Leakage-Resilience of Shamir's Secret Sharing: Identifying Secure Evaluation Places

Hemanta K. Maji
Purdue University, USA

Hai H. Nguyen
ETH, Zurich & Purdue University, USA

Anat Paskin-Cherniavsky
Ariel University, Israel

Xiuyu Ye
Purdue University, USA

Abstract

Secrets are safe in Shamir's secret sharing when only a few shares are compromised. Even probing a single bit from every share can reveal some information about the secret, turning the secret-sharing insecure. The specific places where the secret-sharing polynomial is evaluated to generate the shares determine the scheme's security. Although most evaluation places yield schemes secure against such side-channel attacks, algorithms to identify them are unknown.

Our work investigates Shamir's secret sharing among 2 or 3 parties over prime fields, where any two parties can reconstruct the secret. It presents:

1. An algorithm to classify evaluation places as secure or vulnerable against the least significant bit leakage.
2. A modulus choice where the algorithm above extends to identifying secure/vulnerable evaluation places against attacks that probe arbitrary single-bit from each share.

These results also discover new side-channel threats to Shamir's secret sharing.

Our work introduces new techniques to analyze the security of secret-sharing schemes against side-channel threats. 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.

2012 ACM Subject Classification

Keywords and phrases Shamir secret sharing, leakage resilience, physical bit probing, secure evaluation places, secure modulus choice, square wave families, Fourier analysis

Digital Object Identifier 10.4230/LIPIcs.ICALP.2024.

1 Introduction

Shamir's secret-sharing [33] underlies nearly all 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. [19, 20, 9] side-channel attacks have repetitively circumvented such "all-or-nothing" corruption models to compromise cryptosystems by aggregating leakage from all its components. Characterizing the security of Shamir's scheme against various leakage attacks has become even more compelling due to the ongoing NIST standardization efforts, [8]

where Shamir's secret sharing is widely used to distribute keys and in other higher-level primitives like secure computation.

One such security metric, namely, *local leakage resilience*, introduced by Benhamouda et al. [5, 6] & Goyal and Kumar [11], requires the statistical independence of the leakage from the secret. Guaranteeing leakage resilience of Shamir's scheme has been challenging – even against (seemingly) innocuous attacks that *probe physical bits* in the memory storing the shares.[1] Ishai et al. [17] introduced this physical bit probing model to unify several side-channel threats and, subsequently, has been central to leakage resilience research [18]. Surprisingly, *leakage resilience of Shamir's scheme hinges on the evaluation places used to generate the shares.* For example, leaking only the *least significant bit* (LSB) of each share reveals information about the secret for some evaluation places [27, 1, 28].

On the other hand, most evaluation places are locally leakage-resilient against arbitrary physical probes [27, 29]. To instantiate locally leakage-resilient Shamir's scheme, choosing random evaluation places would suffice. However, this strategy is *susceptible to adversarially set randomness*, where vulnerable evaluation places may be picked unbeknownst to the honest parties. To neutralize this threat, a natural question arises:

> *Is there an algorithm to determine whether the picked evaluation places yield a locally leakage-resilient Shamir's secret sharing?*
>
> Any meaningful classifier in this context must have the following features.
>
> 1. *No false positives.* No evaluation places can be incorrectly determined to be leakage-resilient; otherwise, adversarially set randomness can ensure they are picked.
> 2. *A small number of false negatives.* Ideally, the algorithm should correctly identify most (or at least a large fraction) of the leakage-resilient evaluation places.
> 3. *Efficiency.* The runtime of the classifier should not be "prohibitively large."

Before our work, over prime modulus, even against the specific LSB leakage, such a classifier was unknown.

Summary of our results. Our work presents such classifiers for (A) $(n, k) = (2, 2)$, (B) $(n, k) = (3, 2)$, and (C) $n = k > 2$ over Mersenne prime modulus against arbitrary single-bit probes into each share. Our algorithms have $\mathsf{poly}(\log p)$ running time and $\sqrt{p} \cdot \mathsf{poly}(\log p)$ false negatives. The main technical workhorse for these results is our classifier for the specific LSB leakage.

▶ Remark 1 (Subsequent work: Comparison & Discussion). Recently, [29] presented these algorithms for $n \geqslant k = 2$ over *extension fields*. Due to the vector space structure of the extension field over the base field, their results rely on properties of the rank of linear maps. For example, in their case, the leakage is independent of the secret or reveals it entirely – a dichotomy. In contrast, our work considers *prime fields*, which lack a vector space structure; leakage correlates with the secret more subtly, making the analysis significantly involved.

[1] A long line of research [2, 34, 3, 22, 7, 16, 10, 23, 30] constructs secret-sharing schemes to protect against specific side-channel threats. However, these schemes lack linearity, multiplication-friendliness, and optimal information rate; applications using secret sharing rely upon these features. Additionally, from practicality considerations, considering the widespread deployment of Shamir's scheme, it would be ideal to ensure its leakage resilience with minimal to no change to its specification.

2 Basic Definitions & Our Formal 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 prime 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 $\{0, 1, \ldots, (p-1)\}$ of F_p.

Leakage functions & families. This work studies *physical bit leakage* $\mathrm{PHYS}_i \colon F_p \to \{0,1\}$ 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: $\mathrm{PHYS} := \left\{ \vec{\mathrm{PHYS}}_{i_1,\ldots,i_n} \;:\; i_1, \ldots, i_n \in \{0, 1, \ldots, \lambda - 1\} \right\}$.
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:

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

Small insecurity implies the statistical independence of the leakage from the secret, i.e., the *secret-sharing is locally leakage-resilient* [5, 11].

High insecurity implies that a leakage function can distinguish the secret 0 and some $s^* \in F^*$ using the leakage. Maji et al. [27] analyzed the insecurity against the PHYS leakage family when *evaluation places are chosen randomly*. Their result implies the following corollary for $k = 2$ and prime modulus $p \geqslant 3$.

Randomized Construction of Maji et al. [27] for Prime Fields

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

Recently, [29] extended the randomized construction from prime fields to composite ones.

This work investigates the security against the leakage family PHYS; i.e., the adversary obtains arbitrary *one physical bit leakage from each share*.

Our Research Question

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

If $\varepsilon_{\mathrm{PHYS}}(\vec{\alpha}) > p^{-1/2}$, then output a secret $s^* \in F_p^*$ such that the shares of 0 can be distinguished from the shares of s^* with (roughly) $\varepsilon_{\mathrm{PHYS}}(\vec{\alpha})$ advantage. *All algorithms should*

be computationally efficient – run-time polynomial in λ. Furthermore, concrete security analysis (over asymptotic analysis) is prioritized.

3 Our Results

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. Section 5 presents a high-level overview of the key technical ideas of our results.

Technical Result: Security against LSB Leakage when $(n, k) = (2, 2)$. Consider *arbitrary prime* $p \geqslant 3$ (not just a Mersenne prime) and the LSB leakage. The technical workhorse for our results is the classifier for $(n, k) = (2, 2)$; other results bootstrap from it.

1. Figure 1 presents our efficient algorithm to classify $\vec{\alpha}$ as secure or not. If our algorithm classifies $\vec{\alpha}$ as secure, then
$$\varepsilon_{\mathrm{LSB}}(\vec{\alpha}) \leqslant \frac{1 + 8^{5/4}}{\sqrt{p}} + \frac{13/2}{p} \leqslant \frac{14.46}{\sqrt{p}},$$
which is exponentially small in the security parameter λ. The number of false negatives is $\mathcal{O}\big(\sqrt{p} \cdot \log p\big)$.
2. We present an efficient adversary that generates $s^* \in F^*$ such that it distinguishes the secret 0 from s^* by leaking the LSB of each share with an advantage
$$\geqslant \varepsilon_{\mathrm{LSB}}(\vec{\alpha}) - \frac{2 \cdot 8^{5/4}}{\sqrt{p}} - \frac{13}{p} \geqslant \varepsilon_{\mathrm{LSB}}(\vec{\alpha}) - \frac{26.91}{\sqrt{p}}.$$
Therefore, our efficient leakage attack achieves a comparable distinguishing advantage when the insecurity $\varepsilon_{\mathrm{LSB}}(\vec{\alpha})$ is large.

Section 6 presents the corollary statements relevant to LSB leakage and their proofs (Section 6.2 to Section 6.4 state and prove Corollary 11 to Corollary 13, respectively).

Result A: Security against Physical Bit Leakage when $(n, k) = (2, 2)$. For the $n = k = 2$ case, we analyze a prime field F_p, where p is a Mersenne prime – a prime of the form $2^\lambda - 1$. We reduce arbitrary physical bit leakage to LSB leakage for related evaluation places over these fields. In this context, our work proves the following results.

1. Figure 2 presents our efficient classifier against PHYS leakage. For $\vec{\alpha}$ classified secure, the insecurity is $\varepsilon_{\mathrm{PHYS}}(\vec{\alpha}) \leqslant 14.46/\sqrt{p}$. The number of false negatives is $\mathcal{O}\Big(\sqrt{p} \cdot (\log p)^2\Big)$.
2. 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 $f \in \mathrm{PHYS}$ from the shares with an advantage $\geqslant \varepsilon_{\mathrm{PHYS}}(\vec{\alpha}) \geqslant \varepsilon_{\mathrm{PHYS}}(\vec{\alpha}) - 26.91/\sqrt{p}$.
3. We explicitly identify secure evaluation places against PHYS leakage: all (α_1, α_2) satisfying $\alpha_2 \cdot \alpha_1^{-1} = 2^{\lfloor \lambda/2 \rfloor} - 1$. For these evaluation places $\varepsilon_{\mathrm{PHYS}}(\vec{\alpha}) \leqslant 8.49/\sqrt{p}$.

Appendix D presents the corollary statements relevant to these results and their proofs.

Result B: 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?* At the outset, it is unclear whether evaluation places (α_i, α_j) would retain their security in the presence of additional leakage from the third share. However, we prove the security of this lifting technique for $(n, k) = (3, 2)$.

Consider distinct evaluation places $(\alpha_1, \alpha_2, \alpha_3)$ satisfying: $\varepsilon_{\text{PHYS}}(\ (\alpha_i, \alpha_j)\ ) \leqslant \varepsilon$, for all distinct $i, j \in \{1, 2, 3\}$. Lemma 41 proves that the $\varepsilon_{\text{PHYS}}(\ (\alpha_1, \alpha_2, \alpha_3)\ ) \leqslant 3\varepsilon$. 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 $k = 2$ (the reconstruction threshold) is less than the degree of the correlation, which is 3. This lifting technique does not extend to $n \in \{4, 5, \dots\}$ because the "four-wise correlation" (in general, any "even-wise correlation") *may be correlated* with the secret.

For the converse, note that if there are two 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.

Result C: Security against Physical Bit Leakage when $n = k > 2$. Consider a Mersenne prime field F_p, such that $p = 2^\lambda - 1$. Corollary 19 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 8 presents Theorem 18, which implies this corollary. Appendix F.2 proves this theorem using Fourier analysis. Appendix F.1 presents the proof of Corollary 19.

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 $\vec{\beta}$ using our linear map, and (3) test the security of $\mathsf{ShamirSS}(2, 2, (\beta_1, \beta_2))$ using Corollary 17.

4 Illustrating Technical Challenges: Resilience to LSB Leakage

Before presenting the technical overview of our results, it is instructive to illustrate the challenges of constructing such a classifier against the LSB leakage.

4.1 A New Vulnerability to LSB Leakage

Consider Shamir's secret sharing scheme among $n = 2$ parties and threshold $k = 2$ over the prime fields 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 $s_1 := P(1)$, the evaluation of $P(X)$ at $X = 1$, and the second is $s_2 := P(3)$. The two shares are elements of the following set:

$$(s_1, s_2) \in \Big\{\ (P_1, 3 \cdot P_1)\ :\ P_1 \in F_p \Big\}. \tag{2}$$

The LSB attack – a specific type of bit probe – leaks each share's *parity*. For example, a share in the set $\{0, 2, 4, \dots, (p-1)\}$ has "even" parity, while a share in the complementary set $\{1, 3, \dots, (p-2)\}$ has "odd" parity. We aim to investigate the leakage joint distribution:

Is the LSB *leakage uniformly distributed over* $\{even, odd\} \times \{even, odd\}$*?*

Observation 1. Let us calculate the probability that the parity of s_1 differs from that of s_2. There are *two exhaustive cases.*

A: Share $s_1 = 2 \cdot x$, 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: Share $s_1 = 2 \cdot x$, 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; the leakage is *not* uniformly random.

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

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

where $s, P_1 \in F_p$ are uniformly and independently random. In this case, the leakage is uniformly random, and 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 algorithms efficiently generate the secret s^*.

Conclusion. These two observation demonstrate that the LSB leakage is not independent of the secret; the secret 0 and s^* are distinguishable with advantage $\geqslant 1/2 - 1/3 = 1/6$. For brevity, we say that *the leakage is* 1/6*-dependent on the secret* and this scheme is *vulnerable*.

This vulnerability extends to all $\alpha_1 \cdot \alpha_2^{-1} \in \{\pm 3, \pm 3^{-1}\}$ using properties of Generalized Reed Solomon codes [13]. Before our work, the only known vulnerable evaluation places satisfied $\alpha_1 \cdot \alpha_2^{-1} = -1$ [27, 1, 28].

4.2 An Example for Leakage-Resilience to LSB Leakage

Now consider evaluation places $(1, 2)$. In this case, the shares of 0 satisfy:

$$(s_1, s_2) \in \left\{ (P_1, 2 \cdot P_1) : P_1 \in F_p \right\}. \tag{4}$$

Similar to Observation 1, the probability of the parity of s_1 and s_2 being different is (roughly) 1/2; the leakage is uniformly random.[2] From this fact, using some additional analysis, one can prove that the LSB leakage is statistically independent of the secret.[3]

▶ Remark 2. Looking ahead, the evaluation places $(1, 2)$ is vulnerable to physical bit leakage over Mersenne prime fields (see Remark 4).

4.3 Classifier Construction: First Attempt

Consider distinct evaluation places $\alpha_1, \alpha_2 \in F_p$. The corresponding shares of 0 are:

$$(s_1, s_2) \in \left\{ (\alpha_1 \cdot P_1, \alpha_2 \cdot P_1) : P_1 \in F_p \right\}. \tag{5}$$

Using the presentation above, it suffices to determine the probability of the two shares having different parity. This probability is computable in $\mathcal{O}(p)$ time by exhaustively considering all $P_1 \in F_p$. This brute-force algorithm is "efficient" only for small primes; however, any

[2] The shares have different parity when $(s_1, s_2) = (2 \cdot x, 4 \cdot x)$ and $x \in \mathbb{Z} \cap [p/4, 3p/4]$.
[3] The LSB leakage being uniformly random for secret 0 *does not* outrightly imply that the LSB leakage is independent of the secret. For example, it is possible that the probability of the shares having different parity is $> 1/2$ for half the secrets, and for the remaining secrets, this probability is $< 1/2$, such that their average is 1/2. However, our technical analysis rules out this possibility.

Shamir's scheme is $1/p$-dependent on the secret. Hence, Shamir's scheme is vulnerable to the LSB leakage when the prime modulus is small. For large primes, as is standard in this line of works, the length of the binary representation of the elements in F_p, i.e., "$\lambda := \log_2 p$," denotes the problem size. Any efficient algorithm must have a $\mathsf{poly}(\lambda)$ runtime, but the brute-force algorithm takes exponential time.

4.4 Classifier Construction: Second Attempt

This section focuses on developing an efficient algorithm. Suppose $(\alpha_1 = 1, \alpha_2)$ are the evaluation places. Extrapolating from the examples in Section 4.1 and Section 4.2, a "reasonable conjecture" would be the following characterization.

- If α_2 is odd: Declare "LSB leakage is $1/2\alpha_2$-dependent on the secret"
- (Else) If α_2 is even: Declare "LSB leakage is independent of the secret."

Fascinatingly, this classifier is so near, yet so far; it has *false positives*. For example, consider a prime $p = 6t + 1$, where t is a large integer. Consider the evaluation places $(\alpha_1, \alpha_2) = (1, 2t + 2)$; the algorithm above misclassifies it as resilient to LSB leakage (because α_2 is even). However, these evaluation places are $1/30$-dependent on the secret.

Using properties of Generalized Reed-Solomon codes [13], the shares of 0 for evaluation places (α_1, α_2) and evaluation places (u, v) are identical when $\alpha_1 \cdot \alpha_2^{-1} = u \cdot v^{-1}$; represented by $(u, v) \in [\alpha_1 : \alpha_2]$. In our example, for instance, $(3, 5) \in [1 : 2t + 2]$ and, as in the previous examples, the shares are $(6x, 10x)$, for $x \in F_p$. The two shares have different parity when

$$x \in \mathbb{Z} \cap \left(\left[\frac{3p}{30}, \frac{5p}{30}\right] \cup \left[\frac{6p}{30}, \frac{9p}{30}\right] \cup \left[\frac{10p}{30}, \frac{12p}{30}\right] \cup \left[\frac{18p}{30}, \frac{20p}{30}\right] \cup \left[\frac{21p}{30}, \frac{24p}{30}\right] \cup \left[\frac{25p}{30}, \frac{27p}{30}\right] \right).$$

The probability of this event is $1/2 - 1/30$; therefore, the LSB leakage is $1/30$-dependent on the secret.

How do we identify the evaluation places yielding LSB *resilient sharing?* Their pattern is fairly complex, as our algorithm illustrates in Figure 1; Section 5.1 presents an overview. The exposition above introduces several technical components of our algorithm.

5 Technical Overview

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

We outline our classification algorithm for $(n, k) = (2, 2)$ and, en route, highlight our technical contributions (Figure 1 presents the pseudocode).

Step 1. The prime modulus p and the distinct non-zero evaluation places $\alpha_1, \alpha_2 \in F_p$ are inputs to the LSB classification algorithm. The security/vulnerability of evaluation places (α_1, α_2) is identical to any evaluation places (u, v) satisfying $\alpha_1 \cdot \alpha_2^{-1} = u \cdot v^{-1}$ (follows from Generalized Reed-Solomon codes' properties [13]). We find "small norm" $u, v \in \left\{-\lceil\sqrt{p}\rceil, \ldots, 0, 1, \ldots, \lceil\sqrt{p}\rceil\right\}$ with the property mentioned above – a Dirichlet approximation problem. We solve it with a small constant multiplicative slack using the LLL [25] algorithm in $\mathsf{poly}(\lambda)$ runtime, where $\lambda := \lceil \log_2(p + 1) \rceil$ (Appendix A has the details). The reasoning for choosing "small norm" u, v will be evident in Step 3.

Step 2. We aim to compute the probability that the shares s_1 and s_2 have different parity when the secret is 0; represent this probability by $1/2 + \varepsilon$. If ε has a small magnitude, the leakage is independent of the secret; otherwise, the LSB leakage can distinguish two secrets

with an advantage of $|\varepsilon|$. By exhaustively considering all possible shares, one can compute ε in $\mathcal{O}(p)$ time, which is unfortunately exponential in our problem size λ.

Step 3. To develop an efficient algorithm to compute ε, we express the quantity ε as the inner product of two oscillatory $\{\pm 1\}$ sequences, approximated by the following integral.

$$\int_0^1 \operatorname{sign}\sin(2\pi|u|\cdot t)\cdot \operatorname{sign}\sin(2\pi|v|\cdot t)\ \mathrm{d}t.$$

Here $\operatorname{sign}\sin(2\pi|u|\cdot t)$ is a *square wave* that oscillates $|u|$ times in the domain $[0,1]$. The integral above measures the similarity/dependence between the two square waves, one oscillating $|u|$ times and the other oscillating $|v|$ times. The error of our approximation is directly proportional to the total number of oscillations of the square waves. For small norm u, v, the approximation error is $\leqslant (|u|+|v|)/p = \mathcal{O}\big(1/\sqrt{p}\big)$, exponentially small in λ. The presentation below ignores this approximation error for simplicity.

Step 4. Finally, we compute ε by obtaining a closed-form expression for the integral. For $g := \gcd(|u|,|v|)$ and $\rho := |u|\cdot|v|/g^2$, we prove that:

$$\varepsilon = \begin{cases} 0, & \text{if } \rho \text{ is even} \\ \frac{1}{2\rho}, & \text{if } \rho \text{ is odd.} \end{cases}$$

When $\varepsilon = 0$, Shamir's scheme with evaluation places (α_1, α_2) is resilient to LSB leakage. Otherwise, there is an efficient algorithm to distinguish secret 0 from some $s^* \in F_p$ using the LSB leakage. Our toy example is insecure because $\rho = 1/6$ (since $u = \alpha_1 = 1$ and $v = \alpha_2 = 3$). One way for evaluation places α_1, α_2 to be secure is: there are small norm u, v such that $\alpha_1 \cdot \alpha_2^{-1} = u \cdot v^{-1}$ and the highest powers of 2 dividing u and v are different (in which case ρ is even). Our classification algorithm for arbitrary physical bit probes will build on the result outlined in this section.

▶ Remark 3. Our work connects the security of secret-sharing schemes against leakage attacks with the properties of a family of square waves; see, for example, [35, 15, 14]. Various families of square waves like the ones by Haar [12], Walsh [36], and Rademacher [32] are central to science and engineering. This conceptual contribution, we feel, will be interesting to the broader community.

5.2 Overview of Result A: Physical Bit Leakage $(n,k) = (2,2)$

Suppose the evaluation places are $\vec{\alpha} = (\alpha_1, \alpha_2)$. We aim to *determine whether Shamir's secret-sharing scheme with these evaluation places is secure against all physical bit leakage attacks Mersenne prime fields.* For $i, j \in \{0, 1, \ldots, \lambda - 1\}$, consider the physical bit leakage attack $\mathrm{PH}\vec{\mathrm{Y}}\mathrm{S}_{i,j}$. This leakage attack leaks the i-th LSB of the share s_1 and the j-th LSB of the share s_2. For a Mersenne prime p and an element $x \in F_p$, the binary representation of $x \cdot 2^{-1}$ is the *right rotation* of the binary representation of x by one position. Therefore, $\mathrm{PH}\vec{\mathrm{Y}}\mathrm{S}_{i,j}$ leakage with evaluation places (α_1, α_2) is identical to the LSB leakage with evaluation places $(2^{-i}\cdot\alpha_1, 2^{-j}\cdot\alpha_2)$. By Generalized Reed-Solomon codes' properties [13], the leakage is identical to the LSB leakage with evaluation places $(2^{j-i}\cdot\alpha_1, \alpha_2)$. Consequently,

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

Thus, security against PHYS leakage reduces to a sequence of LSB security estimations. Figure 2 presents this pseudocode.

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 [24] 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 $B := \lceil 2^{3/4} \cdot \sqrt{p} \rceil$. Refer to Figure 3 in Appendix A.
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 against LSB leakage
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 against LSB leakage
6. (Else) Declare that the security of $\mathsf{ShamirSS}(2, 2, (\alpha_1, \alpha_2))$ against LSB attacks may be insecure

Figure 1 Identify secure evaluation places for Shamir's secret-sharing scheme against the LSB leakage attack.

▶ Remark 4 (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 15 proves that this edge case is insecure. This case captures why evaluation places $(1, 2)$ are insecure against physical bit leakage.

5.3 Overview of Result B: Physical Bit Leakage $(n, k) = (3, 2)$

Suppose the evaluation places are $\vec{\alpha} = (\alpha_1, \alpha_2, \alpha_3)$. We aim 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. The following integral approximates the three-wise correlation between the leakage bits:

$$\int_0^1 \operatorname{sign}\sin(2\pi|u| \cdot t) \cdot \operatorname{sign}\sin(2\pi|v| \cdot t) \cdot \operatorname{sign}\sin(2\pi|w| \cdot t)\, \mathrm{d}t,$$

where $(u, v, w) \in [\alpha_1 : \alpha_2 : \alpha_3]$. This integral is 0 because square waves are odd functions.

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

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 1 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 2 Identify secure evaluation places for Shamir's secret-sharing scheme against all physical bit leakage attacks.

▶ Remark 6. *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 the three-wise correlation expression using an integral. The error in this estimation would be proportional to $(|u| + |v| + |w|)/p$, where $(u, v, w) \in [\alpha_1 : \alpha_2 : \alpha_3]$. Dirichlet's approximation theorem [25] can only ensure that $|u|, |v|, |w| \leqslant p^{2/3}$ simultaneously. Consequently, our estimation error will be in the order $p^{-1/3}$. Therefore, we would only be able to guarantee that insecurity is $\leqslant p^{-1/3}$. Note that currently, we ensure that the insecurity is $\leqslant p^{-1/2}$, which is $\ll p^{-1/3}$.

5.4 Overview of Result C: 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 18) 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 F.2.

6 Security against Least Significant Bit Leakage

This section presents our results regarding the security of Shamir's secret-sharing scheme when $n = k = 2$ against the LSB leakage. We begin with a powerful technical result.

▶ **Theorem 7** (Technical Result). *Consider the* ShamirSS$(2, 2, (\alpha_1, \alpha_2))$ *secret-sharing scheme over a prime field* F_p*, where* $p \geqslant 3$*. For any* $(u, v) \in [\alpha_1 : \alpha_2]$*,*

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

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

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

using the LSB *leakage on the secret shares.*

Essentially, this theorem helps estimate the insecurity efficiently. Section 6.1 presents the proof outline for this result and Appendix B presents the full proof. With this theorem, we will state and prove the corollaries mentioned in Section 3.

6.1 Proof outline of Theorem 7

For any $s \in F^*$, we start by obtaining 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. Below, we present a high-level overview of the proof of Theorem 7.

Step 1. We connect the statistical distance between the leakages to the difference between two sums of oscillatory functions. We define the function $\mathrm{sign}_p \colon \mathbb{Z} \to \pm 1$.

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

For $k, \ell, \Delta \in F$, we define the following measurement of similarity between two lines kT and $\ell(T - \Delta)$ on F.

$$\Sigma^{(\Delta)}_{k,\ell} := \sum_{T \in F} \mathrm{sign}_p(kT) \cdot \mathrm{sign}_p(\ell(T - \Delta)). \tag{6}$$

▶ **Lemma 8.** *Consider the* 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 B.1 proves Lemma 8.

Step 2. Next, our objective is to estimate the sum $\frac{1}{p} \cdot \Sigma^{(\Delta)}_{k,\ell}$ using the integral $I^{(\delta)}_{k,\ell}$ defined as an inner product of two square wave functions as follow.

$$I^{(\delta)}_{k,\ell} := \int_0^1 \mathrm{sign}\sin(2\pi|k| \cdot t) \cdot \mathrm{sign}\sin(2\pi|\ell| \cdot (t - \delta))\ \mathrm{d}t.$$

▶ **Lemma 9.** *For any $k, \ell, \Delta \in F_p$, and $\delta = \frac{\mathrm{sign}_p(\Delta)\cdot|\Delta|}{p} \in \mathbb{Q}$,*

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

Appendix B.2 proves Lemma 9.

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

▶ **Lemma 10.** *For any $k, \ell \in \{1, 2, \dots\}, \delta \in \mathbb{R}$, and $g = \gcd(k, \ell)$*

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

Appendix B.3 proves Lemma 10. 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 Theorem 7 after maximizing over every $s \in F^*$.

Efficient distinguisher construction. We present an efficient maximum likelihood distinguisher in Appendix B.7.

6.2 Insecurity Estimation

Using Theorem 7, we prove that the estimated insecurity achieved by our classifier in Figure 1 is close to the true insecurity.

▶ **Corollary 11.** *Consider distinct evaluation places $\vec{\alpha} = (\alpha_1, \alpha_2)$ and the corresponding* 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 $|u|, |v| \leqslant B$, where $B = \lceil 8^{1/4}\cdot\sqrt{p}\rceil$. Let $g = \gcd(|u|, |v|)$. Define*

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

Then,

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

Proof. Use the LLL algorithm [25] 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 7 is identical to $\varepsilon_{\mathrm{LSB}}(\vec{\alpha})$ by our definition in Equation 1. From this observation, the corollary is immediate. ◀

Next, we state and prove the corollaries mentioned in Section 3 through this tight estimation.

6.3 Statement and Proof of Corollary 12

▶ **Corollary 12.** *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 1 determines $\vec{\alpha}$ to be secure. Then,*

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

Among all possible distinct evaluation places $\alpha_1, \alpha_2 \in F_p^*$, the algorithm of Figure 1 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 1 declares $\vec{\alpha}$ to be secure either in Step 4 or Step 5.

Suppose our algorithm in Figure 1 declared that Shamir's secret-sharing scheme is secure in Step 4. In this case, $|u| \cdot |v|/g^2$ is even, where $g = \gcd(|u|, |v|)$. Using Corollary 11, we get that our estimation $\varepsilon_{\text{LSB}}^{(\text{est})} = 0$. The relation between our estimation and insecurity yields

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

Suppose our algorithm in Figure 1 declared that Shamir's secret-sharing scheme is secure in Step 5. In this case, $|u| \cdot |v|/g^2 \geqslant \sqrt{p}$ and it is odd. Using Corollary 11, we get that our estimation $\varepsilon_{\text{LSB}}^{(\text{est})} \leqslant 1/\sqrt{p}$. The relation between our estimate and insecurity yields

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

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

We prove the second part in Appendix B.4 with a similar case argument. ◀

6.4 Statement and Proof of Corollary 13

▶ **Corollary 13.** *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 $\varepsilon_{\text{LSB}}(\vec{\alpha}) > \frac{2 \cdot 8^{5/4}}{\sqrt{p}} + \frac{13}{p}$, 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*

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

by leaking the LSB *of the secret shares.*

Consider an efficient adversary outputs the s indicated in Theorem 7. After observing the leakage (ℓ_1, ℓ_2), the 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. Appendix B.5 provides a full proof of the distinguishing advantage and security guarantee of this adversary.

7 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 $2^{82,589,933} - 1$. Mersenne primes have fascinating properties.

▶ **Proposition 14.** *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 $2^\lambda = 1 \mod p$. We note that if $\mathrm{PHYS}_i(x) = 0$, then $\mathrm{PHYS}_0(x \cdot 2^{-i}) = 0$.

7.1 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 2. 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

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

Let $v := u2^{-j}$ and $t := s2^{-j}$. By Proposition 14, the joint distribution of leakage is equivalent as (for uniformly random $v \in F$)

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

because $2^k\alpha_1 = \alpha_2$. When $t = 0$, 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 15.** *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 $s = (2^k - 1)^{-1} \cdot 2^j$.

7.2 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 16.** *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 $\vec{\text{PHYS}}_{i,j}$ 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 $\vec{\text{PHYS}}_{i,j}$ 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 $\vec{\text{LSB}}$ 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 D.5 proves that the distributions D and D' are identical, for all $s \in F_p$, using Proposition 14.

7.3 Upper bound on insecurity

▶ **Corollary 17.** *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 2 determines $\vec{\alpha}$ to be secure. Then,*

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

Among all possible distinct evaluation places $\alpha_1, \alpha_2 \in F_p^*$, the algorithm of Figure 1 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 $p \geqslant 11$.

8 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 $n \in \{2, 3, \ldots\}$. We begin by stating the following general lifting theorem.

▶ **Theorem 18.** *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. Corollary 19 is a consequence of the above theorem.

▶ **Corollary 19.** *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

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

We present the full proof of Theorem 18 and Corollary 19 in Appendix F.

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.
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.
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.
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.
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.
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.
7. 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.
8. 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.
9. 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.
10. Eshan Chattopadhyay, Jesse Goodman, Vipul Goyal, and Xin Li. Leakage-resilient extractors and secret-sharing against bounded collusion protocols. Cryptology ePrint Archive, Report 2020/478, 2020. https://eprint.iacr.org/2020/478.
11. 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.
12. Alfréd Haar. Aur theorie der orthogonalen funcktionensysteme. *Math. Annalen*, 69:331–371, 1910.
13. Jonathan I. Hall. Notes on coding theory. https://users.math.msu.edu/users/halljo/classes/codenotes/GRS.pdf, 2015.
14. 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.
15. 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.
16. 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.

17 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.

18 Yael Tauman Kalai and Leonid Reyzin. A survey of leakage-resilient cryptography. In *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*, pages 727–794. 2019.

19 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.

20 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.

21 Steven G Krantz. *A panorama of harmonic analysis*, volume 27. American Mathematical Soc., 2019.

22 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.

23 Ashutosh Kumar, Raghu Meka, and David Zuckerman. Bounded collusion protocols, cylinder-intersection extractors and leakage-resilient secret sharing. Cryptology ePrint Archive, Report 2020/473, 2020. https://eprint.iacr.org/2020/473.

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

25 Arjen K Lenstra, Hendrik Willem Lenstra, and László Lovász. Factoring polynomials with rational coefficients. *Mathematische annalen*, 261(ARTICLE):515–534, 1982.

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

27 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.

28 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.

29 Hemanta K. Maji, Hai H. Nguyen, Anat Paskin-Cherniavsky, and Xiuyu Ye. Constructing leakage-resilient shamir's secret sharing: Over composite order fields. In *EUROCRYPT*, 2024.

30 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.

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

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

33 Adi Shamir. How to share a secret. *Communications of the Association for Computing Machinery*, 22(11):612–613, November 1979. doi:10.1145/359168.359176.

34 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.

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

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

A Solving Simultaneous Diophantine Equations

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

▶ **Theorem 20** (LLL [25, Proposition 1.39]). *There exists a polynomial-time algorithm that, given a positive integer d and rational numbers $r_1, r_2, \ldots, r_d, \varepsilon$ satisfying $0 < \varepsilon < 1$, finds integers $s_1, s_2, \ldots, s_d$, and t for which*

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

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

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

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

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

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

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 $u = \alpha_1 \cdot t \in F$ and $v = \alpha_2 \cdot t \in F$

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

Let us proceed to analyze our algorithm of Figure 3. The parameter setting needs to ensure that $t \leqslant 2^{d(d+1)/4}\varepsilon^{-d} < p$. Recall that $\varepsilon = B/p$. Substituting this value and rearranging, one needs to ensure that $2^{d(d+1)/4} \cdot p^{d-1} < B^d$. 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 Proof of Technical Lemmas

B.1 Proof of Lemma 8

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 $(u, v) \in [\alpha_1 : \alpha_2]$.

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

▷ Claim 21. 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

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

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.

B.2 Proof of Lemma 9

Recall that $\text{sign}_p(X=0)=+1$ and $\text{sign}(x=0)=0$. Due to this mismatch, we defined an intermediate function satisfying $\widetilde{\text{sign}}_p(X=0)=0$.

$$\widetilde{\text{sign}}_p(X) := \begin{cases} +1, & \text{if } X \in \{1,\ldots,(p-1)/2\} \mod p \\ 0, & \text{if } X = 0 \mod p \\ -1, & \text{if } X \in \{-(p-1)/2,\ldots,-1\} \mod p. \end{cases} \tag{7}$$

(8)

Analogously, we define

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

So, our next objective is to relate the quantities $\Sigma^{(\Delta)}_{k,\ell}$ with $\widetilde{\Sigma}^{(\Delta)}_{k,\ell}$.

▷ Claim 22. For any $k,\ell,\Delta\in F_p$,

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

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

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

▷ Claim 23 (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 $\delta=\Delta/p\in\frac{1}{p}\cdot\mathbb{Z}$,

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

▷ Claim 24. 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 $\delta':=\frac{\text{sign}_p(\Delta)\cdot|\Delta|_p}{p}\in\frac{1}{p}\cdot\mathbb{Z}$, 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, $\mathrm{sign}_p(\Delta) = -1, |\Delta|_p = p - \Delta$ and $\delta' = \delta - 1$. Then,

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

◀

◀

▷ Claim 25. For $k \in F_p$ and $x, \delta \in \frac{1}{p} \cdot \mathbb{Z}$, the following holds.

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

Proof. Consider the following exhaustive case analysis.

- **Case 1:** If $k \in \{0, 1, \ldots, (p-1)/2\}$, $|k|_p = k, \mathrm{sign}_p(k) = 1$ and $\varphi(k \cdot (x - \delta)) = \mathrm{sign}_p(k) \cdot \varphi(|k|_p \cdot (x - \delta))$ 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 $\mathrm{sign}_p(k) = -1$. Substituting in $\mathrm{sign}_p(k) \cdot \varphi(|k|_p \cdot (x - \delta))$, we get

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

◀

◀

Given the Transference Property (Claim 23), Claim 24 and Claim 25, we observe that for $k, \ell, \Delta \in F_p, T \in F, t = T/p \in \mathbb{Q}$ and $\delta = \frac{\mathrm{sign}_p(\Delta) \cdot |\Delta|_p}{p} \in \mathbb{Q}$,

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

▶ **Definition 26** (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 27 (Counting Number of Oscillations). For any $|k|_p, |\ell|_p \in \{1,\dots,(p-1)/2\}$,

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 28 (Sum and Integral Connection). Fix an integer $n \in \{1,2,\dots\}$. Let $f\colon[0,1]\to\{\pm1\}$ be a Boolean function that oscillates H times in the range $[0,1]$. Then,

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

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

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

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

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

Adding over all $r \in \{0/n, 1/n, \dots, (n-1)/n\}$, we get the 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 27 and Claim 28, we conclude Claim 22.

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

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

Therefore, applying Claim 22,

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

B.3 Proof of Lemma 10

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

▶ **Proposition 29** (Orthogonality of Sine/Cosine Waves [21, 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* [35, 15, 14] $\varphi\colon \mathbb{R} \to \{-1, 0, +1\}$.

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

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

$$\varphi(x) = \sum_{\text{odd } n>0} \frac{4}{\pi n} \cdot \sin(2n\pi x). \tag{9}$$

We prove the following claim for standardization.

▷ Claim 30. 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 [35, 15]. 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 31. 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

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

Therefore,

$$\begin{aligned}
\int_0^1\sin(2n\pi\cdot kt)\cdot\sin(2m\pi\cdot\ell(t-\delta))\,\mathrm{d}t &= \int_0^{1/2}\sin(2n\pi\cdot kt)\cdot\sin(2m\pi\cdot\ell(t-\delta))\,\mathrm{d}t\\
&\quad+\int_{1/2}^1\sin(2n\pi\cdot kt)\cdot\sin(2m\pi\cdot\ell(t-\delta))\,\mathrm{d}t\\
&=\int_0^{1/2}\sin(2n\pi\cdot kt)\cdot\sin(2m\pi\cdot\ell(t-\delta))\,\mathrm{d}t\\
&\quad-\int_0^{1/2}\sin(2n\pi\cdot kt)\cdot\sin(2m\pi\cdot\ell(t-\delta))\,\mathrm{d}t\\
&=0. \qquad (10)
\end{aligned}$$

Now, we can prove the lemma.

$$\begin{aligned}
I^{(\delta)}_{k,\ell} &= \int_0^1\varphi(kt)\cdot\varphi(\ell(t-\delta))\,\mathrm{d}t\\
&=\frac{16}{\pi^2}\sum_{\text{odd } n>0}\sum_{\text{odd } m>0}\frac{1}{mn}\int_0^1\sin(2n\pi\cdot kt)\cdot\sin(2m\pi\cdot\ell(t-\delta))\,\mathrm{d}t \qquad \text{(By Equation 9)}\\
&=0 \qquad \text{(By Equation 10)}
\end{aligned}$$

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

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

Again, Equation 10 holds, and the proof of this case goes through. ◀ ◀

▷ Claim 32. For relatively prime $k, \ell \in \{1, 2, \dots\}$ such that $k \cdot \ell$ is odd,

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

for all $\delta \in \mathbb{R}$. Therefore, $I^{(\delta)}_{k,\ell}$ 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 29.

▷ Claim 33.

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

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 29 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 29 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 $I_{k,\ell}^{(\delta)}$.

$$\begin{aligned}I_{k,\ell}^{(\delta)} &= \int_0^1 \varphi(kt)\cdot\varphi(\ell(t-\delta))\,\mathrm{d}t \\ &= \frac{16}{\pi^2}\sum_{\text{odd } n>0}\sum_{\text{odd } m>0}\frac{1}{mn}\int_0^1 \sin(2n\pi\cdot kt)\sin(2m\pi\cdot\ell(t-\delta))\,\mathrm{d}t \qquad \text{(By Equation 9)}\end{aligned}$$

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

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

With this observation and Proposition 29, we get

$$\begin{aligned}I_{k,\ell}^{(\delta)} &= \frac{16}{\pi^2}\sum_{(n,m)\in J}\frac{\cos(2\ell\pi\delta)}{mn}\int_0^1 \sin(2n\pi\cdot kt)\sin(2m\pi\cdot\ell t)\,\mathrm{d}t \\ &= \frac{16}{\pi^2}\sum_{\text{odd } a>0}\frac{\cos(2\ell\pi\delta)}{k\ell\cdot a^2}\int_0^1 \sin(2k\ell a\pi\cdot t)\sin(2k\ell a\pi\cdot t)\,\mathrm{d}t \\ &= \frac{16}{\pi^2}\cdot\frac{1}{k\ell}\sum_{\text{odd } a>0}\frac{1}{a^2}\cdot\frac{\cos(2\ell\pi\delta)}{2} \qquad \text{(By Proposition 29)} \\ &= \frac{\cos(2\ell\pi\delta)}{k\ell}\cdot\frac{\cancel{8}}{\cancel{\pi^2}}\cdot\frac{\cancel{\pi^2}}{\cancel{8}} = \frac{\cos(2\ell\pi\delta)}{k\ell} \qquad \text{(Because } \sum_{\text{odd } a>0}\tfrac{1}{a^2} = \tfrac{3}{4}\cdot\zeta(2) = \tfrac{\pi^2}{8}\text{)}\end{aligned}$$

Combining Claim 31 and Claim 32, 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 30 generalizes the result to all $k, \ell \in F_p$ by considering $g = \gcd(k, \ell)$. This proves our lemma Lemma 10 that

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

◀ ◀

B.4 Proof of Corollary 12 second part

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 $[1:2]$, $[1:3]$, $\dots$, $[1:(p-1)]$ (because $\alpha_1 \neq \alpha_2$ and $0 \notin \{\alpha_1, \alpha_2\}$).

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

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

In this set, for any particular a, the corresponding positive b lies in the set $\{1, 3, 5, \dots, 2n_a - 1\}$, 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

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

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 B.4.1 proves the upper bound

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

for all $p \geqslant 11$.

B.4.1 Proof of inequality

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.

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

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

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

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 $p \geqslant 11$.

B.5 Proof of Corollary 13

Proof. Our efficient adversary outputs the s indicated in Theorem 7. 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 [25] to obtain $(u, v) \in [\alpha_1 : \alpha_2]$ such that $|u|_p, |v|_p \leqslant B$, where $B = \lceil 8^{1/4}\cdot\sqrt{p}\rceil$. Define $g = \gcd(|u|_p, |v|_p)$.

We are given that $\varepsilon_{\mathrm{LSB}}(\vec{\alpha}) > 2\cdot\mathrm{err}$. We claim that $\varepsilon^{(\mathrm{est})}_{\mathrm{LSB}}(\vec{\alpha}) > \mathrm{err}$ 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, $\varepsilon^{(\mathrm{est})}_{\mathrm{LSB}}(\vec{\alpha}) = 0$ and, hence, $\varepsilon_{\mathrm{LSB}}(\vec{\alpha}) \leqslant \mathrm{err}$, by Corollary 11; a contradiction.
2. If $\varepsilon^{(\mathrm{est})}_{\mathrm{LSB}}(\vec{\alpha}) \leqslant \mathrm{err}$ 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 11; a contradiction.

So, the signs of $\varepsilon^{(\mathrm{est})}_{\mathrm{LSB}}(\vec{\alpha})$ 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 34). Using this property, Appendix B.6 proves that the advantage of the maximum likelihood decoder is

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

◀

B.6 Additional Proof for Corollary 13

▷ Claim 34. 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 $\varepsilon_{\mathrm{LSB}}(\vec{\alpha}) > 2 \cdot \mathrm{err}$,

$$\mathrm{sign}\left(\varepsilon^{(\mathrm{est})}_{\mathrm{LSB}}(\vec{\alpha})\right) = \mathrm{sign}\left(\frac{\Sigma^{(0)}_{\alpha_1,\alpha_2} - \Sigma^{(\Delta)}_{\alpha_1,\alpha_2}}{p}\right)$$

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

Proof.

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

(Lemma 9, $\delta = \frac{\mathrm{sign}_p(\Delta)|\Delta|_p}{p}$)

Equivalently,

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

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

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

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

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

Hence,

$$\begin{aligned}
\mathrm{sign}\left(\frac{\Sigma^{(0)}_{\alpha_1,\alpha_2} - \Sigma^{(\Delta)}_{\alpha_1,\alpha_2}}{p}\right) &= \mathrm{sign}\left(\mathrm{sign}_p(\alpha_1) \cdot \mathrm{sign}_p(\alpha_2) \cdot \left(I^{(0)}_{|\alpha_1|_p,|\alpha_2|_p} - I^{(\delta)}_{|\alpha_1|_p,|\alpha_2|_p}\right)\right) \\
&= \mathrm{sign}\left(\mathrm{sign}_p(\alpha_1) \cdot \mathrm{sign}_p(\alpha_2) \cdot \left(\sin^2(|v|_p \pi \cdot \delta) \cdot \frac{g^2}{|u|_p \cdot |v|_p}\right)\right) \\
&\qquad \text{(Lemma 10)} \\
&= \mathrm{sign}\left(\mathrm{sign}_p(\alpha_1) \cdot \mathrm{sign}_p(\alpha_2)\right) \qquad \left(\sin^2(|v|_p \pi \cdot \delta) \cdot \tfrac{g^2}{|u|_p \cdot |v|_p} > 0\right) \\
&= \mathrm{sign}\left(\varepsilon^{(\mathrm{est})}_{\mathrm{LSB}}(\vec{\alpha})\right)
\end{aligned}$$

.

◀ ◀

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 $\varepsilon^{(\mathrm{est})}_{\mathrm{LSB}}(\vec{\alpha}; s) \in [0,1]$ satisfying

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

where $\mathrm{err} := \frac{8^{5/4}}{\sqrt{p}} + \frac{13/2}{p}$. Given Claim 34, we know that for any secret $s \in F$,

$$\varepsilon_{\mathrm{LSB}}(\vec{\alpha}; s) \geqslant \varepsilon^{(\mathrm{est})}_{\mathrm{LSB}}(\vec{\alpha}; s) - \mathrm{err}. \tag{11}$$

and

$$\varepsilon^{(\mathrm{est})}_{\mathrm{LSB}}(\vec{\alpha}; s) \geqslant \varepsilon_{\mathrm{LSB}}(\vec{\alpha}; s) - \mathrm{err}. \tag{12}$$

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

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

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

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

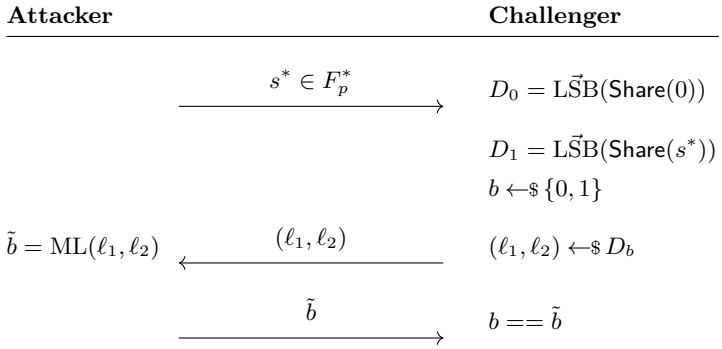
$$\begin{aligned}
\varepsilon_{\mathrm{LSB}}(\vec{\alpha}; s^*) &\geqslant \varepsilon^{(\mathrm{est})}_{\mathrm{LSB}}(\vec{\alpha}; s^*) - \mathrm{err} = \varepsilon^{(\mathrm{est})}_{\mathrm{LSB}}(\vec{\alpha}) - \mathrm{err} && \text{(Equation 11)} \\
&\geqslant \varepsilon^{(\mathrm{est})}_{\mathrm{LSB}}(\vec{\alpha}; \tilde{s}^*) - \mathrm{err} && (\varepsilon^{(\mathrm{est})}_{\mathrm{LSB}}(\vec{\alpha}; s^*) = \max_{s \in F} \varepsilon^{(\mathrm{est})}_{\mathrm{LSB}}(\vec{\alpha}; s)) \\
&\geqslant \varepsilon_{\mathrm{LSB}}(\vec{\alpha}; \tilde{s}^*) - 2 \cdot \mathrm{err} && \text{(Equation 12)} \\
&= \varepsilon_{\mathrm{LSB}}(\vec{\alpha}) - 2 \cdot \mathrm{err} > 0
\end{aligned}$$

Therefore, the distinguishing advantage of the maximum likelihood decoder is

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

B.7 Efficient Distinguisher 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 $b = \tilde{b}$.



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

$$\begin{aligned}
&\Pr[(\ell_1, \ell_2)|s = 0] - \Pr[(\ell_1, \ell_2)|s = s^*] \\
&= (-1)^{\ell_1+\ell_2} \cdot \frac{\Sigma^{(0)}_{u,v} - \Sigma^{(\Delta)}_{u,v}}{4p} && \text{(Appendix B.1)} \\
&= \frac{(-1)^{\ell_1+\ell_2} \cdot \mathrm{sign}_p(u) \cdot \mathrm{sign}_p(v)}{4} \cdot \left(I^{(0)}_{|u|,|v|} - I^{(\delta)}_{|u|,|v|} \pm 2 \cdot \frac{4(|u| + |v|) - (3/2)}{p} \right) \\
& && \text{(Lemma 9, } \delta = \tfrac{\mathrm{sign}_p(\Delta)|\Delta|_p}{p}\text{)} \\
&= \frac{(-1)^{\ell_1+\ell_2} \cdot \mathrm{sign}_p(u) \cdot \mathrm{sign}_p(v)}{4} \cdot \left(\sin^2(|v|\pi \cdot \delta) \cdot \frac{g^2}{|u| \cdot |v|} \pm 2 \cdot \frac{4(|u| + |v|) - (3/2)}{p} \right) \\
& && \text{(Lemma 10)}
\end{aligned}$$

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

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

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

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

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 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 [31] 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 35** (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 [13, 26]. 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 $[\alpha_1 \colon \cdots \colon \alpha_n]$.

D Security against Physical Bit Leakage Corollaries

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.

D.1 Statement and Proof of Corollary 36

▶ **Corollary 36.** *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*

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

Then,

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

Proof. If $2^t \cdot \alpha_1 = \alpha_2$, for some $t \in \{0, 1, \ldots, \lambda - 1\}$, we have $\varepsilon^{(\mathrm{est})}_{\mathrm{PHYS}}(\vec{\alpha}) = 1$. Lemma 15 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

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

If $2^t \alpha_1 \neq \alpha_2$, for all $t \in \{0, 1, \ldots, \lambda - 1\}$, Lemma 16 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 35 in Appendix C. Therefore, we conclude the following:

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

We know that our estimation $\varepsilon^{(\text{est})}_{\text{LSB}}(\cdot)$ is a tight estimation of $\varepsilon_{\text{LSB}}(\cdot)$, by Corollary 11. Therefore, we conclude that

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

◀

D.2 Statement and Proof of Corollary 17

▶ **Corollary 37.** *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 2 determines $\vec{\alpha}$ to be secure. Then,*

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

Among all possible distinct evaluation places $\alpha_1, \alpha_2 \in F_p^*$, the algorithm of Figure 1 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 2 determined (α_1, α_2) to be secure, then the algorithm in Figure 1 determined $(2^t\alpha_1, \alpha_2)$ to be secure, for all $t \in \{0, 1, \dots, \lambda - 1\}$. For $t \in \{0, 1, \dots, \lambda - 1\}$, by Corollary 12, we get the bound that

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

Just like the proof of Corollary 36, we have

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

Proof of the second part. If the algorithm in Figure 2 outputs "may be insecure" then there is some $k \in \{0, 1, \dots, \lambda - 1\}$ such that the algorithm in Figure 1 outputs "may be insecure" for $(2^k\alpha_1, \alpha_2)$. Corollary 12 proves that the algorithm in Figure 1 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 $k \in \{0, 1, \dots, \lambda - 1\}$, Figure 2 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. ◀

D.3 Statement and Proof of Corollary 38

▶ **Corollary 38.** *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 15 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 16 helps relate physical bit attacks and LSB attacks. Suppose t is the witness such that $\varepsilon^{(\mathrm{est})}_{\mathrm{PHYS}}(\vec{\alpha}) = \varepsilon^{(\mathrm{est})}_{\mathrm{LSB}}(\ (2^t \alpha_1, \alpha_2)\ )$. Then, consider the adversary against $\mathsf{ShamirSS}(2, 2,\ (2^t \alpha_1, \alpha_2)\ )$ that uses the LSB attack as guaranteed by Corollary 13. Lemma 16 proves that the leakage distribution of the physical bit attack $\mathrm{P}\vec{\mathrm{H}}\mathrm{Y}\mathrm{S}_{0,t}$ on $\mathsf{ShamirSS}(2, 2, \vec{\alpha})$ secret-sharing scheme has an identical distribution. So, we run the adversary of Corollary 13 by leaking $\mathrm{P}\vec{\mathrm{H}}\mathrm{Y}\mathrm{S}_{0,t}$ from the secret shares of the $\mathsf{ShamirSS}(2, 2, \vec{\alpha})$ secret-sharing scheme. ◀

D.4 Statement and Proof of Corollary 39

▶ **Corollary 39.** *Let F_p be the prime field of order $p = 2^\lambda - 1$. Define $t := \lfloor \lambda/2 \rfloor$. Consider $\vec{\alpha} = (\alpha_1, \alpha_2) \in [1 \colon 2^t - 1]$. 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 Theorem 7. 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 Theorem 7, 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 Theorem 7, 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

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

Substitute $u' = 2^j$, where $1 \leqslant j \leqslant \lfloor \lambda/2 \rfloor$, and $v' = -(2^{\lambda-t}-1)$. Therefore, by Theorem 7, 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 D.4.1 proves the following upper bound on the insecurity for all $0 \leqslant i < \lambda$.

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

◀

D.4.1 Proof of maximum insecurity bound in Corollary 39

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.5 Proof of Lemma 16

$$
\begin{aligned}
&2\mathsf{SD}\left(\vec{\mathrm{PHYS}}_{i,j}(\mathsf{Share}(0))\ ,\ \vec{\mathrm{PHYS}}_{i,j}(\mathsf{Share}(s))\right)\\
&\quad=\sum_{\vec{\ell}\in\{0,1\}^2}\left|\Pr\left[\vec{\mathrm{PHYS}}_{i,j}(\mathsf{Share}(0))=\vec{\ell}\right]-\Pr\left[\vec{\mathrm{PHYS}}_{i,j}(\mathsf{Share}(s))=\vec{\ell}\right]\right|\\
&\quad=\sum_{\vec{\ell}\in\{0,1\}^2}\Bigg|\mathop{\mathbb{E}}_{x}\left[\mathbb{1}_{\mathrm{PHYS}_i^{-1}(\ell_1)}(\alpha_1 x)\cdot\mathbb{1}_{\mathrm{PHYS}_j^{-1}(\ell_2)}(\alpha_2 x)\right]\\
&\qquad\qquad-\mathop{\mathbb{E}}_{x}\left[\mathbb{1}_{\mathrm{PHYS}_i^{-1}(\ell_1)}(\alpha_1 x+s)\cdot\mathbb{1}_{\mathrm{PHYS}_j^{-1}(\ell_2)}(\alpha_2 x+s)\right]\Bigg|\\
&\quad=\sum_{\vec{\ell}\in\{0,1\}^2}\Bigg|\mathop{\mathbb{E}}_{x}\left[\mathbb{1}_{\mathrm{PHYS}_i^{-1}(0)}(\alpha_1 x)\cdot\mathbb{1}_{\mathrm{PHYS}_j^{-1}(0)}(\alpha_2 x)\right]\\
&\qquad\qquad-\mathop{\mathbb{E}}_{x}\left[\mathbb{1}_{\mathrm{PHYS}_i^{-1}(0)}(\alpha_1 x+s)\cdot\mathbb{1}_{\mathrm{PHYS}_j^{-1}(0)}(\alpha_2 x+s)\right]\Bigg|\\
&\qquad\qquad\qquad\qquad\text{(Using the fact that } \mathbb{1}_{\mathrm{PHYS}_k^{-1}(1)}=1-\mathbb{1}_{\mathrm{PHYS}_k^{-1}(0)}\text{)}\\
&\quad=4\cdot\Bigg|\mathop{\mathbb{E}}_{x}\left[\mathbb{1}_E(2^{-i}\alpha_1 x)\cdot\mathbb{1}_E(2^{-j}\alpha_2 x)\right]\\
&\qquad\qquad-\mathop{\mathbb{E}}_{x}\left[\mathbb{1}_E(2^{-i}\alpha_1 x+2^{-i}s)\cdot\mathbb{1}_E(2^{-j}\alpha_2 x+2^{-j}s)\right]\Bigg| \qquad (13)
\end{aligned}
$$

At this point, we introduce the following variable renaming.

▷ Claim 40. The quantity

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

is identical to

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

where

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

The proof of this claim is by direct substitution. Note that $s\mapsto s'$ is an automorphism over F^*. We continue the derivation from the expression in Equation 13 as follows.

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

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.

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

▶ **Lemma 41.** *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 $\varepsilon_{\text{PHYS}}(\alpha_i, \alpha_j)$. Then,*

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

Note that if $\varepsilon_{\text{PHYS}}(\alpha_i, \alpha_j)$ is large, then there is a leakage attack on $\mathsf{ShamirSS}(3, 2, \vec{\alpha})$.

E.1 Proof of Lemma 41

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.

E.1.1 Against LSB Leakage

$$\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\}^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| \\
&\quad= \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| \\
&\quad= \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 21)} \\
&\quad= \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| \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (X \cdot 2^{-1} \mapsto Y, t = s \cdot 2^{-1}) \\
&\quad= \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|
\end{aligned}$$

Observe that

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

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

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

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} \mathrm{sign}_p(\alpha_i Y) \, \mathrm{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} \mathrm{sign}_p(\alpha_i Y + t) \, \mathrm{sign}_p(\alpha_j Y + t) \right) \\
&\qquad + (-1)^{\ell_1 + \ell_2 + \ell_3} \sum_{Y \in F_p} \mathrm{sign}_p(\alpha_1 Y) \, \mathrm{sign}_p(\alpha_2 Y) \, \mathrm{sign}_p(\alpha_3 Y) \\
&\qquad \left. - (-1)^{\ell_1 + \ell_2 + \ell_3} \sum_{Y \in F_p} \mathrm{sign}_p(\alpha_1 Y + t) \, \mathrm{sign}_p(\alpha_2 Y + t) \, \mathrm{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} \mathrm{sign}_p(\alpha_i Y) \, \mathrm{sign}_p(\alpha_j Y) - \sum_{Y \in F_p} \mathrm{sign}_p(\alpha_i Y + t) \, \mathrm{sign}_p(\alpha_j Y + t) \right) \right. \\
&\qquad + (-1)^{\ell_1 + \ell_2 + \ell_3} \cdot \sum_{Y \in F_p} \mathrm{sign}_p(\alpha_1 Y) \, \mathrm{sign}_p(\alpha_2 Y) \, \mathrm{sign}_p(\alpha_3 Y) \\
&\qquad \left. - (-1)^{\ell_1 + \ell_2 + \ell_3} \cdot \sum_{Y \in F_p} \mathrm{sign}_p(\alpha_1 Y + t) \, \mathrm{sign}_p(\alpha_2 Y + t) \, \mathrm{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(\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)}
\end{aligned}$$

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

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

Then,

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

Analogously, we define

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

Consider the following generalization of Claim 22.

▷ Claim 42. For $k, \ell, m \in \{1, 2, \dots\}$ and $\Delta, \Delta' \in \{0, 1, \dots, (p-1)\}$,

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

Proof.

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

◀ ◀

▷ Claim 43. 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.

$$\begin{aligned}
\widetilde{\Sigma}^{(\Delta,\Delta')}_{k,\ell,m} &= \sum_{X \in F_p} \widetilde{\mathrm{sign}}_p(k \cdot X) \cdot \widetilde{\mathrm{sign}}_p(\ell \cdot (X-\Delta)) \cdot \widetilde{\mathrm{sign}}_p(m \cdot (X-\Delta')) \\
&= \sum_{X \in F_p} \varphi(k \cdot X/p) \cdot \varphi(\ell \cdot (X-\Delta)/p) \cdot \varphi(m \cdot (X-\Delta')/p) \quad (\widetilde{\mathrm{sign}}_p(X) = \varphi(X/p)) \\
&= \sum_{x \in \{\frac{0}{p}, \frac{1}{p}, \dots, \frac{p-1}{p}\}} \varphi(k \cdot x) \cdot \varphi(\ell \cdot (x-\Delta/p)) \cdot \varphi(m \cdot (x-\Delta'/p))
\end{aligned}$$

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

$$\varphi(x) = \sum_{\text{odd } n>0} \frac{4}{\pi n} \cdot \sin(2n\pi x). \tag{14}$$

Substituting $\varphi(x)$ in the expression for $\widetilde{\Sigma}^{(\Delta,\Delta')}_{k,\ell,m}$ with Equation 14,

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

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

$$\begin{aligned}
&4\cdot\sin(2n_1\pi kx)\cdot\sin(2n_2\pi\ell\cdot(x-\Delta/p))\cdot\sin(2n_3\pi m\cdot(x-\Delta'/p))\\
&\quad=\sin(2\pi x\cdot(n_1k-n_2\ell+n_3m)+2\pi\cdot(n_2\ell\Delta-n_3m\Delta')/p)\\
&\quad\quad-\sin(2\pi x\cdot(n_1k-n_2\ell-n_3m)+2\pi\cdot(n_2\ell\Delta+n_3m\Delta')/p)\\
&\quad\quad-\sin(2\pi x\cdot(n_1k+n_2\ell+n_3m)+2\pi\cdot(-n_2\ell\Delta-n_3m\Delta')/p)\\
&\quad\quad+\sin(2\pi x\cdot(n_1k+n_2\ell-n_3m)+2\pi\cdot(-n_2\ell\Delta+n_3m\Delta')/p)
\end{aligned}$$

Define $a_1 = n_1k-n_2\ell+n_3m, a_2 = n_1k-n_2\ell-n_3m, a_3 = n_1k+n_2\ell+n_3m, a_4 = n_1k+n_2\ell-n_3m$ where $a_1,a_2,a_3,a_4\in\mathbb{Z}$ and define $b_1 = n_2\ell\Delta-n_3m\Delta', b_2 = n_2\ell\Delta+n_3m\Delta', b_3 = n_2\ell\Delta+n_3m\Delta', b_4 = -n_2\ell\Delta+n_3m\Delta'$ where $b_1,b_2,b_3,b_4\in\mathbb{Z}$ as well.

$$\begin{aligned}
&\sum_{x\in\{\frac{0}{p},\frac{1}{p},\ldots,\frac{p-1}{p}\}}\sin(2\pi\cdot a_1x+2\pi\cdot b_1/p)\\
=&\sum_{y\in\{\frac{0}{p},\frac{1}{p},\ldots,\frac{p-1}{p}\}}\sin(2\pi\cdot(y+b_1/p)) && (a_1\in\mathbb{Z})\\
=&\sum_{y\in\{\frac{0}{p},\frac{1}{p},\ldots,\frac{p-1}{p}\}}\sin(2\pi\cdot y) && (b_1/p\in 1/p\cdot\mathbb{Z})\\
=&0
\end{aligned}$$

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

$$\begin{aligned}
&\sum_{x\in\{\frac{0}{p},\frac{1}{p},\ldots,\frac{p-1}{p}\}}\sin(2\pi\cdot a_2x+2\pi\cdot b_2/p)=0\\
&\sum_{x\in\{\frac{0}{p},\frac{1}{p},\ldots,\frac{p-1}{p}\}}\sin(2\pi\cdot a_3x+2\pi\cdot b_3/p)=0\\
&\sum_{x\in\{\frac{0}{p},\frac{1}{p},\ldots,\frac{p-1}{p}\}}\sin(2\pi\cdot a_4x+2\pi\cdot b_4/p)=0
\end{aligned}$$

Combining all terms, we get

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

which implies that

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

◀ ◀

Apply Claim 43 to Claim 42, we get

▷ Claim 44. For $k, \ell, m \in \{1, 2, \dots\}$ and $\Delta, \Delta' \in \{0, 1, \dots, (p-1)\}$,

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

Claim 44 implies that

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

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,

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

E.1.2 Against arbitrary physical bit leakage attack

Let $\mathrm{PHYS}_i \colon F \to \{0,1\}$ be defined as in Section 7. $\mathrm{PHYS}_i \colon F \to \{0,1\}$ is the function that outputs the i-th least significant bit in the binary representation.

▷ Claim 45. For all $i \in \{0, 1, \dots, \lambda - 1\}$, we have $\mathrm{PHYS}_i(x) = \mathrm{LSB}(x \cdot 2^{-i})$ for $x \in F$.

$$
\begin{aligned}
&2\mathsf{SD}\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}\left|\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]\right.\\
&\qquad\qquad\left.-\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]\right|\\
&\quad=\sum_{\vec{\ell}\in\{0,1\}^3}\left|\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]\right.\\
&\quad\left.-\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]\right|\\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\text{(By Claim 45)}\\
&\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\text{(Claim 21)}\\
&\quad=\frac{1}{8}\cdot\frac{1}{p}\sum_{\vec{\ell}\in\{0,1\}^3}\left|\sum_{X\in F_p}\prod_{j=1}^{3}\left(1+(-1)^{\ell_j}\operatorname{sign}_p(\alpha_jX\cdot2^{-i_j})\right)\right.\\
&\qquad\qquad\left.-\sum_{X\in F_p}\prod_{j=1}^{3}\left(1+(-1)^{\ell_j}\operatorname{sign}_p((\alpha_jX+s)\cdot2^{-i_j})\right)\right|
\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,

$$\begin{aligned}
&2\mathsf{SD}\left(\vec{\mathrm{PHYS}}_{i_1,i_2,i_3}(\mathsf{Share}(0))\ ,\ \vec{\mathrm{PHYS}}_{i_1,i_2,i_3}(\mathsf{Share}(s))\right)\\
=&\frac{1}{8p}\cdot\sum_{\vec{\ell}\in\{0,1\}^3}\left|\sum_{1\leqslant j_1<j_2\leqslant 3}(-1)^{\ell_{j_1}+\ell_{j_2}}\cdot\left(\sum_{X\in F_p}\mathrm{sign}_p(\alpha_{j_1}X\cdot 2^{-i_{j_1}})\,\mathrm{sign}_p(\alpha_{j_2}X\cdot 2^{-i_{j_2}})\right.\right.\\
&\qquad\left.-\sum_{X\in F_p}\mathrm{sign}_p((\alpha_{j_1}X+s)\cdot 2^{-i_{j_1}})\,\mathrm{sign}_p((\alpha_{j_2}X+s)\cdot 2^{-i_{j_2}})\right)\\
&\quad+(-1)^{\ell_1+\ell_2+\ell_3}\cdot\left(\sum_{X\in F_p}\mathrm{sign}_p(\alpha_1X\cdot 2^{-i_1})\,\mathrm{sign}_p(\alpha_2X\cdot 2^{-i_2})\,\mathrm{sign}_p(\alpha_3X\cdot 2^{-i_2})\right.\\
&\qquad\left.\left.-\sum_{X\in F_p}\mathrm{sign}_p((\alpha_1X+s)\cdot 2^{-i_1})\,\mathrm{sign}_p((\alpha_2X+s)\cdot 2^{-i_2})\,\mathrm{sign}_p((\alpha_3X+s)\cdot 2^{-i_3})\right)\right| \qquad (15)
\end{aligned}$$

At this point, we introduce the following variable renaming.

▷ Claim 46.

$$\begin{aligned}
&\mathrm{sign}_p(\alpha_1X\cdot 2^{-i_1}+2^{-i_1}\cdot s)\cdot\mathrm{sign}_p(\alpha_2X\cdot 2^{-i_2}+2^{-i_2}\cdot s)\\
&=\mathrm{sign}_p(\alpha_1Y\cdot 2^{-i_1}+s')\cdot\mathrm{sign}_p(\alpha_2Y\cdot 2^{-i_2}+s')
\end{aligned}$$

where

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

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

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

$$\begin{aligned}
&\sum_{X\in F_p}\mathrm{sign}_p(\alpha_{j_1}X\cdot 2^{-i_{j_1}})\,\mathrm{sign}_p(\alpha_{j_2}X\cdot 2^{-i_{j_2}})-\sum_{X\in F_p}\mathrm{sign}_p((\alpha_{j_1}X+s)\cdot 2^{-i_{j_1}})\,\mathrm{sign}_p((\alpha_{j_2}X+s)\cdot 2^{-i_{j_2}})\\
&=\sum_{X\in F_p}\mathrm{sign}_p(\alpha_{j_1}X\cdot 2^{-i_{j_1}})\,\mathrm{sign}_p(\alpha_{j_2}X\cdot 2^{-i_{j_2}})-\sum_{Y\in F_p}\mathrm{sign}_p(\alpha_{j_1}Y\cdot 2^{-i_{j_1}}+s')\,\mathrm{sign}_p(\alpha_{j_2}Y\cdot 2^{-i_{j_2}}+s')\\
&\qquad\qquad\text{(By Claim 46)}\\
&=\sum_{X\in F_p}\mathrm{sign}_p(\alpha'_{j_1}X)\,\mathrm{sign}_p(\alpha'_{j_2}X)-\sum_{Y\in F_p}\mathrm{sign}_p(\alpha'_{j_1}Y+s')\,\mathrm{sign}_p(\alpha'_{j_2}Y+s')\\
&\qquad\qquad(\alpha_{j_1}\cdot 2^{-i_{j_1}}\mapsto\alpha'_{j_1}\text{ and }\alpha_{j_2}\cdot 2^{-i_{j_2}}\mapsto\alpha'_{j_2})\\
&=\Sigma^{(0)}_{\alpha'_{j_1},\alpha'_{j_2}}-\Sigma^{(\Delta_{j_1,j_2})}_{\alpha'_{j_1},\alpha'_{j_2}} \qquad (16)
\end{aligned}$$

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,

$$\begin{aligned}
&\sum_{X\in F_p} \mathrm{sign}_p(\alpha_1 X \cdot 2^{-i_1}) \,\mathrm{sign}_p(\alpha_2 X \cdot 2^{-i_2}) \,\mathrm{sign}_p(\alpha_3 X \cdot 2^{-i_2}) \\
&\qquad - \sum_{X\in F_p} \mathrm{sign}_p((\alpha_1 X + s)\cdot 2^{-i_1}) \,\mathrm{sign}_p((\alpha_2 X + s)\cdot 2^{-i_2}) \,\mathrm{sign}_p((\alpha_3 X + s)\cdot 2^{-i_3}) \\
&= \sum_{X\in F_p} \mathrm{sign}_p(\alpha'_1 X) \,\mathrm{sign}_p(\alpha'_2 X) \,\mathrm{sign}_p(\alpha'_3 X) \\
&\qquad - \sum_{X\in F_p} \mathrm{sign}_p(\alpha'_1 X + s\cdot 2^{-i_1}) \,\mathrm{sign}_p(\alpha'_2 X + s\cdot 2^{-i_2}) \,\mathrm{sign}_p(\alpha'_3 X + s\cdot 2^{-i_3}) \\
&= \sum_{X\in F_p} \mathrm{sign}_p(\alpha'_1 X) \,\mathrm{sign}_p(\alpha'_2 X) \,\mathrm{sign}_p(\alpha'_3 X) \\
&\qquad - \sum_{Y\in F_p} \mathrm{sign}_p(\alpha'_1 Y) \,\mathrm{sign}_p(\alpha'_2 (Y-\Delta)) \,\mathrm{sign}_p(\alpha'_3 (Y-\Delta')) \\
&\qquad\qquad\qquad\qquad\qquad\qquad (X + s\cdot 2^{-i_1}\cdot(\alpha'_1)^{-1} \mapsto Y) \\
&= \Sigma^{(0,0)}_{\alpha'_1,\alpha'_2,\alpha'_3} - \Sigma^{(\Delta,\Delta')}_{\alpha'_1,\alpha'_2,\alpha'_3} \qquad (17)
\end{aligned}$$

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 44, we get

$$\begin{aligned}
&\Sigma^{(0,0)}_{\alpha'_1,\alpha'_2,\alpha'_3} - \Sigma^{(\Delta,\Delta')}_{\alpha'_1,\alpha'_2,\alpha'_3} \\
&\quad = - \sum_{T\in\{\Delta,\Delta'\}} \mathrm{sign}_p(\alpha'_1\cdot T)\cdot \mathrm{sign}_p(\alpha'_2\cdot(T-\Delta))\cdot \mathrm{sign}_p(\alpha'_3\cdot(T-\Delta'))
\end{aligned}$$

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 16 and Equation 17 to the expression in Equation 15 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,

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

F Extension to arbitrary Number of Parties and proof

F.1 Proof of Corollary 19

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 18, 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 47.** *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.1.1 proves this lemma. We use the algorithm in Figure 2 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 17. The probability of the algorithm in Figure 2 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 17). If no such pair of secure indices exit, then report *failure*. Otherwise, if one such pair exists, by Theorem 18, $\mathsf{ShamirSS}(n, n, \vec{\alpha})$ has insecurity

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

By union bound, the failure probability is

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

◀

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

F.1.1 Proof of Lemma 47

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 $[1:2], [1:3], \ldots, [1:p-1]$.

F.2 Proof of Theorem 18

F.2.1 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 [13, 26].

▶ **Theorem 48** (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.

F.3 Fourier Basics

F.3.1 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 49** (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 50.** *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 51** (Properties of Fourier Coefficients). *For all $S \subseteq F$ and $x, \alpha \in F$, it holds that*

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

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

F.4 Some Preparatory Results

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

▶ **Proposition 52.** *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* $s \in F$*.*

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

Proof. The following identity is known in the literature (see [27] for proof).

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

By Proposition 50, $\widehat{\mathbb{1}_{\tau_i^{-1}(\ell_i)}}(\gamma_i) = \widehat{\mathbb{1}_{\tau_i^{-1}(1-\ell_i)}}(\gamma_i)$ since $\tau_i^{-1}(\ell_i)$ and $\tau_i^{-1}(1-\ell_i)$ are a partition of F. Using this property, one can verify for every $\vec{\ell},\vec{\ell'}\in\{0,1\}^n$, it holds that

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

Therefore, we have

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

as desired. ◀ ◀

▶ **Proposition 53.** *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.

$$\sum_{t\in F}\prod_{i=1}^{n}\left(\widehat{\mathbb{1}_{A_i\cdot\beta_i}}(t)\cdot\omega^{s\cdot t\cdot\beta_i}\right)$$

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

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

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

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

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

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

$$=\frac{1}{p^{n-1}}\sum_{\substack{x_n\in A_n\cdot\beta_n\\ \vdots\\ x_3\in A_3\cdot\beta_3}}\sum_{x_2\in F}\mathbb{1}_{A_2\cdot\beta_2}(x_2)\cdot\mathbb{1}_{A_1\cdot\beta_1}(s\cdot(\beta_1+\cdots+\beta_n)-(x_2+\cdots+x_n))$$

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

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

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

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

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

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

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

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

which completes the proof. ◀ ◀

F.5 Putting things together and proving Theorem 18

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 48, the dual code $C_0^{\perp}$ is the set

$\{t \cdot (\beta_1, \beta_2, \ldots, \beta_n) \colon t \in F\}$, where

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

Consider the following manipulation.

$$\begin{aligned}
&\mathsf{2SD}\left(\vec{\tau}(\mathsf{Share}(0)) \ , \ \vec{\tau}(\mathsf{Share}(s))\right) \\
&= 2^n \cdot \left| \sum_{\vec{\gamma} \in \mathcal{C}_0^{\perp} \setminus \vec{0}} \prod_{i=1}^{n} \widehat{\mathbb{1}_{\tau_i^{-1}(0)}}(\gamma_i) \cdot \left(1 - \omega^{s \cdot (\gamma_1 + \cdots + \gamma_n)}\right) \right| && (\textit{Proposition } 52) \\
&= 2^n \cdot \left| \sum_{t \in F^*} \prod_{i=1}^{n} \widehat{\mathbb{1}_{A_i}}(t \cdot \beta_i) \cdot \left(1 - \omega^{s \cdot t \cdot (\beta_1 + \cdots + \beta_n)}\right) \right| \\
&= 2^n \cdot \left| \sum_{t \in F^*} \prod_{i=1}^{n} \widehat{\mathbb{1}_{A_i \cdot \beta_i}}(t) - \sum_{t \in F^*} \prod_{i=1}^{n} \widehat{\mathbb{1}_{A_i \cdot \beta_i}}(t) \cdot \omega^{s \cdot t \cdot \beta_i} \right|
\end{aligned}$$

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 53 that

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

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

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

where $\Delta^{(s)}_{x_3,\ldots,x_n} := 2^{-1} \cdot (\sum_{i=3}^{n} x_i - s \cdot \sum_{i=1}^{n} \beta_i)$. Similar to the proof of Lemma 8 in Appendix B.1, we have

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

Suppose $\mathsf{ShamirSS}(2,2,(\beta_1,\beta_2))$ have ε insecurity against LSB. Then, it follows from Lemma 8 that

$$\left|\Sigma^{(\Delta^{(0)}_{x_3,\ldots,x_n})}_{\beta_1^{-1},\beta_2^{-1}} - \Sigma^{(\Delta^{(s)}_{x_3,\ldots,x_n})}_{\beta_1^{-1},\beta_2^{-1}}\right| \leqslant 2\varepsilon p. \tag{18}$$

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

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

which completes the proof.

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 54 (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 2 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 2 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 39 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 2.

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.