Multiplicative Masking for AES in Hardware

CHES 2018
Lauren De Meyer, Oscar Reparaz, Begül Bilgin
PROBLEM: SIDE-CHANNEL ANALYSIS
SOLUTION: MASKING
EXTRA PROBLEM: GLITCHES!
 BOOLEAN MASKING

\[ x = (x_0, x_1, \ldots, x_d) \iff x = \sum_i x_i \]

Tricky: Nonlinear functions
MUSEUM OF CRYPTO ART

Moradi et al.

Bilgin et al.

De Cnudde et al.

Gross et al.
Our Result:

• 1st order S-box:
  0.71x

• 2nd order S-box:
  0.82x
How?
BACK TO THE BEGINNING
BACK TO THE BEGINNING

Akkar-Giraud 2001

SubBytes

Boolean → Multiplicative

Multiplicative → Boolean

ShiftRows

MixColumns

AddRoundKey

Genelle et al. 2010
The Zero Problem

$$0 = (x_0, x_1, ..., x_d) \iff 0 = \prod_{i} x_i$$

$$x_i = 0$$
\[ \delta(x) = \begin{cases} 1 & \text{if } x = 0 \\ 0 & \text{if } x \neq 0 \end{cases} \]
Masked GF Inversion

boolean to multiplicative
local inversion
multiplicative to boolean

$\delta(x)$
MASKED GF INVERSION

\[ \delta(x) \]

(Boolean to Multiplicative) \rightarrow (Local Inversion) \rightarrow (Multiplicative to Boolean)
**FIRST-ORDER MASKED CONVERSIONS**

\[ x = A \oplus B \]

- \( b_0 \rightarrow B \)
- \( b_1 \rightarrow A \)
FIRST-ORDER MASKED CONVERSIONS

$$x = C^{-1} \cdot (A \oplus B)$$

1. Expansion
FIRST-ORDER MASKED CONVERSIONS

$x = C^{-1} \cdot (A \oplus B)$

2. Synchronization
FIRST-ORDER MASKED CONVERSIONS

\[ x = C^{-1} \cdot B \]

3. Compression
First-Order Masked Conversions

\[ x = C^{-1} \cdot B \quad \iff \quad x^{-1} = C \cdot B^{-1} \]

3. Compression
FIRST-ORDER MASKED CONVERSIONS

\[ x = C^{-1} \cdot B \quad \iff \quad x^{-1} = C \cdot B^{-1} \]
FIRST-ORDER MASKED CONVERSIONS

\[ x^{-1} = C \cdot (D \oplus E) \]

1. Expansion
FIRST-ORDER MASKED CONVERSIONS

\[ x^{-1} = C \cdot (D \oplus E) \]

2. Synchronization
FIRST-ORDER MASKED CONVERSIONS

\[ x^{-1} = D \oplus E \]

3. Compression
SECOND-ORDER MASKED CONVERSIONS

\[ p_0 = q_0 \]

\[ p_1 = q_1 \]

\[ p_2^{-1} = q_2 \]
SECOND-ORDER MASKED CONVERSIONS

Extra Remasking Required
Second-Order Masked Conversions

Still only 1 inversion!

Extra Remaskng Required
MASKED GF INVERSION

\[ \delta(x) \]

Boolean to Multiplicative

Local Inversion

Multiplicative to Boolean
**Masked Kronecker Delta**

\[
\delta(x) = \overline{x_0} \, x_1 \, \overline{x_2} \, x_3 \, \overline{x_4} \, x_5 \, \overline{x_6} \, x_7
\]
AN INTERESTING OBSERVATION

\[ C_1 = A_1B_1 \oplus A_1B_2 \oplus R \]
\[ = A_1B \]

\[ C_2 = A_2B \oplus R \]
Masked Kronecker Delta

Independent of $r_2$

Independent of $r_4$
Masked Kronecker Delta

\[ \overline{x_0} \rightarrow r_1 \]
\[ \overline{x_1} \rightarrow r_2 \]
\[ \overline{x_2} \rightarrow r_2 \]
\[ \overline{x_3} \rightarrow r_1 \]
\[ \overline{x_4} \rightarrow r_1 \]
\[ \overline{x_5} \rightarrow r_2 \]
\[ \overline{x_6} \rightarrow r_2 \]
\[ \overline{x_7} \rightarrow r_1 \]

\[ \delta(x) \]
MASKED KRONECKER DELTA
MASKED GF INVERSION

- No registers
- Precompute

δ(x)

Boolean to Multiplicative

Local Inversion

Multiplicative to Boolean
RESULTS
**S-box Area**

- **1\textsuperscript{st} order:**
  - 0.71x

- **2\textsuperscript{nd} order:**
  - 0.82x

<table>
<thead>
<tr>
<th></th>
<th>De Cnudde et al. 2016</th>
<th>Gross et al. 2017</th>
<th>This Work 2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>1\textsuperscript{st} order</td>
<td>2348 GE</td>
<td>2432 GE</td>
<td>1685 GE</td>
</tr>
<tr>
<td>2\textsuperscript{nd} order</td>
<td>4744 GE</td>
<td>4759 GE</td>
<td>3891 GE</td>
</tr>
</tbody>
</table>
**AES Area**

- **1st order:**
  - 0.89x

- **2nd order:**
  - 0.91x
RANDOMNESS PER S-BOX

• 1st order:

- De Cnudde et al. 2016: 54
- Gross et al. 2017: 18
- This Work 2018: 19

• 2nd order:

- De Cnudde et al. 2016: 162
- Gross et al. 2017: 54
- This Work 2018: 53
Latency per Encryption

De Cnudde et al. 2016
Gross et al. 2017
This Work 2018

# clock cycles

276
246
256
TVLA: 1\textsuperscript{ST} ORDER AES

First Order

Second Order
TVLA: 2\textsuperscript{ND} ORDER AES

First Order

Third Order
TVLA: BIVARIATE
Take-Away

✓ Keep it Simple 😊
✓ Find inspiration in early works
✓ Push the limits:
  ✓ Reuse Randomness
  ✓ Customize!
A CRYPTO NERD'S IMAGINATION:

 HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.

 NO GOOD! IT'S 4096-BIT RSA!

 BLAST! OUR EVIL PLAN IS FOILED!

WHAT WOULD ACTUALLY HAPPEN:

 HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.

 GOT IT.

Thank You