Side-Channel Analysis of Cryptographic Processor CEC 1702

Tereza Horníčková, Tomáš Přeučil, Martin Novotný
Czech Technical University in Prague
Faculty of Information Technology
Czech Republic
{horniter|preucto2|novotnym}@fit.cvut.cz

Zdeněk Martinásek
Brno University of Technology
Faculty of Electrical Engineering and Communication
Czech Republic
martinasek@vut.cz

***Abstract*—Cryptography is omnipresent in our daily life, as we need it for trusted authentication (e.g., in access systems), secure communication, ensuring data integrity and confidentiality, and many more. However, even if mathematically secure ciphers are used, the device running the cryptographic algorithms is still vulnerable to side-channel attacks that may reveal the secrets. These attacks exploit the fact that power consumption or electromagnetic emanation of the device depends on processed data. To prevent such an attack, the designer must employ countermeasures, such as masking, hiding, or shuffling.**

In this paper, we focus on Microchip CEC1702 microcontroller that supports common cryptographic operations in hardware. We analyze the resistance of its AES accelerator against correlation power analysis (CPA). We analyzed 100 million power traces by first-order CPA and univariate second-order CPA. In neither case did we find any vulnerability.

***Index Terms*—AES, CEC1702, PicoScope, CPA, Higher-order CPA, SICAK, Side-channel attacks, ChipWhisperer**

I. Introduction

Side-channel attacks are types of attacks based on exploiting physical manifestation of the handled data. Vital information may leak based on the device's power consumption [1]–[4], electromagnetic radiation [5]–[8], time of cryptographic operation [9], etc., as all of these are closely tied to the values of handled data. As such, even a mathematically secure cipher's implementation can be successfully attacked if it doesn't incorporate appropriate countermeasures against these attacks.

With the rise of communication security, some microcontrollers have been equipped with hardware accelerators for cryptographic operations. As an example, we mention Atmel/Microchip AT97SC3205T, Maxim MAX32510, Microchip CEC1302, Microchip CEC1702, or NXP P71D321. For the reasons mentioned above, it is necessary for their designers to ensure that these accelerators are resistant to side-channel attacks.

CEC1702 is an ARM Cortex-M4 based microcontroller produced by Microchip. It provides a number of hardware-based cryptography features such as True Random Number generator, AES/Rijndael [10], SHA, or RSA [11] accelerator. In this work, we evaluate the resistance of its AES hardware accelerator against Correlation Power Analysis [2]. We use 128-bit variant of AES.

This paper is structured as follows: In section II, we summarize the basic principle of Correlation Power Analysis. In section III, we describe the measurement carried out on software implementation of AES and hardware accelerator of AES. Results of our measurements are summarized in section IV. Our work is concluded in section V.

This research has been supported by the grant VJ02010010 of the Ministry of the Interior of the Czech Republic, "Tools for AI-enhanced Security Verification of Cryptographic Devices" in the program Impakt1 (2022-2025).

II. Correlational Power Analysis Attack

Correlational Power Analysis (CPA) [2] is a type of side-channel attack using a relationship between power consumption and handled data. This method stands on measurements of power consumed by the device while performing encryption and having access to either the original plaintext or resulting ciphertext. Following the measurements, a power consumption prediction model needs to be computed. This model predicts approximate power consumption for a given sample (e.g., using Hamming's weight of processed intermediate data) for each possible key candidate. After the model is computed, the search for correlation between the hypothetical model and actual measurements begins. The correlation between measured values and a correct hypothetical key candidate is significantly higher compared to the rest.

III. Measurement Setup

The measurements and subsequent attacks were carried out in three distinctly different setups listed in Table I. All measurements were performed using ChipWhisperer C308 UFO standalone evaluation board [12] with CEC1702 target mounted on it.

A. Setup A: SW implementation of AES + ChipWhisperer toolchain

Protection against side-channel attacks can be carried out on different levels. One can protect, e.g., the whole processor or just the cryptographic accelerator. To distinguish whether and on what level the protections are implemented, we first evaluated the pure software version of AES with no countermeasures.

The power consumption was measured as a drop-off voltage on a shunt resistor at the CEC1702 target board (SMA connector J17 on CW 308 UFO board). Power traces were sampled using ChipWhisperer-Lite Capture board [13]. To improve power

TABLE I
MOUNTED ATTACKS CONFIGURATIONS

AES type	SW		HW			
Measurement & Analysis						
Setup	A	B	C			
Capture	ChipWhisperer	PicoScope	PicoScope			
Sampling Rate	48.51 MSa/s	2.5 GSa/s	2.5 GSa/s			
#Samples/Trace	24400	150k	1375			
Analysis	1^{st} order CPA	1^{st} order CPA	1^{st} order CPA		2^{nd} order CPA	
#Traces	10k	16k	100M		100M	
Success	✓	✓	✗		✗	
Time & Space Complexity of Measurement and Analysis						
Command		Time	File Size	Time	File Size	Time	File Size
`meas`	—	3m 15s	4.69 GB	53h 20m	268.6 GB	reused from 1^{st} order CPA	
`prep`	—	1s	64 MB	6h 40m	400 GB		
`stan - create`	—	120m	4.84 GB	130h	444 MB	355h	888 MB
`stan - merge`	—	—	—	9s	399.6 MB	9s	799.2 MB
`stan - finalize`	—	43s	4.8 GB	1s	44 MB	1s	44 MB
`correv`	—	6s	—	1s	—	1s	—

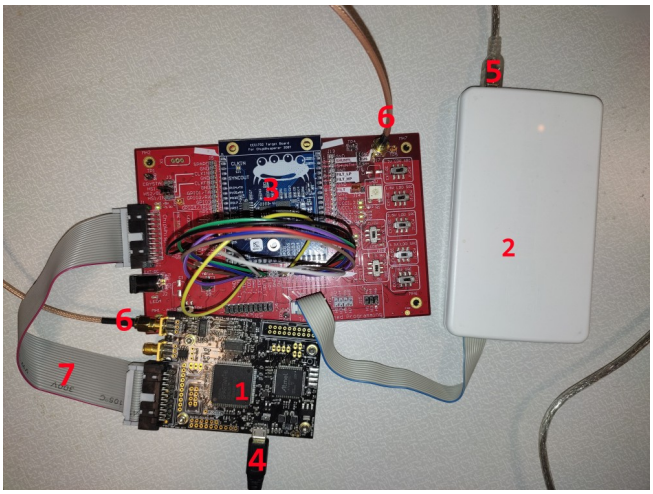

Fig. 1. Setup for trace capture on CEC1702 using ChipWhisperer Lite. 1—Chipwhisperer Lite, 2—mikroProg For CEC, 3—CEC1702 connected to UFO board, 4—ChipWhisperer Lite connection to PC via microUSB, 5—mikroProg For CEC connection to PC via miniUSB, 6—measuring probe connected to J17, 7—20pin cable connection between UFO board and ChipWhisperer Lite

analysis attacks, the capture board enables synchronization of sampling with a clock signal [14]. As CEC1702 is clocked by an internal oscillator and does not allow an external clock signal, we synchronized sampling indirectly via PWM. We captured one sample per clock cycle; the sampling rate was 48.51 MSa/s.

To align measured power traces, the measurement was triggered by a signal that was set and cleared by a program running AES encryption. Measured power traces were analyzed in Wolfram Mathematica [15]. The setup is to be seen in Figure 1.

B. Setup B: SW implementation of AES + PicoScope/SICAK toolchain

We analyzed the software implementation of AES using a second measurement setup as well. In this case, power traces were captured using PicoScope6404D [16]. Measurement was controlled by utility `meas` from SICAK toolkit software [17].

The communication between the computer and the target device (transfer of plaintext and ciphertext to/from the CEC1702), as well as the communication between the computer and the oscilloscope (transfer of power traces), dominates the entire measurement in terms of time. To reduce it, we perform the measurements in bursts. In each burst, we measure 100 encryptions. At the beginning of the burst, we send the initial plaintext to CEC 1702. The code inside CEC1702 then generates the next 99 plaintexts according to a specified pattern. The last ciphertext is sent back to the control computer. The oscilloscope is configured to make 100 measurements in one burst. All 100 power traces are transferred to the computer at once, reducing communication overhead.

Utility `meas` communicates with both the oscilloscope (PicoScope6404D) and the measured device (CEC1702). It configures the oscilloscope, sends initial plaintext to CEC1702 via UART, receives the final ciphertext, and collects measured traces. Configuration of utility `meas` involved:

- measuring time post-trigger: 60 μs
- UART settings: 115 200 bps; no parity; one stopbit
- number of `captures`[1]: 100
- samples per trace: 150 000

Note that channels A and B of PicoScope share the same sampling circuit, which may result in halving the maximum sampling rate if both channels are used. The same applies to channels C and D. To preserve the maximum sampling rate, we measured the power consumption (SMA connector J17 on UFO board) by channel A, while the trigger signal (pin TP7) was captured by channel C. The sampling rate was then 2.5 GS/s. The setup is to be seen in Figure 2 with a closer look at connections to the UFO board provided in Figure 3. Measured power traces were analyzed by utility `stan` from SICAK toolkit.

[1]number of power traces to be captured in one burst; limited by specific oscilloscope's buffer memory and ability to store multiple captures

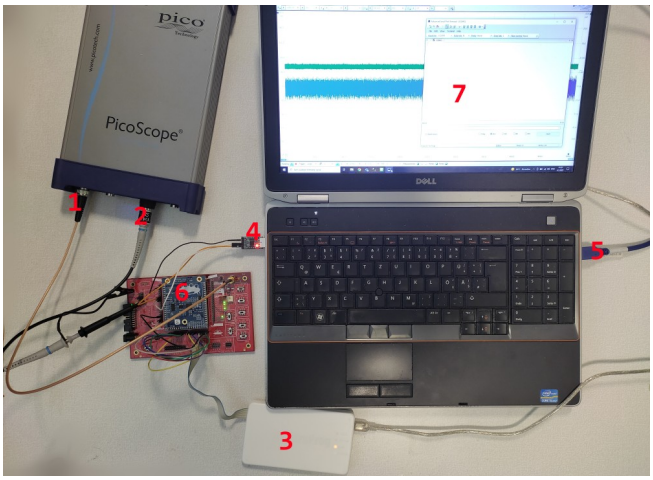

Fig. 2. Setup when using PicoScope. 1—PicoScope A channel probe (power consumption), 2—PicoScope C channel probe (trigger), 3—mikroProg for CEC, 4—6pin UART to USB converter: CP2102, 5—USB connection to PicoScope, 6—CEC1702 target mounted to UFO target board, 7—Advanced Serial Port Terminal

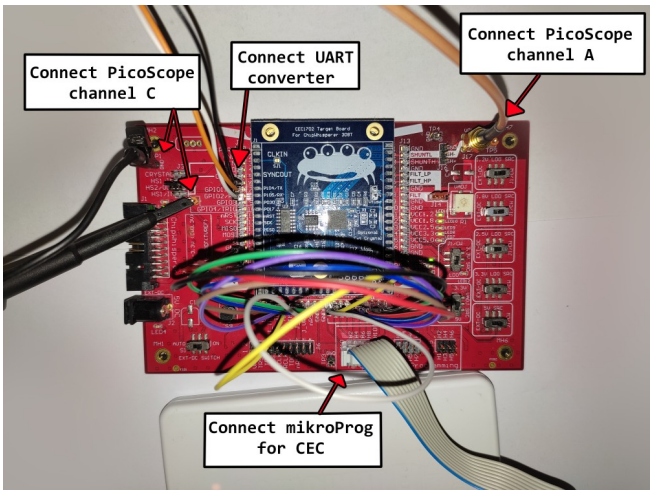

Fig. 3. Setup when using PicoScope

C. Setup C: HW accelerator of AES + PicoScope/SICAK toolchain

We assumed that millions of power traces would be needed to analyze the AES HW accelerator. Measuring such a large number of power traces using the ChipWhisperer toolchain would take too much time since, due to the limited memory of the ChipWhisperer-Lite Capture board, we could only measure one or a few power traces at once. For this reason, we focused only on measurements with PicoScope, which, due to its deep memory, easily allows 1000 measurements in one burst.

We modified the code in CEC1702 accordingly—the software implementation of AES was replaced with a function call of AES hardware accelerator, and AES encryption is run 1000 times in one burst, with plaintexts generated according to a specified pattern. The measurement setup matches the one described in subsection III-B, except for following changes in `meas` configuration:

- measuring time post-trigger: 8.8 μs
- UART settings: 115 200 bps; no parity; one stopbit
- number of `captures`: 1 000
- samples per trace: 1 375

The attack was mounted multiple times, with the number of captured traces rising from the initial 1M up to the last 100M. To minimize the damage incurred by possible failure during the capture of 100M traces, the measuring itself was split into ten separate runs of `meas` over 10M traces each. The runs were later merged during analysis by `stan` utility.

IV. Measurement Results

Measured power traces were analyzed on a desktop PC equipped with Intel i3-4170 CPU, RAM with a capacity of 16 GB and HDD with a capacity of 2 TB. The attack results are presented in Table I.

A. Setup A: SW implementation of AES + ChipWhisperer toolchain

The entire encryption in the software implementation of AES takes about 520 μs. ChipWhisperer-Lite Capture board has a buffer of a maximum capacity of 24400 samples, i.e., with a sampling rate of 48.51 MSa/s, we could sample almost the whole power trace.

We analyzed the captured power traces using a script in Wolfram Mathematica running first-order CPA. We focused on the SubBytes operation during the first round of AES execution. The power model was the Hamming weight of the S-box output. We needed 10 000 power traces to successfully reveal the secret key. We can state that there are no countermeasures protecting the processor as a whole.

B. Setup B: SW implementation of AES + PicoScope/SICAK toolchain

We repeated the previous analysis with the setup that was later used for the analysis of the hardware accelerator. PicoScope6404D has more than 50 times higher sampling rate compared to the ChipWhisperer-Lite Capture board. To minimize the volume of analyzed data, we measured only the first 60 μs of each power trace. This safely covers the first round of AES, where the operation of our interest appears.

We again analyzed captured power traces using first-order CPA. This time we used utilities `prep`, `stan`, and `correv` from SICAK toolkit. We needed 16 000 power traces to successfully reveal the secret key, which is 60% more compared to Setup A. This proves that, despite the fact that PicoScope provided a significantly more fine-grained sampling of power traces, the most important factor is the synchronicity of sample rate and the clock frequency [14].

In the bottom part of Table I, we provide information on the time and space complexity of the measurement and subsequent analysis. As can be seen, measurement took slightly more than 3 minutes, and measured traces occupied almost 5 GB. Compared to that, the analysis of captured traces is much more time demanding, as it took about two hours.

TABLE II
GUESSING ENTROPY – AVERAGE PLACEMENT OF A CORRECT KEY GUESS

#traces	10M	100M
1^{st} order	18.88	13.4
2^{nd} order	18.3	23.44

C. Setup C: HW accelerator of AES + PicoScope/SICAK toolchain

Hardware accelerator runs one AES encryption in about 550 ns. We measured the entire encryption, capturing 1375 samples per trace when sampling at the rate of 2.5 GSa/s. We did ten measurement runs. In each run, we captured ten million power traces (together with corresponding plaintexts and ciphertexts), which occupied 26.86 GB of disk space. Measurement of one run lasted 5 hours and 20 minutes, i.e., all measurements combined took over 53 hours (see Table I). We analyzed measured data using first-order CPA and second-order CPA.

1) First-order CPA: To evaluate the resistance of the AES hardware accelerator against first-order CPA, we used all 100 million power traces. Every run of ten million measurements was analyzed separately (utilities `prep` and `stan -create`). Partial results of every run were then merged (utility `stan - merge`), and the final keyguess was calculated (utilities `stan - finalize` and `correv`).

Analysis of all 100 million traces took more than 136 hours. Despite the effort and time invested in the analysis, we were not successful in revealing the correct key.

Subsequent calculation of guessing entropy revealed that the values of the correct key placed around 18^{th} place in case of analysis of 10 million traces (see Table II) while analysis of 100 million traces evaluated the correct key to be 13^{th} most likely guess on average. The guesses placed considerably high considering the number of possible candidates (256), and the results improved with the number of traces.

2) Second-order CPA: Second-order CPA has the potential to surmount the first-order countermeasures. Its power is however paid off by increased computational complexity. To evaluate the resistance of the AES hardware accelerator against univariate second-order CPA, we used the same 100 million power traces. The computations lasted additional 355 hours (about 2 weeks), however, we were not successful in revealing the correct key even in this case.

Calculation of guessing entropy revealed that the values of the correct key placed around 18^{th} place in case of analysis of 10 million traces (see Table II) while analysis of 100 million traces evaluated the correct key to be 23^{rd} most likely guess on average. While the guess placed considerably high, the decline in placement with a growing number of traces is worth noting.

V. CONCLUSION

We evaluated the resistance of Microchip CEC1702 against Correlation Power Analysis when running AES encryption. First, we focused on the software implementation of AES without any countermeasures. We used two different measurement setups, and we successfully mounted an attack in both cases—in the case of the ChipWhisperer toolchain, we needed 10 000 power traces to reveal the secret key, while PicoScope/SICAK toolchain required 16 000 power traces. This proves that there are no countermeasures protecting the CEC1702 microcontroller as a whole.

Then we focused on the AES hardware accelerator of CEC1702. We analyzed 100 million power traces by first-order CPA and univariate second-order CPA. In neither case were we successful in mounting the attack. We have not found any vulnerability of CEC1702's AES hardware accelerator towards a power analysis attack.

ACKNOWLEDGMENT

This work was supported by the Student Summer Research Program 2023 of FIT CTU in Prague.

REFERENCES

[1] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," in *Advances in Cryptology — CRYPTO' 99*, pp. 388–397, Springer Berlin Heidelberg, 1999.

[2] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in *Cryptographic Hardware and Embedded Systems - CHES 2004* (M. Joye and J.-J. Quisquater, eds.), (Berlin, Heidelberg), pp. 16–29, Springer Berlin Heidelberg, 2004.

[3] B. den Boer, K. Lemke, and G. Wicke, "A dpa attack against the modular reduction within a crt implementation of rsa," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 228–243, Springer, 2002.

[4] S. Chari, J. R. Rao, and P. Rohatgi, "Template attacks," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 13–28, Springer, 2002.

[5] J.-J. Quisquater and D. Samyde, "Electromagnetic analysis (ema): Measures and counter-measures for smart cards," in *Smart Card Programming and Security*, pp. 200–210, Springer, 2001.

[6] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, "The em side—channel (s)," in *International workshop on cryptographic hardware and embedded systems*, pp. 29–45, Springer, 2002.

[7] D. Carluccio, K. Lemke, and C. Paar, "Electromagnetic side channel analysis of a contactless smart card: first results," in *ECrypt Workshop on RFID and Lightweight Crypto*, 2005.

[8] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis: Concrete results," in *International workshop on cryptographic hardware and embedded systems*, pp. 251–261, Springer, 2001.

[9] P. C. Kocher, "Timing attacks on implementations of die-hellman, rsa, dss, and other systems," in *Advances in Cryptology— Crypto*, vol. 96, p. 104113, 1996.

[10] J. Daemen and V. Rijmen, "The block cipher rijndael," in *International Conference on Smart Card Research and Advanced Applications*, pp. 277–284, Springer, 1998.

[11] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, p. 120–126, feb 1978.

[12] NewAE Technology Inc., "CW308 UFO [online]." https://rtfm.newae.com/Targets/CW308%20UFO/. [cit. 2023-04-08].

[13] NewAE Technology Inc., "CW1173 ChipWhisperer-Lite [online]." https://rtfm.newae.com/Capture/ChipWhisperer-Lite/. [cit. 2023-04-08].

[14] C. O'Flynn and Z. Chen, "Synchronous sampling and clock recovery of internal oscillators for side channel analysis and fault injection," *Journal of Cryptographic Engineering*, vol. 5, pp. 53–69, 2015.

[15] Wolfram, "Wolfram Mathematica [online]." https://www.wolfram.com/mathematica/. [cit. 2023-04-08].

[16] Pico Technology Ltd., "PicoScope 6000CD Series Datasheet [online]." https://www.picotech.com/download/datasheets/PicoScope6000CDSeriesDataSheet.pdf. [cit. 2023-04-08].

[17] P. Socha, "SICAK: SIde-Channel Analysis toolKit [online]." https://petrsocha.github.io/sicak/. [cit. 2023-04-08].