Constructing Leakage-resilient Shamir's Secret Sharing: Over Composite Order Fields

Hemanta K. Maji and Hai H. Nguyen and Anat Paskin-Cherniavsky and Xiuyu Ye

Abstract

Probing physical bits in hardware has compromised cryptographic systems. This work investigates how to instantiate Shamir's secret sharing so that the physical probes into its shares reveal statistically insignificant information about the secret.

Over prime fields, Maji, Nguyen, Paskin-Cherniavsky, Suad, and Wang (EUROCRYPT 2021) proved that choosing random evaluation places achieves this objective with high probability. Our work extends their randomized construction to composite order fields – particularly for fields with characteristic 2. Next, this work fully derandomizes this result for some specific cases.

Our security analysis of the randomized construction is Fourier-analytic, and the derandomization techniques are combinatorial. Our analysis relies on (1) contemporary Bézout-theorem-type algebraic complexity results that bound the number of simultaneous zeroes of a system of polynomial equations over composite order fields and (2) characterization of the zeroes of an appropriate generalized Vandermonde determinant.

1 Introduction

Threshold secret-sharing schemes, like *Shamir's secret-sharing* [Sha79], distribute a secret among parties so that a quorum can reconstruct the secret. Their security is against an adversary who obtains the shares of a group of parties (who do not form the quorum) and has no information on the remaining shares. Side-channel attacks have repeatedly circumvented such "all-or-nothing" corruption models and revealed partial information about the secret by accumulating small leakage from all shares. A broad mathematical model for such side-channel attacks considers independent leakage from each share, i.e., local leakage.

Locally leakage-resilient secret sharing, introduced by Benhamouda et al. [BDIR18, BDIR21] and (also implicit in) Goyal & Kumar [GK18], is a security metric that ensures the statistical independence of the secret and the local leakage from the shares. Inspired by real-world side-channel attacks, Ishai et al. [ISW03] introduced the prominent physical bit probing model that locally leaks physical bits from memory storing the shares. Given the ubiquity of Shamir's secret sharing in privacy and cryptography technologies, it is natural to wonder:

How do we instantiate Shamir's secret sharing
to protect its secret against physical bit probes on the shares?

Maji, Nguyen, Paskin-Cherniavsky, Suad, and Wang [MNP$^+$21] proved that for large prime moduli and reconstruction threshold $\geqslant 2$, choosing the evaluation places for Shamir's secret sharing at random results in a locally leakage-resilient scheme secure against physical bit leakage with high probability. This work investigates the secret sharing over composite order fields, specifically large characteristic-2 fields used widely in practice.

Additional motivation. Our research contributes to NIST's recent standardization efforts for threshold cryptographic schemes [BP23]. The security of Shamir's secret sharing is critical to this effort due to its applications in distributed key generation (for private and public-key primitives) and as a gadget in other higher-level primitives like secure computation. Section 1.3 presents another motivation for the question investigated in this work from the perspective of side-channel attacks.

1.1 Basic Preliminaries

This section presents basic definitions to facilitate the presentation of our results. Consider Shamir's secret sharing among n parties with reconstruction threshold k. Let F be a finite field of order $q = p^d$, where $p \geqslant 2$ is a prime and $d \in \{1, 2, \dots\}$. Elements of F are stored as length-d vectors of F_p elements, each stored in their binary representation. The security parameter λ is the number of bits required to represent each share, i.e., $\lambda = d \cdot \lceil \log_2 p \rceil$. Shamir's secret sharing chooses a random F-polynomial $P(Z)$ of degree $< k$ such that $P(0) = s$, the secret. The shares are $s_i = P(X_i)$, for $i \in \{1, 2, \dots, n\}$, where $X_1, X_2, \dots, X_n \in F^*$ are distinct evaluation places.

For a secret $s \in F$, represent the leakage joint distribution by $\vec{\ell}(s)$, where $\vec{\ell}(\cdot)$ represents the leakage function. Following [BDIR18, BDIR21], the insecurity of a secret sharing against a leakage class $\mathcal{L}$ is

$$\max_{\vec{\ell} \in \mathcal{L}} \max_{s, s' \in F} \mathsf{SD}\left(\vec{\ell}(s)\ ,\ \vec{\ell}(s')\right). \tag{1}$$

Here, $\mathsf{SD}\left(\vec{\ell}(s)\ ,\ \vec{\ell}(s')\right)$ represents the statistical distance between the leakage distributions when the secrets are s and s'.

This work considers physical bit leakages introduced by [ISW03]. They leak arbitrary m_i physical bits from the i-th share, for $i \in \{1, 2, \dots, n\}$ and $m_i \in \{0, 1, \dots\}$. The total leakage $M = m_1 + m_2 + \cdots + m_n$ parameterizes our leakage class; this family of local leakages is represented by $\mathrm{PHYS}(M)$. This leakage class, in particular, allows the adversary to obtain the entire shares of a few parties and partial information from the remaining shares.[1]

1.2 Our Results

Result 1 (Randomized Construction for Composite Order Fields)**.** *Consider Shamir's secret sharing with evaluation places $X_1, X_2, \dots, X_n \in F^*$ chosen uniformly at random. Suppose the total leakage $m_1 + m_2 + \cdots + m_n \leqslant \rho \cdot (k-1) \cdot \lambda$, where*

$$\rho := \begin{cases} (1 - 1/p), & \text{for } 2 \leqslant p < (k-1), \\ 1, & \text{otherwise.} \end{cases}$$

With probability $1 - \mathsf{poly}(k)/\sqrt{q}$ over the choice of evaluation places, the resulting secret sharing has $\mathsf{poly}(k)/\sqrt{q}$ insecurity against physical bit leakages.

A randomness beacon [NIS] or coin-tossing protocol (depending on the application scenario) can generate public randomness to instantiate our randomized construction. In cryptographic applications, the number of parties n and the reconstruction threshold k are (at most) $\mathsf{poly}(\lambda)$ and, in several scenarios, constants as well. On the other hand, the order of the field F_q is exponential in the security parameter λ. Therefore, our result guarantees that the insecurity is exponentially

[1] Leakage-resilient secure computation considers adversaries that corrupt parties to obtain their shares and leak additional information from honest parties' shares.

small with probability exponentially close to 1. Section 1.4 presents the technical overview of our randomized construction.

Remark 1 (Clarification)**.** *The result above ignores a* $\mathsf{poly}\log(\lambda)$ *term for clarity of presentation. Corollary 2, Theorem 3, and Theorem 4 present the exact technical statement.*

Comparison with the result over prime fields. For prime fields (i.e., $q = p$), Maji, Nguyen, Paskin-Cherniavsky, Suad, Wang [MNP+21] proved that randomly choosing evaluation places results in a secure scheme as long as the total physical bit leakage $m_1 + m_2 + \ldots + m_n$ is less than the total entropy in the secret shares of the secret 0, which is (roughly) $(k-1) \cdot \lambda$. In our result, the permissible leakage tolerance may be slightly smaller for composite order fields, depending on the field characteristic. When $p \geqslant (k-1)$, our tolerance coincides with theirs. For small characteristic fields $2 \leqslant p < (k-1)$, our tolerance is $(1 - 1/p)$ times smaller.

Ideally, it is desirable to derandomize such randomized constructions because adversarially set randomness can make the scheme insecure, unbeknownst to the honest parties. Even for a fixed leakage $\vec{\ell}$, non-trivial techniques to estimate the insecurity expression in Equation 1 are unknown. We derandomize our randomized construction for $k = 2$ against single *block-leakage* per share. Recall that the $x \in F_q$ is represented as a length-d vector of F_p elements. The adversary can leak one F_p element from this vector representation of x. Single block leakage can simulate multiple physical bit leakages from the same block of the share.

Result 2. *Against single block leakage from each share, Shamir's secret sharing is either perfectly secure or completely insecure. Given evaluation places* $X_1, X_2, \ldots, X_n$ *as input, our algorithm (Figure 1) correctly classifies them as secure or not.*

The leakage distribution is independent of the secret in a perfectly secure secret sharing. A completely insecure secret sharing has two secrets the leakage can always distinguish. We also identify a block leakage attack if the evaluation places are insecure. Evaluation places satisfy a dichotomy; they are either perfectly secure or completely insecure – there is no "partial" insecurity. We prove that at least $1 - d^n p^{n-1}/q$ fraction of the evaluation places are secure, which is close to 1 for n close to d. The run-time of our algorithm is $d^n \mathsf{poly}(\lambda)$, which may be inefficient for large n. However, avoiding this factor seems challenging because there are d^n different block leakage attacks, and our algorithm outputs the leakage attack when evaluation places are vulnerable. Section 1.5 presents the technical overview of our derandomization result.

Remark 2 (A Comparison)**.** *[MNPY23] considers similar derandomization problems over Mersenne prime fields, one physical bit leakage per share, and they derandomized the construction of [MNP+21] for* $(n, k) \in \{\ (2,2)\ ,\ (3,2)\ \}$*. On the other hand, our derandomization result considers arbitrary composite order fields, all* $n \geqslant k = 2$*, and single block leakage per share.*

1.3 Prior Related Works

Physical bit probing attacks. Motivated by attacks on cryptosystems, Ishai et al. [ISW03] introduced a powerful leakage model that *probes physical bits* in the memory storing the shares. On the *additive secret-sharing* scheme over prime fields F_p among n parties, Maji et al. [MNP+21] introduced a local attack that leaks the parity of each share by probing their least significant bit (namely, the parity-of-the-parities attacker). This attack can distinguish two secrets with $(2/\pi)^n \approx (0.63)^n$ advantage [MNP+21, AMN+21, MNP+22] for any prime p. Thus, additive secret sharing is vulnerable when the number of shares is small. Furthermore, the distinguishing advantage of the attack increases as the order p of the prime field decreases. In particular, over F_2, this leakage can always distinguish secrets 0 and 1, irrespective of the number of parties.

Shamir's secret sharing inherits these vulnerabilities if its evaluation places are carelessly chosen [MNP+21, CS21]. Over composite order fields, the threat of these attacks is determined by the field's characteristic – the smaller the characteristic, the more devastating the attack. For example, over characteristic-2 fields, the parity-of-the-parities attacker can distinguish the secret $0, 1 \in F_{2^d}$ with certainty, where $d \in \{1, 2, \dots\}$.

The set of these specific vulnerable evaluation places is known to have an exponentially small density in the set of all possible evaluation places.

Given this background, it is natural to wonder: *Are there additional vulnerable evaluation places? What is the density of the set of all vulnerable evaluation places against physical bit probing attacks? Can we identify the vulnerable evaluation places?* Our work proves that the density of these vulnerable evaluation places is exponentially small, even when allowing multiple probes per share. We also characterize all vulnerable evaluation places for a few parameter choices.

Other related works. A large body of works constructs non-linear leakage-resilient secret-sharing schemes [BPRW16, ADN+19, SV19, BS19, KMS19, BIS19, FY19, FY20, HVW20, CGG+20, MSV20, CKOS22]. Benhamouda et al. [BDIR18] initiated the investigation of the security of additive and Shamir's secret sharing against local leakage attacks. A sequence of works considers arbitrary single-bit local leakage from each share of Shamir's secret sharing. Against such schemes, when the ratio of the reconstruction threshold to the number of parties is $\geqslant 0.69$, the secret sharing is secure for all evaluation places [BDIR18, BDIR21, MPSW21, MNPW22, KK23]. However, such schemes *cannot facilitate secure multiplication*, which requires the ratio to be < 0.5. The scope of our work includes small reconstruction thresholds, for example, $k \geqslant 2$, and many parties. So, our results lead to leakage-resilient secure multiplication of secrets against physical bit probes.

Codeword repairing – an antithetical objective. Guruswami and Wootters [GW16, GW17] introduced repairing Reed-Solomon codewords. There is a vast literature on this topic [DGW+10, ERR10, GERCP13, GFV17, PDC13, TWB12, WTB16, RSK11, YB17a, YB17b, CT22]; refer to [CT22, Section 6] for the applicability of these results to the security of Shamir's secret sharing. These repairing algorithms reconstruct the entire secret using small leakage per share, a strongly antithetical objective to leakage resilience. Leakage resilience insists that leakage from the shares reveals no statistically significant information about the secret, not just ruling out the possibility of reconstructing the entire secret. Nielsen and Simkin [NS20] demonstrated such attacks that reconstruct the secret with some probability. Unsurprisingly, leakage resilience has been significantly challenging to achieve.

1.4 Technical Overview: Randomized Construction

We will prove that Shamir's secret sharing is leakage-resilient against physical probes for most evaluation places $\vec{X} = (X_1, X_2, \dots, X_n)$. We illustrate the technical ideas using $m = 1$, i.e., a single physical bit probe per share. The extension of the analysis for the general case is included at the end of this section. Our analysis will follow the blueprint of [MNP+21], and this section follows their technical overview outline. It highlights the primary differences along the way.

Reduction 1. Fix two secrets $s.s' \in F$. We prove the following two bounds. By now, standard Fourier-analytic techniques in the literature [BDIR18, MNP+21] upper bound the statistical distance of the leakage as follows (see Proposition 3),

$$\mathsf{SD}\left(\vec{\ell}(s)\ ,\ \ell(\vec{s'})\right) \leqslant \sum_{\vec{t}\in\{0,1\}^n} \sum_{\vec{\alpha}\in C_{\vec{X}}^{\perp}\setminus\{\vec{0}\}} \left(\prod_{i=1}^{n}\left|\widehat{\mathbb{1}_{t_i}}(\alpha_i)\right|\right),$$

where $\mathbb{1}_{t_i}$ is the indicator of the set $\{x \in F : \ell_i(x) = t_i\}$, $C_{\vec{X}}$ is the generalized Reed-Solomon code and is the set of all possible secret shares of secret 0 in Shamir's scheme with evaluation places $\vec{X}$, and $C_{\vec{X}}^{\perp}$ is the dual code of $C_{\vec{X}}$.

Next, we prove that this upper bound is small in expectation over randomly chosen evaluation places $\vec{X} \in (F^*)^n$ (Lemma 8). That is,

$$\mathbb{E}_{\vec{X}}\left[\sum_{\vec{t}\in\{0,1\}^n} \sum_{\vec{\alpha}\in C_{\vec{X}}^{\perp}\setminus\{\vec{0}\}} \left(\prod_{i=1}^{n}\left|\widehat{\mathbb{1}_{t_i}}(\alpha_i)\right|\right)\right] \leqslant \exp(-\Theta(\lambda)).$$

This upper bound is sufficient for our objective. We use a union bound over all possible leakage functions in the family to conclude that most evaluation places result in a locally leakage-resilient Shamir's secret sharing. Next, a Markov inequality leads to the conclusion that nearly all evaluation places are leakage-resilient, except an exponentially small fraction.

Remark 3. *These two steps in our analysis are identical to those in [MNP+21]. The difference is that we use Fourier analysis over composite order fields. The result above relies on the Poisson summation formula, which extends to composite order fields (refer to Proposition 5).*

Reduction 2. We use Fourier analysis over composite order fields to establish the second bound mentioned above. The left-hand side of the inequality is rewritten as

$$\sum_{\vec{t}\in\{0,1\}^n} \sum_{\vec{\alpha}\in F^n\setminus\{0\}} \left(\prod_{i=1}^{n}\left|\widehat{\mathbb{1}_{t_i}}(\alpha_i)\right|\right) \cdot \Pr_{\vec{X}}\left[\vec{\alpha} \in C_{\vec{X}}^{\perp}\right]$$

Section 5 reduces this estimation to the following two subproblems.

Subproblem 1: Our aim is to upper-bound the probability that a vector $\vec{\alpha}$ belongs to the dual code $C_{\vec{X}}^{\perp}$. Estimating this probability is equivalent to counting the simultaneous zeroes of the equation below.

$$\begin{pmatrix} X_1 & X_2 & \cdots & X_n \\ X_1^2 & X_2^2 & \cdots & X_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ X_1^{k-1} & X_2^{k-1} & \cdots & X_n^{k-1} \end{pmatrix} \cdot \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Our objective is to count the number of $\vec{X} \in (F^*)^n$ satisfying the equation above such that $X_1, X_2, \ldots, X_n$ are distinct.

We rely on a contemporary Bézout-like theorem, particularly a form with an easy-to-verify analytic test (refer to Imported Theorem 1), to claim that the number of solutions is bounded. [MNP+21] used [Woo96]'s result for prime fields; we use [BSVX21]'s very recent result for composite order fields. There are further nuances when working over composite order fields highlighted below. Consider the following cases:

1. If $p \geqslant k$, then we fix $(n-k+1)$ variables to reduce the above equation to a square system of polynomials with $(k-1)$ variables and $(k-1)$ polynomials. By Imported Theorem 1, there will be at most $(k-1)!$ solutions. Consequently, overall, the number of solutions $\vec{X} \in (F^*)^n$ is at most $(k-1)! \cdot p^{n-k+1}$ (Lemma 1).

2. If $p = 2$, we have to do a more subtle analysis, reducing the equation to a square system with $k/2$ variables and $k/2$ polynomials. The subtlety arises because we cannot use even powers in our system of equations, a concern similar to Example 1 in Section 1.6. Instead, we will use equations with odd powers, cutting the size of the system of equations to (roughly) $k/2$, down from $(k-1)$. Like the previous case, the number of solutions is at most $(k-1)! \cdot p^{n-k/2}$ (Lemma 2).

3. If $3 \leqslant p < k$, we prove the result for $p = (k-1)$ or $p = k-2$ explicitly (Lemma 4). We can also write the solution in general with roughly $2k^2/(q-1)$ density of roots (Lemma 3).

Section 1.6 elaborates on this aspect of our technical analysis.

Subproblem 2: After problem 1 is solved, we bound the ℓ_1-Fourier norm of the physical bit leakage function (Section 4). That is, for every $t_i \in \{0, 1\}$, the objective is to upper bound

$$\left\| \widehat{\mathbb{1}_{t_i}} \right\|_1 := \sum_{\alpha_i \in F} \left| \widehat{\mathbb{1}_{t_i}(\alpha_i)} \right|$$

Our proof heavily relies on the composite order field F having subgroups (subspaces). We show that ℓ_1-Fourier norm of a one-bit physical leakage function over F is (less than or) equal to that over the base (prime) field F_p. Then, we apply the bound for ℓ_1-Fourier norm of physical leakage over the prime field in [MNP+21] when $p > 2$. Using a different analysis, we provide a stronger bound when $p = 2$. See Section 4 for details.

Resolving the two problems above completes the proof of Theorem 1.

Extension to multiple-bit leakage. Suppose that the adversary leaks m_i bits from the i-th share. We employ the approach in [MNP+21] to prove the result. Consider secret sharing, where the i-th share is repeated m_i times. The leakage distribution induced by the m_i-bit physical leakage on Shamir's scheme is identical to that induced by the one-bit physical leakage on the new scheme with repeated shares. Then, the technical analysis proceeds analogously to the presentation above. Theorem 2 summarizes this result.

1.5 Technical Overview: Derandomization

Consider $n = 2$ parties and reconstruction threshold $k = 2$. Consider Shamir's secret sharing over F_q, where $q = p^d$ and $d \in \{2, 3, \dots\}$. To begin, suppose the evaluation places are $(X_1, X_2) \in (F_q)^n$.

Interpret $F_q \cong F_p[\zeta]/\Pi(\zeta)$, where $\Pi(\zeta)$ is an irreducible F_p-polynomial with degree d. Represent elements of F_q as a length-d vector of F_p elements. An element $x \in F_q$ that is the polynomial $x_0 + x_1\zeta + \cdots + x_{d-1}\zeta^{d-1}$ is represented as the vector $(x_0, x_1, \dots, x_{d-1}) \in F_p^d$. This section considers *single block leakage* – leaking the i-th block of $x \in F_q$ reveals $x_i \in F_p$, where $i \in \{0, 1, \dots, d-1\}$. *Our objective is to determine whether Shamir's secret sharing (with the specific evaluation places) is secure against single block leakage from each share.*

Consider a secret $s \in F_q$. The polynomial to generate its shares is $P(Z) = s + P_1 \cdot Z$, where $P_1 \in F_p$ is chosen uniformly at random. The two shares are

$$(\ s + P_1 X_1\ ,\ s + P_1 X_2\ ).$$

Consider arbitrary $i,j \in \{0,1,\ldots,d-1\}$ and the leakage function that leaks the first share's i-th block and the second share's j-th block. So, the leakage joint distribution is:

$$\Big(\ (s+P_1X_1)_i \ , \ (s+P_1X_2)_j \ \Big).$$

By a change of random variable, this distribution is identical to

$$\Big(\ (Q)_i \ , \ (Q\cdot(X_2X_1^{-1})+s')_j \ \Big),$$

where $s' = s\cdot\left(1 - X_2X_1^{-1}\right)$, an F_q linear automorphism and $Q \in F_q$ is chosen uniformly at random.

We prove a technical result (Proposition 4) similar to the proof strategy of [MNPY23]: There is $\eta^{(i)} \in F_q$ such that $(x)_i = \left(x\cdot\eta^{(i)}\right)_0$, for all $x \in F_q$ and $i \in \{0,1,\ldots,d-1\}$. Therefore, the leakage is identical to

$$\Big(\ \Big(Q\cdot\eta^{(i)}\Big)_0 \ , \ \Big(Q\cdot(X_2X_1^{-1})\cdot\eta^{(j)}+s''\Big)_0 \ \Big),$$

where $s \mapsto s''$ is a linear automorphism over F_q. Next, by renaming the random variables, the leakage distribution is:

$$\Big(\ (R)_0 \ , \ \Big(R\cdot(X_2X_1^{-1})\cdot\Big(\eta^{(j)}{\eta^{(i)}}^{-1}\Big)+s''\Big)_0 \ \Big).$$

To conclude, the leakage joint distribution is

$$\big(\ R_0 \ , \ \left(R\cdot\beta(i,j)+s''\right)_0 \ \big),$$

where $\beta(i,j) := X_2X_1^{-1}\cdot\eta^{(j)}(\eta^{(i)})^{-1}$.

Fix the leakage $r_0 := R_0 \in F_p$. Define $V = \{x \in F_q : \ x_0 = 0\}$. We know that R is a uniformly random sample from the set $V + r_0 \subseteq F_q$. We will present a technical result (Lemma 9) proving the following: For any $\beta \in F_q \setminus F_p$, for x sampled uniformly at random from $V+q_0$, the distribution $(x\cdot\beta)_0$ is uniformly at random over F_p.[2]

Using this result, we conclude that the distribution $(R\cdot\beta(i,j)+s''')_0$ is uniformly at random over F_p, conditioned on the leakage from the first share being q_0. Therefore, the leakage is uniformly distributed over $(F_p)^2$, irrespective of the secret s, as long as

$$\beta(i,j) := X_2X_1^{-1}\cdot\eta^{(i)}(\eta^{(j)})^{-1} \in F_q \setminus F_p.$$

So, Shamir's secret sharing with evaluation places (X_1,X_2) is perfectly secure against block leakage if the above condition holds for all $i,j \in \{0,1,\ldots,d-1\}$.

Furthermore, this characterization is tight. When $\beta(i,j) \in F_p$, then two appropriate secrets can always be distinguished. Without loss of generality, consider $i=j=0$ and $X_2 = c\cdot X_1$, for some $c \in F_p$. For secret $s=0$, the identity $c\cdot(s_1)_0+(s_2)_0 = 0$ will be satisfied, where s_1,s_2 are the two shares. For secret $s=1$, this identity will never be satisfied.

Based on this analysis, the following algorithm tests the security of evaluation places (X_1,X_2):

1. Initialize the bad set $B = \emptyset$.
2. For each $i,j \in \{0,1,\ldots,d-1\}$: Update $B \longleftarrow B \bigcup F_p\cdot(\eta^{(i)})^{-1}\eta^{(j)}$.
3. If $\alpha_2\alpha_1^{-1} \notin B$: return "Secure;" else, return "Insecure."

[2] Looking ahead, we will prove a significantly stronger generalization of Lemma 9 for arbitrary number of parties.

This proves that at least $1 - d^2p/q$ fraction of evaluation places are secure.

Extension to Larger Number n of Parties. Consider Shamir's secret sharing for n parties and reconstruction threshold $k = 2$. The evaluation places are $X_1, X_2, \dots, X_n \in F^*$ and the shares are $s_1, s_2, \dots, s_n$. Consider leaking blocks $i_1, i_2, \dots, i_n$ from shares $s_1, s_2, \dots, s_n$, respectively, where $i_1, i_2, \dots, i_n \in \{0, 1, \dots, d-1\}$. The joint leakage distribution is:

$$\Big((s_1)_{i_1} \,,\ (s_2)_{i_2} \,, \dots,\ (s_n)_{i_n} \Big),$$

where $s_i = s + P_1 \cdot X_i$, for $i \in \{1, 2, \dots, n\}$ and uniformly at random $P_1 \in F_q$.

Similar to the analysis for $(n, k) = (2, 2)$ above, the previous distribution is identical to the leakage distribution:

$$\Big(\left(QX_1\eta^{(i_1)}\right)_0 \,,\ \left(QX_2\eta^{(i_2)}\right)_0 + t_2 \,, \dots,\ \left(QX_n\eta^{(i_n)}\right)_0 + t_n \Big),$$

where $s \mapsto t_j$ are appropriate linear automorphisms over F_q, for all $j \in \{2, 3, \dots, n\}$ and uniformly at random $Q \in F_q$. Similar to the approach before, our objective is to show that the evaluation places $X_1, X_2, \dots, X_n$ are secure if (and only if) the following elements

$$X_1\eta^{(i_1)}, X_2\eta^{(i_2)}, \dots, X_n\eta^{(i_n)} \in F_q$$

are all F_p-linearly independent.

If some of these elements are linearly dependent over F_p, then the leakages also satisfy the same linear dependence when the secret $s = 0$. For $s = 1$, this particular linear dependence will not hold. We prove a technical result (Lemma 10) showing that if these elements above are linearly independent, then the distribution

$$\Big(\left(QX_1\eta^{(i_1)}\right)_0 \,,\ \left(QX_2\eta^{(i_2)}\right)_0 \,, \dots,\ \left(QX_n\eta^{(i_n)}\right)_0 \Big)$$

is identical to the uniform distribution over $(F_p)^n$ for uniformly random $Q \in F_q$. From this fact, it is clear that the leakage distribution is also uniformly random over $(F_p)^n$. So, the secret sharing is perfectly secure against this particular leakage.

Building on this, we have the following algorithm to test the security of evaluation places $X_1, X_2, \dots, X_n$:

1. For each $i_1, i_2, \dots, i_n \in \{0, 1, \dots, d-1\}$: If the set $\left\{X_1\eta^{(i_1)}, X_2\eta^{(i_2)}, \dots, X_n\eta^{(i_n)}\right\} \subseteq F_q$ is *not* F_p-linearly independent, return "Insecure."
2. Return "Secure."

This algorithm demonstrates that (roughly) at least $1 - d^n p^{n-1}/q$ fraction of the evaluation places are secure. This fraction is $1 - \mathrm{o}(1)$ for $d = \lambda - \mathrm{o}(\lambda)$. The running time of our algorithm is $d^n \mathsf{poly}(\lambda)$, which may be inefficient for large n.

1.6 Discussion: Jacobian Test & the Number of Isolated Zeroes

Overview. Generally speaking, there are two types of "bad" cases for our randomized construction: (1) zeroes of a Jacobian and (2) (isolated) zeroes of a system of polynomial equations. The zeroes of the Jacobian are due to "redundancies" in the system of equations; for example, two evaluation places being identical. For prime fields, this was the only form of badness it captured.

For composite order fields, there are additional such bad cases; worked-out examples below will illustrate them. However, the density of the set of these zeroes is $\mathsf{poly}(k)/q$, an exponentially small number. Outside the Jacobian's zeroes, the (isolated) zeroes of the system of polynomial equations (specifically corresponding to a generalized Vandermonde matrix being rank deficient) are the "Bézout-like" zeroes. Their number is upper-bounded by $k!$ (the product of degree), and their density is $k!/q^k \ll k/q$, exponentially small as well.

The Details. This section closely follows the notation and presentation in [BSVX21], which we felt was more approachable. Let $f_j \in F[X_1, X_2, \dots, X_k]$ be a polynomial of degree $d_j \in \{1, 2, \dots\}$, where $j \in \{1, 2, \dots, k\}$ and F is an arbitrary finite field. The objective is to count the simultaneous zeroes of $f_j = 0$ for all $j \in \{1, 2, \dots, k\}$. We represent the system as $\mathbf{f} = 0$ for brevity. We define the corresponding Jacobian as the determinant below:

$$J(\mathbf{f}) := \det\left(\frac{\partial f_j}{\partial X_i}\right)_{i,j\in\{1,2,\dots,k\}} \in F[X_1, X_2, \dots, X_k].$$

For $\mathbf{a} \in F^k$, $\mathbf{f}(\mathbf{a})$ represents the evaluation of the system of polynomials at $\mathbf{a}$, and $J(\mathbf{f}; \mathbf{a})$ represents the evaluation of the Jacobian $J(\mathbf{f})$ at $\mathbf{a}$.

Definition 1 (Isolated Zero)**.** *An* $\mathbf{a} \in F^k$ *is an* isolated zero *of the system* $\mathbf{f} = 0$*, if* $\mathbf{f}(\mathbf{a}) = 0$ *but* $J(\mathbf{f}; \mathbf{a}) \neq 0$*.*

Counting all the zeroes of $\mathbf{f} = 0$ is challenging. However, [BSVX21] presents a bound for the number of *isolated zeroes* of a system of polynomial equations.

Imported Result 1 (Corollary 1.3 in [BSVX21])**.** *Let* $\mathcal{N}(\mathbf{f})$ *represent the number of isolated zeroes of the system of equations* $\mathbf{f} = 0$*, then* $\mathcal{N}(\mathbf{f}) \leqslant d_1 \cdot d_2 \cdots d_k$*.*

Wooley [Woo96] proved this result for prime fields F, and Maji et al. [MNP$^+$21] used Wooley's result to prove the leakage resilience of Shamir's secret sharing over prime fields. Zhao [Zha12] extended Wooley's result to arbitrary finite fields, and Bafna et al. [BSVX21] present an elementary proof for this result (and fill some missing gaps in the proof of [Zha12]).

Our high-level strategy for using this imported result is the following. We will pick random $\mathbf{a} \in F^k$ and hope that only a few of them will satisfy $J(\mathbf{f}; \mathbf{a}) = 0$ or $\mathbf{f}(\mathbf{a}) = 0$. For the remaining $\mathbf{a}$ (whose density will be close to 1), our analysis will show that they correspond to "secure Shamir's scheme."

Worked-out examples. Example 1. Let F be a finite field of characteristic 2. Consider the system of equations $f_1 = X_1 + X_2 = 0$ and $f_2 = X_1^2 + X_2^2 = 0$, where $k = 2$. Note that the Jacobian of this system of equations is

$$J(\mathbf{f}) = \det\begin{pmatrix} 1 & 2 \cdot X_1 \\ 1 & 2 \cdot X_2 \end{pmatrix} = 0,$$

for all $(X_1, X_2) \in F^k$, because F has characteristic 2 and $2 \cdot X = 0$ for any $X \in F$. Since the Jacobian is (identical to) the 0 polynomial, there are no isolated zeroes.

Example 2. Let F be a finite field of characteristic 2. Consider the system of equations $f_1 = X_1 + X_2 = 0$ and $f_2 = X_1^3 + X_2^3 = 0$, where $k = 2$. Note that the Jacobian of this system of equations is

$$J(\mathbf{f}) = \det\begin{pmatrix} 1 & 3 \cdot X_1^2 \\ 1 & 3 \cdot X_2^2 \end{pmatrix} = 3 \cdot (X_1^2 - X_2^2).$$

Note that (for a characteristic 2 field F) the Jacobian $J(\mathbf{f};\mathbf{a}) \neq 0$ if (and only if) a_1, a_2 are distinct. So, among all $\mathbf{a} \in F^k$, the number of isolated solution (i.e., where $J(\mathbf{f};\mathbf{a}) \neq 0$) is at most $d_1 \cdot d_2 = 1 \cdot 3 = 3$.

Example 3. Let F be a finite field of characteristic 3. Consider the system of equations $f_1 = X_1 + X_2 + X_3 = 0$, $f_2 = X_1^2 + X_2^2 + X_3^2 = 0$, and $f_3 = X_1^4 + X_2^4 + X_3^4 = 0$, where $k = 3$. The Jacobian is

$$J(\mathbf{f}) = \det \begin{pmatrix} 1 & 2 \cdot X_1 & 4 \cdot X_1^3 \\ 1 & 2 \cdot X_2 & 4 \cdot X_2^3 \\ 1 & 2 \cdot X_3 & 4 \cdot X_3^3 \end{pmatrix} = 8 \cdot (X_1 - X_2)(X_2 - X_3)(X_3 - X_1) \cdot (X_1 + X_2 + X_3)\,.$$

Note that $J(\mathbf{f};\mathbf{a}) = 0$ if (and only if)

1. a_1, a_2, a_3 are not distinct, or

2. $a_1 + a_2 + a_3 = 0$.

This example highlights that the Jacobian can also be 0 in many new and unexpected ways over composite order fields. Such determinants are referred to as *generalized Vandermonde* determinants, and identifying their zeroes is an open research problem in mathematics. When the Jacobian is not zero, there are at most $d_1 \cdot d_2 \cdot d_3 = 8$ values of $\mathbf{a} \in F^k$ such that $\mathbf{f}(\mathbf{a}) = 0$.

Example 4. A more typical example will be the following. Suppose F is a finite field of characteristic $p > k$. For $j \in \{1, 2, \ldots, k\}$, consider the equation $f_j = \sum_{i=1}^{k} X_i^j = 0$. In this case, the Jacobian is the standard Vandermonde matrix

$$J(\mathbf{f}) = \det \left(j X_i^{j-1} \right)_{i,j \in \{1,2,\ldots,k\}} = k! \cdot \prod_{1 \leqslant i < j \leqslant k} (X_i - X_j)\,.$$

The Jacobian is 0 if (and only if) $X_1, X_2, \ldots, X_k$ are not all distinct. When, $X_1, X_2, \ldots, X_k$ are all distinct, then $\mathbf{f}(\mathbf{a}) = 0$ has at most $d_1 \cdot d_2 \cdots d_k = k!$ isolated zeroes.

1.7 Open Problems

The technical connections established by our work pose natural open problems in diverse research areas.

1. Our work motivates estimating the number of simultaneous zeroes of generalized Vandermonde-type systems of polynomial equations (irrespective of whether they are isolated or not).

2. Clearly, the derandomization problem for general (n, k) parameters and leakage families is an immediate open problem.

2 Preliminaries

We always use F to denote a finite field of order p^d for some prime p and positive integer d. The set $F[X_1, X_2, \ldots, X_n]$ denotes the set of all multivariate polynomials on $X_1, X_2, \ldots, X_n$ whose coefficients are in F. We use bold letters $\vec{X}, \vec{\ell}, \vec{\alpha}, \ldots$ to denote vectors whose length will be apparent in the context. For example, $\vec{X}$ usually denotes the vector $(X_1, X_2, \ldots, X_n)$ of length n.

For any set S, we use U_S to denote the uniform distribution over the set S. The $\mathbb{1}_S$ represents its indicator function.

Statistical Distance. For any two distributions P and Q over a countable sample space, the statistical distance between the two distributions, represented by $\mathsf{SD}(P,Q)$, is defined as

$$\frac{1}{2}\sum_{x}|\Pr[P=x]-\Pr[Q=x]|.$$

We shall use $f(\lambda)\sim g(\lambda)$ if $f(\lambda)=(1+\mathrm{o}(1))\,g(\lambda)$. Additionally, we write $f(\lambda)\lesssim g(\lambda)$ if $f(\lambda)\leqslant(1+\mathrm{o}(1))\,g(\lambda)$.

2.1 Secret Sharing Schemes

Definition 2 ($(n,k,\vec{X})_F$-Shamir Secret Sharing)**.** *Let F be a finite field and n,k be positive integers such that $k\leqslant n$. Let $\vec{X}=(X_1,X_2,\ldots,X_n)\in(F^*)^n$ be n distinct evaluation places. The corresponding $(n,k,\vec{X})_F$-Shamir secret sharing, denoted as $\mathsf{ShamirSS}(n,k,\vec{X})_F$, is defined as follows.*

1. *Sharing phase: For any secret $s\in F$, $\mathsf{Share}^{\vec{X}}(s)$ randomly picks a F-polynomial $P(z)$ of degree strictly less than k such that $P(0)=s$. The shares are $s_i=P(X_i)$ for $i\in\{1,2,\ldots,n\}$.*
2. *Reconstruction phase: Given any $s_{i_1},s_{i_2},\ldots,s_{i_t}$ shares for some $t\geqslant k$, the reconstruction algorithm $\mathsf{Rec}^{\vec{X}}$ interpolates to obtain the unique polynomial $f\in F[X]/X^k$ satisfying $f(X_{i_j})=s_{i_j}$ for every $1\leqslant j\leqslant t$, and outputs $f(0)$ to be the reconstructed secret.*

2.2 Physical-bit Leakages and Leakage-resilient Secret Sharing

Every element $x=x_0+x_1\zeta+\cdots+x_{d-1}\zeta^{d-1}\in F$ is equivalently represented as $\vec{x}=(x_0,x_1,\ldots,x_{d-1})$. Effectively, each element of F is stored as a length-d vector of F_p elements, each stored as $\lceil\log_2 p\rceil$-bit in their binary representation. The security parameter $\lambda=d\lceil\log_2 p\rceil$ is the number of bits for each element in F. For example, in the finite field F_{5^2} with 25 elements, $\lambda=6$, the element 3 is stored as (011, 000), and the element $1+4\zeta$ is stored as $(001,100)$.

Definition 3. *An m-bit physical leakage function $\vec{\ell}=(\ell_1,\ell_2,\ldots,\ell_n)$ on $(n,k,\vec{X})_F$-Shamir secret sharing leaks m physical bits from every share locally, where each $\ell_i\colon F\to\{0,1\}^m$ for $1\leqslant i\leqslant n$. For a secret $s\in F$, the joint leakage distribution, denoted as $\vec{\ell}(s)$, is defined as the following experiment.*

1. *Sample $(s_1,s_2,\ldots,s_n)\leftarrow\mathsf{Share}^{\vec{X}}(s)$,*
2. *Output $(\ell_1(s_1),\ell_2(s_2),\ldots,\ell_n(s_n))$.*

Definition 4 ($(\vec{m},\varepsilon)_F$-LLRSS)**.** *Let $\vec{m}=(m_1,m_2,\ldots,m_n)$. An $(n,k,\vec{X})_F$-Shamir secret sharing scheme is an $(\vec{m},\varepsilon)$-local-leakage-resilient secret sharing scheme against $\vec{m}$ physical-bit leakage (represented as $(\vec{m},\varepsilon)_F$-LLRSS), if it provides the following guarantee. For any two secrets $s,s'\in F$ and any $\vec{m}$-bit physical leakage function $\vec{\ell}=(\ell_1,\ell_2,\ldots,\ell_n)$, where $\ell_i\colon F\to\{0,1\}^{m_i}$ for $1\leqslant i\leqslant n$, it holds that*

$$\mathsf{SD}\left(\vec{\ell}(s)\ ,\ \vec{\ell}(s')\right)\leqslant\varepsilon.$$

2.3 Generalized Reed-Solomon Codes and Vandermonde Matrices

Definition 5 ($(n, k, \vec{X}, \vec{\alpha})_F$-GRS)**.** *A* generalized Reed-Solomon code *over a finite field F with message length k and block length n consists of an encoding function* $\mathsf{Enc}\colon F^k \to F^n$ *and decoding function* $\mathsf{Dec}\colon F^n \to F^k$*. It is specified by the* evaluation places $\vec{X} = (X_1, \ldots, X_n) \in (F^*)^n$ *such that X_i's are all distinct, and a* scaling vector $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n) \in (F^*)^n$*. Given $\vec{X}$ and $\vec{\alpha}$, the* encoding function *is defined as*

$$\mathsf{Enc}(m_1, \ldots, m_k) := (\alpha_1 \cdot f(X_1), \ldots, \alpha_n \cdot f(X_n)),$$

where $f(X) := m_1 + m_2 X + \cdots + m_k X^{k-1}$.

In particular, the generator matrix of the linear $(n, k, \vec{X}, \vec{\alpha})_F$-GRS code is the matrix

$$\begin{pmatrix} \alpha_1 \cdot 1 & \alpha_2 \cdot 1 & \cdots & \alpha_n \cdot 1 \\ \alpha_1 \cdot X_1 & \alpha_2 \cdot X_2 & \cdots & \alpha_n \cdot X_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1 \cdot X_1^{k-1} & \alpha_2 \cdot X_2^{k-1} & \cdots & \alpha_n \cdot X_n^{k-1} \end{pmatrix}.$$

We denote $C_{\vec{X}}$ as the set of all possible secret shares of secret 0 for $(n, k, \vec{X})_F$-Shamir secret sharing. The following fact will be useful.

Fact 1. *The set $C_{\vec{X}}$ is a $(n, k-1, \vec{X}, \vec{X})_F$-GRS code.*

Definition 6 (Generalized Vandermonde Matrix)**.** *A generalized Vandermonde matrix over a finite field F is an $n \times n$ matrix of the form*

$$V_n(\vec{\mu}) = \begin{pmatrix} x_1^{\mu_1} & x_1^{\mu_2} & \cdots & x_1^{\mu_n} \\ x_2^{\mu_1} & x_2^{\mu_2} & \cdots & x_2^{\mu_n} \\ \vdots & \vdots & \ddots & \vdots \\ x_n^{\mu_1} & x_n^{\mu_2} & \cdots & x_n^{\mu_n} \end{pmatrix} = \left(x_i^{\mu_j}\right)_{i,j \in \{1,2,\ldots,n\}}.$$

where $x_i \in F$ and $\mu_i \in \{0, 1, 2, \ldots\}$. In particular, $V_n(0, 1, \ldots, n-1)$ is the classical Vandermonde matrix.

Observe that if μ_i's are not all distinct, then $\det V_n(\mu) = 0$. The following result is a well-known fact about the determinant of the Vandermonde matrix.

Fact 2. *It hold that* $\det V_n(0, 1, \ldots, n-1) = \prod_{1 \leqslant i < j \leqslant n} (x_i - x_j)$*.*

Note that $\det V_n(\vec{\mu})$ is divisible by $\det V_n(0, 1, \ldots, n-1)$ for any $\vec{\mu}$.

Fact 3. *It holds that* $\det V_n(\mu) = \det(V_n(0, 1, \ldots, n-1)) \cdot \Phi(x_1, x_2, \ldots, x_n)$*, where $\Phi(x_1, x_2, \ldots, x_n)$ is a symmetric multivariate polynomial in $x_1, x_2, \ldots, x_n$.*

Note that $\det V_n(\vec{\mu})$ can be computed efficiently in $\mathsf{poly}(n)$-time.[3]

2.4 Field Trace

Definition 7. *The trace of an extension field $F = F_{p^d}$ over a base field F_p is a mapping, denoted as Tr_{F/F_p}, from F to F_p such that $\mathsf{Tr}_{F/F_p}(y) := \sum_{i=0}^{d-1} y^{p^i}$.*

Proposition 1. *The trace $\mathsf{Tr}_{F/F_p}\colon F \to F_p$ is a linear map. That is, for every $a, b \in F_p$ and $x, y \in F$,*

$$\mathsf{Tr}_{F/F_p}(ax + by) = a\mathsf{Tr}_{F/F_p}(x) + b\mathsf{Tr}_{F/F_p}(y).$$

[3] First perform Gaussian elimination, and then the determinant is the product of the diagonal elements.

2.5 Fourier Analysis

We shall use Fourier analysis over the additive group of a finite field $F = F_{p^d}$ for some $d \in \{1, 2, \dots\}$. Let $q = p^d$. Define $\omega := \exp(2\pi\imath/p)$. Define the Fourier function $\widehat{f}\colon F \to \mathbb{C}$ as follows. For any $\alpha \in F$,

$$\widehat{f}(\alpha) = \frac{1}{q}\sum_{x\in F} f(x)\cdot\omega^{\mathsf{Tr}_{F/F_p}(\alpha\cdot x)}.$$

The value $\widehat{f}(\alpha)$ is called the *Fourier coefficient* of f at α. The ℓ_1-*Fourier norm* of f is defined as $\left\|\widehat{f}\right\|_1 := \sum_{\alpha\in F}\left|\widehat{f}(\alpha)\right|$.

Fact 4 (Fourier Inversion Formula)**.** $f(x) = \sum_{\alpha\in F}\widehat{f}(\alpha)\cdot\omega^{-\mathsf{Tr}_{F/F_p}(\alpha\cdot x)}$.

Fact 5 (Parseval's Identity)**.** $\frac{1}{q}\sum_{x\in F}|f(x)|^2 = \sum_{\alpha\in F}\left|\widehat{f}(\alpha)\right|^2$.

2.6 Counting Isolated Roots

Definition 8 (Degree, Derivative, Determinant, and Jacobian)**.**

1. *Let F be a fintie field. The* degree *of a monomial $X_1^{t_1}X_2^{t_2}\cdots X_n^{t_n}$ is $\sum_{i=1}^n t_i$. For a polynomial $f \in F[X_1, X_2, \dots, X_n]$, the degree of f is the largest degree of its monomial.*

2. *Let*
$$f = a_tX_i^t + a_{t-1}X_i^{t-1} + \cdots + a_1X_i + a_0,$$
where $a_0, \dots, a_t \in F[X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_n]$. Then, the derivative of f with respect to X_i *is the polynomial in $F[X_1, X_2, \dots, X_n]$ defined below.*
$$\frac{\partial f}{\partial X_i} := (t\cdot a_t)X_i^{t-1} + ((t-1)\cdot a_{t-1})X_i^{t-2} + \cdots + (2\cdot a_2)X_i + a_1.$$

3. *For a $k\times k$ matrix M with elements in $F[X_1, X_2, \dots, X_n]$, the* determinant *of M, denoted as* $\det(M)$*, is defined as follows.*
$$\det(M) := \sum_{\substack{\sigma\colon\{1,2,\dots,k\}\to\{1,2,\dots,k\}\\ \sigma \text{ is a permutation}}} \operatorname{sign}(\sigma)\cdot\prod_{i=1}^k M_{i,\sigma(i)},$$
where $\operatorname{sign}(\sigma)$ *represents the $\{+1,-1\}$ sign of the permutation σ.Note that* $\det(M) \in F[X_1, X_2, \dots, X_n]$.

4. *For a system of polynomials $\vec{f} = (f_1, \dots, f_k) \in (F[X_1, X_2, \dots, X_n])^k$, the* Jacobian *of $\vec{f}$ is defined as*
$$\mathbf{J}(\vec{f}) := \det\begin{pmatrix} \frac{\partial f_1}{\partial X_1} & \frac{\partial f_2}{\partial X_1} & \cdots & \frac{\partial f_k}{\partial X_1}\\ \frac{\partial f_1}{\partial X_2} & \frac{\partial f_2}{\partial X_2} & \cdots & \frac{\partial f_k}{\partial X_2}\\ \vdots & \vdots & \ddots & \vdots\\ \frac{\partial f_1}{\partial X_n} & \frac{\partial f_2}{\partial X_n} & \cdots & \frac{\partial f_k}{\partial X_n}\end{pmatrix}.$$
For $\vec{a} \in F^k$, we use $J(\vec{f};\vec{a})$ to denote the evaluation of $J(\vec{f})$ at $\vec{a}$.

Definition 9 (Isolated Roots)**.** *For a system of polynomials $\vec{f} = (f_1, f_2, \dots, f_k) \in (F[X_1, X_2, \dots, X_k])^k$, we say that $\vec{a} \in F^k$ is an* isolated root *of $\vec{f}$ if $f_i(a) = 0$ for every $i \in \{1, 2, \dots, k\}$ and* $\det(J(\vec{f};\vec{a})) \neq 0$*. Let $\mathcal{N}(\vec{f})$ denote the number of isolated roots of $\vec{f}$.*

Imported Theorem 1 (Bézout-like Theorem [BSVX21]). *Let $\vec{f} = (f_1, f_2, \ldots, f_k)$ be a system of polynomials in $F[X_1, X_2, \ldots, X_k]$ with $\deg(f_i) \leqslant d_i$ for every $i \in \{1, 2, \ldots, k\}$. Then $\mathcal{N}(f) \leqslant d_1 \cdot d_2 \cdots d_k$.*

3 Bounding the Number of Solutions of an Equation

This section presents one of our main technical results. An important step in proving the leakage-resilient Shamir's secret sharing is to upper bound the number of solutions of the equation $G_{\vec{X}} \cdot \vec{\alpha}^T = 0$ (refer to Problem 1 in Section 1.4), where $\vec{X} = (X_1, X_2, \ldots, X_n) \in (F^*)^n$ is randomly chosen such that they are all distinct, $\vec{\alpha} \in F^n$, and

$$G_{\vec{X}} = \begin{pmatrix} X_1 & X_2 & \cdots & X_n \\ X_1^2 & X_2^2 & \cdots & X_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ X_1^{k-1} & X_2^{k-1} & \cdots & X_n^{k-1} \end{pmatrix}.$$

Let $\mathcal{S}(G_{\vec{X}}, \vec{\alpha})_F$ denote the number of solutions of the above equation over the finite field F. The following subsections provide the bounds for different parameter settings.

3.1 Over Finite Fields with Large Characteristics

Lemma 1. *Let F be a finite field with characteristic $p \geqslant k$. It holds that*

$$\mathcal{S}(G_{\vec{X}}, \vec{\alpha})_F \leqslant (q-1)(q-2) \cdots (q-(n-k+1)) \cdot (k-1)!.$$

The proof of Lemma 1 follows closely to the proof of the prime field case in [MNP+21]. The key difference is that our proof employs the contemporary Bézout-like theorem [Zha12, BSVX21], while [MNP+21] used the result by Wooley [Woo96].

Proof. Observe that $G_{\vec{X}} \cdot \vec{\alpha}^T = \vec{0}$ implies that $\vec{\alpha} \in C_{\vec{X}}^{\perp}$, where $C_{\vec{X}}$ is the code containing all possible secret share of secret 0 of $(n, k, \vec{X})_F$-Shamir secret sharing. Note that $C_{\vec{X}}^{\perp}$ is an $(n, n-k+1, k)$-GRS. Thus, the codeword $\vec{\alpha}$ has at least k non-zero entries. Without loss of generality, assume $\alpha_i \neq 0$ for every $1 \leqslant i \leqslant k$. We rewrite the equation $G_{\vec{X}} \cdot \vec{\alpha}^T = \vec{0}$ as a system of polynomial equations with n variables and $(k-1)$ equations as follows.

$$f_i(X_1, X_2, \ldots, X_n) := \alpha_1 X_1^i + \alpha_2 X_2^i + \ldots + \alpha_n X_n^i = 0 \text{ for } i \in \{1, 2, \ldots, n\}$$

Observe that the above system is not a square system of polynomials. To make it a square system and apply Imported Theorem 1, we fix X_i to be distinct non-zero values in F for $i = k, k+1, \ldots, n$. Notice that there are $(q-1)(q-2) \cdots (q-(n-k+1))$ ways of doing the fixing. Define $c_i := \sum_{j=k}^{n} \alpha_j X_j^i$ for $i = 1, 2, \ldots, k-1$. The above system is now rewritten as, for $i \in \{1, 2, \ldots, k-1\}$,

$$g_i(X_1, X_2, \ldots, X_{k-1}) := \alpha_1 X_1^i + \alpha_2 X_2^i + \ldots + \alpha_{k-1} X_{k-1}^i + c_i = 0$$

Since $\alpha_i \neq 0$, it is a square polynomials system with $\deg(f_i) = i$ for every $1 \leqslant i \leqslant k-1$. Next, we shall show that

$$\mathbf{J}(g_1, g_2, \ldots, g_{k-1})(X_1, X_2, \ldots, X_{k-1}) \neq 0 \text{ if } X_i \neq X_j \text{ for every } i \neq j.$$

One can compute the Jacobian of the above system as follows.

$$
\begin{aligned}
&\mathbf{J}\left(g_1, g_2, \ldots, g_{k-1}\right)\left(X_1, X_2, \ldots, X_{k-1}\right) \\
&= \det \begin{pmatrix} \alpha_1 & 2\alpha_1 X_1 & \cdots & (k-1)\alpha_1 X_1^{k-2} \\ \alpha_2 & 2\alpha_2 X_2 & \cdots & (k-1)\alpha_2 X_2^{k-2} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{k-1} & 2\alpha_{k-1} X_{k-1} & \cdots & (k-1)\alpha_{k-1} X_{k-1}^{k-2} \end{pmatrix} \\
&= \left(\prod_{i=1}^{k-1} \alpha_i\right) \cdot (k-1)! \cdot \det \begin{pmatrix} 1 & X_1 & \cdots & X_1^{k-2} \\ 1 & X_2 & \cdots & X_2^{k-2} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & X_{k-1} & \cdots & X_{k-1}^{k-2} \end{pmatrix} \\
&= \left(\prod_{i=1}^{k-1} \alpha_i\right) \cdot (k-1)! \cdot \prod_{1 \leqslant i < j \leqslant k-1} (X_i - X_j) \qquad \text{(Fact 2)}
\end{aligned}
$$

We show that all three terms in the last equation are non-zero. The first term $\prod_{i=1}^{k-1} \alpha_i$ is non-zero since $\alpha_i \neq 0$ for every $1 \leqslant i \leqslant k-1$. Since $p \geqslant k$, it is clear that the second term $(k-1)! \neq 0 \mod p$. The third term is non-zero since X_i's are distinct. Thus, the determinant is non-zero. By Imported Theorem 1, $\mathcal{N}(f_1, f_2, \ldots, f_{k-1}) \leqslant (k-1)!$. Hence, the total number of solutions $\mathcal{S}(G_{\vec{X}}, \vec{\alpha})_F$ is at most $(q-1)(q-2)\cdots(q-(n-k+1)) \cdot (k-1)!$. □

3.2 Over Finite Fields with Characteristic Two

Lemma 2. *Let F be a finite field with characteristic two. It holds that*

$$\mathcal{S}(G_{\vec{X}}, \vec{\alpha})_F \leqslant (q-1)(q-2)\cdots(q-(n-\lfloor k/2 \rfloor)) \cdot (k-1)!.$$

Proof. If $k = 2$, then a similar proof as of Lemma 1 works since $(k-1)! = 1$ is not divisible by 2. Therefore, the total number of solutions for $G_{\vec{X}} \cdot \vec{\alpha}^T = 0$ is at most $(q-1)(q-2)\ldots(q-(n-1))$.

From now on, we consider $k \geqslant 3$. We first note that a similar proof for Lemma 1 does not work since $(k-1)!$ is divisible by 2, so the determinant is zero. Our idea is to remove all the equations with even powers. Without loss of generality, assume k is odd (the proof for even k is similar). Let $t = (k-1)/2$. Observe that $\mathcal{S}(G_{\vec{X}}, \vec{\alpha})_F$ is upper bounded by the number of solutions for the system removing the equations $f_{2i}(X_1, X_2, \ldots, X_n) = 0$ for $1 \leqslant i \leqslant t$. So, there will be only t equations left. We construct a square polynomial system as follows. Fix $X_{t+1}, \ldots, X_n$ as arbitrary distinct non-zero elements in F. Define $c_i = \sum_{j=t+1}^{n} \alpha_j X_j^{2i-1}$ for $1 \leqslant i \leqslant t$. Consider the following square polynomial system with t variables and also t equations. For $i \in \{1, 2, \ldots, t\}$,

$$h_i(X_1, X_2, \ldots, X_t) := \alpha_1 X_1^{2i-1} + \alpha_2 X_2^{2i-1} + \ldots + \alpha_t X_t^{2i-1} + c_i = 0$$

Using a similar idea as in the case $p \geqslant k$, we have

$$
\begin{aligned}
&\mathbf{J}\left(h_1, h_2, \ldots, h_t\right)\left(X_1, X_2, \ldots, X_t\right) \\
&= \left(\prod_{i=1}^{t} \alpha_i\right) \cdot \left(\prod_{i=1}^{t} (2i-1)\right) \cdot \prod_{1 \leqslant i < j \leqslant t} (X_i^2 - X_j^2) \qquad \text{(Fact 2)}
\end{aligned}
$$

$$= \left(\prod_{i=1}^{t} \alpha_i\right) \cdot \left(\prod_{i=1}^{t}(2i-1)\right) \cdot \prod_{1 \leqslant i<j \leqslant t} (X_i - X_j)^2 \qquad (\text{ since } X = -X \text{ for } X \in F_{2^d})$$

Note that the first two terms are non-zero. The last term $\prod_{1 \leqslant i<j \leqslant k-1}(X_i - X_j)^2$ is also non-zero since X_i's are all distinct. These imply that the Jacobian is not zero. Applying Imported Theorem 1 yields that the number of solutions for the square polynomial system is at most $1 \cdot 3 \cdots (2t-1)$. Therefore, the number of solutions for $G_{\vec{X}} \cdot \vec{\alpha}^T = 0$ is at most

$$(q-1)(q-2)\cdots(q-(n-t)) \cdot 1 \cdot 3 \cdots (2t-1) \leqslant (q-1)(q-2)\cdots(q-(n-t)) \cdot (k-1)!,$$

which is $(q-1)(q-2)\cdots(q-(n-(k-1)/2)) \cdot (k-1)!$. This completes the proof. $\square$

3.3 Over Finite Fields with Small Characteristic

Finally, we consider the finite field F with characteristic $3 \leqslant p < k$. Inspired by the proof of Lemma 2, it is natural to remove all the equations whose powers (degrees) are divisible by p to avoid the determinant being equal to zero. That is, consider the following square system of equations.

$$h_i(X_1, X_2, \ldots, X_t) = \alpha_1 X_1^i + \alpha_2 X_2^i + \cdots + \alpha_t X_t^i + c_i = 0 \text{ for } i \in I,$$

where $I = \{i \colon 1 \leqslant i \leqslant k-1,\ i \text{ is not divisible by } p\}$, $c_i \in F$, and $t = (k-1) - \lfloor (k-1)/p \rfloor$. Note that both the number of variables and the number of equations are t. Let $\vec{h}_I = (h_i \colon i \in I)$. The Jacobian is

$$\mathbf{J}(\vec{h}_I) = \left(\prod_{i=1}^{t} \alpha_i\right) \cdot \left(\prod_{j \in I} j\right) \cdot \det(V_t(\mu))$$

Here $\vec{\mu} = (i-1 \colon i \in I)$, and $V_t(\vec{\mu}) = \left(X_i^{\mu_j}\right)_{i,j \in \{1,2,\ldots,t\}}$ is the generalized Vandermonde matrix (refer to Section 2.3). Now, we are done if $\mathbf{J}(\vec{h}_I) \neq 0$, which is equivalent to $\det(V_t(\vec{\mu})) \neq 0$. However, it is not always non-zero. The following result claims that the determinant is non-zero with high probability.

Lemma 3. *It holds that* $\det(V_t(\mu)) \neq 0$ *with probability at least* $1 - \frac{2k^2}{q-1}$*, where the probability is taken over randomly chosen* $\vec{X}$*.*

We provide a proof of Lemma 3 in Supporting Material 8.

Next, we show that for some particular values of p, we can derive a good upper bound on the number of solutions $\mathcal{S}(G_{\vec{X}}, \vec{\alpha})_F$.

Lemma 4. *Let F be a finite field with characteristic $p = k-1$ or $p = k-2$. It holds that*

$$\mathcal{S}(G_{\vec{X}}, \vec{\alpha})_F \leqslant (q-1)(q-2)\cdots(q-(n-p+1)) \cdot (p-1)!.$$

Proof. For $p = k-1$, the index set $I = \{1, 2, \ldots, k-2\}$. This implies that $\vec{\mu} = \{0, 1, \ldots, k-3\}$. Thus, $V_t(\vec{\mu})$ is a Vandermonde matrix whose determinant is always non-zero as long as all X_i are distinct. So we have $\mathcal{S}(G_{\vec{X}}, \vec{\alpha})_F \leqslant (q-1)(q-2)\cdots(q-(n-p+1)) \cdot (p-1)!$.

For $p = k-2$, we choose $I = \{1, 2, \ldots, k-3\}$. With a similar argument, we have $\mathcal{S}(G_{\vec{X}}, \vec{\alpha})_F \leqslant (q-1)(q-2)\cdots(q-(n-p+1)) \cdot (p-1)!$. $\square$

4 Bounding ℓ_1-Fourier Norms of Physical-bit Leakage Functions

This section shows that the ℓ_1-Fourier norm of physical-bit leakage is small. We shall prove the following result.

Lemma 5. *Let $f\colon F \to \{0,1\}$ be a one-bit physical leakage function. Then, for any leakage value $t \in \{0,1\}$, the ℓ_1-Fourier norm of f is bounded as follows.*

1. $\left\| \widehat{\mathbb{1}_{f^{-1}(t)}} \right\|_1 = 1$ *if the finite field F has characteristic two.*

2. $\left\| \widehat{\mathbb{1}_{f^{-1}(t)}} \right\|_1 \lesssim (\log_2 p)^3/\pi^2$ *otherwise.*

We first study the ℓ_1-Fourier norm of physical leakage function over finite fields with characteristic two. We need the following technical result.

Proposition 2. *Let G be a subgroup of $F = F_{p^d}$ and $\alpha \in F$. We abuse notation and define the distribution $\mathsf{Tr}_{F/F_p}(\alpha \cdot G)$ as the following experiment.*

1. *Sample x uniformly at random over G,*

2. *Output $\mathsf{Tr}_{F/F_p}(\alpha x)$*

Then, it holds that

$$\mathsf{Tr}_{F/F_p}(\alpha G) = \begin{cases} U_{\{0\}} & \text{if } \alpha = 0 \text{ or } \alpha G \subseteq \ker(\mathsf{Tr}_{F/F_p}) \\ U_{F_p} & \text{otherwise.} \end{cases}$$

Proof. The first case is straightforward from the definition. So, we will focus on showing the second case. Let $\phi_\alpha\colon G \to F_p$ be a function defined as $\phi_\alpha(x) = \mathsf{Tr}_{F/F_p}(\alpha x)$. For any $a, b \in F_p$ and $x, y \in F$, by the linear property of the trace function (Proposition 1),

$$\phi_\alpha(ax + by) = \mathsf{Tr}_{F/F_p}(\alpha(ax + by)) = a\mathsf{Tr}_{F/F_p}(\alpha x) + b\mathsf{Tr}_{F/F_p}(\alpha y).$$

Thus, the mapping ϕ_α is linear over F_p.

Next, we will show that, if $\alpha \neq 0$ and αG is not a subset of $\ker(\mathsf{Tr}_{F/F_p})$, then ϕ_α is surjective. First, by the assumption, there must exist a $x^* \in G$ such that $\phi_\alpha(x^*) = \mathsf{Tr}_{F/F_p}(\alpha x^*) \neq 0$. Let $b = \phi_\alpha(x^*)$. Since G is a subgroup of F, $ax^* \in G$ for every $a \in F_p$. Therefore, for every $c \in F_p$, we have

$$\phi_\alpha(cb^{-1}x^*) = cb^{-1}\phi_\alpha(x^*) = cb^{-1}b = c.$$

It implies that ϕ_α is surjective. Together with the linear property, for every $c, c' \in F_p$,

$$\left|\phi_\alpha^{-1}(c)\right| = \left|\phi_\alpha^{-1}(c')\right|.$$

Hence, the distribution $\mathsf{Tr}_{F/F_p}(\alpha G)$ is uniform over F_p when $\alpha \neq 0$ and αG is not a subset of $\ker(\mathsf{Tr}_{F/F_p})$, which completes the proof. $\square$

Lemma 6. *Let F be a finite field with characteristic two. Let $f\colon F \to \{0,1\}$ be an one-bit physical leakage function that outputs the bit x_i on input $x = x_0 + x_1\zeta + \ldots + x_{d-1}\zeta^{d-1} \in F$ for some $i \in \{0, 1, \ldots, d-1\}$. Let $C = \{x \in F : x_i = 0\}$. Then, for any $t \in \{0,1\}$ and $\alpha \in F$,*

$$\left|\widehat{\mathbb{1}_{f^{-1}(t)}}(\alpha)\right| = \begin{cases} 1/2 & \text{if } \alpha C = \ker(\mathsf{Tr}_{F/F_p}) \\ 0 & \text{otherwise,} \end{cases}$$

where $\ker(\mathsf{Tr}_{F/F_p}) := \{x \in F \colon \mathsf{Tr}_{F/F_p}(x) = 0\}$. *Consequently, we have*

$$\left\| \widehat{\mathbb{1}_{f^{-1}(t)}} \right\|_1 = 1.$$

Proof. Observe that $f^{-1}(t) = v + C$ for some $v \in \{0, \zeta^i\}$. For any $\alpha \in F$,

$$\begin{aligned}
\left|\widehat{\mathbb{1}_{f^{-1}(t)}}(\alpha)\right| &= \left|\frac{1}{q}\sum_{x\in f^{-1}(t)} \omega^{\mathsf{Tr}_{F/F_p}(\alpha\cdot x)}\right| && \text{(Definition)}\\
&= \left|\frac{1}{q}\sum_{x\in v+C} \omega^{\mathsf{Tr}_{F/F_p}(\alpha\cdot x)}\right| && \text{(Since } f^{-1}(t) = v + C\text{)}\\
&= \left|\frac{1}{q}\sum_{y\in C} \omega^{\mathsf{Tr}_{F/F_p}(\alpha\cdot v)}\cdot \omega^{\mathsf{Tr}_{F/F_p}(\alpha\cdot y)}\right| && \text{(Substitute } x = v + y\text{)}\\
&= \left|\frac{1}{q}\omega^{\mathsf{Tr}_{F/F_p}(\alpha\cdot v)}\cdot \sum_{y\in C} \omega^{\mathsf{Tr}_{F/F_p}(\alpha\cdot y)}\right|
\end{aligned}$$

By Proposition 2, the sum $\sum_{y\in C}\omega^{\mathsf{Tr}_{F/F_p}(\alpha\cdot y)}$ is equal to $|C| = 2^{d-1}$ if $\alpha C = \ker(\mathsf{Tr}_{F/F_p})$, and is equal to 0 otherwise. This yields

$$\left|\widehat{\mathbb{1}_{f^{-1}(t)}}(\alpha)\right| = \begin{cases} 1/2 & \text{if } \alpha C = \ker(\mathsf{Tr}_{F/F_p}) \\ 0 & \text{otherwise.}\end{cases}$$

Note that there are exactly two $\alpha \in F$ such that $\alpha C = \ker(\mathsf{Tr}_{F/F_p})$. Consequently, we have $\left\| \widehat{\mathbb{1}_{f^{-1}(t)}} \right\|_1 = 1$, which completes the proof. □

Next, we state the bound for a finite field with a characteristic greater than 2.

Lemma 7. *Let F be a finite field. Let $f \colon F \to \{0,1\}^n$ be a 1-bit physical leakage function. Then, for every $t \in \{0,1\}$, it holds that*

$$\left\| \widehat{\mathbb{1}_{f^{-1}(t)}} \right\|_1 \lesssim \frac{(\log_2 p)^3}{\pi^2}.$$

We proves Lemma 7 in Supporting Material 9. Lemma 5 follows from Lemma 6 and Lemma 7.

5 Leakage Resilience over Finite Fields with Characteristic Two

This section considers Shamir's secret sharing schemes over finite fields with characteristic 2. We will prove the following theorem.

Theorem 1. *Let F be a finite field with characteristic two. For any $\varepsilon > 0$, the following bound holds.*

$$\Pr_{\vec{X}}[\mathsf{ShamirSS}(n,k,\vec{X})_F \textit{ is not an } (1,\varepsilon)\textit{-LLRS}] \lesssim \frac{1}{\varepsilon}\cdot\frac{2^n\cdot\lambda^n\cdot(k-1)!}{(q-n)^{\lfloor k/2\rfloor}}$$

We recall that $\vec{X} = (X_1, X_2, \ldots, X_n) \in (F^*)^n$ is the uniform distribution over the set of distinct evaluation places. We interpret the Theorem 1 as follows.

Corollary 1. *Let F be a finite field with order 2^d. For any number of parties $n \in \{2, 3, \ldots, \}$, reconstruction threshold $k \leqslant n$, and insecurity parameter $\varepsilon = 2^{-t}$, if the security parameter $\lambda = d \cdot \lceil \log_2 p \rceil$ satisfies $\lambda \geqslant 2t/k + 2n(1 + \log_2 \lambda)/k$, then $\mathsf{ShamirSS}(n, k, \vec{X})_F$ is an $(1, \varepsilon)$-LLRSS with probability at least $1 - \exp(-\Theta(\lambda))$.*

Our result extends to multiple-bit leakage, which is summarized as follows.

Theorem 2. *Let F be a finite field with characteristic two. For any $m \in \{1, 2, \ldots\}$ and $\varepsilon > 0$, the following bound holds.*

$$\Pr_{\vec{X}}[\mathsf{ShamirSS}(n, k, \vec{X})_F \textit{ is not an } (m, \varepsilon)\textit{-LLRS}] \lesssim \frac{1}{\varepsilon} \cdot \binom{\lambda}{m}^n \cdot \frac{2^{mn} \cdot (k-1)!}{(q-n)^{\lfloor k/2 \rfloor}}$$

Remark 4. *The above result extends to the setting where m_i bits are leakages from the i-th share for $1 \leqslant i \leqslant n$. The probability that $\mathsf{ShamirSS}(n, k, \vec{X})_F$ is not $(\vec{m}, \varepsilon)$-LLRSS is upper-bounded by*

$$\frac{1}{\varepsilon} \cdot \binom{\lambda}{m_1}\binom{\lambda}{m_2} \cdots \binom{\lambda}{m_n} \cdot \frac{2^{mn} \cdot (k-1)!}{(q-n)^{\lfloor k/2 \rfloor}} \leqslant \frac{1}{\varepsilon} \cdot \binom{\lambda}{M/n}^n \cdot \frac{2^M (k-1)!}{(q-n)^{\lfloor k/2 \rfloor}}.$$

This bound is maximized when all $m_i = M/n$, where M is the total number of physical bits probed.

We also interpret Theorem 2 as follows.

Corollary 2. *Let F be a finite field with order 2^d. For any number of parties $n \in \{2, 3, \ldots, \}$, reconstruction threshold $k \leqslant n$, the number of leaked bits m, and insecurity parameter $\varepsilon = 2^{-t}$, if the security parameter $\lambda = d$ satisfies $\lambda \geqslant 2tM/(nk) + 2M(1 + \log_2 \lambda)/k$, then $\mathsf{ShamirSS}(n, k, \vec{X})_F$ is an (m, ε)-LLRSS with probability at least $1 - \exp(-\Theta(\lambda))$.*

In the following subsections, we provide a proof of Theorem 1. The proof of Theorem 2 is analogous. The main idea is to reduce the m-bit physical leakage on n secret shares to the 1-bit physical leakage on mn secret shares. We make m copies of each secret share. Then, leaking m bits on the secret share is identical to leaking one bit from the i-th copy for $i \in \{1, 2, \ldots, m\}$. This idea was used in [MNP+21] to reduce multiple-bit leakage for Shamir's secret sharing over prime fields to 1-bit leakage.

5.1 Claims Needed for Theorem 1

Proposition 3. *Let $\vec{\ell} = (\ell_1, \ell_2, \ldots, \ell_n)$ be an arbitrary m-bit physical leakage function, where $\ell_i \colon F \to \{0,1\}^m$ for $1 \leqslant i \leqslant n$. The following bound holds for every pair of secret $s, s' \in F$.*

$$\mathsf{SD}\left(\vec{\ell}(s)\ ,\ \ell(\vec{s'})\right) \leqslant \sum_{\vec{t} \in (\{0,1\}^m)^n} \sum_{\vec{\alpha} \in C_{\vec{X}}^{\perp} \setminus \{\vec{0}\}} \left(\prod_{i=1}^{n} \left| \widehat{\mathbb{1}_{t_i}}(\alpha_i) \right| \right)$$

The following result states that the average of the upper bound over randomly chosen evaluation places $\vec{X}$ is sufficiently small.

Lemma 8. *Let F be a finite field with characteristic 2. The following inequality holds.*

$$\mathop{\mathrm{E}}_{\vec{X}}\left[\sum_{\vec{t} \in \{0,1\}^n} \sum_{\vec{\alpha} \in C_{\vec{X}}^{\perp} \setminus \{\vec{0}\}} \left(\prod_{i=1}^{n} \left| \widehat{\mathbb{1}_{t_i}}(\alpha_i) \right| \right) \right] \lesssim \frac{2^n \cdot (k-1)!}{(q-n)^{\lfloor k/2 \rfloor}}$$

We provide the proof of Proposition 3 and Lemma 8 in Supporting Material 10. We prove Theorem 1 in the following subsection.

5.2 Proof of Theorem 1

Our proof closely follows the idea in [MNP+21]. We have

$$\begin{aligned}
&\Pr_{\vec{X}}\left[\mathsf{ShamirSS}(n,k,\vec{X},F)\text{ is not a }(m,\varepsilon)-LLRS\right]\\
&=\Pr_{\vec{X}}\left[\exists s,\ s',\ \vec{\ell}\,\text{s.t. }\mathsf{SD}\left(\vec{\ell}(s)\ ,\ \vec{\ell}(s')\right)\geqslant\varepsilon\right]\\
&\leqslant\Pr_{\vec{X}}\left[\exists s,\ s',\ \vec{\ell}\,\text{s.t.}\sum_{\vec{t}\in(\{0,1\}^m)^n}\ \sum_{\vec{\alpha}\in C^{\perp}_{\vec{X}}\setminus\{\vec{0}\}}\left(\prod_{i=1}^{n}\left|\widehat{\mathbb{1}_{t_i}}(\alpha_i)\right|\right)\geqslant\varepsilon\right] && \text{(Proposition 3)}\\
&=\Pr_{\vec{X}}\left[\exists\ \vec{\ell}\,\text{s.t.}\sum_{\vec{t}\in(\{0,1\}^m)^n}\ \sum_{\vec{\alpha}\in C^{\perp}_{\vec{X}}\setminus\{\vec{0}\}}\left(\prod_{i=1}^{n}\left|\widehat{\mathbb{1}_{t_i}}(\alpha_i)\right|\right)\geqslant\varepsilon\right] && \text{(Independence of } s,s'\text{)}\\
&=\sum_{\vec{\ell}}\Pr_{\vec{X}}\left[\sum_{\vec{t}\in(\{0,1\}^m)^n}\ \sum_{\vec{\alpha}\in C^{\perp}_{\vec{X}}\setminus\{\vec{0}\}}\left(\prod_{i=1}^{n}\left|\widehat{\mathbb{1}_{t_i}}(\alpha_i)\right|\right)\geqslant\varepsilon\right] && \text{(Union bound)}\\
&\leqslant\sum_{\vec{\ell}}\frac{1}{\varepsilon}\cdot\mathbb{E}_{\vec{X}}\left[\sum_{\vec{t}\in(\{0,1\}^m)^n}\ \sum_{\vec{\alpha}\in C^{\perp}_{\vec{X}}\setminus\{\vec{0}\}}\left(\prod_{i=1}^{n}\left|\widehat{\mathbb{1}_{t_i}}(\alpha_i)\right|\right)\right] && \text{(Markov's inequality)}\\
&\lesssim\sum_{\vec{\ell}}\frac{1}{\varepsilon}\cdot\frac{2^n\cdot(k-1)!}{(q-n)^{\lfloor k/2\rfloor}} && \text{(Lemma 8)}\\
&=\frac{1}{\varepsilon}\cdot\frac{2^n\cdot\lambda^n\cdot(k-1)!}{(q-n)^{\lfloor k/2\rfloor}}
\end{aligned}$$

Therefore, we have completed the proof of Theorem 1.

6 Leakage Resilience over Finite Fields with Large Characteristics

This section presents the results over finite fields with characteristics greater than two. The following theorems summarize our results.

Theorem 3. *Let the reconstruction threshold $k\in\{2,3,\dots\}$. Let F be a finite field with characteristic $p\geqslant k$ and M be the total leaked bits. For $\varepsilon>0$, the following bound holds.*

$$\Pr_{\vec{X}}[\mathsf{ShamirSS}(n,k,\vec{X})_F\textit{ is not an }(M/n,\varepsilon)\text{-}LLRS]\ \lesssim\ \frac{1}{\varepsilon}\cdot\binom{\lambda}{M/n}^n\cdot\frac{2^M\cdot(\log_2 p)^M\cdot(k-1)!}{\pi^M\cdot(q-n)^{k-1}}.$$

Theorem 4. *Let the reconstruction threshold $k\in\{2,3,\dots\}$. Let F be a finite field with characteristic $p=k-1$ or $p=k-2$ and M be the total leaked bits. For any $\varepsilon>0$, the following bound holds.*

$$\Pr_{\vec{X}}[\mathsf{ShamirSS}(n,k,\vec{X})_F\textit{ is not an }(M/n,\varepsilon)\text{-}LLRS]\ \lesssim\ \frac{1}{\varepsilon}\cdot\binom{\lambda}{M/n}^n\cdot\frac{2^M\cdot(\log_2 p)^M\cdot(p-1)!}{\pi^M\cdot(q-n)^{p-1}}.$$

The proofs of Theorem 3 and Theorem 4 are analogous to the proof presented in Section 5. The main differences are that these proofs (1) use Lemma 7 to bound ℓ_1-Fourier norm, and (2) use Lemma 1 and Lemma 4 to upper bound the number of solutions of the equation, respectively.

7 Our Derandomization Results

This section presents an explicit algorithm to identify secure evaluation places $X_1, X_2, \ldots, X_n \in F^*$ for $(n, 2, (X_1, \ldots, X_n))$-Shamir secret sharing over a finite field F with characteristic $p \geqslant 2$ against the single block leakage from every share.

Consider the finite field $F = F_{p^d}$ where $d \in \{2, 3, \ldots\}$. We will interpret F as $F_p[\zeta]/\Pi(\zeta)$, where $\Pi(\zeta)$ is an irreducible degree-d F_p-polynomial. Every element $\vec{x} \in F$ can be written as a length-d vector of F_p elements. We represent $x \in F$ as $\vec{x} = (x_0, x_1, \ldots, x_{d-1}) \in (F_p)^d$ when $x = x_0 + x_1\zeta + \cdots + x_{d-1}\zeta^{d-1}$. We define the *single block leakage* function $\ell_i^{\text{block}} \colon F \to F_p$ as the $\lceil \log_2(p) \rceil$-bit physical leakage function that leaks the i-th coefficient $x_i \in F_p$ for $\vec{x} \in F$, i.e. $\ell_i^{\text{block}}(\vec{x}) = x_i$.

Theorem 5. *Let F be a finite field with characteristic $p \geqslant 2$. Consider the $(n, 2, (X_1, \ldots, X_n))$-Shamir secret-sharing scheme over F. Consider the block physical bit leakage function $\vec{\ell}^{\text{block}} = (\ell_{i_1}^{\text{block}}, \ell_{i_2}^{\text{block}}, \ldots, \ell_{i_n}^{\text{block}})$ where $i_1, i_2, \ldots, i_n \in \{0, 1, 2, \ldots, d-1\}$ and $\ell_{i_j}^{\text{block}} \colon F \to F_p$ for all $j \in \{0, 1, \ldots, n\}$. Define the shifting factor $\eta^{(i_j)} \in F_q$ such that $(x)_{i_j} = \left(x \cdot \eta^{(i_j)}\right)_0$, for all $x \in F_q$. For any secret $s \in F$, if*

$$X_1\eta^{(i_1)}, X_2\eta^{(i_2)}, \ldots, X_n\eta^{(i_n)} \in F_q$$

are all F_p-linearly independent, then

$$\mathsf{SD}\left(\vec{\ell^{\text{block}}}(0)\ ,\ \vec{\ell^{\text{block}}}(s)\right) = 0.$$

Theorem 5 implies that all evaluation places $(X_1, \ldots, X_n) \in F_q^n$ satisfying

$$X_1\eta^{(i_1)}, X_2\eta^{(i_2)}, \ldots, X_n\eta^{(i_n)} \in F_q$$

being all F_p-linearly independent, are perfectly secure against single block leakage attack. Figure 1 shows a test to identify secure evaluation places $(X_1, \ldots, X_n) \in F_q^n$ for $(n, 2, (X_1, \ldots, X_n))$-Shamir secret sharing over finite field F_q with characteristic $p \geqslant 2$ against the single block leakage from every share. Note that the algorithm outputs secure for at least $1 - d^n p^{n-1}/q$ fraction of evaluation places.

7.1 Proof of Theorem 5

Consider leakage distribution

$$\left((s + P \cdot X_1)_{i_1}, (s + P \cdot X_2)_{i_1}, \ldots, (s + P \cdot X_n)_{i_n}\right)$$

where $i_1, i_2, \ldots, i_n \in \{0, 1, \ldots, d-1\}$ and $P \in F_q$ is chosen uniformly at random. Then, the above distribution is identical to

$$\left((Q \cdot X_1)_{i_1}, (Q \cdot X_2 + t_2)_{i_1}, \ldots, (Q \cdot X_n + t_n)_{i_n}\right)$$

where $(s \cdot X_1^{-1} + P) \mapsto Q$ is an automorphism over F_q and $t_i = s \cdot (1 - X_i \cdot X_1^{-1})$ By Proposition 4, the shifting factor $\eta^{(i_1)}, \eta^{(i_2)}, \ldots, \eta^{(i_n)} \in F_q$ allow us to equivalent study the leakage distribution on the 0-th block

$$\left(\left(QX_1\eta^{(i_1)}\right)_0, \left(QX_2\eta^{(i_2)} + t'_2\right)_0, \ldots, \left(QX_n\eta^{(i_n)} + t'_n\right)_0\right)$$

Input. Distinct evaluation places $X_1, X_2, \ldots, X_n \in F$, and p is a prime

Output. Decide whether the evaluation places $(X_1, \ldots, X_n)$ are secure to all single-block leakage attacks.

Algorithm.
1. For $i \in \{0, 1, \ldots, d-1\}$:
   (a) Compute the shift factor $\eta^{(i,0)}$ as defined in Proposition 4
2. For $i_1, i_2, \ldots, i_n \in \{0, 1, \ldots, d-1\}$:
   (a) If $\left\{X_1\eta^{(i_1)}, X_2\eta^{(i_2)}, \ldots, X_n\eta^{(i_n)}\right\} \subseteq F_q$ is *not* F_p-linearly independent, return "Insecure."
3. Return "Secure."

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

where Q is uniformly at random from F_q and $t'_j = t_j \cdot \eta^{(i_j)}$ for $j \in \{1, 2, \ldots, n\}$. Finally, the previous distribution is identical to

$$\left(\left(QX_1\eta^{(i_1)}\right)_0 , \left(QX_2\eta^{(i_2)}\right)_0 + t''_2 , \ldots, \left(QX_n\eta^{(i_n)}\right)_0 + t''_n \right),$$

where Q is uniformly at random from F_q and $s \mapsto t''_j$ are appropriate linear automorphisms over F_q, for all $j \in \{2, 3, \ldots, n\}$.

By Lemma 10, the distribution

$$\left(\left(QX_1\eta^{(i_1)}\right)_0 , \left(QX_2\eta^{(i_2)}\right)_0 , \ldots, \left(QX_n\eta^{(i_n)}\right)_0 \right)$$

is equivalent as a uniform distribution over $(F_p)^n$ for uniformly random $Q \in F_q$.

Thus, if

$$X_1\eta^{(i_1)}, X_2\eta^{(i_2)}, \ldots, X_n\eta^{(i_n)} \in F_q$$

are all F_p-linearly independent,

$$\mathsf{SD}\left(\ell^{\vec{\text{block}}}(0) , \ell^{\vec{\text{block}}}(s)\right) = 0.$$

7.2 Technical Results

The following result says that every block leakage is emulated by another block leakage.

Proposition 4. *For $i \in \{0, 1, \ldots, d-1\}$, define $C_i := \{x \in F : x_i = 0\}$. For $i, j \in \{0, 1, \ldots, d-1\}$, there exists $\eta^{(i,j)} \in F^*$ such that $C_i \cdot \eta^{(i,j)} = C_j$.*

Proof. Let D be the set of all subgroups of order p^{d-1} of the additive group $(F, +)$. Observe that $x \cdot C_i \in D$ for every $x \in F^*$. Consider the following map $\phi_{C_i} : F^* \to D$ such that $\phi_{C_i}(x) := x \cdot C_i$. One can easily verify that ϕ_{C_i} is one-to-$(p-1)$ mapping. That is, $\phi_{C_i}(x) = \phi_{C_i}(ax)$ for every $a \in F_p^*$, and $\phi_{C_i}(x) \neq \phi_{C_i}(y)$ if $x \neq ay$ for some $a \in F_p^*$. Observe now that $|D| = (p^d - 1)/(p-1)$ and $|F^*| = p^d - 1$. Therefore, $\left|\phi_{C_i}^{-1}(C)\right| = p - 1$ for every $C \in D$. This implies that there exists some $\eta^{(i,j)} \in F^*$ such that $C_j = \eta^{(i,j)} \cdot C_i$ since $C_j \in D$. $\square$

Lemma 9. *For $i \in \{0, 1, \ldots, d-1\}$, define $C_i := \{x \in F : x_i = 0\}$. Then, the following statements hold.*

1. *If $\alpha = 0$, $C_i \cdot \alpha = \{0\}$.*
2. *If $\alpha \in F_p^* \subseteq F$, then $C_i \cdot \alpha = C_i$ and $(C_i \cdot \alpha)_i = \{0\}$.*
3. *If $\alpha \in F \setminus F_p$, then $(U_{C_i} \cdot \alpha)_i = U_{F_p}$.*

Proof. The first two cases are straightforward from the definition. Suppose $\alpha \in F \setminus F_p$. Let D be the set of all subgroups of order p^{d-1} of F. Consider the mapping $\psi_\alpha \colon C_i \to F_p$ defined as $\psi_\alpha(x) = (\alpha \cdot x)_i$. One can verify that this mapping is linear over F_p. Therefore, to complete the proof, it suffices to show that there is an $x \in F$ such that $\psi_\alpha(x) \neq 0$. By the property of the mapping ϕ_{C_i} in the proof of Proposition 2, it is clear that $\alpha \cdot C_i \neq C_i$. This implies that, there exists $x' \in F$ such that $\psi_\alpha(x') = (\alpha \cdot x')_i \neq 0$ since C_i is the only subgroup of order p^{d-1} satisfying $x_i = 0$ for element x in that subgroup. Thus, for every $a, b \in F_p$, $\left|\psi_\alpha^{-1}(a)\right| = \left|\psi_\alpha^{-1}(b)\right|$, which completes the proof. $\square$

Corollary 3. *For $i \in \{0, 1, \ldots, d-1\}$, define $C_i := \{x \in F : x_i = 0\}$. If $\alpha \in F \setminus F_p$, then for all $c \in F$, $(U_{C_i} \cdot \alpha + c)_i = U_{F_p}$.*

Recall that U_Ω is the uniform distribution over the set Ω.

Lemma 10. *Fix arbitrary $Y_1, Y_2, \ldots, Y_n \in F_q^*$ such that the set $\{Y_1, Y_2, \ldots, Y_n\} \subseteq F_q$ is F_p-linearly independent. Then, for uniformly random $Q \in F_q$, the distribution $\left((QY_1)_0\ , (QY_2)_0\ , \ldots,\ (QY_n)_0 \right)$ is uniformly random over $(F_p)^n$.*

Note that, for the set to be independent, it must be the case that $d \leqslant n$ because the ambient space F_q is an F_p-vector space of dimension d. The proof of this result will crucially rely on the fact that the elements belong to a field. Supporting Material 12 proves this lemma.

References

[ADN+19] 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, *Advances in Cryptology – CRYPTO 2019, Part II*, volume 11693 of *Lecture Notes in Computer Science*, pages 510–539, Santa Barbara, CA, USA, August 18–22, 2019. Springer, Heidelberg, Germany. doi:10.1007/978-3-030-26951-7_18. 4

[AMN+21] 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 *ISIT*, 2021. 3

[BDIR18] 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, *Advances in Cryptology – CRYPTO 2018, Part I*, volume 10991 of *Lecture Notes in Computer Science*, pages 531–561, Santa Barbara, CA, USA, August 19–23, 2018. Springer, Heidelberg, Germany. doi:10.1007/978-3-319-96884-1_18. 1, 2, 4

[BDIR21] Fabrice Benhamouda, Akshay Degwekar, Yuval Ishai, and Tal Rabin. On the local leakage resilience of linear secret sharing schemes. *Journal of Cryptology*, 34(2):10, April 2021. doi:10.1007/s00145-021-09375-2. 1, 2, 4

[BIS19] Andrej Bogdanov, Yuval Ishai, and Akshayaram Srinivasan. Unconditionally secure computation against low-complexity leakage. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology – CRYPTO 2019, Part II*, volume 11693 of *Lecture Notes in Computer Science*, pages 387–416, Santa Barbara, CA, USA, August 18–22, 2019. Springer, Heidelberg, Germany. doi:10.1007/978-3-030-26951-7_14. 4

[BP23] 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. 2

[BPRW16] 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, *Advances in Cryptology – EUROCRYPT 2016, Part I*, volume 9665 of *Lecture Notes in Computer Science*, pages 58–86, Vienna, Austria, May 8–12, 2016. Springer, Heidelberg, Germany. doi:10.1007/978-3-662-49890-3_3. 4

[BS19] Saikrishna Badrinarayanan and Akshayaram Srinivasan. Revisiting non-malleable secret sharing. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2019, Part I*, volume 11476 of *Lecture Notes in Computer Science*, pages 593–622, Darmstadt, Germany, May 19–23, 2019. Springer, Heidelberg, Germany. doi:10.1007/978-3-030-17653-2_20. 4

[BSVX21] Mitali Bafna, Madhu Sudan, Santhoshini Velusamy, and David Xiang. Elementary analysis of isolated zeroes of a polynomial system. *arXiv preprint arXiv:2102.00602*, 2021. 5, 9, 14

[CGG+20] 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 Annual Symposium on Foundations of Computer Science*, pages 1226–1242, Durham, NC, USA, November 16–19, 2020. IEEE Computer Society Press. doi:10.1109/FOCS46700.2020.00117. 4

[CKOS22] 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, *Advances in Cryptology – CRYPTO 2022, Part I*, volume 13507 of *Lecture Notes in Computer Science*, pages 178–207, Santa Barbara, CA, USA, August 15–18, 2022. Springer, Heidelberg, Germany. doi:10.1007/978-3-031-15802-5_7. 4

[CS21] Nicolas Costes and Martijn Stam. Redundant code-based masking revisited. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2021(1):426–450, 2021. https://tches.iacr.org/index.php/TCHES/article/view/8740. doi:10.46586/tches.v2021.i1.426-450. 4

[CT22] 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. 4

[DGW+10] 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. 4

[ERR10] 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. 4

[FY19] Serge Fehr and Chen Yuan. Towards optimal robust secret sharing with security against a rushing adversary. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2019, Part III*, volume 11478 of *Lecture Notes in Computer Science*, pages 472–499, Darmstadt, Germany, May 19–23, 2019. Springer, Heidelberg, Germany. doi:10.1007/978-3-030-17659-4_16. 4

[FY20] 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: 18th Theory of Cryptography Conference, Part III*, volume 12552 of *Lecture Notes in Computer Science*, pages 470–498, Durham, NC, USA, November 16–19, 2020. Springer, Heidelberg, Germany. doi:10.1007/978-3-030-64381-2_17. 4

[GERCP13] 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. 4

[GFV17] Sreechakra Goparaju, Arman Fazeli, and Alexander Vardy. Minimum storage regenerating codes for all parameters. *IEEE Transactions on Information Theory*, 63(10):6318–6328, 2017. 4

[GK18] Vipul Goyal and Ashutosh Kumar. Non-malleable secret sharing. In Ilias Diakonikolas, David Kempe, and Monika Henzinger, editors, *50th Annual ACM Symposium on*

Theory of Computing, pages 685–698, Los Angeles, CA, USA, June 25–29, 2018. ACM Press. doi:10.1145/3188745.3188872. 1

[GW16] Venkatesan Guruswami and Mary Wootters. Repairing reed-solomon codes. In Daniel Wichs and Yishay Mansour, editors, *48th Annual ACM Symposium on Theory of Computing*, pages 216–226, Cambridge, MA, USA, June 18–21, 2016. ACM Press. doi:10.1145/2897518.2897525. 4

[GW17] Venkatesan Guruswami and Mary Wootters. Repairing reed-solomon codes. *IEEE Trans. Inf. Theory*, 63(9):5684–5698, 2017. doi:10.1109/TIT.2017.2702660. 4

[HVW20] Carmit Hazay, Muthuramakrishnan Venkitasubramaniam, and Mor Weiss. The price of active security in cryptographic protocols. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology – EUROCRYPT 2020, Part II*, volume 12106 of *Lecture Notes in Computer Science*, pages 184–215, Zagreb, Croatia, May 10–14, 2020. Springer, Heidelberg, Germany. doi:10.1007/978-3-030-45724-2_7. 4

[ISW03] Yuval Ishai, Amit Sahai, and David Wagner. Private circuits: Securing hardware against probing attacks. In Dan Boneh, editor, *Advances in Cryptology – CRYPTO 2003*, volume 2729 of *Lecture Notes in Computer Science*, pages 463–481, Santa Barbara, CA, USA, August 17–21, 2003. Springer, Heidelberg, Germany. doi:10.1007/978-3-540-45146-4_27. 1, 2, 3

[KK23] Ohad Klein and Ilan Komargodski. New bounds on the local leakage resilience of shamir's secret sharing scheme. In *CRYPTO*, 2023. 4

[KMS19] Ashutosh Kumar, Raghu Meka, and Amit Sahai. Leakage-resilient secret sharing against colluding parties. In David Zuckerman, editor, *60th Annual Symposium on Foundations of Computer Science*, pages 636–660, Baltimore, MD, USA, November 9–12, 2019. IEEE Computer Society Press. doi:10.1109/FOCS.2019.00045. 4

[MNP+21] 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, *Advances in Cryptology – EUROCRYPT 2021, Part II*, volume 12697 of *Lecture Notes in Computer Science*, pages 344–374, Zagreb, Croatia, October 17–21, 2021. Springer, Heidelberg, Germany. doi:10.1007/978-3-030-77886-6_12. 1, 3, 4, 5, 6, 9, 14, 19, 20, 29

[MNP+22] 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. 3

[MNPW22] 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 *IEEE International Symposium on Information Theory, ISIT 2022, Espoo, Finland, June 26 - July 1, 2022*, pages 2678–2683. IEEE, 2022. doi:10.1109/ISIT50566.2022.9834695. 4

[MNPY23] Hemanta K. Maji, Hai H. Nguyen, Anat Paskin-Cherniavsky, and Xiuyu Ye. Security of shamir's secret-sharing against physical bit leakage: Secure evaluation places. https://www.cs.purdue.edu/homes/hmaji/papers/MNPY23.pdf, 2023. 3, 7

[MPSW21] 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, *Advances in Cryptology – CRYPTO 2021, Part III*, volume 12827 of *Lecture Notes in Computer Science*, pages 779–808, Virtual Event, August 16–20, 2021. Springer, Heidelberg, Germany. doi:10.1007/978-3-030-84252-9_26. 4

[MSV20] Pasin Manurangsi, Akshayaram Srinivasan, and Prashant Nalini Vasudevan. Nearly optimal robust secret sharing against rushing adversaries. In Daniele Micciancio and Thomas Ristenpart, editors, *Advances in Cryptology – CRYPTO 2020, Part III*, volume 12172 of *Lecture Notes in Computer Science*, pages 156–185, Santa Barbara, CA, USA, August 17–21, 2020. Springer, Heidelberg, Germany. doi:10.1007/978-3-030-56877-1_6. 4

[NIS] NIST. Randomness beacon project. http://www.nist.gov/itl/csd/ct/nist_beacon.cfm. 2

[NS20] Jesper Buus Nielsen and Mark Simkin. Lower bounds for leakage-resilient secret sharing. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology – EUROCRYPT 2020, Part I*, volume 12105 of *Lecture Notes in Computer Science*, pages 556–577, Zagreb, Croatia, May 10–14, 2020. Springer, Heidelberg, Germany. doi:10.1007/978-3-030-45721-1_20. 4

[PDC13] 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. 4

[RSK11] 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. 4

[Sha79] Adi Shamir. How to share a secret. *Communications of the Association for Computing Machinery*, 22(11):612–613, November 1979. 1

[SV19] Akshayaram Srinivasan and Prashant Nalini Vasudevan. Leakage resilient secret sharing and applications. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology – CRYPTO 2019, Part II*, volume 11693 of *Lecture Notes in Computer Science*, pages 480–509, Santa Barbara, CA, USA, August 18–22, 2019. Springer, Heidelberg, Germany. doi:10.1007/978-3-030-26951-7_17. 4

[TWB12] 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. 4

[Woo96] Trevor D Wooley. A note on simultaneous congruences. *journal of number theory*, 58(2):288–297, 1996. 5, 9, 14

[WTB16] Zhiying Wang, Itzhak Tamo, and Jehoshua Bruck. Explicit minimum storage regenerating codes. *IEEE Transactions on Information Theory*, 62(8):4466–4480, 2016. 4

[YB17a] 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. 4

[YB17b] 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. 4

[Zha12] Xiaomei Zhao. A note on multiple exponential sums in function fields. *Finite Fields and Their Applications*, 18(1):35–55, 2012. 9, 14

8 Bounding Number of Solutions

of Lemma 3. It follows from Fact 3 that

$$\det(V_t(\vec{\mu})) = \Phi(X_1, X_2, \ldots, X_t) \cdot \prod_{1 \leqslant i < j \leqslant t} (X_i - X_j),$$

where $\Phi(X_1, X_2, \ldots, X_t)$ is a (symmetric) multivariate polynomial. Observe that $\deg(P) \leqslant k^2$ since $\det(V_t(\vec{\mu}))$ is a multivariate polynomial with degree at most $\sum_{i \in I} i \leqslant k^2$. Consider $\vec{X} = (X_1, X_2, \ldots, X_t)$ in which each X_i is independently and randomly chosen from F^*. The Schwartz-Zipple lemma for multivariate polynomials implies that

$$\Pr_{\vec{X}}[\Phi(X_1, X_2, \ldots, X_n) = 0] \leqslant k^2/(q-1).$$

Applying union bound twice yields

$$\begin{aligned}
\Pr_{\vec{X}}[\det(V_t(\vec{\mu})) = 0] &\leqslant \Pr_{\vec{X}}[\Phi(\vec{X}) = 0] + \Pr_{\vec{X}}[\exists 1 \leqslant i < j \leqslant t \colon X_i = X_j] \\
&\leqslant k^2/(q-1) + \sum_{1 \leqslant i < j \leqslant t} \Pr_{\vec{X}}[X_i = X_j] \\
&\leqslant k^2/(q-1) + k^2 \cdot 1/(q-1) \\
&= 2k^2/(q-1).
\end{aligned}$$

□

9 Bounding ℓ_1-Fourier Norms

of Lemma 7. Suppose f leaks one bit on the i-th block. Let $C = \{x \in F \colon x_i = 0\}$. Unlike in the characteristic 2 case, now we have $f^{-1}(t) = V + C$, where $V \subseteq D = \{0, \zeta^i, \ldots, (p-1)\zeta^i\}$. We have

$$\left|\widehat{\mathbb{1}_{f^{-1}(t)}}(\alpha)\right| = \left|\frac{1}{q} \sum_{v \in V} \omega^{\mathsf{Tr}_{F/F_p}(\alpha \cdot v)} \cdot \sum_{y \in C} \omega^{\mathsf{Tr}_{F/F_p}(\alpha \cdot y)}\right|$$

By Proposition 2, if $\alpha C \neq \ker(\mathsf{Tr}_{F/F_p})$, then $\left|\widehat{\mathbb{1}_{f^{-1}(t)}}(\alpha)\right| = 0$. Otherwise, we have

$$\left|\widehat{\mathbb{1}_{f^{-1}(t)}}(\alpha)\right| = \frac{1}{p}\left|\sum_{v \in V} \omega^{\mathsf{Tr}_{F/F_p}(\alpha \cdot v)}\right| = \frac{1}{p}\left|\sum_{c \in V_i} \omega^{\mathsf{Tr}_{F/F_p}(\alpha c \zeta^i)}\right| = \frac{1}{p}\left|\sum_{c \in V_i} \omega^{c \cdot \mathsf{Tr}_{F/F_p}(\alpha \zeta^i)}\right|,$$

where $V_i = \{x_i \colon x \in V\}$. This implies that $\left|\widehat{\mathbb{1}_{f^{-1}(t)}}(\alpha)\right| = \widehat{\mathbb{1}_{V_i}}(\mathsf{Tr}_{F/F_p}(\alpha\zeta^i))$.

Observe that $\{\mathsf{Tr}_{F/F_p}(\alpha\zeta^i) \colon \alpha D \neq \ker(\mathsf{Tr}_{F/F_p})\} = F_p$. This implies that $\left\|\widehat{\mathbb{1}_{f^{-1}(t)}}\right\|_1 = \left\|\widehat{\mathbb{1}_{V_i}}\right\|_1$. To prove our result, we shall use a result from [MNP+21] saying that V can be partitioned into at most $\log_2 p$ generalized arithmetic progressions (GAPs) of rank two, and the ℓ_1-Fourier norm of these GAPs bounded. It follows from the result in [MNP+21](see corollary 1) that

$$\left\|\widehat{\mathbb{1}_{f^{-1}(t)}}\right\|_1 \leqslant (\log_2 p)^3/\pi^2,$$

which completes the proof. □

10 Omitted Proofs for the Randomized Constructions

10.1 Proof of Proposition 3

We shall need the following results. The first result is a (generalized) Poisson Summation Formula.

Proposition 5. *For any leakage function $\vec{\ell}$ and any leakage value $\vec{t} \in (\{0,1\}^m)^n$, it holds that*

$$\Pr_{\vec{s} \leftarrow \mathsf{Share}^{\vec{X}}(s)}[\vec{\ell}(\vec{s}) = \vec{t}\,] = \sum_{\vec{\alpha} \in C^{\perp}_{\vec{X}}} \left(\prod_{i=1}^{n} \widehat{\mathbb{1}_{\ell_i}}(\alpha_i)\right) \cdot \omega^{-\mathsf{Tr}_{F/F_p}(s \cdot \langle \vec{\alpha}, \vec{1} \rangle)},$$

where $\langle \vec{x}, \vec{y} \rangle = x_1 \cdot y_1 + x_2 \cdot y_2 + \cdots + x_n \cdot y_n$ for any $\vec{x}, \vec{y} \in F^n$.

We provide the proof of this result in the later section.

Now, we are ready to prove Proposition 3.

of Proposition 3. Recall that $\mathbb{1}_{t_i}$ is the indicator function of the set $\ell_i^{-1}(t_i)$ for $t_i \in \{0,1\}^m$ and $1 \leqslant i \leqslant n$. We have

$$\begin{aligned}
&\mathsf{SD}\left(\vec{\ell}(s)\ ,\ \ell(\vec{s'})\right) \\
&= \frac{1}{2} \sum_{\vec{t} \in (\{0,1\}^m)^n} \left| \Pr_{\vec{s} \leftarrow \mathsf{Share}^{\vec{X}}(s)}[\vec{\ell}(\vec{s}) = \vec{t}] - \Pr_{\vec{s'} \leftarrow \mathsf{Share}^{\vec{X}}(s)}[\vec{\ell}(\vec{s'}) = \vec{t}] \right| \\
&= \frac{1}{2} \sum_{\vec{t} \in (\{0,1\}^m)^n} \left| \sum_{\vec{\alpha} \in C^{\perp}} \left(\prod_{i=1}^{n} \widehat{\mathbb{1}_{t_i}}(\alpha_i)\right) \cdot \left(\omega^{-\mathsf{Tr}_{F/F_p}(s \cdot \langle \vec{\alpha}, \vec{1} \rangle)} - \omega^{-\mathsf{Tr}_{F/F_p}(s' \cdot \langle \vec{\alpha}, \vec{1} \rangle)}\right) \right| && \text{(Proposition 5)} \\
&= \frac{1}{2} \sum_{\vec{t} \in (\{0,1\}^m)^n} \left| \sum_{\vec{\alpha} \in C^{\perp} \setminus \{\vec{0}\}} \left(\prod_{i=1}^{n} \widehat{\mathbb{1}_{t_i}}(\alpha_i)\right) \cdot \left(\omega^{-\mathsf{Tr}_{F/F_p}(s \cdot \langle \vec{\alpha}, \vec{1} \rangle)} - \omega^{-\mathsf{Tr}_{F/F_p}(s' \cdot \langle \vec{\alpha}, \vec{1} \rangle)}\right) \right| \\
&\leqslant \frac{1}{2} \sum_{\vec{t} \in (\{0,1\}^m)^n} \sum_{\vec{\alpha} \in C^{\perp} \setminus \{\vec{0}\}} \left| \left(\prod_{i=1}^{n} \widehat{\mathbb{1}_{t_i}}(\alpha_i)\right) \right| \cdot \left| \left(\omega^{-\mathsf{Tr}_{F/F_p}(s \cdot \langle \vec{\alpha}, \vec{1} \rangle)} - \omega^{-\mathsf{Tr}_{F/F_p}(s' \cdot \langle \vec{\alpha}, \vec{1} \rangle)}\right) \right| \\
& && \text{(Triangle inequality)} \\
&\leqslant \frac{1}{2} \sum_{\vec{t} \in (\{0,1\}^m)^n} \sum_{\vec{\alpha} \in C^{\perp} \setminus \{\vec{0}\}} \prod_{i=1}^{n} \left| \widehat{\mathbb{1}_{t_i}}(\alpha_i) \right| \cdot 2
\end{aligned}$$

$$= \sum_{\vec{t}\in(\{0,1\}^m)^n} \sum_{\vec{\alpha}\in C^\perp\setminus\{\vec{0}\}} \prod_{i=1}^{n} \left|\widehat{\mathbb{1}_{t_i}}(\alpha_i)\right|,$$

which completes the proof. □

10.2 Proof of Lemma 8

We have

$$
\begin{aligned}
&\mathop{\mathrm{E}}_{\vec{X}}\left[\sum_{\vec{t}\in\{0,1\}^n} \sum_{\vec{\alpha}\in C_{\vec{X}}^\perp\setminus\{\vec{0}\}} \left(\prod_{i=1}^{n}\left|\widehat{\mathbb{1}_{t_i}}(\alpha_i)\right|\right)\right] \\
&= \sum_{\vec{t}\in\{0,1\}^n} \mathop{\mathrm{E}}_{\vec{X}}\left[\sum_{\vec{\alpha}\in C_{\vec{X}}^\perp\setminus\{\vec{0}\}} \left(\prod_{i=1}^{n}\left|\widehat{\mathbb{1}_{t_i}}(\alpha_i)\right|\right)\right] && \text{(Linearity)} \\
&= \sum_{\vec{t}\in\{0,1\}^n} \sum_{\vec{\alpha}\in F^n\setminus\{\vec{0}\}} \left(\prod_{i=1}^{n}\left|\widehat{\mathbb{1}_{t_i}}(\alpha_i)\right|\right) \cdot \Pr_{\vec{X}}\left[\vec{\alpha}\in C_{\vec{X}}^\perp\right] && \text{(Linearity of expectation)} \\
&\leqslant \sum_{\vec{t}\in\{0,1\}^n} \sum_{\vec{\alpha}\in F^n\setminus\{\vec{0}\}} \left(\prod_{i=1}^{n}\left|\widehat{\mathbb{1}_{t_i}}(\alpha_i)\right|\right) \cdot \frac{(q-1)(q-2)\cdots(q-(n-\lfloor k/2\rfloor))\cdot(k-1)!}{(q-1)(q-2)\cdots(q-n)} && \text{()} \\
&\leqslant \sum_{\vec{t}\in\{0,1\}^n} \sum_{\vec{\alpha}\in F^n\setminus\{\vec{0}\}} \left(\prod_{i=1}^{n}\left|\widehat{\mathbb{1}_{t_i}}(\alpha_i)\right|\right) \cdot \frac{(p-1)(p-2)\cdots(q-(n-\lfloor k/2\rfloor))\cdot(k-1)!}{(q-1)(q-2)\cdots(q-n)} && \text{(Lemma 2)} \\
&\leqslant \sum_{\vec{t}\in\{0,1\}^n} \prod_{i=1}^{n} \left(\sum_{\alpha_i\in F}\left|\widehat{\mathbb{1}_{t_i}}(\alpha_i)\right|\right) \cdot \frac{(k-1)!}{(q-(n-\lfloor k/2\rfloor+1))\cdots(q-n)} \\
&\lesssim \sum_{\vec{t}\in\{0,1\}^n} 1\cdot \frac{(k-1)!}{(q-(n-\lfloor k/2\rfloor+1))\cdots(q-n)} \\
&\lesssim \frac{2^n\cdot(k-1)!}{(q-n)^{\lfloor k/2\rfloor}}
\end{aligned}
$$

This completes the proof.

10.3 Proof of Proposition 5

We need the following claim for the proof.

Proposition 6. *It holds that*

$$\mathop{\mathrm{E}}_{\vec{x}\leftarrow C_{\vec{X}}}\left[\omega^{-\mathsf{Tr}_{F/F_p}(\langle\vec{\alpha},\vec{x}\rangle)}\right] = \begin{cases} 1 & \text{if } \vec{\alpha}\in C_{\vec{X}}^\perp \\ 0 & \text{otherwise.}\end{cases}$$

This follows from the standard Fourier analysis, the linear properties of the linear code $C_{\vec{X}}$ and the field trace.

of Proposition 5. The proof proceeds by applying standard Fourier analysis over the additive group $(F, +)$. We have

$$\begin{aligned}
&\Pr_{\vec{s} \leftarrow \mathsf{Share}^{\vec{X}}(s)} [\vec{\ell}(\vec{s}) = \vec{t}\,] \\
&= \mathop{\mathrm{E}}_{\vec{x} \leftarrow C_{\vec{X}}} \left[\prod_{i=1}^{n} \mathbb{1}_{t_i}(x_i + s) \right] \\
&= \mathop{\mathrm{E}}_{\vec{x} \leftarrow C_{\vec{X}}} \left[\prod_{i=1}^{n} \sum_{\alpha_i \in F} \widehat{\mathbb{1}_{\ell_i}}(\alpha_i) \cdot \omega^{-\mathsf{Tr}_{F/F_p}(\alpha_i \cdot (x_i + s))} \right] && \text{(Lemma 4)} \\
&= \mathop{\mathrm{E}}_{\vec{x} \leftarrow C_{\vec{X}}} \left[\sum_{\vec{\alpha} \in F^n} \left(\prod_{i=1}^{n} \widehat{\mathbb{1}_{\ell_i}}(\alpha_i) \right) \cdot \prod_{i=1}^{n} \omega^{-\mathsf{Tr}_{F/F_p}(\alpha_i \cdot (x_i + s))} \right] && \text{(Linearity)} \\
&= \mathop{\mathrm{E}}_{\vec{x} \leftarrow C_{\vec{X}}} \left[\sum_{\vec{\alpha} \in F^n} \left(\prod_{i=1}^{n} \widehat{\mathbb{1}_{\ell_i}}(\alpha_i) \right) \cdot \omega^{-\mathsf{Tr}_{F/F_p}(\langle \vec{\alpha}, \vec{x} \rangle + s \cdot \langle \vec{\alpha}, \vec{1} \rangle)} \right] && \text{(Proposition 1)} \\
&= \sum_{\vec{\alpha} \in F^n} \left(\prod_{i=1}^{n} \widehat{\mathbb{1}_{\ell_i}}(\alpha_i) \right) \cdot \omega^{-\mathsf{Tr}_{F/F_p}(s \cdot \langle \vec{\alpha}, \vec{1} \rangle)} \cdot \mathop{\mathrm{E}}_{\vec{x} \leftarrow C_{\vec{X}}} \left[\omega^{-\mathsf{Tr}_{F/F_p}(\langle \vec{\alpha}, \vec{x} \rangle)} \right] && \text{(Linearity)} \\
&= \sum_{\vec{\alpha} \in C_{\vec{X}}^{\perp}} \left(\prod_{i=1}^{n} \widehat{\mathbb{1}_{\ell_i}}(\alpha_i) \right) \cdot \omega^{-\mathsf{Tr}_{F/F_p}(s \cdot \langle \vec{\alpha}, \vec{1} \rangle)} && \text{(Proposition 6)}
\end{aligned}$$

This completes the proof. □

11 Derandomization results for $(2, 2, (X_1, X_2))$-Shamir's secret sharing scheme

This section studies a special case of our results from Section 7. We presents an algorithm to identify secure evaluation places $(X_1, X_2) \in F_q^2$ for $(2, 2, (X_1, X_2))$-Shamir secret sharing over finite field F_q with characteristic $p \geqslant 2$ against the single block leakage from every share.

Consider the finite field $F_q = F_{p^d}$ where $d \in \{2, 3, \ldots\}$. We will interpret F_q as $F_p[\zeta]/\Pi(\zeta)$, where $\Pi(\zeta)$ is an irreducible degree-d F_p-polynomial. Every element $\vec{x} \in F$ can be written as a length-d vector of F_p elements. We represent $x \in F$ as $\vec{x} = (x_0, x_1, \ldots, x_{d-1}) \in (F_p)^d$ when $x = x_0 + x_1\zeta + \cdots + x_{d-1}\zeta^{d-1}$. We define the *single block leakage* function $\ell_i^{\text{block}} \colon F \to F_p$ as the $\lceil \log_2(p) \rceil$-bit physical leakage function that leaks the i-th coefficient $x_i \in F_p$ for $\vec{x} \in F$, i.e. $\ell_i^{\text{block}}(\vec{x}) = x_i$. Our goal is to show that $(2, 2, (X_1, X_2))$-Shamir secret sharing scheme is secure against the single block leakage if $X_1^{-1}X_2 \notin F_p \subseteq F_q$.

Theorem 6. *Let F be a finite field with characteristic $p \geqslant 2$. Consider the $(2, 2, (X_1, X_2))$-Shamir secret-sharing scheme over F and the block physical bit leakage function $\vec{\ell}^{\text{block}} = (\ell_i^{\text{block}}, \ell_j^{\text{block}})$ where $\ell_1^{\text{block}}, \ell_2^{\text{block}} \colon F \to F_p$. For any secret $s \in F$, if $X_1^{-1} \cdot X_2 \notin F_p \subseteq F$,*

$$\mathsf{SD}\left(\vec{\ell^{\text{block}}}(0)\ , \ \vec{\ell^{\text{block}}}(s) \right) = 0.$$

Theorem 6 implies that all pair of evaluation places $(X_1, X_2) \in F_q^2$ satisfying $X_1^{-1} \cdot X_2 \notin F_p \subseteq F$ are perfectly secure against single block leakage attack. Figure 2 shows a test to identify secure evaluation places $(X_1, X_2) \in F_q^2$ for $(2, 2, (X_1, X_2))$-Shamir secret sharing over finite field F_q with characteristic $p \geqslant 2$ against the single block leakage from every share. Note that the algorithm outpus secure for at least $1 - d^2p/q$ fraction of evaluation places.

Input. Distinct evaluation places $X_1, X_2 \in F$, and p is a prime

Output. Decide whether the evaluation places (X_1, X_2) are secure to all single-block leakage attacks.

Preprocessing.

1. For $i \in \{0, 1, \ldots, d-1\}$:
   (a) Compute the shift factor $\eta^{(i,0)}$ as defined in Proposition 4
2. $B = \emptyset$
3. For $u, v \in \{\eta^{(0,0)}, \eta^{(1,0)}, \ldots, \eta^{(d-1,0)}\}$:
   (a) Compute $B \leftarrow B \cup (uv^{-1}) \cdot F_p$

Test.

1. If $X_1^{-1}X_2 \notin B$, return secure. Else, return insecure

Figure 2: Identify secure evaluation places for Shamir's secret-sharing scheme against all single-block leakage attacks.

11.1 Proof of Theorem 6

Let $C_i := \{\vec{x} \in F : x_i = 0\}$ be the set of elements in F whose leakage on the i-th block is $\ell_i^{\text{block}}(\vec{x}) = 0$. For all $i, j \in \{0, 1, \ldots, d-1\}$, Proposition 4 establishes a linear map from C_i to C_j through multiplication with an element $\eta^{(i,j)} \in F$ such that $C_i \cdot \eta^{(i,j)} = C_j$. Then, for $i \in \{0, 1, \ldots, d-1\}$, there exists $\eta^{(i)} \in F_q$ that can shift leakage on the i-block to leakage on the 0-th block, i.e. $(x)_i = \left(x \cdot \eta^{(i)}\right)_0$ for all $x \in F_q$.

Therefore,

$$
\begin{aligned}
&\mathsf{SD}\left(\vec{\ell}^{\text{block}}(0)\ ,\ \vec{\ell}^{\text{block}}(s)\right) \\
&= \frac{1}{2}\sum_{\vec{t}\in F_p^2}\left|\Pr_{\vec{s}\leftarrow \mathsf{Share}^{\vec{X}}(0)}[\vec{\ell}^{\text{block}}(\vec{s}) = \vec{t}] - \Pr_{\vec{s'}\leftarrow \mathsf{Share}^{\vec{X}}(s)}[\vec{\ell}^{\text{block}}(\vec{s'}) = \vec{t}]\right| \\
&= \frac{1}{2}\sum_{\vec{t}\in F_p^2}\left|\Pr_Q[\ell_i^{\text{block}}(Q) = t_1, \ell_j^{\text{block}}(X_2X_1^{-1}\cdot Q) = t_2] - \right. \\
&\qquad\qquad \left. \Pr_Q[\ell_i^{\text{block}}(Q) = t_1, \ell_j^{\text{block}}(X_2X_1^{-1}\cdot Q + s') = t_2]\right| \\
&\qquad\qquad\qquad (s\cdot(1 - X_2X_1^{-1}) \mapsto s', \text{ by Proposition 7}) \\
&= \frac{1}{2}\sum_{\vec{t}\in F_p^2}\left|\Pr_Q\left[\ell_0^{\text{block}}\left(Q\cdot\eta^{(i)}\right) = t_1, \ell_0^{\text{block}}\left(X_2X_1^{-1}\cdot Q\cdot\eta^{(j)}\right) = t_2\right] - \right.
\end{aligned}
$$

$$\Pr_{Q}\left[\ell_0^{\text{block}}\left(Q\cdot\eta^{(i)}\right)=t_1,\ell_0^{\text{block}}\left(X_2X_1^{-1}\cdot Q\cdot\eta^{(j)}+s''\right)=t_2\right]\Bigg|$$

(By Proposition 4 and renaming $s'\cdot\eta^{(j)}\mapsto s''$)

$$=\frac{1}{2}\sum_{\vec{t}\in F_p^2}\Bigg|\Pr_{P}\left[\ell_0^{\text{block}}(P)=t_1,\ell_0^{\text{block}}\left(X_2X_1^{-1}\cdot P\cdot\eta^{(j)}\eta^{(i)^{-1}}\right)=t_2\right]-$$

$$\Pr_{P}\left[\ell_0^{\text{block}}(P)=t_1,\ell_0^{\text{block}}\left(X_2X_1^{-1}\cdot P\cdot\eta^{(j)}\eta^{(i)^{-1}}+s''\right)=t_2\right]\Bigg|$$

($Q\cdot\eta^{(i)}\mapsto P$)

$$=\frac{1}{2}\sum_{\vec{t}\in F_p^2}\Bigg|\Pr_{P}\left[\ell_0^{\text{block}}(P)=t_1,\ell_0^{\text{block}}(P\cdot\beta(i,j))=t_2\right]-$$

$$\Pr_{P}\left[\ell_0^{\text{block}}(P)=t_1,\ell_0^{\text{block}}\left(P\cdot\beta(i,j)+s''\right)=t_2\right]\Bigg|$$

($\beta(i,j):=\alpha_2\alpha_1^{-1}\cdot\eta^{(j)}(\eta^{(i)})^{-1}$)

$$=\frac{1}{2}\sum_{\vec{t}\in F_p^2}\Bigg|\Pr_{P}\left[\ell_0^{\text{block}}(P\cdot\beta(i,j))=t_2|\ell_0^{\text{block}}(P)=t_1\right]\cdot\Pr_{P}\left[\ell_0^{\text{block}}(P)=t_1\right]-$$

$$\Pr_{P}\left[\ell_0^{\text{block}}\left(P\cdot\beta(i,j)+s''\right)=t_2|\ell_0^{\text{block}}(P)=t_1\right]\cdot\Pr_{P}\left[\ell_0^{\text{block}}(P)=t_1\right]\Bigg|$$

(Bayes Rule)

Fix the leakage $t\in F_p$. Define $C_0=\{x\in F_q:\ x_0=0\}$. We know that P is a uniformly random sample from the set $C_0+t\subseteq F_q$. By Lemma 9 and Corollary 3, for any $\beta\in F_q\setminus F_p$, when x sampled uniformly at random from C_0+t, x_0 is uniformly distributed over F_p. We conclude that the leakage distribution $\ell_0^{\text{block}}(P\cdot\beta(i,j)+s'')$ is uniformly at random over F_p, conditioned on the leakage from the first share being t.

Therefore, the joint leakage distribution $\left(\ell_0^{\text{block}}(P),\ell_0^{\text{block}}(P\cdot\beta(i,j))\right)$ is uniformly distributed over $(F_p)^2$, regardless of secret s, as long as

$$\beta(i,j):=X_2X_1^{-1}\cdot\eta^{(i)}(\eta^{(j)})^{-1}\in F_q\setminus F_p.$$

The following proposition states that for single block leakage function, the leakage distribution when sharing a secret $s\in F_q$ with evaluation places $(X_1,X_2)\in F_q^2$ is identical to the leakage distribution on $(Q,X_2X_1^{-1}\cdot Q+s')$ where Q is a random element from F_q and $s'=s\cdot(1-X_2X_1^{-1})\in F_q$

11.2 Additional Technical result

Proposition 7. *Consider evaluation places $\vec{X}=(X_1,X_2)\in F_q^2$. For $i,j\in\{0,1,\ldots,d-1\}$, let $\vec{\ell}^{\text{block}}=(\ell_i^{\text{block}},\ell_j^{\text{block}})$ where $\ell_i^{\text{block}},\ell_j^{\text{block}}\colon F\to F_p$ are the single block leakage functions. For a secret $s\in F_q$ and leakage $\vec{t}\in F_p^2$,*

$$\Pr_{\vec{s}\leftarrow\mathsf{Share}^{\vec{X}}(s)}[\vec{\ell}^{\text{block}}(\vec{s})=\vec{t}]=\Pr_{Q\leftarrow F_q}[\ell_i^{\text{block}}(Q)=t_1,\ell_j^{\text{block}}(X_2X_1^{-1}\cdot Q+s')=t_2]$$

where $s'=s\cdot(1-X_2X_1^{-1})\in F_q$.

Proof. The proof follows from straight forward variable renaming.

$$
\begin{aligned}
&\Pr_{\vec{s} \leftarrow \mathsf{Share}^{\vec{X}}(s)}[\vec{\ell}^{\text{block}}(\vec{s}) = \vec{t}] \\
&= \mathop{\mathbb{E}}_{P}\left[\mathbb{1}_{(\ell_i^{\text{block}})^{-1}(t_1)}(X_1 \cdot P + s) \cdot \mathbb{1}_{(\ell_j^{\text{block}})^{-1}(t_2)}(X_2 \cdot P + s)\right] \\
&= \mathop{\mathbb{E}}_{Q}\left[\mathbb{1}_{(\ell_i^{\text{block}})^{-1}(t_1)}(Q) \cdot \mathbb{1}_{(\ell_j^{\text{block}})^{-1}(t_2)}(X_2 X_1^{-1} \cdot (Q - s) + s)\right] && (X_1 \cdot P + s \mapsto Q) \\
&= \mathop{\mathbb{E}}_{Q}\left[\mathbb{1}_{(\ell_i^{\text{block}})^{-1}(t_1)}(Q) \cdot \mathbb{1}_{(\ell_j^{\text{block}})^{-1}(t_2)}(X_2 X_1^{-1} \cdot Q + (1 - X_2 X_1^{-1}) \cdot s)\right] \\
&= \Pr_{Q}[\ell_i^{\text{block}}(Q) = t_1, \ell_j^{\text{block}}(X_2 X_1^{-1} \cdot Q + s') = t_2] && ((1 - X_2 X_1^{-1}) \cdot s \mapsto s')
\end{aligned}
$$

□

12 Proof of Lemma 10

In this lemma, we interchangeably represent $Y \in F_q$ as an element of $(F_p)^d$, where $q = p^d$ and $d \in \{1, 2, \ldots\}$. Suppose $F_q \cong F_p[\zeta]/\Pi(\zeta)$, where $\Pi(\zeta)$ is an arbitrary monic irreducible F_p-polynomial of degree d. So, an element $Y \in F_q$ is identical to a polynomial $Y_0 + Y_1\zeta + \cdots + Y_{d-1}\zeta^{d-1}$ and is equivalently written as the vector $(Y_0, Y_1, \ldots, Y_{d-1}) \in (F_p)^d$. In particular, for $Y \in F_q$, $Y_i \in F_p$ represents the coefficient of ζ^i in the polynomial representation, for $i \in \{0, 1, \ldots, d-1\}$.

Lemma 11. *The set of vectors $\{Y^{(1)}, Y^{(2)}, \ldots, Y^{(n)}\} \subseteq (F_p)^d$ is F_p-linearly independent, for arbitrary elements $Y^{(1)}, Y^{(2)}, \ldots, Y^{(n)} \in F_q$ and $n \in \{1, 2, \ldots\}$. Then, for uniformly random $Q \in F_q$, the joint distribution $\left(\left(QY^{(1)}\right)_0, \left(QY^{(2)}\right)_0, \ldots, \left(QY^{(n)}\right)_0 \right)$ is uniformly random over $(F_p)^n$.*

Proof. At the outset, our objective is to formalize the linear map $Q \longmapsto (QY)_0$ behaves for $Q, Y \in F_q$, where $q = p^d$. Note that it is identical to the map

$$
(Q_0, Q_1, \ldots, Q_{d-1}) \longmapsto \left((Q_0, Q_1, \ldots, Q_{d-1}) \cdot \begin{pmatrix} (Y \cdot 1)_0 & (Y \cdot 1)_1 & \cdots & (Y \cdot 1)_{d-1} \\ (Y \cdot \zeta)_0 & (Y \cdot \zeta)_1 & \cdots & (Y \cdot \zeta)_{d-1} \\ \vdots & \vdots & \ddots & \vdots \\ (Y \cdot \zeta^{d-1})_0 & (Y \cdot \zeta^{d-1})_1 & \cdots & (Y \cdot \zeta^{d-1})_{d-1} \end{pmatrix} \right)_0
$$

In the matrix above, we clarify that $(Y \cdot \zeta^i)_j$ represents the coefficient of ζ^j in the polynomial representation of the product of $Y \in F_q$ and $\zeta^i \in F_q$. So, the $Q \longmapsto (Q \cdot Y)_0$ map is equivalent to the $F_q \longmapsto F_p$ linear map:

$$
Q \equiv (Q_0, Q_1, \ldots, Q_{d-1}) \longmapsto Q_0 \cdot (Y \cdot 1)_0 + Q_1 \cdot (Y \cdot \zeta)_0 + \cdots + Q_{d-1} \cdot \left(Y \cdot \zeta^{d-1}\right)_0 \tag{2}
$$

Now, we begin proving the lemma. We are given $Y^{(1)}, Y^{(2)}, \ldots, Y^{(n)} \in F_q$. Each $Y^{(i)} \in F_q$ is equivalently interpreted as $(Y_0^{(i)}, Y_1^{(i)}, \ldots, Y_{d-1}^{(i)}) \in (F_p)^d$, where $i \in \{1, 2, \ldots, n\}$. We are given that the following set of $(F_p)^d$ vectors are linearly independent:

$$
\left\{ \left(Y_0^{(i)}, Y_1^{(i)}, \ldots, Y_{d-1}^{(i)}\right) \;:\; i \in \{1, 2, \ldots, n\} \right\}
$$

Our aim is to prove that, for uniformly random $Q \in F_q$, the following joint distribution is the uniform distribution over $(F_p)^n$.

$$
\left(\left(QY^{(1)}\right)_0, \left(QY^{(2)}\right)_0, \ldots, \left(QY^{(n)}\right)_0 \right).
$$

Note that this joint distribution is identical to the following distribution, where $Q_0, Q_1, \ldots, Q_{d-1} \in (F_p)^d$ are chosen uniformly and independently at random (due to Equation 2).

$$\left(Q_0, \quad Q_1, \quad \ldots, \quad Q_{d-1}\right) \cdot \begin{pmatrix} (Y^{(1)} \cdot 1)_0 & (Y^{(2)} \cdot 1)_0 & \ldots & (Y^{(n)} \cdot 1)_0 \\ (Y^{(1)} \cdot \zeta)_0 & (Y^{(2)} \cdot \zeta)_0 & \ldots & (Y^{(n)} \cdot \zeta)_0 \\ \vdots & \vdots & \ddots & \vdots \\ (Y^{(1)} \cdot \zeta^{d-1})_0 & (Y^{(2)} \cdot \zeta^{d-1})_0 & \ldots & (Y^{(n)} \cdot \zeta^{d-1})_0 \end{pmatrix}$$

Therefore, it is equivalent to proving that the following set of vectors is linearly independent:

$$\left\{ \left(\left(Y^{(i)} \cdot 1\right)_0, \left(Y^{(i)} \cdot \zeta\right)_0, \ldots, \left(Y^{(i)} \cdot \zeta^{d-1}\right)_0 \right) \; : \; i \in \{1, 2, \ldots, n\} \right\}.$$

Toward this objective, it suffices to prove that the following $(F_p)^d \longmapsto (F_p)^d$ is a full-rank map:

$$(Y_0, Y_1, \ldots, Y_{d-1}) \longmapsto \left((Y \cdot 1)_0, (Y \cdot \zeta)_0, \ldots, \left(Y \cdot \zeta^{d-1}\right)_0 \right). \tag{3}$$

Let $\Pi(\zeta) = \zeta^d - \Pi_{d-1}\zeta^{d-1} - \Pi_{d-2}\zeta^{d-2} - \cdots - \Pi_0$ be the irreducible polynomial, where $\Pi_0, \Pi_1, \ldots, \Pi_{d-1} \in F_p$. Here is an essential observation. For $i \in \{1, 2, \ldots, d-1\}$ the following identity holds:

$$\left(\zeta^i \cdot \zeta^{d-i}\right)_0 = \Pi_0 \neq 0.$$

Using this essential observation, Equation 3 establishes the following maps of the basis vectors.

$$\begin{aligned} (1, 0, 0, \ldots, 0) &\longmapsto (1, 0, 0, \ldots, 0, 0) \\ (0, 1, 0, \ldots, 0) &\longmapsto (0, 0, 0, \ldots, 0, \Pi_0) \\ (0, 0, 1, \ldots, 0) &\longmapsto (0, 0, 0, \ldots, \Pi_0, *) \\ &\vdots \\ (0, 0, 0, \ldots, 1) &\longmapsto (0, \Pi_0, *, \ldots, *, *) \end{aligned}$$

In the maps above, $*$ elements represent arbitrary elements of F_p. Let $A \in (F_p)^{d \times d}$ be the matrix such that for all $Y_0, Y_1, \ldots, Y_{d-1} \in F_p$ and $Y = Y_0 + Y_1\zeta + \cdots Y_{d-1}\zeta^{d-1} \in F_q$, the following identity is satisfied.

$$(Y_0, Y_1, \ldots, Y_{d-1}) \cdot A = \left((Y \cdot 1)_0, (Y \cdot \zeta)_0, \ldots, \left(Y \cdot \zeta^{d-1}\right)_0 \right).$$

From the basis maps above, we conclude that the matrix $A \in (F_p)^{d \times d}$ has the following structure.

$$A = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & \Pi_0 \\ 0 & 0 & 0 & \cdots & \Pi_0 & * \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \Pi_0 & * & \cdots & * & * \end{pmatrix}$$

This structure shows that the matrix A has full rank, whence the lemma. $\square$