Analysis and Improvement of the Generic Higher Order Masking Scheme of FSE 2012

Arnab Roy and Srinivas Vivek

UNIVERSITÉ DU LUXEMBOURG

August 23, 2013

Outline

Outline

Higher-Order Masking

- Counter measure against side-channel attacks
- Complexity of the attack increases exponentially with the masking order
- Secret variable is split into $d+1$ variables

$$x = x_0 + x_1 + .. + x_d$$

- Affine functions are easy to mask:

$$\mathcal{A}(x_0) + \mathcal{A}(x_1) + \ldots + \mathcal{A}(x_d) = \mathcal{A}(x)$$

- For a non-linear function: $y = \mathcal{G}(x)$

$$(y_0, \ldots, y_d) \leftarrow \mathcal{G}(x_0, \ldots, x_d)$$

Masking S-box and Polynomial evaluation

- A generic method proposed by Carlet-Goubin-Prouff-Quisquater-Rivain in FSE'12, for any order and any S-box
- S-box $S(x) = \sum_{i=0}^{2^n-1} A_i x^i$ over $\mathbb{F}_{2^n}$, where $A_i \in \mathbb{F}_{2^n}$
- Shares for $S(b)$ are obtained by evaluating the polynomial with b_j
- Masking of S-box is achieved by masking non-linear multiplications using ISW [Ishai-Sahai-Wagner CRYPTO'03] scheme
- Two methods for efficient evaluation of polynomials: Cyclotomic class, Parity Split [CGPQR12]

Relation to Addition Chain

- Example: In $\mathbb{F}_{2^4}$, x^{14} $(= x^8 \cdot x^4 \cdot x^2)$

Relation to Addition Chain

- Example: In $\mathbb{F}_{2^4}$, x^{14} $(= x^8 \cdot x^4 \cdot x^2)$
- A structured way: (Cyclotomic Class) [CGPQR12]

$$C(\alpha) = \{\alpha \cdot 2^i \mod (2^n - 1) : i = 0, 1, .., n-1\}$$

κ	Cyclotomic classes
0	$C_0 = \{0\}$, $C_1 = \{1, 2, 4, 8\}$
1	$C_3 = \{3, 6, 12, 9\}$, $C_5 = \{5, 10\}$
2	$C_7 = \{7, 14, 13, 11\}$

Relation to Addition Chain

- Example: In $\mathbb{F}_{2^4}$, x^{14} $(= x^8 \cdot x^4 \cdot x^2)$
- A structured way: (Cyclotomic Class) [CGPQR12]

$$C(\alpha) = \{\alpha \cdot 2^i \mod (2^n - 1) : i = 0, 1, .., n-1\}$$

κ	Cyclotomic classes
0	$C_0 = \{0\}$, $C_1 = \{1, 2, 4, 8\}$
1	$C_3 = \{3, 6, 12, 9\}$, $C_5 = \{5, 10\}$
2	$C_7 = \{7, 14, 13, 11\}$

- 14 has chains $\{8, 4, 2\}$ and $\{8, 6\}$
- **Shortest** *Cyclotomic Class*-addition chain is optimal for x^α

Outline

- Introduction
  - Background and Previous work
- Our Analysis
  - Analysis of CC-Addition Chain
  - Formalization of Masking Complexity
  - New Bounds
- Improved Method
  - A General Description
  - DES S-box
  - Masking Method
  - Other S-boxes

Outline

Analysis of CC-Addition Chain

- For a fixed $\mathbb{F}_{2^n}$, $m_n(\alpha)$ denotes the length of a shortest CC-addition chain
- (**Lower Bound**) $m_n(\alpha) \geq log_2(\nu(\alpha))$
- We use this later to give new bounds on Masking Complexity
- "For fixed n, x^{2^n-2} has maximum $m_n(\alpha)$" [CGPQR'12] NOT TRUE

Analysis (contd.)

- Monotonicity of $m_n(\alpha)$ w.r.t. n : Can we gain in a subfield ($\mathbb{F}_\ell \subset \mathbb{F}_{2^n}$) or in a super field ($\mathbb{F}_\ell \supset \mathbb{F}_{2^n}$) ?

Analysis (contd.)

- Monotonicity of $m_n(\alpha)$ w.r.t. n : Can we gain in a subfield ($\mathbb{F}_\ell \subset \mathbb{F}_{2^n}$) or in a super field ($\mathbb{F}_\ell \supset \mathbb{F}_{2^n}$) ?
- *In general*, $m_n(\alpha)$ may increase or decrease with the change of field $\mathbb{F}_{2^n}$.
- Example: $m_5(23) = 2$, $m_6(23) = 3$. Also $m_7(83) = 3$, $m_7(83) = 2$

Analysis (contd.)

- Monotonicity of $m_n(\alpha)$ w.r.t. n : Can we gain in a subfield ($\mathbb{F}_\ell \subset \mathbb{F}_{2^n}$) or in a super field ($\mathbb{F}_\ell \supset \mathbb{F}_{2^n}$) ?
- *In general*, $m_n(\alpha)$ may increase or decrease with the change of field $\mathbb{F}_{2^n}$.
- Example: $m_5(23) = 2$, $m_6(23) = 3$. Also $m_7(83) = 3$, $m_7(83) = 2$
- However, it may be useful to work in a subfield

Proposition

If $n|q$ and $\lceil \log_2(\alpha + 2) \rceil \leq n \leq q$, then $m_n(\alpha) \leq m_q(\alpha)$.

Outline

Non-linear (Masking) Complexity

Definition

A $\mathbb{F}_{2^n}$- **polynomial chain** $\mathcal{S}$, for a polynomial $P(x) \in \mathbb{F}_{2^n}[x]$ is defined as

$$\lambda_{-1} = 1,\ \lambda_1 = x,\ \ldots\ ,\ \lambda_r = P(x)$$

where

$$\lambda_i = \begin{cases} \lambda_j + \lambda_k & -1 \leq j, k < i, \\ \lambda_j \cdot \lambda_k & -1 \leq j, k < i, \\ \alpha_i \odot \lambda_j & -1 \leq j < i,\ \alpha_i \text{ is a scalar}, \\ \lambda_j^2 & -1 \leq j < i. \end{cases}$$

The **minimum** number of *non-linear* multiplications over all such chains $\mathcal{S}$ is the *non-linear* complexity, denoted as $\mathcal{M}(P(x))$

Masking Complexity

- Let Q be the polynomial for a given S-box, then $\mathcal{M}(Q(x))$ is the *masking complexity* (MC).

- Is the above formalization of masking complexity well-defined ? YES

Theorem

Masking complexity of an $\mathbb{S}$*-box is invariant w.r.t. to field representation*

Outline

Relation to CC-addition chain

- The notion of $\mathbb{F}_{2^n}$- **polynomial chain** is more general
- Can be reduced to the notion of CC-addition chain when given polynomial is power function
- $P(x) := \sum_{i=0}^{2^n-1} a_i x^i$, then $\mathcal{M}(P(x)) \geq \max_{\substack{0<i<2^n-1 \\ a_i \neq 0}} m_n(i)$.
- MC of DES is at least 3 and MC of PRESENT is at least 2.

Outline

Introduction

- Background and Previous work

Our Analysis

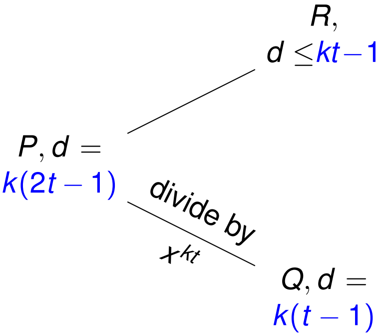
- Analysis of CC-Addition Chain
- Formalization of Masking Complexity
- New Bounds

Improved Method

- A General Description
- DES S-box
- Masking Method
- Other S-boxes

Outline

Polynomial evaluation: A general strategy



Polynomial evaluation: A general strategy

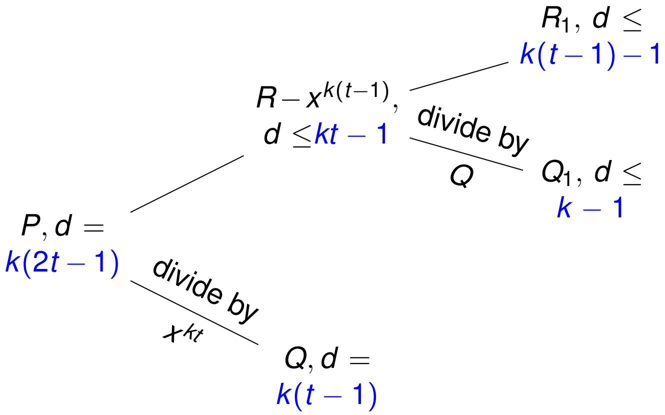
$R - x^{k(t-1)}$,
$d \leq kt - 1$

$P, d =$
$k(2t - 1)$

divide by x^{kt}

$Q, d =$
$k(t - 1)$

Polynomial evaluation: A general strategy



Non-linear multiplications

- $P(x) = (x^{kt} + Q_1(x)) \cdot Q(x) + x^{k(t-1)} + R_1(x)$
- Apply this technique to Q and $x^{k(t-1)} + R$ recursively
- Assume $t = 2^{i-1}$, then after evaluating $x^2, x^3, \ldots, x^k$, we can evaluate $(x^k)^t$ easily
- Number of nonlinear multiplications:

$$\mathcal{T}(k(2^i - 1)) = 2\mathcal{T}(k(2^{i-1} - 1)) + 1$$

Outline

Example: DES

$R, d \leq 35$

$P_{DES}, d = 62$

$9(2 \cdot 2^2 - 1)$

divide by x^{36}

$Q, d = 26$

Example: DES

$R + x^{27}$

$d \leq 35$

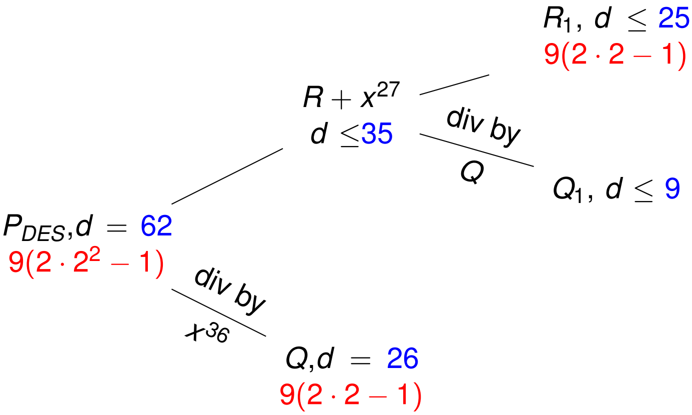
$P_{DES}, d = 62$

$9(2 \cdot 2^2 - 1)$

divide by x^{36}

$Q, d = 26$

Example: DES


$R_1,\ d \le 25$
$9(2 \cdot 2 - 1)$
$R + x^{27}$
$d \le 35$
div by
Q
$Q_1,\ d \le 9$
$P_{DES}, d = 62$
$9(2 \cdot 2^2 - 1)$
div by
x^{36}
$Q, d = 26$
$9(2 \cdot 2 - 1)$

Example: DES

$R_1,\ d \leq 25$

$9(2 \cdot 2 - 1)$

$R + x^{27}$

$d \leq 35$

div by Q

$Q_1,\ d \leq 9$

$P_{DES}, d = 62$

$9(2 \cdot 2^2 - 1)$

div by x^{36}

$Q, d = 26$

$9(2 \cdot 2 - 1)$

$$P_{DES}(x) = (x^{36} + Q_1(x)) \cdot Q(x) + x^{27} + R_1(x)$$

Number of Non-linear multiplications for DES

- Applying this recursively to R_1 and Q

$$P_{DES} = (x^{36} + Q_1(x)) \cdot \Big(((x^{18} + r_1(x)) \cdot q_1(x)) + (x^9 + s_1(x))\Big)$$
$$+ \Big((x^{18} + r_2(x)) \cdot q_2(x) + (x^9 + s_2(x))\Big)$$

Number of Non-linear multiplications for DES

- Applying this recursively to R_1 and Q

$$P_{DES} = (x^{36} + Q_1(x)) \cdot \Big(((x^{18} + r_1(x)) \cdot q_1(x)) + (x^9 + s_1(x)) \Big) \\ + \Big((x^{18} + r_2(x)) \cdot q_2(x) + (x^9 + s_2(x)) \Big)$$

- Number of non-linear multiplications: 4 (computing $x, x^2, \ldots, x^9$) + 3 = 7

Outline

Masking Method

- Express the polynomial $S(x) = \sum_{i=0}^{2^n-1} a_i\, x^i$ as function of polynomials of degree $\leq k$ and $(x^k)^{2^i}$
- Evaluate $x, x^2, \ldots, x^k$ with the $d+1$ shares by masking the non-linear multiplications
- Combine the polynomials by masking any non-linear multiplications involved

Outline

Comparison

- We applied this technique to other S-boxes

	AES	CAMELLIA	CLEFIA	DES	PRESENT	SERPENT
Cyclotomic	4	33	33	11	3	3
Parity-Split	6	22	22	10	4	4
Our Result	**4**	**15**	**16** (S_0)/**15** (S_1)	**7**	**3**	**3**