INL/EXP-19-54970-Revision-0

A Little Something on the Side: Exploration of Power Side-channels in Embedded Cryptography

Riley Myers, Robert J Erbes

August 2019

The INL is a U.S. Department of Energy National Laboratory
operated by Battelle Energy Alliance

INL/EXP-19-54970-Revision-0

A Little Something on the Side: Exploration of Power Side-channels in Embedded Cryptography

Riley Myers, Robert J Erbes

August 2019

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy

Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

www.inl.gov

Idaho National Laboratory

A Little Something on the Side: Exploration of Power Side-channels in Embedded Cryptography

Riley Myers [1 2] Robert Erbes [2]

[1]New Mexico Institute of Mining and Technology [2]Idaho National Laboratory

Abstract

Given the ubiquity of embedded devices in modern society, strong cryptographic solutions are a necessity to ensure privacy and security. In addition to the challenges that traditional cryptography faces, embedded cryptography is more vulnerable to side-channel attacks due to its location in the hands of the (un)trusted user. We propose that adjusting the mathematical properties of the cryptosystems can affect the information leakage through these side-channels. Our experimental results confirm that the information leakage from power side-channels is heavily affected by both the mathematical structure as well as discrete implementation choices.

Introduction

As technology improves, there is an increasing amount of computing surrounding us in our daily lives. From watches and mirrors to car chargers, a startling array of products sport embedded processors to make our lives more convenient and connected. Strong cryptographic implementations are needed to protect these devices and ensure the privacy of the data that they collect. However, these devices often are resource-constrained, with limited ability to run complex cryptographic algorithms. Additionally, due to the widespread deployment of these devices, they are particularly vulnerable to hardware attacks attempting to extract encryption keys.

GIFT

Currently there is an effort to standardize lightweight cryptographic algorithms spearheaded by the National Institute of Standards and Technology (NIST) [2]. One of the submissions is a block cypher named GIFT, which is an evolution of an older algorithm named PRESENT. GIFT is designed to have small hardware implementations, as well as have quick software implementations, and supports two block sizes, 64- and 128-bit, with a 128-bit key size.

The substitution-permutation network construction of GIFT can be broken down into three distinct parts, which are repeated for some number of rounds (at least 40 rounds for GIFT-128 and 28 rounds for GIFT-64). The cypher first performs a substitution transform (GS) on 4-bit blocks of the input, shuffles (or permutes) the entire output, and then combines the resulting bitstream with the corresponding round key (RK^i), as shown in Figure 1.

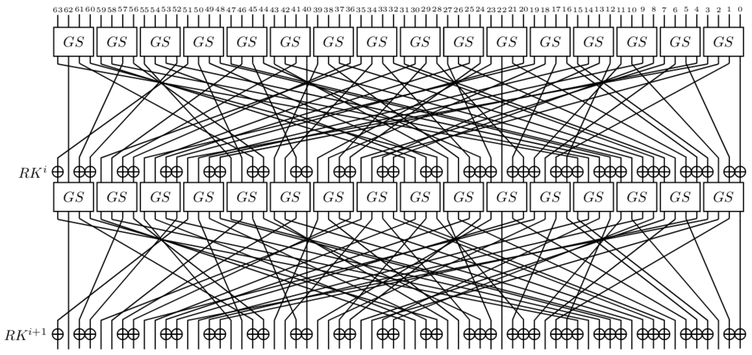


Figure 1. 2 rounds of GIFT-64 [1]

Power Analysis

While not directly related to the algorithmic design of cryptographic systems, side-channel attacks are an important consideration in choosing and evaluating cryptographic algorithms [2]. One of the vectors for performing a side-channel attack on a cryptographic implementation is to analyze the power consumed by a device while it is performing cryptographic operations. Statistical analysis of spikes in the power drawn by the device can then be used, through differential or correlation power analysis, to recover encryption keys or other secrets used by the device.

Leakage Assesment

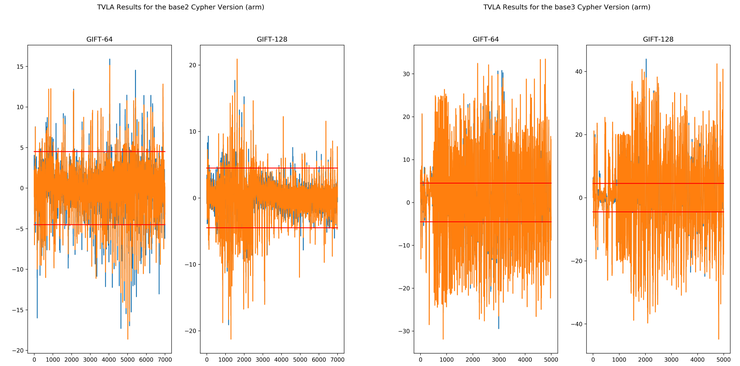
Performing full differential or correlation attacks on a device can be very time consuming. As a first-order estimation of whether a device is vulnerable to power analysis, a leakage analysis ([3]) can be performed on the device. First, a large number (n) of traces of the power consumption of the device during cryptographic operations are collected. Then, the traces are broken into two groups and Welch's t-test (1) is computed across the two groups for each point in the trace.

$$t = \frac{\bar{X}_1 - \bar{X}_2}{\sqrt{\frac{s_1^2}{N_1} + \frac{s_2^2}{N_2}}} \tag{1}$$

This resulting t-statistic is the ratio of the difference between the mean values of the two measured groups to the standard error of the measurement. For the leakage analysis, a high statistical difference indicates that there is *some form* of information leakage. This test can not determine what information is being leaked or how easy it would be to retrieve information like encryption keys. A device is considered to have 'passed' the analysis if $t \in [-4.5, 4.5]$. This provides a 99.99% confidence interval for $n \in [100, 5000]$

Results

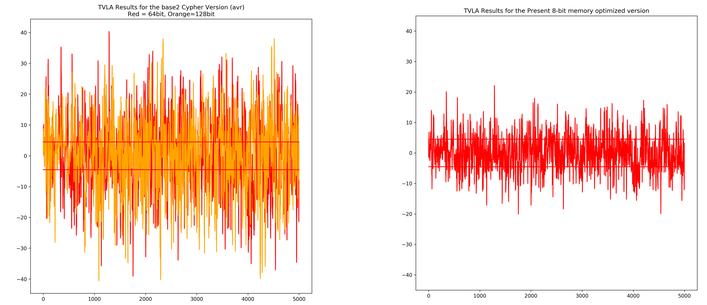
From examining the results of the leakage assessment for both of the GIFT families (Figure 2), we can see an impact from the change of the cryptosystem construction. The new construction has a both different leakage, as well as a larger amount of leakage overall.



(a) Leakage assessment for the base2 cypher (b) Leakage assessment for the base3 cypher

Figure 2. Comparison of leakage results between base-2 and base-3 implementations on the STM32

Additionally, preliminary results suggest that the cryptosystem performs approximately twice as well on the leakage analysis when the implementation is optimized to use the platform's native datatype size rather than utilizing a single size (64-bits) for both, as shown in Figure 3.



(a) Leakage test for the original base2 cypher (b) Leakage test for the 8-bit cypher

Figure 3. Comparison of leakage results between non-native and native bit-size code on the XMEGA

Experimental Setup

Four versions of GIFT were tested: GIFT-64, GIFT-128, and analogous versions of GIFT ported to work with base-3 numbers, rather than base-2 (binary) numbers. All of the algorithms were written in C99, using 64-bit datatypes and lookup tables to perform both the substitutions and permutations of GIFT.

The algorithms were tested across two targets: an Microchip (formerly ATMEL) XMEGA128D4 and a ST Microelectronics STM32F303. These were located on a host board that provided easy access to the signals shown in Figure 4. The XMEGA provides an 8-bit RISC architecture to test on, while the STM32 is a 32-bit ARM Cortex-M4. Data collection, communication with the device under test, and programming of the device were handled through the Chipwhisperer CW1200 platform [4].

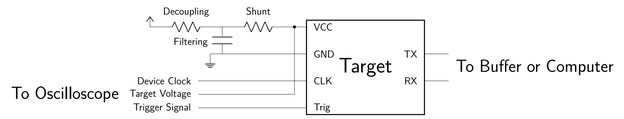


Figure 4. Experimental Setup

Conclusion

- The mathematical design of cryptographic routines has a large impact on their power consumption when implemented in embedded processors
- Utilizing native datatype sizes reduces amount of leakage

Future Work

- Complete porting the GIFT cryptosystem to 8- and 32-bit native code
- Explore further modifications to the base-3 cryptosystem
- Attempt key extraction attacks on the varying configurations of the GIFT cryptosystem
- Explore the effect of other mathematical changes to the GIFT algorithm

Acknowledgments

This research was performed in collaboration with Liljana Babinkostova and William Unger at Boise State University.

References

[1] Subhadeep Banik, Sumit Kumar Pandey, Thomas Peyrin, Siang Meng Sim, Yosuke Todo, and Yu Sasaki.
Gift: A small present.
IACR Transactions on Cryptographic Hardware and Embedded Systems, 2017.

[2] Lawrence Bassham, Çağdaş Çalık, Kerry McKay, and Meltem Sönmez Turan.
Submission requirements and evaluation criteria for the lightweight cryptography standardization process.
Technical report, US National Institute of Standards and Technology, August 2018.

[3] Gilbert Goodwill, Benjamin Jun, Josh Jaffe, and Pankaj Rohatgi.
A testing methodology for side--channel resistance validation.
Technical report, Cryptography Research Inc,
`http://csrc.nist.gov/news_events/non-invasive-attack-testing-workshop/papers/08_Goodwill.pdf`, 2011.

[4] Colin O'Flynn and Zhizhang (David) Chen.
Chipwhisperer: An open-source platform for hardware embedded security research.
In Emmanuel Prouff, editor, *Constructive Side-Channel Analysis and Secure Design*, pages 243–260. Springer International Publishing, Mar 2014.

INL/EXP-19-54970