New Bounds on the Local Leakage Resilience of Shamir's Secret Sharing Scheme

Ohad Klein[1] and Ilan Komargodski[2].

[1] Hebrew University of Jerusalem, Israel
ohadkel@gmail.com
[2] Hebrew University of Jerusalem and NTT Research, Israel
ilank@cs.huji.ac.il

Abstract. We study the local leakage resilience of Shamir's secret sharing scheme. In Shamir's scheme, a random polynomial f of degree t is sampled over a field of size $p > n$, conditioned on $f(0) = s$ for a secret s. Any t shares $(i, f(i))$ can be used to fully recover f and thereby $f(0)$. But, any $t-1$ evaluations of f at non-zero coordinates are completely independent of $f(0)$. Recent works ask whether the secret remains hidden even if say only 1 bit of information is leaked from each share, independently. This question is well motivated due to the wide range of applications of Shamir's scheme. For instance, it is known that if Shamir's scheme is leakage resilient in some range of parameters, then known secure computation protocols are secure in a local leakage model.

Over characteristic-2 fields, the answer is known to be negative (e.g., Guruswami and Wootters, STOC '16). Benhamouda, Degwekar, Ishai, and Rabin (CRYPTO '18) were the first to give a positive answer assuming computation is done over prime-order fields. They showed that if $t \geq 0.907n$, then Shamir's scheme is leakage resilient. Since then, there has been extensive efforts to improve the above threshold and after a series of works, the current record shows leakage resilience for $t \geq 0.78n$ (Maji et al., ISIT '22). All existing analyses of Shamir's leakage resilience for general leakage functions follow a single framework for which there is a known barrier for any $t \leq 0.5n$.

In this work, we a develop a new analytical framework that allows us to significantly improve upon the previous record and obtain additional new results. Specifically, we show:

1. Shamir's scheme is leakage resilient for any $t \geq 0.69n$.
2. If the leakage functions are guaranteed to be "balanced" (i.e., splitting the domain of possible shares into 2 roughly equal-size parts), then Shamir's scheme is leakage resilient for any $t \geq 0.58n$.
3. If the leakage functions are guaranteed to be "unbalanced" (i.e., splitting the domain of possible shares into 2 parts of very different sizes), then Shamir's scheme is leakage resilient as long as $t \geq 0.01n$. Such a result is *provably* impossible to obtain using the previously known technique.

All of the above apply more generally to any MDS codes-based secret sharing scheme.

Confirming leakage resilience is most important in the range $t \leq n/2$, as in many applications, Shamir's scheme is used with thresholds $t \leq n/2$.

As opposed to the previous approach, ours does not seem to have a barrier at $t = n/2$, as demonstrated by our third contribution.

Keywords: Secret sharing, Shamir's scheme, local leakage resilience.

1 Introduction

Secret sharing schemes, introduced by Shamir [35] and Blakley [6] are methods that enable a dealer, that holds a secret piece of information, to distribute this secret among n parties such that any subset of at least t parties can reconstruct the secret, while subsets that contain fewer than t parties learn nothing about it.

Secret sharing schemes are extremely useful in various applications across multiple sub-areas of computer science, including cryptography, complexity, and distributed computing and storage. Secret sharing schemes are also strongly related to error correcting codes. We name just a few concrete applications where secret sharing schemes are a fundamental building block: secure multiparty computation protocols [17, 3, 11], threshold cryptography schemes [16, 13, 34], and leakage-resilient circuit compilers [21, 15, 33].

At their basic use-case, secret sharing schemes have an "all-or-nothing"-style security guarantee, wherein an adversary is allowed to corrupt up to t parties but must know absolutely nothing about the others parties' shares. While this assumption is often made in an ideal world, it is a very strong assumption in many practical scenarios. Indeed, it has been long known that side-channel information is widely available [22, 23].

Research then has focused on designing new leakage resilient cryptographic protocols in various models of leakage, for example, [30, 14, 31, 2, 7]. However, it is also worth understanding whether existing schemes are leakage resilient. Indeed, if an existing method is already leakage resilient, it alleviates the necessity to design, analyse, and deploy new schemes. In this work, we focus on the latter and continue the recent line of works studying the leakage resilience of Shamir's secret sharing scheme [5, 26, 27, 28, 25, 1], the most well-known and useful secret sharing scheme.

(Local) leakage resilience of Shamir's scheme. Shamir's scheme is very simple to describe: For a secret s, the dealer samples a random degree $t-1$ (univariate) polynomial f over a sufficiently large finite field $\mathbb{F}$, conditioned on $f(0) = s$. Then, the dealer gives party i the field element $f(i)$. Evaluations of f at t different points can be used to fully recover f and thereby $s = f(0)$. Also, it is known that any $< t$ evaluations of f (excluding $f(0)$) are completely uncorrelated with $f(0)$. This scheme is the most commonly used (threshold) secret sharing scheme, both in theory and in practice. This is mostly due to its simplicity, elegance, and various useful features it supports like additive homomorphism (i.e., linearity).

We consider local leakage attacks: In addition to fully learning some of the shares, the attacker can leak few bits of information about each other parties' share locally, independently of the other parties' state. That is, the adversary can specify $t' < t$ indices $i_1, \ldots, i_{t'} \in [n]$ and n functions $f_1, \ldots, f_n$ with a short output. Denoting the shares by $\pi_1, \ldots, \pi_n$, it then receives back $\pi_{i_1} \ldots, \pi_{i_t}$ and $f_1(\pi_1), \ldots, f_n(\pi_n)$, and it needs to guess (something about) $f(0)$.

The motivation of the problem comes from that if Shamir's scheme is leakage resilient, then some applications that use it are more secure than what they are currently known to be. For instance, the work of Benhamouda, Degwekar, Ishai, and Rabin [4, 5] (who initiated the study of the problem that we consider) showed that Shamir's scheme leakage resilience implies that a minor variant of the Goldreich-Micali-Wigderson's [17] secure computation protocol is secure even in a local leakage model. Apart from its applications, understanding the leakage resilience of Shamir's scheme is a very natural question on its own right, especially due to its connection to error correcting codes, and more precisely to Reed-Solomon codes. (Shamir's scheme is in particular a Reed-Solomon code.)

State of the art. The local leakage resilience of Shamir's scheme is far from being understood. Despite significant efforts, there is essentially only one method for analyzing it and for this method there are known barriers showing that it cannot lead to full resolution of the problem. This method, based on Fourier analysis over prime-order fields, was introduced by [4] and since then all works improving upon their bound, somewhat incrementally optimize various parts of the analysis.

For concreteness and simplicity of presentation, we focus on the most studied case where each leakage function (i.e., each f_i) outputs a single bit. Benhamouda et al.'s [4] original work showed that Shamir's scheme is leakage resilient as long as $t \geq 0.907n$. Then, Maji et al. [28] and Benhamouda et al. [5] independently lowered this threshold to $t \geq 0.8675n$ and $t \geq 0.85n$, respectively. The state of the art is due to Maji et al. [27] who showed that Shamir's scheme is leakage resilient as long as $t \geq 0.78n$.

All of the above works, use an analytic proxy (introduced already in [4]'s original work) for upper bounding the statistical distance between leakage distributions of different secrets. Maji et al. [28] showed an inherent barrier for this proof strategy: It is impossible to prove any meaningful result for any $t \leq 0.5n$ (which is required to, say, execute secure computation protocols in the honest majority setting). It is worth noting that Shamir's scheme is *not* leakage resilient if $t = O(n/\log n)$ [32, 28].[3]

At a very high level, the analytical proxy bounds the statistical distance between certain distributions via direct expansion and summing up the distances at every point in the sample space. Then, a triangle inequality is performed

[3] Shamir's scheme uses $t \cdot \log p$ bits of entropy if we work over a p-size field, and so intuitively, the total amount of entropy leaked should not exceed this number. If we leak just one bit from every share, then $n < t \cdot \log p$ is required for security. As mentioned, $\log p$ can be replaced by $\log n$.

so that each term in the summation could be analyzed and bound by itself. This triangle inequality, however, is very lossy and causes the proof approach to provably fail whenever $t \leq 0.5n$ [28]. Since many of the applications of Shamir's scheme require $t < n/2$ or $t < n/3$ (for example, BGW [3] or GMW [17] with fairness) there is currently no path to handle them.

1.1 Our Results

In this work, we introduce a completely new analytical framework that, in particular, bypasses the barrier of the only previously known approach. We use our approach to prove several new results that were out of reach previously. At a very high level, we obtain our improvements because our analysis is roughly an ℓ_2 bound on the distance between the corresponding distributions, whereas the previous approach is an ℓ_1 bound. In particular, we never apply lossy triangle inequalities.

Using our new framework, we prove several new results for the leakage resilience of Shamir's scheme. In what follows, we assume that the leakage functions output a single bit, either -1 or 1. Further, we assume that the field size, p, is at most $2^{O(n)}$.[4]

1. We improve the previously best bound on the leakage resilience of Shamir's scheme from $0.78n$ to $0.69n$. That is, Shamir's scheme is leakage resilient as long as $t \geq 0.69n$.
2. We further improve the threshold to $0.58n$ for all "balanced" leakage functions. That is, assuming that the leakage functions satisfy $|\mathbb{E}[f_i]| \leq c$,[5] where $c > 0$ a universal constant, then Shamir's scheme is leakage resilient as long as $t \geq 0.58n$.
3. For the complementary case, where the leakage functions are unbalanced, we break the $t \geq 0.5n$ barrier. Specifically, we show that if the leakage functions satisfy $|\mathbb{E}[f_i]| \geq C$ with a specific constant $C < 1$, then Shamir's scheme is leakage resilient as long as $t \geq 0.01n$. We show that it is *provably* impossible to obtain such a result using the previously known technique.

All of the results above directly generalize to the setting where the adversary further obtains some of the shares in their entirety.[6] Also, we note that all of the above results apply to any MDS code-based secret sharing scheme (i.e., so called Massey secret sharing schemes [29]) of which Shamir's scheme is a special case obtained by using the Reed-Solomon code (see Section 2.1).

[4] Typically, Shamir's scheme is used with p proportional to n.

[5] The bias $\mathbb{E}[f_i]$ is the proportion of inputs for which f_i outputs 1 minus the proportion of inputs f_i outputs -1. Note that intuitively, the balanced case has the highest leakage of information.

[6] This is a standard reduction. The view of a distinguisher that sees t' of the n shares in their entirety, can be reduced to a distinguisher for a Shamir secret sharing scheme over $n - t'$ parties that sees none of the shares in their entirety.

Technical highlight. Our analysis completely deviates from the previous approach that all works followed. In our view this is one of the highlights of this work and we believe that further improvements and results are achievable with our framework. We also believe that some of our intermediate technical transitions are of independent interest. We highlight some of the technical ideas behind our analysis in Section 1.3.

Paper organization. In Section 1.2 we survey some related work. In Section 1.3 we highlight some of the main technical ideas underlying our analyses. In Section 2 we provide preliminary definitions and notation. The main analytical framework is given in Section 3. The improved bound for Shamir's scheme leakage resilience for $t \geq 0.69n$ is given in Section 4. The bound for $t \geq 0.58n$ and balanced leakage functions is given in Section 5. The bound for $t \geq 0.01n$ and unbalanced leakage functions is given in Section 6.

1.2 Related Work

While the notion of local leakage may seem rather weak, it can be quite powerful. In particular, it is not hard to see that if we work over a field $\mathbb{F}_{2^k}$ of characteristic 2, then a bit of the secret can be learnt by leaking just one bit from each share. (This is true for any linear secret sharing scheme.) Surprisingly, for Shamir's scheme and in some settings of parameters, Guruswami and Wooters [20] showed that full recovery of a multi-bit secret is possible by leaking only one bit from each share.

Benhamouda et al. [4] were the first to study the local leakage resilience of Shamir's scheme (over prime-order fields) showing that whenever $t \geq 0.907n$, Shamir's scheme is leakage resilient. Maji et al. [28] and Benhamouda et al. [5] independently lowered the threshold to $t \geq 0.8675n$ and $t \geq 0.85n$, respectively. Before the current work, the record was leakage resilience whenever $t \geq 0.78n$ due to Maji et al. [27]. Nielsen and Simkin [32] presented an attack that requires $m > t \log p/(n-t)$ bits of leakage from each secret share, where p is the field size, and then guesses the secret with probability $1/2$.

With the lack of progress in analyzing Shamir's scheme for general leakage functions, efforts have been made to analyze restricted classes of leakage functions or "random" constructions. Maji et al. [25] considered a leakage family that is only allowed to leak an arbitrary single bit from each share (given in their binary representation). This was later generalized to arbitrary bounded-size families of leakage functions by Maji et al. [26]. Maji et al. [28] also proved that a random (linear) secret sharing scheme is leakage resilient to one-bit local leakage when $t \geq 0.5n$. This was partially derandomized in [28, 26] who studied the leakage resilience of Shamir's scheme with random evaluation points.

All of the above works essentially use the analytic proxy from [4]'s work for upper bounding the statistical distance between leakage distributions of different secrets. Maji et al. [28] showed that this technique cannot be used to go below threshold $t = n/2$ for general leakage functions.

New (non-linear) schemes. A large body of work focused on designing new leakage resilient secret sharing schemes from scratch. Such schemes were constructed for the first time by Dziembowski and Pietrzak [14]. Their scheme involved an interactive reconstruction procedure, which was needed for allowing the reconstruction to access only small part of the shares. Simpler constructions (without the latter efficiency feature) were proposed by Davì et al. [12]. In particular, they presented a simple two-party scheme based on any two-source extractor, such as the inner-product extractor. More general constructions of leakage-resilient secret-sharing schemes were given by Goyal and Kumar [18, 19], Srinivasan and Vasudevan [36], Kumar, Meka, and Sahai [24], Chattopadhyay et al. [10], and Chandran et al. [8, 9]. All of these works, design specialized secret sharing schemes that have strong leakage resilience properties and/or apply to more general access structures. It is noteworthy that in all of these works, the schemes are non-linear, making them less applicable.

1.3 Main Techniques

A bound on the statistical distance. While the previous approaches directly bound the statistical distance between leakage distributions corresponding to different secrets via a point-by-point analysis, we rather take a more "average case" approach. As our starting point, we use the following inequality[7]. Consider two random variables X and Y, where X is uniform over a size p set and Y is arbitrary. Then for all x_1, x_2 we have

$$\mathsf{SD}(Y|X = x_1, Y|X = x_2) \leq p \cdot \sqrt{\mathop{\mathbb{E}}_{Y}\left[\|P(X|Y) - 1/p\|_2^2\right]}, \tag{1}$$

where $\mathsf{SD}(\cdot, \cdot)$ stands for statistical distance and $P(X|Y)$ is the length-p vector of probabilities of X conditioned on Y. (See Lemma 2.2 for the statement.) The proof of this inequality follows by applying a Pinsker inequality and then expanding via the definition of the Kullback–Leibler (KL) divergence.

In our use case, Y is the output of the leakage functions and X is the the secret. The left hand side captures the advantage of an adversary in guessing which secret was used given the leakage. The lemma says that this advantage is upper bounded, roughly, by the average distance of the "distribution of the secret given the leakage" from random.

After reducing the problem to bounding the right-hand side, the analysis continues via (discrete) high-order Fourier analysis. We refer to Section 2.4 for an introduction and preliminaries. After several Fourier analytic manipulations, we obtain our main technical result "proxy" for analyzing the leakage resilience of Shamir's scheme, stated next.

Let $f_1, \ldots, f_n \colon \mathbb{F}_p \to \{\pm 1\}$ be arbitrary leakage functions. Further, assume that the secret sharing scheme generates shares π_i via linear functions $\ell_i \colon \mathbb{F}_p^t \to$

[7] We suspect that this inequality is well known, but we could not find it in the literature. Thus, we include a self contained proof.

$\mathbb{F}_p$. Since each ℓ_i is linear, we will sometimes view it as a vector which represents the function by performing inner product with the input. Let ℓ_0 be the function/vector that corresponds to the secret. Lastly, for a set $S \subseteq [n]$, let

$$f_S(x) := \prod_{i \in S} f_i(\ell_i(x)).$$

We show that the chance of guessing the secret correctly given the leakage via the f_i's is at most

$$2\left(p^3 \sum_{k \in \mathbb{F}\setminus\{0\}} \sum_{S \subseteq [n]} \left|\widehat{f_S}(k \cdot \ell_0)\right|^2\right)^{1/4}. \tag{2}$$

Here, $\widehat{f_S}(\alpha)$ is a Fourier coefficient of f_S corresponding to a frequency $\alpha \in \mathbb{F}_p^t$. (See Theorem 3.1 for the statement.)

Interpretation of Eq. (2)**.** Let $S \subseteq [n]$. The attacker is able to compute $f_S(x)$ using the leakage information $f_i(\ell_i(x))$. The correlation between $f_S(x)$ and $\exp(2\pi\iota k\ell_0(x)/p)$ is by definition $\widehat{f_S}(k \cdot \ell_0)$. If the attacker arranges functions f_i (of his choice) with $|\widehat{f_S}(k \cdot \ell_0)|$ large, then by computing $f_S(x)$ the attacker ends up with significant statistical knowledge regarding the secret $\ell_0(x)$. Roughly speaking, the bound in Eq. (2) states that this attack is in some sense optimal – the advantage of the attacker is bounded by the aggregation (sum) of the advantages over all $S \subseteq [n]$ and $k \in \mathbb{F}_p$. We note that the additional p factors in the right hand side of Eq. (2) are presumably an artifact of our proof, and the (standard) choice to bound the left hand side of Eq. (1) rather than a more average-case measure of advantage, such as $\mathsf{SD}(\textbf{Secret}|\textbf{Leakage}, \text{Uniform}(\mathbb{F}_p))$.

General case $t \geq 0.69n$. We proceed by bounding Eq. (2) in various ways. For instance, when $t \geq n/2$ and $S \subseteq n$, we show that

$$|\widehat{f_S}(\ell_0)| \leq O((2/\pi)^{2t-|S|}). \tag{3}$$

Plugging this in Eq. (2), and replacing ℓ_0 with $k \cdot \ell_0$, we get a geometric sum which is $\exp(-\Omega(n))$ as long as $t \geq 0.69n$ and $p \leq \exp(O(n))$, where the hidden term in the "O" is some fixed small constant. This confirms leakage resilience. In order to prove Eq. (3), we split S into half $S = L \cup R$ and consider

$$\widehat{f_S}(\ell_0) = \mathop{\mathbb{E}}_x\left[f_L(x) \cdot f_R(x) \cdot \exp\left(\frac{2\pi\iota\langle \ell_0, x\rangle}{p}\right)\right] \tag{4}$$

as an inner product of two functions. Using Plancherel's identity we move to Fourier representation. Since the ℓ_i's are MDS (that is, no short linear combination of the ℓ_i's is zero), and the Fourier spectrum of f_L is contained in $\mathrm{span}\{\ell_i \colon i \in L\}$ (likewise for R), most summands vanish, being equal to 0 in one of the Fourier transforms, and allowing to obtain Eq. (3).

Balanced case $t \geq 0.58n$. Assume the f_i are completely balanced, that is, $\mathbb{E}[f_i] = 0$. Then, $\{f_S\}_{S \subseteq [n] \setminus [n-t]}$ is an orthonormal set of functions. To see this, note that $f_S \cdot f_T = f_{S \triangle T}$ and that $|f_S| = 1$. It is hence sufficient to verify $\mathbb{E}[f_S] = 0$ whenever $S \neq \emptyset$. The premise of t-out-of-n secret sharing scheme implies that as $|S| \leq t$, there is no annihilating linear combination of $\{\ell_i\}_{i \in S}$, which yields that $\mathbb{E}[f_S] = \widehat{f_S}(0) = 0$ through discrete Fourier expansion.

Viewing Eq. (2) as a sum of squares of inner products, we use a variant of the classical Pythagorean theorem to leverage Eq. (3) to the bound

$$\sum_{S\colon S \cap [n-t] = I} \widehat{f_S}(\ell_0)^2 \leq O((2/\pi)^{2t-2|I|})$$

for any $I \subseteq [n-t]$ (see further details in Lemma 5.3). Finally, we use induction to relax this argument for quite (and not completely) balanced functions.

Unbalanced case $t \geq 0.01n$. This is the simplest of the cases and it applies whenever the leakage functions f_i are sufficiently (but constantly) biased. We first reduce the problem to bounding $\widehat{g_{[n]}}(\ell_0)$ where $g_i = f_i - \mathbb{E}[f_i]$. Then we use that $\mathbb{E}[g_i^2] = \mathbb{E}[f_i^2] - \mathbb{E}[f_i]^2 = \epsilon_i$ with $\epsilon_i > 0$ small to proceed with a Cauchy-Schwarz argument.

2 Preliminaries

For a distribution X we denote by $x \leftarrow X$ the process of sampling a value x from the distribution X. For a set X, we denote by $x \leftarrow X$ the process of sampling a value x from the uniform distribution on X. The support of the distribution X is denoted $\mathsf{supp}(X)$. For an integer $n \in \mathbb{N}$ we denote by $[n]$ the set $\{1, 2, \ldots, n\}$.

2.1 Coding and Secret Sharing

Coding. Let $\mathbb{F}_p$ be a finite field of order p. A linear code C over $\mathbb{F}_p$ of length $n+1$ and rank t is a t-dimensional vector space of $\mathbb{F}_p^{n+1}$. It is often referred to as a $[n+1, t]_{\mathbb{F}_p}$-code. The generator matrix $\mathbf{G} \in \mathbb{F}_p^{t \times (n+1)}$ of C satisfies that for every $\overrightarrow{y} \in C$, there is $\overrightarrow{x} \in \mathbb{F}_p^t$ such that $\overrightarrow{x}\mathbf{G} = \overrightarrow{y}$. We say that a generator matrix $\mathbf{G}$ is in *standard form* if $\mathbf{G} = [\mathbf{I}_t \mid \mathbf{P}]$ where $\mathbf{I}_t \in \mathbb{F}_p^{t \times t}$ is the identity matrix and $\mathbf{P} \in \mathbb{F}_p^{t \times (n-t+1)}$ is the parity check matrix of C. We always assume that generating matrices are in standard form.

Secret sharing. Secret sharing schemes allow a dealer to distribute a secret piece of information among several parties such that only qualified subsets of parties can reconstruct the secret. The most famous scheme is due to Shamir [35]. In this scheme, a secret is shared among n parties such that any $1 < t < n$ parties can recover the secret while any $t-1$ parties learn nothing about the secret. The scheme is often described as follows: the dealer chooses a random polynomial of degree $t-1$ conditioned on setting the free coefficient to be the secret, and gives the i-th party the evaluation of the polynomial at the point i (the computation is done over a field of size $p > n$). Another way to describe this scheme is by sampling a codeword from a Reed-Solomon code. In fact, any (linear) code gives rise to a secret sharing scheme, as we describe next.

Massey secret sharing. Let $C \subseteq \mathbb{F}_p^{n+1}$ be a code. Let $s \in \mathbb{F}_p$ be a secret that we wish to share among n parties. Sample a random codeword $(s_0, \ldots, s_n) \in C$ conditioned on $s_0 = s$. Give party i the share s_i, for $i \in [n]$. If the code C is linear with associated generating matrix $\mathbf{G}$, this process can be done as follows. Pick $x_2, \ldots, x_t \in \mathbb{F}_p$ uniformly at random and set $x_1 = s$ be the secret. Let $(y_0, \ldots, y_n) = (x_1, x_2, \ldots, x_t) \cdot \mathbf{G}$. The secret share of party i is y_i. Observe that since $\mathbf{G}$ is in standard form, $y_0 = s$. Since y_i is some linear function of $\{x_j\}_j$, we usually write $y_i = \ell_i(x)$ where $\ell_i \colon \mathbb{F}_p^t \to \mathbb{F}_p$ is a linear function.

2.2 Entropy and Distances

Given a random variable X supported in a finite set $\mathcal{X}$, its entropy is

$$H(X) = -\sum_{x \in \mathcal{X}} \Pr[X = x] \cdot \log \Pr[X = x].$$

The conditional entropy of a random variable Y supported in a finite set $\mathcal{Y}$ given that the value of another random variable X supported in a finite set $\mathcal{Y}$

$$H(Y \mid X) = -\sum_{x \in \mathcal{X}, y \in \mathcal{Y}} \Pr[X = x, Y = y] \cdot \log \frac{\Pr[X = x, Y = y]}{\Pr[X = x]}.$$

Let P and Q be two distributions over a finite set Ω. The statistical distance between P and Q is

$$\mathsf{SD}(P, Q) = \frac{1}{2} \sum_{x \in \Omega} |P(x) - Q(x)|.$$

We say that P and Q are ϵ-close if $\mathsf{SD}(P, Q) \leq \epsilon$.
The KL-divergence between the distributions P and Q is defined to be

$$\mathsf{KL}(P \| Q) = \sum_{x \in \Omega} P(x) \cdot \log \frac{P(x)}{Q(x)} = H(P, Q) - H(P),$$

where and $H(P) = -\sum_{x \in \Omega} P(x) \cdot \log P(x)$ is the entropy of P and $H(P, Q) = -\sum_{x \in \Omega} P(x) \cdot \log Q(x)$ is the cross entropy of P and Q.

The well-known Pinsker inequality relates the statistical distance and the KL-divergence of P and Q.

Theorem 2.1 (Pinsker inequality).

$$\mathsf{SD}(P, Q) \leq \sqrt{\frac{1}{2} \cdot \mathsf{KL}(P \| Q)}.$$

Using Pinsker's inequality, we prove the following useful inequality.

Lemma 2.2. *Let X, Y be (possibly dependent) random variables. Assume that X is uniformly distributed in a set $\mathcal{X}$ of size p. Then, for every $x_1, x_2 \in \mathcal{X}$, it holds that*

$$\mathsf{SD}(Y|X = x_1, Y|X = x_2) \leq p \cdot \sqrt{\mathop{\mathbb{E}}_{Y}\left[\|P(X|Y) - P(X)\|_2^2\right]},$$

where $P(X)$ is the length-p vector of probabilities of X.

Proof. For X distributed uniformly over $\mathcal{X}$ and for every $x_1, x_2 \in \mathcal{X}$ (assuming $x_1 \neq x_2$), applying the triangle inequality, we have that

$$\begin{aligned}(\mathsf{SD}(Y|X = x_1, Y|X = x_2))^2 &\leq \sum_{k=1}^{2} 2 \cdot (\mathsf{SD}(Y|X = x_k, Y))^2 \\ &\leq \sum_{x \in \mathcal{X}} 2 \cdot (\mathsf{SD}(Y|X = x, Y))^2 .\end{aligned}$$

By Pinsker's inequality (Theorem 2.1), the above can be bounded by

$$\leq \sum_{x \in \mathcal{X}} \mathsf{KL}\left(Y|X = x \| Y\right)$$

Let $\mathcal{Y}$ be the support of Y. By definition of KL divergence, we expand the above as

$$\begin{aligned}&= \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} \Pr[Y = y|X = x] \cdot \log \frac{\Pr[Y = y|X = x]}{\Pr[Y = y]} \\ &= \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} \Pr[X = x|Y = y] \cdot \frac{\Pr[Y = y]}{\Pr[X = x]} \cdot \log \frac{\Pr[X = x|Y = y]}{\Pr[X = x]} \\ &= p \cdot \sum_{x \in \mathcal{X}} \mathop{\mathbb{E}}_{y \leftarrow Y}\left[\Pr[X = x|Y = y] \cdot \log \frac{\Pr[X = x|Y = y]}{1/p}\right]\end{aligned}$$

Since $\log x \leq x - 1$ and by linearity of expectation, we get

$$\begin{aligned}&\leq p^2 \cdot \sum_{x \in \mathcal{X}} \mathop{\mathbb{E}}_{y \leftarrow Y}\left[\Pr[X = x|Y = y] \cdot \left(\Pr[X = x|Y = y] - \frac{1}{p}\right)\right] \\ &= p^2 \cdot \mathop{\mathbb{E}}_{y \leftarrow Y}\left[\sum_{x \in \mathcal{X}} \Pr[X = x|Y = y] \cdot \left(\Pr[X = x|Y = y] - \frac{1}{p}\right)\right] \\ &= p^2 \cdot \mathop{\mathbb{E}}_{Y}\left[\|P(X|Y) - P(X)\|_2^2\right],\end{aligned}$$

where the last equality holds since $\sum_{x \in \mathcal{X}} \Pr[Z = x](\Pr[Z = x] - 1/p) = \sum_{x \in \mathcal{X}}(\Pr[Z = x] - 1/p)^2$ for a random variable Z supported on a set $\mathcal{X}$ of size p. □

2.3 Leakage Resilient Secret Sharing

We consider the local leakage resilience notion, following Benhamounda et al. [4] and [5, Definition 4.1]. In this model, in addition to fully learning some of the shares, the attacker can leak few bits of information about each other parties' share locally and independently of the other parties' state.

Consider a t-out-of-n secret sharing scheme with shares ranging in a set $\mathcal{X}$ of size p. Denote by $\mathsf{Share}(s)$ the function that takes as input a secret s and outputs n shares $\pi_1, \ldots, \pi_n$ (fed with uniform randomness). We say that the scheme is (t', m, ϵ)-*local leakage resilient* if for any two secrets s_0, s_1, any $f_1, \ldots, f_n \colon \mathcal{X} \to \{-1, 1\}^m$ and any subset of parties $\Theta \subseteq [n]$ of size at most t', it holds that the distributions

$$(\{\pi_i\}_{i \in \Theta}, f_1(\pi_1), \ldots, f_n(\pi_n)) \quad | \quad \pi_1, \ldots, \pi_n \leftarrow \mathsf{Share}(s_0)$$

and

$$(\{\pi_i\}_{i \in \Theta}, f_1(\pi_1), \ldots, f_n(\pi_n)) \quad | \quad \pi_1, \ldots, \pi_n \leftarrow \mathsf{Share}(s_1)$$

are ϵ-close in statistical distance.

Assuming that $t' = 0$. Following all previous works in this area, in our technical part, we assume that $t' = 0$. This is justified since it can be made somewhat without loss of generality, up to a loss in parameters. Specifically, since we consider MDS code-based secret sharing schemes, once some t' shares are fully leaked, the rest behaves as an MDS code except on fewer parties. That is, if we fully leak t' shares, then we remain with an identical secret sharing scheme on $n - t'$ parties. So, if we prove $(0, m, \epsilon)$-leakage resilience for a t-out-of-n scheme, then it implies a (t', m, ϵ)-leakage resilience for a t-out-of-$(n - t')$ scheme.

2.4 Fourier Analysis

We introduce basic notation and recall facts from Fourier analysis. We interchangeably write $\mathbb{F}_p$ either for the field with p (prime) elements, or the group $\mathbb{Z}/p\mathbb{Z}$, or the set of numbers $\{0, 1, \ldots, p-1\}$ where the meaning is clear from the context.

The characters of the group $\mathbb{F}_p$ are the complex-valued functions $\chi_a \colon \mathbb{F}_p \to \mathbb{C}$, where a ranges over $\mathbb{F}_p$, defined as $\chi_a(x) = \exp(2\pi\iota a x/p)$. For a complex number $z \in \mathbb{C}$, we let $\overline{z}$ be its complex conjugate. The characters are an orthonormal basis with respect to the inner product $\langle f, g \rangle = \mathbb{E}_x[f(x) \cdot \overline{g(x)}]$ with x chosen uniformly from $\mathbb{F}_p$. The characters inherit the group structure: $\chi_a \cdot \chi_b = \chi_{a+b}$ and $\chi_a^{-1} = \overline{\chi_a} = \chi_{-a}$. Every function $f \colon \mathbb{F}_p \to \mathbb{C}$ can then be uniquely written as a linear combination $f = \sum_{a \in \mathbb{F}_p} \widehat{f}(a) \cdot \chi_a$ with the Fourier coefficients $\widehat{f}(a)$ given by $\widehat{f}(a) = \langle f, \chi_a \rangle = \mathbb{E}_x[f(x) \cdot \overline{\chi_a(x)}]$.

The L_2-norm of f is $\|f\|_2 = (\mathbb{E}_x[|f(x)|^2])^{1/2}$ and its L_∞ norm is $\|f\|_\infty = \max_x |f(x)|$. The ℓ_2 norm of $\widehat{f}$ is $\|\widehat{f}\|_2 = \sqrt{\sum_{\alpha \in \mathbb{F}_p} \left|\widehat{f}(\alpha)\right|^2}$. Parseval's identity is

$\|f\|_2^2 = \sum_{\alpha\in\mathbb{F}_p} \left|\widehat{f}(\alpha)\right|^2$. All of the above naturally extends to $\mathbb{F}_p^n$ by tensoring. Explicitly, a character of $\mathbb{F}_p^n$ associated with the frequency $\alpha \in \mathbb{F}_p^n$ is given by $\chi_\alpha(x) := \exp(2\pi\iota\langle\alpha, x\rangle/p)$, and the Fourier expansion of $f\colon \mathbb{F}_p^n \to \mathbb{C}$ is given by $f = \sum_{\alpha\in\mathbb{F}_p^n} \widehat{f}(\alpha)\chi_\alpha$ with $\widehat{f}(\alpha) \in \mathbb{C}$ satisfying $\widehat{f}(\alpha) = \mathbb{E}_x[f(x)\overline{\chi_\alpha(x)}]$, where $x \sim \mathbb{F}_p^n$ is uniformly distributed. In addition, α is interchangeably identified with the linear function $\alpha(x) = \langle\alpha, x\rangle$. Plancherel's identity gives $\mathbb{E}_x[f(x)\overline{g(x)}] = \sum_{\alpha\in\mathbb{F}_p^n} \widehat{f}(\alpha)\overline{\widehat{g}(\alpha)}$ where $g\colon \mathbb{F}_p^n \to \mathbb{C}$.

Euler's formula states that for any real number x, $\exp(ix) = \cos(x) + i\sin(x)$ and therefore $\mathsf{Re}(\exp(ix)) = \cos(x)$, where $\mathsf{Re}(z) = (z + \overline{z})/2$.

3 Main Analytical Framework

Let $\ell_0, \ldots, \ell_n\colon \mathbb{F}_p^t \to \mathbb{F}_p$ be linear functions (i.e., $\ell_i(x) = \sum_{j=1}^t \ell_{ij}x_j$), and let $f_1, \ldots, f_n\colon \mathbb{F}_p \to \{-1, 1\}$ be arbitrary functions. In applications, x is the internal randomness generating the secret sharing scheme, while $\ell_i(x)$ is the i'th share, with $\ell_0(x)$ the secret. We may sometimes view the ℓ_i's as functions and other times as vectors, depending on the context. We denote

$$\mathsf{leak}(x) := (f_1(\ell_1(x)), \ldots, f_n(\ell_n(x))).$$

Moreover, when ℓ_i are clear from the context, define the function $f_S\colon \mathbb{F}_p^t \to \{-1, 1\}$ as

$$f_S(x) := \prod_{i\in S} f_i(\ell_i(x)).$$

The main theorem of this section is stated next.

Theorem 3.1. *Let $\ell_0, \ldots, \ell_n\colon \mathbb{F}_p^t \to \mathbb{F}_p$ be $n+1$ nonzero linear functions. Let $f_1, \ldots, f_n\colon \mathbb{F}_p \to \{-1, 1\}$ be arbitrary functions. Then, for every $s_1, s_2 \in \mathbb{F}_p$, it holds that*

$$\begin{gathered}\mathsf{SD}(\mathsf{leak}(X)|\ell_0(X) = s_1, \mathsf{leak}(X)|\ell_0(X) = s_2) \\ \leq \\ 2\left(p^3 \sum_{k\in\mathbb{F}_p\setminus\{0\}} \sum_{S\subseteq[n]} \left|\widehat{f_S}(k\cdot\ell_0)\right|^2\right)^{1/4},\end{gathered} \tag{5}$$

where X is distributed uniformly over $\mathbb{F}_p^t$.

Proof. Let

$$(*) := \left(\mathsf{SD}(\mathsf{leak}(X)|\ell_0(X) = s_1, \mathsf{leak}(X)|\ell_0(X) = s_2)\right)^2.$$

For X distributed uniformly over $\mathbb{F}_p^t$ and for every $s_1, s_2 \in \mathbb{F}_p$, applying Lemma 2.2, we have that

$$(*) \leq p^2 \cdot \mathop{\mathbb{E}}_{b\leftarrow\mathsf{leak}(X)} \left[\|P(\ell_0(X)|\mathsf{leak}(X) = b) - P(\ell_0(X))\|_2^2\right].$$

For $b \in \{-1,1\}^n$, let $D_b \colon \mathbb{F}_p \to \mathbb{R}$ be $D_b = P(\ell_0(X) | \mathsf{leak}(X) = b)$, that is

$$D_b(k) = \Pr_{X \leftarrow \mathbb{F}_p^t} [\ell_0(X) = k | \mathsf{leak}(X) = b] .$$

Further, recall that ℓ_0 is some nonzero linear function from $\mathbb{F}_p^t$ to $\mathbb{F}_p$, and as such, it satisfies

$$\Pr[\ell_0(X) = k] = 1/p.$$

We immediately deduce that

$$(*) \leq p^2 \cdot \mathop{\mathbb{E}}_{b \leftarrow \mathsf{leak}(X)} \left[\sum_{k \in \mathbb{F}_p} |D_b(k) - 1/p|^2 \right].$$

Observe that for all b,

$$\widehat{D_b}(0) = \mathop{\mathbb{E}}_{k \leftarrow \mathbb{F}_p} [D_b(k)] = \frac{1}{p} \sum_{k \in \mathbb{F}_p} \Pr_{x \leftarrow \mathbb{F}_p^t} [\ell_0(x) = k | \mathsf{leak}(x) = b] = \frac{1}{p} \cdot 1.$$

Therefore, by Parseval's identity,

$$\sum_{k \in \mathbb{F}_p} |D_b(k) - 1/p|^2 = \sum_{k \in \mathbb{F}_p} |D_b(k) - \widehat{D_b}(0)|^2 = p \sum_{k \in \mathbb{F}_p \setminus \{0\}} \left| \widehat{D_b}(k) \right|^2 .$$

Hence,

$$\begin{aligned} (*) &\leq p^3 \cdot \mathop{\mathbb{E}}_{b \leftarrow \mathsf{leak}(X)} \left[\sum_{k \in \mathbb{F}_p \setminus \{0\}} \left| \widehat{D_b}(k) \right|^2 \right] && (6) \\ &= p^3 \cdot \sum_{k \in \mathbb{F}_p \setminus \{0\}} \mathop{\mathbb{E}}_{b \leftarrow \mathsf{leak}(X)} \left[\left| \widehat{D_b}(k) \right|^2 \right] && (7) \end{aligned}$$

For $b \in \{-1,1\}^n$, let A_b be the set of x's with $\mathsf{leak}(x) = b$. Define $\mu(A_b) = |A_b|/p^t$ to be its density. For a set A, we let $\mathbf{1}_A(x)$ be the indicator function that outputs 1 if $x \in A$, and 0 otherwise. Likewise, for an event E, we denote $\mathbf{1}_E$ as the indicator that is 1 if E happens and 0 otherwise. For each $k \in \mathbb{F}_p$, it holds that

$$\begin{aligned}
\widehat{D_b}(k) = \langle D_b, \chi_k \rangle &= \frac{1}{p} \cdot \sum_{z \in \mathbb{F}_p} D_b(z) \cdot \overline{\chi_k(z)} \\
&= \frac{1}{p} \cdot \sum_{z \in \mathbb{F}_p} \Pr_{x \leftarrow \mathbb{F}_p^t} [\ell_0(x) = z | \mathsf{leak}(x) = b] \cdot \overline{\chi_k(z)} \\
&= \frac{1}{p} \cdot \sum_{z \in \mathbb{F}_p} \sum_{x \in \mathbb{F}_p^t} \frac{\mathbf{1}_{x \in A_b}}{\mu(A_b)} \cdot \frac{\mathbf{1}_{\ell_0(x)=z}}{p^t} \cdot \overline{\chi_k(z)} \\
&= \frac{1}{p \cdot \mu(A_b)} \sum_{x \in \mathbb{F}_p^t} \frac{1}{p^t} \cdot \mathbf{1}_{x \in A_b} \sum_{z \in \mathbb{F}_p} \mathbf{1}_{\ell_0(x)=z} \cdot \overline{\chi_k(z)} \\
&= \frac{1}{p \cdot \mu(A_b)} \sum_{x \in \mathbb{F}_p^t} \frac{1}{p^t} \cdot \mathbf{1}_{x \in A_b} \cdot \overline{\chi_k(\ell_0(x))} \\
&= \frac{1}{p \cdot \mu(A_b)} \mathop{\mathbb{E}}_{x \leftarrow \mathbb{F}_p^t} \left[\mathbf{1}_{A_b}(x) \cdot \overline{\chi_k(\ell_0(x))} \right] \\
&= \frac{\widehat{\mathbf{1}_{A_b}}(k \cdot \ell_0)}{p \cdot \mu(A_b)}.
\end{aligned}$$

In order to simplify $\widehat{\mathbf{1}_{A_b}}(k \cdot \ell_0)$, we denote $f_S(x) = \prod_{i \in S} f_i(\ell_i(x))$ and $b^S = \prod_{i \in S} b_i$, as well as $g_b(x) = 2^{-n} \sum_{S \subseteq [n]} \left(b^S \cdot f_S(x) \right)$. We prove $g_b = \mathbf{1}_{A_b}$:

$$\mathbf{1}_{A_b}(x) = \prod_{i=1}^{n} \mathbf{1}_{f_i(\ell_i(x))=b_i} = \prod_{i=1}^{n} \frac{1 + b_i \cdot f_i(\ell_i(x))}{2} = \frac{1}{2^n} \sum_{S \subseteq [n]} = g_b(x).$$

In particular,

$$\widehat{\mathbf{1}_{A_b}}(k \cdot \ell_0) = \widehat{g_b}(k \cdot \ell_0).$$

Plugging it back in (6) we get

$$\begin{aligned}
(*) \leq p^3 \cdot &\sum_{k \in \mathbb{F}_p \setminus \{0\}} \mathop{\mathbb{E}}_{b \leftarrow \mathsf{leak}(X)} \left[\left| \widehat{D_b}(k) \right|^2 \right] \\
&= p \cdot \sum_{k \in \mathbb{F}_p \setminus \{0\}} \mathop{\mathbb{E}}_{b \leftarrow \mathsf{leak}(X)} \left[\left| \frac{\widehat{g_b}(k \cdot \ell_0)}{\mu(A_b)} \right|^2 \right] \\
&= p \cdot \sum_{k \in \mathbb{F}_p \setminus \{0\}} \sum_{\substack{b \in \{-1,1\}^n, \\ \mu(A_b) \neq 0}} \frac{|\widehat{g_b}(k \cdot \ell_0)|^2}{\mu(A_b)},
\end{aligned} \tag{8}$$

where the last equality holds since each $b \in \{-1, 1\}^n$ is attained as $\mathsf{leak}(X)$ with probability $\mu(A_b)$.

To bound the last term on (8), we separately bound the b's with $\mu(A_b) < C/2^n$, and b's with $\mu(A_b) \geq C/2^n$, where $C > 0$ is a parameter that will be optimized later. For the first type of summands, we note that always $|\widehat{g_b}(k \cdot$

$\ell_0)| \leq \mathbb{E}\,|g_b| = \mu(A_b)$, as $\widehat{g_b}(k \cdot \ell_0)$ is a Fourier coefficient of $g_b = \mathbf{1}_{A_b}$. Hence, $|\widehat{g_b}(k \cdot \ell_0)|^2/\mu(A_b)$ is bounded by $\mu(A_b)$. For b's with $\mu(A_b) \geq C/2^n$, we are going to replace $\mu(A_b)$ in the denominator by $C/2^n$.

$$\begin{aligned}
(*) &\leq p \cdot \sum_{k \in \mathbb{F}_p \setminus \{0\}} \sum_{\substack{b \in \{-1,1\}^n, \\ 0 < \mu(A_b) < C/2^n}} \mu(A_b) + p \cdot \sum_{k \in \mathbb{F}_p \setminus \{0\}} \frac{2^n}{C} \cdot \sum_{\substack{b \in \{-1,1\}^n, \\ \mu(A_b) \geq C/2^n}} |\widehat{g_b}(k \cdot \ell_0)|^2 \\
&\leq p^2 \cdot 2^n \cdot \frac{C}{2^n} + p \cdot \frac{\sum_{k \in \mathbb{F}_p \setminus \{0\}} \mathbb{E}_{b \leftarrow \{-1,1\}^n} \left[\left| \sum_{S \subseteq [n]} b^S \cdot \widehat{f_S}(k \cdot \ell_0) \right|^2 \right]}{C} \\
&= p^2 \cdot C + \frac{p \cdot \sum_{k \in \mathbb{F}_p \setminus \{0\}} \sum_{S \subseteq [n]} \left| \widehat{f_S}(k \cdot \ell_0) \right|^2}{C},
\end{aligned} \tag{9}$$

where the last inequality is Parseval's identity for functions over $\{-1,1\}^n$. Optimizing the value of C, we conclude

$$(*) \leq 2 \cdot \sqrt{p^3 \sum_{k \in \mathbb{F}_p \setminus \{0\}} \sum_{S \subseteq [n]} \left| \widehat{f_S}(k \cdot \ell_0) \right|^2},$$

finishing the proof (recall the definition of $(*)$). □

Remark 1 (Multi-bit output leakage). It is possible to extend the statement and analysis of Theorem 3.1 to the setting where each f_i outputs more than 1 bit. (Specifically, the definition of f_S would need to be adjusted). We leave this direction for future research.

4 Leakage Resilience for $t \geq 0.69n$

The main theorem we prove in this section is as follows.

Theorem 4.1. *Let $\ell_0, \ldots, \ell_n \colon \mathbb{F}_p^t \to \mathbb{F}_p$ be $n+1$ linear functions such that every t of them are linearly independent. Let $f_1, \ldots, f_n \colon \mathbb{F}_p \to \{-1,1\}$ be arbitrary functions. Let $f_S(x) = \prod_{i \in S} f_i(\ell_i(x))$. Then, for $t \geq 0.69n$, it holds that*

$$\sum_{k \in \mathbb{F}_p \setminus \{0\}} \sum_{S \subseteq [n]} \left| \widehat{f_S}(k \cdot \ell_0) \right|^2 \leq (p-1) \cdot 2^{-\Omega(n)}.$$

Theorem 4.1 is an implication of the following lemma:

Lemma 4.2. *Let $\ell_0, \ldots, \ell_n \colon \mathbb{F}_p^t \to \mathbb{F}_p$ be $n+1$ linear functions such that every t of them are linearly independent. Let $f_1, \ldots, f_n \colon \mathbb{F}_p \to \{-1,1\}$ be arbitrary functions. If $n \leq 2t$ and $p \geq n$, then*

$$\left| \widehat{f_{[n]}}(\ell_0) \right| \leq O((2/\pi)^{2t-n}). \tag{10}$$

To deduce Theorem 4.1 we plug in the above lemma with $[n]$ replaced by S. That is, because the assumptions of Lemma 4.2 apply to $\{\ell_i\}_{i\in S}$ and $\{f_i\}_{i\in S}$ from Theorem 4.1, we may deduce (10) with $[n]$ replaced by S, that is,

$$\left|\widehat{f_S}(\ell_0)\right| \leq O((2/\pi)^{2t-|S|}).$$

We note that once $|S| < t$ then in fact

$$\widehat{f_S}(\ell_0) = 0,$$

as the Fourier coefficients of f_S are supported on characters corresponding to functionals of the form $\sum_{i\in S} \alpha_i \ell_i$ with $\alpha_i \in \mathbb{F}_p$. However, non of these functionals is being ℓ_0, by assumption.

Proof (Proof of Theorem 4.1). For each $k \in \mathbb{F} \setminus \{0\}$ and $S \subseteq [n]$, we bound $\left|\widehat{f_S}(k \cdot \ell_0)\right|$ separately. Specifically, Lemma 4.2 implies that for every $k \in \mathbb{F} \setminus \{0\}$ and $S \subseteq [n]$, it holds that

$$\left|\widehat{f_S}(k \cdot \ell_0)\right|^2 \leq O\left((2/\pi)^{4t-2|S|}\right). \tag{11}$$

Hence,

$$\begin{aligned}\sum_{S\subseteq[n]} \left|\widehat{f_S}(k \cdot \ell_0)\right|^2 &\leq \sum_{z=0}^{n} \binom{n}{z} \cdot O\left((2/\pi)^{4t-2z}\right)\\ &= O\left((2/\pi)^{4t} \cdot \left((\pi/2)^2 + 1\right)^n\right).\end{aligned}$$

This last term is exponentially small in n as long as t/n is strictly larger than a constant C that we find next. The ratio of t/n in which the bound is $\exp(0\cdot n) = 1$ corresponds to $(2/\pi)^{4t} \cdot ((\pi/2)^2 + 1)^n = 1$, that is

$$4t \log(2/\pi) = -n \left(\log\left((\pi/2)^2 + 1\right)\right)$$

which means that

$$C = \frac{t}{n} = \frac{\log((\pi/2)^2 + 1)}{4\log(\pi/2)} \approx 0.688.$$

Since we assume $t \geq 0.69n$, then

$$\sum_{k\in\mathbb{F}_p\setminus\{0\}} \sum_{S\subseteq[n]} \left(\widehat{f_S}(k \cdot \ell_0)\right)^2 \leq (p-1) \cdot 2^{-\Omega(n)},$$

as required. □

We proceed with the proof of Lemma 4.2.

Notation. Let $g\colon \mathbb{F}_p \to \mathbb{R}$ be a function. We define the max-norm of its Fourier spectrum as

$$\|\widehat{g}\|_\infty := \max_{k \in \mathbb{F}_p} |\widehat{g}(k)|.$$

Lemma 4.3. *Let $t \leq n \leq 2t$ $\ell_0, \dots, \ell_n \colon \mathbb{F}_p^t \to \mathbb{F}_p$ be linear functions, with every t of them being linearly independent. Let $A, B \colon \mathbb{F}_p^{n-t} \to \{-1,1\}$ and $C \colon \mathbb{F}_p^{2t-n} \to \{-1,1\}$ be any functions, write*

$$F(x) = A(\ell_1(x), \dots, \ell_{n-t}(x)) \cdot C(\ell_{n-t+1}(x), \dots, \ell_t(x)) \cdot B(\ell_{t+1}(x), \dots, \ell_n(x)),$$

then

$$|\widehat{F}(\ell_0)| \leq \|A\|_2 \, \|B\|_2 \left\| \widehat{C} \right\|_\infty \tag{12}$$

Corollary 4.4. *Let ℓ_i be as in Lemma 4.3 and let $g_1, \dots, g_n \colon \mathbb{F}_p \to \mathbb{R}$ be arbitrary functions, and set $m = 2n - 2t$, then*

$$|\widehat{g_{[n]}}(\ell_0)| \leq \prod_{i=1}^{m} \|g_i\|_2 \cdot \prod_{i=m+1}^{n} \|\widehat{g_i}\|_\infty . \tag{13}$$

Proof. We get the result by applying Lemma 4.3 with

$$\begin{aligned} A(z_1, \dots, z_{n-t}) &= g_1(z_1) \cdots g_{n-t}(z_{n-t}) \\ B(z_1, \dots, z_{n-t}) &= g_{n-t+1}(z_1) \cdots g_{2n-2t}(z_{n-t}) \\ C(z_1, \dots, z_{2t-n}) &= g_{2n-2t+1}(z_1) \cdots g_n(z_{2t-n}), \end{aligned}$$

Hence $F(x)$ from Lemma 4.3 is $g_{[n]}$. Moreover, note that ranging over the entire input space of A, the inputs to g_i in the definition of A are independent of each other (likewise for B and C). This implies that we have

$$\|A\|_2 = \prod_{i=1}^{n-t} \|g_i\|_2 , \quad \|C\|_\infty = \prod_{i=n-t+1}^{t} \|g_i\|_\infty , \quad \|B\|_2 = \prod_{i=t+1}^{n} \|g_i\|_2 ,$$

which completes the proof. To see that indeed the inputs of the g_i's are independent random variables, recall that $n - t \leq t$ (likewise $2t - n \leq t$), and the assumption that any t of the ℓ_i's are linearly independent. □

Corollary 4.4 is insufficient for proving Lemma 4.2. It may give a poor upper bound of 1 when, say, $g_i \equiv 1$. Combining this lemma with the following claim, we can strengthen this estimate and deduce Lemma 4.2.

Claim 4.5 *Let $f\colon \mathbb{F}_p \to [-1,1]$ where $\mathbb{E}[f] = \mu$. Then, for all $k \neq 0$ we have*

$$|\widehat{f}(k)| \leq \frac{2}{\pi} \cos\left(\frac{\pi}{2}\mu\right) + O(1/p^2). \tag{14}$$

For completeness we give the proof of the above claim in Appendix A.

At this point the essence of the proof of Lemma 4.2 is already available. Corollary 4.4 bounds the Fourier coefficient $\widehat{g}_{[n]}(\ell_0)$ with a product of $2t-n$ Fourier coefficients of g_i. In case that $|\mathbb{E}[g_i]| \leq 2/\pi$, Claim 4.5 gives that actually $\|\widehat{g_i}\| \lesssim 2/\pi$, which gives the required $|\widehat{g}_{[n]}(\ell_0)| \leq (2/\pi)^{2t-n}$. Hence, the following proof focuses on extending this to the case where some of the g_i's have $|\mathbb{E}[g_i]| > 2/\pi$.

Proof (Proof of Lemma 4.2). For the proof, we go through the following generalization of Corollary 4.4.

Let n, t, m, g_i, ℓ_i be exactly as in Corollary 4.4. If additionally $M \geq m = 2n - 2t$ satisfies that $|g_i| \leq 1$ for $i = 1 \dots M$ and $\|g_i\|_2 \leq 1$ for $i = M+1 \dots n$, then

$$|\widehat{g_{[n]}}(\ell_0)| \leq (2/\pi)^{M-m} \prod_{i=M+1}^{n} \|\widehat{g_i}\|_\infty . \tag{15}$$

We note that Eq. (15) interpolates between Corollary 4.4 ($M = m$) which we will prove later, and Lemma 4.2 ($M = n$) which is what we are trying to prove. The proof is by induction on M.

A minor detail that we omit is that the $2/\pi$ in Eq. (15) should be replaced by $2/\pi + O(1/p^2)$, where the error term stems from Eq. (14). Since we raise $2/\pi + O(1/p^2)$ to a power smaller than n, the ratio between the bounds we state, and the actual bounds we get is $1 + O(n/p^2)$. Though, as we assume $p \geq n$, the overall effect of this error term translates to a $1 + O(1/n)$ multiplicative factor appearing in the bound in Eq. (10).

Base case. The $M = m$ case of Eq. (15) is already covered in Corollary 4.4.

Induction step. To prove Eq. (15) for some values of n, t, M (with $M > 2n - 2t$), we suppose it holds whenever M is replaced by smaller values (maybe with different n, t).

In the case where $\|\widehat{g_M}\|_\infty \leq 2/\pi + O(1/p^2)$ we immediately deduce Eq. (15) by applying it with $M' = M - 1$ (and same n, t).

In the case where $\|\widehat{g_M}\|_\infty \geq 2/\pi$, we first deduce that $\mu := \mathbb{E}[g_M]$ satisfies $|\mu| > 2/\pi$, as Eq. (14) shows that regardless of the value of μ, we have all other Fourier coefficients of g_M smaller than $2/\pi$ (note that $|g_M| \leq 1$ by assumption). Plugging in

$$2/\pi \leq |\mu| \leq 1 \tag{16}$$

we see $g := g_M - \mu$ satisfies $\|\widehat{g}\|_\infty \leq \frac{2}{\pi}\cos(\frac{\pi}{2}\mu)$.

The decomposition $g_M = \mu + g$ translates to

$$\widehat{g_{[n]}}(\ell_0) = \mu\widehat{(g_{[n]\setminus\{M\}})}(\ell_0) + \widehat{(g \cdot g_{[n]\setminus\{M\}})}(\ell_0). \tag{17}$$

We henceforth bound each of the summands in Eq. (17) using the induction hypothesis, and deduce Eq. (15).

The bound on $\widehat{g_{[n]\setminus M} \cdot \mu}(\ell_0)$ is obtained by applying Eq. (15) with $(n', t', M') = (n-1, t, M-1)$ (note that $M' \geq 2n' - 2t'$ by the assumption $M > 2n - 2t$):

$$\begin{aligned} |\widehat{g_{[n]\setminus M} \cdot \mu}(\ell_0)| &\leq |\mu|(2/\pi)^{M'-(2n'-2t')} \prod_{i=M+1}^{n} \|\widehat{g_i}\|_\infty \\ &= |\mu|(2/\pi)^{M-m+1} \prod_{i=M+1}^{n} \|\widehat{g_i}\|_\infty . \end{aligned} \tag{18}$$

The bound on $\widehat{g_{[n]\setminus M} \cdot g}(\ell_0)$ is obtained by applying Eq. (15) with $(n'', t'', M'') = (n, t, M-1)$:

$$\begin{aligned} |\widehat{g_{[n]\setminus M} \cdot g}(\ell_0)| &\leq (2/\pi)^{M''-(2n''-2t'')} \|\widehat{g}\|_\infty \prod_{i=M+1}^{n} \|\widehat{g_i}\|_\infty \\ &= (2/\pi)^{M-m-1} \|\widehat{g}\|_\infty \prod_{i=M+1}^{n} \|\widehat{g_i}\|_\infty . \end{aligned} \tag{19}$$

Note that while $|g_M| \leq 1$ it is not necessary that $|g| \leq 1$. However, the application of Eq. (15) is valid as $\|g\|_2 \leq \|g_M\|_2 \leq 1$.

In order to combine the two estimates in Eqs. (18) and (19), and conclude with Eq. (15) we must show

$$\begin{aligned} |\mu|(2/\pi)^{M-m+1} \prod_{i=M+1}^{n} \|\widehat{g_i}\|_\infty + (2/\pi)^{M-m-1} \|\widehat{g}\|_\infty \prod_{i=M+1}^{n} \|\widehat{g_i}\|_\infty \\ \leq (2/\pi)^{M-m} \prod_{i=M+1}^{n} \|\widehat{g_i}\|_\infty . \end{aligned}$$

Dividing by the common factor $2^{M-m} \prod_{i=M+1}^{n} \|\widehat{g_i}\|_\infty$, our task boils down to verifying

$$\frac{2}{\pi}|\mu| + \frac{\pi}{2} \|\widehat{g}\|_\infty \leq 1.$$

Recall $\|\widehat{g}\|_\infty \leq \frac{2}{\pi}\cos(\frac{\pi}{2}\mu)$, so we only need to check

$$\frac{2}{\pi}|\mu| + \cos(\frac{\pi}{2}\mu) \leq 1.$$

This inequality is not true in general (witnessed by $\mu = \pm 1/4$), but in the present case $2/\pi \leq |\mu| \leq 1$ it does hold. To see that, notice $\cos(\frac{\pi}{2}\mu) = \sin(\frac{\pi}{2}(1-|\mu|)) \leq \frac{\pi}{2}(1-|\mu|)$, hence it is sufficient to check that

$$\frac{2}{\pi}|\mu| + \frac{\pi}{2} - \frac{\pi}{2}|\mu| \leq 1.$$

In the range of Eq. (16), this inequality is most tight at $|\mu| = \frac{2}{\pi}$, where it reads

$$0.98 \approx (\frac{2}{\pi} - \frac{\pi}{2})\frac{2}{\pi} + \frac{\pi}{2} \leq 1,$$

completing the proof. □

Proof (Proof of Lemma 4.3). Set

$$\begin{aligned} I &= \{1, \dots, n-t\}, \\ K &= \{n-t+1, \dots, t\}, \\ J &= \{t+1, \dots, n\}, \end{aligned}$$

and denote

$$A'(x) = A((\ell_i(x))_{i \in I}), \quad B'(x) = B((\ell_j(x))_{j \in J}), \quad C'(x) = C((\ell_k(x))_{k \in K})$$

As we are required in Eq. (12) to bound $|\widehat{(A' \cdot B' \cdot C')}(\ell_0)|$, we present

$$\widehat{(A' \cdot B' \cdot C')}(\ell_0) = \sum_{\alpha+\beta+\gamma=\ell_0} \widehat{A'}(\alpha)\widehat{B'}(\beta)\widehat{C'}(\gamma), \tag{20}$$

where $\alpha, \beta, \gamma \in \mathbb{F}_p^t$ correspond to Fourier characters.

Note that $\widehat{A'}(\alpha)$ may be nonzero only when $\alpha \in \operatorname{span}\{\ell_i \colon i \in I\}$. This is because the Fourier expansion of a product, is the convolution of Fourier expansions, so that

$$\widehat{A'}(\alpha) = \sum_{\substack{a_i \in \mathbb{F}_p \\ \sum_{i \in I} a_i \ell_i = \alpha}} \prod_{i \in I} \widehat{g_i}(a_i).$$

The analogous claims hold also to $\widehat{B'}(\beta)$ and to $\widehat{C'}(\gamma)$. Hence, for $\widehat{B'}(\beta)\widehat{C'}(\gamma)$ to be non-zero we must have $\beta + \gamma \in \operatorname{span}\{\ell_i \colon i \in J \cup K\}$. Since $|J \cup K| = t$, $\{\ell_i\}_{i \in J \cup K}$ are linearly independent, and so every α may have at most one pair of (β, γ) with $\alpha + \beta + \gamma = \ell_0$ and $\widehat{B'}(\beta)\widehat{C'}(\gamma) \neq 0$.

Since each of α and β appear at most once in any nonzero term of the sum in Eq. (20), we may find a matching $\alpha \sim \beta$, so that if α (or β) appears in a nonzero term, it must be the term indexed by $(\alpha, \beta, \ell_0 - \alpha - \beta)$. Hence, we may rewrite Eq. (20) as

$$A' \cdot B' \cdot C' = \sum_{\alpha \sim \beta} \widehat{A'}(\alpha)\widehat{B'}(\beta)\widehat{C'}(\ell_0 - \alpha - \beta).$$

We bound the $\widehat{C'}(\ell_0 - \alpha - \beta)$ term in the last equation by $\left\|\widehat{C'}\right\|_\infty$. Note that C depends on $\leq t$ indpendent variables $\{\ell_i(x)\}_{i \in K}$ and hence $\left\|\widehat{C'}\right\|_\infty = \left\|\widehat{C}\right\|_\infty$.

Hence,

$$\left|\widehat{(A' \cdot B' \cdot C')}(\ell_0)\right| \leq \sum_{\alpha \sim \beta} |\widehat{A'}(\alpha)||\widehat{B'}(\beta)| \cdot \|C'\|_\infty .$$

Therefore, it is sufficient to show that

$$\sum_{\alpha \sim \beta} |\widehat{A'}(\alpha)||\widehat{B'}(\beta)| \leq \|A\|_2 \cdot \|B\|_2 . \tag{21}$$

Cauchy-Schwarz inequality shows that

$$\sum_{\alpha\sim\beta} |\widehat{A'}(\alpha)||\widehat{B'}(\beta)| \leq \sqrt{\sum_{\alpha} |\widehat{A'}(\alpha)|^2} \cdot \sqrt{\sum_{\beta} |\widehat{B'}(\beta)|^2}.$$

Notice that we used that each of α and β appears exactly once in the sum. Plugging in Parseval's identity, we find

$$\sum_{\alpha\sim\beta} |\widehat{A'}(\alpha)||\widehat{B'}(\beta)| \leq \|A'\|_2 \|B'\|_2 .$$

However, since each t of the ℓ_i's are independent, and both A and B depend on $n-t \leq t$ variables, we have $\|A'\|_2 = \|A\|$ as well as $\|B'\|_2 = \|B\|$. Hence we deduce Eq. (21), as required. □

5 Balanced Leakage Resilience for $t \geq 0.58n$

It is intuitive that in order for an attacker to leak the most information from the shares, they should leak the most from each share, that is choose functions $f_i \colon \mathbb{F}_p \to \{-1,1\}$ which are unbiased, that is $\Pr[f_i = 1] \approx 1/2$.

We do not know to formalize this intuition. All the more so, we show security in broader range of parameters when the functions are unbiased. We believe this 'unbiased' regime is instructive – first because almost all functions are unbiased, and second because our proxy Theorem 3.1 may (conceivably) be improved in the biased regime. Meanwhile, in the unbiased case, we expect even the most deleterious part in Theorem 3.1, that is (9), to be quite tight.

The main theorem we prove in this section is as follows.

Theorem 5.1. *Let $\ell_0, \dots, \ell_n \colon \mathbb{F}_p^t \to \mathbb{F}_p$ be $n+1$ linear functions such that every t of them are linearly independent. Let $C > 0$ and let $f_1, \dots, f_n \colon \mathbb{F}_p \to \mathbb{R}$ be functions satisfying*

- $\|f_i\|_2 \leq 1$,
- $\left\|\widehat{f_i}\right\|_\infty \leq \frac{2}{\pi} + O(1/p^2)$,
- $|\mathbb{E}[f_i]| \leq C$.

If $n \leq p$, then

$$\sum_{S\subseteq[n]} \left|\widehat{f_S}(\ell_0)\right|^2 \leq (1+\pi^2/4)^{n-t} e^{1.5Cn} \left(\frac{2}{\pi} + O\left(\frac{1}{p^2}\right)\right)^{2t}. \tag{22}$$

Corollary 5.2. *Let ℓ_i be as in Theorem 5.1 and let $f_1, \dots, f_n \colon \mathbb{F}_p \to \{-1,1\}$ be functions satisfying $|\mathbb{E}[f_i]| \leq 1/1000$. Then, for $t \geq 0.58n$, it holds that*

$$\sum_{k\in\mathbb{F}\setminus\{0\}} \sum_{S\subseteq[n]} \left|\widehat{f_S}(k\cdot\ell_0)\right|^2 \leq O(p)\cdot 2^{-\Omega(n)}. \tag{23}$$

Proof. The functions f_i satisfy the requirements in Theorem 5.1 by Claim 4.5, with $C = 1/1000$.

The bound (22) is exponentially small in n so long as

$$-(2t\log(2/\pi) + (n-t)\log(1+\pi^2/4) + 1.5Cn) \geq \Omega(n),$$

that is

$$t/n > \frac{\log(1+\pi^2/4) + 1.5C}{2\log(\pi/2) + \log(1+\pi^2/4)} \approx 0.57995.$$

As usual we omitted the $O(1/p^2)$ term, which contributes a $1 + O(n/p^2)$ multiplicative factor. Since we assume $t/n \geq 0.58$ the bound (22) is exponentially small in n.

Finally, ℓ_0 may be replaced by $k \cdot \ell_0$ for any $k \neq 0$, thus yielding the $O(p)$ factor in the right hand side of Eq. (23). □

In the proof, we use the following variant of the Pythagorean theorem:

Lemma 5.3. *Let $v = \sum_i v_i$ be a vector such that $\langle v_i, v_j\rangle = 0$ whenever $i \neq j$. Further let $\{u_j\}$ be a set of vectors satisfying $\langle v_i, u_j\rangle = 0$ whenever $i \neq j$. Further assume that $|\langle v_i, u_i\rangle| \leq \beta \|v_i\|$, then*

$$\sum_j |\langle v, u_j\rangle|^2 \leq \beta^2 \|v\|^2 . \tag{24}$$

Proof (Proof of Lemma 5.3). By direct calculation:

$$\begin{aligned}\sum_j |\langle v, u_j\rangle|^2 &= \sum_j |\langle \sum_i v_i, u_j\rangle|^2 = \sum_j |\langle v_j, u_j\rangle|^2 \\ &\leq \sum_j \beta^2 \|v_j\|^2 = \beta^2 \|v\|^2 ,\end{aligned}$$

where the last equality is the Pythagorean theorem. □

We demonstrate the core of the proof of Theorem 5.1, by restricting ourselves to the case $\mathbb{E}[f_i] = 0$. Later, we will reduce to this case.

Lemma 5.4. *Theorem 5.1 holds if $C = 0$, that is, if $\mathbb{E}[f_i] = 0$ for all $i = 1 \ldots n$.*

Proof (Proof of Lemma 5.4). Let $I \subseteq [n-t]$. We will later show that Lemma 5.3 implies the following inequality:

$$\sum_{H \subseteq [n]\setminus[n-t]} |\widehat{f_{I\cup H}}(\ell_0)|^2 \leq \left(\frac{2}{\pi} + O(1/p^2)\right)^{2(t-|I|)} . \tag{25}$$

Using Eq. (25), we obtain

$$\begin{aligned}\sum_{S\subseteq[n]}\left|\widehat{f_S}(\ell_0)\right|^2 &= \sum_{I\subseteq[n-t]}\ \sum_{H\subseteq[n]\setminus[n-t]}\left|\widehat{f_{I\cup H}}(\ell_0)\right|^2\\ &\le \sum_{I\subseteq[n-t]}\left(\frac{2}{\pi}\right)^{2(t-|I|)}\cdot(1+O(1/p^2))^n\\ &= O\left(\sum_{i=0}^{n-t}\binom{n-t}{i}\left(\frac{2}{\pi}\right)^{2(t-i)}\right)\\ &= O\left(\left(\frac{2}{\pi}\right)^{2t}(1+\pi^2/4)^{n-t}\right).\end{aligned}$$

To derive Eq. (25), we consider the vector space of functions $\mathbb{F}_p^t\to\mathbb{C}$ associated with the inner product $\langle f,g\rangle=\mathbb{E}[f\bar{g}]$. Let

$$u_J(x)=f_J(x)\cdot\chi_{\ell_0}(x)=f_J(x)\cdot\exp\left(\frac{2\pi\iota\ell_0(x)}{p}\right)$$

for $J\subseteq[n]\setminus[n-t]$. Note that $\widehat{f\cdot f_H}(\ell_0)=\langle f,u_H\rangle$, and in particular

$$|\widehat{f_{I\cup H}}(\ell_0)|^2=|\langle f_I,u_H\rangle|^2, \tag{26}$$

hence the bound from Eq. (24) is relevant for proving Eq. (25).

Let $v:=f_I$, we apply Lemma 5.3 with v,u_J and with $\beta=\left(\frac{2}{\pi}+O(1/p^2)\right)^{t-|I|}$. For this we need to decompose $v=\sum_J v_J$ so that $\langle v_J,v_{J'}\rangle=0$ whenever $J\neq J'$.

Since $\ell_{n-t+1},\dots,\ell_n$ are linearly independent, each linear function $\alpha\colon\mathbb{F}_p^t\to\mathbb{F}_p$ can uniquely be written as $\alpha=\ell_0+\sum_{i=n-t+1}^n\alpha_i\ell_i$. We denote the *dual-support* by

$$\operatorname{supp}^*(\alpha)=\{i\in[n]\setminus[n-t]\colon\alpha_i\neq0\}.$$

For $J\subseteq[n]\setminus[n-t]$ we write

$$v_J=\sum_{\alpha\colon\operatorname{supp}^*(\alpha)=J}\widehat{v}(\alpha)\chi_\alpha.$$

Since $\ell_{n-t+1},\dots,\ell_n$ is a basis of linear functions, we have $v=\sum_J v_J$, as every linear function has some dual-support. Moreover, two distinct v_J's are orthogonal, because their Fourier spectrum are disjoint. Moreover, $\langle v_{J'},u_J\rangle\neq0$ only if $J'=J$. To see this, note the the Fourier-spectrum of $u_J=f_J$ is contained in $\ell_0+\sum_{j\in J}(\mathbb{F}_p\setminus\{0\})\ell_j$. This is the crucial place in which this proof requires that $\mathbb{E}[f_j]=0$ (for all $j\in[n]\setminus[n-t]$). This fact implies that the Fourier spectrum of $v_{J'}$ and u_J can intersect only if $J=J'$.

Finally, to apply Lemma 5.3 we need to verify

$$|\langle v_J,u_J\rangle|\le\beta\left\|v_J\right\|, \tag{27}$$

with $\beta = (2/\pi + O(1/p^2))^{t-|I|}$.

First, recall Eq. (26) that $\langle v_J, u_J \rangle = \widehat{v_J \cdot f_J}(\ell_0)$; hence we must bound $\widehat{v_J \cdot f_J}(\ell_0)$. Recall further that v_J constitutes only from a part of the Fourier decomposition of $v = f_I$. Since v depends only on $\{\ell_i(x)\}_{i \in I}$, also v_J is a function of these variables.

We split the proof of Eq. (27) into two cases.

Case $|J| < t - |I|$. Since $|I \cup J| < t$, $\{\ell_i\}_{i \in I \cup J \cup \{0\}}$ are linearly independent, therefore there is no vanishing linear combination of ℓ_i, $i \in I \cup J$, and the Fourier spectrum of $v = f_I$ is disjoint from that of u_J, hence $v_J = 0$ and in particular

$$|\langle v_J, u_J \rangle| = 0 \leq \beta \, \|v_J\| \, .$$

Case $|J| > t - |I|$. In this case, we use Lemma 4.3 with the linear functions $\{\ell_i\}_{i \in \{0\} \cup I \cup J}$, namely $n' = |I| + |J|$ in that lemma. Specifically, we set $A((\ell_i)_{i \in I}) := v_J$. We arbitrarily split the product $u_J = \chi_{\ell_0}(x) \cdot \prod_{j \in J} f_j(\ell_j(x))$ and the associated linear functions between B and C, with B depending on $n' - t$ variables, and C on $2t - n'$. We get

$$|\langle v_J, u_J \rangle| = |\widehat{\overline{v_J} \cdot f_J}(\ell_0)| \leq \|A\|_2 \, \|B\|_2 \left\| \widehat{C} \right\|_\infty .$$

Note that $\|A\|_2 = \|v_J\|$ as well as $\|B\| \leq 1$ (recall the assumption $\|f_i\|_2 \leq 1$). For $\left\| \widehat{C} \right\|_\infty$, we note that C is a product of $2t - n'$ functions. Since we assume $n' = |I| + |J| \geq t$, C is a product of at most t functions. Using again that every t ℓ_i's are linearly independent, and that $\mathbb{E}[f_i] = 0$, every Fourier coefficient of C is a product of $2t - n'$ Fourier coefficients of the corresponding f_i's. As $2t - n' = 2t - (|I| + |J|) \geq 2t - (|I| + t) = t - |I|$ functions with $\mathbb{E}[f_i] = 0$. Hence we have through Claim 4.5,

$$\left\| \widehat{C} \right\|_\infty \leq \left(2/\pi + O(1/p^2)\right)^{t-|I|} .$$

We summarize

$$|\widehat{\overline{v_J} \cdot f_J}(\ell_0)| \leq \left(\frac{2}{\pi} + O(1/p^2) \right)^{t-|I|} \|v_J\| \, ,$$

which proves Eq. (27), and concludes the proof. □

For the proof of Theorem 5.1 we need the following simple lemma, which, roughly speaking, reduces our attention to unbiased functions.

Definition 5. *Let $\ell_0, \ldots, \ell_n \colon \mathbb{F}_p^t \to \mathbb{F}_p$ be $n+1$ linear functions. For functions $f_1, \ldots, f_n \colon \mathbb{F}_p \to \mathbb{R}$ define*

$$B(f_1, \ldots, f_n) := \sum_{S \subseteq [n]} \left| \widehat{f_S}(\ell_0) \right|^2 .$$

Lemma 5.6. *Let ℓ_i and f_i be as in Definition 5. If $\mu := \mathbb{E}[f_1]$, then*

$$B(f_1, f_2, \ldots, f_n) \leq (1 + |\mu| + \mu^2) B(f_1 - \mu, f_2, \ldots, f_n). \tag{28}$$

Note that B does not depend on the order of the f_i's, given that ℓ_i are ordered accordingly. Hence the index 1 is not special in Eq. (28).

Proof. Write $f'_i = f_i$ except when $i = 1$ in which case $f'_1 = f_1 - \mu$.

$$\begin{aligned} B(f_1, \ldots, f_n) &= \sum_{S \subseteq [n]} \left| \widehat{f_S}(\ell_0) \right|^2 \\ &= \sum_{1 \notin S} \left| \widehat{f_S}(\ell_0) \right|^2 + \sum_{1 \in S} \left| \widehat{f_S}(\ell_0) \right|^2 \qquad (29) \\ &= \sum_{1 \notin S} \left| \widehat{f'_S}(\ell_0) \right|^2 + \sum_{1 \in S} \left| \widehat{f'_S}(\ell_0) + \mu \widehat{f'_{S \setminus \{1\}}}(\ell_0) \right|^2 . \end{aligned}$$

Note the final term has the form $|a + \mu b|^2$. It can be bounded as

$$|a + \mu b|^2 = |a|^2 + \mu^2 |b|^2 + 2\mu \mathrm{Re}(ab) \leq (1 + |\mu|)|a|^2 + (|\mu| + \mu^2)|b|^2.$$

Plugging it back in Eq. (29), we get

$$\begin{aligned} B(f_1, \ldots, f_n) &\leq \sum_{1 \notin S} \left| \widehat{f'_S}(\ell_0) \right|^2 + (1 + |\mu|) \sum_{1 \in S} \left| \widehat{f'_S}(\ell_0) \right|^2 + (|\mu| + \mu^2) \sum_{1 \notin S} \left| \widehat{f'_S}(\ell_0) \right|^2 \\ &= (1 + |\mu| + \mu^2) \sum_{1 \notin S} \left| \widehat{f'_S}(\ell_0) \right|^2 + (1 + |\mu|) \sum_{1 \in S} \left| \widehat{f'_S}(\ell_0) \right|^2 \\ &\leq (1 + |\mu| + \mu^2) B(f'_1, \ldots, f'_n). \end{aligned}$$

□

Proof (Proof of Theorem 5.1). Given $f_1, \ldots, f_n$, we will show that

$$B(f_1, \ldots, f_n) \leq (1 + \pi^2/4)^{n-t} e^{1.5Cn} \left(\frac{2}{\pi} + O\left(\frac{1}{p^2} \right) \right)^{2t} .$$

Using Lemma 5.6 repeatedly, we get that

$$B(f_1, \ldots, f_n) \leq B(f_1 - \mu_1, \ldots, f_n - \mu_n) \cdot \prod_{i=1}^{n} (1 + |\mu_i| + \mu_i^2),$$

with $\mu_i := \mathbb{E}[f_i]$. Note that $(1 + |\mu_i| + \mu_i^2) \leq \exp(1.5|\mu_i|)$, and because we assume $|\mu_i| \leq C$ we get

$$B(f_1, \ldots, f_n) \leq e^{1.5Cn} B(f_1 - \mu_1, \ldots, f_n - \mu_n). \qquad (30)$$

Note that the functions $f_1 - \mu_1, \ldots, f_n - \mu_n$ satisfy the requirements of Lemma 5.4. Hence,

$$B(f_1 - \mu_1, \ldots, f_n - \mu_n) \leq (1 + \pi^2/4)^{n-t} \left(\frac{2}{\pi} + O\left(\frac{1}{p^2} \right) \right)^{2t} . \qquad (31)$$

The combination of Eq. (30) and Eq. (31) concludes the proof. □

6 Unbalanced Leakage Resilience for $t \geq 0.01n$

Contrast to the previous section, if the leakage functions are sufficiently biased, then the security of the scheme applies to an even broader regime of parameters Recall that we define $B(f_1, \ldots, f_n) := \sum_{S \subseteq [n]} \widehat{f_S}(\ell_0)^2$.

Theorem 6.1. *Let $\ell_0, \ldots, \ell_n \colon \mathbb{F}_p^t \to \mathbb{F}_p$ be $n+1$ linear functions such that every t of them are linearly independent. Let $C > 0$ and let $f_1, \ldots, f_n \colon \mathbb{F}_p \to \{-1, 1\}$ be functions satisfying*

$$|\mathbb{E}[f_i]| \geq C \qquad \textit{for } i = 1 \ldots n.$$

Then,

$$B(f_1, \ldots, f_n) \leq 15^n \cdot \left(\frac{1 - C^2}{5}\right)^t. \tag{32}$$

Corollary 6.2. *In the setting of Theorem 6.1, if $|\mathbb{E}[f_i]| \geq 1 - 2/15^{n/t}$, then $B(f_1, \ldots, f_n) \leq (4/5)^t$, and consequently the advantage of an adversary to guess the secret is exponentially small given the leakage, assuming $p = 2^{o(n)}$.*

Proof. Setting $C = 1 - \alpha$ (for α defined below) in Theorem 6.1 we have

$$B(f_1, \ldots, f_n) \leq \left(15 \cdot \left(\frac{1 - C^2}{5}\right)^{t/n}\right)^n \leq \left(15 \cdot (2\alpha/5)^{t/n}\right)^n.$$

This bound is exponentially small in n as long as $\alpha < \frac{5}{2 \cdot 15^{n/t}}$. Hence, $\alpha = 2/15^{n/t}$ is sufficient. The result follows from Theorem 3.1. □

Example 3. Shamir's secret sharing scheme with $n \leq 100t$ and $p = 2^{o(n)}$ is resilient against binary leakage functions that each of them discloses at most $H(1/15^{100})$ bits of information (corresponding to $|\mathbb{E}[f_i]| \geq 1 - 2/15^{100}$). Here, $H(q) = -q \log_2(q) - (1-q)\log_2(1-q)$.

Proof (Proof of Theorem 6.1). Let $\mu_i := \mathbb{E}[f_i]$. Note that $|\mu_i| \leq 1$, hence repeated applications of Lemma 5.6 yield that

$$B(f_1, \ldots, f_n) \leq 3^n B(f_1 - \mu_i, \ldots, f_n - \mu_n). \tag{33}$$

Hence, we restrict our attention to bounding $B(g_1, \ldots, g_n) = \sum_{S \subseteq [n]} \widehat{g_S}(\ell_0)^2$ with $g_i = f_i - \mu_i$.

Recall the definition

$$\widehat{g_S}(\ell_0) = \mathop{\mathbb{E}}_x \left[\prod_{j \in S} g_j(x) \cdot \exp\left(\frac{-2\pi\iota\ell_0(x)}{p}\right)\right].$$

If $|S| < t$, the fact that ℓ_0 is not a linear combination of less that t of the other linear functions implies $\widehat{g_S}(\ell_0) = 0$, hence we consider $|S| \geq t$.

Splitting an S with $|S| \geq t$ as $S = U \sqcup V$ with $|U| = t$, the Cauchy-Schwarz inequality implies $|\widehat{g_S}(\ell_0)| \leq \|g_U\|_2 \|g_V\|_2$:

$$|\widehat{g_S}(\ell_0)| = |\langle g_U g_V, \chi_{\ell_0}\rangle| = |\langle g_U, \overline{g_V}\chi_{\ell_0}\rangle| \leq \|g_U\|_2 \left\|\overline{g_V} \cdot \chi_{\ell_0}\right\|_2 = \|g_U\|_2 \|g_V\|_2 .$$

In order to bound $\|g_V\|_2$, note that $\|g_i\|_\infty \leq \|f_i\|_\infty + |\mu_i| \leq 2$, hence

$$\|g_V\|_2 \leq \|g_V\|_\infty \leq 2^{|V|}.$$

In order to bound $\|g_U\|_2$, note that $\{\ell_i\}_{i\in U}$ are independent linear functions, hence

$$\|g_U\|_2 = \prod_{i\in U} \|g_i\|_2 .$$

However, Parseval's identity implies that

$$\|g_i\|_2^2 = \mathbb{E}[f_i^2] - \mathbb{E}[f_i]^2 \leq 1 - C^2,$$

and hence

$$\|g_U\|_2 \leq (1 - C^2)^{t/2}.$$

We deduce that $g_S(\ell_0)^2 \leq 2^{2(|S|-t)}(1 - C^2)^t$, and overall

$$B(g_1, \dots, g_n) \leq \sum_{k=0}^{n} \binom{n}{k} 2^{2(k-t)}(1 - C^2)^t \leq (1 - C^2)^t \cdot 5^{n-t}.$$

Combining with Eq. (33), we conclude with

$$B(f_1, \dots, f_n) \leq 15^n \cdot \left(\frac{1 - C^2}{5}\right)^t .$$

□

6.1 A Barrier of Previous Methods

It is already known that previous methods cannot prove local leakage resilience of Shamir's scheme for any $t \leq n/2$ for general leakage functions. Indeed, [28] showed a particular leakage function for which a proxy quantity in their analysis becomes too large. The leakage function is the quadratic-residue function. This leakage function is balanced and therefore cannot be used to claim that previous techniques cannot be used to derive a result similar to what we get in Example 3. We show an unbalanced variant of the quadratic-residue function for which a similar barrier for previous techniques can be shown. We refer to Appendix B for details.

A Proof of Claim 4.5

Let $f\colon \mathbb{F}_p \to [-1,1]$ have $\mathbb{E}[f] = \mu$. Then, for all $k \neq 0$, we must show that

$$|\widehat{f}(k)| \leq \frac{2}{\pi}\cos\left(\frac{\pi}{2}\mu\right) + O(1/p^2). \tag{34}$$

Note $\widehat{f}(k)$ is a complex number, which we write as $\widehat{f}(k) = |\widehat{f}(k)| \cdot e^{i\theta}$ with $\theta \in [-\pi,\pi]$ and $|\widehat{f}(k)| \geq 0$ a positive real number. It is sufficient we prove

$$e^{-i\theta}\widehat{f}(k) = |\widehat{f}(k)| \leq \frac{2}{\pi}\cos\left(\frac{\pi}{2}\mu\right) + O(1/p^2).$$

Note that

$$\begin{aligned} e^{-i\theta}\widehat{f}(k) &= \mathrm{Re}(e^{-i\theta}\widehat{f}(k)) = \mathrm{Re}(e^{-i\theta}\mathop{\mathbb{E}}_{x\sim\mathbb{F}_p}[f(x)\exp(-2\pi kxi/p)]) \\ &= \mathop{\mathbb{E}}_{x\sim\mathbb{F}_p}[f(x)\mathrm{Re}(\exp(-(2\pi kx/p+\theta)i))] = \mathop{\mathbb{E}}_{x\sim\mathbb{F}_p}[f(x)\cos(2\pi kx/p+\theta)] \\ &= \mathop{\mathbb{E}}_{x\sim\mathbb{F}_p}[f(x/k)\cos(2\pi x/p+\theta)] \end{aligned}$$

We define the function $g\colon \mathbb{F}_p \to [-1,1]$ having $g(x) = f(x/k)$ which satisfies $\mathbb{E}[g] = \mathbb{E}[f] = \mu$ and

$$e^{-i\theta}\widehat{f}(k) = \underbrace{\mathop{\mathbb{E}}_{x\sim\mathbb{F}_p}[g(x)\cos(2\pi x/p+\theta)]}_{F(g)} \tag{35}$$

We now find a function g that maximizes $F(g)$ among functions satisfying $\mathbb{E}[g] = \mu$, and show this value is upper bounded by the right hand side of (34).

Intuitively, a g that maximizes $F(g)$ "should" have $g(x)$ larger as $\cos(2\pi x/p+\theta)$ is larger (among $x \in \{0,1,\ldots,p-1\}$) and smaller when $\cos(2\pi x/p+\theta)$ is smaller. This intuition can be formalized as follows. Write $P(x) := \cos(2\pi x/p+\theta)$. If $P(y) \leq P(z)$ and both $-1 < g(y)$ and $g(z) < 1$, we may outflow a small quantity from $g(y)$ (thus decreasing it) while increasing $g(z)$, so that both $\mathbb{E}[g]$ is preserved and (35) grows. Specifically, letting $\nu = \min\{g(y)+1, 1-g(z)\}$ and defining $g'\colon \mathbb{F}_p \to [-1,1]$ as

$$g'(x) = g(x) + \nu(\mathbf{1}_{\{x=z\}} - \mathbf{1}_{\{x=y\}}),$$

has $|g'| \leq 1$ and $\mathbb{E}[g'] = \mathbb{E}[g] = \mu$ and

$$F(g',\theta) = F(g) + \nu(P(z) - P(y)) > F(g).$$

Hence, for all $\mu \in [-1,1]$ there is a function g_μ which maximizes $F(g_\mu,\theta)$ under the condition $\mathbb{E}[g_\mu] = \mu$, that has $|g(x)| = 1$ for all points $x \in \mathbb{F}_p$, except for at most one point x'. Moreover, $g_\mu(x)$ is monotonically non-decreasing in $P(x)$. We must show

$$F(g_\mu,\theta) \leq \frac{2}{\pi}\cos\left(\frac{\pi}{2}\mu\right) + O(1/p^2).$$

Consider first the case where $\mu = -1 + \frac{2}{p}t$, for some positive integer t. In this case, $g_\mu(x) = 1$ on t x's with largest $P(x)$, and $g_\mu(x) = -1$ on the remaining $p - t$ x's.

For the purpose of computing $F(g_\mu, \theta)$, these x's for which $g_\mu(x) = 1$ can be described as $m \leq x \leq m+t-1$ for some integer m. Using that $\sum_{x=0}^{p-1} \cos(2\pi x/p + \theta) = 0$, we see that

$$\left| \sum_{x:\ g_\mu(x)=1} \cos(2\pi x/p + \theta) \right| = \left| \sum_{x:\ g_\mu(x)=-1} \cos(2\pi x/p + \theta) \right|$$

and so

$$F(g) = \frac{2}{p} \sum_{x=m}^{m+t-1} \cos(2\pi x/p + \theta) = \frac{2}{p} \frac{\sin(\pi t/p) \cos((2m+t-1)\pi/p + \theta)}{\sin(\pi/p)} \tag{36}$$

where the last equality follows from an elementary trigonometric summation. Using that $|\cos| \leq 1$ and that $t = p/2(1+\mu)$ we get

$$F(g) \leq \left| \frac{2\sin((1+\mu)\pi/2)}{p\sin(\pi/p)} \right| \cdot 1 = \frac{2\cos(\pi\mu/2)}{p\sin(\pi/p)}. \tag{37}$$

Using that $1/\sin(\epsilon) = \frac{1}{\epsilon} + O(\epsilon)$ for $|\epsilon| \leq 1$ in Eq. (37), we get

$$F(g) = 2\cos\left(\frac{\pi}{2}\mu\right) \cdot (1/\pi + O(1/p^2) = \frac{2}{\pi}\cos\left(\frac{\pi}{2}\mu\right) + O(1/p^2),$$

as required. For the case of general $\mu \in [-1, 1]$, it holds that $F(g_\mu)$ is a piecewise-linear function in μ. Thus, the almost-coincidence of $F(g_\mu)(1)$ with $\frac{2}{\pi}\cos(\frac{\pi}{2}\mu)$ on $\mu \in -1 + \frac{2}{p}\mathbb{Z}$, implies a similar $O(1/p^2)$ approximation for interpolated μ values, as $\frac{2}{\pi}\cos(\frac{\pi}{2}\mu)$ has bounded second derivative (Taylor-approximation type estimate).

B Details for a Barrier of Previous Methods

As pointed out in [28], previous studies of the leakage resilience of Shamir's secret sharing scheme aim at upper bounding some proxy quantity, which can be too large if $n \geq 2t$. Their analytic proxy is[8]

$$\sum_{c \in \ell^\perp \setminus \{0\}} \prod_{i=1}^{n} |\widetilde{f_i}(c_i)|, \qquad \text{with} \quad \widetilde{f_i}(c_i) = \begin{cases} \widehat{f_i}(c_i) & c_i \neq 0 \\ 1 & c_i = 0, \end{cases} \tag{38}$$

where $\ell^\perp$ is the set of all linear combinations $c \in \mathbb{F}_p^n$ for which the equation $\sum_{i=1}^{n} c_i \ell_i = 0$ holds. In particular, $|\ell^\perp| = p^{n-t}$. See Section 2.3 for the interpretation of what Eq. (38) bounds.

[8] The proxy found in [28, Section 5] is $\sum_{b \in \{-1,1\}^n} \sum_{c \in \ell^\perp \setminus \{0\}} \prod_{i=1}^{n} |\widehat{\frac{1+b_i f_i}{2}}(c_i)|$. However syntactially different from Eq. (38), it is identical.

In order to show that the quantity in Eq. (38) may be large if $n \geq 2t$, Maji et al. [28] presented the quadratic-residue function

$$f_i(s) = f(s) := \begin{cases} 1 & s = y^2 \pmod p \\ -1 & \text{otherwise} \end{cases}$$

which satisfies $|\widehat{f_i}(\alpha)| \sim \sqrt{1/p}$ for all $\alpha \in \mathbb{F}_p$. Hence, Eq. (38) is a sum of p^{n-t} terms, each of the order of $p^{-n/2}$, thus being > 1 if $n > 2t$.

In order to see the similar barrier in the case where the f_i's are constantly biased (that is, as in the setting of Example 3), consider some constant $\mu < 1$ (the bias), and set

$$g_i(s) = g(s) := (1-\mu) f_i(s) + \mu.$$

Note that the range of g is $[-1,1]$, unlike f whose range is $\{-1,1\}$. Anyways, it follows that $|\widehat{g}(\alpha)| \gtrsim (1-\mu)/\sqrt{p}$ for all α. Also, $\mathbb{E}[g] = \mu + (1-\mu)\,\mathbb{E}[f] \approx \mu$.

Substituting g_i in place of f_i in (38), we get p^{n-t} summands, each of the order of $(1-\mu)^n / p^{n/2}$, thus being

$$(1-\mu)^n p^{n/2-t}.$$

In case $t = (1/2 - \epsilon)n$, the sum in Eq. (38) is hence at least

$$(1-\mu)^n p^{\epsilon n} \gg 1, \tag{39}$$

for any constant $\epsilon > 0$. This gives a barrier on how effective Eq. (38) can be if $t = (1/2-\epsilon)n$.

Note however that g does not strictly output a single bit. We sketch how to fix this issue (since this section only points out a barrier with previous approaches, we skip technical details.) Observe that g is an average of functions whose range is $\{-1,1\}$. Then, we notice that Eq. (38) is a convex function of the g_i's (as a composition of convex functions). If we hence choose g_i randomly (and independently across i's) from a distribution whose mean is g, we get in expectation a value larger than Eq. (39). Note that it is important to surely have g_i with mean $\approx \mu$. For this, we note that g is two-valued with values 1 and $2\mu - 1$. By rounding μ-fraction out of these s with $g(s) = 2\mu - 1$ to have $g_i(s) = 1$, and the rest with $g_i(s') = -1$, we guarantee $\mathbb{E}[g_i] = \mu$. That is, the number of s's we round to 1 is

$$\frac{p \cdot \mu \cdot (1 - \mathbb{E}[f])}{2}.$$

There is a fine net of μ's in $[-1,1]$ for which this quantity turns out an integer. We may choose any μ with that property.

Acknowledgements

Research supported in part by an Alon Young Faculty Fellowship, by a grant from the Israel Science Foundation (ISF Grant No. 1774/20), and by a grant from the US-Israel Binational Science Foundation and the US National Science Foundation (BSF-NSF Grant No. 2020643).

References

1. Adams, D.Q., Maji, H.K., Nguyen, H.H., Nguyen, M.L., Paskin-Cherniavsky, A., Suad, T., Wang, M.: Lower bounds for leakage-resilient secret-sharing schemes against probing attacks. In: IEEE International Symposium on Information Theory, ISIT. pp. 976–981 (2021) 2
2. Akavia, A., Goldwasser, S., Vaikuntanathan, V.: Simultaneous hardcore bits and cryptography against memory attacks. In: TCC. pp. 474–495 (2009) 2
3. Ben-Or, M., Goldwasser, S., Wigderson, A.: Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended abstract). In: STOC. pp. 1–10 (1988) 2, 4
4. Benhamouda, F., Degwekar, A., Ishai, Y., Rabin, T.: On the local leakage resilience of linear secret sharing schemes. In: CRYPTO. pp. 531–561 (2018) 3, 5, 11
5. Benhamouda, F., Degwekar, A., Ishai, Y., Rabin, T.: On the local leakage resilience of linear secret sharing schemes. J. Cryptol. **34**(2), 10 (2021) 2, 3, 5, 11
6. Blakley, G.R.: Safeguarding cryptographic keys. Proceedings of the AFIPS National Computer Conference **22**, 313–317 (1979) 2
7. Boyle, E., Segev, G., Wichs, D.: Fully leakage-resilient signatures. J. Cryptol. **26**(3), 513–558 (2013) 2
8. Chandran, N., Kanukurthi, B., Obbattu, S.L.B., Sekar, S.: Adaptive extractors and their application to leakage resilient secret sharing. In: CRYPTO. pp. 595–624 (2021) 6
9. Chandran, N., Kanukurthi, B., Obbattu, S.L.B., Sekar, S.: Short leakage resilient and non-malleable secret sharing schemes. In: CRYPTO. pp. 178–207 (2022) 6
10. Chattopadhyay, E., Goodman, J., Goyal, V., Kumar, A., Li, X., Meka, R., Zuckerman, D.: Extractors and secret sharing against bounded collusion protocols. In: FOCS. pp. 1226–1242 (2020) 6
11. Chaum, D., Crépeau, C., Damgård, I.: Multiparty unconditionally secure protocols (extended abstract). In: STOC. pp. 11–19 (1988) 2
12. Davì, F., Dziembowski, S., Venturi, D.: Leakage-resilient storage. In: SCN. pp. 121–137 (2010) 6
13. Desmedt, Y., Frankel, Y.: Threshold cryptosystems. In: Advances in Cryptology - CRYPTO. pp. 307–315 (1989) 2
14. Dziembowski, S., Pietrzak, K.: Leakage-resilient cryptography. In: FOCS. pp. 293–302 (2008) 2, 6
15. Faust, S., Rabin, T., Reyzin, L., Tromer, E., Vaikuntanathan, V.: Protecting circuits from computationally bounded and noisy leakage. SIAM J. Comput. **43**(5), 1564–1614 (2014) 2
16. Frankel, Y.: A practical protocol for large group oriented networks. In: Advances in Cryptology - EUROCRYPT. pp. 56–61 (1989) 2
17. Goldreich, O., Micali, S., Wigderson, A.: How to play any mental game or A completeness theorem for protocols with honest majority. In: STOC. pp. 218–229 (1987) 2, 3, 4
18. Goyal, V., Kumar, A.: Non-malleable secret sharing. In: STOC. pp. 685–698 (2018) 6
19. Goyal, V., Kumar, A.: Non-malleable secret sharing for general access structures. In: CRYPTO. pp. 501–530 (2018) 6
20. Guruswami, V., Wootters, M.: Repairing Reed-Solomon codes. IEEE Trans. Inf. Theory **63**(9), 5684–5698 (2017) 5
21. Ishai, Y., Sahai, A., Wagner, D.A.: Private circuits: Securing hardware against probing attacks. In: Advances in Cryptology - CRYPTO. pp. 463–481 (2003) 2

22. Kocher, P.C.: Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In: Advances in Cryptology - CRYPTO. pp. 104–113 (1996) 2
23. Kocher, P.C., Jaffe, J., Jun, B.: Differential power analysis. In: Advances in Cryptology - CRYPTO. pp. 388–397 (1999) 2
24. Kumar, A., Meka, R., Sahai, A.: Leakage-resilient secret sharing against colluding parties. In: FOCS. pp. 636–660 (2019) 6
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: Advances in Cryptology - EUROCRYPT. pp. 344–374 (2021) 2, 5
26. Maji, H.K., Nguyen, H.H., Paskin-Cherniavsky, A., Suad, T., Wang, M., Ye, X., Yu, A.: Tight estimate of the local leakage resilience of the additive secret-sharing scheme & its consequences. In: Information-Theoretic Cryptography, ITC. pp. 16:1–16:19 (2022) 2, 5
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. pp. 2678–2683 (2022) 2, 3, 5
28. Maji, H.K., Paskin-Cherniavsky, A., Suad, T., Wang, M.: Constructing locally leakage-resilient linear secret-sharing schemes. In: Advances in Cryptology - CRYPTO. pp. 779–808 (2021) 2, 3, 4, 5, 27, 29, 30
29. Massey, J.L.: Some applications of source coding in cryptography. Eur. Trans. Telecommun. **5**(4), 421–430 (1994) 4
30. Micali, S., Reyzin, L.: Physically observable cryptography (extended abstract). In: TCC. pp. 278–296 (2004) 2
31. Naor, M., Segev, G.: Public-key cryptosystems resilient to key leakage. SIAM J. Comput. **41**(4), 772–814 (2012) 2
32. Nielsen, J.B., Simkin, M.: Lower bounds for leakage-resilient secret sharing. In: Advances in Cryptology - EUROCRYPT. pp. 556–577 (2020) 3, 5
33. Rothblum, G.N.: How to compute under AC^0 leakage without secure hardware. In: Advances in Cryptology - CRYPTO. pp. 552–569 (2012) 2
34. Santis, A.D., Desmedt, Y., Frankel, Y., Yung, M.: How to share a function securely. In: STOC. pp. 522–533 (1994) 2
35. Shamir, A.: How to share a secret. Commun. ACM **22**(11), 612–613 (1979) 2, 8
36. Srinivasan, A., Vasudevan, P.N.: Leakage resilient secret sharing and applications. In: CRYPTO. pp. 480–509 (2019) 6