RUB

RUHR-UNIVERSITÄT BOCHUM
Horst Görtz Institute for IT-Security

Assessment of Hiding the Higher-Order

--what are the achievements versus overheads?--

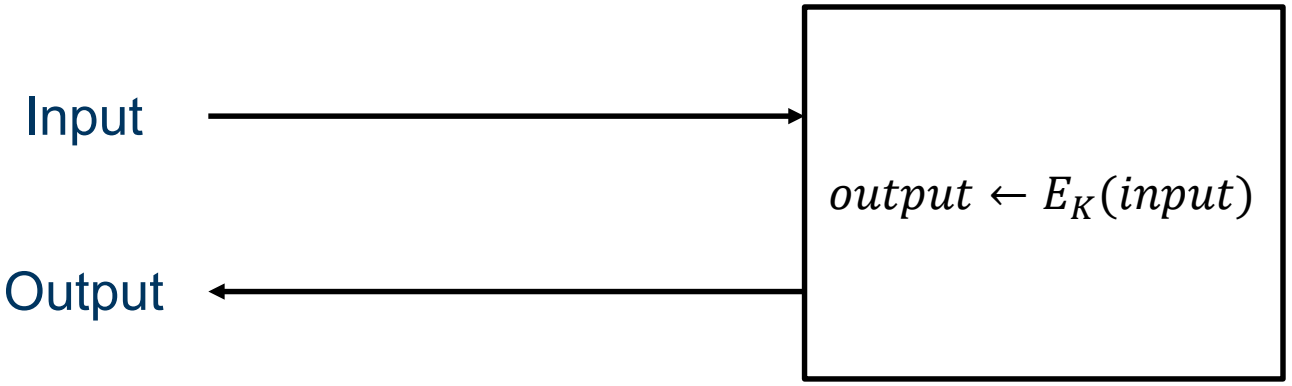
Amir Moradi, Alexander Wild

hgi
Horst Görtz Institute
for IT-Security

September 16, 2015

Intro to SCA

Attack Model

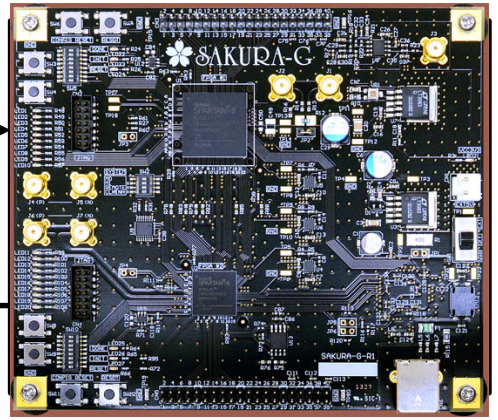


Intro to SCA

Attack Model

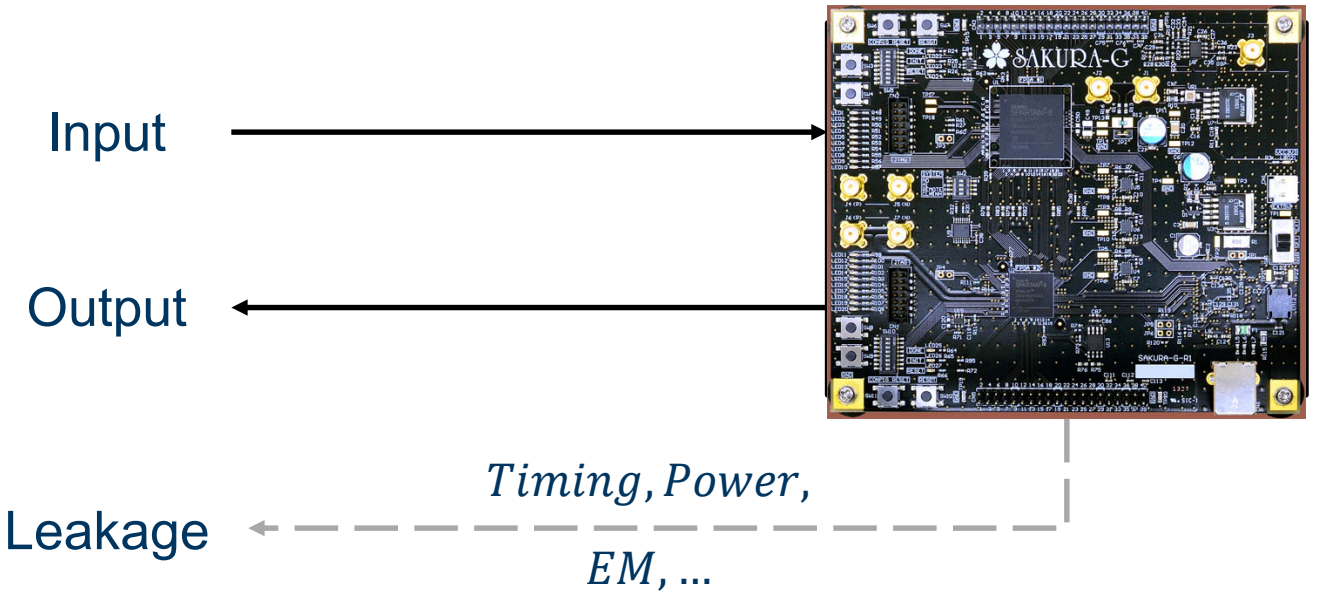
Input

Output



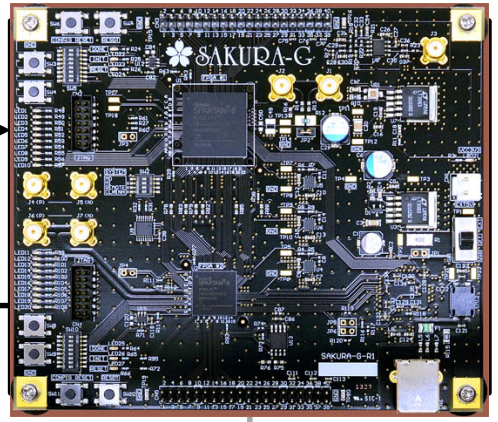
Intro to SCA

Attack Model



Intro to SCA

Attack Model



Input

Output

Leakage

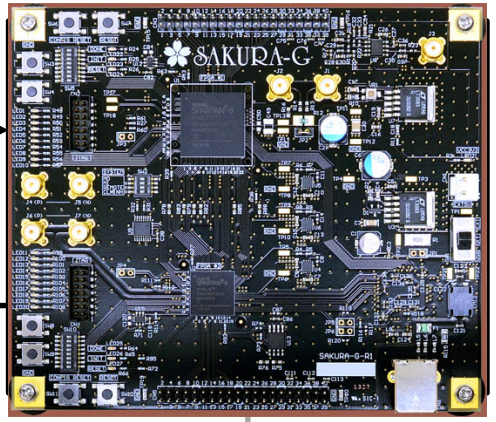
$Timing, Power, EM, \ldots$

Countermeasures

Masking

Intro to SCA

Attack Model



Input

Output

Leakage

$Timing, Power, EM, \ldots$

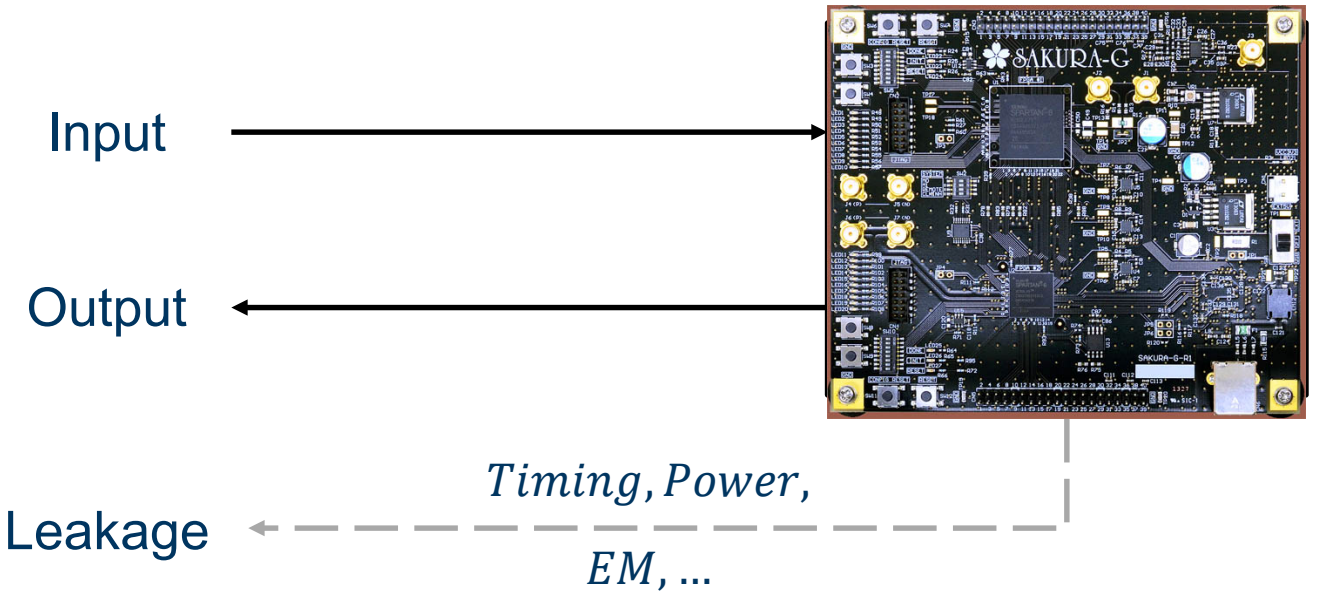
Countermeasures

Masking

Hiding

Intro to SCA

Attack Model



Countermeasures

Masking

Hiding

Rekeying

Introduction

Motivation

Introduction

Motivation

- Threshold Implementation provide 1st-order security.

S. Nikova, C. Rechberger, and V. Rijmen. Threshold Implementations Against Side-Channel Attacks and Glitches. ICICS'06

  - Might be restricted to univariate.
  - Area overhead might be problematic.
  - Finding uniform representation might be challenging.

Introduction

Motivation

- Threshold Implementation provide 1st-order security.

S. Nikova, C. Rechberger, and V. Rijmen. Threshold Implementations Against Side-Channel Attacks and Glitches. ICICS'06

  - Might be restricted to univariate.
  - Area overhead might be problematic.
  - Finding uniform representation might be challenging.

- Hiding schemes should not used solely.
  - Expected hardening on each statistical order.
  - Higher-Order attacks are hard on noisy traces. Power-Equalization schemes reduce signal level and have the same effect.

    E. Prouff M. Rivain, and R. Bevan. Statistical Analysis of Second Order Differential Power Analysis. IEEE Trans. Computers 2009

Introduction

Motivation

- Threshold Implementation provide 1st-order security.

S. Nikova, C. Rechberger, and V. Rijmen. Threshold Implementations Against Side-Channel Attacks and Glitches. ICICS'06

  - Might be restricted to univariate.
  - Area overhead might be problematic.
  - Finding uniform representation might be challenging.

- Hiding schemes should not used solely.
  - Expected hardening on each statistical order.
  - Higher-Order attacks are hard on noisy traces. Power-Equalization schemes reduce signal level and have the same effect.

    E. Prouff M. Rivain, and R. Bevan. Statistical Analysis of Second Order Differential Power Analysis. IEEE Trans. Computers 2009

- Combine hiding with TI
  - Often suggested but "never" examined.

GliFreD

Concept

GliFreD

Concept

- Dual-rail logic styles, (ideally) equalize the power/energy consumption.

GliFreD

Concept

- Dual-rail logic styles, (ideally) equalize the power/energy consumption.
- They usually fail to be ideal, but can for sure reduce the signal.

GliFreD

Concept

- Dual-rail logic styles, (ideally) equalize the power/energy consumption.
- They usually fail to be ideal, but can for sure reduce the signal.
- Limited routing resources in FPGAs → not much success to mount.

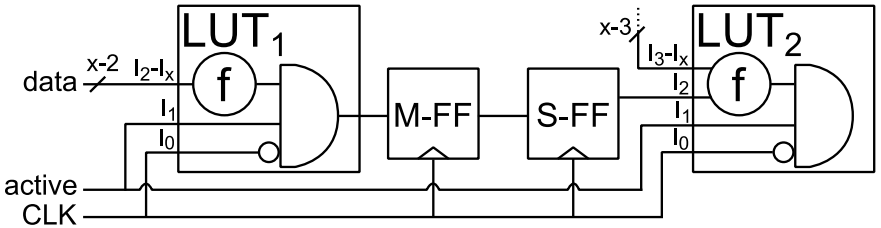
GliFreD

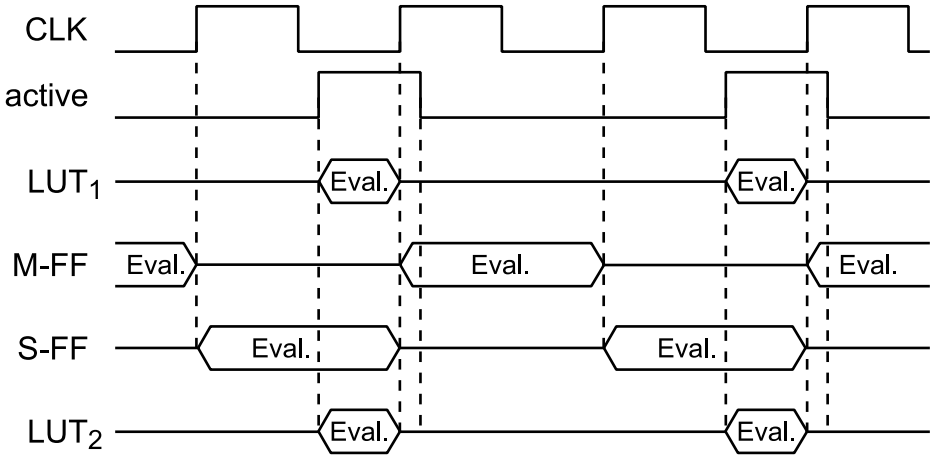
Concept

- Dual-rail logic styles, (ideally) equalize the power/energy consumption.
- They usually fail to be ideal, but can for sure reduce the signal.
- Limited routing resources in FPGAs → not much success to mount.
- Slightly different approach: Glitch-Free Duplication (GliFreD)

A. Wild, A. Moradi, and T. Güneysu. GliFreD: Glitch-Free Duplication – Towards Power-Equalized Circuits on FPGAs. Cryptology ePrint Archive, Report 2015/124.

  - Each LUT enabled once at each two clock cycles (precharge vs eval) and is followed by a two flip-flips (master-slave)





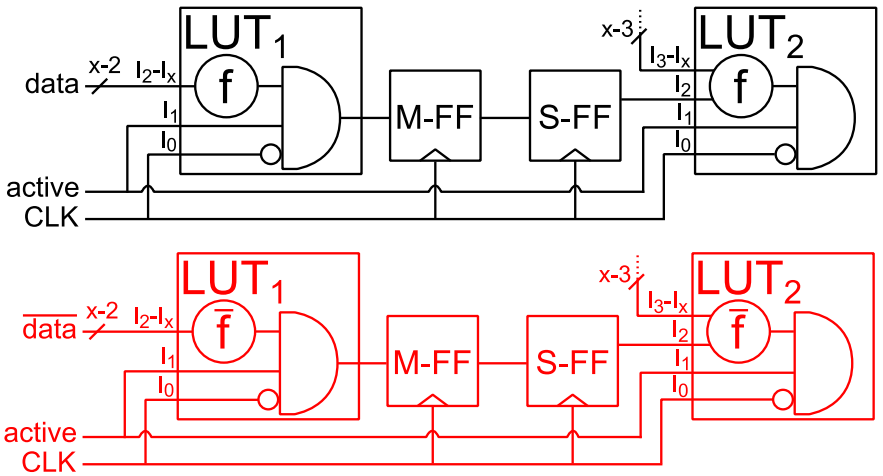
GliFreD

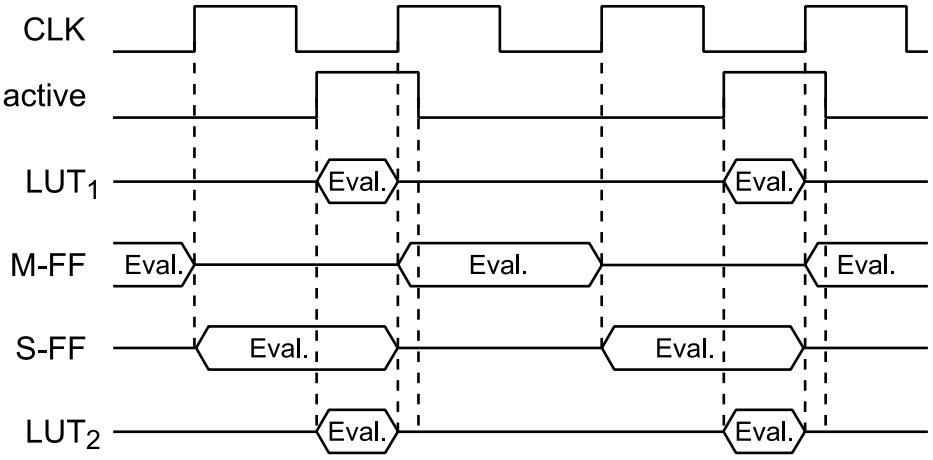
Concept

- Dual-rail logic styles, (ideally) equalize the power/energy consumption.
- They usually fail to be ideal, but can for sure reduce the signal.
- Limited routing resources in FPGAs → not much success to mount.
- Slightly different approach: Glitch-Free Duplication (GliFreD)

A. Wild, A. Moradi, and T. Güneysu. GliFreD: Glitch-Free Duplication – Towards Power-Equalized Circuits on FPGAs. Cryptology ePrint Archive, Report 2015/124.

  - Each LUT enabled once at each two clock cycles (precharge vs eval) and is followed by a two flip-flips (master-slave)

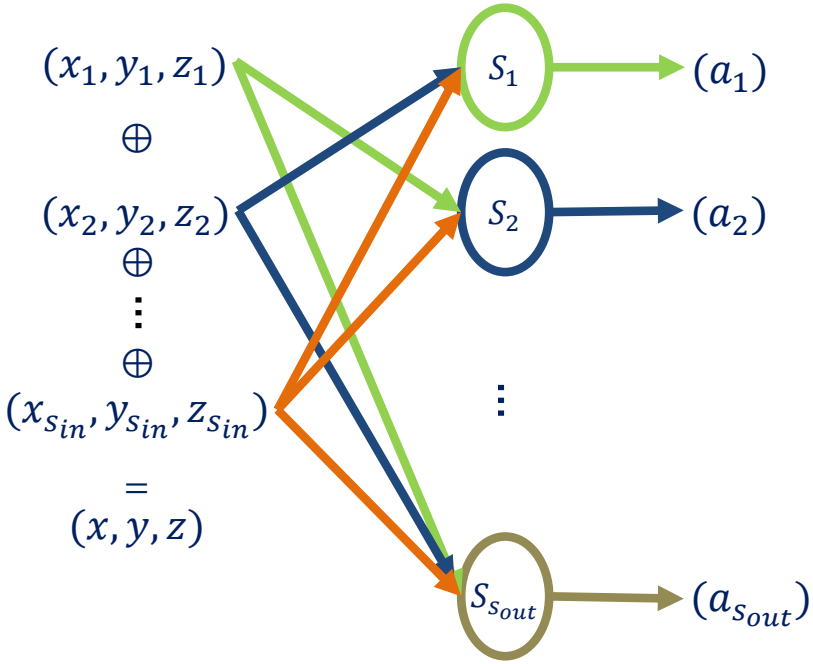




Higher-Order TI

Concept

B. Bilgin, B. Gierlichs, S. Nikova, V. Nikov, and V. Rijmen. Higher-Order Threshold Implementations. ASIACRYPT 2014,

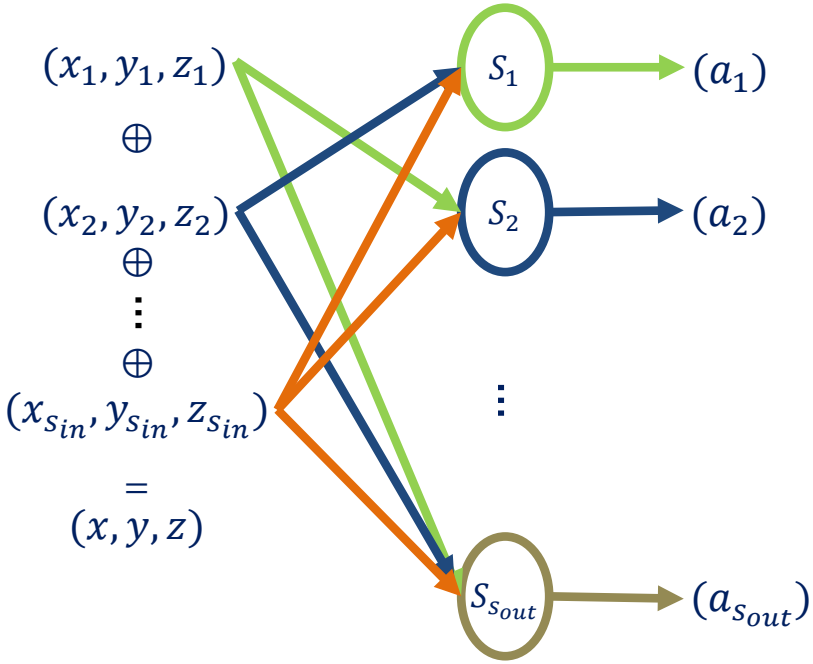


Higher-Order TI

Concept

B. Bilgin, B. Gierlichs, S. Nikova, V. Nikov, and V. Rijmen. Higher-Order Threshold Implementations. ASIACRYPT 2014,

- Correctness

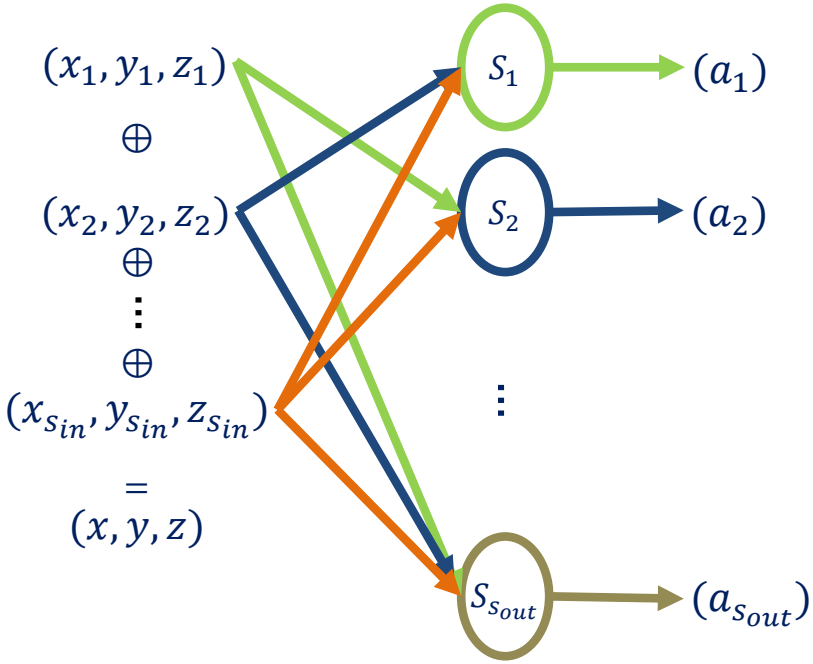


Higher-Order TI

Concept

B. Bilgin, B. Gierlichs, S. Nikova, V. Nikov, and V. Rijmen. Higher-Order Threshold Implementations. ASIACRYPT 2014,

- Correctness
- d^{th}-order non completeness

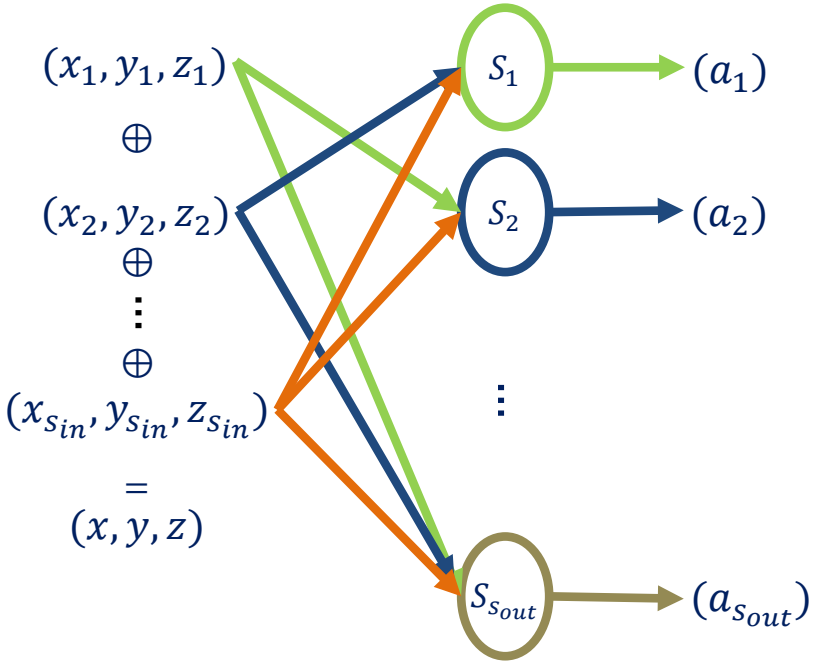


Higher-Order TI

Concept

B. Bilgin, B. Gierlichs, S. Nikova, V. Nikov, and V. Rijmen. Higher-Order Threshold Implementations. ASIACRYPT 2014,

- Correctness
- d^{th}-order non completeness
  - Linear Functions:
    - $s \geq d + 1$

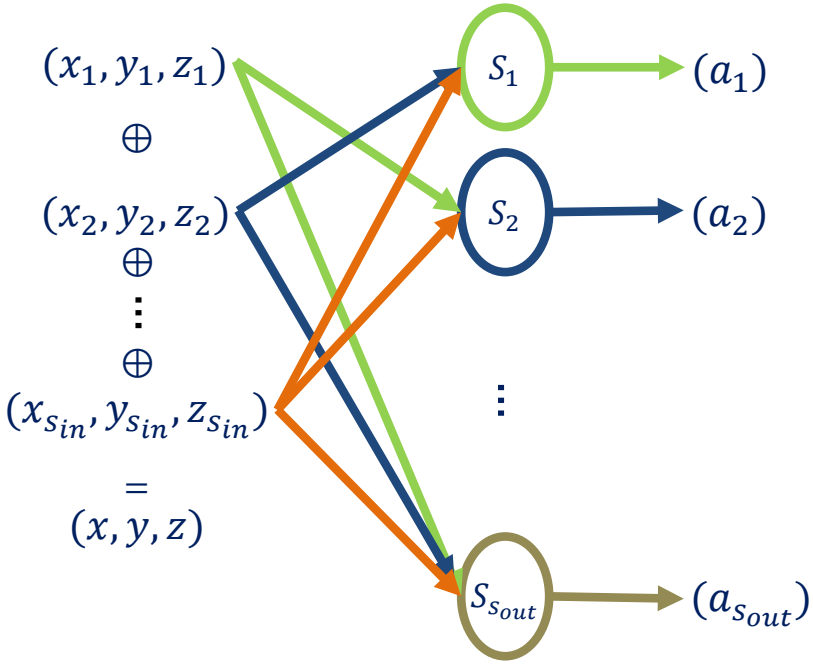


Higher-Order TI

Concept

B. Bilgin, B. Gierlichs, S. Nikova, V. Nikov, and V. Rijmen. Higher-Order Threshold Implementations. ASIACRYPT 2014,

- Correctness
- d^{th}-order non completeness
  - Linear Functions:
    - $s \geq d + 1$
  - Nonlinear Functions:
    - $t =$ algebraic degree
    - $s_{in} \geq td + 1$
    - $s_{out} \geq \binom{s_{in}}{t}$
    - $1^{st}: s_{in} \geq 3, s_{out} \geq 3$
    - $2^{nd}: s_{in} \geq 5, s_{out} \geq 10$

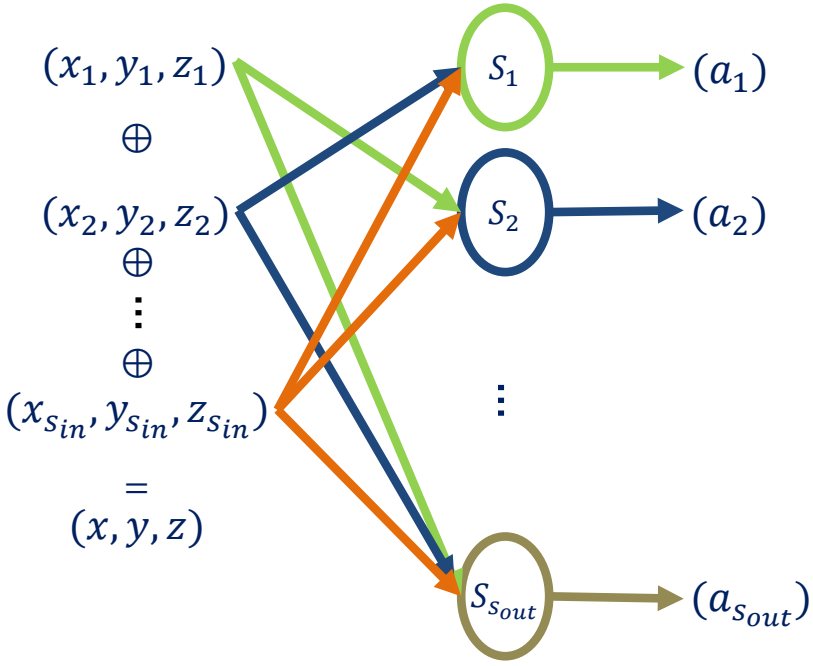


Higher-Order TI

Concept

B. Bilgin, B. Gierlichs, S. Nikova, V. Nikov, and V. Rijmen. Higher-Order Threshold Implementations. ASIACRYPT 2014,

- Correctness
- d^{th}-order non completeness
  - Linear Functions:
    - $s \geq d + 1$
  - Nonlinear Functions:
    - $t =$ algebraic degree
    - $s_{in} \geq td + 1$
    - $s_{out} \geq \binom{s_{in}}{t}$
    - $1^{st}: s_{in} \geq 3, s_{out} \geq 3$
    - $2^{nd}: s_{in} \geq 5, s_{out} \geq 10$
- Uniformity

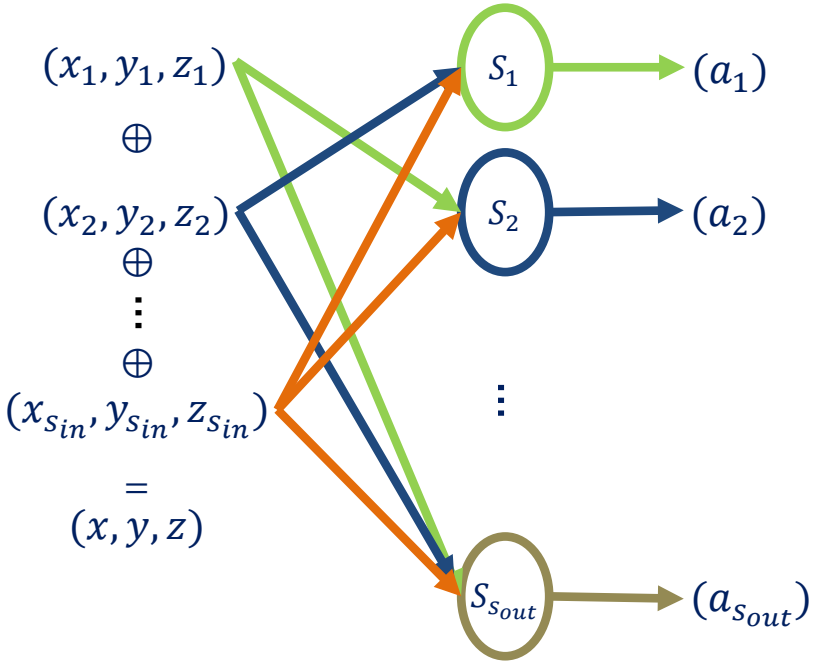


Higher-Order TI

Concept

B. Bilgin, B. Gierlichs, S. Nikova, V. Nikov, and V. Rijmen. Higher-Order Threshold Implementations. ASIACRYPT 2014,

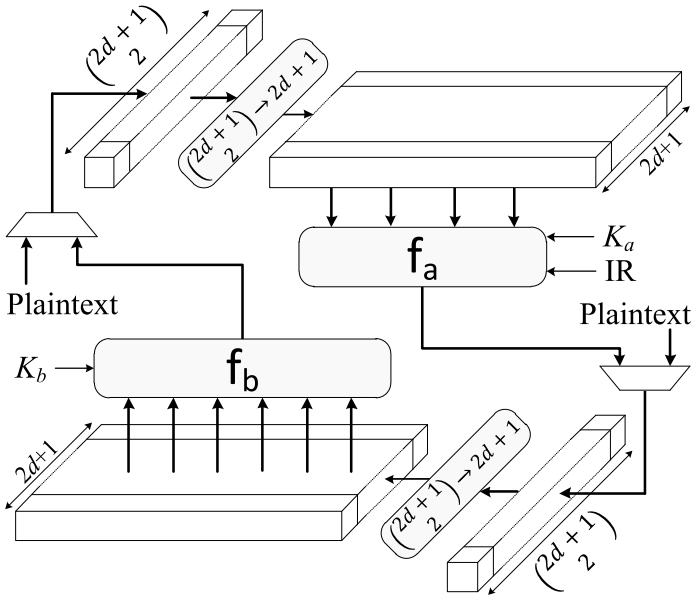
- Correctness
- d^{th}-order non completeness
  - Linear Functions:
    - $s \geq d + 1$
  - Nonlinear Functions:
    - $t =$ algebraic degree
    - $s_{in} \geq td + 1$
    - $s_{out} \geq \binom{s_{in}}{t}$
    - $1^{st}: s_{in} \geq 3, s_{out} \geq 3$
    - $2^{nd}: s_{in} \geq 5, s_{out} \geq 10$
- Uniformity
- Registers after nonlinear functions



Case Studies

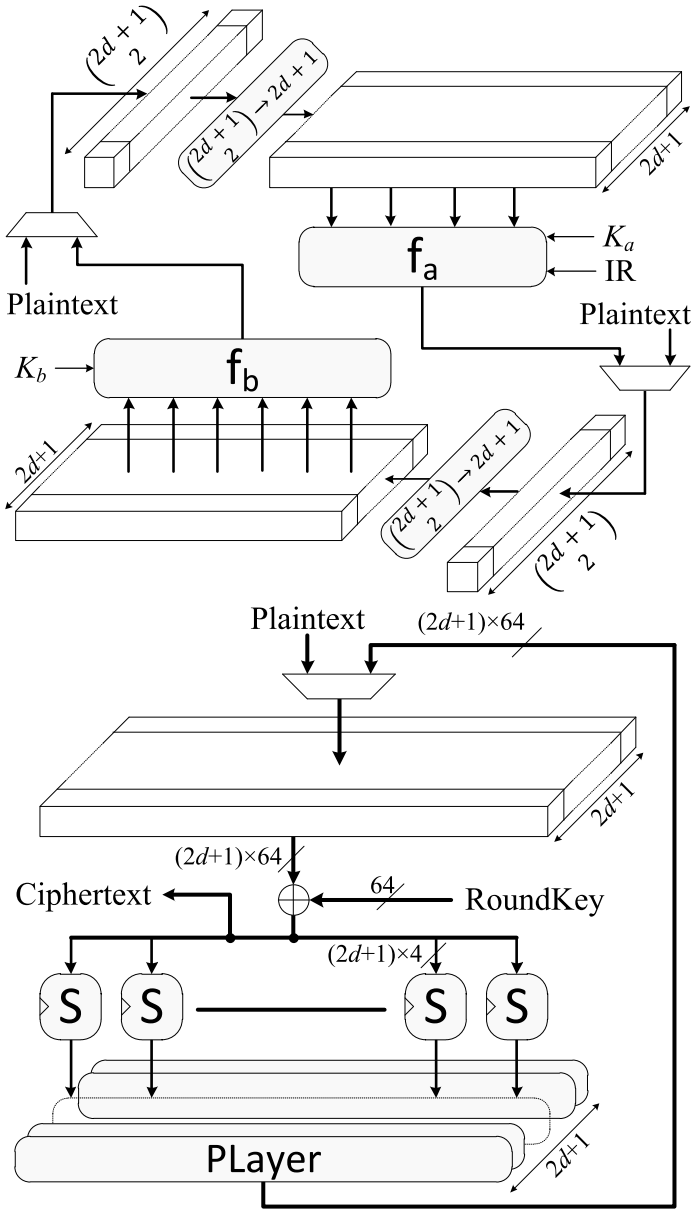
Case Studies

- KATAN-32
  - 1st-order TI
  - 2nd-order TI
  - 1st-order TI by GliFreD



Case Studies

- KATAN-32
  - 1st-order TI
  - 2nd-order TI
  - 1st-order TI by GliFreD
- PRESENT-80
  - 1st-order TI
  - 2nd-order TI
  - 1st-order TI by GliFreD



Higher-Order TI

PRESENT

Higher-Order TI

PRESENT

- S(x) is cubic bijection with t=3

Higher-Order TI

PRESENT

- S(x) is cubic bijection with t=3
- Bilgin, Nikova, Nikov, Rijmen, Tokareva, Vitkup: Threshold implementations of small S-boxes. Cryptography and Communications 7(1): 3-33 (2015)
  - $S(x) = A'\left(C_{266}(A(x))\right)$

Higher-Order TI

PRESENT

- S(x) is cubic bijection with t=3
- Bilgin, Nikova, Nikov, Rijmen, Tokareva, Vitkup: Threshold implementations of small S-boxes. Cryptography and Communications 7(1): 3-33 (2015)
  - $S(x) = A'\left(C_{266}(A(x))\right)$
  - #shares: 1st = 4 ; 2nd = 7

Higher-Order TI

PRESENT

- S(x) is cubic bijection with t=3
- Bilgin, Nikova, Nikov, Rijmen, Tokareva, Vitkup: Threshold implementations of small S-boxes. Cryptography and Communications 7(1): 3-33 (2015)
  - $S(x) = A'\left(C_{266}(A(x))\right)$
  - #shares: 1st = 4 ; 2nd = 7
- Decomposition reduces shares

Higher-Order TI

PRESENT

- S(x) is cubic bijection with t=3
- Bilgin, Nikova, Nikov, Rijmen, Tokareva, Vitkup: Threshold implementations of small S-boxes. Cryptography and Communications 7(1): 3-33 (2015)
  - $S(x) = A'\left(C_{266}(A(x))\right)$
  - #shares: 1st = 4 ; 2nd = 7
- Decomposition reduces shares
  - $S(x) = A_3\left(Q_{299}\left(A_2\left(Q_{294}(A_1(x))\right)\right)\right)$

Higher-Order TI

PRESENT

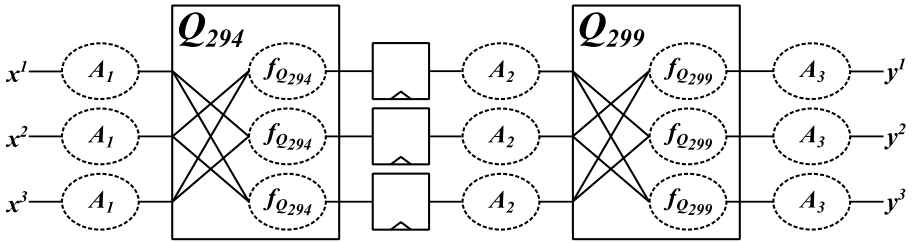
- S(x) is cubic bijection with t=3
- Bilgin, Nikova, Nikov, Rijmen, Tokareva, Vitkup: Threshold implementations of small S-boxes. Cryptography and Communications 7(1): 3-33 (2015)
  - $S(x) = A'\left(C_{266}(A(x))\right)$
  - #shares: 1st = 4 ; 2nd = 7
- Decomposition reduces shares
  - $S(x) = A_3\left(Q_{299}\left(A_2\left(Q_{294}(A_1(x))\right)\right)\right)$
  - #shares: 1st = 3 ; 2nd = 5

Higher-Order TI

PRESENT

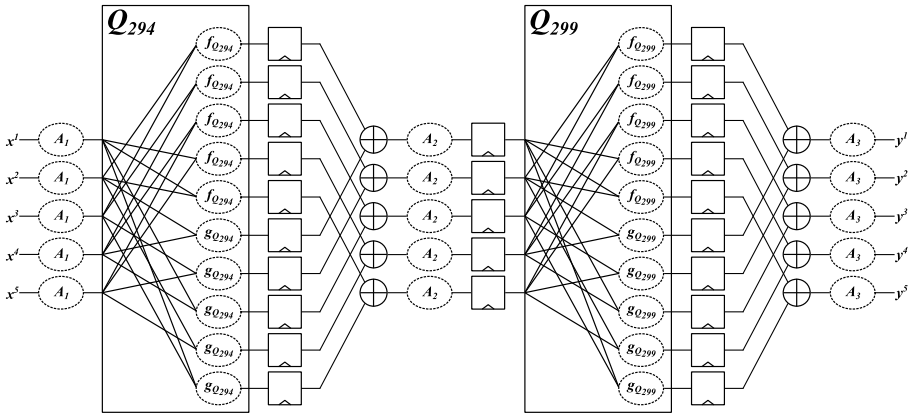
- S(x) is cubic bijection with t=3
- Bilgin, Nikova, Nikov, Rijmen, Tokareva, Vitkup: Threshold implementations of small S-boxes. Cryptography and Communications 7(1): 3-33 (2015)
  - $S(x) = A'\left(C_{266}(A(x))\right)$
  - #shares: 1st = 4 ; 2nd = 7

1ST-ORDER TI



- Decomposition reduces shares
  - $S(x) = A_3\left(Q_{299}\left(A_2\left(Q_{294}(A_1(x))\right)\right)\right)$
  - #shares: 1st = 3 ; 2nd = 5

2ND-ORDER TI



Implementation

Profile	Resources		Frequency	Latency	Pipeline	Throughput
	LUT	FF	(MHz)	(#clock)	(stages)	(Mbit/s)
KATAN-1st	34	96	225.38	273	1	26.42
KATAN-2nd	65	180	321.54	273	1	37.69
KATAN-1st-G	114	548	438.21	546	1	25.68
PRESENT-1st	808	384	206.61	64	2	413.22
PRESENT-2nd	2245	1680	203.46	128	4	406.92
PRESENT-1st-G	5442	12672	458.09	704	11	458.09

Xilinx Spartan-6 FPGA of SAKURA-G

Implementation

- GliFreD circuits form a pipeline with a very short critical path

Profile	Resources		Frequency	Latency	Pipeline	Throughput
	LUT	FF	(MHz)	(#clock)	(stages)	(Mbit/s)
KATAN-1st	34	96	225.38	273	1	26.42
KATAN-2nd	65	180	321.54	273	1	37.69
KATAN-1st-G	114	548	438.21	546	1	25.68
PRESENT-1st	808	384	206.61	64	2	413.22
PRESENT-2nd	2245	1680	203.46	128	4	406.92
PRESENT-1st-G	5442	12672	458.09	704	11	458.09

Xilinx Spartan-6 FPGA of SAKURA-G

Implementation

- GliFreD circuits form a pipeline with a very short critical path
  - Frequency (hence throughput) can be higher than non-GliFreD designs

Profile	Resources		Frequency	Latency	Pipeline	Throughput
	LUT	FF	(MHz)	(#clock)	(stages)	(Mbit/s)
KATAN-1st	34	96	225.38	273	1	26.42
KATAN-2nd	65	180	321.54	273	1	37.69
KATAN-1st-G	114	548	438.21	546	1	25.68
PRESENT-1st	808	384	206.61	64	2	413.22
PRESENT-2nd	2245	1680	203.46	128	4	406.92
PRESENT-1st-G	5442	12672	458.09	704	11	458.09

Xilinx Spartan-6 FPGA of SAKURA-G

Implementation

- GliFreD circuits form a pipeline with a very short critical path
  - Frequency (hence throughput) can be higher than non-GliFreD designs
  - Achievements depend on the application and the design nature

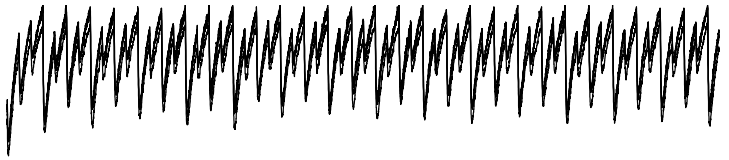
Profile	Resources		Frequency	Latency	Pipeline	Throughput
	LUT	FF	(MHz)	(#clock)	(stages)	(Mbit/s)
KATAN-1st	34	96	225.38	273	1	26.42
KATAN-2nd	65	180	321.54	273	1	37.69
KATAN-1st-G	114	548	438.21	546	1	25.68
PRESENT-1st	808	384	206.61	64	2	413.22
PRESENT-2nd	2245	1680	203.46	128	4	406.92
PRESENT-1st-G	5442	12672	458.09	704	11	458.09

Xilinx Spartan-6 FPGA of SAKURA-G

Welch's t-test

Welch's t-test

- Measure power traces.



Welch's t-test

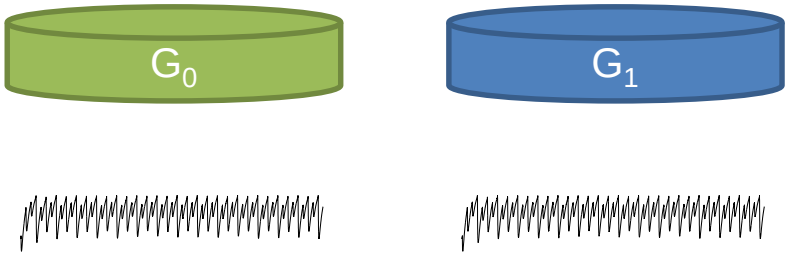
- Measure power traces.
- Determine distinguisher, e.g.:
  - fix vs. random plaintext (*non-specific t*-test)

Welch's t-test

- Measure power traces.
- Determine distinguisher, e.g.:
  - fix vs. random plaintext (*non-specific t*-test)
- Group traces depending on distinguisher.

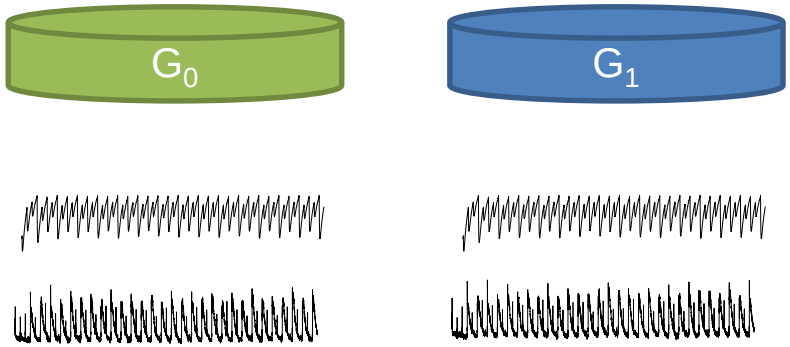
Welch's t-test

- Measure power traces.
- Determine distinguisher, e.g.:
  - fix vs. random plaintext (*non-specific t*-test)
- Group traces depending on distinguisher.
- Compute *sample mean* for each point in time.



Welch's t-test

- Measure power traces.
- Determine distinguisher, e.g.:
  - fix vs. random plaintext (*non-specific t*-test)
- Group traces depending on distinguisher.
- Compute *sample mean* for each point in time.
- Compute *sample variance* for each point in time.



Welch's t-test

- Measure power traces.
- Determine distinguisher, e.g.:
  - fix vs. random plaintext (*non-specific t*-test)
- Group traces depending on distinguisher.
- Compute *sample mean* for each point in time.
- Compute *sample variance* for each point in time.
- Determine *t*-statistic for each point in time:

$$t = \frac{\mu(T \in G_1) - \mu(T \in G_0)}{\sqrt{\frac{\delta^2(T \in G_1)}{|G_1|} + \frac{\delta^2(T \in G_0)}{|G_0|}}}$$

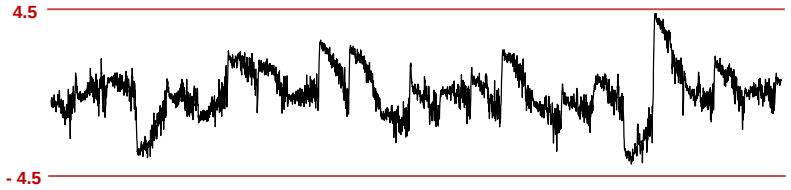
Where μ denotes the *sample mean* and δ denotes the *sample variance*.

Welch's t-test

- Measure power traces.
- Determine distinguisher, e.g.:
  - fix vs. random plaintext (*non-specific t*-test)
- Group traces depending on distinguisher.
- Compute *sample mean* for each point in time.
- Compute *sample variance* for each point in time.
- Determine *t*-statistic for each point in time:

$$t = \frac{\mu(T \in G_1) - \mu(T \in G_0)}{\sqrt{\frac{\delta^2(T \in G_1)}{|G_1|} + \frac{\delta^2(T \in G_0)}{|G_0|}}}$$

Where μ denotes the *sample mean* and δ denotes the *sample variance*.



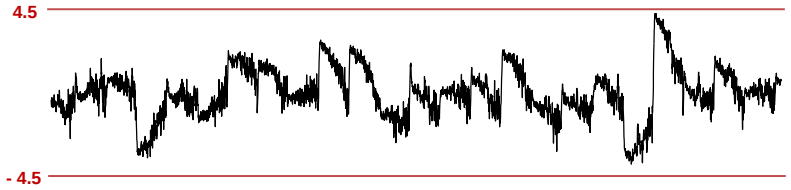
Fail/Pass Criteria: If there is any point in time for which the t-statistic exceeds a threshold of $\pm$ 4.5 the device under test fails.

Welch's t-test

- Measure power traces.
- Determine distinguisher, e.g.:
  - fix vs. random plaintext (*non-specific t*-test)
- Group traces depending on distinguisher.
- Compute *sample mean* for each point in time.
- Compute *sample variance* for each point in time.
- Determine *t*-statistic for each point in time:

$$t = \frac{\mu(T \in G_1) - \mu(T \in G_0)}{\sqrt{\frac{\delta^2(T \in G_1)}{|G_1|} + \frac{\delta^2(T \in G_0)}{|G_0|}}}$$

Where μ denotes the *sample mean* and δ denotes the *sample variance*.



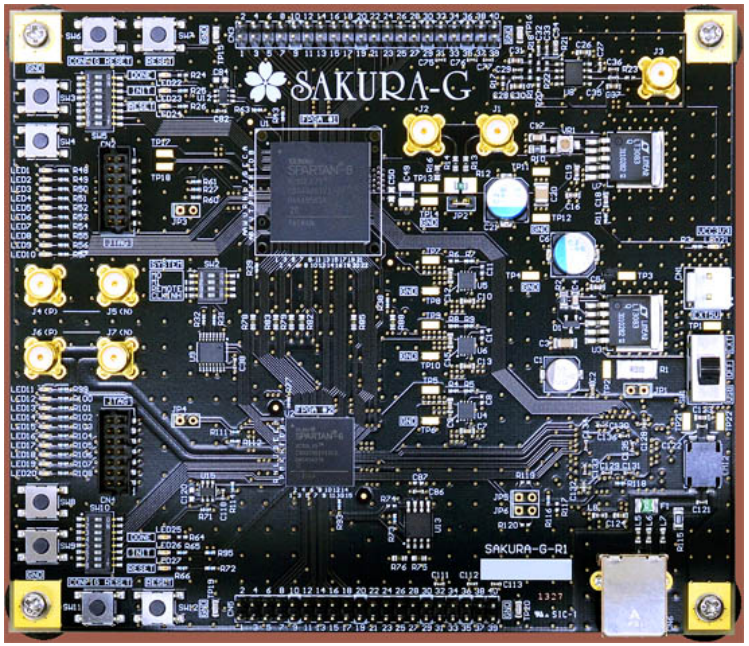
Fail/Pass Criteria: If there is any point in time for which the t-statistic exceeds a threshold of $\pm$ 4.5 the device under test fails.

T. Schneider, A. Moradi. Leakage Assessment Methodology - a clear roadmap for side-channel evaluations. CHES 2015

Evaluation

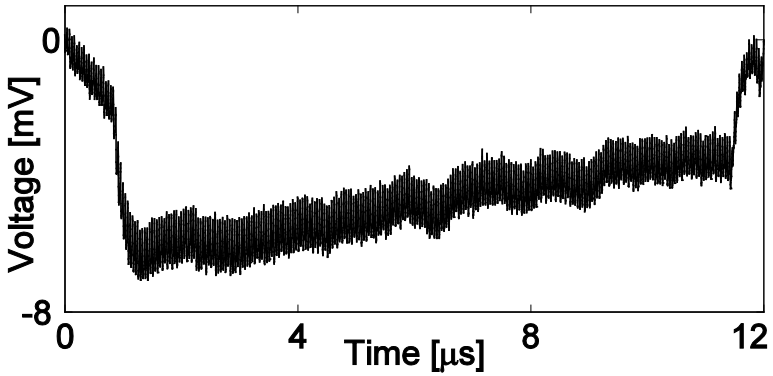
Setup

- SAKURA-G
- Running the designs @ 24MHz
- Measurements with 500MS/s
- Several million traces
- Non-specific *t*-test
  - 1st- to 5th-order
  - Depends on used shares

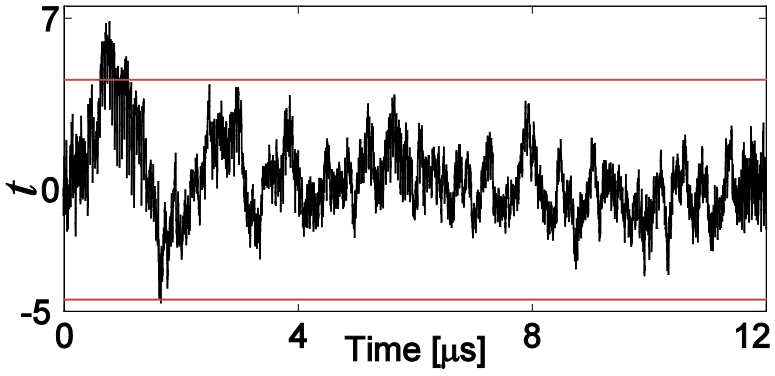


Evaluation

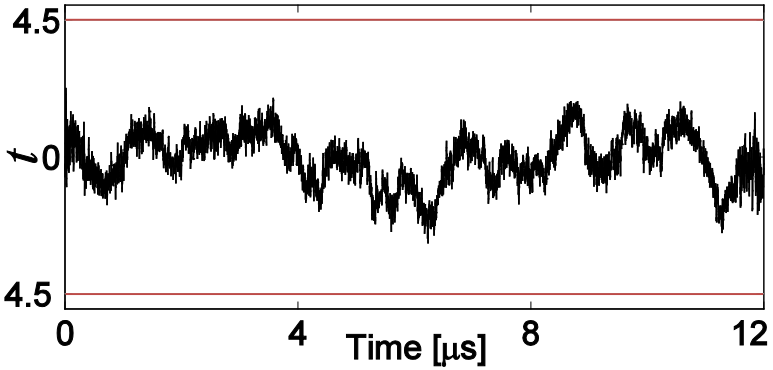
KATAN-1 ST (1 Million Traces)



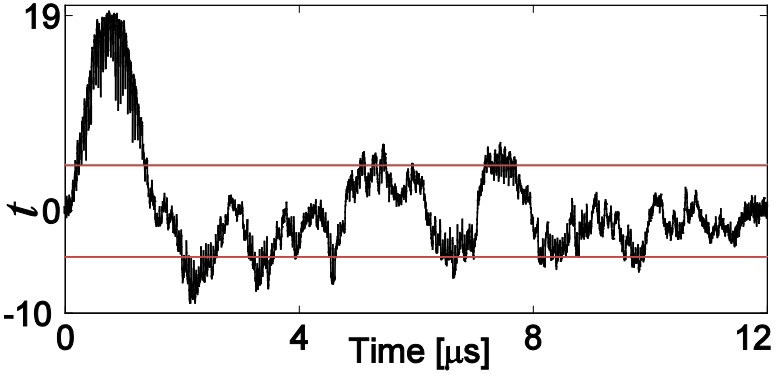
Sample Trace



Second-Order



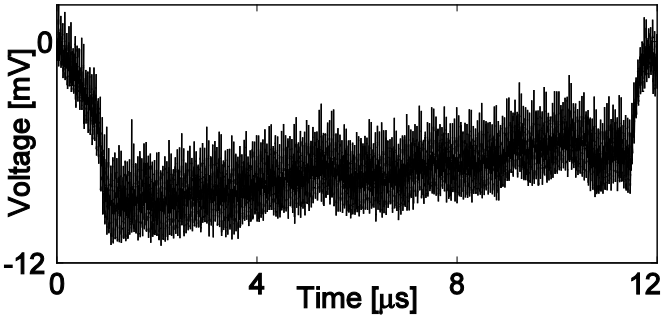
First-Order



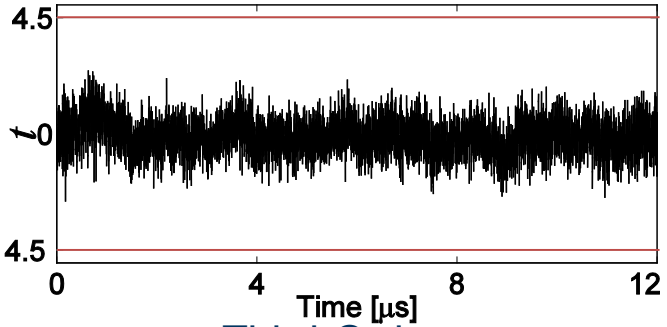
Third-Order

Evaluation

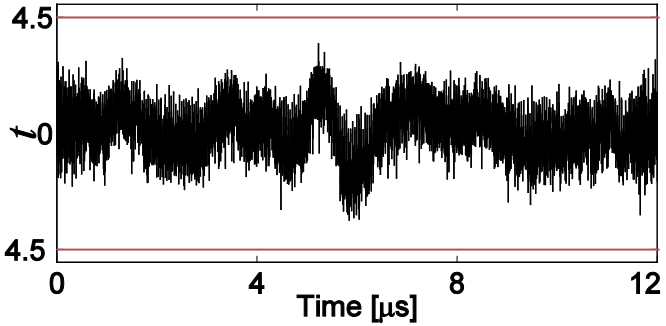
KATAN-2ND (100 Million Traces)



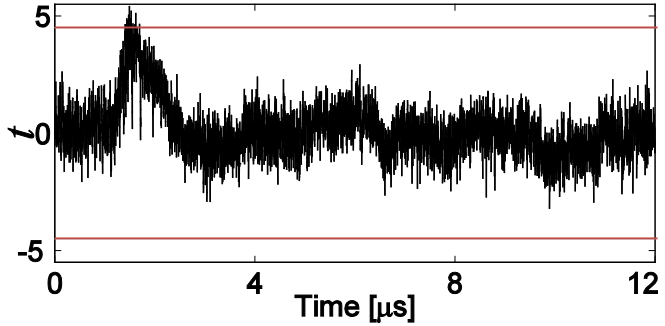
Sample Trace



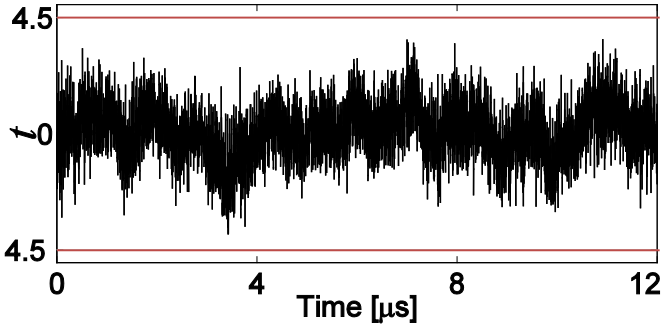
Third-Order



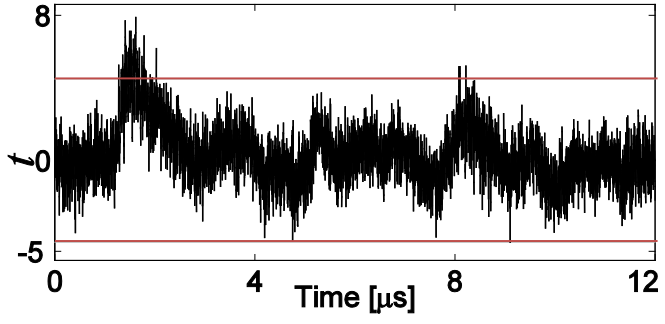
First-Order



Fourth-Order



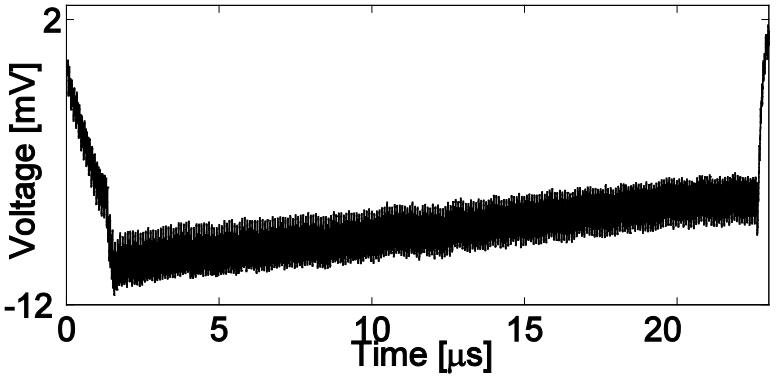
Second-Order



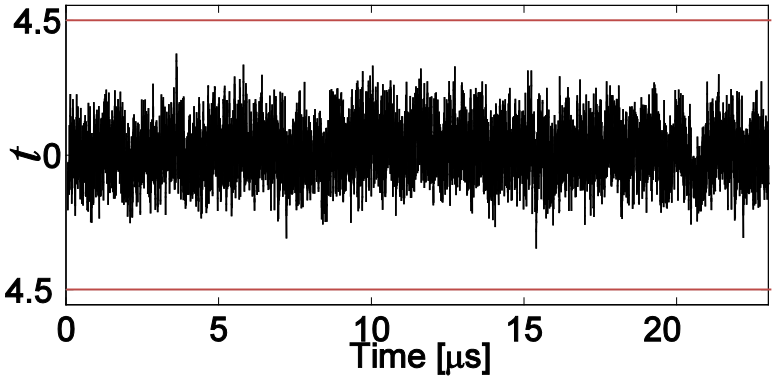
Fifth-Order

Evaluation

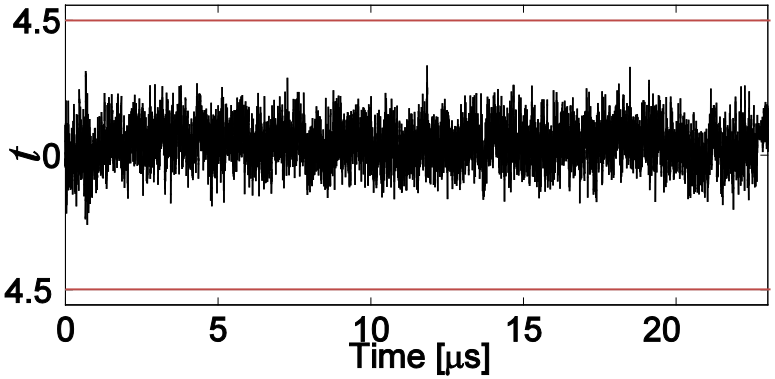
KATAN-1ST-G (1 Billion Traces)



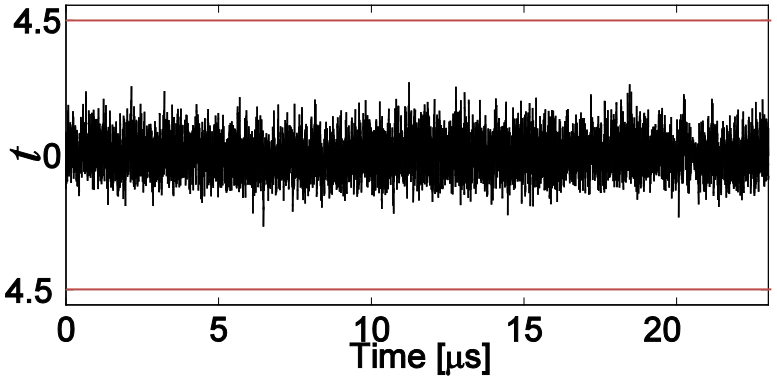
Sample Trace



Second-Order



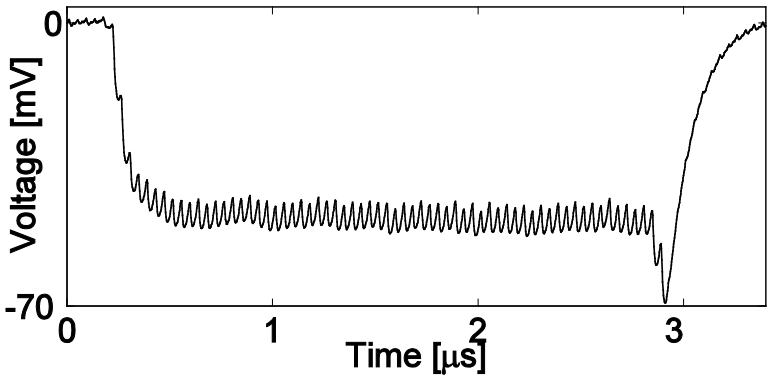
First-Order



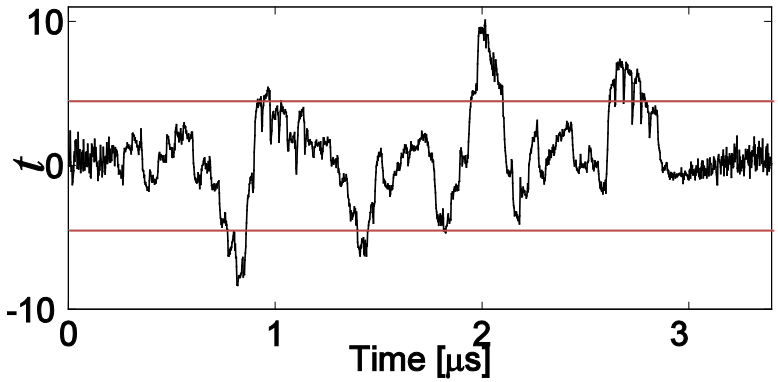
Third-Order

Evaluation

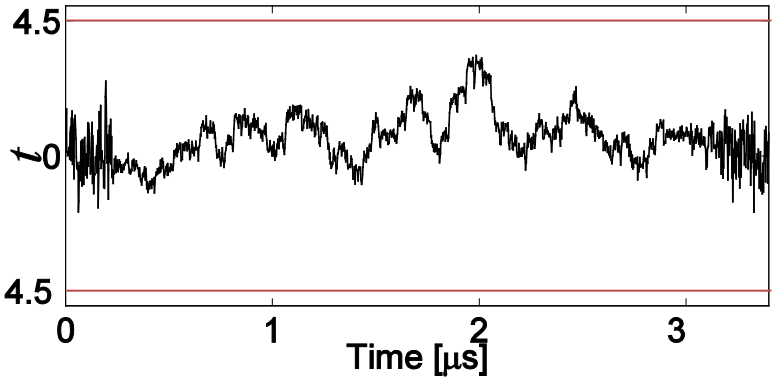
PRESENT-1ST (10 Million Traces)



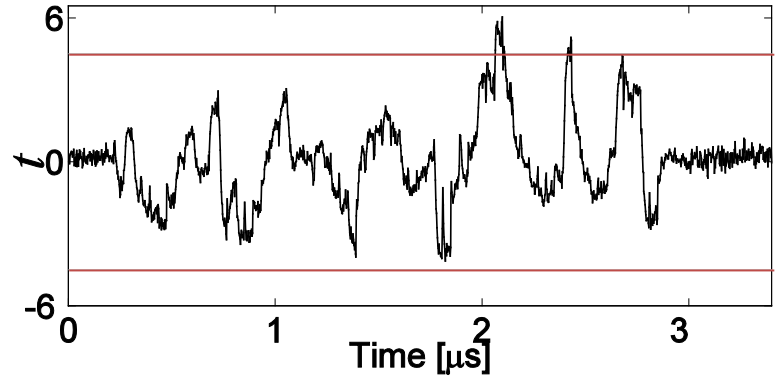
Sample Trace



Second-Order



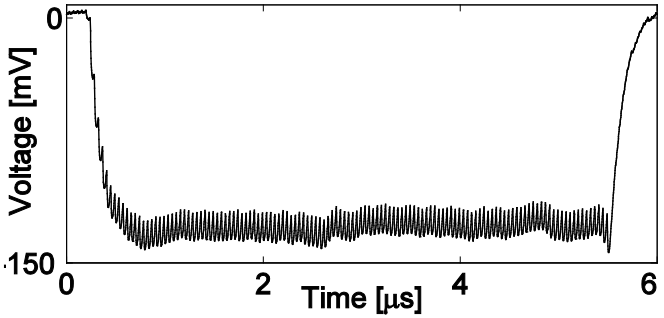
First-Order



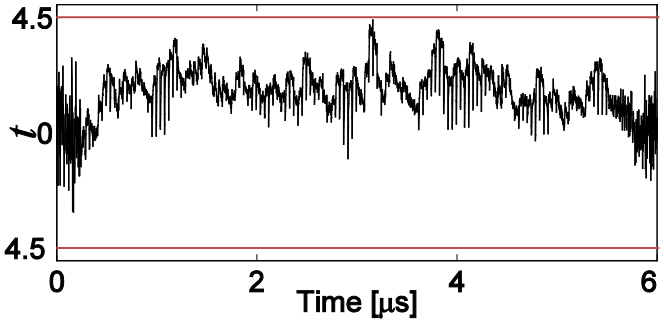
Third-Order

Evaluation

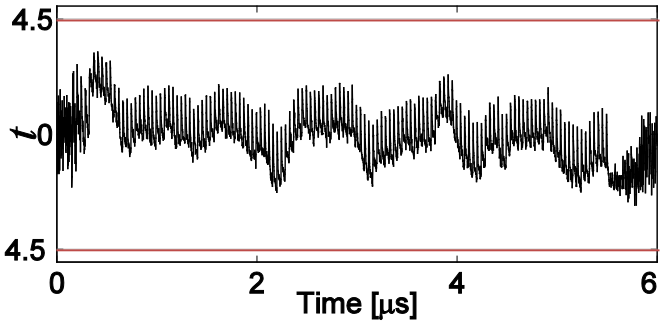
PRESENT-2ND (300 Million Traces)



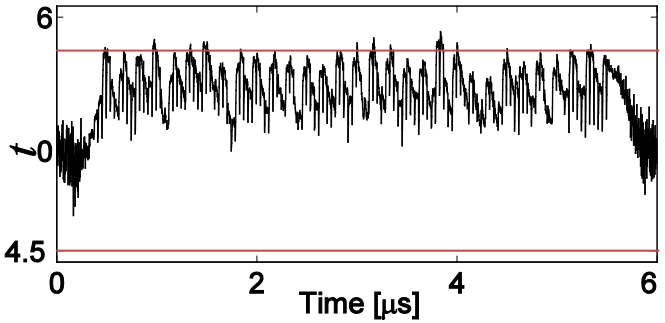
Sample Trace



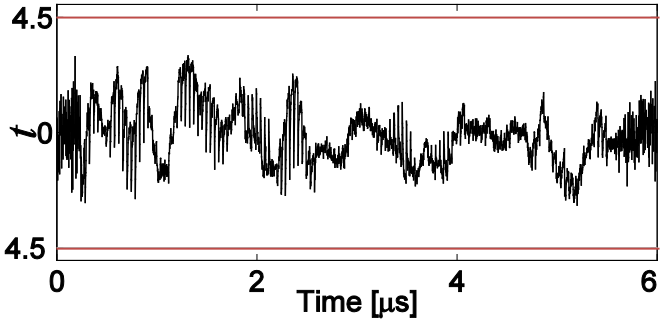
Third-Order



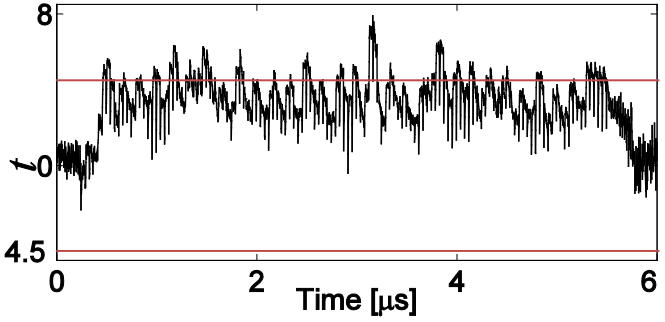
First-Order



Fourth-Order



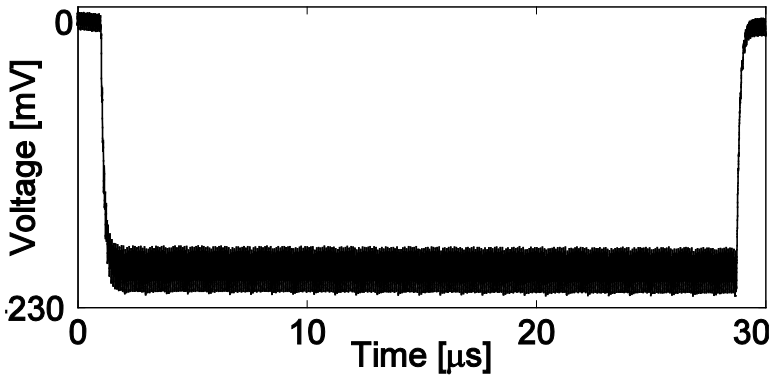
Second-Order



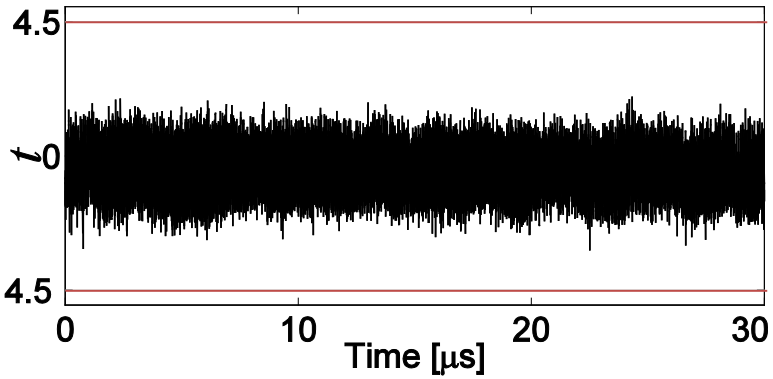
Fifth-Order

Evaluation

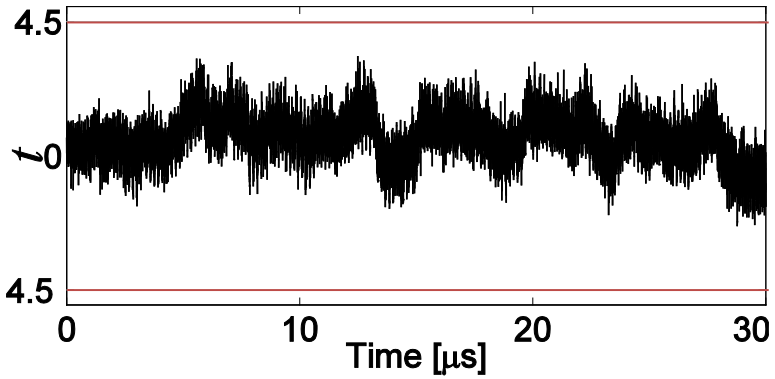
PRESENT-1ST-G (1 Billion Traces)



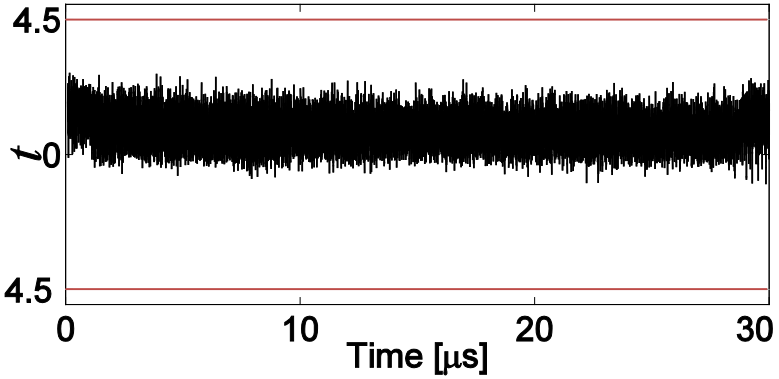
Sample Trace



Second-Order



First-Order



Third-Order

Conclusion

Conclusion

GliFreD + TI

Conclusion

GliFreD + TI

- Consumes more power

Conclusion

GliFreD + TI

- Consumes more power
  - Higher resource utilization

Conclusion

GliFreD + TI

- Consumes more power
  - Higher resource utilization
  - Natural behavior of power equalization

Conclusion

GliFreD + TI

- Consumes more power
  - Higher resource utilization
  - Natural behavior of power equalization
- Increases latency

Conclusion

GliFreD + TI

- Consumes more power
  - Higher resource utilization
  - Natural behavior of power equalization
- Increases latency
  - Design and application dependent

Conclusion

GliFreD + TI

- Consumes more power
  - Higher resource utilization
  - Natural behavior of power equalization
- Increases latency
  - Design and application dependent
  - Increases frequency → comparable throughput

Conclusion

GliFreD + TI

- Consumes more power
  - Higher resource utilization
  - Natural behavior of power equalization
- Increases latency
  - Design and application dependent
  - Increases frequency → comparable throughput
- Restricted to FPGAs

Conclusion

GliFreD + TI

- Consumes more power
  - Higher resource utilization
  - Natural behavior of power equalization
- Increases latency
  - Design and application dependent
  - Increases frequency → comparable throughput
- Restricted to FPGAs
  - ASIC: DPL + TI might have similar security level

Conclusion

GliFreD + TI

- Consumes more power
  - Higher resource utilization
  - Natural behavior of power equalization
- Increases latency
  - Design and application dependent
  - Increases frequency → comparable throughput
- Restricted to FPGAs
  - ASIC: DPL + TI might have similar security level
- No provable resistance for higher-order

Conclusion

GliFreD + TI

- Consumes more power
  - Higher resource utilization
  - Natural behavior of power equalization
- Increases latency
  - Design and application dependent
  - Increases frequency → comparable throughput
- Restricted to FPGAs
  - ASIC: DPL + TI might have similar security level
- No provable resistance for higher-order
  - Still 1st-order secure

Conclusion

GliFreD + TI

- Consumes more power
  - Higher resource utilization
  - Natural behavior of power equalization
- Increases latency
  - Design and application dependent
  - Increases frequency → comparable throughput
- Restricted to FPGAs
  - ASIC: DPL + TI might have similar security level
- No provable resistance for higher-order
  - Still 1st-order secure
- Higher-order attacks practically infeasible

Conclusion

GliFreD + TI

- Consumes more power
  - Higher resource utilization
  - Natural behavior of power equalization
- Increases latency
  - Design and application dependent
  - Increases frequency → comparable throughput
- Restricted to FPGAs
  - ASIC: DPL + TI might have similar security level
- No provable resistance for higher-order
  - Still 1st-order secure
- Higher-order attacks practically infeasible
  - EM analysis

Conclusion

GliFreD + TI

- Consumes more power
  - Higher resource utilization
  - Natural behavior of power equalization
- Increases latency
  - Design and application dependent
  - Increases frequency → comparable throughput
- Restricted to FPGAs
  - ASIC: DPL + TI might have similar security level
- No provable resistance for higher-order
  - Still 1st-order secure
- Higher-order attacks practically infeasible
  - EM analysis
  - Fair to compare with 3rd-order TI

Thanks for Listening!

Any Questions?