Modelling of power consumption for Advanced Encryption Standard and PRESENT ciphers

E Maro
Southern Federal University, Chehova str., 2, Taganrog, Rostov-on-Don region, 347922, Russia

E-mail: eamaro@sfedu.ru

Abstract. Paper presents a result of modelling by ELMO tool and measuring on hardware stand power consumption traces for encryption algorithms Advanced Encryption Standard and PRESENT. Power consumption traces for different version of AES (basic one-round AES algorithm are compared with AESMasked_R1 and MBedAES versions) and PRESENT (with various round numbers) are generated. Assessment of instructions with leaks were made by comparison power consumption traces for fixed-input and power consumption traces for random-inputs (total quantity of traces is $10^4$). Numbers of total and potentially leakage instructions for each examined version of AES and PRESENT ciphers implementation are estimated.

1. Introduction
The cryptographic algorithms used are mathematically (computationally) secure schemes for current computation resources of the attackers and existing approaches of ciphers analysis. At the same time analyzing the security of cryptographic systems is important to consider their implementation in software and hardware tools of information protection. Thus, computationally secure cryptographic algorithms could be vulnerable to attacks using additional information about the data encryption process in real physical devices.

The research topic is focused on theoretical and experimental analysis of the power consumption traces during execution of cryptographic algorithms and assessment of instructions with identified leaks. To collect measurements a hardware stand was assembled on Arduino Nano board, which performs AES and PRESENT encryption algorithms in different versions, and a high-precision oscilloscope RIGOL DS1054. Experimental hardware stand is shown on figure 1. To point encryption area's during measurements of power consumption an output signals were sent to fixed pin. An independent power supply source (4 cells, 1.5 V nominal) was used (to minimize possible voltage fluctuations from an external device). The measurements were carried out through a shunt resistor.

Power consumption traces were modeled using ELMO software [1, 2]. The ELMO simulator consists of two main components: a device emulator (a modified version of the Thumbulator emulator is used) and a set of leak detection algorithms. During constructing a model of hardware equipment in ELMO bit values and bit's changes at inputs and outputs of the arithmetic logic unit (ALU), as well as in commands for working with memory, are considered. Each operand is compared with the corresponding
operand of the previous instruction. The resulting power consumption is modeled as a linear combination of processed bit values or bit changes. ELMO provides the ability to simulate 21 instructions, which are often always used in cryptography tasks: ldr, ldrb, ldrh, str, strb, strh, lsls, lsrs, rors, muls, eors, ands, adds, adds #imm, subs, subs #imm, orrs, cmp, cmp #imm, movs and movs #imm. All instructions are modeled independently and divided into 5 separate groups:

- **ALU instructions** (adds, adds #imm, ands, eors, movs, movs #imm, orrs, subs, subs #imm, cmp, cmp #imm).
- **Shift instructions** (lsls, lsrs, rors).
- **Load instructions** (ldr, ldrb, ldrh)
- **Save instructions** (str, strb, strh)
- **Multiplication instruction** (muls).

![Experimental hardware stand based on Arduino Nano board and oscilloscope RIGOL DS1054.](image)

The data for generating power consumption model is collected after processor executes a sequence of three instructions. Each constructed power consumption trace is preprocessed to find a point-of-interest, after which linear regression is applied to find the coefficients of the model.

The general device model consists of 19 main components, each of which simulates a fixed part of the architecture:

- A linear combination of bit state change between each operand of the current instruction and the corresponding operand of the previous and subsequent instructions.
- A linear combination of the bit values of the operands of the current instruction.
- Groups of the previous and subsequent instructions.

### 2. AES and PRESENT ciphers description

Advanced Encryption Standard (AES) [3] is symmetric block cipher with 128-bits block size and 128, 192 or 256-bits key length. Round transformation consists of 4 different operations (figure 2): substitutions in eight 8-bits length blocks (S-boxes), state shift ShiftRows() for a different bytes positions, shuffle columns MixColumns() by multiplication of state (considered as polynomials over GF
(2^3)) to polynomial \( g(x) = 03x^3 + 01x^2 + 01x + 02 \) by modulo \( x^4 + 1 \), addition modulo two AddRoundKey() with round keys. AES general scheme is presented at figure 2.

\[ \begin{align*}
\text{Plain text} & \quad \xrightarrow{\text{AddRoundKey}} \quad 1^{\text{st}} \text{round} \\
\text{Round key} & \quad \xrightarrow{\text{AddRoundKey}} \quad \text{from 2}\text{nd to (N-1) rounds} \\
\text{Round key} & \quad \xrightarrow{\text{AddRoundKey}} \quad \text{last (N) round} \\
\text{Cipher text} & \\
\end{align*} \]

\textbf{Figure 2. AES cipher scheme.}

PRESENT cipher [4] (figure 3) is based on substitution-permutation network (SP-network) and contains 31 rounds with three operations: addition modulo 2 with round key, substitutions in sixteen 4-bits length blocks (S-boxes) and permutation (H).

\[ \begin{align*}
\text{Plain text} & \\
\text{Permutation H} & \\
\text{Cipher text} & \\
\end{align*} \]

\textbf{Figure 3. PRESENT cipher scheme.}

3. AES and PRESENT power traces modelling and measurement
Model of power consumption trace was generated by ELMO tool during AES encryption. Figure 4 presents power measurement trace for one-round AES encryption. We use version of AES algorithm with directly implemented encryption scheme [5].
Figure 4. A model of power consumption trace during one-round AES encryption in ELMO.

Modeling of power consumption measurements by ELMO tool allows to estimate number of instructions containing information about the protected data (instruction with leaks) based on execution of t-test (with a threshold value of $|4.5|$) for fixed and random plaintexts. Based on the results of comparing power consumption traces of one-round AES cipher ($10^4$ traces), a graph Fix vs Random power consumption test for instructions is presented at figure 5.

Figure 5. Fix vs Random test result for one-round AES instructions.

Table 1 shows results of simulating first-order side-channel leaks for several implementations of the AES cipher.

| AES cipher implementation | Total number of instructions | Number of instructions with identified power consumption leaks |
|--------------------------|------------------------------|-------------------------------------------------------------|
| AES (one-round)          | 741                          | 514                                                          |
| AESMasked_R1             | 451                          | 83                                                           |
| MBedAES                  | 2402                         | 1755                                                         |

Table 1. Simulation results for side-channel leaks for various AES cipher implementations.

We simulated power consumption traces for PRESENT cipher [6] by ELMO tool. Example of generated trace is shown on figure 6. After that we compare traces for fix and random input values (plain texts) and evaluate count of instruction with leaks. Result of leakage assessment for different number of rounds is presented at table 2.
Figure 6. A model of power consumption trace during one-round PRESENT encryption in ELMO.

Fix vs Random instruction graph for one-round PRESENT is shown at figure 7. This graph allows to mark instructions with leaks (evaluate peak points).

Figure 7. Fix vs Random test result for one-round PRESENT instructions.

Table 2. Simulation results for side-channel leaks for various rounds of PRESENT cipher.

| Number of rounds | Total number of instructions | Number of instructions with identified power consumption leaks |
|------------------|-----------------------------|-------------------------------------------------------------|
| 1 round          | 938                         | 379                                                         |
| 2 rounds         | 1771                        | 774                                                         |
| 10 rounds        | 8435                        | 3929                                                        |
| 20 rounds        | 16765                       | 7773                                                        |
| 31 rounds (full-round) | 26047                   | 12137                                                       |

Acknowledgments
This research was funded by RSF research project No 19-71-00041.

References
[1] McCann D, Oswald E and Whitnall C 2017 Towards Practical Tools for Side Channel Aware Software Engineering: Grey Box Modelling for Instruction Leakages USENIX Security
Symposium 199-216

[2] *ELMO: Evaluating Leaks for the ARM Cortex-M0 Instructions of Use and Documentation* (The ELMO Developers https://raw.githubusercontent.com/scaresearch/ELO/master/ELMODocumentation.pdf)

[3] *Advanced Encryption Standard (AES)* (Federal Information Processing Standards Publications (FIPS PUBS) 197, https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf)

[4] Bogdanov A, Knudsen L, Leander G, Paar C, Poschmann A, Robshaw M, Seurin Y and Vikkelsoe C 2007 PRESENT: an ultra-lightweight block cipher *Lect Note. Comput. Sci.* 4727 450-66 doi: 10.1007/978-3-540-74735-2_31

[5] *C++ AES* (Advanced Encryption Standard) implementation (GitHub, https://github.com/SergeyBel/AES)

[6] *PRESENT-C* (GitHub, https://github.com/bozhu/PRESENT-C)