High Order Masking of Look-up Tables with Common Shares
J-S. Coron, F. Rondepierre, R. Zeitoun

12th September 2018
Outline

1 Introduction
   1st Order Solution
   Higher Order Masking of Look-Up Tables

2 Higher Order: Optimizations

3 Conclusion
1 Introduction
   1st Order Solution
   Higher Order Masking of Look-Up Tables

2 Higher Order: Optimizations

3 Conclusion
SCA Countermeasure

Sharing Principle

- Given a sensitive data $x$
- Given $t$ random values $x_1, \ldots, x_t$
- Let $x_0$ be such that:

$$x = \bigoplus_{i=0}^{t} x_i$$

- $(x_0, \ldots, x_t)$ is a sharing of $x$ secure at order $t$
SBox Evaluation

The problematic

- Given sensitive data \( x \)
- Given a known table \( S \)
- How to compute securely:

\[ x \mapsto S(x) \]
SBox Evaluation

The problematic

- Given sensitive data $x$
- Given a known table $S$
- How to compute securely for $\ell$ evaluations:

$$x^{(\ell)} \mapsto S(x^{(\ell)})$$
Secure at 1st Order

The $\ell$-th evaluation of $S$ is:

$$x^{(\ell)} = (x_0^{(\ell)}, m) \mapsto S(x^{(\ell)}) = (y_0^{(\ell)}, m)$$
Masked SBox Construction

\[ T = \begin{cases} 
S(0 \oplus m) \oplus m \\
\vdots \\
S((2^k - 1) \oplus m) \oplus m
\end{cases} \]

Masked SBox Evaluation

\[ S(x) = (T(x_0), m) \]
Higher Order

Secure at Higher Order (Coron EUROCRYPT’14)

The $\ell$-th evaluation of $S$ is:

$$x^{(\ell)} = (x_0^{(\ell)}, x_1^{(\ell)}, \ldots, x_{2t}^{(\ell)}) \mapsto S(x^{(\ell)}) = (y_0^{(\ell)}, y_1^{(\ell)}, \ldots, y_{2t}^{(\ell)})$$
Example at 3rd Order

\[ x = 2 = (0, 1, 1, 2) \]

\[
\begin{cases}
S(0) & 0 & 0 & 0 \\
S(1) & 0 & 0 & 0 \\
S(2) & 0 & 0 & 0 \\
S(3) & 0 & 0 & 0
\end{cases}
\]
Higher Order

Example at 3rd Order

\[ x = 2 = (0, 1, 1, 2) \]

\[
\begin{pmatrix}
S(2) & 0 & 0 & 0 \\
S(3) & 0 & 0 & 0 \\
S(0) & 0 & 0 & 0 \\
S(1) & 0 & 0 & 0
\end{pmatrix}
\]
Higher Order

Example at 3rd Order

\[ x = 2 = (0, 1, 1, 2) \]

\[
\begin{cases}
\begin{array}{cccc}
S(2) & \oplus & 3 & 1 & 2 & 0 \\
S(3) & \oplus & 1 & 0 & 0 & 1 \\
S(0) & \oplus & 0 & 2 & 3 & 1 \\
S(1) & \oplus & 0 & 0 & 0 & 0
\end{array}
\end{cases}
\]
Higher Order

Example at 3rd Order

\[ x = 2 = (0, 1, 1, 2) \]

\[
\begin{align*}
S(2) \oplus 3 & \quad 1 \quad 2 \quad 0 \\
S(3) \oplus 1 & \quad 0 \quad 0 \quad 1 \\
S(0) \oplus 0 & \quad 2 \quad 3 \quad 1 \\
S(1) \oplus 0 & \quad 0 \quad 0 \quad 0
\end{align*}
\]

\[ \Rightarrow \]

\[
\begin{align*}
S(3) \oplus 1 & \quad 0 \quad 0 \quad 1 \\
S(2) \oplus 3 & \quad 1 \quad 2 \quad 0 \\
S(1) \oplus 0 & \quad 0 \quad 0 \quad 0 \\
S(0) \oplus 0 & \quad 2 \quad 3 \quad 1
\end{align*}
\]
Example at 3rd Order

\[ x = 2 = (0, 1, 1, 2) \]

\[
\begin{align*}
S(3) &\;\oplus\; 1 & 1 & 2 & 2 \\
S(2) &\;\oplus\; 1 & 0 & 2 & 3 \\
S(1) &\;\oplus\; 3 & 2 & 1 & 0 \\
S(0) &\;\oplus\; 0 & 1 & 0 & 1
\end{align*}
\]
Higher Order

Example at 3rd Order

\[ x = 2 = (0, 1, 1, 2) \]

\[
\begin{align*}
\{ S(2) \oplus 1 & \quad 0 & 2 & 3 \\
S(3) \oplus 1 & \quad 1 & 2 & 2 \\
S(0) \oplus 0 & \quad 1 & 0 & 1 \\
S(1) \oplus 3 & \quad 2 & 1 & 0 \\
\end{align*}
\]
Higher Order

Example at 3rd Order

\[ x = 2 = (0, 1, 1, 2) \]

\[
\begin{align*}
S(2) \oplus 2 & \quad 2 & \quad 2 & \quad 2 \\
S(3) \oplus 1 & \quad 1 & \quad 2 & \quad 2 \\
S(0) \oplus 1 & \quad 1 & \quad 1 & \quad 1 \\
S(1) \oplus 3 & \quad 3 & \quad 3 & \quad 3
\end{align*}
\]
Higher Order

Example at 3rd Order

\[ x = 2 = (0, 1, 1, 2) \]

\[ S(2) \oplus 2 \ 2 \ 2 \ 2 \]
Higher Order

Example at 3rd Order

\[ x = 2 = (0, 1, 1, 2) \]

\[ S(2) \oplus 0 \quad 1 \quad 2 \quad 3 \]
Higher Order

Masked SBox Construction (Coron EUROCRYPT’14)

\[ T^{(0)} = \left\{ \begin{array}{l}
\text{sharing of } S(0) \\
\vdots \\
\text{sharing of } S(2^k - 1)
\end{array} \right\} \]
Higher Order

Masked SBox Construction (Coron EUROCRYPT’14)

\[ T^{(1)} = \begin{cases} 
\text{new sharing of } T^{(0)}(0 \oplus x_{2t}) \\
\vdots \\
\text{new sharing of } T^{(0)}((2^k - 1) \oplus x_{2t}) 
\end{cases} \]
Higher Order

Masked SBox Construction (Coron EUROCRYPT’14)

\[ T^{(2)} = \begin{cases} 
\text{new sharing of } T^{(1)}(0 \oplus x_{2t-1}) \\
\vdots \\
\text{new sharing of } T^{(1)}((2^k - 1) \oplus x_{2t-1}) 
\end{cases} \]
Higher Order

Masked SBox Construction (Coron EUROCRYPT’14)

\[ T^{(2t)} = \begin{cases} 
\text{new sharing of } T^{(2t-1)}(0 \oplus x_1) \\
\vdots \\
\text{new sharing of } T^{(2t-1)}((2^k - 1) \oplus x_1) 
\end{cases} \]
Higher Order

Masked SBox Construction (Coron EUROCRYPT’14)

\[
T^{(2^t)} = \begin{cases} 
\text{new sharing of } T^{(2^t - 1)}(0 \oplus x_1) \\
\vdots \\
\text{new sharing of } T^{(2^t - 1)}((2^k - 1) \oplus x_1)
\end{cases}
\]

Masked SBox Evaluation

\[
S(x) = \text{new sharing of } T^{(t)}(x_0)
\]
Table of Contents

1 Introduction
   1st Order Solution
   Higher Order Masking of Look-Up Tables

2 Higher Order: Optimizations

3 Conclusion
Contributions

Our Contributions

- Security proof at order $t$ with $n = t + 1$ shares instead of $n = 2t + 1$ shares (t-sni formalism)
  - Saves a factor 4 (running time)
- A variant with increasing number of output shares
  - Saves a factor 2 (running time)
- Adapt the common shares technique for multiple SBox evaluations
  - Saves a factor 2 (running time)
Two values $a$ and $b$ may be securely shared such that at most half of the shares are common:

\[
\left( a_0, \ldots, a_{\frac{t}{2}}, m_0, \ldots, m_{\frac{t-1}{2}} \right)
\]

\[
\left( b_0, \ldots, b_{\frac{t}{2}}, m_0, \ldots, m_{\frac{t-1}{2}} \right)
\]
Look-Up Tables with Common Shares

Secure at Higher Order

The $\ell$-th evaluation of $S$ is:

$$(x_0^{(\ell)}, x_1^{(\ell)}, \ldots, x_t^{(\ell)}, m_0, \ldots, m_{t-1}) \mapsto S(x^{(\ell)}) = (y_0^{(\ell)}, y_1^{(\ell)}, \ldots, y_t^{(\ell)})$$
Look-Up Tables with Common Shares

Masked SBox Construction (Common Table)

\[
T^{(0)} = \begin{cases} 
\text{sharing of } S(0) \\
\vdots \\
\text{sharing of } S(2^k - 1) 
\end{cases}
\]
Look-Up Tables with Common Shares

Masked SBox Construction (Common Table)

\[ T^{(1)} = \left\{ \begin{array}{c}
\text{new sharing of } T^{(0)}(0 \oplus m_0) \\
\vdots \\
\text{new sharing of } T^{(0)}((2^k - 1) \oplus m_0)
\end{array} \right\} \]
Look-Up Tables with Common Shares

Masked SBox Construction (Common Table)

\[ T^{(2)} = \begin{cases} 
\text{new sharing of } T^{(1)}(0 \oplus m_1) \\
\vdots \\
\text{new sharing of } T^{(1)}((2^k - 1) \oplus m_1) 
\end{cases} \]
Look-Up Tables with Common Shares

Masked SBox Construction (Common Table)

\[ T^{\left(\frac{t+1}{2}\right)} = \begin{cases} 
\text{new sharing of } T^{\left(\frac{t-1}{2}\right)}(0 \oplus m_{\frac{t-1}{2}}) \\
\vdots \\
\text{new sharing of } T^{\left(\frac{t-1}{2}\right)}((2^k - 1) \oplus m_{\frac{t-1}{2}}) 
\end{cases} \]
Look-Up Tables with Common Shares

Masked SBox Construction (Common Table)

\[ T^{(t+1)/2} = \left\{ \begin{array}{l}
\text{new sharing of } T^{(t-1)/2}(0 \oplus m_{t-1}/2) \\
\vdots \\
\text{new sharing of } T^{(t-1)/2}((2^k - 1) \oplus m_{t-1}/2) \\
\end{array} \right\} \]

Masked SBox Evaluation

1. Compute tables \( T^{(t+3)/2}, \ldots, T^{(t)} \) using shares \( x_1, \ldots, x_{t/2} \)
2. Evaluate using table \( T^{(t)} \):

\[ S(x) = \text{new sharing of } T^{(t)}(x_0) \]
## Performances

### AES

<table>
<thead>
<tr>
<th>SBox Implementation</th>
<th>2</th>
<th>3</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>[RP10]</td>
<td>119</td>
<td>185</td>
<td>485</td>
</tr>
<tr>
<td>[Cor14]</td>
<td>2104</td>
<td>4413</td>
<td>17136</td>
</tr>
<tr>
<td>All optimizations</td>
<td>463</td>
<td>771</td>
<td>2767</td>
</tr>
</tbody>
</table>

*Table: Software AES implementation, in thousand of clock cycles*

### DES

<table>
<thead>
<tr>
<th>SBox Implementation</th>
<th>2</th>
<th>3</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>[CGP+12]+[CRV14]</td>
<td>219</td>
<td>290</td>
<td>602</td>
</tr>
<tr>
<td>[Cor14]</td>
<td>491</td>
<td>907</td>
<td>3075</td>
</tr>
<tr>
<td>All optimizations</td>
<td>203</td>
<td>308</td>
<td>764</td>
</tr>
</tbody>
</table>

*Table: Software DES implementation, in thousand of clock cycles*
Table of Contents

1 Introduction
   1st Order Solution
   Higher Order Masking of Look-Up Tables

2 Higher Order: Optimizations

3 Conclusion
Conclusion

- Generalization of SBox recomputation, proven secure at any order
- Reduce the running time of common table by a factor of 2
- Reduce the running time by a factor of 8 (from Coron’14)
- Remaining task: build a proof to generalize common shares in outputs

\[(x_0^{(\ell)}, x_1^{(\ell)}, \ldots, x_{\frac{\ell}{2}}^{(\ell)}, m_0, \ldots, m_{\frac{\ell-1}{2}}) \mapsto S(x^{(\ell)}) = (y_0^{(\ell)}, y_1^{(\ell)}, \ldots, y_{\frac{\ell}{2}}^{(\ell)}, m_0, \ldots, m_{\frac{\ell-1}{2}})\]

- Correct solution for generic small SBox (e.g. DES)