Very High-Order Masking: Efficient Implementation and Security Evaluation

Anthony Journault and François-Xavier Standaert

UCL (Louvain-la-Neuve, Belgium)

CHES 2017, Taipei, Taiwan

Outline

- **Background**
  - Masking
  - Barthe *et al.* masking scheme
- **How fast can be very high-order masking ?**
  - Data representation
  - AES results and discussion
- **How can we evaluate security at very high order ?**
  - Limitation of leakage detection strategy
  - Multi-model approach
- **Conclusion/Open problems**

Outline

- **Background**
  - Masking
  - Barthe *et al.* masking scheme
- **How fast can be very high-order masking ?**
  - Data representation
  - AES results and discussion
- **How can we evaluate security at very high order ?**
  - Limitation of leakage detection strategy
  - Multi-model approach
- **Conclusion/Open problems**

Masking

- Masking (e.g. Boolean encoding)

$$a = a_1 \oplus a_2 \oplus \cdots \oplus a_d$$

- With $a_2, \cdots, a_d$ random

Masking

- Masking (e.g. Boolean encoding)

$$a = a_1 \oplus a_2 \oplus \cdots \oplus a_d$$

- With $a_2, \cdots, a_d$ random

- Abstract security
  - Probing model
  - Security order
    $d - 1$ (at best)

Masking

- Masking (e.g. Boolean encoding)

$$a = a_1 \oplus a_2 \oplus \cdots \oplus a_d$$

- With $a_2, \cdots, a_d$ random

- Abstract security
  - Probing model
  - Security order $d - 1$ (at best)

- Concrete security
  - Noisy leakage model
  - $N = (\sigma^2)^{d-1}$ (under assumptions)

Barthe *et al.* 2017 masking scheme

- Parallel masking scheme by design
- All shares manipulated at once

Barthe *et al.* 2017 masking scheme

- Parallel masking scheme by design
- All shares manipulated at once

- Example of mult. $a * b = c$ for $d = 3$

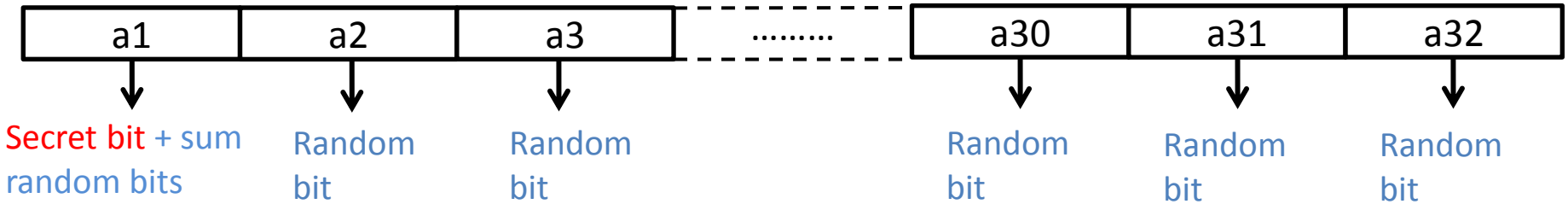
$$\begin{vmatrix} a_1b_1 \\ a_2b_2 \\ a_3b_3 \end{vmatrix} \oplus \begin{vmatrix} r_1 \\ r_2 \\ r_3 \end{vmatrix} \oplus \begin{vmatrix} a_1b_3 \\ a_2b_1 \\ a_3b_2 \end{vmatrix} \oplus \begin{vmatrix} a_3b_1 \\ a_1b_2 \\ a_2b_3 \end{vmatrix} \oplus \begin{vmatrix} r_3 \\ r_1 \\ r_2 \end{vmatrix} \equiv \begin{vmatrix} c_1 \\ c_2 \\ c_3 \end{vmatrix}$$

Outline

- **Background**
  - Masking
  - Barthe *et al.* masking scheme
- **How fast can be very high-order masking ?**
  - Data representation
  - AES results and discussion
- **How can we evaluate security at very high order ?**
  - Limitation of leakage detection strategy
  - Multi-model approach
- **Conclusion/Open problems**

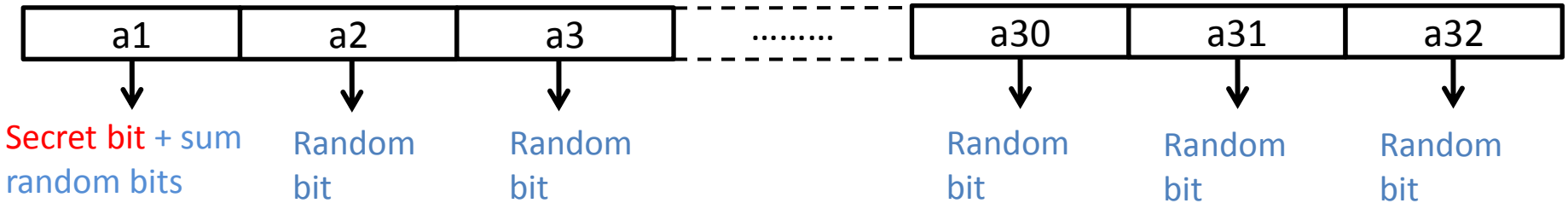
Data representation and implementation 3

- 32-bit register



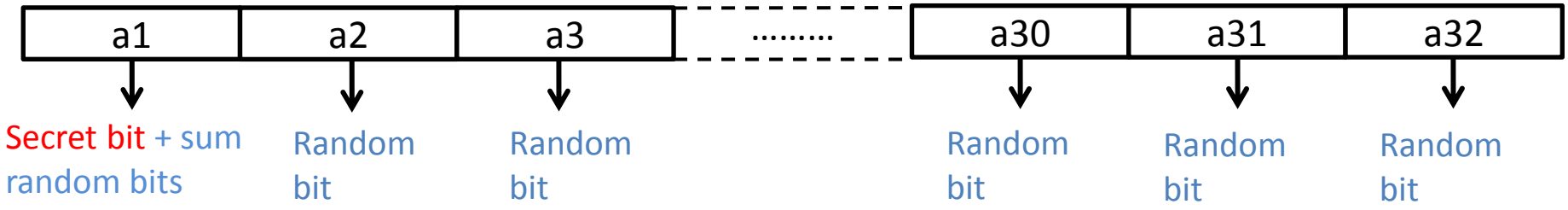
Data representation and implementation 3

- 32-bit register



- Use bitwise operators (XOR, AND, …)

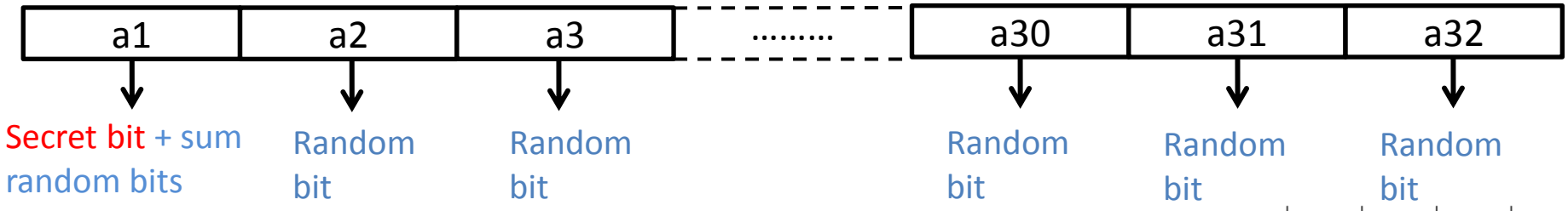
- 32-bit register



- Use bitwise operators (XOR, AND, …)

- Implementation on 32-bit ARM
- Optimal case: register size = nb of shares

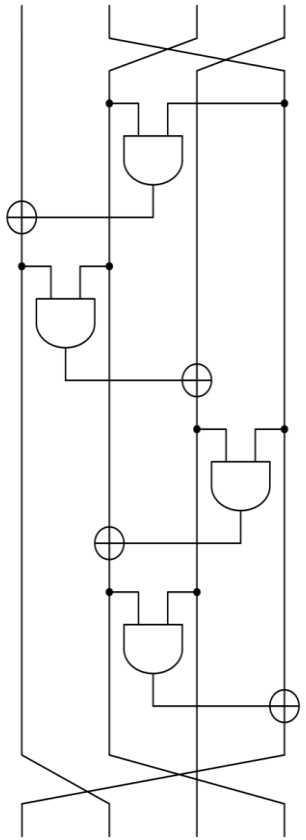
- 32-bit register



- Use bitwise operators (XOR, AND, …)

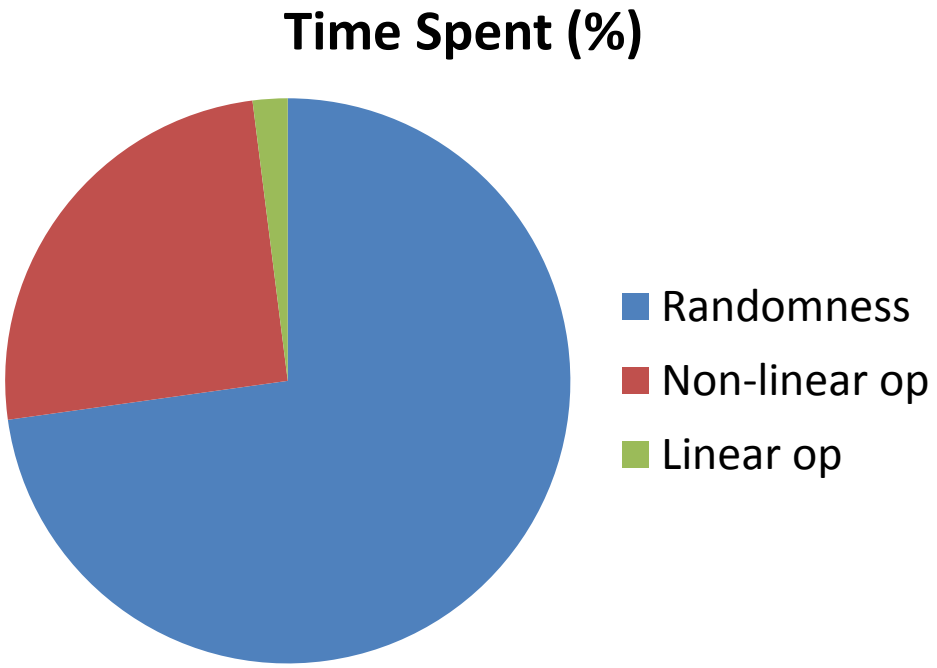
- Implementation on 32-bit ARM
- Optimal case: register size = nb of shares

- Well suited for bitslice ciphers ➔



Implementation Results: AES

- Application to AES
- Gate level representation of AES S-box (Boyar, Peralta 2010)



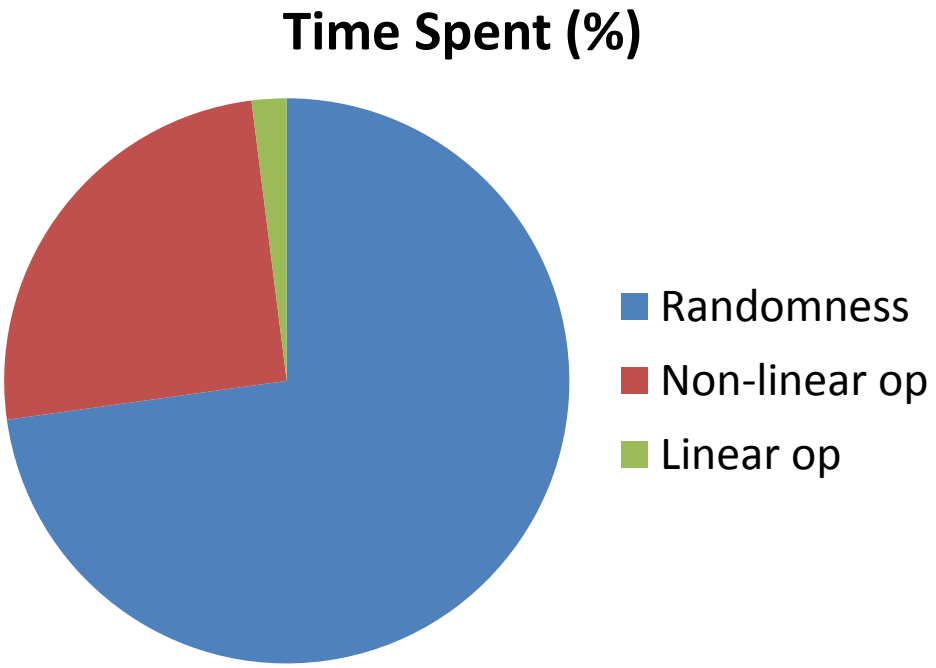
10 cycles to generate 32-bit random value

Total = 2 800 000 cycles

Implementation Results: AES

- Application to AES
- Gate level representation of AES S-box (Boyar, Peralta 2010)

- SNI refreshing of one input of each multiplication (conservative)

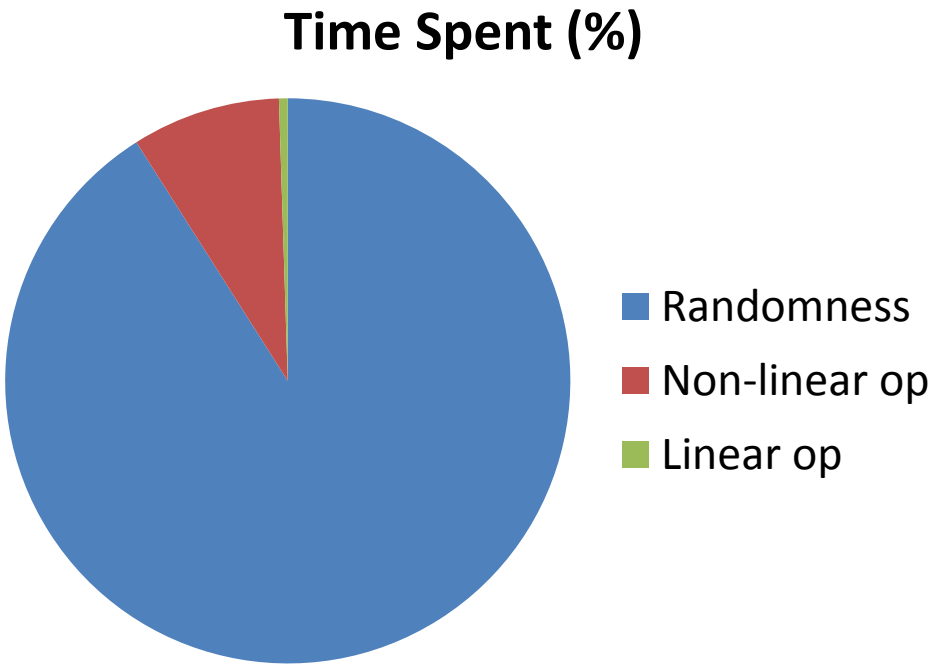


10 cycles to generate 32-bit random value
Total = 2 800 000 cycles

Implementation Results: AES

- Application to AES
- Gate level representation of AES S-box (Boyar, Peralta 2010)

- SNI refreshing of one input of each multiplication (conservative)



80 cycles to generate 32-bit random value

Total = 9 700 000 cycles

Comparison with Goudarzi-Rivain

- Goudarzi-Rivain 2017: Generic ISW implementation and application to bitsliced AES

Goudarzi-Rivain	This paper
3,821,312	2,783,510

Comparison with Goudarzi-Rivain

- Goudarzi-Rivain 2017: Generic ISW implementation and application to bitsliced AES

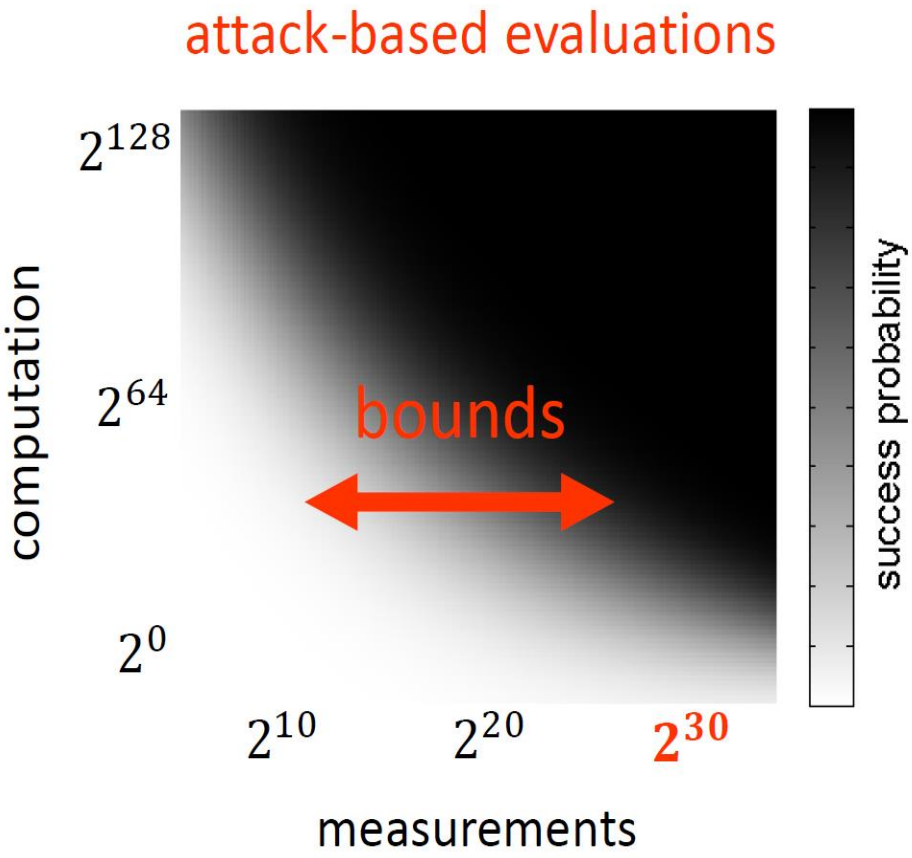
Goudarzi-Rivain	This paper
3,821,312	2,783,510

- Same order of magnitude of cycles
- Very high-order masking is **not out of reach !**

Outline

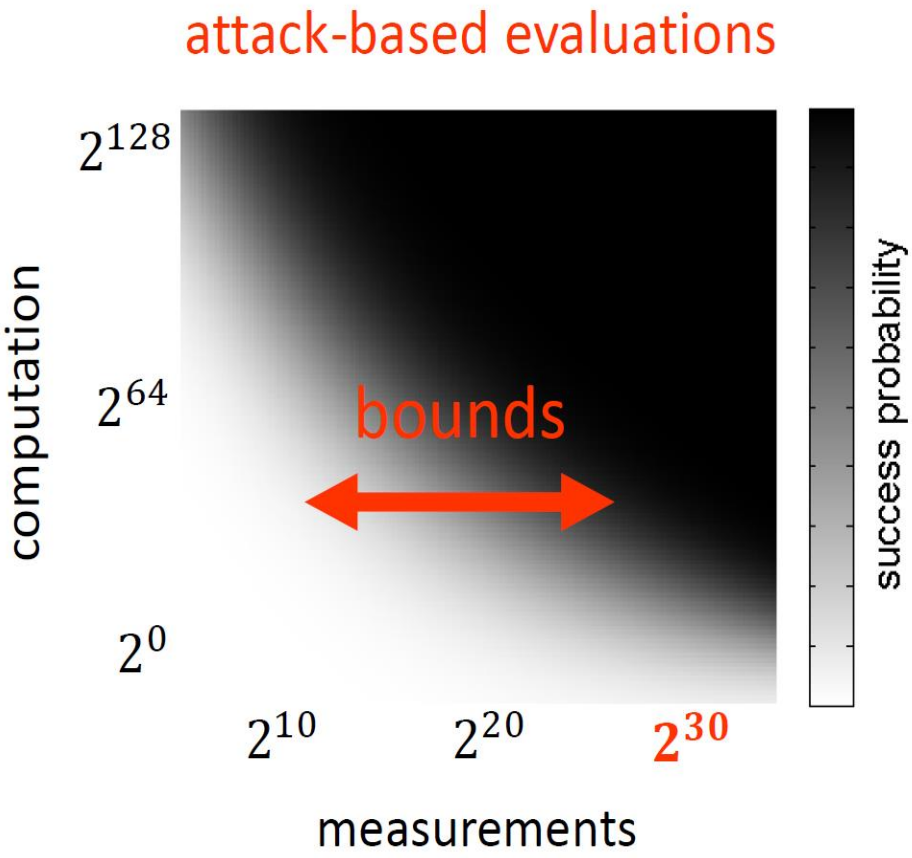
- **Background**
  - Masking
  - Barthe *et al.* masking scheme
- **How fast can be very high-order masking ?**
  - Data representation
  - AES results and discussion
- **How can we evaluate security at very high order ?**
  - Limitation of leakage detection strategy
  - Multi-model approach
- **Conclusion/Open problems**

Limitations of leakage detection strategy



- Evaluator power = 2^30
- If security <= 2^30, security level
- What if security > 2^30 ?
- Security claims bounded by evaluator power

Limitations of leakage detection strategy



- Evaluator power = 2^30
- If security <= 2^30, security level
- What if security > 2^30 ?
- Security claims bounded by evaluator power

We expect 31th-security order (or 31/f-security order)

Multi-Model Approach

Multi-Model Approach

Probing model

Abstract

Qualitative

Algorithmic security order

d

Risk captured:

Lack of refreshing

Multi-Model Approach

Probing model	Bounded-Moment Model
Abstract	Physical
Qualitative	Qualitative
Algorithmic security order **d**	Physical security order **f**
Risk captured: Lack of refreshing	Risk captured: Share recombination

Multi-Model Approach

Probing model	Bounded-Moment Model	Noisy Leakage Model
Abstract	Physical	Physical
Qualitative	Qualitative	Quantitative
Algorithmic security order **d**	Physical security order **f**	Physical security order **MI,SNR**
Risk captured: Lack of refreshing	Risk captured: Share recombination	Risk captured: Lack of noise

Multi-Model Approach

Probing model	Bounded-Moment Model	Noisy Leakage Model
Abstract	Physical	Physical
Qualitative	Qualitative	Quantitative
Algorithmic security order	Physical security order	Physical security order
d + f + SNR + MI => Security level		
Risk captured: Lack of refreshing	Risk captured: Share recombination	Risk captured: Lack of noise

Probing security (state of the art)

- 2 possible options:
  - Composable gadgets (SNI)
    - Simple to analyse
    - Implementation becomes expensive
  - Full code evaluation
    - Hard to analyse
    - Reduced implementation cost

Bounded-Moment security

Bounded-Moment security

- Leakage detection hard in practice with 32 shares

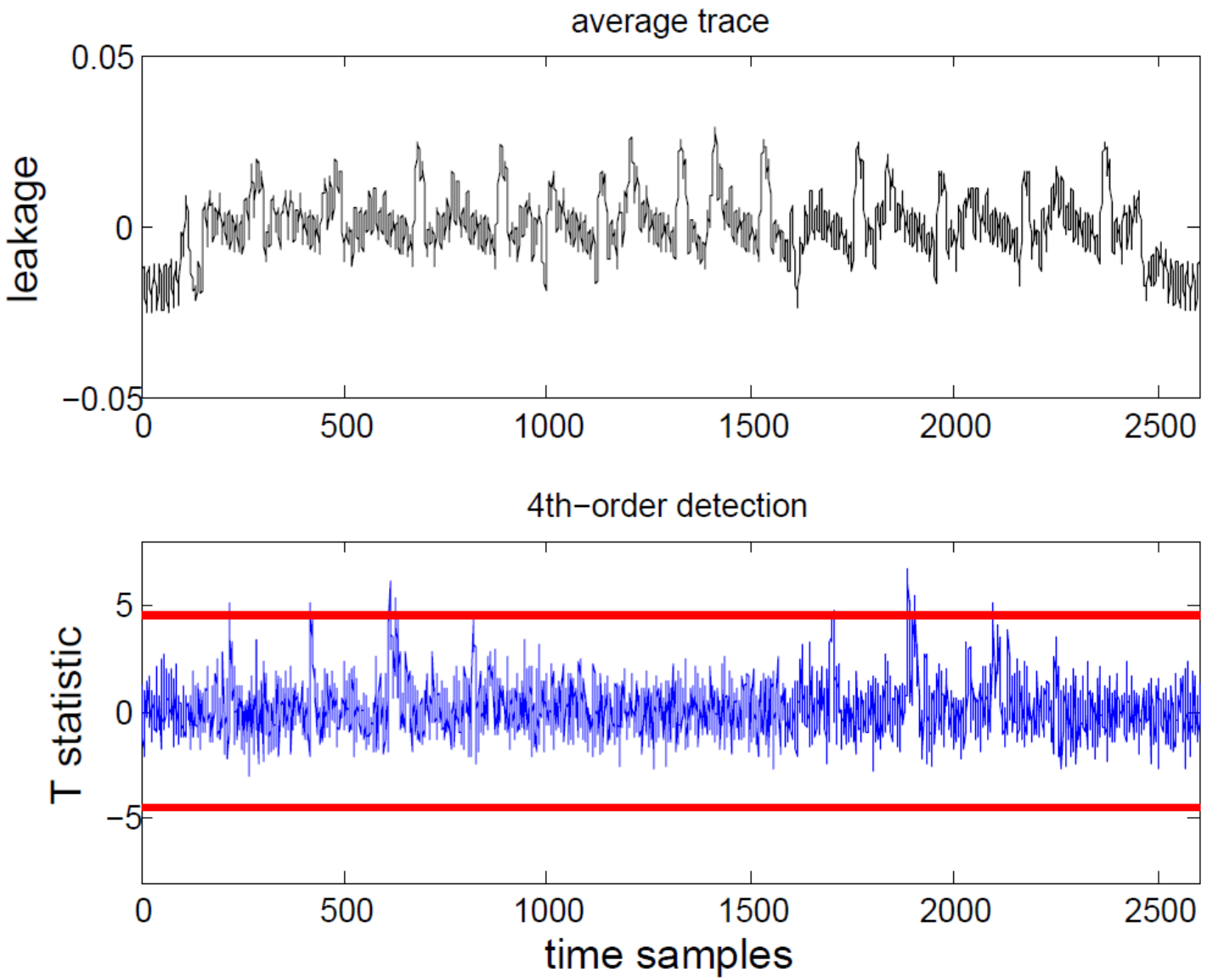
Bounded-Moment security

- Leakage detection hard in practice with 32 shares
- Idea similar to symmetric cryptanalysis: security based on reduced version
- Leakage detection on small order (e.g. on 4 shares)

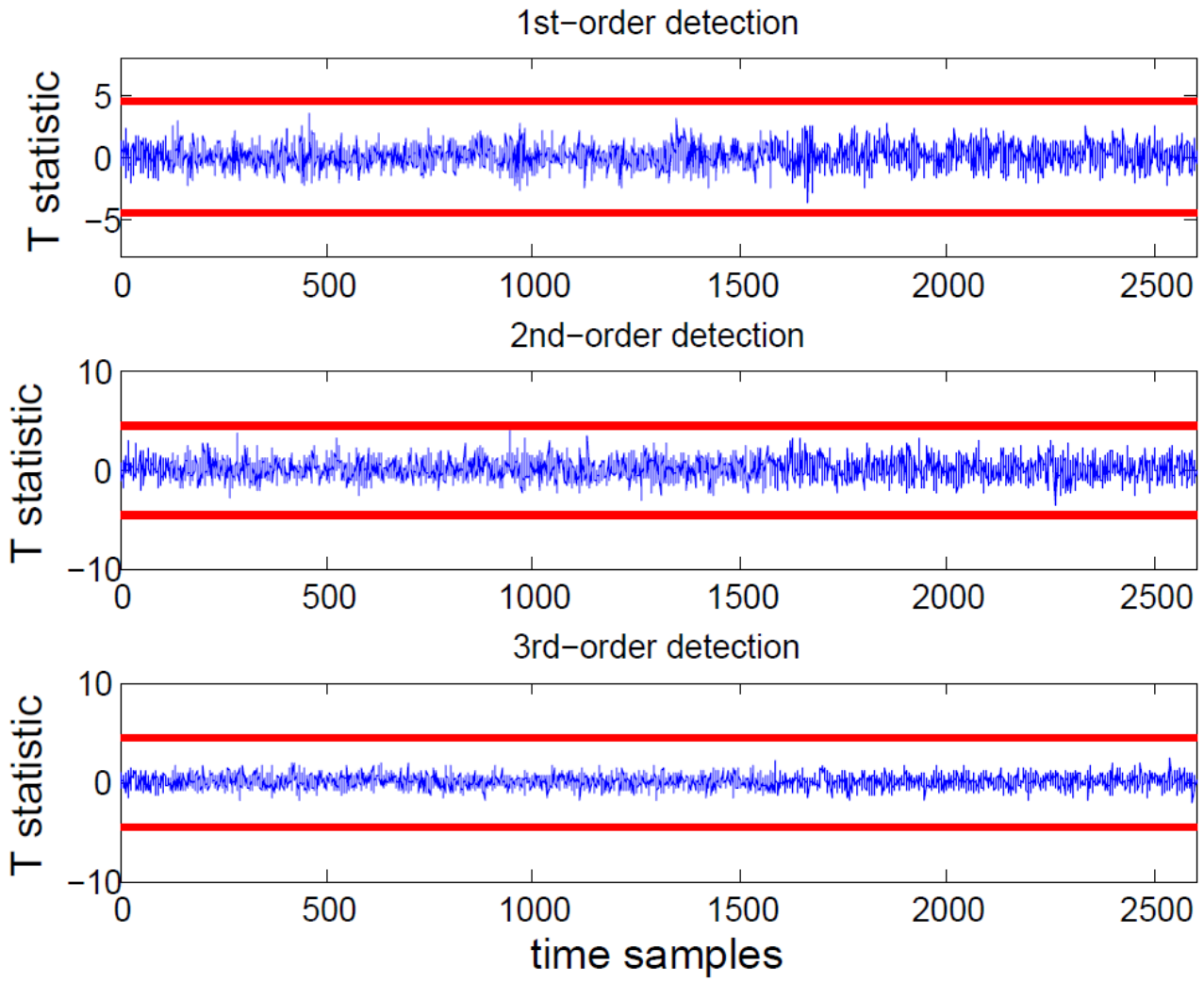
Bounded-Moment security

- Leakage detection hard in practice with 32 shares
- Idea similar to symmetric cryptanalysis: security based on reduced version
- Leakage detection on small order (e.g. on 4 shares)
- Extraction of a risk factor **f** from possible share recombination
- Extrapolation of security

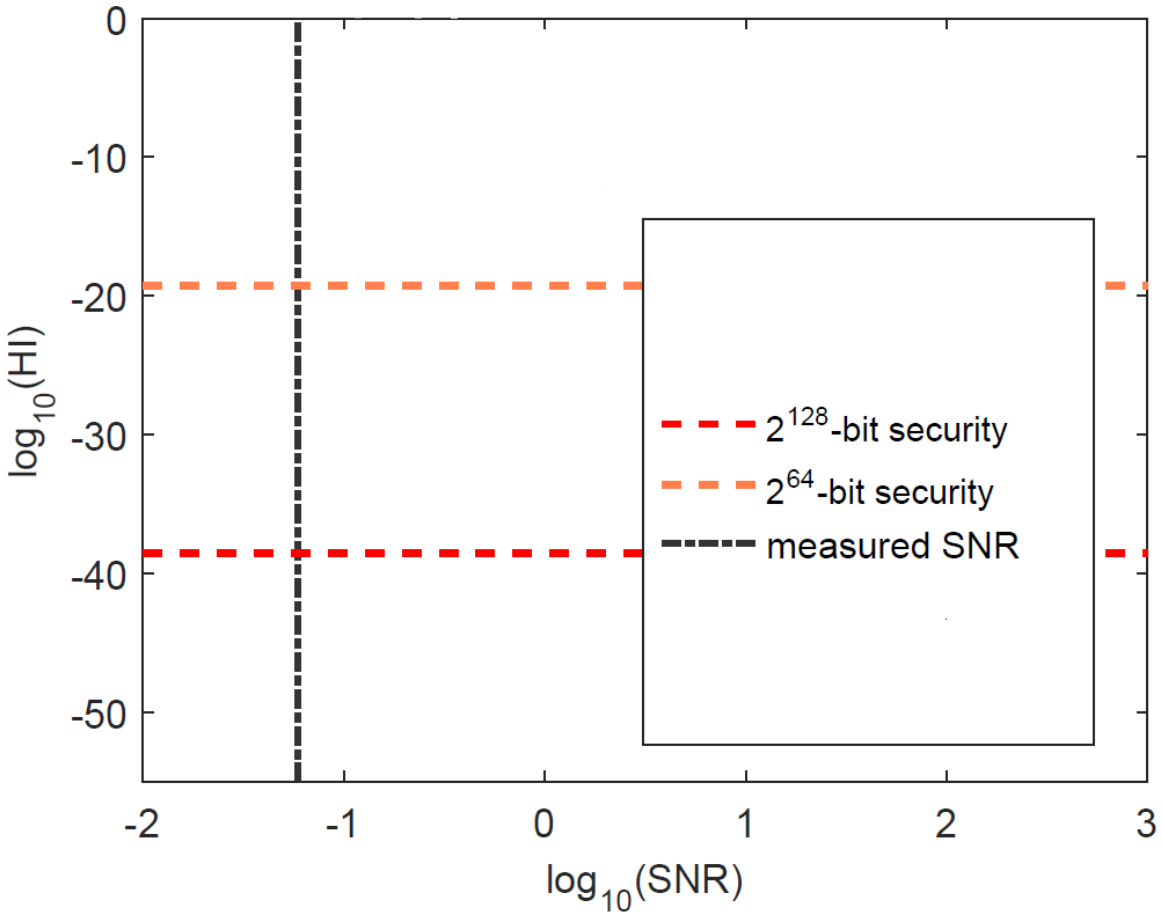
Leakage detection results



Leakage detection results

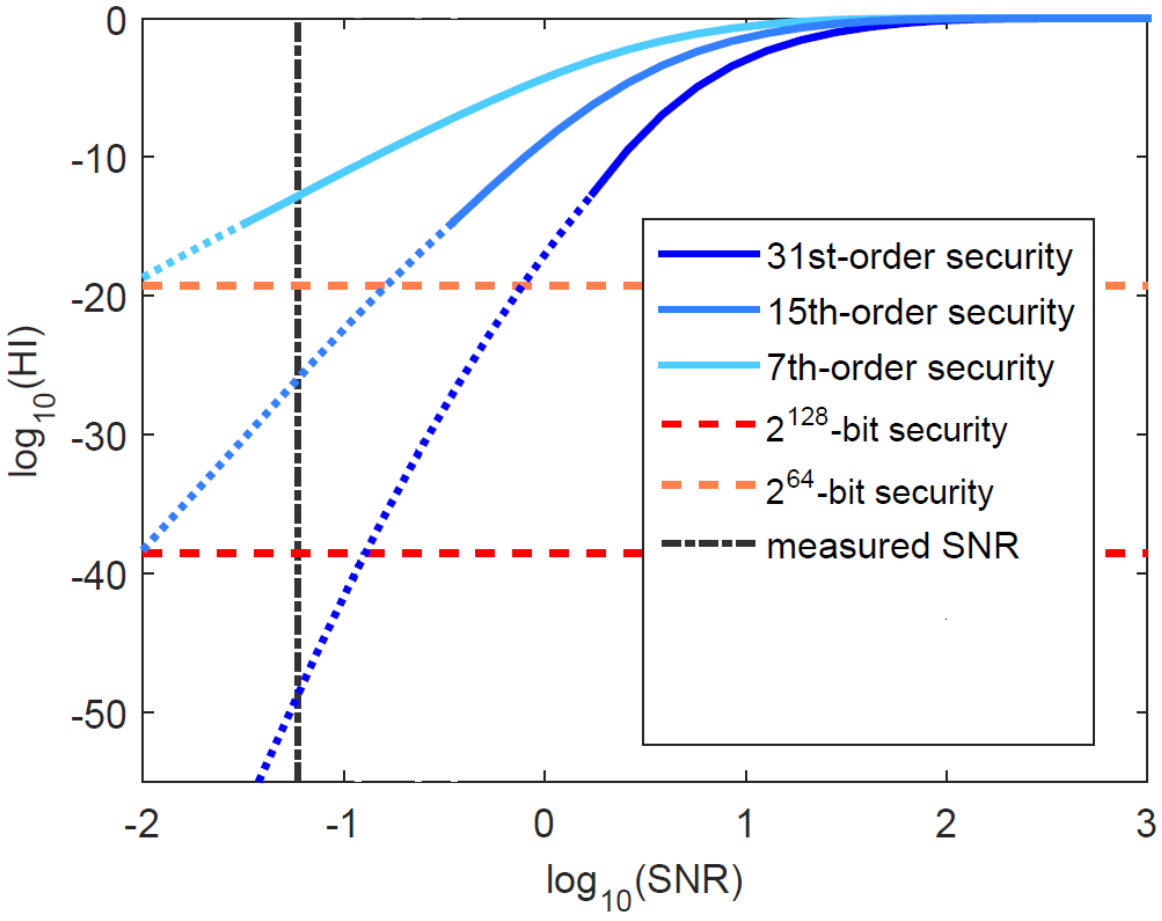


Noisy Leakage Model



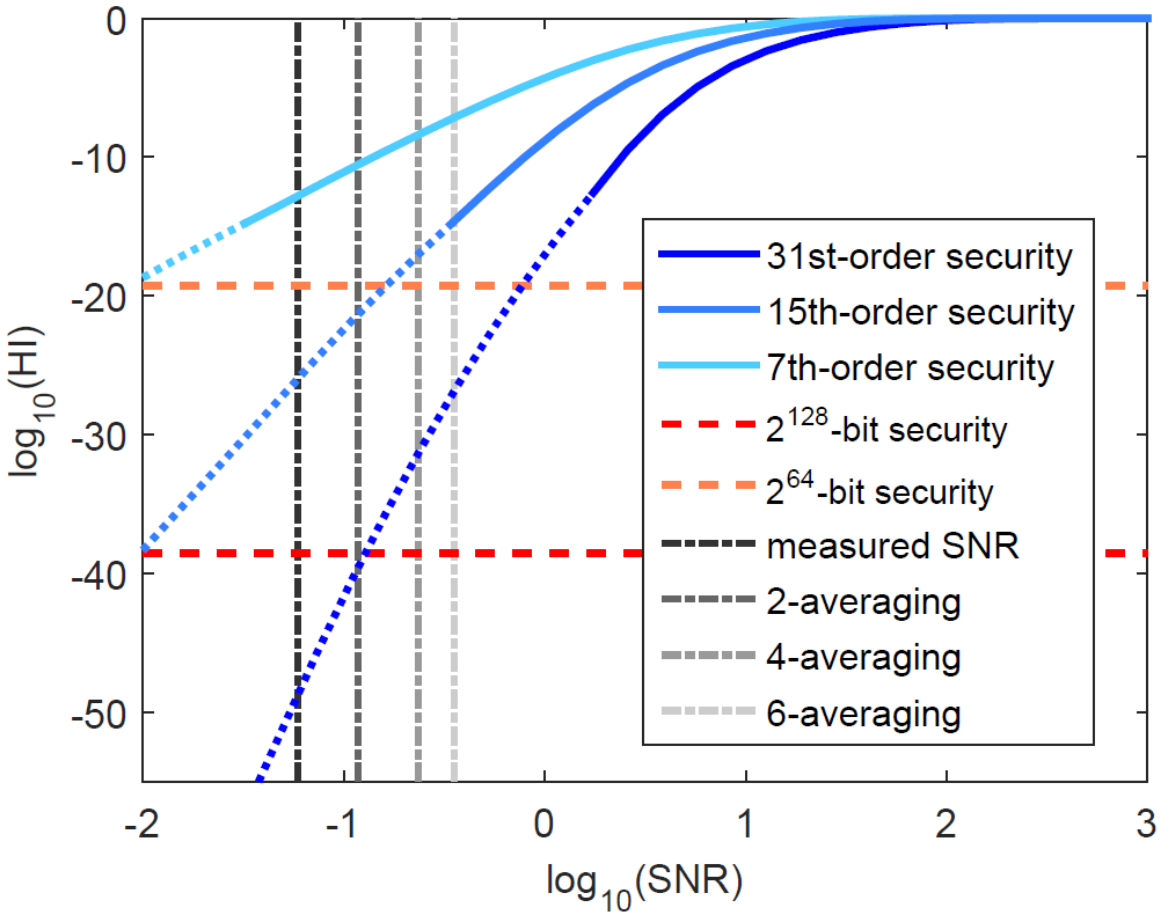
- SNR(=0,05) computed with linear regression
- **MI** of the encoding
- **31**/**15**/**7**-order security if flaw **f**=**1**/**2**/**4**

Noisy Leakage Model



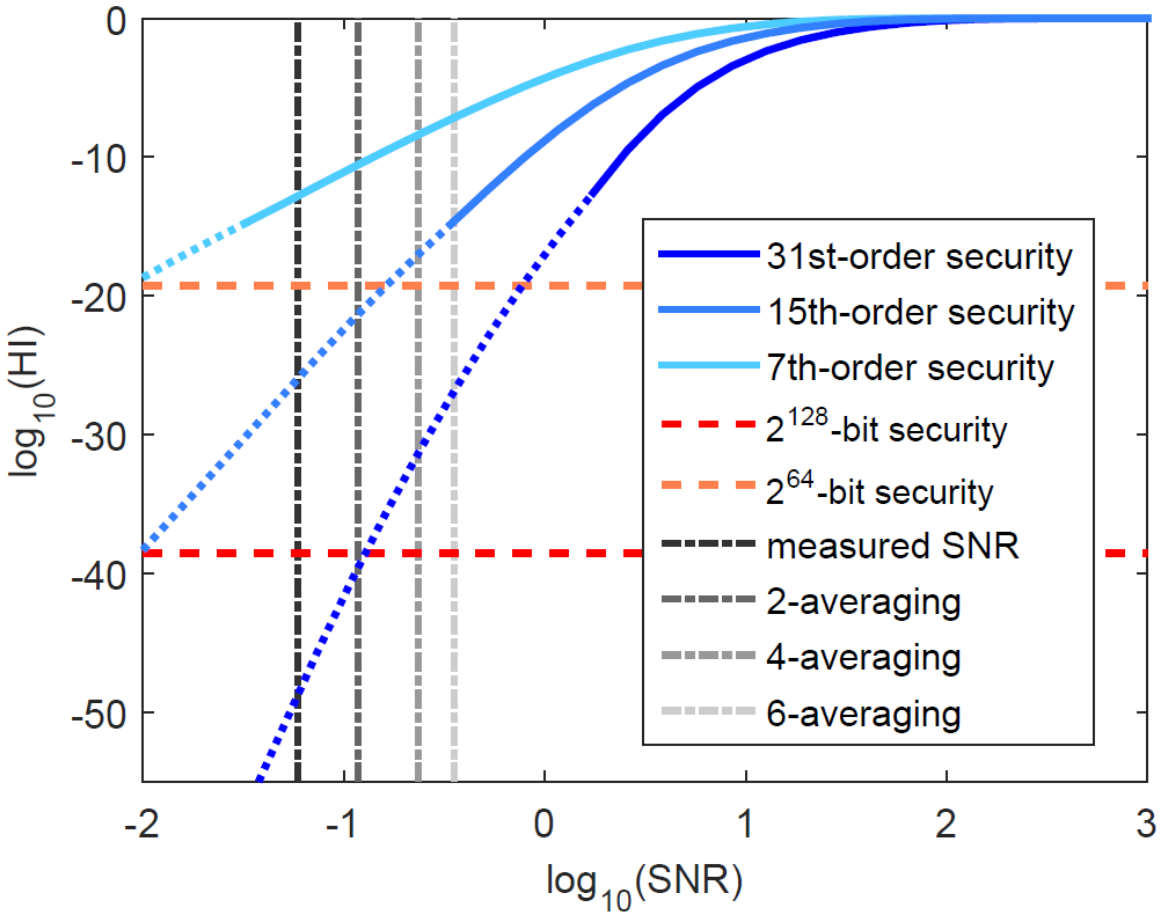
- SNR(=0,05) computed with linear regression
- **MI** of the encoding
- **31**/**15**/**7**-order security if flaw **f**=**1**/**2**/**4**

Noisy Leakage Model



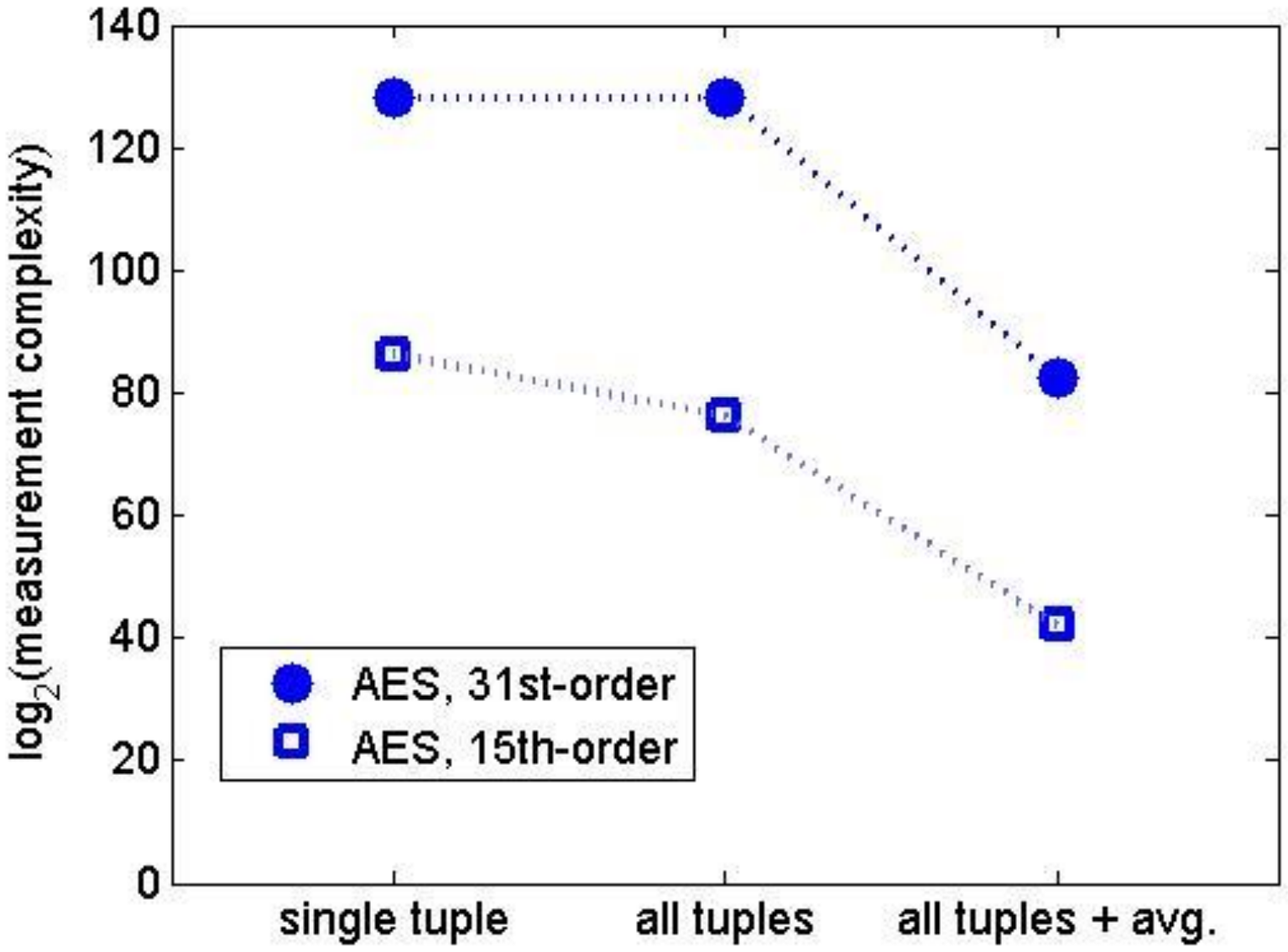
- SNR(=0,05) computed with linear regression
- **MI** of the encoding
- **31**/**15**/**7**-order security if flaw **f**=**1**/**2**/**4**

Noisy Leakage Model

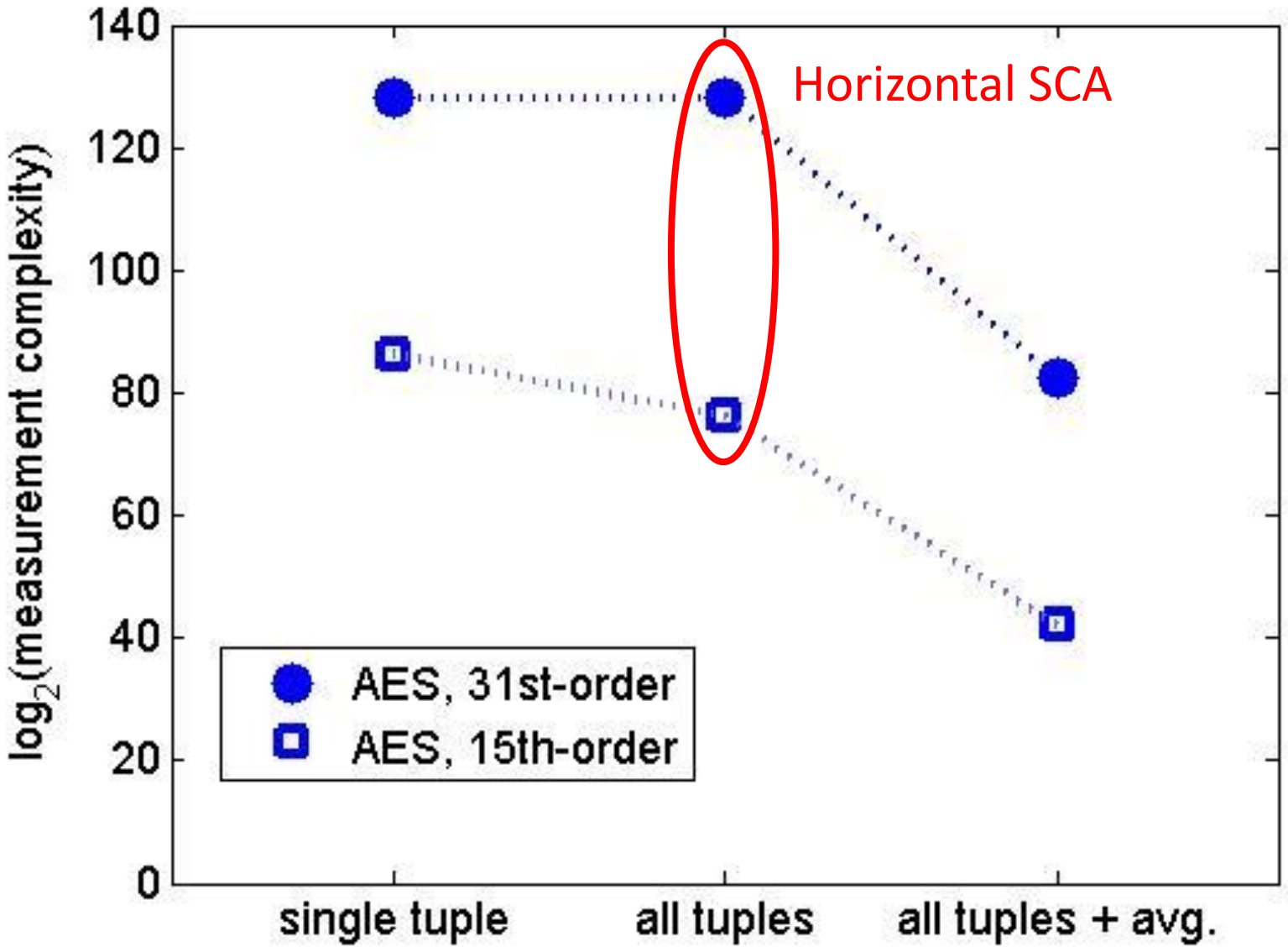


- SNR(=0,05) computed with linear regression
- **MI** of the encoding
- **31**/**15**/**7**-order security if flaw **f**=**1**/**2**/**4**
- Averaging: multiple apparition of sensitive values

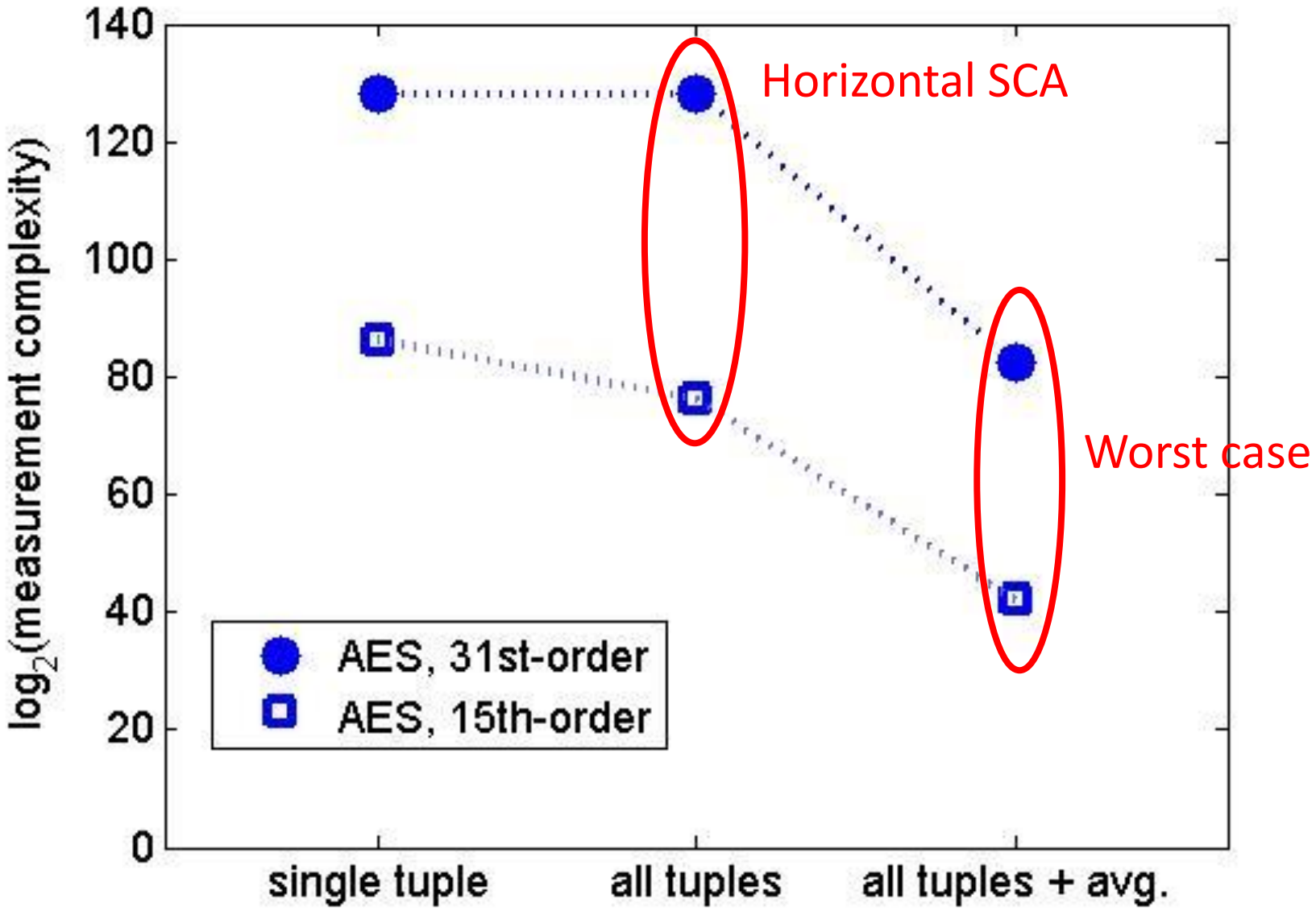
Putting things together



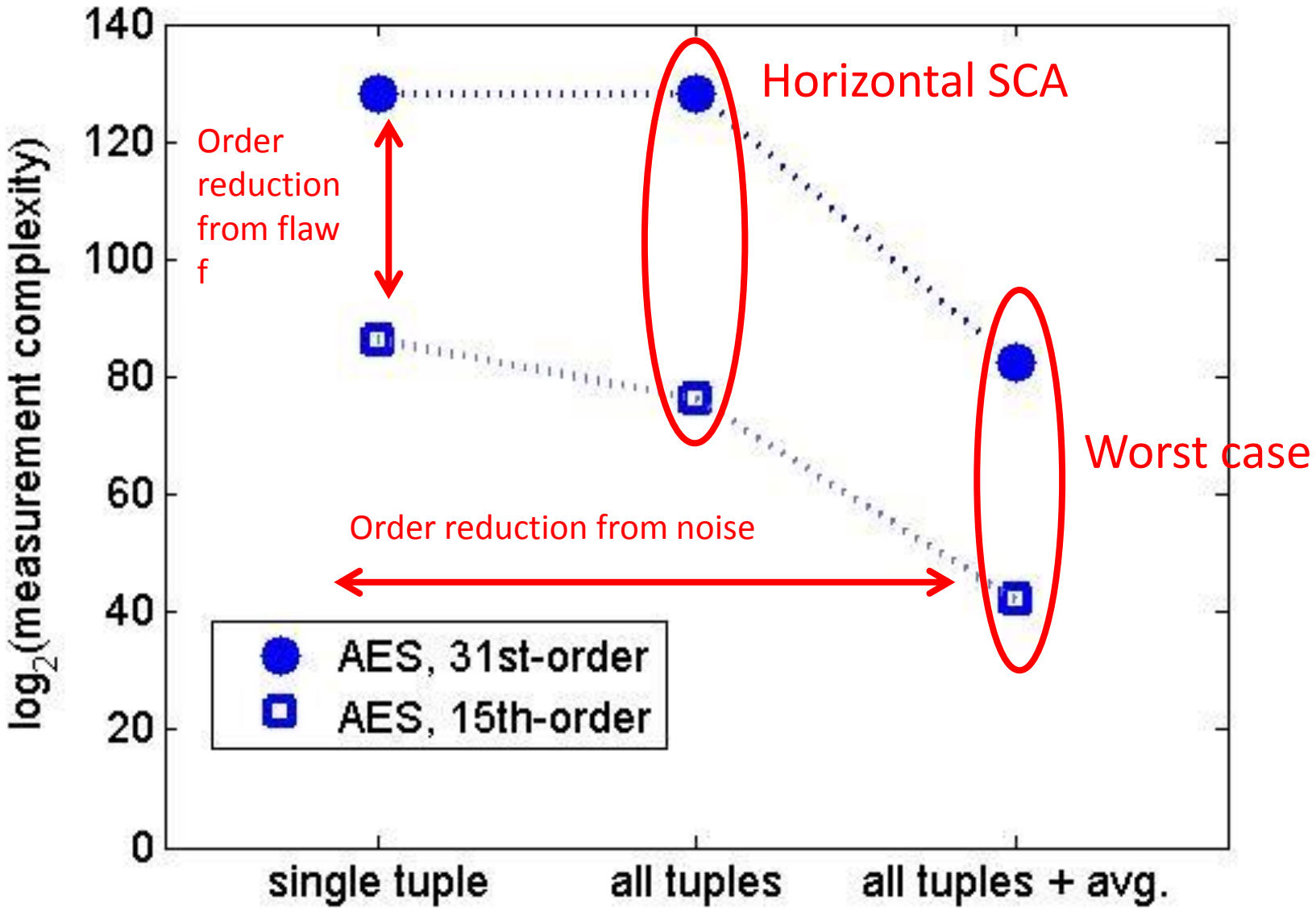
Putting things together



Putting things together



Putting things together



Outline

- **Background**
  - Masking
  - Barthe *et al.* masking scheme
- **How fast can be very high-order masking ?**
  - Data representation
  - AES results and discussion
- **How can we evaluate security at very high order ?**
  - Limitation of leakage detection strategy
  - Multi-model approach
- **Conclusion/Open problems**

Conclusion

Conclusion

- Very high order (32 shares) implementation **is not out of reach !**

Conclusion

- Very high order (32 shares) implementation **is not out of reach !**
- Multi-model approach proposed to evaluate very HO masked implementations (**security level**)

Conclusion

- Very high order (32 shares) implementation **is not out of reach !**
- Multi-model approach proposed to evaluate very HO masked implementations (**security level**)
- Based on **falsifiable assumptions**

Conclusion

- Very high order (32 shares) implementation **is not out of reach !**
- Multi-model approach proposed to evaluate very HO masked implementations (**security level**)
- Based on **falsifiable assumptions**

- Open problems:
  - Implem. when size register ≠ number of shares ?
  - Full code analysis to reduce refreshing
  - Thwart averaging with better S-box representation ?

Conclusion

- Very high order (32 shares) implementation **is not out of reach !**
- Multi-model approach proposed to evaluate very HO masked implementations (**security level**)
- Based on **falsifiable assumptions**

- Open problems:
  - Implem. when size register ≠ number of shares ?
  - Full code analysis to reduce refreshing
  - Thwart averaging with better S-box representation ?

Thanks for your attention