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 Mingyuan Wang

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 proposed by 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.

1 Introduction

Typically, the design and analysis of cryptographic primitives proceed by assuming 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 [Koc96, KJJ99], several innovative side-channel attacks reveal partial information about the intermediate values and stored secrets of computations (for introductory exposition, refer to [OP03, KS04, ZF05, BT18, SLS19, RD20]). 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 can design mechanical countermeasures, hardware solutions, and algorithmic representations to mitigate known threats [Ava05, BSS05, CFA$^+$05, FGM$^+$10, FV12, AVL19]. 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 that perform leakage statically/adaptively (refer to the excellent recent survey [KR19]).

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 [GW16, GW17] (and follow-up works [TYB17, GR17, DDKM18, MBW19]) demonstrates 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 $k \geqslant 0.867n$ [BDIR18, MPSW20], 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. Similar to the seminal work of Ishai, Sahai, and Wagner [ISW03], 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, [CJRR99] 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 [HKN$^+$05, MPW07, HIKN08, IMSW14, CDFR17] in furthering the state-of-the-art of general correlation extractors [IKOS09, BMN17, BGMN18], and the techniques in protecting circuits against probing attacks [ISW03, IPSW06, DDF14] impacting the study of leakage-resilient secure computation [KR19]. There has also been a vast literature studying security against an active adversary, who changes the values of the wires inside a cryptosystem (for example, *non-malleable codes* against bit-wise tampering functions [DPW10, CG14, AGM$^+$15a, AGM$^+$15b]).

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 noise parameter.

1.1 Background and State-of-the-art Results

Following the recent work of Benhamouda, Degwekar, Ishai, and Rabin [BDIR18] (also, independently, introduced by [GK18] as an intermediate primitive), there has been a sequence of works analyzing the leakage-resilience of prominent secret-sharing schemes [HIMV19, CGN19, LCG$^+$20, MPSW20, MNP$^+$21] and constructing new leakage-resilient secret-sharing schemes [BPRW16, ADN$^+$19, SV19, BS19, KMS19, BIS19, FY19, FY20, HVW20, CGG$^+$20, MSV20]. 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 appropriate secrets such that the joint distributions of the leakage on the secret shares have statistical distance (at least) ε.

General Leakage. Guruswami and Wooters [GW16, GW17] 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 finite field. Subsequently, for the additive secret-sharing scheme over prime fields, [BDIR18] presented an attack that leaks $m = 1$ bit from every secret share and achieves a distinguishing advantage of $\varepsilon = 1/k^k$. [MPSW20] extended this attack to any Massey secret-sharing scheme [Mas01] 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 [NS20] 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 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 [BDIR18, MPSW20] 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. [MNP+21] observed that any leakage attack on the additive secret-sharing scheme among k parties also 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. [MNP+21] 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 $k \in \mathbb{N}$.

1.2 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 in the representation of 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.

We say that a secret-sharing scheme is $(1-\varepsilon)$-*secure locally leakage-resilient* secret-sharing scheme against $m = 1$ physical-bit probe 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 at most ε. As per convention, a secure secret-sharing scheme requires ε to decay faster than any inverse-polynomial in the security parameter λ, represented as $\varepsilon = \mathsf{negl}(\lambda)$.

Additive secret-sharing scheme results. $\mathsf{AddSS}(k)$ 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 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* $\left(\widetilde{b}_1,\dots,\widetilde{b}_k \middle| s^{(0)}\right)$ *and* $\left(\widetilde{b}_1,\dots,\widetilde{b}_k \middle| s^{(1)}\right)$ *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,* $\varepsilon \geqslant \left(\prod_{i=1}^{k}\rho_i\right)\cdot\left(\frac{1}{2(k-1)!}-\frac{3(k-1)^2+1}{p}\right)$.

To interpret this theorem, it is instructive to consider the simplification $\rho_i = \rho$, a constant, for all $i \in \{1,\dots,k\}$. For this simplification, the lower bound in the expression above, essentially, reduces to $\varepsilon \geqslant \Theta\left(\frac{(\rho/2)^k}{(k-1)!}\right)$ for all meaningful values of $k = \mathsf{poly}(\lambda)$. When $\rho = 1$, the bound above is equivalent to $k \geqslant \Theta\left(\Gamma^{-1}(1/\varepsilon)\right) = \Theta(\log(1/\varepsilon)/\log\log(1/\varepsilon))$. 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.

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 [BDIR18]. They proved 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 [BDIR18], 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 $\vec{X} = (X_1,\dots,X_n)$. The evaluation places $X_1,\dots,X_n$ 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 $i \in \{1,\dots,n\}$, the i-th secret share is $f(X_i)$.

Corollary 2. *Let* $p = 1 \mod k$ *and* $\alpha \in F^*$ *be such that* $\{\alpha,\alpha^2,\dots,\alpha^k = 1\} \subseteq F^*$ *is the set of all roots of the equation* $Z^k - 1 = 0$*. Suppose there exists* $\rho \in F^*$ *such that* $\{\rho\alpha,\rho\alpha^2,\dots,\rho\alpha^k = \rho\}$ *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 $G = \{\alpha,\alpha^2,\dots,\alpha^k = 1\}$ 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. For a general Shamir's secret sharing scheme, the only known attack is by [NS20]; however, their leakage function is *not* explicit.

Suppose one is not careful in choosing the parameters of the $\mathsf{ShamirSS}$ and it 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. [NS20] 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. [MNP+21] proved that the attack of [BDIR18] on the additive secret-sharing scheme extends to Shamir's secret sharing scheme. Therefore, similar to the discussion above for the additive secret-sharing scheme, our leakage attack relies on (noisy) physical-bit leakage attack to achieve as identical lower bound as [BDIR18].

1.3 Parity of Parity Attack

This section summarizes the "parity of parity" attack of Maji et al. [MNP+21] 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 $s_1, \dots, s_k \in F$ be the secret shares. Conditioned on the secret s, the secret shares $s_1, \dots, s_{k-1}$ 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 $(\ell_1, \dots, \ell_k) = (1, \dots, 1)$. That is, the leakage $(b_1, \dots, b_k)$ are the least significant bits of the secret shares $(s_1, \dots, s_k)$. 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. [MNP+21] 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.

2 Technical Overview

At the outset, it suffices to assume $\rho_i = 1$, for all $i \in \{1, \dots, n\}$. 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 2.4).

Let $\mathbb{N}_0 := \{0, 1, 2, \dots\}$ 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 $s_1, \dots, s_{k-1} \in F$ 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 $s_1, \dots, s_k$ as elements from the set $\{0, 1, \dots, p-1\} \subseteq \mathbb{N}_0$. Let the corresponding elements be $S_1, \dots, S_k \in \mathbb{N}_0$.

Now, we have the following identity over $\mathbb{N}_0$. For any secret $s \in \{0, 1, \dots, p-1\}$ and secret shares $S_1, \dots, S_k$, 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 $S_1, \dots, S_{k-1} \in \{0, 1, \dots, p-1\}$.

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

This formulation of the problem has the salient feature that $S_1, \dots, S_{k-1}$ are independent and uniformly random over the set $\{0, 1, \dots, p-1\}$.[1] 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 $s_1, \dots, s_k$ are the secret shares of the secret $s^{(0)}$.

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

On the other hand, for a random secret s, the secret shares $s_1, \dots, s_k$ are uniformly and independently random elements of F. Therefore, $b_1, \dots, b_k$ are independent bits of 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 $s_1, \dots, s_k$ 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 $\left(b_1, \dots, b_k \middle| s^{(0)}\right)$ and $\left(b_1, \dots, b_k \middle| s^{(1)}\right)$ 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 2.1 presents the calculation of "discrepancy of Irwin-Hall distribution" (a terminology introduced in [MNP+21]). Finally, Section 2.2 characterizes the slight loss in the lower bound when transitioning from the Irwin-Hall distribution to the actual probability distribution.

2.1 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 $\widehat{\mathbb{N}}_0 = \{0, 1/p, 2/p, \dots\}$, represented by $\frac{1}{p} \cdot \mathbb{N}_0$. Let $\widehat{s} = s/p \in \{0, 1/p, 2/p, \dots, (p-1)/p\}$. 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 $\widehat{S}_1, \widehat{S}_2, \dots, \widehat{S}_{k-1}$ be independent and uniformly random distributions over the set $\{0, 1/p, 2/p, \dots, (p-1)/p\}$. Therefore, our objective is to find

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

Next, consider the simplification $p \to \infty$. For this simplification, observe that (1) $\widehat{s} \in [0, 1)$, and (2) $\widehat{S}_1, \dots, \widehat{S}_{k-1}$ 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 $(k-1)$ [JKB95], represented by IH_{k-1} over the sample space $[0, k-1)$. For $x \in [0, 1)$, observe that

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

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

2.2 Additive Secret-Sharing Scheme: Lower Bound

The analysis in Section 2.1 assumed $p \to \infty$. Our objective is to translate this analysis for the lower bound of ε to any finite p. Towards this objectively, 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 $\{0, 1/p, \dots, (p-1)/p\}$. This is sufficient to prove that the discrepancy of the Irwin-Hall distribution and the discrete distribution are (at most) k^2/p far. These results are summarized in Section 5.

2.3 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 $\rho \in F^*$ such that $\rho G = \{\rho\alpha, \ldots, \rho\alpha^k = \rho\}$ is a coset in F^*/G.

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

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

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

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

Without loss of generality, assume that the evaluation places $X_1 = \rho\alpha, X_2 = \rho\alpha^2, \ldots, X_k = \rho\alpha^k = \rho$ are the evaluation places. So, the conclusion above implies that the sum of the secret shares $1, 2, \ldots, k$ is ks. Furthermore, the secret shares $1, 2, \ldots, k-1$ 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, for all $k \in \{1, 2, \ldots, p-1\}$, the leakage attack on the additive secret-sharing scheme carries over to Shamir's secret-sharing scheme.

2.4 Thermal Noise Parameter

Suppose δ is the advantage in predicting the parity of the secret $s^{(0)}$ from Section 2, 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 [O'D14], 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 $\left(\prod_{i=1}^k \rho_i\right) \delta$.

3 Explicit Probing Attack of Maji et al. [MNP+21]

In this section, let us recall a probing attack on Shamir's secret sharing proposed recently by [MNP+21].

Let $p \in \mathbb{N}$ be a prime number and let F be the prime field of order p. Let $k \in \mathbb{N}$ be an odd integer satisfying that $p = 1 \mod k$. Consequently, equation $X^k - 1 = 0$ has k roots in the multiplicative group F^*. Let $\alpha \in F^*$ be such that $\{\alpha, \alpha^2, \ldots, \alpha^k = 1\} \subseteq F^*$ is the set of roots of the equation $X^k - 1 = 0$.

Consider the Shamir secret sharing scheme with k parties and threshold k, where the evaluation places are an arbitrary coset of $F^*/\{\alpha, \alpha^2, \ldots, \alpha^k\}$. In particular, the secret shares are sampled as follows. Let s represent the secret and let $\rho \in F^*$ be an arbitrary element. A random polynomial $f \in F[X]$ of degree $< k$ is sampled conditioned on that $f(0) = s$. For any $i \in \{1, 2, \ldots, k\}$, the i^{th} party shall get $s_i := f\left(\rho \cdot \alpha^i\right) \in F$ as its secret share. We assume s_i is stored in binary representation as an element from $\{0, 1, \ldots, p-1\}$.

Consider the following probing attack against this scheme. The attack shall leak the least significant bit (LSB, in short) from each share. Let b_i be the LSB of the i^{th} share s_i. In what follows, we shall explain why the parity of b_i, i.e., $b_1 \oplus b_2 \oplus \cdots \oplus b_k$, gives the attacker an advantage in predicting the secret s.

Recall that $\{\alpha, \alpha^2, \ldots, \alpha^k\}$ is the set of solutions of the equation $X^k - 1 = 0$. Therefore, by Vieta's formulas and Newton's identities, we have that, for any integer $0 < j < k$, $(\alpha)^j + \left(\alpha^2\right)^j + \cdots + \left(\alpha^k\right)^j = 0$. Hence, we have

$$s_1 + s_2 + \cdots + s_k = f(\rho \cdot \alpha) + f\left(\rho \cdot \alpha^2\right) + \cdots + f\left(\rho \cdot \alpha^k\right) = ks.$$

Therefore, the secret shares $s_1, \ldots, s_k$ satisfy the following properties.

1. $s_1, s_2, \ldots, s_{k-1}$ are uniformly random over the set F;

2. $s_1 + s_2 + \cdots + s_k = ks$.

Let $\mathbb{N}_0 := \{0, 1, 2, \ldots\}$ be the set of whole numbers (i.e., all non-negative integers). Let $0 \leqslant S_1, S_2, \ldots, S_k \leqslant p-1$ be elements from $\mathbb{N}_0$ corresponding to the elements $s_1, s_2, \ldots, s_k \in F$. Similarly, let $0 \leqslant S \leqslant p-1$ be elements from $\mathbb{N}_0$ corresponding to the secret s. We rely on this notation to make it explicit that $S_1 + S_2 + \cdots + S_{k-1}$ and $k \cdot S = \overbrace{S + S + \cdots + S}^{k\text{-times}}$, are integer additions; instead of over the field F. Define the following partitions of the integers,

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

We have the following claim.

Claim 1 (Parity of the "Parity of Shares")**.** *If $S_1 + S_2 + \cdots + S_{k-1} \in S_{\mathsf{same}}$, then $b_1 \oplus b_2 \oplus \cdots \oplus b_k$ is identical to the parity of kS; Otherwise, $S_1 + S_2 + \cdots + S_{k-1} \in S_{\mathsf{diff}}$ and $b_1 \oplus b_2 \oplus \cdots \oplus b_k$ is opposite to the parity of kS.*

Proof. Since $s_1 + s_2 + \cdots + s_k = ks$, we have

$$S_1 + S_2 + \cdots + S_k = kS + ip,$$

for some integer i.

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 kS if and only if i is even.

Finally, note that since $S_k \in \{0, 1, \ldots, p-1\}$, $S_1 + S_2 + \cdots + S_k = kS + ip$ for some even i is equivalent to that

$$S_1 + S_2 + \cdots + S_{k-1} \in S_{\mathsf{same}}.$$

□

Given this claim, our objective is to find a secret s^* such that difference between $\Pr[S_1 + S_2 + \cdots + S_{k-1} \in S_{\mathsf{same}}]$ and $\Pr[S_1 + S_2 + \cdots + S_{k-1} \in S_{\mathsf{diff}}]$ is large and hence the advantage in predicting the parity of s^* is large.

In particular, we shall pick secret s^* as $(p-1)/2$.[2] For this particular choice of secret, we define

$$S^*_{\mathsf{same}} := \mathbb{N}_0 \cap \bigcup_{\substack{i \in \mathbb{Z} \\ i \text{ odd}}} \left[ip + \frac{k(p-1)}{2} + 1, (i+1)p + \frac{k(p-1)}{2}\right],$$
$$S^*_{\mathsf{diff}} := \mathbb{N}_0 \cap \bigcup_{\substack{i \in \mathbb{Z} \\ i \text{ even}}} \left[ip + \frac{k(p-1)}{2} + 1, (i+1)p + \frac{k(p-1)}{2}\right].$$

And we are interested in

$$\mathsf{disc}\,(k-1, p) \;:=\; \Pr[S_1 + S_2 + \cdots + S_{k-1} \in S^*_{\mathsf{same}}] - \Pr[S_1 + S_2 + \cdots + S_{k-1} \in S^*_{\mathsf{diff}}].$$

Naturally, $|\mathsf{disc}\,(k-1,p)|$ is the bias of the output of this probing attack when the secret is $s^* = (p-1)/2$. Note that, for a random secret s, the probability difference between s is even and s is odd is $1/p$. Therefore, the bias of the output of this probing attack is at most $1/p$. Hence, we have the following theorem.

Theorem 2. *There exist two secrets $s^{(0)}, s^{(1)} \in F$ such that this probing attack can distinguish between $s^{(0)}$ and $s^{(1)}$ with advantage $\geqslant |\mathsf{disc}\,(k-1,p)| - 1/p$.*

[2] To give some intuitions for this choice, note that

$$\mathbb{E}[S_1 + S_2 + \cdots + S_{k-1}] = \mu := (k-1)(p-1)/2.$$

We aim to set s^* such that the sequence $\{(k-2)(p-1)/2, (k-2)(p-1)/2 + 1, \ldots, k(p-1)/2\}$, the middle value of which is μ, belong entirely to either S_{same} or S_{diff}. Therefore, we shall pick s^* as $(p-1)/2$.

Roadmap. In the rest of this paper, we shall show that $|\mathsf{disc}\,(k-1,p)|$ is large. Towards this objective, we consider the normalized version of this problem. That is, let $S_1, S_2, \ldots, S_{k-1}$ be uniform distribution over $\{0, 1/p, 2/p, \ldots, (p-1)/p\}$. Correspondingly, we normalize S^*_{same} and S^*_{diff}. We first consider the limit of $\mathsf{disc}\,(k-1,p)$ as $p \to \infty$. It turns out that this is closely related to the Irwin-Hall distribution. In particular, we formally define what we call the *discrepancy* of the Irwin-Hall distribution, denoted by $\mathsf{disc}\,(k-1)$. We prove that $\mathsf{disc}\,(k-1) \geqslant 1/\left(2^{k-1} \cdot (k-1)!\right)$. These results are presented in Section 4. Next, we examine how quickly does $\mathsf{disc}\,(k-1,p)$ tend to its limit $\mathsf{disc}\,(k-1)$ as $p \to \infty$. This result is presented in Section 5. Finally, we combine everything and prove Theorem 1 in Section 6.

4 Discrepancy of the Irwin-Hall Distribution

In this section, we study the discrepancy of the Irwin-Hall Distribution. We shall set up some notations first.

Let $U \colon \mathbb{R} \to \mathbb{R}$ be the uniform distribution over the interval $[0,1)$. Formally, $U(x) = 1$ if $x \in [0,1)$; otherwise, $U(x) = 0$. For $k \in \mathbb{N}$, let $\mathsf{IH}_k \colon \mathbb{R} \to \mathbb{R}$ be the density function of the k^{th} Irwin-Hall distribution. That is, $\mathsf{IH}_1 = U$ and, for $k > 1$, we have

$$\mathsf{IH}_k(x) = \int_{-\infty}^{\infty} \mathsf{IH}_{k-1}(y) U(x-y)\,\mathrm{d}y.$$

Observe that IH_k is non-zero only in the interval $(0,k)$.

The close form of the probability density function of the Irwin-Hall distribution is well-known.

Fact 1. *The probability density function of the Irwin-Hall distribution is the following.*[3]

$$\mathsf{IH}_k(x) = \frac{1}{(k-1)!} \sum_{j=0}^{\lfloor x \rfloor} (-1)^j \binom{k}{j} (x-j)^{k-1}.^{4}$$

We define the discrepancy of the k^{th} Irwin-Hall distribution with respect to a *canonical offset* $x \in [0, 1/2]$ as

$$\mathsf{Disc}_k(x) := \int_{-\infty}^{\infty} (-1)^{\lceil y-x \rceil} \cdot \mathsf{IH}_k(y)\,\mathrm{d}y.$$

In particular, we are interested in (refer to Figure 1)

- $\mathsf{Disc}_k(0)$ if k is odd;
- $\mathsf{Disc}_k(1/2)$ if k is even.

In this section, we shall prove a lower bound on these discrepancies. For $1 < k \in \mathbb{N}$, we define function $f_k \colon [0, 1/2] \to \mathbb{R}$ as follows to facilitate our analysis.

$$f_k(x) := \sum_{i=-\infty}^{\infty} (-1)^i \cdot \mathsf{IH}_k(x+i).$$

We shall first prove some properties of f_k.

Claim 2. *For any $1 < k \in \mathbb{N}$ and $x \in (0,k)$, the following identity holds.*

$$\frac{\mathrm{d}}{\mathrm{d}x} \mathsf{IH}_k(x) =: \mathsf{IH}'_k(x) = \mathsf{IH}_{k-1}(x) - \mathsf{IH}_{k-1}(x-1).$$

Proof. First, note that, because $U(x) = 0$ for $x \notin [0,1)$, we have the following definition for $\mathsf{IH}_k(x)$,

$$\mathsf{IH}_k(x) = \int_{x-1}^{x} \mathsf{IH}_{k-1}(y)\,\mathrm{d}y.$$

[3] One can refer to, for example, https://www.randomservices.org/random/special/IrwinHall.html for a proof.
[4] Here, $\lfloor x \rfloor$ is the floor function.

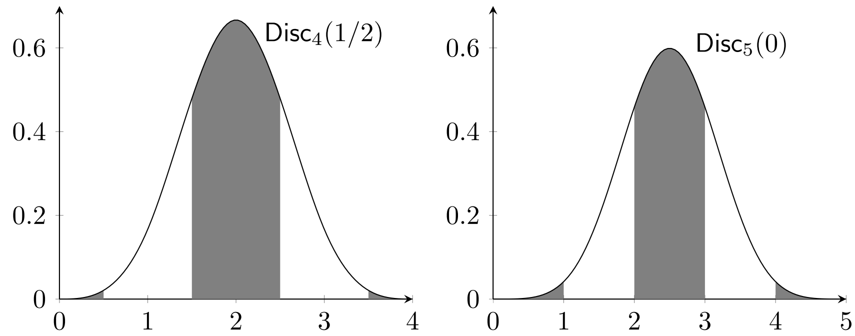

Figure 1: Plot of the Irwin-Hall distribution for $k = 4$ and $k = 5$. Intuitively, the discrepancy of the Irwin-Hall distribution is the difference between the probability mass inside the black bands and the total probability mass outside the black bands. We are interested in how the discrepancy changes as the black bands shifts along the x-axis, which is defined as $\mathsf{Disc}_k(x)$. In particular, we are interested in the discrepancy when the black bands is placed symmetrically, which is $\mathsf{Disc}_k(1/2)$ when k is even and $\mathsf{Disc}_k(0)$ when k is odd.

Therefore, taking the derivative with respect to x yields the following expression, thus proving Claim 2.

$$\frac{\mathrm{d}}{\mathrm{d}x}\mathsf{IH}_k(x) = \frac{\mathrm{d}}{\mathrm{d}x}\int_{x-1}^{x} \mathsf{IH}_{k-1}(y)\,\mathrm{d}y = \mathsf{IH}_{k-1}(x) - \mathsf{IH}_{k-1}(x-1). \qquad \square$$

Corollary 3. *For all $k > 2$, $\mathsf{IH}'_k(x)$ is continuous at all $x \in \mathbb{R}$.*

Proof. Since, for all $k > 1$, $\mathsf{IH}_k(x)$ is continuous at any $x \in \mathbb{R}$, we have

$$\lim_{\delta\to 0} \mathsf{IH}_k(x+\delta) - \mathsf{IH}_k(x-\delta) = 0$$

Then

$$\begin{aligned}&\lim_{\delta\to 0} \mathsf{IH}'_k(x+\delta) - \mathsf{IH}'_k(x-\delta)\\ =& \lim_{\delta\to 0} \mathsf{IH}_{k-1}(x+\delta) - \mathsf{IH}_{k-1}(x-\delta) + \lim_{\delta\to 0} \mathsf{IH}_{k-1}(x-1+\delta) - \mathsf{IH}_{k-1}(x-1-\delta) = 0 \qquad \square\end{aligned}$$

Claim 3. *For any $1 < k \in \mathbb{N}$ and $x \in (0, 1/2)$, the following identity holds.*

$$\frac{\mathrm{d}}{\mathrm{d}x} f_k(x) =: f'_k(x) = 2 \cdot f_{k-1}(x).$$

Proof. We begin by using the linearity of differentiation and the equation from Claim 2 to get the following expression for $\frac{\mathrm{d}}{\mathrm{d}x} f_k(x)$:

$$\begin{aligned}\frac{\mathrm{d}}{\mathrm{d}x} f_k(x) &= \frac{\mathrm{d}}{\mathrm{d}x} \sum_{i=-\infty}^{\infty} (-1)^i \cdot \mathsf{IH}_k(x+i)\\ &= \sum_{i=-\infty}^{\infty} (-1)^i \cdot \frac{\mathrm{d}}{\mathrm{d}x}\mathsf{IH}_k(x+i)\\ &= \sum_{i=-\infty}^{\infty} (-1)^i \cdot (\mathsf{IH}_{k-1}(x+i) - \mathsf{IH}_{k-1}(x+i-1))\\ &= \sum_{i=-\infty}^{\infty} (-1)^i \cdot \mathsf{IH}_{k-1}(x+i) - \sum_{i=-\infty}^{\infty} (-1)^i \cdot \mathsf{IH}_{k-1}(x+i-1)\end{aligned}$$

We remark that one can swap the order between the infinite sum and derivative since there are only finite many non-zero terms in the infinite sum.

Next, we bring one of the (-1)s out of the second summation to get:

$$\frac{\mathrm{d}}{\mathrm{d}x} f_k(x) = \sum_{i=-\infty}^{\infty} (-1)^i \cdot \mathsf{IH}_{k-1}(x+i) + \sum_{i=-\infty}^{\infty} (-1)^{i-1} \cdot \mathsf{IH}_{k-1}(x+i-1)$$

Now, we substitute $j = i-1$ into the second summation, and by eliminating the -1 in the bounds of the summation, we obtain the definition for $f_{k-1}(x)$ in both summations, thus proving Claim 3.

$$\begin{aligned}\frac{\mathrm{d}}{\mathrm{d}x} f_k(x) &= \sum_{i=-\infty}^{\infty} (-1)^i \cdot \mathsf{IH}_{k-1}(x+i) + \sum_{j=-\infty}^{\infty} (-1)^j \cdot \mathsf{IH}_{k-1}(x+j) \\ &= f_{k-1}(x) + f_{k-1}(x) \\ &= 2 \cdot f_{k-1}(x)\end{aligned}$$

□

Trivially, the following observations is correct due to symmetry (refer to Figure 2).

Observation 1.

- *For even* $k \in \mathbb{N}$, $f_k(1/2) = 0$.
- *For odd* $k \in \mathbb{N}$, $f_k(0) = 0$.
- *For* $k = 1$, *for all* $x \in (0, 1/2]$, $f_k(x) > 0$.

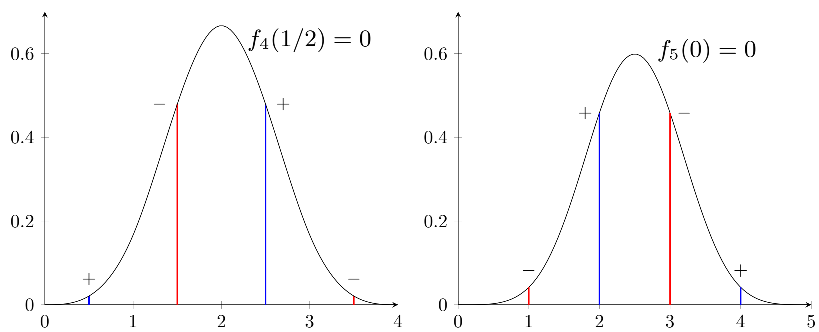

Figure 2: A pictorial proof of Observation 1.

Given these observations, we conclude with the following lemma on f_k.

Lemma 1. *For all* $1 < k \in \mathbb{N}$ *and all* $x_1, x_2 \in (0, 1/2)$,

$$f_k(x_1) f_k(x_2) > 0.$$

Intuitively, this lemma claims that f_k *has the same sign in* $(0, 1/2)$.

Proof. We will prove this using mathematical induction on k.

First, by the third property of Observation 1, we know that $f_1(x) > 0$ for all $x \in (0, 1/2)$. Hence the base case is proven.

Now, assume the statement is correct for $k-1$. The inductive hypothesis implies that either $f_{k-1}(x) < 0$ for all $x \in (0, 1/2)$ or $f_{k-1}(x) > 0$ for all $x \in (0, 1/2)$. Without loss of generality, let us assume that $f_{k-1}(x) < 0$ for all $x \in (0, 1/2)$.

Next, we do a case analysis based on the parity of k.

For even values of k, we have $f_k(1/2) = 0$. Therefore,

$$f_k(x) = -(f_k(1/2) - f_k(x)) = -2 \int_x^{1/2} f_{k-1}(x)\, \mathrm{d}x.$$

Since $f_{k-1}(x) < 0$ for all $x \in (0, 1/2)$, this implies that $f_k(x) > 0$ for all $x \in (0, 1/2)$ and hence the inductive step is proven.

For odd values of k, we have $f_k(0) = 0$. Therefore,

$$f_k(x) = f_k(x) - f_k(0) = 2\int_0^x f_{k-1}(x)\,\mathrm{d}x.$$

Since $f_{k-1}(x) < 0$ for all $x \in (0, 1/2)$, this implies that $f_k(x) < 0$ for all $x \in (0, 1/2)$ and hence the inductive step is proven.

This completes the proof. □

Now, we are ready to prove the properties of $\mathsf{Disc}_k(x)$. Similar to Observation 1, one can observe the following because of symmetry.

Observation 2.

- $\mathsf{Disc}_k(1/2) = 0$ *if* k *is odd;*
- $\mathsf{Disc}_k(0) = 0$ *if* k *is even.*

The following claim says that the rate at which $\mathsf{Disc}_k(x)$ changes as the offset x changes is exactly $2f_k(x)$.

Claim 4. *For all* $k \geqslant 2$ *and* $x \in (0, 1/2)$*, the following identity holds.*

$$\frac{\mathrm{d}}{\mathrm{d}x}\mathsf{Disc}_k(x) := \mathsf{Disc}'_k(x) = 2f_k(x).$$

Proof. Since x is restricted to the range $(0, 1/2)$, we can rewrite $\mathsf{Disc}_k(x)$ as followed:

$$\sum_{i=-\infty}^{\infty} (-1)^i \int_i^{i+x} \mathsf{IH}_k(y)\,\mathrm{d}y + (-1)^{i+1} \int_{i+x}^{i+1} \mathsf{IH}_k(y)\,\mathrm{d}y$$

Applying the Leibniz integral rule, we get

$$\begin{aligned}\mathsf{Disc}'_k(x) &= \sum_{i=-\infty}^{\infty} (-1)^i \cdot \mathsf{IH}_k(x+i) - (-1)^{i+1} \cdot \mathsf{IH}_k(x+i) \\ &= \sum_{i=-\infty}^{\infty} (-1)^i \cdot 2\mathsf{IH}_k(x+i) \\ &= 2f_k(x)\end{aligned}$$

□

Finally, we have the following theorem, which states that the discrepancy we are interested in is non-zero.

Theorem 3. *For* $k \in \mathbb{N}$*, we have*

- $|\mathsf{Disc}_k(0)| > 0$ *if* k *is odd;*
- $|\mathsf{Disc}_k(1/2)| > 0$ *if* k *is even.*

Proof. For this proof, we consider two separate cases, depending on whether k is odd or even. First, when k is odd, then by Observation 2, we know that $\mathsf{Disc}_k(1/2) = 0$.

Next, by Claim 4, we have that $\frac{\mathrm{d}}{\mathrm{d}x}\mathsf{Disc}_k(x) = 2f_k(x)$ for all $x \in (0, 1/2)$, and by Lemma 1, we can conclude $f_k(x)$ is nonzero for all $x \in (0, 1/2)$ and has a constant sign. Thus $\frac{\mathrm{d}}{\mathrm{d}x}\mathsf{Disc}_k(x)$ is nonzero and has a constant sign for $x \in (0, 1/2)$.

Therefore, because $\mathsf{Disc}_k(1/2) = 0$ and its derivative is nonzero with a constant sign for $x \in (0, 1/2)$, then $\mathsf{Disc}_k(x)$ is nonzero for all $x \in [0, 1/2)$, so if k is odd, then $|\mathsf{Disc}_k(0)| > 0$.

Likewise, when k is even, then by Observation 2, $\mathsf{Disc}_k(0) = 0$, and by Claim 4 and Lemma 1, we again conclude that $\frac{\mathrm{d}}{\mathrm{d}x}\mathsf{Disc}_k(x)$ is nonzero and has a constant sign for $x \in (0, 1/2)$.

Therefore, because $\mathsf{Disc}_k(0) = 0$ and its derivative is nonzero with a constant sign for $x \in (0, 1/2)$, then $\mathsf{Disc}_k(x)$ is nonzero for all $x \in (0, 1/2]$, so if k is even, then $|\mathsf{Disc}_k(1/2)| > 0$. □

Theorem 3 implies the following corollary, which is our main result on the discrepancy of the Irwin-Hall distribution.

Corollary 4 (Main Result)**.**

- $|\mathsf{Disc}_k(0)| \geqslant 1/k!$ *if* k *is odd;*
- $|\mathsf{Disc}_k(1/2)| \geqslant 1/(2^k k!)$ *if* k *is even.*

For the probing attack against secret sharing scheme with threshold k*, the quality of our attack is related to* $\mathsf{Disc}_{k-1}(x)$ *(refer to Section 3). Correspondingly, our lower bound can be stated as follows.*

- $|\mathsf{Disc}_{k-1}(0)| \geqslant 1/(k-1)!$ *if* k *is even;*
- $|\mathsf{Disc}_{k-1}(1/2)| \geqslant 1/(2^{k-1}(k-1)!)$ *if* k *is odd.*

Proof. First, we prove that

$$\mathsf{Disc}_k(x) = f_{k+1}(x)$$

for all k and $x \in [0, 1/2]$. Due to symmetry, it is trivial to show that in cases of odd $k, \mathsf{Disc}_k(1/2) = f_{k+1}(1/2) = 0$. Similarly, in cases of even $k, \mathsf{Disc}_k(0) = f_{k+1}(0) = 0$. Furthermore, we have proven in Claim 3 and Claim 4 that $\mathsf{Disc}'_k = f'_{k+1} = 2f_k$. Thus, $\forall x \in [0,1], \mathsf{Disc}_k(x) = f_{k+1}(x)$. Thus, we need to prove that for odd values of k, $|f_k(1/2)| \geqslant 1/\left(2^{(k-1)}(k-1)!\right)$ and for even values of k, $|f_k(0)| \geqslant 1/(k-1)!$.

Since we have proven that for odd k, $|\mathsf{Disc}_k(0)| > 0$ and for even k, $|\mathsf{Disc}_k(1/2)| > 0$, it suffices to prove that

- $f_k(0) \cdot (k-1)!$ is an integer;
- $f_k(1/2) \cdot 2^{k-1}(k-1)!$ is an integer.

To see this, recall that we have (Fact 1)

$$\mathsf{IH}_k(x) = \frac{1}{(k-1)!} \sum_{i=0}^{\lfloor x \rfloor} (-1)^i \binom{k}{i} (x-i)^{k-1}.$$

Then we have the following formula for $k! \cdot f_{k+1}(0)$, which is clearly an integer.

$$k! \cdot f_{k+1}(0) = k! \sum_{u=1}^{k} (-1)^u \cdot \mathsf{IH}_{k+1}(0) = \sum_{u=1}^{k} (-1)^u \sum_{i=0}^{u} (-1)^i \binom{k+1}{i} (-i)^k.$$

Therefore, $k! \cdot \mathsf{Disc}_k(0)$ is an integer and therefore $|k! \cdot \mathsf{Disc}_k(0)| \geqslant 1$, which implies that $|\mathsf{Disc}_k(0)| \geqslant 1/k!$ for odd k, thus proving the first part of the corollary.

For even cases of k with respect to $\mathsf{Disc}_k(1/2)$, which corresponds to odd $k+1$ with respect to $f_{k+1}(1/2)$, we have the following

$$\begin{aligned}
k! \cdot f_{k+1}\left(\frac{1}{2}\right) &= \sum_{u=0}^{k} (-1)^u \sum_{i=0}^{u} (-1)^i \binom{k+1}{i} \left(u + \frac{1}{2} - i\right)^k && \text{(Fact 1)} \\
&= \sum_{u=0}^{k} (-1)^u \sum_{j=0}^{u} (-1)^{u-j} \binom{k+1}{u-j} \left(j + \frac{1}{2}\right)^k \\
&= \sum_{u=0}^{k} \sum_{j=0}^{u} (-1)^j \binom{k+1}{u-j} \sum_{t=0}^{k} \binom{k}{t} \frac{1}{2}^t j^{k-t}
\end{aligned}$$

Thus, $2^k k! \cdot f_{k+1}(1/2)$ is an integer. Therefore, $|\mathsf{Disc}_k(1/2)| \geqslant 1/(2^k k!)$ for all even k, thus proving the second part of the corollary. $\square$

Remark 1. *Our proof is sufficient to prove that*

$$\left(\arg\max_x \ |\mathsf{Disc}_k(x)|\right) = 1/2,$$

when k is even and

$$\left(\arg\max_x \ |\mathsf{Disc}_k(x)|\right) = 0,$$

when k is odd. To see this, we note that Claim 4 and Lemma 1 together imply that $\mathsf{Disc}_k(x)$ is monotone on $(0, 1/2)$. Plus the fact that $\mathsf{Disc}_k(x)$ is 0 at one end point of the interval $(0, 1/2)$, we get the above statement.

In light of the probing attack as discussed in Section 3, this gives a strong evidence that secret $s^* = \frac{p-1}{2}$ is the secret that maximize the discrepancy. In words, $s^* = \frac{p-1}{2}$ is likely to be the most vulnerable secret with respect to this probing attack.

5 Discrepancy for Discrete Distribution

In this section, we consider the discrepancy of the discrete distribution related to the attack presented in Section 3. Let us set up notations first.

For any $p \in \mathbb{N}$,[5] let U_p be the density function of the discrete uniform distribution over $\{0, 1/p, \ldots, (p-1)/p\}$. That is, $U_p(x) = 1/p$ when $x \in \{0, 1/p, \ldots, (p-1)/p\}$ and 0 otherwise. For any $k \in \mathbb{N}$, we are interested in the convolutions of k copies of U_p. In particular, let $F_{k,p}$ be the density function defined as follows. When $k = 1$, $F_{k,p} := U_p$ and when $k > 1$,

$$F_{k,p}(x) := \frac{1}{p} \cdot \sum_{i=0}^{p-1} F_{k-1,p}(x - i/p).$$

Note that for all k, p, and x, $F_{k,p}(x) \leqslant 1/p$.

We first prove the following claim, which bounds the closeness between $F_{k,p}$ and the k^{th} Irwin-Hall distribution.

Claim 5. *For all integers α,*

$$\left| \sum_{i=0}^{\alpha} F_{k,p}(i/p) - \int_0^{(\alpha+1)/p} \mathsf{IH}_k(x)\,\mathrm{d}x \right| \leqslant k/p.$$

Proof. We shall prove this claim inductively on k. One can trivially verify the base case, i.e., $k = 1$.

Assume the statement is correct for $k - 1$, we have

$$\begin{aligned}
&\left| \sum_{i=0}^{\alpha} F_{k,p}(i/p) - \int_0^{(\alpha+1)/p} \mathsf{IH}_k(x)\,\mathrm{d}x \right| \\
=&\left| \sum_{i=0}^{\alpha} \frac{1}{p} \cdot \sum_{j=1}^{p} F_{k-1,p}(i/p - 1 + j/p) - \int_0^{(\alpha+1)/p} \int_{x-1}^{x} \mathsf{IH}_{k-1}(y)\,\mathrm{d}y\,\mathrm{d}x \right| \\
\overset{\text{(i)}}{=}&\left| \frac{1}{p} \cdot \sum_{j=1}^{p} \left(\sum_{i=0}^{\alpha+j-p} F_{k-1,p}(i/p) \right) - \int_{(\alpha+1)/p-1}^{(\alpha+1)/p} \left(\int_0^{x} \mathsf{IH}_{k-1}(y)\,\mathrm{d}y \right) \mathrm{d}x \right| \\
=&\left| \frac{1}{p} \cdot \sum_{j=1}^{p} \left(\sum_{i=0}^{\alpha+j-p} F_{k-1,p}(i/p) \right) - \sum_{j=1}^{p} \int_{(\alpha+j-p)/p}^{(\alpha+j+1-p)/p} \left(\int_0^{x} \mathsf{IH}_{k-1}(y)\,\mathrm{d}y \right) \mathrm{d}x \right| \\
\leqslant& \sum_{j=1}^{p} \int_{(\alpha+j-p)/p}^{(\alpha+j+1-p)/p} \left| \sum_{i=0}^{\alpha+j-p} F_{k-1,p}(i/p) - \int_0^{x} \mathsf{IH}_{k-1}(y)\,\mathrm{d}y \right| \mathrm{d}x
\end{aligned} \tag{1}$$

[5] In the application to leakage-resilient secret sharing, we shall only consider the case when p is a prime number. The result in this section regarding the discrepancy, however, works for all $p \in \mathbb{N}$.

Intuitively, for identity (i), we switch from the convolution of the density function to the convolution of the distribution function.

Now, for all $1 \leqslant j \leqslant p$ and $x \in ((\alpha + j - p)/p, (\alpha + j + 1 - p)/p)$, we have

$$\begin{aligned}
&\left|\sum_{i=0}^{\alpha+j-p} F_{k-1,p}(i/p) - \int_0^x \mathsf{IH}_{k-1}(y)\,\mathrm{d}y\right| \\
\leqslant&\left|\sum_{i=0}^{\alpha+j-p} F_{k-1,p}(i/p) - \int_0^{(\alpha+j+1-p)/p} \mathsf{IH}_{k-1}(y)\,\mathrm{d}y\right| + \left|\int_0^{(\alpha+j+1-p)/p} \mathsf{IH}_{k-1}(y)\,\mathrm{d}y - \int_0^x \mathsf{IH}_{k-1}(y)\,\mathrm{d}y\right| \\
\leqslant&(k-1)/p + \left|\int_x^{(\alpha+j+1-p)/p} \mathsf{IH}_{k-1}(y)\,\mathrm{d}y\right| \qquad \text{(Inductive Hypothesis)} \\
\leqslant&(k-1)/p + 1/p = k/p.
\end{aligned}$$

In the last inequality, we use the fact that, for all $y \in \mathbb{R}$, $|\mathsf{IH}_{k-1}(y)| \leqslant 1$, which can be proven trivially. Finally, continuing from Equation 1, we have

$$\leqslant \sum_{j=1}^{p} \int_{(\alpha+j-p)/p}^{(\alpha+j+1-p)/p} \Big(k/p\Big)\,\mathrm{d}x = p \cdot (1/p) \cdot (k/p) = k/p.$$

This completes the proof of the inductive step and hence the claim. □

The following corollary follows from Claim 5 and triangle inequality trivially.

Corollary 5. *For all integers $\alpha \leqslant \beta$, we have*

$$\left|\sum_{\alpha}^{\beta} F_{k,p}(i/p) - \int_{\beta/p}^{(\alpha+1)/p} \mathsf{IH}_k(x)\,\mathrm{d}x\right| \leqslant (2k)/p.$$

Recall that for the Irwin-Hall distribution, we define the discrepancy (with offset x) as

$$\mathsf{Disc}_k(x) := \int_{-\infty}^{\infty} (-1)^{\lceil y-x \rceil} \cdot \mathsf{IH}_k(y)\,\mathrm{d}y.$$

In particular, we are interested in $\mathsf{Disc}_k(0)$ when k is odd and $\mathsf{Disc}_k(1/2)$ when k is even. Equivalently, we are interested in

$$\begin{aligned}
\mathsf{disc}\,(k) \; &:= \mathsf{Disc}_k\left(\frac{k-1}{2}\right) \\
&= \int_{-\infty}^{\infty} (-1)^{\left\lceil y - \frac{k-1}{2} \right\rceil} \cdot \mathsf{IH}_k(y)\,\mathrm{d}y.
\end{aligned}$$

Similarly, we define the discrepancy for the discrete distribution $F_{k,p}$ as follows.

$$\mathsf{disc}\,(k,p) \; := \sum_{i=-\infty}^{\infty} (-1)^{\left\lceil \frac{i-(k-1)(p-1)/2-1}{p} \right\rceil} F_{k,p}(i/p).^{6}$$

In the rest of this section, we prove the following theorem, which says that the discrepancy for the discrete distribution $F_{k,p}$ is close to the discrepancy of the Irwin-Hall distribution.

Theorem 4. *For all $k, p \in \mathbb{N}$,*

$$|\mathsf{disc}\,(k) - \mathsf{disc}\,(k,p)| \leqslant \left(3k^2\right)/p.$$

In particular, it implies $\Big||\mathsf{disc}\,(k)| - |\mathsf{disc}\,(k,p)|\Big| \leqslant \left(3k^2\right)/p.$

[6] One can verify that $\mathsf{disc}\,(k,p)$ is $\Pr[S_1 + S_2 + \cdots + S_{k-1} \in S^*_{\mathsf{same}}]$-$\Pr[S_1 + S_2 + \cdots + S_{k-1} \in S^*_{\mathsf{diff}}]$ for secret $s^* = (p-1)/2$ as discussed in Section 3.

Proof. Without loss of generality, we assume $k = 1 \mod 4$. The other cases can be proven in a similar manner. By definition,

$$
\begin{aligned}
&|\mathsf{disc}\,(k) - \mathsf{disc}\,(k,p)| \\
=&\left|\int_{-\infty}^{\infty} (-1)^{\lceil y - \frac{k-1}{2} \rceil} \cdot \mathsf{IH}_k(y)\,\mathrm{d}y - \sum_{i=-\infty}^{\infty} (-1)^{\lceil \frac{i-(k-1)(p-1)/2-1}{p} \rceil} F_{k,p}(i/p)\right| \\
=&\left|\int_{-\infty}^{\infty} (-1)^{\lceil y \rceil} \cdot \mathsf{IH}_k(y)\,\mathrm{d}y - \sum_{i=-\infty}^{\infty} (-1)^{\lceil \frac{i+(k-1)/2-1}{p} \rceil} F_{k,p}(i/p)\right| && \text{(Since } k = 1 \mod 4\text{)} \\
\leqslant& \sum_{i=0}^{k-1} \left|(-1)^{i+1} \int_i^{i+1} \mathsf{IH}_k(y)\,\mathrm{d}y - \sum_{j=ip}^{(i+1)p-1} (-1)^{\lceil \frac{j+(k-1)/2-1}{p} \rceil} F_{k,p}(j/p)\right| \\
\overset{\text{(i)}}{\leqslant}& \sum_{i=0}^{k-1} \left(\left|\int_i^{i+1} \mathsf{IH}_k(y)\,\mathrm{d}y - \sum_{j=ip}^{(i+1)p-1} F_{k,p}(j/p)\right| + k/p\right) \\
\leqslant& \sum_{i=0}^{k-1} ((2k)/p + k/p) && \text{(Corollary 5)} \\
=& \left(3k^2\right)/p
\end{aligned}
$$

Inequality (i) is due to the facts that (a) there are at most $(k-1)/2$ many j's from ip to $(i+1)p-1$ such that $(-1)^{\lceil \frac{j+(k-1)/2-1}{p} \rceil} \neq (-1)^{i+1}$; (b) we always have $F_{k,p}(x) \leqslant 1/p$ for all x. This completes the proof. ☐

6 Proof of Theorem 1

First, we prove the following claims that are needed for the proof of Theorem 1.

Claim 6. *For every secret $s \in F$, the following equality holds.*

$$\Pr\left[\widetilde{b}_1 \oplus \ldots \oplus \widetilde{b}_k = b_1 \oplus \ldots \oplus b_k | s\right] = \frac{1}{2}\left(1 + \prod_{i=1}^{k} \rho_i\right).$$

Proof. We prove by induction on k.
Base case. For $k = 1$, it is clearly that $\Pr[\widetilde{b}_1 = b_1] = \frac{1}{2}(1+\rho_1)$ since $\widetilde{b}_1$ is a ρ_1-correlated copy of b_1.
Inductive hypothesis. Suppose $\Pr\left[\widetilde{b}_1 \oplus \ldots \oplus \widetilde{b}_{k-1} = b_1 \oplus \ldots \oplus b_{k-1} | s\right] = \frac{1}{2}\left(1 + \prod_{i=1}^{k-1} \rho_i\right)$.
Inductive step. We have

$$
\begin{aligned}
&\Pr\left[\widetilde{b}_1 \oplus \ldots \oplus \widetilde{b}_k = b_1 \oplus \ldots \oplus b_k | s\right] \\
&= \Pr\left[\widetilde{b}_1 \oplus \ldots \oplus \widetilde{b}_{k-1} = b_1 \oplus \ldots \oplus b_{k-1} | s\right] \cdot \Pr\left[\widetilde{b}_k = b_k | s\right] + \Pr\left[\widetilde{b}_1 \oplus \ldots \oplus \widetilde{b}_k \neq b_1 \oplus \ldots \oplus b_k | s\right] \cdot \Pr\left[\widetilde{b}_k \neq b_k | s\right] \\
&= \frac{1}{2}\left(1 + \prod_{i=1}^{k-1} \rho_i\right) \frac{1}{2}(1+\rho_k) + \frac{1}{2}\left(1 - \prod_{i=1}^{k-1} \rho_i\right) \frac{1}{2}(1-\rho_k) \\
&= \frac{1}{2}\left(1 + \prod_{i=1}^{k} \rho_i\right)
\end{aligned}
$$

which completes the proof. ☐

Remark. An alternative way to prove this is to apply basic Fourier property of the convolution operator. Observe that each $\widetilde{b}_i$ is the convolution of the bit b_i with a noise operator.

Claim 7. *For every two secrets $s^{(0)}, s^{(1)} \in F$, the following equality holds.*

$$\mathsf{SD}\left(\widetilde{b}_1 \oplus \ldots \oplus \widetilde{b}_k | s^{(0)}\ ,\ \widetilde{b}_1 \oplus \ldots \oplus \widetilde{b}_k | s^{(1)}\right) = \left(\prod_{i=1}^{k} \rho_i\right) \mathsf{SD}\left(b_1 \oplus \ldots \oplus b_k | s^{(0)}\ ,\ b_1 \oplus \ldots \oplus b_k | s^{(1)}\right)$$

Proof. By Claim 6, we have

$$\begin{aligned}
&\mathsf{SD}\left(\widetilde{b}_1 \oplus \ldots \oplus \widetilde{b}_k | s^{(0)}\ ,\ \widetilde{b}_1 \oplus \ldots \oplus \widetilde{b}_k | s^{(1)}\right) \\
&= \frac{1}{2} \sum_b \left| \Pr\left[\widetilde{b}_1 \oplus \ldots \oplus \widetilde{b}_k = b | s^{(0)}\right] - \Pr\left[\widetilde{b}_1 \oplus \ldots \oplus \widetilde{b}_k = b | s^{(1)}\right] \right| \\
&= \sum_b \left| \Pr\left[b_1 \oplus \ldots \oplus b_k = b | s^{(0)}\right] \cdot \frac{1}{2}\left(1 + \prod_{i=1}^{k} \rho_i\right) + \Pr\left[b_1 \oplus \ldots \oplus b_k = 1 - b | s^{(0)}\right] \cdot \frac{1}{2}\left(1 - \prod_{i=1}^{k} \rho_i\right) \right. \\
&\qquad \left. - \Pr\left[b_1 \oplus \ldots \oplus b_k = b | s^{(1)}\right] \cdot \frac{1}{2}\left(1 + \prod_{i=1}^{k} \rho_i\right) + \Pr\left[b_1 \oplus \ldots \oplus b_k = 1 - b | s^{(1)}\right] \cdot \frac{1}{2}\left(1 - \prod_{i=1}^{k} \rho_i\right) \right| \\
&= \left(\prod_{i=1}^{k} \rho_i\right) \frac{1}{2} \sum_b \left| \Pr[b_1 \oplus \ldots \oplus b_k = b | s^{(0)}] - \Pr[b_1 \oplus \ldots \oplus b_k = b | s^{(0)}] \right| \\
&= \left(\prod_{i=1}^{k} \rho_i\right) \mathsf{SD}\left(b_1 \oplus \ldots \oplus b_k | s^{(0)}\ ,\ b_1 \oplus \ldots \oplus b_k | s^{(1)}\right)
\end{aligned}$$

as desired. □

Now, we are ready to prove Theorem 1.

Proof of Theorem 1 . For any two secrets $s^{(0)}$ and $s^{(1)}$, we have

$$\begin{aligned}
&\mathsf{SD}\left(\left(\widetilde{b}_1, \ldots, \widetilde{b}_k \middle| s^{(0)}\right),\ \left(\widetilde{b}_1, \ldots, \widetilde{b}_k \middle| s^{(1)}\right)\right) \\
&\geqslant \left| \Pr\left[\widetilde{b}_1 \oplus \ldots \oplus \widetilde{b}_k = 0 | s^{(0)}\right] - \Pr\left[\widetilde{b}_1 \oplus \ldots \oplus \widetilde{b}_k = 0 | s^{(1)}\right] \right| \\
&= \mathsf{SD}\left(\widetilde{b}_1 \oplus \ldots \oplus \widetilde{b}_k | s^{(0)}\ ,\ \widetilde{b}_1 \oplus \ldots \oplus \widetilde{b}_k | s^{(1)}\right) \\
&= \left(\prod_{i=1}^{k} \rho_i\right) \cdot \mathsf{SD}\left(b_1 \oplus \ldots \oplus b_k | s^{(0)}\ ,\ b_1 \oplus \ldots \oplus b_k | s^{(1)}\right) \qquad \text{(Claim 7)}
\end{aligned}$$

By Corollary 4 and Theorem 4, we know that there exists a secret $s^{(0)}$ such that the bias of the output of the probing attack is $\mathsf{disc}\,(k-1) \geqslant \frac{1}{2^{k-1}(k-1)!} - \frac{3(k-1)^2}{p}$.

On the other hand, for a random secret s, it is easy to see that the bias of the output of our probing attack is upper bounded by $1/p$.

Therefore, there exists a secret $s^{(1)}$ such that

$$\begin{aligned}
\mathsf{SD}\left(b_1 \oplus \ldots \oplus b_k | s^{(0)}\ ,\ b_1 \oplus \ldots \oplus b_k | s^{(1)}\right) &\geqslant \frac{1}{2} \cdot (\mathsf{disc}\,(k-1) - 1/p) \\
&\geqslant \frac{1}{2^k (k-1)!} - \frac{3(k-1)^2 + 1}{p}.
\end{aligned}$$

Consequently,

$$\mathsf{SD}\left(\left(\widetilde{b}_1, \ldots, \widetilde{b}_k \middle| s^{(0)}\right),\ \left(\widetilde{b}_1, \ldots, \widetilde{b}_k \middle| s^{(1)}\right)\right) \geqslant \left(\prod_{i=1}^{k} \rho_i\right) \cdot \left(\frac{1}{2^k (k-1)!} - \frac{3(k-1)^2 + 1}{p}\right).$$

In particular, when k is even, we know there exists a secret $s^{(0)}$ such that the bias of the output of the probing attack is $\mathsf{disc}\,(k-1) \geqslant \frac{1}{(k-1)!} - \frac{3(k-1)^2}{p}$. Hence, similarly, we get

$$\mathsf{SD}\left(\left(\widetilde{b}_1, \ldots, \widetilde{b}_k \middle| s^{(0)}\right), \left(\widetilde{b}_1, \ldots, \widetilde{b}_k \middle| s^{(1)}\right)\right) \geqslant \left(\prod_{i=1}^{k} \rho_i\right) \cdot \left(\frac{1}{2(k-1)!} - \frac{3(k-1)^2+1}{p}\right). \qquad \square$$

References

[ADN+19] Divesh Aggarwal, Ivan Damgård, Jesper Buus Nielsen, Maciej Obremski, Erick Purwanto, João Ribeiro, and Mark Simkin. Stronger leakage-resilient and non-malleable secret sharing schemes for general access structures. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology – CRYPTO 2019, Part II*, volume 11693 of *Lecture Notes in Computer Science*, pages 510–539, Santa Barbara, CA, USA, August 18–22, 2019. Springer, Heidelberg, Germany. doi:10.1007/978-3-030-26951-7_18. 2

[AGM+15a] Shashank Agrawal, Divya Gupta, Hemanta K. Maji, Omkant Pandey, and Manoj Prabhakaran. Explicit non-malleable codes against bit-wise tampering and permutations. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *Advances in Cryptology – CRYPTO 2015, Part I*, volume 9215 of *Lecture Notes in Computer Science*, pages 538–557, Santa Barbara, CA, USA, August 16–20, 2015. Springer, Heidelberg, Germany. doi:10.1007/978-3-662-47989-6_26. 2

[AGM+15b] Shashank Agrawal, Divya Gupta, Hemanta K. Maji, Omkant Pandey, and Manoj Prabhakaran. A rate-optimizing compiler for non-malleable codes against bit-wise tampering and permutations. In Yevgeniy Dodis and Jesper Buus Nielsen, editors, *TCC 2015: 12th Theory of Cryptography Conference, Part I*, volume 9014 of *Lecture Notes in Computer Science*, pages 375–397, Warsaw, Poland, March 23–25, 2015. Springer, Heidelberg, Germany. doi:10.1007/978-3-662-46494-6_16. 2

[Ava05] Roberto 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

[AVL19] Rodrigo Abarzúa, Claudio Valencia, and Julio 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

[BDIR18] Fabrice Benhamouda, Akshay Degwekar, Yuval Ishai, and Tal Rabin. On the local leakage resilience of linear secret sharing schemes. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology – CRYPTO 2018, Part I*, volume 10991 of *Lecture Notes in Computer Science*, pages 531–561, Santa Barbara, CA, USA, August 19–23, 2018. Springer, Heidelberg, Germany. doi:10.1007/978-3-319-96884-1_18. 2, 3, 4

[BGMN18] Alexander R. Block, Divya Gupta, Hemanta K. Maji, and Hai H. Nguyen. Secure computation using leaky correlations (asymptotically optimal constructions). In Amos Beimel and Stefan Dziembowski, editors, *TCC 2018: 16th Theory of Cryptography Conference, Part II*, volume 11240 of *Lecture Notes in Computer Science*, pages 36–65, Panaji, India, November 11–14, 2018. Springer, Heidelberg, Germany. doi:10.1007/978-3-030-03810-6_2. 2

[BIS19] Andrej Bogdanov, Yuval Ishai, and Akshayaram Srinivasan. Unconditionally secure computation against low-complexity leakage. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology – CRYPTO 2019, Part II*, volume 11693 of *Lecture Notes in Computer Science*, pages 387–416, Santa Barbara, CA, USA, August 18–22, 2019. Springer, Heidelberg, Germany. doi:10.1007/978-3-030-26951-7_14. 2

[BMN17] Alexander R. Block, Hemanta K. Maji, and Hai H. Nguyen. Secure computation based on leaky correlations: High resilience setting. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology – CRYPTO 2017, Part II*, volume 10402 of *Lecture Notes in Computer Science*, pages 3–32, Santa Barbara, CA, USA, August 20–24, 2017. Springer, Heidelberg, Germany. doi:10.1007/978-3-319-63715-0_1. 2

[BPRW16] Allison Bishop, Valerio Pastro, Rajmohan Rajaraman, and Daniel Wichs. Essentially optimal robust secret sharing with maximal corruptions. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology – EUROCRYPT 2016, Part I*, volume 9665 of *Lecture Notes* *in Computer Science*, pages 58–86, Vienna, Austria, May 8–12, 2016. Springer, Heidelberg, Germany. doi:10.1007/978-3-662-49890-3_3. 2

[BS19] Saikrishna Badrinarayanan and Akshayaram Srinivasan. Revisiting non-malleable secret sharing. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2019, Part I*, volume 11476 of *Lecture Notes in Computer Science*, pages 593–622, Darmstadt, Germany, May 19–23, 2019. Springer, Heidelberg, Germany. doi:10.1007/978-3-030-17653-2_20. 2

[BSS05] Ian F Blake, Gadiel Seroussi, and Nigel P Smart. *Advances in elliptic curve cryptography*, volume 317. Cambridge University Press, 2005. 1

[BT18] Swarup Bhunia and Mark Tehranipoor. *Hardware security: a hands-on learning approach*. Morgan Kaufmann, 2018. 1

[CDFR17] Ignacio Cascudo, Ivan Damgård, Oriol Farràs, and Samuel Ranellucci. Resource-efficient OT combiners with active security. In Yael Kalai and Leonid Reyzin, editors, *TCC 2017: 15th Theory of Cryptography Conference, Part II*, volume 10678 of *Lecture Notes in Computer Science*, pages 461–486, Baltimore, MD, USA, November 12–15, 2017. Springer, Heidelberg, Germany. doi:10.1007/978-3-319-70503-3_15. 2

[CFA+05] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren, editors. *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. Chapman and Hall/CRC, 2005. doi:10.1201/9781420034981. 1

[CG14] Mahdi Cheraghchi and Venkatesan Guruswami. Non-malleable coding against bit-wise and split-state tampering. In Yehuda Lindell, editor, *TCC 2014: 11th Theory of Cryptography Conference*, volume 8349 of *Lecture Notes in Computer Science*, pages 440–464, San Diego, CA, USA, February 24–26, 2014. Springer, Heidelberg, Germany. doi:10.1007/978-3-642-54242-8_19. 2

[CGG+20] Eshan Chattopadhyay, Jesse Goodman, Vipul Goyal, Ashutosh Kumar, Xin Li, Raghu Meka, and David Zuckerman. Extractors and secret sharing against bounded collusion protocols. In *FOCS–2020*, 2020. 2

[CGN19] Gaëlle Candel, Rémi Géraud-Stewart, and David Naccache. How to compartment secrets. In Maryline Laurent and Thanassis Giannetsos, editors, *Information Security Theory and Practice - 13th IFIP WG 11.2 International Conference, WISTP 2019, Paris, France, December 11-12, 2019, Proceedings*, volume 12024 of *Lecture Notes in Computer Science*, pages 3–11. Springer, 2019. doi:10.1007/978-3-030-41702-4_1. 2

[CJRR99] Suresh Chari, Charanjit S. Jutla, Josyula R. Rao, and Pankaj Rohatgi. Towards sound approaches to counteract power-analysis attacks. In Michael J. Wiener, editor, *Advances in Cryptology – CRYPTO'99*, volume 1666 of *Lecture Notes in Computer Science*, pages 398–412, Santa Barbara, CA, USA, August 15–19, 1999. Springer, Heidelberg, Germany. doi:10.1007/3-540-48405-1_26. 2

[DDF14] Alexandre Duc, Stefan Dziembowski, and Sebastian Faust. Unifying leakage models: From probing attacks to noisy leakage. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology – EUROCRYPT 2014*, volume 8441 of *Lecture Notes in Computer Science*, pages 423–440, Copenhagen, Denmark, May 11–15, 2014. Springer, Heidelberg, Germany. doi:10.1007/978-3-642-55220-5_24. 2

[DDKM18] Hoang Dau, Iwan M. Duursma, Han Mao Kiah, and Olgica Milenkovic. Repairing reed-solomon codes with multiple erasures. *IEEE Trans. Inf. Theory*, 64(10):6567–6582, 2018. doi:10.1109/TIT.2018.2827942. 2

[DPW10] Stefan Dziembowski, Krzysztof Pietrzak, and Daniel Wichs. Non-malleable codes. In Andrew Chi-Chih Yao, editor, *ICS 2010: 1st Innovations in Computer Science*, pages 434–452, Tsinghua University, Beijing, China, January 5–7, 2010. Tsinghua University Press. 2

[FGM+10] Junfeng Fan, Xu Guo, Elke De Mulder, Patrick Schaumont, Bart Preneel, and Ingrid Verbauwhede. State-of-the-art of secure ECC implementations: A survey on known side-channel attacks and countermeasures. In Jim Plusquellic and Ken Mai, editors, *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*, pages 76–87. IEEE Computer Society, 2010. doi:10.1109/HST.2010.5513110. 1

[FV12] Junfeng Fan and Ingrid Verbauwhede. An updated survey on secure ECC implementations: Attacks, countermeasures and cost. In David Naccache, editor, *Cryptography and Security: From Theory to Applications - Essays Dedicated to Jean-Jacques Quisquater on the Occasion of His 65th Birthday*, volume 6805 of *Lecture Notes in Computer Science*, pages 265–282. Springer, 2012. doi:10.1007/978-3-642-28368-0_18. 1

[FY19] Serge Fehr and Chen Yuan. Towards optimal robust secret sharing with security against a rushing adversary. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2019, Part III*, volume 11478 of *Lecture Notes in Computer Science*, pages 472–499, Darmstadt, Germany, May 19–23, 2019. Springer, Heidelberg, Germany. doi:10.1007/978-3-030-17659-4_16. 2

[FY20] Serge Fehr and Chen Yuan. Robust secret sharing with almost optimal share size and security against rushing adversaries. In Rafael Pass and Krzysztof Pietrzak, editors, *TCC 2020: 18th Theory of Cryptography Conference, Part III*, volume 12552 of *Lecture Notes in Computer Science*, pages 470–498, Durham, NC, USA, November 16–19, 2020. Springer, Heidelberg, Germany. doi:10.1007/978-3-030-64381-2_17. 2

[GK18] Vipul Goyal and Ashutosh Kumar. Non-malleable secret sharing. In Ilias Diakonikolas, David Kempe, and Monika Henzinger, editors, *50th Annual ACM Symposium on Theory of Computing*, pages 685–698, Los Angeles, CA, USA, June 25–29, 2018. ACM Press. doi:10.1145/3188745.3188872. 2

[GR17] Venkatesan Guruswami and Ankit Singh Rawat. MDS code constructions with small sub-packetization and near-optimal repair bandwidth. In Philip N. Klein, editor, *28th Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 2109–2122, Barcelona, Spain, January 16–19, 2017. ACM-SIAM. doi:10.1137/1.9781611974782.137. 2

[GW16] Venkatesan Guruswami and Mary Wootters. Repairing reed-solomon codes. In Daniel Wichs and Yishay Mansour, editors, *48th Annual ACM Symposium on Theory of Computing*, pages 216–226, Cambridge, MA, USA, June 18–21, 2016. ACM Press. doi:10.1145/2897518.2897525. 2

[GW17] Venkatesan Guruswami and Mary Wootters. Repairing reed-solomon codes. *IEEE Trans. Inf. Theory*, 63(9):5684–5698, 2017. doi:10.1109/TIT.2017.2702660. 2

[HIKN08] Danny Harnik, Yuval Ishai, Eyal Kushilevitz, and Jesper Buus Nielsen. OT-combiners via secure computation. In Ran Canetti, editor, *TCC 2008: 5th Theory of Cryptography Conference*, volume 4948 of *Lecture Notes in Computer Science*, pages 393–411, San Francisco, CA, USA, March 19–21, 2008. Springer, Heidelberg, Germany. doi:10.1007/978-3-540-78524-8_22. 2

[HIMV19] Carmit Hazay, Yuval Ishai, Antonio Marcedone, and Muthuramakrishnan Venkitasubramaniam. LevioSA: Lightweight secure arithmetic computation. In Lorenzo Cavallaro, Johannes Kinder, XiaoFeng Wang, and Jonathan Katz, editors, *ACM CCS 2019: 26th Conference on Computer and Communications Security*, pages 327–344. ACM Press, November 11–15, 2019. doi:10.1145/3319535.3354258. 2

[HKN+05] Danny Harnik, Joe Kilian, Moni Naor, Omer Reingold, and Alon Rosen. On robust combiners for oblivious transfer and other primitives. In Ronald Cramer, editor, *Advances in Cryptology – EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 96–113, Aarhus, Denmark, May 22–26, 2005. Springer, Heidelberg, Germany. doi:10.1007/11426639_6. 2

[HVW20] Carmit Hazay, Muthuramakrishnan Venkitasubramaniam, and Mor Weiss. The price of active security in cryptographic protocols. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology – EUROCRYPT 2020, Part II*, volume 12106 of *Lecture Notes in Computer Science*, pages 184–215, Zagreb, Croatia, May 10–14, 2020. Springer, Heidelberg, Germany. doi:10.1007/978-3-030-45724-2_7. 2

[IKOS09] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Extracting correlations. In *50th Annual Symposium on Foundations of Computer Science*, pages 261–270, Atlanta, GA, USA, October 25–27, 2009. IEEE Computer Society Press. doi:10.1109/FOCS.2009.56. 2

[IMSW14] Yuval Ishai, Hemanta K. Maji, Amit Sahai, and Jürg Wullschleger. Single-use ot combiners with near-optimal resilience. In *2014 IEEE International Symposium on Information Theory, Honolulu, HI, USA, June 29 - July 4, 2014*, pages 1544–1548. IEEE, 2014. doi:10.1109/ISIT.2014.6875092. 2

[IPSW06] Yuval Ishai, Manoj Prabhakaran, Amit Sahai, and David Wagner. Private circuits II: Keeping secrets in tamperable circuits. In Serge Vaudenay, editor, *Advances in Cryptology – EUROCRYPT 2006*, volume 4004 of *Lecture Notes in Computer Science*, pages 308–327, St. Petersburg, Russia, May 28 – June 1, 2006. Springer, Heidelberg, Germany. doi:10.1007/11761679_19. 2

[ISW03] Yuval Ishai, Amit Sahai, and David Wagner. Private circuits: Securing hardware against probing attacks. In Dan Boneh, editor, *Advances in Cryptology – CRYPTO 2003*, volume 2729 of *Lecture Notes in Computer Science*, pages 463–481, Santa Barbara, CA, USA, August 17–21, 2003. Springer, Heidelberg, Germany. doi:10.1007/978-3-540-45146-4_27. 2

[JKB95] Norman L Johnson, Samuel Kotz, and Narayanaswamy Balakrishnan. *Continuous univariate distributions, volume 2*, volume 289. John wiley & sons, 1995. 6

[KJJ99] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In Michael J. Wiener, editor, *Advances in Cryptology – CRYPTO'99*, volume 1666 of *Lecture Notes in Computer Science*, pages 388–397, Santa Barbara, CA, USA, August 15–19, 1999. Springer, Heidelberg, Germany. doi:10.1007/3-540-48405-1_25. 1

[KMS19] Ashutosh Kumar, Raghu Meka, and Amit Sahai. Leakage-resilient secret sharing against colluding parties. In David Zuckerman, editor, *60th Annual Symposium on Foundations of Computer Science*, pages 636–660, Baltimore, MD, USA, November 9–12, 2019. IEEE Computer Society Press. doi:10.1109/FOCS.2019.00045. 2

[Koc96] Paul C. Kocher. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In Neal Koblitz, editor, *Advances in Cryptology – CRYPTO'96*, volume 1109 of *Lecture Notes in Computer Science*, pages 104–113, Santa Barbara, CA, USA, August 18–22, 1996. Springer, Heidelberg, Germany. doi:10.1007/3-540-68697-5_9. 1

[KR19] Yael Tauman Kalai and Leonid Reyzin. A survey of leakage-resilient cryptography. In Oded Goldreich, editor, *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*, pages 727–794. ACM, 2019. doi:10.1145/3335741.3335768. 1, 2

[KS04] François Koeune and François-Xavier Standaert. A tutorial on physical security and side-channel attacks. In Alessandro Aldini, Roberto Gorrieri, and Fabio Martinelli, editors, *Foundations of Security Analysis and Design III, FOSAD 2004/2005 Tutorial Lectures*, volume 3655 of *Lecture Notes in Computer Science*, pages 78–108. Springer, 2004. doi:10.1007/11554578_3. 1

[LCG+20] Fuchun Lin, Mahdi Cheraghchi, Venkatesan Guruswami, Reihaneh Safavi-Naini, and Huaxiong Wang. Leakage-resilient secret sharing in non-compartmentalized models. In Yael Tauman Kalai, Adam D. Smith, and Daniel Wichs, editors, *1st Conference on Information-Theoretic Cryptography, ITC 2020, June 17-19, 2020, Boston, MA, USA*, volume 163 of *LIPIcs*, pages 7:1–7:24. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020. doi:10.4230/LIPIcs.ITC.2020.7. 2

[Mas01] James L Massey. Some applications of code duality in cryptography. *Mat. Contemp*, 21(187-209):16th, 2001. 2

[MBW19] Jay Mardia, Burak Bartan, and Mary Wootters. Repairing multiple failures for scalar MDS codes. *IEEE Trans. Inf. Theory*, 65(5):2661–2672, 2019. doi:10.1109/TIT.2018.2876542. 2

[MNP+21] Hemanta K. Maji, Hai H. Nguyen, Anat Paskin-Cherniavsky, Tom Suad, and Mingyuan 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, 6, 7

[MPSW20] Hemanta K. Maji, Anat Paskin-Cherniavsky, Tom Suad, and Mingyuan Wang. On leakage-resilient secret sharing. Cryptology ePrint Archive, Report 2020/1517, 2020. https://eprint.iacr.org/2020/1517. 2, 3

[MPW07] Remo Meier, Bartosz Przydatek, and Jürg Wullschleger. Robuster combiners for oblivious transfer. In Salil P. Vadhan, editor, *TCC 2007: 4th Theory of Cryptography Conference*, volume 4392 of *Lecture Notes in Computer Science*, pages 404–418, Amsterdam, The Netherlands, February 21–24, 2007. Springer, Heidelberg, Germany. doi:10.1007/978-3-540-70936-7_22. 2

[MSV20] Pasin Manurangsi, Akshayaram Srinivasan, and Prashant Nalini Vasudevan. Nearly optimal robust secret sharing against rushing adversaries. In Daniele Micciancio and Thomas Ristenpart, editors, *Advances in Cryptology – CRYPTO 2020, Part III*, volume 12172 of *Lecture Notes in Computer Science*, pages 156–185, Santa Barbara, CA, USA, August 17–21, 2020. Springer, Heidelberg, Germany. doi:10.1007/978-3-030-56877-1_6. 2

[NS20] Jesper Buus Nielsen and Mark Simkin. Lower bounds for leakage-resilient secret sharing. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology – EUROCRYPT 2020, Part I*, volume 12105 of *Lecture Notes in Computer Science*, pages 556–577, Zagreb, Croatia, May 10–14, 2020. Springer, Heidelberg, Germany. doi:10.1007/978-3-030-45721-1_20. 3, 4

[O'D14] Ryan O'Donnell. *Analysis of Boolean Functions*. Cambridge University Press, 2014. 7

[OP03] Elisabeth Oswald and Bart 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

[RD20] Mark Randolph and William Diehl. Power side-channel attack analysis: A review of 20 years of study for the layman. *Cryptogr.*, 4(2):15, 2020. doi:10.3390/cryptography4020015. 1

[SLS19] Asanka P. Sayakkara, Nhien-An Le-Khac, and Mark Scanlon. A survey of electromagnetic side-channel attacks and discussion on their case-progressing potential for digital forensics. *Digit. Investig.*, 29:43–54, 2019. doi:10.1016/j.diin.2019.03.002. 1

[SV19] Akshayaram Srinivasan and Prashant Nalini Vasudevan. Leakage resilient secret sharing and applications. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology – CRYPTO 2019, Part II*, volume 11693 of *Lecture Notes in Computer Science*, pages 480–509, Santa Barbara, CA, USA, August 18–22, 2019. Springer, Heidelberg, Germany. doi:10.1007/978-3-030-26951-7_17. 2

[TYB17] Itzhak Tamo, Min Ye, and Alexander Barg. Optimal repair of reed-solomon codes: Achieving the cut-set bound. In Chris Umans, editor, *58th Annual Symposium on Foundations of Computer Science*, pages 216–227, Berkeley, CA, USA, October 15–17, 2017. IEEE Computer Society Press. doi:10.1109/FOCS.2017.28. 2

[ZF05] YongBin Zhou and DengGuo 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