# Comparing the Cost of Protecting Selected Lightweight Block Ciphers Against Differential Power Analysis in Low-Cost FPGA

**William Diehl**, Abubakr Abdulgadir, Jens-Peter Kaps and Kris Gaj

*ECE Department, George Mason University, Fairfax, Virginia, USA*

*http://cryptography.gmu.edu*

12/11/2017

# Outline

- Introduction
- Background
- Methodology
- Results
- Conclusion

# Introduction

# Introduction

- Lightweight cryptography suitable for Internet of Things (IoT)
    - ➢ Small devices constrained by resources, power, energy
- CAESAR Competition
    - ➢ Lightweight authenticated ciphers in resource-constrained platforms
    - ➢ Evaluation of resistance to side-channel attack
- NIST Lightweight Cryptography Project
    - ➢ Evaluate algorithms based on physical, performance, security
- Side-channel attack
    - ➢ Measurement of physical phenomena used to recover sensitive information
    - ➢ Power analysis side-channel attack (e.g. Differential Power Analysis DPA)

# Introduction (cont'd)

- Implement AES, SIMON, SPECK, PRESENT, LED & TWINE
  - ➢ Primitives for CAESAR Round 3 Candidate Authenticated Ciphers
- Show that ciphers vulnerable to DPA through t-test
- Protect against 1st order DPA with equivalent level of protection
- Verify protection against 1st DPA
- Compare costs of protection (area, throughput, power, energy)

# Contributions of this Research

- Large-scale comparison of side-channel resistance and evaluation of countermeasures in lightweight block ciphers
  - Supports CAESAR Competition & NIST Lightweight Cryptography Project
  - Moderate speed/Moderate area optimization target (TP/A ratio)
- Validates Use-case of T-test leakage detection methodology in lieu of attack-based testing
  - Not feasible (at budget) through attack-based testing
- Quantification of effects of anti-optimization constraints in FPGA

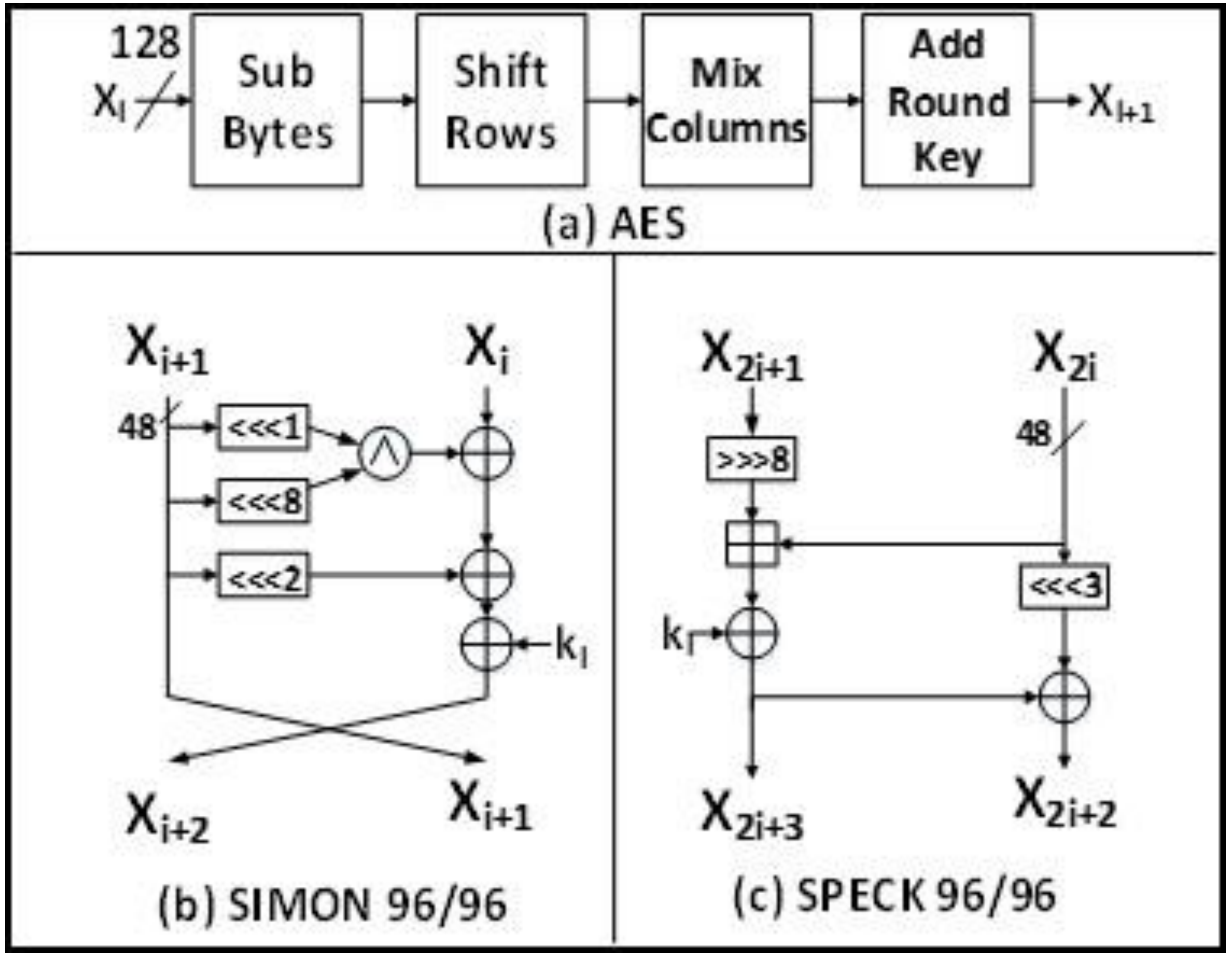
# Background

# Block Ciphers in this Research

| Cipher | Block Size | Key Size | Rounds | Type | Authenticated Ciphers |
|---|---|---|---|---|---|
| AES | 128 | 128 | 10 | SPN | CLOC, SILC, JAMBU |
| SIMON 96/96 | 96 | 96 | 52 | Feistel, ARX | JAMBU |
| SPECK 96/96 | 96 | 96 | 28 | Feistel, ARX | |
| PRESENT 64/80 | 64 | 80 | 31 | SPN | SILC |
| LED 64/80 | 64 | 80 | 48 | SPN | SILC |
| TWINE 64/80 | 64 | 80 | 36 | SPN | CLOC |

Block cipher versions match primitives used in CAESAR Round 3 Authenticated Cipher Candidates

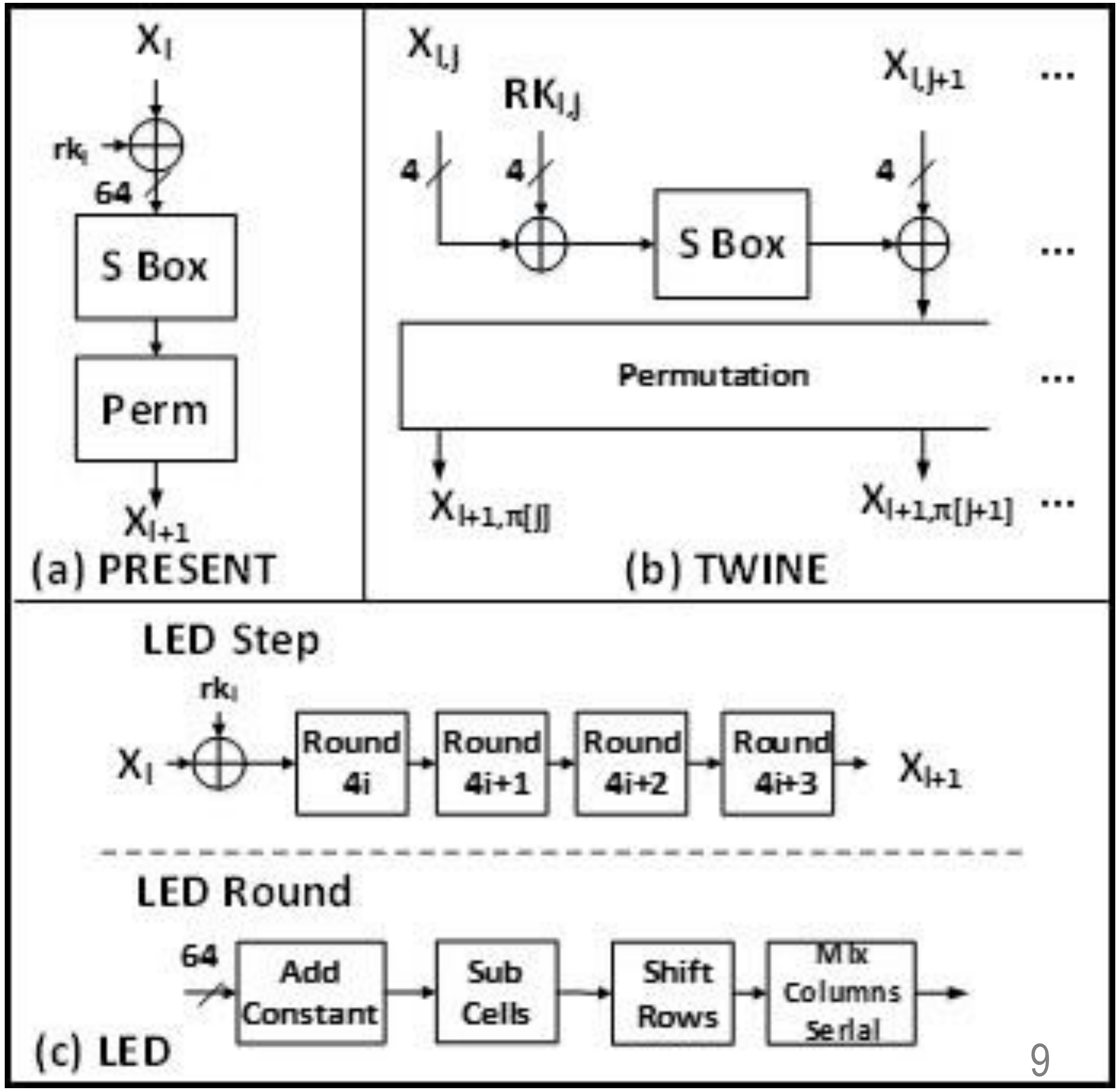
# Block Ciphers in this Research (cont’d)



(a) AES

(b) SIMON 96/96

(c) SPECK 96/96



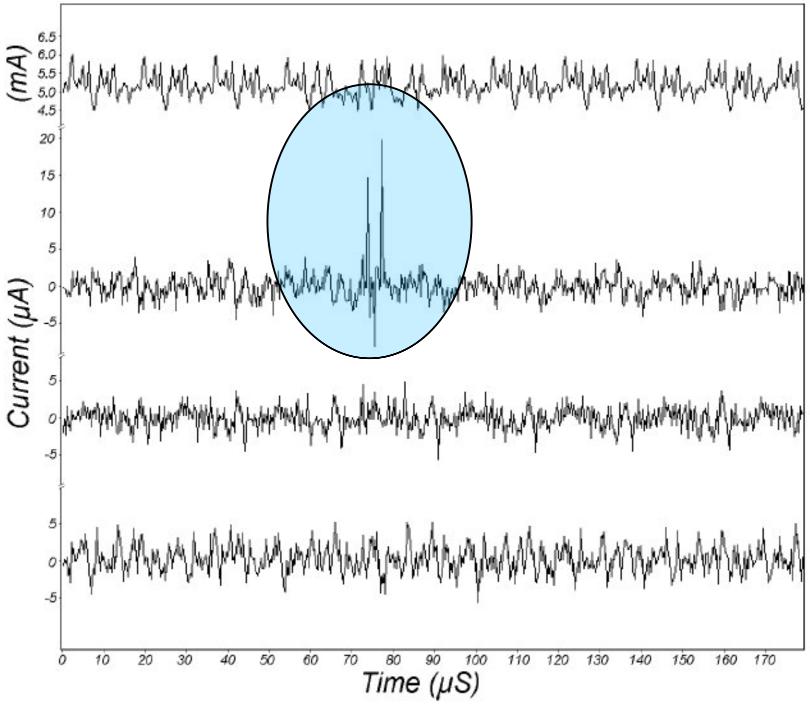
(a) PRESENT

(b) TWINE

(c) LED

# Differential Power Analysis

- Look for correlations of a guessed sub key to intermediate values at a vulnerable point
  - ➢ Measure statistical outcomes of many power analyses
  - ➢ Test hypothesis outcomes to reveal presence of 0 or 1 in a single bit
- 1st order DPA: Examining statistical correlation of 1 intermediate bit[1,2]



University of Colorado “Side Channel Attacks”

[1] – P. C. Kocher, J. Jaffe, and B. Jun, “Differential Power Analysis,” 1999

[2] - P. Kocher, J. Jaffe, B. Jun, and P. Rohatgi, “Introduction to Differential Power Analysis,” 2011

# Countermeasure to DPA: Threshold Implementations[1]

- Data separated into two or more “shares”
- To share function of degree *d*, *d*+1 shares are required (i.e., $z = xy$ has algebraic degree 2, needs 3 shares)
- Secure in presence of glitches, but can be costly and complex
- Properties
  - ➢ ***Non-completeness***. Every function is independent of at least one share of each of the input variables.
  - ➢ ***Correctness***. The sum of the output shares gives the desired output.
  - ➢ ***Uniformity***. Output distribution should preserve input distribution.

1 – S. Nikova, C. Rechberger and V. Rijmen, “Threshold Implementations Against Side-Channel Attacks and Glitches,” 2006

# Leakage Detection using Welch's t-test[1]

<u>Advantages</u>

Find leakage without attack

Don't need power model

Don't need to know architecture

<u>Disadvantages</u>

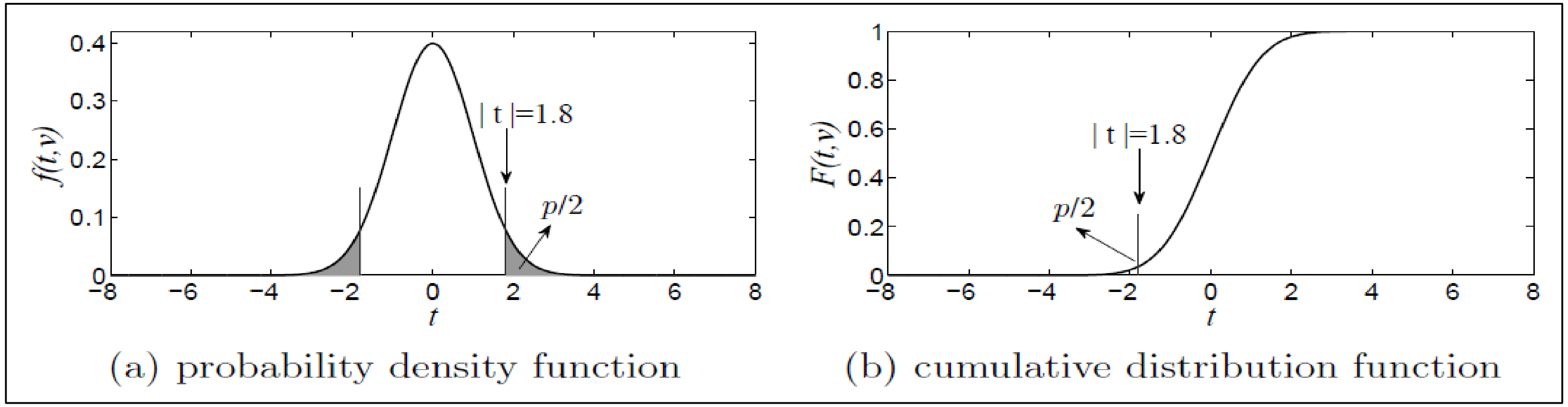
Doesn't recover key

Doesn't show difficulty of attack

$$t = \frac{\mu_0 - \mu_1}{\sqrt{\frac{{s_0}^2}{n_0} + \frac{{s_1}^2}{n_1}}}$$

$$p = 2\int_{|t|}^{\infty} f(t,v)dt$$

$$p = 2F(-4.5, v\ > 1000) < -0.00001$$



(a) probability density function

(b) cumulative distribution function

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

Null hypothesis ($H_0$): "Distributions $Q_0$ and $Q_1$ are not distinguishable."

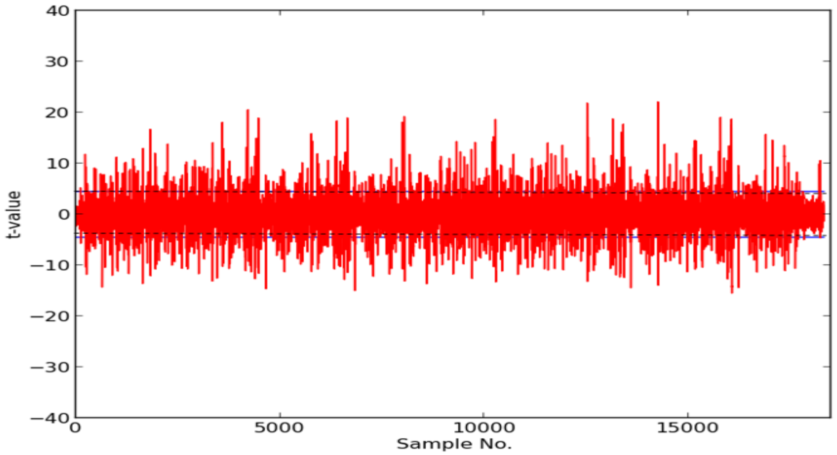
If |*t*| > 4.5 we reject $H_0$ (with 99.999% probability) and conclude "$Q_0$ and $Q_1$ are distinguishable" (i.e., (some sort of) information leaks)

[1] – G. Goodwill, B. Jun, J. Jaffe and P. Rohatgi, "A testing methodology for side channel resistance validation," 2011.

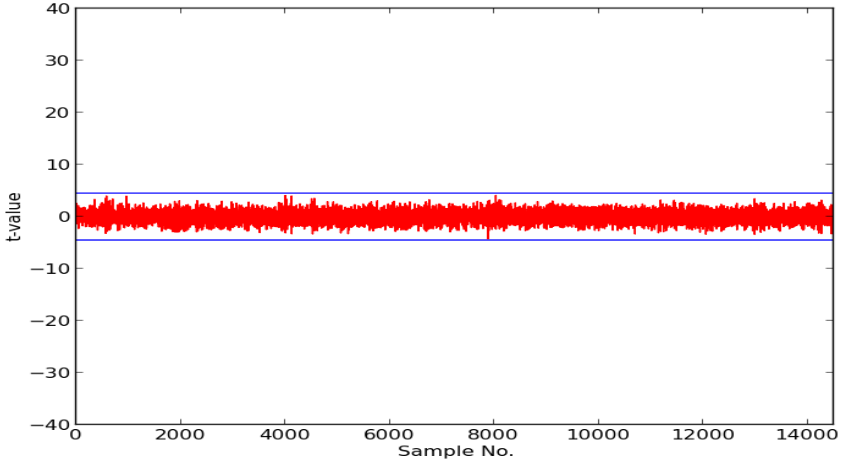
[2] - T. Schneider and A. Moradi, "Leakage Assessment Methodology", 2016

# Leakage Assessment using t-test

T-test fails; |t|>4.5; design leaks information



T-test does not fail; |t|<4.5; leakage not detected



Measure of Effectiveness: “Leaks or doesn’t leak”

# Methodology

# Approach

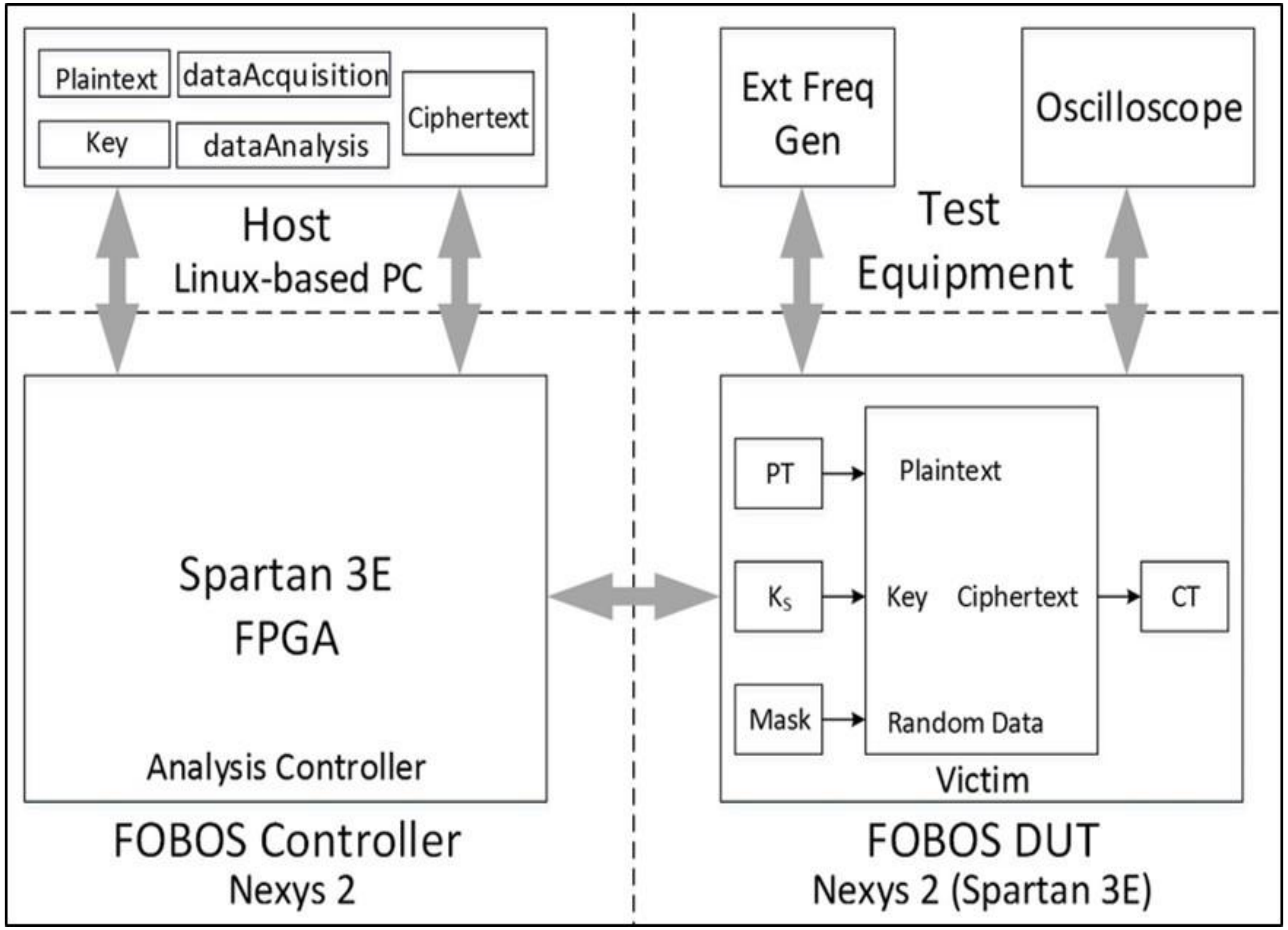
- Start with unprotected full-width datapath, basic iterative architectures[1]
  - Optimization target: TP/A ratio
- Perform t-tests on unprotected ciphers using FOBOS test bench
- Protected with maximum of 3-share Threshold Implementation
  - If full-width/basic-iterative not feasible, change architecture
- Retest w/FOBOS; verify resistance to 1st order DPA
- Benchmark in FPGA, compare in terms of area, throughput, throughput-to-area (TP/A), power, energy-bit
  - Ensure comparison of analogous architectures

[1] - W. Diehl, F. Farahmand, P. Yalla, J. P. Kaps and K. Gaj, "Comparison of hardware and software implementations of selected lightweight block ciphers," 2017

# Flexible Open-source workBench fOr Side-channel analysis (FOBOS)

Agilent Technologies DSO6054A Oscilloscope, Instek SFG-2120 20 MHz Function Generator, Agilent E3620A DC power supply

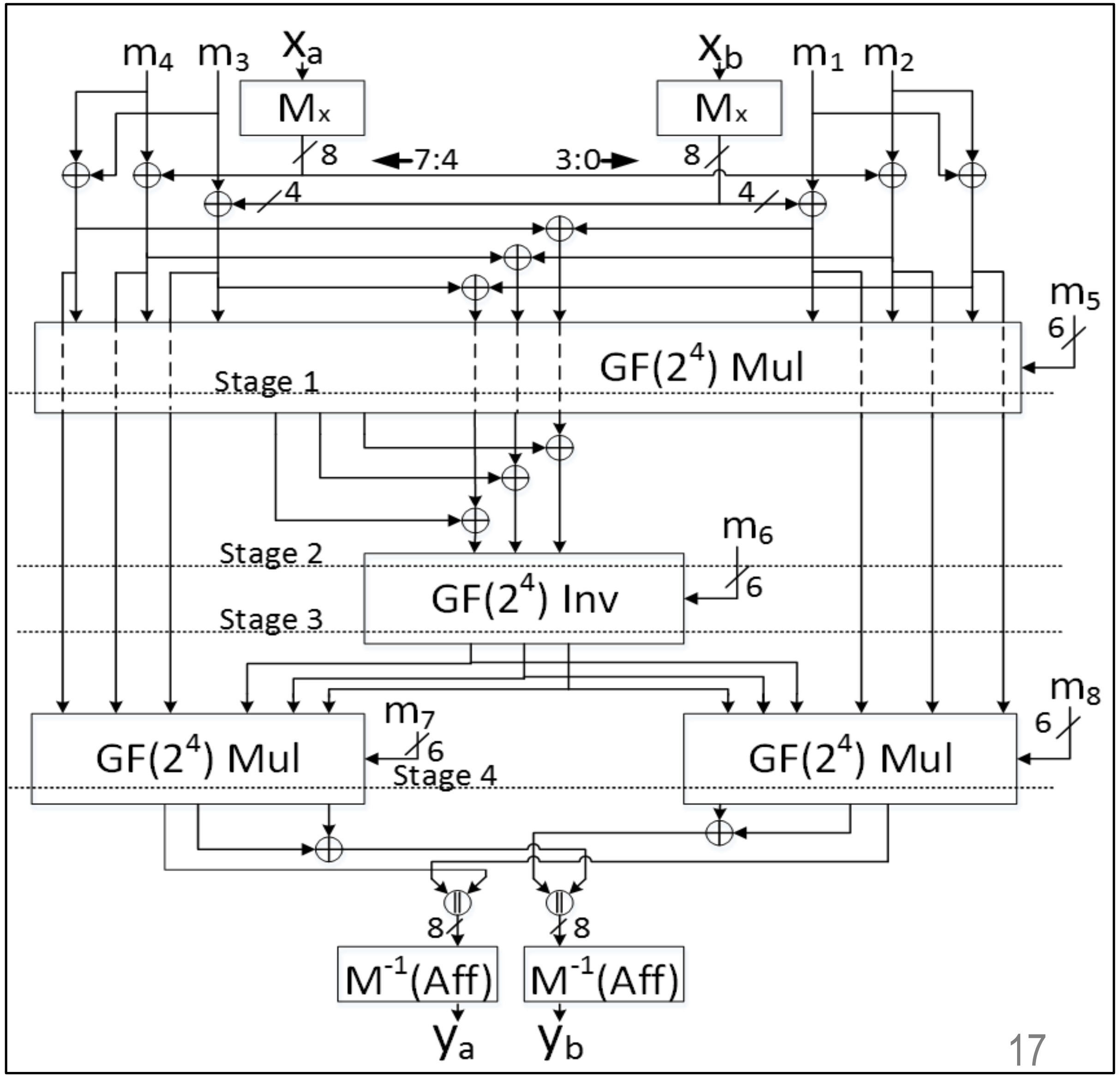
Control Board (Diligent Nexys 2), Victim Board (Spartan 3 FPGA), connected by custom PCB



Additional detail available at https://cryptography.gmu.edu/fobos/

# Protection of AES[1 – 4]

- Hybrid 2- / 3-share protection
- S-Box protected using Tower Fields
  - GF($2^8$) -> GF($2^4$) -> GF($2^2$)
  - However, single 8-bit S-Box very costly
  - Cannot get full-width/basic iterative AES
- 8-bit, 5-stage pipelined AES
- One 3-share TI-protected S-Box
  - 17 cycles/round -> 175 cycles/block
  - 40 random bits/cycle
  - Externally-supplied randomness



[1] - D. Canright and L. Batina, "A Very Compact 'Perfectly Masked' S-Box for AES, 2008

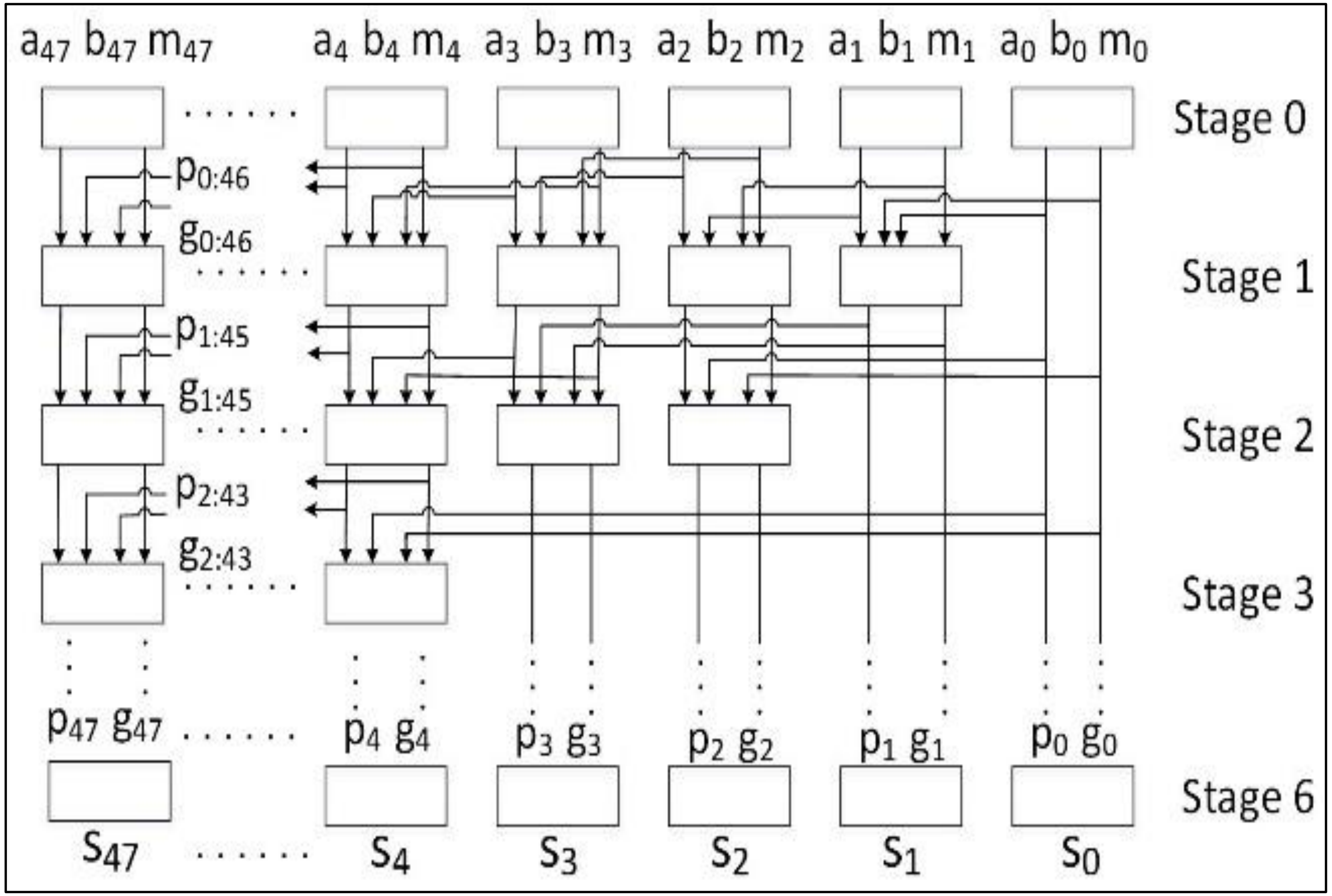
[2] - K. Gaj and P. Chodowiec, "FPGA and ASIC Implementations of AES," 2009

[3] - B. Bilgin, B. Gierlichs, S. Nikova, V. Nikov and V. Rijmen, "A More Efficient AES Threshold Implementation," 2014

[4] - A. Moradi, A. Poschmann, S. Ling, C. Paar and H. Wang, "Pushing the Limits: A Very Compact and a Threshold Implementation of AES," 2011

# Protection of SPECK

- Addition modulo $2^{48}$
  - Boolean-to-Arithmetic masking
  - Pure Boolean approach
- Kogge-Stone Adder[1,2]
  - Recursive Generate/Propagate
  - $\lceil log_2 k \rceil + 1$ stages ($k$ = 48 bits)
  - 273 random bits for $2^{48}$ adder
- Basic-iterative arch fails t-test
  - Likely because of glitches
- 8-cycle / round protection
  - 34 random bits / cycle



[1] - T. Schneider, A. Moradi and T. Güneysu, “Arithmetic Addition over Boolean Masking,” 2015

[2] - P. Kogge and H. Stone, "A Parallel Algorithm for the Efficient Solution of a General Class of Recurrence Equations,“ 1973

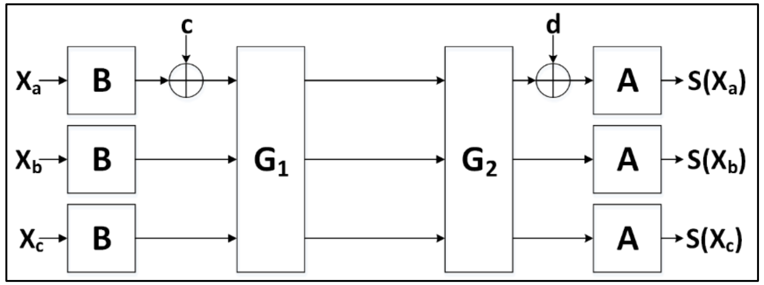
# Protection of SIMON, PRESENT, LED and TWINE

## SIMON

- Simplest 3-share TI protection[1]
- 1 2-input 48-bit AND gate
- Uniformity satisfied by inclusion of round keys

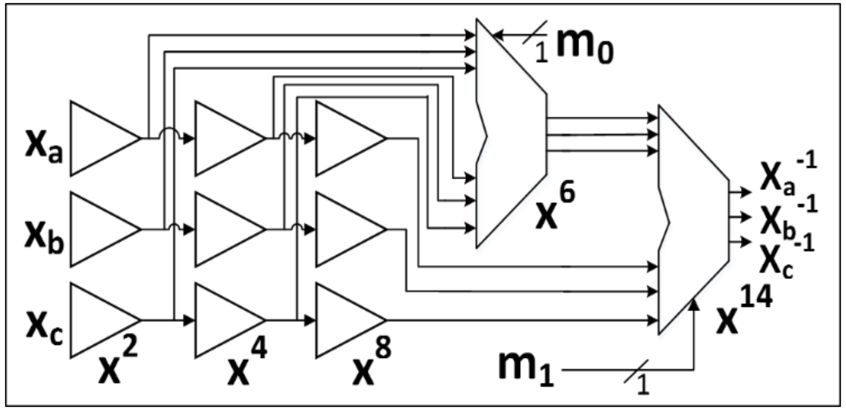
## PRESENT & LED

- 4-bit S-Box of degree 3
- Decomposed into two quadratic functions[2,3]
- Permutations – no refresh randomness required



## TWINE

- 4-bit S-Box of degree 3
- $x^{14} \equiv x^{-1}$ in GF($2^4$)
- Refresh randomness required



Successful full-width datapaths with basic iterative architectures for protected versions

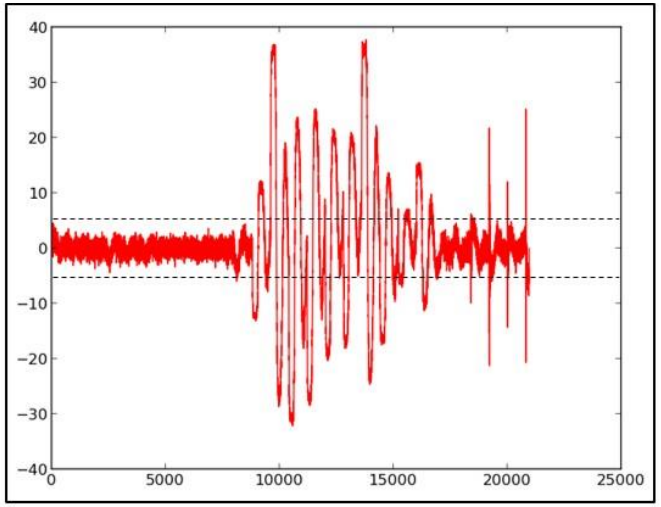
1 - A. Shahverdi, M. Taha and T. Eisenbarth, "Lightweight Side Channel Resistance: Threshold Implementations of Simon,“ 2017
2 - A. Poschmann, A. Moradi, K. Khoo, C. Lim, H. Wang and S. Ling, “Side-Channel Resistant Crypto for Less than 2,300 GE,” 2011
3 - S. Kutzner, P. Nguyen, A. Poschmann and H. Wang, “On 3-Share Threshold Implementations for 4-Bit S-boxes,” 2013

# Results

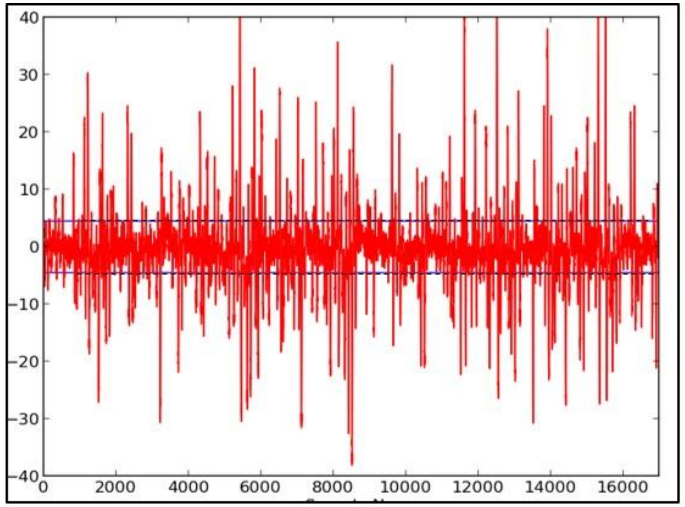
# T-tests on AES

- 2000 “Fixed-versus-random” FOBOS traces, 20,000 samples per trace
  - ➢ Samples (time-domain) on x-axis
  - ➢ T-value on y-axis (lines show ±4.5)
- Ext. Frequency Generator @ 500 KHz

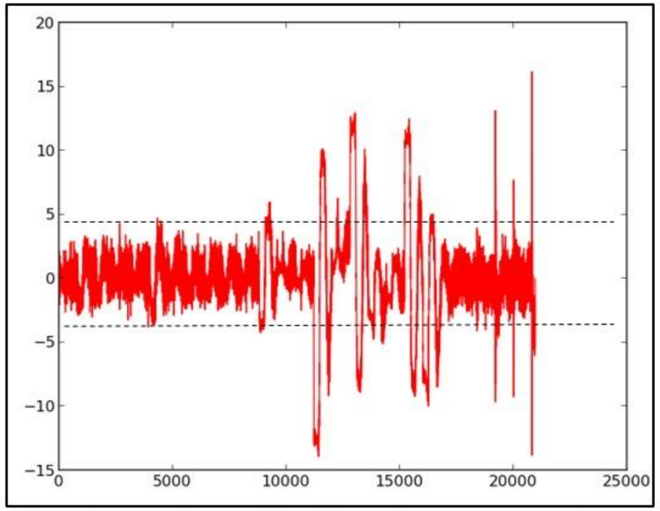
- Full-width, basic-iterative architecture cannot be protected
- Full-width with Boolean Masking fails t-test



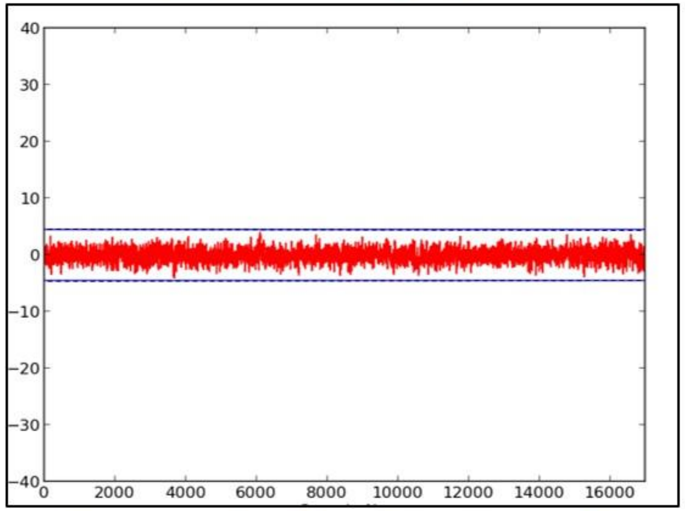
Full-width basic-iterative architecture



5-stage pipelined (unprotected)



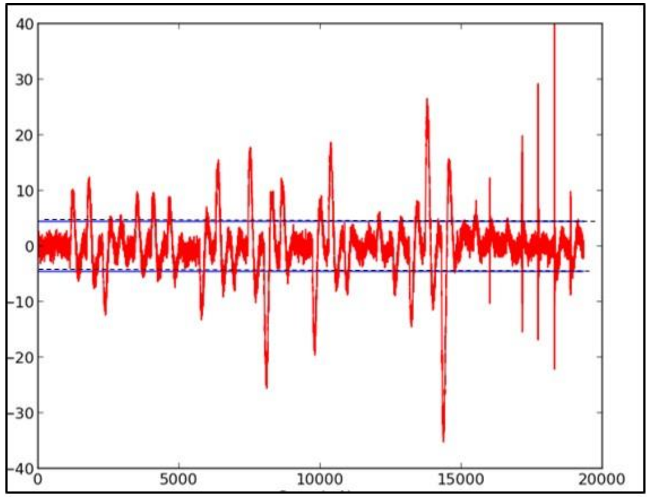
Full-width with Boolean masking



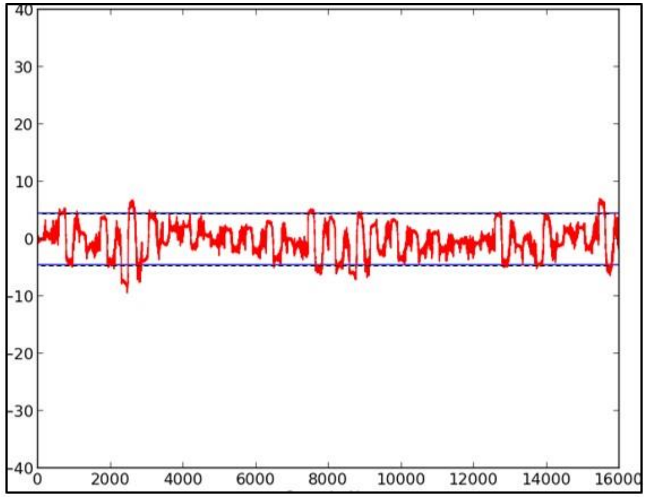
5-stage pipelined (protected)

# T-tests on SPECK

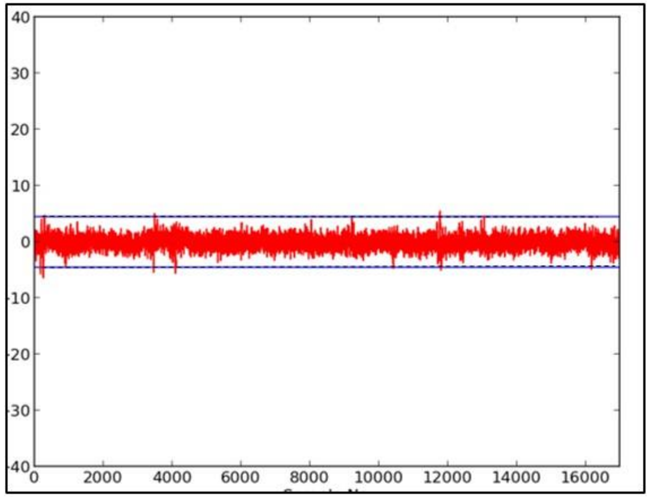
- Full-width with basic-iterative architecture (upper right) fails t-test
- Likely due to glitches
- 8-cycle applying random bits to 1st stage of Kogge-Stone adder only (48 bits) fails t-test
  - Fails uniformity property



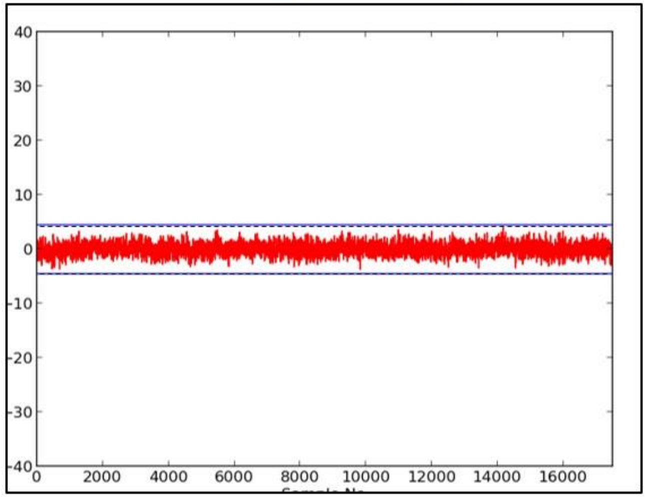
Full-width basic iterative architecture



Full-width (protected)

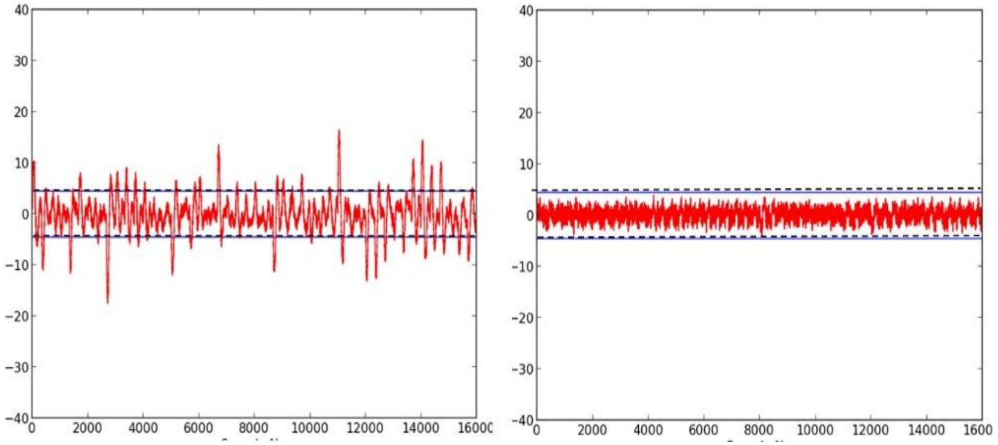


Full-width multi-cycle (6 rnd bits/cycle)

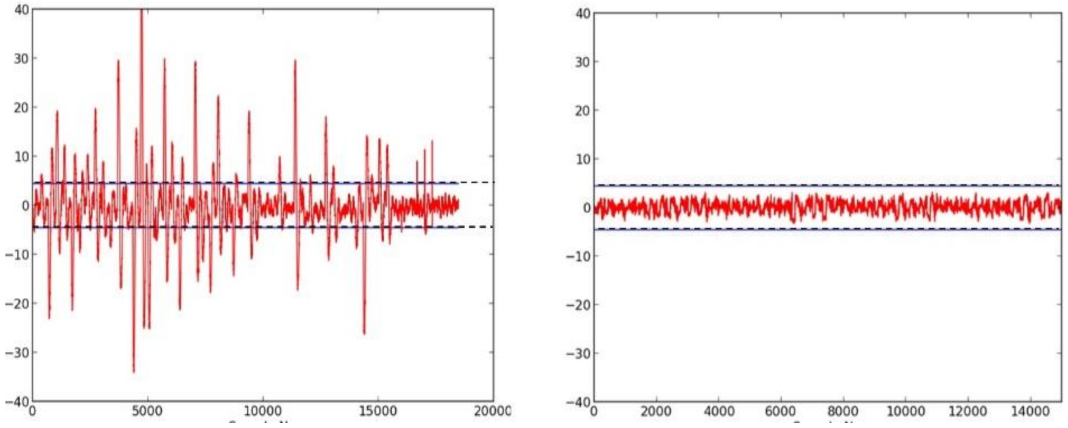


Full-width multi-cycle (34 rnd bits/cycle)

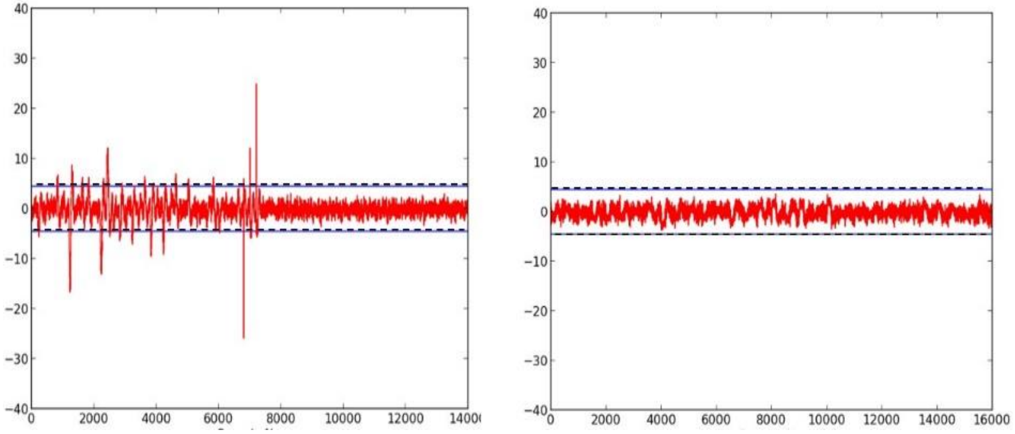
# T-tests on Remaining Ciphers



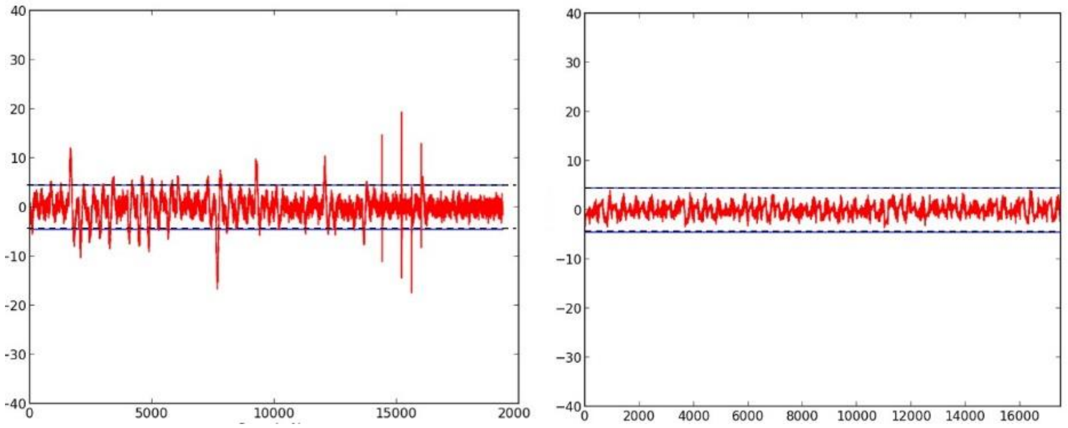
SIMON



LED



PRESENT

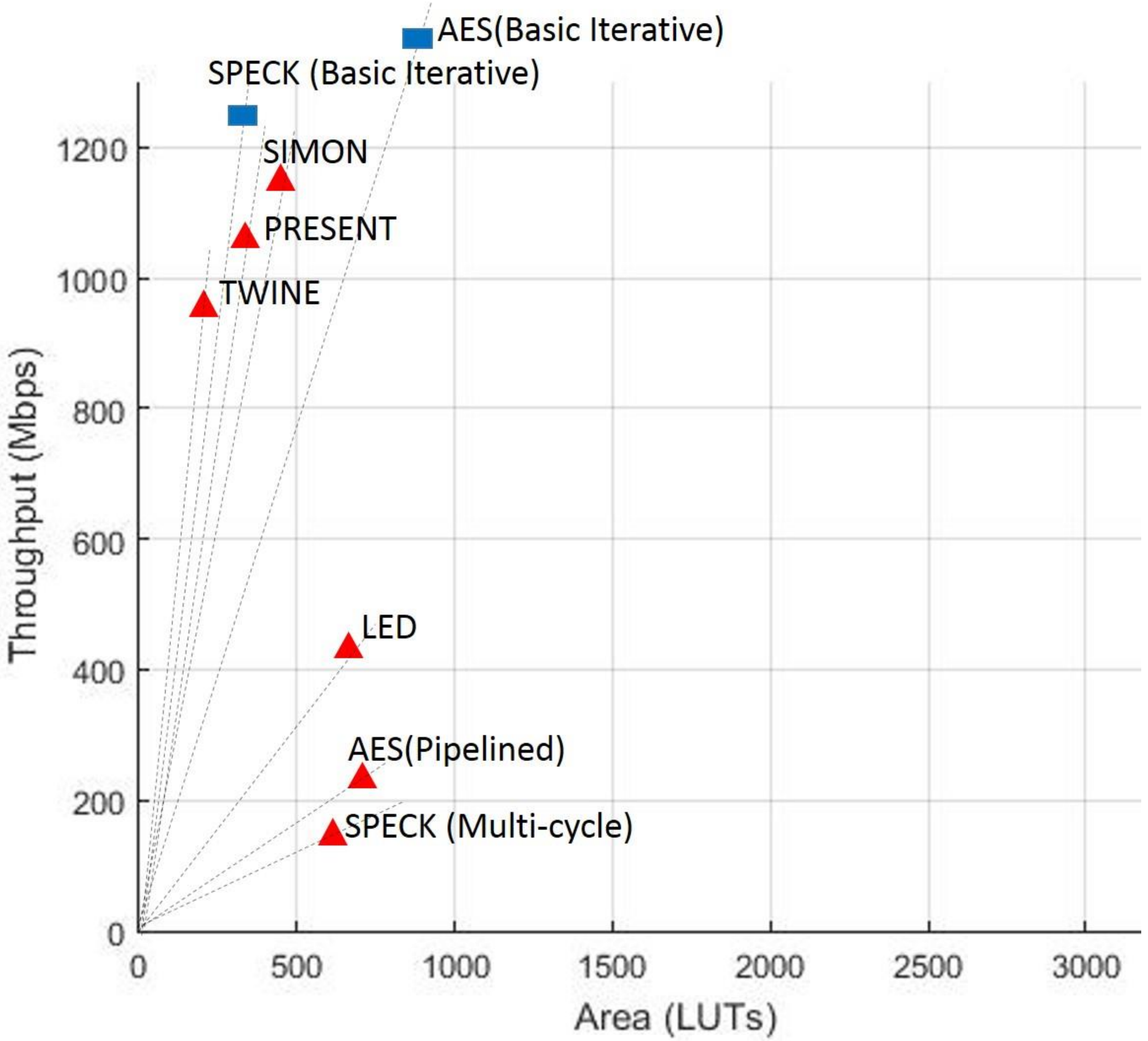


TWINE

Successful full-width datapaths with basic iterative architectures for protected versions

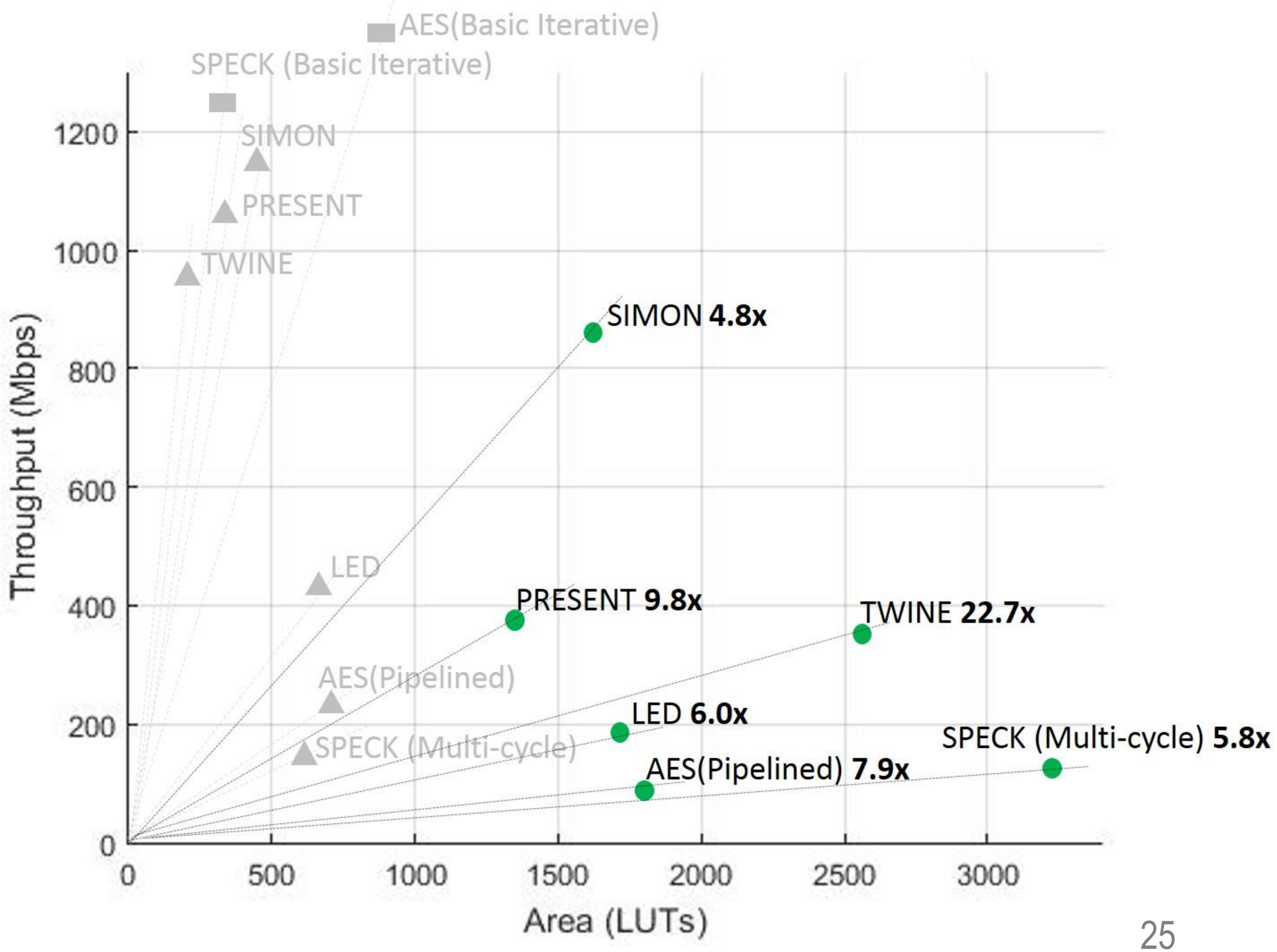
# Benchmarking of Unprotected Ciphers

- Results shown for Virtex-7 FPGA
- Smallest (LUTs)
  - ➢ TWINE
  - ➢ PRESENT
  - ➢ SPECK (Basic Iterative)
- Highest Throughput (Mbps)
  - ➢ AES (Basic Iterative)
  - ➢ SPECK (Basic Iterative)
  - ➢ SIMON
- Highest TP/A ratio (Mbps/LUT)
  - ➢ TWINE
  - ➢ SPECK (Basic Iterative)
  - ➢ PRESENT



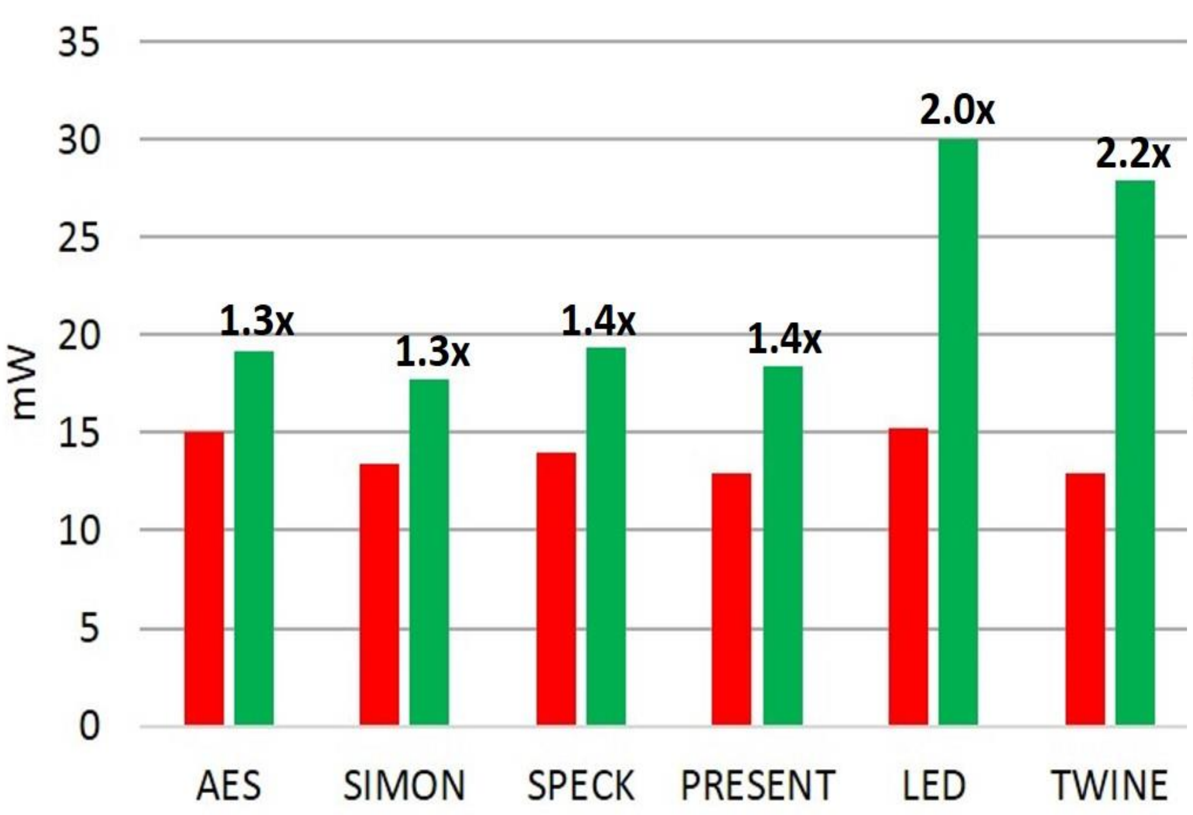
# Benchmarking of Protected Ciphers

- Smallest (LUTs)
  - PRESENT
  - SIMON
  - LED
- Highest Throughput (Mbps)
  - SIMON
  - PRESENT
  - TWINE
- Highest TP/A ratio (Mbps/LUT)
  - SIMON
  - PRESENT
  - TWINE
- Area growth: **4.3x**
- TP reduction: **2.2x**
- TP/A reduction: **9.5x**

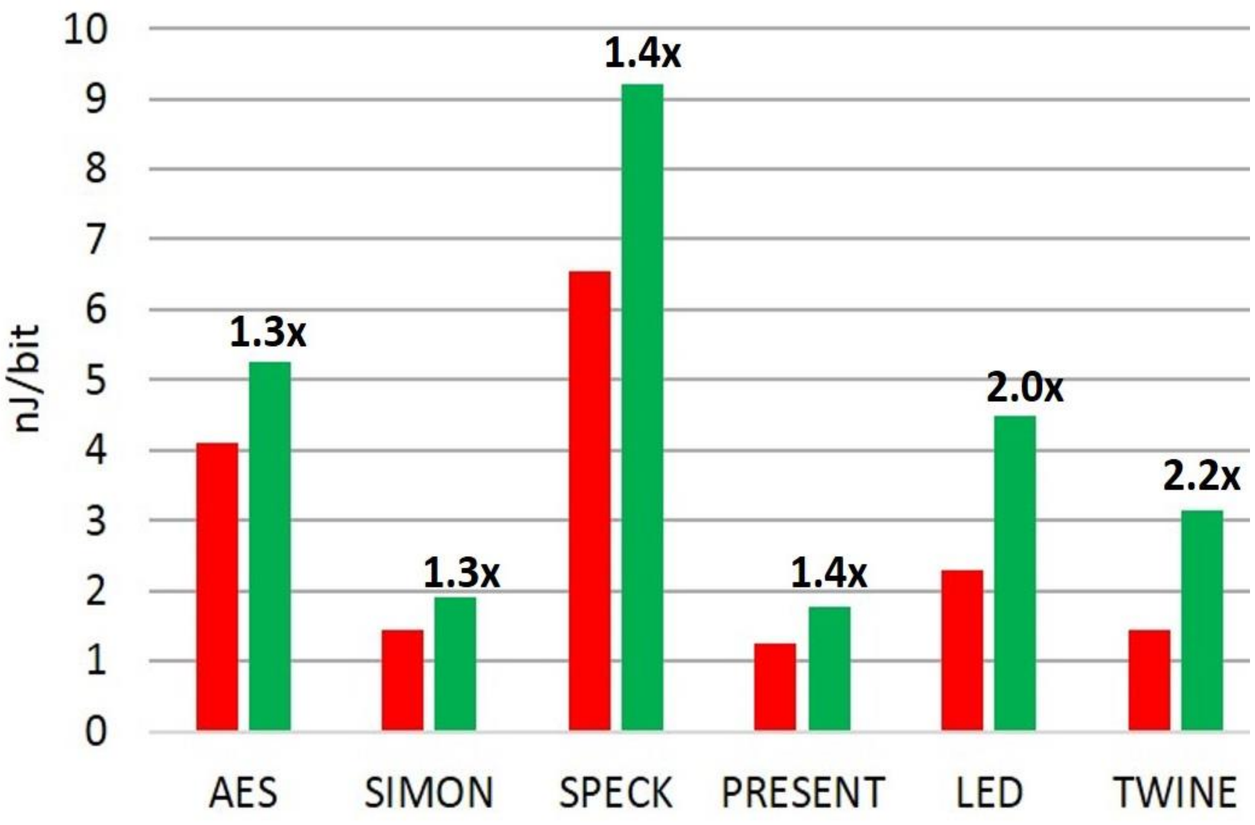


# Comparison of Power & Energy

Power



Energy



🟥 Unprotected 🟩 Protected

Mean: **1.6x** increase

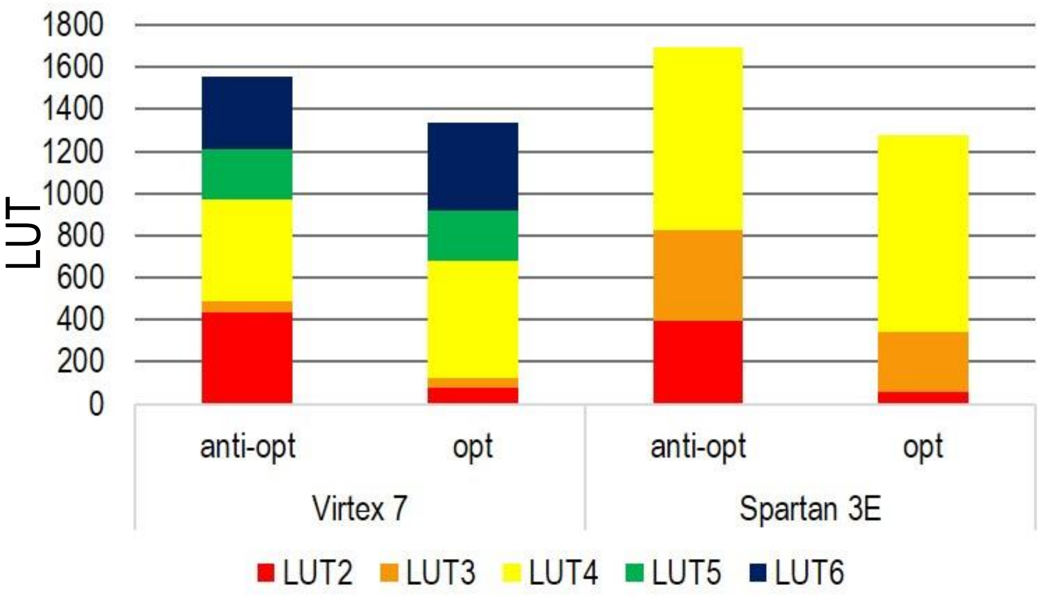
# Cost of Anti-optimization Constraints

- Keep HIERARCHY and Keep SIGNAL
- Supports algorithmic DPA protection, but cost in area & throughput

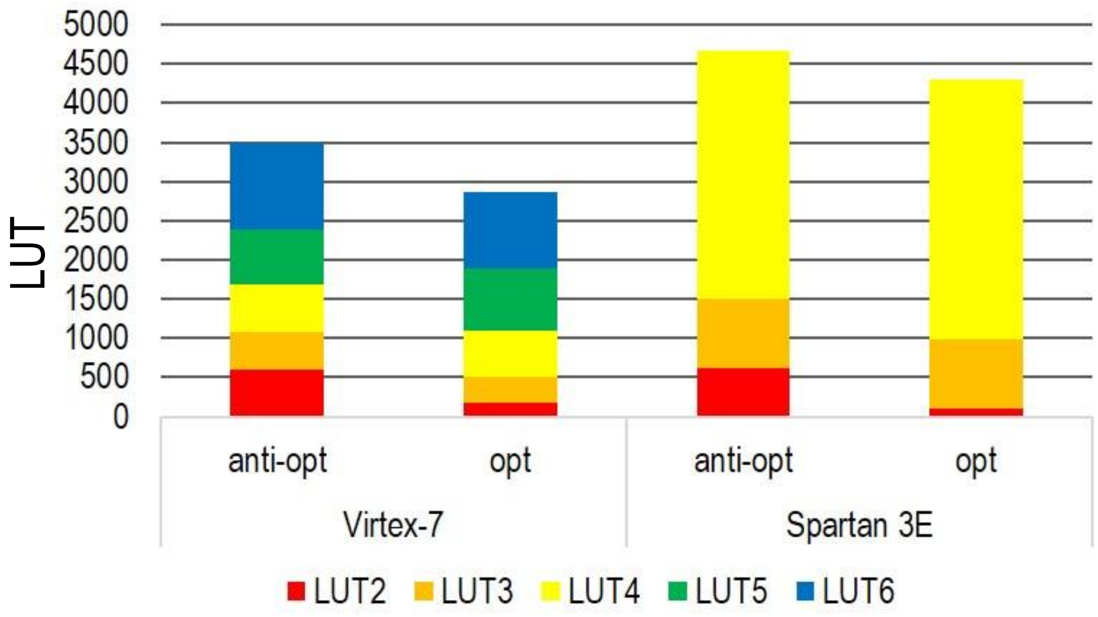
Change in area, throughput, and throughput-to-area ratio in Virtex-7 and Spartan-3E FPGAs due to KEEP Constraints

| FPGA | Area (LUTs) | Throughput (Mbps) | TP/A Ratio |
|---|---|---|---|
| Virtex-7 | +22% | -4% | -21% |
| Spartan-3E | +5% | -16% | -20% |

Change in BEL distribution in **SIMON** due to KEEP Constraint



Change in BEL distribution in **SPECK** due to KEEP Constraint



# Conclusions

- All unprotected cipher implementations vulnerable to DPA
- Achieved versions of all 6 ciphers protected against 1st order DPA
  - SIMON, PRESENT, LED, TWINE full-width, basic-iterative architectures
  - AES protected using 8-bit pipelined, SPECK with full-width multi-cycle
- PRESENT, SIMON, LED smallest protected ciphers
- SIMON, PRESENT, TWINE highest Throughput, TP/A Ratios
- SIMON lowest power, PRESENT lowest energy-per-bit
- SIMON lowest relative reduction in TP/A, TWINE largest reduction
- 20% reduction in TP/A ratios due to FPGA anti-optimization constraints

Questions?