Higher-Order Masking Schemes for S-boxes

Matthieu Rivain

Joint work with

C. Carlet, L. Goubin, E. Prouff and M. Quisquater

FSE 2012

Washington DC, 21st March 2012

WE INNOVATE TO SECURE YOUR BUSINESS

Outline

Higher-Order Masking

- Countermeasure to side-channel attacks

Higher-Order Masking

- Countermeasure to side-channel attacks
- Every key-dependent variable x is shared into $d+1$ variables:

$$x = x_0 + x_1 + \cdots + x_d$$

Higher-Order Masking

- Countermeasure to side-channel attacks
- Every key-dependent variable x is shared into $d+1$ variables:

$$x = x_0 + x_1 + \cdots + x_d$$

- In this work, $+$ is the bitwise addition

Higher-Order Masking

- Countermeasure to side-channel attacks
- Every key-dependent variable x is shared into $d+1$ variables:

$$x = x_0 + x_1 + \cdots + x_d$$

- In this work, $+$ is the bitwise addition
- Attack complexity increases exponentially with d

Higher-Order Masking Schemes

- Consider a block cipher:

$$c \leftarrow \mathrm{E}(m, k)$$

Higher-Order Masking Schemes

- Consider a block cipher:

$$c \leftarrow \mathrm{E}(m, k)$$

- A dth-order masking scheme for E is an algorithm:

$$(c_0, c_1, \ldots, c_d) \leftarrow \mathrm{E}'\big((m_0, m_1, \ldots, m_d), (k_0, k_1, \ldots, k_d)\big)$$

Higher-Order Masking Schemes

- Consider a block cipher:

$$c \leftarrow \mathrm{E}(m, k)$$

- A dth-order masking scheme for E is an algorithm:

$$(c_0, c_1, \ldots, c_d) \leftarrow \mathrm{E}'\big((m_0, m_1, \ldots, m_d), (k_0, k_1, \ldots, k_d)\big)$$

- *dth-order security :*
$\forall (iv_1, iv_2, \ldots, iv_d) \in \{\text{intermediate var. of } \mathrm{E}'\}^d$:

$$\mathrm{MI}\big((iv_1, iv_2, \ldots, iv_d), (m, k)\big) = 0$$

Higher-Order Masking Schemes

- Consider a block cipher:

$$c \leftarrow \mathrm{E}(m, k)$$

- A dth-order masking scheme for E is an algorithm:

$$(c_0, c_1, \ldots, c_d) \leftarrow \mathrm{E}'\big((m_0, m_1, \ldots, m_d), (k_0, k_1, \ldots, k_d)\big)$$

- *dth-order security :*
$\forall (iv_1, iv_2, \ldots, iv_d) \in \{\text{intermediate var. of } \mathrm{E}'\}^d$:

$$\mathrm{MI}\big((iv_1, iv_2, \ldots, iv_d), (m, k)\big) = 0$$

- The main issue is masking the S-box

Literature

- Software masking schemes:

	$d = 1$	$d = 2$	any d
AES	Many works	x	[RP10,KHL11,GPQ11]
any s-box	Many works	[SP06,RDP08]	This work

[SP06] = [Schramm-Paar CT-RSA'06]
[RPD08] = [Rivain-Dottax-Prouff FSE'08]
[RP10] = [Rivain-Prouff CHES'10]
[KHL11] = [Kim-Hong-Lim CHES'11]
[GPQ11] = [Genelle-Prouff-Quisquater CHES'11]

Literature

- Software masking schemes:

	$d = 1$	$d = 2$	any d
AES	Many works	x	[RP10,KHL11,GPQ11]
any s-box	Many works	[SP06,RDP08]	This work

[SP06] = [Schramm-Paar CT-RSA'06]
[RPD08] = [Rivain-Dottax-Prouff FSE'08]
[RP10] = [Rivain-Prouff CHES'10]
[KHL11] = [Kim-Hong-Lim CHES'11]
[GPQ11] = [Genelle-Prouff-Quisquater CHES'11]

- Hardware masking schemes:
  - $d = 1 \Rightarrow$ many works

Literature

- Software masking schemes:

	$d = 1$	$d = 2$	any d
AES	Many works	x	[RP10,KHL11,GPQ11]
any s-box	Many works	[SP06,RDP08]	This work

[SP06] = [Schramm-Paar CT-RSA'06]
[RPD08] = [Rivain-Dottax-Prouff FSE'08]
[RP10] = [Rivain-Prouff CHES'10]
[KHL11] = [Kim-Hong-Lim CHES'11]
[GPQ11] = [Genelle-Prouff-Quisquater CHES'11]

- Hardware masking schemes:
  - $d = 1 \Rightarrow$ many works
  - [Ishai-Sahai-Wagner CRYPTO'03]
    - any circuit, any order d

Literature

- Software masking schemes:

	$d = 1$	$d = 2$	any d
AES	Many works	x	[RP10,KHL11,GPQ11]
any s-box	Many works	[SP06,RDP08]	This work

[SP06] = [Schramm-Paar CT-RSA'06]
[RPD08] = [Rivain-Dottax-Prouff FSE'08]
[RP10] = [Rivain-Prouff CHES'10]
[KHL11] = [Kim-Hong-Lim CHES'11]
[GPQ11] = [Genelle-Prouff-Quisquater CHES'11]

- Hardware masking schemes:
  - $d = 1 \Rightarrow$ many works
  - [Ishai-Sahai-Wagner CRYPTO'03]
    - any circuit, any order d
  - [Faust *et al.* EUROCRYPT'10]
    - generalization to further security models

Ishai-Sahai-Wagner (ISW) Scheme

- Probing model: intermediate variable = wire
- Any circuits composed of NOT and AND gates

Ishai-Sahai-Wagner (ISW) Scheme

- Probing model: intermediate variable = wire
- Any circuits composed of NOT and AND gates
- NOT gate encoding:

$$\mathrm{NOT}(x) = \mathrm{NOT}(x_0) \oplus x_1 \cdots \oplus x_d$$

Ishai-Sahai-Wagner (ISW) Scheme

- Probing model: intermediate variable = wire
- Any circuits composed of NOT and AND gates
- NOT gate encoding:

$$\mathrm{NOT}(x) = \mathrm{NOT}(x_0) \oplus x_1 \cdots \oplus x_d$$

- AND gate encoding:

$$\begin{aligned} \mathrm{AND}(x, y) = xy &= \left(\bigoplus_i x_i\right)\left(\bigoplus_j y_j\right) \\ &= \bigoplus_{i,j} x_i y_j = \bigoplus_i z_i \end{aligned}$$

Ishai-Sahai-Wagner (ISW) Scheme

- Probing model: intermediate variable = wire
- Any circuits composed of NOT and AND gates
- NOT gate encoding:

$$\mathrm{NOT}(x) = \mathrm{NOT}(x_0) \oplus x_1 \cdots \oplus x_d$$

- AND gate encoding:

$$\begin{aligned} \mathrm{AND}(x, y) = xy &= \Big(\bigoplus_i x_i\Big)\Big(\bigoplus_j y_j\Big) \\ &= \bigoplus_{i,j} x_i y_j = \bigoplus_i z_i \end{aligned}$$

  - $(d+1)^2$ ANDs $+\ 2d(d+1)$ XORs
    $+\ d(d+1)/2$ random bits

Application to AES in Software

- [Rivain-Prouff CHES 2010]

Application to AES in Software

- [Rivain-Prouff CHES 2010]
- AES S-box: $\mathsf{S} = \mathsf{Exp} \circ \mathsf{Af}$
  - Af: affine transformation over $\mathrm{GF}(2)^8$
  - Exp : $x \mapsto x^{254}$ over $\mathrm{GF}(2^8)$

Application to AES in Software

- [Rivain-Prouff CHES 2010]
- AES S-box: $\mathsf{S} = \mathsf{Exp} \circ \mathsf{Af}$
  - Af: affine transformation over $\mathrm{GF}(2)^8$
  - Exp : $x \mapsto x^{254}$ over $\mathrm{GF}(2^8)$
- Masking Af is efficient:

$$\mathsf{Af}(x) = \mathsf{Af}(x_0) + \mathsf{Af}(x_1) + \cdots + \mathsf{Af}(x_d) \qquad (+\mathtt{0x63} \text{ iff } d \text{ is odd})$$

Application to AES in Software

- [Rivain-Prouff CHES 2010]
- AES S-box: $\mathsf{S} = \mathsf{Exp} \circ \mathsf{Af}$
  - Af: affine transformation over $\mathrm{GF}(2)^8$
  - Exp : $x \mapsto x^{254}$ over $\mathrm{GF}(2^8)$
- Masking Af is efficient:

$$\mathsf{Af}(x) = \mathsf{Af}(x_0) + \mathsf{Af}(x_1) + \cdots + \mathsf{Af}(x_d) \qquad (+\texttt{0x63} \text{ iff } d \text{ is odd})$$

- Masking Exp
  - masked square: $x_0^2 + x_1^2 + \cdots + x_d^2 = x^2$

Application to AES in Software

- [Rivain-Prouff CHES 2010]
- AES S-box: $\mathsf{S} = \mathsf{Exp} \circ \mathsf{Af}$
  - Af: affine transformation over $\mathrm{GF}(2)^8$
  - Exp : $x \mapsto x^{254}$ over $\mathrm{GF}(2^8)$
- Masking Af is efficient:

  $\mathsf{Af}(x) = \mathsf{Af}(x_0) + \mathsf{Af}(x_1) + \cdots + \mathsf{Af}(x_d) \quad (+\mathtt{0x63} \text{ iff } d \text{ is odd})$
- Masking Exp
  - masked square: $x_0^2 + x_1^2 + \cdots + x_d^2 = x^2$
  - masked multiplications : ISW on $\mathrm{GF}(2^8)$

Application to AES in Software

- [Rivain-Prouff CHES 2010]
- AES S-box: $\mathsf{S} = \mathsf{Exp} \circ \mathsf{Af}$
  - Af: affine transformation over $\mathrm{GF}(2)^8$
  - Exp : $x \mapsto x^{254}$ over $\mathrm{GF}(2^8)$
- Masking Af is efficient:

$$\mathsf{Af}(x) = \mathsf{Af}(x_0) + \mathsf{Af}(x_1) + \cdots + \mathsf{Af}(x_d) \quad (+\mathtt{0x63} \text{ iff } d \text{ is odd})$$

- Masking Exp
  - masked square: $x_0^2 + x_1^2 + \cdots + x_d^2 = x^2$
  - masked multiplications : ISW on $\mathrm{GF}(2^8)$
  - addition chain for 254 with only 4 multiplications (and 7 squares)

Outline

General Method

- Generalization of Rivain-Prouff scheme

General Method

- Generalization of Rivain-Prouff scheme

- We consider an s-box $\mathrm{S} : \{0,1\}^n \to \{0,1\}^m$ as a polynomial function over $\mathrm{GF}(2^n)$:

$$\mathrm{S}(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{2^n-1} x^{2^n-1}$$

General Method

- Generalization of Rivain-Prouff scheme
- We consider an s-box $\mathrm{S} : \{0,1\}^n \to \{0,1\}^m$ as a polynomial function over $\mathrm{GF}(2^n)$:

$$\mathrm{S}(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{2^n-1} x^{2^n-1}$$

- We evaluate this polynomial on the shared input $(x_i)_i$

General Method

- Four kinds of operations over $\mathrm{GF}(2^n)$:
  1. additions
  2. scalar multiplications (*i.e.* by constants)
  3. squares
  4. regular multiplications

General Method

- Four kinds of operations over $\mathrm{GF}(2^n)$:
  1. additions
  2. scalar multiplications (*i.e.* by constants)
  3. squares
  4. regular multiplications
- Masking is efficient for the 3 first kinds

General Method

- Four kinds of operations over $\mathrm{GF}(2^n)$:
  1. additions
  2. scalar multiplications (*i.e.* by constants)
  3. squares
  4. regular multiplications

- Masking is efficient for the 3 first kinds
  - $(x + y) = (x_0 + y_0) + (x_1 + y_1) + \cdots + (x_d + y_d)$

General Method

- Four kinds of operations over $\mathrm{GF}(2^n)$:
  1. additions
  2. scalar multiplications (*i.e.* by constants)
  3. squares
  4. regular multiplications

- Masking is efficient for the 3 first kinds
  - $(x + y) = (x_0 + y_0) + (x_1 + y_1) + \cdots + (x_d + y_d)$
  - $x^2 = x_0^2 + x_1^2 + \cdots + x_d^2$

General Method

- Four kinds of operations over $\mathrm{GF}(2^n)$:
  1. additions
  2. scalar multiplications (*i.e.* by constants)
  3. squares
  4. regular multiplications

- Masking is efficient for the 3 first kinds
  - $(x + y) = (x_0 + y_0) + (x_1 + y_1) + \cdots + (x_d + y_d)$
  - $x^2 = x_0^2 + x_1^2 + \cdots + x_d^2$
  - $a \cdot x = a \cdot x_0 + a \cdot x_1 + \cdots + a \cdot x_d$

General Method

- Four kinds of operations over $\mathrm{GF}(2^n)$:
  1. additions
  2. scalar multiplications (*i.e.* by constants)
  3. squares
  4. regular multiplications $\Rightarrow$ *nonlinear multiplications*

- Masking is efficient for the 3 first kinds
  - $(x + y) = (x_0 + y_0) + (x_1 + y_1) + \cdots + (x_d + y_d)$
  - $x^2 = x_0^2 + x_1^2 + \cdots + x_d^2$
  - $a \cdot x = a \cdot x_0 + a \cdot x_1 + \cdots + a \cdot x_d$

General Method

- Four kinds of operations over $\mathrm{GF}(2^n)$:
  1. additions
  2. scalar multiplications (*i.e.* by constants)
  3. squares
  4. regular multiplications $\Rightarrow$ *nonlinear multiplications*

- Masking is efficient for the 3 first kinds
  - $(x + y) = (x_0 + y_0) + (x_1 + y_1) + \cdots + (x_d + y_d)$
  - $x^2 = x_0^2 + x_1^2 + \cdots + x_d^2$
  - $a \cdot x = a \cdot x_0 + a \cdot x_1 + \cdots + a \cdot x_d$

- nonlinear multiplication masked with ISW scheme

Masking Complexity

- Masking an operation $\in$ {addition, square, scalar mult.}
  $\Rightarrow$ $d+1$ operations
- Masking a nonlinear multiplication
  $\Rightarrow$ $(d+1)^2$ mult. $+\ 2d(d+1)$ add. $+\ nd(d+1)/2$ random bits

Masking Complexity

- Masking an operation $\in$ {addition, square, scalar mult.}
  $\Rightarrow$ $d+1$ operations
- Masking a nonlinear multiplication
  $\Rightarrow$ $(d+1)^2$ mult. $+$ $2d(d+1)$ add. $+$ $nd(d+1)/2$ random bits

Definition

The *masking complexity* of a (n, m) s-box is the minimal number of nonlinear multiplications required to evaluate its polynomial representation over $\mathrm{GF}(2^n)$.

Straightforward schemes

- Goal: evaluate $\mathsf{S}(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{2^n-1} x^{2^n-1}$
- first solution :
  - compute $\mathsf{S}(x) = a_0 + x(a_1 + x(a_2 + x(\cdots)))$
  - $\Rightarrow 2^n - 2$ nonlinear multiplications

Straightforward schemes

- Goal: evaluate $\mathsf{S}(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{2^n-1} x^{2^n-1}$
- first solution :
  - compute $\mathsf{S}(x) = a_0 + x(a_1 + x(a_2 + x(\cdots)))$
  - $\Rightarrow 2^n - 2$ nonlinear multiplications
- second solution :
  - first compute x^2, x^3, x^4, ... then evaluate $\mathsf{S}(x)$
  - $x^j \leftarrow (x^{j/2})^2$ when j even, $x^j \leftarrow x \cdot x^{j-1}$ when j odd
  - $\Rightarrow 2^{n-1} - 1$ nonlinear multiplications

Straightforward schemes

- Goal: evaluate $\mathsf{S}(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{2^n-1} x^{2^n-1}$
- first solution :
  - compute $\mathsf{S}(x) = a_0 + x(a_1 + x(a_2 + x(\cdots)))$
  - $\Rightarrow 2^n - 2$ nonlinear multiplications
- second solution :
  - first compute x^2, x^3, x^4, ... then evaluate $\mathsf{S}(x)$
  - $x^j \leftarrow (x^{j/2})^2$ when j even, $x^j \leftarrow x \cdot x^{j-1}$ when j odd
  - $\Rightarrow 2^{n-1} - 1$ nonlinear multiplications
- Can we do better ?

Straightforward schemes

- Goal: evaluate $\mathsf{S}(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{2^n-1} x^{2^n-1}$
- first solution :
  - compute $\mathsf{S}(x) = a_0 + x(a_1 + x(a_2 + x(\cdots)))$
  - $\Rightarrow 2^n - 2$ nonlinear multiplications
- second solution :
  - first compute x^2, x^3, x^4, ... then evaluate $\mathsf{S}(x)$
  - $x^j \leftarrow (x^{j/2})^2$ when j even, $x^j \leftarrow x \cdot x^{j-1}$ when j odd
  - $\Rightarrow 2^{n-1} - 1$ nonlinear multiplications
- Can we do better ? YES, WE CAN !

Straightforward schemes

- Goal: evaluate $\mathsf{S}(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{2^n-1} x^{2^n-1}$
- first solution :
  - compute $\mathsf{S}(x) = a_0 + x(a_1 + x(a_2 + x(\cdots)))$
  - $\Rightarrow 2^n - 2$ nonlinear multiplications
- second solution :
  - first compute x^2, x^3, x^4, ... then evaluate $\mathsf{S}(x)$
  - $x^j \leftarrow (x^{j/2})^2$ when j even, $x^j \leftarrow x \cdot x^{j-1}$ when j odd
  - $\Rightarrow 2^{n-1} - 1$ nonlinear multiplications
- Can we do better ? YES, WE CAN !
  - Optimal methods for power functions
  - Efficient heuristic for the general case

Outline

CryptoExperts

Optimal Masking of Power Functions

Problem

For a given $\alpha \in [1; 2^n - 1]$ compute x^α with the least number of nonlinear multiplications.

Optimal Masking of Power Functions

Problem

For a given $\alpha \in [1; 2^n - 1]$ compute x^α with the least number of nonlinear multiplications.

$$\Longleftrightarrow$$

Problem

Find the shortest 2-addition chain for α (modulo $2^n - 1$).

Optimal Masking of Power Functions

- *Cyclotomic class of α* : $C_\alpha = \{\alpha \cdot 2^j \bmod (2^n - 1);\ j \leq n\}$

Optimal Masking of Power Functions

- *Cyclotomic class of* α : $C_\alpha = \{\alpha \cdot 2^j \bmod (2^n - 1);\ j \leq n\}$
- If $\beta \in C_\alpha$ ($\Leftrightarrow C_\beta = C_\alpha$)

Optimal Masking of Power Functions

- *Cyclotomic class of α* : $C_\alpha = \{\alpha \cdot 2^j \bmod (2^n - 1);\ j \leq n\}$
- If $\beta \in C_\alpha$ ($\Leftrightarrow C_\beta = C_\alpha$)
  - x^α can be computed from x^β with 0 nonlinear multiplication

Optimal Masking of Power Functions

- *Cyclotomic class of α* : $C_\alpha = \{\alpha \cdot 2^j \bmod (2^n - 1);\ j \leq n\}$
- If $\beta \in C_\alpha$ ($\Leftrightarrow C_\beta = C_\alpha$)
  - x^α can be computed from x^β with 0 nonlinear multiplication
  - x^α and x^β have the same masking complexity

Optimal Masking of Power Functions

- *Cyclotomic class of α* : $C_\alpha = \{\alpha \cdot 2^j \bmod (2^n - 1);\ j \leq n\}$
- If $\beta \in C_\alpha$ ($\Leftrightarrow C_\beta = C_\alpha$)
  - x^α can be computed from x^β with 0 nonlinear multiplication
  - x^α and x^β have the same masking complexity
- Exhaustive search for best 2-addition chains

Optimal Masking of Power Functions

- *Cyclotomic class of* α : $C_\alpha = \{\alpha \cdot 2^j \bmod (2^n - 1);\ j \leq n\}$
- If $\beta \in C_\alpha$ ($\Leftrightarrow C_\beta = C_\alpha$)
  - x^α can be computed from x^β with 0 nonlinear multiplication
  - x^α and x^β have the same masking complexity
- Exhaustive search for best 2-addition chains
  - $x \to x^2, x^4, x^8, \ldots$ (0 nonlinear multiplications)

Optimal Masking of Power Functions

- *Cyclotomic class of α* : $C_\alpha = \{\alpha \cdot 2^j \bmod (2^n - 1);\ j \leq n\}$
- If $\beta \in C_\alpha$ ($\Leftrightarrow C_\beta = C_\alpha$)
  - x^α can be computed from x^β with 0 nonlinear multiplication
  - x^α and x^β have the same masking complexity
- Exhaustive search for best 2-addition chains
  - $x \rightarrow x^2, x^4, x^8, \ldots$ (0 nonlinear multiplications)
  - with 1 nonlinear multiplication
    - $x^3 = x \cdot x^2$

Optimal Masking of Power Functions

- *Cyclotomic class of α* : $C_\alpha = \{\alpha \cdot 2^j \bmod (2^n - 1);\ j \leq n\}$
- If $\beta \in C_\alpha$ ($\Leftrightarrow C_\beta = C_\alpha$)
  - x^α can be computed from x^β with 0 nonlinear multiplication
  - x^α and x^β have the same masking complexity
- Exhaustive search for best 2-addition chains
  - $x \rightarrow x^2, x^4, x^8, \ldots$ (0 nonlinear multiplications)
  - with 1 nonlinear multiplication
    - $x^3 = x \cdot x^2 \rightarrow x^6, x^{12}, x^{24}, \ldots$

Optimal Masking of Power Functions

- *Cyclotomic class of α* : $C_\alpha = \{\alpha \cdot 2^j \bmod (2^n - 1);\ j \leq n\}$
- If $\beta \in C_\alpha$ ($\Leftrightarrow C_\beta = C_\alpha$)
  - x^α can be computed from x^β with 0 nonlinear multiplication
  - x^α and x^β have the same masking complexity
- Exhaustive search for best 2-addition chains
  - $x \rightarrow x^2, x^4, x^8, \ldots$ (0 nonlinear multiplications)
  - with 1 nonlinear multiplication
    - $x^3 = x \cdot x^2 \rightarrow x^6, x^{12}, x^{24}, \ldots$
    - $x^5 = x \cdot x^4$

Optimal Masking of Power Functions

- *Cyclotomic class of α* : $C_\alpha = \{\alpha \cdot 2^j \bmod (2^n - 1);\ j \leq n\}$
- If $\beta \in C_\alpha$ ($\Leftrightarrow C_\beta = C_\alpha$)
  - x^α can be computed from x^β with 0 nonlinear multiplication
  - x^α and x^β have the same masking complexity
- Exhaustive search for best 2-addition chains
  - $x \to x^2, x^4, x^8, \ldots$ (0 nonlinear multiplications)
  - with 1 nonlinear multiplication
    - $x^3 = x \cdot x^2 \to x^6, x^{12}, x^{24}, \ldots$
    - $x^5 = x \cdot x^4 \to x^{10}, x^{20}, x^{40}, \ldots$

Optimal Masking of Power Functions

- *Cyclotomic class of α* : $C_\alpha = \{\alpha \cdot 2^j \bmod (2^n - 1);\ j \leq n\}$
- If $\beta \in C_\alpha$ ($\Leftrightarrow C_\beta = C_\alpha$)
  - x^α can be computed from x^β with 0 nonlinear multiplication
  - x^α and x^β have the same masking complexity
- Exhaustive search for best 2-addition chains
  - $x \rightarrow x^2, x^4, x^8, \ldots$ (0 nonlinear multiplications)
  - with 1 nonlinear multiplication
    - $x^3 = x \cdot x^2 \rightarrow x^6, x^{12}, x^{24}, \ldots$
    - $x^5 = x \cdot x^4 \rightarrow x^{10}, x^{20}, x^{40}, \ldots$
    - *etc.*

Optimal Masking of Power Functions

- *Cyclotomic class of α* : $C_\alpha = \{\alpha \cdot 2^j \bmod (2^n - 1);\ j \leq n\}$
- If $\beta \in C_\alpha$ ($\Leftrightarrow C_\beta = C_\alpha$)
  - x^α can be computed from x^β with 0 nonlinear multiplication
  - x^α and x^β have the same masking complexity
- Exhaustive search for best 2-addition chains
  - $x \rightarrow x^2, x^4, x^8, \ldots$ (0 nonlinear multiplications)
  - with 1 nonlinear multiplication
    - $x^3 = x \cdot x^2 \rightarrow x^6, x^{12}, x^{24}, \ldots$
    - $x^5 = x \cdot x^4 \rightarrow x^{10}, x^{20}, x^{40}, \ldots$
    - *etc.*
  - with 2 nonlinear multiplications
    - $x^7 = x^3 \cdot x^4$

Optimal Masking of Power Functions

- *Cyclotomic class of α* : $C_\alpha = \{\alpha \cdot 2^j \bmod (2^n - 1);\ j \leq n\}$
- If $\beta \in C_\alpha$ ($\Leftrightarrow C_\beta = C_\alpha$)
  - x^α can be computed from x^β with 0 nonlinear multiplication
  - x^α and x^β have the same masking complexity
- Exhaustive search for best 2-addition chains
  - $x \rightarrow x^2, x^4, x^8, \ldots$ (0 nonlinear multiplications)
  - with 1 nonlinear multiplication
    - $x^3 = x \cdot x^2 \rightarrow x^6, x^{12}, x^{24}, \ldots$
    - $x^5 = x \cdot x^4 \rightarrow x^{10}, x^{20}, x^{40}, \ldots$
    - *etc.*
  - with 2 nonlinear multiplications
    - $x^7 = x^3 \cdot x^4 \rightarrow x^{14}, x^{28}, \ldots$

Optimal Masking of Power Functions

- *Cyclotomic class of α* : $C_\alpha = \{\alpha \cdot 2^j \bmod (2^n - 1);\ j \leq n\}$
- If $\beta \in C_\alpha$ ($\Leftrightarrow C_\beta = C_\alpha$)
  - x^α can be computed from x^β with 0 nonlinear multiplication
  - x^α and x^β have the same masking complexity
- Exhaustive search for best 2-addition chains
  - $x \rightarrow x^2, x^4, x^8, \ldots$ (0 nonlinear multiplications)
  - with 1 nonlinear multiplication
    - $x^3 = x \cdot x^2 \rightarrow x^6, x^{12}, x^{24}, \ldots$
    - $x^5 = x \cdot x^4 \rightarrow x^{10}, x^{20}, x^{40}, \ldots$
    - *etc.*
  - with 2 nonlinear multiplications
    - $x^7 = x^3 \cdot x^4 \rightarrow x^{14}, x^{28}, \ldots$
    - $x^{11} = x^3 \cdot x^8$

Optimal Masking of Power Functions

- *Cyclotomic class of α* : $C_\alpha = \{\alpha \cdot 2^j \bmod (2^n - 1);\ j \leq n\}$
- If $\beta \in C_\alpha$ ($\Leftrightarrow C_\beta = C_\alpha$)
  - x^α can be computed from x^β with 0 nonlinear multiplication
  - x^α and x^β have the same masking complexity
- Exhaustive search for best 2-addition chains
  - $x \rightarrow x^2, x^4, x^8, \ldots$ (0 nonlinear multiplications)
  - with 1 nonlinear multiplication
    - $x^3 = x \cdot x^2 \rightarrow x^6, x^{12}, x^{24}, \ldots$
    - $x^5 = x \cdot x^4 \rightarrow x^{10}, x^{20}, x^{40}, \ldots$
    - *etc.*
  - with 2 nonlinear multiplications
    - $x^7 = x^3 \cdot x^4 \rightarrow x^{14}, x^{28}, \ldots$
    - $x^{11} = x^3 \cdot x^8 \rightarrow x^{22}, x^{44}, \ldots$
    - *etc.*

k	Cyclotomic classes in $\mathcal{M}_k^n$
	$n = 4$
0	$C_0 = \{0\}$, $C_1 = \{1, 2, 4, 8\}$
1	$C_3 = \{3, 6, 12, 9\}$, $C_5 = \{5, 10\}$
2	$C_7 = \{7, 14, 13, 11\}$
	$n = 6$
0	$C_0 = \{0\}$, $C_1 = \{1, 2, 4, 8, 16, 32\}$
1	$C_3 = \{3, 6, 12, 24, 48, 33\}$, $C_5 = \{5, 10, 20, 40, 17, 34\}$, $C_9 = \{9, 18, 36\}$
2	$C_7 = \{7, 14, 28, 56, 49, 35\}$, $C_{11} = \{11, 22, 44, 25, 50, 37\}$, $C_{13} = \{13, 26, 52, 41, 19, 38\}$, $C_{15} = \{15, 30, 29, 27, 23\}$, $C_{21} = \{21, 42\}$, $C_{27} = \{27, 54, 45\}$
3	$C_{23} = \{23, 46, 29, 58, 53, 43\}$, $C_{31} = \{31, 62, 61, 59, 55, 47\}$
	$n = 8$
0	$C_0 = \{0\}$, $C_1 = \{1, 2, 4, 8, 16, 32, 64, 128\}$
1	$C_3 = \{3, 6, 12, 24, 48, 96, 192, 129\}$, $C_5 = \{5, 10, 20, 40, 80, 160, 65, 130\}$, $C_9 = \{9, 18, 36, 72, 144, 33, 66, 132\}$, $C_{17} = \{17, 34, 68, 136\}$
2	$C_7 = \{7, 14, 28, 56, 112, 224, 193, 131\}$, $C_{11} = \{11, 22, 44, 88, 176, 97, 194, 133\}$, $C_{13} = \{13, 26, 52, 104, 208, 161, 67, 134\}$, $C_{15} = \{15, 30, 60, 120, 240, 225, 195, 135\}$, $C_{19} = \{19, 38, 76, 152, 49, 98, 196, 137\}$, $C_{21} = \{21, 42, 84, 168, 81, 162, 69, 138\}$, $C_{25} = \{25, 50, 100, 200, 145, 35, 70, 140\}$, $C_{27} = \{27, 54, 108, 216, 177, 99, 198, 141\}$, $C_{37} = \{37, 74, 148, 41, 82, 164, 73, 146\}$, $C_{45} = \{45, 90, 180, 105, 210, 165, 75, 150\}$, $C_{51} = \{51, 102, 204, 153\}$, $C_{85} = \{85, 170\}$
3	$C_{23} = \{23, 46, 92, 184, 113, 226, 197, 139\}$, $C_{29} = \{29, 58, 116, 232, 209, 163, 71, 142\}$, $C_{31} = \{31, 62, 124, 248, 241, 227, 199, 143\}$, $C_{39} = \{39, 78, 156, 57, 114, 228, 201, 147\}$, $C_{43} = \{43, 86, 172, 89, 178, 101, 202, 149\}$, $C_{47} = \{47, 94, 188, 121, 242, 229, 203, 151\}$, $C_{53} = \{53, 106, 212, 169, 83, 166, 77, 154\}$, $C_{55} = \{55, 110, 220, 185, 115, 230, 205, 155\}$, $C_{59} = \{59, 118, 236, 217, 179, 103, 206, 157\}$, $C_{61} = \{61, 122, 244, 233, 211, 167, 79, 158\}$, $C_{63} = \{63, 126, 252, 249, 243, 231, 207, 159\}$, $C_{87} = \{87, 174, 93, 186, 117, 234, 213, 171\}$, $C_{91} = \{91, 182, 109, 218, 181, 107, 214, 173\}$, $C_{95} = \{95, 190, 125, 250, 245, 235, 215, 175\}$, $C_{111} = \{111, 222, 189, 123, 246, 237, 219, 183\}$, $C_{119} = \{119, 238, 221, 187\}$
4	$C_{127} = \{127, 254, 253, 251, 247, 239, 223, 191\}$

Outline

Cyclotomic Method

$$\begin{aligned} \mathsf{S}(x) &= a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + a_5 x^5 + a_6 x^6 + a_7 x^7 \\ &\quad + a_8 x^8 + a_9 x^9 + a_{10} x^{10} + a_{11} x^{11} + a_{12} x^{12} + \ldots \end{aligned}$$

Cyclotomic Method

$$\begin{aligned} \mathsf{S}(x) \;\; &= \;\; a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + a_5 x^5 + a_6 x^6 + a_7 x^7 \\ &\quad + a_8 x^8 + a_9 x^9 + a_{10} x^{10} + a_{11} x^{11} + a_{12} x^{12} + \ldots \end{aligned}$$

Cyclotomic Method

$$\begin{aligned} \mathsf{S}(x) &= a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + a_5 x^5 + a_6 x^6 + a_7 x^7 \\ &\quad + a_8 x^8 + a_9 x^9 + a_{10} x^{10} + a_{11} x^{11} + a_{12} x^{12} + \dots \end{aligned}$$

Cyclotomic Method

$$\begin{aligned} \mathsf{S}(x) &= a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + a_5 x^5 + a_6 x^6 + a_7 x^7 \\ &\quad + a_8 x^8 + a_9 x^9 + a_{10} x^{10} + a_{11} x^{11} + a_{12} x^{12} + \dots \end{aligned}$$

Cyclotomic Method

$$\begin{aligned}
\mathsf{S}(x) &= a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + a_5 x^5 + a_6 x^6 + a_7 x^7 \\
&\quad + a_8 x^8 + a_9 x^9 + a_{10} x^{10} + a_{11} x^{11} + a_{12} x^{12} + \ldots \\
&= a_0 + a_1 x + a_2 x^2 + a_4 x^4 + a_8 x^8 + \ldots \\
&\quad + a_3 x^3 + a_6 x^6 + a_{12} x^{12} + a_{24} x^{24} + \ldots \\
&\quad + a_5 x^5 + a_{10} x^{10} + a_{20} x^{20} + a_{40} x^{40} + \ldots \\
&\quad + \ldots
\end{aligned}$$

Cyclotomic Method

$$
\begin{aligned}
\mathsf{S}(x) &= a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + a_5 x^5 + a_6 x^6 + a_7 x^7 \\
&\quad + a_8 x^8 + a_9 x^9 + a_{10} x^{10} + a_{11} x^{11} + a_{12} x^{12} + \dots \\
&= a_0 + a_1 x + a_2 x^2 + a_4 x^4 + a_8 x^8 + \dots \\
&\quad + a_3 x^3 + a_6 (x^3)^2 + a_{12} (x^3)^4 + a_{24} (x^3)^8 + \dots \\
&\quad + a_5 x^5 + a_{10} (x^5)^2 + a_{20} (x^5)^4 + a_{40} (x^5)^8 + \dots \\
&\quad + \dots
\end{aligned}
$$

Cyclotomic Method

$$\begin{aligned}
\mathsf{S}(x) &= a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + a_5 x^5 + a_6 x^6 + a_7 x^7 \\
&\quad + a_8 x^8 + a_9 x^9 + a_{10} x^{10} + a_{11} x^{11} + a_{12} x^{12} + \dots \\
&= a_0 + a_1 x + a_2 x^2 + a_4 x^4 + a_8 x^8 + \dots \\
&\quad + a_3 x^3 + a_6 (x^3)^2 + a_{12} (x^3)^4 + a_{24} (x^3)^8 + \dots \\
&\quad + a_5 x^5 + a_{10} (x^5)^2 + a_{20} (x^5)^4 + a_{40} (x^5)^8 + \dots \\
&\quad + \dots \\
&= a_0 + L_1(x) + L_3(x^3) + L_5(x^5) + \dots
\end{aligned}$$

where

- $L_1(X) = a_1 X + a_2 X^2 + a_4 X^4 + a_8 X^8 + \dots$
- $L_3(X) = a_3 X + a_6 X^2 + a_{12} X^4 + a_{24} X^8 + \dots$
- $L_5(X) = a_5 X + a_{10} X^2 + a_{20} X^4 + a_{40} X^8 + \dots$
- ...

Cyclotomic Method

1. Compute one power per cyclotomic class x, x^3, x^5, x^7, ...

Cyclotomic Method

1. Compute one power per cyclotomic class x, x^3, x^5, x^7, ...
2. Evaluate the corresponding linearized polynomials $L_1(x)$, $L_3(x^3)$, $L_5(x^5)$, $L_7(x^7)$, ...

Cyclotomic Method

1. Compute one power per cyclotomic class x, x^3, x^5, x^7, ...
2. Evaluate the corresponding linearized polynomials $L_1(x)$, $L_3(x^3)$, $L_5(x^5)$, $L_7(x^7)$, ...
3. Compute the sum
   $\mathsf{S}(x) = a_0 + L_1(x) + L_3(x^3) + L_5(x^5) + L_7(x^7) + \dots$

Cyclotomic Method

1. Compute one power per cyclotomic class x, x^3, x^5, x^7, ...
2. Evaluate the corresponding linearized polynomials $L_1(x)$, $L_3(x^3)$, $L_5(x^5)$, $L_7(x^7)$, ...
3. Compute the sum $\mathsf{S}(x) = a_0 + L_1(x) + L_3(x^3) + L_5(x^5) + L_7(x^7) + \ldots$

Number of nonlinear multiplication

$=$

$\#\{$**cyclotomic classes**$\}\backslash(C_0 \cup C_1)$

Cyclotomic Method

1. Compute one power per cyclotomic class x, x^3, x^5, x^7, ...
2. Evaluate the corresponding linearized polynomials $L_1(x)$, $L_3(x^3)$, $L_5(x^5)$, $L_7(x^7)$, ...
3. Compute the sum
   $\mathsf{S}(x) = a_0 + L_1(x) + L_3(x^3) + L_5(x^5) + L_7(x^7) + \dots$

Number of nonlinear multiplication

$=$

$\#\{$**cyclotomic classes**$\}\backslash(C_0 \cup C_1)$

n	3	4	5	6	7	8	9	10
# nlm	1	3	5	11	17	33	53	105

Parity-Split Method

$$\begin{aligned} \mathsf{S}(x) &= a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + a_5 x^5 + a_6 x^6 + a_7 x^7 \\ &\quad + a_8 x^8 + a_9 x^9 + a_{10} x^{10} + a_{11} x^{11} + a_{12} x^{12} + \dots \end{aligned}$$

Parity-Split Method

$$\begin{aligned} \mathsf{S}(x) &= a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + a_5 x^5 + a_6 x^6 + a_7 x^7 \\ &\quad + a_8 x^8 + a_9 x^9 + a_{10} x^{10} + a_{11} x^{11} + a_{12} x^{12} + \dots \end{aligned}$$

Parity-Split Method

$$\begin{aligned} \mathsf{S}(x) \quad = \quad & a_0 + a_2 x^2 + a_4 x^4 + a_6 x^6 + a_8 x^8 + \ldots \\ & a_1 x + a_3 x^3 + a_5 x^5 + a_7 x^7 + a_9 x^9 + \ldots \end{aligned}$$

Parity-Split Method

$$
\begin{aligned}
\mathsf{S}(x) \quad &= \quad a_0 + a_2 x^2 + a_4 x^4 + a_6 x^6 + a_8 x^8 + \ldots \\
&\quad\;\; (a_1 + a_3 x^2 + a_5 x^4 + a_7 x^6 + a_9 x^8 + \ldots) \cdot x
\end{aligned}
$$

- Nonlinear mult. : 1

Parity-Split Method

$$\begin{aligned} \mathsf{S}(x) &= a_0 + a_2x^2 + a_4x^4 + a_6x^6 + a_8x^8 + \ldots \\ & \quad (a_1 + a_3x^2 + a_5x^4 + a_7x^6 + a_9x^8 + \ldots) \cdot x \end{aligned}$$

- Nonlinear mult. : 1

Parity-Split Method

$$
\begin{aligned}
\mathsf{S}(x) \quad &= \quad a_0 + a_2 X + a_4 X^2 + a_6 X^3 + a_8 X^4 + \ldots \\
&\qquad (a_1 + a_3 X + a_5 X^2 + a_7 X^3 + a_9 X^4 + \ldots) \cdot x
\end{aligned}
$$

where $X = x^2$

- Nonlinear mult. : 1

Parity-Split Method

$$\begin{aligned}\mathsf{S}(x) &= a_0 + a_2 X + a_4 X^2 + a_6 X^3 + a_8 X^4 + \ldots \\ &\quad (a_1 + a_3 X + a_5 X^2 + a_7 X^3 + a_9 X^4 + \ldots) \cdot x\end{aligned}$$

where $X = x^2$

- Nonlinear mult. : 1

Parity-Split Method

$$\begin{aligned}\mathsf{S}(x) &= a_0 + a_4X^2 + a_8X^4 + \ldots + a_2X + a_6X^3 + \ldots \\ &\quad (a_1 + a_5X^2 + a_9X^4 + \ldots + a_3x^2 + a_7X^3 + \ldots) \cdot x\end{aligned}$$

where $X = x^2$

- Nonlinear mult. : 1

Parity-Split Method

$$\begin{aligned} \mathsf{S}(x) &= a_0 + a_4 X^2 + a_8 X^4 + \ldots + (a_2 + a_6 X^2 + \ldots) \cdot X + \\ &\quad (a_1 + a_5 X^2 + a_9 X^4 + \ldots + (a_3 + a_7 X^2 + \ldots) \cdot X) \cdot x \end{aligned}$$

where $X = x^2$

- Nonlinear mult. : $1{+}2$

Parity-Split Method

$$\begin{aligned}\mathsf{S}(x) &= a_0 + a_4x^4 + a_8x^8 + \ldots + (a_2 + a_6x^4 + \ldots)\cdot x^2 + \\ &\quad (a_1 + a_5x^4 + a_9x^8 + \ldots + (a_3 + a_7x^4 + \ldots)\cdot x^2)\cdot x\end{aligned}$$

- Nonlinear mult. : $1{+}2$

Parity-Split Method

$$\begin{aligned} \mathsf{S}(x) &= a_0 + a_4 X + a_8 X^2 + \ldots + (a_2 + a_6 X + \ldots) \cdot x^2 + \\ & \quad (a_1 + a_5 X + a_9 X^2 + \ldots + (a_3 + a_7 X + \ldots) \cdot x^2) \cdot x \end{aligned}$$

where $X = x^4$

- Nonlinear mult. : $1{+}2$

Parity-Split Method

$$\begin{aligned} \mathsf{S}(x) &= a_0 + a_4 X + a_8 X^2 + \ldots + (a_2 + a_6 X + \ldots) \cdot x^2 + \\ &\quad (a_1 + a_5 X + a_9 X^2 + \ldots + (a_3 + a_7 X + \ldots) \cdot x^2) \cdot x \end{aligned}$$

where $X = x^4$

- Nonlinear mult. : $1+2+\cdots+2^{r-1} = 2^r - 1$

Parity-Split Method

$$\begin{aligned} \mathsf{S}(x) &= a_0 + a_4 X + a_8 X^2 + \ldots + (a_2 + a_6 X + \ldots) \cdot x^2 + \\ &\quad (a_1 + a_5 X + a_9 X^2 + \ldots + (a_3 + a_7 X + \ldots) \cdot x^2) \cdot x \end{aligned}$$

where $X = x^4$

- Nonlinear mult. : $1+2+\cdots+2^{r-1} = 2^r - 1$
- and the evaluation of 2^{r+1} polynomials in $X = x^{2^r}$

Parity-Split Method

$$\begin{aligned} \mathsf{S}(x) &= a_0 + a_4 X + a_8 X^2 + \ldots + (a_2 + a_6 X + \ldots) \cdot x^2 + \\ &\quad (a_1 + a_5 X + a_9 X^2 + \ldots + (a_3 + a_7 X + \ldots) \cdot x^2) \cdot x \end{aligned}$$

where $X = x^4$

- Nonlinear mult. : $1+2+\cdots+2^{r-1} = 2^r - 1$
- and the evaluation of 2^{r+1} polynomials in $X = x^{2^r}$
  - we derive X^j for $j < 2^{n-r}$

Parity-Split Method

$$\begin{aligned}\mathsf{S}(x) &= a_0 + a_4 X + a_8 X^2 + \ldots + (a_2 + a_6 X + \ldots) \cdot x^2 + \\ &\quad (a_1 + a_5 X + a_9 X^2 + \ldots + (a_3 + a_7 X + \ldots) \cdot x^2) \cdot x\end{aligned}$$

where $X = x^4$

- Nonlinear mult. : $1+2+\cdots+2^{r-1} = 2^r - 1$
- and the evaluation of 2^{r+1} polynomials in $X = x^{2^r}$
  - we derive X^j for $j < 2^{n-r}$
  - $2^{n-r-1} - 1$ nonlinear mult.

Parity-Split Method

$$\begin{aligned} \mathsf{S}(x) &= a_0 + a_4 X + a_8 X^2 + \ldots + (a_2 + a_6 X + \ldots) \cdot x^2 + \\ & \quad (a_1 + a_5 X + a_9 X^2 + \ldots + (a_3 + a_7 X + \ldots) \cdot x^2) \cdot x \end{aligned}$$

where $X = x^4$

- Nonlinear mult. : $1+2+\cdots+2^{r-1} = 2^r - 1$
- and the evaluation of 2^{r+1} polynomials in $X = x^{2^r}$
  - we derive X^j for $j < 2^{n-r}$
  - $2^{n-r-1} - 1$ nonlinear mult.

$\Rightarrow 2^{n-r-1} + 2^r - 2$ nonlinear mult.

Comparison

Number of nonlinear multiplications w.r.t. the evaluation method

Method $\setminus$ n	3	4	5	6	7	8	9	10
Cyclotomic	1	3	5	11	17	33	53	105
Parity-Split	2	4	6	10	14	22	30	46

Comparison

Number of nonlinear multiplications w.r.t. the evaluation method

Method $\setminus$ n	3	4	5	6	7	8	9	10
Cyclotomic	1	3	5	11	17	33	53	105
Parity-Split	2	4	6	10	14	22	30	46

- For PRESENT ($n = 4$), we shall prefer the cyclotomic method
- For DES ($n = 6$), we shall prefer the parity-split method

CryptoExperts

Implementation Results

	Method	Reference	cycles	RAM (bytes)
		Second Order Masking		
1.	AES s-box	[RP10]	832	18
2.	AES s-box	[KHL11]	594	24
3.	DES s-box	Simple version in [RDP08]	1045	69
4.	DES s-box	Improved version in [RDP08]	652	39
5.	DES s-box	new scheme	7000	78
6.	PRESENT s-box	Simple Version [RDP08]	277	21
7.	PRESENT s-box	Improved Version [RDP08]	284	15
8.	PRESENT s-box	new scheme	400	31
		Third Order Masking		
1.	AES s-box	[RP10]	1905	28
2.	AES s-box	[KHL11]	965	38
3.	DES s-box	new scheme	10500	108
4.	PRESENT s-box	new scheme	630	44

Open Issues

- Find more efficient methods for random s-boxes

Open Issues

- Find more efficient methods for random s-boxes
- Find faster scheme for specific s-boxes
  - *e.g.* DES s-boxes

Open Issues

- Find more efficient methods for random s-boxes
- Find faster scheme for specific s-boxes
  - *e.g.* DES s-boxes
- Extend the approach to smaller fields
  - Mult. on $\mathrm{GF}(2^4)$ more efficient than on $\mathrm{GF}(2^8)$ in software
  - Hardware masking complexity related to mult. on $\mathrm{GF}(2)$

Open Issues

- Find more efficient methods for random s-boxes
- Find faster scheme for specific s-boxes
  - *e.g.* DES s-boxes
- Extend the approach to smaller fields
  - Mult. on $\mathrm{GF}(2^4)$ more efficient than on $\mathrm{GF}(2^8)$ in software
  - Hardware masking complexity related to mult. on $\mathrm{GF}(2)$

Open Issues

- Find more efficient methods for random s-boxes
- Find faster scheme for specific s-boxes
  - *e.g.* DES s-boxes
- Extend the approach to smaller fields
  - Mult. on $\mathrm{GF}(2^4)$ more efficient than on $\mathrm{GF}(2^8)$ in software
  - Hardware masking complexity related to mult. on $\mathrm{GF}(2)$
- Find families of s-boxes with good cryptographic criteria and small masking complexity