Mid-Size Primes for Symmetric Cryptography with Strong Embedded Security (Low-Noise Masking and Hard Physical Learning Problems)

François-Xavier Standaert
UCLouvain, Crypto Group
STAP 2023
Lyon, France, April 23, 2023
• Side-channel analysis & the need of masking
• Boolean masking and the need of noise
• Prime masking and design challenges

• Fresh re-keying & basic models
• Hard physical learning problems

• General conclusions for symmetric crypto
Outline

• **Side-channel analysis & the need of masking**
  • Boolean masking and the need of noise
  • Prime masking and design challenges

• Fresh re-keying & basic models

• Hard physical learning problems

• General conclusions for symmetric crypto
Power Analysis Analysis [KJJ99]

- Leakage trace: $l_i$
- Comparison: $\tilde{k}$
- Subkey candidate
- Model: $m_i^{k^*}$
- Executed operations: $x_i$, $k$, $y_i$, $S$-box, $z_i$, $V_i$
DPA vs. SPA taxonomy

- Differential Power Analysis (many-traces attacks)

\[
\Pr \left[ A_{KR} \left( x_1, L(x_1, K), \ldots, x_q, L(x_q, K) \right) \rightarrow K | K \leftarrow $ \right] \approx 2^{-128+q\cdot\lambda}
\]

\[
\lambda \approx \text{MI}(Z; L)
\]
DPA vs. SPA taxonomy

- Differential Power Analysis (many-traces attacks)
  \[ \Pr \left[ A_{KR} \left( x_1, L(x_1, K), \ldots, x_q, L(x_q, K) \right) \rightarrow K \mid K \leftarrow \$ \right] \approx 2^{-128 + q \cdot \lambda} \]

- Simple Power Analysis (few-traces attacks)
  \[ \lambda \approx \text{MI}(Z; L) \]

\[ q = 50 \]
DPA security is needed

- Everywhere for standard modes of operation

OCB
DPA security is needed

- Everywhere for standard modes of operation
- Mildly for leakage-resistant modes of operation
  - $\propto$ requirements (e.g., integrity, confidentiality)
Noise is not enough for DPA security

- Additive noise $\approx$ cost $\times$ 2 $\Rightarrow$ security $\times$ 2 $\Rightarrow$ not a good (crypto) security parameter
- $\approx$ same holds for all hardware countermeasures
Outline

- Side-channel analysis & the need of masking
- **Boolean masking and the need of noise**
- Prime masking and design challenges

- Fresh re-keying & basic models
- Hard physical learning problems

- General conclusions for symmetric crypto
• Private circuits / probing security [ISW03]

\[ Z = Z_1 \oplus Z_2 \oplus \cdots \oplus Z_{d-1} \oplus Z_d \]

Masking \( \approx \) noise amplification

\[ z = z_1 \oplus z_2 \oplus \cdots \oplus z_{d-1} \oplus z_d \]

• Goal: bounded information \( \text{MI}(Z; L) < \text{MI}(Z_i; L_{Z_i})^d \)
Masking is expensive (e.g., ARM Cortex-M4)

- Multiplications $\approx$ quadratic overheads

$$\begin{bmatrix} a_1 b_1 & a_1 b_2 & a_1 b_3 \\ a_2 b_1 & a_2 b_2 & a_2 b_3 \\ a_3 b_1 & a_3 b_2 & a_3 b_3 \end{bmatrix} + \begin{bmatrix} 0 & r_1 & r_2 \\ -r_1 & 0 & r_3 \\ -r_2 & -r_3 & 0 \end{bmatrix} \Rightarrow \begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix}$$

$\Rightarrow$ Current approach: bitslice ciphers + noise
Boolean masking with noise: OK

\[ \text{MI}(Z; L) \]

- \( d = 6 \)
- \( d = 5 \)
- \( d = 4 \)
- \( d = 3 \)
- \( d = 2 \)
Boolean masking with noise: OK

MI(Z; L)

noise variance

d = 6
- 

d = 5
- 

d = 4
- 

d = 3
- 

d = 2
- 

z = 0

z = 1
Boolean masking with noise: OK

\[
\begin{align*}
\text{MI}(Z; L) & \\
\text{noise variance} & \\
\end{align*}
\]

\[z_1 \rightarrow l_1\]

\[z_2 \rightarrow l_2\]

\[
\begin{array}{c|c|c|c|c}
& 3/8 & 1/4 & 1/8 & 1/8 \\
\hline
3/8 & | & | & | & \\
1/8 & | & | & | & \\
\end{array}
\]

\[
\begin{array}{c|c|c|c|c}
& 0.23 & 0.21 & 0.15 & 0.15 \\
\hline
0.23 & | & | & | & \\
0.15 & | & | & | & \\
\end{array}
\]

\[
\begin{array}{c|c|c|c|c}
& 0 & 0 & 0 & 0 \\
\hline
0 & | & | & | & \\
0 & | & | & | & \\
\end{array}
\]

\[
\begin{array}{c|c|c|c|c}
& 0 & 0 & 0 & 0 \\
\hline
0 & | & | & | & \\
0 & | & | & | & \\
\end{array}
\]
Boolean masking without noise: KO

\[
\begin{align*}
\text{MI}(Z; L) &= \text{noise variance} \\
\end{align*}
\]

\[
\begin{align*}
z_1 &= \begin{cases} 0 & \text{with probability } 1/2 \\ 1/2 & \text{with probability } 1/2 \end{cases} \\
z_2 &= \begin{cases} 1/2 & \text{with probability } 1/2 \\ 0 & \text{with probability } 1/2 \end{cases}
\end{align*}
\]

\[
z = (l_1, l_2)
\]
Noise issue in practice

- Masked bitslice AES implementation
  - ARM Cortex-M0

- ARM Cortex-M3
Outline

• Side-channel analysis & the need of masking
• Boolean masking and the need of noise
• **Prime masking and design challenges**

• Fresh re-keying & basic models
• Hard physical learning problems

• General conclusions for symmetric crypto
Prime masking with noise: OK

$$z_1 = \ldots 0$$

$$z_2 = \ldots 1$$

$$z \leftarrow (l_1, l_2)$$
• Increasing the field size (sometimes) helps
  • Example for Hamming weight leakages
  • And Mersenne primes for efficiency
• Prime computations overheads can be mild
  • In software and hardware implementations

<table>
<thead>
<tr>
<th>Cycle Counts (ARM Cortex-M3):</th>
<th>Resource Utilization (Xilinx Spartan-6):</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Binary Field $\mathbb{F}_{2^n}$</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>$d$</td>
<td>$F_{2^n}$</td>
</tr>
<tr>
<td>2</td>
<td>1321</td>
</tr>
<tr>
<td>3</td>
<td>2902</td>
</tr>
<tr>
<td>4</td>
<td>5213</td>
</tr>
<tr>
<td>5</td>
<td>8255</td>
</tr>
<tr>
<td>6</td>
<td>12038</td>
</tr>
</tbody>
</table>

• Especially if efficient arithmetic operations (in SW) and DSP blocks (in HW) are available
• Theoretical gains are observed in the field
  • Example of attacks against an ARM Cortex-M3

\begin{align*}
x^5 + 2 & \quad \text{in } \mathbb{F}_{2^7} \\
x^5 + 2 & \quad \text{in } \mathbb{F}_{2^7-1}
\end{align*}

• And seem to increase with the # of shares
Conclusions for part #1

- Prime field masking can significantly increase side-channel security in low-noise contexts
- At the cost of manageable overheads
- Gains are maintained in high-noise context!

⇒ Next: show cost vs. security gains for full ciphers
Conclusions for part #1

- Prime field masking can significantly increase side-channel security in low-noise contexts.
- At the cost of manageable overheads.
- Gains are maintained in high-noise context!

⇒ Next: show cost vs. security gains for full ciphers.

- This requires ciphers adapted to prime masking:
  - $2^7 - 1$ for hardware, $2^{31} - 1$ for software?
  - Taking advantage of secure squaring (CHES 2023)
- To be compared with the best bitslice ciphers.
Conclusions for part #1

• Prime field masking can significantly increase side-channel security in low-noise contexts
• At the cost of manageable overheads
• Gains are maintained in high-noise context!

⇒ Next: show cost vs. security gains for full ciphers

• This requires ciphers adapted to prime masking
  • $2^7 - 1$ for hardware, $2^{31} - 1$ for software?
  • Taking advantage of secure squaring (CHES 2023)
• To be compared with the best bitslice ciphers

• More details this Monday at Eurocrypt 2023
Outline

- Side-channel analysis & the need of masking
- Boolean masking and the need of noise
- Prime masking and design challenges

- **Fresh re-keying & basic models**
  - Hard physical learning problems

- General conclusions for symmetric crypto
• Find a re-keying function that is easy to protect against DPA (e.g., key homomorphic, ...)
• Main question: how to formalize RK security?
Security requirements

- Avoiding attack path #1 is well understood
- Avoiding attack path #2 much less (≠ models)
Model 1: Medwed et al.

- Noisy leakages
- Proposed instance
  - $k^* = r \cdot k$ over $\mathbb{F}_{2^\kappa}$
  - Key homomorphic
- Efficient but insecure w/o noise

- Somewhat similar to Boolean masking
  - LSB of Hamming weight leakage is linear in $\mathbb{F}_{2^\kappa}$
Model 2: Dziembowsk{e} et al.

- Unbounded leakages on $k^*$
- Proposed instance (wPRF)
  - $k^* = \langle r, k \rangle_p$, with $k, r \in \mathbb{Z}_{2q}^n$
  - Nearly key-homomorphic
  $\Rightarrow$ Needs $\log(d)$ bits of error correction

- Very large key requirements
  - Poor performances in software & hardware
Outline

• Side-channel analysis & the need of masking
• Boolean masking and the need of noise
• Prime masking and design challenges
• Fresh re-keying & basic models
• **Hard physical learning problems**
• General conclusions for symmetric crypto
• Noise-free (compressive) leakages
• Similar to “crypto dark matter”
  • \( F_K(r) = \text{map}(r \cdot K) \)
  \( \approx \) security by combining different fields
• But assumes a physical mapping \( L \)
  \( \Rightarrow \) Crypto-physical dark matter
Model 3: Duval et al.

- Noise-free (compressive) leakages
- Similar to “crypto dark matter”
  - $F_K(r) = \text{map}(r \cdot K)$
  - ≈ security by combining different fields
- But assumes a physical mapping $L$
  - $\Rightarrow$ Crypto-physical dark matter

- Interest for re-keying: $L$ never has to be computed explicitly by the leaking device (and therefore masked), the physics does it
- Challenge: $L$ is not controlled by the designer
Learning with Physical Rounding (LWPR)

- Adv. gets samples $(\mathbf{r}, L(K \cdot (\mathbf{r}, \mathbf{1})))$ with $\mathbf{r} \in \mathbb{F}_p^n$ and $K \in \mathbb{F}_p^{m \times (n+1)}$ and tries to recover $K$

- Requires an embedding $g: \mathbb{F}_p \to \{0,1\}^{\log(p)}$

- And a physical assumption on the mapping $L$
• Adv. gets samples \((r, L(K \cdot (r, 1)))\) with \(r \in \mathbb{F}_p^n\) and \(K \in \mathbb{F}_p^{m \times (n+1)}\) and tries to recover \(K\)

• Requires an embedding \(g: \mathbb{F}_p \rightarrow \{0,1\}^{\lfloor \log(p) \rfloor}\)

• And a physical assumption on the mapping \(L\)

• CHES 2021: Hamming weight (HW) assumption
  • First instance: \(m = 4, n = 4, p = 2^{31} - 1\)
  • Parallel implem.: if \(k_i^* = K \cdot (r, 1)\), adversary gets \(\text{HW}(g(k_1^*)) + \text{HW}(g(k_2^*)) + \text{HW}(g(k_3^*)) + \text{HW}(g(k_4^*))\)
  • Lower bound on algebraic degree and degree-1 approximations in \(\mathbb{F}_p\), MELP/MEDP in \(\mathbb{F}_2\)
Hardware implementation results

- 128-bit FPGA implementation

![Graph showing latency and data complexity vs. number of shares](image-url)
Conclusions for part #2

- Other advantages (improved security against glitches, ...)

**Glitch-extended probes:** probing any output of a combinatorial sub-circuit allows the adversary to observe all the sub-circuit inputs

Example: $p_1$ gives $a$, $b$ and $c$
Conclusions for part #2

- Other advantages (improved security against glitches, trivial composition, linear refreshing)
Conclusions for part #2

• Other advantages (improved security against glitches, trivial composition, linear refreshing)

• If secure, game changer for embedded security

• Concrete relevance requires generalization
  • From Hamming weight leakages to linear, ...
  • From univariate to multivariate leakages
  • Will possibly require noise again!
  • Or considering errors in measurements
Conclusions for part #2

• Other advantages (improved security against glitches, trivial composition, linear refreshing)
• If secure, game changer for embedded security
• Concrete relevance requires generalization
  • From Hamming weight leakages to linear, ...
  • From univariate to multivariate leakages
  • Will possibly require noise again!
    • Or considering errors in measurements
• Also raises important theoretical challenges
  • Learning with Leakage reduces to LPN
  • What about LWPR, LWPE? Can we connect them?
Outline

• Side-channel analysis & the need of masking
• Boolean masking and the need of noise
• Prime masking and design challenges

• Fresh re-keying & basic models
• Hard physical learning problems

• General conclusions for symmetric crypto
General conclusions

• The reduced “compatibility” between physical leakages and prime computations is a source of improved security for masking & re-keying
• Yet the meaning of “compatible” differs for both
General conclusions

• The reduced “compatibility” between physical leakages and prime computations is a source of improved security for masking & re-keying
  • Yet the meaning of “compatible” differs for both

• Leakage in symmetric crypto so far drove
  • Bitslice primitives with low AND complexity
  • Modes of operation for levelled implementations

• Could also drive new (prime) ciphers & the integration of hard physical learning problems in modes of operation (with the same primes?)
General conclusions

• The reduced “compatibility” between physical leakages and prime computations is a source of improved security for masking & re-keying
  • Yet the meaning of “compatible” differs for both

• Leakage in symmetric crypto so far drove
  • Bitslice primitives with low AND complexity
  • Modes of operation for levelled implementations

• Could also drive new (prime) ciphers & the integration of hard physical learning problems in modes of operation (with the same primes?)

• Both have application in PQ asymmetric crypto!
THANKS!

https://perso.uclouvain.be/fstandae/

We are hiring on these topics
Proposition 3 (Properties of $s$-bounded pseudo-linear functions). Let $f \in C_1^s$ with $ts < p$, where $t = \lceil \log p \rceil$, then the following holds:

- $v_f \geq \lceil \frac{p}{ts+1} \rceil$,
- $w_f \geq p - ts - 1$.

And assuming $v_f \neq p$, we further have:

- $\text{deg}(f) \geq \lceil \frac{p}{ts+1} \rceil$,
- $\text{nl}(f) \geq \min \left( p - v_f, \max \left( \left\lceil \frac{p}{ts+1} \right\rceil - 1, p - ts - 1 \right) \right)$.