A Survey of Power and Electromagnetic-Based Side-Channel Attack Countermeasures

Robert Kramer, Mark Reith, Wayne Henry and Anthony Rose
Air Force Institute of Technology, Wright-Patterson Air Force Base, USA

robert.kramer.10@us.af.mil
mark.reith.3@us.af.mil
wayne.henry@us.af.mil
anthony.rose.3@us.af.mil

Abstract: Cryptography is a cornerstone of modern computing security, but it remains vulnerable to Side-Channel Attacks (SCAs), which exploit hardware implementations to compromise encryption. SCAs pose significant cybersecurity risks by extracting sensitive information, such as encryption keys, through passive observation of side-channel leakage or active manipulation of system operations. This paper reviews non-invasive power and EM-based SCAs, evaluates the effectiveness and limitations of existing countermeasures, and identifies gaps that warrant further research. The analysis aims to guide the development of robust defenses and inform future efforts to secure cryptographic systems against evolving threats.

Keywords: Side-Channel attack, Power analysis, Electromagnetic analysis, Cryptography, Countermeasures

1. Introduction

Cryptographic systems play a vital role in protecting sensitive data. Researchers have developed numerous methods and algorithms to secure data; however, these systems are not impervious to attack. Piessens et al (2024) describe Side-Channel Attacks (SCAs) as attacks that exploit the physical and operational implementation of these cryptographic methods by observing different side-channel leakage, such as power and timing, posing a significant threat to data security. An infamous example of SCA exploitation is the Spectre and Meltdown attacks. These attacks implemented SCAs to recover encrypted data and could hack practically all Intel x86 microprocessors, IBM Power processors, and AMD processors as noted by Abu-Ghazaleh et al (2019).

The primary objectives of this survey are to consolidate existing research on power and electromagnetic (EM) based SCA countermeasures, compare these countermeasures to identify strengths and weaknesses, and promote discussion on countermeasures as a whole. Lastly, we identify areas for future research based on these findings. Understanding these attacks and their defenses is essential for enhancing the security of cryptographic systems as threats adapt and evolve.

The structure of this paper is as follows: Section 2 discusses the scope of research and Section 3 provides a background of power-based SCAs and EM-based SCAs. Section 4 examines a range of countermeasures developed for power-based SCAs and EM-based SCAs. Section 5 presents a comparative analysis of the countermeasures and Section 6 provides suggestions for future research. Lastly, Section 7 concludes the survey.

2. Scope of Research

The background section covers power and EM-based SCAs because they are both passive, non-invasive SCA methods and there is an inherent relationship between power and EM radiation. Providing a background on the numerous types of SCAs is implausible and outside the scope of this paper. In this survey, countermeasures refer to methods that detect or prevent SCAs. The countermeasures discussed are representative of a much broader range of techniques. A comprehensive survey of all countermeasures is impractical, so this paper aims to promote discussion to improve future development.

3. Background

3.1 Power-Based Side-Channel Attacks

Two simple facts about conventional computers are that they require power and use ones and zeros. Power-based SCAs (P-SCAs) exploit these facts. Ones and zeros are stored in transistors which are modified by either applying power or removing power. When a system performs an operation, it changes these ones and zeros based on the operations, so the resulting overall power of the system fluctuates (Gupta et al, 2019; Zadeh et al, 2012). This fluctuation is visible on a graph as a function of power and time on an oscilloscope. P-SCAs require the attacker to have physical access to the system to accurately measure the slight power changes that occur. There are various types of P-SCAs; however, this survey focuses on Simple Power Analysis (SPA), Differential

Power Analysis (DPA), and Correlation Power Analysis (CPA) attacks because they are the most prevalent as described in Taouil et al (2021).

3.1.1 Simple power analysis

SPA is considered the most basic type of P-SCA due to its simplicity. It attempts to retrieve the key based on passive observations of power changes. The power changes are measured by an oscilloscope with the probes placed near the cryptographic processor. Detection by the target system is difficult because of its non-invasive nature. The attacker then runs the cryptographic algorithm and measures the power fluctuation, resulting in an output known as a trace. Comparing the power fluctuations to the cryptographic operations can provide the attacker with information on what operations were performed and when. Using this information, the encryption key can be deduced. A limitation of this type of attack is that it requires basic knowledge of the encryption algorithm in order to analyze the trace; however, many commonly used encryption algorithms are publicly available, so the operations are not difficult to find (Zadeh et al, 2013; Mayer-Sommer, 2000). A famous example of this was an attack against the Rivest-Shamir-Adleman (RSA) encryption, which uses square and multiply operations to encrypt. Because the attacker knew RSA uses square and multiply operations, the attacker was able to deduce the encryption key based on the power fluctuations (Diehl, 2020).

3.1.2 Differential power analysis

DPA is more complex than SPA because it relies on creating statistical models of power consumption to compare with actual power consumption in order to reduce noise; however, it does not require prior knowledge of the system (Diehl, 2020; Duan et al, 2016; Martinasek, et al 2013). To create a statistical model, the attacker measures thousands of traces against different inputs and the same key, then divides them into two classes based on the output of a single pre-determined bit. Generally, the more traces, the higher the chance of key recovery. Using statistical analysis, the difference in means between the two classes can be calculated using a graph, allowing the attacker to infer subkeys, 8 bits, of the encryption key and, subsequently, the entire encryption key (Zadeh et al, 2013).

3.1.3 Correlation power analysis

CPA is similar to DPA as it also creates statistical models to deduce the encryption key and having more traces increases the chance of key recovery. However, while DPA looks at the difference in means, CPA looks for a high correlation coefficient between the hypothesized and measured power consumption (Kang et al, 2015; Kundrata et al, 2020). The traces display high correlation visually as spikes for the correctly guessed subkeys in the generated graphs. Once the attacker has verified the subkey for each part of the key, they are able to piece together the full encryption key as described in Safta et al (2016) and Damian et al (2017).

3.2 Electromagnetic-Based Side-Channel Attacks

EM-Based SCAs (EM-SCAs) operate on the same principles as P-SCAs, except instead of exploiting power consumption, the attacker exploits the EM field radiated by the target system. These fields are generated during data processing and operations as a result of changes in current and power. EM-SCAs use oscilloscopes and spectrum analyzers, but instead of attaching power probes directly to the target system like a P-SCA, a single EM probe is positioned above the system to measure the EM field.

Common types of EM-SCAs are Simple EM Analysis (SEMA), Differential EM Analysis (DEMA), and Correlation EM Analysis (CEMA) attacks (Das et al, 2023). SEMA, DEMA, and CEMA all use the same principles as their P-SCA counterparts. SEMA directly analyzes the EM emissions using a spectrum analyzer to infer the encryption key. DEMA uses statistical analysis to compare measured EM emissions and hypothetical models to reveal the encryption key using difference of means analysis. CEMA calculates the correlation coefficient between measured EM emissions and hypothetical models to deduce the encryption key (Zhou et al, 2019; Hatun et al, 2019; Montminy et al, 2013).

Table 1 provides a concise comparison of the discussed SCAs based on technique used.

Table 1: Types of Side-Channel Attacks

Attack Type	Technique
SPA	Direct observation of power
DPA	Statistical analysis using difference of means
CPA	Statistical analysis using correlation coefficients
SEMA	Direct analysis of EM radiation
DEMA	Statistical analysis using difference of means
CEMA	Statistical analysis using correlation coefficients

4. Countermeasures

This section covers countermeasures for P-SCAs and EM-SCAs. Some of the countermeasures are designed specifically for P-SCA or EM-SCA while some are designed for both due to the inherit relationship between power and EM radiation.

4.1 Shuffling

Shuffling is a common SCA countermeasure method. This specific implementation of shuffling proposed by Nozaki et al (2021) was designed to prevent Model Extraction P-SCAs. Model Extraction P-SCAs are used against multi-layer perceptron (MLP), a type of Neural Network. Model Extraction P-SCAs use CPA to exploit the multiplication operations done in an MLP to recreate the model for themselves by comparing power consumption to the Hamming weight (HW) of registers during a calculation. This implementation shuffles the multiplication operation order to prevent modeling extraction. This randomizes the power fluctuations so that the correlation between power consumption and HW of registers is weaker. Nozaki et al (2021) tested this countermeasure and successfully prevented the attacker from extracting the MLP model after 1,000 traces.

4.2 Machine Learning On-Chip Security Network

The basic concept presented in Kenarangi et al (2019) is to create a machine learning (ML) integrated circuit (IC) to develop an on-chip security network. The ML model detects voltage variations across the device and predicts its security level using a network of integrated sensors. Researchers trained the ML IC security network with an external probe connected to the power delivery network (PDN) to simulate a compromised system and without a probe to simulate a secure system. The ML IC security network compares the voltage levels of the secure system and the compromised system. When simulated against a P-SCA, the ML IC security network detected differences up to 50 millivolts. In a simulation against a DC-shifted P-SCA, where the voltage difference was reduced to less than 10 millivolts, the ML IC security network was still able to successfully detect a P-SCA with up to 90% accuracy. When simulated against an EM-SCA, Kenarangi et al (2019) found the security network was able to detect an EM-SCA with up to 90% accuracy on the running device.

4.3 Battery Impedance Monitoring (BIM)

As discussed previously, power is measured using probes, and these probes introduce a slight resistance that is exploited by the BIM method introduced in Munny et al (2021). Using a similar method to the previous countermeasure, BIM compares the impedance of a secure system with the impedance of a compromised system to determine if it is under attack. Experiments showed that the speed BIM detects attacks varies based on the resistance of the probes. Munny et al (2021) found that with an 8.26 Ohm probe, the system was able to detect an attack in 22.020 milliseconds after probing began, while the attacker needs approximately 1,000 milliseconds to reveal the key.

4.4 Real-Time Switched Capacitor Detection (EoH)

A real-time switched capacitor P-SCA detection technique, named EoH, was developed in Younes et al (2023). EoH utilizes a switched capacitor DC-DC (SC-DCDC) converter within the power management unit alongside a lightweight Artificial Intelligence (AI) engine. The purpose of the SC-DCDC is to facilitate non-invasive load measurement by collecting switching activity. The SC-DCDC is used because it is likely already on most systems-on-chip (SoC). The AI trains on the switching activity collected during standard cryptographic operations and learns the normal behaviour. When the AI detects abnormal activity, it identifies it as an attack and uses the SC-DCDC converter to dynamically scale the voltage to mitigate the P-SCA as stated in Younes et al (2023).

4.5 Attenuated Signature Noise Injection (ASNI)

There are two concepts behind ASNI described in Maity et al (2018). First, embed the cryptographic system into a high efficiency Signature Attenuation Hardware (SAH) so that the current fluctuations produced by the AES are suppressed and not detectable by an SPA. Second, inject noise to further decorrelate measured power traces. The SAH reduces the amount of noise injection required to mask thus reducing the required overhead to generate noise. This countermeasure was tested with a CPA attack that measured over 1 million traces and successfully prevented recovery of the encryption key (Maity et al, 2018).

4.6 FRIES Electromagnetic Noise Generator

The FRIES noise generator proposed in Frieslaar et al (2018) uses cryptographic hash functions. The hash functions are given random inputs to generate hashes which creates random EM noise. The noise generator runs indefinitely in the background while the target system performs standard cryptographic operations. Frieslaar et al (2018) tested this countermeasure on a Raspberry Pi using AES-128 encryption and an attempted CEMA was unable to discover correlation between the noise and the EM radiation of the AES-128 encryption after more than 1 million traces.

4.7 Coplanar Capacitive Asymmetry Sensing (CEASE)

The foundational idea of CEASE in Seo et al (2023) is to measure the capacitance between pairs of metal plates that are on the top metal layer of an IC or printed circuit board using LC oscillator circuits. As metallic and non-metallic objects approach the plates, they interact with the plate's electric field, causing a minor change in capacitance. CEASE measures the difference between the two pairs to determine if a probe is approaching. Simulation results shown in Seo et al (2023) state that CEASE successfully sensed approaching EM probes from a distance of >1 mm with a >17% deviation from base-line interplate capacitance.

4.8 Electromagnetic Obfuscation (EO) Shield

The EO-Shield is designed in Gao et al (2023) to protect against EM-SCAs and focused ion beam (FIB) attacks, a type of invasive attack not covered in this survey. A basic overview of FIB is that it edits a circuit to extract information through reverse engineering. The EO-Shield incorporates an active shield and an information leakage obfuscation module. The shield uses the top metal layer of a circuit to detect and inhibit FIB attacks. The information leakage obfuscation module uses a linear feedback shift register, a ring oscillator (RO) oscillation circuit, and a signal comparison module to generate random signals. It emanates these signals, essentially EM noise, from the active shield to obfuscate cryptographic operations. This was tested against CEMA on an AES encryption circuit and prevented key recovery for 1000 traces as stated in Gao et al (2023).

4.9 Secure Reconfigurable Cryptographic Co-processor (SRCP)

SRCP is a reconfigurable co-processor able to support AES, DES, Rivest Cipher 6 (RC6), and international data encryption algorithm (IDEA), while being resistant to different types of SCAs as described in Shan et al (2015). SRCP is different from the previous countermeasures as there are five configurable countermeasures. There are three global and two encryption flow related countermeasures.

The first global countermeasure is randomization, essentially a form of noise generation, which enhances DPA resistance. This uses idle processing elements to perform random operations to randomize the power fluctuations (Shan et al, 2015). The next global countermeasure is partial complementary operation storage. This configures idle flip-flops to store data because flip-flops leak less data than registers as stated in Shan et al (2015). The last global countermeasure is out of order execution or shuffling. This shuffles the order of independent encryption operations to increase SCA resistance in a similar way to the shuffling countermeasure from Nozaki et al (2021).

The first encryption flow related countermeasure uses dummy operations that are randomly inserted during encryption to reduce correlation between encryption operation and key, adding more noise (Shan et al, 2015). The second encryption flow related countermeasure is dynamic storage exchanging which counters CPA by exchanging the storage locations of intermediate data from two consecutive rounds. This prevents CPA from calculating the correct Hamming distance that it uses to determine correlation coefficients (Shan et al, 2015).

SRCP was tested using DES and AES encryption against CPA and CEMA. CPA was unable to determine the encryption key after one million power traces against both DES and AES. CEMA was able to determine the DES encryption key after 27,679 traces, which is 36 times the amount needed for unprotected DES. CEMA was unable to determine the AES encryption key after 1.2 million traces as shown in the results of Shan et al, (2015).

5. Comparative Analysis of Countermeasures

In this section, we compare the countermeasures discussed previously by compiling them into Table 2 and discuss potential areas of strength and areas of weakness.

5.1 Variables

We first establish the variables examined in Table 2 to determine the general strengths and weaknesses of the techniques. Type indicates whether the countermeasure was implemented using software or hardware. It is assumed that hardware implementation also requires some form of software implementation. SCA Type signifies the type of SCA the countermeasure was designed and tested against. Algorithm refers to the algorithm the countermeasure is trying to protect. Countermeasure type involves whether the countermeasure was designed to detect or prevent SCAs. Effectiveness represents how well the countermeasure responded to an SCA. These are the results from the research papers. Immunity describes a technique that was able to completely prevent the encryption key from being deduced during testing. Additional overhead refers to any additional cost in terms of power, area, storage, or performance that the implementation of the countermeasure may incur. If there was no stated overhead cost, it is represented by *N/A* versus *None* for a stated overhead cost of nothing.

Scalability refers to the ease of implementing this countermeasure in existing computer systems. This is measured in terms of high, medium, and low. High means it will likely be easy to implement, medium means that it is likely challenging to implement, and low means that it is likely to be difficult to implement. Compatibility indicates how seamlessly the countermeasure can be integrated with other countermeasures. This is also measured on a scale of high, medium, and low. High means that it can likely be integrated with minimal difficulty, medium means that it is likely challenging but possible to integrate, and low means it is likely to be very difficult to integrate with other countermeasures.

Table 2: Comparison of Countermeasures

Counter-measure	**Type**	**SCA Type**	**Algorithm**	**Counter-measure Type**	**Effectiveness**	**Additional Overhead**	**Scalability**	**Compatibility**
Shuffling	Software	CPA	MLP	Prevention	Immunity from 1,000 traces	N/A	High	High
ML On-Chip Security Network	Hardware	Power, EM	N/A	Detection	90% accuracy detecting Power and EM-SCAs	Variable, AI/ML training	Low	Medium
BIM	Hardware	CPA	AES-128	Detection	Detection in 22.020 ms at 8.26 Ω	400 mW at 5V_{DD}	Medium	High
EoH	Hardware	Power	N/A	Detection, Prevention	N/A	AI/ML training	Medium	Medium
ANI	Hardware	CPA	AES-128	Prevention	Immunity from >1 million traces	1.23x additional power overhead	Low	High
FRIES Noise Generator	Software	EM	AES-128	Prevention	No correlation found in tests	100% CPU usage on all cores but no lag from device	High	High
Counter-measure	Type	SCA Type	Algorithm	Counter-measure Type	Effectiveness	Additional Overhead	Scalability	Compatibility
CEASE	Hardware	EM	Agnostic	Detection	Detects EM probes at >1 mm	4 on-die 300μm metal plates	Low	High
EO-Shield	Hardware	CEMA, FIB	AES-128	Detection, Prevention	Alerts if shield is broken, immunity from 1,000 traces	1.75% area increase, max 9.74% power increase	Low	Medium

Counter-measure	Type	SCA Type	Algorithm	Counter-measure Type	Effectiveness	Additional Overhead	Scalability	Compatibility
SRCP	Hardware	CPA, CEMA	AES, DES, RC6, IDEA	Prevention	Immune to CPA & CEMA after 1 million traces for AES	6% power increase, co-processor placement	Medium	High

5.2 Strengths

A common trend between several of these countermeasures is noise generation/injection. The strength of noise generation is its versatility. Because noise generation can typically be generated using only software, it can be applied to various cryptographic systems without major redesign or hardware modifications.

The majority of these countermeasures have low additional overhead. Many of them increase the overall power usage, but that is expected for these countermeasures, since many of them involve performing random operations, which takes more power. Low overhead countermeasures are necessary to ensure that the primary functions of the underlying system are not compromised.

A strength of software-based countermeasures is their high scalability ratings due to the ease that software can be added to existing systems. The overall cost of building and adding software-based countermeasures is lower than creating precise hardware. Additionally, if an update is necessary, software can be easily changed.

A notable strength of the surveyed countermeasures is that the average compatibility is between medium and high. Being able to combine different countermeasures will only improve security because an attacker will not stop simply because their initial attempt at CPA did not work. Additionally, a detection countermeasure could be combined with a prevention countermeasure to increase efficiency so the prevention is only active when an SCA is detected. An example of this is combining CEASE with ASNI so that ASNI only activates when CEASE detects a probe nearby, thereby reducing overall power draw.

A strength of many of the countermeasures is how they are algorithm agnostic. This is not apparent upon initial view of Table 2, but a deeper look into their design shows that the implementation of countermeasures does not rely on specific encryption algorithms to protect against SCAs. This likely allows the countermeasures to be used for all common encryption algorithms. This will allow for higher versatility and future proofing for when new encryption algorithms are developed as the countermeasures will not need to be adapted to them.

5.3 Weaknesses

Looking at Table 2, an apparent weakness for hardware-based countermeasures is scalability. It is, on average, low because applying a hardware upgrade to existing systems is likely to be difficult, especially due to the diversity of processors that are used in commercial products. For example, the ASNI countermeasure requires embedding the encryption engine into the SAH and it is unclear if most encryption engines are compatible with the SAH. Several of these countermeasures attempt to make use of hardware that is likely present on the system; however, there is no guarantee that the system in question will have the necessary hardware.

A potential weakness of software-based countermeasures is that the new software could have errors or exploits that are vulnerable to traditional types of hacking, such as zero-day vulnerabilities or malware. Additionally, since pure software countermeasures use the existing resources of the system, it could impact performance due to the different computational operations being done. This is easily seen with the Frieslaar et al (2018) FRIES noise generator, where the stated overhead is 100% CPU usage, which if implemented on other systems could slow overall performance.

Looking specifically at the detection techniques, their major weakness is that they only detect. While useful, it does not make it any more challenging for the attacker to recover the encryption key, which is why having high compatibility is beneficial, as mentioned in the strengths section above.

For countermeasures that implement AI/ML, they are each trained on data specific to the system. Implementing these countermeasures on other systems likely requires collecting new training data and running the AI/ML until they are properly trained. This adds additional overhead and complexity to the overall implementation not discussed in the papers.

6. Future Work

Several areas of future work can be explored based on the findings of this survey. Efforts should focus on improving the scalability of hardware-based countermeasures for integration into commercially available systems, perhaps by utilizing hardware more likely to be on commercial systems. Optimizing software-based countermeasures to reduce impacts on system performance and continuous testing to mitigate potential vulnerabilities in code is crucial for countermeasures to be effective on a large scale. Further research into combining detection and prevention techniques can create more comprehensive and efficient countermeasures. Finding additional ways to advance AI/ML-based countermeasures can enhance adaptability as they train and learn. The pursuit of these research directions may result in the development of more efficient, effective, scalable, and adaptable SCA countermeasures.

7. Conclusion

This survey provides an overview of power and EM-based SCAs and their respective countermeasures. By consolidating existing research, we highlight the strengths and weaknesses of various techniques, offering valuable insights into their effectiveness, scalability, and compatibility. The comparative analysis underscores the need for low-overhead solutions that do not compromise the primary functions of the system and the benefits of having algorithm agnostic protections. While the surveyed countermeasures offer significant strengths, they have notable weaknesses. Hardware-based countermeasures face scalability and compatibility challenges, while software-based solutions can introduce new vulnerabilities and detrimentally impact system performance. The integration of detection and prevention techniques, as well as advancements in AI/ML-based countermeasures, present promising directions for future research. Combining multiple countermeasures and leveraging their strengths can enhance overall device security, providing robust protection against SCAs while maintaining system efficiency and functionality. This approach ensures that security measures are both effective and practical, potentially resulting in the development of more resilient cryptographic systems.

Disclaimer: The views expressed in this paper are those of the authors, and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. Government.

Ethics Declaration: I confirm that my research did not involve human participants and therefore does not require ethical clearance.

AI Declaration: I acknowledge the use of AI tools in the creation of this paper. Specifically, AI was utilized for literature review and feedback to refine wording.

References

Abu-Ghazeleh, N., Ponomarev, D. and Evtyushkin, D. (Mar. 2019). "How the Spectre and Meltdown Hacks Really Worked". In: *IEEE Spectrum,* Vol 56, No. 3, pp. 42–49.

Damian, D. M., Hascsi, Z. and Sandulescu, A. B. (Oct. 2017). "Presilicon Evaluation on Correlation Power Analysis Attacks and Countermeasures". In: *2017 IEEE 23rd International Symposium for Design and Technology in Electronic Packaging (SIITME)*. IEEE, pp. 313–317.

Das, Debayan et al. (Oct. 2018). "ASNI: Attenuated Signature Noise Injection for Low-Overhead Power Side-Channel Attack Immunity". In: *IEEE Transactions on Circuits and Systems I: Regular Papers,* Vol 65, No. 10, pp. 3300–3311. doi: 10.1109/TCSI.2018.2819499.

Das, Devajit and Boro, Debojit (2023). "Electromagnetic Signal Analysis: A Vulnerability to Edge Computing Driven IoT Devices". In: *2023 4th International Conference on Computing and Communication Systems (I3CS)*. IEEE, doi: 10.1109/I3CS58314.2023.10127273.

Duan, Xiaoyi et al. (June 2016). "Differential Power Analysis Attack and Efficient Countermeasures on PRESENT". In: *2016 8th IEEE International Conference on Communication Software and Networks (ICCSN)*. IEEE, pp. 8–12.

Frieslaar, I and Irwin, B (Dec. 2018). "Developing an Electromagnetic Noise Generator to Protect a Raspberry PI from Side Channel Analysis". In: *SAIEEE Africa Research Journal* Vol 109, No. 2, pp. 85–101.

Gao, Ya et al. (Jan. 2023). "EO-Shield: A Multi-Function Protection Scheme against Side Channel and Focused Ion Beam Attacks". In: *Asia and South Pacific Design Automation Conference, ASP-DAC*. IEEE, pp. 670–675. doi: 10.1145/3566097.3567924.

Gupta, Himanshu et al. (Dec. 2019). "Impact of Side Channel Attack in Information Security". In: *2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)*. IEEE, pp. 291–295.

Hatun, E et al. (June 2019). "Side Channel Analysis Using EM Radiation of RSA Algorithm Implemented on Raspberry Pi". In: *2019 International Symposium on Networks, Computers and Communications (ISNCC)*. IEEE, pp. 1–6.

Hettiarachchi, M. J. et al. (2023). "Time Analysis Side Channeling Attack in Symmetric Key Cryptography". In: *8th International Conference on Information Technology Research: The Next Evolution in Digital Transformation.* IEEE, doi: 10.1109/ICITR61062.2023.10382746.

Kang, Young Jin et al. (Apr. 2015). “Correlation power analysis attack on the Ping Pong-128 key stream generator”. In: *International Conference on Advanced Information Networking and Applications, AINA*. IEEE, pp. 506–509. doi: 10.1109/AINA.2015.228.

Kenarangi, Farid and Partin-Vaisband, Inna (June 2019). “Security Network On-Chip for Mitigating Side-Channel Attacks”. In: *2019 ACM/IEEE International Workshop on System Level Interconnect Prediction (SLIP)*. IEEE, pp. 1–6.

Kundrata, J et al. (Sept. 2020). “Comparison of Pearson Correlation Coefficient and Distance Correlation in Correlation Power Analysis on Digital Multiplier”. In: *2020 43rd International Convention on Information, Communication and Electronic Technology (MIPRO)*. IEEE, pp. 146–151.

Martinasek, Zdenek, Clupek, Vlastimil and Krisztina, Trasy (July 2013). “General Scheme of Differential Power Analysis”. In: *2013 36th International Conference on Telecommunications and Signal Processing (TSP)*. IEEE, pp. 358–362.

Mayer-Sommer, Rita (2000). “Smartly Analyzing the Simplicity and the Power of Simple Power Analysis on Smartcards”. In: Vol. 1965. Springer, Berlin, Heidelberg, pp. 78–92.

Montminy, David P. et al. (Oct. 2013). “Differential electromagnetic attacks on a 32-Bit microprocessor using software defined radios”. In: *IEEE Transactions on Information Forensics and Security* 8 (12), pp. 2101–2114. doi: 10.1109/TIFS.2013.2287600.

Munny, Rowshon and Hu, John (May 2021). “Power Side-Channel Attack Detection through Battery Impedance Monitoring”. In: *IEEE International Symposium on Circuits and Systems.* IEEE, pp. 1–5. doi: 10.1109/ISCAS51556.2021.9401542.

Nozaki, Yusuke and Yoshikawa, Masaya (2021). “Shuffling Countermeasure against Power Side-Channel Attack for MLP with Software Implementation”. In: *2021 IEEE 4th International Conference on Electronics and Communication Engineering*. IEEE, pp. 39–42. doi: 10.1109/ICECE54449.2021. 9674668.

Piessens, Frank and Van Oorschot, Paul C. (Mar. 2024). “Side-Channel Attacks: A Short Tour”. In: *IEEE Security and Privacy,* Vol 22, No. 2, pp. 75–80. doi: 10.1109/MSEC.2024.3352848.

Randolph, Mark and Diehl, William (June 2020). *Power Side-Channel Attack Analysis: A Review of 20 Years of Study for the Layman*. doi: 10.3390/cryptography4020015.

Safta, Mariana et al. (Oct. 2016). “Design and Setup of Power Analysis Attacks”. In: *2016 IEEE 22nd International Symposium for Design and Technology in Electronic Packaging (SIITME)*. IEEE, pp. 110–13.

Seo, Dong Hyunet al. (Dec. 2023). “Improved EM Side-Channel Analysis Attack Probe Detection Range Utilizing Coplanar Capacitive Asymmetry Sensing”. In: *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems,* Vol 42, No. 12, pp. 4583–4596. doi: 10.1109/TCAD.2022.3227077.

Shan, Weiwei, Fu, Xingyuan and Xu, Zhipeng (July 2015). “A Secure Reconfig urable Crypto IC With Countermeasures Against SPA, DPA, and EMA”. In: *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems,* Vol 34, No. 7, pp. 1201–1205. doi: 10.1109/TCAD.2015.2419621.

Tauoil, Mottaqiallah, Aljuffri, Abdullah and Hamdioui, Said (2021). “Power Side Channel Attack Where Are We Standing”. In: *2021 16th International Conference on Design & Technology of Integrated Systems in Nanoscale Era (DTIS)*, pp. 1–6.

Younes, Leen et al. (Dec. 2023). “Real-Time Switched Capacitor Based Power Side-Channel Attack Detection”. In: *International Conference on Microelectronics (ICM)*. IEEE, pp. 253–257. doi: 10.1109/ ICM60448.2023.10378898.

Zadeh, Abdulah Abdulah and Heys, H. M. (Apr. 2012). “Applicability of Simple Power Analysis To Stream Ciphers Constructed Using Multiple LFSRs”. In: *2012 25th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE).* IEEE, pp. 1–6.

Zhou, Wen-hai and Kong, Fan-tong (Oct. 2019). “Electromagnetic Side Channel Attack Against Embedded Encryption Chips”. In: *2019 IEEE 19th International Conference on Communication Technology (ICCT).* IEEE, pp. 140-144.