Lower Bounds for Leakage-Resilient Secret-Sharing Schemes against Probing Attacks

Donald Q. Adams*, Hemanta K. Maji*, Hai H. Nguyen*, Minh L. Nguyen*,
Anat Paskin-Cherniavsky†, Tom Suad†, and Mingyuan Wang*
*Purdue University {adams391, hmaji, nguye245, nguye330, wang1929}@purdue.edu
†Ariel University anatpc@ariel.ac.il, tom.suad@msmail.ariel.ac.il

2021 IEEE International Symposium on Information Theory (ISIT) | 978-1-5386-8209-8/21/$31.00 ©2021 IEEE | DOI: 10.1109/ISIT45174.2021.9518230

***Abstract*—Historically, side-channel attacks have revealed partial information about the intermediate values and secrets of computations to compromise the security of cryptographic primitives. The objective of leakage-resilient cryptography is to model such avenues of information leakage and study techniques to realize them securely. This work studies the local leakage-resilience of prominent secret-sharing schemes like Shamir's secret-sharing scheme and the additive secret-sharing scheme against probing attacks that leak physical-bits from the memory hardware storing the secret shares.**

Consider the additive secret-sharing scheme among k parties over a prime field such that the prime needs λ-bits for its binary representation, where λ is the security parameter. We prove that k must be at least $\omega(\log \lambda / \log\log \lambda)$ for the scheme to be secure against even one physical-bit leakage from each secret share. This result improves the previous state-of-the-art result where an identical lower bound was known for one-bit general leakage from each secret share (Benhamouda, Degwekar, Ishai, and Rabin, CRYPTO–2018).

This lower bound on the reconstruction threshold extends to Shamir's secret-sharing scheme if one does not carefully choose the evaluation places for generating the secret shares. For this scheme, our result additionally improves another lower bound on the reconstruction threshold k of Shamir's secret-sharing scheme (Nielsen and Simkin, EUROCRYPT–2020) when the total number of parties is $\mathcal{O}(\lambda \log \lambda / \log\log \lambda)$.

Our work provides the analysis of the recently-proposed (explicit) physical-bit leakage attack of Maji, Nguyen, Paskin-Cherniavsky, Suad, and Wang (EUROCRYPT–2021), namely the "parity of parity" attack. This analysis relies on lower-bounding the "discrepancy" of the Irwin-Hall probability distribution.

A full version of this paper is accessible at: https://www.cs.purdue.edu/homes/hmaji/papers/AMNNPSW21.pdf

I. Introduction

Typically, the design and analysis of cryptographic primitives assume cryptosystems as impervious black-boxes, faithfully realizing the desired input-output behavior while providing no additional information. However, real-world implementations and deployments have repetitively proven this assumption to be false. Beginning with the works of [1], [2], several innovative side-channel attacks reveal partial information about the intermediate values and stored secrets of computations (for introductory exposition, refer to [3]–[8]). These diverse side-channel attacks on fundamental cryptographic building blocks pose a threat to the security of all cryptographic constructions incorporating them.

To address these concerns, one designs mechanical countermeasures, hardware solutions, and algorithmic representations to mitigate known threats [9]–[14]. More generally, *leakage-resilient cryptography* formally models such potential avenues of information leakage (even encompassing attacks beyond those already known) and securely realizes cryptographic primitives against adversaries augmented to leverage these leakage attacks. In the last few decades, a large body of highly influential research has studied the feasibility and efficiency of realizing leakage-resilient variants of fundamental cryptographic primitives against active/passive adversaries performing leakage statically/adaptively (refer to the excellent recent survey [15]).

One such fundamental cryptographic primitive is *threshold secret-sharing schemes* – an essential component of nearly all threshold cryptography. A side-channel attack on a secret-sharing scheme provides the adversary (some restricted or noisy) access to every party's secret share. For instance, a passive adversary can leak a few bits from every secret share. Consequently, this joint leakage may get correlated with the secret; thus, compromising its secrecy. This model is a significant divergence from the (so-called) standard model where an adversary gets access to only some corrupted parties' shares. In general, our understanding of the leakage-resilience of secret-sharing schemes is in a nascent state. The exact characterization of the leakage-resilience of even prominent secret-sharing schemes like Shamir's secret-sharing scheme and the additive secret-sharing scheme are not well-understood.

A *locally leakage-resilient secret-sharing scheme* ensures the following guarantee. A (static) adversary chooses leakage functions for all the secret shares. However, the observed leakage's joint distribution is statistically independent of the secret. Intriguingly, this research direction is closely related to the fascinating problem of efficiently reconstructing secret shares of error-correcting codes. For example, the reconstruction algorithm for Reed-Solomon codes by Guruswami and Wootters [16] (and follow-up works [17]–[20]) demonstrates

Hemanta K. Maji, Hai H. Nguyen, and Mingyuan Wang are supported in part by an NSF CRII Award CNS–1566499, NSF SMALL Awards CNS–1618822 and CNS–2055605, the IARPA HECTOR project, MITRE Innovation Program Academic Cybersecurity Research Awards (2019–2020, 2020–2021), a Purdue Research Foundation (PRF) Award, and The Center for Science of Information, an NSF Science and Technology Center, Cooperative Agreement CCF–0939370.

Anat Paskin-Cherniavsky is supported by the Ariel Cyber Innovation Center in conjunction with the Israel National Cyber directorate in the Prime Minister's Office.

that leaking even one-bit from each secret share of Shamir's secret-sharing over a characteristic 2 field renders it insecure. At the outset, achieving leakage-resilience appears to be a challenging task. For example, the leakage-resilience of Shamir's secret-sharing scheme over prime fields, even when the adversary leaks $m = 1$ bit from each secret share, is known only for reconstruction threshold $k \geqslant 0.867n$ [21], [22], where n is the number of parties. The primary hurdle stems from the fact that the leakage need not entirely determine the secret; revealing any partial information of the secret suffices to preclude leakage-resilience.

This work studies the resilience of Shamir's secret-sharing scheme and the additive secret-sharing scheme when the secret shares, which are elements of an arbitrary finite field, are stored in their natural *binary representation* in memory hardware. As in the seminal work of Ishai, Sahai, and Wagner [23], the adversary chooses a bounded number of positions to probe each of the hardware storing the secret shares. The adversary receives a noisy version of the bit stored at that physical address from each probe, where the noise depends on the device's thermal noise characteristic (see, for example, [24] for motivation). Furthermore, the particular choice of the physical-bit leakage draws inspiration from, for instance, the crucial role of the studies on oblivious transfer combiners [25]–[29] in furthering the state-of-the-art of general correlation extractors [30]–[32], and the techniques in protecting circuits against probing attacks [23], [33], [34] impacting the study of leakage-resilient secure computation [15].

Summary of our work. Our work's objective is to lower-bound the reconstruction threshold for Shamir's secret-sharing scheme and the additive secret-sharing scheme as a function of the statistical indistinguishability parameter and the thermal noise parameter. Towards this objective, we study the quality of local physical-bit leakage attacks on these secret-sharing schemes [35]. Our technical contribution is the analysis of the "parity of parity" leakage attack proposed in [35]. This analysis proceeds by lower-bounding the "discrepancy of the Irwin-Hall distribution," which may be of independent interest.

II. Our Contribution

This section introduces some informal definitions to facilitate the presentation of our results.

Notation. Fix a prime field F of order p. The elements of F are naturally represented as λ-bit binary strings corresponding to the elements $\{0, 1, \ldots, p-1\}$, where $2^{\lambda-1} < p \leqslant 2^{\lambda}$. For $\ell \in \{1, 2, \ldots, \lambda\}$, one can probe the bit at the ℓ-th least significant position from a λ-bit representation of an element of F. For example, $\ell = 1$ indexes to the least significant bit and $\ell = \lambda$ indexes to the most significant bit of the element's binary representation.

Our work shall consider secret-sharing schemes among n parties with a reconstruction threshold k. The secret and the secret shares are all elements of F. For asymptotic results, as per convention, the security parameter is λ, the number of bits representing the secret and the secret shares.

This work considers a (static) adversary who requests $m = 1$ physical-bit leakage from each secret share. Therefore, the adversary chooses the leakage function $(\ell_1, \ell_2, \ldots, \ell_n)$, such that $\ell_i \in \{1, \ldots, \lambda\}$, for all $1 \leqslant i \leqslant n$. For $1 \leqslant i \leqslant n$, let b_i represent the ℓ_i-th bit in the i-th secret share.

For $1 \leqslant i \leqslant n$, let $\rho_i \in [0, 1]$ be the thermal noise parameter of the hardware storing the i-th secret share. Let $\widetilde{b}_i$ be a bit that is ρ_i-*correlated* with the bit b_i. That is, $\widetilde{b}_i = b_i$ with probability ρ_i; otherwise, $\widetilde{b}_i$ is an independent and uniformly random bit. For example, if $\rho_i = 1$, then $\widetilde{b}_i = b_i$, and, if $\rho_i = 0$, then $\widetilde{b}_i$ is a uniformly random bit independent of the bit b_i. Intuitively, if the storage hardware has high thermal noise, then $\widetilde{b}_i$ is less correlated with the actual bit b_i.

A secret-sharing scheme is $(1-\varepsilon)$-*secure locally leakage-resilient* secret-sharing scheme against one physical-bit probing attacks, if, for all secrets $s^{(0)}, s^{(1)} \in F$, the leakage distributions $\left(\widetilde{b}_1, \ldots, \widetilde{b}_k \middle| s^{(0)}\right)$ and $\left(\widetilde{b}_1, \ldots, \widetilde{b}_k \middle| s^{(1)}\right)$ have statistical distance $\leqslant \varepsilon$. As per convention, the ε of a secure secret-sharing scheme decays faster than any inverse-polynomial in the security parameter λ, represented as $\varepsilon = \mathsf{negl}(\lambda)$.

Additive secret-sharing scheme results. Let $\mathsf{AddSS}(k)$ be the additive secret-sharing scheme over the finite field F among $n = k$ parties. This secret-sharing scheme provides the k parties uniformly random secret shares from F conditioned on the fact that their sum is the secret $s \in F$. Section 6 of the full version proves the following technical result.

Theorem 1 (Distinguishing Advantage of the "Parity of Parity" Leakage Attack)**.** *Let $\ell_i = 1$, for all $i \in \{1, \ldots, k\}$. There exists two secrets $s^{(0)}, s^{(1)} \in F$ such that the statistical distance between the leakage distributions $\left(\widetilde{b}_1, \ldots, \widetilde{b}_k \middle| s^{(0)}\right)$ and $\left(\widetilde{b}_1, \ldots, \widetilde{b}_k \middle| s^{(1)}\right)$ is*

$$\varepsilon \geqslant \left(\prod_{i=1}^{k} \rho_i\right) \cdot \left(\frac{1}{2^k (k-1)!} - \frac{3(k-1)^2 + 1}{p}\right).$$

In particular, when k is even,[1]

$$\varepsilon \geqslant \left(\prod_{i=1}^{k} \rho_i\right) \cdot \left(\frac{1}{2(k-1)!} - \frac{3(k-1)^2 + 1}{p}\right).$$

We shall interpret this theorem for reconstruction thresholds k such that $2^k k! \ll p/k^2$. To interpret this theorem, consider the simplification $\rho_i = \rho$, a constant, for all $i \in \{1, \ldots, k\}$. For this simplification, the lower bound in the expression above, essentially, reduces to $\varepsilon \geqslant \Theta\left(\frac{(\rho/2)^k}{(k-1)!}\right)$. When $\rho = 1$, the bound above is equivalent to $k \geqslant \Theta\big(\Gamma^{-1}(1/\varepsilon)\big) = \Theta(\log(1/\varepsilon)/\log\log(1/\varepsilon))$. More generally, if all $\rho_i = \rho$, then the bound is equivalent to $k \geqslant \Theta(\log(1/\varepsilon)/(\log\log(1/\varepsilon) + \log(2/\rho)))$.

For the simplicity of presentation, we use $\rho_i = 1$ to derive the corollaries below.

[1]The distinction between odd and even k arises from the intervals of interest having non-integer endpoints. Refer to Section V for the definition of the intervals of interest.

Corollary 1. *Let* $\mathsf{AddSS}(k)$ *is* $(1-\mathsf{negl}(\lambda))$*-secure locally leakage-resilient secret-sharing scheme against one physical-bit leakage from each secret share. Then, it must be the case that* $k = \omega(\log \lambda / \log\log \lambda)$.

For the additive secret-sharing scheme, the only previously known lower bound on k is by [21]. Their bounds are in terms of the number of parties k, which they treat as the security parameter. [35] and our work decouple the number of parties k from the number of bits λ in the binary representation of the prime p, the security parameter in our work. The analysis technique of [21], in the setting where k and λ are decoupled, implies an identical lower bound on k by leaking one bit from every secret share. One can simulate this *general* one-bit leakage by leaking $m = \log k$ physical-bits from each secret share. However, in contrast, our attack only leaks one (noisy) physical-bit, a significantly weaker leakage attack and, consequently, a more serious security threat. As an aside, we remark that our distinguishing advantage $\frac{1}{2^k(k-1)!} \geqslant \frac{1}{k^k}$, the distinguishing advantage of [21], for all $k \geqslant 2$.

Shamir secret-sharing scheme results. $\mathsf{ShamirSS}(n, k, \vec{X})$ represents Shamir's secret-sharing scheme among n parties, reconstruction threshold k, and evaluation places $\vec{X} = (X_1, \ldots, X_n)$. The evaluation places $X_1, \ldots, X_n$ are distinct elements of F^*. Let $s \in F$ be the secret. The secret-sharing scheme picks a random polynomial $f(Z) \in F[Z]/Z^k$ conditioned on the fact that $f(0) = s$. For $i \in \{1, \ldots, n\}$, the i-th secret share is $f(X_i)$.

We prove that, for some adversarially chosen evaluation places, the "Parity of Parity" leakage attack on Shamir's secret-sharing scheme behaves similarly as that on the additive secret-sharing schemes (refer to Section V-C). Therefore, it achieves a similar advantage in distinguishing the secrets. In particular, we prove the following corollary.

Corollary 2. *Let* $p = 1 \mod k$ *and* $\alpha \in F^*$ *be such that* $\{\alpha, \alpha^2, \ldots, \alpha^k = 1\} \subseteq F^*$ *is the set of* k *roots of the equation* $Z^k - 1 = 0$. *Suppose there exists* $\beta \in F^*$ *such that* $\{\beta\alpha, \beta\alpha^2, \ldots, \beta\alpha^k = \beta\}$ *is a subset of the evaluation places* $\vec{X}$. *If* $\mathsf{ShamirSS}(n, k, \vec{X})$ *is* $(1-\mathsf{negl}(\lambda))$*-secure locally leakage-resilient secret-sharing scheme against one physical-bit leakage from each secret share, then it must be the case that* $k = \omega(\log \lambda / \log\log \lambda)$.

Intuitively, the corollary states that if one chooses any coset F^*/G among the evaluation places, where $G = \{\alpha, \alpha^2, \ldots, \alpha^k = 1\}$ is an order k multiplicative subgroup of F^*, then the reconstruction threshold k must be high.

This corollary demonstrates that one has to be careful in choosing the prime p, reconstruction threshold k, and the evaluation places $\vec{X}$; otherwise, Shamir's secret-sharing scheme is vulnerable to even $m = 1$ physical-bit leakage from every secret share. The only previously known attack on Shamir's secret-sharing scheme with arbitrary evaluation places $\vec{X}$ is by [36]; however, their leakage is *not* explicit.[2]

Suppose one is not careful in choosing the parameters of the $\mathsf{ShamirSS}$ and they satisfies the preconditions of the corollary. For a comparison with known leakage attacks, let us restrict to $m = 1$ bit leakage attack from every secret share. [36] implies that $k \geqslant n/(\lambda+1) \sim n/\lambda$ using a leakage attack that is not explicit. Consequently, for $n = O(\lambda \log \lambda / \log\log \lambda)$, our bound improves the lower bound on k. [35] proved that the attack of [21] on the additive secret-sharing scheme extends to Shamir's secret-sharing scheme.[3] Therefore, similar to the discussion above for the additive secret-sharing scheme, our leakage attack (relying only on noisy physical-bit leakage) implies an identical lower bound as [21].

III. Background and State-of-the-art Results

Following the recent work of Benhamouda, Degwekar, Ishai, and Rabin [21] (also, independently, introduced by [37] as an intermediate primitive), there has been a sequence of works analyzing the leakage-resilience of prominent secret-sharing schemes and constructing new leakage-resilient secret-sharing schemes (refer to the full version for the references). The sequel summarizes the most relevant state-of-the-art results specific to Shamir's secret-sharing scheme and the additive secret-sharing scheme, which are the focus of this work. A leakage attack has *distinguishing advantage* ε if there are two secrets such that the joint distributions of the leakage on the secret shares have statistical distance (at least) ε.

General Leakage. Guruswami and Wooters [16], presented an attack that leaks $m = 1$ bit from each secret share and has distinguishing advantage $\varepsilon = 1$ for Shamir's secret-sharing scheme over any characteristic 2 field. Subsequently, for the additive secret-sharing scheme over prime fields, [21] presented an attack that leaks $m = 1$ bit from every secret share and achieves a distinguishing advantage of $\varepsilon = 1/k^k$. [22] extended this attack to any Massey secret-sharing scheme [38] corresponding to a linear error-correcting code (over prime fields) such that some subset of k parties can reconstruct the secret. In particular, this attack extends to Shamir's secret-sharing scheme, which is the Massey secret-sharing scheme corresponding to (punctured) Reed-Solomon codes, with reconstruction threshold k.

Nielsen and Simkin [36] present a probabilistic argument to construct a leakage attack on any secret-sharing scheme. For Shamir's secret-sharing scheme among n parties with reconstruction threshold k, their result implies the existence of a leakage function and a secret such that the leakage is consistent only with that particular secret with probability (at least) $1/2$. Their attack needs $m \geqslant \frac{k \log p}{n-k}$ bits of leakage from

[2] In more detail, [36] showed that when one picks the leakage function as a random function, the probability of a unique secret being consistent with the observed leakage is significant and, hence, a random function has a significant advantage in distinguishing this unique secret from any other secret. However, they did not present one deterministic leakage function that witnesses a significant advantage. Instead, they gave a distribution over such functions.

[3] However, the leakage function is highly sophisticated compared to physical-bit leakage. It needs to perform finite field multiplications.

each secret share. Consequently, their proof-strategy does not extend to the case when $n = k$ (for example, the additive secret-sharing scheme).

Physical-bit Leakage. Suppose the secret and its secret shares are elements of a prime field of order p. Consider the scenario where each party stores their secret share in its natural (fixed length) binary representation corresponding to the integers $\{0, 1, 2, \ldots, p-1\}$, and the adversary may (independently) probe m physical-bits from each secret share. For clarity, the presentation in this section ignores the thermal noise parameter. The attack of [21], [22] on the additive secret-sharing scheme among k parties performs one-bit general leakage from each secret share and achieves a distinguishing advantage of (roughly) $\varepsilon = 1/k^k$. One can simulate this attack using $m = \lceil \lg k \rceil$ physical-bit leakage by probing the m most significant bits of each secret share. Maji et al. [35] observed that any leakage attack on the additive secret-sharing scheme among k parties extends to Shamir's secret-sharing scheme with reconstruction threshold k, if the evaluation places to generate the secret shares are not chosen cautiously.

Maji et al. [35] introduce a new physical-bit leakage attack, namely, the "parity of parities" attack, on the additive secret-sharing scheme that leaks only $m = 1$ bit (the least significant bit) from each secret share. They analyze this attack for the special cases of $k = 2$ and $k = 3$ and prove that the advantage of the attack is (roughly) $\varepsilon = 1/2$ and $\varepsilon = 1/4$, respectively, for any prime p. For a few larger values of k, they presented empirical evidence supporting the conjectured quality of this physical-bit leakage attack. Our work resolves their conjecture in the positive and proves that the advantage is (roughly) $\varepsilon = 1/k!$, for all $k \in \mathbb{N}$.

IV. Parity of Parity Attack

This section summarizes the "parity of parity" attack of Maji et al. [35] on the additive secret-sharing scheme.

Let F be a prime field of order $p > 2$. Consider the additive secret-sharing scheme $\mathsf{AddSS}(k)$ among k parties. Let $s \in F$ be the secret, and $s_1, \ldots, s_k \in F$ be the secret shares. Conditioned on the secret s, the secret shares $s_1, \ldots, s_{k-1}$ are independent and uniformly random over F, and $s_k = s - (s_1 + \cdots + s_{k-1})$.

The "parity of parity" attacker chooses the leakage function $(\ell_1, \ldots, \ell_k) = (1, \ldots, 1)$. That is, the leakage $(b_1, \ldots, b_k)$ are the least significant bits of the secret shares $(s_1, \ldots, s_k)$. The idea of the attack is to identify a secret $s \in F$ such that the correlation between the least significant bit of s and the bit $b_1 \oplus \cdots \oplus b_k$ is maximized. [35] explicitly computed the s that maximized the correlation for $k = 2$ and $k = 3$, and experimentally supported their conjecture that this correlation is lower bound by an exponential decreasing function of k.

V. Technical Overview

At the outset, it suffices to assume the thermal noise parameter $\rho_i = 1$, for all $i \in \{1, \ldots, n\}$. That is, the leaked bit $\widetilde{b}_i$ is identical to the stored bit b_i at the hardware location ℓ_i that the adversary probes, for all $1 \leqslant i \leqslant n$. After that, one can reintroduce the thermal noise parameter into the analysis at the end (see Section V-D).

Let $\mathbb{N}_0 := \{0, 1, 2, \ldots\}$ be the set of all non-negative integers. Consider $\mathsf{AddSS}(k)$ over a prime field F of order $p > 2$. Recall that the secret shares $s_1, \ldots, s_{k-1} \in F$ are independent and uniformly random over F, and the secret share $s_k = s - (s_1 + \cdots + s_{k-1})$, where $s \in F$ is the secret. We interpret $s_1, \ldots, s_k$ as elements from the set $\{0, 1, \ldots, p-1\} \subseteq \mathbb{N}_0$. Let the corresponding elements be $S_1, \ldots, S_k \in \mathbb{N}_0$.

Now, we have the following identity over $\mathbb{N}_0$. For any secret $s \in \{0, 1, \ldots, p-1\}$ and secret shares $S_1, \ldots, S_k$, there exists some $i \in \mathbb{N}_0$, such that

$$S_1 + S_2 + \cdots + S_k = s + ip.$$

An integer has parity 0 if it is even; otherwise, if it is odd, its parity is 1. Observe that $b_1 \oplus b_2 \oplus \cdots \oplus b_k$ is the parity of $S_1 + S_2 + \cdots + S_k$, which is identical to the parity of the secret s if and only if i is even.

Define the following two partitions of the set $\mathbb{N}_0$.

$$S_{\mathsf{same}}(s) := \mathbb{N}_0 \cap \bigcup_{\substack{i \in \mathbb{Z} \\ i \text{ odd}}} [ip + s + 1, (i+1)p + s]$$

$$S_{\mathsf{diff}}(s) := \mathbb{N}_0 \cap \bigcup_{\substack{i \in \mathbb{Z} \\ i \text{ even}}} [ip + s + 1, (i+1)p + s]$$

Observe that if $S_1 + S_2 + \cdots + S_{k-1} \in S_{\mathsf{same}}(s)$ then $b_1 \oplus \cdots \oplus b_k$ will be identical to the parity of s. Furthermore, if $S_1 + S_2 + \cdots + S_{k-1} \in S_{\mathsf{diff}}(s)$ then $b_1 \oplus \cdots \oplus b_k$ will be the complement of the parity of s.

Our objective is to solve the following optimization problems. The probability below is over the independent and uniformly random choices of $S_1, \ldots, S_{k-1} \in \{0, 1, \ldots, p-1\}$.

$$s^{(0)} := \underset{s \in \{0, \ldots, p-1\}}{\arg\max} \Big| \Pr[S_1 + \cdots + S_{k-1} \in S_{\mathsf{same}}(s)] - \Pr[S_1 + \cdots + S_{k-1} \in S_{\mathsf{diff}}(s)] \Big|$$

$$\varepsilon := \max_{s \in \{0, \ldots, p-1\}} \Big| \Pr[S_1 + \cdots + S_{k-1} \in S_{\mathsf{same}}(s)] - \Pr[S_1 + \cdots + S_{k-1} \in S_{\mathsf{diff}}(s)] \Big|$$

This formulation of the problem has the salient feature that $S_1, \ldots, S_{k-1}$ are independent and uniformly random over the set $\{0, 1, \ldots, p-1\}$.[4] One concludes that there exists a bit $b \in \{0, 1\}$ such that

$$\Pr[b_1 \oplus b_2 \oplus \cdots \oplus b_k = b] = \frac{1 + \varepsilon}{2},$$

where $s_1, \ldots, s_k$ are the secret shares of the secret $s^{(0)}$.

On the other hand, for a random secret s, the secret shares $s_1, \ldots, s_k$ are uniformly and independently chosen random elements of F. Therefore, $b_1, \ldots, b_k$ are independent bits of

[4]The $|\cdot|$ sign in the expressions is necessary because for some k the probability difference may be non-positive for every secret s.

bias $1/p$. Consequently, by convolution, the bias of the bit $b_1 \oplus \cdots \oplus b_k$ is $1/p^k$. That is,

$$\Pr[b_1 \oplus b_2 \oplus \cdots \oplus b_k = b] \leqslant \frac{1}{2} + \frac{1}{p^k}.$$

By an averaging argument, there exists a secret $s^{(1)}$ such that when $s_1, \ldots, s_k$ are secret shares of $s^{(1)}$ we have

$$\Pr[b_1 \oplus b_2 \oplus \cdots \oplus b_k = b] \leqslant \frac{1}{2} + \frac{1}{p^k} \leqslant \frac{1}{2} + \frac{1}{p}.$$

Consequently, one concludes that the statistical distance between the distributions $\left(b_1, \ldots, b_k \middle| s^{(0)}\right)$ and $\left(b_1, \ldots, b_k \middle| s^{(1)}\right)$ is at least $\frac{\varepsilon}{2} - \frac{1}{p}$. All that remains is to prove that ε is sufficiently large, which is the technical contribution of our work. The proof follows two high-level steps. First, Section V-A presents the calculation of the "discrepancy of Irwin-Hall distribution" (a terminology introduced in [35]). Finally, Section V-B characterizes the slight loss in the lower bound when transitioning from the Irwin-Hall distribution to the actual (discrete) probability distribution.

A. Normalization: Irwin-Hall Distribution

Let us normalize the $S_{\mathsf{same}}(s)$ and $S_{\mathsf{diff}}(s)$ by scaling the length-p intervals into length-one intervals. Define $\widehat{\mathbb{N}}_0 = \{0, 1/p, 2/p, \ldots\}$, represented by $\frac{1}{p} \cdot \mathbb{N}_0$. Let $\widehat{s} = s/p \in \{0, 1/p, 2/p, \ldots, (p-1)/p\}$. Next, define $\widehat{S}_{\mathsf{same}}(\widehat{s}) = \frac{1}{p} \cdot S_{\mathsf{same}}(s)$ and $\widehat{S}_{\mathsf{diff}}(\widehat{s}) = \frac{1}{p} \cdot S_{\mathsf{diff}}(s)$. Let $\widehat{S}_1, \widehat{S}_2, \ldots, \widehat{S}_{k-1}$ be independent and uniformly random distributions over the set $\{0, 1/p, 2/p, \ldots, (p-1)/p\}$. Our objective is to find

$$\varepsilon := \max_{\widehat{s} \in \{0, 1/p, \ldots, (p-1)/p\}} \left| \Pr\left[\widehat{S}_1 + \cdots + \widehat{S}_{k-1} \in \widehat{S}_{\mathsf{same}}(\widehat{s})\right] - \Pr\left[\widehat{S}_1 + \cdots + \widehat{S}_{k-1} \in \widehat{S}_{\mathsf{diff}}(\widehat{s})\right] \right|.$$

Next, consider the simplification $p \to \infty$. For this simplification, observe that (1) $\widehat{s} \in [0, 1)$, and (2) $\widehat{S}_1, \ldots, \widehat{S}_{k-1}$ are independent and uniformly random distribution over $[0, 1)$. The distribution $\widehat{S}_1 + \cdots + \widehat{S}_{k-1}$ is the well-studied *Irwin-Hall distribution* with parameter $(k-1)$ [39], represented by IH_{k-1}, over the sample space $[0, k-1)$. For $x \in [0, 1)$, observe that

$$\widehat{S}_{\mathsf{same}}(x) := x + \left(\bigcup_{\substack{i \in \mathbb{Z} \\ i \text{ odd}}} (i, i+1] \right)$$

$$\widehat{S}_{\mathsf{diff}}(x) := x + \left(\bigcup_{\substack{i \in \mathbb{Z} \\ i \text{ even}}} (i, i+1] \right)$$

Therefore, our objective is to lower-bound the expression

$$\varepsilon := \max_{x \in [0,1)} \left| \Pr\left[\mathsf{IH}_{k-1} \in \widehat{S}_{\mathsf{same}}(x)\right] - \Pr\left[\mathsf{IH}_{k-1} \in \widehat{S}_{\mathsf{diff}}(x)\right] \right|,$$

namely the *discrepancy* of the Irwin-Hall distribution.

The non-triviality is to prove that this expression is positive. If the expression is guaranteed to be positive, then ε is at least $1/(k-1)!$ when $(k-1)$ is odd; otherwise, if $(k-1)$ is even, then $\varepsilon \geqslant 1/\left(2^{k-1}(k-1)!\right)$. This result follows from the probability mass distribution function of the Irwin-Hall probability distribution (refer to Section 4 of the full version).

B. Additive Secret-Sharing Scheme: Lower Bound

The analysis in Section V-A assumed $p \to \infty$. Our objective is to translate this analysis for the lower bound of ε to any finite p. Towards this objective, we prove that for any positive integer p and k, the k^{th} Irwin-Hall distribution is at most k/p far from the k convolutions of the discrete uniform distribution over the set $\{0, 1/p, \ldots, (p-1)/p\}$. This observation suffices to prove that the discrepancy of the Irwin-Hall distribution and the discrete distribution are (at most) k^2/p far in absolute value (refer to Section 5 of the full version for details).

C. Shamir's Secret-Sharing Scheme: Lower Bound

Let F be a prime field of order $p = 1 \mod k$ and $\alpha \in F^*$ be an element such that $G = \{\alpha, \alpha^2, \ldots, \alpha^k = 1\} \subseteq F^*$ be the set of all k roots of the equation $Z^k - 1 = 0$. Observe that G is a multiplicative subgroup of F^*. Consider any $\beta \in F^*$ such that $\beta G = \{\beta\alpha, \ldots, \beta\alpha^k = \beta\}$ is a coset in F^*/G.

Consider $\mathsf{ShamirSS}(n, k, \vec{X})$ such that the evaluation places $\vec{X}$ contains βG. Next, for any $j \in \{1, 2, \ldots, k-1\}$, the following identity holds

$$\sum_{x \in \beta G} x^j = 0.$$

Fix a secret $s \in F$. Let $f(Z) \in F[Z]/Z^k$ be an arbitrary polynomial with F-coefficients of degree $< k$ such that $f(0) = s$. Based on the identity above, one concludes that

$$\sum_{x \in \beta G} f(x) = ks.$$

Without loss of generality, assume that we have evaluation places $X_1 = \beta\alpha, X_2 = \beta\alpha^2, \ldots, X_k = \beta\alpha^k = \beta$. So, the conclusion above implies that the sum of the secret shares $s_1, s_2, \ldots, s_k$ is ks. Furthermore, the secret shares $s_1, s_2, \ldots, s_{k-1}$ are uniformly random over F for $\mathsf{ShamirSS}$ with reconstruction threshold k. These two properties are identical to the properties of the additive secret-sharing scheme that we leverage in our leakage attack. Since $x \mapsto kx$ is an automorphism over F when $k \in \{1, 2, \ldots, p-1\}$, the leakage attack on the additive secret-sharing scheme carries over to Shamir's secret-sharing scheme.

D. Thermal Noise Parameter

Suppose δ is the advantage in predicting the parity of the secret $s^{(0)}$ from Section V, where there was no thermal noise. Now, assume that instead of b_i our predictor instead uses $\widetilde{b}_i$, which is ρ_i-correlated with the actual physical-bit b_i, for some $\rho_i \in [0, 1]$. In this case, relying on results on the noise operator in discrete Boolean function analysis [40], the advantage of the new predictor is $\rho_i\delta$. Consequently, if the leakage bits $\widetilde{b}_1, \ldots, \widetilde{b}_k$ are, respectively, $\rho_1, \ldots, \rho_k$ correlated with the actual physical bits $b_1, \ldots, b_k$, then the advantage of the predictor using the noisy bits is $\left(\prod_{i=1}^k \rho_i\right)\delta$.

REFERENCES

[1] P. C. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," in *CRYPTO'96*, ser. LNCS, N. Koblitz, Ed., vol. 1109. Springer, Heidelberg, Aug. 1996, pp. 104–113. 1

[2] P. C. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *CRYPTO'99*, ser. LNCS, M. J. Wiener, Ed., vol. 1666. Springer, Heidelberg, Aug. 1999, pp. 388–397. 1

[3] E. Oswald and B. Preneel, "A survey on passive side-channel attacks and their countermeasures for the nessie public-key cryptosystems," *NESSIE public reports, https://www. cosic. esat. kuleuven. ac. be/nessie/reports*, 2003. 1

[4] F. Koeune and F. Standaert, "A tutorial on physical security and side-channel attacks," in *Foundations of Security Analysis and Design III, FOSAD 2004/2005 Tutorial Lectures*, 2004. 1

[5] Y. Zhou and D. Feng, "Side-channel attacks: Ten years after its publication and the impacts on cryptographic module security testing," Cryptology ePrint Archive, Report 2005/388, 2005, http://eprint.iacr.org/2005/388. 1

[6] S. Bhunia and M. Tehranipoor, *Hardware security: a hands-on learning approach*, 2018. 1

[7] A. P. Sayakkara, N. Le-Khac, and M. Scanlon, "A survey of electromagnetic side-channel attacks and discussion on their case-progressing potential for digital forensics," *Digit. Investig.*, 2019. 1

[8] M. Randolph and W. Diehl, "Power side-channel attack analysis: A review of 20 years of study for the layman," *Cryptogr.*, 2020. 1

[9] R. M. Avanzi, "Side channel attacks on implementations of curve-based cryptographic primitives," Cryptology ePrint Archive, Report 2005/017, 2005, http://eprint.iacr.org/2005/017. 1

[10] I. F. Blake, G. Seroussi, and N. P. Smart, *Advances in elliptic curve cryptography*, 2005. 1

[11] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren, Eds., *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, 2005. 1

[12] J. Fan, X. Guo, E. D. Mulder, P. Schaumont, B. Preneel, and I. Verbauwhede, "State-of-the-art of secure ECC implementations: A survey on known side-channel attacks and countermeasures," in *HOST 2010, Proceedings of the 2010 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 13-14 June 2010, Anaheim Convention Center, California, USA*, 2010. 1

[13] J. Fan and I. Verbauwhede, "An updated survey on secure ECC implementations: Attacks, countermeasures and cost," in *Cryptography and Security: From Theory to Applications - Essays Dedicated to Jean-Jacques Quisquater on the Occasion of His 65th Birthday*, 2012. 1

[14] R. Abarzúa, C. Valencia, and J. López, "Survey for performance & security problems of passive side-channel attacks countermeasures in ECC," Cryptology ePrint Archive, Report 2019/010, 2019, https://eprint.iacr.org/2019/010. 1

[15] Y. T. Kalai and L. Reyzin, "A survey of leakage-resilient cryptography," in *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*, O. Goldreich, Ed., 2019. 1, 2

[16] V. Guruswami and M. Wootters, "Repairing reed-solomon codes," in *48th ACM STOC*, D. Wichs and Y. Mansour, Eds. ACM Press, Jun. 2016, pp. 216–226. 1, 3

[17] I. Tamo, M. Ye, and A. Barg, "Optimal repair of reed-solomon codes: Achieving the cut-set bound," in *58th FOCS*, C. Umans, Ed. IEEE Computer Society Press, Oct. 2017, pp. 216–227. 1

[18] V. Guruswami and A. S. Rawat, "MDS code constructions with small sub-packetization and near-optimal repair bandwidth," in *28th SODA*, P. N. Klein, Ed. ACM-SIAM, Jan. 2017, pp. 2109–2122. 1

[19] H. Dau, I. M. Duursma, H. M. Kiah, and O. Milenkovic, "Repairing reed-solomon codes with multiple erasures," *IEEE Trans. Inf. Theory*, 2018. 1

[22] H. K. Maji, A. Paskin-Cherniavsky, T. Suad, and M. Wang, "On leakage-resilient secret sharing," Cryptology ePrint Archive, Report 2020/1517, 2020, https://eprint.iacr.org/2020/1517. 2, 3, 4

[20] J. Mardia, B. Bartan, and M. Wootters, "Repairing multiple failures for scalar MDS codes," *IEEE Trans. Inf. Theory*, 2019. 1

[21] F. Benhamouda, A. Degwekar, Y. Ishai, and T. Rabin, "On the local leakage resilience of linear secret sharing schemes," in *CRYPTO 2018, Part I*, ser. LNCS, H. Shacham and A. Boldyreva, Eds., vol. 10991. Springer, Heidelberg, Aug. 2018, pp. 531–561. 2, 3, 4

[23] Y. Ishai, A. Sahai, and D. Wagner, "Private circuits: Securing hardware against probing attacks," in *CRYPTO 2003*, ser. LNCS, D. Boneh, Ed., vol. 2729. Springer, Heidelberg, Aug. 2003, pp. 463–481. 2

[24] S. Chari, C. S. Jutla, J. R. Rao, and P. Rohatgi, "Towards sound approaches to counteract power-analysis attacks," in *CRYPTO'99*, ser. LNCS, M. J. Wiener, Ed., vol. 1666. Springer, Heidelberg, Aug. 1999, pp. 398–412. 2

[25] D. Harnik, J. Kilian, M. Naor, O. Reingold, and A. Rosen, "On robust combiners for oblivious transfer and other primitives," in *EUROCRYPT 2005*, ser. LNCS, R. Cramer, Ed., vol. 3494. Springer, Heidelberg, May 2005, pp. 96–113. 2

[26] R. Meier, B. Przydatek, and J. Wullschleger, "Robuster combiners for oblivious transfer," in *TCC 2007*, ser. LNCS, S. P. Vadhan, Ed., vol. 4392. Springer, Heidelberg, Feb. 2007, pp. 404–418. 2

[27] D. Harnik, Y. Ishai, E. Kushilevitz, and J. B. Nielsen, "OT-combiners via secure computation," in *TCC 2008*, ser. LNCS, R. Canetti, Ed., vol. 4948. Springer, Heidelberg, Mar. 2008, pp. 393–411. 2

[28] Y. Ishai, H. K. Maji, A. Sahai, and J. Wullschleger, "Single-use ot combiners with near-optimal resilience," in *ISIT*, 2014. 2

[29] I. Cascudo, I. Damgård, O. Farràs, and S. Ranellucci, "Resource-efficient OT combiners with active security," in *TCC 2017, Part II*, ser. LNCS, Y. Kalai and L. Reyzin, Eds., vol. 10678. Springer, Heidelberg, Nov. 2017, pp. 461–486. 2

[30] Y. Ishai, E. Kushilevitz, R. Ostrovsky, and A. Sahai, "Extracting correlations," in *50th FOCS*. IEEE Computer Society Press, Oct. 2009, pp. 261–270. 2

[31] A. R. Block, H. K. Maji, and H. H. Nguyen, "Secure computation based on leaky correlations: High resilience setting," in *CRYPTO 2017, Part II*, ser. LNCS, J. Katz and H. Shacham, Eds., vol. 10402. Springer, Heidelberg, Aug. 2017, pp. 3–32. 2

[32] A. R. Block, D. Gupta, H. K. Maji, and H. H. Nguyen, "Secure computation using leaky correlations (asymptotically optimal constructions)," in *TCC 2018, Part II*, ser. LNCS, A. Beimel and S. Dziembowski, Eds., vol. 11240. Springer, Heidelberg, Nov. 2018, pp. 36–65. 2

[33] Y. Ishai, M. Prabhakaran, A. Sahai, and D. Wagner, "Private circuits II: Keeping secrets in tamperable circuits," in *EUROCRYPT 2006*, ser. LNCS, S. Vaudenay, Ed., vol. 4004. Springer, Heidelberg, May / Jun. 2006, pp. 308–327. 2

[34] A. Duc, S. Dziembowski, and S. Faust, "Unifying leakage models: From probing attacks to noisy leakage," in *EUROCRYPT 2014*, ser. LNCS, P. Q. Nguyen and E. Oswald, Eds., vol. 8441. Springer, Heidelberg, May 2014, pp. 423–440. 2

[35] H. K. Maji, H. H. Nguyen, A. Paskin-Cherniavsky, T. Suad, and M. Wang, "Leakage-resilient secret-sharing schemes against physical-bit leakage," in *EUROCRYPT*, 2021, https://www.cs.purdue.edu/homes/hmaji/papers/MNPSW20.pdf. 2, 3, 4, 5

[36] J. B. Nielsen and M. Simkin, "Lower bounds for leakage-resilient secret sharing," in *EUROCRYPT 2020, Part I*, ser. LNCS, A. Canteaut and Y. Ishai, Eds., vol. 12105. Springer, Heidelberg, May 2020, pp. 556–577. 3

[37] V. Goyal and A. Kumar, "Non-malleable secret sharing," in *50th ACM STOC*, I. Diakonikolas, D. Kempe, and M. Henzinger, Eds. ACM Press, Jun. 2018, pp. 685–698. 3

[38] J. L. Massey, "Some applications of code duality in cryptography," *Mat. Contemp*, vol. 21, no. 187-209, p. 16th, 2001. 3

[39] N. L. Johnson, S. Kotz, and N. Balakrishnan, *Continuous univariate distributions, volume 2*. John wiley & sons, 1995, vol. 289. 5

[40] R. O'Donnell, *Analysis of Boolean Functions*. Cambridge University Press, 2014. 5