Evaluation of DPA Protected Implementations of CAESAR Finalists ACORN and Ascon and other Candidates

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

Cryptographic Engineering Research Group (CERG)
`http://cryptography.gmu.edu`
Department of ECE, Volgenau School of Engineering
George Mason University, Fairfax, VA, USA

CryptArchi 2018

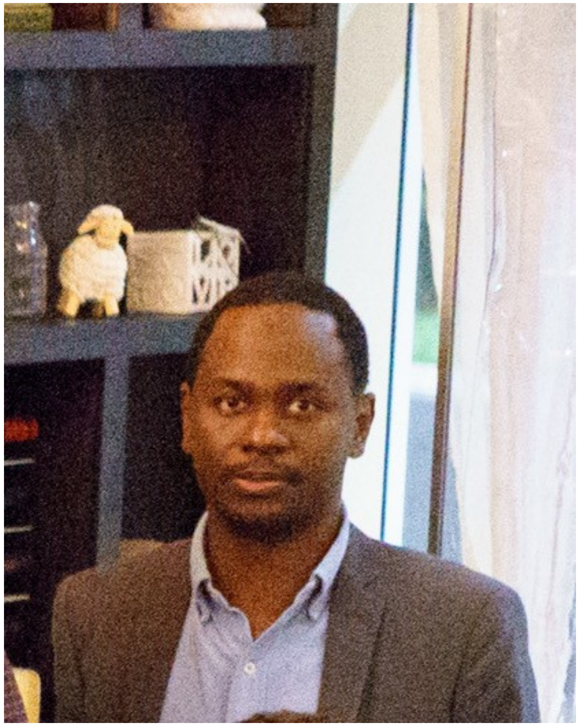
Outline

1. Introduction & Background
2. Methodology
3. Results
4. Improved Comparison
5. Conclusions & Future Work

Introduction & Background

CERG Team

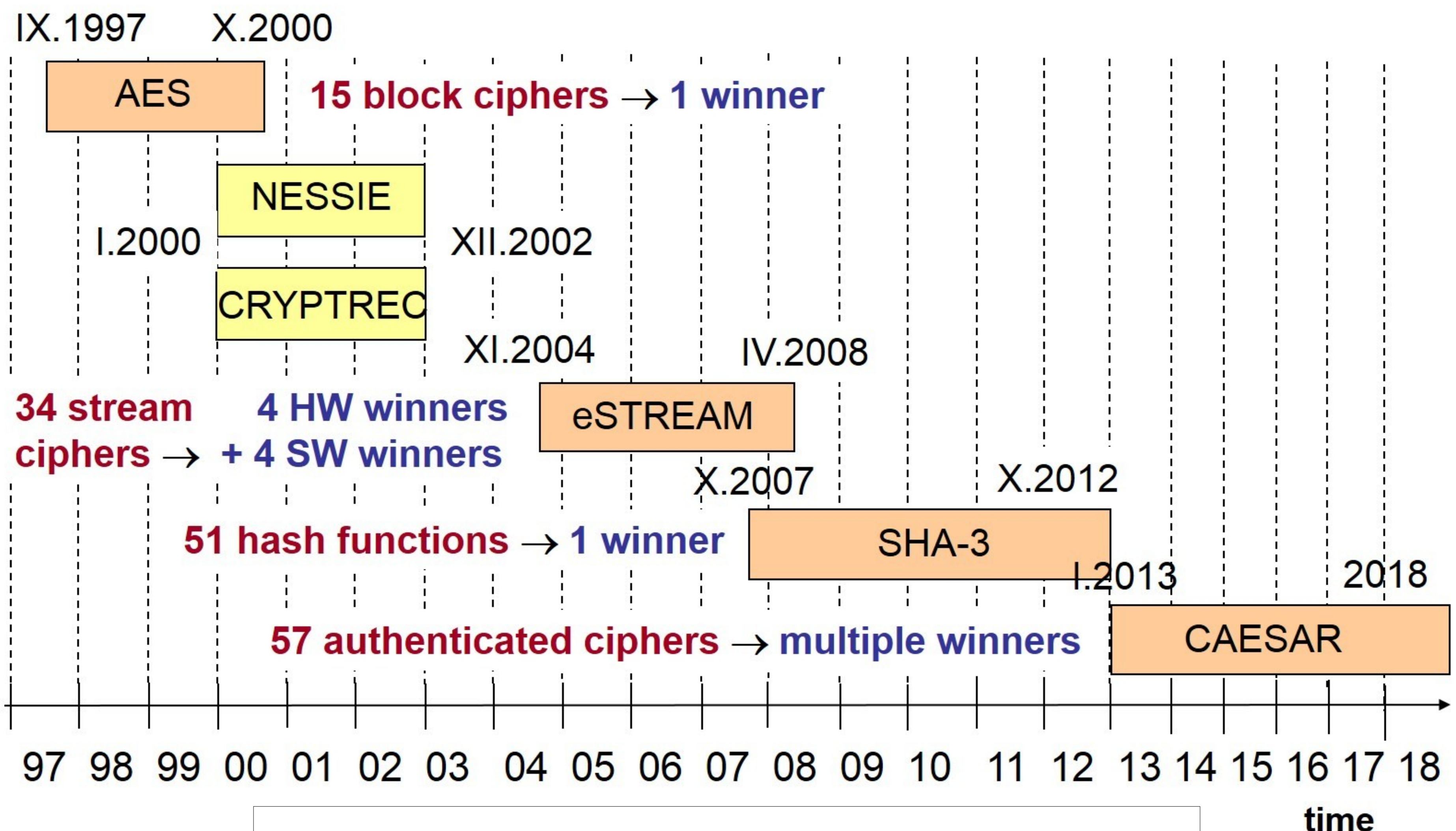
William Diehl
Associate Professor
Virgina Tech



Abubakr Abdulgadir
Ph.D. Candidate

Farnoud Farahmand
Ph.D. Candidate

Comparison Supporting Competitions



Competitions need metrics

Motivation

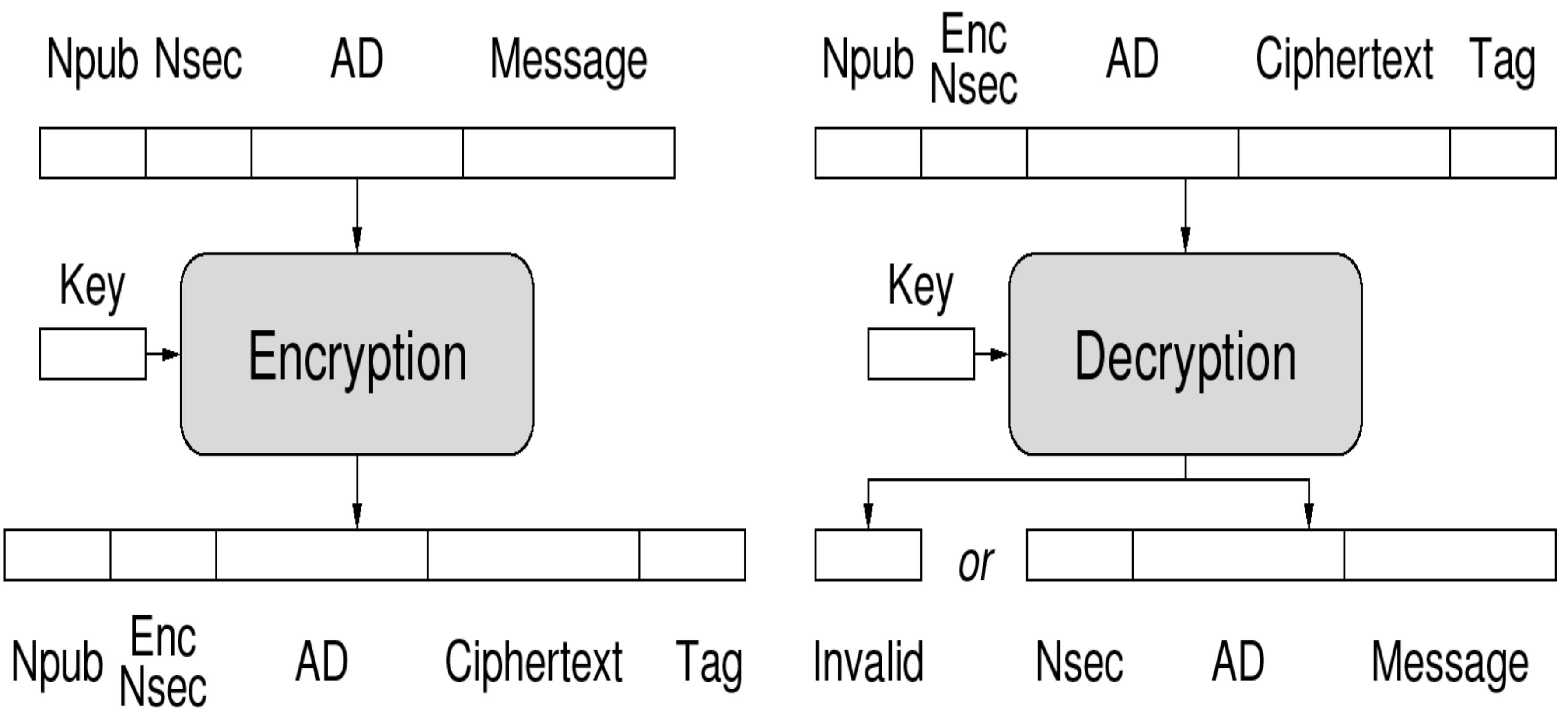
- Competition for Authenticated Encryption: Security, Applicability and Robustness (CAESAR)
  - 2014 – 57 Candidates in Round 1
  - 2015 – 29 Candidates in Round 2
  - **2016 – 15 Candidates in Round 3**
  - **2018 – 7 Candidates (2 lightweight) in Final Round**
- NIST Lightweight Cryptography Standardization (2018 – ?)
  - Now includes Lightweight Authenticated Ciphers!
- NIST Post-quantum Cryptography (PQC) Standardization (2017 - ?)

Comparing Cost of Protection Against DPA

- Support to CAESAR Evaluations
  - Authenticated Ciphers
  - Evaluation of side-channel resistance
- Some evaluation of countermeasures in block ciphers
  - Very few evaluations of authenticated ciphers
- No large scale evaluation of multiple authenticated ciphers

Authenticated Ciphers

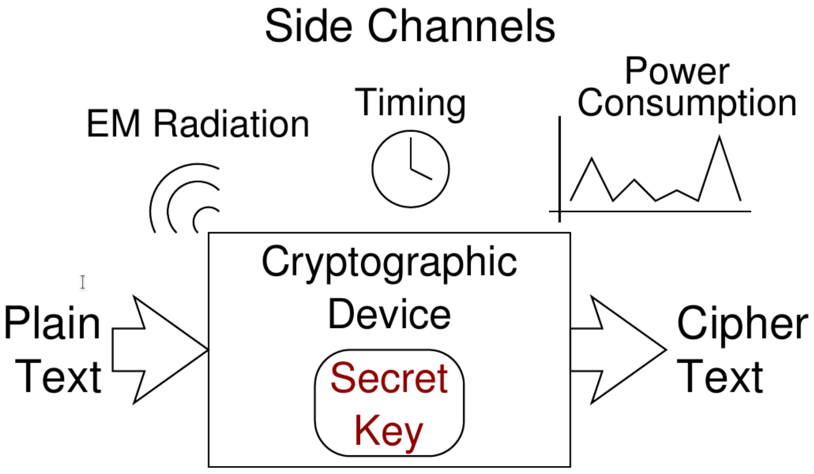
Combine the functionality of **confidentiality**, **integrity**, and **authentication**



Notation: Npub = Public Message Number; (Enc) Nsec = (Encrypted) Secret Message Number; AD = Associated Data

Side Channel Attacks

- Cryptographic Algorithms mathematically sound
  - Cryptanalysis not easier than brute-force attacks
- However, cryptography conducted in the physical world
  - Hardware and software
- 1990s – Development of Side Channel Attack techniques
  - Timing Analysis
  - **Power Analysis**
  - Electromagnetic Analysis
  - Fault Injection

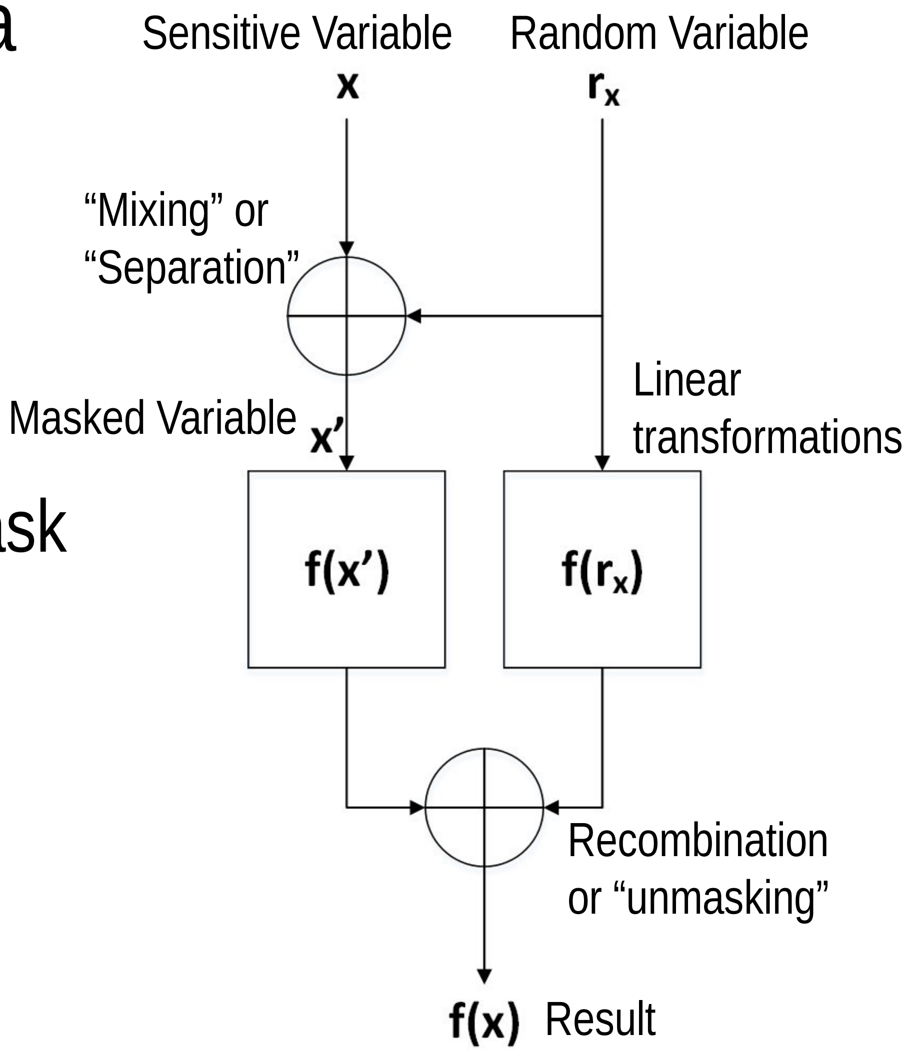


Countermeasures

- Since early 2000s – emphasis on SCA countermeasures
- Algorithmic
  - **Masking** (**Boolean**, arithmetic, table recomputation)
  - **Threshold Implementations**
- Non-algorithmic (hiding)
  - Balancing schemes (DPL/DDL)
  - Random Noise and Timing Randomization

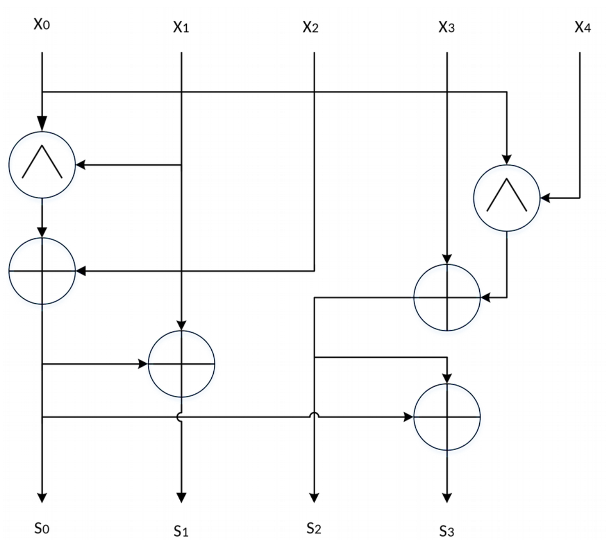
Masking

- Masking - divide sensitive data into shares
- **Boolean Masking** separates shares using XOR
- Masking is costly
  - Hardware area increases in mask order *d*;
    - Linear: area(*d*) ~ *d*
    - Non-linear: area(*d*) ~ d^2



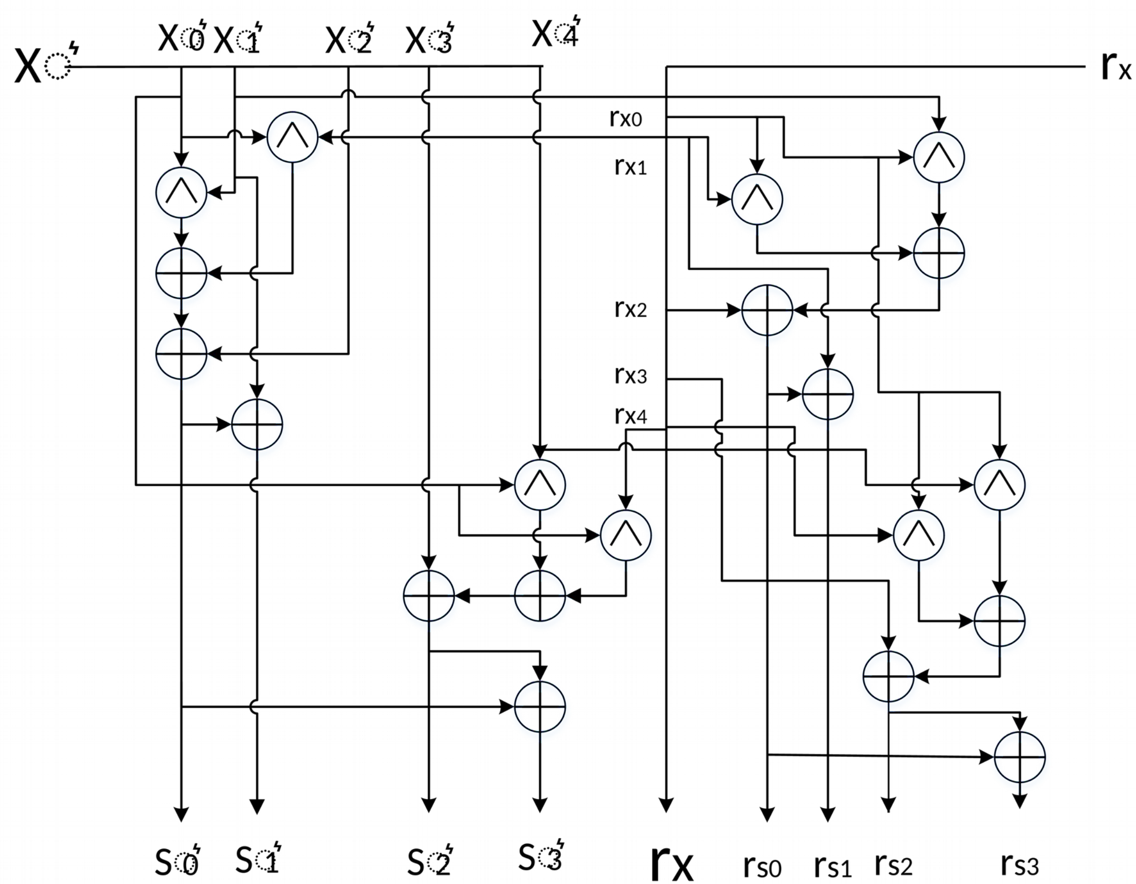
Example: Masking of Non-linear Transformation

No masking



All bus widths are same

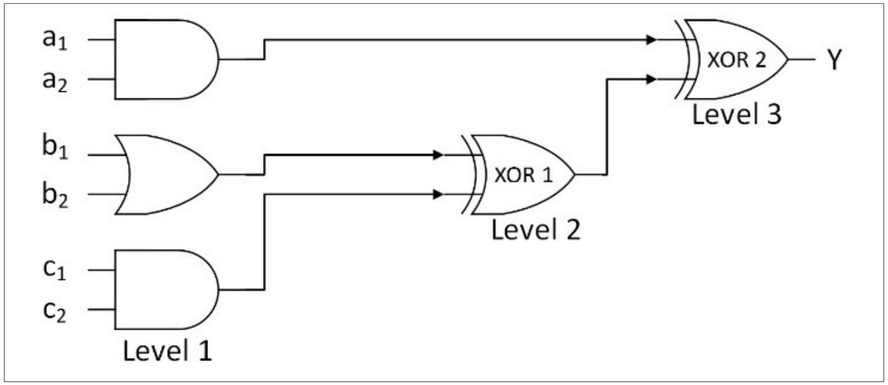
1st order masking



Masking and Glitches

Boolean Masking not secure given CMOS glitches

Masked implementation attacked using glitch measurement [MPO05].



- >1 transition per clock cycle
- Varying effect on number of gates which change output
- Example: Different effect for toggles in *a*, *b*, or *c*.
- Dependence used to build correlation for DPA

Threshold Implementations[1]

- Similar to Boolean masking, but data masked by more than one random variable
- To share function of degree ***d***, ***d*+1** shares are required
  - Function of degree 2 (z = xy) needs **3** shares
- Advantages: Secure in presence of glitches
- Disadvantages: Area growth ≥ Boolean Masking, Complexity (for large S-Box)

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

Threshold Implementations (Properties)

TI implementation secure in presence of glitches if **three** properties satisfied:

Property 1 - ***Non-completeness***. Every function is independent of at least one share of each of the input variables.

If $z = N(x, y)$ and x and y are shared in n shares, then

$$z_1 = f_1(x_2, x_3, \ldots, x_n, y_2, y_3, \ldots, y_n)$$
$$z_2 = f_2(x_1, x_3, \ldots, x_n, y_1, y_3, \ldots, y_n)$$
$$\ldots$$
$$z_n = f_n(x_1, x_2, \ldots, x_{n-1}, y_1, y_2, \ldots, y_{n-1})$$

If z_i does not depend on x_i and y_i, it cannot leak information about x_i or y_i.

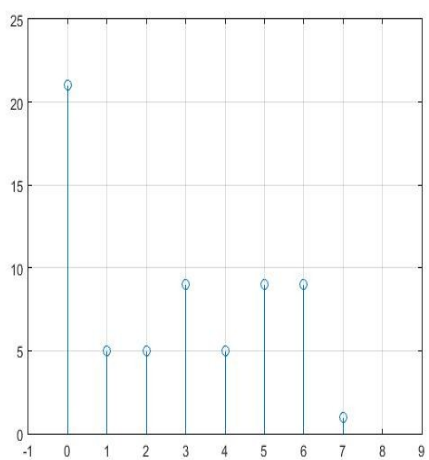
Threshold Implementations (Properties -cont'd)

Property 2 – ***Correctness***. The sum of the output shares gives the desired output.

$$z = \oplus_{i=1}^{n} z_i = N(x)$$

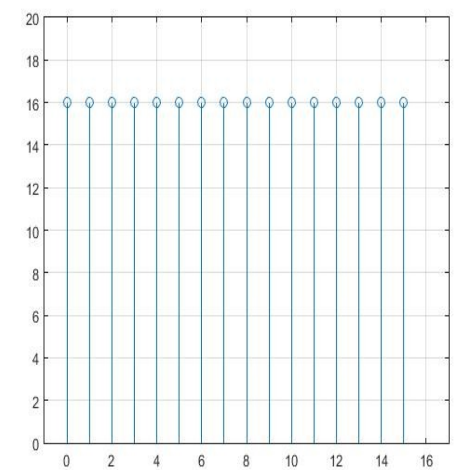
Property 3 – ***Uniformity***. A realization of $z = N(x, y) = xy$ is uniform if for all distributions of the inputs *x*,*y*,…, the sharing preserves the output distribution.

Number of occurrences



Binary 3-tuple $[z_1, z_2, z_3]$

Number of occurrences



Binary 4-tuple $[z_1, z_2, z_3, z_4]$

Non-uniform output distribution using 3 shares (does not satisfy Property 3

Uniform output distribution using 4 shares (satisfies Property 3)

Previous Research

Analysis of DPA and countermeasures:

Block Ciphers

AES - **[MPLP+11]**, **[BGNN+14]**, many others …
SIMON – [SSA14], **[STE17]**
PRESENT – **[PMKL+11]**, **[KNPW+13]**, [DCWF16], [HPGM17]
LED – [SSA14], [SMG16]
TWINE – [Gup15]

Authenticated Ciphers

ACORN – [DRA16] [1], [DFL17] [1], [SSMC17] [1]
Ascon – **[GWDE15]**, [GMK16], **[GM17]**, [SD17]
Cloc & Silc – None
Jambu - None
Ketje – [BDNN+14] [2], [LFFD+14] [2], [TS13] [2]
AES-GCM – **[Jaf07]**, **[BFG14]**, [VRM17]

Medium Scale analysis of LW Block Ciphers

AES, SIMON, SPECK, PRESENT, LED,TWINE: **[DAKG17, DAKG18]**

AES, SIMON, SPECK, PRESENT, KHUDRA: [SMGP+17]

Large Scale analysis of Authenticated Ciphers

ACORN, Ascon, Cloc & Silc, Jambu, Ketje:**[DAF+18a, DAF+18b]**

Medium Scale analysis of Authenticated Ciphers
ACORN, Ascon, AES-GCM: **[DFA+18]**

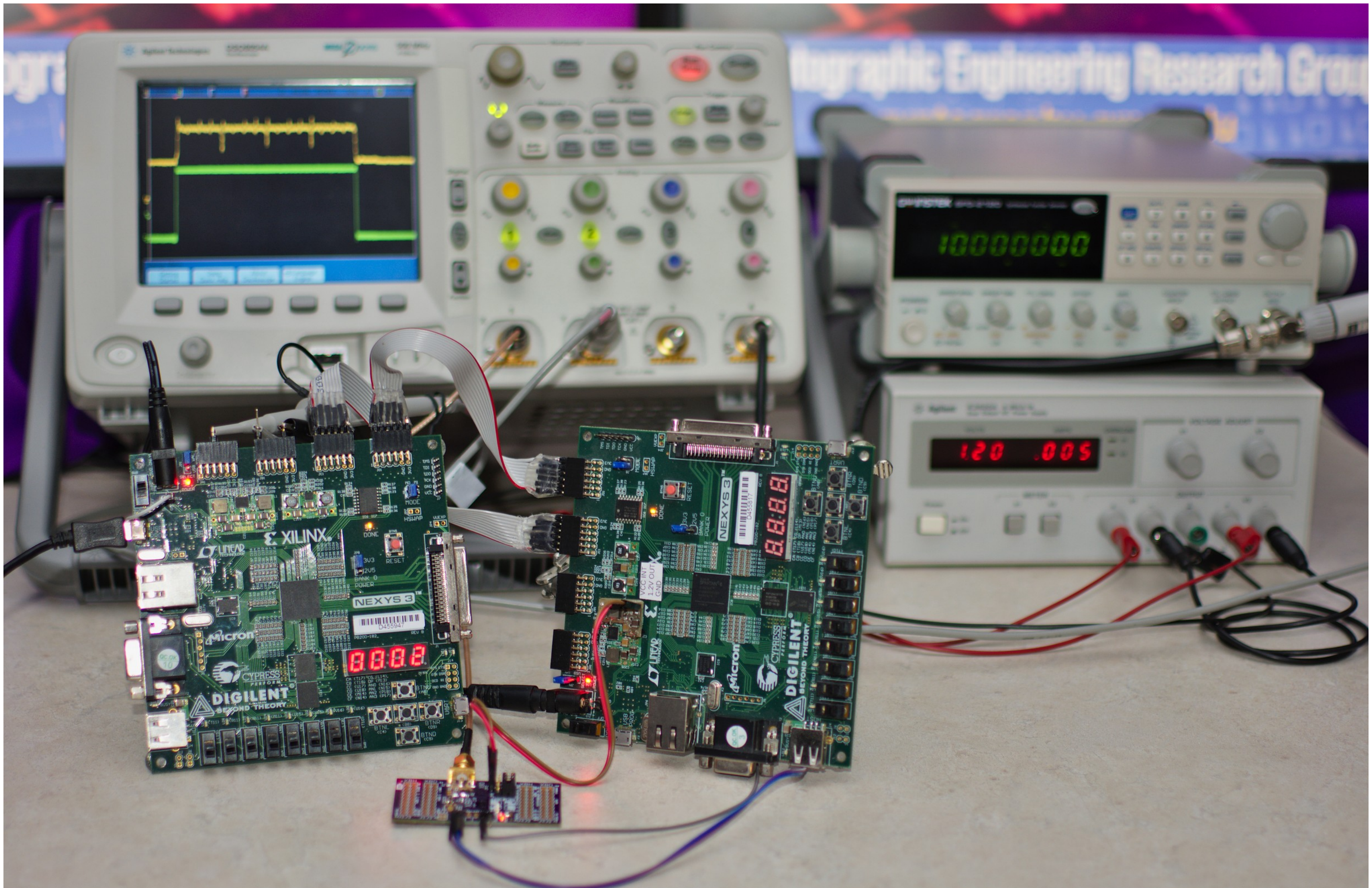
1 – Fault Attacks, not DPA
2 – Strictly Keccak-f in SHA-3, not Ketje

Methodology

Approach

- Augment existing testbench (FOBOS)
- Start with CAESAR Round 3 candidate authenticated ciphers
  - Test for leakage
  - Implement countermeasures
  - Verify reduced leakage
- Benchmark protected and unprotected versions – compare costs

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 and Victim Board: Xilinx Spartan 6

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

Attack-based Testing

Examples

Cipher	Counter-measures	# of Traces	Recovered	Equipment	Reference
Lake Keyak	No	60,000	5-bit key fragment	SAKURA-G	Samwel & Daemen 2017
MAC-Keccak	No	500,000	1 byte @ 90%	SASEBO GII	Luo et al. 2014
SIMON	No	4000	Key fragment	SASEBO GII	Shaverdi et al 2017
SIMON	Yes	100,000	Not recovered	SASEBO GII	Shaverdi et al 2017

Measure of Effectiveness:

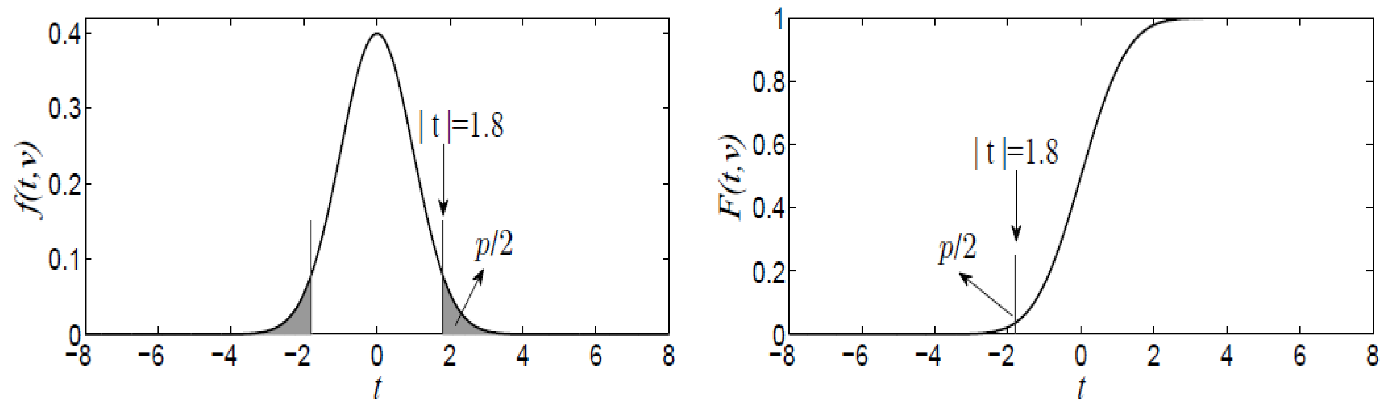
"How many traces" to recover *n*-bit key fragment?

Leakage Detection Using Welch's t-test[1]

Advantages
- Find leakage without attack
- Don't need power model
- Don't need to know architecture

Disadvantages
- Doesn't recover key
- Doesn't show difficulty of attack

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



(a) probability density function (b) cumulative distribution function

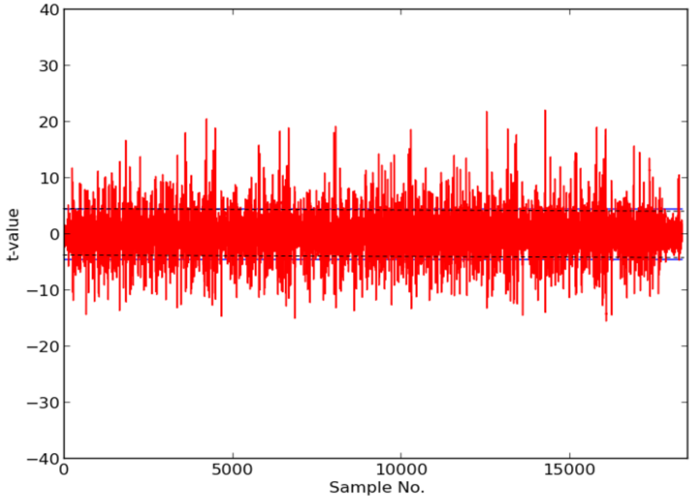
$$p = 2\int_{|t|}^{\infty} f(t,v)dt$$

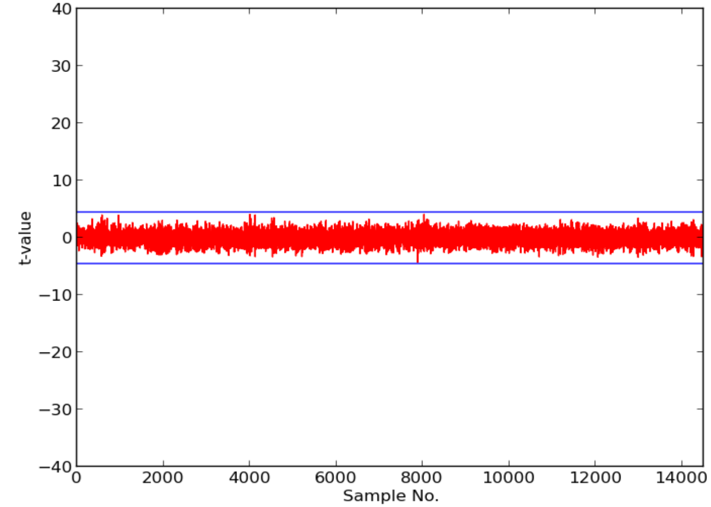
$$p = 2F(-|4.5|, v > 1000) < 0.00001$$

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

1 – [GJJR11], [SM16]

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"**

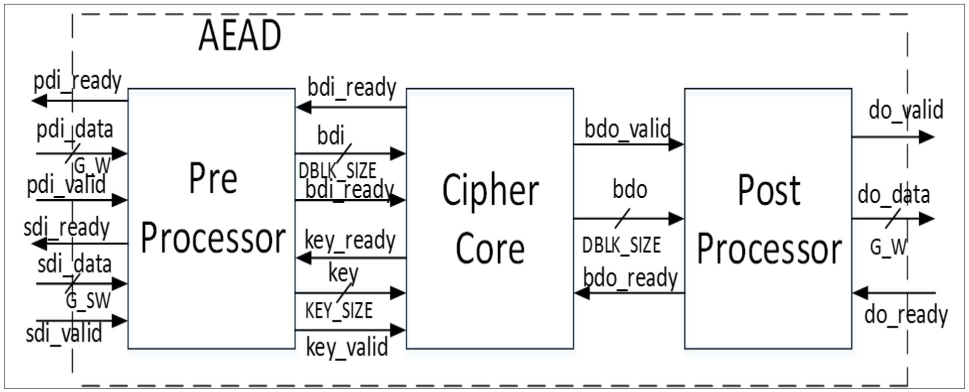
Challenge of DPA Evaluations on AEAD Ciphers

- Block Ciphers easy to evaluate[1]
  - **Simple interface**
  - **Short text vectors**
  - **Limited protocol**
- Authenticated Ciphers more complex
  - **Lots of Parts**
  - **Long test vectors**
  - **Complex protocol**
- Difficult to evaluate many ciphers with different interfaces

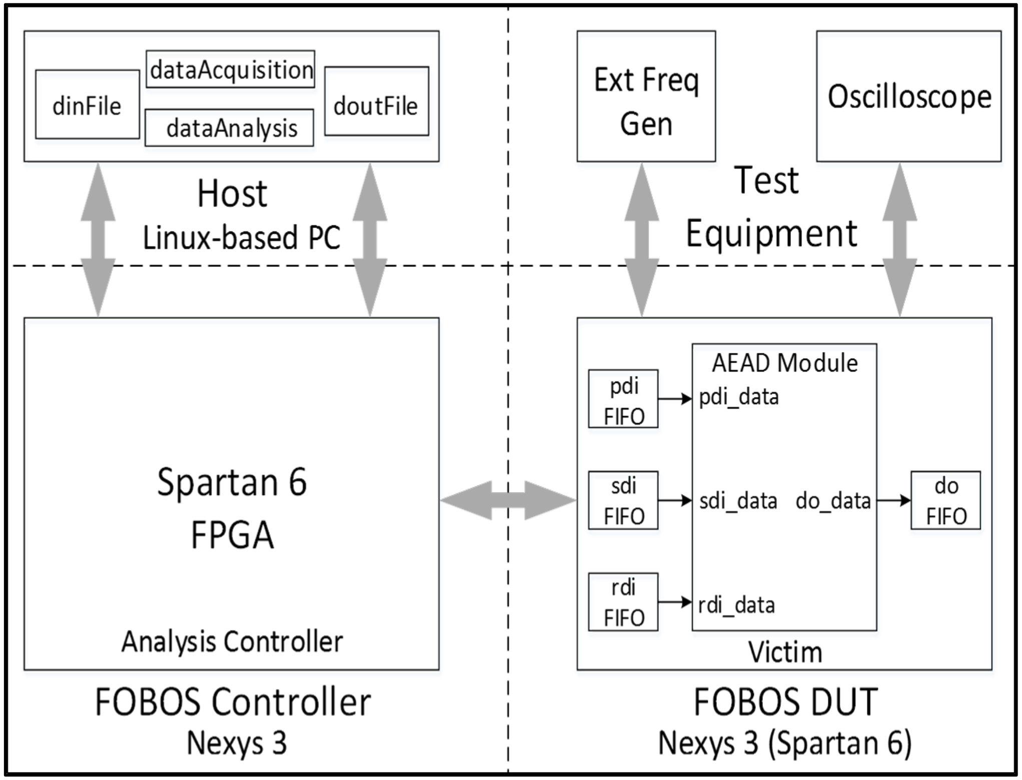
1 – [BGNN+14], [MPLP+11], [PMKL+11], [KNPW+13], [CITE16], [SMG16], [STE17]

Solution: Leakage Detection for AEAD Ciphers

Interface Using CAESAR HW API



FOBOS w/ CAESAR API Test Vectors



- Interface & Protocol
  - Compatibility
  - Fairness
- Common test vector generator
- Development Package has I/O modules

Results

Authenticated Ciphers Investigated[1]

Completed:

AES-GCM

ACORN

Ascon

CLOC (based on AES, TWINE)

SILC (based on AES, PRESENT, LED)

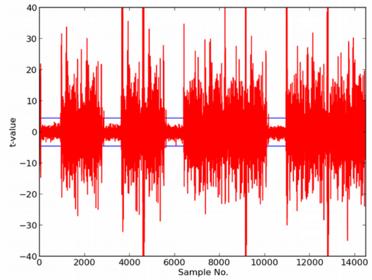
JAMBU (based on AES, SIMON)

Ketje Jr.

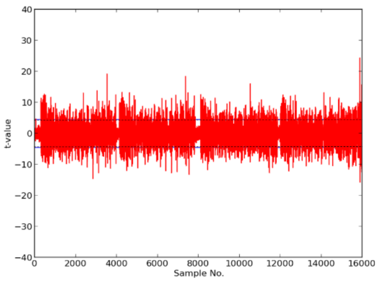
1 – [MV05], [Wu16], [DEMS16], [IMGM+16], [WH16], [GMU17], [Huang17a], [Iwata17], [Huang17b], [BDPV+16]

T-Tests on Unprotected Cipher Implementations

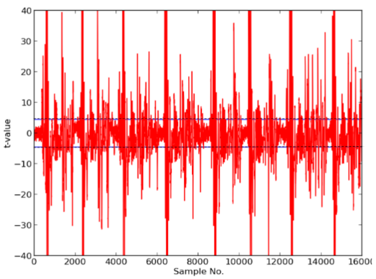
- 2000 “fixed-versus-random” traces
- T-test leakage detection methodology using FOBOS @ 780 KHz
- 4 – 8 authenticated encryptions and decryptions (test vectors 500 – 1000 bytes)



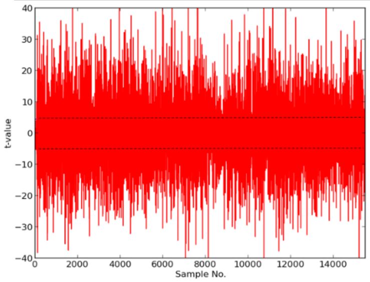
AES-GCM



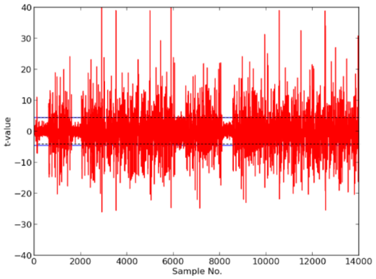
ACORN



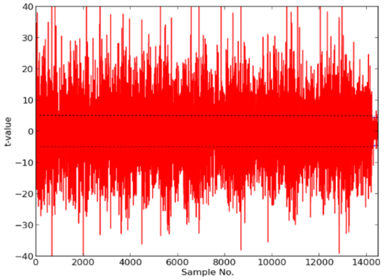
ASCON



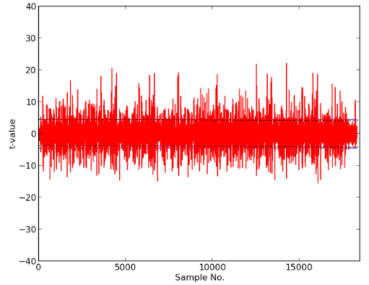
CLOC-AES



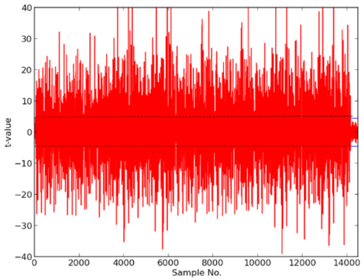
CLOC-TWINE



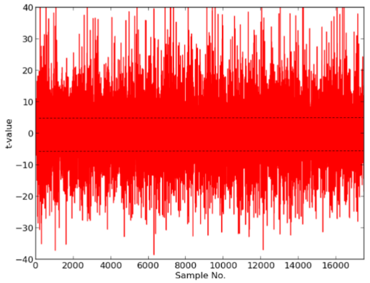
SILC-AES



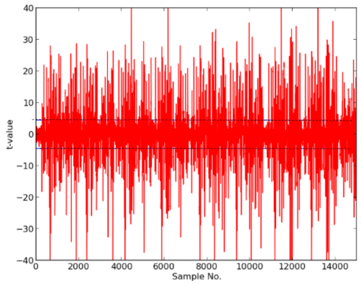
SILC-PRESENT



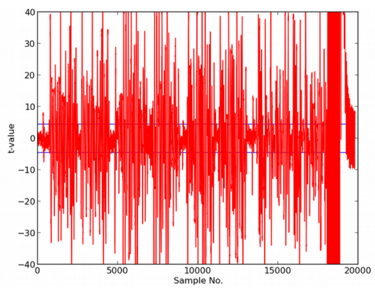
SILC-LED



JAMBU-AES



JAMBU-SIMON



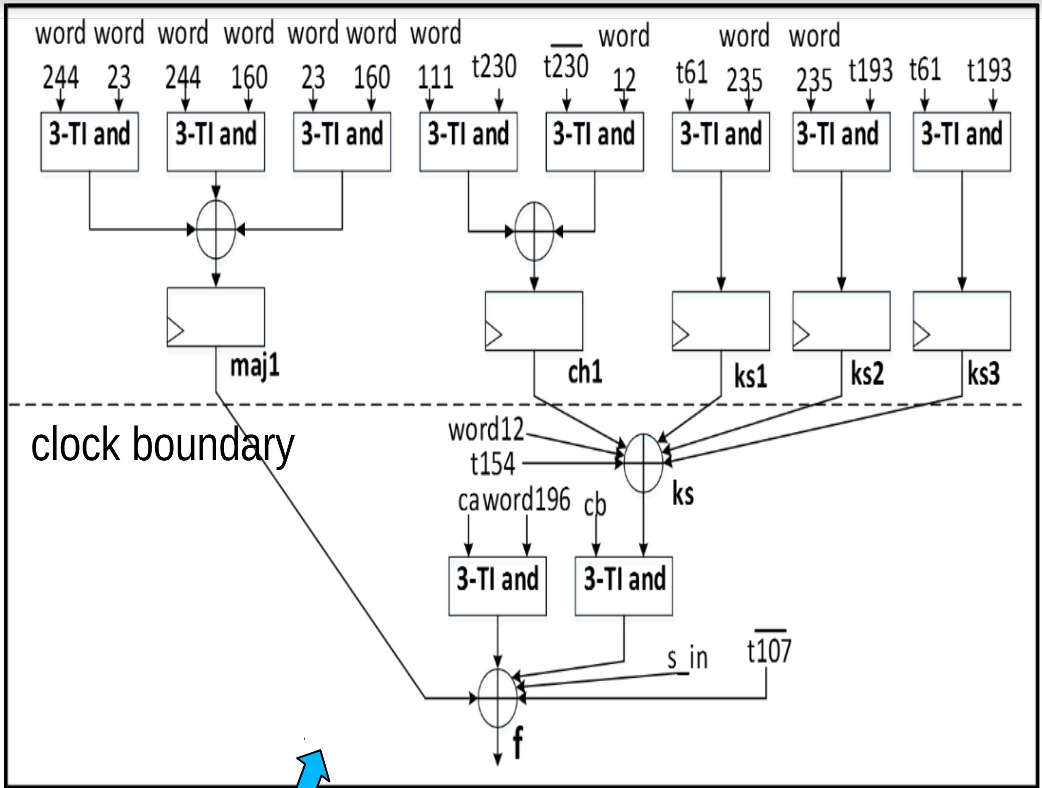
KETJE JR

General Steps to Protect Authenticated Ciphers against DPA

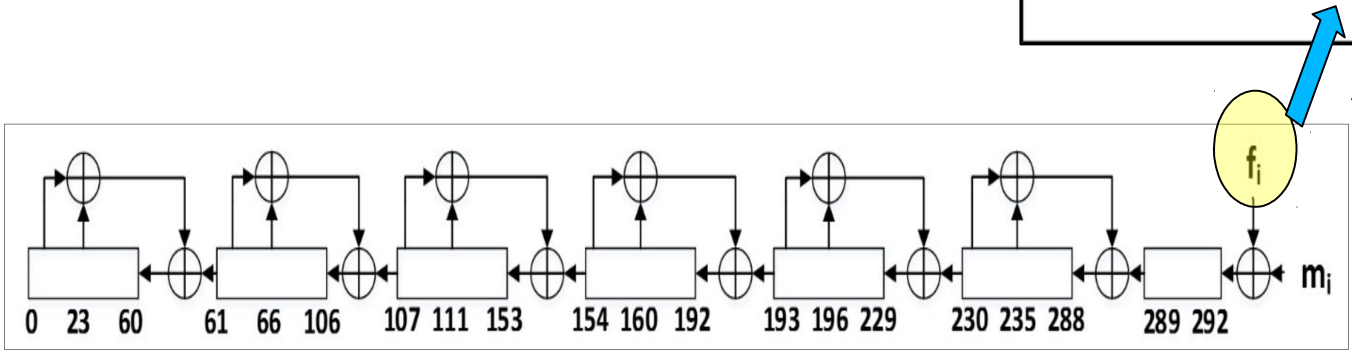
- Protect the primitive (Using 2 or 3-share TI)
  - Investigate best option for protecting non-linearity
  - Add pseudorandom number generator (PRNG)
- Protect authenticated cipher layer
  - Straightforward, except AES-GCM
- Encapsulate in protected Pre- and Post-Processors
- Run the t-tests
- If required, produce unprotected version with same architecture
  - Apples to apples!

ACORN

- Hybrid 2- / 3-share TI Protection
- 2 clock cycles per state update
- 10 *n*-bit TI-protected AND modules
- (10 x (2 reshare + 1 refresh) x *n*) / 2 = 120 random bits/ clock cycle (*n* = 8 for ACORN-8)



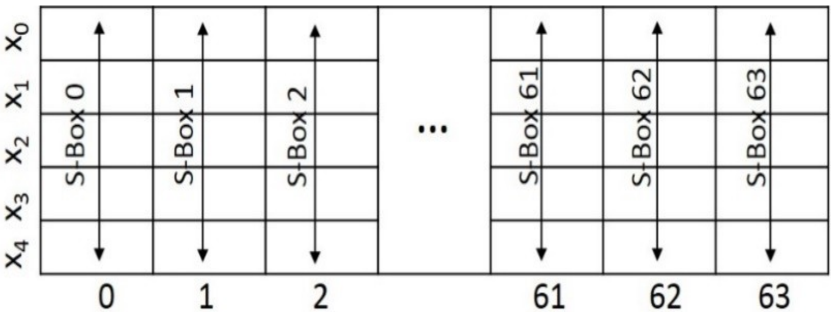
ACORN State Update



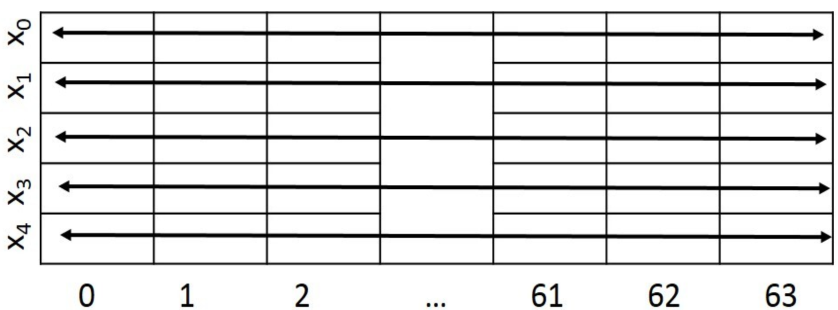
ACORN Linear Feedback Shift Register

Ascon

- Sponge Construction (Absorption & Squeezing)
- Large internal state (320 bits)
- 5-bit S-Box; Low-algebraic degree

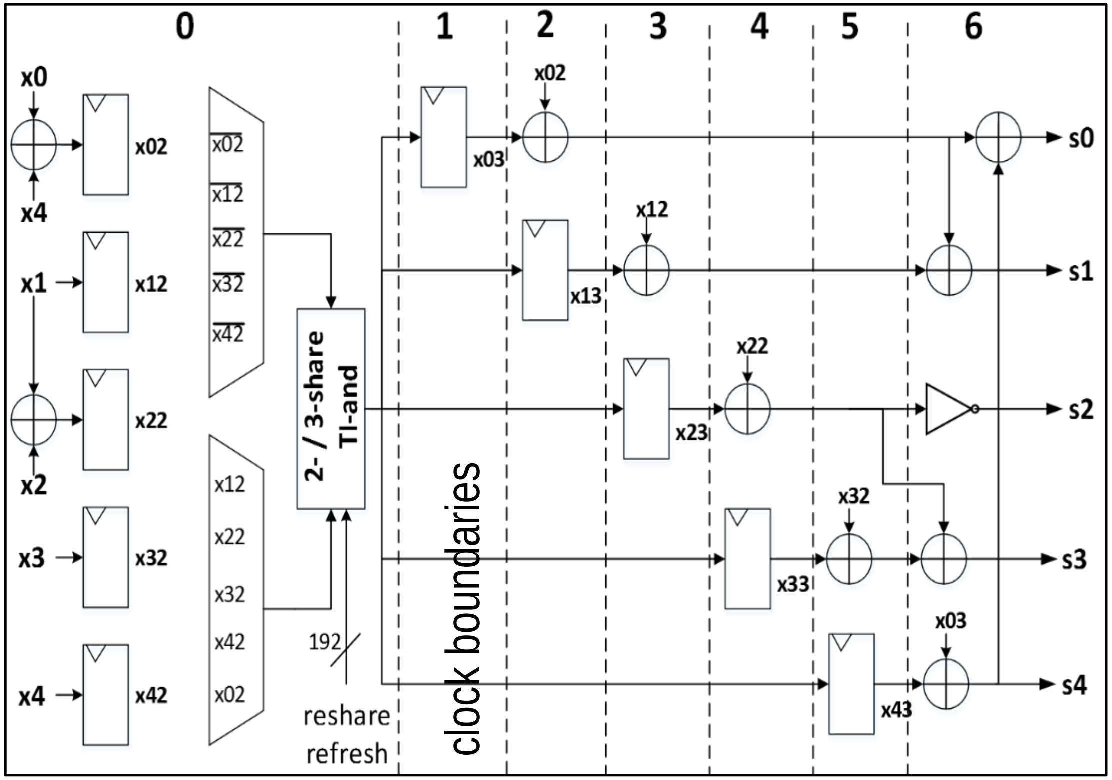


Substitution Layer



Permutation Layer

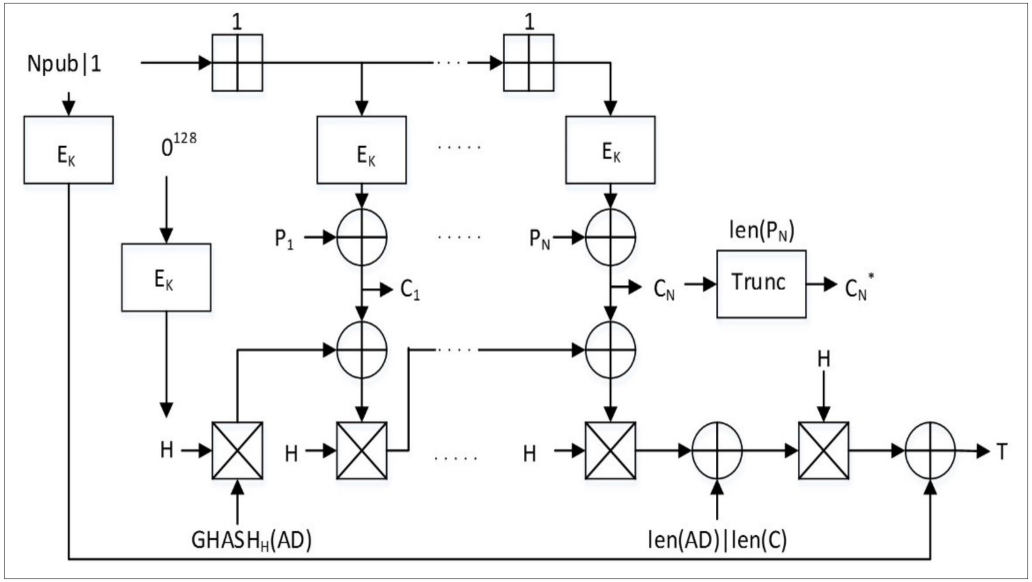
Hybrid 2- / 3- share with bitslice S-Box

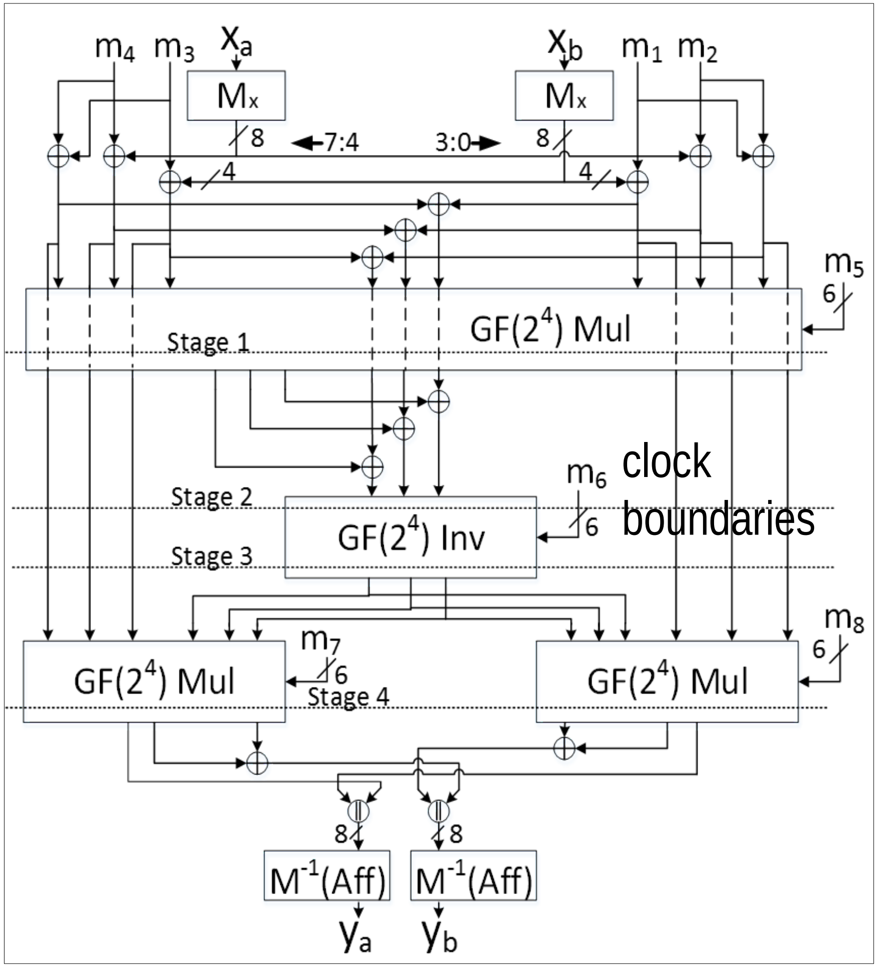


7 cycles/round
192 random bits per clock cycle (128 reshare + 64 refresh)

AES-GCM (Galois Counter Mode)

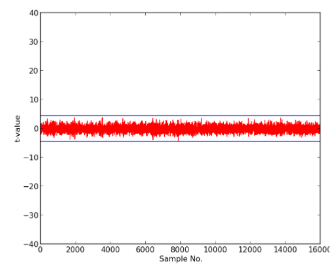
- Non-linearity (S-Box) of degree 7
- Use "Tower Fields" to reduce to composition of degree 2 functions
- Hybrid 2- /3-share TI protection
- 20 cycles / round x 10 rounds = 205 clock cycles per block
- Non-linear multiplier (128 clock cycles per block)
- 40 random bits per clock cycle



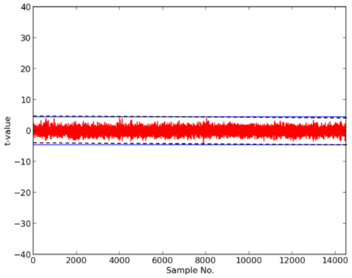


W. Diehl, A. Abdulgadir, J. P. Kaps and K. Gaj," Comparing the Cost of Protecting Selected Lightweight Block Ciphers Against Differential Power Analysis in Low-Cost FPGAs," *MDPI Computers Special Issue "Reconfigurable Computing Technologies and Applications*," Apr. 9, 2018.

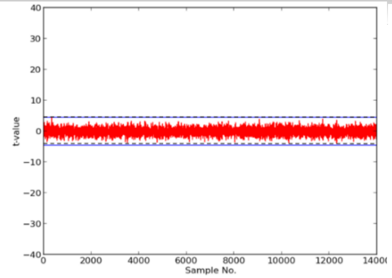
Protected Authenticated Ciphers



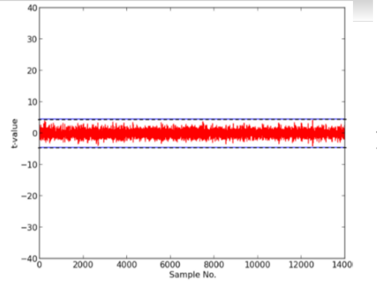
ASCON



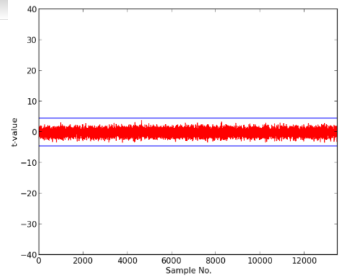
ACORN



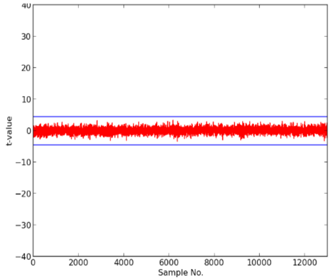
SILC-PRESENT



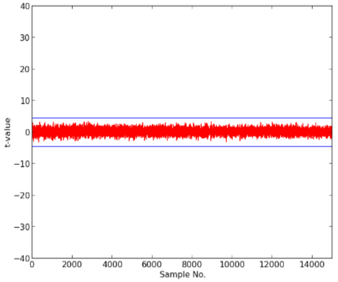
SILC-LED



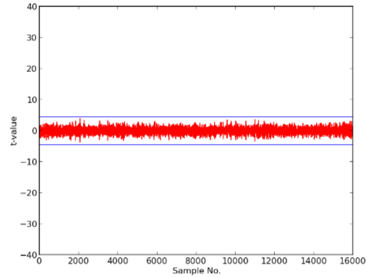
AES-GCM



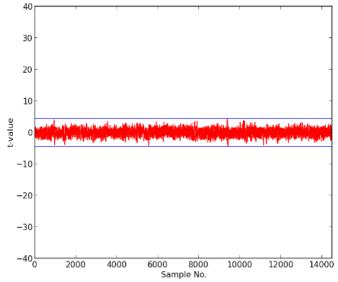
JAMBU-SIMON



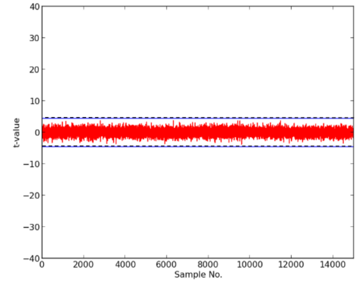
CLOC-AES



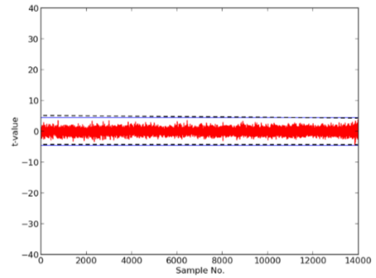
CLOC-TWINE



KETJE JR



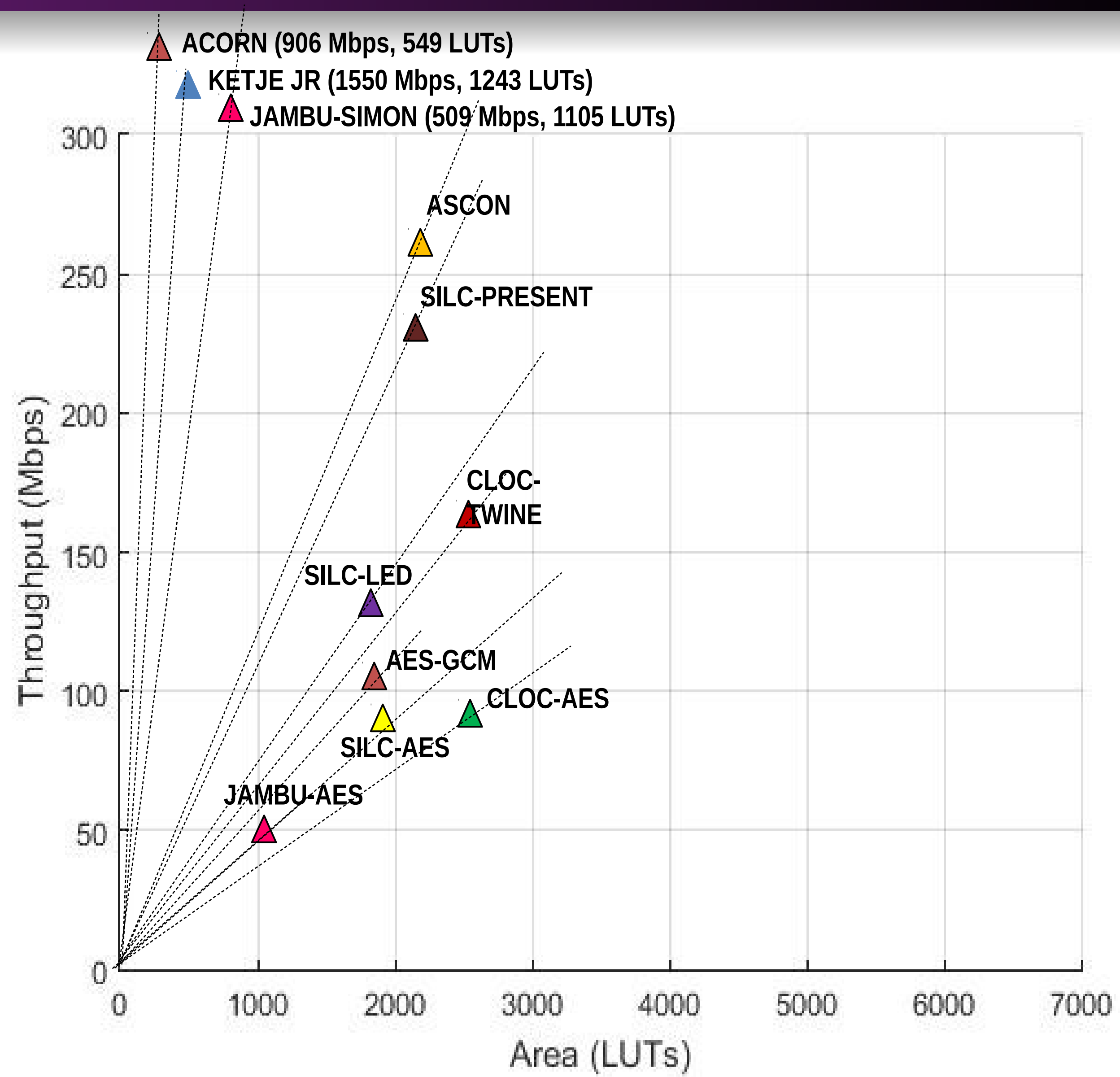
JAMBU-AES



SILC-AES

Benchmarking of Unprotected Implementations

- Xilinx ISE 14.7 Spartan-6
- Identical architectures
- Optimized using ATHENa[1]
- Smallest:
  1) ACORN
  2) JAMBU-AES
  3) JAMBU-SIMON
- Highest Throughput:
  1) Ketje
  2) ACORN
  3) JAMBU-SIMON



1 – [ATHENa17]

Benchmarking of Protected Implementations

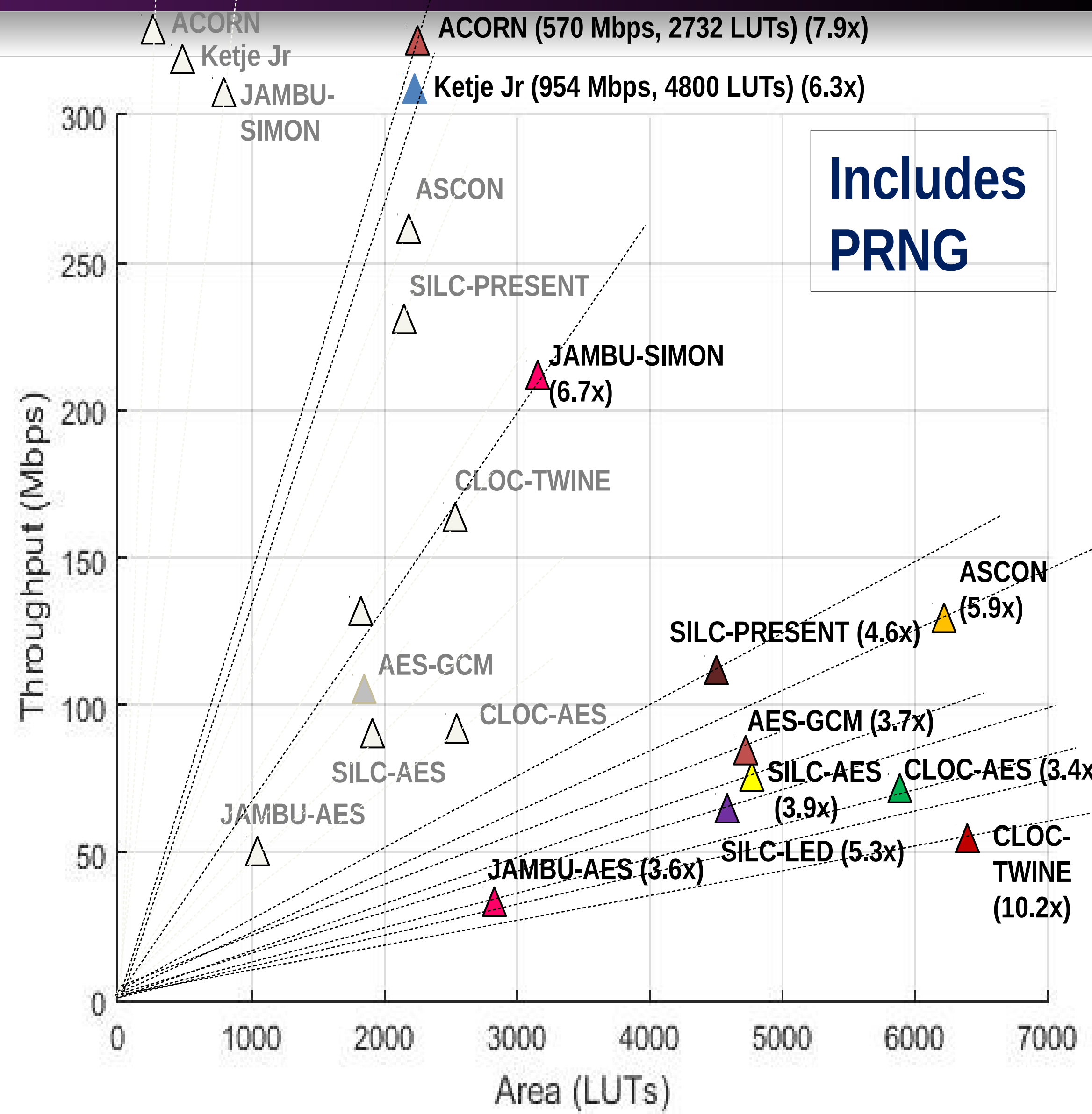
- Smallest:
  1) ACORN
  2) JAMBU-AES
  3) JAMBU-SIMON

No change in order

- Highest Throughput:
  1) Ketje
  2) ACORN
  3) JAMBU-SIMON

No change in order

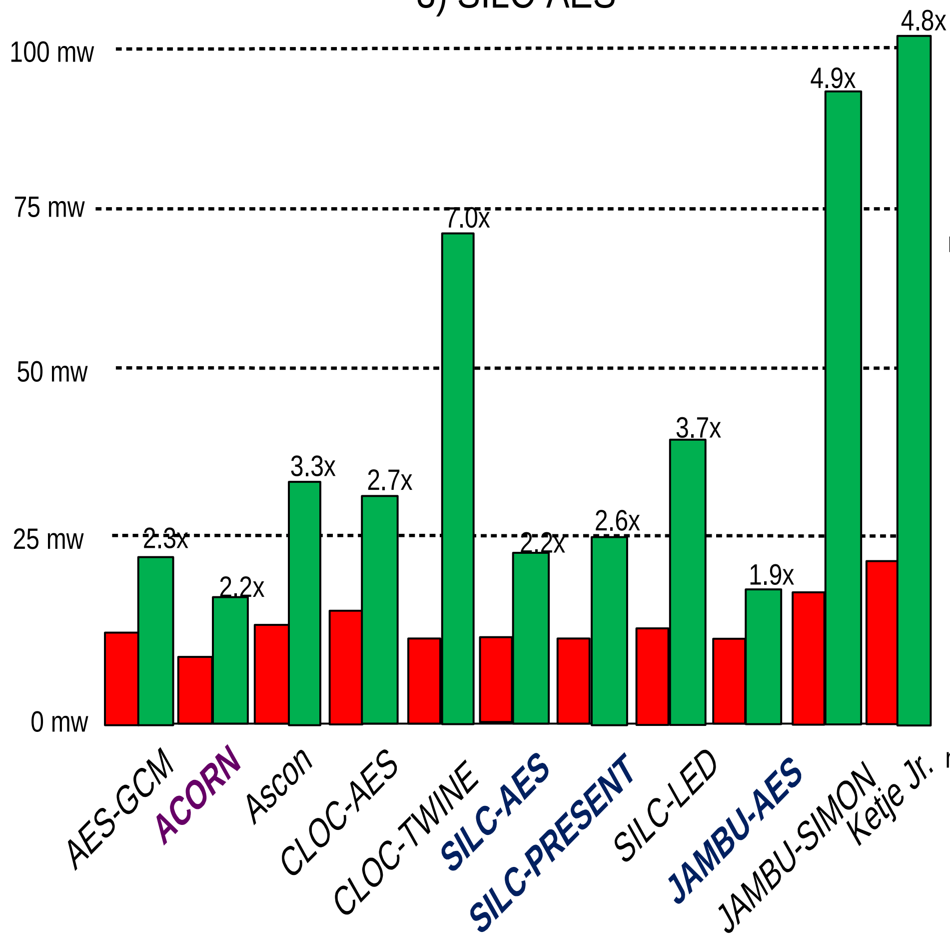
- On average
  - Area increase: **3.1x**
  - TP reduction: **1.8x**
  - TP/A reduction: **5.6x**



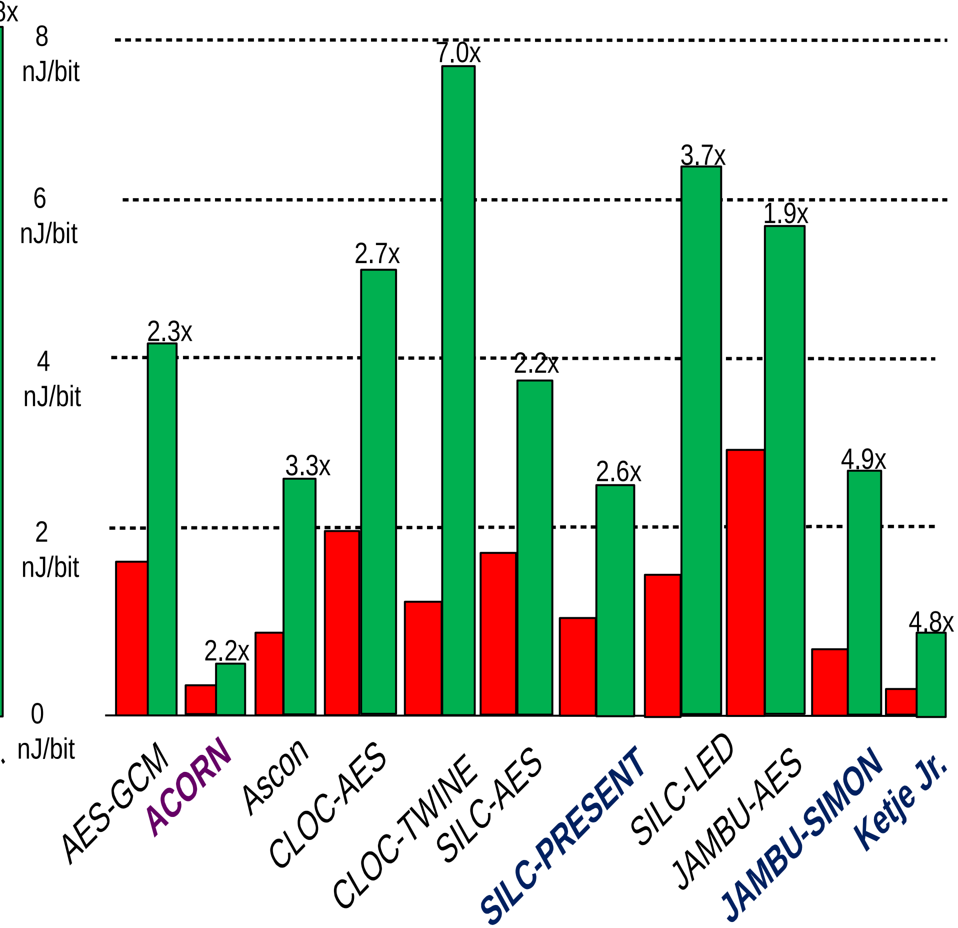
Power and Energy-per-bit (Spartan 6 @ 10 MHz)

Lowest power (unprotected): 1) ACORN 2) JAMBU-AES 3) SILC-PRESENT
Lowest power (protected): 1) ACORN 2) JAMBU-AES 3) SILC-AES

Lowest E/bit (unprotected): 1) Ketje Jr 2) ACORN 3) JAMBU-SIMON
Lowest E/bit (protected): 1) ACORN 2) Ketje Jr 3) SILC-PRESENT



Power (mW)



Average increase: 3.4x

Energy (nJ/bit)

Summary of Results

Best Performers

Rank	Area	Throughput	Throughput / Area	Power	Energy
1	**ACORN**	Ketje Jr.	**ACORN**	**ACORN**	**ACORN**
2	JAMBU-AES	**ACORN**	Ketje Jr.	JAMBU-AES	Ketje Jr.
3	JAMBU-SIMON	JAMBU-SIMON	JAMBU-SIMON	SILC-AES	SILC-PRESENT

Problem Areas

Area	**Ascon** (64-bit datapath, growth in S-Box, folded architecture); **CLOC-TWINE** (S-Box growth)
Throughput	**JAMBU-AES** (only one AES Core; Tag generation requires second call)
Power	**Ketje Jr.** (200-bit state in basic iterative architecture); **JAMBU-SIMON** (48-bit unrolled x4 architecture)
Energy	**CLOC-TWINE** (High non-linearity in **TWINE** primitive & CLOC layer)
Randomness	**Ketje** Jr. (200 bits/cycle); **Ascon** (192 bits/cycle); **ACORN** (120 bits/cycle)

W. Diehl, A. Abdulgadir, F. Farahmand, J.P. Kaps and K. Gaj, "Comparison of Cost of Protection Against Differential Power Analysis for Selected Authenticated Ciphers," HOST 2018

Improved Comparison
ACORN vs. Ascon

Areas for Improvement

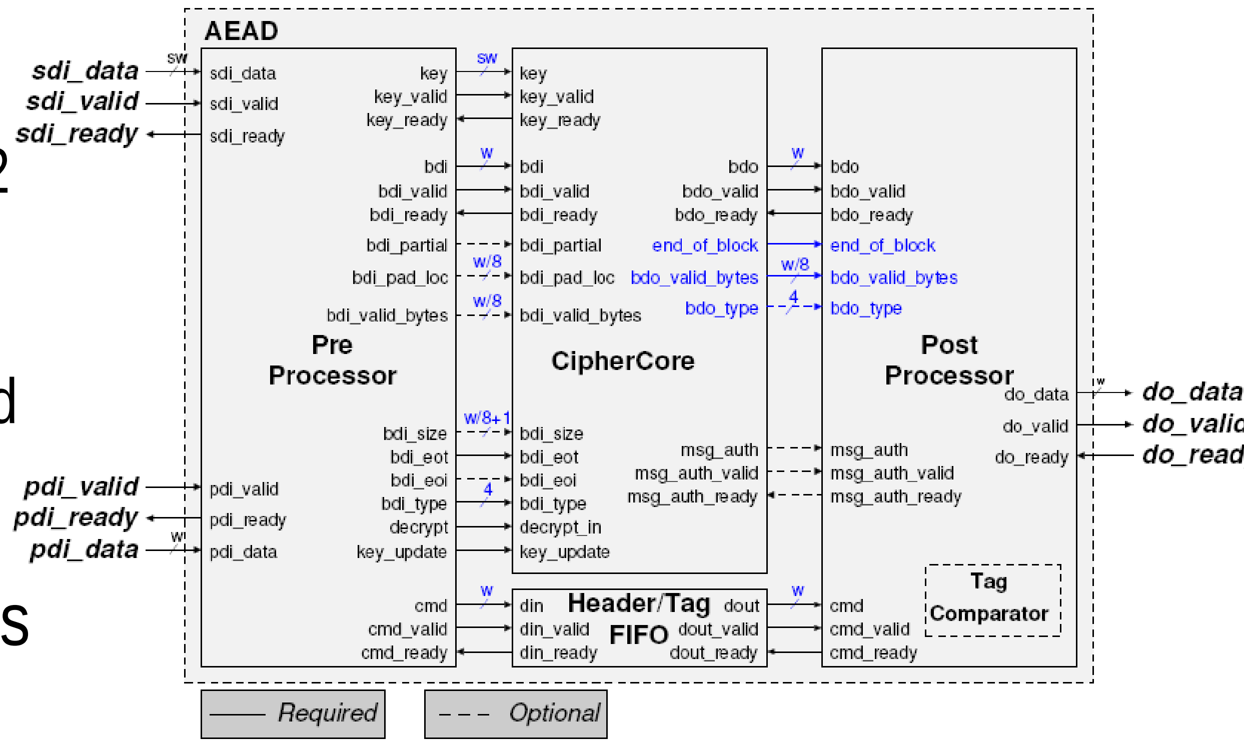
- **Better lightweight implementations**
- **Improved ability to pin-point leakage**
- Reduced requirements for randomness
- Improved Random Number Generation
- Estimation of side channel resistance through glitch transitions

Suboptimal Protected Implementations

- CAESAR Round 3 HW submissions optimized for TP/A ratio
  - Full-width datapaths (= more register writes/cycle, higher power)
  - Basic iterative architectures (= longer critical paths; glitch chains)
- But threshold implementations (TI) favor smaller designs
  - Quadratic growth in area
  - Smaller critical paths (= register after each non-linearity)
  - Fewer random bits / cycle
- CAESAR HW Development Package optimized for High Speed
  - External I/O bus widths ≥ 32 bits
  - Includes extra functionality

Solution: Build Improved Lightweight Implementations

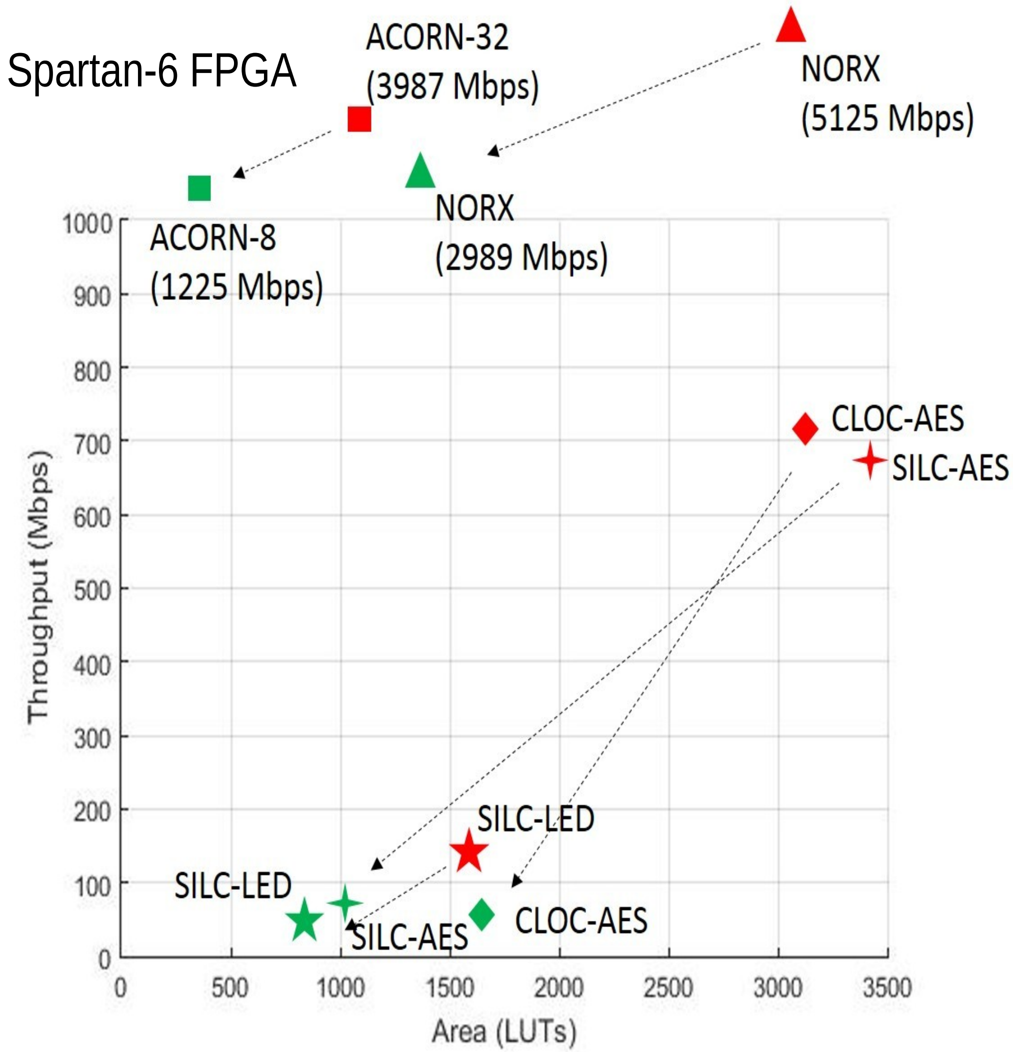
- Development Package v2.0 (Dec 2017)
  - I/O bus widths of 8, 16, or 32 bits
  - User-defined padding
  - Potentially reduced overhead compared to High Speed[1]
- Redesigned implementations
  - Reduced datapath widths
    - 16-bit AES
    - ACORN-8 vs. ACORN-32
  - Increased clock cycles

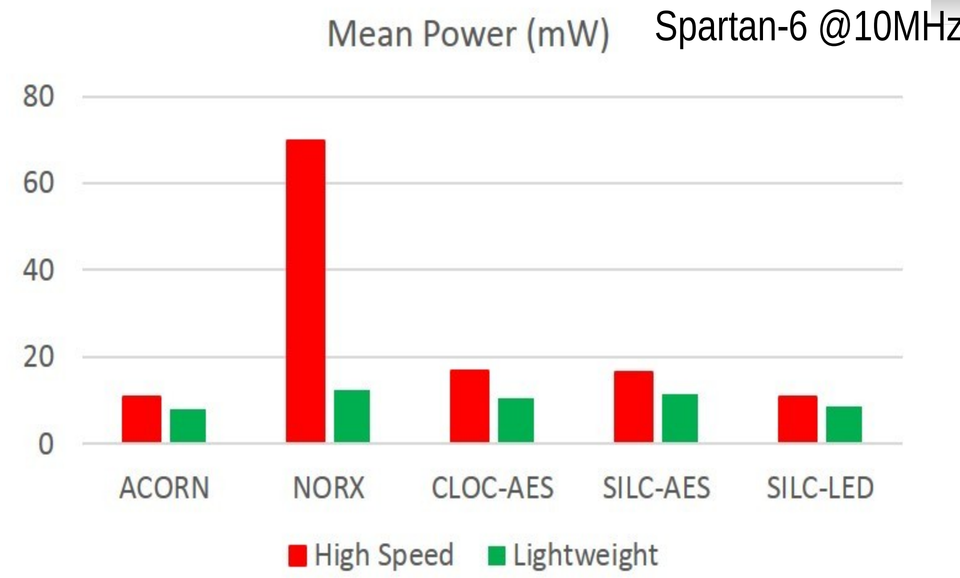


AEAD using Development Package v2.0

1 - Yalla & Kaps, ReConfig 2017

Improved Unprotected Lightweight Implementations



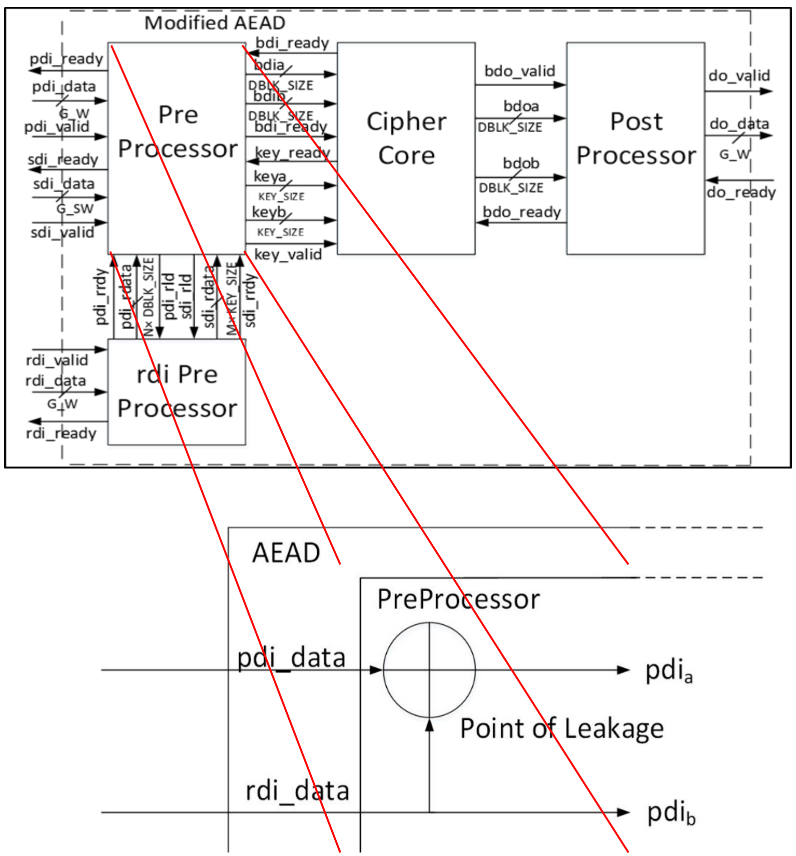


40% area reduction
55% power reduction
But…
44% reduction in TP/A ratio
3.6x increase in E/bit

F. Farahmand, W. Diehl, A. Abdulgadir, J. P. Kaps and K. Gaj,"Improved Lightweight Implementations of CAESAR Authenticated Ciphers," FCCM 2018

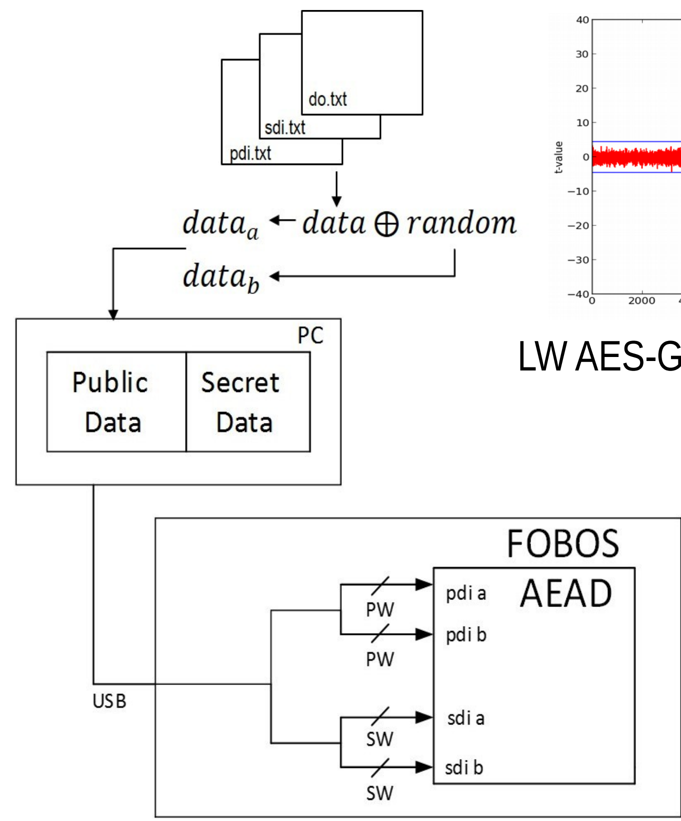
How to fix the leakage?

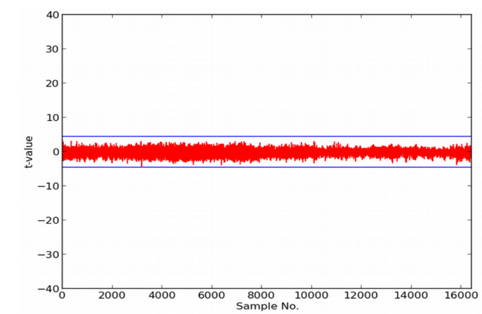
Problem



Share Separation in Hardware

Solution





LW AES-GCM @ 20,000 traces after fix

Share Separation in Software

Improved Comparison of Protected Implementations

- New lighterweight implementations of ACORN, Ascon, AES-GCM
  - Development Package v2.0
  - Share Separation in Software (FOBOS upgrade)
- **Two** optimization targets: ACORN & Ascon (2 each) which are
  1) Close to (but less than) area of (protected) AES-GCM
     - **"area-equivalent" – How does TP change?**
  2) Close to (but greater than) throughput of (protected) AES-GCM
     - **"TP-equivalent" – How does area change?**

How to hit targets?

Given: Results of new (LW) AES-GCM: 4429 LUTs, 77 Mbps

Given: Results of previous protected ACORN & Ascon (*)

Estimate:

1) **"Area-equivalent"**

ACORN: Since Area$_{\text{AES-GCM}}$ >> Area$_{\text{ACORN-8}}$, pick largest ACORN = **ACORN-32**

Ascon: Since Area$_{\text{Ascon}}$ ~ Area$_{\text{AES-GCM}}$, pick 64-bit, 5-cycle **Ascon-*large***

2) **"TP-equivalent"**

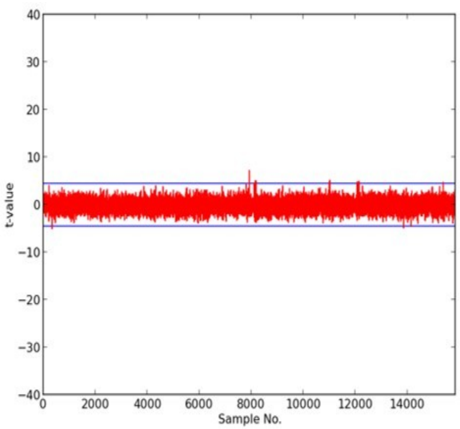
ACORN: TP$_{\text{ACORN-8}}$ (570 Mbps) ÷8 = 71 Mbps ≈ TP$_{\text{AES-GCM}}$ so pick **ACORN-1**

Ascon: TP$_{\text{Ascon}}$ (134) ÷ 2 = 67 Mbps ≈ TP$_{\text{AES-GCM}}$ so pick 10+ cycle **Ascon-*small***

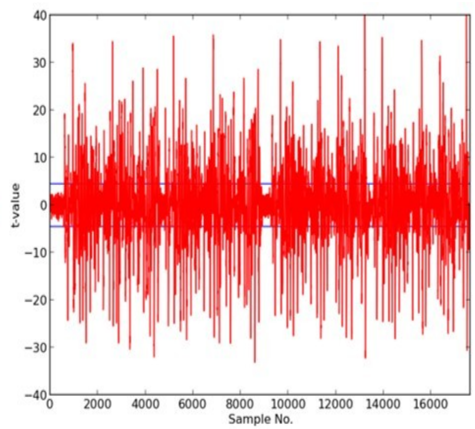
* Including PRNG

Results of T-Tests

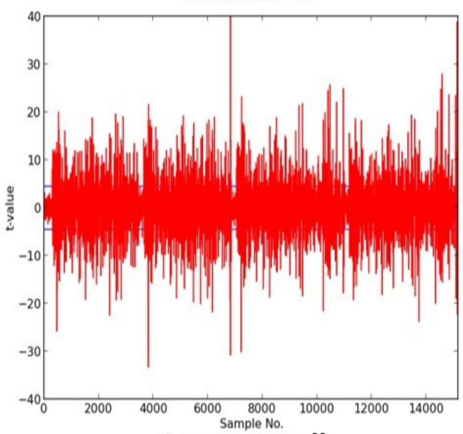
Unprotected



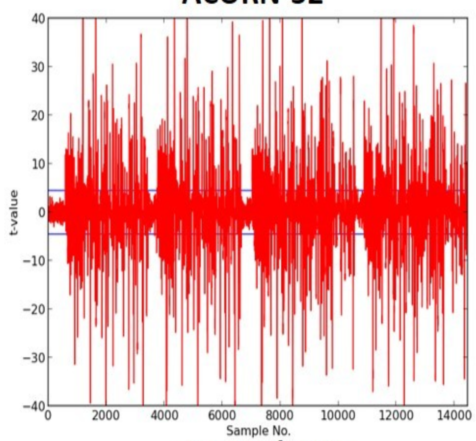
ACORN-1



ACORN-32

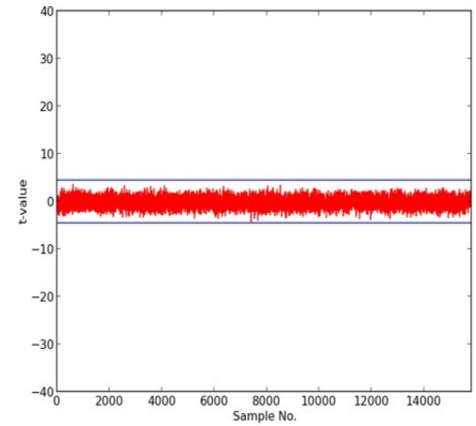


Ascon-*small*

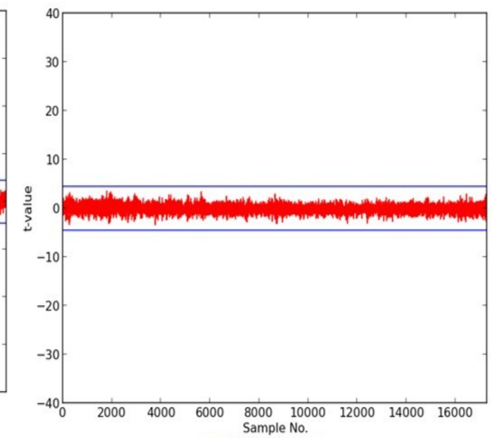


Ascon-*large*

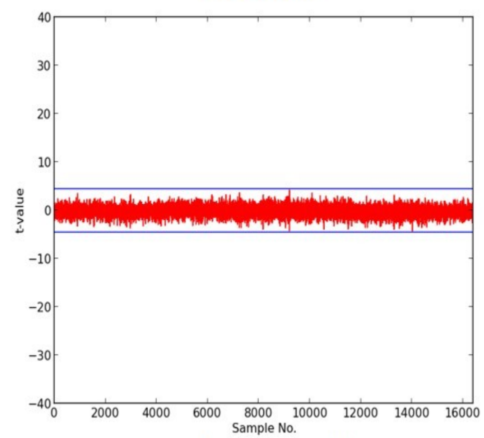
Protected



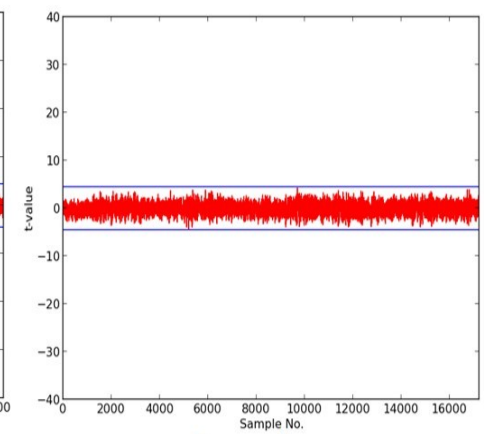
ACORN-1



ACORN-32



Ascon-*small*



Ascon-*large*

ACORN vs. Ascon: Results

Area-equivalent

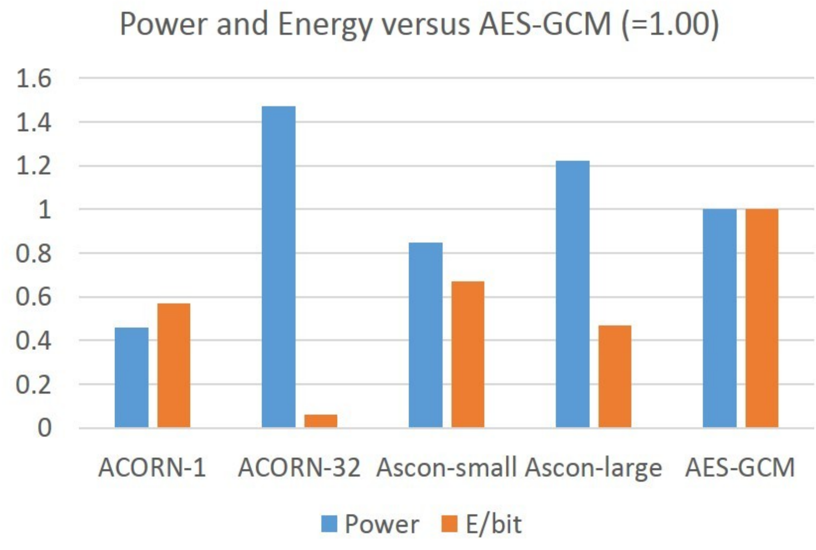
ACORN-32 – 92% Area$_{\text{AES-GCM}}$, but **23.3x** TP$_{\text{AES-GCM}}$

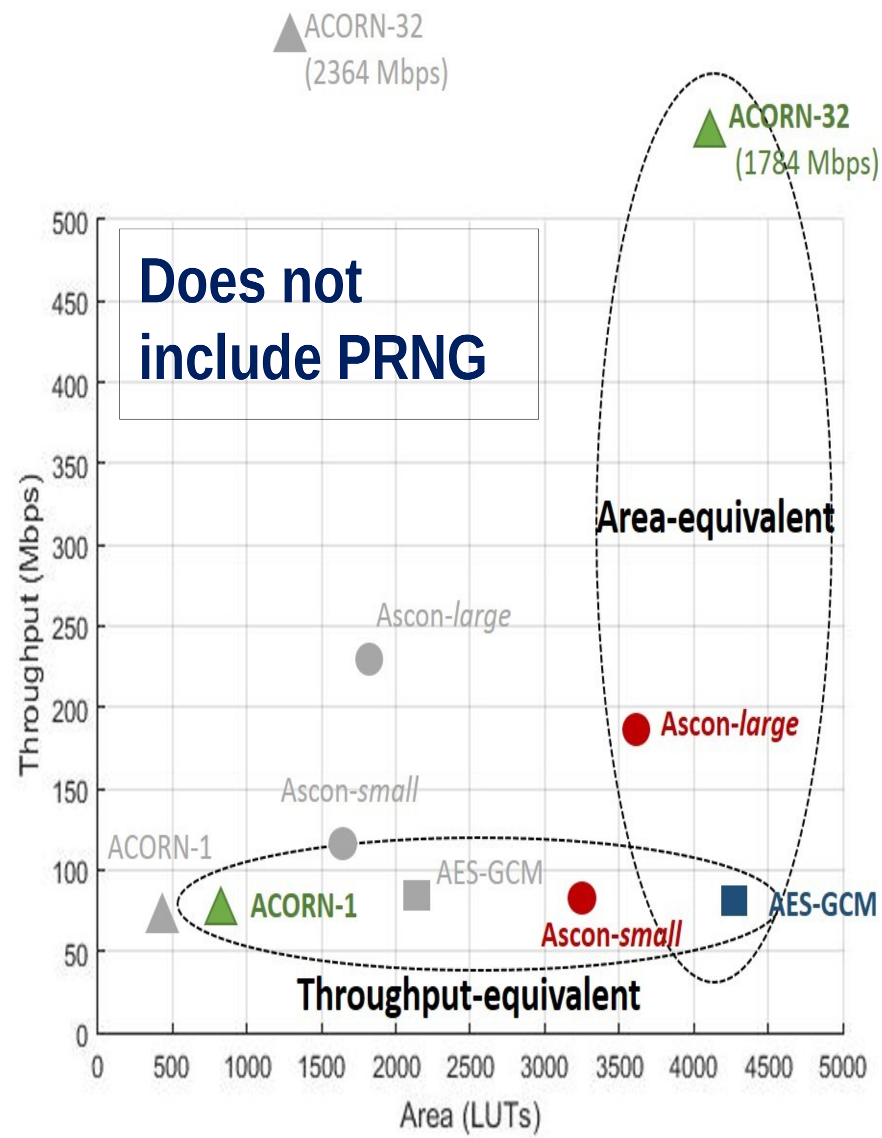
Ascon-large – 83% Area$_{\text{AES-GCM}}$, but **2.5x** TP$_{\text{AES-GCM}}$

TP-equivalent

ACORN-1 ≈ TP$_{\text{AES-GCM}}$, but **18%** Area$_{\text{AES-GCM}}$

Ascon-small – 1.2x TP$_{\text{AES-GCM}}$, but **74%** Area$_{\text{AES-GCM}}$





Conclusions & Future Work

Summary

- CAESAR Round 3 Candidates
- ACORN-8 best in area, TP/A ratio, power, energy per bit
  - Ketje Jr. and JAMBU-SIMON high TP, but high power;
  - JAMBU-AES, SILC-AES, SILC-PRESENT place well (various metrics)
- Effects of implementations not optimized for protection
- Challenge of initial mixing of randomness
- Improved LW implementations
- Improved comparison of CAESAR finalists: ACORN & Ascon
  - Both improve over AES-GCM, but **ACORN is best**

Future Research

- Reduce randomness requirements
- Improve random number generation
- Measure leakage due to glitches
- Signature analysis
- Heterogeneous architectures
- Post Quantum Cryptography

Thanks for your Attention