A Review on Investigating On-chip Sensor based RPA Attack Vulnerabilities of Lightweight Cipher Algorithms

Bandara S. M. P. C.
Dept. of Computer Engineering
University of Peradeniya
Peradeniya, Sri Lanka
e17027@eng.pdn.ac.lk

Kumara W. M. E. S. K.
Dept. of Computer Engineering
University of Peradeniya
Peradeniya, Sri Lanka
e17176@eng.pdn.ac.lk

Nawarathna K. G. I. S.
Dept. of Computer Engineering
University of Peradeniya
Peradeniya, Sri Lanka
e17219@eng.pdn.ac.lk

Dr. Darshana Jayasinghe
Dept. of Electrical and Information Engineering
University of Sydney
Sydney, Australia
darshana.jayasinghe@gmail.com

Dr. Damayanthi Herath
Dept. of Computer Engineering
University of Peradeniya
Peradeniya, Sri Lanka
damayanthiherath@eng.pdn.ac.lk

Dr. Mahanama Wickramasinghe
Dept. of Computer Engineering
University of Peradeniya
Peradeniya, Sri Lanka
mahanamaw@eng.pdn.ac.lk

I. Introduction

Side channel attacks can be used in extracting sensitive information from cryptographic systems. These attacks exploit various factors such as power consumption, timing information, and defective computations to reveal the secrets of a cryptosystem. Correlation Power Analysis (CPA) [2] and Different Power Analysis (DPA) [1] are major side channel attacking techniques. They have been successfully executed across a wide range of devices, from small chips to complex systems characterized by noisy power measurements and intricate parallel operations.

The correlation factor between power consumption and the Hamming Distance plays a crucial role in side channel analysis, as there is an obvious relationship between power consumption and the Hamming Distance. Power consumption tends to increase when bits transition within transistors, resulting in higher power consumption compared to unchanged bits. By monitoring power measurements during cryptographic operations and considering the Hamming Distance for the process, there are ways to exploit side channel attacks. Understanding and analyzing this correlation factor allows for quantifying the degree of linear correlation and its implications for extracting sensitive information from side channels.

Cryptographic algorithms, such as Advanced Encryption Standard (AES), Elliptic Curve Cryptography (ECC), and RSA are found vulnerable to power analysis attacks despite being widely considered secure. Countermeasures to mitigate these attacks have been suggested, emphasizing the need for a combination of techniques to ensure the security of cryptographic systems.

FPGAs (Field-Programmable Gate Arrays) are reconfigurable hardware devices that allow for the implementation of digital circuits. Due to their flexibility and programmable nature, FPGAs are commonly used in various fields, including cryptography and security. The highly parallel nature of FPGA architectures, combined with their ability to perform rapid and precise operations, can inadvertently lead to unintended side channel leakage, which can be exploited to extract sensitive information. On-chip voltage sensors, such as Time-to-Digital Converters (TDC) [4], [16] and Ring Oscillator-based (RO) sensors [14], [15], are employed to monitor power fluctuations and detect potential voltage-related issues that can impact power consumption and circuit performance. The utilization of these sensors facilitates the extraction and transmission of internally-measured side channel leakages, enhancing the understanding of power consumption patterns within the system.

The concept of FPGA-based side channel attacks plays a vital role in different scenarios where these attacks can occur, including Intra-FPGA Attacks, Inter-chip Attacks, and Heterogeneous Chip Attacks [14]. The ability to execute side channel attacks without physical access or specialized equipment raises concerns regarding the security of multi-user FPGA environments and emphasizes the need for effective countermeasures.

Machine learning techniques have emerged as powerful tools in the context of CPA attacks. By leveraging the capabilities of machine learning algorithms, researchers have achieved notable success in extracting sensitive information from side channels. These techniques involve training models on a large dataset of power traces, enabling them to learn patterns and correlations between power consumption and the underlying data. Through machine learning algorithms, it is able to accurately predict secret information, even in complex cryptographic systems. The integration of machine learning with CPA attacks opens up new avenues for advancing the field of side channel analysis and underscores the importance of robust countermeasures to safeguard cryptographic systems against such attacks.

Low-performance devices, such as Internet of Things (IoT) devices, may employ cryptographic algorithms for various purposes. The utilization of lightweight ciphers like Simon [22] and PRESENT [21] is prevalent due to their efficiency on resource-constrained platforms. However, it is crucial to acknowledge the inherent vulnerability of IoT devices, as they often lack robust security measures. Given the susceptibility of lightweight ciphers to potential attacks, it becomes important to actively identify vulnerabilities within these cryptographic implementations. Consequently, appropriate countermeasures can be devised and implemented to mitigate the risks associated with these devices.

II. Literature Review

A. Power Analysis

The power consumed by a circuit is influenced by the activity of its individual components, including transistors. Consequently, when measuring the power usage of real-world computers or microchips, valuable insights can be gained regarding the operations and data being processed. Traditional cryptographic designs have operated under the assumption that secrets are manipulated within environments that provide no additional information beyond the specified inputs and outputs. However, the analysis of information leaked through power consumption and other side channels, with the aim of extracting secret keys from a diverse range of devices. These attacks are practical, non-invasive, and remarkably effective, even when targeting complex and noisy systems where cryptographic computations constitute only a small fraction of the overall power consumption [1].

Modern ciphers are specifically designed to withstand classical cryptanalysis techniques such as differential cryptanalysis [5] and linear cryptanalysis [6] which can exploit extremely small statistical characteristics in a cipher's inputs and outputs. However, it is important to note that the mentioned analysis primarily focuses on a specific aspect of a system's architecture: the mathematical structure of an algorithm.

It is crucial to recognize that even if a correct implementation incorporates robust algorithms and protocols, it does not guarantee complete security. Vulnerabilities can still emerge from other layers of the implementation [1]. In addition to the cryptographic algorithms themselves, other factors such as defective computations [7], [8] timing information [9] and invasive measuring techniques [10] can be used to reveal the secrets of the cryptosystem.

Side channel attacks have been successfully executed against a wide array of devices, encompassing implementations in ASICs, FPGAs and software-based systems [1]. These attacks have targeted a broad spectrum of targets, ranging from small single-purpose chips to intricate devices characterised by noisy power measurements and intricate parallel operations that obscure the underlying power consumption patterns. The versatility of side channel attacks highlights their potential applicability across diverse hardware and software platforms, therefore taking countermeasures against these attacks is a vital part of cryptographic systems.

The power consumption of an integrated circuit or a larger device is a reflection of the combined activity of its individual elements, as well as the electrical properties, such as capacitance, of the overall system [1]. This means that different operations within the circuit can consume varying amounts of power. For instance, a microprocessor might employ different circuits for performing additional operations compared to register loads, resulting in differing power consumption for these operations. Furthermore, the net power consumption is influenced by the specific transistors that are switching within the active circuits at any given time. The dynamic nature of power consumption highlights the complexity involved in analysing side channels and extracting meaningful information from them. Similar to this , it can be gathered that power consumption differs based on the data as well. This is the data-dependent power consumption.

B. CPA Attacks Based On Hamming Distance Model

In the realm of side channel attacks, several methods exist for revealing secrets. Two prominent techniques are Differential Power Analysis (DPA) [1] and leveraging the correlation factor between power consumption and the Hamming Weight of the data [11], [12]. However, this paper places specific emphasis on the application of the Hamming Distance and the leakage model. The utilisation of the Hamming Distance, as well as the leakage model, was initially introduced in a paper authored by Eric Brier, Christophe Clavier, and Francis Olivier [2]. This approach incorporates the use of CPA to identify the parameters of the leakage model. By employing CPA, the paper aims to further investigate the significance of the Hamming Distance and explore its effectiveness in extracting sensitive information.

Indeed, the Hamming Distance and Hamming Weight are closely related concepts in the context of binary sequences or strings. The Hamming Distance refers to the number of bit positions that differ or "flip" when transitioning from one state to another. It measures the dissimilarity or the number of changes required to transform one string into another. On the other hand, the Hamming Weight represents the count of '1' bits or the number of '1's present in the current state. For an example, consider the byte '00110011'. Here, the Hamming Weight is 4 since there are 4 '1's in it.

There is a relationship between the Hamming Distance and the Hamming Weight. If we consider the current state as an all-zero string, transitioning to the next state implies that the '1' bits are the positions where the bits have flipped. Therefore, the Hamming Weight in this case would precisely correspond to the number of bits that have changed or flipped, which is the same as the Hamming Distance.

In essence, the Hamming Distance can be seen as a generalisation of the Hamming Weight, as it takes into account both the bits that have changed ('1' bits) and those that have remained the same ('0' bits) when transitioning from one state to another.

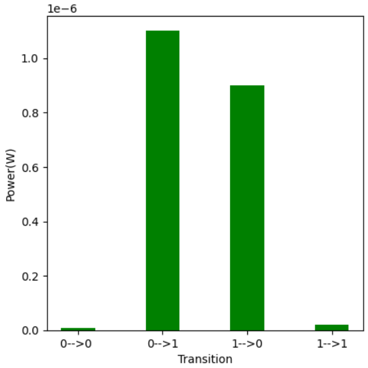

Fig. 1. Power Consumption When bits fipping.

As shown in Figure 1, Power consumption tends to increase when bits in transistors transition from '0' to '1' or '1' to '0'. These transitions involve the charging or discharging of capacitances, resulting in higher power consumption compared to when the bits remain unchanged [2].

By monitoring power measurements during cryptographic operations, it becomes possible to infer the transitions occurring within the device and deduce the Hamming Distance. The power variations observed during these transitions can be used as a side channel to extract information about the underlying data and potentially reveal secret keys.

Additionally, previous research papers have made certain assumptions and observations that support a linear relationship between the Hamming Distance and power consumption. These assumptions provide a foundation for understanding and analysing the leakage of information through power measurements [4]. The linear relationship assumption allows for the estimation of the Hamming Distance based on power measurements, facilitating the extraction of sensitive information using side channel analysis techniques [2], [3].

The correlation factor [2] is a crucial element when comparing the Hamming Distance with power consumption in side channel analysis. The correlation factor measures the strength and direction of the linear relationship between power consumption and the Hamming Distance. In the upcoming sections of the paper, a more detailed explanation of the correlation factor [2] and its significance in analysing the relationship between power consumption and the Hamming Distance will be provided. This exploration will shed light on how the correlation factor can be utilised to quantify the degree of linear correlation and its implications for extracting sensitive information from side channels. Correlation factor can be accurately estimated using the Pearson correlation coefficient, given by the following formula:

$$r = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \bar{x})^2 \sum_{i=1}^{n}(y_i - \bar{y})^2}}$$

C. *Ciphers which are found vulnerable against CPA*

Cryptographic algorithms serve as essential tools for safeguarding information and shielding it against unauthorized access and tampering. These algorithms employ intricate mathematical functions and operations to convert data into encrypted form, making it incomprehensible to anyone lacking the appropriate decryption key. They find application in diverse domains such as secure communication protocols, data storage, digital signatures, and authentication mechanisms. By delivering robust encryption and decryption capabilities, cryptographic algorithms ensure the confidentiality, integrity, and authenticity of sensitive information. However, certain popular cryptographic algorithms have been susceptible to side channel attacks employing the Correlation Power Analysis (CPA) technique. Notably, public key cryptographic algorithms like ECC, RSA, and private key cryptographic algorithms like AES have exhibited vulnerabilities against CPA attacks.

Power analysis techniques, while unable to directly determine secret keys, can provide valuable insights. Even though the secret key holds significant importance in most cryptographic algorithms, concealing the cryptographic algorithms used within a cryptographic system can enhance security. Kocher et al. [17] demonstrated how power analysis can gather useful information when the underlying architecture of the cryptographic system is unknown. In many proposed attacks, specific operations within cryptographic processes are targeted to execute CPA attacks. Owen et al. [18] focused on the substitution box operation of the AES-128 algorithm to launch a CPA attack and demonstrated the superior performance of this approach compared to the Differential Power Analysis (DPA) method. Despite the DPA method successfully identifying the correct key guess, the CPA approach provided a clearer visualization of the peak, unlike the noisy result obtained through DPA (This is called the Ghost Peak problem of DPA).

Researchers in [13] have investigated existing side channel attacks against commonly used cryptographic algorithms, namely AES, ECC, and RSA. They also explored countermeasures to mitigate these attacks. Surprisingly, all three algorithms, widely considered secure, were found vulnerable to CPA and DPA attacks. No single countermeasure proved effective in preventing these attacks. Instead, a combination of several countermeasure techniques is necessary to ensure the security of a cryptographic system against side channel attacks. Thus, it is essential to examine vulnerabilities against CPA attacks in other ciphers employed across various domains where information confidentiality is of utmost importance. Finding those vulnerabilities will be helpful for proposing countermeasures against those attacks [3].

According to Tawalbeh et al. [13], their comprehensive review on countermeasures for ciphers against side channel attacks highlighted a significant number of proposed countermeasures. One such technique is Noise Injection [23], which aims to prevent attackers from extracting useful information by analyzing the power consumption of a cryptographic device. This method involves injecting random noise during crypto-

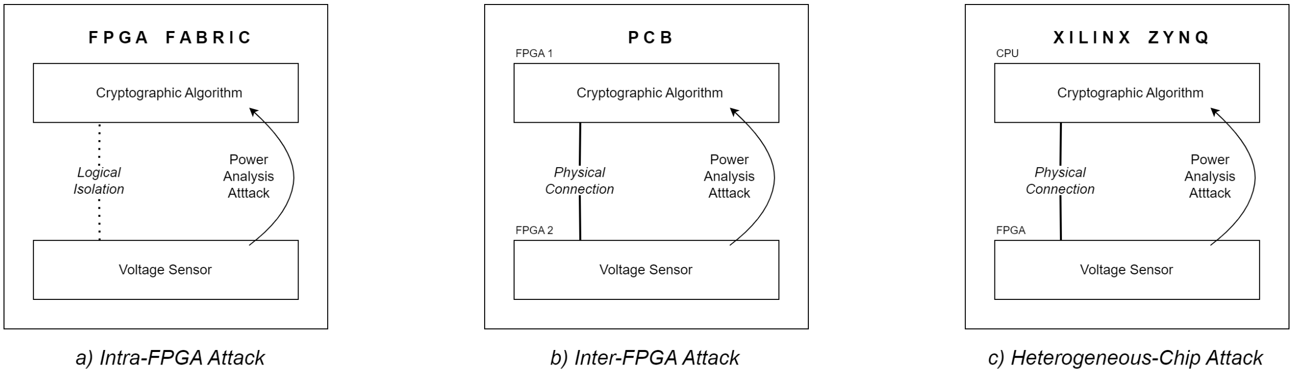

Fig. 2. Overview of FPGA-based Power Side Channel Exploits

graphic operations to disrupt the leakage of side channel information. Another existing method is Instruction Injection [24], which distorts side channel leakage by randomly injecting a number of instructions at various points in the cryptographic algorithm. These injected instructions do not affect the flow or results of the cipher. It is important to note that most of the existing countermeasures have been proposed for ciphers such as AES, ECC, and RSA

D. On-chip Sensors for Power Analysis

One of the key types of on-chip sensors is the voltage sensor, which monitors voltage levels at various points on the chip, allowing for the detection of potential voltage-related issues that can impact power consumption and circuit performance.

Additionally, there have been advancements in the development of internal sensors utilizing FPGA primitives. These sensors facilitate the extraction and transmission of internally-measured side channel leakages. Specifically, calibrated delay sensors that are distributed throughout the system are employed to indirectly gauge voltage fluctuations resulting from power consumption [4].

Over the past few years, FPGAs have gained significant popularity in cloud data centers and System-on-Chip applications for hardware acceleration [14]. While logical isolation is typically implemented to safeguard each tenant, the use of multi-user FPGA environments raises important concerns regarding potential security threats. Recently, a series of research papers have demonstrated that a malicious user, utilizing their rented logic, could potentially launch remote Side Channel Attacks on other users' assets within the fabric or neighboring chips [14].

Unlike traditional hardware attacks, software-induced hardware attacks do not require physical access or specialized equipment like probes and oscilloscopes. These attacks leverage the resources provided by the targeted devices and can be executed from any location and at any time through a network connection. To estimate the voltage fluctuation within the fabric, various techniques can be employed, such as designing Propagation Delay Sensors like RO based sensors or on-chip sensors utilizing TDC.

The utilization of FPGA-based power analysis intensifies the risk posed by Side Channel Attacks, eliminating the need for direct physical access to the target system or specialized equipment. Past instances of FPGA-based Side Channel Attacks have been executed across three distinct scenarios [14] (Refer the Figure 2 for an overview of the scenarios):

- ***Intra-FPGA Attack***: In the adversary model, multiple users share an FPGA fabric, with each user being individually protected from the others through logical isolation. To monitor voltage fluctuations caused by neighboring computations, a malicious user has the ability to incorporate voltage sensors into their rented logic.
- ***Inter-Chip Attack***: Through the Power Distribution Network (PDN), an untrusted chip embedded within a PCB has the capability to detect voltage fluctuations caused by other chips. In this particular exploit, an adversarial FPGA fabric can execute a CPA attack on an AES module and an SPA attack on an RSA module, both of which are operating on a separate FPGA fabric.
- ***Heterogeneous Chip Attack***: In certain technological advancements, a System-on-Chip (SoC) combines a processor and an FPGA fabric. Within this configuration, malevolent on-chip sensors are incorporated into the FPGA fabric with the intention of executing a Side Channel Power Analysis (SPA) on the program operating within the CPU core.

Reconfigurable logic mechanisms exist to facilitate the monitoring of voltage variations or fluctuations within FPGAs, spanning from their source to the point of measurement. These fluctuations in the power supply within a chip are primarily caused by the switching activity of its transistors.

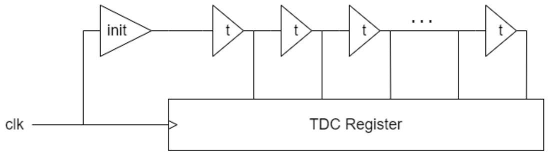

Fig. 3. Functional Schematic of TDC Sensor.

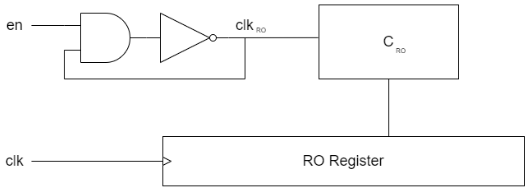

Fig. 4. Functional Schematic RO Sensor.

Accurate estimation of the internal power supply voltage of a chip can be achieved by measuring the propagation delays of logic gates. Two commonly employed sensors for power monitoring are the RO-based sensor (based on Ring Oscillators) and the TDC-based sensor (based on Time-to-Digital Converters) [14].

- ***Time-To-Digital Converter***: This transforms timing variances caused by power supply fluctuations into digital data, offering a cost-effective design with a high level of precision. Figure 3 shows the functional schematic of the TDC Sensor.
- ***Ring Oscillator based Sensor***: By measuring the oscillation frequency of its Ring Oscillator (RO), this effectively monitors variations in propagation delay. A Ring Oscillator is a configuration consisting of an odd number of inverters connected in series. Figure 4 shows the functional schematic of the RO Sensor.

E. Machine Learning on Side Channel Attacks

Machine learning techniques are commonly employed to extract useful information and identify patterns from a given dataset. In addition to the statistical analysis techniques typically used in side channel attacks, researchers have also explored the application of machine learning techniques in this context. One of the strategies utilized in side channel attacks is the divide-and-conquer strategy, which involves breaking down the key recovery problem into several subproblems. Each of these subproblems can be treated as a classification problem, aiming to classify a given power trace based on possible subkeys. In their work, the authors of [19] demonstrated the use of the Least Square Support Vector Machines (LS-SVMs) [20] learning algorithm to conduct a side channel attack on the AES cipher without employing any countermeasures. However, their results indicate that the LS-SVM classifier and the traditional statistical method they used for comparison yield somewhat similar outcomes.

In recent years, profiled side channel attacks, such as Template attacks, have gained popularity. However, due to their reliance on unrealistic assumptions, novel profiling methods incorporating machine learning and deep learning have emerged. These approaches offer advantages when targeting cryptographic implementations, both unprotected and protected [25]. Machine learning techniques like Support Vector Machine (SVM) [26] and Random Forest (RF) [27], as well as deep learning techniques, employ a two-phase approach consisting of training and attack phases to construct a profiling model. The deep learning technique proposed in [25] distinguishes itself from the machine learning approach primarily through the method employed for data profiling.

The latest progress in deep learning for side channel attacks has prioritized the development of novel techniques aimed at enhancing the accuracy and robustness of such attacks. For instance, the authors of [28] proposed several new techniques for improving the accuracy of deep learning-based side channel attacks. The lack of correlation between accuracy, commonly used in machine learning, and established SCA metrics like Guessing entropy or key-discrimination success rate has been questioned. The paper establishes that minimizing the Negative Log Likelihood (NLL) [29] loss function during deep neural network training is asymptotically equivalent to maximizing the Perceived Information (PI) [30], which serves as a lower bound for the Mutual Information between the leakage and the target secret. This gives more relevant estimations of the mutual information between a sensitive variable and the corresponding power trace.

References

[1] P. Kocher, J. Jaffe, B. Jun and P. Rohatgi, ”Introduction to differential power analysis”, J. Cryptograph. Eng., vol. 1, no. 1, 2011.

[2] Brier, E., Clavier, C., Olivier, F., ”Correlation power analysis with a leakage model”, Cryptographic Hardware and Embedded Systems–CHES, Lecture Notes in Computer Science, vol. 3156, Springer, Berlin, 2004.

[3] Biryukov, A., Dinu, D., Großschädl, J., ”Correlation power analysis of lightweight block ciphers: from theory to practice”, ACNS 2016. LNCS, vol. 9696, Springer, Heidelberg, 2016.

[4] F. Schellenberg, D. R. E. Gnad, A. Moradi and M. B. Tahoori, ”An inside job: Remote power analysis attacks on FPGAs”, Proc. Design Autom. Test Eur. Conf. Exhibit. (DATE), pp. 1111-1116, Mar. 2018.

[5] Biham, E., Shamir, A., ”Differential Cryptanalysis of DES-like Cryptosystems”, CRYPTO, Lec-ture Notes in Computer Science, vol. 537, pp. 2–21. Springer,Berlin, 1990.

[6] Matsui, M., Yamagishi, A., ”A new method for known plaintext attack of FEAL Cipher”, EUROCRYPT, pp. 81–91, 1992.

[7] Boneh, D., DeMillo, R. A., Lipton, R.J., ”On the importance of checking cryptographic protocols for faults (extended abstract)”, EUROCRYPT, pp. 37–51, 1997.

[8] Biham, E., Shamir, A., ”Differential fault analysis of secret key cryptosystems”, CRYPTO, Lecture Notes In Computer Science, vol. 1294, pp. 513–525. Springer, Berlin, 1997.

[9] Kocher, P.C., ”Timing Attacks on Implementations of Dif-fie-Hellman, RSA, DSS, and Other Systems”, CRYPTO, Lecture Notes in Computer Science, vol.1109, pp. 104–113. Springer, Berlin, 1996.

[10] Anderson, R., Kuhn, M., ”Tamper resistance—a caution-ary note”, Second Usenix Workshop on Smart Card Technol-ogy1, 1, 1996.

[11] J.-S. Coron, P. Kocher, D. Naccache, ”Statistics and secret leakage”, InFinan-cial Cryptography (FC 2000), LNCS 1972, pp. 157–173, Springer-Verlag, 2001.

[12] R. Mayer-Sommer, ”Smartly analysing the simplicity and the power of simple power analysis on smartcards”, Cryptographic Hardware and Embedded Systems— CHES 2000. LNCS 1965, pp. 78–92, Springer-Verlag, 2000.

[13] Lo’ai A. Tawalbeh, Hilal Houssain, Turki F. Al-Somani, “Review of Side Channel Attacks and Countermeasures on ECC, RSA, and AES Cryptosystems”,journal of Internet Technology and Secured Transactions (JITST), Volume 5, Issues 3/4, September/December 2016.

[14] J. Gravellier, J.-M. Dutertre, Y. Teglia and P. Loubet-Moundi, ”High-speed ring oscillator based sensors for remote side-channel attacks on fpgas”, International Conference on ReConFigurable Computing and FPGAs (ReConFig), 2019.

[15] Kenneth M. Zick, John P. Hayes, ”Low-cost sensing with ring oscillator arrays for healthier reconfigurable systems”, ACM Transactions on Reconfigurable Technology and Systems, 5(1):1–26, 2012.

[16] Kenneth M. Zick, Meeta Srivastav, Wei Zhang, Matthew French, ”Sensing nanosecond-scale voltage attacks and natural transients in FPGAs”, Proceedings of the ACM/SIGDA international symposium on Field programmable gate arrays, 2013.

[17] Kocher P, Jaffe J, Jun B, ”Differential power analysis”, Wiener M, editor. Advances in cryptology - CRYPTO’99: 19th annual international cryptology conference; Aug 15–19;Santa Barbara (CA). Berlin: Springer; 1999.

[18] Lo O, Buchanan WJ, Carson D, ”Power analysis attacks on the AES-128 S-box using differential power analysis (DPA) and correlation power analysis (CPA)”, J Cyber Secur Technol, 2016.

[19] G. Hospodar, B. Gierlichs, E. De Mulder, I. Verbauwhede, J. Vandewalle, “Machine learning in side-channel analysis: a first study”, Journal of Cryptographic Engineering, 2011.

[20] Suykens, J., Gestel, T.V., Brabanter, J.D., Moor, B.D., Vandewalle,J. ”Least Squares Support Vector Machines”, World Scientific, Singapore, 2002.

[21] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. Robshaw, et al., ”PRESENT: An Ultra-lightweight Block Cipher” in Cryptographic Hardware and Embedded Systems, Berling, Germany:Springer, 2007.

[22] Beaulieu R, Shors D, Smith J, Treatman-Clark S, Weeks B, Wingers L., ”The SIMON and SPECK families of lightweight block ciphers”, cryptology eprint archive, 2013.

[23] Das, D., Maity, S., Nasir, S.B., Ghosh, S., Raychowdhury, A. and Sen, S., ”High efficiency power side-channel attack immunity using noise injection in attenuated signature domain”, In 2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST) (pp. 62-67). IEEE, 2017.

[24] Ambrose, J.A., Ragel, R.G. and Parameswaran, S., ”Randomized instruction injection to counter power analysis attacks”, ACM Transactions on Embedded Computing Systems (TECS), 11(3), pp.1-28, 2012.

[25] H. Maghrebi, T. Portigliatti and E. Prouff, ”Breaking cryptographic implementations using deep learning techniques”, Proc. Int. Conf. Security Privacy Appl. Cryptography Eng., pp. 3-26, 2016.

[26] Cortes, C., Vapnik, V. ”Support-vector networks. Mach. Learn.” 20, 273–297, 1995.

[27] Breiman, L., ”Random forests. Mach. Learn.”, 2001.

[28] Loïc Masure, Cécile Dumas, and Emmanuel Prouff., ”A comprehensive study of deep learning for side-channel analysis”, IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020.

[29] E. Cagli, C. Dumas and E. Prouff, ”Convolutional neural networks with data augmentation against jitter-based countermeasures”, Proc. Int. Conf. Cryptogr. Hardw. Embedded Syst., pp. 45-68, 2017.

[30] Renauld, M., Standaert, F.-X., Veyrat-Charvillon, N., Kamel, D., Flandre, D. ”A formal study of power variability issues and side-channel attacks for nanoscale devices”, Paterson, K.G. (ed.) EUROCRYPT 2011, 2011.