Constructing Locally Leakage-Resilient Linear Secret-Sharing Schemes

Hemanta K. Maji[1(✉)], Anat Paskin-Cherniavsky[2], Tom Suad[2], and Mingyuan Wang[1]

[1] Department of Computer Science, Purdue University, West Lafayette, USA
{hmaji,wang1929}@purdue.edu
[2] Department of Computer Science, Ariel University, Ariel, Israel
anatpc@ariel.ac.il, tom.suad@msmail.ariel.ac.il

Abstract. Innovative side-channel attacks have repeatedly falsified the assumption that cryptographic implementations are opaque black-boxes. Therefore, it is essential to ensure cryptographic constructions' security even when information leaks via unforeseen avenues. One such fundamental cryptographic primitive is the secret-sharing schemes, which underlies nearly all threshold cryptography. Our understanding of the leakage-resilience of secret-sharing schemes is still in its preliminary stage.

This work studies locally leakage-resilient linear secret-sharing schemes. An adversary can leak m bits of arbitrary local leakage from each n secret shares. However, in a locally leakage-resilient secret-sharing scheme, the leakage's joint distribution reveals no additional information about the secret.

For every constant m, we prove that the Massey secret-sharing scheme corresponding to a random linear code of dimension k (over sufficiently large prime fields) is locally leakage-resilient, where $k/n > 1/2$ is a constant. The previous best construction by Benhamouda, Degwekar, Ishai, Rabin (CRYPTO–2018) needed $k/n > 0.907$. A technical challenge arises because the number of all possible m-bit local leakage functions is exponentially larger than the number of random linear codes. Our technical innovation begins with identifying an appropriate pseudorandomness-inspired family of tests; passing them suffices to ensure leakage-resilience. We show that most linear codes pass all tests in this family. This Monte-Carlo construction of linear secret-sharing scheme that is locally leakage-resilient has applications to leakage-resilient secure computation.

H.K. Maji and M. Wang—The research effort is supported in part by an NSF CRII Award CNS–1566499, NSF SMALL Awards CNS–1618822 and CNS–2055605, the IARPA HECTOR project, MITRE Innovation Program Academic Cybersecurity Research Awards (2019–2020, 2020–2021), a Ross-Lynn Research Scholars Grant (2021–2022), a Purdue Research Foundation (PRF) Award (2017–2018), and The Center for Science of Information, an NSF Science and Technology Center, Cooperative Agreement CCF–0939370.

A. Paskin-Cherniavsky and T. Suad—Research supported by the Ariel Cyber Innovation Center in conjunction with the Israel National Cyber directorate in the Prime Minister's Office.

T. Malkin and C. Peikert (Eds.): CRYPTO 2021, LNCS 12827, pp. 779–808, 2021.
https://doi.org/10.1007/978-3-030-84252-9_26

Furthermore, we highlight a crucial bottleneck for all the analytical approaches in this line of work. Benhamouda et al. introduced an analytical proxy to study the leakage-resilience of secret-sharing schemes; if the proxy is small, then the scheme is leakage-resilient. However, we present a one-bit local leakage function demonstrating that the converse is false, motivating the need for new analytically well-behaved functions that capture leakage-resilience more accurately.

Technically, the analysis involves probabilistic and combinatorial techniques and (discrete) Fourier analysis. The family of new "tests" capturing local leakage functions, we believe, is of independent and broader interest.

Keywords: Local leakage-resilience · Massey secret-sharing scheme · Random linear codes · Shamir's secret-sharing scheme · Discrete fourier analysis

1 Introduction

Traditionally, one treats the cryptosystems implementing cryptographic primitives as impervious black-boxes that faithfully realize the intended input-output behavior and provide no additional information. In the real-world implementations and deployments, however, this assumption has been repeatedly proven false. Beginning with the works of Kocher et al. [33,34], several innovative and sophisticated side-channel attacks reveal partial information about the intermediate values and stored secrets of computation (for a summary of the history of several of these attacks, refer to [10,35,46,48,50,56]). These side-channel attacks on fundamental cryptographic building blocks like secret-sharing schemes pose a threat to the security of all cryptographic constructions relying on them.

Towards addressing these concerns, one can design mechanical countermeasures, hardware solutions, and algorithmic representation to protect against known threats [1,5,12,17,20,21]. However, this approach creates unknown risks, the risk of undiscovered attacks compromising a scheme's security. On the other hand, *leakage-resilient cryptography* formally models potential avenues of information leakage and the leakage attacks that an adversary may undertake. This approach has the benefit that the general model encompasses leakage attacks beyond those that are already known. Furthermore, one knows the formal security guarantees and risks of using such cryptographic schemes. In the last few decades, there has been a large body of highly influential research on the feasibility and efficiency of realizing leakage-resilient variants of fundamental cryptographic primitives against active/passive adversaries that perform leakage statically/adaptively (refer to the excellent survey [32]).

One such fundamental cryptographic primitive is *secret-sharing schemes*, which are essential to nearly all threshold cryptography. In the (so-called) standard model, the adversary can corrupt a few parties and obtain their secret-shares; however, it obtains no additional information about the remaining secret shares. The security of secret-sharing schemes crucially relies on the fact that the

corruption threshold is lower than the secret-sharing schemes' privacy threshold. However, a side-channel attack on a secret-sharing scheme provides the adversary a restricted or noisy access to every party's secret share. For instance, a *passive adversary* can leak a few bits from each secret share. Although it has a partial view of each secret share, the leakages' joint distribution may be correlated with the secret to compromise its secrecy.

Our understanding of the leakage-resilience of secret-sharing schemes is still in its preliminary stage. Even for prominent secret-sharing schemes like Shamir's secret-sharing scheme, the exact characterization of the leakage-resilience is not well-understood. A *locally leakage-resilient secret-sharing scheme* (LLRSS) [7] (also implicit in the constructions of [26]) protects against a static passive adversary. The adversary chooses leakage functions from all the secret shares. However, an LLRSS secret-sharing scheme ensures that the leakage's joint distribution is statistically independent of the secret. Guruswami and Wootters's reconstruction algorithm [28,29] for Reed-Solomon codes (and follow-up works [18,27,42,52]) demonstrate that Shamir's secret-sharing scheme on characteristic-2 finite fields is insecure even when the adversary can leak only one bit from every secret share. Achieving leakage-resilience seems challenging because the adversary need not reconstruct the complete secret; obtaining only some partial information about the secret precludes leakage-resilience. For example, over characteristic-two fields, if the secret is a linear combination of some parties' secret shares, then the adversary can leak only one bit from these secret shares and reconstruct the least significant bit of the secret. Although this attack does not suffice to reconstruct the complete secret (which is impossible using entropy arguments), it suffices to distinguish the secret 0 from secret 1.

There has been a significant amount of research into constructing new leakage-resilient secret-sharing schemes [3,6,11,13,15,23,24,31,36,41,51]. However, it seems insurmountable to replace every deployed secret-sharing scheme with their leakage-resilient version or an entirely new leakage-resilient secret-sharing scheme. Furthermore, in specific contexts, cryptographic constructions crucially rely on the secret-sharing scheme's additional salient features (for example, their linearity and algebraic structure); thus, making such a substitution impossible. Inspired by these concerns, recently, there have been studies on the leakage-resilience of prominent secret-sharing schemes, like Shamir's secret-sharing scheme and the additive secret-sharing scheme [2,14,30,37,39].

A Summary of Our Model and Results. This work studies the leakage-resilience of Massey secret-sharing schemes [43] corresponding to various linear codes, for example, random linear codes, Reed-Solomon codes, and the parity code. We remind the readers that prominent secret-sharing schemes like Shamir's secret-sharing scheme and the additive secret-sharing scheme are the Massey secret-sharing schemes corresponding to (punctured) Reed-Solomon codes and the parity code. Our work considers m-bit *general leakage* from each secret share, where m is a constant.

Result 1. We present a Monte Carlo algorithm for a linear secret-sharing scheme that is secure against m-bit leakage from each secret share, where m is

a constant. We prove that the Massey secret-sharing scheme corresponding to a random linear code is leakage-resilient if k/n is a constant $> 1/2$. Towards this objective, the technical challenge is that the number of potential constructions is exponentially smaller than the number of all such leakage functions. Overcoming this hurdle requires identifying a significantly smaller set of "tests," passing them suffices to guarantee leakage-resilience.

Result 2. Next, we show an explicit leakage function (leaking only $m = 1$ bit from each secret share) that highlights a significant shortcoming of the analytic techniques employed in this line of work. Ever since the work of Benhamouda et al. [7], analytic techniques employ a (natural) "proxy analytic function" to study the leakage resilience of secret-sharing schemes. If this proxy is small, then the insecurity of the secret-sharing scheme to leakage attacks is small as well. However, we present an explicit attack demonstrating that the converse is false, making a case for discovering new (analytically well-behaved) proxies that represent the insecurity of secret-sharing schemes more accurately.

Result 3. Using the new analytical techniques developed for "Result 1" in our work, we improve the leakage-resilience guarantees for Shamir's secret-sharing scheme for n parties. We prove that if the reconstruction threshold $k \geqslant 0.8675 \cdot n$ then it is secure against $m = 1$ bit leakage from each secret share improving the previous state-of-the-art from $k \geqslant 0.907 \cdot n$.[1] Independent to our work, the journal version [9] of [8] also improved the threshold to $k \geqslant 0.85n$.

Result 4. Finally, we note that an attack for additive secret-sharing schemes proposed by Benhamouda et al. [7] can be extended to all linear secret-sharing schemes. By this observation, we prove that to achieve $2^{-\lambda}$ insecurity, the threshold k must be at least $\Omega\left(\frac{\lambda}{\log \lambda}\right)$. This generalizes a similar result by Nielsen and Simkin [44] as their result works only for polynomially large fields while our result works for fields of arbitrary size.

1.1 Our Contributions

This section introduces some basic definitions to facilitate an intuitive presentation of our results.

F is a prime field such that $|F|$ needs λ bits for its binary representation, i.e., $2^{\lambda-1} \leqslant |F| < 2^{\lambda}$. We interpret λ as the security parameter and, therefore, the number of parties $n = \mathsf{poly}(\lambda)$. Typically, in cryptography, the objective is to demonstrate the insecurity of cryptographic constructions is $\mathsf{negl}(\lambda)$, a function that decays faster than any inverse-polynomial in λ. However, in this work, as is common in information theory and coding theory literature, all our results shall further ensure that the insecurity is exponentially decaying in the security parameter.

Massey Secret-Sharing Scheme. Let $C \subseteq F^{n+1}$ be a subset, referred to as a *code*. The Masey secret-sharing scheme [43] corresponding to code C secret-

[1] The older full version of [8] claims a smaller constant in Theorem 1.2, which is a consequence of an incorrect calculation. $k \geqslant 0.907n$ is an accurate reflection of the result in their full version.

shares the secret $s \in F$ by choosing a random $(c_0, c_1, \ldots, c_n) \in C$ conditioned on $c_0 = s$. The secret share of party i is $s_i = c_i$, for all $i \in \{1, \ldots, n\}$.

Linear Codes. A vector subspace $V \subseteq F^{n+1}$ of dimension $(k+1)$ is an $[n+1, k+1]_F$-code. A matrix $G^+ \in F^{(k+1)\times(n+1)}$ succinctly represents this vector space V if the linear span of its rows, represented by $\langle G^+ \rangle$, is identical to the vector space V. (Punctured) Reed-Solomon codes and parity codes are linear codes. Fix distinct evaluation places $X_1, \ldots, X_n \in F^*$. The set of elements $(f(0), f(X_1), \ldots, f(X_n))$, for all polynomials $f(X) \in F[X]$ of degree $< (k+1)$, is the (punctured) Reed-Solomon code. The set of all elements $(c_0, c_1, \ldots, c_n) \in F^{n+1}$ such that $c_0 + c_1 + \cdots + c_n = 0$ is the parity code.

This work considers Massey secret-sharing schemes of linear codes.

Local Leakage-Resilience of Secret-Sharing Schemes. An (n, m) local leakage function leaks m-bit leakage from each of the secret shares of the n parties. The output of an (n, m) local leakage function is the joint distribution of the mn leakage bits. A secret-sharing scheme for n parties is $(m, \varepsilon) - locally leakage - resilient$ if any (n, m) local leakage function cannot distinguish whether the secret $s^{(0)} \in F$ from the secret $s^{(1)} \in F$ based on the joint leakage distributions, for arbitrary $s^{(0)}, s^{(1)} \in F$.

Remark 1. In the literature (e.g., [7]), the following definition of leakage-resilience has also been considered. The adversary is given some secret shares explicitly and then allowed to leak from the remaining secret shares. We note that, for an MDS code G^+, the leakage-resilience of Massey secret-sharing corresponding to G^+ in these two definitions are equivalent as follows.

Suppose G^+ is an MDS code of dimension $(k+1) \times (n+1)$. If the adversary obtains t shares explicitly, the remaining secret shares is exactly a Massey secret-sharing scheme corresponding to some G' of dimension $(k+1-t) \times (n+1-t)$. Hence, G^+ is leakage-resilient to an adversary who obtains t shares explicitly if and only if Massey secret-sharing corresponding to G' is leakage-resilient when the adversary only leaks from every secret share.

In this paper, we only work with G^+ that is MDS.[2] Therefore, we restrict to the simple setting where the adversary only leaks from every secret share.

Result 1. Leakage-Resilience of Random Linear Codes. For the presentation in this section, a *random* $[n+1, k+1]_F$*-code* is the linear code $\langle G^+ \rangle$ where $G^+ \in F^{(k+1)\times(n+1)}$ is a rank-$(k+1)$ random matrix. Section 2.2 provides additional details on efficiently sampling such a matrix.

Corollary 1 (Random Linear Secret-sharing Schemes are Leakage-resilient). *Fix constants $m \in \mathbb{N}$, $\delta \in (0,1)$, and $\eta \in (0,1)$. Define $n = (1-\eta)\cdot\lambda$ and $k = (1/2+\delta)\cdot n$. Let F be a prime field of order $\in \{2^{\lambda-1}, \ldots, 2^\lambda - 1\}$. For all sufficiently large λ, the Massey secret-sharing scheme corresponding to a random $[n+1, k+1]_F$-code is (m, ε)-locally leakage-resilient, where $\varepsilon = \exp(-\Theta\lambda)$, except with $\exp(-\Theta\lambda)$ probability.*

[2] In particular, our main result considers a random G^+, which is MDS with overwhelming probability.

We highlight that one can publicly choose the randomness determining G^+ once (say, using a CRS) and use this code for all future applications. With high probability, as long as the local leakage is $\leqslant m$, the Massey secret-sharing scheme corresponding to the linear code $\langle G^+ \rangle$ shall be leakage-resilient.[3] Intuitively, the Massey secret-sharing scheme corresponding to a random $[n+1, k+1]_F$-code (where F is a finite field of order $> 2^{\lambda-1}$, $n = 0.97\lambda$, and $k = 0.49\lambda$) shall be leakage-resilient to arbitrary m-bit local leakages when λ is sufficiently large (except with exponentially small probability). The threshold of λ being sufficiently large depends on the choices of m, δ, and η. For example, when $m = 1$ and using 2000-bit prime numbers, the insecurity of the above scheme is $< 2^{-50}$.

Efficiency. Linear codes, in contrast to non-linear codes, result in efficient Massey secret-sharing schemes. In particular, when $G^+ = [I_{k+1} \mid P]$ is in the *standard form*, as is the case in this work, then the corresponding Massey secret-sharing scheme is easy to specify, where $I_{k+1} \in F^{(k+1)\times(k+1)}$ is the identity matrix. Observe that the secret shares of the secret $s \in F$ is

$$(s, s_1, \ldots, s_n) := (s, r_1, \ldots, r_k) \cdot G^+,$$

where $r_1, \ldots, r_k$ are independently and uniformly distributed over F. Reconstruction of the secret is efficient as well for this secret-sharing scheme. Suppose $G^+_{*,0} = \lambda_1 \cdot G^+_{*,j_1} + \cdots + \lambda_t \cdot G^+_{*,j_t}$, where $G^+_{*,j}$ represents the j-th column of the matrix G^+ and $\lambda_1, \ldots, \lambda_t \in F$ are appropriate constants. Then, parties $j_1, \ldots, j_t$ can efficiently reconstruct the secret $s = \lambda_1 \cdot s_{j_1} + \cdots + \lambda_t \cdot s_{j_t}$, where s_j represents the secret share of party j. Furthermore, any $t = k+1$ shall be able to reconstruct the secret because any $(k+1)$ columns of a random G^+ is full rank, except with an exponentially small probability.

The efficient reconstruction of the secret depends on parties reporting their secret shares correctly. If there are $(k+1)$ publicly identifiable honest parties, all parties can efficiently reconstruct the secret from these parties' secret-shares. Additionally, information-theoretic primitives like *message authentication codes* can ensure that malicious parties cannot disclose incorrect secret shares.[4] Using such information-theoretic cryptographic primitives, all parties can efficiently reconstruct the secret in applications using such secret-sharing schemes.

Applications. Linear secret-sharing schemes have applications in secure multi-party computation [25,55] due to their additive structure. In particular, an additive secret-sharing scheme is useful for the secure computation of circuits that use only addition gates, i.e., the *aggregation functionality*. The secure computation protocol proceeds as follows. Party i secret-shares its inputs $x^{(i)}$ using a linear secret-sharing scheme. Let the secret share of $x^{(i)}$ for party j be $x^{(i,j)}$. Now, party

[3] However, as are typical for probabilistic existential results in information theory and coding theory, one cannot efficiently test whether the sampled G^+ is leakage-resilient.

[4] This step is necessary because *efficient error-correction algorithms* for (dense) random linear codes shall require incredible breakthroughs in mathematics. In fact, a lot of cryptography assumes that error-correction for random linear codes is inefficient [47,49]. Efficient error-correction is known only when the matrix G^+ has additional algebraic structures.

j has the secret shares $x^{(1,j)}, \ldots, x^{(n,j)}$. Party j defines $s^{(j)} := \sum_{i=1}^{n} x^{(i,j)}$. Now, the secret shares $s^{(1)}, \ldots, s^{(n)}$ are secret shares of the sum $s = x^{(1)} + \cdots + x^{(n)}$. If any $(k+1)$ parties can reconstruct the secret in the linear secret-sharing scheme, any subset of $(k+1)$ parties can come online to recover the sum s.

When using our linear secret-sharing scheme[5] robust to arbitrary m-bit local leakage, this secure computation is leakage-resilient to arbitrary m-bit leakage as well, when k/n is a constant $> 1/2$. The previous state-of-the-art construction [7] used Shamir's secret-sharing scheme and needed $k/n \geqslant 0.907$, which was a significantly larger fraction. [39] proved the leakage-resilience of Shamir's secret-sharing scheme for an extremely restricted family of leakage functions, namely, the physical-bit leakage function, for every $k > 1$.

Derandomization. We highlight that we significantly derandomized the space of all possible codes to demonstrate that a *linear* code suffices to construct a leakage-resilient secret-sharing scheme. For example, against active adversaries who tamper the secret shares, the probabilistic construction of Cheraghchi and Guruswami [16] used (inefficient) non-linear codes.[6]

Technical Highlights. At the outset, linear codes as potential candidate constructions for leakage-resilient secret-sharing schemes seem far-fetched. Observe that the set of all possible (n, m) local leakage functions is $2^{mn|F|} \gg 2^{2^{\lambda}}$, where m is a constant, $n = \mathsf{poly}(\lambda)$, and $p \approx 2^{\lambda}$. However, there are only $|F|^{kn} \approx 2^{\mathsf{poly}(\lambda)}$ different matrices G^{+}. Typically, the proofs of similar results (see, for example, [16,22,39]) proceed by "union bound" techniques and need the set of adversarial strategies to be significantly smaller than the potential choices available for the construction. One of our work's key technical contributions is to address this apparent handicap that our construction faces.

We introduce a new family of "tests" (see Sect. 3) inspired by the various notions of pseudorandomness [53,54]. We show that if a generator matrix G^{+} passes all these tests, then the Massey secret-sharing scheme corresponding to the linear code $\langle G^{+} \rangle$ is leakage-resilient (see Sect. 3.3). The advantage here is that the number of all possible tests is significantly smaller than the number of choices for choosing G^{+}. Finally, we show that nearly all matrices G^{+} pass all our tests (see Sect. 3.2). Lemmas 1 and 2 abstract these two technical innovations, which, the authors believe, are of potential independent interest in the broader field of probabilistic analysis. Section 3 presents the proof of this result.

Result 2. A Barrier in the Analytic Modeling. Benhamouda et al. [7] introduced an analytic proxy (Refer to Eq. 6) for upper bounding the statistical distance between leakage distributions of different secrets. All the works in this line of research ([7,39] and this work) essentially study leakage-resilience of the secret-sharing scheme through this analytic proxy. We present an inherent barrier

[5] Additionally, one can use information-theoretic message authentication codes to avoid incorrect revelation of secret-shares.

[6] We note that non-malleability naturally requires the code to be non-linear. However, our point is that the union bound technique would not have worked if one considers a very small family of constructions such as linear codes.

for this proof strategy. We prove that one cannot prove any meaningful result when the threshold is less than half of the number of parties.

In particular, we present an explicit leakage function $\vec{L}$, which tests whether the field element is a *quadratic residue* or not. We prove that for *any* linear secret-sharing scheme with threshold k and n parties such that $k < n/2$, the analytic proxy with respect to this secret-sharing scheme and our leakage function $\vec{L}$ is at least 1.[7] Therefore, using this analytic proxy, it is hopeless to prove leakage-resilience against *general leakage* when $k < n/2$. This result is summarized as Theorem 1 in Sect. 4.

In light of this, our first result that states a random linear code is leakage-resilient when $k \geqslant (\frac{1}{2} + \delta)n$ for an arbitrary constant $\delta \in (0, 1/2)$ is the optimal result one could hope to obtain using the current proof technique. To obtain better results, significantly different ideas are required.

We note that the recent work of Maji et al. [39] also employs this analytic proxy. They show that Shamir's secret-sharing with random evaluation places is leakage-resilient even for the most stringent case $k = 2$ and $n = \mathsf{poly}(\lambda)$. Their results, however, do not contradict the barrier we present here. They only consider the family of leakage functions that leak physical-bit when the field elements are store in their natural binary representations. The counter-example we present, i.e., testing whether a field element is a quadratic residue or not, cannot be simulated by leaking a constant number of physical-bits.

Result 3. We prove the following result on the leakage-resilience of Shamir's secret-sharing scheme.

Corollary 2. *There exists a universal constant p_0 such that, for all finite field F of prime order $p > p_0$, the following holds. Shamir's secret-sharing scheme with number of parties n and threshold k is $(1, \exp(-\Theta n)$-leakage-resilient if $k \geqslant 0.8675n$.*

We improve from the previous state-of-the-art result of $k \geqslant 0.907n$ of [7] to $k \geqslant 0.8675n$. In an independent work, Benhamouda et al. [9] also improved their results to $k \geqslant 0.85n$. Note that achieving $k < n/2$ shall enable parties to multiply their respective secret shares to obtain secret shares of the product of the secrets.

Technically, we prove this result by employing a more fine-grained (compared to [7]) analysis on the analytic proxy. Section 5 presents the proof overview.

Result 4. Consider a secret-sharing scheme with n parties and threshold k over a prime field F of order p that is leakage-resilient to m-bit leakage from each share. Nielsen and Simkin [44] proved that it must hold that $k \cdot \log p \geqslant m \cdot (n-k)$. Intuitively, they prove this result using an entropy argument.[8] Consequently, their result is inevitably sensitive to the size of the field. They used this result

[7] Note that this analytic proxy is used as an upper bound of the statistical distance. Hence, it gives an inconsequential bound if it is $\geqslant 1$.

[8] Note that a secret-sharing scheme contains exactly $k \cdot \log p$ amount of entropy. Hence, intuitively, the total amount entropy leaked $m \cdot n$ cannot exceed $k \cdot \log p$.

to show that if the field size satisfies $p = \mathsf{poly}(n)$, the threshold k must be at least $\Omega(n/\log n)$.

For linear secret-sharing schemes, we obtain a similar result, independent of the field size.

Corollary 3. *If a linear secret-sharing scheme (over an arbitrarily large field) with n parties and threshold k is $(1,\varepsilon)$-leakage-resilient, then it must hold that $\varepsilon \geqslant \left(\frac{1}{2k}\right)^k$. Consequently, if it is $(1,\exp(-\Theta n))$-leakage-resilient, it must hold that $k = \Omega(n/\log n)$.*

We prove our result through a similar attack proposed by [7] (on additive secret-sharing schemes). A proof of this result is provided in the full version [40].

1.2 Prior Works

Local leakage-resilient secret-sharing schemes were introduced by Benhamouda, Degwekar, Ishai, and Rabin [7] (also, independently by [26] as an intermediate primitive). There has been a sequence of works analyzing the leakage-resilience of prominent secret-sharing schemes [2,14,30,37,39] and constructing new leakage-resilient secret-sharing schemes [3,6,11,13,15,23,24,31,36,41,51].

There is an exciting connection between repairing a linear code in the distributed storage setting and the leakage-resilience of its corresponding Massey secret-sharing scheme [43]. In the distributed storage setting, every coordinate of the linear code is separately stored. The objective is to repair a block of the code by obtaining information from all other blocks. For example, Guruswami and Wootters [28,29] present a reconstruction algorithm that obtains $m = 1$ bit from every block of a Reed-Solomon code to repair any block when the field has characteristic two. These reconstruction algorithms ensure that by leaking m bits from the secret-shares corresponding to the Massey secret-sharing scheme corresponding to the linear code, it is possible to reconstruct the secret. For example, the Reed-Solomon reconstruction algorithm of Guruswami-Wootters translates into a leakage attack on Shamir's secret-sharing scheme (for characteristic two fields), the Massey secret-sharing scheme corresponding to a (punctured) Reed-Solomon code.

However, when working over prime fields, [7] proved that Shamir's secret-sharing scheme is robust to $m = 1$ bit leakage if the reconstruction threshold is sufficiently high. In particular, their analysis proved that it suffices for the reconstruction threshold k to be at least $0.907n$, where n is the total number of parties. Moreover, their results extend to arbitrary MDS codes. They complement this positive result with an attack on the additive secret-sharing scheme that has a distinguishing advantage of $\varepsilon \geqslant k^{-k}$. After that, Nielsen and Simkin [44] present a probabilistic argument to construct a leakage attack on any Massey secret-sharing scheme. Roughly, their attack needs $m \geqslant k \log p/(n-k)$ bits of leakage from each secret share, where p is the order of the prime field.

Recently, [39] studied a restricted family of leakage on Shamir's secret-sharing schemes. The secret-shares, which are elements of the prime field, are represented

in their natural binary representation and stored in hardware. The adversary can leak only physical bits from the memory storage. They proved that Shamir's secret-sharing scheme with random evaluation places is leakage-resilient to this leakage family.

2 Preliminaries and Notations

The *binary entropy function* $h_2 \colon [0,1] \to [0,1]$ is

$$h_2(p) := -p\log_2 p - (1-p)\log_2(1-p).$$

We shall use the following elementary upper bound on the binomial coefficients.

Claim 1 (Estimation of Binomial Coefficients). *For all $n \in \mathbb{N}$ and $k \in \{0,1,\ldots,n\}$, we have*

$$\binom{n}{k} \leqslant 2^{h_2(k/n)\cdot n}.$$

Proof. Observe that

$$1 = \left(\frac{k}{n} + \frac{n-k}{n}\right)^n \geqslant \binom{n}{k}\left(\frac{k}{n}\right)^k \left(1-\frac{k}{n}\right)^{n-k} = \binom{n}{k} 2^{-h_2(k/n)\cdot n}.$$

This completes the proof of the claim.

Our work uses the length of the binary representation of the order of the prime field F as the security parameter λ. The total number of parties $n = \mathsf{poly}(\lambda)$ and the reconstruction threshold $k = \mathsf{poly}(\lambda)$ as well. The objective of our arguments shall be to show the insecurity of the cryptographic constructions is $\varepsilon = \mathsf{negl}(\lambda)$, i.e., a function that decays faster than any inverse-polynomial of the λ.

We shall also use the following Vinogradov notations for brevity in our analysis (as consistent with, for example, [4]). For functions $f(\lambda)$ and $g(\lambda)$, one writes $f(\lambda) \sim g(\lambda)$ to represent $f(\lambda) = (1 + \mathrm{o}(1)) \cdot g(\lambda)$, where $\mathrm{o}(1)$ is a decreasing function in λ. Similarly, $f(\lambda) \lesssim g(\lambda)$ is equivalent to $f(\lambda) \leqslant (1 + \mathrm{o}(1)) \cdot g(\lambda)$. Finally, $f(\lambda) \ll g(\lambda)$ represents that $f(\lambda) = \mathrm{o}(1) \cdot g(\lambda)$. We explicitly mention the definitions of these notations because there are multiple interpretations of these symbols even in the field of analysis.

2.1 General Notation: Vectors, Random Variables, Sets

Let X be a sample space. Particular elements of X are represented using the small-case letter x. A random variable of sampling x from the sample space X shall be represented by $\mathbf{x}$.

For any two distributions $\mathbf{A}$ and $\mathbf{B}$ over the same sample space (which is enumerable), the *statistical distance* between the two distributions, represented by $\mathsf{SD}(\mathbf{A},\mathbf{B})$, is defined as $\frac{1}{2}\sum_x |\Pr[\mathbf{A}=x] - \Pr[\mathbf{B}=x]|$.

A vector $\vec{v} \in \Omega^n$ is interpreted as $\vec{v} = (v_1,\ldots,v_n)$, where each $v_i \in \Omega$. For any $I \subseteq \{1,\ldots,n\}$, the vector $\vec{v}_I \in \Omega^{|I|}$ represents the vector $(v_i \colon i \in I)$.

Let $(S,\circ)$ be a group. Let $A \subseteq S$ and $x \in S$ be an arbitrary element of S. Then $x \circ S$ is the set $\{x \circ y : y \in S\}$.

2.2 Matrices

We adopt the following notations for matrices as consistent with [45].

Let F be a finite field. A matrix $M \in F^{k \times n}$ has k-rows and n-columns, and each of its element is in F. For $i \in \{1, \ldots, k\}$ and $j \in \{1, \ldots, n\}$, $M_{i,j}$ represents the (i, j)-th elements in the matrix M. Furthermore, $M_{i,*}$ represents the i-th row of M and $M_{*,j}$ represents the j-th column of M. The *transpose* of the matrix $M \in F^{k \times n}$ is the matrix $N \in F^{n \times k}$ such that $M_{i,j} = N_{j,i}$, for all $i \in \{1, \ldots, k\}$ and $j \in \{1, \ldots, n\}$. We represent $N = M^\intercal$.

Let $I \subseteq \{1, \ldots, k\}$ and $J \subseteq \{1, \ldots, n\}$ be a subset of row and column indices, respectively. The matrix M restricted to rows I and columns J is represented by $M_{I,J}$. If $I = \{i\}$ is a singleton set, then we represent $M_{i,J}$ for $M_{\{i\},J}$. The analogous notation also holds for singleton J. Furthermore, $G_{*,J}$ represents the columns of G indexed by J (all rows are included). Similarly, $G_{*,j}$ represents the j-th column of the matrix G. Analogously, one defines $G_{I,*}$ and $G_{i,*}$.

Some parts of the documents use $\{0, 1, \ldots, k\}$ as row indices and $\{0, 1, \ldots, n\}$ as column indices for a matrix $G \in F^{(k+1) \times (n+1)}$. We will be explicit in mentioning the row and column indices in this work.

Random Matrices. A *random matrix M of dimension $k \times n$* is a uniformly random element of $F^{k \times n}$. This sampling is equivalent to choosing every element $M_{i,j}$ of the matrix uniformly and independently at random from F, for all $i \in \{1, \ldots, k\}$ and $j \in \{1, \ldots, n\}$.

2.3 Codes and Massey Secret-Sharing Schemes

We use the following notations for error-correcting codes as consistent with [38].

Let F be a finite field. A *linear code* C (over the finite field F) of *length* $(n+1)$ and *rank* $(k+1)$ is a $(k+1)$-dimension vector subspace of F^{n+1}, referred to as an $[n+1, k+1]_F$-code. The *generator matrix* $G \in F^{(k+1) \times (n+1)}$ of an $[n+1, k+1]_F$ linear code C ensures that every element in C can be expressed as $\vec{x} \cdot G$, for an appropriate $\vec{x} \in F^{k+1}$. Given a generator matrix G, the row-span of G, i.e., the code generated by G, is represented by $\langle G \rangle$. A generator matrix G is in the *standard form* if $G = [I_{k+1} | P]$, where $I_{k+1} \in F^{(k+1) \times (k+1)}$ is the identity matrix and $P \in F^{(k+1) \times (n-k)}$ is the parity check matrix. In our work, we always assume that the generator matrices are in their standard form.

Let $C \subseteq F^{n+1}$ be the linear code that G generates. The *dual code* of C, represented by $C^\perp \subseteq F^{n+1}$, is the set of all elements in F^{n+1} that are orthogonal to *every* element in C. The dual code of an $[n+1, k+1]_F$-code happens to be an $[n+1, n-k]_F$-code. The generator matrix H for the dual code of the $[n+1, k+1]_F$ linear code C generated by $G = [I_{k+1} | P]$ satisfies $H = [-P^\intercal | I_{n-k}]$, where $P^\intercal \in F^{(n-k) \times (k+1)}$ is the transpose of the matrix $P \in F^{(k+1) \times (n-k)}$. For brevity, we shall refer to the generator matrix H as the *dual* of the generator matrix G.

Maximum Distance Separable Codes. The *distance* of a linear code is the minimum weight of a non-zero codeword. An $[n, k]_F$-code is *maximum distance*

separable (MDS) if its distance is $(n-k+1)$. Furthermore, the dual code of an $[n,k]_F$-MDS code is an $[n,n-k]_F$-MDS code.

Massey Secret-Sharing Scheme. Let $C \subseteq F^{n+1}$ be a code (not necessarily a linear code). Let $s \in F$ be a secret. The secret-sharing scheme picks a random element $(s, s_1, \ldots, s_n) \in C$ to share the secret s. The secret shares of parties $1, \ldots, n$ are $s_1, \ldots, s_n \in F$, respectively. Below, we elaborate on the Massey secret-sharing scheme and its properties specifically for a linear code C such that its generator matrix G^+ is in the standard form.

Recall that the set of all codewords of the linear code generated by the generator matrix $G^+ \in F^{(k+1)\times(n+1)}$ is

$$\left\{ \vec{y} : \ \vec{x} \in F^{k+1}, \vec{x} \cdot G^+ =: \vec{y} \right\} \subseteq F^{n+1}.$$

For such a generator matrix, its rows are indexed by $\{0, 1, \ldots, k\}$ and its columns are indexed by $\{0, 1, \ldots, n\}$. Let $s \in F$ be the secret. The *secret-sharing scheme* picks independent and uniformly random $r_1, \ldots, r_k \in F$. Let

$$(y_0, y_1, \ldots, y_n) := (s, r_1, \ldots, r_k) \cdot G^+.$$

Observe that $y_0 = s$ because the generator matrix G^+ is in the standard form. The secret shares for the parties $1, \ldots, n$ are $s_1 = y_1, s_2 = y_2, \ldots, s_n = y_n$, respectively. Observe that every party's secret-share is an element of the field F. Of particular interest will be the set of all secret shares of the secret $s = 0$. Observe that the secret-shares form an $[n,k]_F$-code that is $\langle G \rangle$, where $G = G^+_{\{1,\ldots,k\}\times\{1,\ldots,n\}}$. Note that the matrix G is also in the standard form. The secret shares of $s \in F^*$ form the affine space $s \cdot \vec{v} + \langle G \rangle$, where $\vec{v} = G^+_{0,\{1,\ldots,n\}}$. Refer to Fig. 1 for a pictorial summary.

Suppose parties $i_1, \ldots, i_t \in \{1, \ldots, n\}$ come together to reconstruct the secret with their, respective, secret shares $s_{i_1}, \ldots, s_{i_t}$. Let $G^+_{*,i_1}, \ldots, G^+_{*,i_t} \in F^{(k+1)\times 1}$ represent the columns indexed by $i_1, \ldots, i_t \in \{1, \ldots, n\}$, respectively. If the column $G^+_{*,0} \in F^{(k+1)\times 1}$ lies in the span of $\left\{G^+_{*,i_1}, \ldots, G^+_{*,i_t}\right\}$ then these parties can reconstruct the secret s using a linear combination of their secret shares. If the column G^+_{*0} *does not* lie in the span of $\left\{G^+_{*,i_1}, \ldots, G^+_{*,i_t}\right\}$ then the secret remains *perfectly hidden* from these parties. The perfectly-hiding property is specific to the case that a linear code is used for the Massey secret-sharing scheme. In particular, this perfectly-hiding property need not necessarily hold for Massey secret-sharing schemes that use a non-linear secret-sharing scheme.

In this document, we shall use the "Massey secret-sharing scheme of G^+" to refer to the Massey secret-sharing scheme corresponding to the linear code generated by the generator matrix G^+. The underlying field F, the length of the code $(n+1)$, and the rank $(k+1)$ of the linear code are implicit given the definition of the generator matrix G^+. These parameters, in turn, define the space of the secret-shares, the total number of parties, and the randomness needed to generate the secret shares for the Massey secret-sharing scheme, respectively.

Specific Linear Codes. The (punctured) *Reed-Solomon code* of rank $(k+1)$ and evaluation places $\vec{X} = (X_1, \ldots, X_n) \in (F^*)^n$, where $i \neq j$ implies $X_i \neq X_j$,

is the following code. Let $f(X)$ be the *unique polynomial* with F-coefficients and degree $\leqslant k$ such that $f(0) = y_0, f(X_1) = y_1, f(X_2) = y_2, \ldots, f(X_k) = y_k$, for any $y_0, y_1, \ldots, y_k \in F$. Define $c_{k+1} = f(X_{k+1}), \ldots, c_n = f(X_n)$. The set of all codewords $(y_0, y_1, \ldots, y_k, c_{k+1}, \ldots, c_n) \in F^{n+1}$ is an $[n+1, k+1]_F$-code. Furthermore, the mapping

$$(y_0, y_1, \ldots, y_k) \mapsto (y_0, y_1, \ldots, y_k, c_{k+1}, \ldots, c_n)$$

is linear and a generator matrix in the standard form establishes this mapping.

Specific Secret-Sharing Schemes. *Shamir's secret-sharing scheme* is the Massey secret-sharing scheme corresponding to (punctured) Reed-Solomon codes. Suppose the evaluation places of the (punctured) Reed-Solomon code are $\vec{X} = (X_1, \ldots, X_n) \in (F^*)^n$. Suppose the secret is $s \in F$. Let $f(X)$ be the unique polynomial with F-coefficients and degree $\leqslant k$ such that $f(0) = s, f(X_1) = r_1, \ldots, f(X_k) = r_k$. Define the secret shares $(s_1, \ldots, s_n)$, where $s_i = f(X_i)$, for all $i \in \{1, \ldots, n\}$.

2.4 Locally Leakage-Resilient Secret-Sharing Scheme

Fix a finite field F and an n-party secret-sharing scheme for secrets $s \in F$, where every party gets an element in F as their secret share. An (n, m) *local leakage function* $\vec{L} = (L_1, \ldots, L_n)$ is an n-collection of m-bit leakage functions $L_i \colon F \to \{0,1\}^m$, for $i \in \{1, \ldots, n\}$. Note that there are a total of $2^{mn \cdot |F|}$ different (n, m) local leakage functions. Let $\vec{\mathbf{L}}(s)$ be the joint distribution of the (n, m) leakage function $\vec{L}$ over the sample space $(\{0,1\}^m)^n$ defined by the experiment: (a) sample secret shares $(s_1, \ldots, s_n)$ for the secret s, and (b) output $(L_1(s_1), \ldots, L_n(s_n))$. We emphasize that the secret-sharing scheme and the finite field F shall be evident from the context. So, we do not include the description of the secret-sharing scheme and the finite field in the random variables above to avoid excessively cumbersome notation.

A secret-sharing scheme for n-parties is (m, ε)-*locally leakage-resilient secret-sharing scheme* if, for all (n, m) local leakage functions $\vec{L} = (L_1, \ldots, L_n)$ and secret pairs $(s^{(0)}, s^{(1)})$, the statistical distance between the leakage joint distributions $\vec{\mathbf{L}}(s^{(0)})$ and $\vec{\mathbf{L}}(s^{(1)})$ is at most ε.

For brevity, we shall say that a generator matrix G is (m, ε)-locally leakage-resilient if the Massey secret-sharing scheme corresponding to the linear code generated by G is (m, ε)-locally leakage-resilient.

3 Leakage-Resilience of Random Linear Codes

In this section, we prove Corollary 1. We start by recalling some notations. Refer to Fig. 1 for a pictorial summary of the notations. The secret shares of 0 is the vector space

$$(0, r_1, \ldots, r_k) \cdot G_{\{0,\ldots,k\},\{1,\ldots,n\}} \in F^n.$$

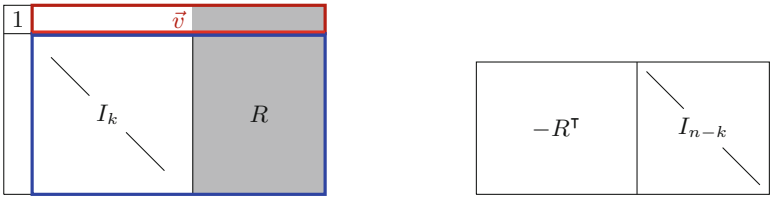

Fig. 1. The matrix on the left is $G^+ = [I_{k+1} \mid P]$, where P is the random matrix in the shaded region. The indices of rows and columns of G^+ are $\{0, 1, \ldots, k\}$ and $\{0, 1, \ldots, n\}$, respectively. The blue $G = [I_k \mid R]$ is a submatrix of G^+. The vector highlighted in red is the vector $\vec{v}$. On the right-hand side, we have the matrix H, where $\langle H \rangle$ is the dual code of $\langle G \rangle$. (Color figure online)

Observe that this vector space is an $[n, k]_F$-code, represented by $\langle G \rangle$, where $G = G^+_{\{1,\ldots,k\},\{1,\ldots,n\}}$. Each element of $\langle G \rangle$ is equally likely to be chosen as the secret share for the n parties. Next, consider the secret $s \in F^*$. The secret shares of s form the affine space

$$(s, r_1, \ldots, r_k) \cdot G^+_{*,\{1,\ldots,n\}} \in F^n.$$

Observe that, one can express this affine space as

$$s \cdot \vec{v} + \langle G \rangle \subseteq F^n,$$

where $\vec{v} = G^+_{0,\{1,\ldots,n\}} \in F^n$.

To demonstrate that the Massey secret-sharing scheme corresponding to the linear code generated by a generator matrix $G^+ \in F^{(k+1)\times(n+1)}$ is vulnerable to leakage attacks, the adversary needs to present two secrets $s^{(0)}, s^{(1)} \in F$ and an (n, m) local leakage function $\vec{L}$ such that the statistical distance between the joint leakage distributions for these two secrets is large.

First Attempt. Fix an (n, m) local leakage function $\vec{L}$. Let $\vec{\ell} \in (\{0,1\}^m)^n$ be a leakage value. Let $L_i^{-1}(\ell_i) \subseteq F$ be the subset of i-th party's secret shares such that the leakage function L_i outputs $\ell_i \in \{0,1\}^m$ as output. Therefore, we have $s_i \in L_i^{-1}(\ell_i)$ if and only if $L_i(s_i) = \ell_i$. Furthermore, the leakage is $\vec{\ell}$ if and only if the secret shares $\vec{s}$ belongs to the set

$$\vec{L}^{-1}(\vec{\ell}) := L_1^{-1}(\ell_1) \times \cdots \times L_n^{-1}(\ell_n).$$

So, the probability of the leakage being $\vec{\ell}$ conditioned on the secret being $s^{(0)}$ is

$$\frac{1}{|F|^k} \cdot \left| \, s^{(0)} \cdot \vec{v} + \langle G \rangle \, \cap \, \vec{L}^{-1}(\vec{\ell}) \, \right|.$$

Similarly, the probability of the leakage being $\vec{\ell}$ conditioned on the secret being $s^{(1)}$ is

$$\frac{1}{|F|^k} \cdot \left| \, s^{(1)} \cdot \vec{v} + \langle G \rangle \, \cap \, \vec{L}^{-1}(\vec{\ell}) \, \right|.$$

The absolute value of the difference in the probabilities is, therefore, the following expression.

$$\frac{1}{|F|^k} \cdot \left| \left| s^{(0)} \cdot \vec{v} + \langle G \rangle \ \cap \ \vec{L}^{-1}(\vec{\ell}) \right| \ - \ \left| s^{(1)} \cdot \vec{v} + \langle G \rangle \ \cap \ \vec{L}^{-1}(\vec{\ell}) \right| \right|.$$

The statistical distance between the joint leakage distributions is

$$\frac{1}{2} \cdot \frac{1}{|F|^k} \sum_{\vec{\ell} \in (\{0,1\}^m)^n} \left| \left| s^{(0)} \cdot \vec{v} + \langle G \rangle \ \cap \ \vec{L}^{-1}(\vec{\ell}) \right| \ - \ \left| s^{(1)} \cdot \vec{v} + \langle G \rangle \ \cap \ \vec{L}^{-1}(\vec{\ell}) \right| \right|. \tag{1}$$

If the expression in Eq. 1 is $\leqslant \varepsilon$ for all (n, m) leakage functions $\vec{L}$ and all pairs of secrets $s^{(0)}$ and $s^{(1)}$, then the generator matrix G^+ is (m, ε)-locally leakage-resilient.

Remark 2. Observe that if one can choose $\vec{L}$ to ensure that any codeword $\vec{c} \in \langle G \rangle$ that belongs to $\vec{L}^{-1}(\vec{\ell})$ (for some $\vec{\ell}$) also has $\vec{c} + s^{(1)} \cdot \vec{v} \notin \vec{L}^{-1}(\vec{\ell})$ for some secret $s^{(1)}$, then the expression in Eq. 1 is identical to 1.

For example, if the finite field is characteristic-2, even with $m = 1$ bit leakage from each secret share, an adversary can ensure this condition. The attack works as follows. Suppose the secret s can be reconstructed by $\alpha_1 s_1 + \alpha_2 s_2 + \cdots + \alpha_k s_k$ where $\alpha_1, \ldots, \alpha_k$ are fixed field elements and s_i is the i-th secret share. The adversary leaks the least significant symbol b_i of $\alpha_i s_i$ from the i-th secret share. Afterwards, the adversary can reconstruct the least significant symbol of the secret s by computing $b_1 \oplus b_2 \oplus \cdots \oplus b_k$. This leakage attack extends to linear secret-sharing schemes over finite fields with small characteristics. More specifically, the above attack generalize to characteristic-p field when the adversary is allowed to leak $\lceil \log p \rceil$ bits from each secret share.

Recall that the number of (n, m) local leakage functions is $2^{mn \cdot |F|}$. One encounters the following hurdle while proceeding by the union bound technique to prove our result. Suppose that for every leakage function $\vec{L}$ there is one generator matrix such that the statistical distance in Eq. 1 is $> \varepsilon$. Using naïve union bound technique, one shall rule out $2^{mn \cdot |F|}$ generator matrices. However, there are only a total of $|F|^{(k+1)\times(n-k)}$ generator matrices. For the event of encountering generator matrices that are (m, ε)-locally leakage-resilient with high probability, we shall require

$$2^{mn \cdot |F|} \ll |F|^{(k+1)\cdot(n-k)} \sim 2^{kn \cdot \log_2 |F|}.$$

For simplicity, consider the minimal non-trivial case of $m = 1$ and $k = n(1 - o(1))$. Our result is impossible to prove even for this minimal non-trivial case where $|F| = p \geqslant 2^{\lambda - 1}$ and $m = 1$.

Remark 3. We note that the recent result of [39] uses a union bound technique. In their work, however, they consider physical-bit leakage functions. The total

number of physical-bit leakage functions is extremely small;[9] otherwise, their approach (despite all the exciting new technical tools) would not have worked.

Remark 4. In the active adversary setting, to the authors' best knowledge, union bound (over all possible adversaries) is the only general technique known in the literature. See, for instance, the probabilistic proofs of the existence of non-malleable extractors [19] and non-malleable codes [16,22]. The proof of [16] even employs non-linear codes (which provide significantly more degrees of freedom in designing the encoding schemes) to push a "union bound based proof" through.

A New Set of Tests. To circumvent the hurdles associated with the naïve union bound, we propose a new set of tests. We emphasize that it is *non-trivial* to prove that if a generator matrix G passes all these tests, then G^+ is (m, ε)-locally leakage-resilient. Section 3.3 elaborates this implication. The inspiration for these tests stems from the literature in pseudorandomness [53,54].[10]

Recall that $G^+ \in F^{(k+1)\times(n+1)}$ is the generator matrix of the code, and $G^+ = [I_{k+1}|P]$ is in the standard form, where $P \in F^{(k+1)\times(n-k)}$. The secret shares of secret 0 is the $[n,k]_F$-code $\langle G\rangle$. The matrix G is also in the standard form, say $G = [I_k|R]$, where $R = P_{\{1,\ldots,k\}\times\{1,\ldots,n-k\}} \in F^{k\times(n-k)}$. Then, the matrix $H = [-R^\intercal|I_{n-k}]$ generates the dual code of the code generated by the matrix $G = [I_k|R]$. We introduce the matrix H because it is easy to express our tests using the row-span of H, i.e. $\langle H\rangle$.

Fix parameters $\sigma \in [0,1]$, $\gamma \in \mathbb{N}$, and $a \in \mathbb{N}$. The set of all tests $\mathsf{Test}_{\sigma,\gamma,a}$ is defined as follows. Every test is *additionally* indexed by $(\vec{V}, J)$, where $\vec{V} = (V_1, \ldots, V_n)$, each V_i is a size-γ subset of the finite field F, and J is a size-$(1-\sigma)\cdot n$ subset of $\{1,\ldots,n\}$. A codeword $c \in F^n$ *fails the test* indexed by $(\vec{V}, J)$ if $c_j \in V_j$, for all $j \in J$.

The generator matrix H *fails the test* indexed by $(\vec{V}, J)$ if at least a^n codewords fail this test. The generator matrix H *passes* $\mathsf{Test}_{\sigma,\gamma,a}$ if H does not fail for *any* test in $\mathsf{Test}_{\sigma,\gamma,a}$.

Lemma 1 (Technical Lemma 1). *Let G^+ be the generator matrix of an $[n+1,k+1]_F$-code. Consider a Massey secret-sharing scheme corresponding to the linear code $\langle G^+\rangle$. Let $\langle G\rangle$ be the $[n,k]_F$-code formed by the set of all secret shares of the secret 0. Let $\langle H\rangle$ be the $[n,n-k]_F$-code that is the dual code of $\langle G\rangle$. Let $\mathsf{Test}_{\sigma,\gamma,a}$ be a set of tests, where $\gamma = 2^m \cdot T^2$ and $T \in \mathbb{N}$. If H passes $\mathsf{Test}_{\sigma,\gamma,a}$, $\langle H\rangle$ is an MDS code, and $\sigma \in (0, 2k/n - 1]$, then G^+ is (m,ε)-locally leakage-resilient, where*

$$\varepsilon = 2^{-(\log_2(C_m)\cdot(k/n)-\log_2(a)-h_2(\sigma))\cdot n} + 2^{-\left(\log_2(T)\cdot\sigma-\left(\sigma+k^\perp/n\right)m-h_2(\sigma)\right)\cdot n},$$

[9] For example, consider a physical-bit leakage function that leaks one bit from the field F. There are $\log_2|F|$ such functions. In comparison, there are $2^{|F|}$ general 1-bit leakage functions.

[10] Intuitively, a set whose correlation with any Fourier character is small can be interpreted as a pseudorandom object. On the other side, a large Fourier coefficient indicates a correlation with a Fourier character; thus, the object is *not* pseudorandom. In a similar spirit, as we shall explain, our tests find whether a code $\langle H\rangle$ has many codewords with large Fourier coefficients or not.

and $C_m > 1$ *is a suitable constant depending on* m.[11]

Remark 5. Note that this lemma is where we inherently need $k > n/2$. Otherwise, we are unable to pick a σ. We discuss this barrier further when we go into the proof in Remark 6 and Sect. 4.

In Sect. 3.1, we shall set the parameters properly to ensure the insecurity is negligible. There are potentially several techniques to prove this result. We prove this technical lemma using Fourier analysis in Sect. 3.3.

Most Matrices Pass the Tests. Let us do a sanity check first. The total number of tests in $\mathsf{Test}_{\sigma,\gamma,a}$ is

$$\binom{|F|}{\gamma}^n \cdot \binom{n}{(1-\sigma)n} = \Theta|F|^{\gamma \cdot n} \cdot 2^{h_2(\sigma)\cdot n}.$$

Furthermore, the total number of generator matrices G is $|F|^{k\cdot(n-k)}$. So, it is plausible that the union bound technique may work for this result.

However, naïve accounting does not suffice. Section 3.2 presents the careful accounting needed to prove the following result.

Lemma 2 (Technical Lemma 2). *Fix constant* σ, γ, a. *Let* $p \geqslant 2^{\lambda-1}$ *be a prime and* $\lim_{\lambda\to\infty} n/\lambda \in (0,1)$, *where* λ *is the security parameter. Let* G^+ *be the generator matrix of an* $[n+1, k+1]_F$*-code in the standard form such that each element of its parity check matrix is independently and uniformly chosen from* F, *where constant* $k/n \in (\sigma, 1)$. *Consider a Massey secret-sharing scheme corresponding to the linear code* $\langle G^+\rangle$. *Let* $\langle G\rangle$ *be the* $[n,k]_F$*-code formed by the set of all secret shares of the secret* 0. *Let* $\langle H\rangle$ *be the* $[n, n-k]_F$*-code that is the dual code of* $\langle G\rangle$. *Then, the following bound holds.*

$$\Pr_{G^+ \xleftarrow{\$} \mathbf{G}^+}[H \text{ is MDS and passes } \mathsf{Test}_{\sigma,\gamma,a}] = 1 - 2^{-(1-n/\lambda)\cdot\lambda} - \exp(-\Theta\lambda^3).$$

3.1 Parameter Setting for Corollary 1

Before we go into the proof of Lemmas 1 and 2, let us first show how we can set up the parameters in both lemmas to imply Corollary 1. Let us restate the corollary first.

Corollary 4. (Restatement of Corollary 1). *Fix constants* $m \in \mathbb{N}$, $\delta \in (0,1)$, *and* $\eta \in (0,1)$. *Define* $n = (1-\eta)\cdot\lambda$ *and* $k = (1/2+\delta)\cdot n$. *Let* F *be a prime field of order* $\in \{2^{\lambda-1}, \ldots, 2^\lambda - 1\}$. *For all sufficiently large* λ, *the Massey secret-sharing scheme corresponding to a random* $[n+1, k+1]_F$*-code is* (m, ε)*-locally leakage-resilient, where* $\varepsilon = \exp(-\Theta\lambda)$, *except with* $\exp(-\Theta\lambda)$ *probability.*

The sequence of parameter choices is as follows. We emphasize that all parameters below are constants.

[11] Refer to the full version [40] for the relation between m and the constant C_m.

1. We are given the number of bits leaked from each share m and the target threshold δ as constants. Therefore, $C_m > 1$ is also fixed as a constant.
2. We shall pick constants $\sigma > 0$ and $a > 1$ arbitrarily satisfying the following constraints.
   (a) $\sigma < \min(2\delta, 1/2 + \delta)$. This parameter choice ensures that $\sigma < 2k/n - 1$ and $\sigma < k/n$.
   (b) $\log_2(C_m) \cdot (1/2 + \delta) - \log_2(a) - h_2(\sigma) > 0$. This choice ensures that the first part in the expression of ε in Lemma 1 is negligible.
3. Next, we pick any constant T satisfying $\log_2(T) \cdot \sigma - (\sigma + (1/2 - \delta))\, m - h_2(\sigma) > 0$. This choice ensures that the second part in the expression of ε in Lemma 1 is negligible.
4. Since we have picked T, this implicitly fixes γ as $\gamma = 2^m \cdot T^2$.

Clearly, all the steps above are feasible, and we have now fixed all the constants involved. One can verify that all the prerequisites of Lemmas 1 and 2 are satisfied. Consequently, Lemmas 1 and 2 together imply that the Massey secret-sharing scheme corresponding to a random linear code is negligibly-insecure with overwhelming probability.

As a concrete example, suppose $m = 1$, $n = 0.97\lambda$, and $k = 0.49\lambda$. In this case $C_m = \sqrt{2}$, by setting, $\sigma = 0.01$, $a = 1.5$, and $T = 2^{50}$, one can verify that $\lambda > 2000$ ensures that we achieve 2^{-50}-insecurity.[12]

3.2 Proof of Lemma 2

The proof of Lemma 2 proceeds by a combinatorial argument. Fix a test $(\vec{V}, J)$ in the set of tests $\mathsf{Test}_{\sigma,\gamma,a}$. Consider the experiment where $G^+ \xleftarrow{\$} \mathbf{G}^+$, and $H \in F^{k^\perp \times n}$ be the matrix corresponding to G^+ as described in the statement of Lemma 2, where $k^\perp = n - k$. Our entire analysis is for this distribution of the matrix H.

Observe that $\langle H \rangle$ is a maximum distance separable (MDS) code, with high probability. We defer the proof of this claim to the full version [40].

Claim 2. *The linear codes $\langle G \rangle$ and $\langle H \rangle$ are maximum distance separable codes, except with probability (at most) $2^n/p = \exp(-\Theta\lambda)$.*

Henceforth, our analysis shall assume that G^+ is random as well as $\langle G \rangle$ and $\langle H \rangle$ are MDS (without loss of generality). Therefore $\langle G \rangle$ is an $[n, k]_F$-MDS code and $\langle H \rangle$ is an $[n, k^\perp]_F$-MDS code, where $k^\perp = n - k$. Recall that $H = [-R^\intercal | I_{n-k}]$, where every element of $-R^\intercal$ is independent and uniformly random over F.

Without loss of generality, assume that $J = \{\sigma n + 1, \sigma n + 2, \ldots, n\}$. Among the indices in J, let us fix the indices $J' = \{k+1, k+2, \ldots, n\}$ as the information set for the linear code $\langle H \rangle$.[13] Let us fix a set of witnesses $B \subseteq F^{k^\perp}$ of size a^n.

[12] For similar range of parameter choices, e.g., when n is close to λ, the dominant failure probability is the probability that a random matrix is not MDS, which is $2^{n-\lambda}$.

[13] Since $\langle H \rangle$ is MDS, we can pick any $k^\perp$ coordinates to be the information set. We choose the last $k^\perp$ coordinates (to coincide with the I_{n-k} block identity matrix of H) for simplicity. All remaining coordinates of a codeword in $\langle H \rangle$ are derived via a linear combination of the information set.

Objective. Over the distribution of $\langle H \rangle$, what is the probability that every codeword $c \in \langle H \rangle$ such that c restricted to the information set J' is in the set B fails the test $(\vec{V}, J)$? That is, compute the probability of the event "if $c_{J'} \in B$ then $c_j \in V_j$, for all $j \in J$."

Proof for a Weaker Bound. The total number of choices for $\vec{V}$ is at most $(|F|^{\gamma})^n = |F|^{\gamma \cdot n}$. The total number of choices for J is at most $\binom{n}{(1-\sigma)n} = 2^{h_2(\sigma) \cdot n}$. Finally, the total number of sets of witnesses B is at most $\binom{\gamma^{k^\perp}}{a^n}$.[14] Therefore, the total number of possibilities is

$$|F|^{\gamma \cdot n} \cdot 2^{h_2(\sigma) \cdot n} \cdot \binom{\gamma^{k^\perp}}{a^n}. \tag{2}$$

Next, fix a column index $j \in J \setminus J' = \{\sigma n + 1, \sigma n + 2, \ldots, k\}$. Pick one non-zero witness $d^{\vec{(1)}} \in B$. Over the randomness of choosing $H_{*,j}$, the random variable $d^{\vec{(1)}} \cdot H_{*,j}$ is uniformly random over the field F. So, the probability of this coordinate being in V_j is $\gamma / |F|$. This statement is true for all $j \in J \setminus J'$ independently. Therefore, for all $j \in J \setminus J'$, the probability of the j-th coordinate of the codeword $d^{\vec{(1)}} \cdot H$ being in V_j is

$$\left(\frac{\gamma}{|F|}\right)^{(1-\sigma)n-k^\perp}.$$

Now, choose a second witness $d^{\vec{(2)}} \in B$. Suppose $d^{\vec{(2)}}$ is a scalar multiple of $d^{\vec{(1)}}$. In this case, the random variables $d^{(1)} \cdot H_{*,j}$ and $d^{\vec{(2)}} \cdot H_{*,j}$ are scalar multiples of each other as well. However, if $d^{\vec{(2)}}$ is not in the span of $d^{\vec{(1)}}$, then the random variable $d^{\vec{(2)}} \cdot H_{*,j}$ is uniformly random over the field F and (most importantly) *independent* of the random variable $d^{\vec{(1)}} \cdot H_{*,j}$. Therefore, the probability of all coordinates of the codeword $d^{\vec{(2)}} \cdot H$ indexed by $j \in J \setminus J'$ being in V_j is (independently) $(\gamma/|F|)^{(1-\sigma)n-k^\perp}$. We highlight that if, indeed, the witnesses are linearly dependent then the columns are linearly dependent as well. Consequently, identifying *linearly independent* witnesses seems necessary (not merely sufficient) for our proof strategy to succeed.

Generalizing this technique, one claims the following result. We defer the proof to the full version [40].

Claim 3. *Fix any r linearly independent $d^{\vec{(1)}}, d^{\vec{(2)}}, \ldots, d^{\vec{(r)}} \in F^{k^\perp}$. For all $j \in J \setminus J'$, over the randomness of choosing $H_{*,j}$, the distribution of the random matrix*

[14] Because there are γ options for every $k^\perp$ information coordinates in $\langle H \rangle$. Among these $\gamma^{k^\perp}$ choices for the information coordinates, one can choose any a^n of them as the witness set B.

$$\left(d^{(\vec{i})} \cdot H_{*,j}\right)_{i\in\{1,2,\ldots,r\}}^{j\in J\setminus J'}$$

is identical to the uniform distribution over $F^{r\times((1-\sigma)n-k^{\perp})}$.

Consequently, the probability of all the codewords corresponding to these r linearly independent witnesses in B failing the test (V, J) is

$$\left[\left(\frac{\gamma}{|F|}\right)^{(1-\sigma)n-k^{\perp}}\right]^{r} \tag{3}$$

Now how many linearly independent witnesses can one identify among a^n witnesses of B? Towards this objective, we prove a bound similar in spirit to matrix rank lower bounds from communication complexity theory. We defer the proof to the full version [40].

Claim 4 (Rank bound for 'Bounded-Diversity' Matrices). *Let* $M \in F^{u\times v}$, *where* $u = 2^{\alpha v}$, *be an arbitrary matrix such that each row of this matrix is distinct. Suppose every column* $j \in \{1, \ldots, v\}$ *of* M *satisfies*

$$\left|\{M_{1,j}, M_{2,j}, \ldots, M_{u,j}\}\right| \leqslant \gamma.$$

Then, $rank(M) \geqslant \frac{\alpha}{\log_2 \gamma} \cdot v$.

Back to Proving Lemma 2. Construct M such that every row of M is a witness in B. Therefore, the matrix $M \in F^{u\times v}$, where $u = a^n$ and $v = k^{\perp}$. Applying Claim 4 for $u = a^n = 2^{\log_2(a)\cdot n}$ and $v = k^{\perp}$, we get $r \geqslant \frac{\log_2 a}{\log_2 \gamma} \cdot k^{\perp}$. For our end application scenario, we shall have $k^{\perp} = \Theta n$, and positive constant a and $\gamma \geqslant 2$. Therefore, we shall have $r = \Theta n$. So, the probability expression in Eq. 3 effectively behaves like $|F|^{-\Theta n^2}$. On the other hand, the total number of possibilities given by Eq. 2 are dominated by $|F|^{\gamma n}$ and $\binom{\gamma^{k^{\perp}}}{a^n} \leqslant \gamma^{k^{\perp}\cdot a^n}$. When $n \leqslant \Theta\log\lambda$, using union bound, one can conclude that the probability of a random $\langle H\rangle$ failing some test $(\vec{V}, J)$ with some witness B is $1 - \exp(-\Theta\lambda)$.

However, $n \leqslant \Theta\log\lambda$ is unacceptably small. Our objective is to achieve $n = \Theta\lambda$. In fact, we have recklessly indulged in significant over-counting. Let us fix this proof to get the desired bound.

Final Fix. Observe that we do not need to pick B of size a^n from $V_{k+1}\times\cdots\times V_n$. For any B, identify the (unique) lexicographically smallest set $\widehat{B} \subseteq B$ of r linearly independent witnesses. In the analysis presented above, we have significantly over-counted by separately considering all $B \supseteq \widehat{B}$. To fix this situation, we consider the argument below that analyzes $\widehat{B}$ to account for *all* $B \supseteq \widehat{B}$.

Now, fix the (canonical) set $\widehat{B}$ of r linearly independent witnesses. The proof above says that the probability of a random $\langle H\rangle$ failing the test $(\vec{V}, J)$ with some witness $B \supseteq \widehat{B}$ is at most $(\gamma/|F|)^{\left((1-\sigma)n-k^{\perp}\right)\cdot r}$. We emphasize that B may have more linearly independent elements; however, it is inconsequential for our

analysis. So, we need only to pick $\widehat{B}$ of size r such that the witnesses are linearly independent of each other. Consequently, the total number of possibilities of Eq. 2 drastically reduces to the following bound.

$$|F|^{\gamma \cdot n} \cdot 2^{h_2(\sigma) \cdot n} \cdot \binom{\gamma^{k^\perp}}{r}, \tag{4}$$

where $r = \frac{\log_2 a}{\log_2 \gamma} \cdot k^\perp$. Now, we can put together the total number of witnesses of Eq. 4 with the failure probability of Eq. 3 using a union bound. The probability that a random $\langle H \rangle$ fails some test $(\vec{V}, I)$ witnessed by r linearly independent witnesses in $\widehat{B}$ is at most

$$\begin{aligned}
&|F|^{\gamma \cdot n} \cdot 2^{h_2(\sigma) \cdot n} \cdot \binom{\gamma^{k^\perp}}{r} \cdot \left(\frac{\gamma}{|F|}\right)^{\left((1-\sigma)n - k^\perp\right) \cdot r} \\
\leqslant\, &|F|^{\gamma \cdot n} \cdot 2^{h_2(\sigma) n} \cdot \cancel{\gamma^{k^\perp \cdot r}} \cdot \gamma^{(1-\sigma) n \cdot r - \cancel{k^\perp \cdot r}} \cdot \frac{1}{|F|^{((1-\sigma)n - k^\perp) r}} \\
=\, &|F|^{\gamma n} \cdot 2^{h_2(\sigma) \cdot n} \cdot 2^{(1-k/n)(1-\sigma)\log_2(a) \cdot n^2} \cdot \frac{1}{|F|^{(\log_\gamma a)(1-k/n)(k/n-\sigma) \cdot n^2}}.
\end{aligned}$$

In our scenario, we have constant $k/n \in (\sigma, 1)$, constant a, and $\lim_{\lambda \to \infty} n/\lambda \in (0, 1)$. For these setting of the parameters, the numerator is dominated by the term $2^{\Theta\lambda^2}$. Furthermore, we have constant γ, so the denominator is $2^{\Theta\lambda^3}$. So, the probability expression above is $\exp(-\Omega(\lambda))$.

To summarize, we incur two forms of failures in our analysis. (1) $\langle H \rangle$ is not MDS, and (2) $\langle H \rangle$ fails some test. The probability of the first failure is $\exp(-\Theta\lambda)$, and the probability of the second failure is $\exp(-\Omega(\lambda))$.

3.3 Proof of Lemma 1

We prove Lemma 1 using Fourier analysis. The full version [40] provides the preliminaries of Fourier analysis that suffices for the proofs in this paper.

To begin, let us summarize what we are provided. We are given a fixed generator matrix $H \in F^{k^\perp \times n}$, where $k^\perp = (n - k)$. The code $\langle H \rangle$ is MDS and the matrix H passes all tests in $\mathsf{Test}_{\sigma,\gamma,a}$, where $\gamma = 2^m \cdot T^2$.

Consider any (n, m) local leakage function $\vec{L} = (L_1, \ldots, L_n)$, such that each $L_i \colon F \to \{0,1\}^m$. Our objective is to prove that this leakage function cannot distinguish the secret shares of the secret 0 from the secret 1. Fix any $i \in \{1, \ldots, n\}$ and leakage $\ell \in \{0,1\}^m$. Let $\mathbf{1}_{i,\ell} \colon F \to \{0,1\}$ be the indicator function for $L_i(s_i) = \ell$, where s_i is the secret share of party i.

Claim 5. *Let $i \in \{1, \ldots, n\}$ and $\ell \in \{0,1\}^m$. The size of the following set is at most T^2.*

$$\mathsf{Big}_{i,\ell} = \left\{ \alpha \,:\, \alpha \in F, \left| \widehat{\mathbf{1}_{i,\ell}}(\alpha) \right| \leqslant 1/T \right\}.$$

This result follows from Parseval's identity, and that function $\mathbf{1}_{i,\ell}$ has a binary output. Refer to the full version [40] for a proof of this claim. Given the leakage function $\vec{L} = (L_1, \ldots, L_n)$ and $i \in \{1, \ldots, n\}$, define the sets

$$V_i = \bigcup_{\ell \in \{0,1\}^m} \mathsf{Big}_{i,\ell}.$$

Extend each V_i arbitrarily, if needed, to be of size $\gamma = 2^m T^2$. Now, we have defined the $\vec{V} = (V_1, \ldots, V_n)$ corresponding to the leakage function $\vec{L}$.

Algebraization of Leakage-Resilience. Benhamouda et al. [7] showed that proving that the statistical distance expression in Eq. 1 is smaller than some quantity is implied by upper-bounding the analytical expression below by the same quantity. That is,

$$\begin{aligned}
&\mathsf{SD}\left(\vec{\mathbf{L}}(s^{(0)}), \vec{\mathbf{L}}(s^{(1)})\right) \\
=&\frac{1}{2} \sum_{\ell \in (\{0,1\}^m)^n} \left| \sum_{\alpha \in \langle H \rangle} \prod_{i=1}^{n} \widehat{\mathbf{1}_{i,\ell_i}}(\alpha_i) \cdot \omega^{\alpha_i \cdot s^{(0)} \cdot v_i} - \sum_{\alpha \in \langle H \rangle} \prod_{i=1}^{n} \widehat{\mathbf{1}_{i,\ell_i}}(\alpha_i) \cdot \omega^{\alpha_i \cdot s^{(1)} \cdot v_i} \right| \qquad (5) \\
\leqslant & \sum_{\vec{x} \in F^{k^\perp} \setminus \{0^{k^\perp}\}} \sum_{\vec{\ell} = (\ell_1, \ldots, \ell_n) \in (\{0,1\}^m)^n} \left| \prod_{i=1}^{n} \widehat{\mathbf{1}_{i,\ell_i}}(\vec{x} \cdot H_{*,i}) \right|. \qquad (6)
\end{aligned}$$

For completeness, we include proof of this in the full version [40]. We now proceed to upper bound this expression for an H that passes all tests in $\mathsf{Test}_{\sigma,\gamma,a}$.

Remark 6. We emphasize that the analytical expression above is only an upper bound to the statistical distance. We show that using the expression above as a proxy to analyze the exact statistical distance encounters some bottlenecks. Section 4 highlights one such bottleneck.

Upper-Bounding Eq. 6. We partition the elements $\vec{x} \in F^{k^\perp} \setminus \{0^{k^\perp}\}$ into two sets.

$$\mathsf{Bad} := \left\{ \vec{x} : \exists J \text{ s.t. } \vec{x} \neq 0^n \ \& \ \vec{x} \cdot H \text{ fails the test indexed by } (\vec{V}, J) \in \mathsf{Test}_{\sigma,\gamma,a} \right\}.$$

We emphasize that $J \subseteq \{1, 2, \ldots, n\}$ is of size $(1-\sigma)n$. The remaining elements form the subset

$$\overline{\mathsf{Bad}} = \left(F^{k^\perp} \setminus \{0^{k^\perp}\}\right) \setminus \mathsf{Bad}.$$

Next, we upper-bound the expression of Eq. 6 for elements $\vec{x} \in \mathsf{Bad}$ and $\vec{x} \in \overline{\mathsf{Bad}}$ separately.

Upper Bound: Part 1. First we consider the sum of Eq. 6 restricted to $\vec{x} \in \mathsf{Bad}$.

$$\begin{aligned}
&\sum_{\vec{x}\in\mathsf{Bad}} \sum_{\vec{\ell}\in(\{0,1\}^m)^n} \left|\prod_{i=1}^{n} \widehat{\mathbf{1}_{i,\ell_i}}(\vec{x}\cdot H_{*,i})\right| \\
&= \sum_{\vec{x}\in\mathsf{Bad}} \prod_{i=1}^{n} \sum_{\ell_i\in\{0,1\}^m} \left|\widehat{\mathbf{1}_{i,\ell_i}}(\vec{x}\cdot H_{*,i})\right| \\
&\leqslant a^n 2^{h_2(\sigma)n} \cdot \max_{\vec{x}\in\mathsf{Bad}} \prod_{i=1}^{n} \sum_{\ell_i\in\{0,1\}^m} \left|\widehat{\mathbf{1}_{i,\ell_i}}(\vec{x}\cdot H_{*,i})\right| \qquad (7)
\end{aligned}$$

The last inequality is due to the fact that there are $\binom{n}{(1-\sigma)n} = 2^{h_2(\sigma)n}$ subsets J, and each test indexed by (V, J) has at most a^n different codewords failing it.[15]

Next, fix any element $\vec{x} \in \mathsf{Bad}$. The codeword $\vec{x} \cdot H$ has $< k^\perp$ zeroes.[16] Therefore, the codeword $\vec{x} \cdot H$ has $> k$ elements from F^*. Using this property, we claim the following result.

Claim 6. *Let $\langle H\rangle$ be an $[n, n-k]_F$-MDS code, and $\vec{x} \in F^{k^\perp} \setminus \{0^{k^\perp}\}$ be an arbitrary message. Then, there exists a constant $C_m > 1$ such that*

$$\prod_{i=1}^{n} \sum_{\ell_i\in\{0,1\}^m} \left|\widehat{\mathbf{1}_{i,\ell_i}}(\vec{x}\cdot H_{*,i})\right| \leqslant C_m^{-k}.$$

We defer the proof to the full version [40]. Substituting this upper bound in Eq. 7, we get the following upper bound

$$2^{-(\log_2(C_m)\cdot(k/n)-\log_2(a)-h_2(\sigma))\cdot n}, \qquad (8)$$

which completes the first upper bound. By picking our parameters as in Sect. 3.1, this upper bound is negligibly small.

Upper Bound: Part 2. Now, it remains to upper-bound

$$\sum_{\vec{x}\in\overline{\mathsf{Bad}}} \sum_{\vec{\ell}\in(\{0,1\}^m)^n} \left|\prod_{i=1}^{n} \widehat{\mathbf{1}_{i,\ell_i}}(\vec{x}\cdot H_{*,i})\right|.$$

The crucial observation about any codeword $c = \vec{x}\cdot H \in \overline{\mathsf{Bad}}$ is the following. The number of $j \in \{1, \ldots, n\}$ such that $c_j \notin V_j$ is at least σn. For the coordinates where $c_j \notin V_j$, we utilize the fact that the magnitude of the Fourier coefficients contributed in the above expression is at most $1/T$. Based on these observations, using Fourier analysis, we prove the following bound.

[15] Since H passes all tests in the set $\mathsf{Test}_{\sigma,\gamma,a}$, at most a^n codewords fail any test indexed by $(\vec{V}, J)$.

[16] If the codeword has $k^\perp$ zeroes, we can choose their indices as the information set (because $\langle H\rangle$ is MDS). That implies that the entire codeword is 0^n, which contradicts the fact that Bad has non-zero elements.

Claim 7. *For $0 < \sigma \leqslant 1 - 2k^{\perp}/n$, the expression above is upper-bounded by*

$$2^{-\left(\log_2(T)\cdot\sigma - \left(\sigma + k^{\perp}/n\right)m - h_2(\sigma)\right)\cdot n}.$$

A proof of this claim is provided in the full version [40]. By picking our parameters as in Sect. 3.1, this upper bound is negligibly small.

Remark 7. We highlight that if we pick a σ such that $\sigma > 1 - 2k^{\perp}/n$, then naïvely using the analysis above yields an upper bound of

$$p^{k^{\perp} - (1-\sigma)n/2} \cdot 2^{-\left(\log_2(T)\cdot\sigma - \left(\sigma + k^{\perp}/n\right)m - h_2(\sigma)\right)\cdot n}.$$

The full version [40] of our paper present a proof sketch of this bound. Observe that the leading term $p^{\Theta\lambda}$ forces the choice of T to be $\omega(1)$. However, in our analysis, we crucially rely on T to be a constant.

In particular, if $2k^{\perp} > n$, no suitable σ can be choosen to avoid this bottleneck. We discuss this barrier further in Sect. 4.

4 The $k > n/2$ Barrier

In this section, we discuss why $k > n/2$ is inherently required for the current proof techniques (which are common to [7,39] and this work). In particular, we pinpoint the step where one uses Eq. 6 to upper bound the Eq. 5 as the place where this barrier arises.[17] That is, when one uses the magnitude of the Fourier coefficients to upper bound the statistical distance as

$$\sum_{\vec{x} \in F^{k^{\perp}} \setminus \{0^{k^{\perp}}\}} \quad \sum_{\vec{\ell} \in (\{0,1\}^m)^n} \left| \prod_{i=1}^{n} \widehat{\mathbf{1}_{i,\ell_i}}(\vec{x} \cdot H_{*,i}) \right|.$$

To justify our claim, we prove the following theorem.

Theorem 1. *There exists a leakage function $\vec{L}$ that leaks one bit from each share such that the following holds. Let $\langle G \rangle$ be* any *$[n,k]_F$ code such that $k < n/2$. Let $\langle H \rangle$ be the dual code of $\langle G \rangle$. The above equation is lower bounded by 1. That is,*

$$\sum_{\vec{x} \in F^{k^{\perp}} \setminus \{0^{k^{\perp}}\}} \quad \sum_{\vec{\ell} \in \{0,1\}^n} \left| \prod_{i=1}^{n} \widehat{\mathbf{1}_{i,\ell_i}}(\vec{x} \cdot H_{*,i}) \right| \gtrsim p^{(n-2k)/2} > 1.$$

Consequently, one cannot prove any meaningful upper-bound when $k < n/2$.

In fact, we identify the leakage function explicitly as follows. Define the set of *quadratic residues* as

$$\mathcal{QR} := \{\alpha \in F : \exists \beta \text{ s.t. } \beta^2 = \alpha\}.$$

[17] Note that Eq. 5 is an identity transformation of the statistical distance. Hence, the proof until this step must not produce any barriers.

Define $\vec{L} = (L_1, \ldots, L_n)$ as for all $i \in \{1, 2, \ldots, n\}$,

$$L_i(x) := \begin{cases} 1 & \text{if } x \in \mathcal{QR} \\ 0 & \text{if } x \notin \mathcal{QR} \end{cases}.$$

By standard techniques in the Fourier analysis and the well-known facts about the *quadratic Gaussian sum*, one can verify this theorem with this particular leakage function. We refer the readers to the full version [40] for a detailed proof.

5 Leakage-Resilience of Shamir's Secret-Sharing

In this section, we present our result that Shamir's secret-sharing with threshold k and n parties is leakage-resilient when $k \geqslant 0.8675n$. This improves the state-of-the-art result of Benhamouda et al. [7]. In fact, we prove a more general theorem as follows.

Theorem 2. *There exists a universal constant p_0 such that, for all finite field F of prime order $p > p_0$, the following holds. Let G^+ be an* arbitrary *MDS $[n+1, k+1]_F$ code such that $k \geqslant 0.8675n$. The Massey secret-sharing scheme corresponding to G^+ is $(1, \exp(-\Theta n)$-leakage-resilient.*

As Shamir's secret-sharing is a Massey secret-sharing scheme corresponding to the punctured Reed-Solomon codes, this theorem applies to Shamir's secret-sharing directly.

We refer the readers to the full version [40] for a detailed proof. In what follows, we present an overview of our proof. Starting from the upper bound Eq. 6, i.e.,

$$\sum_{\vec{x} \in F^{k^\perp} \setminus \{0^{k^\perp}\}} \sum_{\vec{\ell} \in \{0,1\}^n} \left| \prod_{i=1}^{n} \widehat{\mathbf{1}_{i,\ell_i}}(\vec{x} \cdot H_{*,i}) \right|,$$

our main idea is that we shall bound it with the exact information where the zeros of the codeword (from $\langle H \rangle$) are. This is motivated by the fact that the Fourier coefficient corresponds to 0 has the dominant weight.

Note that since $\langle H \rangle$ is an MDS $[n, k^\perp = n - k]_F$-code, a non-zero codeword from $\langle H \rangle$ has at most $k^\perp - 1$ zeros. For any collection of indices $A \subseteq \{1, 2, \ldots, n\}$ such that $|A| \leqslant k^\perp - 1$, let us define set

$$\mathcal{S}_A := \{\vec{x} \mid a \in A \iff \vec{x} \cdot H_{*,a} = 0\}.$$

That is, the collection of messages whose codewords satisfy that 0 appears exactly at those indices from A. Clearly, $F^{k^\perp} \setminus \left\{0^{k^\perp}\right\} = \bigcup_{A\colon |A| \leqslant k^\perp - 1} \mathcal{S}_A$. We shall break the summation based on A, i.e.,

$$\sum_{A\colon |A| \leqslant k^\perp - 1} \sum_{\vec{x} \in \mathcal{S}_A} \sum_{\vec{\ell} \in \{0,1\}^n} \left| \prod_{i=1}^{n} \widehat{\mathbf{1}_{i,\ell_i}}(\vec{x} \cdot H_{*,i}) \right|.$$

To bound each summation over some A, i.e.,

$$\Gamma_A := \sum_{\vec{x} \in \mathcal{S}_A} \sum_{\vec{\ell} \in \{0,1\}^n} \left| \prod_{i=1}^{n} \widehat{\mathbf{1}_{i,\ell_i}}(\vec{x} \cdot H_{*,i}) \right|,$$

we use the following ideas. (Refer to Fig. 2 for notations.)

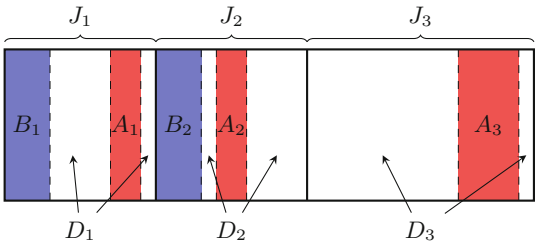

Fig. 2. The dual generator matrix $H \in F^{k^\perp \times n}$. We pick the first $k^\perp$ columns as J_1 and the second $k^\perp$ columns as J_2. Let J_3 be the rest of the columns. The set of columns $A = A_1 \cup A_2 \cup A_3$ is exactly where the codeword will be 0. We pick B_1 and B_2 to ensure that $|B_1| + |A| = |B_2| + |A| = k^\perp$.

We know the codewords are 0 at columns in $A = A_1 \cup A_2 \cup A_3$ and non-zero at columns outside A. Since $\vec{x} \cdot H_{*,a} = 0$ for $a \in A$, bounding over columns from A can be easily handled. Next, we shall use the worst-case bound to bound the summation over columns from $D_1 \cup D_2 \cup D_3$. Finally, for the columns of B_1 and B_2, we let them enumerate all possibilities from F^* and bound them appropriately.

We refer the readers to the full version [40] for the subtleties in the proof. Overall, we are able to prove that

$$\Gamma_A \leqslant \left(\frac{\pi}{2}\right)^{-(|A|+2k-n)}.$$

Finally, our upper bound is now

$$\leqslant \sum_{A\colon |A| \leqslant k^\perp - 1} \left(\frac{\pi}{2}\right)^{-(|A|+2k-n)} = \sum_{i=0}^{k^\perp - 1} 2^{n\left[h_2(i/n) - (i/n + 2k/n - 1)\log_2\left(\frac{\pi}{2}\right)\right]}.$$

Suppose $k/n = \sigma$, it suffices to ensure that

$$\max_{q \in [0, 1-\sigma)} \; h_2(q) - (q + 2\sigma - 1)\log_2(\pi/2) < 0.$$

We prove that $\sigma \geqslant 0.8675$ suffices, which completes the proof of the theorem.

References

1. Abarzúa, R., Valencia, C., López, J.: Survey for performance & security problems of passive side-channel attacks countermeasures in ECC. Cryptology ePrint Archive, Report 2019/010 (2019). https://eprint.iacr.org/2019/010
2. Adams, D.Q., Nguyen, H.H., Nguyen, M.L., Paskin-Cherniavsky, A., Suad, T., Wang, M.: Lower bounds for leakage-resilient secret sharing schemes against probing attacks. Manuscript (2021)
3. Aggarwal, D., et al.: Stronger leakage-resilient and non-malleable secret sharing schemes for general access structures. In: Boldyreva, A., Micciancio, D. (eds.) CRYPTO 2019, Part II. LNCS, vol. 11693, pp. 510–539. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-26951-7_18
4. Arora, S., Barak, B.: Computational Complexity: A Modern Approach. Cambridge University Press, Cambridge (2009)
5. Avanzi, R.M.: Side channel attacks on implementations of curve-based cryptographic primitives. Cryptology ePrint Archive, Report 2005/017 (2005). http://eprint.iacr.org/2005/017
6. Badrinarayanan, S., Srinivasan, A.: Revisiting non-malleable secret sharing. In: Ishai, Y., Rijmen, V. (eds.) EUROCRYPT 2019, Part I. LNCS, vol. 11476, pp. 593–622. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-17653-2_20
7. Benhamouda, F., Degwekar, A., Ishai, Y., Rabin, T.: On the local leakage resilience of linear secret sharing schemes. In: Shacham, H., Boldyreva, A. (eds.) CRYPTO 2018, Part I. LNCS, vol. 10991, pp. 531–561. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-96884-1_18
8. Benhamouda, F., Degwekar, A., Ishai, Y., Rabin, T.: On the local leakage resilience of linear secret sharing schemes. Cryptology ePrint Archive, Report 2019/653 (2019). https://eprint.iacr.org/2019/653
9. Benhamouda, F., Degwekar, A., Ishai, Y., Rabin, T.: On the local leakage resilience of linear secret sharing schemes. J. Cryptology **34**(2), 10 (2021)
10. Bhunia, S., Tehranipoor, M.: Hardware Security: A Hands-on Learning Approach. Morgan Kaufmann, San Francisco (2018)
11. Bishop, A., Pastro, V., Rajaraman, R., Wichs, D.: Essentially optimal robust secret sharing with maximal corruptions. In: Fischlin, M., Coron, J.-S. (eds.) EUROCRYPT 2016, Part I. LNCS, vol. 9665, pp. 58–86. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-49890-3_3
12. Blake, I.F., Seroussi, G., Smart, N.P.: Advances in Elliptic Curve Cryptography, vol. 317. Cambridge University Press, Cambridge (2005)
13. Bogdanov, A., Ishai, Y., Srinivasan, A.: Unconditionally secure computation against low-complexity leakage. In: Boldyreva, A., Micciancio, D. (eds.) CRYPTO 2019, Part II. LNCS, vol. 11693, pp. 387–416. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-26951-7_14
14. Candel, G., Géraud-Stewart, R., Naccache, D.: How to compartment secrets. In: Laurent, M., Giannetsos, T. (eds.) WISTP 2019. LNCS, vol. 12024, pp. 3–11. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-41702-4_1
15. Chattopadhyay, E., et al.: Extractors and secret sharing against bounded collusion protocols. In: 61st FOCS, pp. 1226–1242. IEEE Computer Society Press, November 2020
16. Cheraghchi, M., Guruswami, V.: Capacity of non-malleable codes. In: Naor, M. (ed.) ITCS 2014, pp. 155–168. ACM, January 2014

17. Cohen, H., et al. (eds.): Handbook of Elliptic and Hyperelliptic Curve Cryptography. Chapman and Hall/CRC, Boca Raton (2005)
18. Dau, H., Duursma, I.M., Kiah, H.M., Milenkovic, O.: Repairing reed-solomon codes with multiple erasures. IEEE Trans. Inf. Theory **64**(10), 6567–6582 (2018)
19. Dodis, Y., Wichs, D.: Non-malleable extractors and symmetric key cryptography from weak secrets. In: Mitzenmacher, M. (ed.) 41st ACM STOC, pp. 601–610. ACM Press, May/June (2009)
20. Fan, J., Guo, X., De Mulder, E., Schaumont, P., Preneel, B., Verbauwhede, I.: State-of-the-art of secure ECC implementations: a survey on known side-channel attacks and countermeasures. In: Plusquellic, J., Mai, K. (eds.) HOST 2010, Proceedings of the 2010 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), Anaheim Convention Center, California, USA, 13–14 June 2010, pp. 76–87. IEEE Computer Society (2010)
21. Fan, J., Verbauwhede, I.: An updated survey on secure ECC implementations: attacks, countermeasures and cost. In: Naccache, D. (ed.) Cryptography and Security: From Theory to Applications. LNCS, vol. 6805, pp. 265–282. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-28368-0_18
22. Faust, S., Mukherjee, P., Venturi, D., Wichs, D.: Efficient non-malleable codes and key-derivation for poly-size tampering circuits. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 111–128. Springer, Heidelberg (2014)
23. Fehr, S., Yuan, C.: Towards optimal robust secret sharing with security against a rushing adversary. In: Ishai, Y., Rijmen, V. (eds.) EUROCRYPT 2019, Part III. LNCS, vol. 11478, pp. 472–499. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-17659-4_16
24. Fehr, S., Yuan, C.: Robust secret sharing with almost optimal share size and security against rushing adversaries. In: Pass, R., Pietrzak, K. (eds.) TCC 2020, Part III. LNCS, vol. 12552, pp. 470–498. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-64381-2_17
25. Goldreich, O., Micali, S., Wigderson, A.: How to play any mental game or a completeness theorem for protocols with honest majority. In: Aho, A. (ed.) 19th ACM STOC, pp. 218–229. ACM Press, May 1987
26. Goyal, V., Kumar, A.: Non-malleable secret sharing. In: Diakonikolas, I., Kempe, D., Henzinger, M. (eds.) 50th ACM STOC, pp. 685–698. ACM Press, June 2018
27. Guruswami, V., Rawat, A.S.: MDS code constructions with small sub-packetization and near-optimal repair bandwidth. In: Klein, P.N. (ed.) 28th SODA, pp. 2109–2122. ACM-SIAM, January 2017
28. Guruswami, V., Wootters, M.: Repairing reed-solomon codes. In: Wichs, D., Mansour, Y. (eds.) 48th ACM STOC, pp. 216–226. ACM Press, June 2016
29. Guruswami, V., Wootters, M.: Repairing reed-solomon codes. IEEE Trans. Inf. Theory **63**(9), 5684–5698 (2017)
30. Hazay, C., Ishai, Y., Marcedone, A., Venkitasubramaniam, M.: LevioSA: lightweight secure arithmetic computation. In: Cavallaro, L., Kinder, J., Wang, X., Katz, J., (eds.) ACM CCS 2019, pp. 327–344. ACM Press, November 2019
31. Hazay, C., Venkitasubramaniam, M., Weiss, M.: The price of active security in cryptographic protocols. In: Canteaut, A., Ishai, Y. (eds.) EUROCRYPT 2020, Part II. LNCS, vol. 12106, pp. 184–215. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-45724-2_7
32. Kalai, Y.T., Reyzin, L.: A survey of leakage-resilient cryptography. In: Goldreich, O. (ed.) Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali, pp. 727–794. ACM (2019)

33. Kocher, P.C.: Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In: Koblitz, N. (ed.) CRYPTO 1996. LNCS, vol. 1109, pp. 104–113. Springer, Heidelberg (1996). https://doi.org/10.1007/3-540-68697-5_9
34. Kocher, P., Jaffe, J., Jun, B.: Differential power analysis. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 388–397. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-48405-1_25
35. Koeune, F., Standaert, F.-X.: A tutorial on physical security and side-channel attacks. In: Aldini, A., Gorrieri, R., Martinelli, F. (eds.) FOSAD 2004-2005. LNCS, vol. 3655, pp. 78–108. Springer, Heidelberg (2005). https://doi.org/10.1007/11554578_3
36. Kumar, A., Meka, R., Sahai, A.: Leakage-resilient secret sharing against colluding parties. In: Zuckerman, D. (ed.) 60th FOCS, pp. 636–660. IEEE Computer Society Press, November 2019
37. Lin, F., Cheraghchi, M., Guruswami, V., Safavi-Naini, R., Wang, H.: Leakage-resilient secret sharing in non-compartmentalized models. In: Kalai, Y.T., Smith, A.D., Wichs, D. (eds.) ITC 2020, pp. 7:1–7:24. Schloss Dagstuhl, June 2020
38. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error Correcting Codes, vol. 16. Elsevier, New York (1977)
39. Maji, H.K., Nguyen, H.H., Paskin-Cherniavsky, A., Suad, T., Wang, M.: Leakage-resilience of the Shamir secret-sharing scheme against physical-bit leakages. In: Canteaut, A., Standaert, F.-X. (eds.) EUROCRYPT 2021. LNCS, vol. 12697, pp. 344–374. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-77886-6_12
40. Maji, H.K., Paskin-Cherniavsky, A., Suad, T., Wang, M.: Constructing locally leakage-resilient linear secret-sharing schemes (2021). https://www.cs.purdue.edu/homes/hmaji/papers/MPSW21.pdf
41. Manurangsi, P., Srinivasan, A., Vasudevan, P.N.: Nearly optimal robust secret sharing against rushing adversaries. In: Micciancio, D., Ristenpart, T. (eds.) CRYPTO 2020, Part III. LNCS, vol. 12172, pp. 156–185. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-56877-1_6
42. Mardia, J., Bartan, B., Wootters, M.: Repairing multiple failures for scalar MDS codes. IEEE Trans. Inf. Theory **65**(5), 2661–2672 (2019)
43. Massey, J.L.: Some applications of code duality in cryptography. Mat. Contemp. **21**, 187–209 (2001). 16th
44. Nielsen, J.B., Simkin, M.: Lower bounds for leakage-resilient secret sharing. In: Canteaut, A., Ishai, Y. (eds.) EUROCRYPT 2020, Part I. LNCS, vol. 12105, pp. 556–577. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-45721-1_20
45. O'Donnell, R.: Analysis of Boolean Functions (2014)
46. Oswald, E., Preneel, B.: A survey on passive side-channel attacks and their countermeasures for the nessie public-key cryptosystems. NESSIE public reports (2003). https://www.cosic.esat.kuleuven.ac.be/nessie/reports
47. Pietrzak, K.: Cryptography from learning parity with noise. In: International Conference on Current Trends in Theory and Practice of Computer Science (2012)
48. Randolph, M., Diehl, W.: Power side-channel attack analysis: a review of 20 years of study for the layman. Cryptography **4**(2), 15 (2020)
49. Regev, O.: The learning with errors problem
50. Sayakkara, A.P., Le-Khac, N.-A., Scanlon, M.: A survey of electromagnetic side-channel attacks and discussion on their case-progressing potential for digital forensics. Digit. Investig. **29**, 43–54 (2019)

51. Srinivasan, A., Vasudevan, P.N.: Leakage resilient secret sharing and applications. In: Boldyreva, A., Micciancio, D. (eds.) CRYPTO 2019, Part II. LNCS, vol. 11693, pp. 480–509. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-26951-7_17
52. Tamo, I., Ye, M., Barg, A.: Optimal repair of reed-solomon codes: achieving the cut-set bound. In Umans, C. (ed.) 58th FOCS, pp. 216–227. IEEE Computer Society Press, October 2017
53. Tao, T.: Higher order Fourier analysis. Citeseer
54. Vadhan, S.P., et al.: Pseudorandomness, vol. 7. Now Delft (2012)
55. Yao, A.C.-C.: Protocols for secure computations (extended abstract). In: 23rd FOCS, pp. 160–164. IEEE Computer Society Press, November 1982
56. Zhou, Y., Feng, D.: Side-channel attacks: ten years after its publication and the impacts on cryptographic module security testing. Cryptology ePrint Archive, Report 2005/388 (2005). http://eprint.iacr.org/2005/388