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

Jihun Hwang, Hemanta K. Maji, Hai H. Nguyen, Xiuyu Ye

Abstract

Can Shamir's secret-sharing protect its secret even when all shares are partially compromised?

For instance, repairing Reed-Solomon codewords, when possible, recovers the entire secret in the corresponding Shamir's secret sharing. Yet, Shamir's secret sharing mitigates various side-channel threats, depending on where its "secret-sharing polynomial" is evaluated. Although most evaluation places yield secure schemes, none are known explicitly; even techniques to identify them are unknown. Our work initiates research into such classifier constructions and derandomization objectives.

In this work, we focus on Shamir's scheme over prime fields, where every share is required to reconstruct the secret. We investigate the security of these schemes against single-bit probes into shares stored in their native binary representation. Technical analysis is particularly challenging when dealing with Reed-Solomon codewords over prime fields, as observed recently in the code repair literature. Furthermore, ensuring the statistical independence of the leakage from the secret necessitates the elimination of any subtle correlations between them.

In this context, we present:

1. An efficient algorithm to classify evaluation places as secure or vulnerable against the least-significant-bit leakage.
2. Modulus choices where the classifier above extends to any single-bit probe per share.
3. Explicit modulus choices and secure evaluation places for them.

On the way, we discover new bit-probing attacks on Shamir's scheme, revealing surprising correlations between the leakage and the secret, leading to vulnerabilities when choosing evaluation places naïvely.

Our results rely on new techniques to analyze the security of secret-sharing schemes against side-channel threats. We connect their leakage resilience to the orthogonality of square wave functions, which, in turn, depends on the 2-adic valuation of rational approximations. These techniques, novel to the security analysis of secret sharings, can potentially be of broader interest.

2012 ACM Subject Classification

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

Digital Object Identifier 10.4230/LIPIcs.ITC.2025.

1 Introduction

Secret-sharing schemes protect their secrets when only a few shares are compromised. *Side-channel attacks* have repeatedly circumvented their security by accumulating partial information from all shares [36, 37, 12]. For instance, *repairing Reed-Solomon codes* [27, 28], when possible, recovers the entire secret in the corresponding *Shamir's secret sharing* [60] by downloading a small amount of information per share. More alarmingly, ingenious side-channel attacks have revealed critical information about cryptographic secrets (without completely recovering them). Securing our secret-sharing schemes against various side-channel threats has become even more compelling due to the ongoing NIST standardization efforts [10], considering their wide use in key distribution [51, 64], masking schemes [12, 25], and other higher-level primitives like secure computation [22].

Local leakage resilience [4, 26] is a security metric for secret sharing against a broad spectrum of side-channel threats that leak from each share independently. Local leakages are surprisingly powerful; even single-bit probes into every share partially reveal an additively

6th Conference on Infor mation-Theoretic Cryptography (ITC 2025).
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

shared secret [43, 1, 45, 19]. Shamir's secret-sharing is a more promising alternative – its security depends on where its secret-sharing polynomial is evaluated. Most evaluation places, in particular, ensure that the cumulative leakage from bit probes into shares is statistically independent of the secret [43, 47]. However, not one choice is known explicitly; even techniques to identify them have yet to be discovered. As a result, *NIST can neither recommend evaluation places for Shamir's secret sharing nor certify their security against such attacks.* Towards alleviating this situation, it is natural to wonder:

Question: *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, they could be picked unbeknownst to the honest parties.
2. *A small number of false negatives.* Ideally, the algorithm should correctly identify most (or at least a significant fraction) of the leakage-resilient evaluation places.
3. *Efficiency.* The runtime of the classifier should not be "prohibitively large."

In fact, *explicitly identifying secure evaluation places* would be ideal. Our work initiates research into such classifier constructions and derandomization objectives.

Summary of our results. We consider Shamir's schemes where *shares of all parties are required to reconstruct the secret* and investigate their security against *arbitrary single bit-probe in each share.* We present such classifiers for *Mersenne* and *Fermat* prime modulus. Our algorithms have $\mathsf{poly}(\log p)$ running time and $\sqrt{p}\cdot\mathsf{poly}(\log p)$ false negatives for prime modulus p. For the two-party case, we present secure evaluation places explicitly. The technical workhorse is our classifier for the specific leakage that obtains each share's *least significant bit* (LSB); this classifier works for *arbitrary prime modulus.* Our classifier is accurate; we present *new bit-probing attacks* on those identified to be insecure.

Summary of our key technical challenge. For an arbitrary prime modulus $p \geqslant 3$, define the function $\mathrm{LSB}\colon F_p \to F_2$ by $\mathrm{LSB}(x) := 0$, for $x \in \{0, 2, \dots, (p-1)\}$; otherwise, $\mathrm{LSB}(x) := 1$. Fix arbitrary elements $\alpha_1, \alpha_2 \in F_p$.

Technical Question: *For a uniformly random $X \in F_p$, are the distributions $\mathrm{LSB}(\alpha_1 \cdot X)$ and $\mathrm{LSB}(\alpha_2 \cdot X)$ statistically independent?*

Answering this technical question is challenging because $x \longmapsto \mathrm{LSB}(x)$ is a *non-linear map.* Linear maps are either (perfectly) independent or (completely) correlated; answering this question for them is easy. Subtle correlations can surreptitiously manifest between non-linear maps, which is the case here. The pattern of (α_1, α_2) resulting in statistically independent distributions is highly non-trivial. We prove that it depends on the *2-adic valuation of their rational approximation*; our classifier algorithm is outlined below.

1. Solve for relatively prime integers $u, v \in \left\{-\lceil\sqrt{p}\rceil, \dots, 0, \dots, \lceil\sqrt{p}\rceil\right\}$ such that $u \cdot \alpha_2 = v \cdot \alpha_1 \mod p$.
2. Distributions are independent if (and only if) u/v has non-zero 2-adic valuation; i.e., either u or v is even.
3. Otherwise, for odd u and v, the 2-adic valuation of u/v is 0, and the dependence between these two distributions is $1/|u \cdot v|$. When this dependence is significant, we identify *new side-channel attacks.*

The connection between 2-adic valuations with security of secret sharings is novel and possibly of broader interest. Our work highlights the challenges in determining the leakage resilience of secret sharing. There are several natural follow-up questions; Section 3 presents a few and the hurdles in approaching them.

▶ Remark 1 (Recent relevant works). Maji et al. [47] and, very recently, Nguyen [52] drew inspiration from our approach and constructed such classifiers over *characteristic-2 composite-order fields*. The analogous map in their technical analysis is F_2-linear, making their technical question approachable via elementary "rank arguments" (a.k.a., dual distance of the concatenated Reed-Solomon codes over the binary alphabet). Analyzing non-linear leakage in the related literature on repairing Reed-Solomon codewords has also been technically challenging; *non-linear repairing* was only recently addressed [15, 14]. Appendix B summarizes this discussion and other prior relevant works motivating this research.

▶ Remark 2 (Other leakage-resilient alternatives). The additive and Shamir's schemes are deployed widely. It is crucial to determine their security; this work contributes to this effort. New constructions (like [6, 2, 61, 3, 39, 7, 20, 61, 21, 33, 13, 49, 11]) cannot match their simplicity and high information rate or replace them in security technologies.

1.1 Basic Definitions & Our Formal Problem Statement

Shamir's secret sharing. Shamir's secret-sharing scheme among n parties with reconstruction threshold k over a finite field F and distinct evaluation places $\alpha_1, \alpha_2, \dots, \alpha_n \in F^*$ 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: $s_1 := P(\alpha_1)$, $s_2 := P(\alpha_2)$, …, 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. *This work only considers* $n = k$.

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 $\{0, 1, \dots, (p-1)\}$.

▶ Remark 3. For a Fermat prime $p = 2^\lambda + 1$, elements of F_p require $(\lambda + 1)$ bits in their binary representation. However, only the binary representation of 2^λ has 1 in the most significant bit. For simplicity of presentation, we assume that elements are represented using λ bits only; disregarding the element $2^\lambda \in F_p$ adds only an additive $1/p$ slack to the analysis.

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

1. Physical bit leakage family: $\mathrm{PHYS} := \left\{ \vec{\mathrm{PHYS}}_{\mathbf{i}} \,:\, \mathbf{i} = (i_1, \dots, i_n) \in \{0, 1, \dots, \lambda - 1\}^n \right\}$.
2. LSB leakage family: $\mathrm{LSB} := \left\{ \vec{\mathrm{PHYS}}_{\mathbf{0}} \right\}$, where $\mathbf{0} = (0, 0, \dots, 0)$

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

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

Low insecurity indicates the statistical independence of the leakage from the secret, i.e., the *secret-sharing is locally leakage-resilient* [4, 26]. Recently, Faust et al. [19] connected this definition to practice.

High insecurity indicates a leakage function can distinguish the secret 0 and some $s^* \in F^*$ using the leakage. Maji et al. [43] analyzed the insecurity against the PHYS leakage family when *evaluation places were chosen randomly*. Their result implies the following corollary for prime modulus $p \geqslant 3$ and $n = k \geqslant 2$.

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

Recently, [47] extended the randomized construction from prime fields to composite ones.

Our 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 can be rewritten using these terminologies and notations as follows.

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

If $\varepsilon_{\text{PHYS}}(\vec{\alpha}) > p^{-1/2}$, then output a secret $s^* \in F_p^*$ such that the shares of 0 can be distinguished from the shares of s^* with (roughly) $\varepsilon_{\text{PHYS}}(\vec{\alpha})$ advantage. *All algorithms must be computationally efficient – runtime is a polynomial in λ; i.e.,* $\mathsf{poly}(\log p)$. Furthermore, concrete security analysis (over asymptotic analysis) is prioritized.

1.2 Our Results

Below, for $x, y, z \in \mathbb{R}$, the expression $x = y \pm z$ is a concise representation for "$x \in [y-z, y+z]$." For example, "x is close to y" is expressed using $x = y \pm \varepsilon$, for a small ε. Section 2 presents a high-level overview of the critical technical ideas underlying our results.

Technical Result: Security against LSB Leakage when $n = 2$ (Section 4)**.** Consider *arbitrary prime $p \geqslant 3$* (not just a Mersenne/Fermat 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 Corollary 14 and Corollary 15 shows that
$$\varepsilon_{\text{LSB}}(\vec{\alpha}) \leqslant \frac{1 + 8^{5/4}}{\sqrt{p}} + \frac{13/2}{p} \leqslant \frac{14.46}{\sqrt{p}},$$
which is exponentially small in the security parameter λ. The number of false negatives is $\mathcal{O}\left(\sqrt{p} \cdot \log p\right)$.
2. We present an efficient adversary (Corollary 16) that generates $s^* \in F^*$ such that it distinguishes the secret 0 from s^* by leaking the LSB of each share with an advantage
$$\geqslant \varepsilon_{\text{LSB}}(\vec{\alpha}) - \frac{2 \cdot 8^{5/4}}{\sqrt{p}} - \frac{13}{p} \geqslant \varepsilon_{\text{LSB}}(\vec{\alpha}) - \frac{26.91}{\sqrt{p}}.$$
Therefore, our efficient leakage attack achieves a comparable distinguishing advantage when the insecurity $\varepsilon_{\text{LSB}}(\vec{\alpha})$ is significant.

Result A: Security against Physical Bit Leakage when $n = 2$ (Section 5)**.** For the $n = k = 2$ case, we analyze a prime field F_p, where p is a Mersenne/Fermat prime – primes of the form $2^\lambda \pm 1$. 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 $\vec{\alpha}$ that is classified secure, Corollary 19 shows that the insecurity is $\varepsilon_{\text{PHYS}}(\vec{\alpha}) \leqslant 14.46/\sqrt{p}$ and the number of false negatives is $\mathcal{O}\left(\sqrt{p}\cdot(\log p)^2\right)$.
2. We present an efficient adversary that generates $(s^*, f) \in F_p^* \times \text{PHYS}$ such that it distinguishes the secret 0 from secret s^* by leaking $f \in \text{PHYS}$ from the shares with an advantage $\geqslant \varepsilon_{\text{PHYS}}(\vec{\alpha}) - 26.91/\sqrt{p}$. *These are new side-channel attacks; their existence demonstrates the tightness of our analysis and accuracy of our classifier.*
   This is direct consequence of the properties of Mersenne and Fermat primes and Corollary 16; Appendix F has the details.
3. We explicitly identify secure evaluation places against PHYS leakage: all (α_1, α_2) satisfying $\alpha_2 \cdot \alpha_1^{-1} \in \{\ \gamma,\ -\gamma,\ \gamma^{-1},\ -\gamma^{-1}\ \}$, where $\gamma = 2^{\lfloor \lambda/2 \rfloor} - 1$. For these evaluation places, we get $\varepsilon_{\text{PHYS}}(\vec{\alpha}) \leqslant 8.49/\sqrt{p}$, which Corollary 20 and Corollary 21 prove. Appendix I provides an example for Mersenne prime $p = 2^{13} - 1$.

Result B: Security against Physical Bit Leakage when $n > 2$ (Section 6)**.** Consider a prime field F_p such that $p = 2^\lambda \pm 1$ a Mersenne/Fermat prime. Figure 2 presents an efficient classifier for $\vec{\alpha}$ such that the corresponding $\mathsf{ShamirSS}(n, n, \vec{\alpha})$ is secure to physical bit probes; the insecurity is at most $1/\sqrt{p}$, as shown in Corollary 23 (Appendix G presents the proof).

Given evaluation places $\vec{\alpha} := (\alpha_1, \alpha_2, \dots, \alpha_n)$ we efficiently compute an appropriate $\vec{\beta} := (\beta_1, \beta_2, \dots, \beta_n)$ (see Equation 3). Corollary 23 proves 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. Clarifications below highlight the subtlety of this classifier:

▶ Remark 4 (Clarifications). **1.** High insecurity of $\mathsf{ShamirSS}(2, 2, (\beta_1, \beta_2))$ *does not imply* high insecurity of $\mathsf{ShamirSS}(n, n, \vec{\alpha})$; *our result lifts security only in one direction.*

2. Can the security of $\mathsf{ShamirSS}(2, 2, (\alpha_i, \alpha_j))$, for all $1 \leqslant i < j \leqslant n$, imply the security of $\mathsf{ShamirSS}(n, n, \vec{\alpha})$? *This natural classifier has false positives.* Consider $n = 3$, a prime $p = 4w^2 + 6w + 9$, and evaluation places $\vec{\alpha} = (1, \sigma, \sigma^2)$, where $w \geqslant 4$, $w \neq 0 \mod 3$, and $\sigma = 2w \cdot 3^{-1}$. For example, $p = 97$ and $\sigma = 35$; Bunyakovsky conjecture [9] implies infinitude of such primes. Against LSB leakage, although every $\mathsf{ShamirSS}(2, 2, (\alpha_i, \alpha_j))$ is secure, $\mathsf{ShamirSS}(n, n, \vec{\alpha})$ is $(2/\pi)^3 > 0.25$ insecure [45, 19]; Appendix H presents the details.

So, the following randomized strategy suffices to construct secure schemes: (1) randomly sample $\vec{\alpha}$, (2) compute $\vec{\beta}$ using our map in Figure 3, and (3) test the security of $\mathsf{ShamirSS}(2, 2, (\beta_1, \beta_2))$ using Corollary 19.

We also present explicit secure evaluation places for $n = k > 2$ case by bootstrapping from the explicit secure evaluation places for $n = k = 2$ case in Appendix I. For example, $\alpha_1 = (n-1)$, $\alpha_2 = (n-1) - (1+\gamma)$, and $\alpha_j = (j-2)\cdot(\gamma+1)$, for $j \in \{3, 4, \dots, n\}$, is secure against one physical bit probe per share if $(1, \gamma)$ is secure evaluation place for $n = k = 2$ case. Specifically, $\gamma = \sqrt{(p \pm 1)/2} - 1$ suffices for Mersenne/Fermat prime modulus.

2 Technical Overview

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

For *any prime field* F_p, we outline our classification algorithm for $(n, k) = (2, 2)$ and, en route, highlight our technical contributions (Figure 1 presents the 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 [40] 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 4 in Appendix C.
2. Remark: Our algorithm interprets $u, v \in \{-B, \ldots, 0, 1, \ldots, B\} \mod p$ as integers below.
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 $|u \cdot v / g^2| \geqslant \sqrt{p}$: 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 against LSB leakage.

Step 1. The prime modulus p and the distinct 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 [30]). We find "small norm" $u, v \in \{-\lceil\sqrt{p}\rceil, \ldots, 0, 1, \ldots, \lceil\sqrt{p}\rceil\}$ with the property mentioned above – a Dirichlet approximation problem. We solve it with a small constant multiplicative slack using the LLL [41] algorithm in $\mathsf{poly}(\lambda)$ runtime, where $\lambda := \lceil \log_2(p+1) \rceil$ (Appendix C has the details). The reasoning for choosing "small norm" u, v will be evident below in Step 3.

Step 2. We proceed to solve the technical question from Page 2: determine whether the bits $\mathrm{LSB}(u \cdot X)$ and $\mathrm{LSB}(v \cdot X)$ are statistically independent, for uniformly random $X \in F_p$. We will calculate the similarity/dependence between these two distributions, which is equivalent to the bias ε of the distribution $\mathrm{LSB}(u \cdot X) \oplus \mathrm{LSB}(v \cdot X)$. In this context, the bias is the probability that $\mathrm{LSB}(u \cdot X) = \mathrm{LSB}(v \cdot X)$ minus the probability that $\mathrm{LSB}(u \cdot X) \neq \mathrm{LSB}(v \cdot X)$. Appendix A presents some elementary failed attempts with examples; the challenge is to estimate ε efficiently and accurately.

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, $\operatorname{sign} \sin(2\pi|u| \cdot t) \in \{\pm 1\}$ 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, the first oscillating $|u|$ times and the second oscillating $|v|$ times. We provide an illustration of the integration of square waves in Appendix J. The error of our approximation is directly proportional to the total number of oscillations of the square waves. The approximation error is $\leqslant (|u|+|v|)/p = \mathcal{O}(1/\sqrt{p})$, exponentially small in λ, for small norm u, v. For simplicity, the presentation below ignores this approximation error. See Appendix J for visualizations.

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

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

Step 5. Consider the $\varepsilon = 0$ case. This happens when the highest powers of 2 dividing $|u|$ and $|v|$ differ. In this case, we prove that $\mathrm{LSB}(u \cdot X + s)$ is independent of $\mathrm{LSB}(v \cdot X + s)$, for every secret $s \in F_p$. Technically, we prove the following integral representing the bias for this general case – a phase-shifted integral from Step 2 above – is 0 for all $\delta \in [0, 1)$.

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

Note that the marginal $\mathrm{LSB}(u \cdot X + s)$ is a uniformly random bit, and so is the marginal $\mathrm{LSB}(v \cdot X + s)$. Therefore, these leakage bits are uniformly and independently random. Furthermore, the distribution of $(u \cdot X + s, v \cdot X + s)$, for uniformly random $X \in F_p$, is identical to the distribution of the shares $(s_1, s_2) = (\alpha_1 \cdot X + s, \alpha_2 \cdot X + s)$ by properties of General Reed-Solomon codes [30]. Consequently, Shamir's scheme is secure in this case because all secrets produce identical leakage distribution.

When $\varepsilon \neq 0$, $|u|$ and $|v|$ have the identical highest power of 2 dividing them. Theorem 10 presents a (closed-form) expression for a secret $s^* \in F_p^*$ such that the distributions of LSB leakage for secret 0 and secret s^* are distinguishable with an advantage of ε. We achieve this by giving the formula for the $\delta^* \in \{1/p, 2/p, \ldots, (p-1)/p\}$, such that the following integral's value is farthest from ε.

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

We then reconstruct s^* from this δ^*.

Our classification algorithm for arbitrary physical bit probes will build on the classifier outlined in this section.

▶ Remark 5. Our work connects the security of secret-sharing schemes against leakage attacks with the orthogonality properties of a family of square waves [63, 32, 31]. Various families of square waves, like the ones by Haar [29], Walsh [65], and Rademacher [55], are central to science and engineering. These techniques are new to the security analysis of secret sharings and possibly of broader interest.

2.2 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 in Mersenne prime fields.* For $i, j \in \{0, 1, \ldots, \lambda - 1\}$, consider the physical bit leakage attack $\vec{\mathrm{PHYS}}_{i,j}$. 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, $\vec{\mathrm{PHYS}}_{i,j}$ 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 [30], the leakage is identical to the LSB leakage with evaluation places $(2^{j-i} \cdot \alpha_1, \alpha_2)$. Consequently,

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

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

▶ Remark 6 (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 $t \in \{0, 1, \dots, \lambda-1\}$. So, the call to the "LSB security check subroutine" with the argument $(2^t\alpha_1, \alpha_2)$ would be invalid. Lemma 18 proves that this edge case is insecure. This case captures why evaluation places $(1, 2)$ are insecure against physical bit leakage.

Input. Distinct evaluation places $\alpha_1, \alpha_2 \in F_p^*$, and p is a Mersenne/Fermat prime.

Output. Decide whether the evaluation places (α_1, α_2) are secure to an arbitrary single physical bit leakage per share.

Algorithm.

1. If there is $t \in \{0, 1, \dots, \lambda-1\}$ such that $2^t\alpha_1 = \alpha_2$: Return insecure
2. For $t \in \{0, 1, \dots, \lambda-1\}$:
   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 ShamirSS$(2, 2, (\alpha_1, \alpha_2))$ is secure against physical bit attacks.

Figure 2 Identify secure evaluation places for Shamir's secret sharing against physical bit leakage.

For *Fermat prime* p, $x \in F_p$, and $i \in \{1, 2, \dots, \lambda-1\}$ we prove following identity.[1]

$$\text{PHYS}_{i-1}(x) = \text{PHYS}_i(2x+1). \tag{2}$$

Therefore, $\text{PHYS}_i(x) = \text{LSB}(2^{-i} \cdot x + 2^{-i} - 1)$. Like the Mersenne prime case above, arbitrary physical bit leakage translates into LSB leakage, except the map here is an *affine map* instead of a *linear map*. As a result, the secret $s^* \in F_p^*$ witnessing the maximum insecurity is different; it is still efficiently computable. See Section 5.1 for details.

▶ Remark 7. Investigating Mersenne prime modulus in the context of Shamir secret-sharing has also been done by Faust et al. [19]; the ideas to analyze Fermat prime modulus are new.

2.3 Overview of Result B: Physical Bit Leakage $n = k > 2$

Our objective is to choose n distinct evaluation places $\alpha_1, \alpha_2, \dots, \alpha_n \in F^*$ such that the corresponding ShamirSS$(n, n, \vec{\alpha})$ is secure against physical bit leakage attacks. We prove a lifting theorem (Theorem 22) that proves the following result. Given evaluation places $\vec{\alpha}$, consider $\vec{\beta}$ related to Lagrange multipliers (where $i \in \{1, 2, \dots, n\}$):

$$\beta_i := \left(\alpha_i \prod_{j \neq i} (\alpha_i - \alpha_j) \right)^{-1}. \tag{3}$$

[1] For primes other than Mersenne and Fermat primes, there is no such affine transformation.

Now consider the $\mathsf{ShamirSS}(2, 2, (\beta_i, \beta_j))$ secret-sharing scheme for all distinct $i, j \in \{1, 2, \ldots, n\}$. Suppose one of these secret-sharing schemes is secure against physical bit leakage. In that case, 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 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.

Whether the evaluation places of $\mathsf{ShamirSS}(2, 2, (\beta_i, \beta_j))$ is secure or not can be determined efficiently using our algorithm in Figure 2. We can use this algorithm to detect if our chosen $\vec{\alpha}$ has such a secure (β_i, β_j) pair of evaluation places. Corollary 23 formally states this result; its proof is entirely Fourier-analytic – Appendix G presents the necessary Fourier analysis background and proves it.

Input. Distinct evaluation places $\vec{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in (F_p^*)^n$, and p is a Mersenne or Fermat prime

Output. Decide whether the evaluation places $\vec{\alpha}$ are secure to all physical bit leakage attacks

Algorithm.

1. For $i \in \{1, 2, \ldots, n\}$, compute
$$\beta_i := \left(\alpha_i \prod_{j \neq i} (\alpha_i - \alpha_j)\right)^{-1}.$$
2. If there exist $1 \leqslant i < j \leqslant n$ such that $\mathsf{ShamirSS}(2, 2, (\beta_i, \beta_j))$ is secure per the algorithm in Figure 2, then declare that $\mathsf{ShamirSS}(n, n, \vec{\alpha})$ is <u>secure</u>.
3. Otherwise, the algorithm states that $\mathsf{ShamirSS}(n, n, \vec{\alpha})$ <u>may be insecure</u>.

Figure 3 Identify secure evaluation places for $\mathsf{ShamirSS}(n, n)$ against physical bit leakage.

▶ Remark 8. Analyzing this classifier has some subtleties. The $\vec{\alpha} \mapsto \vec{\beta}$ mapping is not a bijection; few $\vec{\beta}$ have multiple preimages, most have one, and some have none. We prove that (β_1, β_2) are (nearly) independent when $\vec{\alpha}$ is chosen uniformly at random, for $n \geqslant 3$.

▶ Remark 9 (Clarifications).

1. High insecurity of $\mathsf{ShamirSS}(2, 2, (\beta_1, \beta_2))$ *does not imply* high insecurity of $\mathsf{ShamirSS}(n, n, \vec{\alpha})$; *our result lifts security only in one direction.*
2. Can the security of $\mathsf{ShamirSS}(2, 2, (\alpha_i, \alpha_j))$, for all $1 \leqslant i < j \leqslant n$, imply the security of $\mathsf{ShamirSS}(n, n, \vec{\alpha})$? *This natural classifier has false positives.* Consider $n = 3$, a prime $p = 4w^2 + 6w + 9$, and evaluation places $\vec{\alpha} = (1, \sigma, \sigma^2)$, where $w \geqslant 4$, $w \neq 0 \mod 3$, and $\sigma = 2w \cdot 3^{-1}$. For example, $p = 97$ and $\sigma = 35$; Bunyakovsky conjecture [9] implies infinitude of such primes. Against LSB leakage, although every $\mathsf{ShamirSS}(2, 2, (\alpha_i, \alpha_j))$ is secure, $\mathsf{ShamirSS}(n, n, \vec{\alpha})$ is $(2/\pi)^3 > 0.25$ insecure [45, 19]; Appendix H presents the details.

3 Future Research Directions

There are several natural research directions for future work. A few immediate ones and their respective technical hurdles are presented below.

LSB **classifier construction for $n > 2$.** To illustrate the challenges, consider $n = 3$ and evaluation places $(\alpha_1, \alpha_2, \alpha_3)$. The rational approximation problem will require finding

small-norm u, v, w such that $\alpha_1 : \alpha_2 : \alpha_3 = u : v : w$. Dirichlet approximation theorem only guarantees $|u|, |v|, |w| \leqslant p^{(n-1)/n}$. Therefore, *the accuracy error in estimating the summation by an integral will be* $p^{(n-1)/n}/p = p^{-1/n} \gg p^{-1/2}$, for $n \geqslant 3$.
Moreover, for $\varphi(x) = \operatorname{sign}\sin(2\pi x)$, *the estimate of the integral below is not known.*

$$\int_0^1 \varphi(ut) \cdot \varphi(vt) \cdot \varphi(wt)\, \mathrm{d}t. \tag{4}$$

Arbitrary physical bit leakage in general prime modulus. Against arbitrary physical bit leakage, extension to general prime modulus seems challenging. For example, when $n = 2$, the technical challenge is to characterize (α_1, α_2) such that the distributions $\mathrm{PHYS}_i(\alpha_1 X)$ is independent of $\mathrm{PHYS}_j(\alpha_2 X)$, where X is chosen uniformly at random. The bottleneck is to establish an integral that estimates this expression for a *general prime modulus.*

More physical probes. Consider $(n, k) = (2, 2)$, evaluation places (α_1, α_2), a Mersenne prime modulus p, and physical bit leakage probing the first share twice & the second share once. The technical problem is to show the independence of the following three distributions

$$\Big(\ \mathrm{PHYS}_i(\alpha_1 X),\ \mathrm{PHYS}_j(\alpha_1 X),\ \mathrm{PHYS}_k(\alpha_2 X)\ \Big),$$

where $X \in F_p$ is chosen uniformly at random. The analysis *reduces to estimating the integral in Equation 4*, where $u = 2^{-i}\alpha_1$, $v = 2^{-j}\alpha_1$, and $w = 2^{-k}\alpha_2$, which is not known.

More general (n, k). For concreteness, consider $(n, k) = (3, 2)$ and resilience to LSB leakage. This resilience requires t-wise independence of the leakage bits, where $k \leqslant t \leqslant n$. The 2-wise independence of leakage bits can be tested using the classifier in Figure 1. The 3-wise independence test has identical hurdles as the "LSB classifier construction for $n > 2$" case discussed above. There are evaluation places where *the* LSB *leakage is 2-wise independent but 3-wise correlated* for $(n, k) = (3, 2)$. The evaluation places of Appendix H with $(n, k) = (3, 2)$ (instead of $(n, k) = (3, 3)$) have this property.

4 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 10** (Technical Result). *Consider the* $\mathsf{ShamirSS}(2, 2, (\alpha_1, \alpha_2))$ *secret-sharing scheme over a prime field* F_p*, where* $p \geqslant 3$*.*

$$\max_{s \in F} \mathsf{SD}\Big(\vec{\mathrm{LSB}}(\mathsf{Share}(0))\ ,\ \vec{\mathrm{LSB}}(\mathsf{Share}(s))\Big) = \begin{cases} \dfrac{4(|u| + |v|) - (3/2)}{p}, & \text{if } |u| \cdot |v|/g^2 \text{ is even,} \\[2ex] \left(2 - \frac{1}{2p}\right) \cdot \dfrac{g^2}{|u| \cdot |v|} \pm \dfrac{4(|u| + |v|) - (3/2)}{p} & \text{if } |u| \cdot |v|/g^2 \text{ is odd,} \end{cases}$$

where $\alpha_1 \cdot \alpha_2^{-1} = u \cdot v^{-1}$ *and* $g = \gcd(|u|, |v|)$.
Furthermore, for $s \in F_p^*$ *satisfying* $(2^{-1} \cdot s) \cdot (u^{-1} - v^{-1}) \in \frac{(2\mathbb{Z}+1)\cdot p \pm 1}{2|u||v|}$*, if*

$$\mathsf{SD}\Big(\vec{\mathrm{LSB}}(\mathsf{Share}(0))\ ,\ \vec{\mathrm{LSB}}(\mathsf{Share}(s))\Big) > \frac{4(|u| + |v|) - (3/2)}{p}$$

then there is an efficient distinguisher to distinguish the secret 0 and s with advantage at least

$$\left(2 - \frac{1}{2p}\right) \cdot \frac{g^2}{|u| \cdot |v|} \quad - \frac{4(|u|+|v|) - (3/2)}{p}$$

using the LSB *leakage on the secret shares.*

Essentially, this theorem helps estimate the insecurity efficiently. Section 4.1 presents the proof outline for this result and Appendix D presents the full proof. With this theorem, we will state and prove the corollaries mentioned in Section 1.2.

4.1 Proof outline of Theorem 10

For any $s \in F^*$, we start by obtaining a closed-form estimate of

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

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 10.

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 $u, v, \Delta \in F$, we define the following measurement of similarity between two lines uT and $v(T - \Delta)$ on F.

$$\Sigma^{(\Delta)}_{u,v} := \sum_{T \in F} \mathrm{sign}_p(uT) \cdot \mathrm{sign}_p(v(T - \Delta)). \tag{5}$$

▶ **Lemma 11.** *Consider the* $\mathsf{ShamirSS}(2, 2, (\alpha_1, \alpha_2))$ *secret-sharing scheme over a prime field* F_p*. For any secret* $s \in F_p$ *and* $(u, v) \in [\alpha_1 : \alpha_2]$*,*

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

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

Appendix D.1 proves Lemma 11.

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

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

▶ **Lemma 12.** *For any* $u, v, \Delta \in F_p$*, and* $\delta = \frac{\mathrm{sign}_p(\Delta) \cdot |\Delta|}{p} \in \mathbb{Q}$*,*

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

Appendix D.2 proves Lemma 12.

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

▶ **Lemma 13.** *Let* $\triangle\colon \mathbb{R} \to [-1,+1]$ *be the triangle wave function defined as*

$$\triangle(t) := 4 \cdot \left| t + \frac{1}{2} - \lceil t \rceil \right| - 1.$$

Then, for any $u, v \in \{1,2,\dots\}, \delta \in \mathbb{R}$, *and* $g = \gcd(u,v)$

$$I_{u,v}^{(\delta)} = \begin{cases} 0, & \text{if } u \cdot v/g^2 \text{ is even} \\ \triangle(uv \cdot \delta) \cdot \dfrac{g^2}{uv}, & \text{if } u \cdot v/g^2 \text{ is odd.} \end{cases}$$

Appendix D.3 proves Lemma 13. Intuitively, if the highest power of 2 dividing u is different from the highest power of 2 dividing v, then uv/g^2 is even and $I_{u,v}^{(\delta)} = 0$. If the highest power of 2 dividing u is identical to the highest power of 2 dividing v, then uv/g^2 is odd and $I_{u,v}^{(\delta)} \neq 0$.

Step 4. Sequentially performing the substitutions above, we can estimate the statistical distance using the integrals, which yields Theorem 10 after maximizing over every $s \in F^*$.

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

4.2 Insecurity Estimation: Statement and Proof of Corollary 14

Using Theorem 10, we prove that the estimated insecurity achieved by our classifier in Figure 1 is close to the true insecurity.

▶ **Corollary 14.** *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* $(u, v) \in [\alpha_1 \colon \alpha_2]$ *such that* $|u|, |v| \leqslant B$, *where* $B = \lceil 8^{1/4} \cdot \sqrt{p} \rceil$. *Let* $\triangle\colon \mathbb{R} \to [-1,+1]$ *be the triangle wave function* $\triangle(t) := 4 \cdot \left|t + \frac{1}{2} - \lceil t \rceil\right| - 1$. *Let* $g = \gcd(|u|, |v|)$. *Define*

$$\varepsilon_{\mathrm{LSB}}^{(\mathrm{est})}(\vec{\alpha}) := \begin{cases} 0, & \text{if } |u| \cdot |v|/g^2 \text{ is even,} \\ \triangle(|u||v| \cdot \delta) \cdot \dfrac{g^2}{|u| \cdot |v|}, & \text{if } |u| \cdot |v|/g^2 \text{ is odd.} \end{cases}$$

Then,

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

Proof. Use the LLL algorithm [41] to efficiently find $(u, v) \in [\alpha_1 \colon \alpha_2]$ with properties mentioned in the corollary (see Appendix C for details). Observe that the LHS of the expression in Theorem 10 is identical to $\varepsilon_{\mathrm{LSB}}(\vec{\alpha})$ by our definition in Equation 1. From this observation, the corollary is immediate. ◀

Next, we state the corollaries mentioned in Section 1.2 through this tight estimation.

4.3 Insecurity Identification: Statement of Corollary 15

▶ **Corollary 15.** *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* $p \geqslant 3$. *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 $p \geqslant 11$.

Appendix D.4 proves Corollary 15.

4.4 Advantage of Adversary: Statement of Corollary 16

▶ **Corollary 16.** *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 $p \geqslant 3$. 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 10. 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 D.5 provides a full proof of the distinguishing advantage and security guarantee of this adversary.

5 Security against all Physical Bit Leakage

We consider ShamirSS$(n = 2, k = 2, (\alpha_1, \alpha_2))$ over prime field F_p of order $p \geqslant 3$. Let λ be the security parameter. This section considers Mersenne and Fermat primes, i.e., primes of the form $p = 2^\lambda \pm 1$. Some initial Mersenne primes are $3, 7, 31, 127, 8191$, and 131071, and Fermat primes are $3, 5, 17, 257$, and 65537.

Mersenne and Fermat's primes satisfy the following property.

▶ **Proposition 17.** *Let λ be the security parameter. Fix an arbitrary $i \in \{0, 1, 2, \ldots, \lambda - 1\}$. For all $x \in F_p$,*

$$\text{PHYS}_i(x) = \begin{cases} \text{PHYS}_0(2^{-i}\cdot x) & \text{if } p = -1 \mod 2^{i+1} \\ \text{PHYS}_0(2^{-i}\cdot x + (2^{-i} - 1)) & \text{if } p = 1 \mod 2^{i+1} \end{cases}$$

We prove this proposition in Appendix F.1.

5.1 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 $s \in F_p$. 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 $t := s2^{-j}$. Appendix F.2 uses Proposition 17 to show that when the order of the field is a Mersenne or Fermat's prime, the joint distribution of leakage is equivalent as (for uniformly random $v \in F$)

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

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

$$(\mathrm{PHYS}_0(1 + t^* + v\alpha_1), \mathrm{PHYS}_0(t^* + v\alpha_2))$$

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 (see Appendix F.2 for details).

▶ **Lemma 18.** *Let F be the prime field of order $p = 2^\lambda \pm 1$. Consider distinct evaluation places $\alpha_1, \alpha_2 \in F^*$ such that $2^k \cdot \alpha_1 = \alpha_2$ for some $k \in \{0, 1, \ldots, \lambda - 1\}$. Then,*

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

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

5.2 Upper Bound on insecurity

▶ **Corollary 19.** *Let F be the prime field of order $p = 2^\lambda \pm 1$. 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. Suppose the algorithm in Figure 2 determines $\vec{\alpha}$ to be secure. Then,*

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

Among all possible distinct evaluation places $\alpha_1, \alpha_2 \in F^*$, 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 $p \geqslant 11$.

The proof of this corollary can be found in Appendix F.3.

5.3 Derandomization

We conclude this section by presenting a 'derandomization' result that is a direct consequence of Theorem 10.

▶ **Corollary 20.** *Let F be the prime field of Mersenne prime order $p = 2^\lambda - 1$ where $\lambda > 3$. Define $t := \lfloor \lambda/2 \rfloor$. Consider $\vec{\alpha} = (\alpha_1, \alpha_2) \in [1\colon 2^t - 1]$ respectively. Then*

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

A similar result holds for Fermat primes as well. Note that if $p = 2^\lambda + 1$ is a prime, then $\lambda/2$ is an integer because λ must be a power of 2.

▶ **Corollary 21.** *Let F be the prime field of Fermat prime order $p = 2^\lambda + 1$. Define $t := \lambda/2$. Consider $\vec{\alpha} = (\alpha_1, \alpha_2) \in [1\colon 2^t - 1]$ respectively. Then*

$$\varepsilon_{\text{PHYS}}(\vec{\alpha}) \leqslant \frac{8 \cdot 2^{\lambda/2} - 3/2}{p}.$$

See Appendix F.4 for their proofs.

6 Extension to arbitrary Number of Parties

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

▶ **Theorem 22.** *Consider $\mathsf{ShamirSS}(n, n, \vec{\alpha})$ over a prime field F. For every $i \in \{1, 2, \dots, n\}$, define*

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

Suppose there are two indices $1 \leqslant i^* < j^* \leqslant n$ such that $\mathsf{ShamirSS}(2, 2, (\beta_{i^*}, \beta_{j^*}))$ has ε-insecurity against physical bit leakages. Then, $\mathsf{ShamirSS}(n, n, (\alpha_1, \alpha_2, \dots, \alpha_n))$ has at most 2ε-insecurity against physical bit leakages.

The proof of this theorem is Fourier-analytic and uses properties of the Generalized Reed-Solomon (GRS) codes. Corollary 23 is a consequence of this theorem.

▶ **Corollary 23.** *Let F_p be the prime field of order $p = 2^\lambda \pm 1$ and $n \in \{2, 3, \dots\}$. Consider distinct evaluation places $\vec{\alpha} = (\alpha_1, \alpha_2, \dots, \alpha_n)$ and the corresponding $\mathsf{ShamirSS}(n, n, \vec{\alpha})$ secret-sharing scheme over the prime field F_p. Suppose the algorithm in Figure 3 determines $\vec{\alpha}$ to be secure. Then,*

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

Among all possible distinct evaluation places $\vec{\alpha} \in (F_p^*)^n$, the algorithm of Figure 3 determines at least

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

fraction of them to be secure.

We present the full proof of Theorem 22 and Corollary 23 in Appendix G.

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 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.

5 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.

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

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 Dan Boneh, Richard A. DeMillo, and Richard J. Lipton. On the importance of checking cryptographic protocols for faults (extended abstract). In Walter Fumy, editor, *EUROCRYPT'97*, volume 1233 of *LNCS*, pages 37–51. Springer, Heidelberg, May 1997. doi:10.1007/3-540-69053-0_4.

9 Viktor Bouniakowsky. *Sur les diviseurs numériques invariables des fonctions rationnelles entieres*. De l'Imprimerie de l'Académie impériale des sciences, 1854.

10 Luís T. A. N. Brandão and René Peralta. NIST first call for multi-party threshold schemes. https://csrc.nist.gov/publications/detail/nistir/8214c/draft, January 25, 2023.

11 Nishanth Chandran, Bhavana Kanukurthi, Sai Lakshmi Bhavana Obbattu, and Sruthi Sekar. Short leakage resilient and non-malleable secret sharing schemes. In Yevgeniy Dodis and Thomas Shrimpton, editors, *CRYPTO 2022, Part I*, volume 13507 of *LNCS*, pages 178–207. Springer, Heidelberg, August 2022. doi:10.1007/978-3-031-15802-5_7.

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

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

14 Roni Con, Noah Shutty, Itzhak Tamo, and Mary Wootters. Repairing reed-solomon codes over prime fields via exponential sums. In *2023 IEEE International Symposium on Information Theory (ISIT)*, pages 1330–1335. IEEE, 2023.

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

16 Nicolas Costes and Martijn Stam. Redundant code-based masking revisited. *IACR TCHES*, 2021(1):426–450, 2021. https://tches.iacr.org/index.php/TCHES/article/view/8740. doi:10.46586/tches.v2021.i1.426-450.

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

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

19 Sebastian Faust, Loïc Masure, Elena Micheli, Maximilian Orlt, and François-Xavier Standaert. Connecting leakage-resilient secret sharing to practice: Scaling trends and physical dependencies of prime field masking. In Marc Joye and Gregor Leander, editors, *Advances in Cryptology – EUROCRYPT 2024*, pages 316–344, Cham, 2024. Springer Nature Switzerland.

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

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

22 Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game or A completeness theorem for protocols with honest majority. In Alfred Aho, editor, *19th ACM STOC*, pages 218–229. ACM Press, May 1987. doi:10.1145/28395.28420.

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

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

25 Louis Goubin and Jacques Patarin. DES and differential power analysis (the "duplication" method). In Çetin Kaya Koç and Christof Paar, editors, *CHES'99*, volume 1717 of *LNCS*, pages 158–172. Springer, Heidelberg, August 1999. doi:10.1007/3-540-48059-5_15.

26 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.

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

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

29 Alfréd Haar. Aur theorie der orthogonalen funcktionensysteme. *Math. Annalen*, 69:331–371, 1910.

30 Jonathan I. Hall. Notes on coding theory. https://users.math.msu.edu/users/halljo/classes/codenotes/GRS.pdf, 2015.

31 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.

32 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.

33 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.

34 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.

35 Ohad Klein and Ilan Komargodski. New bounds on the local leakage resilience of Shamir's secret sharing scheme. In Helena Handschuh and Anna Lysyanskaya, editors, *CRYPTO 2023, Part I*, volume 14081 of *LNCS*, pages 139–170. Springer, Heidelberg, August 2023. doi:10.1007/978-3-031-38557-5_5.

36 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.

37 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.

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

39 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.

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

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

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

43 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.

44 Hemanta K. Maji, Hai H. Nguyen, Anat Paskin-Cherniavsky, Tom Suad, Mingyuan Wang, Xiuyu Ye, and Albert Yu. Leakage-resilient linear secret-sharing against arbitrary bounded-size leakage family. In Eike Kiltz and Vinod Vaikuntanathan, editors, *TCC 2022, Part I*, volume 13747 of *LNCS*, pages 355–383. Springer, Heidelberg, November 2022. doi:10.1007/978-3-031-22318-1_13.

45 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.

46 Hemanta K. Maji, Hai H. Nguyen, Anat Paskin-Cherniavsky, and Mingyuan Wang. Improved bound on the local leakage-resilience of shamir's secret sharing. In *2022 IEEE International Symposium on Information Theory (ISIT)*, pages 2678–2683, 2022. doi:10.1109/ISIT50566.2022.9834695.

47 Hemanta K. Maji, Hai H. Nguyen, Anat Paskin-Cherniavsky, and Xiuyu Ye. Constructing leakage-resilient shamir's secret sharing: Over composite order fields. In Marc Joye and Gregor Leander, editors, *Advances in Cryptology — EUROCRYPT 2024*, pages 286–315. Springer Nature Switzerland, 2024.

48 Hemanta K. Maji, Anat Paskin-Cherniavsky, Tom Suad, and Mingyuan Wang. Constructing locally leakage-resilient linear secret-sharing schemes. In Tal Malkin and Chris Peikert, editors,

CRYPTO 2021, Part III, volume 12827 of *LNCS*, pages 779–808, Virtual Event, August 2021. Springer, Heidelberg. doi:10.1007/978-3-030-84252-9_26.

49 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.

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

51 Moni Naor, Benny Pinkas, and Omer Reingold. Distributed pseudo-random functions and kdcs. In *International conference on the theory and applications of cryptographic techniques*, pages 327–346. Springer, 1999.

52 Hai Nguyen. Physical bit leakage resilience of linear code-based secret sharing. In *Eurocrypt 2025*. Springer, 2025.

53 Jesper Buus Nielsen and Mark Simkin. Lower bounds for leakage-resilient secret sharing. In Anne Canteaut and Yuval Ishai, editors, *EUROCRYPT 2020, Part I*, volume 12105 of *LNCS*, pages 556–577. Springer, Heidelberg, May 2020. doi:10.1007/978-3-030-45721-1_20.

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

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

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

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

58 Wolfgang M Schmidt. *Diophantine approximation*. Springer Science & Business Media, 1996.

59 Wolfgang M Schmidt. *Diophantine approximations and Diophantine equations*. Springer, 2006.

60 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.

61 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.

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

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

64 Anastassios Voudouris, Ilias Politis, and Christos Xenakis. Secret sharing a key in a distributed way, lagrange vs newton. In *Proceedings of the 17th International Conference on Availability, Reliability and Security*, ARES '22, New York, NY, USA, 2022. Association for Computing Machinery. doi:10.1145/3538969.3544424.

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

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

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

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

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

A Illustrating Technical Challenges: Resilience to LSB Leakage

This section illustrates the challenges of constructing such a classifier (Figure 1) against the LSB leakage. Appendix A.3 to Appendix A.5 present three natural approaches that are incorrect. *How do we identify the evaluation places yielding* LSB *resilient sharing?* Their pattern is complex; our algorithm is illustrated in Figure 1; Section 2.1 presents an overview. The exposition in Appendix A.5 introduces several technical components of our algorithm.

A.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:

$$(s_1, s_2) \in \Big\{ (P_1, 3 \cdot P_1) : P_1 \in F_p \Big\}. \tag{6}$$

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

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

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: <u>Share $s_1 = 2 \cdot x$, where $x \in \mathbb{Z} \cap [p/6, 2p/6]$</u>: 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: <u>Share $s_1 = 2 \cdot x$, where $x \in \mathbb{Z} \cap [4p/6, 5p/6]$</u>: 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:

$$(s_1, s_2) = (s + P_1, s + 3 \cdot P_1), \tag{7}$$

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 observations 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 [30]. Before our work, the only known vulnerable evaluation places satisfied $\alpha_1 \cdot \alpha_2^{-1} = -1$ [43, 1, 45, 19]. *Any* (α_1, α_2) *pair deemed insecure by our algorithm in Figure 1 will result in a new attack.*

A.2 An Example of Leakage-Resilience to LSB Leakage

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

$$(s_1, s_2) \in \Big\{ \ (P_1, 2 \cdot P_1) \ : \ P_1 \in F_p \Big\}. \tag{8}$$

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 24. Looking ahead, the evaluation places $(1, 2)$ is vulnerable to *physical bit leakage* over Mersenne/Fermat prime fields (see Remark 6).

A.3 Classifier Construction: First Attempt

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

$$(s_1, s_2) \in \Big\{ \ (\alpha_1 \cdot P_1, \alpha_2 \cdot P_1) \ : \ P_1 \in F_p \Big\}. \tag{9}$$

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 Shamir's scheme is $1/p$-dependent on the secret. Hence, Shamir's scheme is vulnerable to LSB leakage when the prime modulus is small. For large primes, as is standard in this line of research, 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 this brute-force algorithm takes exponential time.*

A.4 Classifier Construction: Second Attempt

Draw t elements $\left\{P_1^{(1)}, \dots, P_1^{(t)}\right\}$ from F_p uniformly and independently at random. Compute the corresponding leakage for each sample and estimate the leakage distribution from these samples. Using the tightness of the Chernoff bound, the accuracy of this estimation is only $\mathsf{poly}(1/t)$, which is *too coarse-grained for any tractable number of samples.* So, this strategy will have false positives.

A.5 Classifier Construction: Third Attempt

This section focuses on developing an efficient algorithm. Let $(\alpha_1 = 1, \alpha_2)$ be the evaluation places. Extrapolating from the examples in Appendix A.1 and Appendix A.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."

---

[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.

Fascinatingly, *this classifier also 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 [30], 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.

B Prior Related Works

The literature on leakage resilience and related areas is vast. It is challenging to cover all of them exhaustively; representative ones, most relevant to our work, are presented below.

B.1 Physical bit probing attacks

Probing wires and introducing random faults into them seem innocuous but lead to devastating attacks – the more straightforward the attack, the greater a security threat it poses. For example, Boneh et al. [8] showed the vulnerability of computing RSA signatures to random fault injection into memory. Ishai, Sahai, and Wagner [34] introduced the *bit probing model* to theoretically investigate real-world threats posed by an adversary that can probe a bounded number of memory locations. Bit probes on a share can also be used to estimate its Hamming weight, which leads to realistic threats like (1) algebraic side-channel attacks (beginning with the work of Renauld et al. [57]) and (2) recent attacks like Hertzbleed [66]. Recently, Faust et al. [19] provided a more comprehensive presentation. Maji et al. [43] introduced the "parity-of-parities" attack on the *additive secret-sharing* scheme. This attack leaks the LSB of each share, and the parity of the leaked bits is correlated with the secret's parity; this attack leads to $(2/\pi)^n \approx 0.63^n$ insecurity [1, 45, 19]. This simple attack matches the upper bound on the insecurity of the additive secret-sharing scheme against *arbitrary local leakage* proved in [4, 5]. Maji et al. [43] & Costes and Stam [16] independently observed that *Shamir's secret-sharing* scheme inherits this vulnerability if the modulus and the evaluation places are carelessly chosen. *Our work identifies more vulnerable evaluation places using the same* LSB *attack.*

B.2 Local leakage resilience

Benhamouda et al. [4] introduced leakage-resilient secret-sharing, which was implicit in the work of Goyal and Kumar [26]. Several works have *constructed new secret-sharing schemes* resilient to leakage attacks [6, 2, 61, 3, 39, 7, 20, 61, 21, 33, 13, 49, 11, 11]. There is a significant interest in characterizing the leakage-resilience of practical secret-sharing schemes, like the additive and Shamir's secret-sharing scheme. [43, 47] proved that, for reconstruction threshold $k = 2$ and an arbitrary number of parties n, choosing evaluation places at random yields a leakage-resilient Shamir secret-sharing scheme with a high probability against physical bit leakage. A sequence of works also determined the optimal leakage attack [43, 1, 45].

Other Monte Carlo constructions have also been proposed in [48, 44]. Faust et al. [19] present additional motivations for this research direction from practical motivations and a security analysis against the Hamming weight leakage (specialized to Mersenne primes).

Another flavor of results characterizes the leakage-resilience of Shamir's secret-sharing scheme for a large number of parties. For example, when $k \geqslant 0.69n$, Shamir's secret sharing (with any evaluation places) is leakage-resilient to (arbitrary) one-bit local leakage. Here, the insecurity is exponentially small in n [4, 5, 48, 46, 35]. Contrast this with our scenario, where the insecurity is exponentially small in the security parameter, independent of n. [53] proved that Shamir's secret-sharing scheme is insecure to local leakage when n/k is large.

B.3 Reed-Solomon Code Repair

Guruswami and Wooters [27, 28] considered the exact repair problem for Reed-Solomon codes – an antithetical objective to leakage resilience. They aim to repair the codeword by obtaining partial information from each block. Subsequently, a large body of work focused on repairing Reed-Solomon codes [17, 18, 23, 24, 54, 62, 67, 56, 68, 69, 15, 14]. Massey [50] connected linear secret-sharing schemes and linear codes. For example, Shamir's secret-sharing scheme is the Massey secret-sharing scheme corresponding to (punctured) Reed-Solomon codes. Repairing strategies for Reed-Solomon codes translate into techniques to reconstruct the secret in Shamir's secret-sharing scheme. However, there are crucial differences though. The literature on Reed-Solomon codes evaluates the secret polynomial on *all* finite field elements; they have $n = \mathsf{card}(F)$. For leakage resilience, typically, the secret polynomial is evaluated at $n \leqslant \mathsf{poly}(\log \mathsf{card}(F))$ evaluation places; [15, Section VI] highlights this distinction. Furthermore, they need to reconstruct the entire secret; however, the family of information that they obtain from each block is more general than simply bit probes. *Even in this literature, reconstruction using a small number of (arbitrary) bits per share and prime fields has been challenging due to non-linearity [15, 14].*

B.4 Square wave function families

Various families of square waves find wide applications in science and engineering. For example, consider the ones proposed by Haar [29], Walsh [65], and Rademacher [55]. In our work, we connect the leakage resilience of secret-sharing schemes with the properties of another family of square waves (see, for example, [63, 32, 31])

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

Previous works [63, 32] have studied the orthogonality of this family of waves. We investigate, more generally, the "similarity" among these waves and their offsets – functions of the form $\operatorname{sign}\sin(2\pi k \cdot (x - \delta))$, for $\delta \in \mathbb{R}$. In our context, zero similarity coincides with orthogonality; non-zero similarity represents correlation.

B.5 Simultaneous Diophantine Approximation

Solving simultaneous Diophantine approximation problems is a well-studied problem. This problem arises when choosing a "good basis" for a lattice. In our context, for an odd prime p, given distinct $\alpha_1, \alpha_2 \in \{1, 2, \ldots, p-1\}$, our objective is to find $q \in \{1, 2, \ldots, p-1\}$ such that $q\alpha_1 \mod p$ and $q\alpha_2 \mod p$ are either in the range $\{1, \ldots, \sqrt{p}\}$ or $\{p - \sqrt{p}, \ldots, p-1\}$. The integers $q\alpha_1 \mod p$ and $q\alpha_2 \mod p$, intuitively, have "small norm $\mod p$." We will use the classical LLL algorithm [41] to efficiently achieve this objective (see Appendix C).

The Dirichlet approximation theorem [58, 59] states that, for any $\alpha \in \mathbb{R}^d$ and any positive integer N, there is a denominator $1 \leqslant q \leqslant N^d$ such that

$$\max_{i \in \{1,2,\ldots,d\}} \{q\alpha_i\} \leqslant \frac{1}{N}. \tag{10}$$

Computing this solution is computationally challenging [40]. However, we can efficiently solve this problem by slightly weakening the upper bound on q. The seminal LLL algorithm [41], in particular, for $\alpha \in \mathbb{Q}^d$, finds $1 \leqslant q \leqslant 2^{d(d+1)/4} \cdot N^d$ satisfying Equation 10.

C Solving Simultaneous Diophantine Equations

Figure 4 presents our algorithm. In this section, the "LLL algorithm" refers to the algorithm with the following guarantees.

▶ **Theorem 25** (LLL [41, 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 4 Our Algorithm to obtain (u, v) from (α_1, α_2) using the LLL-algorithm.

Let us proceed to analyze our algorithm of Figure 4. 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."

D Proof of Technical Lemmas

D.1 Proof of Lemma 11

Proof of Lemma 11. 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 $(u, v) \in [\alpha_1 : \alpha_2]$.

$$
\begin{aligned}
&2\mathsf{SD}\Big(\vec{\mathrm{LSB}}(\mathsf{Share}(0))\ ,\ \vec{\mathrm{LSB}}(\mathsf{Share}(s))\Big) \\
&\quad= \sum_{\vec{\ell}\in\{0,1\}^2} \left|\Pr\Big[\vec{\mathrm{LSB}}(\mathsf{Share}(0)) = \vec{\ell}\Big] - \Pr\Big[\vec{\mathrm{LSB}}(\mathsf{Share}(s)) = \vec{\ell}\Big]\right| \\
&\quad= \sum_{\vec{\ell}\in\{0,1\}^2} \bigg|\mathop{\mathbb{E}}_{X}\big[\mathbb{1}_{\mathrm{LSB}^{-1}(\ell_1)}(uX)\cdot \mathbb{1}_{\mathrm{LSB}^{-1}(\ell_2)}(vX)\big] \\
&\qquad\qquad\qquad - \mathop{\mathbb{E}}_{X}\big[\mathbb{1}_{\mathrm{LSB}^{-1}(\ell_1)}(uX+s)\cdot \mathbb{1}_{\mathrm{LSB}^{-1}(\ell_2)}(vX+s)\big]\bigg|
\end{aligned} \tag{11}
$$

▷ Claim 26. For $\ell \in \{0, 1\}$ and $X \in F_p$, we have

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

Applying Claim 26 to Equation 11, we get

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

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,

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

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

◀

D.2 Proof of Lemma 12

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

$$\widetilde{\text{sign}}_p(X) := \begin{cases} +1, & \text{if } X \in \{1, \ldots, (p-1)/2\} \mod p \\ 0, & \text{if } X = 0 \mod p \\ -1, & \text{if } X \in \{-(p-1)/2, \ldots, -1\} \mod p. \end{cases} \tag{12}$$

Analogously, we define

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

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

▷ Claim 27. For any $k, \ell, \Delta \in F_p$,

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

Proof of Claim 27. This claim follows directly from the definition of $\Sigma_{k,\ell}^{(\Delta)}$, $\text{sign}_p(X)$, $\widetilde{\Sigma}_{k,\ell}^{(\Delta)}$, and $\widetilde{\text{sign}}_p(X)$, for $k, \ell, \Delta \in F_p$. The primary observation is that $\text{sign}_p(X) = \widetilde{\text{sign}}_p(X)$, for all $X \in F_p^*$, and $\widetilde{\text{sign}}_p(X = 0) = 0$.

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

◀

▷ Claim 28 (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 29. 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 $\delta' := \frac{\mathrm{sign}_p(\Delta) \cdot |\Delta|_p}{p} \in \frac{1}{p} \cdot \mathbb{Z}$. Then,

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

Proof of Claim 29. Consider the following exhaustive case analysis.

- **Case 1:** $\Delta \in \{0, 1, \ldots, (p-1)/2\}$.
  In this scenario, $\mathrm{sign}_p(\Delta) = 1, |\Delta|_p = \Delta$ 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,

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

whence the claim. ◀

▷ Claim 30. 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 of Claim 30. Similar to the previous claim, we prove this via exhaustive case analysis.

- **Case 1:** $k \in \{0, 1, \ldots, (p-1)/2\}$.
  We can see $|k|_p = k$, $\mathrm{sign}_p(k) = 1$, 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:** $k \in \{(p+1)/2, (p+3)/2, \ldots, p-1\}$.
  Substituting $|k|_p = p - k$ and $\mathrm{sign}_p(k) = -1$ into $\mathrm{sign}_p(k) \cdot \varphi(|k|_p \cdot (x - \delta))$ gives us

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

This proves the claim. ◀

Given the Transference Property (Claim 28), Claim 29 and Claim 30, we observe that for $k, \ell, \Delta \in F_p, T \in F, t = T/p \in \mathbb{Q}$ and $\delta = \frac{\mathrm{sign}_p(\Delta) \cdot |\Delta|_p}{p} \in \mathbb{Q}$,

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

▶ **Definition 31** (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 32 (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 the following general result that connects the sum of a Boolean function to its integral.

▷ Claim 33 (Sum and Integral Connection). Fix an integer $n \in \{1,2,\dots\}$. Let $f\colon [0,1] \to \{\pm 1\}$ be a Boolean function that oscillates 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 of Claim 33. 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 this over all $r \in \{0/n, 1/n, \dots, (n-1)/n\}$ proves the claim. ◀

Claim 27 is essentially a consequence of Claim 32 and Claim 33 when

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

We are now ready to prove Lemma 12.

Proof of Lemma 12. For any $k,\ell,\Delta \in F_p$ and $\delta = \frac{\mathrm{sign}_p(\Delta)\cdot|\Delta|_p}{p} \in \mathbb{Q}$.

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

Combining the two cases, we get

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

Applying Claim 27, we conclude the following

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

which completes the proof of Lemma 12. ◀

D.3 Proof of Lemma 13

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

▶ **Proposition 34** (Orthogonality of Sine/Cosine Waves [38, Page 38]). *For* $k, \ell \in \{1, 2, \dots\}$

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

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

For the periodic *square wave* [63, 32, 31] $\varphi \colon \mathbb{R} \to \{-1, 0, +1\}$.

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

[32] uses (basic) Fourier analysis and Proposition 34 to determine the Fourier expansion of $\varphi(x)$.

$$\varphi(x) = \sum_{\text{odd } n>0} \frac{4}{\pi n} \cdot \sin(2n\pi x). \tag{13}$$

We prove the following claim for standardization.

▷ Claim 35. For $k, \ell \in F_p$ and $\delta \in \mathbb{R}$, the following identity holds

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

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

Proof of Claim 35. Define $\psi_{k,\ell}^{(\delta)}(x) := \varphi(kx) \cdot \varphi(\ell \cdot (x - \delta))$.

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

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

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

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

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

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

◀

Previously only $I^{(0)}_{k,\ell}$ was studied [63, 32]. 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 36. 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 of Claim 36. Suppose k is even and ℓ is odd. In this case, for any odd $m, n > 0$,

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

Hence,

$$\begin{aligned}
&\int_0^1 \sin(2n\pi \cdot kt) \cdot \sin(2m\pi \cdot \ell(t-\delta))\,\mathrm{d}t \\
&= \int_0^{1/2} \sin(2n\pi \cdot kt) \cdot \sin(2m\pi \cdot \ell(t-\delta))\,\mathrm{d}t + \int_{1/2}^1 \sin(2n\pi \cdot kt) \cdot \sin(2m\pi \cdot \ell(t-\delta))\,\mathrm{d}t \\
&= \int_0^{1/2} \sin(2n\pi \cdot kt) \cdot \sin(2m\pi \cdot \ell(t-\delta))\,\mathrm{d}t - \int_0^{1/2} \sin(2n\pi \cdot kt) \cdot \sin(2m\pi \cdot \ell(t-\delta))\,\mathrm{d}t \\
&= 0. \qquad (14)
\end{aligned}$$

Therefore,

$$\begin{aligned}
I^{(\delta)}_{k,\ell} &= \int_0^1 \varphi(kt) \cdot \varphi(\ell(t-\delta))\,\mathrm{d}t \\
&= \frac{16}{\pi^2} \sum_{\text{odd } n>0} \sum_{\text{odd } m>0} \frac{1}{mn} \int_0^1 \sin(2n\pi \cdot kt) \cdot \sin(2m\pi \cdot \ell(t-\delta))\,\mathrm{d}t \quad \text{(By Equation 13)} \\
&= 0 \quad \text{(By Equation 14)}
\end{aligned}$$

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

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

which is the same as the previous case. Therefore, Equation 14 again holds and the proof of this case still goes through; the final result remains the same. ◀

▷ Claim 37. Let $\triangle\colon \mathbb{R} \to [-1, +1]$ be the triangle wave function defined as

$$\triangle(t) := 4 \cdot \left| t + \frac{1}{2} - \lceil t \rceil \right| - 1.$$

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

$$I_{k,\ell}^{(\delta)} = \frac{\triangle(k\ell \cdot \delta)}{k\ell},$$

for all $\delta \in \mathbb{R}$. This also shows that $I_{k,\ell}^{(\delta)}$ achieves its maximum at $\delta \in \frac{1}{k\ell} \cdot \mathbb{Z}$, and the minimum at $\delta \in \frac{1}{2k\ell} + \frac{1}{k\ell} \cdot \mathbb{Z}$.

To prove this claim, we first need to generalize Proposition 34 a bit.

▷ Claim 38.

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

Proof of Claim 38.

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

because, for all $k, \ell \in \{1, 2, \dots\}$, Proposition 34 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 34 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. ◀

Now we can prove Claim 37.

Proof of Claim 37. We simplify the expression for $I_{k,\ell}^{(\delta)}$.

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

In light of Claim 38 above, the integral in the RHS survives if and only if $nk = m\ell$. Since $\gcd(k, \ell) = 1$, note that $nk = m\ell$ if and only if

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

With this observation and Proposition 34, we get

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

$$= \frac{16}{\pi^2} \cdot \frac{1}{k\ell} \sum_{\text{odd } a>0} \frac{1}{a^2} \cdot \frac{\cos(2a\pi \cdot k\ell\delta)}{2} \qquad \text{(By Proposition 34 and Claim 38)}$$

$$= \frac{1}{k\ell} \cdot \left(\frac{8}{\pi^2} \cdot \sum_{\text{odd } a>0} \frac{1}{a^2} \cdot \cos(2a\pi \cdot k\ell\delta) \right)$$

$$= \frac{1}{k\ell} \cdot \triangle(k\ell \cdot \delta) \qquad (\triangle(t) := 4 \cdot \left| t + \tfrac{1}{2} - \lceil t \rceil \right| - 1)$$

The last equality follows from Fourier expansion of triangle wave function

$$\triangle(t) = \frac{8}{\pi^2} \cdot \sum_{\text{odd } a>0} \frac{\cos(2a\pi \cdot t)}{a^2}.$$

◀

We are finally ready to prove Lemma 13.

Proof of Lemma 13. Combining Claim 36 and Claim 37, we showed that for relatively prime $k, \ell \in F_p$,

$$I_{k,\ell}^{(\delta)} = \begin{cases} 0 & \text{if } k \cdot \ell \text{ is even} \\ \dfrac{\triangle(k\ell \cdot \delta)}{k\ell} & \text{if } k \cdot \ell \text{ is odd} \end{cases}$$

Claim 35 generalizes the result to all $k, \ell \in F_p$ by considering $g = \gcd(k, \ell)$. This proves our lemma that

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

◀

D.4 Proof of Corollary 15

Proof of the first part of Corollary 15. 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 14, 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 14, we get that our estimation $\varepsilon_{\text{LSB}}^{(\text{est})} \leqslant 1/\sqrt{p}$. The relation between our estimate and insecurity yields

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

◀

Proof of the second part of Corollary 15. We prove that our algorithm outputs "may be insecure" only for an exponentially small fraction of the equivalence classes $[\alpha_1 \colon \alpha_2]$, for distinct evaluation places $\alpha_1, \alpha_2 \in F_p^*$.

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

Next, let us account for the instances when Figure 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

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

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

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

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 D.4.1 proves the upper bound

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

for all $p \geqslant 11$. ◀

D.4.1 Proof of inequality used in the proof of Corollary 15

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

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

We simplify this inequality into a simpler equivalent inequality.

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

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

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 $p \geqslant 11$.

D.5 Proof of Corollary 16

Proof of Corollary 16. Our efficient adversary outputs the s indicated in Theorem 10. 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 [41] to obtain $(u, v) \in [\alpha_1 \colon \alpha_2]$ 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 14; 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 14; 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 39). Using this property, Appendix D.6 proves that the advantage of the maximum likelihood decoder is

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

◀

D.6 Alternative Proof for Corollary 16

▷ Claim 39. 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 of Claim 39. By Lemma 12 and $\delta = \frac{\mathrm{sign}_p(\Delta)|\Delta|_p}{p}$,

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

which we can rewrite equivalently as

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

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 $\frac{\Sigma^{(0)}_{\alpha_1,\alpha_2} - \Sigma^{(\Delta)}_{\alpha_1,\alpha_2}}{p}$. Hence,

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

and therefore,

$$\begin{aligned}&\mathrm{sign}\left(\frac{\Sigma^{(0)}_{\alpha_1,\alpha_2} - \Sigma^{(\Delta)}_{\alpha_1,\alpha_2}}{p}\right)\\ &\quad = \mathrm{sign}\Big(\mathrm{sign}_p(\alpha_1)\cdot\mathrm{sign}_p(\alpha_2)\cdot\left(I^{(0)}_{|\alpha_1|_p,|\alpha_2|_p} - I^{(\delta)}_{|\alpha_1|_p,|\alpha_2|_p}\right)\Big)\\ &\quad = \mathrm{sign}\left(\mathrm{sign}_p(\alpha_1)\cdot\mathrm{sign}_p(\alpha_2)\cdot\left(\sin^2(|v|_p\pi\cdot\delta)\cdot\frac{g^2}{|u|_p\cdot|v|_p}\right)\right) && \text{(By Lemma 13)}\\ &\quad = \mathrm{sign}\big(\mathrm{sign}_p(\alpha_1)\cdot\mathrm{sign}_p(\alpha_2)\big) && \left(\text{Since } \sin^2(|v|_p\pi\cdot\delta)\cdot\frac{g^2}{|u|_p\cdot|v|_p} > 0\right)\\ &\quad = \mathrm{sign}\left(\varepsilon^{(\mathrm{est})}_{\mathrm{LSB}}(\vec{\alpha})\right)\end{aligned}$$

◀

Alternative Proof for Corollary 16. 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 39, we know that for any secret $s \in F$,

$$\varepsilon_{\mathrm{LSB}}(\vec{\alpha}; s) \geqslant \varepsilon^{(\mathrm{est})}_{\mathrm{LSB}}(\vec{\alpha}; s) - \mathrm{err}. \tag{15}$$

and

$$\varepsilon^{(\mathrm{est})}_{\mathrm{LSB}}(\vec{\alpha}; s) \geqslant \varepsilon_{\mathrm{LSB}}(\vec{\alpha}; s) - \mathrm{err}. \tag{16}$$

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

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

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

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

Then,

$$\begin{aligned}
\varepsilon_{\mathrm{LSB}}(\vec{\alpha}; s^*) &\geqslant \varepsilon^{(\mathrm{est})}_{\mathrm{LSB}}(\vec{\alpha}; s^*) - \mathrm{err} = \varepsilon^{(\mathrm{est})}_{\mathrm{LSB}}(\vec{\alpha}) - \mathrm{err} && \text{(By Equation 15)} \\
&\geqslant \varepsilon^{(\mathrm{est})}_{\mathrm{LSB}}(\vec{\alpha}; \tilde{s}^*) - \mathrm{err} && \left(\text{Because } \varepsilon^{(\mathrm{est})}_{\mathrm{LSB}}(\vec{\alpha}; s^*) = \max_{s \in F} \varepsilon^{(\mathrm{est})}_{\mathrm{LSB}}(\vec{\alpha}; s)\right) \\
&\geqslant \varepsilon_{\mathrm{LSB}}(\vec{\alpha}; \tilde{s}^*) - 2 \cdot \mathrm{err} && \text{(By Equation 16)} \\
&= \varepsilon_{\mathrm{LSB}}(\vec{\alpha}) - 2 \cdot \mathrm{err} > 0
\end{aligned}$$

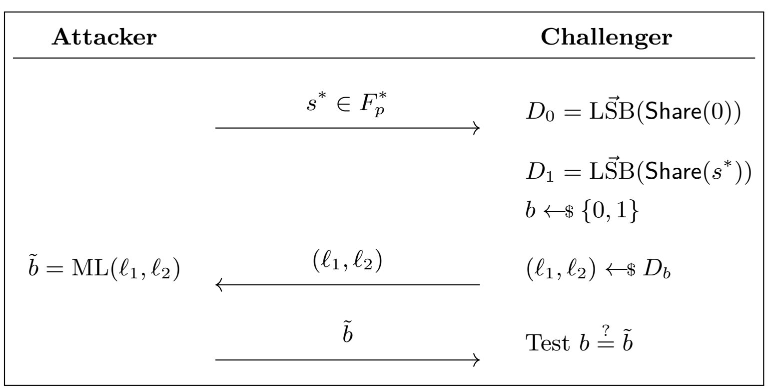
and therefore, the distinguishing advantage of the maximum likelihood decoder is

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

◀

D.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

$$\tilde{b} = \begin{cases} 0 & \text{if } \Pr[(\ell_1, \ell_2) | s = 0] \geqslant \Pr[(\ell_1, \ell_2) | s = s^*] \\ 1 & \text{if } \Pr[(\ell_1, \ell_2) | s = 0] < \Pr[(\ell_1, \ell_2) | s = s^*] \end{cases}$$

In other words, the output depends on $\mathrm{sign}(\Pr[(\ell_1,\ell_2)|s=0]-\Pr[(\ell_1,\ell_2)|s=s^*])$.

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

$$\begin{aligned}
&\Pr[(\ell_1,\ell_2)|s=0]-\Pr[(\ell_1,\ell_2)|s=s^*]\\
&=(-1)^{\ell_1+\ell_2}\cdot\frac{\Sigma^{(0)}_{u,v}-\Sigma^{(\Delta)}_{u,v}}{4p} && \text{(Appendix D.1)}\\
&=\frac{(-1)^{\ell_1+\ell_2}\cdot\mathrm{sign}_p(u)\cdot\mathrm{sign}_p(v)}{4}\cdot\left(I^{(0)}_{|u|,|v|}-I^{(\delta)}_{|u|,|v|}\pm 2\cdot\frac{4(|u|+|v|)-(3/2)}{p}\right)\\
&&& \left(\text{Lemma 12 and } \delta=\frac{\mathrm{sign}_p(\Delta)|\Delta|_p}{p}\right)\\
&=\frac{(-1)^{\ell_1+\ell_2}\cdot\mathrm{sign}_p(u)\cdot\mathrm{sign}_p(v)}{4}\cdot\left((1-\triangle(|u||v|\cdot\delta))\cdot\frac{g^2}{|u|\cdot|v|}\pm 2\cdot\frac{4(|u|+|v|)-(3/2)}{p}\right)\\
&&& \text{(Lemma 13)}
\end{aligned}$$

To maximize the likelihood of distinguishing between two secrets, attacker picks secret $s^*\in F_p$ with the corresponding $\Delta^*:=\left(s^*\cdot 2^{-1}\right)\cdot\left(u^{-1}-v^{-1}\right)\in F_p$ and $\delta^*:=\frac{\Delta^*}{p}\in\frac{1}{p}\mathbb{Z}$ satisfying $\delta^*\in\left(\frac{1}{2}\pm\frac{1}{2p}+\mathbb{Z}\right)\cdot\frac{1}{|u|\cdot|v|}$.

▷ Claim 40. Consider $\Delta\in F_p$, define $\delta:=\frac{\Delta}{p}\in\frac{1}{p}\cdot\mathbb{Z}$. For $k,\ell\in F_p$, the triangle wave function $\triangle(k\ell\cdot\delta)$ achieves minimum when $\delta^*\in\left(\frac{1}{2}\pm\frac{1}{2p}+\mathbb{Z}\right)\cdot\frac{1}{k\ell}$, equivalently, $\Delta^*\in\frac{(2\mathbb{Z}+1)\cdot p\pm 1}{2k\ell}$ and the minimum achieved is $\triangle(k\ell\cdot\delta^*)=-1+\frac{2}{p}$.

▷ Claim 41. For prime $p>2$, consider $k,\ell\in F_p$. Then,

$$\min\left|\frac{1}{p}\cdot\mathbb{Z}-\left(\frac{1}{2}+\mathbb{Z}\right)\cdot\frac{1}{k\ell}\right|=\frac{1}{2pk\ell}.$$

Proof. For $k,\ell\in F_p$, $\gcd(p,2k\ell)=1$. Then, there exists $a,b\in\mathbb{Z}$ such that $a\cdot p+b\cdot 2k\ell=1$. $b\cdot 2k\ell\in 2\mathbb{Z}$ implies that $a\in 2\mathbb{Z}+1$. Since p is odd and $2k\ell$ is even, then

$$\min|2k\ell\cdot\mathbb{Z}-p\cdot(2\mathbb{Z}+1)|\geqslant 1.$$

There exists $-a\in 2\mathbb{Z}+1, b\in\mathbb{Z}$ that $|b\cdot 2k\ell-a\cdot p|=1$. Therefore,

$$\min|2k\ell\cdot\mathbb{Z}-(2\mathbb{Z}+1)\cdot p|=1.$$

$$\min\left|\frac{1}{p}\cdot\mathbb{Z}-\left(\frac{1}{2}+\mathbb{Z}\right)\cdot\frac{1}{k\ell}\right|=\frac{1}{2pk\ell}\cdot\min|2k\ell\cdot\mathbb{Z}-(2\mathbb{Z}+1)\cdot p|=\frac{1}{2pk\ell}$$

◀

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

$$\left(2-\frac{1}{2p}\right)\cdot\frac{g^2}{|u|\cdot|v|}-2\cdot\frac{4(|u|+|v|)-(3/2)}{p}>0.$$

Hence,

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

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 $\tilde{b}=1$.

E Equivalence classes for Evaluation Places

Consider Shamir's secret-sharing scheme among n parties with reconstruction threshold k over the prime field F_p of order $p \geqslant 3$. The secret-sharing scheme is the Massey secret-sharing scheme [50] corresponding to the (punctured) Reed-Solomon code with evaluation places $(0, \alpha_1, \alpha_2, \dots, \alpha_n)$. That is, the dealer chooses a random F_p-polynomial $P(Z)$ of degree $< k$ conditioned on $P(Z = 0)$ being the secret s. Evaluating this polynomial at evaluation places $Z = \alpha_1, \alpha_2, \dots, \alpha_n$ generates the secret shares $s_1, s_2, \dots, s_n$, respectively.

▶ **Lemma 42** (Equivalence Classes of Evaluation Places)**.** *The (punctured) Reed-Solomon code corresponding to evaluation places* $(0, \alpha_1, \alpha_2, \dots, \alpha_n)$ *is identical to the (punctured) Reed-Solomon code corresponding to evaluation places* $(0, \Lambda \cdot \alpha_1, \Lambda \cdot \alpha_2, \dots, \Lambda \cdot \alpha_n)$*, for any* $\Lambda \in F_p^*$*.*

This proposition is a consequence of the properties of Generalized Reed-Solomon codes [30, 42] (see Appendix G.2.1 for definition and one of its primitive properties). In particular, since the linear codes are identical, the corresponding Massey secret-sharing schemes have identical resilience/vulnerability to attacks. That is, two secret-sharing schemes

$$\mathsf{ShamirSS}(n, k, (\alpha_1, \alpha_2, \dots, \alpha_n)) \quad \text{and} \quad \mathsf{ShamirSS}(n, k, (\Lambda \cdot \alpha_1, \Lambda \cdot \alpha_2, \dots, \Lambda \cdot \alpha_n))$$

have identical resilience/vulnerability to attacks, for any $\Lambda \in F_p^*$. Therefore, for given distinct evaluation places $\alpha_1, \alpha_2, \dots, \alpha_n \in F_p^*$, we define the equivalence class

$$[\alpha_1 \colon \alpha_2 \colon \cdots \colon \alpha_n] := \left\{ (\Lambda \cdot \alpha_1, \Lambda \cdot \alpha_2, \dots, \Lambda \cdot \alpha_n) \colon \Lambda \in F_p^* \right\}.$$

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

F Security against Physical Bit Leakage: Corollaries and Proofs

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 or Fermat prime, i.e., $p = 2^\lambda \pm 1$, where λ is the security parameter.

F.1 Proof of Proposition 17

The following proposition will be used without proof.

▶ **Proposition 43.** *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 $2^\lambda = 1 \mod p$.

Proof of Proposition 17. Let λ be the security parameter.

- **Case 1:** $p = 2^\lambda - 1$ is a Mersenne prime.
  Then for all $i \in \{0, 1, 2, \ldots, \lambda - 1\}$, we have $p = -1 \mod 2^{i+1}$.
  Note that, by Proposition 43, if $\mathrm{PHYS}_i(x) = 0$, then $\mathrm{PHYS}_0(x \cdot 2^{-i}) = 0$; similarly, if $\mathrm{PHYS}_i(x) = 1$, then $\mathrm{PHYS}_0(x \cdot 2^{-i}) = 1$. Therefore, $\mathrm{PHYS}_i(x) = \mathrm{PHYS}_0(x \cdot 2^{-i})$.
- **Case 2:** $p = 2^\lambda + 1$ is a Fermat prime.
  Then for all $i \in \{0, 1, 2, \ldots, \lambda - 1\}$, $p = 1 \mod 2^{i+1}$. Let F be a prime field of order $p = 2^\lambda + 1$. Then, for $x \in F$, $\mathrm{PHYS}_i(2x + 1) = \mathrm{PHYS}_{i-1}(x)$. Therefore,

$$\mathrm{PHYS}_i(x) = \mathrm{PHYS}_{i-1}\left(\frac{x-1}{2}\right) = \mathrm{PHYS}_{i-2}\left(\frac{x-3}{4}\right) = \cdots = \mathrm{PHYS}_0\left(\frac{x - 2^i + 1}{2^i}\right).$$

  Upon Simplification, we can conclude $\mathrm{PHYS}_i(x) = \mathrm{PHYS}_0\big(2^{-i}x + 2^{-i} - 1\big)$.

◀

F.2 Reduction: Leakage attack when $2^k\alpha_1 = \alpha_2$

This section provides the detailed calculations behind the reduction from joint distribution of physical-bit leakages to of LSBs, illustrated in Section 5.1, which leads to Lemma 18.

▶ **Proposition 44.** *Let F be the prime field of order $p = 2^\lambda \pm 1$. Let $\alpha_1, \alpha_2 \in F$ such that $\alpha_1 \neq \alpha_2$ yet $2^k\alpha_1 = \alpha_2$ for some $k \in \{0, 1, \ldots, \lambda - 1\}$. Given $s \in F$, for uniformly random $u \in F$, there exists $t^* \in F$ that makes the two following joint distributions equivalent.*

$$(\mathrm{PHYS}_i(s + u\alpha_1), \mathrm{PHYS}_j(s + u\alpha_2)) \equiv (\mathrm{PHYS}_0(1 + t^* + v\alpha_1), \mathrm{PHYS}_0(t^* + v\alpha_2))$$

where $v := v(u)$ is a uniform distribution i.i.d. to the distribution of u.

Proof of Proposition 44. We divide it into two cases.

- **Case 1:** $p = 2^\lambda - 1$.
  Applying Proposition 17 and substituting $t := s2^{-j}$, $v := u2^{-j}$, and $k := i - j$ gives us

$$\begin{aligned}&(\mathrm{PHYS}_i(s + u\alpha_1), \mathrm{PHYS}_j(s + u\alpha_2))\\ &\equiv \big(\mathrm{PHYS}_0((s + u\alpha_1) \cdot 2^{-i}), \mathrm{PHYS}_0((s + u\alpha_2) \cdot 2^{-j})\big) && \text{(By Proposition 17)}\end{aligned}$$

$$\equiv \big(\mathrm{PHYS}_0(s\cdot 2^{-i}+u\alpha_1\cdot 2^{-i}), \mathrm{PHYS}_0(s\cdot 2^{-j}+u\alpha_2\cdot 2^{-j})\big)$$
$$\equiv \big(\mathrm{PHYS}_0(t\cdot 2^{k}+\alpha_1\cdot v2^{k}), \mathrm{PHYS}_0(t+\alpha_2\cdot v)\big) \qquad \text{(By aforesaid substitutions)}$$

Let $t^* := (2^k-1)^{-1}$. Then $t^*(2^k-1)=1$ which simplifies to $t^*2^k = t^*+1$. Hence, by substituting t^* for t in above equation, we conclude

$$(\mathrm{PHYS}_i(s+u\alpha_1), \mathrm{PHYS}_j(s+u\alpha_2)) \equiv (\mathrm{PHYS}_0(1+t^*+v\alpha_1), \mathrm{PHYS}_0(t^*+v\alpha_2))$$

- **Case 2:** $p = 2^\lambda + 1$.
  We again apply Proposition 17, but for this case we substitute $t := (s+1)2^{-j}$, $v := u2^{-j}$ and $k := i-j$, and choose $t^* := (2^k-1)^{-1}-1$.

$$(\mathrm{PHYS}_i(s+u\alpha_1), \mathrm{PHYS}_j(s+u\alpha_2))$$
$$\equiv \big(\mathrm{PHYS}_0(s2^{-i}+u\alpha_1 2^{-i}+(2^{-i}-1)), \mathrm{PHYS}_0(s2^{-j}+u\alpha_2 2^{-j}+(2^{-j}-1))\big)$$
$$\equiv \big(\mathrm{PHYS}_0(2^{-i}(s+1)+u\alpha_1 2^{-i}-1), \mathrm{PHYS}_0(2^{-j}(s+1)+u\alpha_2 2^{-j}-1)\big)$$
$$\equiv \big(\mathrm{PHYS}_0(2^{k}t+\alpha_1\cdot v2^{k}-1), \mathrm{PHYS}_0(t+\alpha_2 v-1)\big) \qquad \text{(By aforesaid substitutions)}$$
$$\equiv (\mathrm{PHYS}_0(1+t^*+v\alpha_1), \mathrm{PHYS}_0(t^*+v\alpha_2)) \qquad \text{(Substitute } t^* \text{ for } t)$$

As F is a prime field, the mapping $u \mapsto v := u2^{-j}$ an automorphism over F, making the distribution of v also uniform. ◀

Lemma 18 is then a direct consequence of Proposition 44, so Lemma 18 is also proved.

F.3 Proof of Corollary 19

We prove Corollary 19 separately for p is a Mersenne or Fermat prime.

F.3.1 Case A: p is a Mersenne Prime

Due to the properties of the F, when $p = 2^\lambda - 1$ 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 45.** *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 $k \in \{0,1,\dots,\lambda-1\}$. Consider the leakage attack $\vec{\mathrm{PHYS}}_{i,j}$ for any $i,j \in \{0,1,\dots,\lambda-1\}$. Define $\alpha_1' = 2^{-i}\cdot\alpha_1$ and $\alpha_2' = 2^{-j}\cdot\alpha_2$. For any $s \in F_p$, let D denote the joint leakage distribution generated by the leakage function $\vec{\mathrm{PHYS}}_{i,j}$ when the secret shares are generated using the $\mathsf{ShamirSS}(2,2,\vec{\alpha})$ secret-sharing scheme. Likewise, D' denotes the joint leakage distribution generated by the leakage function $\vec{\mathrm{LSB}}$ when the secret shares are generated using the $\mathsf{ShamirSS}(2,2,\vec{\alpha}')$ secret-sharing scheme instead. Then, the distributions D and D' are identical.*

Since $2^k\cdot\alpha_1 \neq \alpha_2$, for all $k \in \{0,1,\dots,\lambda-1\}$, we conclude that $\alpha_1' \neq \alpha_2'$, for all $i,j \in \{0,1,\dots,\lambda-1\}$. Therefore, the secret-sharing scheme $\mathsf{ShamirSS}(2,2,\vec{\alpha}')$ is valid. We prove that the distributions D and D' are identical, for all $s \in F_p$, using Proposition 17.

Proof of Lemma 45. Given $s \in F_p$,

$$2\mathsf{SD}\Big(\vec{\mathrm{PHYS}}_{i,j}(\mathsf{Share}(0))\ ,\ \vec{\mathrm{PHYS}}_{i,j}(\mathsf{Share}(s))\Big)$$
$$= \sum_{\vec{\ell}\in\{0,1\}^2} \Big|\Pr\Big[\vec{\mathrm{PHYS}}_{i,j}(\mathsf{Share}(0)) = \vec{\ell}\Big] - \Pr\Big[\vec{\mathrm{PHYS}}_{i,j}(\mathsf{Share}(s)) = \vec{\ell}\Big]\Big|$$

$$= \sum_{\vec{\ell}\in\{0,1\}^2} \Big| \mathop{\mathbb{E}}_{x}\Big[\mathbb{1}_{\mathrm{PHYS}_i^{-1}(\ell_1)}(\alpha_1 x)\cdot \mathbb{1}_{\mathrm{PHYS}_j^{-1}(\ell_2)}(\alpha_2 x)\Big] - \mathop{\mathbb{E}}_{x}\Big[\mathbb{1}_{\mathrm{PHYS}_i^{-1}(\ell_1)}(\alpha_1 x + s)\cdot \mathbb{1}_{\mathrm{PHYS}_j^{-1}(\ell_2)}(\alpha_2 x + s)\Big]\Big|$$

$$= \sum_{\vec{\ell}\in\{0,1\}^2} \Big| \mathop{\mathbb{E}}_{x}\Big[\mathbb{1}_{\mathrm{PHYS}_i^{-1}(0)}(\alpha_1 x)\cdot \mathbb{1}_{\mathrm{PHYS}_j^{-1}(0)}(\alpha_2 x)\Big] - \mathop{\mathbb{E}}_{x}\Big[\mathbb{1}_{\mathrm{PHYS}_i^{-1}(0)}(\alpha_1 x + s)\cdot \mathbb{1}_{\mathrm{PHYS}_j^{-1}(0)}(\alpha_2 x + s)\Big]\Big|$$

$$\text{(Because } \mathbb{1}_{\mathrm{PHYS}_k^{-1}(1)} = 1 - \mathbb{1}_{\mathrm{PHYS}_k^{-1}(0)}\text{)}$$

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

$$\text{(By Proposition 17, } E := \mathrm{PHYS}_0^{-1}(0)\text{)}$$

$$= 4\cdot\Big| \mathop{\mathbb{E}}_{x}\big[\mathbb{1}_E(2^{-i}\alpha_1 x)\cdot \mathbb{1}_E(2^{-j}\alpha_2 x)\big] - \mathop{\mathbb{E}}_{y}\big[\mathbb{1}_E(2^{-i}\alpha_1 \cdot y)\cdot \mathbb{1}_E(2^{-j}\alpha_2 \cdot y + s')\big]\Big| \qquad (17)$$

where $y := \left(x + \alpha_1^{-1}\cdot s\right)$ and $s' := \left((1-\alpha_1^{-1}\alpha_2)\cdot 2^{-j}s\right)$. These substitutions are automorphisms over F^*.

Observe that Equation 17 equals $\varepsilon_{\mathrm{LSB}}(2^{-i}\alpha_1, 2^{-j}\alpha_2)$. Therefore, we conclude that the insecurity of ShamirSS$(2,2,(\alpha_1,\alpha_2))$ secret-sharing scheme against the $\vec{\mathrm{PHYS}}_{i,j}$ is identical to the insecurity of the ShamirSS$(2,2,(2^{-i}\alpha_1, 2^{-j}\alpha_2))$ secret-sharing scheme against the LSB attack. ◀

Before we start proving Corollary 19 for Mersenne primes, we first prove the following two corollaries on the estimated insecurity of ShamirSS$(2,2,\vec{\alpha})$.

▶ **Corollary 46.** *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* ShamirSS$(2,2,\vec{\alpha})$. *Define*

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

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 of Corollary 46. If $2^t\cdot\alpha_1 = \alpha_2$, for some $t\in\{0,1,\dots,\lambda-1\}$, we have $\varepsilon^{(\mathrm{est})}_{\mathrm{PHYS}}(\vec{\alpha}) = 1$. Lemma 18 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

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

We are left with the case where $2^t\alpha_1 \neq \alpha_2$ for all $t \in \{0, 1, \ldots, \lambda - 1\}$. Lemma 45 shows that the leakage distribution of $\text{PHYS}_{i,j}$ on $\mathsf{ShamirSS}(2, 2, \vec{\alpha})$ is identical to the leakage distribution $\vec{\text{LSB}}$ 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 42 in Appendix E. Hence,

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

We know that our estimation $\varepsilon^{(\text{est})}_{\text{LSB}}(\cdot)$ is a tight estimation of $\varepsilon_{\text{LSB}}(\cdot)$ due to Corollary 14. Therefore, we conclude that

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

◀

▶ **Corollary 47.** *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 $\varepsilon_{\text{PHYS}}(\vec{\alpha}) > \frac{2\cdot 8^{5/4}}{\sqrt{p}} + \frac{13}{p}$, then there is an efficient algorithm that generates $(s, f) \in F_p^* \times \text{PHYS}$ and can distinguish the secret 0 from the secret s with an advantage*

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

by leaking f from the secret shares.

Proof of Corollary 47. If there is $t \in \{0, 1, \ldots, \lambda - 1\}$ such that $2^t\alpha_1 = \alpha_2$, then Lemma 18 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 45 helps relate physical bit attacks and LSB attacks. Suppose t is the witness such that $\varepsilon^{(\text{est})}_{\text{PHYS}}(\vec{\alpha}) = \varepsilon^{(\text{est})}_{\text{LSB}}(\ (2^t\alpha_1, \alpha_2)\ )$. Then, consider the adversary against $\mathsf{ShamirSS}(2, 2,\ (2^t\alpha_1, \alpha_2)\ )$ that uses the LSB attack as guaranteed by Corollary 16. Lemma 45 proves that the leakage distribution of the physical bit attack $\vec{\text{PHYS}}_{0,t}$ on $\mathsf{ShamirSS}(2, 2, \vec{\alpha})$ secret-sharing scheme has an identical distribution. So, we run the adversary of Corollary 16 by leaking $\vec{\text{PHYS}}_{0,t}$ from the secret shares of the $\mathsf{ShamirSS}(2, 2, \vec{\alpha})$ secret-sharing scheme. ◀

Finally, we prove Corollary 19 for Mersenne primes.

Proof of Corollary 19, for Mersenne primes. **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 $t \in \{0, 1, \ldots, \lambda - 1\}$. For $t \in \{0, 1, \ldots, \lambda - 1\}$, by Corollary 15, we get the bound that

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

Just like the proof of Corollary 46, we have

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

Proof of the second part. If the algorithm in Figure 2 outputs “may be insecure” then there is some $k \in \{0, 1, \ldots, \lambda - 1\}$ such that the algorithm in Figure 1 outputs “may be insecure" for $(2^k\alpha_1, \alpha_2)$. Corollary 15 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. ◀

F.3.2 Case B: p is a Fermat Prime

We start by extending Lemma 11 from $\vec{\mathrm{LSB}}$ to $\vec{\mathrm{PHYS}}_{i,j}$, over Fermat primes.

▶ **Lemma 48.** *Fix prime $p = 2^\lambda + 1$. Consider* $\mathsf{ShamirSS}(2,2,(\alpha_1,\alpha_2))$ *over prime field F of order p. Define $u := 2^{-i}\cdot\alpha_1$ and $v := 2^{-j}\cdot\alpha_2$.*

$$\mathsf{SD}\Big(\vec{\mathrm{PHYS}}_{i,j}(\mathsf{Share}(0))\ ,\ \vec{\mathrm{PHYS}}_{i,j}(\mathsf{Share}(s))\Big) = \frac{1}{2p}\cdot\left|\Sigma_{u,v}^{(\Delta_1)} - \Sigma_{u,v}^{(\Delta_2)}\right|$$

where $\Delta_1 = \alpha_2^{-1}2^{-1}\cdot(2^j-1) - \alpha_1^{-1}2^{-1}\cdot(2^i-1)$ and $\Delta_2 = (s\cdot 2^{-1})\cdot(\alpha_1^{-1}-\alpha_2^{-1}) + \alpha_2^{-1}2^{-1}\cdot(2^j-1) - \alpha_1^{-1}2^{-1}\cdot(2^i-1)$, both are automorphisms over F.

Note that $\Delta_2 = (s\cdot 2^{-1})\cdot(\alpha_1^{-1}-\alpha_2^{-1}) + \Delta_1$ and Δ_1 is a constant independent of s.

Proof. Given $s \in F_p$, by following the same derivation as in the proof of Lemma 45, we get

$$\begin{aligned}
&\mathsf{SD}\Big(\vec{\mathrm{PHYS}}_{i,j}(\mathsf{Share}(0))\ ,\ \vec{\mathrm{PHYS}}_{i,j}(\mathsf{Share}(s))\Big)\\
&= 2\cdot\Big|\mathop{\mathbb{E}}_x\big[\mathbb{1}_E(2^{-i}\alpha_1 x + 2^{-i}-1)\cdot\mathbb{1}_E(2^{-j}\alpha_2 x + 2^{-j}-1)\big]\\
&\qquad - \mathop{\mathbb{E}}_x\big[\mathbb{1}_E(2^{-i}\alpha_1 x + 2^{-i}s + 2^{-i}-1)\cdot\mathbb{1}_E(2^{-j}\alpha_2 x + 2^{-j}s + 2^{-j}-1)\big]\Big|\\
&\qquad\qquad (\text{By Proposition 17, } E := \mathrm{PHYS}_0^{-1}(0))\\
&= 2\cdot\Big|\mathop{\mathbb{E}}_y\big[\mathbb{1}_E(2^{-i}\alpha_1 y)\cdot\mathbb{1}_E(2^{-j}\alpha_2 y - s')\big]\\
&\qquad - \mathop{\mathbb{E}}_x\big[\mathbb{1}_E(2^{-i}\alpha_1 x + 2^{-i}s + 2^{-i}-1)\cdot\mathbb{1}_E(2^{-j}\alpha_2 x + 2^{-j}s + 2^{-j}-1)\big]\Big|\\
&\qquad\qquad \Big(\text{By substituting } y := x + \alpha_1^{-1} - 2^i\cdot\alpha_1^{-1}\\
&\qquad\qquad\quad \text{and } s' := 2^{i-j}\alpha_1^{-1}\alpha_2\cdot(2^{-i}-1) - 2^{-j}+1\Big)\\
&= 2\cdot\Big|\mathop{\mathbb{E}}_y\big[\mathbb{1}_E(2^{-i}\alpha_1 y)\cdot\mathbb{1}_E(2^{-j}\alpha_2 y + s')\big]\\
&\qquad - \mathop{\mathbb{E}}_z\big[\mathbb{1}_E(2^{-i}\alpha_1 z)\cdot\mathbb{1}_E(2^{-j}\alpha_2 z - s'')\big]\Big|\\
&\qquad\qquad \Big(\text{By substituting } z := x + \alpha_1^{-1}\cdot s + \alpha_1^{-1} - 2^i\cdot\alpha_1^{-1}\\
&\qquad\qquad\quad \text{and } s'' := 2^{-j}\cdot(\alpha_1^{-1}\alpha_2 - 1)s + 2^{i-j}\alpha_1^{-1}\alpha_2\cdot(2^{-i}-1) - 2^{-j}+1\Big)
\end{aligned}$$

All variable substitutions $x \mapsto y$, $x \mapsto z$, and $s \mapsto s''$ made above are automorphisms over F^*. Applying Claim 26 to above, we get

$$\mathsf{SD}\Big(\vec{\mathrm{PHYS}}_{i,j}(\mathsf{Share}(0))\ ,\ \vec{\mathrm{PHYS}}_{i,j}(\mathsf{Share}(s))\Big)$$

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

$$= \frac{1}{2}\cdot\left|\mathop{\mathbb{E}}_{y}\left[\text{sign}_p(2^{-i}\alpha_1 y\cdot 2^{-1})\cdot \text{sign}_p((2^{-j}\alpha_2 y - s')\cdot 2^{-1})\right] - \mathop{\mathbb{E}}_{z}\left[\text{sign}_p(2^{-i}\alpha_1 z\cdot 2^{-1})\cdot \text{sign}_p((2^{-j}\alpha_2 z - s'')\cdot 2^{-1})\right]\right|$$

$$= \frac{1}{2p}\cdot\left|\sum_{X\in F}\text{sign}_p(2^{-i}\alpha_1 X)\cdot\text{sign}_p(2^{-j}\alpha_2 X - s'\cdot 2^{-1}) - \sum_{X'\in F}\text{sign}_p(2^{-i}\alpha_1 X')\cdot\text{sign}_p(2^{-j}\alpha_2 X' - s''\cdot 2^{-1})\right|$$

$$= \frac{1}{2p}\cdot\left|\sum_{X\in F}\text{sign}_p(2^{-i}\alpha_1 X)\cdot\text{sign}_p(2^{-j}\alpha_2\cdot(X - s'\cdot 2^{-1}\cdot 2^{j}\cdot\alpha_2^{-1})) - \sum_{X\in F}\text{sign}_p(2^{-i}\alpha_1 X)\cdot\text{sign}_p(2^{-j}\alpha_2(X - s''\cdot 2^{-1}\cdot 2^{j}\cdot\alpha_2^{-1}))\right|$$

$$= \frac{1}{2p}\cdot\left|\Sigma^{(\Delta_1)}_{2^{-i}\alpha_1,2^{-j}\alpha_2} - \Sigma^{(\Delta_2)}_{2^{-i}\alpha_1,2^{-j}\alpha_2}\right|$$

where Δ_1 and Δ_2 are:

$$\begin{aligned}\Delta_1 &= s'\cdot 2^{-1}\cdot 2^{j}\cdot\alpha_2^{-1} = \alpha_2^{-1}2^{-1}\cdot(2^{j}-1) - \alpha_1^{-1}2^{-1}\cdot(2^{i}-1)\\ \Delta_2 &= s''\cdot 2^{-1}\cdot 2^{j}\cdot\alpha_2^{-1}\\ &= (s\cdot 2^{-1})\cdot(\alpha_1^{-1}-\alpha_2^{-1}) + \alpha_2^{-1}2^{-1}\cdot(2^{j}-1) - \alpha_1^{-1}2^{-1}\cdot(2^{i}-1)\end{aligned}$$

◀

With this lemma, one can follow the same lines of calculations as in the proof for Theorem 10 in Section 4.1, and achieve a tight bound for $\mathsf{SD}\left(\vec{\text{PHYS}}_{i,j}(\mathsf{Share}(0))\ ,\ \vec{\text{PHYS}}_{i,j}(\mathsf{Share}(s))\right)$ as the one stated in Theorem 10. This then generates a variant of Corollary 14 and Corollary 15 for physical bit leakages for Fermat primes, proving Corollary 19 for Fermat primes.

F.4 Proof of Corollary 20 and Corollary 21

Proof of Corollary 20. For the proof, fix $\alpha_1 = 1$ and $\alpha_2 = 2^{\lfloor\lambda/2\rfloor} - 1$. We shall compute $\varepsilon_{\text{LSB}}(2^i\cdot\alpha_1,\alpha_2)$ for all $i\in\{0,1,\dots,\lambda-1\}$ using Theorem 10. The bound in our corollary will be the maximum of these individual upper bounds on $\varepsilon_{\text{LSB}}(\cdot)$.

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 10, we have

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

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 10, we have

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

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

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

Substitute $u' = 2^j$, where $1 \leqslant j \leqslant \lfloor \lambda/2 \rfloor$, and $v' = -(2^{\lambda-t} - 1)$. Therefore, by Theorem 10, we have

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

Appendix F.4.1 proves the following upper bound on the insecurity for all $0 \leqslant i < \lambda$.

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

and this concludes the proof. ◀

Proof of Corollary 21. Just as we did for the proof of Corollary 20 above, we begin by fixing $\alpha_1 = 1$ and $\alpha_2 = 2^{\lambda/2} - 1$, and consider $\varepsilon_{\text{LSB}}(2^i \cdot \alpha_1, \alpha_2)$ for all $i \in \{0, 1, \ldots, \lambda\}$. Note that when $p = 2^\lambda + 1$ is a Fermat prime, $\lambda \bmod 2 = 0$, i.e. $\lambda/2 \in \mathbb{Z}$. As defined in the algorithm in Figure 4, set $B := \lceil 2^{3/4}\sqrt{p} \rceil > \lceil \sqrt{p} \rceil = 2^{\lambda/2} + 1$.

Case A: $i = 0$. Since $(2^i\alpha_1, \alpha_2) = (\alpha_1, \alpha_2) = (1, 2^{\lambda/2} - 1)$, we may choose $(u, v) = (1, 2^{\lambda/2} - 1)$ because both $|u|_p = 1$ and $|v|_p = 2^{\lambda/2} - 1$ are less than B. Hence, the LSB advantage is, by Theorem 10,

$$\begin{aligned} \varepsilon_{\text{LSB}}(2^i \cdot \alpha_1, \alpha_2) &\leqslant \frac{g^2}{|u|_p |v|_p} + \frac{4(|u|_p + |v|_p) - 3/2}{p} \\ &= \frac{1}{2^{\lambda/2} - 1} + \frac{4 \cdot 2^{\lambda/2} - 3/2}{p} = \frac{4 \cdot 2^{\lambda/2}}{4 \cdot (2^\lambda - 2^{\lambda/2})} + \frac{4 \cdot 2^{\lambda/2} - 3/2}{p} \\ &\leqslant \frac{4 \cdot 2^{\lambda/2}}{p} + \frac{4 \cdot 2^{\lambda/2} - 3/2}{p} \qquad (p = 2^\lambda + 1 \leqslant 4(2^\lambda - 2^{\lambda/2}) \text{ for } \lambda \geqslant 2) \\ &= \frac{8 \cdot 2^{\lambda/2} - 3/2}{p} \end{aligned}$$

Case B: $i \in \{1, 2, \ldots, \lambda/2\}$. We have $(2^i\alpha_1, \alpha_2) = (2^i, 2^{\lambda/2} - 1)$. We can still choose $u = 2^i\alpha_1 = 2^i$ and $v = \alpha_2 = 2^{\lambda/2} - 1$ as both $|u|_p$ and $|v|_p$ would be still less than B, except $|u|_p$ would be even this time. Then, again by Theorem 10,

$$\begin{aligned} \varepsilon_{\text{LSB}}(2^i \cdot \alpha_1, \alpha_2) &\leqslant \frac{4(|u|_p + |v|_p) - 3/2}{p} = \frac{4 \cdot 2^i + 4 \cdot 2^{\lambda/2} - 11/2}{p} \\ &\leqslant \frac{4 \cdot 2^{\lambda/2} + 4 \cdot 2^{\lambda/2} - 11/2}{p} \\ &= \frac{8 \cdot 2^{\lambda/2} - 11/2}{p} \end{aligned}$$

Case C: $i \in \{\lambda/2+1, \lambda/2+2, \ldots, \lambda\}$**.** For this case, $2^i > \sqrt{p}$ and hence we need to choose u and v differently. For simplicity, denote $i = \lambda/2 + j$ for $j \in \{1, 2, \ldots, \lambda/2\}$. Let $u = 2^{\lambda/2}2^i$ and $v = 2^{\lambda/2}(2^{\lambda/2} - 1)$. Clearly $(u, v) \in [\alpha_1 \colon \alpha_2]$ and they can be simplified as follows

$$u = 2^{\lambda/2}2^i = 2^{\lambda}2^j = -2^j \quad \bmod p$$
$$v = 2^{\lambda/2}(2^{\lambda/2} - 1) = 2^{\lambda} - 2^{\lambda/2} = -(2^{\lambda/2} + 1) \quad \bmod p$$

Then $|u|_p = 2^j < \sqrt{p} < B$ and $|v|_p = 2^{\lambda/2} + 1 = \lceil \sqrt{p} \rceil < B$. Hence, by Theorem 10,

$$\begin{aligned}\varepsilon_{\mathrm{LSB}}(2^i \cdot \alpha_1, \alpha_2) &\leqslant \frac{4(|u|_p + |v|_p) - 3/2}{p} = \frac{4 \cdot 2^j + 4 \cdot 2^{\lambda/2} + 4 - 3/2}{p} \\ &\leqslant \frac{8 \cdot 2^{\lambda/2} - 5/2}{p}.\end{aligned}$$

This completes the proof. ◀

F.4.1 Proof of inequality used in the proof of Corollary 20

Observe that $\lambda - t = \lambda - \lfloor \lambda/2 \rfloor = \lceil \lambda/2 \rceil \geqslant \lfloor \lambda/2 \rfloor = t$. 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 $p = 2^{\lambda} - 1$ 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

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

which is true for all $t \geqslant 1$. Therefore, the overall maximum is

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

◀

G Extension to arbitrary Number of Parties: Proofs

G.1 Proof of Corollary 23

Proof of Corollary 23. Choose arbitrary distinct evaluation places $\alpha_1, \alpha_2, \alpha_4, \dots, \alpha_n \in F_p^*$. Choose α_3 uniformly at random from the set $F_p \setminus \{\alpha_1, \alpha_2, \alpha_4, \dots, \alpha_n\}$.

Define $\beta_i := \left(\alpha_i \prod_{j \neq i} (\alpha_i - \alpha_j)\right)^{-1}$ as in Theorem 22, for $i \in \{1, \dots, n\}$. 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.

Define

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

Then, we have

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

We make the following observations.

1. $\Delta \neq 0$, because $\alpha_2 \neq 0$ and $\alpha_2 \notin \{\alpha_4, \dots, \alpha_n\}$.
2. $\left|\left\{\Delta \cdot \left(1 + \frac{\alpha_2 - \alpha_1}{\alpha_1 - \alpha_3}\right) \colon \alpha_3 \in F_p^* \setminus \{\alpha_1, \alpha_2, \alpha_4, \dots, \alpha_n\}\right\}\right| = (p-1) - (n-1) = p - n$, since the mapping $\alpha_3 \mapsto \Gamma$ is a bijection.

Note that $[\beta_1 : \beta_2]$ is identical to $[\gamma_1^{-1} : \gamma_2^{-1}] = \left[1 : \Gamma^{-1}\right]$. By Corollary 19, there are at most

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

values of $\alpha_3 \in F_p^* \setminus \{\alpha_1\}$ such that the algorithm in Figure 3 returns "may be insecure" for $\mathsf{ShamirSS}(2, 2, (\beta_1, \beta_2))$. Thus, there are at most

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

values of $\alpha_3 \in F_p^* \setminus \{\alpha_1, \alpha_2, \alpha_4, \dots, \alpha_n\}$ that are classified as "may be insecure". This implies that, when $\alpha_3 \leftarrow F_p^* \setminus \{\alpha_1, \alpha_2, \alpha_4, \dots, \alpha_n\}$, the probability the algorithm reports "may be insecure" is at most

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

This completes the proof. ◀

G.2 Proof of Theorem 22

Before we dive into the proof of Theorem 22, we shall recall some definitions and basic results regarding generalized Reed-Solomon (GRS) code and Fourier analysis of Boolean functions that are necessary to understand the proof of Theorem 22.

G.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 [30, 42].

▶ **Theorem 49** (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.

G.2.2 Fourier Analysis Basics

We use Fourier analysis on prime field F of order p. Define $\omega := \exp(2\pi \mathrm{i}/p)$. 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 50** (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 51.** *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 52** (Properties of Fourier Coefficients)**.** *For all $S \subseteq F$ and $x, \alpha \in F$, it holds that*

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

G.2.3 Some Preparatory Results

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

▶ **Proposition 53.** *Consider* ShamirSS(n, n) *over a prime field F. Let $C_0^{\perp}$ be the dual code of* Share(0)*. For any one-bit leakage function, $\vec{\tau}\colon F^n \to \{0,1\}^n$, the following identity holds for any secret $s \in F$.*

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

Proof of Proposition 53. The following identity is known in the literature (see [43] for proof).

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

By Proposition 51, $\widehat{\mathbb{1}_{\tau_i^{-1}(\ell_i)}}(\gamma_i) = \widehat{\mathbb{1}_{\tau_i^{-1}(1-\ell_i)}}(\gamma_i)$ since $\tau_i^{-1}(\ell_i)$ and $\tau_i^{-1}(1-\ell_i)$ are a partition of F. Using this property, one can verify for every $\vec{\ell}, \vec{\ell'} \in \{0,1\}^n$, it holds that

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

Therefore, we have

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

as desired. ◀

▶ **Proposition 54.** *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.*

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

$$= \frac{1}{p^{n-1}} \sum_{\substack{x_n \in A_n \cdot \beta_n \\ \vdots \\ x_3 \in A_3 \cdot \beta_3}} \mathsf{card}(A_2) - \mathsf{card}\left(\left(A_2 \cdot \beta_2 + \sum_{i=3}^{n} x_i - s \cdot \sum_{i=1}^{n} \beta_i\right) \bigcap A_1 \cdot \beta_1\right)$$

Proof of Proposition 54. 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. ◀

G.2.4 Putting things together and proving Theorem 22

We can now prove Theorem 22.

Proof of Theorem 22. 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 49, the dual code $C_0^\perp$ is the set $\{t\cdot(\beta_1,\beta_2,\dots,\beta_n)\colon t\in F\}$, where

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

Consider the following manipulation.

$$\begin{aligned}
&2\mathsf{SD}(\vec{\tau}(\mathsf{Share}(0))\ ,\ \vec{\tau}(\mathsf{Share}(s)))\\
&= 2^n\cdot\left|\sum_{\vec{\gamma}\in\mathcal{C}_0^\perp\setminus\vec{0}}\prod_{i=1}^n \widehat{\mathbb{1}_{\tau_i^{-1}(0)}}(\gamma_i)\cdot\left(1-\omega^{s\cdot(\gamma_1+\cdots+\gamma_n)}\right)\right| \qquad \text{(By Proposition 53)}\\
&= 2^n\cdot\left|\sum_{t\in F^*}\prod_{i=1}^n \widehat{\mathbb{1}_{A_i}}(t\cdot\beta_i)\cdot\left(1-\omega^{s\cdot t\cdot(\beta_1+\cdots+\beta_n)}\right)\right|\\
&= 2^n\cdot\left|\sum_{t\in F^*}\prod_{i=1}^n \widehat{\mathbb{1}_{A_i\cdot\beta_i}}(t) - \sum_{t\in F^*}\prod_{i=1}^n \widehat{\mathbb{1}_{A_i\cdot\beta_i}}(t)\cdot\omega^{s\cdot t\cdot\beta_i}\right|
\end{aligned}$$

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

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

Then, it follows from Proposition 54 that

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

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

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

where $\Delta_{x_3,\dots,x_n}^{(s)} := 2^{-1}\cdot\left(\sum_{i=3}^n x_i - s\cdot\sum_{i=1}^n\beta_i\right)$. Similar to the proof of Lemma 11 in Appendix D.1, we have

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

$$\leqslant \frac{2^{n-2}}{p^{n-1}} \cdot \sum_{x_n \in E \cdot \beta_n} \cdots \sum_{x_3 \in E \cdot \beta_3} \left| \left(\Sigma_{\beta_1^{-1}, \beta_2^{-1}}^{\left(\Delta_{x_3,\ldots,x_n}^{(0)}\right)} - \Sigma_{\beta_1^{-1}, \beta_2^{-1}}^{\left(\Delta_{x_3,\ldots,x_n}^{(s)}\right)} \right) \right| \qquad \text{(By triangle inequality)}$$

Suppose $\mathsf{ShamirSS}(2, 2, (\beta_1, \beta_2))$ have ε insecurity against LSB. Then, it follows from Lemma 11 that

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

Applying the above inequality for every term under the summand yields:

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

which completes the proof. ◀

H Attack on $\mathsf{ShamirSS}(3, 3, \vec{\alpha})$

Consider $\mathsf{ShamirSS}(3, 3, \vec{\alpha})$ and the underlying prime field F of order $p = 4w^2 + 6w + 9$ where $w \geqslant 4$ and $w \neq 0 \mod 3$. The evaluation places are $\vec{\alpha} = (1, \sigma, \sigma^2)$ for $\sigma = 2w \cdot 3^{-1} \in F_p$.

▷ Claim 55. $\left(2w \cdot 3^{-1}\right)^3 = 1 \mod p$ when $p = w^2 + 6w + 9$ and $w \geqslant 4$.

Proof. $\left(2w \cdot 3^{-1}\right)^3 = 1 \mod p \iff (2w)^3 - 3^3 = 0 \mod p \iff (2w-3) \cdot (4w^2+6w+9) = 0 \mod p$ holds since $p = 4w^2 + 6w + 9$. ◀

Observe that $2w < \sqrt{p}$ and $3 < \sqrt{p}$. Then, by our classifier in Figure 1, $[1 : \sigma]$ is a good evaluation place since $[1 : \sigma] = [3 : 2w]$, $\gcd(3, 2w) = 1$, and $3 \cdot 2w$ is an even integer.

Note that $1 + \sigma + \sigma^2 = 1$; therefore, this secret sharing inherits the vulnerability of the additive secret sharing against LSB leakage [43]. Therefore, $\mathsf{ShamirSS}(3, 3, \vec{\alpha})$ is insecure against LSB leakage, where its insecurity is $\geqslant (2/\pi)^3 \geqslant 0.25$ [45, 19].

I 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

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

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 56 (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).

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 20 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.

I.1 Finding secure evaluation places for $n = k > 2$

Consider the derandomization problem for $n = k = 3$. Recall that we would have

$$\beta_1 = \frac{1}{\alpha_1(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)} \quad \text{and} \quad \beta_2 = \frac{1}{\alpha_2(\alpha_2 - \alpha_1)(\alpha_2 - \alpha_3)}.$$

Suppose our target is to ensure that $\frac{\beta_1}{\beta_2} = \gamma$; that is, the equivalence class $[1 \colon \gamma]$ are good evaluation places for $\mathsf{ShamirSS}(2, 2)$. Substituting β_1 and β_2 into the condition, we get

$$\gamma := \frac{\beta_1}{\beta_2} = -\frac{\alpha_2(\alpha_2 - \alpha_3)}{\alpha_1(\alpha_1 - \alpha_3)}$$

The following assignments should clearly satisfy the above constraint:

$$\begin{cases}\alpha_1 - \alpha_3 = \alpha_2\\ \alpha_2 - \alpha_3 = -\gamma \cdot \alpha_1\end{cases}$$

which, upon solving in terms of α_3, we get

$$\alpha_1 = \frac{2}{1 + \gamma} \cdot \alpha_3 \quad \text{and} \quad \alpha_2 = \frac{1 - \gamma}{1 + \gamma} \cdot \alpha_3.$$

Specifically, $\alpha_1 = 2$, $\alpha_2 = 1 - \gamma$, and $\alpha_3 = 1 + \gamma$ suffices, and we can ensure that $[\beta_1 \colon \beta_2]$ is secure with these evaluation places.

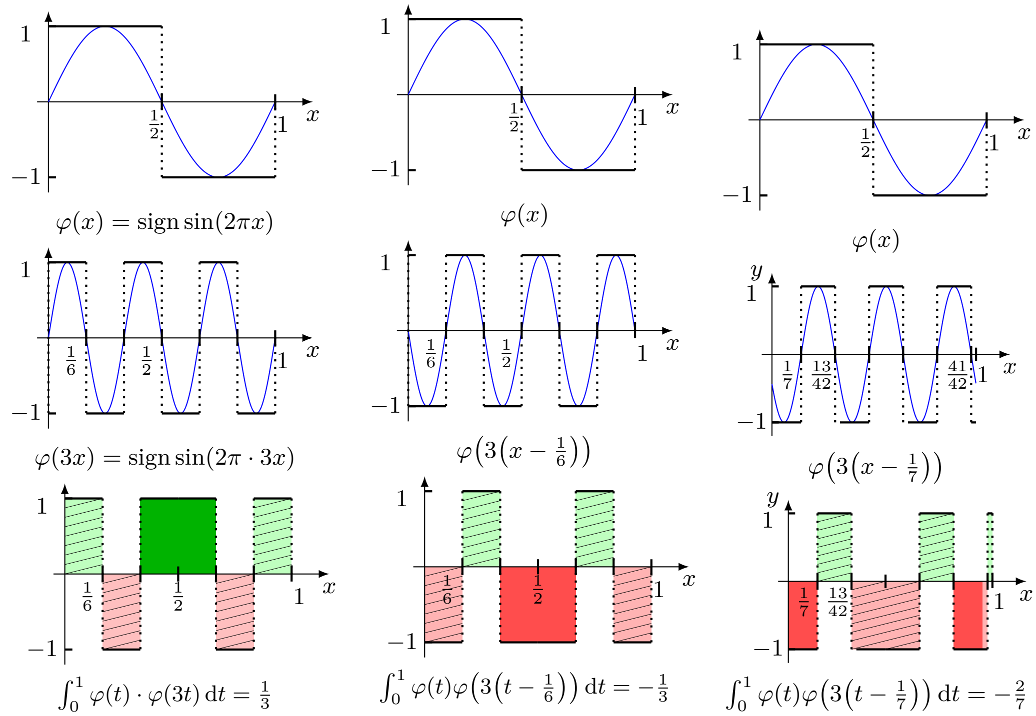
We can further generalize this argument to $n = k > 3$ cases; concretely, one can choose the following evaluation places (and so does their equivalence class).

$$\alpha_1 = (n-1)$$
$$\alpha_2 = (n-1) - (1+\gamma) = (n-2-\gamma)$$
$$\alpha_j = (j-2)\cdot(1+\gamma). \qquad \text{(For } j \in \{3,4,5,\dots,n\}\text{)}$$

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.

J Figure for square waves



(a) Square waves $\varphi(x)$ and $\varphi(3x)$ have the largest correlation.

(b) $\varphi(x)$ and $\varphi\big(3\big(x - \frac{1}{6}\big)\big)$ have the largest negative correlation.

(c) Largest "achievable" negative correlation when $p = 7$.

Figure 5