Side-Channel Leakage: A Case Study of GIFT-COFB

11 de junio de 2023

Rogelio Calvillo Juárez

Department of Computer Science

1. Introduction
2. GIFT Cipher Family
3. CPA Attack
4. Results
5. Conclusion
6. Future Work

Introduction

- Lightweight crypto seeks to protect devices with limited resources
- Side-channel attacks exploits leakeages such as power consumption from a device to extract secret information
- GIFT-COFB is a finalist in the NIST LWC [Banik et al., 2020]

GIFT Cipher

- Introduced at CHES 2017 with 2 different block sizes and same key lenght: GIFT-64-128 and GIFT-128-128 [Banik et al., 2017]
- GIFT block ciphers are Subtitution-Permution Networks (SPN)

GIFT-64

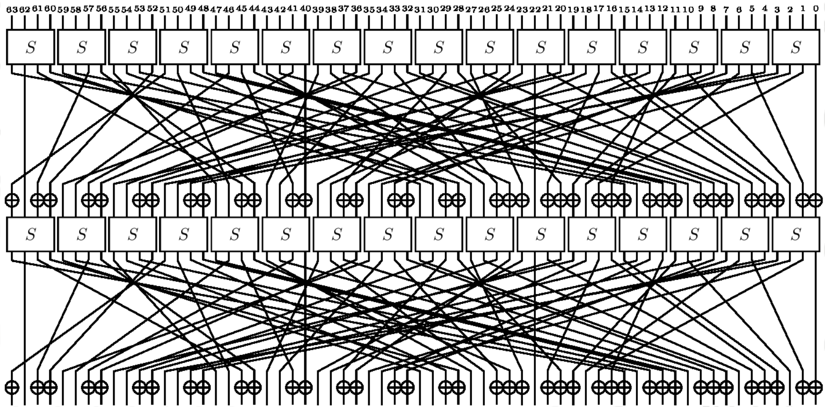


Figure 1: 2 rounds of GIFT-64 (from https://www.iacr.org/authors/tikz/)

Correlation Power Analysis

The methodology of a correlational power analysis (CPA) attack consists of the following:

- Identify the point of interest (PoI)
- Capture power traces
- Calculate intermediate values
- Propose possible hypothetical power consumption
- Compare actual power values with hypothesized values using Pearson's correlation coefficient

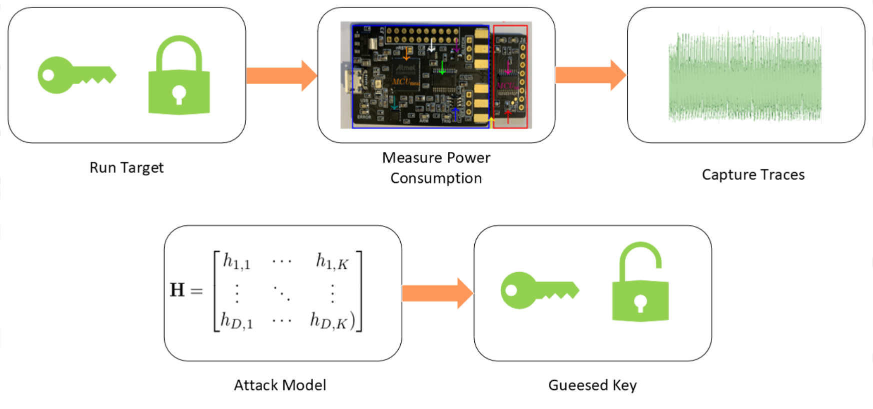
Execution Environment

For the research we used the ChipWhisperer ecosystem to provide the device under the test (target).

The target used was the CW308T-STM32F3. C implementations were used to analyze GIFT-64, GIFT-128 and GIFT-COFB algorithms using 8-bit data types into the “simpleserial” firmware provided with the ChipWhisperer.

All experimental data was collected using this implementation and hardware. The CPA attacks and data analysis was performed using Python.

CPA Attack



Run Target

Measure Power Consumption

Capture Traces

$$\mathbf{H} = \begin{bmatrix} h_{1,1} & \cdots & h_{1,K} \\ \vdots & \ddots & \vdots \\ h_{D,1} & \cdots & h_{D,K}) \end{bmatrix}$$

Attack Model

Gueesed Key

Figure: Methodology

Leakage model

Hamming Height

- The leakeage model connects subkeys and power traces by estimating power usage for each subkeys guess
- Converting a 0 to 1 or 1 to 0 requires different amounts of power so Hamming Weight can estimate power usage by counting 1s in a byte
- The subkey with max correlaction value will be selected as the most probably subkey

CPA attack against GIFT-64

- The 64-bit block is divided into nibbles
- 32 bits of the key are used in each round
- 4 rounds are necessary to obtain the 128 bits of the key
- 2 bits of the key are used for each nibble
- The number of possible subkey combinations is 2^2
- The point of interest is at the exit of box S of round 2, 3, 4 and 5

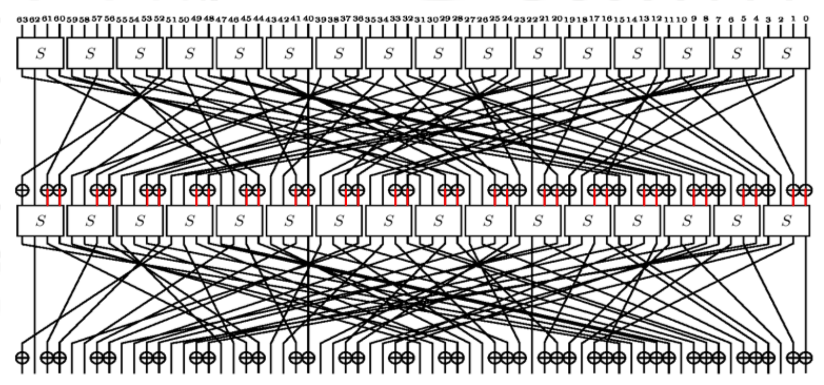


Figure 2: Proposed Subkey Values (from https://www.iacr.org/authors/tikz/)

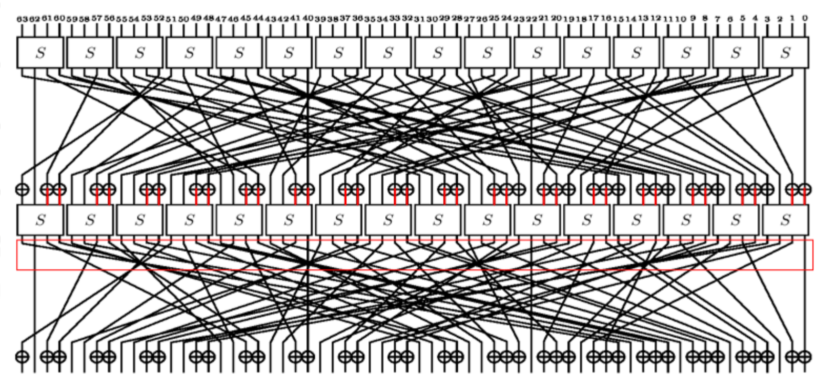


Figure 3: Point of interest (from https://www.iacr.org/authors/tikz/)

CPA attack against GIFT-128

- The 128-bit block is divided into nibbles
- 64 bits of the key are used in each round
- 2 rounds are necessary to obtain the 128 bits of the key
- 2 bits of the key are used for each nibble
- The number of possible subkey combinations is 2^2
- The point of interest is at the exit of box S of round 2 and 3

Rounds

GIFT-128

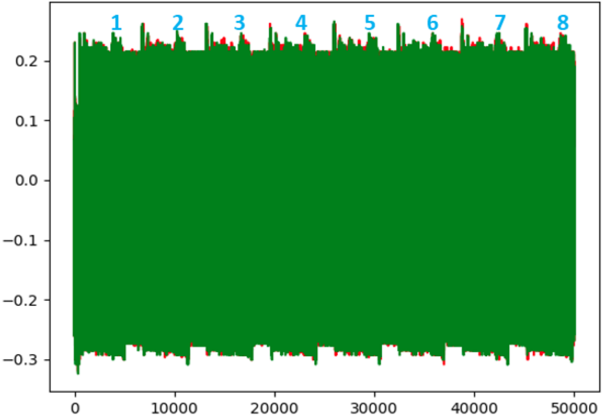


Figure: Power analysis

CPA

Proposed power consumption

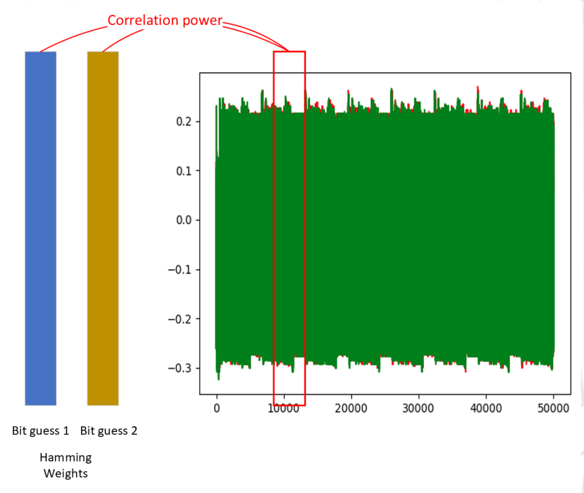


Figure: Bit guees values

CPA Success

The CPA success notes whether an attack successfully recovered the key used by the cryptographic algorithm running on the target.

$$\text{success} = \begin{cases} 1, & \text{if the key is correct} \\ 0, & \text{otherwise} \end{cases}$$

Experiment

An experiment is a CPA attack result which consist of following:

- 1000 Random Plaintexts
- 1 Random key known
- Pair plaintext/voltage of algorithm running on the target (Traces)

Results

Cipher	Experiments	Success	Success Rate	Traces
GIFT-64	120	119	99.1 %	1000
GIFT-128	120	120	100 %	1000

Why it is important?

Since COFB uses GIFT-128 as its block cipher, in an unprotected implementation the key could be obtained by attaching the attack to the cipher input.

Attacking the nonce encryption would reveal the key with exit.

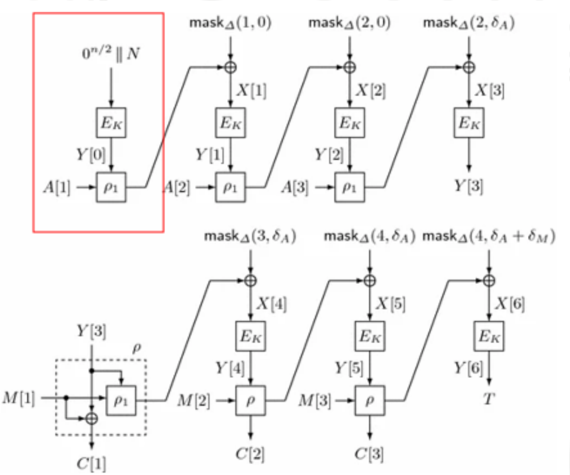


Figure 4: Encryption of COFB for 3-block associated data and plaintext [Chakraborti et al., 2017]

Conclusion

Unprotected GIFT and GIFT-COFB are vulnerable to side channel attacks against CPAs. Taking the output of the Sbox box as a point of interest, the extracted information can be used to successfully recover the key with the help of a CPA.

Future Work

Further masked data should show strength against CPA attack. The masking countermeasure adds randomness by splitting up processes into shares. Share number relates directly to the degree of security but has a computational cost. We have implemented masking on GIFT-COFB but have not conducted attacks on it.
Additional experiments are necessary to observe the relation to number of traces and correlation for key guessed.

References

Banik, S., Chakraborti, A., Inoue, A., Iwata, T., Minematsu, K., Nandi, M., Peyrin, T., Sasaki, Y., Sim, S. M., and Todo, Y. (2020).
Gift-cofb.
Cryptology ePrint Archive, Paper 2020/738.

Banik, S., Pandey, S. K., Peyrin, T., Sasaki, Y., Sim, S. M., and Todo, Y. (2017).
Gift: A small present.
In Fischer, W. and Homma, N., editors, *Cryptographic Hardware and Embedded Systems – CHES 2017*, pages 321–345.

Chakraborti, A., Iwata, T., Minematsu, K., and Nandi, M. (2017).
Blockcipher-based authenticated encryption: How small can we go?
In Fischer, W. and Homma, N., editors, *Cryptographic Hardware and Embedded Systems – CHES 2017*, pages 277–298.

Thank you