ACTA IMEKO
ISSN: 2221-870X
June 2023, Volume 12, Number 2, 1 - 6

The role of metrology in the cyber-security of embedded devices

Pasquale Arpaia[1,2,3], Francesco Caputo[1,2], Antonella Cioffi[1], Antonio Esposito[1,2]

[1] *Department of Electrical Engineering and Information Technology (DIETI), Università degli Studi di Napoli Federico II, Naples, Italy*
[2] *Augmented Reality for Health Monitoring Laboratory (ARHeMLab), Università degli Studi di Napoli Federico II, Naples, Italy*
[3] *Centro Interdipartimentale di Ricerca in Management Sanitario e Inno vazione in Sanità (CIRMIS), Università degli Studi di Napoli Federico II, Naples, Italy*

ABSTRACT
The cyber-security of an embedded device is a crucial issue especially in the Internet of Things (IoT) paradigm, since the physical accessibility to the smart transducers eases an attacker to eavesdrop the exchanged messages. In this manuscript, the role of metrology in improving the characterization and security testing of embedded devices is discussed in terms of vulnerability testing and robustness evaluation. The presented methods ensure an accurate assessment of the device's security by relying on statistical analysis and design of experiments. A particular focus is given on power analysis by means of a scatter attack. In this context, the metrological approach contributes to guaranteeing the confidentiality and integrity of the data exchanged by IoT transducers.

Section: RESEARCH PAPER

Keywords: Smart card; vulnerability assessment; side-channel attack; metrology

Citation: Pasquale Arpaia, Francesco Caputo, Antonella Cioffi, Antonio Esposito, The role of metrology in the cyber-security of embedded devices, Acta IMEKO, vol. 12, no. 2, article 8, June 2023, identifier: IMEKO-ACTA-12 (2023)-02-08

Section Editor: Paolo Carbone, University of Perugia, Italy

Received January 23, 2023; **In final form** January 23, 2023; **Published** June 2023

Funding: This work was supported by the "Programma Operativo Nazionale 2014-2020, Dottorati di ricerca su tematiche dell'innovazione e green, 10/08/2021 D.M. 10 agosto 2021, n. 1061, a.a. 2021/2022 - CICLO 37 – TEMATICHE GREEN (AZIONE IV.5)".

Corresponding author: Antonio Esposito, e-mail: antonio.esposito9@unina.it

1. INTRODUCTION

The progress in information and communication technology favoured the development of a new paradigm, known as Internet of Things (IoT) [1], [2]. This consists of distributed smart transducers that acquire data continuously and communicate with each other by wireless connection, so as to support everyday tasks and improve the quality of life [3]. These transducer networks concern a broad range of applications, such as environmental monitoring, smart power grids, transportation, healthcare, agriculture, and electronic payments [4]–[8].

Most of the IoT transducers are physically accessible, and this allows certain types of attacks and security breaches [9]. Indeed, an attacker can gain access to the network nodes in order to control them or to eavesdrop on exchanged messages. The security of the processed information should be typically guaranteed by encrypting messages through cryptographic algorithms [10], e.g., based on the well-known Advanced Encryption Standard (AES). Such an algorithm is implemented in the IoT transducer to encrypt the transmitted messages and decrypt the received ones. However, although mathematically safe, the implementation of these algorithms presents some vulnerabilities to side-channel attacks, namely attacks based on the measurement of physical quantities associated with the encryption/decryption operations [11]. Measured quantities may involve power consumption, electromagnetic emissions, execution time, light, or heat associated with device cryptographic operations. This side-channel information, also referred to as "leakages", can be exploited to discover the secret key of the cryptographic algorithm.

The side-channel attacks have been extensively studied by researchers and test laboratories for more than two decades. The attacks that have received most of the attention are based on the measurement of power consumption, which is dissipated by the embedded device during its operations. These are known as power analysis attacks and they were firstly introduced in 1999 by Kocher [12], who managed to break a public key cryptographic algorithm by measuring the power consumption of a device. Indeed, by exploiting the dependence between power

consumption and the internal state of the device during the execution of cryptographic operations, he was able to obtain information about the secret key being used. The implementation of this type of attack simply consists of two main phases: (i) the acquisition of power traces and (ii) a statistical analysis. With regard to the actual statistical analysis, different types of attacks can be distinguished: Simple Power Analysis, Differential Power Analysis [12], Correlation Power Analysis [13], and scatter analysis [14]. Moreover, machine learning-based approaches to data analysis are gaining more and more interest due to their capability of decoding patterns generated by complex systems [15]-[17].

In previous studies, many proposals concerned methods to improve the attack efficiency [18]–[20], techniques to make cryptographic algorithms robust against the power attacks [21]–[23], and tests aiming to evaluate the robustness of IoT devices with respect to the side-channel attacks. Broadly speaking, the appealing sensitive and personal information encourages the attackers, on the one hand, to break a cryptographic system in order to make profits. On the other hand, the security offered by such systems must be increased and tested in order to ensure confidentiality. Most cryptography papers present resource usages for breaking the cryptographic scheme analysed in function of the security parameters. This allows the system designers to choose the parameter values in order to make it more expensive to achieve a successful attack [24]. In this context, the rigor offered by metrology can contribute to the characterization of embedded and consumer-grade devices [25]. Notably, metrology has been recently allowing substantial progress in the field of information security of smart transducers thanks to a characterization of the AES vulnerability [26] or an evaluation of the robustness offered by countermeasures implemented in many devices [27].

The present work focuses on the role of metrology in improving security testing for embedded devices. In particular, results from previous works on the topic are recalled, integrated, and discussed. In detail, a vulnerability assessment will be presented by also providing some examples of enhanced power analysis attacks. Next, the discussion will move to robustness evaluation by means of design of experiments. The overall aim is to highlight the role that metrology can have in cyber-security. The paper is organized as follows. Section 2 introduces the instruments and the setup adopted to implement a power analysis scatter attack. Section 3 presents the results achieved thanks to the metrological approach to security testing. Conclusions are drawn in section 4 along with addressing future works.

2. MATERIALS AND METHODS

Power analysis attacks are side-channel attacks that exploit the variations in the power consumption of a cryptographic device to reveal the secret key [28]. In particular, the data-dependency and the operation dependency are exploited. The following subsections present a power analysis attack known as "scatter attack", the instruments adopted in power traces acquisition, and the measurement setup. Then, how to perform an optimized attack and security testing will be discussed in the next section with inherent results.

2.1. Scatter attack

The scatter attack was chosen to demonstrate the vulnerability of the AES. The attack was implemented against an IoT microcontroller (a.k.a. IoT device under test), secured by the

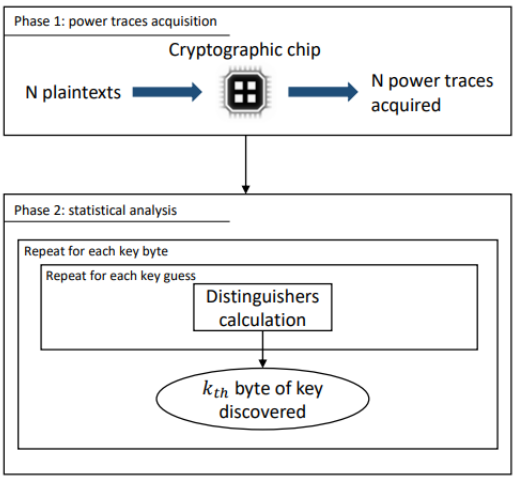

Figure 1. Flow diagram of a scatter attack.

AES cryptographic algorithm with a 16-bytes-long secret key, i.e., AES-128. The scatter attack consists of statistical analysis of several power traces, whose variations in amplitude are related to the value of the key. The attack implements a "divide-and-conquer" strategy by discovering a single byte of the key at a time. The workflow of the attack is shown in Figure 1. For each i_{th} byte of the key ($i \in [0, 15]$), a simple discriminant related to each key byte hypothesis k is obtained by means of a Pearson's chi-squared (χ^2) statistical test. When the key byte hypothesis is correct, the discriminant related to the real value should be characterized by the highest value with respect to other guesses. Therefore, high values in the discriminant maximizes the likelihood that the key byte hypothesis coincides with the secret key byte. The secret key is thus discovered by repeating the described procedure for all the key bytes.

For the implementation of the attack, a malicious measurement system is wired to the IoT microcontroller under test for monitoring the power consumption (power trace acquisition phase) during the encryption. The measured data of the power consumption are processed by a method of signature analysis (statistical analysis phase) in order to reveal the secret key of the AES-128 algorithm. For the advanced encryption standard, the portion of the power traces whose variations in amplitude are related to the key value is represented by the AddRoundKey and SubBytes steps of the first AES round. Indeed, the key expansion of the AES algorithm produces 10 round keys, the first of those generated coinciding with the secret key. Therefore, the first round employs the secret key in clear. Moreover, among the operations computed in the first round, the AES SBox output has a statistical influence on the power consumption [29].

2.2. Instruments

The device under test (DUT) was the ATMega-163, a low-power CMOS 8-bit microcontroller based on the AVR architecture, embedded on a smart card. The microcontroller presents 16 kB in-system flash, 512 bytes EEPROM, 1024 bytes Internal SRAM, and 8 MHz maximum clock, and implements the advanced encryption standard with a key of 128 bits. The cryptographic algorithm is implemented in software, and it does not include the side-channel countermeasures. The acquisition phase exploited the oscilloscope Teledyne Lecroy HDO9304, characterized by 3 GHz bandwidth, 40 GSa/s sample rate, and 8-bit analog-to-digital converter (ADC). A further hardware

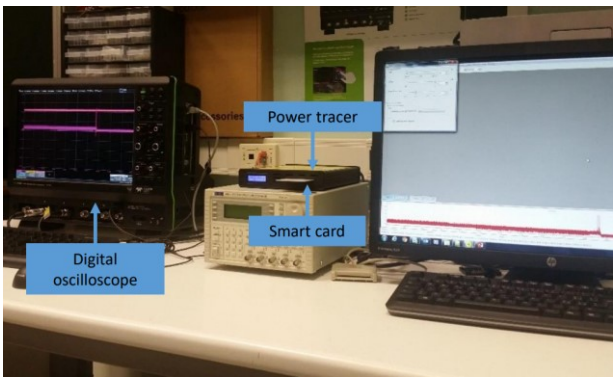

Figure 2. Instruments and devices for the scatter attack implementation.

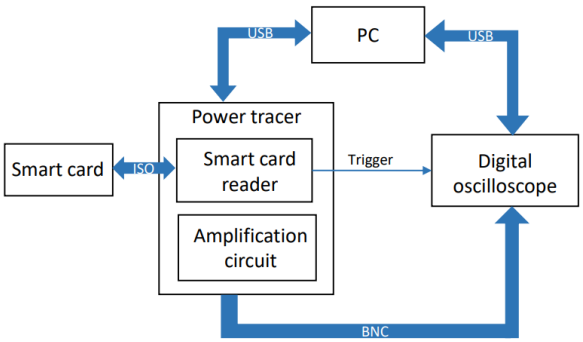

Figure 3. Block diagram of the measurement setup for power traces acquisition.

component, useful for the communication between the DUT and the oscilloscope, was employed. This component consisted of Power Tracer by Riscure [30], a low-noise card reader for side-channel power measurements with precise triggering capabilities. The Power Tracer supplies the integrated circuit on the smart card and communicates with it via ISO/IEC 7816-3 protocol. Moreover, it contains a low noise amplifier (26 pA/ $\sqrt{}$ Hz @ 1 MHz) with top end low-noise and high bandwidth analogue components that are electrically isolated from digital circuitry. Thanks to this circuitry, the Power Tracer provides the power consumption in output with a good signal-to-noise ratio. The capacitors inside the Power Tracer are pre-charged to power the smart card during each single measurement to avoid any external noise in the circuit. Typically, power consumption of contact smart cards is measured via a resistor inserted between the ground pin of a smart card and the ground of a card reader. The Power Tracer measured power consumption without measurement resistance in the power chain, thus allowing stable card voltage, maximum signal bandwidth, high sensitivity, and low insertion error [31]. An illustration of the instruments and devices used for the attack is shown in Figure 2.

2.3. Measurement setup

The block diagram of the measurement setup for power traces acquisition, is shown in Figure 3. A market-leading and professional tool, namely Inspector by Riscure, was installed on a personal computer. This sends the initial configuration parameters to the digital oscilloscope by means of a USB protocol. Moreover, the software communicates with the smart card through the Power Tracer. In particular, the PC provides the smart card reader with the plaintexts to be sent to the smart card in the APDU (Application Protocol Data Unit) format. Note that the APDU is a standard protocol, defined by ISO/IEC 7816-4, allowing the communication between a smart card reader and a smart card. In the communication between smart card and smart card reader, the Inspector tool on the PC appeared as the user interface of the card reader allowing to prepare the commands that will be physically sent by the reader to the smart card.

The smart card encrypts the message by using the AES-128 algorithm and returns the encrypted message to the PC by means of the smart card reader. The power tracer is also used to send a trigger signal to the oscilloscope by means of serial I/O line to synchronize the acquisition on the encryption. The oscilloscope acquires the power traces from the output signal of the power tracer, i.e., power consumption with an excellent signal-to-noise ratio. The sample data are sent to the PC by means of a USB interface. Before the oscilloscope acquires the power consumption, a BNC coaxial low pass filter (Mini Circuits BLP-50+, DC to 48 MHz, 50 Ω) cuts the signal frequencies over 48 MHz as they represent no significant information.

3. RESULTS

In this section, the results achieved by the adoption of the metrology in the security of embedded devices are reported. The discussion is conducted by analyzing the contributions in optimization of power analysis attack and of vulnerability assessment. The overall aim is to give some indications about the current state of metrology role for cybersecurity of embedded devices.

3.1. Optimization of power analysis attack

The success rate of the power attacks is significantly affected by the signal-to-noise ratio (SNR) of the power traces [19]. Techniques for noise reduction are particularly important when measuring power consumption because power analysis attacks are very sensitive to the magnitude of these signals to recover the value of the secret key. Therefore, it is important to eliminate noise effectively and improve the SNR of power traces to extract the secret key with minor effort. Indeed, a good level of signal to noise ratio involves in reducing the number of power traces needed to correctly reveal the secret key, and, consequently, in decreasing the time to perform a successful attack.

In [32], a filtering operation was employed in order to enhance the test attack effectiveness. The filter adopted is a low pass digital filter, which makes each sample a weighted average of the previous and the current sample. The improvement of the signal to noise ratio is also obtained by the decimation operation applied after an operation of oversampling. In fact, the decimation contributes to improving the signal to noise ratio by reducing the noise floor. An assessment is conducted to establish the best configuration for the filter weight. The experiment proved that the number of disclosed bytes by keeping the number of power tracks fixed increases according to the filter weight. Indeed, with 50000 power traces, a filter weight equal to 400 allows to discover the 16 bytes key while a weight of 300 returns only 15 bytes. Therefore, a filter weight equal to 400 was considered as the best configuration. The effectiveness of the enhanced scatter attack was proved experimentally in the best configuration by reducing the sample size of power traces. The Figure 4, shows the results. The number of bytes disclosed correctly are reported as a function of the number of power traces, where the filter weight is fixed to 400. The plot highlights that, with a filter weight of 400, a number of 30 000 power traces is sufficient to find the encryption key exactly. Contrarily, in absence of filtering operation, a successful attack needs 50 000

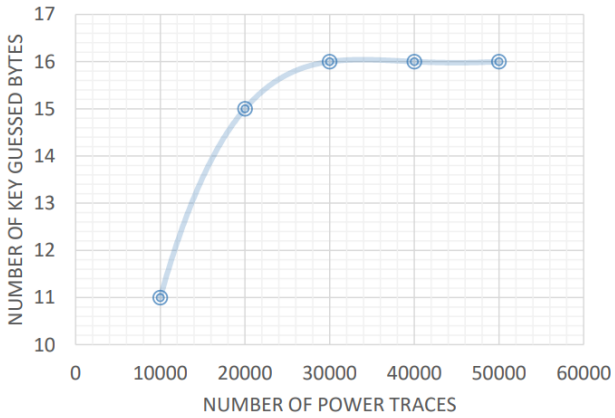

Figure 4. Number of bytes disclosed by the scatter attack as a function of the number of power traces for a weight of the filter equal to 400 (dotted line: 3rd-order polynomial interpolation).

power traces. Definitely, the use of a filter allows to discover the entire key unlike the lack of pre-processing with the same number of traces. Moreover, the filter is able to reduce the number of traces needed for a successful attack. Decreasing the number of power traces also reduces the time needed to find the secret key.

3.2. Vulnerability assessment enhancement

The Vulnerability Assessment allows us to evaluate the robustness and security of cryptographic devices with respect to "side-channel attacks". These consist in assessing the effort made to penetrate the device, quantified in terms of computational resources and time necessary for a potential attacker. A good as the robustness of a cryptographic device is important to guarantee, with greater reliability, the confidentiality and integrity of the data. A correct and reliable vulnerability assessment depends on a correct choice of the factors involved in the attack phases, such as sampling frequency, pre-processing techniques and number of traces acquired. Indeed, when the parameters are not optimal, an attack could require more effort to reveal the secret key, such as a higher number of traces to acquire and a longer time to reveal the secret key. This occurrence can distort the outcome of the vulnerability analysis.

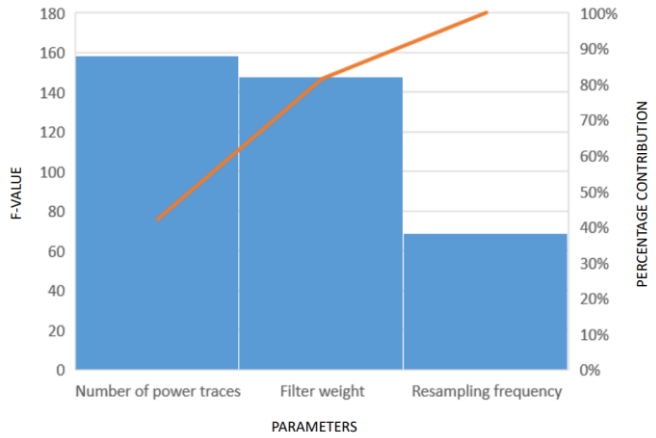

Figure 5. Pareto chart of the parameters: the histogram bars represent the F-values (left axis) and the orange line the cumulative percentage contributions (right axis).

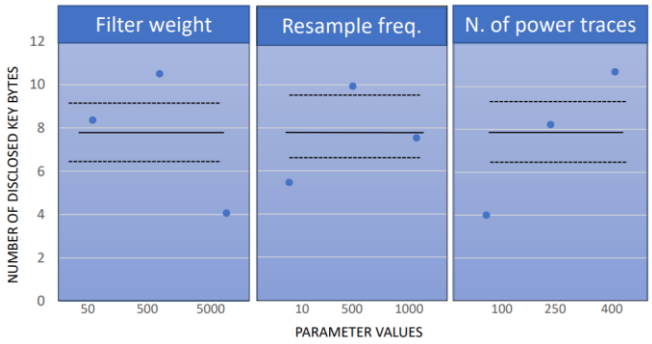

Figure 6. Plot summarizing the number of disclosed bytes in each experiment obtained with a fixed number of power traces and weight of the filter.

In recent years, metrology has been contributing to the world of cybersecurity in order to improve the characterization of devices in terms of security. In [26], the experimental design method was investigated to evaluate the factors affecting the attack system and to identify the values that maximize the number of bytes correctly identified with a minimum number of experimental tests. The attack system analysed in [26], consists of (i) the measurement devices used to acquire the power traces, (ii) the pre-processing techniques adopted to improve the power traces, and (iii) the statistical analysis of the scatter attack to discover the secret key of the AES-128 implemented in a smart card. The pre-processing techniques employed are a fast bidirectional filter to enhance the signal-to-noise ratio of the power traces and the resampling operation to reduce their dimensionality. The factors chosen for the analysis are the filter weight of the fast bidirectional filter, the resampling rate, and the number of power traces. For each parameter, 3 values are investigated. Therefore, a L9 orthogonal array is chosen for the experimental planning. Indeed, this design allows us to model a problem of 3 parameters and 3 values.

The experimental design method implemented for the attack system under analysis allows to identify the parameters that mostly influence the attack and the values that increase the number of correctly discovered bytes. The results of the statistical significance analysis are shown in the Pareto chart of Figure 5. The histogram bars report the F-value for each attack parameter, while the line represents the related percentage contribution. The bars presented in descending order highlight the number of power traces as the most important parameter among those considered. The Figure 6 exhibits the parameter value effects obtained by and the estimated error (for a confidence level of 99.97 %). In particular, each point is computed as the mean of the objective function values obtained for a fixed value of the factor analyzed. This plot allows to establish the best configuration for the attacking parameters able to maximize the disclosed key bytes. The best configuration for the case under analysis is 500 for the filter weight, 500 kSa/s for the resampling frequency, and 400 for the number of power traces.

3.3. Metric for robustness evaluation

The security of cryptographic algorithms with respect to power analysis attacks is improved by software and hardware countermeasures. Power analysis attacks success in discovering the secret key because the power consumption of cryptographic devices depends on intermediate values of the executed cryptographic algorithms. Therefore, the goal of power countermeasures is to make the power consumption of

cryptographic devices independent of the processed data. The countermeasures include hiding and masking techniques. The hiding countermeasures introduces variations of power consumption in the time domain or amplitude domain, while masking implements a data randomization by concealing each intermediate value. In [27], a method was proposed to assess the security performance among different power countermeasures designed to reinforce a software implementation of AES-128. Moreover, the method provides a metric to express the effectiveness of a countermeasure in straightening the IoT transducer security.

The method consists of conducting a power analysis attack at varying the security measures and in computing, for each combination of attack and countermeasure, the number of traces needed to discover the secret key. This parameter is typically used for assessing the countermeasure effectiveness. The more the countermeasure is effective, the more the number of traces increases. The calculation of the minimum number of power traces needed to succeed in the attack for each countermeasure is obtained as the mean of the minimum number of power traces obtained on N repetitions of the attack on different batches of power traces. A successive-approximation method in a range with extremes determined in a preliminary experimental campaign was adopted for the first repetition of the attack. The successive $N-1$ repetitions implement a grid search method with a variable step initialized to the minimum number of power traces found in the first repetition. The step is an increment of a certain number of power traces until the secret key is not fully recovered, and a decrement of an order of magnitude lower until the minimum number of power traces for a particular repetition is identified. The method employs the minimum numbers of power traces needed to discover the secret key obtained by each combination of attack and countermeasure to compute the strength factors (SFs). This parameter quantifies the level of protection for each countermeasure, and it is calculated as

$$SF_{C^*} = \frac{\sum_{i=1}^{N_A} \min_{A,C^*}}{\sum_{i=1}^{N_A} \min_{A,1}}, \quad (1)$$

where N_A is the number of implemented power attacks, min_{A,C^*} is the minimum number of power traces for a fixed countermeasure C^* at varying of the power attack, and $min_{A,1}$ is the minimum number of power traces for no-countermeasure at varying of the power attack.

The proposed method for the robustness evaluation of countermeasures was applied to a case study consisting of a software implementation of the AES-128 reinforced by countermeasures. The countermeasures under analysis are (i) random delay insertion, (ii) random SBox, and (iii) Boolean masking. Moreover, the configuration with no countermeasures was evaluated. The result of the analysis is reported in Table 1. Random delay strengthens the AES of a 1.3 factor with respect to no countermeasure condition; the strengthening factor for random SBox is 208, while more than 318 for masking. In case of masking, the non-availability of a minimum number of power traces does not allow to determine a strength factor value but only a low limit. The comparison of strength factors highlights masking as the most effective over other power countermeasures as it increases the number of power traces needed to succeed in the attack to a greater extent than the other countermeasure.

Table 1. Strength factor for each countermeasure

Countermeasures	Strength Factor (SF)
None	1
Random delay	1.3
Random SBox	208
Masking	> 318

4. CONCLUSIONS

In this work, the role of metrology to improve the characterization and security testing of embedded devices was discussed. This was done by recalling previous works focusing on vulnerability testing and robustness evaluation. Such results were recalled, integrated, and discussed. In detail, a method based on the design of experiments was presented to enhance the vulnerability assessment. Meanwhile, a metric was introduced to express the effectiveness of a countermeasure in straightening the IoT transducer security. Overall, the discussion suggests that metrology plays an important role in cyber-security, especially in a contest where IoT transducers are spread more and more, and their physical accessibility demands rigorous security testing. Future works will continue these investigations by extending the metrological approach to machine learning-based attacks. Indeed, these have great potential in security breaches, and they thus deserve further investigation.

REFERENCES

[1] L. Atzori, A. Iera, G. Morabito, The internet of things: A survey, Computer networks 54(15) (2010), pp. 2787–2805. DOI: 10.1016/j.comnet.2010.05.010

[2] I. Ahmed, E. Balestrieri, F. Lamonaca, IoMT-based biomedical measurement systems for healthcare monitoring: A review, Acta IMEKO 10(2) (2021), pp. 174-184. DOI: 10.21014/acta_imeko.v10i2.1080

[3] T. Yousuf, R. Mahmoud, F. Aloul, I. Zualkernan, Internet of things (iot) security: Current status, challenges and countermeasures, International Journal for Information Security Research (IJISR) 5(4) (2015), pp. 608–616. DOI: 10.1109/ICITST.2015.7412116

[4] W. T. Sung, S. J. Hsiao, The application of thermal comfort control based on smart house system of iot, Measurement 149 (2020), p. 106997. DOI: 10.1016/j.measurement.2019.106997

[5] F. Abate, M. Carratù, C. Liguori, V. Paciello, A low cost smart power meter for iot, Measurement 136 (2019), pp. 59–66. DOI: 10.1016/j.measurement.2018.12.069

[6] A. H. Alavi, P. Jiao, W. G. Buttlar, N. Lajnef, Internet of things-enabled smart cities: State-of-the-art and future trends, Measurement 129 (2018), pp. 589–606. DOI: 10.1016/j.measurement.2018.07.067

[7] J. Gutiérrez, J. F. Villa-Medina, A. Nieto-Garibay, an M. A. Porta-Gàndara, Automated irrigation system using a wireless sensor network and GPRS module, IEEE transactions on instrumentation and measurement 63(1) (2013), pp. 166–176. DOI: 10.1109/TIM.2013.2276487

[8] H. Ozkan, O. Ozhan, Y. Karadana, M. Gulcu, S. Macit, F. Husain, A portable wearable tele-ecg monitoring system, IEEE Transactions on Instrumentation and Measurement (2019). DOI: 10.1109/TIM.2019.2895484

[9] J. Deogirikar, A. Vidhate, Security attacks in IoT: A survey, in 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(ISMAC). IEEE (2017), pp. 32–37. DOI: 10.1109/I-SMAC.2017.8058363

[10] H. A. Abdul-Ghani, D. Konstantas, A comprehensive study of security and privacy guidelines, threats, and countermeasures: An iot perspective, Journal of Sensor and Actuator Networks 8(2) (2019), p. 22, 2019. DOI: 10.3390/jsan8020022

[11] F. X. Standaert, Introduction to side-channel attacks, in Secure integrated circuits and systems. Springer (2010), pp. 27–42.
DOI: 10.1007/978-0-387-71829-3_2

[12] P. Kocher, J. Jaffe, B. Jun, Differential power analysis, Proc. of the 19th Annual Int. Cryptology Conference "Advances in Cryptology - CRYPTO '99", Santa Barbara, California, USA, 15-19 August 1999, pp. 388–397.
DOI: 10.1007/3-540-48405-1_25

[13] E. Brier, C. Clavier, F. Olivier, Correlation power analysis with a leakage model, in International Workshop on Cryptographic Hardware and Embedded Systems. Springer (2004), pp. 16–29.
DOI: 10.1007/978-3-540-28632-5_2

[14] H. Thiebeauld, G. Gagnerot, A. Wurcker, C. Clavier, Scatter: A new dimension in side-channel, Int. Workshop on Constructive Side-Channel Analysis and Secure Design, Springer, (2018), pp. 135–152.

[15] T. Kubota, K. Yoshida, M. Shiozaki, T. Fujino, Deep learning side-channel attack against hardware implementations of AES, Microprocessors and Microsystems 87 (2021), p.103383.
DOI: 10.1016/j.micpro.2020.103383

[16] P. Arpaia, A. Esposito, A. Natalizio, M. Parvis, How to successfully classify EEG in motor imagery BCI: a metrological analysis of the state of the art, Journal of Neural Engineering (2022).
DOI: 10.1088/1741-2552/ac74e0

[17] M. K. Nanjundaswamy, A. A. Babu, S. Shet, N. Selvaraj, J. Kovelakuntla, Mitigation of spectrum sensing data falsification attack using multilayer perception in cognitive radio networks, Acta IMEKO 11(1) (2022), pp. 1-7.
DOI: 10.21014/acta_imeko.v11i1.1199

[18] Y. Kim, T. Sugawara, N. Homma, T. Aoki, A. Satoh, Biasing power traces to improve correlation power analysis attacks, in First international workshop on constructive side-channel analysis and secure design (cosade 2010). Citeseer (2010), pp. 77–80.

[19] W. Liu, L. Wu, X. Zhang, A. Wang, Wavelet-based noise reduction in power analysis attack, in 2014 Tenth International Conference on Computational Intelligence and Security. IEEE, (2014), pp. 405–409.
DOI: 10.1109/CIS.2014.103

[20] B. Hettwer, S. Gehrer, T. Guneysu, Profiled power analysis attacks using convolutional neural networks with domain knowledge, Proc. of the 25th International Conference "Selected Areas in Cryptography – SAC 2018", Calgary, AB, Canada, 15–17 August 2018, pp. 479–498.
DOI: 10.1007/978-3-030-10970-7_22

[21] G. B. Ratanpal, R. D. Williams, T. N. Blalock, An on-chip signal suppression countermeasure to power analysis attacks, IEEE Transactions on Dependable and Secure Computing, 1(3) (2004), pp. 179–189.
DOI: 10.1109/TDSC.2004.25

[22] T. Popp, S. Mangard, E. Oswald, Power analysis attacks and countermeasures, IEEE Design & test of Computers, 24(6) (2007), pp. 535–543.
DOI: 10.1109/MDT.2007.200

[23] C. Herbst, E. Oswald, S. Mangard, An AES smart card implementation resistant to power analysis attacks, Proc. of the 4th Int. Conf. on applied cryptography and network security ACNS 2006, Singapore, 6-9 June 2006, pp. 239–252.
DOI: 10.1007/11767480_16

[24] B. S. Yee, Security metrology and the Monty Hall problem, in Workshop on Information Security System Rating and Ranking (2001).

[25] P. Arpaia, L. Callegaro, A. Cultrera, A. Esposito, M. Ortolano, Metrological characterization of consumer-grade equipment for wearable brain–computer interfaces and extended reality, IEEE Transactions on Instrum. and Measurement 71 (2021), pp. 1-9.
DOI: 10.1109/TIM.2021.3127650

[26] P. Arpaia, F. Bonavolontà, A. Cioffi, N. Moccaldi, Reproducibility enhancement by optimized power analysis attacks in vulnerability assessment of iot transducers, IEEE Transactions on Instrum. and Measurement 70 (2021), pp. 1–8.
DOI: 10.1109/TIM.2021.3107610

[27] P. Arpaia, F. Bonavolontà, A. Cioffi, N. Moccaldi, Power measurement-based vulnerability assessment of IoT medical devices at varying countermeasures for cybersecurity, IEEE Transactions on Instrum. and Measurement 70 (2021), pp. 1–9.
DOI: 10.1109/TIM.2021.3088491

[28] S. Mangard, E. Oswald, T. Popp, Power analysis attacks: Revealing the secrets of smart card, Springer Science & Business Media 31 (2008)

[29] P. Kocher, J. Jaffe, B. Jun, P. Rohatgi, Introduction to differential power analysis, Journal of Cryptographic Engineering, 1(1) 2021, pp. 5–27.
DOI: 10.1007/s13389-011-0006-y

[30] Riscure inspector sca. Online [Accessed 11 March 2023].
https://www.riscure.com/securitytools/inspector-sca/

[31] M. Bucci, L. Giancane, R. Luzzi, M. Marino, G. Scotti, A. Trifiletti, Enhancing power analysis attacks against cryptographic devices, IET circuits, devices & systems 2(3) (2008), pp. 298–305.
DOI: 10.1049/iet-cds:20070166

[32] P. Arpaia, F. Bonavolontà, A. Cioffi, Problems of the advanced encryption standard in protecting internet of things sensor networks, Measurement 161 (2020), art. No. 107853.
DOI: 10.1016/j.measurement.2020.107853