Leakage-resilient Linear Secret-sharing against arbitrary Bounded-size Leakage Family

Abstract. Side-channel attacks on threshold secret-sharing schemes have revealed partial information about the secrets, in turn compromising any cryptographic primitives built using them. Leakage-resilient cryptography studies the construction of cryptographic primitives and their vulnerability to such unintentional information revelation. For example, in the context of secure computation, linear leakage-resilient secret-sharing schemes naturally facilitate the leakage-resilient addition of secrets. However, the leakage-resilient secure multiplication requires $k/n < 0.5$, where k is the reconstruction threshold and n is the total number of secret shares. Motivated by leakage-resilient secure computation of circuits with addition and multiplication gates, this work studies the leakage-resilience of Massey secret-sharing schemes corresponding to linear codes with small reconstruction thresholds against a family of joint leakage attacks, i.e., the leakage function can leak *global* information from all secret shares.

Even against the highly restrictive class of *local* leakage attacks, where the leakage functions perform independent leakage from each secret share, the leakage-resilience of linear secret-sharing schemes with $k/n < 0.5$ is not well-understood. Benhamouda, Degwekar, Ishai, and Rabin (Journal of Cryptology–2021) proved the leakage-resilience of Shamir secret-sharing scheme against one-bit local leakage from each secret share when $k/n > 0.8$. Maji, Paskin-Cherniavsky, Suad, and Wang (CRYPTO–2021) proved that the Massey secret-sharing scheme corresponding to a random linear code is leakage-resilient to one-bit local leakage when $k/n > 0.5$. In the small reconstruction threshold regime, Maji, Paskin-Cherniavsky, Nguyen, Suad, and Wang (EUROCRYPT–2021) proved that the Shamir secret-sharing scheme with random evaluation places is leakage-resilient to physical-bit leakage (with high probability) for any $k \geqslant 2$, which makes them useful for leakage-resilient secure multiplication. However, handling more sophisticated leakages seems challenging because Maji, Paskin-Cherniavsky, Suad, and Wang (CRYPTO–2021) demonstrate the shortcomings of the state-of-the-art techniques against the *specific* local leakage attack that leaks the quadratic residuosity of each secret share; unless $k/n > 0.5$.

Our work, first, characterizes the leakage-resilience of linear secret sharing schemes against *bounded-size* (possibly global) leakage families. Let λ be the security parameter and F be a finite field (possibly of composite order), whose size is roughly 2^{λ}. Fix any family $\mathcal{L}$ of ℓ-bit leakage-attacks of size at most $|F|^{k-2-c}/8^{\ell}$, for any positive constant c. This paper proves that the Massey secret-sharing scheme corresponding to a random linear code over F of dimension $(k+1)$ is leakage-resilient against every leakage attack in the family $\mathcal{L}$, except with an exponentially small probability in λ. In particular, $k = 3$ suffices when $\mathcal{L}$ is the singleton set containing the quadratic residuosity local leakage or $\mathcal{L}$ is the set of all physical-bit leakage functions. Furthermore, when $\mathcal{L}$ is the family of all NC^0-local leakage attacks, which subsumes physical-bit leakage attacks, any $k = \omega(n/\lambda)$ suffices (ignoring a $\log \lambda$ multiplicative factor). As long as the reconstruction threshold $k \leqslant \sqrt{n}$, one can use these secret-sharing schemes to multiply secrets securely. Our result is *near-optimal* because there is a (global) leakage family of size $|F|^{k+1}$ and $\ell = 1$ that breaks the leakage-resilience of the Massey secret-sharing scheme corresponding to any dimension-$(k+1)$ linear code.

Finally, our work presents a tight Fourier-analytic analysis of the "parity-of-parity" local leakage attack proposed by Maji, Paskin-Cherniavsky, Nguyen, Suad, and Wang (EUROCRYPT–2021), which leaks one physical bit from every secret share. We show that the reconstruction threshold of the additive secret-sharing scheme must be $\Omega(\log \lambda)$ to be leakage-resilient to this attack; improving the best previous bound of $\Omega(\log \lambda / \log \log \lambda)$. The proof proceeds by tightly estimating an exponential sum. This result yields a local leakage family of size $|F|^{k+1}$ such that the leakage-resilience of the Massey secret-sharing scheme corresponding to any dimension-$(k+1)$ linear code must satisfy $k = \Omega(\log \lambda)$.

1 Introduction

Traditionally, the security of cryptographic primitives assumes cryptosystems as impervious black-boxes, faithfully realizing the desired input-output behavior while providing no additional information. Real-world implementations, however, do not always maintain this idealized assumption. Innovative side-channel attacks starting with the seminal works of [20, 21] have repetitively found success in obtaining partial information on the secret states. These diverse side-channel attacks pose significant threats to the security of underlying cryptographic primitives and all the cryptographic constructions that rely on them.

Towards resolving such concerns, one could develop ad hoc countermeasures for every existing side-channel attack. This approach, however, is unable to address the threat of unknown attacks. On the other hand, leakage-resilient cryptography aims to define potential avenues of information leakages formally and provide provable security guarantees against all such information leakages, even including the unforeseen ones. In the last few decades, a large body of influential works has studied the feasibility and efficiency of leakage-resilient cryptography against various models of potential leakages. We refer the readers to the excellent survey [19] for more details.

Secret-sharing schemes, a fundamental primitive in cryptography that is essential to all threshold cryptography constructions, are also threatened by such leakage attacks. The standard security of secret-sharing schemes guarantees that, given the (entire) secret shares of any unauthorized set of parties, one cannot learn any information about the secret. However, the security of the secret is not apparent if an adversary obtains (partial) information from every secret share. Such potential loss in security may percolate to cryptographic constructions built using these vulnerable secret-sharing schemes.

Application: Leakage-resilient secure computation. For example, secret-sharing schemes are commonplace in *secure multi-party computation* schemes that privately compute over private data using the GMW-technique [14]. Linear secret-sharing schemes naturally enable the secure addition of secrets. Secure multiplication of secrets typically uses multiplication-friendly secret-sharing schemes (for example, Shamir's secret-sharing scheme [33] and secret-sharing schemes based on other Goppa codes [28, 15, 13, 11]) or, more generally, some restrictive versions of linear secret-sharing schemes. Multiplication-friendly secret-sharing schemes require the reconstruction threshold k to be less than half the number of parties n to facilitate secure multiplication. More generally, linear secret-sharing schemes facilitate secure multiplication when $k \leqslant \sqrt{n}$. If the secret-sharing scheme used in the secure computation is leakage-resilient, then the resulting computation is itself leakage-resilient. Motivated by this application in leakage-resilient secure computation involving the addition and multiplication of secrets, our work studies the leakage-resilience of *linear secret-sharing schemes* with a *small reconstruction threshold*.

State-of-the-art. Initiated by Benhamouda, Degwekar, Ishai, and Rabin [5], many recent works [29, 25, 26, 1] study the leakage-resilience of linear secret-sharing schemes against *local leakage* attacks. In the local leakage model, the adversary picks an independent leakage function for each secret share. The final leakage is the union of the local leakages from every secret share. Even for this restrictive model, our understanding of the leakage-resilience of secret-sharing schemes is still far from complete.

Benhamouda, Degwekar, Ishai, and Rabin [6] proved that k-out-of-n Shamir secret-sharing is locally leakage-resilient when $k/n > 0.8$. Maji, Paskin-Cherniavsky, Suad, and Wang [26] proved that the Massey secret-sharing scheme [28] corresponding to a random linear code of dimension-$(k + 1)$ is locally leakage-resilient with overwhelming probability when $k/n > 0.5$. Since these secret-sharing schemes require $k/n > 0.5$ to achieve leakage-resilience, they cannot facilitate the secure multiplication of secrets as motivated above. Furthermore, Maji et al. [26] pointed out an inherent barrier when $k/n < 0.5$ for existing works' Fourier-analytic technical approaches. In particular, they pinpoint a local leakage function that leaks the quadratic residuosity of every secret share, and existing Fourier-analytic approaches cannot even prove leakage-resilience against this single function when $k/n < 0.5$. Proving the leakage-resilience against the quadratic residuosity leakage when $k/n < 0.5$ shall require a significantly different technical approach, which is one of the technical contributions of our current work.

Maji, Nguyen, Paskin-Cherniavsky, Suad, and Wang [25] consider the natural physical-bit leakage family in the small reconstruction threshold regime. In this model, the secret shares are stored in their natural binary representation, and the leakage function can learn physical bits stored at specified locations. [25] proved that Shamir secret-sharing with random evaluation places is leakage-resilient to the physical-bit leakage even for the most stringent reconstruction threshold $k = 2$ (and polynomially large n). However, their approach still follows the Fourier-analytic approach. Consequently, one cannot hope to extend their result to any family of leakage functions containing the quadratic residuosity leakage.

Summary of our results and technical contribution. This work studies the construction of leakage-resilience secret-sharing schemes and the analysis of leakage attacks on secret-sharing schemes. (I) This work studies the *general leakage-resilience* of the Massey secret-sharing scheme corresponding to a random linear code, i.e., the leakage function can leak global information from all secret shares, and (II) Our work quantifies the distinguishing advantage of the *parity-of-parity* local leakage attack on linear secret-sharing schemes proposed by Maji et al. [25].

First, we show that the Massey secret-sharing scheme corresponding to a random linear code is leakage-resilient to any bounded-size family of (joint) leakage functions, except with an exponentially small probability. For example, one can consider the family of leakage functions containing all physical-bit leakages, NC^0 leakages, and circuits of bounded size. In the context of leakage-resilient secure computation, we also consider a collusion of adversarial parties who (in addition to their respective secret shares) obtain leakage on the honest parties' secret shares. Our result is near-optimal as evidenced by the leakage attack family presented in Remark 1. We also present a partial derandomization of this Monte-Carlo construction using a variant of the Wozencraft ensemble. Technically, we prove our results using a purely combinatorial argument and the second-moment technique. This argument is a significant departure from existing works [5, 25, 26] as all of them rely on a Fourier-analytic approach to prove leakage-resilience. In particular, our technical approach bypasses the bottleneck result from the quadratic residuosity local leakage function, as indicated by [26].

Next, we prove that the parity of "the parity of each secret share" in the additive secret-sharing scheme has $\varepsilon^* = \exp(-\Theta(k))$ advantage in distinguishing two specific secrets, irrespective of the finite field – positively resolving a conjecture of Maji et al. [25] based on empirical data. This local physical bit leakage attack was proposed by Maji et al. [25], and [1] made partial progress towards bounding this attack's advantage by showing an $\exp(-\Theta(k \log k))$ lower bound for the advantage. Our result proves the optimality of the parity-of-parity attack because the additive secret-sharing scheme over a large prime field is known to be at most $\Theta(\varepsilon^*)$-insecure against any one-bit local leakage attack [5]. Technically, the proof of this result proceeds by Fourier analysis and a tight estimation of an appropriate exponential sum.

1.1 Our Contribution

This section introduces some notations to facilitate the introduction of our results. Let λ denote the security parameter, the number of bits in the secret shares of every party. Let F be a finite field such that $2^{\lambda-1} \leqslant |F| < 2^{\lambda}$. We emphasize that F may have a composite order. The number of parties $n = \mathsf{poly}(\lambda)$ and threshold $k = \mathsf{poly}(\lambda)$.

Leakage-resilient secret-sharing. Consider a secret-sharing scheme among n parties, where every secret share is an element in F. An *ℓ-bit leakage function* is any function $L\colon F^n \to \{0,1\}^\ell$. That is, L takes all the secret shares as input and outputs an ℓ-bit (joint) leakage. For any ℓ-bit leakage function L and any secret $s \in F$, we define $\mathbf{L}(s)$ as the distribution of the leakage when one applies L to the secret shares of s. A secret-sharing scheme is ε-leakage-resilient against L if for all secrets $s^{(0)}$ and $s^{(1)}$, the statistical distance between the leakage joint distributions $\mathbf{L}\left(s^{(0)}\right)$ and $\mathbf{L}\left(s^{(1)}\right)$ is (at most) ε. Finally, let $\mathcal{L}$ be a collection of some ℓ-bit leakage functions. A secret-sharing scheme is an *$(\mathcal{L},\varepsilon)$-leakage-resilient secret-sharing scheme* if it is ε-leakage-resilient against every leakage function $L \in \mathcal{L}$.

Linear code. A linear code $C \subseteq F^{(n+1)}$ is a linear subspace. Suppose the dimension of C is $k+1$. A matrix $G^+ \in F^{(k+1)\times(n+1)}$ is a *generator matrix* of C if the rows of G^+ span the subspace C. The generator matrix G^+ is in the *standard form* if $G^+ = [I_{k+1}|P]$. That is, the first $k+1$ columns of G^+ is the identity matrix. We refer to P as the *parity-check matrix*.

Massey secret-sharing schemes. Given a linear code $C \subseteq F^{(n+1)}$, the Massey secret-sharing scheme [28] corresponding to a code C is defined as follows. For a secret $s \in F$, one samples a random codeword $(s_0, s_1, \ldots, s_n) \in C$ such that $s_0 = s$. For $i \in \{1,2,\ldots,n\}$, the i^{th} secret share is $s_i \in F$.

Result I: Leakage-resilience of random linear codes. We prove the following theorem regarding the leakage-resilience of a random linear code.

Theorem 1 (Technical Result). *Let $\mathcal{L}$ be a family of ℓ-bit (joint) leakage functions and F be a finite field (possibly, of composite order). Let $n,k \in \mathbb{N}$ be arbitrary parameters such that $k < n$. Define $\mathbf{G}^+ = [I_{k+1}|\mathbf{P}]$ as a random variable over the sample space $F^{(k+1)\times(n+1)}$, where every element of $\mathbf{P} \in F^{(k+1)\times(n-k)}$ is sampled independently and uniformly at random from the field F. The Massey secret-sharing scheme corresponding to $\mathbf{G}^+$ is $(\mathcal{L},\varepsilon)$-leakage-resilient* except *with probability (at most)*

$$\frac{8^\ell}{\varepsilon^2} \cdot \frac{|\mathcal{L}|}{|F|^{k-2}}.$$

In particular, if $\varepsilon = \left(8^\ell \cdot |\mathcal{L}|/|F|^{k-2}\right)^{1/3}$, then this failure probability is also at most ε.

Observe that the randomness complexity of this Monte-Carlo construction for leakage-resilient secret-sharing scheme is $\mathcal{O}(k \cdot (n-k) \cdot \lg|F|)$ bits. Next, we interpret our technical result via a sequence of corollaries.

Corollary 1. *Let $c > 0$ be an arbitrary positive constant. Let $\mathcal{L}$ be an arbitrary ℓ-bit leakage family such that*

$$|\mathcal{L}| \leqslant |F|^{k-2-c}/8^\ell.$$

Let F be a finite field such that $2^{\lambda-1} \leqslant |F| < 2^\lambda$, and $n,k = \mathsf{poly}(\lambda)$. Then, the Massey secret-sharing scheme corresponding to $\mathbf{G}^+$ is $(\mathcal{L}, \exp(-\Omega(\lambda)))$-leakage-resilient except with probability $\exp(-\Omega(\lambda))$.

We remark that for a small leakage family $\mathcal{L}$, such as the physical-bit leakage family, any constant n and $k = 3$ suffices to ensure leakage-resilience. For the Massey secret-sharing scheme corresponding to an arbitrary linear code, having a small reconstruction threshold is desirable in the following two ways.

First, when $n > (k+1)^2$, parties can locally transform the secret shares of two secrets into the secret shares of their product. This enables secret-sharing-based multiparty computation protocols to do secure multiplication. Supporting Material B provides more discussion on the local transformation of secret shares.

Second, when we consider malicious parties who may not report their shares honestly, reconstructing the secret is significantly challenging. In fact, decoding erroneous random linear code is believed to be computationally hard [31, 32]. However, if k is a constant, one can efficiently decode using (exhaustive search-based) majority voting techniques. Supporting Material D provides additional discussion on this efficiency aspect.

Remark 1. Our result is near-optimal as follows. Define $\mathcal{L}^*$ as the set of all leakage functions defined by $(S, \alpha_1, \alpha_2, \dots, \alpha_{k+1})$, where $S = \{i_1, i_2, \dots, i_{k+1}\} \subseteq \{1, 2, \dots, n\}$, and $\alpha_1, \dots \alpha_{k+1} \in F$. The $(\ell = 1)$-bit leakage function corresponding to $(S, \alpha_1, \dots, \alpha_{k+1})$ indicates whether

$$\alpha_1 \cdot s_{i_1} + \alpha_2 \cdot s_{i_2} + \cdots + \alpha_{k+1} \cdot s_{i_{k+1}} = 0,$$

or not. Here $s_{i_1}, \dots, s_{i_{k+1}}$ represents the i_1-th, …, i_{k+1}-th secret share, respectively. The size of this leakage family is $\mathcal{O}\left(n^{k+1} \cdot |F|^{k+1}\right)$.

For any Massey secret-sharing scheme corresponding to the linear code generated by $[I_{k+1}|P]$, there is a leakage function in the family $\mathcal{L}$ that can distinguish the secret $s^{(0)} = 0$ from the secret $s^{(1)} = 1$. Given the generator matrix $[I_{k+1}|P]$ there are (at most) $k+1$ columns $i_1, \dots, i_{k+1}$ that span the generator matrix's 0-th column. Therefore, there exists a linear reconstruction $\alpha_1 \cdot s_{i_1} + \cdots + \alpha_{k+1} \cdot s_{i_{k+1}}$ for the secret. The leakage function corresponding to $(S = \{i_1, \dots, i_{k+1}\}, \alpha_1, \dots, \alpha_{k+1})$ distinguishes the secret $s^{(0)} = 0$ from any $s^{(1)} \in F^*$ (for example, $s^{(1)} = 1$).

In comparison, we show that G^+ is leakage-resilient to any family $\mathcal{L}$ if $|\mathcal{L}| \leqslant |F|^{k-2-c}$ for an arbitrary constant $c > 0$. The near optimality of our result follows from the fact that $n = \mathsf{poly}(\lambda)$ and $|F| \approx 2^\lambda$.

Next, we interpret our result in context of the motivating example of leakage-resilient secure computation. Suppose t parties participating in the secure computation protocol collude and obtain additional one-bit physical-bit local leakage on the secret shares of the remaining honest parties. The total number of bits leaked is

$$\ell = t \cdot \lambda + (n - t) \leqslant t\lambda + n.$$

The total number of leakage functions is

$$|\mathcal{L}| = \binom{n}{t} \cdot \lambda^{n-t} \leqslant 2^n \cdot \lambda^n.$$

Therefore, $k = \omega(n \log \lambda/\lambda)$ and $t \leqslant k/3 - c'$ ensures that $|\mathcal{L}| \leqslant |F|^{k-2-c}/8^{\ell}$, for any positive constant c'. The following corollary summarizes this result.

Corollary 2. *Let $\mathcal{L}$ be leakage family that leaks t secret shares in the entirety and one physical-bit from the remaining shares. Let F be a finite field such that $2^{\lambda-1} \leqslant |F| < 2^{\lambda}$, and $n, k = \mathsf{poly}(\lambda)$. Massey secret-sharing scheme corresponding to $\mathbf{G}^{+}$ is $(\mathcal{L}, \exp(-\Omega(\lambda)))$-leakage-resilient except with $\exp(-\Omega(\lambda))$ probability if we have*

$$k = \omega(n \log \lambda/\lambda) \qquad \text{and} \qquad t \leqslant k/3 - c',$$

where c' is an arbitrary constant.

Next, we interpret our result in the context of more sophisticated local leakage attacks. We omit the discussion on the scenario when the adversary leaks some secret shares in the entirety as it can be handled similarly as the previous discussion. In particular, we consider the local leakage attack where every local leakage function is a small circuit. These circuits take the λ-bit binary representation of F as input. We consider two natural families of circuits.

Local leakage with bounded-depth circuits. Let NC^0_d be the set of circuits with depth at most d. The size of NC^0_d is upper-bounded by $\binom{\lambda}{2^d} \cdot 2^{2^d}$. Let $\mathcal{L}$ be the local leakage family where every local leakage function is NC^0_d that leaks one bit. Then, the size of $\mathcal{L}$ is upper-bounded by $\left(\binom{\lambda}{2^d} \cdot 2^{2^d}\right)^n$. Consequently, the prerequisite of Corollary 1 holds (for all constant d) as long as $k = \omega(n \log \lambda/\lambda)$. Hence, we have the following corollary.

Corollary 3. *Let $\mathcal{L}$ be the local leakage family where every local leakage function is NC^0 that leaks one bit. Let F be a finite field such that $2^{\lambda-1} \leqslant |F| < 2^{\lambda}$, and $n, k = \mathsf{poly}(\lambda)$. Massey secret-sharing scheme corresponding to $\mathbf{G}^{+}$ is $(\mathcal{L}, \exp(-\Omega(\lambda)))$-leakage-resilient except with $\exp(-\Omega(\lambda))$ probability if we have*

$$k = \omega(n \log \lambda/\lambda).$$

In particular, for any constant n and $k = 3$, the corresponding Massey secret-sharing scheme is leakage-resilient.

We remark that the NC^0-local leakage family is a superset of the physical-bit local leakage family (for example, as considered in the recent work of [25]). [25] proved that the Shamir secret-sharing scheme with reconstruction threshold $k \geqslant 2$ and random evaluation places is leakage-resilient to physical-bit leakages, which is a significantly smaller subset of the NC^0_d local leakage considered in our work.

Local leakage with bounded-size circuits. Let $\mathcal{L}$ be the local leakage family where every local leakage function is a circuit of size (at most) s that leaks one bit. Note that the number of circuits of size (at most) s is upper-bounded by $(10s) \cdot 2^s$ [3]. Hence, the size of $\mathcal{L}$ is upper-bounded by $(10s \cdot 2^s)^n$. Consequently, the prerequisite of Corollary 1 holds as long as $k = \omega(n \cdot s/\lambda)$. Hence, we have the following corollary.

Corollary 4. *Let $\mathcal{L}$ be the local leakage family where every local leakage function is a circuit of size (at most) s that leaks one bit. Let F be a finite field such that $2^{\lambda-1} \leqslant |F| < 2^{\lambda}$, and $n, k = \mathsf{poly}(\lambda)$. Massey secret-sharing scheme corresponding to $\mathbf{G}^{+}$ is $(\mathcal{L}, \exp(-\Omega(\lambda)))$-leakage-resilient except with $\exp(-\Omega(\lambda))$ probability if we have*

$$k = \omega(n \cdot s/\lambda).$$

In particular, when $s = o(\lambda/\sqrt{n})$, one may pick $k \leqslant \sqrt{n}$.

For example, using a large-enough finite field F such that $\lambda = n^2$, the Massey secret-sharing scheme corresponding to random linear codes is leakage-resilient to size-$(s = n)$ local leakage circuits.

The Monte-Carlo construction presented above samples a fully random parity check matrix $P \in F^{(k+1)\times(n-k)}$, which requires $k(n-k)$ independent and uniformly random elements from the finite field F. We partially derandomize this result using (a variant of) the Wozencraft ensemble. In particular, we use two types of partially random matrices.

Wozencraft Ensemble $\mathbf{W}$*.* Consider a finite field K, which is a degree k extension of F. The Wozencraft ensemble maps every element $\alpha \in K$ to a matrix $M(\alpha) \in F^{k\times k}$. To sample a $k \times (n-k)$ matrix, one picks $m = \lceil (n-k)/k \rceil$ random elements $\boldsymbol{\alpha}^{(1)}, \dots, \boldsymbol{\alpha}^{(m)} \in K$. The sampled matrix $\mathbf{W}$ shall be the first $n-k$ columns of the matrix $\left[M\left(\boldsymbol{\alpha}^{(1)}\right)|\cdots|M\left(\boldsymbol{\alpha}^{(m)}\right)\right]$. We refer the readers to Definition 3 for more details and Supporting Material C for an example.

t-Row Random Matrix $\mathbf{M}^{(t)}$*.* For this random matrix, the first t rows are sampled independently and uniformly at random. The remaining rows are fixed to be 0. Refer to Definition 2 for more details.

Using these two type of partially random matrix, we prove the following theorem. A proof is provided in Supporting Material A.

Theorem 2. *Let $\mathcal{L}$ be an arbitrary family of ℓ-bit leakage functions and F be a finite field (possibly, of composite order). Let $n, k \in \mathbb{N}$ be arbitrary parameters such that $k < n$. Define $\mathbf{G}^{+} = [I_{k+1}|\mathbf{P}]$ as a random variable over the sample space $F^{(k+1)\times(n+1)}$, where $\mathbf{P}$ is sampled as follows.*

- *Entries of the first row of $\mathbf{P}$ are sampled independently and uniformly at random from F.*
- *The submatrix consisting of the rest of the rows, refer to as $\mathbf{R}$, is sampled as $\mathbf{W} + \mathbf{M}^{(t)}$, where $\mathbf{W}$ and $\mathbf{M}^{(t)}$ are sampled independently.*

The Massey secret-sharing scheme corresponding to $\mathbf{G}^{+}$ is $(\mathcal{L}, \varepsilon)$-leakage-resilient except *with probability (at most)*

$$\frac{8^{\ell}}{\varepsilon^2} \cdot \frac{|\mathcal{L}|}{|F|^{t-2}}.$$

In particular, $\varepsilon = \left(8^{\ell} \cdot |\mathcal{L}|/|F|^{t-2}\right)^{1/3}$ *ensures that the failure probability is at most* ε*. Furthermore,* ε *is exponentially decaying when* $|\mathcal{L}| \leqslant |F|^{t-2-c}/8^{\ell}$*, where* $c > 0$ *is a constant. The random* F*-elements required to sample* $\mathbf{G}^{+}$ *is* $(t+1)(n-k) + k \cdot \left\lceil \frac{n-k}{k} \right\rceil$.

Result II: Advantage of the "parity-of-parity" attack. Consider the *additive secret-sharing scheme* with reconstruction threshold $k = n$ over a finite field F (possibly of composite order). For a secret $s \in F$, this secret-sharing scheme chooses random secret shares $s_1, \dots, s_k \in F$ such that $s_1 + \cdots + s_k = s$. We assume that if F is a prime field, then parties store the secret shares $s_1, \dots, s_k$ in their natural binary representation. However, if F is a composite field of characteristic p, then the secret shares are stored as a vector of F_p elements and every F_p element is represented in its natural binary representation.

If F is characteristic 2 then the parity of the j-th bit of all the secret shares yields the j-th bit of the secret share, completely breaking the leakage-resilience of the additive secret-sharing scheme. So, without loss of generality, assume that the characteristic of F is an odd prime. Maji et al. [25] introduced the *parity-of-parity* local leakage attack on the additive secret sharing scheme that leaks one physical bit from every secret share. If F is a prime field then it leaks the least significant bit of each secret share (a physical bit in its natural binary representation), i.e., whether $s_i \in \{0, 2, \dots, |F|-1\}$ or $s_i \in \{1, 3, \dots, |F|-3\}$. If F is degree-a extension of the prime field F_p, then every secret share $s_i \in F$ has equivalent representation $(s_{i,1}, \dots, s_{i,a}) \in F_p^a$. The leakage attack leaks the parity of the element $s_{i,j}$, for any fixed $j \in \{1, \dots, a\}$.

Finally, the leakage attack uses the parity of the leaked parities from each secret share to distinguish the secret shares generated by two different secrets. Given ε and k, our objective is to identify whether there are two distinct secrets $s^{(0)}, s^{(1)} \in F$ such that the parity-of-parity attack has (at least) ε-advantage in distinguishing the secret shares that these secrets generate. We prove the following technical result.

Theorem 3. *Consider the additive secret sharing scheme with reconstruction threshold* $k = n$ *over the finite field* F*. There exists two secrets* $s^{(0)}, s^{(1)} \in F$ *such that the parity-of-parity attack has* ε*-advantage in distinguishing the secret shares of* $s^{(0)}$ *from the secret shares of* $s^{(1)}$*, where*

$$\varepsilon \geqslant \frac{1}{2} \cdot \left(\frac{2}{\pi}\right)^{k}.$$

Maji et al. [25] conjectured this bound based on empirical data. Recently, [1] made partial progress towards non-trivially lower-bounding the advantage of the parity-of-parity attack by proving $\varepsilon \geqslant 1/k!$. Our bound also proves the optimality of the parity-of-parity attack in the following sense: over prime fields, [5] proved that the additive secret-sharing scheme is $2.47 \cdot (2/\pi)^k$-secure against *any* local leakage attack that leaks one bit from every secret share. Technically, the bound proceeds via a Fourier-analytic approach that requires estimating an exponential sum. We identify the dominant term in that sum and prove that the remainder of the sum effectively is an exponentially small noise.

Next, we summarize a few consequences of our technical result. As a consequence of our result, the reconstruction threshold of the additive secret-sharing scheme must satisfy $k \geqslant \Theta(\log \lambda)$ to be leakage-resilient to one physical-bit leakage from every secret share. Our result improves the previous best-known lower bound of $k \geqslant \Theta(\log \lambda / \log \log \lambda)$ for additive secret-sharing schemes using the leakage attack presented in [5]. Furthermore, using the line of reasoning in Remark 1, there is a family of local leakages of size $|F|^{k+1}$ that leaks one bit from every secret share such that the reconstruction threshold k must be $\Omega(\log \lambda)$ for the Massey secret-sharing scheme corresponding to any dimension-$(k+1)$ linear code to be leakage-resilient.

1.2 Prior Relevant Works

Since the introduction of leakage-resilient secret-sharing [5, 16], there are two main research directions. The first direction is to construct new secret-sharing schemes that are leakage-resilient against various models of leakages [16, 2, 34, 4, 22, 7, 9]. The other direction is to investigate the leakage-resilience of prominent secret-sharing schemes against local leakages [5, 23, 25, 1, 26]. We shall focus our discussion on the second line of works.

Interestingly, the leakage-resilience of the Massey secret-sharing scheme is connected to the exciting problem of repairing a linear code in the distributed storage setting. For example, Guruswami and Wootters [17, 18] presented a reconstruction algorithm that obtains one bit from every block of a Reed-Solomon code to repair any block when the field has characteristic two. Their results show that Shamir secret-sharing schemes over characteristic two fields are utterly broken against general one-bit local leakages.

For the case of prime-order fields, [6, 26] proved that Shamir secret-sharing scheme is robust to one-bit local leakage if the reconstruction threshold $k \geqslant 0.85n$. Furthermore, [26] proved that when $k > 0.5n$, the Massey secret-sharing scheme corresponding to a random linear code is leakage-resilient even if a constant number of bits are leaked from every share. For restricted families of leakages, [25] studied the physical-bit leakage attacks on the Shamir secret-sharing scheme. They proved that the Shamir secret-sharing scheme with random evaluation places is leakage-resilient to this family when reconstruction threshold $k \geqslant 2$.

On the other hand, [5] first showed that, for additive secret-sharing schemes, an adversary might perform a one-bit general leakage from each share to get a distinguishing advantage of k^{-k}. Hence, additive secret-sharing is not leakage-resilient over a constant number of parties. [25, 1] further showed that one might perform a one-bit physical-bit leakage from each share to get a distinguishing advantage of $1/k!$. They also extended their result to Shamir secret-sharing schemes. They proved that if one chooses the evaluation places adversarially, an adversary might perform a one-bit physical-bit leakage from each share to get a distinguishing advantage of $1/k!$.

Finally, Nielsen and Simkin [29] presented a probabilistic argument to construct a general leakage attack on any Massey secret-sharing scheme. Roughly, their attack needs $m \geqslant k \log|F|/(n-k)$ bits of leakage from each secret share.

1.3 Technical Overview

Let λ represent the security parameter. Let F be a finite field (possibly, of composite order) such that $2^{\lambda-1} \leqslant |F| < 2^{\lambda}$. That is, every element of F has a λ-bit representation. Let $n = \mathsf{poly}(\lambda)$ represent the number of secret shares and $k = \mathsf{poly}(\lambda)$ represent the threshold for reconstruction on the secret-sharing scheme. Consider a generator matrix $G^+ \in F^{(k+1)\times(n+1)}$ in the standard form, i.e., $G^+ = [I_{k+1}|P]$. The linear code generated by G^+ (i.e., the row span of G^+) is denoted by $\langle G^+\rangle$. We shall index the rows of G^+ by $\{0, 1, \ldots, k\}$ and the columns of G^+ by $\{0, 1, \ldots, n\}$. We refer to the submatrix $G^+_{\{1,\ldots,k\},\{1,\ldots,n\}}$ as G.

Overview of result I. Consider the Massey secret-sharing scheme corresponding to the linear code $\langle G^+\rangle$. Observe that the secret shares corresponding to the secret 0 are identical to the linear code $\langle G\rangle$. Furthermore, we refer to the row vector $G^+_{0,\{1,\ldots,n\}}$ as $\vec{v}$. This representation has the benefit of succinctly expressing the secret shares of s as the affine subspace $s \cdot \vec{v} + \langle G\rangle$. Refer to Figure 1 for a pictorial summary of these notations.

For now, we shall consider a fully random $\mathbf{G}^+$ such that every element of the parity check matrix $\mathbf{P}$ is sampled independently and uniformly at random from the finite field F.

Reduction 1. Fix any ℓ-bit (joint) leakage family $\mathcal{L}$. Our objective is to prove that the Massey secret-sharing scheme corresponding to a random code $\mathbf{G}^+$ is $(\mathcal{L}, \varepsilon)$-leakage-resilient, with overwhelming probability. Observe that it is sufficient to consider an arbitrary function L and prove an upper bound on the probability that $\mathbf{G}^+$ is not ε-leakage-resilient against L. Once we have this upper bound, invoking a union bound over all leakage functions contained in the set $\mathcal{L}$ yields an upper bound on the probability that $\mathbf{G}^+$ is not $(\mathcal{L}, \varepsilon)$-leakage-resilient. Hence, in the rest of the discussion, we fix the leakage function L and consider the probability that $\mathbf{G}^+$ is *not* ε-leakage-resilient against a particular ℓ-bit leakage function L.

Reduction 2. By definition, if $\mathbf{G}^+$ is not ε-leakage-resilient against L, there exists two secrets $s^{(0)}$ and $s^{(1)}$ such that the statistical distance between $\mathbf{L}(s^{(0)})$ and $\mathbf{L}(s^{(1)})$ is $> \varepsilon$. However, note that it suffices to restrict $s^{(0)} = 0$. This restriction is justified because the triangle inequality ensures that there must be a secret $s \in F^*$ such that the statistical distance between the leakage joint distributions $\mathbf{L}(0)$ and $\mathbf{L}(s)$ must be at least $\varepsilon/2$. Henceforth, our objective is to consider a pair of secret 0 and $s \in F^*$ and estimate the probability that the statistical distance between the joint leakage distribution $\mathbf{L}(0)$ and $\mathbf{L}(s)$ is $> \varepsilon/2$.

Reduction 3. Observe that the statistical distance between $\mathbf{L}(0)$ and $\mathbf{L}(s)$ is

$$\frac{1}{2} \cdot \sum_{\vec{w} \in \{0,1\}^{\ell}} \frac{1}{|F|^k} \Big| |\langle \mathbf{G} \rangle \cap A_{\vec{w}}| - \big| \big(s \cdot \vec{\mathbf{v}} + \langle \mathbf{G} \rangle \big) \cap A_{\vec{w}} \big| \Big|,$$

where $A_{\vec{w}} := L^{-1}(\vec{w})$ is the preimage of the observed leakage $\vec{w}$. For any $A \subseteq F^n$ and secret $s \in F$, we define the random variable

$$\mathbf{X}_{s,A} := \frac{1}{|F|^k} \Big| |\langle \mathbf{G} \rangle \cap A| - \big| \big(s \cdot \vec{\mathbf{v}} + \langle \mathbf{G} \rangle \big) \cap A \big| \Big|.$$

Our objective can be further reduced to show that the random variable $\mathbf{X}_{s,A}$ is sufficiently small with overwhelming probability. This bound is sufficient because one may complete the proof by union bounding over all the choices of $s \in F^*$ and $A_{\vec{w}} \subseteq F^n$.

Upper bounding the second moment. We proceed via a second-moment technique to prove that the random variable $\mathbf{X}_{s,A}$ is sufficiently small with overwhelming probability. An upper bound on the expectation of the second moment suffices for our proof because one can use the Chebyshev inequality to prove that $\mathbf{X}_{s,A}$ is sufficiently small with overwhelming probability. Indeed, we prove that, when $\mathbf{G}^+$ is fully random, the expectation of the second moment is small. Our results on the second moment of the random variable $\mathbf{X}_{s,A}$ are summarized as Lemma 1.

Partial derandomization. Finally, we show that one may prove a similar bound on the second moment of $\mathbf{X}_{s,A}$ when $\mathbf{G}^+$ is only partially random. In particular, we consider the sampling part of the parity check matrix $\mathbf{P}$ as the sum of the Wozencraft ensemble and the set of matrices with few random rows. Supporting Material A provides additional details on this result.

Comparison with [25]. In recent work, Maji et al. [25] considered the leakage-resilience of Shamir secret-sharing against physical-bit leakage. They proved that the Shamir secret-sharing scheme with random evaluation places is leakage-resilient to the physical-bit leakage family for any reconstruction threshold $k \geqslant 2$. The Shamir secret-sharing scheme is multiplication-friendly for any $k < n/2$. In comparison, for the physical-bit leakage family, we prove that the Massey secret-sharing scheme corresponding to a random linear code is leakage-resilient for any reconstruction threshold $(k+1) \geqslant 4$. The product of the Massey secret-sharing scheme corresponding to a general linear code is a ramp secret-sharing scheme (with k-privacy and $(k+1)^2$-reconstruction threshold). Hence, Massey secret-sharing scheme corresponding to a general linear code is multiplication-friendly when $n \geqslant (k+1)^2$. However, our result is significantly more general as it applies to arbitrary small (potentially joint) leakage families. In contrast, the techniques of [25] follow the Fourier analytic approach and, hence, cannot be extended to arbitrary local leakage families (due to the bottleneck presented by [26]).

Comparison with [26, 6]. Benhamouda et al. [6] proved that the Shamir secret-sharing scheme is leakage-resilient to all local leakage functions when $k > 0.85n$. Similarly, Maji et al. [26] proved that the Massey secret-sharing scheme corresponding to a random linear code is leakage-resilient to all local leakage functions when $k > 0.5n$. Both results are incomparable to ours as they proved a stronger result, i.e., leakage-resilience against all local leakage functions, but for significantly higher k. In particular, the parameter settings for k and n in their results are not multiplication-friendly.

Comparison with [10, 12]. Our work considers passive adversaries who perform leakage attacks on a random code. Several works [10, 12] in the literature of non-malleable code consider the security of a random code against active adversaries who perform tampering attacks on the codeword. In particular, they show that certain randomized constructions[1] will be secure with overwhelming probability against arbitrary tampering families of bounded size. Our work is, in spirit, similar to those works.

Open problem: extension to Shamir secret-sharing scheme. We leave as a fascinating open problem to extend our results to Shamir secret-sharing schemes with randomly chosen evaluation places. To apply our techniques to Shamir secret-sharing schemes with randomly chosen evaluation places, one encounters non-trivial challenges in algebraic geometry involving degree-k curves. We believe that resolving this technical challenge shall require resolving new algebro-geometric problems.

Overview of result II. Let F be a prime field of order p. Consider the additive secret-sharing scheme over F. Let L be the leakage attack that leaks the least significant bit from every share. By the Fourier-analytic approach from prior works [5, 25, 26], we have[2]

$$\mathsf{SD}\left(\mathbf{L}\left(s^{(0)}\right), \mathbf{L}\left(s^{(1)}\right)\right) = \frac{1}{2} \cdot \sum_{\ell \in \{0,1\}^n} \left| \sum_{\alpha \in F^*} \left(\prod_{i=1}^{n} \widehat{\mathbb{1}_{\ell_i}}(\alpha) \right) \left(\omega^{n \cdot \alpha \cdot s^{(0)}} - \omega^{n \cdot \alpha \cdot s^{(1)}} \right) \right|,$$

where $\omega = \exp(2\pi\imath/p)$ is the p^{th} root of unity. Furthermore, $\mathbb{1}_0$ is the indicator function for the set $S_0 := \{0, 2, \ldots, p-1\}$ and, similarly, $\mathbb{1}_1$ is the indicator function for the set $S_1 := \{1, 3, \ldots, p-2\}$. That is, S_b is the set of field elements whose least significant bit is b. Note that the above expression is an *identity*.

We observe that, for any $\ell \in \{0,1\}^n$, the *magnitude* of the expression

$$U(\alpha) := \prod_{i=1}^{n} \widehat{\mathbb{1}_{\ell_i}}(\alpha)$$

[1] Their randomized construction is more sophisticated compared to a random linear code that we consider. This is inevitable for non-malleable code as any structure of the code (e.g., linearity) could render it malleable.

[2] Refer to Section 4.1 for the definition of Fourier coefficients.

is exponentially decaying as α goes from the middle points $\frac{p-1}{2}$ and $\frac{p+1}{2}$ to the end points 1 and $p-1$. Informally, it holds that

$$|U(\alpha)| \approx \left(\frac{2}{\pi}\right)^n \cdot \left(\frac{1}{|2\alpha - p|}\right)^n .$$

As for the magnitude of the other term

$$V(\alpha) := \left(\omega^{n\cdot\alpha\cdot s^{(0)}} - \omega^{n\cdot\alpha\cdot s^{(1)}}\right),$$

we use the naive triangle inequality to upper bound it by 2 for the tail terms (i.e., $\alpha \neq \frac{p-1}{2}, \frac{p+1}{2}$). And we argue that there exists two secrets $s^{(0)}$ and $s^{(1)}$ such that $V\left(\frac{p-1}{2}\right)$ and $V\left(\frac{p+1}{2}\right)$ are constantly large.

Together, these observations enable us to lower bound the statistical distance by (approximately) the magnitude of the dominant term $U\left(\frac{p-1}{2}\right)$ and $U\left(\frac{p+1}{2}\right)$, which is $\Theta\left(\left(\frac{2}{\pi}\right)^n\right)$.

Finally, observe that the two distributions $\mathbf{L}\left(s^{(0)}\right)$ and $\mathbf{L}\left(s^{(1)}\right)$ are $(n-1)$-indistinguishable. That is, these two distributions restricted to any proper subset of their coordinates are identical. Therefore, by standard techniques, parity is the optimal distinguisher for these two distributions (we provide a formal discussion on this in Supporting Material E). Consequently, the parity-of-parity attack [25] has an distinguishing advantage of $\Theta\left(\left(\frac{2}{\pi}\right)^n\right)$.

2 Preliminaries

Throughout this paper, we use F for a finite field. We do not restrict to that F is a prime field. In particular, our results hold even if F is a characteristic-2 field.

Our work uses the length of the binary representation of the order of the field F as the security parameter λ, i.e., $\lambda = \log_2|F|$. 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.

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 $\frac{1}{2}\sum_x |\Pr[\mathbf{A} = x] - \Pr[\mathbf{B} = x]|$.

For any set A, we denote the indicator function of the set A as $\mathbb{1}_A$. That is, $\mathbb{1}_A(x) = 1$ if $x \in A$ and 0 otherwise.

For an element x and a set S, we use $x + S$ to denote the set $\{x + s \colon s \in S\}$.

2.1 Matrices

A matrix $M \in F^{k\times n}$ has k-rows and n-columns, and each of its element is in F. 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 $\{0, 1, \dots, k\}$ as row indices and $\{0, 1, \dots, n\}$ as column indices for a matrix $G^+ \in F^{(k+1)\times(n+1)}$.

2.2 Codes and Massey Secret-sharing Schemes

We use the following notations for error-correcting codes as consistent with [24].

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 this work, we always assume that the generator matrices are in their standard form.

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 $(n - k + 1)$.

Massey Secret-sharing Schemes. Let $C \subseteq F^{n+1}$ be a linear code. Let $s \in F$ be a secret. The Massey secret-sharing scheme corresponding to C picks a random element $(s, s_1, \dots, s_n) \in C$ to share the secret s. The secret shares of parties $1, \dots, n$ are $s_1, \dots, s_n$, respectively.

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 $\{0, 1, \dots, k\}$ and its columns are indexed by $\{0, 1, \dots, n\}$. Let $s \in F$ be the secret. The secret-sharing scheme picks independent and uniformly random $r_1, \dots, r_k \in F$. Let

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

Observe that $y_0 = s$ because the generator matrix G^+ is in the standard form. The secret shares for the parties $1, \dots, n$ are $s_1 = y_1, s_2 = y_2, \dots, s_n = y_n$, 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 $G = G^+_{\{1,\dots,k\}\times\{1,\dots,n\}}$. 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 $\vec{v} = G^+_{0,\{1,\dots,n\}}$. Refer to Figure 1 for a pictorial summary.

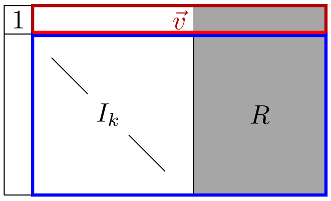

Fig. 1. A pictorial summary of the generator matrix $G^+ = [I_{k+1} \mid P]$, where P is the shaded matrix. The indices of rows and columns of G^+ are $\{0,1,\dots,k\}$ and $\{0,1,\dots,n\}$, respectively. The (blue) matrix $G = [I_k \mid R]$ is a submatrix of G^+. In particular, the secret shares of secret $s = 0$ form the code $\langle G\rangle$. The (red) vector is $\vec{v}$. In particular, for any secret s, the secret shares of s form the affine subspace $s \cdot \vec{v} + \langle G\rangle$.

Suppose parties $i_1,\dots,i_t \in \{1,\dots,n\}$ come together to reconstruct the secret with their, respective, secret shares $s_{i_1},\dots,s_{i_t}$. Let $G^+_{*,i_1},\dots,G^+_{*,i_t} \in F^{(k+1)\times 1}$ represent the columns indexed by $i_1,\dots,i_t \in \{1,\dots,n\}$, respectively. If the column $G^+_{*,0} \in F^{(k+1)\times 1}$ lies in the span of $\left\{G^+_{*,i_1},\dots,G^+_{*,i_t}\right\}$ 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 $\left\{G^+_{*,i_1},\dots,G^+_{*,i_t}\right\}$ then the secret remains *perfectly hidden* from these parties.

2.3 Joint Leakage-resilience of Secret-sharing Scheme

Consider an n-party secret-sharing scheme, where every party gets an element in F as their secret share. Let L be an ℓ-bit joint leakage function, i.e., $L : F^n \to \{0,1\}^\ell$. Let $\mathbf{L}(s)$ be the distribution of the leakage defined by the experiment: (a) sample secret shares $(s_1,\dots,s_n)$ for the secret s, and (b) output $L(s_1,\dots,s_n)$.

Definition 1. *Let $\mathcal{L}$ be a family of ℓ-bit joint leakage functions. We say a secret-sharing scheme is* ε-leakage-resilient against $\mathcal{L}$ *if for all leakage functions $L \in \mathcal{L}$ and for all secrets $s^{(0)}$ and $s^{(1)}$, we have*

$$\mathsf{SD}\left(\mathbf{L}\left(s^{(0)}\right), \mathbf{L}\left(s^{(1)}\right)\right) \leqslant \varepsilon.$$

3 Leakage-resilience of Fully Random Matrix

In this section, we consider the fully random generator matrix $\mathbf{G}^+ = [I_{k+1}|\mathbf{P}]$. That is, every entry of the parity check matrix P is sampled as an independently uniformly random element from F. Fix any small leakage family $\mathcal{L}$. We shall show that the Massey secret-sharing scheme corresponding to $\mathbf{G}^+$ is leakage-resilient to $\mathcal{L}$ with overwhelming probability. In particular, we prove the following theorem.

Theorem 4. *Let $\mathcal{L}$ be an arbitrary family of ℓ-bit joint leakage functions. The Massey secret-sharing scheme corresponding to fully random $\mathbf{G}^+$ is ε-leakage-resilient against $\mathcal{L}$* except *with probability*

$$\leqslant \frac{|\mathcal{L}| \cdot 8^\ell}{\varepsilon^2 \cdot |F|^{k-2}}.$$

In particular, letting $\varepsilon = \left(|\mathcal{L}| \cdot 8^\ell / |F|^{k-2}\right)^{1/3}$ ensures that the failure probability is at most ε. Furthermore, ε is exponentially decaying when $|\mathcal{L}| \leqslant |F|^{k-2-c}/8^\ell$, where $c > 0$ is an arbitrary constant.

Remark 2. We note that a fully random matrix over (exponentially large) F is *maximum distance separable* (MDS) with overwhelming probability when $2^n = \mathrm{o}(|F|)$. Hence, the resulting Massey secret-sharing scheme is a $(k+1)$-out-of-n threshold secret-sharing scheme with overwhelming probability. We refer the readers to Appendix B.1 of [26] for a proof.

We shall present a combinatorical proof of this theorem. First, it shall be convenient to define the following random variable. For any secret $s \in F$ and any subset $A \subseteq F^n$, define

$$\mathbf{X}_{s,A} := \frac{1}{|F|^k} \cdot \Big(|\langle \mathbf{G} \rangle \cap A| - \big| \big(\langle \mathbf{G} \rangle + s \cdot \vec{\mathbf{v}} \big) \cap A \big| \Big).$$

Recall that $\langle G \rangle$ is the set of all the secret shares of secret 0. Furthermore, $\langle G \rangle + s \cdot \vec{v}$ is the set of all the secret shares of secret s. Hence, the random variable $\mathbf{X}_{s,A}$ represents the difference in the probability that the secret shares falls into the set A between secret being 0 and s. Our key technical lemma is the following.

Lemma 1 (Key Technical Lemma). *For any secret $s \in F$ and any subset $A \subseteq F^n$, it holds that*

$$\mathop{\mathrm{E}}_{\mathbf{G}^+}\left[(\mathbf{X}_{s,A})^2 \right] \leqslant \frac{1}{|F|^{k-1}}.$$

Let us first show why Lemma 1 is sufficient to prove Theorem 4.

Proof (of Theorem 4 using Lemma 1). First, Lemma 1 implies that, for all $t > 0$, we have

$$\Pr_{\mathbf{G}^+}\left[|\mathbf{X}_{s,A}| \geqslant t \right] \leqslant \frac{1}{t^2 \cdot |F|^{k-1}} \tag{1}$$

since

$$\begin{aligned} \Pr_{\mathbf{G}^+}\left[|\mathbf{X}_{s,A}| \geqslant t \right] &\leqslant \frac{\mathrm{E}\Big[(\mathbf{X}_{s,A})^2 \Big]}{t^2} && \text{(Chebyshev inequality)} \\ &\leqslant \frac{1}{t^2 \cdot |F|^{k-1}}. && \text{(Lemma 1)} \end{aligned}$$

Given this, observe that

$$\begin{aligned}
&\Pr_{\mathbf{G}^+}\left[\mathbf{G}^+ \text{ is } \textit{not } \varepsilon\text{-leakage-resilient against } \mathcal{L}\right] \\
&= \Pr_{\mathbf{G}^+}\left[\exists s^{(0)}, s^{(1)},\ \exists L \in \mathcal{L},\ \mathsf{SD}\left(\mathbf{L}\left(s^{(0)}\right), \mathbf{L}\left(s^{(1)}\right)\right) > \varepsilon\right] \\
&\leqslant \Pr_{\mathbf{G}^+}\left[\exists s,\ \exists L \in \mathcal{L},\ \mathsf{SD}\left(\mathbf{L}\left(0\right), \mathbf{L}\left(s\right)\right) > \varepsilon/2\right] \\
&\leqslant \sum_{L \in \mathcal{L}} \left(\Pr_{\mathbf{G}^+}\left[\exists s,\ \mathsf{SD}\left(\mathbf{L}\left(0\right), \mathbf{L}\left(s\right)\right) > \varepsilon/2\right]\right). && \text{(Union bound)}
\end{aligned}$$

Fix any $L \in \mathcal{L}$. For any leakage $\vec{w} \in \{0,1\}^\ell$, let $A_{\vec{w}} := L^{-1}\left(\vec{w}\right)$. That is, $A_{\vec{w}}$ is the set of secret shares that would result in the leakage $\vec{w}$. It holds that

$$\begin{aligned}
&\Pr_{\mathbf{G}^+}\left[\exists s,\ \mathsf{SD}\left(\mathbf{L}\left(0\right), \mathbf{L}\left(s\right)\right) > \varepsilon/2\right] \\
&= \Pr_{\mathbf{G}^+}\left[\exists s,\ \frac{1}{2} \cdot \sum_{\vec{w} \in \{0,1\}^\ell} \left|\mathbf{X}_{s,A_{\vec{w}}}\right| > \varepsilon/2\right] && \text{(By definition of } \mathsf{SD} \text{ and } \mathbf{X}_{s,A_{\vec{w}}}\text{)} \\
&\leqslant \sum_{s \in F} \left(\Pr_{\mathbf{G}^+}\left[\sum_{\vec{w} \in \{0,1\}^\ell} \left|\mathbf{X}_{s,A_{\vec{w}}}\right| > \varepsilon\right]\right) && \text{(Union bound)} \\
&\leqslant \sum_{s \in F} \left(\Pr_{\mathbf{G}^+}\left[\exists \vec{w} \in \{0,1\}^\ell,\ \left|\mathbf{X}_{s,A_{\vec{w}}}\right| > \varepsilon/2^\ell\right]\right) && \text{(Pigeon-hole principle)} \\
&\leqslant \sum_{s \in F} \sum_{\vec{w} \in \{0,1\}^\ell} \left(\Pr_{\mathbf{G}^+}\left[\left|\mathbf{X}_{s,A_{\vec{w}}}\right| > \varepsilon/2^\ell\right]\right) && \text{(Union bound)} \\
&\leqslant |F| \cdot 2^\ell \cdot \frac{2^{2\ell}}{\varepsilon^2 \cdot |F|^{k-1}} && \text{(since Equation 1 applies to arbitrary } A \text{ and } s\text{)} \\
&= \frac{8^\ell}{\varepsilon^2 \cdot |F|^{k-2}}.
\end{aligned}$$

Combining everything, we get

$$\Pr_{G,v}\left[G^+ \text{ is not } \varepsilon\text{-leakage-resilient}\right] \leqslant \frac{|\mathcal{L}| \cdot 8^\ell}{\varepsilon^2 \cdot |F|^{k-2}}.$$

We complete the proof of Theorem 4 by proving our key technical lemma.

Proof (of Lemma 1). Recall that

$$\mathbf{X}_{s,A} = \frac{1}{|F|^k} \cdot \Big(\left|\langle \mathbf{G} \rangle \cap A\right| - \big|\big(\langle \mathbf{G} \rangle + s \cdot \vec{\mathbf{v}}\big) \cap A\big|\Big).$$

Hence, the second moment of $\mathbf{X}_{s,A}$ can be written as

$$\left(\mathbf{X}_{s,A}\right)^2 = \frac{1}{|F|^{2k}} \cdot \sum_{\vec{x},\vec{y} \in F^k} \Big(\mathbb{1}_A\left(\vec{x} \cdot \mathbf{G}\right) - \mathbb{1}_A\left(\vec{x} \cdot \mathbf{G} + s \cdot \vec{\mathbf{v}}\right)\Big)\Big(\mathbb{1}_A\left(\vec{y} \cdot \mathbf{G}\right) - \mathbb{1}_A\left(\vec{y} \cdot \mathbf{G} + s \cdot \vec{\mathbf{v}}\right)\Big).$$

For short, for all $\vec{x}$ and $\vec{y}$, let us define

$$\mathbf{T}_{\vec{x},\vec{y}} := \Big(\mathbb{1}_A\left(\vec{x}\cdot\mathbf{G}\right) - \mathbb{1}_A\left(\vec{x}\cdot\mathbf{G} + s\cdot\vec{\mathbf{v}}\right)\Big)\Big(\mathbb{1}_A\left(\vec{y}\cdot\mathbf{G}\right) - \mathbb{1}_A\left(\vec{y}\cdot\mathbf{G} + s\cdot\vec{\mathbf{v}}\right)\Big).$$

Recall that $\mathbf{G} = [I_k|\mathbf{R}]$ is in the standard form and the first k coordinates of $\vec{\mathbf{v}}$ are 0 (refer to Figure 1). Hence, one may write

$$\begin{aligned}\mathbf{T}_{\vec{x},\vec{y}} = \Big(\mathbb{1}_{A(\vec{x})}\left(\vec{x}\cdot\mathbf{R}\right) - \mathbb{1}_{A(\vec{x})}\left(\vec{x}\cdot\mathbf{R} + s\cdot\vec{\mathbf{v}}_{\{k+1,\dots,n\}}\right)\Big)&\\ \Big(\mathbb{1}_{A(\vec{y})}\left(\vec{y}\cdot\mathbf{R}\right) - \mathbb{1}_{A(\vec{y})}\left(\vec{y}\cdot\mathbf{R} + s\cdot\vec{\mathbf{v}}_{\{k+1,\dots,n\}}\right)\Big)&\end{aligned}$$

where

$$A(\vec{x}) := A \quad \bigcap \quad \{x_1\}\times\cdots\times\{x_k\}\times\underbrace{F\times\cdots\times F}_{n-k\text{ times}}$$

and

$$A(\vec{y}) := A \quad \bigcap \quad \{y_1\}\times\cdots\times\{y_k\}\times\underbrace{F\times\cdots\times F}_{n-k\text{ times}}.$$

Clearly, $\vec{x}\cdot\mathbf{R}$ and $\vec{y}\cdot\mathbf{R}$ are both uniform over F^{n-k}. Moreover, observe that $\vec{x}\cdot\mathbf{R}$ and $\vec{y}\cdot\mathbf{R}$ are *independent* random variables when $\vec{x}$ and $\vec{y}$ are linearly independent. Therefore, fix any linearly independent $\vec{x}$ and $\vec{y}$, we have

$$\begin{aligned}\underset{\mathbf{G}^+}{\mathrm{E}}\left[\mathbf{T}_{\vec{x},\vec{y}}\right] =& \underset{\vec{\mathbf{v}}}{\mathrm{E}}\Bigg[\underset{\mathbf{R}}{\mathrm{E}}\Big[\Big(\mathbb{1}_{A(\vec{x})}\left(\vec{x}\cdot\mathbf{R}\right) - \mathbb{1}_{A(\vec{x})}\left(\vec{x}\cdot\mathbf{R} + s\cdot\vec{\mathbf{v}}_{\{k+1,\dots,n\}}\right)\Big)\Big]\\ &\cdot\underset{\mathbf{R}}{\mathrm{E}}\Big[\Big(\mathbb{1}_{A(\vec{y})}\left(\vec{y}\cdot\mathbf{R}\right) - \mathbb{1}_{A(\vec{y})}\left(\vec{y}\cdot\mathbf{R} + s\cdot\vec{\mathbf{v}}_{\{k+1,\dots,n\}}\right)\Big)\Big]\Bigg]\\ =& \underset{\vec{\mathbf{v}}}{\mathrm{E}}\left[\left(\frac{|A(\vec{x})|}{|F|^{n-k}} - \frac{|A(\vec{x})|}{|F|^{n-k}}\right)\left(\frac{|A(\vec{x})|}{|F|^{n-k}} - \frac{|A(\vec{x})|}{|F|^{n-k}}\right)\right] = 0\end{aligned}$$

Let us define the bad set as

$$\mathsf{Bad} := \left\{(\vec{x},\vec{y})\ :\ \vec{x}\text{ and }\vec{y}\text{ are linearly dependent}\right\}.$$

Hence, we have shown that

$$(\vec{x},\vec{y})\notin\mathsf{Bad} \implies \underset{\mathbf{G}^+}{\mathrm{E}}\left[\mathbf{T}_{\vec{x},\vec{y}}\right] = 0.$$

On the other hand, for all $\vec{x}$ and $\vec{y}$, it trivially holds that

$$\underset{\mathbf{G}^+}{\mathrm{E}}\left[\mathbf{T}_{\vec{x},\vec{y}}\right] \leqslant 1.$$

Therefore, this completes the proof as

$$\underset{\mathbf{G}^+}{\mathrm{E}}\left[\left(\mathbf{X}_{s,A}\right)^2\right] = \frac{1}{|F|^{2k}}\sum_{\vec{x},\vec{y}\in F^k}\underset{\mathbf{G}^+}{\mathrm{E}}\left[\mathbf{T}_{\vec{x},\vec{y}}\right] \qquad \text{(Linearity of expectation)}$$

$$\leqslant \frac{1}{|F|^{2k}} \left(\sum_{(\vec{x},\vec{y})\notin \mathsf{Bad}} 0 + \sum_{(\vec{x},\vec{y})\in \mathsf{Bad}} 1 \right)$$

$$\leqslant \frac{1}{|F|^{k-1}}.$$

4 Tight Analysis of the Parity-of-parity Attack on Additive Secret-sharing Schemes

Maji et al. [25] proposed the following parity-of-parity attack. Suppose the field elements are stored in their natural binary representation. The adversary leaks the least significant bit (LSB) as the local leakage of every secret share. Finally, the adversary outputs the parity of the LSB from every secret share as the prediction of the secret. Adams et al. [1] proved that the distinguishing advantage of this adversary is at least $\Omega(1/n!)$. In this section, we shall present a tight analysis of this attack. In particular, we shall show that the distinguishing advantage is $\exp(-\mathcal{O}(n))$.

This lower bound we prove is tight up to a small constant, as Benhamouda et al. [5] prove that the distinguishing advantage of the adversary is upper-bounded by $\left(\frac{2}{\pi}\right)^{n-2}$. Note that the upper bound of [5] holds for any local leakage attack on the additive secret-sharing scheme. Therefore, our result also demonstrates that *the "parity-of-parity" attack is the optimal attack.*

Formally, let $\mathsf{AddSS}(s)$ represent the distribution of the additive secret shares of the secret s. That is, $\mathsf{AddSS}(s) = (s_1, \dots, s_n)$ is sampled uniformly at random conditioned on that $s_1 + s_2 + \cdots + s_n = s$. For any $x \in F$, let $\mathsf{lsb}(x)$ represent the least significant bit of x.[3]

Let τ represent the local leakage function that leaks the LSB of every secret share. That is,

$$\tau(\mathsf{AddSS}(s)) := \Big(\mathsf{lsb}(s_1), \mathsf{lsb}(s_2), \dots, \mathsf{lsb}(s_n)\Big).$$

We prove the following theorem.

Theorem 5. *There exists two secrets $s^{(0)}$ and $s^{(1)}$ such that*

$$\mathsf{SD}\left(\tau(\mathsf{AddSS}(s^{(0)}))\ ,\ \tau(\mathsf{AddSS}(s^{(1)}))\right) \geqslant \frac{1}{2} \cdot \left(\frac{2}{\pi}\right)^n .$$

[3] In this section, we restrict our discussion to field F of prime order. If E is an degree t extension field of a prime order field F. Then, every element α of E can be seen as a polynomial $a_{t-1}X^{t-1} + \cdots + a_1X + a_0$ in $F[X]$. We shall call a_0 the least significant symbol of α. Observe that, for an additive secret sharing of the secret s over E, the least significant symbol of every secret share forms an additive secret sharing of the least significant symbol of s over F. Therefore, the result for prime order fields naturally extends to composite order fields when the attacker leaks the LSB of the least significant symbol of every share.

In particular, to ensure that the adversary has a negligible distinguishing advantage $\mathsf{negl}(\lambda)$*, it must hold that* $n = \omega(\log\lambda)$.

We emphasize that our result is independent of the characteristic of the field F. Intuitively, as the characteristic of the field increases, the advantage of the adversary shall decrease. However, our result shows that the advantage of the adversary is guaranteed to be higher than $\frac{1}{2}\cdot\left(\frac{2}{\pi}\right)^n$, irrespective of the characteristic of the field.

Finally, observe that $\tau(\mathsf{AddSS}(s^{(0)}))$ and $\tau(\mathsf{AddSS}(s^{(1)}))$ are $(n-1)$-indistinguishable distributions since the additive secret sharing is $(n-1)$-private. By standard techniques in Fourier analysis, the parity of all the bits is the best distinguisher (up to a small constant) for any two $(n-1)$-indistinguishable distributions. For completeness, we provide a formal proof of this in Supporting Material E. This observation, together with the theorem, implies the optimality of the parity-of-parity attack.

Surprisingly, our proof of Theorem 5 is based on Fourier analysis. Typically, Fourier analytic approach is employed to *upper bound* the distinguishing advantage of the adversary. However, we shall use it to prove a *lower bound* result.

We start by introducing some basics of Fourier analysis that suffices for our purposes. Next, we present the proof of Theorem 5.

4.1 Preliminaries on Fourier Analysis

Let F be a prime field of order p. For any complex number $x \in \mathbb{C}$, let $\overline{x}$ represent its conjugate. For any two functions $f, g\colon F \to \mathbb{C}$, their *inner product* is

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

Let $\omega = \exp(2\pi\imath/p)$ be the p^{th} root of unity. For all $\alpha \in F$, the function χ_α is defined to be

$$\chi_\alpha(x) := \omega^{\alpha\cdot x},$$

and the respective Fourier coefficient $\widehat{f}(\alpha)$ is defined as

$$\widehat{f}(\alpha) := \langle f, \chi_\alpha\rangle\,.$$

Our proof relies on the following lemma. We refer the readers to [5] for a proof.

Lemma 2 (Poisson Summation Formula). *Let* $C \subseteq F^n$ *be a linear code with dual code* $C^\perp$*. For all* $i \in \{1, 2, \ldots, n\}$*, let* $f_i\colon F \to \mathbb{C}$ *be an arbitrary function. It holds that*

$$\mathop{\mathrm{E}}_{\vec{x}\leftarrow C}\left[\prod_{i=1}^{n} f_i(x_i)\right] = \sum_{\vec{y}\in C^\perp}\left(\prod_{i=1}^{n}\widehat{f_i}(y_i)\right).$$

The following claims will also be useful, which follows directly from the definition.

Claim 1 *Let $S, T \subseteq F$ be a bipartition of F. For all $\alpha \in F$,*

$$\widehat{\mathbb{1}_S}(\alpha) = -\widehat{\mathbb{1}_T}(\alpha).$$

Claim 2 *For all $S \subseteq F$ and $x \in F$, it holds that*

$$\widehat{\mathbb{1}_{x+S}}(\alpha) = \widehat{\mathbb{1}_S}(\alpha) \cdot \omega^{-\alpha \cdot x}.$$

4.2 Proof of Theorem 5

We start by introducing some notations and facts. Define a bipartition of F as

$$S_0 := \{0, 2, \ldots, p-1\} \qquad \text{and} \qquad S_1 := \{1, 3, \ldots, p-2\}.$$

That is, S_b is the set of field elements on which the LSB function will output b.

Claim 3 *For $\alpha \in F^*$, it holds that*

$$\widehat{\mathbb{1}_{S_0}}(\alpha) = \frac{1}{2p} \cdot \frac{1}{\cos(\pi\alpha/p)} \cdot \omega^{\alpha/2},$$

and

$$\widehat{\mathbb{1}_{S_1}}(\alpha) = -\frac{1}{2p} \cdot \frac{1}{\cos(\pi\alpha/p)} \cdot \omega^{\alpha/2}.$$

Furthermore,

$$\left|\widehat{\mathbb{1}_{S_0}}(\alpha)\right| = \left|\widehat{\mathbb{1}_{S_1}}(\alpha)\right| = \frac{1}{2p} \cdot \frac{1}{|\cos(\pi\alpha/p)|}.$$

Proof. By definition, we have

$$\begin{aligned}\widehat{\mathbb{1}_{S_0}}(\alpha) = \langle \mathbb{1}_{S_0}, \chi_\alpha \rangle = \frac{1}{p} \sum_{x \in F} \omega^{-\alpha \cdot x} &= \frac{1}{p} \cdot \sum_{j=0}^{(p-1)/2} \omega^{-\alpha \cdot (2j)} \\ =& \frac{1}{p} \cdot \frac{1 - \omega^{-(2\alpha)\cdot(p+1)/2}}{1 - \omega^{-2\alpha}} = \frac{1}{p} \cdot \frac{1 - \omega^{-\alpha}}{1 - \omega^{-2\alpha}}.\end{aligned}$$

One could verify that

$$1 - \omega^{-\alpha} = 2\sin(\pi\alpha/p) \cdot \omega^{\frac{p}{4} - \frac{\alpha}{2}}.$$

Hence,

$$\widehat{\mathbb{1}_{S_0}}(\alpha) = \frac{1}{p} \cdot \frac{2\sin(\pi\alpha/p) \cdot \omega^{\frac{p}{4} - \frac{\alpha}{2}}}{2\sin(\pi(2\alpha)/p) \cdot \omega^{\frac{p}{4} - \frac{2\alpha}{2}}} = \frac{1}{2p} \cdot \frac{1}{\cos(\pi\alpha/p)} \cdot \omega^{\alpha/2}.$$

By Claim 1, we have

$$\widehat{\mathbb{1}_{S_1}}(\alpha) = -\frac{1}{2p} \cdot \frac{1}{\cos(\pi\alpha/p)} \cdot \omega^{\alpha/2}.$$

Finally, it is easy to see

$$\left|\widehat{\mathbb{1}_{S_0}}(\alpha)\right| = \left|\widehat{\mathbb{1}_{S_1}}(\alpha)\right| = \frac{1}{2p} \cdot \frac{1}{|\cos(\pi\alpha/p)|}.$$

Let C be the parity code. That is, $(c_1, \dots, c_n) \in C$ if $c_1 + \cdots + c_n = 0$. The secret shares of a secret s is uniformly distributed over the set $(s, \dots, s) + C$. Additionally, $C^\perp$ is simply the repetition code, i.e., $C^\perp = \{(\alpha, \dots, \alpha) \colon \alpha \in F\}$.

We are ready to prove Theorem 5 as follows. We shall abuse notation and write $\mathbb{1}_b$ for $\mathbb{1}_{S_b}$. Observe that

$$
\begin{aligned}
&\mathsf{SD}\left(\tau\left(\mathsf{AddSS}(s^{(0)})\right), \tau\left(\mathsf{AddSS}(s^{(1)})\right)\right)\\
=&\frac{1}{2} \cdot \sum_{\ell \in \{0,1\}^n} \left| \mathop{\mathrm{E}}_{\vec{x} \leftarrow C}\left[\prod_{i=1}^{n} \mathbb{1}_{\ell_i}(x_i + s^{(0)})\right] - \mathop{\mathrm{E}}_{\vec{x} \leftarrow C}\left[\prod_{i=1}^{n} \mathbb{1}_{\ell_i}(x_i + s^{(1)})\right] \right|\\
&\hfill \text{(By definition of SD)}\\
=&\frac{1}{2} \cdot \sum_{\ell \in \{0,1\}^n} \left| \sum_{\vec{y} \in C^\perp} \left(\prod_{i=1}^{n} \widehat{\mathbb{1}_{\ell_i}}(y_i + s^{(0)})\right) - \sum_{\vec{y} \in C^\perp} \left(\prod_{i=1}^{n} \widehat{\mathbb{1}_{\ell_i}}(y_i + s^{(1)})\right) \right|\\
&\hfill \text{(Lemma 2)}\\
=&\frac{1}{2} \cdot \sum_{\ell \in \{0,1\}^n} \left| \sum_{\alpha \in F} \left(\prod_{i=1}^{n} \widehat{\mathbb{1}_{\ell_i}}(\alpha + s^{(0)})\right) - \sum_{\alpha \in F} \left(\prod_{i=1}^{n} \widehat{\mathbb{1}_{\ell_i}}(\alpha + s^{(1)})\right) \right|\\
&\hfill \text{(By the definition of } C^\perp\text{)}\\
=&\frac{1}{2} \cdot \sum_{\ell \in \{0,1\}^n} \left| \sum_{\alpha \in F} \left(\prod_{i=1}^{n} \widehat{\mathbb{1}_{\ell_i}}(\alpha)\right) \left(\omega^{n \cdot \alpha \cdot s^{(0)}} - \omega^{n \cdot \alpha \cdot s^{(1)}}\right) \right| \qquad \text{(Claim 2)}\\
=&\frac{1}{2} \cdot \sum_{\ell \in \{0,1\}^n} \left| \sum_{\alpha \in F^*} \left(\prod_{i=1}^{n} \left((-1)^{\ell_i} \frac{1}{2p} \cdot \frac{1}{\cos(\pi\alpha/p)} \cdot \omega^{\alpha/2}\right)\right) \left(\omega^{n \cdot \alpha \cdot s^{(0)}} - \omega^{n \cdot \alpha \cdot s^{(1)}}\right) \right|\\
&\hfill \text{(Claim 3)}\\
=&2^{n-1} \cdot \left| \sum_{\alpha \in F^*} \left(\frac{1}{2p} \cdot \frac{1}{\cos(\pi\alpha/p)} \cdot \omega^{\alpha/2}\right)^n \left(\omega^{n \cdot \alpha \cdot s^{(0)}} - \omega^{n \cdot \alpha \cdot s^{(1)}}\right) \right|\\
&\hfill \text{(Identity transformation)}
\end{aligned}
$$

Note that the proof so far has not used any inequalities. The expression above is identical to the statistical distance. For brevity, let us define

$$
U(\alpha) := \left(\frac{1}{2p} \cdot \frac{1}{\cos(\pi\alpha/p)} \cdot \omega^{\alpha/2}\right)^n,
$$

and

$$
V(\alpha) := \omega^{n \cdot \alpha \cdot s^{(0)}} - \omega^{n \cdot \alpha \cdot s^{(1)}}.
$$

Additionally, let $W(\alpha) := U(\alpha) \cdot V(\alpha)$.

Intuitively, we shall prove that the magnitude of $\sum_{\alpha \in F^*} W(\alpha)$ is approximately the magnitude of its leading term $W((p-1)/2)$ and $W((p+1)/2)$. In particular, we prove the following claims.

Claim 4 *There exists a universal constant $\mu \geqslant 3/2$ and two secrets $s^{(0)}, s^{(1)} \in F$ such that*

$$\left|W\left(\frac{p-1}{2}\right) + W\left(\frac{p+1}{2}\right)\right| \geqslant \mu \cdot \pi^{-n}.$$

Claim 5 *For all secrets $s^{(0)}, s^{(1)}$, we have*

$$\left|\sum_{\alpha \in F^* \setminus \{\frac{p-1}{2}, \frac{p+1}{2}\}} W(\alpha)\right| \leqslant \exp(-\Theta(n)) \cdot \pi^{-n}.$$

Using Claim 4 and Claim 5, the proof of the Theorem 5 follows from the fact that

$$\begin{aligned}
\mathsf{SD}\left(\tau\left(\mathsf{AddSS}(s^{(0)})\right), \tau\left(\mathsf{AddSS}(s^{(1)})\right)\right) &\geqslant 2^{n-1} \cdot (\mu - \exp(-\Theta(n))) \cdot \pi^{-n}, \\
&\geqslant 2^{n-1} \cdot \left(\frac{3}{2} - \mathrm{o}(1)\right) \cdot \pi^{-n}, \\
&\geqslant \frac{1}{2} \cdot 1 \cdot \left(\frac{2}{\pi}\right)^n \\
&\qquad \text{(for large enough } n.)
\end{aligned}$$

Consequently, it suffices to prove Claim 4 and Claim 5 to complete the proof of Theorem 5.

Proof (of Claim 4). Observe that

$$\begin{aligned}
W\left(\frac{p-1}{2}\right) &= \left(\frac{1}{2p} \cdot \frac{1}{\cos\left(\pi \cdot \frac{p-1}{2p}\right)} \cdot \omega^{\frac{p-1}{4}}\right)^n \cdot V\left(\frac{p-1}{2}\right) \\
&= \left(\frac{1}{2p} \cdot \frac{1}{\sin\left(\pi \cdot \frac{1}{2p}\right)}\right)^n \cdot \omega^{n \cdot \frac{p-1}{4}} \cdot V\left(\frac{p-1}{2}\right)
\end{aligned}$$

and

$$\begin{aligned}
W\left(\frac{p+1}{2}\right) &= \left(\frac{1}{2p} \cdot \frac{1}{\cos\left(\pi \cdot \frac{p+1}{2p}\right)} \cdot \omega^{\frac{p+1}{4}}\right)^n \cdot V\left(\frac{p+1}{2}\right) \\
&= \left(\frac{1}{2p} \cdot \frac{1}{\sin\left(\pi \cdot \frac{1}{2p}\right)}\right)^n \cdot (-1)^n \cdot \omega^{n \cdot \frac{p+1}{4}} \cdot V\left(\frac{p+1}{2}\right)
\end{aligned}$$

Therefore,

$$\left|W\left(\frac{p-1}{2}\right) + W\left(\frac{p+1}{2}\right)\right|$$

$$=\left|\left(\frac{1}{2p}\cdot\frac{1}{\sin\left(\pi\cdot\frac{1}{2p}\right)}\right)^n\right|\cdot\left|\omega^{n\cdot\frac{p-1}{4}}\cdot V\left(\frac{p-1}{2}\right)+(-1)^n\cdot\omega^{n\cdot\frac{p+1}{4}}\cdot V\left(\frac{p+1}{2}\right)\right|$$
$$=\left|\left(\frac{1}{2p}\cdot\frac{1}{\sin\left(\pi\cdot\frac{1}{2p}\right)}\right)^n\right|\cdot\left|V\left(\frac{p-1}{2}\right)+(-1)^n\cdot\omega^{\frac{n}{2}}\cdot V\left(\frac{p+1}{2}\right)\right|$$

Note that $x\cdot\sin(1/x)$ is strictly increasing as x increases and tends to 1 as $x\to\infty$.[4] Therefore,

$$\left|W\left(\frac{p-1}{2}\right)+W\left(\frac{p+1}{2}\right)\right|\geqslant\pi^{-n}\cdot\left|V\left(\frac{p-1}{2}\right)+(-1)^n\cdot\omega^{\frac{n}{2}}\cdot V\left(\frac{p+1}{2}\right)\right|.$$

It remains to prove that there exist secrets $s^{(0)}$ and $s^{(1)}$ such that $V\left(\frac{p-1}{2}\right)$ and $(-1)^n\cdot\omega^{\frac{n}{2}}\cdot V\left(\frac{p+1}{2}\right)$ does not cancel its other to be too small. More formally, for any p and n, we shall show that there exist a universal constant μ and secrets $s^{(0)}$ and $s^{(1)}$ such that

$$\left|\left(\omega^{n\cdot\frac{p-1}{2}\cdot s^{(0)}}-\omega^{n\cdot\frac{p-1}{2}\cdot s^{(1)}}\right)+(-1)^n\cdot\omega^{\frac{n}{2}}\cdot\left(\omega^{n\cdot\frac{p+1}{2}\cdot s^{(0)}}-\omega^{n\cdot\frac{p+1}{2}\cdot s^{(1)}}\right)\right|\geqslant\mu.$$

Let $f(s^{(0)})$ (resp., $g(s^{(1)})$) denote the terms involving $s^{(0)}$ (resp., $s^{(1)}$) in the above expression. And we are interested in $\left|f(s^{(0)})+g(s^{(1)})\right|$. Observe that

$$\sum_{s^{(1)}\in F}g(s^{(1)})=0.$$

Therefore,

$$\max_{s^{(1)}}\left|f(s^{(0)})+g(s^{(1)})\right|\geqslant\frac{1}{p}\sum_{s^{(1)}\in F}\left|f(s^{(0)})+g(s^{(1)})\right|$$
$$\geqslant\frac{1}{p}\left|\sum_{s^{(1)}\in F}\left(f(s^{(0)})+g(s^{(1)})\right)\right|=\left|f(s^{(0)})\right|.$$

Hence, it suffices to show that there exists an $s^{(0)}$ such that $\left|f(s^{(0)})\right|$ is sufficiently large. That is,

$$\max_{s^{(0)}}\left|\omega^{n\cdot\frac{p-1}{2}\cdot s^{(0)}}+(-1)^n\cdot\omega^{\frac{n}{2}}\cdot\omega^{n\cdot\frac{p+1}{2}\cdot s^{(0)}}\right|\geqslant\mu,$$

which is equivalent to

$$\max_{s^{(0)}}\left|1+(-1)^n\cdot\omega^{\frac{n}{2}}\cdot\omega^{n\cdot s^{(0)}}\right|\geqslant\mu.$$

[4] Intuitively, the advantage of the adversary decreases as the characteristic of the field increases.

It is easy to see that the phase of $\omega^{n \cdot s^{(0)}}$ could be an arbitrary multiple of $2\pi/p$. Hence, this must exist an $s^{(0)}$ such that its magnitude is $\geqslant 3/2$.[5]

This completes the proof.

Proof (of Claim 5). By a simple triangle inequality, we have $|V(\alpha)| \leqslant 2$. Hence,

$$\begin{aligned}
&\left|\sum_{\alpha \in F^* \setminus \{\frac{p-1}{2}, \frac{p+1}{2}\}} W(\alpha)\right| \\
&\leqslant \sum_{\alpha \in F^* \setminus \{\frac{p-1}{2}, \frac{p+1}{2}\}} |W(\alpha)| && \text{(Triangle inequality)} \\
&\leqslant 2 \cdot \sum_{\alpha \in F^* \setminus \{\frac{p-1}{2}, \frac{p+1}{2}\}} |U(\alpha)| && \text{(Triangle inequality)} \\
&= 2 \cdot \sum_{\alpha \in F^* \setminus \{\frac{p-1}{2}, \frac{p+1}{2}\}} \left|\frac{1}{2p} \cdot \frac{1}{\cos(\pi\alpha/p)}\right|^n && \text{(Identity transformation)} \\
&= 4 \cdot \sum_{j=1}^{(p-3)/2} \left(\frac{1}{2p} \cdot \frac{1}{\cos(\pi j/p)}\right)^n && \text{(Identity transformation)} \\
&= 4 \cdot \sum_{j=1}^{(p-3)/2} \left(\frac{1}{2p} \cdot \frac{1}{\sin(\pi(p-2j)/(2p))}\right)^n && \text{(Identity transformation)}
\end{aligned}$$

Observe that $\sin(x) \geqslant x/2$ for every $x \in (0, \pi/2)$. Hence,

$$\begin{aligned}
&\left|\sum_{\alpha \in F^* \setminus \{\frac{p-1}{2}, \frac{p+1}{2}\}} W(\alpha)\right| \\
&\leqslant 4 \cdot \sum_{j=1}^{(p-3)/2} \left(\frac{1}{2p} \cdot \frac{2}{\pi(p-2j)/(2p)}\right)^n \\
&= \pi^{-n} \cdot 4 \cdot \sum_{j=1}^{(p-3)/2} \left(\frac{2}{p-2j}\right)^n \\
&\leqslant \pi^{-n} \cdot 4 \cdot \left(\left(\frac{2}{3}\right)^n + \int_3^\infty \left(\frac{1}{x}\right)^n \mathrm{d}x\right) \\
&= \pi^{-n} \cdot 4 \cdot \left(\left(\frac{2}{3}\right)^n + \frac{1}{n+1}\left(\frac{1}{3}\right)^{n+1}\right) \\
&= \pi^{-n} \cdot \exp(-\Theta(n)).
\end{aligned}$$

This completes the proof.

[5] As p tends to infinity, it gets arbitrarily close to 2.

References

1. Donald Q. Adams, Hemanta K. Maji, Hai H. Nguyen, Minh L. Nguyen, Anat Paskin-Cherniavsky, Tom Suad, and Mingyuan Wang. Lower bounds for leakage-resilient secret sharing schemes against probing attacks. In *IEEE International Symposium on Information Theory ISIT 2021*. 3, 4, 9, 10, 20
2. 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. 10
3. Sanjeev Arora and Boaz Barak. *Computational complexity: a modern approach*. Cambridge University Press, 2009. 7
4. 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. 10
5. 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. 3, 4, 9, 10, 13, 20, 21
6. Fabrice Benhamouda, Akshay Degwekar, Yuval Ishai, and Tal Rabin. On the local leakage resilience of linear secret sharing schemes. *J. Cryptol.*, 34(2):10, 2021. 3, 10, 13
7. Andrej Bogdanov, Yuval Ishai, and Akshayaram Srinivasan. Unconditionally secure computation against low-complexity leakage. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology – CRYPTO 2019, Part II*, volume 11693 of *Lecture Notes in Computer Science*, pages 387–416, Santa Barbara, CA, USA, August 18–22, 2019. Springer, Heidelberg, Germany. 10
8. Ignacio Cascudo, Ronald Cramer, Diego Mirandola, and Gilles Zémor. Squares of random linear codes. *IEEE Transactions on Information Theory*, 61(3):1159–1173, 2015. 35
9. Eshan Chattopadhyay, Jesse Goodman, Vipul Goyal, Ashutosh Kumar, Xin Li, Raghu Meka, and David Zuckerman. Extractors and secret sharing against bounded collusion protocols. In *61st Annual Symposium on Foundations of Computer Science*, pages 1226–1242, Durham, NC, USA, November 16–19, 2020. IEEE Computer Society Press. 10
10. Mahdi Cheraghchi and Venkatesan Guruswami. Capacity of non-malleable codes. In Moni Naor, editor, *ITCS 2014: 5th Conference on Innovations in Theoretical Computer Science*, pages 155–168, Princeton, NJ, USA, January 12–14, 2014. Association for Computing Machinery. 13
11. Ronald Cramer. The arithmetic codex: Theory and applications (invited talk). In Kenneth G. Paterson, editor, *Advances in Cryptology – EUROCRYPT 2011*, volume 6632 of *Lecture Notes in Computer Science*, page 1, Tallinn, Estonia, May 15–19, 2011. Springer, Heidelberg, Germany. 3

12. Sebastian Faust, Pratyay Mukherjee, Daniele Venturi, and Daniel Wichs. Efficient non-malleable codes and key-derivation for poly-size tampering circuits. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology – EUROCRYPT 2014*, volume 8441 of *Lecture Notes in Computer Science*, pages 111–128, Copenhagen, Denmark, May 11–15, 2014. Springer, Heidelberg, Germany. 13
13. Arnaldo Garcia and Henning Stichtenoth. A tower of artin-schreier extensions of function fields attaining the drinfeld-vladut bound. *Inventiones mathematicae*, 121(1):211–222, 1995. 3
14. Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game or A completeness theorem for protocols with honest majority. In Alfred Aho, editor, *19th Annual ACM Symposium on Theory of Computing*, pages 218–229, New York City, NY, USA, May 25–27, 1987. ACM Press. 3
15. Valerii Denisovich Goppa. A new class of linear correcting codes. *Problemy Peredachi Informatsii*, 6(3):24–30, 1970. 3
16. 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. 10
17. 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. 10
18. Venkatesan Guruswami and Mary Wootters. Repairing reed-solomon codes. *IEEE Trans. Inf. Theory*, 63(9):5684–5698, 2017. 10
19. Yael Tauman Kalai and Leonid Reyzin. A survey of leakage-resilient cryptography. Cryptology ePrint Archive, Report 2019/302, 2019. https://eprint.iacr.org/2019/302. 2
20. 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. 2
21. 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. 2
22. 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. 10
23. Fuchun Lin, Mahdi Cheraghchi, Venkatesan Guruswami, Reihaneh Safavi-Naini, and Huaxiong Wang. Leakage-resilient secret sharing in non-compartmentalized models. In Yael Tauman Kalai, Adam D. Smith, and Daniel Wichs, editors, *ITC 2020: 1st Conference on Information-Theoretic Cryptography*, pages 7:1–7:24, Boston, MA, USA, June 17–19, 2020. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik. 10
24. Florence Jessie MacWilliams and Neil James Alexander Sloane. *The theory of error correcting codes*, volume 16. Elsevier, 1977. 15
25. Hemanta K. Maji, Hai H. Nguyen, Anat Paskin-Cherniavsky, Tom Suad, and Mingyuan Wang. Leakage-resilience of the shamir secret-sharing scheme against physical-bit leakages. In Anne Canteaut and François-Xavier Standaert, editors,

Advances in Cryptology – EUROCRYPT 2021, Part II, volume 12697 of *Lecture Notes in Computer Science*, pages 344–374, Zagreb, Croatia, October 17–21, 2021. Springer, Heidelberg, Germany. 3, 4, 7, 9, 10, 12, 13, 14, 20

26. Hemanta K. Maji, Anat Paskin-Cherniavsky, Tom Suad, and Mingyuan Wang. Constructing locally leakage-resilient linear secret-sharing schemes. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology – CRYPTO 2021, Part III*, volume 12827 of *Lecture Notes in Computer Science*, pages 779–808, Virtual Event, August 16–20, 2021. Springer, Heidelberg, Germany. 3, 4, 10, 12, 13, 17
27. James L Massey. Threshold decoding. 1963. 31
28. James L. Massey. Some applications of coding theory in cryptography. *Mat. Contemp*, 21(16):187–209, 2001. 3, 5
29. Jesper Buus Nielsen and Mark Simkin. Lower bounds for leakage-resilient secret sharing. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology – EUROCRYPT 2020, Part I*, volume 12105 of *Lecture Notes in Computer Science*, pages 556–577, Zagreb, Croatia, May 10–14, 2020. Springer, Heidelberg, Germany. 3, 11
30. Ryan O'Donnell. *Analysis of Boolean Functions*. 2014. 37
31. Krzysztof Pietrzak. Cryptography from learning parity with noise. In *International Conference on Current Trends in Theory and Practice of Computer Science*, 2012. 6
32. Oded Regev. The learning with errors problem. 6
33. Adi Shamir. How to share a secret. *Communications of the Association for Computing Machinery*, 22(11):612–613, November 1979. 3
34. 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. 10

Supporting Materials.

A Leakage-resilience of Partially Random Matrices

In the previous section, we have shown that, with high probability, the Massey secret-sharing scheme corresponding to a fully random generator matrix is leakage-resilient against $\mathcal{L}$ when $|\mathcal{L}| \leqslant |F|^{k-2-c}/8^{\ell}$ for any constant $c > 0$. Note that a fully random generator matrix requires $k \cdot (n-k)$ random elements from F.

In this section, we show a natural trade off between the amount of randomness one uses and the size of the leakage family that the secret-sharing scheme is resilient against. Intuitively, we show that, for any constant $t \in \mathbb{N}$, one may employ $t \cdot (n-k)$ random elements from F to sample the random generator matrix such that the Massey secret-sharing scheme is resilient against any $\mathcal{L}$ of size (approximately) $|F|^{t}/8^{\ell}$.

Let us start by defining some ways of sampling partially random matrices.

Definition 2 (t-row random matrix). *The t-row random matrix $\mathbf{M}^{(t)}$ is a matrix where elements $\mathbf{M}^{(t)}_{i,j}$ in the first t rows of the matrix are chosen independently uniformly random from F, and all the other elements are fixed to be zero.*

$$\mathbf{M}^{(t)} = \begin{pmatrix} \mathbf{M}^{(t)}_{1,1} & \mathbf{M}^{(t)}_{1,2} & \cdots & \mathbf{M}^{(t)}_{1,n-k} \\ \mathbf{M}^{(t)}_{2,1} & \mathbf{M}^{(t)}_{2,2} & \cdots & \mathbf{M}^{(t)}_{2,n-k} \\ \vdots & \vdots & & \vdots \\ \mathbf{M}^{(t)}_{t,1} & \mathbf{M}^{(t)}_{t,2} & \cdots & \mathbf{M}^{(t)}_{t,n-k} \\ 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$

Clearly, one needs $t(n-k)$ random field elements to sample $\mathbf{M}^{(t)}$.

Next, we define Wozencraft ensemble, standard technique in derandomization.

Definition 3 (Wozencraft Ensemble [27]). *Let finite field K be a degree k extension of the finite field F. There is a bijection between elements of K and F^k. For every element $\vec{\alpha} \in F^k$, we shall represent the corresponding element in K to be $(\vec{\alpha})_K \in K$. Fix an element $(\vec{\beta})_K \in K$. There exists a (unique) matrix $M(\vec{\beta}) \in F^{k\times k}$ such that, for any $(\vec{x})_K \in K$, it ensures*

$$(\vec{x})_K \cdot (\vec{\beta})_K = \left(\vec{x} \cdot M(\vec{\beta})\right)_K$$

That is, for all $\vec{x}$, the matrix product of $\vec{x}$ and $M(\vec{\beta})$ over F (which is a vector in F^k), corresponds to the product of $(\vec{x})_K$ and $(\vec{\beta})_K$ over K.

One may use the Wozencraft ensemble to sample a partially random matrix in $F^{k\times(n-k)}$ as follows. Let $m = \lceil (n-k)/k \rceil$ (i.e., $(m-1)k < (n-k) \leqslant mk$).

One samples m random vectors $\vec{\boldsymbol{\alpha}}^{(1)}, \vec{\boldsymbol{\alpha}}^{(2)}, \dots, \vec{\boldsymbol{\alpha}}^{(m)}$ in F^k. One picks the first $(n-k)$ columns of the matrix

$$\left[M\left(\vec{\boldsymbol{\alpha}}^{(1)}\right) \middle| M\left(\vec{\boldsymbol{\alpha}}^{(2)}\right) \middle| \cdots \middle| M\left(\vec{\boldsymbol{\alpha}}^{(m)}\right) \right]$$

as the sampled random matrix in $F^{k\times(n-k)}$. We shall use $\mathbf{W}$ as a partially random matrix sampled using Wozencraft ensemble. Clearly, one needs $\left\lceil \frac{n-k}{k} \right\rceil \cdot k \approx (n-k)$ random elements from F to sample $\mathbf{W}$.

We discuss some properties of the Wozencraft ensembles and provide some examples in Supporting Material C. We are now ready to state our theorem for this section.

Theorem 6. *Let $\mathcal{L}$ be an arbitrary collection of ℓ-bit joint leakage functions. Let $\mathbf{G}^+$ be the generator matrix (refer to Figure 1) sampled as follows.*

1. *Entries of $\vec{\mathbf{v}}_{\{k+1,\dots,n\}}$ are sampled independently uniformly random from F.*
2. *Matrix $\mathbf{R} \in F^{k\times(n-k)}$ is sampled as $\mathbf{M}^{(t)} + \mathbf{W}$, where $\mathbf{M}^{(t)}$ and $\mathbf{W}$ are sampled independently according to Definition 2 and Definition 3.*

The Massey secret-sharing scheme corresponding to $\mathbf{G}^+$ is ε-leakage-resilient to the leakage family $\mathcal{L}$ except *with probability (at most)*

$$\frac{|\mathcal{L}| \cdot 8^{\ell}}{\varepsilon^2 \cdot |F|^{t-2}}.$$

In particular, $\varepsilon = \left(|\mathcal{L}| \cdot 8^{\ell}/|F|^{t-2}\right)^{1/3}$ ensures that the failure probability is at most ε. Furthermore, ε is exponentially decaying when $|\mathcal{L}| \leqslant |F|^{t-2-\delta}/8^{\ell}$, where $\delta \in (0,1)$ is an appropriate constant. The random field elements required to sample $\mathbf{G}^+$ is (approximately) $(t+2)(n-k)$.

Intuitively, the Wozencraft ensemble ensures that G^+ is MDS with high probability and we rely on the t-row random matrix to prove our key technical lemma below.

The proof of this theorem follows analogously as the proof of Theorem 4. We present an outline of the proof below. First, we have our key technical lemma.

Lemma 3 (Key Technical Lemma). *For any secret $s \in F$ and any subset $A \subseteq F^n$, it holds that*

$$\mathop{\mathrm{E}}_{\mathbf{G}^+}\left[\left(\mathbf{X}_{s,A}\right)^2 \right] \leqslant \frac{1}{|F|^{t-1}}.$$

The proof of Theorem 6 from Lemma 3 is identical to the previous section. Hence, we omit it. Before we present the proof of Lemma 3, we define the following notion of bad set.

Definition 4 (Bad Set). *A pair of vectors $\vec{x}, \vec{y} \in F^k$ is "bad" if the following $2(n-k)$ random variables are* not *independently uniform.*

$$\vec{x} \cdot \mathbf{R}_{*,j} \quad \textit{and} \quad \vec{y} \cdot \mathbf{R}_{*,j} \qquad j \in \{1, 2, \ldots, n-k\}.$$

Succinctly, we use $\mathsf{Bad} \subseteq F^k \times F^k$ to denote the set of all "bad" $\vec{x}$ and $\vec{y}$. The density of badness of a (partially) random generator matrix is the density of the bad set, i.e., $|\mathsf{Bad}|/|F|^{2k}$.

Let us assume that the density of badness is β. One may prove Lemma 3 in the exactly manner as in the previous section. That is,

$$\begin{aligned}
\mathop{\mathrm{E}}_{\mathbf{G}^+}\left[(\mathbf{X}_{s,A})^2\right] &= \frac{1}{|F|^{2k}} \left(\sum_{(\vec{x},\vec{y}) \notin \mathsf{Bad}} \mathop{\mathrm{E}}_{\mathbf{G}^+}\left[\mathbf{T}_{\vec{x},\vec{y}}\right] + \sum_{(\vec{x},\vec{y}) \in \mathsf{Bad}} \mathop{\mathrm{E}}_{\mathbf{G}^+}\left[\mathbf{T}_{\vec{x},\vec{y}}\right] \right) \\
&\leqslant \frac{1}{|F|^{2k}} \left(\sum_{(\vec{x},\vec{y}) \notin \mathsf{Bad}} 0 + \sum_{(\vec{x},\vec{y}) \in \mathsf{Bad}} 1 \right) \\
&= \beta.
\end{aligned}$$

Now, we have reduced our problem to computing the density of badness. Note that, when $\mathbf{G}^+$ is the fully random matrix, the characterization of "bad" set is straightforward. "Bad" set is *exactly* those $\vec{x}$ and $\vec{y}$ that are linearly dependent.

However, for a partially random matrix such as the $\mathbf{G}^+$ that we consider in this section, the characterization of "bad" set might be highly non-trivial. Nevertheless, we note that an upper bound on the density of the badness suffices for this proof. And one may prove such upper bound by showing what $\vec{x}$ and $\vec{y}$ is *not* "bad". In particular, we note that

$$(x_1, \ldots, x_t) \text{ and } (y_1, \ldots, y_t) \text{ are linearly independent } \implies (\vec{x}, \vec{y}) \notin \mathsf{Bad}.$$

Clearly, when $(x_1, \ldots, x_t)$ and $(y_1, \ldots, y_t)$ are not linearly dependent, $\vec{x} \cdot \mathbf{M}^{(t)}$ and $\vec{y} \cdot \mathbf{M}^{(t)}$ are independently uniformly random. Since we sample $\mathbf{R}$ as $\mathbf{M}^{(t)} + \mathbf{W}$ where $\mathbf{W}$ is independent of $\mathbf{M}^{(t)}$, $\vec{x} \cdot \mathbf{R}$ and $\vec{y} \cdot \mathbf{R}$ are also independently uniformly random. Consequently, the density of badness is (at most) $1/|F|^{t-1}$, which completes the proof of Lemma 3 and, in turn, the proof of Theorem 6.

B On the Schur Product of Linear Codes

Consider the Massey secret-sharing scheme corresponding to a generator matrix $G^+ \in F^{(k+1)\times n}$. Suppose secrets s and t are secret-shared using this scheme, where the i^{th} party holds secret share s_i and t_i for $i \in \{1, 2, \ldots, n\}$.

In this section, we discuss when parties could locally transform the secret shares of s and t into the secret shares of $s \cdot t$. In particular, we show that, when we have the guarantee that $(k+1)^2 \leqslant n$, the products $s_i \cdot t_i,\ i \in \{1, 2, \ldots, n\}$ form the secret shares of the secret $s \cdot t$ (under a different Massey secret-sharing scheme).

Let us start with some necessary definitions.

Definition 5 (Schur Product). *For two vectors $A, B \in F^n$, where $A = (a_1, \dots, a_n)$ and $B = (b_1, \dots, b_n)$, the* Schur product *(i.e., coordinate-wise product) of A and B is defined as*

$$A \odot B := (a_1 \cdot b_1, a_2 \cdot b_2, \dots, a_n \cdot b_n).$$

Definition 6. *For a generator matrix $G^+ \in F^{(k+1)\times n}$, we use $\{0, 1, \dots, k\}$ to index its rows and $\{1, 2, \dots, n\}$ to index its columns. Given G^+, we define $\widetilde{G^+} \in F^{(k+1)^2\times n}$ as follows. The rows of $\widetilde{G^+}$ are indexed by $\{(i, j) : 0 \leqslant i, j \leqslant k\}$ and columns indexed by $\{1, 2, \dots, n\}$. The $(i, j)^{th}$ row of $\widetilde{G^+}$ is defined as*

$$\left(\widetilde{G^+}\right)_{(i,j),*} := G^+_{i,*} \odot G^+_{j,*}.$$

That is, the $(i, j)^{th}$ row of $\widetilde{G^+}$ is the Schur product of the i^{th} row and the j^{th} row of G^+.

Lemma 4. *For any two codewords $c^{(1)}, c^{(2)} \in \langle G^+\rangle$,*

$$c^{(1)} \odot c^{(2)} \in \left\langle \widetilde{G^+} \right\rangle.$$

That is, the Schur products of codewords of G^+ are codewords generated by the generator matrix $\widetilde{G^+}$.

Proof. For the ease of presentation, let $\mathcal{I}$ represent the set $\{0, 1, \dots, k\}\times\{0, 1, \dots, k\}$. For $0 \leqslant i \leqslant k$ and $1 \leqslant j \leqslant n$, let g_{ij} represent $(i, j)^{th}$ element of G^+. Suppose $x, y \in F^{k+1}$, where $x = (x_0, x_1, \dots, x_k)$ and $y = (y_0, y_1, \dots, y_k)$, such that

$$\begin{aligned} c^{(1)} &= x \cdot G^+ \\ c^{(2)} &= y \cdot G^+ \end{aligned}$$

We have

$$\begin{aligned} c^{(1)} \odot c^{(2)} &= \left(\dots, \sum_{i=0}^{k} x_i g_{i,j}\ , \dots\right) \odot \left(\dots, \sum_{i=0}^{k} y_i g_{i,j}\ , \dots\right) \\ &= \left(\dots, \left(\sum_{i=0}^{k} x_i g_{i,j}\right)\left(\sum_{i=0}^{k} y_i g_{i,j}\right), \dots\right) \\ &= \left(\dots, \sum_{(i_1,i_2)\in\mathcal{I}} x_{i_1} y_{i_2} g_{i_1,j} g_{i_2,j}, \dots\right) \\ &= \left(\dots, \sum_{(i_1,i_2)\in\mathcal{I}} x_{i_1} y_{i_2} \left(\widetilde{G^+}\right)_{(i_1,i_2),j}, \dots\right) \\ &= z \cdot \widetilde{G^+}, \end{aligned}$$

where $z \in F^{(k+1)^2}$ such that its entries are indexed by $\mathcal{I}$ and the $(i, j)^{th}$ entry is $x_i \cdot y_j$.

Lemma 4 says that if secrets s and t are secret-shared using the Massey secret-sharing scheme corresponding to G^{+}, then the local products of their secret shares, i.e., $s_i \cdot t_i$, become the secret shares of $s \cdot t$ using the Massey secret-sharing scheme corresponding to $\widetilde{G^{+}}$. Since the dimension of $\widetilde{G^{+}}$ is at most $(k+1)^2$, parties can reconstruct the secret if we have $n \geqslant (k+1)^2$.

We stress that the (Schur) square of codewords in $\langle G^{+} \rangle$ are not uniformly distributed. Moreover, since the square of $\langle G^{+} \rangle$ is only a subset of $\left\langle \widetilde{G^{+}} \right\rangle$, one may not need the $(k+1)^2$ parties to reconstruct the secret. As a notable example, when $\langle G^{+} \rangle$ is the Reed-Solomon code, i.e., the original secret-sharing is Shamir secret-sharing, it is well-known that the square of $\langle G^{+} \rangle$ resides inside a linear subspace of dimension $2k+1$. Hence, any $2k+1$ parties can reconstruct the product of the secret. Therefore, the Shamir secret-sharing-based MPC only requires $k < n/2$ to compute multiplication gates securely. For a random linear code, some works study the (expected) dimension of the square of the code. See, for example, [8] for discussions on a random linear code over a constant-size finite field.

C Properties and Examples of the Wozencraft Ensemble

C.1 Some properties of the Wozencraft Ensemble

Since field multiplication is a bilinear map, we have, for all $\vec{\alpha}, \vec{\beta} \in F^k$,

$$M(\vec{\alpha}) + M(\vec{\beta}) = M(\vec{\alpha} + \vec{\beta}).$$

Moreover, let $\vec{\delta}^{(i)} \in F^k$ be the vector that is 1 at the i^{th} coordinate and 0 otherwise. Then,

$$M(\vec{\alpha}) = \sum_{i=1}^{k} \alpha_i \cdot M(\vec{\delta}^{(i)}).$$

This observation implies why $M(\vec{\alpha})$ uniquely exists. Plus, sampling a random matrix corresponding to $M(\vec{\boldsymbol{\alpha}})$ is equivalent to sample $\boldsymbol{\alpha}_1, \dots, \boldsymbol{\alpha}_k$ independently and uniformly from F and compute

$$M(\vec{\boldsymbol{\alpha}}) = \sum_{i=1}^{k} \boldsymbol{\alpha}_i \cdot M(\vec{\delta}^{(i)}).$$

Finally, for any nonzero $\vec{\alpha}$, $M(\vec{\alpha})$ is full-rank since, for all $(\vec{\alpha})_K, \left(\vec{\beta}\right)_K \in K^*$, $(\vec{\alpha})_K \cdot \left(\vec{\beta}\right)_K \neq 0$. Moreover, fix any non-zero vector $\vec{x} \in F^k$, $\vec{x} \cdot M(\vec{\boldsymbol{\alpha}})$ is uniformly random over F^k since $(\vec{x})_K \cdot (\vec{\boldsymbol{\alpha}})_K$ is uniformly random over K.

C.2 A Concrete Example

We show a simple example of the Wozencraft matrix. Let $F = \mathbb{GF}(2)[X]/(X^2 + X + 1)$ be a field of order 4. Let $K = F[Z]/(Z^3 + Z + 1)$ be a degree 3 extension of F. The order of K is $4^3 = 64$.

Let $\vec{\beta} = (1, X, X+1) \in F^3$. In particular, $(\vec{\beta})_K = 1 \cdot Z^2 + X \cdot Z + (X+1) \cdot 1 \in K$. One may compute the Wozencraft matrix $M(\vec{\beta})$ corresponding to $\vec{\beta}$ as follows.

- For $\vec{\delta}^{(1)} = (1, 0, 0) \in F^3$, the corresponding $(\vec{\delta}^{(1)})_K = Z^2$ and
$$(\vec{\delta}^{(1)})_K \cdot (\vec{\beta})_K = Z^2 \cdot (Z^2 + X \cdot Z + (X+1)) = X \cdot Z^2 + (X+1) \cdot Z + X.$$
Therefore, $(1, 0, 0) \cdot M(\vec{\beta}) = (X, X+1, X)$ is the first row of $M(\vec{\beta})$.
- For $\vec{\delta}^{(2)} = (0, 1, 0) \in F^3$, the corresponding $(\vec{\delta}^{(2)})_K = Z$ and
$$(\vec{\delta}^{(2)})_K \cdot (\vec{\beta})_K = Z \cdot (Z^2 + X \cdot Z + (X+1)) = X \cdot Z^2 + X \cdot Z + 1.$$
Therefore, $(0, 1, 0) \cdot M(\vec{\beta}) = (X, X, 1)$ is the second row of $M(\vec{\beta})$.
- For $\vec{\delta}^{(3)} = (0, 0, 1) \in F^3$, the corresponding $(\vec{\delta}^{(3)})_K = 1$ and
$$(\vec{\delta}^{(3)})_K \cdot (\vec{\beta})_K = 1 \cdot (Z^2 + X \cdot Z + (X+1)) = Z^2 + X \cdot Z + X + 1.$$
Therefore, $(0, 0, 1) \cdot M(\vec{\beta}) = (1, X, X+1)$ is the third row of $M(\vec{\beta})$.

Thus, for $\vec{\beta} = (1, X, X+1) \in F^3$,

$$M(\vec{\beta}) = \begin{pmatrix} X & X+1 & X \\ X & X & 1 \\ 1 & X & X+1 \end{pmatrix} \in F^{3\times 3}.$$

D Efficient Decoding of any Linear MDS Codes with Small Dimension

For completeness, we shall include the following standard result in the theory of error-correcting codes.

Theorem 7. *Let $G \in F^{k\times n}$ be an MDS code. The decoding procedure* decode *in Figure 2 satisfies the following. For all (erroneous) codeword $c \in F^n$ and message $m \in F^k$ such that*[6]

$$\mathsf{HD}\Big(c\ ,\ m \cdot G \Big) < (n - k + 1)/2,$$

we have $\mathsf{decode}(c) = m$. *In particular,* decode *is efficient when k is a constant.*

[6] For two vectors $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in F^n$, $\mathsf{HD}(x, y)$ represents the Hamming distance between x and y. That is, $\mathsf{HD}(x, y) := |\{i : x_i \neq y_i\}|$.

```
decode($c$):

  1. For all subsets $J \subseteq \{1,2,\ldots,n\}$ of size $k$, compute
         $m^{(J)} := c_J \cdot \left(G_{*,J}\right)^{-1}$ .
     Intuitively, every $m^{(J)}$ is a vote for the correct message.
  2. Take the majority vote among all $m^{(J)}$, i.e.,
         $m^* := \arg\max_{m} \left|\left\{J \,:\, m = m^{(J)}\right\}\right|$.
     That is, $m^*$ is the message that receives the most votes.
  3. Output $m^*$ as the correct message.
```

Fig. 2. The decoding procedure decode.

Proof. Clearly, the time complexity of decode is $\mathcal{O}\big(n^k \cdot \mathsf{poly}(k)\big)$ and, hence, is efficient when k is a constant.

To see the correctness, let e represent $\mathsf{HD}(c, m \cdot G)$. Observe that the correct message m satisfies $\mathsf{HD}(c, m \cdot G) = e$ and, hence, will receive $\binom{n-e}{k}$ votes.

On the other hand, for any other message $m' \neq m$, $\mathsf{HD}(c, m' \cdot G) \geqslant (n - k + 1) - e$ and, hence, m' shall receive at most $\binom{k+e-1}{k}$ votes.

Therefore, since we require $e < (n - k + 1)/2$, the message that receives the most votes will be the correct message m.

E On the optimality of the parity distinguisher

Let $\mathcal{D}^{(0)}$ and $\mathcal{D}^{(1)}$ be two distributions over the universe $\{0,1\}^n$. Suppose $\mathcal{D}^{(0)}$ and $\mathcal{D}^{(1)}$ are $(n-1)$-indistinguishable.[7] That is, for any proper subset $S \subset \{1,2,\ldots,n\}$, we have

$$\mathsf{SD}\left(\left\{\begin{array}{c}\vec{x} \leftarrow \mathcal{D}^{(0)} \\ \text{Output } \vec{x}_S\end{array}\right\}, \left\{\begin{array}{c}\vec{x} \leftarrow \mathcal{D}^{(1)} \\ \text{Output } \vec{x}_S\end{array}\right\}\right) = 0.$$

For a distribution $\mathcal{D}$ and any set $S \subseteq 1, 2, \ldots, n$, define the bias of $\mathcal{D}$ over S as

$$\mathsf{bias}(\mathcal{D}, S) := \mathop{\mathrm{E}}_{\vec{x} \leftarrow \mathcal{D}}\left[(-1)^{\sum_{i \in S} x_i}\right].$$

The following fact about the bias shall be useful. We refer the readers to [30] for a proof.

[7] We do not use the term $(n-1)$-independent since the LSB of a uniformly random field element is not exactly uniform over $\{0,1\}$.

Lemma 5.

$$\mathsf{SD}\left(\mathcal{D}^{(0)}, \mathcal{D}^{(1)}\right) \leqslant \frac{1}{2} \cdot \sqrt{\sum_{S \in \mathit{\Omega}} \left(\mathsf{bias}(\mathcal{D}^{(0)}, S) - \mathsf{bias}(\mathcal{D}^{(1)}, S)\right)^2},$$

where $\mathit{\Omega}$ *is power set of* $\{1, 2, \ldots, n\}$.

Observe that $\mathcal{D}^{(0)}$ and $\mathcal{D}^{(1)}$ are $(n-1)$-indistinguishable implies that

$$\mathsf{bias}(\mathcal{D}^{(0)}, S) = \mathsf{bias}(\mathcal{D}^{(1)}, S)$$

for any proper subset $S \subset \{1, 2, \ldots, n\}$.

Therefore, this lemma implies that

$$\mathsf{SD}\left(\mathcal{D}^{(0)}, \mathcal{D}^{(1)}\right) \leqslant \frac{1}{2} \cdot \left|\mathsf{bias}(\mathcal{D}^{(0)}, \{1, 2, \ldots, n\}) - \mathsf{bias}(\mathcal{D}^{(1)}, \{1, 2, \ldots, n\})\right|.$$

This shows that the parity is the optimal distinguisher up to a constant as the right hand side is exactly the advantage of the parity distinguisher.