R. Jevtic and M. G. Otero, "Methodology for Complete Decorrelation of Power Supply EM Side-Channel Signal and Sensitive Data," in IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 69, no. 4, pp. 2256-2260, April 2022, doi: 10.1109/TCSII.2022.3144071

Methodology for Complete Decorrelation of Power Supply EM Side-Channel Signal and Sensitive Data

Ruzica Jevtic, *Senior Member, IEEE*, and Mariano Garcia Otero

***Abstract*—Electro-magnetic (EM) side channel attacks have become a serious threat to security of Internet-of-Things (IoT) devices. Power supply generated by voltage regulators is one of the most common attack targets due to its strong EM emanations. In this brief we derive analytical conditions for complete theoretical decorrelation of the power supply EM side-channel signal and the sensitive data. The output of the power supply converter is modelled as amplitude modulation (AM) of the load signal by the converter capacitance that acts as a carrier. By applying Price theorem (Papoulis and Pillai, 2002), we obtain the exact theoretical conditions that converter capacitance needs to fulfil in order to prevent EM side-channel attacks. The conditions are further adapted for practical implementation. When the proposed methodology is applied to AES measured traces, the correlation coefficient between the leaked signal and the sensitive data is 0.05. Such low correlation indicates the proposed methodology is a promising candidate against the attacks that exploit AM signals to extract sensitive data, such as, TEMPEST and active EM attacks. Test Vector Leakage Assessment (TVLA) ρ-test detects no leaky points, thereby confirming circuit protection against differential and correlation EM attacks as well.**

***Index Terms*—Security, Price theorem, side-channel attacks, switched-capacitor DC-DC converters, signal statistics.**

I. Introduction

SIDE-CHANNEL attacks rely on measurement of physical leakages of the device while running a cryptographic algorithm or a malware program that serves to exfiltrate sensitive data. Leakages such as EM radiation, power consumption or execution time can reveal confidential information. This can be extremely dangerous especially when tampering with the device can result in life-threating conditions, such as, for example, hacking into pace-makers or cars.

In this brief, we focus on EM side-channel attacks as they pose a more serious threat to the security when compared to power side-channel attacks [2], [3]. They can be either passive, where the hidden information like cryptographic secret key, is extracted from unintentional EM radiation [6]–[16], or active, where the attacker creates a covert channel and manipulates the EM emanations in order to obtain sensitive data [17]–[20]. Passive attacks aimed to find a secret key used in cryptographic engines are based on differential and correlation analysis of the leaked signal. TEMPEST attacks are another type of passive attacks, where the sensitive data, the so-called red signal is modulated by some other high-frequency signal such as CPU or memory clock, i.e., black signal, and transmitted accidentally in form of EM radio waves. To perform an active attack, an attacker needs to be able to create and run a small program inside the device to create EM patterns that reveal sensitive information.

The focus of this brief are EM emanations of the power supply signal. The signal is created by the voltage regulators and produces one of the strongest EM emanations in the device [6]. We assume the power supply is generated by switched capacitor (SC) converters, an attractive solution for power supply of small IoT devices. They can be fully integrated on-chip and reconfigured to achieve multiple voltages without significant loss in the efficiency [4], [5].

We derive conditions the capacitance signal needs to fulfil in order to completely decorrelate the measured signal from the load signal. We prove that the changes in the capacitance signal need to be determined according to the load fluctuations in order to achieve device full protection.

Based on the physical behavior of the SC converter, the leaked signal is represented as a load signal amplitude-modulated by the capacitance [7]. Thus, we compute the correlation coefficient directly between the load signal and AM load signal. By making this coefficient equal to zero for complete decorrelation and then using Price theorem [1], we derive an expression for capacitance signal. Afterwards, we apply design constraints to obtain the conditions for the construction of the capacitance signal in the real-world conditions.

In order to address both types of EM attacks, active and passive, we test the proposed methodology on measured AES traces by computing the correlation coefficient between the load and the leaked signal, and also by applying Test Vector Leakage Assessment. The correlation coefficient is a measure of how much information can be extracted from the leaked signal (e.g., during an active or TEMPEST attack), while TVLA estimates the number of leaky points in differential and correlation attacks (e.g., during an attack on AES engine).

II. Related Work

There are many countermeasures applied to the switched-capacitor converters that are designed against passive power side-channel attacks. Most of them are based on random power scrambling [8]–[11], where the capacitance is changed randomly in order to introduce random noise in

Manuscript received January 7, 2022; accepted January 14, 2022. Date of publication January 18, 2022; date of current version March 28, 2022. This research was funded by the Ministry of Science, Innovation and Universities of Spain, and the European Regional Development Fund of the European Commission, Grant No. RTI2018-095324-B-I00. This brief was recommended by Associate Editor A. J. Acosta. *(Corresponding author: Ruzica Jevtic.)*

Ruzica Jevtic is with the Escuela Politecnica Superior, Universidad San Pablo-CEU, CEU Universities, 28668 Madrid, Spain (e-mail: ruzica.jevtic@ceu.es).

Mariano Garcia Otero is with the Information Processing and Telecommunications Center, Universidad Politecnica de Madrid, 28040 Madrid, Spain (e-mail: mariano@gaps.ssr.upm.es).

Digital Object Identifier 10.1109/TCSII.2022.3144071

the attacked power signal. EM attack countermeasures are often time-consuming as they optimize the design at the gate and/or layout level [12], [13], contrary to this brief that proposes modifications at the architectural level. The work in [7] targets EM side-channel attacks on switched-capacitor converters, and proposes to change the capacitance signal in a deterministic manner, similar to the work presented here. However, the capacitance fluctuations are derived by using a frequency-domain analysis and do not completely decorrelate the sensitive data from the leaked signal.

It is worth mentioning countermeasures that target different voltage regulators: inductive buck regulators in [14] and linear dropout regulators in [15]. They are also based on introducing randomness in the leaked power supply signal and improve protection against power attacks. However, inductive regulators suffer from large area due to the inductance, while the linear regulators suffer from efficiency degradation over a broad range of output voltages, and are not considered here.

Active EM attacks are based on building a covert channel to be able to encode and leak the sensitive data. They include using memory [17], [18], power management unit [19] and peripheral [20] to actively control EM radiations. Many of them can extract information from isolated (air-gapped) laptops, can penetrate through wall separation or are successful even from hundreds of meters of distance as reported in [18].

All these attacks are recent, powerful and call for novel countermeasures. The common feature with our methodology is that the leaked signal is obtained by amplitude modulation of the sensitive data: e.g., in [17], [18] it is a signal proceeding from memory, in [19] from power unit and [20] from monitor.

Many of the TEMPEST passive attacks are also based on amplitude modulation of the sensitive data [6], [20], [21]. For example, one of the mechanisms that allows for modulation of red signal with the black one, is through a crosstalk of data buses. Although the mechanism to achieve the modulation is different from this brief, the final result is similar: the hidden data gets multiplied by another signal that acts as a carrier.

The theoretical analysis presented in the next section is by no means limited to power supply signal generated by SC DC-DC converters. It can be applied to any type of AM signal as long as the distributions of the signal and the carrier can be approximated with the Gaussian distribution. Adapting the proposed methodology to different types of signals could be a promising approach to build efficient countermeasures against the attacks that exploit AM signals.

III. Theoretical Bound for Complete Decorrelation

The changes in the voltage and load current produced by the device activity, create EM field around the converter according to Faraday's law. Due to a direct relation between the EM field components and the changing voltage [22], the power supply voltage is considered to be the leaked EM signal.

The switched capacitor converter chosen here is single-phased. This type of converter allows for larger energy savings compared to the multi-phased one, at a cost of more complicated clocking mechanism and mandatory presence of error correction circuits [4], [5]. As shown in [7], the converter output voltage signal indirectly carries full information on the product of the load, $R(t)$, and capacitance, $C(t)$, i.e., the load signal amplitude modulated by the capacitance signal. Consequently, we consider this product to be the leaked EM signal that is available to the attacker.

Let $M = R \cdot C$ be the leaked EM signal. Time variable has been omitted for the sake of clarity in this section. In order to make the leaked signal completely decorrelated from the load signal, R, the covariance of the two signals needs to be zero, i.e., $Cov[M, R] = E[MR] - E[M] \cdot E[R] = 0$.

First, we consider the following case: the load signal and the flying capacitor are two independent variables. Then:

$$Cov[M, R] = E[R^2]E[C] - E^2[R]E[C] = Var[R]E[C] \quad (1)$$

The covariance of the leaked signal and the load signal in (1) is never zero, since the mean of the flying capacitor is always a positive value as well as the variance of the load (assuming that the load is not constant). Therefore, it is impossible to achieve a complete decorrelation when the load and the flying capacitor are independent variables.

Next, we consider that the load signal and the flying capacitor are two dependent variables. Then:

$$Cov[M, R] = E[R^2C] - E[RC]E[R] \quad (2)$$

In order to completely decorrelate the leaked signal from the load, the following must be fulfilled:

$$E[R^2C] = E[RC]E[R] \quad (3)$$

The goal is to construct the flying capacitor variable so that the equation (3) is fulfilled. Since the load current is a result of the activity of millions of logic gates in a standard microprocessor, the central limit theorem allows us to approximate the load as a Gaussian signal. We then apply Price theorem to simplify the left-hand side of equation (3).

The Price theorem states the following: given two Gaussian random variables X and Y, and a function of the two variables, marked with g, the following stands true for the relationship between the expectance of the g, marked with I and the covariance of the two variables, marked with ρ:

$$\begin{aligned} I(\rho) &= E[g(X, Y)] \\ \frac{\partial^n I(\rho)}{\partial \rho^n} &= E\left[\frac{\partial^{2n} g(X, Y)}{\partial X^n \partial Y^n}\right] \end{aligned} \quad (4)$$

In our case, $g(X, Y) = X^2 \cdot Y$, where $X = R$ and $Y = C$. We apply the Price theorem, by assigning $n = 1$. As a result:

$$\frac{\partial I(\rho)}{\partial \rho} = E\left[\frac{\partial^2 g(X, Y)}{\partial X \partial Y}\right] = E[2X] = 2E[X] \quad (5)$$

By integrating the equation (5), we obtain:

$$I(\rho) = 2 \cdot E[X] \cdot \rho + I(0) \quad (6)$$

Since $I(0) = E[X^2 \cdot Y] = E(X^2) \cdot E(Y)$ when $\rho = 0$, i.e., $Cov(X, Y) = 0$, we obtain:

$$E[X^2 \cdot Y] = 2 \cdot E[X] \cdot Cov(X, Y) + E(X^2) \cdot E(Y) \quad (7)$$

Replacing this in the left-hand side of the equation (3) results in:

$$2E[R]Cov(R, C) + E(R^2)E(C) = E[RC] \cdot E[R] \quad (8)$$

By substituting $Cov[R, C] = E[RC] - E[R] \cdot E[C]$ and rearranging the terms, we obtain:

$$E[RC]E[R] - 2E^2[R]E[C] + E(R^2)E(C) = 0 \tag{9}$$

Finally:

$$\begin{aligned} &E[R] \cdot Cov(R, C) + Var[R] \cdot E[C] = 0 \\ &Cov(R, C) = -Var[R] \cdot \frac{E[C]}{E[R]} \end{aligned} \tag{10}$$

The equation (10) is a necessary condition for the covariance of R and C to achieve complete decorrelation of the load and the leaked signal. Since the load and the flying capacitance are dependent variables and assuming they have a linear relationship, the capacitance can be obtained as $C = \alpha R + Z$, where α is a proportional constant and Z is a random variable with Gaussian distribution, independent from R. The model chosen in this brief is linear for the sake of simplicity, but any other model can be chosen as long as it is guaranteed that it satisfies condition (10) derived by using the Price theorem.

We proceed to calculate the left-hand side of equation (10), by computing the following terms:

$$\begin{aligned} E[RC] &= \alpha E[R^2] + E[ZR] = \alpha E[R^2] + E[Z]E[R] \\ E[C] &= \alpha \cdot E[R] + E[Z] \end{aligned} \tag{11}$$

By replacing (11) into the expression for $Cov(R, C)$, and rearranging the terms, we obtain:

$$Cov[R, C] = \alpha \cdot Var[R] \tag{12}$$

From (10) and (12), we obtain:

$$\alpha \cdot Var[R] = -Var[R] \cdot \frac{E[C]}{E[R]} \tag{13}$$

It can be seen from the last equation that $\alpha = -\frac{E[C]}{E[R]}$.

After calculating the expectance of the flying capacitance and replacing α, the only condition that Z needs to fulfil is:

$$E[C] = -\frac{E[C]}{E[R]} \cdot E[R] + E[Z] \tag{14}$$

Therefore, $E[Z] = 2 \cdot E[C]$.

As a result, if the flying capacitance values satisfy:

$$C = -\frac{E[C]}{E[R]} \cdot R + Z \tag{15}$$

where Z is a random variable with $E[Z] = 2E[C]$, the load can be completely decorrelated from the leaked signal.

IV. Real-World Conditions

We derive rigorous conditions for flying capacitance signal generation so that equation (15) is satisfied and two necessary conditions are fulfilled: at any point in time, capacitance value needs to be a positive number, and the value assigned to the capacitance needs to be between the minimum capacitance value C_{min}, and the maximum capacitance value C_{max}, both specified by the converter design.

The signal Z(t) in equation (15) can be represented as $Z(t) = 2 \cdot E[C(t)] + a \cdot N(t)$, where $N(t)$ is a standard normal random variable, and a is a positive constant. In practice, $N(t)$ is a symmetric truncated normal distribution bounded by a certain minimum N_{min} and maximum N_{max} value. However, if $N_{max} - N_{min}$ is much larger than 1, the error introduced in the model for the capacitance derived in Section III, can be considered to be small.

There are two unknowns that need to be determined: a and $E[C(t)]$. For the sake of clarity, we mark $E[R(t)]$ as μ_R and $E[C(t)]$ as μ_C. At all times the following needs to be fulfilled:

$$C_{min} < -\frac{\mu_C}{\mu_R} \cdot R(t) + Z(t) < C_{max} \tag{16}$$

In the worst case:

$$\begin{aligned} C_{max} &> -\frac{\mu_C}{\mu_R} \cdot min(R(t)) + 2\mu_C + a \cdot N_{max} \\ C_{min} &< -\frac{\mu_C}{\mu_R} \cdot max(R(t)) + 2\mu_C + a \cdot N_{min} \end{aligned} \tag{17}$$

From these inequalities, we obtain:

$$\begin{aligned} a &< \frac{C_{max} - 2 \cdot \mu_C + \frac{\mu_C}{\mu_R} \cdot min(R(t))}{N_{max}} \\ a &< \frac{C_{min} - 2 \cdot \mu_C + \frac{\mu_C}{\mu_R} \cdot max(R(t))}{N_{min}} \end{aligned} \tag{18}$$

As a result, the amplitude a needs to be chosen as a minimum of the two right-hand sides in the inequalities (18) and is dependent on the unknown μ_C.

Next, we derive the necessary conditions for μ_C. As N_{max} and a are positive, from the first inequality in (18), we obtain that the numerator in (18a) needs to be positive too. Thus:

$$\mu_C < \frac{C_{max}}{2 - \frac{min(R(t))}{\mu_R}} = capmean_{max} \tag{19}$$

The second condition for μ_C is obtained from (18b). The numerator of this inequality needs to be a negative number, since N_{min} is negative too. From here:

$$\mu_C > \frac{C_{min}}{2 - \frac{max(R(t))}{\mu_R}} = capmean_{min} \tag{20}$$

It can be seen that indirectly, the denominator in inequality (20) also needs to be a positive number, i.e., $2 - \frac{max(R(t))}{\mu_R} > 0$. There are very few loads that correspond to the execution of the cryptographic algorithm and are able to fulfil this condition. The condition is essentially demanding the maximum load value to be smaller than twice the mean load value. However, load current has high peaks at the beginning of every clock cycle since this is when the changes in millions of flip-flops take place. These peaks are most likely to be an order of magnitude larger than the load mean. Failure to comply the condition leads to a negative value for a, and many values of the generated capacitance signal out of $[C_{min}, C_{max}]$ range.

To overcome this problem, we propose to use the above analysis as a guideline for flying capacitance generation but without strict fulfilment of all conditions. The conditions for both, μ_C and a are inequalities, implying there might be more than one solution for the flying capacitance signal. We propose to fix one value for μ_C and sweep the values for a. For each pair (μ_C, a), we generate the flying capacitance signal. All values that fall below C_{min} and above C_{max} are then mapped to C_{min} and C_{max} respectively. Statistical distribution obtained in such way deviates slightly from the Gaussian distribution, but as we will show later, has a very small impact on the efficiency of the proposed methodology. Finally, we repeat

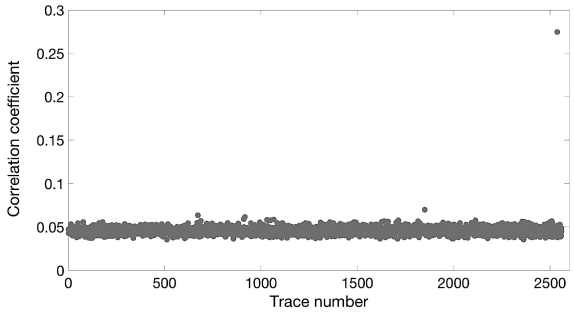

Fig. 1. Correlation coefficients for AES traces.

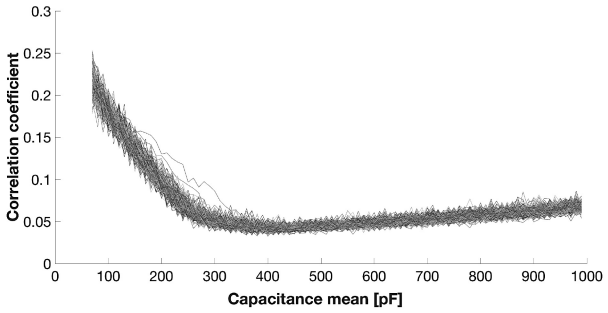

Fig. 2. Correlation coefficients for different capacitance mean values.

this process for many different values for μ_C and choose the pair (μ_C, a) that results in the smallest correlation coefficient between the load and the leaked signal.

V. Experimental Results

We evaluate the proposed technique for a cryptographic algorithm execution. In order to make an assessment for attacks that search for information through demodulation of the power supply signal, the correlation coefficient is computed between the AES measured traces ($R(t)$) and the leaked signal ($R(t)C(t)$). It is important to note that instead of a cryptographic execution, we could be using any other program execution, since we are evaluating if the leaked data can be related to the load data. Afterwards, both TVLA *t*-test and *rho*-test are employed to estimate the number of leaky points for differential and correlation attacks. These tests do need to be applied to EM radiations from cryptographic executions to provide passive attack protection assessment. In all experiments, flying capacitor values are limited between $C_{min} = 60pF$ and $C_{max} = 1000pF$, values that correspond to switched-capacitor design used in [5].

Our experimental framework is built in MATLAB. We generate $C(t)$ by sweeping the values for μ_C and a, and choose the pair (μ_C, a) that results in the lowest correlation between $R(t)$ and $R(t)C(t)$, as explained in the previous section.

A. Correlation Coefficient Comparison

We use AES measured power traces from [24] as a load. The power traces are collected for AES 128 software implementation executed on Chip-Whisperer Lite FPGA platform. There are 2560 traces in the set and correspond to 256 different values of the input plaintexts. Fig. 1 shows the best correlation coefficient that was achieved for each trace. All correlation coefficients are around 0.05 except for one trace. Closer observation of the trace has shown that it has one power value that is several orders of magnitude larger than other values, probably due to larger amount of noise during that particular measurement. This causes the correlation coefficient to increase. Even with this anomaly, the correlation coefficient for this trace is also low and equal to 0.27. The proposed countermeasure clearly outperforms the countermeasure in [7] where the correlation coefficient for the AES load is 0.35.

To the best of our knowledge, this is the first work to report such low correlation coefficients between the load and the leaked signal. Nearly all correlation coefficients are close to zero as predicted by the analysis presented above. Furthermore, even though the condition $2 - \frac{min(R(t))}{\mu_R} > 0$ is not fulfilled for the AES load, and the flying capacitance values are adjusted so that they fall in $[C_{min}, C_{max}]$ range, the proposed methodology achieves almost complete decorrelation between the EM leaked signal and AES secret key.

Fig. 2 shows correlation coefficients for 200 traces when the flying capacitance mean is swept between $C_{min} + 10pF$ and $C_{max} - 10pF$. It can be seen that the capacitance mean value does not have a significant effect on the correlation coefficient as long as it is larger than 350pF. Consequently, the capacitance mean can be set to a fixed value to simplify the flying capacitance signal generation.

B. Test Vector Leakage Assessment

TVLA is primarily used to test if a particular countermeasure protects the device from differential and correlation attacks. It offers two types of tests: *t*-test and *rho*-test and identifies the points that are possible leaks of sensitive data.

We apply the TVLA ρ-test on the measured AES traces as in [24]. The 2560 measured traces are divided into 10 sets. Ten different partitions are created, with one set as a test set, and the rest, the profile set. Traces with the input plaintexts that have the same first byte are grouped together. Each group is reduced to one trace by taking the average, and the correlation coefficient is computed sample-wise between the reduced profile set and the test set. The procedure is repeated for each partition and Fisher z-transformation is applied to the mean of the corresponding coefficients. All time points with the correlation coefficient larger than 4.5 count as leaky points.

We apply the ρ-test to the unsecured circuit and obtain 62 leaky points, the same number reported in [24] (see Fig. 3a). Then, the proposed technique is applied to the circuit for the same AES load resulting in 0 leaky points (see Fig. 3b)). The proposed technique not only lowers the correlation between the load and the leaked signal, but is also very robust against differential and correlation EM side-channel attacks.

When *t*-test is applied to the proposed methodology with traces provided in [24], the number of leaky points drops from 9390 to 373 for one fixed input class and from 9421 to 345 for a different fixed input class, resulting in 25.1X and 27.31X reduction respectively. To provide a fair comparison with previous works regarding the number of traces, we perform additional t-test on 1 million traces for AES hardware implementation executed on CW305 FPGA platform and the number of leaky points drops from 127 to 0. All three t-tests achieve reduction larger than 22.7X reduction reported in [11] for multi-phase switched capacitor converters, 5X reported in [14] for buck voltage regulators and 21.68X reported in [15]

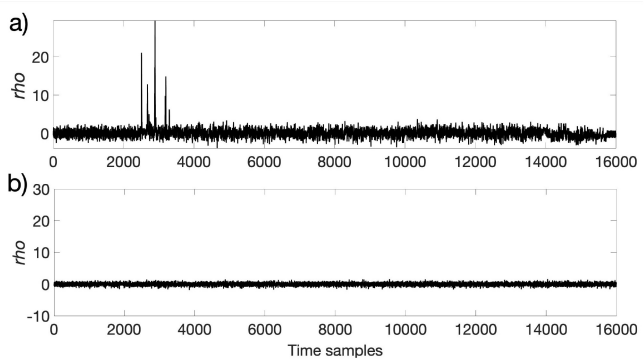

Fig. 3. Normalized correlation coefficients for a) unsecured and b) secured AES execution.

TABLE I
TVLA STATISTICS AND CORRELATION COEFFICIENT COMPARISON

Method	This work	[7]	[11]	[14]	[15]
Correl.	0.05	0.35	N/A	N/A	N/A
ρ-test	0/62	0/62	N/A	N/A	N/A
t-test	373/9390	3/9390	8.37/190.1	37.9/197.1	11.9/258
Attack	EM	EM	Power	Power	Pow&EM

for digital linear regulators (see Table I). The work in [7] reports better *t*-test results (3130X) for traces from [24], at the cost of larger correlation coefficient of 0.35.

The practical implementation of the proposed methodology can be achieved by partitioning the flying capacitor into unit-cells that can be turned on and off, as in [7]. Thus, we expect overhead estimations to be similar to [7]: 15% area overhead, 10% efficiency reduction and no performance penalty.

Consequently, the proposed methodology offers an excellent protection from a broad range of EM side-channel attacks: differential and correlation, usually applied for secret key retrieval, as well as the side-channel attacks that demodulate the leaked AM signal in order to extract information on sensitive data stored and processed in electronic devices.

VI. CONCLUSION

We present a methodology that completely decorrelates the power supply EM side-channel signal from the secret key information. The methodology is based on modelling of the voltage regulator functionality. We derive theoretical conditions that need to be fulfilled for complete decorrelation, which are then revised to allow for practical implementation. The results show that the correlation coefficient for AES measured traces drops to only 0.05, while TVLA *rho*-test reveals a complete absence of leaky points. *t*-test leakage reduction is larger than most of the state-of-the-art countermeasures, making the proposed countermeasure an extremely attractive solution for improved security in IoT devices.

REFERENCES

[1] A. Papoulis and U. Pillai, *Probability, Random Variables and Stochastic Processes*, 4th ed. London, U.K.: McGraw-Hill Eur., 2002.

[2] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, "The EM side—Channel(s)," in *Proc. CHES*, 2002, pp. 29–45.

[3] D. Das, M. Nath, B. Chatterjee, S. Ghosh, and S. Sen, "Ground-up root-cause analysis guided low-overhead generic countermeasure for electro-magnetic side-channel attack," IACR Cryptol. ePrint Arch., Lyon, France, Rep. 2018/620, 2018, p. 620.

[4] R. Jevtić *et al.*, "Per-core DVFS with switched-capacitor converters for energy efficiency in manycore processors," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 23, no. 4, pp. 723–730, Apr. 2015.

[5] B. Zimmer *et al.*, "A RISC-V vector processor with simultaneous-switching switched-capacitor DC–DC converters in 28 nm FDSOI," *IEEE J. Solid-State Circuits*, vol. 51, no. 4, pp. 930–942, Apr. 2016.

[6] R. Callan, A. Zajić, and M. Prvulovic, "FASE: Finding amplitude-modulated side-channel emanations," in *Proc. 42nd Annu. Int. Symp. Comput. Archit. (ISCA)*, Jun. 2015, pp. 592–603.

[7] R. Jevtic, M. Ylitolva, C. Calonge, M. Ojanen, T. Santti, and L. Koskinen, "EM side-channel countermeasure for switched-capacitor DC–DC converters based on amplitude modulation," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 29, no. 7, pp. 1061–1072, Jun. 2021.

[8] O. A. Uzun and S. Köse, "Converter-gating: A power efficient and secure on-chip power delivery system," *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 4, no. 2, pp. 169–179, Jun. 2014.

[9] W. Yu and S. Köse, "Charge-withheld converter-reshuffling: A countermeasure against power analysis attacks," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 63, no. 5, pp. 438–442, May 2016.

[10] R. Jevtic, M. Ylitolva, and L. Koskinen, "Reconfigurable switched capacitor DC-DC converter for improved security in IoT devices," in *Proc. 28th Int. Symp. Power Timing Model. Optim. Simul. (PATMOS)*, Jul. 2018, pp. 243–247.

[11] A. Ghosh, D. Das, and S. Sen, "Physical time-varying transfer functions as generic low-overhead power-SCA countermeasure," 2020, *arXiv:2003.07440*.

[12] C. Wang, Y. Cai, H. Wang, and Q. Zhou, "Electromagnetic equalizer: An active countermeasure against EM side-channel attack," in *Proc. ICCAD*, Nov. 2018, p. 112.

[13] D. Das *et al.*, "27.3 EM and power SCA-resilient AES-256 in 65nm CMOS through > 350X current-domain signature attenuation," in *Proc. IEEE Int. Solid-State Circuits Conf. (ISSCC)*, Feb. 2020, pp. 424–426.

[14] A. Singh, M. Kar, S. K. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "Improved power/EM side-channel attack resistance of 128-bit AES engines with random fast voltage dithering," *IEEE J. Solid-State Circuits*, vol. 54, no. 2, pp. 569–583, Feb. 2019.

[15] A. Singh, M. Kar, S. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "25.3 a 128b AES engine with higher resistance to power and electromagnetic side-channel attacks enabled by a security-aware integrated all-digital low-dropout regulator," in *Proc. IEEE Int. Solid-State Circuits Conf. (ISSCC)*, Feb. 2019, pp. 404–406.

[16] Y. Xiang *et al.*, "Open DNN box by power side-channel attack," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 67, no. 11, pp. 2717–2721, Nov. 2020.

[17] M. Guri, A. Kachlon, O. Hasson, G. Kedma, Y. Mirsky, and Y. Elovici, "GSMem: Data exfiltration from air-gapped computers over GSM frequencies," in *Proc. 24th USENIX Security Symp.*, 2015, pp. 849–864.

[18] C. Shen, T. Liu, J. Huang, and R. Tan, "When LoRa meets EMR: Electromagnetic covert channels can be super resilient," in *Proc. IEEE Symp. Security Privacy (SP)*, 2021, pp. 1304–1317.

[19] N. Sehatbakhsh, B. B. Yilmaz, A. Zajic, and M. Prvulovic, "A new side-channel vulnerability on modern computers by exploiting electromagnetic emanations from the power management unit," in *Proc. IEEE Int. Symp. High Perform. Comput. Archit. (HPCA)*, 2020, pp. 123–138.

[20] M. G. Kuhn and R. J. Anderson, "Soft tempest: Hidden data transmission using electromagnetic emanations," in *Proc. Int. Workshop Inf. Hiding*, 1998, pp. 124–142.

[21] C. Lavaud, R. Gerzaguet, M. Gautier, O. Berder, E. Nogues, and S. Molton, "Whispering devices: A survey on how side-channels lead to compromised information," *J. Hardw. Syst. Security*, vol. 5, pp. 143–168, Mar. 2021.

[22] D. J. Griffiths, *Introduction to Electrodynamics*, 4th ed. London, U.K.: Pearson, 2014.

[23] F. Durvaux and F-X. Standaert, "From Improved Leakage Detection to the Detection of Points of Interests in Leakage Traces," in *Advances in Cryptology EUROCRYPT* (Lecture Notes in Computer Science), vol. 9665. Heidelberg, Germany: Springer, May 2016, pp. 240–262. [Online]. Available: https://link.springer.com/chapter/10.1007%2F978-3-662-49890-3_10#citeas

[24] REASSURE Consortium, "Understanding leakage detection," in *Proc. Tutorial Co-Organized CARDIS*, Montpellier, France, Nov. 2018, pp. 1–34.