Leakage-resilient Linear Secret-sharing Against Arbitrary Bounded-size Leakage Family

Hemanta K. Maji[1], Hai H. Nguyen[1(✉)], Anat Paskin-Cherniavsky[2], Tom Suad[2], Mingyuan Wang[3], Xiuyu Ye[1], and Albert Yu[1]

[1] Department of Computer Science, Purdue University, West Lafayette, USA
{hmaji,nguye245,ye151,yu646}@purdue.edu, nhhai196@gmail.com
[2] Department of Computer Science, Ariel University, Ariel, Israel
anatpc@ariel.ac.il, tom.suad@msmail.ariel.ac.il
[3] Department of EECS, University of California Berkeley, Berkeley, USA
mingyuan@berkeley.edu

Abstract. Motivated by leakage-resilient secure computation of circuits with addition and multiplication gates, this work studies the leakage-resilience of linear secret-sharing schemes with a small reconstruction threshold against any *bounded-size* family of joint leakage attacks, i.e., the leakage function can leak *global* information from all secret shares.

We first prove that, with high probability, the Massey secret-sharing scheme corresponding to a random linear code over a finite field F is leakage-resilient against any ℓ-bit joint leakage family of size at most $|F|^{k-2.01}/8^{\ell}$, where k is the reconstruction threshold. Our result (1) bypasses the bottleneck due to the existing Fourier-analytic approach, (2) enables secure multiplication of secrets, and (3) is near-optimal. We use combinatorial and second-moment techniques to prove the result.

Next, we show that the Shamir secret-sharing scheme over a prime-order field F with randomly chosen evaluation places and with threshold k is leakage-resilient to any ℓ-bit joint leakage family of size at most $|F|^{2k-n-2.01}/(k! \cdot 8^{\ell})$ with high probability. We prove this result by marrying our proof techniques for the first result with the existing Fourier

Hemanta K. Maji, Hai H. Nguyen, Mingyuan Wang, Xiuyu Ye, and Albert Yu are supported in part by an NSF CRII Award CNS–1566499, NSF SMALL Awards CNS–1618822 and CNS–2055605, the IARPA HECTOR project, MITRE Innovation Program Academic Cybersecurity Research Awards (2019–2020, 2020–2021), a Ross-Lynn Research Scholars Grant (2021–2022), a Purdue Research Foundation (PRF) Award (2017–2018), and The Center for Science of Information, an NSF Science and Technology Center, Cooperative Agreement CCF–0939370. Anat Paskin-Cherniavsky and Tom Suad are supported by the Ariel Cyber Innovation Center in conjunction with the Israel National Cyber directorate in the Prime Minister's Office. Mingyuan Wang is also supported in part by DARPA under Agreement No. HR00112020026, AFOSR Award FA9550-19-1-0200, NSF CNS Award 1936826, and research grants by the Sloan Foundation, and Visa Inc. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Government or DARPA.

E. Kiltz and V. Vaikuntanathan (Eds.): TCC 2022, LNCS 13747, pp. 355–383, 2022.
https://doi.org/10.1007/978-3-031-22318-1_13

analytical approach. Moreover, it is unlikely that one can extend this result beyond $k/n \leqslant 0.5$ due to the technical hurdle for the Fourier-analytic approach.

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 into 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 [34] and secret-sharing schemes based on other Goppa codes [12,13,15,30]) or, more generally, some restrictive versions of linear secret-sharing schemes. Multiplication-friendly secret-sharing schemes require the reconstruction threshold $k+1$ to be less than half the number of parties n to facilitate secure multiplication. More generally, linear secret-sharing schemes facilitate secure multiplication when $(k+1) \leqslant \sqrt{n}$. 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 [1,25,28,31] 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 $(k+1)$-out-of-n Shamir secret-sharing is locally 1-bit leakage-resilient when $k/n > 0.85$. Recently, Maji, Nguyen, Paskin-Cherniavsky, and Wang [27] improved this to $k/n > 0.78$. Maji, Paskin-Cherniavsky, Suad, and Wang [28] proved that the Massey secret-sharing scheme [30] 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. [28] 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 prove leakage-resilience against this single function when $k/n \leqslant 0.5$.

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 $(k+1) = 2$ (and polynomially large n). However, their approach still follows the Fourier-analytic approach. Consequently, one cannot hope to extend their result to any small family of leakage functions containing the quadratic residuosity leakage.

Summary of Our Results and Technical Contribution. This work studies the Monte-Carlo construction of leakage-resilience secret-sharing schemes. Our work studies the *general leakage-resilience* of (1) the Massey secret-sharing scheme corresponding to a random linear code, and (2) the Shamir secret-sharing scheme with random evaluation places. The leakage function can leak global information from all secret shares.

First, we show that the Massey secret-sharing scheme corresponding to a random linear code[1] with dimension $(k+1) \geqslant 4$ is leakage-resilient to any

[1] This random linear code only needs to be chosen once. With only an exponentially small failure probability, the Massey secret-sharing scheme corresponding to this code shall be leakage-resilient. For instance, this random linear code can be specified by, for example, a common random string (CRS).

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 the 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 different from existing works [5,25,27,28] as all of them rely on a Fourier-analytic approach to prove the leakage-resilience. In particular, our technical approach bypasses the bottleneck result from the quadratic residuosity local leakage function, as indicated by [28].

Second, we show that a $(k+1)$-out-of-n Shamir secret-sharing scheme with $k > n/2$ and random evaluation places is leakage-resilience to any bounded-size leakage family except with an exponentially small probability. This result is a partial derandomization of the leakage-resilience of the Massey secret-sharing scheme corresponding to a random linear code. We prove our result using the second-moment technique inspired by the first result and the Fourier-analytic approach together with Bézout's theorem inspired by [25]. Our result is near-optimal due to the inherent barrier when $k/n \leqslant 0.5$ for the Fourier-analytic approach pointed out in [28] (see Remark 2 for details).

1.1 Our Contribution

Table 1. Summary of relevant prior work (in chronological order) and our results, where λ is the security parameter.

Relevant work	Secret sharing scheme	Leakage family	Reconstruction threshold $(k+1)$
BDIR'18 [5]	Shamir secret-sharing with any fixed evaluation places	arbitrary local	$k > 0.85 \cdot n$
MPSW'21 [28]	Massey secret-sharing of a random linear code	arbitrary local	$k > 0.5 \cdot n$
MNPSW'21 [25]	Shamir secret-sharing with random evaluation places	physical-bit	$k \geqslant 1$, $n = \mathsf{poly}(\lambda)$
MNPW'22 [27]	Shamir secret-sharing with any fixed evaluation places	arbitrary local	$k > 0.78 \cdot n$
Our work	Massey secret-sharing of a random linear code	arbitrary global of bounded size	$k \geqslant 3$, $n = \mathsf{poly}(\lambda)$
	Shamir secret-sharing with random evaluation places	arbitrary global of bounded size	$k > 0.5 \cdot n$, $n = \mathsf{poly}(\lambda)$

In this section, we present the main result of this paper. We refer the readers to Table 1 for a comparison between our results and the state-of-the-art results.

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 $2^{\lambda-1} \leqslant |F| < 2^{\lambda}$. Let n be the number of parties and $k+1$ be the reconstruction threshold.

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 [30]. Given a linear code $C \subseteq F^{(n+1)}$, the Massey secret-sharing scheme 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 $s_i \in F$.

Shamir Secret-Sharing Schemes [34]. Let $s \in F$ be the secret and $\vec{X} = (X_1, X_2, \ldots, X_n) \in (F^*)^n$ be distinct evaluation places, i.e., $X_i \neq X_j$ for all $i \neq j$. The $[n, k+1, \vec{X}]_F$-Shamir secret-sharing scheme picks a random polynomial $P(X) \in F[X]/X^{k+1}$ conditioned on the fact that $P(0) = s$. The secret shares of parties $1, 2, \ldots, n$ are $s_1 = P(X_1), s_2 = P(X_2), \ldots, s_n = P(X_n)$, respectively.

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. We always consider a finite field F such that $2^{\lambda-1} \leqslant |F| < 2^{\lambda}$ and $n, k = \mathsf{poly}(\lambda)$ unless specified.

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

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

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 perform secure multiplication.

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 [32,33]. However, if k is a constant, one can efficiently decode using (exhaustive search-based) majority voting techniques.

Remark 1. Our result is near-optimal as follows. Define $\mathcal{L}^*$ as the set of all leakage functions defined by $(S, \alpha_1, \alpha_2, \ldots, \alpha_{k+1})$, where $S = \{i_1, i_2, \ldots, i_{k+1}\} \subseteq \{1, 2, \ldots, n\}$, and $\alpha_1, \ldots \alpha_{k+1} \in F$. The $(\ell = 1)$-bit leakage function corresponding to $(S, \alpha_1, \ldots, \alpha_{k+1})$ 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 $s_{i_1}, \ldots, s_{i_{k+1}}$ represents the i_1-th, $\ldots$, i_{k+1}-th secret share, respectively. The size of this leakage family is $\mathcal{O}(n^{k+1} \cdot |F|^{k+1})$.

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 $i_1, \ldots, i_{k+1}$ 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 $(S = \{i_1, \ldots, i_{k+1}\}, \alpha_1, \ldots, \alpha_{k+1})$ 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 the leakage family that leaks t secret shares in the entirety and one physical bit from the remaining shares. Then, 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 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 $\binom{\lambda}{2^d} \cdot 2^{2^d}$. The size of the local leakage family where every local leakage function is NC^0_d that leaks one bit 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. 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. The number of circuits of size (at most) s is upper-bounded by $(10s) \cdot 2^s$ [3]. Hence, the size of the local leakage family where every local leakage function is a circuit of size (at most) s that leaks one bit is upper-bounded by $(10s \cdot 2^s)^n$. Consequently, the prerequisite of Corollary 1 holds as long as $k = \omega(n \cdot s/\lambda)$. Thus, 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. 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.

Leakage-resilience of Randomly Twisted Additive Secret-Sharing. Fix a finite field F. The *additive secret-sharing scheme* over F for n parties chooses random secret shares $s_1, s_2, \ldots, s_n \in F$ conditioned on $s_1 + s_2 + \cdots + s_n = s$, where $s \in F$ is the secret. For a (publicly-known) *twist* $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in (F^*)^n$, the corresponding *twisted additive secret-sharing scheme* chooses random secret shares $s_1, s_2, \ldots, s_n \in F$ conditioned on $\sum_{i=1}^n \alpha_i \cdot s_i = s$. The *randomly twisted additive secret-sharing scheme* picks a uniformly random public twist $(\alpha_1, \ldots, \alpha_n) \in (F^*)^n$ and shares the secret using the corresponding twisted additive secret-sharing scheme.

When the reconstruction threshold is identical to the number of parties, our result also implies the leakage-resilience of randomly twisted additive secret-sharing.[2]

Corollary 5. *Let $c > 0$ be an arbitrary positive constant. Let $\mathcal{L}$ be an arbitrary ℓ-bit leakage family such that*

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

If $n = o(\lambda)$, the randomly twisted additive secret-sharing scheme is $(\mathcal{L}, \exp(-\Omega(\lambda)))$-leakage-resilient except with probability $\exp(-\Omega(\lambda))$.

Reverse Multiplication Friendly Embedding (RMFE). The *reverse multiplication friendly embedding (RMFE)* [7,8,10] is a *bilinear map* that embeds SIMD-style multiple instances of the multiplication over a small field (say F') into a single multiplication instance over an extension field F. Therefore, RMFE *modularly packs* multiple F' secrets into one F secret in a manner that is addition and multiplication friendly, making these mappings suitable for cryptographic applications.

[2] This observation is due to that a random *square matrix* over a large enough field F is full-rank with overwhelming probability.

The number of packed secrets is linear in the degree of the extension [8,10]. For example, one can pack $\Theta(\lambda)$ secrets in $F' = GF[2])$ (i.e., binary secrets) into one $F = GF[2^\lambda]$ secret. An *RMFE-based packed secret-sharing scheme* packs F' secrets into one F secret and secret shares this F secret.

Observe that our leakage-resilience result for the Massey secret-sharing schemes corresponding to random linear codes also holds for extension fields F with arbitrary small characteristics (e.g., characteristic-2). Consequently, the RMFE-based packed secret-sharing scheme over F' (as described above) is leakage-resilient because the secret-sharing over F is leakage-resilient. This consequence extends our technical results to construct leakage-resilient secret-sharing schemes for (multiple) constant-size secrets.

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 $\boldsymbol{\alpha}^{(1)}, \ldots, \boldsymbol{\alpha}^{(m)} \in K$. 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.

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 types of partially random matrices, we prove the following theorem. A proof is provided in Appendix 6.

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 $(t+1)(n-k) + k \cdot \lceil \frac{n-k}{k} \rceil$.

Result II: Leakage resilience of Shamir's secret sharing schemes with random evaluation places. Our second result is the following.

Theorem 3. *Let F be a prime order field of size p. Let $\mathcal{L}$ be an arbitrary family of ℓ-bit joint leakage functions. Define $\vec{\mathbf{X}}$ be a random variable, where $\vec{\mathbf{X}}$ is chosen uniformly at random from the set $(F^*)^n$ such that $\mathbf{X}_i \neq \mathbf{X}_j$ for all $i \neq j$. The $[n, k+1, \vec{\mathbf{X}}]_F$-Shamir's secret-sharing scheme corresponding to randomly chosen evaluation places $\vec{\mathbf{X}}$ is $(\mathcal{L}, \varepsilon)$-leakage-resilient* except *with probability at most*

$$\frac{4 \cdot |\mathcal{L}| \cdot 8^\ell \cdot p^{n-k+1} \cdot k!}{\varepsilon^2 \cdot (p-n)^k}.$$

In particular, setting $\varepsilon = \left(4 \cdot |\mathcal{L}| \cdot 8^\ell \cdot p^{n-k+1} \cdot k!/(p-n)^k\right)^{1/3}$ ensures that the failure probability is at most ε.

Our proof of this theorem combines the combinatorial proof techniques used in our first result with the Fourier-analytic approach in the literature [5,25,27,28].

Observe that the randomness complexity of this construction is $\mathcal{O}(n \cdot \lg|F|)$ bits. Next, we interpret our technical result as follows. We omit the details for the leakage-resilience of Shamir secret-sharing schemes against local leakage with bounded-depth or bounded-size circuits.

Corollary 6. *Let c and δ be arbitrary positive constants. Let $\mathcal{L}$ be an arbitrary ℓ-bit leakage family such that*

$$|\mathcal{L}| \leqslant \frac{(p-n)^{k-c}}{4 \cdot 8^\ell \cdot p^{n-k+1} \cdot k!}.$$

Let F be a finite field such that $2^{\lambda-1} \leqslant |F| < 2^\lambda$, $k = (1/2+\delta)n$, and $n = \mathsf{poly}(\lambda)$. Then, the $[n, k+1, \vec{\mathbf{X}}]_F$-Shamir's secret-sharing scheme is $(\mathcal{L}, \exp(-\Omega(\lambda)))$-leakage-resilient except with *probability* $\exp(-\Omega(\lambda))$.

We note that any constant n and $k > (n+1)/2$ suffices to ensure leakage-resilience for any small enough leakage family, for example, the physical-bit leakage family.

Remark 2. The inherent barrier of the existing Fourier's analytic approach as pointed out in [28] tells us that k/n must be greater than $1/2$ to achieve leakage-resilient even against a leakage family of size one that contains only the quadratic residue leakage function. Our result shows that any $k > (n+1)/2$ suffices, and the larger value of k the bigger size of the leakage family. Let $\mathcal{L}^{**}$ be the set of all 1-bit leakage functions that indicate whether $\lambda_1 \cdot s_1 + \lambda_2 \cdot s_2 + \cdots + \lambda_{k+1} \cdot s_{k+1} = 0$, where $s_1, s_2, \ldots, s_{k+1}$ are the secret shares of parties $1, 2, \ldots, k+1$, respectively, and λ_j are the Lagrange coefficients defined as

$$\lambda_j := \prod_{i \in \{1,2,\cdots,k+1\} \setminus \{j\}} \left(\frac{X_i}{X_i - X_j}\right).$$

The size of $\mathcal{L}^{**}$ is equal to the number of tuples $(\lambda_1, \lambda_2, \cdots, \lambda_k)$, which is equal to $(p-1)\cdot(p-2)\cdots(p-k-1)$. For any Shamir's secret-sharing scheme corresponding to the evaluation places $\vec{\mathbf{X}}$, there is a leakage function in the family $\mathcal{L}^{**}$ that can distinguish the secret $s^{(0)} = 0$ from any other secret. Observe that when k is close to n, our result is near-optimal.

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 [2,4,9,11, 16,22,35]. The other direction is to investigate the leakage-resilience of prominent secret-sharing schemes against local leakages [1,5,23,25,28]. We shall focus our discussion on the second line of work.

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's secret-sharing schemes over characteristic two fields are utterly broken against general one-bit local leakages.

For the case of prime-order fields, [6,28] proved that Shamir secret-sharing scheme is robust to one-bit local leakage if the reconstruction threshold $k \geqslant 0.85n$. Very recently, [27] improved this threshold to $k \geqslant 0.78n$. Furthermore, [28] 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 $k \geqslant 2$.

From the lower bound perspective, Nielsen and Simkin [31] proved that Shamir secret-sharing scheme is not locally leakage-resilient if $m \approx k \cdot \log|F|/n$ bits is leaked from every secret share. Finally, the recent work of [26] proved that the "parity-of-parity" attack [25] on the additive secret sharing scheme has the optimal distinguishing advantage of $2^{-\Theta(n)}$. Hence, if an additive secret sharing scheme is 1-bit locally leakage-resilient it must hold that $n = \omega(\log \lambda)$.

2 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 represent the number of secret shares and $k+1$ represent the reconstruction threshold of the secret-sharing scheme.

Overview of Result I. 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. 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 Fig. 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

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

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

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

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 2.

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. Appendix 6 provides additional details on this result.

On the Combinatorial Approach. Our combinatorial approach deviates from the Fourier-analytical approach of prior works and, hence, circumvents the roadblocks that are inherent to it. Surprisingly, this elementary approach already gives us near-optimal results in terms of the size of the leakage family. However, our approach does not extend to proving the leakage-resilience of Massey secret-sharing corresponding to a fixed linear code or Shamir secret-sharing with fixed evaluation places. It seems that our ideas does not extend to large leakage family, for example, the entire local leakage family.

Overview of Result II. We shall restrict the field F to be a prime order field of size p in the following discussion. Let $\vec{X}$ be distinct evaluation places in $(F^*)^n$. Consider the $[n, k+1, \vec{X}]_F$-Shamir's secret-sharing scheme. Observe that the secret shares corresponding to the secret 0 are identical to the linear code $C_{\vec{X}} = \langle G_{\vec{X}} \rangle$, where $G_{\vec{X}}$ is the following matrix.

$$G_{\vec{X}} = \begin{pmatrix} X_1 & X_2 & \cdots & X_n \\ X_1^2 & X_2^2 & \cdots & X_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ X_1^k & X_2^k & \cdots & X_n^k \end{pmatrix}.$$

Observe also that the secret shares of a secret $s \in F$ is the affine subspace $s \cdot \vec{1} + \langle G_{\vec{X}} \rangle$, where $\vec{1}$ is the vector of length n whose every coordinate is one. We note that $C_{\vec{X}}$ is an $[n, k]_F$ maximum distance separable code.

We shall consider random distinct evaluation places $\vec{\mathbf{X}}$, and so the random matrix $\mathbf{G}_{\vec{\mathbf{X}}}$, which is a partial derandomization of the matrix $\mathbf{G}$ considered in the first result. Our objective is to prove that Shamir's secret-sharing scheme corresponding to $\mathbf{G}_{\vec{\mathbf{X}}}$ is $(\mathcal{L}, \varepsilon)$-leakage-resilient, with overwhelming probability.

Using a similar argument as in the case of random linear code, our objective is reduced to show that the random variable $\mathbf{Y}_{s,A}$ is sufficiently small with overwhelming probability, where

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

We once again use the second-moment technique to prove that the random variable $\mathbf{Y}_{s,A}$ is sufficiently small with high probability (see Lemma 3). However, we use a Fourier-analytical approach instead of the combinatorial approach for the random linear code. The randomness in $\mathbf{G}_{\vec{\mathbf{X}}}$ is much less compared to the randomness in $\mathbf{G}$. Consequently, the combinatorial proof does not go through for $\mathbf{G}_{\vec{\mathbf{X}}}$. To circumvent this, we rely on the Fourier-analytical approach [5,25,28]. However, unlike prior works, our analysis can handle not only local leakage but also global leakage. In addition, our proof imports a result (Claim 3) from [25] that upper-bounds the probability that a codeword $\vec{\alpha}$ belongs to a random code $\langle \mathbf{G}_{\vec{\mathbf{X}}} \rangle^{\perp}$, which follows from a generalization of Bézout's theorem.

Comparison with **[25].** In a 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 $(k+1) \geqslant 2$. The Shamir secret-sharing scheme is multiplication-friendly for any $k < n/2$.

In comparison to our result I, 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's 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 [28]).

The result in [25] is incomparable to our result II. Their result is only for the physical-bit leakage family but works for any $(k+1) \geqslant 2$, while our result works for any bounded-size joint leakage family but requires that the reconstruction threshold is $> (n+1)/2$.

Comparison with **[6,28].** 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. [28] proved that the Massey secret-sharing scheme corre-

sponding to a random linear code is leakage-resilient to all local leakage functions when $k > 0.5n$.

Both results are incomparable to our result I as they require a significantly higher threshold k, but proved a stronger result, i.e., leakage-resilience against all local leakage functions. In particular, the parameter settings for k and n in their results are not multiplication-friendly.

Again both results are incomparable to our result II as the size of all the local leakage functions is significantly larger than the size of the bounded-size joint leakage family in ours. Theirs and ours require a high reconstruction threshold.

3 Preliminaries

Throughout this paper, we use F for a finite 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 $\frac{1}{2} \cdot \sum_x |\Pr[\mathbf{A} = x] - \Pr[\mathbf{B} = x]|$.

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 $\{x + s \colon s \in S\}$.

3.1 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 $\{0, 1, \ldots, k\}$ as row indices and $\{0, 1, \ldots, n\}$ as column indices for a matrix $G^+ \in F^{(k+1)\times(n+1)}$.

3.2 Codes and Linear 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 $(s, s_1, \ldots, s_n) \in C$ to share the secret s. The secret shares of parties $1, \ldots, n$ are $s_1, \ldots, s_n$, 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 $\{0, 1, \ldots, k\}$ and its columns are indexed by $\{0, 1, \ldots, n\}$. Let $s \in F$ be the secret. The secret-sharing scheme picks independent and uniformly random $r_1, \ldots, r_k \in F$. Let

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

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

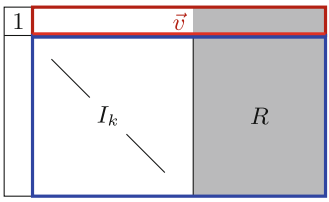

Fig. 1. A pictorial summary of the generator matrix $G^+ = [I_{k+1} \mid P]$, where P is the shaded matrix. The indices of rows and columns of G^+ are $\{0, 1, \ldots, k\}$ and $\{0, 1, \ldots, n\}$, respectively. The (blue) matrix $G = [I_k \mid R]$ is a submatrix of G^+. In particular, the secret shares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

Suppose parties $i_1, \ldots, i_t \in \{1, \ldots, n\}$ come together to reconstruct the secret with their, respective, secret shares $s_{i_1}, \ldots, s_{i_t}$. Let $G^+_{*,i_1}, \ldots, G^+_{*,i_t} \in F^{(k+1)\times 1}$ represent the columns indexed by $i_1, \ldots, i_t \in \{1, \ldots, n\}$, respectively. If the column $G^+_{*,0} \in F^{(k+1)\times 1}$ lies in the span of $\left\{G^+_{*,i_1}, \ldots, G^+_{*,i_t}\right\}$ then these parties can reconstruct the secret s using a linear combination of their secret shares. If the column G^+_{*0} *does not* lie in the span of $\left\{G^+_{*,i_1}, \ldots, G^+_{*,i_t}\right\}$ then the secret remains *perfectly hidden* from these parties.

Shamir Secret-sharing Schemes. Let F be a prime field. Let $\vec{X} = (X_1, \ldots, X_n)$ be *evaluation places* satisfying (1) $X_i \in F^*$ for all $1 \leqslant i \leqslant n$, and (2) $X_i \neq X_j$ for all $1 \leqslant i < j \leqslant n$. The corresponding $[n, k, \vec{X}]_F$-Shamir secret-sharing is defined as follows.

- Given secret $s \in F$, $\mathsf{Share}^{\vec{X}}(s)$ independently samples a random $a_i \in F$, for all $1 \leqslant i < k$. The i^{th} share of $\mathsf{Share}^{\vec{X}}(s)$ is

$$\mathsf{Share}^{\vec{X}}(s)_i := s + a_1 X_i + a_2 X_i^2 + \cdots + a_{k-1} X_i^{k-1}.$$

- Given shares $\left(\mathsf{Share}^{\vec{X}}(s)_{i_1}, \ldots, \mathsf{Share}^{\vec{X}}(s)_{i_t}\right)$, $\mathsf{Rec}^{\vec{X}}$ interpolates to obtain the unique polynomial $f \in F[X]/X^k$ such that $f(X_{i_j}) = \mathsf{Share}^{\vec{X}}(s)_{i_j}$ for all $1 \leqslant j \leqslant t$, and outputs $f(0)$ to be the reconstructed secret.

3.3 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 $(s_1, \ldots, s_n)$ for the secret s, and (b) output $L(s_1, \ldots, s_n)$.

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*

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

3.4 Fourier Analysis

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

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

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

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

where $\vec{\alpha} \cdot \vec{x}$ is the inner product over F^n. The respective Fourier coefficient $\widehat{f}(\vec{\alpha})$ is defined as

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

We have the following facts and lemma.

Fact 1 (Fourier Inversion Formula) $f(\vec{x}) = \sum_{\alpha \in F^n} \widehat{f}(\vec{\alpha}) \cdot \omega^{\vec{\alpha} \cdot \vec{x}}$.

Fact 2 (Parseval's Identity) $\frac{1}{p^n} \sum_{\vec{x} \in F^n} |f(\vec{x})|^2 = \sum_{\vec{\alpha} \in F^n} |\widehat{f}(\vec{\alpha})|^2$.

Lemma 1 (Poisson Summation Formula). *Let $C \subseteq F^n$ be a linear code with dual code $C^\perp$. Let $f \colon F^n \to \mathbb{C}$ be an arbitrary function. Then, the following identity holds.*

$$\mathop{\mathrm{E}}_{\vec{x} \in C} [f(\vec{x})] = \sum_{\vec{\alpha} \in C^\perp} \widehat{f}(\vec{\alpha})$$

In particular, if $f(\vec{x}) = f_1(x_1) \cdot f_2(x_2) \cdots f_n(x_n)$, where $f_i \colon F \to \mathbb{C}$ for every $1 \leqslant i \leqslant n$, it holds that

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

4 Leakage-resilience of Fully Random Code

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 3. 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 [28] 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

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

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

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

Let us first show why Lemma 2 is sufficient to prove Theorem 4.

Proof (Proof of Theorem 4 *using* Lemma 2*).* First, Lemma 2 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

$$\begin{aligned} \Pr_{\mathbf{G}^+} \left[|\mathbf{X}_{s,A}| \geqslant t \right] &\leqslant \frac{\mathbb{E}[\left(\mathbf{X}_{s,A} \right)^2]}{t^2} && \text{(Markov's inequality)} \\ &\leqslant \frac{1}{t^2 \cdot |F|^{k-1}}. && \text{(Lemma 2)} \end{aligned}$$

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

$$\begin{aligned} & \Pr_{\mathbf{G}^+} \left[\exists s,\ \mathsf{SD}\left(\mathbf{L}\left(0 \right), \mathbf{L}\left(s \right) \right) > \varepsilon/2 \right] \\ = & \Pr_{\mathbf{G}^+} \left[\exists s,\ \frac{1}{2} \cdot \sum_{\vec{w} \in \{0,1\}^\ell} |\mathbf{X}_{s,A_{\vec{w}}}| > \varepsilon/2 \right] && \text{(By definition of SD and } \mathbf{X}_{s,A_{\vec{w}}}) \end{aligned}$$

$$\leqslant \sum_{s\in F}\left(\Pr_{\mathbf{G}^+}\left[\sum_{\vec{w}\in\{0,1\}^\ell}|\mathbf{X}_{s,A_{\vec{w}}}|>\varepsilon\right]\right) \qquad \text{(Union bound)}$$

$$\leqslant \sum_{s\in F}\left(\Pr_{\mathbf{G}^+}\left[\exists\vec{w}\in\{0,1\}^\ell,\ |\mathbf{X}_{s,A_{\vec{w}}}|>\varepsilon/2^\ell\right]\right) \qquad \text{(Pigeon-hole principle)}$$

$$\leqslant \sum_{s\in F}\sum_{\vec{w}\in\{0,1\}^\ell}\left(\Pr_{\mathbf{G}^+}\left[|\mathbf{X}_{s,A_{\vec{w}}}|>\varepsilon/2^\ell\right]\right) \qquad \text{(Union bound)}$$

$$\leqslant |F|\cdot 2^\ell\cdot\frac{2^{2\ell}}{\varepsilon^2\cdot|F|^{k-1}} \qquad \text{(since Eq. 1 applies to arbitrary } A \text{ and } s)$$

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

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 (Proof of Lemma 2*).* Recall that

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

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

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

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 Fig. 1). Hence, one may write

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

where

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

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

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

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

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

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

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

Therefore, this completes the proof as

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

5 Leakage-resilience of Shamir Secret-sharing Schemes with Random Evaluation Places

This section considers Shamir secret-sharing over a prime order field and with randomly chosen evaluation places. Fix any small (joint) leakage family $\mathcal{L}$. We shall show that Shamir secret-sharing with distinct random evaluation places is leakage-resilient to $\mathcal{L}$.

In this section, we write $f(\lambda) \lesssim g(\lambda)$ for $f(\lambda) = (1 + \mathrm{o}(1)) \cdot g(\lambda)$.

Theorem 5. *Let $\mathcal{L}$ be an arbitrary family of ℓ-bit joint leakage functions. The $[n, k+1, \vec{\mathbf{X}}]_F$-Shamir's secret-sharing scheme corresponding to randomly chosen evaluation places $\vec{\mathbf{X}}$ is ε-leakage-resilient against $\mathcal{L}$* except with *probability at most*

$$\frac{4 \cdot |\mathcal{L}| \cdot 8^\ell \cdot p^{n-k+1} \cdot k!}{\varepsilon^2 \cdot (p-n)^k}.$$

In particular, letting $\varepsilon = \left(4 \cdot |\mathcal{L}| \cdot 8^\ell \cdot p^{n-k+1} \cdot k!/(p-n)^k\right)^{1/3}$ ensures that the failure probability δ is at most ε. Furthermore, ε is exponentially decaying when $|\mathcal{L}| \lesssim (p-n)^{k-c}/(4 \cdot 8^\ell \cdot p^{n-k+1} \cdot k!)$, where $c > 0$ is an arbitrary constant.

In contrast to the proof of Theorem 4, we rely on Fourier-analytical techniques to prove Theorem 5. In this section, we restrict to prime field F of order p. Consider an $[n, k+1, \vec{\mathbf{X}}]_F$-Shamir secret-sharing scheme with randomly chosen evaluation places $\vec{\mathbf{X}}$. Let $C_{\vec{\mathbf{X}}}$ be the set of all possible secret shares corresponding to the secret 0. Recall that $C_{\vec{\mathbf{X}}} = \left\langle G_{\vec{\mathbf{X}}} \right\rangle$, where the generator matrix of $G_{\vec{\mathbf{X}}}$ is the following matrix.

$$G_{\vec{\mathbf{X}}} = \begin{pmatrix} \mathbf{X}_1 & \mathbf{X}_2 & \cdots & \mathbf{X}_n \\ \mathbf{X}_1^2 & \mathbf{X}_2^2 & \cdots & \mathbf{X}_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{X}_1^k & \mathbf{X}_2^k & \cdots & \mathbf{X}_n^k \end{pmatrix}.$$

Furthermore, $\left\langle G_{\vec{\mathbf{X}}} \right\rangle + s \cdot \vec{1}$ is the set of all the secret shares of secret s for any $s \in F$. For any secret $s \in F$ and any subset $A \subseteq F^n$, define

$$\begin{aligned} \mathbf{Y}_{s,A} &:= \frac{1}{p^k} \cdot \left(\left| \left\langle \mathbf{G}_{\vec{\mathbf{X}}} \right\rangle \cap A \right| - \left| \left(\left\langle \mathbf{G}_{\vec{\mathbf{X}}} \right\rangle + s \cdot \vec{\mathbf{1}} \right) \cap A \right| \right) \\ &= \mathop{\mathrm{E}}_{\vec{x} \in C_{\vec{\mathbf{X}}}} \left[\mathbb{1}_A(\vec{x}) \right] - \mathop{\mathrm{E}}_{\vec{x} \in C_{\vec{\mathbf{X}}}} \left[\mathbb{1}_A(\vec{x} + s \cdot \vec{1}) \right] \end{aligned}$$

Intuitively, the random variable $\mathbf{Y}_{s,A}$ represents the difference in the probability that the secrets shares falls into the set A between the secret being 0 and s. The following lemma is the main technical result of Theorem 5.

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

$$\mathop{\mathrm{E}}_{\vec{\mathbf{X}}} \left[(\mathbf{Y}_{s,A})^2 \right] \leqslant \frac{4 \cdot p^{n-k+1} \cdot k!}{(p-(n-k+1)) \cdots (p-n)} \lesssim \frac{4 \cdot p^{n-k+1} \cdot k!}{(p-n)^k}$$

Note that A need not be a product space. Now, we first prove Theorem 5 using Lemma 3.

Proof (Proof of Theorem 5*).* Using a similar argument as in the proof of Theorem 4, one can show that

$$\Pr_{\vec{\mathbf{X}}} \left[\mathbf{G}_{\vec{\mathbf{X}}} \text{ is } \textit{not } \varepsilon\text{-leakage-resilient against } \mathcal{L} \right]$$

$$\leqslant \sum_{L\in\mathcal{L}}\sum_{s\in F}\sum_{\vec{w}\in\{0,1\}^\ell}\left(\Pr_{\mathbf{G}_{\vec{\mathbf{X}}}}\left[|\mathbf{Y}_{s,A_{\vec{w}}}|\geqslant \varepsilon/2^\ell\right]\right) \qquad \text{(Union bound)}$$

$$\leqslant \sum_{L\in\mathcal{L}}\sum_{s\in F}\sum_{\vec{w}\in\{0,1\}^\ell}\frac{4\cdot p^{n-k}\cdot k!}{(p-(n-k+1))\cdots(p-n)}\cdot\left(\frac{2^\ell}{\varepsilon}\right)^2$$

(Lemma 3 and Markov's inequality)

$$=|\mathcal{L}|\cdot p\cdot 2^\ell\cdot\frac{2^{2\ell}\cdot 4\cdot p^{n-k}\cdot k!}{\varepsilon^2\cdot(p-(n-k+1))\cdots(p-n)}$$

$$\lesssim\frac{4\cdot|\mathcal{L}|\cdot 8^\ell\cdot p^{n-k+1}\cdot k!}{\varepsilon^2\cdot(p-n)^k},$$

which completes the proof.

Next, we state all the claims that are needed for the proof of Lemma 3. Using the Poisson summation formula (Lemma 1), the variable $\mathbf{Y}_{s,A}$ can be rewritten as follow.

Claim 1. $\mathbf{Y}_{s,A}=\sum_{\vec{\alpha}\in C^\perp_{\vec{\mathbf{X}}}\setminus\{\vec{0}\}}\widehat{\mathbb{1}\,A}(\vec{\alpha})\left(1-\omega^{\langle\vec{\alpha},s\cdot\vec{1}\rangle}\right).$

The next claim upper bounds the ℓ_2 norm of the Fourier weights corresponding to an indicator function of an arbitrary subset of F^n. This result follows from Parseval's identity directly.

Claim 2. For any subset $A\subseteq F^n$, it holds that

$$\sum_{\vec{\alpha}\in F^n\setminus\{\vec{0}\}}|\widehat{\mathbb{1}\,A}(\vec{\alpha})|^2\leqslant 1.$$

Finally, the following claim upper bounds the probability of a non-zero vector that is in the dual space $C^\perp_{\vec{\mathbf{X}}}$, where the probability is taken over the randomness of the evaluation places $\vec{\mathbf{X}}$. This result was proven in [25] using a generalization of Bezout's theorem.

Claim 3 (Claim 4 of [25]). For any non-zero vector $\vec{\alpha}\in F^n$, the following bound holds.

$$\Pr_{\vec{\mathbf{X}}}\left[\vec{\alpha}\in C^\perp_{\vec{\mathbf{X}}}\right]\leqslant\frac{k!}{(p-(n-k+1))\cdots(p-n)}$$

Now, we are ready to prove Lemma 3.

Proof (Proof of Lemma 3*).* We have

$$\mathop{\mathrm{E}}_{\vec{\mathbf{X}}}\left[(\mathbf{Y}_{s,A})^2\right]=\mathop{\mathrm{E}}_{\vec{\mathbf{X}}}\left[\left(\sum_{\vec{\alpha}\in C^\perp_{\vec{\mathbf{X}}}\setminus\{\vec{0}\}}\widehat{\mathbb{1}_A}(\vec{\alpha})\left(1-\omega^{\langle\vec{\alpha},s\cdot\vec{1}\rangle}\right)\right)^2\right] \qquad \text{(Claim 1)}$$

$$\leqslant \mathop{\mathrm{E}}_{\vec{\mathbf{X}}}\left[\left(\sum_{\vec{\alpha}\in C_{\vec{\mathbf{X}}}^{\perp}\setminus\{\vec{0}\}} |1-\omega^{\langle\vec{\alpha},s\cdot\vec{1}\rangle}|^2\right)\cdot\left(\sum_{\vec{\alpha}\in C_{\vec{\mathbf{X}}}^{\perp}\setminus\{\vec{0}\}} |\widehat{\mathbb{1}_A}(\vec{\alpha})|^2\right)\right]$$

(Cauchy-Schwarz)

$$\leqslant \mathop{\mathrm{E}}_{\vec{\mathbf{X}}}\left[\left(\sum_{\vec{\alpha}\in C_{\vec{\mathbf{X}}}^{\perp}\setminus\{\vec{0}\}} 4\right)\cdot\left(\sum_{\vec{\alpha}\in C_{\vec{\mathbf{X}}}^{\perp}\setminus\{\vec{0}\}} |\widehat{\mathbb{1}_A}(\vec{\alpha})|^2\right)\right]$$

(Triangle inequality)

$$\leqslant 4\cdot p^{n-k+1}\cdot \mathop{\mathrm{E}}_{\vec{\mathbf{X}}}\left[\sum_{\vec{\alpha}\in C_{\vec{\mathbf{X}}}^{\perp}\setminus\{\vec{0}\}} |\widehat{\mathbb{1}_A}(\vec{\alpha})|^2\right]$$

$$= 4\cdot p^{n-k}\cdot \sum_{\vec{\alpha}\in F^n\setminus\{\vec{0}\}} |\widehat{\mathbb{1}_A}(\vec{\alpha})|^2\cdot \Pr_{\vec{\mathbf{X}}}\left[\vec{\alpha}\in C_{\vec{\mathbf{X}}}^{\perp}\right]$$

(Linearity of expectation)

$$\leqslant 4\cdot p^{n-k}\cdot \sum_{\vec{\alpha}\in F^n\setminus\{\vec{0}\}} |\widehat{\mathbb{1}_A}(\vec{\alpha})|^2\cdot \frac{k!}{(p-(n-k+1))\cdots(p-n)}$$

(Claim 3)

$$\leqslant \frac{4\cdot p^{n-k}\cdot k!}{(p-(n-k+1))\cdots(p-n)}$$

(Claim 2)

$$\lesssim \frac{4\cdot p^{n-k}\cdot k!}{(p-n)^k}.$$

This completes the proof.

6 Leakage-resilience of Partially Random Code

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.*

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

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 [29].). *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 $\vec{\boldsymbol{\alpha}}^{(1)}, \vec{\boldsymbol{\alpha}}^{(2)}, \ldots, \vec{\boldsymbol{\alpha}}^{(m)}$ 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 $\lceil \frac{n-k}{k} \rceil \cdot k \approx (n-k)$ random elements from F to sample $\mathbf{W}$.

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 Fig. 1) sampled as follows.*

1. *Entries of $\vec{\mathbf{v}}_{\{k+1,\ldots,n\}}$ 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 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 4 (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 4 is identical to the previous section. Hence, we omit it. Before we present the proof of Lemma 4, 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.*

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

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 4 in the exactly manner as in the previous section. That is,

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

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 4 and, in turn, the proof of Theorem 6.

References

1. Adams, D. Q., et al.: Lower bounds for leakage-resilient secret sharing schemes against probing attacks. In: IEEE International Symposium on Information Theory ISIT 2021 (2021)
2. Aggarwal, D., et al.: Stronger leakage-resilient and non-malleable secret sharing schemes for general access structures. In: Boldyreva, A., Micciancio, D. (eds.) CRYPTO 2019. LNCS, vol. 11693, pp. 510–539. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-26951-7_18
3. Arora, S., Barak, B.: Computational Complexity: A Modern Approach. Cambridge University Press, Cambridge (2009)
4. Badrinarayanan, S., Srinivasan, A.: Revisiting non-malleable secret sharing. In: Ishai, Y., Rijmen, V. (eds.) EUROCRYPT 2019. LNCS, vol. 11476, pp. 593–622. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-17653-2_20
5. Benhamouda, F., Degwekar, A., Ishai, Y., Rabin, T.: On the local leakage resilience of linear secret sharing schemes. In: Shacham, H., Boldyreva, A. (eds.) CRYPTO 2018. LNCS, vol. 10991, pp. 531–561. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-96884-1_18
6. Benhamouda, F., Degwekar, A., Ishai, Y., Rabin, T.: On the local leakage resilience of linear secret sharing schemes. J. Cryptol. **34**(2), 1–65 (2021). https://doi.org/10.1007/s00145-021-09375-2
7. Block, A.R., Maji, H.K., Nguyen, H.H.: Secure computation based on leaky correlations: high resilience setting. In: Katz, J., Shacham, H. (eds.) CRYPTO 2017. LNCS, vol. 10402, pp. 3–32. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-63715-0_1
8. Block, A.R., Maji, H.K., Nguyen, H.H.: Secure computation with constant communication overhead using multiplication embeddings. In: Chakraborty, D., Iwata, T. (eds.) INDOCRYPT 2018. LNCS, vol. 11356, pp. 375–398. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-05378-9_20
9. Bogdanov, A., Ishai, Y., Srinivasan, A.: Unconditionally secure computation against low-complexity leakage. In: Boldyreva, A., Micciancio, D. (eds.) CRYPTO 2019. LNCS, vol. 11693, pp. 387–416. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-26951-7_14
10. Cascudo, I., Cramer, R., Xing, C., Yuan, C.: Amortized complexity of information-theoretically secure MPC revisited. In: Shacham, H., Boldyreva, A. (eds.) CRYPTO 2018. LNCS, vol. 10993, pp. 395–426. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-96878-0_14

11. Chattopadhyay, E., et al.: Extractors and secret sharing against bounded collusion protocols. In: 61st Annual Symposium on Foundations of Computer Science, Durham, NC, USA, 16–19 November 2020, pp. 1226–1242. IEEE (2020). https://doi.org/10.1109/FOCS46700.2020.00117
12. Cramer, R.: The arithmetic codex: theory and applications. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 1–1. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-20465-4_1
13. Garcia, A., Stichtenoth, H.: A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound. Inventiones Math. **121**(1), 211–222 (1995)
14. Goldreich, O., Micali, S., Wigderson, A.: How to play any mental game or A completeness theorem for protocols with honest majority. In: Alfred A., ed., 19th Annual ACM Symposium on Theory of Computing, New York City, NY, USA, 25–27 May 1987, pp. 218–229. ACM Press (1987). https://doi.org/10.1145/28395.28420
15. Goppa, V.D.: A new class of linear correcting codes. Problemy Peredachi Informatsii **6**(3), 24–30 (1970)
16. Goyal, V., Kumar, A.: Non-malleable secret sharing. In: Diakonikolas, I., Kempe, D., Henzinger, M., (eds.), 50th Annual ACM Symposium on Theory of Computing, Los Angeles, CA, USA, 25–29 June 2018, pp. 685–698. ACM Press (2018). https://doi.org/10.1145/3188745.3188872
17. Guruswami, V., Wootters, M.: Repairing reed-solomon codes. In: Wichs, D., Mansour, Y., (eds.), 48th Annual ACM Symposium on Theory of Computing, Cambridge, MA, USA, 18–21 June 2016, pp. 216–226. ACM Press (2018). https://doi.org/10.1145/2897518.2897525
18. Guruswami, V., Wootters, M.: Repairing reed-solomon codes. IEEE Trans. Inf. Theory **63**(9), 5684–5698 (2017). https://doi.org/10.1109/TIT.2017.2702660
19. Kalai, Y.T., Reyzin, L.: A survey of leakage-resilient cryptography. Cryptology ePrint Archive, Report 2019/302 (2019). https://eprint.iacr.org/2019/302
20. Kocher, P.C.: Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In: Koblitz, N. (ed.) CRYPTO 1996. LNCS, vol. 1109, pp. 104–113. Springer, Heidelberg (1996). https://doi.org/10.1007/3-540-68697-5_9
21. Kocher, P., Jaffe, J., Jun, B.: Differential power analysis. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 388–397. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-48405-1_25
22. Kumar, A., Meka, R., Sahai, A.: Leakage-resilient secret sharing against colluding parties. In: Zuckerman, D., ed., 60th Annual Symposium on Foundations of Computer Science, Baltimore, MD, USA, 9–12 November 2019, pp. 636–660. IEEE Computer Society Press (2019). https://doi.org/10.1109/FOCS.2019.00045
23. Lin, F., Cheraghchi, M., Guruswami, V., Safavi-Naini, R., Wang, H.: Leakage-resilient secret sharing in non-compartmentalized models. In: Kalai, Y.T., Smith, A.D., Wichs, D., (eds.), ITC 2020: 1st Conference on Information-Theoretic Cryptography, Boston, MA, USA, 17–19 June 2020, pp. 7:1–7:24. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik. https://doi.org/10.4230/LIPIcs.ITC.2020.7
24. Florence Jessie MacWilliams and Neil James Alexander Sloane: The Theory of Error Correcting Codes, vol. 16. Elsevier, Amsterdam (1977)
25. Maji, H.K., Nguyen, H.H., Paskin-Cherniavsky, A., Suad, T., Wang, M.: Leakage-resilience of the Shamir secret-sharing scheme against physical-bit leakages. In: Canteaut, A., Standaert, F.-X. (eds.) EUROCRYPT 2021. LNCS, vol. 12697, pp. 344–374. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-77886-6_12

26. Maji, H.K., et al.: Tight estimate of the local leakage resilience of the additive secret-sharing scheme & its consequences. In: Dachman-Soled, D., ed., 3rd Conference on Information-Theoretic Cryptography, ITC 2022, 5–7 July 2022, Cambridge, MA, USA, volume 230 of LIPIcs, pp. 16:1–16:19. Schloss Dagstuhl - Leibniz-Zentrum für Informatik (2022). https://doi.org/10.4230/LIPIcs.ITC.2022.16
27. Maji, H.K., Nguyen, H.H., Paskin-Cherniavsky, A., Wang, M.: Improved bound on the local leakage-resilience of Shamir's secret sharing. In IEEE International Symposium on Information Theory, ISIT 2022, Espoo, Finland, 26 June–1 July 2022, pp. 2678–2683. IEEE (2022). https://doi.org/10.1109/ISIT50566.2022.9834695
28. Maji, H.K., Paskin-Cherniavsky, A., Suad, T., Wang, M.: Constructing locally leakage-resilient linear secret-sharing schemes. In: Malkin, T., Peikert, C. (eds.) CRYPTO 2021. LNCS, vol. 12827, pp. 779–808. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-84252-9_26
29. Massey, J.L.: Threshold decoding (1963)
30. Massey, J.L.: Some applications of coding theory in cryptography. Mat. Contemp. **21**(16), 187–209 (2001)
31. Nielsen, J.B., Simkin, M.: Lower bounds for leakage-resilient secret sharing. In: Canteaut, A., Ishai, Y. (eds.) EUROCRYPT 2020. LNCS, vol. 12105, pp. 556–577. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-45721-1_20
32. Pietrzak, K.: Cryptography from learning parity with noise. In: Bieliková, M., Friedrich, G., Gottlob, G., Katzenbeisser, S., Turán, G. (eds.) SOFSEM 2012. LNCS, vol. 7147, pp. 99–114. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-27660-6_9
33. Regev, O.: The learning with errors problem. Invited Surv. CCC **7**(30), 11 (2010)
34. Shamir, A.: How to share a secret. Commun. Assoc. Comput. Mach. **22**(11), 612–613 (1979)
35. Srinivasan, A., Vasudevan, P.N.: Leakage resilient secret sharing and applications. In: Boldyreva, A., Micciancio, D. (eds.) CRYPTO 2019. LNCS, vol. 11693, pp. 480–509. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-26951-7_17