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 \( \lambda \)-bits for its binary representation, where \( \lambda \) 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 \( O(\lambda \log \lambda / \log \log \lambda) \).

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—a 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 Wooters [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 scheme 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 \( k \geq 0.867n \) [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, HWW20, 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 \( \varepsilon \) if there are two appropriate secrets such that the joint distributions of the leakage on the secret shares have statistical distance (at least) \( \varepsilon \).

**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 \(m \geq \frac{k \log p}{n + k}\) 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 \(m = \lfloor \lg k \rfloor\) 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 \(\lambda\)-bit binary strings corresponding to the elements \(\{0, 1, \ldots, p - 1\}\), where \(2^{\lambda-1} < p \leq 2^\lambda\). For \(\ell \in \{1, 2, \ldots, \lambda\}\), one can probe the bit at the \(\ell\)-th least significant position from a \(\lambda\)-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 \(\lambda\), 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 \(1 \leq i \leq n\). For \(1 \leq i \leq n\), let \(\rho_i \in [0, 1]\) be the thermal noise parameter of the hardware storing the \(i\)-th secret share.

Let \(\tilde{b}_i\) be a bit that is \(\rho_i\)-correlated with the bit \(b_i\). That is, \(\tilde{b}_i = b_i\) with probability \(\rho_i\); otherwise \(\tilde{b}_i\) is an independent and uniformly random bit. For example, if \(\rho_i = 1\), then \(\tilde{b}_i = b_i\), and, if \(\rho_i = 0\), then \(\tilde{b}_i\) is a uniformly random bit independent of the bit \(b_i\). Intuitively, if the storage hardware has high thermal noise then \(\tilde{b}_i\) 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 \((\tilde{b}_1, \ldots, \tilde{b}_k | s^{(0)})\) and \((\tilde{b}_1, \ldots, \tilde{b}_k | s^{(1)})\) have statistical distance at most \(\varepsilon\). As per convention, a secure secret-sharing scheme requires \(\varepsilon\) to decay faster than any inverse-polynomial in the security parameter \(\lambda\), represented as \(\varepsilon = \text{negl}(\lambda)\).

**Additive secret-sharing scheme results.** 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
In particular, when \( k \) is even, \( \varepsilon \geq \left( \prod_{i=1}^{k} \rho_i \right) \cdot \left( \frac{1}{2^{k(k-1)!}} - \frac{3(k-1)^2 + 1}{p} \right) \).

To interpret this theorem, it is instructive to consider the simplification \( \rho_i = \rho, \) a constant, for all \( i \in \{1, \ldots, k\} \). For this simplification, the lower bound in the expression above, essentially, reduces to

\[
\varepsilon \geq \Theta\left( \frac{(\rho/2)^k}{(k-1)!} \right) \quad \text{for all meaningful values of } k = \text{poly}(\lambda).
\]

When \( \rho = 1 \), the bound above is equivalent to

\[
k \geq \Theta\left( \Gamma^{-1}(1/\varepsilon) \right) = \Theta\left( \log(1/\varepsilon)/\log(1/\varepsilon) \right).
\]

More generally, if all \( \rho_i = \rho \), then the bound is equivalent to

\[
k \geq \Theta\left( \log(1/\varepsilon)/(\log\log(1/\varepsilon) + \log(2/\rho)) \right).
\]

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

**Corollary 1.** Let \( \text{AddSS}(k) \) is \((1 - \text{negl}(\lambda))\)-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 \( 1/2^{\frac{k(k-1)!}{2}} \geq 1/k^k \), the distinguishing advantage of [BDIR18], for all \( k \geq 2 \).

**Shamir secret-sharing scheme results.** 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 \( f(X_i) \).

**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 all roots of the equation \( Z^k - 1 = 0 \). Suppose there exists \( \rho \in F^* \) such that \( \{\rho, \rho^2, \ldots, \rho^k = \rho\} \) is a subset of the evaluation places \( \vec{X} \). If ShamirSS\((n, k, \vec{X})\) is \((1 - \text{negl}(\lambda))\)-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. 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 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 \( k \geq n/(\lambda + 1) \sim n/\lambda \) 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 $\text{AddSS}(k)$ 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. [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 $i \in \{1, \ldots, n\}$. That is, the leaked bit $\tilde{b}_i$ is identical to the stored bit $b_i$ at the hardware location $\ell_i$ that the adversary probes, for all $1 \leq i \leq n$. After that, one can reintroduce the thermal noise parameter into the analysis at the end (see Section 2.4).

Let $\mathbb{N}_0 := \{0, 1, 2, \ldots \}$ be the set of all non-negative integers. Consider $\text{AddSS}(k)$ 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 $\mathbb{N}_0$.

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

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

Observe that if $S_1 + S_2 + \cdots + S_{k-1} \in S_{\text{same}}(s)$ then $b_1 \oplus \cdots \oplus b_k$ will be identical to the parity of $s$. Furthermore, if $S_1 + S_2 + \cdots + S_{k-1} \in S_{\text{diff}}(s)$ 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 $S_1, \ldots, S_{k-1} \in \{0, 1, \ldots, p-1\}$.

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

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

This formulation of the problem has the salient feature that $S_1, \ldots, S_{k-1}$ are independent and uniformly random over the set $\{0, 1, \ldots, p-1\}$.

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 $s^{(0)}$.

\(^1\)The $|$ 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 $s_1, \ldots, s_k$ are uniformly and independently random elements of $F$. Therefore, $b_1, \ldots, b_k$ 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,

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

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

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

Consequently, one concludes that the statistical distance between the distributions $(b_1, \ldots, b_k | s^{(0)})$ and $(b_1, \ldots, b_k | s^{(1)})$ is at least $\varepsilon - \frac{1}{p}$. All that remains is to prove that $\varepsilon$ 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 $S_{\text{same}}(s)$ and $S_{\text{diff}}(s)$ by scaling the length-$p$ intervals into length-one intervals. Define $\mathbb{N}_0 = \{0, 1/p, 2/p, \ldots\}$, represented by $\frac{1}{p} \cdot \mathbb{N}_0$. Let $\hat{s} = s/p \in \{0, 1/p, 2/p, \ldots, (p-1)/p\}$. Next, define $\hat{S}_\text{same}(\hat{s}) = \frac{1}{p} \cdot S_{\text{same}}(s)$ and $\hat{S}_\text{diff}(\hat{s}) = \frac{1}{p} \cdot S_{\text{diff}}(s)$. Let $\hat{S}_1, \hat{S}_2, \ldots, \hat{S}_{k-1}$ be independent and uniformly random distributions over the set $\{0, 1/p, 2/p, \ldots, (p-1)/p\}$. Therefore, our objective is to find

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

Next, consider the simplification $p \to \infty$. For this simplification, observe that (1) $\hat{s} \in [0, 1)$, and (2) $\hat{S}_1, \ldots, \hat{S}_{k-1}$ are independent and uniformly random distribution over $[0, 1)$. The distribution $\hat{S}_1 + \cdots + \hat{S}_{k-1}$ is the well-studied Irwin-Hall distribution with parameter $(k-1)$ [JKB95], represented by $\text{IH}_{k-1}$ over the sample space $[0, k-1)$. For $x \in [0, 1)$, observe that

$$\hat{S}_\text{same}(x) := x + \left( \bigcup_{i \in \mathbb{Z}} (i, i+1) \right), \quad \text{and} \quad \hat{S}_\text{diff}(x) := x + \left( \bigcup_{i \text{ even}} (i, i+1) \right).$$

Therefore, our objective is to lower-bound the expression

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

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 $\varepsilon$ must be at least $1/k!$ when $(k-1)$ is odd; otherwise, if $(k-1)$ is even, then $\varepsilon \geq 1/(2^{k!} k!)$. 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 $\varepsilon$ 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 $\{0, 1/p, \ldots, (p-1)/p\}$. 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 ShamirSS$(n, k, \overline{X})$ such that the evaluation places $\overline{X}$ contains $\rho G$. 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, …, $k-1$ are uniformly random over $F$ for 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 $\delta$ 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 $\overline{b}_i$, which is $\rho_i$-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 $\overline{b}_1, \ldots, \overline{b}_k$ 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 $(\prod_{i=1}^k \rho_i) \delta$.

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 $s_i := f(\rho \cdot \alpha^i) \in F$ 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., $\overline{b}_1 \oplus \overline{b}_2 \oplus \cdots \oplus \overline{b}_k$, 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 $0 < j < k$, $(\alpha)^j + (\alpha^2)^j + \cdots + (\alpha^k)^j = 0$. Hence, we have

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

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

7
Let \( N_0 := \{0, 1, 2, \ldots \} \) be the set of whole numbers (i.e., all non-negative integers). Let \( 0 \leq S_1, S_2, \ldots, S_k \leq p - 1 \) be elements from \( N_0 \) corresponding to the elements \( s_1, s_2, \ldots, s_k \in F \). Similarly, let \( 0 \leq S \leq p - 1 \) be elements from \( N_0 \) 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,

\[
S_{\text{same}} := N_0 \cap \bigcup_{i \in \mathbb{Z}, i \text{ odd}} [ip + kS + 1, (i + 1)p + kS],
\]

\[
S_{\text{diff}} := N_0 \cap \bigcup_{i \in \mathbb{Z}, i \text{ even}} [ip + kS + 1, (i + 1)p + kS].
\]

We have the following claim.

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

Given this claim, our objective is to find a secret \( s^* \) such that difference between \( \Pr[S_1 + S_2 + \cdots + S_{k-1} \in S_{\text{same}}] \) and \( \Pr[S_1 + S_2 + \cdots + S_{k-1} \in S_{\text{diff}}] \) 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

\[
S_{\text{same}}^{\ast} := N_0 \cap \bigcup_{i \in \mathbb{Z}, i \text{ odd}} \left[ ip + \frac{k(p - 1)}{2} + 1, (i + 1)p + \frac{k(p - 1)}{2} \right],
\]

\[
S_{\text{diff}}^{\ast} := N_0 \cap \bigcup_{i \in \mathbb{Z}, i \text{ even}} \left[ ip + \frac{k(p - 1)}{2} + 1, (i + 1)p + \frac{k(p - 1)}{2} \right].
\]

And we are interested in

\[
\text{disc} \,(k - 1, p) := \Pr[S_1 + S_2 + \cdots + S_{k-1} \in S_{\text{same}}^{\ast}] - \Pr[S_1 + S_2 + \cdots + S_{k-1} \in S_{\text{diff}}^{\ast}].
\]

Naturally, \( |\text{disc} \,(k - 1, p)| \) 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 \( \geq |\text{disc} \,(k - 1, p)| - 1/p \).

\(^2\)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 \( \mu \), belong entirely to either \( S_{\text{same}} \) or \( S_{\text{diff}} \). Therefore, we shall pick \( s^* \) as \((p - 1)/2\).
**Roadmap.** In the rest of this paper, we shall show that $|\text{disc}(k-1,p)|$ 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 $S^*_{\text{same}}$ and $S^*_{\text{diff}}$. We first consider the limit of $\text{disc}(k-1,p)$ 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 $\text{disc}(k-1)$. We prove that $\text{disc}(k-1) \geq 1/(2^{k-1} \cdot (k-1)!)$.

These results are presented in Section 4. Next, we examine how quickly does $\text{disc}(k-1,p)$ tend to its limit $\text{disc}(k-1)$ 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 $U: \mathbb{R} \to \mathbb{R}$ 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 $I_{H_k}: \mathbb{R} \to \mathbb{R}$ be the density function of the $k^{th}$ Irwin-Hall distribution. That is, $I_{H_1} = U$ and, for $k > 1$, we have

$$I_{H_k}(x) = \int_{-\infty}^{\infty} I_{H_{k-1}}(y)U(x-y)\,dy.$$  

Observe that $I_{H_k}$ 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.\(^3\)

$$I_{H_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

$$\text{Disc}_k(x) := \int_{-\infty}^{\infty} (-1)^{[y-x]} \cdot I_{H_k}(y)\,dy.$$  

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

- $\text{Disc}_k(0)$ if $k$ is odd;
- $\text{Disc}_k(1/2)$ 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 $f_k: [0, 1/2] \to \mathbb{R}$ as follows to facilitate our analysis.

$$f_k(x) := \sum_{i=-\infty}^{\infty} (-1)^i \cdot I_{H_k}(x+i).$$

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.

$$\frac{d}{dx} I_{H_k}(x) = I_{H_k}'(x) = I_{H_{k-1}}(x) - I_{H_{k-1}}(x-1).$$

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

$$I_{H_k}(x) = \int_{x-1}^{x} I_{H_{k-1}}(y)\,dy.$$  

\(^3\)One can refer to, for example, https://www.randomservices.org/random/special/IrwinHall.html for a proof.
\(^4\)Here, $[x]$ 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 $\text{Disc}_k(x)$. In particular, we are interested in the discrepancy when the black bands is placed symmetrically, which is $\text{Disc}_k(1/2)$ when $k$ is even and $\text{Disc}_k(0)$ when $k$ is odd.

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

\[
\frac{d}{dx} \text{IH}_k(x) = \frac{d}{dx} \int_{x-1}^{x} \text{IH}_{k-1}(y) \, dy = \text{IH}_{k-1}(x) - \text{IH}_{k-1}(x-1).
\]

\[\square\]

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

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

\[
\lim_{\delta \to 0} \text{IH}_k(x + \delta) - \text{IH}_k(x - \delta) = 0
\]

Then

\[
\lim_{\delta \to 0} \text{IH}_k'(x + \delta) - \text{IH}_k'(x - \delta)
= \lim_{\delta \to 0} \text{IH}_{k-1}(x + \delta) - \text{IH}_{k-1}(x - \delta) + \lim_{\delta \to 0} \text{IH}_{k-1}(x - 1 + \delta) - \text{IH}_{k-1}(x - 1 - \delta) = 0
\]

\[\square\]

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

\[
\frac{d}{dx} f_k(x) =: f_k'(x) = 2 \cdot f_{k-1}(x).
\]

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

\[
\frac{d}{dx} f_k(x) = \frac{d}{dx} \sum_{i=-\infty}^{\infty} (-1)^i \cdot \text{IH}_k(x + i)
= \sum_{i=-\infty}^{\infty} (-1)^i \cdot \frac{d}{dx} \text{IH}_k(x + i)
= \sum_{i=-\infty}^{\infty} (-1)^i \cdot (\text{IH}_{k-1}(x + i) - \text{IH}_{k-1}(x + i - 1))
= \sum_{i=-\infty}^{\infty} (-1)^i \cdot \text{IH}_{k-1}(x + i) - \sum_{i=-\infty}^{\infty} (-1)^i \cdot \text{IH}_{k-1}(x + i - 1)
\]
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 \((-1)^i\)s out of the second summation to get:

\[
\frac{d}{dx}f_k(x) = \sum_{i=-\infty}^{\infty} (-1)^i \cdot IH_{k-1}(x+i) + \sum_{i=-\infty}^{\infty} (-1)^{i-1} \cdot IH_{k-1}(x+i-1)
\]

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.

\[
\frac{d}{dx}f_k(x) = \sum_{i=-\infty}^{\infty} (-1)^i \cdot IH_{k-1}(x+i) + \sum_{j=-\infty}^{\infty} (-1)^j \cdot IH_{k-1}(x+j)
\]

\[
= f_{k-1}(x) + f_{k-1}(x)
\]

\[
= 2 \cdot f_{k-1}(x)
\]

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.](image)

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,

\[
f_k(x) = -(f_k(1/2) - f_k(x)) = -2 \int_x^{1/2} f_{k-1}(x) \, dx.
\]

11
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,

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

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. \hfill \qed

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

**Observation 2.**

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

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

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

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

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

$$\sum_{i=-\infty}^{\infty} (-1)^i \int_i^{i+1} \text{IH}_k(y) \, dy + (-1)^{i+1} \int_{i+1}^{i+2} \text{IH}_k(y) \, dy$$

Applying the Leibniz integral rule, we get

$$\text{Disc}_k'(x) = \sum_{i=-\infty}^{\infty} (-1)^i \cdot \text{IH}_k(x+i) - (-1)^{i+1} \cdot \text{IH}_k(x+i)$$

$$= \sum_{i=-\infty}^{\infty} (-1)^i \cdot 2\text{IH}_k(x+i)$$

$$= 2f_k(x)$$

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

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

Next, by Claim 4, we have that $\frac{d}{dx}\text{Disc}_k(x) = 2f_k(x)$ 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 $\frac{d}{dx}\text{Disc}_k(x)$ is nonzero and has a constant sign for $x \in (0, 1/2)$.

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

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

Therefore, because $\text{Disc}_k(0) = 0$ and its derivative is nonzero with a constant sign for $x \in (0, 1/2)$, then $\text{Disc}_k(x)$ is nonzero for all $x \in (0, 1/2)$, so if $k$ is even, then $|\text{Disc}_k(1/2)| > 0$. \hfill \qed
Theorem 3 implies the following corollary, which is our main result on the discrepancy of the Irwin-Hall distribution.

**Corollary 4 (Main Result).**
- \(|\text{Disc}_k(0)| \geq 1/k!\) if \(k\) is odd;
- \(|\text{Disc}_k(1/2)| \geq 1/(2^k k!\) if \(k\) is even.

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

- \(|\text{Disc}_{k-1}(0)| \geq 1/(k - 1)!\) if \(k\) is even;
- \(|\text{Disc}_{k-1}(1/2)| \geq 1/(2^{k-1}(k - 1)!)\) if \(k\) is odd.

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

Since we have proven that for odd \(k\), \(|\text{Disc}_k(0)| > 0\) and for even \(k\), \(|\text{Disc}_k(1/2)| > 0\), it suffices to prove that
- \(f_k(0) \cdot (k - 1)!\) is an integer;
- \(f_{k+1}(1/2) \cdot 2^{k-1}(k - 1)!\) is an integer.

To see this, recall that we have (Fact 1)
\[
\text{IH}_k(x) = \frac{1}{(k - 1)!} \sum_{i=0}^{\lfloor x \rfloor} (-1)^i \binom{k}{i} (x - i)^{k-1}.
\]
Then we have the following formula for \(k! \cdot f_{k+1}(0)\), which is clearly an integer.
\[
k! \cdot f_{k+1}(0) = k! \sum_{u=1}^{k} (-1)^u \cdot \text{IH}_{k+1}(0) = \sum_{u=1}^{k} (-1)^u \sum_{i=0}^{u} (-1)^i \binom{k+1}{i} (-1)^i.
\]
Therefore, \(k! \cdot \text{Disc}_k(0)\) is an integer and therefore \(|k! \cdot \text{Disc}_k(0)| \geq 1\), which implies that \(|\text{Disc}_k(0)| \geq 1/k!\) for odd \(k\), thus proving the first part of the corollary.

For even cases of \(k\) with respect to \(\text{Disc}_k(1/2)\), which corresponds to odd \(k + 1\) with respect to \(f_{k+1}(1/2)\), we have the following
\[
k! \cdot f_{k+1} \left(\frac{1}{2}\right) = \sum_{u=0}^{k} (-1)^u \sum_{i=0}^{u} (-1)^i \binom{k+1}{i} \left(u + \frac{1}{2} - i\right)^k = \sum_{u=0}^{k} (-1)^u \sum_{j=0}^{u-j} (-1)^{u-j} \binom{k+1}{j} \left(j + \frac{1}{2}\right)^k
\]
\[
= \sum_{u=0}^{k} (-1)^u \sum_{j=0}^{u-j} (-1)^{k-j} \binom{k}{j} \frac{1}{2} j^{k-j}
\]
Thus, \(2^k k! \cdot f_{k+1}(1/2)\) is an integer. Therefore, \(|\text{Disc}_k(1/2)| \geq 1/(2^k k!\) for all even \(k\), thus proving the second part of the corollary.

\(\square\)
Remark 1. Our proof is sufficient to prove that

\[
\left( \arg \max_x |\text{Disc}_k(x)| \right) = 1/2,
\]

when \( k \) is even and

\[
\left( \arg \max_x |\text{Disc}_k(x)| \right) = 0,
\]

when \( k \) is odd. To see this, we note that Claim 4 and Lemma 1 together imply that \( \text{Disc}_k(x) \) is monotone on \((0,1/2)\). Plus the fact that \( \text{Disc}_k(x) \) 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 \( x \), \( F_{k,p}(x) \leq 1/p \).

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 \( \alpha \),

\[
\left| \sum_{i=0}^{\alpha} F_{k,p}(i/p) - \int_0^{(\alpha+1)/p} \text{I}_k(x) \, dx \right| \leq k/p.
\]

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

\[
\left| \sum_{i=0}^{\alpha} F_{k,p}(i/p) - \int_0^{(\alpha+1)/p} \text{I}_k(x) \, dx \right| = \left| \sum_{i=0}^{\alpha} \frac{1}{p} \cdot \sum_{j=1}^{p} F_{k-1,p}(i/p - 1 + j/p) - \int_0^{(\alpha+1)/p} \int_{x-1}^x \text{I}_{k-1}(y) \, dy \, dx \right|
\]

\[
= \left| \frac{1}{p} \cdot \sum_{j=1}^{p} \left( \sum_{i=0}^{\alpha+j-p} F_{k-1,p}(i/p) \right) - \int_0^{(\alpha+1)/p} \int_{x-1}^x \text{I}_{k-1}(y) \, dy \, dx \right|
\]

\[
= \left| \frac{1}{p} \cdot \sum_{j=1}^{p} \left( \sum_{i=0}^{\alpha+j-p} F_{k-1,p}(i/p) \right) - \sum_{j=1}^{p} \int_0^{(\alpha+j+1-p)/p} \int_{x-1}^x \text{I}_{k-1}(y) \, dy \, dx \right|
\]

\[
\leq \sum_{j=1}^{p} \int_0^{(\alpha+j+1-p)/p} \left| \sum_{i=0}^{\alpha+j-p} F_{k-1,p}(i/p) - \int_0^x \text{I}_{k-1}(y) \, dy \right| \, dx
\]

\[\quad (1)\]

\(^5\)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 \(1 \leq j \leq p\) and \(x \in ((\alpha + j - p)/p, (\alpha + j + 1 - p)/p)\), we have

\[
\left| \sum_{i=0}^{\alpha+j-p} F_{k,p}(i/p) - \int_0^x |H_{k-1}(y)| \, dy \right| \\
\leq \sum_{i=0}^{\alpha+j-p} F_{k,p}(i/p) - \int_0^{(\alpha+j-1-p)/p} |H_{k-1}(y)| \, dy + \int_{(\alpha+j-1-p)/p}^{(\alpha+j+1-p)/p} |H_{k-1}(y)| \, dy - \int_0^x |H_{k-1}(y)| \, dy \\
\leq (k-1)/p + \int_x^{(\alpha+j+1-p)/p} |H_{k-1}(y)| \, dy \\
\leq (k-1)/p + 1/p = k/p.
\]

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

\[
\sum_{j=1}^p \int_{(\alpha+j-p)/p}^{(\alpha+j+1-p)/p} (k/p) \, dx = p \cdot (1/p) \cdot (k/p) = k/p.
\]

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 \(\alpha \leq \beta\), we have

\[
\left| \sum_{\alpha}^{\beta} F_{k,p}(i/p) - \int_{\beta/p}^{(\alpha+1)/p} |H_k(x)| \, dx \right| \leq (2k)/p.
\]

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

\[
\text{Disc}_k(x) := \int_{-\infty}^{\infty} (-1)^{[y-x]} \cdot |H_k(y)| \, dy.
\]

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

\[
\text{disc} (k) := \text{Disc}_k \left( \frac{k-1}{2} \right) \\
= \int_{-\infty}^{\infty} (-1)^{[y-\frac{k-1}{2}]} \cdot |H_k(y)| \, dy.
\]

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

\[
\text{disc} (k, p) := \sum_{i=-\infty}^{\infty} (-1)^{[\frac{i-(k-1)(p-1)/p}{p}]} F_{k,p}(i/p).
\]

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 \(k, p \in \mathbb{N}\),

\[
|\text{disc} (k) - \text{disc} (k, p)| \leq (3k^2)/p.
\]

In particular, it implies

\[
|\text{disc} (k) - |\text{disc} (k, p)|| \leq (3k^2)/p.
\]

\(^6\)One can verify that \(\text{disc} (k, p)\) is \(\Pr[S_1 + S_2 + \cdots + S_{k-1} \in S_{\text{same}}] - \Pr[S_1 + S_2 + \cdots + S_{k-1} \in S_{\text{diff}}]\) for secret \(s^* = (p-1)/2\) as discussed in Section 3.
\[ \text{Proof.} \] Without loss of generality, we assume \( k = 1 \mod 4 \). The other cases can be proven in a similar manner. By definition,

\[
\begin{align*}
|\text{disc}(k) - \text{disc}(k, p)| &= \left| \int_{-\infty}^{\infty} \left(-1\right)^{\left\lfloor \frac{k-1}{2} \right\rfloor} \cdot \mathbb{I}H_k(y) \, dy - \sum_{i=-\infty}^{\infty} \left(-1\right)^{\left\lfloor \frac{k-1}{2} \right\rfloor} F_{k,p}(i/p) \right| \\
&= \left| \int_{-\infty}^{\infty} \left(-1\right)^{\left\lfloor \frac{k-1}{2} \right\rfloor} \cdot \mathbb{I}H_k(y) \, dy - \sum_{i=-\infty}^{\infty} \left(-1\right)^{\left\lfloor \frac{k-1}{2} \right\rfloor} F_{k,p}(i/p) \right| \\
&= \left| \int_{-\infty}^{\infty} \left(-1\right)^{\left\lfloor \frac{k-1}{2} \right\rfloor} \cdot \mathbb{I}H_k(y) \, dy - \sum_{i=-\infty}^{\infty} \left(-1\right)^{\left\lfloor \frac{k-1}{2} \right\rfloor} F_{k,p}(i/p) \right| \\
&\leq \sum_{i=0}^{k-1} \left| \left(-1\right)^{i+1} \int_{i}^{i+1} \mathbb{I}H_k(y) \, dy - \sum_{j=ip}^{(i+1)p-1} \left(-1\right)^{i} F_{k,p}(j/p) \right| \\
&\leq \sum_{i=0}^{k-1} \left| \left(-1\right)^{i+1} \int_{i}^{i+1} \mathbb{I}H_k(y) \, dy - \sum_{j=ip}^{(i+1)p-1} F_{k,p}(j/p) \right| + k/p \\
&= \frac{3k^2}{p} \tag{Corollary 5}
\]

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 \( \left(-1\right)^{i} \neq \left(-1\right)^{i+1} \); (b) we always have \( F_{k,p}(x) \leq 1/p \) for all \( x \). This completes the proof. \( \square \)

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.

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

Proof. We prove by induction on \( k \).

Base case. For \( k = 1 \), it is clearly that \( \Pr[\bar{b}_1 = b_1] = \frac{1}{2}(1 + \rho_1) \) since \( \bar{b}_1 \) is a \( \rho_1 \)-correlated copy of \( b_1 \).

Inductive hypothesis. Suppose \( \Pr \left[ \bar{b}_1 \oplus \ldots \oplus \bar{b}_{k-1} = b_1 \oplus \ldots \oplus b_{k-1} | s \right] = \frac{1}{2} \left( 1 + \prod_{i=1}^{k-1} \rho_i \right) \).

Inductive step. We have

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

which completes the proof. \( \square \)

Remark. An alternative way to prove this is to apply basic Fourier property of the convolution operator. Observe that each \( \bar{b}_i \) 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.

\[
\text{SD} \left( \tilde{b}_1 \oplus \ldots \oplus \tilde{b}_k | s^{(0)} \right) = \left( \prod_{i=1}^{k} \rho_i \right) \text{SD} \left( b_1 \oplus \ldots \oplus b_k | s^{(0)} \right)
\]

Proof. By Claim 6, we have

\[
\text{SD} \left( \tilde{b}_1 \oplus \ldots \oplus \tilde{b}_k | s^{(0)} \right) = \frac{1}{2} \left( \sum_{b} \left| \text{Pr} \left[ \tilde{b}_1 \oplus \ldots \oplus \tilde{b}_k = b | s^{(0)} \right] - \text{Pr} \left[ \tilde{b}_1 \oplus \ldots \oplus \tilde{b}_k = b | s^{(1)} \right] \right)
\]

\[
= \frac{1}{2} \left( \sum_{b} \left| \text{Pr} \left[ b_1 \oplus \ldots \oplus b_k = b | s^{(0)} \right] \cdot \frac{1}{2} \left( 1 + \prod_{i=1}^{k} \rho_i \right) + \text{Pr} \left[ b_1 \oplus \ldots \oplus b_k = 1 - b | s^{(0)} \right] \cdot \frac{1}{2} \left( 1 - \prod_{i=1}^{k} \rho_i \right)
\right.
\]

\[
- \text{Pr} \left[ b_1 \oplus \ldots \oplus b_k = b | s^{(1)} \right] \cdot \frac{1}{2} \left( 1 + \prod_{i=1}^{k} \rho_i \right) + \text{Pr} \left[ b_1 \oplus \ldots \oplus b_k = 1 - b | s^{(1)} \right] \cdot \frac{1}{2} \left( 1 - \prod_{i=1}^{k} \rho_i \right)
\]

\[
= \frac{1}{2} \left( \sum_{b} \left| \text{Pr} \left[ b_1 \oplus \ldots \oplus b_k = b | s^{(0)} \right] - \text{Pr} \left[ b_1 \oplus \ldots \oplus b_k = b | s^{(1)} \right] \right)
\]

\[
= \frac{1}{2} \prod_{i=1}^{k} \rho_i \cdot \text{SD} \left( b_1 \oplus \ldots \oplus b_k | s^{(0)} \right)
\]

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

\[
\text{SD} \left( \tilde{b}_1, \ldots, \tilde{b}_k \right) \geq \left| \text{Pr} \left[ \tilde{b}_1 \oplus \ldots \oplus \tilde{b}_k = 0 | s^{(0)} \right] - \text{Pr} \left[ \tilde{b}_1 \oplus \ldots \oplus \tilde{b}_k = 0 | s^{(1)} \right] \right|
\]

\[
= \text{SD} \left( \tilde{b}_1 \oplus \ldots \oplus \tilde{b}_k | s^{(0)} \right) \prod_{i=1}^{k} \rho_i \cdot \text{SD} \left( b_1 \oplus \ldots \oplus b_k | s^{(0)} \right)
\]

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 \(\text{disc} \left( k - 1 \right) \geq \frac{1}{2^{k-1}(k-1)!} - \frac{3(k-1)^2}{p}\).

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

\[
\text{SD} \left( b_1 \oplus \ldots \oplus b_k | s^{(0)} \right) \geq \frac{1}{2} \cdot \left( \text{disc} \left( k - 1 \right) - 1/p \right)
\]

\[
\geq \frac{1}{2^{k-1}(k-1)!} - \frac{3(k-1)^2 + 1}{p}.
\]

Consequently,

\[
\text{SD} \left( \tilde{b}_1, \ldots, \tilde{b}_k | s^{(0)} \right) \geq \prod_{i=1}^{k} \rho_i \cdot \left( \frac{1}{2^{k-1}(k-1)!} - \frac{3(k-1)^2 + 1}{p} \right).
\]

17
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 \( \text{disc} (k - 1) \geq \frac{1}{(k-1)!} - \frac{3(k-1)^2}{p} \). Hence, similarly, we get

\[
\text{SD} \left( \left( \tilde{b}_1, \ldots, \tilde{b}_k \middle| s^{(0)} \right), \left( \tilde{b}_1, \ldots, \tilde{b}_k \middle| s^{(1)} \right) \right) \geq \left( \prod_{i=1}^{k} \rho_i \right) \cdot \left( \frac{1}{2(k-1)!} - \frac{3(k-1)^2 + 1}{p} \right).
\]

\[\square\]
References


