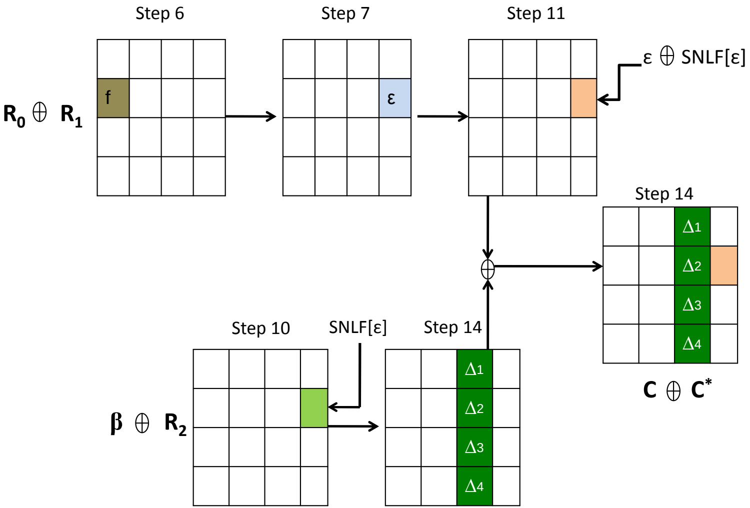




FDTC 2013 Attack



FDTC 2013 Attack



FDTC 2013 Attack: Infection Caused by the 10^{th} Cipher Round

1. The difference between correct (R_1) and faulty computation (R_0) is:

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ f & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

FDTC 2013 Attack: Infection Caused by the 10^{th} Cipher Round

1. The difference between correct (R_1) and faulty computation (R_0) is:

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ f & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \text{—S—} \begin{pmatrix} 0 & 0 & 0 & 0 \\ \varepsilon & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

FDTC 2013 Attack: Infection Caused by the 10^{th} Cipher Round

1. The difference between correct (R_1) and faulty computation (R_0) is:

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ f & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \text{—S—} \begin{pmatrix} 0 & 0 & 0 & 0 \\ \varepsilon & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \text{—SR—} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \varepsilon \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

FDTC 2013 Attack: Infection Caused by the 10^{th} Cipher Round

1. The difference between correct (R_1) and faulty computation (R_0) is:

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ f & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \text{—S—} \begin{pmatrix} 0 & 0 & 0 & 0 \\ \varepsilon & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \text{—SR—} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \varepsilon \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

2. After Infection Step, the difference is:

$$R_0 \oplus R_1 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \varepsilon \oplus SNLF[\varepsilon] \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

where $\varepsilon = S[I_1^{10} \oplus f] \oplus S[I_1^{10}]$

FDTC 2013 Attack: Infection Caused by the Compulsory Dummy Round

3. The differential of R_2 and β is:

$$R_2 \oplus \beta = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & SNLF[\varepsilon] \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

FDTC 2013 Attack: Infection Caused by the Compulsory Dummy Round

3. The differential of R_2 and β is:

$$R_2 \oplus \beta = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & SNLF[\varepsilon] \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

4. When $R_2 = \beta$, $RoundFunction(R_2, k^0) \oplus \beta = 0$

FDTC 2013 Attack: Infection Caused by the Compulsory Dummy Round

3. The differential of R_2 and β is:

$$R_2 \oplus \beta = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & SNLF[\varepsilon] \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

4. When $R_2 = \beta$, $RoundFunction(R_2, k^0) \oplus \beta = 0$
5. When $R_2 \neq \beta$, $RoundFunction(R_2, k^0) \oplus \beta \neq 0$

FDTC 2013 Attack: Infection Caused by the Compulsory Dummy Round

3. The differential of R_2 and β is:

$$R_2 \oplus \beta = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & SNLF[\varepsilon] \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

4. When $R_2 = \beta$, $RoundFunction(R_2, k^0) \oplus \beta = 0$
5. When $R_2 \neq \beta$, $RoundFunction(R_2, k^0) \oplus \beta \neq 0$
6. $\therefore RoundFunction(R_2, k^0) \oplus \beta =$

$$\begin{pmatrix} 0 & 0 & \Delta_1 & 0 \\ 0 & 0 & \Delta_2 & 0 \\ 0 & 0 & \Delta_3 & 0 \\ 0 & 0 & \Delta_4 & 0 \end{pmatrix}$$

FDTC 2013 Attack: Final Difference

7. Infection caused by compulsory dummy round does not affect ε.

$$C \oplus C^* = \begin{pmatrix} 0 & 0 & \Delta_1 & 0 \\ 0 & 0 & \Delta_2 & \varepsilon \oplus SNLF[\varepsilon] \\ 0 & 0 & \Delta_3 & 0 \\ 0 & 0 & \Delta_4 & 0 \end{pmatrix}$$

FDTC 2013 Attack: Final Difference

7. Infection caused by compulsory dummy round does not affect ε.

$$C \oplus C^* = \begin{pmatrix} 0 & 0 & \Delta_1 & 0 \\ 0 & 0 & \Delta_2 & \varepsilon \oplus SNLF[\varepsilon] \\ 0 & 0 & \Delta_3 & 0 \\ 0 & 0 & \Delta_4 & 0 \end{pmatrix}$$

8. Infection SNLF[ε] caused by 10^{th} cipher round is ineffective.

FDTC 2013 Attack: Final Difference

7. Infection caused by compulsory dummy round does not affect ε.

$$C \oplus C^* = \begin{pmatrix} 0 & 0 & \Delta_1 & 0 \\ 0 & 0 & \Delta_2 & \varepsilon \oplus SNLF[\varepsilon] \\ 0 & 0 & \Delta_3 & 0 \\ 0 & 0 & \Delta_4 & 0 \end{pmatrix}$$

8. Infection SNLF[ε] caused by 10^{th} cipher round is ineffective.
9. Attacker uses the value of $\varepsilon = S[I_1^{10} \oplus f] \oplus S[I^{10}]$ to make hypotheses on I_1^{10} and key byte k_{13}^{11}.

FDTC 2013 Attack: Final Difference

7. Infection caused by compulsory dummy round does not affect ε.

$$C \oplus C^* = \begin{pmatrix} 0 & 0 & \Delta_1 & 0 \\ 0 & 0 & \Delta_2 & \varepsilon \oplus SNLF[\varepsilon] \\ 0 & 0 & \Delta_3 & 0 \\ 0 & 0 & \Delta_4 & 0 \end{pmatrix}$$

8. Infection SNLF[ε] caused by 10^{th} cipher round is ineffective.
9. Attacker uses the value of $\varepsilon = S[I_1^{10} \oplus f] \oplus S[I^{10}]$ to make hypotheses on I_1^{10} and key byte k_{13}^{11}.
10. Repeat this process with two more pairs of faulty and correct ciphertexts, using constant byte fault model.

FDTC 2013 Attack: Final Difference

7. Infection caused by compulsory dummy round does not affect ε.

$$C \oplus C^* = \begin{pmatrix} 0 & 0 & \Delta_1 & 0 \\ 0 & 0 & \Delta_2 & \varepsilon \oplus SNLF[\varepsilon] \\ 0 & 0 & \Delta_3 & 0 \\ 0 & 0 & \Delta_4 & 0 \end{pmatrix}$$

8. Infection SNLF[ε] caused by 10^{th} cipher round is ineffective.
9. Attacker uses the value of $\varepsilon = S[I_1^{10} \oplus f] \oplus S[I^{10}]$ to make hypotheses on I_1^{10} and key byte k_{13}^{11}.
10. Repeat this process with two more pairs of faulty and correct ciphertexts, using constant byte fault model.
11. The attack targets **last three rows** of the 10^{th} round input.

FDTC 2013 Attack: Final Difference

7. Infection caused by compulsory dummy round does not affect ε.

$$C \oplus C^* = \begin{pmatrix} 0 & 0 & \Delta_1 & 0 \\ 0 & 0 & \Delta_2 & \varepsilon \oplus SNLF[\varepsilon] \\ 0 & 0 & \Delta_3 & 0 \\ 0 & 0 & \Delta_4 & 0 \end{pmatrix}$$

8. Infection SNLF[ε] caused by 10^{th} cipher round is ineffective.
9. Attacker uses the value of $\varepsilon = S[I_1^{10} \oplus f] \oplus S[I^{10}]$ to make hypotheses on I_1^{10} and key byte k_{13}^{11}.
10. Repeat this process with two more pairs of faulty and correct ciphertexts, using constant byte fault model.
11. The attack targets **last three rows** of the 10^{th} round input.
12. Recover remaining 4 bytes of top row using brute force search.

Flaws Exploited by FDTC 2013 attack

1. The last cipher round is always the penultimate round: The attacker can verify target round using side channel.

Flaws Exploited by FDTC 2013 attack

1. The last cipher round is always the penultimate round: The attacker can verify target round using side channel.
2. A fault in last three rows of 10^{th} round $\Longrightarrow$
   Infection caused by compulsory dummy round does not affect the erroneous byte.

Remark

What happens if the infection caused by compulsory dummy round affects the erroneous byte of 10^{th} round??

Further Loop Holes in LatinCrypt 2012 Countermeasure

Extending FDTC 2013 Attack to the Top Row

Extending FDTC 2013 Attack to the Top Row

- Fault f in I_0^{10}, *i.e.*, first byte of the top row in the input of 10^{th} *cipher round*

Extending FDTC 2013 Attack to the Top Row

- Fault f in I_0^{10}, *i.e.*, first byte of the top row in the input of 10^{th} *cipher round*
- Countermeasure infects the faulty computation twice

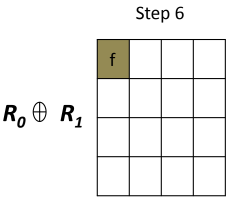
Extending FDTC 2013 Attack to the Top Row

- Fault f in I_0^{10}, $i.e.$, first byte of the top row in the input of 10^{th} *cipher round*
- Countermeasure infects the faulty computation twice
  - After the execution of 10^{th} cipher round

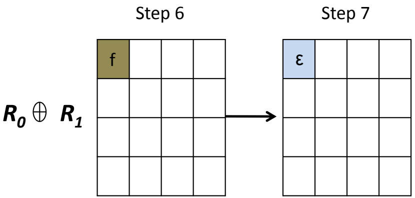
Extending FDTC 2013 Attack to the Top Row

- Fault f in I_0^{10}, *i.e.*, first byte of the top row in the input of 10^{th} *cipher round*
- Countermeasure infects the faulty computation twice
  - After the execution of 10^{th} cipher round
  - After the execution of compulsory dummy round

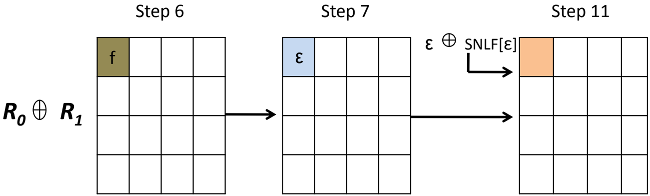
Extending FDTC 2013 Attack to the Top Row

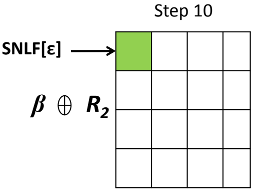


Extending FDTC 2013 Attack to the Top Row

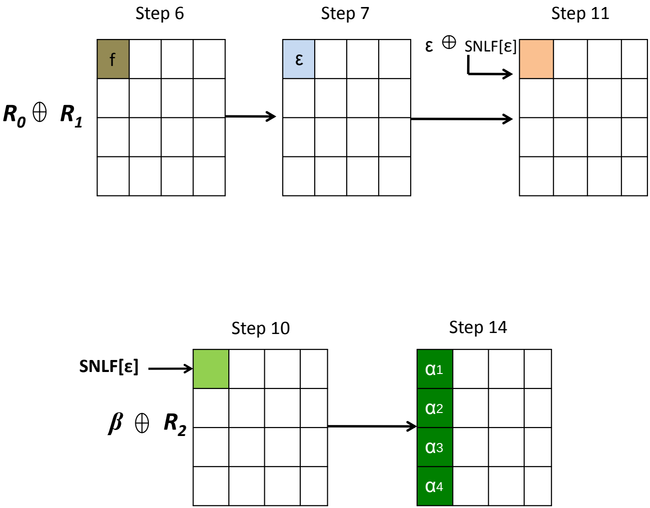


Extending FDTC 2013 Attack to the Top Row

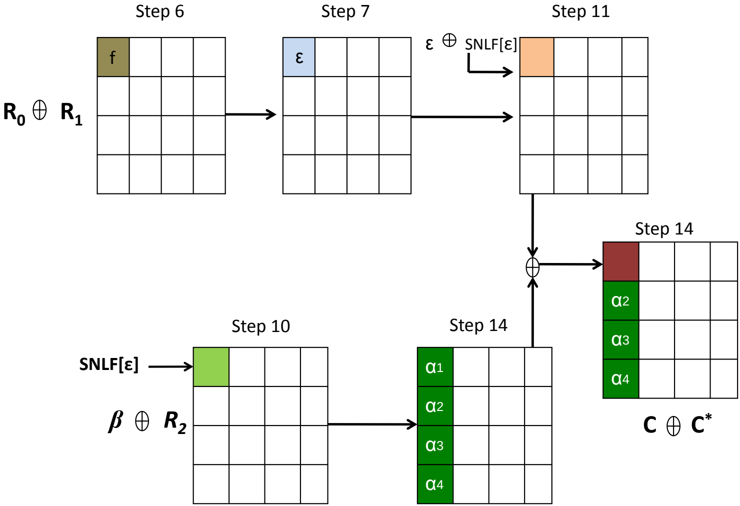




Extending FDTC 2013 Attack to the Top Row



Extending FDTC 2013 Attack to the Top Row



Extending FDTC 2013 Attack to the Top Row

1. The differential between correct (R_1) and faulty computation (R_0) is:

$$\begin{pmatrix} f & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Extending FDTC 2013 Attack to the Top Row

1. The differential between correct (R_1) and faulty computation (R_0) is:

$$\begin{pmatrix} f & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \text{—S—} \begin{pmatrix} \varepsilon & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Extending FDTC 2013 Attack to the Top Row

1. The differential between correct (R_1) and faulty computation (R_0) is:

$$\begin{pmatrix} f & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \text{—S—} \begin{pmatrix} \varepsilon & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \text{—SR—} \begin{pmatrix} \varepsilon & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Extending FDTC 2013 Attack to the Top Row

1. The differential between correct (R_1) and faulty computation (R_0) is:

$$\begin{pmatrix} f & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \text{—S—} \begin{pmatrix} \varepsilon & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \text{—SR—} \begin{pmatrix} \varepsilon & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

2. After Infection Step, the differential is:

$$R_0 \oplus R_1 = \begin{pmatrix} \varepsilon \oplus SNLF[\varepsilon] & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

where $\varepsilon = S[I_0^{10} \oplus f] \oplus S[I_0^{10}]$

Extending FDTC 2013 Attack to the Top Row

3. The differential of R_2 and β is:

$$R_2 \oplus \beta = \begin{pmatrix} SNLF[\varepsilon] & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Extending FDTC 2013 Attack to the Top Row

3. The differential of R_2 and β is:

$$R_2 \oplus \beta = \begin{pmatrix} SNLF[\varepsilon] & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

4. $RoundFunction(R_2, k^0) \oplus \beta =$

$$\begin{pmatrix} \alpha_1 & 0 & 0 & 0 \\ \alpha_2 & 0 & 0 & 0 \\ \alpha_3 & 0 & 0 & 0 \\ \alpha_4 & 0 & 0 & 0 \end{pmatrix}$$

Extending FDTC 2013 Attack to the Top Row

5. Infection caused by compulsory dummy round affects ε.

$$C \oplus C^* = \begin{pmatrix} \alpha_1 \oplus \varepsilon \oplus SNLF[\varepsilon] & 0 & 0 & 0 \\ \alpha_2 & 0 & 0 & 0 \\ \alpha_3 & 0 & 0 & 0 \\ \alpha_4 & 0 & 0 & 0 \end{pmatrix}$$

Extending FDTC 2013 Attack to the Top Row

5. Infection caused by compulsory dummy round affects ε.

$$C \oplus C^* = \begin{pmatrix} \alpha_1 \oplus \varepsilon \oplus SNLF[\varepsilon] & 0 & 0 & 0 \\ \alpha_2 & 0 & 0 & 0 \\ \alpha_3 & 0 & 0 & 0 \\ \alpha_4 & 0 & 0 & 0 \end{pmatrix}$$

6. Attack of FDTC 2013 will not work.

Extending FDTC 2013 Attack to the Top Row

5. Infection caused by compulsory dummy round affects ε.

$$C \oplus C^* = \begin{pmatrix} \alpha_1 \oplus \varepsilon \oplus SNLF[\varepsilon] & 0 & 0 & 0 \\ \alpha_2 & 0 & 0 & 0 \\ \alpha_3 & 0 & 0 & 0 \\ \alpha_4 & 0 & 0 & 0 \end{pmatrix}$$

6. Attack of FDTC 2013 will not work.
7. α_1 has to be unmasked.

Extending FDTC 2013 Attack to the Top Row

5. Infection caused by compulsory dummy round affects ε.

$$C \oplus C^* = \begin{pmatrix} \alpha_1 \oplus \varepsilon \oplus SNLF[\varepsilon] & 0 & 0 & 0 \\ \alpha_2 & 0 & 0 & 0 \\ \alpha_3 & 0 & 0 & 0 \\ \alpha_4 & 0 & 0 & 0 \end{pmatrix}$$

6. Attack of FDTC 2013 will not work.
7. α_1 has to be unmasked.

We show that α_i are interrelated and **infection caused by compulsory dummy round is ineffective.**

A Major Flaw in the Infection Scheme

Since $RoundFunction(\beta, k^0) = \beta$ we can write:

$$RoundFunction(R_2, k^0) \oplus \beta = RoundFunction(R_2, k^0) \oplus RoundFunction(\beta, k^0)$$

A Major Flaw in the Infection Scheme

Since $RoundFunction(\beta, k^0) = \beta$ we can write:

$$\begin{aligned} RoundFunction(R_2, k^0) \oplus \beta &= RoundFunction(R_2, k^0) \oplus RoundFunction(\beta, k^0) \\ &= MC(SR(S(R_2))) \oplus k^0 \oplus MC(SR(S(\beta))) \oplus k^0 \end{aligned}$$

A Major Flaw in the Infection Scheme

Since $RoundFunction(\beta, k^0) = \beta$ we can write:

$$\begin{aligned} RoundFunction(R_2, k^0) \oplus \beta &= RoundFunction(R_2, k^0) \oplus RoundFunction(\beta, k^0) \\ &= MC(SR(S(R_2))) \oplus k^0 \oplus MC(SR(S(\beta))) \oplus k^0 \\ &= MC(SR(S(R_2))) \oplus MC(SR(S(\beta))) \end{aligned}$$

A Major Flaw in the Infection Scheme

Since $RoundFunction(\beta, k^0) = \beta$ we can write:

$$\begin{aligned} RoundFunction(R_2, k^0) \oplus \beta &= RoundFunction(R_2, k^0) \oplus RoundFunction(\beta, k^0) \\ &= MC(SR(S(R_2))) \oplus k^0 \oplus MC(SR(S(\beta))) \oplus k^0 \\ &= MC(SR(S(R_2))) \oplus MC(SR(S(\beta))) \\ &= MC(SR(S(R_2) \oplus S(\beta))) \end{aligned}$$

A Major Flaw in the Infection Scheme

Since $RoundFunction(\beta, k^0) = \beta$ we can write:

$$\begin{aligned} RoundFunction(R_2, k^0) \oplus \beta &= RoundFunction(R_2, k^0) \oplus RoundFunction(\beta, k^0) \\ &= MC(SR(S(R_2))) \oplus k^0 \oplus MC(SR(S(\beta))) \oplus k^0 \\ &= MC(SR(S(R_2))) \oplus MC(SR(S(\beta))) \\ &= MC(SR(S(R_2) \oplus S(\beta))) \end{aligned}$$

1. When $R_2 = \beta$, $RoundFunction(R_2, k^0) \oplus \beta = 0$

A Major Flaw in the Infection Scheme

Since $RoundFunction(\beta, k^0) = \beta$ we can write:

$$\begin{aligned} RoundFunction(R_2, k^0) \oplus \beta &= RoundFunction(R_2, k^0) \oplus RoundFunction(\beta, k^0) \\ &= MC(SR(S(R_2))) \oplus k^0 \oplus MC(SR(S(\beta))) \oplus k^0 \\ &= MC(SR(S(R_2))) \oplus MC(SR(S(\beta))) \\ &= MC(SR(S(R_2) \oplus S(\beta))) \end{aligned}$$

1. When $R_2 = \beta$, $RoundFunction(R_2, k^0) \oplus \beta = 0$
2. When $R_2 \neq \beta$, $RoundFunction(R_2, k^0) \oplus \beta \neq 0$

Infection Removal of Compulsory Dummy Round

3. The differential of R_2 and β is:

$$R_2 \oplus \beta = \begin{pmatrix} SNLF[\varepsilon] & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Infection Removal of Compulsory Dummy Round

3. The differential of R_2 and β is:

$$R_2 \oplus \beta = \begin{pmatrix} SNLF[\varepsilon] & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

4. $RoundFunction(R_2, k^0) \oplus \beta = MC(SR(S(R_2) \oplus S(\beta)))$

$$\begin{pmatrix} SNLF[\varepsilon] & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Infection Removal of Compulsory Dummy Round

3. The differential of R_2 and β is:

$$R_2 \oplus \beta = \begin{pmatrix} SNLF[\varepsilon] & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

4. $RoundFunction(R_2, k^0) \oplus \beta = MC(SR(S(R_2) \oplus S(\beta)))$

$$\begin{pmatrix} SNLF[\varepsilon] & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \text{–S \& SR–} \begin{pmatrix} y & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Infection Removal of Compulsory Dummy Round

3. The differential of R_2 and β is:

$$R_2 \oplus \beta = \begin{pmatrix} SNLF[\varepsilon] & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

4. $RoundFunction(R_2, k^0) \oplus \beta = MC(SR(S(R_2) \oplus S(\beta)))$

$$\begin{pmatrix} SNLF[\varepsilon] & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \text{–S \& SR–} \begin{pmatrix} y & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \text{–MC–} \begin{pmatrix} 2y & 0 & 0 & 0 \\ 1y & 0 & 0 & 0 \\ 1y & 0 & 0 & 0 \\ 3y & 0 & 0 & 0 \end{pmatrix}$$

Infection Removal of Compulsory Dummy Round

5. Therefore we can write the difference between correct and faulty computation as:

$$C \oplus C^* = \begin{pmatrix} 2y \oplus \varepsilon \oplus SNLF[\varepsilon] & 0 & 0 & 0 \\ 1y & 0 & 0 & 0 \\ 1y & 0 & 0 & 0 \\ 3y & 0 & 0 & 0 \end{pmatrix}$$

Infection Removal of Compulsory Dummy Round

5. Therefore we can write the difference between correct and faulty computation as:

$$C \oplus C^* = \begin{pmatrix} 2y \oplus \varepsilon \oplus SNLF[\varepsilon] & 0 & 0 & 0 \\ 1y & 0 & 0 & 0 \\ 1y & 0 & 0 & 0 \\ 3y & 0 & 0 & 0 \end{pmatrix}$$

6. y can be deduced from the above matrix.

Infection Removal of Compulsory Dummy Round

5. Therefore we can write the difference between correct and faulty computation as:

$$C \oplus C^* = \begin{pmatrix} 2y \oplus \varepsilon \oplus SNLF[\varepsilon] & 0 & 0 & 0 \\ 1y & 0 & 0 & 0 \\ 1y & 0 & 0 & 0 \\ 3y & 0 & 0 & 0 \end{pmatrix}$$

6. y can be deduced from the above matrix.
7. $2y$ can be unmasked.

Infection Removal of Compulsory Dummy Round

5. Therefore we can write the difference between correct and faulty computation as:

$$C \oplus C^* = \begin{pmatrix} 2y \oplus \varepsilon \oplus SNLF[\varepsilon] & 0 & 0 & 0 \\ 1y & 0 & 0 & 0 \\ 1y & 0 & 0 & 0 \\ 3y & 0 & 0 & 0 \end{pmatrix}$$

6. y can be deduced from the above matrix.
7. $2y$ can be unmasked.
8. And the attack of FDTC 2013 can be mounted.

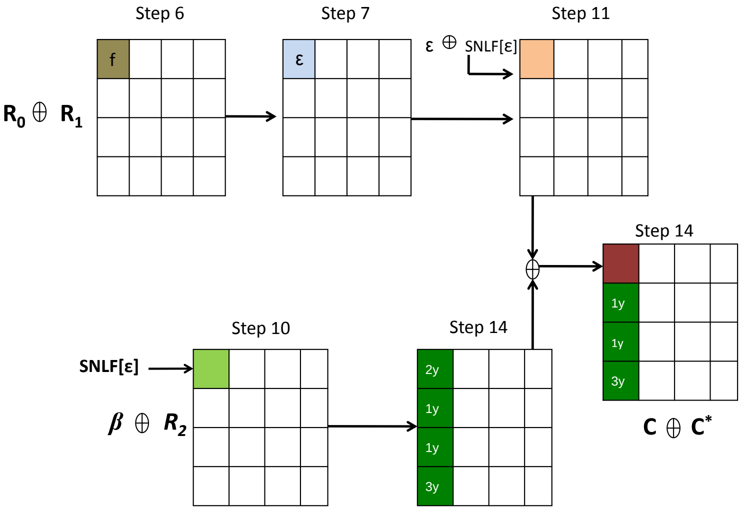
Infection Removal of Compulsory Dummy Round

5. Therefore we can write the difference between correct and faulty computation as:

$$C \oplus C^* = \begin{pmatrix} 2y \oplus \varepsilon \oplus SNLF[\varepsilon] & 0 & 0 & 0 \\ 1y & 0 & 0 & 0 \\ 1y & 0 & 0 & 0 \\ 3y & 0 & 0 & 0 \end{pmatrix}$$

6. y can be deduced from the above matrix.
7. $2y$ can be unmasked.
8. And the attack of FDTC 2013 can be mounted.
9. Now, this attack can target any 12 bytes of 10^{th} round input.

FDTC 2013 Attack Extended to the Top Row



Piret and Quisquater's Attack

Relaxing the Restrictions of FDTC 2013 Attack

Relaxing the Restrictions of FDTC 2013 Attack

1. The attack assumes **constant byte fault model** which requires precise control over fault position and value.

Relaxing the Restrictions of FDTC 2013 Attack

1. The attack assumes **constant byte fault model** which requires precise control over fault position and value.
2. The attack can retrieve only last 3 rows of k^{11} using $\mathbf{12*3 = 36}$ **faults**.

Relaxing the Restrictions of FDTC 2013 Attack

1. The attack assumes **constant byte fault model** which requires precise control over fault position and value.
2. The attack can retrieve only last 3 rows of k^{11} using **12*3 = 36 faults**.
3. The top row of k^{11} has to be recoverd using brute force search.

Piret and Quisquater's Attack in absence of Random Dummy Rounds

- The attack targets the penultimate round of AES, e.g, in case of AES128, input of 9^{th} round is the target.

Piret and Quisquater's Attack in absence of Random Dummy Rounds

- The attack targets the penultimate round of AES, e.g, in case of AES128, input of 9^{th} round is the target.
- Fault f in I_0^9, *i.e.*, first byte of the top row in the input of 9^{th} *cipher round*

Piret and Quisquater's Attack in absence of Random Dummy Rounds

- The attack targets the penultimate round of AES, e.g, in case of AES128, input of 9^{th} round is the target.
- Fault f in I_0^9, *i.e.*, first byte of the top row in the input of 9^{th} *cipher round*
- Countermeasure infects faulty computation thrice

Piret and Quisquater's Attack in absence of Random Dummy Rounds

- The attack targets the penultimate round of AES, e.g, in case of AES128, input of 9^{th} round is the target.
- Fault f in I_0^9, *i.e.*, first byte of the top row in the input of 9^{th} *cipher round*
- Countermeasure infects faulty computation thrice
  - After the execution of 9^{th} cipher round

Piret and Quisquater's Attack in absence of Random Dummy Rounds

- The attack targets the penultimate round of AES, e.g, in case of AES128, input of 9^{th} round is the target.
- Fault f in I_0^9, *i.e.*, first byte of the top row in the input of 9^{th} *cipher round*
- Countermeasure infects faulty computation thrice
  - After the execution of 9^{th} cipher round
  - After the execution of 10^{th} cipher round

Piret and Quisquater's Attack in absence of Random Dummy Rounds

- The attack targets the penultimate round of AES, e.g, in case of AES128, input of 9^{th} round is the target.
- Fault f in I_0^9, *i.e.*, first byte of the top row in the input of 9^{th} *cipher round*
- Countermeasure infects faulty computation thrice
  - After the execution of 9^{th} cipher round
  - After the execution of 10^{th} cipher round
  - After the execution of compulsory dummy round

Differential after 9^{th} round

1. Without Countermeasure

$$R_0 \oplus R_1 = \begin{pmatrix} 2f' & 0 & 0 & 0 \\ f' & 0 & 0 & 0 \\ f' & 0 & 0 & 0 \\ 3f' & 0 & 0 & 0 \end{pmatrix}$$

Differential after 9^{th} round

1. Without Countermeasure

$$R_0 \oplus R_1 = \begin{pmatrix} 2f' & 0 & 0 & 0 \\ f' & 0 & 0 & 0 \\ f' & 0 & 0 & 0 \\ 3f' & 0 & 0 & 0 \end{pmatrix}$$

2. With Countermeasure

$$R_0 \oplus R_1 = \begin{pmatrix} 2f' \oplus SNLF[2f'] & 0 & 0 & 0 \\ f' \oplus SNLF[f'] & 0 & 0 & 0 \\ f' \oplus SNLF[f'] & 0 & 0 & 0 \\ 3f' \oplus SNLF[3f'] & 0 & 0 & 0 \end{pmatrix}$$

Differential after 10^{th} round

1. Without Countermeasure

$$R_0 \oplus R_1 = \begin{pmatrix} S[I_0^{10}] \oplus S[I_0^{10} \oplus P_0] & 0 & 0 & 0 \\ 0 & 0 & 0 & S[I_1^{10}] \oplus S[I_1^{10} \oplus P_1] \\ 0 & 0 & S[I_2^{10}] \oplus S[I_2^{10} \oplus P_2] & 0 \\ 0 & S[I_3^{10}] \oplus S[I_3^{10} \oplus P_3] & 0 & 0 \end{pmatrix}$$

Differential after 10^{th} round

1. Without Countermeasure

$$R_0 \oplus R_1 = \begin{pmatrix} S[I_0^{10}] \oplus S[I_0^{10} \oplus P_0] & 0 & 0 & 0 \\ 0 & 0 & 0 & S[I_1^{10}] \oplus S[I_1^{10} \oplus P_1] \\ 0 & 0 & S[I_2^{10}] \oplus S[I_2^{10} \oplus P_2] & 0 \\ 0 & S[I_3^{10}] \oplus S[I_3^{10} \oplus P_3] & 0 & 0 \end{pmatrix}$$

2. With Countermeasure

$$R_0 \oplus R_1 = \begin{pmatrix} z_0 \oplus SNLF[z_0] & 0 & 0 & 0 \\ 0 & 0 & 0 & z_1 \oplus SNLF[z_1] \\ 0 & 0 & z_2 \oplus SNLF[z_2] & 0 \\ 0 & z_3 \oplus SNLF[z_3] & 0 & 0 \end{pmatrix}$$

where $z_i = S[I_i^{10}] \oplus S[I_i^{10} \oplus P_i \oplus SNLF[P_i]], \ i \in \{0, \ldots, 3\}$.

Equations for the keys

1. Without Countermeasure

$$
\begin{aligned}
2 \cdot f' &= S^{-1}[T_0 \oplus k_0^{11}] \oplus S^{-1}[T_0^* \oplus k_0^{11}] \\
1 \cdot f' &= S^{-1}[T_{13} \oplus k_{13}^{11}] \oplus S^{-1}[T_{13}^* \oplus k_{13}^{11}] \\
1 \cdot f' &= S^{-1}[T_{10} \oplus k_{10}^{11}] \oplus S^{-1}[T_{10}^* \oplus k_{10}^{11}] \\
3 \cdot f' &= S^{-1}[T_7 \oplus k_7^{11}] \oplus S^{-1}[T_7^* \oplus k_7^{11}]
\end{aligned}
$$

where T and T^* is correct and faulty ciphertext resp.

Equations for the keys

1. Without Countermeasure

$$
\begin{aligned}
2 \cdot f' &= S^{-1}[T_0 \oplus k_0^{11}] \oplus S^{-1}[T_0^* \oplus k_0^{11}] \\
1 \cdot f' &= S^{-1}[T_{13} \oplus k_{13}^{11}] \oplus S^{-1}[T_{13}^* \oplus k_{13}^{11}] \\
1 \cdot f' &= S^{-1}[T_{10} \oplus k_{10}^{11}] \oplus S^{-1}[T_{10}^* \oplus k_{10}^{11}] \\
3 \cdot f' &= S^{-1}[T_7 \oplus k_7^{11}] \oplus S^{-1}[T_7^* \oplus k_7^{11}]
\end{aligned}
$$

where T and T^* is correct and faulty ciphertext resp.

2. With Countermeasure

$$
\begin{aligned}
2 \cdot f' \oplus SNLF[2 \cdot f'] &= S^{-1}[T_0 \oplus k_0^{11}] \oplus S^{-1}[T_0^* \oplus k_0^{11}] \\
1 \cdot f' \oplus SNLF[1 \cdot f'] &= S^{-1}[T_{13} \oplus k_{13}^{11}] \oplus S^{-1}[T_{13}^* \oplus k_{13}^{11}] \\
1 \cdot f' \oplus SNLF[1 \cdot f'] &= S^{-1}[T_{10} \oplus k_{10}^{11}] \oplus S^{-1}[T_{10}^* \oplus k_{10}^{11}] \\
3 \cdot f' \oplus SNLF[3 \cdot f'] &= S^{-1}[T_7 \oplus k_7^{11}] \oplus S^{-1}[T_7^* \oplus k_7^{11}]
\end{aligned}
$$

where T and T^* is correct and faulty ciphertext resp.

Infection of Compulsory dummy round

1. Due to the presence of compulsory dummy round, the difference between the final faulty and correct ciphertext:

$$T \oplus T^* = \begin{pmatrix} m_0 \oplus cdr_0 & cdr_4 & cdr_8 & cdr_{12} \\ cdr_1 & cdr_5 & cdr_9 & m_1 \oplus cdr_{13} \\ cdr_2 & cdr_6 & m_2 \oplus cdr_{10} & cdr_{14} \\ cdr_3 & m_3 \oplus cdr_7 & cdr_{11} & cdr_{15} \end{pmatrix}$$

$m_j = z_j \oplus SNLF[z_j], j \in \{0, \ldots, 3\}$.

Infection of Compulsory dummy round

1. Due to the presence of compulsory dummy round, the difference between the final faulty and correct ciphertext:

$$T \oplus T^* = \begin{pmatrix} m_0 \oplus cdr_0 & cdr_4 & cdr_8 & cdr_{12} \\ cdr_1 & cdr_5 & cdr_9 & m_1 \oplus cdr_{13} \\ cdr_2 & cdr_6 & m_2 \oplus cdr_{10} & cdr_{14} \\ cdr_3 & m_3 \oplus cdr_7 & cdr_{11} & cdr_{15} \end{pmatrix}$$

$m_j = z_j \oplus SNLF[z_j], j \in \{0, \ldots, 3\}$.

2. Using the relation:
$RoundFunction(R_2, k^0) \oplus \beta = MC(SR(S(R_2) \oplus S(\beta)))$ we have:

$$T \oplus T^* = \begin{pmatrix} m_0 \oplus g_1(F_1, F_2) & 1F_3 & h_1(F_4, F_5, F_6) & 3F_7 \\ g_2(F_1, F_2) & 1F_3 & h_2(F_4, F_5, F_6) & m_1 \oplus 2F_7 \\ g_3(F_1, F_2) & 3F_3 & m_2 \oplus h_3(F_4, F_5, F_6) & 1F_7 \\ g_4(F_1, F_2) & m_3 \oplus 2F_3 & h_4(F_4, F_5, F_6) & 1F_7 \end{pmatrix}$$

$F_i, i \in \{1, \ldots, 7\}$ is infection caused by compulsory dummy round and g_j and h_j, $j \in \{1, \ldots, 4\}$ are linear functions.

P&Q's Attack on LatinCrypt 2012 Countermeasure: Infection Removal

1. After removing infection caused by compulsory dummy round we obtain:

$$T \oplus T^* = \begin{pmatrix} m_0 & 0 & 0 & 0 \\ 0 & 0 & 0 & m_1 \\ 0 & 0 & m_2 & 0 \\ 0 & m_3 & 0 & 0 \end{pmatrix}$$

where $m_j = z_j \oplus SNLF[z_j], j \in \{0, \ldots, 3\}$.

P&Q's Attack on LatinCrypt 2012 Countermeasure: Infection Removal

1. After removing infection caused by compulsory dummy round we obtain:

$$T \oplus T^* = \begin{pmatrix} m_0 & 0 & 0 & 0 \\ 0 & 0 & 0 & m_1 \\ 0 & 0 & m_2 & 0 \\ 0 & m_3 & 0 & 0 \end{pmatrix}$$

   where $m_j = z_j \oplus SNLF[z_j], j \in \{0, \ldots, 3\}$.
2. We can deduce z_j(two possibilities) from m_j which gives 2^4 possibilities for T^*.

P&Q's Attack on LatinCrypt 2012 Countermeasure: Infection Removal

1. After removing infection caused by compulsory dummy round we obtain:

$$T \oplus T^* = \begin{pmatrix} m_0 & 0 & 0 & 0 \\ 0 & 0 & 0 & m_1 \\ 0 & 0 & m_2 & 0 \\ 0 & m_3 & 0 & 0 \end{pmatrix}$$

   where $m_j = z_j \oplus SNLF[z_j], j \in \{0, \ldots, 3\}$.
2. We can deduce z_j(two possibilities) from m_j which gives 2^4 possibilities for T^*.
3. Now, we can make hypotheses on 4 bytes of last round key k^{11}.

$$2 \cdot f' \oplus SNLF[2 \cdot f'] = S^{-1}[T_0 \oplus k_0^{11}] \oplus S^{-1}[T_0^* \oplus k_0^{11}]$$
$$1 \cdot f' \oplus SNLF[1 \cdot f'] = S^{-1}[T_{13} \oplus k_{13}^{11}] \oplus S^{-1}[T_{13}^* \oplus k_{13}^{11}]$$
$$1 \cdot f' \oplus SNLF[1 \cdot f'] = S^{-1}[T_{10} \oplus k_{10}^{11}] \oplus S^{-1}[T_{10}^* \oplus k_{10}^{11}]$$
$$3 \cdot f' \oplus SNLF[3 \cdot f'] = S^{-1}[T_7 \oplus k_7^{11}] \oplus S^{-1}[T_7^* \oplus k_7^{11}]$$

Complexity Analysis

1. 2^4 values of T^* gives $2^4 * 1036$ candidate values for 4 bytes of k^{11}.

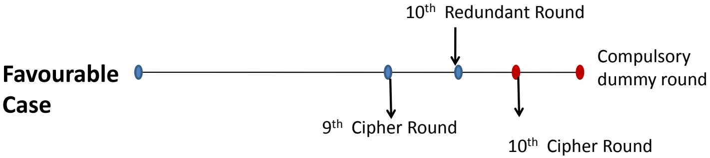
Complexity Analysis

1. 2^4 values of T^* gives $2^4 * 1036$ candidate values for 4 bytes of k^{11}.
2. Repeating the attack with another pair of faulty and correct ciphertext gives atmost 2 candidate values.

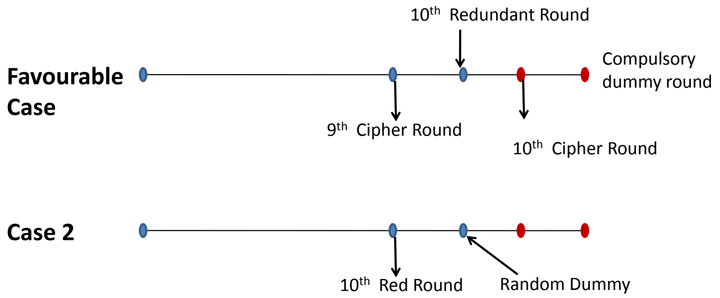
Complexity Analysis

1. 2^4 values of T^* gives $2^4 * 1036$ candidate values for 4 bytes of k^{11}.
2. Repeating the attack with another pair of faulty and correct ciphertext gives atmost 2 candidate values.
3. Total 8 faulty ciphertexts required to retrieve all 16 bytes of k^{11}.

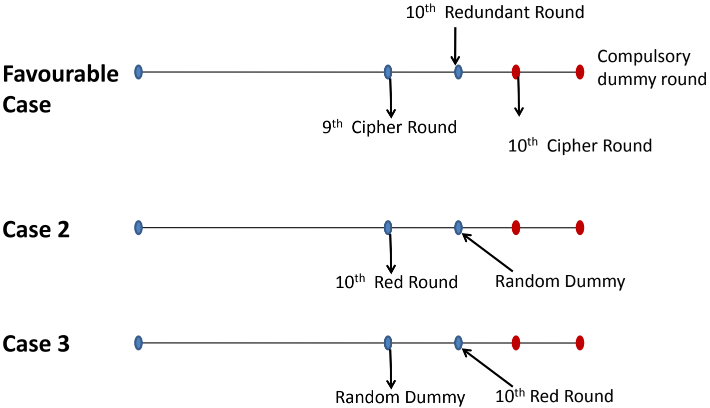
Attack in Presence of Random Dummy Rounds



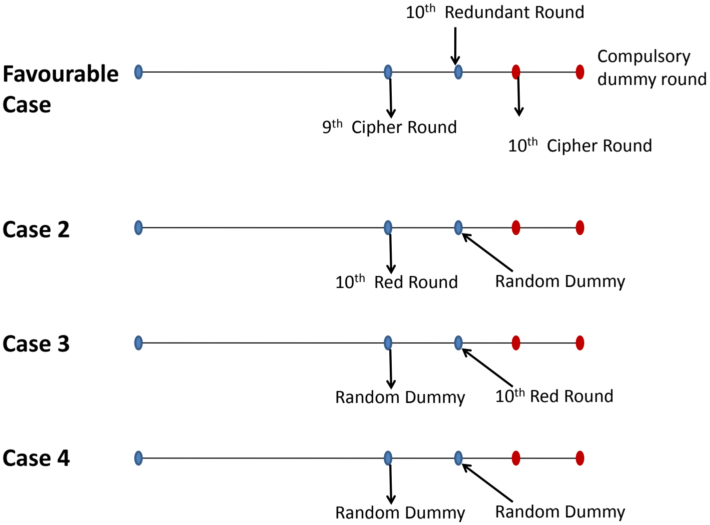
Attack in Presence of Random Dummy Rounds



Attack in Presence of Random Dummy Rounds



Attack in Presence of Random Dummy Rounds



Attack in Presence of Random Dummy Rounds

1. Number of random dummy rounds : d

Attack in Presence of Random Dummy Rounds

1. Number of random dummy rounds : d
2. Total number of rounds : $22 + d + 1$

Attack in Presence of Random Dummy Rounds

1. Number of random dummy rounds : d
2. Total number of rounds : $22 + d + 1$
3. Target round of fault injection : $(22 + d - 2)^{th}$ RoundFunction.

Attack in Presence of Random Dummy Rounds

1. Number of random dummy rounds : d
2. Total number of rounds : $22 + d + 1$
3. Target round of fault injection : $(22 + d - 2)^{th}$ RoundFunction.
4. $(22 + d)^{th}$ RoundFunction: 10^{th} cipher round.

Attack in Presence of Random Dummy Rounds

1. Number of random dummy rounds : d
2. Total number of rounds : $22 + d + 1$
3. Target round of fault injection : $(22 + d - 2)^{th}$ RoundFunction.
4. $(22 + d)^{th}$ RoundFunction: 10^{th} cipher round.
5. $\therefore$ The probability of $(22 + d - 2)^{th}$ *RoundFunction* being a 9^{th} cipher round: $\frac{(19+d)!/((19)!\cdot(d)!)}{(21+d)!/((21)!\cdot(d)!)}$

Attack in Presence of Random Dummy Rounds

1. Number of random dummy rounds : d
2. Total number of rounds : $22 + d + 1$
3. Target round of fault injection : $(22 + d - 2)^{th}$ RoundFunction.
4. $(22 + d)^{th}$ RoundFunction: 10^{th} cipher round.
5. $\therefore$ The probability of $(22 + d - 2)^{th}$ *RoundFunction* being a 9^{th} cipher round: $\frac{(19+d)!/((19)!\cdot(d)!)}{(21+d)!/((21)!\cdot(d)!)}$
6. If $d = 20$ then the probability that 40^{th} *RoundFunction* is a 9^{th} cipher round is nearly 0.26.

Simulation Results

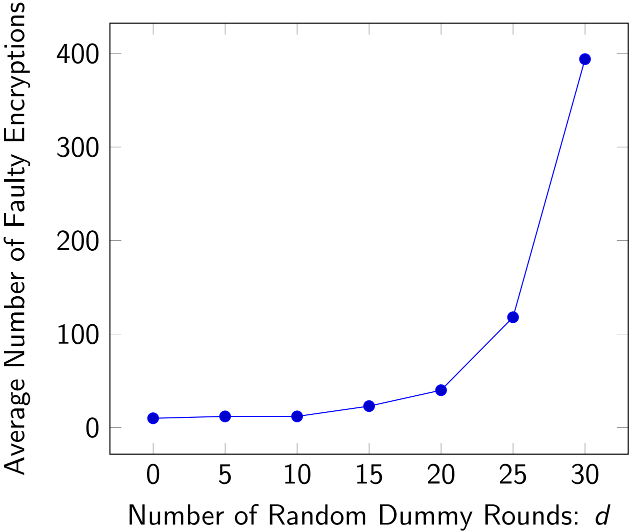


Figure: Piret & Quisquater's Attack on Algorithm 1

Flaws in LatinCrypt 2012 Countermeasure

1. The last cipher round is always the penultimate round: The attacker can verify target round using side channel.

Flaws in LatinCrypt 2012 Countermeasure

1. The last cipher round is always the penultimate round: The attacker can verify target round using side channel.
2. A fault in last three rows of 10^{th} round $\Longrightarrow$
   Infection caused by compulsory dummy round does not affect the erroneous byte.

Flaws in LatinCrypt 2012 Countermeasure

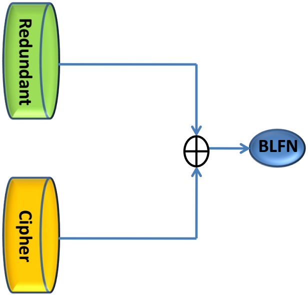
1. The last cipher round is always the penultimate round: The attacker can verify target round using side channel.
2. A fault in last three rows of 10^{th} round $\Longrightarrow$
   Infection caused by compulsory dummy round does not affect the erroneous byte.
3. Countermeasure uses same value to infect erroneous as well as non-erroneous byte.

Flaws in LatinCrypt 2012 Countermeasure

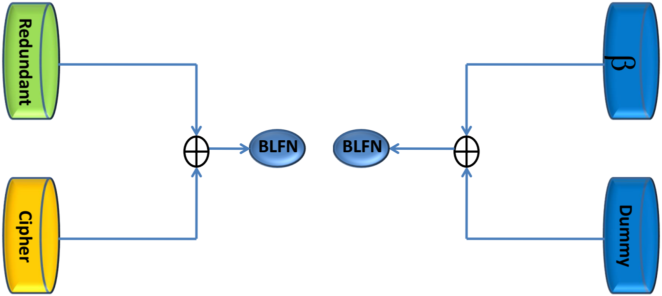
1. The last cipher round is always the penultimate round: The attacker can verify target round using side channel.
2. A fault in last three rows of 10^{th} round $\Longrightarrow$
   Infection caused by compulsory dummy round does not affect the erroneous byte.
3. Countermeasure uses same value to infect erroneous as well as non-erroneous byte.
4. The effect of infection varies for different rounds.

Improved Countermeasure

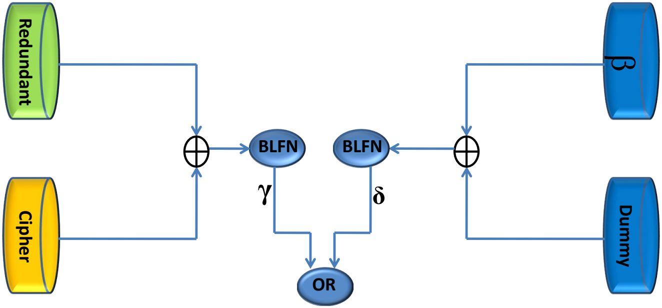
Improved Countermeasure



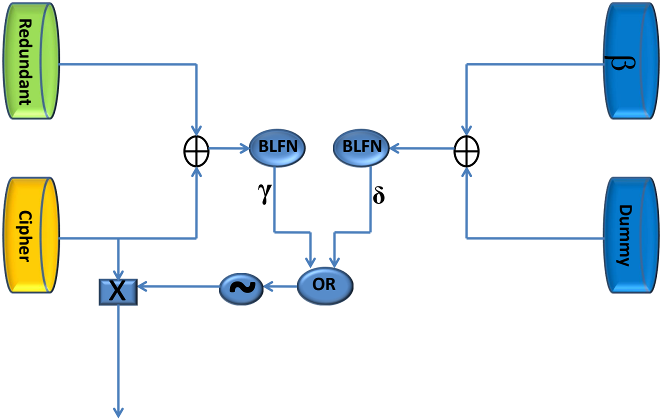
Improved Countermeasure



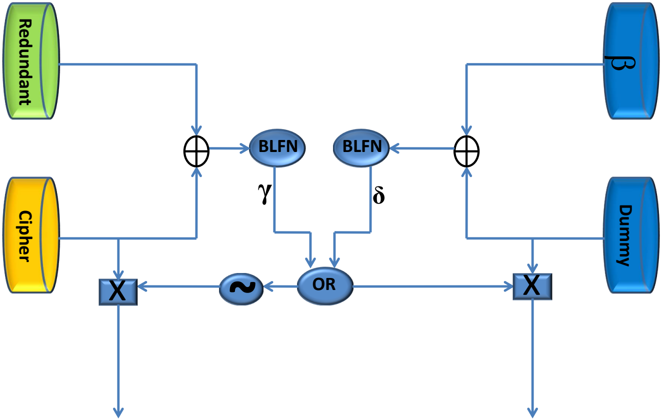
Improved Countermeasure



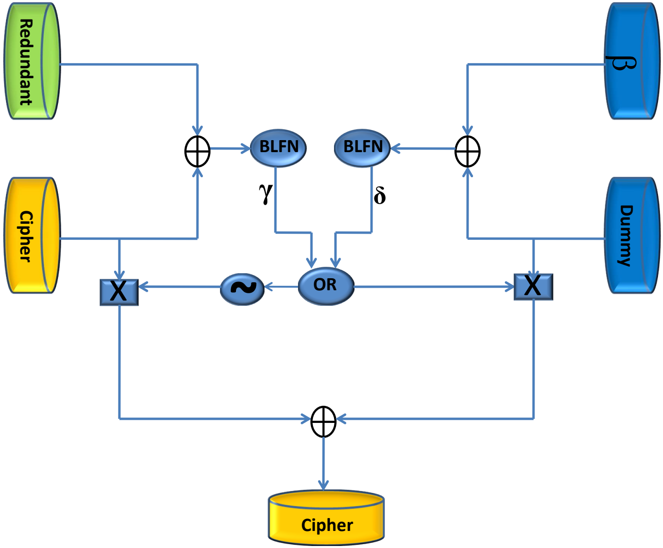
Improved Countermeasure



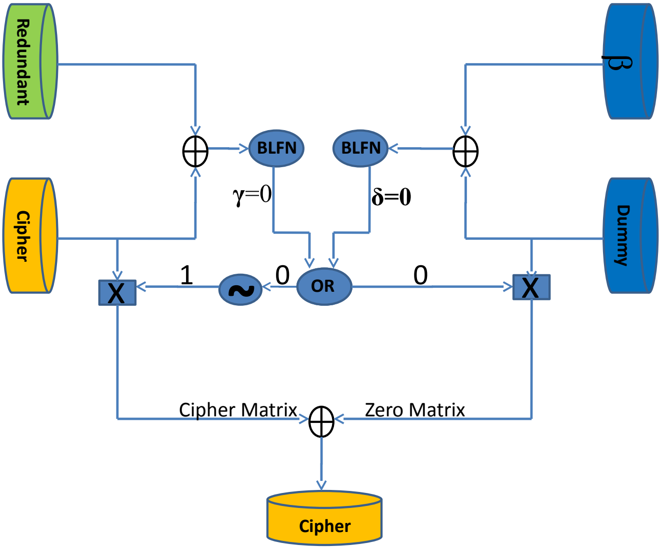
Improved Countermeasure



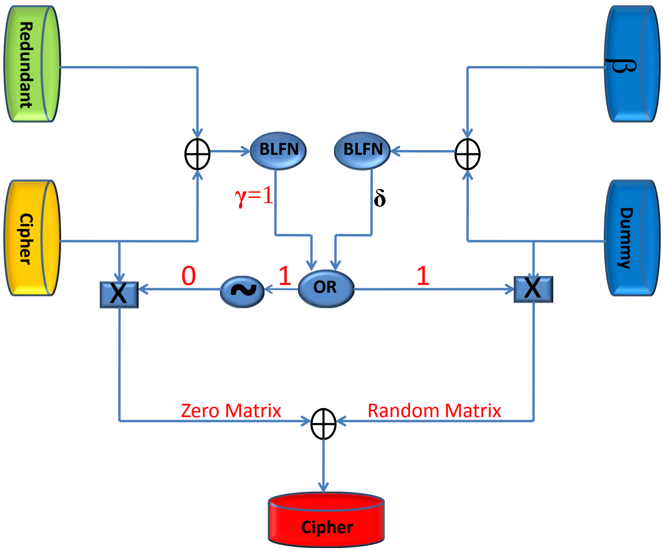
Improved Countermeasure



Improved Countermeasure



Improved Countermeasure



Improved Countermeasure

1. Fault injection in any of the cipher, redundant or dummy round $\Longrightarrow$ **Every** byte in the resulting ciphertext is infected with a different value.
2. The resulting infected faulty ciphertext is completely random.
3. More than one random dummy round after the last cipher round.
4. The improved countermeasure protects both SPN ciphers and Feistel ciphers.

Summary & Conclusion

1. The infection mechanism of LatinCrypt 2012 countermeasure is shown to be ineffective.

Summary & Conclusion

1. The infection mechanism of LatinCrypt 2012 countermeasure is shown to be ineffective.
2. An improved countermeasure is developed, which outputs a completely random value in case of fault injection so that fault attack is impossible.

Thank You !

References

1. D.Boneh, R.A.DeMillo, and R.J.Lipton. On the Importance of Checking Cryptographic Protocols for Faults (ExtendedAbstract). In W. Fumy, editor, Advances in Cryptology - EUROCRYPT 97, volume 1233 of Lecture Notes in Computer Science, pages 37-51. Springer, 1997.
2. E.Biham and A.Shamir. Differential cryptanalysis of DES-like cryptosystems.In B.S. Kaliski (ed.) Advances in Cryptology CRYPTO 97, LNCS, vol. 1294, pp. 513-525. Springer (1997).
3. C.Giraud. DFA on AES. In H. Dobbertin, V. Rijmen, A. Sowa (eds.) AES Conference, Lecture Notes in Computer Science, vol. 3373, pp. 27-41. Springer(2004).
4. J.Blömer and J-P.Seifert. Fault based cryptanalysis of the Advanced Encryption Standard. In R.N. Wright (ed.) Financial Cryptography, Lecture Notes in Computer Science, vol. 2742, pp. 162-181. Springer (2003).

5. G.Piret and J.J.Quisquater. A Differential Fault Attack Technique against SPN Structures, with Application to the AES and KHAZAD . In Cryptographic Hardware and Embedded Systems - CHES 2003 , volume 2779 Lecture Notes in Computer Science, pp 77-88. Springer, 2003.
6. D.Mukhopadhyay. An Improved Fault Based Attack of the Advanced Encryption Standard. In B. Preneel editor, AFRICACRYPT 2009, volume 5580 of Lecture Notes in Computer Science, pages 421-434.Springer,2009.
7. Thomas Fuhr, Éliane Jaulmes, Victor Lomné, Adrian Thillard. Fault Attacks on AES with Faulty Ciphertexts Only, fdtc, pp.108-118, 2013. In Fault Diagnosis and Tolerance in Cryptography, 2013.
8. D.Mukhopadhyay, M.Tunstall, S.Ali. Differential Fault Analysis of the Advanced Encryption Standard Using a Single Fault. In Information Security Theory and Practice. Security and Privacy of Mobile Devices in Wireless Communication 2011, Volume 6633 of Lecture Notes in Computer Science, pages 224-233 . Springer,2011.

9. R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers. The SIMON and SPECK Families of Lightweight Block Ciphers. Cryptology ePrint Archive, Report 2013/404, 2013. Available at http://eprint.iacr.org/.
10. L. Genelle, C. Giraud, and E. Prouff. Securing AES Implementation Against Fault Attacks. In L. Breveglieri, I. Koren, D. Naccache, E. Oswald, and J.-P. Seifert, editors, Fault Diagnosis and Tolerance in Cryptography FDTC 2009. IEEE Computer Society, 2009.
11. M. Medwed and Jorn-Marc-Schmidt. A Continuous Fault Countermeasure for AES Providing a Constant Error Detection Rate. In L. Breveglieri, M. Joye, I. Koren, D. Naccache, and I. Verbauwhede, editors, FDTC. IEEE Computer Society, 2010.
12. M. Joye, P. Manet, and J.-B. Rigaud. Strengthening Hardware AES Implementations against Fault Attacks. IET Information Security, 1:106-110, 2007.

13. J. Fournier, J.-B. Rigaud, S. Bouquet, B. Robisson, A. Tria, J.-M. Dutertre, and M. Agoyan. Design and Characterisation of an AES Chip Embedding Countermeasures. International Journal of Intelligent Engineering Informatics 2011, 1:328347, 2011.
14. T. Malkin, F.-X. Standaert, and M. Yung. A Comparative Cost/Security Analysis of Fault Attack Countermeasures. Fault Diagnosis and Tolerance in Cryptography(FDTC), 2006.
15. Lomne, V., Roche, T., Thillard, A. On The Need of Randomness in Fault Attack Countermeasures-Application to AES. Fault Diagnosis and Tolerance in Cryptography(FDTC), 2012.
16. A.Battistello and C.Giraud. Fault Analysis of Infective AES Computations, fdtc, pp: 101-107, 2013. In Fault Diagnosis and Tolerance in Cryptography, 2013. Also available at 'http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=06623560'.

17. Benedikt Gierlichs, Jörn-Marc Schmidt, Michael Tunstall: Infective Computation and Dummy Rounds: Fault Protection for Block Ciphers without Check-before-Output. In A. Hevia and G. Neven, editors, LATINCRYPT 2012, volume 7533 of LNCS, pages 305-321. Springer, 2012.
18. Daemen, J., Rijmen, V.: AES proposal: Rijndael (1999).
19. FIPS PUB 197: Advanced Encryption Standard (AES). Federal Information Processing Standards Publication 197, National Institute of Standards and Technology (NIST), Gaithersburg (2001).
20. R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers. The SIMON and SPECK Families of Lightweight Block Ciphers. Cryptology ePrint Archive, Report 2013/404, 2013. Available at http://eprint.iacr.org/

21. H. A. Alkhzaimi and M. M. Lauridsen. Cryptanalysis of the SIMON Family of Block Ciphers. Cryptology ePrint Archive, Report 2013/543, 2013. Avaliable at http://eprint.iacr.org/
22. F. Abed, E. List, S. Lucks, and J. Wenzel. Differential Cryptanalysis of Reduced-Round Simon. Cryptology ePrint Archive, Report 2013/526, 2013. Available at http://eprint.iacr.org/.
23. Javad Alizadeh, Nasour Bagheri, Praveen Gauravaram, Abhishek Kumar and Somitra Kumar Sanadhya. Linear Cryptanalysis of Round Reduced SIMON. IACR Cryptology eprint Archive, Report 2013/663, 2013. Available at http://eprint.iacr.org/2013/663