Investigating On-chip Sensor based RPA Attack Vulnerabilities of Lightweight Cipher Algorithms

Final Year Project

Group 18

Group Members

E/17/027	Pubudu Bandara
E/17/176	Esara Sithumal
E/17/219	Ishara Nawarathna

Supervisors

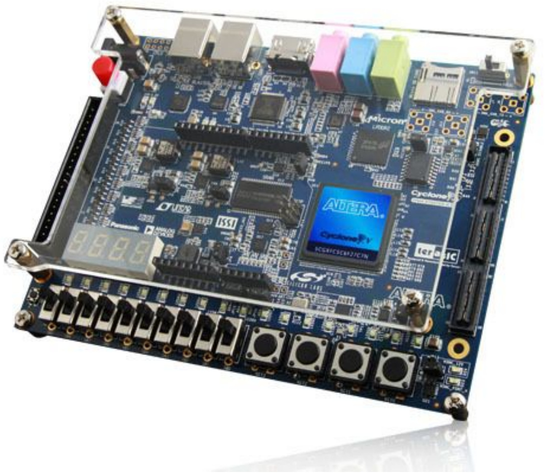
Dr. Damayanthi Herath	UOP
Dr. Mahanama Wickramasinghe	UOP
Dr. Darshana Jayasinghe	UNSW

In our research...

- Lightweight Ciphers : Ciphers designed to run on Resource Constrained devices

  Lightweight Ciphers → Used in **FPGA, IoT, Microcontrollers ...**
  FPGA → Used in **Airbus, Electric Vehicles ...**

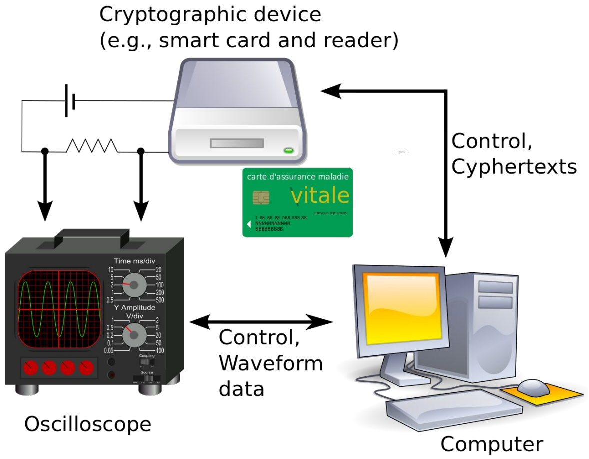
- Not tested against **Remote Power Analysis** attacks before.
- Most work has been carried out on Xilinx FPGA.
- On our project ⇒ Testing the vulnerabilities of **Lightweight Ciphers** on **Intel Altera FPGAs**.



Recap

- Modern cipher algorithms
  - ➔ Highly **Mathematically Complex**
  - ➔ Nearly impossible to break
- Alternative method : **Side Channel Attacks (SCA)**
- Side Channel Attack uses:
  - Power Consumption
  - Timing Information
  - Electromagnetic Analysis

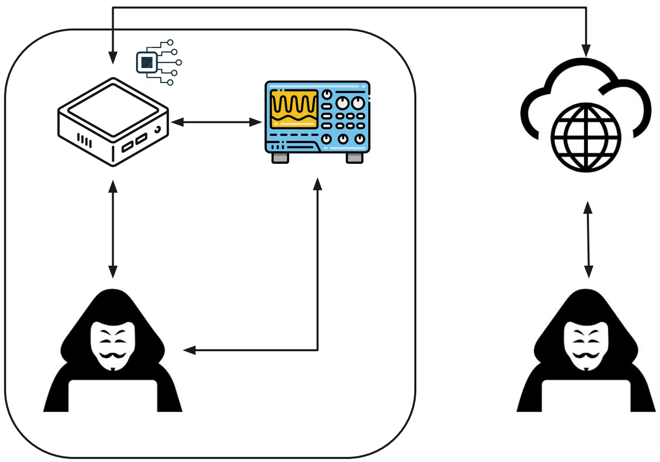
to extract secret keys from cryptographic systems



How a Side-Channel Attack is Performed

Recap (continued...)

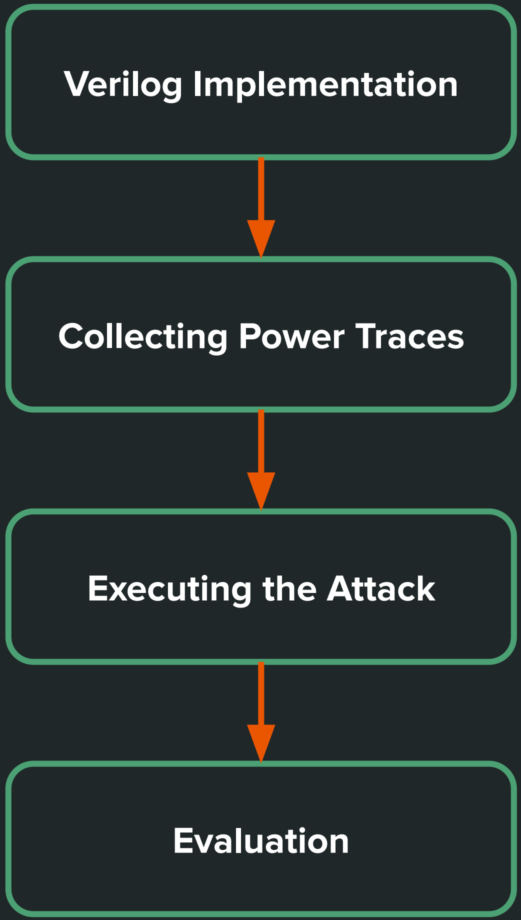
- Power Analysis : Using power as the side channel.
- CPA[2] : **Correlation Power Analysis** is the main method of Power Analysis
- Advisory needs to be present in the premise
- Alternative method
  - RPA[3] : **Remote Power Analysis**
- Planting an on chip sensor(hardware design) on victims system.



RPA : Remote Power Analysis

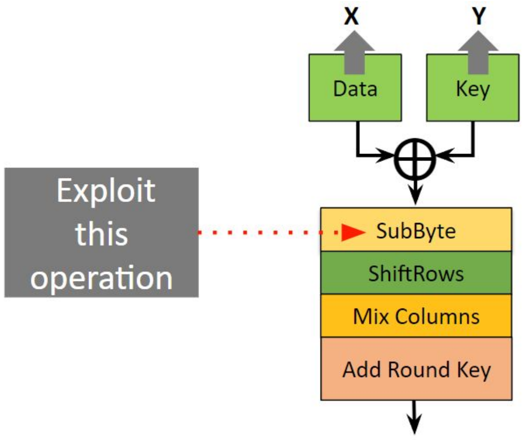
CPA : Correlation Power Analysis

Methodology



Investigating AES Cipher

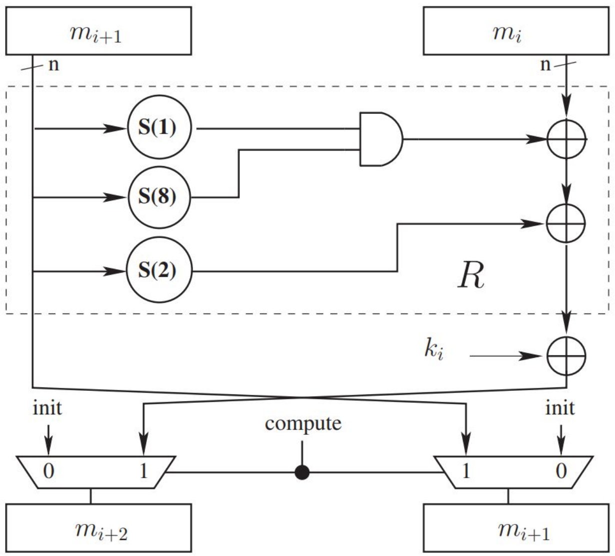
1. Hardware implementation of AES.
2. Collected traces for a specific key.
3. Target **S-box** operation of AES.
4. Consider **one byte** of key at a time.
    - Guess possible keys.
    - Model hypothetical power using **Hamming Distance**[2] model.
    - **Hamming Distance (HD)**: 1001 0001 → 1110 0001 : 3 (# of bit flips)
5. Calculate the correlation coefficient between hypothetical power and actual power consumption.
6. Sort key guesses according to correlation coefficient.



S-box Operation of AES

SIMON algorithm

- SIMON 32/64
- Has a Feistel structure.
- 64 bit key
  - 4 * 16 bit key blocks
- 32 rounds
  - First 4 round uses 4 key blocks in encryption



Round Operation of SIMON

Output of the jth bit of the ith round:

$$L_j^{i+1} = K_j^i \oplus R_j^i \oplus L_{(j+2) \bmod n}^i \oplus (L_{(j+1) \bmod n}^i \,\&\, L_{(j+8) \bmod n}^i)$$

Investigating SIMON Cipher

1. Hardware implementation of Simon(Verilog).
2. Collected traces for a specific key.
3. Target **second round** of the SIMON algorithm
4. Consider **five key bits** at a time
    - Guess possible keys.
    - Model hypothetical power using **Hamming Distance** model.
5. Calculate the correlation coefficient between hypothetical power and actual power consumption.
6. Sort key guesses according to correlation coefficient.

$$\underbrace{(K_1^1 \oplus R_1^1 \oplus L_{15}^1 \oplus (L_{16}^1 \& L_9^1))}_{L_1^2}$$

An Input bit of 2nd Round Operation

$$\underbrace{(K_1^2 \oplus R_1^2 \oplus L_{15}^2 \oplus (L_{16}^2 \& L_9^2))}_{L_1^3}$$

An output bit of 2nd Round Operation

$$HD = HW(L_j^{i+1} \oplus L_j^i)$$

Hamming Distance Model

Evaluation of the Attacks

Success Rate[14] can be used,

→ Execute attack n times using same data

→ Count successful guesses

$$Success\ Rate = \frac{Number\ of\ Successful\ Attacks}{Total\ Number\ of\ Attacks} \times 100\%$$

Experiments and Results

RPA attack results on AES

- Performed the RPA attack on AES with 128 bit key.
  - Used Intel Cyclone X FPGA to get traces.
- Used CUDA parallel processing to reduce the runtime
- Evaluated outcomes using the success rate.
- Good baseline for attacking lightweight ciphers

Experimental Setup

RPA attack results on SIMON

```
 |0|
 00
0.0273

 01
0.0273

 02
0.0273

 03
0.0273

 08
0.0273

 09
0.0273

 0a
0.0273

 0b
0.0273

 04
0.0142

 05
0.0142
```

Correlation values are same

00	0 0 0 0 0
01	0 0 0 0 1
02	0 0 0 1 0
03	0 0 0 1 1
08	0 1 0 0 0
09	0 1 0 0 1
0A	0 1 0 1 0
0B	0 1 0 1 1

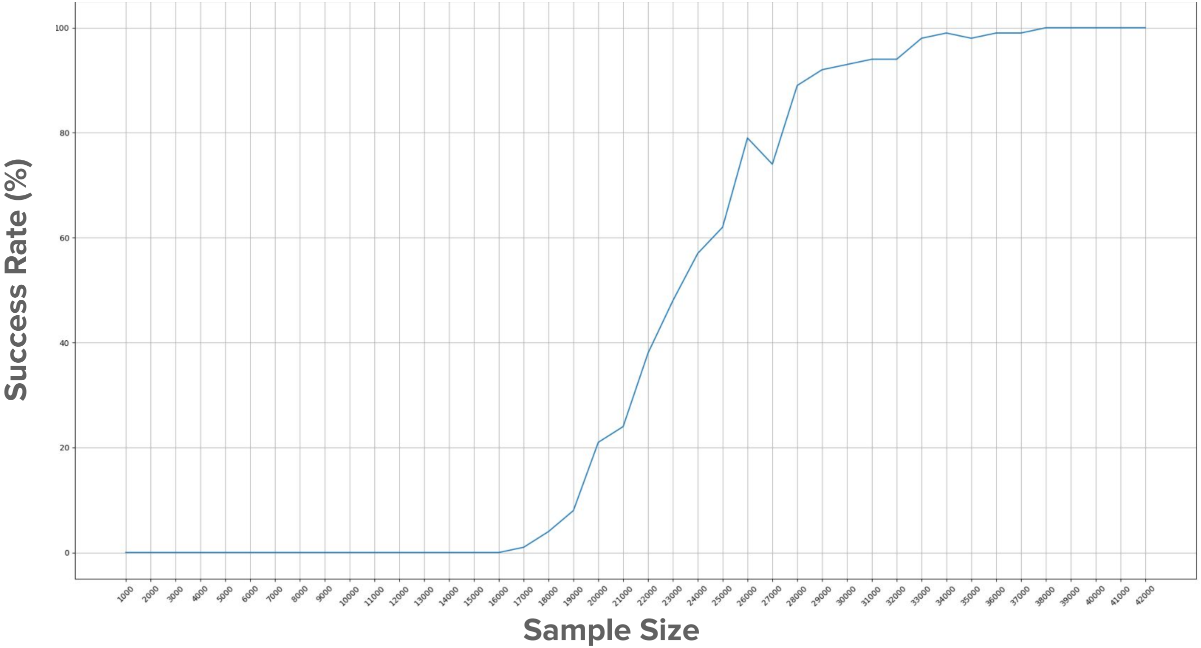
Guessed Bits	1,16	1,15	1,9	1,1	2,1
Expected values	0	1	0	1	1

$$\underbrace{(K_1^2 \oplus R_1^2 \oplus L_{15}^2 \oplus (L_{16}^2 \& L_9^2))}_{L_1^3}$$

AND operation of SIMON cipher is vulnerable to RPA attack

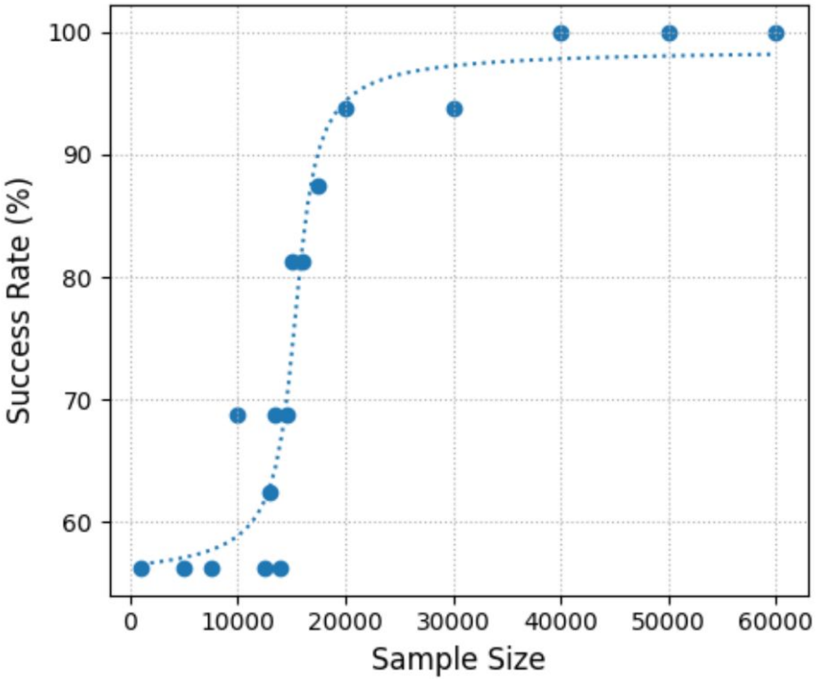
Evaluate success rates for RPA on AES

- Success rate vs sample size.
- Sample size > 38,000 ⇒ Success rate = 100%.
- AES is 100% vulnerable on Intel FPGA.



Evaluate success rates for RPA on SIMON

- Success rate vs Sample size.
- Sample size > 40,000 ⇒ Success rate = 100%.
- SIMON is 100% vulnerable on Intel FPGA.



Comparison of attacks on AES and SIMON

	AES	SIMON
	128-bit key	64-bit key
	Number of attacking rounds	
Target	One byte at a time	Five bits at a time
Number of key guesses in one execution	$2^8 = 256$	$2^5 = 32$
Total number of executions to generate key	256*16 * NOS = 4096 * NOS	32 * 9 * 4 * NOS = 1152 * NOS

Conclusions

- **AES** and **SIMON** are vulnerable to **RPA** attacks on **Intel FPGAs**
- **AND** operation of **SIMON** is vulnerable to **RPA** attacks
- When determining remaining keyblocks in **SIMON**, the error of the previous guesses accumulates

Demonstration

Obtaining Power Traces

RPA Attack on AES

RPA Attack on Simon

Problems and Challenges

- **Finding vulnerable points of SIMON to be attacked**
  - **Two approaches** were considered
- **Low Power Consumption in SIMON**
  - Increase the **number of SIMON units**
  - After attacking successfully, reduce the number of units
- **Having same Correlation values for different guesses**
  - Only AND operation is have significant impact on the power traces
- **Inaccurate power traces for SIMON**
  - Changed the values of the TDC delay elements, to identify the vulnerable key bits

Project Outcomes

- The first experiment of **RPA** attacks on **Intel FPGA**s
- The first RPA attack research on **Lightweight Ciphers**
- Manuscript is in progress
- Peradeniya University Research Excellence Showcase 2023

Acknowledgement

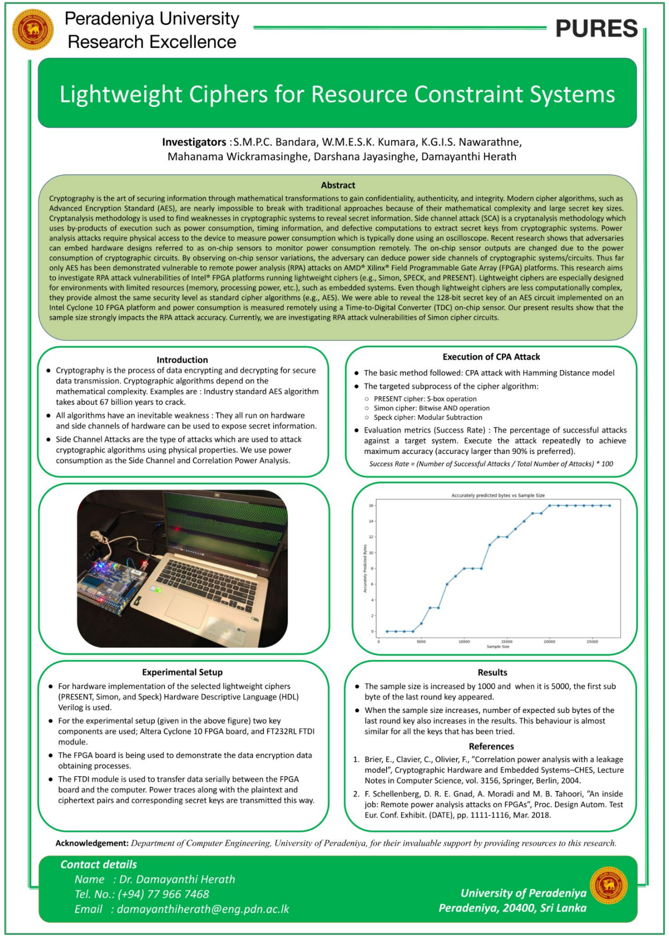
For providing Resources

Department of Computer Engineering

For your Guidance and Support

Dr. Darshana Jayasinghe	*UNSW*
Dr. Damayanthi Herath	*UOP*
Dr. Mahanama Wickramasinghe	*UOP*

PURES 2023



Peradeniya University Research Excellence

PURES

Lightweight Ciphers for Resource Constraint Systems

Investigators :S.M.P.C. Bandara, W.M.E.S.K. Kumara, K.G.I.S. Nawarathne, Mahanama Wickramasinghe, Darshana Jayasinghe, Damayanthi Herath

Abstract

Cryptography is the art of securing information through mathematical transformations to gain confidentiality, authenticity, and integrity. Modern cipher algorithms, such as Advanced Encryption Standard (AES), are nearly impossible to break with traditional approaches because of their mathematical complexity and large secret key sizes. Cryptanalysis methodology is used to find weaknesses in cryptographic systems to reveal secret information. Side channel attack (SCA) is a cryptanalysis methodology which uses by-products of execution such as power consumption, timing information, and defective computations to extract secret keys from cryptographic systems. Power analysis attacks require physical access to the device to measure power consumption which is typically done using an oscilloscope. Recent research shows that adversaries can embed hardware designs referred to as on-chip sensors to monitor power consumption remotely. The on-chip sensor outputs are changed due to the power consumption of cryptographic circuits. By observing on-chip sensor variations, the adversary can deduce power side channels of cryptographic systems/circuits. Thus far only AES has been demonstrated vulnerable to remote power analysis (RPA) attacks on AMD® Xilinx® Field Programmable Gate Array (FPGA) platforms. This research aims to investigate RPA attack vulnerabilities of Intel® FPGA platforms running lightweight ciphers (e.g., Simon, SPECK, and PRESENT). Lightweight ciphers are especially designed for environments with limited resources (memory, processing power, etc.), such as embedded systems. Even though lightweight ciphers are less computationally complex, they provide almost the same security level as standard cipher algorithms (e.g., AES). We were able to reveal the 128-bit secret key of an AES circuit implemented on an Intel Cyclone 10 FPGA platform and power consumption is measured remotely using a Time-to-Digital Converter (TDC) on-chip sensor. Our present results show that the sample size strongly impacts the RPA attack accuracy. Currently, we are investigating RPA attack vulnerabilities of Simon cipher circuits.

Introduction

- Cryptography is the process of data encrypting and decrypting for secure data transmission. Cryptographic algorithms depend on the mathematical complexity. Examples are : Industry standard AES algorithm takes about 67 billion years to crack.
- All algorithms have an inevitable weakness : They all run on hardware and side channels of hardware can be used to expose secret information.
- Side Channel Attacks are the type of attacks which are used to attack cryptographic algorithms using physical properties. We use power consumption as the Side Channel and Correlation Power Analysis.

Execution of CPA Attack

- The basic method followed: CPA attack with Hamming Distance model
- The targeted subprocess of the cipher algorithm:
  - PRESENT cipher: S-box operation
  - Simon cipher: Bitwise AND operation
  - Speck cipher: Modular Subtraction
- Evaluation metrics (Success Rate) : The percentage of successful attacks against a target system. Execute the attack repeatedly to achieve maximum accuracy (accuracy larger than 90% is preferred).

*Success Rate = (Number of Successful Attacks / Total Number of Attacks) * 100*

Accurately predicted bytes vs Sample Size

Experimental Setup

- For hardware implementation of the selected lightweight ciphers (PRESENT, Simon, and Speck) Hardware Descriptive Language (HDL) Verilog is used.
- For the experimental setup (given in the above figure) two key components are used; Altera Cyclone 10 FPGA board, and FT232RL FTDI module.
- The FPGA board is being used to demonstrate the data encryption data obtaining processes.
- The FTDI module is used to transfer data serially between the FPGA board and the computer. Power traces along with the plaintext and ciphertext pairs and corresponding secret keys are transmitted this way.

Results

- The sample size is increased by 1000 and when it is 5000, the first sub byte of the last round key appeared.
- When the sample size increases, number of expected sub bytes of the last round key also increases in the results. This behaviour is almost similar for all the keys that has been tried.

References

1. Brier, E., Clavier, C., Olivier, F., ”Correlation power analysis with a leakage model”, Cryptographic Hardware and Embedded Systems–CHES, Lecture Notes in Computer Science, vol. 3156, Springer, Berlin, 2004.
2. F. Schellenberg, D. R. E. Gnad, A. Moradi and M. B. Tahoori, ”An inside job: Remote power analysis attacks on FPGAs”, Proc. Design Autom. Test Eur. Conf. Exhibit. (DATE), pp. 1111-1116, Mar. 2018.

Acknowledgement: *Department of Computer Engineering, University of Peradeniya, for their invaluable support by providing resources to this research.*

Contact details

Name : Dr. Damayanthi Herath

Tel. No.: (+94) 77 966 7468

Email : damayanthiherath@eng.pdn.ac.lk

University of Peradeniya

Peradeniya, 20400, Sri Lanka

References

1. Daemen, Joan, and Vincent Rijmen, “AES proposal: Rijndael”, 1999.
2. Brier, E., Clavier, C., Olivier, F., ”Correlation power analysis with a leakage model”, Cryptographic Hardware and Embedded Systems–CHES, Lecture Notes in Computer Science, vol. 3156, Springer, Berlin, 2004.
3. F. Schellenberg, D. R. E. Gnad, A. Moradi and M. B. Tahoori, “An inside job: Remote power analysis attacks on FPGAs”, Proc. Design Autom. Test Eur. Conf. Exhibit. (DATE), pp. 1111-1116, Mar. 2018.
4. A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. Robshaw, et al., ”PRESENT: An Ultra-lightweight Block Cipher” in Cryptographic Hardware and Embedded Systems, Berling, Germany:Springer, 2007.
5. Beaulieu R, Shors D, Smith J, Treatman-Clark S, Weeks B, Wingers L., “The SIMON and SPECK families of lightweight block ciphers”, cryptology eprint archive, 2013.
6. P. Kocher, J. Jaffe, B. Jun and P. Rohatgi, “Introduction to differential power analysis”, J. Cryptograph. Eng., vol. 1, no. 1, 2011.

7. Kenneth M. Zick, Meeta Srivastav, Wei Zhang, Matthew French, ”Sensing nanosecond-scale voltage attacks and natural transients in FPGAs”, Proceedings of the ACM/SIGDA international symposium on Field programmable gate arrays, 2013.
8. Kenneth M. Zick, John P. Hayes, ”Low-cost sensing with ring oscillator arrays for healthier reconfigurable systems”, ACM Transactions on Reconfigurable Technology and Systems, 5(1):1–26, 2012.
9. Udugama, Brian, Darshana Jayasinghe, Hassaan Saadat, Aleksandar Ignjatovic, and Sri Parameswaran, "VITI: A tiny self-calibrating sensor for power-variation measurement in FPGAs." IACR Transactions on Cryptographic Hardware and Embedded Systems, 2022.
10. Udugama B, Jayasinghe D, Saadat H, Ignjatovic A, Parameswaran S, “A power to pulse width modulation sensor for remote power analysis attacks”, IACR Transactions on Cryptographic Hardware and Embedded Systems, 2022.
11. Lo, Owen, William J. Buchanan, and Douglas Carson. "Power analysis attacks on the AES-128 S-box using differential power analysis (DPA) and correlation power analysis (CPA)." Journal of Cyber Security Technology 1.2, 2017.

12. Lo, Owen, William J. Buchanan, and Douglas Carson, “Correlation power analysis on the PRESENT block cipher on an embedded device” Proceedings of the 13th International Conference on Availability, Reliability and Security, 2018.

13. Biryukov, A., Dinu, D., Großschadl, J., “Correlation power analysis of lightweight block ciphers: from theory to practice”, ACNS 2016. LNCS, vol. 9696, Springer, Heidelberg, 2016.

14. Standaert, François-Xavier, Tal G. Malkin, and Moti Yung. “A unified framework for the analysis of side-channel key recovery attacks.”, Advances in Cryptology-EUROCRYPT 2009: 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, 2009.