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

Background

Cryptography → **Encrypting** and **Decrypting**

Used in **Smart Card**, **Wi-Fi**, ...

Widely used algorithm : Advanced Encryption Standard (AES)[1]

To perform a **Brute-force Attack** on **AES -128**:

- **10** computers
- **8 billion** people
- **1 billion** combinations / second
- **50%** possibilities

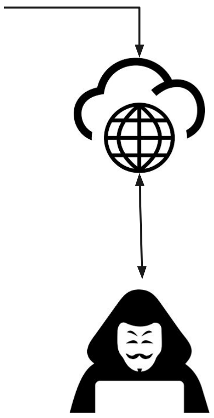
67,000,000,000 years

Introduction

Side-Channel Attack (SCA) is a type of attack that exploits information that is leaked from a Cryptographic Systems.

Data leaking channels:

- **Power Consumption (CPA[2], RPA[3])**
- Timing Information
- Electromagnetic Leaks



nalysis

Smart Devices → IoT devices → Lightweight Ciphers

Introduction (continued...)

Resource constraints and High reachability of IoT

→ Challenge when minimizing **Side-Channel Attacks**

→ IoT devices have become easy targets

Problem Statement

No concrete studies have been conducted before, about the vulnerabilities of lightweight ciphers against RPA attacks.

Purpose of the Research

To check whether the selected Lightweight Ciphers are vulnerable, and if so how does the leakage compare to AES

Expected Outcomes

Find out vulnerabilities of Lightweight Ciphers; **PRESENT**[4], **Simon**[5], **Speck**[5], on Remote Power Analysis (RPA) Attacks

Compare the data leakage of those Lightweight Ciphers against AES

Impact

To introduce **Countermeasures** or to **improve the algorithms** of these ciphers, which are running on IoT / Smart devices to be secure against RPA attacks.

Summary of Literature

Power Analysis Attacks

Revealing secret information using power dissipation.

CMOS gates → building blocks of ICs. Power dissipation →CMOS gate inputs

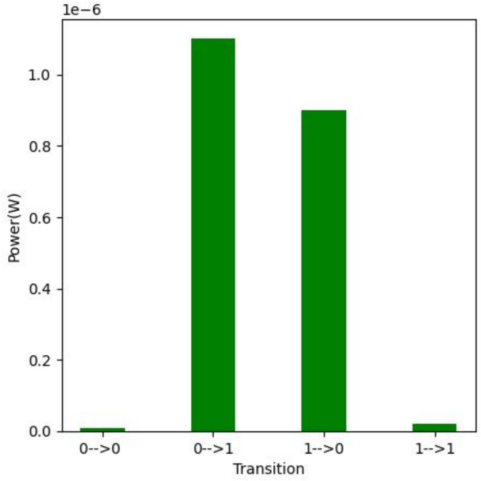
Hamming Distance (HD)[2]: 1001 0001 → 1110 0001 : 3 (# of bit flips)

Assumption : Hamming distance correlates to power dissipation.

Hamming Weight (HW)[6]: 1001 0101 : 4 (# of ones)

HW : Special case of hamming distance(initial state all ‘0’s → Hamming Distance = Hamming Weight).

HW,HD : **Hypothetical power**



Correlation Power Analysis (CPA)[2] Attacks

Needs : Cryptographic device, Oscilloscope, PC

Consider one sub byte of the plain-text of AES & guessed key as 0x00.

$$r = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \bar{x})^2 \sum_{i=1}^{n}(y_i - \bar{y})^2}}$$

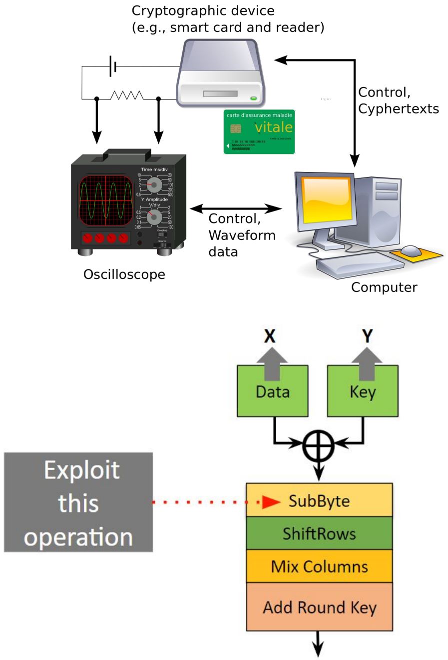
Pearson Correlation Coefficient

Plaint (P)					ning t	Actual Power Consumption (µW)
3F						50
6E	00	6E	9F	10011111	6	34
07	00	07	C5	11000101	4	32
…	…	…	…	…	…	…
B3	00	B3	6D	01101101	5	25

X Y

Find the pearson correlation for all 256 keys.

Choose the key with the maximum correlation coefficient(most correlated with the power and the hypothetical power).



Remote Power Analysis (RPA)[3] Attacks

RPA, Oscilloscope → On chip sensor

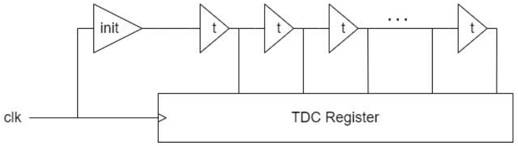
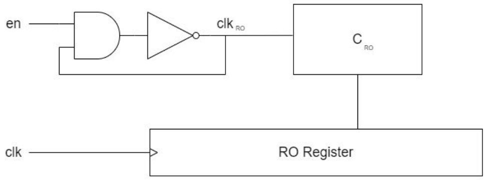
On chip Sensors : Physical parameter → An electrical signal

Can be used in devices like FPGAs (Field Programmable Gate Arrays) to measure the power consumption.

Example for on chip sensors :

1. TDC (Time to Digital Converter) Sensor[7]
2. RO (Ring Oscillator) Sensor[8]
3. VITI (Voltage Induced Time Interval) Sensor[9]
4. PPWM (Power to Pulse Width Modulation) Sensor[10]

TDC Sensor And RO Sensor

Sensor Types	TDC sensor[7]	RO sensor[8]
Schematic Diagram		
Functionality	Timing variances caused by power supply fluctuations → digital data	By measuring oscillation frequency of its Ring Oscillator (RO)
Sensitivity	Higher	Lower
Range	Smaller	Larger
Transient voltage drops	Better at detecting	Worse at detecting

Previous work

Previous experiments done against some Lightweight Ciphers

Cipher	Used Platform	Used Method
AES	Arduino Uno, Xilinx Spartan-6	CPA[11], DPA[11], RPA[3]
PRESENT	Arduino Uno	CPA : Hamming Weight model[12]
Simon	8-bit AVR processor	CPA[13]
Speck	8-bit AVR processor	CPA[13]

Proposed Methodology

Methodology

Hardware implementation of PRESENT, Simon and Speck : **Verilog**

Run on: **Altera DE2 Cyclone IV**

→ Known plaintexts

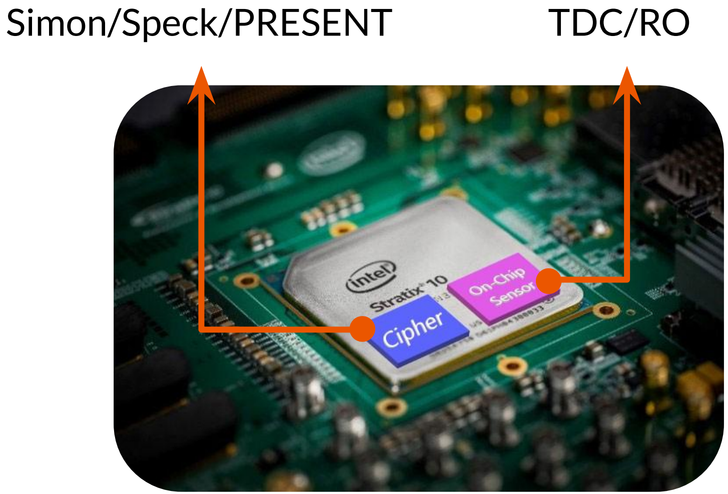
→ Same Key

An On-chip sensor developed inside FPGA: **TDC, RO**

→ Captures waveform for each encryption

Transmit data serially (Ciphertext, Plaintext, Key & Trace)

Data capturing workflow



Methodology

CPA attack with **Hamming Distance** model

Executing Attack

PRESENT cipher

S-box operation[12]

Simon cipher

Bitwise AND operation[13]

Speck cipher

Modular Subtraction[13]

Methodology

Evaluating Results

Two popular Metrics:

→ Guessing Entropy[14]: How many guesses required to guess the correct key

→ Success Rate[14]: The percentage of successful attacks against a target system

Success Rate can be used,

→ Execute attack n times using same data

→ Count successful guesses

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

Current work done

Current work done

Observing Power Traces using C#

Revealing Secret Keys using Cuda

```
E:\Academics\7th Semester\CO421(FYP)\CPA Attack Cuda Code\CPA-AttackCudaCode\CPA-AttackCudaCode>nvcc -w kernel-TDC.cu helpers.cu -o main-TDC
kernel-TDC.cu
tmpxft_00004364_00000000-10_kernel-TDC.cudafe1.cpp
helpers.cu
tmpxft_00004364_00000000-14_helpers.cudafe1.cpp
   Creating library main-TDC.lib and object main-TDC.exp

E:\Academics\7th Semester\CO421(FYP)\CPA Attack Cuda Code\CPA-AttackCudaCode\CPA-AttackCudaCode>main-TDC.exe waveTDC2022-10-18_11-58-11.data
.data file is detected
calculating 0 0
calculating 0 1
  |0|     |1|     |2|     |3|     |4|     |5|     |6|     |7|     |8|     |9|     |10|    |11|    |12|    |13|    |14|    |15|
  4a      d8      52      96      e2      40      2a      5b      ea      b7      ee      b2      66      b9      42      ce
0.0327  0.0351  0.0395  0.0386  0.0446  0.0318  0.0435  0.0324  0.0408  0.0376  0.0351  0.0465  0.0279  0.0366  0.0375  0.0473

  05      db      e8      a3      13      95      37      85      c0      fc      22      1f      72      dd      35      e0
0.0301  0.0266  0.0285  0.0321  0.0299  0.0303  0.0271  0.0267  0.0314  0.0302  0.0288  0.0259  0.0257  0.0295  0.0283  0.0289

  8b      4c      c7      da      ca      dc      cf      e4      f3      c9      d2      e5      fe      95      7d      df
0.0281  0.0265  0.0282  0.0303  0.0251  0.0292  0.0266  0.0261  0.0291  0.0296  0.0283  0.0250  0.0252  0.0276  0.0278  0.0283

  70      9b      f5      b8      e8      e3      6c      8b      8d      9d      55      98      00      72      89      f6
0.0277  0.0264  0.0259  0.0258  0.0249  0.0289  0.0264  0.0259  0.0267  0.0255  0.0270  0.0250  0.0250  0.0259  0.0270  0.0268

  a2      ba      8c      55      dd      89      8a      d4      a2      3b      ec      84      a7      c5      23      bb
0.0276  0.0263  0.0253  0.0258  0.0245  0.0279  0.0261  0.0257  0.0264  0.0249  0.0262  0.0249  0.0241  0.0253  0.0254  0.0249
```

Workplan

Semester 7 : 7 weeks

Semester 8 : 14 weeks

- **SEM 7 | W 3** — Literature Review
- **SEM 7 | W 6** — Attacking AES with the Hardware Setup
- **SEM 7 | W 7** — Project Proposal
- **SEM 8 | W 9** — Attacking other Lightweight Ciphers
- **SEM 8 | W 12** — Assessing the Outcomes
- **SEM 8 | W 14** — Finalizing Research Paper

Thank You!

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.

References

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.

References

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.