Thwarting Higher-Order SCA with Additive and Multiplicative Masking

Laurie Genelle[1], Emmanuel Prouff[1] and Michael Quisquater[2]
[1] Oberthur Technologies
[2] University of Versailles

Context

Context

Cryptographic Algorithm: **perfect** from a logical point of view **but** processing leaks information

Context

Cryptographic Algorithm: **perfect** from a logical point of view **but** processing leaks information

Side Channel Analysis (SCA): analyzes the physical leakage to recover the secret

Context

Cryptographic Algorithm: **perfect** from a logical point of view **but** processing leaks information

Side Channel Analysis (SCA): analyzes the physical leakage to recover the secret

Countermeasure?

Context

Cryptographic Algorithm: **perfect** from a logical point of view **but** processing leaks information

Side Channel Analysis (SCA): analyzes the physical leakage to recover the secret

Masking/Secret Sharing: renders any intermediate value independent from the secret . . . without modifying algorithm's results

Context

Cryptographic Algorithm: **perfect** from a logical point of view **but** processing leaks information

Side Channel Analysis (SCA): analyzes the physical leakage to recover the secret

Masking/Secret Sharing: renders any intermediate value independent from the secret . . . without modifying algorithm's results

Order?

Context

Cryptographic Algorithm: **perfect** from a logical point of view **but** processing leaks information

Side Channel Analysis (SCA): analyzes the physical leakage to recover the secret

Masking/Secret Sharing: renders any intermediate value independent from the secret . . . without modifying algorithm's results

d^{th}-order SCA (dO-SCA): d intermediate values targeted

Context

Cryptographic Algorithm: **perfect** from a logical point of view **but** processing leaks information

Side Channel Analysis (SCA): analyzes the physical leakage to recover the secret

Masking/Secret Sharing: renders any intermediate value independent from the secret ... without modifying algorithm's results

d^{th}-order SCA (dO-SCA): d intermediate values targeted

d^{th}-order Masking: renders any vector of d intermediate values independent from the secret

d^{th}-order masking:

- Every secret-dependent variable x is shared into $d+1$ variables:

$$x = x_0 \perp {x_1}^{-1} \perp \ldots \perp {x_d}^{-1} \qquad (1)$$

- A group operation $\perp$

d^{th}-Order Masking

d^{th}-order masking:

- Every secret-dependent variable x is shared into $d+1$ variables:

$$x = x_0 \perp x_1{}^{-1} \perp \ldots \perp x_d{}^{-1} \qquad (1)$$

- A group operation $\perp$
- The masks $(x_i)_{i \geq 1}$ are randomly generated

d^{th}-Order Masking

d^{th}-order masking:

- Every secret-dependent variable x is shared into $d+1$ variables:

$$x = x_0 \perp {x_1}^{-1} \perp \ldots \perp {x_d}^{-1} \qquad (1)$$

- A group operation $\perp$
- The masks $(x_i)_{i \geq 1}$ are randomly generated
- The masked variable: $x_0 \leftarrow x \perp x_1 \perp \ldots \perp x_d$

d^{th}-Order Masking

d^{th}-order masking:

- Every secret-dependent variable x is shared into $d+1$ variables:

$$x = x_0 \perp {x_1}^{-1} \perp \ldots \perp {x_d}^{-1} \qquad (1)$$

- A group operation $\perp = \{\oplus\}$
- The masks $(x_i)_{i \geq 1}$ are randomly generated
- The masked variable: $x_0 \leftarrow x \perp x_1 \perp \ldots \perp x_d$

  Additive $\longrightarrow$ $x_0 \leftarrow x \oplus x_1 \oplus \ldots \oplus x_d$

d^{th}-Order Masking

d^{th}-order masking:

- Every secret-dependent variable x is shared into $d+1$ variables:

$$x = x_0 \perp {x_1}^{-1} \perp \ldots \perp {x_d}^{-1} \qquad (1)$$

- A group operation $\perp = \{\oplus, \otimes\}$

- The masks $(x_i)_{i \geq 1}$ are randomly generated

- The masked variable: $x_0 \leftarrow x \perp x_1 \perp \ldots \perp x_d$

  Additive $\longrightarrow$ $x_0 \leftarrow x \oplus x_1 \oplus \ldots \oplus x_d$

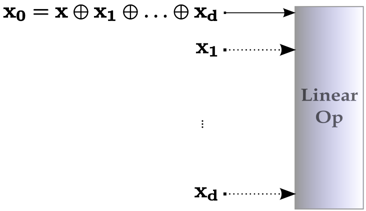
  Multiplicative $\longrightarrow$ $x_0 \leftarrow x \otimes x_1 \otimes \ldots \otimes x_d$, $\quad x, x_i \neq 0$

Masking Propagation

Additive masking and linear operation.

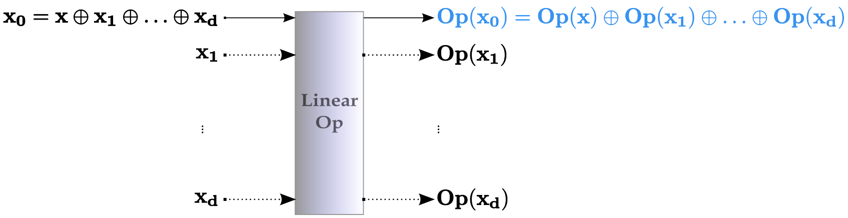
$\mathbf{x_0} = \mathbf{x} \oplus \mathbf{x_1} \oplus \ldots \oplus \mathbf{x_d}$

Additive masking and linear operation.



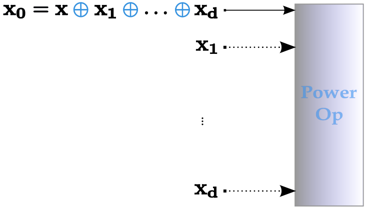
Masking Propagation

Additive masking and linear operation.



Masking Propagation

Additive masking and power operation.



Masking Propagation

Additive masking and power operation.

$$\mathbf{x_0 = x \oplus x_1 \oplus \ldots \oplus x_d} \longrightarrow \text{Power Op} \longrightarrow \mathbf{Op(x_0) \neq Op(x) \oplus Op(x_1) \oplus \ldots \oplus Op(x_d)}$$

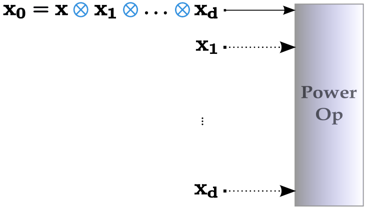
$$\mathbf{x_1} \dashrightarrow \text{Power Op} \dashrightarrow \mathbf{Op(x_1)}$$

$$\vdots \qquad\qquad \vdots$$

$$\mathbf{x_d} \dashrightarrow \text{Power Op} \dashrightarrow \mathbf{Op(x_d)}$$

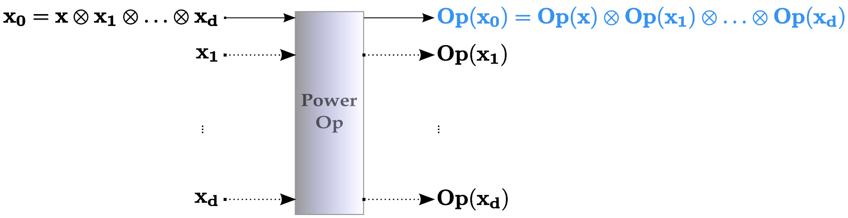
Masking Propagation

Multiplicative masking and power operation.



Masking Propagation

Multiplicative masking and power operation.



How to apply masking on block ciphers implementations which mix affine transformations and power functions?

Application

How to apply masking on block ciphers implementations which mix affine transformations and power functions?

Related Works for $d \geq 2$:

$d = 2$: [RivainDottaxProuff08]
[SchrammPaar06]
$d > 2$: [RivainProuff10]

Application

How to apply masking on block ciphers implementations which mix affine transformations and power functions?

Related Works for $d \geq 2$:

$$\left.\begin{array}{ll} d = 2: & \text{[RivainDottaxProuff08]} \\ & \text{[SchrammPaar06]} \\ d > 2: & \text{[RivainProuff10]} \end{array}\right\} \text{additive masking}$$

Application

How to apply masking on block ciphers implementations which mix affine transformations and power functions?

Related Works for $d \geq 2$:

$$\left.\begin{array}{ll} d = 2: & \text{[RivainDottaxProuff08]} \\ & \text{[SchrammPaar06]} \\ d > 2: & \text{[RivainProuff10]} \end{array}\right\} \text{additive masking}$$

Our Approach: use multiplicative masking for power functions and additive masking for affine transformations

Application

How to apply masking on block ciphers implementations which mix affine transformations and power functions?

Related Works for $d \geq 2$:

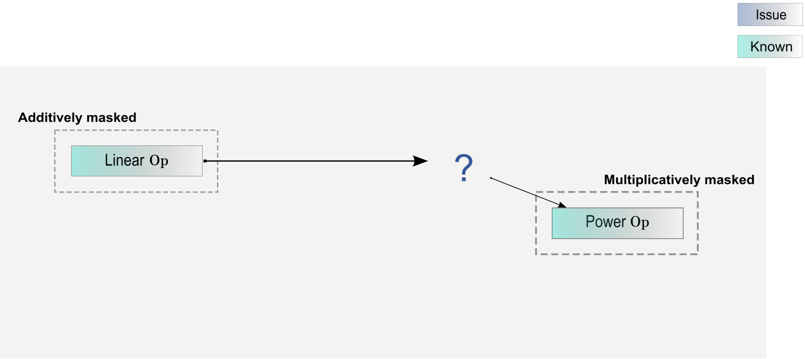
$$\left.\begin{array}{ll} d = 2: & \text{[RivainDottaxProuff08]} \\ & \text{[SchrammPaar06]} \\ d > 2: & \text{[RivainProuff10]} \end{array}\right\} \text{additive masking}$$

Our Approach: use multiplicative masking for power functions and additive masking for affine transformations

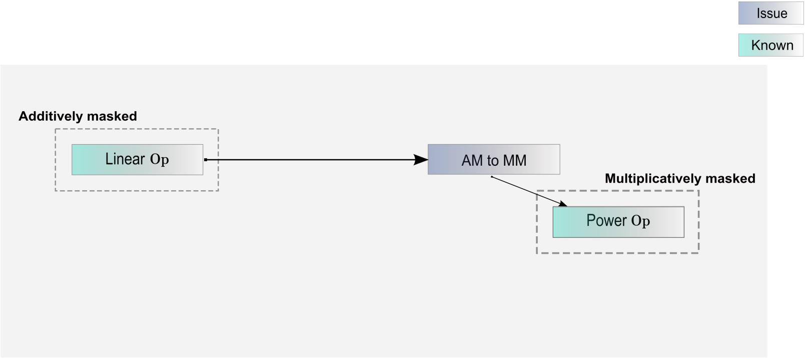
[GenelleProuffQuisquater10] for $d = 1$

General Processing

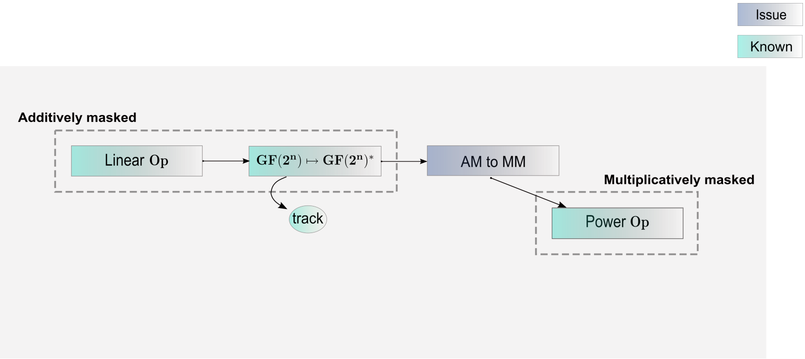
General Processing



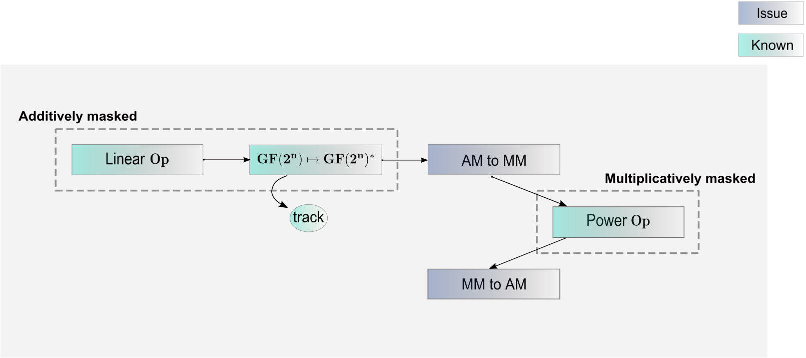
General Processing



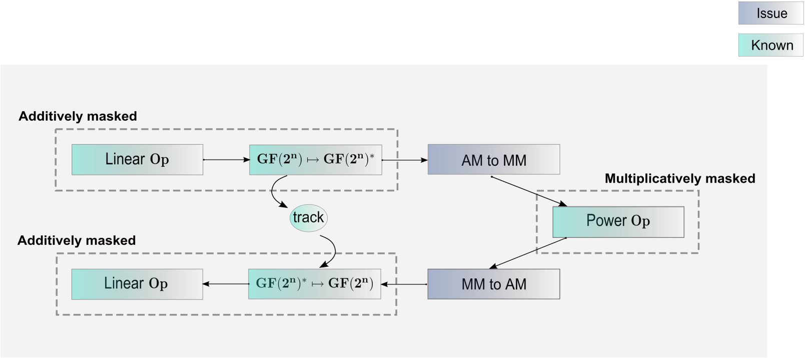
General Processing



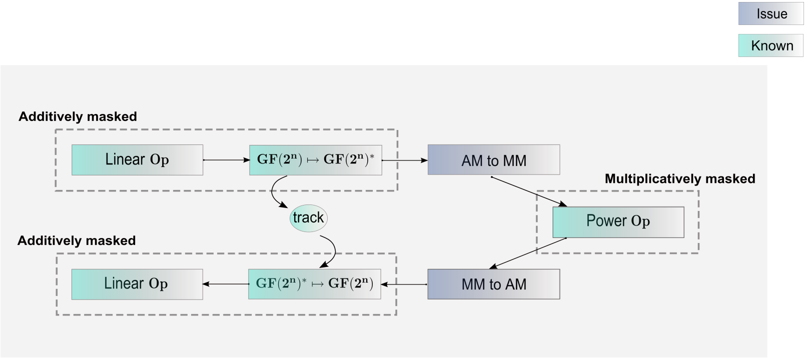
General Processing



General Processing



General Processing



Mapping from $GF(2^n)$ into $GF(2^n)^*$ (and conversely):
[GenelleProuffQuisquater2011]

Issue

Conversion from additive to multiplicative masking (`AMtoMM`), which is d^{th}-**order secure**

Issue

Conversion from additive to multiplicative masking (`AMtoMM`), which is $d^{\mathbf{th}}$-**order secure**

Notations:

- Additive masks $x_1, \ldots, x_d$ ($\mathcal{S}_{AM}$)
- Multiplicative masks $z_1, \ldots, z_d$ ($\mathcal{S}_{MM}$)

Issue

Conversion from additive to multiplicative masking (`AMtoMM`), which is d^{th}-**order secure**

Notations:

- Additive masks $x_1, \ldots, x_d$ ($\mathcal{S}_{AM}$)
- Multiplicative masks $z_1, \ldots, z_d$ ($\mathcal{S}_{MM}$)

Conversion from additive to multiplicative masking (AMtoMM), which is d^{th}**-order secure**

Notations:

- Additive masks $x_1, \ldots, x_d$ ($\mathcal{S}_{AM}$)
- Multiplicative masks $z_1, \ldots, z_d$ ($\mathcal{S}_{MM}$)

Issue

Conversion from additive to multiplicative masking (AMtoMM), which is d^{th}-**order secure**

Notations:

- Additive masks $x_1, \ldots, x_d$ ($\mathcal{S}_{AM}$)
- Multiplicative masks $z_1, \ldots, z_d$ ($\mathcal{S}_{MM}$)

Goal:

Input **Output**

$$\begin{array}{l} \mathbf{x_0 = x \oplus x_1 \oplus \ldots \oplus x_d}, \\ \mathcal{S}_{\mathbf{AM}} = \{\mathbf{x_1}, \ldots, \mathbf{x_d}\}, \\ \mathcal{S}_{\mathbf{MM}} = \emptyset \end{array} \xrightarrow{\texttt{AMtoMM}} \begin{array}{l} \mathbf{z_0 = x \otimes z_1 \otimes \ldots \otimes z_d}, \\ \mathcal{S}_{\mathbf{AM}} = \emptyset, \\ \mathcal{S}_{\mathbf{MM}} = \{\mathbf{z_1}, \ldots, \mathbf{z_d}\} \end{array}$$

Issue

Conversion from additive to multiplicative masking (AMtoMM), which is d^{th}-**order secure**

Notations:

- Additive masks $x_1, \ldots, x_d$ ($\mathcal{S}_{AM}$)
- Multiplicative masks $z_1, \ldots, z_d$ ($\mathcal{S}_{MM}$)

Goal:

Input **Output**

$$\begin{array}{l} \mathbf{x_0} = \mathbf{x} \oplus \mathbf{x_1} \oplus \ldots \oplus \mathbf{x_d}, \\ \mathcal{S}_{\mathbf{AM}} = \{\mathbf{x_1}, \ldots, \mathbf{x_d}\}, \\ \mathcal{S}_{\mathbf{MM}} = \emptyset \end{array} \xrightarrow{\texttt{AMtoMM}} \begin{array}{l} \mathbf{z_0} = \mathbf{x} \otimes \mathbf{z_1} \otimes \ldots \otimes \mathbf{z_d}, \\ \mathcal{S}_{\mathbf{AM}} = \emptyset, \\ \mathcal{S}_{\mathbf{MM}} = \{\mathbf{z_1}, \ldots, \mathbf{z_d}\} \end{array}$$

Issue

Conversion from additive to multiplicative masking (`AMtoMM`), which is d^{th}**-order secure**

Notations:

- Additive masks $x_1, \ldots, x_d$ ($\mathcal{S}_{AM}$)
- Multiplicative masks $z_1, \ldots, z_d$ ($\mathcal{S}_{MM}$)

Goal:

Input **Output**

$$\begin{array}{l} \mathbf{x_0} = \mathbf{x} \oplus \mathbf{x_1} \oplus \ldots \oplus \mathbf{x_d}, \\ \mathcal{S}_{\mathbf{AM}} = \{\mathbf{x_1}, \ldots, \mathbf{x_d}\}, \\ \mathcal{S}_{\mathbf{MM}} = \emptyset \end{array} \xrightarrow{\mathtt{AMtoMM}} \begin{array}{l} \mathbf{z_0} = \mathbf{x} \otimes \mathbf{z_1} \otimes \ldots \otimes \mathbf{z_d}, \\ \mathcal{S}_{\mathbf{AM}} = \emptyset, \\ \mathcal{S}_{\mathbf{MM}} = \{\mathbf{z_1}, \ldots, \mathbf{z_d}\} \end{array}$$

An Intuitive Attempt

Masked value	Additive masks ($\mathcal{S}_{\mathrm{AM}}$)		Multiplicative masks ($\mathcal{S}_{\mathrm{MM}}$)
$\mathbf{x_0}$	$\mathbf{x_1}$	$\mathbf{x_2}$	$\emptyset$

An Intuitive Attempt

Masked value	Additive masks ($\mathcal{S}_{\mathrm{AM}}$)		Multiplicative masks ($\mathcal{S}_{\mathrm{MM}}$)
x_0	x_1	x_2	$\emptyset$
$\mathbf{x_0} \otimes \mathbf{z_1}$	$\mathbf{x_1} \otimes \mathbf{z_1}$	$\mathbf{x_2} \otimes \mathbf{z_1}$	

An Intuitive Attempt

Masked value	Additive masks ($\mathcal{S}_{\mathrm{AM}}$)		Multiplicative masks ($\mathcal{S}_{\mathrm{MM}}$)
x_0	x_1	x_2	$\emptyset$
$\mathbf{x_0 \otimes z_1}$	$\mathbf{x_1 \otimes z_1}$	$\mathbf{x_2 \otimes z_1}$	$\mathbf{z_1}$

An Intuitive Attempt

Masked value	Additive masks ($\mathcal{S}_{\mathrm{AM}}$)		Multiplicative masks ($\mathcal{S}_{\mathrm{MM}}$)
x_0	x_1	x_2	$\emptyset$
$\mathbf{x_0} \otimes \mathbf{z_1}$	$\mathbf{x_1} \otimes \mathbf{z_1}$	$\mathbf{x_2} \otimes \mathbf{z_1}$	$\mathbf{z_1}$

$\oplus$

An Intuitive Attempt

Masked value	Additive masks ($\mathcal{S}_{\mathrm{AM}}$)		Multiplicative masks ($\mathcal{S}_{\mathrm{MM}}$)
$\mathbf{x_0}$	$\mathbf{x_1}$	$\mathbf{x_2}$	$\emptyset$
$\mathbf{x_0} \otimes \mathbf{z_1}$	$\mathbf{x_1} \otimes \mathbf{z_1}$	$\mathbf{x_2} \otimes \mathbf{z_1}$	$\mathbf{z_1}$
$(\mathbf{x_0} \oplus \mathbf{x_1}) \otimes \mathbf{z_1}$			

An Intuitive Attempt

Masked value	Additive masks ($\mathcal{S}_{\mathrm{AM}}$)		Multiplicative masks ($\mathcal{S}_{\mathrm{MM}}$)
x_0	x_1	x_2	$\emptyset$
$x_0 \otimes z_1$	$x_1 \otimes z_1$	$x_2 \otimes z_1$	z_1
$\mathbf{(x_0 \oplus x_1) \otimes z_1}$		$\mathbf{x_2 \otimes z_1}$	$\mathbf{z_1}$

An Intuitive Attempt

Masked value	Additive masks ($\mathcal{S}_{\mathrm{AM}}$)		Multiplicative masks ($\mathcal{S}_{\mathrm{MM}}$)
x_0	x_1	x_2	$\emptyset$
$x_0 \otimes z_1$	$x_1 \otimes z_1$	$x_2 \otimes z_1$	z_1
$(x_0 \oplus x_1) \otimes z_1$		$x_2 \otimes z_1$	z_1
$\mathbf{(x_0 \oplus x_1) \otimes z_1 \otimes z_2}$		$\mathbf{x_2 \otimes z_1 \otimes z_2}$	$\mathbf{z_1}$

An Intuitive Attempt

Masked value	Additive masks ($\mathcal{S}_{\mathrm{AM}}$)		Multiplicative masks ($\mathcal{S}_{\mathrm{MM}}$)	
x_0	x_1	x_2	$\emptyset$	
$x_0 \otimes z_1$	$x_1 \otimes z_1$	$x_2 \otimes z_1$	z_1	
$(x_0 \oplus x_1) \otimes z_1$		$x_2 \otimes z_1$	z_1	
$\mathbf{(x_0 \oplus x_1) \otimes z_1 \otimes z_2}$		$\mathbf{x_2 \otimes z_1 \otimes z_2}$	$\mathbf{z_1}$	$\mathbf{z_2}$

An Intuitive Attempt

Masked value	Additive masks ($\mathcal{S}_{\mathrm{AM}}$)		Multiplicative masks ($\mathcal{S}_{\mathrm{MM}}$)	
x_0	x_1	x_2	$\emptyset$	
$x_0 \otimes z_1$	$x_1 \otimes z_1$	$x_2 \otimes z_1$	z_1	
$(x_0 \oplus x_1) \otimes z_1$		$x_2 \otimes z_1$	z_1	
$\mathbf{(x_0 \oplus x_1) \otimes z_1 \otimes z_2}$		$\mathbf{x_2 \otimes z_1 \otimes z_2}$	$\mathbf{z_1}$	$\mathbf{z_2}$

$\oplus$

An Intuitive Attempt

Masked value	Additive masks ($\mathcal{S}_{\mathrm{AM}}$)		Multiplicative masks ($\mathcal{S}_{\mathrm{MM}}$)	
x_0	x_1	x_2	$\emptyset$	
$x_0 \otimes z_1$	$x_1 \otimes z_1$	$x_2 \otimes z_1$	z_1	
$(x_0 \oplus x_1) \otimes z_1$		$x_2 \otimes z_1$	z_1	
$(x_0 \oplus x_1) \otimes z_1 \otimes z_2$		$x_2 \otimes z_1 \otimes z_2$	z_1	z_2
$\mathbf{(x_0 \oplus x_1 \oplus x_2) \otimes z_1 \otimes z_2}$				

An Intuitive Attempt

Masked value	Additive masks ($\mathcal{S}_{\mathrm{AM}}$)		Multiplicative masks ($\mathcal{S}_{\mathrm{MM}}$)	
x_0	x_1	x_2	$\emptyset$	
$x_0 \otimes z_1$	$x_1 \otimes z_1$	$x_2 \otimes z_1$	z_1	
$(x_0 \oplus x_1) \otimes z_1$		$x_2 \otimes z_1$	z_1	
$(x_0 \oplus x_1) \otimes z_1 \otimes z_2$		$x_2 \otimes z_1 \otimes z_2$	z_1	z_2
$\mathbf{(x_0 \oplus x_1 \oplus x_2) \otimes z_1 \otimes z_2}$	$\emptyset$		$\mathbf{z_1}$	$\mathbf{z_2}$

An Intuitive Attempt

Masked value	Additive masks ($\mathcal{S}_{\mathrm{AM}}$)		Multiplicative masks ($\mathcal{S}_{\mathrm{MM}}$)	
x_0	x_1	x_2	$\emptyset$	
$x_0 \otimes z_1$	$x_1 \otimes z_1$	$x_2 \otimes z_1$	z_1	
$(x_0 \oplus x_1) \otimes z_1$		$x_2 \otimes z_1$	z_1	
$(x_0 \oplus x_1) \otimes z_1 \otimes z_2$		$x_2 \otimes z_1 \otimes z_2$	z_1	z_2
$(x_0 \oplus x_1 \oplus x_2) \otimes z_1 \otimes z_2$	$\emptyset$		$\mathbf{z_1}$	$\mathbf{z_2}$
$\mathbf{x \otimes z_1 \otimes z_2}$				

Three intermediate values:

- x_d,
- $x_d \otimes z_1 \otimes \ldots \otimes z_d$
- $x \otimes z_1 \otimes \ldots \otimes z_d$

Three intermediate values:

- x_d,
- $x_d \otimes z_1 \otimes \ldots \otimes z_d \longrightarrow z_1 \otimes \ldots \otimes z_d$
- $x \otimes z_1 \otimes \ldots \otimes z_d$

Three intermediate values:

- x_d,
- $x_d \otimes z_1 \otimes \ldots \otimes z_d \longrightarrow z_1 \otimes \ldots \otimes z_d$
- $x \otimes z_1 \otimes \ldots \otimes z_d \longrightarrow x$

Three intermediate values:

- x_d,
- $x_d \otimes z_1 \otimes \ldots \otimes z_d \longrightarrow z_1 \otimes \ldots \otimes z_d$
- $x \otimes z_1 \otimes \ldots \otimes z_d \longrightarrow x$

Conversion algorithm is secure when $d = 1$ or $d = 2$, but not when $d > 2$.

Security

Three intermediate values:

- x_d,
- $x_d \otimes z_1 \otimes \ldots \otimes z_d \longrightarrow z_1 \otimes \ldots \otimes z_d$
- $x \otimes z_1 \otimes \ldots \otimes z_d \longrightarrow x$

Conversion algorithm is secure when $d = 1$ or $d = 2$, but not when $d > 2$.

Idea: mask at order 1 some additional intermediate values in such that propagation stays straightforward.

Our Proposal (AMtoMM)

Masked value	Additive masks ($\mathcal{S}_{\mathrm{AM}}$)		Multiplicative masks ($\mathcal{S}_{\mathrm{MM}}$)
$\mathbf{x_0}$	$\mathbf{x_1}$	$\mathbf{x_2}$	$\emptyset$

Our Proposal (AMtoMM)

Masked value	Additive masks ($\mathcal{S}_{\mathrm{AM}}$)		Multiplicative masks ($\mathcal{S}_{\mathrm{MM}}$)
x_0	x_1	x_2	$\emptyset$
$\mathbf{x_0} \otimes \mathbf{z_1}$	$\mathbf{x_1} \otimes \mathbf{z_1}$	$\mathbf{x_2} \otimes \mathbf{z_1}$	$\mathbf{z_1}$

Our Proposal (AMtoMM)

Masked value	Additive masks ($\mathcal{S}_{\mathrm{AM}}$)		Multiplicative masks ($\mathcal{S}_{\mathrm{MM}}$)
x_0	x_1	x_2	$\emptyset$
$x_0 \otimes z_1$	$\mathbf{x_1 \otimes z_1}$	$x_2 \otimes z_1$	z_1
	$\mathbf{x_1 \otimes z_1 \oplus m_1}$ $\mathbf{m_1}$		

Our Proposal (AMtoMM)

Masked value	Additive masks ($\mathcal{S}_{\mathrm{AM}}$)			Multiplicative masks ($\mathcal{S}_{\mathrm{MM}}$)
x_0	x_1		x_2	$\emptyset$
$x_0 \otimes z_1$	$x_1 \otimes z_1$		$x_2 \otimes z_1$	z_1
$\mathbf{x_0 \otimes z_1}$	$\mathbf{x_1 \otimes z_1 \oplus m_1}$	$\mathbf{m_1}$	$\mathbf{x_2 \otimes z_1}$	$\mathbf{z_1}$

Our Proposal (AMtoMM)

Masked value	Additive masks ($\mathcal{S}_{\mathrm{AM}}$)			Multiplicative masks ($\mathcal{S}_{\mathrm{MM}}$)
x_0	x_1		x_2	$\emptyset$
$x_0 \otimes z_1$	$x_1 \otimes z_1$		$x_2 \otimes z_1$	z_1
$\mathbf{x_0 \otimes z_1} \xleftarrow{\oplus}$	$\mathbf{x_1 \otimes z_1 \oplus m_1}$	$\mathbf{m_1}$	$\mathbf{x_2 \otimes z_1}$	$\mathbf{z_1}$

Our Proposal (AMtoMM)

Masked value	**Additive masks** ($\mathcal{S}_{\mathrm{AM}}$)			**Multiplicative masks** ($\mathcal{S}_{\mathrm{MM}}$)
$\mathrm{x_0}$		$\mathrm{x_1}$	$\mathrm{x_2}$	$\emptyset$
$\mathrm{x_0 \otimes z_1}$		$\mathrm{x_1 \otimes z_1}$	$\mathrm{x_2 \otimes z_1}$	$\mathrm{z_1}$
$\mathrm{x_0 \otimes z_1}$	$\mathrm{x_1 \otimes z_1 \oplus m_1}$	$\mathrm{m_1}$	$\mathrm{x_2 \otimes z_1}$	$\mathrm{z_1}$
$\mathbf{(x_0 \oplus x_1) \otimes z_1 \oplus m_1}$				

Our Proposal (AMtoMM)

Masked value	Additive masks ($\mathcal{S}_{\mathrm{AM}}$)			Multiplicative masks ($\mathcal{S}_{\mathrm{MM}}$)
x_0		x_1	x_2	$\emptyset$
$x_0 \otimes z_1$		$x_1 \otimes z_1$	$x_2 \otimes z_1$	z_1
$x_0 \otimes z_1$	$x_1 \otimes z_1 \oplus m_1$	m_1	$x_2 \otimes z_1$	z_1
$\mathbf{(x_0 \oplus x_1) \otimes z_1 \oplus m_1}$		$\mathbf{m_1}$	$\mathbf{x_2 \otimes z_1}$	$\mathbf{z_1}$

Our Proposal (AMtoMM)

Masked value	Additive masks ($\mathcal{S}_{\mathrm{AM}}$)			Multiplicative masks ($\mathcal{S}_{\mathrm{MM}}$)	
x_0	x_1		x_2	$\emptyset$	
$x_0 \otimes z_1$	$x_1 \otimes z_1$		$x_2 \otimes z_1$	z_1	
$x_1 \otimes z_1$	$x_1 \otimes z_1 \oplus m_1$	m_1	$x_2 \otimes z_1$	z_1	
$\mathbf{(x_0 \oplus x_1) \otimes z_1 \otimes z_2 \oplus m_1 \otimes z_2}$		$\mathbf{m_1 \otimes z_2}$	$\mathbf{x_2 \otimes z_1 \otimes z_2}$	$\mathbf{z_1}$	$\mathbf{z_2}$

Our Proposal (AMtoMM)

Masked value	Additive masks ($\mathcal{S}_{\mathrm{AM}}$)			Multiplicative masks ($\mathcal{S}_{\mathrm{MM}}$)	
x_0	x_1		x_2	$\emptyset$	
$x_0 \otimes z_1$	$x_1 \otimes z_1$		$x_2 \otimes z_1$	z_1	
$x_0 \otimes z_1$	$x_1 \otimes z_1 \oplus m_1$	m_1	$x_2 \otimes z_1$	z_1	
$(x_0 \oplus x_1) \otimes z_1 \otimes z_2 \oplus m_1 \otimes z_2$		$m_1 \otimes z_2$	$x_2 \otimes z_1 \otimes z_2$	z_1	z_2
	$\oplus$				
	$\oplus$				

Our Proposal (AMtoMM)

Masked value	Additive masks ($\mathcal{S}_{\mathrm{AM}}$)			Multiplicative masks ($\mathcal{S}_{\mathrm{MM}}$)	
x_0	x_1		x_2	$\emptyset$	
$x_0 \otimes z_1$	$x_1 \otimes z_1$		$x_2 \otimes z_1$	z_1	
$x_0 \otimes z_1$	$x_1 \otimes z_1 \oplus m_1$	m_1	$x_2 \otimes z_1$	z_1	
$(x_0 \oplus x_1) \otimes z_1 \otimes z_2 \oplus m_1 \otimes z_2$		$m_1 \otimes z_2$	$x_2 \otimes z_1 \otimes z_2$	z_1	z_2
$\mathbf{(x_0 \oplus x_1 \oplus x_2) \otimes z_1 \otimes z_2}$					

Our Proposal (AMtoMM)

Masked value	Additive masks ($\mathcal{S}_{\mathrm{AM}}$)			Multiplicative masks ($\mathcal{S}_{\mathrm{MM}}$)	
x_0	x_1		x_2	$\emptyset$	
$x_0 \otimes z_1$	$x_1 \otimes z_1$		$x_2 \otimes z_1$	z_1	
$x_0 \otimes z_1$	$x_1 \otimes z_1 \oplus m_1$	m_1	$x_2 \otimes z_1$	z_1	
$(x_0 \oplus x_1) \otimes z_1 \otimes z_2 \oplus m_1 \otimes z_2$		$m_1 \otimes z_2$	$x_2 \otimes z_1 \otimes z_2$	z_1	z_2
$\mathbf{(x_0 \oplus x_1 \oplus x_2) \otimes z_1 \otimes z_2}$		$\emptyset$		$\mathbf{z_1}$	$\mathbf{z_2}$

Our Proposal (AMtoMM)

Masked value	Additive masks ($\mathcal{S}_{\mathrm{AM}}$)			Multiplicative masks ($\mathcal{S}_{\mathrm{MM}}$)	
x_0	x_1		x_2	$\emptyset$	
$x_0 \otimes z_1$	$x_1 \otimes z_1$		$x_2 \otimes z_1$	z_1	
$x_0 \otimes z_1$	$x_1 \otimes z_1 \oplus m_1$	m_1	$x_2 \otimes z_1$	z_1	
$(x_0 \oplus x_1) \otimes z_1 \otimes z_2 \oplus m_1 \otimes z_2$		$m_1 \otimes z_2$	$x_2 \otimes z_1 \otimes z_2$	z_1	z_2
$(x_0 \oplus x_1 \oplus x_2) \otimes z_1 \otimes z_2$		$\emptyset$		$\mathbf{z_1}$	$\mathbf{z_2}$
$\mathbf{x \otimes z_1 \otimes z_2}$					

Application to a known block cipher

Application to a known block cipher

AES:

- linear layers
- non-linear layer (s-box): composition of an extended multiplicative inverse in $GF(2^8)$ and an affine transformation

Application to a known block cipher

AES:

- linear layers
- non-linear layer (s-box): composition of an extended multiplicative inverse in $GF(2^8)$ and an affine transformation

Inverse: $x \mapsto x^{254}$ if $x \neq 0$, and equals 0 otherwise

Application to a known block cipher

AES:

- linear layers
- non-linear layer (s-box): composition of an extended multiplicative inverse in $GF(2^8)$ and an affine transformation

Inverse: $x \mapsto x^{254}$ if $x \neq 0$, and equals 0 otherwise

Sum-up: AES mixes affine transformations and a power function

Comparison of AES implementations

Implementation of existing secure methods (encryption AES-128, 8051 based 8-bit architecture)

Comparison of AES implementations

Implementation of existing secure methods (encryption AES-128, 8051 based 8-bit architecture)

For $d = 1$:

- *table re-computation* [Messerges00]
- *tower fields* [OswaldMangardPramstaller04]
- *multiplicative masking* [GenelleProuffQuisquater10]
- *secure exponentiation* [RivainProuff10]

Comparison of AES implementations

Implementation of existing secure methods (encryption AES-128, 8051 based 8-bit architecture)

For $d = 1$:

- *table re-computation* [Messerges00]
- *tower fields* [OswaldMangardPramstaller04]
- *multiplicative masking* [GenelleProuffQuisquater10]
- *secure exponentiation* [RivainProuff10]

For $d = 2$:

- *double re-computation* [SchrammPaar06]
- *single re-computation* [RivainDottaxProuff08]
- *secure exponentiation* [RivainProuff10]

For $d = 3$:

- *secure exponentiation* [RivainProuff10]

Comparison of AES implementations

Method	Cycles (10^3)	Memory (bytes)
Unprotected Implementation		
No Masking	2	32
$d = 1$		
table re-computation	10	256
tower fields	77	42
multiplicative masking	22	256
secure exponentiation for $d = 1$	73	24
our scheme for d = 1	**25**	**50**

Comparison of AES implementations

Method	Cycles (10^3)	Memory (bytes)
Unprotected Implementation		
No Masking	2	32
$d = 1$		
table re-computation	10	256
tower fields	77	42
multiplicative masking	22	256
secure exponentiation for $d = 1$	73	24
our scheme for d = 1	**25**	**50**

Comparison of AES implementations

Method	Cycles (10^3)	Memory (bytes)
Unprotected Implementation		
No Masking	2	32
$d = 1$		
table re-computation	10	256
tower fields	77	42
multiplicative masking	22	256
secure exponentiation for $d = 1$	73	24
our scheme for d = 1	**25**	**50**
$d = 2$		
double re-computations	594	$512 + 28$
single re-computation	672	$256 + 22$
secure exponentiation for $d = 2$	189	48
our scheme for d = 2	**69**	**86**

Comparison of AES implementations

Method	Cycles (10^3)	Memory (bytes)
Unprotected Implementation		
No Masking	2	32
$d = 1$		
table re-computation	10	256
tower fields	77	42
multiplicative masking	22	256
secure exponentiation for $d = 1$	73	24
our scheme for d = 1	**25**	**50**
$d = 2$		
double re-computations	594	$512 + 28$
single re-computation	672	$256 + 22$
secure exponentiation for $d = 2$	189	48
our scheme for d = 2	**69**	**86**

Comparison of AES implementations

Method	Cycles (10^3)	Memory (bytes)
Unprotected Implementation		
No Masking	2	32
$d = 1$		
table re-computation	10	256
tower fields	77	42
multiplicative masking	22	256
secure exponentiation for $d = 1$	73	24
our scheme for d = 1	**25**	**50**
$d = 2$		
double re-computations	594	$512 + 28$
single re-computation	672	$256 + 22$
secure exponentiation for $d = 2$	189	48
our scheme for d = 2	**69**	**86**
$d = 3$		
secure exponentiation for $d = 3$	326	72
our scheme for d = 3	**180**	**128**

Comparison of AES implementations

Method	Cycles (10^3)	Memory (bytes)
Unprotected Implementation		
No Masking	2	32
$d = 1$		
table re-computation	10	256
tower fields	77	42
multiplicative masking	22	256
secure exponentiation for $d = 1$	73	24
our scheme for d = 1	**25**	**50**
$d = 2$		
double re-computations	594	$512 + 28$
single re-computation	672	$256 + 22$
secure exponentiation for $d = 2$	189	48
our scheme for d = 2	**69**	**86**
$d = 3$		
secure exponentiation for $d = 3$	326	72
our scheme for d = 3	**180**	**128**

Conclusion

Our countermeasure:

- dO-SCA resistant (proved)
- best trade-off timing/memory consumptions
- applicable at order 2 and 3 for today products

Thank you!
Questions?