FDTC 2010
Fault Diagnosis and Tolerance in Cryptography

PACA on AES
Passive and Active Combined Attacks

Christophe Clavier
Limoges University

Benoît Feix
Inside Contactless

Georges Gagnerot
Inside Contactless

Mylène Roussellet
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

- S. Mangard, N. Pramstaller, and E. Oswald. *Successfully Attacking Masked AES Hardware Implementations.* CHES 2005

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


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
  
  

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

\[ M'\_0 = K_0 \oplus r_0 \quad \square \quad \ldots \quad \square \quad M_1 \quad \ldots \quad \square \quad M_{14} \quad \square \quad M_{15} \]

\[ \square \quad B_0 \oplus r_0 \quad \ldots \quad \square \quad B_{14} \oplus r_{14} \quad \square \quad B_{15} \oplus r_{15} \]

AES Rounds

Unmask

Ciphertext C'
Effect: a differential $\delta$ has been introduced in the calculation

- Indeed fault effect is the same as if we introduced a modification on $M_0$
- For $cst = 0$

\[
AES_{\text{faulted}}(M) = AES_{\text{secure}}(M_0 \oplus \delta, M_1, \ldots, M_{15}) = C'
\]

\[
\delta = M_0 \oplus K_0 \oplus r_m 0 \oplus r_k 0 = M_0 \oplus K_0 \oplus r_0
\]

\[
AES_{\text{faulted}}(M) = AES_{\text{secure}}(K_0 \oplus r_0, M_1, \ldots, M_{15}) = C'
\]

For sake of simplicity use $M = (0 \ldots 0)$

Search $M' = (M'_0 | 0 | \ldots | 0)$ 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 $W_0$ of the faulted AES
By repeating it we obtain many relations and power curves:

\[ M'_{0,0} = K_0 \oplus r_{0,0} \quad W_0 \]
\[ M'_{0,1} = K_0 \oplus r_{0,1} \quad W_1 \]
\[ \ldots \]
\[ M'_{0,k-1} = K_0 \oplus r_{0,k-1} \quad W_{k-1} \]

We obtain the relations set:

\[ SK_0 = \{ M'_{0,0} \oplus K_0 = r_{0,0}, M'_{0,1} \oplus K_0 = r_{0,1}, \ldots, M'_{0,k-1} \oplus K_0 = r_{0,k-1} \} \]

Correlation then occurs between the two following sets:

\[ SK_0 \]
\[ W = \{ W_0, W_1, \ldots, W_{k-1} \} \]

... as random values are generated and manipulated in \( W_i \).
A guess $g$ on $K_0$ can then be validated if correlation occurs between the two following sets:

$$S_g = \{ \oplus M'_{0,0} \oplus g, \oplus M'_{0,1} \oplus g, \ldots, \oplus M'_{0,k-1} \oplus g \}$$

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

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

Reproduce same analysis for other key bytes.
• Expected faults to obtain $k$ relations:

<table>
<thead>
<tr>
<th>Delta Values</th>
<th>Faults needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>50</td>
<td>56</td>
</tr>
<tr>
<td>100</td>
<td>126</td>
</tr>
<tr>
<td>150</td>
<td>226</td>
</tr>
<tr>
<td>200</td>
<td>388</td>
</tr>
<tr>
<td>256</td>
<td>1568</td>
</tr>
</tbody>
</table>

Phase 1: dictionary precomputation

\[ M = (M_0, \ldots, M_{15}) \leftarrow (0, \ldots, 0) \]

for $u = 0$ to 255 do
  \[ C_u \leftarrow \text{AES}(M | M_n = u) \]

Phase 2: collision search

\[ \Gamma = \emptyset \]

$i \leftarrow 1$

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

Phase 3: correlation

for $g = 0$ to 255 do
  for $i = 1$ to $k$ do
    $r_{n,i} \leftarrow \delta_i \oplus g$
    $\rho_g \leftarrow \text{correlation trace between } \{r_{n,1}, \ldots, r_{n,k}\} \text{ and } \{W_1, \ldots, W_k\}$
    $K_n \leftarrow g$ 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\textsuperscript{inverse}

\[ K_0 \oplus r_0 \quad M_1 \quad \ldots \quad M_{14} \quad M_{15} \]

\[ \text{rm}_0 \quad \ldots \quad \text{rm}_{15} \]

\[ \text{r}_k_0 \oplus K_0 \quad \ldots \quad \text{r}_k_{15} \oplus K_{15} \]

~1/256
r_0 = B_0 \oplus \text{CST}
B_0 \oplus r_0 = \text{CST} (=0)

0 \quad B_1 \oplus r_1 \quad \ldots \quad B_{14} \oplus r_{14} \quad B_{15} \oplus r_{15}

AES Rounds

Unmasking

Reverse Computation + Comparison

Ciphertext C

No Answer
Assuming $Cst=0$, we get the relations:

\[ AES_{\text{faulted}}^\text{secure}(M) = AES(M) \]
\[ AES(K_0 \oplus r_0, M_1, \ldots, M_{15}) = AES(M) \]
\[ M_0 = K_0 \oplus r_0 \]

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

<table>
<thead>
<tr>
<th>CFA+CPA</th>
<th>IFA+CPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Can verify fault effect with collision</td>
<td>Works on implementations protected against DPA/Fault</td>
</tr>
<tr>
<td>Easy to setup</td>
<td>Known message Attack</td>
</tr>
<tr>
<td>Obvious countermeasures</td>
<td>Hard to protect against</td>
</tr>
<tr>
<td>Doesn’t Work on Fault protected Implementations</td>
<td>Fault injection system must be very reliable</td>
</tr>
<tr>
<td></td>
<td>Hard to setup with desynchronization</td>
</tr>
<tr>
<td></td>
<td>Requires more faults injection</td>
</tr>
</tbody>
</table>
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

- Msg
- Mask
- Masked Key
- Masked Sbox Input

- LRC1
- LRC2
- LRC3

Masked Sbox Input?