RUB

SafeDRP: Yet Another Way Toward Power-Equalized Designs in FPGA

Maik Ender, Alexander Wild, and Amir Moradi

COSADE 2017 13.04.17

hgi EMSEC

Motivation and Background

- Variety of countermeasures
  - Rekeying
  - Masking
  - Hiding

Motivation and Background

- Variety of countermeasures
  - Rekeying
  - Masking
  - Hiding
- This talk: power equalization on FPGAs
  - Dynamic power consumption ⇔ switches

Motivation and Background

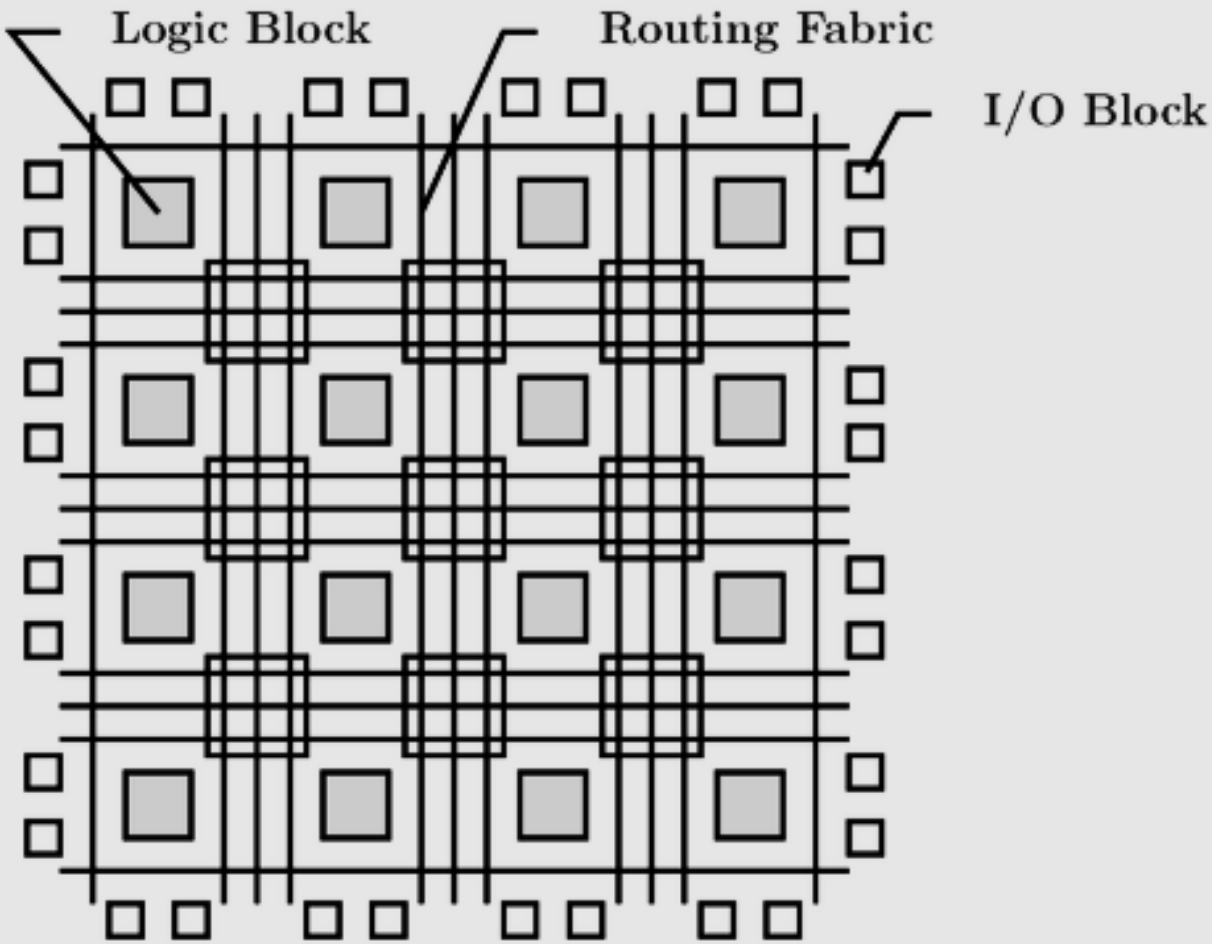
- Variety of countermeasures
  - Rekeying
  - Masking
  - Hiding
- This talk: power equalization on FPGAs
  - Dynamic power consumption ⇔ switches
- Why do we need another scheme?
  - Pitfalls in implementation
  - Lastly published GliFreD has high resource consumption of FF

Motivation and Background

- Variety of countermeasures
  - Rekeying
  - Masking
  - Hiding
- This talk: power equalization on FPGAs
  - Dynamic power consumption ⇔ switches
- Why do we need another scheme?
  - Pitfalls in implementation
  - Lastly published GliFreD has high resource consumption of FF
- Idea: less FF while addressing all pitfalls

Field Programmable Gate Array

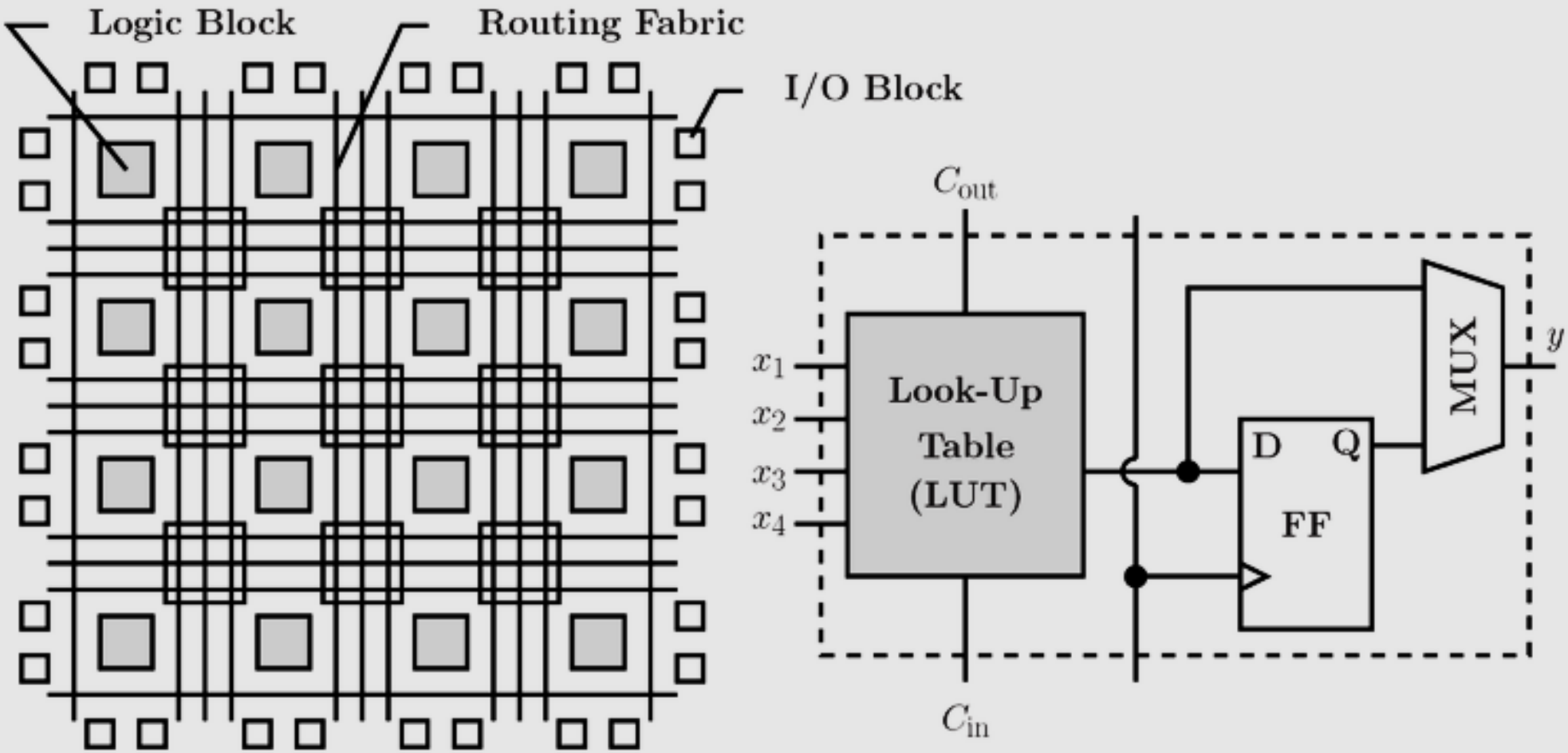
Concept



Source: Electronics **2015;** Optimally Fortifying Logic Reliability through Criticality Ranking; **http://www.mdpi.com/2079-9292/4/1/150/htm**

Field Programmable Gate Array

Concept

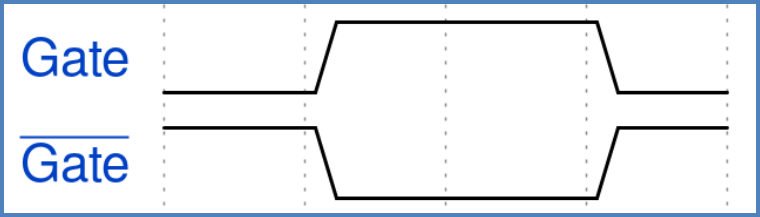


Source: Electronics **2015;** Optimally Fortifying Logic Reliability through Criticality Ranking; **http://www.mdpi.com/2079-9292/4/1/150/htm**

Dual-Rail-Precharge (DRP)

Dual-Rail Logic

- Differential encoding
- Valid values: 10 or 01
- No Inverter

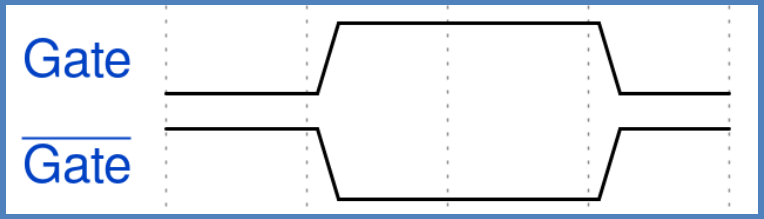


Dual-Rail-Precharge (DRP)

RUB

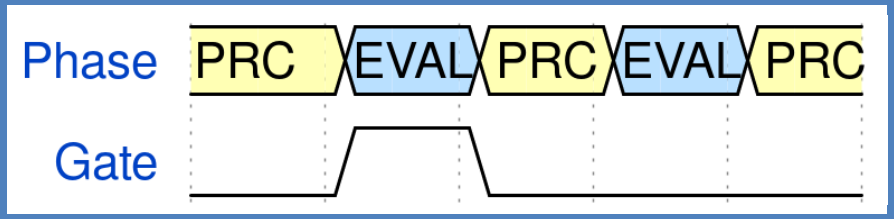
Dual-Rail Logic

- Differential encoding
- Valid values: 10 or 01
- No Inverter



Precharge Logic

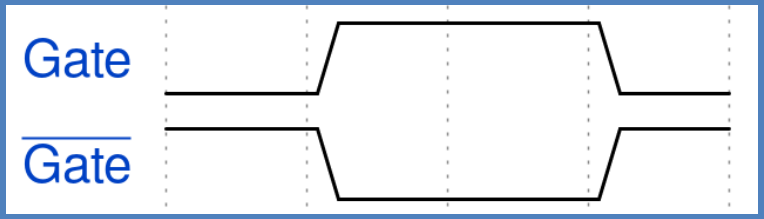
- Alternates between Precharge and logic value
- Precharge and evaluation phase



Dual-Rail-Precharge (DRP)

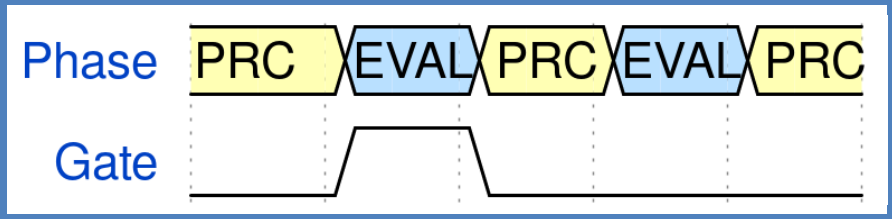
Dual-Rail Logic

- Differential encoding
- Valid values: 10 or 01
- No Inverter



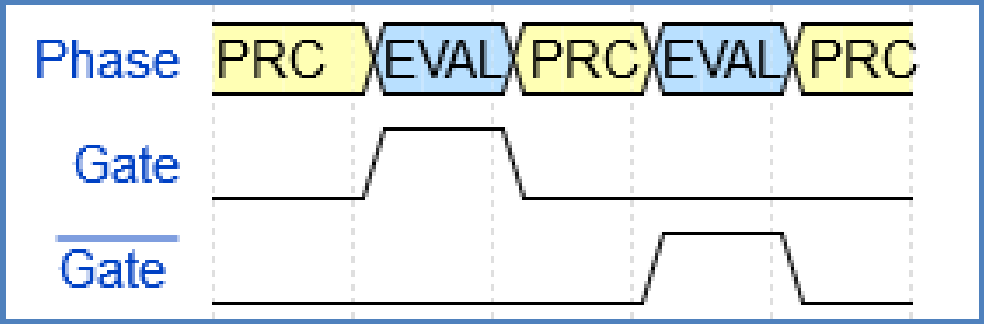
Precharge Logic

- Alternates between Precharge and logic value
- Precharge and evaluation phase



Dual-Rail Precharge Logic

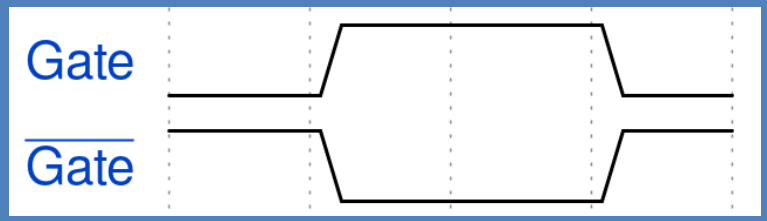
- Differential encoding
  - Precharge phase: 00 or 11
  - Evaluation phase: 01 or 10
- One transition per phase



Dual-Rail-Precharge (DRP)

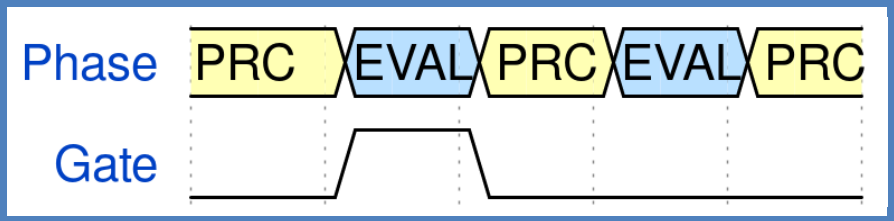
Dual-Rail Logic

- Differential encoding
- Valid values: 10 or 01
- No Inverter



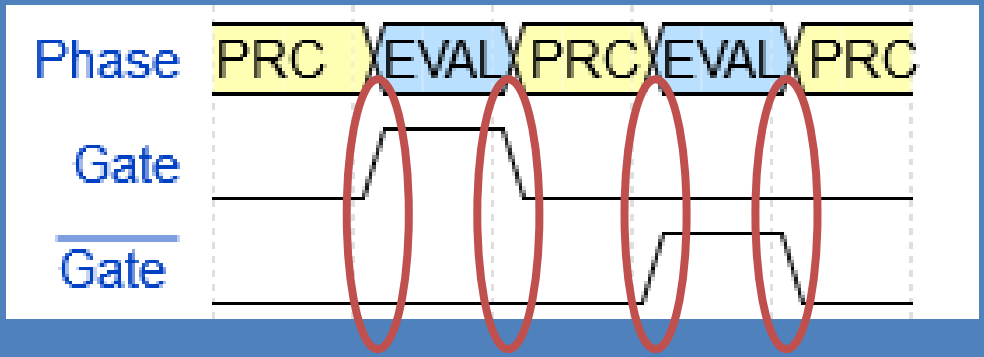
Precharge Logic

- Alternates between Precharge and logic value
- Precharge and evaluation phase



Dual-Rail Precharge Logic

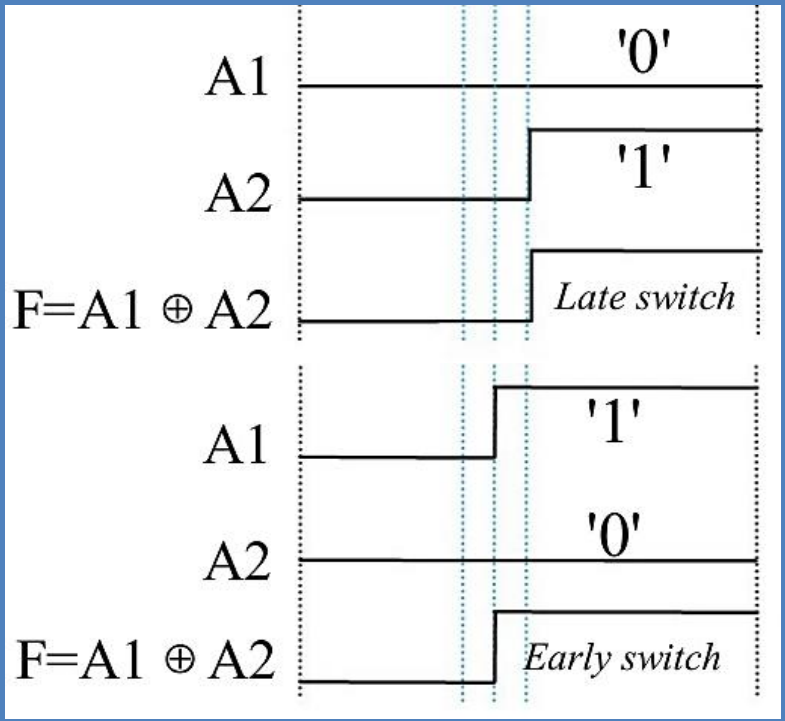
- Differential encoding
  - Precharge phase: 00 or 11
  - Evaluation phase: 01 or 10
- One transition per phase



Pitfalls

Early Evaluation

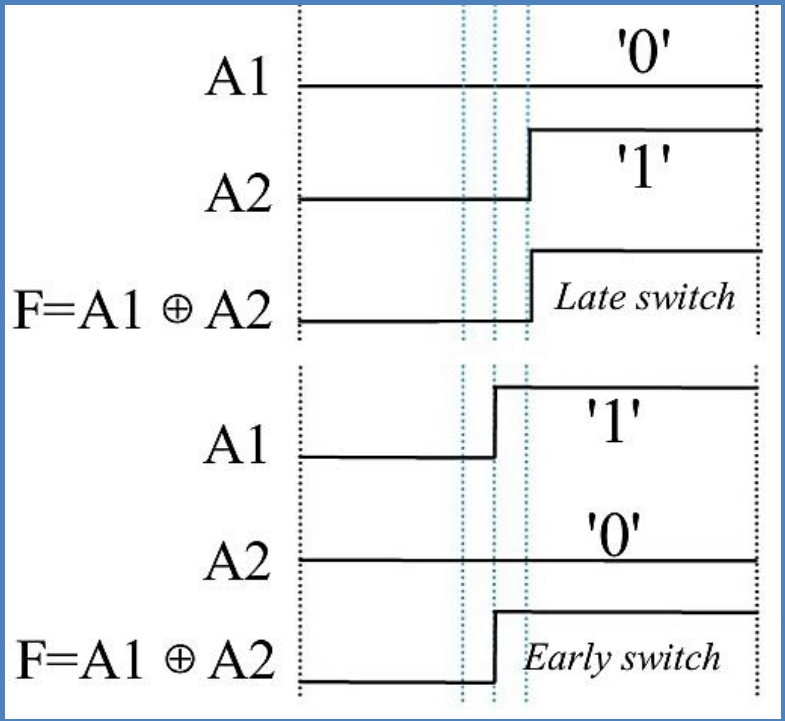
- Transition based on the arriving signals



Pitfalls

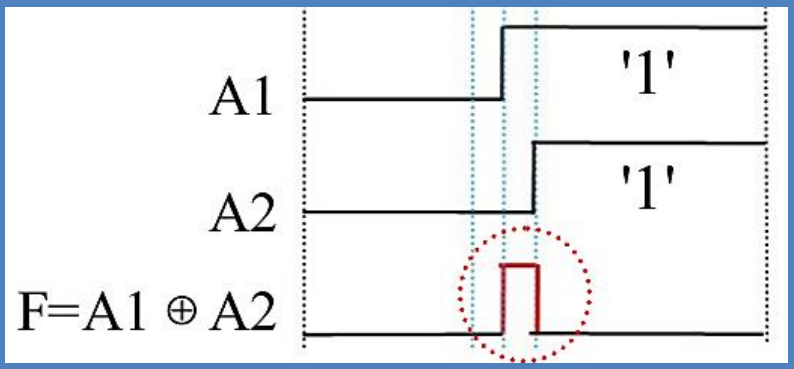
Early Evaluation

- Transition based on the arriving signals



Glitches

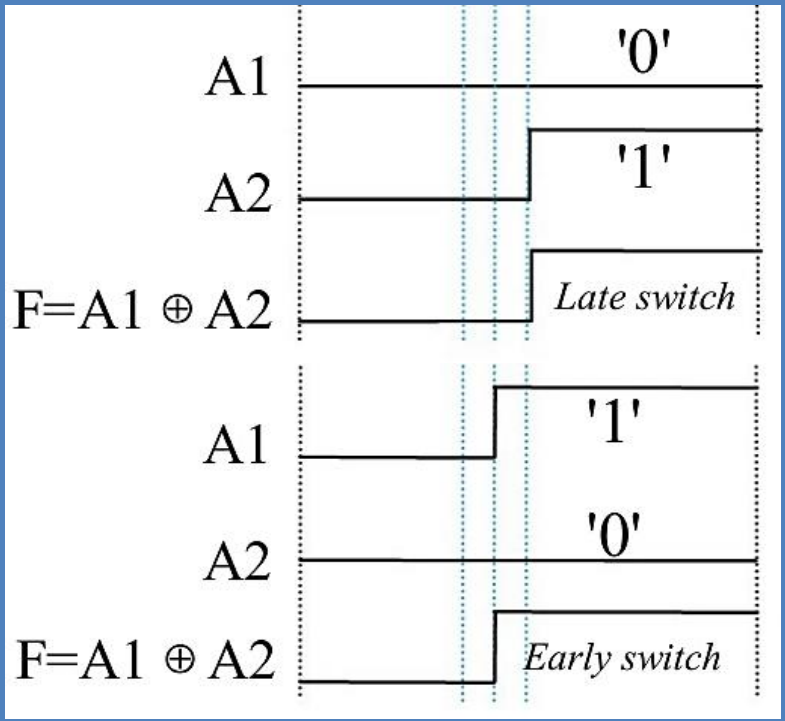
- Undesired transition



Pitfalls

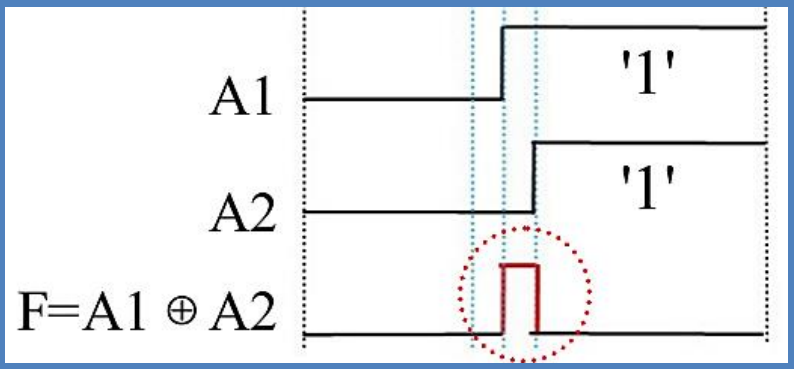
Early Evaluation

- Transition based on the arriving signals



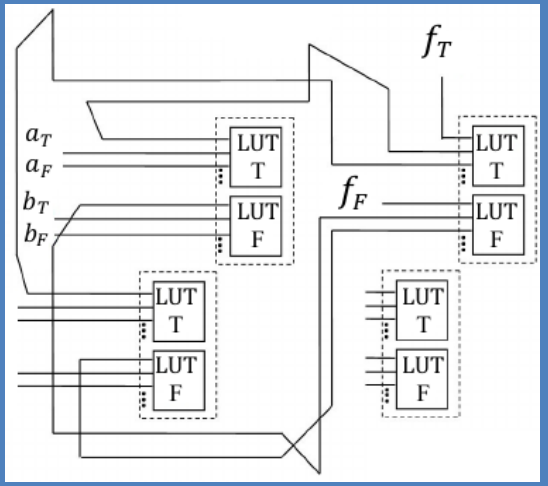
Glitches

- Undesired transition



Routing

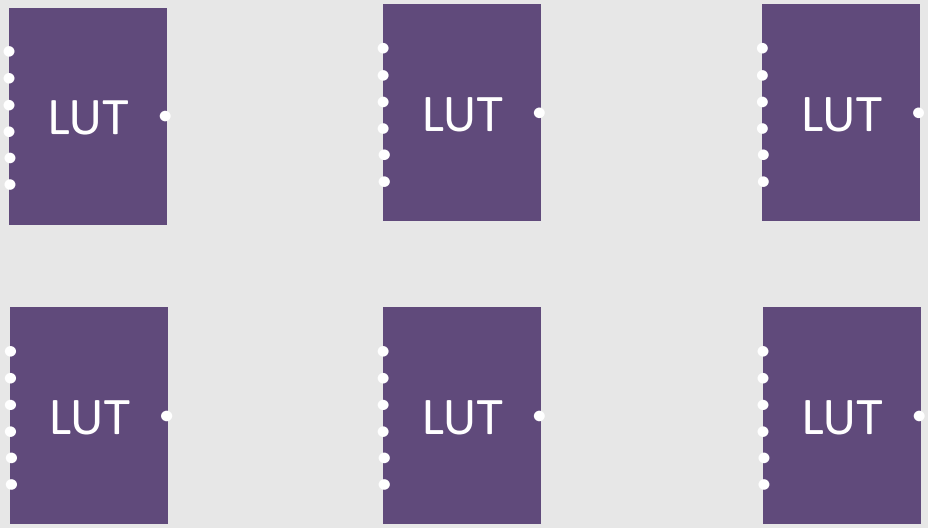
- Different capacities



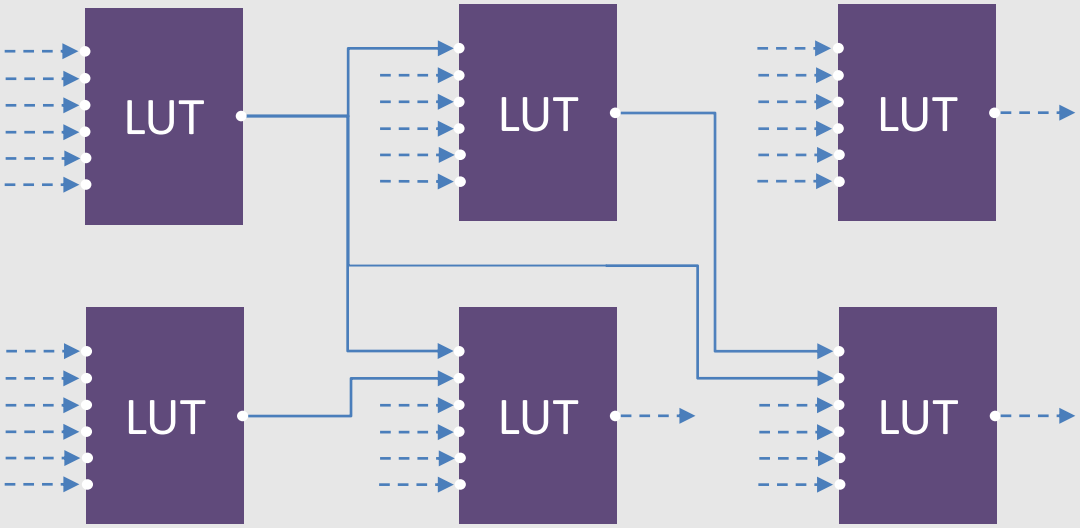
Pictures Soruce: Wei He, et.al.: A Precharge-Absorbed DPL Logic for Reducing Early Propagation Effects on FPGA Implementations

Idea of Our Advanced Hiding Schemes

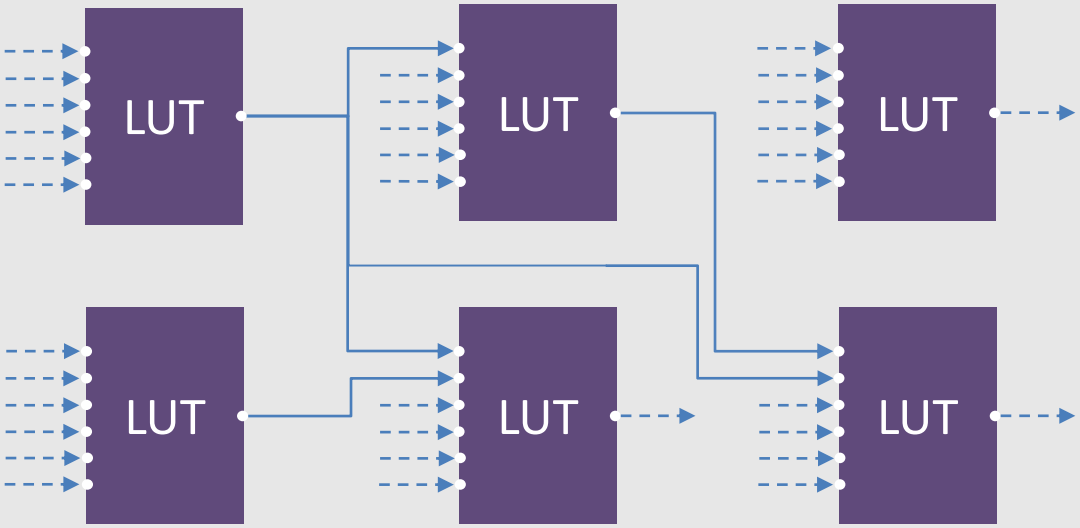
Idea of Our Advanced Hiding Schemes



Idea of Our Advanced Hiding Schemes

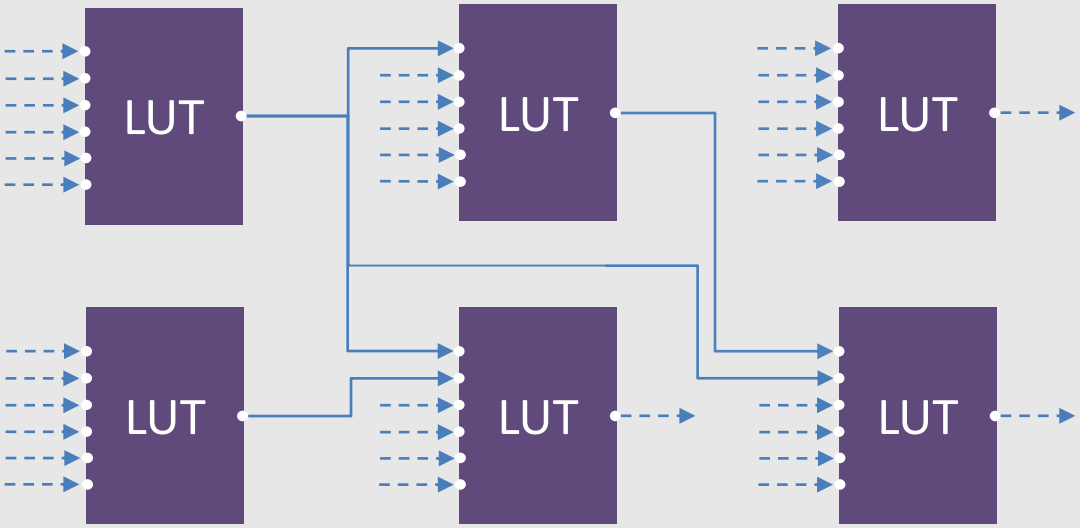


Idea of Our Advanced Hiding Schemes



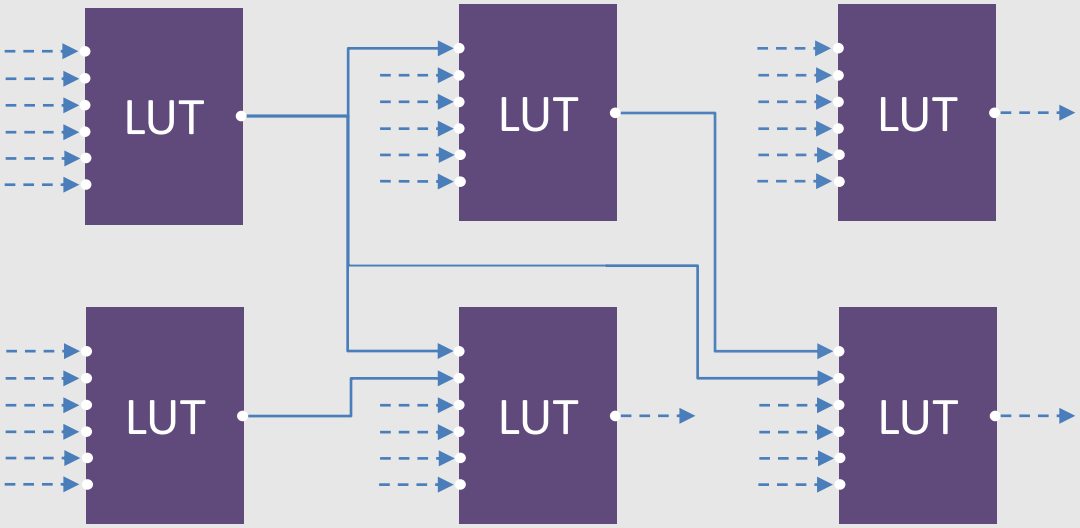
- Early evaluation, glitches

Idea of Our Advanced Hiding Schemes



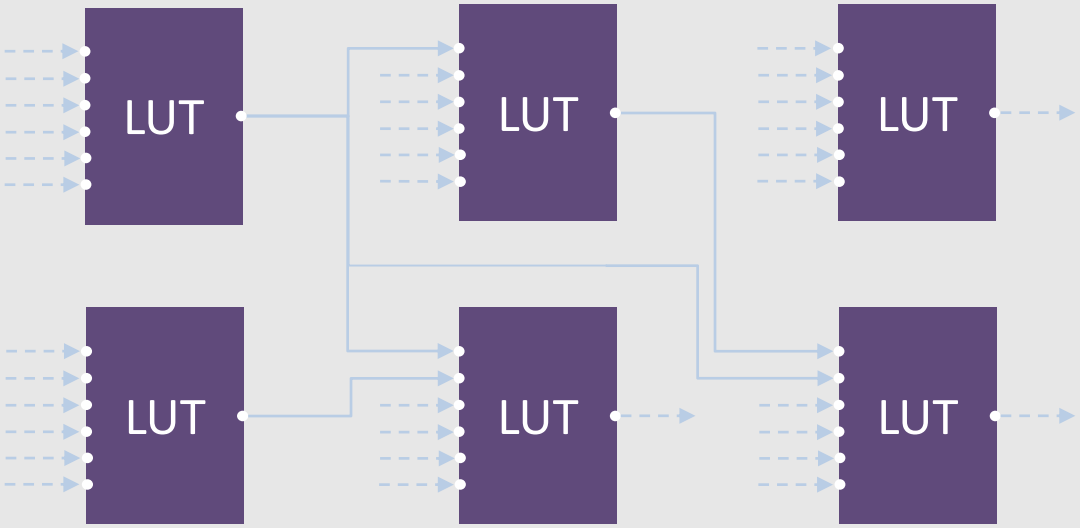
- Early evaluation, glitches
- I/O-Handling

Idea of Our Advanced Hiding Schemes



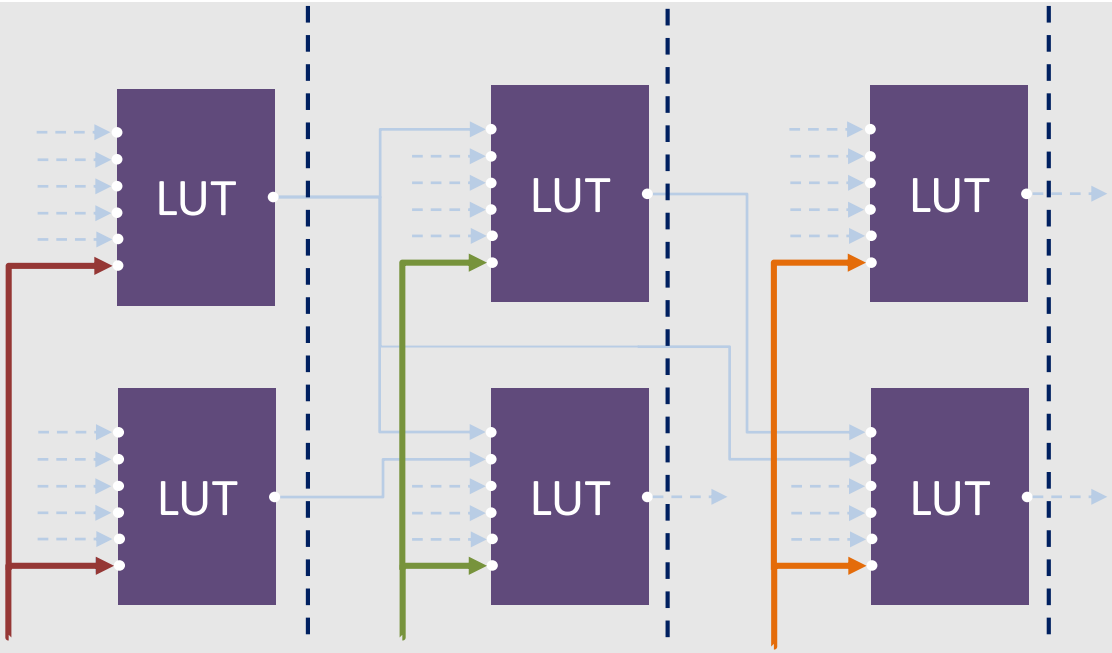
- Early evaluation, glitches
- I/O-Handling
- Consider routing

Idea of Our Advanced Hiding Schemes



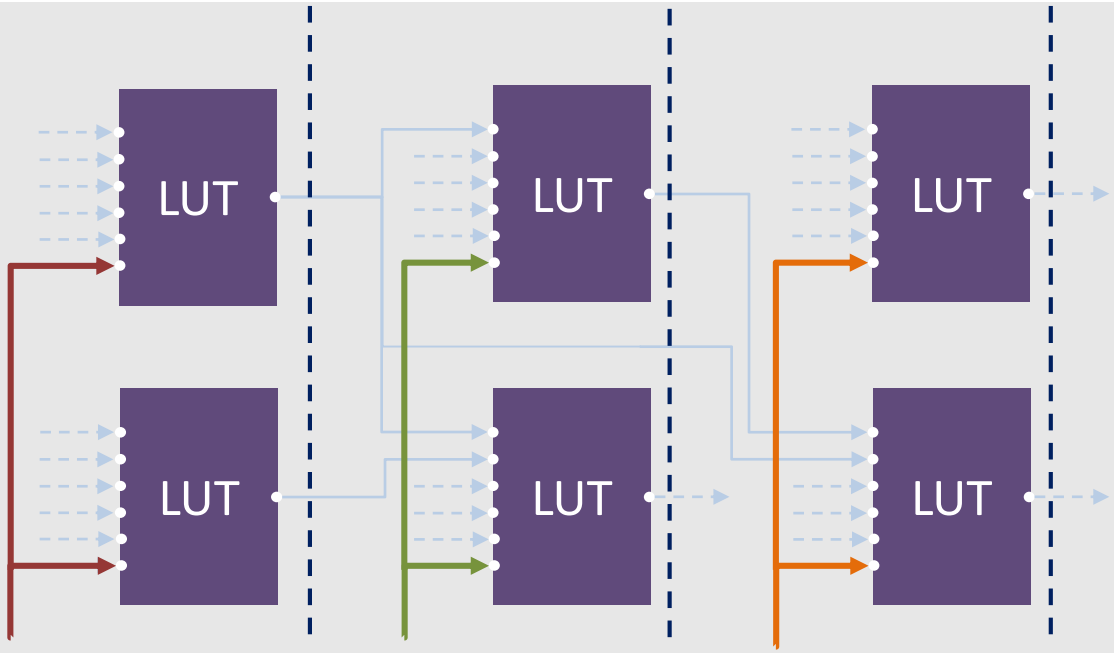
- Early evaluation, glitches
- I/O-Handling
- Consider routing

Idea of Our Advanced Hiding Schemes



- Early evaluation, glitches
  active signal
- I/O-Handling
- Consider routing

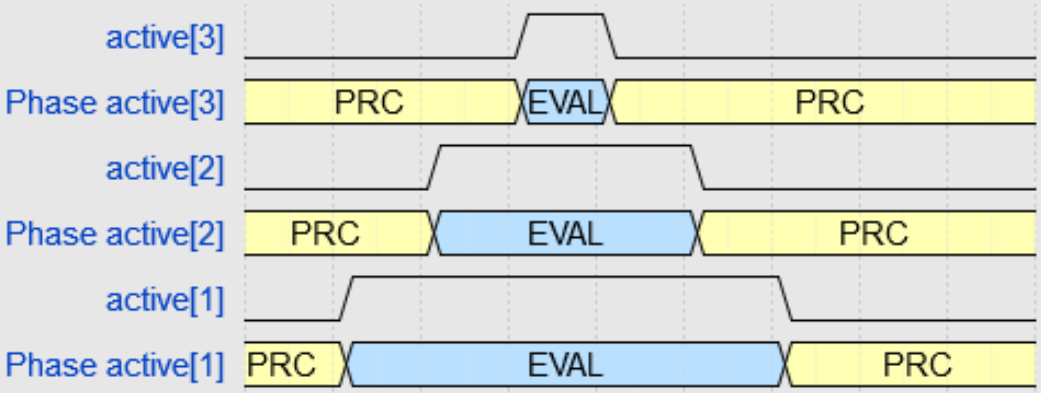
Idea of Our Advanced Hiding Schemes



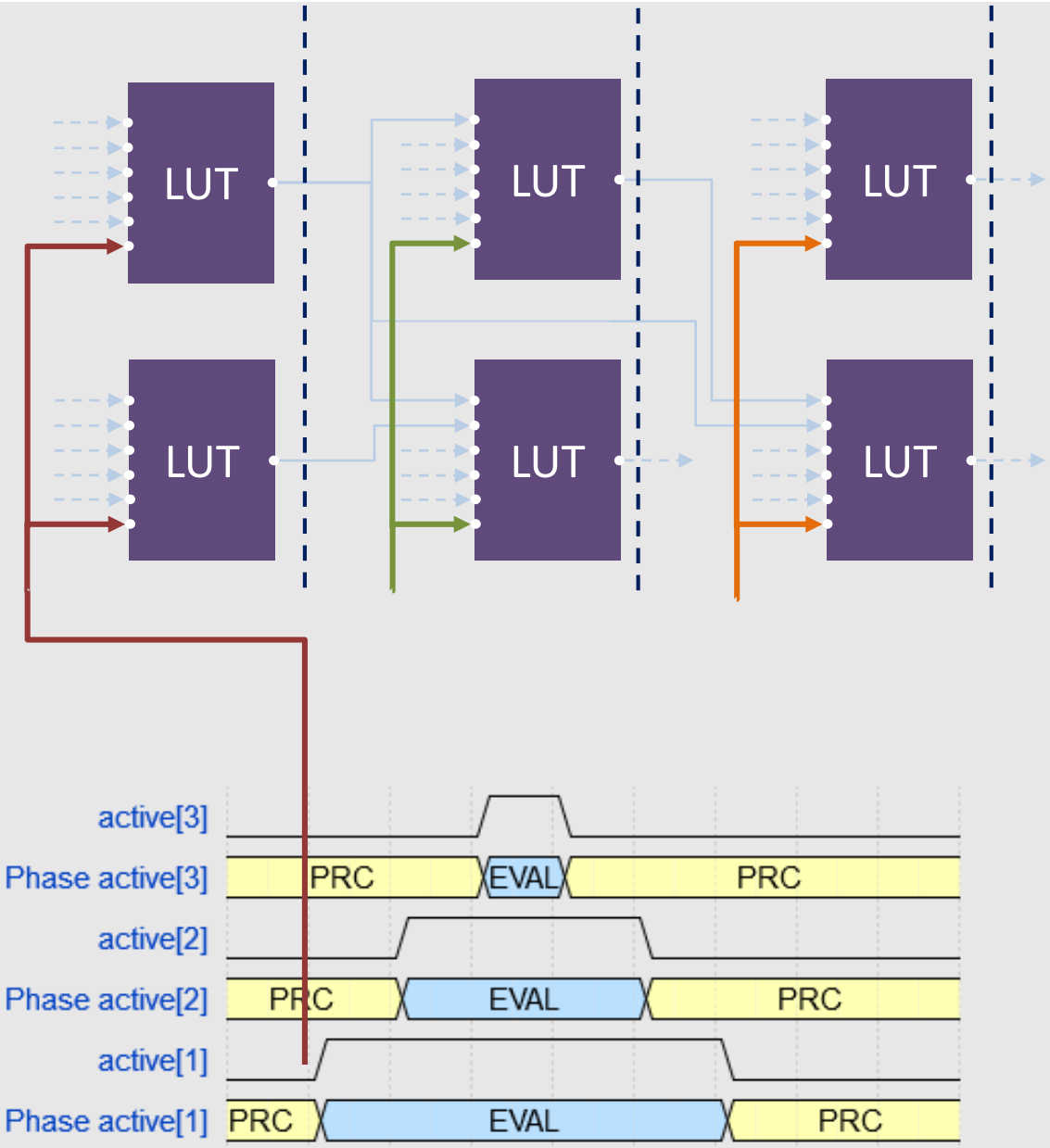
- Early evaluation, glitches
  active signal one after another

I/O-Handling

- Consider routing



Idea of Our Advanced Hiding Schemes

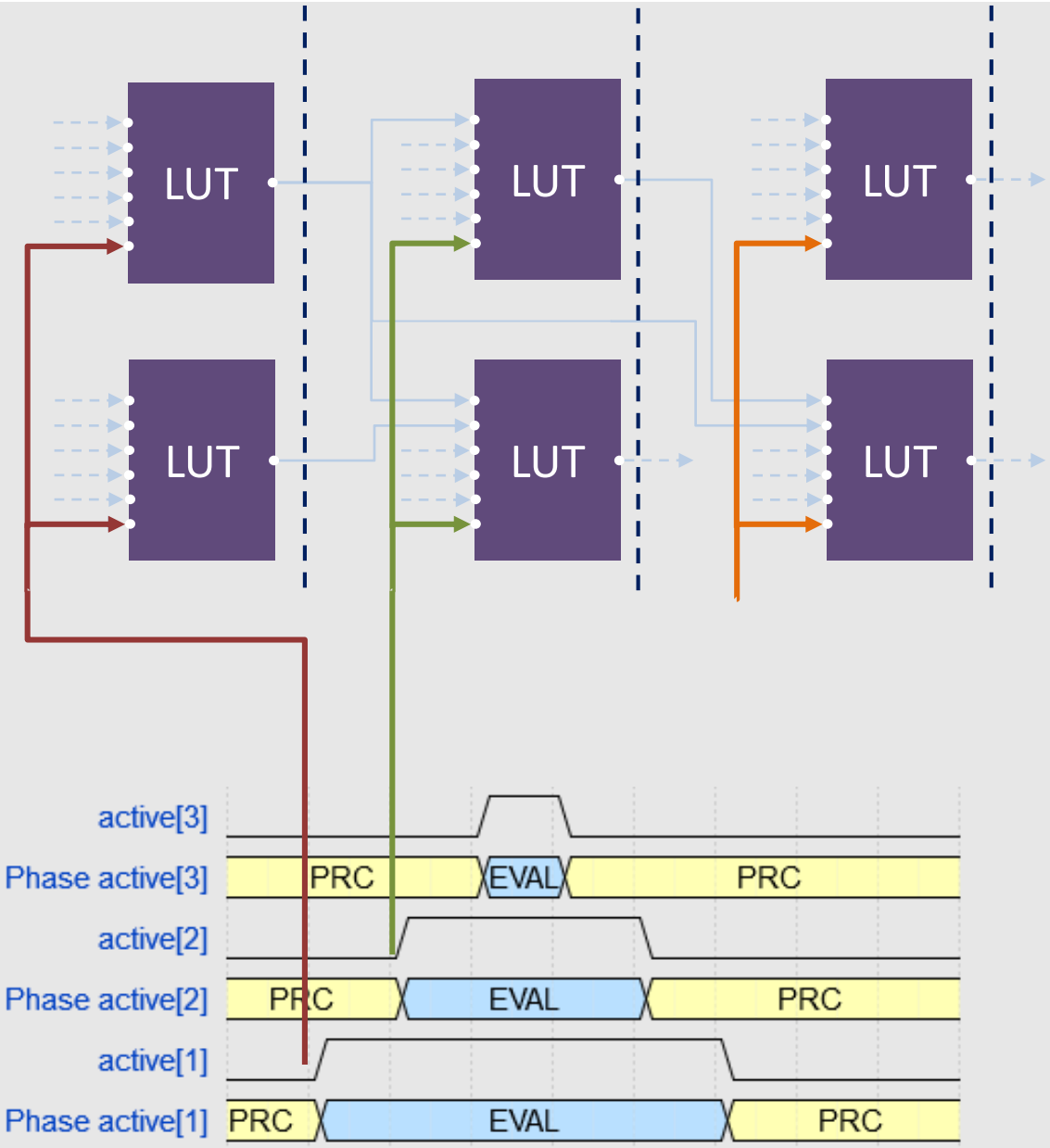


- Early evaluation, glitches
  active signal one after another

I/O-Handling

- Consider routing

Idea of Our Advanced Hiding Schemes

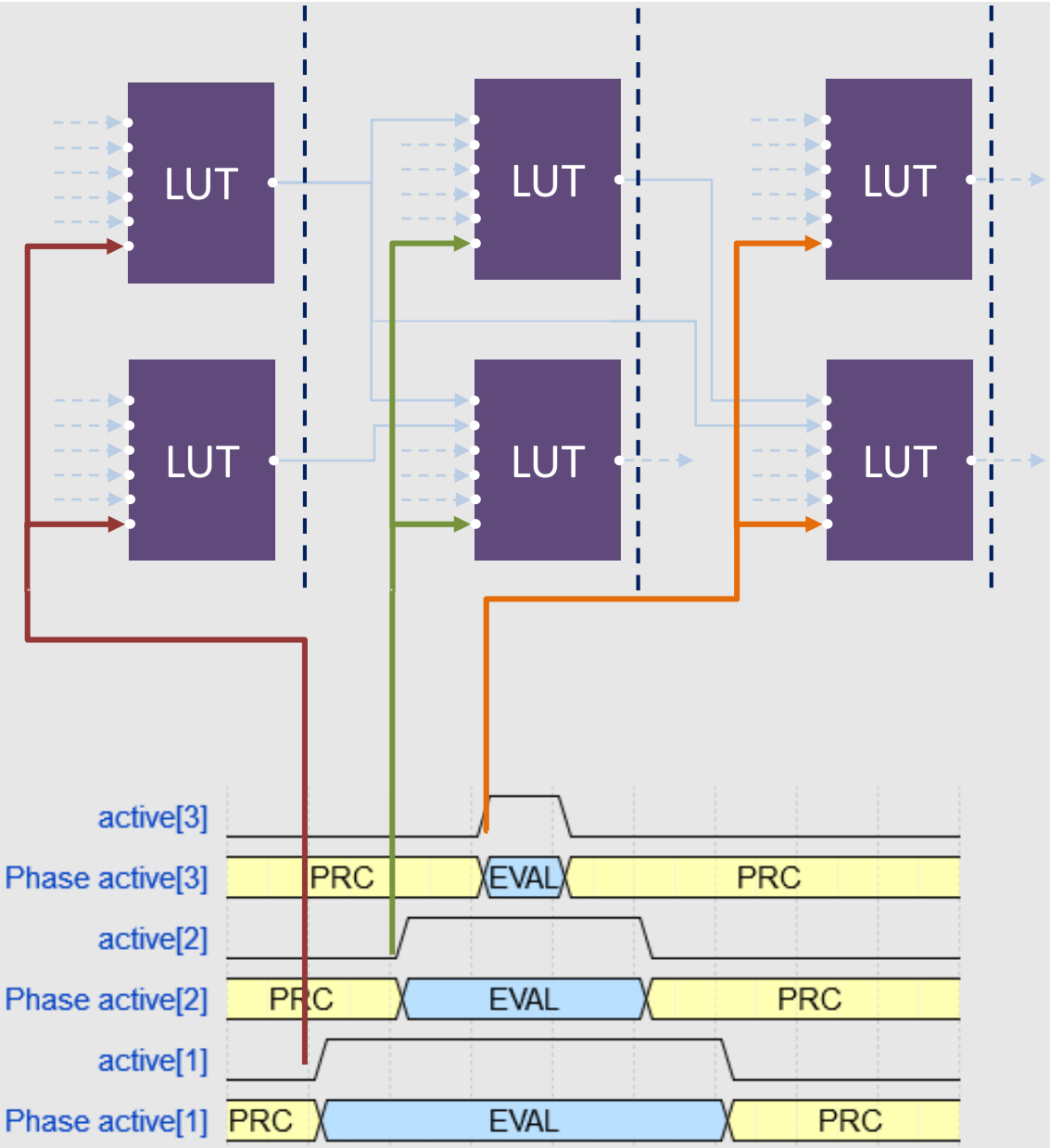


- Early evaluation, glitches
  active signal one after another

I/O-Handling

- Consider routing

Idea of Our Advanced Hiding Schemes

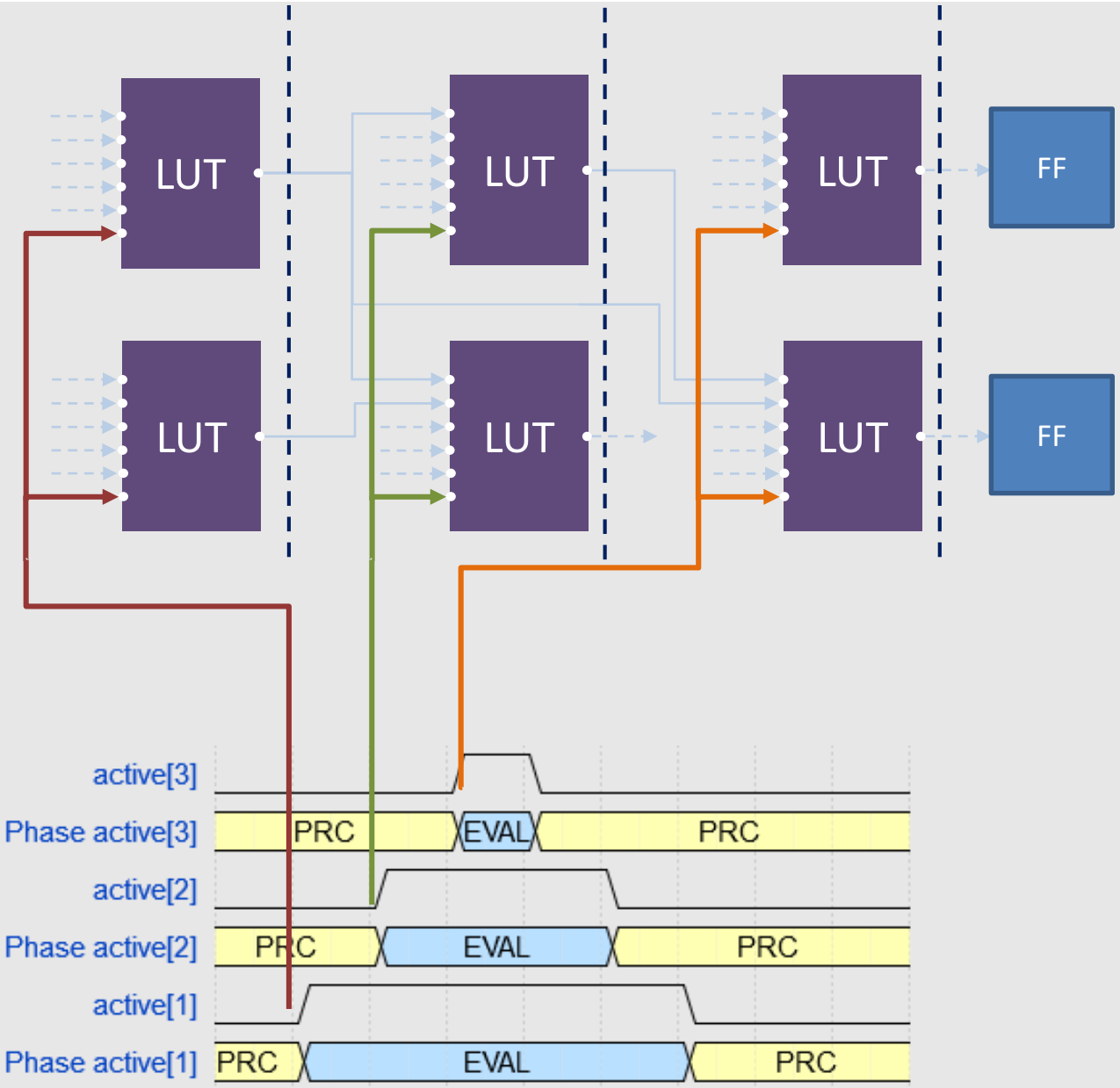


- Early evaluation, glitches
  active signal one after another

I/O-Handling

- Consider routing

Idea of Our Advanced Hiding Schemes

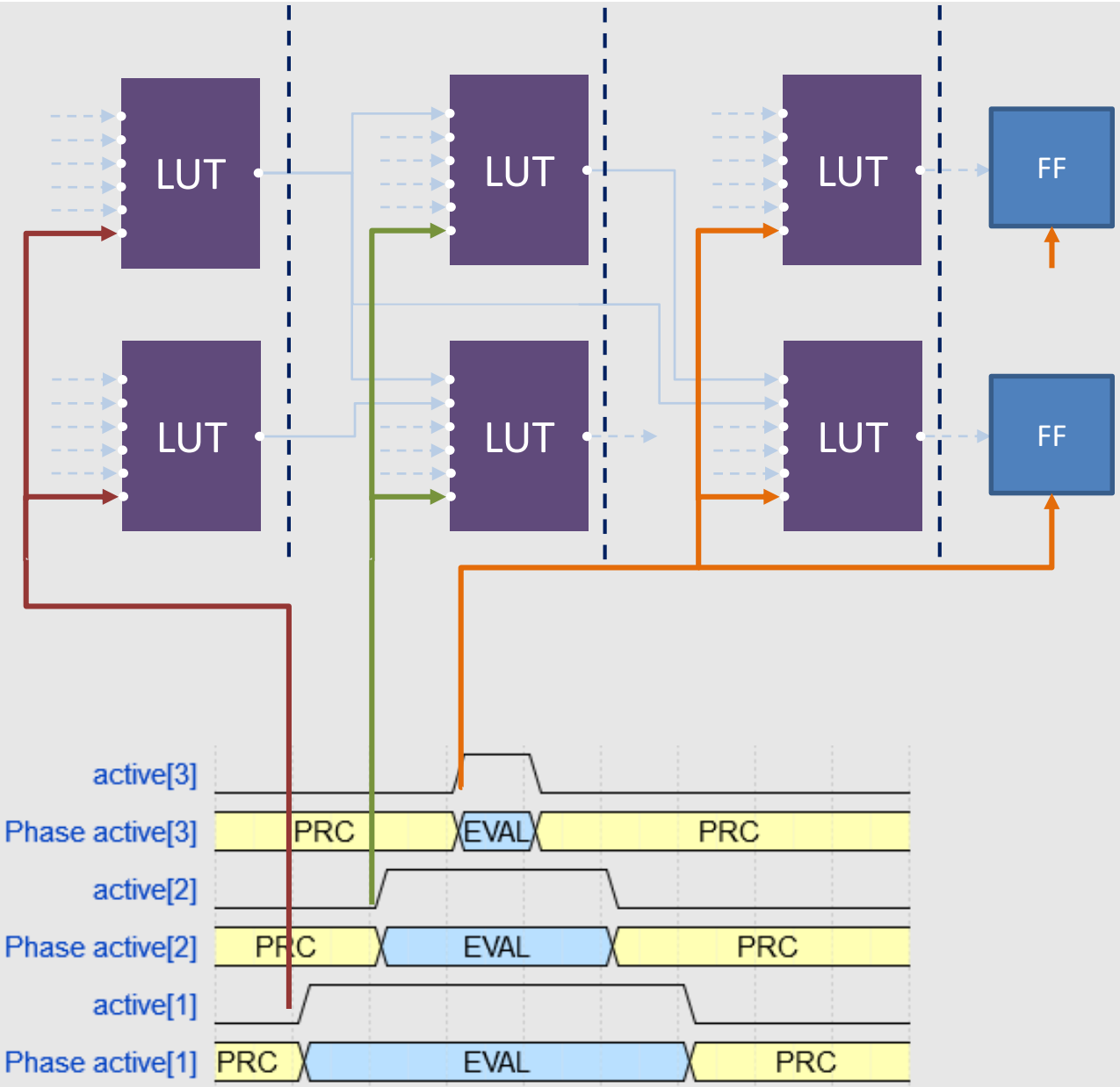


- Early evaluation, glitches
  active signal one after another

I/O-Handling
  use FF/latches

Consider routing

Idea of Our Advanced Hiding Schemes

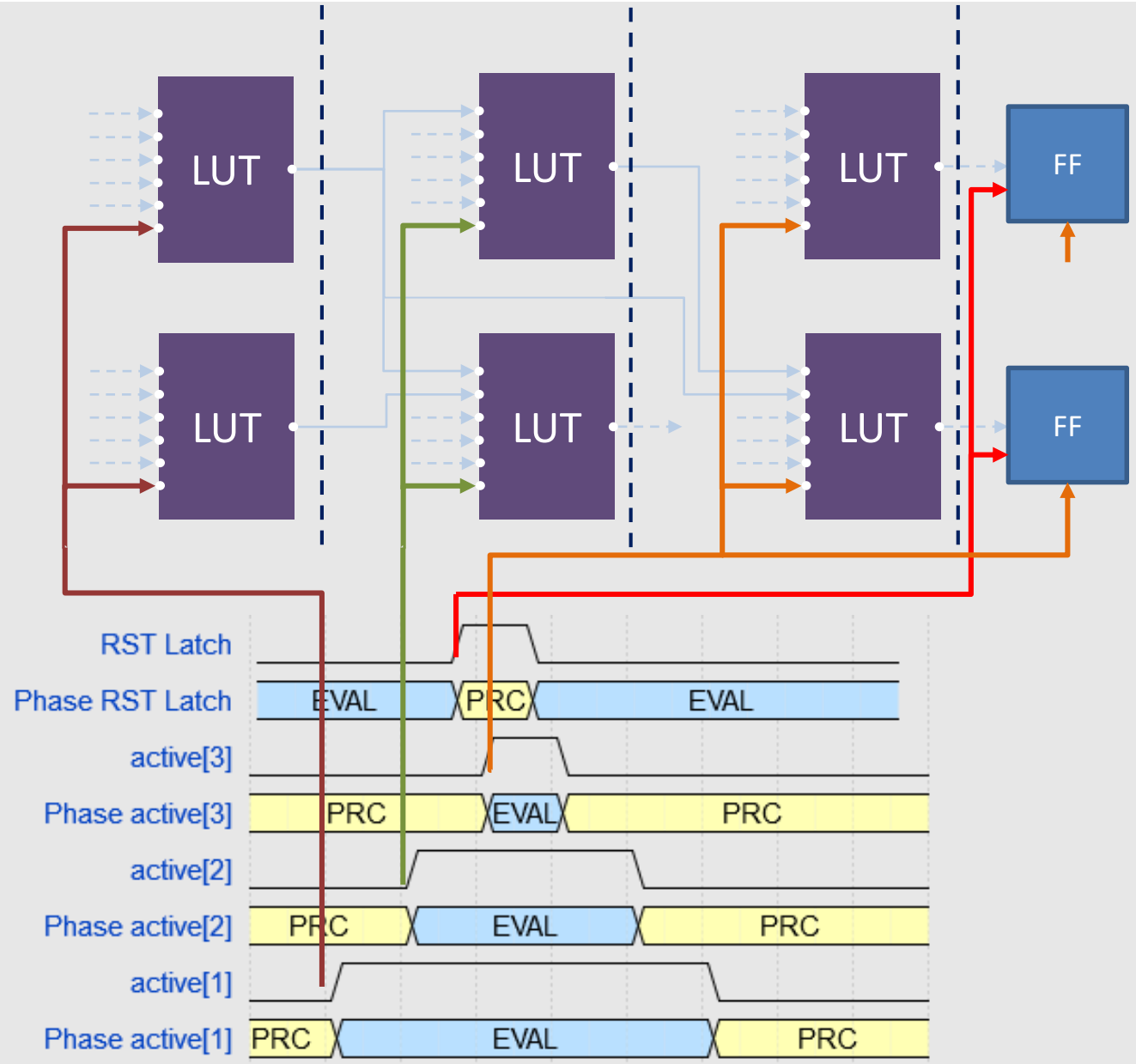


- Early evaluation, glitches
  active signal one after another

I/O-Handling
  use FF/latches

Consider routing

Idea of Our Advanced Hiding Schemes

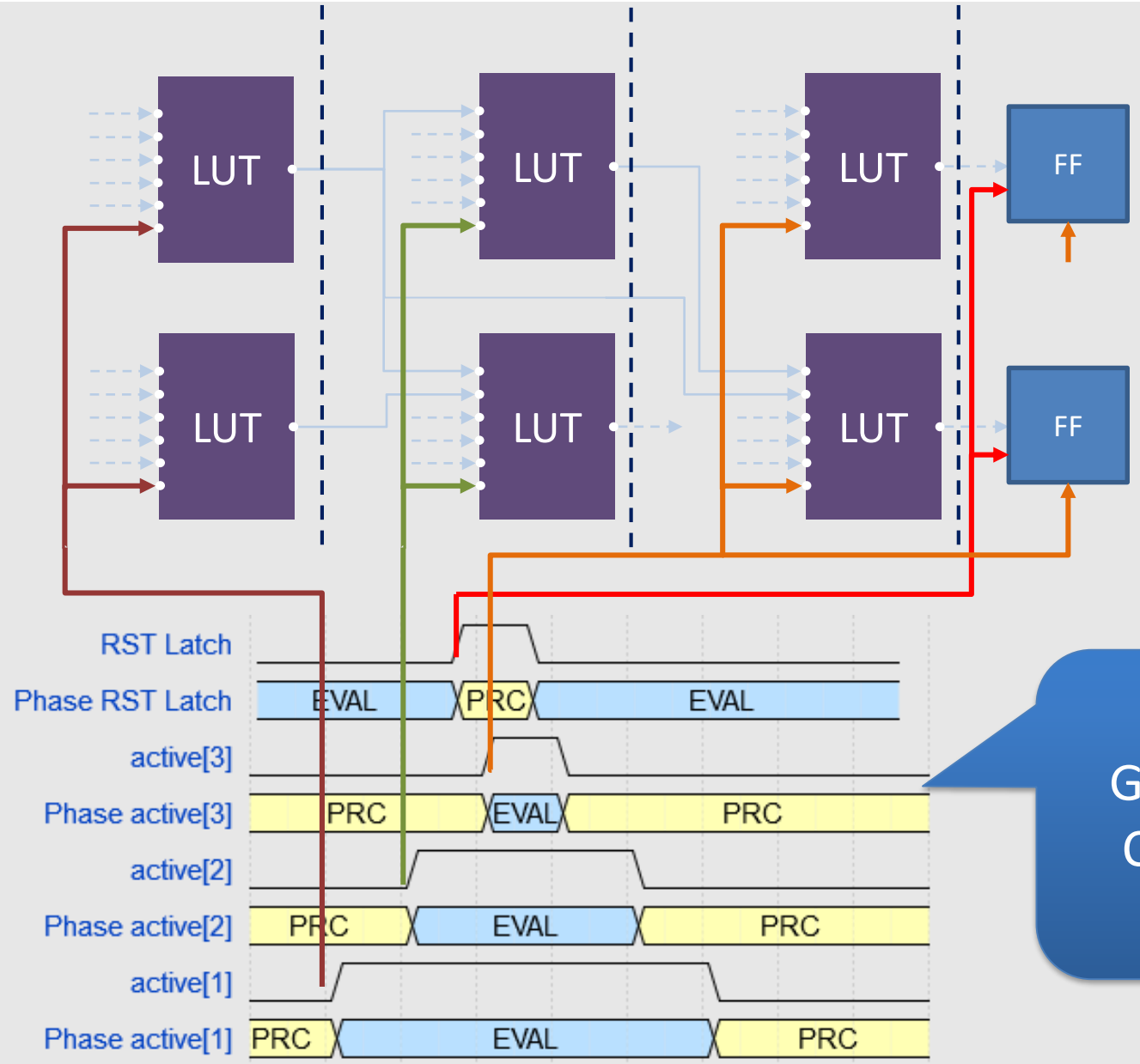


- Early evaluation, glitches
  active signal one after another

I/O-Handling
  use FF/latches

Consider routing

Idea of Our Advanced Hiding Schemes



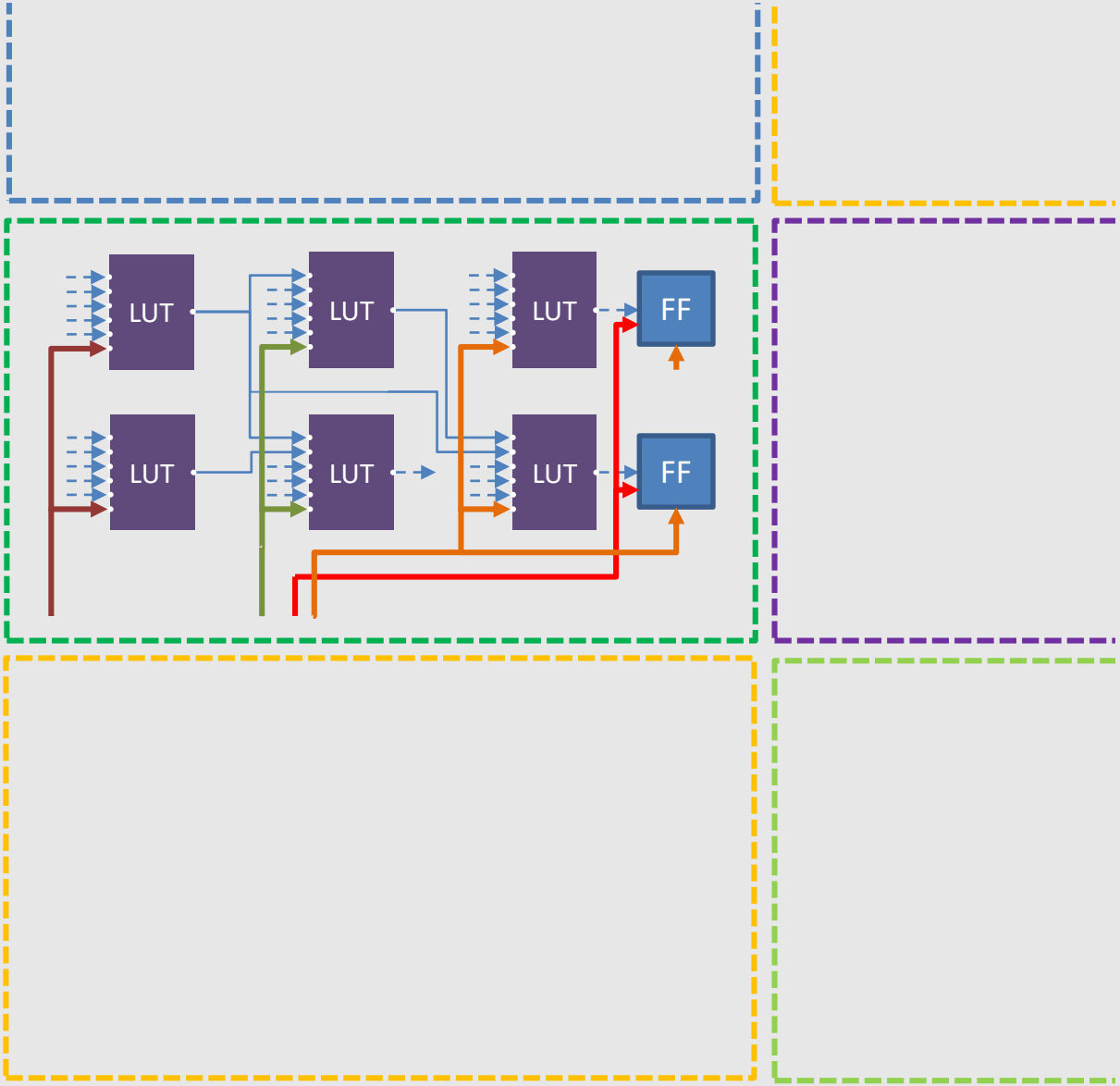
- Early evaluation, glitches
  active signal one after another

I/O-Handling
  use FF/latches

Consider routing

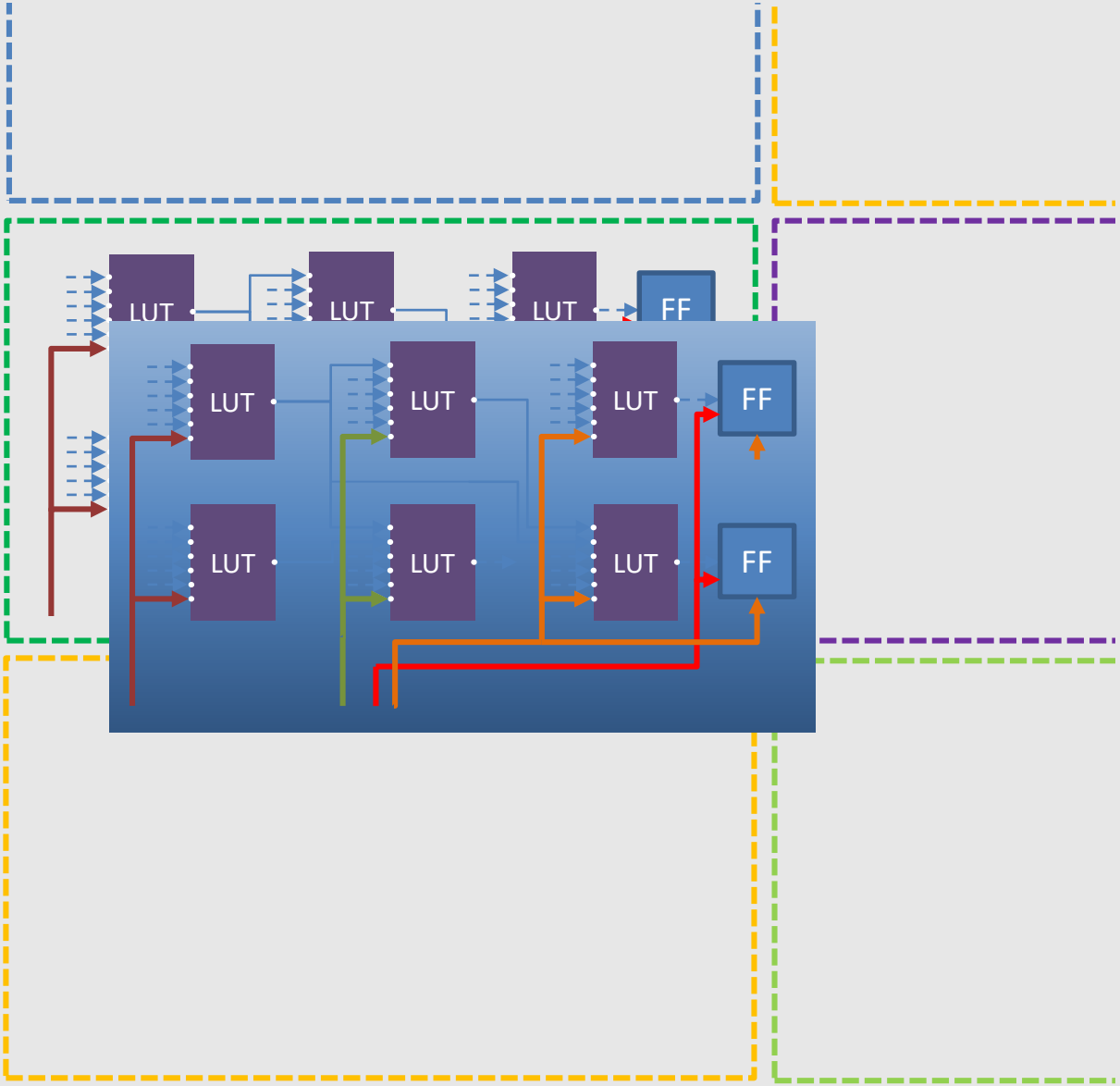
Generate by Mixed-Mode Clock Manager (MMCM)

Idea of Our Advanced Hiding Schemes



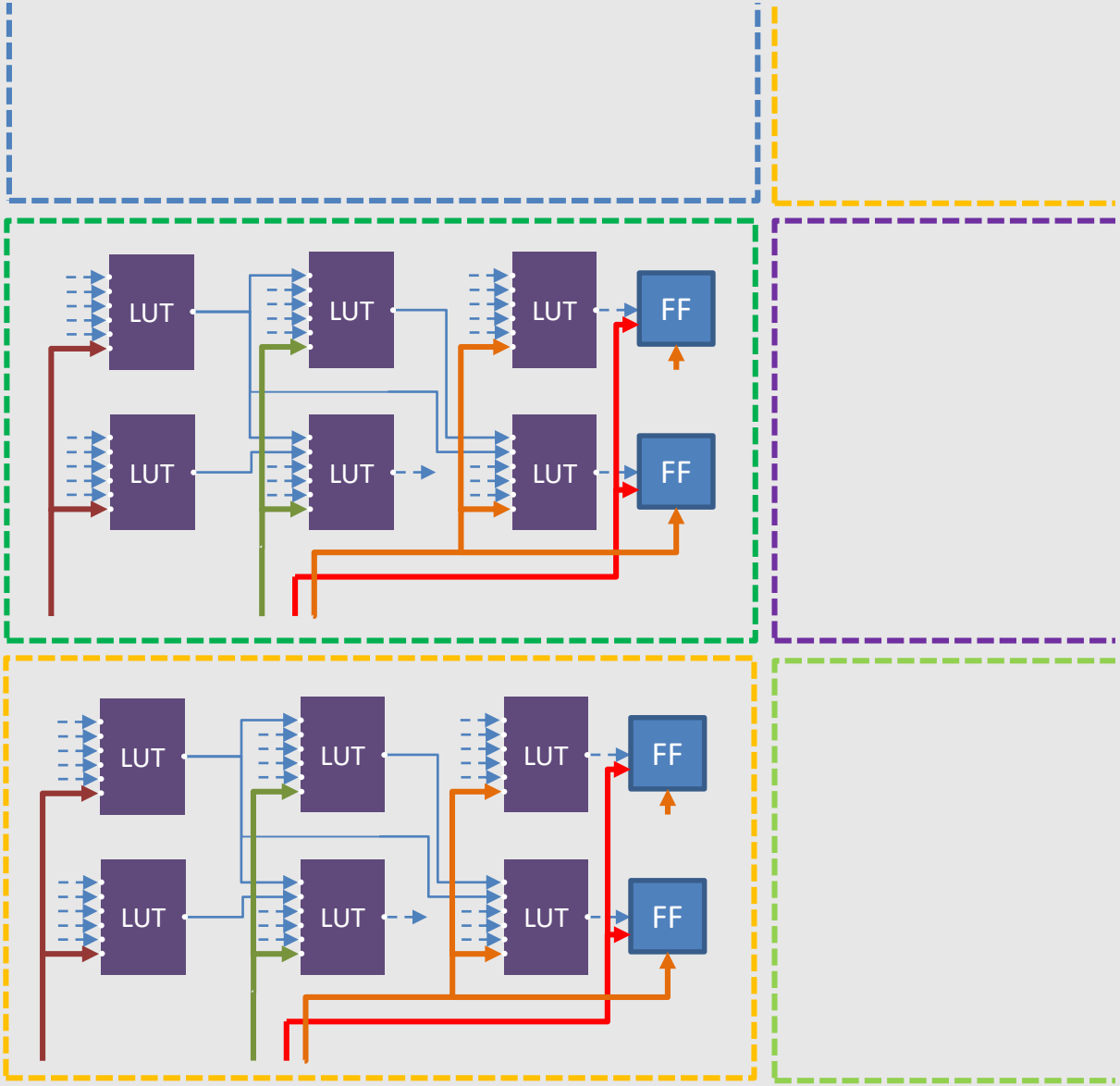
- Early evaluation, glitches
  active signal one after another
- I/O-Handling
  use FF/latches
- Consider routing
  duplication
  1. Place&Route

Idea of Our Advanced Hiding Schemes



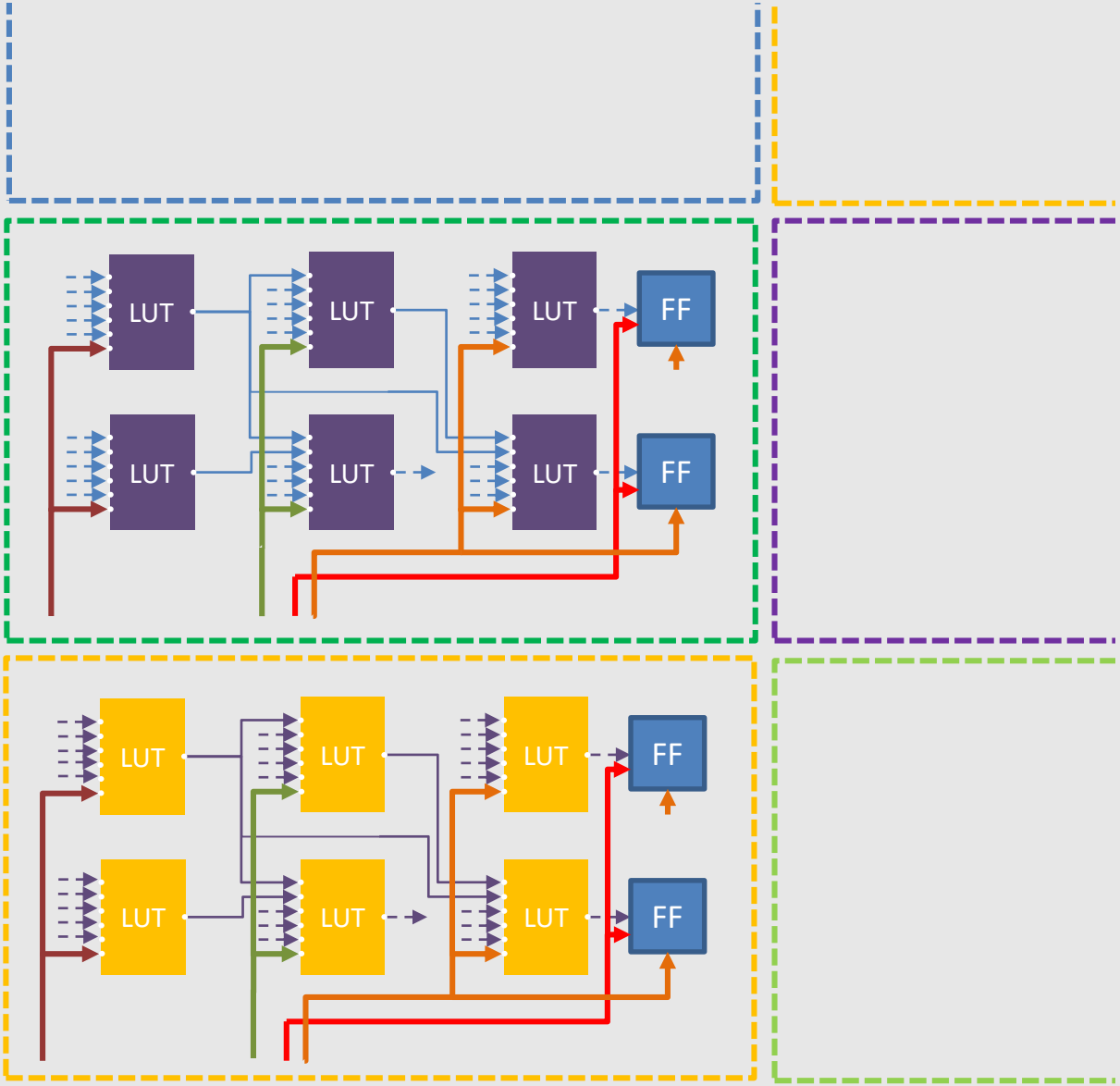
- Early evaluation, glitches
  active signal one after another
- I/O-Handling
  use FF/latches
- Consider routing
  duplication
  1. Place&Route
  2. Clone

Idea of Our Advanced Hiding Schemes



- Early evaluation, glitches
  active signal one after another
- I/O-Handling
  use FF/latches
- Consider routing *duplication*
  1. Place&Route
  2. Clone
  3. Place clone

Idea of Our Advanced Hiding Schemes



- Early evaluation, glitches
  active signal one after another
- I/O-Handling
  use FF/latches
- Consider routing *duplication*
  1. Place&Route
  2. Clone
  3. Place clone
  4. Invert

→ Equal routing

Side-Channel Evaluation

Measurement Setup

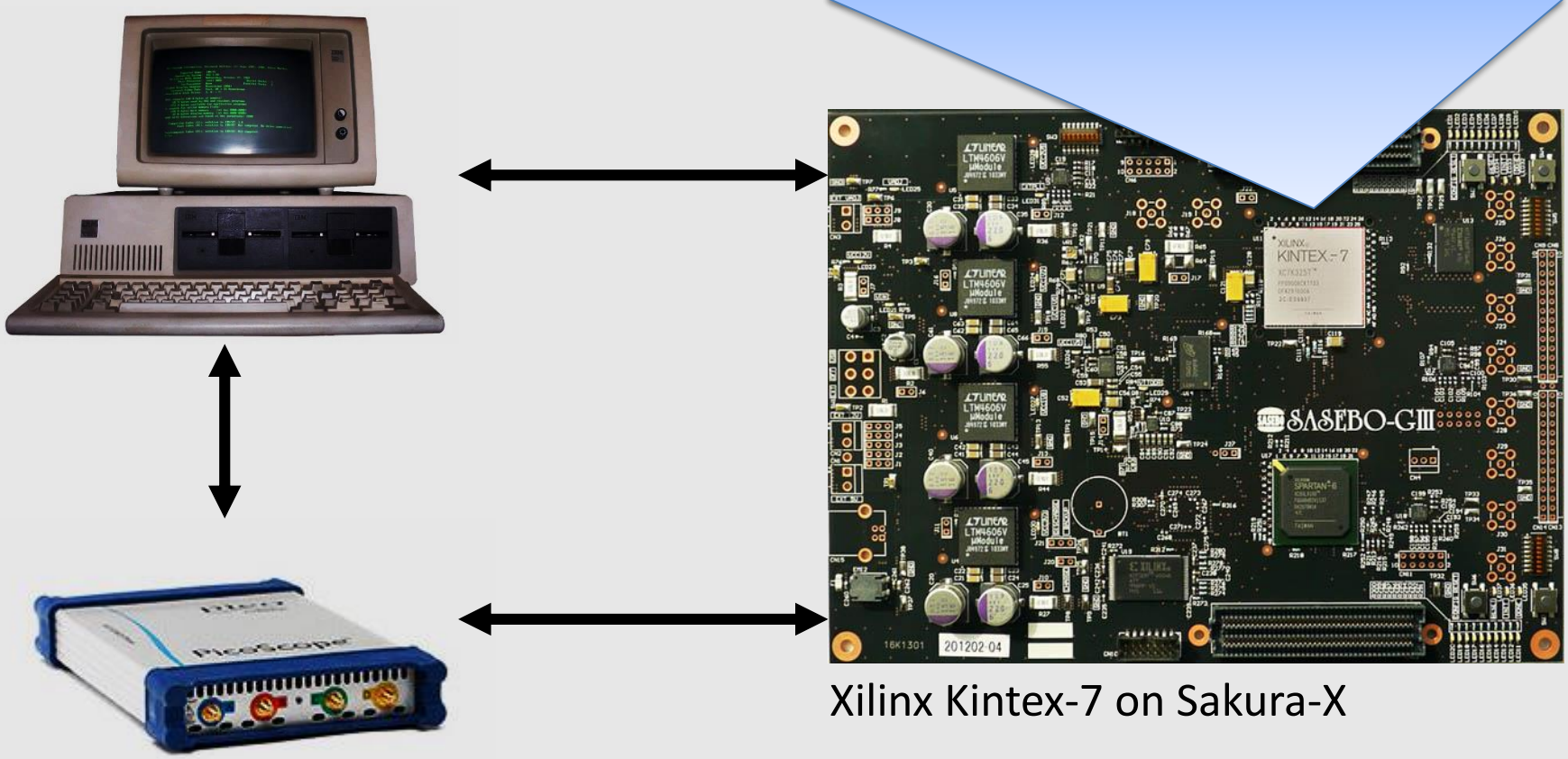
Round based AES-128

Xilinx Kintex-7 on Sakura-X

Source Sakura in Specification Guide and http://satoh.cs.uec.ac.jp/SAKURA/hardware/SAKURA-X.html
Source Picoscope: https://www.picotech.com/oscilloscope/6407/high-speed-digitizer
Source IBM: https://commons.wikimedia.org/wiki/File:IBM_PC_5150.jpg User Zarex

Side-Channel Evaluation

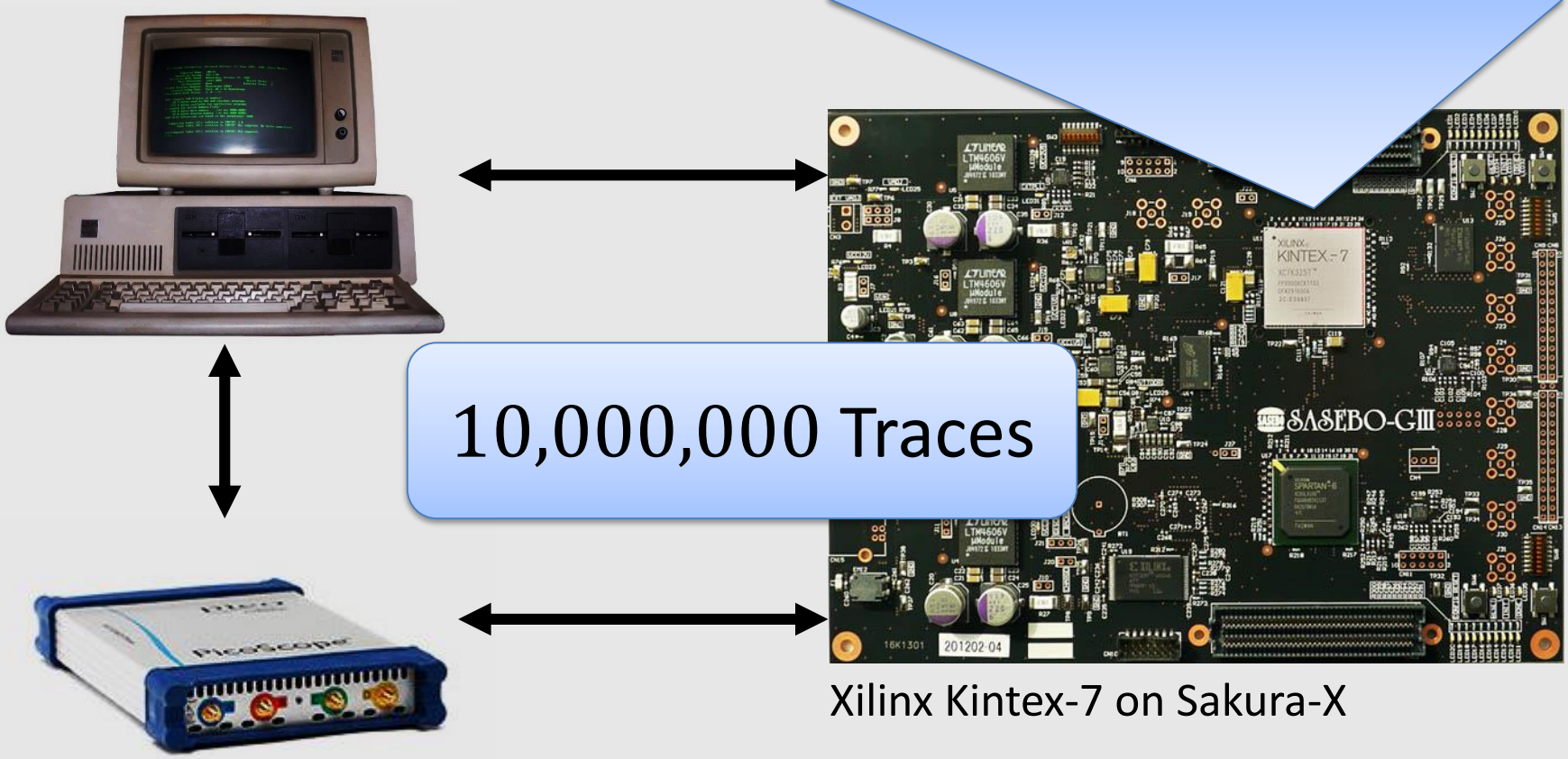
Measurement Setup



Source Sakura in Specification Guide and http://satoh.cs.uec.ac.jp/SAKURA/hardware/SAKURA-X.html
Source Picoscope: https://www.picotech.com/oscilloscope/6407/high-speed-digitizer
Source IBM: https://commons.wikimedia.org/wiki/File:IBM_PC_5150.jpg User Zarex

Side-Channel Evaluation

Measurement Setup



Source Sakura in Specification Guide and http://satoh.cs.uec.ac.jp/SAKURA/hardware/SAKURA-X.html
Source Picoscope: https://www.picotech.com/oscilloscope/6407/high-speed-digitizer
Source IBM: https://commons.wikimedia.org/wiki/File:IBM_PC_5150.jpg User Zarex

Comparison

	SafeDRP	
	Doubled	Single
LUTs	3712	1856
Register	1276	638
Slices	1296	648
Latency[a]	11	
Pipeline	0	
Throughput[b]	116	

[a] clock cycles
[b] MBit/s @ 10 MHz

[17] A. Moradi and A. Wild. Assessment of Hiding the Higher-Order Leakages in Hardware - what are the achievements versus overheads? In CHES 2015
[30] A. Wild, et.al. GliFreD: Glitch-Free Duplication – Towards Power-Equalized Circuits on FPGAs. IEEE Transactions on Computers, 2017.

Comparison

	SafeDRP		Improved GliFreD [30]		GliFreD [17]		Plain
	Doubled	Single	Doubled	Single	Doubled	Single	
LUTs	3712	1856	3466	1733	3466	1733	1262
Register	1276	638	11360	5680	22080	11040	256
Slices	1296	648	11638	5819	15502	7751	392
Latency[a]	11		154		308		11
Pipeline	0		14		14		0
Throughput[b]	116		116		58		116

[a] clock cycles
[b] MBit/s @ 10 MHz

[17] A. Moradi and A. Wild. Assessment of Hiding the Higher-Order Leakages in Hardware - what are the achievements versus overheads? In CHES 2015
[30] A. Wild, et.al. GliFreD: Glitch-Free Duplication – Towards Power-Equalized Circuits on FPGAs. IEEE Transactions on Computers, 2017.

Comparison

	SafeDRP		Improved GliFreD [30]		GliFreD [17]		Plain
	Doubled	Single	Doubled	Single	Doubled	Single	
LUTs	3712	1856	3466	1733	3466	1733	1262
Register	1276	638	11360	5680	22080	11040	256
Slices	1296	648	11638	5819	15502	7751	392
Latency[a]	11		154		308		11
Pipeline	0		14		14		0
Throughput[b]	116		116		58		116

[a] clock cycles
[b] MBit/s @ 10 MHz

[17] A. Moradi and A. Wild. Assessment of Hiding the Higher-Order Leakages in Hardware - what are the achievements versus overheads? In CHES 2015
[30] A. Wild, et.al. GliFreD: Glitch-Free Duplication – Towards Power-Equalized Circuits on FPGAs. IEEE Transactions on Computers, 2017.

Comparison

	SafeDRP		Improved GliFreD [30]		GliFreD [17]		Plain
	Doubled	Single	Doubled	Single	Doubled	Single	
LUTs	3712	1856	3466	1733	3466	1733	1262
Register	1276	638	11360	5680	22080	11040	256
Slices	1296	648	11638	5819	15502	7751	392
Latency[a]	11		154		308		11
Pipeline	0		14		14		0
Throughput[b]	116		116		58		116

[a] clock cycles
[b] MBit/s @ 10 MHz

- Reduced FF utilization
  - 8.9 Improved GliFreD

[17] A. Moradi and A. Wild. Assessment of Hiding the Higher-Order Leakages in Hardware - what are the achievements versus overheads? In CHES 2015
[30] A. Wild, et.al. GliFreD: Glitch-Free Duplication – Towards Power-Equalized Circuits on FPGAs. IEEE Transactions on Computers, 2017.

Comparison

	SafeDRP		Improved GliFreD [30]		GliFreD [17]		Plain
	Doubled	Single	Doubled	Single	Doubled	Single	
LUTs	3712	1856	3466	1733	3466	1733	1262
Register	1276	638	11360	5680	22080	11040	256
Slices	1296	648	11638	5819	15502	7751	392
Latency[a]	11		154		308		11
Pipeline	0		14		14		0
Throughput[b]	116		116		58		116

[a] clock cycles
[b] MBit/s @ 10 MHz

- Reduced FF utilization
  - 8.9 Improved GliFreD
  - 17.3 GliFreD

[17] A. Moradi and A. Wild. Assessment of Hiding the Higher-Order Leakages in Hardware - what are the achievements versus overheads? In CHES 2015
[30] A. Wild, et.al. GliFreD: Glitch-Free Duplication – Towards Power-Equalized Circuits on FPGAs. IEEE Transactions on Computers, 2017.

Comparison

	SafeDRP		Improved GliFreD [30]		GliFreD [17]		Plain
	Doubled	Single	Doubled	Single	Doubled	Single	
LUTs	3712	1856	3466	1733	3466	1733	1262
Register	1276	638	11360	5680	22080	11040	256
Slices	1296	648	11638	5819	15502	7751	392
Latency[a]	11		154		308		11
Pipeline	0		14		14		0
Throughput[b]	116		116		58		116

[a] clock cycles
[b] MBit/s @ 10 MHz

- Reduced FF utilization
  - 8.9 Improved GliFreD
  - 17.3 GliFreD

[17] A. Moradi and A. Wild. Assessment of Hiding the Higher-Order Leakages in Hardware - what are the achievements versus overheads? In CHES 2015
[30] A. Wild, et.al. GliFreD: Glitch-Free Duplication – Towards Power-Equalized Circuits on FPGAs. IEEE Transactions on Computers, 2017.

Comparison

	SafeDRP		Improved GliFreD [30]		GliFreD [17]		Plain
	Doubled	Single	Doubled	Single	Doubled	Single	
LUTs	3712	1856	3466	1733	3466	1733	1262
Register	1276	638	11360	5680	22080	11040	256
Slices	1296	648	11638	5819	15502	7751	392
Latency[a]	11		154		308		11
Pipeline	0		14		14		0
Throughput[b]	116		116		58		116

[a] clock cycles
[b] MBit/s @ 10 MHz

- Reduced FF utilization
  - 8.9 Improved GliFreD
  - 17.3 GliFreD

[17] A. Moradi and A. Wild. Assessment of Hiding the Higher-Order Leakages in Hardware - what are the achievements versus overheads? In CHES 2015
[30] A. Wild, et.al. GliFreD: Glitch-Free Duplication – Towards Power-Equalized Circuits on FPGAs. IEEE Transactions on Computers, 2017.

Comparison

	SafeDRP		Improved GliFreD [30]		GliFreD [17]		Plain
	Doubled	Single	Doubled	Single	Doubled	Single	
LUTs	3712	1856	3466	1733	3466	1733	1262
Register	1276	638	11360	5680	22080	11040	256
Slices	1296	648	11638	5819	15502	7751	392
Latency[a]	11		154		308		11
Pipeline	0		14		14		0
Throughput[b]	116		116		58		116

[a] clock cycles
[b] MBit/s @ 10 MHz

- Reduced FF utilization
  - 8.9 Improved GliFreD
  - 17.3 GliFreD
- Reduced latency but GliFreD might reach a higher max. frequency

[17] A. Moradi and A. Wild. Assessment of Hiding the Higher-Order Leakages in Hardware - what are the achievements versus overheads? In CHES 2015
[30] A. Wild, et.al. GliFreD: Glitch-Free Duplication – Towards Power-Equalized Circuits on FPGAs. IEEE Transactions on Computers, 2017.

Side-Channel Evaluation

Methods

- Signal-to-Noise ratio $SNR = \frac{var(Signal)}{var(Noise)}$
  - Dependency of the power traces to the plaintext

Side-Channel Evaluation

Methods

- Signal-to-Noise ratio $SNR = \frac{var(Signal)}{var(Noise)}$
  - Dependency of the power traces to the plaintext
- Information-Theoretic mutual information
  - Amount of exploitable information

Side-Channel Evaluation

Methods

- Signal-to-Noise ratio $SNR = \frac{var(Signal)}{var(Noise)}$
  - Dependency of the power traces to the plaintext
- Information-Theoretic mutual information
  - Amount of exploitable information
- Correlation power analysis (CPA)
  - Common key recovery attack
  - HW and bit model of intermediate S-Box state

Side-Channel Evaluation

Methods

- Signal-to-Noise ratio $SNR = \frac{var(Signal)}{var(Noise)}$
  - Dependency of the power traces to the plaintext
- Information-Theoretic mutual information
  - Amount of exploitable information
- Correlation power analysis (CPA)
  - Common key recovery attack
  - HW and bit model of intermediate S-Box state
- Moments-Correlating DPA (MC-DPA)
  - Key recovery attack w/o particular power model

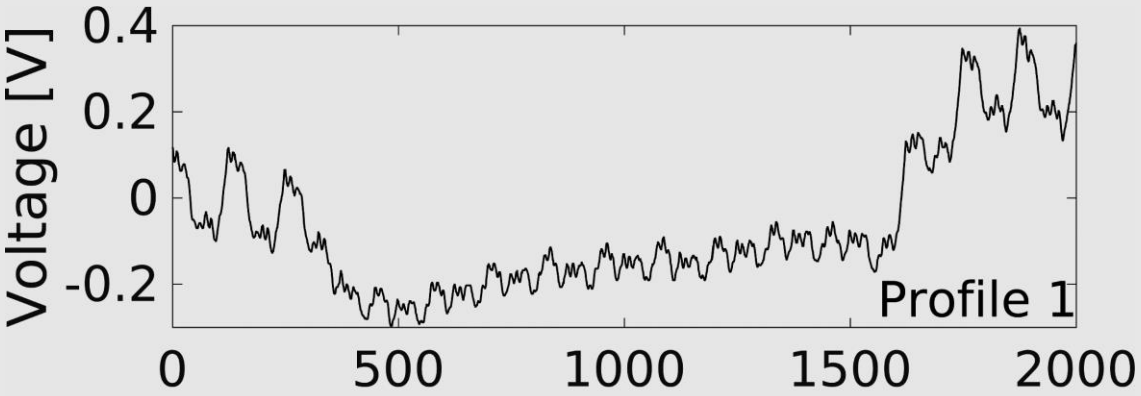
Side-Channel Evaluation

Methods

- Signal-to-Noise ratio $SNR = \frac{var(Signal)}{var(Noise)}$
  - Dependency of the power traces to the plaintext
- Information-Theoretic mutual information
  - Amount of exploitable information
- Correlation power analysis (CPA)
  - Common key recovery attack
  - HW and bit model of intermediate S-Box state
- Moments-Correlating DPA (MC-DPA)
  - Key recovery attack w/o particular power model
- Semi-fix vs. random Welch's t-test
  - Overview of the existing detectable leakage

Side-Channel Evaluation

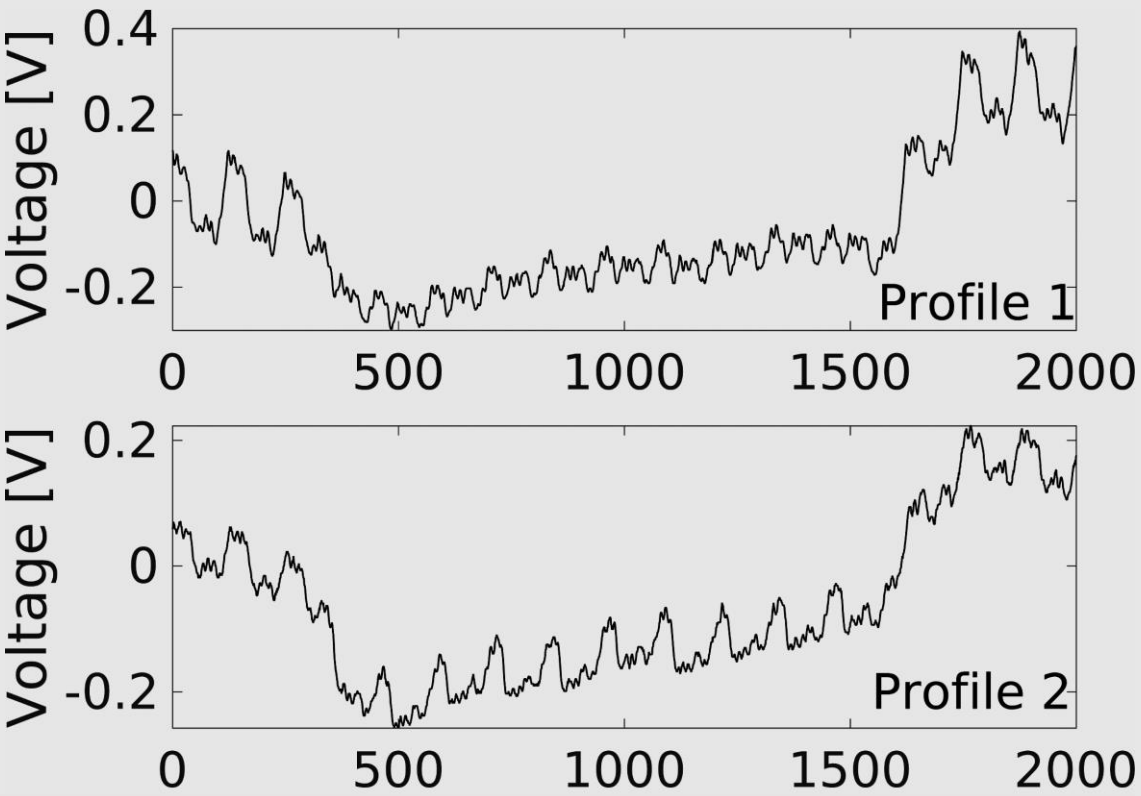
Profiles



Profile 1 (SafeDRP)	
Duplication ±	Active & Pre 🔔
✓	✓

Side-Channel Evaluation

Profiles

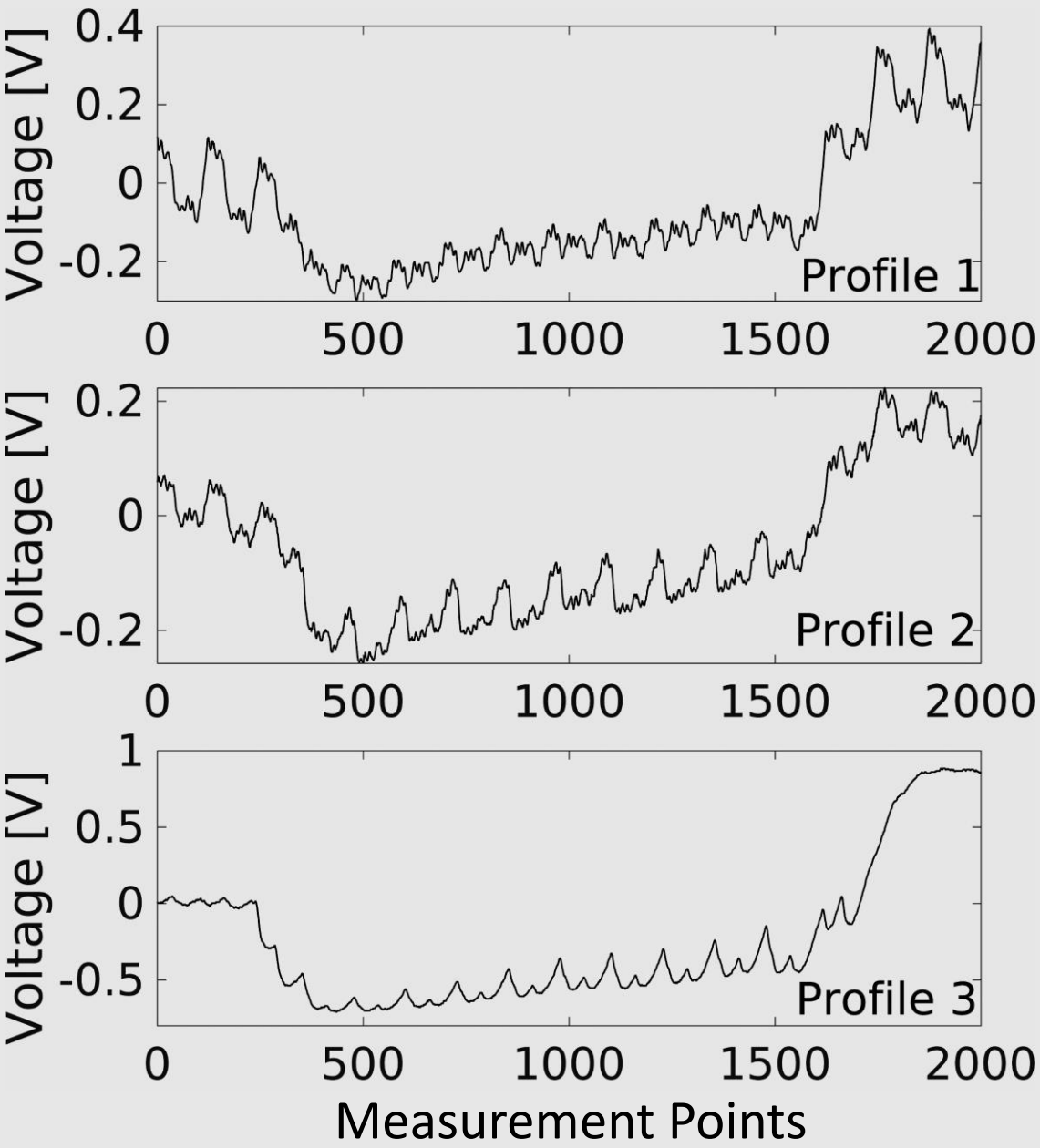


Profile 1 (SafeDRP)	
Duplication ±	Active & Pre 🔔
✓	✓

Profile 2	
Duplication ±	Active & Pre 🔔
✘	✓

Side-Channel Evaluation

Profiles



Profile 1 (SafeDRP)	
Duplication ±	Active & Pre
✓	✓

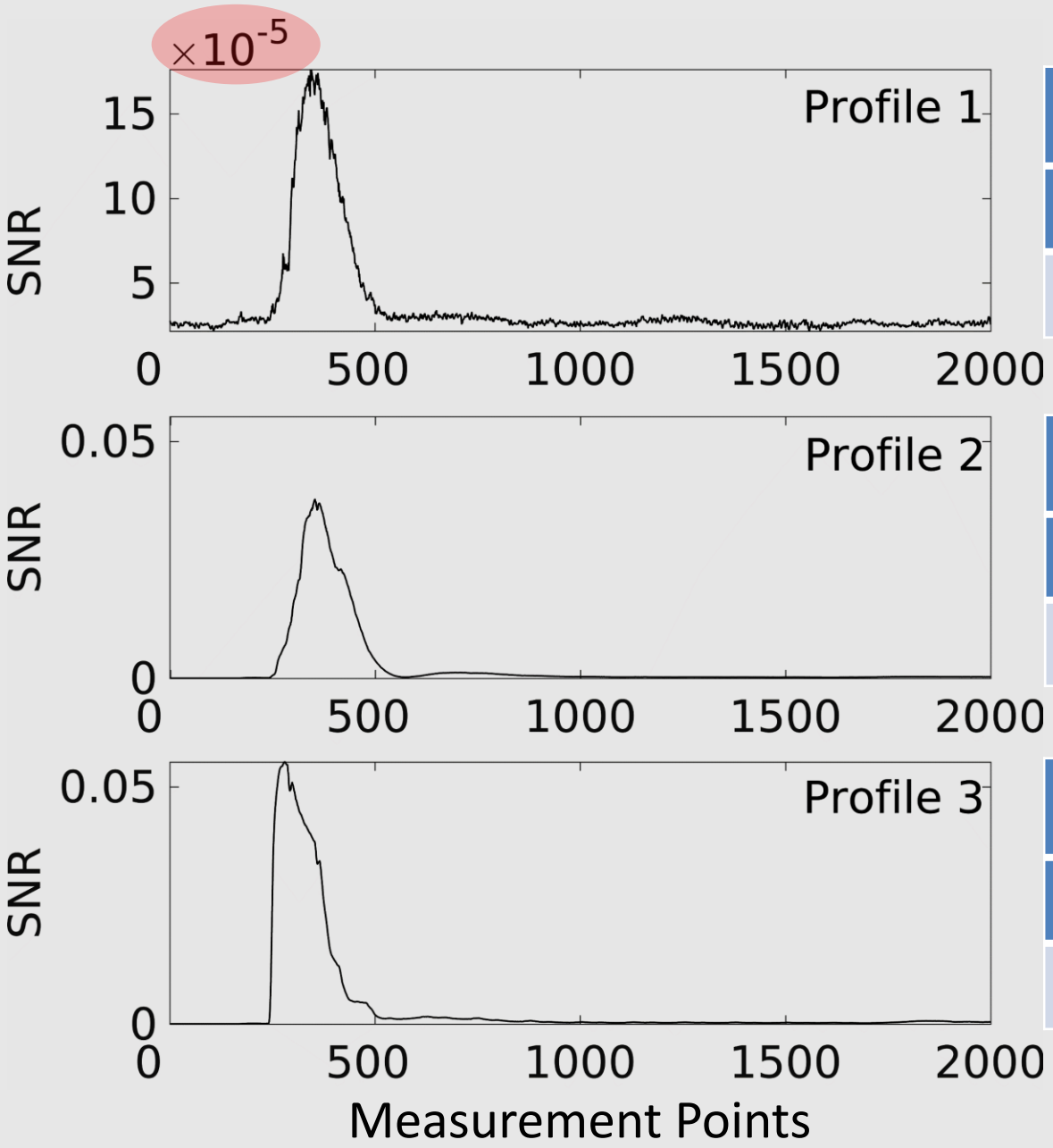
Profile 2	
Duplication ±	Active & Pre
✘	✓

Profile 3 (Unprotected)	
Duplication ±	Active & Pre
✘	✘

Side-Channel Evaluation

SNR

$$SNR = \frac{var(Signal)}{var(Noise)}$$



Profile 1 (SafeDRP)	
Duplication ±	Active & Pre
✓	✓

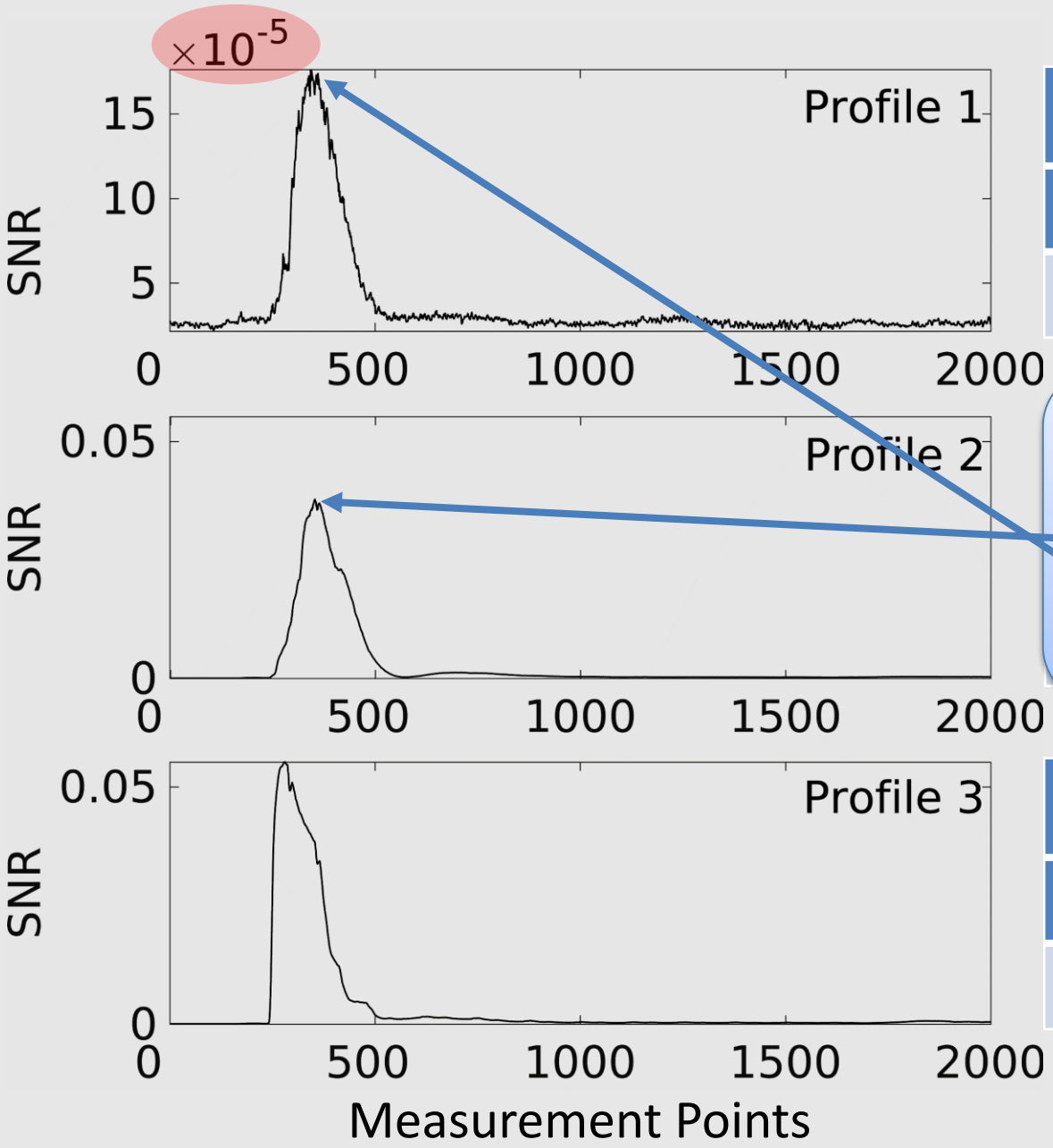
Profile 2	
Duplication ±	Active & Pre
✗	✓

Profile 3 (Unprotected)	
Duplication ±	Active & Pre
✗	✗

Side-Channel Evaluation

SNR

$$SNR = \frac{var(Signal)}{var(Noise)}$$



Profile 1 (SafeDRP)	
Duplication ±	Active & Pre
✓	✓

Decrease Factor 2

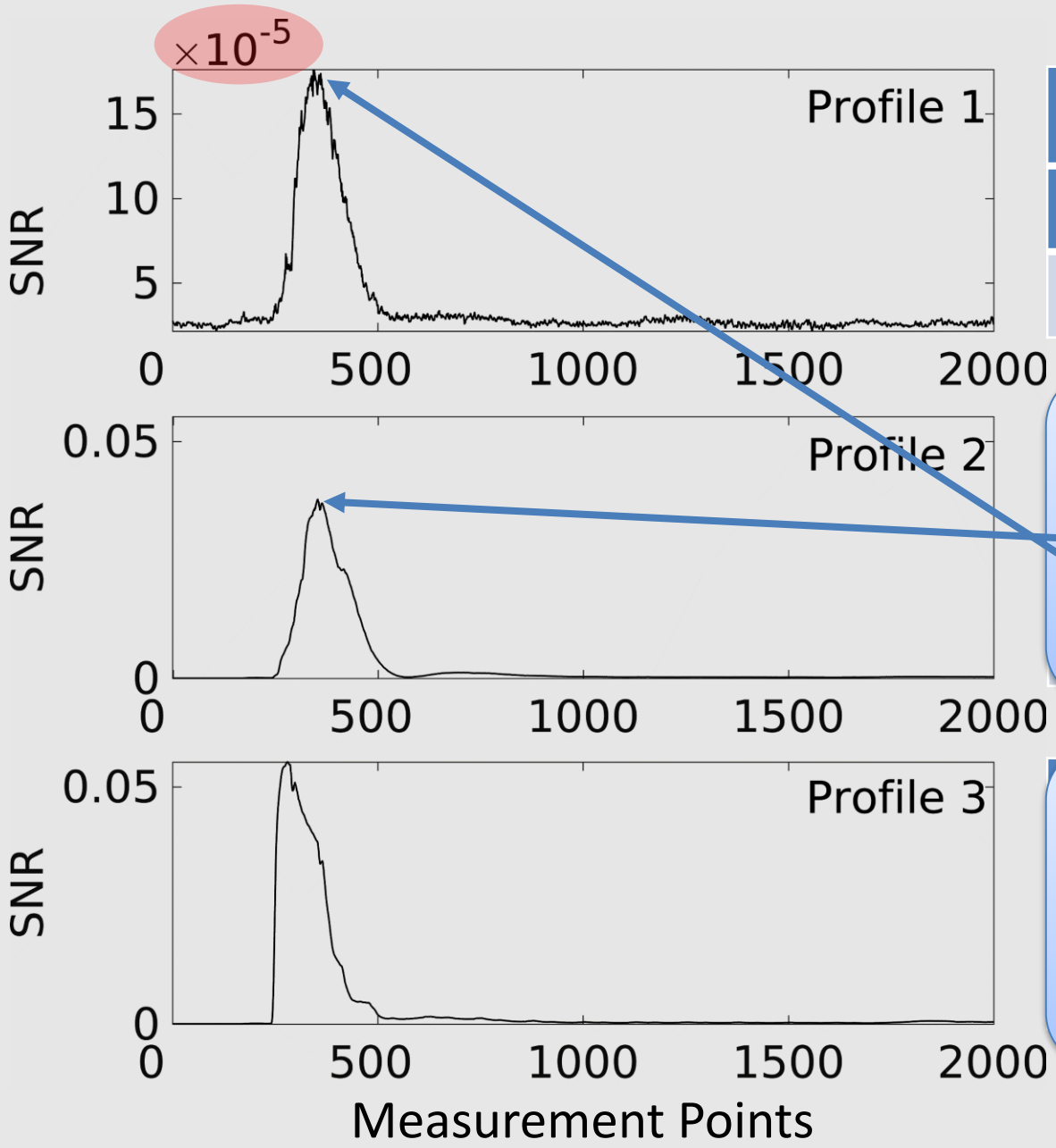
$$\frac{0.03784}{0.00018} \approx 214$$

Profile 3 (Unprotected)	
Duplication ±	Active & Pre
✗	✗

Side-Channel Evaluation

SNR

$$SNR = \frac{var(Signal)}{var(Noise)}$$



Profile 1 (SafeDRP)	
Duplication ±	Active & Pre 🔔
✓	✓

Decrease Factor 2

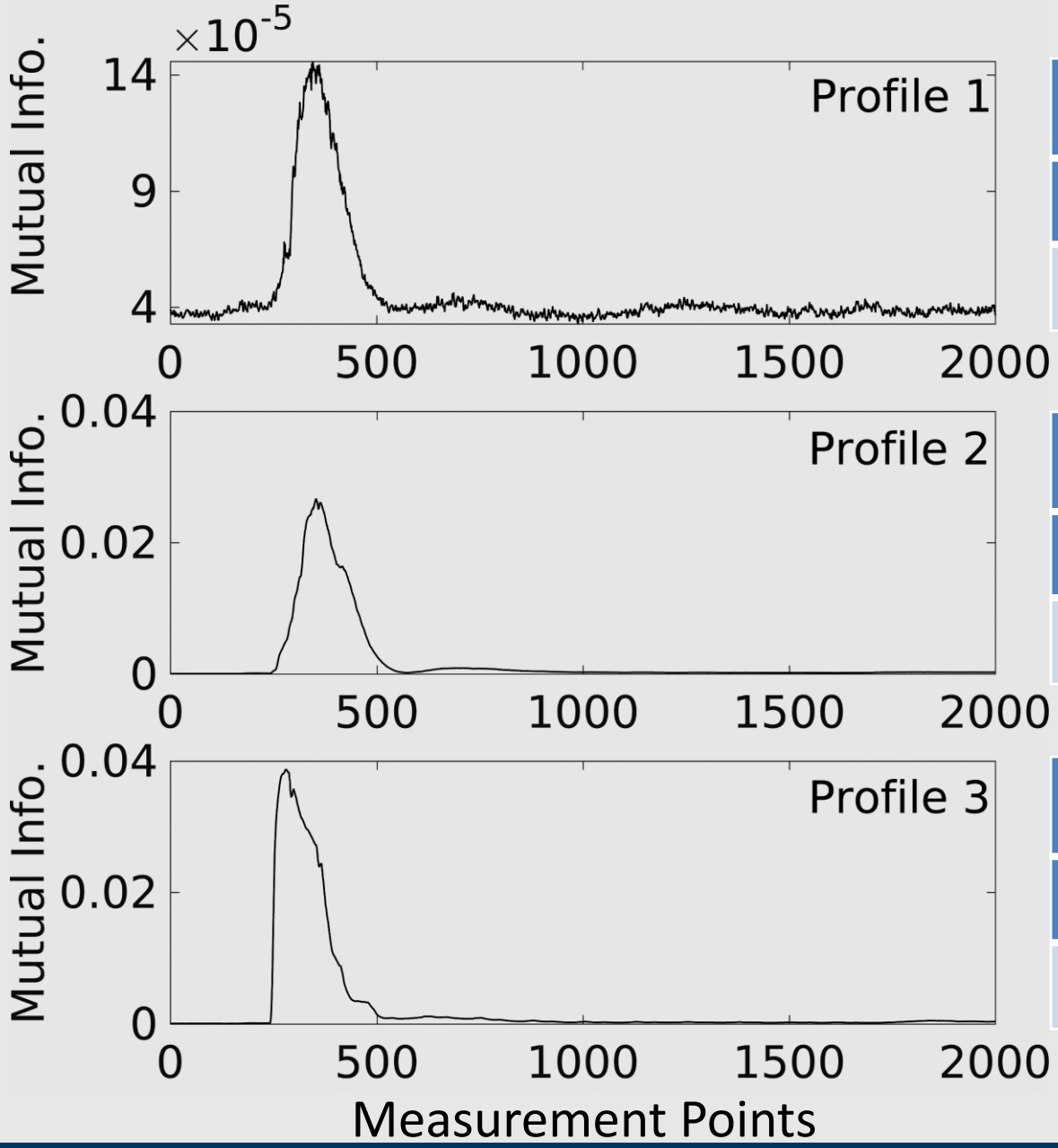
$$\frac{0.03784}{0.00018} \approx 214$$

Decrease Factor 3

$$\frac{0.05523}{0.00018} \approx 313$$

Side-Channel Evaluation

IT (Mutual Information)



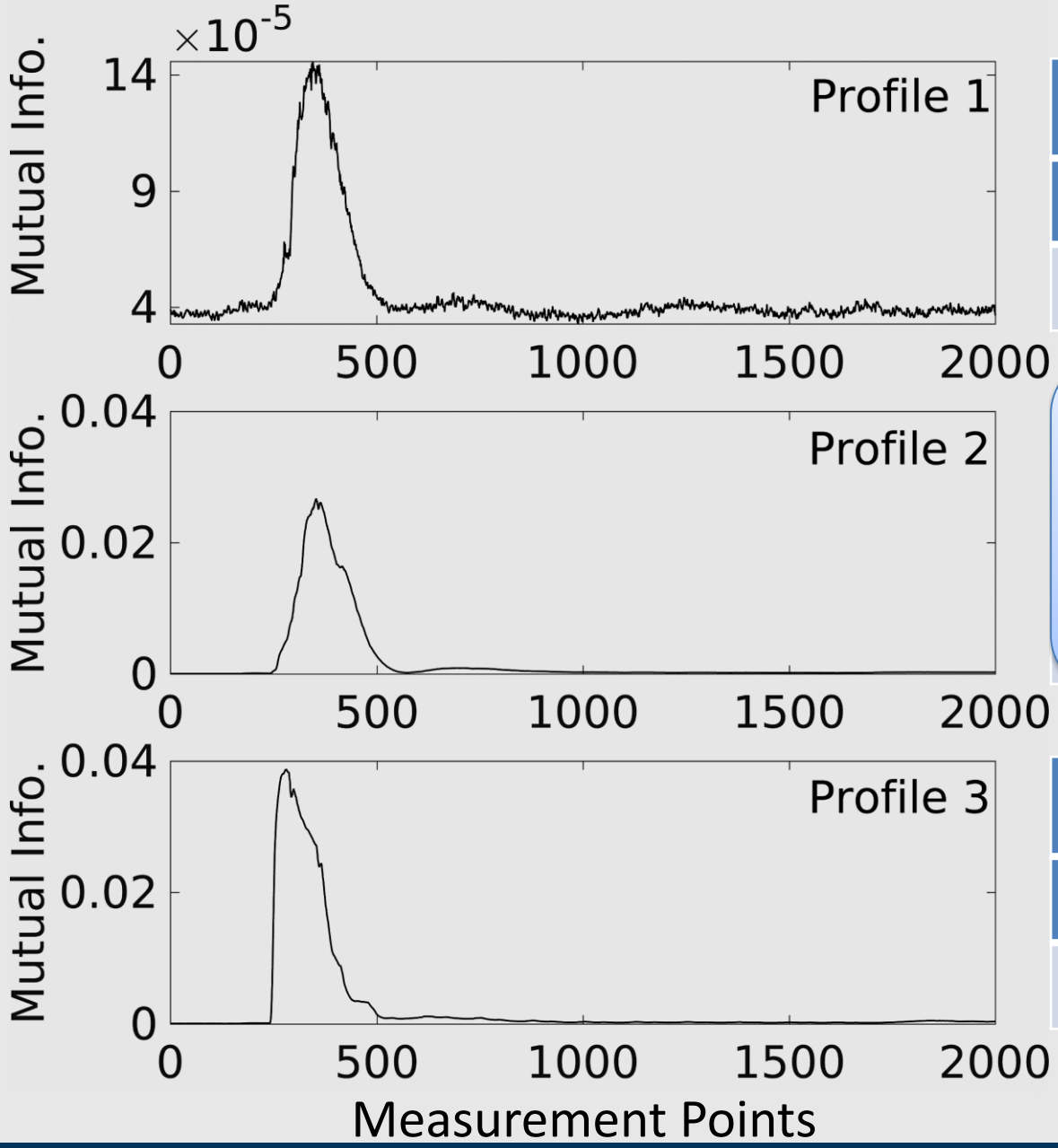
Profile 1 (SafeDRP)	
Duplication ±	Active & Pre 🔔
✓	✓

Profile 2	
Duplication ±	Active & Pre 🔔
✗	✓

Profile 3 (Unprotected)	
Duplication ±	Active & Pre 🔔
✗	✗

Side-Channel Evaluation

IT (Mutual Information)



Profile 1 (SafeDRP)	
Duplication ±	Active & Pre 🔔
✓	✓

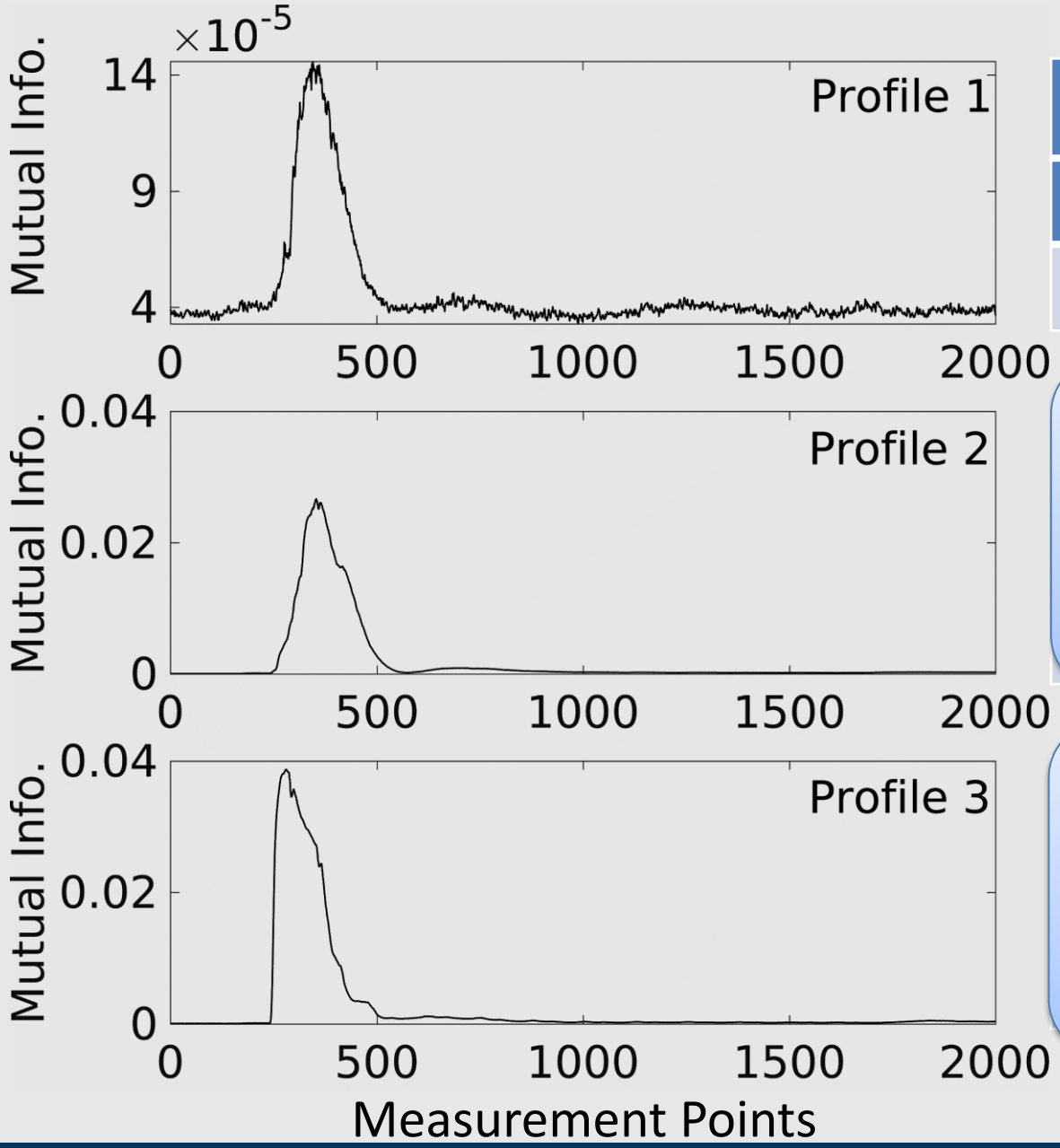
Decrease Factor 2

$$\frac{0.0267}{0.00015} \approx 183$$

Profile 3 (Unprotected)	
Duplication ±	Active & Pre 🔔
✗	✗

Side-Channel Evaluation

IT (Mutual Information)



Profile 1 (SafeDRP)	
Duplication ±	Active & Pre 🔔
✓	✓

Decrease Factor 2

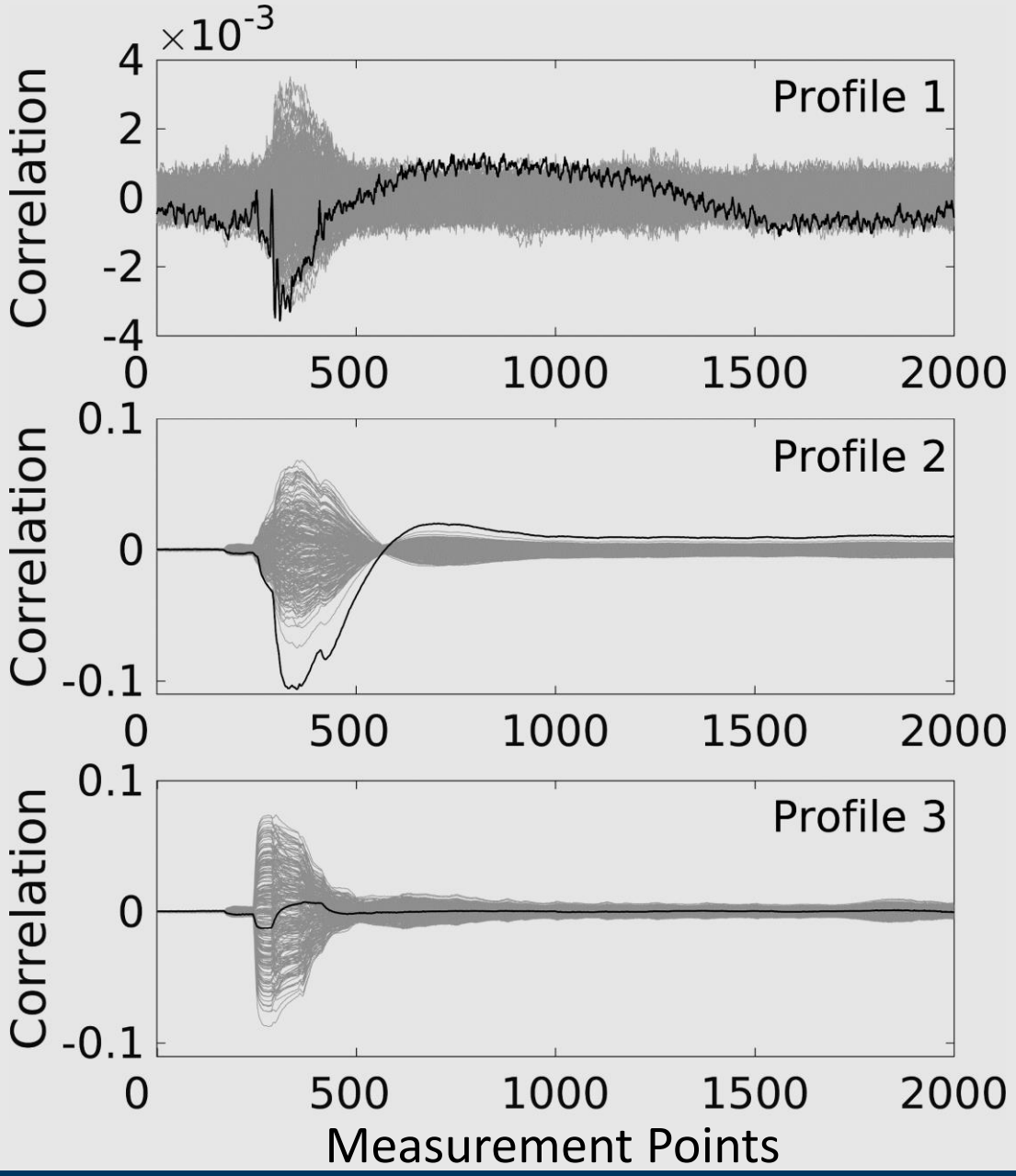
$$\frac{0.0267}{0.00015} \approx 183$$

Decrease Factor 3

$$\frac{0.0386}{0.00015} \approx 265$$

Side-Channel Evaluation

CPA HW S-Box Intermediate Model



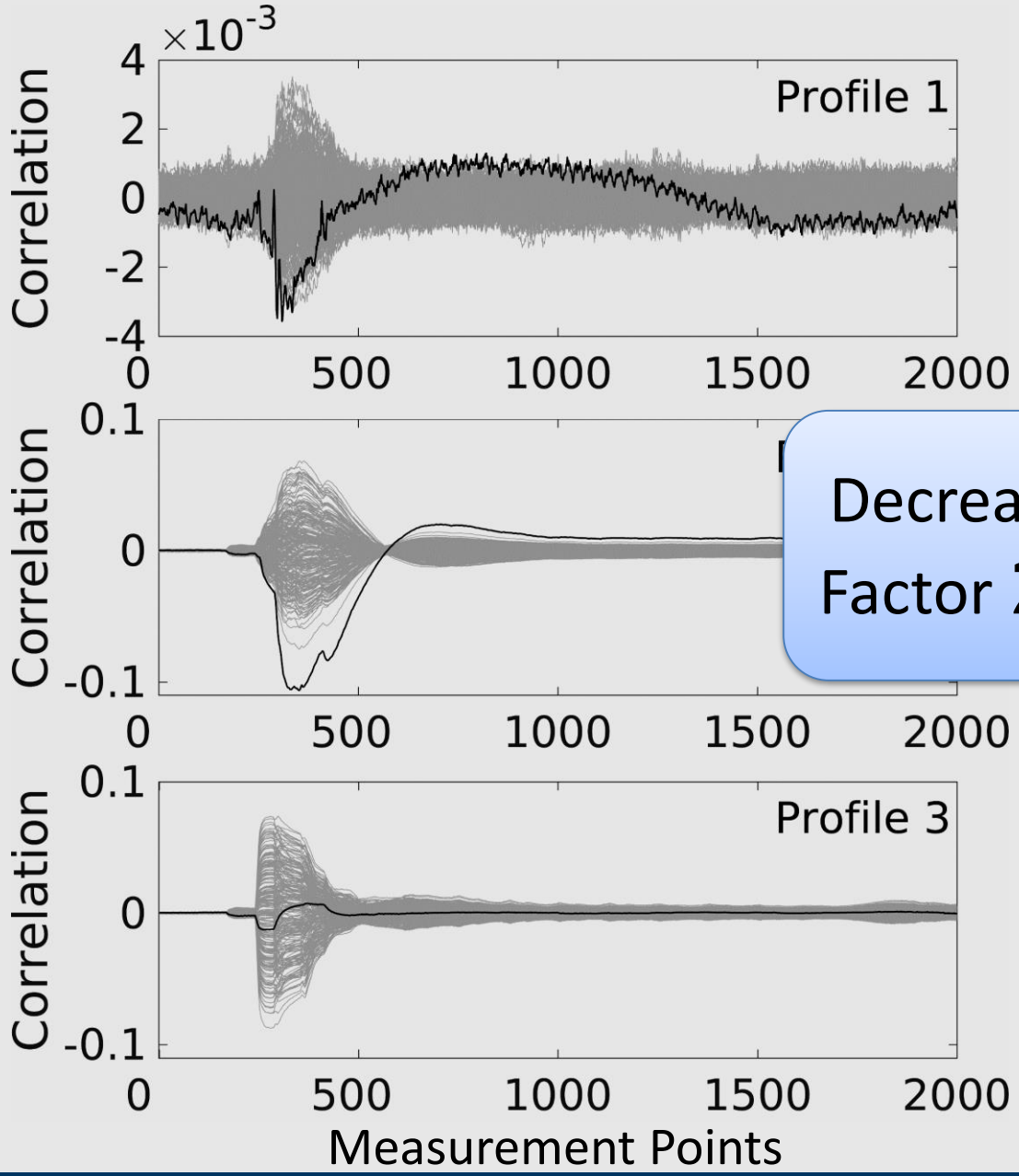
Profile 1 (SafeDRP)	
Duplication ±	Active & Pre 🔔
✓	✓

Profile 2	
Duplication ±	Active & Pre 🔔
✗	✓

Profile 3 (Unprotected)	
Duplication ±	Active & Pre 🔔
✗	✗

Side-Channel Evaluation

CPA HW S-Box Intermediate Model



Decrease Factor 29

Profile 1 (SafeDRP)	
Duplication ±	Active & Pre
✓	✓

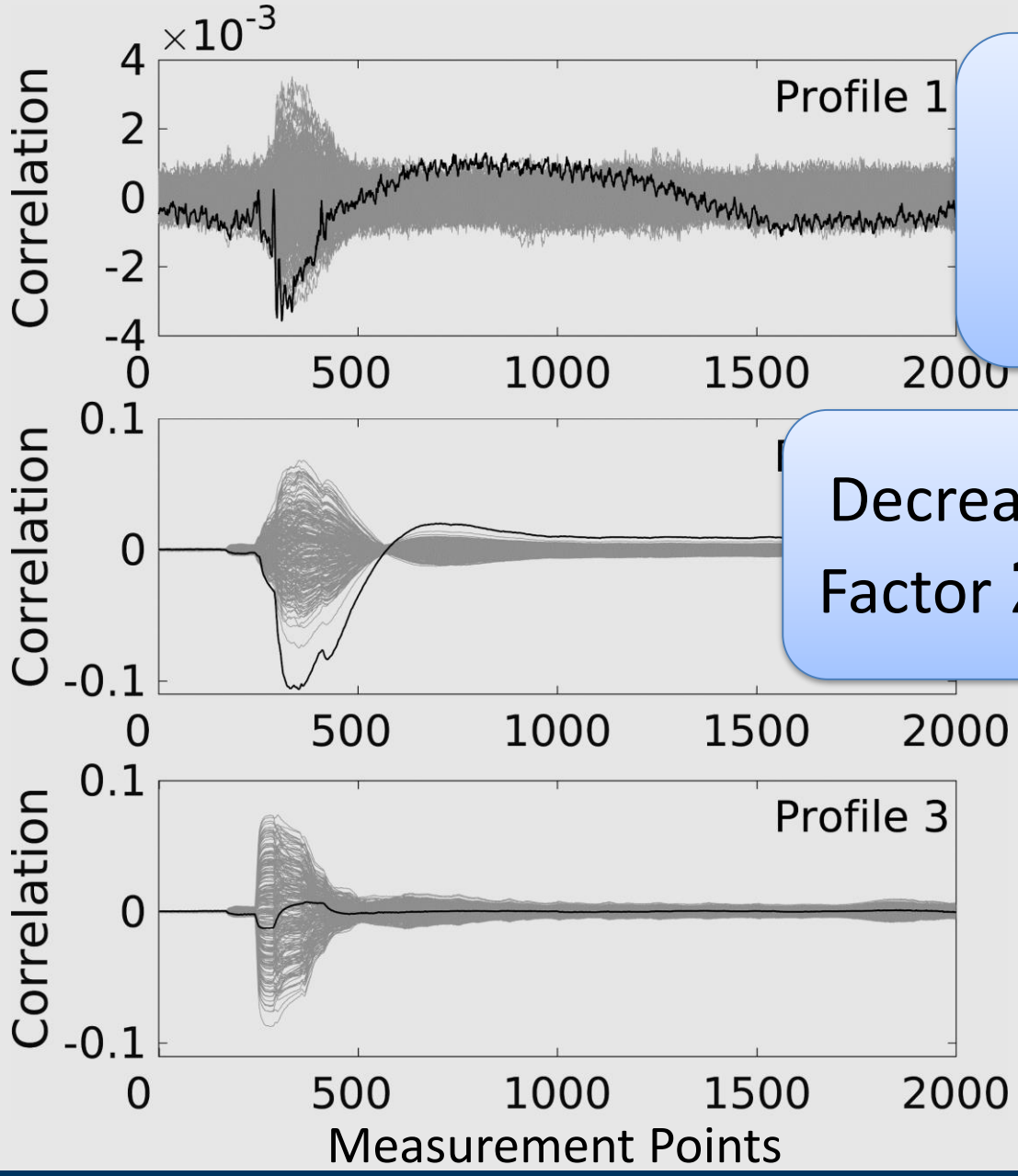
ofile 2	
plication ±	Active & Pre
✗	✓

Profile 3 (Unprotected)	
Duplication ±	Active & Pre
✗	✗

Side-Channel Evaluation

CPA HW S-Box Intermediate Model

$$n \approx \frac{28}{\rho^2}$$



Rule of Thumb (RoT):
2,184,700 *Traces*
to recover the key

Decrease
Factor 29

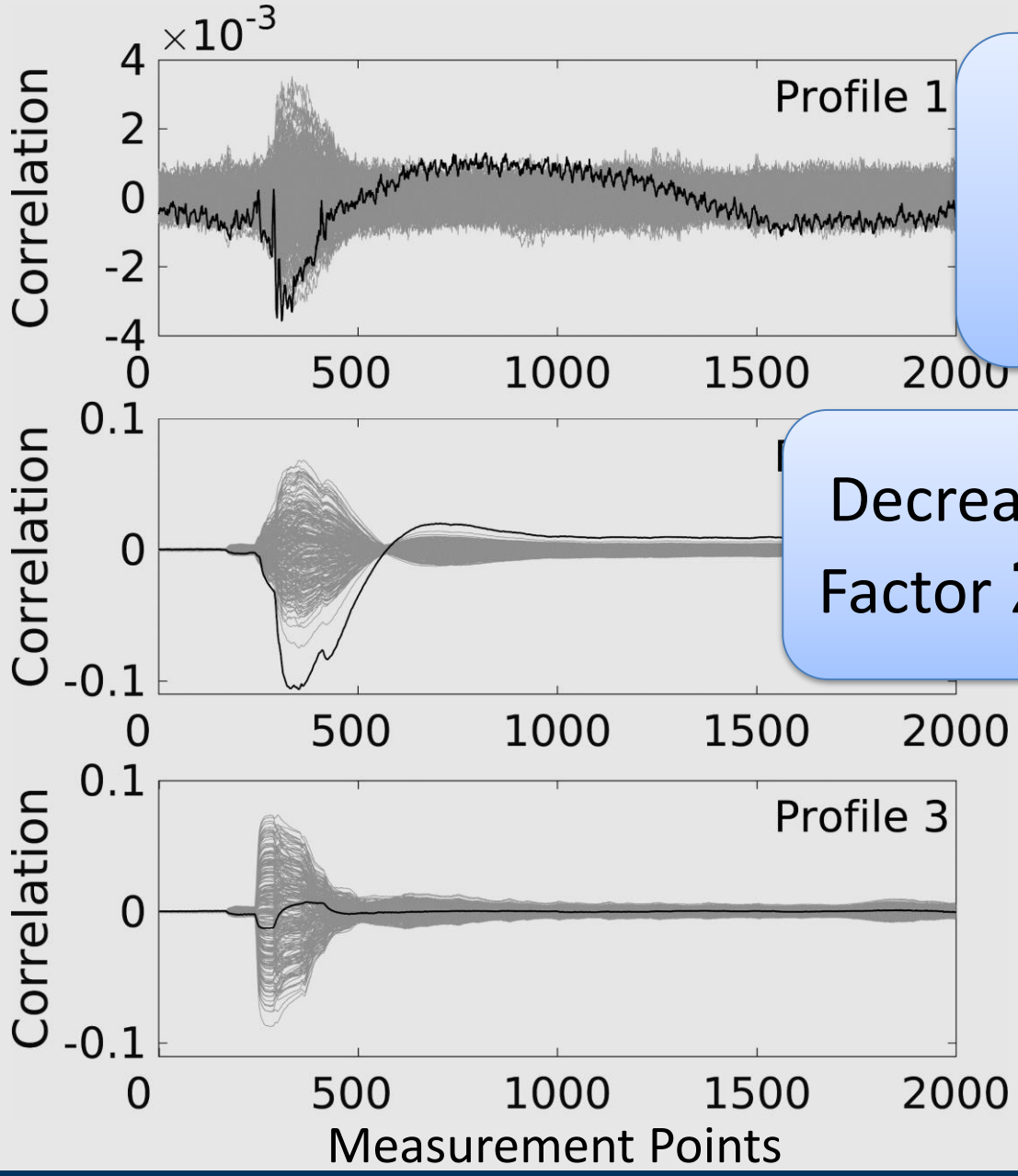
ofile 2	
plication ±	Active & Pre 🔔
✗	✓

Profile 3 (Unprotected)	
Duplication ±	Active & Pre 🔔
✗	✗

Side-Channel Evaluation

CPA HW S-Box Intermediate Model

$$n \approx \frac{28}{\rho^2}$$



Rule of Thumb (RoT):
2,184,700 *Traces*
to recover the key

Decrease Factor 29

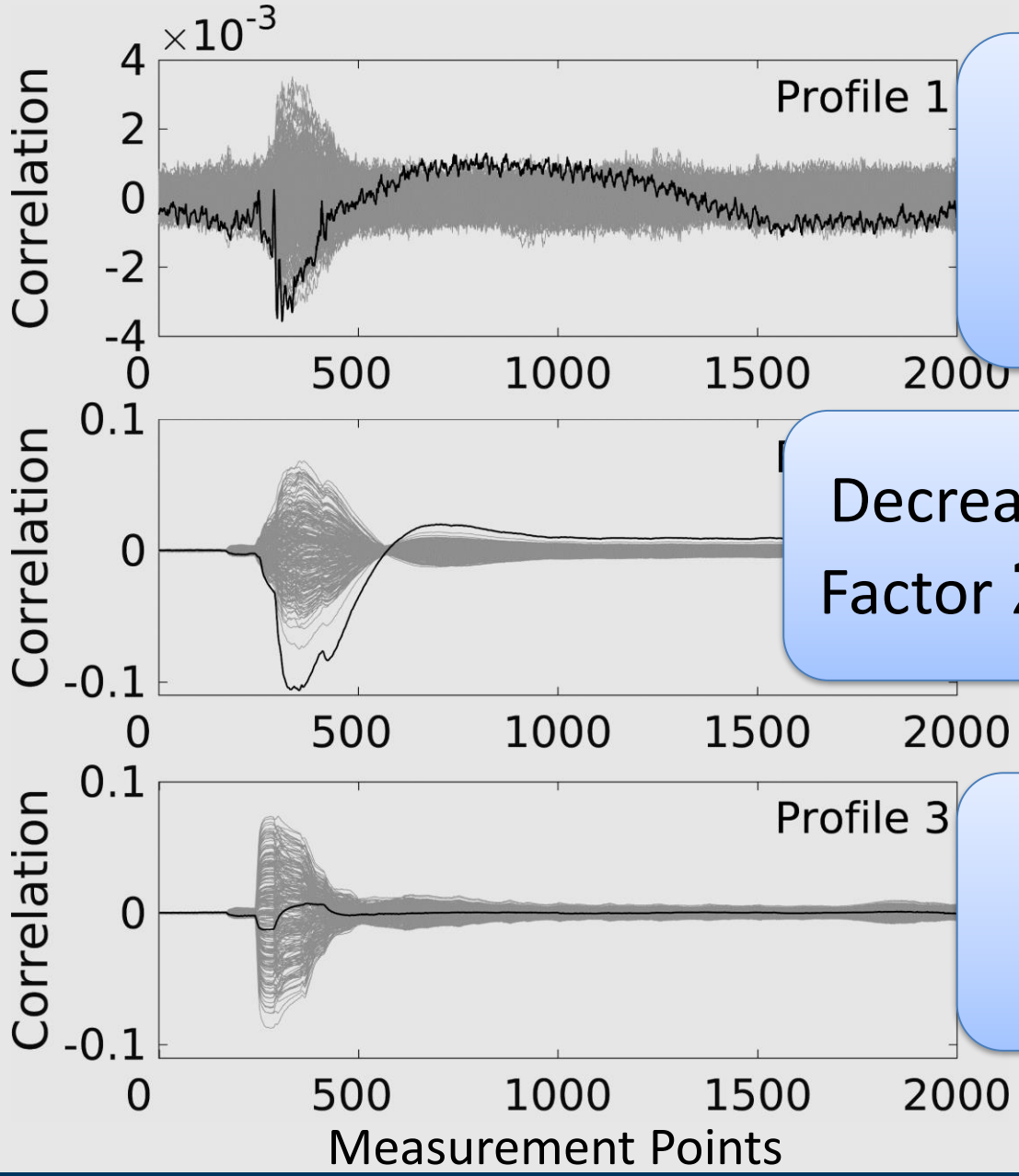
RoT: $\left(\frac{\rho_2}{\rho_1}\right)^2 \approx 881$

Profile 3 (Unprotected)	
Duplication ±	Active & Pre 🔔
✗	✗

Side-Channel Evaluation

CPA HW S-Box Intermediate Model

$$n \approx \frac{28}{\rho^2}$$



Rule of Thumb (RoT):
2,184,700 $Traces$
to recover the key

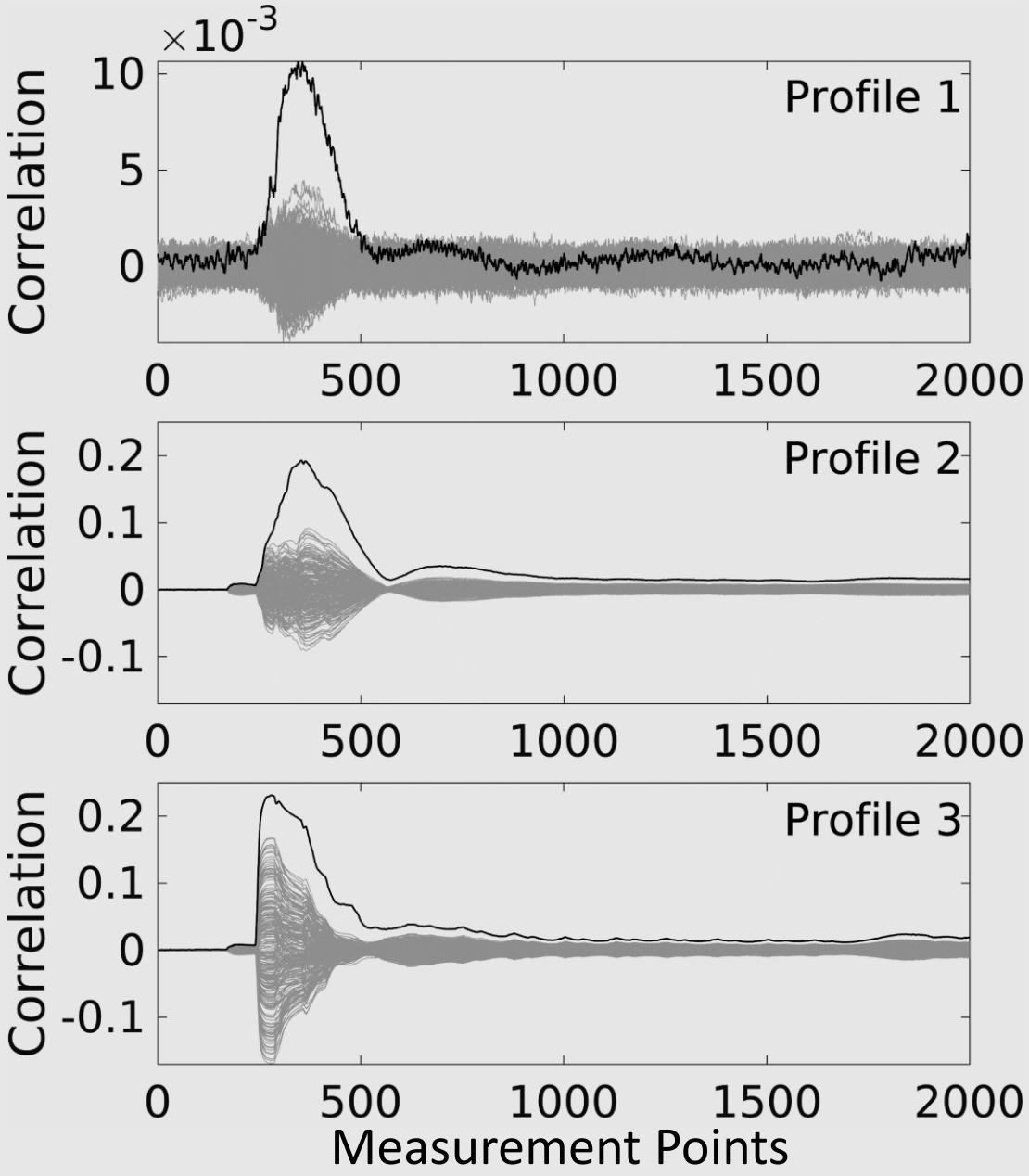
Decrease
Factor 29

RoT: $\left(\frac{\rho_2}{\rho_1}\right)^2 \approx 881$

HW Model
does not fit

Side-Channel Evaluation

MC-DPA



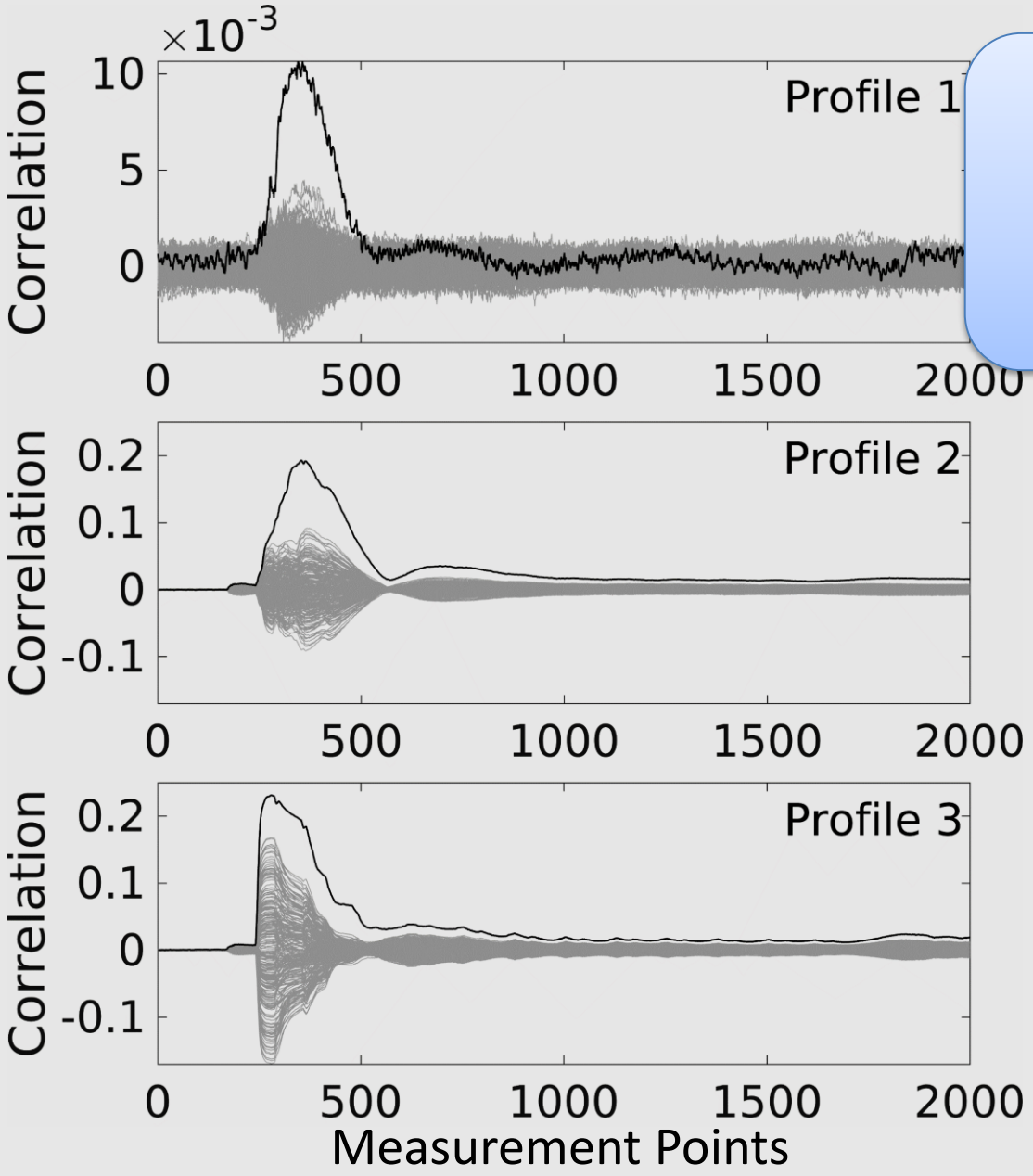
Profile 1 (SafeDRP)	
Duplication ±	Active & Pre 🔔
✓	✓

Profile 2	
Duplication ±	Active & Pre 🔔
✗	✓

Profile 3 (Unprotected)	
Duplication ±	Active & Pre 🔔
✗	✗

Side-Channel Evaluation

MC-DPA



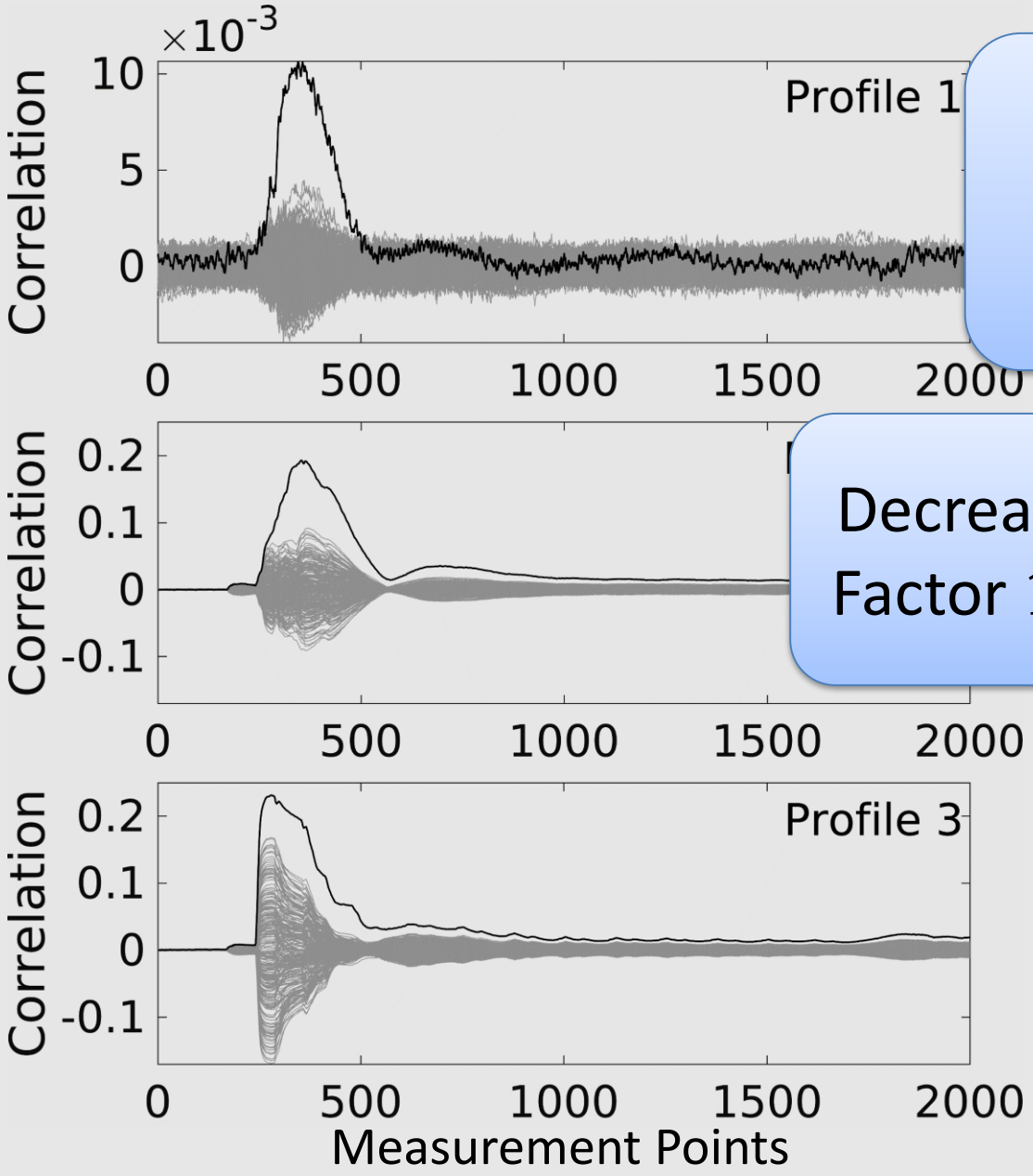
Rule of Thumb (RoT):
$244{,}000\ Traces$
to recover the key

Profile 2	
Duplication ±	Active & Pre 🔔
✗	✓

Profile 3 (Unprotected)	
Duplication ±	Active & Pre 🔔
✗	✗

Side-Channel Evaluation

MC-DPA



Rule of Thumb (RoT):
$244{,}000\ Traces$
to recover the key

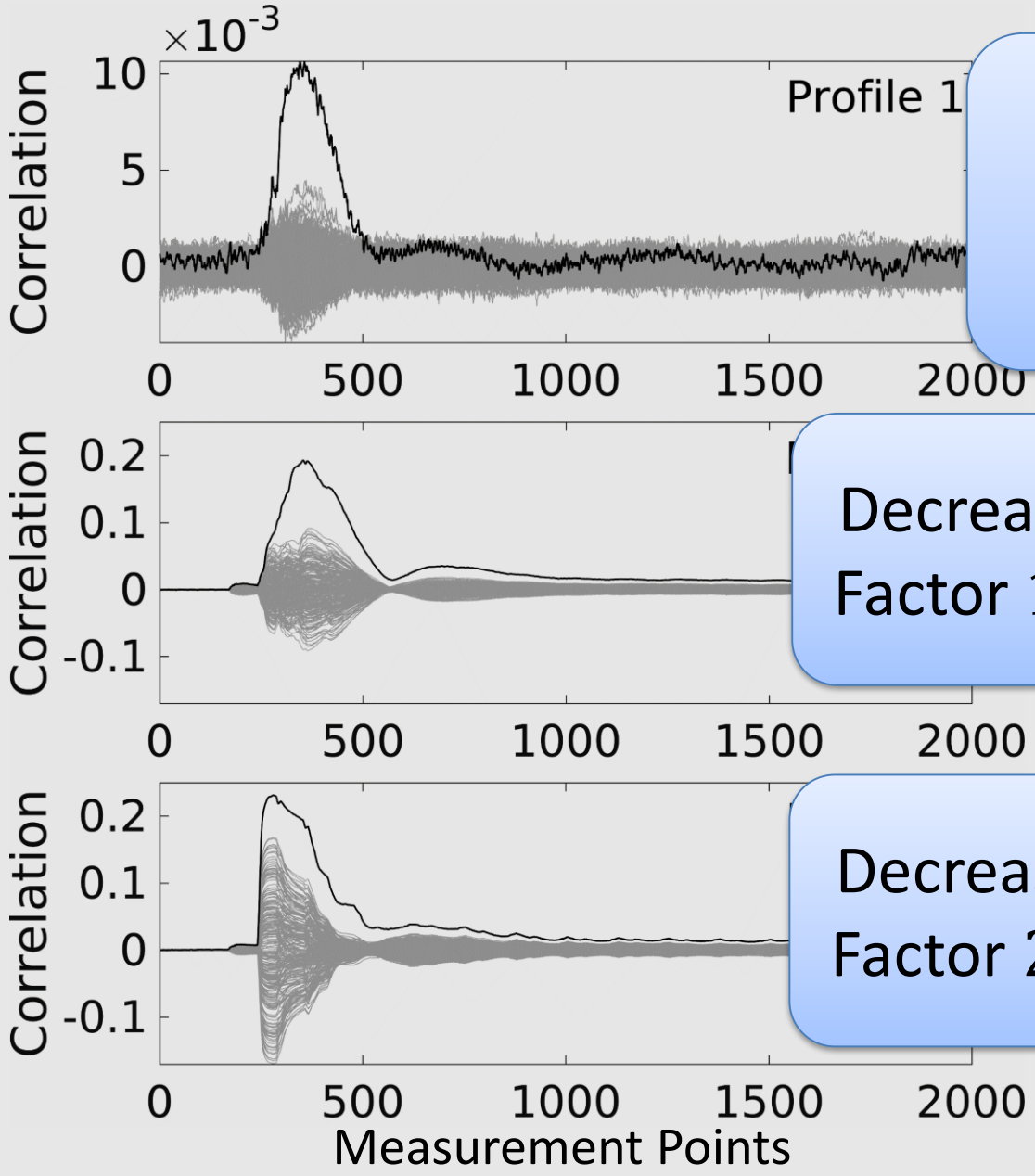
Decrease Factor 18

RoT: $\left(\frac{\rho_2}{\rho_1}\right)^2 \approx 327$

Profile 3 (Unprotected)	
Duplication ±	Active & Pre
✗	✗

Side-Channel Evaluation

MC-DPA



Rule of Thumb (RoT):
$244{,}000\ Traces$
to recover the key

Decrease Factor 18

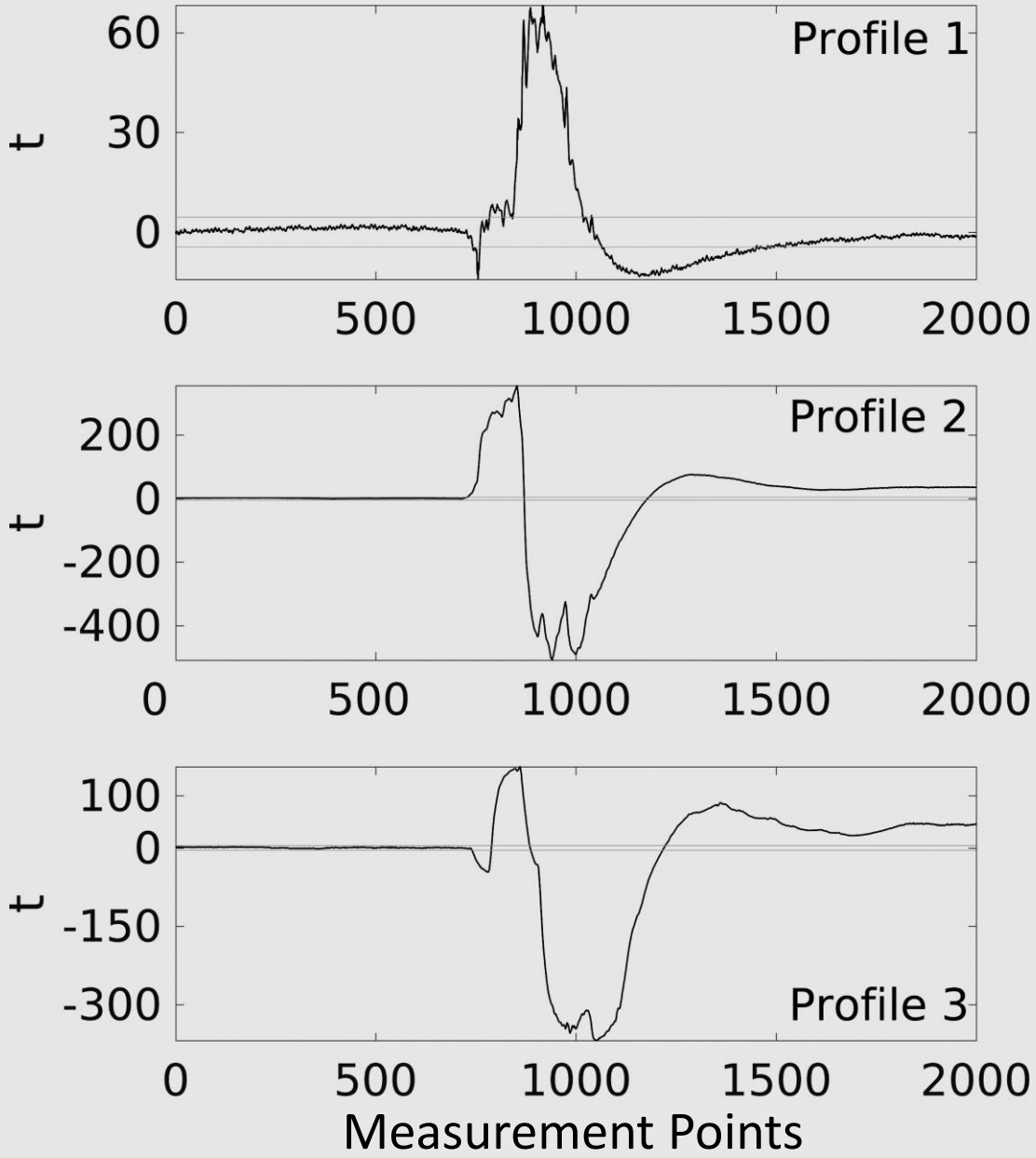
RoT: $\left(\frac{\rho_2}{\rho_1}\right)^2 \approx 327$

Decrease Factor 21

RoT: $\left(\frac{\rho_3}{\rho_1}\right)^2 \approx 468$

Side-Channel Evaluation

Welch's T-Test



- Semi-fix vs. random
- 5th round first 64 bit zero [1]
- 1,000,000 Traces
- Leakage only in 5th round

[1] Evaluating the Duplication of Dual-Rail Precharge Logics on FPGAs; Alexander Wild, Amir Moradi, Tim Güneysu; COSDAE 2015

Conclusion

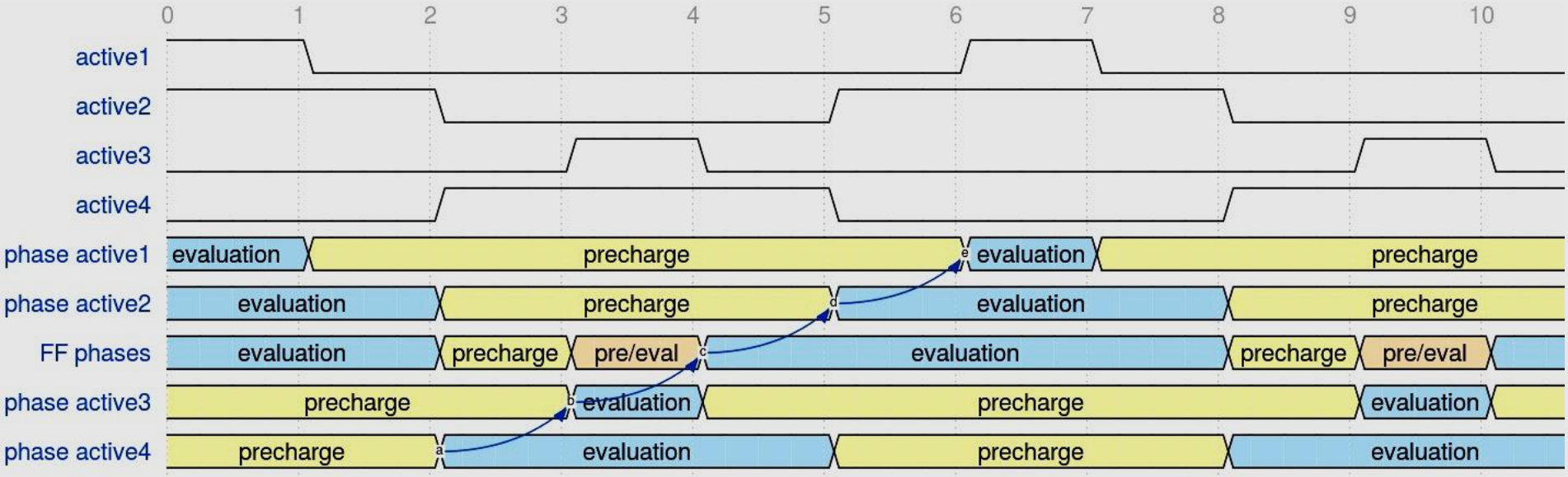
- Improved DRP scheme
  - Reduce the FF utilization
  - Complex control logic
- Addressing all pitfalls
  - Avoiding glitches
  - Preventing early evaluation
  - Mitigate the imbalanced routings
- Combination [2] with sound masking scheme for a practical secure implementation

[2] A. Wild and A. Moradi; Assessment of Hiding the Higher-Order Leakage in Hardware – what are the achievements versus overheads?; CHES 2015

Conclusion

- Improved DRP scheme
  - Reduce the FF utilization
  - Complex control logic
- Addressing all pitfalls
  - Avoiding glitches
  - Preventing early evaluation
  - Mitigate the imbalanced routings
- Combination [2] with sound masking scheme for a practical secure implementation

Thank you!


0
1
2
3
4
5
6
7
8
9
10
active1
active2
active3
active4
phase active1
phase active2
FF phases
phase active3
phase active4
evaluation
precharge
pre/eval
a
b
c
d
e