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







### Outline

Outline

1 Introduction1st Order SolutionHigher Order Masking of Look-Up Tables

**2** Higher Order: Optimizations

3 Conclusion



#### **Table of Contents**

Introduction

1 Introduction1st Order SolutionHigher Order Masking of Look-Up Tables



2 Higher Order: Optimizations



3 Conclusion



#### **Sharing Principle**

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

$$\mathbf{x} = \bigoplus_{i=0}^{l} \mathbf{x}$$

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

#### The problematic

- Given sensitive data x
- Given a known table 5
- How to compute securely :

 $x \mapsto S(x)$ 



#### The problematic

- Given sensitive data x
- Given a known table 5
- 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

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



#### Secure at Higher Order (Coron EUROCRYPT'14)

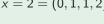
The  $\ell$ -th evaluation of S is:

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



Introduction

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



$$S(1) \quad 0 \quad 0$$



Introduction

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



$$(S(2) \ 0 \ 0)$$

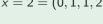


Introduction

# Example at 3rd Order

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

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





# Introduction

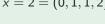
$$x = 2 = (0, 1, 1, 2)$$

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



Introduction

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



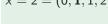






Introduction

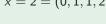
$$x = 2 = (0, 1, 1, 2)$$





Introduction

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







Introduction

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





Introduction

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





$$T^{(0)} = \left\{ egin{array}{l} ext{sharing of } S(0) \ dots \ ext{sharing of } S(2^k-1) \end{array} 
ight\}$$



Introduction

$$\mathcal{T}^{(1)} = \left\{ egin{array}{ll} \mathsf{new sharing of} \ \mathcal{T}^{(0)}(0 \oplus \mathsf{x_{2t}}) \ &dots \ \mathsf{new sharing of} \ \mathcal{T}^{(0)}((2^k-1) \oplus \mathsf{x_{2t}}) \end{array} 
ight\}$$



Introduction

$$\mathcal{T}^{(2)} = \left\{ egin{array}{ll} \mathsf{new \ sharing \ of} \ \mathcal{T}^{(1)}(0 \oplus \mathsf{x_{2t-1}}) \ dots \ \mathsf{new \ sharing \ of} \ \mathcal{T}^{(1)}((2^k-1) \oplus \mathsf{x_{2t-1}}) \end{array} 
ight\}$$



Introduction

$$\mathcal{T}^{(2t)} = \left\{egin{array}{l} \mathsf{new} \; \mathsf{sharing} \; \mathsf{of} \; \mathcal{T}^{(2t-1)}(\mathsf{0} \oplus \mathsf{x_1}) \ dots \ \mathsf{new} \; \mathsf{sharing} \; \mathsf{of} \; \mathcal{T}^{(2t-1)}((2^k-1) \oplus \mathsf{x_1}) \end{array}
ight\}$$



Introduction

## Masked SBox Construction (Coron EUROCRYPT'14)

$$\mathcal{T}^{(2t)} = \left\{ egin{array}{l} \mathsf{new} \; \mathsf{sharing} \; \mathsf{of} \; \mathcal{T}^{(2t-1)}(\mathsf{0} \oplus \mathsf{x_1}) \ dots \ \mathsf{new} \; \mathsf{sharing} \; \mathsf{of} \; \mathcal{T}^{(2t-1)}((2^k-1) \oplus \mathsf{x_1}) \end{array} 
ight\}$$

#### Masked SBox Evaluation

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



#### **Table of Contents**

Higher Order: Optimizations

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

**2** Higher Order: Optimizations

3 Conclusion

#### 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 (CGPZ CHES16)

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

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

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



Higher Order: Optimizations

#### Secure at Higher Order

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

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



Higher Order: Optimizations

$$T^{(0)} = \left\{ egin{array}{l} ext{sharing of } S(0) \ dots \ ext{sharing of } S(2^k-1) \end{array} 
ight\}$$



Higher Order: Optimizations

$$\mathcal{T}^{(1)} = \left\{ egin{array}{ll} \mathsf{new} \; \mathsf{sharing} \; \mathsf{of} \; \mathcal{T}^{(0)}(0 \oplus \mathbf{m_0}) \ & dots \ \mathsf{new} \; \mathsf{sharing} \; \mathsf{of} \; \mathcal{T}^{(0)}((2^k-1) \oplus \mathbf{m_0}) \end{array} 
ight\}$$



Higher Order: Optimizations

$$\mathcal{T}^{(2)} = \left\{egin{array}{ll} \mathsf{new} \; \mathsf{sharing} \; \mathsf{of} \; \mathcal{T}^{(1)}(0 \oplus \mathsf{m_1}) \ & dots \ \mathsf{new} \; \mathsf{sharing} \; \mathsf{of} \; \mathcal{T}^{(1)}((2^k-1) \oplus \mathsf{m_1}) \end{array}
ight\}$$



Higher Order: Optimizations

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





# Masked SBox Construction (Common Table)

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

#### Masked SBox Evaluation

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

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



Higher Order: Optimizations

#### **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**

Conclusio

1 Introduction1st Order SolutionHigher 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

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

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