Leakage-resilience of Shamir's Secret-sharing: Derandomization Challenges

Abstract

Can Shamir's secret-sharing protect its secret when all shares are partially compromised? Guruswami and Wootters (STOC 2016, IEEE Trans. Inf. Theory 2017) reconstructed the secret from such leakage. For other leakage families, randomly choosing evaluation places decouples the leakage from the secret; these constructions, however, are vulnerable to adversarially set randomness. This work initiates the investigation of derandomization objectives arising from this context.

We aim to identify leakage-resilient modulus and evaluation places that ensure the independence of the leakage from the secret. This work considers the family of bit-probing attacks on the shares, which are known to reveal partial information about the secret in specific cases. Although most evaluation places are leakage-resilient, no algorithm is known to find them. With this background, our work introduces the following technical innovations.

1. An algorithm to efficiently identify leakage-resilient and vulnerable evaluation places against an attack that probes every share's least significant bit (LSB).
2. A modulus choice for which protection against the LSB attack ensures protection from arbitrary physical bit leakage.

Building on these, we characterize modulus and evaluation places that make Shamir's secret-sharing resilient to physical bit leakage – the first derandomization of Monte-Carlo constructions. We discover new attacks on vulnerable evaluation places to complement these results.

To prove these results, our work introduces new techniques to analyze the security of secret-sharing schemes. It connects their leakage resilience to the orthogonality/independence properties of a system of square wave functions. The accuracy of this connection depends on finding good simultaneous rational approximations – a Dirichlet-type approximation problem efficiently solved using the LLL algorithm. In the context of security analysis of secret-sharing schemes, these techniques are new and possibly of broader interest.

Keywords: Shamir secret-sharing, leakage resilience, derandomization, physical bit leakage, secure evaluation places, secure modulus choice, square wave families, Fourier analysis.

Contents

1 Introduction

Shamir's secret-sharing [54] underlies nearly all threshold privacy and cryptography technologies [4]. This scheme distributes a secret among several parties so that any k could reconstruct the secret. It chooses a random polynomial of degree $< k$ whose Y-intercept is the secret, and the shares are the evaluation of this polynomial at different places. Any collection of $< k$ shares reveals no information about the secret, keeping it secure. Starting with the works of Kocher et al. [33, 34, 12], side-channel attacks have repetitively circumvented such "all-or-nothing" corruption models and compromised cryptosystems by accumulating leakage from all its components. For instance, using small leakage per share, the exact repair algorithm for Reed-Solomon codewords by Guruswami and Wootters [24, 25] can reconstruct Shamir secret-sharing's secret. Characterizing the security of Shamir's scheme against various leakage attacks has become even more compelling due to ongoing NIST standardization efforts [10].

One such security metric, namely, *local leakage resilience*, introduced by Benhamouda et al. [5, 6] & Goyal and Kumar [23], requires the statistical independence of the leakage from the secret. In this sense, leakage resilience and code repair objectives are strongly antithetical. Guaranteeing leakage resilience has been challenging – even against (seemingly) innocuous attacks that *probe physical bits* in the memory storing the shares. Surprisingly, *leakage resilience hinges on the evaluation places that generate the shares.* For example, leaking only the *least significant bit* (LSB) of each share reveals information about the secret for specific evaluation places [40, 1, 42].

On the other hand, Shamir's scheme with randomly chosen evaluation places is locally leakage-resilient against arbitrary physical probes with high probability [40]. However, this randomized construction is susceptible to adversarially set randomness because no algorithm is known to determine the leakage-resilience of Shamir's scheme, given its evaluation places. With this background, more generally, for arbitrary leakage family, a natural "searching-hay-in-haystack" derandomization question arises:

Which evaluation places result in locally leakage-resilient Shamir's secret-sharing?

1.1 A Toy Example: New Vulnerability for LSB Leakage

This section highlights a *new form of vulnerability* in Shamir's secret-sharing identified by our work, which will illustrate one of the critical technical ideas underlying our derandomization results.

Observation 1. Consider Shamir's secret-sharing scheme among $n = 2$ parties and threshold $k = 2$ over the prime field F_p, where $p \geqslant 5$. To share the secret $s = 0$, choose a polynomial $P(X) := P_1 \cdot X$ for uniformly random $P_1 \in F_p$. Suppose the first share is the evaluation $s_1 := P(X = 1)$, and the second is $s_2 := P(X = 3)$. The two shares are elements of the following set:

$$(s_1, s_2) \in \Big\{ \ (P_1, 3 \cdot P_1) \ : P_1 \in F_p \Big\}.$$

The LSB attack leaks each share's *parity*. For example, a share in the set $\{0, 2, 4, \ldots, (p-1)\}$ has "even" parity, while a share in the set $\{1, 3, \ldots, (p-2)\}$ has "odd" parity. We aim to calculate the probability that the parity of s_1 differs from that of s_2. There are *two exhaustive cases*:

A: $\underline{s_1 = 2 \cdot x, \text{ where } x \in \mathbb{Z} \cap [p/6, 2p/6]}$: The parity of s_1 is even, and the parity of $s_2 = 3 \cdot s_1 = 6 \cdot x$ is odd (because of one " mod p" wraparound).

B: $\underline{s_1 = 2 \cdot x, \text{ where } x \in \mathbb{Z} \cap [4p/6, 5p/6]}$: The parity of s_1 is odd (because of one " mod p" wraparound), and $s_2 = 6 \cdot x$ is even (because of four " mod p" wraparounds).

Therefore, the probability of the parity of s_1 and s_2 being different is (roughly) $1/3$.

Observation 2. Next, secret-share a uniformly random secret $s \in F_p$. The two shares are:

$$(s_1, s_2) = (s + P_1, s + 3 \cdot P_1),$$

where $s, P_1 \in F_p$ are uniformly and independently random. Therefore, the probability of the parity of s_1 and s_2 being different is (roughly) $1/2$ (because the two shares are also uniformly and independently distributed over F_p). By an averaging argument, there is a secret $s^* \in F_p^*$ such that the probability of the parity-of-shares-being-different is $\geqslant 1/2$. Our work presents an algorithm to efficiently compute s^*, which maximizes this distinguishing advantage.

Conclusion for toy example. These two observations show that the LSB leakage joint distribution is not independent of the secret; the secrets 0 and s^* are distinguishable with advantage $\geqslant 1/2 - 1/3 = 1/6$.

Questions & discussion. Suppose the shares are $s_1 := P(X = \alpha_1)$ and $s_2 := P(X = \alpha_2)$, where α_1, α_2 are distinct non-zero evaluation places in the prime field F_p of order p. The following natural question arises:

Is the LSB *leakage for the pair of evaluation places* (α_1, α_2) *statistically independent of the secret?*

Nearly all evaluation places satisfy this condition [40]; however, no algorithm was known to identify them. In fact, not even one such (α_1, α_2) was known.

Evaluation places are vulnerable if the leakage is *not independent* of the secret. Before our work, the only known vulnerable evaluation places satisfied $\alpha_1 \cdot \alpha_2^{-1} = -1$ [40, 1, 42]. The vulnerability of our toy example extends to all $\alpha_1 \cdot \alpha_2^{-1} \in \{\pm 3, \pm 3^{-1}\}$ using properties of generalized Reed-Solomon codes [27]. *Are there additional vulnerable evaluation places* (α_1, α_2)*? Can we find all of them?*

Sneak peek into our LSB **derandomization.** Roughly, our security characterization against LSB leakage is the following.

Input. Distinct non-zero evaluation places (α_1, α_2) and a prime modulus p

1. Find $u, v \in \{-\lceil\sqrt{p}\rceil, \ldots, 0, 1, \ldots, \lceil\sqrt{p}\rceil\}$ such that $\alpha_1 \cdot \alpha_2^{-1} = u \cdot v^{-1}$ (in this step, interpret u, v as elements of F_p)
2. Compute $g := \gcd(\,|u|, |v|\,)$ (in this step, interpret u, v as elements of $\mathbb{Z}$)
3. Compute $\rho := \left|u \cdot v / g^2\right|$ (in this step, interpret u, v, g as elements of $\mathbb{Z}$)
4. Define
$$\varepsilon := \begin{cases} 0, & \text{if } \rho \text{ is even} \\ \frac{1}{2\rho}, & \text{if } \rho \text{ is odd.} \end{cases}$$
5. If $\varepsilon = 0$, Shamir's scheme with evaluation places (α_1, α_2) is resilient to LSB leakage. Otherwise, there is an efficiently computable secret $s \in F_p^*$ such that the LSB leakage can distinguish secret 0 from secret s with advantage (roughly) ε.

Our toy example has $u = \alpha_1 = 1$, $v = \alpha_2 = 3$, and $\rho = 1/6$. To conclude, for even ρ, the LSB leakage is independent of the secret; otherwise, there is an LSB leakage attack with a distinguishing advantage of $1/2\rho$. Appendix G lists secure evaluation places using our derandomization algorithm against all physical bit probes (not just the LSB attack); the remaining are vulnerable.

Remark 1. *A few comments regarding our analysis techniques leading to this derandomization algorithm:*

1. *Step 1 in the algorithm above is a Dirichlet approximation problem. We solve it with a small constant multiplicative slack using the LLL [38] algorithm in* $\mathsf{poly}(\lambda)$ *run-time (Appendix A has the details).*

2. *Step 4 is (the closed-form expression of) the similarity/correlation measure between two* square waves*: (a) one that oscillates* $|u|$ *times in the interval* $[0,1]$ *and (b) another that oscillates* $|v|$ *times in the same interval. Refer to Section 3.2 for the definition of relevant functions, and Lemma 5 for the value of the similarity (in Section 4.4). We improve the distinguishing advantage from* $1/2\rho$ *to* $\cos^2(\pi/2p)/\rho \in [3/4\rho, 1/\rho)$ *(refer to Theorem 1 for details).*

3. *In our work, we connect the security of secret-sharing schemes against leakage attacks with the properties of a family of square waves; see, for example, [58, 29, 28]. Various families of square waves like the ones by Haar [26], Walsh [60], and Rademacher [49] are central to science and engineering.*

1.2 Basic Definitions & Our Problem Statement

Shamir's secret-sharing scheme. Shamir's secret-sharing scheme among n parties with reconstruction threshold k over a finite field F and distinct evaluation places $\alpha_1, \alpha_2, \ldots, \alpha_n \in F^*$ proceeds as follows. To share a secret $s \in F$, sample a random F-polynomial $P(X)$ such that $\deg P < k$ and $P(0) = s$. Define the shares: $s_1 := P(\alpha_1)$, $s_2 := P(\alpha_2)$, $\ldots$, and $s_n := P(\alpha_n)$. Denote this secret-sharing by $\mathsf{ShamirSS}(n, k, \vec{\alpha})$ and the joint distribution of the shares by $\mathsf{Share}(s)$ – other parameters will be clear from the context.

Representing finite field elements. Consider a prime field F_p of order p, where $2^{\lambda-1} < p < 2^\lambda$ and λ is the security parameter. The elements of F_p are represented as λ-bit binary strings representing the elements $\{0, 1, \ldots, (p-1)\}$.

Leakage functions & families. This work studies *physical bit leakage* $\mathrm{PHYS}_i \colon F \to \{0,1\}$ that outputs the i-th least significant bit, where $i \in \{0, 1, \ldots, \lambda-1\}$. For example, PHYS_0 (also referred to as LSB) outputs 0 for the elements in $\{0, 2, \ldots, (p-1)\}$, where $p \geqslant 3$, and PHYS_1 outputs 0 for the elements in $\{0, 1, 4, 5, \ldots\}$. The *leakage function* $\vec{\mathrm{PHYS}}_{i_1,i_2,\ldots,i_n} \colon F^n \to \{0,1\}^n$ leaks the i_t-th bit of the t-th share, where $t \in \{1, 2, \ldots, n\}$ and $i_1, i_2, \ldots, i_n \in \{0, 1, \ldots, \lambda-1\}$. For a secret $s \in F$, the joint distribution of the leakage is $\vec{\mathrm{PHYS}}_{i_1,i_2,\ldots,i_n}(\mathsf{Share}(s))$. We consider two *leakage families*.

1. Physical bit leakage family: $\mathrm{PHYS} := \left\{ \vec{\mathrm{PHYS}}_{i_1,i_2,\ldots,i_n} \ : \ i_1, i_2, \ldots, i_n \in \{0, 1, \ldots, \lambda-1\} \right\}$.

2. LSB leakage family: $\mathrm{LSB} := \left\{ \vec{\mathrm{PHYS}}_{0,0,\ldots,0} \right\}$.

Insecurity & randomized construction. *Insecurity* of $\mathsf{ShamirSS}(n, k, \vec{\alpha})$ against a leakage family $\mathcal{F}$ is:

$$\varepsilon_{\mathcal{F}}(\vec{\alpha}) := \max_{s \in F^*, f \in \mathcal{F}} \mathsf{SD}\left(f(\mathsf{Share}(0)) \ , \ f(\mathsf{Share}(s)) \right). \tag{1}$$

Small insecurity implies the statistical independence of the leakage from the secret, i.e., the *secret-sharing is locally leakage-resilient* [5, 23].

High insecurity implies that a leakage function can distinguish the secret 0 and some $s \in F^*$ using the leakage. Maji et al. [40] analyzed the insecurity against the PHYS leakage family when evaluation places are chosen at random. Their result implies the following corollary for $k = 2$ and prime modulus $p \geqslant 3$.

Randomized Construction of Maji et al. [40]

For randomly chosen evaluation places $\vec{\alpha} \in \left(F_p^*\right)^n$, the insecurity $\varepsilon_{\text{PHYS}}(\vec{\alpha}) \leqslant p^{-1/2}$ with probability $\geqslant 1 - p^{-1/2}$.

We initiate the derandomization of locally leakage-resilient construction of Shamir's secret-sharing over prime fields. This work investigates the security against the leakage family PHYS; i.e., the adversary obtains one physical bit leakage from each share.

Our Derandomization Objective

Given evaluation places $\vec{\alpha}$ and prime modulus p, identify whether (1) $\varepsilon_{\text{PHYS}}(\vec{\alpha}) \leqslant p^{-1/2}$ or (2) $\varepsilon_{\text{PHYS}}(\vec{\alpha}) > p^{-1/2}$.

If $\varepsilon_{\text{PHYS}}(\vec{\alpha}) > p^{-1/2}$, then output a secret $s \in F_p^*$ such that the shares of 0 can be distinguished from the shares of All algorithms should be computationally efficient – run-time polynomial in λ. Furthermore, concrete security analysis (instead of asymptotic analysis) is prioritized.

Summary of our results. We derandomize the randomized construction of Maji et al. [40] for (A) $(n, k) = (2, 2)$ and (B) $(n, k) = (3, 2)$ over Mersenne prime modulus, i.e., primes of the form $p = 2^\lambda - 1$ [59]. Given evaluation places $\vec{\alpha}$, we present an algorithm to classify them as either secure (in which case, the insecurity is $\leqslant p^{-1/2}$) or insecure (in which case, the insecurity is $> p^{-1/2}$. For the insecure evaluation places, we demonstrate an efficient distinguishing attack. We also present explicit evaluation places that are secure. Finally, we lift the security of the $(n, k) = (2, 2)$ case to the leakage resilience of the general $n = k > 2$ case.

1.3 Our Results

This section presents our results for the (A) $(n, k) = (2, 2)$, (B) $(n, k) = (3, 2)$, and (C) $n = k > 2$ cases. We aim to efficiently identify secure evaluation places (i.e., ones with low insecurity as per Equation 1) and demonstrate efficient attacks on vulnerable evaluation places (i.e., ones with high insecurity). Below, for $x, y, z \in \mathbb{R}$, the expression $x = y \pm z$ is a succinct representation for $x \in [y - z, y + z]$. For example, "x is close to y," is represented by $x = y \pm \varepsilon$, for a small ε.

1.3.1 Result 1: Security against Physical Bit Leakage when $(n, k) = (2, 2)$.

For the $n = k = 2$ case, we analyze field F_p, where p is a Mersenne prime – a prime of the form $2^\lambda - 1$. We reduced arbitrary physical bit leakage to LSB leakage for related evaluation places over these fields. In this context, our work proves the following results.

1. Corollary 4: Given evaluation places $\vec{\alpha} = (\alpha_1, \alpha_2)$ as input, we efficiently compute a closed-form estimate $\varepsilon^{(\text{OUR})}_{\text{PHYS}}(\vec{\alpha}) \in [0, 1]$ satisfying

$$\varepsilon^{(\text{OUR})}_{\text{PHYS}}(\vec{\alpha}) = \varepsilon_{\text{PHYS}}(\vec{\alpha}) \quad \pm \left(\frac{8^{5/4}}{\sqrt{p}} + \frac{13/2}{p} \right).$$

Intuitively, our estimation $\varepsilon^{(\text{OUR})}_{\text{PHYS}}(\vec{\alpha})$ is within an additive error of $\mathcal{O}\big(1/\sqrt{p}\big)$ of the actual insecurity $\varepsilon_{\text{PHYS}}(\vec{\alpha})$. The results below analyze this accurate estimation as a proxy for actual insecurity. If our estimate is small, then the evaluation places are secure – leakage cannot distinguish any pair of secrets. If our estimate is large, we present a leakage attack with a matching distinguishing advantage for two vulnerable secrets.

2. Corollary 5: Using our estimation, Figure 1 presents our efficient algorithm to classify $\vec{\alpha}$ as secure or not. If our algorithm classifies $\vec{\alpha}$ as secure, then

$$\varepsilon_{\text{PHYS}}(\vec{\alpha}) \leqslant \frac{1+8^{5/4}}{\sqrt{p}} + \frac{13/2}{p},$$

which is exponentially small in the security parameter λ. Among all possible distinct evaluation places, our algorithm classifies (at least)

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

fraction of them as secure. Appendix G enumerates all secure evaluation places for a small Mersenne prime $p = 2^{13}-1$ using our algorithm.

3. Corollary 6: Using our estimation technique, we present an efficient adversary that generates $(s, f) \in F^* \times \mathcal{F}$ such that it distinguishes the secret 0 from secret s by leaking f from the secret shares with an advantage

$$\geqslant \varepsilon_{\text{PHYS}}(\vec{\alpha}) - \frac{2\cdot 8^{5/4}}{\sqrt{p}} - \frac{13}{p}.$$

Intuitively, for vulnerable evaluation places $\vec{\alpha}$, we present an efficient leakage attack that achieves a comparable distinguishing advantage. For example, evaluation places $\vec{\alpha} = (1,2)$ and $\vec{\alpha} = (1,3)$ have insecurity (roughly) 1 and 1/3, respectively.[1]

4. Corollary 7: We identify explicit evaluation places that are secure against physical bit leakages. If evaluation places (α_1, α_2) satisfy $\alpha_2 \cdot \alpha_1^{-1} = 2^{\lfloor \lambda/2 \rfloor} - 1$, then

$$\varepsilon_{\text{PHYS}}(\vec{\alpha}) \leqslant \frac{4\cdot\big(2^{\lfloor\lambda/2\rfloor} + 2^{\lceil\lambda/2\rceil}\big) - 6}{p} = \mathcal{O}\bigg(\frac{1}{\sqrt{p}}\bigg).$$

The upper bound is meaningful (i.e., less than 1) for all $\lambda \geqslant 7$ (Mersenne prime $p \geqslant 127$).

Section 5 presents the corollary statements and their proofs (Section 5.3 to Section 5.6 state and prove Corollary 4 to Corollary 7, respectively).

1.3.2 Technical Result: Security against LSB Leakage when $(n,k) = (2,2)$.

Our results on physical bit leakage bootstrap from similar results against the LSB leakage. The results in this section hold for *any prime field* F_p, where $p \geqslant 3$, not just for Mersenne primes. We emphasize that the derandomization was not known earlier, even for the LSB leakage.

[1] Recall that in the toy example, the insecurity for the evaluation places $(1,3)$ was demonstrated to be $\geqslant 1/2 - 1/3 = 1/6$. We perform a more careful analysis to conclude that the insecurity is roughly $\cos^2(\pi/2p)/3 \to 1/3$, as $p \to \infty$.

1. Corollary 1: Given evaluation places $\vec{\alpha} = (\alpha_1, \alpha_2)$ as input, we efficiently compute a closed-form estimate $\varepsilon_{\text{LSB}}^{(\text{OUR})}(\vec{\alpha}) \in [0, 1]$ satisfying

$$\varepsilon_{\text{LSB}}^{(\text{OUR})}(\vec{\alpha}) = \varepsilon_{\text{LSB}}(\vec{\alpha}) \quad \pm \left(\frac{8^{5/4}}{\sqrt{p}} + \frac{13/2}{p} \right).$$

2. Corollary 2: Using the estimation above, Figure 2 presents an efficient algorithm to classify $\vec{\alpha}$ as secure or not. If our algorithm classifies $\vec{\alpha}$ as secure, then

$$\varepsilon_{\text{LSB}}(\vec{\alpha}) \leqslant \frac{1 + 8^{5/4}}{\sqrt{p}} \quad + \frac{13/2}{p},$$

   which is exponentially small in the security parameter λ. Among all possible distinct evaluation places, our algorithm classifies (at least)

$$1 \quad - \frac{\ln p}{4\sqrt{p}} - \frac{5/2}{\sqrt{p}}$$

   fraction of them as secure.

3. Corollary 3: Using our estimation technique, we present an efficient adversary that generates $s \in F^*$ such that it distinguishes the secret 0 from secret s by leaking the LSB of each secret share with an advantage

$$\geqslant \varepsilon_{\text{LSB}}(\vec{\alpha}) \quad - \frac{2 \cdot 8^{5/4}}{\sqrt{p}} - \frac{13}{p}$$

   Therefore, if the insecurity $\varepsilon_{\text{LSB}}(\vec{\alpha})$ is large, then our efficient leakage attack achieves a comparable distinguishing advantage.

   For example, evaluation places $\vec{\alpha} = (1, 2)$ and $\vec{\alpha} = (1, 3)$ have insecurity (roughly) 0 and $\geqslant \cos^2(\pi/2p) \cdot (1/3)$, respectively. Note that $\vec{\alpha} = (1, 2)$ is secure against LSB leakage but not against physical bit leakage. However, $\vec{\alpha} = (1, 3)$ is insecure against the LSB attack and, hence, against general physical bit leakage.

Section 4 presents the corollary statements and their proofs (Section 4.1 to Section 4.3 state and prove Corollary 1 to Corollary 3, respectively).

1.3.3 Result 2: Security against Physical Bit Leakage when $(n, k) = (3, 2)$.

Can we lift the secure evaluation places for $(n, k) = (2, 2)$ to the $(n, k) = (3, 2)$ case? For example, consider the following natural lifting technique: *When all evaluation pairs (α_i, α_j) are secure, is $\vec{\alpha}$ also secure?* It is unclear whether evaluation places (α_i, α_j) would retain their security in the presence of additional leakage from the remaining secret share. However, we prove the security of this lifting technique for $(n, k) = (3, 2)$.

For the $(n, k) = (3, 2)$ case, consider distinct evaluation places $(\alpha_1, \alpha_2, \alpha_3)$ satisfying the following property. Suppose the $\mathsf{ShamirSS}(2, 2, (\alpha_i, \alpha_j))$ secret sharing scheme has ε insecurity against physical bit leakages, for all distinct $i, j \in \{1, 2, 3\}$. Lemma 8 proves that the $\mathsf{ShamirSS}(3, 2, (\alpha_1, \alpha_2, \alpha_3))$ has (at most) 3ε insecurity against physical bit leakages.

The key technical contribution of this lifting theorem is the following result. The statistical distance between two leakage distributions has a "three-wise correlation term." We prove that

this correlation term is independent of the secret, even though $k = 2$ is less than the degree of the correlation, which is 3. This lifting technique does not extend for $n \in \{4, 5, \dots\}$ because the "four-wise correlation" (in general, any "even-wise correlation") is *not* independent of the secret.

For the converse, note that if there are insecure evaluation places (α_i, α_j), then the entire $\mathsf{ShamirSS}(3, 2, \vec{\alpha})$ is also vulnerable.

Table 2 in Appendix G presents secure evaluation places $(\alpha_1, \alpha_2, \alpha_3)$ when $\alpha_1 = 1$, $\alpha_2 = 95$. The exhaustive list (for arbitrary α_2) is too long to include in the paper.

1.3.4 Result 3: Security against Physical Bit Leakage when $n = k > 2$.

Consider a prime field F_p, such that $p = 2^\lambda - 1$. Corollary 8 presents an efficient (randomized) algorithm to choose evaluation places $\vec{\alpha}$ such that the corresponding $\mathsf{ShamirSS}(n, n, \vec{\alpha})$ is secure to physical bit leakages; the insecurity is at most $1/\sqrt{p}$. One can identify when this algorithm fails to choose secure $\vec{\alpha}$, and this failure probability is exponentially small in the security parameter λ. Using repeated sampling, the failure probability can be further reduced exponentially. Section 7 presents Theorem 2, which implies this corollary. Appendix E proves this theorem using Fourier analysis. Section 7.1 presents the proof of Corollary 8.

The proof strategy of this result is a lifting technique using the properties of generalized Reed-Solomon codes. Given evaluation places $\vec{\alpha} := (\alpha_1, \alpha_2, \dots, \alpha_n)$ we construct $\vec{\beta} := (\beta_1, \beta_2, \dots, \beta_n)$ using an efficiently computable linear map. We prove that if $\mathsf{ShamirSS}(2, 2, (\beta_1, \beta_2))$ has ε-insecurity against physical bit leakage, then $\mathsf{ShamirSS}(n, n, \vec{\alpha})$ has 2ε-insecurity against physical bit leakage. So, the following strategy suffices to construct secure schemes: (1) randomly sample $\vec{\alpha}$, (2) compute $\vec{\beta}$, and (3) test the security of $\mathsf{ShamirSS}(n, n, (\beta_1, \beta_2))$ using Corollary 5.

1.4 Open problems

Maji et al.'s randomized construction [40] holds for arbitrary $n \geqslant 2$, arbitrary prime fields, and $(c \cdot k\lambda/n)$ physical bit probes per share, for an appropriate constant $c \in (0, 1)$. The open questions below enumerate various dimensions of extending our derandomization results. These questions (and their combinations) are well-motivated derandomization problems and appear technically challenging.

Open Question 1 (Explicit Characterization)**.** *Explicitly characterize secure modulus and evaluation place choices.*

For $(n, k) = (2, 2)$, our work explicitly presents $(p - 1)$ of secure evaluation places for any Mersenne prime modulus p (see Corollary 7). These evaluation places are essentially all equivalent to each other. Can we find more explicit evaluation places? However, we could not explicitly find secure evaluation places for $(n, k) = (3, 2)$.[2] We could not identify any reasonable pattern from the exhaustive lists of secure evaluation places for a plausible conjecture. Explicitly finding more secure evaluation places for $(n, k) = (2, 2)$ could lead to explicit evaluation places for $(n, k) = (3, 2)$.

Open Question 2 (More Parties)**.** *Characterize the security of Shamir's secret-sharing scheme when the number of parties $n \in \{4, 5, \dots\}$.*

For the general $(n, k = 2)$ case, Maji et al. [40] proved that nearly all evaluation places are $p^{-1/2}$-insecure. Our techniques extend to prove a $p^{-\frac{1}{2\lceil n/2 \rceil}}$ insecurity bound, which is $\gg p^{-1/2}$, for

[2] Using the strategy of Corollary 7, we can find explicit evaluation places with $p^{-1/3}$ insecurity. However, our target is to achieve $p^{-1/2}$ insecurity, as indicated by the randomized construction of [40].

$n \in \{4, 5, \dots\}$. As n increases, the loss in estimation quality is due to an increase in the size of the "simultaneous rational approximations" problem; the parameter d in Appendix A. Circumventing this challenge will require new techniques for estimating the summation of oscillatory functions.

Open Question 3 (General Prime Fields)**.** *Characterize the security of Shamir's secret-sharing scheme for arbitrary prime fields.*

In this case, our reduction of physical bit leakage to LSB leakage breaks down. Directly derandomizing for arbitrary prime fields seems technically challenging. A more tractable pit-stop would be to extend to other specialized primes numbers like pseudo-Mersenne/Crandall [16] and generalized Mersenne/Solinas [55] primes. Their use is motivated by computational efficiency considerations in applications. For these cases, the authors believe that "approximate versions" of our reduction to LSB leakage should continue to hold, which is supported by numerical experiments. However, establishing this connection formally seems technically non-trivial.

Open Question 4 (More Leakage per Share)**.** *Characterize the security of Shamir's secret-sharing scheme for leakages that obtain (up to)* $\Theta(k\lambda/n)$ *bits per share.*

Consider an attack that leaks multiple physical bits per share. Even for the Mersenne prime modulus, one cannot convert arbitrary (multi-bit) physical bit leakage to an easy-to-analyze canonical attack. The analysis requires fine-grained characterization of the correlation between different physical bits of the same share, which will require new techniques.

Open Question 5 (Greater Threshold)**.** *Characterize the security of Shamir's secret-sharing scheme for threshold* $k \in \{3, 4, \dots\}$.

The randomized construction of Maji et al. [40] holds for arbitrary threshold k, the insecurity's dependence on k is (roughly) $p^{-k+3/2}$. For more general $k \in \{3, 4, \dots\}$, leakage resilience is connected to the correlation between higher-dimension analogs of lines (like hyperplanes in high dimensions). Estimating leakage resilience would be connected to higher dimensional integrals.

Open Question 6 (Other Leakage Functions)**.** *Characterize the security of Shamir's secret-sharing scheme against other local leakages, like Hamming-weight leakage.*

Hamming weight leakage reveals the number of ones in the binary representation of a share. The Hamming weight of a share can be estimated (using concentration bounds) by probing a few random positions and computing the fraction of those probes being 1. Resilience against the Hamming weight leakage is motivated by real threats: (1) algebraic side-channel attacks (beginning with the work of Renauld et al. [51]) and (2) recent attacks like Hertzbleed [61]. This leakage attack obtains $\log \lambda \ll \lambda$ bits of information per share, and the randomized construction of Maji et al. [40] also extends to this leakage function (estimated using $\Theta(\log \lambda)$ random probes per share). Determining the leakage resilience against this attack requires estimating the summation of a doubly exponential oscillatory function accurately (and efficiently), which seems technically challenging.

Achieving leakage resilience is turning out to be incredibly challenging; even randomized constructions are rare against most leakage families. For Shamir's secret-sharing, the only known randomized construction is against physical bit leakage [40]. However, characterizing leakage resilience is critical for threat assessment against side-channel attacks.

1.5 Organization of the Paper

1. Section 2 presents a high-level overview of our technical approach to these derandomization problems.

2. Section 3 presents the preliminaries and notations.

3. Section 4 states and proves our results pertaining to LSB leakage.

4. Section 5 states and proves our results for general physical bit leakages.

5. Section 6 presents our results for $(n, k) = (3, 2)$ case.

6. Section 7 lifts the $(n, k) = (2, 2)$ results to more general $n = k > 2$.

7. Section 8 summarizes the prior relevant works.

2 Technical Overview

This section outlines our technical approach for some representative results. At a high-level, for $(n, k) = (2, 2)$, our strategy is the following:

1. For Mersenne primes, we prove that

$$\varepsilon_{\text{PHYS}}(\ (\alpha_1, \alpha_2)\ ) = \max\left\{\ \varepsilon_{\text{LSB}}(\ (\alpha_1, \alpha_2)\ ),\ \varepsilon_{\text{PHYS}}(\ (2\alpha_1, \alpha_2)\ ),\ \ldots,\ \varepsilon_{\text{PHYS}}(\ (2^{\lambda-1}\alpha_1, \alpha_2)\ )\ \right\}.$$

2. For any odd prime p, we prove that $\varepsilon_{\text{LSB}}(\ (\alpha_1, \alpha_2)\ )$ can be determined using the algorithm in our toy problem in Section 1.1. We consider the lattice $\mathcal{C}^{(0)} \subseteq F^n$ of all shares of 0 and determine the correlation between the parity of s_1 and the parity of s_2. If the correlation is high, then the secret-sharing is vulnerable, and, if the correlation is low, then the secret-sharing is secure.

Our approach is the following for $(n, k) = (3, 2)$.

1. For evaluation places $(\alpha_1, \alpha_2, \alpha_3)$, we prove the following bound for security.

$$\varepsilon_{\text{PHYS}}(\ (\alpha_1, \alpha_2, \alpha_3)\ ) = \varepsilon_{\text{PHYS}}(\ (\alpha_1, \alpha_2)\ ) + \varepsilon_{\text{PHYS}}(\ (\alpha_2, \alpha_3)\ ) + \varepsilon_{\text{PHYS}}(\ (\alpha_3, \alpha_1)\ ).$$

   This result relies on a "three-wise correlation" between three square waves being independent of the secret.

2. The following complementary bound follows by considering the leakage from any two shares.

$$\varepsilon_{\text{PHYS}}(\ (\alpha_1, \alpha_2, \alpha_3)\ ) \geqslant \max\left\{\ \varepsilon_{\text{PHYS}}(\ (\alpha_1, \alpha_2)\ )\ ,\ \varepsilon_{\text{PHYS}}(\ (\alpha_2, \alpha_3)\ )\ ,\ \varepsilon_{\text{PHYS}}(\ (\alpha_3, \alpha_1)\ )\ \right\}.$$

For $n = k > 2$, given evaluation places $\vec{\alpha}$, we construct an $\vec{\beta}$ using an appropriate linear map. Using Fourier-analytic techniques, we prove that

$$\varepsilon_{\text{PHYS}}(\ (\alpha_1, \alpha_2)\ ) \leqslant 2 \cdot \varepsilon_{\text{PHYS}}(\ (\beta_1, \beta_2)\ ).$$

2.1 Result 1: Physical Bit Leakage $(n, k) = (2, 2)$

Suppose the evaluation places are $\vec{\alpha} = (\alpha_1, \alpha_2)$. Our objective is to *determine whether Shamir's secret-sharing scheme with these evaluation places is secure against all physical bit leakage attacks.*

For $i, j \in \{0, 1, \ldots, \lambda - 1\}$, consider the physcial bit leakage attack $\text{PH}\vec{\text{Y}}\text{S}_{i,j}$. This leakage attack leaks the i-th LSB of the secret share 1 and the j-th LSB of the secret share 2. We will refer the $\text{PH}\vec{\text{Y}}\text{S}_{0,0}$ leakage attack as the $\text{L}\vec{\text{S}}\text{B}$ attack. We prove that, for a Mersenne prime

$p = 2^\lambda - 1$, the security of $\mathsf{ShamirSS}(2, 2, \vec{\alpha})$ against the $\vec{\text{PHYS}}_{i,j}$ leakage is equivalent to the security of $\mathsf{ShamirSS}(2, 2, \vec{\alpha'})$ against the LSB attack, where $\alpha'_1 = 2^{-i}\alpha_1$ and $\alpha'_2 = 2^{-j}\alpha_2$ (see Lemma 7). Consequently, it suffices to test the security of the evaluation places $(2^{-i}\alpha_1, 2^{-j}\alpha_2)$ against the LSB attacks, for all $i, j \in \{0, 1, \ldots, \lambda - 1\}$.

For each i, j, the call to the "LSB security check subroutine" identifies evaluation places potentially vulnerable to the $\vec{\text{PHYS}}_{i,j}$ leakage attack. Using a naïve union bound, the total number of potentially vulnerable evaluation places would be proportional to λ^2. However, using properties of Shamir's secret-sharing scheme, one can improve upon this naïve estimate, which is a significant overestimation of the actual number of vulnerable evaluation places.

We use a "normalization result" to improve this bound. Properties of the generalized Reed Solomon codes imply that $\mathsf{ShamirSS}(n, k, \vec{\gamma})$ is identical to $\mathsf{ShamirSS}(n, k, \Lambda \cdot \vec{\gamma})$, for any $\Lambda \in F^*$, evaluation places $\vec{\gamma}$, and $n, k \in \{1, 2, \ldots\}$ (see Lemma 10 in Appendix B). Therefore, it suffices to test the security of the evaluation places $(2^t\alpha_1, \alpha_2)$ against the LSB attack, for all $t \in \{0, 1, \ldots, \lambda - 1\}$. As a result, only a linear number of calls are made to the LSB security testing algorithm instead of the naïve quadratic calls.

Figure 1 presents this pseudocode. The next section presents the pseudocode to determine security against the LSB attack.

Input. Distinct evaluation places $\alpha_1, \alpha_2 \in F_p^*$, and p is 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 $t \in \{0, 1, \ldots, \lambda - 1\}$ such that $2^t\alpha_1 = \alpha_2$: Return insecure
2. For $t \in \{0, 1, \ldots, \lambda - 1\}$:
   (a) Call the algorithm in Figure 2 with evaluation places $(2^t\alpha_1, \alpha_2)$
   (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.

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

Remark 2 (An Edge Case)**.** *The algorithm determining the security of Shamir's secret-sharing scheme to* LSB *attack requires the evaluation places to be distinct. Even though α_1 and α_2 are distinct, it may be the case that $2^t\alpha_1 = \alpha_2$, for some $t \in \{0, 1, \ldots, \lambda - 1\}$. So, the call to the "*LSB *security check subroutine" with argument $(2^t\alpha_1, \alpha_2)$ would be invalid. Lemma 6 proves that this edge case is insecure. This case captures why evaluation places $(1, 2)$ are insecure against physical bit leakage.*

2.2 Technical Result: LSB Leakage $(n, k) = (2, 2)$

Suppose the evaluation places are $\vec{\alpha} = (\alpha_1, \alpha_2)$. Our objective is to *determine whether these evaluation places are secure against the* LSB *attack*. The presentation below is for all prime fields F of order p such that $p \geqslant 3$ – not just for a Mersenne prime p.

Consider a secret $s \in F^*$. Our objective is to estimate the statistical distance between the joint leakage distributions when (a) the secret is 0 and (b) the secret is s. Using a combinatorial argument, we prove that the statistical distance is identical to the following expression (see Lemma 2) for an appropriate Δ.

$$\frac{1}{2p} \cdot \left| \Sigma^{(0)}_{\alpha_1,\alpha_2} - \Sigma^{(\Delta)}_{\alpha_1,\alpha_2} \right|,$$

where

$$\Sigma^{(\Delta)}_{k,\ell} := \sum_{T \in F} \mathrm{sign}_p(kT) \cdot \mathrm{sign}_p(\ell(T-\Delta))$$

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

The $s \mapsto \Delta$ mapping is an efficient linear automorphism over F.

Remark 3 (Intuition of the Expression)**.** *The elements $\{0, 1, \ldots, (p-1)/2\} \subseteq F_p$ are positive elements, and the remaining elements are negative. We are considering functions that are the "signs of lines." For example, $\mathrm{sign}_p(kX)$ is the sign of the line $Y = kX$ over the finite field, which is an oscillating function. Likewise, $\mathrm{sign}_p(\ell(X-\Delta))$ is the sign of the (shifted) line $Y = \ell(X-\Delta)$ over the finite field, another oscillating function. The expression $\Sigma^{(\Delta)}_{k,\ell}$ – the inner product of these two functions – measures the correlation between these two functions. Leakage resilience to* LSB *attacks is equivalent to this correlation being independent of the secret s and, in turn, the parameter Δ.*

The evaluation places $\vec{\alpha}$ are secure if (and only if) $\frac{1}{2p} \cdot \left| \Sigma^{(0)}_{\alpha_1,\alpha_2} - \Sigma^{(\Delta)}_{\alpha_1,\alpha_2} \right|$ is small for all $\Delta \in F^*$. To this end, we aim to estimate $\frac{1}{p} \cdot \Sigma^{(\Delta)}_{\alpha_1,\alpha_2}$, for all $\Delta \in F$. This expression is the sum of an oscillating function that appears challenging to estimate accurately.

Our technical solution's innovation is to estimate (1) a real extension of this function using integration and (2) establish a connection between the sum of the oscillating function and the integration. Toward the first sub-objective, the integral is defined as follows.

$$I^{(\delta)}_{k,\ell} := \int_0^1 \varphi(kt) \cdot \varphi(\ell(t-\delta))\, \mathrm{d}t$$

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

$$\mathrm{sign}(x) := \begin{cases} +1, & \text{if } x > 0 \\ 0, & \text{if } x = 0 \\ -1, & \text{if } x < 0. \end{cases}$$

The function $\varphi(kx)$ is a *square wave function* with period 1 for all $k \in \mathbb{Z}$. This function is the real extension of the "sign of lines" function $\mathrm{sign}_p(X)$ above (with a scaling factor). The connection is that $\mathrm{sign}_p(X) = \varphi(x)$, where $x = X/p$ and $X \in F^*$. The square wave family $\{\varphi(kx)\}_{k \in \{1,2,\ldots\}}$ have been studied in the literature [58, 29, 28]. However, only $I^{(0)}_{k.\ell}$ was determined. Our work presents a closed-form expression for $I^{(\delta)}_{k,\ell}$, for all $\delta \in [0,1]$ (see Lemma 5).

Now, the second sub-objective is to estimate $\frac{1}{p} \cdot \Sigma^{(\Delta)}_{k,\ell}$ using the integral $I^{(\delta)}_{k,\ell}$, where $\delta := \Delta/p$. The accuracy of estimating the sum of an oscillating function using its integral depends on how many times the function oscillates. The number of oscillations of the function $\mathrm{sign}_p(kX) \cdot \mathrm{sign}_p(\ell(X-\Delta))$

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 [37] 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 $B := \lceil 2^{3/4} \cdot \sqrt{p} \rceil$. For completeness, Figure 5 in Appendix 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

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

is proportional to $\left(|k|_p + |\ell|_p\right)/p$, where the "norm- $\mod p$" function is defined below.

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

The estimation error is $(|k|_p + |\ell|_p)/p$ and will drown the value of the integral for large $|k|_p + |\ell|_p$.

At this point, the "normalization result" from the previous section is useful. The security of $\mathsf{ShamirSS}(2, 2, \vec{\alpha})$ is identical to the security of $\mathsf{ShamirSS}(2, 2, \vec{\gamma})$, if $\vec{\gamma} = \Lambda \cdot \vec{\alpha}$ and $\Lambda \in F^*$. So, instead of estimating $\frac{1}{p} \cdot \Sigma^{(\Delta)}_{\alpha_1, \alpha_2}$, we estimate $\frac{1}{p} \cdot \Sigma^{(\Delta)}_{u,v}$, where $vu^{-1} = \alpha_2 \alpha_1^{-1}$ and $|u|_p, |v|_p$ are small. Dirichlet's approximation theorem [52, 53] ensures that there are u and v such that $|u|_p, |v|_p$ are at most $\sqrt{p}$. However, finding this (u, v) in $\mathsf{poly}(\lambda)$ run-time is challenging. We efficiently solve this problem with (a small) constant multiplicative slack using the LLL algorithm [38].

To conclude, given (α_1, α_2), we use the LLL algorithm to construct appropriate "small norm" (u, v). Next, we use the closed-form expressions for $I^{(0)}_{u,v}$ and $I^{(\delta)}_{u,v}$ to estimate $\frac{1}{2p}\left|\Sigma^{(0)}_{\alpha_1,\alpha_2} - \Sigma^{(\Delta)}_{\alpha_1,\alpha_2}\right|$, where $\delta = \Delta/p$. Finally, we maximize over $\Delta \in F^*$ and determine the insecurity of the evaluation places (α_1, α_2) against the LSB attack. We also present the closed-form expressions for the maximum value, which our decision algorithm directly uses. Figure 2 presents the pseudocode of this algorithm.

The insecurity is at most $(|u|_p + |v|_p)/p = \mathcal{O}\big(1/\sqrt{p}\big)$ for secure evaluation places, which is exponentially small in the security parameter. Our analysis identifies the concrete constants. Our

analysis is tight and, consequently, also identifies new leakage attacks for insecure evaluation places.

Remark 4 (Minor Subtlety)**.** *Observe that* $\text{sign}_p(0) = +1$ *but* $\text{sign}(0) = 0$*. Using careful accounting, we show that the impact of this disagreement is only* $\pm 1/p$ *in the overall insecurity estimation.*

2.3 Result 2: Physical Bit Leakage $(n, k) = (3, 2)$

Suppose the evaluation places are $\vec{\alpha} = (\alpha_1, \alpha_2, \alpha_3)$. Our objective is to determine whether these evaluation places are secure against all physical bit leakage attacks.

A necessary condition is that $\mathsf{ShamirSS}(2, 2, (\alpha_i, \alpha_j))$ must be secure, for distinct $i, j \in \{1, 2, 3\}$. Surprisingly, we prove that this condition is essentially sufficient. Technically, we shall prove that the "three-wise correlation" among the three leakage bits is statistically independent of the secret.

Using the triangle inequality, we prove that the statistical distance between the joint leakage distributions for (a) the secret 0 and (b) secret $s \in F^*$ is upper-bounded by the sum of four terms.

1. Three terms corresponding to
$$\frac{1}{2p}\left|\Sigma^{(0)}_{\alpha_i,\alpha_j} - \Sigma^{(\Delta_{i,j})}_{\alpha_i,\alpha_j}\right|,$$
for distinct $i, j \in \{1, 2, 3\}$ and appropriate $\Delta_{i,j}$ determined by a linear automorphism $s \mapsto \Delta_{i,j}$. These terms ensure that the leakage from any two secret shares is statistically independent of the secret.

2. The final term corresponds to
$$\frac{1}{2p}\left|\Sigma^{(0,0)}_{\alpha_1,\alpha_2,\alpha_3} - \Sigma^{(\Delta,\Delta')}_{\alpha_1,\alpha_2,\alpha_3}\right|,$$
where
$$\Sigma^{(\Delta,\Delta')}_{k,\ell,m} := \sum_{T \in F} \text{sign}_p(kT) \cdot \text{sign}_p(\ell(T - \Delta)) \cdot \text{sign}_p(m(T - \Delta'))$$
and the mappings $s \mapsto \Delta$ and $s \mapsto \Delta'$ are two linear automorphisms. This term captures the three-wise correlation between the leakage bits. We prove that the contribution of this term is $\pm\frac{1}{p}$, which is exponentially small in the security parameter.

What did we gain by proving that the three-wise correlation between the leakage bits is statistically independent of the secret? Without this independence property, we would be forced to estimate this expression using an integral. The error in this estimation would be proportional to $(|u|_p + |v|_p + |w|_p)/p$, where $(u, v, w) \in [\alpha_1 : \alpha_2 : \alpha_3]$. Using Dirichlet's approximation theorem [38], one can only ensure that $|u|_p, |v|_p, |w|_p \leqslant p^{2/3}$ simutaneously. Consequently, our estimation error will be of the order $p^{-1/3}$. Therefore, we would only be able to guarantee that insecurity is $\leqslant p^{-1/3}$. Note that currently, we are able to ensure that the insecurity is $\leqslant p^{-1/2} \ll p^{-1/3}$.

Remark 5 (Odd-wise Correlation)**.** *In general, the* $(2t + 1)$*-wise correlation terms contribute at most* $\pm\frac{t}{p}$ *to the statistical distance, where* $t \in \{0, 1, \dots\}$*.*

2.4 Result 3: Physical Bit Leakage $n = k > 2$

Our objective is to choose n distinct evaluation places $\alpha_1, \alpha_2, \ldots, \alpha_n \in F^*$ such that the corresponding $\mathsf{ShamirSS}(n, n, \vec{\alpha})$ is secure against physical bit leakage attacks. We prove a lifting theorem (Theorem 2) that proves the following result. Given, evaluation places $\vec{\alpha}$ we define new evaluation places (where $i \in \{1, 2, \ldots, n\}$):

$$\beta_i := \left(\alpha_i \prod_{j \neq i} (\alpha_i - \alpha_j) \right)^{-1}.$$

Now consider the $\mathsf{ShamirSS}(2, 2, (\beta_i, \beta_j))$ secret-sharing scheme for all distinct $i, j \in \{1, 2, \ldots, n\}$. If one of these secret-sharing schemes is secure against physical bit leakage, then the $\mathsf{ShamirSS}(n, n, \vec{\alpha})$ secret-sharing scheme is also secure. More concretely, if the insecurity of $\mathsf{ShamirSS}(2, 2, (\beta_i, \beta_j))$ is (at most) ε, for some distinct $i, j \in \{1, 2, \ldots, n\}$, then the $\mathsf{ShamirSS}(n, n, \vec{\alpha})$ secret-sharing scheme is (at most) 2ε insecure.

We already have an efficient algorithm to classify evaluation places of $\mathsf{ShamirSS}(2, 2, (\beta_i, \beta_j))$ as secure or not. We can use this algorithm to detect whether our chosen $\vec{\alpha}$ has such a secure (β_i, β_j) pair of evaluation places. The proof of this result is entirely Fourier-analytic, and it is presented in Appendix E.

3 Preliminaries

For real numbers $a \leqslant b$ 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 interval $[a - \varepsilon, a + \varepsilon]$. For ease of readability, we write $x = a \pm \varepsilon$ to indicate $x \in a \pm \varepsilon$.

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 $f \colon F \to \{0, 1\}$, define the set $f^{-1}(b) := \{x \in F \colon f(x) = b\}$, where $b \in \{0, 1\}$.

For a finite field F, parameter $n \in \{2, 3, \ldots\}$, and elements $\alpha_1, \alpha_2, \ldots, \alpha_n \in F$, define the following *equivalence class*

$$[\alpha_1 \colon \alpha_2 \colon \cdots \colon \alpha_n] := \{(\Lambda \cdot \alpha_1, \Lambda \cdot \alpha_2, \ldots, \Lambda \cdot \alpha_n) : \Lambda \in F^*\}$$

Appendix B shows that all elements in the same equivalence class have identical resilience/vulnerability to attacks.

3.1 Functions over Finite Fields

Let F be a prime field of order $p \geqslant 3$. This section defines some $F \to \mathbb{Z}$ functions.

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

$$\operatorname{sign}_p(X) := \begin{cases} +1, & \text{if } X \in \{0, 1, \ldots, (p-1)/2\} \mod p \\ -1, & \text{if } X \in \{-(p-1)/2, \ldots, -1\} \mod p. \end{cases} \tag{3}$$

We define the following quantity for $k, \ell, \Delta \in F$.

$$\Sigma_{k,\ell}^{(\Delta)} := \sum_{T \in F} \mathrm{sign}_p(kT) \cdot \mathrm{sign}_p(\ell(T - \Delta)). \tag{4}$$

Similarly, we define the following quantity for $k, \ell, m, \Delta, \Delta' \in F$.

$$\Sigma_{k,\ell,m}^{(\Delta,\Delta')} := \sum_{T \in F} \mathrm{sign}_p(kT) \cdot \mathrm{sign}_p(\ell(T - \Delta)) \cdot \mathrm{sign}_p(m(T - \Delta')). \tag{5}$$

We will require the following intermediate definitions for technical analysis: slight variations of the definitions above.

$$\widetilde{\mathrm{sign}}_p(X) := \begin{cases} +1, & \text{if } X \in \{1, \ldots, (p-1)/2\} \mod p \\ 0, & \text{if } X = 0 \mod p \\ -1, & \text{if } X \in \{-(p-1)/2, \ldots, -1\} \mod p. \end{cases} \tag{6}$$

$$\widetilde{\Sigma}_{k,\ell}^{(\Delta)} := \sum_{T \in F} \widetilde{\mathrm{sign}}_p(kT) \cdot \widetilde{\mathrm{sign}}_p(\ell(T - \Delta)) \tag{7}$$

$$\widetilde{\Sigma}_{k,\ell,m}^{(\Delta,\Delta')} := \sum_{T \in F} \widetilde{\mathrm{sign}}_p(kT) \cdot \widetilde{\mathrm{sign}}_p(\ell(T - \Delta)) \cdot \widetilde{\mathrm{sign}}_p(m(T - \Delta')). \tag{8}$$

3.2 Functions over Real Numbers

This section defines some $\mathbb{R} \to \mathbb{R}$ functions.

$$\mathrm{sign}(x) := \begin{cases} +1, & \text{if } x > 0 \\ 0, & \text{if } x = 0 \\ -1, & \text{if } x < 0. \end{cases} \tag{9}$$

$$\varphi(x) := \mathrm{sign}\sin(2\pi x) \tag{10}$$

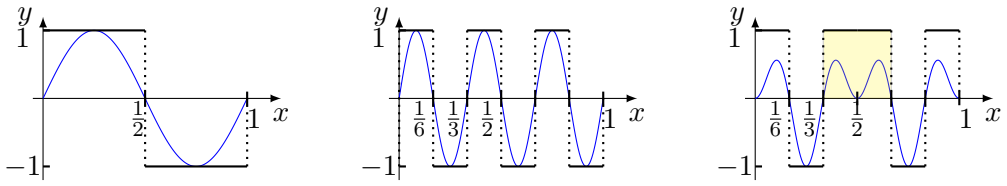
We define the following integral for $k, \ell \in \mathbb{Z}$ and $\delta \in \mathbb{R}$.

$$I_{k,\ell}^{(\delta)} := \int_0^1 \varphi(kt) \cdot \varphi(\ell(t - \delta))\, \mathrm{d}t. \tag{11}$$

Remark 6 (Intuition of the Square Waves)**.** *From standard Fourier analysis, it is well known that sine waves* $\sin(2\pi \cdot x)$ *and* $\sin(2\pi \cdot 3x)$ *are orthonormal, i.e.,* $\int_0^1 \sin(2\pi \cdot x) \cdot \sin(2\pi \cdot 3x)\, \mathrm{d}t = 0$*. However, the square waves* $\varphi(x) = \mathrm{sign}\sin(2\pi \cdot x)$ *and* $\varphi(3x) = \mathrm{sign}\sin(2\pi \cdot 3x)$ *are not orthogonal (see Figure 3). Surprisingly, the square wave* $\varphi(x)$ *and the shifted square wave* $\varphi(3(x - 1/12))$ *are orthogonal (see Figure 4). A technical objective of our work will be to determine the inner product* $I_{k,\ell}^{(\delta)}$ *between a square wave* $\varphi(kx)$ *and another shifted square wave* $\varphi(\ell(x - \delta))$*. For example, we have* $I_{1,3}^{(0)} = 1/3$ *and* $I_{1,3}^{(1/12)} = 0$*.*

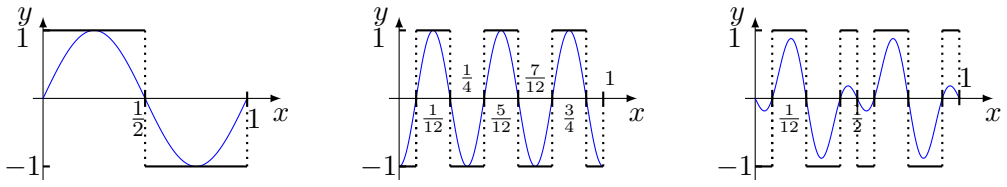
4 Security against Least Significant Bit Leakage

This section presents all results pertaining to the security of Shamir's secret-sharing scheme when $n = k = 2$. We begin with a powerful technical result that we prove.



$\varphi(x) = \operatorname{sign}\sin(2\pi x)$ $\varphi(3x) = \operatorname{sign}\sin(2\pi \cdot 3x)$ $\varphi(x) \cdot \varphi(3x)$

Figure 3: Square waves $\varphi(x) = \operatorname{sign}\sin(2\pi \cdot x)$ and $\varphi(3x) = \operatorname{sign}\sin(2\pi \cdot 3x)$ are not orthogonal since $\int_0^1 \varphi(t) \cdot \varphi(3t)\,\mathrm{d}t = 1/3$. Blue lines draw the functions without the $\operatorname{sign}(\cdot)$ function.



$\varphi(x) = \operatorname{sign}\sin(2\pi x)$ $\varphi(3(x-1/12))$ $\varphi(x) \cdot \varphi(3(x-1/12))$

Figure 4: Square waves $\varphi(x) = \operatorname{sign}\sin(2\pi \cdot x)$ and $\varphi(3(x-1/12)) = \operatorname{sign}\sin(2\pi \cdot 3(x-1/12))$ are orthogonal since $\int_0^1 \varphi(t) \cdot \varphi(3(t-1/12))\,\mathrm{d}t = 0$. Blue lines draw the functions without the $\operatorname{sign}(\cdot)$ function.

Theorem 1 (Technical Result)**.** *Consider the* $\mathsf{ShamirSS}(2, 2, (\alpha_1, \alpha_2))$ *secret-sharing scheme over a prime field* F_p*, where* $p \geqslant 3$*. For any* $(u, v) \in [\alpha_1 : \alpha_2]$*,*

$$\max_{s \in F} \mathsf{SD}\left(\mathrm{LSB}(\mathsf{Share}(0))\ ,\ \mathrm{LSB}(\mathsf{Share}(s))\right) = \begin{cases} \pm\frac{4(|u|_p+|v|_p)-(3/2)}{p}, & \text{if } |u|_p \cdot |v|_p/g^2 \text{ is even,} \\ \cos^2(\pi/2p) \cdot \frac{g^2}{|u|_p \cdot |v|_p} \pm \frac{4(|u|_p+|v|_p)-(3/2)}{p} & \text{if } |u|_p \cdot |v|_p/g^2 \text{ is odd,} \end{cases}$$

where $g = \gcd\left(|u|_p, |v|_p\right)$*. Furthermore, for* $s = \pm(u^{-1} \cdot v - 1)^{-1} \in F^*$*, if* $\mathsf{SD}\left(\mathrm{LSB}(\mathsf{Share}(0))\ ,\ \mathrm{LSB}(\mathsf{Share}(s))\right) > \frac{4(|u|_p+|v|_p)-(3/2)}{p}$*, then there is an efficient distinguisher to distinguish the secret 0 and* s *with advantage at least*

$$\cos^2(\pi/2p) \cdot \frac{g^2}{|u|_p \cdot |v|_p} - \frac{4(|u|_p + |v|_p) - (3/2)}{p}$$

using the LSB *leakage on the secret shares.*

Section 4.4 presents the proof outline for this result and Appendix C.6 presents the full proof. Using this theorem, we begin by stating and proving the corollaries mentioned in Section 1.3.

4.1 Statement and Proof of Corollary 1

Corollary 1. *Consider distinct evaluation places* $\vec{\alpha} = (\alpha_1, \alpha_2)$ *and the corresponding* $\mathsf{ShamirSS}(2, 2, \vec{\alpha})$ *secret-sharing scheme over the prime field* F_p*, where* $p \geqslant 3$*. Let* $(u, v) \in [\alpha_1 : \alpha_2]$ *such that*

$|u|_p, |v|_p \leqslant B$, *where* $B = \lceil 8^{1/4} \cdot \sqrt{p} \rceil$. *Let* $g = \gcd(|u|_p, |v|_p)$. *Define*

$$\varepsilon_{\mathrm{LSB}}^{(\mathrm{OUR})}(\vec{\alpha}) := \begin{cases} 0, & \text{if } |u|_p \cdot |v|_p / g^2 \text{ is even,} \\ \cos^2(\pi/2p) \cdot \frac{g^2}{|u|_p \cdot |v|_p}, & \text{if } |u|_p \cdot |v|_p / g^2 \text{ is odd.} \end{cases}$$

Then,

$$\varepsilon_{\mathrm{LSB}}^{(\mathrm{OUR})}(\vec{\alpha}) = \varepsilon_{\mathrm{LSB}}(\vec{\alpha}) \quad \pm \left(\frac{8^{5/4}}{\sqrt{p}} + \frac{13/2}{p} \right).$$

Proof. Use the LLL algorithm [38] to efficiently find $(u, v) \in [\alpha_1 : \alpha_2]$ with properties mentioned in the corollary (see Appendix A for details). Observe that the LHS of the expression in Theorem 1 is identical to $\varepsilon_{\mathrm{LSB}}(\vec{\alpha})$. From this observation, the corollary is immediate. □

4.2 Statement and Proof of Corollary 2

Corollary 2. *Consider distinct evaluation places* $\vec{\alpha} = (\alpha_1, \alpha_2)$ *and the corresponding* $\mathsf{ShamirSS}(2, 2, \vec{\alpha})$ *secret-sharing scheme over the prime field* F_p, *where* $p \geqslant 3$. *Suppose the algorithm in Figure 2 determines* $\vec{\alpha}$ *to be secure. Then,*

$$\varepsilon_{\mathrm{LSB}}(\vec{\alpha}) \leqslant \frac{1 + 8^{5/4}}{\sqrt{p}} + \frac{13/2}{p}.$$

Among all possible distinct evaluation places $\alpha_1, \alpha_2 \in F_p^*$, *the algorithm of Figure 2 determines at least*

$$\geqslant 1 \quad - \frac{\frac{1}{4} \cdot \sqrt{p} \cdot \ln p + \frac{3}{2} \cdot \sqrt{p} + \frac{1}{2}}{p - 2} \geqslant^{(*)} 1 \quad - \left(\frac{\ln p}{4\sqrt{p}} + \frac{5/2}{\sqrt{p}} \right).$$

fraction of them to be secure. The $(*)$ *inequality holds for any prime* $p \geqslant 11$.

Proof. **Proof of the first part.** The algorithm in Figure 2 declares $\vec{\alpha}$ to be secure either in Step 4 or Step 5.

Suppose our algorithm in Figure 2 declared that Shamir's secret-sharing scheme is secure in Step 4. In this case, $|u|_p \cdot |v|_p / g^2$ is even, where $g = \gcd(|u|_p, |v|_p)$. Using Corollary 1, we get that our estimation $\varepsilon_{\mathrm{LSB}}^{(\mathrm{OUR})} = 0$. The relation between our estimation and insecurity yields

$$\varepsilon_{\mathrm{LSB}}(\vec{\alpha}) \leqslant \frac{8^{5/4}}{\sqrt{p}} + \frac{13/2}{p}.$$

Suppose our algorithm in Figure 2 declared that Shamir's secret-sharing scheme is secure in Step 5. In this case, $|u|_p \cdot |v|_p / g^2 \geqslant \sqrt{p}$ and it is odd. Using Corollary 1, we get that our estimation $\varepsilon_{\mathrm{LSB}}^{(\mathrm{OUR})} \leqslant 1/\sqrt{p}$. The relation between our estimate and insecurity yields

$$\varepsilon_{\mathrm{LSB}}(\vec{\alpha}) \leqslant \frac{1}{\sqrt{p}} + \frac{8^{5/4}}{\sqrt{p}} + \frac{13/2}{p}.$$

This completes the proof of the first part of the corollary.

Proof of the second part. We prove that our algorithm outputs "may be insecure" only for an exponentially small fraction of the equivalence classes $[\alpha_1 : \alpha_2]$, for distinct evaluation places $\alpha_1, \alpha_2 \in F_p^*$.

First, observe that there are $(p-2)$ equivalence classes $[1\colon 2]$, $[1\colon 3]$, $\ldots$, $[1\colon (p-1)]$ (because $\alpha_1 \neq \alpha_2$ and $0 \notin \{\alpha_1, \alpha_2\}$).

Next, let us account for the instances when Figure 2 determines evaluation places $\vec{\alpha}$ may be insecure. Suppose $a = (u/g)$ and $b = (v/g)$, where $g = \gcd(u, v) \in \{1, 2, \ldots\}$. We need to upper bound the cardinality of the following set

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

In this set, for any particular a, the corresponding 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

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

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 $\leqslant \mathsf{card}(S)/2$. The fraction of equivalence classes that our algorithm declares "may be insecure" is

$$\leqslant \frac{\mathsf{card}(S)/2}{p-2} \leqslant \frac{\frac{1}{4} \cdot \sqrt{p} \cdot \ln p + \frac{3}{2} \cdot \sqrt{p} + \frac{1}{2}}{p-2}.$$

Asymptotically, the upper bound is $\lesssim \frac{1}{4} \cdot \frac{\ln p}{\sqrt{p}}$. Concretely, Appendix C.7 proves the upper bound

$$\leqslant \frac{\ln p}{4\sqrt{p}} + \frac{5/2}{\sqrt{p}},$$

for all $p \geqslant 11$. □

4.3 Statement and Proof of Corollary 3

Corollary 3. *Consider distinct evaluation places $\vec{\alpha} = (\alpha_1, \alpha_2)$ and the corresponding $\mathsf{ShamirSS}(2, 2, \vec{\alpha})$ secret-sharing scheme over the prime field F_p, where $p \geqslant 3$. If $\varepsilon_{\mathrm{LSB}}(\vec{\alpha}) > \frac{2 \cdot 8^{5/4}}{\sqrt{p}} + \frac{13}{p}$, then there is an efficient algorithm that generates $s \in F_p^*$ and can distinguish the secret 0 from the secret s with an advantage*

$$\geqslant \varepsilon_{\mathrm{LSB}}(\vec{\alpha}) \quad - \frac{2 \cdot 8^{5/4}}{\sqrt{p}} - \frac{13}{p}$$

by leaking the LSB *of the secret shares.*

Proof. Our efficient adversary outputs the s indicated in Theorem 1. After observing the leakage (ℓ_1, ℓ_2), this algorithm performs maximum likelihood decoding – computes whether secret 0 or

secret s is more likely to have generated the observed leakage. Then, it predicts the most likely of the two events.

We emphasize that the secret $s' \in F^*$ that witnesses the maximum statistical distance between the leakage distributions $\mathrm{LSB}(\mathsf{Share}(0))$ and $\mathrm{LSB}(\mathsf{Share}(s'))$ may be different from the secret s defined above. Secret $s \in F^*$ witnesses the maximum *estimate* of the statistical distance between the distributions $\mathrm{LSB}(\mathsf{Share}(0))$ and $\mathrm{LSB}(\mathsf{Share}(s))$.

For brevity, define $\mathrm{err} := \frac{8^{5/4}}{\sqrt{p}} + \frac{13/2}{p}$. Given $\vec{\alpha}$, we run the LLL algorithm [38] to obtain $(u, v) \in [\alpha_1 : \alpha_2]$ such that $|u|_p, |v|_p \leqslant B$, where $B = \left\lceil 8^{1/4} \cdot \sqrt{p} \right\rceil$. Define $g = \gcd(|u|_p, |v|_p)$.

We are given that $\varepsilon_{\mathrm{LSB}}(\vec{\alpha}) > 2 \cdot \mathrm{err}$. We claim that $\varepsilon^{(\mathrm{OUR})}_{\mathrm{LSB}}(\vec{\alpha}) > \mathrm{err}$ and $|u|_p \cdot |v|_p / g^2$ is odd. Suppose not; then, there are two possibilities.

1. If $|u|_p \cdot |v|_p / g^2$ is even. In this case, $\varepsilon^{(\mathrm{OUR})}_{\mathrm{LSB}}(\vec{\alpha}) = 0$ and, hence, $\varepsilon_{\mathrm{LSB}}(\vec{\alpha}) \leqslant \mathrm{err}$, by Corollary 1; a contradiction.
2. If $\varepsilon^{(\mathrm{OUR})}_{\mathrm{LSB}}(\vec{\alpha}) \leqslant \mathrm{err}$ and $|u|_p \cdot |v|_p / g^2$ is odd. In this case, $\varepsilon_{\mathrm{LSB}}(\vec{\alpha}) \leqslant 2 \cdot \mathrm{err}$, by Corollary 1; a contradiction.

So, the signs of $\varepsilon^{(\mathrm{OUR})}_{\mathrm{LSB}}(\vec{\alpha})$ and $\left(\frac{1}{p}\Sigma^{(0)}_{\alpha_1,\alpha_2} - \frac{1}{p} \cdot \Sigma^{(\Delta)}_{\alpha_1,\alpha_2}\right)$ are identical (by Claim 12). Using this property, Appendix C.8 proves that the advantage of the maximum likelihood decoder is

$$\geqslant \varepsilon^{(\mathrm{OUR})}_{\mathrm{LSB}}(\vec{\alpha}) - \mathrm{err} \geqslant \varepsilon_{\mathrm{LSB}}(\vec{\alpha}) - 2 \cdot \mathrm{err}.$$

□

4.4 Proof outline of Theorem 1

For any $s \in F^*$, we prove Lemma 1 that obtains a closed-form estimate of

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

Then, we can solve for the optimal $s \in F^*$ that maximizes the statistical distance.

Lemma 1. *Consider the* $\mathsf{ShamirSS}(2, 2, (\alpha_1, \alpha_2))$ *secret-sharing scheme over a prime field* F_p*. For any secret* $s \in F_p^*$ *and* $(u, v) \in [\alpha_1 : \alpha_2]$*,*

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

$$\begin{cases} \pm\frac{4(|u|_p+|v|_p)-(3/2)}{p}, & \text{if } |u|_p \cdot |v|_p / g^2 \text{ is even} \\ \sin^2\left(|v|_p \pi \cdot \delta\right) \cdot \frac{g^2}{|u|_p \cdot |v|_p} \pm \frac{4(|u|_p+|v|_p)-(3/2)}{p}, & \text{if } |u|_p \cdot |v|_p / g^2 \text{ is odd,} \end{cases}$$

where $g = \gcd\left(|u|_p, |v|_p\right)$, $\delta = \frac{\mathrm{sign}_p(\Delta) \cdot |\Delta|_p}{p} \in \mathbb{Q}$, *and* $\Delta = \left(s \cdot 2^{-1}\right) \cdot \left(u^{-1} - v^{-1}\right) \in F_p^*$.

Appendix C.5 proves Lemma 1. Below, we present a high-level overview of the proof.

Step 1. Using a combinatorial argument, we connect the statistical distance between the leakages to the difference between two sums of oscillatory functions.

Lemma 2. *Consider the* $\mathsf{ShamirSS}(2,2,(\alpha_1,\alpha_2))$ *secret-sharing scheme over a prime field* F_p*. For any secret* $s \in F_p$ *and* $(u,v) \in [\alpha_1 : \alpha_2]$*,*

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

where $\Delta := \left(s \cdot 2^{-1}\right) \cdot \left(u^{-1} - v^{-1}\right)$*, a linear automorphism over* F_p*.*

Appendix C.1 proves Lemma 2.

Step 2. Recall that $\mathrm{sign}_p(X=0) = +1$ and $\mathrm{sign}(x=0) = 0$. Due to this mismatch, we defined an intermediate function $\widetilde{\mathrm{sign}}_p(X=0) = 0$. So, our next objective is to relate the quantities $\Sigma^{(\Delta)}_{k,\ell}$ with $\widetilde{\Sigma}^{(\Delta)}_{k,\ell}$.

Lemma 3. *For any* $k, \ell, \Delta \in F_p$*,*

$$\Sigma^{(\Delta)}_{k,\ell} = \widetilde{\Sigma}^{(\Delta)}_{k,\ell} \quad + \left(\sum_{T \in \{0,\Delta\}} \mathrm{sign}_p(kT) \cdot \mathrm{sign}_p(\ell(T-\Delta))\right).$$

Appendix C.2 proves Lemma 3.

Step 3. Next, our objective is to estimate the sum $\frac{1}{p} \cdot \widetilde{\Sigma}^{(\Delta)}_{k,\ell}$ using the integral $I^{(\delta)}_{k,\ell}$, for an appropriately define $\delta \in \mathbb{R}$.

Lemma 4. *For any* $k, \ell, \Delta \in F_p$*,*

$$\frac{1}{p} \cdot \widetilde{\Sigma}^{(\Delta)}_{k,\ell} = \mathrm{sign}_p(k) \cdot \mathrm{sign}_p(\ell) \cdot I^{(\delta)}_{|k|_p,|\ell|_p} \quad \pm \frac{4(|k|_p + |\ell|_p) - 2}{p},$$

where $\delta = \frac{\mathrm{sign}_p(\Delta) \cdot |\Delta|_p}{p} \in \mathbb{Q}$*.*

Appendix C.3 proves Lemma 4.

Step 3. Finally, we compute the value of the integral $I^{(\delta)}_{k,\ell}$.

Lemma 5. *For any* $k, \ell \in \{1, 2, \dots\}$ *and* $\delta \in \mathbb{R}$*,*

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

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

Appendix C.4 proves Lemma 5. Intuitively, if the highest power of 2 dividing k is different from the highest power of 2 dividing ℓ, then $k\ell/g^2$ is even and $I^{(\delta)}_{k,\ell} = 0$. If the highest power of 2 dividing k is identical to the highest power of 2 dividing ℓ, then $k\ell/g^2$ is odd and $I^{(\delta)}_{k,\ell} \neq 0$.

Step 4. Sequentially performing the substitutions above, we can estimate the statistical distance using the integrals, which yields Lemma 1.

Efficient distinguisher construction. We present an efficient maximum likelihood distinguisher in Appendix C.6.

5 Security against all Physical Bit Leakage

We consider $\mathsf{ShamirSS}(n = 2, k = 2, (\alpha_1, \alpha_2))$ over the prime field F of order $p \geqslant 3$. This section considers 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 $2^{82,589,933} - 1$.

5.1 Properties of Mersenne Primes

Mersenne primes have fascinating properties.

Proposition 1. *Let F be a prime field of order $p = 2^\lambda - 1$. 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 2. *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 1.

5.2 Leakage Resilience to Physical Bit Leakage

Let $\mathrm{PHYS}_i \colon F \to \{0, 1\}$ represent the function that outputs the i-th least significant bit in the binary representation. So, for example, $\mathrm{PHYS}_i^{-1}(0) = E_i = E \cdot (2^i)$. 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 $\vec{\mathrm{PHYS}}_{i,j}$.

5.2.1 Leakage attack when $2^k\alpha_1 = \alpha_2$.

Although $\alpha_1 \neq \alpha_2$, it may be possible that $2^k\alpha_1 = \alpha_2$, for some $k \in \{0, 1, \ldots, \lambda - 1\}$. We prove 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 $s \in F$. Then, the secret share at evaluation place α is $s + u\alpha$, for uniformly random $u \in F$. The joint distribution of leakage is

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

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

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

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

$$\Big(\mathrm{PHYS}_0(t2^k + v\alpha_1 2^k), \mathrm{PHYS}_0(t + v\alpha_2)\Big) \equiv \Big(\mathrm{PHYS}_0(t2^k + v\alpha_2), \mathrm{PHYS}_0(t + v\alpha_2)\Big),$$

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

For $t = 0$, both the leakage bits are identical. On the other hand, for $t = t^* := (2^k - 1)^{-1}$, the joint distribution of leakage is

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

These two leakage bits are different with $(1 - 1/p)$ probability. Therefore, one can distinguish the secret 0 and secret t^*2^j with $(1 - 1/p) \sim 1$ advantage by leaking $\vec{\mathrm{PHYS}}_{i,j}$; whence the following lemma follows.

Lemma 6. *Let F_p be the prime field of order $p = 2^\lambda - 1$. Consider distinct evaluation places $\alpha_1, \alpha_2 \in F_p^*$ such that $2^k \cdot \alpha_1 = \alpha_2$ for some $k \in \{0, 1, \ldots, \lambda - 1\}$. Then,*

$$\mathsf{SD}\left(\vec{\mathrm{PHYS}}_{i,j}(\mathsf{Share}(0)) \;,\; \vec{\mathrm{PHYS}}_{i,j}(\mathsf{Share}(s))\right) \geqslant 1 - \frac{1}{p},$$

where $i, j \in \{0, 1, \ldots, \lambda - 1\}$, $j - i = k \mod \lambda$, and $s = (2^k - 1)^{-1} \cdot 2^j$.

5.2.2 Reduction to the LSB Attack.

Due to the properties of the F_p, where p is a Mersenne prime, we can reduce arbitrary physical bit attacks on $\mathsf{ShamirSS}(2, 2, \vec{\alpha})$ to LSB leakage attacks on $\mathsf{ShamirSS}(2, 2, \vec{\alpha'})$, for an appropriately defined $\vec{\alpha'}$.

Lemma 7. *Let F_p be a prime field of order $p = 2^\lambda - 1$. Consider evaluation places $\alpha_1, \alpha_2 \in F_p^*$ such that $2^k \cdot \alpha_1 \neq \alpha_2$, for all $k \in \{0, 1, \ldots, \lambda - 1\}$. Consider the leakage attack $\vec{\mathrm{PHYS}}_{i,j}$ for any $i, j \in \{0, 1, \ldots, \lambda - 1\}$. Define $\alpha'_1 = 2^{-i} \cdot \alpha_1$ and $\alpha'_2 = 2^{-j} \cdot \alpha_2$. For any $s \in F_p$, let D denote the joint leakage distribution generated by the leakage function $\vec{\mathrm{PHYS}}_{i,j}$ when the secret shares are generated using the $\mathsf{ShamirSS}(2, 2, \vec{\alpha})$ secret-sharing scheme. Likewise, D' denotes the joint leakage distribution generated by the leakage function $\vec{\mathrm{LSB}}$ when the secret shares are generated using the $\mathsf{ShamirSS}(2, 2, \vec{\alpha'})$ secret-sharing scheme instead. Then, the distributions D and D' are identical.*

Since $2^k \cdot \alpha_1 \neq \alpha_2$, for all $k \in \{0, 1, \ldots, \lambda - 1\}$, we conclude that $\alpha'_1 \neq \alpha'_2$, for all $i, j \in \{0, 1, \ldots, \lambda - 1\}$. Therefore, the secret-sharing scheme $\mathsf{ShamirSS}(2, 2, \vec{\alpha'})$ is valid. Appendix C.9 proves that the distributions D and D' are identical, for all $s \in F_p$, using Proposition 2.

5.3 Statement and Proof of Corollary 4

Corollary 4. *Let F_p be the prime field of order $p = 2^\lambda - 1$. Consider distinct evaluation places $\vec{\alpha} = (\alpha_1, \alpha_2)$ and the corresponding secret-sharing scheme $\mathsf{ShamirSS}(2, 2, \vec{\alpha})$. Define*

$$\varepsilon^{(\mathrm{OUR})}_{\mathrm{PHYS}} = \begin{cases} 1, & \text{if } 2^t \cdot \alpha_1 = \alpha_2 \\ & \text{for some } t \in \{0, 1, \ldots, \lambda - 1\}, \\ \max\limits_{k \in \{0,1,\ldots,p-1\}} \varepsilon^{(\mathrm{OUR})}_{\mathrm{LSB}}\left((2^k\alpha_1, \alpha_2)\right), & \text{if } 2^t \cdot \alpha_1 = \alpha_2 \\ & \text{for all } t \in \{0, 1, \ldots, \lambda - 1\}. \end{cases}$$

Then,

$$\varepsilon^{(\mathrm{OUR})}_{\mathrm{PHYS}}(\vec{\alpha}) = \varepsilon_{\mathrm{PHYS}}(\vec{\alpha}) \quad \pm \left(\frac{8^{5/4}}{\sqrt{p}} + \frac{13/2}{p} \right).$$

Proof. If $2^t \cdot \alpha_1 = \alpha_2$, for some $t \in \{0, 1, \ldots, \lambda - 1\}$, we have $\varepsilon^{(\mathrm{OUR})}_{\mathrm{PHYS}}(\vec{\alpha}) = 1$. Lemma 6 presents a physical bit leakage attack with distinguishing advantage $1 - 1/p$; therefore, $\varepsilon_{\mathrm{PHYS}}(\vec{\alpha}) \geqslant 1 - 1/p$. So, we conclude that

$$\varepsilon^{(\mathrm{OUR})}_{\mathrm{PHYS}}(\vec{\alpha}) = \varepsilon_{\mathrm{PHYS}}(\vec{\alpha}) \pm \frac{1}{p}.$$

If $2^t\alpha_1 \neq \alpha_2$, for all $t \in \{0, 1, \ldots, \lambda-1\}$, Lemma 7 shows that the leakage distribution of $\mathrm{PHYS}_{i,j}$ on $\mathsf{ShamirSS}(2, 2, \vec{\alpha})$ is identical to the leakage distribution $\vec{\mathrm{LSB}}$ on $\mathsf{ShamirSS}(2, 2, \ (2^{-i}\alpha_1, 2^{-j}\alpha_j)\ )$. Recall that the secret-sharing scheme $\mathsf{ShamirSS}(2, 2, \ (2^{-i}\alpha_1, 2^{-j}\alpha_j)\ )$ is identical to the secret-sharing scheme $\mathsf{ShamirSS}(2, 2, \ (2^{j-i}\alpha_1, \alpha_j)\ )$, by Lemma 10 in Appendix B. Therefore, we conclude the following:

$$\varepsilon_{\mathrm{PHYS}}(\vec{\alpha}) = \max_{t \in \{0,1,\ldots\}} \varepsilon_{\mathrm{LSB}}\left(\ (2^t\alpha_1, \alpha_2)\ \right).$$

We know that our estimation $\varepsilon^{(\mathrm{OUR})}_{\mathrm{LSB}}(\cdot)$ is a tight estimation of $\varepsilon_{\mathrm{LSB}}(\cdot)$, by Corollary 1. Therefore, we conclude that

$$\varepsilon^{(\mathrm{OUR})}_{\mathrm{PHYS}}(\vec{\alpha}) = \varepsilon_{\mathrm{PHYS}}(\vec{\alpha}) \quad \pm \left(\frac{8^{5/4}}{\sqrt{p}} + \frac{13/2}{p} \right).$$

□

5.4 Statement and Proof of Corollary 5

Corollary 5. *Let F_p be the prime field of order $p = 2^\lambda - 1$. Consider distinct evaluation places $\vec{\alpha} = (\alpha_1, \alpha_2)$ and the corresponding $\mathsf{ShamirSS}(2, 2, \vec{\alpha})$ secret-sharing scheme over the prime field F_p. Suppose the algorithm in Figure 1 determines $\vec{\alpha}$ to be secure. Then,*

$$\varepsilon_{\mathrm{PHYS}}(\vec{\alpha}) \leqslant \frac{1 + 8^{5/4}}{\sqrt{p}} + \frac{13/2}{p}.$$

Among all possible distinct evaluation places $\alpha_1, \alpha_2 \in F_p^*$, the algorithm of Figure 2 determines at least

$$\geqslant 1 \quad - \frac{\ln p}{\ln 2} \cdot \frac{\frac{1}{4} \cdot \sqrt{p} \cdot \ln p + \frac{3}{2} \cdot \sqrt{p} + \frac{1}{2}}{p - 2} \geqslant^{(*)} 1 \quad - \frac{\ln p}{\ln 2} \cdot \left(\frac{\ln p}{4\sqrt{p}} + \frac{5/2}{\sqrt{p}} \right).$$

fraction of them to be secure. The $(*)$ inequality holds for all $p \geqslant 11$.

Proof. **Proof of the first part.** If the algorithm in Figure 1 determined (α_1, α_2) to be secure, then the algorithm in Figure 2 determined $(2^t\alpha_1, \alpha_2)$ to be secure, for all $t \in \{0, 1, \ldots, \lambda - 1\}$. For $t \in \{0, 1, \ldots, \lambda - 1\}$, by Corollary 2, we get the bound that

$$\varepsilon_{\mathrm{LSB}}\left(\ (2^t\alpha_1, \alpha_2)\ \right) \leqslant \frac{1 + 8^{5/4}}{\sqrt{p}} + \frac{13/2}{p}.$$

Just like the proof of Corollary 4, we have

$$\varepsilon_{\mathrm{PHYS}}(\vec{\alpha}) = \max_{t \in \{0,1,\ldots,\lambda-1\}} \varepsilon_{\mathrm{LSB}}\left(\ (2^t\alpha_1, \alpha_2)\ \right) \leqslant \frac{1 + 8^{5/4}}{\sqrt{p}} + \frac{13/2}{p}.$$

Proof of the second part. If the algorithm in Figure 1 outputs "may be insecure" then there is some $k \in \{0, 1, \ldots, \lambda - 1\}$ such that the algorithm in Figure 2 outputs "may be insecure" for $(2^k\alpha_1, \alpha_2)$. Corollary 2 proves that the algorithm in Figure 2 outputs "may be insecure" for at most

$$\frac{\frac{1}{4} \cdot \sqrt{p} \cdot \ln p + \frac{3}{2} \cdot \sqrt{p} + \frac{1}{2}}{p - 2}$$

fraction of the equivalence classes. By, a union bound over $k \in \{0, 1, \ldots, \lambda - 1\}$, Figure 1 outputs "may be insecure" for at most

$$\log_2 p \cdot \frac{\frac{1}{4} \cdot \sqrt{p} \cdot \ln p + \frac{3}{2} \cdot \sqrt{p} + \frac{1}{2}}{p - 2}$$

fraction of the equivalence classes. □

5.5 Statement and Proof of Corollary 6

Corollary 6. *Let F_p be the prime field with order $p = 2^\lambda - 1$. Consider distinct evaluation places $\vec{\alpha} = (\alpha_1, \alpha_2)$ and the corresponding $\mathsf{ShamirSS}(2, 2, \vec{\alpha})$ over F_p. If $\varepsilon_{\mathrm{PHYS}}(\vec{\alpha}) > \frac{2 \cdot 8^{5/4}}{\sqrt{p}} + \frac{13}{p}$, then there is an efficient algorithm that generates $(s, f) \in F_p^* \times \mathrm{PHYS}$ and can distinguish the secret 0 from the secret s with an advantage*

$$\geqslant \varepsilon_{\mathrm{PHYS}}(\vec{\alpha}) \quad - \frac{2 \cdot 8^{5/4}}{\sqrt{p}} - \frac{13}{p}$$

by leaking f from the secret shares.

Proof. If there is $t \in \{0, 1, \ldots, \lambda - 1\}$ such that $2^t\alpha_1 = \alpha_2$, then Lemma 6 presents an explicit leakage attack that suffices for this corollary.

If there $2^t\alpha_1 \neq \alpha_2$ for all $t \in \{0, 1, \ldots, \lambda - 1\}$, then Lemma 7 helps relate physical bit attacks and LSB attacks. Suppose t is the witness such that $\varepsilon^{(\mathrm{OUR})}_{\mathrm{PHYS}}(\vec{\alpha}) = \varepsilon^{(\mathrm{OUR})}_{\mathrm{LSB}}\left((2^t\alpha_1, \alpha_2)\right)$. Then, consider the adversary against $\mathsf{ShamirSS}(2, 2, (2^t\alpha_1, \alpha_2))$ that uses the LSB attack as guaranteed by Corollary 3. Lemma 7 proves that the leakage distribution of the physical bit attack $\vec{\mathrm{PHYS}}_{0,t}$ on $\mathsf{ShamirSS}(2, 2, \vec{\alpha})$ secret-sharing scheme has an identical distribution. So, we run the adversary of Corollary 3 by leaking $\vec{\mathrm{PHYS}}_{0,t}$ from the secret shares of the $\mathsf{ShamirSS}(2, 2, \vec{\alpha})$ secret-sharing scheme. □

5.6 Statement and Proof of Corollary 7

Corollary 7. *Let F_p be the prime field of order $p = 2^\lambda - 1$. Define $t := \lfloor \lambda/2 \rfloor$. Consider $\vec{\alpha} = (\alpha_1, \alpha_2) \in \left[1 \colon 2^t - 1\right]$. Then*

$$\varepsilon_{\mathrm{PHYS}}(\vec{\alpha}) \leqslant \frac{4 \cdot \left(2^{\lfloor \lambda/2 \rfloor} + 2^{\lceil \lambda/2 \rceil}\right) - 6}{p}.$$

Proof. For the proof, fix $\alpha_1 = 1$ and $\alpha_2 = 2^{\lfloor \lambda/2 \rfloor} - 1$. We shall compute $\varepsilon_{\mathrm{LSB}}(2^i \cdot \alpha_1, \alpha_2)$ for all $i \in \{0, 1, \ldots, \lambda - 1\}$ using Lemma 1. The bound in our corollary will be the maximum of these individual upper bounds on $\varepsilon_{\mathrm{LSB}}(\cdot)$.

Case A: $i = 0$. We are interested in computing the security of the evaluation places $(2^i\alpha_1, \alpha_2)$ We use $(u, v) = (1, 2^t - 1)$, where $t = \lfloor \lambda/2 \rfloor$. Note that u, v are relatively prime and $|u|_p = 1$ and $|v|_p = 2^t - 1$. Both these evaluation places are odd. Therefore, by Lemma 1, we have

$$\varepsilon_{\mathrm{LSB}}(2^i \cdot \alpha_1, \alpha_2) \leqslant \frac{1}{2^t - 1} + \frac{4 + 4 \cdot (2^t - 1) - 2}{p}.$$

Case B: $1 \leqslant i \leqslant \lfloor \lambda/2 \rfloor$. We are interested in the security of $(u, v) = (2^i, 2^t - 1)$, where $t = \lfloor \lambda/2 \rfloor$. Note that u and v are relatively prime, u is even, and v is odd. Therefore, by Lemma 1, we have

$$\varepsilon_{\mathrm{LSB}}(2^i \cdot \alpha_1, \alpha_2) \leqslant \frac{4 \cdot 2^i + 4 \cdot (2^t - 1) - 2}{p}.$$

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

$$\begin{aligned} u' &= 2^{\lambda - t} \cdot u \mod 2^\lambda - 1 = 2^{i - t} \\ v' &= 2^{\lambda - t} \cdot v \mod 2^\lambda - 1 = -(2^{\lambda - t} - 1). \end{aligned}$$

Substitute $u' = 2^j$, where $1 \leqslant j \leqslant \lfloor \lambda/2 \rfloor$, and $v' = -(2^{\lambda - t} - 1)$. Therefore, by Lemma 1, we have

$$\varepsilon_{\mathrm{LSB}}(2^i \cdot \alpha_1, \alpha_2) \leqslant \frac{4 \cdot 2^j + 4 \cdot (2^{\lambda - t} - 1) - 2}{p}.$$

Appendix C.10 proves the following upper bound on the insecurity for all $0 \leqslant i < \lambda$.

$$\varepsilon_{\mathrm{LSB}}(2^i \cdot \alpha_1, \alpha_2) \leqslant \frac{4 \cdot (2^{\lfloor \lambda/2 \rfloor} + 2^{\lceil \lambda/2 \rceil}) - 6}{p}$$

□

6 The Case of $(n, k) = (3, 2)$

Lemma 8. *Let F_p be a prime field of order $p = 2^\lambda - 1$. Consider distinct evaluation places $(\alpha_1, \alpha_2, \alpha_3)$. Let $\varepsilon(\vec{\alpha})$ denote the insecurity of the* $\mathsf{ShamirSS}(3, 2, \vec{\alpha})$ *secret-sharing scheme against physical bit leakage attacks. For $1 \leqslant i < j \leqslant 3$, denote the insecurity of the* $\mathsf{ShamirSS}(2, 2, (\alpha_i, \alpha_j))$ *secret-sharing scheme against physical bit leakage attacks by $\varepsilon_{\mathrm{PHYS}}(\alpha_i, \alpha_j)$. Then,*

$$\varepsilon_{\mathrm{PHYS}}(\vec{\alpha}) \leqslant \sum_{1 \leqslant i < j \leqslant 3} \varepsilon_{\mathrm{PHYS}}(\alpha_i, \alpha_j) + \frac{1}{p}.$$

Appendix D presents the full proof of this lemma. Note that if $\varepsilon_{\mathrm{PHYS}}(\alpha_i, \alpha_j)$ is large, then there is a leakage attack on $\mathsf{ShamirSS}(3, 2, \vec{\alpha})$.

7 Extension to arbitrary Number of Parties

We extend our derandomization results to Shamir's secret-sharing scheme with the reconstruction threshold k equal to the number of parties $n \in \{2, 3, \dots\}$. We prove the following general lifting theorem. Corollary 8 is a consequence of this theorem.

Theorem 2. *Consider* $\mathsf{ShamirSS}(n, n, \vec{\alpha})$ *over a prime field* F*. For every* $i \in \{1, 2, \ldots, n\}$*, 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,* $\mathsf{ShamirSS}(n, n, (\alpha_1, \alpha_2, \ldots, \alpha_n))$ *has at most* 2ε*-insecurity against physical bit leakages.*

The proof of this theorem is Fourier-analytic and uses properties of the 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 distinct *evaluation places* $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n)$ 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

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

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 [27, 39].

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 $k = n - 1$*, the dual code is the set* $\{\beta \cdot (v_1, v_2, \ldots, v_n)\colon \beta \in F\}$*, 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 $[n, n-1, \vec{\alpha}]$-Shamir secret-sharing.

Since the proof of Theorem 2 is entirely Fourier-analytic, it is presented in Appendix E along with a brisk introduction to (elementary) Fourier analysis.

7.1 Statement and Proof of Corollary 8

Corollary 8. *Let* F_p *be the prime field of order* $p = 2^\lambda - 1$*. Fix any* $n \in \{3, 4, \ldots\}$*. There is a probabilistic efficient algorithm to choose distinct evaluation places* $\vec{\alpha}$ *such that*

$$\varepsilon_{\text{PHYS}}(\vec{\alpha}) \leqslant \frac{2 \cdot 8^{5/4}}{\sqrt{p}} + \frac{13}{p}.$$

The failure probability of this algorithm is

$$\leqslant \frac{n+1}{p} + \left(\frac{1}{4 \ln 2} \cdot \frac{(\ln p)^2}{\sqrt{p}} + \frac{5}{2 \ln 2} \cdot \frac{\ln p}{\sqrt{p}}\right).$$

Proof. Choose arbitrary distinct evaluation places $\alpha_1, \alpha_2, \alpha_4, \ldots, \alpha_n \in F_p^*$. Choose α_3 uniformly at random from the set $F_p \setminus \{\alpha_1\}$. The probability that the evaluation places $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ are *not* all distinct is

$$\leqslant \frac{n-2}{p}.$$

Define $\beta_i := \left(\alpha_i(\prod_{j\neq i}(\alpha_i - \alpha_j)\right)^{-1}$ as in Theorem 2, for $i \in \{1, \ldots, n\}$. Observe that choosing $\vec{\alpha}$ at random does not necessarily imply that $\vec{\beta}$ is uniformly and independently random over F_p. For this paper, we will prove a result that is easy to prove and sufficient for our context.

Lemma 9. *For $n \geqslant 3$, the distribution of the equivalence class $[\beta_1 : \beta_2]$ is $2/(p-1)$-close to the uniform distribution over the equivalence classes $[1:2], [1:3], \ldots, [1:p-1]$, for*

1. *Arbitrary $\alpha_1, \alpha_2 \in F_p^*$ such that $\alpha_1 \neq \alpha_2$,*
2. *Arbitrary $\alpha_4, \ldots, \alpha_n$ satisfying $\{\alpha_1, \alpha_2\} \cap \{\alpha_4, \ldots, \alpha_n\} = \emptyset$, and*
3. *The evaluation place α_3 is chosen uniformly at random from the set $F_p \setminus \{\alpha_1\}$.*

Appendix F.1 proves this lemma. We use the algorithm in Figure 1 to test whether evaluation places in the equivalence class $[\beta_1 : \beta_2]$ is ε-secure, where

$$\varepsilon \leqslant \frac{8^{5/4}}{\sqrt{p}} + \frac{13/2}{p}.$$

This guarantee is from Corollary 5. The probability of the algorithm in Figure 1 to return "may be insecure" is also exponentially small

$$\leqslant \left(\frac{1}{4\ln 2} \cdot \frac{(\ln p)^2}{\sqrt{p}} + \frac{5}{2\ln 2} \cdot \frac{\ln p}{\sqrt{p}}\right)$$

(again by Corollary 5). If no such pair of secure indices exit, then report *failure*. Otherwise, if one such pair exists, by Theorem 2, $\mathsf{ShamirSS}(n, n, \vec{\alpha})$ has insecurity

$$\varepsilon_{\mathrm{PHYS}}(\vec{\alpha}) \leqslant 2\varepsilon.$$

By union bound, the failure probability is

$$\begin{aligned}
&\leqslant \frac{n-2}{p} + \frac{2}{p-1} + \left(\frac{1}{4\ln 2} \cdot \frac{(\ln p)^2}{\sqrt{p}} + \frac{5}{2\ln 2} \cdot \frac{\ln p}{\sqrt{p}}\right) \\
&\leqslant \frac{n+1}{p} + \left(\frac{1}{4\ln 2} \cdot \frac{(\ln p)^2}{\sqrt{p}} + \frac{5}{2\ln 2} \cdot \frac{\ln p}{\sqrt{p}}\right). \qquad \text{(for } p \geqslant 3\text{)}
\end{aligned}$$

□

One can boost the success probability exponentially by repeating this experiment.

8 Prior Related Works

Reed-Solomon Code Repair. Guruswami and Wootters [24, 25] considered the exact repair problem for Reed-Solomon codes. They repaired the codeword by obtaining partial information from each block. Subsequently, there has been a large body of work on repairing Reed-Solomon codes [17, 18, 21, 22, 48, 57, 62, 50, 63, 64, 14]. Massey [46] established a connection between linear secret-sharing schemes and linear codes. For example, Shamir's secret-sharing scheme is the Massey secret-sharing scheme corresponding to (punctured) Reed-Solomon codes. Repairing strategies for Reed-Solomon codes translate into techniques to reconstruct the secret in Shamir's secret-sharing scheme. However, there is a crucial difference. The literature on Reed-Solomon codes evaluates the secret polynomial on *all* finite field elements; they have $n = \mathsf{card}(F)$. For leakage resilience, typically, the secret polynomial is evaluated at $n \leqslant \mathsf{poly}(\log \mathsf{card}(F))$ evaluation places; [14, Section VI] highlights this distinction.

Local leakage resilience. Benhamouda et al. [5] introduced leakage-resilient secret-sharing, which was implicit in the work of Goyal and Kumar [23]. Several works have constructed new secret-sharing schemes that are resilient to leakage attacks [7, 2, 56, 3, 36, 8, 19, 20, 30, 13, 45, 11]. There is a significant interest in characterizing the leakage-resilience of practical secret-sharing schemes, like the additive and Shamir's secret-sharing scheme. [40] 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 [40, 1, 42]. Other Monte Carlo constructions have also been proposed in [44, 41].

Another flavor of results characterizes the leakage-resilience of Shamir's secret-sharing scheme for a large number of parties. For example, when $k \geqslant 0.69n$, 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 [5, 6, 44, 43, 32]. Contrast this with our scenario, where the insecurity is exponentially small in the security parameter, which is independent of n. [47] proved that Shamir's secret-sharing scheme is insecure to local leakage when n/k is large.

Physical bit probing attacks. 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. [9] showed the vulnerability of computing RSA signatures to random fault injection into memory. Ishai, Sahai, and Wagner [31] introduced the *bit probing model* to theoretically investigate threats posed by an adversary that can probe a bounded number of memory locations. Bit probes on a share can also be used to estimate its Hamming weight, which leads to real threats like (1) algebraic side-channel attacks (beginning with the work of Renauld et al. [51]) and (2) recent attacks like Hertzbleed [61]. Maji et al. [40] introduced the "parity-of-parities" attack on the *additive secret-sharing* scheme. This attack leaks the LSB of each share, and the parity of the leaked bits is correlated with the secret's parity; this attack leads to $(2/\pi)^n \approx 0.63^n$ insecurity [1, 42]. This simple attack matches the upper bound on the insecurity of the additive secret-sharing scheme against *arbitrary local leakage* proved in [5, 6]. Maji et al. [40] & Costes and Stam [15] independently observed that *Shamir's secret-sharing* scheme inherits this vulnerability if the modulus and the evaluation places are carelessly chosen. Our work identifies more vulnerable evaluation places using the same LSB attack.

Square wave function families. Various families of square waves find wide applications in science and engineering. For example, consider the ones proposed by Haar [26], Walsh [60], and Rademacher [49]. In our work, we connect the leakage resilience of secret-sharing schemes with the properties of another family of square waves (see, for example, [58, 29, 28])

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

Previous works [58, 29] 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.

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 [38] to efficiently achieve this objective (see Appendix A).

The Dirichlet approximation theorem [52, 53] 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 [37]. However, we can efficiently solve this problem by slightly weakening the upper bound on q. The seminal LLL algorithm [38], in particular, for $\alpha \in \mathbb{Q}^d$, finds $1 \leqslant q \leqslant 2^{d(d+1)/4} \cdot N^d$ such that

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

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. 1, 2, 28

[2] Divesh Aggarwal, Ivan Damgård, Jesper Buus Nielsen, Maciej Obremski, Erick Purwanto, João Ribeiro, and Mark Simkin. Stronger leakage-resilient and non-malleable secret sharing schemes for general access structures. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 510–539. Springer, Heidelberg, August 2019. doi:10.1007/978-3-030-26951-7_18. 28

[3] Saikrishna Badrinarayanan and Akshayaram Srinivasan. Revisiting non-malleable secret sharing. In Yuval Ishai and Vincent Rijmen, editors, *EUROCRYPT 2019, Part I*, volume 11476 of *LNCS*, pages 593–622. Springer, Heidelberg, May 2019. doi:10.1007/978-3-030-17653-2_20. 28

[4] 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

[5] 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. 1, 3, 28

[6] 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. 1, 28

[7] Allison Bishop, Valerio Pastro, Rajmohan Rajaraman, and Daniel Wichs. Essentially optimal robust secret sharing with maximal corruptions. In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016, Part I*, volume 9665 of *LNCS*, pages 58–86. Springer, Heidelberg, May 2016. doi:10.1007/978-3-662-49890-3_3. 28

[8] Andrej Bogdanov, Yuval Ishai, and Akshayaram Srinivasan. Unconditionally secure computation against low-complexity leakage. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 387–416. Springer, Heidelberg, August 2019. doi:10.1007/978-3-030-26951-7_14. 28

[9] 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. 28

[10] 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

[11] Nishanth Chandran, Bhavana Kanukurthi, Sai Lakshmi Bhavana Obbattu, and Sruthi Sekar. Short leakage resilient and non-malleable secret sharing schemes. In Yevgeniy Dodis and

Thomas Shrimpton, editors, *CRYPTO 2022, Part I*, volume 13507 of *LNCS*, pages 178–207. Springer, Heidelberg, August 2022. doi:10.1007/978-3-031-15802-5_7. 28

[12] Suresh Chari, Charanjit S. Jutla, Josyula R. Rao, and Pankaj Rohatgi. Towards sound approaches to counteract power-analysis attacks. In Michael J. Wiener, editor, *CRYPTO'99*, volume 1666 of *LNCS*, pages 398–412. Springer, Heidelberg, August 1999. doi:10.1007/3-540-48405-1_26. 1

[13] Eshan Chattopadhyay, Jesse Goodman, Vipul Goyal, Ashutosh Kumar, Xin Li, Raghu Meka, and David Zuckerman. Extractors and secret sharing against bounded collusion protocols. In *61st FOCS*, pages 1226–1242. IEEE Computer Society Press, November 2020. doi:10.1109/FOCS46700.2020.00117. 28

[14] Roni Con and Itzhak Tamo. Nonlinear repair of reed-solomon codes. *IEEE Trans. Inf. Theory*, 68(8):5165–5177, 2022. doi:10.1109/TIT.2022.3167615. 27

[15] 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. 28

[16] Richard E Crandall and Carl Pomerance. *Prime numbers: a computational perspective*, volume 2. Springer, 2005. 8

[17] Alexandros G Dimakis, P Brighten Godfrey, Yunnan Wu, Martin J Wainwright, and Kannan Ramchandran. Network coding for distributed storage systems. *IEEE transactions on information theory*, 56(9):4539–4551, 2010. 27

[18] Salim El Rouayheb and Kannan Ramchandran. Fractional repetition codes for repair in distributed storage systems. In *2010 48th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pages 1510–1517. IEEE, 2010. 27

[19] Serge Fehr and Chen Yuan. Towards optimal robust secret sharing with security against a rushing adversary. In Yuval Ishai and Vincent Rijmen, editors, *EUROCRYPT 2019, Part III*, volume 11478 of *LNCS*, pages 472–499. Springer, Heidelberg, May 2019. doi:10.1007/978-3-030-17659-4_16. 28

[20] Serge Fehr and Chen Yuan. Robust secret sharing with almost optimal share size and security against rushing adversaries. In Rafael Pass and Krzysztof Pietrzak, editors, *TCC 2020, Part III*, volume 12552 of *LNCS*, pages 470–498. Springer, Heidelberg, November 2020. doi:10.1007/978-3-030-64381-2_17. 28

[21] Sreechakra Goparaju, Salim El Rouayheb, Robert Calderbank, and H Vincent Poor. Data secrecy in distributed storage systems under exact repair. In *2013 International Symposium on Network Coding (NetCod)*, pages 1–6. IEEE, 2013. 27

[22] Sreechakra Goparaju, Arman Fazeli, and Alexander Vardy. Minimum storage regenerating codes for all parameters. *IEEE Transactions on Information Theory*, 63(10):6318–6328, 2017. 27

[23] 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. 1, 3, 28

[24] Venkatesan Guruswami and Mary Wootters. Repairing reed-solomon codes. In Daniel Wichs and Yishay Mansour, editors, *48th ACM STOC*, pages 216–226. ACM Press, June 2016. doi:10.1145/2897518.2897525. 1, 27

[25] Venkatesan Guruswami and Mary Wootters. Repairing reed-solomon codes. *IEEE Trans. Inf. Theory*, 63(9):5684–5698, 2017. doi:10.1109/TIT.2017.2702660. 1, 27

[26] Alfréd Haar. Aur theorie der orthogonalen funcktionensysteme. *Math. Annalen*, 69:331–371, 1910. 3, 28

[27] Jonathan I. Hall. Notes on coding theory. https://users.math.msu.edu/users/halljo/classes/codenotes/GRS.pdf, 2015. 2, 26, 36

[28] 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. 3, 11, 28, 40

[29] Walter J Harrington and John W Cell. A set of square-wave functions orthogonal and complete in $l\_2(0, 2)$. *Duke Math. J.*, 28(1):393–407, 1961. 3, 11, 28, 40

[30] Carmit Hazay, Muthuramakrishnan Venkitasubramaniam, and Mor Weiss. The price of active security in cryptographic protocols. In Anne Canteaut and Yuval Ishai, editors, *EUROCRYPT 2020, Part II*, volume 12106 of *LNCS*, pages 184–215. Springer, Heidelberg, May 2020. doi:10.1007/978-3-030-45724-2_7. 28

[31] 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. 28

[32] Ohad Klein and Ilan Komargodski. New bounds on the local leakage resilience of shamir's secret sharing scheme. In *CRYPTO*, 2023. 28

[33] Paul C. Kocher. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In Neal Koblitz, editor, *CRYPTO'96*, volume 1109 of *LNCS*, pages 104–113. Springer, Heidelberg, August 1996. doi:10.1007/3-540-68697-5_9. 1

[34] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In Michael J. Wiener, editor, *CRYPTO'99*, volume 1666 of *LNCS*, pages 388–397. Springer, Heidelberg, August 1999. doi:10.1007/3-540-48405-1_25. 1

[35] Steven G Krantz. *A panorama of harmonic analysis*, volume 27. American Mathematical Soc., 2019. 40

[36] Ashutosh Kumar, Raghu Meka, and Amit Sahai. Leakage-resilient secret sharing against colluding parties. In David Zuckerman, editor, *60th FOCS*, pages 636–660. IEEE Computer Society Press, November 2019. doi:10.1109/FOCS.2019.00045. 28

[37] Jeffrey C Lagarias. The computational complexity of simultaneous diophantine approximation problems. *SIAM Journal on Computing*, 14(1):196–209, 1985. 12, 29

[38] Arjen K Lenstra, Hendrik Willem Lenstra, and László Lovász. Factoring polynomials with rational coefficients. *Mathematische annalen*, 261(ARTICLE):515–534, 1982. 3, 12, 13, 17, 19, 29, 35

[39] Yehuda Lindell. Introduction to coding theory lecture notes. https://u.cs.biu.ac.il/~lindell/89-662/coding_theory-lecture-notes.pdf, 2010. 26, 36

[40] 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. 1, 2, 4, 7, 8, 28, 58

[41] 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. 28

[42] 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. 1, 2, 28

[43] 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. 28

[44] 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. 28

[45] Pasin Manurangsi, Akshayaram Srinivasan, and Prashant Nalini Vasudevan. Nearly optimal robust secret sharing against rushing adversaries. In Daniele Micciancio and Thomas Ristenpart, editors, *CRYPTO 2020, Part III*, volume 12172 of *LNCS*, pages 156–185. Springer, Heidelberg, August 2020. doi:10.1007/978-3-030-56877-1_6. 28

[46] James L Massey. Some applications of code duality in cryptography. *Mat. Contemp*, 21(187-209):16th, 2001. 27, 35

[47] 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. 28

[48] Dimitris S Papailiopoulos, Alexandros G Dimakis, and Viveck R Cadambe. Repair optimal erasure codes through hadamard designs. *IEEE Transactions on Information Theory*, 59(5):3021–3037, 2013. 27

[49] Hans Rademacher. Einige sätze über reihen von allgemeinen orthogonalfunktionen. *Mathematische Annalen*, 87(1-2):112–138, 1922. 3, 28

[50] Korlakai Vinayak Rashmi, Nihar B Shah, and P Vijay Kumar. Optimal exact-regenerating codes for distributed storage at the msr and mbr points via a product-matrix construction. *IEEE Transactions on Information Theory*, 57(8):5227–5239, 2011. 27

[51] Mathieu Renauld, François-Xavier Standaert, and Nicolas Veyrat-Charvillon. Algebraic side-channel attacks on the AES: Why time also matters in DPA. In Christophe Clavier and Kris Gaj, editors, *CHES 2009*, volume 5747 of *LNCS*, pages 97–111. Springer, Heidelberg, September 2009. doi:10.1007/978-3-642-04138-9_8. 8, 28

[52] Wolfgang M Schmidt. *Diophantine approximation*. Springer Science & Business Media, 1996. 12, 29

[53] Wolfgang M Schmidt. *Diophantine approximations and Diophantine equations*. Springer, 2006. 12, 29

[54] Adi Shamir. How to share a secret. *Communications of the Association for Computing Machinery*, 22(11):612–613, November 1979. 1

[55] Jerome A Solinas et al. *Generalized mersenne numbers*. Citeseer, 1999. 8

[56] Akshayaram Srinivasan and Prashant Nalini Vasudevan. Leakage resilient secret sharing and applications. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 480–509. Springer, Heidelberg, August 2019. doi:10.1007/978-3-030-26951-7_17. 28

[57] Itzhak Tamo, Zhiying Wang, and Jehoshua Bruck. Zigzag codes: Mds array codes with optimal rebuilding. *IEEE Transactions on Information Theory*, 59(3):1597–1616, 2012. 27

[58] R Titsworth. Coherent detection by quasi-orthogonal square-wave pulse functions (corresp.). *IRE Transactions on Information Theory*, 6(3):410–411, 1960. 3, 11, 28, 40

[59] Samuel S Wagstaff. *The joy of factoring*, volume 68. American Mathematical Soc., 2013. 4

[60] Joseph L Walsh. A closed set of normal orthogonal functions. *American Journal of Mathematics*, 45(1):5–24, 1923. 3, 28

[61] Yingchen Wang, Riccardo Paccagnella, Elizabeth Tang He, Hovav Shacham, Christopher W. Fletcher, and David Kohlbrenner. Hertzbleed: Turning power side-channel attacks into remote timing attacks on x86. In Kevin R. B. Butler and Kurt Thomas, editors, *USENIX Security 2022*, pages 679–697. USENIX Association, August 2022. 8, 28

[62] Zhiying Wang, Itzhak Tamo, and Jehoshua Bruck. Explicit minimum storage regenerating codes. *IEEE Transactions on Information Theory*, 62(8):4466–4480, 2016. 27

[63] Min Ye and Alexander Barg. Explicit constructions of high-rate mds array codes with optimal repair bandwidth. *IEEE Transactions on Information Theory*, 63(4):2001–2014, 2017. 27

[64] Min Ye and Alexander Barg. Explicit constructions of optimal-access mds codes with nearly optimal sub-packetization. *IEEE Transactions on Information Theory*, 63(10):6307–6317, 2017. 27

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

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 $v = \alpha \cdot t \in F$

Figure 5: Our Algorithm to obtain (u, v) from (α_1, α_2) using the LLL-algorithm.

A Solving Simultaneous Diophantine Equations

Figure 5 presents our algorithm. In this section, the "LLL algorithm" refers to the algorithm with the following guarantees.

Imported Theorem 2 (LLL [38, 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 $1 \leqslant t \leqslant 2^{d(d+1)/4} \cdot \varepsilon^{-d}$.

Let us proceed to analyze our algorithm of Figure 5. 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 $2^{d(d+1)/4} \cdot p^{d-1} < B^d$. Therefore we have chosen $B = \lceil 2^{(d+1)/4} p^{1-1/d} \rceil$. 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 Equivalence classes for Evaluation Places

Consider Shamir's secret-sharing scheme among n parties with reconstruction threshold k over the prime field F of order $p \geqslant 3$. The secret-sharing scheme is the Massey secret-sharing scheme [46]

corresponding to the (punctured) Reed-Solomon code with evaluation places $(0, \alpha_1, \alpha_2, \ldots, \alpha_n)$. 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 evaluation places $Z = \alpha_1, \alpha_2, \ldots, \alpha_n$ generates the secret shares $s_1, s_2, \ldots, s_n$, respectively.

Lemma 10 (Equivalence Classes of Evaluation Places)**.** *The (punctured) Reed-Solomon code corresponding to evaluation places $(0, \alpha_1, \alpha_2, \ldots, \alpha_n)$ is identical to the (punctured) Reed-Solomon code corresponding to evaluation places $(0, \Lambda \cdot \alpha_1, \Lambda \cdot \alpha_2, \ldots, \Lambda \cdot \alpha_n)$, for any $\Lambda \in F^*$.*

This proposition is a consequence of the properties of Generalized Reed-Solomon codes [27, 39]. In particular, since the linear codes are identical, the corresponding Massey secret-sharing schemes have identical resilience/vulnerability to attacks. That is, the $\mathsf{ShamirSS}(n, k, (\alpha_1, \alpha_2, \ldots, \alpha_n))$ and the $\mathsf{ShamirSS}(n, k, (\Lambda{\cdot}\alpha_1, \Lambda{\cdot}\alpha_2, \ldots, \Lambda{\cdot}\alpha_n))$ secret-sharing schemes have identical resilience/vulnerability to attacks, for any $\Lambda \in F^*$. Therefore, for given distinct evaluation places $\alpha_1, \alpha_2, \ldots, \alpha_n \in F^*$, we define the equivalence class

$$[\alpha_1 \colon \alpha_2 \colon \cdots \colon \alpha_n] \coloneqq \{(\Lambda \cdot \alpha_1, \Lambda \cdot \alpha_2, \ldots, \Lambda \cdot \alpha_n) : \Lambda \in F^*\}.$$

Determining the security of the evaluation places $(\alpha_1, \ldots, \alpha_n)$ is equivalent to determining the security of *any element* in the equivalence class $[\alpha_1 \colon \cdots \colon \alpha_n]$.

C Proof of Technical Lemmas

C.1 Proof of Lemma 2

Consider the $\mathsf{ShamirSS}(2, 2, (\alpha_1, \alpha_2))$ secret-sharing scheme over a prime field F_p. Consider an arbitrary secret $s \in F_p$ and evaluation places $(u, v) \in [\alpha_1 \colon \alpha_2]$.

$$\begin{aligned}
&2\mathsf{SD}\left(\vec{\mathrm{LSB}}(\mathsf{Share}(0))\ ,\ \vec{\mathrm{LSB}}(\mathsf{Share}(s))\right) \\
&\quad= \sum_{\vec{\ell} \in \{0,1\}^2} \left| \Pr\left[\vec{\mathrm{LSB}}(\mathsf{Share}(0)) = \vec{\ell}\right] - \Pr\left[\vec{\mathrm{LSB}}(\mathsf{Share}(s)) = \vec{\ell}\right] \right| \\
&\quad= \sum_{\vec{\ell} \in \{0,1\}^2} \Bigg| \mathop{\mathbb{E}}_{X}\left[\mathbb{1}_{\mathrm{LSB}^{-1}(\ell_1)}(uX) \cdot \mathbb{1}_{\mathrm{LSB}^{-1}(\ell_2)}(vX)\right] \\
&\qquad\qquad - \mathop{\mathbb{E}}_{X}\left[\mathbb{1}_{\mathrm{LSB}^{-1}(\ell_1)}(uX + s) \cdot \mathbb{1}_{\mathrm{LSB}^{-1}(\ell_2)}(vX + s)\right] \Bigg|
\end{aligned}$$

Claim 1. *For $\ell \in \{0, 1\}$ and $X \in F_p$, we have*

$$\mathbb{1}_{\mathrm{LSB}^{-1}(\ell)}(X) = \frac{1}{2}\left(1 + (-1)^{\ell} \cdot \mathrm{sign}_p(X \cdot 2^{-1})\right).$$

Substituting, we get

$$\begin{aligned}
&2\mathsf{SD}\left(\vec{\mathrm{LSB}}(\mathsf{Share}(0))\ ,\ \vec{\mathrm{LSB}}(\mathsf{Share}(s))\right) \\
&\quad= \sum_{\vec{\ell} \in \{0,1\}^2} \left| \mathop{\mathbb{E}}_{X}\left[\left(\frac{1 + (-1)^{\ell_1}\,\mathrm{sign}_p(uX \cdot 2^{-1})}{2}\right) \cdot \left(\frac{1 + (-1)^{\ell_2}\,\mathrm{sign}_p(vX \cdot 2^{-1})}{2}\right)\right]\right.
\end{aligned}$$

$$
\begin{aligned}
&\quad - \mathop{\mathbb{E}}_{X}\left[\left(\frac{1+(-1)^{\ell_1}\operatorname{sign}_p((uX+s)\cdot 2^{-1})}{2}\right)\cdot\left(\frac{1+(-1)^{\ell_2}\operatorname{sign}_p((vX+s)\cdot 2^{-1})}{2}\right)\right]\Bigg| \\
&= \frac{1}{4}\cdot\sum_{\vec{\ell}\in\{0,1\}^2}\left|\mathop{\mathbb{E}}_{X}\left[\operatorname{sign}_p(uX\cdot 2^{-1})\cdot\operatorname{sign}_p(vX\cdot 2^{-1})\right]-\mathop{\mathbb{E}}_{X}\left[\operatorname{sign}_p((uX+s)\cdot 2^{-1})\cdot\operatorname{sign}_p((vX+s)\cdot 2^{-1})\right]\right| \\
&= \left|\mathop{\mathbb{E}}_{X}\left[\operatorname{sign}_p(uX\cdot 2^{-1})\cdot\operatorname{sign}_p(vX\cdot 2^{-1})\right]-\mathop{\mathbb{E}}_{X}\left[\operatorname{sign}_p((uX+s)\cdot 2^{-1})\cdot\operatorname{sign}_p((vX+s)\cdot 2^{-1})\right]\right| \\
&= \frac{1}{p}\cdot\left|\sum_{X\in F_p}\operatorname{sign}_p(uX\cdot 2^{-1})\cdot\operatorname{sign}_p(vX\cdot 2^{-1})-\sum_{X\in F_p}\operatorname{sign}_p((uX+s)\cdot 2^{-1})\cdot\operatorname{sign}_p((vX+s)\cdot 2^{-1})\right| \\
&= \frac{1}{p}\cdot\left|\sum_{Y\in F_p}\operatorname{sign}_p(uY)\cdot\operatorname{sign}_p(vY)-\sum_{Z\in F_p}\operatorname{sign}_p(uZ)\cdot\operatorname{sign}_p(v(Z-s\cdot 2^{-1}\cdot(u^{-1}-v^{-1})))\right|
\end{aligned}
$$

The last step uses the renaming $X\cdot 2^{-1}\mapsto Y$ (an F automorphism) and $(X+s\cdot u^{-1})\cdot 2^{-1}\mapsto Z$ (an F automorphism).

Therefore,

$$
\mathsf{SD}\left(\mathrm{LSB}(\mathsf{Share}(0))\ ,\ \mathrm{LSB}(\mathsf{Share}(s))\right)=\frac{\left|\Sigma^{(0)}_{u,v}-\Sigma^{(\Delta)}_{u,v}\right|}{2p},
$$

where $\Delta:=\left(s\cdot 2^{-1}\right)\cdot\left(u^{-1}-v^{-1}\right)$, a linear automorphism over F_p.

C.2 Proof of Lemma 3

For $k,\ell,\Delta\in F_p$, the proof follows directly from our definition of $\Sigma^{(\Delta)}_{k,\ell}$, $\operatorname{sign}_p(X)$, $\widetilde{\Sigma}^{(\Delta)}_{k,\ell}$, and $\widetilde{\operatorname{sign}}_p(X)$. The primary observation is that $\operatorname{sign}_p(X)=\widetilde{\operatorname{sign}}_p(X)$, for all $X\in F_p^*$, and $\widetilde{\operatorname{sign}}_p(X=0)=0$.

$$
\begin{aligned}
\Sigma^{(\Delta)}_{k,\ell} &= \sum_{T\in F}\operatorname{sign}_p(kT)\cdot\operatorname{sign}_p(\ell(T-\Delta)) \\
&= \left(\sum_{T\in F}\widetilde{\operatorname{sign}}_p(kT)\cdot\widetilde{\operatorname{sign}}_p(\ell(T-\Delta))\right)+\left(\sum_{T\in\{0,\Delta\}}\operatorname{sign}_p(kT)\cdot\operatorname{sign}_p(\ell(T-\Delta))\right) \\
&= \widetilde{\Sigma}^{(\Delta)}_{k,\ell}+\left(\sum_{T\in\{0,\Delta\}}\operatorname{sign}_p(kT)\cdot\operatorname{sign}_p(\ell(T-\Delta))\right)
\end{aligned}
$$

The expressions above do not require $0,\Delta,\Delta'$ to be distinct.

C.3 Proof of Lemma 4

Claim 2 (Transference Property)**.** *For all $k,\Delta\in F_p, X\in\mathbb{Z}, X=X' \mod p, x=X'/p\in\frac{1}{p}\cdot\mathbb{Z}$, and $\delta=\Delta/p\in\frac{1}{p}\cdot\mathbb{Z}$,*

$$
\widetilde{\operatorname{sign}}_p(k\cdot(X-\Delta))=\varphi(k\cdot(x-\delta)).
$$

Claim 3. *For $k,\Delta\in F_p$ and $x\in\frac{1}{p}\cdot\mathbb{Z}$, define $\delta:=\frac{\Delta}{p}\in\frac{1}{p}\cdot\mathbb{Z}$ and $\delta':=\frac{\operatorname{sign}_p(\Delta)\cdot|\Delta|_p}{p}\in\frac{1}{p}\cdot\mathbb{Z}$, then*

$$
\varphi(k\cdot(x-\delta))=\varphi(k\cdot(x-\delta')).
$$

Proof. Consider the following exhaustive case analysis.

- **Case 1:** $\Delta \in \{0, 1, \ldots, (p-1)/2\}$. In this scenario, $\text{sign}_p(\Delta) = 1, |\Delta|_p = \Delta$ and $\delta = \delta'$. Then, $\varphi(k \cdot (x - \delta)) = \varphi(k \cdot (x - \delta'))$.
- **Case 2:** $\Delta \in \{(p+1)/2, (p+3)/2, \ldots, p-1\}$. In this scenario, $\text{sign}_p(\Delta) = -1, |\Delta|_p = p - \Delta$ and $\delta' = \delta - 1$. Then,

$$\begin{aligned}
\varphi(k \cdot (x - \delta')) =& \varphi(k \cdot (x - \delta + 1)) \\
=& \text{sign}(\sin(2\pi k \cdot (x - \delta + 1))) \\
=& \text{sign}(\sin(2\pi k \cdot (x - \delta) + 2\pi k)) \\
=& \text{sign}(\sin(2\pi k \cdot (x - \delta))) \\
=& \varphi(k \cdot (x - \delta))
\end{aligned}$$

□

□

Claim 4. *For $k \in F_p$ and $x, \delta \in \frac{1}{p} \cdot \mathbb{Z}$, the following holds.*

$$\varphi(k \cdot (x - \delta)) = \text{sign}_p(k) \cdot \varphi(|k|_p \cdot (x - \delta)).$$

Proof. Consider the following exhaustive case analysis.

- **Case 1:** If $k \in \{0, 1, \ldots, (p-1)/2\}$, $|k|_p = k, \text{sign}_p(k) = 1$ and $\varphi(k \cdot (x - \delta)) = \text{sign}_p(k) \cdot \varphi(|k|_p \cdot (x - \delta))$ holds by simply plugging in the values.
- **Case 2:** If $k \in \{(p+1)/2, (p+3)/2, \ldots, p-1\}$, then $|k|_p = p - k$, and $\text{sign}_p(k) = -1$. Substituting in $\text{sign}_p(k) \cdot \varphi(|k|_p \cdot (x - \delta))$, we get

$$\begin{aligned}
\text{sign}_p(k) \cdot \varphi(|k|_p \cdot (x - \delta)) =& \text{sign}(\sin(2\pi |k|_p \cdot (x - \delta))) && (|k|_p = p - k) \\
=& \text{sign}_p(k) \cdot \text{sign}(\sin(2\pi (p - k) \cdot (x - \delta))) \\
=& \text{sign}_p(k) \cdot \text{sign}(\sin(2\pi (px - p\delta) - 2\pi k \cdot (x - \delta))) \\
& && (x, \delta \in \tfrac{1}{p} \cdot \mathbb{Z} \implies px, p\delta \in \mathbb{Z}) \\
=& \text{sign}_p(k) \cdot \text{sign}(\sin(-2\pi k \cdot (x - \delta))) \\
=& -\text{sign}_p(k) \cdot \text{sign}(\sin(2\pi k \cdot (x - \delta))) && (\text{sign}_p(k) = -1) \\
=& \text{sign}(\sin(2\pi k \cdot (x - \delta))) \\
=& \varphi(k \cdot (x - \delta))
\end{aligned}$$

□

□

Given the Transference Property (Claim 2), Claim 3 and Claim 4, we observe that for $k, \ell, \Delta \in F_p, T \in F, t = T/p \in \mathbb{Q}$ and $\delta = \frac{\text{sign}_p(\Delta) \cdot |\Delta|_p}{p} \in \mathbb{Q}$,

$$\begin{aligned}
\widetilde{\Sigma}^{(\Delta)}_{k,\ell} &= \sum_{T \in F} \widetilde{\text{sign}}_p(kT) \cdot \widetilde{\text{sign}}_p(\ell(T - \Delta)) \\
&= \sum_{t \in \left\{\frac{0}{p}, \frac{1}{p}, \ldots, \frac{p-1}{p}\right\}} \text{sign}_p(k) \cdot \text{sign}_p(\ell) \cdot \varphi(|k|_p t) \cdot \varphi(|\ell|_p (t - \delta))
\end{aligned}$$

Definition 1 (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.

Claim 5 (Counting Number of Oscillations). *For any $|k|_p, |\ell|_p \in \{1,\ldots,(p-1)/2\}$,*

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

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

Claim 6 (Sum and Integral Connection). *Fix an integer $n \in \{1,2,\ldots\}$. Let $f\colon [0,1] \to \{\pm 1\}$ be a Boolean function that oscillates H times in the range $[0,1]$. Then,*

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

Proof. Consider an interval $[r, r+1/n)$, for $r \in \{0/n, 1/n, \ldots, (n-1)/n\}$. 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 $r \in \{0/n, 1/n, \ldots, (n-1)/n\}$, we get the claim. □ □

Consider $f(t) = \mathrm{sign}_p(k)\cdot\mathrm{sign}_p(\ell)\cdot\varphi(|k|_p t)\cdot\varphi(|\ell|_p(t-\delta))$, as a consequence of Claim 5 and Claim 6, we conclude Lemma 3.

For any $k,\ell,\Delta \in F_p$ and $\delta = \frac{\mathrm{sign}_p(\Delta)\cdot|\Delta|_p}{p} \in \mathbb{Q}$.

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

Combining the two cases, we get

$$\frac{1}{p}\cdot\widetilde{\Sigma}^{(\Delta)}_{k,\ell} = \mathrm{sign}_p(k)\cdot\mathrm{sign}_p(\ell)\cdot I^{(\delta)}_{|k|_p,|\ell|_p} \pm \frac{4(|k|_p+|\ell|_p)-2}{p}.$$

C.4 Proof of Lemma 5

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

Proposition 3 (Orthogonality of Sine/Cosine Waves [35, Page 38]). *For $k, \ell \in \{1, 2, \dots\}$*

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

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

For the periodic *square wave* [58, 29, 28] $\varphi\colon \mathbb{R} \to \{-1, 0, +1\}$.

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

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

$$\varphi(x) = \sum_{\text{odd } n>0} \frac{4}{\pi n} \cdot \sin(2n\pi x). \tag{12}$$

We prove the following claim for standardization.

Claim 7. *For $k, \ell \in F_p$ and $\delta \in \mathbb{R}$, the following identity holds*

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

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

Proof. Define $\psi^{(\delta)}_{k,\ell}(x) := \varphi(kx) \cdot \varphi(\ell \cdot (x - \delta))$.

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

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

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

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

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

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

□ □

Previously only $I^{(0)}_{k,\ell}$ was studied [58, 29]. In particular, motivated by our application scenario, we study $I^{(\delta)}_{k,\ell}$, for all $\delta \in \mathbb{R}$. To begin our analysis, we assume that k and ℓ are relatively prime.

Claim 8. *For relatively prime $k, \ell \in F_p$ such that $k \cdot \ell$ is even, $I^{(\delta)}_{k,\ell} = 0$, 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,

$$\begin{aligned}
\int_0^1 \sin(2n\pi \cdot kt) \cdot \sin(2m\pi \cdot \ell(t-\delta))\,\mathrm{d}t &= \int_0^{1/2} \sin(2n\pi \cdot kt) \cdot \sin(2m\pi \cdot \ell(t-\delta))\,\mathrm{d}t \\
&\quad + \int_{1/2}^1 \sin(2n\pi \cdot kt) \cdot \sin(2m\pi \cdot \ell(t-\delta))\,\mathrm{d}t \\
&= \int_0^{1/2} \sin(2n\pi \cdot kt) \cdot \sin(2m\pi \cdot \ell(t-\delta))\,\mathrm{d}t \\
&\quad - \int_0^{1/2} \sin(2n\pi \cdot kt) \cdot \sin(2m\pi \cdot \ell(t-\delta))\,\mathrm{d}t \\
&= 0. \qquad (13)
\end{aligned}$$

Now, we can prove the lemma.

$$\begin{aligned}
I_{k,\ell}^{(\delta)} &= \int_0^1 \varphi(kt) \cdot \varphi(\ell(t-\delta))\,\mathrm{d}t \\
&= \frac{16}{\pi^2} \sum_{\text{odd } n>0} \sum_{\text{odd } m>0} \frac{1}{mn} \int_0^1 \sin(2n\pi \cdot kt) \cdot \sin(2m\pi \cdot \ell(t-\delta))\,\mathrm{d}t \qquad \text{(By Equation 12)} \\
&= 0 \qquad \text{(By Equation 13)}
\end{aligned}$$

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 13 holds, and the proof of this case goes through. □ □

Claim 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 10.

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

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 $I_{k,\ell}^{(\delta)}$.

$$\begin{aligned}I_{k,\ell}^{(\delta)} &= \int_0^1 \varphi(kt)\cdot\varphi(\ell(t-\delta))\,\mathrm{d}t \\ &= \frac{16}{\pi^2}\sum_{\text{odd } n>0}\sum_{\text{odd } m>0}\frac{1}{mn}\int_0^1 \sin(2n\pi\cdot kt)\sin(2m\pi\cdot\ell(t-\delta))\,\mathrm{d}t \qquad \text{(By Equation 12)}\end{aligned}$$

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

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

With this observation and Proposition 3, we get

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

Combining Claim 8 and Claim 9, we showed that for relatively prime $k, \ell \in F_p$,

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

Claim 7 generalizes the result to all $k, \ell \in F_p$ by considering $g = \gcd(k, \ell)$. This proves our lemma Lemma 5 that

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

□ □

C.5 Proof of Lemma 1

Consider evaluation places $(u, v) \in [\alpha_1 : \alpha_2]$ and secret $s \in F_p$.

Define $\Delta := \left(s \cdot 2^{-1}\right) \cdot \left(u^{-1} - v^{-1}\right) \in F_p$.

Lemma 2 shows that

$$\mathsf{SD}\left(\mathrm{LSB}(\mathsf{Share}(0)) \ , \ \mathrm{LSB}(\mathsf{Share}(s))\right) = \frac{\left|\Sigma_{u,v}^{(0)} - \Sigma_{u,v}^{(\Delta)}\right|}{2p} \tag{14}$$

Lemma 3 proves

$$\Sigma_{u,v}^{(\Delta)} = \widetilde{\Sigma}_{u,v}^{(\Delta)} + \left(\sum_{T \in \{0,\Delta\}} \mathrm{sign}_p(uT) \cdot \mathrm{sign}_p(v(T-\Delta))\right). \tag{15}$$

Apply Lemma 3 to Equation 14,

$$\begin{aligned} \mathsf{SD}\left(\mathrm{LSB}(\mathsf{Share}(0)) \ , \ \mathrm{LSB}(\mathsf{Share}(s))\right) &= \frac{\left|\widetilde{\Sigma}_{u,v}^{(0)} - \widetilde{\Sigma}_{u,v}^{(\Delta)} - \left(\sum_{T \in \{0,\Delta\} \setminus \{0\}} \mathrm{sign}_p(uT) \cdot \mathrm{sign}_p(v(T-\Delta))\right)\right|}{2p} \\ &= \frac{\left|\widetilde{\Sigma}_{u,v}^{(0)} - \widetilde{\Sigma}_{u,v}^{(\Delta)} - \mathrm{sign}_p(u\Delta)\right|}{2p} \\ &= \frac{\left|\widetilde{\Sigma}_{u,v}^{(0)} - \widetilde{\Sigma}_{u,v}^{(\Delta)}\right|}{2p} \pm \frac{1}{2p} \end{aligned} \tag{16}$$

Define $\delta = \frac{\mathrm{sign}_p(\Delta) \cdot |\Delta|_p}{p} \in \mathbb{Q}$.

Lemma 4 states that

$$\frac{1}{p} \cdot \widetilde{\Sigma}_{u,v}^{(\Delta)} = \mathrm{sign}_p(u) \cdot \mathrm{sign}_p(v) \cdot I_{|u|_p,|v|_p}^{(\delta)} \pm \frac{4(|u|_p + |v|_p) - 2}{p} \tag{17}$$

.

Apply Lemma 4 to Equation 16,

$$\mathsf{SD}\left(\mathrm{LSB}(\mathsf{Share}(0)) \ , \ \mathrm{LSB}(\mathsf{Share}(s))\right) = \frac{\left|I_{|u|_p,|v|_p}^{(0)} - I_{|u|_p,|v|_p}^{(\delta)}\right|}{2} \pm \frac{4(|u|_p + |v|_p) - 2}{p} \pm \frac{1}{2p}. \tag{18}$$

Lemma 5 proves that for $g = \gcd(|u|_p, |v|_p)$,

$$I^{(\delta)}_{|u|_p,|v|_p} = \begin{cases} 0, & \text{if } |u|_p \cdot |v|_p/g^2 \text{ is even} \\ \frac{g^2}{|u|_p \cdot |v|_p} \cdot \cos(2|v|_p \pi \cdot \delta), & \text{if } |u|_p \cdot |v|_p/g^2 \text{ is odd.} \end{cases},$$

Finally, apply Lemma 5 to Equation 18.

$$\mathsf{SD}\left(\mathrm{LSB}(\mathsf{Share}(0))\ ,\ \mathrm{LSB}(\mathsf{Share}(s))\right) =$$
$$\begin{cases} \pm\frac{4(|u|_p+|v|_p)-(3/2)}{p}, & \text{if } |u|_p \cdot |v|_p/g^2 \text{ is even} \\ (1-\cos(2|v|_p\pi\cdot\delta)) \cdot \frac{g^2}{2\cdot|u|_p\cdot|v|_p} \pm \frac{4(|u|_p+|v|_p)-(3/2)}{p}, & \text{if } |u|_p \cdot |v|_p/g^2 \text{ is odd,} \end{cases}$$

Replace $(1-\cos(2|v|_p\pi\cdot\delta))$ with $2\sin^2(|v|_p\pi\cdot\delta)$ concludes our proof.

C.6 Proof of Theorem 1

Consider the $\mathsf{ShamirSS}(2,2,(\alpha_1,\alpha_2))$ secret-sharing scheme over a prime field F_p. For $(u,v) \in [\alpha_1,\alpha_2], g = \gcd(|u|_p,|v|_p), \Delta = (s\cdot 2^{-1})\cdot(u^{-1}-v^{-1}) \in F_p^*$ and $\delta = \frac{\mathrm{sign}_p(\Delta)\cdot|\Delta|_p}{p} \in \mathbb{Q}$,

$$\mathsf{SD}\left(\mathrm{LSB}(\mathsf{Share}(0))\ ,\ \mathrm{LSB}(\mathsf{Share}(s))\right) =$$
$$\begin{cases} \pm\frac{4(|u|_p+|v|_p)-(3/2)}{p}, & \text{if } |u|_p \cdot |v|_p/g^2 \text{ is even} \\ (1-\cos(2|v|_p\pi\cdot\delta)) \cdot \frac{g^2}{2\cdot|u|_p\cdot|v|_p} \pm \frac{4(|u|_p+|v|_p)-(3/2)}{p}, & \text{if } |u|_p \cdot |v|_p/g^2 \text{ is odd.} \end{cases}$$

If $|u|_p \cdot |v|_p/g^2$ is even, then

$$\max_{s\in F} \mathsf{SD}\left(\mathrm{LSB}(\mathsf{Share}(0))\ ,\ \mathrm{LSB}(\mathsf{Share}(s))\right) = \pm\frac{4(|u|_p+|v|_p)-(3/2)}{p}.$$

If $|u|_p\cdot|v|_p/g^2$ is odd, then $\max_{s\in F}\mathsf{SD}\left(\mathrm{LSB}(\mathsf{Share}(0))\ ,\ \mathrm{LSB}(\mathsf{Share}(s))\right)$ is achieved when $\cos(2|v|_p\pi\cdot\delta)$ is closest to -1.

Claim 11. *For prime $p \geqslant 3$ and $v, \Delta \in F_p$,*

$$\cos\left(2\pi\cdot\frac{\mathrm{sign}_p(\Delta)|\Delta|_p|v|_p}{p}\right) = \cos\left(2\pi\cdot\frac{(\Delta\cdot v) \mod p}{p}\right).$$

By Claim 11, $\cos(2|v|_p\pi\cdot\delta) = \cos\left(2\pi\cdot\frac{(\Delta\cdot v) \mod p}{p}\right)$.

For $\Delta = (s\cdot 2^{-1})\cdot(u^{-1}-v^{-1}) \in F_p^*$ and $v \in F_p$, $\Delta\cdot v = (s\cdot 2^{-1})\cdot(u^{-1}v-1) \in F_p$.

$\min_{s\in F_p^*}\cos(2|v|_p\pi\cdot\delta)$ is achieved when $\Delta\cdot v = (s\cdot 2^{-1})\cdot(u^{-1}v-1) = (p-1)/2 \in F_p$ or $\Delta\cdot v = (s\cdot 2^{-1})\cdot(u^{-1}v-1) = (p+1)/2 \in F_p$ which is equivalent as $s = \pm(u^{-1}v-1)^{-1} \in F_p^*$.

When $\Delta\cdot v = (p-1)/2 \in F_p$,

$$\cos(2|v|_p\pi\cdot\delta) = \cos\left(2\pi\frac{(p-1)/2}{p}\right) = -\cos(\pi/p).$$

Similarly, when $\Delta \cdot v = (p+1)/2 \in F_p$,

$$\cos(2|v|_p \pi \cdot \delta) = \cos\left(2\pi \frac{(p+1)/2}{p}\right) = -\cos(\pi/p).$$

Therefore, if $|u|_p \cdot |v|_p / g^2$ is odd, then

$$\max_{s \in F} \mathsf{SD}\left(\mathrm{LSB}(\mathsf{Share}(0))\ ,\ \mathrm{LSB}(\mathsf{Share}(s))\right) = \left(\frac{1+\cos(\pi/p)}{2}\right) \cdot \frac{g^2}{|u|_p \cdot |v|_p} \quad \pm \frac{4(|u|_p + |v|_p) - (3/2)}{p}$$

and the maximum is achieved when $s = \pm(u^{-1}v - 1)^{-1} \in F_p^*$.

Efficient distinguished construction. Consider the following security game (illustrated in the figure below). The attacker picks a secret $s \in F_p^*$ and sends it to the challenger. The challenger picks a random bit $b \in \{0,1\}$. If $b = 0$, the challenger samples (ℓ_1, ℓ_2) from distribution $D_0 := \vec{\mathrm{LSB}}(\mathsf{Share}(0))$ and sends it to the attacker. Otherwise, the challenger samples (ℓ_1, ℓ_2) from distribution $D_1 := \vec{\mathrm{LSB}}(\mathsf{Share}(s))$ and sends it to the attacker. The attacker aims to guess which distribution (ℓ_1, ℓ_2) is sampled from. It uses the maximum likelihood decoder and then returns its guess $\tilde{b}$ to the challenger. The attacker wins the security game if $b = \tilde{b}$.

Attacker		**Challenger**
	$\xrightarrow{\quad s^* \in F_p^* \quad}$	$D_0 = \vec{\mathrm{LSB}}(\mathsf{Share}(0))$
		$D_1 = \vec{\mathrm{LSB}}(\mathsf{Share}(s^*))$
		$b \leftarrow\$ \{0,1\}$
$\tilde{b} = \mathrm{ML}(\ell_1, \ell_2)$	$\xleftarrow{\quad (\ell_1, \ell_2) \quad}$	$(\ell_1, \ell_2) \leftarrow\$ D_b$
	$\xrightarrow{\quad \tilde{b} \quad}$	$b == \tilde{b}$

The maximum likelihood distinguisher outputs $\tilde{b} = 0$ if $\Pr[(\ell_1, \ell_2) | s = 0] \geqslant \Pr[(\ell_1, \ell_2) | s = s^*]$ and $\tilde{b} = 1$ if $\Pr[(\ell_1, \ell_2) | s = 0] < \Pr[(\ell_1, \ell_2) | s = s^*]$. The output depends on sign $(\Pr[(\ell_1, \ell_2) | s = 0] - \Pr[(\ell_1, \ell_2) | s = s$

For evaluation places (u, v), where $|u|_p \cdot |v|_p / g^2$ is odd and $g = \gcd(|u|_p, |v|_p)$, and $\Delta = (s^* \cdot 2^{-1}) \cdot (u^{-1} - v^{-1}) \in F^*$, we get

$$\begin{aligned}
&\Pr[(\ell_1, \ell_2) | s = 0] - \Pr[(\ell_1, \ell_2) | s = s^*] \\
&= (-1)^{\ell_1 + \ell_2} \cdot \frac{\Sigma^{(0)}_{u,v} - \Sigma^{(\Delta)}_{u,v}}{4p} && \text{(Appendix C.1)} \\
&= (-1)^{\ell_1 + \ell_2} \cdot \frac{\widetilde{\Sigma}^{(0)}_{u,v} - \widetilde{\Sigma}^{(\Delta)}_{u,v} - \mathrm{sign}_p(u\Delta)}{4p} && \text{(Lemma 3)} \\
&= (-1)^{\ell_1 + \ell_2} \cdot \frac{\widetilde{\Sigma}^{(0)}_{u,v} - \widetilde{\Sigma}^{(\Delta)}_{u,v}}{4p} \pm \frac{1}{4p} \\
&= \frac{(-1)^{\ell_1 + \ell_2} \cdot \mathrm{sign}_p(u) \cdot \mathrm{sign}_p(v)}{4} \cdot \left(I^{(0)}_{|u|_p, |v|_p} - I^{(\delta)}_{|u|_p, |v|_p} \pm 2 \cdot \frac{4(|u|_p + |v|_p) - (3/2)}{p} \right) \\
& && \text{(Lemma 4, } \delta = \tfrac{\mathrm{sign}_p(\Delta)|\Delta|_p}{p}\text{)}
\end{aligned}$$

$$= \frac{(-1)^{\ell_1+\ell_2} \cdot \mathrm{sign}_p(u) \cdot \mathrm{sign}_p(v)}{4} \cdot \left(\sin^2(|v|_p \pi \cdot \delta) \cdot \frac{g^2}{|u|_p \cdot |v|_p} \pm 2 \cdot \frac{4(|u|_p + |v|_p) - (3/2)}{p} \right)$$

(Lemma 5)

Consider attacker picks $s = \pm(u^{-1} \cdot v - 1)^{-1} \in F^*$ such that

$$\begin{aligned} &\Pr[(\ell_1, \ell_2) | s = 0] - \Pr[(\ell_1, \ell_2) | s = s^*] \\ =&\frac{(-1)^{\ell_1+\ell_2} \cdot \mathrm{sign}_p(u) \cdot \mathrm{sign}_p(v)}{4} \cdot \left(\cos^2(\pi/2p) \cdot \frac{g^2}{|u|_p \cdot |v|_p} \pm 2 \cdot \frac{4(|u|_p + |v|_p) - (3/2)}{p} \right) \end{aligned}$$

Since $\mathsf{SD}\left(\mathrm{LSB}(\mathsf{Share}(0)) \ , \ \mathrm{LSB}(\mathsf{Share}(s))\right) > \frac{4(|u|_p+|v|_p)-(3/2)}{p}$ by our assumption, then

$$\cos^2(\pi/2p) \cdot \frac{g^2}{|u|_p \cdot |v|_p} - 2 \cdot \frac{4(|u|_p + |v|_p) - (3/2)}{p} > 0.$$

Hence,

$$\mathrm{sign}\left(\Pr[(\ell_1, \ell_2) | s = 0] - \Pr[(\ell_1, \ell_2) | s = s^*]\right) = (-1)^{\ell_1+\ell_2} \cdot \mathrm{sign}_p(u) \cdot \mathrm{sign}_p(v).$$

There exists an efficient maximum likelihood distinguisher computing $(-1)^{\ell_1+\ell_2} \cdot \mathrm{sign}_p(u) \cdot \mathrm{sign}_p(v)$. If $(-1)^{\ell_1+\ell_2} \cdot \mathrm{sign}_p(u) \cdot \mathrm{sign}_p(v) > 0$, then the maximum likelihood distinguisher outputs $\tilde{b} = 0$. Otherwise, it outputs $\tilde{b} = 1$.

C.7 Proof of inequality in Corollary 2

Our objective is to prove the following inequality for primes $p \geqslant 11$.

$$\frac{\frac{1}{4} \cdot \sqrt{p} \cdot \ln p + \frac{3}{2} \cdot \sqrt{p} + \frac{1}{2}}{p - 2} \leqslant \frac{\ln p}{4\sqrt{p}} + \frac{5/2}{\sqrt{p}}.$$

We simplify this inequality into a simpler equivalent inequality.

$$\begin{aligned} &\frac{\frac{1}{4} \cdot \sqrt{p} \cdot \ln p + \frac{3}{2} \cdot \sqrt{p} + \frac{1}{2}}{p - 2} \leqslant \frac{\ln p}{4\sqrt{p}} + \frac{5/2}{\sqrt{p}} \\ \iff &\cancel{\frac{1}{4} \cdot \sqrt{p} \cdot \ln p} + \cancel{\frac{3}{2} \cdot \sqrt{p}} + \frac{1}{2} \leqslant \cancel{\frac{1}{4} \cdot \sqrt{p} \cdot \ln p} + \frac{5}{\cancel{2}_{1}} \cdot \sqrt{p} - \frac{1}{2} \cdot \frac{\ln p}{\sqrt{p}} - \frac{5}{\sqrt{p}} \\ \iff &\frac{1}{2}\sqrt{p} + \frac{1}{2}\ln p \leqslant \sqrt{p} \leqslant p - 5. \end{aligned}$$

Thus, it suffices to prove the final inequality. Toward this objective, observe that

1. $\ln p \leqslant \sqrt{p}$, for $p \geqslant 2$, and
2. $\sqrt{p} \leqslant p - 5$, for $p \geqslant 11$.

Then, for $p \geqslant 11$,

$$\frac{1}{2}\sqrt{p} + \frac{1}{2}\ln p \leqslant \sqrt{p} \leqslant p - 5.$$

Therefore,

$$\frac{\frac{1}{4} \cdot \sqrt{p} \cdot \ln p + \frac{3}{2} \cdot \sqrt{p} + \frac{1}{2}}{p - 2} \leqslant \frac{\ln p}{4\sqrt{p}} + \frac{5/2}{\sqrt{p}}$$

for all $p \geqslant 11$.

C.8 Additional Proof for Corollary 3

Claim 12. *For* $\mathsf{ShamirSS}(2,2,\vec{\alpha}=(\alpha_1,\alpha_2))$ *and secret* $s\in F$*, define* $\mathrm{err}:=\frac{8^{5/4}}{\sqrt{p}}+\frac{13/2}{p}$*. Consider* $|\alpha_1|_p,|\alpha_2|_p<\lceil 8^{1/4}\sqrt{p}\rceil$ *and* $|\alpha_1|_p\cdot|\alpha_2|_p/g^2$ *is odd with* $g=\gcd(|\alpha_1|_p,|\alpha_2|_p)$*. When* $\varepsilon_{\mathrm{LSB}}(\vec{\alpha})>2\cdot\mathrm{err}$*,*

$$\mathrm{sign}\left(\varepsilon_{\mathrm{LSB}}^{(\mathrm{OUR})}(\vec{\alpha})\right)=\mathrm{sign}\left(\frac{\Sigma_{\alpha_1,\alpha_2}^{(0)}-\Sigma_{\alpha_1,\alpha_2}^{(\Delta)}}{p}\right)$$

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

Proof.

$$\begin{aligned}\frac{\Sigma_{\alpha_1,\alpha_2}^{(0)}-\Sigma_{\alpha_1,\alpha_2}^{(\Delta)}}{p}&=\frac{\widetilde{\Sigma}_{\alpha_1,\alpha_2}^{(0)}-\widetilde{\Sigma}_{\alpha_1,\alpha_2}^{(\Delta)}-\mathrm{sign}_p(\alpha_1\Delta)}{p} && \text{(Lemma 3)}\\ &=\mathrm{sign}_p(\alpha_1)\cdot\mathrm{sign}_p(\alpha_2)\cdot\left(I_{|\alpha_1|_p,|\alpha_2|_p}^{(0)}-I_{|\alpha_1|_p,|\alpha_2|_p}^{(\delta)}\right)\pm 2\cdot\frac{4(|\alpha_1|_p+|\alpha_2|_p)-(3/2)}{p}\\ & && \text{(Lemma 4, } \delta=\tfrac{\mathrm{sign}_p(\Delta)|\Delta|_p}{p}\text{)}\end{aligned}$$

Equivalently,

$$\frac{\Sigma_{\alpha_1,\alpha_2}^{(0)}-\Sigma_{\alpha_1,\alpha_2}^{(\Delta)}}{p}\pm 2\cdot\frac{4(|\alpha_1|_p+|\alpha_2|_p)-(3/2)}{p}=\mathrm{sign}_p(\alpha_1)\cdot\mathrm{sign}_p(\alpha_2)\cdot\left(I_{|\alpha_1|_p,|\alpha_2|_p}^{(0)}-I_{|\alpha_1|_p,|\alpha_2|_p}^{(\delta)}\right).$$

For $|\alpha_1|_p,|\alpha_2|_p<\lceil 8^{1/4}\sqrt{p}\rceil$,

$$2\cdot\frac{4(|\alpha_1|_p+|\alpha_2|_p)-(3/2)}{p}\leqslant 2\cdot\mathrm{err}<\varepsilon_{\mathrm{LSB}}(\vec{\alpha})=\frac{\left|\Sigma_{\alpha_1,\alpha_2}^{(0)}-\Sigma_{\alpha_1,\alpha_2}^{(\Delta)}\right|}{p}.$$

which implies that $\pm 2\cdot\frac{4(|\alpha_1|_p+|\alpha_2|_p)-(3/2)}{p}$ does not change the sign of $\frac{\Sigma_{\alpha_1,\alpha_2}^{(0)}-\Sigma_{\alpha_1,\alpha_2}^{(\Delta)}}{p}$,

$$\mathrm{sign}\left(\frac{\Sigma_{\alpha_1,\alpha_2}^{(0)}-\Sigma_{\alpha_1,\alpha_2}^{(\Delta)}}{p}\pm 2\cdot\frac{4(|\alpha_1|_p+|\alpha_2|_p)-(3/2)}{p}\right)=\mathrm{sign}\left(\frac{\Sigma_{\alpha_1,\alpha_2}^{(0)}-\Sigma_{\alpha_1,\alpha_2}^{(\Delta)}}{p}\right)$$

Hence,

$$\begin{aligned}\mathrm{sign}\left(\frac{\Sigma_{\alpha_1,\alpha_2}^{(0)}-\Sigma_{\alpha_1,\alpha_2}^{(\Delta)}}{p}\right)&=\mathrm{sign}\left(\mathrm{sign}_p(\alpha_1)\cdot\mathrm{sign}_p(\alpha_2)\cdot\left(I_{|\alpha_1|_p,|\alpha_2|_p}^{(0)}-I_{|\alpha_1|_p,|\alpha_2|_p}^{(\delta)}\right)\right)\\ &=\mathrm{sign}\left(\mathrm{sign}_p(\alpha_1)\cdot\mathrm{sign}_p(\alpha_2)\cdot\left(\sin^2(|v|_p\pi\cdot\delta)\cdot\frac{g^2}{|u|_p\cdot|v|_p}\right)\right) && \text{(Lemma 5)}\\ &=\mathrm{sign}\left(\mathrm{sign}_p(\alpha_1)\cdot\mathrm{sign}_p(\alpha_2)\right) && (\sin^2(|v|_p\pi\cdot\delta)\cdot\tfrac{g^2}{|u|_p\cdot|v|_p}>0)\\ &=\mathrm{sign}\left(\varepsilon_{\mathrm{LSB}}^{(\mathrm{OUR})}(\vec{\alpha})\right)\end{aligned}$$

. □ □

For any secret $s \in F$, let us first define the distinguishing advantage of the maximum likelihood decoder as

$$\varepsilon_{\mathrm{LSB}}(\vec{\alpha}; s) := \frac{\Sigma^{(0)}_{\alpha_1,\alpha_2} - \Sigma^{(\Delta)}_{\alpha_1,\alpha_2}}{p}$$

where $\Delta := (s \cdot 2^{-1}) \cdot (\alpha_1^{-1} - \alpha_2^{-1}) \in F$ and the estimate $\varepsilon^{(\mathrm{OUR})}_{\mathrm{LSB}}(\vec{\alpha}; s) \in [0,1]$ satisfying

$$\varepsilon^{(\mathrm{OUR})}_{\mathrm{LSB}}(\vec{\alpha}; s) = \varepsilon_{\mathrm{LSB}}(\vec{\alpha}; s) \quad \pm \mathrm{err}$$

where $\mathrm{err} := \frac{8^{5/4}}{\sqrt{p}} + \frac{13/2}{p}$. Given Claim 12, we know that for any secret $s \in F$,

$$\varepsilon_{\mathrm{LSB}}(\vec{\alpha}; s) \geqslant \varepsilon^{(\mathrm{OUR})}_{\mathrm{LSB}}(\vec{\alpha}; s) - \mathrm{err}. \tag{19}$$

and

$$\varepsilon^{(\mathrm{OUR})}_{\mathrm{LSB}}(\vec{\alpha}; s) \geqslant \varepsilon_{\mathrm{LSB}}(\vec{\alpha}; s) - \mathrm{err}. \tag{20}$$

Consider secret $s^* \in F$ that achieves the maximum $\varepsilon^{(\mathrm{OUR})}_{\mathrm{LSB}}(\vec{\alpha}; s)$, we define $\varepsilon^{(\mathrm{OUR})}_{\mathrm{LSB}}(\vec{\alpha}; s^*)$ as follows

$$\varepsilon^{(\mathrm{OUR})}_{\mathrm{LSB}}(\vec{\alpha}) := \max_{s \in F} \varepsilon^{(\mathrm{OUR})}_{\mathrm{LSB}}(\vec{\alpha}; s) = \varepsilon^{(\mathrm{OUR})}_{\mathrm{LSB}}(\vec{\alpha}; s^*).$$

Similarly, consider $\tilde{s}^* \in F$ that reaches maximum $\varepsilon_{\mathrm{LSB}}(\vec{\alpha}; s)$, we define $\varepsilon_{\mathrm{LSB}}(\vec{\alpha}; s^*)$ as

$$\varepsilon_{\mathrm{LSB}}(\vec{\alpha}) := \max_{s \in F} \varepsilon_{\mathrm{LSB}}(\vec{\alpha}; s) = \varepsilon_{\mathrm{LSB}}(\vec{\alpha}; \tilde{s}^*).$$

$$\begin{aligned}
\varepsilon_{\mathrm{LSB}}(\vec{\alpha}; s^*) \geqslant & \varepsilon^{(\mathrm{OUR})}_{\mathrm{LSB}}(\vec{\alpha}; s^*) - \mathrm{err} = \varepsilon^{(\mathrm{OUR})}_{\mathrm{LSB}}(\vec{\alpha}) - \mathrm{err} && \text{(Equation 19)} \\
\geqslant & \varepsilon^{(\mathrm{OUR})}_{\mathrm{LSB}}(\vec{\alpha}; \tilde{s}^*) - \mathrm{err} && (\varepsilon^{(\mathrm{OUR})}_{\mathrm{LSB}}(\vec{\alpha}; s^*) = \max_{s \in F} \varepsilon^{(\mathrm{OUR})}_{\mathrm{LSB}}(\vec{\alpha}; s)) \\
\geqslant & \varepsilon_{\mathrm{LSB}}(\vec{\alpha}; \tilde{s}^*) - 2 \cdot \mathrm{err} && \text{(Equation 20)} \\
= & \varepsilon_{\mathrm{LSB}}(\vec{\alpha}) - 2 \cdot \mathrm{err} > 0
\end{aligned}$$

Therefore, the distinguishing advantage of the maximum likelihood decoder is

$$\geqslant \varepsilon^{(\mathrm{OUR})}_{\mathrm{LSB}}(\vec{\alpha}) - \mathrm{err} \geqslant \varepsilon_{\mathrm{LSB}}(\vec{\alpha}) - 2 \cdot \mathrm{err}.$$

C.9 Proof of Lemma 7

$$\begin{aligned}
& 2\mathsf{SD}\left(\mathrm{P\vec{H}YS}_{i,j}(\mathsf{Share}(0)) \,,\, \mathrm{P\vec{H}YS}_{i,j}(\mathsf{Share}(s))\right) \\
&= \sum_{\vec{\ell} \in \{0,1\}^2} \left| \Pr\left[\mathrm{P\vec{H}YS}_{i,j}(\mathsf{Share}(0)) = \vec{\ell}\right] - \Pr\left[\mathrm{P\vec{H}YS}_{i,j}(\mathsf{Share}(s)) = \vec{\ell}\right] \right| \\
&= \sum_{\vec{\ell} \in \{0,1\}^2} \Bigg| \mathop{\mathbb{E}}_{x} \left[\mathbb{1}_{\mathrm{PHYS}_i^{-1}(\ell_1)}(\alpha_1 x) \cdot \mathbb{1}_{\mathrm{PHYS}_j^{-1}(\ell_2)}(\alpha_2 x) \right] \\
&\qquad\qquad - \mathop{\mathbb{E}}_{x} \left[\mathbb{1}_{\mathrm{PHYS}_i^{-1}(\ell_1)}(\alpha_1 x + s) \cdot \mathbb{1}_{\mathrm{PHYS}_j^{-1}(\ell_2)}(\alpha_2 x + s) \right] \Bigg| \\
&= \sum_{\vec{\ell} \in \{0,1\}^2} \left| \mathop{\mathbb{E}}_{x} \left[\mathbb{1}_{\mathrm{PHYS}_i^{-1}(0)}(\alpha_1 x) \cdot \mathbb{1}_{\mathrm{PHYS}_j^{-1}(0)}(\alpha_2 x) \right] \right.
\end{aligned}$$

$$- \mathop{\mathbb{E}}_{x}\left[\mathbb{1}_{\mathrm{PHYS}_i^{-1}(0)}(\alpha_1 x+s)\cdot\mathbb{1}_{\mathrm{PHYS}_j^{-1}(0)}(\alpha_2 x+s)\right]\Bigg|$$

(Using the fact that $\mathbb{1}_{\mathrm{PHYS}_k^{-1}(1)} = 1 - \mathbb{1}_{\mathrm{PHYS}_k^{-1}(0)}$)

$$= 4\cdot\left|\mathop{\mathbb{E}}_{x}\left[\mathbb{1}_{E_i}(\alpha_1 x)\cdot\mathbb{1}_{E_j}(\alpha_2 x)\right] - \mathop{\mathbb{E}}_{x}\left[\mathbb{1}_{E_i}(\alpha_1 x+s)\cdot\mathbb{1}_{E_j}(\alpha_2 x+s)\right]\right|$$

$$= 4\cdot\left|\mathop{\mathbb{E}}_{x}\left[\mathbb{1}_{E\cdot(2^i)}(\alpha_1 x)\cdot\mathbb{1}_{E\cdot(2^j)}(\alpha_2 x)\right] - \mathop{\mathbb{E}}_{x}\left[\mathbb{1}_{E\cdot(2^i)}(\alpha_1 x+s)\cdot\mathbb{1}_{E\cdot(2^j)}(\alpha_2 x+s)\right]\right|$$

(By Proposition 2)

$$= 4\cdot\Bigg|\mathop{\mathbb{E}}_{x}\left[\mathbb{1}_{E}(2^{-i}\alpha_1 x)\cdot\mathbb{1}_{E}(2^{-j}\alpha_2 x)\right]$$

$$- \mathop{\mathbb{E}}_{x}\left[\mathbb{1}_{E}(2^{-i}\alpha_1 x+2^{-i}s)\cdot\mathbb{1}_{E}(2^{-j}\alpha_2 x+2^{-j}s)\right]\Bigg| \tag{21}$$

At this point, we introduce the following variable renaming.

Claim 13. *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

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

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 21 as follows.

$$= 4\cdot\Bigg|\mathop{\mathbb{E}}_{x}\left[\mathbb{1}_{E}(2^{-i}\alpha_1 x)\cdot\mathbb{1}_{E}(2^{-j}\alpha_2 x)\right]$$

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

$$= \varepsilon_{\mathrm{LSB}}(2^{-i}\alpha_1, 2^{-j}\alpha_2).$$

Therefore, we conclude that the insecurity of $\mathsf{ShamirSS}(2,2,(\alpha_1,\alpha_2))$ secret-sharing scheme against the $\vec{\mathrm{PHYS}}_{i,j}$ 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.

C.10 Proof of maximum insecurity bound in Corollary 7

Observe that $\lambda - \lfloor\lambda/2\rfloor = \lceil\lambda/2\rceil \geqslant \lfloor\lambda/2\rfloor$. Therefore, for $1 \leqslant i \leqslant \lambda - 1$, we have

$$\varepsilon_{\mathrm{LSB}}(2^i\cdot\alpha_1,\alpha_2) \leqslant \frac{4\cdot 2^t + 4\cdot(2^{\lambda-t}-1)-2}{p}.$$

All that remains is to prove that this upper bound also holds for $\varepsilon_{\mathrm{LSB}}(2^0\cdot\alpha_1,\alpha_2)$.

For $\lambda = 2$, we have $t = 1$. In this case, one can verify that the upper bound holds.

$$\varepsilon(2^0 \cdot \alpha_1, \alpha_2) \leqslant \frac{4 \cdot 2^t + 4 \cdot (2^{\lambda - t} - 1) - 2}{p}.$$

For $\lambda \geqslant 3$, note that if p is a Mersenne prime, then λ must be odd. Therefore, we have $\lambda - t = t + 1$ and $p = 2^{2t+1} - 1$. Therefore, we need to prove that

$$\varepsilon(2^0 \cdot \alpha_1, \alpha_2) = \frac{1}{2^t - 1} + \frac{4 + 4 \cdot (2^t - 1) - 2}{p} \leqslant \frac{4 \cdot 2^t + 4 \cdot (2^{t+1} - 1) - 2}{p}.$$

This bound is equivalent to proving

$$\begin{aligned}
& \frac{1}{2^t - 1} \leqslant \frac{4 \cdot (2^{t+1} - 1)}{2^{2t+1} - 1} \\
\iff \quad & \frac{1}{T - 1} \leqslant \frac{4 \cdot (2T - 1)}{2T^2 - 1} && \text{(substitute } T = 2^t\text{)} \\
\iff \quad & 0 \leqslant 6T^2 - 12T + 5 \\
\iff \quad & 1/6 \leqslant (T - 1)^2,
\end{aligned}$$

which is true for all $t \geqslant 1$.

So, the overall maximum is

$$\frac{4 \cdot 2^{\lfloor \lambda/2 \rfloor} + 4 \cdot (2^{\lceil \lambda/2 \rceil} - 1) - 2}{p} = \frac{4 \cdot (2^{\lfloor \lambda/2 \rfloor} + 2^{\lceil \lambda/2 \rceil}) - 6}{p}.$$

D Proof of Lemma 8

Consider the $\mathsf{ShamirSS}(3, 2, (\alpha_1, \alpha_2, \alpha_3))$ secret-sharing scheme over a prime field F_p. Let $s \in F$ be an arbitrary secret. Let us begin by proving the insecurity of $\mathsf{ShamirSS}(3, 2, (\alpha_1, \alpha_2, \alpha_3))$ against LSB leakage attack and then generalize to arbitrary physical bit leakage attack.

D.1 Against LSB Leakage

$$\begin{aligned}
& \mathsf{2SD}\left(\vec{\mathrm{LSB}}(\mathsf{Share}(0)) \,,\, \vec{\mathrm{LSB}}(\mathsf{Share}(s))\right) \\
&= \sum_{\vec{\ell} \in \{0,1\}^3} \left| \Pr\left[\vec{\mathrm{LSB}}(\mathsf{Share}(0)) = \vec{\ell}\right] - \Pr\left[\vec{\mathrm{LSB}}(\mathsf{Share}(s)) = \vec{\ell}\right] \right| \\
&= \sum_{\vec{\ell} \in \{0,1\}^3} \Bigg| \mathop{\mathbb{E}}_{X} \left[\mathbb{1}_{\mathrm{LSB}^{-1}(\ell_1)}(\alpha_1 X) \cdot \mathbb{1}_{\mathrm{LSB}^{-1}(\ell_2)}(\alpha_2 X) \cdot \mathbb{1}_{\mathrm{LSB}^{-1}(\ell_3)}(\alpha_3 X) \right] \\
&\qquad\qquad - \mathop{\mathbb{E}}_{X} \left[\mathbb{1}_{\mathrm{LSB}^{-1}(\ell_1)}(\alpha_1 X + s) \cdot \mathbb{1}_{\mathrm{LSB}^{-1}(\ell_2)}(\alpha_2 X + s) \cdot \mathbb{1}_{\mathrm{LSB}^{-1}(\ell_3)}(\alpha_3 X + s) \right] \Bigg| \\
&= \sum_{\vec{\ell} \in \{0,1\}^3} \left| \mathop{\mathbb{E}}_{X} \left[\prod_{i=1}^{3} \frac{\left(1 + (-1)^{\ell_i} \operatorname{sign}_p(\alpha_i X \cdot 2^{-1})\right)}{2} \right] - \mathop{\mathbb{E}}_{X} \left[\prod_{i=1}^{3} \frac{\left(1 + (-1)^{\ell_i} \operatorname{sign}_p((\alpha_i X + s) \cdot 2^{-1})\right)}{2} \right] \right| \\
& \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{(Claim 1)}
\end{aligned}$$

$$= \sum_{\vec{\ell}\in\{0,1\}^3} \left| \mathop{\mathbb{E}}_{Y} \left[\prod_{i=1}^{3} \frac{\left(1+(-1)^{\ell_i}\operatorname{sign}_p(\alpha_i Y)\right)}{2} \right] - \mathop{\mathbb{E}}_{Y} \left[\prod_{i=1}^{3} \frac{\left(1+(-1)^{\ell_i}\operatorname{sign}_p(\alpha_i Y+t)\right)}{2} \right] \right|$$

$$(X \cdot 2^{-1} \mapsto Y, t = s \cdot 2^{-1})$$

$$= \frac{1}{8} \cdot \frac{1}{p} \sum_{\vec{\ell}\in\{0,1\}^3} \left| \sum_{Y\in F_p} \prod_{i=1}^{3} \left(1+(-1)^{\ell_i} \cdot \operatorname{sign}_p(\alpha_i Y)\right) - \sum_{Y\in F} \prod_{i=1}^{3} \left(1+(-1)^{\ell_i} \cdot \operatorname{sign}_p(\alpha_i Y+t)\right) \right|$$

Observe that

$$\begin{aligned}\prod_{i=1}^{3} \left(1+(-1)^{\ell_i} \cdot \operatorname{sign}_p(\alpha_i Y+t)\right) = 1 &+ \left(\sum_{i=1}^{3} (-1)^{\ell_i} \cdot \operatorname{sign}_p(\alpha_i Y+t) \right) \\ &+ \left(\sum_{i<j} (-1)^{\ell_i+\ell_j} \cdot \operatorname{sign}_p(\alpha_i Y+t) \operatorname{sign}_p(\alpha_j Y+t) \right) \\ &+ (-1)^{\ell_1+\ell_2+\ell_3} \cdot \operatorname{sign}_p(\alpha_1 Y+t) \operatorname{sign}_p(\alpha_2 Y+t) \operatorname{sign}_p(\alpha_3 Y+t)\end{aligned}$$

Since for $\alpha_i, t, Y \in F_p$, $\alpha_i \cdot Y + t$ is an automorphism on F, then for all $\alpha_i, t \in F$

$$\sum_{Y\in F_p} \operatorname{sign}_p(\alpha_i Y+t) = 1.$$

Hence,

$$\begin{aligned}&2\mathsf{SD}\left(\vec{\mathrm{LSB}}(\mathsf{Share}(0)),\ \vec{\mathrm{LSB}}(\mathsf{Share}(s))\right) \\ &= \frac{1}{8p} \cdot \sum_{\vec{\ell}\in\{0,1\}^3} \left| \left(\sum_{1\leqslant i<j\leqslant 3} (-1)^{\ell_i+\ell_j} \cdot \sum_{Y\in F_p} \operatorname{sign}_p(\alpha_i Y) \operatorname{sign}_p(\alpha_j Y) \right) \right. \\ &\qquad - \left(\sum_{1\leqslant i<j\leqslant 3} (-1)^{\ell_i+\ell_j} \cdot \sum_{Y\in F_p} \operatorname{sign}_p(\alpha_i Y+t) \operatorname{sign}_p(\alpha_j Y+t) \right) \\ &\qquad + (-1)^{\ell_1+\ell_2+\ell_3} \sum_{Y\in F_p} \operatorname{sign}_p(\alpha_1 Y) \operatorname{sign}_p(\alpha_2 Y) \operatorname{sign}_p(\alpha_3 Y) \\ &\qquad \left. -(-1)^{\ell_1+\ell_2+\ell_3} \sum_{Y\in F_p} \operatorname{sign}_p(\alpha_1 Y+t) \operatorname{sign}_p(\alpha_2 Y+t) \operatorname{sign}_p(\alpha_3 Y+t) \right| \\ &= \frac{1}{8p} \cdot \sum_{\vec{\ell}\in\{0,1\}^3} \left| \sum_{1\leqslant i<j\leqslant 3} (-1)^{\ell_i+\ell_j} \cdot \left(\sum_{Y\in F_p} \operatorname{sign}_p(\alpha_i Y) \operatorname{sign}_p(\alpha_j Y) - \sum_{Y\in F_p} \operatorname{sign}_p(\alpha_i Y+t) \operatorname{sign}_p(\alpha_j Y+t) \right) \right. \\ &\qquad + (-1)^{\ell_1+\ell_2+\ell_3} \cdot \sum_{Y\in F_p} \operatorname{sign}_p(\alpha_1 Y) \operatorname{sign}_p(\alpha_2 Y) \operatorname{sign}_p(\alpha_3 Y) \\ &\qquad \left. -(-1)^{\ell_1+\ell_2+\ell_3} \cdot \sum_{Y\in F_p} \operatorname{sign}_p(\alpha_1 Y+t) \operatorname{sign}_p(\alpha_2 Y+t) \operatorname{sign}_p(\alpha_3 Y+t) \right|\end{aligned}$$

$$=\frac{1}{8p}\cdot\sum_{\vec{\ell}\in\{0,1\}^3}\left|\sum_{1\leqslant i<j\leqslant 3}(-1)^{\ell_i+\ell_j}\cdot\left(\Sigma^{(0)}_{\alpha_i,\alpha_j}-\Sigma^{(\Delta_{i,j})}_{\alpha_i,\alpha_j}\right)+(-1)^{\ell_1+\ell_2+\ell_3}\cdot\left(\Sigma^{(0,0)}_{\alpha_1,\alpha_2,\alpha_3}-\Sigma^{(\Delta_{1,2},\Delta_{1,3})}_{\alpha_1,\alpha_2,\alpha_3}\right)\right|$$

$$\leqslant\frac{1}{p}\cdot\sum_{1\leqslant i<j\leqslant 3}\left|\Sigma^{(0)}_{\alpha_i,\alpha_j}-\Sigma^{(\Delta_{i,j})}_{\alpha_i,\alpha_j}\right|+\frac{1}{p}\cdot\left|\Sigma^{(0,0)}_{\alpha_1,\alpha_2,\alpha_3}-\Sigma^{(\Delta_{1,2},\Delta_{1,3})}_{\alpha_1,\alpha_2,\alpha_3}\right| \qquad \text{(Triangle Inequiality)}$$

where $\Delta_{i,j}:=(s\cdot 2^{-1})\cdot(\alpha_i^{-1}-\alpha_j^{-1})$ for all $1\leqslant i<j\leqslant 3$.

Then,

$$\mathsf{SD}\left(\vec{\mathrm{LSB}}(\mathsf{Share}(0))\ ,\ \vec{\mathrm{LSB}}(\mathsf{Share}(s))\right)\leqslant\sum_{1\leqslant i<j\leqslant 3}\frac{\left|\Sigma^{(0)}_{\alpha_i,\alpha_j}-\Sigma^{(\Delta_{i,j})}_{\alpha_i,\alpha_j}\right|}{2p}+\frac{\left|\Sigma^{(0,0)}_{\alpha_1,\alpha_2,\alpha_3}-\Sigma^{(\Delta_{1,2},\Delta_{1,3})}_{\alpha_1,\alpha_2,\alpha_3}\right|}{2p}$$

$$=\sum_{1\leqslant i<j\leqslant 3}\varepsilon_{\mathrm{LSB}}(\alpha_i,\alpha_j)+\frac{\left|\Sigma^{(0,0)}_{\alpha_1,\alpha_2,\alpha_3}-\Sigma^{(\Delta_{1,2},\Delta_{1,3})}_{\alpha_1,\alpha_2,\alpha_3}\right|}{2p}$$

Consider the following generalization of Lemma 3.

Claim 14. *For $k,\ell,m\in\{1,2,\dots\}$ and $\Delta,\Delta'\in\{0,1,\dots,(p-1)\}$,*

$$\Sigma^{(\Delta,\Delta')}_{k,\ell,m}=\widetilde{\Sigma}^{(\Delta,\Delta')}_{k,\ell,m}\quad+\left(\sum_{T\in\{0,\Delta,\Delta'\}}\mathrm{sign}_p(kT)\cdot\mathrm{sign}_p(\ell(T-\Delta))\cdot\mathrm{sign}_p(m(T-\Delta'))\right).$$

Proof.

$$\begin{aligned}\Sigma^{(\Delta,\Delta')}_{k,\ell,m}&=\sum_{X\in F_p}\mathrm{sign}_p(k\cdot X)\cdot\mathrm{sign}_p(\ell\cdot(X-\Delta))\cdot\mathrm{sign}_p(m\cdot(X-\Delta'))\\&=\sum_{X\in F_p}\widetilde{\mathrm{sign}_p}(k\cdot X)\cdot\widetilde{\mathrm{sign}_p}(\ell\cdot(X-\Delta))\cdot\widetilde{\mathrm{sign}_p}(m\cdot(X-\Delta'))\\&\qquad+\sum_{X\in\{0,\Delta,\Delta'\}}\mathrm{sign}_p(k\cdot X)\cdot\mathrm{sign}_p(\ell\cdot(X-\Delta))\cdot\mathrm{sign}_p(m\cdot(X-\Delta'))\\&=\widetilde{\Sigma}^{(\Delta,\Delta')}_{k,\ell,m}\quad+\left(\sum_{T\in\{0,\Delta,\Delta'\}}\mathrm{sign}_p(kT)\cdot\mathrm{sign}_p(\ell(T-\Delta))\cdot\mathrm{sign}_p(m(T-\Delta'))\right)\end{aligned}$$

□ □

Claim 15. *For $k,\ell,m\in\{1,2,\dots\}$ and $\Delta,\Delta'\in\{0,1,\dots,(p-1)\}$,*

$$\widetilde{\Sigma}^{(\Delta,\Delta')}_{k,\ell,m}=0.$$

Proof.

$$\begin{aligned}\widetilde{\Sigma}^{(\Delta,\Delta')}_{k,\ell,m}&=\sum_{X\in F_p}\widetilde{\mathrm{sign}_p}(k\cdot X)\cdot\widetilde{\mathrm{sign}_p}(\ell\cdot(X-\Delta))\cdot\widetilde{\mathrm{sign}_p}(m\cdot(X-\Delta'))\\&=\sum_{X\in F_p}\varphi(k\cdot X/p)\cdot\varphi(\ell\cdot(X-\Delta)/p)\cdot\varphi(m\cdot(X-\Delta')/p)\qquad(\widetilde{\mathrm{sign}_p}(X)=\varphi(X/p))\end{aligned}$$

$$= \sum_{x \in \{\frac{0}{p}, \frac{1}{p}, \ldots, \frac{p-1}{p}\}} \varphi(k \cdot x) \cdot \varphi(\ell \cdot (x - \Delta/p)) \cdot \varphi(m \cdot (x - \Delta'/p))$$

Recall the Fourier expansion of $\varphi(x)$ is as follows.

$$\varphi(x) = \sum_{\text{odd } n>0} \frac{4}{\pi n} \cdot \sin(2n\pi x). \tag{22}$$

Substituting $\varphi(x)$ in the expression for $\widetilde{\Sigma}^{(\Delta,\Delta')}_{k,\ell,m}$ with Equation 22,

$$\begin{aligned}
&\widetilde{\Sigma}^{(\Delta,\Delta')}_{k,\ell,m} \\
&= \sum_{x \in \{\frac{0}{p}, \frac{1}{p}, \ldots, \frac{p-1}{p}\}} \sum_{\text{odd } n_1,n_2,n_3>0} \frac{4^3}{\pi^3 n_1 n_2 n_3} \cdot \sin(2n_1\pi kx) \cdot \sin(2n_2\pi\ell \cdot (x - \Delta/p)) \cdot \sin(2n_3\pi m \cdot (x - \Delta'/p))
\end{aligned}$$

Consider the following trignometric identity,

$$\sin A \cdot \sin B \cdot \sin C = \frac{\sin(A - B + C) - \sin(A - B - C) - \sin(A + B + C) + \sin(A + B - C)}{4}.$$

Substituting $A = 2n_1\pi kx, B = 2n_2\pi\ell \cdot (x - \Delta/p), C = 2n_3\pi m \cdot (x - \Delta'/p)$, we get

$$\begin{aligned}
&4 \cdot \sin(2n_1\pi kx) \cdot \sin(2n_2\pi\ell \cdot (x - \Delta/p)) \cdot \sin(2n_3\pi m \cdot (x - \Delta'/p)) \\
&\quad = \sin(2\pi x \cdot (n_1 k - n_2\ell + n_3 m) + 2\pi \cdot (n_2\ell\Delta - n_3 m\Delta')/p) \\
&\quad\quad - \sin(2\pi x \cdot (n_1 k - n_2\ell - n_3 m) + 2\pi \cdot (n_2\ell\Delta + n_3 m\Delta')/p) \\
&\quad\quad - \sin(2\pi x \cdot (n_1 k + n_2\ell + n_3 m) + 2\pi \cdot (-n_2\ell\Delta - n_3 m\Delta')/p) \\
&\quad\quad + \sin(2\pi x \cdot (n_1 k + n_2\ell - n_3 m) + 2\pi \cdot (-n_2\ell\Delta + n_3 m\Delta')/p)
\end{aligned}$$

Define $a_1 = n_1 k - n_2\ell + n_3 m, a_2 = n_1 k - n_2\ell - n_3 m, a_3 = n_1 k + n_2\ell + n_3 m, a_4 = n_1 k + n_2\ell - n_3 m$ where $a_1, a_2, a_3, a_4 \in \mathbb{Z}$ and define $b_1 = n_2\ell\Delta - n_3 m\Delta', b_2 = n_2\ell\Delta + n_3 m\Delta', b_3 = n_2\ell\Delta + n_3 m\Delta', b_4 = -n_2\ell\Delta + n_3 m\Delta'$ where $b_1, b_2, b_3, b_4 \in \mathbb{Z}$ as well.

$$\begin{aligned}
&\sum_{x \in \{\frac{0}{p}, \frac{1}{p}, \ldots, \frac{p-1}{p}\}} \sin(2\pi \cdot a_1 x + 2\pi \cdot b_1/p) \\
&= \sum_{y \in \{\frac{0}{p}, \frac{1}{p}, \ldots, \frac{p-1}{p}\}} \sin(2\pi \cdot (y + b_1/p)) && (a_1 \in \mathbb{Z}) \\
&= \sum_{y \in \{\frac{0}{p}, \frac{1}{p}, \ldots, \frac{p-1}{p}\}} \sin(2\pi \cdot y) && (b_1/p \in 1/p \cdot \mathbb{Z}) \\
&= 0
\end{aligned}$$

Note that the last equality holds because for all $i \in \{1, 2, \ldots, (p-1)/2\}$, we have

$$\sin(2\pi \cdot (p - i)/p) = -\sin(2\pi \cdot i/p).$$

Similarly, we can obtain that

$$\sum_{x\in\{\frac{0}{p},\frac{1}{p},\ldots,\frac{p-1}{p}\}} \sin(2\pi\cdot a_2 x + 2\pi\cdot b_2/p) = 0$$
$$\sum_{x\in\{\frac{0}{p},\frac{1}{p},\ldots,\frac{p-1}{p}\}} \sin(2\pi\cdot a_3 x + 2\pi\cdot b_3/p) = 0$$
$$\sum_{x\in\{\frac{0}{p},\frac{1}{p},\ldots,\frac{p-1}{p}\}} \sin(2\pi\cdot a_4 x + 2\pi\cdot b_4/p) = 0$$

Combining all terms, we get

$$\sum_{x\in\{\frac{0}{p},\frac{1}{p},\ldots,\frac{p-1}{p}\}} \sin(2n_1\pi k x)\cdot\sin(2n_2\pi\ell\cdot(x-\Delta/p))\cdot\sin(2n_3\pi m\cdot(x-\Delta'/p)) = 0$$

which implies that

$$\widetilde{\Sigma}^{(\Delta,\Delta')}_{k,\ell,m} = 0.$$

□ □

Apply Claim 15 to Claim 14, we get

Claim 16. *For $k,\ell,m\in\{1,2,\ldots\}$ and $\Delta,\Delta'\in\{0,1,\ldots,(p-1)\}$,*

$$\Sigma^{(\Delta,\Delta')}_{k,\ell,m} = \left(\sum_{T\in\{0,\Delta,\Delta'\}} \mathrm{sign}_p(kT)\cdot\mathrm{sign}_p(\ell(T-\Delta))\cdot\mathrm{sign}_p(m(T-\Delta'))\right).$$

Claim 16 implies that

$$\begin{aligned}\Sigma^{(0,0)}_{\alpha_1,\alpha_2,\alpha_3} &- \Sigma^{(\Delta_{1,2},\Delta_{1,3})}_{\alpha_1,\alpha_2,\alpha_3}\\ &= -\sum_{T\in\{\Delta_{1,2},\Delta_{1,3}\}} \mathrm{sign}_p(k\cdot T)\cdot\mathrm{sign}_p(\ell\cdot(T-\Delta_{1,2}))\cdot\mathrm{sign}_p(m\cdot(T-\Delta_{1,3})).\end{aligned}$$

Then,

$$\left|\Sigma^{(0,0)}_{\alpha_1,\alpha_2,\alpha_3} - \Sigma^{(\Delta_{1,2},\Delta_{1,3})}_{\alpha_1,\alpha_2,\alpha_3}\right| \leqslant 2.$$

Therefore,

$$\varepsilon_{\mathrm{LSB}}(\vec{\alpha}) := \mathsf{SD}\left(\vec{\mathrm{LSB}}(\mathsf{Share}(0))\ ,\ \vec{\mathrm{LSB}}(\mathsf{Share}(s))\right) \leqslant \sum_{1\leqslant i<j\leqslant 3}\varepsilon_{\mathrm{LSB}}(\alpha_i,\alpha_j) + \frac{1}{p}.$$

D.2 Against arbitrary physical bit leakage attack

Let $\mathrm{PHYS}_i\colon F\to\{0,1\}$ be defined as in Section 5. $\mathrm{PHYS}_i\colon F\to\{0,1\}$ is the function that outputs the i-th least significant bit in the binary representation.

We begin by considering a generalization of Proposition 2.

Claim 17. *For all $i\in\{0,1,\ldots,\lambda-1\}$, we have $\mathrm{PHYS}_i(x) = \mathrm{LSB}(x\cdot 2^{-i})$ for $x\in F$.*

$$
\begin{aligned}
&\mathsf{2SD}\left(\vec{\mathrm{PHYS}}_{i_1,i_2,i_3}(\mathsf{Share}(0))\ ,\ \vec{\mathrm{PHYS}}_{i_1,i_2,i_3}(\mathsf{Share}(s))\right)\\
&\quad=\sum_{\vec{\ell}\in\{0,1\}^3}\left|\Pr\left[\vec{\mathrm{PHYS}}_{i_1,i_2,i_3}(\mathsf{Share}(0))=\vec{\ell}\right]-\Pr\left[\vec{\mathrm{PHYS}}_{i_1,i_2,i_3}(\mathsf{Share}(s))=\vec{\ell}\right]\right|\\
&\quad=\sum_{\vec{\ell}\in\{0,1\}^3}\Bigg|\mathop{\mathbb{E}}_{X}\left[\mathbb{1}_{\mathrm{PHYS}_{i_1}^{-1}(\ell_1)}(\alpha_1X)\cdot\mathbb{1}_{\mathrm{PHYS}_{i_2}^{-1}(\ell_2)}(\alpha_2X)\cdot\mathbb{1}_{\mathrm{PHYS}_{i_3}^{-1}(\ell_3)}(\alpha_3X)\right]\\
&\qquad\qquad-\mathop{\mathbb{E}}_{x}\left[\mathbb{1}_{\mathrm{PHYS}_{i_1}^{-1}(\ell_1)}(\alpha_1X+s)\cdot\mathbb{1}_{\mathrm{PHYS}_{i_2}^{-1}(\ell_2)}(\alpha_2X+s)\cdot\mathbb{1}_{\mathrm{PHYS}_{i_3}^{-1}(\ell_3)}(\alpha_3X+s)\right]\Bigg|\\
&\quad=\sum_{\vec{\ell}\in\{0,1\}^3}\Bigg|\mathop{\mathbb{E}}_{X}\left[\mathbb{1}_{\mathrm{LSB}^{-1}(\ell_1)}(\alpha_1X\cdot2^{-i_1})\cdot\mathbb{1}_{\mathrm{LSB}^{-1}(\ell_2)}(\alpha_2X\cdot2^{-i_2})\cdot\mathbb{1}_{\mathrm{LSB}^{-1}(\ell_3)}(\alpha_3X\cdot2^{-i_3})\right]\\
&\quad-\mathop{\mathbb{E}}_{X}\left[\mathbb{1}_{\mathrm{LSB}^{-1}(\ell_1)}((\alpha_1X+s)\cdot2^{-i_1})\cdot\mathbb{1}_{\mathrm{LSB}^{-1}(\ell_2)}((\alpha_2X+s)\cdot2^{-i_2})\cdot\mathbb{1}_{\mathrm{LSB}^{-1}(\ell_3)}((\alpha_3X+s)\cdot2^{-i_3})\right]\Bigg|\\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\text{(By Claim 17)}\\
&\quad=\sum_{\vec{\ell}\in\{0,1\}^3}\left|\mathop{\mathbb{E}}_{X}\left[\prod_{j=1}^{3}\frac{\left(1+(-1)^{\ell_j}\operatorname{sign}_p(\alpha_jX\cdot2^{-i_j})\right)}{2}\right]-\mathop{\mathbb{E}}_{X}\left[\prod_{j=1}^{3}\frac{\left(1+(-1)^{\ell_j}\operatorname{sign}_p((\alpha_jX+s)\cdot2^{-i_j})\right)}{2}\right]\right|\\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\text{(Claim 1)}\\
&\quad=\frac{1}{8}\cdot\frac{1}{p}\sum_{\vec{\ell}\in\{0,1\}^3}\Bigg|\sum_{X\in F_p}\prod_{j=1}^{3}\left(1+(-1)^{\ell_j}\operatorname{sign}_p(\alpha_jX\cdot2^{-i_j})\right)\\
&\qquad\qquad\qquad\qquad-\sum_{X\in F_p}\prod_{j=1}^{3}\left(1+(-1)^{\ell_j}\operatorname{sign}_p((\alpha_jX+s)\cdot2^{-i_j})\right)\Bigg|
\end{aligned}
$$

Observe that

$$
\begin{aligned}
&\prod_{j=1}^{3}\left(1+(-1)^{\ell_j}\cdot\operatorname{sign}_p((\alpha_jX+s)\cdot2^{-i_j})\right)\\
&\quad=1+\left(\sum_{j=1}^{3}(-1)^{\ell_j}\cdot\operatorname{sign}_p((\alpha_jX+s)\cdot2^{-i_j})\right)\\
&\qquad+\left(\sum_{1\leqslant j_1<j_2\leqslant3}(-1)^{\ell_{j_1}+\ell_{j_2}}\cdot\operatorname{sign}_p((\alpha_{j_1}X+s)\cdot2^{-i_{j_1}})\operatorname{sign}_p((\alpha_{j_2}X+s)\cdot2^{-i_{j_2}})\right)\\
&\qquad+(-1)^{\ell_1+\ell_2+\ell_3}\cdot\operatorname{sign}_p((\alpha_1X+s)\cdot2^{-i_1})\operatorname{sign}_p((\alpha_2X+s)\cdot2^{-i_2})\operatorname{sign}_p((\alpha_3X+s)\cdot2^{-i_3})
\end{aligned}
$$

Since for $\alpha_j,s,X\in F_p$, $\alpha_j\cdot2^{-i_j}\cdot X+s\cdot2^{-i_j}$ is an automorphism on F, then

$$
\sum_{X\in F_p}\operatorname{sign}_p(\alpha_j\cdot2^{-i_j}\cdot X+s\cdot2^{-i_j})=1.
$$

Hence,

$$
\mathsf{2SD}\left(\vec{\mathrm{PHYS}}_{i_1,i_2,i_3}(\mathsf{Share}(0))\ ,\ \vec{\mathrm{PHYS}}_{i_1,i_2,i_3}(\mathsf{Share}(s))\right)
$$

$$=\frac{1}{8p}\cdot\sum_{\vec{\ell}\in\{0,1\}^3}\left|\sum_{1\leqslant j_1<j_2\leqslant 3}(-1)^{\ell_{j_1}+\ell_{j_2}}\cdot\left(\sum_{X\in F_p}\operatorname{sign}_p(\alpha_{j_1}X\cdot 2^{-i_{j_1}})\operatorname{sign}_p(\alpha_{j_2}X\cdot 2^{-i_{j_2}})\right.\right.$$
$$\left.-\sum_{X\in F_p}\operatorname{sign}_p((\alpha_{j_1}X+s)\cdot 2^{-i_{j_1}})\operatorname{sign}_p((\alpha_{j_2}X+s)\cdot 2^{-i_{j_2}})\right)$$
$$+(-1)^{\ell_1+\ell_2+\ell_3}\cdot\left(\sum_{X\in F_p}\operatorname{sign}_p(\alpha_1X\cdot 2^{-i_1})\operatorname{sign}_p(\alpha_2X\cdot 2^{-i_2})\operatorname{sign}_p(\alpha_3X\cdot 2^{-i_2})\right.$$
$$\left.\left.-\sum_{X\in F_p}\operatorname{sign}_p((\alpha_1X+s)\cdot 2^{-i_1})\operatorname{sign}_p((\alpha_2X+s)\cdot 2^{-i_2})\operatorname{sign}_p((\alpha_3X+s)\cdot 2^{-i_3})\right)\right| \tag{23}$$

At this point, we introduce the following variable renaming.

Claim 18.

$$\operatorname{sign}_p(\alpha_1X\cdot 2^{-i_1}+2^{-i_1}\cdot s)\cdot\operatorname{sign}_p(\alpha_2X\cdot 2^{-i_2}+2^{-i_2}\cdot s)$$
$$=\operatorname{sign}_p(\alpha_1Y\cdot 2^{-i_1}+s')\cdot\operatorname{sign}_p(\alpha_2Y\cdot 2^{-i_2}+s')$$

where

$$Y:=X+\frac{2^{-i_1}-2^{-i_2}}{2^{-i_1}\alpha_1-2^{-i_2}\alpha_2},\qquad \textit{and}\qquad s':=\frac{2^{-i_1}2^{-i_2}(\alpha_1-\alpha_2)}{2^{-i_1}\alpha_1-2^{-i_2}\alpha_2}\cdot s$$

The proof of this claim is by direct substitution. Note that $s\mapsto s'$ is an automorphism over F^* and s' depends on i_{j_1} and i_{j_2}. Then, for

$$Y:=X+\frac{2^{-i_{j_1}}-2^{-i_{j_2}}}{2^{-i_{j_1}}\alpha_{j_1}-2^{-i_{j_2}}\alpha_{j_2}},\qquad \text{and}\qquad s':=\frac{2^{-i_{j_1}}2^{-i_{j_2}}(\alpha_{j_1}-\alpha_{j_2})}{2^{-i_{j_1}}\alpha_{j_1}-2^{-i_{j_2}}\alpha_{j_2}}\cdot s$$

$$\sum_{X\in F_p}\operatorname{sign}_p(\alpha_{j_1}X\cdot 2^{-i_{j_1}})\operatorname{sign}_p(\alpha_{j_2}X\cdot 2^{-i_{j_2}})-\sum_{X\in F_p}\operatorname{sign}_p((\alpha_{j_1}X+s)\cdot 2^{-i_{j_1}})\operatorname{sign}_p((\alpha_{j_2}X+s)\cdot 2^{-i_{j_2}})$$
$$=\sum_{X\in F_p}\operatorname{sign}_p(\alpha_{j_1}X\cdot 2^{-i_{j_1}})\operatorname{sign}_p(\alpha_{j_2}X\cdot 2^{-i_{j_2}})-\sum_{Y\in F_p}\operatorname{sign}_p(\alpha_{j_1}Y\cdot 2^{-i_{j_1}}+s')\operatorname{sign}_p(\alpha_{j_2}Y\cdot 2^{-i_{j_2}}+s')$$
(By Claim 18)
$$=\sum_{X\in F_p}\operatorname{sign}_p(\alpha'_{j_1}X)\operatorname{sign}_p(\alpha'_{j_2}X)-\sum_{Y\in F_p}\operatorname{sign}_p(\alpha'_{j_1}Y+s')\operatorname{sign}_p(\alpha'_{j_2}Y+s')$$
$(\alpha_{j_1}\cdot 2^{-i_{j_1}}\mapsto\alpha'_{j_1}$ and $\alpha_{j_2}\cdot 2^{-i_{j_2}}\mapsto\alpha'_{j_2})$
$$=\Sigma^{(0)}_{\alpha'_{j_1},\alpha'_{j_2}}-\Sigma^{(\Delta_{j_1,j_2})}_{\alpha'_{j_1},\alpha'_{j_2}} \tag{24}$$

where $\Delta_{j_1,j_2}=(s'\cdot 2^{-1})\cdot((\alpha'_{j_1})^{-1}-(\alpha'_{j_2})^{-1})$.

Define $\alpha'_1:=\alpha_1\cdot 2^{-i_1},\alpha'_2:=\alpha_2\cdot 2^{-i_2},\alpha'_3:=\alpha_3\cdot 2^{-i_3}$. Then,

$$\sum_{X\in F_p}\operatorname{sign}_p(\alpha_1X\cdot 2^{-i_1})\operatorname{sign}_p(\alpha_2X\cdot 2^{-i_2})\operatorname{sign}_p(\alpha_3X\cdot 2^{-i_2})$$

$$
\begin{aligned}
&\quad - \sum_{X\in F_p} \operatorname{sign}_p((\alpha_1 X+s)\cdot 2^{-i_1}) \operatorname{sign}_p((\alpha_2 X+s)\cdot 2^{-i_2}) \operatorname{sign}_p((\alpha_3 X+s)\cdot 2^{-i_3}) \\
&= \sum_{X\in F_p} \operatorname{sign}_p(\alpha_1' X) \operatorname{sign}_p(\alpha_2' X) \operatorname{sign}_p(\alpha_3' X) \\
&\quad - \sum_{X\in F_p} \operatorname{sign}_p(\alpha_1' X + s\cdot 2^{-i_1}) \operatorname{sign}_p(\alpha_2' X + s\cdot 2^{-i_2}) \operatorname{sign}_p(\alpha_3' X + s\cdot 2^{-i_3}) \\
&= \sum_{X\in F_p} \operatorname{sign}_p(\alpha_1' X) \operatorname{sign}_p(\alpha_2' X) \operatorname{sign}_p(\alpha_3' X) \\
&\quad - \sum_{Y\in F_p} \operatorname{sign}_p(\alpha_1' Y) \operatorname{sign}_p(\alpha_2'(Y-\Delta)) \operatorname{sign}_p(\alpha_3'(Y-\Delta')) \quad (X + s\cdot 2^{-i_1}\cdot(\alpha_1')^{-1} \mapsto Y) \\
&= \Sigma^{(0,0)}_{\alpha_1',\alpha_2',\alpha_3'} - \Sigma^{(\Delta,\Delta')}_{\alpha_1',\alpha_2',\alpha_3'} \qquad (25)
\end{aligned}
$$

where $\Delta := s\cdot 2^{-i_1}\cdot(\alpha_1')^{-1} - s\cdot 2^{-i_2}\cdot(\alpha_2')^{-1}$ and $\Delta' := s\cdot 2^{-i_1}\cdot(\alpha_1')^{-1} - s\cdot 2^{-i_3}\cdot(\alpha_3')^{-1}$.

By Claim 16, we get

$$
\begin{aligned}
&\Sigma^{(0,0)}_{\alpha_1',\alpha_2',\alpha_3'} - \Sigma^{(\Delta,\Delta')}_{\alpha_1',\alpha_2',\alpha_3'} \\
&\quad = - \sum_{T\in\{\Delta,\Delta'\}} \operatorname{sign}_p(\alpha_1'\cdot T)\cdot \operatorname{sign}_p(\alpha_2'\cdot(T-\Delta))\cdot \operatorname{sign}_p(\alpha_3'\cdot(T-\Delta'))
\end{aligned}
$$

Then,

$$
\left|\Sigma^{(0,0)}_{\alpha_1',\alpha_2',\alpha_3'} - \Sigma^{(\Delta,\Delta')}_{\alpha_1',\alpha_2',\alpha_3'}\right| \leqslant 2.
$$

Substituting Equation 24 and Equation 25 to the expression in Equation 23 as follows.

$$
\begin{aligned}
&2\mathsf{SD}\left(\vec{\mathrm{PHYS}}(\mathsf{Share}(0))\ ,\ \vec{\mathrm{PHYS}}(\mathsf{Share}(s))\right) \\
&\quad = \frac{1}{8p}\cdot \sum_{\vec{\ell}\in\{0,1\}^3} \left| \sum_{1\leqslant j_1<j_2\leqslant 3} (-1)^{\ell_{j_1}+\ell_{j_2}} \cdot \left(\Sigma^{(0)}_{\alpha_{j_1}',\alpha_{j_2}'} - \Sigma^{(\Delta_{j_1,j_2})}_{\alpha_{j_1}',\alpha_{j_2}'}\right) \right. \\
&\qquad\qquad \left. +(-1)^{\ell_1+\ell_2+\ell_3}\cdot\left(\Sigma^{(0,0)}_{\alpha_1',\alpha_2',\alpha_3'} - \Sigma^{(\Delta,\Delta')}_{\alpha_1',\alpha_2',\alpha_3'}\right)\right|
\end{aligned}
$$

where $\Delta_{j_1,j_2} = (s'\cdot 2^{-1})\cdot((\alpha_{j_1}')^{-1} - (\alpha_{j_2}')^{-1})$, $\Delta := s\cdot 2^{-i_1}\cdot(\alpha_1')^{-1} - s\cdot 2^{-i_2}\cdot(\alpha_2')^{-1}$ and $\Delta' := s\cdot 2^{-i_1}\cdot(\alpha_1')^{-1} - s\cdot 2^{-i_3}\cdot(\alpha_3')^{-1}$.

By triangle inequality,

$$
\mathsf{SD}\left(\vec{\mathrm{PHYS}}(\mathsf{Share}(0))\ ,\ \vec{\mathrm{PHYS}}(\mathsf{Share}(s))\right) \leqslant \sum_{1\leqslant j_1<j_2\leqslant 3} \frac{\left|\Sigma^{(0)}_{\alpha_{j_1}',\alpha_{j_2}'} - \Sigma^{(\Delta_{j_1,j_2})}_{\alpha_{j_1}',\alpha_{j_2}'}\right|}{2p} + \frac{1}{p}
$$

Define $\varepsilon := \max_{1\leqslant i<j\leqslant 3}\{\varepsilon_{\mathrm{PHYS}}(\alpha_i,\alpha_j)\}$. Thus,

$$
\varepsilon_{\mathrm{PHYS}}(\vec{\alpha}) \leqslant 3\cdot\varepsilon + \frac{1}{p}.
$$

E Proof of Theorem 2

E.1 Fourier Basics

E.1.1 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 11 (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 4. *Let $S, T \subseteq F$ be a partition of F. For all $\alpha \in F$,*

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

Proposition 5 (Properties of Fourier Coefficients)**.** *For all $S \subseteq F$ and $x, \alpha \in F$, it holds that*

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

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

E.2 Some Preparatory Results

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

Proposition 6. *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, $\vec{\tau}\colon F^n \to \{0,1\}^n$, the following identity holds for any secret $s \in F$.*

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

Proof. The following identity is known in the literature (see [40] for 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 4, $\widehat{\mathbb{1}_{\tau_i^{-1}(\ell_i)}}(\gamma_i) = \widehat{\mathbb{1}_{\tau_i^{-1}(1-\ell_i)}}(\gamma_i)$ 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

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

Therefore, we have

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

as desired. □ □

Proposition 7. *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.

$$\begin{aligned} &\sum_{t \in F} \prod_{i=1}^n \left(\widehat{\mathbb{1}_{A_i \cdot \beta_i}}(t) \cdot \omega^{s \cdot t \cdot \beta_i} \right) \\ &= \sum_{t \in F} \prod_{i}^n \left(\frac{1}{p} \sum_{x_i \in F} \mathbb{1}_{A_i \cdot \beta_i}(x_i) \cdot \omega^{-t \cdot x_i} \cdot \omega^{s \cdot t \cdot \beta_i} \right) && \text{(Fourier expansion)} \\ &= \frac{1}{p^n} \sum_{t \in F} \sum_{\vec{x} \in F^n} \left(\prod_{i=1}^n \mathbb{1}_{A_i \cdot \beta_i}(x_i) \cdot \omega^{-t \cdot x_i} \cdot \omega^{s \cdot t \cdot \beta_i} \right) && \text{(Linearity)} \\ &= \frac{1}{p^n} \sum_{\vec{x} \in F^n} \left(\prod_{i=1}^n \mathbb{1}_{A_i \cdot \beta_i}(x_i) \right) \sum_{t \in F} \omega^{-t \cdot (x_1 + \cdots + x_n - s \cdot (\beta_1 + \cdots + \beta_n))} && \text{(Linearity)} \\ &= \frac{1}{p^{n-1}} \sum_{\substack{\vec{x} \in F^n : \\ x_1 + \cdots + x_n = s \cdot (\beta_1 + \cdots + \beta_n)}} \left(\prod_{i=1}^n \mathbb{1}_{A_i \cdot \beta_i}(x_i) \right) && \text{(Sum of roots of unity)} \end{aligned}$$

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

$$\begin{aligned}
&\frac{1}{p^{n-1}} \sum_{x_2,\ldots,x_n \in F} \mathbb{1}_{A_1 \cdot \beta_1}(s \cdot (\beta_1 + \cdots + \beta_n) - (x_2 + \cdots + x_n)) \cdot \prod_{i=2}^{n} \mathbb{1}_{A_i \cdot \beta_i}(x_i) \\
&= \frac{1}{p^{n-1}} \sum_{x_n \in A_n \cdot \beta_n} \sum_{x_2 \in F} \mathbb{1}_{A_2 \cdot \beta_2}(x_2) \cdot \mathbb{1}_{A_1 \cdot \beta_1}(s \cdot (\beta_1 + \cdots + \beta_n) - (x_2 + \cdots + x_n)) \\
&\qquad \vdots \\
&\qquad x_3 \in A_3 \cdot \beta_3
\end{aligned}$$

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

$$\begin{aligned}
&\sum_{x_2 \in F} \mathbb{1}_{A_2 \cdot \beta_2}(x_2) \cdot \mathbb{1}_{A_1 \cdot \beta_1}(s \cdot (\beta_1 + \cdots + \beta_n) - (x_2 + \cdots + x_n)) \\
&= \sum_{x_2 \in F} \mathbb{1}_{A_2 \cdot \beta_2}(x_2) \cdot \mathbb{1}_{A_1 \cdot \beta_1 - s \cdot (\beta_1 + \cdots + \beta_n) + (x_3 + \cdots + x_n)}(-x_2) \\
&= \sum_{x_2 \in F} \mathbb{1}_{A_2 \cdot \beta_2}(x_2) \cdot \mathbb{1}_{-A_1 \cdot \beta_1 + s \cdot (\beta_1 + \cdots + \beta_n) - (x_3 + \ldots + x_n)}(x_2) \\
&= \mathsf{card}(A_2 \cdot \beta_2 \cap (-A_1 \cdot \beta_1 - (x_3 + \ldots + x_n) + s \cdot (\beta_1 + \cdots + \beta_n))) \\
&= \mathsf{card}(A_2 \cdot \beta_2 + (x_3 + \cdots + x_n) - s \cdot (\beta_1 + \cdots + \beta_n) \cap (-A_1 \cdot \beta_1)) \\
&= \mathsf{card}(A_2 \cdot \beta_2) - \mathsf{card}(A_2 \cdot \beta_2 + (x_3 + \cdots + x_n) - s \cdot (\beta_1 + \cdots + \beta_n) \cap A_1 \cdot \beta_1) \\
&= \mathsf{card}(A_2) - \mathsf{card}(A_2 \cdot \beta_2 + (x_3 + \cdots + x_n) - s \cdot (\beta_1 + \cdots + \beta_n) \cap A_1 \cdot \beta_1)\,,
\end{aligned}$$

which completes the proof. □ □

E.3 Putting things together and proving Theorem 2

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.

$$\begin{aligned}
&2\mathsf{SD}\left(\vec{\tau}(\mathsf{Share}(0))\,,\ \vec{\tau}(\mathsf{Share}(s))\right) \\
&= 2^n \cdot \left| \sum_{\vec{\gamma} \in \mathcal{C}_0^{\perp} \setminus \vec{0}} \prod_{i=1}^{n} \widehat{\mathbb{1}_{\tau_i^{-1}(0)}}(\gamma_i) \cdot \left(1 - \omega^{s \cdot (\gamma_1 + \cdots + \gamma_n)}\right) \right| && (\textit{Proposition 6}) \\
&= 2^n \cdot \left| \sum_{t \in F^*} \prod_{i=1}^{n} \widehat{\mathbb{1}_{A_i}}(t \cdot \beta_i) \cdot \left(1 - \omega^{s \cdot t \cdot (\beta_1 + \cdots + \beta_n)}\right) \right| \\
&= 2^n \cdot \left| \sum_{t \in F^*} \prod_{i=1}^{n} \widehat{\mathbb{1}_{A_i \cdot \beta_i}}(t) - \sum_{t \in F^*} \prod_{i=1}^{n} \widehat{\mathbb{1}_{A_i \cdot \beta_i}}(t) \cdot \omega^{s \cdot t \cdot \beta_i} \right|
\end{aligned}$$

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

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

Then, it follows from Proposition 7 that

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

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

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

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 2 in Appendix C.1, we have

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

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

$$\left|\Sigma^{\left(\Delta^{(0)}_{x_3,\ldots,x_n}\right)}_{\beta_1^{-1},\beta_2^{-1}} - \Sigma^{\left(\Delta^{(s)}_{x_3,\ldots,x_n}\right)}_{\beta_1^{-1},\beta_2^{-1}}\right| \leqslant 2\varepsilon p. \tag{26}$$

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.

F Some Technical Results

F.1 Proof of Lemma 9

Define

$$\gamma_1 := \alpha_1 \prod_{j \neq 1} (\alpha_1 - \alpha_j)$$
$$\gamma_2 := \alpha_2 \prod_{j \neq 2} (\alpha_2 - \alpha_j).$$

First, we will show that $[\gamma_1 \colon \gamma_2]$ is a random equivalence class when α_3 is chosen randomly (and everything else is arbitrarily fixed).

Toward this objective, fix arbitrary $\alpha_1, \alpha_2 \in F_p^*$ such that $\alpha_1 \neq \alpha_2$, and arbitrary $\alpha_4, \alpha_5, \ldots, \alpha_n \in F_p$, such that $\{\alpha_1, \alpha_2\} \cap \{\alpha_4, \ldots, \alpha_n\} = \emptyset$. *Consider* $\alpha_3 \leftarrow F_p \setminus \{\alpha_1\}$.

$$\begin{aligned}
[\gamma_1 \colon \gamma_2] &= \left[\alpha_1 \prod_{j \neq 1} (\alpha_1 - \alpha_j) \ : \ \alpha_2 \prod_{j \neq 2} (\alpha_2 - \alpha_j) \right] && \text{(by definition)} \\
&= \left[1 \ : \ -\frac{\alpha_2}{\alpha_1} \cdot \prod_{j \geqslant 3} \left(\frac{\alpha_2 - \alpha_j}{\alpha_1 - \alpha_j} \right) \right] && \text{(because } \alpha_1 \neq 0 \text{ and } \alpha_1 \notin \{\alpha_3, \alpha_4, \ldots, \alpha_n\}\text{)} \\
&= \left[1 \colon \Delta \cdot \left(\frac{\alpha_2 - \alpha_3}{\alpha_1 - \alpha_3} \right) \right], \text{ where } \Delta := -\frac{\alpha_2}{\alpha_1} \cdot \prod_{j \geqslant 4} \left(\frac{\alpha_2 - \alpha_j}{\alpha_1 - \alpha_j} \right) \\
&= \left[1 \colon \underbrace{\Delta \cdot \left(1 + \frac{\alpha_2 - \alpha_1}{\alpha_1 - \alpha_3} \right)}_{\Gamma} \right]
\end{aligned}$$

We make the following observations.

1. $\Delta \neq 0$, because $\alpha_2 \neq 0$ and $\alpha_2 \notin \{\alpha_4, \ldots, \alpha_n\}$.
2. $(\alpha_1 - \alpha_3)$ is a uniform distribution over F_p^*, because $\alpha_1 \neq \alpha_3$.
3. $\frac{\alpha_2 - \alpha_1}{\alpha_1 - \alpha_3}$ is a uniform distribution over F_p^*, because $\alpha_1 \neq \alpha_2$.
4. $\left(1 + \frac{\alpha_2 - \alpha_1}{\alpha_1 - \alpha_3}\right)$ is a uniform distribution over $F_p \setminus \{1\}$.
5. Γ is a uniform distribution over $F_p \setminus \{\Delta\}$.

Let Γ' be the uniform distribution over $F_p \setminus \{0, 1\}$. Note that

$$\mathsf{SD}\left(\Gamma \ , \ \Gamma'\right) \leqslant \frac{2}{p-1}.$$

Therefore, $[1 : \Gamma]$ is $2/(p-1)$-close to a uniform distribution over the equivalence classes $[1 : 2], [1 : 3], \ldots, [1 : p-1]$. Note that $[\beta_1 : \beta_2]$ is identical to $[\gamma_1^{-1} : \gamma_2^{-1}] = \left[1 : \Gamma^{-1}\right]$, which is $2/(p-1)$-close to a uniform distribution over the equivalence classes $[1 : 2], [1 : 3], \ldots, [1 : p-1]$.

G 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 PHYS 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, when we mention α, it implies that any $(\alpha_1,\alpha_2)\in[1:\alpha']$ is secure against physical bit leakage attacks, where $\alpha'\in\alpha\langle 2\rangle$.

Remark 7 (Adversarial LLL: A worst-case analysis)**.** *For one (α_1,α_2), there may be multiple $(u,v)\in[\alpha_1,\alpha_2]$ that the LLL algorithm can output. The output of the LLL algorithm is crucial in assessing whether evaluation places are secure. The LLL output can change our algorithm's output in Figure 1 from "secure" to "may be insecure."*

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."

Consider 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 1 output "may be insecure," the adversarial LLL outputs that (u,v).

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 is used. Our code (running on Intel Core i7 7700K) returns all the secure evaluation places in 45.515 seconds.

For example, the element "95" in Table 1 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

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

Corollary 7 presents explicit evaluation places $(\alpha_1,\alpha_2)\in\left[1\colon 2^{\lfloor\lambda/2\rfloor}-1\right]$ such that for security parameter λ,

$$\varepsilon_{\mathrm{PHYS}}(\vec{\alpha})\leqslant\frac{4\cdot\left(2^{\lfloor\lambda/2\rfloor}+2^{\lceil\lambda/2\rceil}\right)-6}{p}.$$

When $\lambda=13$ and $p=2^{13}-1$, it implies that $[1:63]$ would have $\varepsilon_{\mathrm{PHYS}}(\vec{\alpha})\lesssim 0.093$. However, $63\cdot\langle 2\rangle$ is not listed in Table 1 because the "adversarial LLL" algorithm may pick $(u,v)=(1,63)$ which is characterized as "may be insecure" by our algorithm in Figure 1.

To generalize to $\mathsf{ShamirSS}(3, 2, (\alpha_1, \alpha_2, \alpha_3))$ over the prime field F of order $p = 2^\lambda - 1$, we consider the equivalence class $[1 : \alpha : \alpha']$ where $\alpha = \alpha_2\alpha_1^{-1}$ and $\alpha' = \alpha_3\alpha_1^{-1}$. If α, α' and $\alpha'\alpha^{-1}$ all belong to different cosets in Table 1, then the equivalence class $[1 : \alpha : \alpha']$ is secure against arbitrary physical bit leakage.

For example, $[1 : 95 : 103]$ is a good equivalence class of evaluation places against physical bit leakage attack for $\mathsf{ShamirSS}(3, 2, (\alpha_1, \alpha_2, \alpha_3))$. Consider $\alpha = 95 \in 95 \cdot \langle 2 \rangle$ and $\alpha' = 103 \in 103 \cdot \langle 2 \rangle$ which are good evaluation places in Table 1. Then, $\alpha'\alpha^{-1} = 6209 \in 225 \cdot \langle 2 \rangle$ is also a good evaluation place against physical bit leakage attacks.

Table 2 presents choices of α such that evaluation places in equivalence classes of the form $[1 : 95 : \alpha]$ are secure for $\mathsf{ShamirSS}(3, 2, \vec{\alpha})$. If we choose $\alpha \in \alpha' \cdot \langle 2 \rangle$ from one of the cosets in Table 1, we only need to check $\alpha \cdot 95^{-1}$ is also contained in one of the coset.

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.

97	99	103	111	113	119	121	125	135	139	143
151	155	159	165	173	175	181	185	187	191	203
207	215	217	225	229	231	233	235	237	239	243
245	251	269	271	275	277	279	281	291	293	295
297	299	305	309	313	317	325	331	335	339	349
351	355	357	361	363	365	371	373	377	379	391
393	395	397	399	403	405	407	413	415	429	435
437	445	447	457	459	461	467	469	471	473	477
487	491	495	497	499	501	503	505	551	553	555
559	575	581	583	603	607	611	613	615	617	621
623	637	651	653	655	661	667	671	679	687	693
695	697	701	713	715	719	725	729	735	743	755
757	797	799	805	807	811	813	815	823	825	829
843	847	857	859	863	869	871	873	877	879	883
885	891	893	915	921	923	937	939	947	951	955
959	973	975	987	989	991	997	1005	1007	1011	1175
1197	1199	1205	1207	1211	1213	1227	1231	1237	1239	1245
1247	1253	1259	1261	1275	1327	1335	1341	1355	1357	1371
1373	1389	1397	1403	1405	1447	1451	1461	1467	1469	1485
1495	1511	1519	1525	1691	1693	1695	1703	1709	1711	1723
1725	1743	1751	1757	1783	1851	1853	1855	1871	1885	1903
1909	1915	1963	1965	1973	1975	1979	1983	2013	2795	2807
2911	2935	2939	2991	2999	3035					

Table 2: Secure Evaluation Places against Physical Bit Leakage when $p = 2^{13}-1$ and $(n, k) = (3, 2)$. If an element $\alpha \in F$ appears in the list above, it implies the following. Any evaluation places $(\alpha_1, \alpha_2, \alpha_3) \in [1 : 95 : \alpha']$, where $\alpha' \in \alpha \cdot \langle 2 \rangle$, is secure against all physical bit leakage attacks.