TVLA, Correlation Power Analysis and Side-Channel Leakage Assessment Metrics

William Unger[1], Liljana Babinkostova[1], Mike Borowczak, Robert Erbes[3], and Aparna Srinath[1]

[1]Boise State University, [2]University of Wyoming, [3]Idaho National Laboratory

Lightweight Cryptography Workshop 2022
May 9-11, 2022

Overview of GIFT-COFB

GIFT-COFB is a lightweight block cipher based AEAD with the GIFT block cipher. Each round of GIFT consists of 3 steps:

SubCells, PermBits and AddRoundKey

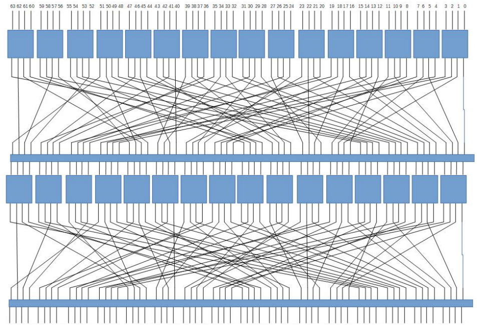


Figure: GIFT-64 Round Function

- GIFT-64, 28-rounds with 64-bit block size, and 128-bit key size.
- GIFT-128, 40-rounds with 128-bit block size, and 128-bit key size.
- The underlying algebraic structure is the field $\mathbb{F}_{2^{64}}$ with the irreducible polynomial $p_{64}(x) = x^{64} + x^4 + x^3 + x + 1.$

Correlation Power Analysis (CPA)

Iterated Block Cipher. A block cipher obtained by iterating r times a round function $R : \mathbb{F}_2^n \to \mathbb{F}_2^n$, each time with a different key $K_i \in \mathcal{K}$.

$$X_i = R_{K_i}\left(X_{(i-1)}\right) \text{ for } 1 \leq i \leq r$$

Correlation Power Analysis (CPA). Given a set of power traces and the corresponding sets of intermediate values, Correlation Power Analysis (CPA) aims at recovering the secret subkey using a correlation factor between the measured power samples and the power model of the computed sensitive values.

- Hamming Weight (HW) Model
- Hamming Distance (HD) Model

Correlation Power Analysis (CPA): Success Rate

Let $g = \left[g_1, g_2, \ldots, g_{2^{|k|}}\right]$ be a vector of guessed values for the subkey k with the possible candidates sorted in descending order. The success rate of order $o \leq 2^{|k|}$ of a side-channel key recovery attack is

$$\mathrm{SR}_o\left(k^*, g\right) = \begin{cases} 1, & \text{if } k^* \in [g_1, g_2, \ldots, g_o] \\ 0, & \text{otherwise} \end{cases}$$

The SR quantifies the amount of effort required to recover the correct subkey k^* from the guess vector and it serves as an indicator of how efficient an attack is.

Correlation Power Analysis: Execution Environment Hardware

- ChipWhisperer Lite as a control board and oscilloscope.
- ATXMEGA128D4 8-bit RISC micro-controller on a Chip Whisperer CW308 UFO target board.
- C-language implementation of GIFT-64 using 8-bit data types into the “simple serial” firmware provided with the ChipWhisperer.
- The CPA attack and the data analysis was performed using Python.

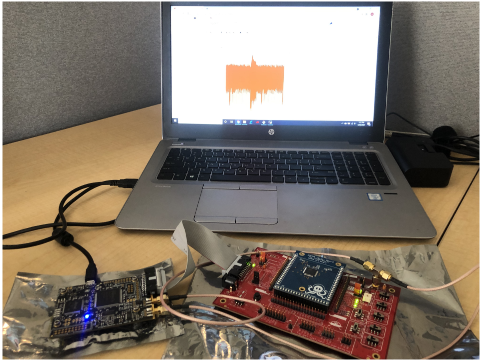
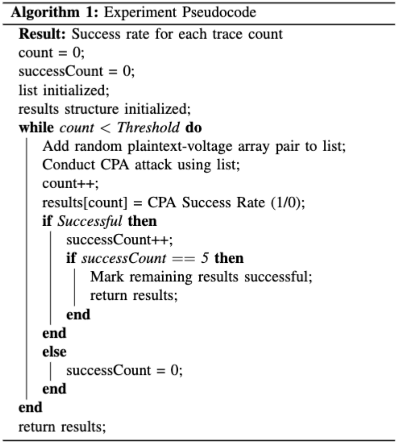


Figure: Hardware environment - Left:ChipWhisperer Lite - Right: XMEGA on CW308 UFO Board

Implementation of CPA: Execution Environment



Algorithm 1: Experiment Pseudocode

```
Result: Success rate for each trace count
count = 0;
successCount = 0;
list initialized;
results structure initialized;
while count < Threshold do
    Add random plaintext-voltage array pair to list;
    Conduct CPA attack using list;
    count++;
    results[count] = CPA Success Rate (1/0);
    if Successful then
        successCount++;
        if successCount == 5 then
            Mark remaining results successful;
            return results;
        end
    end
    else
        successCount = 0;
    end
end
return results;
```

- A threshold cap of 150 iterations and a pool of plaintext/voltage array pairs containing 2,000 entries.
- The Success Rate (SR) metric is used in order to quantify the amount of effort required to recover the correct key.
- We consider a trial to be a collection of 100 experiments in which the trial results output has ordered pairs similar to the output of the experiment, but the ’y’ values hold the mean success rate of the 100 executions of the experiments.

Implementation of CPA Using Hamming Weight Model

Point of Interest (POI): S-Box output in rounds 2, 3, 4, and 5 of the GIFT-64 algorithm.

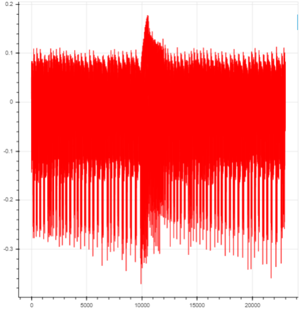


Figure: Sample voltage capture for execution of a portion of GIFT-64 on the XMEGA

Pearson's Correlation Coefficient

$$\frac{\sum (R_i - R_{avg}) \cdot (G_i - G_{avg})}{\sqrt{\sum (R_i - R_{avg})^2 \cdot \sum (G_i - G_{avg})^2}}$$

- A correlation is computed for each possible value of the targeted sub-key used in the round, and the sub-key with the highest correlation becomes the predicted value for that sub-key.

Non-Linearity and Transparency Order

Walsh-Hadamard Transform

$W_F(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{F(x) \oplus x \cdot u}$, where $u \in \mathbb{F}_2^n$ and $x \cdot u$ is an inner product.

Non-Linearity (NL) [1]

$$NL(F) = 2^{n-1} - \frac{1}{2} \max_{u \in \mathbb{F}_2^n, v \in \mathbb{F}_2^{n*}} |W_F(u, v)|$$

[1] M. Matsui. Linear Cryptanalysis Method for DES Cipher. In Advances in Cryptology EUROCRYPT'93,386-397. Springer, 1994.

Transparency Order and Revisited Transparency Order

Transparency Order (TO) [2]

$$\max_{\beta\in\mathbb{F}_2^n}\left(|n-2H(\beta)| - \frac{1}{2^{2n}-2^n}\sum_{a\in\mathbb{F}_2^{n*}} |\sum_{v\in\mathbb{F}_2^n, H(v)=1} (-1)^{v\cdot\beta} W_{D_aF}(0,v)|\right)$$

where D_aF represents the discrete derivative of a function F with input a.

Revisited Transparency Order (RTO)[3].

$$\max_{\beta\in\mathbb{F}_2^m}(m - \frac{1}{2^{2n}-2^n}\sum_{a\in\mathbb{F}_2^{n*}} |\sum_{j=1}^{m}\sum_{i=1}^{m}(-1)^{\beta_i\oplus\beta_j}\mathcal{C}_{F_i}, F_j(a)|)$$

where $C_{F_i,F_j}(a)$ is a cross correlation of functions F_i and F_j with input a.

[2] E. Prouff. DPA Attacks and S-boxes. In Fast Software Encryption, 424-441.Springer, 2005.

[3] K. Chakraborty et al. Redefining the Transparency Order. In Designs, Codes and Cryptography Vol. 82, 95–115 (2017)

Signal to Noise Ratio (SNR) and DPA-SNR

Signal to Noise Ratio (SNR)

Probabilistic measurement (commonly expressed in decibels as $20\log(SNR)$) of the quotient of the signal and noise in a cryptographic implementation

$$\text{SNR} = \frac{Var(Signal)}{Var(Noise)}^{4} \tag{1}$$

Differential Power Analysis SNR (DPA-SNR)[5]

$$n2^n\left(\sum_{a\in\mathbb{F}_2^n}\left(\sum_{i=0}^{n-1}\left(\sum_{x\in\mathbb{F}_2^n}(-1)^{F_i(x)+x\cdot a}\right)\right)\right)$$

[4] Rodger E. Ziemer, W. H. Tranter. Principles of Communications: Systems, Modulation, and Noise. Wiley (2002).

[5] Guilley, S. et al. Smart Card Research and Advanced Applications VI (2004). vol 153. Springer, Boston, MA.

SCA Resistance Metric Scores of the Analyzed Ciphers

S-Box	Non-Linearity	SNR	DPA-SNR	TO	RTO
GIFT	4	39.348	2.399	3.466	3.066
PICCOLO	4	39.401	3.108	3.666	3.333
PRESENT	4	34.665	2.129	3.533	3.266
S_1	2	39.968	2.946	3.4	3.266
S_2	0	39.252	2.484	2.933	2.933
S_3	0	34.148	2.484	2.933	2.933

Biryukov, Dinu, and Großschädl (2016)

- AES, Fantomas, LBlock, Piccolo, PRINCE, RC5, Simon, and Speck on an 8-bit AVR processor.
- Non-Linearity (NL), Transparency Order (TO) and Improved Transparency Order (RTO).

Mean Success Rate Comparison of The Analyzed Ciphers

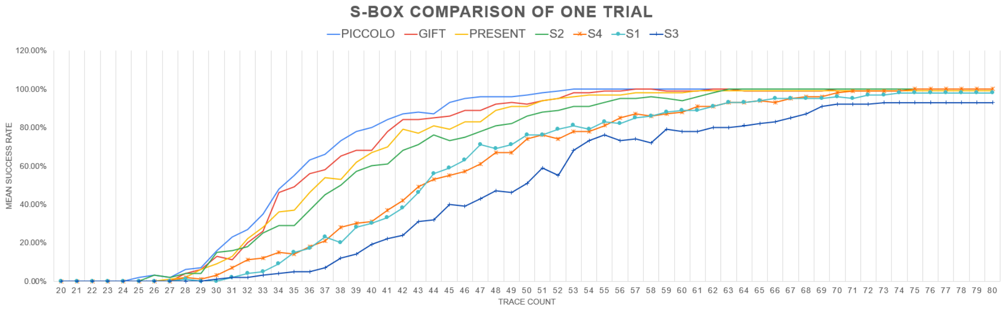


Figure: A Comparison of Mean Success Rate of the S-Boxes

SCA Resistance Metric Scores: Comparison of GIFT, PICCOLO and PRESENT

S-Box	Non-Linearity	SNR	DPA-SNR	TO	RTO
PICCOLO	4	39.401	3.108	3.666	3.333
GIFT	4	39.348	2.399	3.466	3.066
PRESENT	4	34.665	2.129	3.533	3.266

Table: GIFT, PICCOLO and PRESENT: Side Channel Leakage Metric Scores

In the case of equal non-linearity (e.g. NL=4 or NL=0) the values of SNR and DPA-SNR have a similar behavior as the value of NL among the S-boxes with different NL values.

GIFT, PICCOLO and PRESENT: Mean Success Rate Comparison

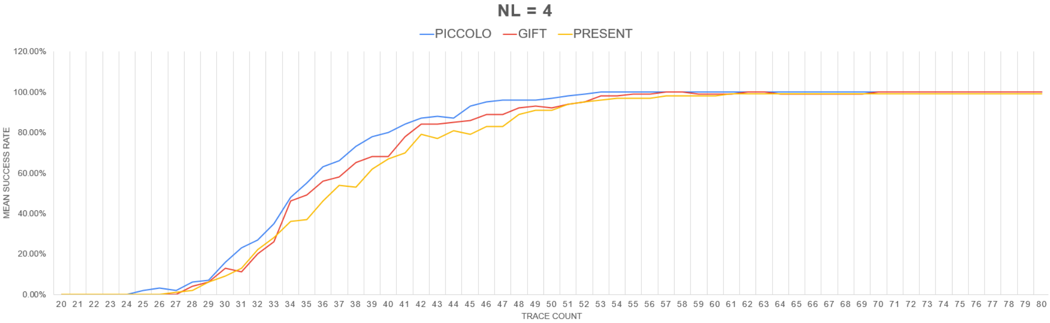


Figure: GIFT, PICCOLO and PRESENT: Mean Success Rate of the S-Boxes

Test Vector Leakage Assessment of LWC and CAESAR Hardware Implementation of GIFT-COFB [7]

TVLA identifies differences between two sets of side channel measurements, such as power and traces, by computing Welch's t-test for the two sets of measurements.

$$t = \frac{\left(\overline{T_A} - \overline{T_B}\right)}{\sqrt{\left(S_A^2/N_A\right) + \left(S_B^2/N_B\right)}},$$

where T_A and T_B are the two trace sets, $\overline{T_A}$, $\overline{T_B}$, S_A, S_B, N_A, and N_B are the means, variances, and size of T_A and T_B, respectively [6].

[6] Flexible Open-source workBench fOr Side-channel analysis (FOBOS)

[7] SAL: NIST Lightweight Cryptography Implementations (https:// github.com/vtsal)

TVLA: Experimental Setup

FOBOS Hardware Setup: Digilent Basys3 control board, Digilent Nexys A7 DUT board and Picoscope 5000 series (5244D) respectively.

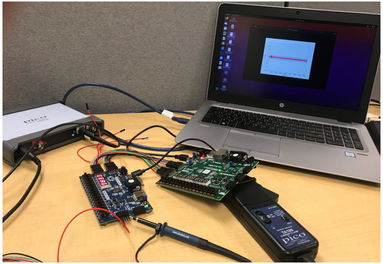


Figure: FOBOS experimental setup

- CAESAR and LWC hardware implementation of GIFT-COFB [8]
- DUT board: jumper on the power line (core FPGA voltage) was added and several capacitors on the voltage rail were removed.
- Generated the input fixed-vs-random test vector by using the same key, nonce and associated data.

[8] SAL: NIST Lightweight Cryptography Implementations (https:// github.com/vtsal)

GIFT-COFB TVLA: Experimental Results

- The DUT clock was set to 10 MHz and the oscilloscope sampling rate was set at 12000 samples/sec.
- A collection of 2000 traces were made using fixed-vs-random test vectors.

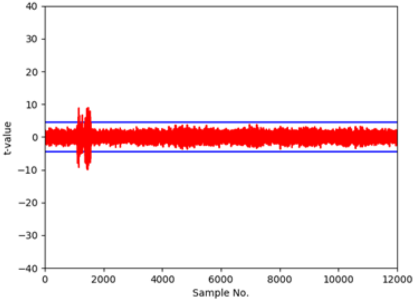


Figure: TVLA results on LWC hardware implementation of GIFT-COFB.

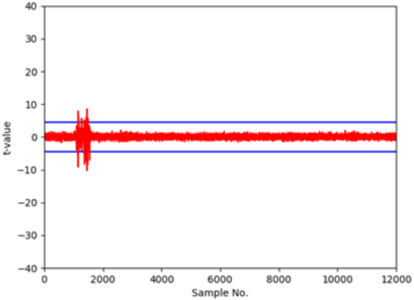


Figure: TVLA results of CAESAR hardware implementation of GIFT-COFB.

Non-Profiled Deep Learning Based CPA on GIFT-64: Preliminary Results

- 2016: Deep Learning Based SCA Techniques (Profiled Attacks) [9]
- 2019: Deep Learning-based Side-Channel Attacks (Non-Profiled Attacks) [10]

Preliminary Results: [11]

CPA, Multi Layer Perceptron Based CPA (CPA-MLP), and onvolutional Neural Networks Based CPA (CPA-CNN) on 10 datasets of 345 power traces of GIFT-64, each with 1250 time samples.

Attack	Accuracy
CPA	100%
CPA-CNN	100%
CPA-MLP	60%

[9] H. Maghrebi, T. Portigliatti, and E. Prouff. Breaking cryptographic implementations using deep learning techniques. In Security, Privacy, and Applied Cryptography Engineering, Vol.10076, 3-26 (2016).

[10] Timon, B. Non-Profiled Deep Learning-based Side-Channel attacks with Sensitivity Analysis. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2019(2), 107–131.

[11] L. Babinkostova, A. Benjamin, J. Herzoff, E. Serra, Deep Learning Based Side Channel Attacks on Lightweight Cryptography, 36th AAAI Conference on Artificial Intelligence, February 22 – March 1, 2022

Non-Profiled Deep Learning Based CPA on GIFT-64: De-synchronization

The traces were de-synchronized through shifting each trace left or right by random values chosen in the interval [-25, 25].

Attack	Accuracy
CPA	0%
CPA-CNN	100%
CPA-MLP	0%

Table: Attacks performed on 10 different de-synchronize datasets, each with a different fixed key and 345 traces

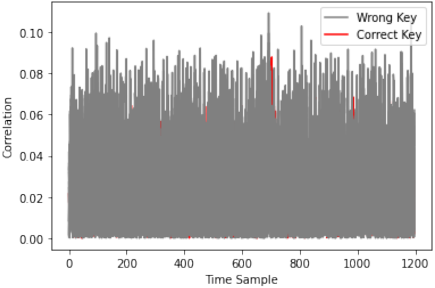


Figure: CPA conducted on de-synchronized traces. The correct key does not produce a singular spike in correlation or the highest correlation

Acknowledgements

- Idaho National Laboratory Directed Research & Development (LDRD) Program under DOE Idaho Operations Office Contract DE-AC07-05ID14517.
- National Science Foundation Under Grant CCF-950599.
- High-performance computing support of the R2 compute cluster (DOI: 10.18122/B2S41H) provided by Boise State University's Research Computing Center.

References I

- Subhadeep Banik, Avik Chakraborti, Tetsu Iwata, Minematsu Minematsu, Mridul Nandi, Thomas Peyrin, Yu Sasaki, Siang Meng Sim, and Yosuke Todo, *Gift-cofb*, Submission to NIST Competition **1** (2021).

- E. Brier, C. Clavier, and F. Olivier, *Correlation power analysis with a leakage model*, International workshop on cryptographic hardware and embedded systems, 2004, pp. 16–29.

- A. Biryukov, D. Dinu, and J. Großschädl, *Correlation power analysis of lightweight block ciphers: From theory to practice*, International Conference on Applied Cryptography and Network Security, Springer, 2016, pp. 537–557.

- A. Bogdanov et al., *Present: An ultra-lightweight block cipher*, International Workshop on Cryptographic Hardware and Embedded Systems (2007), 450–466.

References II

- S. Guilley, P. Hoogvorst, R. Pacalet, and J. Schmidt, *Improving side-channel attacks by exploiting substitution boxes properties*, International Conference on Boolean Functions: Cryptography and Applications (BFCA) (2007), 1–25.

- G. Goodwill, B. Jun, J. Jaffe, and P. A. Rohatgi, *A testing methodology for side-channel resistance validation*, NIST non-invasive attack testing workshop **7** (2011), 115–136.

- P. Kocher, J. Jaffe, and B. Jun, *Differential power analysis*, Annual international cryptology conference, Springer, 1999, pp. 388–397.

- H. Li, Y. Zhou, J. Ming, G. Yang, and C. Jin, *The notion of transparency order, revisited*, The Computer Journal **63** (2020), no. 12, 1915–1938.

References III

- Houssem Maghrebi, Thibault Portigliatti, and Emmanuel Prouff, *Breaking cryptographic implementations using deep learning techniques*, Security, Privacy, andApplied Cryptography Engineering **10076** (2016), 3–26.
- C. O'Flynn and D. Chen, *Chipwhisperer: An open-source platform for hardware embedded security research*, International Workshop on Constructive Side-Channel Analysis and Secure Design, Springer, 2014, pp. 243–260.
- K. Shibutani, T. Isobe, H. Hiwatari, A. Mitsuda, T. Akishita, and T. Shirai, *Piccolo: an ultra-lightweight blockcipher*, International Workshop on Cryptographic Hardware and Embedded Systems, Springer, 2011, pp. 342–357.

References IV

- W. Unger, L. Babinkostova, R. Erbes, and M. Borowczak, *Side-channel leakage assessment metrics: A case study of gift block ciphers*, IEEE Computer Society Annual Symposium on VLSI (ISVLSI), 2021, pp. 236–241.
- Rajesh Velegalati and Jens-Peter Kaps, *Towards a flexible, opensource board for side-channel analysis (fobos)*, Cryptographic architectures embedded in reconfigurable devices, CRYPTARCHI (2013).