

Local Leakage Resilience of Shamir Secret Sharing: Below Half Threshold Rate

Hai H. Nguyen*

Abstract

We study the local leakage resilience of Shamir secret sharing, where an adversary leaks a bounded number of bits from every share. For n parties and reconstruction threshold k over a prime field $\mathbb{F}_p$ with $p > n$, we prove the following.

- There is an absolute constant $c_{\text{bh}} < 1/2$ such that, for $k \geq c_{\text{bh}}n$, Shamir sharing is resilient to arbitrary one-bit leakage from every share. The best previous threshold was $0.668n$.
- For every fixed $0 < \delta < 1/2$ and $k \geq (1/2 + \delta)n$, Shamir sharing is resilient to $\lfloor \frac{\delta}{24} \log_2 n \rfloor$ bits of arbitrary local leakage per share. By a recent attack, this number of bits is optimal up to a constant factor depending on δ .
- For every fixed threshold rate $c > 0$ and $k \geq cn$, Shamir sharing is resilient to quadratic-residue leakage and to almost all local leakage functions of up to $\eta_c \log_2 p$ bits, for a constant $\eta_c > 0$.

All three results follow from one analytic framework, which we develop for generalized Reed–Solomon codes: local leakage from a uniform codeword is statistically close to the same leakage from independent uniform field elements. The framework expresses the leakage distance as the norm of a function on the leakage outputs. The Efron–Stein decomposition splits this function into orthogonal components indexed by supports of dual codewords. Two tools bound the components: list recovery of the dual code, which is ordinary list decoding for one-bit leakage, and a generalized von Neumann inequality for MDS systems of linear forms that retains linearly many Gowers norms. The first tool gives the result above half, the second gives the constant-rate result, and applying both to different ranges of supports in the same decomposition gives the result below half.

*CQT at NUS, Singapore. hai.h.nguyen@nus.edu.sg

Contents

1	Introduction	1
1.1	Our contributions	1
1.2	Technical overview	4
1.3	Related work	8
2	Preliminaries	10
2.1	Generalized Reed–Solomon codes	10
2.2	Shamir secret sharing	11
2.3	Local leakage resilience	11
2.4	Fourier analysis and Gowers norms	12
2.5	List decoding and list recovery	13
3	An orthogonal decomposition of the leakage distance	13
3.1	Efron–Stein decomposition	14
3.2	The leakage distance as a norm on the output space	15
3.3	The orthogonal components	16
3.4	One-bit leakage	17
4	Dual-code list recovery and resilience above half	18
4.1	Bounding the leakage components	18
4.2	Applying list recovery	20
5	Structured leakage at constant-rate thresholds	22
5.1	A product bound for Gowers norms	23
5.2	From Gowers norms to leakage resilience	25
5.3	Quadratic-residue leakage	25
5.4	Almost all logarithmic-bit leakage functions	26
5.5	Field size for square-root thresholds	27
6	Leakage resilience below half	28
6.1	List recovery for small supports	28
6.2	Iterated Cauchy–Schwarz for large supports	30
6.3	Combining the estimates	32
7	AI Acknowledgments	33
A	List recovery with growing input lists	39
B	An alternative list-recovery calculation from DKT	42

1 Introduction

Shamir secret sharing [Sha79] is a fundamental cryptographic primitive with many applications. In an (n, k) -Shamir scheme, a secret is encoded in n evaluations, called shares, of a random polynomial of degree below k whose constant coefficient is the secret. Any k shares determine the secret, and any fewer reveal nothing about it. The algebraic structure also allows efficient computation on shared secrets, which makes the scheme a central building block of secure multiparty computation (MPC) [BOGW88, CCD88]. Classical MPC protocols tolerate passive corruption of fewer than half the parties, or active corruption of fewer than one third, with reconstruction thresholds near $n/2$ and $n/3$ respectively.

What happens if, instead of learning a few shares in full, an adversary learns a little about *every* share? The question is motivated by side-channel attacks, which extract information from physical implementations through observations such as running time and power consumption [Koc96, KJJ99]. Benhamouda, Degwekar, Ishai, and Rabin [BDIR18] formalized *locally leakage-resilient secret sharing*.¹ In this model the adversary obtains a bounded number of bits from each share through a function of its choice, and local leakage resilience requires the joint leakage to be statistically independent of the secret. The guarantee is strong because the leakage functions are arbitrary: even one-bit leakage permits any Boolean function of each share, not merely a bit of its representation.

Local leakage can be surprisingly powerful. For suitable parameters over binary extension fields, Reed–Solomon repair algorithms [GW16] even recover the entire secret from one bit of leakage per share. Over prime fields, Benhamouda et al. [BDIR18] proved resilience to arbitrary one-bit local leakage when $k \geq 0.907n$, and substantial effort has gone into lowering this threshold: independent improvements gave $0.8675n$ [MPCSW21] and $0.85n$ [BDIR21], followed by $0.78n$ [MNPCW22], $0.69n$ [KK23], and $0.668n$ [Kas25].² Below half, resilience is known only for restricted leakage classes: physical-bit leakage with high probability over randomly chosen evaluation points in sufficiently large prime fields [MNPC⁺21], quadratic-residue and almost all one-bit local leakage [Ngu24], and sufficiently unbalanced leakage [KK23]. Previous guarantees against arbitrary one-bit local leakage all require threshold rates strictly above half.

Benhamouda et al. [BDIR18, BDIR21] conjectured that Shamir sharing over prime fields is resilient to arbitrary one-bit local leakage at every positive constant rate.³ Despite the subsequent improvements, this conjecture remained open even at rate half. There is also a technical obstacle. Maji et al. [MPCSW21] showed that the bound obtained by summing Fourier magnitudes in earlier analyses cannot establish resilience below rate half, already for quadratic-residue leakage.⁴

Summary of our results. We prove that (n, k) -Shamir sharing is resilient whenever $k \geq c_{\text{bh}}n$, for an absolute constant $c_{\text{bh}} < 1/2$, establishing the conjecture in a range that extends below half. We also obtain logarithmic-bit leakage resilience above half (by any fixed constant), and guarantees against restricted leakage families at every positive constant rate.

1.1 Our contributions

We first introduce notation. Consider (n, k) -Shamir sharing with n parties, reconstruction threshold k , and distinct nonzero evaluation points $\alpha = (\alpha_1, \dots, \alpha_n)$ over a prime field $\mathbb{F}_p$, where $p > n$. To share a secret $s \in \mathbb{F}_p$, this scheme samples a uniformly random polynomial $P \in \mathbb{F}_p[X]$ of degree less than k such that $P(0) = s$ and gives party i the share $P(\alpha_i)$. An m -bit local leakage function is a

¹The notion also appears implicitly in the work of Goyal and Kumar [GK18].

²The last two assume a field of size $2^{o(n)}$.

³Their conjecture applies more generally to secret-sharing schemes based on MDS codes.

⁴For a share $x \in \mathbb{F}_p$, this one-bit leakage outputs 1 if $x = y^2$ for some $y \in \mathbb{F}_p$, and 0 otherwise.

tuple of maps $\tau = (\tau_1, \tau_2, \dots, \tau_n)$, where $\tau_i: \mathbb{F}_p \rightarrow \{0, 1\}^m$. For $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{F}_p^n$, write

$$\tau(\mathbf{x}) := (\tau_1(x_1), \dots, \tau_n(x_n)).$$

The *leakage distribution* induced by τ on secret s is the distribution of $(\tau_1(P(\alpha_1)), \dots, \tau_n(P(\alpha_n)))$, where P is sampled as above. The scheme is ε -resilient to m -bit local leakage if, for every such m -bit local leakage function, the leakage distributions of any two secrets have statistical distance at most ε . We call k/n the *threshold rate* and $m/\log_2 p$ the *leakage rate*, the fraction of each share's bit length revealed by the leakage. All following results hold for every choice of evaluation points and all sufficiently large n , with constants and the required lower bound on n depending only on the fixed parameters. In particular, there is no upper bound on p .

Below half. Our first result crosses the $1/2$ rate for one-bit local leakage.

Theorem 1 (Below half). *There is an absolute constant $c_{\text{bh}} < 1/2$ such that every (n, k) -Shamir scheme with $k \geq c_{\text{bh}}n$ is $\exp(-\Omega(n))$ -resilient to one-bit local leakage.*

The previous best bound for arbitrary one-bit leakage was $0.668n$, under the field-size restriction $p = 2^{o(n)}$ [Kas25]. Our theorem crosses half without this restriction.⁵ In particular, the theorem covers $k = \lceil n/2 \rceil$, the reconstruction threshold at the classical $n/2$ passive-corruption bound in MPC. The proof gives the explicit, unoptimized constant $c_{\text{bh}} = 1/2 - 10^{-14}$ (Corollary 6). The full BDIR conjecture remains open, in particular at threshold rate $1/3$. At smaller thresholds, Nielsen and Simkin [NS20] give an inefficient one-bit leakage attack when k is of order $n/\log p$, which is $n/\log n$ when $p = \text{poly}(n)$. Closing this gap remains an open problem.

Asymptotically optimal leakage above half. Progress on the reconstruction threshold has concentrated on one-bit leakage. A second basic question is how many bits per share Shamir sharing withstands. We show that, at every threshold rate above half, the answer is logarithmic in n : for polynomial-size fields $p = \text{poly}(n)$, this is a constant fraction of each share's bit length.

Theorem 2 (Logarithmic leakage above half). *Fix $0 < \delta < 1/2$. Any (n, k) -Shamir sharing with $k \geq (1/2 + \delta)n$ is $\exp(-\Omega_\delta(n^{1-\delta/12}))$ -resilient to $\lfloor (\delta/24) \log_2 n \rfloor$ -bit local leakage.*

Previous guarantees of a constant leakage rate required a threshold rate tending to one. Benhamouda et al. [BDIR21, Corollary 4.13] obtain it for $n < p \leq 2n$ and $k > n - n^{1/4}$. Our threshold rate stays fixed above half, and the field may be arbitrarily large.

The number of leaked bits is tight up to a constant factor depending on δ . Boudgoust and Simkin [BS26] give an efficient attack using $\log_2 k + O(1)$ bits per share over arbitrary finite fields.

The proof reduces m -bit leakage resilience to list recovery of the dual code with input lists of size $2^m - 1$; for one bit this is ordinary list decoding. Letting m grow requires the dependence of the list size on the input-list size, which we extract from the proofs of Jeronimo [Jer26] and of Dao, Kominers, and Thaler (DKT) [DKT26] in Sections A and B.

The criterion of Maji, Paskin-Cherniavsky, Suad, and Wang [MPCSW21, Technical Lemma 1] is also a list-recovery condition on the dual code, and combined with the same bound it yields Theorem 2 for every fixed m . Its parameters, however, degrade doubly exponentially in m : its input lists have size $2^m T^2$ with $T = 2^{\Theta(m/\sigma)}$ and $\sigma = O(4^{-m})$, because the underlying ℓ_1 bound sums over all 2^{mn} leakage outputs. This direct application gives only $O(\log \log n)$ bits.

⁵This allows a λ -bit prime p with $n = O(\lambda)$, a common parameter regime in MPC.

Restricted leakage families at every constant threshold rate. Our third result concerns every positive constant threshold rate, including below half, for two restricted leakage families: quadratic-residue leakage, where party i reveals whether $a_i P(\alpha_i) + b_i$ is a square, for arbitrary $a_i \in \mathbb{F}_p^*$ and $b_i \in \mathbb{F}_p$; and almost all tuples of local leakage functions revealing $\Theta(\log p)$ bits per share.

Theorem 3 (Structured leakage at constant threshold rate). *Fix $0 < c < 1$. There are constants $\eta_c, a_c, b_c > 0$ such that any (n, k) -Shamir sharing with $k \geq cn$ is*

1. $\exp(-a_c n \log p)$ -resilient to quadratic-residue leakage (with arbitrary affine shifts), and
2. for every integer $1 \leq m \leq \eta_c \log_2 p$, $\exp(-a_c n \log p)$ -resilient to all but an $\exp(-b_c \sqrt{p})$ fraction of m -bit local leakage functions.

Nguyen [Ngu24] proved resilience to quadratic-residue and random one-bit leakage using higher-order Fourier analysis, but the bounds require a field size exponential in n at constant threshold rate. Unlike Theorem 2, the leakage rate in part 2 stays constant for every prime $p > n$, not only polynomial-size fields, and below half. For superpolynomial-size fields, this separates worst-case from average-case leakage: the attack of Boudgoust and Simkin [BS26] limits the worst-case leakage rate to $O(\log k / \log p) = o(1)$.

At smaller thresholds, quadratic-residue leakage can be insecure: for $n = p - 1$ and $k = O(\sqrt{n})$, Kopparty’s algorithm for recovering a polynomial from noisy quadratic-character values [Kop26] yields an attack with the same shifted quadratic-residue leakage (Section 5.5).

From Shamir sharing to codes. For distinct evaluation points $\alpha \in \mathbb{F}_p^n$ and nonzero multipliers $v \in (\mathbb{F}_p^*)^n$, the generalized Reed–Solomon code of dimension d is

$$\text{GRS}_{\alpha, v}(n, d) = \{(v_i Q(\alpha_i))_{i=1}^n : Q \in \mathbb{F}_p[X], \deg Q < d\}.$$

The shares of the zero secret in an (n, k) -Shamir sharing are uniform on $C_0 = \text{GRS}_{\alpha, \alpha}(n, k - 1)$, and the shares of secret s are uniform on the translate $s\mathbf{1} + C_0$, where $\mathbf{1} = (1, \dots, 1)$. Call a linear code $C \subseteq \mathbb{F}_p^n$ ε -resilient to m -bit local leakage if, under every tuple of m -bit leakage maps, a uniform codeword and a vector of n independent uniform field elements have leakage distributions within statistical distance ε . We prove all three results in this code form (Theorems 6 to 8), as a pseudorandomness property of GRS codes under local leakage, and the guarantees for Shamir sharing follow: for arbitrary m -bit local leakage, resilience of the code implies resilience of the scheme with twice the error, and conversely with error larger by a factor $O(n)$ (Lemma 1).

Technical Highlights. We develop an analytical framework in which all three theorems are proved. It combines the Efron–Stein orthogonal decomposition over the product space of leakage outputs with Fourier analysis over the uniform measure on the inputs. Its key feature is flexibility: the framework organizes the leakage analysis into orthogonal components, and each component can be analyzed either through its L^2 -norm using linear Fourier analysis, or through its L^1 -norm using higher-order Fourier analysis. Previous analyses each took a single route. Benhamouda et al. [BDIR18, BDIR21] and their successors [MNPC⁺21, MPCSW21] bound an ℓ_1 sum of Fourier magnitudes over the dual code; Klein and Komargodski [KK23, Kas25] bound an ℓ_2 quantity obtained from Pinsker’s inequality; Nguyen [Ngu24] bounds Gowers norms of the leakage functions. The framework brings these analytic approaches together, allowing different estimates on different components. Their combination within the same decomposition is what crosses half.

Concurrent and independent work. Sun and Wootters [SW26a] independently prove one-bit local leakage resilience of Shamir sharing at a constant threshold rate below half, obtaining the same qualitative guarantee as [Theorem 1](#). They also prove resilience to any fixed number of leaked bits per share above half. The approaches share an important feature: both use list recovery of the dual code for small supports and Gowers-norm estimates for large supports. Our work additionally establishes logarithmic-bit resilience above half and the restricted-leakage guarantees at every positive constant threshold rate ([Theorems 2 and 3](#)). Sun and Wootters also obtain existential and quantum-algorithmic results for worst-case optimal polynomial intersection, which we do not study here.

1.2 Technical overview

By the reduction described above ([Lemma 1](#)), it suffices to prove the code form of our results: local leakage cannot distinguish a uniform codeword from independent uniform field elements. Fix a GRS code $C = \text{GRS}_{\alpha,v}(n, k-1)$ and leakage maps $\tau_i: \mathbb{F}_p \rightarrow \{0, 1\}^m$. Let $\mathbf{U}_C$ and $\mathbf{U}_{\mathbb{F}_p^n}$ be uniformly distributed on C and $\mathbb{F}_p^n$, respectively. The goal is to show that the statistical distance between $\tau(\mathbf{U}_C)$ and $\tau(\mathbf{U}_{\mathbb{F}_p^n})$, which is called *leakage distance*, is small.

The framework. Under independent uniform inputs, the leakage outputs are independent. Thus $\tau(\mathbf{U}_{\mathbb{F}_p^n})$ has a product distribution $\nu = \prod_i \nu_i$, where ν_i is the distribution of $\tau_i(\mathbf{U}_{\mathbb{F}_p})$. This allows us to use Fourier analysis on general product spaces ([O'D14, Chapter 8]). In particular, the Efron–Stein decomposition is a standard way to group a Fourier expansion into orthogonal components indexed by coordinate sets, without choosing an explicit basis. We first express the leakage distance as a norm under ν , then apply this decomposition and use the code’s linear structure to identify the components. [Section 3](#) develops this approach in the following steps.

Step 1: Write the leakage distance as a norm. For each leakage output $\mathbf{b} = (b_1, b_2, \dots, b_n)$, we compare its probability under leakage from a uniform codeword with $\nu(\mathbf{b})$. To express this ratio, start with the corresponding ratio on the inputs:

$$f_C(\mathbf{x}) = \frac{\Pr[\mathbf{U}_C = \mathbf{x}]}{\Pr[\mathbf{U}_{\mathbb{F}_p^n} = \mathbf{x}]} = \frac{p^n}{|C|} \mathbb{1}[\mathbf{x} \in C],$$

whose mean under uniform input is one. Leakage forgets which input produced $\mathbf{b}$, so the output ratio is the average of this input ratio over all compatible inputs. This naturally gives the Markov operator ([Definition 11](#))

$$(\mathsf{T}f)(\mathbf{b}) = \mathbb{E}[f(\mathbf{U}_{\mathbb{F}_p^n}) \mid \tau(\mathbf{U}_{\mathbb{F}_p^n}) = \mathbf{b}].$$

Its one-coordinate version is $(\mathsf{T}_i f)(b) = \mathbb{E}[f(\mathbf{U}_{\mathbb{F}_p^n}) \mid \tau_i(\mathbf{U}_{\mathbb{F}_p^n}) = b]$, and independence gives $\mathsf{T} = \bigotimes_i \mathsf{T}_i$. Thus, we have ([Lemma 5](#))

$$(\mathsf{T}f_C)(\mathbf{b}) = \frac{\Pr[\tau(\mathbf{U}_C) = \mathbf{b}]}{\nu(\mathbf{b})}.$$

The leakage distance is therefore the average deviation of this ratio from one:

$$\text{SD}(\tau(\mathbf{U}_C), \tau(\mathbf{U}_{\mathbb{F}_p^n})) = \frac{1}{2} \mathbb{E}_{\mathbf{b} \sim \nu} |(\mathsf{T}f_C)(\mathbf{b}) - 1| = \frac{1}{2} \|\mathsf{T}f_C - 1\|_{1,\nu}.$$

Thus we need to bound how far $\mathsf{T}f_C$ is from the constant function 1, averaging over the product distribution ν . Here and below, we only consider outputs with $\nu(\mathbf{b}) > 0$.

Step 2: Separate the contributions of different coordinate sets. The Efron–Stein decomposition separates a function on a product space into orthogonal components indexed by coordinate sets

$A \subseteq [n]$ (Definition 10). A component depends only on A and disappears when any coordinate in A is averaged out: it records an interaction requiring all those coordinates. Apply this decomposition to $\mathsf{T}f_C$ under the leakage distribution ν . Its constant component ($A = \emptyset$) is one, so $\mathsf{T}f_C - 1$ is the sum of its nonconstant components. To identify them, we can instead decompose f_C under the uniform distribution on $\mathbb{F}_p^n$ and then apply T . Because leakage acts separately on each coordinate, the two operations commute (Lemma 4):

$$(\mathsf{T}f_C)^{=A} = \mathsf{T}(f_C^{=A}), \quad \mathsf{T}f_C - 1 = \sum_{\emptyset \neq A \subseteq [n]} \mathsf{T}(f_C^{=A}).$$

For all distinct coordinate sets A and B , the corresponding output components are orthogonal under ν . We can therefore analyze the dependence on each coordinate set separately.

Step 3: Identify the components using the dual code. To make these components explicit, use the linear structure of the code. Fourier characters detect its linear constraints: the character $\chi_{\mathbf{y}}(\mathbf{x}) = \prod_i \chi_{y_i}(x_i)$, where $\chi_a(x) = \exp(2\pi i ax/p)$, is identically one on C when $\mathbf{y} \in C^\perp$, and otherwise averages to zero over C . Thus the Fourier coefficients of f_C are one on $C^\perp$ and zero elsewhere. Grouping these characters by their nonzero coordinates gives exactly the Efron–Stein components (Lemmas 2 and 3):

$$f_C^{=A} = \sum_{\mathbf{y} \in C^\perp: \text{supp}(\mathbf{y})=A} \chi_{\mathbf{y}}.$$

Since $C^\perp$ has minimum distance k , all components with $0 < |A| < k$ vanish. We therefore only need to bound components with $|A| \geq k$.

Step 4: Choose how to bound the components. The two tools below provide different kinds of estimates: list recovery bounds squared L^2 norms, while Gowers norms bound L^1 norms. We need not choose one tool for every support. Using $\|\cdot\|_{1,\nu} \leq \|\cdot\|_{2,\nu}$ and orthogonality, we can bound a group of components by the square root of the sum of their squared L^2 norms. For the others, the triangle inequality lets us add individual L^1 bounds. Choosing a cutoff $k-1 \leq r_0 \leq n$ gives (Proposition 1)

$$\text{SD}(\tau(\mathbf{U}_C), \tau(\mathbf{U}_{\mathbb{F}_p^n})) \leq \frac{1}{2} \left(\sum_{k \leq |A| \leq r_0} \|\mathsf{T}(f_C^{=A})\|_{2,\nu}^2 \right)^{1/2} + \frac{1}{2} \sum_{|A| > r_0} \|\mathsf{T}(f_C^{=A})\|_{1,\nu}.$$

Above half we take $r_0 = n$, using only the first part. For the restricted leakage families we take $r_0 = k-1$, using only the second. Below half we choose an intermediate cutoff close to n and combine both tools.

Above half: L^2 norms and list recovery of the dual code. Here we take $r_0 = n$ and then bound the sum of squared component norms. The first question is how the leakage acts on a component, which is a sum of characters $\chi_{\mathbf{y}}$ over dual words with support A . Applying T to every coordinate loses the orthogonality among them, but applying it to only $k-1$ coordinates $I \subseteq A$ does not: two dual words with support A that agree outside I differ on at most $k-1$ coordinates, hence coincide, so their characters on $A \setminus I$ are distinct and still orthogonal; and applying the remaining T_i afterwards can only shrink an L^2 norm by the contraction property of Markov operators. This gives (Lemma 8)

$$\|\mathsf{T}(f_C^{=A})\|_{2,\nu}^2 \leq \sum_{\mathbf{y} \in C^\perp: \text{supp}(\mathbf{y})=A} \prod_{i \in I} \|\mathsf{T}_i \chi_{y_i}\|_{2,\nu_i}^2.$$

So each dual word is charged $k-1$ one-coordinate factors $\|\mathsf{T}_i \chi_a\|_{2,\nu_i}^2$. There are two facts about them (Lemma 9). Their sum over $a \neq 0$ is at most $Q-1$, where $Q = 2^m$. And each is at most $\eta_Q < 1$.

Now comes the counting problem: a sum over all dual words with support A , summed over A , of products of $k - 1$ factors. Spending all $k - 1$ factors on decay leaves a bare count of dual words, which is p^{n-k+1} and useless. The trick is to split the factors. Keep j of them, bound the other $k - 1 - j$ by η_Q , and look at the sum that remains. It is linear in the weights $w_i(a) = \|\mathbf{T}_i \chi_a\|_{2, \nu_i}^2$ of each coordinate separately, with nonnegative coefficients, under the constraints $w_i(a) \in [0, 1]$ and $\sum_{a \neq 0} w_i(a) \leq Q - 1$. Such a sum is maximized at an extreme point, which puts weight one on $Q - 1$ frequencies and zero elsewhere (Lemma 10). After this replacement the sum counts dual words that agree with lists $V_i \subseteq \mathbb{F}_p^*$ of size $Q - 1$ on at least j coordinates (Lemma 11). This count is bounded by the list size at radius $n - j$, in the notation $\text{List}_{C^\perp}(R, \ell)$ (Definition 9):

$$\sum_{|A| \geq k} \|\mathbf{T}(f_C^{\bar{A}})\|_{2, \nu}^2 \leq \eta_Q^{k-1-j} \text{List}_{C^\perp}(n - j, Q - 1).$$

The lists live on Fourier frequencies. For one bit they are singletons and this is list decoding.

The dual of a GRS code is a GRS code, so either of the list-recovery results of Jeronimo and DKT [Jer26, DKT26] makes $\text{List}_{C^\perp}(R, \ell)$ polynomial in n for fixed input-list size ℓ and fixed gap $\zeta > 0$, at radius $R \leq k - 1 - \zeta n$ (Theorem 4). With $j = n - R$ there are at least $2R - n$ factors left for decay, and the bound is $\frac{1}{2} \eta_Q^{R-n/2} \sqrt{\text{List}_{C^\perp}(R, Q - 1)}$ (Theorem 5). This also says exactly where the argument stops: it needs $R > n/2$ with $R < k$, hence $k > n/2$. Below half no choice of $j \leq k - 1$ reaches a radius covered by this polynomial-list bound. Above $1/2 + \delta$, a linear number of decay factors remain, so their product absorbs the polynomial list size. Increasing the leakage alphabet has two costs: the local decay becomes weaker, and the list-recovery bound becomes larger. The same linear number of factors can absorb both costs as long as the logarithm of the list bound stays smaller than the decay exponent. Keeping the dependence on Q explicit in these proofs (Sections A and B) allows Q to grow to $n^{\delta/24}$, giving the logarithmic leakage in Theorem 2.

Every constant threshold rate: L^1 norms and iterated Cauchy–Schwarz. For the restricted families, we take $r_0 = k - 1$ and bound each component in L^1 . By a simple calculation, the L^1 norm of each component is a sum of absolute values of averages (Lemma 6), each of the following form:

$$\Lambda_\Psi(\mathbf{f}) = \mathbb{E}_z \left[\prod_{i \in A} f_i(L_i(\mathbf{z})) \right].$$

Here $\mathbf{z} \in \mathbb{F}_p^{k-1}$ is the vector of independently and uniformly chosen polynomial coefficients, and $L_i(\mathbf{z})$ is the i -th coordinate of the resulting codeword. We write $\Psi = (L_i)_{i \in A}$, where $|A| \geq k$. The functions f_i are bounded by one and determined by the leakage maps and outputs (see Section 5.1).

Such averages arise naturally in additive combinatorics. For indicator functions, they give normalized counts of configurations described by linear forms, such as arithmetic progressions [TV06, GT10]. Repeated applications of Cauchy–Schwarz bound these averages in terms of Gowers norms [Gow01, GT10].

Nguyen [Ngu24] uses the scalar generalized von Neumann inequality to bound such averages. For a suitable Gowers order t , it gives

$$|\Lambda_\Psi(\mathbf{f})| \leq \min_{i \in A} \|f_i\|_{U^t}.$$

This retains only one small factor to compensate for exponentially many averages, leading to the large field sizes in that analysis. Nguyen [Ngu24, Remark 1] conjectured that a better understanding of this inequality for the linear forms of MDS codes and the leakage functions arising here could lead to smaller-field bounds.

We observe that Manners’s formulation [Man21] allows us to retain a product of Gowers norms. The idea is to group several independent forms into one vector-valued map. The Gowers norm of the corresponding product function then factors into the individual Gowers norms. The coordinate forms of a GRS code are MDS: any $k - 1$ of them are independent. This structure gives, at every constant threshold rate $c > 0$, a constant Gowers order t and a set $J \subseteq A$ such that

$$|\Lambda_\Psi(\mathbf{f})| \leq \prod_{i \in J} \|f_i\|_{U^t}, \quad |J| = \Omega_c(n).$$

See Lemma 12 and Corollary 3. The key saving comes from multiplying linearly many factors: even when the retained Gowers norms are close to one, a fixed gap below one gives $\exp(-\Omega(n))$ decay for each average. This will be crucial for the result below half, where the norms need not decrease with p .

For quadratic-residue leakage and almost all local leakage maps, the local Gowers norms are at most $p^{-\Omega_c(1)}$, by character-sum estimates and concentration, respectively (Sections 5.3 and 5.4). The product bound therefore gives the stronger $\exp(-\Omega_c(n \log p))$ decay. This absorbs the sum over supports and leakage outputs even when the number of leaked bits is a sufficiently small constant multiple of $\log p$. Hence $p > n$ suffices, giving Theorem 3; the parameter calculation is in Proposition 3.

Why not arbitrary leakage at every constant rate? For arbitrary one-bit leakage, the Gowers norms need not be small enough for the resulting exponential decay to outweigh the exponentially many terms. This becomes more restrictive at smaller threshold rates, where the bound retains fewer Gowers-norm factors.

Below half: both tools, and a uniform bound for one bit. We combine the two tools to handle arbitrary one-bit leakage below half, choosing a cutoff r_0 close to n , using L^2 bounds for the smaller supports and L^1 bounds for the larger ones.

Smaller supports. The dual words contributing to these components have many zero coordinates. These zeros provide additional agreements with the list $\{0\}$ when applying list decoding. Fewer agreements must therefore come from the Fourier factors, leaving more factors available to provide decay. A modification of the earlier counting argument uses these extra agreements and bounds all supports of a given size together (Lemma 14 and Corollary 5). The resulting estimate makes their total squared L^2 contribution exponentially small for supports that omit a fixed fraction of the coordinates, at threshold rates sufficiently close to half (Lemma 15).

Larger supports. These supports have too few zero coordinates for the counting argument, so we turn to the linear-form averages. For one-bit leakage, the L^1 norm of each component is the absolute value of a single such average (Lemma 7). Its factors f_i are obtained by representing each leaked bit as ± 1 and subtracting its mean under uniform input. Using Fourier symmetry and the fact that these functions take at most two values, we prove that

$$\|f_i\|_{U^3} \leq \kappa_0 < 1$$

for an absolute constant κ_0 (Lemma 16). The product bound retains linearly many such factors even for full support at rate half (Corollary 3).

The Gowers-norm bound controls only some of the factors in the average. The other factors are bounded by their maximum absolute values, which can be as large as two. Multiplying these bounds can therefore offset the saving from the Gowers norms. When the total squared bias is small, this loss is controlled; otherwise, the smaller variances give exponential decay by Cauchy–Schwarz and MDS independence, following a principle similar to that in [KK23, Section 6]. Together, these

estimates make each large-support contribution exponentially small, uniformly over the leakage maps (Lemma 17). Taking the cutoff sufficiently close to n makes the number of remaining supports small enough for this decay to survive summation (Proposition 4).

Putting it together. At the limiting parameters of rate half and zero decoding gap, both estimates leave a strict exponential margin. By continuity, this margin survives at a fixed rate slightly below half and a small positive decoding gap, with both ranges of supports still covered. The list-decoding theorem is used only at that positive gap. This proves Theorem 1; Section 6.3 gives the parameter choices.

1.3 Related work

New constructions of leakage-resilient secret sharing. Following [GK18, BDIR18], a line of work has developed secret-sharing schemes designed to withstand local leakage. General compilers support arbitrary monotone access structures while providing strong leakage guarantees with controlled share-size overhead [SV19, ADN⁺19]. Other constructions address adaptive leakage involving bounded groups of colluding parties [KMS19, CGG⁺20], or improve share sizes [CKOS22]. Such constructions need not preserve the algebraic structure of the underlying scheme, including linearity, which is important in applications such as MPC. In contrast, our work establishes leakage resilience of Shamir scheme.

Local leakage resilience of existing linear schemes. Shamir and additive secret sharing are the most common linear schemes widely used in applications. For additive n -out-of- n sharing over prime fields, Maji et al. [MNPC⁺22] give a tight analysis of the parity-of-parity attack, establishing an optimal lower bound on the number of shares needed for resilience to one-bit leakage. Koga and Abe [KA26] obtain tight one-bit leakage bounds and further bounds for larger output alphabets.

Attacks on local leakage resilience. Nielsen and Simkin present one-bit attacks at sublinear thresholds of order $n/\log n$ [NS20]; Hoffmann and Simkin develop robust attacks that can tolerate noise in a constant fraction of the leakage outputs [HS23]. Other attacks exploit particular leakage functions or prime-field repair procedures [Ngu24, CSTW24]. Boudgoust and Simkin give a perfectly correct attack on schemes with linear reconstruction using $\log_2 k + O(1)$ leaked bits per share over arbitrary finite fields [BS26]. The shifted quadratic-residue attack from [Kop26] is discussed in Section 5. None of these statements establishes impossibility at threshold rate half for exactly one-bit leakage. Our logarithmic-bit guarantee against arbitrary maps is above half; the below-half result concerns one bit and does not cover the full sublinear-threshold range.

Physical-bit, Hamming-weight, and noisy leakage. Physical-bit leakage reveals selected bits in a fixed binary representation of each share, rather than the output of an arbitrary bounded-output function. Over prime fields, Maji et al. [MNPC⁺21] prove resilience to multiple physical bits per share for every reconstruction threshold $k \geq 2$, using random evaluation points and sufficiently large fields. Subsequent work studies physical-bit leakage over extension fields [MNPCY24, Ngu25]. Hwang et al. [HMNY25] characterize secure evaluation points for n -out-of- n Shamir sharing over prime fields, while Venkitesh [Ven26] provides partial derandomization in certain extension-field regimes. For public-coefficient inner-product masking, Faust et al. [FMM⁺26] establish physical-bit leakage guarantees over Mersenne prime fields.

Hamming-weight leakage reveals the number of ones in a share’s binary representation. It has been analyzed for inner-product masking over binary extension fields [BHMY26] and for additive

sharing over cyclic groups whose moduli are close to powers of two [BHM⁺26a, BHM⁺26b]. Noisy-leakage models instead constrain the leakage channel through a noise assumption rather than its output length [PR13, DDF14, FMM⁺24, JMB26, GM26]. These results exploit the prescribed leakage function, the representation of shares, or the noise; they do not give resilience to arbitrary local leakage.

List decoding of Reed–Solomon codes. Sudan’s interpolation algorithm and its extension by Guruswami and Sudan established the classical algorithmic approach and the Johnson-radius benchmark [Sud97, GS99]. Progress beyond that benchmark includes random puncturing, generalized Singleton bounds, and improved large-error-radius and list-recovery guarantees [RW14, ST20, FKS22, GLS⁺24]. For a code of rate R , the large-alphabet capacity target is an error fraction $1 - R - \zeta$, for any fixed gap $\zeta > 0$. Brakensiek, Gopi, and Makam proved that generic Reed–Solomon codes reach this target over sufficiently large fields [BGM23]; [AGG⁺25] reduced the field-size requirement for random evaluation points to a sufficiently large constant times the block length. These guarantees concern generic or random codes, not every evaluation tuple.

The recent results of [BCP⁺26, Jer26] reach capacity for arbitrarily fixed evaluation points over prime fields. The former supplies a new interpolation-based algorithmic approach; Jeronimo’s theorem gives the field-independent list bound $n^{c_{\zeta, \ell}}$ for every fixed input-list size ℓ , every prime $p \geq n$, and sufficiently large n . Dao, Kominers, and Thaler [DKT26, Theorem G.2] also obtain list-recovery guarantees for fixed evaluation points, providing another route to the field-independent bound used here. We use $\ell = 1$ for ordinary list decoding and $\ell = 2^m - 1$ for m -bit leakage. For growing m , we keep the dependence on ℓ explicit in Jeronimo’s proof and in DKT’s finite estimates (Sections A and B). The field-independent bound matters because our security bound must not deteriorate when p grows. Coordinate scaling extends these guarantees to generalized Reed–Solomon dual codes.

Random linear codes provide a different route to capacity for list decoding [GHSZ02, GHK11, LW21] and list recovery [LS25, DMRR25, GG26]; folded Reed–Solomon codes also achieve list-recovery capacity [GR08]. For fixed alphabets, list-decoding capacity is expressed using the appropriate entropy function and should not be identified with the large-alphabet limit $1 - R$. Our transfer applies coding guarantees to the *dual* code: the same statement uses ordinary list decoding for one-bit outputs and list recovery with input lists of size $2^m - 1$ for m -bit outputs. This is not direct recovery of shares from the leakage. A preimage of a bit can contain $\Theta(p)$ symbols; the lists in the transfer instead arise by replacing the Fourier weights $\|\mathbf{T}_i \chi_a\|_2^2$ by list indicators in a weighted counting bound.

Repairing Reed–Solomon codes. Repair bandwidth measures the amount of data downloaded to recover an erased symbol and is a central parameter in distributed storage [DGW⁺10]. For Reed–Solomon codes, Guruswami and Wootters [GW16] develop bandwidth-efficient linear repair schemes, and Tamo, Ye, and Barg [TYB17] achieve the cut-set bound over suitable large extension fields. Over prime fields, Con, Shutty, Tamo, and Wootters [CSTW24] use exponential sums to construct nonlinear repair procedures for low-rate Reed–Solomon codes that download only a constant number of bits from each helper. These results connect repair to local leakage: viewing the secret as an erased evaluation, a repair procedure yields a reconstruction attack whenever each helper’s message fits the permitted leakage budget.

Discrepancy, zero-error list recovery, and OPI. The survey of Resch and Venkitesh [RV25] discusses the relation between local leakage and zero-error list recovery above capacity. Doron et

al. [DLM⁺26] prove near-expected codeword counts for random linear codes and derive local leakage resilience for ramp sharing with arbitrary positive linear reconstruction thresholds and a sublinear threshold gap. Their polynomial field sizes are smaller than the block length, and their codes and privacy/reconstruction tradeoff differ from the GRS threshold setting here. This prior connection is distinct from the dual-code transfer in Section 4.

Sun and Wootters [SW26b] connect Fourier estimates for local leakage to worst-case optimal polynomial intersection (OPI) and obtain improvements over the semicircle satisfaction guarantee. Horinaga and Yamakawa [HY26] improve both existential and quantum-algorithmic bounds; Jo [Jo26] gives a quantum sampler based on complete list decoding.

Organization. Section 2 gives the preliminaries and the Shamir reduction. Section 3 develops the orthogonal decomposition of the leakage distance. Section 4 proves the list-recovery transfer and logarithmic-bit leakage resilience above half. Section 5 uses the product bound for Gowers norms to establish the restricted-leakage results at every constant threshold rate. Section 6 combines the two tools to go below half. Section A gives the quantitative list-recovery bound used for logarithmic-bit leakage; Section B gives an alternative derivation from DKT.

2 Preliminaries

Throughout, p is an odd prime and $\mathbb{F}_p$ the field with p elements; the main theorems take $p > n$. Logarithms are natural unless a base is shown. Vectors are written in bold. Write $[n] = \{1, \dots, n\}$, $\text{supp}(\mathbf{y}) = \{i : y_i \neq 0\}$, $\text{wt}(\mathbf{y}) = |\text{supp}(\mathbf{y})|$, and $d_H(\mathbf{x}, \mathbf{y}) = \text{wt}(\mathbf{x} - \mathbf{y})$. The binary entropy is $h(t) = -t \log t - (1-t) \log(1-t)$, with $h(0) = h(1) = 0$. For a finite set S , U_S denotes the uniform distribution on S ; a uniform random vector is written $\mathbf{U}_S$.

Definition 1 (Statistical distance). For distributions P, Q on a finite set Ω , the statistical distance between them is defined as

$$\text{SD}(P, Q) = \frac{1}{2} \sum_{x \in \Omega} |P(x) - Q(x)|.$$

2.1 Generalized Reed–Solomon codes

Definition 2 (Linear codes and Reed–Solomon codes). A linear code C of length n over $\mathbb{F}_p$ is a subspace of $\mathbb{F}_p^n$; its elements are codewords. Its parameters $[n, k, d]_p$ are its length, dimension, and minimum Hamming distance between distinct codewords. Its rate is k/n . Its dual is $C^\perp = \{\mathbf{y} \in \mathbb{F}_p^n : \sum_i x_i y_i = 0 \text{ for every } \mathbf{x} \in C\}$.

For distinct evaluation points $\boldsymbol{\alpha} \in \mathbb{F}_p^n$, $1 \leq k \leq n$, and multipliers $\mathbf{v} \in (\mathbb{F}_p^*)^n$, the generalized Reed–Solomon code of length n and dimension k is

$$\text{GRS}_{\boldsymbol{\alpha}, \mathbf{v}}(n, k) = \{(v_i Q(\alpha_i))_{i=1}^n : \deg Q < k\}.$$

Taking $\mathbf{v} = \mathbf{1}$ gives an Reed–Solomon code. A code of dimension k is maximum-distance-separable (MDS) if its minimum distance is $n - k + 1$, or equivalently if projection onto any k coordinates is a bijection onto $\mathbb{F}_p^k$.

GRS codes are MDS, and their duals are GRS codes on the same evaluation points: for $C = \text{GRS}_{\boldsymbol{\alpha}, \mathbf{v}}(n, k - 1)$ with $2 \leq k \leq n$, $C^\perp$ is a GRS code of dimension $n - k + 1$ and minimum distance k . Rescaling coordinate i by v_i^{-1} yields an ordinary Reed–Solomon code of the same dimension and preserves Hamming distances.

2.2 Shamir secret sharing

Definition 3 (Shamir secret sharing). Let $\alpha \in (\mathbb{F}_p^*)^n$ have distinct coordinates. The (n, k, α) -Shamir scheme with n parties and reconstruction threshold k is defined as follows.

1. *Sharing*: to share $s \in \mathbb{F}_p$, $\text{share}_\alpha(s)$ samples $Z_1, \dots, Z_{k-1}$ independent and uniform in $\mathbb{F}_p$, forms $P(X) = s + \sum_{j=1}^{k-1} Z_j X^j$, and gives party i the share $P(\alpha_i)$.
2. *Reconstruction*: any k shares determine s by Lagrange interpolation.

The shares of the zero secret are uniform on $C_0 = \text{GRS}_{\alpha, \alpha}(n, k-1)$, and the shares of secret s are uniform on $s\mathbf{1} + C_0$. For every secret, any $k-1$ shares are independent uniform field elements, so they reveal nothing about the secret.

2.3 Local leakage resilience

Definition 4 (m -bit local leakage). For a positive integer m , an m -bit local leakage function is a tuple $\tau = (\tau_1, \dots, \tau_n)$ of maps $\tau_i: \mathbb{F}_p \rightarrow \{0, 1\}^m$. For $\mathbf{x} \in \mathbb{F}_p^n$ write $\tau(\mathbf{x}) = (\tau_1(x_1), \dots, \tau_n(x_n))$.

Definition 5 (Leakage resilience of a code). A linear code $C \subseteq \mathbb{F}_p^n$ is ε -resilient to m -bit local leakage if $\text{SD}(\tau(U_C), \tau(U_{\mathbb{F}_p^n})) \leq \varepsilon$ for every m -bit local leakage function τ . We call this statistical distance the leakage distance.

Thus local leakage cannot distinguish a uniform codeword from a vector of independent uniform field elements.

Definition 6 (Leakage resilience of Shamir sharing). The (n, k, α) -Shamir scheme is ε -resilient to m -bit local leakage if $\text{SD}(\tau(\text{share}_\alpha(s)), \tau(\text{share}_\alpha(s'))) \leq \varepsilon$ for every m -bit local leakage function τ and all secrets $s, s' \in \mathbb{F}_p$.

When no error bound is stated, resilience means that the leakage distance is negligible in n , namely smaller than every inverse polynomial for sufficiently large n .

Remark 1 (Code monotonicity). Translations can be absorbed into the leakage maps, and statistical distance is convex in its first argument [BDIR18, BDIR21]. Hence if $C \subseteq \mathbb{F}_p^n$ is ε -resilient to m -bit local leakage, the same bound against $U_{\mathbb{F}_p^n}$ holds for every mixture of uniform distributions on translates of C ; in particular, every linear code containing C is ε -resilient.

Remark 2 (Threshold monotonicity). Increasing the reconstruction threshold preserves leakage resilience [BDIR18, BDIR21]: if the (n, k, α) -Shamir scheme is ε -resilient to m -bit local leakage, so is the (n, k', α) -scheme for every $k \leq k' \leq n$.

Lemma 1 (Equivalence of code and Shamir leakage resilience). *Let $\alpha \in (\mathbb{F}_p^*)^n$ have distinct coordinates, let $\mathbf{v} \in (\mathbb{F}_p^*)^n$, and let $2 \leq k \leq n$. Resilience to m -bit local leakage of $\text{GRS}_{\alpha, \mathbf{v}}(n, k-1)$ and of the (n, k, α) -Shamir scheme are equivalent up to a linear factor in the error. More precisely, code error ε gives Shamir error at most 2ε , and Shamir error ε gives code error at most $(n-k+1)\varepsilon$.*

Proof. Code to Shamir is the reduction of [BDIR18, BDIR21]. Coordinate scalings by nonzero elements can be absorbed into the leakage maps, so we may take $C_0 = \text{GRS}_{\alpha, \alpha}(n, k-1)$. If C_0 is ε -resilient, applying its guarantee to the maps $x \mapsto \tau_i(x + s)$ gives $\text{SD}(\tau(\text{share}_\alpha(s)), \tau(U_{\mathbb{F}_p^n})) \leq \varepsilon$ for every secret s , and the triangle inequality gives Shamir error at most 2ε . For the zero-secret code C_0 , this direction holds for any leakage class closed under coordinatewise translations. For arbitrary multipliers, closure under nonzero coordinate scalings is also needed.

Conversely, suppose the Shamir scheme is ε -resilient at threshold k , hence at every larger threshold by [Remark 2](#). For $k-1 \leq r < n$ and multipliers $\mathbf{v}$, put $C = \text{GRS}_{\alpha, \mathbf{v}}(n, r)$ and $C' = \text{GRS}_{\alpha, \mathbf{w}}(n, r+1)$ with $w_i = v_i/\alpha_i$. At threshold $r+1$, multiplying a sharing of zero coordinatewise by $\mathbf{w}$ gives $\mathbf{U}_C$, and doing the same to a sharing of a uniform secret gives $\mathbf{U}_{C'}$, since all $r+1$ coefficients are then independent and uniform. Hence, with $\sigma_i(x) = \tau_i(w_i x)$ and sharings at threshold $r+1$, convexity gives

$$\text{SD}(\boldsymbol{\tau}(\mathbf{U}_C), \boldsymbol{\tau}(\mathbf{U}_{C'})) \leq \frac{1}{p} \sum_{s \in \mathbb{F}_p} \text{SD}(\boldsymbol{\sigma}(\text{share}_{\alpha}(0)), \boldsymbol{\sigma}(\text{share}_{\alpha}(s))) \leq \varepsilon.$$

Starting with the given multipliers $\mathbf{v}$, these steps form the nested chain

$$\begin{aligned} \text{GRS}_{\alpha, \mathbf{v}}(n, k-1) &\subseteq \text{GRS}_{\alpha, \mathbf{v}/\alpha}(n, k) \subseteq \cdots \\ &\subseteq \text{GRS}_{\alpha, \mathbf{v}/\alpha^{n-k+1}}(n, n) = \mathbb{F}_p^n, \end{aligned}$$

where division and powers of the multipliers are coordinatewise. The triangle inequality over the $n-k+1$ steps gives code error at most $(n-k+1)\varepsilon$. $\square$

2.4 Fourier analysis and Gowers norms

For $f: \mathbb{F}_p \rightarrow \mathbb{C}$, write $\|f\|_q = (\mathbb{E}_x |f(x)|^q)^{1/q}$ for $1 \leq q < \infty$ and $\|f\|_{\infty} = \max_x |f(x)|$.

Definition 7 (Fourier transform). Let $e_p(t) = \exp(2\pi i t/p)$ and $\chi_a(x) = e_p(ax)$ for $a \in \mathbb{F}_p$; the index a is a frequency. The normalized Fourier transform is $\hat{f}(a) = \mathbb{E}_x [f(x) \overline{\chi_a(x)}]$. For vectors, $\chi_{\mathbf{y}}(\mathbf{x}) = e_p(\sum_i y_i x_i)$ and $\hat{f}(\mathbf{y}) = \mathbb{E}_{\mathbf{x} \in \mathbb{F}_p^n} [f(\mathbf{x}) \chi_{\mathbf{y}}(\mathbf{x})]$.

Orthogonality of the characters gives Fourier inversion and Parseval's identity:

$$f(x) = \sum_{a \in \mathbb{F}_p} \hat{f}(a) \chi_a(x), \quad \|f\|_2^2 = \sum_{a \in \mathbb{F}_p} |\hat{f}(a)|^2.$$

Averages over a linear code. For a linear code $C \subseteq \mathbb{F}_p^n$, a set $A \subseteq [n]$, and functions $\mathbf{f}_A = (f_i: \mathbb{F}_p \rightarrow \mathbb{C})_{i \in A}$, write

$$\Gamma_C(\mathbf{f}_A) = \mathbb{E}_{\mathbf{X} \sim U_C} \left[\prod_{i \in A} f_i(X_i) \right],$$

with $\Gamma_C(\mathbf{f}_{\emptyset}) = 1$. We use the Poisson summation formula for a linear code [[BDir21](#), Lemma 4.16].

Lemma 2 (Dual-code formula). *Let $C \subseteq \mathbb{F}_p^n$ be a linear code. For every $\mathbf{x} \in \mathbb{F}_p^n$,*

$$\frac{p^n}{|C|} \mathbf{1}[\mathbf{x} \in C] = \sum_{\mathbf{y} \in C^{\perp}} \chi_{\mathbf{y}}(\mathbf{x}).$$

The identity follows from Fourier inversion and $\mathbb{E}_{\mathbf{X} \sim U_C} [\chi_{\mathbf{y}}(\mathbf{X})] = \mathbf{1}[\mathbf{y} \in C^{\perp}]$.

Definition 8 (Gowers norms). For a positive integer t and $f: \mathbb{F}_p \rightarrow \mathbb{C}$,

$$\|f\|_{U^t}^{2^t} = \mathbb{E}_{x, h_1, \dots, h_t \in \mathbb{F}_p} \left[\prod_{\boldsymbol{\omega} \in \{0,1\}^t} \mathcal{C}^{|\boldsymbol{\omega}|} f(x + \boldsymbol{\omega} \cdot \mathbf{h}) \right],$$

where $\mathbf{h} = (h_1, \dots, h_t)$, $\mathcal{C}$ denotes complex conjugation, $|\boldsymbol{\omega}| = \omega_1 + \dots + \omega_t$, and the $t+1$ averaging variables are independent and uniform. The same definition applies to functions on any finite abelian group, in particular on $\mathbb{F}_p^J$ for a finite set J .

The conjugations make these averages real and nonnegative; the U^2 and U^3 norms average products of four and eight translated values. For $t \geq 2$, $\|\cdot\|_{U^t}$ is a norm, and $|\mathbb{E}f| = \|f\|_{U^1} \leq \|f\|_{U^2} \leq \dots \leq \|f\|_\infty$ [TV06]. Fourier orthogonality gives $\|f\|_{U^2}^4 = \sum_{a \in \mathbb{F}_p} |\hat{f}(a)|^4$, and with $\Delta_h f(x) = f(x+h)\overline{f(x)}$ the definition gives $\|f\|_{U^3}^8 = \mathbb{E}_h[\|\Delta_h f\|_{U^2}^4]$.

2.5 List decoding and list recovery

Definition 9 (List size). For a code $D \subseteq \mathbb{F}_p^n$, an integer radius $0 \leq R \leq n$, and an input-list size $\ell \geq 1$,

$$\text{List}_D(R, \ell) = \max_{\substack{S_1, \dots, S_n \subseteq \mathbb{F}_p \\ |S_i| \leq \ell}} |\{\mathbf{y} \in D : |\{i : y_i \in S_i\}| \geq n - R\}|.$$

Write $\text{List}_D(R) = \text{List}_D(R, 1)$.

Thus $\text{List}_D(R, \ell) \leq L$ means that every choice of input lists admits at most L codewords agreeing with them in at least $n - R$ coordinates (list recovery). For $\ell = 1$, $\text{List}_D(R) = \max_{\mathbf{y} \in \mathbb{F}_p^n} |\{\mathbf{v} \in D : d_H(\mathbf{v}, \mathbf{y}) \leq R\}|$ (list decoding). We use only these counting bounds, not decoding algorithms.

We use a field-size-independent list-recovery bound supplied by Jeronimo [Jer26, Theorem 1.1], building on the decoding method of Brakensiek et al. [BCP⁺26], and also by Dao, Kominers, and Thaler [DKT26, Theorem G.2]. For growing leakage alphabets, we need the dependence on the input-list size explicit. The following quantitative form is derived from Jeronimo’s proof in Section A and from DKT’s finite estimates in Section B.

Theorem 4 (Reed–Solomon list recovery, derived from [Jer26, DKT26]). *Fix $0 < \zeta < 1$. There is a constant $c_\zeta \geq 1$ such that, for every integer $\ell \geq 1$, every $n \geq c_\zeta \ell^{9/\zeta}$, every prime $p > n$, and every integer $1 \leq h \leq (1 - \zeta)n$,*

$$\text{List}_{\text{GRS}_{\alpha, v(n, h)}}(\lfloor n - h - \zeta n \rfloor, \ell) \leq n^{c_\zeta \ell^{3/\zeta}}.$$

The exponent is independent of p , so there is no upper bound on the field size; the gap ζ is fixed, while ℓ may grow subject to the length condition. The statement for ordinary Reed–Solomon codes gives the GRS version by replacing each input list S_i with $v_i^{-1}S_i$, which preserves list sizes and agreement counts.

For $C = \text{GRS}_{\alpha, v(n, k-1)}$ with $2 \leq k \leq n$, the dual has dimension $n - k + 1$, which is at most $(1 - \zeta)n$ when $k - 1 \geq \zeta n$, and the radius in the theorem is then exactly $\lfloor k - 1 - \zeta n \rfloor$. Hence, whenever $k - 1 \geq \zeta n$ and $n \geq c_\zeta \ell^{9/\zeta}$,

$$\text{List}_{C^\perp}(\lfloor k - 1 - \zeta n \rfloor, \ell) \leq n^{c_\zeta \ell^{3/\zeta}}.$$

Taking $\ell = 1$ gives the corresponding list-decoding bound. All later estimates are uniform in the leakage maps, so no union bound over maps is needed.

For comparison, [BCP⁺26, Corollary 5.1] gives list size $p^{O(1)}$ at fixed rate and gap when $p \geq Cn$, which also suffices for our arguments when $\log p = o(n)$; Theorem 4 removes this upper restriction and allows every prime $p > n$.

3 An orthogonal decomposition of the leakage distance

This section writes the leakage distance as a norm of one function of the outputs and decomposes that function into orthogonal components indexed by sets of coordinates; Section 3.4 specializes to one-bit leakage.

3.1 Efron–Stein decomposition

Throughout this subsection, $\Omega = \prod_{i=1}^n \Omega_i$ is a product of finite sets and $\mu = \prod_{i=1}^n \mu_i$ is a product probability measure on Ω in which every μ_i has full support. For $f, g: \Omega \rightarrow \mathbb{C}$ write $\langle f, g \rangle_\mu = \mathbb{E}_\mu[f\bar{g}]$ and $\|f\|_{q,\mu} = (\mathbb{E}_\mu|f|^q)^{1/q}$ for $1 \leq q < \infty$; we omit the measure when it is clear from context.

Definition 10 (Efron–Stein decomposition [O’D14, Chapter 8]). Every $f: \Omega \rightarrow \mathbb{C}$ has a unique expansion

$$f = \sum_{A \subseteq [n]} f^{=A}$$

in which $f^{=A}$ depends only on the coordinates in A and $\mathbb{E}_{x_i \sim \mu_i}[f^{=A}(\mathbf{x})] = 0$ for every $i \in A$ and every fixing of the other coordinates. The components are pairwise orthogonal in $L^2(\Omega, \mu)$; in particular

$$f^{=\emptyset} = \mathbb{E}_\mu[f] \quad \text{and} \quad \|f\|_{2,\mu}^2 = \sum_{A \subseteq [n]} \|f^{=A}\|_{2,\mu}^2.$$

Concretely, choose for each i an orthonormal basis of $L^2(\Omega_i, \mu_i)$ that contains the constant function 1. Their products, one factor per coordinate, form an orthonormal basis of $L^2(\Omega, \mu)$, and $f^{=A}$ is the part of the expansion of f whose factors are nonconstant at exactly the coordinates in A [O’D14, Chapter 8]. Equivalently, let E_i^μ average coordinate i according to μ_i , leaving the others fixed. Then

$$f^{=A} = \left(\prod_{i \in A} (\text{Id} - E_i^\mu) \right) \left(\prod_{i \notin A} E_i^\mu \right) f.$$

On $\mathbb{F}_p^n$ with the uniform measure and the character basis this reads as follows [O’D14, Proposition 8.36]; see also [KM22, Proposition 7].

Lemma 3 (Fourier form of the components). *For every $f: \mathbb{F}_p^n \rightarrow \mathbb{C}$ and $A \subseteq [n]$, under the uniform measure on $\mathbb{F}_p^n$,*

$$f^{=A} = \sum_{\mathbf{y} \in \mathbb{F}_p^n: \text{supp}(\mathbf{y})=A} \hat{f}(\mathbf{y}) \chi_{\mathbf{y}}.$$

Leakage enters through conditional expectation.

Definition 11 (Markov operator [KM22, Section 4.4]). Let (X, Y) be a pair of random variables on finite sets $\Omega \times \Omega'$ with marginal distributions μ and ν . Its *Markov operator* $\mathsf{T}: L^2(\Omega, \mu) \rightarrow L^2(\Omega', \nu)$ is

$$(\mathsf{T}f)(y) = \mathbb{E}[f(X) \mid Y = y], \quad y \in \text{supp}(\nu).$$

The operator T is linear, $\mathsf{T}1 = 1$, and $\mathbb{E}_\nu[\mathsf{T}f] = \mathbb{E}_\mu[f]$. If $(X_i, Y_i)_{i \in [n]}$ are independent pairs with Markov operators T_i , then the Markov operator of $\mathbf{X} = (X_i)_i$ and $\mathbf{Y} = (Y_i)_i$ is the tensor product $\mathsf{T} = \bigotimes_i \mathsf{T}_i$: for $f(\mathbf{x}) = \prod_i f_i(x_i)$ one has $(\mathsf{T}f)(\mathbf{y}) = \prod_i (\mathsf{T}_i f_i)(y_i)$. We use two standard properties [KM22, Proposition 5].

Lemma 4 (Markov operators and components). *Let T be the Markov operator of a pair (X, Y) with marginal distributions μ, ν .*

1. $\|\mathsf{T}f\|_{2,\nu} \leq \|f\|_{2,\mu}$ for every $f \in L^2(\Omega, \mu)$.
2. If (X, Y) is a product of independent pairs as above, then $(\mathsf{T}f)^{=A} = \mathsf{T}(f^{=A})$ for every f and every $A \subseteq [n]$, where the components of f are taken under μ and those of $\mathsf{T}f$ under ν .

Proof. Conditional Jensen gives

$$\|\mathsf{T}f\|_{2,\nu}^2 = \mathbb{E}_Y |\mathbb{E}[f(X) \mid Y]|^2 \leq \mathbb{E}_Y [\mathbb{E}[|f(X)|^2 \mid Y]] = \|f\|_{2,\mu}^2.$$

For independent coordinate pairs, averaging coordinate i before or after applying its Markov operator gives the same constant: $\mathsf{T}E_i^\mu = E_i^\nu \mathsf{T}$. Applying this identity to the product formula for the components above gives

$$\mathsf{T}(f^{=A}) = \left(\prod_{i \in A} (\text{Id} - E_i^\nu) \right) \left(\prod_{i \notin A} E_i^\nu \right) \mathsf{T}f = (\mathsf{T}f)^{=A}. \quad \square$$

3.2 The leakage distance as a norm on the output space

Fix a linear code $C \subseteq \mathbb{F}_p^n$ and local maps $\tau_i: \mathbb{F}_p \rightarrow \mathcal{B}_i$ into finite sets; m -bit leakage is the case $\mathcal{B}_i = \{0,1\}^m$. Replacing each $\mathcal{B}_i$ by the image $\tau_i(\mathbb{F}_p)$, we may assume that every output symbol occurs, so that

$$\nu_i(b) = \Pr[\tau_i(U_{\mathbb{F}_p}) = b] > 0 \quad \text{for all } b \in \mathcal{B}_i, \quad \nu(\mathbf{b}) = \prod_{i=1}^n \nu_i(b_i).$$

Thus ν is the reference leakage distribution, namely the distribution of $\boldsymbol{\tau}(U_{\mathbb{F}_p^n})$. Let T_i be the Markov operator of Definition 11 for the pair $(U_{\mathbb{F}_p}, \tau_i(U_{\mathbb{F}_p}))$, and T the one for $(U_{\mathbb{F}_p^n}, \boldsymbol{\tau}(U_{\mathbb{F}_p^n}))$; the pairs are independent, so $\mathsf{T} = \bigotimes_i \mathsf{T}_i$. Norms of functions on the inputs are taken under the uniform measure, and norms of functions on the outputs under ν , or under ν_i for a function of one coordinate.

The object we decompose is the *normalized indicator* $f_C: \mathbb{F}_p^n \rightarrow \mathbb{R}$,

$$f_C(\mathbf{x}) = \frac{\Pr[\mathbf{U}_C = \mathbf{x}]}{\Pr[\mathbf{U}_{\mathbb{F}_p^n} = \mathbf{x}]} = \frac{p^n}{|C|} \mathbb{1}[\mathbf{x} \in C],$$

the likelihood ratio of the two input distributions. Its conditional mean given the leakage is the likelihood ratio of the two leakage distributions.

Lemma 5 (Leakage probabilities and statistical distance). *For every $\mathbf{b} \in \prod_i \mathcal{B}_i$,*

$$\Pr[\boldsymbol{\tau}(\mathbf{U}_C) = \mathbf{b}] = \nu(\mathbf{b}) (\mathsf{T}f_C)(\mathbf{b}), \quad \Pr[\boldsymbol{\tau}(\mathbf{U}_{\mathbb{F}_p^n}) = \mathbf{b}] = \nu(\mathbf{b}).$$

Consequently,

$$\text{SD}(\boldsymbol{\tau}(\mathbf{U}_C), \boldsymbol{\tau}(\mathbf{U}_{\mathbb{F}_p^n})) = \frac{1}{2} \|\mathsf{T}f_C - 1\|_{1,\nu}.$$

Proof. Write $\mathbf{U} = \mathbf{U}_{\mathbb{F}_p^n}$. Since $\Pr[\mathbf{U}_C = \mathbf{x}] = p^{-n} f_C(\mathbf{x})$,

$$\Pr[\boldsymbol{\tau}(\mathbf{U}_C) = \mathbf{b}] = \sum_{\mathbf{x}: \boldsymbol{\tau}(\mathbf{x}) = \mathbf{b}} p^{-n} f_C(\mathbf{x}) = \Pr[\boldsymbol{\tau}(\mathbf{U}) = \mathbf{b}] \mathbb{E}[f_C(\mathbf{U}) \mid \boldsymbol{\tau}(\mathbf{U}) = \mathbf{b}].$$

The second factor is $(\mathsf{T}f_C)(\mathbf{b})$ by definition, and the first is $\nu(\mathbf{b})$ because the coordinates of $\boldsymbol{\tau}(\mathbf{U})$ are independent with distributions ν_i . Substituting both identities into the definition of statistical distance gives $\frac{1}{2} \sum_{\mathbf{b}} \nu(\mathbf{b}) |(\mathsf{T}f_C)(\mathbf{b}) - 1|$. $\square$

3.3 The orthogonal components

For the rest of this section we assume that $C^\perp$ has minimum distance at least k . This is the only property of C used below; for $C = \text{GRS}_{\alpha, v}(n, k-1)$ it holds because $C^\perp$ is a GRS code of dimension $n - k + 1$.

Since T is a product Markov operator, Lemma 4 gives $(\mathsf{T}f_C)^{\perp A} = \mathsf{T}(f_C^{\perp A})$, so it remains to identify the input components. By Lemma 2, $\hat{f}_C(\mathbf{y}) = \mathbb{1}[\mathbf{y} \in C^\perp]$ for every $\mathbf{y} \in \mathbb{F}_p^n$, and Lemma 3 then gives

$$f_C^{\perp A} = \sum_{\mathbf{y} \in \mathbb{F}_p^n: \text{supp}(\mathbf{y})=A} \hat{f}_C(\mathbf{y}) \chi_{\mathbf{y}} = \sum_{\mathbf{y} \in C^\perp: \text{supp}(\mathbf{y})=A} \chi_{\mathbf{y}}. \quad (1)$$

In particular $f_C^{\perp \emptyset} = 1$, and $f_C^{\perp A} = 0$ whenever $1 \leq |A| < k$, because every nonzero dual word has weight at least k . Since $\mathsf{T}1 = 1$,

$$\mathsf{T}f_C - 1 = \sum_{A \subseteq [n]: |A| \geq k} \mathsf{T}(f_C^{\perp A}),$$

and the summands are pairwise orthogonal in $L^2(\nu)$, being the components of $\mathsf{T}f_C$ under ν (Lemma 4 and Definition 10).

List decoding of $C^\perp$ controls squared L^2 norms of components, which add across supports by orthogonality (Sections 4 and 6); Gowers-norm estimates control L^1 norms one support at a time (Sections 5 and 6). The next proposition allows any cutoff between the two regimes, and Corollary 1 records the extreme cutoffs.

Proposition 1 (Splitting the leakage distance). *For every integer r_0 with $k-1 \leq r_0 \leq n$,*

$$\text{SD}(\tau(\mathbf{U}_C), \tau(\mathbf{U}_{\mathbb{F}_p^n})) \leq \frac{1}{2} \left(\sum_{k \leq |A| \leq r_0} \|\mathsf{T}(f_C^{\perp A})\|_2^2 \right)^{1/2} + \frac{1}{2} \sum_{|A| > r_0} \|\mathsf{T}(f_C^{\perp A})\|_1.$$

Proof. Split the decomposition of $\mathsf{T}f_C - 1$ at $|A| = r_0$ and apply the triangle inequality in $L^1(\nu)$ to the two parts. For the supports of size at most r_0 , Cauchy–Schwarz gives $\|\cdot\|_1 \leq \|\cdot\|_2$, and by orthogonality the squared L^2 norm of the sum is the sum of the squared norms. For the larger supports, the triangle inequality bounds the L^1 norm of the sum by the sum of the L^1 norms. Lemma 5 supplies the factor $\frac{1}{2}$. $\square$

The extreme cutoffs $r_0 = n$ and $r_0 = k-1$ give the following.

Corollary 1 (The two extreme cutoffs). *The following bounds hold.*

$$\text{SD}(\tau(\mathbf{U}_C), \tau(\mathbf{U}_{\mathbb{F}_p^n})) \leq \frac{1}{2} \left(\sum_{|A| \geq k} \|\mathsf{T}(f_C^{\perp A})\|_2^2 \right)^{1/2} \quad \text{and} \quad \text{SD}(\tau(\mathbf{U}_C), \tau(\mathbf{U}_{\mathbb{F}_p^n})) \leq \frac{1}{2} \sum_{|A| \geq k} \|\mathsf{T}(f_C^{\perp A})\|_1.$$

The large-support bound has an exact form for arbitrary output alphabets in terms of centered output indicators.

Lemma 6 (Output-indicator form of the components). *For $i \in [n]$ and $b \in \mathcal{B}_i$, let*

$$f_{i,b}(x) = \mathbb{1}[\tau_i(x) = b] - \nu_i(b).$$

These functions have mean zero and $\|f_{i,b}\|_\infty \leq 1$. For every $A \subseteq [n]$,

$$\|\mathsf{T}(f_C^{\perp A})\|_{1,\nu} = \sum_{\mathbf{b}_A \in \prod_{i \in A} \mathcal{B}_i} \left| \mathbb{E}_{\mathbf{X} \sim \mathbf{U}_C} \left[\prod_{i \in A} f_{i,b_i}(X_i) \right] \right|.$$

Proof. Expanding the product formula in [Section 3.1](#) gives

$$(\mathsf{T}f_C)^{=A} = \sum_{S \subseteq A} (-1)^{|A \setminus S|} \left(\prod_{i \notin S} E_i^\nu \right) \mathsf{T}f_C.$$

Each term averages all output coordinates outside S . By [Lemma 5](#), each marginal of $\mathsf{T}f_C$ is the corresponding marginal leakage probability divided by its reference probability. Hence

$$\begin{aligned} (\mathsf{T}f_C^{=A})(\mathbf{b}_A) &= \sum_{S \subseteq A} (-1)^{|A \setminus S|} \frac{\Pr[\boldsymbol{\tau}_S(\mathbf{U}_C) = \mathbf{b}_S]}{\prod_{i \in S} \nu_i(b_i)} \\ &= \mathbb{E}_{\mathbf{X} \sim U_C} \left[\prod_{i \in A} \left(\frac{\mathbb{1}[\tau_i(X_i) = b_i]}{\nu_i(b_i)} - 1 \right) \right] = \frac{\mathbb{E}_{\mathbf{X} \sim U_C} [\prod_{i \in A} f_{i,b_i}(X_i)]}{\prod_{i \in A} \nu_i(b_i)}. \end{aligned}$$

Taking the $L^1(\nu)$ norm cancels the denominator and proves the identity. No lower bound on the positive probabilities $\nu_i(b)$ is needed; unused output symbols have $f_{i,b} = 0$ and may also be included in the sum. $\square$

3.4 One-bit leakage

Now let $\tau_i: \mathbb{F}_p \rightarrow \{0, 1\}$. Each $L^2(\nu_i)$ is then spanned by 1 and one centered function, so every output component is a scalar multiple of a single product function; the scalar is an average over the code of centered leakage functions.

Put $\theta_i = \mathbb{E}_x[\tau_i(x)]$. If τ_i is nonconstant, so that $0 < \theta_i < 1$, define

$$g_i(x) = \frac{\tau_i(x) - \theta_i}{\sqrt{\theta_i(1 - \theta_i)}}, \quad f_i(x) = 2(\tau_i(x) - \theta_i);$$

if τ_i is constant, put $g_i = f_i = 0$. Both functions have mean zero, $\|g_i\|_2 \leq 1$ with equality for nonconstant τ_i , and $\|f_i\|_\infty \leq 2$. Write $\mathbf{g}_A = (g_i)_{i \in A}$ and $\mathbf{f}_A = (f_i)_{i \in A}$, and recall that $\Gamma_C(\mathbf{h}_A) = \mathbb{E}_{\mathbf{X} \sim U_C} [\prod_{i \in A} h_i(X_i)]$ for functions $h_i: \mathbb{F}_p \rightarrow \mathbb{C}$.

Lemma 7 (Norms of the binary components). *For every $A \subseteq [n]$,*

$$\|\mathsf{T}(f_C^{=A})\|_2^2 = |\Gamma_C(\mathbf{g}_A)|^2 \quad \text{and} \quad \|\mathsf{T}(f_C^{=A})\|_1 = |\Gamma_C(\mathbf{f}_A)|.$$

Both sides vanish when $1 \leq |A| < k$, and when A contains a coordinate whose map is constant. Moreover, $\|\mathsf{T}_i \chi_a\|_2^2 = |\hat{g}_i(a)|^2$ for every i and every $a \neq 0$.

Proof. If τ_i is constant, then $L^2(\nu_i)$ consists of the constant functions, so every output component with $i \in A$ vanishes, as do $\Gamma_C(\mathbf{g}_A)$ and $\Gamma_C(\mathbf{f}_A)$ by the convention $g_i = f_i = 0$; also $\mathsf{T}_i \chi_a = \mathbb{E}_x[\chi_a(x)] = 0 = \hat{g}_i(a)$ for $a \neq 0$. We may therefore assume that every τ_i is nonconstant.

For an output bit put $\phi_i(b) = (b - \theta_i)/\sqrt{\theta_i(1 - \theta_i)}$, so that $g_i = \phi_i \circ \tau_i$, and let $\phi_A(\mathbf{b}) = \prod_{i \in A} \phi_i(b_i)$. The functions $1, \phi_i$ form an orthonormal basis of $L^2(\nu_i)$, so the product basis of [Section 3.1](#) contains exactly one function nonconstant precisely on A , namely ϕ_A , and the component of $\mathsf{T}f_C$ on A is $\langle \mathsf{T}f_C, \phi_A \rangle_\nu \phi_A$. By [Lemma 5](#), $\nu(\mathbf{b})(\mathsf{T}f_C)(\mathbf{b}) = \Pr[\boldsymbol{\tau}(\mathbf{X}) = \mathbf{b}]$ for $\mathbf{X} \sim U_C$, so

$$\langle \mathsf{T}f_C, \phi_A \rangle_\nu = \mathbb{E}_{\mathbf{X} \sim U_C} [\phi_A(\boldsymbol{\tau}(\mathbf{X}))] = \Gamma_C(\mathbf{g}_A).$$

Together with $(\mathsf{T}f_C)^{=A} = \mathsf{T}(f_C^{=A})$ this gives $\mathsf{T}(f_C^{=A}) = \Gamma_C(\mathbf{g}_A) \phi_A$, and $\|\phi_A\|_{2,\nu} = 1$ proves the first identity. For the second, independence under ν and $\mathbb{E}_{\nu_i} |\phi_i| = 2\sqrt{\theta_i(1 - \theta_i)}$ give

$$\|\mathsf{T}(f_C^{=A})\|_{1,\nu} = |\Gamma_C(\mathbf{g}_A)| \prod_{i \in A} 2\sqrt{\theta_i(1 - \theta_i)} = |\Gamma_C(\mathbf{f}_A)|,$$

since $f_i = 2\sqrt{\theta_i(1-\theta_i)}g_i$. Vanishing for $1 \leq |A| < k$ is (1) together with the dual-distance assumption.

Finally, for $a \neq 0$ the function $\mathsf{T}_i\chi_a$ has mean zero and is therefore a multiple of ϕ_i , with coefficient $\langle \mathsf{T}_i\chi_a, \phi_i \rangle_{\nu_i} = \mathbb{E}_x[\chi_a(x)g_i(x)] = \widehat{g}_i(-a)$. Since g_i is real, $|\widehat{g}_i(-a)| = |\widehat{g}_i(a)|$. $\square$

Substituting the lemma into [Proposition 1](#) gives the form of the decomposition used for one-bit leakage.

Proposition 2 (Splitting small and large supports). *For every integer r_0 with $k-1 \leq r_0 \leq n$,*

$$\text{SD}(\tau(U_C), \tau(U_{\mathbb{F}_p^n})) \leq \frac{1}{2} \left(\sum_{k \leq |A| \leq r_0} |\Gamma_C(\mathbf{g}_A)|^2 \right)^{1/2} + \frac{1}{2} \sum_{|A| > r_0} |\Gamma_C(\mathbf{f}_A)|. \quad (2)$$

By [Lemma 7](#), supports containing a constant-map coordinate contribute nothing to (2); this is how constant maps are handled from now on.

4 Dual-code list recovery and resilience above half

This section proves that list recovery of $C^\perp$ with input lists of size $Q-1$ implies resilience to leakage with Q output symbols per coordinate; for one-bit leakage the hypothesis is ordinary list decoding. [Lemma 8](#) bounds each component of [Section 3](#) by a weighted count of dual codewords, [Lemma 11](#) replaces the weights by list indicators, and [Theorem 6](#) follows at the end.

Theorem 5 (List recovery implies leakage resilience). *For every integer $Q \geq 2$ there is a constant $0 < \eta_Q \leq 1 - 1/(16Q^2)$, with $\eta_2 = 1/2$, such that the following holds. Let $p \geq 16Q$ be prime, let $C \subseteq \mathbb{F}_p^n$ be a linear code, and let R be an integer with $n/2 < R < n$ such that every nonzero word of $C^\perp$ has weight at least $R+1$. Then for every tuple of local maps $\tau_i: \mathbb{F}_p \rightarrow \mathcal{B}_i$ with $|\mathcal{B}_i| \leq Q$,*

$$\text{SD}(\tau(U_C), \tau(U_{\mathbb{F}_p^n})) \leq \frac{1}{2} \eta_Q^{R-n/2} \sqrt{\text{List}_{C^\perp}(R, Q-1)}.$$

For $Q = 2$ the conclusion holds for every odd prime p .

The constant η_Q is given explicitly in [Lemma 9](#). The theorem uses only the dual distance of C ; no MDS property is needed.

Throughout this section, $C \subseteq \mathbb{F}_p^n$ is a linear code whose dual has minimum distance at least k , and $f_C, \mathsf{T}, \mathsf{T}_i, \nu, \nu_i$ are as in [Section 3](#) for local maps $\tau_i: \mathbb{F}_p \rightarrow \mathcal{B}_i$ in which every output symbol occurs. We write $q_i = |\mathcal{B}_i|$ and assume $q_i \leq Q$ for a fixed integer $Q \geq 2$.

4.1 Bounding the leakage components

We apply the leakage on only $k-1$ coordinates of a support. The dual distance ensures that the remaining coordinates distinguish the contributing dual words, so their characters stay orthogonal; applying the leakage on those coordinates afterwards can only decrease the L^2 norm.

Lemma 8 (Bounding a leakage component). *Let $A \subseteq [n]$ have size at least k , and let $J \subseteq A$ have size $|A| - k + 1$. Then*

$$\|\mathsf{T}(f_C^{\overline{A}})\|_2^2 \leq \sum_{\mathbf{y} \in C^\perp: \text{supp}(\mathbf{y})=A} \prod_{i \in A \setminus J} \|\mathsf{T}_i\chi_{y_i}\|_2^2.$$

Proof. Put $I = A \setminus J$, so $|I| = k - 1$, and write $\nu_I = \prod_{i \in I} \nu_i$. Since $f_C^{\bar{A}}$ depends only on the coordinates in A , we may regard T as $\mathsf{T}_I \otimes \mathsf{T}_J$ with $\mathsf{T}_I = \bigotimes_{i \in I} \mathsf{T}_i$ and $\mathsf{T}_J = \bigotimes_{i \in J} \mathsf{T}_i$.

First, fix $\mathbf{b}_I$ and apply Lemma 4(1) to $\mathbf{x}_J \mapsto (\mathsf{T}_I f_C^{\bar{A}})(\mathbf{x}_J, \mathbf{b}_I)$; averaging over $\mathbf{b}_I \sim \nu_I$ gives

$$\|\mathsf{T}(f_C^{\bar{A}})\|_2^2 \leq \|\mathsf{T}_I(f_C^{\bar{A}})\|_2^2,$$

where the norm on the right is under ν_I on the outputs of I and the uniform measure on $\mathbf{x}_J \in \mathbb{F}_p^J$.

Second, expanding $f_C^{\bar{A}}$ by (1) and applying T_I factor by factor,

$$(\mathsf{T}_I f_C^{\bar{A}})(\mathbf{x}_J, \mathbf{b}_I) = \sum_{\mathbf{y} \in C^\perp: \text{supp}(\mathbf{y})=A} \chi_{\mathbf{y}_J}(\mathbf{x}_J) \prod_{i \in I} (\mathsf{T}_i \chi_{y_i})(b_i).$$

Two dual words in the sum that agree on J differ on at most $|I| = k - 1$ coordinates, hence coincide by the dual-distance assumption. The characters $\chi_{\mathbf{y}_J}$ are therefore distinct, and Parseval in $\mathbf{x}_J$ gives

$$\|\mathsf{T}_I(f_C^{\bar{A}})\|_2^2 = \mathbb{E}_{\mathbf{b}_I \sim \nu_I} \sum_{\mathbf{y} \in C^\perp: \text{supp}(\mathbf{y})=A} \prod_{i \in I} |(\mathsf{T}_i \chi_{y_i})(b_i)|^2 = \sum_{\mathbf{y} \in C^\perp: \text{supp}(\mathbf{y})=A} \prod_{i \in I} \|\mathsf{T}_i \chi_{y_i}\|_2^2,$$

by independence of the outputs under ν_I . $\square$

The bound leaves $k - 1$ factors of the form $\|\mathsf{T}_i \chi_a\|_2^2$. We need two facts about them: their sum over nonzero frequencies is at most $Q - 1$, which will let us replace the weights by lists of size $Q - 1$; and each is at most $\eta_Q < 1$, which supplies the decay.

Lemma 9 (Fourier weight after leakage). *For every i and every $a \in \mathbb{F}_p$, with norms of $\mathsf{T}_i \chi_a$ taken under ν_i ,*

$$\mathsf{T}_i \chi_0 = 1, \quad \|\mathsf{T}_i \chi_a\|_{2, \nu_i} = \|\mathsf{T}_i \chi_{-a}\|_{2, \nu_i} \leq 1, \quad \sum_{a \neq 0} \|\mathsf{T}_i \chi_a\|_{2, \nu_i}^2 = q_i - 1.$$

If $p \geq 16Q$, or if $Q = 2$ and p is odd, then for every $a \neq 0$,

$$\|\mathsf{T}_i \chi_a\|_2^2 \leq \eta_Q := \min\left\{\frac{Q-1}{2}, \cos^2 \frac{\pi}{8Q}\right\} \leq 1 - \frac{1}{16Q^2}.$$

In particular $\eta_2 = 1/2$.

Proof. Let $S_{i,b} = \{x \in \mathbb{F}_p : \tau_i(x) = b\}$, so $\nu_i(b) = |S_{i,b}|/p$ and $(\mathsf{T}_i \chi_a)(b) = \widehat{\mathbb{1}_{S_{i,b}}}(-a)/\nu_i(b)$. Hence

$$\|\mathsf{T}_i \chi_a\|_2^2 = \sum_{b \in \mathcal{B}_i} \frac{|\widehat{\mathbb{1}_{S_{i,b}}}(a)|^2}{\nu_i(b)}, \quad \sum_{a \in \mathbb{F}_p} \|\mathsf{T}_i \chi_a\|_2^2 = \sum_{b \in \mathcal{B}_i} \frac{\|\mathbb{1}_{S_{i,b}}\|_2^2}{\nu_i(b)} = q_i,$$

by Parseval. Removing the zero frequency, where $\mathsf{T}_i \chi_0 = 1$, gives the sum over $a \neq 0$. The symmetry follows from $\chi_{-a} = \overline{\chi_a}$, and $\|\mathsf{T}_i \chi_a\|_2 \leq 1$ from $|\chi_a| = 1$. For odd p , the frequencies a and $-a$ are distinct when $a \neq 0$, so $2\|\mathsf{T}_i \chi_a\|_2^2 \leq \sum_{a' \neq 0} \|\mathsf{T}_i \chi_{a'}\|_2^2 \leq Q - 1$. This is the first term of the minimum, and for $Q = 2$ it is the whole bound.

Now suppose $p \geq 16Q$ and fix $a \neq 0$. Write $z_b = (\mathsf{T}_i \chi_a)(b) = |z_b|e^{i\phi_b}$, with ϕ_b arbitrary when $z_b = 0$. Since $|z_b| \leq 1$,

$$\|\mathsf{T}_i \chi_a\|_2^2 = \sum_b \nu_i(b) |z_b|^2 \leq \sum_b \nu_i(b) |z_b| = \frac{1}{p} \sum_{x \in \mathbb{F}_p} \text{Re}(e^{-i\phi_{\tau_i(x)}} \chi_a(x)).$$

The values $\chi_a(x)$ are the p equally spaced points of the unit circle. Around each of the at most Q angles ϕ_b take the arc of angular radius $\pi/(4Q)$; each arc contains at most $p/(4Q) + 1$ of the points, so their union contains at most $p/4 + Q \leq 3p/8$ since $p \geq 16Q$. Thus at least half the points lie outside every arc, where the real part above is at most $\cos(\pi/(4Q))$; elsewhere it is at most one. Hence

$$\|\mathsf{T}_i \chi_a\|_2^2 \leq \frac{1 + \cos(\pi/(4Q))}{2} = \cos^2 \frac{\pi}{8Q}.$$

Finally, $\sin u \geq 2u/\pi$ for $0 \leq u \leq \pi/2$ gives $\sin^2(\pi/(8Q)) \geq 1/(16Q^2)$. $\square$

From now on we assume $p \geq 16Q$, or $Q = 2$ and p odd. Note that $\eta_Q < 1$ bounds individual characters, not every function of mean zero: a function of $\tau_i(x)$ alone is fixed by T_i , which is why [Lemma 8](#) first reduces to a sum of products of character norms.

4.2 Applying list recovery

We keep j of the $k - 1$ factors in [Lemma 8](#) and bound the rest by η_Q . An extremal argument then replaces the retained weights by indicators of input lists, so the sum counts dual words with at least j agreements.

Lemma 10 (Replacing weights by list indicators). *Let Ω be a finite set and $2 \leq Q \leq |\Omega| + 1$ an integer. Let $P(w_1, \dots, w_n)$ be a nonnegative linear combination of terms of the form*

$$\prod_{i \in S} w_i(a_i), \quad S \subseteq [n], \quad a_i \in \Omega.$$

For all functions $w_i: \Omega \rightarrow [0, 1]$ with $\sum_{a \in \Omega} w_i(a) \leq Q - 1$, there are sets $V_i \subseteq \Omega$ of size $Q - 1$ such that

$$P(w_1, \dots, w_n) \leq P(\mathbf{1}_{V_1}, \dots, \mathbf{1}_{V_n}).$$

Proof. Fix all weights except w_i . Each term contains at most one factor from coordinate i , so P has the form $c_0 + \sum_{a \in \Omega} c_a w_i(a)$ with all $c_a \geq 0$. Subject to $0 \leq w_i(a) \leq 1$ and $\sum_a w_i(a) \leq Q - 1$, this is maximized by putting weight one on the $Q - 1$ largest coefficients and zero elsewhere; let V_i be the set of those $Q - 1$ indices. Replacing w_i by $\mathbf{1}_{V_i}$ does not decrease P . Repeating for each coordinate in turn gives the claim. $\square$

Lemma 11 (A list-recovery bound for the components). *For every integer $1 \leq j < k$ with $j \leq n$,*

$$\sum_{A \subseteq [n]: |A| \geq k} \|\mathsf{T}(f_C^{\bar{A}})\|_2^2 \leq \eta_Q^{k-1-j} \text{List}_{C^\perp}(n - j, Q - 1).$$

Proof. Let $\sum_A$ range over supports of size at least k . For each such A fix $I_A \subseteq A$ with $|I_A| = k - 1$ and $J_A \subseteq I_A$ with $|J_A| = j$. Apply [Lemma 8](#) with $J = A \setminus I_A$. Every word with support A is nonzero at each coordinate of A , so [Lemma 9](#) bounds each of the $k - 1 - j$ factors indexed by $I_A \setminus J_A$ by η_Q :

$$\sum_A \|\mathsf{T}(f_C^{\bar{A}})\|_2^2 \leq \sum_A \sum_{\mathbf{y} \in C^\perp: \text{supp}(\mathbf{y})=A} \prod_{i \in I_A} \|\mathsf{T}_i \chi_{y_i}\|_2^2 \leq \eta_Q^{k-1-j} \sum_A \sum_{\mathbf{y} \in C^\perp: \text{supp}(\mathbf{y})=A} \prod_{i \in J_A} \|\mathsf{T}_i \chi_{y_i}\|_2^2.$$

Regard the last double sum as a function P of the weights $w_i(a) = \|\mathsf{T}_i \chi_a\|_2^2$, $a \in \mathbb{F}_p^*$: it is a sum of monomials $\prod_{i \in J_A} w_i(y_i)$, one for each dual word, each with coefficient one. [Lemma 10](#) applies to P with $\Omega = \mathbb{F}_p^*$, since $Q - 1 \leq p - 1$ and [Lemma 9](#) gives the constraints on the weights. This

yields lists $V_i \subseteq \mathbb{F}_p^*$ of size $Q - 1$ with $P(\mathbf{w}) \leq P(\mathbb{1}_{V_1}, \dots, \mathbb{1}_{V_n})$. With indicator weights, a monomial equals one exactly when its dual word agrees with the lists on all j coordinates of J_A , and each dual word occurs once because its support determines A . With input lists $S_i = V_i$ for every i , each counted word therefore has at least j agreements, so

$$P(\mathbb{1}_{V_1}, \dots, \mathbb{1}_{V_n}) = \sum_A \sum_{\mathbf{y} \in C^\perp : \text{supp}(\mathbf{y})=A} \prod_{i \in J_A} \mathbb{1}[y_i \in V_i] \leq \text{List}_{C^\perp}(n - j, Q - 1),$$

which proves the lemma. $\square$

Proof of Theorem 5. Set $k = R + 1$ and $j = n - R$. Then $1 \leq j < k$, $k - 1 - j = 2R - n$, and $n - j = R$. Corollary 1 and Lemma 11 give

$$\text{SD}(\tau(\mathbf{U}_C), \tau(\mathbf{U}_{\mathbb{F}_p^n})) \leq \frac{1}{2} \left(\sum_{|A| \geq k} \|\mathbf{T}(f_C^A)\|_2^2 \right)^{1/2} \leq \frac{1}{2} \eta_Q^{R-n/2} \sqrt{\text{List}_{C^\perp}(R, Q - 1)}. \quad \square$$

Corollary 2 (List decoding implies one-bit leakage resilience). *Let p be an odd prime, $C \subseteq \mathbb{F}_p^n$ a linear code, and R an integer with $n/2 < R < n$ such that every nonzero word of $C^\perp$ has weight at least $R + 1$. Then, for every tuple of one-bit maps,*

$$\text{SD}(\tau(\mathbf{U}_C), \tau(\mathbf{U}_{\mathbb{F}_p^n})) \leq \frac{1}{2} 2^{n/2-R} \sqrt{\text{List}_{C^\perp}(R)}.$$

Proof. Take $Q = 2$ in Theorem 5; then $\eta_2 = 1/2$ and $\text{List}_{C^\perp}(R, 1) = \text{List}_{C^\perp}(R)$. $\square$

We now derive the above-half result for GRS codes from the transfer and Theorem 4.

Theorem 6 (Logarithmic leakage above half). *Fix $0 < \delta < 1/2$. There are constants $c_\delta > 0$ and $n_0(\delta)$ such that, for $n \geq n_0(\delta)$ and every prime $p > n$, every GRS code over $\mathbb{F}_p$ of length n and rate at least $1/2 + \delta$ is $\exp(-c_\delta n^{1-\delta/12})$ -resilient to $\lfloor (\delta/24) \log_2 n \rfloor$ -bit local leakage.*

Proof of Theorem 6. Fix an integer $1 \leq m \leq (\delta/24) \log_2 n$. Write $C = \text{GRS}_{\alpha, v}(n, k - 1)$; the full-space code is immediate, so assume $k - 1 < n$. We prove the code estimate under the slightly weaker condition $k \geq (1/2 + \delta)n$, which covers both codes of rate at least $1/2 + \delta$ and the zero-secret codes of the Shamir schemes in the theorem. Throughout, n is sufficiently large depending only on δ .

Put $Q = 2^m \leq n^{\delta/24}$ and $R = \lfloor k - 1 - (\delta/2)n \rfloor$. Since $k \geq (1/2 + \delta)n$, we have $R - n/2 \geq \delta n/2 - 2 \geq \delta n/4$; also $R < k$ and $p > n \geq 16Q$. The dual code has dimension $n - k + 1$ and minimum distance $k \geq R + 1$, so Theorem 5 applies. We use the specialization of Theorem 4 to dual GRS codes stated after it, with gap $\delta/2$ and input-list size $Q - 1$: its hypotheses hold since $k - 1 \geq \delta n/2$ and $c_{\delta/2}(Q - 1)^{18/\delta} \leq c_{\delta/2} n^{3/4} \leq n$, and its radius is exactly R . Consequently

$$\log \text{List}_{C^\perp}(R, Q - 1) \leq c_{\delta/2} Q^{6/\delta} \log n \leq c_{\delta/2} n^{1/4} \log n.$$

With $\eta_Q \leq 1 - 1/(16Q^2)$, the transfer gives

$$\text{SD}(\tau(\mathbf{U}_C), \tau(\mathbf{U}_{\mathbb{F}_p^n})) \leq \frac{1}{2} \exp\left(-\frac{\delta n}{64Q^2} + \frac{c_{\delta/2}}{2} n^{1/4} \log n\right) \leq \frac{1}{2} \exp\left(-\frac{\delta n}{128Q^2}\right),$$

where the last step holds for all sufficiently large n , because $Q^2 \leq n^{\delta/12}$ and $\delta/12 + 1/4 < 1$ give $c_{\delta/2} Q^2 n^{1/4} \log n \leq \delta n/64$. For Shamir sharing, apply Lemma 1 to the zero-secret code; its factor two cancels the prefactor $1/2$. Thus $c_\delta = \delta/128$ suffices in both cases, and $2^{2m} \leq n^{\delta/12}$ gives the stated bound. $\square$

5 Structured leakage at constant-rate thresholds

This section introduces the second tool, an iterated Cauchy–Schwarz inequality of generalized von Neumann type tailored to MDS systems of linear forms (Lemma 12 and Corollary 3). It bounds an average of a product of functions along the forms of a GRS code by a product of Gowers norms, and for an MDS system it retains linearly many such norms at every constant rate. We apply it on its own, through the L^1 bound of Proposition 1 with $r_0 = k - 1$, to prove Theorem 7: resilience to quadratic-residue leakage and to almost all $\Theta_c(\log_2 p)$ -bit local leakage functions at every positive constant rate. Section 6 combines the same inequality with the list-decoding estimates of Section 4.

Nguyen [Ngu24] relates leakage security to Gowers norms and bounds these norms for quadratic-residue and random leakage, but retains a single Gowers-norm factor, so the bounds need an exponentially large field at constant rate. The MDS von Neumann inequality supplies linearly many factors from the same local estimates, which allows fields of size just above n .

Recall that $\tau_{\text{QR}}(x) = 1$ if x is a square in $\mathbb{F}_p$, including zero, and $\tau_{\text{QR}}(x) = 0$ otherwise.

Theorem 7 (Structured leakage at constant rate). *Fix $0 < c < 1$. There are constants $\eta_c, a_c, b_c > 0$ and $n_0(c)$ such that, for $n \geq n_0(c)$ and every prime $p > n$, the following hold for GRS codes $C = \text{GRS}_{\alpha, v}(n, k - 1)$ with $k \geq cn$.*

1. For $\tau_i(x) = \tau_{\text{QR}}(a_i x + b_i)$, where $a_i \in \mathbb{F}_p^*$ and $b_i \in \mathbb{F}_p$,

$$\text{SD}(\tau(U_C), \tau(U_{\mathbb{F}_p^n})) \leq \exp(-a_c n \log p).$$

2. For every integer $1 \leq m \leq \eta_c \log_2 p$, all but an $\exp(-b_c \sqrt{p})$ fraction of tuples $\tau = (\tau_i: \mathbb{F}_p \rightarrow \{0, 1\}^m)_{i \in [n]}$ satisfy

$$\text{SD}(\tau(U_C), \tau(U_{\mathbb{F}_p^n})) \leq \exp(-a_c n \log p)$$

simultaneously for every such code C .

Both conclusions hold for (n, k) -Shamir sharing between every pair of secrets, with the same error bounds.

The product bound for Gowers norms, together with standard concentration estimates (Lemma 13), gives resilience to almost all local leakage functions in part 2. This does not assert resilience to every local leakage function as in Definition 5.

Remark 3 (Affine changes of the leakage input). Replacing $f(x)$ by $f(ax + b)$ with $a \neq 0$ changes no Gowers norm: substitute $x \mapsto ax + b$ and $h_t \mapsto ah_t$ in the definition. This gives the affine form of quadratic-residue leakage in Theorem 7, and likewise every tuple of random maps that satisfies the Gowers-norm event below remains successful after coordinatewise affine changes of input. The changes may depend on the public parameters but are fixed before the codeword is sampled.

For Shamir sharing with $k \geq cn$, Lemma 1 applied to $C_0 = \text{GRS}_{\alpha, \alpha}(n, k - 1)$, together with the translation closure in Remark 3, gives the code bounds with an extra factor two; we choose the constant a_c below small enough to absorb it.

Section 5.2 turns a uniform bound on the local Gowers norms into a leakage bound with explicit finite parameters; Sections 5.3 and 5.4 supply the local bounds for the two classes; Section 5.5 extracts a sufficient field size at square-root thresholds, where the attack discussed at the end of that subsection shows that some field-size condition is needed.

5.1 A product bound for Gowers norms

Iterated Cauchy–Schwarz is a standard tool in additive combinatorics and higher-order Fourier analysis [Gow01, TV06, GT10]. We use the following consequence of Manners’s generalized von Neumann inequality for vector-valued linear maps [Man21, Section 3.1]. Grouping several forms into one map gives a product of Gowers norms. We include a self-contained proof of the form used below.

Fix a prime p , integers $k \geq 2$ and $r \geq 1$, and write $V = \mathbb{F}_p^{k-1}$.

Definition 12 (Linear forms and systems of forms). A *linear form* on V is a map $L(\mathbf{z}) = \sum_{a=1}^{k-1} c_a z_a$, with $\mathbf{c} \in \mathbb{F}_p^{k-1}$. A *system of linear forms* is an ordered tuple $(L_1, \dots, L_r)$. A subfamily is independent if its coefficient vectors are linearly independent over $\mathbb{F}_p$. The system is *MDS* (maximum-distance-separable) if every subfamily of at most $k-1$ forms is independent.

An *affine-linear form* is a map $\psi = b + L$, with $b \in \mathbb{F}_p$ and L linear. For a system $\Psi = (\psi_i)_{i=1}^r$, where $\psi_i = b_i + L_i$, independence and the MDS property always refer to the linear parts L_i .

Definition 13 (Average along a system of forms). For functions $\mathbf{f} = (f_1, \dots, f_r)$, with $f_i : \mathbb{F}_p \rightarrow \mathbb{C}$, define

$$\Lambda_\Psi(\mathbf{f}) = \mathbb{E}_{\mathbf{z} \in V} \left[\prod_{i=1}^r f_i(\psi_i(\mathbf{z})) \right].$$

For $C = \text{GRS}_{\alpha, v}(n, k-1)$, the forms $L_i(\mathbf{z}) = v_i \sum_{j=1}^{k-1} z_j \alpha_i^{j-1}$ give a uniform codeword when $\mathbf{z}$ is uniform in V . They form an MDS system by the Vandermonde determinant. More generally, independent linear parts give independent uniform evaluations, even after adding constants. We use $\sqcup$ for a disjoint union and regard the empty family as independent.

Lemma 12 (A product of Gowers norms). *Let $\Psi = (b_i + L_i)_{i=1}^r$ be a system on V , and let $f_i : \mathbb{F}_p \rightarrow \mathbb{C}$. Suppose $[r] = J \sqcup I_1 \sqcup \dots \sqcup I_t$, with $t \geq 2$, and the linear parts indexed by $I_a \cup J$ are independent for every a . Then*

$$|\Lambda_\Psi(\mathbf{f})| \leq \prod_{j \in J} \|f_j\|_{U^t} \prod_{i \in [r] \setminus J} \|f_i\|_\infty.$$

Proof. The claim is immediate if $J = \emptyset$ or some f_i is zero. By homogeneity, assume $\|f_i\|_\infty \leq 1$ for every $i \notin J$. Replacing $f_i(x)$ by $f_i(b_i + x)$, which preserves both norms, reduces to linear forms. Group the forms in J into one map and their functions into one function, and do the same for each I_a :

$$\begin{aligned} L_J(\mathbf{z}) &= (L_j(\mathbf{z}))_{j \in J}, & F(\mathbf{x}) &= \prod_{j \in J} f_j(x_j), & \mathbf{x} &\in \mathbb{F}_p^J; \\ L_{I_a}(\mathbf{z}) &= (L_i(\mathbf{z}))_{i \in I_a}, & G_a(\mathbf{y}) &= \prod_{i \in I_a} f_i(y_i), & \mathbf{y} &\in \mathbb{F}_p^{I_a}. \end{aligned}$$

Then $\|G_a\|_\infty \leq 1$ and $\Lambda_\Psi(\mathbf{f}) = \mathbb{E}_{\mathbf{z}} [F(L_J \mathbf{z}) \prod_{a=1}^t G_a(L_{I_a} \mathbf{z})]$. Put $K_a = \ker L_{I_a} = \bigcap_{i \in I_a} \ker L_i$, with $K_a = V$ if $I_a = \emptyset$. Independence of the forms indexed by $I_a \cup J$ says that $(L_J, L_{I_a}) : V \rightarrow \mathbb{F}_p^J \times \mathbb{F}_p^{I_a}$ is surjective; hence

$$L_J(K_a) = \mathbb{F}_p^J \quad \text{for every } a, \quad L_J(V) = \mathbb{F}_p^J.$$

For $0 \leq s \leq t$, let $\mathbf{h}_u, \mathbf{h}'_u$ be independent and uniform in K_u for $u \leq s$, independent of the uniform $\mathbf{z} \in V$. Write $\mathbf{h} = (\mathbf{h}_u)_{u \leq s}$ and $\mathbf{h}' = (\mathbf{h}'_u)_{u \leq s}$ for these collections. For $\omega \in \{0, 1\}^s$, write $\mathbf{h}_\omega = \sum_{u \leq s} \mathbf{h}_u^{(\omega_u)}$, where $\mathbf{h}_u^{(0)} = \mathbf{h}_u$ and $\mathbf{h}_u^{(1)} = \mathbf{h}'_u$. Define

$$\Lambda_s = \mathbb{E}_{\mathbf{z}, \mathbf{h}, \mathbf{h}'} \left[\prod_{\omega \in \{0, 1\}^s} C^{|\omega|} \left(F(L_J(\mathbf{z} + \mathbf{h}_\omega)) \prod_{a > s} G_a(L_{I_a}(\mathbf{z} + \mathbf{h}_\omega)) \right) \right],$$

so that $\Lambda_0 = \Lambda_\Psi(\mathbf{f})$. We claim that $|\Lambda_s|^2 \leq \Lambda_{s+1}$ for $0 \leq s < t$, where $\Lambda_{s+1} \geq 0$. Indeed, write the integrand of Λ_s as

$$\prod_{\omega} C^{|\omega|} G_{s+1}(L_{I_{s+1}}(\mathbf{z} + \mathbf{h}_\omega)) \cdot \Phi(\mathbf{z}, \mathbf{h}, \mathbf{h}'),$$

where Φ collects the factors involving F and G_a for $a > s + 1$. Translating $\mathbf{z}$ by an independent uniform $\mathbf{h}_{s+1} \in K_{s+1}$ preserves its distribution and leaves the G_{s+1} factors unchanged. Their product has modulus at most one, so Cauchy–Schwarz in $(\mathbf{z}, \mathbf{h}, \mathbf{h}')$ gives

$$\begin{aligned} |\Lambda_s|^2 &\leq \mathbb{E}_{\mathbf{z}, \mathbf{h}, \mathbf{h}'} |\mathbb{E}_{\mathbf{h}_{s+1}} [\Phi(\mathbf{z} + \mathbf{h}_{s+1}, \mathbf{h}, \mathbf{h}')] |^2 \\ &= \mathbb{E}_{\mathbf{z}, \mathbf{h}, \mathbf{h}', \mathbf{h}_{s+1}, \mathbf{h}'_{s+1}} \left[\Phi(\mathbf{z} + \mathbf{h}_{s+1}, \mathbf{h}, \mathbf{h}') \overline{\Phi(\mathbf{z} + \mathbf{h}'_{s+1}, \mathbf{h}, \mathbf{h}')} \right] = \Lambda_{s+1}. \end{aligned}$$

The last integrand is exactly that of Λ_{s+1} : the new coordinate ω_{s+1} selects $\mathbf{h}_{s+1}$ or $\mathbf{h}'_{s+1}$ and contributes one conjugation.

Iterating gives

$$|\Lambda_\Psi(\mathbf{f})|^{2^t} \leq \Lambda_t = \mathbb{E}_{\mathbf{z}, \mathbf{h}, \mathbf{h}'} \left[\prod_{\omega \in \{0,1\}^t} C^{|\omega|} F(L_J(\mathbf{z} + \mathbf{h}_\omega)) \right].$$

Put $\mathbf{d}_u = \mathbf{h}'_u - \mathbf{h}_u$, so that $\mathbf{z} + \mathbf{h}_\omega = \mathbf{z} + \sum_u \mathbf{h}_u + \sum_u \omega_u \mathbf{d}_u$, and set $\mathbf{x} = L_J(\mathbf{z} + \sum_u \mathbf{h}_u)$ and $\mathbf{y}_u = L_J(\mathbf{d}_u)$. Surjectivity of L_J makes $\mathbf{x}$ uniform on $\mathbb{F}_p^J$ and independent of $(\mathbf{h}, \mathbf{h}')$. Each $\mathbf{d}_u$ is uniform on K_u , so $L_J(K_u) = \mathbb{F}_p^J$ makes $\mathbf{y}_u$ uniform on $\mathbb{F}_p^J$, and all these variables are independent. Therefore

$$\Lambda_t = \mathbb{E}_{\mathbf{x}, \mathbf{y}_1, \dots, \mathbf{y}_t \in \mathbb{F}_p^J} \left[\prod_{\omega \in \{0,1\}^t} C^{|\omega|} F\left(\mathbf{x} + \sum_{u=1}^t \omega_u \mathbf{y}_u\right) \right] = \|F\|_{U^t(\mathbb{F}_p^J)}^{2^t}.$$

Finally, the definition of the Gowers norm factors over coordinates:

$$\|F\|_{U^t(\mathbb{F}_p^J)}^{2^t} = \mathbb{E}_{\mathbf{x}, \mathbf{h}_1, \dots, \mathbf{h}_t \in \mathbb{F}_p^J} \left[\prod_{\omega \in \{0,1\}^t} \prod_{j \in J} C^{|\omega|} f_j \left(x_j + \sum_{u=1}^t \omega_u h_{u,j} \right) \right] = \prod_{j \in J} \|f_j\|_{U^t}^{2^t}.$$

Taking 2^t -th roots and restoring the original scaling proves the claim. $\square$

For an MDS system, the lemma's independence conditions reduce to $|I_a| + |J| \leq k - 1$. This is the only use of the MDS property in the following corollary.

Corollary 3 (Number of U^t factors). *Let Ψ be an MDS system, let $r \geq k$ and $t \geq 2$, and define*

$$q_t(r, k) = \left\lfloor \frac{t(k-1) - r}{t-1} \right\rfloor.$$

If $q_t(r, k) \geq 1$, then, for every $J \subseteq [r]$ of size $q_t(r, k)$,

$$|\Lambda_\Psi(\mathbf{f})| \leq \prod_{j \in J} \|f_j\|_{U^t} \prod_{i \in [r] \setminus J} \|f_i\|_\infty.$$

Proof. Put $q = q_t(r, k)$. Since $r \geq k$, we have $q \leq k-2 < r$. The definition of q gives $r-q \leq t(k-1-q)$. Thus we can partition the indices outside J into t groups I_a , each of size at most $k-1-q$. Every $I_a \cup J$ has size at most $k-1$, so [Lemma 12](#) applies. $\square$

If the functions are bounded by one and their U^t norms are at most $\rho < 1$, this gives $\rho^{q_t(r,k)}$. For structured leakage, we allow t to grow with n . In [Section 6](#), we will reuse the bound with $t = 3$ for the below-half theorem.

5.2 From Gowers norms to leakage resilience

Let $\tau_i: \mathbb{F}_p \rightarrow \{0, 1\}^m$, and put $f_{i,b}(x) = \mathbb{1}[\tau_i(x) = b] - \nu_i(b)$, as in Lemma 6. The L^1 bound of Proposition 1 with $r_0 = k - 1$ reduces the leakage distance to averages of products of these functions.

Proposition 3 (Finite-parameter leakage bound). *Let C be an $[n, k - 1, n - k + 2]_p$ MDS code, and let $t \geq 2$ be an integer with $q_t(n, k) \geq 1$. If $\|f_{i,b}\|_{U^t} \leq \rho \leq 1$ for all $i \in [n]$ and $b \in \{0, 1\}^m$, then*

$$\text{SD}(\tau(U_C), \tau(U_{\mathbb{F}_p^n})) \leq \frac{1}{2}(1 + 2^m)^n \rho^{q_t(n,k)}.$$

For one-bit maps, if the functions $f_i = 2(\tau_i - \mathbb{E}_x[\tau_i(x)])$ satisfy $\|f_i\|_{U^t} \leq \rho \leq 1$, the distance is at most $3^n \rho^{q_t(n,k)}$.

Proof. The dual of C has minimum distance k , so Proposition 1 and Lemma 6 give

$$\text{SD}(\tau(U_C), \tau(U_{\mathbb{F}_p^n})) \leq \frac{1}{2} \sum_{|A| \geq k} \sum_{b_A \in (\{0,1\}^m)^A} \left| \mathbb{E}_{\mathbf{X} \sim U_C} \left[\prod_{i \in A} f_{i,b_i}(X_i) \right] \right|.$$

Fix A with $|A| = r \geq k$. The coordinate forms of a linear parametrization of C , restricted to A , form an MDS system, since any $k - 1$ of them are independent, and $\|f_{i,b_i}\|_\infty \leq 1$. Since $q_t(r, k) \geq q_t(n, k)$, Corollary 3 bounds each average by $\rho^{q_t(r,k)} \leq \rho^{q_t(n,k)}$. Hence

$$\text{SD}(\tau(U_C), \tau(U_{\mathbb{F}_p^n})) \leq \frac{1}{2} \rho^{q_t(n,k)} \sum_{r=k}^n \binom{n}{r} 2^{mr} \leq \frac{1}{2} (1 + 2^m)^n \rho^{q_t(n,k)}.$$

For one-bit maps, $f_{i,1} = f_i/2$ and $f_{i,0} = -f_i/2$, so the first bound gives $\frac{1}{2} 3^n (\rho/2)^{q_t(n,k)} \leq 3^n \rho^{q_t(n,k)}$, which completes the proof. $\square$

At constant rate, fix an integer $t \geq 2$ with $tc > 1$ and put $\beta = (tc - 1)/(t - 1) > 0$. For $k \geq cn$, the number of retained Gowers factors satisfies

$$q_t(n, k) = \left\lfloor \frac{t(k - 1) - n}{t - 1} \right\rfloor \geq \beta n - \frac{t}{t - 1} - 1 \geq \beta n - 3. \quad (3)$$

Thus local norms of size $p^{-\Omega_c(1)}$ give $\exp(-\Omega_c(n \log p))$ leakage distance even when m is a sufficiently small constant times $\log_2 p$.

5.3 Quadratic-residue leakage

Let $\chi: \mathbb{F}_p \rightarrow \{-1, 0, 1\}$ be the quadratic character, with $\chi(0) = 0$. The character-sum estimate of [Ngu24, Lemma 2] gives $\|\chi\|_{U^t}^{2^t} \leq 2^t/\sqrt{p}$. For $\tau = \tau_{\text{QR}}$ we have $2\mathbb{E}_x[\tau(x)] = 1 + 1/p$, so the centered function is $f = \chi + \mathbb{1}_{\{0\}} - 1/p$. The Gowers product of $\mathbb{1}_{\{0\}}$ is one exactly when $x = h_1 = \dots = h_t = 0$, so $\|\mathbb{1}_{\{0\}}\|_{U^t} = p^{-(t+1)/2^t}$, and the triangle inequality gives

$$\|f\|_{U^t} \leq \left(\frac{2^t}{\sqrt{p}} \right)^{1/2^t} + p^{-(t+1)/2^t} + \frac{1}{p} \leq 4p^{-1/2^{t+1}}.$$

The same bound holds if the output at zero is changed to 0, where the centered function is $\chi - \mathbb{1}_{\{0\}} + 1/p$.

Proof of Theorem 7, part 1. Fix t and β as in (3), and write $q = q_t(n, k)$. For n sufficiently large, $q \geq 1$ and $4p^{-1/2^{t+1}} \leq 1$ for every $p > n$, and the affine changes of input preserve the local bound by Remark 3. Proposition 3 bounds the distance by

$$3^n (4p^{-1/2^{t+1}})^q = \exp\left(n \log 3 + q \log 4 - \frac{q}{2^{t+1}} \log p\right).$$

Since $\beta n - 3 \leq q \leq n$ and $p > n$, the exponent is at most $-a_1 n \log p$ with $a_1 = \beta/2^{t+3}$, for n sufficiently large depending only on c . The bound is uniform over the code and the affine changes of input. $\square$

5.4 Almost all logarithmic-bit leakage functions

For a random map $\tau: \mathbb{F}_p \rightarrow \{0, 1\}^m$, each output indicator minus 2^{-m} has independent centered values. The cube-collision argument for random signs in [Ngu24, Lemma 4] therefore applies to these indicators as well. Subtracting their empirical means costs at most a factor two in the Gowers norm; no balance assumption on the output probabilities is needed.

Lemma 13 (Gowers norm of a random leakage function). *Let $t \geq 2$, $m \geq 1$, and $0 < \rho \leq 1$. For a uniformly random map $\tau: \mathbb{F}_p \rightarrow \{0, 1\}^m$ and a fixed output b , put $f_b(x) = \mathbb{1}[\tau(x) = b] - \Pr_{u \sim U_{\mathbb{F}_p}}[\tau(u) = b]$. If $p(\rho/2)^{2^t} \geq 2\binom{2^t}{2}$, then*

$$\Pr_{\tau}[\|f_b\|_{U^t} > \rho] \leq \exp\left(-\frac{p(\rho/2)^{2^{t+1}}}{2^{2t+3}}\right).$$

Proof. Put $\xi_b(x) = \mathbb{1}[\tau(x) = b] - 2^{-m}$ and $T(\tau) = \|\xi_b\|_{U^t}^{2^t}$. If all 2^t vertices of a Gowers cube are distinct, independence and $\mathbb{E}_{\tau}[\xi_b(x)] = 0$ make its expected product zero. Each pair of vertices coincides with probability $1/p$, and $|\xi_b| \leq 1$, so

$$\mathbb{E}_{\tau}[T] \leq \frac{\binom{2^t}{2}}{p}, \quad \|f_b\|_{U^t} = \|\xi_b - \mathbb{E}_x[\xi_b(x)]\|_{U^t} \leq \|\xi_b\|_{U^t} + |\mathbb{E}_x[\xi_b(x)]| \leq 2 \|\xi_b\|_{U^t}.$$

Changing one value $\tau(a)$ affects at most a $2^t/p$ fraction of the cube products, each by at most two. Thus T changes by at most $2^{t+1}/p$, and bounded differences [McD89] gives

$$\Pr_{\tau}[T - \mathbb{E}_{\tau}[T] \geq u] \leq \exp\left(-\frac{pu^2}{2^{2t+1}}\right).$$

The hypothesis gives $\mathbb{E}_{\tau}[T] \leq \frac{1}{2}(\rho/2)^{2^t}$, whereas $\|f_b\|_{U^t} > \rho$ implies $T > (\rho/2)^{2^t}$. Taking $u = \frac{1}{2}(\rho/2)^{2^t}$ proves the claim. $\square$

Proof of Theorem 7, part 2. Fix t and β as in (3), and choose

$$\rho = p^{-1/2^{t+2}}, \quad \eta_c = \frac{\beta}{2^{t+4}}, \quad 1 \leq m \leq \eta_c \log_2 p.$$

For large p , the hypothesis of Lemma 13 holds because $p(\rho/2)^{2^t} = 2^{-2^t} p^{3/4}$. Its conclusion is $\Pr[\|f_{i,b}\|_{U^t} > \rho] \leq \exp(-b_0 \sqrt{p})$ for a constant $b_0 > 0$ depending only on t . A union bound over the $n2^m$ pairs (i, b) gives

$$\Pr[\|f_{i,b}\|_{U^t} > \rho \text{ for some } (i, b)] \leq n2^m \exp(-b_0 \sqrt{p}) \leq p^{1+\eta_c} \exp(-b_0 \sqrt{p}) \leq \exp(-b_0 \sqrt{p}/2).$$

On the complementary event, take n large enough that $q_t(n, k) \geq 3\beta n/4$. Since $\log(1 + 2^m) \leq \log 2 + \eta_c \log p$, [Proposition 3](#) gives

$$\begin{aligned} \text{SD}(\tau(U_C), \tau(U_{\mathbb{F}_p^n})) &\leq \frac{1}{2} \exp \left(n \log(1 + 2^m) - \frac{q_t(n, k)}{2^{t+2}} \log p \right) \\ &\leq \frac{1}{2} \exp(n \log 2 - 2\eta_c n \log p) \leq \frac{1}{2} \exp(-\eta_c n \log p). \end{aligned}$$

The event depends only on the maps, so this holds simultaneously for all codes in the theorem and, by [Remark 3](#), after all coordinatewise affine changes of input. Take $b_c = b_0/2$ and $a_c = \min\{a_1/2, \eta_c\}$, increasing $n_0(c)$ if needed. The factor two in the Shamir reduction is absorbed by the displayed factor $1/2$ here and by the slack in a_1 for part 1. $\square$

For fixed m , the same proof gives the stronger success probability $1 - \exp(-\Omega_{c,m}(p))$ with leakage distance $\exp(-\Omega_{c,m}(n))$: choose a constant $\rho > 0$ such that $\beta \log(1/\rho) > \log(1 + 2^m)$ and apply the same two bounds.

5.5 Field size for square-root thresholds

When $k = \Theta(\sqrt{n})$, the Cauchy–Schwarz order t must grow with n , so we use the finite-parameter bound rather than the constant-rate theorem. The next corollary gives an explicit sufficient field size for leakage error $\exp(-n)$ in both applications.

Corollary 4 (An explicit field-size bound). *Let $3 \leq k \leq n$ and $t = \lceil (n-1)/(k-2) \rceil$. If $\log p \geq 8n2^t$, then for every $C = \text{GRS}_{\alpha,v}(n, k-1)$, $\text{SD}(\tau(U_C), \tau(U_{\mathbb{F}_p^n})) \leq \exp(-n)$ for quadratic-residue leakage with the affine input changes of [Theorem 7](#); and for independent uniformly random Boolean maps, with probability at least $1 - \exp(-n)$, the same bound holds simultaneously for every such code. Both conclusions hold for Shamir leakage between every pair of secrets with the same error.*

Proof. By the choice of t , $t(k-2) \geq n-1$, i.e. $t(k-1) - n \geq t-1$, so $q = q_t(n, k) \geq 1$. Put $\rho = \exp(-n)/(2 \cdot 3^n)$ and $f_i = 2(\tau_i - \mathbb{E}_x[\tau_i(x)])$. If $\|f_i\|_{U^t} \leq \rho$ for every i , then [Proposition 3](#) gives $3^n \rho^q \leq 3^n \rho = \frac{1}{2} \exp(-n)$, and the factor $\frac{1}{2}$ yields the Shamir error through [Lemma 1](#).

For quadratic-residue leakage, [Section 5.3](#) gives $\|f_i\|_{U^t} \leq 4p^{-1/2^{t+1}} \leq \rho$ whenever $\log p \geq 2^{t+1} \log(4/\rho) = 2^t(2 \log 8 + 2(1 + \log 3)n)$, which follows from $\log p \geq 8n2^t$ since $n \geq 3$.

For a random Boolean map, $2\tau - 1$ has independent uniform signs. The same cube-collision argument as in [Lemma 13](#) gives $\mathbb{E}_\tau[\|2\tau - 1\|_{U^t}^{2^t}] \leq \binom{2^t}{2}/p$, and $\|2(\tau - \mathbb{E}_x[\tau(x)])\|_{U^t} \leq 2\|2\tau - 1\|_{U^t}$. Markov's inequality and a union bound therefore give

$$\Pr[\|f_i\|_{U^t} > \rho \text{ for some } i \in [n]] \leq \frac{n 2^{2^t} \binom{2^t}{2}}{p \rho^{2^t}} \leq \exp(-n),$$

the last step because $2^t \log(2/\rho) + n + \log n + \log \binom{2^t}{2} \leq 2^t((1 + \log 3)n + 2 \log 2) + n + \log n + 2t \log 2 \leq 8n2^t \leq \log p$, using $2 \leq t \leq n-1$ and $n + \log n + 2t \log 2 \leq 4n \leq n2^t$. The event depends only on the maps and is preserved by affine input changes, so the bound holds simultaneously for all codes and input changes in the statement. $\square$

For $k = \Theta(\sqrt{n})$ we have $t = n/k + O(1)$, so the condition reads $\log p \geq Cn 2^{n/k}$ for a constant C . Concretely, for $n = k^2$ with $k \geq 5$, one gets $t = k + 3$ and $q = 1$, so $\log p \geq 64n 2^{\sqrt{n}}$ suffices; a single Gowers factor carries the bound. This field size is doubly exponential in $\sqrt{n}$; we do not claim it is necessary.

A contrasting attack at square-root thresholds. Kopparty's algorithm for recovering a monic squarefree polynomial from noisy quadratic-character values [Kop26] attacks Shamir sharing when $n = p - 1$ and k is at most a small constant times $\sqrt{n}$: party i leaks $\tau_{\text{QR}}(P(\alpha_i) + \alpha_i^k)$, which is the character value of the monic polynomial $Q(X) = X^k + P(X)$ at α_i up to at most $k + 1$ discrepancies (the roots of Q and the missing point 0). The decoder tolerates these in this degree range and recovers Q , hence the secret $Q(0)$, whenever Q is squarefree. For each fixed secret s , the discriminant of Q is a nonzero polynomial of degree at most $2k - 2$ in the random coefficients of P (it is nonzero at $X^k + s$ for $s \neq 0$ and at $X^k + X$ for $s = 0$, both squarefree since $k < p$), so Q fails to be squarefree with probability at most $(2k - 2)/p$. The attack uses only the fixed input shifts covered by Theorem 7, not additional leaked bits. At every positive constant rate our theorem gives security even for $p = n + 1$; at square-root thresholds the corollary above gives security over sufficiently large fields. The intermediate range is open.

6 Leakage resilience below half

Theorem 8 (GRS codes below half). *There are absolute constants $c_{\text{bh}} < 1/2$, $\gamma > 0$, and n_0 such that, for $n \geq n_0$ and every prime $p > n$, every GRS code over $\mathbb{F}_p$ of length n and rate at least c_{bh} is $e^{-\gamma n}$ -resilient to one-bit local leakage.*

We prove Theorem 8 by combining the three tools: Proposition 2 with an intermediate cutoff r_0 close to n ; a supportwise form of the list-recovery argument of Section 4, which controls the squared components below the cutoff (Section 6.1); and the MDS von Neumann inequality of Section 5.1 together with a second-moment bound, which control the components above it (Section 6.2). The supportwise form is needed because the list bound of Theorem 4 is available only at radius $R < k$, and below rate half Lemma 11 cannot use it. Both estimates have negative exponents at rate half; continuity gives a fixed rate below half (Section 6.3). Throughout, C is a GRS code of dimension $k - 1$ unless a statement says otherwise, and g_i, f_i are as in Section 3.4.

6.1 List recovery for small supports

Lemma 11 needs the list bound at radius $n - j$ with $j \leq k - 1$, whereas Theorem 4 supplies it at radius $R < k$; below rate half, $n - k + 1 > k - 1$, so no admissible j satisfies $n - j \leq R$. At a fixed support size r , however, every dual word has $n - r$ zero coordinates, which count as agreements with the list $\{0\}$. Retaining j Fourier factors on a common set H and putting $\{0\}$ outside H brings the radius down to $r - j$, so $j = r - R$ suffices, and $j \leq k - 1$ as long as $r \leq k + R - 1$. Summing over H gives the following bound.

Lemma 14 (List recovery for a fixed support size). *In the setting of Section 4, so that $C^\perp$ has minimum distance at least k , the maps τ_i have at most Q output symbols, and $p \geq 16Q$ or $Q = 2$ with p odd, for all integers $k \leq r \leq n$ and $1 \leq j < k$,*

$$\sum_{|A|=r} \|\mathsf{T}(f_C^{\perp A})\|_2^2 \leq \eta_Q^{k-1-j} \text{List}_{C^\perp}(r - j, Q - 1) \frac{\binom{n}{j}}{\binom{r}{j}}.$$

Proof. Fix $H \subseteq [n]$ with $|H| = j$. For each $A \supseteq H$ of size r , choose I_A with $H \subseteq I_A \subseteq A$ and $|I_A| = k - 1$, which is possible since $j \leq k - 1 < r$. Apply Lemma 8 with $J = A \setminus I_A$, and bound the $k - 1 - j$ factors indexed by $I_A \setminus H$ by η_Q using Lemma 9:

$$\sum_{\substack{A \supseteq H \\ |A|=r}} \|\mathsf{T}(f_C^{\perp A})\|_2^2 \leq \sum_{\substack{A \supseteq H \\ |A|=r}} \sum_{\substack{\mathbf{y} \in C^\perp \\ \text{supp}(\mathbf{y})=A}} \prod_{i \in I_A} \|\mathsf{T}_i \chi_{y_i}\|_2^2 \leq \eta_Q^{k-1-j} \sum_{\substack{\mathbf{y} \in C^\perp \\ \text{wt}(\mathbf{y})=r, H \subseteq \text{supp}(\mathbf{y})}} \prod_{i \in H} \|\mathsf{T}_i \chi_{y_i}\|_2^2.$$

As in Lemma 11, the last sum is a nonnegative linear combination of monomials $\prod_{i \in H} w_i(y_i)$ in the weights $w_i(a) = \|\mathsf{T}_i \chi_a\|_2^2$, $a \in \mathbb{F}_p^*$. The constraints on the weights follow from Lemma 9. Lemma 10 (the coordinates outside H play no role) yields lists $V_i \subseteq \mathbb{F}_p^*$ of size $Q - 1$, $i \in H$, with

$$\sum_{\substack{\mathbf{y} \in C^\perp \\ \text{wt}(\mathbf{y})=r, H \subseteq \text{supp}(\mathbf{y})}} \prod_{i \in H} \|\mathsf{T}_i \chi_{y_i}\|_2^2 \leq |\{\mathbf{y} \in C^\perp : \text{wt}(\mathbf{y}) = r, y_i \in V_i \text{ for all } i \in H\}|.$$

Take input lists $S_i = V_i$ on H and $S_i = \{0\}$ outside H . Every counted word agrees with the lists on H and on its $n - r$ zero coordinates, which lie outside H ; so the count is at most $\text{List}_{C^\perp}(r - j, Q - 1)$.

Finally, sum over H . Each support of size r contains exactly $\binom{r}{j}$ sets H , so

$$\binom{r}{j} \sum_{|A|=r} \|\mathsf{T}(f_C^{\bar{A}})\|_2^2 = \sum_{|H|=j} \sum_{\substack{A \supseteq H \\ |A|=r}} \|\mathsf{T}(f_C^{\bar{A}})\|_2^2 \leq \binom{n}{j} \eta_Q^{k-1-j} \text{List}_{C^\perp}(r - j, Q - 1).$$

Dividing by $\binom{r}{j}$ proves the claim. $\square$

For one-bit leakage the input lists have size one, so list recovery becomes list decoding.

Corollary 5 (List decoding for a fixed support size). *Let p be an odd prime and $C \subseteq \mathbb{F}_p^n$ a linear code whose dual has minimum distance at least k . For all integers $k \leq r \leq n$ and R with $1 \leq r - R < k$,*

$$\sum_{|A|=r} |\Gamma_C(\mathbf{g}_A)|^2 \leq \text{List}_{C^\perp}(R) 2^{r-R-k+1} \frac{\binom{n}{r-R}}{\binom{r}{r-R}}.$$

Proof. Take $Q = 2$ and $j = r - R$ in Lemma 14. Then $\eta_2 = 1/2$, $\text{List}_{C^\perp}(r - j, 1) = \text{List}_{C^\perp}(R)$, and $\|\mathsf{T}(f_C^{\bar{A}})\|_2^2 = |\Gamma_C(\mathbf{g}_A)|^2$ by Lemma 7. $\square$

Write $D = C^\perp$ for the remainder of this subsection. For our decoding radius $R < k$, the condition $1 \leq r - R < k$ requires $k \leq r \leq \min\{n, k + R - 1\}$; below rate half this leaves the largest supports untreated, and Section 6.2 bounds those by Cauchy–Schwarz. The next lemma gives a uniform estimate below the cutoff $(1 - \varepsilon)n$.

Lemma 15 (Bound for smaller supports). *Fix $0 < \zeta < c < 1/2$ and $0 < \varepsilon < 1$ with $1 - \varepsilon < 2c - \zeta$. Let $k = k_n$ with $(k_n - 1)/n \rightarrow c$, and $R = \lfloor k - 1 - \zeta n \rfloor$. Assume $\text{List}_D(R) \leq L_n$ with $\log L_n = o(n)$. Then every support size $k \leq r \leq (1 - \varepsilon)n$ satisfies*

$$\sum_{|A|=r} |\Gamma_C(\mathbf{g}_A)|^2 \leq \exp(nG(c, \zeta, \varepsilon) + o(n)),$$

uniformly in the support size and the leakage maps, where

$$G(c, \zeta, \varepsilon) = (1 - 2c + \zeta) \log 2 + \log \frac{1}{2(c - \zeta)} - \frac{\varepsilon^2}{2}.$$

In particular, if $G(c, \zeta, \varepsilon) < 0$, the sum is exponentially small at each of these support sizes.

Proof. We first obtain an estimate with the integer parameters explicit. Suppose $\text{List}_D(R) \leq L$ with $1 \leq R < k$. For $k \leq r \leq \min\{n, k + R - 1\}$, put $j = r - R$; then $1 \leq j < k$ and $r - j = R$, so Corollary 5 gives

$$\sum_{|A|=r} |\Gamma_C(\mathbf{g}_A)|^2 \leq L 2^{j-k+1} \frac{\binom{n}{j}}{\binom{r}{j}}.$$

Set $t = n - r$ and $g = n - k - R + 1$. The binomial ratio has the exact product form

$$2^{j-k+1} \frac{\binom{n}{j}}{\binom{r}{j}} = 2^g \prod_{u=0}^{t-1} \frac{n-u}{2(R+t-u)}.$$

For $0 \leq u < t$ we have $R+t-u \geq R+1$, and $1-v \leq \exp(-v)$ with $R+1 \leq n$ gives $R/(R+1) \leq \exp(-1/(R+1)) \leq \exp(-1/n)$. Hence

$$\frac{n-u}{2(R+t-u)} \leq \frac{n}{2R} \left(1 - \frac{u}{n}\right) \frac{R}{R+1} \leq \frac{n}{2R} \exp\left(-\frac{u+1}{n}\right),$$

and multiplying over u gives the finite bound

$$\sum_{|A|=r} |\Gamma_C(\mathbf{g}_A)|^2 \leq L 2^g \left(\frac{n}{2R}\right)^t \exp\left(-\frac{t^2}{2n}\right),$$

since $t(t+1)/(2n) \geq t^2/(2n)$. Empty products cause no difficulty when $t = 0$.

Now take $R = \lfloor k-1-\zeta n \rfloor$ and $L = L_n$. For large n , $1 \leq R < k$ and $2R < n$, since $R/n \rightarrow c-\zeta < 1/2$. Moreover, $k+R-1 = (2c-\zeta)n + o(n) > (1-\varepsilon)n$, so $r \leq k+R-1$ throughout the stated range. Using $\varepsilon n \leq t \leq n$ in the finite bound gives

$$\begin{aligned} \sum_{|A|=r} |\Gamma_C(\mathbf{g}_A)|^2 &\leq L_n 2^{n-k-R+1} \left(\frac{n}{2R}\right)^n \exp\left(-\frac{\varepsilon^2 n}{2}\right) \\ &= \exp(nG(c, \zeta, \varepsilon) + o(n)), \end{aligned}$$

where the equality uses $(k-1)/n \rightarrow c$, $R/n \rightarrow c-\zeta$, and $\log L_n = o(n)$. The bound is independent of the support size and the leakage maps. $\square$

6.2 Iterated Cauchy–Schwarz for large supports

We bound the second term of (2). The proof separates two cases: Cauchy–Schwarz controls leakage functions with sufficiently large total squared bias, while the product of U^3 norms controls the remaining functions. Put

$$\kappa_0 = (3/4)^{1/8} < 1, \quad \beta_0 = \frac{(\log \kappa_0)^2}{64}.$$

Proposition 4 (Bound for large supports). *Suppose $2k-2 \leq n < 3k-3$, put $c = (k-1)/n$, and fix $0 < \varepsilon < 1/2$. Let $r_0 = \lfloor (1-\varepsilon)n \rfloor$, and define*

$$H(c, \varepsilon) = h(\varepsilon) + \max\left\{\frac{3c-1}{2} \log \kappa_0 + \sqrt{\beta_0}, (1-2c)(\log 2 + 1/2) - \frac{\beta_0}{2}\right\}.$$

Then

$$\frac{1}{2} \sum_{A \subseteq [n]: |A| > r_0} |\Gamma_C(\mathbf{f}_A)| \leq \exp(nH(c, \varepsilon) + O(\log n)).$$

In particular, $H(1/2, 0) = \max\{\frac{1}{8} \log \kappa_0, -\beta_0/2\} < 0$, with the formula extended continuously to $\varepsilon = 0$.

The strict inequality persists when c is slightly below half and ε is sufficiently small. We first establish the local U^3 bound, then give the two estimates for an individual support.

6.2.1 A uniform bound for centered bits

Lemma 16 (Bounds for a centered bit). *For every map $\tau: \mathbb{F}_p \rightarrow \{0, 1\}$ over an odd prime field, the function $f = 2(\tau - \mathbb{E}[\tau])$, with $\mu = 1 - 2\mathbb{E}[\tau]$, satisfies*

$$\|f\|_2 = \sqrt{1 - \mu^2}, \quad \|f\|_{U^3} \leq \kappa_0, \quad \|f\|_\infty \leq 1 + |\mu| \leq 2.$$

Proof. Put $V = 1 - \mu^2$. The values $1 + \mu$ and $-(1 - \mu)$ occur with probabilities $(1 - \mu)/2$ and $(1 + \mu)/2$, respectively. This proves the L^2 and pointwise bounds, and gives

$$\mathbb{E}[f] = 0, \quad \mathbb{E}[f^2] = V, \quad f^2 = V + 2\mu f.$$

The U^3 estimate uses the symmetry of the Fourier transform of a real function. Specifically, every real q satisfies

$$\|q\|_{U^2}^4 \leq (\mathbb{E}[q])^4 + \frac{1}{2}(\|q\|_2^2 - (\mathbb{E}[q])^2)^2 \leq \frac{1}{2}\|q\|_2^4 + \frac{1}{2}(\mathbb{E}[q])^4.$$

To see this, pair each nonzero frequency a with $-a$; the two Fourier magnitudes are equal, and the frequencies are distinct because p is odd. If $b_a = |\widehat{q}(a)|^2$, with one representative from each pair, then

$$\sum_{a \neq 0} |\widehat{q}(a)|^4 = 2 \sum_{\text{pairs}} b_a^2 \leq 2 \left(\sum_{\text{pairs}} b_a \right)^2.$$

Adding the zero frequency and using Parseval gives the first inequality; the second follows from $(\mathbb{E}[q])^2 \leq \|q\|_2^2$.

Now let $q_t(x) = f(x+t)f(x)$ and $K(t) = \mathbb{E}_x[q_t(x)]$. Expanding $f(x+t)^2 f(x)^2$ with $f^2 = V + 2\mu f$ and using $\mathbb{E}[f] = 0$ gives

$$\|q_t\|_2^2 = V^2 + 4\mu^2 K(t), \quad \mathbb{E}_t[K(t)] = 0.$$

Cauchy–Schwarz and the real-function bound applied to f give

$$|K(t)| \leq V, \quad \mathbb{E}_t[K(t)^2] = \|f\|_{U^2}^4 \leq \frac{1}{2}V^2.$$

Applying the same bound to each q_t , we obtain

$$\begin{aligned} \|f\|_{U^3}^8 &= \mathbb{E}_t[\|q_t\|_{U^2}^4] \\ &\leq \frac{1}{2}\mathbb{E}_t[(V^2 + 4\mu^2 K(t))^2] + \frac{1}{2}\mathbb{E}_t[K(t)^4] \\ &\leq \frac{1}{2}V^4 + \left(8\mu^4 + \frac{1}{2}V^2\right)\mathbb{E}_t[K(t)^2] \\ &\leq \frac{3}{4}V^4 + 4\mu^4 V^2 \leq \frac{3}{4}(V + \mu^2)^4 = \frac{3}{4}. \end{aligned}$$

The second inequality uses $\mathbb{E}_t[K(t)] = 0$ and $K(t)^4 \leq V^2 K(t)^2$; the last inequality follows by the binomial theorem, since $V, \mu^2 \geq 0$. $\square$

6.2.2 Two bounds for each support

Write $\mu_i = 1 - 2\theta_i$. The preceding lemma gives two ways to make the average small: bias decreases the L^2 norms, whereas small bias keeps the supremum norms close to one and lets the U^3 bounds act.

Lemma 17 (Bounds on $\Gamma_C(\mathbf{f}_A)$). *Suppose $2k - 2 \leq n < 3k - 3$. For every $A \subseteq [n]$ with $|A| \geq k$, put $B = \sum_{i \in A} \mu_i^2$, $e = n - 2k + 2$, and $q = q_3(n, k) = \lfloor (3k - 3 - n)/2 \rfloor$. Then*

$$|\Gamma_C(\mathbf{f}_A)| \leq \min \left\{ \exp(q \log \kappa_0 + \sqrt{nB}), \exp(e(\log 2 + 1/2) - B/2) \right\}.$$

Proof. For the first bound, use all n evaluation forms defining C , with the constant function one outside A ; any $k - 1$ of the forms are independent by the MDS property, and q is the number of retained Gowers factors for $t = 3$. Since $0 \leq q \leq (k - 1)/2 < |A|$, choose $J \subseteq A$ of size q . The MDS von Neumann inequality (Corollary 3) with $t = 3$, followed by Lemma 16, gives

$$|\Gamma_C(\mathbf{f}_A)| \leq \prod_{j \in J} \|f_j\|_{U^3} \prod_{i \in A \setminus J} \|f_i\|_{\infty} \leq \kappa_0^q \prod_{i \in A \setminus J} (1 + |\mu_i|) \leq \kappa_0^q \exp\left(\sum_{i \in A} |\mu_i|\right) \leq \kappa_0^q \exp(\sqrt{nB}).$$

If $q = 0$, the first inequality is just the supremum bound.

For the second bound, partition $[n] = I_1 \sqcup I_2 \sqcup E$ with $|I_1| = |I_2| = k - 1$ and $|E| = e$. Bound the factors on E by two and apply Cauchy–Schwarz to the other two products. For $\mathbf{X} \sim U_C$,

$$|\Gamma_C(\mathbf{f}_A)| \leq 2^e \prod_{t=1}^2 \left(\mathbb{E}_{\mathbf{X} \sim U_C} \left[\prod_{i \in A \cap I_t} |f_i(X_i)|^2 \right] \right)^{1/2} = 2^e \prod_{i \in A \setminus E} \sqrt{1 - \mu_i^2},$$

where the equality uses independence and uniformity within each I_t , again from the MDS property. Since $\sqrt{1 - x} \leq \exp(-x/2)$ and $\sum_{i \in A \cap E} \mu_i^2 \leq e$,

$$2^e \prod_{i \in A \setminus E} \sqrt{1 - \mu_i^2} \leq \exp\left(e \log 2 - \frac{1}{2} \sum_{i \in A \setminus E} \mu_i^2\right) \leq \exp(e(\log 2 + 1/2) - B/2). \quad \square$$

Proof of Proposition 4. We have $r_0 \geq k - 1$, so Lemma 17 applies to every support in the sum. If $B \leq \beta_0 n$, use its first bound; otherwise use its second. Since $q = (3c - 1)n/2 + O(1)$ and $e = (1 - 2c)n$, in either case

$$|\Gamma_C(\mathbf{f}_A)| \leq \exp\left(n \max\left\{ \frac{3c - 1}{2} \log \kappa_0 + \sqrt{\beta_0}, (1 - 2c)(\log 2 + 1/2) - \frac{\beta_0}{2} \right\} + O(1)\right).$$

There are at most $\sum_{0 \leq t < \varepsilon n} \binom{n}{t} \leq (n + 1) \exp(nh(\varepsilon))$ such supports, since their complements have fewer than εn elements. Multiplying the two bounds proves the proposition. $\square$

6.3 Combining the estimates

Both estimates have strictly negative exponents at rate half when the cutoff is sufficiently close to n . We use continuity to keep both exponents negative at a slightly smaller rate.

Proof of Theorem 8. Consider the continuous formulas for G and H in Lemma 15 and Proposition 4. Since $H(1/2, 0) < 0$, fix $0 < \varepsilon < 1/4$ with $H(1/2, \varepsilon) < 0$. For this ε , $G(1/2, 0, \varepsilon) = -\varepsilon^2/2 < 0$. By continuity there is a fixed $0 < \delta < \min\{\varepsilon/3, 1/6\}$ such that, with $c_0 = 1/2 - \delta$ and $\zeta = \delta$,

$$G(c_0, \zeta, \varepsilon) < 0, \quad H(c_0, \varepsilon) < 0.$$

These choices also give $1/3 < c_0 < 1/2$, $0 < \zeta < c_0$, and $1 - \varepsilon < 1 - 3\delta = 2c_0 - \zeta$, as the two estimates require. All these constants are independent of n and p .

Put

$$k_n = \lceil c_0 n \rceil + 1, \quad r_0 = \lfloor (1 - \varepsilon)n \rfloor, \quad R_n = \lfloor k_n - 1 - \zeta n \rfloor.$$

We first prove the claim for a code C of dimension $k_n - 1$, and write $D = C^\perp$. Since $k_n - 1 \geq \zeta n$, the consequence of [Theorem 4](#) described in [Section 2.5](#) gives $\text{List}_D(R_n) \leq L_n = n^{c_\zeta}$ for a constant c_ζ and all sufficiently large n , uniformly over the code parameters; as ζ is fixed, $\log L_n = O(\log n) = o(n)$.

All averages $\Gamma_C(\mathbf{g}_A)$ on nonempty supports of size smaller than k_n vanish by [Lemma 7](#). For $k_n \leq r \leq r_0$, [Lemma 15](#) and $G(c_0, \zeta, \varepsilon) < 0$ give

$$\sum_{|A|=r} |\Gamma_C(\mathbf{g}_A)|^2 \leq \exp(-\beta_L n)$$

for a fixed $\beta_L > 0$ and all sufficiently large n , uniformly in r . For the remaining support sizes, $2(k_n - 1) \leq n < 3(k_n - 1)$ for large n , and [Proposition 4](#) gives

$$\frac{1}{2} \sum_{A \subseteq [n]: |A| > r_0} |\Gamma_C(\mathbf{f}_A)| \leq \exp(-\beta_H n)$$

for a fixed $\beta_H > 0$; here $(k_n - 1)/n \rightarrow c_0$, so continuity and $H(c_0, \varepsilon) < 0$ ensure that the rounding in k_n does not change the sign of the exponent for large n .

[Proposition 2](#) now yields

$$\text{SD}(\boldsymbol{\tau}(\mathbf{U}_C), \boldsymbol{\tau}(\mathbf{U}_{\mathbb{F}_p^n})) \leq \frac{1}{2} \sqrt{n \exp(-\beta_L n) + \exp(-\beta_H n)} \leq \exp(-\gamma n)$$

for some $\gamma > 0$ and all sufficiently large n ; the factor n counts the support sizes in the first sum and is absorbed by the exponential decay. None of the constants depends on the leakage maps. For a larger GRS code, the subcode obtained by restricting the polynomial degree to less than $k_n - 1$ has the dimension just treated, and [Remark 1](#) gives the same guarantee for every larger dimension.

Choose any fixed c_{bh} with $c_0 < c_{\text{bh}} < 1/2$. The code theorem follows because every GRS code of rate at least c_{bh} has dimension at least $\lceil c_0 n \rceil$. If a Shamir scheme has $k \geq c_{\text{bh}} n$, then for sufficiently large n , $k - 1 \geq c_{\text{bh}} n - 1 \geq c_0 n$, so its code dimension is also at least $\lceil c_0 n \rceil$, and [Lemma 1](#) proves [Theorem 1](#) with the same c_{bh} and leakage distance at most $2e^{-\gamma n}$. $\square$

Corollary 6 (An explicit constant). *The conclusions of [Theorems 1](#) and [8](#) hold with $c_{\text{bh}} = 1/2 - 10^{-14}$.*

Proof. Taking $\varepsilon = 6 \cdot 10^{-7}$, $\zeta = 2 \cdot 10^{-14}$, and $c_0 = 1/2 - 2 \cdot 10^{-14}$ gives $G(c_0, \zeta, \varepsilon) < -5.6 \cdot 10^{-14}$ and $H(c_0, \varepsilon) < -3.7 \cdot 10^{-7}$. These choices satisfy $0 < \zeta < c_0 < 1/2$, $1 - \varepsilon < 2c_0 - \zeta$, and $c_0 < c_{\text{bh}} < 1/2$, so the preceding proof applies. $\square$

7 AI Acknowledgments

The author used ChatGPT (Sol and Astra) as interactive research assistants throughout this work: to discuss and refine ideas and arguments, to check calculations and parameter choices, to locate related work, and to help draft and revise the text. Some mathematical suggestions made by the models were incorporated after the author's own verification. In particular, discussions with the models brought recent list-decoding and list-recovery results for Reed–Solomon codes to the author's attention and helped assess their applicability. The author supplied the research questions and the main ideas, evaluated and corrected the models' output, and takes full responsibility for the correctness of the results, the references, and the final presentation.

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 *Advances in Cryptology – CRYPTO 2019, Part II*, volume 11693 of *Lecture Notes in Computer Science*, pages 510–539. Springer, 2019.
- [AGG⁺25] Omar Alrabiah, Zeyu Guo, Venkatesan Guruswami, Ray Li, and Zihan Zhang. Random Reed–Solomon codes achieve list-decoding capacity with linear-sized alphabets. *Advances in Combinatorics*, 2025(8):1–39, 2025.
- [BCP⁺26] Joshua Brakensiek, Yeyuan Chen, Aaron Putterman, Zihan Zhang, and Kai Zhe Zheng. Algorithmic list decoding of Reed–Solomon codes up to capacity, 2026. arXiv:2609.08005, version 1.
- [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, Cham, 2018. Springer.
- [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), 2021. Article 10.
- [BGM23] Joshua Brakensiek, Sivakanth Gopi, and Visu Makam. Generic Reed–Solomon codes achieve list-decoding capacity. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, pages 1488–1501. ACM, 2023.
- [BHM⁺26a] Aniruddha Biswas, Jihun Hwang, Hemanta K. Maji, Ilya D. Shkredov, and Xiuyu Ye. Beyond all-or-nothing corruption: Additive secret sharing under Hamming-weight leakage, 2026. Manuscript.
- [BHM⁺26b] Aniruddha Biswas, Jihun Hwang, Hemanta K. Maji, Ilya D. Shkredov, and Xiuyu Ye. Energy estimation of the Hamming slice and its applications, 2026. arXiv:2609.08056.
- [BHMY26] Aniruddha Biswas, Jihun Hwang, Hemanta K. Maji, and Xiuyu Ye. Resilience of inner-product masking scheme against Hamming weight leakage. In *7th Conference on Information-Theoretic Cryptography (ITC 2026)*, volume 385 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 9:1–9:23. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2026.
- [BOGW88] Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing*, pages 1–10. ACM, 1988.
- [BS26] Katharina Boudgoust and Mark Simkin. Scale, round, break: Simple leakage attacks on secret sharing schemes. Cryptology ePrint Archive, Paper 2026/833, 2026.
- [CCD88] David Chaum, Claude Crépeau, and Ivan Damgård. Multiparty unconditionally secure protocols. In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing*, pages 11–19. ACM, 1988.
- [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 *2020 IEEE 61st Annual Symposium on Foundations of Computer Science*, pages 1226–1242. IEEE, 2020.
- [CKOS22] Nishanth Chandran, Bhavana Kanukurthi, Sai Lakshmi Bhavana Obbattu, and Sruthi Sekar. Short leakage resilient and non-malleable secret sharing schemes. In *Advances in Cryptology – CRYPTO 2022, Part I*, volume 13507 of *Lecture Notes in Computer Science*, pages 178–207. Springer, 2022.

- [CSTW24] Roni Con, Noah Shetty, Itzhak Tamo, and Mary Wootters. Repairing Reed–Solomon codes over prime fields via exponential sums. *IEEE Transactions on Information Theory*, 70(12):8587–8594, 2024.
- [DDF14] Alexandre Duc, Stefan Dziembowski, and Sebastian Faust. Unifying leakage models: From probing attacks to noisy leakage. In *Advances in Cryptology – EUROCRYPT 2014*, volume 8441 of *Lecture Notes in Computer Science*, pages 423–440. Springer, 2014.
- [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.
- [DKT26] Quang Dao, Scott Duke Kominers, and Justin Thaler. Reed–Solomon codes beyond Johnson: Efficient decoding and smaller cryptographic proofs, 2026. Cryptology ePrint Archive, Report 2026/2056.
- [DLM⁺26] Dean Doron, Tal Leonov, Jonathan Mosheiff, Henrique Navas, Nicolas Resch, and João Ribeiro. Discrepancy for random linear codes, 2026. arXiv:2606.24471, version 2.
- [DMRR25] Dean Doron, Jonathan Mosheiff, Nicolas Resch, and João Ribeiro. List-recovery of random linear codes over small fields. *IEEE Transactions on Information Theory*, 71(12):9548–9562, 2025.
- [FKS22] Asaf Ferber, Matthew Kwan, and Lisa Sauermann. List-decodability with large radius for Reed–Solomon codes. *IEEE Transactions on Information Theory*, 68(6):3823–3828, 2022.
- [FMM⁺24] 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, Part IV*, volume 14654 of *Lecture Notes in Computer Science*, pages 316–344, Cham, 2024. Springer.
- [FMM⁺26] Sebastian Faust, Loïc Masure, Elena Micheli, Hai Hoang Nguyen, Maximilian Orlt, and François-Xavier Standaert. IP masking with generic security guarantees under minimum assumptions, and applications. In *Advances in Cryptology – ASIACRYPT 2025, Part II*, volume 16246 of *Lecture Notes in Computer Science*, pages 544–575. Springer, 2026.
- [GG26] Rohan Goyal and Venkatesan Guruswami. Improved analysis of list-decodability of random linear codes: It’s all about counting constraints, 2026. ECC Report TR26-074.
- [GHK11] Venkatesan Guruswami, Johan Håstad, and Swastik Kopparty. On the list-decodability of random linear codes. *IEEE Transactions on Information Theory*, 57(2):718–725, 2011.
- [GHSZ02] Venkatesan Guruswami, Johan Håstad, Madhu Sudan, and David Zuckerman. Combinatorial bounds for list decoding. *IEEE Transactions on Information Theory*, 48(5):1021–1034, 2002.
- [GK18] Vipul Goyal and Ashutosh Kumar. Non-malleable secret sharing. In *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing*, pages 685–698. ACM, 2018.
- [GLS⁺24] Zeyu Guo, Ray Li, Chong Shangguan, Itzhak Tamo, and Mary Wootters. Improved list-decodability and list-recoverability of Reed–Solomon codes via tree packings. *SIAM Journal on Computing*, 53(2):389–430, 2024.
- [GM26] Utkarsh Gupta and Hessam Mahdaviifar. On the security of linear secret sharing with general noisy side-channel leakage. In Joan Daemen and Emmanuel Thomé, editors, *Advances in Cryptology – EUROCRYPT 2026, Part VII*, volume 16547 of *Lecture Notes in Computer Science*, pages 477–505, Cham, 2026. Springer.
- [Gow01] W. T. Gowers. A new proof of Szemerédi’s theorem. *Geometric and Functional Analysis*, 11(3):465–588, 2001.
- [GR08] 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.

- [GS99] Venkatesan Guruswami and Madhu Sudan. Improved decoding of Reed–Solomon and algebraic-geometry codes. *IEEE Transactions on Information Theory*, 45(6):1757–1767, 1999.
- [GT10] Ben Green and Terence Tao. Linear equations in primes. *Annals of Mathematics*, 171(3):1753–1850, 2010.
- [GW16] Venkatesan Guruswami and Mary Wootters. Repairing Reed–Solomon codes. In *Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing*, pages 216–226. ACM, 2016.
- [HMNY25] Jihun Hwang, Hemanta K. Maji, Hai H. Nguyen, and Xiuyu Ye. Leakage-resilience of Shamir’s secret sharing: Identifying secure evaluation places. In Niv Gilboa, editor, *6th Conference on Information-Theoretic Cryptography (ITC 2025)*, volume 343 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 3:1–3:20. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2025.
- [HS23] Charlotte Hoffmann and Mark Simkin. Stronger lower bounds for leakage-resilient secret sharing. In *Progress in Cryptology – LATINCRYPT 2023*, volume 14168 of *Lecture Notes in Computer Science*, pages 215–228, Cham, 2023. Springer.
- [HY26] Shuji Horinaga and Takashi Yamakawa. Worst-case quantum algorithm for optimal polynomial intersection beyond decoded quantum interferometry, 2026. arXiv:2607.14650.
- [Jer26] Fernando Granha Jeronimo. Algorithmic list decoding at capacity and optimal proximity gaps for Reed–Solomon codes, 2026. arXiv:2609.05870, version 1; ECCC Report TR26-169.
- [JMB26] Vahid Jahandideh, Bart Mennink, and Lejla Batina. A decomposition approach for evaluating security of masking. In *Advances in Cryptology – ASIACRYPT 2025, Part I*, volume 16245 of *Lecture Notes in Computer Science*, pages 580–612. Springer, 2026.
- [Jo26] Sunghyeon Jo. Efficient exact quantum sampling from the Sun–Wootters distribution for optimal polynomial intersection, 2026. arXiv:2607.16541.
- [KA26] 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 *Advances in Cryptology – ASIACRYPT 2025, Part VIII*, volume 16252 of *Lecture Notes in Computer Science*, pages 34–66. Springer, 2026.
- [Kas25] Dustin Kasser. An improvement upon the bounds for the local leakage resilience of Shamir’s secret sharing scheme. In Elette Boyle and Mohammad Mahmoody, editors, *Theory of Cryptography – TCC 2024, Part IV*, volume 15367 of *Lecture Notes in Computer Science*, pages 395–422, Cham, 2025. Springer. Proceedings of TCC 2024; publisher citation year 2025.
- [KJJ99] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In *Advances in Cryptology – CRYPTO 1999*, volume 1666 of *Lecture Notes in Computer Science*, pages 388–397. Springer, 1999.
- [KK23] Ohad Klein and Ilan Komargodski. New bounds on the local leakage resilience of Shamir’s secret sharing scheme. In Helena Handschuh and Anna Lysyanskaya, editors, *Advances in Cryptology – CRYPTO 2023, Part I*, volume 14081 of *Lecture Notes in Computer Science*, pages 139–170, Cham, 2023. Springer.
- [KMN22] Hamidreza Amini Khorasgani, Hemanta K. Maji, and Hai H. Nguyen. Secure non-interactive simulation from arbitrary joint distributions. In *Theory of Cryptography – TCC 2022, Part II*, volume 13748 of *Lecture Notes in Computer Science*, pages 378–407. Springer, 2022.
- [KMS19] 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*, pages 636–660. IEEE, 2019.
- [Koc96] Paul C. Kocher. Timing attacks on implementations of Diffie–Hellman, RSA, DSS, and other systems. In *Advances in Cryptology – CRYPTO 1996*, volume 1109 of *Lecture Notes in Computer Science*, pages 104–113. Springer, 1996.

- [Kop26] Swastik Kopparty. Recovering polynomials over finite fields from noisy character values, 2026. To appear in FOCS 2026. arXiv:2601.07137.
- [LS25] Ray Li and Nikhil Shagrithaya. Near-optimal list-recovery of linear code families. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM 2025)*, volume 353 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 53:1–53:14. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2025.
- [LW21] Ray Li and Mary Wootters. Improved list-decodability of random linear binary codes. *IEEE Transactions on Information Theory*, 67(3):1522–1536, 2021.
- [Man21] Freddie Manners. True complexity and iterated Cauchy–Schwarz, 2021. arXiv:2109.05731.
- [McD89] Colin McDiarmid. On the method of bounded differences. In J. Siemons, editor, *Surveys in Combinatorics, 1989*, volume 141 of *London Mathematical Society Lecture Note Series*, pages 148–188. Cambridge University Press, 1989.
- [MNPC⁺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 *Advances in Cryptology – EUROCRYPT 2021, Part II*, volume 12697 of *Lecture Notes in Computer Science*, pages 344–374, Cham, 2021. Springer.
- [MNPC⁺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 *3rd Conference on Information-Theoretic Cryptography (ITC 2022)*, volume 230 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 16:1–16:19. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2022.
- [MNPCW22] 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. IEEE, 2022.
- [MNPCY24] 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, Part IV*, volume 14654 of *Lecture Notes in Computer Science*, pages 286–315, Cham, 2024. Springer.
- [MPCSW21] 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, Cham, 2021. Springer.
- [Ngu24] Hai H. Nguyen. Towards breaking the half-barrier of local leakage-resilient Shamir’s secret sharing. In Leonid Reyzin and Douglas Stebila, editors, *Advances in Cryptology – CRYPTO 2024, Part V*, volume 14924 of *Lecture Notes in Computer Science*, pages 257–285, Cham, 2024. Springer.
- [Ngu25] 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, Part VIII*, volume 15608 of *Lecture Notes in Computer Science*, pages 64–93, Cham, 2025. Springer.
- [NS20] Jesper Buus Nielsen and Mark Simkin. Lower bounds for leakage-resilient secret sharing. In *Advances in Cryptology – EUROCRYPT 2020, Part I*, volume 12105 of *Lecture Notes in Computer Science*, pages 556–577, Cham, 2020. Springer.
- [O’D14] Ryan O’Donnell. *Analysis of Boolean Functions*. Cambridge University Press, 2014.
- [PR13] Emmanuel Prouff and Matthieu Rivain. Masking against side-channel attacks: A formal security proof. In *Advances in Cryptology – EUROCRYPT 2013*, volume 7881 of *Lecture Notes in Computer Science*, pages 142–159. Springer, 2013.

- [RV25] Nicolas Resch and S. Venkitesh. List recoverable codes: The good, the bad, and the unknown (hopefully not ugly), 2025. arXiv:2510.07597.
- [RW14] Atri Rudra and Mary Wootters. Every list-decodable code for high noise has abundant near-optimal rate puncturings. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, pages 764–773. ACM, 2014.
- [Sha79] Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.
- [ST20] Chong Shangguan and Itzhak Tamo. Combinatorial list-decoding of Reed–Solomon codes beyond the Johnson radius. In *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing*, pages 538–551. ACM, 2020.
- [Sud97] Madhu Sudan. Decoding of Reed Solomon codes beyond the error-correction bound. *Journal of Complexity*, 13(1):180–193, 1997.
- [SV19] Akshayaram Srinivasan and Prashant Nalini Vasudevan. Leakage resilient secret sharing and applications. In *Advances in Cryptology – CRYPTO 2019, Part II*, volume 11693 of *Lecture Notes in Computer Science*, pages 480–509. Springer, 2019.
- [SW26a] Yihang Sun and Mary Wootters. Improved local leakage resilience of Shamir secret sharing and worst-case optimal polynomial intersection, 2026. arXiv:2610.12357, version 1.
- [SW26b] Yihang Sun and Mary Wootters. On worst-case optimal polynomial intersection, 2026. arXiv:2604.09533.
- [TV06] Terence Tao and Van H. Vu. *Additive Combinatorics*, volume 105 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, 2006.
- [TYB17] Itzhak Tamo, Min Ye, and Alexander Barg. Optimal repair of Reed–Solomon codes: Achieving the cut-set bound. In *2017 IEEE 58th Annual Symposium on Foundations of Computer Science*, pages 216–227. IEEE, 2017.
- [Ven26] S. Venkitesh. Partial derandomization for leakage-resilient Shamir’s secret sharing over composite order fields. In Yevgeniy Dodis, editor, *7th Conference on Information-Theoretic Cryptography (ITC 2026)*, volume 385 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 12:1–12:19. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2026.

A List recovery with growing input lists

We prove [Theorem 4](#), keeping the dependence on the input-list size explicit. Interpolation gives a differential equation satisfied by every candidate. We then count its solutions using their initial coefficients and their agreement equations. We state the interpolation input from [\[Jer26\]](#) explicitly and give the remaining counting argument below.

The Hasse derivatives are defined by $P(X + U) = \sum_{j \geq 0} P^{[j]}(X)U^j$. Write $\deg_Y^{\text{tot}} Q$ for total degree in all the Y -variables.

Lemma 18 (Interpolation, from [\[Jer26, Proposition 3.7\]](#)). *Fix $0 < \zeta < 1$. There are constants $b_\zeta > 0$ and $t_\zeta \geq 1$ such that the following holds. Let $\alpha_1, \dots, \alpha_n \in \mathbb{F}_p$ be distinct, let $S_1, \dots, S_n \subseteq \mathbb{F}_p$, and put $M = \sum_i |S_i|$. If integers K, A, t satisfy*

$$2 \leq K \leq A \leq n, \quad t_\zeta \leq t < K, \quad \frac{A}{K-1} \geq \frac{1}{1-\zeta/2}, \quad M \leq b_\zeta(K-1)t^{\zeta/3},$$

then there is a nonzero $Q(X, Y_0, \dots, Y_t)$ with

$$\deg_X Q \leq t^3 n, \quad \deg_Y^{\text{tot}} Q \leq \left\lceil \frac{t^3 A}{K-1} \right\rceil,$$

such that every $P \in \mathbb{F}_p[X]$ of degree below K agreeing with the lists on at least A coordinates satisfies $Q(X, P, P^{[1]}, \dots, P^{[t]}) = 0$.

Apply the cited proposition with derivative order t , multiplicity t^3 , $\vartheta = \zeta/2$, and $\lambda = 2/3$. Its incidence exponent is $\lambda\vartheta = \zeta/3$. The monomial restrictions in [\[Jer26, Equations \(11\)–\(12\)\]](#) give the stated total Y -degree bound and $\deg_X Q < t^3 A \leq t^3 n$. The interpolation works over any coefficient field; no upper bound on p is required.

Lemma 19 (Counting solutions with many agreements). *Let $1 \leq h \leq n$, $t, B \geq 1$, and $D_0 \geq 0$ be integers, with $p > \max\{h-1, B\}$. Fix distinct $\alpha_i \in \mathbb{F}_p$, lists S_i with $M = \sum_i |S_i| \geq 1$, and a nonzero $Q \in \mathbb{F}_p[X, Y_0, \dots, Y_t]$ with $\deg_X Q \leq D_0$ and $\deg_Y^{\text{tot}} Q \leq B$. The number of polynomials $P \in \mathbb{F}_p[X]$ of degree below h satisfying*

$$Q(X, P, P^{[1]}, \dots, P^{[t]}) = 0, \quad |\{i : P(\alpha_i) \in S_i\}| \geq h$$

is at most

$$B^2(D_0 + B(h-1) + 1) \sum_{j=0}^t (ME)^j, \quad E = 8B(h+1)^2.$$

Proof. We make the recurrence and counting arguments of [\[Jer26, Lemmas 5.6–5.7 and 6.2\]](#) explicit. If $h \leq t$, there are at most M^h ordered choices of h agreements at distinct coordinates, each determining at most one polynomial P . This satisfies the claimed bound. Assume $h > t$, and work over the algebraic closure $\overline{\mathbb{F}_p}$.

We use the following standard form of Bézout's inequality (see [\[Jer26, Lemma 5.3\]](#)). The degree of an irreducible algebraic set is the number of points, counted with multiplicity, in a generic linear section of complementary dimension. A hypersurface defined by a nonzero polynomial of degree at most B has sum of component degrees at most B . Intersecting an irreducible component with a degree- E equation that does not vanish identically on it lowers its dimension and increases the sum of degrees by a factor of at most E . A zero-dimensional algebraic set has at most its sum of degrees many points.

If Q is independent of all Y -variables, there are no solutions. Otherwise let $s \leq t$ be its largest Y -index and put $H = \partial Q / \partial Y_s \neq 0$; nonvanishing follows from $B < p$. First count candidates with $H(X, P, \dots, P^{[s]}) \neq 0$. Fix a set of $D_0 + B(h-1) + 1$ distinct points $\alpha \in \overline{\mathbb{F}_p}$, independently of P . Since this polynomial has degree at most $D_0 + (B-1)(h-1)$, it is nonzero at one of these points. The algebraic closure allows this choice even when the number of points exceeds p .

Recovering the coefficients at a fixed α . Write $P(\alpha + U) = \sum_{q=0}^{h-1} c_q U^q$, with $c_q \in \overline{\mathbb{F}_p}$, put $\mathbf{c} = (c_0, \dots, c_s)$, and set $H_\alpha(\mathbf{c}) = H(\alpha, c_0, \dots, c_s)$. The identity

$$P^{[i]}(\alpha + U) = \sum_{q=i}^{h-1} \binom{q}{i} c_q U^{q-i}$$

shows that the coefficient of U^j , for $1 \leq j \leq h-1-s$, in the substituted equation is

$$\binom{s+j}{s} H_\alpha(\mathbf{c}) c_{s+j} + R_j(c_0, \dots, c_{s+j-1}) = 0.$$

Indeed, in $P^{[s]}(\alpha + U)$, the coefficient c_{s+j} first occurs as $\binom{s+j}{s} c_{s+j} U^j$. In every lower derivative $P^{[i]}$ it occurs at order $s+j-i > j$. Thus it contributes to the coefficient of U^j only through a single Y_s factor, with all other factors evaluated at $U=0$; the resulting multiplier is $H_\alpha(\mathbf{c})$. Since $s+j \leq h-1 < p$, the binomial coefficient is nonzero. On $H_\alpha \neq 0$, these equations recursively give

$$c_{s+j} = \frac{N_j(\mathbf{c})}{H_\alpha(\mathbf{c})^{2j-1}}, \quad \deg N_j \leq 4Bj^2.$$

Here and below, degrees are in the initial coefficients $\mathbf{c}$. To verify the bound, consider the noninitial factors $c_{s+a_1}, \dots, c_{s+a_v}$ in a monomial of R_j . Their orders satisfy $\sum_u a_u \leq j$, and the case $v=1, a_1=j$ is absent. Thus, for $j \geq 2$,

$$\sum_u (2a_u - 1) \leq 2j - 2, \quad \sum_u a_u^2 \leq j^2 - 2j + 2.$$

Using the previous recurrences and clearing denominators with H_α^{2j-2} gives

$$\deg N_j \leq B + 4B(j^2 - 2j + 2) + (2j - 2)B \leq 4Bj^2.$$

For $j=1$, directly $\deg N_1 \leq B$. This proves the bounds without any hidden dependence on B or t .

Counting the initial coefficients. The recurrences define a polynomial $P_\mathbf{c}$ of degree below h whenever $H_\alpha(\mathbf{c}) \neq 0$. Its first Taylor coefficients are $\mathbf{c}$, so this parametrization is injective. Every candidate at this α lies in

$$Q(\alpha, c_0, \dots, c_s) = 0, \quad H_\alpha(\mathbf{c}) \neq 0.$$

We may count all such initial vectors over $\overline{\mathbb{F}_p}$ satisfying the agreement equations, even if their polynomials do not solve the full differential equation. When this set is nonempty, its defining polynomial is nonzero, because its derivative in c_s is H_α . The hypersurface therefore has dimension at most s and sum of component degrees at most B .

Each of the M possible agreements becomes a polynomial equation after multiplication by H_α^{2h} :

$$H_\alpha(\mathbf{c})^{2h} (P_\mathbf{c}(\alpha_i) - b) = 0, \quad b \in S_i.$$

The preceding numerator bounds give

$$\deg_c[H_\alpha^{2h}(P_c(\alpha_i) - b)] \leq 4B(h-1)^2 + 2hB + 1 \leq E.$$

Any h satisfied agreements at distinct coordinates determine P_c , hence $\mathbf{c}$, uniquely where $H_\alpha \neq 0$. Let W be a positive-dimensional irreducible component through a candidate $\mathbf{c}$. Since $H_\alpha(\mathbf{c}) \neq 0$, the set $W \cap \{H_\alpha \neq 0\}$ is a nonempty open subset of W . If all of the candidate's agreement equations vanished identically on W , every point in this open subset would give the same polynomial P_c , hence the same initial vector $\mathbf{c}$, a contradiction. At least one agreement equation therefore cuts W properly. Repeating lowers the dimension to zero after at most s cuts. Hence every candidate at this α lies in a zero-dimensional component obtained from a component of $\{Q(\alpha, \mathbf{c}) = 0\}$ by at most s successive proper cuts with agreement equations. Components contained in $H_\alpha = 0$ can be discarded. For each ordered choice of equations, retain only proper intersections at each step. For j cuts there are at most M^j such choices, and Bézout bounds their contribution by BE^j for each choice. Hence

$$\#\{\text{candidates at this } \alpha\} \leq B \sum_{j=0}^s (ME)^j.$$

The remaining candidates satisfy $H(X, P, \dots, P^{[s]}) = 0$ identically. Repeat with H in place of Q . Each repetition lowers the total Y -degree without increasing the X -degree, so there are at most B stages. At each stage there are at most $D_0 + B(h-1) + 1$ choices of α from the fixed set. Summing the displayed bound over these stages and points proves the lemma. $\square$

Proof of Theorem 4. Write h for the code dimension. Scaling S_i by v_i^{-1} reduces GRS codes to ordinary RS codes. Fix lists of size at most ℓ and put $M = \sum_i |S_i| \leq n\ell$; if $M = 0$, there are no candidates. Set

$$A = h + \lceil \zeta n \rceil \leq n, \quad K = \lceil (1 - \zeta/2)A \rceil.$$

The agreement threshold A corresponds exactly to the radius $\lfloor n - h - \zeta n \rfloor$. For sufficiently large n , depending only on ζ (ensured by enlarging c_ζ),

$$K - h \geq \zeta n/2, \quad K - 1 \geq (1 - \zeta/2)A/2 \geq \zeta n/4, \quad \frac{A}{K-1} > \frac{1}{1 - \zeta/2}.$$

Choose $a_\zeta \geq t_\zeta$ with $b_\zeta \zeta a_\zeta^{\zeta/3} \geq 4$, and put $t = \lceil a_\zeta \ell^{3/\zeta} \rceil$. Then

$$M \leq n\ell \leq b_\zeta (K-1)t^{\zeta/3}.$$

Increasing c_ζ , the hypothesis $n \geq c_\zeta \ell^{9/\zeta}$ ensures $t < K$ and $5t^3 \leq n$. Apply Lemma 18; every candidate of degree below $h \leq K$ satisfies its equation, with

$$D_0 = t^3 n \leq n^2, \quad B = \left\lceil \frac{t^3 A}{K-1} \right\rceil \leq 5t^3 \leq n < p.$$

Thus Lemma 19 applies. Since $h \leq n < p$, $M \leq n^2$, and $E = 8B(h+1)^2 \leq 32n^3$, it gives

$$\#\{\text{candidates}\} \leq 3n^4(t+1)(32n^5)^t \leq n^{18t} \leq n^{c_\zeta \ell^{3/\zeta}},$$

after enlarging c_ζ once more. All constants depend only on ζ , and none depend on p . $\square$

B An alternative list-recovery calculation from DKT

We give a separate derivation of [Theorem 4](#) from Dao, Kominers, and Thaler (DKT) [[DKT26](#)]. Their Theorem G.2 states a list-recovery bound for fixed input-list size. The finite estimates in their Lemma 6.2 and the proof of Theorem 6.7 make the dependence on that size explicit, as follows.

Alternative proof of [Theorem 4](#). Write h for the code dimension and fix lists S_i of size at most ℓ . Scaling S_i by v_i^{-1} reduces GRS codes to ordinary RS codes. We count polynomials of degree below h with at least $A = h + \lceil \zeta n \rceil$ agreements; this is exactly the radius $\lfloor n - h - \zeta n \rfloor$ in the theorem.

Parameters. Set

$$\rho = \max\{h/n, \zeta/4\}, \quad a = \rho + \zeta/2.$$

Since $h \leq (1 - \zeta)n$,

$$\zeta/4 \leq \rho \leq 1 - 3\zeta/4, \quad a \leq 1 - \zeta/4 < 1, \quad h \leq \rho n, \quad an \leq A.$$

Choose the derivative order t , interpolation multiplicity s , and total degree bound B in the derivative variables by

$$t = \left\lceil \max \left\{ 519, \frac{1}{6} \left(\frac{320\ell}{9\zeta} \right)^{2/\zeta} \right\} \right\rceil, \quad s = \left\lceil 300t^2 \log(6t) \right\rceil, \quad B = \lceil 8s/\zeta \rceil.$$

Here t is denoted by d in DKT. Their Equation (83) gives

$$\begin{aligned} \Gamma(\rho, a, t) &= \frac{9\rho}{40} (6t)^{(a-\rho)/a} (1 + 1/t) \\ &\geq \frac{9\zeta}{160} (6t)^{\zeta/2} (1 + 1/t) \geq 2\ell(1 + 1/t). \end{aligned}$$

DKT's Lemma 6.2 bounds the finite interpolation ratio from below by $\Gamma(\rho, a, t)e^{-1677/10^6} > \ell$ when the local constraint rank is nonzero; when it is zero, the same lemma gives a nonzero interpolation space directly. Thus the interpolation condition in the proof of their Theorem G.2 holds for lists of size ℓ , with the displayed finite choice of s .

Length and characteristic. The interpolant in the proof of DKT's Theorem 6.7 has total degree at most $\lceil 2s/\rho \rceil \leq B$ in the derivative variables, and the construction requires

$$n \geq \left\lceil \max \left\{ \frac{t+1}{\rho}, \lceil 2s/\rho \rceil + 1, \frac{1}{1-\rho} \right\} \right\rceil.$$

Our choices give $t \geq \ell$, $s \geq t + 1$, and

$$\frac{t+1}{\rho} \leq \frac{4(t+1)}{\zeta} \leq B, \quad \frac{1}{1-\rho} \leq \frac{4}{3\zeta} < B, \quad \ell \leq B, \quad 4/\zeta < B.$$

Consequently $n \geq B + 2$ suffices. It also gives $p > n > \max\{h - 1, t, B\}$, satisfying the characteristic condition of DKT's Theorem G.2. Finally,

$$t = O_\zeta(\ell^{2/\zeta}), \quad B = O_\zeta(\ell^{4/\zeta} \log(2\ell)),$$

so the theorem's hypothesis $n \geq c_\zeta \ell^{9/\zeta}$ ensures $n \geq B + 2$ after increasing c_ζ .

List size. DKT's Theorem G.2, Equation (147), now gives

$$\begin{aligned} \#\{\text{candidate polynomials}\} &\leq B^2 \left(\frac{2\ell B}{a - \rho} \right)^t n^t = B^2 \left(\frac{4\ell B}{\zeta} \right)^t n^t \\ &\leq n^{4t+2} \leq n^{5t} \leq n^{c_\zeta \ell^{3/\zeta}}. \end{aligned}$$

The second line uses $B, \ell, 4/\zeta \leq n$ and $t \geq 2$; the last inequality follows by increasing c_ζ once more. All constants depend only on ζ , not on p . $\square$