On Leakage-resilient Secret Sharing

Hemanta K. Maji, Anat Paskin-Cherniavsky, Tom Suad, and Mingyuan Wang

Abstract. The security of cryptographic primitives typically relies on the storage of private secrets by each participant in a perfect manner. However, increasingly, side-channel attacks are demonstrating the pitfalls of assuming these cryptographic entities as opaque monolithic objects over the entire duration the primitive remains alive. Motivated by such concerns, there is a significant interest in revisiting well-established cryptographic primitives and their implementations to identify whether their security continues to hold in the presence of such side-channel attacks.

Although there are compilers to convert any secret sharing scheme into one that is robust to local leakage on each of their shares, it is not feasible to replace every instance of traditional secret sharing schemes in use with a leakage-resilient counterpart. Beyond efficiency considerations, there may be an appropriate structure in specific secret-sharing schemes that are fundamental to their usage in a particular context. For example, the use of a linear secret sharing scheme helps perform secure aggregation of statistics in parallel (for example, the sum of the private inputs of the participants) even in the presence of malicious parties. The reconstruction threshold of these secret sharing schemes determines the threshold of corruption permissible in the secure computation protocol; a lower reconstruction threshold implies a higher efficiency.

This paper makes a two-fold contribution. First, we continue to study the local leakage resilience of Reed-Solomon codes as initiated by Benhamouda, Degwekar, Ishai, and Rabin (2018). We improve their lower bound on the reconstruction threshold for Reed Solomon codes from $0.907n$ to $0.867n$ for one-bit leakage from each secret share, where n represents the number of parties receiving the secret shares.

Next, we explore whether, in the presence of local leakage, there is something inherent to maximum-distance separable (MDS) codes (Reed Solomon code is a particular example from this class of codes) that innately demands high reconstruction thresholds. Towards this investigation, we study random MDS codes and their necessary reconstruction threshold to remain resilient to a constant local leakage from each share. Given any $\delta \in (0, 1/2)$, we prove that most random MDS codes over suitably large fields with reconstruction threshold $(1/2 + \delta)n$ are resilient to constant local leakage.

In terms of techniques, both results rely on a Fourier-analytic approach to this problem. In particular, the second result relies on new and subtle analysis techniques for random MDS codes, which we believe shall be of independent interest.

Finally, we also contribute to the impossibility of designing secret-sharing schemes based on MDS codes over prime-order fields, where the dimension of the code is very small. If one insists on exponentially small indistinguishability among the shares generated by two different secrets,

then the dimension of the code needs to be $\Omega(n/\log n)$ even when the adversary obtains only $m = 1$ bit leakage from each of the shares and the field size is arbitrarily large.

Keywords: Random maximum distance separable codes, Local leakage resilience, Discrete Fourier analysis.

1 Introduction

Traditionally, we interpret participants in cryptographic protocols as impervious objects interacting with their computing devices remaining shielded from all external snooping or meddling. However, sophisticated side-channel attacks have increasingly proven this assumption false. Private keys, for example, may leak during storage or computation via surprisingly novel side-channel attacks [12]. The cryptographic protocols are typically not designed to be robust to such leakage. However, some primitives have turned out to be robust to such leakage attacks [4].

One such fundamental primitive is secret-sharing schemes. In the presence of *local leakage* from each secret share, our objective is to characterize the specific security achieved by these secret-sharing schemes. For example, if an adversary can perform one-bit local leakage from each party's secret share, then any linear secret-sharing scheme over fields of characteristic two is rendered entirely insecure; because an adversary who learns the last bit of each secret share can reconstruct the last bit of the secret as well.

Consequently, there are compilers to convert a linear secret sharing scheme into one that is resilient to m-bit local leakage from every share. However, the leakage-resilient counterpart may not be able to replace every instance of the original secret sharing scheme. The scenarios where one uses these secret-sharing schemes possibly rely on other salient features innate to them, for example, their additive nature, their ability to participate in cut-and-choose protocols, and their ability to efficiently correct errors during reconstruction. Typically, one may use linear secret sharing schemes (over large prime fields) for secure data aggregation (for example, performing the summation of private inputs of parties) in the presence of malicious participants. A reduction in the reconstruction threshold allows a smaller set of parties to recover the secret. Therefore, such a scheme can tolerate a higher number of (colluding) malicious parties in the secure computation protocol (as long as the reconstruction threshold is higher than the number of adversarial parties).

Consequently, there is a significant interest in constructing secret-sharing schemes with lower reconstruction threshold. However, ensuring local leakage resilience may require the reconstruction threshold to be high. This paper studies the reconstruction threshold necessary for some fundamental secret-sharing schemes.

1.1 Our Contribution

Our paper makes two contributions towards enhancing our understanding of local leakage resilience of secret-sharing schemes over prime-order fields. Briefly, in this setting, an adversary chooses an arbitrary vector of leakage functions with m bit output each to be applied to every share, and receives the output of these functions to a random sharing of a secret. Its goal is to distinguish between some pair of secrets with as large an advantage as possible. The m-leakage error of a scheme corresponds to the distinguishing advantage of the best such adversary. See [4] for more details and motivation on the setting.

In this paper, we focus on the easiest case for local leakage resilience of $m = 1$ bits of leakage, which is still far from well-understood. First, we study the local leakage resilience of the Shamir secret-sharing scheme.

Informal Theorem 1 (Shamir Secret Sharing: Reconstruction Threshold for One-bit Leakage) *Consider (n, t)-Shamir secret sharing scheme over a prime-order field $\mathbb{F}_p$, where t is the reconstruction threshold. If the reconstruction threshold satisfies $t \geq 0.867n$ then the leakage error for $m = 1$ is at most $2^{-\Omega(n)}$.*

Recently, Benhamouda, Degwekar, Ishai, and Rabin [4] proved that the threshold needs to be $t \geq 0.907n$.[1] The decrease in the reconstruction threshold for the Shamir's secret sharing scheme potentially helps increase the security of its applications; for example, in a verifiable secret sharing scheme implemented using a linear error-correcting code, the reconstruction threshold directly translates into the number of honest parties required to force adversarial parties into behaving honestly. So, a higher reconstruction threshold must need a large number of honest parties. Shamir's scheme is, in fact, a special case of a linear scheme for (n, t)-threshold access structure derived from a linear $[n + 1, t, \mathbb{F}_p]$-MDS codes via [17]. In fact, both our and [4]'s result holds for every such scheme derived from an MDS code as described above - hereafter referred to as a 'Massey scheme [17].'

Next, we proceed to exploring whether the structure of linear *maximum distance separable* (MDS) codes have some inimical property to local leakage resilience. Towards this objective, we explore the local leakage resilience of random linear MDS codes over prime-order fields of sufficiently large (yet still practical) size. We prove that, roughly, a random Massey scheme is m-leakage resilient for constant m for t arbitrarily close to $n/2$ with high probability.

Informal Theorem 2 (Random MDS Codes: Reconstruction Threshold for Constant Leakage) *Fix a constant $\delta \in (0, 1/2)$ and a constant leakage threshold m. Let n be the number of parties receiving the secret shares. Let C be*

[1] Our techniques can be used to improve the upper bounds for larger m appearing in [4] to a certain extent, but we explicitly state the results for $m = 1$ for simplicity and clarity. The eprint version of their paper [5] claims a smaller constant in Theorem 1.2, which is a consequence of an incorrect calculation. We have interacted with the authors to ensure that the constant mentioned here is an accurate reflection of their result.

a random MDS code over a prime-order field $\mathbb{F} = \mathbb{F}_p$ such that $|\mathbb{F}| = 2^{O_{\delta,m}(n)}$. Let Sh_C be the secret sharing scheme corresponding to the code C with reconstruction threshold t. An adversary can perform at most m-bit leakage from each party's secret share. If the reconstruction threshold of Sh_C is $t \geq (1/2+\delta)n$ then it is m-leakage resilient with leakage error $2^{-\Omega(n)}$ with overwhelming probability over the choice of C.

Our proof of the above theorem is non-constructive, making use of the probabilistic method (overcoming some technical hurdles to get reasonable parameters for the size of p). This leaves open the intriguing question of whether a threshold below $n/2$ is possible. A positive answer would open the door to "BGW-based" information-theoretic leakage resilient MPC with honest majority for general functions in the *plain model*. As we show below, new analysis techniques are required to resolve this question.

On applications to MPC. Leakage resilient MPC has been constructed in various setting based on leakage resilient secret sharing schemes constructed using general compilers as described above against local leakage with very large m, approaching share size. However, these compilers do not preserve linearity of the secret sharing scheme, for instance, incurring additional overhead on the resulting MPC scheme. Furthermore, it is important to note that achieving an LSSS for $t < 0.5n$ is not directly sufficient for general MPC. The LSSS should also be multiplicative, as is Shamir's scheme, but additional linear schemes have this property as well (see [6] for details). We hope that if we manage to prove that a random $[n, t, \mathbb{F}_p]$ linear code is an LSSS with high probability, we will be able to make a similar argument for random multiplicative additive codes.

Both positive results above proceed by undertaking a Fourier analytic approach to the problem of upper bounding the distinguishing advantage for m-bit local leakage from each party's secret share. In particular, our bound for Shamir secret sharing proceeds along the lines of [4]'s analysis, and we gain an extra advantage by more precise accounting for the 0-coordinates of the dual code $C^\perp$ of the Reed-Solomon code corresponding to Shamir's secret sharing. In a nutshell, this helps as these 0-coordinates correspond to the 0-Fourier coefficients of certain boolean functions related to the leakage functions, which are the largest (in absolute value) coefficient for each of these functions. For a given local leakage function vector, the leakage error is such that many large coefficients in a single codeword of $C^\perp$ make a large contribution to the overall achievable leakage error.

The analysis of the second result proceeds by carefully carrying out subtle accounting for the magnitude of Fourier coefficients. In some more detail, we observe that non-0 coefficients may be large as well, and rely on Parseval's identity to bound their number in each coordinates' leakage function. Then, we prove that with high probability over the choice of the code, only few codewords of $C^\perp$ have "many" coordinates corresponding to large Fourier coefficients simultaneously, so their overall contribution to the maximal achievable leakage advantage can not be very large.

We also extend the known lower-bounds for locally leakage-resilient secret sharing schemes that are constructed from MDS error-correcting codes. First, we observe that k, the dimension of the error-correcting code, cannot be very small relative to n, if an exponentially-small local leakage resilience of $\epsilon = 2^{-\Omega(n)}$ is to be achieved even for $m = 1$ bits of local leakage, for any field size p. In particular, we must have $k = \Omega(n/\log(n))$. Previously, a similar bound was known only for fields of size polynomial in n [19].

Informal Theorem 3 (Lower bound on k) *Let C denote an linear MDS code $[n+1, k, \mathbb{F}_p]$ such that the corresponding (k, n)-secret sharing scheme (Sh_C, Rec_C) has leakage resilience $\epsilon = 2^{-\Omega(n)}$ for $m = 1$ bits of leakage from each share, and any field size $p(n)$. Then, it must be the case that $k = \Omega(n/\log(n))$.*

In a somewhat different direction, we observe regarding natural hurdles to proving the result for $k < n/2$ using Fourier analytic techniques used in the LSS papers so far (including the current results). Consider an approach where we bound the Fourier coefficients using only their absolute values and rely on the Parseval's identity. Then, such approaches shall fail in meaningfully bounding the distinguishing advantage. We provide a (hypothetical) Fourier spectrum that is transparent to the class of techniques used in the line of work. In this example, the upper-bound for the distinguishing advantage diverges (to infinity) with the field size p. This indicates that additional properties of the Fourier spectrum of boolean functions should be used to improve the upper bounds, if at all.

1.2 Prior Works

Leakage-resilience has been a major topic in cryptography and there is a vast literature in this line of work (to name a few, [14, 9, 15, 13, 18, 8, 7]). Below, we only discuss those works that are closely related to this work.

In the field of code repairing, Guruswami and Wootters [11] showed that, for fields of characteristic 2, it might be possible to recover the secret by learning one-bit information from each share. Inspired by their work, Benhamouda, Degwekar, Ishai, and Rabin [4] initiated the study of leakage resilience of linear secret sharing schemes over a prime order field. Subsequently, Nielsen and Simkin [19] studied the upper bound on the amount of leakage. In particular, for (n, t)-Shamir-secret sharing, they showed that the amount of leakage from each share cannot exceed $\frac{t \log n}{n-t}$.

Recently, there also have been many works [10, 2, 16, 20, 1] trying to construct compilers that strengthen existing secret-sharing schemes with various guarantees of leakage-resilience.

2 Preliminaries

We denote by $\mathbf{I}(p) = -p \cdot \ln(p) - (1-p) \cdot \ln(1-p)$ the Shannon entropy of $0 < p < 1$. For $j \leq k$, where $(n-j)/n, j/n = \Theta(1)$ it follows from Stirling's

approximation that

$$\binom{n}{j} = (1 + o(1))\, 2^{\mathbf{I}(j/n)n} \tag{1}$$

By $\log(x)$ we refer to the base 2 logarithm unless stated otherwise.

Given two matrices $M_1 \in \mathbb{F}^{a_1 \times b}, M_2 \in \mathbb{F}^{a_2 \times b}$, we denote by $(M_1; M_2)$ the matrix resulting from concatenating M_2 under M_1, i.e., the matrix $\left[\begin{smallmatrix} M_1 \\ M_2 \end{smallmatrix}\right]$. We denote the rows (resp., columns) of M_1 by $Rows(M_1)$ (resp., $Cols(M_1)$), and the number of rows (resp., columns) by $rows(M_1)$ (resp., $cols(M_1)$). By default, vectors are row vectors (which are sometimes viewed as $1 \times a$ matrices). A submatrix corresponding to index sets of rows and columns X, Y respectively is denoted by $M[X, Y]$. In this context, '*' stands for the set of all rows or columns respectively, and abbreviate singleton sets via the element contained in it. We sometimes use $M[X]$ as an abbreviation for $M[X, *]$. Similarly, for a vector v, $v[I]$ denotes the vector resulting from projecting v to a subset I of its coordinates. For a set of vectors $\mathcal{G} \subseteq A^r$, and a set of indices $I \subseteq [r]$, we also denote $\mathcal{G}[I] = \{a[I] \mid a \in \mathcal{G}\}$.

For a set A, when there is no risk of confusion, we sometimes abuse notation, and view A as the uniform distribution over A.

2.1 Error correcting codes.

An $[n, k, \mathbb{F}_p]$ linear error-correcting code (ECC) C is a subspace of $\mathbb{F}_p^n$ of dimension k. A code is said to have distance d if every pair of distinct codewords have Hamming distance at least d. A generating matrix $G = (g_1; ...; g_n) \in \mathbb{F}_p^{n \times k}$ of C is a matrix whose columns constitute a basis of C. The dual code $C^\perp$ of a linear code C is $\{x \in \mathbb{F}_p^n \mid \forall c \in C, \langle x, c\rangle = 0\}$, and we denote the generating matrix of $C^\perp$ by $H = (h_1; \ldots; h_n) \in \mathbb{F}_p^{n \times (n-k)}$.

We say a code is Maximum Distance Separable (MDS) if $d = n - k + 1$. We will need a few well known equivalent formulations of MDS codes.

Claim. Let C be a linear $[n, k, \mathbb{F}_p]$ code. Then the following statements are equivalent:

- C is a linear $[n, k, \mathbb{F}_p]$-MDS code.
- $C^\perp$ is a linear $[n, k' = n - k, \mathbb{F}_p]$-MDS code.
- Every set of k rows of G are linearly independent.

2.2 Fourier Analysis

For our purposes, we only recall Fourier analysis for G which is the additive group of a finite field. Let $\mathbb{F} = \{0, \ldots, p-1\}$ be a field of order p, where p is prime. Let $f \colon \mathbb{F} \to \mathbb{C}$ be an arbitrary complex-valued function. For $z \in \mathbb{C}$, we let $\overline{z}$ denote the complex conjugate of z. We define the inner-product of two functions $f, g \colon \mathbb{F} \to \mathbb{C}$ as follows

$$\langle f, g\rangle := \frac{1}{p} \sum_{x \in \mathbb{F}} f(x)\overline{g(x)}. \tag{2}$$

A character of $\mathbb{F}$ is a homomorphism from the additive group $\mathbb{F}$ to the multiplicative group $\mathbb{C}^*$. The set of characters of $\mathbb{F}$, to which we refer to as $\widehat{\mathbb{F}}$ itself forms a group under coordinate-wise multiplications. In fact $\widehat{\mathbb{F}} = \{\chi_0, \chi_1, \ldots, \chi_{p-1}\}$ precisely satisfies $\chi_i(x) = \exp(2\pi\imath \cdot ix/p)$. The χ_i's form an orthonormal basis of $\mathbb{C}^p$. That is, we have:

$$\langle \chi_i, \chi_j \rangle = \begin{cases} 0, & \text{if } i \neq j \\ 1, & \text{if } i = j \end{cases}. \tag{3}$$

For $i \in \mathbb{F}$, we define the Fourier coefficient $\widehat{f}(i) := \langle f, \chi_i \rangle$. Furthermore, the mapping $f \mapsto \widehat{f}$ is a full-rank linear mapping. Parseval's identity states that

$$\langle f, f \rangle = \sum_{i \in \mathbb{F}} \widehat{f}(i)^2. \tag{4}$$

As [5], we follow the "standard" notation in additive combinatorics. In this notation, when working over $\mathbb{F}$, the Haar measure as in Equation 2, and the counting measure assigning 1 to each $i \in \widehat{\mathbb{F}}$ is used when working over $\widehat{\mathbb{F}}$. So, norms will be taken with respect to the underlying measure. Using this convention, we can compactly rephrase Parseval's identity as $\langle f, f \rangle = \langle \widehat{f}, \widehat{f} \rangle$.

Quoting for completeness, the lemma states that $\sum_{\ell_i} |\widehat{\mathbf{1}}_{\ell_i}(\alpha)| = 1$ if $\alpha = 0$ and is upper-bounded by the constant $c_m < 1$ otherwise (for every constant $m \geq 1$). For instance, $\lim_{p \to \infty} c_1 = 2/\pi$ when $m = 1$.

We will need the following technical Lemma from [5].

Lemma 1. *(Lemma 4.17, [5]) Let $\mathbf{L} \in \mathcal{L}_{m,n,p}$, where m is a constant. Then, for each $i \in [n]$, it holds that*

$$\begin{cases} \sum_{\ell_i} |\widehat{\mathbf{1}}_{\ell_i}(\alpha)| = 1 & \text{if } \alpha = 0 \\ \sum_{\ell_i} |\widehat{\mathbf{1}}_{\ell_i}(\alpha)| \leq c_m & \text{if } \alpha \neq 0 \end{cases}$$

for $c_m = \frac{2^m \sin(\pi/2^m)}{p \sin(\pi/p)}$. Furthermore, $c_m = 1 - \Omega_m(1)$, for sufficiently large p.[2]

2.3 Leakage resilient secret sharing

We consider the standard notion of perfect secret sharing schemes for general (monotone) access structures $\mathcal{A} \subseteq P([n])$ (specifying the qualified sets of parties) for some n parties. For the t-threshold access structure, where the qualified subsets $I \subseteq [n]$ are those of size at least t, we refer to secret sharing schemes implementing this access structure by (n, t)-secret sharing scheme. We will only consider linear secret sharing schemes over some finite field $\mathbb{F}_p$. Recall, that such a secret sharing scheme is a pair of algorithms (Sh, Rec), where $Sh : \mathbb{F}_p \to S_1 \times \ldots \times S_n$ is a randomized mapping taking a secret $s \in \mathbb{F}_p$ to a sequence of shares $\mathbf{sh} = (sh^1, \ldots, sh^n)$, where $S_i = \mathbb{F}_p^{\ell_i}$ for some $\ell_i \in \mathbb{N}^+$. For $I \subseteq [n]$, let us

[2] For instance, for $\lim_{p \to \infty} c_1 = 2/\pi$.

denote $sh^I = (sh^i)_{i\in I}$. Additionally, for each $a, b, s_0, s_1 \in \mathbb{F}_p$, and valid sharings $\mathbf{sh_0}, \mathbf{sh_1}$ respectively, it holds that $a\mathbf{sh_0} + b\mathbf{sh_1} \in support(Sh(as_0 + bs_1))$. A secret sharing scheme (not necessarily linear) implementing $\mathcal{A}$ is correct in the sense that for each $I \in \mathcal{A}$, and $\mathbf{sh} \leftarrow Sh(s)$, it holds that $Rec(I, sh^I) = s$ with probability 1 (over the random choices of Sh). It is private in the sense that for every pair of secrets s_0, s_1, $\mathbf{sh_0} \leftarrow Sh(s_0), \mathbf{sh_1} \leftarrow Sh(s_1)$, and every $I \notin \mathcal{A}$, $\mathsf{SD}\left(sh_0^I, sh_1^I\right) = 0$. See [3] for more details.

In this work, we study the leakage resilience of secret sharing schemes arising from linear codes in a natural way as in Massey's construction [17]. That is, given a linear $[n+1, k, \mathbb{F}_p]$ code C^+ with generating matrix $G^+ = (g_1^+; ...; g_{n+1}^+)$, the corresponding Massey (linear) n-party secret sharing scheme over $\mathbb{F}_p$ is defined as follows. $Sh(s)$ samples a random vector $\beta = (\beta_1, \ldots, \beta_k) \in \mathbb{F}_p^k$ conditioned on $(G^+ \cdot \beta^T)[n+1] = s$, and sets the share of party i to be $sh^i = \langle \beta, g_i^+ \rangle$. For $I \subseteq [n]$ such that $Rows(G^+[I])$ spans $G^+[n+1]$ (otherwise I is not qualified) via $\sum_{i\in I} \alpha_i G^+[i]$, $Rec(I, sh^I)$ outputs $s = \sum_{i\in I} \alpha_i sh^i$.[3]

We observe that the set of sharings of $s = 0$ is a linear $[n, k-1, \mathbb{F}_p]$ code, we denote by C. We denote the secret sharing above by (Sh_C, Rec_C).[4] We will mostly work with C^+ which are MDS codes. Note that in this case, C is also an MDS code, and (Sh_C, Rec_C) is a $(n, t = k-1)$-secret sharing scheme. Here and elsewhere, when we refer to [5], we refer to their eprint version [5]. We follow the definition of local leakage resilient secret sharing schemes as in [5], Definition 4.1. For completeness, we briefly recall this notion, restricted to Massey secret sharing schemes.

For n-party secret sharing schemes with $S_i = \mathbb{F}_p$, we let $\mathcal{L}_{m,n,p}$ denote the set of all functions $\mathbb{F}_p^n \to (\{0,1\}^m)^n$ (representing m-bit local leakage on each share of the n parties). We say the scheme (Sh_C, Rec_C) is a (m, ϵ)-Leakage resilient secret sharing scheme, if for all leakage function vectors $\mathbf{L} = (L_1, \ldots, L_n) \in \mathcal{L}_{m,n,p}$, and all pairs of secrets $s_0, s_1 \in \mathbb{F}_p$, we have $\mathsf{SD}\left(\mathbf{L}(Sh_C(s_0)), \mathbf{L}(Sh_C(s_1))\right) \leq \epsilon$.

For a party P_i, and $\ell_i \in \{0,1\}^m$, let $A_{i,\ell_i} = \{x \in \mathbb{F}_p | L_i(x) = \ell_i\}$. We denote by $\mathbf{1}_{A_{i,\ell_i}}(x) : \mathbb{F}_p \to \mathbb{C}$ the boolean function mapping x to 1 if $x \in A_{i,\ell_i}$ and to 0 otherwise. When i is clear from the context we sometimes abuse notation and let $\mathbf{1}_{\ell_i}$ denote $\mathbf{1}_{A_{i,\ell_i}}$.

For simplicity, our definition above corresponds to the setting with $\Theta = 0$ as considered in [5], where the adversary does not see any parties' shares, but only the output of the leakage function, so we exclude Θ from the notation. Our results can be translated into resilience for other values with a certain loss in parameters of Θ as explained in [5].

It is observed in [5] that given a leakage functions vector $\mathbf{L} = (L_1, \ldots, L_n)$, the *leakage advantage* $(\max_{\mathbf{L}\in\mathcal{L}_{\mathbf{m},\mathbf{n},\mathbf{p}}, s_0\in\mathbb{F}_p, s_1\in\mathbb{F}_p} \mathsf{SD}\left(\mathbf{L}(Sh(s_0)), \mathbf{L}(Sh(s_1))\right))$ of the scheme

[3] Massey schemes in fact capture exactly the linear secret sharing schemes where each party's share is a single field element.

[4] This will usually suffice for our purposes, although some of the information defined by G^+ is not stated explicitly. For instance, when C^+ is MDS, the (threshold) access structure implemented by the scheme is known from C.

is upper bounded by the statistical distance of $\mathbf{L}(X), \mathbf{L}(Y)$ for a certain pair of distributions X, Y.

Observation 1 *Let (Sh_C, Rec_C) denote an n-player Massey secret sharing scheme over $\mathbb{F}_p$. Fix an integer $m \leq \log(p)$. Then for m-bit local leakage functions vector $\mathbf{L} \in \mathcal{L}_{m,n,p}$, we have:* $\max_{\mathbf{L},s_0,s_1} \mathsf{SD}\left(\mathbf{L}(Sh(s_0)), \mathbf{L}(Sh(s_1))\right) \leq 2 \max_{\mathbf{L}} \mathsf{SD}\left(\mathbf{L}(C), \mathbf{L}(\mathbb{F}_p^n)\right)$.

We include a proof, since [5] only prove it for a special case.

Proof. This the case as for every $\mathbf{L}, s_0, s_1$,

$$\mathsf{SD}\left(\mathbf{L}(Sh(s_0)), \mathbf{L}(Sh(s_1))\right) \leq \mathsf{SD}\left(\mathbf{L}(C + v_0), \mathbf{L}(\mathbb{F}_p^n)\right) + \mathsf{SD}\left(\mathbf{L}(C + v_1), \mathbf{L}(\mathbb{F}_p^n)\right) \tag{5}$$

$$\leq 2 \max_{\mathbf{L}} \mathsf{SD}\left(\mathbf{L}(C), \mathbf{L}(\mathbb{F}_p^n)\right) \tag{6}$$

Here v_0, v_1 are some sharings of secrets s_0, s_1 respectively, both are multiples of the same vector v. The inequality 5 is due to the triangle inequality for the Euclidean space with the ℓ_1-norm. Indeed, by linearity of the scheme, $Sh_C(s_0)$ is uniformly distributed over $C + v_0$ for $v_0 = s_0 v$, for every $s_0 \in \mathbb{F}_p$. The inequality 6 follows from the claim that $\mathsf{SD}\left(\mathbf{L}(C + v_0), \mathbf{L}(\mathbb{F}_p^n)\right) = \mathsf{SD}\left(\mathbf{L}'(C), \mathbf{L}'(\mathbb{F}_p^n)\right)$ for $\mathbf{L}' = (L'_1, \ldots, L'_n)$, where $L'_j(x) = L_j(x + s_0 v[j])$ for each $j \in [n]$. In particular, $\mathsf{SD}\left(\mathbf{L}'(C), \mathbf{L}'(\mathbb{F}_p^n)\right) \leq \max_{\mathbf{L}} \mathsf{SD}\left(\mathbf{L}(C), \mathbf{L}(\mathbb{F}_p^n)\right)$. Finally, we get that $\mathsf{SD}\left(\mathbf{L}(C + v_0), \mathbf{L}(\mathbb{F}_p^n)\right) \leq \max_{\mathbf{L}} \mathsf{SD}\left(\mathbf{L}(C), \mathbf{L}(\mathbb{F}_p^n)\right)$. By similar reasoning it holds that $\mathsf{SD}\left(\mathbf{L}(C + v_1), \mathbf{L}(\mathbb{F}_p^n)\right) \leq \max_{\mathbf{L}} \mathsf{SD}\left(\mathbf{L}(C), \mathbf{L}(\mathbb{F}_p^n)\right)$, and the claim follows. [5]

We will need the following claim from [5] connecting $\mathsf{SD}\left(\mathbf{L}(C), \mathbf{L}(\mathbb{F}_p^n)\right)$ to evaluations of the $\widehat{\mathbf{1}}_{\ell_i}$ stemming from $\mathbf{L}$ on elements of $C^\perp$. See Lemma 4.18 [5] for proof details.

Claim. Let C be a linear $[n, k, \mathbb{F}_p]$ code and let $\mathbf{L} \in \mathcal{L}_{m,n,p}$ be an m-bit local leakage functions vector. Then,

$$\begin{aligned}
\mathsf{SD}\left(\mathbf{L}(C), \mathbf{L}(\mathbb{F}_p^n)\right) &= \sum_{\ell \in (\{0,1\}^m)^n} \left| \sum_{\alpha \in C^\perp \setminus \{0\}} \prod_{i=1}^{n} \widehat{\mathbf{1}}_{\ell_i}(\alpha_i) \right| \\
&= \sum_{\ell \in (\{0,1\}^m)^n} \left| \sum_{\beta \in \mathbb{F}_p^{n-t+1} \setminus \{0\}} \prod_{i=1}^{n} \widehat{\mathbf{1}}_{\ell_i}(\langle \beta, h_i \rangle) \right|
\end{aligned}$$

Remark 1. Both our positive results, those applying to all MDS-induced Massey schemes with given parameters n, t (Theorem 1) and those applying to a large fraction of such schemes (Theorem 2), can be extended to work for non-MDS schemes with a certain loss of parameters. The details are a subject of currently ongoing subsequent.

[5] The last step generalizes the reasoning of Claim 4.8.1 in [5]. for additive secret sharing schemes

3 Improved result for Shamir Secret Sharing and $m = 1$

As in [5], we prove that for every linear $[n, k, \mathbb{F}_p]$-MDS code C, the $(n, t = k)$-secret sharing scheme Sh_C induced by it is leakage resilient for sufficiently large t. We improve from about $t > 0.907 \cdot n$ in [5] (their full version), to a smaller constant for Shamir and the case of $m = 1$ and leakage advantage $\epsilon = 2^{-\Omega(n)}$. Our analysis improves the bound for larger constant m as well, but the bound $t = \Omega(n)$ quickly approaches 1 as m grows (similarly to [5] analysis, albeit slightly slower).

Theorem 1. *There exists a constant $\epsilon > 0$, so that for every linear $[n, k, \mathbb{F}_p]$-MDS code C, the corresponding Massey $(n, t = k)$-secret sharing scheme (Sh_C, Rec_C) allows for a leakage of a single bit ($m = 1$) and error $\leq 2^{-\epsilon n}$, for sufficiently large n and any $t \geq 0.867 \cdot n$.*

Because of space constraints, we shall only present a proof overview for this theorem. A complete proof is included in Appendix A.

Proof overview. We follow a Fourier-analysis based approach. We start with a description of [5]'s analysis, and explain where our analysis departs from it. In [5] they prove the following upper bound on the leakage advantage achieved by a leakage functions vector $\mathbf{L} = (L_1, \ldots, L_n)$ for a Massey scheme based on a linear $[n, k, \mathbb{F}_p]$-MDS code. Let H denote the generating matrix of $C^{\perp}$. Then

$$\mathsf{SD}\left(\mathbf{L}(C), \mathbf{L}(\mathbb{F}_p^n)\right) = \sum_{\ell \in (\{0,1\}^m)^n} \left| \sum_{\beta \in \mathbb{F}_p^k \setminus \{0\}} \prod_{i=1}^{n} \widehat{\mathbf{1}}_{\ell_i}(\langle \beta, h_i \rangle) \right| \tag{7}$$

Then, rearrange the sums and take an absolute value of all summands:

$$\mathsf{SD}\left(\mathbf{L}(C), \mathbf{L}(\mathbb{F}_p^n)\right) \leq \sum_{\beta \in \mathbb{F}_p^k \setminus \{0\}} \prod_{i=1}^{n} \left(\sum_{\ell_i} \left| \widehat{\mathbf{1}}_{\ell_i}(\langle \beta, h_i \rangle) \right| \right)$$

Recall that by Observation 1, $2 \max_{\mathbf{L}} \mathsf{SD}\left(\mathbf{L}(C), \mathbf{L}(\mathbb{F}_p^n)\right)$ upper bounds the leakage error of C (but does not necessarily lower-bounds it well). This step may lose on parameters, but greatly simplifies analysis.[6] To evaluate the above bound, one uses the fact that there are at most $k-1$ zero coordinates α_i in every codeword. Thus, the contribution of some β corresponds to

$$\Delta_\beta = \prod_{i \in [n]} \left(\sum_{\ell_i} \left| \widehat{\mathbf{1}}_{\ell_i}(\langle \beta, h_i \rangle) \right| \right) \tag{8}$$

Since every boolean function's Fourier coefficient $\widehat{f}(0)$ is the largest one (in absolute value), it makes sense to bound the number of such coefficients appearing together.

[6] Indeed, as we demonstrate in Section 5.2, taking absolute values is very likely sub-optimal.

Then, leaving out many details, they bound the contribution of any individual non-0 coefficients as $\max_{\alpha \neq 0} \widehat{f}(\alpha)$ by some constant $c_1 < 1$, resulting in a contribution bounded by c_1^k of each β.[7] However, bounding every contribution individually turns out to yield very weak bounds on $t = (1 - o(1))n$ (even for $m = 1$). Cauchy-Schwartz combined with Parseval's identity allows to obtain a better bound. Parseval's identity is useful here, as it bounds the ℓ_2-norm of each $\widehat{\mathbf{1}}_{\ell_i}$ by $|A_{i,\ell_i}|/p \leq 1$. The final bound takes advantage of the fact that $\widehat{f}(0)$ is not much larger than $\widehat{f'}(\alpha)$ for nice boolean functions f'. Then, they replace the $\mathbf{1}_{\ell_i}$'s involved by such nice functions, in a way that the expression for the bound can only increase, and bound this expression instead. The need for the replacement stems from the fact that nothing is assumed about the locations of the 0-coefficients in $H\beta^T$ (indeed, these locations vary for different β's).

Our improvement here stems by grouping the β's by the locations of $H\beta^T$'s 0-coefficients, and bounding the contribution of each group separately. Knowing the locations of 0's allows to use a bound on $\max_{\alpha \neq 0} \widehat{\mathbf{1}}_{\ell_i}(\alpha)$.

4 A result for random MDS code over a large fields

Next, we prove that for sufficiently large prime-order fields, 'almost all' Massey (n, t)-secret sharing schemes over $\mathbb{F}_{p(n)}$ for sufficiently large $p(n)$, are leakage-resilient for smaller values of t - all the way down to $t \geq (0.5 + \delta)n$, for every constant $\delta > 0$.

We will need a few technical linear-algebraic claims. The first one is a certain generalization of the rank method used in the communication complexity literature, stating that boolean matrices with a distinct rows have rank at least $\log a$ over the reals. We show that over any field, a matrix with a distinct rows where the entries in every column belong to a set of constant size, has rank at least $O(\log a)$.

Claim. Let $M \in \mathbb{F}_p^{a \times b}$ denote a matrix with distinct rows, where $a = 2^{cb}$ for some constants $c > 0$ and $\gamma \geq 2$. Assume further, that for every $y \in [b]$, there exists a set $V_y \subseteq \mathbb{F}_p$ of size γ such that for all $x \in [a]$ and $y \in [b]$ it holds that $M[x, y] \in V_y$. Then $rank(M) \geq \frac{c}{\log(\gamma)} b$.

Proof. Let r be the rank of M. Let $M' = (v_1; \ldots; v_r)$ be a submatrix of M, whose rows form a basis for the row space of M. Let I denote the (index) set of r independent columns of M'. w.l.o.g. assume that $I = [r]$. Let $M'' = M'[*, I]$. Then, every vector $u \in V_1 \times \ldots \times V_b \cap \mathbf{rowspan}(M)$ equals some $h \cdot M'$, where $h \cdot M'' \in V_1 \times \ldots \times V_r$. As M'' is invertible, h is of the form $h = u[I]{M''}^{-1}$ - that is, $u[I]$ uniquely determines h. As there are at most γ^r such $u[I]$-values,

$$|V_1 \times \ldots \times V_b \cap \mathbf{rowspan}(M)| \leq \gamma^r \tag{9}$$

So, to generate all (distinct) a rows of M, we would need $r \geq \frac{c}{\log(\gamma)} b$.

[7] The 'max' is enforced by the expression resulting from the Cauchy-Schwartz based expression in the sequel.

Let $C^\perp$ denote a linear $[n, k^\perp, \mathbb{F}_p]$-MDS code generated by the matrix $H = (h_1; \ldots; h_n)$. For a number γ and a vector $\mathbf{V} = (V_1, \ldots, V_n) \in \binom{\mathbb{F}_p}{\gamma}^n$ (each V_i is a set of γ field elements), let us denote

$$\mathrm{Bad}_{I,\mathbf{V}}(C^\perp) = \left\{ \beta \in \mathbb{F}_p^{k^\perp} | \forall i \in I \text{ and } \langle \beta, h_i \rangle \in V_i \right\},$$

and

$$\mathrm{Bad}_{\mathbf{V},\delta}(C^\perp) = \bigcup_{I \subseteq [n] \text{ of size } (1-\delta)n} \mathrm{Bad}_{I,\mathbf{V}}(C^\perp).$$

For a constant c we also denote

$$\mathrm{Bad}_{\delta,c} = \bigcup_{\mathbf{V} \in \binom{\mathbb{F}_p}{\gamma}^n} \left\{ C^\perp : \left| \mathrm{Bad}_{\mathbf{V},\delta}(C^\perp) \right| \geq c^n \right\}.$$

For a vector $v \in \mathbb{F}_p^n$ we write $v \in \mathbf{V}$ to mean that $v_i \in V_i$ for all $i \in [n]$.

The following lemma is a key lemma in our analysis. Roughly, it states that for a small γ, 'most' MDS codes with certain parameters do not have 'many' 'bad' codeword, such that 'many' coordinates out of each bad codeword fall in a set of size γ (sets may differ for different coordinates).

Lemma 2. *Let $p(n) \geq 2^n$ be a function returning primes, and let $c > 1$, $\gamma \geq 2, 0 < \delta < 1/2$ be constants. We further require that $\log c > \mathbf{I}(\delta)$. Consider the set $\mathcal{C}^\perp$ of linear $[n, k^\perp, \mathbb{F}_p]$-MDS codes $C^\perp$, where $\Omega(n) = k^\perp \leq (1-2\delta)n$, and the uniform probability distribution over $\mathcal{C}^\perp$. Then,*

$$Pr_{C^\perp \leftarrow \mathcal{C}^\perp} \left[C^\perp \in \mathrm{Bad}_{\delta,c} \right] = neg(n)$$

Proof. Fix a sufficiently large n and $p(n), c, \gamma, \delta, k^\perp$ as in the lemma. Consider some linear MDS code $C^\perp \in \mathrm{Bad}_{\delta,c}$. So, by definition $\mathrm{Bad}_{\delta,c}$, there exists some $\mathbf{V}$ such that $\mathrm{Bad}_{\mathbf{V},\delta}(C^\perp) \geq c^n$. By the assumption that $c > \mathbf{I}(\delta)$, there exists a set of coordinates I of size $(1-\delta)n$, so that $\mathrm{Bad}_{I,\mathbf{V}}(C^\perp)$ is of size $\tilde{\Omega}(2^{(\log(c)-\mathbf{I}(\delta))n})$. This follows by a simple averaging argument, and approximating the number of I's of size $(1-\delta)n$ using estimation 1 (note that $\mathbf{I}(1-\delta) = \mathbf{I}(\delta)$). Let c' be such that $\log(c') = 0.99(\log(c) - \mathbf{I}(\delta))$, which is by assumption a positive constant. For each I as above, denote the first $k^\perp$ coordinates in I by I'.

Note that for a vector $\mathbf{u} = H\beta^T$ for $\beta \in \mathrm{Bad}_{I,\mathbf{V}}(C^\perp)$, $\mathbf{u}[I']$ uniquely determines a β. This holds since $C^\perp$ is an MDS code, so $H[I']$ is invertible, and determines β. Consequently, to determine an element in $\mathrm{Bad}_{I,\mathbf{V}}(C^\perp)$, it suffices to specify it as a sequence of indices into the set $\mathbf{V}[I']$, where the set $\mathbf{V}[I']$ is ordered according to some fixed ordering (say, lexicographically).

We thus sometimes denote elements of $\mathrm{Bad}_{I,\mathbf{V}}(C^\perp)$ as indices $\mathbf{b} \in [\gamma]^{k^\perp}$, and sometimes explicitly as vectors $\beta \in \mathbb{F}_p^{k^\perp}$ determined by them (for a fixed $\mathbf{V}, I$). For an index $\mathbf{b}$, we denote the (unique) corresponding β by $\beta_{\mathbf{b}}$, and the vector $\mathbf{u} \in \mathbf{V}$ such that $\mathbf{u} = H\beta_{\mathbf{b}}^T$ by $\mathbf{V}_{I,\mathbf{b}}$. From now on, by $\mathbf{V}$ we implicitly refer to $\mathbf{V} \in \binom{\mathbb{F}_p}{\gamma}^n$ and by I we implicitly denote elements of $\binom{n}{(1-\delta)n}$ (with I' defined based on I as above).
Our plan consists of two steps:

1. Fix some $\mathbf{V}$ and I and $Bad' \subseteq [\gamma]^{k^\perp}$ of size c'^n for some c'. Prove the fraction of codes for which $Bad' \subseteq \mathrm{Bad}_{I,\mathbf{V}}(C^\perp)$ is very small. We refer to such codes $C^\perp$ as bad for $(\mathbf{V}, I, Bad')$.
2. Then, take a union bound over all possible $\mathbf{V}, I$ and possible choices of Bad' as above.

The above plan would already work as is, but would require an even larger, double exponential, $p(n)$. Instead, we observe that each $C^\perp$ that is bad for some $(\mathbf{V}, I, Bad')$, is also 'bad' for $(\mathbf{V}, I, B)$ for some $B \subseteq Bad'$ (which is always the case), where B is much smaller than Bad', and has a certain special property. Instead, we bound in step 1 the fraction of the set of $C^\perp$ bad for $(\mathbf{V}, I, B)$, for B's as above, and take a union bound over these in step 2. Here, we gain in step 2, since the number of triples is much smaller than before. As before, the bound for $(\mathbf{V}, I, B)$ we get in step 1 decreases with p, but now we can afford making $p(n)$ only single exponential, due to the smaller number of summands in 2.

We proceed to show how B is derived from Bad'.

Observation 2 *Let $(\mathbf{V}, I, Bad')$ where $Bad' \in \binom{[\gamma]^{k^\perp}}{c'^n}$ and $C^\perp$ bad for it. Then, there exists $B \subseteq Bad'$ of size $r = \theta(n)$, such that $\{\mathbf{V}_{I,\mathbf{d}} | \mathbf{d} \in B\}$ consists of linearly independent vectors. In particular, $C^\perp$ is bad for $(\mathbf{V}, I, B)$ (by definition of bad for $(\mathbf{V}, I, D)$ for some $D \subseteq [\gamma]^{k^\perp}$).*

Proof. We observe that $\left\{\mathbf{V}_{I,\mathbf{b}}[I]\right\}_{\mathbf{b} \in Bad'}$ has rank at least $r = \frac{\log(c')}{\log(\gamma)} n$. The observation follows immediately from applying Claim 4 to $M = (H\beta_1^T[I']; \ldots; H\beta_{c'^n}^T[I'])$ where $Bad' = \{\beta_1^T, \ldots, \beta_{c'^n}^T\}$ (indeed, note that $|rows(M)| = 2^{|cols(M)|\tilde{c}}$ for some constant $\tilde{c}$, since $cols(M) = k^\perp = \Theta(n)$, so the precondition of the claim holds). We set B to be a basis of M's rows.

Next, following our plan outlined above, we bound the fraction of $C^\perp$'s bad for a given $(\mathbf{V}, I, B)$, where B is as guaranteed by Claim 2 for $(\mathbf{V}, I, Bad')$ where $Bad' \in \binom{[\gamma]^{k^\perp}}{c'^n}$.

Claim. Let $\mathbf{V}, I, B$ where $B \in \binom{[\gamma]^{k^\perp}}{c'^n}$ and $D = \{\mathbf{V}_{I,\mathbf{d}} | \mathbf{d} \in B\}$ consists of linearly independent vectors. Then,

$$Pr_{C^\perp \leftarrow \text{linear } [n,k^\perp,\mathbb{F}_p]\text{-MDS codes}}\left[C^\perp \text{ is bad for } (\mathbf{V}, I, B)\right] = p^{-\Omega(n^2 \log p)} \quad (10)$$

Proof. We sample a uniformly $C^\perp$ by sampling its generating matrix H. As the code should be MDS, every set of $k^\perp$ rows of H form a basis for $rows(H)$. In particular, given I, $H[I']$ is a basis of its row set. For simplicity of notation, we assume w.l.o.g. that $I' = [1, \ldots, k^\perp]$. Then to determine the rest of $H[I]$ (which is the part we will be interested in), we should set the variables $\alpha_{i,j}$ in

$$h_i = \sum_{j \in [I']} \alpha_{i,j} h_j$$

for each $i \in I \setminus I'$.
In fact, we do not directly sample the matrix $H[I]$ to be consistent with and MDS code, but rather sample it according to the following distribution $\mathcal{D}_H$,

1. First sample $h_1, \ldots, h_{k^\perp}$ as random linearly independent vectors.
2. Sample the $\alpha_{i,j}$s as random independent element of $\mathbb{F}_p$.

We require that H satisfies the following constraints

1. Every $k^\perp$ rows in the resulting $H[I]$ are linearly independent (to actually obtain $H[I]$ consistent with an MDS code). Let us denote this event by E_1.
2. Every resulting row h_i is consistent with each $\mathbf{V}_{I,\mathbf{d}}$ for each $\mathbf{d} \in B$. Let us denote this event by E_2.

Let us explicitly state condition 2. For each $\mathbf{d} \in B$, and $i \in I \setminus I'$ we have

$$\sum_{j \in [I']} \alpha_{i,j} \mathbf{V}_{I,\mathbf{d}}[j] = \mathbf{V}_{I,\mathbf{d}}[i]. \tag{11}$$

That is, having fixed $H[I']$, $H[I \setminus I']$ satisfies a linear equation system of the form

$$M_B \alpha_i^T = v_i \tag{12}$$

where $M_B \in \mathbb{F}^{r \times k^\perp}$ is a full-rank matrix, whose rows are elements in $\left\{\mathbf{V}_{I,\mathbf{b}}[I']\right\}_{\mathbf{b} \in Bad'}$.
We are now ready to prove our theorem - in particular, note that M_B depends only on $\mathbf{V}, I, B$, rather than on the code itself. This follows as

$$\mathbf{V}_{I,\mathbf{d}}[i] = H\beta_{\mathbf{d}}^T[i] = H[i]\beta_{\mathbf{d}}^T$$

Making the same observation on the left side, together with $h_i = \sum_{j \in [I']} \alpha_{i,j} h_j$ implies Equation 11. We can restate Equation 11, as requiring that every α_i satisfies a linear equation system $M_B \alpha_i^T = \tilde{\mathbf{u}}_i$, where M_B is invertible (note that M_B is the same for all i).

Now we prove that the probability (over a uniform choice of all $\alpha_{i,j} \in \mathbb{F}_p$ and $H[I']$) that constraint 2 holds conditioned on constraint 1 holding, is $p^{-\Omega\left(\left(k^\perp\right)^2 \log(p)\right)}$. That is, we prove

$$Pr_{H \leftarrow \mathcal{D}_H}[C^\perp \in E_2 | C^\perp E_1] \leq$$

$$\frac{Pr_{H \leftarrow \mathcal{D}_H}[C^\perp \in E_2]}{Pr_{H \leftarrow \mathcal{D}_H}[C^\perp \in E_1]} = p^{-\Omega(n^2 \log p)} \tag{13}$$

To prove Equation 13, we bound the denominator and the numerator of the expression in 13 separately.

Claim. $Pr_{H \leftarrow \mathcal{D}_H}[C^\perp \in E_2] = p^{-\Omega(n^2 \log p)}$

Proof. Consider having chosen the first $h_1, \ldots, h_{k^\perp}$ in H (which are linearly independent). Next we move to picking the rows in $I \setminus I'$, represented in basis $h_1, \ldots, h_{k^\perp}$ for convenience (by choosing the $\alpha_{i,j}$'s). Consider the next $i \in I \setminus I'$ for which we pick h_i. By properties of linear transformations, and Equation 12, every such coefficient vector α_i, belongs to a coset $K + x_i$ of the right kernel K of M_B, for some $x_i \in \mathbb{F}_p^r$. Therefore, a randomly chosen such vector α_i only satisfies the above condition with probability $q = p^{-r}$, since $|K| = \mathbb{F}^{k^\perp - r}$ by the rank-nullity theorem. Note that this holds independently of the concrete choice of $H[I']$. Now, q equals $p^{-\Theta(n)}$, since indeed $r = \Theta(n)$ by Observation 2, and $k^\perp = \Theta(n)$ by the choice of δ. As the choice of each h_i is independent of the choice of h_j for every $i, j \in I \setminus I'$, the overall probability of the event E_2 is

$$\prod_{i \in I \setminus I'} p^{-r} = p^{-r((1-\delta)n - k^\perp)} = p^{-\Theta(n^2)} \tag{14}$$

Claim. $Pr_{H \leftarrow \mathcal{D}_H}[C^\perp \in E_1] > 1/2$ assuming $p(n) \geq 2^n$.

Proof. Consider the process of randomly choosing the rows in $H[I \setminus I']$, after picking $H[I']$ according to $\mathcal{D}_H$. We pick the rows h_i ($i \in I \setminus I'$) one by one. For each row h_i being picked, let us denote the set $\tilde{I}$ of rows picked so far (including $H[I']$ and excluding h_i). We require that the invariant, that every $k^\perp \times k^\perp$ submatrix of $H[\tilde{I} \cup \{i\}]$ remains invertible, is not broken upon choosing h_i. To keep the invariant, we need that every submatrix $\tilde{H}$ of $H[\tilde{I}]$ with $k^\perp - 1$ rows, remains invertible when appending h_i to it. In the worst case - when choosing the last row, we have at least a fraction

$$1 - \binom{n}{k^\perp}/p > 1/2 \tag{15}$$

of vectors in $\mathbb{F}_p^{k^\perp}$ to choose from. This follows by taking a union bound over all submatrices $\tilde{H}$ as above. Indeed, complementing each $\tilde{H}$ succeeds with probability $1 - 1/p$. Picking $p(n)$ large enough - $p(n) \geq 2^n$ suffices, keeps Equation 15 true.

Now, Equation 13, follows immediately from Claim 4 and Claim 4, which completes the proof of Claim 4.

Back to the proof of Lemma 2 (following step 2 of the plan), we take a union bound over all possible $\mathbf{V} \in \binom{\mathbb{F}_p}{\gamma}^n, I \in \binom{[n]}{(1-\delta)n}, B \in \binom{[\gamma]^{k^\perp}}{r}$. By a crude estimation, there exist at most

$$\binom{p}{\gamma}^n (2^n)(T^{k^\perp n}) = 2^{O((\log p + k^\perp)n)}$$

such triples. Thus, from Claim 4, the probability of $C^\perp$ being bad for (n, δ, c, γ) is upper bounded by

$$2^{\log p(O(n) - \Omega(n^2)) + O(n^2))} = 2^{n^2(\Omega(\log p) + O(1))} = 2^{\Omega(-n^3)} = neg(n),$$

where the last equality is implied by $\log p = \Omega(n)$. This concludes the proof of Lemma 2.

Theorem 2. *Let $0 < \delta < 1$ and $m \in \mathbb{N}^+$ be constants, where δ is sufficiently small*[8]*. Then for every field size function $p(n) \geq 2^n$ outputting primes, every sufficiently large n, and every $k \geq (0.5+\delta/2)n$, the Massey secret sharing scheme (Sh_C, Rec_C) corresponding to a random linear $[n, k, \mathbb{F}_p]$-MDS code C, allows for a local leakage of m bits from each party's secret share and leakage error $\leq 2^{-\Omega(n)}$ with overwhelming probability $1 - neg(n)$.*

Proof. **Proof overview.** We consider the hardest case of $k = (0.5+\delta/2)n$. Note that since the dual of a linear $[n, k, \mathbb{F}_p]$-MDS code C is a linear $[n, k^\perp = n-k = (0.5-\delta/2)n, \mathbb{F}_p]$-MDS code $C^\perp$, a random C as above (as considered in the theorem), can be uniformly sampled by uniformly sampling a linear $[n, k^\perp, \mathbb{F}_p]$-MDS code (and taking the dual $C = (C^\perp)^\perp$). Indeed, it will be more convenient to consider sampling of $C^\perp$ throughout the proof. We use the probabilistic method to prove that the $C^\perp$ based expression for $\mathsf{SD}\left(\mathbf{L}(C), \mathbf{L}(\mathbb{F}_p^n)\right)$ from Claim 2.3 is small for 'almost all' codes $C^\perp$. This will correspondingly imply the Theorem for almost all codes C as required.

Our proof proceeds by applying Lemma 2 to $\mathbf{V}$, where each V_i represents a set of values $\alpha_i \in \mathbb{F}_p$ corresponding to Fourier coefficients with 'large' (say ≥ 0.01) absolute value, of any of the local leakage functions $\widehat{\mathbf{1}}_{\ell_i}$.

On a high level, we prove that with overwhelming probability, for a random linear $[n, k^\perp, \mathbb{F}_p]$-MDS code $C^\perp$, not only that every non-0 codeword has less than $k^\perp$ 0-coordinates (which holds for every MDS code), but also, for every vector of boolean functions $(\mathbf{1}_{\ell_1}, \ldots, \mathbf{1}_{\ell_n})$, very few codewords $(\alpha_1, \ldots, \alpha_n)$ have a 'large' number of 'large' coefficients (say, coefficients larger than 0.01). That is, 0-coefficients $|\widehat{\mathbf{1}}_{\ell_i}(\alpha_i = 0)|$ are large in absolute value, and contribute a lot to the bound in Claim 2.3 if a lot of them 'come together' in a single codeword. Indeed the 0-coefficient is the largest in absolute value for all boolean functions f.

However, if possibly smaller but still large coefficients (including the 0-coefficient, and a few other that are function-specific) tend to 'come together' sufficiently often in a single codeword, this also pushes the bound up, albeit a bit slower. We can afford more such 'somewhat heavy' codewords, but not much more. In our previous analysis for Shamir, we gained a little by pinpointing the locations of the 0-coefficients exactly, instead of assuming the worst possible $(k^\perp)$ number of 0's in every codeword, as done in [5].

Here we go a step forward, and prove that for almost all $C^\perp$'s as above, for every leakage functions vector $\mathbf{L} \in \mathcal{L}_{m,n,p}$, only few sufficiently 'heavy' codewords $H \cdot \beta$ (where 'too many' of the coefficients $(\widehat{\mathbf{1}}_{\ell_1}(\alpha_1), \ldots, \widehat{\mathbf{1}}_{\ell_n}(\alpha_n))$ are large) exist. Details follow.

[8] The strange situation where we handle small $\delta > 0$ but not larger δ is an artifact of the proof of Lemma 2. A slightly more complicated proof would remove this restriction. See the full version for details.

A key technical observation our proof relies on, is that for any function $f : \mathbb{F}_p \to \{0,1\}$, there are very few large Fourier coefficients. More precisely, for constant (independent of p) ϵ let us define $\mathrm{Big}_{f,\epsilon} = \{\alpha \in \mathbb{F}_p | \widehat{f}(\alpha) \geq \epsilon\}$. Then we have,

Claim. Let p be a prime, and let $f : \mathbb{F}_p \to \{0,1\}$ be a boolean function. Then, for any $\epsilon \in (0,1]$, $|\mathrm{Big}_{f,\epsilon}| \leq \epsilon^{-2}$.

The above simple fact follows immediately from Parseval's identity,

$$\sum_{\alpha \in \mathbb{F}_p} \widehat{f}^2(\alpha) = |f^{-1}(1)|/p \leq 1$$

By Claim 2.3, we have:

$$\mathsf{SD}\left(\mathbf{L}(C), \mathbf{L}(\mathbb{F}_p^n)\right) = \sum_{\ell} \left| \sum_{\beta \in \mathbb{F}_p^k \setminus \{0\}} \prod_{i=1}^{n} \widehat{\mathbf{1}}_{\ell_i}(\langle \beta, h_i \rangle) \right|. \tag{16}$$

Rearranging, we obtain an upper bound

$$\mathsf{SD}\left(\mathbf{L}(C), \mathbf{L}(\mathbb{F}_p^n)\right) \leq \sum_{\beta \in \mathbb{F}_p^k \setminus \{0\}} \sum_{\ell} \left| \prod_{i=1}^{n} \widehat{\mathbf{1}}_{\ell_i}(\langle \beta, h_i \rangle) \right| \tag{17}$$

We now consider parameters $c, \delta, \epsilon, \gamma = \lceil 2^m \epsilon^{-2} \rceil$ for c, ϵ, δ to be determined later in a way satisfying the conditions of Lemma 2. Then, a random linear $[n, k^\perp, \mathbb{F}_p]$-MDS code $C^\perp$ satisfies the condition of Lemma 2 with overwhelming probability. Fix any such code $C^\perp$ and let H be its generating matrix.

Consider the sequence $\mathbf{V} = (V_1, \ldots, V_n) \subseteq \binom{\mathbb{F}_p}{\gamma}^n$ where $V_i = \bigcup_{\ell_i \in \{0,1\}^m} \mathrm{Big}_{\mathbf{1}_{\ell_i}, \epsilon}$ [9] is the set of all values of codeword coordinate α_i corresponding to a large coefficient for some function $\mathbf{1}_{\ell_i}$. [10]

Let $\mathrm{BadNon0}_{\mathbf{V},\delta} = \mathrm{Bad}_{\mathbf{V},\delta}(C^\perp) \setminus \{0\}$, $\mathrm{GoodNon0}_{\mathbf{V},\delta} = \mathbb{F}_p^{k^\perp} \setminus (\mathrm{BadNon0}_{\mathbf{V},\delta} \cup \{0\})$. For a set $I \subseteq [n]$, we denote

$$\mathrm{GoodNon0}_{\delta,I} = \{\beta \in \mathrm{GoodNon0}_{\mathbf{V},\delta} | \forall i \in I \ (H\beta^T[i] \notin V_i)\}$$

Next, we split the sum in Equation 17 applied to $C = (C^\perp)^\perp$ as follows,

$$\mathsf{SD}\left(\mathbf{L}(C), \mathbf{L}(\mathbb{F}_p^n)\right) \leq$$
$$\sum_{\beta \in \mathrm{GoodNon0}_{\mathbf{V},\delta}} \sum_{\ell} \left| \prod_{i=1}^{n} \widehat{\mathbf{1}}_{\ell_i}(\langle \beta, h_i \rangle) \right| + \sum_{\beta \in \mathrm{BadNon0}_{\mathbf{V},\delta}} \sum_{\ell} \left| \prod_{i=1}^{n} \widehat{\mathbf{1}}_{\ell_i}(\langle \beta, h_i \rangle) \right| \tag{18}$$

[9] Padding V_i to size γ arbitrarily

[10] In particular, the V_i's will always include 0. We could further limit the structure of V in Lemma 2, for instance, that V_i consists of pairs of values of the form $\alpha, -\alpha$, but as it seemingly does not help improve our bounds, we do not.

Let us bound each of the two summands separately. For a given $I \subseteq [n]$, let us denote by I_1, I_2 a partition of $[n] \setminus I$ into two subsets of equal size, in some predetermined way (depending only on I). We bound the contribution of $\mathrm{GoodNon0}_{\mathbf{V},\delta}$ first,

$$\sum_{\beta \in \mathrm{GoodNon0}_{\mathbf{V},\delta}} \sum_{\ell} \left| \prod_{i=1}^{n} \widehat{\mathbf{1}}_{\ell_i}(\langle \beta, h_i \rangle) \right| \leq$$

$$\sum_{I \in \binom{[n]}{\delta n}[n]} \sum_{\beta \in \mathrm{GoodNon0}_{\delta,I}} \sum_{\ell} \left| \prod_{i=1}^{n} \widehat{\mathbf{1}}_{\ell_i}(\langle \beta, h_i \rangle) \right| \leq \tag{19}$$

$$\tilde{O}(2^{\mathbf{I}(\delta)n}) \cdot \max_{I} \left(\sqrt{\sum_{\beta \in \mathrm{GoodNon0}_{\mathbf{V},\delta}} \prod_{i \in I_1} \Big(\sum_{\ell_i} |\widehat{\mathbf{1}}_{\ell_i}(\langle \beta, h_i \rangle)|^2 \Big)} \cdot \sqrt{\sum_{\beta \in \mathrm{GoodNon0}_{\mathbf{V},\delta}} \prod_{i \in I_2} \Big(\sum_{\ell_i} |\widehat{\mathbf{1}}_{\ell_i}(\langle \beta, h_i \rangle)|^2 \Big)} \cdot \right.$$

$$\left. \max_{\beta \in \mathrm{GoodNon0}_{\mathbf{V},\delta}} \prod_{i \in I} \Big(\sum_{\ell_i} |\widehat{\mathbf{1}}_{\ell_i}(\langle \beta, h_i \rangle)| \Big) \right) \leq \tag{20}$$

$$\tilde{O}(2^{\mathbf{I}(\delta)n}) \cdot \max_{I} \left(\sqrt{\sum_{\beta \in \mathbb{F}_p^{k^\perp}} \prod_{i \in I_1} \Big(\sum_{\ell_i} |\widehat{\mathbf{1}}_{\ell_i}(\langle \beta, h_i \rangle)|^2 \Big)} \cdot \sqrt{\sum_{\beta \in \mathbb{F}_p^{k^\perp}} \prod_{i \in I_2} \Big(\sum_{\ell_i} |\widehat{\mathbf{1}}_{\ell_i}(\langle \beta, h_i \rangle)|^2 \Big)} \cdot \right.$$

$$\left. \max_{\beta \in \mathrm{GoodNon0}_{\mathbf{V},\delta}} \prod_{i \in I} \Big(\sum_{\ell_i} |\widehat{\mathbf{1}}_{\ell_i}(\langle \beta, h_i \rangle)| \Big) \right) \leq \tag{21}$$

$$\tilde{O}(2^{\mathbf{I}(\delta)n}) \cdot \max_{I} \left(\sqrt{\prod_{i \in I_1} \Big(\sum_{\ell_i} \sum_{\alpha \in \mathbb{F}_p} |\widehat{\mathbf{1}}_{\ell_i}(\alpha)|^2 \Big)} \cdot \sqrt{\prod_{i \in I_2} \Big(\sum_{\ell_i} \sum_{\alpha \in \mathbb{F}_p} |\widehat{\mathbf{1}}_{\ell_i}(\alpha)|^2 \Big)} \cdot \right.$$

$$\left. \max_{\beta \in \mathrm{GoodNon0}_{\mathbf{V},\delta}} \prod_{i \in I} \Big(\sum_{\ell_i} |\widehat{\mathbf{1}}_{\ell_i}(\langle \beta, h_i \rangle)| \Big) \right) \leq \tag{22}$$

$$\tilde{O}(2^{\mathbf{I}(\delta)n}) \cdot (2^{2m}\epsilon)^{\delta n} = \tilde{O}(2^{(\mathbf{I}(\delta) + \delta(2m + \log \epsilon))n}) \leq 2^{-\epsilon' n} \tag{23}$$

for $\epsilon' > 0$ constant, for a proper choice of ϵ.

Inequality 19 follows by Cauchy–Schwarz. Let I be the set selected by the $\max_I$. Inequality 20 holds since each $\beta \in \mathbb{F}_p^{k^\perp}$ contributes a non-negative summand $\prod_{i \in I_1}(\ldots)$ (similarly I_2), and all values in the product are non-negative. Thus, adding β's beyond $\mathrm{GoodNon0}_{\mathbf{V},\delta}$ can only increase the expression's value. Inequality 21 holds since $|I_1|, |I_2| = (1-\delta)n/2 = (0.5-\delta/2)n$ and this equals exactly $k^\perp$. As our code is an MDS code, indeed going over all $\beta \in \mathbb{F}_p^{k^\perp}$, contributes exactly

$$\prod_{i \in I_1} \Big(\sum_{\alpha \in \mathbb{F}_p} |\widehat{\mathbf{1}}_{\ell_i}(\alpha)|^2 \Big),$$

for each fixed vector of $(\ell_i)_{i\in I_1}$. [11] A similar analysis holds for the other $\sqrt{\dots}$ and I_2.

The inequality 22 follows by observing that for every fixed ℓ_i, $\sum_{\alpha\in\mathbb{F}_p} |\widehat{\mathbf{1}}_{\ell_i}(\alpha)|^2 = \frac{|\mathbf{1}_{\ell_i}^{-1}(1)|}{p}$ by Parseval's identity, which is upper bounded by 1. So, summing over all 2^m of the ℓ_i values results in 2^m. This implies a $2^{m\delta n}$ bound on the product of the two squares. Now, each $i \in I$ satisfies $\sum_{\ell_i} |\widehat{\mathbf{1}}_{\ell_i}(\langle\beta, h_i\rangle)| \le 2^m\epsilon$. This is guaranteed to hold for every $\beta \in \text{GoodNon0}_{\mathbf{V},\delta}$, by the choice of $C^\perp$. Thus, the product of the two contributions is bounded by $2^{m\delta n}(2^m\epsilon)^{\delta n} = (2^{2m}\epsilon)^{\delta n}$.

The inequality 23 follows by choosing

$$\epsilon < 2^{-(\mathbf{I}(\delta)/\delta+2m)}, \tag{24}$$

so $\epsilon' > 0$ is indeed constant, which concludes the analysis of the bound on $\text{GoodNon0}_{\mathbf{V},\delta}$'s contribution.

The contribution of $\text{Bad}_{\setminus\{0\},(1-\delta)}$ requires somewhat more care. In particular, we need to show that every fixed β makes a contribution which is (much) smaller than 1. We have

$$\sum_{\beta\in\text{BadNon0}_{\mathbf{V},\delta}} \sum_{\ell} \left| \prod_{i=1}^{n} \widehat{\mathbf{1}}_{\ell_i}(\langle\beta, h_i\rangle) \right| \le$$

$$\sum_{\beta\in\text{BadNon0}_{\mathbf{V},\delta}} \prod_{i=1}^{n} \Big(\sum_{\ell_i} \left| \widehat{\mathbf{1}}_{\ell_i}(\langle\beta, h_i\rangle) \right| \Big) \le \tag{25}$$

$$c^n \cdot c_m^{(0.5+\delta/2)n} = 2^{n(\log c + (0.5+\delta/2)\log c_m)} \le 2^{-\epsilon' n} \tag{26}$$

for $\epsilon' > 0$ constant, for a proper choice of c and δ.

Inequality 25 holds since by Lemma 2, we have $|\text{Bad}_{\setminus\{0\},(1-\delta)}| \le c^n$. The second term in the expression $c^n \cdot c_m^{(0.5+\delta/2)n}$ follows from Lemma 1, applied to each $i \in [n]$, for each fixed $\beta \in \text{BadNon0}_{\mathbf{V},\delta}$. In our case, at most $(0.5-\delta/2)n$ (note that $k^\perp - 1 < (0.5-\delta/2)n$) coordinates $\langle\beta, h_i\rangle$ of the codeword $\alpha = H\beta^T$ equal 0, since $\text{BadNon0}_{\mathbf{V},\delta}$ does not contain $\beta = \mathbf{0}$ and our code $C^\perp$ is MDS. Therefore, the contribution of the non-0 coordinates (at least $(0.5+\delta/2)n$ coordinates) to the product accounts to at most $c_m^{(0.5+\delta/2)n}$.

The inequality 26 and everything so far that relies on Lemma 2 follows by choosing

$$c \le c_m^{-0.5} \quad \text{and} \tag{27}$$

$$c \ge 2^{\mathbf{I}(\delta)}. \tag{28}$$

[11] We should indeed make sure that the rounding works out and $(0.5-\delta/2)n$ is integral and even, because otherwise, if I_1 is smaller by 1 than $k^\perp$, every $\prod_{i\in I_1}\left(\sum_{\alpha\in\mathbb{F}_p} |\widehat{\mathbf{1}}_{\ell_i}(\alpha)|^2\right)$ would appear p times, causing the whole $\sqrt{\prod_{i\in I_1}(\dots)}$ expressing be multiplied by $\sqrt{p}$.

The requirement 27 suffices to ensure $\epsilon' > 0$, since $\delta > 0$. In particular, c satisfying requirement 27 can be chosen to be a constant strictly larger than 1, since c_m is a constant that falls in $(0, 1)$. The requirement 28 is to satisfy the precondition $\log(c) > \mathbf{I}(\delta)$ of Lemma 2. To satisfy requirement 28, we would need to set $\delta > 0$ to be a very small constant, and ϵ about $2^{-\Theta_m(\delta)}$ by requirement 24. This is inconsequential to the scheme's parameters in the current setting. [12]

5 Lower bounds

5.1 A Lower bound on $t(n)$

First, we extend the lower bound of Nielsen et al. [19] to the (hardest) setting of $m = 1$ bits of leakage and arbitrarily large p for the case of linear secret sharing schemes (which have the most applications, as for efficient leakage-resilient MPC). Recall their bound relies on p being relatively small - polynomial in n, as originally considered in [5]) - on the other hand, their bound is more general in the sense that it is not limited to linear schemes. More precisely, we have:

Theorem 3. *Let C^+ be an arbitrary $[n+1, k, \mathbb{F}_p]$ code, where $2k < p, k \leq n$. Let Sh_C be a Massey secret-sharing scheme corresponding to the linear error-correcting code C^+, as described in Section 2. Suppose the secret-sharing scheme Sh_C is ϵ-local leakage resilient against $\mathcal{L}_{m=1,n,p}$. Then $\epsilon \geq (\frac{1}{k})^{ck}$, where c is a universal positive constant.*

The statement in Theorem 3 holds for arbitrary n, p, and is not asymptotic in nature. One simple corollary (as n goes to infinity), restating as a bound on k.

Corollary 1. *Let C^+ be an arbitrary $[n+1, k, \mathbb{F}_p]$ code, where $2k < p, k \leq n$. Let Sh_C be a Massey secret-sharing scheme corresponding to the linear error-correcting code C^+. Let $\mathcal{L}_{m,n,p}$ be the set of all functions $\mathbb{F}_p^n \to (\{0,1\}^m)^n$ representing m-bit local leakage on each share of the n parties. Suppose the secret-sharing scheme Sh_C is $2^{-\Omega(n)}$-local leakage resilient against $\mathcal{L}_{m=1,n,p}$. Then $k = \Omega(\frac{n}{\log(n)})$.*

The proof of Theorem 3 is based on an argument similar to the one made in [5], when proving that n can not be too small, lower bounding the distinguishing advantage attainable for a constant n and additive scheme, by choosing a carefully designed $\mathbf{L}$. The extension of the statement and argument are indeed quite simple, and is brought here mostly for completeness.

Proof. We let G to be the generating matrix of C^+. Consider the shares given to minimal qualified parties $\mathbf{sh}[I]$. It is a well known fact about linear secret sharing schemes as above, that a set of parties can recover the secret iff the rows

[12] It only increases γ in Lemma 2, which only possibly affects the smallest n for which a code $C^\perp$ is guaranteed to exist.

set of $G[I]$ spans $G[n+1]$. As C^+ is of dimension k, we must have $|I| = k' \leq k$ - assume w.l.o.g. that $I = [k']$. Denote $G' = G[I, \cdot]$ and $G'' = G[n+1, \cdot]$ (which is a vector). Let $K = Kernel\big(span(\{G''\})\big)$. Let $\beta \in \mathbb{F}_p^{k'}$ be a vector such that $\beta \cdot G' = G''$. Then, from simple linear algebra, for a random sharing $\mathbf{sh_0}$ of secret $s = 0$, $\mathbf{sh_0}[I]$ is uniform over $C' = \{G' \cdot \mathbf{k}^T | \mathbf{k} \in K\} \subseteq \mathbb{F}_p^{k'}$. In particular, every $\mathbf{sh_0}[I]$ satisfies

$$\langle \beta, \mathbf{sh_0}[I] \rangle = \beta^T \cdot G'\mathbf{k} = G''\mathbf{k} = 0 \tag{29}$$

Where $\mathbf{k}$ is some element of K. Let $i \in [k']$ where $\beta_i \neq 0$ (it exists, as $G'' \neq 0$). Rewriting Equation 29, we get

$$\mathbf{sh_0}[i] = -\sum_{j \in [k'] \setminus \{i\}} \frac{\beta_j}{\beta_i} \mathbf{sh_0}[j] \tag{30}$$

Let $h_0 = \lfloor p/(2k') \rfloor$. For each $j \in [k'] \setminus \{i\}$, if $\beta_j \neq 0$, set $A_j = \{\frac{-\beta_i}{\beta_j} a | a \in \{0, \ldots, h_0 - 1\}\}$. Otherwise, set $A_j = \{0, \ldots, h_0 - 1\}$ (in fact, the latter can be an arbitrary sufficiently large set). For i let $A_i = \{0, \ldots, (p-1)/2\}$. Let $\mathbf{L} = (L_1, \ldots, L_n)$ where $L_n(\mathbf{sh_0}[i]) = 1$ if $sh_i \in A_i$, and $L_n(\mathbf{sh_0}[i]) = 0$ otherwise. Now, we observe

Claim. $Pr[\mathbf{sh_0}[I] \in A_1 \times \ldots \times A_{k'}] = \Pi_{j \in [k'] \setminus \{i\}} |A_j|/p$

Proof. To see this, we observe that for a random $x \in C'$, $x[I \setminus i]$ is uniform over $\mathbb{F}_p^{k'-1}$. Then, by definition of the A_j's, the probability of

$$Pr\left[\mathbf{sh_0}[I \setminus \{i\}] \in A_1 \times \ldots \times A_{i-1} \times A_{i+1} \ldots A_{k'}\right] = \Pi_{j \in [k'] \setminus \{i\}} |A_j|/p.$$

Now, conditioned on the event - $\mathbf{sh_0}[I \setminus \{i\}] \in A_1 \times \ldots \times A_{i-1} \times A_{i+1} \ldots A_{k'}$, $\mathbf{sh_0}[i] \in A_i$ by Equation 30, and the choice of the other A_js. Namely - with probability 1, $\mathbf{sh_0}[i]$ is the sum of at most $k' \leq k$ elements, each in $\{0, \ldots, h_0 - 1\}$, and the result follows.

To prove that $x[I \setminus i]$ is uniform over $\mathbb{F}_p^{k'-1}$, it suffices to prove $C'[I \setminus i]$ is indeed of dimension $k' - 1$. As P_I is a minterm of Sh_C, all rows in G' are linearly independent. Furthermore, as K is the right kernel of $span(G'')$, $span(G'')$ is the entire left kernel of K. Assuming for contradiction that $rowspan(G[I \setminus \{i\}, \cdot])$ has dimension $< k' - 1$, this implies the existence of a vector β' with $\beta'[i] = 0$, such that $\beta' \cdot G''$ is in the left kernel of K, and thus a multiple of G'', contradicting the fact that P_I is a minterm.

Substituting the sizes of the $|A_j|$'s in Claim 5.1, we have

$$\begin{aligned} Pr\Big[\mathbf{sh_0}[I] \in A_1 \times \ldots \times A_{k'}\Big] &\geq \Big(\lfloor p/(2k') \rfloor / p\Big)^{k-1} \\ &\geq \Big(1/(2k) - (1 - 1/2k)/p\Big)^{k-1} \\ &\geq \Big(1/k(2k+1)\Big)^{k} \geq 1/(3k)^{2k} \end{aligned} \tag{31}$$

Here the second transition is due to rounding issues, and the one before last transition uses the fact that $p \geq 2k+1$.[13]

On the other hand, for a random sharing of a random secret $s \in \mathbb{F}_p$, the distribution of $\mathbf{sh}[I]$ is uniform over $\mathbb{F}_p^{k'}$ (as now the randomness vector used by the sharing scheme is picked at random from $\mathbb{F}_p^k$), and G' is of full rank. Thus,

$$\begin{aligned} Pr\Big[\mathbf{sh}[I] \in A_1 \times \ldots \times A_{k'}\Big] &= Pr\Big[\mathbf{sh_0}[I] \in A_1 \times \ldots \times A_{k'}\Big]|A_i|/p \\ &\leq 0.5 Pr\Big[\mathbf{sh_0}[I] \in A_1 \times \ldots \times A_{k'}\Big] \end{aligned}$$

Thus, from Equation 31 we have $Pr\big[\mathbf{L}(\mathbf{sh_0})[I] = \mathbf{1}\big] - Pr\big[\mathbf{L}(\mathbf{sh})[I] = \mathbf{1}\big] \geq 0.5/(3k)^{2k}$. Therefor, by an averaging argument, there exists a secret s_1, such that $\mathsf{SD}\left(\mathbf{sh_{s_1}}[I], \mathbf{sh_0}[I]\right) \geq 0.5/(3k)^{2k}$. Therefore,

$$\begin{aligned} \mathsf{SD}\left(\mathbf{L}(\mathbf{sh_{s_1}})[I], \mathbf{L}(\mathbf{sh_0})[I]\right) &\geq 0.5\Big(Pr\big[\mathbf{L}(\mathbf{sh_0})[I] = \mathbf{1}\big] - Pr\big[\mathbf{L}(\mathbf{sh_{s_1}})[I] = \mathbf{1}\big]\Big) \\ &\geq 0.25/(3k)^{2k} \end{aligned}$$

Remark 2. In fact, it follows from the proof that the lower bound is slightly stronger than stated, if a minterm of size $k' \leq k$ exists. This is possible only in non-MDS codes.

5.2 Limitations of current techniques

In our proofs of Local Leakage Resilience so far, both for all MDS codes, and random MDS codes, we relied on bounding the *magnitudes* of the Fourier coefficient products in the expression for the bound in Equation 7. The bounds were based on combining Parseval's identity to classify the set of possible Fourier distributions of the boolean leakage functions with Cauchy-Shwartz, to obtain our bound on the *leakage advantage* of any function in $\mathcal{L}_{m,n,p}$. Here we prove that this approach is inherently limited to $t = (0.5 + \Omega(1))n$, and the main culprit is not in bounding the coefficients, but rather in replacing them with their asolute values, preventing vital cancellations. We achieve this by demonstrating an explicit subset $A \subseteq \mathbb{F}_p$ of density $\Omega(1)$, so that its characteristic function $\mathbf{1}_A$ has such coefficients, that replacing coefficients by their absolute values results in a bound of $\omega(1)$ on the Leakage error for $t = (0.5 - \Omega(1))n$ (that is, we use the precise coefficients, without using any bounds on them).

Let p be a prime, and let QR_p denote the set of quadratic residues modulo p, and NQR_p the set of quadratic non-residues (0 not included in either). Set $\mathbf{L} = (L_1, \ldots, L_n)$ be such that $L_i(x) = 1$ if x is in $QR_p^+ = QR_p \cup \{0\} = \{x \in \mathbb{F}_p | \exists y \in \mathbb{F}_p \text{ such that } x = y^2\}$, and 0 otherwise. For $a \in \mathbb{F}_p$, the quadratic Gaussian sum $g(a,p)$ is defined as $g(a,p) = \sum_{j=0}^{p-1} \chi_a(j^2)$. It is known that $g(1,p)$ satisfies:

[13] Taking the bound on p to be slightly larger, say $p \geq 3k$ would make the bound on the error about $(1/\Omega(k))^k$, but this is not very significant.

Fact 1

$$g(1,p) = \begin{cases} \sqrt{p}, & \text{if } p \equiv 1 \bmod 4 \\ \imath\sqrt{p}, & \text{if } p \equiv 3 \bmod 4 \end{cases} \tag{32}$$

We limit ourselves to $p \equiv 1 \bmod 4$ to simplify the proof of the following corollary on the Fourier coefficients of 1_{ℓ_i}. The (technical) reason for it is that -1 is a quadratic residue mod p in this case. It's not hard to prove that a similar result holds for $p \equiv 3$ mode 4.

Corollary 2. *Let $p \equiv 1 \bmod 4$. Then, for $\mathbf{L}$ above, for each $i \in [n], \ell_i \in \{0,1\}$ and $a \in \mathbb{F}_p$, we have:*

$$|\widehat{\mathbf{1}}_{\ell_i}(a)| = \begin{cases} 0.5p^{-0.5} \pm O(1)/p, & \text{if } a \neq 0 \\ 0.5 \pm O(1)/p, & \text{if } a = 0 \end{cases} \tag{33}$$

Proof. The corollary follows by:
(1) Calculating $\widehat{\mathbf{1}}_{QR_p^+}(1)$ by observing it equals $(g(1,p)+1)/2p$, which in any case has absolute value in the range $0.5p^{-0.5} \pm 1/(2p)$. Here we use the fact that -1 is in QR_p, so $\widehat{\mathbf{1}}_{QR_p^+}(1) = \widehat{\mathbf{1}}_{QR_p^+}(-1)$ (we need the fact that $-1 \in QR_p$, as $\widehat{\mathbf{1}}_{QR_p^+}(a) = \langle \mathbf{1}_{QR_p^+}, \chi_{-a} \rangle / p$, rather than $\widehat{\mathbf{1}}_{QR_p^+}(a) = \langle \mathbf{1}_{QR_p^+}, \chi_a \rangle / p$, as it appears in $g(a,p)$).
(2) Observing that for each $a \in QR_p$, it holds that $\widehat{\mathbf{1}}_{QR_p^+}(a) = \widehat{\mathbf{1}}_{QR_p^+}(1)$ (as QR_p is a subgroup of $\mathbb{Z}_p^*$), and for $a \in NQR_p$, it holds that $\widehat{\mathbf{1}}_{QR_p^+}(a) = -\widehat{\mathbf{1}}_{QR_p^+}(1) + 1/p$. Here we use the fact that for $a \neq 0$, it holds that

$$\widehat{\mathbf{1}}_A(a) = -\widehat{\mathbf{1}}_{\mathbb{F}_p \setminus A}(a) \tag{34}$$

and the observation that $a \cdot QR_p = NQR_p$ if $a \in NQR_p$.
(3) The corollary for $\mathbf{1}_{NQR_p} = \mathbf{1}_{\mathbb{F}_P \setminus QR_p^+}$ ($\ell_i = 0$) follows directly from 34.

Replacing all coefficients with their absolute values (and neglecting the $1/p$ additive terms) and substituting into Equation 7, we would get a bound of

$$\begin{aligned} \mathsf{SD}\left(\mathbf{L}(C), \mathbf{L}(\mathbb{F}_p^n)\right) &= \sum_{\ell} \left| \sum_{\alpha \in C^\perp \setminus \{0\}} \prod_{i=1}^{n} \widehat{\mathbf{1}}_{\ell_i}(\alpha_i) \right| \\ &\leq 2^m \cdot \left| \sum_{\alpha \in C^\perp \setminus \{0\}} \prod_{i=1}^{n} \widehat{\mathbf{1}}_{\ell_i=0}(\alpha_i) \right| && (35) \\ &\approx 2^m \cdot \prod_{i \in [n-k]} \Big(\sum_{\alpha_i \in \mathbb{F}_p} |\widehat{\mathbf{1}}_{\ell_i=0}(\alpha_i)| \Big) \Big(\frac{1}{2\sqrt{p}} \Big)^k && (36) \\ &= 2^m \cdot \Big(\frac{1}{2\sqrt{p}} \cdot p + O(1) \Big)^{n-k} \Big(\frac{1}{2\sqrt{p}} \Big)^k && (37) \\ &\approx 2^m \cdot \Big(\frac{1}{2} \Big)^n \sqrt{p}^{n-2k} \end{aligned}$$

Here $x \approx y$ means that $y = x \pm o(1)$. The expression in line 35 is the bound actually used by the analysis. Approximation 36 holds as instead of removing the contribution of the zero-codeword, we treat it as if the 0-Fourier coefficients have the same magnitude as other coefficients for the last k functions, which increases the bound only by a negligible fraction.

Equality 37 follows since adding the $O(1)$ to each of the first $n-k$ multiplicands, accounts for the 0-Fourier coefficient of each $\mathbf{1}_{\ell_i}$ that equals 0.5.

Note that indeed, for large enough p ($p \gg 2^n$), the above bound can be made an arbitrarily large integer for for $k = (0.5+\Omega(1))n$, . This is clearly not tight, as *all* leakage vectors' contributions together sum up to 1, as these are expressions for a statistical distance between a certain pair of probability distributions.

Remark 3. A simple calculation reveals that taking absolute values of Fourier coefficients as above, yields similar lower bounds for the true statistical distance between the leakage from sharings of any pair of secrets s_1, s_2 (rather than upper bounding it by a statistical distance between leakage from a sharing of $s = 0$ and leakage from a uniform distribution over $\mathbb{F}_p^n$, as we currently do).

We conclude that to get a true estimation of the leakage, additional ideas will be needed to get a more precise Fourier Analysis (or use a different approach altogether).

References

1. Divesh Aggarwal, Ivan Damgård, Jesper Buus Nielsen, Maciej Obremski, Erick Purwanto, João Ribeiro, and Mark Simkin. Stronger leakage-resilient and non-malleable secret sharing schemes for general access structures. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology – CRYPTO 2019, Part II*, volume 11693 of *Lecture Notes in Computer Science*, pages 510–539, Santa Barbara, CA, USA, August 18–22, 2019. Springer, Heidelberg, Germany. 5
2. Saikrishna Badrinarayanan and Akshayaram Srinivasan. Revisiting non-malleable secret sharing. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2019, Part I*, volume 11476 of *Lecture Notes in Computer Science*, pages 593–622, Darmstadt, Germany, May 19–23, 2019. Springer, Heidelberg, Germany. 5
3. Amos Beimel. Secret-sharing schemes: A survey. In Yeow Meng Chee, Zhenbo Guo, San Ling, Fengjing Shao, Yuansheng Tang, Huaxiong Wang, and Chaoping Xing, editors, *Coding and Cryptology - Third International Workshop, IWCC 2011, Qingdao, China, May 30-June 3, 2011. Proceedings*, volume 6639 of *Lecture Notes in Computer Science*, pages 11–46. Springer, 2011. 8
4. Fabrice Benhamouda, Akshay Degwekar, Yuval Ishai, and Tal Rabin. On the local leakage resilience of linear secret sharing schemes. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology – CRYPTO 2018, Part I*, volume 10991 of *Lecture Notes in Computer Science*, pages 531–561, Santa Barbara, CA, USA, August 19–23, 2018. Springer, Heidelberg, Germany. 2, 3, 4, 5
5. Fabrice Benhamouda, Akshay Degwekar, Yuval Ishai, and Tal Rabin. On the local leakage resilience of linear secret sharing schemes. Cryptology ePrint Archive, Report 2019/653, 2019. https://eprint.iacr.org/2019/653. 3, 7, 8, 9, 10, 16, 20, 27, 28, 29
6. Ronald Cramer, Ivan Damgård, and Ueli M. Maurer. General secure multi-party computation from any linear secret-sharing scheme. In Bart Preneel, editor, *Advances in Cryptology - EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000, Proceeding*, volume 1807 of *Lecture Notes in Computer Science*, pages 316–334. Springer, 2000. 4
7. Yevgeniy Dodis, Yael Tauman Kalai, and Shachar Lovett. On cryptography with auxiliary input. In Michael Mitzenmacher, editor, *41st Annual ACM Symposium on Theory of Computing*, pages 621–630, Bethesda, MD, USA, May 31 – June 2, 2009. ACM Press. 5
8. Stefan Dziembowski. Intrusion-resilience via the bounded-storage model. In Shai Halevi and Tal Rabin, editors, *TCC 2006: 3rd Theory of Cryptography Conference*, volume 3876 of *Lecture Notes in Computer Science*, pages 207–224, New York, NY, USA, March 4–7, 2006. Springer, Heidelberg, Germany. 5
9. Oded Goldreich and Rafail Ostrovsky. Software protection and simulation on oblivious rams. *J. ACM*, 43(3):431–473, 1996. 5
10. Vipul Goyal and Ashutosh Kumar. Non-malleable secret sharing. In Ilias Diakonikolas, David Kempe, and Monika Henzinger, editors, *50th Annual ACM Symposium on Theory of Computing*, pages 685–698, Los Angeles, CA, USA, June 25–29, 2018. ACM Press. 5
11. Venkatesan Guruswami and Mary Wootters. Repairing reed-solomon codes. In Daniel Wichs and Yishay Mansour, editors, *48th Annual ACM Symposium on*

Theory of Computing, pages 216–226, Cambridge, MA, USA, June 18–21, 2016. ACM Press. 5

12. J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten. Lest we remember: Cold boot attacks on encryption keys. In *Proceedings of the 17th USENIX Security Symposium, July 28-August 1, 2008, San Jose, CA, USA*, pages 45–60, 2008. 2
13. Yuval Ishai, Amit Sahai, and David Wagner. Private circuits: Securing hardware against probing attacks. In Dan Boneh, editor, *Advances in Cryptology – CRYPTO 2003*, volume 2729 of *Lecture Notes in Computer Science*, pages 463–481, Santa Barbara, CA, USA, August 17–21, 2003. Springer, Heidelberg, Germany. 5
14. Paul C. Kocher. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In Neal Koblitz, editor, *Advances in Cryptology – CRYPTO'96*, volume 1109 of *Lecture Notes in Computer Science*, pages 104–113, Santa Barbara, CA, USA, August 18–22, 1996. Springer, Heidelberg, Germany. 5
15. Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In Michael J. Wiener, editor, *Advances in Cryptology – CRYPTO'99*, volume 1666 of *Lecture Notes in Computer Science*, pages 388–397, Santa Barbara, CA, USA, August 15–19, 1999. Springer, Heidelberg, Germany. 5
16. Ashutosh Kumar, Raghu Meka, and Amit Sahai. Leakage-resilient secret sharing against colluding parties. In David Zuckerman, editor, *60th Annual Symposium on Foundations of Computer Science*, pages 636–660, Baltimore, MD, USA, November 9–12, 2019. IEEE Computer Society Press. 5
17. James L Massey. Some applications of code duality in cryptography. *Mat. Contemp*, 21(187-209):16th, 2001. 3, 8
18. Silvio Micali and Leonid Reyzin. Physically observable cryptography (extended abstract). In Moni Naor, editor, *TCC 2004: 1st Theory of Cryptography Conference*, volume 2951 of *Lecture Notes in Computer Science*, pages 278–296, Cambridge, MA, USA, February 19–21, 2004. Springer, Heidelberg, Germany. 5
19. Jesper Buus Nielsen and Mark Simkin. Lower bounds for leakage-resilient secret sharing. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10-14, 2020, Proceedings, Part I*, volume 12105 of *Lecture Notes in Computer Science*, pages 556–577. Springer, 2020. 5, 20
20. Akshayaram Srinivasan and Prashant Nalini Vasudevan. Leakage resilient secret sharing and applications. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology – CRYPTO 2019, Part II*, volume 11693 of *Lecture Notes in Computer Science*, pages 480–509, Santa Barbara, CA, USA, August 18–22, 2019. Springer, Heidelberg, Germany. 5

A Proof of Theorem 1

Let C be a linear $[n+1,k,\mathbb{F}_p]$-MDS code. The scheme induces a $(n,t=k)$ linear secret sharing scheme Sh_C as explained in Section 2. As mentioned in Section 2, the leakage advantage of the scheme is upper bounded by $\mathsf{SD}\left(\mathbf{L}(C),\mathbf{L}(\mathbb{F}_p^n)\right)$, which we bound next.

We start as in [5], in the proof of their Lemma 4.18. These (identical) calculations appear in the first three lines of the derivation below. Here I_1,I_2 are disjoint sets of coordinates of size $n-t+1$ each, and $I_3=[n]\setminus(I_1\cup I_2)$. For $\beta\in\mathbb{F}_p^{n-t+1}\setminus\{0\}$ we define $K_j=\{k'\in I_j|\langle\beta,h_{k'}\rangle=0\}$.

$$\mathsf{SD}\left(\mathbf{L}(C),\mathbf{L}(\mathbb{F}_p^n)\right)=\sum_{\ell}\left|\sum_{\alpha\in C^{\perp}\setminus\{0\}}\prod_{i=1}^{n}\widehat{\mathbf{1}}_{\ell_i}(\alpha_i)\right| \tag{38}$$

$$=\sum_{\ell}\left|\sum_{\beta\in\mathbb{F}_p^{n-t+1}\setminus\{0\}}\prod_{i=1}^{n}\widehat{\mathbf{1}}_{\ell_i}(\langle\beta,h_i\rangle)\right| \tag{39}$$

$$=\sum_{\ell}\left|\sum_{\beta\in\mathbb{F}_p^{n-t+1}\setminus\{0\}}\left(\prod_{i\in I_1}\widehat{\mathbf{1}}_{\ell_i}(\langle\beta,h_i\rangle)\right)\cdot\left(\prod_{i\in I_2}\widehat{\mathbf{1}}_{\ell_i}(\langle\beta,h_i\rangle)\right)\cdot\left(\prod_{i\in I_3}\widehat{\mathbf{1}}_{\ell_i}(\langle\beta,h_i\rangle)\right)\right| \tag{40}$$

$$\leq\sum_{\ell}\sum_{0\leq i+j+l\leq n-t+1}\sum_{\substack{\beta\in\mathbb{F}_p^{n-t+1}\setminus\{0\}\\ s.t.\ |K_1|=i,\\ |K_2|=j,\\ |K_3|=l}}\left|\left(\prod_{x\in I_1}\widehat{\mathbf{1}}_{\ell_x}(\langle\beta,h_x\rangle)\right)\cdot\left(\prod_{y\in I_2}\widehat{\mathbf{1}}_{\ell_y}(\langle\beta,h_y\rangle)\right)\cdot\left(\prod_{z\in I_3}\widehat{\mathbf{1}}_{\ell_z}(\langle\beta,h_z\rangle)\right)\right| \tag{41}$$

$$=\sum_{\ell}\sum_{0\leq i+j+l\leq n-t+1}\sum_{\substack{I_1'\subseteq I_1,|I_1'|=i\\ I_2'\subseteq I_2,|I_2'|=j\\ I_3'\subseteq I_3,|I_3'|=l}}\sum_{\substack{\beta\in\mathbb{F}_p^{n-t+1}\setminus\{0\}\\ s.t.\ K_1=I_1'\\ K_2=I_2'\\ K_3=I_3'}}\left|\left(\prod_{x\in I_1}\widehat{\mathbf{1}}_{\ell_x}(\langle\beta,h_x\rangle)\right)\cdot\left(\prod_{y\in I_2}\widehat{\mathbf{1}}_{\ell_y}(\langle\beta,h_y\rangle)\right)\cdot\left(\prod_{z\in I_3}\widehat{\mathbf{1}}_{\ell_z}(\langle\beta,h_z\rangle)\right)\right| \tag{42}$$

$$= \sum_{\ell} \sum_{0 \le i+j+l \le n-t+1} \sum_{\substack{I_1' \subseteq I_1, |I_1'|=i \\ I_2' \subseteq I_2, |I_2'|=j \\ I_3' \subseteq I_3, |I_3'|=l}} S_{I_1', I_2', I_3'} \tag{43}$$

Recall H is a matrix who's columns span $C^{\perp}$, and let h_j denote the j's row of H. Similarly to [5], the next step is to bound the last expression in the chain using the Cauchy-Schwarz inequality. The main innovation we introduce is splitting the sum in the expression into several sums as in Equation 41, and applying the bound separately to each sum. Note the implicit definition of $S_{I_1', I_2', I_3'}$ in the last line.
Let us denote

$$B_{i,j,l} = \left\{ \beta \in \mathbb{F}_p^{n-t+1} \setminus \{0\} \middle| \, |K_1| = i, |K_2| = j, |K_3| = l \right\}.$$

We further denote

$$B_{I_1', I_2', I_3'} = \left\{ \beta \in B_{i,j,l} \middle| I_1' = K_1, I_2' = K_2, I_3' = K_3 \right\}.$$

Rewriting the above inequality, we get

$$\begin{aligned}
&\mathsf{SD}\left(\mathbf{L}(C), \mathbf{L}(\mathbb{F}_p^n)\right) \\
&\le \sum_{\ell} \sum_{0 \le i+j+l \le n-t+1} \sum_{\substack{\beta \in B_{i,j,l} \\ s.t. \ |K_1|=i, \\ |K_2|=j, \\ |K_3|=l}} \left| \left(\prod_{x \in I_1} \widehat{\mathbf{1}}_{\ell_x}(\langle \beta, h_x \rangle) \right) \cdot \left(\prod_{y \in I_2} \widehat{\mathbf{1}}_{\ell_y}(\langle \beta, h_y \rangle) \right) \right| \cdot \\
&\qquad \max_{\beta \in B_{i,j,l}} \left| \prod_{z \in I_3} \widehat{\mathbf{1}}_{\ell_z}(\langle \beta, h_z \rangle) \right| \qquad (44) \\
&\le \sum_{\ell} \sum_{0 \le i+j+l \le n-t+1} \sum_{\substack{I_1' \subseteq I_1, |I_1'|=i, \\ I_2' \subseteq I_2, |I_2'|=j, \\ I_3' \subseteq I_3, |I_3'|=l}} \sqrt{\sum_{\beta \in B_{I_1', I_2', I_3'}} \prod_{x \in I_1} |\widehat{\mathbf{1}}_{\ell_x}(\langle \beta, h_x \rangle)|^2} \cdot \qquad (45) \\
&\qquad \sqrt{\sum_{\beta \in B_{I_1', I_2', I_3'}} \prod_{y \in I_2} |\widehat{\mathbf{1}}_{\ell_y}(\langle \beta, h_y \rangle)|^2} \cdot \max_{\beta \in B_{i,j,l}} \left| \prod_{z \in I_3} \widehat{\mathbf{1}}_{\ell_z}(\langle \beta, h_z \rangle) \right|
\end{aligned}$$

The inequality 44 is simply due to splitting the sum according to the *exact* locations of 0 coordinates in $H\beta^T$. The inequality 45 is by Cauchy-Schwartz, where the maximum is taken over a larger set than needed, which clearly only increases the bound.

To continue, we will use the following technical observation.

Observation 3 *For sets A_1, A_2 with $|A_1|+|A_2| = p$, we have $\sum_{i\in[2]} \sqrt{\sum_{\alpha\neq 0} |\widehat{\mathbf{1}}_{A_i}(\alpha)|^2} \leq 1$.*

Proof. By Parseval's identity, we have $||\widehat{\mathbf{1}}_{A_i}||_2^2 = ||\mathbf{1}_{A_i}||_2^2 = \frac{|A_i|}{p}$. Let us denote $q_i = \frac{|A_i|}{p}$. Thus

$$\sum_{\alpha\neq 0} |\widehat{\mathbf{1}}_{A_i}(\alpha)|^2 = q_i - q_i^2$$

as $|\widehat{\mathbf{1}}_{A_i}(0)| = q_i$. Thus, we have

$$\sum_{i=1}^{2} \sqrt{\sum_{\alpha\neq 0} |\widehat{\mathbf{1}}_{A_i}(\alpha)|^2} = \sqrt{q_1 - q_1^2} + \sqrt{q_2 - q_2^2} \tag{46}$$

We denote $g(x) = \sqrt{x(1-x)}$ and observe that the expression in Equation 46 equals $g(q_1) + g(1-q_1) = 2g(q_1)$ (as $q_2 = (1-q_1)$ and $g(q) = g(1-q)$). The maximum of $2g(q_1)$ in $[0,1]$ is easily seen to be obtained at $q_1 = 0.5$, and equal 1. [14]

Let us bound the contribution of the portion a single I_1', I_2', I_3' contributed to the expression in Equation 45 - we denote this contribution by $S'_{I_1',I_2',I_3'}$.

$$S'_{I_1',I_2',I_3'}$$

$$= \sum_{\ell} \sqrt{\sum_{\beta\in B_{I_1',I_2',I_3'}} \prod_{x\in I_1} |\widehat{\mathbf{1}}_{\ell_x}(\langle\beta, h_x\rangle)|^2} \cdot \sqrt{\sum_{\beta\in B_{I_1',I_2',I_3'}} \prod_{y\in I_2} |\widehat{\mathbf{1}}_{\ell_y}(\langle\beta, h_y\rangle)|^2} \cdot \tag{47}$$
$$\max_{\beta\in B_{i,j,l}} \left| \prod_{z\in I_3} \widehat{\mathbf{1}}_{\ell_z}(\langle\beta, h_z\rangle) \right|$$

$$\leq \sum_{\ell} \sqrt{\prod_{x\in I_1'} (\frac{|A_x|}{p})^2 \cdot \prod_{x\in \text{free}_1} \left(\sum_{\alpha\in\mathbb{F}_p\setminus\{0\}} |\widehat{\mathbf{1}}_{\ell_x}(\alpha)|^2 \right) \cdot \prod_{x\in I_1\setminus(\text{free}_1\cup I_1')} \max_{\alpha\in\mathbb{F}_p\setminus\{0\}} |\widehat{\mathbf{1}}_{\ell_x}(\alpha)|^2} \cdot \tag{48}$$
$$\sqrt{\prod_{y\in I_2'} (\frac{|A_y|}{p})^2 \cdot \prod_{y\in \text{free}_2} \left(\sum_{\alpha\in\mathbb{F}_p\setminus\{0\}} |\widehat{\mathbf{1}}_{\ell_y}(\alpha)|^2 \right) \cdot \prod_{y\in I_2\setminus(\text{free}_2\cup I_2')} \max_{\alpha\in\mathbb{F}_p\setminus\{0\}} |\widehat{\mathbf{1}}_{\ell_y}(\alpha)|^2}.$$

[14] Part of our gain comes from a more careful analysis for the case of two sets. Here we compute the maximum exactly instead of using concavity arguments to bound it, as is done in [5]. This is not surprising, because they did not attempt to optimize bounds for the case of $m = 1$.

$$\prod_{z\in I_3'}\left(\frac{|A_z|}{p}\right)\cdot\prod_{z\in I_3\setminus I_3'}\left|\max_{\alpha\in\mathbb{F}_p\setminus\{0\}}\widehat{\mathbf{1}}_{\ell_z}(\alpha)\right|$$

Therefore we have

$$\mathsf{SD}\left(\mathbf{L}(C),\mathbf{L}(\mathbb{F}_p^n)\right)\leq\sum_{\substack{(I_1',I_2',I_3')\\ s.t.\ \forall j\in[3]\ I_j'\subseteq I_j,\\ |\bigcup_{j\in[3]}I_j'|\leq n-t+1}}S'_{I_1',I_2',I_3'}\tag{49}$$

We start by separately bounding each of the sums $S'_{I_1',I_2',I_3'}$.
We define the notation free $(\cdot;\cdot,\cdot,\cdot)$ and explain the above sequence of inequalities next.

For $I\subseteq[n]$ satisfying $|I|\geq n-t+1$ and I_1',I_2',I_3' with $|\cup_{j\in[3]}I_j'|\leq n-t+1$, we let free $(I;I_1',I_2',I_3')$ denote a subset of $I\setminus\cup_{j\in[3]}I_j'$ of size $n-t+1-|\cup_{j\in[3]}I_j'|$ (picked arbitrarily, say according to lexicographic order). When I_1',I_2',I_3' are clear from the context, we abbreviate $\text{free}_i=\text{free}\,(I_i;I_1',I_2',I_3')$.

Consider a superset $B'_{I_1',I_2',I_3'}$ of $B_{I_1',I_2',I_3'}$ consisting of all $\beta\in\mathbb{F}_p^{n-t+1}$ such that $H\beta^T$ has 0's at all coordinates $\bigcup_{j\in[3]}I_j'$, but may as well have 0's *elsewhere*. Restricting β to $B'_{I_1',I_2',I_3'}$ results in a linear code $B'=\{H\beta^T|\beta\in B'_{I_1',I_2',I_3'}\}$. From now on, for a set $B\subseteq\mathbb{F}_p^{n-t+1}$ we abbreviate the multi-set $\{H\beta^T|\beta\in B\}$ by $H\cdot B$. It is well known that C corresponding to (n,t)-Shamir secret sharing scheme (which is a special case of a Massey code) is linear $[n,k=t-1,\mathbb{F}_p]$-MDS code. Therefore, $C^\perp$ is linear $[n,k^\perp=n-t+1,\mathbb{F}_p]$-MDS code. Therefore (holds for all linear MDS codes), every set of $n-t+1$ rows of H are independent. Therefore, the resulting linear code B_I [15], projected onto any subset $I\subseteq[n]$ with $|I|\geq n-t+1$, is the set of all vectors of the form $(\mathbf{0},\mathbf{g},f^\perp(\mathbf{g}))$ where:

- $\mathbf{0}$ is a vector of 0's corresponding to the coordinate set $I\cap(I_1'\cup I_2'\cup I_3')$.
- $\mathbf{g}$ is an arbitrary vector in $\mathbb{F}_p^{|\text{free}(I;I_1',I_2',I_3')|}$.
- $f^\perp(\mathbf{g})$ is the (vector) value at coordinates $I\setminus\left(\bigcup_{j\in[3]}I_j'\cup\text{free}\,(I;I_1',I_2',I_3')\right)$. This value is obtained by applying the linear function $f^\perp$, determined by $C^\perp$, to $(\mathbf{0},\mathbf{g})$ (that together determine the codeword), complementing the required coordinates.

Now, the set $H\cdot B_{I_1',I_2',I_3'}$ is a subset of $H\cdot B'_{I_1',I_2',I_3'}$, where additionally the codeword at coordinates $I_1\setminus I_i$ (similarly for the I_2 part) must be non-0. The transition from Equation 47 to Equation 48, bounds each of the first two $\sqrt{\cdot}$ expressions by summing over β in $B_{I_1',I_2',I_3'}$, by going over all $\mathbf{g}$ values not containing a 0 coefficient, and *assuming* that the resulting $f^\perp(\mathbf{g})$ also has no 0 coefficients (taking the maximal possible coefficient as a bound for each). However, for some such $\mathbf{g}$'s, additional 0 coefficients may turn up in $f^\perp(\mathbf{g})$, so the contribution of that β shouldn't have been accounted for (as $\beta\notin B_{I_1',I_2',I_3'}$).

[15] Jumping ahead, we will only consider B_I for $I\in\{I_1,I_2\}$.

But, this may only increase the upper bound. This only potentially increasing the expression, as all summands are non-negative (in particular, each $\mathbf{g}$ may appear at most once, as in $H \cdot B_{I'_1,I'_2,I'_3}$). A similar phenomena occurs in the part for responding to I_2, so the inequality follows. Another fact we use in this transition, is that $\widehat{\mathbf{1}}_{\ell_i}(0) = \frac{|A_{i,\ell_i}|}{p}$ for any boolean function $\mathbf{1}_{\ell_i}$ we consider.

Further simplifying, we get:

$$
\begin{aligned}
&S'_{I'_1,I'_2,I'_3} \\
&= \sum_{\ell} \prod_{i \in I'_1 \cup I'_2 \cup I'_3} \frac{|A_{i,\ell_i}|}{p} \cdot \prod_{\substack{i \in \text{free}_1 \cup \\ \text{free}_2}} \sqrt{\frac{|A_{i,\ell_i}|}{p}\left(1 - \frac{|A_{i,\ell_i}|}{p}\right)} \cdot \\
&\qquad \prod_{\substack{i \in I_1 \setminus (\text{free}_1 \cup I'_1) \cup \\ I_2 \setminus (\text{free}_2 \cup I'_2) \cup \\ I_3 \setminus I'_3}} \max_{\alpha \in \mathbb{F}_p \setminus \{0\}} |\widehat{\mathbf{1}}_{\ell_i}(\alpha)| \qquad (50) \\
&= \prod_{i \in I'_1 \cup I'_2 \cup I'_3} \sum_{\ell_i \in \{0,1\}} \frac{|A_{i,\ell_i}|}{p} \cdot \prod_{\substack{i \in \text{free}_1 \cup \\ \text{free}_2}} \left(\sum_{\ell_i \in \{0,1\}} \sqrt{\frac{|A_{i,\ell_i}|}{p}\left(1 - \frac{|A_{i,\ell_i}|}{p}\right)} \right) \cdot \\
&\qquad \prod_{\substack{i \in I_1 \setminus (\text{free}_1 \cup I'_1) \cup \\ I_2 \setminus (\text{free}_2 \cup I'_1) \cup \\ I_3 \setminus I'_3}} \left(\sum_{\ell_i \in \{0,1\}} \max_{\alpha \in \mathbb{F}_p \setminus \{0\}} |\widehat{\mathbf{1}}_{\ell_i}(\alpha)| \right) \\
&\leq c_1^{j+i+2l+n-2(n-t+1)-k} = O(c_1^{2t-n+i+j+l}) \qquad (51)
\end{aligned}
$$

Here the equality 50 is simply using Parseval's identity, and the observation that $\widehat{\mathbf{1}}_{\ell_i}(0) = \frac{|A_{i,\ell_i}|}{p}$, and additionally simple arithmetic manipulation. The inequality 51 relies on Claim 3 for upper bounding each multiplicand in the second product by 1. Each multiplicand in the first product sums to 1, and each multiplicand in the third product is upper bounded by c_1, as follows from Lemma 1.

Let us denote by

$$
S'_{i,j,l} = \sum_{\substack{I'_1 \subseteq I_1, |I_1| = i, \\ I'_2 \subseteq I_2, |I_2| = j, \\ I'_3 \subseteq I_3, |I_3| = l}} S'_{I'_1,I'_2,I'_3}.
$$

The number of summands $S'_{i,j,l}$ in the bound 49, rewritten in terms of the $S'_{i,j,l}$s, is only $poly(n)$ ($O(n^2)$, to be precise). Thus to bound $\mathsf{SD}\left(\mathbf{L}(C), \mathbf{L}(\mathbb{F}_p^n)\right)$ we may as well bound t based on the maximum among the sums:

$$\begin{aligned}\log \mathsf{SD}\left(\mathbf{L}(C), \mathbf{L}(\mathbb{F}_p^n)\right) &\leq \log\left(\sum_{i+j+l\leq n-t+1} S'_{i,j,l}\right)\\ &\leq \log\left(O\left((n-t+1)^3\right)\max_{i,j,l} S'_{i,j,l}\right)\\ &\leq \log\max_{i,j,l} S'_{i,j,l} + O(\log n)\end{aligned}$$

Unless stated otherwise, here and elsewhere log stands for $\log_2$. As the bound on the maximum $\log(S'_{i,j,l})$ will be $\Omega(n)$ (for any $t = c \cdot n$ for constant c), we may indeed search for t for which $\log\left(\max_{i,j} S'_{i,j}\right) = -\Omega(n)$ (for arbitrarily small non-0 hidden constants, so the $O(\log(n))$ factor indeed has no effect).

Let us fix some $n - t + 1 = \gamma n$ for some constant $\gamma \in (0, 1)$. We want to find the range of γ values for which $\max_{i+j+l\leq n-t+1} S'_{i,j,l}$ is $2^{-\Omega(n)}$. Let p and n both go to infinity. The above requirement translates into the following,

$$\log\left(\max_{i+j+l\leq n-t+1} S'_{i,j,l}\right)$$

$$\leq \max_{i+j+l\leq n-t+1}\left(\log\left(\sum_{\substack{I'_1\subseteq I_1, |I_1|=i,\\ I'_2\subseteq I_2, |I_2|=j,\\ I'_3\subseteq I_3, |I_3|=l}} S'_{I'_1,I'_2,I'_3}\right)\right)$$

$$\leq \max_{i+j+l\leq n-t+1}\left(\log\left(\binom{n-t+1}{i}\cdot\binom{n-t+1}{j}\cdot\binom{2t-2-n}{l}\cdot\max_{I'_1,I'_2,I'_3} S'_{I'_1,I'_2,I'_3}\right)\right) \tag{52}$$

$$\begin{aligned}\leq n\cdot\Big(&\gamma\cdot\mathbf{I}(a_1) + \gamma\cdot\mathbf{I}(a_2) + (1-2\gamma)\cdot\mathbf{I}(a_3\cdot b/(1-2\gamma)) -\\ &\big(1+\gamma\cdot(a_1+a_2+a_3-2)\big)\log(c_1)\Big) + \operatorname{poly}\log(n)\end{aligned} \tag{53}$$

Here a_1, a_2, a_3 denote $\frac{i}{n-t+1}, \frac{j}{n-t+1}, \frac{l}{n-t+1}$ respectively. In the last step, we use Stirling's approximation, $\log(n!) = n\log(n) - n\log e + O(\log(n))$, neglecting the $O(\log(n))$ term. Also, we replace c_1 with its limit $\lim_{p\to\infty}$. In this case, c_1 tends (from above) to $\log(2/\pi)$. We conclude that the set of γ's satisfying Equation 54 below, result in $(n, (1-\gamma)n)$-Shamir being Leakage resilient, as required in Theorem 1:

$$\begin{aligned}\max_{a_1,a_2,a_3}\Big(&\mathbf{I}(a_1) + \mathbf{I}(a_2) + (1-2\gamma)\cdot\mathbf{I}(a_3\cdot\gamma/(1-2\gamma)) -\\ &\big(1+\gamma\cdot(a_1+a_2+a_3-2)\big)\log(2/\pi)\Big) < 0\end{aligned} \tag{54}$$

In particular, the left hand side is well defined for all $0 < \gamma < 0.5$. Fix some γ, using standard multi-variate analytic techniques (on the expressions as a function of a_1, a_2, a_3) over the domain $\{(a_1, a_2, a_3) | a_1 + a_2 + a_3 \leq 1, a_1, a_2, a_3 \geq 0\}$, we get that $\gamma \leq 0.133n$ leads to a negative value.
This concludes the proof of Theorem 1.