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

Jihun Hwang
Department of Computer Science, Purdue University, West Lafayette, IN, USA

Hemanta K. Maji
Department of Computer Science, Purdue University, West Lafayette, IN, USA

Hai H. Nguyen
Department of Computer Science, ETH, Zürich, Switzerland

Xiuyu Ye
Department of Computer Science, Purdue University, West Lafayette, IN, USA

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 Theory of computation → Cryptographic primitives; Security and privacy → Cryptanalysis and other attacks

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.2025.3

Related Version *Extended version with full proof*: `https://www.cs.purdue.edu/homes/hmaji/papers/HMNY24.pdf` [27]

Funding *Hemanta K. Maji*: Partly supported by CNS–2055605 and CCF–2327981.
Hai H. Nguyen: Partly supported by the Zurich Information Security & Privacy Center (ZISC), ETH Zurich.

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 [28, 29, 10]. For instance, *repairing Reed-Solomon codes* [20, 21], when possible, recovers the entire secret in the corresponding *Shamir's secret sharing* [40] 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 [8], considering their wide use in key distribution [37, 43], masking schemes [10, 18], and other higher-level primitives like secure computation [17].

Local leakage resilience [4, 19] 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 shared secret [33, 1, 34, 14]. 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 [33, 35]. 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 $x \in \{0, 2, \ldots, (p-1)\}$; 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 $u, v \in \left\{-\lceil\sqrt{p}\rceil, \ldots, 0, \ldots, \lceil\sqrt{p}\rceil\right\}$ 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. [35] and, very recently, Nguyen [38] 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 [13, 12]. We summarizes this discussion and other prior relevant works in the full version [27] of the paper.

▶ 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 [5, 2, 41, 3, 30, 6, 15, 41, 16, 26, 11, 36, 9]) 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 scheme. Shamir's secret-sharing scheme among n parties with reconstruction threshold k over a finite field F and distinct evaluation places $\alpha_1, \alpha_2, \ldots, \alpha_n \in F^*$ proceeds as follows. To share a secret $s \in F$, sample a random F-polynomial $P(X)$ such that $\deg P < k$ and $P(0) = s$. Define the shares: $s_1 := P(\alpha_1)$, $s_2 := P(\alpha_2)$, $\ldots$, and $s_n := P(\alpha_n)$. Denote this secret-sharing by $\mathsf{ShamirSS}(n, k, \vec{\alpha})$ and the joint distribution of the shares by $\mathsf{Share}(s)$ – other parameters will be clear from the context. *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 $\{0, 1, \ldots, (p-1)\}$.

▶ 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 $i \in \{0, 1, \ldots, \lambda - 1\}$. For example, PHYS_0 (also referred to as LSB) outputs 0 for the elements in $\{0, 2, \ldots, (p-1)\}$, where $p \geqslant 3$, and PHYS_1 outputs 0 for the elements in $\{0, 1, 4, 5, \ldots\}$. For $\mathbf{i} = (i_1, i_2, \ldots, i_n) \in \{0, 1, \ldots, \lambda - 1\}^n$, 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 $t \in \{1, 2, \ldots, n\}$. 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: $\mathrm{PHYS} := \left\{ \vec{\mathrm{PHYS}}_{\mathbf{i}} : \mathbf{i} = (i_1, \ldots, i_n) \in \{0, 1, \ldots, \lambda - 1\}^n \right\}$.
2. LSB leakage family: $\mathrm{LSB} := \left\{ \vec{\mathrm{PHYS}}_{\mathbf{0}} \right\}$, where $\mathbf{0} = (0, 0, \ldots, 0)$

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

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

Low insecurity indicates the statistical independence of the leakage from the secret, i.e., the *secret-sharing is locally leakage-resilient* [4, 19]. Recently, Faust et al. [14] 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. [33] 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 $\varepsilon_{\mathrm{PHYS}}(\vec{\alpha}) \leqslant p^{-1/2}$ with probability $\geqslant 1 - p^{-1/2}$.

Recently, [35] 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) $\varepsilon_{\mathrm{PHYS}}(\vec{\alpha}) \leqslant p^{-1/2}$ or (2) $\varepsilon_{\mathrm{PHYS}}(\vec{\alpha}) > p^{-1/2}$.*

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

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 $\mathcal{O}\big(\sqrt{p} \cdot \log p\big)$.
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 LS 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 $n = 2$

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 $\mathcal{O}\Big(\sqrt{p} \cdot (\log p)^2\Big)$.
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.
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. We provide an example for Mersenne prime $p = 2^{13} - 1$ in the full version of our paper [27].

Result B: Security against Physical Bit Leakage when $n > 2$

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.

Given evaluation places $\vec{\alpha} := (\alpha_1, \alpha_2, \ldots, \alpha_n)$ we efficiently compute an appropriate $\vec{\beta} := (\beta_1, \beta_2, \ldots, \beta_n)$ (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 [7] 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 [34, 14]; Appendix C 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 secret sharing scheme $\mathsf{ShamirSS}(2,2,(\beta_1,\beta_2))$ using Corollary 19.

We can obtain secure evaluation places for $n = k > 2$ case by bootstrapping from the explicit secure evaluation places for $n = k = 2$ case. For example, $\alpha_1 = (n-1)$, $\alpha_2 = (n-1) - (1+\gamma)$, and $\alpha_j = (j-2)\cdot(\gamma+1)$, for $j \in \{3,4,\ldots,n\}$, 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).

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 [23]). We find "small norm" $u, v \in \left\{-\lceil\sqrt{p}\rceil, \ldots, 0, 1, \ldots, \lceil\sqrt{p}\rceil\right\}$ with the property mentioned above – a Dirichlet approximation problem. We solve it with a small constant multiplicative slack using the LLL [32] algorithm in $\mathsf{poly}(\lambda)$ runtime, where $\lambda := \lceil \log_2(p+1) \rceil$. 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 $\mathrm{LSB}(u \cdot X) \neq \mathrm{LSB}(v \cdot X)$.

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.

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

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 [31] 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 A.
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 $\left| u \cdot v / g^2 \right| \geqslant \sqrt{p}$: Declare $\mathsf{ShamirSS}(2, 2, (\alpha_1, \alpha_2))$ is secure against LSB leakage
6. (Else) Declare that the security of $\mathsf{ShamirSS}(2, 2, (\alpha_1, \alpha_2))$ against LSB attacks may be insecure

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

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. The error of our approximation is directly proportional to the total number of oscillations of the square waves. The approximation error is $\leqslant (|u| + |v|)/p = \mathcal{O}\big(1/\sqrt{p}\big)$, exponentially small in λ, for small norm u, v. For simplicity, the presentation below ignores this approximation error.

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 [23]. 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 [42, 25, 24]. Various families of square waves, like the ones by Haar [22], Walsh [44], and Rademacher [39], 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 [23], the leakage is identical to the LSB leakage with evaluation places $(2^{j-i} \cdot \alpha_1, \alpha_2)$. Consequently,

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

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

▶ 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 $t \in \{0, 1, \ldots, \lambda - 1\}$. 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.

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

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

Therefore, $\mathrm{PHYS}_i(x) = \mathrm{LSB}(2^{-i} \cdot x + 2^{-i} - 1)$. 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. [14]; the ideas to analyze Fermat prime modulus are new.

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

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

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

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

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

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

Now consider the $\mathsf{ShamirSS}(2, 2, (\beta_i, \beta_j))$ secret-sharing scheme for all distinct $i, j \in \{1, \ldots, n\}$. 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.

▶ 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 the corresponding $\mathsf{ShamirSS}(n, n, \vec{\alpha})$; *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 [7] 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 [34, 14]; Appendix C presents the details.

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 secure.
3. Otherwise, the algorithm states that $\mathsf{ShamirSS}(n, n, \vec{\alpha})$ may be insecure.

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

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 $\alpha_1 \colon \alpha_2 \colon \alpha_3 = u \colon v \colon w$. 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 C 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* $p \geqslant 3$*.*

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

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*

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

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

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

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 we presents the complete proof in the full version of our paper [27]. 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

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

Then, we can solve for the optimal $s \in F^*$ that maximizes the statistical distance. Below, we present a high-level overview of the proof of Theorem 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.

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

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

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

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

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

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

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

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

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

▶ **Lemma 13.** *Let* $\triangle : \mathbb{R} \to [-1, +1]$ *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* $g = \gcd(u, v)$

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

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 B.

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 $(u, v) \in [\alpha_1 : \alpha_2]$ such that $|u|, |v| \leqslant B$, where $B = \lceil 8^{1/4} \cdot \sqrt{p} \rceil$. Let $\triangle : \mathbb{R} \to [-1, +1]$ 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*

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

Then,

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

Proof. Use the LLL algorithm [32] to efficiently find $(u, v) \in [\alpha_1 : \alpha_2]$ with properties mentioned in the corollary (see Appendix A for details). Observe that the LHS of the expression in Theorem 10 is identical to $\varepsilon_{\text{LSB}}(\vec{\alpha})$ 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 $p \geqslant 11$.

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.

5 Security against all Physical Bit Leakage

We consider $\mathsf{ShamirSS}(n = 2, k = 2, (\alpha_1, \alpha_2))$ 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 $x \in F_p$,*

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

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

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

because $2^k\alpha_1 = \alpha_2$. When $t = 0$, both the leakage bits are identical. On the other hand, for $t = t^* := (2^k - 1)^{-1}$, the joint distribution of leakage is

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

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.

▶ **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,*

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

where $i, j \in \{0, 1, \ldots, \lambda - 1\}$, $j - i = k \mod \lambda$. 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 $p \geqslant 11$.

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*

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

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*

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

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,*

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

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.

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. 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.
6. 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.
7. Viktor Bouniakowsky. *Sur les diviseurs numériques invariables des fonctions rationnelles entieres.* De l'Imprimerie de l'Académie impériale des sciences, 1854.
8. Luís T. A. N. Brandão and René Peralta. NIST first call for multi-party threshold schemes. https://csrc.nist.gov/publications/detail/nistir/8214c/draft, January 25, 2023.
9. 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.

10 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.

11 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.

12 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. doi:10.1109/ISIT54713.2023.10206937.

13 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.

14 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. doi:10.1007/978-3-031-58737-5_12.

15 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.

16 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.

17 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.

18 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.

19 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.

20 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.

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

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

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

24 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.

25 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.

26 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.

27 Jihun Hwang, Hemanta K. Maji, Hai H. Nguyen, and Xiuyu Ye. Security of shamir's secret-sharing against physical bit leakage: Secure evaluation places. https://www.cs.purdue.edu/homes/hmaji/papers/HMNY24.pdf, 2023.

28 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.

29 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.

30 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.

31 Jeffrey C Lagarias. The computational complexity of simultaneous diophantine approximation problems. *SIAM Journal on Computing*, 14(1):196–209, 1985. doi:10.1137/0214016.

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

33 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.

34 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.

35 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. doi:10.1007/978-3-031-58737-5_11.

36 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.

37 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. doi:10.1007/3-540-48910-X_23.

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

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

40 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.

41 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.

42 R Titsworth. Coherent detection by quasi-orthogonal square-wave pulse functions (corresp.). *IRE Transactions on Information Theory*, 6(3):410–411, 1960. doi:10.1109/TIT.1960.1057575.

43 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.

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

A Solving Simultaneous Diophantine Equations

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

▶ **Theorem 24** (LLL [32, 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."

B 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 $D_0 := \vec{\mathsf{LSB}}(\mathsf{Share}(0))$ and sends it to

the attacker. Otherwise, the challenger samples (ℓ_1, ℓ_2) from distribution $D_1 := \vec{\mathrm{LSB}}(\mathsf{Share}(s))$ and sends it to the attacker. The attacker aims to guess which distribution (ℓ_1, ℓ_2) is sampled from. It uses the maximum likelihood decoder and then returns its guess $\tilde{b}$ to the challenger. The attacker wins the security game if $b = \tilde{b}$.

Attacker		Challenger
	$s^* \in F_p^*$ →	$D_0 = \vec{\mathrm{LSB}}(\mathsf{Share}(0))$
		$D_1 = \vec{\mathrm{LSB}}(\mathsf{Share}(s^*))$
		$b \leftarrow\$ \{0,1\}$
$\tilde{b} = \mathrm{ML}(\ell_1, \ell_2)$	← (ℓ_1, ℓ_2)	$(\ell_1, \ell_2) \leftarrow\$ D_b$
	$\tilde{b}$ →	Test $b \stackrel{?}{=} \tilde{b}$

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 $\mathrm{sign}\left(\Pr[(\ell_1,\ell_2)|s=0] - \Pr[(\ell_1,\ell_2)|s=s^*]\right)$. The maximum likelihood distinguisher can compute $(-1)^{\ell_1+\ell_2} \cdot \mathrm{sign}_p(u) \cdot \mathrm{sign}_p(v)$. If $(-1)^{\ell_1+\ell_2} \cdot \mathrm{sign}_p(u) \cdot \mathrm{sign}_p(v) > 0$, then it outputs $\tilde{b} = 0$. Otherwise, it outputs $\tilde{b} = 1$. We provide a complete proof of the distinguishing advantage and security guarantee of this adversary in the full version of our paper [27].

C Attack on 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 25. $\left(2w \cdot 3^{-1}\right)^3 = 1 \mod p$ 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 [33]. Therefore, $\mathsf{ShamirSS}(3, 3, \vec{\alpha})$ is insecure against LSB leakage, where its insecurity is $\geqslant (2/\pi)^3 \geqslant 0.25$ [34, 14].

D Derandomization for $n = k = 3$

Consider $\beta_1 = \frac{1}{\alpha_1(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)}$ and $\beta_2 = \frac{1}{\alpha_2(\alpha_2-\alpha_1)(\alpha_2-\alpha_3)}$, we want to ensure $\frac{\beta_1}{\beta_2} = \Lambda$ where $\Lambda \in F^*$ is a good evaluation place in the $\mathsf{ShamirSS}(2, 2, [1 : \Lambda])$ case. After expanding the expressing and solving the corresponding linear constraints, we obtain the following assignment.

$$\alpha_1 = \frac{2}{1+\Lambda}\alpha_3 \qquad \alpha_2 = \frac{1-\Lambda}{1+\Lambda}\alpha_3.$$

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