Partial Derandomization for Leakage-Resilient Shamir's Secret Sharing over Composite Order Fields

S. Venkitesh
Institute for the Theory of Computing, The Stein Faculty of Computer and Information Science, Ben Gurion University of the Negev, Beersheva, Israel

Abstract

We make progress on the question of constructing explicit evaluation places for leakage-resilient Shamir's secret sharing, over composite order fields. Previously, Maji et al. (EUROCRYPT 2024) showed that random evaluation places yield Shamir's secret sharing over the composite order field $\mathbb{F}_{p^d}$ that is statistically secure against physical bit leakage. Later, Nguyen (EUROCRYPT 2025) established a *dichotomy* that linear code-based secret-sharing scheme over the field $\mathbb{F}_{p^d}$ is either statistically secure or completely insecure against such leakage.

Building upon Nguyen's dichotomy, we present a partial derandomization of evaluation places, improving upon the Maji et al. result for a restricted regime of parameters. We replace the random choice of n independent evaluation places by the iterates $x_j = \Phi^j(x_0)$ of a simple fixed rational function Φ, where the initial point $x_0 \in \mathbb{F}_{p^d}^*$ is randomly chosen. The randomness in the evaluation places thus drops from $nd \log p$ bits to $d \log p$ bits. Our construction is valid for the regime $n = O(d/\log_p d)$, and any reconstruction threshold $k \geq 2$; in fact, the scheme attains perfect security (statistical distance exactly zero) against single-block leakage.

Building on Nguyen's dichotomy, our technique is a partial-fraction non-degeneracy argument that exploits the distinct poles of the rational iterates.

2012 ACM Subject Classification Theory of computation → Cryptographic primitives; Security and privacy → Cryptanalysis and other attacks

Keywords and phrases Shamir's secret sharing, leakage resilience, physical bit probing, physical bit leakage, secure evaluation places, rational functions

Digital Object Identifier 10.4230/LIPIcs.ITC.2026.12

Related Version *Full Version*: `https://eprint.iacr.org/2026/1475`

Acknowledgements The author thanks the anonymous reviewers of ITC 2026 for critical feedback, as well as for pointing to [20] and the dichotomy result therein.

1 Introduction

Threshold secret-sharing schemes, such as Shamir's scheme [21], distribute a secret among n parties so that any k of them can reconstruct the secret, while any fewer than k parties learn nothing about it. In the standard corruption model, an adversary obtains the complete shares of some parties and has no information about the remaining shares.

Side-channel attacks have repeatedly circumvented this all-or-nothing assumption. Rather than corrupting entire shares, a side-channel adversary accumulates small amounts of information, like individual bits, power traces, and timing signals, from *all* shares simultaneously (see Ishai, Sahai, and Wagner [10]). The mathematical abstraction of such threats is *independent local leakage*: the adversary applies a bounded function to each share independently and observes only the outputs. The study of locally leakage-resilient secret sharing was initiated by Benhamouda, Degwekar, Ishai, and Rabin [4] and is also implicit in the work of Goyal and Kumar [7].

A particularly natural leakage model, introduced by [10], probes *physical bits* in the memory storing each share. Since elements of a finite field $\mathbb{F}_{p^d}$ are stored as d coordinates over $\mathbb{F}_p$, each represented as a $\lceil \log_2 p \rceil$-bit binary string, a physical bit probe extracts a single bit from this representation. Additive secret sharing is known to be vulnerable to such probes: the parity-of-parities attack of Maji, Nguyen, Paskin-Cherniavsky, Suad, and Wang [15] leaks the least significant bit of each share and distinguishes secrets with advantage $(2/\pi)^n$ over any prime field $\mathbb{F}_p$. Over characteristic-2 fields, this attack can distinguish secrets 0 and 1 with certainty. Shamir's secret sharing inherits these vulnerabilities if its evaluation places are chosen carelessly ([15], and Costes and Stam [5]).

The question, then, is whether Shamir's scheme can be instantiated to resist physical bit probes. Over prime fields, [15] showed that choosing evaluation places uniformly at random yields a leakage-resilient scheme with high probability. Maji, Nguyen, Paskin-Cherniavsky, and Ye [17] extended this randomized construction to composite order fields, particularly fields of characteristic 2, and also gave an exact security classifier for $k = 2$ against single-block leakage. However, no explicit evaluation places were known for $k > 2$ or for the general block-leakage regime over composite fields. Even for $k = 2$, the classifier of [17] certifies individual evaluation-place tuples but does not produce a closed form family. Separately, Hwang, Maji, Nguyen, and Ye [9] initiated the study of explicit constructions over prime fields, providing classifiers and derandomized evaluation places for Mersenne and Fermat primes in the full-threshold regime $n = k$.

In this work, we present a partial derandomization of [17]. Building on the dichotomy of Nguyen [20], which establishes that any linear code-based secret-sharing scheme over the field $\mathbb{F}_{p^d}$ is either statistically secure or completely insecure against physical bit leakage, we replace the random choice of n independent evaluation places by a structured one-parameter family: the evaluation places are $x_j = \Phi^j(x_0)$, where $\Phi(x) := \alpha x/(x+1)$, α is a fixed multiplicative generator of $\mathbb{F}_{p^d}^*$, and $x_0 \in \mathbb{F}_{p^d}^*$ is a randomly chosen *base point*. As it turns out, Φ is a *Möbius transformation*, and the utility of such structured algebraic transformations in defining evaluation places seems unexplored so far. The randomness needed to specify the n evaluation places drops from $nd \log p$ bits to $d \log p$ bits, required to choose the base point x_0. The above mentioned dichotomy argument reduces the security question to a full-rank condition on a test matrix, which we verify for our chosen points by observing a non-degeneracy property that exploits the distinct poles of the iterates.

The dichotomy itself is implicit, for the case $k = 2$, in the linear-algebraic arguments of [17], and [20] later extends this to the case of general k, as well as to general linear code-based secret sharing. We also give an alternative direct derivation of the dichotomy in our setting for completeness, in Appendix A.

1.1 Motivation

The problem of *derandomization of evaluation places* is the central motivation for our work.

The randomized constructions of [15, 17] demonstrate that most evaluation places are secure. In practice, however, they require trusted public randomness, for instance a randomness beacon, to select the places. An adversary who can influence the random seed may steer the construction toward vulnerable evaluation places, unbeknownst to the honest parties. This concern is not merely theoretical; the NIST standardization effort for threshold cryptographic schemes (see Brandão and Peralta [1]), and the practical deployment considerations studied by Faust, Masure, Micheli, Orlt, and Standaert [6] both underscore the need for deterministic, verifiable instantiations.

Ideally, one would like evaluation places that are fixed by the field specification alone, with a proof that they resist physical bit probes. Towards this, [9] initiated the study of classifier and derandomization constructions over prime fields. Their techniques, however, are inherently tied to the structure of prime fields: they exploit square wave orthogonality and 2-adic valuations of rational approximations, both of which rely on the nonlinearity of the bit-extraction map over $\mathbb{F}_p$. Over composite fields $\mathbb{F}_{p^d}$ with $d \geq 2$, the analogous coordinate-extraction map is $\mathbb{F}_p$-linear, and the Fourier-analytic machinery of [9] does not apply. The present work exploits this linearity to make partial progress on the derandomization problem in the composite-field setting; the precise results are stated in Section 1.2.

1.2 Our results

We work over $\mathbb{F} = \mathbb{F}_{p^d}$, where p is any prime and $d \geq 2$. Fix a primitive polynomial $\Pi(t) \in \mathbb{F}_p[t]$ of degree d, and let α be a root of Π in $\mathbb{F}$, so that $\mathrm{ord}(\alpha) = p^d - 1$ and $\mathbb{F} = \mathbb{F}_p[\alpha]$ with canonical basis $\mathcal{B} = \{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$.

Our construction is based on a rational function. Define the *step operator*

$$\Phi(x) = \frac{\alpha x}{x+1},$$

which is a Möbius transformation on the projective line $\mathbb{P}^1(\mathbb{F}) := \mathbb{F} \cup \{\infty\}$ with projective order $p^d - 1$. Our evaluation places are the iterates

$$x_j = \Phi^j(x_0), \quad j = 0, 1, \ldots, n-1,$$

where Φ^j denotes the j-th iterate of Φ under composition, applied to a base point $x_0 \in \mathbb{F}^*$.

The choice of Φ is not arbitrary. The single structural property of the orbit that drives the entire security analysis is that the iterates $\Phi^0, \Phi^1, \ldots, \Phi^{n-1}$, viewed as Möbius transformations on the projective line $\mathbb{P}^1(\mathbb{F})$, have *pairwise distinct finite poles*. This pole-distinctness is what powers the partial-fraction non-degeneracy argument in Section 4. In fact, motivated from the construction of *folded Reed-Solomon codes* [8], which are polynomial codes that can be *list decoded* up to the information theoretic limit, a more obvious and simpler candidate is $\Psi(x) = \alpha x$. Here, every iterate $\Psi^j(x) = \alpha^j x$ is a pure dilation with its only pole at ∞. So the iterates share a single common pole and the partial-fraction argument collapses entirely. We make this contrast precise in Remark 3.6. The role of the $+1$ in the denominator of Φ is therefore not cosmetic; it perturbs each iterate's pole to a distinct finite point of $\mathbb{F}^*$, placing the orbit in sufficiently generic position so that a good bad-set bound becomes possible.

Our main results are as follows.

▶ **Theorem 1.1** (Perfect security against single-block leakage)**.** *Let p be any prime, $d \geq 2$, $k \geq 2$, and $k \leq n \leq d(k-1)$ with $n \leq p^d - 1$. Let α be a multiplicative generator of $\mathbb{F}_{p^d}^*$ and $\Phi(x) = \alpha x/(x+1)$. There exists a set* $\mathrm{Bad} \subset \mathbb{F}_{p^d}^*$ *with*

$$|\mathrm{Bad}| \leq n + n(dp)^n$$

such that for any $x_0 \in \mathbb{F}_{p^d}^* \setminus \mathrm{Bad}$, the evaluation places $\vec{X} = (x_0, \ldots, x_{n-1})$ give a scheme $\mathrm{ShamirSS}(n, k, \vec{X})_{\mathbb{F}_{p^d}}$ *that is* perfectly secure *against all single-$\mathbb{F}_p$-block leakage patterns.*

In particular, the scheme is perfectly secure against all single-physical-bit-per-share leakage (for any p), and against any leakage that applies an arbitrary function $g_j : \mathbb{F}_p \to S_j$ to a single $\mathbb{F}_p$-block of each share, where $S_0, \ldots, S_{n-1}$ are arbitrary nonempty finite sets.

A good base point x_0 exists whenever $d > n(1 + \log_p d) + O(\log_p n)$, giving a practical range of $n = O(d/\log_p d)$ parties.

Table 1 Comparison of our results with the randomized results of [17, 20]. Here $2 \le k \le n$.

Aspect	[17]	[20]	**This work**
Evaluation places	Random in $(\mathbb{F}^*)^n$	Fixed; arbitrary	$\Phi^j(x_0)$ orbit
Multipliers v_i (in shares $v_i P(X_i)$)	All 1	Random in $(\mathbb{F}^*)^n$	All 1
Security guarantee	$\epsilon = 2^{-\Omega(d)}$	$\epsilon = 2^{-\Omega(d)}$	SD $= 0$ for $x_0 \notin$ Bad
Max parties (general k)	$O(dk/\log_p d)$	$O(dk/\log_p d)$	$O(d/\log_p d)$
Multi-block, $M < d$	$\epsilon = 2^{-\Omega(d)}$	$\epsilon = 2^{-\Omega(d)}$	Perfect (fixed pattern)
Random bits in evaluation places	$nd \log p$	0	$d \log p$ (for x_0)
Random bits in multipliers	0	$nd \log p$	0

The security guarantee is *perfect*: the statistical distance is zero, not merely exponentially small. Within the parameter range $n = O(d/\log_p d)$, this is a qualitative strengthening of the statistical security $\epsilon = 2^{-\Omega(d)}$ achieved by the randomized constructions of [17, 20]. The trade-off is on party count: [17, 20] support $n = O(dk/\log_p d)$ parties versus our $n = O(d/\log_p d)$, reflecting the cost of restricting the evaluation places to a one-parameter family.

The construction is a partial derandomization. Once a base point x_0 is fixed, the evaluation places $x_j = \Phi^j(x_0)$ are determined by the field representation alone; the randomness needed to specify the n places thus drops from $nd \log p$ bits (for n independent random places, as in [17]) to $d \log p$ bits needed to fix the single $x_0 \in \mathbb{F}^*$. In the headline regime, $x_0 = \alpha$ is a structured candidate; whether it is good depends on the choice of primitive polynomial Π and is certified by Algorithm 1 (Section 3.3), a sound test whose GOOD verdict guarantees perfect security, with the same worst-case runtime as the classifying algorithm of [20].

For multi-block leakage, we prove the following.

▶ **Theorem 1.2** (Multi-block leakage, improved bound)**.** *Under the hypotheses of Theorem 1.1, fix an admissible multi-block leakage pattern with $M < d - \log_p(2n)$ total $\mathbb{F}_p$-blocks leaked. Then the bad set has size $\le n + n \cdot p^M$, and a good x_0 always exists.*

For universality over all admissible multi-block patterns with $\le M$ blocks total, we get the bound $|\text{Bad}| \le n + n(dpe)^M$, and a good x_0 exists when $M = O(d/\log_p d)$.

For the proof, we observe that the Vandermonde has nontrivial kernel, and the direct bound from Theorem 5.3 is used; obtaining a polynomial bound for this regime remains open (Section 1.6).

1.3 Comparison with prior work

Table 1 summarizes the comparison with [17, 20], and a few gaps remain. First, there is a factor-k loss in the maximum number of parties for large k; we conjecture this loss is inherent to single-parameter constructions, but leave the question open (Section 1.6). Second, multi-block universality is limited to $M = O(d/\log_p d)$ by the pattern enumeration bottleneck. Closing these gaps, particularly by obtaining a polynomial bad-set bound, is an interesting direction for future work; see Section 1.6.

1.4 Related work

We survey the most relevant prior results.

Leakage-resilient secret sharing

[3, 4] proved that Shamir's scheme is leakage-resilient against arbitrary single-bit local leakage when k/n exceeds a constant threshold. Subsequent works [16, 12, 19] improved this threshold, with the current best being $k \geq 0.69n$. These results hold for *all* evaluation places but require a large reconstruction-to-party ratio. Among other lines of work that bring linear algebraic structure to bear on these problems, Koga and Abe [13] determine tight bounds on the local leakage resilience of the additive (n, n)-threshold scheme via the eigenvalues of circulant matrices.

The complementary regime (small k relative to n) is where the choice of evaluation places becomes critical. [15] initiated the study of this regime over prime fields, and [17] extended it to composite fields. Other constructions of leakage-resilient (non-Shamir) secret sharing, including those based on algebraic geometry codes, appear in [14, 18] and the references therein.

Physical bit probing and the [17] framework

The closest prior randomized construction we improve upon is [17]. Their construction works over $\mathbb{F}_{p^d}$ for any prime p and combines three ingredients: (i) a Fourier-analytic upper bound on statistical distance in terms of dual GRS codewords and Fourier coefficients of block-indicator functions, (ii) a Bézout-type bound on simultaneous zeros of polynomial systems over composite fields [22, 2], and (iii) a generalized Vandermonde determinant analysis.

They also proved an exact security classifier for $k = 2$. Both the dichotomy at $k = 2$ and its proof technique (linear algebra plus the cosets-of-subspaces structure) are the entry point for our test-matrix derivation.

The dichotomy result of [20]

A perfect-or-completely-insecure dichotomy for any linear code-based secret-sharing scheme was given by [20], over a binary extension field against arbitrary physical bit leakage, along with a complete characterization of the insecure leakages via minimal codewords of the dual of the binary image. A remark therein also explicitly extends both results to composite order fields $\mathbb{F}_{p^d}$ and to subfield-coordinate leakage, which is the present setting. The work also gives a classifying algorithm whose worst-case cost matches our verification cost (Proposition 3.12). Beyond the dichotomy, [20] gives a Monte-Carlo construction of GRS-based linear code-based secret sharing with random multipliers and fixed evaluation places, achieving $M \leq (k-1)\lambda/\mathrm{poly}(\log \lambda)$ bits of physical bit leakage tolerance with overwhelming probability over the multiplier choice.

Our contribution is complementary to [20] on the construction side. We give a construction of evaluation places $x_j = \Phi^j(x_0)$ using a suitable rational function Φ, that fixes both the multipliers (all equal to 1, as in standard Shamir's scheme) and the evaluation places to a one-parameter family, with the security question reducing (via the dichotomy of [20]) to a closed form bad-set bound on the base point x_0. The trade-off is on party count: [20] supports $n = O(dk/\log_p d)$ parties, and we support $n = O(d/\log_p d)$ parties.

Explicit constructions over prime fields

[9] constructed efficient classifiers for evaluation places over Mersenne and Fermat primes in the $n = k$ regime, connecting leakage resilience to orthogonality of square wave functions and 2-adic valuations of rational approximations. They provide explicit secure evaluation places for $n = k = 2$ and lift to $n = k > 2$ via a Fourier-analytic theorem. Their techniques are specific to prime fields, where bit extraction is a nonlinear map. Over composite fields, the analogous map is $\mathbb{F}_p$-linear, enabling a fundamentally different (and in several respects simpler) approach.

1.5 Technical overview

The proof proceeds in three phases. We outline each here.

Phase 1: The perfect dichotomy (Section 2)

The key structural observation is that the coordinate extraction map $(\cdot)_i : \mathbb{F} \to \mathbb{F}_p$, defined by $(x)_i = \mathrm{Tr}(x \cdot f_i^*)$ where $\{f_i^*\}$ is the dual basis with respect to the field trace, is $\mathbb{F}_p$-linear. It follows that the leakage map $L_{\vec{i}} : \mathbb{F}^{k-1} \to \mathbb{F}_p^n$ is $\mathbb{F}_p$-linear.

This has a clean consequence. By the structure of cosets of $\mathbb{F}_p$-subspaces, the leakage distribution for secret s is uniform over a coset of $\mathrm{Im}(L_{\vec{i}})$. Two cosets are either identical or disjoint, yielding the dichotomy $\mathrm{SD} \in \{0, 1\}$. Consequently, surjectivity of $L_{\vec{i}}$, equivalently a test matrix $\Theta_{\vec{i}}$ having full column rank n over $\mathbb{F}_p$, is a *sufficient* condition for perfect security against the pattern $\vec{i}$, since it forces every coset to equal $\mathbb{F}_p^n$. (Perfect security against $\vec{i}$ is in fact the weaker condition that the secret's coordinate vector $((s)_{i_j})_j$ lies in $\mathrm{Im}(L_{\vec{i}})$ for every s, which is the minimal codeword characterization of [20, Theorem 6]; see also [17, Theorem 5] for the $k = 2$ case. We use only the sufficient direction.) An alternative derivation of the dichotomy $\mathrm{SD} \in \{0, 1\}$ in our setting is given in Appendix A. The rank criterion is the working tool for the rest of the proof.

Phase 2: Partial-fraction non-degeneracy (Section 4)

The test matrix $\Theta_{\vec{i}}$ encodes the map $\vec{c} \mapsto (\sum_j c_j \eta^{(i_j)} x_j^\ell)_{\ell=1}^{k-1}$. To show full rank, we must prove that no nontrivial $\mathbb{F}_p$-linear combination $G_\ell(x) = \sum_j c_j \eta^{(i_j)} (\Phi^j(x))^\ell$ vanishes identically.

The argument is a partial-fraction analysis. Since the Möbius transforms $\Phi^0, \Phi^1, \ldots, \Phi^{n-1}$ have pairwise distinct poles (Corollary 3.4), the residue of G_ℓ at each pole is determined by a single summand. This pole-distinctness is the unique structural property of the orbit on which the entire argument hinges; Remark 3.6 shows that the naive alternative $\Psi(x) = \alpha x$ fails exactly here. If $G_\ell \equiv 0$, all coefficients must vanish. The resulting zero count $\leq n\ell$ at the smallest power $\ell = 1$ gives $\leq n$ bad base points per coefficient vector, and a union bound over all patterns and coefficients yields the bad set of Theorem 1.1.

Phase 3: Multi-block extension (Section 5)

For multi-block leakage, the kernel condition involves $\mathbb{F}$-valued coefficients $d_j = \sum_r c_{j,r} \eta^{(i_j^{(r)})}$ arising from within-share linear combinations. The admissibility of the leakage pattern ensures that $d_j \neq 0$ whenever the corresponding $c_{j,r}$ are not all zero. Once this is established, the partial-fraction argument extends directly to $\mathbb{F}$-coefficients.

1.6 Discussion and open problems

It is worth recording what our proofs will actually rely on regarding the step operator Φ.

(1) *Rational function structure:* each Φ^j is a degree-1 rational function, which will enable the partial-fraction analysis in Section 4.

(2) *Distinct poles:* $\Phi^0, \dots, \Phi^{n-1}$ have pairwise distinct poles in $\mathbb{P}^1(\mathbb{F})$, which is the hypothesis driving our non-degeneracy lemma.

Our proofs make no appeal to the Ramanujan spectral gap, the expander mixing lemma, character sum bounds, or any equidistribution property. These tools are available for torus-based constructions (Möbius maps on μ_{q+1}) and could potentially be brought to bear on the open problems below.

Several natural questions remain.

▶ **Open Question 1.3** (Universal multi-block for $2 \le k \le n$ and $M = \omega(d/\log_p d)$)**.** *The pattern enumeration bottleneck limits universality to $M = O(d/\log_p d)$. Can this be overcome?*

▶ **Open Question 1.4** (Polynomial-size bad set)**.** *For a fixed admissible pattern, the Vandermonde matrix of evaluation places has nontrivial kernel, and the bad-set bound $\le n \cdot p^M$ from Theorem 5.3 is exponential in M. Can this be improved to a polynomial bound?*

▶ **Open Question 1.5** (Factor-k gap)**.** *The randomized constructions of [17, 20] handle $n = O(dk/\log_p d)$ parties; our single-parameter construction handles $n = O(d/\log_p d)$. Can this be overcome?*

2 Preliminaries

Throughout, p denotes a prime and $d \ge 2$ an integer. We write $\mathbb{F} = \mathbb{F}_{p^d}$ and $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$. The security parameter is $\lambda = d \log_2 p$.

2.1 The field and coordinates

Fix a primitive polynomial $\Pi(t) \in \mathbb{F}_p[t]$ of degree d. Then $\mathbb{F} = \mathbb{F}_p[t]/\Pi(t)$, and a root α of Π satisfies $\mathrm{ord}(\alpha) = p^d - 1$, i.e., α generates $\mathbb{F}^*$. The canonical basis of $\mathbb{F}$ over $\mathbb{F}_p$ is $\mathcal{B} = \{1, \alpha, \alpha^2, \dots, \alpha^{d-1}\}$. Every $x \in \mathbb{F}$ is uniquely written as $x = \sum_{i=0}^{d-1} x_i \alpha^i$ with $x_i \in \mathbb{F}_p$, and we define the i-th $\mathbb{F}_p$-coordinate of x by $(x)_i := x_i$.

▶ **Definition 2.1** (Dual basis and shifting factors)**.** *Let* $\mathrm{Tr} := \mathrm{Tr}_{\mathbb{F}/\mathbb{F}_p}$ *denote the field trace. The* dual basis *of $\mathcal{B}$ with respect to* Tr *is the unique basis $\{f_0^*, f_1^*, \dots, f_{d-1}^*\}$ of $\mathbb{F}$ over $\mathbb{F}_p$ satisfying $\mathrm{Tr}(\alpha^i \cdot f_j^*) = \delta_{ij}$ for all i, j. The* shifting factors *are $\eta^{(i)} := f_i^*/f_0^*$ for $i = 0, 1, \dots, d-1$.*

In particular, $\eta^{(0)} = 1$. The dual basis exists and is unique because the Gram matrix $G_{ij} = \mathrm{Tr}(\alpha^i \cdot \alpha^j)$ is invertible (by non-degeneracy of the trace form).

▶ **Proposition 2.2** (Shift property)**.** *For all $x \in \mathbb{F}$ and all $i \in \{0, \dots, d-1\}$,*

$$(x)_i = (x \cdot \eta^{(i)})_0.$$

Proof. We compute $(x \cdot \eta^{(i)})_0 = \mathrm{Tr}(x \cdot \eta^{(i)} \cdot f_0^*) = \mathrm{Tr}(x \cdot (f_i^*/f_0^*) \cdot f_0^*) = \mathrm{Tr}(x \cdot f_i^*) = (x)_i$. ◀

▶ **Lemma 2.3** ($\mathbb{F}_p$-independence of shifting factors)**.** *The shifting factors $\eta^{(0)}, \eta^{(1)}, \dots, \eta^{(d-1)}$ are $\mathbb{F}_p$-linearly independent. In fact, they form a basis of $\mathbb{F}$ over $\mathbb{F}_p$.*

Proof. The dual basis $\{f_0^*, \dots, f_{d-1}^*\}$ is a basis of $\mathbb{F}$ over $\mathbb{F}_p$. The map $f_i^* \mapsto \eta^{(i)} = f_i^*/f_0^*$ is multiplication by the nonzero scalar $1/f_0^* \in \mathbb{F}^*$, hence an $\mathbb{F}_p$-linear isomorphism of $\mathbb{F}$. ◀

2.2 Shamir's secret sharing and leakage models

▶ **Definition 2.4** (Shamir's scheme). *Let $2 \le k \le n$. Given distinct evaluation places $x_0, \dots, x_{n-1} \in \mathbb{F}^*$, the scheme* $\mathrm{ShamirSS}(n, k, \vec{X})_{\mathbb{F}}$ *shares a secret $s \in \mathbb{F}$ as follows: sample $P(x) = s + a_1 x + \cdots + a_{k-1} x^{k-1}$ with $a_1, \dots, a_{k-1} \in \mathbb{F}$ uniform and independent, and output shares $s_j = P(x_j)$ for $j = 0, \dots, n-1$.*

▶ **Definition 2.5** (Block leakage). *In the* single-block leakage *model, the adversary learns one $\mathbb{F}_p$-coordinate $(s_j)_{i_j} \in \mathbb{F}_p$ from each share s_j, where the block indices $\vec{i} = (i_0, \dots, i_{n-1}) \in \{0, \dots, d-1\}^n$ are adversary-chosen (non-adaptively). For $p = 2$, each $\mathbb{F}_p$-block is a single bit, so block leakage coincides with physical bit leakage.*

▶ **Definition 2.6** (Multi-block leakage). *In the* multi-block leakage *model, the adversary learns $m_j \ge 1$ distinct $\mathbb{F}_p$-coordinates from share j, at positions $i_j^{(1)}, \dots, i_j^{(m_j)} \in \{0, \dots, d-1\}$. The total number of blocks leaked is $M = \sum_{j=0}^{n-1} m_j$. A multi-block pattern is* admissible *if the block positions within each share are distinct.*

▶ **Definition 2.7** (Insecurity). *The insecurity of* $\mathrm{ShamirSS}(n, k, \vec{X})_{\mathbb{F}}$ *against a leakage family $\mathcal{F}$ is*

$$\epsilon_{\mathcal{F}}(\vec{X}) := \max_{f \in \mathcal{F}} \max_{s \in \mathbb{F}^*} \mathrm{SD}(f(\mathrm{Share}(0)),\ f(\mathrm{Share}(s))),$$

where SD *denotes statistical distance. We say the scheme is* perfectly secure *against $\mathcal{F}$ if $\epsilon_{\mathcal{F}}(\vec{X}) = 0$.*

2.3 The perfect dichotomy

We now record the structural foundation that the rest of the analysis builds on: the coordinate map $(\cdot)_i = \mathrm{Tr}(\cdot \cdot f_i^*)$ is $\mathbb{F}_p$-linear, which makes the leakage map linear, forces the leakage distribution to be uniform on a coset of an $\mathbb{F}_p$-subspace, and yields a perfect dichotomy for statistical distance.

▶ **Proposition 2.8** (Leakage map). *For block leakage with indices $\vec{i}$, the leakage vector $\vec{\ell} = ((s_j)_{i_j})_{j=0}^{n-1}$ decomposes as*

$$\ell_j = (s)_{i_j} + \sum_{t=1}^{k-1} \mathrm{Tr}(a_t \cdot x_j^t \cdot f_{i_j}^*),$$

where the map $L_{\vec{i}} : \mathbb{F}^{k-1} \to \mathbb{F}_p^n$ defined by $L_{\vec{i}}(a_1, \dots, a_{k-1})_j = \sum_{t=1}^{k-1} \mathrm{Tr}(a_t \cdot x_j^t \cdot f_{i_j}^*)$ is $\mathbb{F}_p$-linear. (Proof in Appendix A.)

▶ **Proposition 2.9** (Perfect dichotomy). *For block leakage with indices $\vec{i}$ and any two secrets $s, s' \in \mathbb{F}$:*

$$\mathrm{SD}(\vec{\ell}|_s,\ \vec{\ell}|_{s'}) = \begin{cases} 0 & \text{if } \vec{v}(s) - \vec{v}(s') \in \mathrm{Im}(L_{\vec{i}}) \\ 1 & \text{if } \vec{v}(s) - \vec{v}(s') \notin \mathrm{Im}(L_{\vec{i}}) \end{cases}$$

where $\vec{v}(s) = ((s)_{i_0}, \dots, (s)_{i_{n-1}})$. In particular, if $L_{\vec{i}}$ is surjective, then $\mathrm{SD} = 0$ *for all pairs of secrets. (Proof in Appendix A.)*

▶ Remark 2.10 (More general result in previous work). [20, Theorem 6] establishes Proposition 2.9 in much greater generality: for any linear code-based secret-sharing scheme over an extension field $\mathbb{F}_{p^\lambda}$, against arbitrary physical bit leakage. By a remark therein, the result also applies to composite order fields $\mathbb{F}_{p^d}$ and to subfield-coordinate leakage, which is our present setting. The $k = 2$ case is also implicit, via linear algebra, in [17, Theorem 5]. For completeness, proofs of Propositions 2.8 and 2.9 in our setting are deferred to Appendix A; the rest of the paper depends only on the conclusion of Proposition 2.9.

2.4 Surjectivity and the test matrix

▶ **Proposition 2.11** (Dual characterization). *The map $L_{\vec{i}}$ is surjective if and only if the adjoint $L_{\vec{i}}^* : \mathbb{F}_p^n \to \mathbb{F}^{k-1}$ is injective. The adjoint is given by*

$$(L_{\vec{i}}^*(\vec{c}))_\ell = f_0^* \cdot \sum_{j=0}^{n-1} c_j \cdot \eta^{(i_j)} \cdot x_j^\ell, \qquad \ell = 1, \dots, k-1.$$

Since $f_0^* \neq 0$, injectivity of $L_{\vec{i}}^*$ is equivalent to: for all $\vec{c} \in \mathbb{F}_p^n \setminus \{\vec{0}\}$, there exists $\ell \in \{1, \dots, k-1\}$ with $\sum_j c_j \eta^{(i_j)} x_j^\ell \neq 0$.

Proof. The first claim is standard: for an $\mathbb{F}_p$-linear map $L : V \to W$ between finite-dimensional $\mathbb{F}_p$-vector spaces, L is surjective if and only if its adjoint L^* is injective. This follows from $\dim(\mathrm{Im}(L)) = \dim(V) - \dim(\ker(L))$ and $\dim(\ker(L^*)) = \dim(W) - \dim(\mathrm{Im}(L))$, so $\mathrm{Im}(L) = W$ iff $\ker(L^*) = \{0\}$.

For the formula, we compute the adjoint explicitly. The relevant inner products are the standard $\mathbb{F}_p$-inner product $\langle \vec{c}, \vec{y} \rangle_{\mathbb{F}_p} = \sum_j c_j y_j$ on $\mathbb{F}_p^n$, and the trace pairing $\langle \vec{a}, \vec{b} \rangle = \sum_{\ell=1}^{k-1} \mathrm{Tr}(a_\ell b_\ell)$ on $\mathbb{F}^{k-1}$. For any $\vec{a} \in \mathbb{F}^{k-1}$ and $\vec{c} \in \mathbb{F}_p^n$:

$$\begin{aligned} \langle \vec{c},\, L_{\vec{i}}(\vec{a}) \rangle_{\mathbb{F}_p} &= \sum_{j=0}^{n-1} c_j \sum_{t=1}^{k-1} \mathrm{Tr}(a_t x_j^t f_{i_j}^*) \\ &= \sum_{t=1}^{k-1} \mathrm{Tr}\left(a_t \sum_{j=0}^{n-1} c_j x_j^t f_{i_j}^* \right), \end{aligned}$$

where we used $\mathbb{F}_p$-linearity of Tr and the fact that $c_j \in \mathbb{F}_p$ can be moved inside Tr. Now substituting $f_{i_j}^* = \eta^{(i_j)} \cdot f_0^*$:

$$= \sum_{t=1}^{k-1} \mathrm{Tr}\left(a_t \cdot f_0^* \cdot \sum_{j=0}^{n-1} c_j \eta^{(i_j)} x_j^t \right) = \left\langle \vec{a},\, \left(f_0^* \cdot \sum_{j=0}^{n-1} c_j \eta^{(i_j)} x_j^\ell \right)_{\ell=1}^{k-1} \right\rangle.$$

Since this holds for all $\vec{a}$, we conclude $(L_{\vec{i}}^*(\vec{c}))_\ell = f_0^* \cdot \sum_j c_j \eta^{(i_j)} x_j^\ell$.

Finally, since $f_0^* \neq 0$ (it is a dual basis element), $L_{\vec{i}}^*(\vec{c}) = 0$ in $\mathbb{F}^{k-1}$ if and only if $\sum_j c_j \eta^{(i_j)} x_j^\ell = 0$ for every $\ell = 1, \dots, k-1$. ◀

▶ **Definition 2.12** (Test matrix). *For block indices $\vec{i} \in \{0, \dots, d-1\}^n$, the* test matrix *$\Theta_{\vec{i}} \in \mathbb{F}_p^{d(k-1) \times n}$ is the $\mathbb{F}_p$-coordinate representation of the map*

$$\vec{c} \mapsto \left(\sum_{j=0}^{n-1} c_j \eta^{(i_j)} x_j^\ell \right)_{\ell=1}^{k-1} \in \mathbb{F}^{k-1} \cong \mathbb{F}_p^{d(k-1)}.$$

▶ **Corollary 2.13.** *$L_{\vec{i}}$ is surjective if and only if $\mathrm{rank}_{\mathbb{F}_p}(\Theta_{\vec{i}}) = n$. Since $\Theta_{\vec{i}}$ has only $d(k-1)$ rows, this (sufficient) full-rank condition can hold only when $n \leq d(k-1)$, the regime in which we work.*

Proof. By Proposition 2.11, $L_{\vec{i}}$ is surjective if and only if $L_{\vec{i}}^*$ is injective, which holds if and only if the $\mathbb{F}_p$-linear map encoded by $\Theta_{\vec{i}}$ has trivial kernel, i.e., $\mathrm{rank}_{\mathbb{F}_p}(\Theta_{\vec{i}}) = n$. Since $\Theta_{\vec{i}}$ has $d(k-1)$ rows, full column rank requires $n \leq d(k-1)$. ◀

3 The construction

We now define the step operator and establish the properties of the orbit $\{x_j = \Phi^j(x_0)\}$ that will be needed for the security analysis. The main point is that three properties – rational function structure, distinct poles, and a short-period bound – follow from elementary algebra, with no conditions to verify beyond $x_0 \notin \{\alpha - 1\} \cup \mathrm{Poles}(n)$.

3.1 The step operator

▶ **Definition 3.1** (Step operator). *Define* $\Phi : \mathbb{P}^1(\mathbb{F}) \to \mathbb{P}^1(\mathbb{F})$ *by*

$$\Phi(x) = \frac{\alpha x}{x+1},$$

where α *is the generator of* $\mathbb{F}^*$ *from Section 2.1. As a Möbius transformation,* Φ *has matrix* $M_\Phi = \begin{pmatrix} \alpha & 0 \\ 1 & 1 \end{pmatrix}$ *with* $\det(M_\Phi) = \alpha \neq 0$.

▶ **Proposition 3.2** (Projective order). *The projective order of* Φ *equals* $\mathrm{ord}(\alpha) = p^d - 1$.

Proof. The eigenvalues of $M_\Phi = \begin{pmatrix} \alpha & 0 \\ 1 & 1 \end{pmatrix}$ are α and 1 (reading off the diagonal, since M_Φ is lower triangular). Hence M_Φ^j has eigenvalues α^j and 1. Now $\Phi^j = \mathrm{id}$ in $\mathrm{PGL}_2(\mathbb{F})$ if and only if $M_\Phi^j = \lambda I$ for some $\lambda \in \mathbb{F}^*$ (since projective transformations are defined up to scalar multiples of the matrix). The condition $M_\Phi^j = \lambda I$ requires both eigenvalues to be equal, i.e., $\alpha^j = 1$. Conversely, if $\alpha^j = 1$, then both eigenvalues equal 1 and M_Φ^j must be the identity (since M_Φ is diagonalizable over the algebraic closure: its eigenvalues α and 1 are distinct for $d \geq 2$, so M_Φ, and hence M_Φ^j, is diagonalizable). The smallest positive j with $\alpha^j = 1$ is $\mathrm{ord}(\alpha) = p^d - 1$. ◀

▶ **Proposition 3.3** (Explicit formula for iterates). *For* $j \geq 1$,

$$\Phi^j(x) = \frac{\alpha^j x}{C_j x + 1}, \qquad C_j := \frac{\alpha^j - 1}{\alpha - 1} = \sum_{i=0}^{j-1} \alpha^i.$$

For $j = 0$, *we have* $\Phi^0(x) = x$.

Proof. By induction on j. For $j = 1$: $C_1 = 1$ and $\Phi(x) = \alpha x/(x+1)$. For the inductive step:

$$\Phi^{j+1}(x) = \Phi(\Phi^j(x)) = \frac{\alpha \cdot \frac{\alpha^j x}{C_j x + 1}}{\frac{\alpha^j x}{C_j x + 1} + 1} = \frac{\alpha^{j+1} x}{(\alpha^j + C_j)x + 1}.$$

It remains to verify that $\alpha^j + C_j = C_{j+1}$. Indeed, $\alpha^j + (\alpha^j - 1)/(\alpha - 1) = (\alpha^{j+1} - \alpha^j + \alpha^j - 1)/(\alpha - 1) = (\alpha^{j+1} - 1)/(\alpha - 1) = C_{j+1}$. ◀

3.2 Distinct poles, fixed points, and pole avoidance

▶ **Corollary 3.4** (Pairwise distinct poles). *For* $0 \leq j \leq n - 1$ *with* $n \leq p^d - 1$, *the Möbius transforms* $\Phi^0, \Phi^1, \ldots, \Phi^{n-1}$ *have pairwise distinct poles in* $\mathbb{P}^1(\mathbb{F})$. *More precisely, the pole of* $\Phi^0 = \mathrm{id}$ *is* ∞, *and the pole of* Φ^j *for* $j \geq 1$ *is* $-(\alpha - 1)/(\alpha^j - 1)$.

Proof. By Proposition 3.3, the pole of Φ^j for $j \geq 1$ is at $x = -1/C_j = -(\alpha - 1)/(\alpha^j - 1)$. For $1 \leq j < j' \leq n - 1$, these coincide if and only if $\alpha^j = \alpha^{j'}$, i.e., $j \equiv j' \pmod{p^d - 1}$. Since $0 < j < j' < p^d - 1$, this is impossible. The pole of $\Phi^0 = \mathrm{id}$ is ∞, which is distinct from all finite poles. ◀

▶ Remark 3.5 (No involution). The map Φ is never an involution for $d \geq 2$, regardless of characteristic. Indeed, $\Phi^2 = \mathrm{id}$ would require $\alpha^2 = 1$, but $\mathrm{ord}(\alpha) = p^d - 1 \geq p^2 - 1 \geq 3$. In particular, no special treatment is needed for $p = 2$.

▶ Remark 3.6 (A naive dilation fails). Deriving motivation from constructions of polynomial codes with optimal list decoding properties (folded Reed-Solomon codes [8]), the most obvious one-parameter candidate is the pure dilation $\Psi(x) = \alpha x$, whose iterates $\Psi^j(x) = \alpha^j x$ form an orbit $x_j = \alpha^j x_0$ on the multiplicative coset $x_0\langle\alpha\rangle$. We record here that this choice fails the structural property driving our analysis, and consequently does not admit the bad-set bound of Theorem 4.5.

The functions Ψ^j are affine, so each has its only pole at ∞. Hence all n iterates share a single common pole, and the pole-distinctness hypothesis of Corollary 3.4 fails completely (rather than failing for at most one j). The partial-fraction argument of Section 4 therefore has no traction: the rational function $G_\ell(x) = \sum_j c_j \eta^{(i_j)} (\alpha^j x)^\ell = x^\ell \cdot \sum_j c_j \eta^{(i_j)} \alpha^{j\ell}$ is a monomial in x, and $G_\ell \equiv 0$ is equivalent to the x_0-independent condition $\sum_j c_j \eta^{(i_j)} \alpha^{j\ell} = 0$. The starting point x_0 has dropped out of the rank condition entirely. In other words, the test matrix $\Theta_{\vec{i}}$ is the same matrix for every $x_0 \in \mathbb{F}^*$, so the dilation scheme is either secure for all nonzero x_0 or for none – there is no parameter to optimize and no closed-form bad-set bound to prove. In particular, the central quantitative result $|\mathrm{Bad}| \leq n + n(dp)^n$ of Theorem 4.5 has no analogue for Ψ.

The role of the $+1$ in the denominator of Φ is thus to perturb each iterate's pole away from ∞ to a distinct finite point of $\mathbb{F}^*$ (Corollary 3.4), placing the orbit in generic position relative to the partial-fraction decomposition. This is the essential algebraic feature that distinguishes Φ from its affine cousin and makes the closed-form bad-set bound possible.

▶ **Lemma 3.7** (Fixed points). *For each $1 \leq j < p^d - 1$, the fixed points of Φ^j in $\mathbb{P}^1(\mathbb{F})$ are exactly $\{0, \alpha - 1\}$. In particular,* $\mathrm{ShortPeriod}(n) := \{x_0 \in \mathbb{F}^* : \exists\, 1 \leq j < n,\ \Phi^j(x_0) = x_0\} = \{\alpha - 1\}$.

Proof. Fix $1 \leq j < p^d - 1$, so that $\Phi^j \neq \mathrm{id}$ by Proposition 3.2. The fixed-point equation $\Phi^j(x) = x$ reads $\alpha^j x/(C_j x + 1) = x$. For $x = 0$: $\Phi^j(0) = 0$, so 0 is a fixed point, but $0 \notin \mathbb{F}^*$. For $x \neq 0$: dividing both sides by x gives $\alpha^j/(C_j x + 1) = 1$, hence $x = (\alpha^j - 1)/C_j$. Since $C_j = (\alpha^j - 1)/(\alpha - 1)$, this gives $x = \alpha - 1$. For $x = \infty$: $\Phi^j(\infty) = \alpha^j/C_j \neq \infty$ (since $C_j \neq 0$ for $j < p^d - 1$). The fixed-point set $\{0, \alpha - 1\}$ is independent of j, so restricting to $\mathbb{F}^*$ gives $\mathrm{ShortPeriod}(n) = \{\alpha - 1\}$. ◀

▶ **Definition 3.8** (Pole set). *Define* $\mathrm{Poles}(n) := \{-1/C_j : 1 \leq j \leq n - 1\} \subset \mathbb{F}^*$. *These are pairwise distinct by Corollary 3.4, so* $|\mathrm{Poles}(n)| = n - 1$.

We note that $\mathrm{Poles}(n) \cap \{\alpha - 1\} = \emptyset$*: the equality* $\alpha - 1 = -(\alpha - 1)/(\alpha^j - 1)$ *would require* $\alpha^j = 0$*, which is impossible.*

▶ **Proposition 3.9** (Distinct evaluation places). *For $x_0 \in \mathbb{F}^* \setminus (\{\alpha - 1\} \cup \mathrm{Poles}(n))$ and $n \leq p^d - 1$, the evaluation places $X_0, X_1, \ldots, X_{n-1}$ are pairwise distinct elements of $\mathbb{F}^*$.*

Proof. We verify three properties. (a) *Each $x_j \in \mathbb{F}^*$:* $x_j = 0$ if and only if $x_0 = 0$ (since 0 is a fixed point of Φ), which is excluded by $x_0 \in \mathbb{F}^*$. $x_j = \infty$ if and only if $x_0 = -1/C_j \in \mathrm{Poles}(n)$, which is excluded by hypothesis. (b) *The orbit avoids $\alpha - 1$:* Since $\alpha - 1$ is a fixed point of Φ itself (not just of Φ^j), we have $\Phi^{-1}(\{\alpha - 1\}) = \{\alpha - 1\}$, and hence $x_j = \alpha - 1$ if and only if $x_0 = \alpha - 1$, which is excluded. (c) *Pairwise distinct:* $x_j = X_{j'}$ for $j < j'$ if and only if x_j is a fixed point of $\Phi^{j'-j}$ in $\mathbb{F}^*$. By Lemma 3.7, the only such point is $\alpha - 1$, and by (b), $x_j \neq \alpha - 1$. ◀

Algorithm 1 CLASSIFY(p, d, k, n, x_0): single-block-leakage classifier for the Möbius orbit $x_j = \Phi^j(x_0)$.

Input: prime p, integer $d \geq 2$, reconstruction threshold $k \geq 2$, number of parties $n \leq d(k-1)$, field representation $\mathbb{F} = \mathbb{F}_p[\alpha]$, candidate base point $x_0 \in \mathbb{F}^*$.
Output: GOOD (certifies perfect security), or BAD$(\vec{i})$ where $\vec{i}$ is a pattern at which the sufficient full-rank certificate fails.

if $x_0 \in \{\alpha - 1\} \cup \mathrm{Poles}(n)$ **then**
  return BAD$(\perp)$ `// structural exclusion`
end
Compute $x_j \leftarrow \Phi^j(x_0)$ for $j = 0, \ldots, n-1$
Compute the dual basis $\{f_0^*, \ldots, f_{d-1}^*\}$ and shifting factors $\eta^{(i)} = f_i^*/f_0^*$
for $\vec{i} \in \{0, \ldots, d-1\}^n$ **do**
  Build $\Theta_{\vec{i}} \in \mathbb{F}_p^{d(k-1)\times n}$ as in Definition 2.12
  if $\mathrm{rank}_{\mathbb{F}_p}(\Theta_{\vec{i}}) < n$ **then**
    return BAD$(\vec{i})$
  end
end
return GOOD

▶ Remark 3.10. The total number of structural exclusions is $|\{\alpha - 1\} \cup \mathrm{Poles}(n)| = n$.

▶ Remark 3.11 (Canonical base point). The generator α is a natural canonical candidate for the base point. Two layers of the goodness condition should be distinguished.

Provably: α avoids the structural exclusion set $\{\alpha - 1\} \cup \mathrm{Poles}(n)$. Indeed, $\alpha \neq \alpha - 1$ (since $1 \neq 0$), and $\alpha \in \mathrm{Poles}(n)$ would require $\alpha^{j+1} = 1$ for some $1 \leq j \leq n-1$, which is impossible whenever $n \leq p^d - 2$. Verification is $O(n)$.

Not provably without verification: whether α avoids the security-bad set in the headline single-block regime of Theorem 4.5 requires running the classifier of Algorithm 1.

3.3 Classifier and choice of base point

We now give an explicit classifier that, given a candidate base point x_0, tests the *sufficient* full-rank condition of Corollary 2.13 for the resulting evaluation places $x_j = \Phi^j(x_0)$: for each block-index tuple $\vec{i} \in \{0, \ldots, d-1\}^n$ it checks whether the test matrix $\Theta_{\vec{i}}$ has full column rank n over $\mathbb{F}_p$, returning GOOD only if all of them do. A GOOD verdict *certifies* perfect security against single-block leakage, so the classifier is a *sound* tester. A BAD $(\vec{i})$ verdict reports a pattern at which the full-rank certificate fails; since full rank is sufficient but not necessary (Corollary 2.13), this does not by itself certify insecurity. On the structured Möbius candidates we propose, this sound test is what we use to certify goodness; we do not claim it decides perfect security on arbitrary evaluation places, for which the exact criterion is the containment/minimal-codeword condition of [20, Theorem 6].

▶ **Proposition 3.12** (Classifier complexity). *Algorithm 1 runs in time $O(d^n \cdot n^2 \cdot dk)$ field operations over $\mathbb{F}_p$.*

Proof. The structural-exclusion check is $O(n)$. Computing the orbit $x_0, \ldots, x_{n-1}$ and the shifting factors is $\mathrm{poly}(d, n, \log p)$, dominated by the main loop. The loop iterates d^n times. Each iteration builds a $d(k-1) \times n$ matrix over $\mathbb{F}_p$ (whose entries are $\mathbb{F}_p$-coordinates of $\eta^{(i_j)} x_j^\ell$, each computable in $\mathrm{poly}(d, k, \log p)$ field operations) and computes its rank in $O(n^2 \cdot d(k-1)) = O(n^2 dk)$ field operations. No enumeration over coefficient vectors $\vec{c} \in \mathbb{F}_p^n$ is needed, since the rank test handles all $\vec{c}$ per pattern simultaneously. ◀

Algorithm 1 matches the cost of the classifying algorithm given by Nguyen [20, Fig. 1] on the corresponding inputs. Our contribution in this regard is therefore not a faster verification algorithm; rather, the classifier exists here as a tool to certify the structured Möbius candidates we propose, complementing the closed form bad-set bounds.

4 Single-block security

The goal of this section is to prove that for all but a small number of base points x_0, the test matrix $\Theta_{\vec{i}}$ has full column rank for *every* block-index tuple $\vec{i}$. The main tool is a partial-fraction non-degeneracy lemma, which exploits the fact that the Möbius transforms $\Phi^0, \dots, \Phi^{n-1}$ have pairwise distinct poles.

4.1 Non-degeneracy via partial fractions

▶ **Lemma 4.1** (Non-degeneracy). *Let $\psi_0, \dots, \psi_{n-1}$ be Möbius transforms on $\mathbb{P}^1(\mathbb{F})$ with pairwise distinct poles. Let $\delta_0, \dots, \delta_{n-1} \in \mathbb{F}^*$, $c_0, \dots, c_{n-1} \in \mathbb{F}_p$ with $\vec{c} \neq \vec{0}$, and $\ell \geq 1$. Then*

$$G_\ell(x) := \sum_{j=0}^{n-1} c_j \delta_j (\psi_j(x))^\ell$$

is not identically zero as a rational function on $\mathbb{P}^1(\mathbb{F})$.

Proof. Write $\psi_j(x) = (A_j x + B_j)/(C_j x + D_j)$ with $A_j D_j - B_j C_j \neq 0$. The poles $p_j = -D_j/C_j$ (for $C_j \neq 0$) or $p_j = \infty$ (for $C_j = 0$) are pairwise distinct by hypothesis, so at most one equals ∞.

Case A. All poles are finite ($C_j \neq 0$ for all j). Near the pole p_j, $\psi_j(x)$ has a simple pole with residue $r_j = -(A_j D_j - B_j C_j)/C_j^2 \neq 0$. Consequently, $(\psi_j(x))^\ell$ has a pole of order ℓ at p_j with leading Laurent coefficient $r_j^\ell \neq 0$. Since the poles are pairwise distinct, the leading term of G_ℓ at p_j comes only from the j-th summand: $G_\ell(x) \sim c_j \delta_j r_j^\ell/(x - p_j)^\ell$ as $x \to p_j$. If $G_\ell \equiv 0$, then $c_j \delta_j r_j^\ell = 0$ for all j. Since $\delta_j \neq 0$ and $r_j \neq 0$, this forces $c_j = 0$ for all j, contradicting $\vec{c} \neq \vec{0}$.

Case B. One pole is at ∞ (say $C_0 = 0$, so that ψ_0 is affine; all other $C_j \neq 0$). The residue argument at each finite pole p_j ($j \geq 1$) gives $c_j \delta_j r_j^\ell = 0$, hence $c_j = 0$ for all $j \geq 1$. Then $G_\ell(x) = c_0 \delta_0 (\psi_0(x))^\ell$. Since ψ_0 is nonconstant ($A_0/D_0 \neq 0$ because $\det(M_0) \neq 0$ and $C_0 = 0$), $\delta_0 \neq 0$, and $c_0 \neq 0$ (as $\vec{c} \neq \vec{0}$), this is not identically zero.

At most one pole equals ∞, so Cases A and B are exhaustive. ◀

▶ **Corollary 4.2** (Zero bound). *Under the hypotheses of Lemma 4.1, G_ℓ has at most $n\ell$ zeros in $\mathbb{P}^1(\mathbb{F})$.*

Proof. Write $\psi_j(x) = (A_j x + B_j)/(C_j x + D_j)$. Let $S = \{j : C_j \neq 0\}$ and $T = \{j : C_j = 0\}$, so $|T| \leq 1$ (at most one pole can be ∞). Define the common denominator

$$D(x) = \prod_{j \in S} (C_j x + D_j)^\ell,$$

and set $N(x) = G_\ell(x) \cdot D(x)$. We compute the degree of $N(x)$.

For $j \in S$: the j-th summand of G_ℓ is $c_j \delta_j (A_j x + B_j)^\ell/(C_j x + D_j)^\ell$. After multiplying by $D(x)$, the denominator $(C_j x + D_j)^\ell$ cancels, contributing to $N(x)$ the term $c_j \delta_j (A_j x + B_j)^\ell \prod_{j' \in S,\, j' \neq j} (C_{j'} x + D_{j'})^\ell$, which has degree $\ell + \ell(|S| - 1) = \ell |S|$.

For $j \in T$: we have $C_j = 0$, so $\psi_j(x) = (A_j/D_j)x + B_j/D_j$ is affine (with $A_j/D_j \neq 0$). The j-th summand of G_ℓ is $c_j\delta_j((A_j/D_j)x + B_j/D_j)^\ell$, a polynomial of degree ℓ. After multiplying by $D(x) = \prod_{j' \in S}(C_{j'}x + D_{j'})^\ell$, which has degree $\ell|S|$, the contribution is a polynomial of degree $\ell + \ell|S|$.

Since $|S| + |T| = n$: if $T = \emptyset$, then $|S| = n$ and $\deg(N) \leq \ell n$. If $|T| = 1$, then $|S| = n - 1$ and $\deg(N) \leq \max(\ell(n-1),\ \ell + \ell(n-1)) = \ell n$. In both cases, $\deg(N) \leq n\ell$.

Since $G_\ell \not\equiv 0$ by Lemma 4.1, $N \not\equiv 0$, so N has at most $\deg(N) \leq n\ell$ roots (counted with multiplicity) in $\mathbb{F}$. The zeros of G_ℓ in $\mathbb{P}^1(\mathbb{F})$ are a subset of the roots of N: indeed, any root of D that is also a root of N must be a pole of some summand of G_ℓ, hence a pole of G_ℓ (since the poles are distinct, there is no cancellation), not a zero. Therefore G_ℓ has at most $n\ell$ zeros in $\mathbb{P}^1(\mathbb{F})$. ◀

4.2 Full rank of the test matrix

▶ **Theorem 4.3.** *Let p be any prime, $d \geq 2$, and $2 \leq k \leq n \leq d(k-1)$ with $n \leq p^d - 1$. For any $\vec{i} \in \{0, \ldots, d-1\}^n$ and $\vec{c} \in \mathbb{F}_p^n \setminus \{\vec{0}\}$, we have*

$$|\{x_0 \in \mathbb{F}^* : \sum_{j=0}^{n-1} c_j \eta^{(i_j)}(\Phi^j(x_0))^\ell = 0 \ \ \forall\, \ell = 1, \ldots, k-1\}| \leq n.$$

Proof. Apply Lemma 4.1 with $\ell = 1$, $\psi_j = \Phi^j$, and $\delta_j = \eta^{(i_j)}$. By Corollary 3.4, the Φ^j have pairwise distinct poles. The shifting factors $\eta^{(i_j)}$ are nonzero (being ratios of dual basis elements). So $G_1(x) = \sum_j c_j \eta^{(i_j)} \Phi^j(x) \not\equiv 0$, and by Corollary 4.2, G_1 has at most n zeros in $\mathbb{P}^1(\mathbb{F})$. The bad set is contained in $\{x_0 \in \mathbb{F}^* : G_1(x_0) = 0\}$, which has size $\leq n$. ◀

▶ Remark 4.4. The bound $\leq n$ comes from the $\ell = 1$ case alone. The bad set requires $G_\ell = 0$ for *all* ℓ, and the containment in the zero set of G_1 already suffices.

▶ **Theorem 4.5** (Perfect security against single-block leakage)**.** *Let p be any prime, $d \geq 2$, and $2 \leq k \leq n \leq d(k-1)$ with $n \leq p^d - 1$. Define*

$$\text{Bad} := \{\alpha - 1\} \cup \text{Poles}(n) \ \cup \bigcup_{\vec{i} \in \{0,\ldots,d-1\}^n} \ \bigcup_{\vec{c} \in \mathbb{F}_p^n \setminus \{\vec{0}\}} \{x_0 \in \mathbb{F}^* : G_1(x_0; \vec{i}, \vec{c}) = 0\}.$$

Then $|\text{Bad}| \leq n + n(dp)^n$. For any $x_0 \in \mathbb{F}^* \setminus \text{Bad}$:
(a) *$x_0, \ldots, x_{n-1}$ are pairwise distinct elements of $\mathbb{F}^*$.*
(b) *$\text{ShamirSS}(n, k, \vec{X})_{\mathbb{F}}$ is perfectly secure against all single-block leakage.*

Proof. Part (a) follows from Proposition 3.9, since $x_0 \notin \{\alpha - 1\} \cup \text{Poles}(n)$.

For part (b): by the security reduction (Corollary 2.13), we need $\text{rank}_{\mathbb{F}_p}(\Theta_{\vec{i}}) = n$ for every block-index tuple $\vec{i} \in \{0, \ldots, d-1\}^n$. By Proposition 2.11, this fails for $\vec{i}$ if and only if there exists $\vec{c} \in \mathbb{F}_p^n \setminus \{\vec{0}\}$ with $\sum_j c_j \eta^{(i_j)} x_j^\ell = 0$ for all $\ell = 1, \ldots, k-1$. For each such pair $(\vec{i}, \vec{c})$, Theorem 4.3 bounds the set of bad base points by $\leq n$.

We now count. The structural exclusion set $\{\alpha - 1\} \cup \text{Poles}(n)$ has size n (by Remark 3.10). The number of block-index tuples is $|\{0, \ldots, d-1\}^n| = d^n$. The number of nonzero coefficient vectors is $|\mathbb{F}_p^n \setminus \{\vec{0}\}| = p^n - 1$. By Theorem 4.3, each pair contributes at most n bad base points. By the union bound:

$$|\text{Bad}| \leq n + d^n \cdot (p^n - 1) \cdot n \leq n + n \cdot d^n \cdot p^n = n + n(dp)^n.$$

For any $x_0 \in \mathbb{F}^* \setminus \text{Bad}$: by construction, x_0 avoids the structural exclusion set (ensuring part (a)) and, for every $\vec{i}$ and every nonzero $\vec{c}$, there exists ℓ with $G_\ell(x_0; \vec{i}, \vec{c}) \neq 0$. This means $\Theta_{\vec{i}}$ has trivial kernel for every $\vec{i}$, i.e., full column rank n. By Corollary 2.13, $L_{\vec{i}}$ is surjective for all $\vec{i}$, and by Proposition 2.9, SD $= 0$ for all pairs of secrets and all block-leakage patterns. ◀

▶ **Corollary 4.6** (Existence). *A good x_0 exists whenever $p^d - 1 > n + n(dp)^n$, i.e., $d > n(1 + \log_p d) + O(\log_p n)$, giving $n = O(d/\log_p d)$.*

4.3 Physical bit security

▶ **Proposition 4.7** (Block security implies sub-block security). *Let $S_0, \ldots, S_{n-1}$ be arbitrary nonempty finite sets. If $\text{ShamirSS}(n, k, \vec{X})_{\mathbb{F}}$ is perfectly secure against single-block leakage, then it is also perfectly secure against any leakage that applies an arbitrary function $g_j : \mathbb{F}_p \to S_j$ to a single $\mathbb{F}_p$-block of each share.*

Proof. By Theorem 4.5, for every block-index tuple $(i_0, \ldots, i_{n-1}) \in \{0, \ldots, d-1\}^n$, the map $L_{\vec{i}}$ is surjective. By Proposition 2.9, this means the leakage vector $((P(X_0))_{i_0}, \ldots, (P(X_{n-1}))_{i_{n-1}}) \in \mathbb{F}_p^n$ has the same distribution for every secret $s \in \mathbb{F}$: it is uniform over $\mathbb{F}_p^n$.

Now suppose the adversary applies deterministic functions $g_j : \mathbb{F}_p \to S_j$ to obtain $(g_0((P(X_0))_{i_0}), \ldots, g_{n-1}((P(X_{n-1}))_{i_{n-1}}))$. Since each g_j is a fixed function, this post-processed leakage is a deterministic function of $((P(x_j))_{i_j})_{j=0}^{n-1}$. By the data processing inequality for statistical distance, for any two secrets s, s':

$$\text{SD}\big((g_j((P(x_j))_{i_j}))_j \,\big|\, s,\ \ (g_j((P(x_j))_{i_j}))_j \,\big|\, s'\big) \leq \text{SD}\big(((P(x_j))_{i_j})_j \,\big|\, s,\ \ ((P(x_j))_{i_j})_j \,\big|\, s'\big) = 0.$$

Hence perfect security is preserved under arbitrary post-processing. ◀

▶ **Corollary 4.8** (Physical bit security, all characteristics). *For any prime p: if the adversary leaks one physical bit per share (from an arbitrary $\mathbb{F}_p$-block, possibly different blocks for different shares), our evaluation places provide perfect security.*

Proof. A physical bit $\text{bit}_{r_j}((P(x_j))_{i_j})$ is a function $g_j : \mathbb{F}_p \to \{0, 1\}$ applied to a single block. The result follows from Proposition 4.7. ◀

5 Multi-block security

We now extend the analysis to the multi-block setting, where the adversary probes multiple $\mathbb{F}_p$-coordinates from each share.

5.1 Setup

For an admissible multi-block leakage pattern with $M = \sum_{j=0}^{n-1} m_j \leq d(k-1)$ total blocks, the leakage map $L : \mathbb{F}^{k-1} \to \mathbb{F}_p^M$ is $\mathbb{F}_p$-linear. The test matrix $\Theta \in \mathbb{F}_p^{d(k-1)\times M}$ has columns indexed by pairs (share j, block $i_j^{(r)}$).

Full column rank $\text{rank}_{\mathbb{F}_p}(\Theta) = M$ is a *sufficient* condition for perfect security, and is the criterion we establish below; as in the single-block case (Corollary 2.13) it need not be necessary.

The structure of the kernel is as follows. A nonzero vector $(c_{j,r})_{j,r} \in \ker(\Theta)$ groups naturally by shares, producing $d_j = \sum_{r=1}^{m_j} c_{j,r}\eta^{(i_j^{(r)})} \in \mathbb{F}$. By admissibility, the shifting factors within each share are $\mathbb{F}_p$-independent, so $d_j = 0$ if and only if all of the corresponding $c_{j,r}$ vanish. In particular, at least one d_j must be nonzero.

▶ Remark 5.1 (Admissibility is necessary). Since any $m_j \leq d$ distinct blocks from the same share have $\mathbb{F}_p$-independent shifting factors (by Lemma 2.3), any pattern with distinct block positions within each share is admissible.

5.2 Non-degeneracy with field coefficients

▶ **Lemma 5.2.** *Let $\psi_0, \ldots, \psi_{n-1}$ be Möbius transforms on $\mathbb{P}^1(\mathbb{F})$ with pairwise distinct poles. Let $d_0, \ldots, d_{n-1} \in \mathbb{F}$ with at least one $d_j \neq 0$, and $\ell \geq 1$. Then $\sum_j d_j(\psi_j(x))^\ell \not\equiv 0$ as a rational function, and has at most $n\ell$ zeros in $\mathbb{P}^1(\mathbb{F})$.*

Proof. Write $\psi_j(x) = (A_j x + B_j)/(C_j x + D_j)$ with $\det(M_j) = A_j D_j - B_j C_j \neq 0$, and let p_j denote the pole of ψ_j. The poles are pairwise distinct by hypothesis. Let $S = \{j : C_j \neq 0\}$ (finite poles) and $T = \{j : C_j = 0\}$ (pole at ∞), so $|T| \leq 1$.

Case A. All poles are finite ($T = \emptyset$). For each j, the residue of ψ_j at its pole $p_j = -D_j/C_j$ is $r_j = -\det(M_j)/C_j^2 \neq 0$. Near p_j, we have $\psi_j(x) = r_j/(x - p_j) + O(1)$, so $(\psi_j(x))^\ell = r_j^\ell/(x - p_j)^\ell + \text{lower-order terms}$. Since $p_j \neq p_{j'}$ for $j \neq j'$, the function $\sum_j d_j(\psi_j(x))^\ell$ has a Laurent expansion near p_j whose leading term is $d_j r_j^\ell/(x - p_j)^\ell$; all other summands are regular at p_j. If $\sum_j d_j(\psi_j(x))^\ell \equiv 0$, this leading coefficient must vanish: $d_j r_j^\ell = 0$. Since $r_j \neq 0$, we get $d_j = 0$ for every $j \in S$. With $T = \emptyset$, this gives $d_j = 0$ for all j, contradicting the hypothesis.

Case B. One pole is at ∞ (say $j = 0$, so $C_0 = 0$; all other $C_j \neq 0$). The residue argument at each finite pole p_j ($j \geq 1$) gives $d_j r_j^\ell = 0$, hence $d_j = 0$ for all $j \geq 1$. Then $\sum_j d_j(\psi_j(x))^\ell = d_0(\psi_0(x))^\ell$. Since $C_0 = 0$, $\psi_0(x) = (A_0/D_0)x + B_0/D_0$ is a nonconstant affine function ($A_0/D_0 \neq 0$ because $\det(M_0) = A_0 D_0 \neq 0$). Thus $d_0(\psi_0(x))^\ell$ is a nonzero polynomial (since $d_0 \neq 0$ by hypothesis, as all other d_j vanish).

The zero bound $\leq n\ell$ follows by the same degree argument as in Corollary 4.2: multiply $\sum_j d_j(\psi_j(x))^\ell$ by $D(x) = \prod_{j \in S}(C_j x + D_j)^\ell$ to obtain a nonzero polynomial $N(x)$ of degree $\leq n\ell$. ◀

5.3 Multi-block theorems

▶ **Theorem 5.3** (Multi-block, fixed pattern)**.** *Fix an admissible multi-block leakage pattern with $M \leq d(k-1)$ total blocks. The set of $x_0 \in \mathbb{F}^*$ for which the scheme is not perfectly secure has size $\leq n + n \cdot p^M$. A good x_0 exists when $M < d - \log_p(2n)$.*

Proof. A nonzero vector $(c_{j,r})_{j,r} \in \mathbb{F}_p^M \setminus \{\vec{0}\}$ lies in $\ker(\Theta)$ if and only if

$$\sum_{j=0}^{n-1} \sum_{r=1}^{m_j} c_{j,r} \eta^{(i_j^{(r)})} x_j^\ell = 0 \quad \text{for all } \ell = 1, \ldots, k-1.$$

Grouping the inner sum by shares, this becomes $\sum_{j=0}^{n-1} d_j x_j^\ell = 0$ for all ℓ, where $d_j := \sum_{r=1}^{m_j} c_{j,r} \eta^{(i_j^{(r)})} \in \mathbb{F}$. By admissibility, the shifting factors $\eta^{(i_j^{(1)})}, \ldots, \eta^{(i_j^{(m_j)})}$ within share j are $\mathbb{F}_p$-independent (Lemma 2.3), so $d_j = 0$ if and only if $c_{j,r} = 0$ for all r. Since $\vec{c} \neq \vec{0}$, at least one $d_j \neq 0$.

By Lemma 5.2 with $\ell = 1$ and $\psi_j = \Phi^j$: the function $G_1(x) = \sum_j d_j \Phi^j(x)$ is not identically zero and has at most n zeros in $\mathbb{P}^1(\mathbb{F})$. The set of $x_0 \in \mathbb{F}^*$ with $G_1(x_0) = 0$ therefore has size $\leq n$.

There are $p^M - 1$ nonzero coefficient vectors in $\mathbb{F}_p^M$. By the union bound over all such vectors, plus the n structural exclusions:

$$|\text{Bad}| \leq n + (p^M - 1) \cdot n \leq n + n \cdot p^M.$$

A good x_0 exists when $|\mathbb{F}^*| = p^d - 1 > n + n \cdot p^M$, which holds when $p^d > 2n \cdot p^M$, i.e., $M < d - \log_p(2n)$. ◀

▶ **Theorem 5.4** (Universal multi-block). *To achieve perfect security against all admissible patterns with $\leq M$ blocks simultaneously, we get $|\text{Bad}| \leq n + n \cdot (dpe)^M$. A good x_0 exists when $d > M\left(\frac{5}{2} + \log_p d\right) + \log_p(2n)$.*

Proof. We take a union bound over all admissible multi-block patterns with $\leq M$ blocks total. An admissible pattern is specified by choosing, for each share j, a nonempty subset of $\{0, \ldots, d-1\}$ of block positions. The total number of such patterns is at most $\binom{d}{m_0} \cdots \binom{d}{m_{n-1}}$ summed over all $(m_0, \ldots, m_{n-1})$ with $\sum m_j \leq M$. Also note that by definition of admissible patterns, we have $m_0, \ldots, m_{n-1} \geq 1$ and $M \geq n$. This gives us the total number as

$$\sum_{\substack{m_0+\cdots+m_{n-1} \leq M \\ m_0,\ldots,m_{n-1} \geq 1}} \binom{d}{m_0} \cdots \binom{d}{m_{n-1}} \leq \sum_{t=n}^{M} \binom{nd}{t} \leq \left(\frac{nde}{M}\right)^M \leq (de)^M.$$

where the first inequality is by the Cauchy-Vandermonde identity [11, Exercise 1.9], the second inequality is by standard estimate on binomial coefficient [11, Proposition 1.4], and the third inequality is due to $M \geq n$.

For each fixed pattern, Theorem 5.3 gives at most $n \cdot p^M$ security-bad base points (beyond the structural exclusions). Taking the union bound over all $\leq (de)^M$ patterns, we get

$$|\text{Bad}| \leq n + (n \cdot p^M) \cdot (de)^M = n + n(dpe)^M.$$

A good x_0 exists when $p^d - 1 > n + n(dpe)^M$. Taking logarithms base p, we need $d > \log_p(2n) + M(\log_p d + 1 + \log_p e)$, which is satisfied when $d > M\left(\frac{5}{2} + \log_p d\right) + \log_p(2n)$. ◀

References

1. Luís T. A. N. Brand ao and René Peralta. NIST first call for multi-party threshold schemes, 2023. URL: `https://csrc.nist.gov/publications/detail/nistir/8214c/draft`.
2. Mitali Bafna, Madhu Sudan, Santhoshini Velusamy, and Dain Xiang. Elementary analysis of isolated zeroes of a polynomial system, 2021. arXiv Preprint. `doi:10.48550/arXiv.2102.00602`.
3. Fabrice Benhamouda, Akshay Degwekar, Yuval Ishai, and Tal Rabin. On the local leakage resilience of linear secret sharing schemes. In *Advances in Cryptology – CRYPTO 2018*, volume 10991 of *LNCS*, pages 531–561. Springer, 2018. `doi:10.1007/978-3-319-96884-1_18`.
4. 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, 2021. `doi:10.1007/s00145-021-09375-2`.
5. Nicolas Costes and Martijn Stam. Redundant code-based masking revisited. *IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES)*, 2021(1):426–450, 2021. `doi:10.46586/tches.v2021.i1.426-450`.
6. Sebastian Faust, Loïc Masure, Elena Micheli, Maximilian Orlt, and François-Xavier Standaert. Connecting leakage-resilient secret sharing to practice: Scaling trends and physical dependencies of prime field masking. In *Advances in Cryptology – EUROCRYPT 2024*, pages 316–344. Springer, 2024. `doi:10.1007/978-3-031-58737-5_12`.

7 Vipul Goyal and Ashutosh Kumar. Non-malleable secret sharing. In *50th ACM Symposium on Theory of Computing (STOC 2018)*, pages 685–698, 2018. doi:10.1145/3188745.3188872.

8 Venkatesan Guruswami and Atri Rudra. Explicit codes achieving list decoding capacity: Error-correction with optimal redundancy. *IEEE Transactions on Information Theory*, 54(1):135–150, 2008. doi:10.1109/TIT.2007.911222.

9 Jihun Hwang, Hemanta K. Maji, Hai H. Nguyen, and Xiuyu Ye. Leakage-resilience of Shamir's secret sharing: Identifying secure evaluation places. In *6th Conference on Information-Theoretic Cryptography (ITC 2025)*, LIPIcs, 2025. doi:10.4230/LIPIcs.ITC.2025.3.

10 Yuval Ishai, Amit Sahai, and David Wagner. Private circuits: Securing hardware against probing attacks. In *Advances in Cryptology – CRYPTO 2003*, volume 2729 of *LNCS*, pages 463–481. Springer, 2003. doi:10.1007/978-3-540-45146-4_27.

11 Stasys Jukna. *Extremal combinatorics: with applications in computer science*, volume 571. Springer, 2011. doi:10.1007/978-3-642-17364-6.

12 Ohad Klein and Ilan Komargodski. New bounds on the local leakage resilience of Shamir's secret sharing scheme. In *Advances in Cryptology – CRYPTO 2023*, volume 14081 of *LNCS*, pages 139–170. Springer, 2023. doi:10.1007/978-3-031-38557-5_5.

13 Hiroki Koga and Hiroto Abe. New tight bounds on the local leakage resilience of the additive (n, n)-threshold scheme determined by the eigenvalues of circulant matrices. In Goichiro Hanaoka and Bo-Yin Yang, editors, *Advances in Cryptology – ASIACRYPT 2025*, pages 34–66, Singapore, 2026. Springer Nature Singapore. doi:10.1007/978-981-95-5125-5_2.

14 Ashutosh Kumar, Raghu Meka, and Amit Sahai. Leakage-resilient secret sharing against colluding parties. In *2019 IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 636–660, 2019. doi:10.1109/FOCS.2019.00045.

15 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 *Advances in Cryptology – EUROCRYPT 2021*, volume 12697 of *LNCS*, pages 344–374. Springer, 2021. doi:10.1007/978-3-030-77886-6_12.

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

17 Hemanta K. Maji, Hai H. Nguyen, Anat Paskin-Cherniavsky, and Xiuyu Ye. Constructing leakage-resilient Shamir's secret sharing: Over composite order fields. In *Advances in Cryptology – EUROCRYPT 2024*, volume 14654 of *LNCS*, pages 286–315. Springer, 2024. doi:10.1007/978-3-031-58737-5_11.

18 Hemanta K. Maji, Anat Paskin-Cherniavsky, Tom Suad, and Mingyuan Wang. Constructing locally leakage-resilient linear secret-sharing schemes. In *Advances in Cryptology – CRYPTO 2021*, volume 12827 of *LNCS*, pages 779–808. Springer, 2021. doi:10.1007/978-3-030-84252-9_26.

19 Hai H. Nguyen. Towards breaking the half-barrier for Shamir's secret sharing scheme. In *Advances in Cryptology – CRYPTO 2024*, 2024. doi:10.1007/978-3-031-68388-6_10.

20 Hai H. Nguyen. Physical-bit leakage resilience of linear code-based secret sharing. In Serge Fehr and Pierre-Alain Fouque, editors, *Advances in Cryptology – EUROCRYPT 2025*, pages 64–93, Cham, 2025. Springer Nature Switzerland. doi:10.1007/978-3-031-91101-9_3.

21 Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979. doi:10.1145/359168.359176.

22 Xiaomei Zhao. A note on multiple exponential sums in function fields. *Finite Fields and Their Applications*, 18(1):35–55, 2012. doi:10.1016/j.ffa.2011.06.003.

A Alternative proof of the dichotomy

The perfect-or-completely-insecure dichotomy used throughout this paper (Proposition 2.9) is a special case of the general dichotomy result of [20]. For completeness, we record here a direct derivation in our setting, working through the leakage map $L_{\vec{i}}$ and the cosets-of-subspaces

structure. The proof depends only on $\mathbb{F}_p$-linearity of coordinate extraction and on Shamir's $\mathbb{F}$-linearity in the randomness; it does not use any property of generalized Reed–Solomon codes or of binary images.

Proof of Proposition 2.8. Since $P(x_j) = s + \sum_{t=1}^{k-1} a_t x_j^t$, the $\mathbb{F}_p$-linearity of the coordinate map gives

$$\ell_j = (P(x_j))_{i_j} = (s)_{i_j} + \sum_{t=1}^{k-1} (a_t x_j^t)_{i_j}.$$

By the definition of coordinates via the dual basis (Proposition 2.2 and Definition 2.1), we have $(a_t x_j^t)_{i_j} = \mathrm{Tr}(a_t x_j^t \cdot f_{i_j}^*)$. This gives the decomposition $\ell_j = (s)_{i_j} + \sum_{t=1}^{k-1} \mathrm{Tr}(a_t \cdot x_j^t \cdot f_{i_j}^*)$.

It remains to verify that $L_{\vec{i}}$ is $\mathbb{F}_p$-linear. For any $\lambda \in \mathbb{F}_p$ and $\vec{a}, \vec{b} \in \mathbb{F}^{k-1}$:

$$L_{\vec{i}}(\lambda\vec{a} + \vec{b})_j = \sum_{t=1}^{k-1} \mathrm{Tr}((\lambda a_t + b_t) \cdot x_j^t \cdot f_{i_j}^*) = \lambda \sum_{t=1}^{k-1} \mathrm{Tr}(a_t x_j^t f_{i_j}^*) + \sum_{t=1}^{k-1} \mathrm{Tr}(b_t x_j^t f_{i_j}^*),$$

where we used $\mathrm{Tr}(\lambda \cdot y) = \lambda \cdot \mathrm{Tr}(y)$ for $\lambda \in \mathbb{F}_p$ (since the trace is $\mathbb{F}_p$-linear) and $\mathrm{Tr}(y + z) = \mathrm{Tr}(y) + \mathrm{Tr}(z)$. Thus $L_{\vec{i}}(\lambda\vec{a} + \vec{b}) = \lambda L_{\vec{i}}(\vec{a}) + L_{\vec{i}}(\vec{b})$. ◀

Proof of Proposition 2.9. Since $\vec{a} = (a_1, \ldots, a_{k-1})$ is uniform over $\mathbb{F}^{k-1}$ and $L_{\vec{i}}$ is $\mathbb{F}_p$-linear, the random variable $L_{\vec{i}}(\vec{a})$ is uniform over the subspace $\mathrm{Im}(L_{\vec{i}}) \subseteq \mathbb{F}_p^n$. By Proposition 2.8, the leakage for secret s is $\vec{v}(s) + L_{\vec{i}}(\vec{a})$, which is uniform over the coset $\vec{v}(s) + \mathrm{Im}(L_{\vec{i}})$. Two cosets of an $\mathbb{F}_p$-subspace of $\mathbb{F}_p^n$ are either identical (when the difference of the shifts lies in the subspace, giving $\mathrm{SD} = 0$) or disjoint (giving $\mathrm{SD} = 1$, since uniform distributions on disjoint sets of equal size have statistical distance 1). If $L_{\vec{i}}$ is surjective, then $\mathrm{Im}(L_{\vec{i}}) = \mathbb{F}_p^n$, so every coset equals $\mathbb{F}_p^n$. ◀