FDTC 2010

Fault Diagnosis and Tolerance in Cryptography

PACA on AES

Passive and Active Combined Attacks

Christophe Clavier	Benoît Feix	Georges Gagnerot	Mylène Roussellet
Limoges University	Inside Contactless	Inside Contactless	Inside Contactless

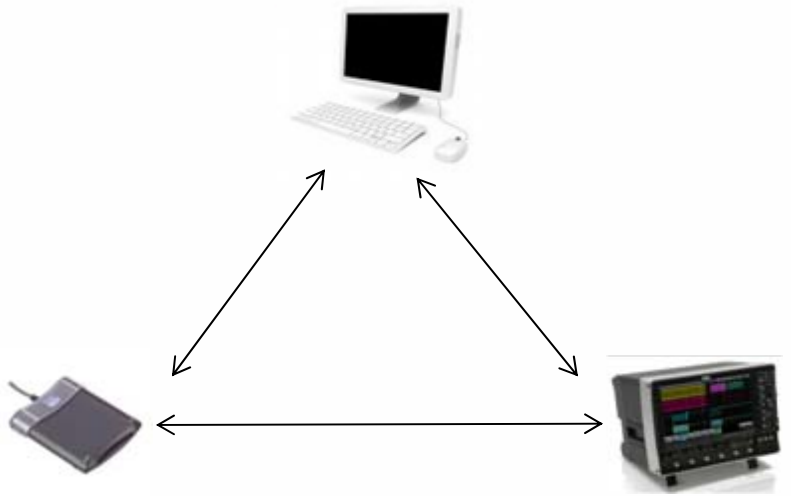
Saturday August, 21, Santa Barbara.

Outline

- Introduction
  - Passive Attacks: SPA, DPA, CPA
  - Active Attacks: DFA, CFA and IFA (Fail Safe Errors)
  - Previous PACA
- Targeted AES Implementation
- PACA on AES
  - CFA + CPA
  - IFA + CPA
- Conclusion

Passive Attacks Notions (some)

- When an IC makes a computation, several transistor are switching states depending on op-code or data manipulated.
- **Side Channel Analysis** exploits that relation
- **Simple Power Analysis**
  Analyze and recover secrets by “reading” curves
- **DPA** and **CPA**
  Usage of statistic Attacks to recover secrets



Passive Attacks

some previous results …

- P. C. Kocher. *Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems.* CRYPTO 1996.
- P. C. Kocher, J. Jaffe, and B. Jun. *Differential power analysis*. CRYPTO ’99,
- E. Brier, C. Clavier, and F. Olivier. *Correlation power analysis with a leakage model.* CHES 2004.
- P-A. Fouque and F. Valette. *The Doubling Attack - why upwards is better than downwards.* CHES 2003.
- S-M. Yen, W-C. Lien, S. Moon, and J. Ha. P*ower Analysis by Exploiting Chosen Message and Internal Collisions - Vulnerability of Checking Mechanism for RSA-Decryption.* Mycrypt 2005.
- S. Mangard, N. Pramstaller, and E. Oswald*. Successfully Attacking Masked AES Hardware Implementations.* CHES 2005
- F. Amiel, B. Feix, and K. Villegas. *Power Analysis for Secret Recovering and Reverse Engineering of Public Key Algorithms.* SAC 2007.
- F-X. Standaert, B. Gierlichs, and I. Verbauwhede. *Partition vs. Comparison Side- Channel Distinguishers: An Empirical Evaluation of Statistical Tests for Univariate Side-Channel Attacks against Two Unprotected CMOS Devices*. ICISC 2008.
- Not exhaustive …

Active Attacks Notions (some)

- **Voluntarily perturb the chip calculations:**
  - Erroneous results or computation can be used and exploited to recover secrets: DFA, CFA
  - Fault has an effect on the chip bits but the results remain correct: IFA, Safe Error
  - …
- **Can be done using glitches, light emission (laser) …**

Active Attacks some previous work …

- E. Biham and A. Shamir. *Differential Fault Analysis of Secret Key Cryptosystems*, CRYPTO 97.
- D. Boneh, R. A. DeMillo, and R. J. Lipton. *On the importance of checking cryptographic protocols for faults.* EUROCRYPT 1997,
- S. P. Skorobogatov and R. J. Anderson. *Optical fault induction attacks*, CHES 2002.
- C. Giraud and H. Thiebeauld. *A survey on fault attacks*. CARDIS 2004.
- G. Piret and J-J. Quisquater . *A Differential Fault Attack Technique against SPN Structures, with Application to the AES and KHAZAD.* CHES 2003.
- S-M. Yen and M. Joye. *The Montgomery Power Ladder.* CHES 2002.
- H. Choukri and M. Tunstall.,*Round Reduction Using Faults.* FDTC 2005
- Blomer and J-P. Seifert . *Fault Based Cryptanalysis of the Advanced Encryption Standard (AES).* FC 2003.
- F. Amiel, C. Clavier and M. Tunstall - Fault Analysis of DPA-Resistant Algorithms – FDTC 2006
- C. Clavier: *Secret External Encodings Do Not Prevent Transient Fault Analysis*. CHES 2007
- J-S. Coron, A. Joux, I. Kizhvatov, D. Naccache, P. Paillier. *Fault Attacks on RSA Signatures with Partially Unknown Messages.* CHES 2009
- Not exhaustive …

Some Previous Work similar to PACA

- **Sergeï Skorobogatov.**
  Optically Enhanced Position-Locked Power Analysis CHES 2006
  Use a focused laser to enhance the power consumption of a sensitive part in a chip.

- **F. Amiel, B. Feix, L. Marcel and K. Villegas.**
  PACA on RSA FDTC 2007
  Use fault injection to perturb message operand settings to create SPA leakage in exponentiation

- **J. Di-Battista, J-C. Courrege, B. Rouzeyre, Li. Torres and P. Perdu.**
  When Failure Analysis Meets Side-Channel Attacks CHES 2010

- … Not exhaustive …

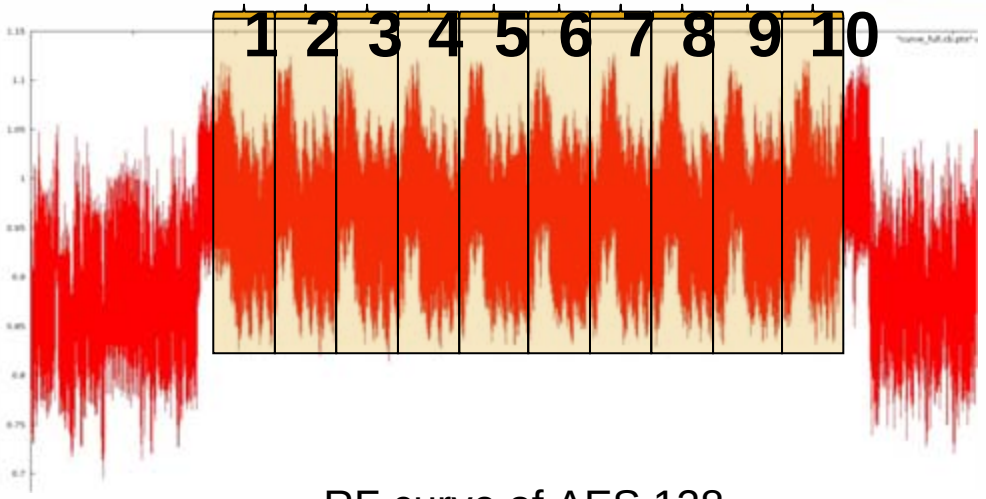
Reminder on AES

- **Advanced Encryption Standard**
  - 128-bit input message blocks
  - 128, 192 or 256 bits key
  - Based on SPN scheme.

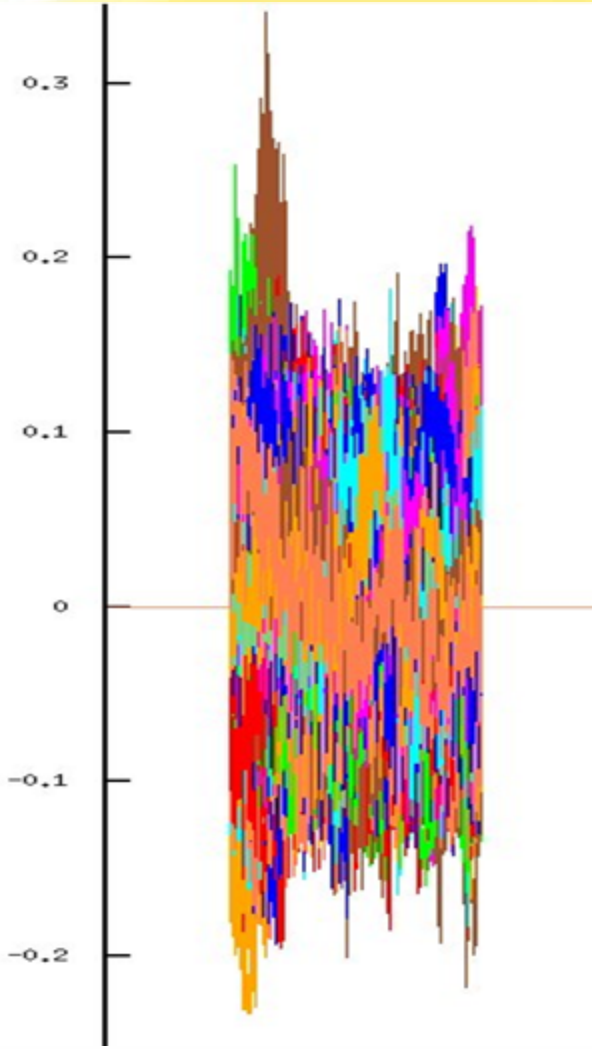
- We choose here AES 128 but our results can be applied to AES 192 and AES 256.

- **Schoolbook implementation not resistant to**
  - Active Attacks
  - Passive Attacks

Correlation on AES



RF curve of AES 128



CPA Sample

Secure AES implementation targeted

- Implementation using an 8-bit architecture core
- **Targeted** to resist classical practical Second Order Power Analysis attacks

  [1] M.-L. Akkar, R. Bevan, and L. Goubin. *Two Power Analysis Attacks against One-Mask Methods*

  [17] S. Mangard, N. Pramstaller, and E. Oswald. *Successfully Attacking Masked AES Hardware Implementations.*

- Computing the inversion with Oswald et al. FSE 2005 trick

  [19] E. Oswald, S. Mangard, N. Pramstaller, and V. Rijmen. A Side-Channel Analysis Resistant Description of the AES S-Box.

  → We use different mask per byte values for intermediate data and between the different rounds

- Such an implementation is resistant to the CFA presented by Amiel et al. at FDTC 2006 as it only applies to single mask protected AES.
  - The attack could not occur when mask uses 16 different bytes.
- We improve here their analysis when intermediate data bytes and key bytes are masked with different bytes …
  - Based on the **same fault model**
  - Using **less fault** injections
  - But adding **power analysis** …

Fault Model

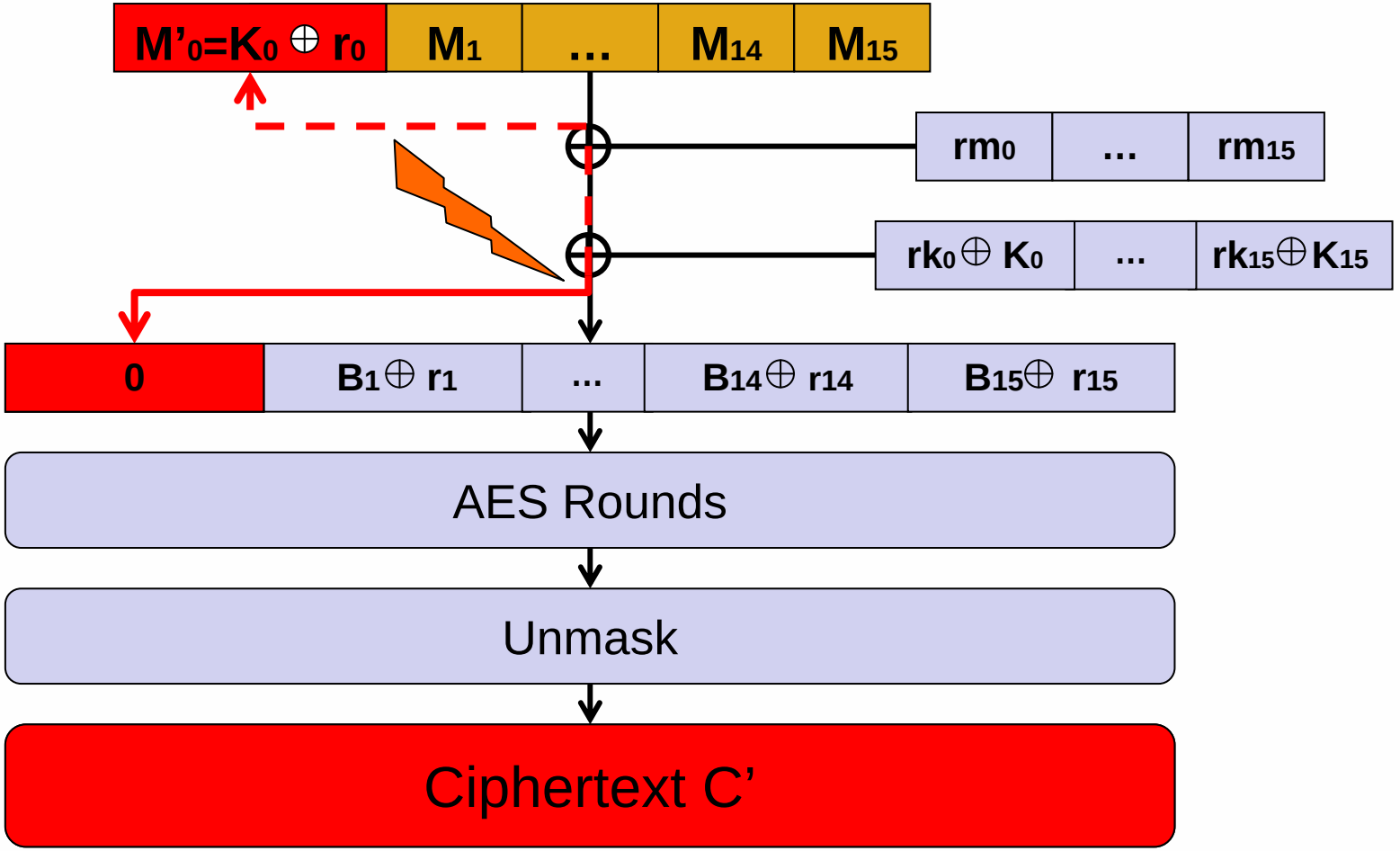
- An instruction can be bypassed
  - For instance by modifying an op-code to a NOP (NOP = 00 in JAVA)
- A loop counter can be modified
  - Reducing the number of byte key additions
- Corruption of Read or Write operations on RAM
- ALU process can be perturbed
  - XOR result can be set to 0 or to a constant value

Combining CPA with CFA

to counterfeit an

Differential SCA Protected AES

PACA on AES


M'0=K0 ⊕ r0
M1
…
M14
M15
rm0
…
rm15
rk0 ⊕ K0
…
rk15⊕K15
0
B1⊕ r1
…
B14⊕ r14
B15⊕ r15
AES Rounds
Unmask
Ciphertext C'

PACA on AES

- Effect: a differential δ has been introduced in the calculation
  - Indeed fault effect is the same as if we introduced a modification on M0
  - *For cst = 0*

$$AES_{\substack{faulted \\ sec\ ure}}(M) = AES_{sec\ ure}(M_0 \oplus \delta, M_1, ..., M_{15}) = C'$$

$$\delta = M_0 \oplus K_0 \oplus rm_0 \oplus rk_0 = M_0 \oplus K_0 \oplus r_0$$

$$AES_{\substack{faulted \\ sec\ ure}}(M) = AES_{sec\ ure}(K_0 \oplus r_0, M_1, ..., M_{15}) = C'$$

- For sake of simplicity use *M = (0 … 0)*
- Search *M'=(M'0 |0 |… | 0)* which collides with *C'*
  - s.t. *AES(M') = C'*
  - *only 256 possible values to test for M'0.*
- We obtain a simple relation between key byte and random byte

$$M'_0 = K_0 \oplus r_0$$

  - We store the power curve W0 of the faulted AES

PACA on AES

- By repeating it we obtain many relations and power curves:

$$\begin{aligned} M'_{0,0} &= K_0 \oplus r_{0,0} & W_0 \\ M'_{0,1} &= K_0 \oplus r_{0,1} & W_1 \\ &\ldots & \ldots \\ M'_{0,k-1} &= K_0 \oplus r_{0,k-1} & W_{k-1} \end{aligned}$$

- We obtain the relations set :

$$SK_0 = \left\{ M'_{0,0} \oplus K_0 = r_{0,0}, M'_{0,1} \oplus K_0 = r_{0,1}, \ldots, M'_{0,k-1} \oplus K_0 = r_{0,k-1} \right\}$$

- Correlation then occurs between the two following sets:

$$SK_0$$

$$W = \left\{ W_0, W_1, \ldots, W_{k-1} \right\}$$

… as random values are generated and manipulated in W_i.

PACA on AES

- A guess *g* on K_0 can then be validated if correlation occurs between the two following sets:

$$Sg = \{ M'_{0,0} \oplus g, M'_{0,1} \oplus g, ..., M'_{0,k-1} \oplus g \}$$

$$W = \{ W_0, W_1, ..., W_{k-1} \}$$

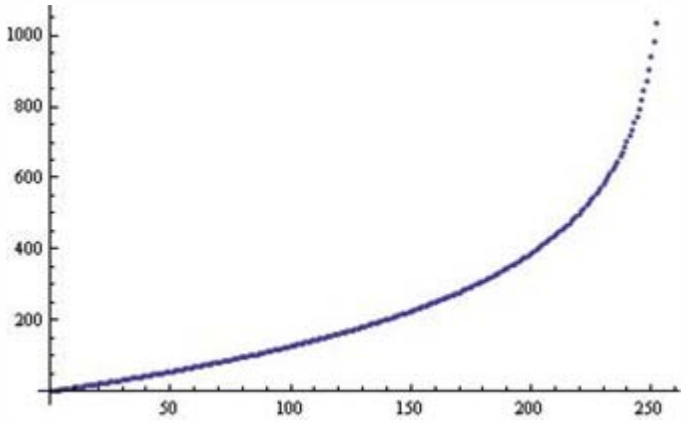
- Try the 256 possible values and when correlation is high we know $K_0 = g$.

- Reproduce same analysis for other key bytes.

PACA on AES

- Expected faults to obtain k relations:

Fault injections



Delta relations

Delta Values	Faults needed
50	56
100	126
150	226
200	388
256	1568

Phase 1: dictionnary precomputation

$M = (M_0, \ldots, M_{15}) \leftarrow (0, \ldots, 0)$
for $u = 0$ to 255 **do**
  $C_u \leftarrow AES(M|M_n = u)$

Phase 2: collision search

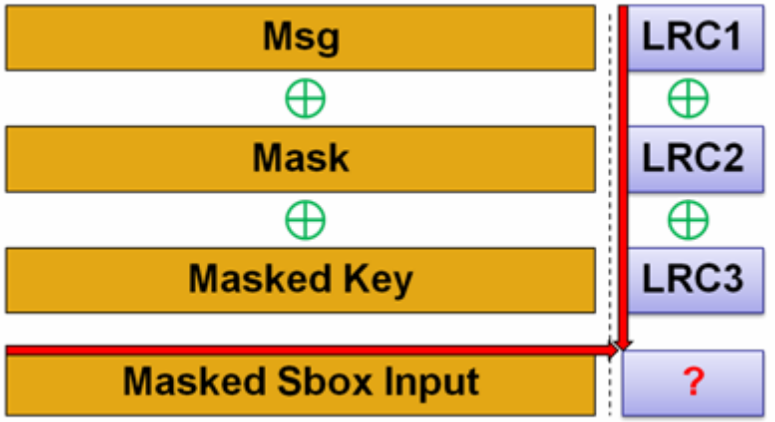
$\Gamma = \varnothing$
$i \leftarrow 1$
while $(i < k)$ **do**
  $C^i = AES^i(M)$
  if $C^i \notin \Gamma$ **do**
    $\delta_i \leftarrow u$ such that $C^i = C_u$ with $u \in \{0, \ldots, 255\}$
    $W_i \leftarrow$ power curve of the faulted execution
    $\Gamma \leftarrow \Gamma \cup \{C^i\}$
    $i \leftarrow i + 1$

Phase 3: correlation

for $g = 0$ to 255 **do**
  for $i = 1$ to k **do**
    $r_{n,i} \leftarrow \delta_i \oplus g$
  $\rho_g \leftarrow$ correlation trace between $\{r_{n,1}, \ldots, r_{n,k}\}$ and $\{W_1, \ldots, W_k\}$
$K_n \leftarrow g$ which gives the highest correlation peak

Countermeasures

- Standard inverse computation
- Duplicated rounds
  - Alternative to full inverse computation
  - Not efficient when both encryption and decryption are both available
- Integrity verifications between calculations



- Resistant HODPA implementation

M. Rivain and E. Prouff. Provably Secure Higher-Order Masking of AES CHES 2010

Combining CPA with IFA / Safe Errors

to counterfeit an

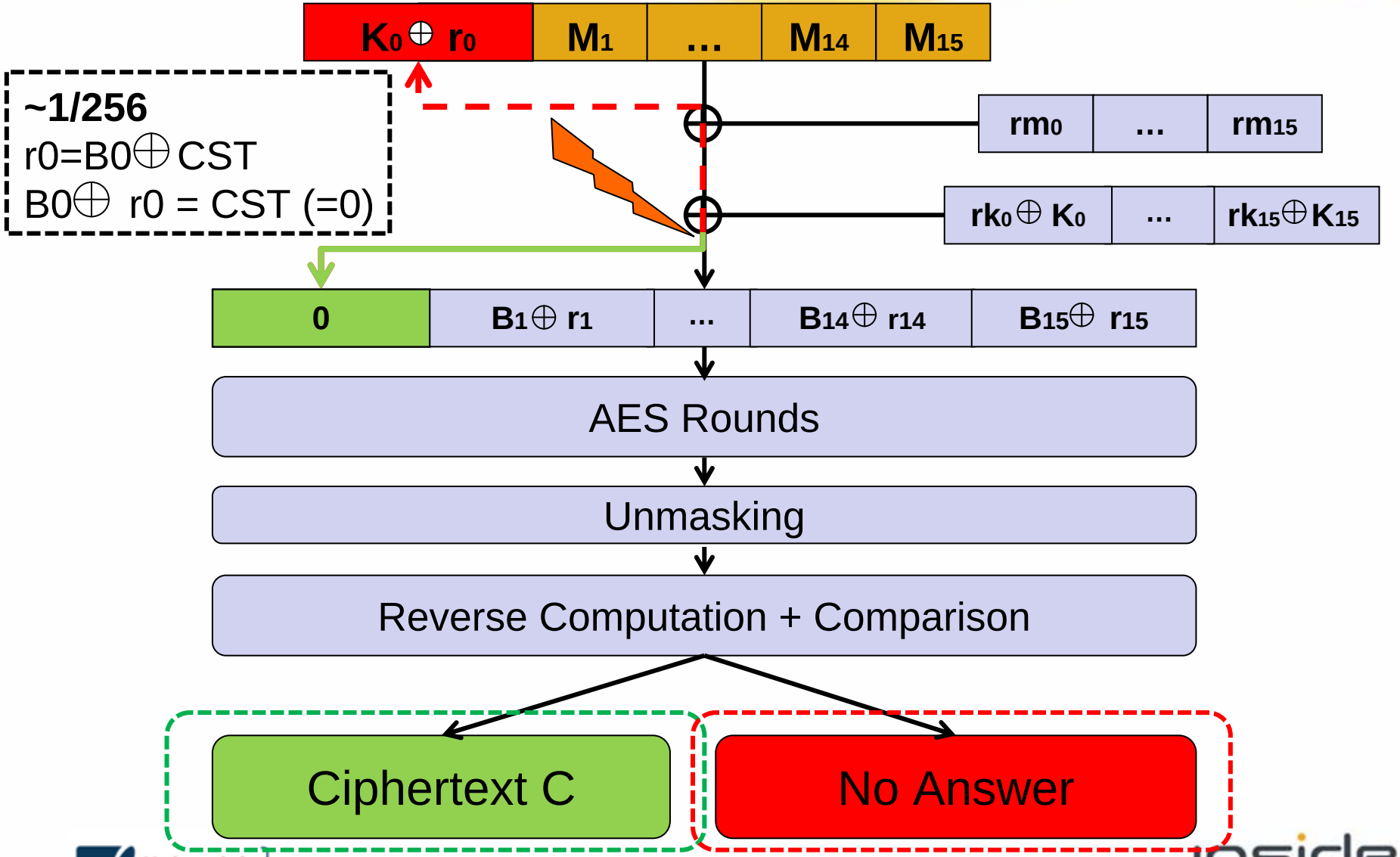
DPA and DFA/CFA Protected AES

PACA with IFA

- We consider the previous Differential SCA resistant AES with a reverse AES computation done at the end to prevent DFA.
- In that case the previous PACA cannot apply as the fault injection will be detected.

  EXCEPT when *delta = 0*
- As previously the KEY addition is faulted to a constant value
- **Repeat fault process until the card returns a Ciphertext rather than "No answer"**

IFA on AES-AES^{-1}



PACA on AES-AES$_{inverse}$

- Assuming Cst=0, We get the relations:

$$AES_{\substack{faulted \\ secure}}(M) = AES(M)$$

$$AES(K_0 \oplus r_0, M_1, ..., M_{15}) = AES(M)$$

$$M_0 = K_0 \oplus r_0$$

- The attack works as previously described
- Hard to tell whether the fault perturbed the IC or not
  - Fault injection system must be very reliable
- More fault injections are needed
- Known message attack is possible while in the first attack it was a chosen message attack.

Countermeasures

- Previous countermeasures like inverse computation doesn't work anymore.
- Improving the difficulty
  - Hardware countermeasures improve the feasibility
    - Clock jitter
    - Fault detectors
  - Code execution randomized
- Lock the card when too many faults have been detected.
- Resistant HODPA implementation

  M. Rivain and E. Prouff. Provably Secure Higher-Order Masking of AES CHES 2010

Attacks Comparison

CFA+CPA

- Can verify fault effect with collision
- Easy to setup

- Obvious countermeasures
- Doesn't Work on Fault protected Implementations

IFA+CPA

- **Works on implementations protected against DPA/Fault**
- **Known message Attack**
- Hard to protect against

- Fault injection system must be very reliable
- Hard to setup with desynchronization
- Requires more faults injection

Conclusion

- **New attack combining FA and SCA** can be used to break DPA resistant implementations in few fault injections combined with classical CPA.
- **Combined with IFA it can bypass full security countermeasures**
  - Very difficult to mount in practice
  - Realistic only if the fault effect is very reliable
- **Not limited to AES...**

Erratum

- Some errors are present in the proceedings paper
  - Minor typos in final scheme AES on masks notations
  - Number of AES rounds to protect is 5 and not 3
  - Our implementation seems to be threatened by some kind of Second Order DPA

- **Corrected and extended version of the paper will be soon published on IACR e-print.**

Thank you for your attention !

Questions ?

Countermeasures