Hardware implementation and comparison of CRA and TRA when trying to recover the AES-128 key

Ivaylo Vladimirov[1], Desislava Nikolova[2] and Zornica Terneva[3]

Abstract – **In this scientific paper, a comparison of two side-channel radio attacks is made: CRA – Correlation Radio Attack and TRA – Template Radio Attack. Both attacks are tested on mixed-signal chips that include both the radio transceiver and the digital logic on the same integrated circuit. In systems like this, the analog transmitter unintentionally leacks sensitive data, related to the cryptographic hardware components and the software being run on the CPU, by broadcasting it on a shifted frequency. The basic conception is that information from the electromagnetic leakage is gathered and then exploited by analyzing it via the side-channel attacks in order to crack the AES-128 algorithm. The system needed for the experiment consists of: a PCA10040 chip by Nordic Semiconductor, an USRP n210 by CP-Ettus Research and a Linux-based computer.**

Keywords – **Side-channel attacks – Correlation Radio Attack, Template Radio Attack, AES-128, Bluethooth, PCA10040, USRP.**

I. Introduction

The mixed-signal chips, also known as Radio Frequency Integrated Circuits (RFICs), have become increasingly popular thanks to the drive for ever smaller and cheaper components in microelectronics. They are used in the construction of widespread wireless communication systems, such as mobile phone, tablet, Bluetooth, Wi-Fi and IoT devices. Structurally their analog and digital circuitry reside on the same piece of a die. This physical proximity naturally leads to noise issues and novel side-channel attacks that can break the implemented cryptography algorithm. [1][2]

The BLE Bluetooth protocol is a wireless standard used for exchanging data between different devices over short distances using radio waves in the 2.4 GHz to 2.48 GHz band. It is used in a combination with AES-128 in these kinds of circuits for secured package based device-to-device communication. [3]

The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data. It is based on a design principle known as a substitution–permutation network, and is efficient in both software and hardware implementations. The key size used for an AES cipher specifies the number of transformation rounds that convert the input, called the plain-text, into the final output, called the cipher-text. The number of rounds are as follows: 10 rounds for 128-bit keys; 12 rounds for 192-bit keys; 14 rounds for 256-bit keys. [4]

[1]Ivaylo Vladimirov is with the Faculty of Telecommunications at Technical University of Sofia, 8 Kl. Ohridski Blvd, Sofia 1000, Bulgaria, E-mail: ivaylo.h.vladimirov@gmail.com.

[2]Desislava Nikolova is with the Faculty of Telecommunications at Technical University of Sofia, 8 Kl. Ohridski Blvd, Sofia 1000, Bulgaria. E-mail: desislava.v.nikolova@gmail.com

[3]Zornitza Terneva is with the Faculty of Telecommunications at Technical University of Sofia, 8 Kl. Ohridski Blvd, Sofia 1000, Bulgaria. E-mail: z.terneva@abv.bg

The two types of side-channel power analysis techniques utilized in the completion of a full key recovery attack against AES-128 compared in this paper are:

The Correlation Radio Attack (CRA) is a model based analysis. It is generally assumed that the data leakage through the power side-channel depends on the energy required to flip the bits from one state to the next at a given time. When used in combination with the Hamming weight model it can be applied to provide a probability value for the likelihood of a given AES-128 sub-key to be the one used in the encryption.[5]

The Template Radio Attack (TRA) exploits the power consumption measured during the operation, expressed as a discrete function of time to reconstruct the sequence of operations during the secret computation and derive information about the AES-128 key. It proceeds in two phases: training (Consisting in measuring the electrical activity of a clone system during numerous encipherments and creating "templates" based on the collected information called "traces") and attacking (Consisting of collecting a few traces and matching them with the existent templates). [6]

II. Concept

The key observation of this research is to make a comparison between and implement in hardware the two power analysis techniques. They are based on the idea that noise coupling propagates sensitive information from the digital domain to the radio transmission chain, which broadcasts it at a much larger distance than normal EM leaks. [1]

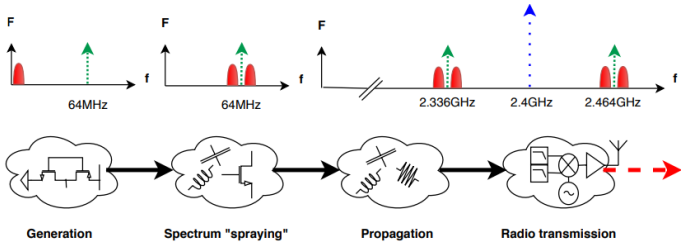

Fig. 1. Steps that lead to the radio transmission of the leak

Information related to the digital processor's activity leaks into other parts of the chip. Components of that leak are likely to reach the transmisive analog portion, in particular the radio transmission chain. They contain frequencies in the range of the radio's baseband signal. The leaked information then couples with the baseband signal via the mixer, amplifier or the Voltage Controlled Oscillator (VCO) that is part of the carrier-frequency synthesizer. In any of the cases the result is unintended amplitude/frequency modulation of the carrier. [7]

The capacitive coupling with the VCO leads to an amplitude modulation of its output signal. Then the parasitically

modulated carrier is amplified by the power amplifier and radiated by the analog antenna over a potentially very long distance. These steps also shown on Figure 1 are as follows: the generation of digital noise, its frequency characteristics, its propagation into other parts of the circuit, and finally its emanation via the radio. [8]

III. Experimental setup and execution

The general setup idea is that one side (See Figure 2 B-left side) there is a computer controlling the RFI cirtuit, which repeatedly transmits data via Bluetooth BLE using the same AES-128 key, on the other (See Figure 2 B-right side) there is another system, functioning as a software defined radio (SDR), tuned at the specific frequency of the leak. The SDR system consists of a USRP device and a PC connected via an Ethernet cable and stores the traces, used for the performance of the two power analysis, on the hardrive of the computer. Figure 2 shows both the preliminary idea and the realised setup.

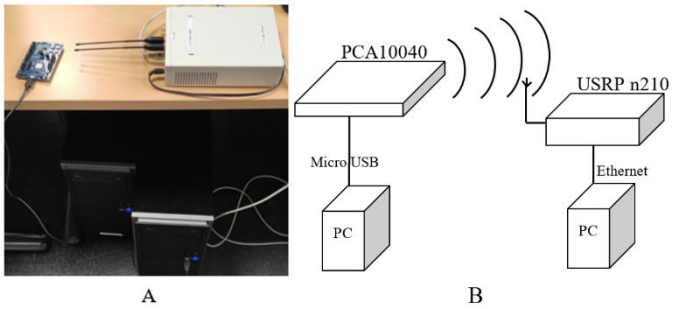

Fig. 2. The experimental setup: A) The physically realised one; B) The preliminary scheme.

In order to use the template attack the attacker needs to have a copy of the whole system, which is needed for the creation of the templates used for its execution. This step may take days even weeks, because for generation of one high quality template a 20 to 30 thousand traces need to be collected. This is equvelent to two to three hours of collection.

After a good set of templates is acquired, the experiment continues with a real time key recovery. First we collect about 3000 traces (about 12 minutes) using the setup shown on figure 2. Then using only PC containing all required software the two attack techniques are run. An example and full description of the attacks and how they run can be found in [9].

After the performance of an attack a table containing the numerical results is displayed in the Linux terminal window, an example result can be seen in figure 3. The first two lines show the bytes of the best guess and of the known key. The PGE is the Partial Guessing Entropy - the "distance" of the best guess from the known byte (0 when the guess is correct). At the end the number of correct bytes is shown.

```
Best Key Guess:    a0   0c   a2   30   3b   d3   3c
Known Key:         a0   0c   a2   30   3b   d3   3c
PGE:              000  000  000  000  000  000  00(
SUCCESS:            1    1    1    1    1    1    1
NUMBER OF CORRECT BYTES: 16
```

Fig. 3. The terminal window results after performing an attack

IV. Comparison and conclusion

This leakage used and described in this scientific paper is not due to the design error of an individual vendor, but to a fundamental difficulty in designing mixed-signal chips.

When making a comparison between the two attacks we can see that the CRA is a simpler technique needing less preparation but using more traces collected at the moment to return a better result. Its computational speed is fairly good depending on the power of the computer and the number of traces provided (the lesser traces the fasted the attack, but also the lower the chance for a full recovery of the key). It also uses all given traces before making a decision on which is the best guess for a certain sub-key, which additionally slows the attack. The full execution took about 11 minutes.

In comparison, the TRA's algorithm is more complex and needs more computation power. It requires a lot of preparation – a copy of the system that will be attacked and its excessive pre evaluation. Its computational speed is very fast and makes a decision decision on which is the best guessed sub-key after a certain value for the probability is reached. The full execution took about 1 minute and 30 seconds, which is 10 times faster and needed a only a little over 100 traces to recover the full key, which is 30 times the traces less than collected.

Acknowledgement

The research described in this paper is partially realized within the Erasmus+ mobility program with the help of the professors at SUPELEC University in Rennes, France.

The implementation of the codes for the two side-channel power analysis techniques used in this paper are described in a scientific document: "Software implementation of CRA and TRA to recover the AES-128 key using side-channel signals with Python3" [9] that will also be presented at the ICEST 2020 conference.

References

[1] G.Camurati S.Poeplau M.Muench T.Hayes A.Francillon, „Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers", 2018;

[2] A.Afzali-Kusha M.Nagata N.K.Verghese D.J. Allstot „Substrate Noise Coupling in SoC Design: Modeling, Avoidance, and Validation", 2006;

[3] I.Hibbert, Itronix Inc, "Bluetooth.4 — Bluetooth Protocol Family", 2006;

[4] D.J.Bernstein, "Cache-timing attacks on AES. Report", 2005;

[5] V.K.Rai B.V.Reddy, "Correlation power analysis and effective defense approach on light encryption device block cipher", 2019;

[6] M.E.Aabid„Template Attacks with a Power Model", 2007;

[7] S.Bronckers G.Van der Plas G.Vandersteen Y.Rolain. "Substrate Noise Coupling in Analog/RF Circuits.", 2009;

[8] H.Li A.T.Markettos S.Moore, „Security Evaluation Against Electromagnetic Analysis at Design Time – 2005;

[9] D.Nikolova I.Vladimirov Z.Terneva, "Software implementation of CRA and TRA to recover the AES-128 key using side-channel signals with Python3", 2020.