Leakage-resilience of the Shamir Secret-sharing Scheme against Physical-bit Leakages

Hemanta K. Maji[1*], Hai H. Nguyen[1*], Anat Paskin-Cherniavsky[2**], Tom Suad[2**], and Mingyuan Wang[1*]

[1] Department of Computer Science, Purdue University
{hmaji,nguye245,wang1929}@purdue.edu
[2] Department of Computer Science, Ariel University
anatpc@ariel.ac.il, tom.suad@msmail.ariel.ac.il

Abstract. Efficient Reed-Solomon code reconstruction algorithms, for example, by Guruswami and Wootters (STOC–2016), translate into local leakage attacks on Shamir secret-sharing schemes over characteristic-2 fields. However, Benhamouda, Degwekar, Ishai, and Rabin (CRYPTO–2018) showed that the Shamir secret sharing scheme over prime-fields is leakage resilient to one-bit local leakage if the reconstruction threshold is roughly 0.87 times the total number of parties. In several application scenarios, like secure multi-party multiplication, the reconstruction threshold must be at most half the number of parties. Furthermore, the number of leakage bits that the Shamir secret sharing scheme is resilient to is also unclear.

Towards this objective, we study the Shamir secret-sharing scheme's leakage-resilience over a prime-field F. The parties' secret-shares, which are elements in the finite field F, are naturally represented as λ-bit binary strings representing the elements $\{0, 1, \ldots, p-1\}$. In our leakage model, the adversary can independently probe m bit-locations from each secret share. The inspiration for considering this leakage model stems from the impact that the study of oblivious transfer combiners had on general correlation extraction algorithms, and the significant influence of protecting circuits from probing attacks has on leakage-resilient secure computation.

Consider arbitrary reconstruction threshold $k \geqslant 2$, physical bit-leakage parameter $m \geqslant 1$, and the number of parties $n \geqslant 1$. We prove that Shamir's secret-sharing scheme with random evaluation places is leakage-resilient with high probability when the order of the field F is sufficiently large; ignoring polylogarithmic factors, one needs to ensure that $\log |F| \geqslant n/k$. Our result, excluding polylogarithmic factors, states that Shamir's scheme is secure as long as the total amount of leakage $m \cdot n$ is less than

[*] The research effort is supported in part by an NSF CRII Award CNS–1566499, an NSF SMALL Award CNS–1618822, the IARPA HECTOR project, MITRE Innovation Program Academic Cybersecurity Research Awards (2019–2020, 2020–2021), a Purdue Research Foundation (PRF) Award, and The Center for Science of Information, an NSF Science and Technology Center, Cooperative Agreement CCF–0939370.

[**] Research supported by the Ariel Cyber Innovation Center in conjunction with the Israel National Cyber directorate in the Prime Minister's Office.

the entropy $k \cdot \lambda$ introduced by the Shamir secret-sharing scheme. Note that our result holds even for small constant values of the reconstruction threshold k, which is essential to several application scenarios.

To complement this positive result, we present a physical-bit leakage attack for $m = 1$ physical bit-leakage from $n = k$ secret shares and any prime-field F satisfying $|F| = 1 \mod k$. In particular, there are (roughly) $|F|^{n-k+1}$ such vulnerable choices for the n-tuple of evaluation places. We lower-bound the advantage of this attack for small values of the reconstruction threshold, like $k = 2$ and $k = 3$, and any $|F| = 1 \mod k$. In general, we present a formula calculating our attack's advantage for every k as $|F| \to \infty$.

Technically, our positive result relies on Fourier analysis, analytic properties of proper rank-r generalized arithmetic progressions, and Bézout's theorem to bound the number of solutions to an equation over finite fields. The analysis of our attack relies on determining the "discrepancy" of the Irwin-Hall distribution. A probability distribution's discrepancy is a new property of distributions that our work introduces, which is of potential independent interest.

Keywords: Random Punctured Reed-Solomon Codes, Physical-bit Leakage, Local Leakage Resilience, Discrete Fourier Analysis, Exponential Sums, Rank-r Generalized Arithmetic Progression, Bézout's Theorem, Irwin-Hall Distribution.

1 Introduction

In the presence of an increasing number of side-channel attacks on cryptographic protocols, theoretical cryptography research has been revisiting its implicit assumptions in modeling secure cryptographic protocols. For example, results in reconstructing Reed-Solomon codes [15, 16, 11] imply that leaking even $(m = 1)$ bit from the secret shares of Shamir's secret-sharing scheme over characteristic-2 finite field F renders this secret sharing scheme insecure. That is, there exist two secrets $s^{(0)}, s^{(1)} \in F$ that an adversary can distinguish by leaking only $(m = 1)$-bit local leakage from every secret share. We emphasize that in locally leakage-resilient secret-sharing schemes,[3] the entire secret's reconstruction is not necessary to qualify as a successful attack. It suffices to achieve a non-negligible advantage in distinguishing any two secrets $s^{(0)}, s^{(1)} \in F$ of adversary's choice. Since secret-sharing schemes (typically, packed [13] Massey secret-sharing schemes [35] corresponding to linear error-correcting codes with "good" properties) are fundamental cryptographic primitives underlying nearly all of conceivable cryptography, such innovative side-channel attacks threaten the security of most cryptographic protocols.

The recent ground-breaking work of Benhamouda, Degwekar, Ishai, and Rabin [3] identified several scenarios where Shamir's secret-sharing scheme and

[3] The term "*local*" in local leakage-resilience refers to the fact that the adversary performs arbitrary leakage on each secret-share *independently*.

the additive secret-sharing scheme are resilient to such local leakage attacks;[4] thus, laying to rest the devastating possibility of side-channel attacks breaking all secret-sharing schemes. Recently, [37] propose even more sophisticated local leakage attacks on secret-sharing schemes. Since the work of Benhamouda et al. [3], several works [1, 41, 2, 29, 6, 22, 9, 34] have introduced transformations to convert existing secret-sharing schemes into leakage-resilient versions. It seems insurmountable to replace every deployed secret-sharing scheme with its leakage-resilient version. Furthermore, the leakage-resilient versions of these secret-sharing schemes introduce encoding overheads that noticeably reduce these secret-sharing schemes' information-rate,[5] adversely affecting the applications' efficiency. Towards the objective of retaining the efficiency of existing secret-sharing schemes with minimal changes, other works [21, 7, 30, 33] analyze the resilience of existing secret-sharing schemes or ensembles of secret-sharing schemes with good properties (for example, packed Massey secret-sharing schemes corresponding to (nearly) *maximum distance separable* linear error-correcting codes) that are already locally leakage-resilient. Currently, our understanding of the local leakage-resilience of existing secret-sharing schemes typically used in cryptography is still in a nascent state. The exact loss in the achievable parameters and information-rate to additionally ensure local leakage-resilience is even less clear. These losses in the feasible parameter regions and information-rate even render secret-sharing schemes unusable for various application scenarios.

For example, Benhamouda et al. [3] proved that if Shamir's secret-sharing scheme, one of the most widely used secret-sharing schemes, has a reconstruction threshold $k \geqslant 0.867n$, where n is the total number of parties, then it is leakage-resilient to $(m = 1)$-bit local leakage. Observe that using a large reconstruction threshold k introduces inefficiencies, which may not be necessary for various applications. Additionally, an even more concerning fact is that some cryptographic constructions crucially rely on the reconstruction threshold being low. For example, the secure computation of the multiplication of two (already secret-shared) secrets requires the reconstruction threshold $k < n/2$ even against honest-but-curious parties.

Summary of our work: problem statement and results. Our work contributes to this research thrust on characterizing the local leakage-resilience of secret-sharing schemes. As a stepping-stone, our work considers the scenario where each party stores their secret-share in its natural λ-bit binary representation, and the adversary may (independently) probe arbitrary m physical-bits from each secret-share. The particular choice of the physical-bit leakage draws inspiration from, for instance, the crucial role of the studies on oblivious transfer combiners [20, 36, 19, 25, 8] in furthering the state-of-the-art of general correlation extractors [24, 5, 4], and the techniques in protecting circuits against probing

[4] Leakage-resilient secret-sharing was also, independently, introduced by [14] as an intermediate primitive.

[5] The information-rate of a secret-sharing scheme is the ratio on the size of the secret to the largest size of the secret-share that a party receives.

attacks [27, 26, 12] impacting the study of leakage-resilient secure computation (refer to the excellent recent survey [28]).

We present both feasibility and hardness of computation results. Roughly, our results prove that Shamir's secret-sharing scheme with n random evaluation places, for any reconstruction threshold $k \geqslant 2$, is locally leakage-resilient. The adversary can leak m physical-bits from each secret-share if the total amount of leakage $m{\cdot}n$ is less than the total entropy $k{\cdot}\lambda$ in the secret-sharing scheme, except with an exponentially small probability in λ. To complement this result, we also present new local physical-bit leakage attacks demonstrating several sets of *bad evaluation places* where Shamir's secret-sharing scheme is not leakage-resilient even when $m = 1$ and $n = k$. Technically, our positive result's analysis proceeds by discrete Fourier analysis relying on the analytical properties of exponential sums involving rank-r generalized arithmetic progressions, and Bézout's theorem to upper-bound the number of solutions to a system of equations over finite fields. On the other hand, our attack's analysis is equivalent to the "discrepancy" of the Irwin-Hall distribution [23, 18], a new mathematical property of probability distributions that we introduce.

1.1 Our Contribution

This section, first, introduces some informal notations to facilitate the introduction of our results and discussion on them. Let λ represent the security parameter. Consider a prime-field F of order p such that $2^{\lambda-1} \leqslant p < 2^{\lambda}$. That is, every element in the finite field (when equivalently interpreted as elements of the set $\{0, 1, \ldots, p-1\}$) has a λ-bit binary representation. The parameter $k \in \mathbb{N}$ represents the reconstruction threshold, and $n \in \mathbb{N}$ represents the total number of parties.

Shamir Secret-sharing Scheme. Suppose the secret is $s \in F$, and the tuple of distinct evaluation places is $\vec{X} := (X_1, X_2, \ldots, X_n) \in (F^*)^n$, such that $i \neq j$ implies $X_i \neq X_j$.[6] Shamir's secret-sharing scheme with threshold $k \in \mathbb{N}$, represented by $\mathsf{ShamirSS}(n, k, \vec{X})$, picks a random secret-sharing polynomial $P(X) \in F[X]/X^k$ conditioned on the fact that $P(0) = s$. The secret-shares for parties $1, 2, \ldots, n$ are $s_1 = P(X_1), s_2 = P(X_2), \ldots, s_n = P(X_n)$, respectively. Observe that, in a Shamir secret-sharing scheme, it is implicit that the number of parties satisfies $n < p$.

Physical Bit-leakage. Our work represents all the secret shares $s_1, \ldots, s_n \in F$ with the parties as λ-bit binary representation. An m-bit local physical-bit leak-

[6] We assume this for the ease of presentation for now, while our results do not require such restrictions. When there are two identical evaluation places, leaking one bit from each share is equivalent to leaking two bits from one of those shares. Since our results naturally extend to leaking multiple bits from each share, we do not need the restriction that all the evaluation places are distinct. Furthermore, when all the evaluation places are chosen independently randomly (at most a polynomial in the security parameter), the probability that there are two identical evaluation places are exponentially small (by the birthday bound) since the field size is exponentially large in the security parameter.

age function specifies probing locations $\{\ell_{i,j}\}_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant m}}$ such that $\ell_{i,j} \in \{1,2,\ldots,\lambda\}$ for each of the n secret shares. The output of the leakage function provides the $\ell_{i,j}$-th bit[7] in the i-th secret-share s_i, for all $1 \leqslant i \leqslant n$ and $1 \leqslant j \leqslant m$. For a fixed secret $s \in F$, the output of the leakage function is a distribution over the sample space $\{0,1\}^{mn}$ induced by the random choice of the secret-sharing polynomial $P(X)$ above.

Local Leakage-resilience against Physical Bit-leakage. $\mathsf{ShamirSS}(n,k,\vec{X})$ is $(1-\varepsilon)$-secure against local physical-bit leakages if, for any two secrets $s^{(0)}, s^{(1)} \in F$ and an m-bit local physical-bit leakage function, the statistical distance between the leakage distributions is at most ε.[8]

Result I: Feasibility. Suppose we are given as input the number of parties $n \in \mathbb{N}$, the reconstruction threshold $2 \leqslant k \in \mathbb{N}$, the length of the binary representations $\lambda \in \mathbb{N}$, the insecurity tolerance $\varepsilon = 2^{-t}$, and the number of leakage bits m from each secret-share. Our experiment picks distinct evaluation places $\vec{X}$ uniformly at random from the set F^*. Given a fixed tuple of distinct evaluation places $\vec{X}$, one tests whether $\mathsf{ShamirSS}(n,k,\vec{X})$ is resilient to m-bit local physical-bit leakage resilient or not.

We prove that the $\mathsf{ShamirSS}(n,k,\vec{X})$ scheme is $(1-\varepsilon)$-secure (except with an exponentially small probability in $(k-1)\cdot\lambda$ over the random choices of the evaluation places $\vec{X}$), if the following conditions are satisfied.

1. The number of bits λ satisfies $\lambda/\log^2\lambda \geqslant \Theta(t/k)$, and
2. The total leakage mn satisfies $mn \leqslant k\lambda/\log^2\lambda$.

This result is the summarized in Theorem 4 and Corollary 4.

The constants in the asymptotic notations are all universal positive constants. Given n, k, F parameters, note that one can choose the random evaluation places once (using a trusted setup, e.g., common random string) for all future instantiations of Shamir secret-sharing scheme. The probability that the instantiation is not $(1-\varepsilon)$-secure is exponentially small. We emphasize that the result above holds for any $k \geqslant 2$, which is the best possible result. Therefore, for every n, k, m, ε, our result proves that Shamir secret-sharing scheme for all large-enough prime fields F is leakage-resilient.

A Concrete Example. As a representative example, consider the following scenario. Suppose the reconstruction threshold is $k = 2$, the number of bits leaked is $m = 1$, and the number of parties $n = 10, 100$, and 1000. Assume we wish to achieve insecurity $\varepsilon = 2^{-50}$ and succeed in picking a set of good evaluation places with probability (at least) $1 - 2^{-50}$. Our Theorem 3 states that picking

[7] For instance, let $\lambda = 5$ and $p = 19$. The element $5 \in F = \{0,1,\ldots,18\}$ is represented as 00101. The first bit is 1, second bit is 0, third bit is 1, and the fourth and the fifth bits are both 0.

[8] One can simulate the leakage joint distribution as follows. The simulator shall fix an arbitrary secret (say, 0), generate its secret shares, and output the evaluation of the leakage function on the respective secret shares. The simulation error for this strategy is a two-approximation of the indistinguishability advantage by the triangle inequality.

a prime number p with more than 430, 4800, and 62000 bits, respectively, in its binary representation suffices. Intuitively, it scales (roughly) linearly with n. As k increases, even smaller primes suffice. The estimates above correspond to the most difficult case for security.

Reinterpretation: Randomly Punctured Reed-Solomon Code. Given a Reed-Solomon code of dimension k over a prime-field F, one punctures $(p-1)-n$ columns among the columns numbered $\{1, 2, \ldots, p-1\}$. Suppose the columns numbered $(0, X_1, \ldots, X_n)$ survive the puncturing operations. The Massey secret-sharing scheme [35] corresponding to this resulting $[n+1, k]_F$ linear error-correcting code is identical to the $\mathsf{ShamirSS}(n, k, \vec{X})$ secret-sharing scheme mentioned above. Consequently, our result proves that all puncturing operations (except an exponentially small fraction of them) result in an $(1-\varepsilon)$-secure leakage-resilient scheme.

Result II: Hardness of Computation. We present an attack strategy for any $k \geqslant 2$, $n \geqslant k$, $m \geqslant 1$, and $p = 1 \mod k$. For a fixed $k \geqslant 2$, there are infinitely many primes satisfying $p = 1 \mod k$ due to Dirichlet's theorem [39]. Our attack leaks only the least-significant bit of the secret-shares, and has a constant advantage in distinguishing two secrets based on this leakage. For given values of k, n, p satisfying the conditions above, there are (roughly) $n^k p^{n-k} \cdot (p-1)/k$ vulnerable tuples of evaluation places where our attack succeeds.

For $k = 2, 3$ (and any p), we calculate the exact advantage of our attack. Next, for any $k \geqslant 2$, as $p \to \infty$, we show that the quality of our attack is lower-bounded by the "discrepancy" of the Irwin-Hall distribution [23, 18] (with parameter $(k-1)$, represented by I_{k-1}). The "discrepancy" of a distribution (see Definition 9) is a new property of probability distributions that we introduce, which is of potential independent interest. We explicitly calculate the discrepancy of the Irwin-Hall distribution for $(k-1) \in \{2, 3, \ldots, 24\}$, and Figure 2 provides the details. If the discrepancy of the Irwin-Hall distribution I_{k-1} is non-zero, then the discrepancy is at least $1/k!$. However, based on our numerical experiments, we conjecture that the discrepancy of Irwin-Hall distribution (with parameter k) behaves as $\geqslant \exp(-\Theta(k))$, which is not negligible for $k = \mathcal{O}(\log \lambda)$. We emphasize that, given a fixed k, the conjectured distinguishing advantage of this attack depends only on k, independent of the security parameter. Intuitively, increasing the size of the prime should only make the scheme more secure, and the conjecture above considers $p \to \infty$.

Reinterpretation: Attack on additive secret-sharing scheme. Our physical bit leakage attack on the Shamir secret-sharing scheme directly translates into physical bit leakage attacks on the additive secret-sharing scheme. If the number of shares in the additive secret sharing scheme is $\mathcal{O}(\log \lambda)$ then, our conjecture above, states that the advantage of our attack is $1/\mathsf{poly}(\lambda)$.

Benhamouda et al. [3] proposed a general leakage attack on additive secret-sharing scheme. Their attack tests whether each share is smaller than $p/2k$ and has an advantage of (roughly) $1/k^k$. In comparison, our attack employs a simpler leakage function, i.e., physical-bit leakage, and will achieve similar advantage if our conjecture holds. Since the leakage function is simpler, the threat it poses is even more significant.

1.2 Technical Overview

Let λ be the security parameter. Let F be a prime field of order p such that p needs λ bits in its binary representation. That is, we have $p \in \{2^{\lambda-1}, 2^{\lambda-1}+1, \dots, 2^{\lambda}-1\}$.

For a secret $s \in F$, assume that Shamir's secret sharing scheme uses a random polynomial $P(X)$ of degree $< k = \mathsf{poly}(\lambda)$ conditioned on $P(0)=s$ to share a secret among $n = \mathsf{poly}(\lambda)$ parties. Let the evaluation places be $\vec{X} = (X_1, X_2, \dots, X_n) \in (F^*)^n$ such that $i \neq j \implies X_i \neq X_j$ (i.e., all evaluation places are distinct). The share of party i is the evaluation of the polynomial $P(X)$ at the evaluation place X_i. $\mathsf{ShamirSS}(n, k, \vec{X})$ represents this secret-sharing scheme.

Fix the local leakage function $\vec{\tau}$ that leaks m physical-bits from the binary representation of the secret-shares of the n parties. Furthermore, $\vec{\tau}\left(\mathsf{Share}^{\vec{X}}(s)\right)$ represents the joint distribution of the leakage conditioned on the fact that the secret is $s \in F$. If this joint distribution of the leakage is independent of the secret, then the secret-sharing scheme is *locally leakage-resilient* to physical bit leakages.

Our objective is to prove that Shamir secret-sharing scheme is locally leakage-resilient for most evaluation places $\vec{X}$, when $\vec{X}$ is chosen uniformly at random from the set $(F^*)^n$ under the constraint that $i \neq j \implies X_i \neq X_j$. Theorem 3 formally states this result. To simplify the presentation of key technical ideas, it is instructive to use $m = 1$. The analysis for larger m is analogous.

Reduction 1. Fix any two secrets $s^{(0)}, s^{(1)} \in F$. We prove the following two bounds. First, by standard Fourier techniques, we prove

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

Here, $\mathbb{1}_{\ell_i}$ is the indicator function of the set $\{x \colon L_i(x) = \ell_i\}$; $C_{\vec{X}}$ is the (punctured) Reed-Solomon code that corresponds to Shamir's secret-sharing with evaluation places $\vec{X}$; $C_{\vec{X}}^{\perp}$ is the dual code of $C_{\vec{X}}$.

Next, we show that it suffices to prove that, over randomly chosen evaluation places $\vec{X} \in (F^*)^n$ (under the constraint that $i \neq j \implies X_i \neq X_j$), this upper bound is small. That is,

$$\mathop{\mathrm{E}}_{\vec{X}}\left[\sum_{\vec{\ell} \in \{0,1\}^n} \sum_{\vec{\alpha} \in C_{\vec{X}}^{\perp} \setminus \{0\}} \left(\prod_{i=1}^{n} \left|\widehat{\mathbb{1}_{\ell_i}}(\alpha_i)\right|\right)\right] \leqslant \exp(-\Theta(\lambda)).$$

This bound above is sufficient for our objective. One could use a union bound on the leakage function to conclude that most evaluation places yield a locally leakage-resilient Shamir secret-sharing scheme. After that, a Markov inequality yields random evaluation places, except an exponentially small fraction of the evaluation places, result in a locally leakage-resilient Shamir secret-sharing scheme. Note that we avoid the union bound over secrets since the upper bound is insensitive to the secret. The above argument can be found in Section 5.2.

Reduction 2. We employ Fourier analysis to estimate the following bound

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

The analysis in Section 5.4 reduces this estimation to two problems, Problems A and B below.

Problem A. For simplicity of presenting the main technical ideas, assume that the parties' secret-shares are elements from the set $\{0,1\}^\lambda$. The Fourier analysis above relies on bounding certain exponential sums over the subset of elements that agree with an apriori fixed m-bit leakage. In particular, these elements will have m bits identical to the leakage, and all remaining $(\lambda - m)$ bits may either be zero or one. The abstraction of *generalized arithmetic progressions* (refer to Section 3.1) is adequate to capture the analytic properties of such subsets.

We import an estimate of the exponential sum mentioned in Imported Theorem 1. For the particular case of $m = 1$, we present a tight estimate of the constant in the above imported theorem (refer to Theorem 2). This tight estimate of the constant translates into near-optimal bounds on the local leakage-resilience of Shamir secret-sharing scheme.

A subtlety in the argument above is that the set of binary representations of a party's secret-share is *not* the set $\{0,1\}^\lambda$. It is, in fact, the set of the binary representations of $\{0,1,\dots,p-1\}$. However, this subset can be partitioned into (at most) λ subsets such that each set is an *MSB-fixing set*, a set whose most significant bits are fixed and the least significant bits are uniformly random (for formal definition and examples, refer to Section 4). This notion of MSB-fixing sets introduced by us helps perform the simplified analysis mentioned above in the context of our problem.

Problem B. Once problem A is solved, the Fourier analysis requires another bound. Fix any $\vec{\alpha} \in F^n$. Next, consider the following equation.

$$\begin{pmatrix} X_1 & X_2 & \cdots & X_n \\ X_1^2 & X_2^2 & \cdots & X_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ X_1^{k-1} & X_2^{k-1} & \cdots & X_n^{k-1} \end{pmatrix} \cdot \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

How many solutions $\vec{X} \in (F^*)^n$ exist of the equation above, such that $i \neq j \implies X_i \neq X_j$?

Consider the simplification when $\vec{\alpha} = \vec{1}$. Fix any distinct values of $X_{k+1}, \dots, X_n \in F^*$. If a solution $X_1, \dots, X_k$ exists (where each $X_1, \dots, X_n$ are distinct as well) then every permutation of $X_1, \dots, X_k$ is also a solution. Consequently, the number of solutions of the equation above is at least $\min\{0, k!\}$.

We rely on Bézout's theorem (in particular, a form that has an easy-to-verify analytic test, refer to Imported Theorem 2) to claim that the number of solutions is, in fact, at most $k!$. Consequently, overall, the number of solutions $\vec{X} \in (F^*)^n$ is $\mathcal{O}\left(k! \cdot p^{n-k}\right)$. This bound holds for any $\vec{\alpha}$, in general, and not just for $\vec{\alpha} = \vec{1}$.

Resolving the problems A and B completes the proof of Theorem 3. Corollary 2 is an easy-to-use corollary of this theorem demonstrating that when $n = \mathsf{poly}(\lambda)$, $k = \mathcal{O}\left(\frac{t}{\lambda} + \frac{\log\lambda}{\lambda} \cdot n\right)$ suffices to ensure that $1 - \exp(-\Theta(\lambda))$ fraction of the evaluation places yield a Shamir secret-sharing scheme that is locally leakage-resilient to $m = 1$ physical-bit leakage with insecurity $\leqslant 2^{-t}$.

Generalization to m-bit leakage from each share. Observe that one can directly consider the leaking m-bit leakage from the secret-shares of the Shamir secret-sharing scheme. Towards this objective, one needs to consider MSB-fixing sets that are consistent with an apriori fixed leakage, which are proper rank-$(m+1)$ generalized arithmetic progressions. However, the constant in Imported Theorem 1 for rank-$(m+1)$ generalized arithmetic progressions is not explicit. Moreover, without an explicit constant, one can not provide concrete bound on the insecurity of the secret-sharing scheme. Consequently, our work relies on a different approach.

We consider secret-sharing scheme where each share of the Shamir secret-sharing scheme is duplicated m-times, and the adversary leaks one physical bit from each secret share. This technique allows using our Theorem 2 that has an explicit and tight constant, which is specifically tailored for our problem. The remainder of the technical analysis proceeds similar to the presentation above. The general result is summarized as Theorem 4.

New physical-bit attack. For reconstruction threshold k, consider the number of parties $n = k$, and the prime $p = 1 \mod k$. Let F be the finite field of order p. Let $\left\{\alpha, \alpha^2, \dots, \alpha^k = 1\right\} \subseteq F^*$ be the set of all solutions to the equation $Z^k - 1 = 0$. Consider $n = k$ evaluation places $X_1 = \alpha$, $X_2 = \alpha^2, \dots,$ and $X_k = \alpha^k$. Let $f(X) \in F[X]/X^k$ be an arbitrary polynomial with $f(0) = s$, for some secret $s \in F$. Observe that $f(X_1) + f(X_2) + \cdots + f(X_k) = ks$.

To present the primary technical ideas, consider $k = 3$. Let s_1 be the secret share of party one. Over the random choice of the polynomial $f(X)$, the secret share s_1 is uniformly random over F. Similarly, the choice of s_2, the secret share of party two, is independent and uniformly random over F. However, the secret share of the k-th party satisfies the constraint $s_k = ks - \sum_{i=1}^{k-1} s_i$, i.e., $s_3 = 3s - (s_1 + s_2)$.

Our leakage functions shall leak the least significant digit of the shares s_1, s_2, and s_3 to construct a test that predicts the least significant digit of ks with constant advantage, for an appropriate $s \in F$. For a random secret, our test has (statistically close to) zero advantage. So, our test distinguishes, by an averaging argument, two secrets with a constant advantage.

Our New Test. Let $S_1, S_2, S_3 \in \{0, 1, \dots, p-1\} \subseteq \mathbb{N}_0 := \{0, 1, 2, \dots\}$ represent the whole numbers corresponding to the secret shares s_1, s_2, s_3. Our test predicts the least significant digit of ks as the parity of the least significant digits of S_1, S_2, S_3. Observe that (the addition in the equation below is over the set of whole numbers $\mathbb{N}_0$, and $(ks) \in F$ is interpreted as an element of $\{0, 1, \ldots, p-1\}$)

$$S_1 + S_2 + S_3 = p\mathbb{Z} + (ks).$$

Therefore, if $S_1 + S_2 + S_3 = ip + ks$, for an even integer i, then the parity of the least significant digits of S_1, S_2, S_3 correctly predicts the least significant digit of ks. On the other hand, if $S_1 + S_2 + S_3 = ip + ks$, for an odd integer i, then the parity of the least significant digits of S_1, S_2, S_3 incorrectly predicts the least significant digit of ks. Our objective is to prove that there exists $s \in F$ such that the absolute value of the difference between the correct and incorrect prediction probabilities is a constant. Equivalently, the objective is to prove that there exists $s \in F$ such that the probability of correct prediction probability is a constant larger than $1/2$ or a constant smaller than $1/2$.

So, for independent and uniformly random $S_1, S_2 \in \{0, 1, \ldots, p-1\}$, our objective is to compute the probability that

$$S_1 + S_2 + S_3 = ip + (ks),$$

where i is even and $S_3 \in \{0, 1, \ldots, p-1\}$. Equivalently, for independent and uniformly random $S_1, S_2 \in \{0, 1, \ldots, p-1\}$, our objective is to compute the probability that

$$S_1 + S_2 \in 2p\mathbb{Z} + (ks) - \{0, 1, \ldots, p-1\} = \mathbb{N}_0 \cap \bigcup_{\substack{i \in \mathbb{Z} \\ i \text{ odd}}} [ip + (ks) + 1, (i+1)p + (ks)] \, .$$

For $k = 3$, we can show that this probability is < 0.25 by choosing $ks = (p-1)/2$.

Extensions. Note that our attack naturally extends to that the evaluation places form an arbitrary coset in $F^*/\{\alpha, \ldots, \alpha^k = 1\}$. For $n > k$, one can choose the remainder of the evaluation places arbitrarily. Consequently, there are a total of $\sim n^k \cdot p^{n-k} \cdot (p-1)/k$ evaluation places where our attack works.

For a fixed k, and prime $p \to \infty$, Section 6.1 shows that the advantage of our test tends to $\mathsf{disc}(I_{k-1})$, where I_{k-1} is the Irwin-Hall distribution for parameter $(k-1)$, and Definition 9 defines the discrepancy of a probability distribution $\mathsf{disc}(\cdot)$. Figure 1 shows this discrepancy for $(k-1) = 4$ and $(k-1) = 5$. Figure 2 shows the conjectured bound for discrepancy for $(k-1) \in \{2, 3, \ldots, 24\}$.

2 Preliminaries

In this work, λ represents the security parameter. Let p be a prime whose binary representation has λ bits. Or, equivalently, the prime satisfies $2^{\lambda-1} \leqslant p < 2^{\lambda}$. For any positive integer a and $i \geqslant 1$, $[a]_i$ denotes the i^{th} least significant bit in the binary representation of a. For example, let $\lambda = 5$ and $p = 19$, the field element $5 \in F = \{0, 1, ..., 18\}$ is binary represented as 00101. Its least significant

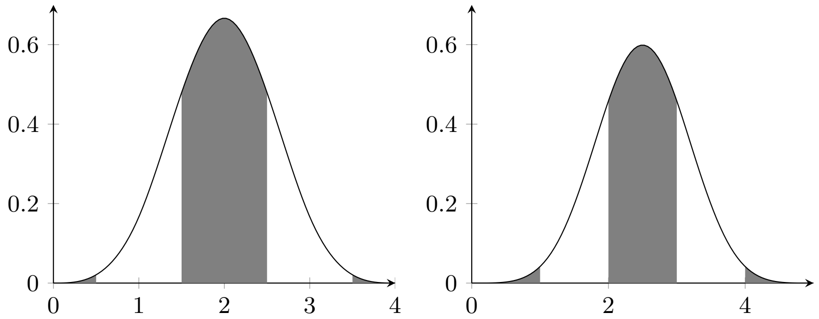

Fig. 1. Plot of the Irwin-Hall distribution for parameters $(k-1)=4$ and $(k-1)=5$. The black intervals have width 1, each black interval is separated from the next nearest black interval by distance 1, and the central mass of probability distribution is captured by a black interval. The discrepancy of the respective distributions is the difference between the probability mass inside the black bands and the total probability mass outside the black bands. For $(k-1)=4$ and $(k-1)=5$, the discrepancies are $5/24$ and $2/15$, respectively.

bit is $[5]_1 = 1$, second least significant bit is $[5]_2 = 0$, and so on. Using our notations, the binary representation of p is $[p]_\lambda \, [p]_{\lambda-1} \cdots [p]_1$.

For any set S, $\mathbb{1}_S$ denotes its indicator function. That is, $\mathbb{1}_S(x) = 1$ if $x \in S$, and $\mathbb{1}_S(x) = 0$, otherwise.

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

We shall use $f(\lambda) \sim g(\lambda)$ if $f(\lambda) = (1 + \mathrm{o}(1))\, g(\lambda)$. Additionally, we write $f(\lambda) \lesssim g(\lambda)$ if $f(\lambda) \leqslant (1 + \mathrm{o}(1))\, g(\lambda)$.

2.1 Secret Sharing Schemes

Definition 1 ($(n,k)_F$-Secret Sharing Scheme). *For any two positive integer $k < n$, 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 function* $(\mathsf{Share}, \mathsf{Rec})$ *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.***[9] *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*
$$\mathsf{SD}\left(\left(\mathsf{Share}(s_0)_{i_1}, \ldots, \mathsf{Share}(s_0)_{i_t}\right), \left(\mathsf{Share}(s_1)_{i_1}, \ldots, \mathsf{Share}(s_1)_{i_t}\right)\right) = 0.$$

[9] The definition considers *perfect* privacy. For secret-sharing schemes based on Massey's construction [35] from linear error-correcting codes, the shares of any set

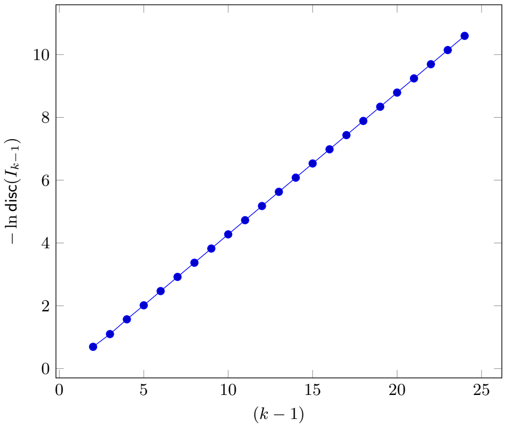

Fig. 2. Plot of $-\ln \mathsf{disc}(I_{k-1})$ versus $(k-1)$ for $(k-1) \in \{2, 3, \ldots, 24\}$.

Definition 2 **($(n, k, \vec{X})_F$-Shamir Secret-sharing).** *Let F be a prime field. For any positive integer $k \leqslant n$ and* evaluation places $\vec{X} = (X_1, \ldots, X_n)$ *the following conditions are satisfied. (1) For all $1 \leqslant i \leqslant n$, $X_i \in F^*$, and (2) for all $1 \leqslant i < j \leqslant n$, $X_i \neq X_j$. The corresponding $(n, k, \vec{X})_F$-Shamir secret sharing is defined as follows.*

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

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

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

2.2 Physical-bit Leakage Function

In this paper, we study the physical-bit leakage. Let F be the prime field of order p. Recall that $2^{\lambda-1} \leqslant p < 2^{\lambda}$. For every element $a \in F$, we let a be an element in the set $\{0, 1, \ldots, p-1\}$. We shall use λ bits for the binary representation of a, i.e., $[a]_\lambda \, [a]_{\lambda-1} \cdots [a]_1$. In particular, we pad with a sufficient number of 0s if $a < 2^{\lambda-1}$. For example, when $\lambda = 5$ the binary representation of $a = 6$ is 00110.

of parties either witness perfect privacy, or the set of shares suffices to reconstruct the secret. A statistical notion of privacy is relevant when using non-linear codes instead. However, in our work we shall primarily study secret-sharing schemes based on Massey's construction from linear error-correcting codes. Consequently, we define perfect privacy only.

Definition 3. *An m-bit physical-bit leakage function $\vec{\tau} = (\tau_1, \dots, \tau_n)$ on $(n, k)_F$-secret sharing, leaks m bits from every share locally. This leakage function is specified by indices $u_1^{(i)}, \dots, u_m^{(i)}$, for all $1 \leqslant i \leqslant n$. Given the indices $u_1^{(i)}, \dots, u_m^{(i)}$, the leakage on the i^{th} share is the joint distribution*

$$\tau_i(\mathsf{Share}(s)_i) := \left([\mathsf{Share}(s)_i]_{u_1^{(i)}}, [\mathsf{Share}(s)_i]_{u_2^{(i)}}, \dots, [\mathsf{Share}(s)_i]_{u_m^{(i)}} \right).$$

Furthermore, $\vec{\tau}\,(\mathsf{Share}(s))$ denotes the collection of leakage from every share

$$(\tau_1(\mathsf{Share}(s)_1), \tau_2(\mathsf{Share}(s)_2), \dots, \tau_n(\mathsf{Share}(s)_n)).$$

2.3 Local Leakage-resilient Secret Sharing Scheme against Physical-bit Leakage

Definition 4 ($[\![n, k, m, \varepsilon]\!]_F$-LLRSS). *An $(n, k)_F$-secret sharing scheme* $(\mathsf{Share}, \mathsf{Rec})$ *is an $[\![n, k, m, \varepsilon]\!]_F$*-local leakage-resilient secret sharing scheme against m physical-bit leakage *(tersely represented as $[\![n, k, m, \varepsilon]\!]_F$-LLRSS), if it provides the following guarantee. For any two secrets $s_0, s_1 \in F$ and any physical-bit leakage function $\vec{\tau}$ that leaks m physical bits from every share locally, we have*

$$\mathsf{SD}\left(\vec{\tau}(\mathsf{Share}(s_0))\ ,\ \vec{\tau}(\mathsf{Share}(s_1))\right) \leqslant \varepsilon.$$

2.4 Generalized Reed-Solomon Code

Definition 5 ($(n, k, \vec{X}, \vec{\alpha})_F$-GRS). *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* evaluation places $\vec{X} = (X_1, \dots, X_n)$*, such that for all $1 \leqslant i \leqslant j \leqslant n$, $X_i \neq X_j$, and a* scaling vector $\vec{\alpha} = (\alpha_1, \dots, \alpha_n)$ *such that for all $1 \leqslant i \leqslant n$, $\alpha_i \in F^*$. Given $\vec{X}$ and $\vec{\alpha}$, the* encoding function *is*

$$\mathsf{Enc}(m_1, \dots, m_k) := (\alpha_1 \cdot f(X_1), \dots, \alpha_n \cdot f(X_n)),$$

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

In particular, the generator matrix of the linear $(n, k, \vec{X}, \vec{\alpha})_F$-GRS code is the matrix

$$\begin{pmatrix} \alpha_1 \cdot 1 & \alpha_2 \cdot 1 & \cdots & \alpha_n \cdot 1 \\ \alpha_1 \cdot X_1 & \alpha_2 \cdot X_2 & \cdots & \alpha_n \cdot X_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1 \cdot X_1^{k-1} & \alpha_2 \cdot X_2^{k-1} & \cdots & \alpha_n \cdot X_n^{k-1} \end{pmatrix}.$$

Observation 1 *The joint distribution of the secret-shares of an $(n, k, \vec{X})_F$-Shamir secret sharing with secret $s = 0$ is identical to the uniform distribution over the codewords in the $(n, k-1, \vec{X}, \vec{X})_F$-GRS code.*

The following standard properties of generalized Reed-Solomon codes shall be helpful.

Theorem 1 (Properties of GRS).

1. *The distance of the* $(n,k,\vec{X},\vec{\alpha})_F$*-GRS is* $(n-k+1)$ *(i.e., the linear code is maximum distance separable [32]).*
2. *The dual code of* $(n,k,\vec{X},\vec{\alpha})_F$*-GRS is identical to the* $(n,n-k,\vec{X},\vec{\beta})_F$*-GRS, where for all* $1 \leqslant i \leqslant n$*,*

$$\beta_i := \left(\alpha_i \prod_{\substack{j=1\\ j\neq i}}^{n} (X_i - X_j) \right)^{-1} .$$

The β_i's are the scalars from Lagrange interpolation. A proof for this theorem can be found in, for example, [31, 17].

2.5 Fourier Analysis Basics

In this paper, we shall use Fourier analysis on prime field F of order p. We follow the notation of [38]. Define $\omega := \exp(2\pi\imath/p)$. For any functions $f,g\colon F \to \mathbb{C}$, define

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

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.

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

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

3 Imported Theorems

3.1 Generalized Arithmetic Progressions

Our first imported theorem is on the ℓ_1-norm of the Fourier-coefficients of the indicator function of a generalized arithmetic progression.

Definition 6 (r-GAP). *Let F be a finite field. A subset $S \subseteq F$ is a* generalized arithmetic progression of rank r *(i.e., an r-GAP) if*

$$S = \{a_0 + a_1h_1 + a_2h_2 + \cdots + a_rh_r \,:\, 0 \leqslant h_i < H_i \text{ for every } 1 \leqslant i \leqslant r\},$$

where $a_0,\ldots,a_r \in F$ and $2 \leqslant H_1,\ldots,H_r \leqslant |F|$.

Furthermore, the set S is proper *if $|S| = H_1H_2\cdots H_r$.*

Intuitively, in a proper GAP every element in the set has a unique decomposition.

Shao [40] proved that for any proper r-GAP S, the ℓ_1-norm of the Fourier-coefficients of its indicator function $\mathbb{1}_S$ is small.

Imported Theorem 1 (Theorem 3.1 of [40])[10] *For every natural number r, there exists a constant $C_r > 0$ such that the following bounds holds for any proper r-GAP $S \subseteq F$.*

$$\sum_{\alpha \in F} \left| \widehat{\mathbb{1}_S}(\alpha) \right| \leqslant C_r \cdot \log(H_1) \cdots \log(H_r).$$

Shao [40] proved this result for vector spaces over F as well. However, we are importing the minimum result sufficient for our derivations.

In our setting, we are interested in a special type of proper 2-GAPs satisfying $a_1 = 1$ and $a_2 = 2H_1$. We carefully calculate the constant D_2 for this special case because a tight estimate itranslates into tight bounds on the insecurity of the cryptographic constructions. Our results are summarized in Theorem 2.

3.2 Number of Isolated Solutions of a Square Polynomial System

Our next imported theorem is regarding the number of the solutions of a square polynomial system. The specific version of Bézout's theorem that we are using is due to Wooley [42]. Before we present Wooley's theorem, let us introduce the minimal necessary definitions. For this part of the presentation, we follow the notations introduced by [10].

Definition 7 (Degree, Formal Derivative, Determinant, and Jacobian).

1. *Let F be a prime field. The* degree *of a monomial $X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}$ is $\sum_{\ell=1}^{n} i_\ell$. For a polynomial $f \in F[X_1, X_2, \ldots, X_n]$, the degree of f is the largest degree of its monomial.*
2. *Suppose*
$$f = g_t X_i^t + g_{t-1} X_i^{t-1} + \cdots + g_1 X_i + g_0,$$
where $g_0, \ldots, g_t \in F[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n]$. Then, the formal derivative of f with respect to X_i *is the polynomial in $F[X_1, X_2, \ldots, X_n]$ defined below.*
$$\frac{\partial f}{\partial X_i} := (t \cdot g_t) X_i^{t-1} + ((t-1) \cdot g_{t-1}) X_i^{t-2} + \cdots + (2 \cdot g_2) X_i + g_1.$$
3. *For a square matrix $M \in \Big(F[X_1, X_2, \ldots, X_n]\Big)^{k \times k}$,* $\det(M)$ *denotes the* determinant *of M defined as follows.*
$$\det(M) := \sum_{\substack{\sigma\colon \{1,2,\ldots,k\} \to \{1,2,\ldots,k\} \\ \sigma \text{ is a permutation}}} \operatorname{sgn}(\sigma) \cdot \prod_{i=1}^{k} M_{i,\sigma(i)},$$

[10] Note that, in the definition of [40], the Fourier coefficients are scaled by the field size compared to our definition.

where $\mathrm{sgn}(\sigma)$ *represents the* $\{+1,-1\}$ *sign of the permutation* σ.[11] *Note that* $\det(M) \in F[X_1, X_2, \ldots, X_n]$.

4. *For polynomials* $f_1, \ldots, f_k \in F[X_1, X_2, \ldots, X_n]$, *their* Jacobian *is*

$$\mathbf{J}(f_1, \ldots, f_k) := \begin{pmatrix} \frac{\partial f_1}{\partial X_1} & \frac{\partial f_2}{\partial X_1} & \cdots & \frac{\partial f_k}{\partial X_1} \\ \frac{\partial f_1}{\partial X_2} & \frac{\partial f_2}{\partial X_2} & \cdots & \frac{\partial f_k}{\partial X_2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial f_1}{\partial X_n} & \frac{\partial f_2}{\partial X_n} & \cdots & \frac{\partial f_k}{\partial X_n} \end{pmatrix}.$$

Intuitively, the Jacobian encodes information pertinent to the independence of a system of polynomials.

A *square polynomial system* has equal number of polynomials and the number of variables. That is, in the presentation above, we have $n = k$. The following theorem bounds the number of isolated solutions of a square polynomial system.

Imported Theorem 2 (Consequence of [42]) *Let* F *be a prime order field. Let* $f_1, \ldots, f_k \in F[X_1, \ldots, X_k]$ *such that the degree of* f_i *is* d_i. *The number of* $(x_1, \ldots, x_k) \in F^k$ *satisfying*

$$\begin{aligned} \forall 1 \leqslant i \leqslant k, \quad f_i(x_1, \ldots, x_k) = 0 & \qquad\qquad \textit{and} \\ \det\Big(\mathbf{J}(f_1, \ldots, f_k)\Big)(x_1, \ldots, x_k) \neq 0. & \end{aligned}$$

is at most $(d_1 d_2 \cdots d_k)$.

Wooley's theorem covers the case of polynomial congruence equations $\mod p^s$, where $s \geqslant 1$. However, we import the result that suffices for our derivations.

Intuitively, a root with high multiplicity also occurs as a root of the Jacobian. On the other hand, the isolated roots occur only in the polynomials but *not* in the Jacobian. This theorem presented above, provides an easy-to-verify test to count the isolated roots of a square polynomial system.

4 Physical-bit Witness Set as A Small Number of 2-GAPs

Let $1 \leqslant u \leqslant \lambda$ be an arbitrary index. Let $b \in \{0, 1\}$ be an arbitrary bit. We are interested in

$$A_{u,b} := \{a \in F \mid [a]_u = b\}.$$

We shall prove that for any u and b, $A_{u,b}$ is the disjoint union of (at most) λ number of 2-GAPs.

We first show that the prime field F can be partitioned as λ number of most-significant-bit-fixing sets, which is defined as follows.

[11] The sign of a permutation is $+1$ is an even number of swaps transform the permutation into the identity-permutation. Otherwise, the sign is -1.

Definition 8 (Most-significant-bit-fixing Set). *A set $S \subseteq F$ is called* most-significant-bit-fixing set *(MSB-fixing set) if there exists an index $1 \leqslant i^* \leqslant \lambda$ and a fixing $a_\lambda, a_{\lambda-1}, \dots, a_{i^*}$ such that S is identical to the following set.*

$$\left\{ b \in \{0,1\}^\lambda \;\middle|\; \forall i^* \leqslant i \leqslant \lambda,\ [b]_i = a_i \right\}.$$

For example, when $\lambda = 5$, the set $S = 01\{0,1\}^3$ (i.e., the bit-strings corresponding to the elements in the set $\{8, 9, 10, \dots, 15\}$) is an MSB-fixing set.

```
procedure PARTITION($F$)
    Let $\mathsf{index} = \lambda$.
    $\forall i \in \{1, 2, \dots, \lambda\}$, let $a_i = \perp$.
    while $\mathsf{index} > 1$ do
        if $\exists b \in F$ such that (1) $\forall \mathsf{index} + 1 \leqslant j \leqslant \lambda$, $[b]_j = a_j$ AND (2) $[b]_{\mathsf{index}} = 1$ then
            $F_{\mathsf{index}} := \left\{ b \;\middle|\; \forall \mathsf{index} + 1 \leqslant j \leqslant \lambda, [b]_j = a_j \text{ and } [b]_{\mathsf{index}} = 0 \right\}$
            $a_{\mathsf{index}} = 1$
        else
            $F_{\mathsf{index}} := \emptyset$
            $a_{\mathsf{index}} = 0$
        end if
        $\mathsf{index} = \mathsf{index} - 1$
    end while
    Until this point, $a_\lambda, a_{\lambda-1}, \dots, a_2$ are fixed. $a_1$ is still undetermined.
    Let $a^{(0)}$ be the integer whose binary representation is $a_\lambda, a_{\lambda-1}, \dots, a_2, 0$.
    Let $a^{(1)}$ be the integer whose binary representation is $a_\lambda, a_{\lambda-1}, \dots, a_2, 1$.
    if $a^{(1)} \leqslant p - 1$ then
        $F_1 := \{a^{(0)}, a^{(1)}\}$
    else
        $F_1 := \{a^{(0)}\}$
    end if
    return $F_\lambda, F_{\lambda-1}, \dots, F_1$
end procedure
```

Fig. 3. Given a finite field F, this procedure partitions F into MSB-fixing sets $F_\lambda, F_{\lambda-1}, \dots, F_1$.

Given a prime field F, Figure 3 demonstrates how to partition it as most significant bit-fixing sets. Easily, one can verify that $F_\lambda, F_{\lambda-1}, \dots, F_1$ are all MSB-fixing sets. For example, when $\lambda = 5$ and $p = 29$, the binary representations of the elements in $\{0, 1, \dots, 28\}$ partitions into subsets $0\{0,1\}^4$, $10\{0,1\}^3$, $110\{0,1\}^2$, and $\{11100\}$.

Now, given $A_{u,b}$, for $0 \leqslant i \leqslant \lambda$, define

$$A_i := A_{u,b} \cap F_i.$$

One can verify that A_i consists of all bit-strings such that the following conditions hold simutaneously. (1) Some of most significant bits are fixed, (2) the u^{th} least significant bit is fixed to b, and (3) finally, all the remaining positions are uniformly random. Continuing with the example above, the set $S_{2,0}$ is the subset of elements in S with their 2-nd LSB fixed to 0. That is, $S_{2,0} = 01\{0,1\}0\{0,1\}$, the binary representation of elements in the set $\{8, 9, 12, 13\}$. Therefore, one can write A_i as

$$A_i = \{a_0 + h_1 + a_2 h_2 \;:\; 0 \leqslant h_i < H_i \text{ for } i = 1, 2 \;\},$$

for some a_0, a_2, H_1, and H_2 such that $a_2 = 2H_1$ and $a_2 H_2 < p$. For example, the elements whose binary representation are in the set $S_{2,0}$ above can be expressed as the proper 2-GAP $8+\{0,1\}+\{0,4\}$. We have the following theorem regarding the ℓ_1-norm of the Fourier coefficient of such special type of 2-GAP sets.

Theorem 2. *Let p be a prime and*

$$S = \{a_0 + h_1 + a_2 h_2 \;:\; 0 \leqslant h_i < H_i \textit{ for } i = 1, 2\},$$

for some a_0, a_2, H_1, and H_2 such that $a_2 = 2H_1$ and $a_2 H_2 < p$. Then

$$\sum_{\alpha \in F} \left| \widehat{\mathbb{1}_S}(\alpha) \right| \leqslant (1 + o(1)) \cdot \left(\frac{2}{\pi}\right)^2 \cdot \log(H_1) \log(H_2).$$

We defer the proof of this theorem to the full version. This theorem immediately implies the following corollary.

Corollary 1. *For any index $1 \leqslant u \leqslant \lambda$ and bit $b \in \{0,1\}$,*

$$\sum_{\alpha \in F} \left| \widehat{\mathbb{1}_{A_{u,b}}}(\alpha) \right| \leqslant (1 + o(1)) \cdot \frac{1}{\pi^2} \cdot (\log p)^2 \cdot \lambda.$$

Proof. We have

$$\begin{aligned}
\sum_{\alpha \in F} \left| \widehat{\mathbb{1}_{A_{u,b}}} \right| &\leqslant \sum_{\alpha \in F} \sum_{i=1}^{\lambda} \left| \widehat{\mathbb{1}_{A_i}} \right| && \text{(Triangle inequality)} \\
&= \sum_{i=1}^{\lambda} \sum_{\alpha \in F} \left| \widehat{\mathbb{1}_{A_i}} \right| \\
&\leqslant \sum_{i=1}^{\lambda} (1 + \mathrm{o}(1)) \cdot \left(\frac{2}{\pi}\right)^2 \cdot \log(H_1) \log(H_2) && \text{(Theorem 2)} \\
&= (1 + \mathrm{o}(1)) \cdot \left(\frac{2}{\pi}\right)^2 \cdot \log(H_1) \log(H_2) \cdot \lambda \\
&\leqslant (1 + \mathrm{o}(1)) \cdot \left(\frac{2}{\pi}\right)^2 \cdot \left(\frac{\log(H_1) + \log(H_2)}{2}\right)^2 \cdot \lambda \\
& && \text{(AM-GM inequality)}
\end{aligned}$$

$$< (1 + \mathrm{o}(1)) \cdot \frac{1}{\pi^2} \cdot (\log p)^2 \cdot \lambda$$

The last inequality uses the fact that $H_1 \cdot H_2 < p$.

5 Physical-bit leakage on Shamir Secret Sharing

In this section, we prove the following theorems.

Theorem 3. *For any $\varepsilon > 0$, the following bound holds.*

$$\Pr_{\vec{X}}\left[\mathsf{ShamirSS}(n,k,\vec{X}) \textit{ is } \text{not} \textit{ an } [\![n,k,1,\varepsilon]\!]_F\textit{-LLRSS}\right] \lesssim \frac{1}{\varepsilon} \cdot \frac{2^n \cdot (\log p)^{3n} \cdot \lambda^n \cdot (k-1)!}{\pi^{2n} \cdot (p-n)^{k-1}}.$$

We emphasize that $\vec{X}$ is the uniform distribution over the set of all n-tuple of unique evaluation places in F^*.

Before we present the proof of this theorem, let us first interpret it through various parameter settings.

Corollary 2. *Let $0 < d < \ln 2$ be an arbitrary constant. There exists a (slightly) super-linear function $P(\cdot,\cdot)$ such that the following holds. For any number of parties $n \in \mathbb{N}$, reconstruction threshold $2 \leqslant k \in \mathbb{N}$, and insecurity tolerance $\varepsilon = 2^{-t}$, if the number of bits λ needed to represent the order of the prime-field F satisfies $\lambda > P(n/k, t/k)$, then $\mathsf{ShamirSS}(n,k,\vec{X})$ is an $[\![n,k,1,\varepsilon]\!]_F$-LLRSS with probability (at least) $1 - \exp(-d \cdot (k-1)\lambda)$.*

In particular, the (slightly super-linear) function $P(n/k, t/k) = d' \cdot \left(\frac{n}{k} + \frac{t}{k}\right) \cdot \log^2\left(\frac{n}{k} + \frac{t}{k}\right)$ suffices, for an appropriate universal positive constant d'.

In fact, our result can be generalized to multiple-bit physical leakage, which is summarized as follows.

Theorem 4. *For any $\varepsilon > 0$, for any positive integer m, the following bound holds.*

$$\Pr_{\vec{X}}\left[\mathsf{ShamirSS}(n,k,\vec{X}) \textit{ is } \text{not} \textit{ an } [\![n,k,m,\varepsilon]\!]_F\textit{-LLRSS}\right] \lesssim \frac{1}{\varepsilon} \cdot \binom{\log p}{m}^n \cdot \frac{2^{mn} \cdot (\log p)^{2mn} \cdot \lambda^{mn} \cdot (k-1)!}{\pi^{2n} \cdot (p-n)^{k-1}}.$$

We remark that this result extends to the setting that m_i bits are leaked from the i^{th} share for $i \in \{1, 2, \ldots, n\}$. In this case, the probability that $\mathsf{ShamirSS}(n,k,\vec{X})$ is not leakage resilient is bounded by

$$\frac{1}{\varepsilon} \cdot \binom{\log p}{m_1}\binom{\log p}{m_2} \cdots \binom{\log p}{m_n} \cdot \frac{2^M \cdot (\log p)^{2M} \cdot \lambda^M \cdot (k-1)!}{\pi^{2n} \cdot (p-n)^{k-1}},$$

where $M = \sum_{i=1}^n m_i$.

The proof of Theorem 4 is analogous to the proof of Theorem 3. Hence, we omit the proof of Theorem 4 and refer the reader to the full version for details.

Similarly, we interpret Theorem 4 as follows.

Corollary 3. *Let $0 < d < \ln 2$ be an arbitrary constant. There exists a (slightly) super-linear function $P(\cdot,\cdot)$ such that the following holds. For any number of parties $n \in \mathbb{N}$, reconstruction threshold $2 \leqslant k \in \mathbb{N}$, number of bits leaked from each share $m \in \mathbb{N}$, and insecurity tolerance $\varepsilon = 2^{-t}$, there exists $\lambda_0 = P\left(mn/k, t/k\right)$ such that if the number of bits λ needed to represent the order of the prime-field F satisfies $\lambda > \lambda_0$, then $\mathsf{ShamirSS}(n,k,\vec{X})$ is an $[\![n,k,m,\varepsilon]\!]_F$-LLRSS with probability (at least) $1 - \exp(-d \cdot (k-1)\lambda)$.*

In particular, function $P\left(mn/k, t/k\right) = d' \cdot \left(\frac{mn}{k} + \frac{t}{k}\right) \cdot \log^2\left(\frac{mn}{k} + \frac{t}{k}\right)$, for an appropriate universal positive constant d', suffices.

On the other hand, one can also interpret Theorem 4 as follows.

Corollary 4. *Let $0 < d < \ln 2$ be an arbitrary constant. For any number of parties $n \in \mathbb{N}$, reconstruction threshold $2 \leqslant k \in \mathbb{N}$, and insecurity tolerance $\varepsilon = 2^{-t}$, there exists $\lambda_0 = (t/k) \cdot \log(t/k)$ such that if the number of bits λ needed to represent the order of the prime-field F satisfies $\lambda > \lambda_0$, then for all m such that*

$$m \leqslant \frac{k\lambda}{n \log^2 \lambda},$$

it holds that $\mathsf{ShamirSS}(n,k,\vec{X})$ is an $[\![n,k,m,\varepsilon]\!]_F$-LLRSS with probability (at least) $1 - \exp(-d \cdot (k-1)\lambda)$.

5.1 Claims needed to prove Theorem 3

We prove Theorem 3 by proving the following claims.

In the first claim, we prove an upper bound on the statistical distance between the leakage of secrets s_0 and s_1. We emphasize that this upper bound is *not sensitive* to the actually secrets, but only sensitive to the leakage function $\vec{\tau}$ and evaluation places $\vec{X}$.

Claim 1 *Let $(\mathsf{Share}^{\vec{X}}, \mathsf{Rec}^{\vec{X}})$ be an $(n,k,\vec{X})$ Shamir secret sharing. Let $C_{\vec{X}}$ be the set of all possible secret shares of the secret 0.*[12] *Let $C_{\vec{X}}^{\perp}$ be the dual code of $C_{\vec{X}}$. For every 1-bit physical leakage function family $\vec{\tau} = (\tau_1, \tau_2, \ldots, \tau_n)$, for every leakage $\vec{\ell} \in \{0,1\}^n$, and for every pair of secrets s_0 and s_1, the following inequality holds.*

$$\mathsf{SD}\left(\vec{\tau}\left(\mathsf{Share}^{\vec{X}}(s_0)\right), \vec{\tau}\left(\mathsf{Share}^{\vec{X}}(s_1)\right)\right) \leqslant \sum_{\vec{\ell} \in \{0,1\}^n} \sum_{\vec{\alpha} \in C_{\vec{X}}^{\perp} \setminus \{0\}} \left(\prod_{i=1}^{n} \left|\widehat{\mathbb{1}_{\ell_i}}(\alpha_i)\right|\right).$$

[12] By Observation 1, $C_{\vec{X}}$ is an $(n, k-1, \vec{X}, \vec{X})$-GRS with generator matrix

$$\begin{pmatrix} X_1 & X_2 & \cdots & X_n \\ X_1^2 & X_2^2 & \cdots & X_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ X_1^{k-1} & X_2^{k-1} & \cdots & X_n^{k-1} \end{pmatrix}.$$

Here, we abuse the notation and use $\mathbb{1}_{\ell_i}$ to stand for the indicator function $\mathbb{1}_{\tau_i^{-1}(\ell_i)}$. That is, $\mathbb{1}_{\ell_i}(s_i) = 1$ if $\tau_i(s_i) = \ell_i$ and $\mathbb{1}_{\ell_i}(s_i) = 0$ otherwise.

Our next claim states that the average of the upper bound proven in Claim 1 over all evaluation places $\vec{X}$ is sufficiently small.

Claim 2 *Let* $(\mathsf{Share}^{\vec{X}}, \mathsf{Rec}^{\vec{X}})$ *be an* $(n, k, \vec{X})$ *Shamir secret sharing. For every* 1*-bit physical leakage function family* $\vec{\tau} = (\tau_1, \tau_2, \ldots, \tau_n)$*, the following inequality holds.*

$$\mathop{\mathrm{E}}_{\vec{X}}\left[\sum_{\vec{\ell}\in\{0,1\}^n}\ \sum_{\vec{\alpha}\in C_{\vec{X}}^{\perp}\setminus\{0\}}\left(\prod_{i=1}^{n}\left|\widehat{\mathbb{1}_{\ell_i}}(\alpha_i)\right|\right)\right] \lesssim \frac{2^n\cdot(\log p)^{2n}\cdot\lambda^n\cdot(k-1)!}{\pi^{2n}\cdot(p-n)^{k-1}}.$$

We defer the proofs to Section 5.3 and Section 5.4. We shall first present why these claims imply Theorem 3.

5.2 Proof of Theorem 3 using Claim 1 and Claim 2

By definition, we have

$$\begin{aligned}
&\Pr_{\vec{X}}\left[\mathsf{ShamirSS}(n,k,\vec{X}) \text{ is } \textit{not} \text{ an } [\![n,k,1,\varepsilon]\!]_F\text{-LLRSS}\right] \\
&= \Pr_{\vec{X}}\left[\exists s_0, s_1, \vec{\tau} \text{ s.t. } \mathsf{SD}\left(\vec{\tau}(\mathsf{Share}^{\vec{X}}(s_0))\ ,\ \vec{\tau}(\mathsf{Share}^{\vec{X}}(s_1)\right) \geqslant \varepsilon\right] \\
&\leqslant \Pr_{\vec{X}}\left[\exists s_0, s_1, \vec{\tau} \text{ s.t. } \sum_{\vec{\ell}\in\{0,1\}^n}\ \sum_{\vec{\alpha}\in C_{\vec{X}}^{\perp}\setminus\{0\}}\left(\prod_{i=1}^{n}\left|\widehat{\mathbb{1}_{\ell_i}}(\alpha_i)\right|\right) \geqslant \varepsilon\right] && \text{(Claim 1)} \\
&= \Pr_{\vec{X}}\left[\exists \vec{\tau} \text{ s.t. } \sum_{\vec{\ell}\in\{0,1\}^n}\ \sum_{\vec{\alpha}\in C_{\vec{X}}^{\perp}\setminus\{0\}}\left(\prod_{i=1}^{n}\left|\widehat{\mathbb{1}_{\ell_i}}(\alpha_i)\right|\right) \geqslant \varepsilon\right] \\
&\leqslant \sum_{\vec{\tau}}\Pr_{\vec{X}}\left[\sum_{\vec{\ell}\in\{0,1\}^n}\ \sum_{\vec{\alpha}\in C_{\vec{X}}^{\perp}\setminus\{0\}}\left(\prod_{i=1}^{n}\left|\widehat{\mathbb{1}_{\ell_i}}(\alpha_i)\right|\right) \geqslant \varepsilon\right] && \text{(Union bound)} \\
&\lesssim \sum_{\vec{\tau}}\frac{1}{\varepsilon}\cdot\frac{2^n\cdot(\log p)^{2n}\cdot\lambda^n\cdot(k-1)!}{\pi^{2n}\cdot(p-n)^{k-1}} && \text{(Markov's Inequality and Claim 2)} \\
&= (\log p)^n\cdot\frac{1}{\varepsilon}\cdot\frac{2^n\cdot(\log p)^{2n}\cdot\lambda^n\cdot(k-1)!}{\pi^{2n}\cdot(p-n)^{k-1}} \\
&\lesssim (\log p)^n\cdot\frac{1}{\varepsilon}\cdot\frac{2^n\cdot(\log p)^{2n}\cdot\lambda^n\cdot k!}{\pi^{2n}\cdot p^{k-1}} \\
&\sim \frac{k!}{\varepsilon}\cdot\left(\frac{2\lambda(\log p)^3}{\pi^2}\right)^n\cdot\frac{1}{2^{\lambda(k-1)}}.
\end{aligned}$$
[13]

This completes the proof of Theorem 3.

5.3 Proof of Claim 1

We start with the following calculation, which can be proven using standard techniques in Fourier analysis. We refer the readers to the full version for a proof.

Claim 3 *For any leakage* $\vec{\ell} \in \{0,1\}^n$*, we have*

$$\Pr_{\vec{s} \leftarrow \mathsf{Share}^{\vec{X}}(s)} \left[\vec{\tau}(\vec{s}) = \vec{\ell} \right] = \sum_{\vec{\alpha} \in C^{\perp}_{\vec{X}}} \left(\prod_{i=1}^{n} \widehat{\mathbb{1}_{\ell_i}}(\alpha_i) \right) \omega^{s(\alpha_1 + \cdots + \alpha_n)}.$$

Now, given Claim 3, Claim 1 can be proven as follows.

$$\begin{aligned}
&\mathsf{SD}\left(\vec{\tau}\left(\mathsf{Share}^{\vec{X}}(s_0) \right), \vec{\tau}\left(\mathsf{Share}^{\vec{X}}(s_1) \right) \right) \\
&= \frac{1}{2} \sum_{\vec{\ell} \in \{0,1\}^n} \left| \Pr_{\vec{s} \leftarrow \mathsf{Share}^{\vec{X}}(s_0)} \left[\vec{\tau}(\vec{s}) = \vec{\ell} \right] - \Pr_{\vec{s} \leftarrow \mathsf{Share}^{\vec{X}}(s_1)} \left[\vec{\tau}(\vec{s}) = \vec{\ell} \right] \right| \\
&= \frac{1}{2} \sum_{\vec{\ell} \in \{0,1\}^n} \left| \sum_{\vec{\alpha} \in C^{\perp}_{\vec{X}} \setminus \{0\}} \left(\prod_{i=1}^{n} \widehat{\mathbb{1}_{\ell_i}}(\alpha_i) \right) \left(\omega^{s_0(\alpha_1 + \cdots + \alpha_n)} - \omega^{s_1(\alpha_1 + \cdots + \alpha_n)} \right) \right| \\
&\hfill \text{(Claim 3)} \\
&\leqslant \frac{1}{2} \sum_{\vec{\ell} \in \{0,1\}^n} \sum_{\vec{\alpha} \in C^{\perp}_{\vec{X}} \setminus \{0\}} \left(\prod_{i=1}^{n} \left| \widehat{\mathbb{1}_{\ell_i}}(\alpha_i) \right| \right) \left| \omega^{s_0(\alpha_1 + \cdots + \alpha_n)} - \omega^{s_1(\alpha_1 + \cdots + \alpha_n)} \right| \\
&\hfill \text{(Triangle inequality)} \\
&\leqslant \frac{1}{2} \sum_{\vec{\ell} \in \{0,1\}^n} \sum_{\vec{\alpha} \in C^{\perp}_{\vec{X}} \setminus \{0\}} \left(\prod_{i=1}^{n} \left| \widehat{\mathbb{1}_{\ell_i}}(\alpha_i) \right| \right) \cdot 2 \\
&= \sum_{\vec{\ell} \in \{0,1\}^n} \sum_{\vec{\alpha} \in C^{\perp}_{\vec{X}} \setminus \{0\}} \left(\prod_{i=1}^{n} \left| \widehat{\mathbb{1}_{\ell_i}}(\alpha_i) \right| \right)
\end{aligned}$$

5.4 Proof of Claim 2

The proof of Claim 2 crucially relies on the following claim, which bounds the number of solutions to a polynomial system. We state and prove this claim first.

[13] We note that the $\lambda = \log_2 p$. However, in Theorem 2, the logrithm is natural log. Hence, we did not merge λ with $\log p$.

Claim 4 *Let $\vec{\alpha} = (\alpha_1, \alpha_2, \dots, \alpha_n)$ be a non-zero vector in F^n. Then the number of solutions $\vec{X} = (X_1, X_2, \dots, X_n) \in (F^*)^n$ of the equation $G_{\vec{X}} \cdot \vec{\alpha}^T = \vec{0}$ such that $X_i \neq X_j$ for every $1 \leqslant i < j \leqslant n$ is at most $(p-1)(p-2)\cdots(p-(n-k+1)) \cdot (k-1)!$. Here, $G_{\vec{X}}$ stands for the generator matrix of $C_{\vec{X}}$, which is*

$$G_{\vec{X}} = \begin{pmatrix} X_1 & X_2 & \cdots & X_n \\ X_1^2 & X_2^2 & \cdots & X_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ X_1^{k-1} & X_2^{k-1} & \cdots & X_n^{k-1} \end{pmatrix}.$$

Proof. Note that $G_{\vec{X}} \cdot \vec{\alpha}^T = \vec{0}$ implies that $\vec{\alpha} \in C_{\vec{X}}^{\perp}$. By Theorem 1, we know $C_{\vec{X}}^{\perp}$ has distance k, which implies that there are at least k non-zero coordinates in $\vec{\alpha}$. Therefore, without loss of generality, assume $\alpha_i \neq 0$ for every $1 \leqslant i \leqslant k-1$. Now, for $i = k, \dots, n$, we fix X_i to be arbitrary distinct non-zero values . Note that there are $(p-1)(p-2)\dots(p-(n-k+1))$ possible ways of doing this fixing. Let $c_i := \sum_{j=k+1}^{n} \alpha_j X_j^i$ for $i = 1, 2, \dots, k-1$. We can rewrite the equation $G_{\vec{X}} \cdot \vec{\alpha}^T = \vec{0}$ as a system of polynomial equations as follows.

$$\begin{aligned} f_1(X_1, X_2, \dots, X_{k-1}) &:= \alpha_1 X_1 + \alpha_2 X_2 + \ldots + \alpha_{k-1} X_{k-1} + c_1 = 0 \\ f_2(X_1, X_2, \dots, X_{k-1}) &:= \alpha_1 X_1^2 + \alpha_2 X_2^2 + \ldots + \alpha_{k-1} X_{k-1}^2 + c_2 = 0 \\ &\vdots \\ f_{k-1}(X_1, X_2, \dots, X_{k-1}) &:= \alpha_1 X_1^{k-1} + \alpha_2 X_2^{k-1} + \ldots + \alpha_{k-1} X_{k-1}^{k-1} + c_{k-1} = 0 \end{aligned}$$

Since $\alpha_i \neq 0$, it is a square polynomials system with $\deg(f_i) = i$, for every $1 \leqslant i \leqslant k-1$. Next, to apply Imported Theorem 2, we shall show that

$$\det\Big(\mathbf{J}(f_1, f_2, \dots, f_{k-1})\Big)(X_1, X_2, \dots, X_{k-1}) \neq 0 \text{ if } X_i \neq X_j \text{ for every } i \neq j.$$

We have

$$\mathbf{J}\Big(f_1, f_2, \dots, f_{k-1}\Big)(X_1, X_2, \dots, X_{k-1}) = \begin{pmatrix} \alpha_1 & 2\alpha_1 X_1 & \cdots & (k-1)\alpha_1 X_1^{k-2} \\ \alpha_2 & 2\alpha_2 X_2 & \cdots & (k-1)\alpha_2 X_2^{k-2} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{k-1} & 2\alpha_{k-1} X_{k-1} & \cdots & (k-1)\alpha_{k-1} X_{k-1}^{k-2} \end{pmatrix}$$

By the properties of determinant,

$$\begin{aligned} &\det\Big(\mathbf{J}\,(f_1, f_2, \dots, f_{k-1})\Big)(X_1, X_2, \dots, X_{k-1}) \\ &= \left(\prod_{i=1}^{k-1} \alpha_i\right) \cdot \det \begin{pmatrix} 1 & 2X_1 & \cdots & (k-1)X_1^{k-2} \\ 1 & 2X_2 & \cdots & (k-1)X_2^{k-2} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 2X_{k-1} & \cdots & (k-1)X_{k-1}^{k-2} \end{pmatrix} \end{aligned}$$

$$
\begin{aligned}
&= \left(\prod_{i=1}^{k-1} \alpha_i\right) (k-1)! \cdot \det \begin{pmatrix} 1 & X_1 & \cdots & X_1^{k-1} \\ 1 & X_2 & \cdots & X_2^{k-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & X_{k-1} & \cdots & X_{k-1}^{k-1} \end{pmatrix} \\
&\neq 0,
\end{aligned}
$$

since α_i are non-zeros and the Vandermonde matrix is full-rank. By Imported Theorem 2, there are at most $(k-1)!$ solutions for the above square polynomial system. Since there are total $(p-1)(p-2)\dots(p-(n-k+1))$ possible ways of fixing $X_k, X_{k+1}, \dots, X_n$, the number of solutions of the equation $G_{\vec{X}} \cdot \vec{\alpha}^T = \vec{0}$ is at most $(p-1)(p-2)\dots(p-(n-k+1)) \cdot (k-1)!$, which completes the proof of Claim 4.

Given Claim 4, we are ready to prove Claim 2 as follows.

$$
\begin{aligned}
&\mathop{\mathrm{E}}_{\vec{X}}\left[\sum_{\vec{\ell}\in\{0,1\}^n} \sum_{\vec{\alpha}\in C_{\vec{X}}^{\perp}\setminus\{0\}} \left(\prod_{i=1}^{n} \left|\widehat{\mathbb{1}_{\ell_i}}(\alpha_i)\right|\right)\right] \\
&= \sum_{\vec{\ell}\in\{0,1\}^n} \mathop{\mathrm{E}}_{\vec{X}}\left[\sum_{\vec{\alpha}\in C_{\vec{X}}^{\perp}\setminus\{0\}} \left(\prod_{i=1}^{n} \left|\widehat{\mathbb{1}_{\ell_i}}(\alpha_i)\right|\right)\right] \\
&= \sum_{\vec{\ell}\in\{0,1\}^n} \sum_{\vec{\alpha}\in F^n\setminus\{0\}} \left(\prod_{i=1}^{n} \left|\widehat{\mathbb{1}_{\ell_i}}(\alpha_i)\right|\right) \cdot \Pr_{\vec{X}}\left[\vec{\alpha}\in C_{\vec{X}}^{\perp}\right] \quad \text{(Linearity of expectation)} \\
&\leqslant \sum_{\vec{\ell}\in\{0,1\}^n} \sum_{\vec{\alpha}\in F^n\setminus\{0\}} \left(\prod_{i=1}^{n} \left|\widehat{\mathbb{1}_{\ell_i}}(\alpha_i)\right|\right) \cdot \frac{(p-1)(p-2)\cdots(p-(n-k+1))\cdot(k-1)!}{(p-1)(p-2)\cdots(p-n)} \\
&\qquad \text{(Claim 4)} \\
&\leqslant \sum_{\vec{\ell}\in\{0,1\}^n} \prod_{i=1}^{n} \left(\sum_{\alpha_i\in F} \left|\widehat{\mathbb{1}_{\ell_i}}(\alpha_i)\right|\right) \cdot \frac{(k-1)!}{(p-(n-k+2))\cdots(p-n)} \\
&\leqslant \sum_{\vec{\ell}\in\{0,1\}^n} \left((1+\mathrm{o}(1))\cdot\frac{1}{\pi^2}\cdot(\log p)^2\cdot\lambda\right)^n \cdot \frac{(k-1)!}{(p-(n-k+2))\cdots(p-n)} \\
&\qquad \text{(Corollary 1)} \\
&\lesssim 2^n \cdot \frac{(\log p)^{2n}\cdot\lambda^n\cdot(k-1)!}{\pi^{2n}\cdot(p-n)^{k-1}}.
\end{aligned}
$$

This gives us the desired upper bound.

6 Physical-bit leakage Attack on Shamir Secret-sharing Scheme

Consider the Shamir secret-sharing scheme with $< k$ degree polynomials, where $k \in \{2,3\}$, for n parties over a prime field F of order $p > 2$. Fix a secret $s \in F$. Suppose the random polynomial used for secret-sharing is $f(X) \in F[X]/X^k$ such that $P(0) = s$.

Suppose $p = 1 \mod k$, that is there exists a solution of the equation $Z^k - 1 = 0$ in the multiplicative group F^*. Let $\alpha \in F$ be such that $E := \{\alpha, \alpha^2, \ldots, \alpha^{k-1}, \alpha^k = 1\} \subseteq F^*$ be the multiplicative sub-group of order k containing all k solutions of the equation $Z^k - 1 = 0$.

Suppose $n \geqslant k$, and the evaluation places for the first k parties be $\{1, \alpha, \alpha^2, \ldots, \alpha^{k-1}\} \subseteq F^*$, respectively. Remaining evaluation places are inconsequential as we shall leak only one bit from the shares of only the first k parties.

Define $s_i := f(\alpha^i)$, for $1 \leqslant i \leqslant k$, to be the secret-share of party i. Observe that we have the following properties

1. The secret shares $s_1, \ldots, s_{k-1}$ are independently and uniformly random over the set F, and
2. The secret share $s_k = ks - (s_1 + \cdots + s_{k-1})$.

Let $0 \leqslant S_1, S_2, \ldots, S_k \leqslant p-1$ be the whole numbers (i.e., the set $\mathbb{N}_0 := \{0,1,2,\ldots\}$) corresponding to the elements $s_1, s_2, \ldots, s_k \in F$. Note that

$$\mathrm{E}[S_1 + S_2 + \cdots + S_{k-1}] = \mu := (k-1)(p-1)/2 \in \mathbb{N}.$$

Define $I_{k,\Delta} := \{\Delta+1, \Delta+2, \ldots, \Delta+p\}$, where $\Delta := \mu - (p-1)/2 - 1$. For $k \in \{2,3\}$, we note that

$$\Pr\left[\sum_{i=1}^{k-1} S_i \in I_{k,\Delta}\right] \geqslant 0.75.[14]$$

Express $\Delta = u \cdot p + \delta$, where $u \in \mathbb{N}_0$ (the set of all whole numbers), and $\delta \in \{0,1,\ldots,p-1\}$. Define the secret $s := k^{-1}\delta \in F$.

Following technical claim, which holds for any secret $s \in F$, is key to our attack strategy.

Claim (Parity of the "Parity of Shares"). Let $P \in \{0,1\}$ represent the LSB (or, equivalently, the parity) of ks when expressed as a whole number. For $1 \leqslant i \leqslant k$, let $P_i \in \{0,1\}$ represent the LSB (or, equivalently, the parity) of the secret share S_i. Define the following subsets of whole numbers

$$S_{\mathsf{same}} := \mathbb{N}_0 \cap \bigcup_{\substack{i \in \mathbb{Z} \\ i \text{ odd}}} [ip + ks + 1, (i+1)p + ks]$$

[14] One can explicit calculate the probability. When $k = 2$, $\Pr[S_1 \in I_{2,\Delta}] = 1$. When $k = 3$, $\Pr[S_1 + S_2 \in I_{3,\Delta}] = \frac{3}{4}\left(1 + \frac{1}{p} - \frac{1}{p^2}\right)$.

$$S_{\mathsf{diff}} := \mathbb{N}_0 \cap \bigcup_{\substack{i\in\mathbb{Z}\\ i \text{ even}}} [ip + ks + 1, (i+1)p + ks] .$$

If $S_1 + S_2 + \cdots + S_{k-1} \in S_{\mathsf{same}}$, then $P_1 \oplus P_2 \oplus \cdots \oplus P_k = P$. Otherwise, if $S_1 + S_2 + \cdots + S_{k-1} \in S_{\mathsf{diff}}$, then $P_1 \oplus P_2 \oplus \cdots \oplus P_k = 1 \oplus P$.

Proof. Since $s_1 + s_2 + \cdots + s_k = ks$, we have

$$S_1 + S_2 + \cdots + S_k = ks + ip,$$

for some $i \in \mathbb{N}_0$.

Observe that $P_1 \oplus P_2 \oplus \cdots \oplus P_k$ is the parity of $S_1 + S_2 + \cdots + S_k$, which is identical to the parity of ks (i.e., P) if and only if i is even.

Finally, since $S_k \in \{0, 1, \ldots, p-1\}$, the constraint "$S_1+S_2+\cdots+S_k = ks+ip$ for some even i" is equivalent to

$$S_1 + S_2 + \cdots + S_{k-1} \in S_{\mathsf{same}}.$$

The above claim gives us an attack for the case $k = 3$ because of the following argument.

Fix $k = 3$, the parity of ks is exactly the parity (LSB) of secret s. Observe that if u is odd, then $I_{k,\Delta} \subseteq S_{\mathsf{same}}$. In this case, the parity $P_1 \oplus P_2 \oplus \cdots \oplus P_k$ is identical to the LSB of the secret with probability > 0.75. Otherwise, if u is even then $I_{k,\Delta} \subseteq S_{\mathsf{diff}}$. In this case, the parity $P_1 \oplus P_2 \oplus \cdots \oplus P_k$ is the opposite to the LSB of the secret with probability > 0.75. In any case, since the adversary knows u, she can predict the LSB of the secret with probability > 0.75.

For a randomly chosen secret, on the other hand, one can predict the LSB (using the strategy above) only with probability (statistically close to) 0.5.

Remark 1. Let $\rho \in F$ be the primitive root of the equation $Z^p - 1 = 0$. That is, ρ is a generator for of the multiplicative group F^*. The discussion above holds for all evaluation places of the form

$$\left\{\rho^i \cdot \alpha, \rho^i \cdot \alpha^2, \ldots, \rho^i \cdot \alpha^k\right\},$$

where $i \in \{0, 1, \ldots, (p-1)/3\}$. More generally, let $G \subseteq F^*$ be the multiplicative subgroup formed by the roots of the equation $Z^k - 1 = 0$. Any coset F^*/G suffices for our purposes.

Consequently, there is not just one k-tuple of evaluation places that witnesses our attack. There are, in fact, $k! \cdot (p-1)/k$ such tuples that witness our attack.

Therefore, the following result holds.

Theorem 5. *Let F be a prime field of order $p > 2$. Consider any natural number n such that $p > n \geqslant k = 3$ and $p = 1 \mod k$. There exist distinct secrets $s^{(0)}, s^{(1)} \in F$, distinct evaluation places $X_1, \ldots, X_n \in F^*$, and one physical-bit local leakage function $\vec{\tau}$ such that, based on the leakage, an adversary can efficiently distinguish the secret being $s^{(0)}$ or $s^{(1)}$ with advantage $> 2 \cdot (0.75 - 0.5) = 0.5$.*

Remark 2. We emphasize that our attacker leaks one bit from the first k shares and tries to predict the secret based solely on this. In particular, we do not rely on the information regarding the remaining $n-k$ shares. Asymptotically, this approach is doomed to fail as k grows. As Benhamouda et al. [3] prove that, Shamir secret sharing is resilient to arbitrary one-bit leakage from each share, as long as $k \geqslant n - n^c$ for some small constant $c > 0$. Therefore, to find more devastating attacks, one has to utilize the fact that n is larger than k and we are leaking from every share.

6.1 Our Attack and Discrepancy of Irwin-Hall distribution

Consider any $2 \leqslant k \in \mathbb{N}$ and prime $p = 1 \mod k$. The following analysis is for the case when $p \to \infty$.

Observe that S_i is uniformly random over the set $\{0, 1, \ldots, p-1\}$. Instead of S_i, we normalize this random variable and consider $\widehat{S}_i$ that is uniformly random over the set $[0, 1) \subset \mathbb{R}$. Now, the random variable $S_1 + \cdots + S_{k-1}$ over whole numbers corresponds to the normalized distribution $\widehat{S}_1 + \cdots + \widehat{S}_{k-1}$ over the set $[0, k-1) \subset \mathbb{R}$. It is well-known that the sum of $(k-1)$ independent and uniform distributions over the unit interval $[0, 1)$ is the Irwin-Hall distribution [23, 18] with parameter $(k-1)$, represented by I_{k-1}.

Let $\delta \in [0, 1)$ be an offset. Define the intervals (as a function of δ)

$$\begin{aligned} \widehat{S}_{\mathsf{same}} &= (1+\delta, 2+\delta] \cup (3+\delta, 4+\delta] \cup (5+\delta, 6+\delta] \cup \cdots, \text{ and} \\ \widehat{S}_{\mathsf{diff}} &= (\delta, 1+\delta] \cup (2+\delta, 3+\delta] \cup (4+\delta, 5+\delta] \cup \cdots. \end{aligned}$$

Intuitively, these two sets correspond to the normalized S_{same} and S_{diff} sets defined above. The attack above corresponds to finding the offset

$$\delta^* := \operatorname*{argmax}_{\delta \in [0,1)} \left| \Pr\left[I_{k-1} \in \widehat{S}_{\mathsf{same}} \right] - \Pr\left[I_{k-1} \in \widehat{S}_{\mathsf{diff}} \right] \right|,$$

and the advantage corresponding to that attack is

$$\varepsilon^* := \max_{\delta \in [0,1)} \left| \Pr\left[I_{k-1} \in \widehat{S}_{\mathsf{same}} \right] - \Pr\left[I_{k-1} \in \widehat{S}_{\mathsf{diff}} \right] \right|.$$

Intuitively, this offset δ^* witnesses the largest discrepancy and, in turn, determines the most vulnerable secret.

Definition 9 (Discrepancy of a Probability Distribution). *Let X be a real-valued random variable. The* discrepancy *of the random variable X, represented by $\mathsf{disc}(X)$, is*

$$\mathsf{disc}(X) := \max_{\delta \in [0,1)} \left| 2 \cdot \Pr[X \in I(\delta)] - 1 \right|,$$

where $I(\delta)$ is the set $\delta + 2\mathbb{Z} + (0, 1]$.

Then, $\mathsf{disc}(I_{k-1})$ represents the advantage of our attack presented above, as $p \to \infty$.

References

1. 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.
2. 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.
3. 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.
4. Alexander R. Block, Divya Gupta, Hemanta K. Maji, and Hai H. Nguyen. Secure computation using leaky correlations (asymptotically optimal constructions). In Amos Beimel and Stefan Dziembowski, editors, *TCC 2018, Part II*, volume 11240 of *LNCS*, pages 36–65. Springer, Heidelberg, November 2018.
5. Alexander R. Block, Hemanta K. Maji, and Hai H. Nguyen. Secure computation based on leaky correlations: High resilience setting. In Jonathan Katz and Hovav Shacham, editors, *CRYPTO 2017, Part II*, volume 10402 of *LNCS*, pages 3–32. Springer, Heidelberg, August 2017.
6. 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.
7. 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.
8. Ignacio Cascudo, Ivan Damgård, Oriol Farràs, and Samuel Ranellucci. Resource-efficient OT combiners with active security. In Yael Kalai and Leonid Reyzin, editors, *TCC 2017, Part II*, volume 10678 of *LNCS*, pages 461–486. Springer, Heidelberg, November 2017.
9. Eshan Chattopadhyay, Jesse Goodman, Vipul Goyal, Ashutosh Kumar, Xin Li, Raghu Meka, and David Zuckerman. Extractors and secret sharing against bounded collusion protocols. In *61st FOCS*, pages 1226–1242. IEEE Computer Society Press, November 2020.
10. Xi Chen, Neeraj Kayal, and Avi Wigderson. *Partial Derivatives in Arithmetic Complexity and Beyond*, volume 6. 2011.
11. 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.
12. Alexandre Duc, Stefan Dziembowski, and Sebastian Faust. Unifying leakage models: From probing attacks to noisy leakage. In Phong Q. Nguyen and Elisabeth Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 423–440. Springer, Heidelberg, May 2014.
13. Matthew K. Franklin and Moti Yung. Communication complexity of secure computation (extended abstract). In *24th ACM STOC*, pages 699–710. ACM Press, May 1992.

14. 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.
15. 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.
16. Venkatesan Guruswami and Mary Wootters. Repairing reed-solomon codes. *IEEE Trans. Inf. Theory*, 63(9):5684–5698, 2017.
17. Jonathan I. Hall. Notes on coding theory, 2015.
18. Philip Hall. The distribution of means for samples of size n drawn from a population in which the variate takes values between 0 and 1, all such values being equally probable. *Biometrika*, pages 240–245, 1927.
19. Danny Harnik, Yuval Ishai, Eyal Kushilevitz, and Jesper Buus Nielsen. OT-combiners via secure computation. In Ran Canetti, editor, *TCC 2008*, volume 4948 of *LNCS*, pages 393–411. Springer, Heidelberg, March 2008.
20. Danny Harnik, Joe Kilian, Moni Naor, Omer Reingold, and Alon Rosen. On robust combiners for oblivious transfer and other primitives. In Ronald Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 96–113. Springer, Heidelberg, May 2005.
21. 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.
22. Carmit Hazay, Muthuramakrishnan Venkitasubramaniam, and Mor Weiss. The price of active security in cryptographic protocols. In Anne Canteaut and Yuval Ishai, editors, *EUROCRYPT 2020, Part II*, volume 12106 of *LNCS*, pages 184–215. Springer, Heidelberg, May 2020.
23. Joseph Oscar Irwin. On the frequency distribution of the means of samples from a population having any law of frequency with finite moments, with special reference to pearson's type ii. *Biometrika*, pages 225–239, 1927.
24. Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Extracting correlations. In *50th FOCS*, pages 261–270. IEEE Computer Society Press, October 2009.
25. Yuval Ishai, Hemanta K. Maji, Amit Sahai, and Jürg Wullschleger. Single-use ot combiners with near-optimal resilience. In *2014 IEEE International Symposium on Information Theory, Honolulu, HI, USA, June 29 - July 4, 2014*, pages 1544–1548. IEEE, 2014.
26. Yuval Ishai, Manoj Prabhakaran, Amit Sahai, and David Wagner. Private circuits II: Keeping secrets in tamperable circuits. In Serge Vaudenay, editor, *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 308–327. Springer, Heidelberg, May / June 2006.
27. Yuval Ishai, Amit Sahai, and David Wagner. Private circuits: Securing hardware against probing attacks. In Dan Boneh, editor, *CRYPTO 2003*, volume 2729 of *LNCS*, pages 463–481. Springer, Heidelberg, August 2003.
28. Yael Tauman Kalai and Leonid Reyzin. A survey of leakage-resilient cryptography. In Oded Goldreich, editor, *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*, pages 727–794. ACM, 2019.
29. 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.

30. 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, *1st Conference on Information-Theoretic Cryptography, ITC 2020, June 17-19, 2020, Boston, MA, USA*, volume 163 of *LIPIcs*, pages 7:1–7:24. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020.
31. Yehuda Lindell. Introduction to coding theory lecture notes, 2010.
32. Florence Jessie MacWilliams and Neil James Alexander Sloane. *The theory of error correcting codes*, volume 16. Elsevier, 1977.
33. Hemanta K. Maji, Anat Paskin-Cherniavsky, Tom Suad, and Mingyuan Wang. On leakage resilient secret sharing, 2020.
34. 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.
35. James L Massey. Some applications of code duality in cryptography. *Mat. Contemp*, 21(187-209):16th, 2001.
36. Remo Meier, Bartosz Przydatek, and Jürg Wullschleger. Robuster combiners for oblivious transfer. In Salil P. Vadhan, editor, *TCC 2007*, volume 4392 of *LNCS*, pages 404–418. Springer, Heidelberg, February 2007.
37. Jesper Buus Nielsen and Mark Simkin. Lower bounds for leakage-resilient secret sharing. In Anne Canteaut and Yuval Ishai, editors, *EUROCRYPT 2020, Part I*, volume 12105 of *LNCS*, pages 556–577. Springer, Heidelberg, May 2020.
38. Anup Rao. An exposition of bourgain's 2-source extractor. 2007.
39. Atle Selberg. An elementary proof of dirichlet's theorem about primes in an arithmetic progression. *Annals of Mathematics*, pages 297–304, 1949.
40. Xuancheng Shao. On character sums and exponential sums over generalized arithmetic progressions. *Bulletin of the London Mathematical Society*, 45(3):541–550, 2013.
41. 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.
42. Trevor D Wooley. A note on simultaneous congruences. *journal of number theory*, 58(2):288–297, 1996.