WPI

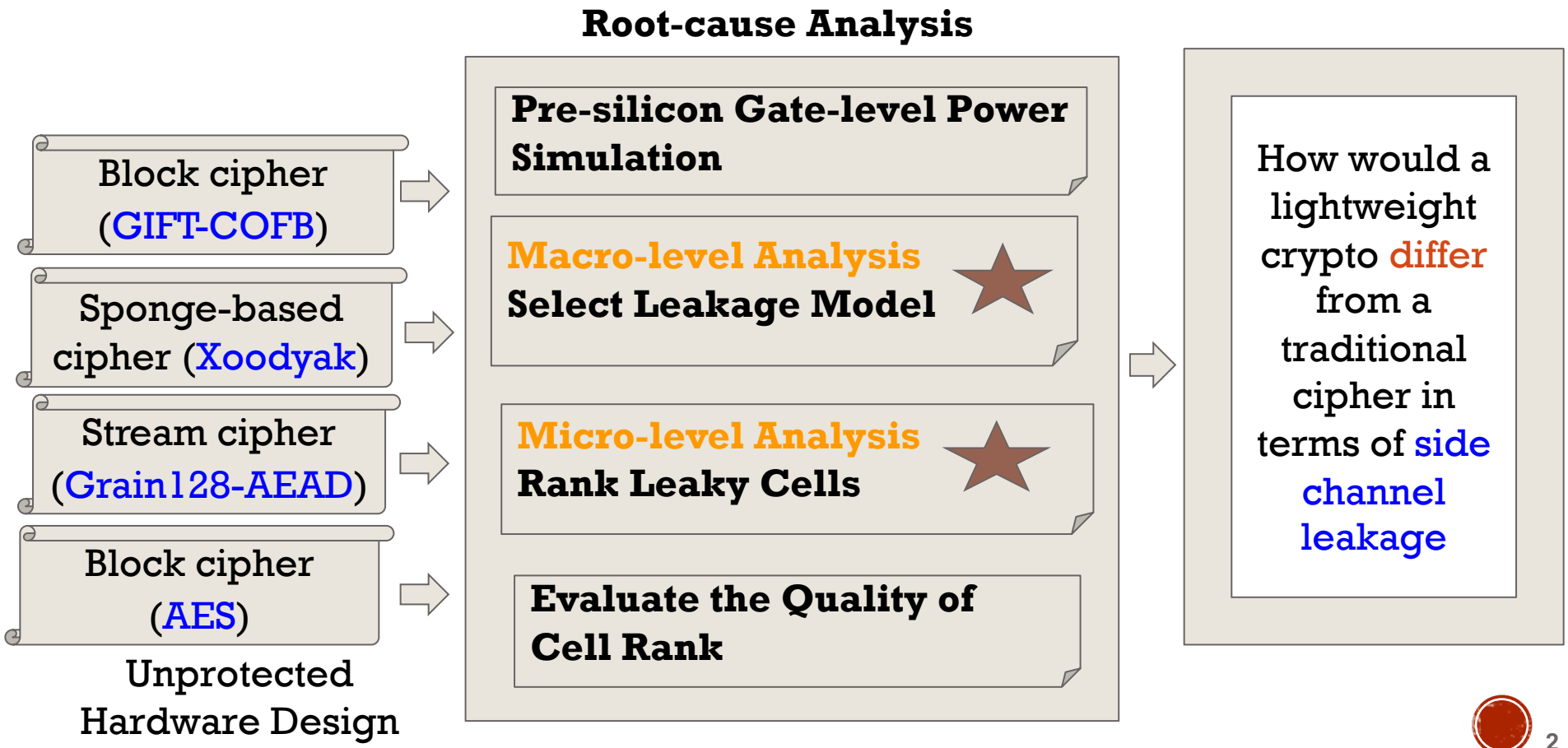
VERNAM LAB
Worcester Polytechnic Institute

ROOT-CAUSE ANALYSIS OF POWER-BASED SIDE-CHANNEL LEAKAGE IN LIGHTWEIGHT CRYPTOGRAPHY CANDIDATES

Zhenyuan Liu and Patrick Schaumont
Worcester Polytechnic Institute, Worcester, Massachusetts

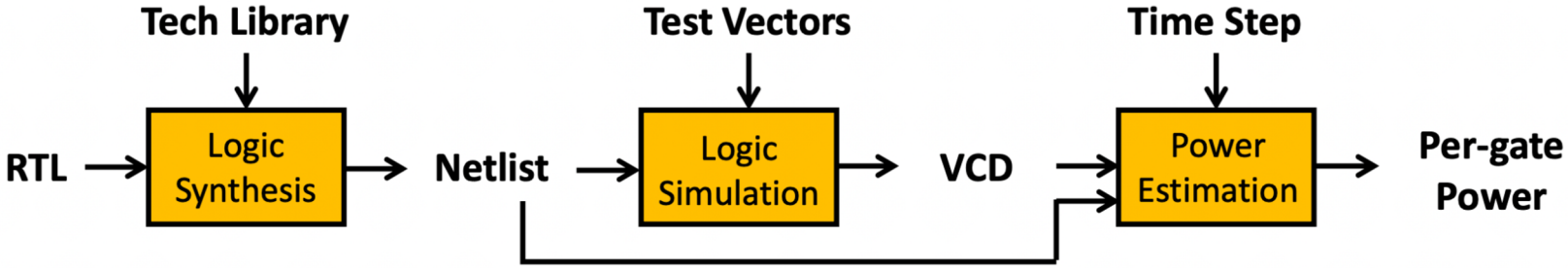
NIST Fifth Lightweight Cryptography Workshop 2022

OVERVIEW

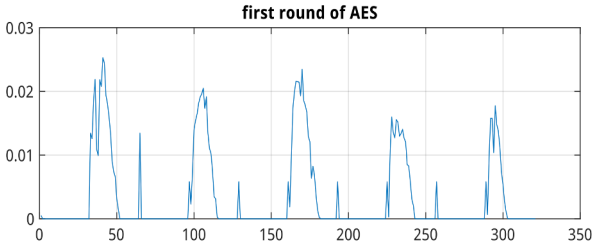

Root-cause Analysis
Block cipher (GIFT-COFB)
Sponge-based cipher (Xoodyak)
Stream cipher (Grain128-AEAD)
Block cipher (AES)
Unprotected Hardware Design
Pre-silicon Gate-level Power Simulation
Macro-level Analysis
Select Leakage Model
Micro-level Analysis
Rank Leaky Cells
Evaluate the Quality of Cell Rank
How would a lightweight crypto differ from a traditional cipher in terms of side channel leakage

PRE-SILICON GATE-LEVEL POWER SIMULATION

- Cadence Genus.
- Cadence Joules.
- SkyWater 130nm.



256 test-vectors,
321 timestamps,
9640 cells



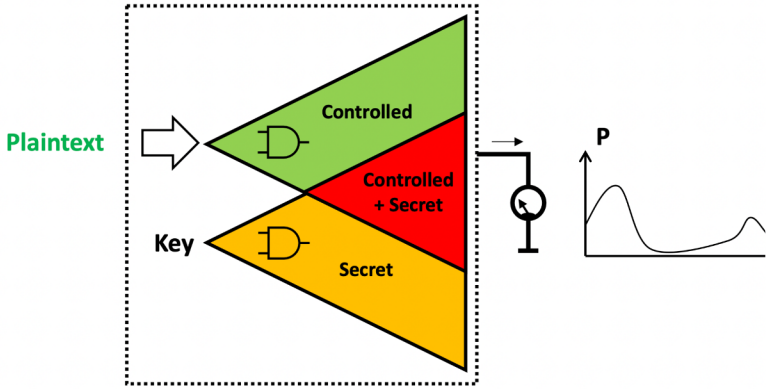
Gate-level Power(v,t,g)

Test-vector

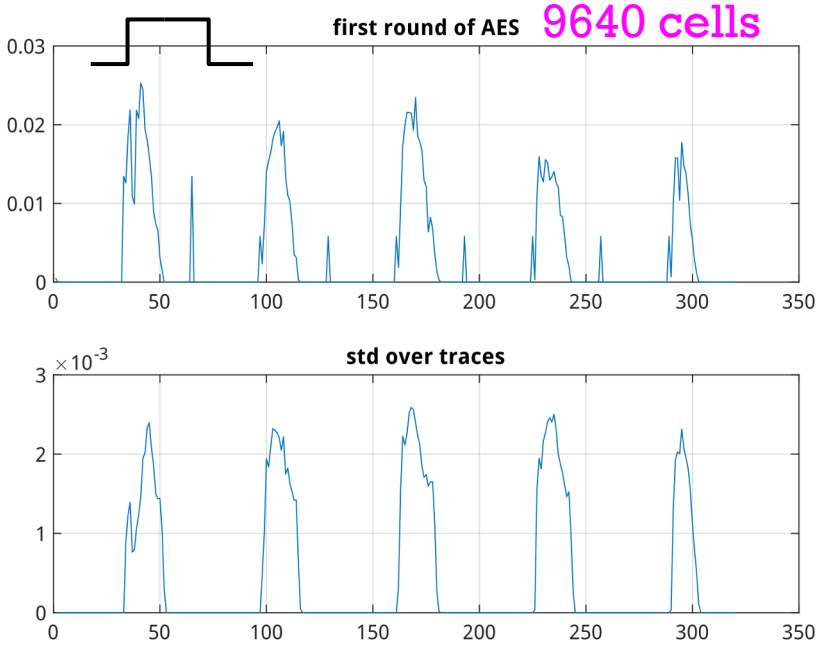
Discrete-time stamp

cells

PRE-SILICON GATE-LEVEL POWER SIMULATION - AES



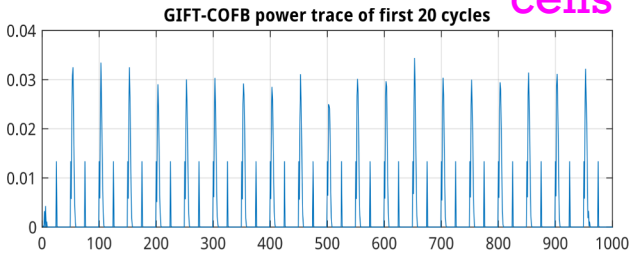
Maximize the proportion of side-channel leakage in the overall power consumption of a design

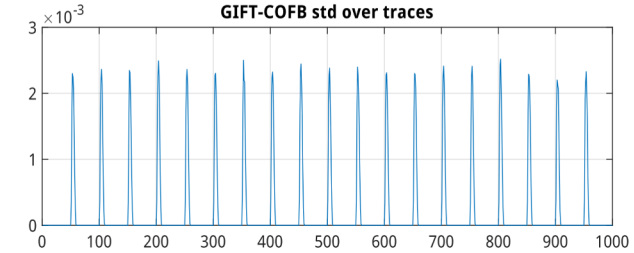


- **First round of AES.**
- 256 test vectors.
- Fixed key and random plaintext.
- Clock freq 50MHz.
- Oversampled at 64 samples per clock cycle.

PRE-SILICON GATE-LEVEL POWER SIMULATION - LWC

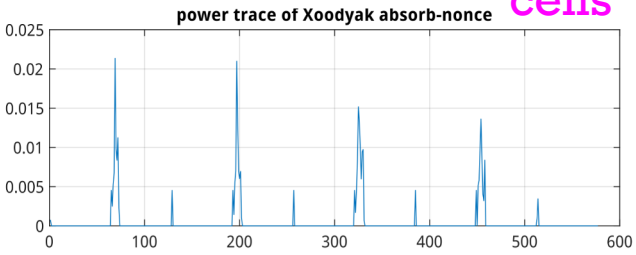
3286 cells

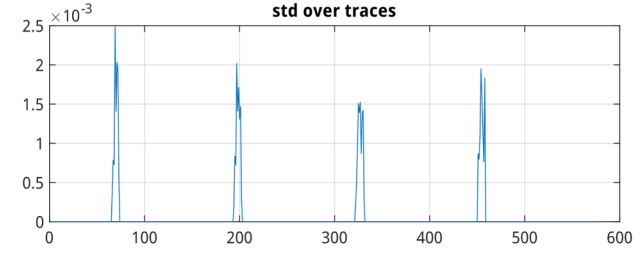




- **First 20 cycles of encryption (40 cycles in total).**
- 256 test vectors.
- Fixed key, random nonce, fixed data.
- Clock freq 50MHz.
- Oversampled at 50 samples per cycle.

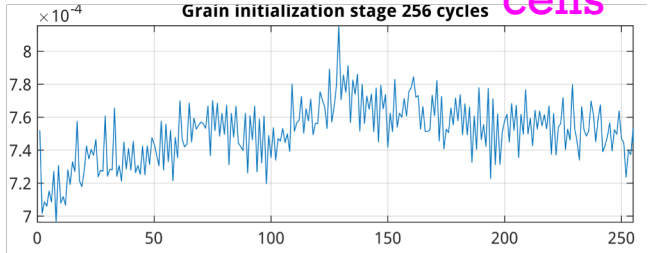
3630 cells

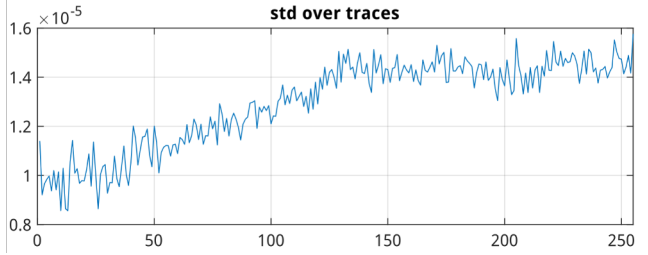




- **4 rounds of absorb-nonce (2 cycles per round).**
- 256 test vectors.
- Fixed key and random nonce.
- Clock freq 50MHz
- Oversampled at 64 samples per cycle.

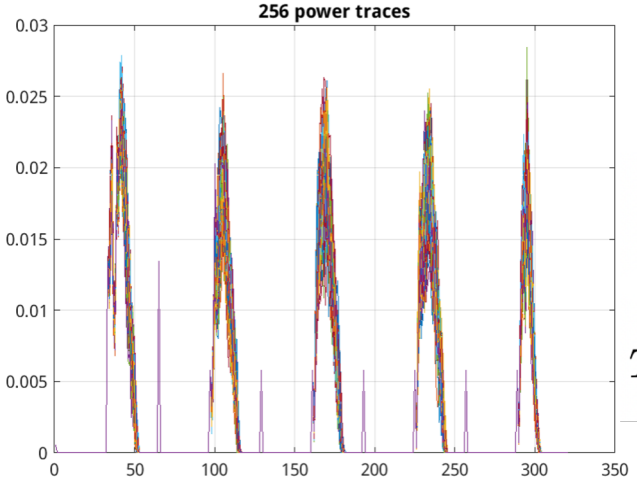
602 cells





- **256 cycles of the initialization.**
- 256 test vectors.
- Fixed key and random nonce.
- Clock freq 50MHz.
- Sampled at 1 samples per cycle.

MACRO-LEVEL ANALYSIS (SELECT LEAKAGE MODEL)



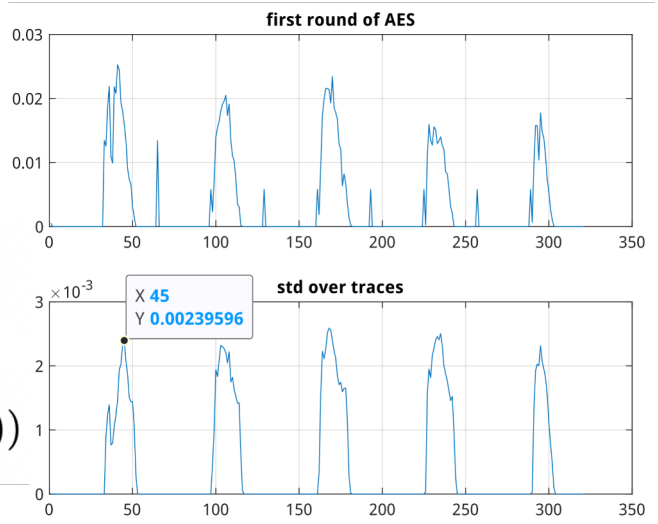
design-global power trace

per-cell power traces

$$P(v,t) = \sum_{g} P(v,t,g)$$

$$s(t) = \underset{v}{std}(P(v,t))$$

$$T = \{t_1, t_2, t_3, ...\} = \underset{t}{localmax}(s(t))$$



Rationale: Identify *leaky points*, **the timestamps of maximum data-dependent variation** in the power traces. Side-channel leakage is **largest** at time points with the **highest data-dependency** of the power consumption.

MICRO-LEVEL ANALYSIS (RANK LEAKY CELLS)

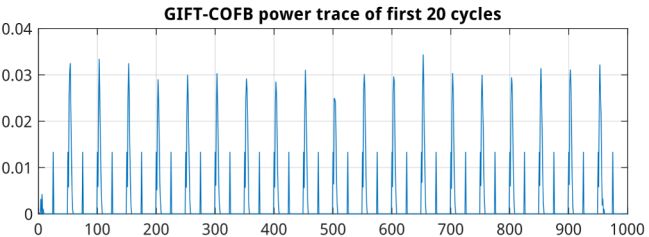
leakage estimation

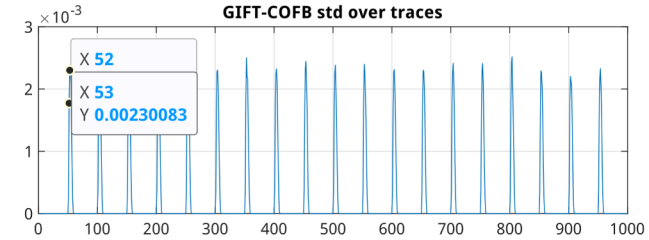
$$leakage(v,g) = \sum_{T} P(v,t,g)$$

$$l(g) = \underset{v}{std}(leakage(v,g))$$

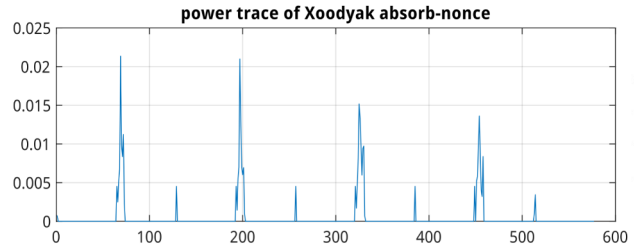
$$G = \{g_1, g_2, g_3, ...\} = argrank(l(g))$$

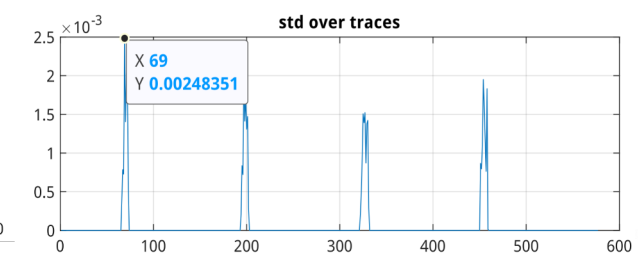
Previous selected leaky points



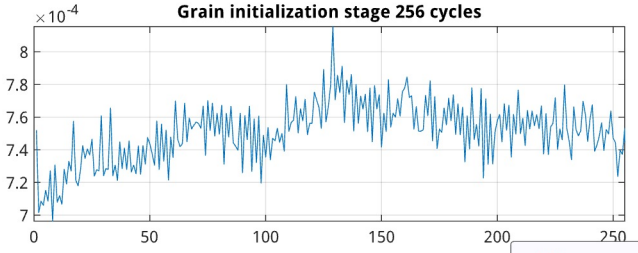


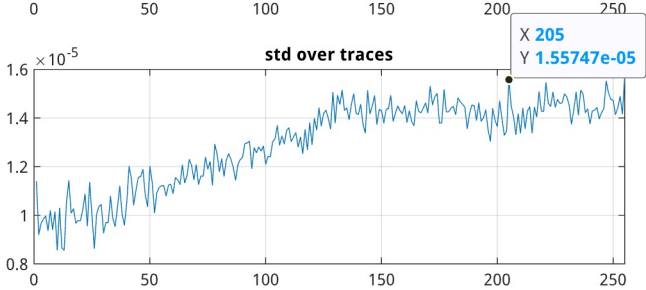
Two leaky points per cycle





One leaky point per cycle

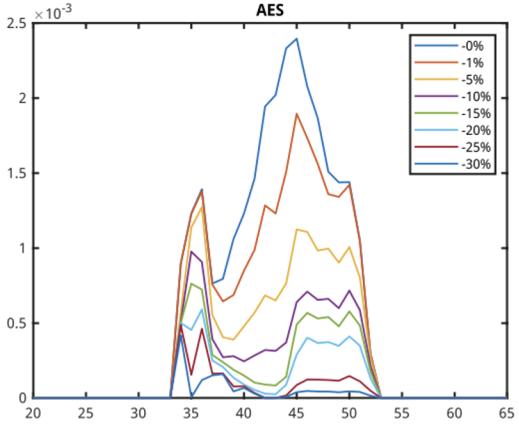


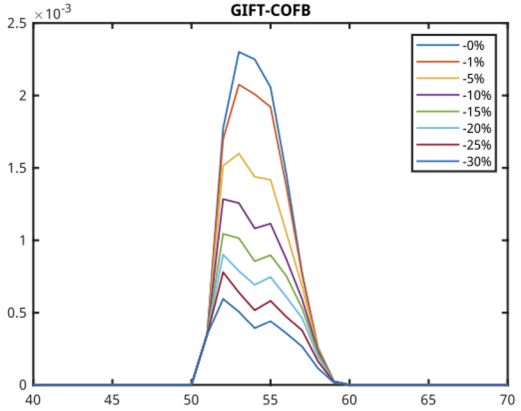


Overall one leaky point

EVALUATE THE QUALITY OF CELL RANK - TOP RANKED CELL REMOVAL

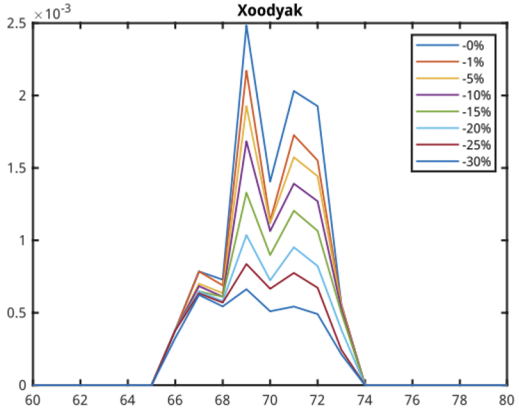
One cycle

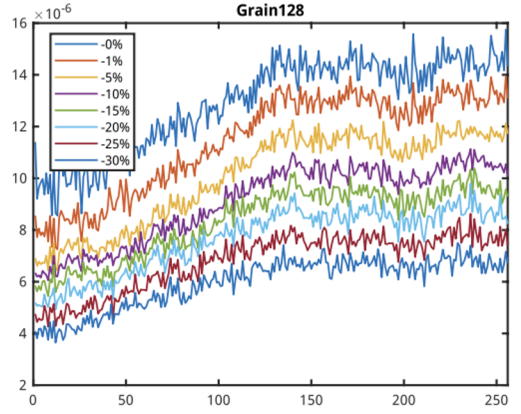




One cycle

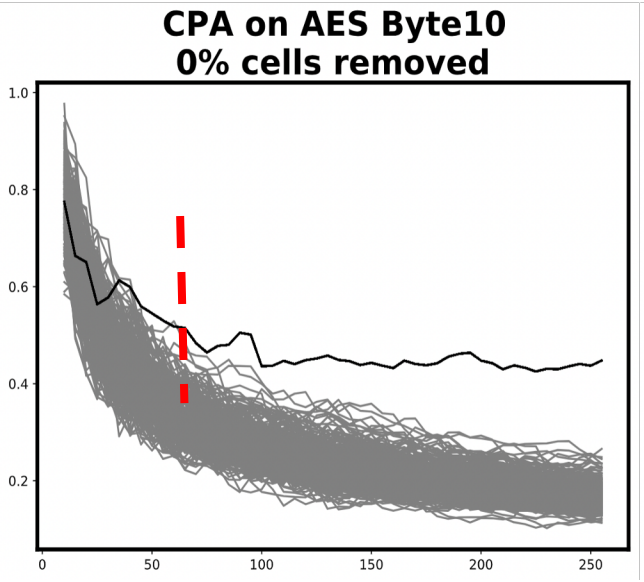
One cycle

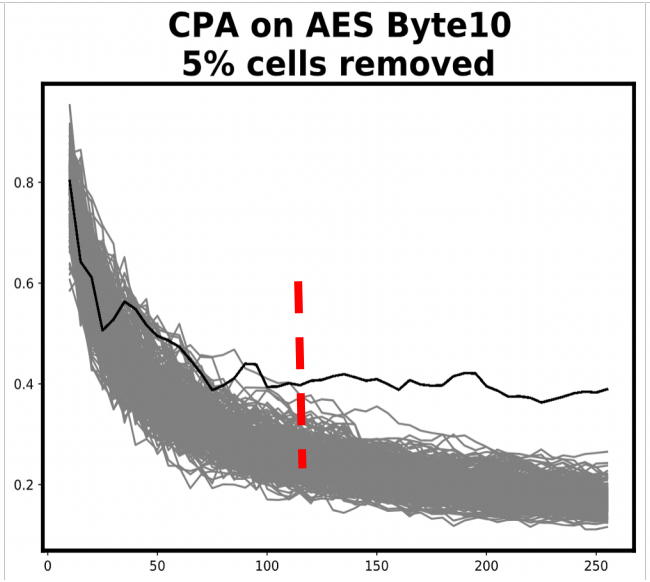


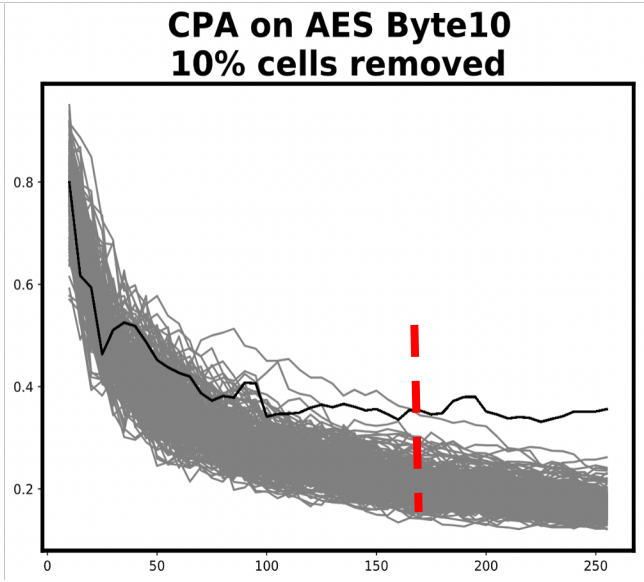


256 cycles

EVALUATE THE QUALITY OF CELL RANK - CPA ON AES



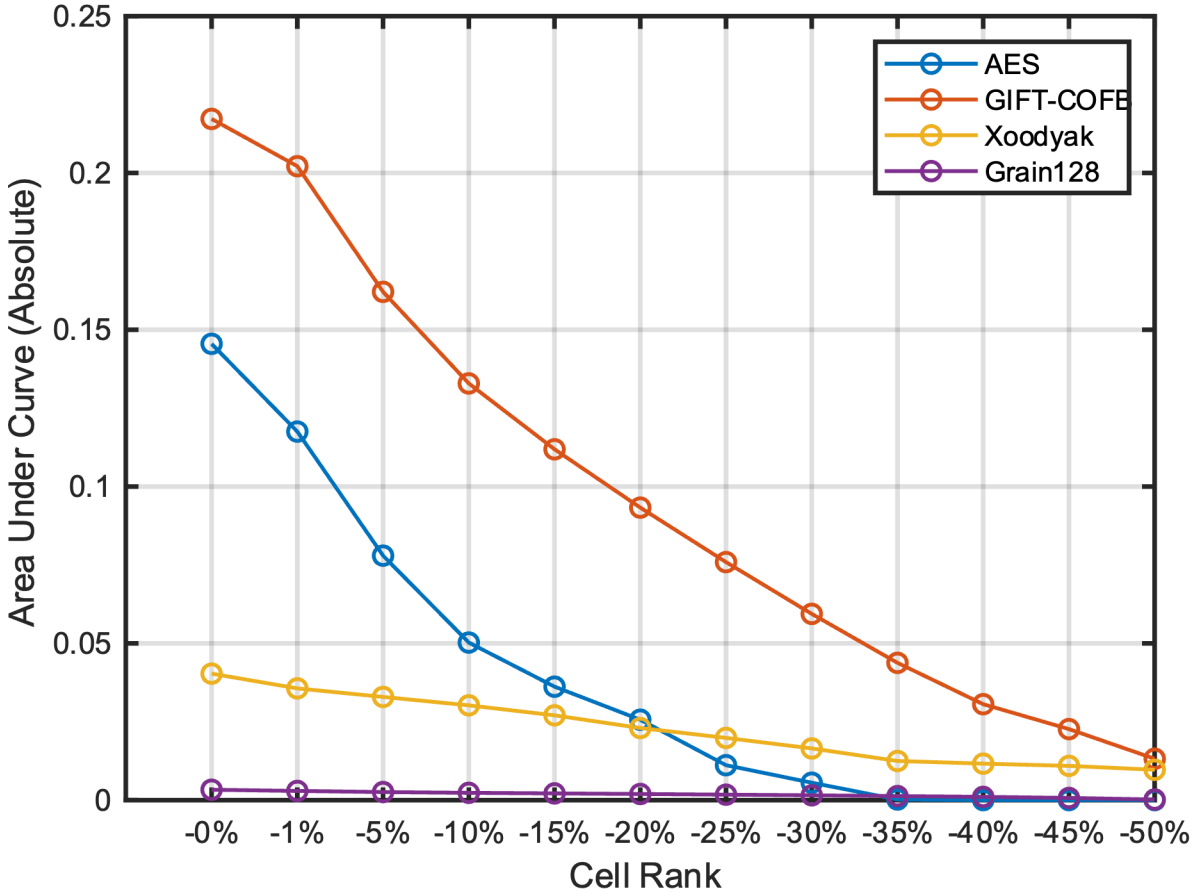




ROOT-CAUSE ANALYSIS OF POWER SIDE-CHANNEL LEAKAGE

the area under the curve of power stdv

the total amount of side channel leakage



the cells that are removed according to cell rank

CONCLUSION

- AES and GIFT leak power side channel information with a sharper slope than Xoodyak and Grain.
- GIFT leaks more power side channel information than AES because more gates are contributing to power side channel in GIFT than AES in a relative term.
- Less leaky than GIFT, Xoodyak also has more gates that are contributing to power side channel than AES in a relative term.
- Grain is less leaky comparing to GIFT and Xoodyak but still has more gates that are contributing to power side channels than AES in a relative term.

REFERENCES

WPI

VERNAM LAB
Worcester Polytechnic Institute

- Ileana Buhan, Lejla Batina, Yuval Yarom, and Patrick Schaumont. Sok: Design tools for side-channel-aware implementations. IACR Cryptol. ePrint Arch., page 497, 2021.
- Subhadeep Banik, Avik Chakraborti, Tetsu Iwata, Kazuhiko Minematsu, Mridul Nandi, Thomas Peyrin, Yu Sasaki, Siang Meng Sim, and Yosuke Todo. Gift-cofb. Cryptology ePrint Archive, 2020.
- Thomas De Cnudde, Begu ̈l Bilgin, Benedikt Gierlichs, Ventzislav Nikov, Svetla Nikova, and Vincent Rijmen. Does coupling affect the security of masked implementations? In Sylvain Guilley, editor, Constructive Side- Channel Analysis and Secure Design, pages 1–18, Cham, 2017. Springer International Publishing.
- Joan Daemen, Seth Hoffert, Micha ̈el Peeters, G Van Assche, and R Van Keer. Xoodyak, a lightweight cryptographic scheme. 2020.
- Svetla Nikova, Christian Rechberger, and Vincent Rijmen. Threshold im- plementations against side-channel attacks and glitches. In Peng Ning, Sihan Qing, and Ninghui Li, editors, Information and Communications Security, 8th International Conference, ICICS 2006, Raleigh, NC, USA, December 4-7, 2006, Proceedings, volume 4307 of Lecture Notes in Com- puter Science, pages 529–545. Springer, 2006.
- Kostas Papagiannopoulos, Ognjen Glamocanin, Melissa Azouaoui, Dorian Ros, Francesco Regazzoni, and Mirjana Stojilovic. The side-channel metric cheat sheet, 2022.
- JonathanSo ̈nnerup,MartinHell,MattiasS ̈onnerup,andRipudaman Khattar. Efficient hardware implementations of grain-128aead. In In- ternational Conference on Cryptology in India, pages 495–513. Springer, 2019.
- Chao Wang and Patrick Schaumont. Security by compilation: an auto- mated approach to comprehensive side-channel resistance. ACM SIGLOG News, 4(2):76–89, 2017.