Mixing Additive and Multiplicative Masking for Probing Secure Polynomial Evaluation Methods

Axel Mathieu-Mahias and Michaël Quisquater

University of Versailles (UVSQ)

CHES'18 September

The Concept of Masking

- Side-channel analysis
  - Information leak through physical leakages
  - Data and physical leakages are dependent

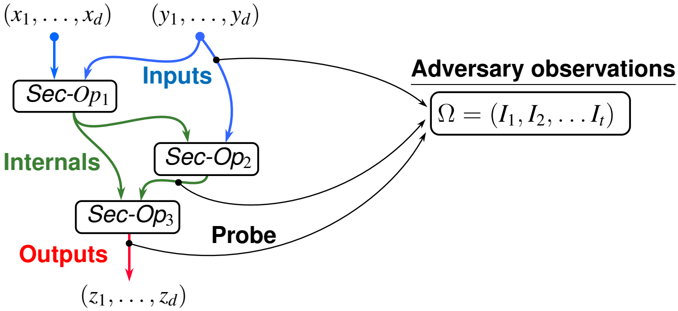
The Concept of Masking

- Side-channel analysis
  - Information leak through physical leakages
  - Data and physical leakages are dependent
- The masking countermeasure
  1. Randomly split every variable into several shares
  2. Secure the processing through internal operations

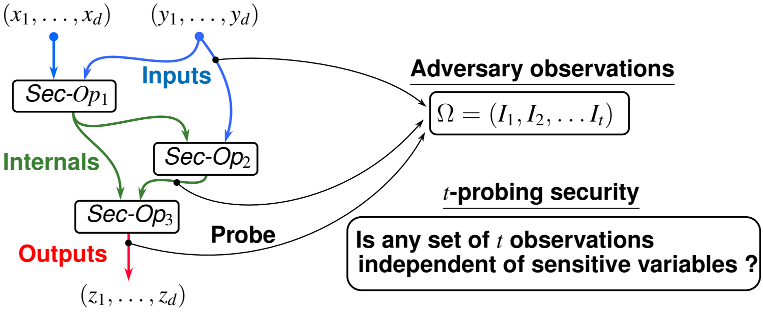
The Concept of Masking

- Side-channel analysis
  - Information leak through physical leakages
  - Data and physical leakages are dependent
- The masking countermeasure
  1. Randomly split every variable into several shares
  2. Secure the processing through internal operations
- Higher-order masking
  - More than 2 shares
  - Sound countermeasure

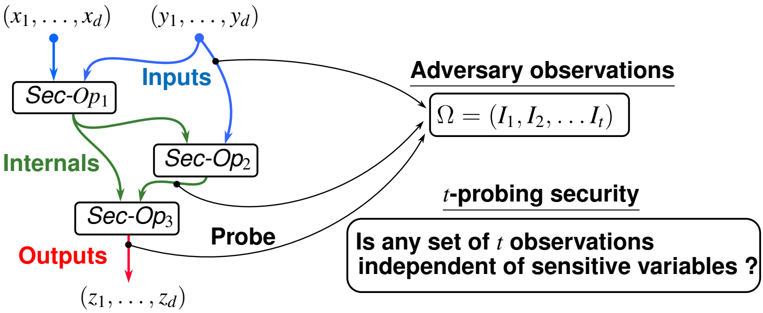
The Probing Model [ISW03]



The Probing Model [ISW03]



The Probing Model [ISW03]



- Two security notions : **t-NI** and **t-SNI** [BBDFG15]
  ↪ t-SNI transformations can be composed safely

State of the Art of Masking S-boxes (Additive Masking)

- Split every variable x into $d = t + 1$ shares such that

$$x_1 \oplus x_2 \oplus \ldots \oplus x_d = x$$

- Processing of **linear transformations** : very efficient
- Processing of **multiplications** : much more expensive

State of the Art of Masking S-boxes (Additive Masking)

- Split every variable x into $d = t + 1$ shares such that

$$x_1 \oplus x_2 \oplus \ldots \oplus x_d = x$$

- Processing of **linear transformations** : very efficient
- Processing of **multiplications** : much more expensive

AES : [RP10]

$$S_{\mathrm{AES}}(x) : x \mapsto x^{254} \text{ over } \mathbb{F}_{2^8}$$

Generic case : [CGPQR12]

$$S(x) : x \mapsto \sum_{i=0}^{2^n-1} a_i x^i \text{ over } \mathbb{F}_{2^n}$$

State of the Art of Masking S-boxes

- **Masking schemes in additive encoding**

FSE'12 : Carlet et al.

CHES'13 : Roy and Vivek

CHES'14 : Coron et al.

State of the Art of Masking S-boxes

- **Masking schemes in additive encoding**

FSE'12 : Carlet et al.
CHES'13 : Roy and Vivek
CHES'14 : Coron et al.

- **Masking schemes in other encodings**

CHES'11 : Prouff and Roche
CRYPTO'15 : Carlet et al.
EUROCRYPT'14 : Coron
EUROCRYPT'15 : Balasch et al.
CHES'16 : Goudarzi and Rivain

The use of several encodings simultaneously

GPQ : masking scheme for **power functions** [GPQ11]

- Mixes **additive** and **multiplicative** masking

The use of several encodings simultaneously

GPQ : masking scheme for **power functions** [GPQ11]

- Mixes **additive** and **multiplicative** masking

The idea

- Linear transformations : efficient in additive masking
- Multiplications : efficient in multiplicative masking

The use of several encodings simultaneously

GPQ : masking scheme for **power functions** [GPQ11]

- Mixes **additive** and **multiplicative** masking

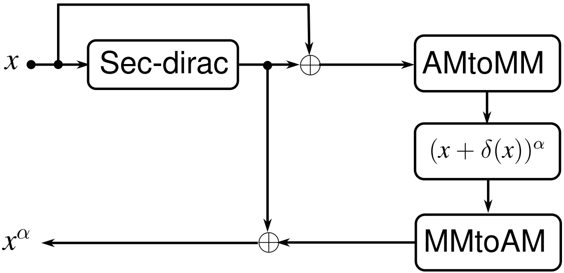
The idea

- Linear transformations : efficient in additive masking
- Multiplications : efficient in multiplicative masking

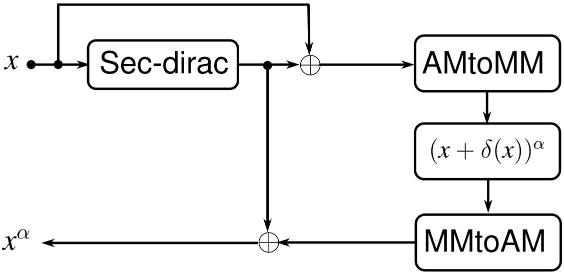
The scheme

- Secure processing of a Dirac function (**Secure-dirac**)
- Transformations to switch from additive into multiplicative masking (**AMtoMM**) and conversely (**MMtoAM**)

GPQ : Masking Scheme for Power Functions



GPQ : Masking Scheme for Power Functions



Our first contribution

GPQ t-NI → GPQ t-SNI

Our Issue and Our Proposals

How to extend **GPQ** to evaluate **polynomials** ?

Our Issue and Our Proposals

How to extend **GPQ** to evaluate **polynomials** ?

Our issues

- **Adding monomials** : not efficient in multiplicative masking
- **Converting every monomials** back in additive masking before adding them : not efficient

Our Issue and Our Proposals

How to extend **GPQ** to evaluate **polynomials** ?

Our issues

- **Adding monomials** : not efficient in multiplicative masking
- **Converting every monomials** back in additive masking before adding them : not efficient

Our t-SNI proposals

1. One method based on the cyclotomic method [CGPQR12]
2. One method based on our first proposal and the CRV method [CRV14]

Our First Proposal : The Alternate Cyclotomic Method

Reminder of the Cyclotomic Method [CGPQR12]

- The cyclotomic class of α : $C_\alpha = \{\alpha \cdot 2^j \bmod 2^n - 1; j < n\}$

Our First Proposal : The Alternate Cyclotomic Method

Reminder of the Cyclotomic Method [CGPQR12]

- The cyclotomic class of α : $C_\alpha = \{\alpha \cdot 2^j \bmod 2^n - 1; j < n\}$
- Any n-bit S-box can be expressed as

$$S(x) = a_0 + \left(\sum_{i=1}^{q} L_i(x^{\alpha_i})\right) + a_{2^n-1}x^{2^n-1}$$

where $L_i(x) = \sum_j a_{i,j}x^{2^j}$ and q is the number of distinct cyclotomic classes

Our First Proposal : The Alternate Cyclotomic Method

Reminder of the Cyclotomic Method [CGPQR12]

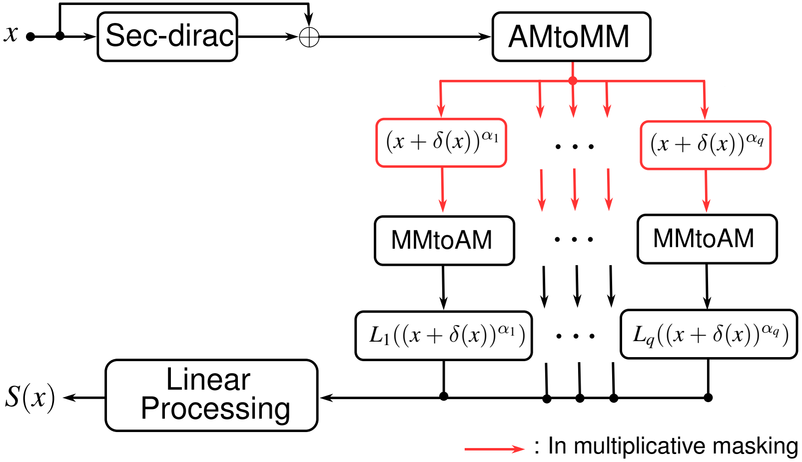
- The cyclotomic class of α : $C_\alpha = \{\alpha \cdot 2^j \bmod 2^n - 1; j < n\}$
- Any n-bit S-box can be expressed as

$$S(x) = a_0 + \left(\sum_{i=1}^{q} L_i(x^{\alpha_i})\right) + a_{2^n-1}x^{2^n-1}$$

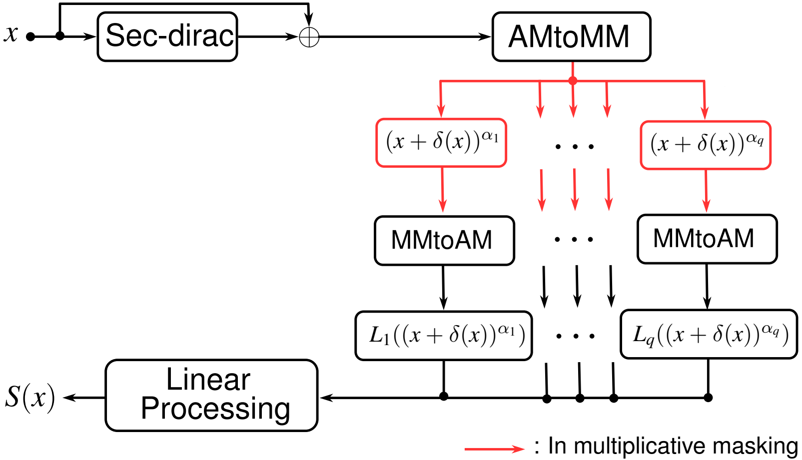
where $L_i(x) = \sum_j a_{i,j}x^{2^j}$ and q is the number of distinct cyclotomic classes

- Deriving the x^{α_i}'s requires multiplications : **expensive in additive masking.**

Our First Proposal : The Alternate Cyclotomic Method



Our First Proposal : The Alternate Cyclotomic Method



The alternate cyclotomic method is **t-SNI**

Assembly Language Performances : 8-bit Architecture

- Costs (in clock cycles) of evaluating S-boxes of size $4 \leq n \leq 8$ with the cyclotomic method and our proposal

		n				
Method	Order	4	5	6	7	8
Our proposal	1	**83**	**246**	**553**	**860**	**1677**
Original		132	780	1716	2652	5148
Our proposal	2	276	**585**	**1362**	**2138**	**4205**
Original		**174**	1770	3894	6018	11682
Our proposal	3	477	**1036**	**2445**	**3854**	**7603**
Original		**293**	3160	6952	10744	20856

Our Second Proposal : The Alternate CRV Method

Reminder of the original CRV Method [CRV14]

- Express any n-bit S-box as

$$S(x) = \sum_{i=1}^{k-1} p_i(x) \cdot q_i(x) + p_k(x)$$

where monomials of $p_i(x), q_i(x)$ belong to x^L with $L \leftarrow \bigcup_{i=1}^{l} C_{\alpha_i}$

Our Second Proposal : The Alternate CRV Method

Reminder of the original CRV Method [CRV14]

- Express any n-bit S-box as

$$S(x) = \sum_{i=1}^{k-1} p_i(x) \cdot q_i(x) + p_k(x)$$

where monomials of $p_i(x), q_i(x)$ belong to x^L with $L \leftarrow \bigcup_{i=1}^{l} C_{\alpha_i}$

- **Evaluation in two steps**
  1. Evaluating $q_i(x), p_i(x)$ requires $l - 2$ multiplications
  2. Evaluating $S(x)$ requires $k - 1$ multiplications

Our Second Proposal : The Alternate CRV Method

Reminder of the original CRV Method [CRV14]

- Express any n-bit S-box as

$$S(x) = \sum_{i=1}^{k-1} p_i(x) \cdot q_i(x) + p_k(x)$$

where monomials of $p_i(x), q_i(x)$ belong to x^L with $L \leftarrow \bigcup_{i=1}^{l} C_{\alpha_i}$

- **Evaluation in two steps**
  1. Evaluating $q_i(x), p_i(x)$ requires $l - 2$ multiplications
  2. Evaluating $S(x)$ requires $k - 1$ multiplications

- **Remark :** trade-off between l and k

Our Second Proposal : The Alternate CRV Method

$$S(x) = \sum_{i=1}^{k-1} p_i(x) \cdot q_i(x) + p_k(x)$$

Our evaluation method

1. Evaluating $q_i(x), p_i(x)$ with our t-SNI **alternate cyclotomic** method
2. Evaluating $S(x)$ in additive masking (**unchanged)**

Our Second Proposal : The Alternate CRV Method

$$S(x) = \sum_{i=1}^{k-1} p_i(x) \cdot q_i(x) + p_k(x)$$

Our evaluation method

1. Evaluating $q_i(x), p_i(x)$ with our t-SNI **alternate cyclotomic** method
2. Evaluating $S(x)$ in additive masking (**unchanged)**

Remarks

- **More choices** of cyclotomic classes to build x^L
- **Larger sets** $L \leftarrow \bigcup_{i=1}^{l} C_{\alpha_i}$ can be considered
- The alternate CRV method is **t-SNI**

Assembly Language Performances : 8-bit Architecture

- Costs (in clock cycles) of evaluating S-boxes of size $4 \leq n \leq 8$ with the CRV method and our alternate proposal

		n				
Method	Order	4	5	6	7	8
Our proposal	1	127	**402**	**559**	**713**	**972**
Original CRV		**88**	624	780	1092	1560
Our proposal	2	276	**939**	**1296**	**1685**	**2300**
Original CRV		**204**	1416	1770	2478	3540
Our proposal	3	477	**1668**	**2305**	**3012**	**4117**
Original CRV		**368**	2528	3160	4424	6320

Conclusion

1. **GPQ t-NI → GPQ t-SNI**

Conclusion

1. **GPQ t-NI → GPQ t-SNI**
2. The **Alternate cyclotomic method**
   - Extends GPQ to polynomial evaluations
   - Three times faster than the original method
   - Satisfies the t-SNI property

Conclusion

1. **GPQ t-NI → GPQ t-SNI**
2. The **Alternate cyclotomic method**
   - Extends GPQ to polynomial evaluations
   - Three times faster than the original method
   - Satisfies the t-SNI property
3. The **Alternate CRV method**
   - Uses Alternate cyclotomic for one evaluation step
   - New sets of parameters can be derived
   - Outperforms the original method in most scenarios
   - Satisfies the t-SNI property

Thanks for your attention!