TURKISH JOURNAL OF ENGINEERING RESEARCH AND EDUCATION

Türk Mühendislik Araştırma ve Eğitimi Dergisi
Turkish Journal of Engineering Research and Education

1(2), 92-99, (2022)

RESEARCH ARTICLE

An Experimental Framework for Power Analysis for Side-channel Attacks

Yan Kanal Saldırılarında Güç Analizi için Deneysel bir Altyapı

Halil Said Cankurtaran[1,*], Ali Boyacı[2] , Serhan Yarkan[2]

[1] Istanbul University – Cerrahpaşa, Electrical-Electronics Eng., Avcilar, İstanbul, Turkiye, 34320

[2] Istanbul Commerce University, Electrical-Electronics Eng., Kucukyali, Istanbul, Turkiye, 34840

Received/Geliş: 19.09.2022
Accepted/Kabul: 15.10.2022
***Corresponding Author:** **Halil Said Cankurtaran, h.cankurtaran@ogr.iuc.edu.tr**

ABSTRACT: Side-channel attacks can be classified as cybersecurity threats that risk the confidentiality, integrity, and authenticity of the information. However, they are often overlooked by developers, manufacturers, and maintainers since adversaries need to access devices physically most of the time. Although they are usually ignored, the development of novel attack methods and countermeasures show that side-channel attacks maintain their importance in cybersecurity. Unfortunately, although advanced analysis methods are presented in detail, the discussion of measurement campaigns and the negative effects of environmental parameters are usually omitted in the articles. In order to close this gap, a measurement campaign that can be used in power analysis side-channel attacks, possible problems that researchers may encounter during measurements, and their solution methods are presented in this article. In addition, interference caused by a signal generator operating in the same environment has been experimentally demonstrated to show that dedicated jammers can significantly affect the performance of analysis methods.

Keywords: Side-channel attacks, power analysis, measurement, interference, framework

ÖZ: Yan kanal saldırıları, günümüzde bilginin gizliliğini, bütünlüğünü ve özgünlüğünü tehdit eden fakat fiziksel erişim gerekliliği yüzünden sıklıkla göz ardı edilen bir siber güvenlik tehdidi olarak sınıflandırılabilir. Her ne kadar göz ardı edilseler de yeni saldırı yöntemlerinin ve önlemlerin literatüre sunuluyor olması, yan kanal saldırılarının önemini koruduğunu göstermektedir. Ne yazık ki, ölçüm düzeneklerinin betimlemesinin ve çevresel değişkenlerin olumsuz etkilerinin açıklamasının yayınlarda genellikle ihmal edildiği gözlemlenmektedir. Bu açığı kapatabilmek amacıyla güç analizi saldırılarında kullanılabilecek bir ölçüm düzeneği, araştırmacıların ölçüm düzeneğinde karşılaşabileceği olası sorunlar ve çözüm yöntemleri bu makalede sunulmuştur. Ek olarak, çevresel etkenlerin önemini vurgulamak ve yüksek güçlü karıştırıcıların, saldırıların performansını etkileyebileceğini göstermek amacı ile ölçüm düzeneğinin yakınlarında çalışan bir işaret üretecinin sebep olduğu girişim deneysel olarak gösterilmiştir.

Anahtar Kelimeler: Yan kanal saldırıları, güç analizi, ölçüm, girişim, altyapı

1. INTRODUCTION

Security, privacy, and confidentiality are all among the essential parts of contemporary communication systems and information services. Recently, they have become integral components of digital technology design, development stages, and manufacturing processes as well. Ranging from signal level approaches such as covert transmission methods [1] to hardware level techniques such as digital (silicon or non-silicon) fingerprinting of physical unclonnable functions [2], information security concepts continuously improve. Of course, with the great advances in digital technology, adversarial techniques also evolve and threaten

Halil Said Cankurtaran, Orcid: 0000-0003-3143-2538 / Ali Boyacı, Orcid:0000-0002-2553-1911 / Serhan Yarkan, Orcid: 0000-0001-6430-3009

these emerging methods and techniques.

Concerns regarding the confidentiality, integrity, and authenticity of the message/information have not been alleviated even the scientific and technological developments have changed the medium that information is stored or transferred, or different encryption algorithms are developed [3, 4]. For instance, Rivest–Shamir–Adleman (RSA) algorithm is developed to restrict third parties' access to sensitive and/or personal information [5]. RSA exploits the complexity of the factorization of large numbers which are generated by the multiplication of two prime numbers. Due to the nature of the factorization problem, it may take thousands of years to solve a message encrypted by the RSA depending on the size of prime numbers used. While certain people try to develop efficient methods to solve encryption algorithms, the nature of electronic devices can also be exploited to reveal disguised information [6].

Depending on the physical structure of electronic devices and computational processes, they unintentionally emit/generate different kinds of signals such as electromagnetic waves [7], heat [8], sound, power consumption [9], and timing [10]. Computations and memory read/write operations are generally determined by previously determined private keys in encryption algorithms. Hence, they are usually embedded into the devices in such a way that third parties cannot access them. However, adversaries can exploit leaked signals to reveal confidential information [9]. A block diagram of encryption process is illustrated in Fig. 1. This figure emphasizes the differences between the ideal and real-world implementation of an encryption method and shows unintentionally generated side-channel signals.

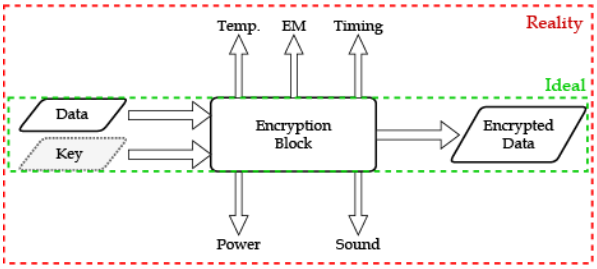

Figure 1: Diagram showing possible side-channel leakages during the encryption.

Recent studies show that encryption modules used in common end-user products can easily be abused by conventional power-analysis techniques [11]. Moreover, it is much easier to access high performance side-channel attack (SCA) algorithms and software due to the developments in electronics, computation, and machine learning algorithms [12]. Hence, developing countermeasures by conducting recently introduced studies and understanding the vulnerabilities of devices is a crucial task for researchers. Taking accurate and precise measurements is the fundamental step in SCAs independent from the scale, device, or application [13]. Hence, measurement methods, devices, device-dependent parameters, and environmental conditions should be optimized for each type of measurement. On the other hand, most of the papers in the literature omit a detailed explanation of their measurement devices, parameters, and environmental conditions. This attitude contradicts the reproducibility principle of the scientific method and increases the steepness of the learning curve for people. As a result, the pace of development in cybersecurity is decelerated since people spend their time optimizing the measurement environment, which is done but not reported before, instead of developing better analysis methods and countermeasures. Thus, this paper aims to close the gap between an expert and a novice in the power analysis SCAs field of research. A typical measurement campaign, connections, and configurations are presented to make researchers familiar with the setup. Additionally, possible issues researchers might encounter, and their solutions are presented. Also, the effects of electronic devices operating near the measurement environment are presented. Results show that even if measurements are taken over a resistor using oscilloscope probes, other electronic devices operating in the same environment might interfere with the measurements. These results raise another question: Can measurements be jammed by using highly directional antennae intentionally? However, these problems will be explored in the upcoming studies.

Article is structured as follows: In Section 2, SCAs, countermeasures and importance of measurements are explained. In Section 3, a typical measurement campaign to conduct a power analysis SCA is presented. Section 4 lists the most common issues

encountered during the measurements and demonstrates their solution methods. Then, in Section 5, effects of an interference source in the vicinity of measurement devices are presented. Finally, conclusions and future directions are given in Section 6.

2. SIDE-CHANNEL ATTACKS

An SCA basically consists of three fundamental steps: (i) data collection, (ii) data preparation, and (iii) analysis. Data collection can also be divided into two cases as intrusive and non-intrusive methods. electromagnetic (EM) waves, sound, and changes in temperature of the device can be measured remotely/non-intrusively, where power consumption and timing measurements require physical access to pins or the power socket of the device. In order to perform an SCA, almost all methods assume that the beginning and end of the encryption process are known for each and every execution. Hence, one of the most important processes before the analysis of data is determining the region of interest (RoI) which can be defined as the region where encryption is executed [14]. Additionally, the pre-processing step might include some sort of filtering to remove noise. Finally, the attacker performs an analysis to obtain the private key from measurements. Several methods have been proposed to overcome inherent noise in the measurements such as differential power analysis (DPA), correlation power analysis (CPA), and template attack (TA) [6]. Additionally, researchers successfully applied machine learning methods to obtain private keys [15].

Several institutions published standards for securing the storage, processing and transmission of information [16–18] and researchers have been developing countermeasures to prevent SCAs [19]. For instance, routing encryption operations to lower-level metal layers inside the chip to prevent emission of electromagnetic waves [20], performing independent sub-procedures randomly or in parallel to hide structural information [21], and adding randomly and redundantly power consuming components to bury characteristic power consumption signature of mathematical operations into a noisy signal [19].

3. A TYPICAL MEASUREMENT CAMPAIGN

A basic measurement campaign for power analysis consists of three elements: (i) A control device, generally a computer, to send messages for encryption, (ii) device under attack (DUA), and (iii) a digital sampling oscilloscope (DSO) to acquire voltage fluctuation during the encryption process. However, a power supply having both floating and earth ground options might be required to prevent grounding issues. A block diagram representing a basic measurement campaign is given in Fig. 2. Each device and its operational requirements will be explained.

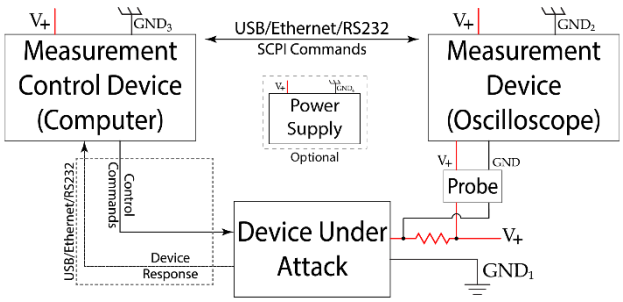

Figure 2: Block diagram of power analysis measurement campaign.

3.1 Device Under Attack (DUA)

Power analysis can be performed on smart cards, microprocessors, central processing units, graphical processing units, mobile phones, etc. All of these devices have an interface to communicate using standard ports like USB, Ethernet, or RS232, or they would have pins supporting I2C, or SPI. An attacker should know the supply voltage of the device and tap a resistor as close as possible to the processing unit of DUA in order to eliminate the noise and effect of other electronic components on the device as much as possible. For instance, in this study measurements are taken by soldering a resistor between Vcc pin of Atmega 328P micro-controller and DIP socket on Arduino UNO board as shown in Fig. 3. Additionally, any filter regulating power input can be removed to increase fluctuations during the processes.

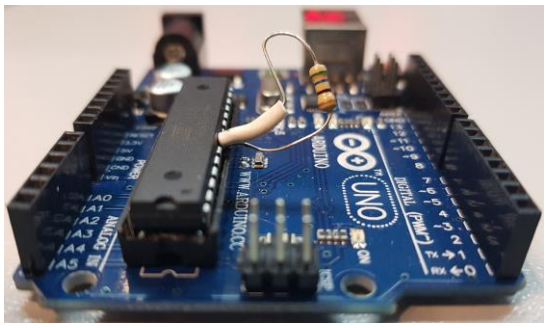

Figure 3: Resistor attached between Vcc pin of Atmega 328p and DIP socket on Arduino UNO.

3.2 Measurement Control Device

A measurement control device, typically a computer, is used to send encryption messages to the DUA and simultaneously control the measurement device. Almost all measurement equipment follows the Standard Commands for Programmable Instruments (SCPI) [22]. Virtual Instrument Software Architecture (VISA) library, which is available in common programming languages such as C++ and Python, can be used to send SCPI commands to control measurement devices remotely. Additionally, the measurement device might have a triggering mechanism that can be activated when encryption is started. For instance, a trigger signal can be sent to the measurement device right after the last byte of input text send to the cryptographic device. However, in most real-world scenarios, it is not possible to control when the last byte of the message is sent to or received by the DUA. Hence, dedicated control and measurement hardware is developed to provide a better triggering mechanism [23].

3.3 Measurement Device

A measurement device is used to acquire fluctuations of input voltage while DUA performing encryption. In order to record an accurate and precise measurement, the parameters of the measurement device should be set correctly. Since most of the data is acquired in the time domain, the sampling frequency of the device should be set twice the clock frequency of the DUA to prevent aliasing in the data. Also, the record length of the DSO should be higher than the duration of encryption. Additionally, if the measurement device does not have an option to directly save the data in the memory, and provides only the data displayed on the screen, then, the vertical resolution of the device should be set in such a way that maximum peak-to-peak voltage fits onto the screen perfectly.

3.4 Measurement Probe

In SCAs, differential probes are used to capture small potential changes over the resistor. Most of the probes have adjustable attenuation options to make sure that the potential difference between the positive and negative end of the probe falls into the operational range of the analog-to-digital converter of the DSO. However, the preferred probe should not attenuate the input signal since voltage fluctuations during a power analysis SCA on a cryptographic electronic device will be in the order of millivolts.

3.5 Power supply

An adjustable power supply might be required to power up DUA. Additionally, it can be used to isolate either measurement control device or measurement device from the earth/chassis ground. Grounding problems will be analyzed in Section 4 in detail.

4. REMARKS

In addition to points emphasized in Section 3, researchers should be careful about the operation and interconnection of devices in order not to damage any equipment and collect accurate data. This section tries to cover most common mistakes.

4.1 Ground Loops

A typical measurement environment consists of four different elements (computer, DSO, probe, and device under attack) which are interconnected to each other as shown in Fig. 2. Computers and DSOs are connected to the same electrical grid in most cases, and they share common ground. If this grid is directly connected to the power line, grounds can be considered zero. However, as shown in Fig. 4, the negative end of the differential probe is connected to a point that approximately equals the supply voltage of the DUA. In case the grounds of the computer and DUA are also connected to each other, DUA will be short-circuited and a current flow through the ground path. Since the impedance of ground paths is very low, the current flowing through the ground path probably damages one of the components in the measurement campaign.

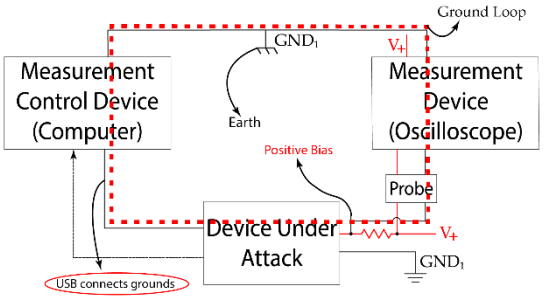

Figure 4: Ground loop schematic representation.

4.2 Common Board Loop

Even computers and DSO connected to different power sources whose grounds are isolated, connecting these two devices via USB might equalize their ground levels since USB ports are directly connected to chassis ground in most electronic devices. Hence, connection between computer and DSO should be established via local area network (LAN) cable if possible.

4.3 Interference

During the measurements, electromagnetic waves generated by other electronic devices running in the same environment might couple with the measurement equipment. For instance, power cables, resistors used to measure voltage fluctuations and DSO probes act as an antenna if they are not properly isolated. As a result, signal-to-noise ratio (SNR) decreases, and the number of measurements required to obtain information increases. Moreover, measurements might be jammed intentionally by people who want to prevent the extraction of private information. Hence, measurement environment should be controlled for interference sources before beginning the measurements.

5. CASE STUDY: EFFECTS OF INTERFERENCE

5.1 Measurement Campaign

Devices used in the measurement campaign are listed on Table 1 and shown in Fig. 5 and Fig. 6. In order to prevent ground loop mentioned in Section 4.1 computer is connected to a Uninterrupted Power Supply (UPS) socket, and DSO directly plugged into the power grid. Additionally, the computer and DSO are connected over LAN using a Cat-5 cable to prevent the issue mentioned in Section 4.2. Advanced Encryption Standard (AES) algorithm is implemented on an Arduino UNO (Atmega 328p micro-controller), and power traces are recorded during the encryption. Arduino UNO was connected to computer via USB cable to power, and send encryption command along with 16 bytes of message. Sampling rate of DSO is set to 33 MSPS since clock of Arduino UNO operates at 16 MHz. It is observed that serial read, encryption and serial write operations on Arduino UNO approximately take 18 ms, hence, record length is set to 50 ms.

Figure 5: A picture of measurement campaign.

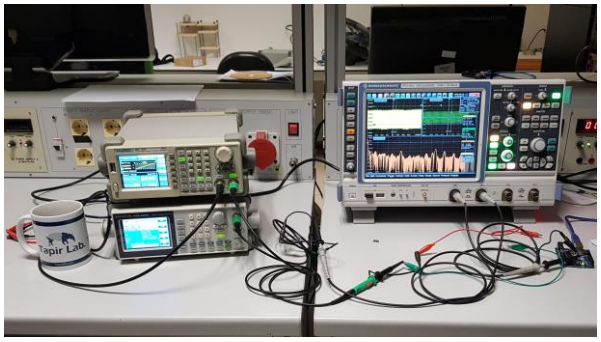

Figure 6: Signal generators and DSO used during measurements.

Measurements are taken under two different conditions. First, all the equipment in the laboratory except measurement devices are turned off. Secondly, square waves are generated to interfere with the power trace measurements. Peak-to-peak voltage, and duty cycle of square wave is set to 10 V and 50% respectively. Frequency is swept from 16 MHz to 20 MHz in one second. A differential probe is connected to output of signal generator to simulate daily operations in a research laboratory.

Table 1: List of equipment in measurement campaign.

Equipment	Brand	Model
DSO	Rohde & Schwarz	RTO 1044
Computer	ASUS	ROG G771JW
Signal Generator	AATech	AWG–1020
MCU	Arduino	Arduino UNO R3

6. RESULTS AND DISCUSSION

Time domain measurements of encryption process including serial read, 10 round AES, and serial write operations are given in Fig. 7 and Fig. 8 in logarithmic scale. In each figure, 17 bytes of serial read and write operations, and 10 rounds of AES encryption can be seen between them. AES algorithm is preferred due to the ease of implementation and easily distinguishable power consumption characteristics generated by S-boxes. Traces, which are defined as the region where calculations that we want to observe are carried on, are aligned by inspection for this study, however, trace alignment should be automated since extraction of the data buried into the noise might require hundreds of distinct measurements.

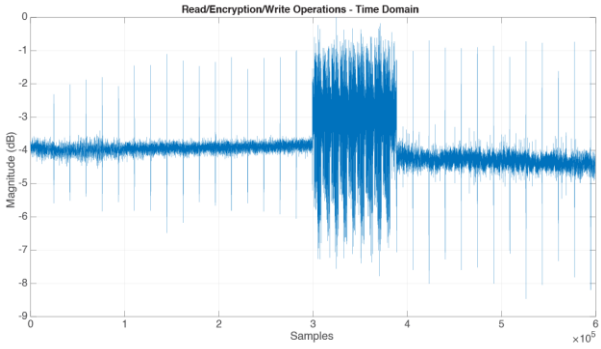

Figure 7: Trace in time domain (no interference)

Frequency domain representation of the trace when interference source is active is shown in Fig. 9. The frequency spectrum is estimated by normalizing traces in the time domain and taking 4096 points Fast Fourier Transform (FFT) in MATLAB. It can be seen that signal consists of several harmonics approximately separated by 0.5 MHz. One of the harmonics of the square wave sweeping from 16 MHz to 20 MHz in one second can be seen between 9 MHz and 10 MHz. Effect of this harmonic also can be seen in Fig. 11. When the signal generator is inactive, the power of the trace is calculated as 0.40 V, and when the signal generator is active power equals to 0.435 V. Also, mean power of 15 traces for no interference and with interference cases calculated as 0.40 V and 0.415 V respectively. These calculations indicate an increase in the noise figure when the interference source is on. Further analysis carried out and magnitude spectrum histograms of the power traces are given in Fig 10.

Figure 8: Trace in time domain: Interference source is active. Note the minuscule power level increase in comparison to Fig 7.

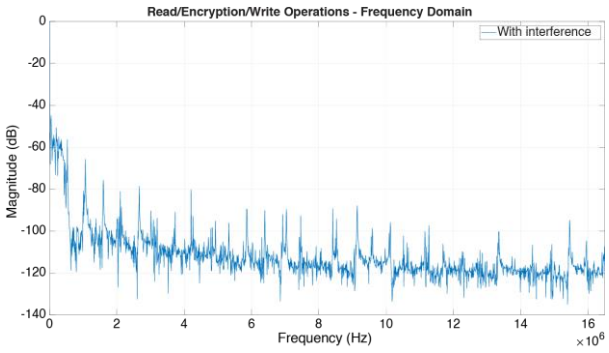

Figure 9: Magnitude spectrum of trace when interference source is on.

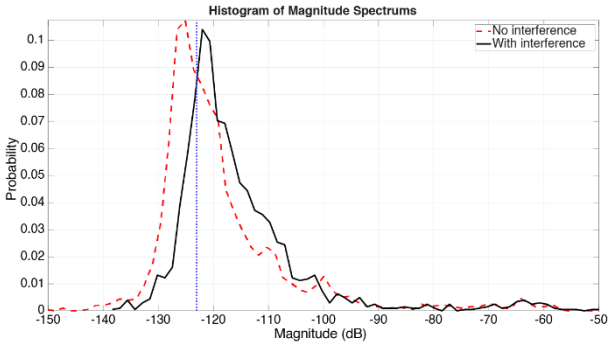

Figure 10: Histograms of magnitude spectrum of traces. Normalized to represent probability mass function

In Fig. 10, histograms of magnitude spectrum (power spectral density) of the traces are drawn together to understand how interference sources alter/perturb the measurements. These histograms are normalized so as to represent the probability mass function of power distribution on logarithmic scale. It can be seen that, when the interference source is active, the distribution of the magnitude spectrum is right-shifted. Therefore, we can deduce that the interference source pushes the noise figure to higher levels and results in degradation of SNR. This observation is also supported by the difference between the mean power of 15 clean and noisy traces. These results demonstrate the detrimental effects of interference sources in the vicinity of the measurement campaigns. Hence, in practical applications, a threshold indicated by a blue vertical dashed line as shown in Fig. 10 can be set to determine whether there exists some sort of device interfering with the measurements. If the mean of the magnitude spectrum histogram is higher than this threshold, then trace under analysis can be discarded due to the lowered SNR. To sum up, effect of the signal generator sweeping certain frequencies is presented along with a method to determine whether trace under analysis is affected by some sort of interfering device or not. Additionally, effects of the signal generator are shown on spectrograms in Fig. 11.

The spectrogram is the temporal visualization of the frequency components in a signal. It basically demonstrates the evolution in the power of harmonics as time passes by. In a spectrogram, the vertical axis represents time, the horizontal axis shows normalized frequency and color indicates the power of the harmonics at the corresponding time and frequency. In this study, spectrograms provide us to represent a better way to show the consequences of interference in the vicinity of the measurement campaign. In Fig. 11, spectrograms of two traces are presented. Windows size which represents the number of samples in each FFT chunk is set to 256 for these figures. In Fig. 11 (b), one of the fundamental harmonics of the sweeping square wave can be seen between 0.5 and 0.6 on the horizontal axis which approximately corresponds to 8 MHz and 10 MHz. Additionally, when we compare the two spectrograms, it can be seen that the power especially in the lower part of the spectrum is increased.

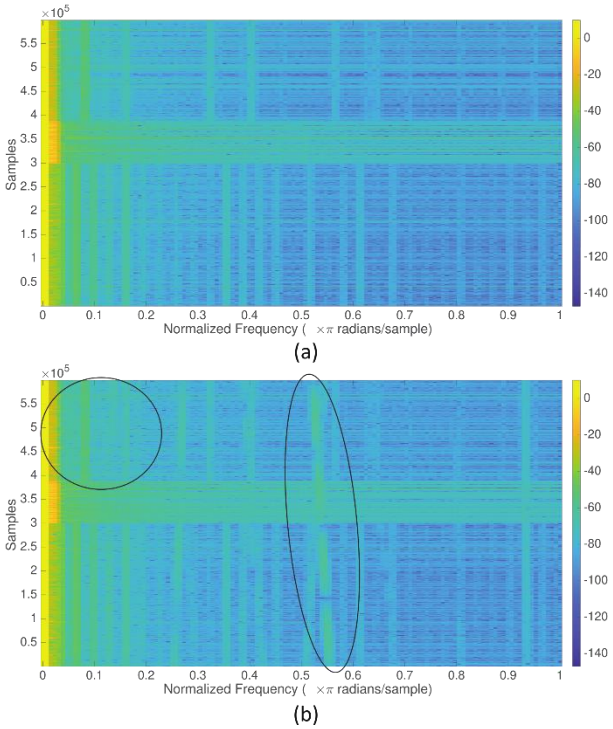

Figure 11: Trace spectrograms: (a) No interference, (b) With interference.

7. CONCLUSIONS AND FUTURE WORK

In this study, a basic measurement campaign to perform a power analysis SCA is presented. Additionally, ground loops, common board loops, and interference issues are presented along with possible solution methods. It is shown that measurement devices and DUA can be damaged if they are not grounded properly due to the current flowing through the ground path. Effects of interference are presented along with the data obtained using the proposed measurement environment. As stated in Section 2, the performance of the side-channel attacks and the number of traces required to obtain private key are inversely correlated with the SNR. Therefore, as emphasized in this study, the measurement environment should be isolated from any type of interference sources. To the best of the authors' knowledge, this study is one of the pioneers in the literature that covers measurement campaigns in such detail and shows the effect of interference sources in power analysis side-channel attacks. People neglect the effects of the interference in the power analysis side-channel attack since traces are obtained using an intrusive method. However, it is shown that measurement equipment might couple with the electromagnetic waves in the environment and introduces noise to the measurements. In the

upcoming studies, the effects of interference sources will be evaluated by conducting standard key extraction methods and measuring both the performance and number of traces required to obtain a private key. Additionally, an algorithm that can automatically align measurements will be proposed.

8. REFERENCES

[1] B. Che, C. Gao, R. Ma, X. Zheng, and W. Yang, "Covert wireless communication in multichannel systems," IEEE Wireless Communications Letters, vol. 11, no. 9, pp. 1790–1794, 2022.

[2] Z. Wang, X. Zhu, S. Jeloka, B. Cline, and W. D. Lu, "Physical unclonable function systems based on pattern transfer of fingerprint like patterns," IEEE Electron Device Letters, vol. 43, no. 4, pp. 655–658, 2022.

[3] W. Duo, M. Zhou, and A. Abusorrah, "A survey of cyber attacks on cyber physical systems: Recent advances and challenges," IEEE/CAA Journal of Automatica Sinica, vol. 9, no. 5, pp. 784–800, 2022.

[4] R. Yegireddi and R. K. Kumar, "A survey on conventional encryption algorithms of Cryptography," in 2016 International Conference on ICT in Business Industry & Government (ICTBIG). IEEE, 2016, pp. 1–4.

[5] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol. 21, no. 2, p. 120–126, feb 1978. [Online]. Available: https://doi.org/10.1145/359340.359342

[6] M. Randolph and W. Diehl, "Power sidechannel attack analysis: A review of 20 years of study for the layman," Cryptography, vol. 4, pp. 1–33, 6 2020.

[7] Y.-I. Hayashi, N. Homma, T. Mizuki, T. Aoki, H. Sone, L. Sauvage, and J.-L. Danger, "Analysis of Electromagnetic Information Leakage From Cryptographic Devices With Different Physical Structures," IEEE Transactions on Electromagnetic Compatibility, vol. 55, no. 3, pp. 571–580, jun 2013.

[8] T. Kim and Y. Shin, "Thermalbleed: A practical thermal side-channel attack," IEEE Access, vol. 10, pp. 1–1, 2022.

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

[10] P. C. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems," in Advances in Cryptology — CRYPTO '96, N. Koblitz, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1996, pp. 104–113.

[11] M. Jurecek, J. Bucek, and R. Lórencz, "Sidechannel attack on the a5/1 stream cipher," in 2019 22nd Euromicro Conference on Digital System Design (DSD), 2019, pp. 633–638.

[12] S. Ghandali, S. Ghandali, and S. Tehranipoor, "Deep k-tsvm: A novel profiled power sidechannel attack on aes-128," IEEE Access, vol. 9, pp. 136 448–136 458, 2021.

[13] N.-T. Do, V.-P. Hoang, and C.-K. Pham, "Low Complexity Correlation Power Analysis by Combining Power Trace Biasing and Correlation Distribution Techniques," IEEE Access, vol. 10, pp. 17 578–17 589, 2022.

[14] A. Jia, W. Yang, and G. Zhang, "Side channel leakage alignment based on longest common subsequence," in 2020 IEEE 14th International Conference on Big Data Science and Engineering (BigDataSE), 2020, pp. 130–137.

[15] P. Kashyap, F. Aydin, S. Potluri, P. D. Franzon, and A. Aysu, "2deep: Enhancing side-channel attacks on lattice-based key-exchange via 2-d deep learning," IEEE Transactions on Computer Aided Design of Integrated Circuits and Systems, vol. 40, no. 6, pp. 1217–1229, 2021.

[16] A. Calder, NIST Cybersecurity Framework - A PocketGuide. ITGovernancePublishing, 2018.

[17] ISO/IEC 17825:2016, "Information technology — security techniques — testing methods for the mitigation of non-invasive attack classes against cryptographic modules," 2016.

[18] FIPS 140-3, "Security requirements for cryptographic modules," 2019.

[19] A. G. Bayrak, F. Regazzoni, D. Novo, P. Brisk, F.-X. Standaert, and P. Ienne, "Automatic Application of Power Analysis Countermeasures," IEEE Transactions on Computers, vol. 64, no. 2, pp. 329–341, feb 2015.

[20] D. Das, M. Nath, B. Chatterjee, S. Ghosh, and S. Sen, "Stellar: A generic em side-channel attack protection through ground-up root-cause analysis," in 2019 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2019, pp. 11–20.

[21] R. Bodduna, V. Ganesan, P. SLPSK, K. Veezhinathan, and C. Rebeiro, "Brutus: Refuting the security claims of the cache timing randomization countermeasure proposed in ceaser," IEEE Computer Architecture Letters, vol. 19, no. 1, pp. 9–12, 2020.

[22] SCPI Consortium, "Standard commands for programmable instruments (scpi)," Available at https://www.ivifoundation.org/docs/ scpi-99.pdf (2022/09/18).

[23] C. O'Flynn and Z. D. Chen, "Chipwhisperer: An open-source platform for hardware embedded security research," in Constructive Side-Channel Analysis and Secure Design, E. Prouff, Ed. Cham: Springer International Publishing, 2014, pp. 243–260.