Bounds on the Statistical Leakage-Resilience of Shamir's Secret Sharing

Utkarsh Gupta and Hessam Mahdavifar
Department of Electrical and Computer Engineering
Northeastern University
Boston, MA, USA
Email: {gupta.utk, h.mahdavifar}@northeastern.edu

***Abstract*—Secret sharing is an instrumental tool for sharing secret keys in distributed systems. In a classical threshold setting, this involves a dealer who has a secret/key, a set of parties/users to which shares of the secret are sent, and a threshold on the number of users whose presence is needed in order to recover the secret. In secret sharing, secure links with no leakage are often assumed between the involved parties. However, when the users are nodes in a communication network and all the links are physical links, e.g., wireless, such assumptions are not valid anymore. In order to study this critical problem, we propose a *statistical leakage* model of secret sharing, where some noisy versions of all the secret shares might be independently leaked to an adversary. We then study the resilience of the seminal Shamir's secret sharing scheme with *statistical leakage*, and bound certain measures of security (i.e., semantic security, mutual information security), given other parameters of the system including the amount of leakage from each secret share. We show that for an *extreme scenario* of Shamir's scheme, in particular when the underlying field characteristic is 2, the security of each bit of the secret against leakage improves exponentially with the number of users. To the best of our knowledge, this is the first attempt towards understanding secret sharing under general statistical noisy leakage.**

I. Introduction

Secret sharing, introduced by Shamir [1], and Blakey [2], is a fundamental cryptographic primitive central to security in many distributed systems. Secret sharing protects against collusion by allowing a secret to be shared among parties/users in such a way that only some selected subsets of users can recover the secret by aggregating their shares together. Such schemes have found several applications, such as in multi-party computation [3]–[6], zero-knowledge proofs [7], [8], threshold cryptographic systems [9]–[11], access control [12], generalized oblivious transfer [13], [14], and others. Secret sharing is widely used, yet it is still not fully understood how communication constraints such as leakage, noise, and scalability impact the security and reliability of such schemes.

The massive deployment of communication networks makes information security unprecedentedly important [15]. Anyone within the geographical range of a communication network can potentially gain unauthorized access to the data transmitted over the physical links. Protocols involving secret sharing often assume that the dealer has a reliable and secure communication channel to all the parties (users in a wireless network), i.e. links with no leakages. However, real-world implementations are susceptible to side-channel attacks which may lead to the adversary gaining some information about the secret shares of the non-colluding (honest) users.

Motivated by the emergence of such attacks, protocols which attempt to provide provable security guarantees against information leakage, have attracted a lot of attention in the cryptographic community (survey [16]). In the context of secret sharing, wireless leakage attacks allow an adversary to obtain some *bounded* leakage from the secret shares of honest parties. Such leakage may help the adversary reconstruct the secret. In the past few years, substantial research has examined the feasibility and efficiency of leakage-resilient secret sharing against diverse models of potential leakages [17]–[26].

Initiated by the fundamental work of Wyner on wiretap channels [27], developing information-theoretic methods for secure communications has been an active area of research [28]–[30]. The wiretap channel is a model of information leakage used to study physical layer security in wireless communications. In this work (Section III), we propose a statistical leakage model for secret sharing schemes where the adversary leaks information from all secret shares through independent wiretap channels. Subsequently, in Section IV, we study the resilience of Shamir's secret sharing scheme with statistical leakage. For the Shamir's scheme with a general threshold, ShamirSS(N, t), we show that the mutual information leaked from the secret is less than the sum of mutual information leaked by the shares individually. Then, for an extreme scenario of the Shamir's scheme, ShamirSS(N, N), in particular when the underlying field characteristic is 2; we show that the mutual information leaked from each bit of the secret reduces exponentially with the number of users.

The rest of this paper is organized as follows. We discuss the preliminaries to the Shamir's secret sharing protocol, and recall the relationship among information-security metrics for the wiretap channel in Section II. Then, we describe the proposed statistical leakage model and discuss some related leakage models in Section III. In Section IV we present results on the leakage resilience of Shamir's secret sharing under the proposed leakage model. Finally, the paper is concluded in Section V.

II. Preliminaries

In this section, we first review the Shamir's secret sharing scheme [1], [2]. The scheme provably leaks no information

from the secret even when an adversary has access to secret shares of some (less than a threshhold t) users. Subsequently, we discuss the wiretap channel [27]; and the relationship among mutual information security (MIS), semantic security (SS), and distinguishing security (DS) metrics for this channel [31]. The new leakage model proposed in Section III is inspired by the wiretap channel, and the relationship between the metrics is used to provide security guarantees in Section IV.

A. Shamir's Secret Sharing Scheme

Given a secret $s \in \mathbb{F}_q$, Shamir's secret sharing scheme aims to distribute secret shares $s_1, s_2, \ldots, s_N \in \mathbb{F}_q$ among N users in such a way that

- the secret s can be reconstructed given any t (threshold) or more secret shares;
- the knowledge of less than t secret shares does not reveal any information about the secret.

Such a scheme with N users and threshold t, denoted as ShamirSS(N,t), achieves this by constructing a $(t-1)$-degree random polynomial $P(x) \in \mathbb{F}_q[x]$ written as

$$P(x) = s + p_1 x + \cdots + p_{t-1} x^{t-1} \tag{1}$$

where the coefficients of the polynomial $p_1, \cdots, p_{t-1}$ are i.i.d. variables selected uniformly at random from $\mathbb{F}_q$. Once the polynomial is constructed, the secret share s_i of user $i \in [N]$ is the evaluation of the polynomial $P(x)$ at distinct predetermined values $\gamma_i \in \mathbb{F}_q$, i.e., $s_i = P(\gamma_i)$. The coefficients of $P(x)$ are determined uniquely by its evaluation on t distinct points, i.e., given at least t of the evaluation points $\{\gamma_1, \cdots, \gamma_N\}$; and their corresponding t secret shares. Then $s = P(0)$ is reconstructed. Using Lagrange's polynomial interpolation formula, given t evaluation points $\gamma_{e_1}, \ldots \gamma_{e_t}$;

$$P(0) = (-1)^{t-1} \sum_{i=1}^{t} \frac{\prod_{j=1, j\neq i}^{t} \gamma_{e_j}}{\prod_{j=1, j\neq i}^{t} (\gamma_{e_i} - \gamma_{e_j})} P(\gamma_{e_i}). \tag{2}$$

Remark 1 ([32]). *This is equivalent to saying that the secret can be represented as a unique linear combination of any t secret shares.*

B. The Wiretap Channel and Security Metrics

The wiretap channel, introduced by Wyner [27], is a pair of communication channels (ChR, ChA) with the same input and output sets where ChR is a channel from the sender to a receiver, and ChA is the wiretap that goes from the sender to an adversary. The setting aims to analyze the security of the communicated data based solely on the assumption that the channel from sender to adversary is "noisier" than the channel from sender to receiver; the adversary considered is computationally unbounded. In their seminal work [31], Bellare et. al. show that security of the communicated data does not depend on the receiver channel and establish a relationship between the classical notions of semantic security (SS), distinguishing security (DS), and mutual information security (MIS). Let M denote the message being sent, and let ChA : $\{0,1\}^m \to \{0,1\}^l$ be the adversary channel.

Definition 1 (Mutual information security, [31]). *The amount of information revealed about the message M can be measured using the MIS-security metric η_{MIS} defined as*

$$\eta_{MIS} = \max_{P_M} I\left(M; ChA(M)\right), \tag{3}$$

where P_M is the probability mass function of the message M.

Theorem 1 ([31], Theorem 1,5). *For the wiretap channel, semantic security η_{SS}, distinguishing security η_{DS}, and mutual-information security η_{MIS} satisfy the following inequality*

$$\eta_{SS} \leq \eta_{DS} \leq \sqrt{2\eta_{MIS}}. \tag{4}$$

We refer the reader to [31] for the exact formulation of semantic security and distinguishing security, which are all statistical measures of security.

III. Statistical Leakage Model

In this section, we formally introduce the problem of statistical leakage in secret sharing schemes. Leakage resilient secret sharing aims to guarantee the security of the secret, even if the adversary obtains partial information from the secret shares of all honest parties. In the proposed model, all honest parties leak information to the adversary independently through wiretap channels (Section II-B), while the adversary has the complete knowledge of the secret shares of the colluding users. Later in this section, we present some other leakage models which have been studied in cyrptography literature.

A. System Model

We study the leakage resilience of secret sharing schemes for communication systems. The wiretap setting (Section II-B) emerges naturally as a model of information leakage for analyzing the information-theoretic security of such schemes. Consider a secret sharing scheme ith N users where the dealer shares the secret s, which is sampled from a random variable S. The leakage we consider has the following properties

- some information can be leaked from every user;
- the information leaked to the adversary from each user is independent of the leakage from other users.

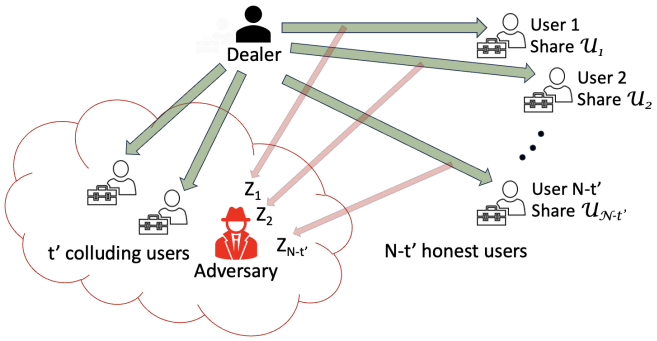

Fig. 1. Secret sharing with statistical leakage

The links between the dealer and users are assumed to be perfect channels while the adversary channels have information capacity constraints. Framing this model mathematically, let the random vector corresponding to the N secret shares

be $\mathcal{U} = (\mathcal{U}_1, \mathcal{U}_2, \ldots, \mathcal{U}_N)$, and let their leaked versions be the random vector $\mathbf{Z} = (Z_1, Z_2, \ldots, Z_N)$. Let l denote the bit-length of the secret and secret shares, assuming they belong to a field of characteristic 2 and represented as vectors over the binary field. Then the proposed model is characterized by the following two assumptions:

- **Leakage.** $I(\mathcal{U}_j; \mathbf{Z})/l = 1$ for the colluding parties, and $I(\mathcal{U}_j; \mathbf{Z})/l \leq \epsilon_j$ for the honest parties.
- **Independence assumption.** The random variables $Z_i/\mathcal{U}_i$ i.e. the leakage channels are mutually independent.

B. Related Prior Work

Leakage resilient secret sharing has garnered a lot of attention in the cryptographic community in recent years [17]–[26]. Guruswami and Wootters' reconstruction algorithm [32], [33] for Reed Solomon codes showed that even a single bit leaked from each secret share compromises the security of Shamir's scheme over fields of characteristic 2. This led Benhamouda et al. [22], [26] to investigate the leakage resilience of linear secret sharing schemes for other finite fields. They prove that Shamir's secret sharing scheme is leakage-resilient against one bit leakages, when the underlying field is of a large prime order, and the reconstruction thresholds is at least 0.92 times the number of parties. This threshold has been progressively refined to 0.69 in a series of works by different authors [18], [22], [23], [34].

Various works have tried to assess the resilience of secret sharing against diverse models of information leakage. The works of Benhamouda et al. [26], and Nielsen and Simkin [25], assume each secret share leaks information independently through arbitrary leakage functions with bounded output-length. Maji et. al. in [24], and Adams et. al. in [21], consider probing attacks which leak physical-bits from the memory hardware storing the secret shares. In a separate work [19], Maji et al. consider joint leakage, where the adversary can leak any bounded output-length joint function of the shares.

A majority of these contributions consider an adversary who is able to obtain the precise outputs of the leakage functions computed on secret shares. However, in practice, side-channel attacks are inherently noisy and there are practical techniques that can amplify this noise. Adams et al. [21] consider noisy physical-bit leakage, where each physical-bit leakage is replaced by noise with some fixed probability. In [17], Hoffmann et. al. consider a leakage model where some random subset of the leakages is replaced by uniformly random noise. In this work, we aim at providing a general framework for secret sharing under statistical leakage from a communication/information-theoretic perspective.

IV. Bounds on Securi ty

In this section, we study the resilience of Shamir's secret sharing under the proposed statistical leakage model. For the Shamir's scheme with a general threshold, ShamirSS(N, t), we show that the mutual information leaked from the secret is less than the sum of mutual information leaked by the shares individually. Then, for an extreme scenario of the Shamir's scheme, ShamirSS(N, N), we show that the mutual information leaked from each bit of the secret reduces exponentially with the number of users. Let the secret being shared be denoted by the random variable S. For the ShamirSS(N, N) scheme, we give bounds for two different cases where

- **Case 1.** the secret S is uniformly distributed but the leakage channel is arbitrary (Proposition 7); and
- **Case 2.** the secret S is arbitrarily distributed but the leakage channels are independent binary symmetric channels (BSCs) (Proposition 11).

The relationship between mutual information security (MIS), and other well-known notions of security in the literature i.e. semantic security(SS), and distinguishing security (DS) (Theorem 1) is used in Corollary 12.

A. Shamir's Scheme with General Threshold

We begin by showing that the analysis of the security guarantees for the Shamir's secret sharing scheme can be reduced to the scenario with no colluding users.

Lemma 2. *ShamirSS(N, t) scheme with $t' < t$ colluding users, under the statistical leakage model introduced in Section III, is as secure as the ShamirSS$(N - t', t - t')$ scheme with no colluding users.*

Proof. The problem of recovering the secret in ShamirSS(N, t) is equivalent to the problem of recovering the corresponding $(t-1)$-degree polynomial from its evaluation on N distinct points in the space $\mathbb{F}_q[x]$. The problem is equivalent to the Chinese Remainder Theorem for rings and reduces to finding the unique element in the ring $\mathbb{F}_q[x]/(x^t)$ which satisfies the given N evaluation points. Using the shares of the colluding users, we can interpolate and find the unique monic polynomial $h(x)$ of degree t' such that it satisfies the interpolation points of the colluding users. The problem is therefore reduced from finding unique element in the ring $\mathbb{F}_q[x]/x^t$, to finding a unique element in the ring $(\mathbb{F}_q[x]/(x^t))/(h(x))$ satisfying the $N - t'$ evaluation points. This is equivalent to finding a unique element in the ring $\mathbb{F}_q[x]/(x^{t-t'})$ satisfying $N - t'$ evaluation points which in turn is equivalent to the ShamirSS$(N - t', t - t')$ scheme. □

Corollary 3. *The security analysis of Shamir's scheme with t' colluding users can be reduced to a scheme with no collusion.*

Proposition 4. *The mutual information leakage in ShamirSS(N, t) with t' colluding users is bounded as*

$$\frac{I(S; \mathbf{Z})}{l} \leq \sum_{i=1}^{N-t'} \epsilon_i, \tag{5}$$

where ϵ_i's are the constants characterizing the per bit information leaked from the honest secret shares i.e., $I(\mathcal{U}_i, Z_i)/l \leq \epsilon_i$.

Proof sketch. Let $\mathcal{U}'$ be a set of $t-1$ secret shares which contains the shares of the t' colluding users. Using Lemma 2, this scheme is as secure as the ShamirSS$(N-t+1, 1)$ scheme with the same adversary leakage channels for the remaining

users. Then $I(S;\mathbf{Z})/l \leq \sum_{i=1}^{i=N-t+1} \epsilon_i$. Refer [35] for the complete proof.

Corollary 5. *The MIS-security metric can be characterized as $\eta_{MIS} \leq \sum_{i=1}^{i=N-t'} l \cdot \epsilon_i$. Using Theorem 1, semantic and distinguishing security metrics can be bounded as $\eta_{SS} \leq \eta_{DS} \leq \sqrt{2l\left(\sum_{i=1}^{i=N-t'} \epsilon_i\right)}$.*

B. The Extreme-Threshold Scenario

In general, it might be possible to improve upon the upper bound on the leakage provided in Proposition 4. In order to demonstrate this, in the remainder of this section, we consider an extreme scenario of the Shamir's scheme, where the ShamirSS(N, N) scheme is deployed, and the adversary has access to a noisy version of all the secret shares. In subsequent analysis, in light of Lemma 2, it is sufficient to consider scenarios without colluding users, that is, assume that the adversary only has a noisy observation of each secret share. Furthermore, we will assume that each secret share is leaked with $I(\mathcal{U}_j;\mathbf{Z})/l \leq \epsilon$ per bit leakage rate for some $\epsilon < 1$. Recall from Section II-A, in (2), once someone has access to the evaluation points, the secret recovery equation for ShamirSS(N, N) can be uniquely written as

$$s = \sum_{i=1}^{N} c_i s_i, \tag{6}$$

for some $c_i \in \mathbb{F}_q$. The unique representation of the secret as a linear combination of all the secret shares is a consequence of the following system of equations having a unique solution:

$$\begin{bmatrix} 1 & \gamma_1 & \gamma_1^2 & \cdots & \gamma_1^{N-1} \\ 1 & \gamma_2 & \gamma_2^2 & \cdots & \gamma_2^{N-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \gamma_N & \gamma_N^2 & \cdots & \gamma_N^{N-1} \end{bmatrix} \begin{bmatrix} s \\ p_1 \\ \vdots \\ p_{N-1} \end{bmatrix} = \begin{bmatrix} s_1 \\ s_2 \\ \vdots \\ s_N \end{bmatrix}.$$

Remark 2. *The coefficients c_i's in* (6)*, i.e. the secret recovery equation for ShamirSS(N, N), are the elements of the first row in the inverse of the Vandermonde matrix:*

$$V^{-1} = \begin{bmatrix} 1 & \gamma_1 & \gamma_1^2 & \cdots & \gamma_1^{N-1} \\ 1 & \gamma_2 & \gamma_2^2 & \cdots & \gamma_2^{N-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \gamma_N & \gamma_N^2 & \cdots & \gamma_N^{N-1} \end{bmatrix}^{-1}.$$

Therefore, replacing the matrix V by any invertible matrix gives us a linear secret sharing scheme with a unique secret recovery equation whose coefficients are determined by the first row of the inverse of the chosen matrix. If the chosen matrix is such that first row of its inverse is filled entirely with 1*s, the resulting linear secret sharing scheme has the recovery equation*

$$s = s_1 + s_2 + \cdots + s_N. \tag{7}$$

To bound the information leaked from the secret S by the leaked secret shares, for the two cases,

- **Case 1.** we will use Mrs. Gerber's Lemma (MGL) [36] (Lemma 6) in proving Proposition 7; and for
- **Case 2.** we will use Corollary 10 in proving Proposition 11.

Note that both the MGL, and Corollary 10 only hold true for the field $\mathbb{F}_2$. Since addition in the field $\mathbb{F}_{2^l}$ can be done by bit-wise addition of the vector representations over $\mathbb{F}_2$, we only provide bit-wise security guarantees. To bound information leakage for each bit, separate equations for each bit of the secret need to be formed from the secret recovery equation (6). But multiplication in the field $\mathbb{F}_{2^l}$ depends on the choice of the primitive (splitting) polynomial. Assuming that the adversary has access to all the coefficients of the secret shares and the splitting polynomial, the adversary has access to the l bit-wise equations for each bit of the secret. Our bounding results, to be presented in Propositions 7, and 11, depend upon the number of summands in the estimation of the sum of the random variables. Alternatively, one can replace the ShamirSS(N, N) with another linear scheme where all the secret shares, s_i's, appear in the reconstruction of the secret s with coefficient 1, as discussed in Remark 2. This automatically improves the bounds, which we will see in Remarks 4 and 5.

Remark 3. *In general, it is not straightforward to characterize the exact number of summands in the l bit-wise equations for the l bits of the secret. Let $\tilde{N}$ denotes the minimum of the number of non-zero summands across the l bit-wise equations (derived from* (6)*). We will utilize $\tilde{N}$ in the expression of the bounds in order to simplify them. Note that given the randomized coefficient selection inherent in Shamir's scheme (Section II-A), it is expected that $\tilde{N}$ grows at least linearly with the number of users, i.e., $\tilde{N} = \Omega(N)$.*

C. Security Analysis

Lemma 6 (Mrs. Gerber's Lemma, [36])**.** *Let A_0, A_1 be independent $\mathbb{Z}_2$-valued random variables with side information $\mathbf{B} = (B_0, B_1)$ (i.e. $B_0 - A_0 - A_1 - B_1$ is a Markov chain) , and $C = A_0 \oplus A_1$. Then*

$$H(C|B) \geq h\left(h^{-1}\left(H(A_0|B_0)\right) \star h^{-1}\left(H(A_1|B_1)\right)\right), \tag{8}$$

where $a \star b = a(1-b) + b(1-a)$.

Proposition 7. *Given that the secret S is a uniform random variable in F_{2^l}, the mutual information leakage from each bit of the secret in ShamirSS(N, N) with t' colluding users is bounded as,*

$$I(S^i;\mathbf{Z}) \leq \delta^{2(\tilde{N}-t')}, \tag{9}$$

where S^i is the random variable characterizing the i^{th} bit of the secret, $\tilde{N}$ is defined in Remark 3, and $\delta = 1 - 2h^{-1}(1-\epsilon)$.

Proof sketch. Using Lemma 2, we can work with a scheme without colluding users i.e. $\tilde{N} \to (\tilde{N} - t')$. Let $S^i = \sqcap_1 + \cdots + \sqcap_{\tilde{N}_i}$, where $\tilde{N}_i > \tilde{N}$ is the number of non-zero summands in the equation for S^i. Since the secret S is uniformly distributed, using Mrs. Gerber's Lemma for each bit and the inequality $h(p) \geq 4p(1-p)$, we get the required result. Refer [35] for the complete proof.

Corollary 8. *For the ShamirSS(N, N) scheme with $\tilde{N} > \kappa N$, where $\kappa < 1$; the mutual information leaked from each bit of the secret reduces exponentially with the number of users.*

Remark 4. *If a linear secret sharing scheme is of the form described in Remark 2, with its secret recovery equation as* (7)*; the bit S^i is the summation of i^{th} bit of each secret share, and the leakage can be bounded as $I(S^i, \mathbf{Z}) \leq \delta^{2(N-t')}$.*

To use Mrs. Gerber's lemma, we need independence of the random variables being added. In this application of Mrs. Gerber's lemma, the summand random variables are the secret shares, and they are independent if and only if the secret S is distributed uniformly. But as seen in Definition 1, MIS-security requires bounding mutual information leakage for all distributions of the secret. Therefore, even for the Shamir's scheme with a general threshold, ShamirSS(N, t), Mrs. Gerber's Lemma cannot be used to provide MIS-security guarantee. To understand the leakage resilience of ShamirSS(N, N), we consider the case of leakage through BSCs.

Lemma 9. *Let $\mathbf{X} = (X_0, \cdots, X_{k-1})$ be $\mathbb{Z}_2$-valued uniformly distributed random variables with every $k-1$ of them being mutually independent. Let $\mathbf{Y} = (Y_0, \cdots, Y_{k-1})$ be the output of a BSC with $\mathbf{X}$ as the input. Then*

$$(X_0 + \cdots + X_{k-1}) - (Y_0 + \cdots + Y_{k-1}) - \mathbf{Y} \tag{10}$$

is a Markov chain.

Proof sketch. Let $\hat{x} = (x_0, \ldots, x_{k-1})$ be a realization of $\mathbf{X}$. Define the parity check function $s(\hat{x}) = x_0 + \cdots + x_{k-1} \mod 2$. Since X_i are binary random variables with every $k-1$ of them being mutually independent, $Pr(\mathbf{X} = \hat{x}) = p_{s(\hat{x})} \in \{p_0, p_1\}$. For leakage through independent BSCs, observe that the probability $Pr(\mathbf{Y} = \hat{y}, s(\mathbf{X} = \hat{x}) = s_x)$, is the same for all $\hat{y}$ with the same parity $s(\hat{y})$, given $s_x \in \mathbb{F}_2$. Thererfore, $Pr(\mathbf{Y} = \hat{y}/s(\hat{x}) = s_x, s(\mathbf{Y}) = s(\hat{y})) = 2^{1-k}$, which implies the Markov chain in (10). Refer [35] for the complete proof.

Corollary 10.

$$I\left((X_0 + \cdots + X_{k-1}); \mathbf{Y}\right) = I\left((X_0 + \cdots + X_{k-1}); (Y_0 + \cdots + Y_{k-1})\right).$$

Proof. From Lemma 9, we know that $(X_0 + \cdots + X_{k-1}) - (Y_0 + \cdots + Y_{k-1}) - \mathbf{Y}$ is a Markov Chain. Since $(Y_0 + \cdots + Y_{k-1})$ is a function of $\mathbf{Y}$, $(X_0 + \ldots + X_{k-1}) - \mathbf{Y} - (Y_0 + \cdots + Y_{k-1})$ is also a Markov chain. The corollary now follows from using the data processing inequality twice. □

Proposition 11. *Given that all the secret shares leak information independently for every bit through BSC(q); the mutual information leakage from each bit of the secret in ShamirSS(N, N) with t' colluding users is bounded as*

$$I(S^i; \mathbf{Z}) \leq \ \delta^{2(\tilde{N}-t')}, \tag{11}$$

where S^i is the random variable characterizing the i^{th} bit of the secret, $\tilde{N}$ is defined in Remark 3, and $\delta = 1 - 2h^{-1}(1-\epsilon)$.

Proof sketch. Using Lemma 2, we can work with a scheme without colluding users i.e. $\tilde{N} \to (\tilde{N} - t')$. Let $S^i = \sqcap_1 + \cdots + \sqcap_{\tilde{N}_i}$, where $\tilde{N}_i > \tilde{N}$ is the number of non-zero summands in the equation for S^i. The secret S is arbitrarily distributed, and the bits of these $(\tilde{N}_i - 1)$ secret shares are uniformly distributed and mutually independent. Using Corollary 10 and the inequality $h(p) \geq 4p(1-p)$ again, we get the required result. Refer [35] for the complete proof.

Corollary 12. *Since Proposition 11 is valid for all distributions of the secret share, the bit-wise MIS-security metric can be characterized as $\eta_{MIS} \leq \delta^{2(\tilde{N}-t')}$. Using Theorem 1, semantic and distinguishing security metrics for each bit of the secret can be bounded as $\eta_{SS} \leq \eta_{DS} \leq \sqrt{2}\delta^{\tilde{N}-t'}$. For $\tilde{N} > \kappa N$, where $\kappa < 1$, the bit-wise security-metrics improve exponentially with the number of users.*

Remark 5. *If a linear secret sharing scheme is of the form described in Remark 2; the bit S^i is the summation of i^{th} bit of each secret share, and the security metrics can be bounded as $\eta_{MIS} \leq \delta^{2(N-t')}$, and $\eta_{SS} \leq \eta_{DS} \leq \sqrt{2}\delta^{N-t'}$.*

V. Conclusion

To examine the leakage resilience of secret sharing schemes in distributed systems, we proposed the *statistical leakage* model. This is an information-theoretic model of leakage, characterized by the honest parties leaking information to an adversary through independent wiretap channels. We then study the leakage resilience of Shamir's secret sharing with statistical leakage. For ShamirSS(N, N) scheme over fields of characteristic 2, we show that the bit-wise mutual information security (MIS), and consequently, the semantic security (SS) and distinguishing security (DS), improve exponentially with the number of users. The leakage model proposed in this work can be adapted to understand the leakage resilience of other protocols, such as for the recently proposed secret sharing in analog domain [37], and for multi-user secret sharing [38].

There are several directions for future research. We believe that Lemma 9 can be generalized to all Abelian groups, which lets us generalize Proposition 11 beyond bit-wise security. Proposition 11 provides security guarantees when the leakage channels are BSCs; similar results should hold true for other channels. For ShamirSS(N, t), the secret has $\binom{N}{t}$ secret recovery equations. By generalizing Lemma 9 to every subset of t random variables being mutually independent for a secret S satisfying a system of linear equations, it might be possible to improve upon the upper bound on the leakage provided in Proposition 4, to grow exponentially with the threshold t.

References

[1] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[2] G. R. Blakley, "Safeguarding cryptographic keys," in *Managing Requirements Knowledge, International Workshop on*. IEEE Computer Society, 1979, pp. 313–313.

[3] H. Goyal and S. Saha, "Multi-party computation in iot for privacy-preservation," in *2022 IEEE 42nd International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2022, pp. 1280–1281.

[4] K. Patel, "Secure multiparty computation using secret sharing," in *2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES)*. IEEE, 2016, pp. 863–866.

[5] D. Chaum, C. Crépeau, and I. Damgard, "Multiparty unconditionally secure protocols," in *Proceedings of the twentieth annual ACM symposium on Theory of computing*, 1988, pp. 11–19.

[6] A. Wigderson, M. Or, and S. Goldwasser, "Completeness theorems for noncryptographic fault-tolerant distributed computations," in *Proceedings of the 20th Annual Symposium on the Theory of Computing (STOC'88)*, 1988, pp. 1–10.

[7] V. Vaikuntanathan and P. N. Vasudevan, "Secret sharing and statistical zero knowledge," in *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 2015, pp. 656–680.

[8] R. Bendlin and I. Damgård, "Threshold decryption and zero-knowledge proofs for lattice-based cryptosystems," in *Theory of Cryptography Conference*. Springer, 2010, pp. 201–218.

[9] V. Shoup, "Practical threshold signatures," in *Advances in Cryptology—EUROCRYPT 2000: International Conference on the Theory and Application of Cryptographic Techniques Bruges, Belgium, May 14–18, 2000 Proceedings 19*. Springer, 2000, pp. 207–220.

[10] Y. Desmedt, "Threshold cryptosystems," in *International Workshop on the Theory and Application of Cryptographic Techniques*. Springer, 1992, pp. 1–14.

[11] Y. Desmedt and Y. Frankel, "Shared generation of authenticators and signatures," in *Annual International Cryptology Conference*. Springer, 1991, pp. 457–469.

[12] M. Naor and A. Wool, "Access control and signatures via quorum secret sharing," in *Proceedings of the 3rd ACM Conference on Computer and Communications Security*, 1996, pp. 157–168.

[13] T. Tassa, "Generalized oblivious transfer by secret sharing," *Designs, Codes and Cryptography*, vol. 58, pp. 11–21, 2011.

[14] B. Shankar, K. Srinathan, and C. P. Rangan, "Alternative protocols for generalized oblivious transfer," in *Distributed Computing and Networking: 9th International Conference, ICDCN 2008, Kolkata, India, January 5-8, 2008. Proceedings 9*. Springer, 2008, pp. 304–309.

[15] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.

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

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

[18] O. Klein and I. Komargodski, "New bounds on the local leakage resilience of shamir's secret sharing scheme," *Cryptology ePrint Archive*, 2023.

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

[20] ——, "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.

[21] D. Q. Adams, H. K. Maji, H. H. Nguyen, M. L. Nguyen, A. Paskin-Cherniavsky, T. Suad, and M. Wang, "Lower bounds for leakage-resilient secret-sharing schemes against probing attacks," in *2021 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2021, pp. 976–981.

[22] F. Benhamouda, A. Degwekar, Y. Ishai, and T. Rabin, "On the local leakage resilience of linear secret sharing schemes," *Journal of Cryptology*, vol. 34, pp. 1–65, 2021.

[23] H. K. Maji, A. Paskin-Cherniavsky, T. Suad, and M. Wang, "Constructing locally leakage-resilient linear secret-sharing schemes," in *Annual International Cryptology Conference*. Springer, 2021, pp. 779–808.

[24] H. K. Maji, H. H. Nguyen, A. Paskin-Cherniavsky, T. Suad, and M. Wang, "Leakage-resilience of the shamir secret-sharing scheme against physical-bit leakages," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2021, pp. 344–374.

[25] J. B. Nielsen and M. Simkin, "Lower bounds for leakage-resilient secret sharing," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2020, pp. 556–577.

[26] F. Benhamouda, A. Degwekar, Y. Ishai, and T. Rabin, *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*, 07 2018, pp. 531–561.

[27] A. D. Wyner, "The wire-tap channel," *Bell system technical journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[28] P. Angueira, I. Val, J. Montalban, Ó. Seijo, E. Iradier, P. S. Fontaneda, L. Fanari, and A. Arriola, "A survey of physical layer techniques for secure wireless communications in industry," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 810–838, 2022.

[29] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 347–376, 2016.

[30] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

[31] M. Bellare, S. Tessaro, and A. Vardy, "Semantic security for the wiretap channel," in *Annual Cryptology Conference*. Springer, 2012, pp. 294–311.

[32] V. Guruswami and M. Wootters, "Repairing reed-solomon codes," in *Proceedings of the forty-eighth annual ACM symposium on Theory of Computing*, 2016, pp. 216–226.

[33] ——, "Repairing reed-solomon codes," *IEEE Transactions on Information Theory*, vol. 63, no. 9, pp. 5684–5698, 2017.

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

[35] U. Gupta and H. Mahdavifar, "Bounds on the statistical leakage-resilience of shamir's secret sharing," *arXiv preprint arXiv:2405.04622*, 2024.

[36] A. Wyner and J. Ziv, "A theorem on the entropy of certain binary sequences and applications–i," *IEEE Transactions on Information Theory*, vol. 19, no. 6, pp. 769–772, 1973.

[37] M. Soleymani, H. Mahdavifar, and A. S. Avestimehr, "Analog secret sharing with applications to private distributed learning," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 1893–1904, 2022.

[38] M. Soleymani and H. Mahdavifar, "Distributed multi-user secret sharing," *IEEE Transactions on Information Theory*, vol. 67, no. 1, pp. 164–178, 2020.