Improved Bound on the Local Leakage-resilience of Shamir's Secret Sharing

Hemanta K. Maji Hai H. Nguyen Anat Paskin-Cherniavsky
Mingyuan Wang

Abstract

Side-channel attacks have repeatedly falsified the assumption that cryptosystems are black boxes. Leakage-resilient cryptography studies the robustness of cryptographic constructions when an unforeseen revelation of information occurs. In this context, recently, Benhamouda, Degwekar, Ishai, and Rabin (CRYPTO–2018) motivated the study of the local leakage resilience of secret-sharing schemes against an adversary who obtains independent leakage from each secret share.

Motivated by applications in secure computation, Benhamouda et al. (CRYPTO–2018) initiated the study of the local leakage resilience of Shamir's secret-sharing scheme, an essential primitive for nearly all threshold cryptography. The objective is to achieve local leakage resilience with as small a fractional reconstruction threshold as possible. Previously, Benhamouda et al. showed that the reconstruction threshold k being at least 0.907 times the number of parties n is sufficient for Shamir's secret-sharing scheme to be resilient against arbitrary single-bit local leakage from each secret share. After that, Maji et al. (CRYPTO–2021) and Benhamouda et al. (Journal of Cryptology–2021) independently lowered this threshold to $k/n \geqslant 0.8675$ and $k/n \geqslant 0.85$, respectively.

This paper contributes to this line of research and proves that $k/n \geqslant 0.78$ is sufficient. Next, motivated by applications in GMW-style leakage-resilient secure computation, our work extends this bound to a more general adversary who corrupts some parties (obtaining their entire secret shares) and obtains leakage from the remaining honest parties' secret shares.

Our technical analysis proceeds by Fourier analysis and accurately estimates an exponential sum arising in this analysis.

1 Introduction

Starting with the works of Koch et al. [Koc96, KJJ99], innovative and sophisticated side-channel attacks have repeatedly falsified the assumption that cryptosystems are impervious black-boxes. Leakage-resilient cryptography formalizes and provides provable security guarantees against such information leakages, including unforeseen ones. Substantial research has examined the feasibility and efficiency of leakage-resilient cryptography against diverse models of potential leakages during the last few decades (refer to the excellent survey [KR19]).

In this context, recently, Benhamouda, Degwekar, Ishai, and Rabin [BDIR18] motivated the study of the *local leakage resilience of secret-sharing schemes* against an adversary who obtains independent leakage from each secret share (this primitive was also implicitly defined in [GK18]). A locally leakage-resilient secret-sharing scheme ensures that the leakage's joint distribution is statistically independent of the secret. Intriguingly, this concept is closely related to the fascinating problem of repairing codes; c.f., for example, Guruswami and Wootter's reconstruction algorithm [GW16, GW17] and subsequent works [TYB17, GR17, DDKM18, MBW19]. The adversary does not need to reconstruct the entire secret to preclude leakage-resilience; obtaining any partial information to distinguish two secrets suffices. For example, over characteristic-two fields, an appropriate one-bit leakage from each share of a linear secret-sharing scheme, determines the least significant bit of the secret. The construction of leakage-resilient secret-sharing schemes [ADN$^+$19, SV19, BS19, KMS19, BIS19, FY19, FY20, CGG$^+$20, MSV20] and the characterization of leakage-resilience of prevalent secret-sharing schemes [HIMV19, CGN19, LCG$^+$20, MNP$^+$21, AMN$^+$21] has been fairly challenging.

Secret-sharing schemes are typical in GMW-style [GMW87] secure multi-party computation protocols. Motivated by this application, Benhamouda et al. [BDIR18] initiated the study of the local leakage-resilience of Shamir's secret-sharing scheme, an essential primitive for nearly all threshold cryptography. The goal is to achieve local leakage resilience with the minimum ratio k/n, where n is the number of parties and k is the reconstruction threshold. Reducing this fractional reconstruction threshold k/n entails that a smaller fraction of honest parties can ensure the security of the GMW-style MPC protocol. Benhamouda et al. [BDIR18] proved that Shamir's secret-sharing scheme over prime fields is locally leakage-resilient against arbitrary one-bit leakage from each secret share when $k/n \geqslant 0.907$. After that, Maji et al. [MPSW21] and Benhamouda et al. [BDIR21] independently improved this lower bound to $k/n \geqslant 0.8675$ and $k/n \geqslant 0.85$, respectively.

Summary of our results. This work contributes to this research and proves that Shamir's secret-sharing scheme is one-bit locally leakage-resilient if $k/n \geqslant 0.78$. More generally, in secure multi-party computation, an *insider* attacker can corrupt a subset of parties and obtain their secret shares. In this scenario, the secret-sharing scheme must remain secure even against these stronger adversaries who obtain the secret shares of the corrupted parties and leakage from the honest parties' secret shares. Motivated by this application, our work extends the leakage-resilience bound for Shamir's secret-sharing scheme to these more general adversaries. Our technical analysis proceeds by Fourier analysis over a prime field and accurately estimates an exponential sum arising in this analysis.

1.1 Our Contribution

This section, first, introduces some notations to facilitate a high-level presentation of our results (refer to Section 2 for details). Let F represent an arbitrary finite field and F_p represent the prime field of order p. Fix an n-party secret-sharing scheme for arbitrary secrets in F and each party gets a secret share in F. An (n, m) *local leakage function* $\vec{\tau} = (\tau_1, \tau_2, \ldots, \tau_n)$ is a collection of m-bit leakage functions $\tau_i \colon F \to \{0,1\}^m$, for $i \in \{1, \ldots, n\}$. Let $\vec{\tau}(s)$ be the joint distribution of (the output of) the (n, m) leakage function $\vec{\tau}$ over the sample space $(\{0,1\}^m)^n$ defined by the experiment: (i) sample random secret shares $(h_1, h_2, \ldots, h_n) \in F^n$ for the secret $s \in F$ and (ii) output the leakage $(\tau_1(h_1), \tau_2(h_2), \ldots, \tau_n(h_n)) \in (\{0,1\}^m)^n$. A secret-sharing scheme is (m, ε)-*locally leakage resilient* if for any m-bit leakage function $\vec{\tau} = (\tau_1, \tau_2, \ldots, \tau_n)$, and for any pair of secrets $s_0, s_1 \in F$, the statistical distance between the joint leakage distributions $\vec{\tau}(s_0)$ and $\vec{\tau}(s_1)$ is at most ε.

Leakage resilience of Shamir's secret-sharing. Our work considers Shamir secret-sharing schemes involving n parties with a reconstruction threshold k over F_p, denoted as $\mathsf{ShamirSS}(n, k)$. Our first result shows that $\mathsf{ShamirSS}(n, k)$ is leakage-resilient if $k \geqslant 0.78n$ against *eavesdropping* attackers who obtain local leakage from all secret shares.

Theorem 1. *Let $\kappa > (2\log_2 \pi - 1)/(3\log_2 \pi - 2) =: c$. For any $n, k \in \mathbb{N}$ and prime $p \geqslant p_0(\kappa)$ satisfying $1 \geqslant k/n \geqslant \kappa$, $\mathsf{ShamirSS}(n, k)$ over F_p is $(1, \varepsilon)$-locally leakage resilient, where $\varepsilon = 2^{-(3\log_2 \pi - 2)(\kappa - c)\cdot n}$.*

For example, in the theorem above, $\kappa = 0.78$ suffices.

Extension to insider attacks. Consider a more general adversary who corrupts θ parties indexed by the size-θ subset $\Theta \subseteq \{1, \ldots, n\}$. The adversary obtains their entire secret shares, and gets m-bit leakage from the secret share of each uncorrupted party. To study this leakage model, consider a leakage function $\vec{\tau} = (\tau_1, \tau_2, \ldots, \tau_n)$, parameterized by a size-θ subset $\Theta \subseteq \{1, \ldots, n\}$ of corrupted parties. The functions satisfy $\tau_i(x) = x$ (for $i \in \Theta$) and $\tau_j \colon F \to \{0,1\}^m$ (for $j \in \{1, \ldots, n\} \setminus \Theta$). A secret-sharing scheme is (θ, m, ε)-*locally leakage resilient* if the statistical distance between the joint leakage distributions $\vec{\tau}(s_0)$ and $\vec{\tau}(s_1)$ is at most ε for any two secrets $s_0, s_1 \in F$ and leakage function $\vec{\tau}$ corresponding to any size-θ subset Θ. In particular, the leakage model of Theorem 1 corresponds to the case $\theta = 0$.

Theorem 2. *Let $\kappa > (2\log_2 \pi - 1)/(3\log_2 \pi - 2) =: c$. For any $n, k, \theta \in \mathbb{N}$ and prime $p \geqslant p_0(\kappa)$ satisfying $1 \geqslant (k-\theta)/(n-\theta) \geqslant \kappa$, $\mathsf{ShamirSS}(n,k)$ over F_p is $(\theta, 1, \varepsilon)$-locally leakage resilient, where $\varepsilon = 2^{-(3\log_2 \pi - 2)(\kappa - c)(n-\theta)}$.*

Despite the possibility that the insider attacker on $\mathsf{ShamirSS}(n,k)$ may be more potent than the eavesdropping attacker on $\mathsf{ShamirSS}(n-\theta, k-\theta)$, our proof bounds both distinguishing advantages by an identical quantity.

Remark. Theorem 1 and Theorem 2 extend to the *Massey secret-sharing scheme* [Mas01] corresponding to any *maximum distance separable* [MS77] linear codes over prime fields. For clarity of presentation, this draft interprets the consequences of our technical result using applications to Shamir's secret-sharing scheme.

Leakage resilience of maximum distance separable (MDS) codes. For a distribution X over the sample space F_p^n and a leakage function $\vec{\tau}$, the joint distribution $\vec{\tau}(X)$ is defined by the experiment: (i) sample $\vec{x}$ from X and (ii) output the leakage $(\tau_1(x_1), \tau_2(x_2), \ldots, \tau_n(x_n))$. For any code $C \subseteq F_p^n$, we overload our notation and use C to represent the uniform distribution over the code C. The following technical result leads to Theorem 1 and Theorem 2.

Theorem 3. *Let C be an $[n,k]_{F_p}$ MDS code. Let $\vec{\tau} = (\tau_1, \tau_2, \ldots, \tau_n)$ be a local leakage function, where $\tau_i \colon F_p \to \{0,1\}$. Then, the following bound holds.*

$$\mathsf{SD}\left(\vec{\tau}(C)\ ,\ \vec{\tau}(F_p^n)\right) \leqslant \left(2 - \frac{1}{p^2}\right)^{n-k} \left(\frac{2}{p\sin(\pi/p)}\right)^{3k-2n+1}.$$

This upper-bound expression yields meaningful bounds even for specific values of p. For example, (assuming $n = p-1$) (1) for $\kappa = 0.99$, any prime $p \geqslant 5$ is sufficient, (2) for $\kappa = 0.85$, any $p \geqslant 13$ suffices, and (3) for $\kappa = 0.78$, any $p \geqslant 1531$ works (refer to www.desmos.com/calculator/buatuebkvb for the plot).

1.2 Technical Overview

This section presents a high-level overview of our technical approach. We refer the readers to [Rao07] for Fourier basics. Fix an arbitrary $[n,k]_F$ MDS code C. Fix the local leakage function $\vec{\tau} = (\tau_1, \tau_2, \ldots, \tau_n)$ that leaks 1-bit from every secret share. Let $\mathbb{1}_{i,\ell_i}$ be the indicator function of the set $\{x \colon \tau_i(x) = \ell_i\} \subseteq F$. Choose arbitrary secrets $s_0, s_1 \in F$. As established in [BDIR18, MNP$^+$21, MPSW21], the statistical distances $\mathsf{SD}\left(\vec{\tau}(C)\ ,\ \vec{\tau}(F_p^n)\right)$ (and, furthermore, $\mathsf{SD}\left(\vec{\tau}(s_0)\ ,\ \vec{\tau}(s_1)\right)$) are upper-bounded by the following Fourier-analytic proxy.

$$\sum_{\vec{\ell} \in \{0,1\}^n} \sum_{\vec{\alpha} \in C^\perp \setminus \{\vec{0}\}} \prod_{i=1}^{n} \left| \widehat{\mathbb{1}_{i,\ell_i}}(\alpha_i) \right|. \tag{1}$$

Next, we utilize the Fourier properties of 1-bit leakage function (see Claim 3) to rewrite the proxy as follows.

$$\sum_{\vec{\ell} \in \{0,1\}^n} \sum_{\vec{\alpha} \in C^\perp \setminus \{\vec{0}\}} \prod_{i=1}^{n} \left| \widehat{\mathbb{1}_{i,\ell_i}}(\alpha_i) \right| = \sum_{\vec{\alpha} \in C^\perp \setminus \{\vec{0}\}} \prod_{i=1}^{n} b_{i,\alpha_i}, \tag{2}$$

where $b_{i,\alpha_i} := 1$ if $\alpha_i = 0$, and $b_{i,\alpha_i} := 2 \cdot \left|\widehat{\mathbb{1}_{i,0}}(\alpha_i)\right|$, otherwise (Lemma 2). This rearrangement of terms removes (i) the summation over all possible leakage values $\vec{\ell} \in \{0,1\}^n$, and (ii) the necessity to bound the Fourier coefficients of the functions $\mathbb{1}_{i,\ell_i}$ at 0. This step is key to precisely estimating this exponential sum. To obtain the above equation, we partition the set of codewords in $C^\perp \setminus \{\vec{0}\}$ into sets A_I that contains codewords in $C^\perp \setminus \{\vec{0}\}$ whose indices of non-zero coordinates are exactly in I, and then extensively apply the Fourier properties (see Claim 3) of one-bit leakage functions.

After that, we use a similar idea as in [BDIR18]. That is, we partition the set $\{1,\dots,n\}$ into three sets I_1, I_2, J, where I_1 and I_2 are information sets of the dual code $C^\perp$. For brevity, let $D' = C^\perp \setminus \{\vec{0}\}$. Then, applying the Cauchy-Schwartz inequality yields

$$\sum_{\vec{\alpha}\in D'} \prod_{i=1}^{n} b_{i,\alpha_i} \leqslant \sqrt{\sum_{\vec{\alpha}\in D'} \prod_{i\in I_1} b_{i,\alpha_i}^2} \cdot \sqrt{\sum_{\vec{\alpha}\in D'} \prod_{i\in I_2} b_{i,\alpha_i}^2} \cdot \max_{\vec{\alpha}\in D'} \prod_{i\in J} b_{i,\alpha_i}$$

Finally, we bound individual terms on the right-hand side separately using Fourier properties of leakage functions and properties of the MDS code $C^\perp$. We bound the first two terms (Claim 1) using (1) I_1 and I_2 are information sets, and (2) the L_2 norm of the Fourier coefficients of the leakage function are bounded using Parseval's identity. The upper bound on the final term follows from the upper bound of $2/\pi$ on the non-zero Fourier coefficients b_{i,α_i} (see Imported Lemma 2).

2 Preliminaries

Notation. For any two distribution A and B over the same finite sample space, the *statistical distance* between the two distributions, denoted as $\mathsf{SD}\left(A\ ,\ B\right)$, is defined as $\frac{1}{2}\sum_x |\Pr[A = x] - \Pr[B = x]|$. We denote $[n] := \{1, 2, \dots, n\}$. For any vector $\vec{v}$ and $I \subseteq [n]$, the vector $\vec{v}_I$ represents the vector $(v_i \colon i \in I)$. 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.

2.1 Codes and Secret-sharing Schemes

We use the following notations for error-correcting codes as consistent with [MS77].

Linear Codes. A *linear code* C over a finite field F of *length* n and *rank* k is a k-dimension vector subspace of F^n, referred to as an $[n,k]_F$-code. 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 $(n-k+1)$.

Fact 1. *The dual code $C^\perp$ of an $[n,k]_F$ MDS code C is itself an $[n,n-k]_F$ MDS code.*

Generalized Reed-Solomon Codes. A *generalized Reed-Solomon code* over prime field F with message length k and block length n consists of an encoding function $\mathsf{Enc}\colon F^k \to F^n$ and decoding function $\mathsf{Dec}\colon F^n \to F^k$. It is specified by the distinct evaluation places $\vec{\alpha} = (\alpha_1,\dots,\alpha_n)$, and a *scaling vector* $\vec{\beta} = (\beta_1,\dots,\beta_n) \in (F^*)^n$. Given $\vec{\alpha}$ and $\vec{\beta}$, the *encoding function* is

$$\mathsf{Enc}(m_1,\dots,m_k) := \left(\beta_1 \cdot f(\alpha_1), \dots, \beta_n \cdot f(\alpha_n)\right),$$

where $f(X) := m_1 + m_2 X + \cdots + m_k X^{k-1}$.

Fact 2. *Generalized Reed-Solomon codes are MDS.*

Threshold Secret Sharing Scheme For any two positive integers $k < n$, an $(n, k)_F$-secret-sharing scheme over a finite field F consists of two functions Share and Rec. Share is a randomized function that takes a secret $s \in F$ and outputs $\mathsf{Share}(s) = (\mathsf{Share}(s)_1, \ldots, \mathsf{Share}(s)_n) \in F^n$. The pair of functions $(\mathsf{Share}, \mathsf{Rec})$ satisfies the following requirements.

- **Correctness.** For any secret $s \in F$ and a set of parties $\{i_1, i_2, \ldots, i_t\} \subseteq \{1, 2, \ldots, n\}$ such that $t \geqslant k$, we have
$$\Pr[\mathsf{Rec}(\mathsf{Share}(s)_{i_1}, \ldots, \mathsf{Share}(s)_{i_t}) = s] = 1.$$

- **Privacy.** For any two secret $s_0, s_1 \in F$ and a set of parties $\{i_1, i_2, \ldots, i_t\} \subseteq \{1, 2, \ldots, n\}$ such that $t < k$, we have
$$\mathsf{SD}\left(\left(\mathsf{Share}(s_0)_{i_1}, \ldots, \mathsf{Share}(s_0)_{i_t}\right)\ ,\ \left(\mathsf{Share}(s_1)_{i_1}, \ldots, \mathsf{Share}(s_1)_{i_t}\right)\right) = 0.$$

Shamir's Secret-sharing. Let F be a prime field. For any positive integer $k \leqslant n$ and *evaluation places* $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n)$ the following conditions are satisfied. (1) For all $1 \leqslant i \leqslant n$, $\alpha_i \in F^*$, and (2) for all $1 \leqslant i < j \leqslant n$, $\alpha_i \neq \alpha_j$. The corresponding Shamir's secret sharing, represented as $\mathsf{ShamirSS}(n, k)$, is defined as follows.

- Given secret $s \in F$, $\mathsf{Share}(s)$ picks a random polynomial $f[X] \in F(X)/X^k$ conditioned on $f(0) = s$. For every $1 \leqslant i \leqslant n$, the i^{th} share of $\mathsf{Share}(s)$ is $f(\alpha_i)$.
- Given shares $(\mathsf{Share}(s)_{i_1}, \ldots, \mathsf{Share}(s)_{i_t})$, Rec interpolates to obtain the unique polynomial $f \in F[X]/X^k$ such that $f(\alpha_{i_j}) = \mathsf{Share}(s)_{i_j}$ for all $1 \leqslant j \leqslant t$, and outputs $f(0)$ to be the reconstructred secret.

Fact 3. *The set of all possible secret shares of secret $s = 0$ of an $[n, k]_F$ Shamir's secret-sharing is an $[n, k-1]_F$ generalized Reed-Solomon code.*

2.2 Local Leakage-resilient Secret Sharing Schemes

Local Leakage. Fix a finite field F and an n-party secret-sharing scheme for secrets $s \in F$ in which each party gets a secret share in F. An (n, m) *local leakage function* $\vec{\tau} = (\tau_1, \tau_2, \ldots, \tau_n)$ is a collection of m-bit leakage functions $\tau_i \colon F \to \{0,1\}^m$ for $i \in [n]$. Let $\vec{\tau}(s)$ be the joint distribution of the (n, m) leakage function $\vec{\tau}$ over the sample space $(\{0,1\}^m)^n$ defined by the experiment (i) sample secret shares $(h_1, h_2, \ldots, h_n)$ for the secret s (ii) output $(\tau_1(h_1), \tau_2(h_2), \ldots, \tau_n(h_n))$.

Definition 1. *A secret sharing scheme for n parties is a (m, ε)-local leakage-resilient, if, for any two secrets $s_0, s_1 \in F$, and any local leakage function $\vec{\tau}$ that leaks m bits from every share locally, it holds that*
$$\mathsf{SD}\left(\vec{\tau}(s_0)\ ,\ \vec{\tau}(s_1)\right) \leqslant \varepsilon.$$

2.3 Fourier Analysis Basics

We use discrete Fourier analysis on prime field F of order p. Define $\omega := \exp(2\pi\imath/p)$. For any functions $f, g \colon F \to \mathbb{C}$, define their inner-product
$$\langle f, g\rangle := \frac{1}{p}\sum_{x \in F} f(x) \cdot \overline{g(x)},$$
where $\overline{z}$ is the complex conjugate of $z \in \mathbb{C}$. For $z \in \mathbb{C}$, $|z| := \sqrt{z\overline{z}}$. For any $\alpha \in F$, define the function $\widehat{f} \colon F \to \mathbb{C}$ as follows.
$$\widehat{f}(\alpha) := \frac{1}{p}\sum_{x \in F} f(x) \cdot \omega^{-\alpha x}.$$

The Fourier transform maps the function f to the function $\widehat{f}$. This transformation is a full-rank linear mapping, i.e., only the zero function has zero Fourier. In particular, it satisfies the following identities.

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

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

For more details on Fourier basics, see [Rao07].

3 Technical Proofs

This section proves Theorem 1 and Theorem 2 from Theorem 3, and then proves Theorem 3.

3.1 Proofs of Theorem 1 and Theorem 2

Observe that Theorem 1 follows from Theorem 2 by fixing $\theta = 0$. Therefore, it suffices to prove Theorem 2. First, we prove the following lemma that is needed for the proof.

Lemma 1. *Let $\vec{\tau} = (\tau_1, \tau_2, \dots, \tau_n)$ be a leakage function such that $\tau_i(x) = x$ for every $x \in F$ and $i \in \Theta$, and $\tau_i \colon F \to \{0,1\}$ for every $i \in [n] \setminus \Theta$. Define $\mathbb{1}_{i,\ell_i}(x) = 1$ if $\tau_i(x) = \ell_i$ and $\mathbb{1}_{i,\ell_i}(x) = 0$ otherwise. Let $C \subseteq F^n$ be the set of all the possible secret shares of the secret zero. Then, for any secrets $s_0, s_1 \in F$, the following bound holds.*

$$\mathsf{SD}\left(\vec{\tau}(s_0)\ ,\ \vec{\tau}(s_1)\right) \leqslant \sum_{\vec{\ell} \in \{0,1\}^{n-\theta}} \ \sum_{\vec{\alpha} \in D^\perp \setminus \{\vec{0}\}} \ \prod_{i \notin \Theta} \left|\widehat{\mathbb{1}_{i,\ell_i}}(\alpha_i)\right|,$$

where $D^\perp$ is the code obtained from puncturing all coordinates in Θ of every codeword in $C^\perp$.

Intuitively, the statistical distance is bounded by the Fourier analytic proxy of the $\mathsf{ShamirSS}(n-\theta, k-\theta)$. We remark that D is a (punctured) generalized Reed-Solomon code. Observe that a punctured MDS code is MDS as well.

Proof of Lemma 1. Observe that $\mathbb{1}_{i,\ell_i}(x) = 1$ if and only if $x = \ell_i$, for leakage value ℓ_i and $i \in \Theta$. Therefore, the magnitude of every Fourier coefficients of the function $\mathbb{1}_{i,\ell_i}$ is constant. That is, $\left|\widehat{\mathbb{1}_{i,\ell_i}}(\alpha)\right| = 1/p$ for every $i \in \Theta$, $\ell_i \in F$, $\alpha \in F$. For brevity, let $\Omega = [n] \setminus \Theta$. Note that

$\vec{\ell} = (\ell_1, \ell_2, \ldots, \ell_n)$, where $\ell_i \in F$ for every $i \in \Theta$ and $\ell_j \in \{0,1\}$ for every $i \in \Omega$. Thus, we have

$$\begin{aligned}
&\mathsf{SD}\left(\vec{\tau}(s_0)\ ,\ \vec{\tau}(s_1)\right) \\
&\leqslant \sum_{\vec{\ell}} \sum_{\vec{\alpha}\in C^{\perp}\setminus\{\vec{0}\}} \prod_{i=1}^{n} \left|\widehat{\mathbb{1}_{i,\ell_i}}(\alpha_i)\right| && \text{(Fourier-analytic proxy)} \\
&= \sum_{\vec{\ell}_\Omega\in\{0,1\}^{n-\theta}} \sum_{\vec{\alpha}\in C^{\perp}\setminus\{\vec{0}\}} \sum_{\vec{\ell}_\Theta\in|F|^{\theta}} \prod_{i=1}^{n} \left|\widehat{\mathbb{1}_{i,\ell_i}}(\alpha_i)\right| \\
&= \sum_{\vec{\ell}_\Omega\in\{0,1\}^{n-\theta}} \sum_{\vec{\alpha}\in C^{\perp}\setminus\{\vec{0}\}} \prod_{i\in\Omega} \left|\widehat{\mathbb{1}_{i,\ell_i}}(\alpha_i)\right| \sum_{\vec{\ell}_\Theta\in|F|^{\theta}} \frac{1}{p^{\theta}} \\
&= \sum_{\vec{\ell}_\Omega\in\{0,1\}^{n-\theta}} \sum_{\vec{\alpha}\in C^{\perp}\setminus\{\vec{0}\}} \sum_{\vec{\ell}_\Theta\in|F|^{\theta}} \frac{1}{p^{\theta}} \prod_{i\in\Omega} \left|\widehat{\mathbb{1}_{i,\ell_i}}(\alpha_i)\right| \\
&= \sum_{\vec{\ell}_\Omega\in\{0,1\}^{n-\theta}} \sum_{\vec{\alpha}\in C^{\perp}\setminus\{\vec{0}\}} \prod_{i\in\Omega} \left|\widehat{\mathbb{1}_{i,\ell_i}}(\alpha_i)\right| \\
&= \sum_{\vec{\ell}\in\{0,1\}^{n-\theta}} \sum_{\vec{\alpha}\in D^{\perp}\setminus\{\vec{0}\}} \prod_{i\notin\Theta} \left|\widehat{\mathbb{1}_{i,\ell_i}}(\alpha_i)\right|,
\end{aligned}$$

which competes the proof. □

Proof of Theorem 2. Consider $\mathsf{ShamirSS}(n,k)$ over F (a prime field of order p). Let $C \subseteq F^n$ be the the set of all possible secret shares of the secret 0 of the $[n,k]_F$ Shamir's secret sharing. Let $C \subseteq F^n$ be the set of all possible secret shares of the secret $s = 0$ in $\mathsf{ShamirSS}(n,k)$. Note that C is an $[n,k-1]_F$ MDS code and $C^{\perp}$ is an $[n, n-k+1]_F$ MDS code. Let Θ be an arbitrary size-θ subset of $\{1,2,\ldots,n\}$. Let $D^{\perp}$ be the code obtained from puncturing all coordinates in Θ of every codeword in $C^{\perp}$. Observe that $D^{\perp}$ is an $[n-\theta, n-(k-\theta)+1]_F$ MDS code, and D is an $[n-\theta,(k-\theta)-1]$ MDS code. By Lemma 1, we have

$$\mathsf{SD}\left(\vec{\tau}(s_0)\ ,\ \vec{\tau}(s_1)\right) \leqslant \sum_{\vec{\ell}\in\{0,1\}^{n-\theta}} \sum_{\vec{\alpha}\in D^{\perp}\setminus\{\vec{0}\}} \prod_{i\notin\Theta} \left|\widehat{\mathbb{1}_{i,\ell_i}}(\alpha_i)\right|.$$

Applying Theorem 3 to the MDS code D , the statistical distance is bounded above by

$$\left(2-\frac{1}{p^2}\right)^{(n-\theta)-(k-\theta-1)} \cdot \left(\frac{2}{p\sin(\pi/p)}\right)^{3(k-\theta-1)-2(n-\theta)+1}.$$

Asymptotically, as the prime $p \to \infty$, the right-hand side expression tends (from above) to

$$\begin{aligned}
&2^{(n-\theta)-(k-\theta)} \cdot (2/\pi)^{3(k-\theta)-2(n-\theta)} \\
=&2^{(n-\theta)(2\log_2\pi-1)-(k-\theta)(3\log_2\pi-2)}.
\end{aligned}$$

Therefore, if $(k-\theta)/(n-\theta) > (2\log_2\pi - 1)/(3\log_2\pi - 2) \approx 0.7795$, the $\mathsf{ShamirSS}(n,k)$ is locally leakage-resilient for sufficiently large p. □

3.2 Proof of Theorem 3

This section states the claims needed to prove Theorem 3. We prove these claims in the subsequent subsections.

Imported Lemma 1 ([BDIR18]). *Let C be any $[n,k]_F$ MDS code. Let $\vec{\tau} = (\tau_1, \tau_2, \ldots, \tau_n)$ be any 1-bit leakage functions where $\tau_i \colon F \to \{0,1\}$. Define $\mathbb{1}_{i,\ell_i}(x) = 1$, if $\tau_i(x) = \ell_i$; otherwise, 0. Then, the following bound holds.*

$$2\mathsf{SD}\left(\vec{\tau}(C)\ ,\ \vec{\tau}(F_p^n)\right) \leqslant \sum_{\vec{\ell}\in\{0,1\}^n} \sum_{\vec{\alpha}\in C^\perp\setminus\{\vec{0}\}} \prod_{i=1}^{n} \left|\widehat{\mathbb{1}_{i,\ell_i}}(\alpha_i)\right|.$$

We remark that, for any two secrets $s_0, s_1 \in F$, the quantity $\mathsf{SD}\left(\vec{\tau}(s_0)\ ,\ \vec{\tau}(s_1)\right)$ is also bounded by the Fourier-analytic proxy above. One does not need to apply a triangle inequality, use the bound in the imported lemma, and incur a multiplicative factor-2 loss in the upper bound.

Lemma 2. *Let C be any $[n,k]_F$ MDS code. Let $\vec{\tau} = (\tau_1, \tau_2, \ldots, \tau_n)$ be any 1-bit leakage function where $\tau_i \colon F \to \{0,1\}$. Define $\mathbb{1}_{i,\ell_i}(x) = 1$, if $\tau_i(x) = \ell_i$; otherwise, 0. Then, it holds that*

$$\sum_{\vec{\ell}\in\{0,1\}^n} \sum_{\vec{\alpha}\in C^\perp\setminus\{\vec{0}\}} \prod_{i=1}^{n} \left|\widehat{\mathbb{1}_{i,\ell_i}}(\alpha_i)\right| = \sum_{\vec{\alpha}\in C^\perp\setminus\{\vec{0}\}} \prod_{i=1}^{n} b_{i,\alpha_i},$$

where, for $i \in \{1,\ldots,n\}$ and $\alpha_i \in F$, we have

$$b_{i,\alpha_i} := \begin{cases} 1, & \text{if } \alpha_i = 0, \text{ and} \\ 2\cdot\left|\widehat{\mathbb{1}_{i,0}}(\alpha_i)\right|, & \text{otherwise.} \end{cases}$$

Claim 1. *Let $k, n \in \mathbb{N}$ be such that $k \leqslant n \leqslant 2k$. Let C be any $[n,k]_F$ MDS code. Let $\vec{\tau} = (\tau_1, \tau_2, \ldots, \tau_n)$ be any 1-bit leakage functions where $\tau_i \colon F \to \{0,1\}$. Let I_1, I_2, J be an arbitrary partition of $\{1,2,\ldots,n\}$ such that information sets satisfy $|I_1| = |I_2| = n-k$. Then, it holds that*

$$\sum_{\vec{\alpha}\in C^\perp\setminus\{\vec{0}\}} \prod_{i=1}^{n} b_{i,\alpha_i} \leqslant \left(2 - \frac{1}{p^2}\right)^{n-k} \cdot \max_{\vec{\alpha}\in C^\perp\setminus\{\vec{0}\}} \prod_{i\in J} b_{i,\alpha_i}.$$

Claim 2. *The following bound holds.*

$$\max_{\vec{\alpha}\in C^\perp\setminus\{\vec{0}\}} \prod_{i\in J} b_{i,\alpha_i} \leqslant \left(\frac{2}{p\sin(\pi/p)}\right)^{3k-2n+1}.$$

Proof of Theorem 3. We have

$$\begin{aligned}
&2\mathsf{SD}\left(\vec{\tau}(C)\ ,\ \vec{\tau}(F_p^n)\right) \\
&\leqslant \sum_{\vec{\ell}\in\{0,1\}^n} \sum_{\vec{\alpha}\in C^\perp\setminus\{\vec{0}\}} \prod_{i=1}^{n} \left|\widehat{\mathbb{1}_{i,\ell_i}}(\alpha_i)\right| && \text{(Imported Lemma 1)} \\
&= \sum_{\vec{\alpha}\in C^\perp\setminus\{\vec{0}\}} \prod_{i=1}^{n} b_{i,\alpha_i} && \text{(Lemma 2)} \\
&\leqslant (2 - 1/p^2)^{n-k} \cdot \max_{\vec{\alpha}\in C^\perp\setminus\{\vec{0}\}} \prod_{i\in J} b_{i,\alpha_i} && \text{(Claim 1)} \\
&\leqslant (2 - 1/p^2)^{n-k} \cdot \left(\frac{2}{p\sin(\pi/p)}\right)^{3k-2n+1}, && \text{(Claim 2)}
\end{aligned}$$

whence the theorem. □

3.3 Proof of Lemma 2

Recall that A_I is the set of all codewords in $C^\perp$ whose non-zero coordinates are in the set I and zero coordinates are not in I. The fact that $C^\perp$ is an $[n, n-k]_F$ MDS code implies that

$$A_\emptyset = \{\vec{0}\}, \text{ and } A_I = \emptyset \text{ for every } 0 < |I| \leqslant k \tag{3}$$

Let $\binom{[n]}{w}$ denote the set of all size-w subsets of $\{1, \ldots, n\}$. The following properties of the Fourier coefficients of leakage functions will be the key to prove Lemma 2.

Claim 3. *Let S and T be a partition of F. The the following statements hold.*

1. $\widehat{\mathbb{1}_S}(0) + \widehat{\mathbb{1}_T}(0) = 1$.
2. $\widehat{\mathbb{1}_S}(\alpha) = -\widehat{\mathbb{1}_T}(\alpha)$, *for every* $\alpha \in F \setminus \{0\}$.

The proof of Claim 3 follows from the linearity of Fourier transform and the (functional) identity $\mathbb{1}_S + \mathbb{1}_T = 1$. Using Claim 3, we shall prove the following result.

Claim 4. *For any $I \subseteq \{1, \ldots, n\}$ and any $\vec{\alpha} \in A_I$, the following identity holds.*

$$\sum_{\vec{\ell} \in \{0,1\}^n} \prod_{i=1}^{n} \left| \widehat{\mathbb{1}_{i,\ell_i}}(\alpha_i) \right| = 2^{|I|} \cdot \prod_{i \in I} \left| \widehat{\mathbb{1}_{i,0}}(\alpha_i) \right|.$$

Proof of Claim 4. Since $\vec{\alpha} \in A_I$, we know exactly the positions of Fourier coefficients at zero. Observe that the two sets $\tau_i^{-1}(0)$ and $\tau_i^{-1}(1)$ are a partition of F since τ_i is one-bit leakage function. Based on this information, the left-hand side term can be rewritten as follows.

$$\begin{aligned}
&\sum_{\vec{\ell} \in \{0,1\}^n} \prod_{i=1}^{n} \left| \widehat{\mathbb{1}_{i,\ell_i}}(\alpha_i) \right| \\
&= \sum_{\vec{\ell} \in \{0,1\}^n} \left(\prod_{i \in I} \left| \widehat{\mathbb{1}_{i,\ell_i}}(\alpha_i) \right| \right) \left(\prod_{i \notin I} \left| \widehat{\mathbb{1}_{i,\ell_i}}(\alpha_i) \right| \right) \\
&= \sum_{\vec{\ell}_I \in \{0,1\}^w} \sum_{\vec{\ell}_{\bar{I}} \in \{0,1\}^{n-w}} \left(\prod_{i \in I} \left| \widehat{\mathbb{1}_{i,\ell_i}}(\alpha_i) \right| \right) \left(\prod_{i \notin I} \left| \widehat{\mathbb{1}_{i,\ell_i}}(0) \right| \right) \\
&= \sum_{\vec{\ell}_I \in \{0,1\}^w} \left(\prod_{i \in I} \left| \widehat{\mathbb{1}_{i,\ell_i}}(\alpha_i) \right| \right) \left(\sum_{\vec{\ell}_{\bar{I}} \in \{0,1\}^{n-w}} \prod_{i \notin I} \left| \widehat{\mathbb{1}_{i,\ell_i}}(0) \right| \right) \\
&= \sum_{\vec{\ell}_I \in \{0,1\}^w} \left(\prod_{i \in I} \left| \widehat{\mathbb{1}_{i,\ell_i}}(\alpha_i) \right| \right) \left(\prod_{i \notin I} \sum_{\ell_i \in \{0,1\}} \left| \widehat{\mathbb{1}_{i,\ell_i}}(0) \right| \right) \\
&= \sum_{\vec{\ell}_I \in \{0,1\}^w} \left(\prod_{i \in I} \left| \widehat{\mathbb{1}_{i,0}}(\alpha_i) \right| \right) \left(\prod_{i \notin I} 1 \right) && \text{(Claim 3)} \\
&= 2^{|I|} \cdot \prod_{i \in I} \left| \widehat{\mathbb{1}_{i,0}}(\alpha_i) \right|. \square
\end{aligned}$$

Now, we are ready to prove Lemma 2.

Proof of Lemma 2. We have

$$
\begin{aligned}
&\sum_{\vec{\ell}\in\{0,1\}^n} \sum_{\vec{\alpha}\in C^\perp\setminus\{\vec{0}\}} \prod_{i=1}^{n} \left|\widehat{\mathbb{1}_{i,\ell_i}}(\alpha_i)\right| \\
&= \sum_{\vec{\ell}\in\{0,1\}^n} \sum_{w=1}^{n} \sum_{I\in\binom{[n]}{w}} \sum_{\vec{\alpha}\in A_I} \prod_{i=1}^{n} \left|\widehat{\mathbb{1}_{i,\ell_i}}(\alpha_i)\right| \\
&= \sum_{\vec{\ell}\in\{0,1\}^n} \sum_{w=k+1}^{n} \sum_{I\in\binom{[n]}{w}} \sum_{\vec{\alpha}\in A_I} \prod_{i=1}^{n} \left|\widehat{\mathbb{1}_{i,\ell_i}}(\alpha_i)\right| && \text{(Fact 3)} \\
&= \sum_{w=k+1}^{n} \sum_{I\in\binom{[n]}{w}} \sum_{\vec{\alpha}\in A_I} \left(\sum_{\vec{\ell}\in\{0,1\}^n} \prod_{i=1}^{n} \left|\widehat{\mathbb{1}_{i,\ell_i}}(\alpha_i)\right| \right) \\
&= \sum_{w=k+1}^{n} \sum_{I\in\binom{[n]}{w}} \sum_{\vec{\alpha}\in A_I} \left(2^w \cdot \prod_{i\in I} \left|\widehat{\mathbb{1}_{i,0}}(\alpha_i)\right| \right) && \text{(Claim 4)} \\
&= \sum_{w=k+1}^{n} \sum_{I\in\binom{[n]}{w}} \sum_{\vec{\alpha}\in A_I} \prod_{i\in I} \left(2 \cdot \left|\widehat{\mathbb{1}_{i,0}}(\alpha_i)\right| \right) \\
&= \sum_{\vec{\alpha}\in C^\perp\setminus\{\vec{0}\}} \prod_{i=1}^{n} b_{i,\alpha_i}. \square
\end{aligned}
$$

3.4 Proof of Claim 1

We need the following bound for the proof of Claim 1.

Claim 5. *It holds that* $\sum_{\alpha_i\in F} b_{i,\alpha_i}^2 \leqslant 2 - 1/p^2$ *for every* $1 \leqslant i \leqslant n$.

Proof of Claim 5. Let $\delta = \mathbb{E}_{x\in F}[\mathbb{1}_{i,\ell_i}(x)] = \widehat{\mathbb{1}_{i,\ell_i}}(0)$. Observe that δ is of the form a/p for some $0 \leqslant a \leqslant p$. This implies that $|1-2\delta| \geqslant 1/p$. Then, by Parseval's identity, it holds that

$$
\begin{aligned}
4 \sum_{\alpha_i\in F^*} \left|\widehat{\mathbb{1}_{i,\ell_i}}(\alpha_i)\right|^2 &= 4\left(\sum_{\alpha_i\in F} \left|\widehat{\mathbb{1}_{i,\ell_i}}(\alpha_i)\right|^2 \right) - 4\left|\widehat{\mathbb{1}_{i,\ell_i}}(0)\right|^2 \\
&= 4(\delta - \delta^2)
\end{aligned}
$$

Therefore, we have

$$
\begin{aligned}
\sum_{\alpha_i\in F} b_{i,\alpha_i}^2 &= 1 + \sum_{\alpha_i\in F^*} b_{i,\alpha_i}^2 = 1 + \sum_{\alpha_i\in F^*} 4\widehat{\mathbb{1}_{i,\ell_i}}(\alpha_i)^2 \\
&= 1 + 4(\delta - \delta^2) = 2 - (1-2\delta)^2 \\
&\leqslant 2 - 1/p^2.
\end{aligned}
$$

The final inequality follows from $|1-2\delta| \geqslant 1/p$. □

Next, we prove Claim 1.

Proof of Claim 1. We use a similar idea as in [BDIR18] to prove the claim. For any vector $\vec{v}$ and $I \subseteq [n]$, the vector $\vec{v}_I$ represents the vector $(v_i\colon i \in I)$. For brevity, we denote $C^\perp \setminus \{\vec{0}\}$ as D'.

Recall that $C^{\perp}$ is an $[n, n-k]_F$ MDS code. This implies that any set of $n-k$ coordinates is an information set. Since $|I_1| = |I_2| = n-k$, it holds that

$$\{\vec{\alpha}_{I_1} : \vec{\alpha} \in C^{\perp}\} = \{\vec{\alpha}_{I_2} : \vec{\alpha} \in C^{\perp}\} = F^{n-k}.$$

Therefore, we have

$$\begin{aligned}
&\sum_{\vec{\alpha}\in D'} \prod_{i=1}^{n} b_{i,\alpha_i} \\
&\leqslant \sqrt{\sum_{\vec{\alpha}\in D'} \prod_{i\in I_1} b_{i,\alpha_i}^2} \cdot \sqrt{\sum_{\vec{\alpha}\in D'} \prod_{i\in I_2\cup J} b_{i,\alpha_i}^2} && \text{(Cauchy-Schwartz's Inequality)} \\
&\leqslant \sqrt{\sum_{\vec{\alpha}\in D'} \prod_{i\in I_1} b_{i,\alpha_i}^2} \cdot \sqrt{\sum_{\vec{\alpha}\in D'} \prod_{i\in I_2} b_{i,\alpha_i}^2} \cdot \max_{\vec{\alpha}\in D'} \prod_{i\in J} b_{i,\alpha_i} \\
&\leqslant \sqrt{\sum_{\vec{\alpha}\in C^{\perp}} \prod_{i\in I_1} b_{i,\alpha_i}^2} \cdot \sqrt{\sum_{\vec{\alpha}\in C^{\perp}} \prod_{i\in I_2} b_{i,\alpha_i}^2} \cdot \max_{\vec{\alpha}\in D'} \prod_{i\in J} b_{i,\alpha_i} \\
&\leqslant \sqrt{\prod_{i\in I_1} \sum_{\alpha_i\in F} b_{i,\alpha_i}^2} \cdot \sqrt{\prod_{i\in I_2} \sum_{\alpha_i\in F} b_{i,\alpha_i}^2} \cdot \max_{\vec{\alpha}\in D'} \prod_{i\in J} b_{i,\alpha_i} \\
&\leqslant \sqrt{2^{|I_1|}} \cdot \sqrt{2^{|I_2|}} \cdot \max_{\vec{\alpha}\in D'} \prod_{i\in J} b_{i,\alpha_i} && \text{(Claim 5)} \\
&= \left(2 - 1/p^2\right)^{n-k} \cdot \max_{\vec{\alpha}\in D'} \prod_{i\in J} b_{i,\alpha_i} . \square
\end{aligned}$$

3.5 Proof of Claim 2

We shall use the following result to prove the claim.

Imported Lemma 2 ([BDIR18]). *It holds that $b_{i,\alpha_i} \leqslant \frac{2}{p\sin(\pi/p)}$ for every $\alpha_i \in F^*$.*

Proof of Claim 2. First, observe that $\vec{\alpha}$ has at least $k+1$ non-zero coordinates for any $\vec{\alpha} \in C^{\perp} \setminus \{\vec{0}\}$ since $C^{\perp}$ is an $[n, n-k]_F$ MDS code. This implies that vector $\vec{\alpha}_J$ has at least $(k+1) - 2(n-k)$ non-zero coordinates. Imported Lemma 2 and the fact that $b_{i,0} = 1$ imply that

$$\prod_{i\in J} b_{i,\alpha_i} \leqslant \left(\frac{2}{p\sin(\pi/p)}\right)^{3k-2n+1},$$

which completes the proof. □

4 Comparison of Technical Approaches

This section compares our technical approaches with previous ones.

Comparison with [BDIR18, BDIR21] Benhamouda et al. relied on estimating the Fourier-analytic proxy (Equation 1). Our analysis, however, employs the properties of the one-bit leakage function to simplify the Fourier proxy. This simplification (Equation 2) removes the summation over the leakage value $\vec{\ell} \in \{0,1\}^n$, which, in turn, results in a tighter bound after applying similar bounding techniques (e.g., Cauchy-Schwartz).

Comparison with [MPSW21] Apart from its fascinating result on the leakage-resilience of random linear codes, Maji et al. also improved the threshold from $k \geqslant 0.907n$ to $k \geqslant 8675n$ for any Shamir's secret-sharing scheme. One of their technical novelty is to analyze the proxy using the precise information on the holes of the codeword. That is, they partition the dual code $C^{\perp}$ into subsets A_I, which enables a tighter bound on the summation within each subset. We adopt similar ideas and sum over each subset A_I first. However, by additionally using special properties of one-bit leakage function, we perform an *identical transformation* to simply the proxy into Equation 2. Therefore, our analysis gives rise to an even tighter bound.

Comparison with [MNP$^+$21] Maji et al. considered leakage resilience of Shamir's secret sharing schemes as well, but against a rather weak family of leakage functions (namely, the physical-bit leakage). Their analysis is also based on the Fourier-analytic approach. However, it crucially relies on that the ℓ_1-norm of the Fourier coefficients of the physical-bit leakage is small, which does not hold in general for arbitrary leakage functions. Therefore, it is not evident if their analysis is applicable to general leakage functions.

References

[ADN+19] Divesh Aggarwal, Ivan Damgård, Jesper Buus Nielsen, Maciej Obremski, Erick Purwanto, João Ribeiro, and Mark Simkin. Stronger leakage-resilient and non-malleable secret sharing schemes for general access structures. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 510–539. Springer, Heidelberg, August 2019. doi:10.1007/978-3-030-26951-7_18. 2

[AMN+21] 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*, 2021. 2

[BDIR18] Fabrice Benhamouda, Akshay Degwekar, Yuval Ishai, and Tal Rabin. On the local leakage resilience of linear secret sharing schemes. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2018, Part I*, volume 10991 of *LNCS*, pages 531–561. Springer, Heidelberg, August 2018. doi:10.1007/978-3-319-96884-1_18. 1, 2, 3, 4, 8, 10, 11

[BDIR21] Fabrice Benhamouda, Akshay Degwekar, Yuval Ishai, and Tal Rabin. On the local leakage resilience of linear secret sharing schemes. *Journal of Cryptology*, 34(2):10, April 2021. doi:10.1007/s00145-021-09375-2. 2, 11

[BIS19] Andrej Bogdanov, Yuval Ishai, and Akshayaram Srinivasan. Unconditionally secure computation against low-complexity leakage. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 387–416. Springer, Heidelberg, August 2019. doi:10.1007/978-3-030-26951-7_14. 2

[BS19] Saikrishna Badrinarayanan and Akshayaram Srinivasan. Revisiting non-malleable secret sharing. In Yuval Ishai and Vincent Rijmen, editors, *EUROCRYPT 2019, Part I*, volume 11476 of *LNCS*, pages 593–622. Springer, Heidelberg, May 2019. doi:10.1007/978-3-030-17653-2_20. 2

[CGG+20] Eshan Chattopadhyay, Jesse Goodman, Vipul Goyal, Ashutosh Kumar, Xin Li, Raghu Meka, and David Zuckerman. Extractors and secret sharing against bounded collusion protocols. In *61st FOCS*, pages 1226–1242. IEEE Computer Society Press, November 2020. doi:10.1109/FOCS46700.2020.00117. 2

[CGN19] Gaëlle Candel, Rémi Géraud-Stewart, and David Naccache. How to compartment secrets. In Maryline Laurent and Thanassis Giannetsos, editors, *Information Security Theory and Practice - 13th IFIP WG 11.2 International Conference, WISTP 2019, Paris, France, December 11-12, 2019, Proceedings*, volume 12024 of *Lecture Notes in Computer Science*, pages 3–11. Springer, 2019. doi:10.1007/978-3-030-41702-4_1. 2

[DDKM18] Hoang Dau, Iwan M. Duursma, Han Mao Kiah, and Olgica Milenkovic. Repairing reed-solomon codes with multiple erasures. *IEEE Trans. Inf. Theory*, 64(10):6567–6582, 2018. doi:10.1109/TIT.2018.2827942. 1

[FY19] Serge Fehr and Chen Yuan. Towards optimal robust secret sharing with security against a rushing adversary. In Yuval Ishai and Vincent Rijmen, editors, *EUROCRYPT 2019, Part III*, volume 11478 of *LNCS*, pages 472–499. Springer, Heidelberg, May 2019. doi:10.1007/978-3-030-17659-4_16. 2

[FY20] Serge Fehr and Chen Yuan. Robust secret sharing with almost optimal share size and security against rushing adversaries. In Rafael Pass and Krzysztof Pietrzak, editors, *TCC 2020, Part III*, volume 12552 of *LNCS*, pages 470–498. Springer, Heidelberg, November 2020. doi:10.1007/978-3-030-64381-2_17. 2

[GK18] Vipul Goyal and Ashutosh Kumar. Non-malleable secret sharing. In Ilias Diakonikolas, David Kempe, and Monika Henzinger, editors, *50th ACM STOC*, pages 685–698. ACM Press, June 2018. doi:10.1145/3188745.3188872. 1

[GMW87] 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 ACM STOC*, pages 218–229. ACM Press, May 1987. doi:10.1145/28395.28420. 2

[GR17] Venkatesan Guruswami and Ankit Singh Rawat. MDS code constructions with small sub-packetization and near-optimal repair bandwidth. In Philip N. Klein, editor, *28th SODA*, pages 2109–2122. ACM-SIAM, January 2017. doi:10.1137/1.9781611974782.137. 1

[GW16] Venkatesan Guruswami and Mary Wootters. Repairing reed-solomon codes. In Daniel Wichs and Yishay Mansour, editors, *48th ACM STOC*, pages 216–226. ACM Press, June 2016. doi:10.1145/2897518.2897525. 1

[GW17] Venkatesan Guruswami and Mary Wootters. Repairing reed-solomon codes. *IEEE Trans. Inf. Theory*, 63(9):5684–5698, 2017. doi:10.1109/TIT.2017.2702660. 1

[HIMV19] Carmit Hazay, Yuval Ishai, Antonio Marcedone, and Muthuramakrishnan Venkitasubramaniam. LevioSA: Lightweight secure arithmetic computation. In Lorenzo Cavallaro, Johannes Kinder, XiaoFeng Wang, and Jonathan Katz, editors, *ACM CCS 2019*, pages 327–344. ACM Press, November 2019. doi:10.1145/3319535.3354258. 2

[KJJ99] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In Michael J. Wiener, editor, *CRYPTO'99*, volume 1666 of *LNCS*, pages 388–397. Springer, Heidelberg, August 1999. doi:10.1007/3-540-48405-1_25. 1

[KMS19] Ashutosh Kumar, Raghu Meka, and Amit Sahai. Leakage-resilient secret sharing against colluding parties. In David Zuckerman, editor, *60th FOCS*, pages 636–660. IEEE Computer Society Press, November 2019. doi:10.1109/FOCS.2019.00045. 2

[Koc96] Paul C. Kocher. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In Neal Koblitz, editor, *CRYPTO'96*, volume 1109 of *LNCS*, pages 104–113. Springer, Heidelberg, August 1996. doi:10.1007/3-540-68697-5_9. 1

[KR19] 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. 1

[LCG$^+$20] 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*, pages 7:1–7:24. Schloss Dagstuhl, June 2020. doi:10.4230/LIPIcs.ITC.2020.7. 2

[Mas01] James L. Massey. Some applications of coding theory in cryptography. *Mat. Contemp*, 21(16):187–209, 2001. 3

[MBW19] Jay Mardia, Burak Bartan, and Mary Wootters. Repairing multiple failures for scalar MDS codes. *IEEE Trans. Inf. Theory*, 65(5):2661–2672, 2019. doi:10.1109/TIT.2018.2876542. 1

[MNP+21] Hemanta K. Maji, Hai H. Nguyen, Anat Paskin-Cherniavsky, Tom Suad, and Mingyuan Wang. Leakage-resilience of the shamir secret-sharing scheme against physical-bit leakages. In Anne Canteaut and François-Xavier Standaert, editors, *EUROCRYPT 2021, Part II*, volume 12697 of *LNCS*, pages 344–374. Springer, Heidelberg, October 2021. doi:10.1007/978-3-030-77886-6_12. 2, 3, 12

[MPSW21] 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, *CRYPTO 2021, Part III*, volume 12827 of *LNCS*, pages 779–808, Virtual Event, August 2021. Springer, Heidelberg. doi:10.1007/978-3-030-84252-9_26. 2, 3, 12

[MS77] Florence Jessie MacWilliams and Neil James Alexander Sloane. *The theory of error correcting codes*, volume 16. Elsevier, 1977. 3, 4

[MSV20] Pasin Manurangsi, Akshayaram Srinivasan, and Prashant Nalini Vasudevan. Nearly optimal robust secret sharing against rushing adversaries. In Daniele Micciancio and Thomas Ristenpart, editors, *CRYPTO 2020, Part III*, volume 12172 of *LNCS*, pages 156–185. Springer, Heidelberg, August 2020. doi:10.1007/978-3-030-56877-1_6. 2

[Rao07] Anup Rao. An exposition of bourgain's 2-source extractor. 2007. 3, 6

[SV19] Akshayaram Srinivasan and Prashant Nalini Vasudevan. Leakage resilient secret sharing and applications. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 480–509. Springer, Heidelberg, August 2019. doi:10.1007/978-3-030-26951-7_17. 2

[TYB17] Itzhak Tamo, Min Ye, and Alexander Barg. Optimal repair of reed-solomon codes: Achieving the cut-set bound. In Chris Umans, editor, *58th FOCS*, pages 216–227. IEEE Computer Society Press, October 2017. doi:10.1109/FOCS.2017.28. 1