M&M: Masks and Macs against Physical Attacks

CHES 2019
Lauren De Meyer, Victor Arribas
Svetla Nikova, Ventzislav Nikov, Vincent Rijmen
BACK TO THE 90’S

• Differential Power Analysis (DPA) – Paul Kocher et al. 1999 [KJJ99]

• Differential Fault Analysis (DFA) – Biham and Shamir 1997 [BS97]
**COUNTERMEASURES**

- Against side-channel attacks:
  - Hiding
  - Masking

- Against fault attacks:
  - Repetition, redundancy (EDC, tags), …
  - Detection, correction or infection
COMBINED COUNTERMEASURES

\[ p_0, \ldots, p_d \]

\[ \tau_0^p, \ldots, \tau_d^p \]

\[ c_0, \ldots, c_d \]

\[ \tau_0^c, \ldots, \tau_d^c \]
**Threshold Crypto**

- **MPC**
  - Shamir’s Secret Sharing [Sha79]
  - Masking ([ISW03], [NRS11], …)

- **Embedded Systems**
  - SPDZ [DPS+12], …
  - …

- **Passive**

- **Active**

- **SCA**

- **SCA+FA**

References:

TWO ROUTES

CAPA [RDB+18]:
Based on active MPC protocol SPDZ

Extension of masking schemes:
- ParTI [SMG16]
- [SFE+18]
- New: M&M

M&M
The essentials
ADVERSARY MODEL

• Side-Channel Adversary:
  o $d$-probing model

• Faulting Adversary:
  o Fault = stochastic additive error
    • Unlimited # bits
  o Fault = exact
    • Limited to $d$ shares

• Combined Adversary
**INFORMATION-THEORETIC MAC TAGS**

Data block: \( x \in GF(2^k) \)

MAC key: \( \alpha \in GF(2^k)^m \)

- Used 1x!
- Secret!

\[ \text{Pr[compromised } (x, \tau^x) = \text{consistent}] = 2^{-km} \]
Suppose $\alpha=$fixed (not secret)
- $\sim$ linear code
- $\sim$ ParTI [SMG16]
- Fault model: limited in HW

Combined Attacks
- Adversary has “some” side-channel information
  - $x \rightarrow x \oplus \Delta \Rightarrow \tau^x \rightarrow \tau^x \oplus \tau^\Delta$
  - make $\alpha$ secret
**MASKED MULTIPLIER**

- ISW, TI, DOM, CMS, ...
- Example ($d = 1$):

\[
\begin{align*}
  z_0 &= [x_0y_0] \oplus [x_0y_1 \oplus r] \\
  z_1 &= [x_1y_1] \oplus [x_1y_0 \oplus r]
\end{align*}
\]
M&M MULTIPLICATION

Masks:

MACs:
M&M MULTIPLICATION

Masks:

MACs:

\[ x \times \alpha^2 xy \times \tau^y = \alpha xy \times \tau^z \]
OR OTHER OPERATIONS …

Masks:

MACs:
And even ...

Masks:

\[ x \rightarrow 0^{-1} \rightarrow x^{-1} \rightarrow z \]

MACs:

\[ \tau^x \rightarrow 0^{-1} \rightarrow \alpha^{-1}x^{-1} \rightarrow \times \rightarrow \alpha x^{-1} \rightarrow \tau^z \]
BUILDING BLOCKS FOR ANY ALGORITHM

MANY FLAVORS OF MASKING ➔ MANY FLAVORS OF M&M
Masked Encryption Datapath

\[ p \xrightarrow{\textbf{MAC}} \tau^p \xrightarrow{\text{Enc}} \tau^c \xrightarrow{\text{Enc}^{\text{MAC}}} c \]

Now what?

Masked Tag Datapath
\[ \alpha c = \tau^c? \]
\[ \alpha c \neq \tau^c \]

Vulnerable to combined attacks!
INFECTIVE COMPUTATION [LRT12]

\[ p \xrightarrow{Enc} c \xrightarrow{PRNG} c \oplus R \cdot (c \oplus c') \]

\[ R \neq 0,1 \]

Broken by [BG13]
(bias on \( R \))

---


Infect

\[ c_i \oplus R \cdot ((\alpha c)_i \oplus \tau^c_i) \]

Unshared:
\[ c \oplus R(\alpha c \oplus \tau^c) = c \text{ if tags ok} \]
Else random

\[ R \neq 0 \]
**NO BIAS?**

- Faulty evaluation gives $\hat{c} = c \oplus \Delta$

- Output:

$$c \oplus \Delta \oplus R \cdot (\alpha (c \oplus \Delta) \oplus \tau^c) = c \oplus \Delta \oplus R \cdot (\alpha \epsilon \oplus \alpha \Delta \oplus \tau^\epsilon) = c \oplus \Delta (1 \oplus R\alpha)$$

- Is $\Delta(1 \oplus R\alpha)$ uniformly random?

- Yes if $\alpha$ uniform in $\mathbb{F}_q$ and $R$ uniform in $\mathbb{F}_q^*$
CASE STUDY
**Example: AES**

- Using S-box from [DRB+16]

- Comparing area-overhead to state-of-the-art:

<table>
<thead>
<tr>
<th>Scheme</th>
<th>SCA-only [kGE]</th>
<th>Combined [kGE]</th>
<th>Overhead factor</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>d = 1</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CAPA [RDB+18]</td>
<td>3.6</td>
<td>30.5</td>
<td>8.47</td>
</tr>
<tr>
<td>ParTI [SMG16]</td>
<td>7.9</td>
<td>20.2</td>
<td>2.56</td>
</tr>
<tr>
<td>M&amp;M</td>
<td>7.6</td>
<td>19.2</td>
<td><strong>2.53</strong></td>
</tr>
<tr>
<td><strong>d = 2</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CAPA [RDB+18]</td>
<td>5.9</td>
<td>55.2</td>
<td>9.35</td>
</tr>
<tr>
<td>M&amp;M</td>
<td>12.6</td>
<td>33.2</td>
<td><strong>2.63</strong></td>
</tr>
</tbody>
</table>

SIDE-CHANNEL EVALUATION

- Spartan6 on SAKURA-G
- TVLA [BCD+13] (t-test)
- 50 million traces

Fault Evaluation

• No “standard” methods of verification

• Adapt HDL with possibility to inject randomized faults (XOR)

• Experiment: 50,000 iterations, 189 faulty ciphertexts not infected → experimental rate of detection/infection = 0.9962

• Theoretical rate of detection/infection: \(1 - 2^{-8} = 0.9961\)

• Verification methodology extended and automized in VerFI (see poster session)
TAKE-AWAY

• Cheaper than CAPA and stronger adversary than ParTI

• Super versatile: use any existing or future(?) masking scheme

• Infective computation can be combined with detection result (see paper)

• Future work:
  o provable security against combined attacks?
  o Verification tools for combined countermeasures?
  o Optimization: don’t update tags: $ax \rightarrow \alpha^{-1}y \rightarrow \cdots \rightarrow \alpha z$
Thank You