Security of Linear Secret Sharing Schemes with Noisy Side-Channel Leakage

Utkarsh Gupta and Hessam Mahdavifar

Northeastern University, Boston, MA, USA
{gupta.utk,h.mahdavifar}@northeastern.edu

Abstract. Secret sharing is a foundational cryptographic primitive for sharing secret keys in distributed systems. In a classical threshold setting, it involves a dealer who has a secret, a set of n users to whom shares of the secret are sent, and a threshold t which is the minimum number of shares required to recover the secret. These schemes offer an *all-or-nothing* security approach where less than t shares reveal no information about the secret. But these guarantees are threatened by side-channel attacks which can leak partial information from each share. Initiated by Benhamouda et. al. (CRYPTO'18), the security of such schemes has been studied for precise and worst-case bounded leakage models. However, in practice, side-channel attacks are inherently noisy. In this work, we propose a noisy leakage model for secret sharing, where each share is independently leaked to an adversary corrupted by additive noise in the underlying field $\mathbb{F}_q$. Under this model, we study the security of linear secret sharing schemes, and show bounds on the mutual information (MI) and statistical distance (SD) security metrics. We do this by using the MacWilliams' identity from the theory of error-correcting codes. For a given secret, it enables us to bound the the statistical deviation of the leaked shares from uniform as δ^t, where δ is the Fourier bias of the added noise. Existing analyses for the security of linear (n, t)-threshold schemes only bound the SD metric, and show resilience for schemes with $t \geq 0.668n$. In this work, we show that these constraints are artifacts of the bounded leakage model. In particular, we show that (n, t)-threshold schemes over $\mathbb{F}_q$ with $t \geq \tau(n + 1)$ leak $\mathcal{O}(q^{-2t(\gamma+1-1/\tau)})$ bits about the secret, given the bias of added noise satisfies $\delta \leq q^{-\gamma}$. To the best of our knowledge, this is the first attempt towards understanding the side-channel security of linear secret sharing schemes for the MI metric.

Keywords: Secret sharing · Side-channel leakage · Information-theoretic cryptography · Leakage-resilient cryptography.

1 Introduction

The design and analysis of cryptographic primitives often assume cryptosystems as impervious black-boxes. However, in real-world applications, adversaries can bypass theoretical security guarantees by exploiting the implementation and physical environment of these cryptosystems. Side-channel attacks constitute a class of cryptanalytic techniques that leverage the operational behavior of hardware systems such as power consumption, electromagnetic emanations etc. to reveal sensitive information. These attacks aim to leak partial information from the intermediate values involved in storage, computation, and communication. Side-channel attacks on fundamental cryptographic building blocks undermine the security guarantees of all computer systems that incorporate them. Motivated by the emergence of such attacks, protocols that attempt to provide provable security guarantees against side-channel attacks have attracted significant attention in the cryptographic community (survey [29]).

Secret sharing, introduced by Shamir [54] and Blakley [8], is a fundamental cryptographic primitive central to security in distributed systems. It protects against collusion by distributing *shares* of a secret among parties/users such that only specific subsets of users, called access structures, can reconstruct the secret by combining their shares. In the classical (n, t)-threshold setting, shares of the secret are distributed among n users such that all subsets of size at least t constitute the access structures. These schemes have found numerous applications such as in the domains of multi-party computation, zero-knowledge proofs, cryptographic masking etc. (survey [5]). Despite their adoption in several real-world systems, the impact of threshold and scalability on the security of secret sharing schemes is not fully understood. In this work, we study the security guarantees of (n, t)-threshold secret sharing schemes constructed using linear codes, where *noisy* version of each secret share are leaked to an adversary. In particular, we propose an additive noise leakage model where the adversary obtains each secret share corrupted by independent additive noise over the underlying field $\mathbb{F}_q$. This model generalizes the ϵ-Bernoulli noise model first studied by Faust et. al. [20].

Although the proposed model may seem unnatural from a perspective of cryptographic engineering, it is amenable to widely used mathematical techniques (such as Fourier analytical methods), while still offering a more general noisy leakage framework. Therefore, this work should be seen as a step in studying the resilience of cryptographic primitives with more realistic leakage models. Initiated by Chari et al. [12], the resilience of (n, n)-threshold schemes has been studied extensively against diverse noisy leakage models [3, 4, 9, 16, 17, 18, 19, 20, 21, 32, 44, 48]. But research in leakage-resilient (n, t)-threshold schemes has largely focused on models where the adversary can leak arbitrary bounded functions of the secret shares [6, 7, 30, 31, 35, 36, 37, 39, 46]. Such models characterize *worst-case* discrete leakage and do not directly capture real-world side-channel attacks [55, 56]. This results in conservative security guarantees and that too with severe constraints on the underlying field $\mathbb{F}_q$. In practice, side-channels are inherently noisy and techniques exist to amplify this noise [40]. Subsequently, the proposed model is more *relaxed*, and the security guarantees are dependent on side-channel noise. Furthermore, existing works usually prove formal security guarantees only for secret sharing schemes with thresholds $t > n/2$, even though schemes with $t \leq n/2$ are often used in practice. Therefore, understanding the security of schemes with general thresholds, and implemented over arbitrary finite fields, for noisy adversarial models is necessary.

1.1 Relation to Prior Work

In context of leakage resilience of (n, t)-threshold secret sharing, most research has focused on bounded leakage models [6, 7, 30, 31, 35, 36, 37, 39, 46]. Guruswami and Wootters' reconstruction algorithm [22, 23] showed that even a single *adversarial* bit leaked from each secret share compromises the security of Shamir's secret sharing scheme over fields of characteristic 2. This led Benhamouda et al. [6, 7] to investigate the leakage resilience of linear secret sharing schemes for other finite fields. They prove that the (n, t)-Shamir's scheme is leakage-resilient against one bit leakages, when the underlying field is of a large prime order, and $t \geq 0.92n$. This ratio has been progressively improved to 0.668 in a series of works by different authors [7, 30, 31, 34, 37]. For the noisy probing model, Adams et al. [1] proved that for additive secret-sharing schemes over a prime field where the prime requires λ-bits for its binary representation, k must be at least $\omega(\log \lambda / \log \log \lambda)$ to ensure security against even a single physical-bit leakage per share. However, a general drawback of such models is the restrictions required on the underlying field $\mathbb{F}_q$. For example, the state-of-art results by Kasser [30] require a prime field $\mathbb{F}$ with size $|\mathbb{F}| = \mathcal{O}(2^n)$. In another series of works [38, 39, 46], it was shown that Shamir's secret sharing scheme constructed using random evaluation points is almost always secure against physical probing attacks over finite fields irrespective of the field size or characteristic. This result seems to suggest that a (n, t)-threshold linear secret sharing with *random* leakage in finite fields might also be secure over all fields. In this work, we answer this affirmatively. Several works have focused on the resilience of (n, n)-threshold schemes against noisy, and consequently more practical leakage models [2, 3, 4, 9, 13, 17, 18, 19, 20, 21, 27, 28, 44, 48].

Information Leakage Measures. In cryptanalysis literature, mutual information (MI) is widely regarded as a fundamental metric for quantifying leakage in side-channel attacks [50, 55]. But all existing works studying leakage-resilient (n, t)-threshold secret sharing have only evaluated security guarantees in the statistical distance (SD) metric. For random variables corresponding to secret S and leakage L, $\mathrm{MI}(S; L)$ quantifies the information revealed about S from observing L by measuring the average reduction in uncertainty about S. The MI metric provides *operationally meaningful* insights, letting hardware engineers translate system design into measurable security guarantees. Motivated by the growing interest in using MI metric for evaluating security of leakage-resilient (n, n)-threshold schemes [2, 13, 17, 21, 28, 44], we adopt this metric to study side-channel leakage in (n, t)-threshold secret sharing. The MI and SD metrics are related by Pinsker's inequality and are formally discussed in Section 2.2.

1.2 Our Contributions

To understand the security guarantees of (n, t)-threshold schemes under the proposed leakage model, we begin by introducing some mathematical notation.

Linear Code-Based Secret Sharing. Let $\mathcal{M} \subseteq \mathbb{F}_q^{n+1}$ be a linear code over a finite field $\mathbb{F}_q$. The secret sharing scheme for n parties based on $\mathcal{M}$ is constructed as follows. Let the secret be $s \in \mathbb{F}_q$. Sample a random codeword $(s, u_1, \ldots, u_n) \in \mathcal{M}$, and assign the secret share u_i to the i^{th} user.

Additive Noise Leakage Model. In the proposed leakage model, each share is leaked to an adversary with i.i.d. additive noise over $\mathbb{F}_q$. The adversary obtains leaked shares $l_i = u_i + e_i$, where $e_i \in \mathbb{F}_q$ are sampled independently according to the noise random variable E. For $q = 2^\lambda$, this generalizes the ϵ-Bernoulli noise model introduced by Faust et. al. [20], where the adversary obtains each bit of every secret share with probability $1 - \epsilon$, and a flipped bit with probability ϵ.

Noise Parameter. The noise random variable E is parametrized by its Fourier bias, $\delta < 1$. This δ quantifies the deviation of E from the uniform distribution, and how evenly it randomizes the leaked shares l_i's. In particular, we have $\delta \leq \sum_{\alpha \in \mathbb{F}_q} |\Pr(E = \alpha) - 1/q|$. For the ϵ-Bernoulli noise model, regardless of the size of the binary extension field $q = 2^\lambda$, we have $\delta = 1 - 2\epsilon$.

For an (n, t)-threshold scheme, define the normalized threshold as $\tau = t/(n+1)$. Then, for some given noise parameter δ, the main result of this work (Theorem 3) can be informally stated as follows. Note that the MI metric is measured in bits.

Theorem 1 (Informal). *The mutual information (MI) leaked about the secret is $\mathcal{O}(q^{2(n+1-t)}\delta^{2t})$. For $\tau > 1/(1 - \log_q(\delta))$, the leaked information is $\mathcal{O}(2^{-\Omega(t)})$.*

Using the Pinsker's inequality, bounds on MI have been used to derive bounds on the SD-metric in Corollary 2. Consequently, we show that the insecurity of the Shamir's secret sharing scheme over fields of characteristic 2 [22, 23], is an artifact of the worst-case nature of the bounded leakage model. Theorem 1 shows that for a sufficiently small δ, linear secret sharing schemes are leakage resilient for arbitrarily small normalized thresholds τ. Countermeasures such as hiding, and noise amplification can be used to make the noise parameter δ smaller.

Corollary 1 (Informal). *For normalized threshold $\tau = t/(n+1)$, if $\delta \leq q^{-\gamma}$, where $\gamma > \frac{1}{\tau} - 1$, then the leakage from the secret for the MI metric is $\mathcal{O}(q^{\frac{1}{\tau} - 1 - \gamma})$.*

For the bounded leakage model, in a series of works [6, 7, 30, 31, 37, 39], Shamir's secret sharing scheme has been shown to be resilient only for $t \geq 0.668n$. However, as noted earlier, bounded leakage models do not translate into real-world side-channel attacks. In Section 3, we formally introduce the proposed leakage model, and discuss its theoretical motivation and connections to other works. Table 1 presents a comparison of the parameter constraints in this work with those in prior works on the security of linear (n, t)-threshold schemes.

1.3 Technical Overview

The extant analysis of leakage-resilient (n, t)-threshold secret sharing has been done using a Fourier analytic framework introduced in [6]. Most of these works [6, 7, 37] directly bound the statistical distance between leakage distributions corresponding to different secrets via a point-by-point analysis. However, the security analysis has been restricted to thresholds $t \geq 0.5n$ [30].

Table 1. Leakage models & constraints in works on security of (n,t)-threshold schemes.

Paper	**Scheme**	**Threshold** t	**Field** $\mathbb{F}_q$	**Leakage**
Beguinot et. al. [3]	Additive	$t = n$	Arbitrary	δ-noisy
Adams et. al. [1]	Shamir	$t = \omega(\log\lambda/\log\log\lambda)$	Prime $p < 2^{\lambda}$	Thermal
Maji et. al. [37]	MDS code	$t \geq 0.78n$	Prime $p > 5$	Bounded
Klein et. al. [31]	MDS code	$t \geq 0.69n$	Prime $p < 2^{o(n)}$	Bounded
Kasser [30]	MDS code	$t \geq 0.668n$	Prime $p < \mathcal{O}(2^n)$	Bounded
This work	Linear	$\frac{t}{n+1} > \frac{1}{1-\log_q(\delta)}$	Arbitrary	δ-additive

In this work, we will also conduct a point-by-point analysis. However, instead of bounding the SD metric, we use this analysis to bound the MI metric. Let $X \leftarrow x$ denote a random variable X, and its realization x. For a linear (n,t)-threshold scheme, let $S \leftarrow s \in \mathbb{F}_q$ be the secret, and the vector of noisy secret shares leaked to the adversary be $\mathbf{L} = (L_1, \ldots, L_n)$. We wish to bound $\mathrm{MI}(\mathrm{S};\mathbf{L})$. To do this, we will exploit the properties of the MI-metric. Under the proposed leakage model, the adversary receives each leaked share $L_i \leftarrow l_i = u_i + e_i$, perturbed by some noise $E \leftarrow e_i \in \mathbb{F}_q$. Recall that, for linear schemes, the coefficients of the secret recovery equations span an $[n,k,t]$ code $\mathcal{C} \subseteq \mathbb{F}_q^n$.

Intuitively, to recover the secret s, it would appear that the best strategy for the adversary would be to simply plug in the leaked shares in place of the actual secret shares, to obtain multiple estimates of the secret. This intuition has been formalized in Proposition 4 and Corollary 4, where we show that $\mathrm{MI}(S;\mathbf{L}) = \mathrm{MI}(S;\tilde{\mathbf{S}} = \mathbf{L}\mathcal{C}^{\top})$, where $\tilde{\mathbf{S}}$, the estimates of the secret and $\mathbf{L}\mathcal{C}^{\top}$ denote the the secret recovery equations with the 'plugged in' leaked shares. Now using the independent and additive nature of proposed noise model, $\mathrm{MI}(S;\mathbf{L}) = \mathrm{H}(\mathbf{L}\mathcal{C}^{\top}) - \mathrm{H}(\mathbf{E}\mathcal{C}^{\top})$, where $\mathbf{E} \sim E^{\otimes n}$. Since the code $\mathcal{C}$ has dimension k, $\mathrm{H}(\mathbf{L}\mathcal{C}^{\top}) \leq k\log_2(q)$. Therefore, all we are left to do is lower bound $\mathrm{H}(\mathbf{E}\mathcal{C}^{\top})$.

Lower bounding the entropy of $\mathbf{E}\mathcal{C}^{\top}$ is trying to characterize its deviation from the uniform distribution. Here we adopt a point-wise analysis approach, and in Lemma 4 show that $|\Pr(\mathbf{E}\mathcal{C}^{\top} = \mathbf{v}) - q^{-k}| \leq \delta^t$, where $\mathbf{v} \in \mathbb{F}_q^k$ and $\delta = \mathrm{bias}(E)$. To prove this bound, we first introduce the complete weight enumerator polynomial (cwe) from the theory of error correcting codes (Section 5). Then, we observe that the required probability is the same as the probability of the error vector lying in some coset of the dual code $\mathcal{C}^{\perp}$, which can be characterized by the cwe polynomial. Mathematically, $\Pr(\mathbf{E}\mathcal{C}^{\top} = \mathbf{v}) = \Pr(\mathbf{E} \in \mathbf{w} + \mathcal{C}^{\perp}) = cwe_{\mathbf{w}+\mathcal{C}^{\perp}}(\mu_0, \ldots, \mu_{q-1})$, where $\mu_i = \Pr(E = \alpha_i \in \mathbb{F}_q)$. To get the pointwise bound, we finally invoke the MacWilliams' identity (Proposition 1), which is a well-known result lying in the intersection of coding theory and Fourier analysis. The MacWilliams identity relates the cwe polynomial of a code to that of its dual, with the coefficients transformed via the discrete Fourier transform, i.e. $cwe_{\mathcal{C}^{\perp}}(\mu_0, \ldots, \mu_{q-1}) = q^{-k} cwe_{\mathcal{C}}(\widehat{\mu_0}, \ldots, \widehat{\mu_{q-1}})$. Therefore, the minimum weight of code $\mathcal{C}$, and the Fourier bias δ appear naturally in the expression for $|\Pr(\mathbf{E}\mathcal{C}^{\top} = \mathbf{v}) - q^{-k}|$. Intuitively, since the minimum weight of the code $\mathcal{C}$ is t, we expect this bound to resemble the addition of t independent $E_i \sim E$'s.

To finally lower bound $\mathrm{H}(\mathbf{E}\mathcal{C}^\top)$, we now simply exploit the Taylor expansion of the entropy function by using $-\ln(q^{-k}+x) \geq 1 - q^k x/(k \ln q)$. This gives us the final expression in the main result of this work, Theorem 3. By Pinsker's inequality, bounds on mutual information directly yield bounds on statistical distance. Specifically, we use $\mathrm{SD}(\mathbf{L}/S = s_0; \mathbf{L}/S = s_1) \leq \sqrt{2 \log_e 2 \cdot \mathrm{MI}(S;\mathbf{L})}$. These results have been discussed in Section 4 (see Theorem 3 and Corollary 2).

1.4 Outline

The remainder of this paper is structured as follows. In Section 2, we recall the preliminaries, including information leakage measures such as mutual information and statistical distance, and the procedure of constructing linear secret sharing schemes from linear error-correcting codes. Additionally, we discuss the construction of Shamir's secret sharing scheme, which is a widely used linear secret sharing scheme. In Section 3, we formally introduce the additive noise leakage model and its relationship to other prior works. In Section 6, we present the main results of this paper, and provide a formal mathematical proof of the central result of this paper, Theorem 3. In Section 7, we investigate the practical implications of our findings, by discussing the relationship between SNR, i.e. signal-to-noise ratio, and the bounds on leakage presented in earlier sections. Finally, the paper is concluded in Section 8.

2 Preliminaries

In this Section, we present the preliminaries required to formally define the mathematical framework of side-channel leakage for linear secret sharing schemes that we consider in our analysis. The notations are given in Subsection 2.1. In Subsection 2.2, we recall the main information leakage measures used as security metrics in side-channel analysis. Then, in Subsection 2.3, we discuss the theory of error-correcting codes, and how they are used in construction of linear secret sharing schemes.

2.1 Notation

Let $\mathbb{F}_q$ be a finite field of order $q = p^d$, where $p \geq 2$ is a prime and $d \in \mathbb{Z}_+$. Let $\mathbb{F}_q^n$ denote the ambient vector space of vectors of length $n \in \mathbb{Z}_+$ over the field $\mathbb{F}_q$. Linear codes of length n over $\mathbb{F}_q$, are subspaces of $\mathbb{F}_q^n$, and are denoted by calligraphic letters, eg. $\mathcal{C} \subseteq \mathbb{F}_q^n$. When specifying a generator matrix for a linear code, we use the same calligraphic letter to denote the matrix associated with the code. For example, $\mathcal{C} \in \mathbb{F}_q^{k \times n}$ is understood as the generator matrix of the code $\mathcal{C}$. This notational overlap emphasizes the centrality of the generator matrix in defining the structure of the code, and any ambiguity is resolved contextually. The transpose of a matrix $A \in \mathbb{F}_q^{m \times n}$ will be denoted by $A^\top \in \mathbb{F}_q^{n \times m}$. The sets of values taken by random variables in this work will be discrete, and usually belong to $\mathbb{F}_q$. Random variables are denoted by uppercase letters, eg. X, and their realization will be denoted by the corresponding smallcase letter $X \leftarrow x$. For some discrete random variable X, its probability mass function (pmf) will be written as $p_X(x) = \Pr(X = x)$. The sets of values taken by the random vectors in this work will usually belong to some linear code over $\mathbb{F}_q$. Random vectors are denoted by boldface uppercase letters, eg. $\mathbf{X} = (X_1, \ldots, X_n)$, and their realization will be denoted by the corresponding boldface smallcase letter $\mathbf{X} \leftarrow \mathbf{x} = (x_1, \ldots, x_n)$. For some random vector $\mathbf{X}$, its probability mass function (pmf) will be written as $p_{\mathbf{X}}(\mathbf{x}) = \Pr(\mathbf{X} = \mathbf{x})$.

The Hamming weight of a vector $\mathbf{x} \in \mathbb{F}_q^n$, denoted by $\mathrm{wt}(\mathbf{x})$, is defined as the number of non-zero coordinates in the standard representation of $\mathbf{x}$, i.e., $wt(\mathbf{x} = (x_1, \ldots, x_n)) = \#\{x_j : x_j \neq 0, 1 \leq j \leq n\}$. We will use the standard inner product notation $\langle \cdot, \cdot \rangle$ to represent the dot product of two vectors over $\mathbb{F}_q$. For $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ and $\mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$, their dot product is defined as $\langle \mathbf{x}, \mathbf{y} \rangle = x_1 y_1 + \cdots + x_n y_n$. For a vector $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ and a random vector $\mathbf{V} = (V_1, \ldots, V_n)$ taking values in $\mathbb{F}_q^n$, we will extend this notation to represent a linear combination of random variables as $\langle \mathbf{x}, \mathbf{V} \rangle = x_1 V_1 + \cdots + x_n V_n$, which is a random variable taking values in $\mathbb{F}_q$. This notation, $\langle \cdot, \cdot \rangle$, is used to emphasize the structural similarity to standard vector operations, even when one of the vectors is random. For such a linear combination of random variables, the vector $\mathbf{x}$ is called the coefficient vector corresponding to equation $\langle \mathbf{x}, \mathbf{V} \rangle$.

2.2 Information Leakage Measures

Following [55], the evaluation of side-channel leakage can be broadly categorized into two types of metrics. First, *information-theoretic metrics* quantify the amount of information leaked through a side-channel, independent of any specific adversarial model. Second, *security metrics* evaluate the practical exploitability of this information by a concrete adversary. A key advantage of information-theoretic metrics is their universality, as they assume an adversary with unbounded computational power, providing an upper bound on the information leakage irrespective of implementation or attack complexity.

Entropy and Mutual Information. Let X be a discrete random variable with probability mass function $p_X(x)$. The base-q entropy of X, denoted by $\mathrm{H}_q(X)$, quantifies the uncertainty of X and is defined as:

$$\mathrm{H}_q(X) = -\sum_x p_X(x) \log_q p_X(x), \tag{1}$$

where the logarithm is taken to base q. For $q = 2$, the base is typically omitted, and $\mathrm{H}_q(X)$ is simply written as $\mathrm{H}(X)$, commonly measured in bits. The relationship between the two is given by $\mathrm{H}(X) = \log_2(q) \cdot \mathrm{H}_q(X)$. Mutual information between two random variables measures the reduction in uncertainty about X given knowledge of another random variable Y. For two random variables X and Y, the base-q mutual information, $\mathrm{MI}_q(X;Y)$, is defined as:

$$\mathrm{MI}_q(X;Y) = \mathrm{H}_q(X) - \mathrm{H}_q(X \mid Y). \tag{2}$$

For $q = 2$, we again omit the base, and $\mathrm{MI}(X;Y) = \log_2(q) \cdot \mathrm{MI}_q(X;Y)$. Mutual information satisfies the *data processing inequality*, which states that post-processing cannot increase the MI between two random variables:

Theorem 2 (Data Processing Inequality). *Let X, Y, Z be discrete random variables such that $X \to Y \to Z$ forms a Markov chain, then*

$$\mathrm{MI}(X;Z) \leq \mathrm{MI}(X;Y). \tag{3}$$

Statistical Distance. The statistical distance, also known as the total variation distance, measures the distinguishability between two probability distributions. For two distributions P and Q over the same domain $\mathcal{X}$, it is defined as

$$\mathrm{SD}(P,Q) = \frac{1}{2}\sum_{x\in\mathcal{X}} |P(x) - Q(x)|. \tag{4}$$

The well-known Pinsker's inequality relates SD and MI metrics. For any x_0, x_1,

$$\mathrm{SD}(Z/X = x_0, Z/X = x_1) \leq \sqrt{2\log_e 2 \cdot \mathrm{MI}(X;Z)}. \tag{5}$$

2.3 Codes and Linear Secret Sharing Schemes

It is well-known that several linear secret-sharing schemes (LSSS) can be constructed from linear error-correcting codes [10, 15, 42, 43, 45]. Massey utilized linear codes for secret sharing schemes and established the relationship between the access structure and the minimal codewords of the dual code of the underlying codes [42, 43]. The seminal Shamir's secret sharing scheme is a specific instance of Massey's secret sharing scheme, where the underlying construction relies upon Reed-Solomon codes [45]. We begin by reviewing the definition of linear error-correcting codes and dual codes.

Linear codes. A linear code $\mathcal{C}$ of length n over $\mathbb{F}_q$ is a subspace of the ambient vector space $\mathbb{F}_q^n$. Recall that weight of a vector $\mathbf{u} \in \mathbb{F}_q^n$, $wt(\mathbf{u})$, is the number of non-zero coordinates of $\mathbf{u}$. The minimum distance of a linear code is the smallest non-zero weight of a vector in $\mathcal{C}$. The notation $[n,k,d]_q$ represents a linear code of length n, dimension k, and minimum distance d, over the finite field $\mathbb{F}_q$. Vectors belonging to some code $\mathcal{C}$ are also called *codewords*.

Definition 1. *An $[n,k,d]_q$ code is a k-dimensional subspace $\mathcal{C} \subseteq \mathbb{F}_q^n$, with minimum distance d, where $d = \min\{\mathrm{wt}(\mathbf{c}) : \mathbf{c} \in \mathcal{C}, \mathbf{c} \neq \mathbf{0}\}$, with $\mathrm{wt}(\mathbf{c})$ denoting the Hamming weight of $\mathbf{c}$.*

A generator matrix of an $[n,k,d]_q$ code $\mathcal{C}$ is a matrix in $\mathbb{F}_q^{k\times n}$ whose rows span the subspace $\mathcal{C} \subseteq \mathbb{F}_q^n$. We use the same calligraphic letter $\mathcal{C}$ to denote the generator matrix of the code $\mathcal{C}$, where $\mathcal{C} \in \mathbb{F}_q^{k\times n}$. Any codeword $\mathbf{c} \in \mathcal{C}$ can be written as $\mathbf{c} = \mathbf{u}\mathcal{C}$ for some row vector $\mathbf{u} \in \mathbb{F}_q^k$. In Section 5, we recall MacWilliams' identity, which relates the weight distribution of a code $\mathcal{C}$ with its dual code $\mathcal{C}^\perp$ (Proposition 1). In Section 6, the MacWilliams' identity is used to prove Lemma 4, which is the main technical result of this paper.

Definition 2. *The dual of an* $[n, k, d]_q$ *code* $\mathcal{C}$ *is an* $[n, n-k, d^{\perp}]_q$ *code* $\mathcal{C}^{\perp}$*, defined as the orthogonal complement of* $\mathcal{C}$ *in* $\mathbb{F}_q^n$*. Formally,*

$$\mathcal{C}^{\perp} = \{\mathbf{v} \in \mathbb{F}_q^n : \langle \mathbf{v}, \mathbf{c} \rangle = 0 \textit{ for all } \mathbf{c} \in \mathcal{C}\},$$

where $\langle \cdot, \cdot \rangle$ *denotes the standard dot product over* $\mathbb{F}_q$*. The dual code* $\mathcal{C}^{\perp}$ *is a linear code of dimension* $n - k$ *and minimum distance* $d^{\perp}$*.*

Massey's Secret Sharing. Given a secret $s \in \mathbb{F}_q$ and a threshold $t \in \mathbb{Z}_+$, Massey's secret-sharing scheme for n users distributes secret shares $u_1, u_2, \dots, u_n \in \mathbb{F}_q$ among n users such that:

- the secret s is a linear combination of at least t shares;
- fewer than t shares reveal no information about the secret.

Such a scheme is constructed using a $[n+1, k+1]_q$ linear code $\mathcal{M} \subseteq \mathbb{F}_q^{n+1}$, where the dual code $\mathcal{M}^{\perp}$ is a $[n+1, n-k, t+1]_q$ code. For a secret $S \leftarrow s \in \mathbb{F}_q$, the scheme samples a uniformly random codeword $\mathbf{s} = (u_0, \dots, u_n) \in \mathcal{M}$ such that $u_0 = s$. The i-th share is defined as $u_i \in \mathbb{F}_q$ for $i \in \{1, 2, \dots, n\}$. Massey established the connection between the access structure of the secret-sharing scheme and the minimal codewords of the dual code $\mathcal{M}^{\perp}$ [42, 43]. Specifically, they showed that there exists a codeword $\mathbf{c} = (c_0, \dots, c_n) \in \mathcal{M}^{\perp}$ with $c_0 \neq 0$ and $\mathrm{wt}(\mathbf{c}) = t + 1$. Such a codeword is orthogonal to $\mathbf{s} \in \mathcal{M}$, i.e., $\langle \mathbf{s}, \mathbf{c} \rangle = 0$, corresponding to a secret recovery equation.

Let the secret shares' vector be denoted by $\mathbf{U} \leftarrow \mathbf{u} = (u_1, \dots, u_n) \in \mathbb{F}_q^n$. This vector is formed by deleting the first coordinate in each codeword of $\mathcal{M}$. The resulting code $\mathcal{U} \subseteq \mathbb{F}_q^n$ is a linear code of length n and is called a *punctured* code of $\mathcal{M}$. A Massey secret-sharing scheme with n users and threshold t, constructed using the codebook $\mathcal{M} \subseteq \mathbb{F}_q^{n+1}$, is denoted by $\mathrm{MasseySS}(n, t, \mathcal{M})$.

Definition 3. *Given* $\mathbf{v} = (v_1, \dots, v_n) \in \mathbb{F}_q^n$*, a linear combination of the secret shares* $\langle \mathbf{v}, \mathbf{U} \rangle = v_1 U_1 + \cdots + v_n U_n$ *is called a secret recovery equation if*

$$S = \langle \mathbf{v}, \mathbf{U} \rangle. \tag{6}$$

Given the $\mathrm{MasseySS}(n, t, \mathcal{M})$ scheme with threshold t, each secret recovery equation has at least t non-zero summands. Therefore, for every coefficient vector $\mathbf{v} \in \mathbb{F}_q^n$ corresponding to a secret recovery equation, we have $\mathrm{wt}(\mathbf{v}) \geq t$. An adversary with knowledge of the underlying codebook $\mathcal{M}$ has access to the coefficients of all secret recovery equations, and consequently, the linear combinations of these equations. The linear subspace spanned by these coefficient vectors is denoted as $\mathcal{C}_{\mathcal{M}}$. This subspace $\mathcal{C}_{\mathcal{M}}$ is a linear code of length n over $\mathbb{F}_q$.

Definition 4. *Let* $\mathcal{V}$ *be the set of coefficient vectors corresponding to all possible secret recovery equations, i.e.,* $\mathcal{V} = \{\mathbf{v} \in \mathbb{F}_q^n : \langle \mathbf{v}, \mathbf{U} \rangle = S\}$*. Let* $\mathcal{C}_{\mathcal{M}}$ *be the subspace of* $\mathbb{F}_q^n$ *spanned by the vectors in* $\mathcal{V}$*,*

$$\mathcal{C}_{\mathcal{M}} = \mathit{span}(\mathcal{V}) = \left\{ \sum_{i=1}^{k} \alpha_i \mathbf{v}_i : \mathbf{v}_i \in \mathcal{V}, \alpha_i \in \mathbb{F}_q, k \in \mathbb{Z}_+ \right\}. \tag{7}$$

Lemma 1 states that the minimum distance of the code $\mathcal{C}_{\mathcal{M}}$ is equal to the threshold t. In Section 6, we formally show how the bounds on the MI metric, for the information leaked about the secret, depend on the threshold t.

Lemma 1. *The code $\mathcal{C}_{\mathcal{M}}$ is an $[n, k, d]_q$ code with $k \leq n - t + 1$, and $d = t$.*

3 Leakage Model: Additive Noise in $\mathbb{F}_q$

In this section, we formally introduce the proposed noisy leakage model. The model assumes that an adversary receives each share corrupted by independent additive noise over $\mathbb{F}_q$. In Section 3.2, we discuss how this model generalizes the ϵ-Bernoulli noise model first studied by Faust et. al. [20], which itself is related to Chari's framework for modeling analog attacks [11]. Finally, we review other leakage models studied in leakage-resilient secret sharing in Section 3.3.

3.1 Mathematical Formulation

Consider the Massey's secret sharing scheme, $\text{MasseySS}(n, t, \mathcal{M})$, with n users, and threshold t, over a finite field $\mathbb{F}_q$. Let $S \leftarrow s$ denote the secret that is shared, and $\mathbf{U} \leftarrow \mathbf{u} = (u_1, \ldots, u_n) \in \mathbb{F}_q^n$ denote the secret shares' vector. Similar to other local leakage models studied in literature [6, 7], we assume

- the adversary obtains a *leaked* version of every secret share;
- information leaked to the adversary from each user is independent of the leakage from other users.

The leaked version of the secret shares' vector will be denoted by $\mathbf{L} \leftarrow \mathbf{l} = (l_1, \ldots, l_n)$. Let the leaked shares l_i be obtained from the secret shares u_i by adding independent noise $E_i \leftarrow e_i \in \mathbb{F}_q$. Let this random noise vector be $\mathbf{E} \leftarrow \mathbf{e} = (e_1, e_2, \ldots, e_n) \in \mathbb{F}_q^n$. Formally, the leaked shares' vector is given by

$$\mathbf{L} = \mathbf{U} + \mathbf{E}. \tag{8}$$

In Proposition 4, it is shown that to recover the secret $S \leftarrow s$ from the leaked secret shares' vector $\mathbf{L} \leftarrow \mathbf{l}$, it is sufficient to estimate s using the secret recovery equations, i.e. $\mathbf{l}\mathcal{C}_{\mathcal{M}}^{\top}$ is a sufficient statistic for estimating s from the vector $\mathbf{l}$. However, to quantify the information leaked, i.e. bound $\text{MI}(S; \mathbf{L})$, we will need $E_i \sim E$ to be i.i.d. copies of some random variable E over $\mathbb{F}_q$, i.e. $\mathbf{E} \sim E^{\otimes n}$.

3.2 Motivation

Noisy leakage models attempt to formalize the physical behavior of embedded devices by assuming that the adversary observes a noisy function of intermediate variables. To model analog leakage, such as in template attacks [12] and differential power analysis [41], Chari et al. [11] proposed the additive Gaussian noise model, wherein the adversary observes the Hamming weight of the target data corrupted by Gaussian noise in $\mathbb{R}$. In parallel, motivated by discrete wire-probing attacks, Ishai et al. [26] introduced the random probing model, in which each intermediate value is revealed to the adversary with probability ϵ or otherwise remains hidden. The ϵ-Bernoulli model studied by Faust et al. [20] occupies a position between these two frameworks: it is discrete in nature like the random probing model, but arises as a consequence of hard-decision decoding of analog leakage. The model proposed in this work generalizes the ϵ-Bernoulli noisy leakage model studied by Faust et al. [20] for leakage-resilient circuit compilers.

ϵ-Bernoullli Noisy Leakage Model. The leakage function reveals all the bits of every secret share to the adversary, perturbed by independent additive binomial noise. Formally, for some $\epsilon \in (0, 1/2]$, each bit is flipped with probability ϵ, and remains unchanged with probability $1-\epsilon$. This leakage model can be reduced to the proposed additive noise leakage model as follows. Consider the scheme $\mathrm{MasseySS}(n, t, \mathcal{M})$ over the binary extension field $\mathbb{F}_{2^\lambda}$. The additive noise model with i.i.d. leakage variable E having distribution $\Pr(\mathrm{E} = \mathrm{e}) = \epsilon^{\mathrm{wt(e)}}(1-\epsilon)^{\lambda-\mathrm{wt(e)}}$, where $e \in \mathbb{F}_{2^\lambda}$ is treated as a binary vector of length λ, is equivalent to the ϵ-Bernoullli noise model.

Channel Models in Information Theory. It is useful to contextualize side-channel models via their correspondence with canonical channels in information theory. In information theory, the erasure channel and the binary symmetric channel (BSC) are the two most widely studied channel frameworks for understanding the capacity of more general noisy channels [14]. The random probing model can be equivalently viewed as an erasure channel [3], and the ϵ-Bernoulli model corresponds to the BSC. For (n, n)-threshold schemes, it has been shown that most noisy discrete leakage models can be reduced to the random probing model [16]. The BSC plays a foundational role in theoretically modeling channels with discrete data corrupted by Gaussian noise in $\mathbb{R}$. Formally, consider an adversary who receives every bit of each secret share individually, and independently corrupted by additive noise $\eta \sim \mathcal{N}(0, \sigma^2)$, i.e., the j^{th} bit of the i^{th} secret share $u_i^{(j)} \in \{0, 1\}$ is received as $u_i^{(j)} + \eta$. If this adversary performs hard-decision Maximum Likelihood estimation of every received bit, then the adversarial model is equivalent to the ϵ-Bernoulli noise model, where $\epsilon = \frac{1}{2}\operatorname{erfc}\left(\frac{1}{2\sqrt{2}\sigma}\right)$ [51]. Although such a leakage model is significantly stronger than Chari's model (where the adversary only receives the corrupted Hamming weight), ML estimation severely limits the adversary's ability. Since the erasure channel has proven useful in analyzing discrete leakage, it is natural to ask whether the BSC model can give insights in understanding analog leakage attacks, particularly the practically relevant model of Chari. This makes the proposed model worth studying.

3.3 Other Leakage Models

Substantial research has been conducted in recent years to analyze the security of (n, t)-threshold schemes against various models of leakage attacks [1, 6, 7, 24, 31, 34, 35, 36, 37, 38, 39, 47]. All these models have been motivated by capturing wire probing side-channel attacks, whose framework was first introduced by Ishai et al. [26]. Such attacks are discrete in nature, and allow adversaries to observe intermediate values during computation by targeting specific hardware wires.

Probing Models in (n,t)-Secret Sharing. Motivated by the λ-probing model [26], leakage-resilience of (n,t)-threshold schemes has been studied against adversaries who can leak precise outputs from each secret share [6, 7, 31, 35, 36, 37, 39]. The works of Benhamouda et al. [6], and Nielsen and Simkin [47], assume each share leaks information independently through arbitrary leakage functions with bounded output-length. Maji et. al. [34], and Adams et. al. [1], consider probing attacks which leak physical-bits from the memory hardware storing these shares. In a separate work [35], Maji et al. consider joint leakage, where the adversary can leak any bounded output-length joint function of the shares.

Noisy Leakage Models in Secret Sharing. A large body of work has studied the security of (n,n)-threshold schemes and circuit compilers for various noisy leakage models [2, 3, 4, 9, 13, 17, 18, 19, 20, 21, 27, 28, 44, 48]. The random probing model introduced by Ishai et. al. [26], and the δ-noisy leakage model introduced by Prouff and Rivian [52], are the most popular frameworks for modeling side-channel attacks in such schemes. In the δ-noisy leakage model, each secret share leaks information with a distortion parameter δ. For the MI metric, this is expressed as $\mathrm{MI}(U_i, L_i) \leq \delta$ for each secret share $u_i \leftarrow U_i$ and its leaked version $l_i \leftarrow L_i$. Several recent works have investigated δ-noisy leakage models in (n,n)-threshold schemes [3, 4, 9, 19, 21, 32, 44, 48]. Results by Duc. et. al. [16], relate the random probing model to the noisy leakage model in (n,n)-threshold schemes. Security guarantees were improved for both models in [3, 17, 44, 50]. Some recent studies have also focused on understanding the security of (n,t)-schemes under noisy leakage [1, 24], but their alignment with real-world side-channel attacks, or their more general theoretical relevance remains unclear.

4 Main Results

Consider the proposed additive noise leakage model (Section 3.1) for the Massey's secret sharing scheme, $\mathrm{MasseySS}(n,t,\mathcal{M})$, with n users, threshold t, over a finite field $\mathbb{F}_q$. Let $S \leftarrow s$ denote the secret that is shared, and $\mathbf{U} \leftarrow \mathbf{u} = (u_1, \ldots, u_n) \in \mathbb{F}_q^n$ denote the secret shares' vector. Let the additive noise vector be $\mathbf{E} \leftarrow \mathbf{e} = (e_1, e_2, \ldots, e_n) \in \mathbb{F}_q^n$, and the leakaed shares' vector $\mathbf{L} = \mathbf{U} + \mathbf{E}$. For the rest of this work, we will need $E_i \sim E$ to be i.i.d. copies of some random variable E over $\mathbb{F}_q$, i.e. $\mathbf{E} \sim E^{\otimes n}$. For a given E, we define the noise parameter δ, which we will use to characterize the security guarantees of $\mathrm{MasseySS}(n,t,\mathcal{M})$.

Definition 5 (Noise parameter δ). *For the additive noise variable E, we define the noise parameter as the Fourier bias of E, i.e. $\delta = \mathrm{bias}(E)$ (Definition 8).*

The noise parameter δ is measure of the deviation of E from the uniform distribution. If E is uniformly distributed, then the adversary receives each share uniformly randomly, i.e. $Pr(L_i = l_i) = 1/q$, and cannot reconstruct the secret.

In such a situation, the $\delta = 0$. In Lemma 2, we show that $\delta \leq 2\,\mathrm{SD}(E;U)$, where U is distributed uniformly over $\mathbb{F}_q$. For the ϵ-Bernoulli leakage model (Section 3.2), where the adversary receives each bit of every secret share flipped with probability ϵ, we have $\delta = 1 - 2\epsilon$ (Lemma 3).

Theorem 3. *For a* MasseySS$(n,t,\mathcal{M})$ *scheme over* $\mathbb{F}_q$*, with the additive noise leakage model, let* $\frac{t}{n+1} \geq \frac{1}{1-(1-\kappa)\log_q \delta}$ *for some* $\kappa < 1$*. Then*

$$\mathrm{MI}(S;\mathbf{L}) \leq \log_2(e)\, q^{2(n-t+1)}\delta^{2t} \leq \log_2(e)\, \delta^{2\kappa t}, \tag{9}$$

where $e \sim 2.718$ *is the Euler's number.*

The condition $\tau = t/(n+1) \geq \frac{1}{1-(1-\kappa)\log_q \delta}$ characterizes the condition on normalized threshold $\tau > 1/(1-\log_q \delta)$ for the given scheme to be secure against leakage with some known noise parameter δ. This condition is such that $\delta^{\kappa t} \geq q^{n-t+1}\delta^t$, i.e. $(\kappa-1)t\log_q \delta \geq (n-t+1)$. Therefore, the constant $\kappa < 1$ is a proof artifact which determines the rate of decay of the leaked information. Using the relationship between MI and SD metrics in (5), we get the following.

Corollary 2. *For a* MasseySS$(n,t,\mathcal{M})$ *scheme with the additive noise leakage model, let* $\frac{t}{n+1} \geq \frac{1}{1-(1-\kappa)\log_q \delta}$ *for some* $\kappa < 1$*. Then*

$$\mathrm{SD}(\mathbf{L}/S = s_0; \mathbf{L}/S = s_1) \leq \sqrt{2}q^{n-t+1}\delta^t \leq \sqrt{2}\delta^{\kappa t}. \tag{10}$$

4.1 Discussion

We now discuss the qualitative impact of design and noise parameters on the security of the implemented secret sharing schemes.

Threshold t. For bounded leakage models, Massey's scheme has been shown to be secure only when $t \geq 0.66n$ [30]. Using the bounds in Theorem 3, for any ratio of the threshold t and n, the Massey's secret sharing scheme is secure for a sufficiently small parameter δ. In particular, for a MasseySS$(n, t \geq c(n+1), \mathcal{M})$ scheme, the expression in Theorem 3 can be written in terms of c as follows.

Corollary 3. *For a* MasseySS$(n,t,\mathcal{M})$ *scheme with the additive noise leakage model, let* $t \geq \tau(n+1)$ *for some* $\tau < 1$*. Then for* $\delta \leq q^{-\gamma}$*, where* $\gamma > \frac{1}{\tau} - 1$*,*

$$\mathrm{MI}(S;\mathbf{L}) \leq \log_2(e)\, q^{-2t(\gamma+1-1/\tau)}. \tag{11}$$

To design secure schemes for small $\tau = t/(n+1)$, the noise parameter δ needs to be made very small. For example, to design secure schemes with $t = 0.5n$, we require $\delta \leq 1/q$. Corollary 3 provides us design inputs for choosing additional security measures (such as noise amplification) to protect each secret share.

Noise Parameter δ. Intuitively, the noise parameter δ can be considered to characterize the capabilities of the same adversary attacking different implementations of (t,n)-secret sharing schemes. The noise parameter δ is a measure of the deviation of the additive noise E from uniformly random noise. For instance,

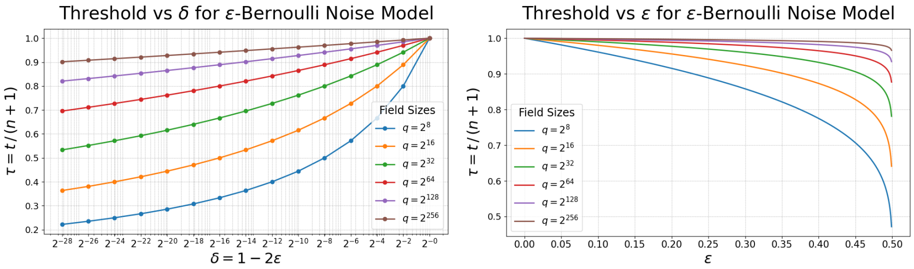

Fig. 1. For the ϵ-Bernoulli noise model over field $\mathbb{F}_q$, i.e. bit-flip probability ϵ, the noise parameter $\delta = 1 - 2\epsilon$. The figures represent the variation of normalized threshold $\tau = t/(n+1)$ with δ and ϵ. Note that for $\delta = 0$, i.e. $\epsilon = 1/2$, the adversary receives each share uniformly randomly, and therefore has no information to recover the secret.

consider the ϵ-Bernoulli noise model over some field $\mathbb{F}_{2^\lambda}$. As shown in Lemma 3, for the same adversary, the noise parameter $\delta = 1 - 2\epsilon$ remains constant regardless of the field size $q = 2^\lambda$. In practical implementations, such as for $q = 2^{32}$ and $\delta = 0.1$, i.e. $\epsilon = 0.45$, Theorem 3 yields the bound $t > 0.906n$, with security guarantees exponentially increasing as the the threshold moves closer to n.

Finite Field $\mathbb{F}_q$. The bounds presented in Theorem 3, do not require any constraints on the size or characteristic of the field $\mathbb{F}_q$. In contrast to the additive noise model, the Shamir's secret sharing scheme is known to be insecure against even 1-bit bounded leakage attacks in fields of characteristic 2. This seems to suggest that the insecurity of (n, t)-threshold schemes over $\mathbb{F}_{2^\lambda}$, is an artifact of the worst-case leakage functions considered in such models. Several results in leakage-resilience of Shamir's secret sharing require bounds on the size of field size. Our results suggest that the Shamir's scheme may be provably secure for noisy leakage models, over all finite fields, at least for large thresholds.

5 Mathematical Background

In this section, we introduce the mathematical background required to prove the main results presented in Section 4. We recall the theory of discrete Fourier transformation and the MacWilliams' identity for error-correcting codes.

Character Function and Fourier Transform. Let $\mathbb{C}$ be the field of complex numbers and $\mathbb{F}_q$ be a finite field with characteristic p, where $q = p^d$. Consider a primitive irreducible polynomial $f(x)$ of degree d over $\mathbb{F}_p$, and let λ be a root of $f(x)$. Then any element $\alpha \in \mathbb{F}_q$ can be uniquely expressed as $\alpha = \lambda_0 + \lambda_1\lambda + \cdots + \lambda_{d-1}\lambda^{d-1}$, where $\lambda_i \in \mathbb{F}_p$. Let α_i denote the elements of $\mathbb{F}_q$, i.e., $\mathbb{F}_q = \{\alpha_0, \ldots, \alpha_{q-1}\}$, such that $\alpha_0 = 0$.

Definition 6 (Character Function). *Let $\omega = e^{\frac{2\pi i}{p}} \in \mathbb{C}$ be a primitive p^{th} root of unity. The mapping $\chi : \mathbb{F}_q \to \mathbb{C}$, defined by $\chi(\alpha) = \omega^{\lambda_0}$, is called the canonical additive character of $\mathbb{F}_q$, where $\alpha = \lambda_0 + \lambda_1\lambda + \cdots + \lambda_{d-1}\lambda^{d-1}$.*

Definition 7 (Fourier Transform). *Let* $\mathbf{z} = (z_0, z_1, \ldots, z_{q-1}) \in \mathbb{C}^q$ *be a complex-valued vector indexed by elements of* $\mathbb{F}_q$*. The Fourier transform of* $\mathbf{z}$*, denoted by* $\widehat{\mathbf{z}} = (\widehat{z}_0, \widehat{z}_1, \ldots, \widehat{z}_{q-1}) \in \mathbb{C}^q$*, is defined as:*

$$\widehat{\mathbf{z}} = (\widehat{z}_0, \ldots, \widehat{z}_{q-1}) = \left(\sum_{j=0}^{q-1} \chi(\alpha_0 \alpha_j) z_j, \ldots, \sum_{j=0}^{q-1} \chi(\alpha_{q-1} \alpha_j) z_j \right). \tag{12}$$

We now introduce the notion of Fourier bias of a random variable. Also called the spectral bias, it characterizes the deviation of a random variable from the uniform distribution. This intuition is captured in Lemma 2.

Definition 8 (bias). *Given a random variable* X *over* $\mathbb{F}_q$*, let* $\mathbf{p} = (p_0, \ldots, p_{q-1}) \in \mathbb{R}^q$ *be the vector with* $p_i := p_X(\alpha_i)$ *for* $0 \leq i < q$*. Then bias of* X *is defined as*

$$\mathrm{bias}(X) = \max_{i \neq 0} |\widehat{p}_i|, \tag{13}$$

where $\widehat{\mathbf{p}} = (\widehat{p}_0, \ldots, \widehat{p}_{q-1})$ *is the Fourier transform of* $\mathbf{p}$*.*

Lemma 2. *Given a random variable* X *over* $\mathbb{F}_q$*, let* p_{med} *denote the median and* $p_{\min}$ *the minimum of the multiset* $\{p_X(\alpha_i) : 0 \leq i < q\}$*. Then for all* $i \neq 0$*,*

$$\mathrm{bias}(X) \leq \sum_{j=0}^{q-1} |p_j - p_{med}| \leq \min\{2\,\mathrm{SD}(X; U), 1 - qp_{min}\}, \tag{14}$$

where U *is a uniformly distributed random variable over* $\mathbb{F}_q$*.*

Proof. Since χ is the canonical additive character, $\sum_{j=0}^{q-1} \chi(\alpha_i \alpha_j) = 0$, for $\alpha_i \neq 0$. This implies that $\widehat{p}_i = \sum_{j=0}^{q-1} \chi(\alpha_i \alpha_j) p_j = \sum_{j=0}^{q-1} \chi(\alpha_i \alpha_j)(p_j - c)$, for any $c \in \mathbb{C}$. Now using the triangle inequality, $|\widehat{p}_i| \leq f(c)$, where $f(c) = \sum_{j=0}^{q-1} |p_j - c|$. For a collection of real numbers, it is well known that $f(c)$ is minimized when c is the median [53]. Observe $f(1/q) = 2\,\mathrm{SD}(X; U)$ and $f(p_{min}) = 1 - qp_{min}$.

Lemma 3 ([49]). *For the* ϵ*-Bernoulli distribution of* E*, i.e., for a random variable* E *over* $\mathbb{F}_{2^\lambda}$*, such that* $Pr(E = e) = \epsilon^{\mathrm{wt}(e)}(1-\epsilon)^{\lambda - \mathrm{wt}(e)}$*,* $\mathrm{bias}(E) = 1 - 2\epsilon$*.*

Codes and Weight Enumerator Polynomials. Recall indexing of the field $\mathbb{F}_q = \{\alpha_0 = 0, \alpha_1, \ldots, \alpha_{q-1}\}$. For a vector $\mathbf{u} = (u_1, \ldots, u_n) \in \mathbb{F}_q^n$, let $\eta_i(\mathbf{u})$ denote the number of coordinates of $\mathbf{u}$ equal to α_i. Thus $\mathrm{wt}(\mathbf{u}) = n - \eta_0(\mathbf{u})$.

$$\eta_i(\mathbf{u}) = \#\{j : u_j = \alpha_i, 1 \leq j \leq n\}, \text{where } 0 \leq i \leq q-1.$$

The composition of vector $\mathbf{u}$, defined to be $\mathrm{comp}(\mathbf{u}) = (n_0(\mathbf{u}), \ldots, \eta_{q-1}(\mathbf{u}))$, is a natural generalization of Hamming weight. The information about the composition of vectors in a subset $\mathcal{V} \subseteq \mathbb{F}_q^n$ can be captured by the complete weight enumerator polynomial $\mathrm{cwe}_{\mathcal{V}} \in \mathbb{C}[z_0, \ldots, z_{q-1}]$.

Definition 9 (CWE Polynomial, [25]). *The complete weight enumerator polynomial of a subset* $\mathcal{V} \subseteq \mathbb{F}_q^n$, $\mathrm{cwe}_{\mathcal{V}} \in \mathbb{C}[z_0, \ldots, z_{q-1}]$, *is defined as*

$$\mathrm{cwe}_{\mathcal{V}}(z_0, \ldots, z_{q-1}) = \sum_{\mathbf{u} \in \mathcal{V}} \prod_{i=0}^{q-1} z_i^{\eta_i(\mathbf{u})}. \tag{15}$$

For an $[n, k, d]_q$ code $\mathcal{C}$ over $\mathbb{F}_q$ and its dual $\mathcal{C}^\perp$, the relationship between the complete weight enumerator polynomials of $\mathcal{C}$ and $\mathcal{C}^\perp$ is given by the MacWilliams' identity. Although it is rarely stated explicitly, the following form of MacWilliams' identity can be understood to be a consequence of the Parserval's identity.

Proposition 1 (MacWilliams' Identity, [33]). *For an* $[n, k]_q$ *code* $\mathcal{C}$ *over* $\mathbb{F}_q$ *and its dual code* $\mathcal{C}^\perp$, *let* $\mathbf{z} = (z_0, \ldots, z_{q-1}) \in \mathbb{C}^q$. *Then*

$$\mathrm{cwe}_{\mathcal{C}^\perp}(z_0, \ldots, z_{q-1}) = \frac{1}{q^k} \mathrm{cwe}_{\mathcal{C}}(\widehat{z}_0, \ldots, \widehat{z}_{q-1}), \tag{16}$$

where $\widehat{\mathbf{z}} = (\widehat{z}_0, \ldots, \widehat{z}_{q-1}) \in \mathbb{C}^q$ *is the Fourier transform of* $\mathbf{z}$ *(Definition 7).*

To characterize the the complete weight enumerator polynomial of a coset of the dual code $\mathbf{v} + \mathcal{C}^\perp$, one can imitate the proof for the weight distribution of non-linear codes in [33] (which is equivalent to using the Parserval's identity).

Proposition 2. *For an* $[n, k]$ *code* $\mathcal{C}$ *over* $\mathbb{F}_q$ *and its dual code* $\mathcal{C}^\perp$, *let* $\mathbf{z} = (z_0, \ldots, z_{q-1}) \in \mathbb{C}^q$. *Consider a vector* $\mathbf{v} \notin \mathcal{C}^\perp$. *If* $\mathcal{D}$ *is the* $[n, n-k+1]$ *code generated by* $\mathcal{C}^\perp$ *and* $\mathbf{v}$, *then*

$$\mathrm{cwe}_{\mathbf{v}+\mathcal{C}^\perp}(z_0, \ldots, z_{q-1}) = \frac{1}{q^k} \sum_{i=0}^{q-1} \chi(\alpha_i)\, \mathrm{cwe}_{\alpha_i \cdot \mathbf{w} + \mathcal{D}^\perp}(\widehat{z}_0, \ldots, \widehat{z}_{q-1}), \tag{17}$$

where codeword $\mathbf{w} \in \mathcal{C}$ *is such that* $\langle \mathbf{v}, \mathbf{w} \rangle = 1$.

6 Formal Security Proofs

In this section, we prove the main results of this work presented in Section 4. Intuitively, an adversary trying to recover the secret $s \leftarrow S$ would treat the leaked secret shares as the original shares. In the absence of any additional information, the best strategy for the adversary seems to be to plug these leaked shares into the secret recovery equations to obtain multiple estimates of s. In Proposition 4 and Corollary 4, we formalize this intuition by showing that for the additive noise leakage model, the estimates of s from secret recovery equations (captured by the estimation vector $\tilde{\mathbf{s}} = \mathbf{l}\mathcal{C}_{\mathcal{M}}^\top$) are a sufficient statistic to recover s from the leaked secret shares' vector $\mathbf{l}$. This is done by proving the Markov Chain in (18), and then using the data processing inequality (Theorem 2). We first begin by showing for a given secret s, all corresponding secret shares' vectors are equiprobable (Proposition 3). This follows from the fact that the $\mathrm{MasseySS}(n, t, \mathcal{M})$ scheme samples a uniformly random codeword $(u_0, \ldots, u_n) \in \mathcal{M}$ such that $u_0 = s$.

Proposition 3. *If two secret shares' vectors* $\mathbf{u}$ *and* $\mathbf{u}'$ *are such that both of them correspond to the same secret* $s \in \mathbb{F}_q$*, i.e.* $\mathbf{u}\mathcal{C}_{\mathcal{M}}^{\top} = \mathbf{u}'\mathcal{C}_{\mathcal{M}}^{\top}$*, then* $p_{\mathbf{U}}(\mathbf{u}) = p_{\mathbf{U}}(\mathbf{u}')$.

Proof. For some secret shares' vector $\mathbf{u}$ corresponding to some secret s, the coefficients $\mathbf{P} \leftarrow p = (s, p_1, \ldots, p_{t-1})$ are uniquely determined. Since the random variables S, and P_i's are independent, $p_{\mathbf{U}}(\mathbf{u}) = p_S(s)\prod_{i=1}^{t-1} p_{P_i}(p_i) = p_S(s)q^{1-t}$.

Proposition 4. *For a* $\mathrm{MasseySS}(N, t, \mathcal{M})$ *scheme over* $\mathbb{F}_q$*, let* $\mathcal{C}_{\mathcal{M}}$ *be the generator matrix of the code spanned by coefficients of the secret recovery equations. If* $\mathbf{L}$ *denotes the leaked secret shares' vector, then*

$$S \to \mathbf{L}\mathcal{C}_{\mathcal{M}}^{\top} \to \mathbf{L} \tag{18}$$

is a Markov chain.

Proof. Let $\tilde{\mathbf{s}} \in \mathbb{F}_q^k$ be a row vector of length k, which lies in the image of the matrix $\mathcal{C}_{\mathcal{M}}^{\top}$, i.e. the equation $\mathbf{l}\mathcal{C}_{\mathcal{M}}^{\top} = \tilde{\mathbf{s}}$ has a solution. We will refer to $\tilde{\mathbf{s}}$ as the estimation vector. To show the Markov chain in (18), we will show that $\Pr(\mathbf{L} = \mathbf{l}/S = s, \mathbf{L}\mathcal{C}_{\mathcal{M}}^{\top} = \tilde{\mathbf{s}})$, is equal for all $s \in \mathbb{F}_q$. Let $\mathcal{C}_{\mathcal{M}}$ be an $[n, k, t]_q$ code,

$$\begin{aligned}
\Pr(\mathbf{L} = \mathbf{l}/S = s, \mathbf{L}\mathcal{C}_{\mathcal{M}}^{\top} = \tilde{\mathbf{s}}) &= \frac{\Pr(\mathbf{L} = \mathbf{l}, S = s)}{\Pr(S = s, \mathbf{L}\mathcal{C}_{\mathcal{M}}^{\top} = \tilde{\mathbf{s}})} && (19)\\
&= \frac{\Pr(\mathbf{L} = \mathbf{l}, S = s)}{\sum_{\mathbf{l}:\mathbf{l}\mathcal{C}_{\mathcal{M}}^{\top} = \tilde{\mathbf{s}}} \Pr(\mathbf{L} = \mathbf{l}, S = s)} && (20)\\
&= \frac{\sum_{\mathbf{u}} p_{\mathbf{U}}(\mathbf{u})\Pr(\mathbf{L} = \mathbf{l}, S = s/\mathbf{U} = \mathbf{u})}{\sum_{\mathbf{l}:\mathbf{l}\mathcal{C}_{\mathcal{M}}^{\top} = \tilde{\mathbf{s}}} \Pr(\mathbf{L} = \mathbf{l}, S = s)} && (21)\\
&= \frac{\sum_{\mathbf{u}:S=s} p_{\mathbf{U}}(\mathbf{u})p_{\mathbf{E}}(\mathbf{l} - \mathbf{u})}{\sum_{\mathbf{l}:\mathbf{l}\mathcal{C}_{\mathcal{M}}^{\top} = \tilde{\mathbf{s}}} \sum_{\mathbf{u}:S=s} p_{\mathbf{U}}(\mathbf{u})p_{\mathbf{E}}(\mathbf{l} - \mathbf{u})} && (22)\\
&= \frac{\sum_{\mathbf{u}:S=s} p_{\mathbf{E}}(\mathbf{l} - \mathbf{u})}{\sum_{\mathbf{l}:\mathbf{l}\mathcal{C}_{\mathcal{M}}^{\top} = \tilde{\mathbf{s}}} \sum_{\mathbf{u}:S=s} p_{\mathbf{E}}(\mathbf{l} - \mathbf{u})}, && (23)
\end{aligned}$$

where (23) follows from (22) by Proposition 3. For some secret s, and an estimation vector $\tilde{\mathbf{s}}$, the summation $\sum_{\mathbf{u}:S=s} p_{\mathbf{E}}(\mathbf{l} - \mathbf{u}) = \sum_{\mathbf{e}:\mathbf{e}\mathcal{C}_{\mathcal{M}}^{\top} = \tilde{\mathbf{s}} - \mathbf{s}^{(k)}} p_{\mathbf{E}}(\mathbf{e})$, where $\mathbf{e} = \mathbf{l} - \mathbf{u}$, and $\mathbf{s}^{(k)} := (s, \ldots, s) \in \mathbb{F}_q^k$ denotes the all s-vector of length k. This summation is constant for all $\mathbf{l}$ which satisfy $\mathbf{l}\mathcal{C}_{\mathcal{M}}^{\top} = \tilde{\mathbf{s}}$. Therefore, we have that $\Pr(\mathbf{L} = \mathbf{l}/S = s, \mathbf{L}\mathcal{C}_{\mathcal{M}}^{\top} = \tilde{\mathbf{s}}) = 1/\#\{\mathbf{l} : \mathbf{l}\mathcal{C}_{\mathcal{M}}^{\top} = \tilde{\mathbf{s}}\} = q^{k-n}$.

For a given linear secret sharing scheme, the matrix of secret recovery equations $\mathcal{C}_{\mathcal{M}}$ is known. Therefore, $\mathbf{L}\mathcal{C}_{\mathcal{M}}^{\top}$ can be considered to be a function of $\mathbf{L}$, and hence $S \to \mathbf{L} \to \mathbf{L}\mathcal{C}_{\mathcal{M}}^{\top}$ is a Markov Chain. Using the data processing inequality twice, for this Markov chain and (18), we get the following corollary.

Corollary 4. *The statistic* $\mathbf{S}^{(k)} + \mathbf{E}\mathcal{C}_{\mathcal{M}}^{\top}$ *is sufficient for recovering* S *from the leaked secret shares in* $\mathbf{L} = \mathbf{U} + \mathbf{E}$*, i.e.,*

$$\mathrm{MI}(S; \mathbf{L}) = \mathrm{MI}(S; \mathbf{S}^{(k)} + \mathbf{E}\mathcal{C}_{\mathcal{M}}^{\top}),$$

where $\mathbf{S}^{(k)} := (S, \ldots, S) \leftarrow (s, \ldots, s) \in \mathbb{F}_q^k$ *denotes the all* S*-vector of length* k.

So far we have not used the assumption that the error random variables E_i are identically distributed. Since $\mathcal{C}_{\mathcal{M}}$ is an $[n,k,t]$ code, the linear map characterized by $\mathbf{E} \to \mathbf{E}\mathcal{C}_{\mathcal{M}}^{\top}$ is such that each output depends on at least t independent coordinates of $\mathbf{E}$. Therefore, for the probability distribution output of this linear map, we expect that any pointwise deviation from uniform can only occur when the biases across these coordinates combine coherently. Independence of coordinates should prevent additive accumulation of bias. In Lemma 4, we show that for $\mathbf{E} \sim E^{\otimes n}$, the output of this linear map is *almost* uniform. In particular, if $\delta = \text{bias}(E)$ denotes the Fourier bias of E, then the outputs of the linear map $\mathbf{E} \to \mathbf{E}\mathcal{C}_{\mathcal{M}}^{\top}$ deviate from the uniform distribution by at most δ^t.

Lemma 4. *For some arbitrary row vector $\mathbf{v} \in \mathbb{F}_q^k$ of length k,*

$$\left|\Pr(\mathbf{E}\mathcal{C}_{\mathcal{M}}^{\top} = \mathbf{v}) - q^{-k}\right| \leq \delta^t, \tag{24}$$

where the random error vector $\mathbf{E} \leftarrow \mathbf{e} = (e_1, \dots, e_n) \in \mathbb{F}_q^n$.

Proof. Let the probability mass of random variable E be given by $p_E(\alpha_j) = \mu_j$, where $\mathbb{F}_q = \{\alpha_0, \dots, \alpha_{q-1}\}$. Recalling the definition of $\eta_i(\mathbf{u})$ and $\text{wt}(\mathbf{u})$ from earlier, for $\mathbf{v} = \mathbf{0}$, and the complete weight enumerator polynomial (Definition 9)

$$\Pr(\mathbf{E}\mathcal{C}_{\mathcal{M}}^{\top} = \mathbf{0}) = \Pr(\mathbf{E} \in \mathcal{C}_{\mathcal{M}}^{\perp}) = \sum_{\mathbf{u} \in \mathcal{C}_{\mathcal{M}}^{\perp}} \prod_{i=0}^{q-1} \mu_i^{\eta_i(\mathbf{u})} = \text{cwe}_{\mathcal{C}_{\mathcal{M}}^{\perp}}(\mu_0, \mu_1, \dots, \mu_{q-1}).$$

Treating $\boldsymbol{\mu} = (\mu_0, \dots, \mu_{q-1}) \in \mathbb{R}^q$ as a vector in $\mathbb{C}^q$, and using the MacWilliams Theorem (Proposition 1),

$$\Pr(\mathbf{E} \in \mathcal{C}_{\mathcal{M}}^{\perp}) = \frac{1}{q^k} \text{cwe}_{\mathcal{C}_{\mathcal{M}}}(\widehat{\mu}_0, \dots, \widehat{\mu}_{q-1}) = q^{-k} \left(1 + \sum_{\substack{\mathbf{u} \in \mathcal{C}_{\mathcal{M}} \\ \mathbf{u} \neq 0}} \prod_{i=0}^{q-1} (\widehat{\mu}_i)^{\eta_i(\mathbf{u})} \right), \tag{25}$$

where $\widehat{\boldsymbol{\mu}} = (\widehat{\mu}_0, \dots, \widehat{\mu}_{q-1})$ is the Fourier transform of $\boldsymbol{\mu}$. In particular, since $\alpha_0 = 0 \in \mathbb{F}_q$, $\widehat{\mu}_0 = \mu_0 + \cdots + \mu_{q-1} = 1$, and $|\widehat{\mu}_i| \leq \text{bias}(E) = \delta$ (Definition 8). Recall from Lemma 1, that $\mathcal{C}_{\mathcal{M}}$ is an $[n,k,t]$ code, i.e., the size of codebook $\mathcal{C}_{\mathcal{M}}$ is q^k, and its minimum weight is the threshold t. Using this with (25),

$$\left|\Pr(\mathbf{E}\mathcal{C}_{\mathcal{M}}^{\top} = \mathbf{0}) - q^{-k}\right| = \frac{1}{q^k} \left| \sum_{\substack{\mathbf{u} \in \mathcal{C}_{\mathcal{M}} \\ \mathbf{u} \neq 0}} \prod_{i=0}^{q-1} (\widehat{\mu}_i)^{\eta_i(\mathbf{u})} \right| \leq \left(1 - \frac{1}{q^k}\right) \delta^t. \tag{26}$$

For $\mathbf{v} \neq \mathbf{0}$ the noise vector $\mathbf{E} \leftarrow \mathbf{e}$, lies in some coset $\mathbf{w} + \mathcal{C}_{\mathcal{M}}^{\perp}$,

$$\Pr(\mathbf{E}\mathcal{C}_{\mathcal{M}}^{\top} = \mathbf{v}) = \Pr(\mathbf{E} \in \mathbf{w} + \mathcal{C}_{\mathcal{M}}^{\perp}) = \text{cwe}_{\mathbf{w} + \mathcal{C}_{\mathcal{M}}^{\perp}}(\mu_0, \mu_1, \dots, \mu_{q-1}). \tag{27}$$

Let $\mathcal{D}$ be the $[n, n-k+1]$ code generated by $\mathcal{C}_{\mathcal{M}}^{\perp}$ and $\mathbf{w}$. Then $\mathcal{D}^{\perp}$ is an $[n, k-1]$ code, and a subcode of $\mathcal{C}_{\mathcal{M}}$, and therefore has size q^{k-1} and minimum distance at least t. Further let $\mathbf{z} \in \mathcal{C}_{\mathcal{M}}$ be a vector such that $\langle \mathbf{w}, \mathbf{z} \rangle = 1$. Using the MacWilliams-like identity from Proposition 2 and triangle inequality,

$$\begin{aligned}
\Pr(\mathbf{E}\mathcal{C}_{\mathcal{M}}^{\top} = \mathbf{v}) &= \frac{1}{q^k} \left(\sum_{i=0}^{q-1} \chi(\alpha_i) \mathrm{cwe}_{\alpha_i \cdot \mathbf{z} + \mathcal{D}^{\perp}} \left(\widehat{\mu}_0, \ldots, \widehat{\mu}_{q-1} \right) \right) \\
&= \frac{1}{q^k} \left(1 + \sum_{\substack{\mathbf{u} \in \mathcal{D}^{\perp} \\ \mathbf{u} \neq 0}} \prod_{i=0}^{q-1} (\widehat{\mu}_i)^{\eta_i(\mathbf{u})} + \sum_{i=1}^{q-1} \chi(\alpha_i) \sum_{\mathbf{u} \in \alpha_i \cdot \mathbf{z} + \mathcal{D}^{\perp}} \prod_{i=0}^{q-1} (\widehat{\mu}_i)^{\eta_i(\mathbf{u})} \right),
\end{aligned}$$

where $\widehat{\boldsymbol{\mu}} = (\widehat{\mu}_0, \ldots, \widehat{\mu}_{q-1})$ is the Fourier transform of $\boldsymbol{\mu}$. Since $\mathbf{z} \in \mathcal{C}$, and $\mathcal{D}^{\perp} \subset \mathcal{C}_{\mathcal{M}}$, the cosets of the form $\alpha \mathbf{z} + \mathcal{D}^{\perp}$, where $\alpha \in \mathbb{F}_q$, are all subsets of the code $\mathcal{C}_{\mathcal{M}}$. Since the minimum weight of $\mathcal{C}$ is t, for $\mathbf{u} \neq \mathbf{0}$ and $\mathbf{u} \in \alpha \mathbf{z} + \mathcal{D}^{\perp}$, $\mathrm{wt}(\mathbf{u}) \geq t$.

$$\begin{aligned}
\left| \Pr(\mathbf{E}\mathcal{C}_{\mathcal{M}}^{\top} = \mathbf{v}) - q^{-k} \right| &= \frac{1}{q^k} \left| \sum_{\substack{\mathbf{u} \in \mathcal{D}^{\perp} \\ \mathbf{u} \neq 0}} \prod_{i=0}^{q-1} (\widehat{\mu}_i)^{\eta_i(\mathbf{u})} + \sum_{i=1}^{q-1} \chi(\alpha_i) \sum_{\mathbf{u} \in \alpha_i \cdot \mathbf{z} + \mathcal{D}^{\perp}} \prod_{i=0}^{q-1} (\widehat{\mu}_i)^{\eta_i(\mathbf{u})} \right| \\
&\leq \frac{1}{q^k} \left| \sum_{\substack{\mathbf{u} \in \mathcal{C}_{\mathcal{M}} \\ \mathbf{u} \neq 0}} \prod_{i=0}^{q-1} (\widehat{\mu}_i)^{\eta_i(\mathbf{u})} \right| \\
&\leq \left(1 - \frac{1}{q^k} \right) \delta^t.
\end{aligned}$$

Proof of Theorem 3. In Corollary 4, we showed that the *secret estimation vector*, is a sufficient statistic for recovering the secret $S \leftarrow s$ from the noisy leaked secret shares. Equivalently, the amount of information leaked about the secret from the leaked versions of secret shares is the same as the amount of information leaked about the secret from the secret recovery equations. Similar to Corollary 4, let $\mathbf{S}^{(k)} := (S, \ldots, S) \leftarrow (s, \ldots, s) \in \mathbb{F}_q^k$ denote the all S random vector of length k. For the rest of this proof, we will use the entropy function with the base q^k, denoted by H_{q^k} (Section 2.2).

$$\begin{aligned}
\mathrm{MI}_{q^k}(S; \mathbf{L}) &= \mathrm{MI}_{q^k}(S; \mathbf{S}^{(k)} + \mathbf{E}\mathcal{C}_{\mathcal{M}}^{\top}) \\
&= \mathrm{H}_{q^k}(\mathbf{S}^{(k)} + \mathbf{E}\mathcal{C}_{\mathcal{M}}^{\top}) - \mathrm{H}_{q^k}(\mathbf{S}^{(k)} + \mathbf{E}\mathcal{C}_{\mathcal{M}}^{\top} / S) \\
&= \mathrm{H}_{q^k}(\mathbf{S}^{(k)} + \mathbf{E}\mathcal{C}_{\mathcal{M}}^{\top}) - \mathrm{H}_{q^k}(\mathbf{E}\mathcal{C}_{\mathcal{M}}^{\top}) \\
&\leq 1 - \mathrm{H}_{q^k}(\mathbf{E}\mathcal{C}_{\mathcal{M}}^{\top}).
\end{aligned}$$

For some positive real numbers $x, y \in \mathbb{R}_+$; let $x \pm y$ denote some real number $z \in [x - y, x + y]$. Now, using the distribution of $\mathbf{E}\mathcal{C}_{\mathcal{M}}^{\top}$ from Lemma 4, and the Taylor expansion of the q^k-ary entropy function,

$$\mathrm{H}_{q^k}(\mathbf{E}\mathcal{C}_{\mathcal{M}}^{\top}) = \mathrm{H}_{q^k}\left(\frac{1}{q^k} \pm \delta^t, \ldots, \frac{1}{q^k} \pm \delta^t \right) \geq 1 - \frac{q^{2k} \delta^{2t}}{\log_e q^k}. \tag{28}$$

Using $\frac{t}{n+1} \geq \frac{1}{1-(1-\kappa)\log_q \delta}$ for some $\kappa < 1$, and $k \leq n - t + 1$ from Lemma 1,

$$\log_q \left(q^k \delta^t\right) = k + t \log_q \delta \leq -t + \left(n + 1 + t \log_q \delta\right) \leq \kappa t \log_q \delta. \tag{29}$$

This implies $q^k \delta^t \leq \delta^{\kappa t}$, and we get the following bound on the leaked MI-metric,

$$\mathrm{MI}(S; \mathbf{L}) = \log_2 (q^k) \left(1 - \mathrm{H}_{q^k}(\mathbf{E}\mathcal{C}_{\mathcal{M}}^\top)\right) \leq \log_2 (e)\, q^{2k} \delta^{2t} \leq \log_2 (e)\, \delta^{2\kappa t}. \tag{30}$$

7 Numerical Results

We conclude by examining the practical implications of our findings. From Section 3.2, we will recall the relationship between the ϵ-Bernoulli noise model, and additive Gaussian noise in $\mathbb{R}$. Consider a MasseySS$(n, t, \mathcal{M})$ scheme over a binary extension field $\mathbb{F}_{2^\lambda}$. The secret s, and all the secret shares $U_i \leftarrow u_i = (u_i^{(1)}, \ldots, u_i^{(\lambda)}) \in \mathbb{F}_{2^\lambda}$ are represented using λ bits, where the j^{th} bit of the i^{th} secret share is $U_i^{(j)} \leftarrow u_i^{(j)} \in \{0, 1\}$. Consider an adversary who receives every bit of each secret share independently, perturbed with additive Gaussian noise $\mathcal{N}(0, \sigma^2)$, i.e. the adversary receives the j^{th} bit of the i^{th} leaked secret share as

$$l_i^{(j)} = u_i^{(j)} + \eta_i^{(j)}, \text{ where } \eta_i^{(j)} \sim \mathcal{N}(0, \sigma^2). \tag{31}$$

For analog leakage, the extent of leakage to an adversary is quantified by the signal-to-noise ratio (SNR) of the leakage function. SNR measures the ratio of the average signal energy per symbol to the noise energy per symbol received by the adversary, allowing the hardware engineer to link to the probability of successful guessing in the presence of additive Gaussian noise [57], to a physically measurable entity. In this setting, the SNR is defined as the ratio of the variance of the bit signal $u_i^{(j)} \in \{0, 1\}$, to the Gaussian noise variance σ^2, i.e.,

$$\mathrm{SNR} = \frac{\mathrm{Var}(u_i^{(j)})}{\sigma^2} = \frac{1}{4\sigma^2}.$$

Consider the additive Gaussian noise model by Chari et. al. [11], where the Hamming weight of each secret share is leaked with additive Gaussian noise $\mathcal{N}(0, \sigma_w^2)$, i.e., the adversary receives $\sum_{j=1}^{\lambda} u_i^{(j)} + \eta_w$, where $\eta_w \sim \mathcal{N}(0, \sigma_w^2)$. Then this model is strictly weaker than the bit-wise leakage model, where $\sigma_w^2 = \lambda \sigma^2$. For an adversary who performs hard-decision Maximum Likelihood (ML) estimation of each received bit, the adversary rounds each leakage value $l_i^{(j)}$ to the nearest bit in $\{0, 1\}$. This induces an effective bit-flip probability

$$\epsilon = \Pr\left(\mathcal{N}(0, \sigma^2) > 1/2\right) = \frac{1}{2} \operatorname{erfc}\left(\frac{1}{2\sqrt{2}\sigma}\right) = \frac{1}{2} \operatorname{erfc}\left(\sqrt{\frac{\mathrm{SNR}}{2}}\right), \tag{32}$$

where $\operatorname{erfc}(x) = \frac{2}{\sqrt{\pi}} \int_x^\infty e^{-u^2}\, du$. Therefore for an adversary doing ML estimation for every received bit, the model in which each bit is leaked with additive Gaussian noise $\mathcal{N}(0, \sigma^2)$, reduces to the ϵ-Bernoulli noise model.

Although most implementations of linear secret sharing schemes require the number of users n to be less than the field size q, this constraint does not apply to (n, n)-threshold schemes. In such schemes, the secret is typically represented as the sum of independently and uniformly sampled shares from $\mathbb{F}_q$. The adversary's gain in guessing probability over random guessing is at most twice the SD-metric. From Corollary 2, this gain is upper bounded by $2\sqrt{2}q^{n-t+1}\delta^t$. For binary extension fields $\mathbb{F}_{2^\lambda}$ under the ϵ-Bernoulli model, Lemma 3 and equation (32) give $\delta = 1 - 2\epsilon = 1 - \mathrm{erfc}(\sqrt{\mathrm{SNR}/2})$. Applying Theorem 3, we obtain the plots in Figure 2, which show mutual information leakage and gain in guessing probability versus adversary SNR. Specifically, for (n, n)-threshold schemes, mutual information leakage is bounded by $\log_2(e)\, 2^{2\lambda}(1 - \mathrm{erfc}(\sqrt{\mathrm{SNR}/2}))^{2n}$, and the gain in guessing probability is bounded by $2^{\lambda+1}\sqrt{2}(1 - \mathrm{erfc}(\sqrt{\mathrm{SNR}/2}))^n$.

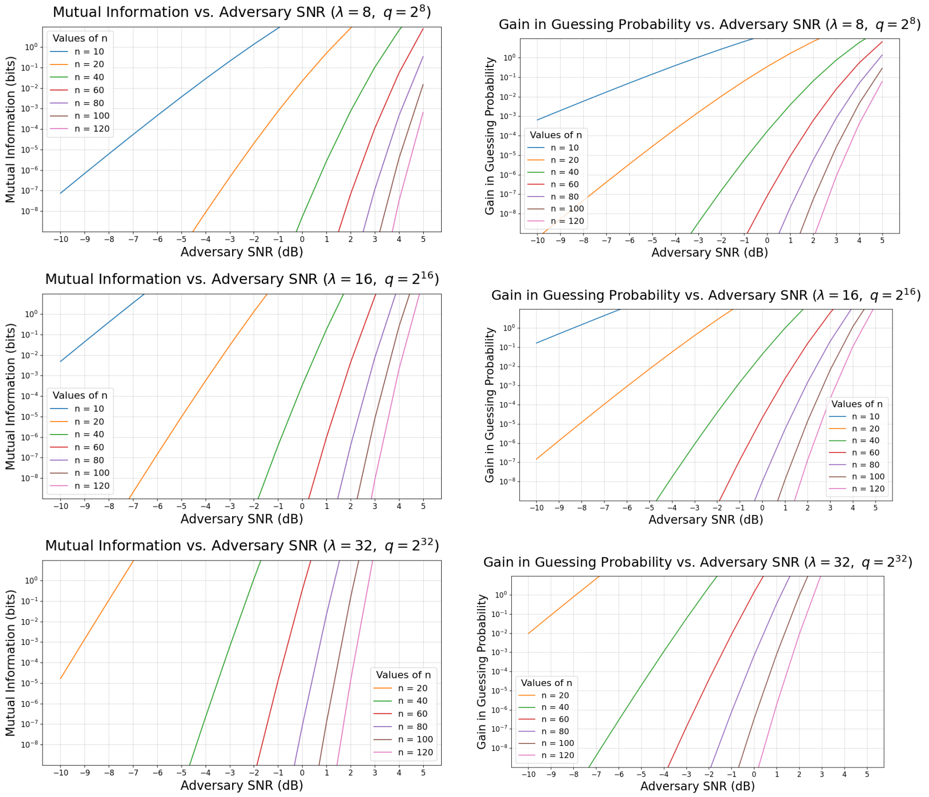

Fig. 2. Mutual Information leakage and gain in guessing probability for the adversary with $\mathrm{SNR} = 1/4\sigma^2$, for (n, n)-threshold schemes over fields $\mathbb{F}_{2^\lambda}$, with $\lambda = 8, 16, 32$.

8 Conclusion

To examine the resilience of linear secret sharing schemes against side-channel leakage attacks, we proposed the *additive noise leakage* model. In this model, each secret share is leaked to the adversary corrupted by independent additive noise in $\mathbb{F}_q$, characterized by the random variable E. For this model, we then study the security of (n, t)-threshold secret sharing schemes constructed using error-correcting codes. For such schemes over some finite field $\mathbb{F}_q$, we show that the information leakage measures, i.e. the mutual information (MI) metric, and consequently the statistical distance (SD) metric improve exponentially with t. In particular, for normalized threshold $\tau = t/(n+1)$, we show that if the Fourier bias the noise variable E, $\delta \leq q^{-\gamma}$ for some $\gamma > 1/\tau - 1$, bounds the mutual information leaked from the secret by $\mathcal{O}(q^{-2t(\gamma+1-1/\tau)})$ bits, thereby making linear secret sharing schemes with $t \geq \tau n$ secure. Through this work, we wish to initiate the study of security of secret sharing schemes with more general noisy side-channel leakage models. The proposed model has been inspired as a generalization of the ϵ-Bernoulli noise model introduced by Faust et. al. [20]. Faust's model corresponds to a binary symmetric channel (BSC) which is a fundamental channel model studied widely in information theory to analyze the behavior of discrete systems with Gaussian noise [51, 57]. We believe that techniques used to study the security of cryptographic schemes with this leakage model can be adapted and extended to adversaries with more general noisy leakage, including analog leakage.

There are several directions for future research. We believe that proofs for Proposition 4 and Corollary 4 can be adapted to find *sufficient statistics* for other noisy leakage models, such as the widely studied random probing model [26]. Then, using proof techniques similar to this work, we can bound mutual information leakage (which satisfies the data processing inequality), and consequently the statistical distance metric for other leakage models. Our results therefore suggest that linear secret sharing sharing schemes with general thresholds, over arbitrary finite fields, can be shown to be resilient against other noisy side-channel attacks. Moreover, similar to the reduction of δ-noisy leakage models to the random probing model for (n, n)-threshold schemes, done by Duc et. al. [16]; it might be possible to reduce the security analysis of more general noisy leakage models to the additive noise leakage model proposed in this work.

Bibliography

[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: 2021 IEEE International Symposium on Information Theory (ISIT). pp. 976–981. IEEE (2021)

[2] Béguinot, J., Cheng, W., Guilley, S., Liu, Y., Masure, L., Rioul, O., Standaert, F.X.: Removing the field size loss from duc et al.'s conjectured bound for masked encodings. In: International Workshop on Constructive Side-Channel Analysis and Secure Design. pp. 86–104. Springer (2023)

[3] Béguinot, J., Cheng, W., Guilley, S., Rioul, O.: Formal security proofs via doeblin coefficients: optimal side-channel factorization from noisy leakage to random probing. In: Annual International Cryptology Conference. pp. 389–426. Springer (2024)

[4] Béguinot, J., Liu, Y., Rioul, O., Cheng, W., Guilley, S.: Maximal leakage of masked implementations using Mrs. Gerber's lemma for min-entropy. In: 2023 IEEE International Symposium on Information Theory (ISIT). pp. 654–659. IEEE (2023)

[5] Beimel, A.: Secret-sharing schemes: A survey. In: International conference on coding and cryptology. pp. 11–46. Springer (2011)

[6] Benhamouda, F., Degwekar, A., Ishai, Y., Rabin, T.: On the Local Leakage Resilience of Linear Secret Sharing Schemes: 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings, Part I, pp. 531–561 (07 2018)

[7] Benhamouda, F., Degwekar, A., Ishai, Y., Rabin, T.: On the local leakage resilience of linear secret sharing schemes. Journal of Cryptology **34**, 1–65 (2021)

[8] Blakley, G.R.: Safeguarding cryptographic keys. In: Managing Requirements Knowledge, International Workshop on. pp. 313–313. IEEE Computer Society (1979)

[9] Brian, G., Dziembowski, S., Faust, S.: From random probing to noisy leakages without field-size dependence. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 345–374. Springer (2024)

[10] Brickell, E.F.: Some ideal secret sharing schemes. In: Workshop on the Theory and Application of of Cryptographic Techniques. pp. 468–475. Springer (1989)

[11] Chari, S., Jutla, C.S., Rao, J.R., Rohatgi, P.: Towards sound approaches to counteract power-analysis attacks. In: Advances in Cryptology—CRYPTO'99: 19th Annual International Cryptology Conference Santa Barbara, California, USA, August 15–19, 1999 Proceedings 19. pp. 398–412. Springer (1999)

[12] Chari, S., Rao, J.R., Rohatgi, P.: Template attacks. In: Cryptographic Hardware and Embedded Systems-CHES 2002: 4th International Workshop Red-

wood Shores, CA, USA, August 13–15, 2002 Revised Papers 4. pp. 13–28. Springer (2003)

[13] Cheng, W., Liu, Y., Guilley, S., Rioul, O.: Attacking masked cryptographic implementations: Information-theoretic bounds. In: 2022 IEEE International Symposium on Information Theory (ISIT). pp. 654–659. IEEE (2022)

[14] Cover, T.M.: Elements of information theory. John Wiley & Sons (1999)

[15] Cramer, R., Daza, V., Gracia, I., Urroz, J.J., Leander, G., Martí-Farré, J., Padró, C.: On codes, matroids, and secure multiparty computation from linear secret-sharing schemes. IEEE Transactions on Information Theory **54**(6), 2644–2657 (2008)

[16] Duc, A., Dziembowski, S., Faust, S.: Unifying leakage models: from probing attacks to noisy leakage. In: Advances in Cryptology–EUROCRYPT 2014: 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings 33. pp. 423–440. Springer (2014)

[17] Duc, A., Faust, S., Standaert, F.X.: Making masking security proofs concrete: or how to evaluate the security of any leaking device. In: Advances in Cryptology–EUROCRYPT 2015: 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I 34. pp. 401–429. Springer (2015)

[18] Dziembowski, S., Faust, S., Skórski, M.: Optimal amplification of noisy leakages. In: Theory of Cryptography: 13th International Conference, TCC 2016-A, Tel Aviv, Israel, January 10-13, 2016, Proceedings, Part II 13. pp. 291–318. Springer (2016)

[19] Faust, S., Masure, L., Micheli, E., Orlt, M., Standaert, F.X.: Connecting leakage-resilient secret sharing to practice: Scaling trends and physical dependencies of prime field masking. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 316–344. Springer (2024)

[20] Faust, S., Rabin, T., Reyzin, L., Tromer, E., Vaikuntanathan, V.: Protecting circuits from leakage: the computationally-bounded and noisy cases. In: Advances in Cryptology–EUROCRYPT 2010: 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30–June 3, 2010. Proceedings 29. pp. 135–156. Springer (2010)

[21] Gupta, U., Mahdavifar, H.: Bounds on the statistical leakage-resilience of shamir's secret sharing. In: 2024 IEEE International Symposium on Information Theory (ISIT). pp. 184–189 (2024). https://doi.org/10.1109/ISIT57864.2024.10619359

[22] Guruswami, V., Wootters, M.: Repairing reed-solomon codes. In: Proceedings of the forty-eighth annual ACM symposium on Theory of Computing. pp. 216–226 (2016)

[23] Guruswami, V., Wootters, M.: Repairing reed-solomon codes. IEEE Transactions on Information Theory **63**(9), 5684–5698 (2017). https://doi.org/10.1109/TIT.2017.2702660

[24] Hoffmann, C., Simkin, M.: Stronger lower bounds for leakage-resilient secret sharing. In: International Conference on Cryptology and Information Security in Latin America. pp. 215–228. Springer (2023)

[25] Huffman, W.C., Pless, V.: Fundamentals of error-correcting codes. Cambridge university press (2010)

[26] Ishai, Y., Sahai, A., Wagner, D.: Private circuits: Securing hardware against probing attacks. In: Advances in Cryptology-CRYPTO 2003: 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003. Proceedings 23. pp. 463–481. Springer (2003)

[27] Ito, A., Ueno, R., Homma, N.: On the success rate of side-channel attacks on masked implementations: information-theoretical bounds and their practical usage. In: Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. pp. 1521–1535 (2022)

[28] Jahandideh, V., Mennink, B., Batina, L.: A decomposition approach for evaluating security of masking. Cryptology ePrint Archive (2025)

[29] Kalai, Y.T., Reyzin, L.: A survey of leakage-resilient cryptography. In: Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali, pp. 727–794 (2019)

[30] Kasser, D.: An improvement upon the bounds for the local leakage resilience of shamir's secret sharing scheme. In: Theory of Cryptography Conference. pp. 395–422. Springer (2025)

[31] Klein, O., Komargodski, I.: New bounds on the local leakage resilience of shamir's secret sharing scheme. In: Annual International Cryptology Conference. pp. 139–170. Springer (2023)

[32] Liu, Y., Béguinot, J., Cheng, W., Guilley, S., Masure, L., Rioul, O., Standaert, F.X.: Improved alpha-information bounds for higher-order masked cryptographic implementations. In: 2023 IEEE Information Theory Workshop (ITW). pp. 81–86. IEEE (2023)

[33] MacWilliams, F.: The theory of error-correcting codes. Elsevier Science Publishers BV google schola **2**, 39–47 (1977)

[34] 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: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 344–374. Springer (2021)

[35] Maji, H.K., Nguyen, H.H., Paskin-Cherniavsky, A., Suad, T., Wang, M., Ye, X., Yu, A.: Leakage-resilient linear secret-sharing against arbitrary bounded-size leakage family. In: Theory of Cryptography Conference. pp. 355–383. Springer (2022)

[36] 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: 3rd Conference on Information-Theoretic Cryptography (ITC 2022). Schloss Dagstuhl-Leibniz-Zentrum für Informatik (2022)

[37] Maji, H.K., Nguyen, H.H., Paskin-Cherniavsky, A., Wang, M.: Improved bound on the local leakage-resilience of shamir's secret sharing. In: 2022 IEEE International Symposium on Information Theory (ISIT). pp. 2678–2683. IEEE (2022)

[38] Maji, H.K., Nguyen, H.H., Paskin-Cherniavsky, A., Ye, X.: Constructing leakage-resilient shamir's secret sharing: Over composite order fields. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 286–315. Springer (2024)

[39] Maji, H.K., Paskin-Cherniavsky, A., Suad, T., Wang, M.: Constructing locally leakage-resilient linear secret-sharing schemes. In: Annual International Cryptology Conference. pp. 779–808. Springer (2021)

[40] Mangard, S., Oswald, E., Popp, T.: Power analysis attacks: Revealing the secrets of smart cards, vol. 31. Springer Science & Business Media (2008)

[41] Mangard, S., Oswald, E., Standaert, F.X.: One for all–all for one: unifying standard differential power analysis attacks. IET Information Security **5**(2), 100–110 (2011)

[42] Massey, J.L.: Minimal codewords and secret sharing. In: Proceedings of the 6th joint Swedish-Russian international workshop on information theory. pp. 276–279 (1993)

[43] Massey, J.L.: Some applications of coding theory in cryptography. Codes and Ciphers: Cryptography and Coding IV pp. 33–47 (1995)

[44] Masure, L., Standaert, F.X.: Prouff and rivain's formal security proof of masking, revisited: Tight bounds in the noisy leakage model. In: Annual International Cryptology Conference. pp. 343–376. Springer (2023)

[45] McEliece, R.J., Sarwate, D.V.: On sharing secrets and reed-solomon codes. Communications of the ACM **24**(9), 583–584 (1981)

[46] Nguyen, H.H.: Physical-bit leakage resilience of linear code-based secret sharing. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 64–93. Springer (2025)

[47] Nielsen, J.B., Simkin, M.: Lower bounds for leakage-resilient secret sharing. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 556–577. Springer (2020)

[48] Obremski, M., Ribeiro, J., Roy, L., Standaert, F.X., Venturi, D.: Improved reductions from noisy to bounded and probing leakages via hockey-stick divergences. In: Annual International Cryptology Conference. pp. 461–491. Springer (2024)

[49] O'Donnell, R.: Analysis of boolean functions. Cambridge University Press (2014)

[50] Prest, T., Goudarzi, D., Martinelli, A., Passelègue, A.: Unifying leakage models on a rényi day. In: Advances in Cryptology–CRYPTO 2019: 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18–22, 2019, Proceedings, Part I 39. pp. 683–712. Springer (2019)

[51] Proakis, J.G., Salehi, M.: Digital communications. McGraw-hill (2008)

[52] Prouff, E., Rivain, M.: Masking against side-channel attacks: A formal security proof. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 142–159. Springer (2013)

[53] Schwertman, N.C., Gilks, A., Cameron, J.: A simple noncalculus proof that the median minimizes the sum of the absolute deviations. The American Statistician **44**(1), 38–39 (1990)

[54] Shamir, A.: How to share a secret. Communications of the ACM **22**(11), 612–613 (1979)

[55] Standaert, F.X., Malkin, T.G., Yung, M.: A unified framework for the analysis of side-channel key recovery attacks. In: Advances in Cryptology-EUROCRYPT 2009: 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, April 26-30, 2009. Proceedings 28. pp. 443–461. Springer (2009)

[56] Standaert, F.X., Pereira, O., Yu, Y.: Leakage-resilient symmetric cryptography under empirically verifiable assumptions. In: Annual Cryptology Conference. pp. 335–352. Springer (2013)

[57] Tse, D., Viswanath, P.: Fundamentals of wireless communication. Cambridge university press (2005)