# Does Coupling Affect the Security of Masked Implementations?

**Thomas De Cnudde**
Begül Bilgin
Benedikt Gierlichs
Ventzislav Nikov
Svetla Nikova
Vincent Rijmen

13/04 – COSADE 2017 – Paris

Does coupling
affect the security of
masked implementations ?

# It Might…

# It Might...

The influence from coupling is observable

# It Might...

The influence from coupling is observable

but pinpointing exact source is hard

# It Might...

The influence from coupling is observable

but pinpointing exact source is hard

and many open questions remain.

# Does coupling affect the security of masked implementations?

**Masking**

What can go wrong?

Sources of coupling

Detecting coupling in practice

Implications

# Masking is a countermeasure against side-channel analysis

# Masking is a countermeasure against side-channel analysis

$Z$

Sensitive Value

# Masking is a countermeasure against side-channel analysis

$$\underbrace{Z}_{\text{Sensitive Value}} \oplus \overbrace{M_1}^{\text{Random Number}}$$

# Masking is a countermeasure against side-channel analysis

Random Number

$$Z_{masked} = Z \oplus M_1$$

Sensitive Value

# Masking is a countermeasure against side-channel analysis

Random Number

$$Z_{masked} = Z \oplus M_1$$

Sensitive Value

Masking Scheme

- How to share a sensitive value

# Masking is a countermeasure against side-channel analysis

Random Number

$$Z_{masked} = Z \oplus M_1$$

Sensitive Value

Masking Scheme

- How to share a sensitive value

- How to compute on the shares

# Masking is a countermeasure against side-channel analysis

Random Number

$$Z_{masked} = Z \oplus M_1$$

Sensitive Value

Masking Scheme

- How to share a sensitive value

- How to compute on the shares

- Assumptions on the device’s leakage behavior

# Wrong assumptions can violate the side-channel resistance

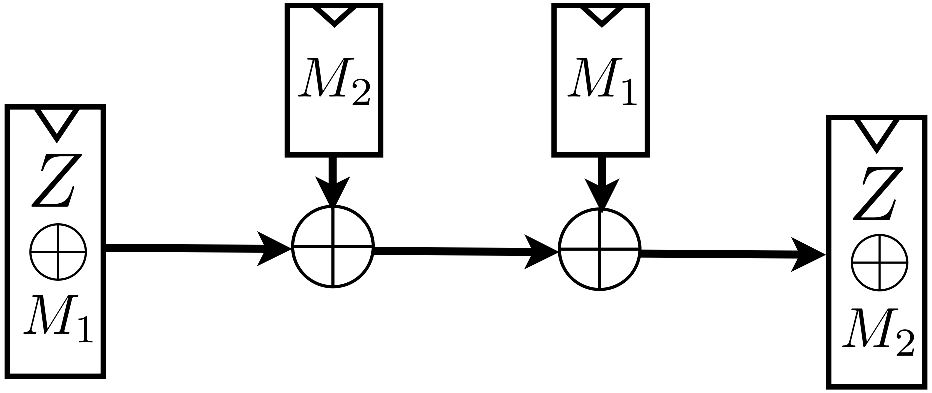
# Wrong assumptions can violate the side-channel resistance

$((Z \oplus M_1) \oplus M_2) \oplus M_1 = Z \oplus M_2$ Mask refreshing

# Wrong assumptions can violate the side-channel resistance

$((Z \oplus M_1) \oplus M_2) \oplus M_1 = Z \oplus M_2$

Mask refreshing



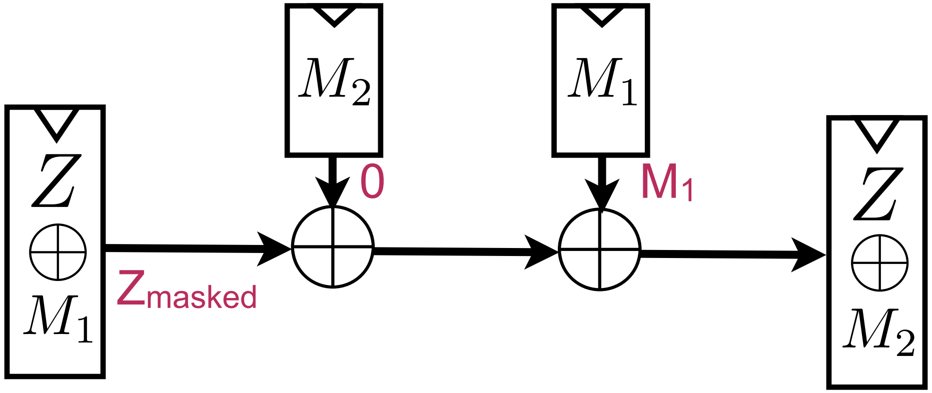
Violated assumption

Delay on $M_2$ unmasks Z

# Wrong assumptions can violate the side-channel resistance

$$((Z \oplus M_1) \oplus M_2) \oplus M_1 = Z \oplus M_2$$

Mask refreshing



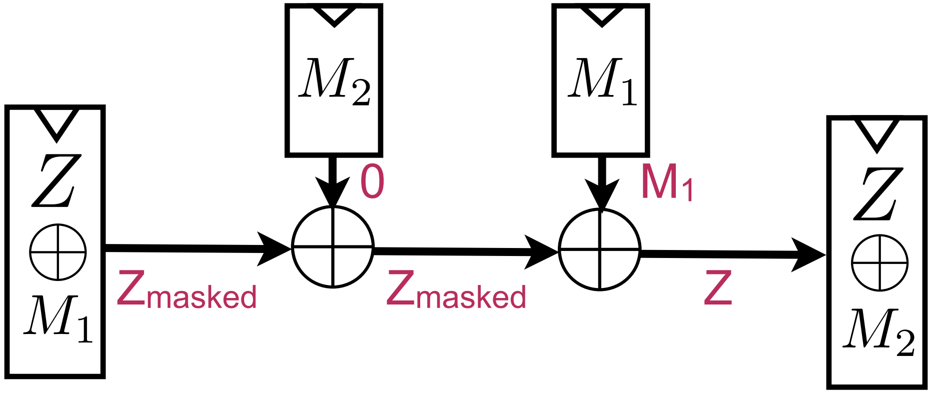
Violated assumption

Delay on $M_2$ unmasks Z

# Wrong assumptions can violate the side-channel resistance

$((Z \oplus M_1) \oplus M_2) \oplus M_1 = Z \oplus M_2$

Mask refreshing

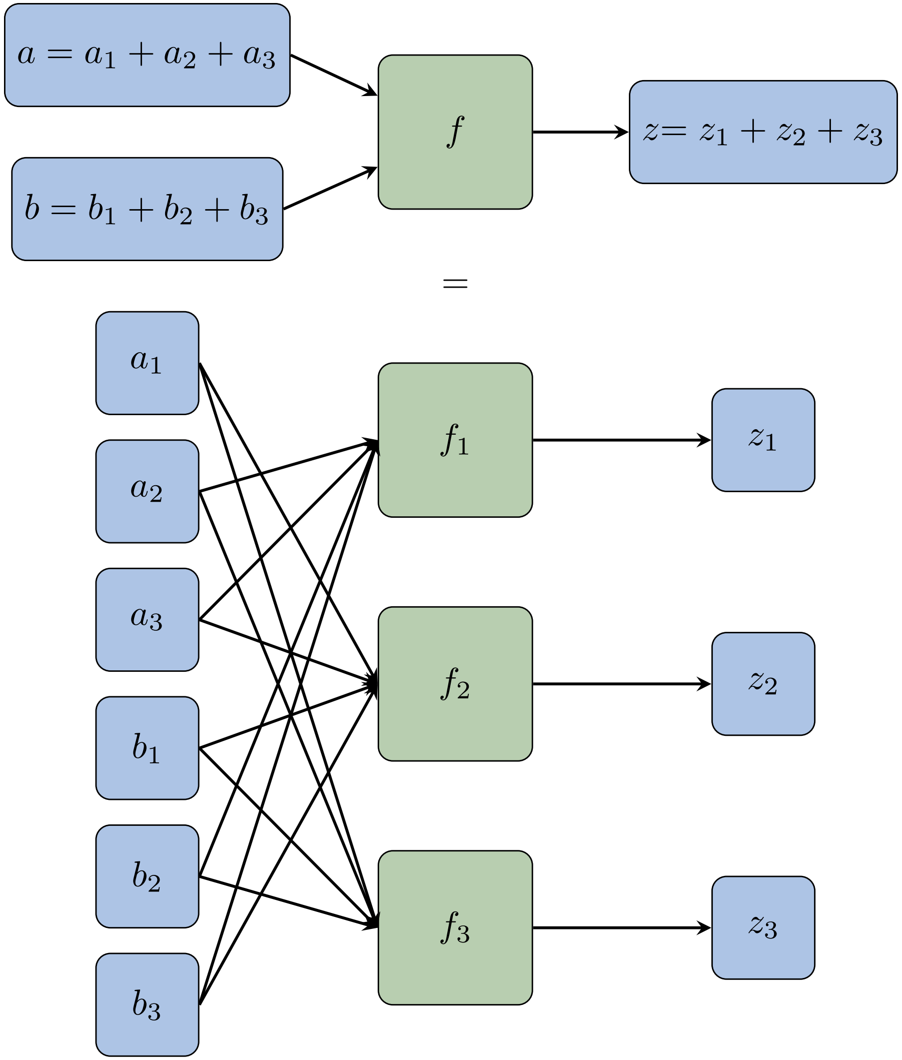


Violated assumption

Delay on $M_2$ unmasks Z

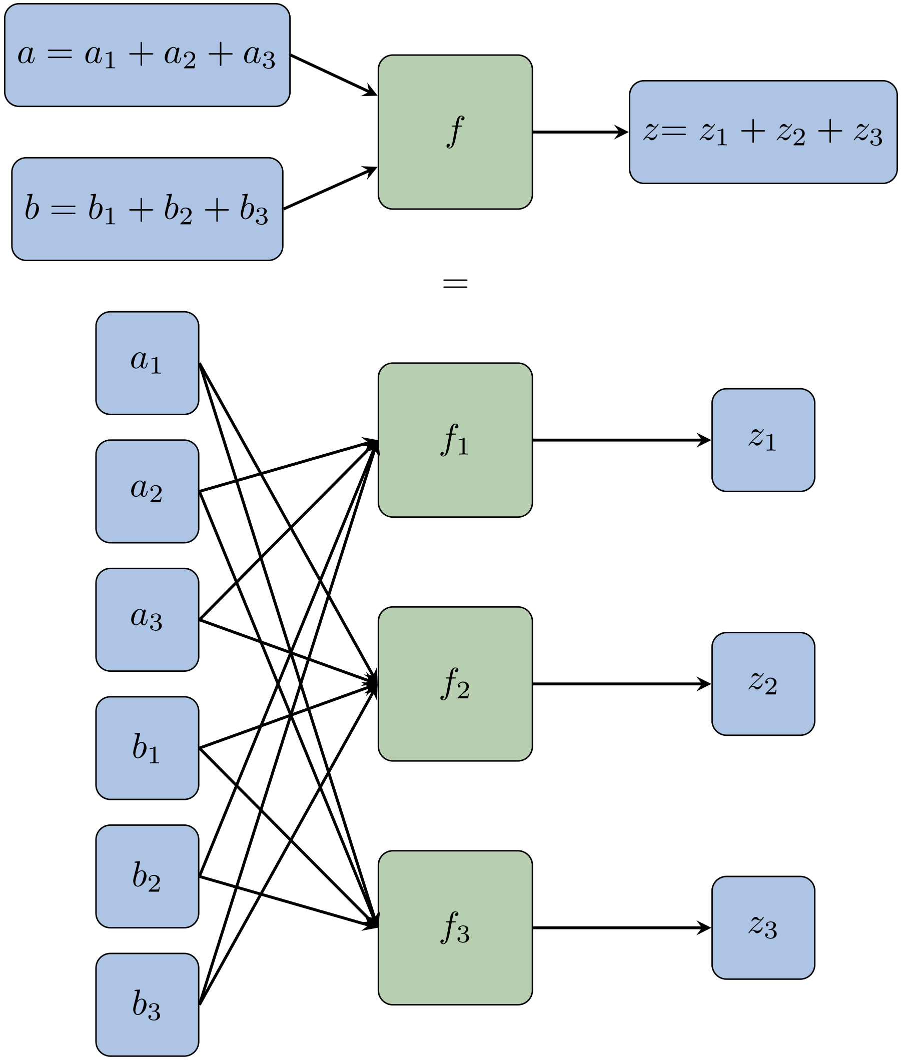
Early propagation and glitches deteriorate the effect of masking

# Threshold implementations are secure in the presence of glitches



Minimal assumptions on the underlying hardware

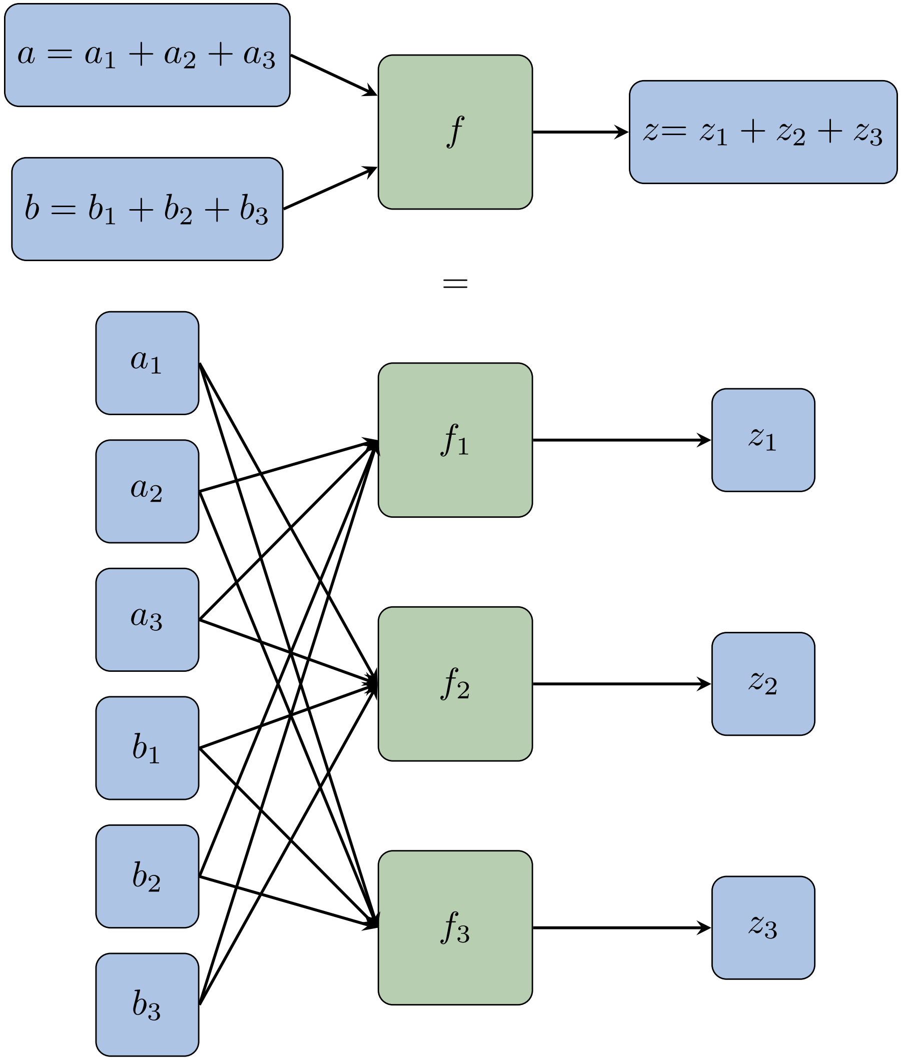
# Threshold implementations are secure in the presence of glitches



Minimal assumptions on the underlying hardware

Non-completeness of component functions against leakage from glitches

# Threshold implementations are secure in the presence of glitches

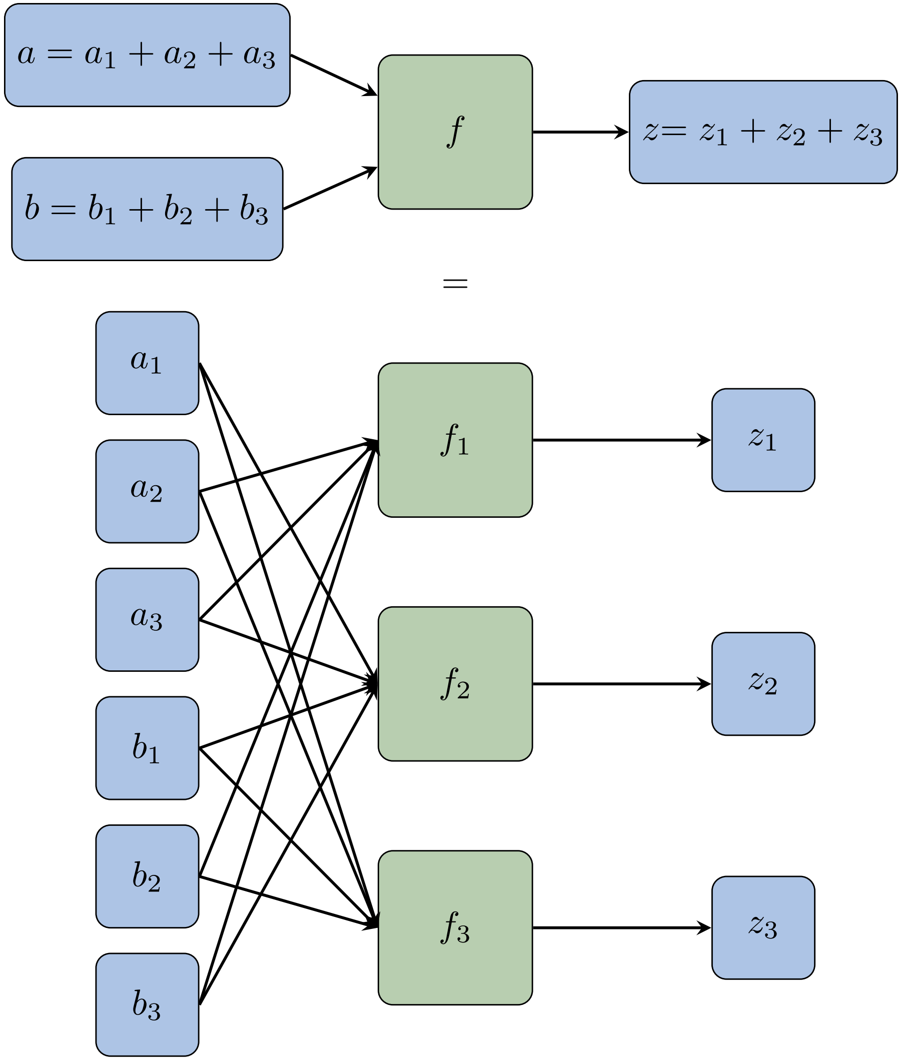


Minimal assumptions on the underlying hardware

Non-completeness of component functions against leakage from glitches

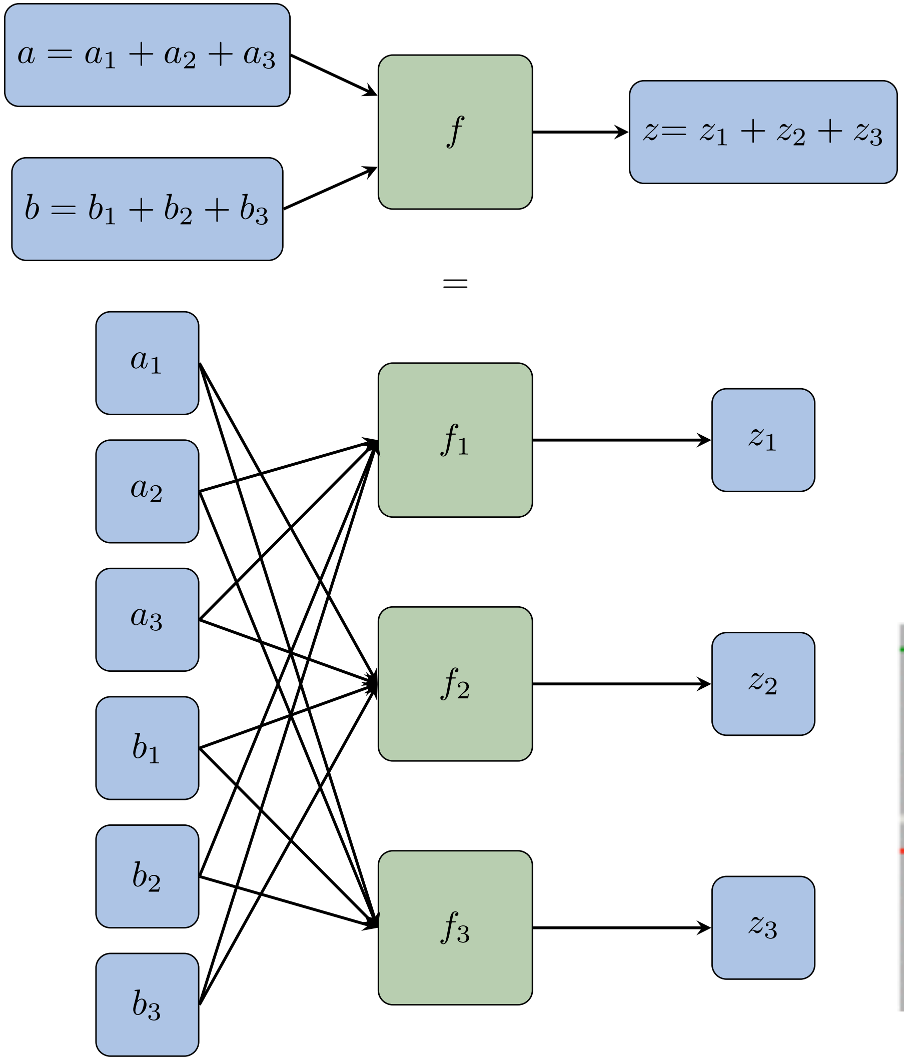
Leakage of the different shares need to be **independent**

# TI assumes the shares to leak independently

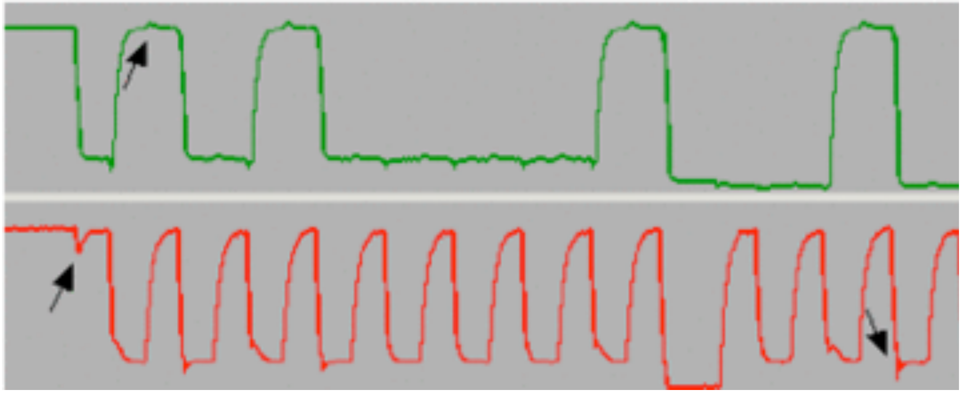


If one component function influences another, non-completeness is broken

# TI assumes the shares to leak independently



If one component function influences another, non-completeness is broken



# Does coupling affect the security of masked implementations?

Masking
  What can go wrong?

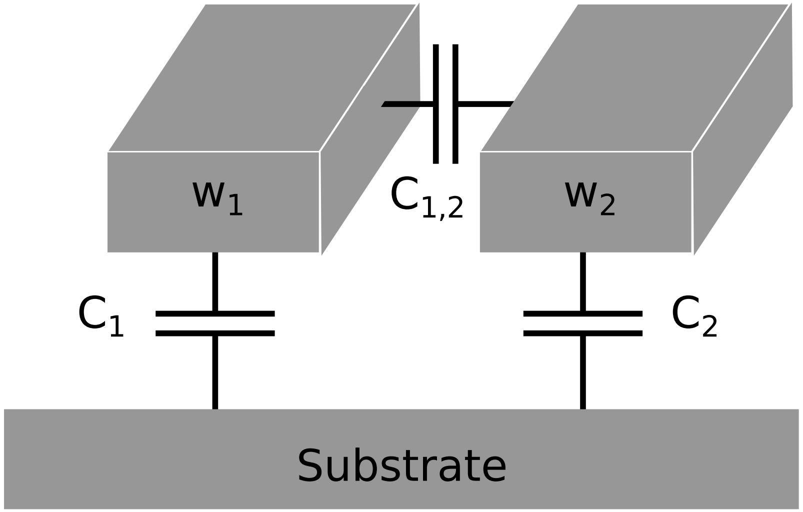
**Sources of coupling**
  Proximity of shares

Detecting coupling in practice

Implications

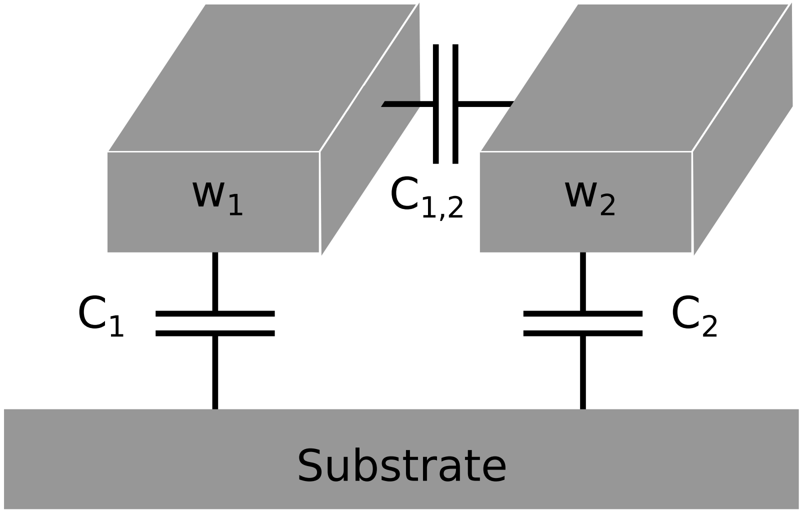
# Crosstalk couples different shares

L(x1, x2) L(x2, x3)



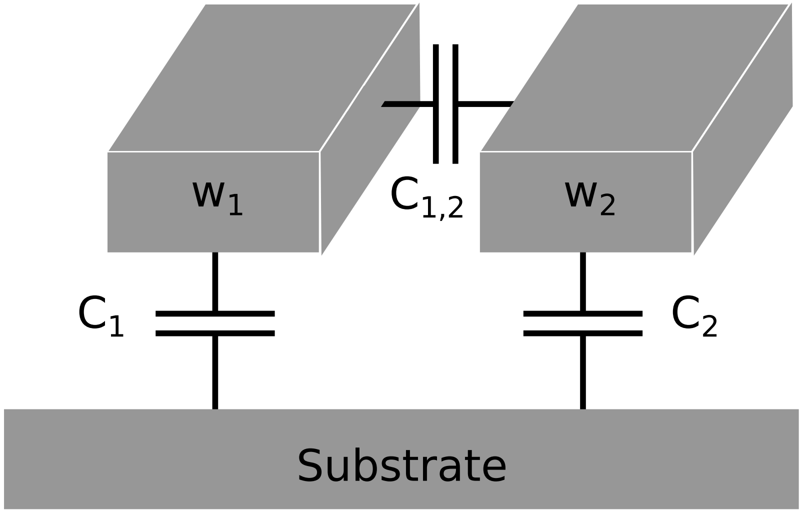
# Crosstalk couples different shares

L(x1, x2)   L(x2, x3) → When coupled: L(x1, x2, x3)



# Crosstalk couples different shares

L(x1, x2)   L(x2, x3) → When coupled: L(x1, x2, x3)



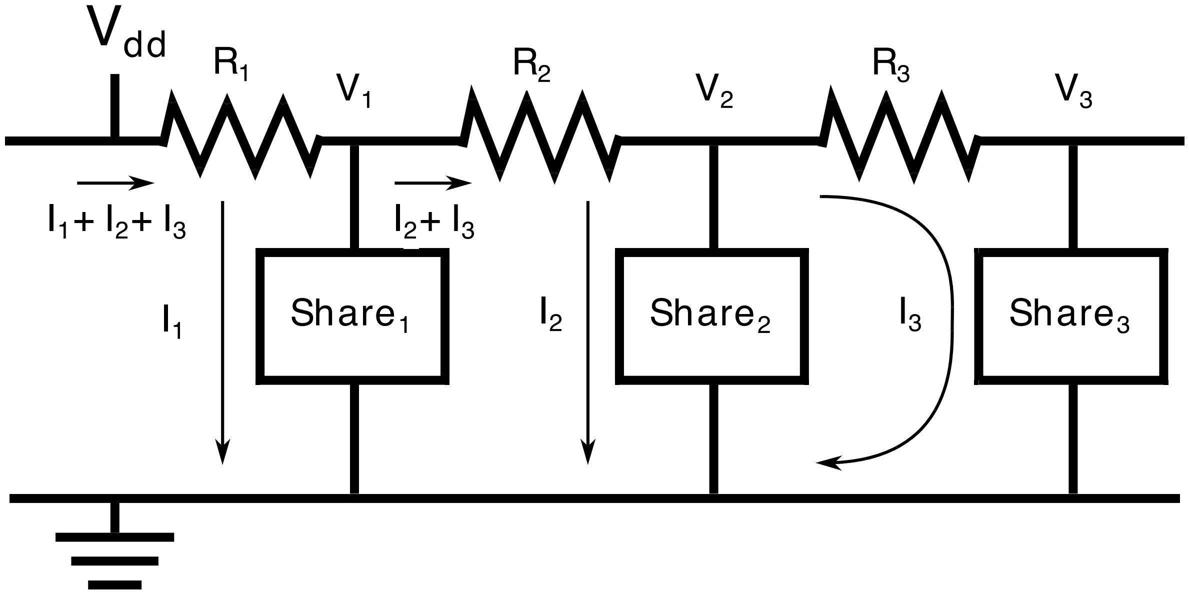
$$C = \frac{e_R \quad e_0 \quad A}{d}$$

A is area

d is **proximity**

# IR Drop couples different shares

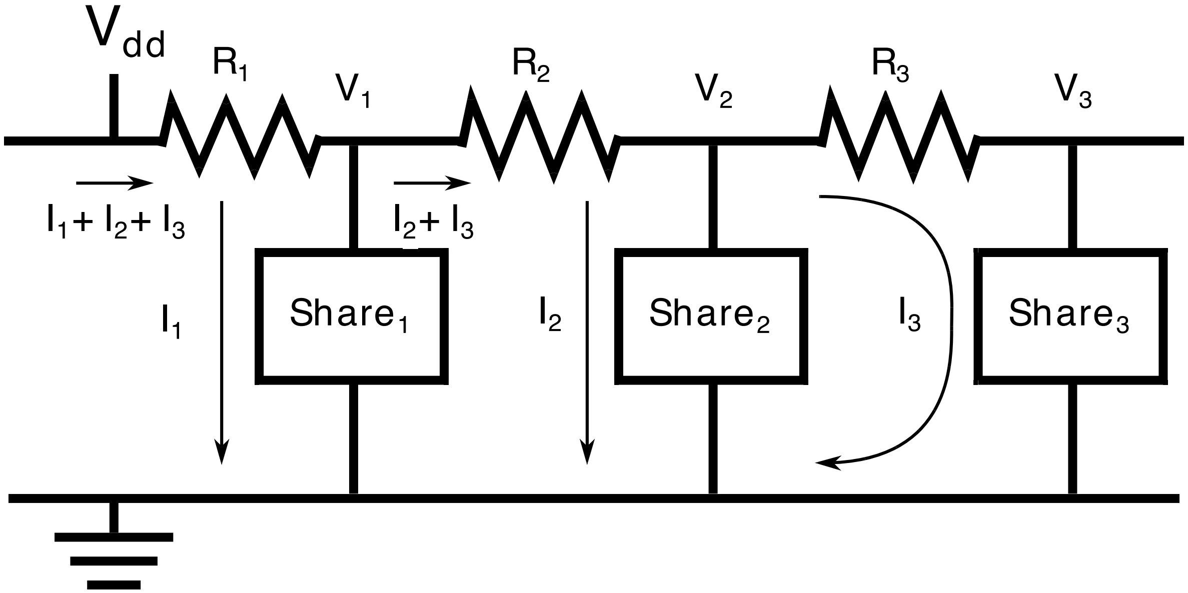
Power and ground distribution
have finite conductance



# IR Drop couples different shares

Power and ground distribution have finite conductance

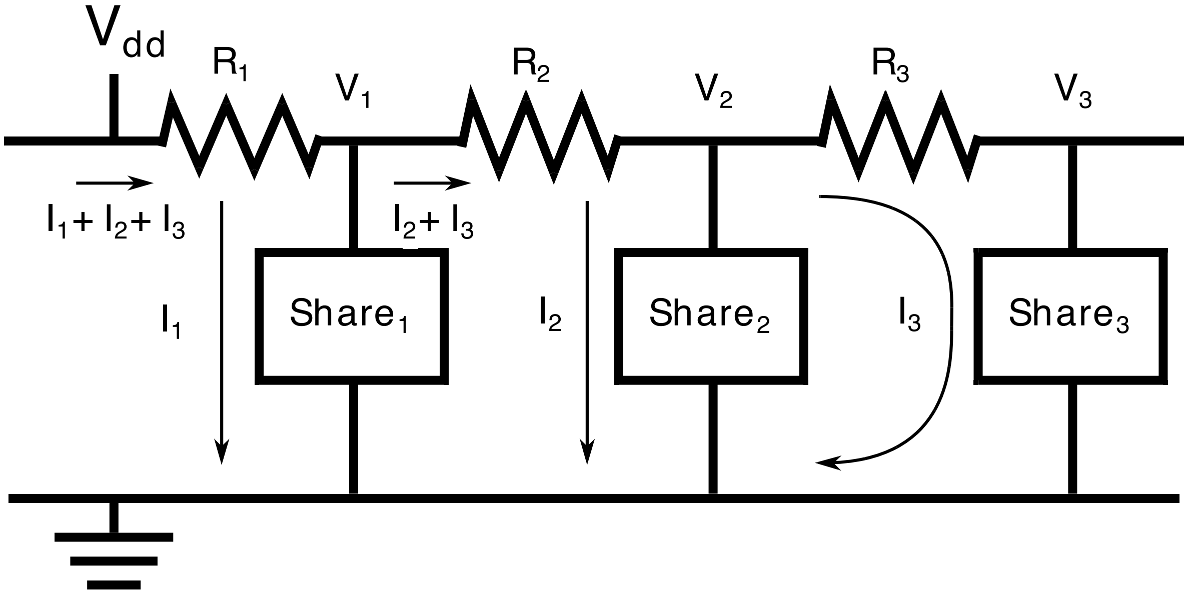
$$V_1 = V_{dd} - (I_1 + I_2 + I_3)R_1$$
$$V_2 = V_{dd} - (I_1 + I_2 + I_3)R_1 - (I_2 + I_3)R_2$$
$$V_3 = V_{dd} - (I_1 + I_2 + I_3)R_1 - (I_2 + I_3)R_2 - I_3R_3\,.$$



# IR Drop couples different shares

Power and ground distribution have finite conductance

$$V_1 = V_{dd} - (I_1 + I_2 + I_3)R_1$$
$$V_2 = V_{dd} - (I_1 + I_2 + I_3)R_1 - (I_2 + I_3)R_2$$
$$V_3 = V_{dd} - (I_1 + I_2 + I_3)R_1 - (I_2 + I_3)R_2 - I_3 R_3 \,.$$

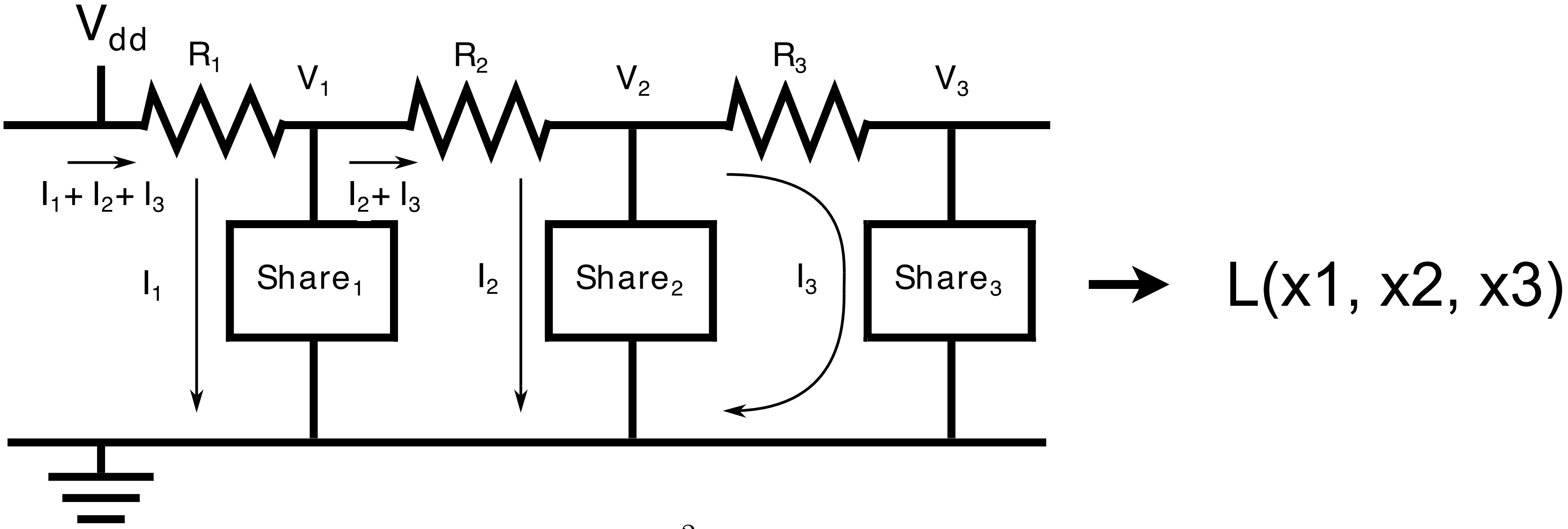


$$P_{inst,Share1} = I_1 V_1 = V_{dd} I_1 - I_1^2 R_1 - I_1 I_2 R_1 - I_1 I_3 R_1$$
$$P_{inst,Share2} = I_2 V_2 = V_{dd} I_2 - I_1 I_2 R_1 - I_2^2 R_1 - I_2 I_3 R_1 - I_2^2 R_2 - I_2 I_3 R_2$$
$$P_{inst,Share3} = I_3 V_3 = V_{dd} I_3 - I_1 I_3 R_1 - I_2 I_3 R_1 - I_3^2 R_1 - I_2 I_3 R_2 - I_3^2 R_2 - I_3^2 R_3 \,.$$

# IR Drop couples different shares

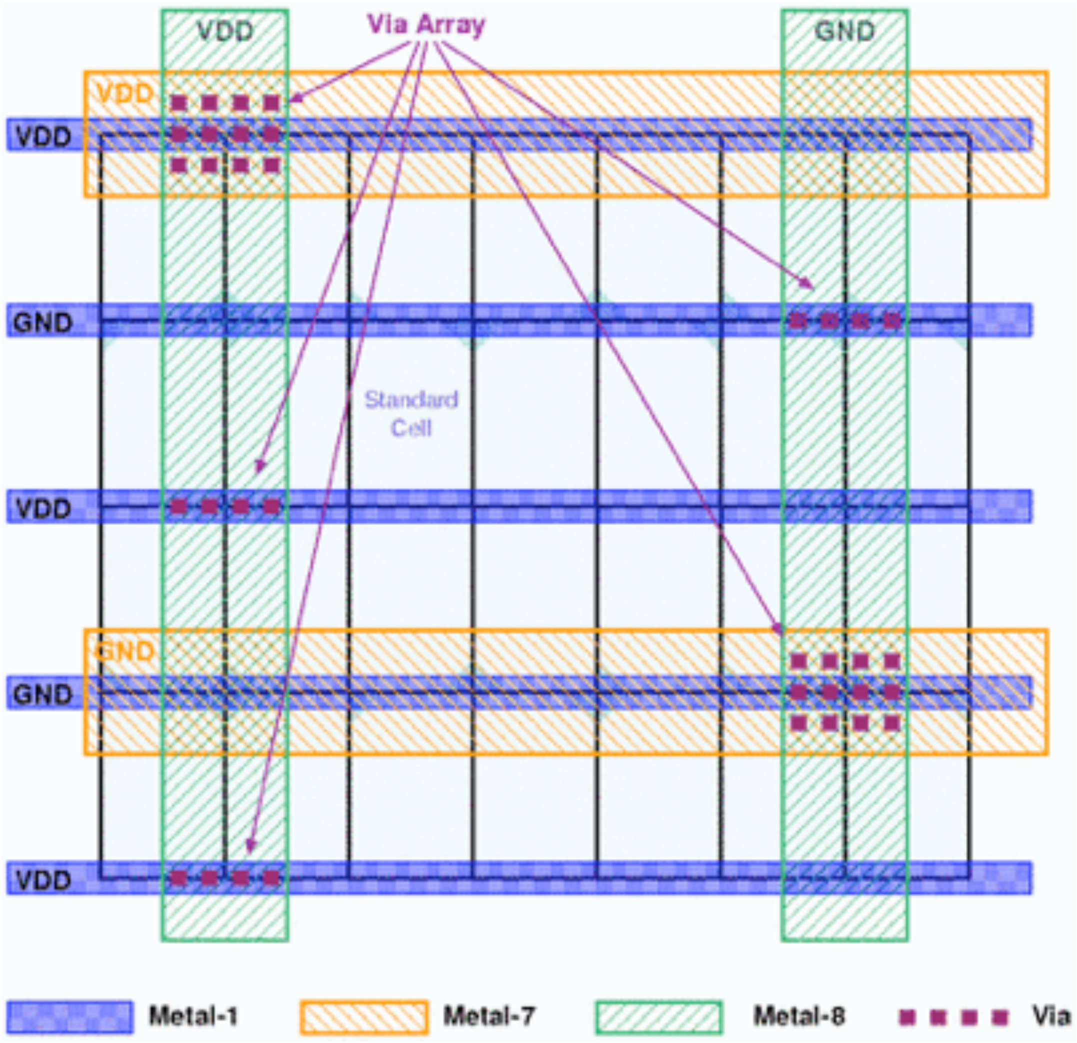
Power and ground distribution have finite conductance

$$V_1 = V_{dd} - (I_1 + I_2 + I_3)R_1$$
$$V_2 = V_{dd} - (I_1 + I_2 + I_3)R_1 - (I_2 + I_3)R_2$$
$$V_3 = V_{dd} - (I_1 + I_2 + I_3)R_1 - (I_2 + I_3)R_2 - I_3R_3\,.$$

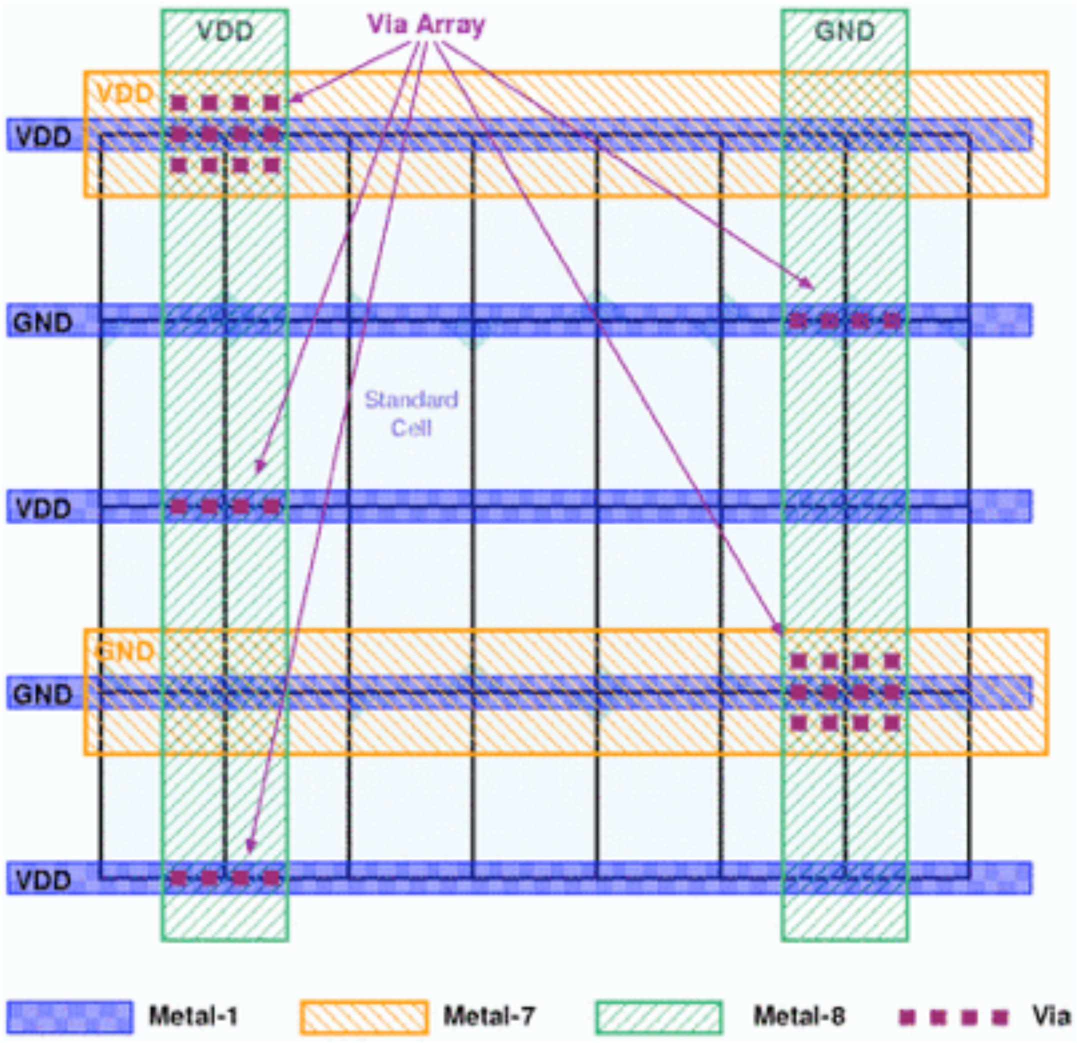


$$P_{inst,Share1} = I_1V_1 = V_{dd}I_1 - I_1^2R_1 - I_1I_2R_1 - I_1I_3R_1$$
$$P_{inst,Share2} = I_2V_2 = V_{dd}I_2 - I_1I_2R_1 - I_2^2R_1 - I_2I_3R_1 - I_2^2R_2 - I_2I_3R_2$$
$$P_{inst,Share3} = I_3V_3 = V_{dd}I_3 - I_1I_3R_1 - I_2I_3R_1 - I_3^2R_1 - I_2I_3R_2 - I_3^2R_2 - I_3^2R_3\,.$$

# Proximity leads again to coupling

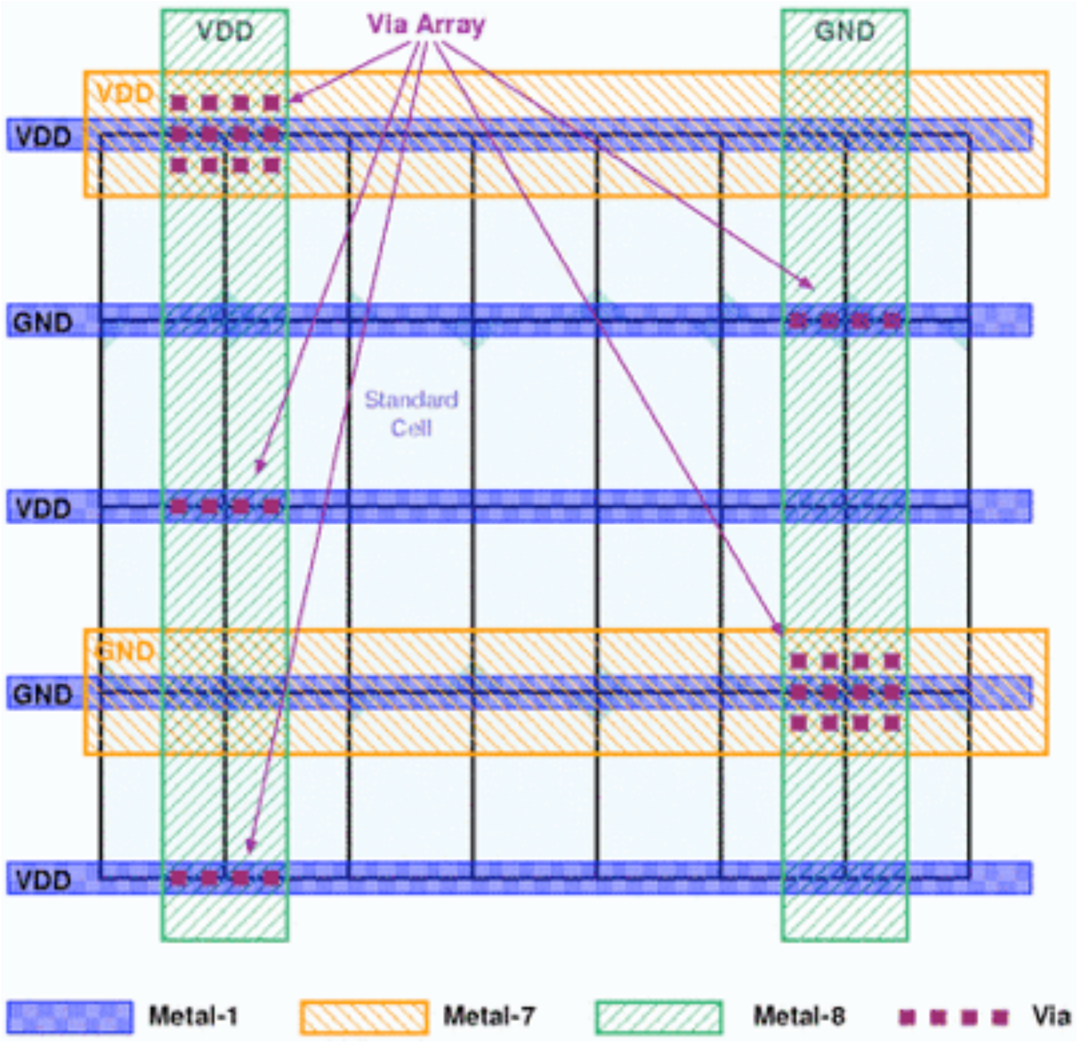


# Proximity leads again to coupling



**Proximity** leads to stronger coupling through power lines

# Proximity leads again to coupling



**Proximity** leads to stronger coupling through power lines

Realistic assumption
**proximity leads to coupling**

# Does coupling affect the security of masked implementations?

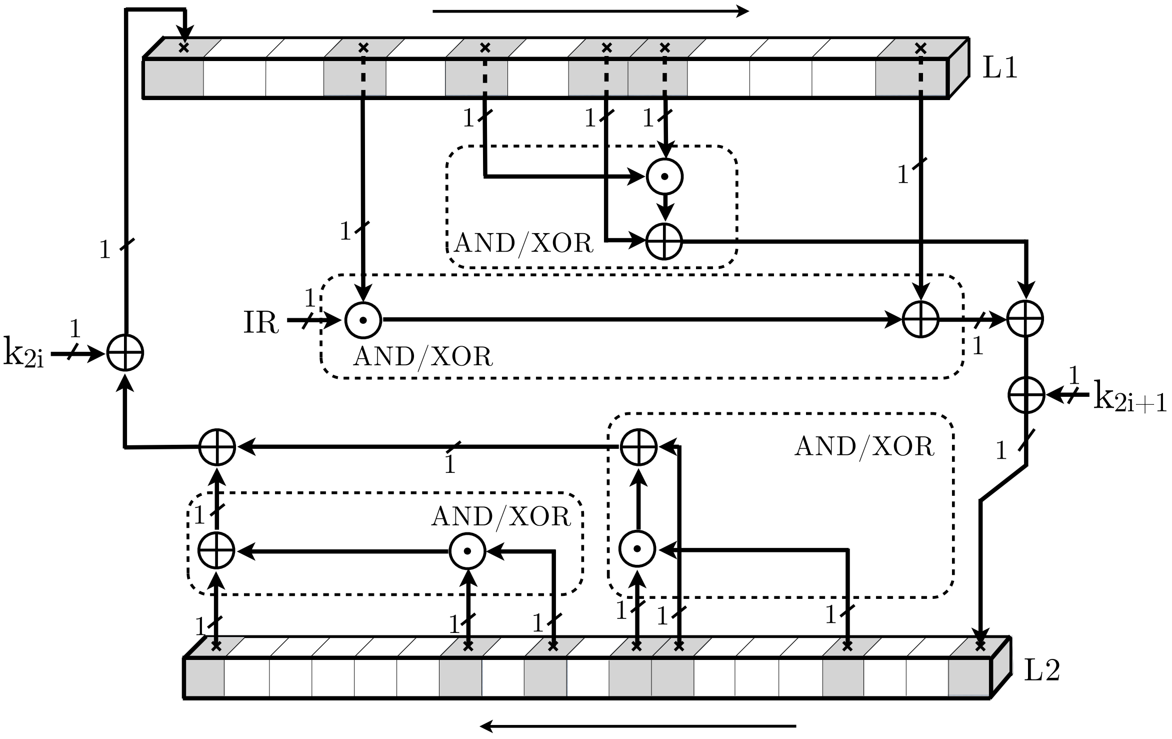
Masking
What can go wrong?

Sources of coupling
Proximity of shares

**Detecting coupling in practice**
Leakage is observable

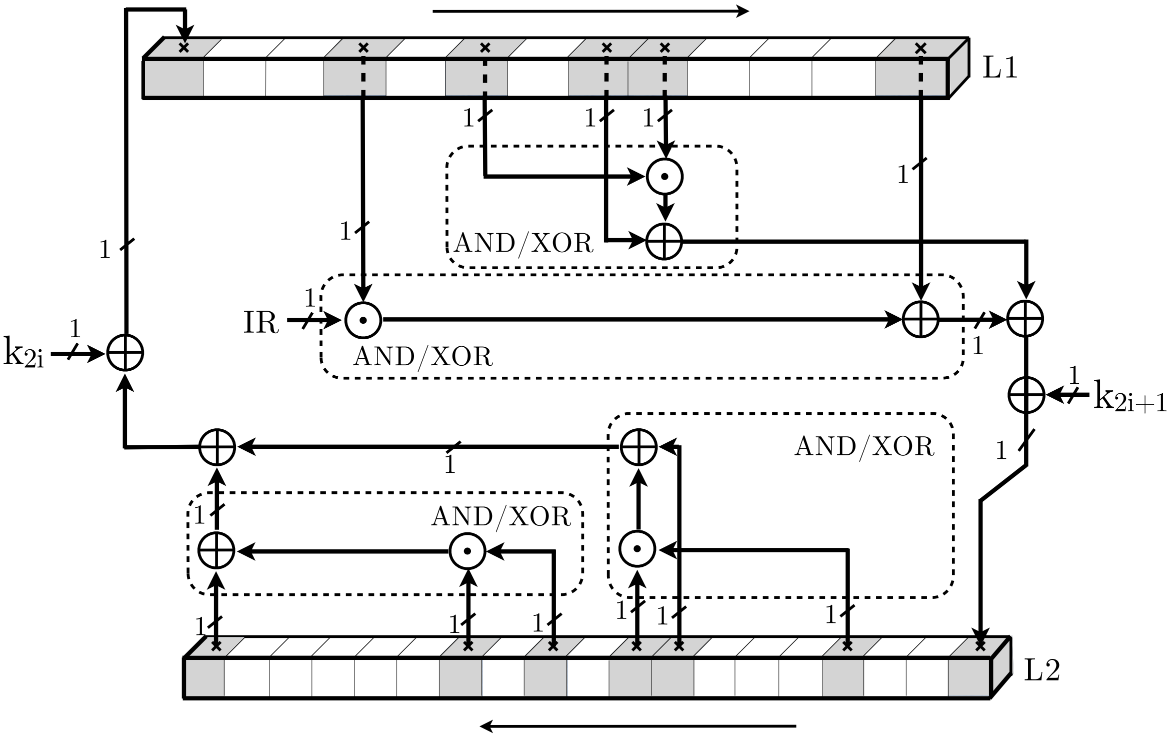
Implications

# TI of KATAN-32 with 3 shares is used in our experiments



Low complexity of the nonlinear layer results in lower switching noise

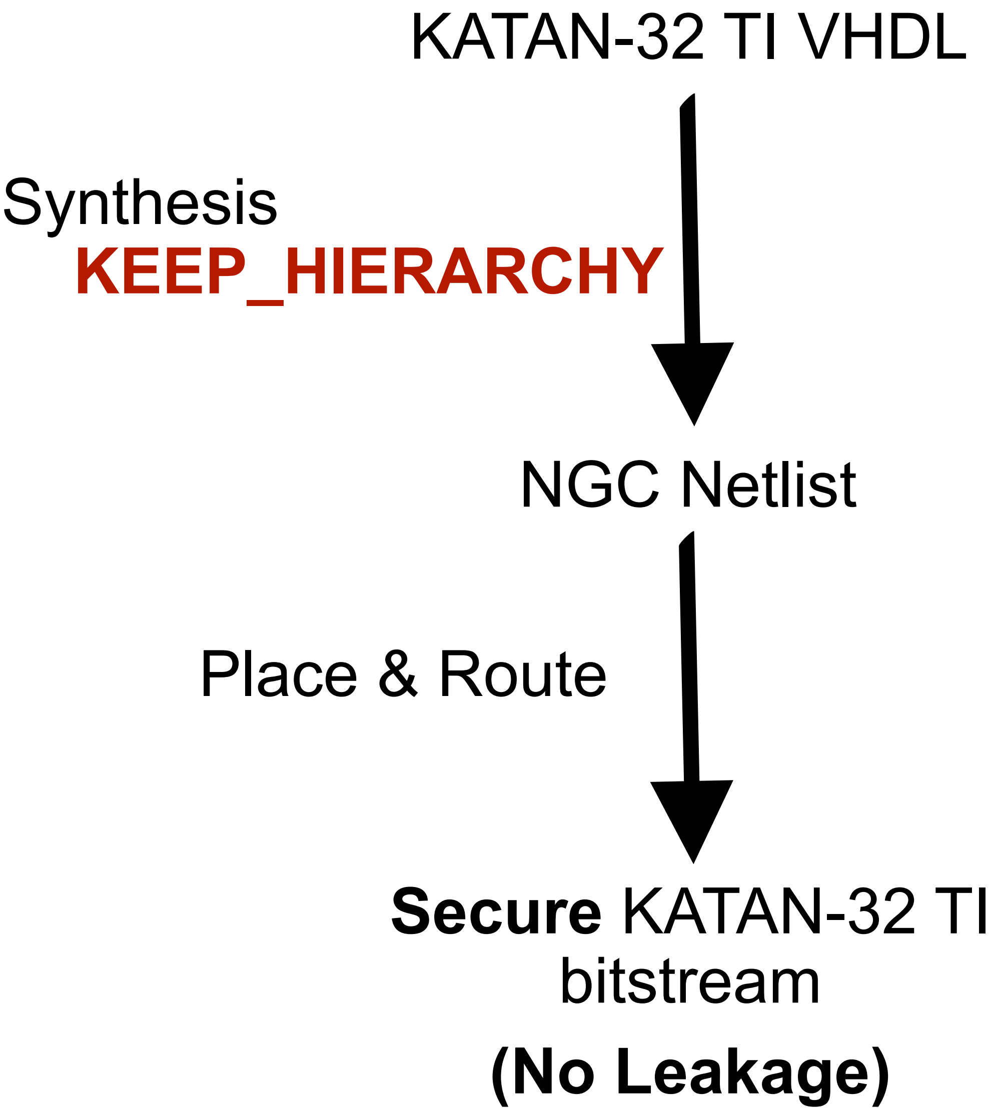
# TI of KATAN-32 with 3 shares is used in our experiments



Low complexity of the nonlinear layer results in lower switching noise

and we expect this makes coupling easier to detect

# Avoiding optimizations over share boundaries is important for security



KATAN-32 TI VHDL

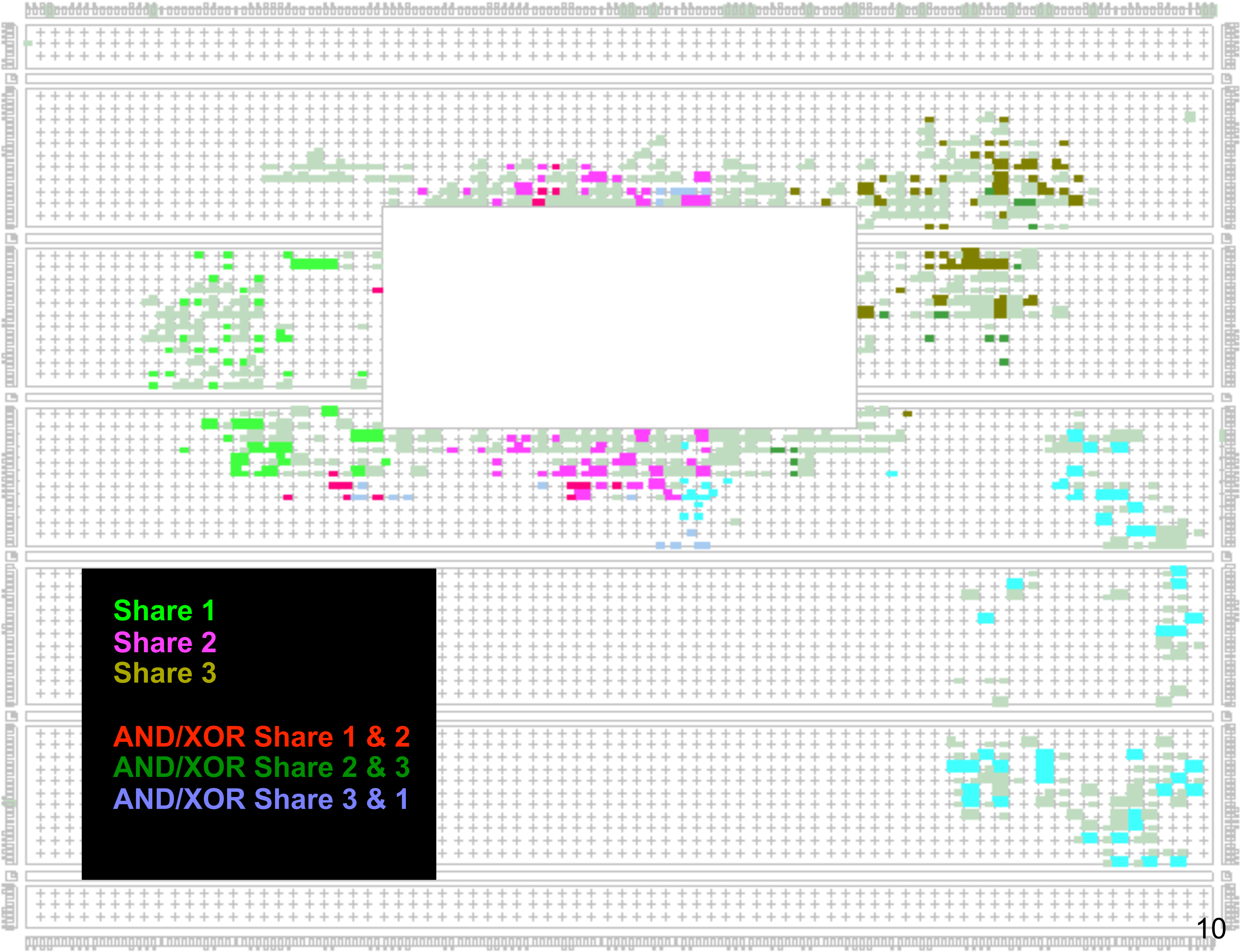
Synthesis
**KEEP_HIERARCHY**

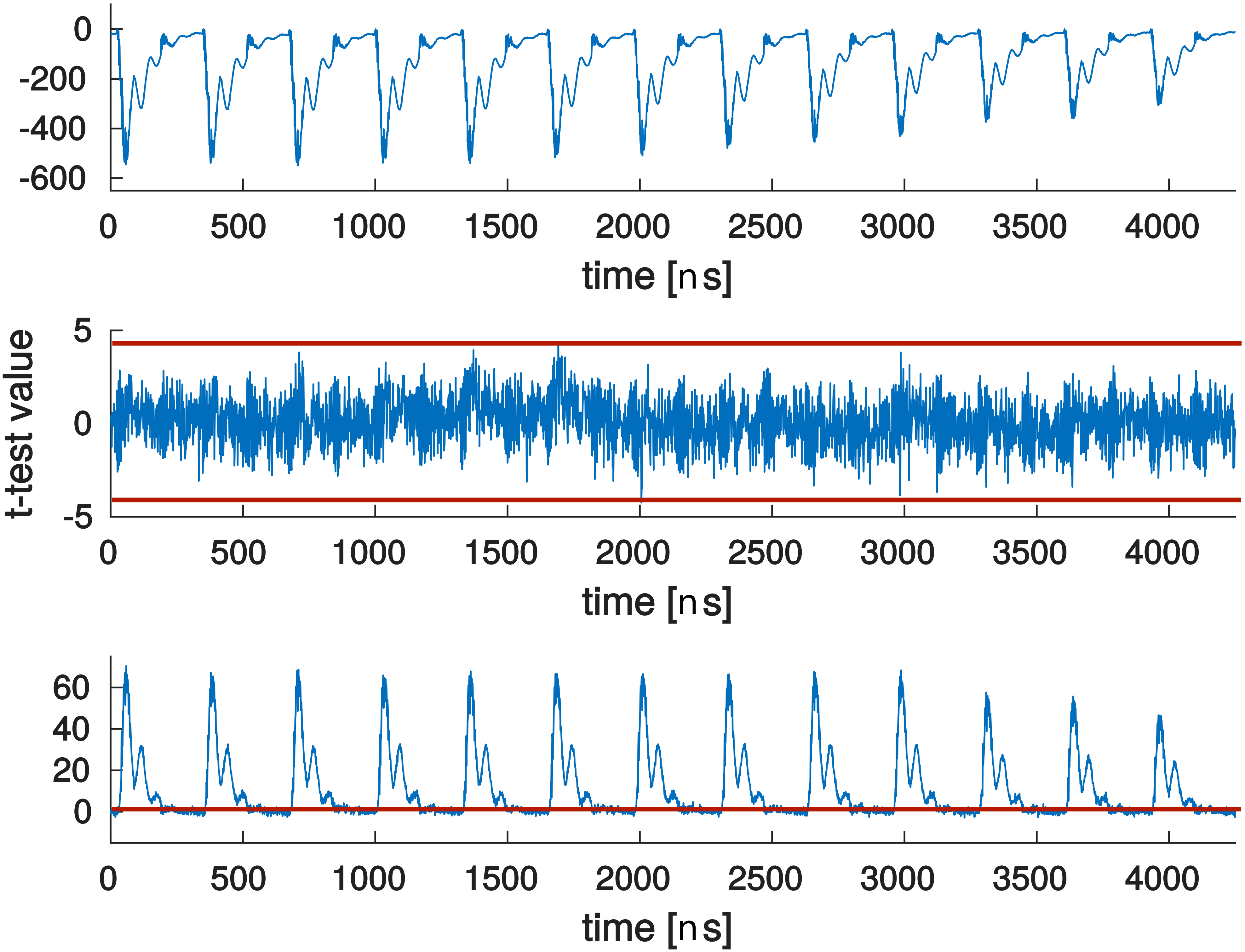
NGC Netlist

Place & Route

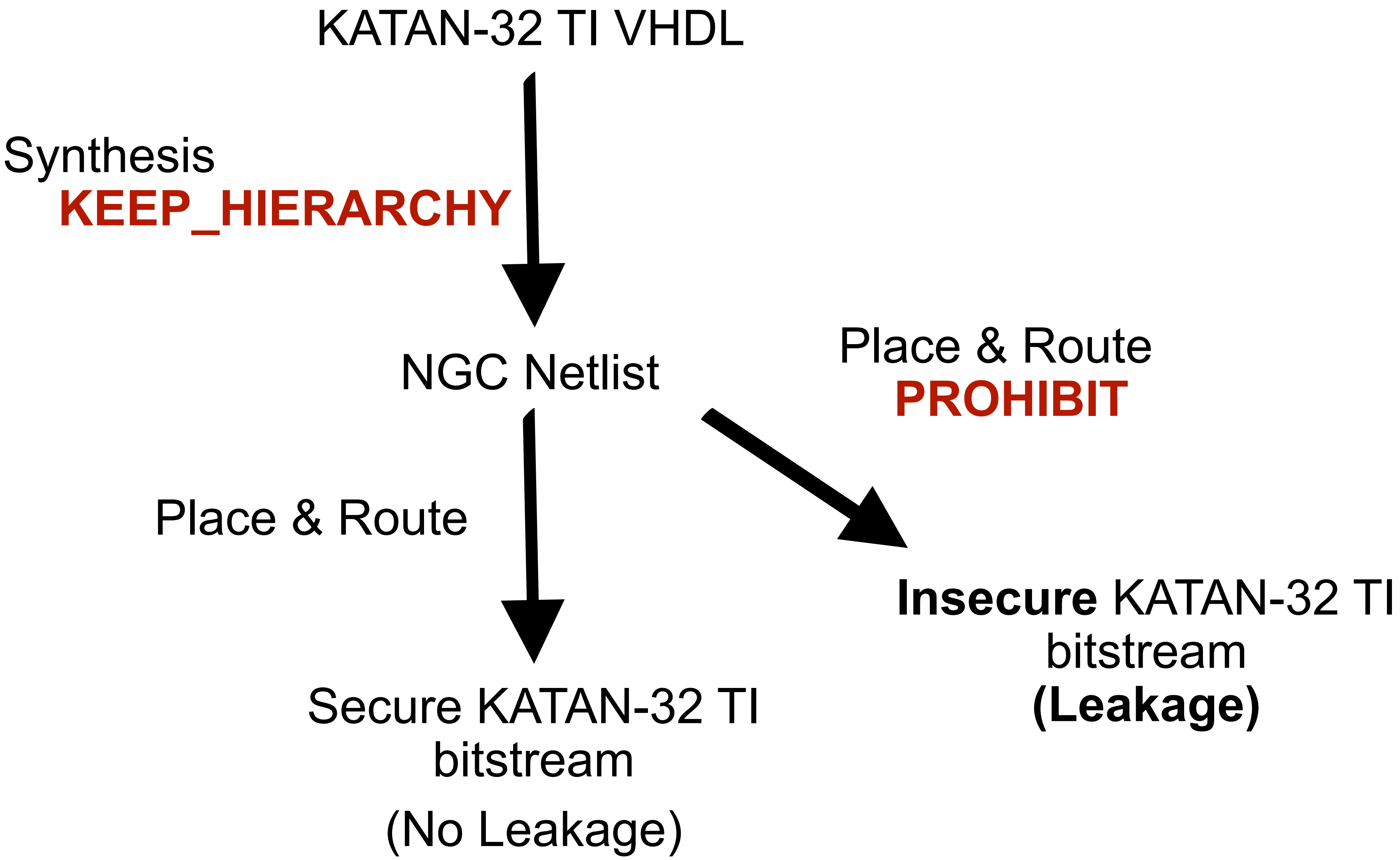
**Secure** KATAN-32 TI bitstream

**(No Leakage)**


Share 1
Share 2
Share 3
AND/XOR Share 1 & 2
AND/XOR Share 2 & 3
AND/XOR Share 3 & 1


0
-200
-400
-600
0
500
1000
1500
2000
2500
3000
3500
4000
time [ns]
t-test value
5
0
-5
0
500
1000
1500
2000
2500
3000
3500
4000
time [ns]
60
40
20
0
0
500
1000
1500
2000
2500
3000
3500
4000
time [ns]

# Bringing shares in close proximity is expected to lead to coupling



KATAN-32 TI VHDL

Synthesis
**KEEP_HIERARCHY**

NGC Netlist

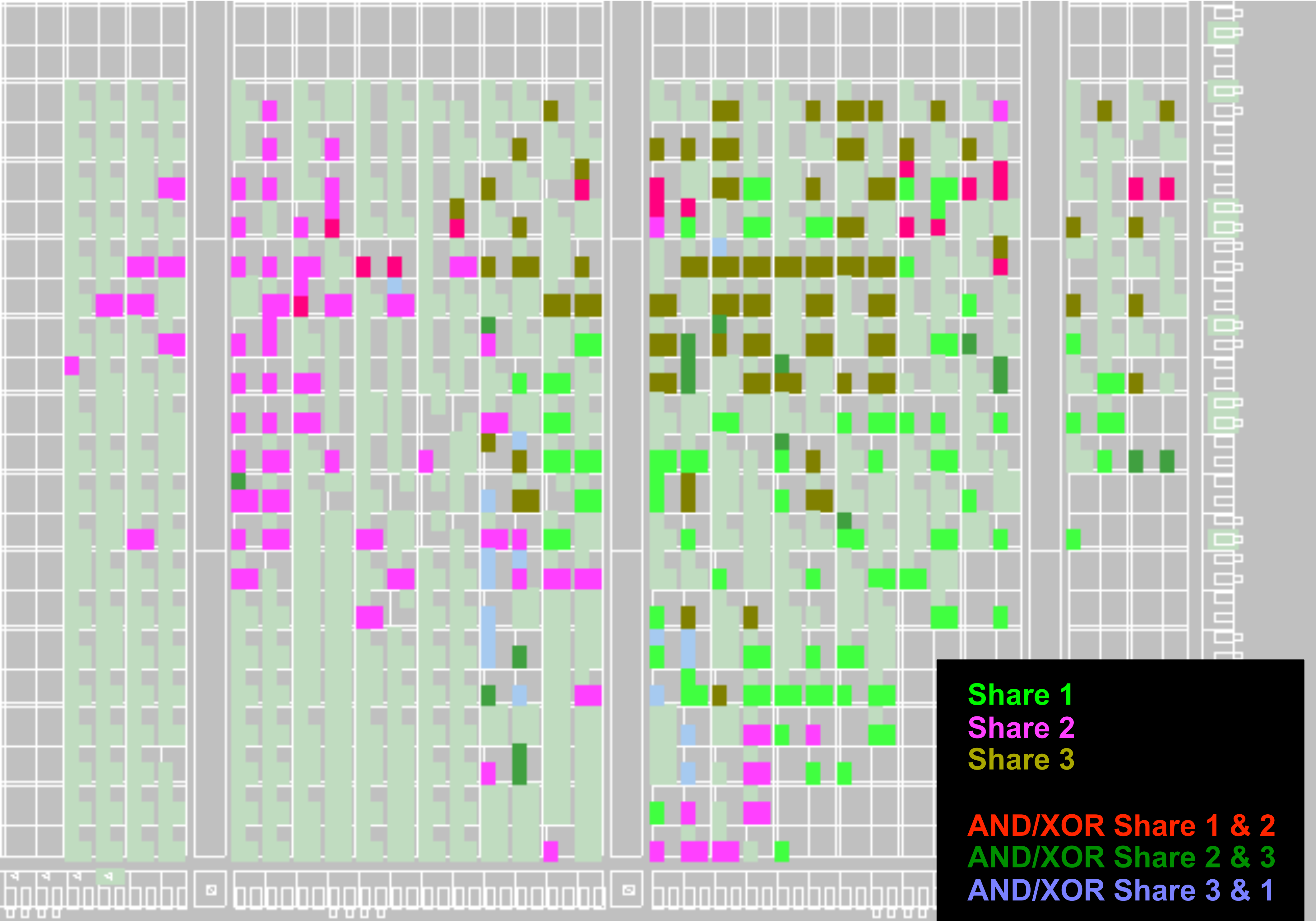
Place & Route

Place & Route
**PROHIBIT**

Secure KATAN-32 TI bitstream

(No Leakage)

**Insecure** KATAN-32 TI bitstream
**(Leakage)**



Share 1

Share 2

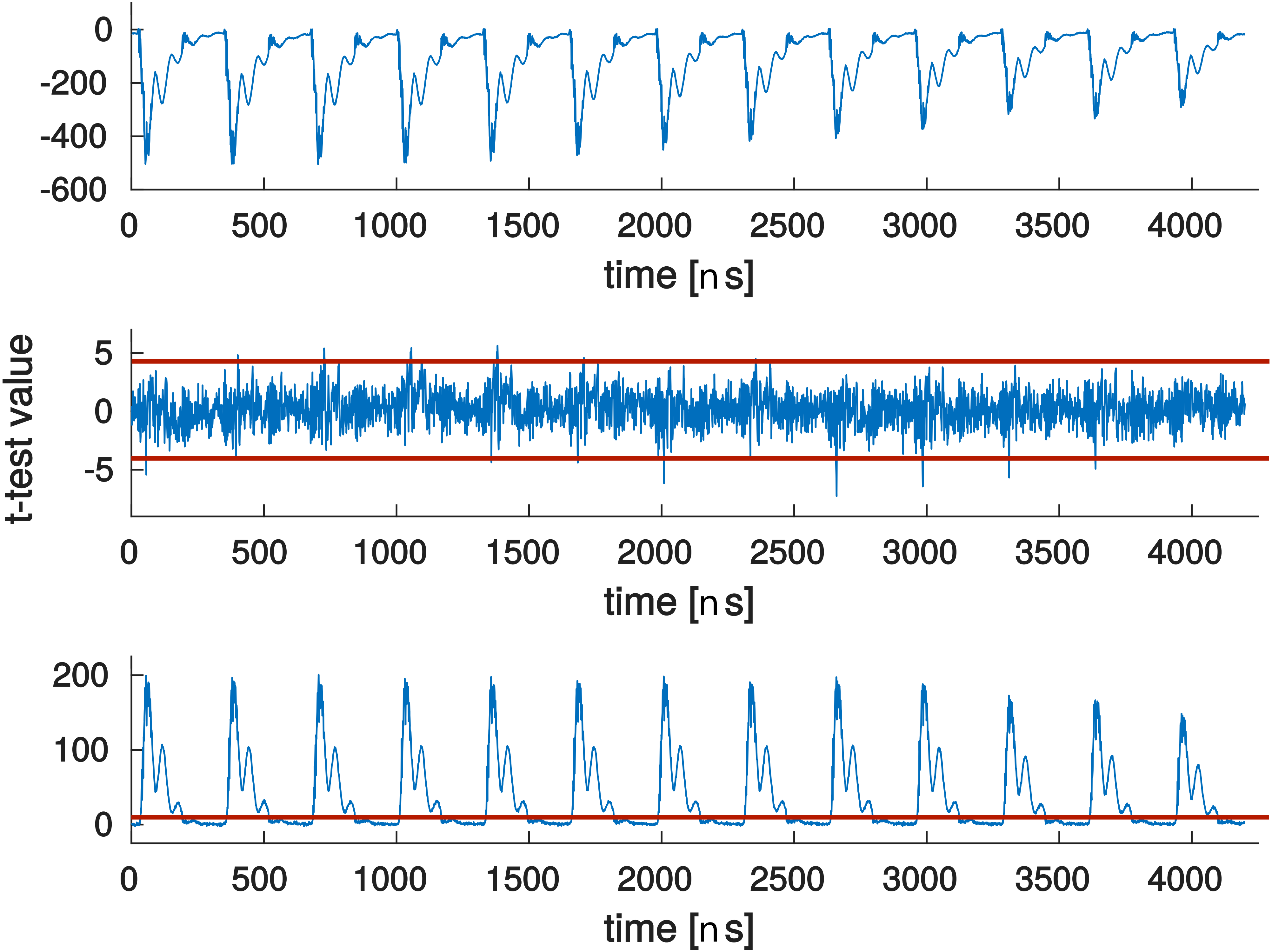
Share 3

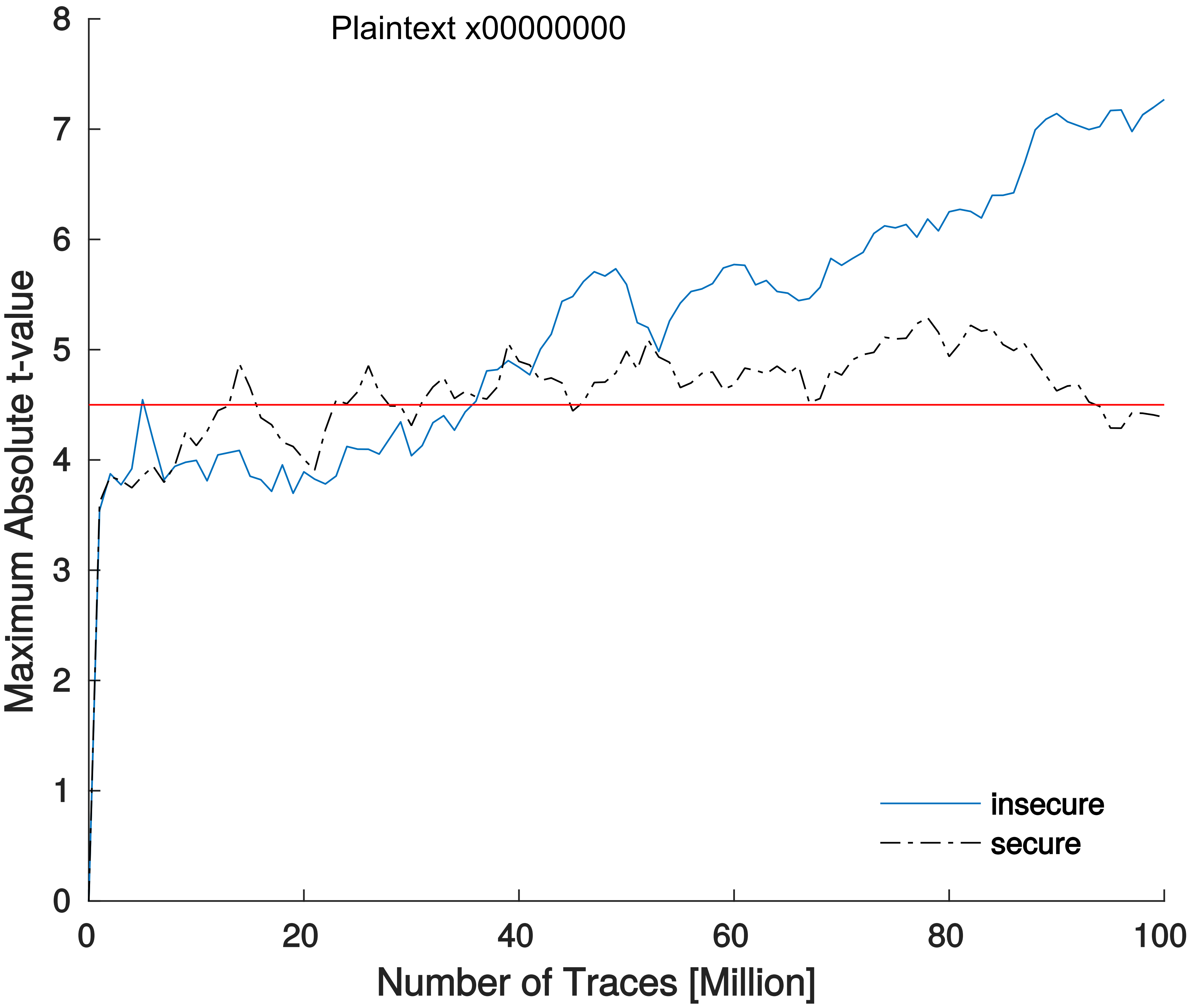
AND/XOR Share 1 & 2

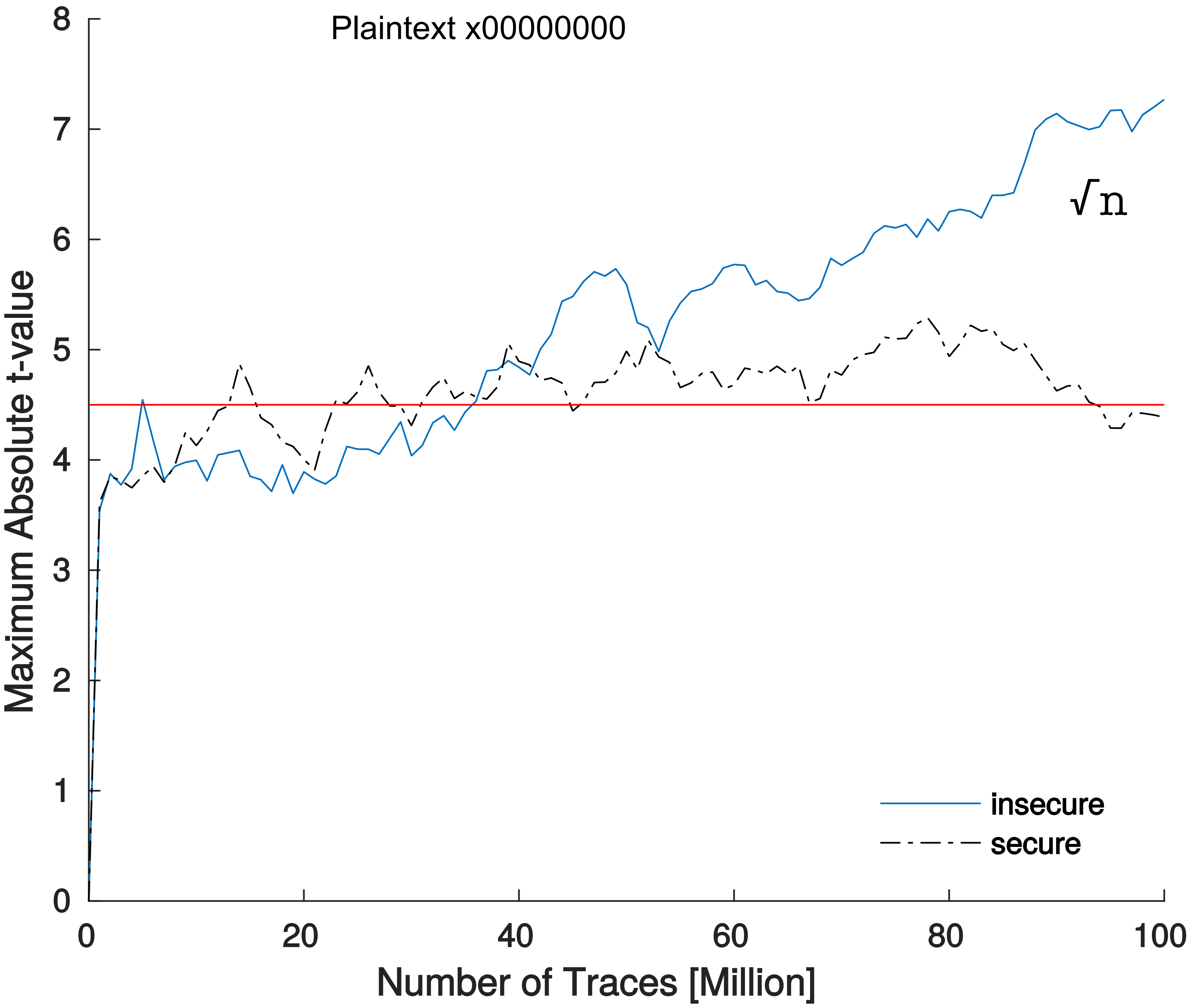
AND/XOR Share 2 & 3

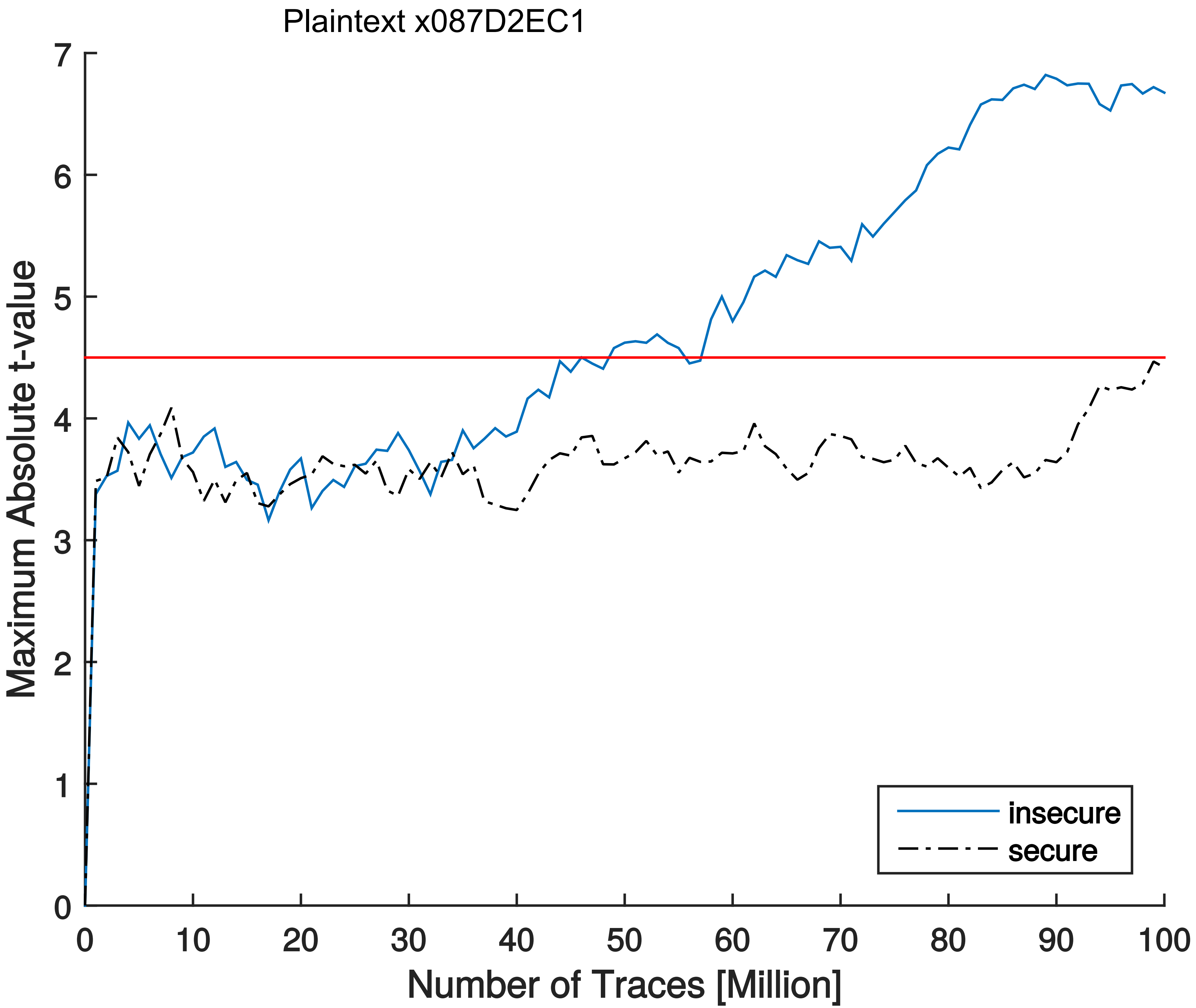
AND/XOR Share 3 & 1

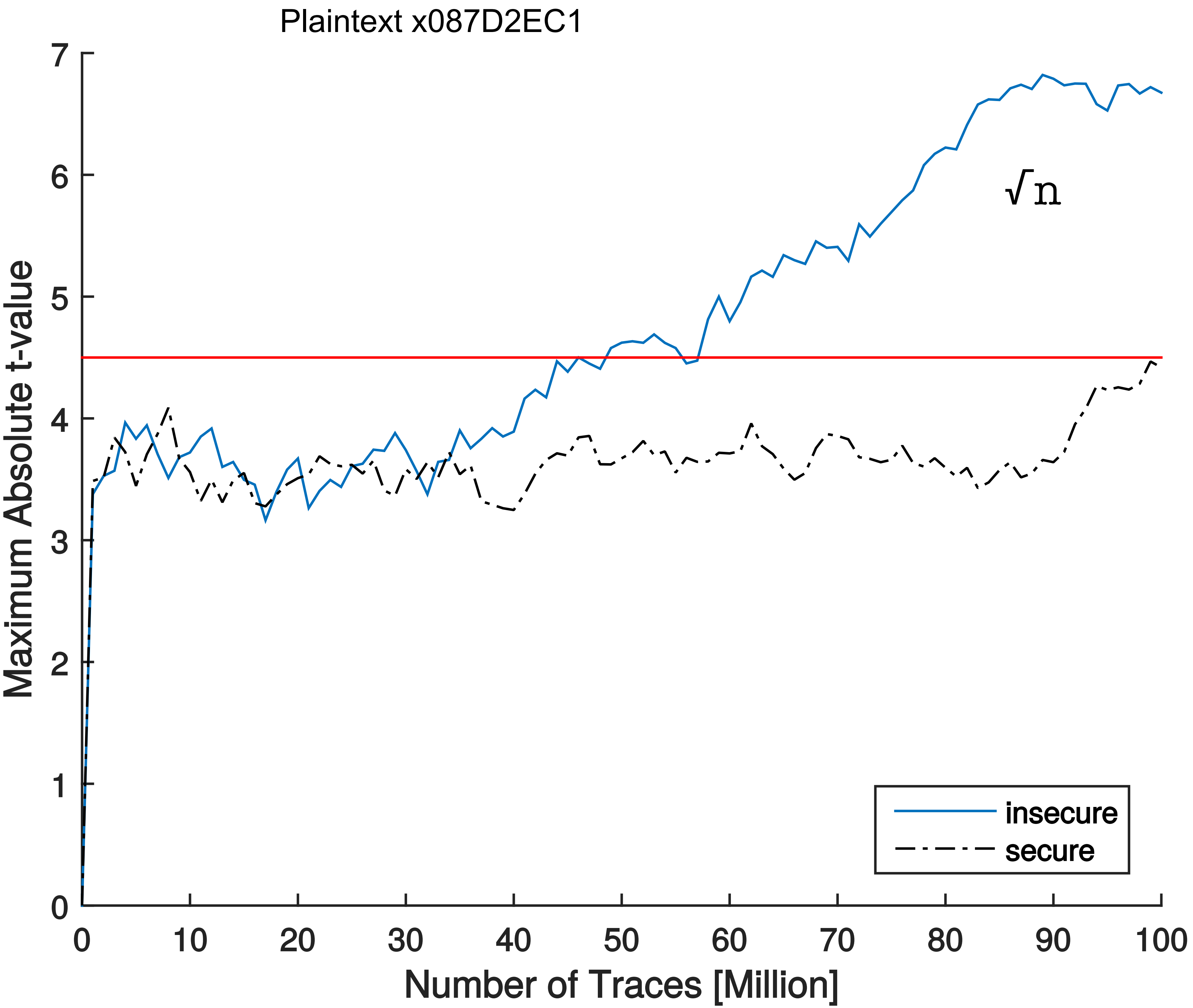
Shares are put in the lower right corner of the FPGA


0
-200
-400
-600
0
500
1000
1500
2000
2500
3000
3500
4000
time [n s]
t-test value
5
0
-5
0
500
1000
1500
2000
2500
3000
3500
4000
time [n s]
200
100
0
0
500
1000
1500
2000
2500
3000
3500
4000
time [n s]


Plaintext x00000000
Maximum Absolute t-value
0
1
2
3
4
5
6
7
8
0
20
40
60
80
100
Number of Traces [Million]
insecure
secure


Plaintext x00000000
√n
Maximum Absolute t-value
0
1
2
3
4
5
6
7
8
0
20
40
60
80
100
Number of Traces [Million]
insecure
secure


Plaintext x087D2EC1
Maximum Absolute t-value
0
1
2
3
4
5
6
7
Number of Traces [Million]
0
10
20
30
40
50
60
70
80
90
100
insecure
secure


Plaintext x087D2EC1
Maximum Absolute t-value
0
1
2
3
4
5
6
7
0
10
20
30
40
50
60
70
80
90
100
Number of Traces [Million]
√n
insecure
secure

# Does coupling affect the security of masked implementations?

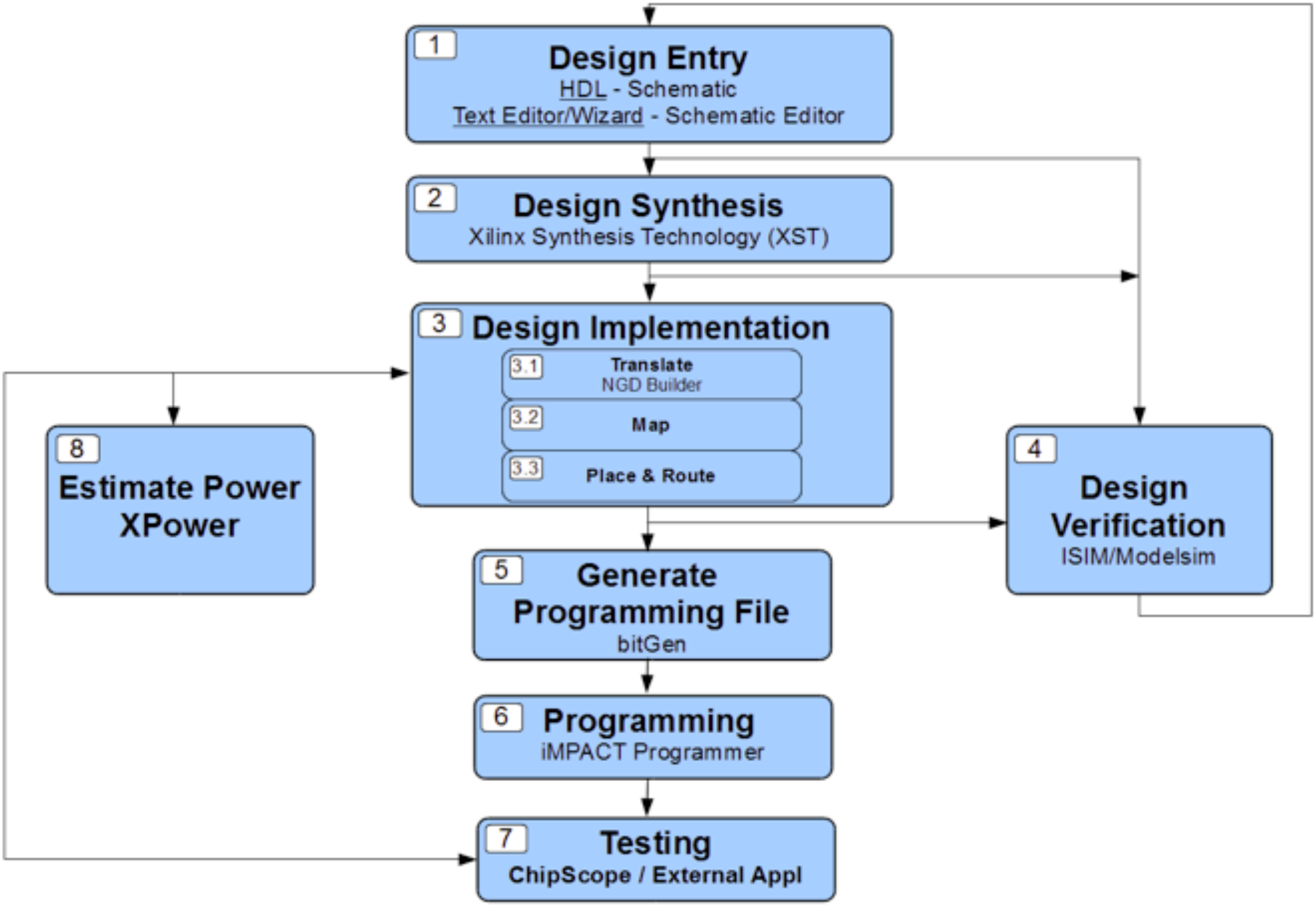
Masking
What can go wrong?

Sources of coupling
Proximity of shares

Detecting coupling in practice
Leakage is observable

**Implications**

# We control up to the placement stage
# Can we be sure?



1 Design Entry
HDL - Schematic
Text Editor/Wizard - Schematic Editor

2 Design Synthesis
Xilinx Synthesis Technology (XST)

3 Design Implementation
3.1 Translate
NGD Builder
3.2 Map
3.3 Place & Route

4 Design Verification
ISIM/Modelsim

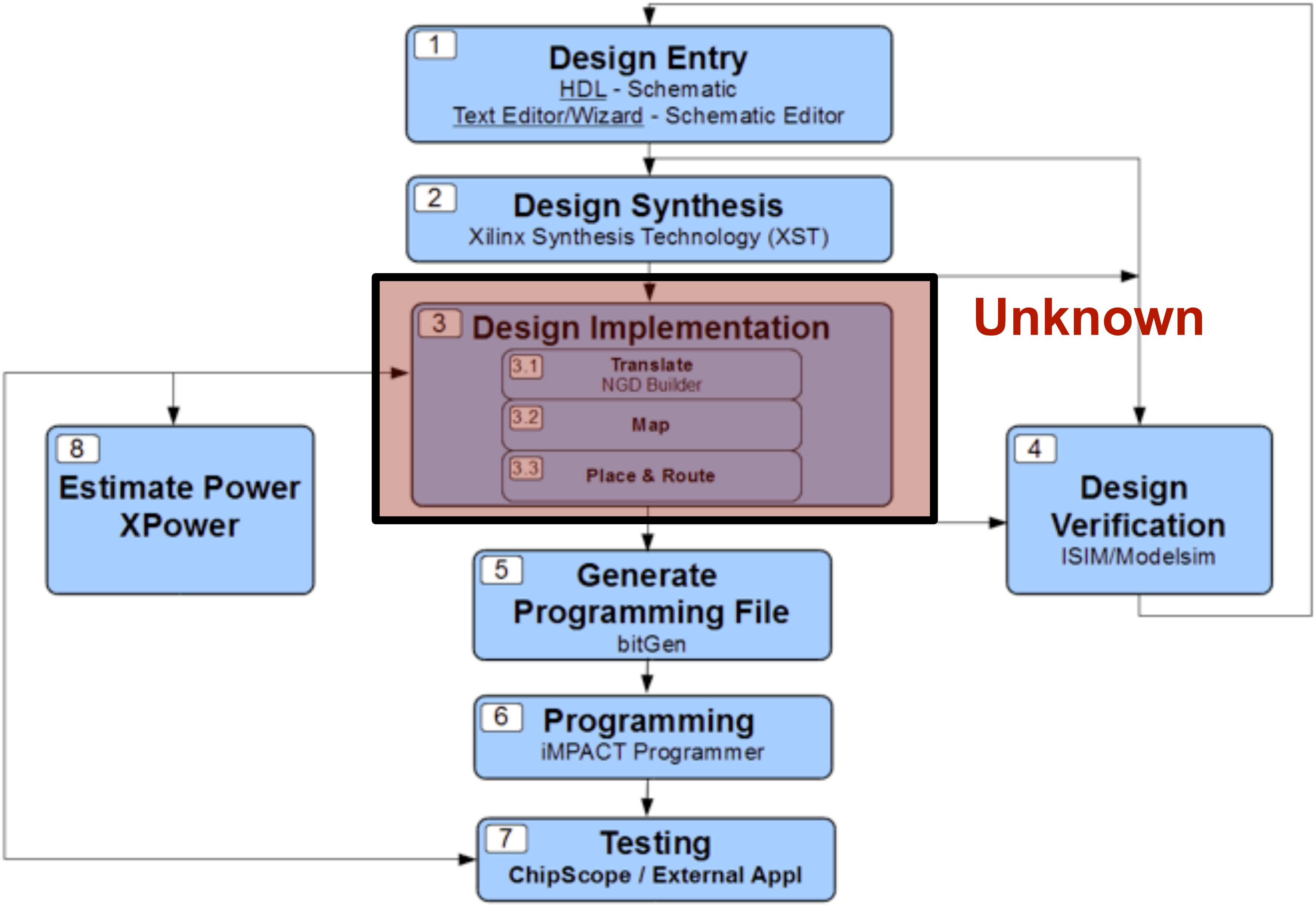
5 Generate Programming File
bitGen

6 Programming
iMPACT Programmer

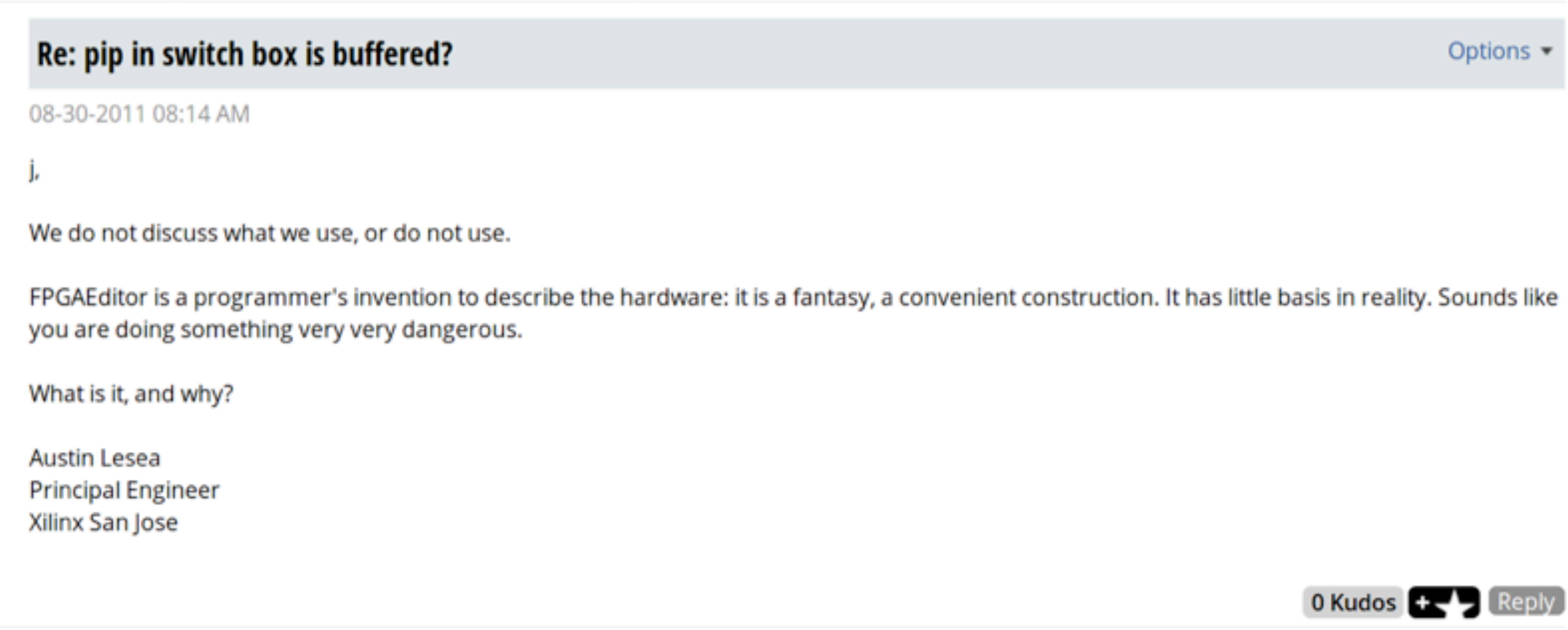
7 Testing
ChipScope / External Appl

8 Estimate Power
XPower

# We control up to the placement stage
# Can we be sure?



# The FPGA is a black box
# Can we be sure?



**Re: pip in switch box is buffered?**

08-30-2011 08:14 AM

j,

We do not discuss what we use, or do not use.

FPGAEditor is a programmer's invention to describe the hardware: it is a fantasy, a convenient construction. It has little basis in reality. Sounds like you are doing something very very dangerous.

What is it, and why?

Austin Lesea
Principal Engineer
Xilinx San Jose

# Coupling becomes more prominent in smaller technology nodes

90nm
SASEBO-G

65nm
SASEBO-GII

45nm
SAKURA-G

28nm
SAKURA-X

# Coupling becomes more prominent in smaller technology nodes

90nm
SASEBO-G

65nm
SASEBO-GII

45nm
SAKURA-G

28nm
SAKURA-X

2004

# Coupling becomes more prominent in smaller technology nodes

90nm
SASEBO-G

65nm
SASEBO-GII

45nm
SAKURA-G

28nm
SAKURA-X

2004

What can we expect for modern and future platforms?

# Does Coupling Affect the Security of Masked Implementations?

# Does Coupling Affect the Security of Masked Implementations?

It might ...

# Does Coupling Affect the Security of Masked Implementations?

It might ...

# Does Coupling Affect the Security of Masked Implementations?
# It might ...

The influence from coupling is observable

# Does Coupling Affect the Security of Masked Implementations? It might ...

The influence from coupling is observable (marginally)

# Does Coupling Affect the Security of Masked Implementations? It might ...

The influence from coupling is observable (marginally)

but pinpointing exact source is hard

and many open questions remain.

# Does Coupling Affect the Security of Masked Implementations? It might ...

The influence from coupling is observable (marginally)
but pinpointing exact source is hard
and many open questions remain.

- What about implementations with 2 shares (d+1)?

# Does Coupling Affect the Security of Masked Implementations?
# It might ...

The influence from coupling is observable (marginally)
but pinpointing exact source is hard
and many open questions remain.

- What about implementations with 2 shares (d+1)?

- Technology? ASIC vs FPGA?

# Does Coupling Affect the Security of Masked Implementations?
# It might ...

The influence from coupling is observable (marginally)
but pinpointing exact source is hard
and many open questions remain.

- What about implementations with 2 shares (d+1)?
- Technology? ASIC vs FPGA?
- How to implement masking schemes securely?

# Does Coupling Affect the Security of Masked Implementations? It might ...

The influence from coupling is observable (marginally)
but pinpointing exact source is hard
and many open questions remain.

- What about implementations with 2 shares (d+1)?
- Technology? ASIC vs FPGA?
- How to implement masking schemes securely?
- **Is key retrieval possible?**

13/04 – COSADE 2017 – Paris