Security of Shamir's Secret-sharing against Physical Bit Leakage: Secure Evaluation Places

Abstract. NIST aims to recommend best practices to make secret-sharing schemes like Shamir's and the additive secret-sharing scheme more secure. The additive secret-sharing scheme's security is completely broken by leaking one physical bit from every secret share – leaking their least significant bit (LSB) suffices. Shamir's secret-sharing scheme inherits these vulnerabilities if its evaluation places are carelessly chosen. To further NIST's efforts in this context, it is natural to wonder which evaluation places would make Shamir's secret-sharing scheme robust to such attacks.

We study Shamir secret-sharing schemes where the number of parties n equals the reconstruction threshold k. A random choice of evaluation places is known to be robust to such leakages with high probability. However, techniques to distinguish secure evaluation places from insecure ones are unknown.

Our work introduces the following innovations.

1. A modulus choice for which protection against the LSB attack ensures protection against any physical bit attack.
2. An algorithm to efficiently identify evaluation places that are secure against the LSB attack.

Building on these, we recommend modulus and evaluation places that make Shamir's secret-sharing scheme robust to physical bit leakage – the first complete derandomization of existing Monte-Carlo results.

Our work introduces new techniques to analyze the security of secret-sharing schemes. It connects the security of secret-sharing schemes to the orthogonality properties of a system of square wave functions. The quality of this connection depends on finding good simultaneous rational approximations – a Dirichlet-type approximation problem efficiently solved using the LLL algorithm.

1 Introduction

Recently, the National Institute of Standards and Technology (NIST) called for submissions for future recommendations and guidelines to make threshold schemes more secure [6]. The additive and Shamir's secret-sharing schemes are fundamental building blocks with numerous applications in threshold cryptography and distributed computing [2], like secure storage and computation over secrets and building sophisticated public-key primitives. The insecurity of these fundamental building blocks endangers any primitive built on top of them.

Probing wires and introducing random faults into them seem innocuous but lead to devastating attacks – the more straightforward the attack, the greater a security threat it poses. For example, Boneh et al. [5] showed the vulnerability of

computing RSA signatures to random fault injection into memory. Ishai, Sahai, and Wagner [13] introduced the bit probing model to theoretically investigate threats posed by an adversary that can probe a bounded number of memory locations. The additive and Shamir's secret-sharing schemes have been used to design masking schemes as countermeasures to side-channel attacks in this model [13, 27]. This work studies the security of secret-sharing schemes when an adversary can probe physical bits from memory that stores the secret shares in their binary representation.

The standard notion of security for secret-sharing schemes considers an adversary who obtains some secret shares and has no information about the remaining secret shares. However, in our context, the adversary can probe a few physical bits from all secret shares in the physical bit probe model. For example, the adversary can leak every secret share's least significant bits (LSB). A secret-sharing scheme is robust to such probing attacks if the leakage remains statistically independent of the secret [3, 8].

The LSB attack breaks the additive secret-sharing scheme's security [19, 21]. For any finite field, there are two secrets that the adversary can distinguish with a constant $(2/\pi)^n$ advantage. Shamir's secret-sharing scheme presents a (potentially) secure alternative to the additive secret-sharing scheme. However, it inherits the additive secret-sharing scheme's vulnerabilities if the evaluation places are carelessly chosen [19, 7]. Although it is known that a random choice of evaluation places is secure with high probability against physical bit probing attacks [19], there is no algorithm to classify a given set of evaluation places as secure or not. This is the classical challenge of searching hay in the haystack (or finding water in the ocean) problems [30].

Model. Our work studies Shamir's secret-sharing scheme over prime fields where the number of parties n equals the reconstruction threshold k. We study the security of such secret-sharing schemes against an adversary who leaks one physical bit from every secret share. The security parameter λ represents the number of bits in the binary representation of a secret share.

Our results. Based on our technical contributions, we recommend choosing prime fields of order $p = 2^\lambda - 1$, i.e., Mersenne primes. For the base $n = k = 2$ case, we present an efficient algorithm to identify secure evaluation places for Shamir's secret-sharing scheme. The statistical distance of any leakage for two secrets is at most $1/\sqrt{p}$ for these secure evaluation places. Our algorithm identifies at least $1 - 1/\sqrt{p}$ fraction of all secure evaluation places. Furthermore, we also present explicit evaluation places secure for any Mersenne prime p.

Next, we lift the security of the base scheme to the security of Shamir's secret-sharing involving more parties, i.e., $n = k > 2$. Choosing 2 (among the n) evaluation places securely ensures that the larger secret-sharing scheme is secure.

Remark 1 (Perspective: A Complete Derandomization). We completely derandomize the Monte Carlo construction of [19] when $n = k = 2$. They showed that a random set of evaluation places is secure, with high probability. Even though nearly all evaluation places are secure, one could not identify one. Such

a phenomenon is relatively common in mathematics and computer science. For example, in designing good randomness extractors and linear codes. We design an efficient algorithm to identify nearly all secure evaluation places. Additionally, we also present explicit secure evaluation places.

Technical innovations. An "exponential-type" sum involving a periodic function over the finite field F captures the statistical distance between the leakage for two different secrets. Estimating this sum is challenging. We establish a new connection to a family of periodic square waves to study our periodic function. The similarity between the square waves and their offsets, captured by an integral, serves as a proxy to estimate the sum. Choosing an appropriate basis (by solving a Dirichlet-type approximation problem using the LLL algorithm [17]) ensures the accuracy of this estimation strategy. These analysis techniques, in the context of security analysis of secret-sharing schemes, are new and possibly of broader interest.

Open problems and technical bottlenecks. Motivated by applications in leakage-resilient MPC [14], there is a significant interest in designing explicit secret-sharing schemes for various access structures (for example, threshold and Q_2 access structures) that are resilient to leakage attacks. Our results contribute to this general research area. Below, we highlight some immediate extensions of our work and their technical challenges.

Investigating the case of composite order fields for our problem is open. Even the probabilistic version of this problem is open for composite order fields – [19] proved their probabilistic result *only for prime fields*. Naïvely interpreting F_{p^t} as an F_p-ring is insufficient. Vulnerabilities to physical bit leakage are associated with the binary representation of the field elements. The monic deg t irreducible polynomial $\Pi(Z)$, such that $F_{p^t} \cong F_p[Z]/\Pi(Z)$, determines this representation. Therefore, the characterization of secure evaluation places must account for this irreducible polynomial $\Pi(Z)$. So, more fundamentally, are there "better" or "worse" choices for the irreducible polynomial?

Investigating our problem for $n > k$ poses non-trivial technical challenges, even for prime fields. For our $n = k$ case, studying leakage-resilience required determining the "similarity" between two square waves. For the $n > k$ case, one needs to determine the "hashing properties" of three or more square waves. For example, three square waves can generate eight sign tuples $(\sigma_1, \sigma_2, \sigma_3) \in \{\pm 1\}^3$. If the preimages of each of these eight sign tuples have (nearly) identical cardinality, then they are good hashes, resulting in leakage resilience.

Leaking multiple bits from each secret share also encounters similar technical challenges. In particular, characterizing good hashing properties is required.

1.1 Prior Related Works

Local leakage resilience. There is a significant interest in characterizing the leakage-resilience of practical secret-sharing schemes, like the additive and Shamir's secret-sharing scheme. [19] proved that, for reconstruction threshold $k = 2$ and

an arbitrary number of parties n, choosing evaluation places at random yields a leakage-resilient Shamir secret-sharing scheme with high probability against physical bit leakage. A sequence of works also determined the optimal leakage attack [19, 1, 21]. Other Monte Carlo constructions have also been proposed in [23, 20].

Another flavor of results characterizes the leakage-resilience of Shamir's secret-sharing scheme for a large number of parties. For example, when $k \geqslant 0.78n$, Shamir's secret-sharing scheme (with any evaluation places) is leakage-resilient to (arbitrary) one-bit local leakage. Here the insecurity is exponentially small in n [3, 4, 23, 22]. Contrast this with our scenario, where the insecurity is exponentially small in the security parameter, which is independent of n. [25] proved that Shamir's secret-sharing scheme is insecure to local leakage when n/k is large.

Square wave function families. Various families of square waves find wide applications in science and engineering. For example, consider the ones proposed by Haar [9], Walsh [32], and Rademacher [26]. In our work, we connect the leakage resilience of secret-sharing schemes with the properties of another family of square waves (see for example [31, 12, 11])

$$\Big\{ \operatorname{sign} \sin(2\pi k \cdot x) \Big\}_{k \in \mathbb{Z}}.$$

Previous works [31, 12] have studied the orthogonality of this family of waves. Our objective is to study, more generally, the "similarity" among these waves and their offsets – functions of the form $\operatorname{sign} \sin(2\pi k \cdot (x - \delta))$, for $\delta \in \mathbb{R}$. Zero similarity, in our context, coincides with orthogonality.

Remark 2 (Perspective: Square waves & their offsets). To appreciate the sophistication of this square wave family, consider the following example. Recall from the orthogonality of sine-waves, that $\sin(2\pi \cdot x)$ and $\sin(2\pi \cdot 3x)$ are orthogonal over the interval $[0, 1]$. However, the functions $\operatorname{sign} \sin(2\pi \cdot x)$ and $\operatorname{sign} \sin(2\pi \cdot 3x)$ are *not* orthogonal – their inner product is $1/3$. Most fascinatingly, the functions $\operatorname{sign} \sin(2\pi \cdot x)$ and (the offset) $\operatorname{sign} \sin(2\pi \cdot 3(x - 1/12))$ are orthogonal over $[0, 1]$.

Simultaneous Diophantine Approximation. Solving simultaneous Diophantine approximation problems is a well-studied problem. This problem arises when choosing a "good basis" for a lattice. In our context, for an odd prime p, given distinct $\alpha_1, \alpha_2 \in \{1, 2, \ldots, p-1\}$, our objective is to find $q \in \{1, 2, \ldots, p-1\}$ such that $q\alpha_1 \mod p$ and $q\alpha_2 \mod p$ are either in the range $\{1, \ldots, \sqrt{p}\}$ or $\{p - \sqrt{p}, \ldots, p-1\}$. The integers $q\alpha_1 \mod p$ and $q\alpha_2 \mod p$, intuitively, have "small norm $\mod p$." We will use the classical LLL algorithm [17] to efficiently achieve this objective (see Supporting Material A).

The Dirichlet approximation theorem [28, 29] states that, for any $\alpha \in \mathbb{R}^d$ and any positive integer N, there is a denominator $1 \leqslant q \leqslant N^d$ such that

$$\max_{i \in \{1,2,\ldots,d\}} \{q\alpha_i\} \leqslant \frac{1}{N}.$$

Computing this solution is computationally challenging [16]. However, we can efficiently solve this problem by slightly weakening the upper bound on q. The seminal LLL algorithm [17], in particular, for $\alpha \in \mathbb{Q}^d$, finds $1 \leqslant q \leqslant 2^{d(d+1)/4} \cdot N^d$ such that

$$\max_{i \in \{1,2,\ldots,d\}} \{q\alpha_i\} \leqslant \frac{1}{N}.$$

1.2 Our Results

We introduce a few definitions to facilitate the presentation of our results.

Shamir's secret-sharing scheme. Shamir's secret-sharing scheme among n parties with reconstruction threshold k over a finite field F works as follows. Fix a secret $s \in F$. Consider arbitrary distinct evaluation places $\alpha_1, \alpha_2, \ldots, \alpha_n \in F^*$. Pick a random F-polynomial $P(X)$ such that $\deg P < k$ and $P(0) = s$. The secret shares are $s_1 = P(\alpha_1)$, $s_2 = P(\alpha_2)$, $\ldots$, and $s_n = P(\alpha_n)$. We denote this secret-sharing scheme by $\mathsf{ShamirSS}(n, k, \vec{\alpha})$. The joint distribution of the secret shares is $\mathsf{Share}(s)$ – other parameters will be apparent from the context.

Representation. The secret shares are stored in their natural binary representation. For the prime field F_p (of order p), the elements of this field correspond to the binary representation of the elements $\{0, 1, \ldots, (p-1)\}$. The security parameter λ is the number of bits in the binary representation. For example, in the case of a prime field F_p, we have $2^{\lambda-1} < \mathsf{card}(F_p) = p < 2^{\lambda}$.

Leakage Functions. This work considers physical bit leakage. So, $\mathrm{LSB}_i \colon F \to \{0,1\}$ is the function that outputs the i-th least significant bit. For example, LSB_0 (or, LSB, for brevity) outputs 0 for the elements $\{0, 2, \ldots, (p-1)\}$, where F is a prime field of order $p \geqslant 3$. Moreover, $\mathrm{LSB}_{\lambda-1}$ outputs the most significant bit of the elements. $\vec{\mathrm{LSB}}_{i_1,\ldots,i_n} := (\mathrm{LSB}_{i_1}, \mathrm{LSB}_{i_2}, \ldots, \mathrm{LSB}_{i_n})$ represents a leakage function, where $i_1, \ldots, i_n \in \{0, 1, \ldots, \lambda - 1\}$. For $k \in \{1, 2, \ldots, n\}$, this leakage function will leak the i_k-th LSB from the k-th secret share. The joint distribution of the leakage is $\vec{\mathrm{LSB}}_{i_1,\ldots,i_n}(\mathsf{Share}(s))$.

Leakage Resilience. $\mathsf{ShamirSS}(n, k, \vec{\alpha})$ has *at most* ε *insecurity* against a family of leakage functions $\mathcal{F}$, if the statistical distance between $f(\mathsf{Share}(0))$ and $f(\mathsf{Share}(s))$ is $\leqslant \varepsilon$, for all $s \in F^*$ and $f \in \mathcal{F}$. $\mathsf{ShamirSS}(n, k, \vec{\alpha})$ has *at least* ε *insecurity* against a family of leakage functions $\mathcal{F}$, if the statistical distance between $f(\mathsf{Share}(0))$ and $f(\mathsf{Share}(s))$ is $\geqslant \varepsilon$, for some $s \in F^*$ and $f \in \mathcal{F}$.

Physical Bit Leakage For the $n = k = 2$ case, we recommend using finite fields F_p, where p is a Mersenne prime – a prime of the form $2^{\lambda} - 1$. Given distinct evaluation places (α_1, α_2) as input, the efficient algorithm in Figure 1 classifies whether it is secure to physical bit leakage attacks or not. Corollary 1 summarizes the properties of this decision algorithm. Section 7 presents the proof. Supporting Material C enumerates all secure evaluation places for a small Mersenne prime $p = 2^{13} - 1$ using our algorithm. Finally, Section 7.4 presents explicit choices of secure evaluation places: any α_1, α_2 satisfying $\alpha_2 \cdot \alpha_1^{-1} = 2^{\lfloor \lambda/2 \rfloor} - 1$ is secure – the resulting secret-sharing schemes have at most $\mathcal{O}\big(1/\sqrt{p}\big)$ insecurity.

Input. Distinct evaluation places $\alpha_1, \alpha_2 \in F^*$, and F is the finite field of order p, a Mersenne prime

Output. Decide whether the evaluation places (α_1, α_2) are secure to all physical bit leakage attacks

Algorithm.

1. If there is $k \in \{0, 1, \ldots, \lambda - 1\}$ such that $2^k \alpha_i = \alpha_2$: Return insecure
2. For $k \in \{0, 1, \ldots, \lambda - 1\}$:
   (a) Call the algorithm in Figure 2 with evaluation places $(2^k \alpha_1, \alpha_2)$
   (b) If the algorithm returns "may be insecure," return may be insecure
3. Declare $\mathsf{ShamirSS}(2, 2, (\alpha_1, \alpha_2))$ is secure against physical bit attacks.

Fig. 1. Identify secure evaluation places for Shamir's secret-sharing scheme against all physical bit leakage attacks.

Corollary 1 (Analysis of Decision Algorithm in Figure 1). *Let F_p be a prime field, where p is the Mersenne prime $2^\lambda - 1$. Among all possible distinct evaluation places, our algorithm classifies at least*

$$1 - \frac{1}{4 \ln 2} \cdot \frac{(\ln n)^2}{\sqrt{p}} \cdot (1 + o(1))$$

fraction of them as secure. The insecurity of $\mathsf{ShamirSS}(2, 2, (\alpha_1, \alpha_2))$ secret-sharing scheme, for any secure (α_1, α_2), against physical bit attacks is

$$\varepsilon \leqslant \frac{1 + 8^{5/3}}{\sqrt{p}} \cdot (1 + o(1)) \,.$$

Theorem 3 (in Section 3.4) presents new LSB attacks on Shamir's secret-sharing scheme for vulnerable evaluation places.

Bootstrapping $n = k > 2$. We recommend using a prime field F_p, such that $p = 2^\lambda - 1$.

Corollary 2 (Lifting Security). *Suppose $\mathsf{ShamirSS}(2, 2, (\beta_1, \beta_2))$ has ε-insecurity against physical bit leakages. For $n \geqslant 2$ and $\vec{\alpha} \in (F^*)^n$, $\mathsf{ShamirSS}(n, n, \vec{\alpha})$ is 2ε insecure against physical bit leakages if the following conditions are satisfied.*

$$\beta_1 = \left(\alpha_1 \prod_{j \neq 1} (\alpha_1 - \alpha_j) \right)^{-1} \text{ and } \beta_2 = \left(\alpha_2 \prod_{j \neq 2} (\alpha_2 - \alpha_j) \right)^{-1} .$$

Section 8 presents Theorem 4 and its proof (using Fourier analysis), which implies this corollary. So, we can construct $\mathsf{ShamirSS}(n, n, \vec{\alpha})$ with $1/\sqrt{p}$ insecurity against physical bit leakage attacks.

Remark 3 (Subtlety). Note that we are *not* recommending choosing (α_1, α_2) to be secure positions and then choose the remaining $(\alpha_3, \ldots, \alpha_n)$ arbitrarily. The

relationship between (β_1, β_2) and $\vec{\alpha}$ is established via the properties of the dual of the Generalized Reed-Solomon codes.

Remark 4. Naïve attempts to use induction to prove this result fails. Fix (β_1, β_2). Then, one chooses $(\alpha_1, \ldots, \alpha_{n-1})$ such that the conditions are satisfied. Extending this vector to $(\alpha_1, \ldots, \alpha_{n-1}, \alpha_n)$ will not satisfy these conditions. Instead, we present a more direct proof of our result.

Input. Distinct evaluation places $\alpha_1, \alpha_2 \in F^*$

Output. Decide whether the evaluation places (α_1, α_2) are secure to the LSB leakage attack

Algorithm.

1. Define the equivalence class
$$[\alpha_1 : \alpha_2] := \left\{ (u, v) \colon u = \Lambda \cdot \alpha_1, v = \Lambda \cdot \alpha_2, \Lambda \in F^* \right\}.$$
Use the LLL [16] algorithm to (efficiently) find $(u, v) \in [\alpha_1 : \alpha_2]$ such that
$$u, v \in \{-B, -(B-1), \ldots, 0, 1, \ldots, (B-1), B\} \mod p,$$
where $B := \left\lceil 2^{3/4} \cdot \sqrt{p} \right\rceil$. For completeness, Figure 3 in Supporting Material A presents this algorithm.
2. Remark: Henceforth, our algorithm interprets $u, v \in \{-B, \ldots, 0, 1, \ldots, B\} \mod p$ as integers.
3. Compute $g = \gcd(u, v)$.
4. If $u \cdot v / g^2$ is even: Declare $\mathsf{ShamirSS}(2, 2, (\alpha_1, \alpha_2))$ is secure to LSB leakage attacks
5. (Else) If $u \cdot v / g^2$ is odd and $\left| u \cdot v / g^2 \right| \geqslant \sqrt{p}$: Declare $\mathsf{ShamirSS}(2, 2, (\alpha_1, \alpha_2))$ is secure to LSB leakage attacks
6. (Else) Declare that the security of $\mathsf{ShamirSS}(2, 2, (\alpha_1, \alpha_2))$ against LSB attacks may be insecure

Fig. 2. Identify secure evaluation places for Shamir's secret-sharing scheme against the LSB leakage attack.

LSB Leakage The algorithm in Figure 1 calls the subroutine in Figure 2, an efficient algorithm to determine if input evaluation places are secure against the LSB leakage. This decision algorithm works for all odd prime fields. Corollary 3 summarizes the properties of this decision algorithm.

Corollary 3 (Analysis of Decision Algorithm in Figure 2). *Let F be the prime field of order $p \geqslant 3$. Among all possible distinct evaluation places (α_1, α_2), our algorithm classifies at least*
$$1 - \frac{1}{4} \cdot \frac{\ln p}{\sqrt{p}} (1 + o(1))$$

fraction of them as secure. The insecurity of $\mathsf{ShamirSS}(2,2,(\alpha_1,\alpha_2))$ *secret-sharing scheme, for any secure* (α_1,α_2)*, against the LSB attack is*

$$\varepsilon \leqslant \frac{1+8^{5/3}}{\sqrt{p}} \cdot (1+o(1))\,.$$

Section 3 proves this corollary. Theorem 3 in Section 3.4 identifies new LSB attacks.

1.3 Organization of the Paper

1. Section 2 introduces some minimal notations.
2. Section 3 considers the LSB attack. It presents our algorithm in Figure 2, elaborates on its underlying technical ideas, and analyzes its properties. Its analysis relies on technical results from the following three sections.
3. Section 4 presents properties of our family of square waves. Section 5 presents results related to a summation (involving a periodic function) that we need to estimate. Finally, Section 6 connects the leakage resilience of secret-sharing schemes to this summation.
4. Section 7 considers physical bit attacks. It presents our algorithm in Figure 1 and analyzes it.
5. Section 8 presents the technical content that lifts the security of 2-party Shamir's secret-sharing scheme to n-party Shamir's secret-sharing scheme.

2 Notations

For real numbers $a < b$ and ε, the notation $[a,b] \pm \varepsilon$ represents the interval $[a-\varepsilon, b+\varepsilon]$. For brevity, $a \pm \varepsilon$ represents $[a,a] \pm \varepsilon$, which is the set $[a-\varepsilon, a+\varepsilon]$.

For a set S, $\mathsf{card}(S)$ represents its cardinality. For $S \subseteq F$ and $x \in F$, we denote $S \cdot x$ as the set $\{s \cdot x : s \in S\}$. For $S \subseteq F$, the function $\mathbb{1}_S \colon F \to \{0,1\}$ is the indicator function of the set S: $\mathbb{1}_S(x) = 1$, if $x \in S$; otherwise, $\mathbb{1}_S(x) = 0$.

For functions $f, g \colon \mathbb{N} \to \mathbb{N}$, we say $f(\lambda) \sim g(\lambda)$ if $f(\lambda) = g(\lambda) \cdot (1 + \mathrm{o}(1))$. We write $f(\lambda) \lesssim g(\lambda)$, if $f(\lambda) \leqslant g(\lambda) \cdot (1 + \mathrm{o}(1))$.

For a leakage function $f \colon F \to \{0,1\}$, we define $f^{-1}(0) = \{x \in F \colon f(x) = 0\}$.

3 Security against Least Significant Bit Leakage

We consider Shamir's secret-sharing scheme among $n = 2$ parties with reconstruction threshold $k = 2$ over the prime field F of order $p \geqslant 3$. The secret-sharing scheme is the Massey secret-sharing scheme [24] corresponding to the (punctured) Reed-Solomon code with evaluation places $(0, \alpha_1, \alpha_2)$. That is, the dealer chooses a random F-polynomial $P(Z)$ of degree $< k$ conditioned on $P(Z=0)$ being the secret s. Evaluating this polynomial at $Z = \alpha_1$ and $Z = \alpha_2$ generates the (respective) secret shares s_1 and s_2. This secret-sharing scheme is referred to as $\mathsf{ShamirSS}(n=2, k=2, (\alpha_1,\alpha_2))$.

Objective 1 *Given* (α_1, α_2) *as input, decide if* $\mathsf{ShamirSS}(2, 2, (\alpha_1, \alpha_2))$ *is secure to the LSB leakage attack.*

To this end, the following "normalization step" is helpful.

Proposition 1 (Equivalence Classes for Evaluation Places). *The (punctured) Reed-Solomon code corresponding to evaluation places* $(0, \alpha_1, \alpha_2)$ *is identical to the (punctured) Reed-Solomon code corresponding to evaluation places* $(0, \Lambda \cdot \alpha_1, \Lambda \cdot \alpha_2)$*, for any* $\Lambda \in F^*$*.*

This proposition is a consequence of the properties of Generalized Reed-Solomon codes [10, 18]. In particular, since the linear codes are identical, the corresponding Massey secret-sharing schemes have identical resilience/vulnerability to attacks. That is, the $\mathsf{ShamirSS}(2, 2, (\alpha_1, \alpha_2))$ and the $\mathsf{ShamirSS}(2, 2, (\Lambda \cdot \alpha_1, \Lambda \cdot \alpha_2))$ secret-sharing schemes have identical resilience/vulnerability to attacks, for any $\Lambda \in F^*$. Therefore, for given distinct evaluation places $\alpha_1, \alpha_2 \in F^*$, we define the equivalence class

$$[\alpha_1 \colon \alpha_2] := \left\{ (u, v) \colon (u, v) = (\Lambda \cdot \alpha_1, \Lambda \cdot \alpha_2), \Lambda \in F^* \right\}.$$

There are $(p - 2)$ such equivalence classes.[1] Our updated objective is:

Objective 2 *Given* (α_1, α_2) *as input (for distinct* $\alpha_1, \alpha_2 \in F^*$*), decide whether* $\mathsf{ShamirSS}(2, 2, (u, v))$ *is secure to the LSB leakage attack, for all* $(u, v) \in [\alpha_1 : \alpha_2]$*.*

If $\mathsf{ShamirSS}(2, 2, (u, v))$ is secure for one $(u, v) \in [\alpha_1 : \alpha_2]$, then all pairs of evaluation places in this equivalence class shall result in a secure secret-sharing scheme. We propose the algorithm for this decision problem in Figure 2.

When our algorithm declares Shamir's secret sharing scheme "secure," the LSB attack can distinguish any two secrets with an advantage of (at most) $\mathcal{O}\big(1/\sqrt{p}\big)$, which is exponentially small in the security parameter. Section 3.2 and Section 3.3 calculate this upper bound on the insecurity. Furthermore, for only an exponentially small fraction of the equivalence classes, our algorithm declares "may be insecure" (see Section 3.1). This case subsumes all insecure instances of Shamir's secret-sharing scheme. For some of these instances, we can (indeed) identify and demonstrate their insecurity (see Section 3.4 for new attacks on Shamir secret-sharing scheme). Corollary 3 follows from the analysis in Section 3.1, and Theorem 1 and Theorem 2.

Remark 5. Our decision algorithm in Figure 2 depends on the LLL algorithm's output. For one (α_1, α_2), there may be multiple $(u, v) \in [\alpha_1, \alpha_2]$ that the LLL algorithm can output. For some of these pairs, our algorithm may declare "secure." For other pairs, our algorithm may declare "may be insecure."

[1] Consider the set $S := \{(1, \alpha) \colon \alpha \in F \setminus \{0, 1\}\}$. Consider the mapping $[\alpha_1 : \alpha_2] \mapsto (1, \alpha_1 \alpha_2^{-1})$. This mapping is a bijection between the set of all equivalence classes and the set S.

For example, consider the prime $p = 127$ and $(\alpha_1, \alpha_2) = (1, 23)$. In this case, $B = \lceil 2^{3/4}\sqrt{p} \rceil = 19$. Note that $(-11, 1) \in [\alpha_1 : \alpha_2]$ and $(6, 11) \in [\alpha_1 : \alpha_2]$. If the LLL algorithm returns $(11, -1)$, our algorithm will declare "may be insecure." If the LLL algorithm returns $(6, 11)$, our algorithm will declare "secure."

Remark 6. When our algorithm in Figure 2 declares "may be insecure," it indicates that there *may* be an attack on the secret-sharing scheme with those evaluation places. The existence of an attack with a significant advantage is not necessary. Section 3.4 reconstructs one such attack, and it has a significant advantage for some instances.

3.1 Analysis of Our Algorithm in Figure 2: "May be Insecure"

We show that our algorithm outputs "may be insecure" only for an exponentially small fraction of the equivalence classes.

Suppose $a = (u/g)$ and $b = (v/g)$, where $g = \gcd(a, b)$. We need to upper bound the cardinality of the set

$$S := \left\{ (a, b) \colon \text{odd } a, \text{ odd } b, \text{ and } |ab| \leqslant \sqrt{p} \right\}.$$

For any a, a positive b lies in the set $\{1, 3, 5, \ldots, 2n_a - 1\}$, such that $(2n_a - 1)$ is the largest odd number satisfying $a \cdot (2n_a - 1) \leqslant \sqrt{p}$. So, the number of potential odd positive b's is $n_a \leqslant (\sqrt{p} + a)/2a$. As a result, the total number of potential positive and negative candidates is at most $(\sqrt{p}+a)/a$. Let $(2s-1)$ be the largest odd number $\leqslant \sqrt{p}$. Therefore, we have

$$\begin{aligned}
\mathsf{card}(S) &\leqslant 2 \cdot \sum_{a \in \{1,3,\ldots,2s-1\}} \frac{\sqrt{p} + a}{a} = 2\sqrt{p} \left(1 + \frac{1}{3} + \frac{1}{5} + \cdots + \frac{1}{2s-1} \right) + 2s \\
&\leqslant 2\sqrt{p} \cdot \left(1 + \int_1^s \frac{1}{2t-1} \, \mathrm{d}t \right) + (\sqrt{p} + 1) \\
&= \sqrt{p} \cdot \ln(2s-1) + 3\sqrt{p} + 1 \leqslant \frac{1}{2}\sqrt{p} \cdot \ln p + 3\sqrt{p} + 1 \sim \frac{1}{2}\sqrt{p} \ln p.
\end{aligned}$$

Note that for every (a, b), we also counted $(-a, -b)$ in this set; both belong to the same equivalence class. So, every equivalence class is represented at least twice. Therefore, the number of equivalence classes for which our algorithm outputs "may be insecure" is $\leqslant \mathsf{card}(S)/2$, which is $(1 + \mathrm{o}(1)) \cdot \frac{1}{4}\sqrt{p} \cdot \ln p$ – an exponentially small fraction of the $(p - 2)$ possible equivalence classes.

3.2 Analysis of Our Algorithm: Even $u \cdot v/g^2$

Suppose our algorithm in Figure 2 declared that Shamir's secret-sharing scheme is secure in Step 4. We will provide general results that will imply the security of Shamir's secret-sharing scheme for all pairs of evaluation places in an equivalence class $[\alpha_1, \alpha_2]$ when $u \cdot v/g^2$ is even. We begin with a definition.

Definition 1 (Length of a Finite Field Element). *Consider an element $x \in F$, the prime field of order $p \geqslant 3$. Suppose $x = x' \mod p$, where $x' \in \{-(p-1)/2, \ldots, 0, 1, \ldots, (p-1)/2\} \subseteq \mathbb{Z}$. The* length of the element *is a function $|\cdot|_p \colon F \to \{0, 1, \ldots, (p-1)/2\}$ defined below.*

$$|x|_p := \begin{cases} x', & \text{if } x' \in \{0, 1, \ldots, (p-1)/2\} \\ -x', & \text{if } x' \in \{-(p-1)/2, \ldots, -1\} \end{cases}$$

For example, if $x = (p-1) \mod p$, then $x' = -1 \in \mathbb{Z}$ and $|x|_p = 1$. We prove the following general result.

Theorem 1. *Consider distinct $\alpha_1, \alpha_2 \in F^*$. Suppose there is $(u, v) \in [\alpha_1 : \alpha_2]$ satisfying $|u|_p \cdot |v|_p / g^2$ is even, where $g := \gcd(|u|_p, |v|_p)$. Then, the* $\mathsf{ShamirSS}(2, 2, (\alpha_1, \alpha_2))$ *secret-sharing scheme has ε insecurity against the LSB attack, where*

$$\varepsilon \leqslant \frac{4\left(|u|_p/g + |v|_p/g\right) - 2}{p}.$$

Recall that a "secret-sharing scheme has insecurity ε" against LSB leakage attack implies the following guarantee. The statistical distance between the joint distributions of the leakage when the secret is 0 and the secret is any $s \in F^*$ is $\leqslant \varepsilon$. If $|u|_p/g$ and $|v|_p/g$ are $\ll p$, then Shamir's secret-sharing scheme is secure.

Corollary 4 (Security of Even $|u|_p \cdot |v|_p / g^2$ Case in Our Algorithm). *In our algorithm of Figure 2, even $|u|_p \cdot |v|_p / g^2$ implies that* $\mathsf{ShamirSS}(2, 2, (\alpha_1, \alpha_2))$ *has ε insecurity against the LSB attack, where*

$$\varepsilon \leqslant \frac{8B}{p} - \frac{2}{p} \leqslant \frac{8^{5/4}}{\sqrt{p}} \cdot (1 + o(1)).$$

Recall that $B = \lceil 2^{3/4} \cdot \sqrt{p} \rceil < 2^{3/4}\sqrt{p} + 1$ (see Figure 2).

Proof overview of Theorem 1. In the sequel, we interpret the finite field F as the set of elements $\{0, 1, \ldots, p-1\}$. We introduce a Boolean function $\mathrm{sign}_p \colon F \to \{\pm 1\}$ defined as follows.

$$\mathrm{sign}_p(x) = \begin{cases} +1, & \text{if } x \in \{0, 1, \ldots, (p-1)/2\} \mod p \\ -1, & \text{if } x \in \{-(p-1)/2, \ldots, -1\} \mod p. \end{cases} \tag{1}$$

Define the periodic function $P \colon \mathbb{Z} \to \{\pm 1\}$ as follows.

$$P(X) := \mathrm{sign}_p(X).$$

For $k, \ell \in \{1, 2, \ldots\}$ and $\Delta \in \{0, 1, \ldots, (p-1)\}$, define the function $S_{k,\ell}^{(\Delta)} \colon \mathbb{Z}/p\mathbb{Z} \to \{\pm 1\}$ as follows.

$$S_{k,\ell}^{(\Delta)} := P(k \cdot X) \cdot P(\ell \cdot (X - \Delta)).$$

Above, we are interpreting $\mathbb{Z}/p\mathbb{Z}$ as the set $\{0, 1, \ldots, p-1\}$. Define the summation

$$\Sigma_{k,\ell}^{(\Delta)} := \sum_{t=0}^{p-1} S_{k,\ell}^{(\Delta)}(t).$$

We prove the following connection between leakage resilience and the above-mentioned expression $\Sigma_{\cdot,\cdot}^{(\cdot)}$.

Lemma 1 (Connection: Leakage Resilience and Similarity). *Consider the* $\mathsf{ShamirSS}(2, 2, (\alpha_1, \alpha_2))$ *secret-sharing scheme and the LSB leakage* $\vec{\mathrm{LSB}} \colon F^2 \to \{0,1\}^2$. *For any* $s \in F$,

$$\mathsf{SD}\left(\vec{\mathrm{LSB}}(\mathsf{Share}(0)) \;,\; \vec{\mathrm{LSB}}(\mathsf{Share}(s))\right) = \frac{\left|\Sigma_{\alpha_1,\alpha_2}^{(0)} - \Sigma_{\alpha_1,\alpha_2}^{(\Delta)}\right|}{2p},$$

where $\Delta = (s \cdot 2^{-1}) \cdot (\alpha_1^{-1} - \alpha_2^{-1})$.

Section 6.1 presents the proof of this lemma.

Intuition. Consider the line $Y = \alpha \cdot X$. Our objective is to consider the "sign of this line" $Y = \mathrm{sign}_p(\alpha \cdot X)$, which is identical to the Boolean function $P(\alpha X)$. Note that any "sign of the line" $P(\alpha X)$ is nearly balanced when $\alpha \in F^*$. Now, consider two "sign of line" Boolean functions $P(\alpha_1 X)$ and $P(\alpha_2 X)$. The quantity $\Sigma_{\alpha_1,\alpha_2}^{(0)}$ is the inner product of these two Boolean functions, which measures their similarity. For example, if this quantity is close to 0, then the two Boolean functions are nearly orthogonal.

The $\Sigma_{k,\ell}^{(\Delta)}$ measures the similarity between the "sign of line" $P(\alpha_1 X)$ and "sign of (affine) line" $P(\alpha_2(X - \Delta))$. For $\mathsf{ShamirSS}(2, 2, (\alpha_1, \alpha_2))$ to be secure against LSB attacks, $\Sigma_{k,\ell}^{(\Delta)}$ has to be *independent* of $\Delta \in F$. Otherwise, if there is some $\Delta \in F$ such that $\Sigma_{k,\ell}^{(0)}$ is different from $\Sigma_{k,\ell}^{(\Delta)}$, then there is a LSB distinguishing attack, because $s \mapsto \Delta = (s \cdot 2^{-1}) \cdot (\alpha_1^{-1} - \alpha_2^{-1})$ is an automorphism over F^*. Then, a distinguisher can distinguish the secret shares of 0 from the secret shares of s using the LSB leakage.

Therefore, at this point, our objective is to estimate this summation $\Sigma_{k,\ell}^{(\Delta)}$.

Estimating the Summation. We introduce some periodic square wave functions. Define the periodic function $\varphi \colon \mathbb{R} \to \{\pm 1\}$ as follows.

$$\varphi(x) := \mathrm{sign} \sin(2\pi x).$$

For $k, \ell \in \{1, 2, \ldots\}$ and $\delta \in \mathbb{R}$, define the function $\psi_{k,\ell}^{(\delta)} \colon [0,1] \to \{\pm 1\}$ as follows

$$\psi_{k,\ell}^{(\delta)}(x) := \varphi(kx) \cdot \varphi(\ell(x - \delta)).$$

Define the integral

$$I_{k,\ell}^{(\delta)} := \int_0^1 \psi_{k,\ell}^{(\delta)}(t)\, \mathrm{d}t.$$

The discussion uses only positive k, ℓ. If they have opposite signs, then the following straightforward observation is helpful.

Proposition 2. *For $k, \ell \in \{1, 2, \dots\}$, we have $I^{(\delta)}_{k,-\ell} = -I^{(\delta)}_{k,\ell}$.*

With these definitions, let us return to our objective of estimating $\Sigma^{(\Delta)}_{k,\ell}$ using $I^{(\delta)}_{k,\ell}$. First, note that the function $P(X)$ is identical to $\varphi(x)$, where $x = X/p \in \mathbb{Q}$. This observation extends to the fact that $P(k(X - \Delta))$ is identical to $\varphi(k(x - \delta))$, where $x = X/p$ and $\delta = \Delta/p$. This intimate connection between the two functions allows us to reason about $P(X)$ (whose domain is $\mathbb{Z}$) using $\varphi(x)$ (whose domain is $\mathbb{R}$) as a proxy. Proposition 4 formalizes this "transference of properties" intuition.

Next, the following result helps connect the summation involving $P(\cdot)$ to the corresponding integral involving $\varphi(\cdot)$.

Lemma 2 (Connection: Similarity and Integrals). *For $k, \ell \in \{1, 2, \dots\}$ and $\Delta \in \{0, 1, \dots, p-1\}$, we have*

$$\frac{1}{p} \cdot \Sigma^{(\Delta)}_{k,\ell} \in I^{(\delta)}_{k,\ell} \pm \frac{4(k+\ell) - 2}{p},$$

where $\delta = \Delta/p$.

This lemma is a consequence of the estimation in Corollary 8. The expression $a \in b \pm c$ is a shorthand for $a \in [b - c, b + c]$.

Intuition. We replaced the line over the integers with the sine function – along with a $1/p$ scaling down of the problem. So, we study $\varphi(x) = \operatorname{sign} \sin(2\pi x)$ as a proxy for $P(X) = \operatorname{sign}_p(X)$. In this context, the integral $I^{(\delta)}_{k,\ell}$ takes the role of the summation $\Sigma^{(\Delta)}_{k,\ell}$. We want to claim that the summation $\Sigma^{(\Delta)}_{k,\ell}$ is close to $I^{(\delta)}_{k,\ell} \cdot p$ – accounting for the $1/p$ scaling down. However, estimating a summation using an integral could be inaccurate. For example, (a) the changes in the function's values are large, or (b) the function oscillates frequently. Our functions $\psi^{(\delta)}_{k,\ell}$ are Boolean; hence concern (a) does not arise. Concern (b) poses a significant (and imminent) threat. Therefore, the lemma above states that the error-bound in the estimation is proportional to the number of oscillations in the function $\psi^{(\delta)}_{k,\ell}$. Lemma 11 summarizes the number of oscillations in the $\psi^{(\delta)}_{k,\ell}$ function.

Estimating the Integral. We have a family of square-wave functions $\varphi(k(x - \delta))$, and our objective is to study the integral $I^{(\delta)}_{k,\ell}$. To this end, we use the following results.

Lemma 3 (Imported from [31, 12]). *Fix $k, \ell \in \{1, 2, \dots\}$. If k and ℓ have different highest powers of 2, then $I^{(0)}_{k,\ell} = 0$.*

For example, the highest power of 2 in 6 is 2, and the highest power of 2 in 20 is 4. So, $I^{(0)}_{6,20} = 0$. However, we also need to investigate $I^{(\delta)}_{k,\ell}$ for non-zero values of δ. This result is inadequate for our research. We extend this result as follows.

Lemma 4. *Fix $k, \ell \in \{1, 2, \dots\}$. If k and ℓ have different highest powers of 2, then $I^{(\delta)}_{k,\ell} = 0$, for all $\delta \in \mathbb{R}$.*

This lemma is a consequence of Lemma 7 and Lemma 8. In particular, we have the following corollary.

Corollary 5. *Fix $k, \ell \in \{1, 2, \dots\}$. Let $g = \gcd(k, \ell)$. If $k \cdot \ell / g^2$ is even then $I_{k,\ell}^{(\delta)} = 0$, for all $\delta \in \mathbb{R}$.*

Putting things together. Consider $(u, v) \in [\alpha_1 : \alpha_2]$ such that (a) $|u|_p \leqslant B$, (b) $|v|_p \leqslant B$, and (c) $|u|_p \cdot |v|_p / g^2$ is even, where $g = \gcd(u, v)$. The properties of $\mathsf{ShamirSS}(2, 2, (\alpha_1, \alpha_2))$ are identical to the properties of $\mathsf{ShamirSS}(2, 2, (u, v))$ (due to Proposition 1). Lemma 1 states that the insecurity ε satisfies

$$\varepsilon \leqslant \max_{\Delta \in F} \frac{\left| \Sigma_{u,v}^{(0)} - \Sigma_{u,v}^{(\Delta)} \right|}{2p}.$$

Lemma 2 states that the integrals can replace the similarities. The upper-bound updates to

$$\varepsilon \leqslant \max_{\Delta \in F} \quad \frac{1}{2} \cdot \left| I_{u,v}^{(0)} - I_{u,v}^{(\Delta/p)} \right| + \frac{4(|k|_p + |\ell|_p) - 2}{p}.$$

Corollary 5 states that, in this case, $I_{k,\ell}^{(\delta)} = 0$ for all $\delta \in \mathbb{R}$. So, we get

$$\varepsilon \leqslant \max_{\Delta \in F} \frac{4(|k|_p + |\ell|_p) - 2}{p} \leqslant \frac{8B}{p} - \frac{2}{p}.$$

This derivation completes the proof of Theorem 1 and Corollary 4.

Remark 7. This proof highlights the need to change the basis from (α_1, α_2) to (u, v) using the LLL [17] algorithm. This new basis has the property that $|u|_p$ and $|v|_p$ are upper-bounded by $B \ll p$.

3.3 Analysis of Our Algorithm: Odd large $u \cdot v / g^2$

Suppose our algorithm in Figure 2 says $\mathsf{ShamirSS}(2, 2, (\alpha_1, \alpha_2))$ is secure in Step 5. The following result determines its resilience to the LSB attack.

Theorem 2. *Consider distinct $\alpha_1, \alpha_2 \in F^*$. Suppose there is $(u, v) \in [\alpha_1 : \alpha_2]$ satisfying $|u|_p |v|_p / g^2$ is odd, where $g := \gcd(|u|_p, |v|_p)$. Then, the $\mathsf{ShamirSS}(2, 2, (\alpha_1, \alpha_2))$ secret-sharing scheme has ε insecurity against the LSB attack, where*

$$\varepsilon \leqslant \frac{g^2}{|u|_p \cdot |v|_p} + \frac{4\left(|u|_p / g + |v|_p / g\right) - 2}{p}$$

If (a) $|u|_p \cdot |v|_p / g^2$ is $\gg 1$ and (b) $|u|_p$ and $|v|_p$ are $\ll p$, then Shamir's secret-sharing scheme will be secure.

Corollary 6 (Security of $|u|_p \cdot |v|_p/g^2$ Case in Our Algorithm). *In our algorithm of Figure 2, odd $|u|_p|v|_p/g^2 \geqslant \sqrt{p}$ implies that* $\mathsf{ShamirSS}(2, 2, (\alpha_1, \alpha_2))$ *has ε insecurity against the LSB attack, where*

$$\varepsilon \leqslant \frac{1}{\sqrt{p}} + \frac{8B}{p} - \frac{2}{p} \lesssim \frac{8^{5/4}+1}{\sqrt{p}}.$$

We need estimations for relevant $I^{(\delta)}_{u,v}$ to begin this proof.

Lemma 5 (Imported from [31, 12]). *Fix $k, \ell \in \{1, 2, \dots\}$. If k and ℓ have identical highest powers of 2, then*

$$I^{(0)}_{k,\ell} = \frac{\gcd(k,\ell)^2}{k \cdot \ell}.$$

As before, this result is inadequate for our setting. We extend this result to all $\delta \in \mathbb{R}$.

Lemma 6. *Fix $k, \ell \in \{1, 2, \dots\}$. If k and ℓ have identical highest powers of 2, then*

$$I^{(\delta)}_{k,\ell} = \frac{\gcd(k,\ell)^2}{k \cdot \ell} \cdot \cos(2\pi\ell \cdot \delta).$$

Furthermore,

1. $I^{(\delta)}_{k,\ell} = \frac{\gcd(k,\ell)^2}{k\cdot\ell}$, *when* $\delta \in \frac{1}{\ell} \cdot \mathbb{Z}$, *and*
2. *For any $p \geqslant 3$, there exists* $\delta \in \frac{1}{p} \cdot F^* \subseteq \frac{1}{p} \cdot \mathbb{Z}$ *such that* $I^{(\delta)}_{k,\ell} = -\frac{\gcd(k,\ell)^2}{k\cdot\ell} \cos(\pi/p)$.

This lemma is a consequence of Lemma 7 and Lemma 9. Part (a) of the "Furthermore, ..." follows from the periodicity of the $\cos(\cdot)$ function. Part (b) of the "Furthermore, ..." follows from Lemma 10. The "Furthermore, ..." part of this lemma shall be used later in Section 3.4; it is not used in the proof of Theorem 2. In particular, the following corollary suffices for the proof of Theorem 2.

Corollary 7. *Fix $k, \ell \in \{1, 2, \dots\}$. Let $g = \gcd(k, \ell)$. If $k \cdot \ell/g^2$ is odd then $I^{(\delta)}_{k,\ell} \in \pm\frac{g^2}{k\cdot\ell}$, for all $\delta \in \mathbb{R}$.*

To prove Theorem 2, we proceed similarly to the proof of Theorem 1. The insecurity ε has the upper bound

$$\varepsilon \leqslant \max_{\Delta \in F} \quad \frac{1}{2} \cdot \left| I^{(0)}_{u,v} - I^{(\Delta/p)}_{u,v} \right| + \frac{4(|k|_p + |\ell|_p) - 2}{p}.$$

By Corollary 7, we have $\left| I^{(0)}_{u,v} - I^{(\Delta/p)}_{u,v} \right| \leqslant \frac{2g^2}{|u|_p \cdot |v|_p}$; thus completing the proof of Theorem 2 and Corollary 6.

3.4 New Attacks on Shamir: Odd small $u \cdot v/g^2$

Are there imminent threats to Shamir's secret-sharing scheme when our algorithm Figure 2 declares "May be Insecure"? We prove the following result.

Theorem 3. *Consider distinct $\alpha_1, \alpha_2 \in F^*$. Suppose there is $(u, v) \in [\alpha_1 : \alpha_2]$ such that $|u|_p \cdot |v|_p / g^2$ is odd, where $g = \gcd(|u|_p, |v|_p)$. Then, there is $s \in F^*$, such that an adversary can distinguish the secret s from the secret 0 with advantage ε, where*

$$\varepsilon \geqslant \frac{(1 + \cos(\pi/p)) \cdot g^2}{2 \cdot |u|_p \cdot |v|_p} - \frac{4\left(|u|_p/g + |v|_p/g\right) - 2}{p}.$$

For example, suppose that u and v are relatively prime and odd constants. Say, $u = 1$ and $v = 3$. Then, $\varepsilon \gtrsim \frac{1}{2|uv|_p}$, a constant. This yields a new attacks on the Shamir secret-sharing scheme using the LSB attack.

The proof of Theorem 3 follows from Lemma 6. This lemma states that $I^{(0)}_{k,\ell} = \frac{g^2}{k\ell}$, where $k = |u|_p$, $\ell = |v|_p$, $g = \gcd(u, v)$, and $k\ell/g^2$ is odd. Additionally, it shows the existence of $\delta \in F^*/p \subseteq \mathbb{Q}$ such that $I^{(\delta)}_{k,\ell} = -\frac{g^2 \cos(\pi/p)}{k\ell}$. Recall that $\Delta = (s \cdot 2^{-1}) \cdot (\alpha_1^{-1} - \alpha_2^{-1})$, where $\Delta = p\delta$. So, we can recover the corresponding $s \in F^*$. The statistical distance between the LSB leakage is at least

$$\frac{(1 + \cos(\pi/p) \cdot g^2}{2 \cdot |u|_p \cdot |v|_p} - \frac{4\left(|u|_p/g + |v|_p/g\right) - 2}{p}.$$

4 Properties of a Family of Square Waves

To begin, we formalize the orthogonal properties of the sine and cosine functions.

Proposition 3 (Orthogonality of Sine/Cosine Waves [15, Page 38]). *For $k, \ell \in \{1, 2, \dots\}$*

$$\int_0^1 \sin(2k\pi t) \cdot \sin(2\ell\pi t)\, \mathrm{d}t = \begin{cases} 0, & \text{if } k \neq \ell \\ \frac{1}{2}, & \text{if } k = \ell. \end{cases}$$

$$\int_0^1 \sin(2k\pi t) \cdot \cos(2\ell\pi t)\, \mathrm{d}t = 0.$$

We shall study the following periodic *square wave* [31, 12, 11] $\varphi\colon \mathbb{R} \to \{\pm 1\}$.

$$\varphi(x) := \operatorname{sign} \sin(2\pi x).$$

[12] uses (basic) Fourier analysis and Proposition 3 to determine the Fourier expansion of $\varphi(x)$.

$$\varphi(x) = \sum_{\text{odd } n > 0} \frac{4}{\pi n} \cdot \sin(2n\pi x). \tag{2}$$

For $k, \ell \in \{1, 2, \dots\}$ and $\delta \in \mathbb{R}$, we shall study the function $\psi_{k,\ell}^{(\delta)} \colon [0,1] \to \{\pm 1\}$ defined below

$$\psi_{k,\ell}^{(\delta)} := \varphi(kx) \cdot \varphi(\ell(x - \delta)),$$

and the integral

$$I_{k,\ell}^{(\delta)} := \int_0^1 \psi_{k,\ell}^{(\delta)}(t)\, \mathrm{d}t.$$

We prove the following lemma for standardization.

Lemma 7. *For $k, \ell \in \{1, 2, \dots\}$ and $\delta \in \mathbb{R}$, the following identity holds*

$$I_{k,\ell}^{(\delta)} = I_{k/g,\ell/g}^{(\delta)},$$

where $g = \gcd(k, \ell)$.

Proof. Observe that $\psi_{k,\ell}^{(\delta)}(x) = \psi_{k,\ell}^{(\delta)}(x + 1/d)$, for any d that divides both k and ℓ. Let $g = \gcd(k, \ell)$. So, from our observation, we conclude that $\psi_{k,\ell}^{(\delta)}$ has period $1/g$. Therefore, we conclude that

$$I_{k,\ell}^{(\delta)} = g \cdot \int_0^{1/g} \psi_{k,\ell}^{(\delta)}(t)\, \mathrm{d}t.$$

Next, note that $\psi_{k,\ell}^{(\delta)}(x) = \psi_{k/d,\ell/d}^{(\delta)}(d \cdot x)$, for any d that divides both k and ℓ. Therefore, we get

$$I_{k,\ell}^{(\delta)} = g \cdot \int_0^{1/g} \psi_{k/g,\ell/g}^{(\delta)}(gt)\, \mathrm{d}t.$$

By substituting the variable $r = gt$, we get

$$I_{k,\ell}^{(\delta)} = g \cdot \int_0^1 \psi_{k/g,\ell/g}^{(\delta)}(r) \cdot \frac{1}{g} \cdot \mathrm{d}r = I_{k/g,\ell/g}^{(\delta)}.$$

□

Henceforth, without loss of generality, assume that k and ℓ are relatively prime.

Supporting Material B contains results already known in the literature, which studied $I_{k,\ell}^{(0)}$ [31, 12]. The following section presents the results we proved. In particular, motivated by our application scenario, we study $I_{k,\ell}^{(\delta)}$, for all $\delta \in \mathbb{R}$.

4.1 Properties of $I_{k,\ell}^{(\delta)}$

In this section we estimate $I_{k,\ell}^{(\delta)}$, for general $\delta \in \mathbb{R}$. Results in this section were not known earlier (as far as authors' knowledge). We show that for relatively prime $k, \ell \in \{1, 2, \dots\}$, for all $\delta \in \mathbb{R}$

$$I_{k,\ell}^{(\delta)} = \begin{cases} 0 & \text{if } k \cdot \ell \text{ is even} \\ \frac{\cos(2\ell\pi \cdot \delta)}{k\ell} & \text{if } k \cdot \ell \text{ is odd} \end{cases}.$$

Lemma 8. *For relatively prime $k, \ell \in \{1, 2, \dots\}$ such that $k \cdot \ell$ is even, $I_{k,\ell}^{(\delta)} = 0$, for all $\delta \in \mathbb{R}$.*

Proof. Suppose k is even, and ℓ is odd. In this case, for any odd $m, n > 0$, observe that

$$\begin{aligned}
&\sin\left(2n\pi \cdot k\left(\frac{1}{2} + t\right)\right) \cdot \sin\left(2m\pi \cdot \ell\left(\frac{1}{2} + t - \delta\right)\right) \\
&= \sin\left(\begin{matrix} 2n\pi \cdot kt \\ + \\ \underbrace{nk}_{\text{even}} \cdot \pi \end{matrix}\right) \cdot \sin\left(\begin{matrix} 2m\pi \cdot \ell(t-\delta) \\ + \\ \underbrace{m\ell}_{\text{odd}} \cdot \pi \end{matrix}\right) \\
&= \sin(2n\pi \cdot kt) \cdot (\ -\sin(2m\pi \cdot \ell(t-\delta))\ )
\end{aligned}$$

Therefore,

$$\begin{aligned}
\int_0^1 \sin(2n\pi \cdot kt) \cdot \sin(2m\pi \cdot \ell(t-\delta))\,\mathrm{d}t &= \int_0^{1/2} \sin(2n\pi \cdot kt) \cdot \sin(2m\pi \cdot \ell(t-\delta))\,\mathrm{d}t \\
&\quad + \int_{1/2}^1 \sin(2n\pi \cdot kt) \cdot \sin(2m\pi \cdot \ell(t-\delta))\,\mathrm{d}t \\
&= \int_0^{1/2} \sin(2n\pi \cdot kt) \cdot \sin(2m\pi \cdot \ell(t-\delta))\,\mathrm{d}t \\
&\quad - \int_0^{1/2} \sin(2n\pi \cdot kt) \cdot \sin(2m\pi \cdot \ell(t-\delta))\,\mathrm{d}t \\
&= 0. \qquad (3)
\end{aligned}$$

Now, we can prove the lemma.

$$\begin{aligned}
I_{k,\ell}^{(\delta)} &= \int_0^1 \varphi(kt) \cdot \varphi(\ell(t-\delta))\,\mathrm{d}t \\
&= \frac{16}{\pi^2} \sum_{\text{odd } n>0} \sum_{\text{odd } m>0} \frac{1}{mn} \int_0^1 \sin(2n\pi \cdot kt) \cdot \sin(2m\pi \cdot \ell(t-\delta))\,\mathrm{d}t \\
&\qquad \text{(By Equation 2)} \\
&= 0 \qquad \text{(By Equation 3)}
\end{aligned}$$

Finally, if k is odd and ℓ is even, then

$$\begin{aligned}
&\sin\left(2n\pi \cdot k\left(\frac{1}{2} + t\right)\right) \cdot \sin\left(2m\pi \cdot \ell\left(\frac{1}{2} + t - \delta\right)\right) \\
&= \sin\left(\begin{matrix} 2n\pi \cdot kt \\ + \\ \underbrace{nk}_{\text{odd}} \cdot \pi \end{matrix}\right) \cdot \sin\left(\begin{matrix} 2m\pi \cdot \ell(t-\delta) \\ + \\ \underbrace{m\ell}_{\text{even}} \cdot \pi \end{matrix}\right) \\
&= (\ -\sin(2n\pi \cdot kt)\ ) \cdot \sin(2m\pi \cdot \ell(t-\delta))
\end{aligned}$$

Again, Equation 3 holds, and the proof of this case goes through. □

Lemma 9. *For relatively prime $k, \ell \in \{1, 2, \dots\}$ such that $k \cdot \ell$ is odd,*

$$I_{k,\ell}^{(\delta)} = \frac{\cos(2\ell\pi \cdot \delta)}{k\ell},$$

for all $\delta \in \mathbb{R}$.

Therefore, $I_{k,\ell}^{(\delta)}$ achieves its maximum at $\delta \in \frac{1}{\ell} \cdot \mathbb{Z}$, and the minimum at $\delta \in \frac{1}{2\ell} + \frac{1}{\ell} \cdot \mathbb{Z}$.

Proof. We begin with a generalization of Proposition 3.

Claim.

$$\int_0^1 \sin(2k\pi t) \cdot \sin(2\ell\pi(t-\delta))\,\mathrm{d}t = \begin{cases} 0, & \text{if } k \neq \ell \\ \frac{1}{2}\cos(2\ell\pi\delta), & \text{if } k = \ell. \end{cases}$$

Proof (of the claim above).

$$\begin{aligned} \int_0^1 \sin(2k\pi t) \cdot \sin(2\ell\pi(t-\delta))\,\mathrm{d}t &= \int_0^1 \sin(2k\pi t) \cdot \sin(2\ell\pi t)\cos(2\ell\pi\delta)\,\mathrm{d}t \\ &\quad - \int_0^1 \sin(2k\pi t) \cdot \cos(2\ell\pi t)\sin(2\ell\pi\delta)\,\mathrm{d}t \\ &= \cos(2\ell\pi\delta)\int_0^1 \sin(2k\pi t) \cdot \sin(2\ell\pi t)\,\mathrm{d}t, \end{aligned}$$

because, for all $k, \ell \in \{1, 2, \dots\}$, Proposition 3 implies

$$\int_0^1 \sin(2k\pi t) \cdot \cos(2\ell\pi t)\,\mathrm{d}t = 0.$$

The proof of our claim follows from Proposition 3 because $\int_0^1 \sin(2k\pi t)\cdot\sin(2\ell\pi t)\,\mathrm{d}t = 1/2$ if (and only if) $k = \ell$; otherwise, it is 0. □

Next, we simplify the expression for $I_{k,\ell}^{(\delta)}$.

$$\begin{aligned} I_{k,\ell}^{(\delta)} &= \int_0^1 \varphi(kt) \cdot \varphi(\ell(t-\delta))\,\mathrm{d}t \\ &= \frac{16}{\pi^2} \sum_{\text{odd } n>0} \sum_{\text{odd } m>0} \frac{1}{mn} \int_0^1 \sin(2n\pi \cdot kt)\sin(2m\pi \cdot \ell(t-\delta))\,\mathrm{d}t \end{aligned}$$

(By Equation 2)

In light of the claim above, the integral in the RHS survives if and only if $nk = m\ell$. Since, $\gcd(k, \ell) = 1$, note that $nk = m\ell$ if and only if

$$(n, m) \in J := \Big\{(\ell, k), (3\ell, 3k), (5\ell, 5k), \dots\Big\}.$$

With this observation and Proposition 3, we get

$$\begin{aligned}
I_{k,\ell}^{(\delta)} &= \frac{16}{\pi^2} \sum_{(n,m)\in J} \frac{\cos(2\ell\pi\delta)}{mn} \int_0^1 \sin(2n\pi \cdot kt) \sin(2m\pi \cdot \ell t)\, \mathrm{d}t \\
&= \frac{16}{\pi^2} \sum_{\text{odd } a>0} \frac{\cos(2\ell\pi\delta)}{k\ell \cdot a^2} \int_0^1 \sin(2k\ell a\pi \cdot t) \sin(2k\ell a\pi \cdot t)\, \mathrm{d}t \\
&= \frac{16}{\pi^2} \cdot \frac{1}{k\ell} \sum_{\text{odd } a>0} \frac{1}{a^2} \cdot \frac{\cos(2\ell\pi\delta)}{2} && \text{(By Proposition 3)} \\
&= \frac{\cos(2\ell\pi\delta)}{k\ell} \cdot \frac{\cancel{8}}{\cancel{\pi^2}} \cdot \frac{\cancel{\pi^2}}{\cancel{8}} = \frac{\cos(2\ell\pi\delta)}{k\ell} && \left(\text{Because } \sum_{\text{odd } a>0} \tfrac{1}{a^2} = \tfrac{3}{4} \cdot \zeta(2) = \tfrac{\pi^2}{8}\right)
\end{aligned}$$

This concludes the proof of our lemma. □

4.2 How low can we go?

Fix a prime $p \geqslant 3$ and relatively prime odd $k, \ell \in \{1, 2, \ldots, p-1\}$. Consider the minimization problem

$$\min_{\delta' \in \frac{1}{p}\cdot\mathbb{Z}} I_{k,\ell}^{(\delta')}.$$

Note that $\delta \in \frac{1}{2\ell} + \frac{1}{\ell} \cdot \mathbb{Z}$ ensures that $I_{k,\ell}^{(\delta)} = -\frac{1}{k\ell}$, the global minimum when $\delta \in \mathbb{R}$. However $\left(\frac{1}{2\ell} + \frac{1}{\ell} \cdot \mathbb{Z}\right) \cap \frac{1}{p} \cdot \mathbb{Z} = \emptyset$, because 2ℓ and p are relatively prime in our context. So, how small can this quantity become when δ is restricted to $\frac{1}{p} \cdot \mathbb{Z}$?

Our strategy is to find an element in $\frac{1}{p} \cdot \mathbb{Z}$ that is closest to the set $\frac{1}{2\ell} + \frac{1}{\ell} \cdot \mathbb{Z}$. Since p and 2ℓ are relatively prime, we can find integers $a, b \in \mathbb{Z}^*$ such that

$$a \cdot p - b \cdot (2\ell) = 1.$$

Note that a must be odd; otherwise, the LHS is even, which is impossible. So, assume that $a = 2a' + 1$. Therefore, we conclude that there are integers $a' \in \mathbb{Z}$ and $b \in \mathbb{Z}^*$ satisfying

$$\frac{2a'+1}{2\ell} - \frac{b}{p} = \frac{1}{2\ell p}.$$

Rearranging, we get

$$\frac{b}{p} = \frac{1}{2\ell} + \frac{a'}{\ell} - \frac{1}{2\ell p}. \tag{4}$$

Now, consider $\delta' = b/p \in \mathbb{Q}$.

$$\begin{aligned}
I_{k,\ell}^{(\delta')} &= \frac{\cos(2\ell\pi \cdot \delta')}{k\ell} && \text{(By Lemma 9)} \\
&= \frac{\cos\left(\pi + 2a'\pi - \pi/p\right)}{k\ell} && \text{(By Equation 4)}
\end{aligned}$$

$$= -\frac{\cos(\pi/p)}{k\ell}.$$

In fact, this value is the global minimum. From this observation, we get the following result.

Lemma 10. *Fix a prime $p \geqslant 3$ and relatively prime odd $k, \ell \in \{1, 2, \ldots, p-1\}$.*

$$\min_{\delta \in \left\{\frac{1}{p}, \frac{2}{p}, \ldots, \frac{p-1}{p}\right\}} I_{k,\ell}^{(\delta)} = -\frac{\cos(\pi/p)}{k\ell} \leqslant -\frac{1}{2k\ell}.$$

5 Estimating Sums involving Signs of Lines

Consider a prime $p \geqslant 3$. In this section, we shall use the following $\mathrm{sign}_p \colon \mathbb{Z} \to \{\pm 1\}$ function

$$\mathrm{sign}_p(x) := \begin{cases} +1, & x \in \{0, 1, \ldots, (p-1)/2\} \mod p \\ -1, & x \in \{-(p-1)/2, \ldots, -2, -1\} \mod p. \end{cases}$$

Consider the periodic Boolean function $P \colon \mathbb{Z} \to \{\pm 1\}$

$$P(X) := \mathrm{sign}_p(X).$$

For integers $k, \ell \in \{1, 2, \ldots\}$ and $\Delta \in \mathbb{Z}$, we shall study the function

$$S_{k,\ell}^{(\Delta)}(X) := P(k \cdot X) \cdot P(\ell \cdot (X - \Delta)),$$

and the sum

$$\Sigma_{k,\ell}^{(\Delta)} := \sum_{X \in \{0,1,\ldots,p-1\}} S_{k,\ell}^{(\Delta)}(X).$$

Our objective is to estimate $\Sigma_{k,\ell}^{(\Delta)}$ using $I_{k,\ell}^{(\delta)}$, where $\delta = \Delta/p \in \mathbb{Q}$. The primary observation that facilitates this transference is the following.

Proposition 4 (Transference Property). *For all $k \in \{1, 2, \ldots\}$, $X \in \mathbb{Z}$, $\Delta \in \mathbb{Z}$, $x = X/p \in \mathbb{Q}$, and $\delta = \Delta/p \in \mathbb{Q}$.*

$$P(k(X - \Delta)) = \varphi(k(x - \delta)).$$

5.1 Estimation Error

Definition 2 (Number of Oscillations). *A Boolean function $f \colon [0, 1] \to \{\pm 1\}$ oscillates at $x \in [0, 1)$ if $f(x) \neq \lim_{h \to 0^+} f(x + h)$. The* number of oscillations *is the cardinality of the following set.*

$$\left\{ x \colon f(x) \neq \lim_{h \to 0^+} f(x + h) \right\}.$$

Since our functions are periodic with period 1, counting the number of oscillations in the interval $[0,1)$ in our context suffices. By straightforward counting, one concludes the following.

Lemma 11 (Counting Number of Oscillations). *For any $k, \ell \in \{1,2,\dots\}$*

1. *$\varphi(k(x-\delta))$ oscillates $(2k-1)$ times, if $\delta \in \frac{1}{2k}\cdot\mathbb{Z}$*
2. *$\varphi(k(x-\delta))$ oscillates $2k$ times, if $\delta \notin \frac{1}{2k}\cdot\mathbb{Z}$*
3. *$\psi^{(\delta)}_{k,\ell}$ oscillates $2(k+\ell)-2$ times, if $\delta \in \frac{1}{2k}\cdot\mathbb{Z} \cap \frac{1}{2\ell}\cdot\mathbb{Z}$*
4. *$\psi^{(\delta)}_{k,\ell}$ oscillates $2(k+\ell)-1$ times, if $\delta \notin \frac{1}{2k}\cdot\mathbb{Z} \cap \frac{1}{2\ell}\cdot\mathbb{Z}$*

We prove a general result connecting Boolean functions' sum and the integral.

Lemma 12 (Sum and Integral Connection). *Fix an integer $n \in \{1,2,\dots\}$. Let $f\colon [0,1] \to \{\pm 1\}$ be a Boolean function that oscillates T times in the range $[0,1]$. Then,*

$$\frac{1}{n}\cdot \sum_{t\in\left\{\frac{0}{n},\frac{1}{n},\dots,\frac{n-1}{n}\right\}} f(t) \in \int_0^1 f(t)\,\mathrm{d}t \pm \frac{2T}{n}.$$

Proof. Consider an interval $[r, r+1/n)$, for $r \in \{0/n, 1/n, \dots, (n-1)/n\}$. If f does not oscillate in this interval, then f is constant in the interval, and we conclude

$$\frac{1}{n}\cdot f(t) = \int_r^{r+1/n} f(t)\,\mathrm{d}t.$$

If f oscillates at some point in this interval, then (due to f being Boolean) we conclude

$$\frac{1}{n}\cdot f(t) \in [-1/n, 1/n] \subseteq \int_r^{r+1/n} f(t)\,\mathrm{d}t \pm \frac{2}{n}.$$

Adding over all $r \in \{0/n, 1/n, \dots, (n-1)/n\}$, we get the lemma. □

As a consequence of Proposition 4, Lemma 11, and Lemma 12, we conclude with the following corollary.

Corollary 8 (Estimation of our Sum). *For prime $p \geqslant 3$, $k, \ell \in \{1,2,\dots\}$, $\Delta \in \mathbb{Z}$, and $\delta = \Delta/p \in \mathbb{Q}$*

$$\frac{1}{p}\cdot \Sigma^{(\Delta)}_{k,\ell} \in \begin{cases} I^{(\delta)}_{k,\ell} \pm \frac{4(k+\ell)-4}{p} & \text{if } \delta \in \frac{1}{2k}\cdot\mathbb{Z} \cap \frac{1}{2\ell}\cdot\mathbb{Z} \\ I^{(\delta)}_{k,\ell} \pm \frac{4(k+\ell)-2}{p} & \text{if } \delta \notin \frac{1}{2k}\cdot\mathbb{Z} \cap \frac{1}{2\ell}\cdot\mathbb{Z} \end{cases}$$

6 Characterizing Leakage-Resilience

6.1 Connecting Leakage Resilience to Summation: Proof of Lemma 1

Consider $\mathsf{ShamirSS}(n=2, k=2, (\alpha_1, \alpha_2))$ over a prime field F of order p. Let $\vec{\mathrm{LSB}}\colon F^2 \to \{0,1\}$ be the leakage function that leaks the LSB of both the secret shares. Let $\mathsf{Share}(s)$ represent the joint distribution over the secret shares

conditioned on the secret being $s \in F$. We aim to study the statistical distance between the leakage distributions when the secret is 0 and when the secret is $s \in F^*$.

$$\mathsf{SD}\left(\vec{\mathrm{LSB}}(\mathsf{Share}(0))\ ,\ \vec{\mathrm{LSB}}(\mathsf{Share}(s))\right).$$

Define the set of all "positive elements" of F as $F^+ := \{0, 1, \ldots, (p-1)/2\} \subseteq F$, and the set of all "even elements" of F as $E := \{0, 2, 4, \ldots, (p-1)\} \subseteq F$. Observe that $\mathrm{sign}_p(X) = +1$ if and only if $X \in F^+$. Moreover, $E = F^+ \cdot 2$ and $F^+ = E \cdot (2^{-1})$.

Consider the following manipulation.

$$\begin{aligned}
&2\mathsf{SD}\left(\vec{\mathrm{LSB}}(\mathsf{Share}(0))\ ,\ \vec{\mathrm{LSB}}(\mathsf{Share}(s))\right)\\
&\quad= \sum_{\vec{\ell}\in\{0,1\}^2} \left|\Pr\left[\vec{\mathrm{LSB}}(\mathsf{Share}(0)) = \vec{\ell}\right] - \Pr\left[\vec{\mathrm{LSB}}(\mathsf{Share}(s)) = \vec{\ell}\right]\right|\\
&\quad= \sum_{\vec{\ell}\in\{0,1\}^2} \Bigg|\mathop{\mathbb{E}}_{x}\left[\mathbb{1}_{\mathrm{LSB}^{-1}(\ell_1)}(\alpha_1 x)\cdot\mathbb{1}_{\mathrm{LSB}^{-1}(\ell_2)}(\alpha_2 x)\right]\\
&\qquad\qquad - \mathop{\mathbb{E}}_{x}\left[\mathbb{1}_{\mathrm{LSB}^{-1}(\ell_1)}(\alpha_1 x + s)\cdot\mathbb{1}_{\mathrm{LSB}^{-1}(\ell_2)}(\alpha_2 x + s)\right]\Bigg|\\
&\quad= \sum_{\vec{\ell}\in\{0,1\}^2} \Bigg|\mathop{\mathbb{E}}_{x}\left[\mathbb{1}_{\mathrm{LSB}^{-1}(0)}(\alpha_1 x)\cdot\mathbb{1}_{\mathrm{LSB}^{-1}(0)}(\alpha_2 x)\right]\\
&\qquad\qquad - \mathop{\mathbb{E}}_{x}\left[\mathbb{1}_{\mathrm{LSB}^{-1}(0)}(\alpha_1 x + s)\cdot\mathbb{1}_{\mathrm{LSB}^{-1}(0)}(\alpha_2 x + s)\right]\Bigg|\\
&\qquad\qquad\qquad\qquad \text{(Using the fact that } \mathbb{1}_{\mathrm{LSB}^{-1}(1)} = 1 - \mathbb{1}_{\mathrm{LSB}^{-1}(0)})\\
&\quad= 4\cdot\left|\mathop{\mathbb{E}}_{x}\left[\mathbb{1}_E(\alpha_1 x)\cdot\mathbb{1}_E(\alpha_2 x)\right] - \mathop{\mathbb{E}}_{x}\left[\mathbb{1}_E(\alpha_1 x + s)\cdot\mathbb{1}_E(\alpha_2 x + s)\right]\right|\\
&\quad= 4\cdot\left|\mathop{\mathbb{E}}_{x}\left[\mathbb{1}_{E\alpha_1^{-1}}(x)\cdot\mathbb{1}_{E\alpha_2^{-1}}(x)\right] - \mathop{\mathbb{E}}_{x}\left[\mathbb{1}_{(E-s)\alpha_1^{-1}}(x)\cdot\mathbb{1}_{(E-s)\alpha_2^{-1}}(x)\right]\right|\\
&\quad= \frac{4}{p}\cdot\left|\mathsf{card}\left(E\alpha_1^{-1}\cap E\alpha_2^{-1}\right) - \mathsf{card}\left((E-s)\alpha_1^{-1}\cap(E-s)\alpha_2^{-1}\right)\right|\\
&\quad= \frac{4}{p}\cdot\left|\mathsf{card}\left(F^+\alpha_1^{-1}\cap F^+\alpha_2^{-1}\right) - \mathsf{card}\left(F^+\alpha_1^{-1}\cap\left(F^+\alpha_2^{-1}+\Delta\right)\right)\right|, \qquad (5)
\end{aligned}$$

where $\Delta = (s\cdot 2^{-1})\cdot(\alpha_1^{-1} - \alpha_2^{-1})$. Note that the mapping $s \mapsto \Delta$ is an automorphism over F (that preserves the 0).

Let us take a detour and understand the set $F^+\alpha_1^{-1}\cap\left(F^+\alpha_2^{-1}+\Delta\right)$. Let X belong to this intersection. Then, $\alpha_1 X$ and $\alpha_2(X-\Delta)$ are both positive. That is, the set of $X \in F$ such that "$\mathrm{sign}_p(\alpha_1 X) = +1$ and $\mathrm{sign}_p(\alpha_2(X-\Delta)) = +1$" is identical to the set $F^+\alpha_1^{-1}\cap\left(F^+\alpha_2^{-1}+\Delta\right)$.

Let $\overline{F^+} := F \setminus F^+$. Define $A_{+1} := F^+$ and $A_{-1} := \overline{F^+}$. More generally, we conclude that, for $\sigma, \sigma' \in \{\pm 1\}$, the set

$$X_{\sigma,\sigma'} := \left\{X \in F\colon\ \mathrm{sign}_p(\alpha_1 X) = \sigma, \mathrm{sign}_p(\alpha_2(X-\Delta)) = \sigma'\right\}$$

is identical to the set $A_\sigma \alpha_1^{-1} \cap \left(A_{\sigma'} \alpha_2^{-1} + \Delta\right)$. Let us express the cardinality of the sets $X_{\sigma,\sigma'}$ in terms of the cardinality of the set $X_{+1,+1}$.

Note that $\mathsf{card}(X_{+1,+1}) + \mathsf{card}(X_{+1,-1}) = \mathsf{card}(F^+) = (p+1)/2$, because $X \mapsto \mathrm{sign}_p(\alpha_1 X)$ is an automorphism over F. Consequently, there are $\mathsf{card}(F^+)$ values of X such that $\alpha_1 X \in F^+$. So,

$$\mathsf{card}(X_{+1,-1}) = (p+1)/2 - \mathsf{card}(X_{+1,+1})\,. \tag{6}$$

Likewise, $\mathsf{card}(X_{-1,-1}) + \mathsf{card}(X_{+1,-1}) = \mathsf{card}\left(\overline{F^+}\right) = (p-1)/2$. So,

$$\mathsf{card}(X_{-1,-1}) = -1 + \mathsf{card}(X_{+1,+1})\,. \tag{7}$$

And, finally $\mathsf{card}(X_{-1,+1}) + \mathsf{card}(X_{-1,-1}) = \mathsf{card}\left(\overline{F^+}\right) = (p-1)/2$. So,

$$\mathsf{card}(X_{-1,+1}) = (p+1)/2 - \mathsf{card}(X_{+1,+1})\,. \tag{8}$$

Next, we study the summation

$$\begin{aligned}
\Sigma^{(\Delta)}_{\alpha_1,\alpha_2} &= \sum_{X \in F} \mathrm{sign}_p(\alpha_1 X) \cdot \mathrm{sign}_p(\alpha_2 (X - \Delta)) \\
&\quad \sum_{\sigma,\sigma' \in \{\pm 1\}} \sigma \cdot \sigma' \cdot \mathsf{card}(X_{\sigma,\sigma'}) \\
&= \mathsf{card}(X_{+1,+1}) + \Big(-1 + \mathsf{card}(X_{+1,+1})\Big) \\
&\qquad - \Big((p+1)/2 - \mathsf{card}(X_{+1,+1})\Big) - \Big((p+1)/2 - \mathsf{card}(X_{+1,+1})\Big) \\
&\qquad\qquad\qquad\qquad \text{(Using Equation 7, Equation 6, and Equation 8)} \\
&= 4 \cdot \mathsf{card}(X_{+1,+1}) - (p+2) \\
&= 4 \cdot \mathsf{card}\big(F^+ \alpha_1^{-1} \cap \left(F^+ \alpha_2^{-1} + \Delta\right)\big) - (p+2).
\end{aligned}$$

Substituting this value in Equation 5, we get that

$$2\mathsf{SD}\left(\vec{\mathsf{LSB}}(\mathsf{Share}(0))\ ,\ \vec{\mathsf{LSB}}(\mathsf{Share}(s))\right) = \frac{1}{p} \cdot \left|\Sigma^{(0)}_{\alpha_1,\alpha_2} - \Sigma^{(\Delta)}_{\alpha_1,\alpha_2}\right|,$$

which proves Lemma 1.

7 Security against Physical Bit Leakage

We consider $\mathsf{ShamirSS}(n = 2, k = 2, (\alpha_1, \alpha_2))$ over the prime field F of order $p \geqslant 3$. In this section, we consider p a Mersenne prime, i.e., $p = 2^\lambda - 1$, where λ is the security parameter. Some initial Mersenne primes are $3, 7, 31, 127, 8191$, and 131071. The largest Mersenne prime, currently known, is $2^{82,589,933} - 1$. Mersenne primes have fascinating properties.

Proposition 5. *Suppose $x \in F$ and define $x' = x \cdot (2^i) \in F$, where $i \in \{-\lambda + 1, \ldots, 0, 1, \ldots, \lambda - 1\}$. Then the binary representation of x' is a cyclic left rotation of the binary representation of x by i bits.*

We clarify that if i is negative, then "i bit cyclic left rotation" is the same as "$|i|$ bit cyclic right rotation." This proposition is straightforward from the identity that $2^\lambda = 1 \mod p$. Additionally, it implies that $2^{\lambda+i} = 2^i \mod p$, for all negative $i \in \{-p+1, \ldots, -1\}$.

Suppose $i \in \{0, 1, \ldots, \lambda - 1\}$. Let $E_i \subseteq \{0, 1, \ldots, p-1\} = F$ be the set of all element $x \in F$ such that the binary representation of x has 0 at its i-th position. We remind the reader that $i = 0$ indicates the least significant bit, and $i = (\lambda - 1)$ indicates the most significant bit. We represent $E = \{0, 2, \ldots, (p-1)/2\}$ as the set of all "even elements" in F.

Proposition 6. *For all $i \in \{0, 1, \ldots, \lambda - 1\}$, we have $E_i = E \cdot (2^i)$.*

Note that if $x \in E_i$ then $x \cdot (2^{-i}) \in E$. Moreover, for any $x' \in E$, we have $x \cdot (2^i) \in E_i$. Both these properties hold due to Proposition 5.

Let $\mathrm{LSB}_i \colon F \to \{0, 1\}$ represent the function that outputs the i-th least significant bit in the binary representation. So, for example, $\mathrm{LSB}_i^{-1}(0) = E_i = E \cdot (2^i)$. We aim to investigate the leakage resilience of $\mathsf{ShamirSS}(2, 2, (\alpha_1, \alpha_2))$ over the prime field F with order $p = 2^\lambda - 1$ against physical bit leakage attacks. Consider a leakage attack that leaks the i-th LSB of the first secret share and the j-th LSB of the second secret share. We represent this leakage as $\vec{\mathrm{LSB}}_{i,j}$.

7.1 A Special Case to Address

There is a subtlety to address. Although $\alpha_1 \neq \alpha_2$, it may be possible that $2^k \alpha_1 = \alpha_2$, for some $k \in \{0, 1, \ldots, \lambda - 1\}$. This section proves that the secret-sharing scheme is insecure, taking care of this case in the algorithm of Figure 1.

Since α_1 and α_2 are distinct, it must be the case that $2^k \alpha_1 = \alpha_2$, where $k \in \{1, 2, \ldots, \lambda - 1\}$. Suppose we are leaking the i-th bit of the first secret share and the j-th bit of the second secret share, such that $j - i = k$.

Suppose the secret is $s \in F$ and the secret share at evaluation place X is $s + uX$, for uniformly random $u \in F$. The joint distribution of leakage is

$$(\mathrm{LSB}_i(s + u\alpha_1), \mathrm{LSB}_j(s + u\alpha_2)) .$$

Since $E_i = E2^i$ and $E_j = E2^j$, this joint distribution is identical to

$$\left(\mathrm{LSB}_0(s2^{-i} + u\alpha_1 2^{-i}), \mathrm{LSB}_0(s2^{-j} + u\alpha_2 2^{-j})\right) .$$

Define some variable renaming. Let $v := u2^{-j}$ and $t := s2^{-j}$. The joint distribution of leakage is (for uniformly random $v \in F$)

$$\left(\mathrm{LSB}_0(t2^k + v\alpha_1 2^k), \mathrm{LSB}_0(t + v\alpha_2)\right) \equiv \left(\mathrm{LSB}_0(t2^k + v\alpha_2), \mathrm{LSB}_0(t + v\alpha_2)\right) ,$$

because $2^k \alpha_1 = \alpha_2$.

Note that for $t = 0$, both the leakage bits are identical. Let $t^* := (2^k - 1)^{-1}$. Then, the joint distribution of leakage is

$$(\mathrm{LSB}_0(1 + t^* + v\alpha_2), \mathrm{LSB}_0(t^* + v\alpha_2))$$

These two leakage bits are different with $(1 - 1/p)$ probability. Therefore, one can distinguish $s = 0$ and $s = t^* 2^j$ with ~ 1 advantage by leaking $\vec{\mathrm{LSB}}_{i,j}$.

7.2 Reduction to the LSB Attack

To study the leakage resilience, we proceed similarly to the proof of Section 6.1.

$$\begin{aligned}
&2\mathsf{SD}\left(\vec{\mathrm{LSB}}_{i,j}(\mathsf{Share}(0)) \;,\; \vec{\mathrm{LSB}}_{i,j}(\mathsf{Share}(s))\right) \\
&\quad= \sum_{\vec{\ell}\in\{0,1\}^2} \left|\Pr\left[\vec{\mathrm{LSB}}_{i,j}(\mathsf{Share}(0)) = \vec{\ell}\right] - \Pr\left[\vec{\mathrm{LSB}}_{i,j}(\mathsf{Share}(s)) = \vec{\ell}\right]\right| \\
&\quad= \sum_{\vec{\ell}\in\{0,1\}^2} \Bigg|\mathop{\mathbb{E}}_x\left[\mathbb{1}_{\mathrm{LSB}_i^{-1}(\ell_1)}(\alpha_1 x)\cdot\mathbb{1}_{\mathrm{LSB}_j^{-1}(\ell_2)}(\alpha_2 x)\right] \\
&\qquad\qquad - \mathop{\mathbb{E}}_x\left[\mathbb{1}_{\mathrm{LSB}_i^{-1}(\ell_1)}(\alpha_1 x + s)\cdot\mathbb{1}_{\mathrm{LSB}_j^{-1}(\ell_2)}(\alpha_2 x + s)\right]\Bigg| \\
&\quad= \sum_{\vec{\ell}\in\{0,1\}^2} \Bigg|\mathop{\mathbb{E}}_x\left[\mathbb{1}_{\mathrm{LSB}_i^{-1}(0)}(\alpha_1 x)\cdot\mathbb{1}_{\mathrm{LSB}_j^{-1}(0)}(\alpha_2 x)\right] \\
&\qquad\qquad - \mathop{\mathbb{E}}_x\left[\mathbb{1}_{\mathrm{LSB}_i^{-1}(0)}(\alpha_1 x + s)\cdot\mathbb{1}_{\mathrm{LSB}_j^{-1}(0)}(\alpha_2 x + s)\right]\Bigg| \\
&\qquad\qquad\qquad\qquad \text{(Using the fact that } \mathbb{1}_{\mathrm{LSB}_k^{-1}(1)} = 1 - \mathbb{1}_{\mathrm{LSB}_k^{-1}(0)}\text{)} \\
&\quad= 4\cdot\left|\mathop{\mathbb{E}}_x\left[\mathbb{1}_{E_i}(\alpha_1 x)\cdot\mathbb{1}_{E_j}(\alpha_2 x)\right] - \mathop{\mathbb{E}}_x\left[\mathbb{1}_{E_i}(\alpha_1 x + s)\cdot\mathbb{1}_{E_j}(\alpha_2 x + s)\right]\right| \\
&\quad= 4\cdot\left|\mathop{\mathbb{E}}_x\left[\mathbb{1}_{E(2^i)}(\alpha_1 x)\cdot\mathbb{1}_{E(2^j)}(\alpha_2 x)\right] - \mathop{\mathbb{E}}_x\left[\mathbb{1}_{E(2^i)}(\alpha_1 x + s)\cdot\mathbb{1}_{E(2^j)}(\alpha_2 x + s)\right]\right| \\
&\qquad\qquad\qquad\qquad \text{(By Proposition 6)} \\
&\quad= 4\cdot\Bigg|\mathop{\mathbb{E}}_x\left[\mathbb{1}_E(2^{-i}\alpha_1 x)\cdot\mathbb{1}_E(2^{-j}\alpha_2 x)\right] \\
&\qquad\qquad - \mathop{\mathbb{E}}_x\left[\mathbb{1}_E(2^{-i}\alpha_1 x + 2^{-i}s)\cdot\mathbb{1}_E(2^{-j}\alpha_2 x + 2^{-j}s)\right]\Bigg| \qquad (9)
\end{aligned}$$

At this point, we introduce the following variable renaming.

Claim. The quantity

$$\mathop{\mathbb{E}}_x\left[\mathbb{1}_E(2^{-i}\alpha_1 x + 2^{-i}s)\cdot\mathbb{1}_E(2^{-j}\alpha_2 x + 2^{-j}s)\right]$$

is identical to

$$\mathop{\mathbb{E}}_y\left[\mathbb{1}_E(2^{-i}\alpha_1 y + s')\cdot\mathbb{1}_E(2^{-j}\alpha_2 y + s')\right],$$

where

$$y := x + \frac{2^{-i} - 2^{-j}}{2^{-i}\alpha_1 - 2^{-j}\alpha_2}, \qquad \text{and} \qquad s' := \frac{2^{-i}2^{-j}(\alpha_1 - \alpha_2)}{2^{-i}\alpha_1 - 2^{-j}\alpha_2} \cdot s$$

The proof of this claim is by direct substitution. Note that $s \mapsto s'$ is an automorphism over F^*. We continue the derivation from the expression in Equation 9 as follows.

$$\begin{aligned} &= 4 \cdot \Big| \mathop{\mathbb{E}}_{x} \left[\mathbb{1}_E(2^{-i}\alpha_1 x) \cdot \mathbb{1}_E(2^{-j}\alpha_2 x) \right] \\ &\qquad\qquad - \mathop{\mathbb{E}}_{y} \left[\mathbb{1}_E(2^{-i}\alpha_1 y + s') \cdot \mathbb{1}_E(2^{-j}\alpha_2 y + s') \right] \Big| \\ &= \varepsilon_{\mathrm{LSB}}(2^{-i}\alpha_1, 2^{-j}\alpha_2). \end{aligned}$$

Therefore, we conclude that the insecurity of $\mathsf{ShamirSS}(2, 2, (\alpha_1, \alpha_2))$ secret-sharing scheme against the $\vec{\mathrm{LSB}}_{i,j}$ is identical to the insecurity of the $\mathsf{ShamirSS}(2, 2, (2^{-i}\alpha_1, 2^{-j}\alpha_2))$ secret-sharing scheme against the LSB attack. Let $\varepsilon_{\mathrm{PHYS}}(\alpha_1, \alpha_2)$ represent the insecurity of the $\mathsf{ShamirSS}(2, 2, (\alpha_1, \alpha_2))$ secret-sharing scheme against all physical bit leakage attacks. Let $\varepsilon_{\mathrm{LSB}}(\alpha, \alpha')$ represent the insecurity of the $\mathsf{ShamirSS}(2, 2, (\alpha, \alpha'))$ secret-sharing scheme against the LSB leakage attack.

We conclude that

$$\begin{aligned} \varepsilon_{\mathrm{PHYS}}(\alpha_1, \alpha_2) &= \max_{i,j \in \{0,1,\ldots,\lambda-1\}} \varepsilon_{\mathrm{LSB}}(2^{-i}\alpha_1, 2^{-j}\alpha_2) \\ &= \max_{i,j \in \{0,1,\ldots,\lambda-1\}} \varepsilon_{\mathrm{LSB}}(2^{j-i}\alpha_1, \alpha_2) && \text{(By Proposition 1)} \\ &= \max_{k \in \{0,1,\ldots,\lambda-1\}} \varepsilon_{\mathrm{LSB}}(2^{k}\alpha_1, \alpha_2) && \text{(By } 2^{\lambda} = 1 \mod p\text{)} \end{aligned}$$

7.3 Proof of Corollary 1

Recall that the algorithm in Figure 2 outputs "insecure" or "may be insecure" for $\sim \frac{\sqrt{p}}{4} \ln p$ equivalence classes among $(p-2)$ equivalence classes (see Section 3.1). So, by union bound, the algorithm in Figure 1 outputs "insecure" or "may be insecure" for (at most) $\sim \lambda \cdot \frac{\sqrt{p}}{4} \ln p = \frac{\sqrt{p}}{4} \mathsf{poly}(\log p)$ equivalence classes. This number is an exponentially small fraction of the $(p-2)$ equivalence classes.

When the algorithm in Figure 2 outputs that the equivalence class is secure, then the insecurity of the $\mathsf{ShamirSS}(2, 2, (\alpha_1, \alpha_2))$ secret-sharing scheme is at most

$$\frac{1}{\sqrt{p}} + \frac{8B}{p} \sim \frac{8^{5/3} + 1}{\sqrt{p}}.$$

7.4 Explicit Pairs of Secure Evaluation Places

We prove the following result.

Lemma 13 (Explicit Recommendation for Evaluation Places). *Define* $(\alpha_1, \alpha_2) := (1, 2^{\lfloor \lambda/2 \rfloor} - 1)$. *For this case, we have*

$$\varepsilon_{\mathrm{LSB}}(2^i \alpha_1, \alpha_2) \leqslant \begin{cases} \frac{1}{\alpha_2} + \frac{4(1+\alpha_2)}{p} & \text{if } i = 0 \\ \frac{4(2^{\lfloor \lambda/2 \rfloor} + \alpha_2)}{p} & \text{if } 1 \leqslant i \leqslant \lfloor \lambda/2 \rfloor \\ \frac{4(2^{\lfloor \lambda/2 \rfloor} + 2\alpha_2 + 1)}{p} & \text{if } \lfloor \lambda/2 \rfloor + 1 \leqslant i \leqslant \lambda - 1. \end{cases}$$

Consequently, $\mathsf{ShamirSS}(2, 2, (\alpha_1, \alpha_2))$ secret-sharing scheme is secure against physical bit attacks. Using the fact that $\alpha_2 \sim 2^{\lfloor \lambda/2 \rfloor}$, the insecurity of this scheme is, at most

$$\varepsilon_{\mathrm{PHYS}} \lesssim \frac{12}{2^{\lceil \lambda/2 \rceil}}.$$

We remark that one can choose any pair of evaluation places in the equivalence class $[\alpha_1 : \alpha_2]$, and it will have identical security.

Proof (of Lemma 13). We go over the individual cases below.

Case A: $i = 0$**.** We are interested in the security of evaluation places $(u, v) = (1, 2^t - 1)$, where $t = \lfloor \lambda/2 \rfloor$. Note that α_1 and α_2 are relatively prime and $|u|_p = 1$ and $|v| = 2^t - 1$. Both these evaluation places are odd. Therefore, we can apply Theorem 2. The insecurity is

$$\varepsilon \leqslant \frac{1}{2^t - 1} + \frac{4 + 4(2^t - 1) - 2}{p}.$$

Case B: $1 \leqslant i \leqslant \lfloor \lambda/2 \rfloor$**.** We are interested in the security of evaluation places $(u, v) = (2^i, 2^t - 1)$, where $t = \lfloor \lambda/2 \rfloor$. Note that u and v are relatively prime and $|u|_p = 2^i$ and $|v|_p = 2^t - 1$. Note that u is even and v is odd. Therefore, we can apply Theorem 1. The insecurity is

$$\varepsilon \leqslant \frac{4 \cdot 2^i + 4(2^t - 1) - 2}{p}.$$

Case C: $\lfloor \lambda/2 \rfloor + 1 \leqslant i \leqslant \lambda - 1$**.** We are interested in the security of evaluation places $(u, v) = (2^i, 2^t - 1)$, where $t + 1 \leqslant i \leqslant \lambda - 1$ and $t = \lfloor \lambda/2 \rfloor$. Note that $(u', v') := 2^{\lambda - t} \cdot (u, v) \in [u : v]$.

Now $u' = 2^{\lambda - t} \cdot 2^i \mod 2^\lambda - 1 = 2^{i-t}$. Moreover, $v' = 2^{\lambda - t} \cdot (2^t - 1) \mod 2^\lambda - 1 = -(2^{\lambda - t} - 1) \mod 2^\lambda - 1$.

Substituting new variables, we have $u' = 2^j$ and $v' = -(2^{\lambda - t} - 1)$, where $1 \leqslant j \leqslant \lambda - t - 1$. This case is identical to Case B above, and we conclude that the insecurity is

$$\varepsilon \leqslant \frac{4 \cdot 2^j + 4(2^{\lambda - t} - 1) - 2}{p}.$$

Now, let us substitute $t = \lfloor \lambda/2 \rfloor$. For this case $1 \leqslant j \leqslant \lambda - t - 1 = \lfloor \lambda/2 \rfloor$. Moreover, $2^{\lambda - t} - 1 = 2(2^t - 1) + 1$. □

7.5 Experimentally-generated Pairs of Secure Evaluation Places

The output of the LLL algorithm is crucial in assessing whether evaluation places are secure. Remark 5 illustrates that the output of the LLL can change the output of our algorithm in Figure 2 from "secure" to "may be insecure."

This section considers an "adversarial LLL" algorithm implementation for the worst-case evaluation. On input (α_1, α_2), if there is $(u, v) \in [\alpha_1 : \alpha_2]$ that makes our algorithm in Figure 2 output "may be insecure," the adversarial LLL outputs that (u, v).

Supporting Material C presents a table to help choose secure evaluation places against any physical bit leakage for the Mersenne prime $p = 2^{13} - 1$.

8 Extension to arbitrary Number of Parties

We extend our derandomization results to Shamir's secret sharing with the reconstruction threshold k equal to the number of parties $n \in \{2, 3, \dots\}$. We prove the following lifting theorem.

Theorem 4. *Consider* $\mathsf{ShamirSS}(n, n, \vec{\alpha})$ *over a prime field* F*. For every* $i \in \{1, 2, \dots, n\}$*, define* $\beta_i := \left(\alpha_i \prod_{j \neq i} (\alpha_i - \alpha_j)\right)^{-1}$*. Suppose there are two indices* $1 \leqslant i^* < j^* \leqslant n$ *such that* $\mathsf{ShamirSS}(2, 2, (\beta_{i^*}, \beta_{j^*}))$ *has* ε*-insecurity against physical bit leakages. Then,* $\mathsf{ShamirSS}(n, n, (\alpha_1, \alpha_2, \dots, \alpha_n))$ *has at most* 2ε*-insecurity against physical bit leakages.*

8.1 Fourier Basics and Generalized Reed-Solomon Codes

Generalized Reed-Solomon Code. A generalized Reed-Solomon code over a prime field F with message length k and block length n consists of an encoding function $\mathsf{Enc}\colon F^k \to F^n$ and decoding function $\mathsf{Dec}\colon F^n \to F^k$. It is specified by the *evaluation places* $\vec{\alpha} = (\alpha_1, \dots, \alpha_n)$, such that for all $1 \leqslant i < j \leqslant n$, $\alpha_i \neq \alpha_j$, and a *scaling vector* $\vec{u}$ such that for all $1 \leqslant i \leqslant n$, $u_i \in F^*$. Given $\vec{\alpha}$ and $\vec{u}$, the *encoding function* is

$$\mathsf{Enc}(m_1, \dots, m_k) := (u_1 \cdot f(\alpha_1), \dots, u_n \cdot f(\alpha_n)),$$

where $f(X) := m_1 + m_2 X + \cdots + m_k X^{k-1}$. We represent this code as $[n, k, \vec{\alpha}, \vec{u}]_F$-GRS.

The following standard properties of generalized Reed-Solomon codes shall be helpful for our extension to an arbitrary number of parties [10, 18].

Imported Theorem 1 (Properties of GRS) *The dual code of* $[n, k, \vec{\alpha}, \vec{u}]_F$*-GRS is identical to the* $[n, n-k, \vec{\alpha}, \vec{v}]_F$*-GRS, where for all* $1 \leqslant i \leqslant n$*,*

$$v_i^{-1} := u_i \prod_{\substack{j=1 \\ j \neq i}}^{n} (\alpha_i - \alpha_j).$$

In particular, when $n = k$*, the dual code is the set* $\{\beta \cdot (v_1, v_2, \dots, v_n)\colon \beta \in F\}$*, a dimension one vector space over* F*.*

We will apply this theorem to the dual of the code containing all possible secret shares of the secret 0 in $[n, n, \vec{\alpha}]$-Shamir secret-sharing.

Fourier Basics We use Fourier analysis on prime field F of order p. Define $\omega := \exp(2\pi\imath/p)$. For any functions $f, g \colon F \to \mathbb{C}$, we define the inner product as

$$\langle f, g \rangle := \frac{1}{p} \sum_{x \in F} f(x) \cdot \overline{g(x)},$$

where $\overline{z}$ is the complex conjugate of $z \in \mathbb{C}$. For $z \in \mathbb{C}$, $|z| := \sqrt{z\overline{z}}$. For any $\alpha \in F$, define the function $\widehat{f} \colon F \to \mathbb{C}$ as follows.

$$\widehat{f}(\alpha) := \frac{1}{p} \sum_{x \in F} f(x) \cdot \omega^{-\alpha x}.$$

The Fourier transform maps the function f to the function $\widehat{f}$.

Lemma 14 (Fourier Inversion Formula). $f(x) = \sum_{\alpha \in F} \widehat{f}(\alpha) \cdot \omega^{\alpha x}$.

The following propositions will be useful, which follow directly from the definition.

Proposition 7. *Let $S, T \subseteq F$ be a bipartition of F. For all $\alpha \in F$,*

$$\widehat{\mathbb{1}_S}(\alpha) = -\widehat{\mathbb{1}_T}(\alpha).$$

Proposition 8 (Properties of Fourier Coefficients). *For all $S \subseteq F$ and $x, \alpha \in F$, it holds that*

$$\widehat{\mathbb{1}_{x+S}}(\alpha) = \widehat{\mathbb{1}_S}(\alpha) \cdot \omega^{-\alpha \cdot x},$$

$$\widehat{\mathbb{1}_S}(x \cdot \alpha) = \widehat{\mathbb{1}_{S \cdot x}}(\alpha).$$

8.2 Some Preparatory Results

The following result rewrites the statistical distance between two leakage distributions using the Fourier coefficients of appropriate indicator functions.

Proposition 9. *Consider* $\mathsf{ShamirSS}(n, n)$ *over a prime field F. Let $C_0^\perp$ be the dual code of* $\mathsf{Share}(0)$*. For any one-bit leakage function $\vec{\tau} \colon F^n \to \{0,1\}^n$, any secret $s \in F$, the following identity holds.*

$$\begin{aligned} &2\mathsf{SD}\left(\vec{\tau}(\mathsf{Share}(0)) \ , \ \vec{\tau}(\mathsf{Share}(s))\right) \\ &\quad = 2^n \left| \sum_{\vec{\gamma} \in \mathcal{C}_0^\perp \setminus \vec{0}} \left(\prod_{i=1}^{n} \widehat{\mathbb{1}}_{\tau_i^{-1}(0)}(\gamma_i) \right) \cdot \left(1 - \omega^{s \cdot (\gamma_1 + \cdots + \gamma_n)}\right) \right|. \end{aligned}$$

Proof. The following identity is known in the literature (see [19] for a proof).

$$\begin{aligned}&\mathsf{2SD}\left(\vec{\tau}(\mathsf{Share}(0))\ ,\ \vec{\tau}(\mathsf{Share}(s))\right)\\&\quad=\sum_{\vec{\ell}\in\{0,1\}^n}\left|\sum_{\vec{\gamma}\in\mathcal{C}_0^\perp}\left(\prod_{i=1}^n\widehat{\mathbb{1}_{\tau_i^{-1}(\ell_i)}}(\gamma_i)\right)\cdot\left(1-\omega^{s\cdot(\gamma_1+\cdots+\gamma_n)}\right)\right|\end{aligned}$$

By Proposition 7, $\widehat{\mathbb{1}_{\tau_i^{-1}(\ell_i)}}(\gamma_i)=\widehat{\mathbb{1}_{\tau_i^{-1}(1-\ell_i)}}(\gamma_i)$ since $\tau_i^{-1}(\ell_i)$ and $\tau_i^{-1}(1-\ell_i)$ are a partition of F. Using this property, one can verify for every $\vec{\ell},\vec{\ell'}\in\{0,1\}^n$, it holds that

$$\begin{aligned}&\left|\sum_{\vec{\gamma}\in\mathcal{C}_0^\perp}\left(\prod_{i=1}^n\widehat{\mathbb{1}_{\tau_i^{-1}(\ell_i)}}(\gamma_i)\right)\cdot\left(1-\omega^{s\cdot(\gamma_1+\cdots+\gamma_n)}\right)\right|\\&\quad=\left|\sum_{\vec{\gamma}\in\mathcal{C}_0^\perp}\left(\prod_{i=1}^n\widehat{\mathbb{1}_{\tau_i^{-1}(\ell'_i)}}(\gamma_i)\right)\cdot\left(1-\omega^{s\cdot(\gamma_1+\cdots+\gamma_n)}\right)\right|.\end{aligned}$$

Therefore, we have

$$\begin{aligned}&\mathsf{2SD}\left(\vec{\tau}(\mathsf{Share}(0))\ ,\ \vec{\tau}(\mathsf{Share}(s))\right)\\&\quad=2^n\left|\sum_{\vec{\gamma}\in\mathcal{C}_0^\perp\setminus\vec{0}}\left(\prod_{i=1}^n\widehat{\mathbb{1}}_{\tau_i^{-1}(0)}(\gamma_i)\right)\cdot\left(1-\omega^{s\cdot(\gamma_1+\cdots+\gamma_n)}\right)\right|,\end{aligned}$$

as desired. □

Proposition 10. *Let $A_1,A_2,\ldots,A_n\subseteq F$ and $\beta_1,\beta_2,\ldots,\beta_n\in F^*$. Then, for any $s\in F$, the following identity holds.*

$$\begin{aligned}&\sum_{t\in F}\prod_{i=1}^n\left(\widehat{\mathbb{1}_{A_i\cdot\beta_i}}(t)\cdot\omega^{s\cdot t\cdot\beta_i}\right)\\&=\frac{1}{p^{n-1}}\sum_{\substack{x_n\in A_n\cdot\beta_n\\\vdots\\x_3\in A_3\cdot\beta_3}}\mathsf{card}(A_2)-\mathsf{card}\left(\left(A_2\cdot\beta_2+\sum_{i=3}^n x_i-s\cdot\sum_{i=1}^n\beta_i\right)\bigcap A_1\cdot\beta_1\right)\end{aligned}$$

Proof. We shall extensively use the linear property of Fourier coefficients.

$$\begin{aligned}&\sum_{t\in F}\prod_{i=1}^n\left(\widehat{\mathbb{1}_{A_i\cdot\beta_i}}(t)\cdot\omega^{s\cdot t\cdot\beta_i}\right)\\&=\sum_{t\in F}\prod_{i}^n\left(\frac{1}{p}\sum_{x_i\in F}\mathbb{1}_{A_i\cdot\beta_i}(x_i)\cdot\omega^{-t\cdot x_i}\cdot\omega^{s\cdot t\cdot\beta_i}\right)\qquad\text{(Fourier expansion)}\end{aligned}$$

$$= \frac{1}{p^n} \sum_{t\in F} \sum_{\vec{x}\in F^n} \left(\prod_{i=1}^{n} \mathbb{1}_{A_i\cdot\beta_i}(x_i) \cdot \omega^{-t\cdot x_i} \cdot \omega^{s\cdot t\cdot \beta_i} \right) \qquad \text{(Linearity)}$$

$$= \frac{1}{p^n} \sum_{\vec{x}\in F^n} \left(\prod_{i=1}^{n} \mathbb{1}_{A_i\cdot\beta_i}(x_i) \right) \sum_{t\in F} \omega^{-t\cdot(x_1+\cdots+x_n - s\cdot(\beta_1+\cdots+\beta_n))} \qquad \text{(Linearity)}$$

$$= \frac{1}{p^{n-1}} \sum_{\substack{\vec{x}\in F^n : \\ x_1+\cdots+x_n = s\cdot(\beta_1+\cdots+\beta_n)}} \left(\prod_{i=1}^{n} \mathbb{1}_{A_i\cdot\beta_i}(x_i) \right) \qquad \text{(Sum of roots of unity)}$$

Now, replacing $x_1 = s\cdot(\beta_1+\cdots+\beta_n) - (x_2+\cdots+x_n)$ yields

$$\frac{1}{p^{n-1}} \sum_{x_2,\ldots,x_n\in F} \mathbb{1}_{A_1\cdot\beta_1}(s\cdot(\beta_1+\cdots+\beta_n) - (x_2+\cdots+x_n)) \cdot \prod_{i=2}^{n} \mathbb{1}_{A_i\cdot\beta_i}(x_i)$$

$$= \frac{1}{p^{n-1}} \sum_{x_n\in A_n\cdot\beta_n} \sum_{x_2\in F} \mathbb{1}_{A_2\cdot\beta_2}(x_2) \cdot \mathbb{1}_{A_1\cdot\beta_1}(s\cdot(\beta_1+\cdots+\beta_n) - (x_2+\cdots+x_n))$$

$$\vdots$$

$$x_3\in A_3\cdot\beta_3$$

Let us take a detour and simplify the inner summand using linear properties of sets and indicator functions as follows.

$$\sum_{x_2\in F} \mathbb{1}_{A_2\cdot\beta_2}(x_2) \cdot \mathbb{1}_{A_1\cdot\beta_1}(s\cdot(\beta_1+\cdots+\beta_n) - (x_2+\cdots+x_n))$$

$$= \sum_{x_2\in F} \mathbb{1}_{A_2\cdot\beta_2}(x_2) \cdot \mathbb{1}_{A_1\cdot\beta_1 - s\cdot(\beta_1+\cdots+\beta_n)+(x_3+\cdots+x_n)}(-x_2)$$

$$= \sum_{x_2\in F} \mathbb{1}_{A_2\cdot\beta_2}(x_2) \cdot \mathbb{1}_{-A_1\cdot\beta_1 + s\cdot(\beta_1+\cdots+\beta_n)-(x_3+\ldots+x_n)}(x_2)$$

$$= \mathsf{card}(A_2\cdot\beta_2 \cap (-A_1\cdot\beta_1 - (x_3+\ldots+x_n) + s\cdot(\beta_1+\cdots+\beta_n)))$$

$$= \mathsf{card}(A_2\cdot\beta_2 + (x_3+\cdots+x_n) - s\cdot(\beta_1+\cdots+\beta_n) \cap (-A_1\cdot\beta_1))$$

$$= \mathsf{card}(A_2\cdot\beta_2) - \mathsf{card}(A_2\cdot\beta_2 + (x_3+\cdots+x_n) - s\cdot(\beta_1+\cdots+\beta_n) \cap A_1\cdot\beta_1)$$

$$= \mathsf{card}(A_2) - \mathsf{card}(A_2\cdot\beta_2 + (x_3+\cdots+x_n) - s\cdot(\beta_1+\cdots+\beta_n) \cap A_1\cdot\beta_1)\,,$$

which completes the proof. □

8.3 Proof of Theorem 4

We begin with some notations. Let $\vec{\tau}\colon F^n \to \{0,1\}^n$ be any one-bit physical leakage. Let $A_i = \tau_i^{-1}(0)$ for $1 \leqslant i \leqslant n$. By Imported Theorem 1, the dual code $C_0^{\perp}$ is the set $\{t\cdot(\beta_1,\beta_2,\ldots,\beta_n)\colon t\in F\}$, where

$$\beta_i = \left(\alpha_i \prod_{j\neq i} (\alpha_i - \alpha_j) \right)^{-1}, \text{ for every } i \in \{1,2,\ldots,n\}.$$

Consider the following manipulation.

$$
\begin{aligned}
&\mathsf{2SD}\left(\vec{\tau}(\mathsf{Share}(0))\ ,\ \vec{\tau}(\mathsf{Share}(s))\right) \\
&= 2^n \cdot \left| \sum_{\vec{\gamma} \in \mathcal{C}_0^{\perp} \setminus \vec{0}} \prod_{i=1}^{n} \widehat{\mathbb{1}_{\tau_i^{-1}(0)}}(\gamma_i) \cdot \left(1 - \omega^{s \cdot (\gamma_1 + \cdots + \gamma_n)}\right) \right| \qquad (\textit{Proposition 9}) \\
&= 2^n \cdot \left| \sum_{t \in F^*} \prod_{i=1}^{n} \widehat{\mathbb{1}_{A_i}}(t \cdot \beta_i) \cdot \left(1 - \omega^{s \cdot t \cdot (\beta_1 + \cdots + \beta_n)}\right) \right| \\
&= 2^n \cdot \left| \sum_{t \in F^*} \prod_{i=1}^{n} \widehat{\mathbb{1}_{A_i \cdot \beta_i}}(t) - \sum_{t \in F^*} \prod_{i=1}^{n} \widehat{\mathbb{1}_{A_i \cdot \beta_i}}(t) \cdot \omega^{s \cdot t \cdot \beta_i} \right|
\end{aligned}
$$

For each $s \in F$ and tuple $(x_3, x_4, \ldots, x_n)$ satisfying $x_i \in A_i \cdot \beta_i$ for $3 \leqslant i \leqslant n$, we define

$$
\begin{aligned}
&\phi_{s,\vec{\tau}}(x_3, x_4, \ldots, x_n) := \\
&\qquad \sum_{x_n \in A_n \cdot \beta_n} \cdots \sum_{x_3 \in A_3 \cdot \beta_3} \mathsf{card}\left(\left(A_2 \cdot \beta_2 + \sum_{i=3}^{n} x_i - s \cdot \sum_{i=1}^{n} \beta_i \right) \bigcap A_1 \cdot \beta_1 \right).
\end{aligned}
$$

Then, it follows from Proposition 10 that

$$
\mathsf{2SD}\left(\vec{\tau}(\mathsf{Share}(0))\ ,\ \vec{\tau}(\mathsf{Share}(s))\right) = \frac{2^{n-1}}{p^{n-1}} \cdot \left| \phi_{0,\vec{\tau}}(x_3, \ldots, x_n) - \phi_{s,\vec{\tau}}(x_3, \ldots, x_n) \right|.
$$

It suffices to prove the result when $\vec{\tau} = \vec{\mathrm{LSB}}$ (the proof for arbitrary physical bit leakage is similar). In this case, note that $A_1 = A_2 = E = F^+ \cdot 2$. Therefore, we have

$$
\begin{aligned}
&\mathsf{card}\left(\left(A_2 \cdot \beta_2 + \sum_{i=3}^{n} x_i - s \cdot \sum_{i=1}^{n} \beta_i \right) \bigcap A_1 \cdot \beta_1 \right) \\
&\quad = \mathsf{card}\left(\left(F^+ \cdot 2 \cdot \beta_2 + \sum_{i=3}^{n} x_i - s \cdot \sum_{i=1}^{n} \beta_i \right) \bigcap F^+ \cdot 2 \cdot \beta_1 \right) \\
&\quad = \mathsf{card}\left(\left(F^+ \cdot \beta_2 + 2^{-1} \cdot \left(\sum_{i=3}^{n} x_i - s \cdot \sum_{i=1}^{n} \beta_i \right) \right) \bigcap F^+ \cdot \beta_1 \right) \\
&\quad = \Sigma^{\left(\Delta^{(s)}_{x_3,\ldots,x_n}\right)}_{\beta_1^{-1}, \beta_2^{-1}},
\end{aligned}
$$

where $\Delta^{(s)}_{x_3,\ldots,x_n} := 2^{-1} \cdot (\sum_{i=3}^{n} x_i - s \cdot \sum_{i=1}^{n} \beta_i)$. Similar to the proof of Lemma 1, we have

$$
\begin{aligned}
&\mathsf{2SD}\left(\vec{\mathrm{LSB}}(\mathsf{Share}(0))\ ,\ \vec{\mathrm{LSB}}(\mathsf{Share}(s))\right) \\
&= \frac{2^{n-2}}{p^{n-1}} \cdot \left| \sum_{x_n \in E \cdot \beta_n} \cdots \sum_{x_3 \in E \cdot \beta_3} \left(\Sigma^{\left(\Delta^{(0)}_{x_3,\ldots,x_n}\right)}_{\beta_1^{-1}, \beta_2^{-1}} - \Sigma^{\left(\Delta^{(s)}_{x_3,\ldots,x_n}\right)}_{\beta_1^{-1}, \beta_2^{-1}} \right) \right|
\end{aligned}
$$

$$\leqslant \frac{2^{n-2}}{p^{n-1}} \cdot \sum_{x_n \in E\cdot\beta_n} \cdots \sum_{x_3 \in E\cdot\beta_3} \left| \left(\Sigma^{\left(\Delta^{(0)}_{x_3,\ldots,x_n}\right)}_{\beta_1^{-1},\beta_2^{-1}} - \Sigma^{\left(\Delta^{(s)}_{x_3,\ldots,x_n}\right)}_{\beta_1^{-1},\beta_2^{-1}} \right) \right|$$

(By triangle inequality)

Suppose $\mathsf{ShamirSS}(2, 2, (\beta_1, \beta_2))$ have ε insecurity against LSB. Then, it follows from Lemma 1 that

$$\left| \Sigma^{\left(\Delta^{(0)}_{x_3,\ldots,x_n}\right)}_{\beta_1^{-1},\beta_2^{-1}} - \Sigma^{\left(\Delta^{(s)}_{x_3,\ldots,x_n}\right)}_{\beta_1^{-1},\beta_2^{-1}} \right| \leqslant 2\varepsilon p. \tag{10}$$

Applying the above equation for every term under the summand yields.

$$\begin{aligned} 2\mathsf{SD}\left(\vec{\mathrm{LSB}}(\mathsf{Share}(0)) \ , \ \vec{\mathrm{LSB}}(\mathsf{Share}(s))\right) &\leqslant \frac{2^{n-2}}{p^{n-1}} \cdot \sum_{x_n \in E\cdot\beta_n} \cdots \sum_{x_3 \in E\cdot\beta_3} 2\varepsilon p \\ &\leqslant \frac{2^{n-2}}{p^{n-1}} \cdot \underbrace{(p/2)\cdots(p/2)}_{(n-2)\text{-times}} \cdot 2\varepsilon p \\ &= 2\varepsilon, \end{aligned}$$

which completes the proof.

References

1. Donald Q. Adams, Hemanta K. Maji, Hai H. Nguyen, Minh L. Nguyen, Anat Paskin-Cherniavsky, Tom Suad, and Mingyuan Wang. Lower bounds for leakage-resilient secret sharing schemes against probing attacks. In *IEEE International Symposium on Information Theory ISIT 2021*, 2021. 4
2. Amos Beimel. Secret-sharing schemes: A survey. In *Coding and Cryptology: Third International Workshop, IWCC 2011, Qingdao, China, May 30-June 3, 2011. Proceedings 3*, pages 11–46. Springer, 2011. 1
3. 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, *CRYPTO 2018, Part I*, volume 10991 of *LNCS*, pages 531–561. Springer, Heidelberg, August 2018. doi:10.1007/978-3-319-96884-1_18. 2, 4
4. Fabrice Benhamouda, Akshay Degwekar, Yuval Ishai, and Tal Rabin. On the local leakage resilience of linear secret sharing schemes. *Journal of Cryptology*, 34(2):10, April 2021. doi:10.1007/s00145-021-09375-2. 4
5. Dan Boneh, Richard A. DeMillo, and Richard J. Lipton. On the importance of checking cryptographic protocols for faults (extended abstract). In Walter Fumy, editor, *EUROCRYPT'97*, volume 1233 of *LNCS*, pages 37–51. Springer, Heidelberg, May 1997. doi:10.1007/3-540-69053-0_4. 1
6. Luís T. A. N. Brandão and René Peralta. NIST first call for multi-party threshold schemes. https://csrc.nist.gov/publications/detail/nistir/8214c/draft, January 25, 2023. 1
7. Nicolas Costes and Martijn Stam. Redundant code-based masking revisited. *IACR TCHES*, 2021(1):426–450, 2021. https://tches.iacr.org/index.php/TCHES/article/view/8740. doi:10.46586/tches.v2021.i1.426-450. 2
8. Vipul Goyal and Ashutosh Kumar. Non-malleable secret sharing. In Ilias Diakonikolas, David Kempe, and Monika Henzinger, editors, *50th ACM STOC*, pages 685–698. ACM Press, June 2018. doi:10.1145/3188745.3188872. 2
9. Alfréd Haar. Aur theorie der orthogonalen funcktionensysteme. *Math. Annalen*, 69:331–371, 1910. 4
10. Jonathan I. Hall. Notes on coding theory. https://users.math.msu.edu/users/halljo/classes/codenotes/GRS.pdf, 2015. 9, 29
11. JL Hammond Jr and RS Johnson. A review of orthogonal square-wave functions and their application to linear networks. *Journal of the Franklin Institute*, 273(3):211–225, 1962. 4, 16
12. Walter J Harrington and John W Cell. A set of square-wave functions orthogonal and complete in l 2 (0, 2). 1961. 4, 13, 15, 16, 17, 40
13. Yuval Ishai, Amit Sahai, and David Wagner. Private circuits: Securing hardware against probing attacks. In Dan Boneh, editor, *CRYPTO 2003*, volume 2729 of *LNCS*, pages 463–481. Springer, Heidelberg, August 2003. doi:10.1007/978-3-540-45146-4_27. 2
14. Yael Tauman Kalai and Leonid Reyzin. A survey of leakage-resilient cryptography. In *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*, pages 727–794. 2019. 3
15. Steven G Krantz. *A panorama of harmonic analysis*, volume 27. American Mathematical Soc., 2019. 16
16. Jeffrey C Lagarias. The computational complexity of simultaneous diophantine approximation problems. *SIAM Journal on Computing*, 14(1):196–209, 1985. 5, 7

17. Arjen K Lenstra, Hendrik Willem Lenstra, and László Lovász. Factoring polynomials with rational coefficients. *Mathematische annalen*, 261(ARTICLE):515–534, 1982. 3, 4, 5, 14, 39
18. Yehuda Lindell. Introduction to coding theory lecture notes. https://u.cs.biu.ac.il/~lindell/89-662/coding_theory-lecture-notes.pdf, 2010. 9, 29
19. Hemanta K. Maji, Hai H. Nguyen, Anat Paskin-Cherniavsky, Tom Suad, and Mingyuan Wang. Leakage-resilience of the shamir secret-sharing scheme against physical-bit leakages. In Anne Canteaut and François-Xavier Standaert, editors, *EUROCRYPT 2021, Part II*, volume 12697 of *LNCS*, pages 344–374. Springer, Heidelberg, October 2021. doi:10.1007/978-3-030-77886-6_12. 2, 3, 4, 31
20. Hemanta K. Maji, Hai H. Nguyen, Anat Paskin-Cherniavsky, Tom Suad, Mingyuan Wang, Xiuyu Ye, and Albert Yu. Leakage-resilient linear secret-sharing against arbitrary bounded-size leakage family. In Eike Kiltz and Vinod Vaikuntanathan, editors, *TCC 2022, Part I*, volume 13747 of *LNCS*, pages 355–383. Springer, Heidelberg, November 2022. doi:10.1007/978-3-031-22318-1_13. 4
21. Hemanta K. Maji, Hai H. Nguyen, Anat Paskin-Cherniavsky, Tom Suad, Mingyuan Wang, Xiuyu Ye, and Albert Yu. Tight estimate of the local leakage resilience of the additive secret-sharing scheme & its consequences. In Dana Dachman-Soled, editor, *3rd Conference on Information-Theoretic Cryptography, ITC 2022, July 5-7, 2022, Cambridge, MA, USA*, volume 230 of *LIPIcs*, pages 16:1–16:19. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022. doi:10.4230/LIPIcs.ITC.2022.16. 2, 4
22. Hemanta K. Maji, Hai H. Nguyen, Anat Paskin-Cherniavsky, and Mingyuan Wang. Improved bound on the local leakage-resilience of shamir's secret sharing. In *2022 IEEE International Symposium on Information Theory (ISIT)*, pages 2678–2683, 2022. doi:10.1109/ISIT50566.2022.9834695. 4
23. Hemanta K. Maji, Anat Paskin-Cherniavsky, Tom Suad, and Mingyuan Wang. Constructing locally leakage-resilient linear secret-sharing schemes. In Tal Malkin and Chris Peikert, editors, *CRYPTO 2021, Part III*, volume 12827 of *LNCS*, pages 779–808, Virtual Event, August 2021. Springer, Heidelberg. doi:10.1007/978-3-030-84252-9_26. 4
24. James L Massey. Some applications of code duality in cryptography. *Mat. Contemp*, 21(187-209):16th, 2001. 8
25. Jesper Buus Nielsen and Mark Simkin. Lower bounds for leakage-resilient secret sharing. In Anne Canteaut and Yuval Ishai, editors, *EUROCRYPT 2020, Part I*, volume 12105 of *LNCS*, pages 556–577. Springer, Heidelberg, May 2020. doi:10.1007/978-3-030-45721-1_20. 4
26. Hans Rademacher. Einige sätze über reihen von allgemeinen orthogonalfunktionen. *Mathematische Annalen*, 87(1-2):112–138, 1922. 4
27. Matthieu Rivain and Emmanuel Prouff. Provably secure higher-order masking of AES. In Stefan Mangard and François-Xavier Standaert, editors, *CHES 2010*, volume 6225 of *LNCS*, pages 413–427. Springer, Heidelberg, August 2010. doi:10.1007/978-3-642-15031-9_28. 2
28. Wolfgang M Schmidt. *Diophantine approximation*. Springer Science & Business Media, 1996. 4
29. Wolfgang M Schmidt. *Diophantine approximations and Diophantine equations*. Springer, 2006. 4
30. Roei Tell et al. Quantified derandomization: How to find water in the ocean. *Foundations and Trends® in Theoretical Computer Science*, 15(1):1–125, 2022. 2
31. R Titsworth. Coherent detection by quasi-orthogonal square-wave pulse functions (corresp.). *IRE Transactions on Information Theory*, 6(3):410–411, 1960. 4, 13, 15, 16, 17, 40

32. Joseph L Walsh. A closed set of normal orthogonal functions. *American Journal of Mathematics*, 45(1):5–24, 1923. 4

Supporting Materials.

A Solving Simultaneous Diophantine Equations

Figure 3 presents our algorithm. In this section, the "LLL algorithm" refers to the algorithm with the following guarantees.

Imported Theorem 2 (LLL [17, Proposition 1.39]) *There exists a polynomial-time algorithm that, given a positive integer d and rational numbers $r_1, r_2, \ldots, r_d, \varepsilon$ satisfying $0 < \varepsilon < 1$, finds integers $s_1, s_2, \ldots, s_d$, and t for which*

$$|s_i - t \cdot r_i| \leqslant \varepsilon,$$

for $1 \leqslant i \leqslant d$ and $1 \leqslant t \leqslant 2^{d(d+1)/4} \cdot \varepsilon^{-d}$.

Input. $\alpha_1, \alpha_2 \in F^*$, where F is the prime field of order p

Output. Elements $u, v \in F^*$ such that $(u, v) \in [\alpha_1 : \alpha_2]$ and

$$u, v \in \{-B, -(B-1), \ldots, 0, 1, \ldots, (B-1), B\} \mod p,$$

where $B := \left\lceil 2^{3/4} \cdot \sqrt{p} \right\rceil$.

Algorithm.

1. Interpret $\alpha_1, \alpha_2 \in \{0, 1, \ldots, p-1\}$ as positive integers
2. Define $d = 2$
3. Define $r_1 = \alpha_1/p \in \mathbb{Q}$ and $r_2 = \alpha_2/p \in \mathbb{Q}$
4. Define $\varepsilon = B/p \in \mathbb{Q}$
5. Use the LLL algorithm to find integers s_1, s_2, and t
6. Interpret t as an element of F. Define $u = \alpha \cdot t \in F$ and $v = \alpha \cdot t \in F$

Fig. 3. Our Algorithm to obtain (u, v) from (α_1, α_2) using the LLL-algorithm.

Let us proceed to analyze our algorithm of Figure 3. The parameter setting needs to ensure that $t \leqslant 2^{d(d+1)/4}\varepsilon^{-d} < p$. Recall that $\varepsilon = B/p$. Substituting this value and rearranging, one needs to ensure that $2^{d(d+1)/4} \cdot p^{d-1} < B$. Therefore we have chosen $B = \left\lceil 2^{(d+1)/4} p^{1-1/4} \right\rceil$. Consequently, one can interpret t as an F^* element.

By definition, $(u, v) \in [\alpha_1 : \alpha_2]$ because $u = t \cdot \alpha_1$ and $v = t \cdot \alpha_2$. Next, note that

$$|\alpha_1 \cdot t - s_1 \cdot p| \leqslant \varepsilon \cdot p = B, \text{ and } |\alpha_2 \cdot t - s_2 \cdot p| \leqslant \varepsilon \cdot p = B.$$

This argument completes the analysis that for every (α_1, α_2) how we obtain $(u, v) \in [\alpha_1 : \alpha_2]$ such that u and v are "small (positive/negative) numbers."

B Properties of $I^{(0)}_{k,\ell}$ identified in [31, 12]

This section contains results that were already known in the literature. For relatively prime $k, \ell \in \{1, 2, \dots\}$,

$$I^{(0)}_{k,\ell} = \begin{cases} 0 & \text{if } k \cdot \ell \text{ is even} \\ \frac{1}{k\ell} & \text{if } k \cdot \ell \text{ is odd} \end{cases}.$$

We prove these results for completeness (and as a warmup). The results in Supporting Material 4.1 generalize the results in this section. Readers can skip this section and directly go to Supporting Material 4.1.

Lemma 15 ([31, 12]). *For relatively prime $k, \ell \in \{1, 2, \dots\}$ such that $k \cdot \ell$ is even, $I^{(0)}_{k,\ell} = 0$.*

Proof. Without loss of generality, assume that k is even and ℓ is odd.

$$\begin{aligned} I^{(0)}_{k,\ell} &= \int_0^1 \varphi(kt) \cdot \varphi(\ell t)\, \mathrm{d}t \\ &= \frac{16}{\pi^2} \sum_{\text{odd } n>0} \sum_{\text{odd } m>0} \frac{1}{mn} \int_0^1 \sin(2n\pi \cdot kt) \sin(2m\pi \cdot \ell t)\, \mathrm{d}t \end{aligned}$$

(By Equation 2)

Note that nk is even, but $m\ell$ is odd. So, $nk \neq m\ell$, for all odd m, n. Therefore, for any odd m, n, the integral

$$\int_0^1 \sin(2n\pi \cdot kt) \sin(2m\pi \cdot \ell t)\, \mathrm{d}t = 0,$$

by Proposition 3. So, $I^{(0)}_{k,\ell} = 0$. □

Lemma 16 ([31, 12]). *For relatively prime $k, \ell \in \{1, 2, \dots\}$ such that $k \cdot \ell$ is odd, $I^{(0)}_{k,\ell} = \frac{1}{k\ell}$.*

Proof. We begin as in the previous proof.

$$\begin{aligned} I^{(0)}_{k,\ell} &= \int_0^1 \varphi(kt) \cdot \varphi(\ell t)\, \mathrm{d}t \\ &= \frac{16}{\pi^2} \sum_{\text{odd } n>0} \sum_{\text{odd } m>0} \frac{1}{mn} \int_0^1 \sin(2n\pi \cdot kt) \sin(2m\pi \cdot \ell t)\, \mathrm{d}t \end{aligned}$$

(By Equation 2)

Since, $\gcd(k, \ell) = 1$, note that $nk = m\ell$ if and only if

$$(n, m) \in J := \left\{ (\ell, k), (3\ell, 3k), (5\ell, 5k), \dots \right\}.$$

With this observation and Proposition 3, we get

$$\begin{aligned}
I^{(0)}_{k,\ell} &= \frac{16}{\pi^2} \sum_{(n,m)\in J} \frac{1}{mn} \int_0^1 \sin(2n\pi \cdot kt) \sin(2m\pi \cdot \ell t)\, \mathrm{d}t \\
&= \frac{16}{\pi^2} \sum_{\text{odd } a>0} \frac{1}{k\ell \cdot a^2} \int_0^1 \sin(2k\ell a\pi \cdot t) \sin(2k\ell a\pi \cdot t)\, \mathrm{d}t \\
&= \frac{16}{\pi^2} \cdot \frac{1}{k\ell} \sum_{\text{odd } a>0} \frac{1}{a^2} \cdot \frac{1}{2} && \text{(By Proposition 3)} \\
&= \frac{1}{k\ell} \cdot \frac{\cancel{8}}{\cancel{\pi^2}} \cdot \frac{\cancel{\pi^2}}{\cancel{8}} = \frac{1}{k\ell} && \text{(Because } \sum_{\text{odd } a>0} \tfrac{1}{a^2} = \tfrac{3}{4} \cdot \zeta(2) = \tfrac{\pi^2}{8}\text{)}
\end{aligned}$$

This derivation completes the proof of our lemma. □

C Example of Secure Evaluation places against Physical Bit Leakage

We consider $\mathsf{ShamirSS}(n = 2, k = 2, (\alpha_1, \alpha_2))$ over the prime field F of order $p = 2^\lambda - 1$ – a Mersenne prime. We deduced earlier that the security of (α_1, α_2) is identical to the security of all (u, v) in the equivalence class $[\alpha_1 : \alpha_2]$. Note that $[\alpha_1 : \alpha_2]$ is identical to the equivalence class $[1 : \alpha]$, where $\alpha = \alpha_2\alpha_1^{-1}$. The equivalence class $[1 : \alpha]$ is secure if and only if all the following equivalence classes

$$\left\{[1 : \alpha], [1 : 2^1 \cdot \alpha], [1 : 2^2 \cdot \alpha], \ldots, [1 : 2^{\lambda-1} \cdot \alpha]\right\}$$

are secure against the LSB leakage.

The elements generated by 2, $\langle 2\rangle = \{1, 2, 2^2, \ldots, 2^{\lambda-1}\}$, is a cyclic subgroup of F^*. Let $\alpha \cdot \langle 2\rangle$ denote the coset $\{\alpha, 2 \cdot \alpha, \ldots, 2^{\lambda-1} \cdot \alpha\} \in F^*/\langle 2\rangle$. Furthermore, the equivalence class $[1 : \alpha]$ is secure against arbitrary physical bit leakage if (and only if) the equivalence classes $[1 : \alpha']$ are secure against arbitrary physical bit leakage, for all $\alpha' \in \alpha \cdot \langle 2\rangle$.

> So, in the table below, if we mention α, then it implies that any $(\alpha_1, \alpha_2) \in [1 : \alpha']$ is secure against physical bit leakage attacks, where $\alpha' \in \alpha\langle 2\rangle$.

Consider an example of secure evaluation places for Mersenne prime $p = 2^{13} - 1 = 8191$. The example evaluation places are secure even if the "adversarial LLL" algorithm in Section 7.5 is used.

For example, the element "95" in the table below represents the following. Any $(\alpha_1, \alpha_2) \in [1 : \alpha']$ is secure against physical bit leakage attacks, where $\alpha' \in 95\langle 2\rangle$. Note that

$$\begin{aligned}
95 \cdot \langle 2\rangle &= \{95, 2 \cdot 95, 2^2 \cdot 95, \ldots, 2^{12} \cdot 95\} \\
&= \{95, 190, 380, 760, 1520, 3040, 6080, 3969, 7938, 7685, 7179, 6167, 4143\}
\end{aligned}$$

95	97	99	101	103	107	111	113	119	121	123
125	131	133	135	137	139	143	145	147	151	153
155	157	159	161	163	165	169	173	175	179	181
183	185	187	191	197	201	203	207	209	211	213
215	217	219	221	223	225	227	229	231	233	235
237	239	243	245	247	249	251	253	267	269	271
275	277	279	281	285	287	291	293	295	297	299
303	305	309	313	317	319	323	325	329	331	333
335	337	339	349	351	355	357	359	361	363	365
369	371	373	375	377	379	391	393	395	397	399
401	403	405	407	411	413	415	419	423	427	429
433	435	437	441	443	445	447	453	457	459	461
465	467	469	471	473	475	477	487	491	493	495
497	499	501	503	505	549	551	553	555	557	559
563	567	569	573	575	581	583	587	589	591	595
599	601	603	607	611	613	615	617	619	621	623
629	633	637	651	653	655	661	667	669	671	675
677	679	687	693	695	697	699	701	713	715	717
719	725	727	729	731	735	739	743	747	751	755
757	759	761	763	795	797	799	805	807	811	813
815	821	823	825	829	843	845	847	855	857	859
863	869	871	873	875	877	879	883	885	887	889
891	893	915	917	921	923	925	927	933	937	939
943	947	949	951	953	955	957	959	971	973	975
979	987	989	991	997	1001	1005	1007	1011	1175	1181
1183	1191	1197	1199	1205	1207	1211	1213	1227	1231	1235
1237	1239	1245	1247	1253	1255	1259	1261	1263	1267	1275
1323	1327	1333	1335	1339	1341	1343	1355	1357	1359	1371
1373	1375	1387	1389	1395	1397	1403	1405	1431	1435	1439
1447	1451	1461	1467	1469	1485	1487	1491	1495	1499	1501
1503	1511	1515	1519	1525	1655	1661	1691	1693	1695	1703
1709	1711	1717	1723	1725	1727	1743	1751	1757	1759	1773
1775	1783	1787	1851	1853	1855	1871	1879	1885	1887	1899
1901	1903	1909	1915	1963	1965	1967	1973	1975	1979	1981
1983	2007	2011	2013	2015	2775	2783	2795	2799	2807	2911
2927	2935	2939	2991	2999	3003	3035	3039	3055	3551	3575

Table 1. Secure Evaluation Places against Physical Bit Leakage when $p = 2^{13} - 1$. If an element $\alpha \in F$ appears in the list above, it implies the following. Any evaluation places $(\alpha_1, \alpha_2) \in [1 : \alpha']$, where $\alpha' \in \alpha \cdot \langle 2 \rangle$, is secure against all physical bit leakage attacks.