

Mutual Information Minimization for Side-Channel Attack Resistance via Optimal Noise Injection

Jiheon Woo*, Donggyun Ryu*, Daewon Seo[†], Young-Sik Kim[‡],
Namyoon Lee*, Yuval Cassuto[‡], and Yongjune Kim*

*Department of Electrical Engineering, POSTECH, Pohang, South Korea
Email: {jhwoo1997, dgryu, nylee, yongjune}@postech.ac.kr

[†]Department of Electrical Engineering and Computer Science, DGIST, Daegu, South Korea
Email: {dwseo, ysk}@dgist.ac.kr

[‡]Viterbi Department of Electrical and Computer Engineering, Technion – Israel Institute of Technology, Haifa, Israel
Email: ycassuto@ee.technion.ac.il

Abstract—Side-channel attacks (SCAs) pose a serious threat to system security by extracting secret keys through physical leakages such as power consumption, timing variations, and electromagnetic emissions. Among existing countermeasures, artificial noise injection is recognized as one of the most effective techniques. However, its high power consumption poses a major challenge for resource-constrained systems such as Internet of Things (IoT) devices, motivating the development of more efficient protection schemes. In this paper, we model SCAs as a communication channel and aim to suppress information leakage by minimizing the mutual information between the secret information and side-channel observations, subject to a power constraint on the artificial noise. We first consider the Gaussian input case, where the mutual information becomes the channel capacity, which is one way to quantify the information leakage. We then extend the framework to arbitrary input distributions by identifying conditions under which the optimization remains convex and by leveraging the fundamental I–MMSE relationship to derive the optimal noise allocation. Numerical results show that the proposed methods substantially reduce mutual information compared with conventional techniques, demonstrating their effectiveness for security-critical systems operating under tight power constraints.

Index Terms—Side-channel attacks, information leakage, mutual information, artificial noise injection.

I. INTRODUCTION

Side-channel attacks (SCAs) pose a serious threat to cryptographic security by targeting confidential information such as secret keys or messages through physical leakages, including power consumption, timing variations, and electromagnetic emissions [1]–[3]. These attacks exploit variations in physical characteristics during secret-dependent operations and include power-analysis attacks [4], timing attacks [5], and electromagnetic attacks [6]. Among these, power-analysis attacks are especially effective, as they rely on monitoring a device’s power consumption during cryptographic computations. By

analyzing the resulting leakage traces, attackers aim to infer secret information [5], [7].

To defend against SCAs, several countermeasures have been proposed, including artificial noise injection [8], masking [9], and hiding techniques [10]. Among these, artificial-noise injection aims to reduce the signal-to-noise ratio (SNR) of the observed leakage by adding external noise [3], [8], [11]. Although effective in principle, the approach is inefficient without careful allocation of artificial-noise power, as it typically requires noise power several times greater than the actual power consumption of encryption algorithms.

Such constraints are particularly pronounced in Internet of Things (IoT) devices, which are susceptible to SCAs due to their limited power and computational resources [12], [13]. While high-resource systems can implement artificial noise injection effectively, IoT devices often lack the capacity to support these high-overhead techniques. Consequently, they remain exposed to power-analysis attacks that exploit distinct power signatures during cryptographic operations.

We propose an artificial-noise injection method that addresses the limitations of existing approaches by using mutual information [14] as a measure of side-channel information leakage. Our approach formulates an optimization problem that minimizes the mutual information under a power constraint on the artificial noise, with particular focus on applicability to resource-constrained devices. To formulate the optimization framework under a power constraint, we need a metric that accurately quantifies information leakage. While maximal leakage [15] is a well-known metric for quantifying information leakage, the mutual information is more appropriate in the context of power-analysis attacks, as it accommodates continuous random variables typically observed in side-channel measurements. In contrast, the maximal leakage diverges under these conditions [15, Example 10].

We begin with the Gaussian input case, where the mutual information is equivalent to the channel capacity. This strategy can be interpreted as a *dual water-filling* problem, which seeks to minimize the channel capacity to enhance security—contrasting with the classical water-filling approach that aims

This work was supported by Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (RS-2024-00399401, Development of Quantum-Safe Infrastructure Migration and Quantum Security Verification Technologies) and NSF-BSF grant 2023627. (Corresponding author: Yongjune Kim.)

to maximize the total capacity of parallel Gaussian channels. We then extend our optimization framework to arbitrary input distributions. To derive the optimal solutions, we utilize the fundamental connection between mutual information and minimum mean squared error (MMSE), known as the I-MMSE relationship [16]. Compared to conventional uniform noise allocation, the proposed method significantly reduces the required artificial noise power while achieving the same level of leakage suppression.

II. SYSTEM MODEL AND BACKGROUND

A. Side-Channel Model

Suppose that the discrete uniform random variable U denotes the secret information, such as a secret key or message, and the observed side-channel output signal, e.g., power consumption, is represented by the random vector $Y^m = \{Y_i\}_{i=1}^m = (Y_1, \dots, Y_m) \in \mathbb{R}^m$. We introduce an intermediate random vector $X^m \in \mathbb{R}^m$, defined as $X^m = g(U)$, where $g(\cdot)$ is a (possibly stochastic) function that models the side-channel of the secret information. Let Z^m and N^m denote the physical and artificial noise vectors, respectively. The side-channel observation model is then given by

$$Y^m = g(U) + N^m + Z^m = X^m + N^m + Z^m, \quad (1)$$

where the power of each intermediate component is denoted by $\mathbb{E}[X_i^2] = P_i$. Both noise vectors are modeled as Gaussian distributions; specifically, $Z_i \sim \mathcal{N}(0, Z_i)$ and $N_i \sim \mathcal{N}(0, N_i)$ for $i = 1, \dots, m$. The use of Gaussian noise is theoretically justified as it minimizes the mutual information between the input and output when the input is Gaussian [14, Exercise 9.21]. From a practical perspective, modeling noise as Gaussian is widely adopted, particularly for artificial noise in countermeasures against power side-channel attacks, as demonstrated in studies such as [3], [17], [18].

B. Information Leakage Metrics for SCA

In this subsection, we introduce representative information-leakage metrics and discuss related works on SCAs.

1) *Mutual Information*: The mutual information measures the amount of information shared between two random variables. In the context of SCAs, it quantifies the information about the secret variable U revealed by the side-channel output Y^m . It is defined as

$$I(U; Y^m) = D_{\text{KL}}(P(u, y^m) || P(u)P(y^m)), \quad (2)$$

where $D_{\text{KL}}(P||Q)$ denotes the Kullback-Leibler divergence. Throughout this paper, $P(\cdot)$ denotes a general probability measure; $p(\cdot)$ and $f(\cdot)$ represent the probability mass function (pmf) of a discrete random variable and the probability density function (pdf) of a continuous random variable, respectively. The mutual information is widely adopted in both discrete and continuous settings for quantifying information leakage, due to its solid theoretical foundation and operational relevance in SCA evaluation [3], [19]. Jin *et al.* [3] adopted the Gaussian channel capacity and formulated an optimization problem to control this capacity by injecting artificial noise that is *uniformly allocated* across a subset of leakage points.

2) *Maximal Leakage*: The maximal leakage quantifies the maximum gain in an adversary's ability to guess the secret variable U after observing the side-channel output Y^m , compared to making a blind guess [15]. Let \hat{U} denote the estimate of U inferred from Y^m . The maximal leakage is defined as

$$L(X^m \rightarrow Y^m) = \sup_{U \rightarrow X^m \rightarrow Y^m \rightarrow \hat{U}} \log \left(\frac{\Pr(U = \hat{U})}{\max_u P(u)} \right). \quad (3)$$

While the maximal leakage provides a worst-case guarantee, it is not suitable for continuous variables, as it diverges in such cases [15]. In [20], the authors minimize the maximal leakage by injecting artificial delay in discrete time.

3) *Sibson Mutual Information*: The Sibson mutual information is a generalization of mutual information, parameterized by a tunable order $\alpha > 0$ [21], [22]. It is defined as

$$I_\alpha(U; Y^m) = \inf_{P(y^m)} D_\alpha(P(u, y^m) || P(u)P(y^m)), \quad (4)$$

where $D_\alpha(P||Q)$ denotes the Rényi divergence of order α . As $\alpha \rightarrow 1$, $I_\alpha(U; Y^m)$ converges to the mutual information. As $\alpha \rightarrow \infty$, it converges to the maximal leakage [15].

C. I-MMSE Relation

To analyze the optimization problem involving the mutual information for arbitrary input distributions, we leverage one of the most fundamental relationships in information theory: the I-MMSE theorem [16]. As in [16], we rewrite $Y = X + N + Z$ in normalized form as

$$\tilde{Y} = \sqrt{\rho}S + W, \quad (5)$$

where W represents the combined physical and artificial noise, and assume that S and W have unit power. The signal-to-noise ratio (SNR) is given by

$$\rho = \frac{P}{N + Z}. \quad (6)$$

As in [23], regardless of their marginal distributions, any nonzero mean of input S contributes to the power but not to the mutual information; hence, we assume zero-mean inputs without loss of generality.

The mutual information between X and Y is expressed as a function of ρ [16]:

$$I(X; Y) = I(S; \tilde{Y}) = I(\rho). \quad (7)$$

Lemma 1 (I-MMSE Relation [16]): For any input distribution, assuming a Gaussian W , the mutual information and MMSE satisfy

$$\frac{d}{d\rho} I(\rho) = \frac{1}{2} \text{mmse}(\rho) = \frac{1}{2} \mathbb{E} \left[(S - \mathbb{E}[S|\tilde{Y}; \rho])^2 \right]. \quad (8)$$

This relation enables the optimization of mutual information with respect to artificial noise allocation, even for arbitrary (non-Gaussian) inputs.

III. OPTIMAL ARTIFICIAL NOISE FOR SIDE-CHANNEL ATTACK RESISTANCE

An attacker attempts to infer the secret variable U from the side-channel observation Y^m , and our objective is to increase the probability of inference error $P_e = \Pr(U \neq \hat{U})$. According to Fano's inequality [14], the probability of inference error satisfies

$$1 + P_e \log |\mathcal{U}| \geq H(U|Y^m), \quad (9)$$

where \mathcal{U} denotes the alphabet of U . This inequality implies that a larger conditional entropy $H(U|Y^m)$ leads to a higher lower bound on P_e . Since the mutual information is defined as $I(U; Y^m) = H(U) - H(U|Y^m)$, minimizing $I(U; Y^m)$ is equivalent to maximizing $H(U|Y^m)$, which in turn increases the lower bound on the probability of inference error. Hence, we aim to minimize the mutual information $I(U; Y^m)$.

We assume that the relationship between the secret information U and the intermediate vector X^m is immutable, and the system designer has control over how Y^m is generated from X^m , as in [20]. Hence, instead of directly minimizing the mutual information $I(U; Y^m)$, we aim to minimize its upper bound, which simplifies the optimization problem. Since $U \rightarrow X^m \rightarrow Y^m$ forms a Markov chain, the following first inequality holds by the data-processing inequality, and the second follows from the chain rule:

$$I(U; Y^m) \leq I(X^m; Y^m) \leq \sum_{i=1}^m I(X_i; Y_i). \quad (10)$$

Moreover, this data-processing inequality also holds for the Sibson mutual information [22], making it applicable in more general settings involving α -parametrized leakage measures.

We aim to minimize information leakage by injecting artificial noise under a fixed artificial-noise power budget. As information-leakage metrics, we adopt the mutual information and the Sibson mutual information. However, the maximal leakage is not suitable in our setting as $Y = X + N + Z$. Note that $L(X^m \rightarrow Y^m) \rightarrow \infty$ for an additive model with continuous variables [15, Example 10].

We can then formulate the following optimization problem:

$$\begin{aligned} & \underset{\{\mathbf{N}_i\}_{i=1}^m}{\text{minimize}} && \sum_{i=1}^m I(X_i; Y_i) \\ & \text{subject to} && \sum_{i=1}^m \mathbf{N}_i \leq \mathbf{N}_0, \quad \mathbf{N}_i \geq 0, \end{aligned} \quad (11)$$

where \mathbf{N}_0 denotes the total artificial-noise power constraint. Note that from (1) each mutual information term $I(X_i; Y_i)$ is a function of \mathbf{N}_i for $i = 1, \dots, m$.

A. Gaussian Input Distribution

Similarly to [3], we adopt a sub-channel perspective, where each leakage point in the side-channel is modeled as a distinct sub-channel. The amount of leakage is quantified by the sub-channel powers, P_i for $i = 1, \dots, m$, and is assumed to be known. In addition, we assume that the variances Z_i of the physical noise are known. We focus on the case where

each input X_i follows a Gaussian distribution and aim to minimize the mutual information. For an additive Gaussian-noise channel, this mutual information equals the channel capacity. Hence, the optimization problem becomes:

$$\begin{aligned} & \underset{\{\mathbf{N}_i\}_{i=1}^m}{\text{minimize}} && \sum_{i=1}^m \frac{1}{2} \log \left(1 + \frac{P_i}{\mathbf{N}_i + Z_i} \right) \\ & \text{subject to} && \sum_{i=1}^m \mathbf{N}_i \leq \mathbf{N}_0, \quad \mathbf{N}_i \geq 0. \end{aligned} \quad (12)$$

Remark 1: The optimization problem in (12) is *convex* with respect to $\{\mathbf{N}_i\}_{i=1}^m$ since the second derivative of the objective function is non-negative.

The optimal solution can be obtained using standard convex optimization solvers. Additionally, we provide an analytical characterization of the optimal solution by applying the KKT conditions.

Theorem 1: The optimal noise allocation $\{\mathbf{N}_i^*\}_{i=1}^m$ of (12) is given by

$$\mathbf{N}_i^* = \begin{cases} 0, & \nu \geq \frac{1}{Z_i} - \frac{1}{Z_i + P_i}, \\ -\frac{(2Z_i + P_i) + \sqrt{P_i^2 + \frac{4P_i}{\nu}}}{2}, & \text{otherwise,} \end{cases} \quad (13)$$

where ν is the dual variable chosen to satisfy the condition $\sum_{i=1}^m \mathbf{N}_i = \mathbf{N}_0$. Also, for $\mathbf{N}_i^* > 0$, the optimal \mathbf{N}_i^* satisfies the following condition:

$$\frac{1}{\mathbf{N}_i^* + Z_i} - \frac{1}{\mathbf{N}_i^* + Z_i + P_i} = \nu. \quad (14)$$

Proof: The proof is given in [24]. ■

Our optimization problem in (12) can be viewed as a *dual* to the classical water-filling problem [14], which maximizes the total capacity of the parallel Gaussian channels by allocating transmit power $\{P_i\}_{i=1}^m$ across channels. In the water-filling problem, artificial noise is not considered; the optimization variables are $\{P_i\}_{i=1}^m$ for a given set of noise powers $\{Z_i\}_{i=1}^m$. For the selected channels, the optimal power allocation satisfies the condition $P_i^* + Z_i = \nu$, where ν represents the water-level. In contrast, our objective is to minimize the total capacity of parallel Gaussian channels by allocating artificial noise $\{\mathbf{N}_i\}_{i=1}^m$. For the selected points (i.e., those with non-zero artificial noise allocation), the optimal noise allocation \mathbf{N}_i^* satisfies the condition in (14), which serves as the dual counterpart to the optimal P_i^* in the water-filling solution.

The optimization problem can be extended to the setting of Sibson mutual information. According to [22], for a Gaussian channel with a Gaussian input, the Sibson mutual information for $\alpha > 0$ is given by

$$I_\alpha(X_i; Y_i) = \frac{1}{2} \log \left(1 + \alpha \cdot \frac{P_i}{\mathbf{N}_i + Z_i} \right). \quad (15)$$

Substituting (15) into (11) yields a variant of (12) with the SNR scaled by α , which remains convex as in Remark 1. The optimal solution can be derived by applying the KKT conditions.

Corollary 1: The optimal noise allocation $\{N_i^*\}_{i=1}^m$ for the optimization problem with the Sibson mutual information is given by:

$$N_i^* = \begin{cases} 0, & \nu \geq \frac{1}{Z_i} - \frac{1}{Z_i + \alpha P_i}, \\ \frac{-(2Z_i + \alpha P_i) + \sqrt{(\alpha P_i)^2 + \frac{4\alpha P_i}{\nu}}}{2}, & \text{otherwise,} \end{cases} \quad (16)$$

where ν is the dual variable. Also, for $N_i^* > 0$, the noise allocation $\{N_i^*\}_{i=1}^m$ satisfies the following condition:

$$\frac{1}{N_i^* + Z_i} - \frac{1}{N_i^* + Z_i + \alpha P_i} = \nu. \quad (17)$$

Our framework is flexible and adaptable to generalized information leakage measures, where α serves as a tunable parameter that modulates the sensitivity to signal power.

Remark 2: As $\alpha \rightarrow \infty$, the Sibson mutual information converges to the maximal leakage [15]. However, in the case of Gaussian inputs and additive Gaussian noise, the maximal leakage becomes unbounded, since (15) diverges as $\alpha \rightarrow \infty$. Therefore, the maximal leakage is not suitable for Gaussian settings.

B. Arbitrary Input Distribution

In this subsection, we investigate the optimization problem in (11) under the assumption that the input signals follow an arbitrary distribution. Although our objective is to derive an optimal solution for arbitrary input distributions, the optimization problem in general is not convex in this setting. To facilitate tractable optimization, we first establish sufficient conditions under which the problem becomes convex.

Theorem 2: The mutual information $I(S; \tilde{Y})$ (equiv. $I(X; Y)$) is convex in N if and only if one of the following (equivalent) conditions is satisfied for the variable $\rho = \frac{P}{N+Z} > 0$.

$$(C1) \quad \text{mmse}(\rho) + \frac{\partial}{\partial \rho} (\rho \cdot \text{mmse}(\rho)) \geq 0, \quad (18)$$

$$(C2) \quad \frac{d}{d\rho} \left(\rho \cdot \mathcal{J}(\tilde{Y}) \right) \leq 1, \quad (19)$$

$$(C3) \quad \mathbb{E} \left[\left(\frac{d^2}{d\tilde{Y}^2} \log f(\tilde{Y}) \right)^2 \right] \leq 1, \quad (20)$$

where $\mathcal{J}(\tilde{Y}) = \mathbb{E} \left[\left(\frac{d}{d\tilde{Y}} \log f(\tilde{Y}) \right)^2 \right]$ is the Fisher information.

Proof: The proof is given in [24]. \blacksquare

Example 1 (Gaussian Input): Consider the case where both the input and the noise are Gaussian. In this case, $\tilde{Y} \sim \mathcal{N}(0, 1+\rho)$, which leads to $\text{mmse}(\rho) = \frac{1}{1+\rho}$. Substituting this into (C1), we verify that the convexity conditions are satisfied.

Example 2 (Binary Input): The MMSE for binary input $S \in \{\pm 1\}$ with equal probability is given in [23] as follows:

$$\text{mmse}(\rho) = 1 - \int_{-\infty}^{\infty} \frac{e^{-y^2/2}}{\sqrt{2\pi}} \tanh(\rho - \sqrt{\rho} y) dy. \quad (21)$$

We observe that the binary input violates (C1); in particular, (18) is negative when $\rho > 3.35$. Thus, the optimization problem (11) is non-convex.

Example 3 (Exponential Input): For an exponential input distribution, the output follows an exponentially modified Gaussian distribution [25], which satisfies (C3). Thus, the optimization problem (11) is convex.

Proof: The proof is given in [24]. \blacksquare

If the optimization problem (11) is convex, we can obtain the global optimal solution using the I-MMSE relation and the KKT conditions.

Theorem 3: For an arbitrary input distribution that satisfies conditions in Theorem 2, the optimal noise allocation $\{N_i\}_{i=1}^m$ is given by

$$N_i = 0, \quad \text{if } \nu \geq \delta_i, \quad (22)$$

$$\frac{P_i}{(N_i + Z_i)^2} \cdot \text{mmse} \left(\frac{P_i}{N_i + Z_i} \right) = \nu, \quad \text{otherwise,} \quad (23)$$

where ν is a dual variable of the corresponding KKT conditions and $\delta_i = \frac{P_i}{Z_i^2} \cdot \text{mmse} \left(\frac{P_i}{Z_i} \right)$.

Proof: The proof is given in [24]. \blacksquare

Remark 3: If $I(\rho_i)$ is convex in N_i , then $\nu = \frac{P_i}{(N_i + Z_i)^2} \cdot \text{mmse} \left(\frac{P_i}{N_i + Z_i} \right)$ is nonincreasing in N_i because this quantity equals $-\frac{\partial}{\partial N_i} I(\rho_i)$.

The optimal artificial noise allocation can be obtained through the following three-step procedure:

- 1) Compute the MMSE function corresponding to the given input distribution.
- 2) Solve for the dual variable ν using (22) and (23) under the constraint $\sum_{i=1}^m N_i = N_0$. This step can be carried out efficiently using a bisection method by leveraging Remark 3.
- 3) Determine the optimal noise allocation $\{N_i\}_{i=1}^m$ based on the computed value of ν .

Example 4 (Gaussian Input): We can obtain the optimal solution for a Gaussian input distribution using Theorem 3. The MMSE of a Gaussian input is $\text{mmse} \left(\frac{P_i}{N_i + Z_i} \right) = \frac{N_i + Z_i}{N_i + Z_i + P_i}$. Using Theorem 3, the optimal solution can be derived as follows:

$$N_i^* = 0, \quad \text{if } \nu \geq \frac{1}{Z_i} - \frac{1}{Z_i + P_i}, \quad (24)$$

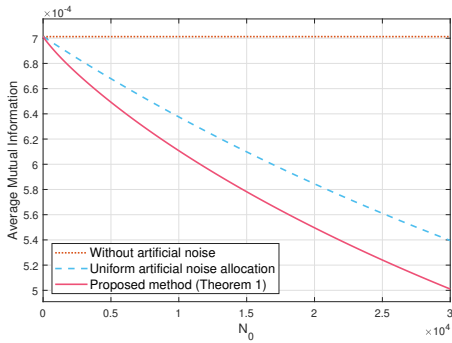
$$\frac{1}{N_i^* + Z_i} - \frac{1}{N_i^* + Z_i + P_i} = \nu, \quad \text{otherwise.} \quad (25)$$

Note that (25) is identical to (14) of Theorem 1.

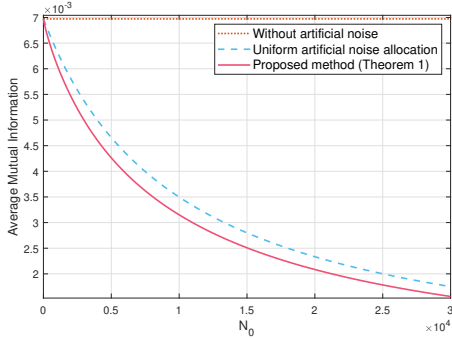
For a broad class of input distributions, the MMSE function has been extensively studied in the context of Gaussian channels [23], thereby enabling the computation of the corresponding optimal solution.

C. Low-SNR Regime

An analysis of the optimization problem in the low-SNR regime reveals useful properties. Specifically, as the SNR approaches zero, the mutual information of the Gaussian



(a)



(b)

Fig. 1. Comparison of mutual information under the proposed method and uniform artificial noise allocation with $X_i \sim \mathcal{N}(0, P_i)$ and $P_i \sim \mathcal{N}(1, 0.5^2)$, where P_i is truncated to ensure nonnegativity: (a) $Z_i = 1000$, (b) $Z_i = 100$.

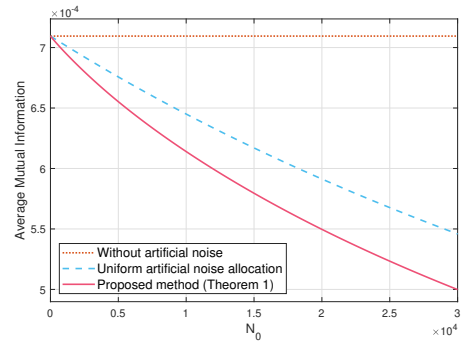
channel is convex in the artificial noise for any input distribution. Following the analysis in [26], the second-order Taylor series expansion of the MMSE for a Gaussian channel around $\rho = 0^+$ is given by

$$\text{mmse}(\rho) = 1 - \rho + (2 - \mathbb{E}[S^3]^2) \frac{\rho^2}{2} + \mathcal{O}(\rho^3). \quad (26)$$

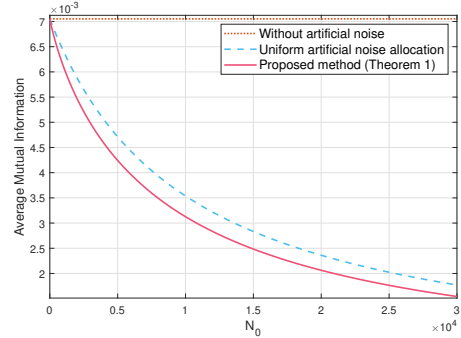
This expansion satisfies (C1) of Theorem 2, indicating that the objective function is always convex in the low-SNR regime. Consequently, the optimization problem remains convex regardless of the input distribution, ensuring that optimal solutions can be obtained for both Gaussian and non-Gaussian inputs. Note that the SCA scenario typically corresponds to the low-SNR regime. Even for the binary input signal in Example 2, the problem is convex when $\rho < 3.35 \approx 5.25$ dB, which lies in the low-SNR regime.

IV. NUMERICAL RESULTS

In this section, we evaluate the effectiveness of the proposed optimal artificial noise allocation. Specifically, we compare three approaches: (1) no artificial-noise allocation, (2) uniform artificial-noise allocation, and (3) optimized artificial-noise allocation. According to [11], the average current consumption during advanced encryption standard (AES) operations is approximately 1 mA, while effective artificial noise injection requires about 17 mA. Given that power scales with the square of current under constant resistance, this corresponds to a power ratio of approximately 1 : 300. Based on this,



(a)



(b)

Fig. 2. Comparison of average (total) mutual information under the proposed method and uniform artificial noise allocation with $X_i \sim \mathcal{N}(0, P_i)$ and $P_i \sim \mathcal{U}[0, 2]$: (a) $Z_i = 1000$, (b) $Z_i = 100$.

the average power consumption is normalized to 1, and the average power of artificial noise is varied from 0 to 300. To evaluate the impact of artificial noise, we vary the total noise power $N_0 = \sum_{i=1}^m N_i$ from 0 to $300 \times m$, with $m = 100$. To reflect a range of practical scenarios, the input powers P_i are randomly drawn from either Gaussian or uniform distributions.

Fig. 1 corresponds to the case where P_i is sampled from a Gaussian distribution, while Fig. 2 considers a uniform distribution. Specifically, to achieve a 50% reduction in the average mutual information, the proposed method requires 19.14%, and 17.92% less artificial noise power than the uniform allocation in Fig. 1(a), and (b), respectively. Similarly, the proposed method reduces the artificial noise power by 22.29%, and 21.13% in Fig. 2(a), and (b), respectively. These results indicate that the proposed method significantly improves noise power efficiency compared to uniform noise allocation, which is particularly critical for resource-constrained devices. Additional numerical results are provided in [24].

V. CONCLUSION

We presented a principled information-theoretic framework for protecting cryptographic systems from power-analysis attacks through optimal artificial-noise injection. Our approach aims to minimize the mutual information for arbitrary input distributions, including the Gaussian case, and we derive the corresponding optimal solution. Numerical results show that our proposed method reduces the mutual information more effectively than conventional uniform allocation.

REFERENCES

- [1] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst. (CHES)*, Aug. 2004, pp. 16–29.
- [2] K. Gandolfi, C. Moutrel, and F. Olivier, "Electromagnetic analysis: Concrete results," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst. (CHES)*, May 2001, pp. 251–261.
- [3] S. Jin, M. Xu, R. Bettati, and M. Christodorescu, "Optimal energy efficient design of artificial noise to prevent side-channel attacks," in *Proc. IEEE Int. Workshop Inf. Forensics Security (WIFS)*, Dec. 2022, pp. 1–6.
- [4] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. Int. Cryptol. Conf. (CRYPTO)*, Aug. 1999, pp. 388–397.
- [5] P. C. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," in *Proc. Int. Cryptol. Conf. (CRYPTO)*, Aug. 1996, pp. 104–113.
- [6] M. A. Al Faruque, S. R. Chhetri, A. Canedo, and J. Wan, "Acoustic side-channel attacks on additive manufacturing systems," in *Proc. IEEE/ACM Int. Conf. Cyber-Phys. Syst. (ICCCPS)*, Apr. 2016, pp. 1–10.
- [7] N. Gattu, M. N. I. Khan, A. De, and S. Ghosh, "Power side channel attack analysis and detection," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design (ICCAD)*, Nov. 2020, pp. 1–7.
- [8] A. Shamir, "Protecting smart cards from passive power analysis with detached power supplies," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst. (CHES)*, Aug. 2000, pp. 71–77.
- [9] E. Prouff and M. Rivain, "Masking against side-channel attacks: A formal security proof," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, May 2013, pp. 142–159.
- [10] N. Veyrat-Charvillon, M. Medwed, S. Kerckhof, and F.-X. Standaert, "Shuffling against side-channel attacks: A comprehensive study with cautionary note," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Security (ASIACRYPT)*, Dec. 2012, pp. 740–757.
- [11] D. Das, S. Maity, S. B. Nasir, S. Ghosh, A. Raychowdhury, and S. Sen, "ASNI: Attenuated signature noise injection for low-overhead power side-channel attack immunity," *IEEE Trans. Circuits Syst. I*, vol. 65, no. 10, pp. 3300–3311, Oct. 2018.
- [12] M. Arsath K F, V. Ganesan, R. Bodduna, and C. Rebeiro, "PARAM: A microprocessor hardened for power side-channel attack resistance," in *Proc. IEEE Int. Symp. Hardware Oriented Secur. (HOST)*, Dec. 2020, pp. 23–34.
- [13] P. Socha, V. Miškovský, and M. Novotný, "A comprehensive survey on the non-invasive passive side-channel analysis," *Sensors*, vol. 22, no. 21, pp. 1–37, Oct. 2022.
- [14] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. Hoboken, NJ: Wiley-Interscience, Jul. 2006.
- [15] I. Issa, A. B. Wagner, and S. Kamath, "An operational approach to information leakage," *IEEE Trans. Inf. Theory*, vol. 66, no. 3, pp. 1625–1657, May 2020.
- [16] D. Guo, S. Shamai, and S. Verdú, "Mutual information and minimum mean-square error in Gaussian channels," *IEEE Trans. Inf. Theory*, vol. 51, no. 4, pp. 1261–1282, Apr. 2005.
- [17] P. Gan, P. Ravi, K. Raj, A. Bakshi, and A. Chattopadhyay, "Classic McEliece hardware implementation with enhanced side-channel and fault resistance," *Cryptology ePrint Archive, Paper 2024/1828*, Nov. 2024.
- [18] T. Güneysu and A. Moradi, "Generic side-channel countermeasures for reconfigurable devices," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst. (CHES)*, Sep. 2011, pp. 33–48.
- [19] B. Gierlichs, L. Batina, P. Tuyls, and B. Preneel, "Mutual information analysis: A generic side-channel distinguisher," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst. (CHES)*, Aug. 2008, pp. 426–442.
- [20] B. Wu, A. B. Wagner, and G. E. Suh, "A case for maximal leakage as a side channel leakage metric," *arXiv:2004.08035*, Apr. 2020.
- [21] R. Sibson, "Information radius," *Z. Wahrscheinlichkeitstheorie Verw. Geb.*, vol. 14, no. 2, pp. 149–160, Jun. 1969.
- [22] S. Verdú, " α -mutual information," in *Proc. Inf. Theory Appl. Workshop (ITA)*, Feb. 2015, pp. 1–6.
- [23] A. Lozano, A. M. Tulino, and S. Verdú, "Optimum power allocation for parallel Gaussian channels with arbitrary input distributions," *IEEE Trans. Inf. Theory*, vol. 52, no. 7, pp. 3033–3051, Jul. 2006.
- [24] J. Woo, D. Seo, Y.-S. Kim, N. Lee, Y. Cassuto, and Y. Kim, "Mutual information minimization for side-channel attack resistance via optimal noise injection," *arXiv preprint arXiv:2504.20556*, 2025. [Online]. Available: <https://arxiv.org/abs/2504.20556>
- [25] E. Grushka, "Characterization of exponentially modified Gaussian peaks in chromatography," *Anal. Chem.*, vol. 44, no. 11, pp. 1733–1738, Sep. 1972.
- [26] D. Guo, Y. Wu, S. S. Shitz, and S. Verdú, "Estimation in Gaussian noise: properties of the minimum mean-square error," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2371–2385, Mar. 2011.