Masking AES with d+1 Shares in Hardware

Thomas De Cnudde
Oscar Reparaz
Begül Bilgin
Svetla Nikova
Ventzislav Nikov
Vincent Rijmen

08/18 – CHES 2016 – Santa Barbara

“In theory there is no difference between theory and practice.

“In theory there is no difference between theory and practice.

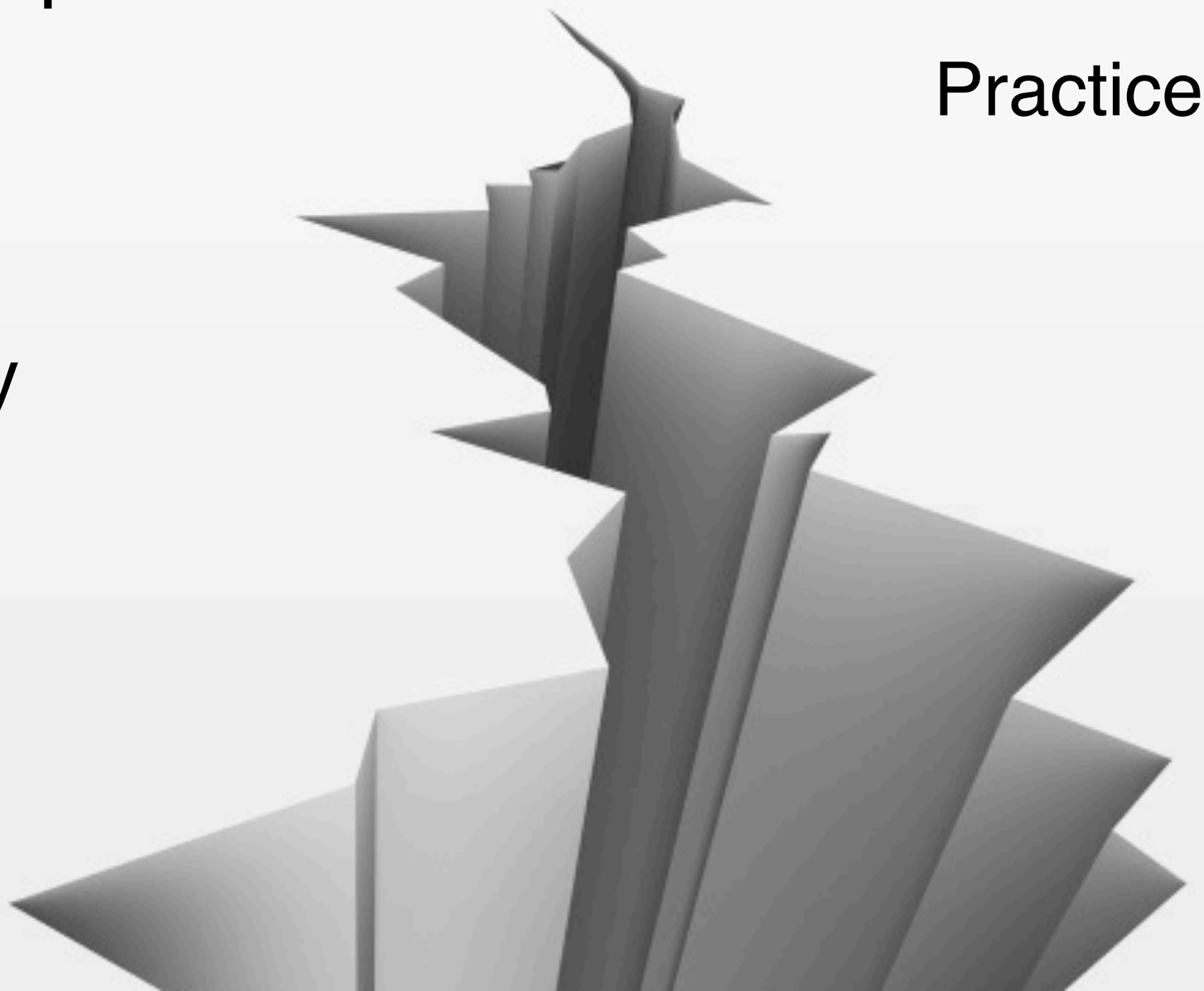
In practice there is.”

“In theory there is no difference between theory and practice.

In practice there is.”

Practice

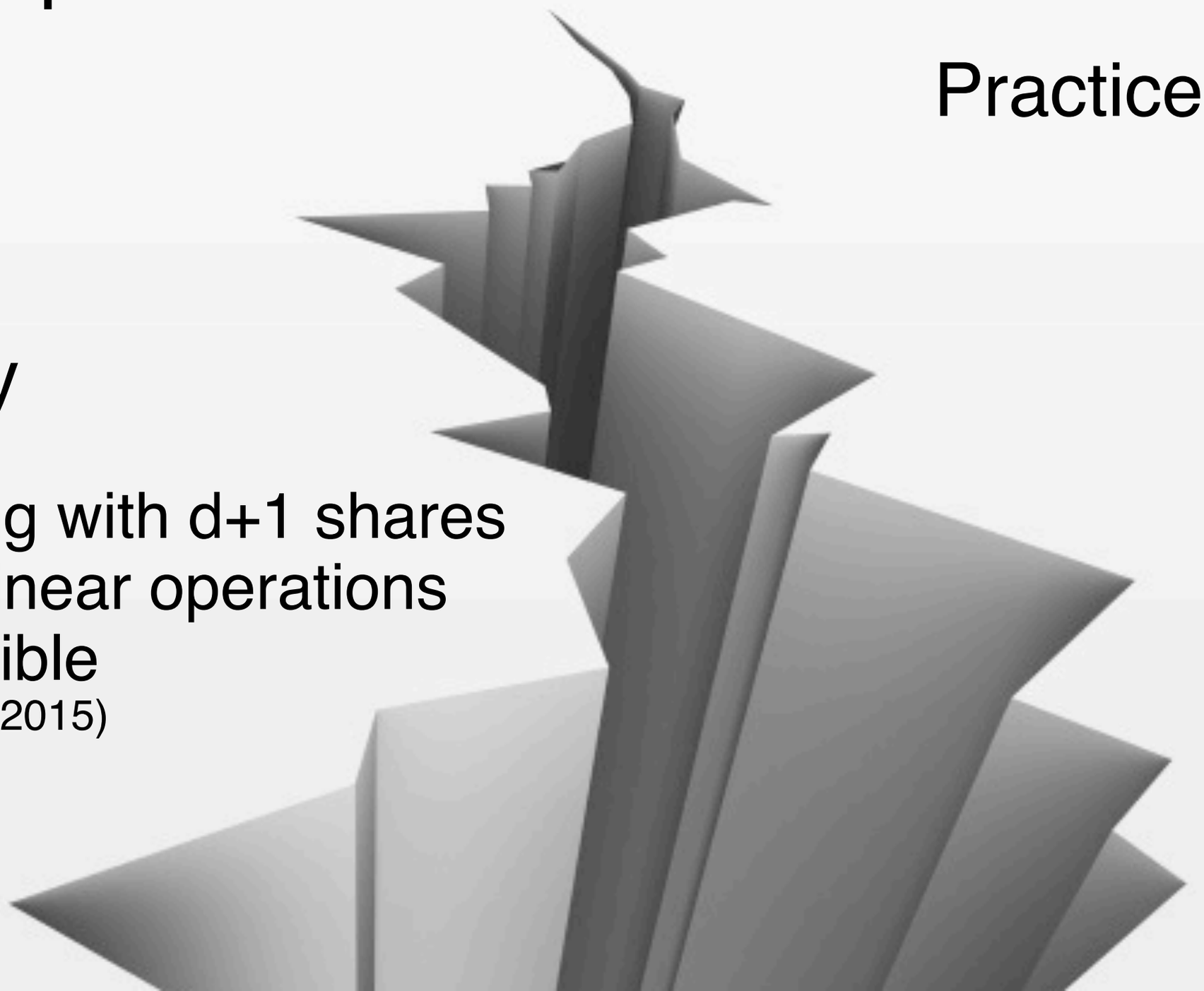
Theory



“In theory there is no difference between theory and practice.

In practice there is.”

Practice

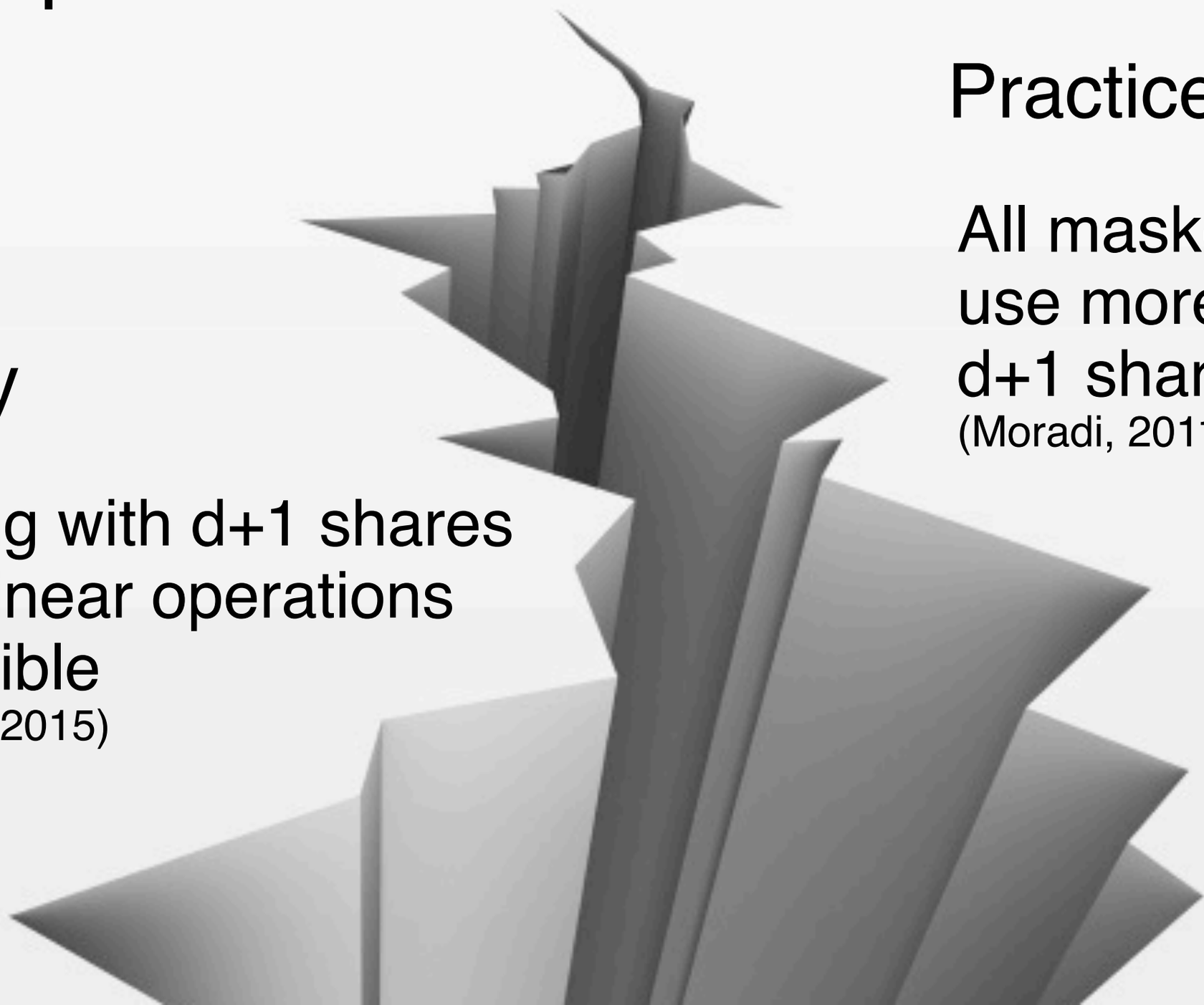


Theory

Masking with d+1 shares in nonlinear operations is possible
(Reparaz, 2015)

"In theory there is no difference between theory and practice.

In practice there is."



Theory

Masking with d+1 shares in nonlinear operations is possible
(Reparaz, 2015)

Practice

All masked AES use more than d+1 shares
(Moradi, 2011, Bilgin, 2015, ...)

We realized and verified the smallest masked AES in hardware

Theory

Masking with d+1 shares
in nonlinear operations
is possible
(Reparaz, 2015)

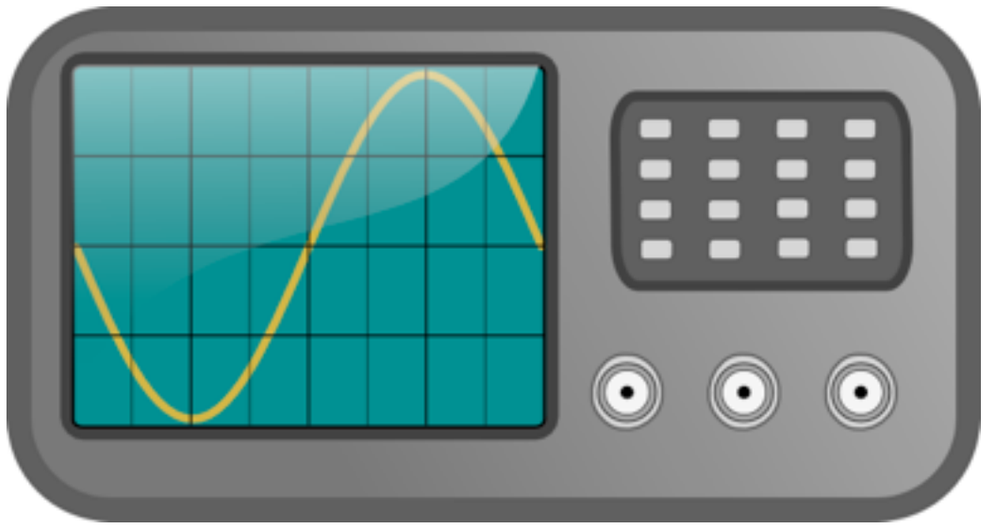
Practice

- 1st - order
- 2nd- order

with d+1 shares

Masking AES with d+1 Shares in Hardware

Threshold Implementations



SCA Evaluation

Implementation Cost

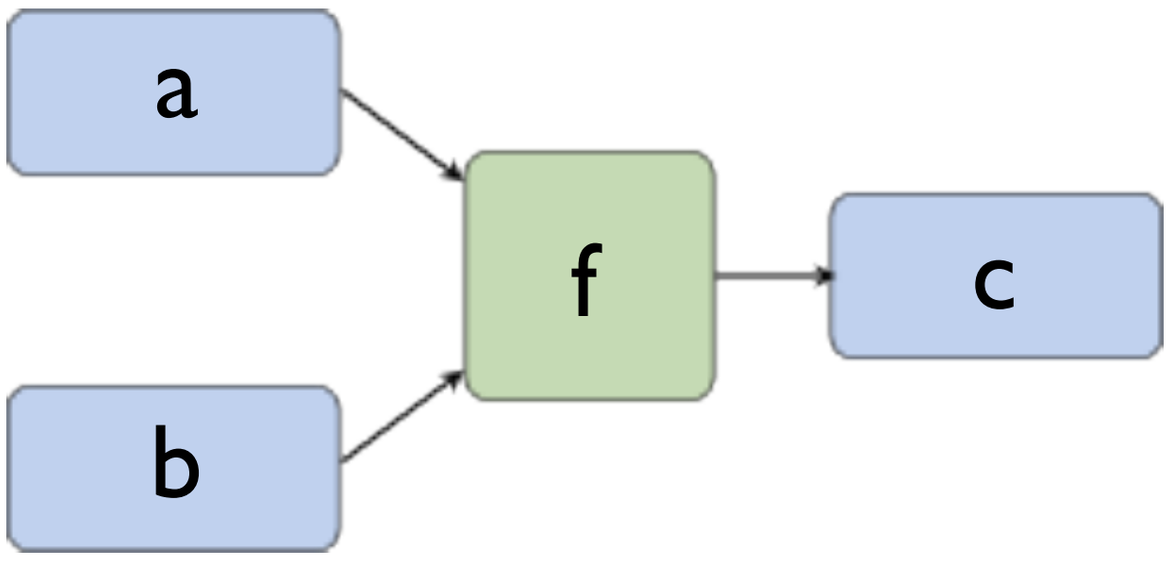
Threshold Implementations is a SCA countermeasure

Provable security with minimal assumptions on the hardware

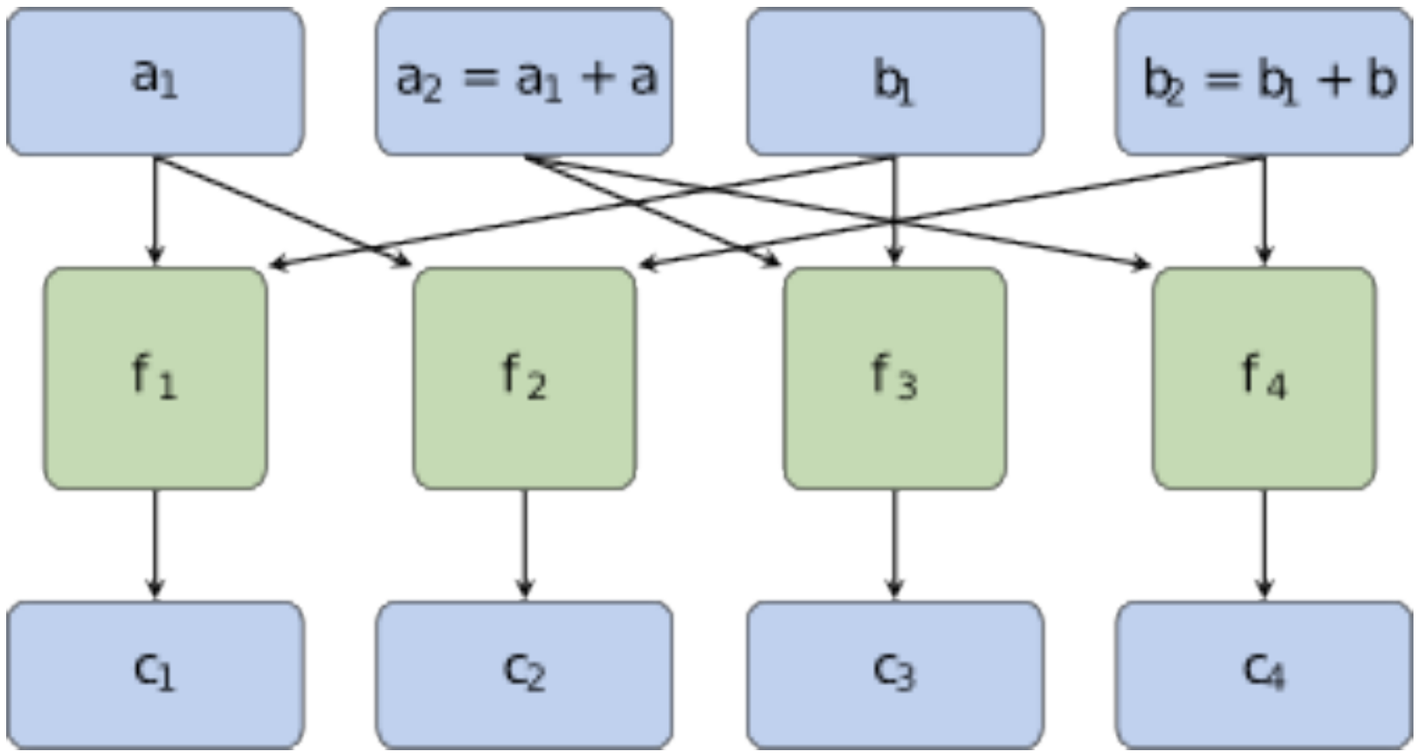
Threshold Implementations is a SCA countermeasure

Provable security with minimal assumptions on the hardware

Boolean masking scheme based on secret sharing and multiparty computation



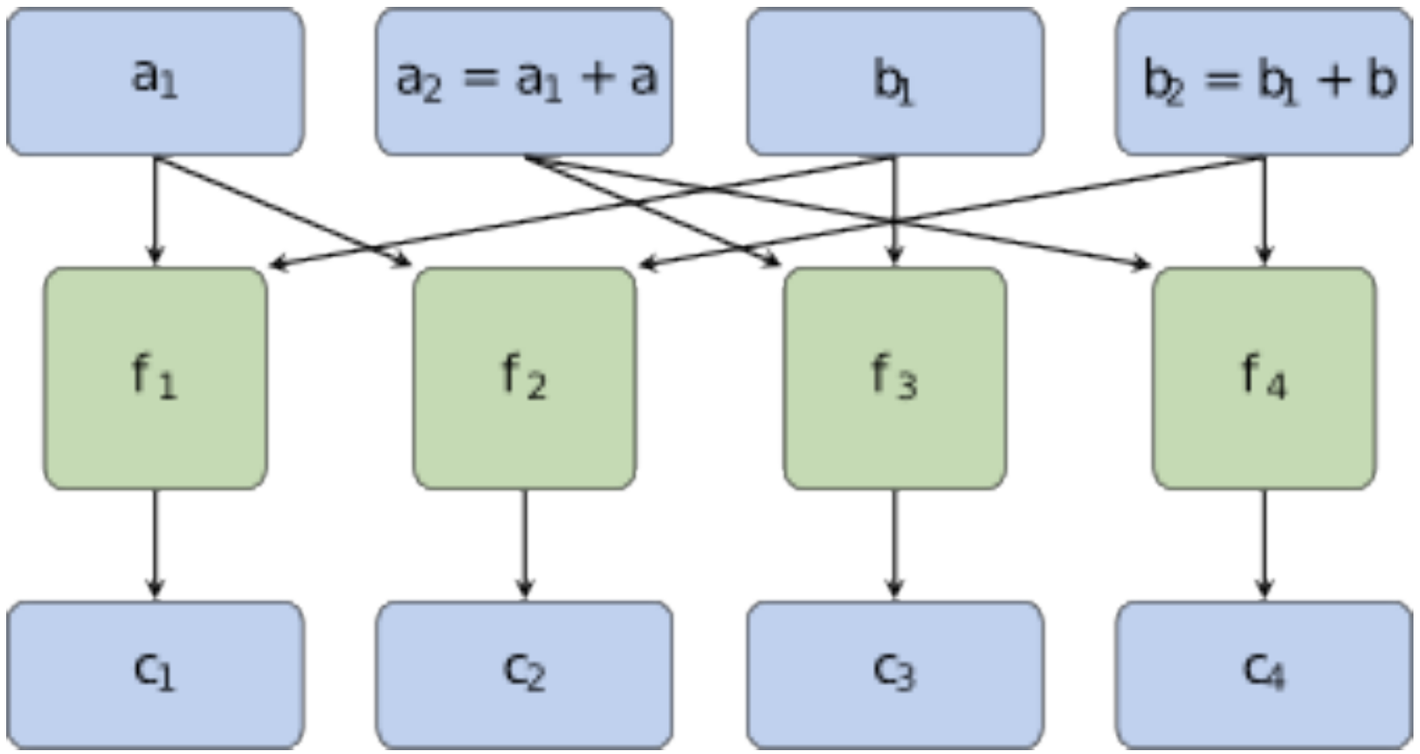
Threshold Implementations must satisfy conditions



Uniform Inputs

Correctness

Threshold Implementations must satisfy conditions

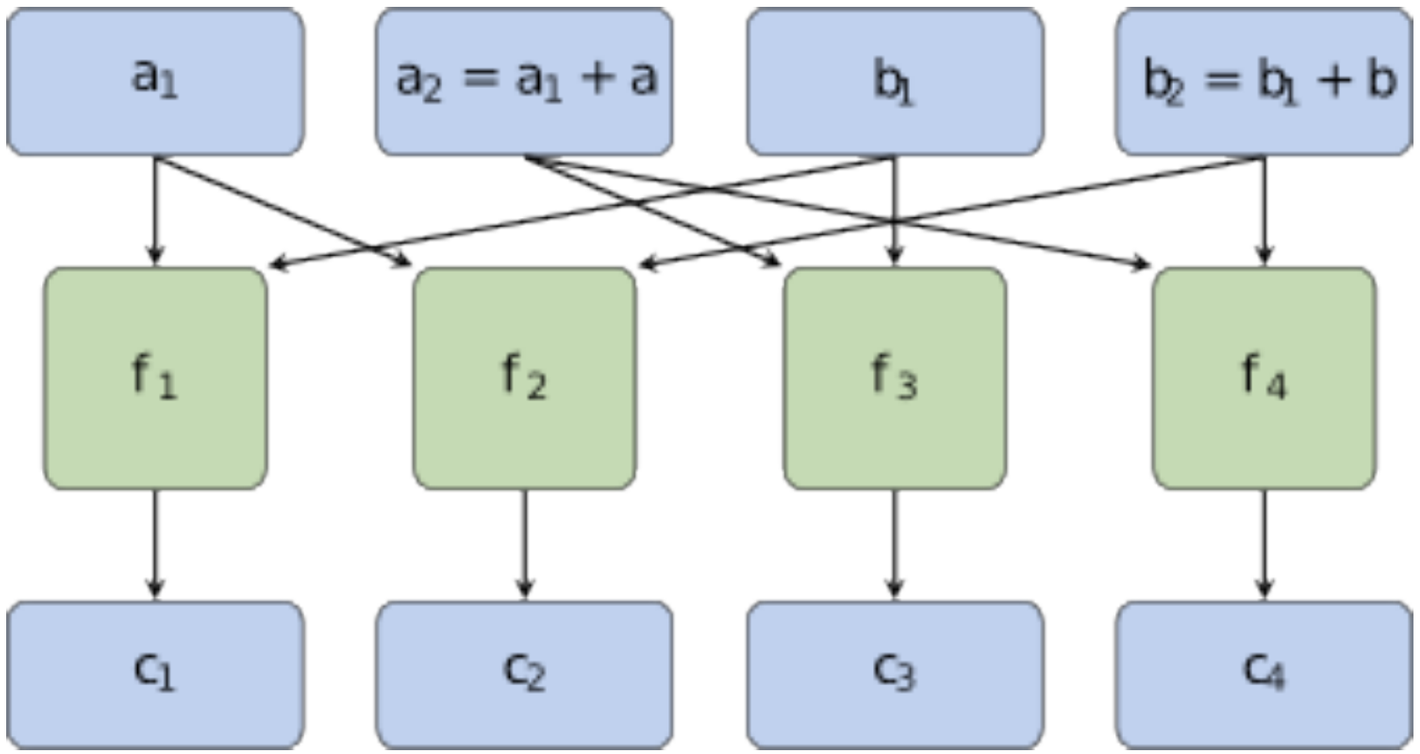


Uniform Inputs

Correctness

d^{th}-order non-completeness

Threshold Implementations must satisfy conditions



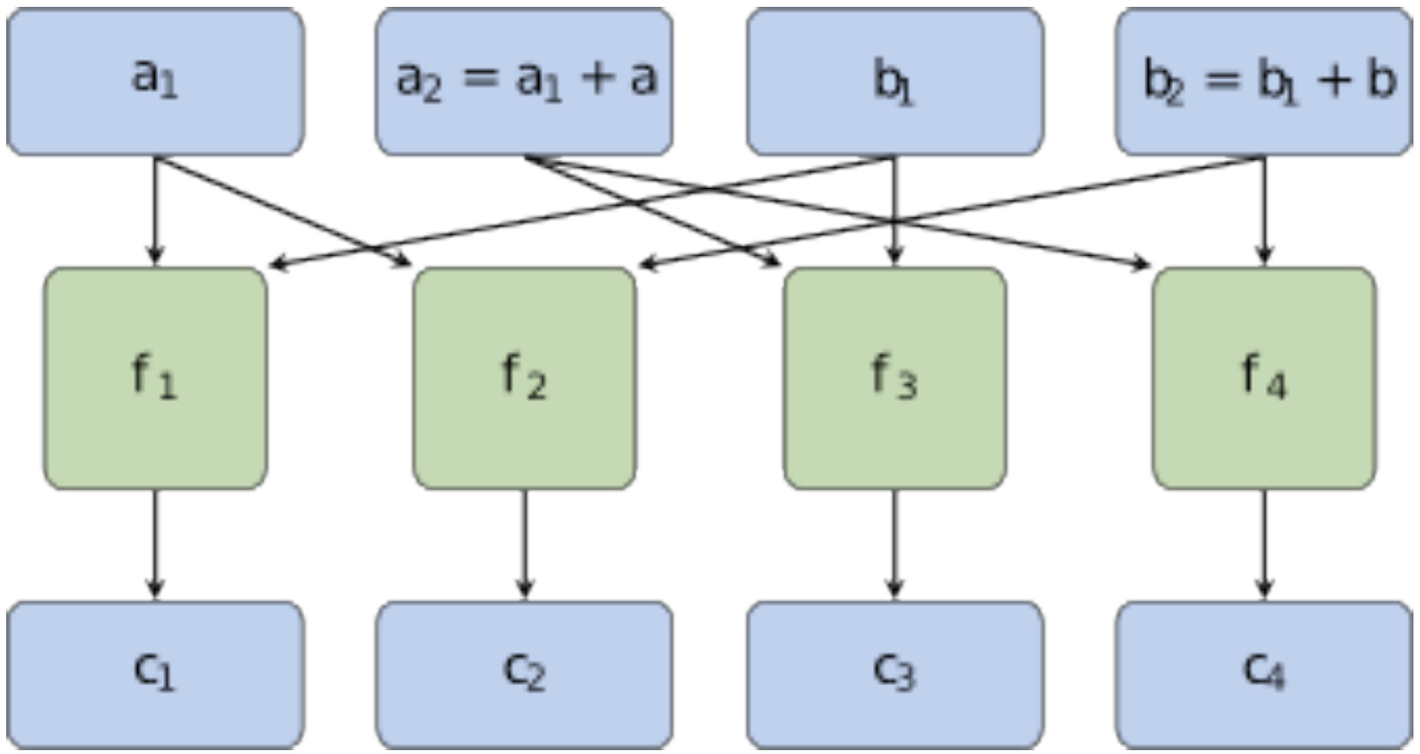
Uniform Inputs

Correctness

d^{th}-order non-completeness

Mask refreshing

One extra condition is required for using d+1 shares



Uniform Inputs

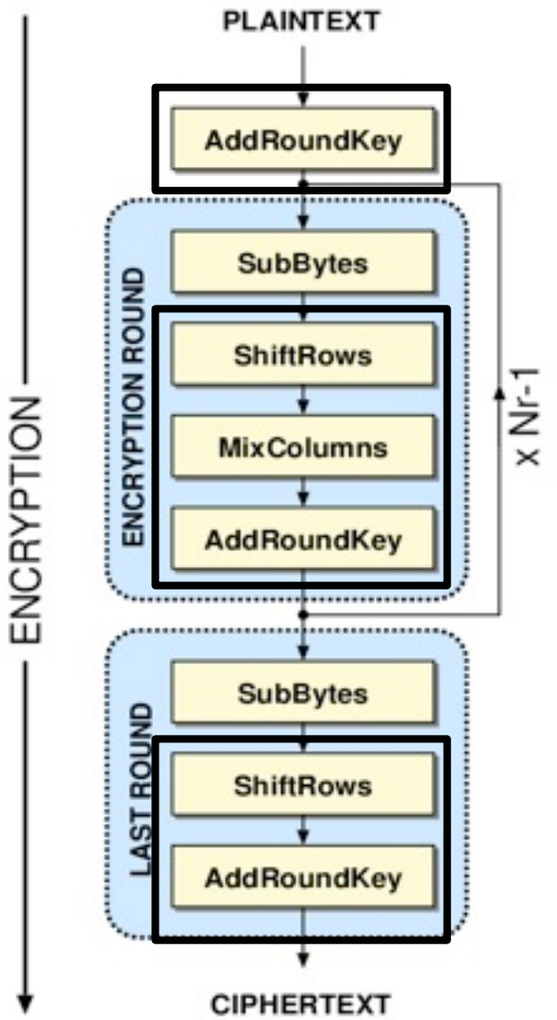
Correctness

d^{th}-order non-completeness

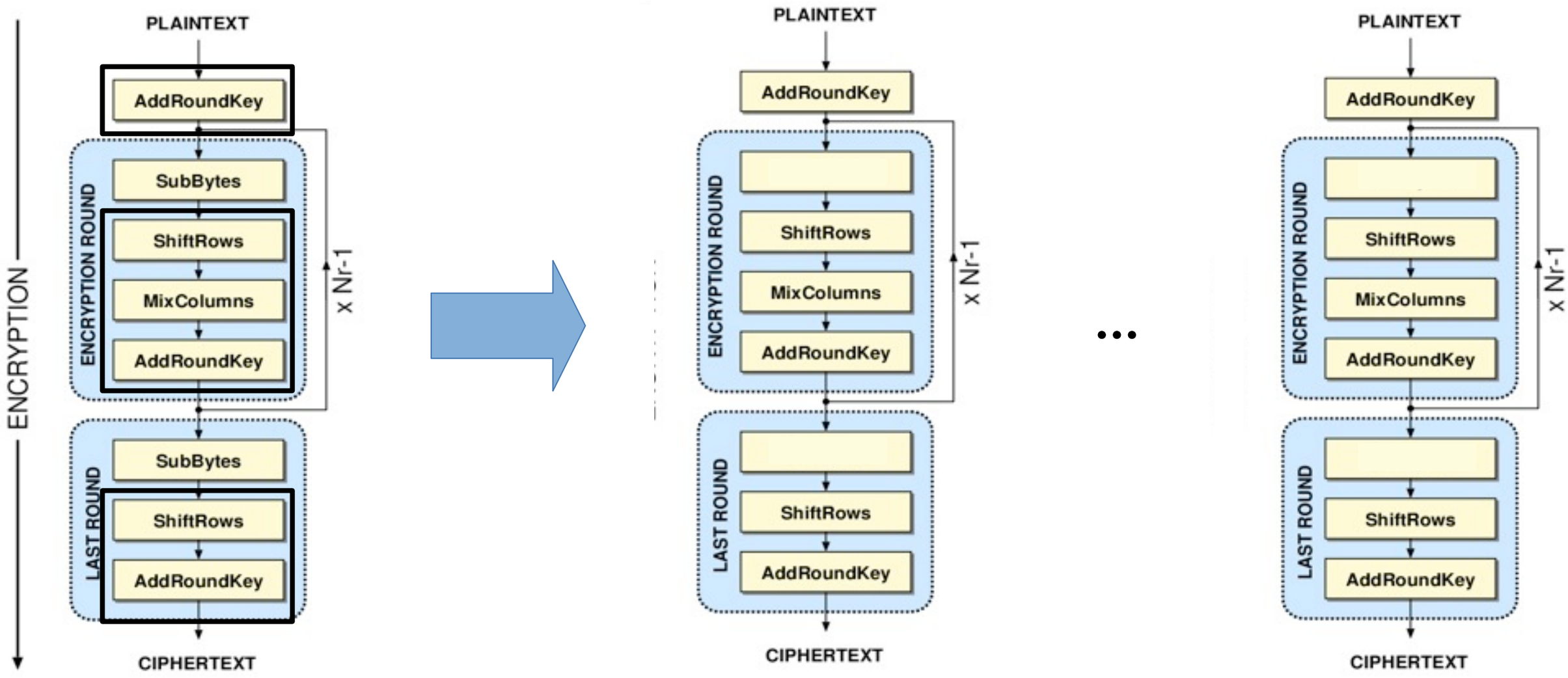
Mask refreshing

Independent input shares

Linear/Affine operations are easy to mask



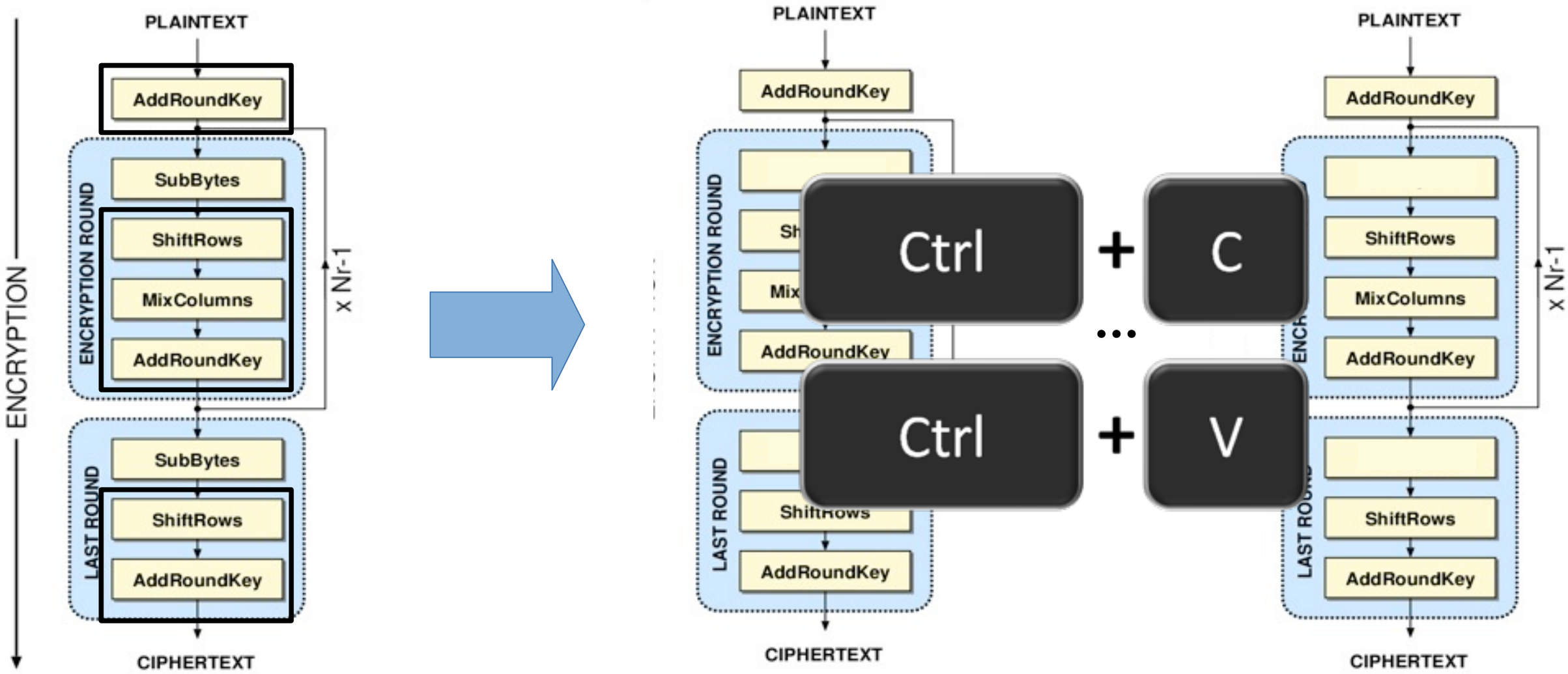
Linear/Affine operations are easy to mask



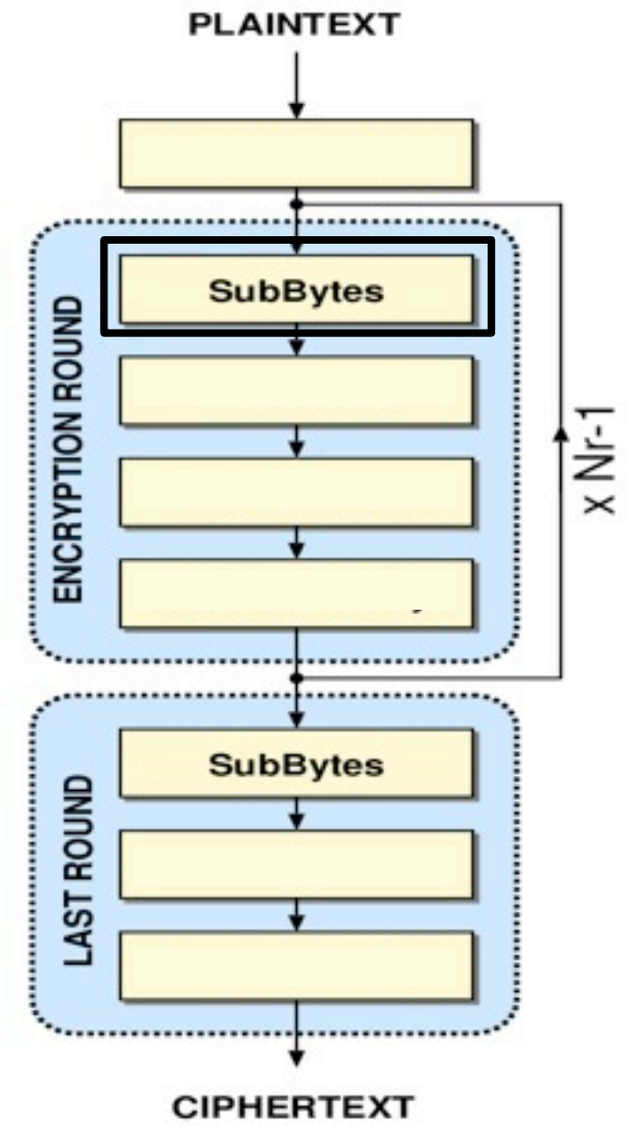
Share 1

Share d+1

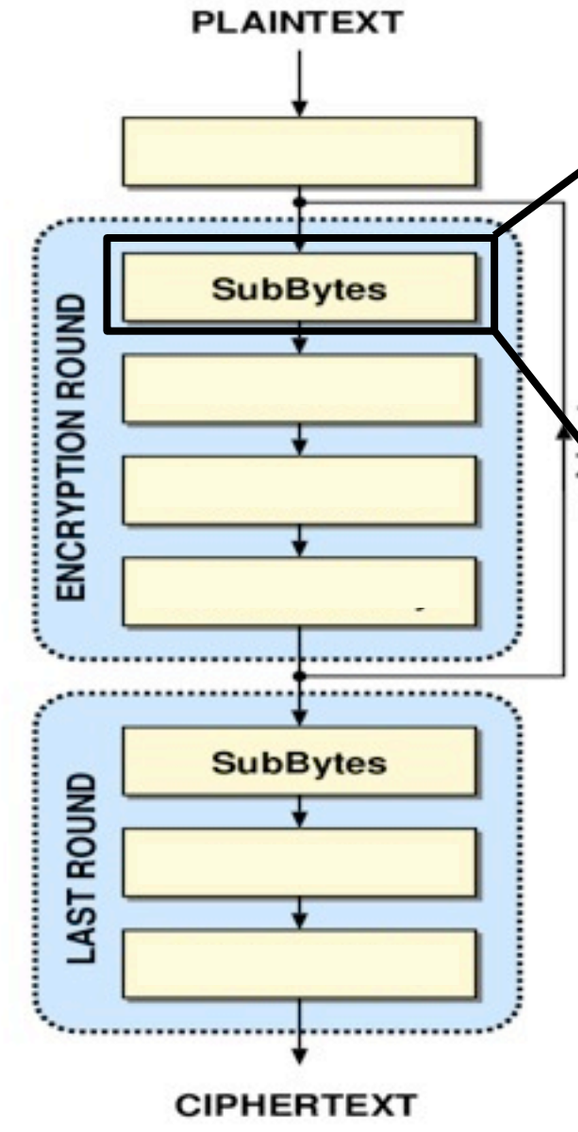
Linear/Affine operations are easy to mask

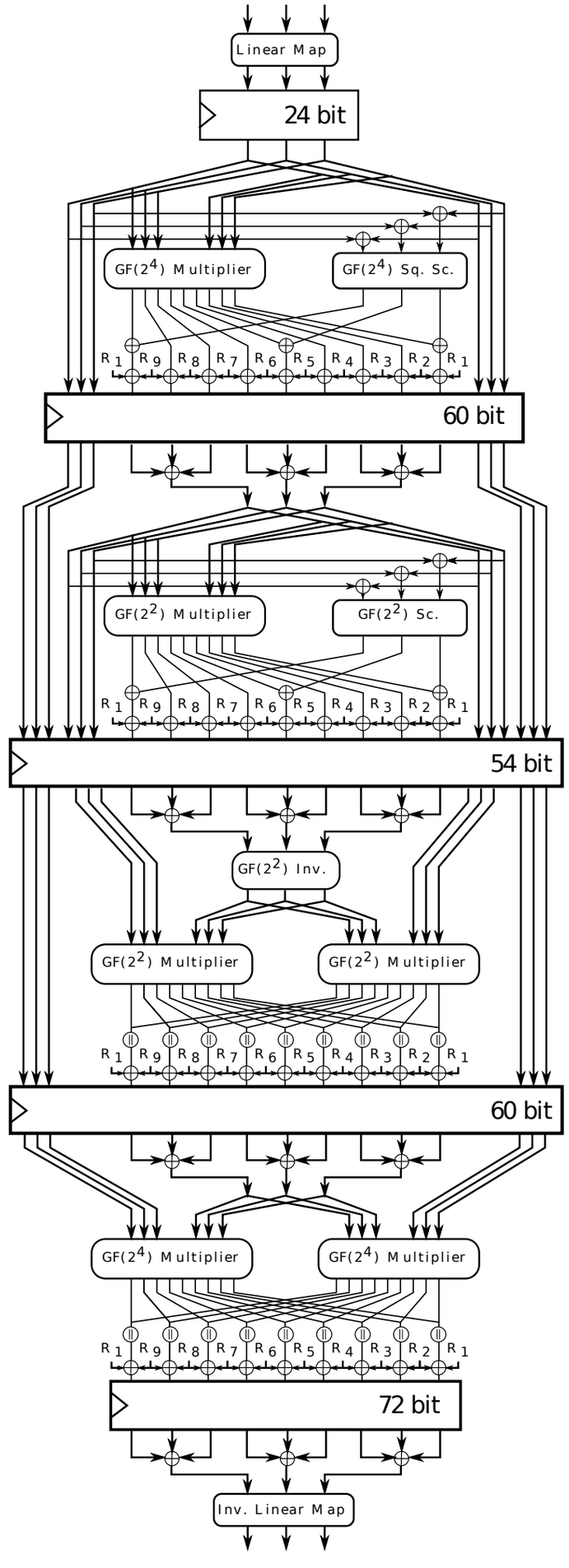


Nonlinear operations are harder to mask

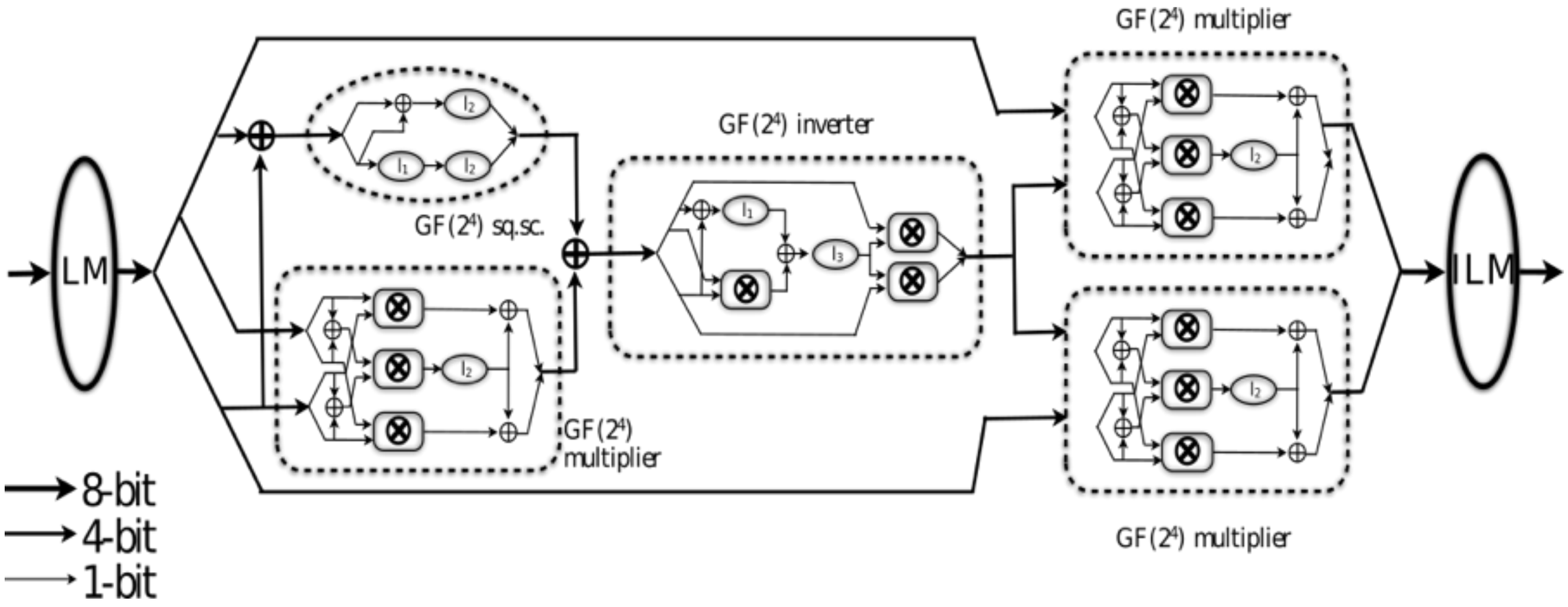


Nonlinear operations are harder to mask

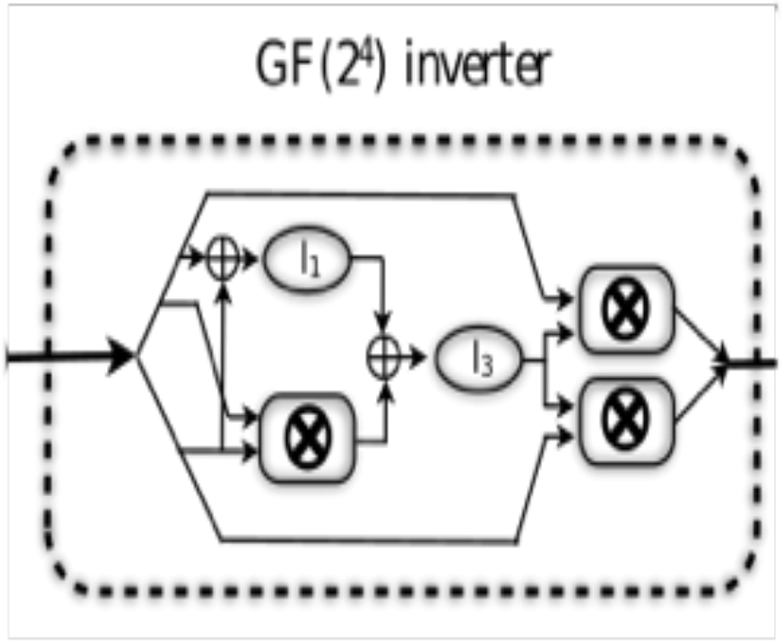




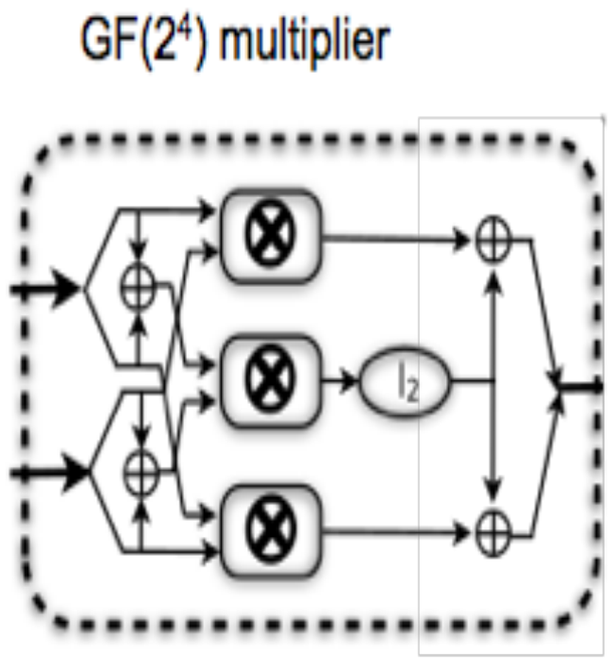
Canright's S-box decomposition has shown to be a good starting point



The number of output shares depends on the algebraic degree

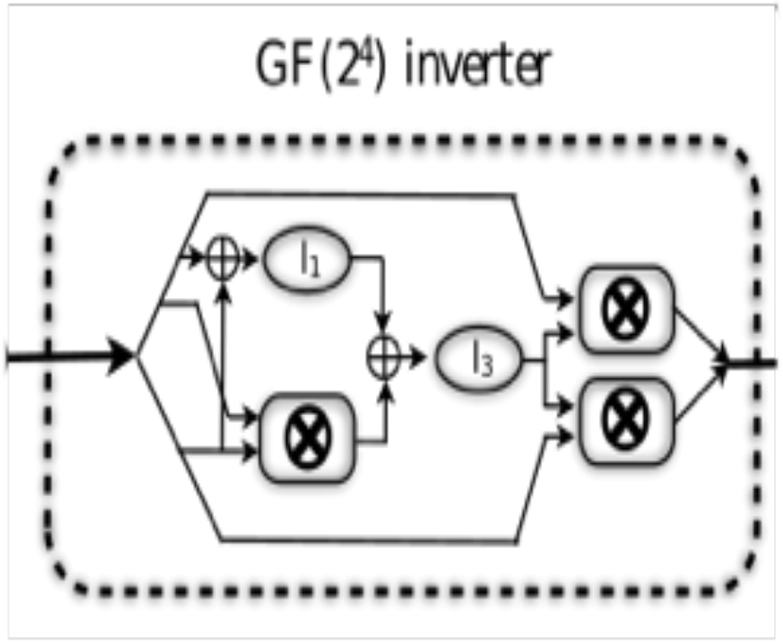


Algebraic degree = 3
$S_{out} = (d+1)^3$

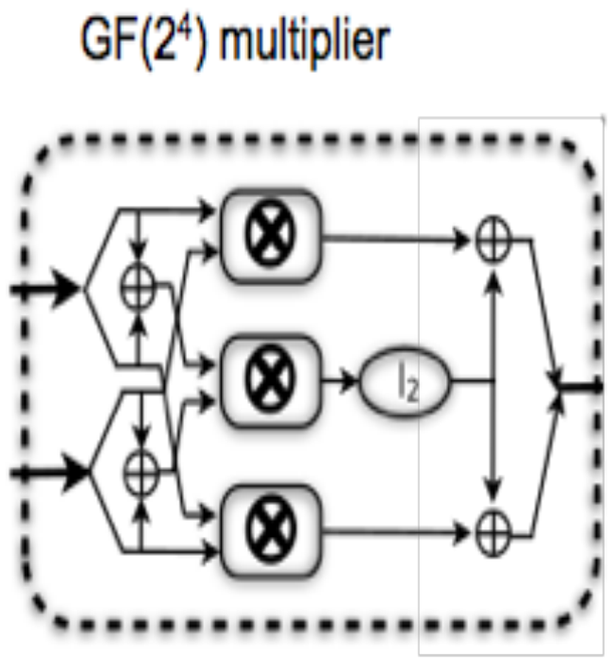


Algebraic degree = 2
$S_{out} = (d+1)^2$

The number of output shares depends on the algebraic degree



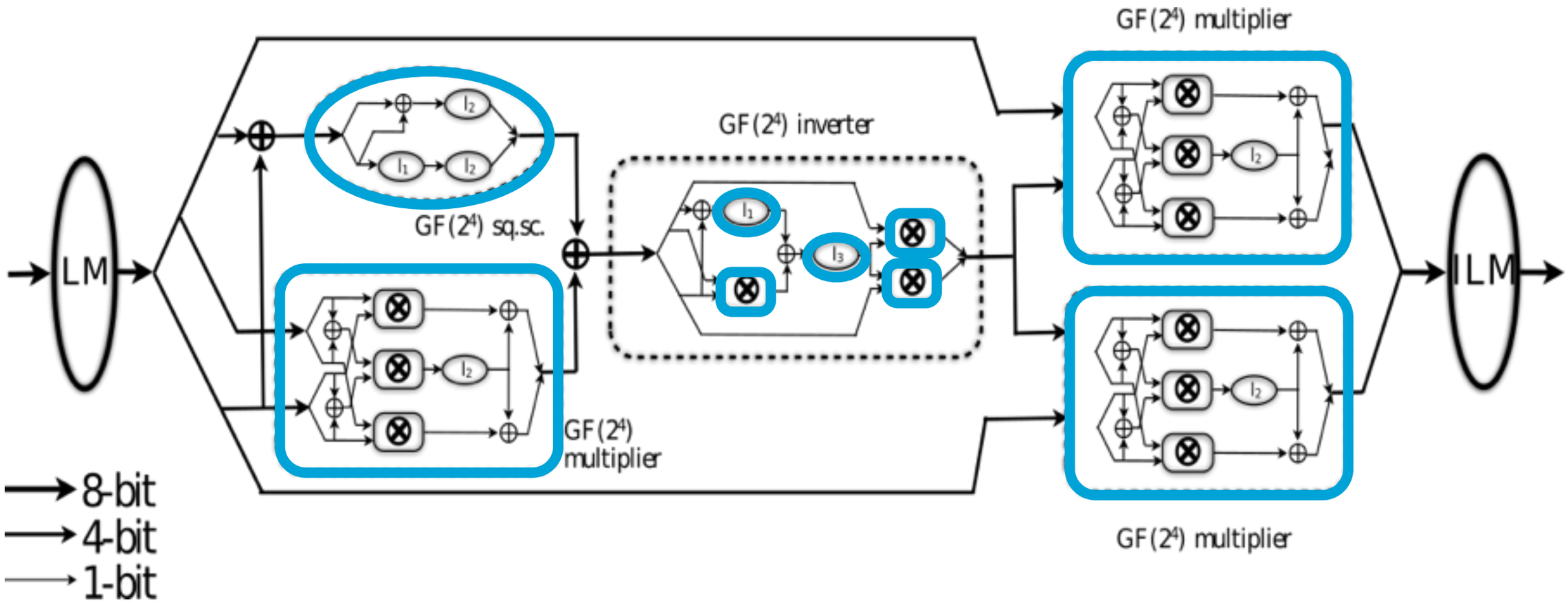
Algebraic degree = 3
$S_{out} = (d+1)^3$



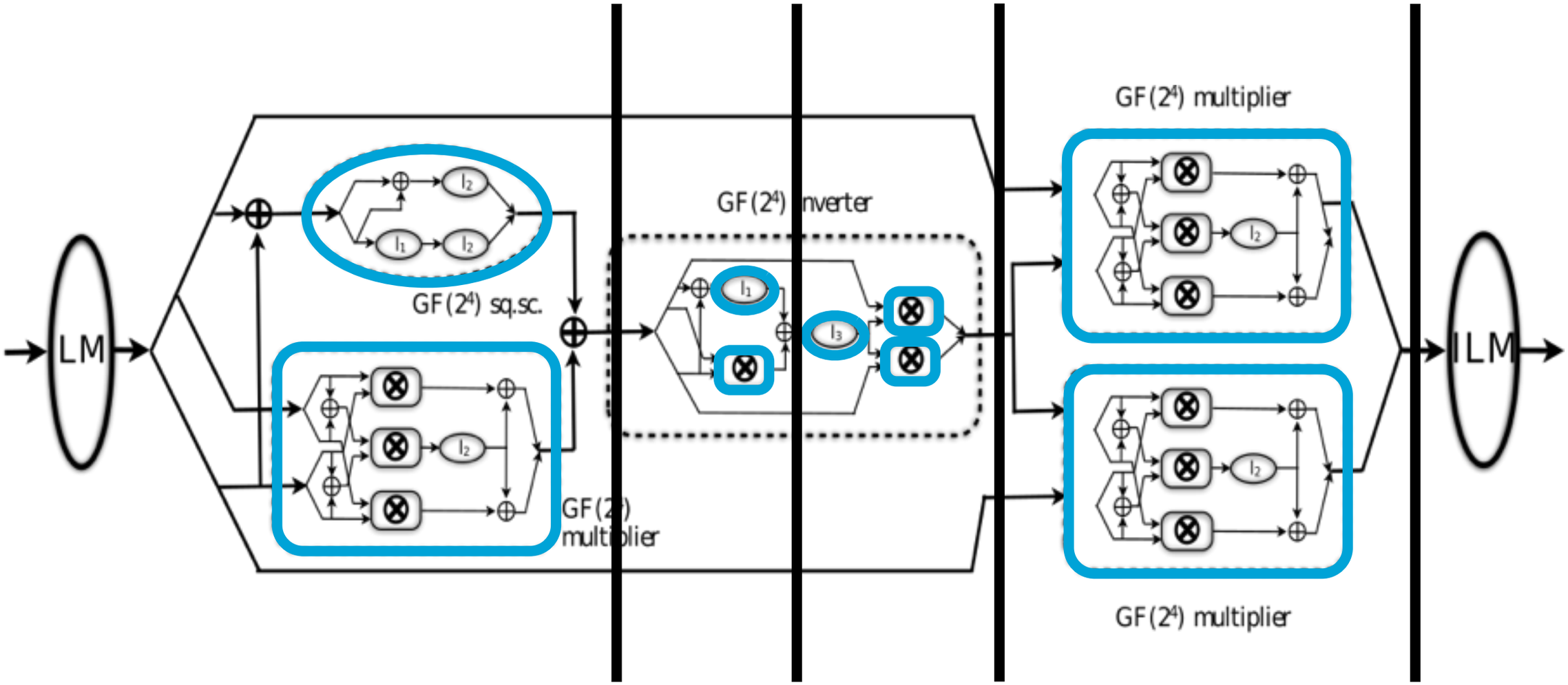
Algebraic degree = 2
$S_{out} = (d+1)^2$

A lower algebraic degree leads to a decrease in number of output registers and number of random masks

We partition Canright's S-box to only use multipliers

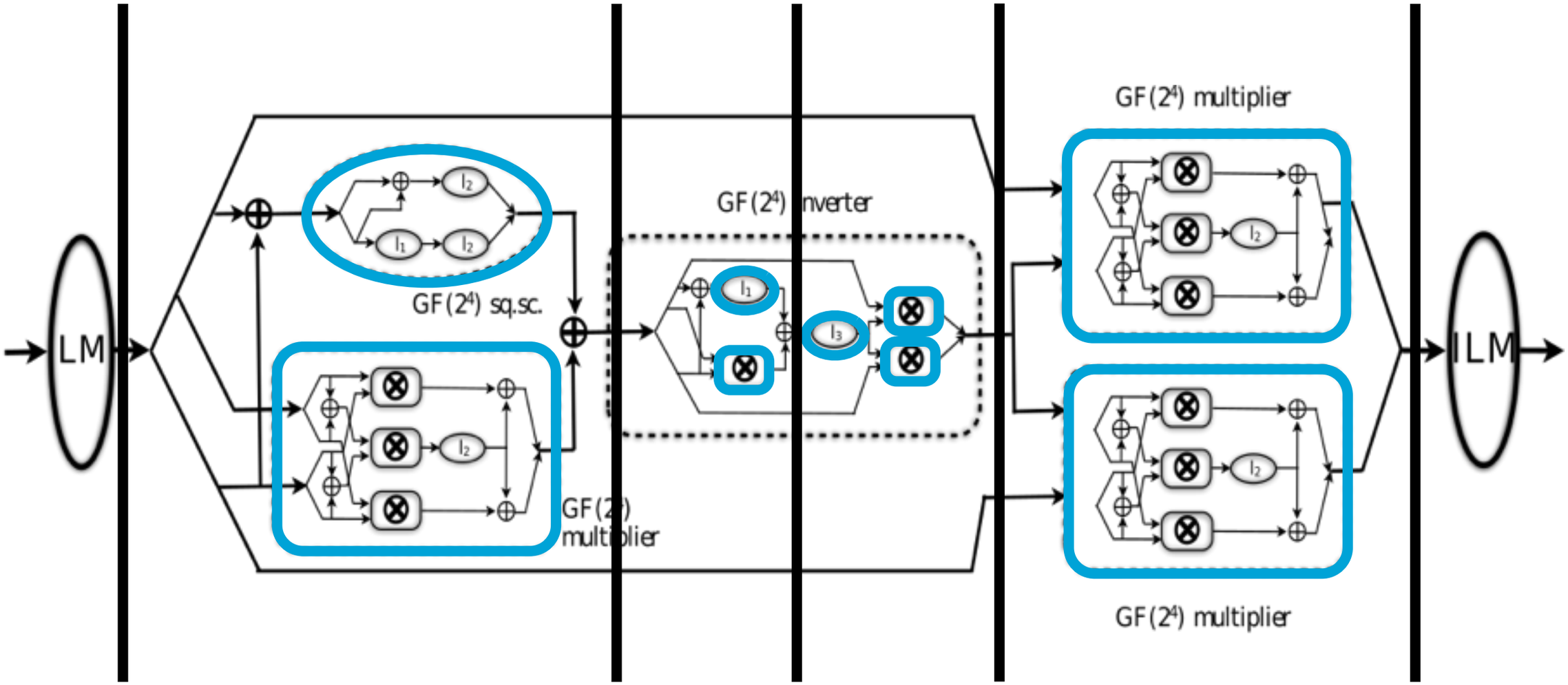


Masks are refreshed after each multiplier



Registers + Mask Refreshing

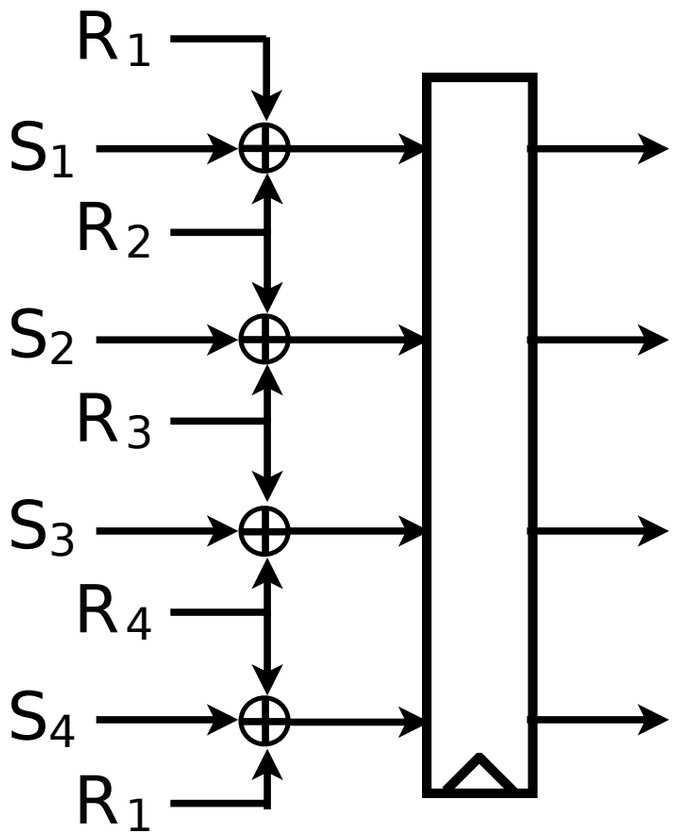
Masks are refreshed after each multiplier

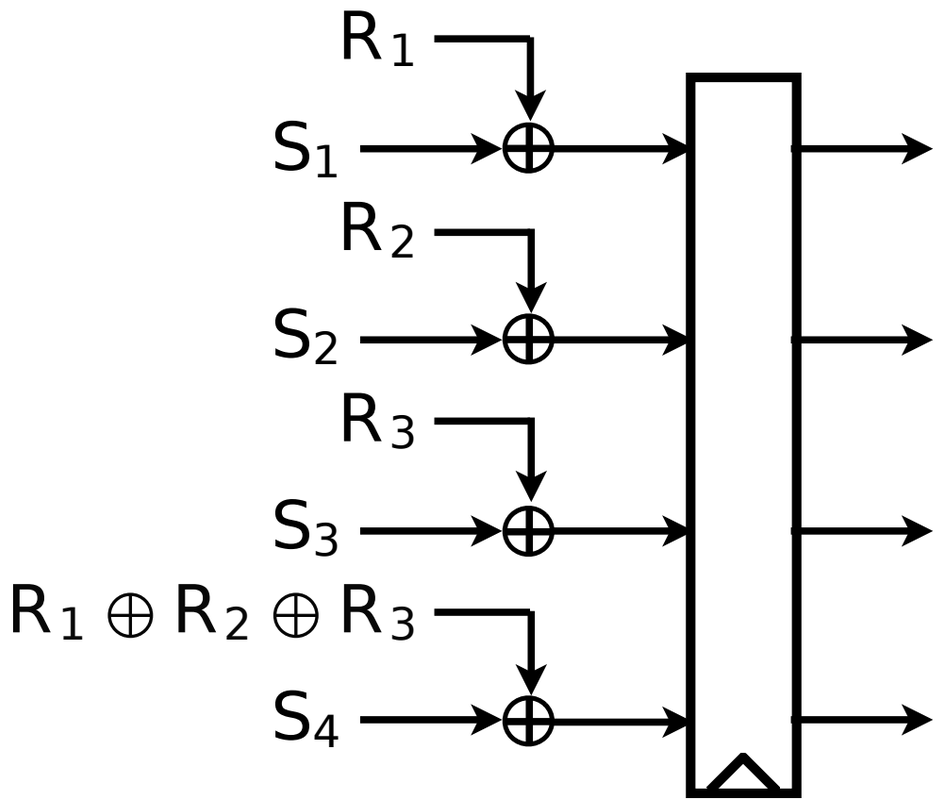


Registers

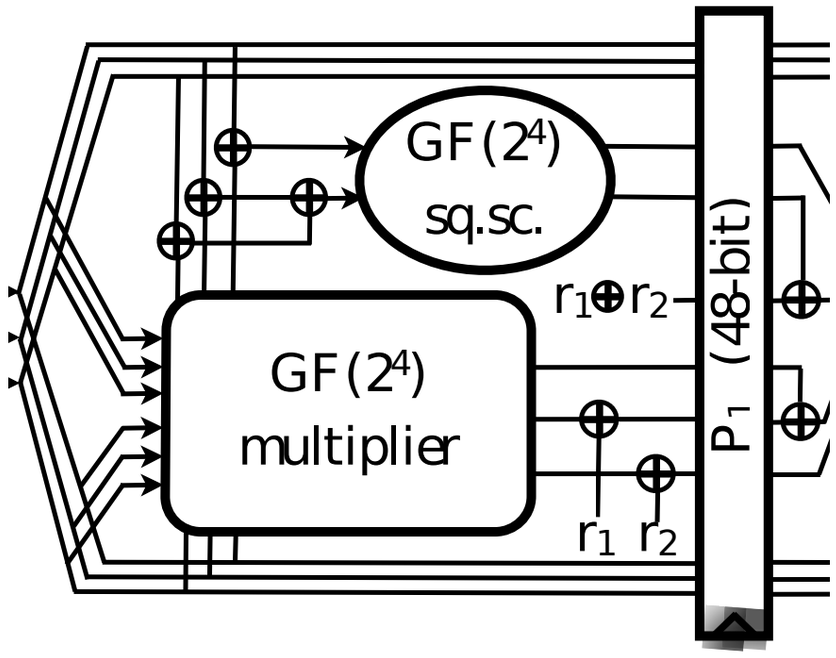
Registers + Mask Refreshing

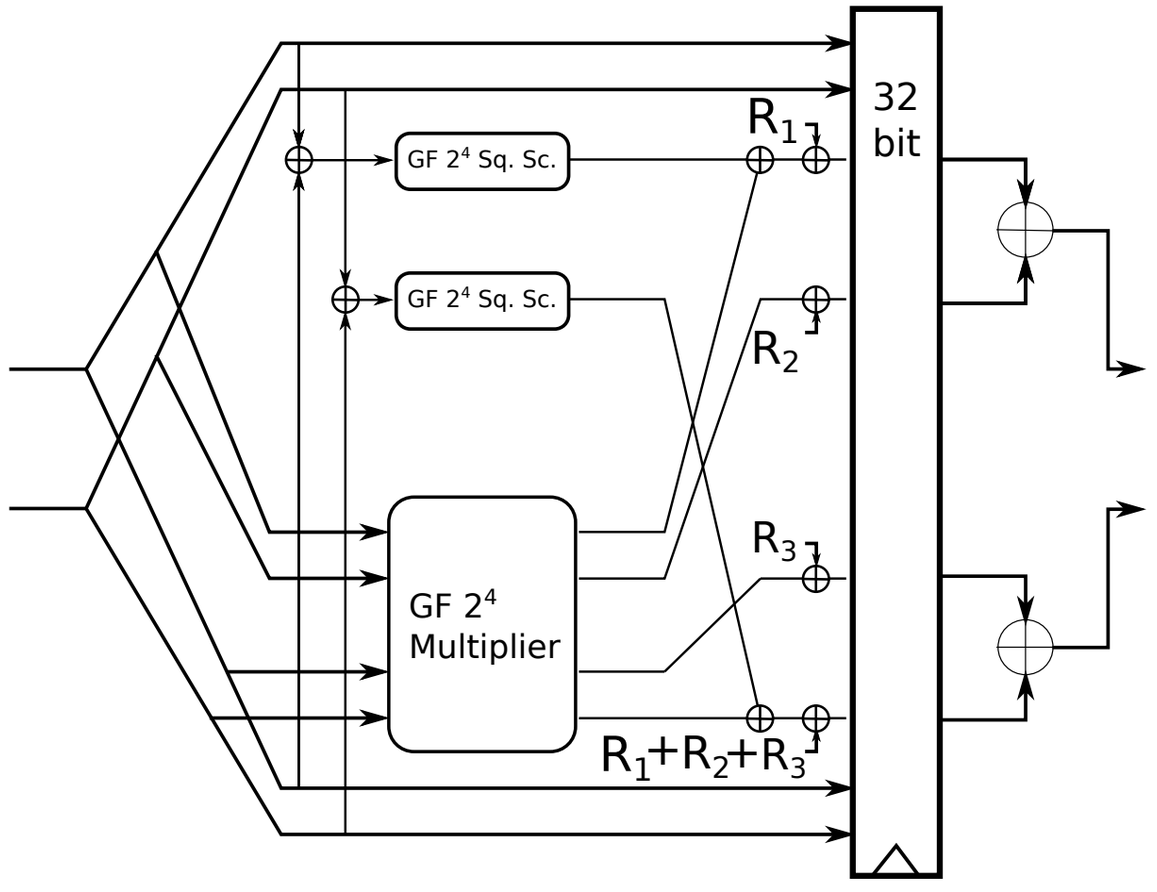
Total randomness was reduced for more efficient first-order security





We further reduce the area by adding outputs in a non-complete way

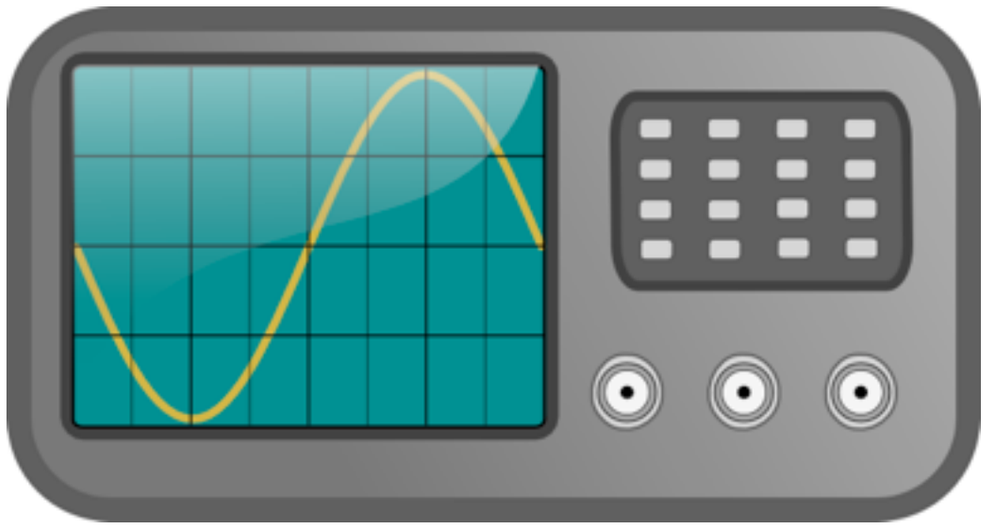




Bilgin, 2015

Masking AES with d+1 Shares in Hardware

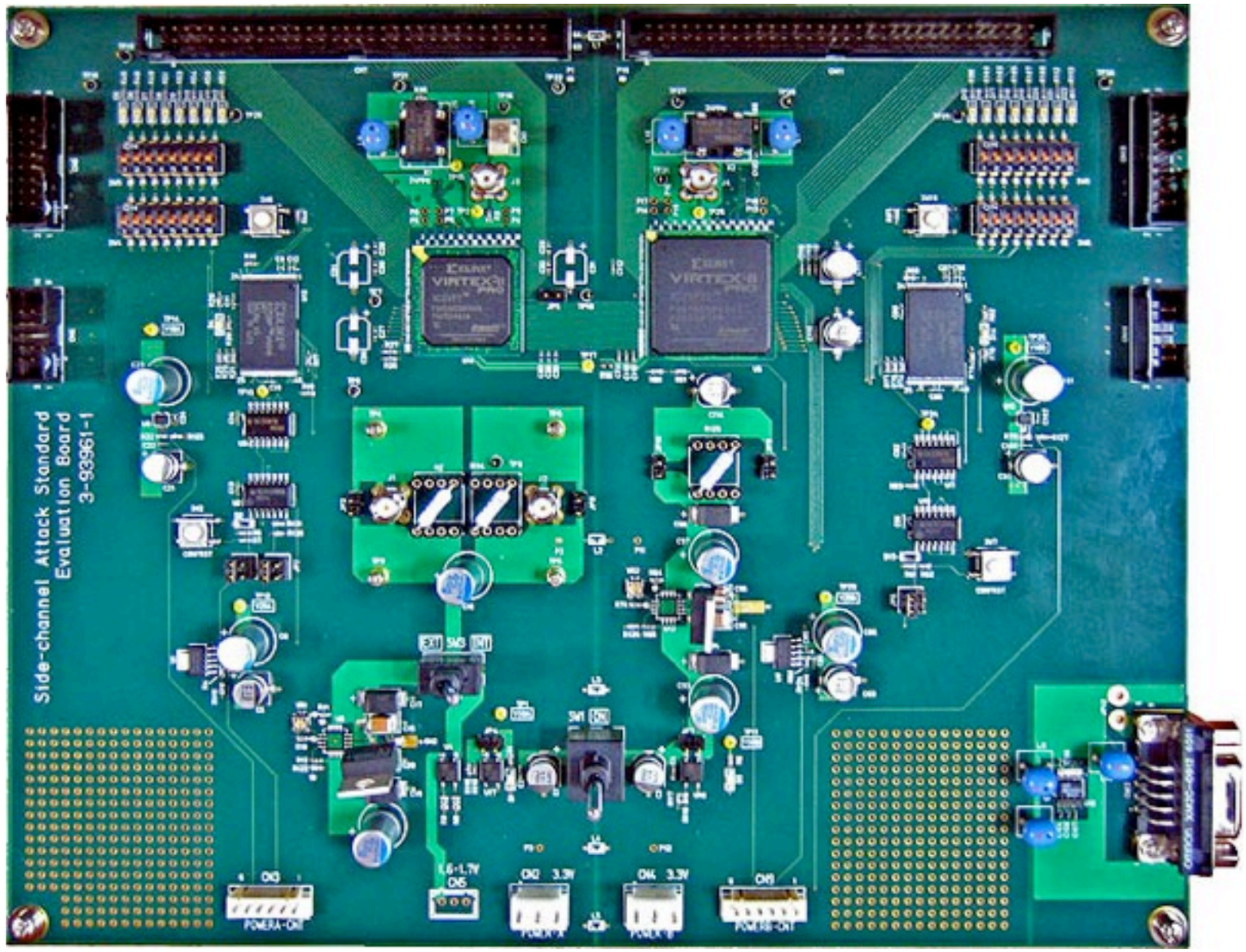
Threshold Implementations



SCA Evaluation

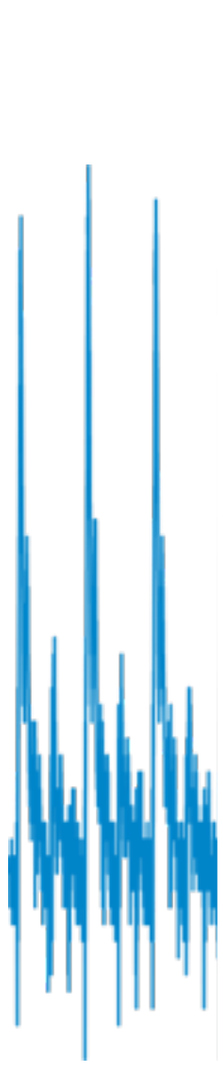
Implementation Cost

The SCA is performed on a low-noise platform

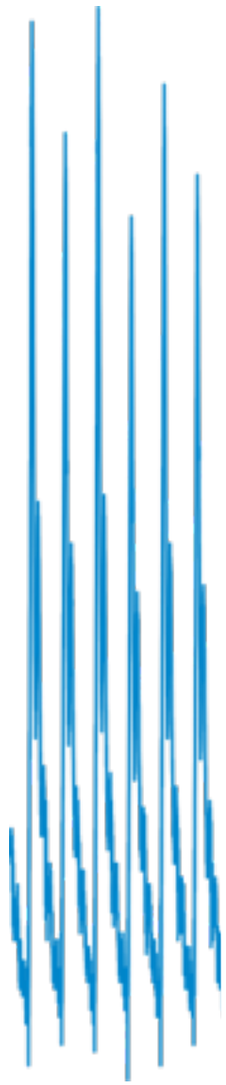


AES and mask generation are alternated to keep the noise low

Power



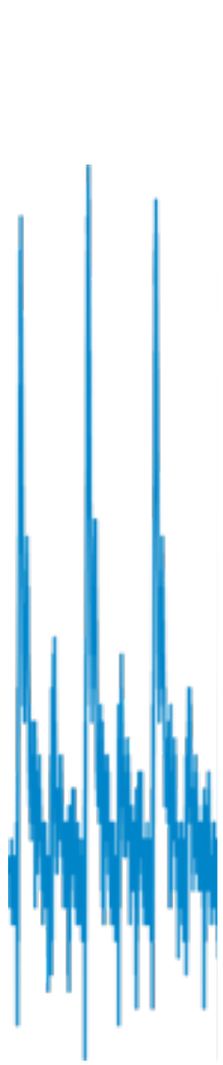
PRNG Off



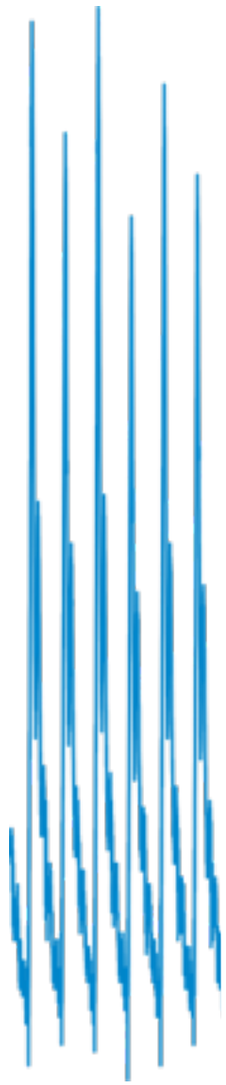
PRNG On

AES and mask generation are alternated to keep the noise low

Power



PRNG Off



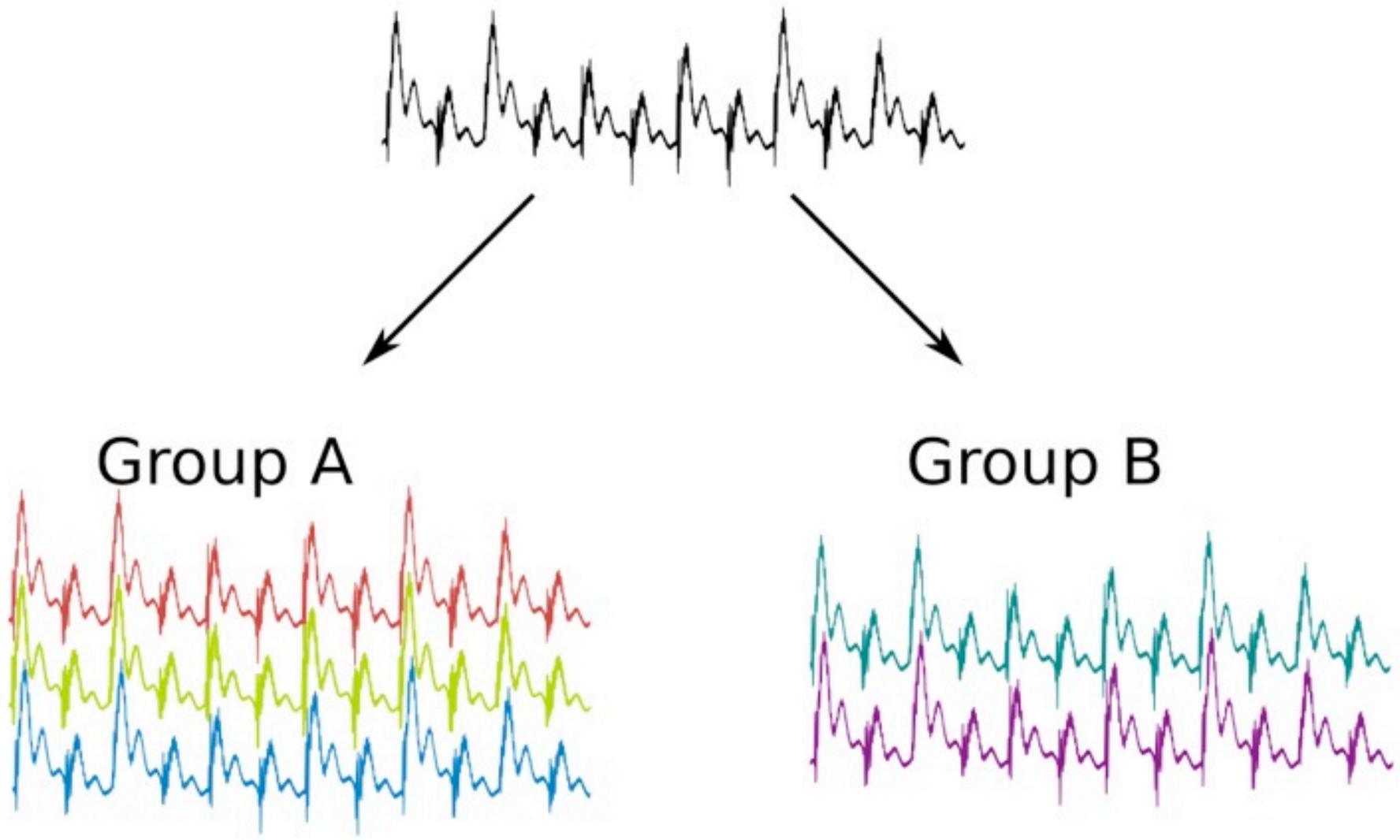
PRNG On

Randomness from parallel PRINCE PRNG

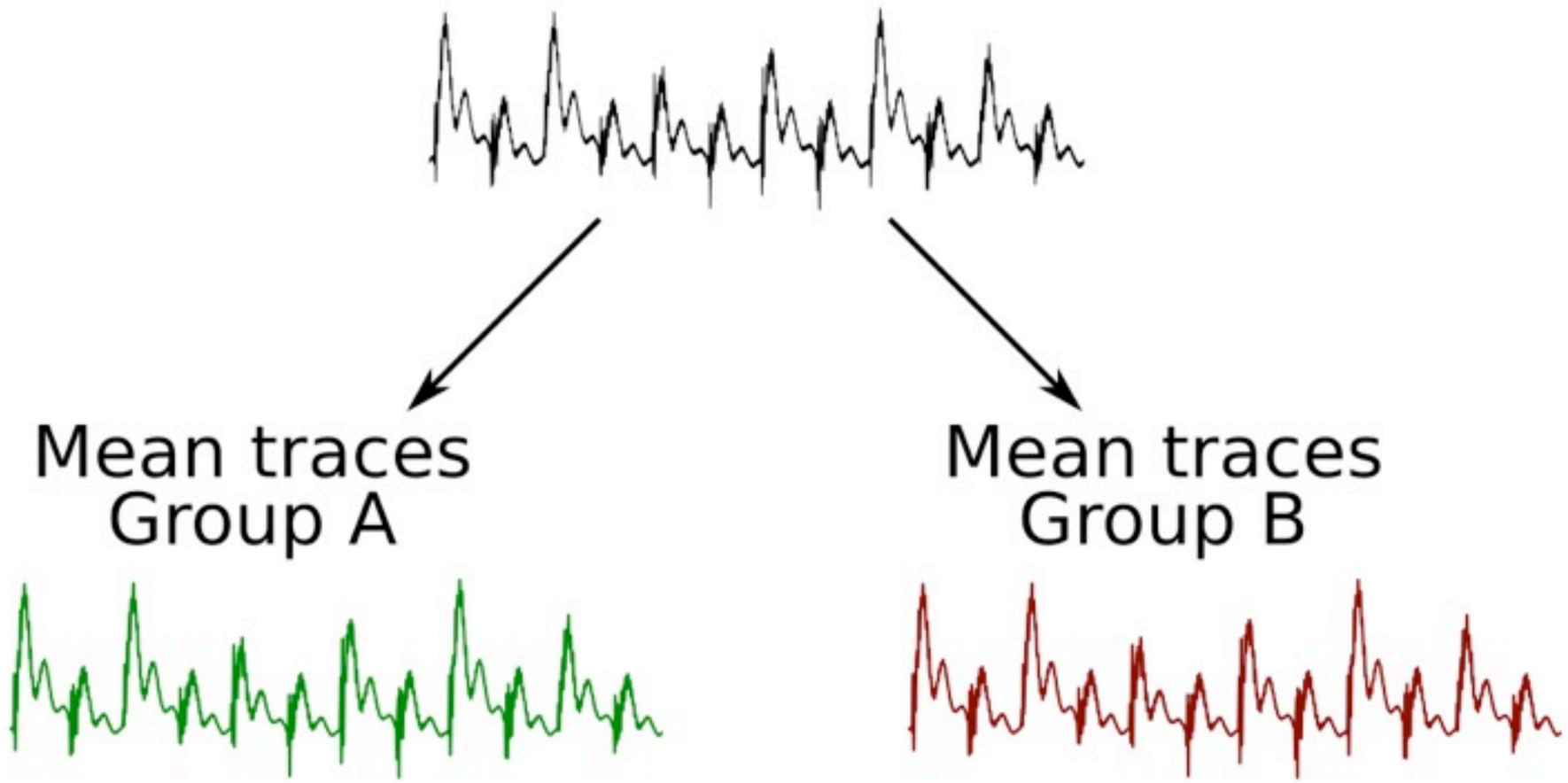
R○S○R’

How leakage detection is performed

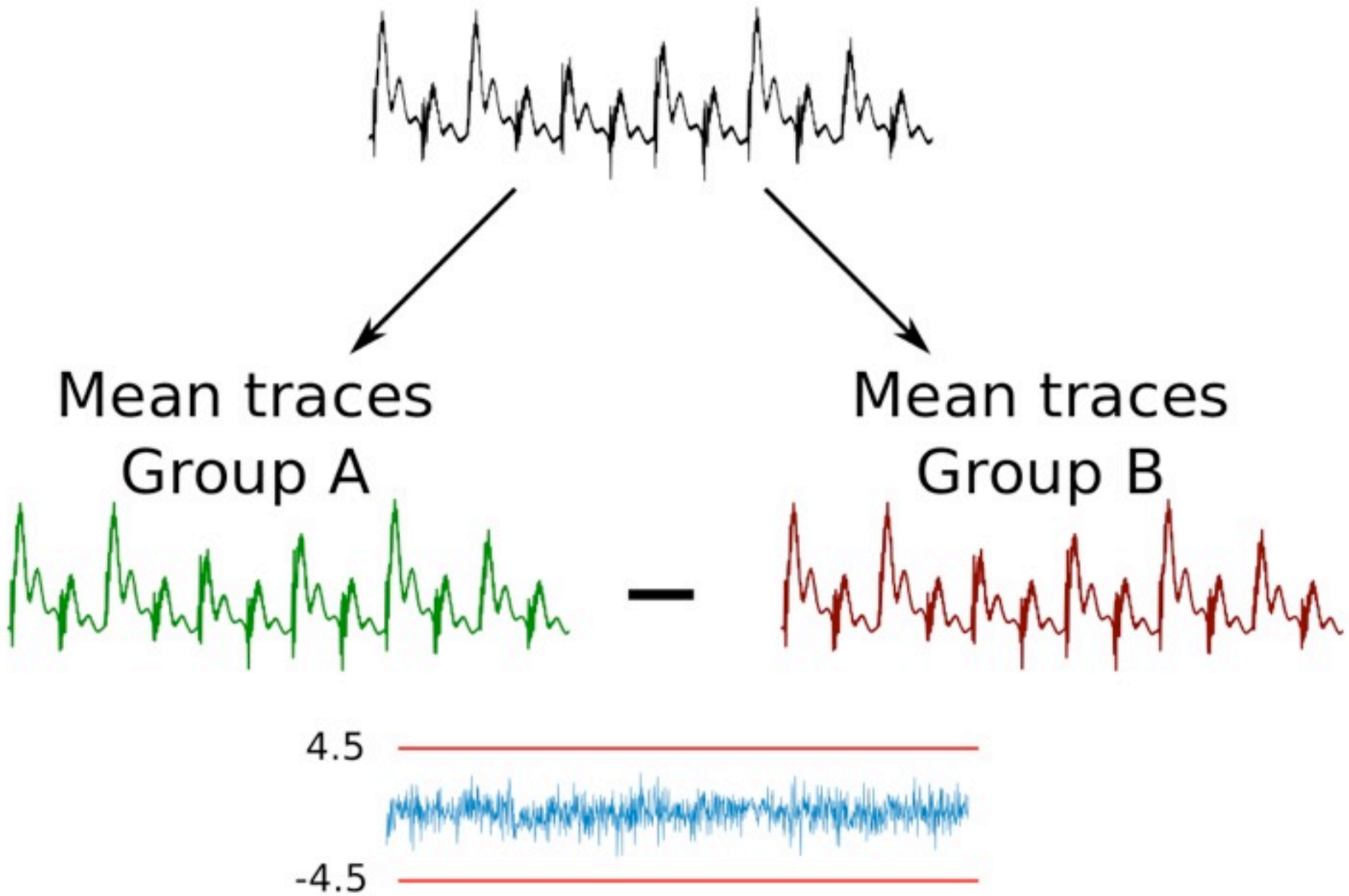
How leakage detection is performed



How leakage detection is performed

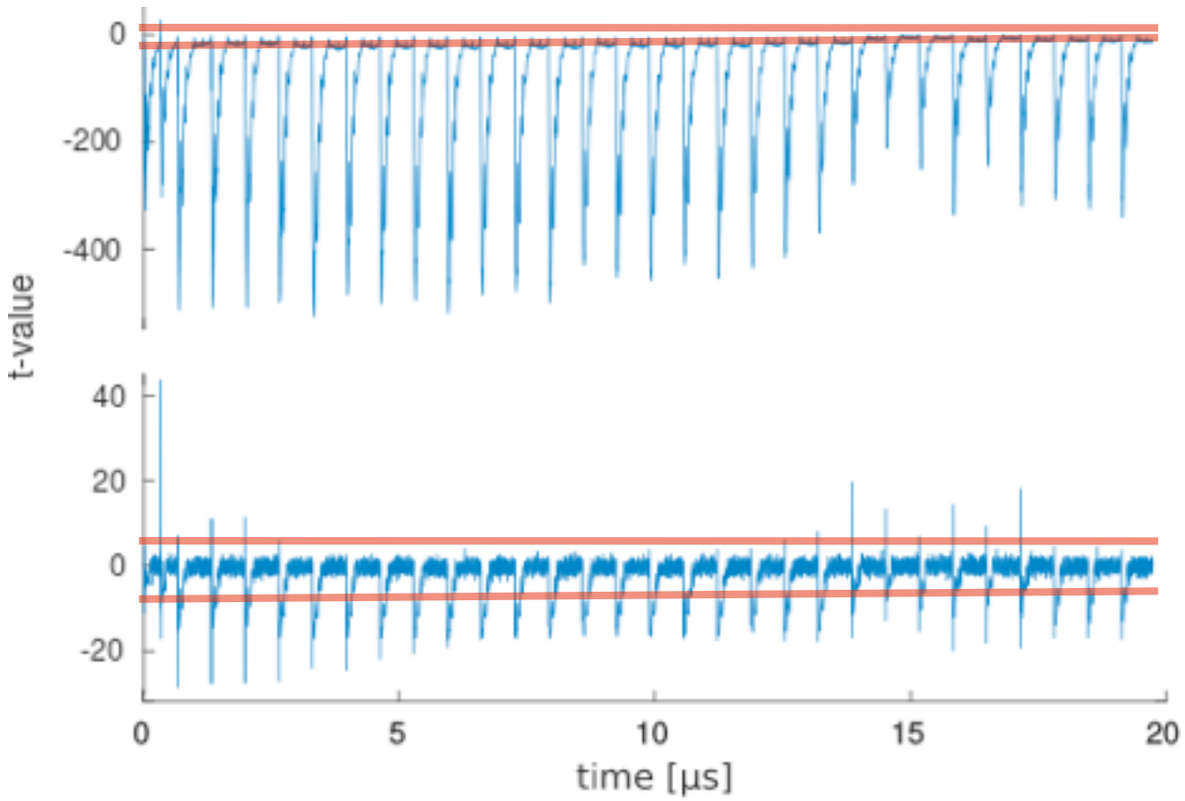


How leakage detection is performed



The 1st-order implementation passes leakage detection with 100M traces

1st-order

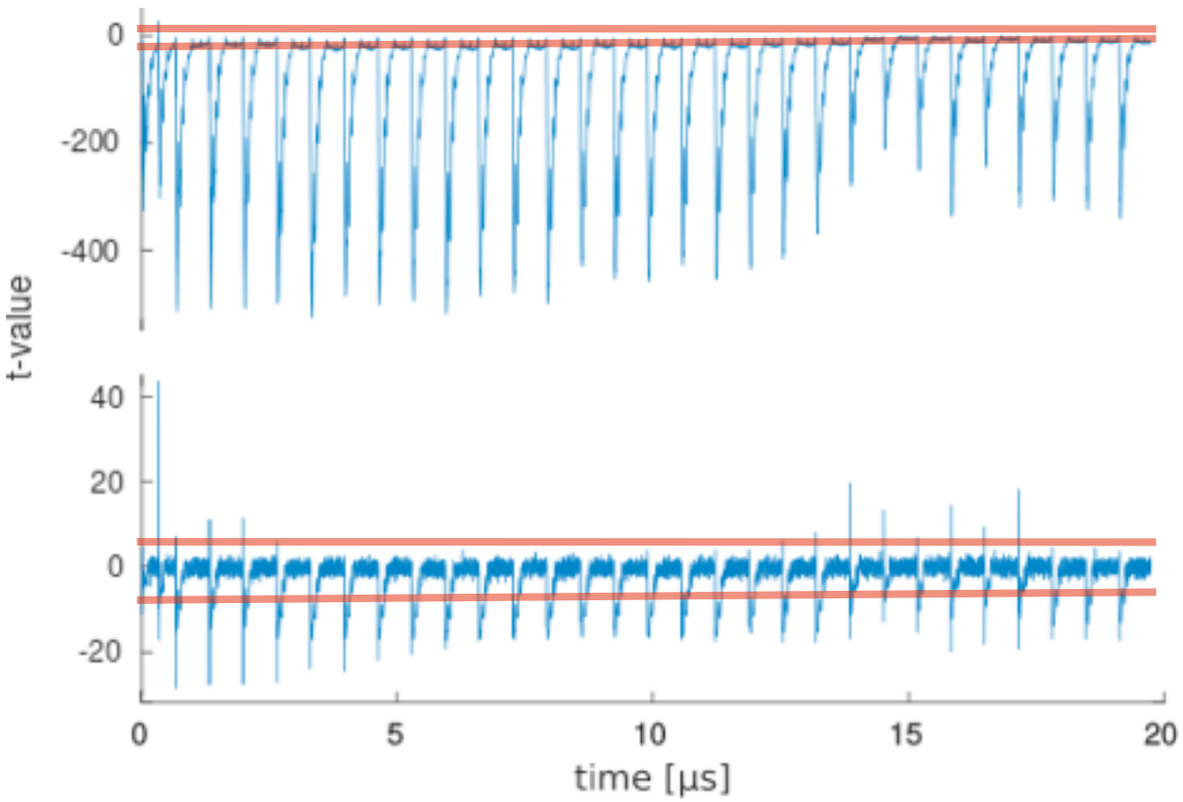


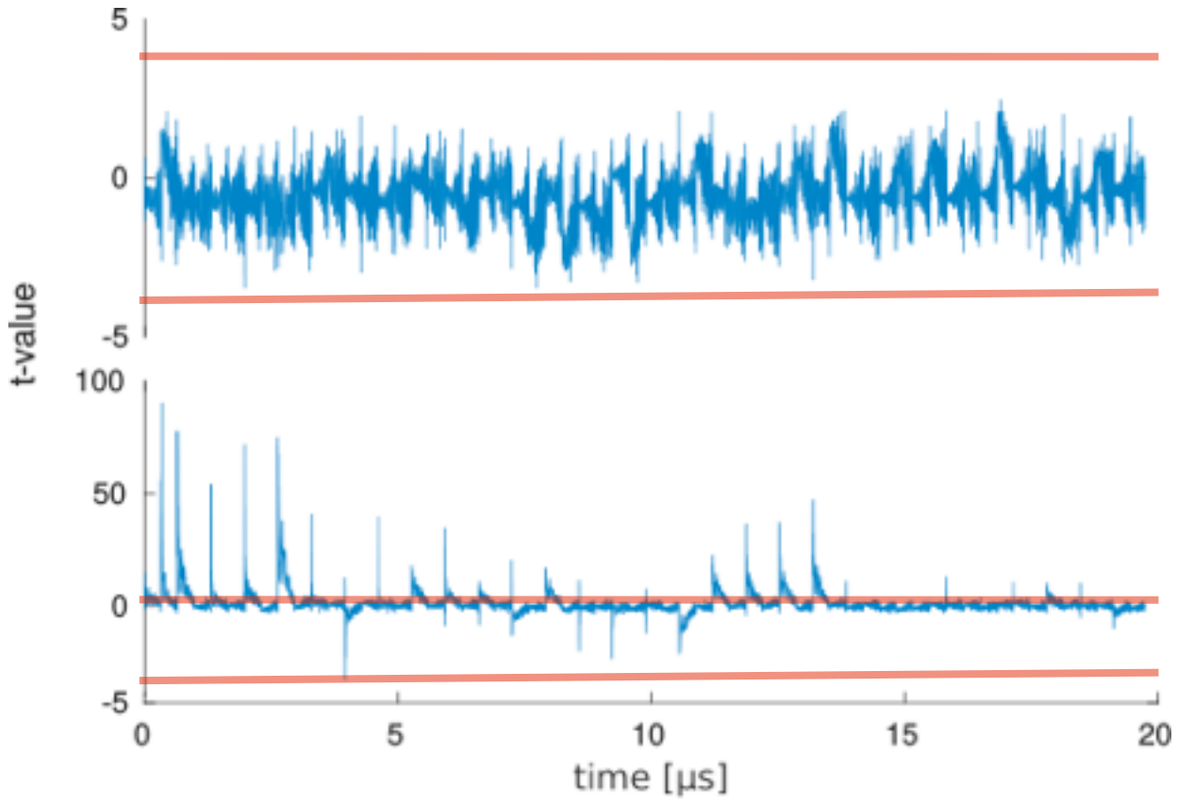
PRNG Off

2nd-order

The 1st-order implementation passes leakage detection with 100M traces

1st-order





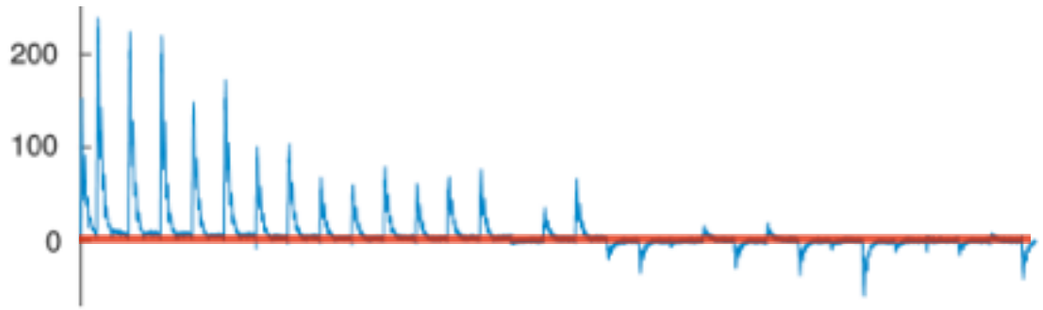
PRNG Off

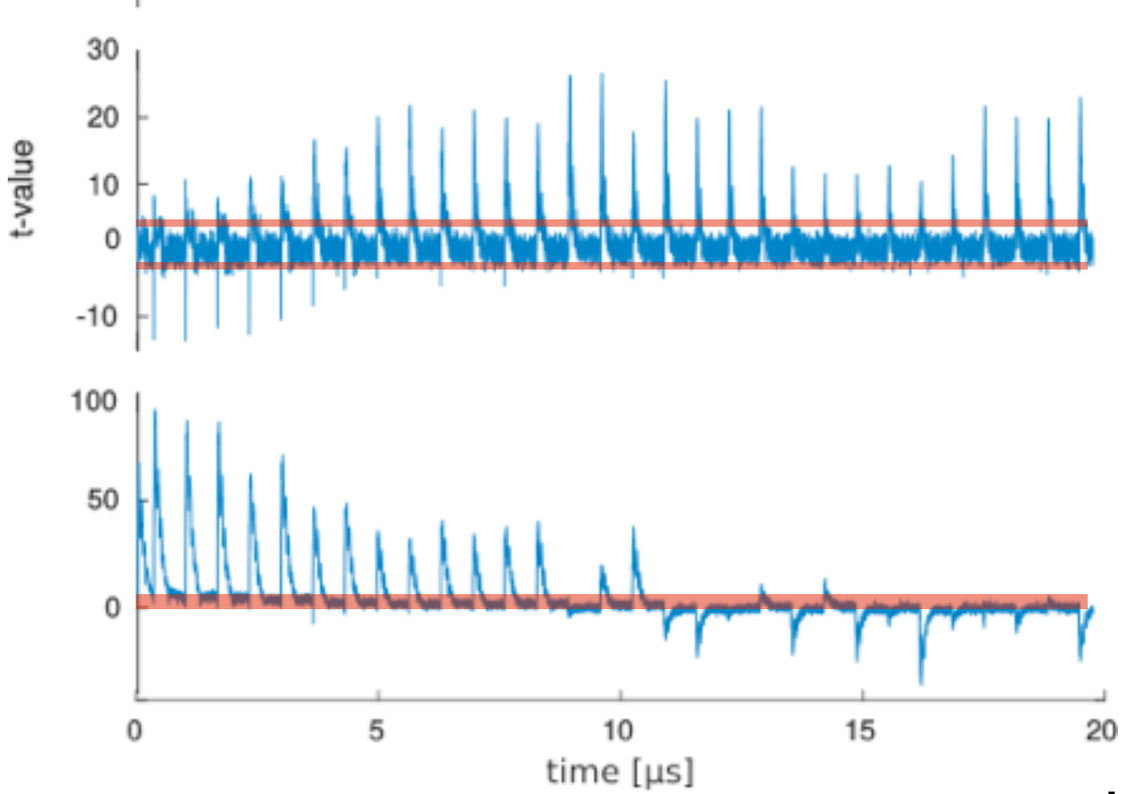
2nd-order

PRNG On

The 2nd-order implementation passes leakage detection with 100M traces

1st-order



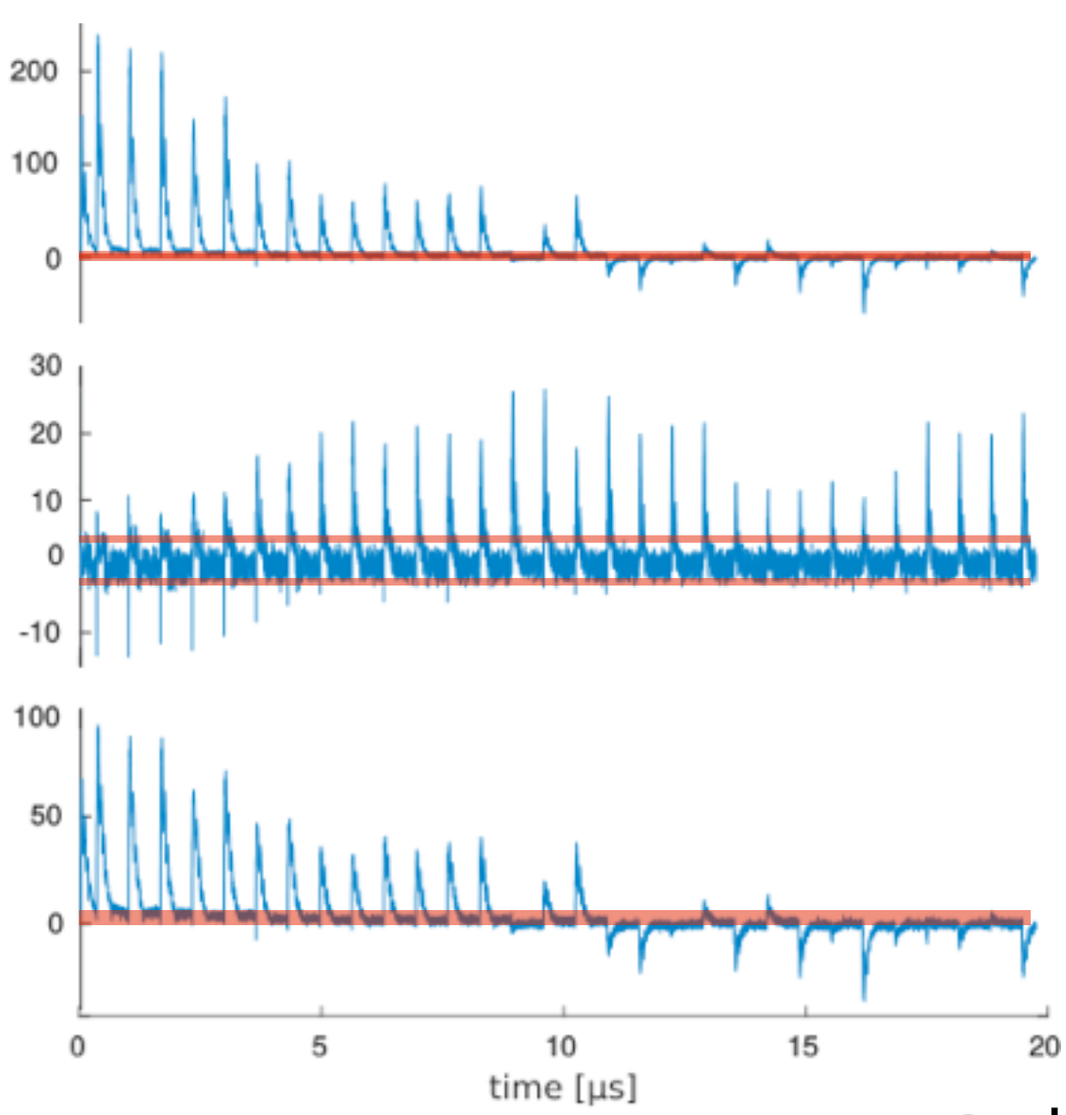


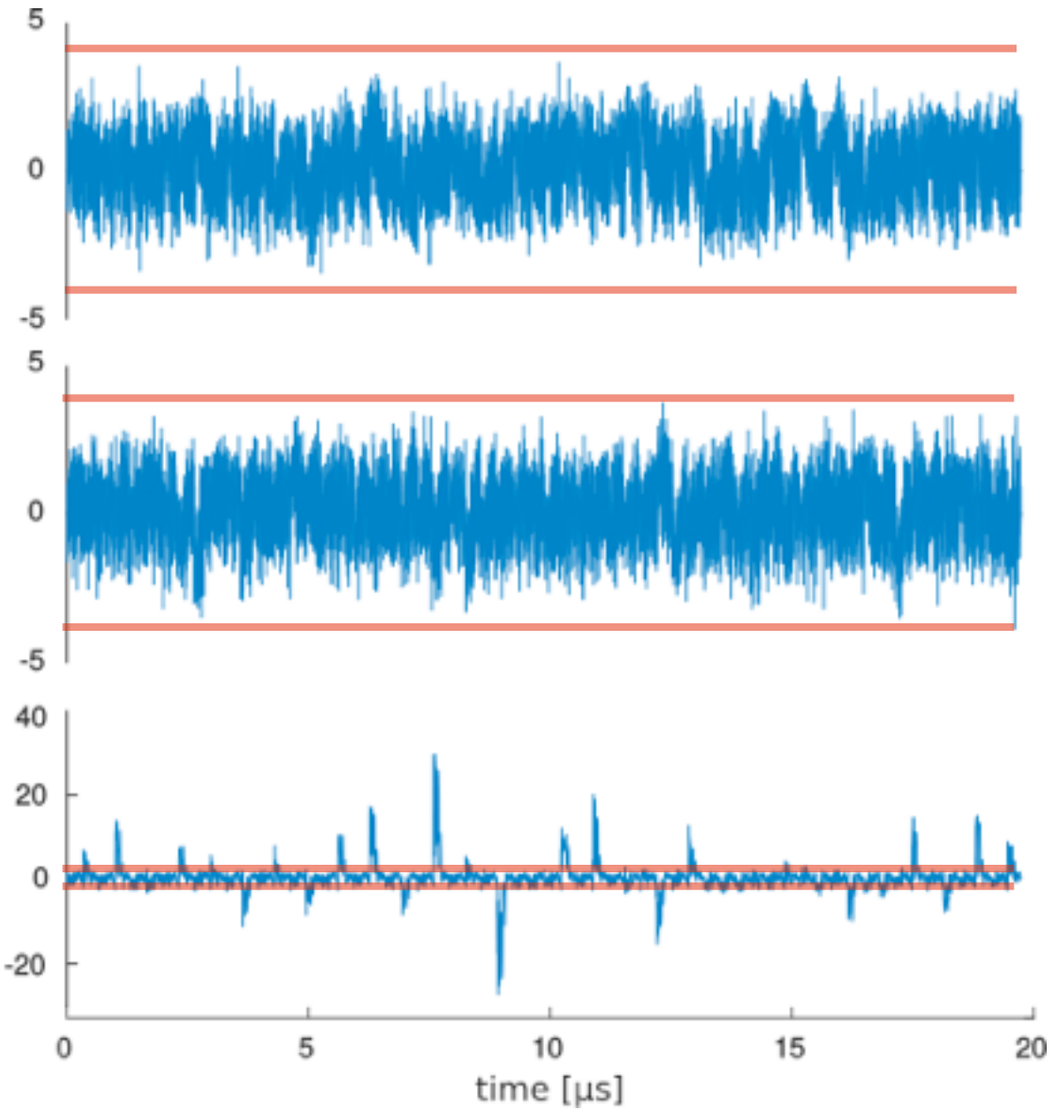
3rd-order

PRNG Off

The 2nd-order implementation passes leakage detection with 100M traces

1st-order



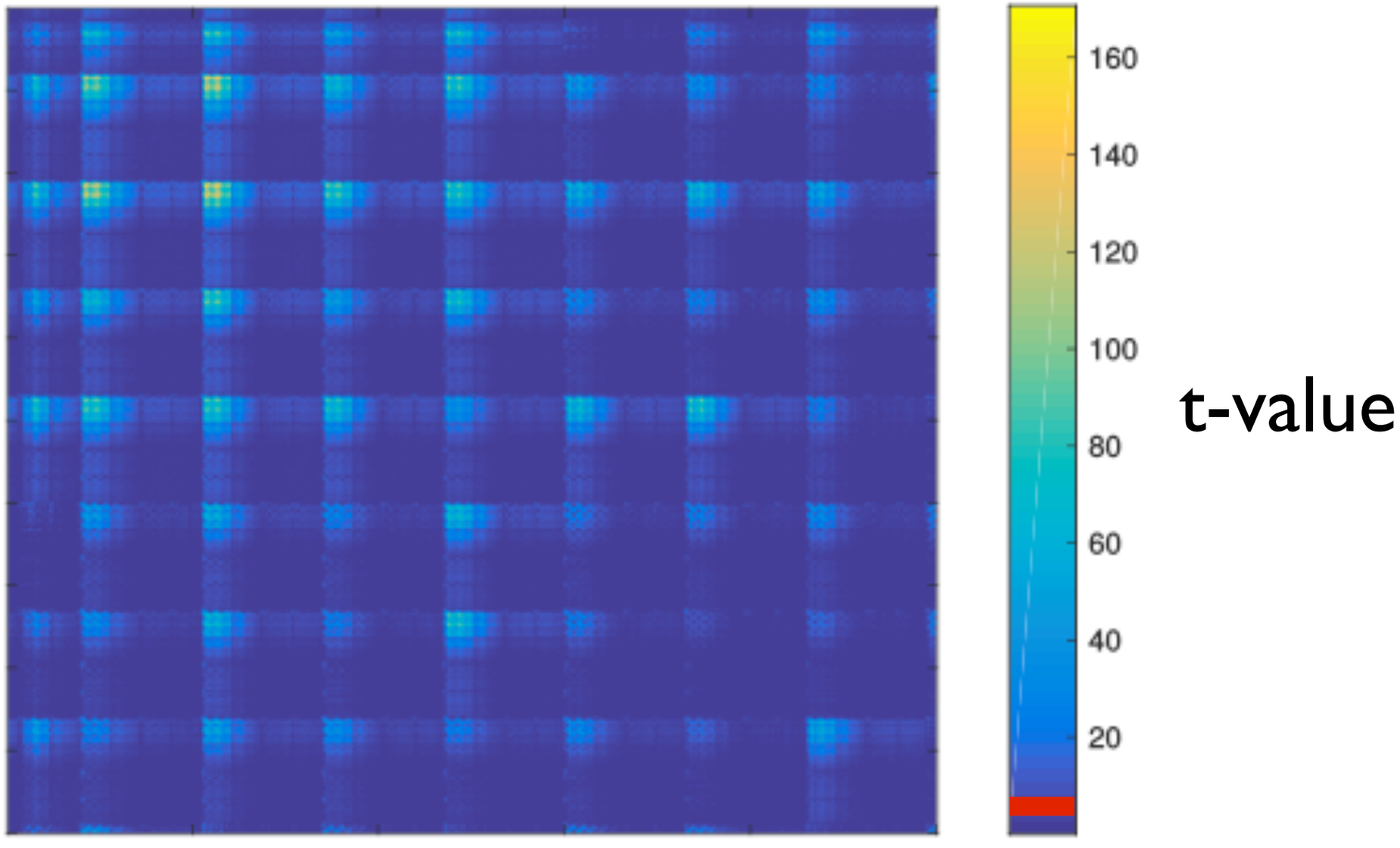


3rd-order

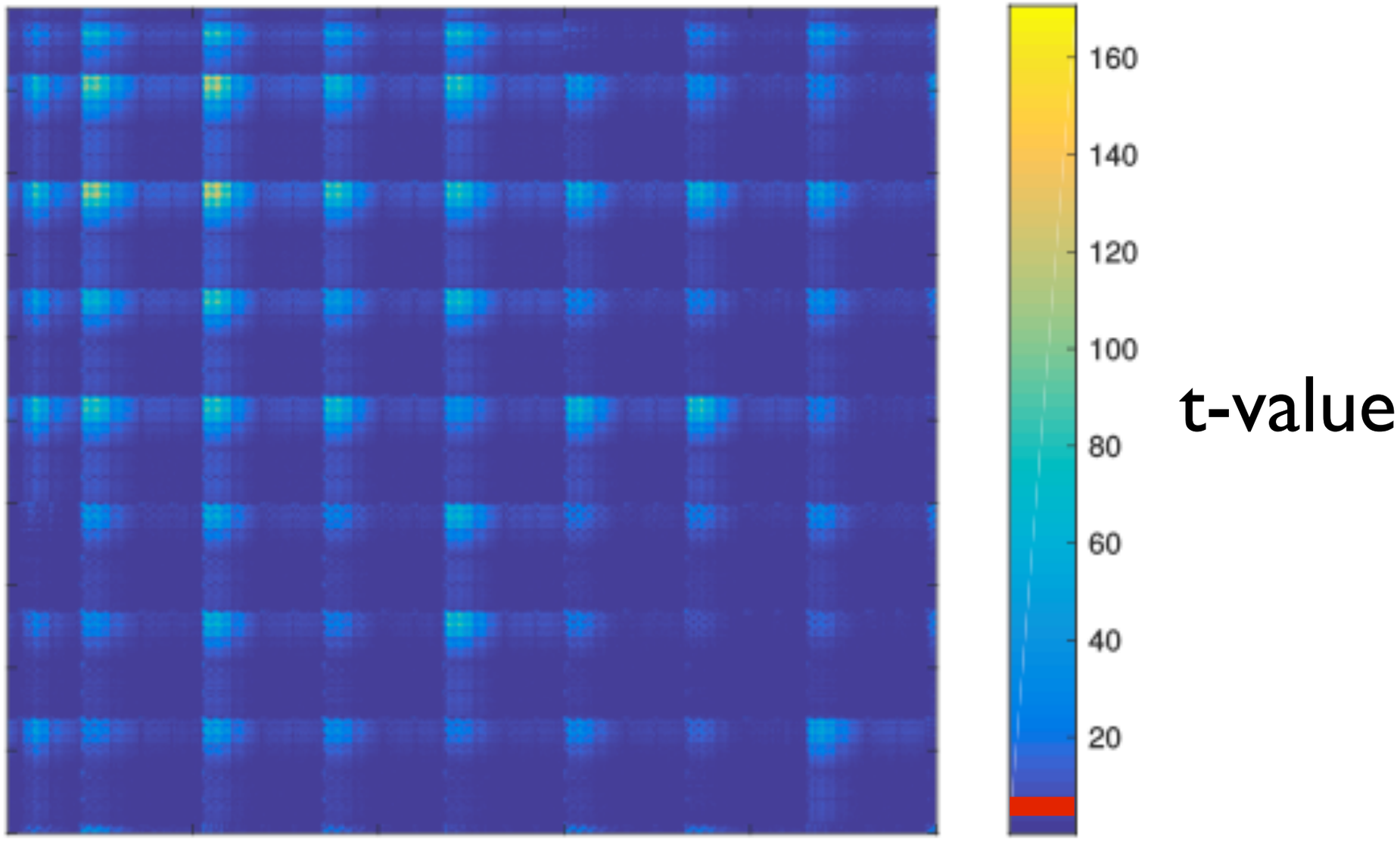
PRNG Off

PRNG On

Bivariate leakage detected in the 2nd-order implementation with PRNG Off

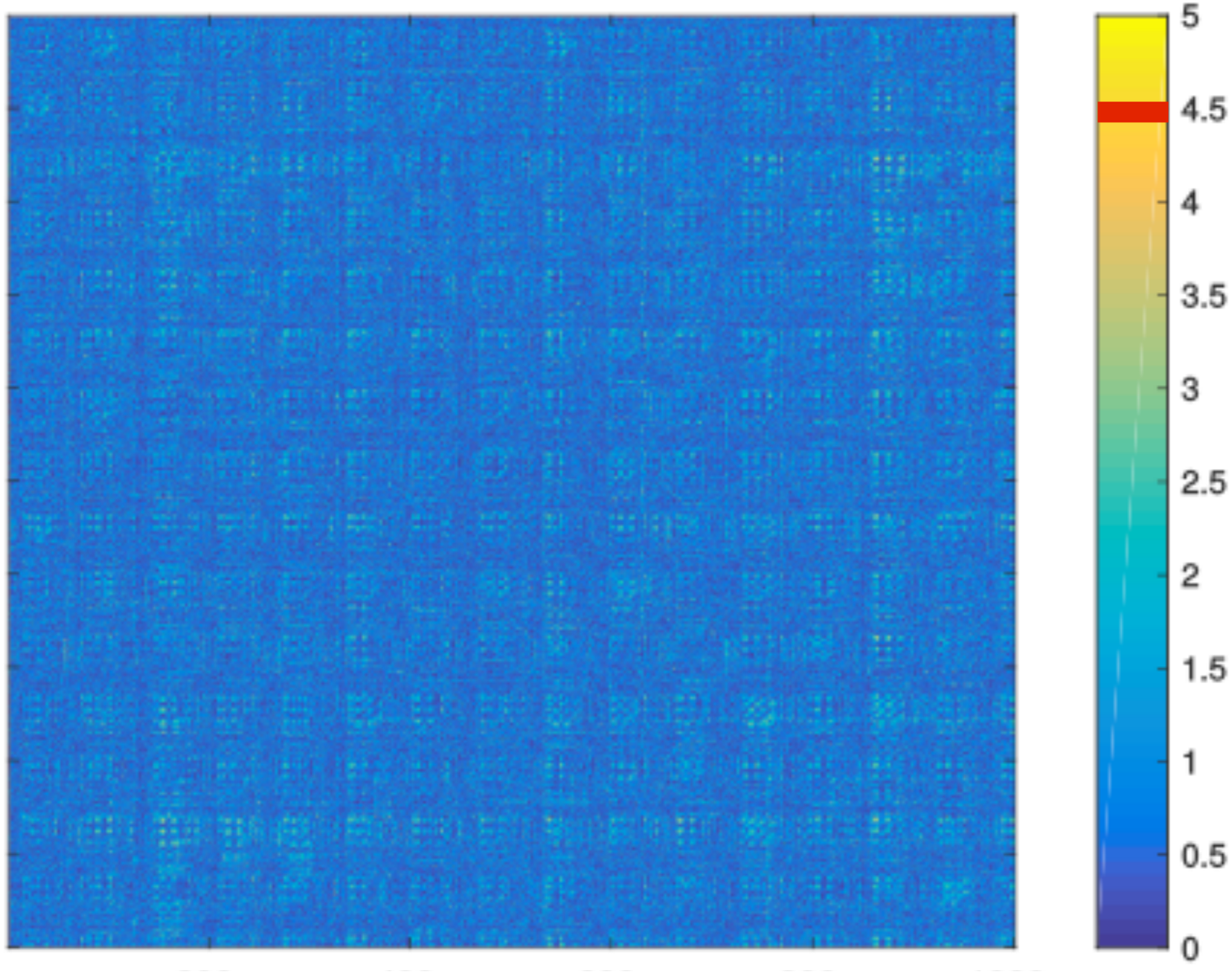


Bivariate leakage detected in the 2nd-order implementation with PRNG Off



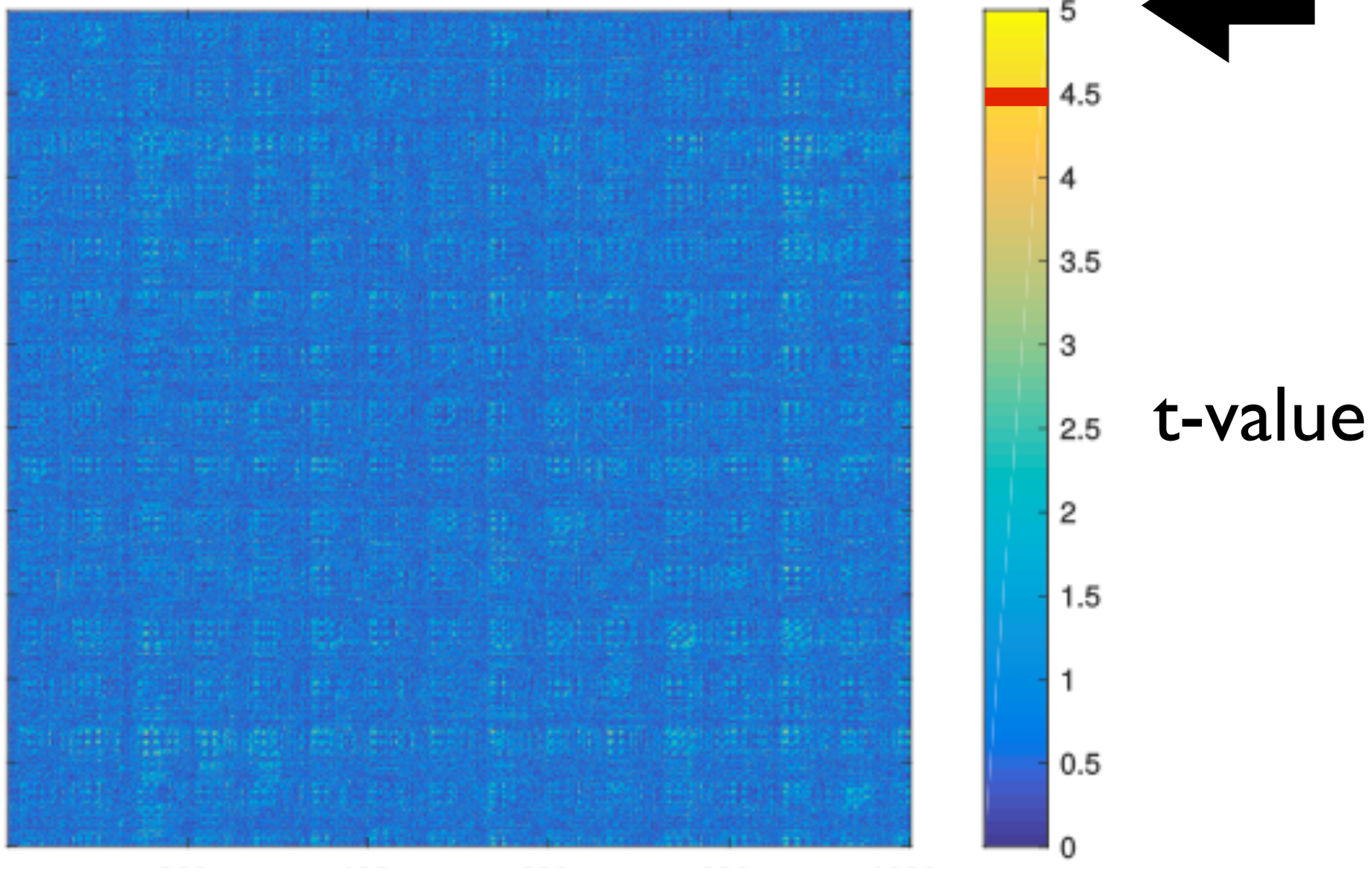
PRNG Off

No leakage detected in the 2nd-order implementation with 100M traces



PRNG On

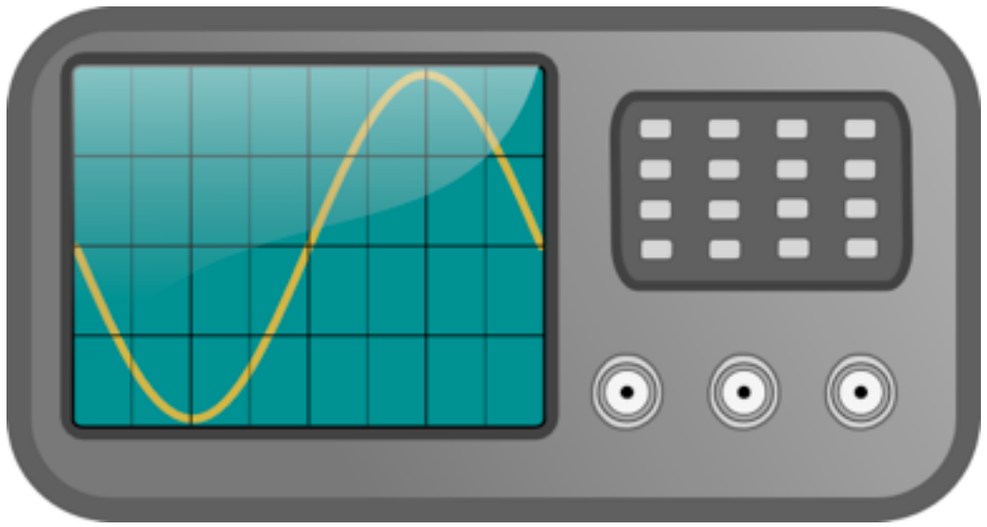
No leakage detected in the 2nd-order implementation with 100M traces



PRNG On

Masking AES with d+1 Shares in Hardware

Threshold Implementations



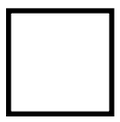
SCA Evaluation

Implementation Cost

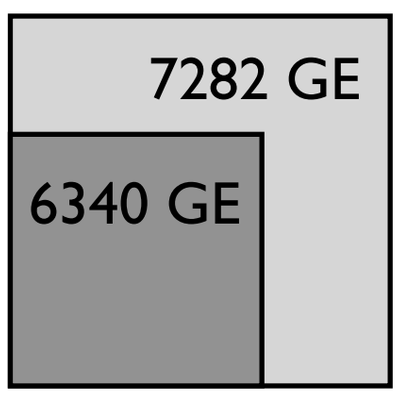
A smaller AES is achieved

unmasked

2421 GE



1st-order



0.9x

This work

Moradi, 2011

Bilgin, 2015

A smaller AES is achieved

unmasked

2421 GE

1st-order

7282 GE

6340 GE

0.9x

2nd-order

14872 GE

10276 GE

0.7x

This work

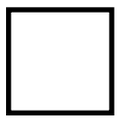
Moradi, 2011

Bilgin, 2015

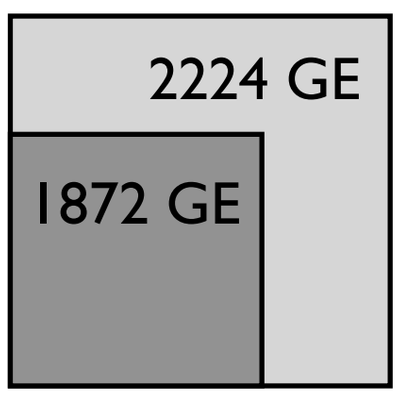
Mostly due to a smaller AES S-box

unmasked

233 GE



1st-order



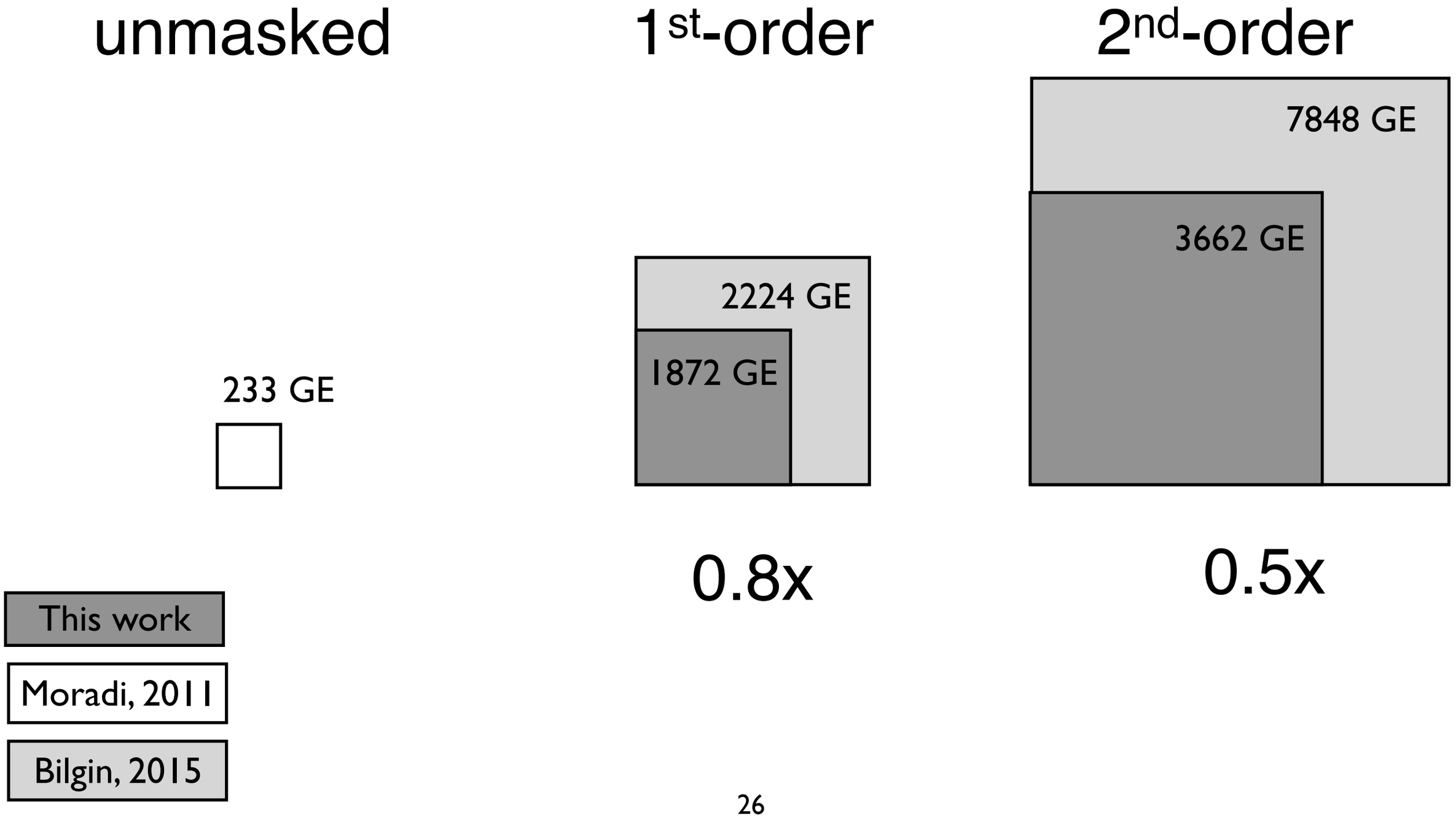
0.8x

This work

Moradi, 2011

Bilgin, 2015

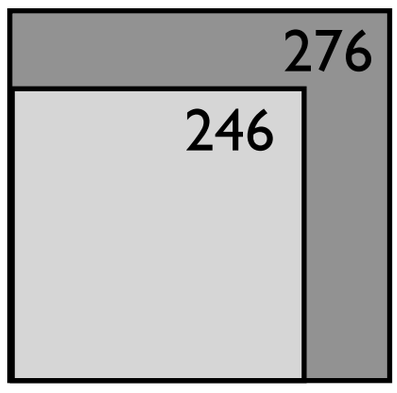
Mostly due to a smaller AES S-box



A similar number of clock cycles suffice

unmasked

1st-order



1.1x

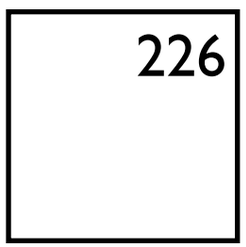
This work

Moradi, 2011

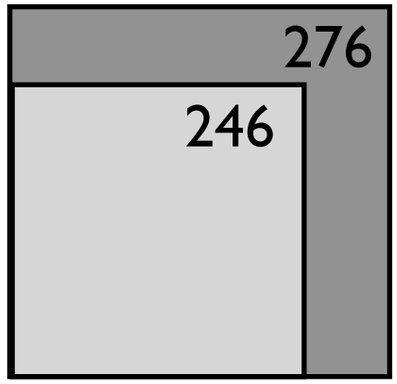
Bilgin, 2015

A similar number of clock cycles suffice

unmasked

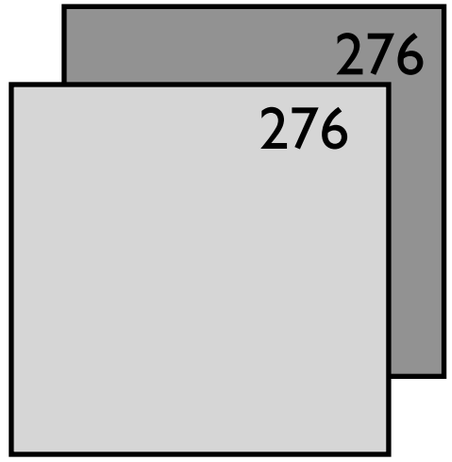


1st-order



1.1x

2nd-order



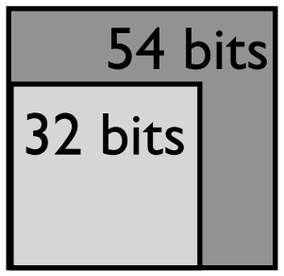
constant*

This work

Moradi, 2011

Bilgin, 2015

More randomness is consumed

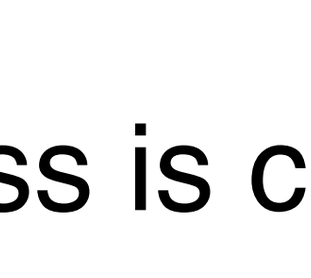
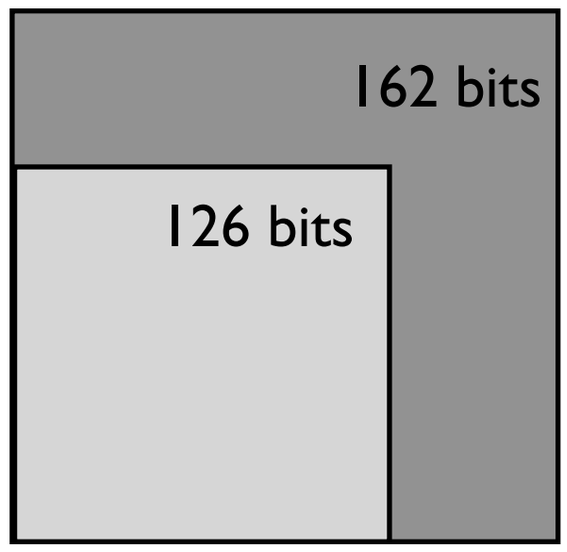
unmasked	1st-order
-	
	1.7x

This work

Moradi, 2011

Bilgin, 2015

More randomness is consumed

unmasked	1st-order	2nd-order
-		
	1.7x	1.3x

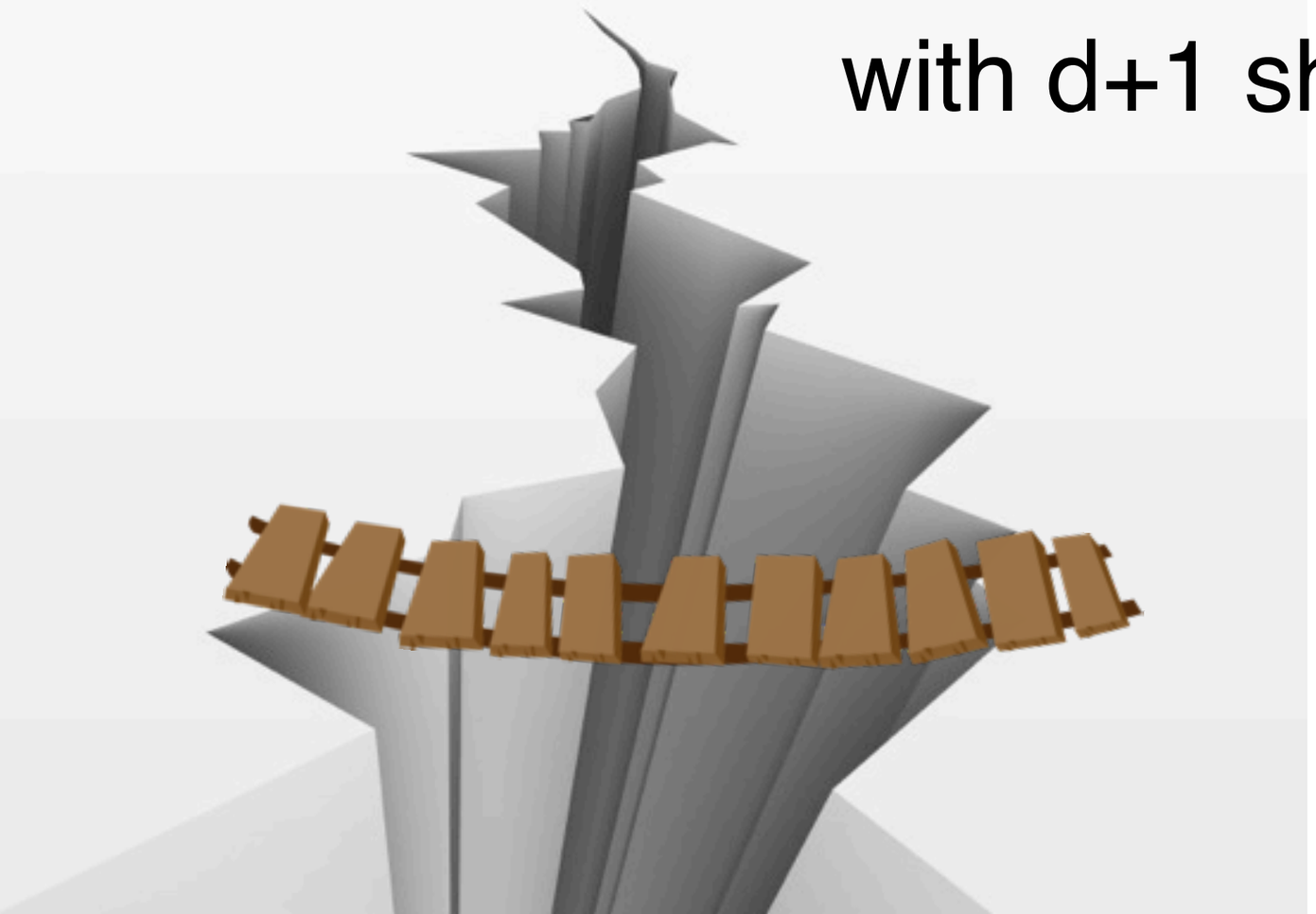
This work

Moradi, 2011

Bilgin, 2015

We realized and verified the smallest masked AES in hardware

Theory



with d+1 shares

Practice

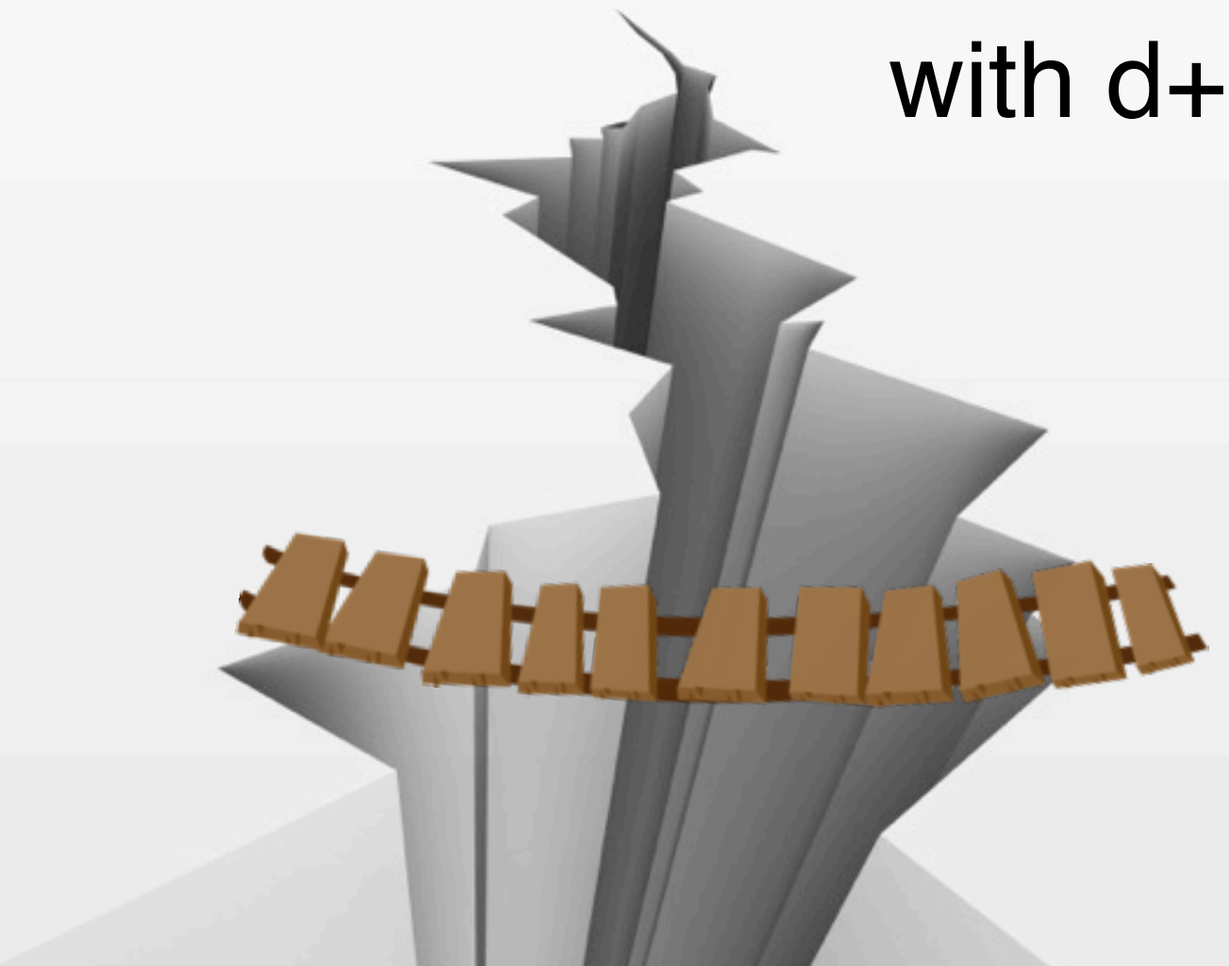
- 1st - order
- 2nd- order

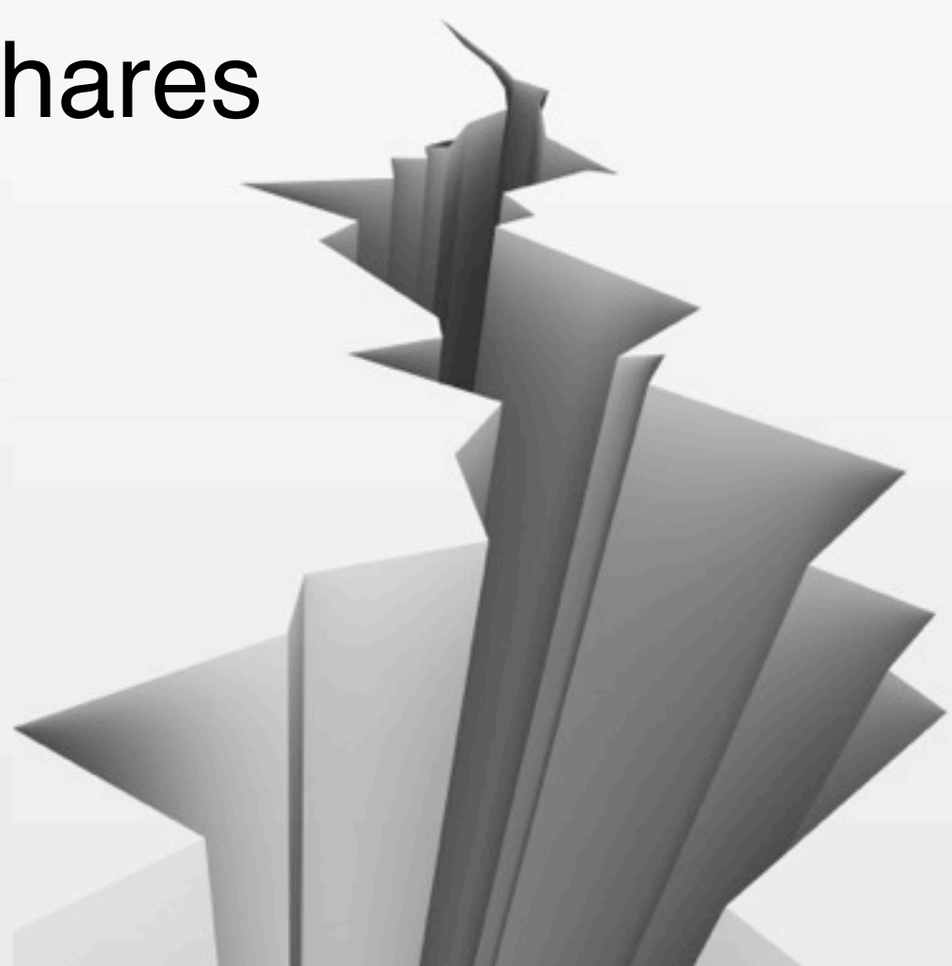
We realized and verified the smallest masked AES in hardware

Theory

Practice
- 1st - order
- 2nd- order

with d+1 shares





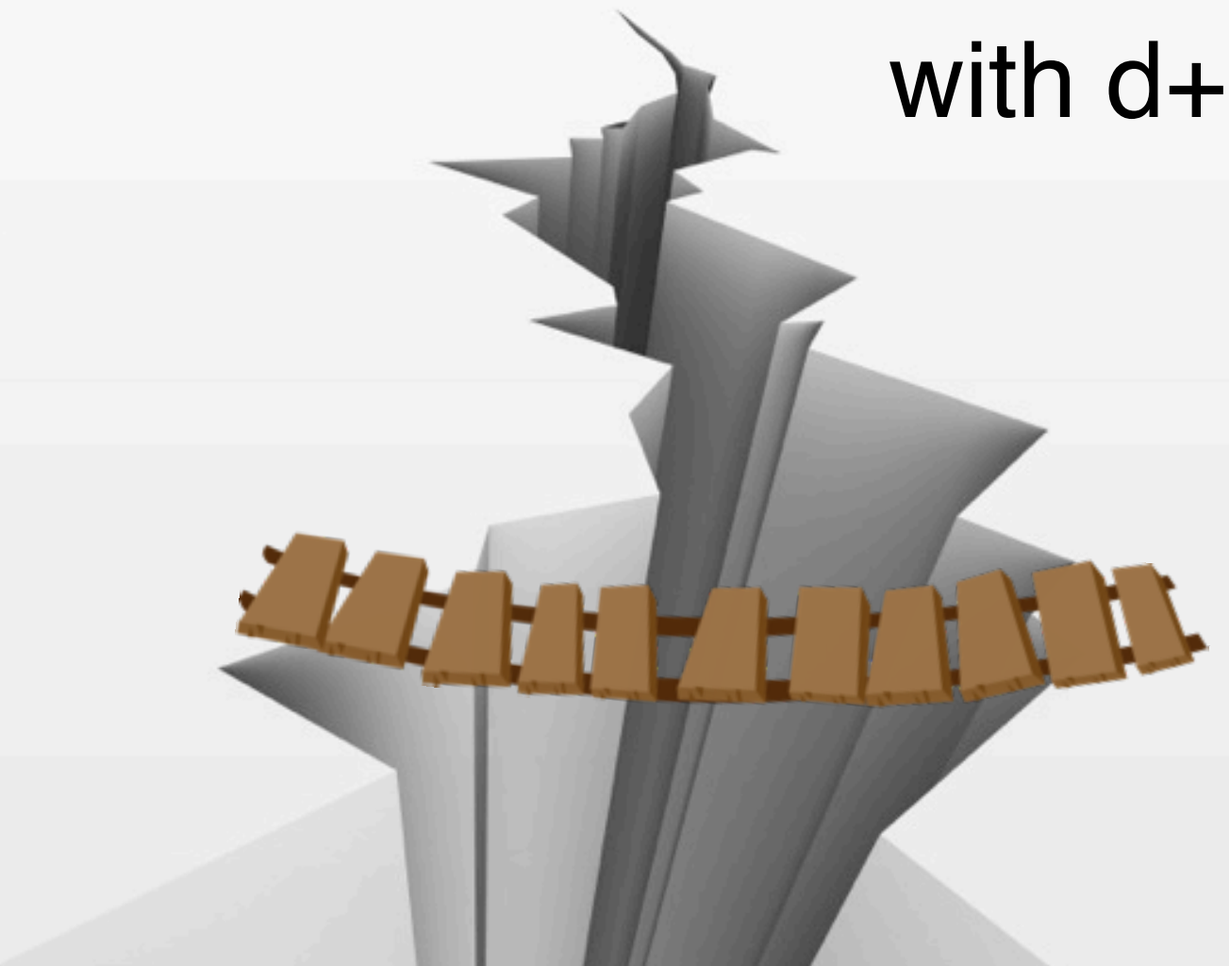
We realized and verified the smallest masked AES in hardware

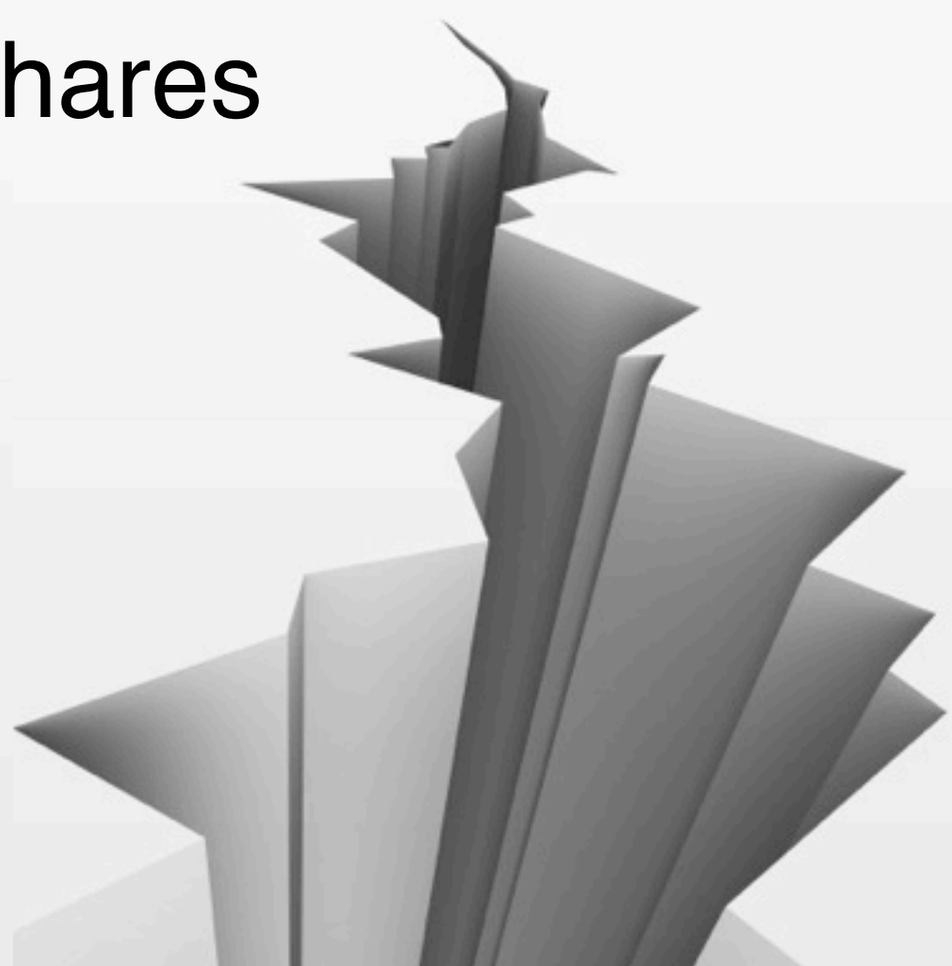
Theory

Practice
- 1st - order
- 2nd- order

Higher-orders

with d+1 shares





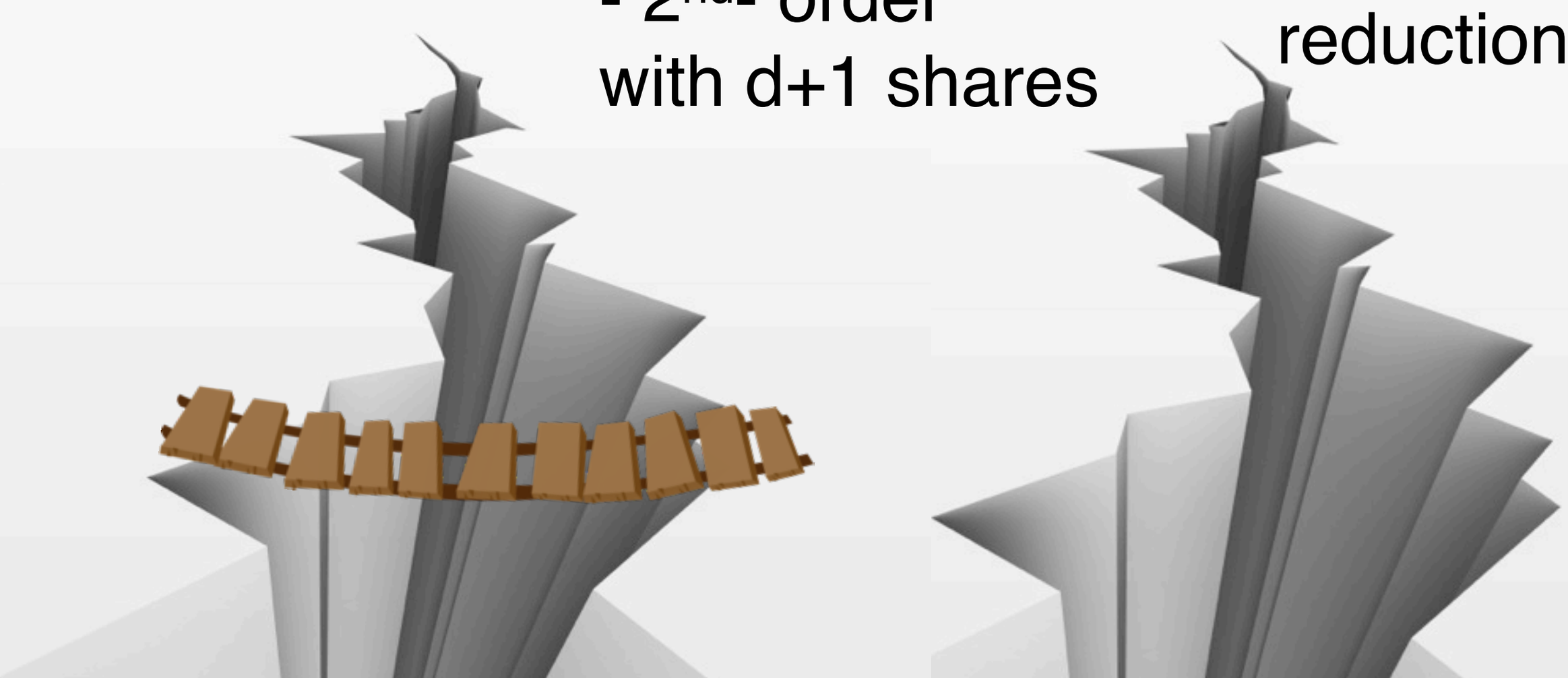
We realized and verified the smallest masked AES in hardware

Theory

Practice
- 1st - order
- 2nd- order
with d+1 shares

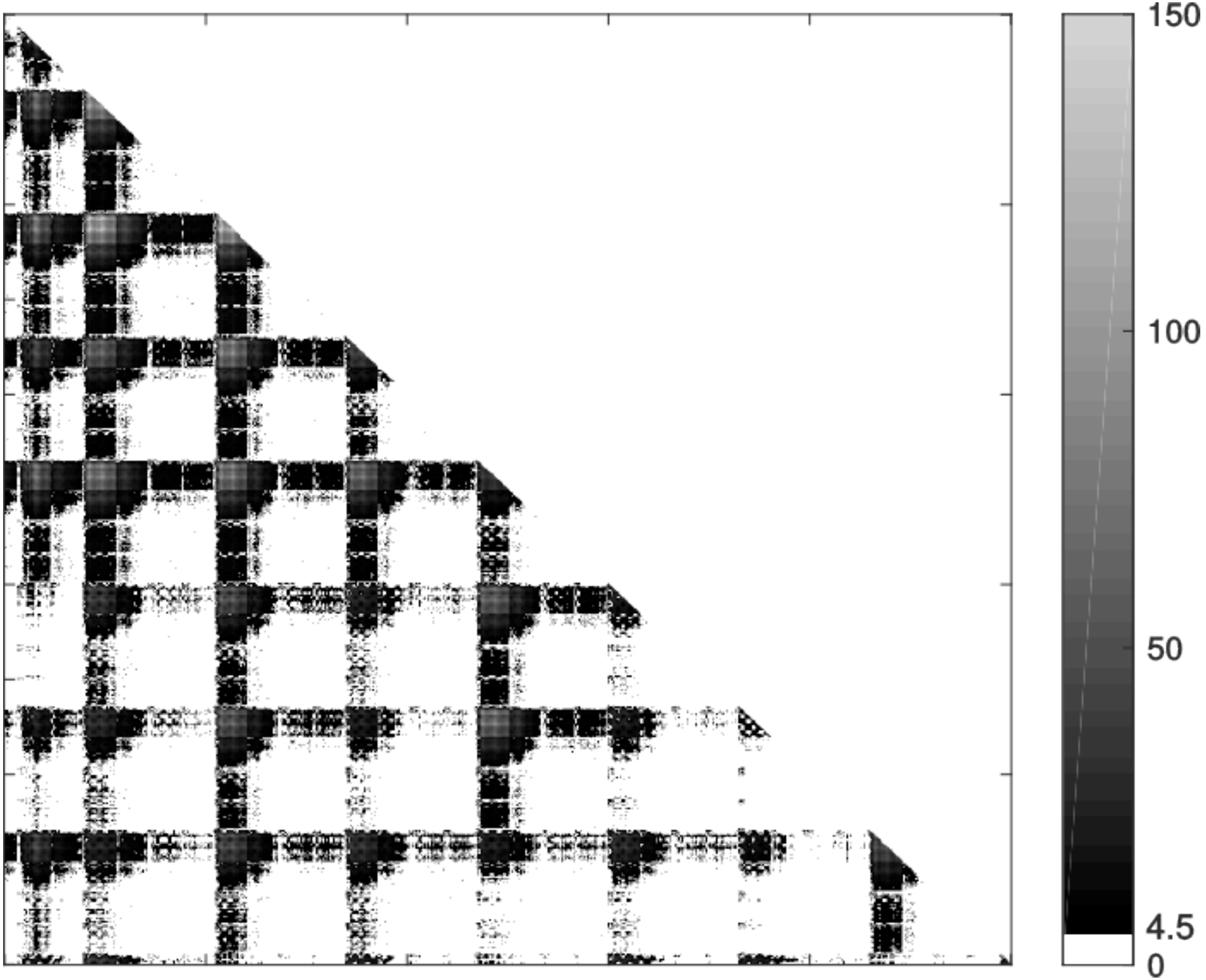
Higher-orders

Randomness reduction



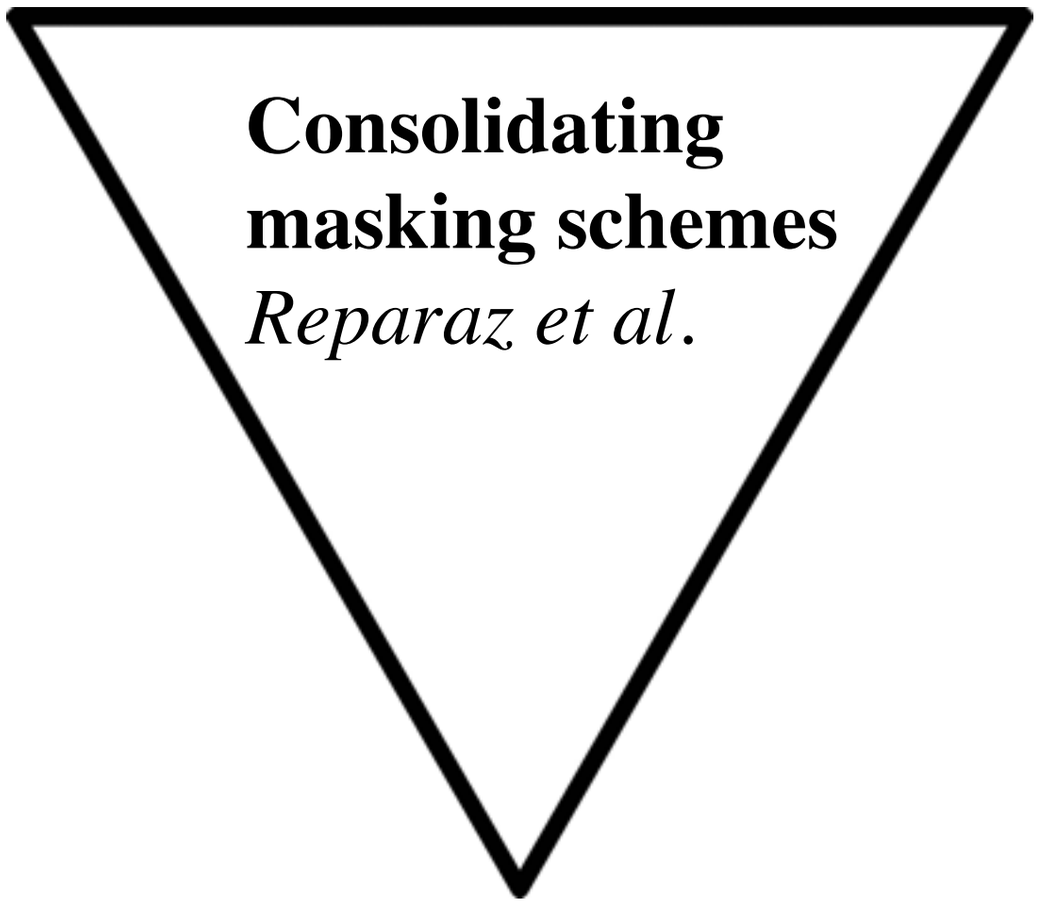
Thank you

Questions ?


150
100
50
4.5
0

A Tale of Two Shares: Why Two-Share Threshold Implementation Seems Worthwhile-and Why it is Not
Chen et al.

Masking AES with d+1 Shares in Hardware
De Cnudde et al.



Domain-Oriented Masking: Compact Masked Hardware Implementations with Arbitrary Protection Order
Gross et al.