High Order Masking of Look-up Tables with Common Shares

J-S.Coron, F.Rondepierre, R.Zeitoun

IDEMIA

UNIVERSITÉ DU LUXEMBOURG

12th September 2018

Outline

Table of Contents

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 ℓ evaluations:

$$x^{(\ell)} \mapsto S(x^{(\ell)})$$

1st Order

Secure at 1st Order

The ℓ-th evaluation of S is:

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

1st Order

Masked SBox Construction

$$T = \left\{ \begin{array}{c} S(0 \oplus m) \oplus m \\ \vdots \\ S((2^k - 1) \oplus m) \oplus m \end{array} \right\}$$

Masked SBox Evaluation

$$S(x) = (T(x_0), m)$$

Higher Order

Secure at Higher Order (Coron EUROCRYPT'14)

The ℓ-th evaluation of S is:

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

Higher Order

Example at 3rd Order

$x = 2 = (0, 1, 1, 2)$

$$\begin{Bmatrix} S(0) & 0 & 0 & 0 \\ S(1) & 0 & 0 & 0 \\ S(2) & 0 & 0 & 0 \\ S(3) & 0 & 0 & 0 \end{Bmatrix}$$

Higher Order

Example at 3rd Order

$x = 2 = (0, 1, 1, \mathbf{2})$

$$\begin{Bmatrix} S(2) & 0 & 0 & 0 \\ S(3) & 0 & 0 & 0 \\ S(0) & 0 & 0 & 0 \\ S(1) & 0 & 0 & 0 \end{Bmatrix}$$

Higher Order

Example at 3rd Order

$x = 2 = (0, 1, 1, 2)$

$$\begin{Bmatrix} S(2) \oplus 3 & 1 & 2 & 0 \\ S(3) \oplus 1 & 0 & 0 & 1 \\ S(0) \oplus 0 & 2 & 3 & 1 \\ S(1) \oplus 0 & 0 & 0 & 0 \end{Bmatrix}$$

Higher Order

Example at 3rd Order

$x = 2 = (0, 1, \mathbf{1}, 2)$

$$\begin{Bmatrix} S(2) \oplus 3 & 1 & 2 & 0 \\ S(3) \oplus 1 & 0 & 0 & 1 \\ S(0) \oplus 0 & 2 & 3 & 1 \\ S(1) \oplus 0 & 0 & 0 & 0 \end{Bmatrix} \Longrightarrow \begin{Bmatrix} S(3) \oplus 1 & 0 & 0 & 1 \\ S(2) \oplus 3 & 1 & 2 & 0 \\ S(1) \oplus 0 & 0 & 0 & 0 \\ S(0) \oplus 0 & 2 & 3 & 1 \end{Bmatrix}$$

Higher Order

Example at 3rd Order

$x = 2 = (0, 1, 1, 2)$

$$\left\{\begin{matrix} S(3) \oplus 1 & 1 & 2 & 2 \\ S(2) \oplus 1 & 0 & 2 & 3 \\ S(1) \oplus 3 & 2 & 1 & 0 \\ S(0) \oplus 0 & 1 & 0 & 1 \end{matrix}\right\}$$

Higher Order

Example at 3rd Order

$x = 2 = (0, \mathbf{1}, 1, 2)$

$$\left\{\begin{matrix} S(2) \oplus 1 & 0 & 2 & 3 \\ S(3) \oplus 1 & 1 & 2 & 2 \\ S(0) \oplus 0 & 1 & 0 & 1 \\ S(1) \oplus 3 & 2 & 1 & 0 \end{matrix}\right\}$$

Higher Order

Example at 3rd Order

$x = 2 = (0, 1, 1, 2)$

$$\left\{\begin{matrix} S(2) \oplus 2 & 2 & 2 & 2 \\ S(3) \oplus 1 & 1 & 2 & 2 \\ S(0) \oplus 1 & 1 & 1 & 1 \\ S(1) \oplus 3 & 3 & 3 & 3 \end{matrix}\right\}$$

Higher Order

Example at 3rd Order

$x = 2 = (\mathbf{0}, 1, 1, 2)$

$$S(2) \oplus 2 \quad 2 \quad 2 \quad 2$$

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)

$$T^{(0)} = \left\{ \begin{array}{c} \text{sharing of } S(0) \\ \vdots \\ \text{sharing of } S(2^k - 1) \end{array} \right\}$$

Higher Order

Masked SBox Construction (Coron EUROCRYPT'14)

$$T^{(1)} = \left\{ \begin{array}{c} \text{new sharing of } T^{(0)}(0 \oplus \mathbf{x_{2t}}) \\ \vdots \\ \text{new sharing of } T^{(0)}((2^k - 1) \oplus \mathbf{x_{2t}}) \end{array} \right\}$$

Higher Order

Masked SBox Construction (Coron EUROCRYPT'14)

$$T^{(2)} = \left\{ \begin{array}{c} \text{new sharing of } T^{(1)}(0 \oplus \mathbf{x_{2t-1}}) \\ \vdots \\ \text{new sharing of } T^{(1)}((2^k - 1) \oplus \mathbf{x_{2t-1}}) \end{array} \right\}$$

Higher Order

Masked SBox Construction (Coron EUROCRYPT'14)

$$T^{(2t)} = \left\{ \begin{array}{c} \text{new sharing of } T^{(2t-1)}(0 \oplus \mathbf{x_1}) \\ \vdots \\ \text{new sharing of } T^{(2t-1)}((2^k - 1) \oplus \mathbf{x_1}) \end{array} \right\}$$

Higher Order

Masked SBox Construction (Coron EUROCRYPT'14)

$$T^{(2t)} = \left\{ \begin{array}{c} \text{new sharing of } T^{(2t-1)}(0 \oplus \mathbf{x_1}) \\ \vdots \\ \text{new sharing of } T^{(2t-1)}((2^k - 1) \oplus \mathbf{x_1}) \end{array} \right\}$$

Masked SBox Evaluation

$$S(x) = \text{new sharing of } T^{(t)}(x_0)$$

Table of Contents

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)

Common Shares

Common Shares (CGPZ CHES16)

Two values a and b may be securely shared such that at most half of the shares are common:

$$(a_0, \ldots, a_{\frac{t}{2}}, m_0, \ldots m_{\frac{t-1}{2}})$$
$$(b_0, \ldots, b_{\frac{t}{2}}, m_0, \ldots m_{\frac{t-1}{2}})$$

Look-Up Tables with Common Shares

Secure at Higher Order

The ℓ-th evaluation of S is:

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

Look-Up Tables with Common Shares

Masked SBox Construction (Common Table)

$$T^{(0)} = \left\{ \begin{array}{c} \text{sharing of } S(0) \\ \vdots \\ \text{sharing of } S(2^k - 1) \end{array} \right\}$$

Look-Up Tables with Common Shares

Masked SBox Construction (Common Table)

$$T^{(1)} = \left\{ \begin{array}{c} \text{new sharing of } T^{(0)}(0 \oplus \mathbf{m_0}) \\ \vdots \\ \text{new sharing of } T^{(0)}((2^k - 1) \oplus \mathbf{m_0}) \end{array} \right\}$$

Look-Up Tables with Common Shares

Masked SBox Construction (Common Table)

$$T^{(2)} = \left\{ \begin{array}{c} \text{new sharing of } T^{(1)}(0 \oplus \mathbf{m_1}) \\ \vdots \\ \text{new sharing of } T^{(1)}((2^k - 1) \oplus \mathbf{m_1}) \end{array} \right\}$$

Look-Up Tables with Common Shares

Masked SBox Construction (Common Table)

$$T^{(\frac{t+1}{2})} = \left\{ \begin{array}{c} \text{new sharing of } T^{(\frac{t-1}{2})}(0 \oplus \mathbf{m}_{\frac{t-1}{2}}) \\ \vdots \\ \text{new sharing of } T^{(\frac{t-1}{2})}((2^k - 1) \oplus \mathbf{m}_{\frac{t-1}{2}}) \end{array} \right\}$$

Look-Up Tables with Common Shares

Masked SBox Construction (Common Table)

$$T^{\left(\frac{t+1}{2}\right)} = \left\{ \begin{array}{c} \text{new sharing of } T^{\left(\frac{t-1}{2}\right)}(0 \oplus \mathbf{m}_{\frac{t-1}{2}}) \\ \vdots \\ \text{new sharing of } T^{\left(\frac{t-1}{2}\right)}((2^k - 1) \oplus \mathbf{m}_{\frac{t-1}{2}}) \end{array} \right\}$$

Masked SBox Evaluation

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

$$S(x) = \text{new sharing of } T^{(t)}(x_0)$$

Performances

AES

SBox Implementation	2	3	6
[RP10]	119	185	485
[Cor14]	2104	4413	17136
All optimizations	463	771	2767

Table: Software AES implementation, in thousand of clock cycles

DES

SBox Implementation	2	3	6
[CGP+12]+[CRV14]	219	290	602
[Cor14]	491	907	3075
All optimizations	203	308	764

Table: Software DES implementation, in thousand of clock cycles

Table of Contents

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

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

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