Conditional Disclosure of Secrets: A Noise and Signal Alignment Approach

Zhou Li and Hua Sun, *Member, IEEE*

***Abstract*— In the conditional disclosure of secrets (CDS) problem, Alice and Bob (each holds an input and a common secret) wish to disclose, as efficiently as possible, the secret to Carol if and only if their inputs satisfy some function. The capacity of CDS is the maximum number of bits of the secret that can be securely disclosed per bit of total communication. We characterize the necessary and sufficient condition for the extreme case where the capacity of CDS is the highest and is equal to $1/2$. For the simplest instance where the capacity is smaller than $1/2$, we show that the linear capacity is $2/5$.**

***Index Terms*— Conditional disclosure of secrets, noise alignment, signal alignment, capacity.**

I. Introduction

IN A seminal work [1], Shannon introduced the notion of information theoretic security [2], [3] based on statistical independence and established the fundamental limits of a single-user secure communication system. While [1] provided an elegant theoretical foundation for cryptography, the optimal solutions are deemed too inefficient to implement in practice [4]. Cryptographers therefore relax the stringent requirement of information theoretic security to computational security, defined based on indistinguishability with limited computation power. Most existing commercial security protocols are built on computational security.

Modern secure communication systems naturally involve multiple users. Interestingly, for multi-user secure communication systems, solutions based on information theoretic security are not necessarily less efficient when compared to those based on computational security (e.g., see [5] for a specific context of private information retrieval). As such, there is much potential for information theoretic security in multi-user networks, especially considering the fact that multi-user security protocols based on both information theoretic and computational security criteria are primarily studied in academia and the potential of large-scale practical implementations is not yet fully exploited. It is thus imperative to understand the fundamental limits of information theoretic security in multi-user networks, which has been studied in the cryptography and theoretical computer science communities [6], although typically not using Shannon theoretic formulations. Due to the increasing importance of security in modern communication systems, it has also recently become one of the focuses for the information theory community [7]–[9], where both classical cryptography formulations are studied [10]–[15] and new models are introduced [16]–[20]. The goal of this paper is to use information theoretic tools to study a canonical theoretical computer science problem (i.e., a cryptographic primitive) - conditional disclosure of secrets (CDS) [21]–[23].

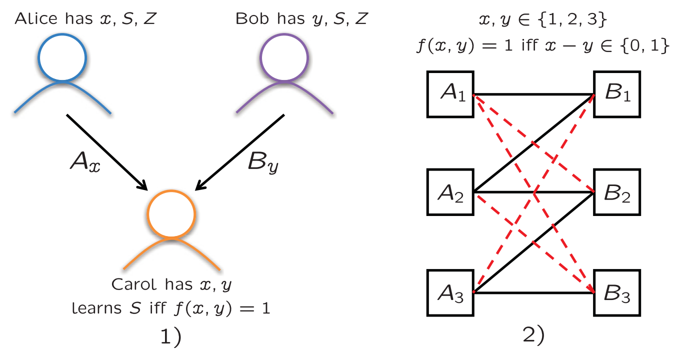


Fig. 1. 1). The CDS problem. 2) An example of $f(x, y)$ represented by a bipartite graph. Nodes in the left (right) column are the signals from Alice (Bob) for various input values. From pair of nodes connected by a solid black edge (i.e., $f(x, y) = 1$), Carol can decode S; from pair of nodes connected by a dashed red edge (i.e., $f(x, y) = 0$), Carol learns nothing about S.

In the CDS problem (see Fig. 1), Alice and Bob hold inputs x and y respectively, in addition to a common secret S. Alice and Bob wish to disclose the secret S to Carol if their inputs x, y satisfy some function f, i.e., when $f(x, y) = 1$. Otherwise $f(x, y) = 0$, absolute no information is revealed to Carol in the information theoretic sense (i.e., statistical independence). A common noise variable Z is available to Alice and Bob to assist the task, while Carol is fully ignorant of Z. Alice and Bob send signals A_x and B_y respectively to Carol. The aim is to find an efficient communication protocol, i.e., we wish to minimize the number of bits contained in A_x and B_y.

A. Motivation

The CDS problem is a minimal model that captures the challenges of characterizing the communication cost of security in multi-user networks. Note that if there is no security constraint (or if the problem is centralized, i.e., the value of $f(x, y)$ is known to either Alice or Bob when $f(x, y) = 1$), the problem is trivial as either Alice or Bob may directly send the secret to Carol. However, once the security constraint is included, the optimal communication cost of the CDS problem

Manuscript received September 12, 2021; revised January 21, 2022 and April 6, 2022; accepted April 9, 2022. Date of publication April 18, 2022; date of current version June 16, 2022. This work was supported in part by funding from NSF grants CCF-2007108 and CCF-2045656. An earlier version of this paper was presented in part at the 2020 IEEE International Symposium on Information Theory (ISIT) [DOI: 10.1109/ISIT44484.2020.9174262]. The associate editor coordinating the review of this article and approving it for publication was L. Ong. *(Corresponding author: Zhou Li.)*

The authors are with the Department of Electrical Engineering, University of North Texas, Denton, TX 76203 USA (e-mail: zhouli@my.unt.edu; hua.sun@unt.edu).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TCOMM.2022.3168282.
Digital Object Identifier 10.1109/TCOMM.2022.3168282

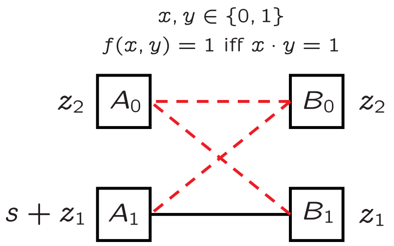


Fig. 2. The secret is disclosed if and only if $x = y = 1$ (i.e., from A_1, B_1). In the code construction shown (which is optimal, see Theorem 1), $S = (s)$ is 1 bit and $Z = (z_1, z_2)$ contains 2 i.i.d. uniform bits.

immediately becomes one of the notable open problems in information theoretic cryptography [24]. Further, considering that there are only three users in the CDS problem, we find it to be the simplest intriguing theoretical model and are interested in understanding its fundamental communication limits.

Beyond the theoretical value, the CDS problem is also relevant in modeling several interesting secure communication scenarios. One may interpret x and y as the queries sent from the user Carol to two distributed non-communicating servers, Alice and Bob, respectively. The signals A_x and B_y are the answers from the servers that enable the user to obtain the desired data, S. The security condition of $f(x, y) = 1$ is to ensure that data retrieval is successful if the queries are qualified while for unqualified queries, nothing is revealed. So if Carol is legal, then qualified queries can be chosen while if Carol is illegitimate, f is not known and unqualified queries cannot reveal the secret. Note that the distributed servers are non-communicating so that Alice only knows x and Bob only knows y. We then need a mechanism for Alice and Bob to produce answers without knowing the other query. In fact, the CDS problem was introduced first in the context of symmetric private information retrieval [21], exactly motivated by this need of providing distributed data access service with protection under unqualified (malicious) queries. Another interesting application may be seen as follows. Alice and Bob wish to share the secret (e.g., a business plan) with Carol if and only if they wish to collaborate, and $f(x, y)$ captures the condition under which they *agree* to collaborate. Alice and Bob do not want to reveal their inputs due to privacy considerations (so that while the function f is globally known, the value of $f(x, y)$ is not known to Alice or Bob in general as Alice only knows x and Bob only knows y). A CDS protocol ensures that if and only if they agree to collaborate, the secret is communicated to Carol. For instance, let $x \in \{0, 1\}$ be Alice's input, where $x = 1$ means Alice agrees to collaborate and $x = 0$ otherwise. Bob's input $y \in \{0, 1\}$ is similarly defined. As a result, $f(x, y) = x \cdot y$, i.e., if and only if $x = y = 1$, Carol can obtain the secret (see Fig. 2). In this manner, the collaboration is realized in a distributed and secure manner.

From a different perspective, the CDS problem could be viewed as a secure data storage system over a bipartite graph (see Fig. 1.2). The nodes in the graph are the storage variables and there are two types of edges, where from the pair of nodes connected by one type of edge, the secret is recoverable and otherwise, from the other type of edge, no information is disclosed. As such, the CDS problem is meant to provide fine-grained access control for encrypted data, where the access structure may be very diverse depending on the underlying graph (i.e., $f(x, y)$). That is, CDS can be viewed as a secret sharing problem [25] with a graph based access structure. For other applications of CDS, we refer to [22], [23], [26], [27] and references therein.

B. Comparison to Previous Approach

In cryptography and theoretical computer science communities, the typical formulation of the CDS problem is as follows [21]–[24], [26]–[28].

- The secret S has *1 bit*. The communication cost (i.e., the number of bits in A_x, B_y) is measured as order functions of the input size (the logarithm of the number of possibilities of inputs x, y). So the studied question is - how does the communication cost of disclosing a one-bit secret *scale with the complexity of the function* $f(x, y)$?
- Implicit to the above formulation is that the proposed protocols must work for *all* functions $f(x, y)$. In other words, the considered setting is the *worst* case scenario that targets at the most challenging $f(x, y)$.

In contrast, in this work we will take a Shannon theoretic formulation.

- We allow the *secret size to scale to infinity while the function* $f(x, y)$ *is fixed*. Our metric is the communication rate,[1] which is defined as the ratio of the secret size to the number of bits communicated to Carol. So our question is - what is the maximum number of bits that can be secretly disclosed, per bit of total communication?
- Regarding the function $f(x, y)$, we are interested in the *instance optimal* setting, i.e., for a fixed instance of $f(x, y)$, what is the optimal communication strategy?

C. Main Contribution and Technique

In this work, we mainly consider the best cases of $f(x, y)$, i.e., when the communication rate is the highest. As long as the security constraint is not empty for any input value (i.e., for any x (y), there exist some y (x) such that $f(x, y) = 0$), the size of A_x, B_y cannot be smaller than the secret size (as each of A_x and B_y must be independent of the secret by itself). Note that we assume each A_x, B_y has the same size and $f(x, y)$ is not always 0. For all such non-degenerate cases, the rate cannot be larger than $1/2$ (a detailed proof appears in Section IV-B), because to disclose 1 bit of the secret, both Alice and Bob must communicate 1 bit to Carol (then the total communication must be at least 2 bits). Our first main result is a complete characterization of all instances of $f(x, y)$ such that the capacity of CDS is $1/2$ (see Theorem 1). The characterization is stated in terms of the graph theoretic properties of $f(x, y)$. Our second main result is the linear capacity characterization of the simplest CDS instance such that its

[1]The metric of rate has also been studied in cryptography [23], [29], whose results will be discussed in more details within our framework in the conclusion section.

capacity is smaller than $1/2$ (see Theorem 2). Interestingly, once we go beyond the best case of capacity $1/2$, the problem becomes significantly more challenging and we are only able to settle the linear capacity.

The main results are obtained using an alignment view of the CDS problem, which can be viewed as generalizations and adaptations of interference alignment [30]. Interference alignment originated in wireless networks [31], [32] and has been applied much beyond the wireless context, e.g., to distributed storage repair [33]–[35], to network coding [36], [37] and index coding [38], [39], and to private information retrieval [40], [41]. Interference alignment aims to let the *multiple* undesired signal spaces overlap as much as possible, so as to maximize the number of dimensions left for the desired signal. It is then obvious that in the CDS problem, we only have two objects - the secret S and the noise Z, so there is no interference to say, not to mention multiple interferences. What we develop in this work is a new look of the CDS problem from the perspective of the overlap of the noise spaces and the signal spaces, i.e., noise alignment and signal alignment. Both the converse results and achievable schemes are based on such an alignment argument.

II. Problem Statement

Consider a pair of inputs (x, y) from some set $\mathcal{I} \subset \{1, 2, \cdots, X\} \times \{1, 2, \cdots, Y\}$. Input x is available (only) to Alice and input y is available (only) to Bob. Alice and Bob also both hold a secret S that is comprised[2] of L i.i.d. uniform symbols from a finite field $\mathbb{F}_p$ and an independent common noise variable Z that is comprised of L_Z i.i.d. uniform symbols from $\mathbb{F}_p$. In p-ary units,

$$\begin{aligned} H(S) = L,\ H(Z) = L_Z,\\ H(S, Z) = H(S) + H(Z) = L + L_Z. \end{aligned} \quad (1)$$

Alice and Bob wish to communicate the secret S to Carol if $f(x, y) = 1$, for a globally known binary output function f, defined over domain $\mathcal{I}$. When $f(x, y) = 0$, zero information about S should be revealed. To this end, Alice sends signal A_x and Bob sends signal B_y to Carol. A_x has L_{A_x} symbols from $\mathbb{F}_p$ and B_y has L_{B_y} symbols from $\mathbb{F}_p$. A_x and B_y are functions of S, Z,

$$H(A_x, B_y|S, Z) = 0, \text{ for all } (x, y) \in \mathcal{I}. \quad (2)$$

From A_x, B_y, Carol can recover S with no error[3] if $f(x, y) = 1$, and otherwise $f(x, y) = 0$, A_x, B_y must be independent[4] of S. For all $(x, y) \in \mathcal{I}$, we have

$$\text{[Correctness] } H(S|A_x, B_y) = 0, \quad \text{if } f(x, y) = 1; \quad (3)$$

$$\text{[Security] } H(S|A_x, B_y) = H(S), \quad \text{else } f(x, y) = 0. \quad (4)$$

The collection of the mappings from x, y, S, Z to A_x, B_y is called a CDS scheme.

A signal rate tuple $(\frac{L}{L_{A_1}}, \frac{L}{L_{A_2}}, \cdots, \frac{L}{L_{A_X}}, \frac{L}{L_{B_1}}, \cdots, \frac{L}{L_{B_Y}})$ is said to be achievable if there exists a CDS scheme, for which the correctness and security constraints (3), (4) are satisfied. The closure of the set of all achievable signal rate tuples is called the capacity region $\mathcal{C}$. The achievable communication rate characterizes how many symbols of the secret are securely disclosed per symbol of total communication and is defined with respect to the symmetric signal rate tuple[5] as follows.

$$R = \frac{L}{2N} \quad \text{s.t. } (\frac{L}{N}, \cdots, \frac{L}{N}) \in \mathcal{C}. \quad (5)$$

The supremum of achievable communicate rates is called the capacity[6] of CDS, C.

For a linear scheme, each signal is a linear function of the secret $S \in \mathbb{F}_p^{L\times 1}$ and the noise $Z \in \mathbb{F}_p^{L_Z \times 1}$, i.e., each signal is equal to $\mathbf{F}S + \mathbf{H}Z$, where $\mathbf{F} \in \mathbb{F}_p^{N\times L}$, and $\mathbf{H} \in \mathbb{F}_p^{N\times L_Z}$. The supremum of $L/(2N)$ for a linear scheme is called the linear capacity of CDS.

The randomness rate specifies how many secret symbols are disclosed per noise symbol and is defined as $R_Z = \frac{L}{L_Z}$. In this work, we focus mainly on the metric of capacity C and allow as much noise as needed, i.e., the randomness rate is unconstrained.

A. Graph Representation of $f(x, y)$

The function $f(x, y)$ can be equivalently specified by its characteristic undirected bipartite graph $G_f(V, E)$, defined as follows. The vertex set of G_f is comprised of all signals sent from Alice and Bob, i.e., $V = \{A_1, \cdots, A_X, B_1, \cdots, B_Y\}$. As the vertices and the signals have an invertible mapping, we use vertex and signal interchangeably in this paper. The edge set of G_f is comprised of the unordered pairs $\{A_x, B_y\}$ from the vertex set such that $(x, y) \in \mathcal{I}$. The edges have two types, $t : E \to \{0, 1\}$. For the first type, $\{A_x, B_y\}$ is a solid black edge and is referred to as a *qualified edge* if $f(x, y) = 1$ and equivalently $t(A_x, B_y) = 1$; for the second type, $\{A_x, B_y\}$ is a dashed red edge and is referred to as an *unqualified edge* if $f(x, y) = 0$ and equivalently $t(A_x, B_y) = 0$ (see Fig. 1.2 for an example).

The following notions of the characteristic graph G_f will be used to state our results. We follow standard graph theory terminologies (e.g., see [42]).

Definition 1 (Qualified/Unqualified Path): A sequence of distinct connecting qualified (unqualified) edges is called a qualified (unqualified) path.

[2]As usual for an information theoretic formulation, the actual size of the secret is allowed to approach infinity. The parameters L and p partition the data into blocks and may be chosen freely by the coding scheme to match the code dimensions. Since the coding scheme for a block can be repeated for each successive block of data with no impact on rate, it suffices to consider one block of data subject to optimization over L and p.

[3]The results of this work also hold under the ϵ-error framework.

[4]Equivalently, security is measured by the mutual information between the signals A_x, B_y and the secret S being 0 (see (4)). Note that the signals A_x, B_y are received perfectly by Carol (without noise), so the leakage can be made exactly zero (while in noisy settings, mutual information leakage is required to approach 0 normalized or not, called weak or strong security).

[5]For simplicity, we have adopted the single parameter of symmetric rate as the metric while leaving the characterization of the full capacity region as an interesting future work. Note that the symmetric rate can be defined equivalently through maximum signal size, i.e., $N = \max(L_{A_1}, \cdots, L_{A_X}, L_{B_1}, \cdots, L_{B_Y})$ in (5) as we may fill in dummy symbols to ensure that all signals have the same size.

[6]As block codes are allowed, i.e., L can approach infinity, we have that $C = \sup_L R = \limsup_{L\to\infty} \frac{L}{2N}$. A short proof is provided in the Appendix. As a result, the limit of $\frac{L}{2N}$ is also called an (asymptotically) achievable rate R.

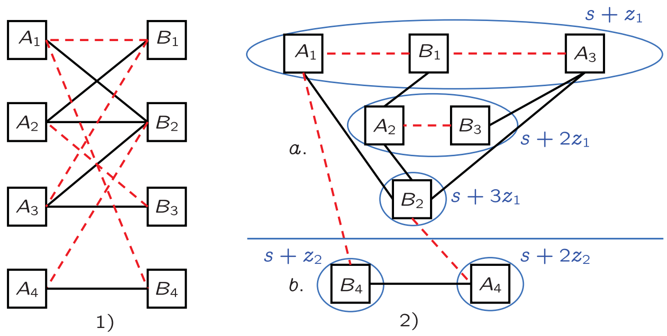


Fig. 3. 1). A CDS instance, described by its characteristic graph G_f. 2) The coding scheme that achieves rate $1/2$. The secret has 1 symbol s from $\mathbb{F}_5$, the noise variable has 2 independent symbols z_1, z_2 from $\mathbb{F}_5$, and each signal has 1 symbol from $\mathbb{F}_5$. G_f contains two qualified components (denoted by $a.$ and $b.$).

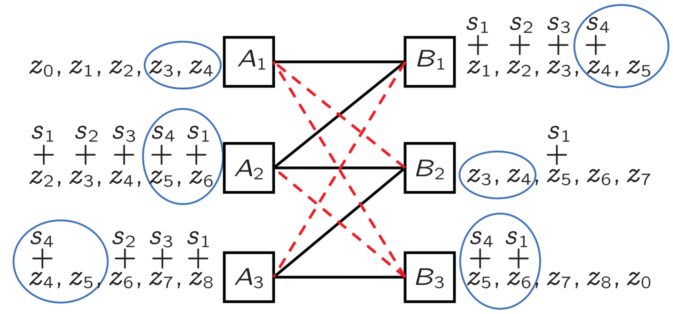


Fig. 4. A CDS instance that has an internal qualified edge $\{B_2, A_2\}$ in an unqualified path (B_2, A_1, B_3, A_2) within a qualified component G_f, and the achievable scheme of rate $2/5$. The secret has $L = 4$ bits, s_1, s_2, s_3, s_4, the noise has $L_Z = 9$ independent uniform bits, $z_0, z_1, \cdots, z_8$, and each signal has $N = 5$ bits. The rate achieved is $R = L/(2N) = 2/5$.

For example, in Fig. 1.2, $P = (\{A_1, B_1\}, \{B_1, A_2\}, \{A_2, B_2\}, \{B_2, A_3\}, \{A_3, B_3\})$ is a qualified path while $P = (\{B_2, A_1\}, \{A_1, B_3\}, \{B_3, A_2\})$ is an unqualified path. Note that a path can be equivalently specified by a sequence of vertices or edges.

Definition 2 (Internal Qualified Edge): A qualified edge that connects two vertices in an unqualified path is called an internal qualified edge.

For example, consider the unqualified path $P = (\{B_2, A_1\}, \{A_1, B_3\}, \{B_3, A_2\})$ in Fig. 1.2, which can be equivalently specified by a vertex sequence (B_2, A_1, B_3, A_2). The qualified edge $\{B_2, A_2\}$ is an internal qualified edge.

Definition 3 (Qualified Component): A qualified (connected) component *is a maximal induced subgraph of G_f such that any two vertices in the subgraph are connected by a qualified path.*

In this work, to avoid degenerate settings and to simplify the presentation of results,[7] we restrict ourselves to functions $f(x, y)$ such that the security constraint (4) is not empty for any individual x and any individual y.

Definition 4 (Non-Degenerate Condition): A CDS instance, described by the characteristic graph $G_f(V, E)$ is called non-degenerate *if for any vertex $v \in V$, there exists some vertex $u \in V$ such that $\{u, v\} \in E$ is an unqualified edge.*

III. Results

Our first main result is the necessary and sufficient condition for all CDS instances such that the capacity is $1/2$ (highest), stated in Theorem 1.

Theorem 1: The capacity of CDS is $1/2$ if and only if within any qualified component, there is no internal qualified edge in an unqualified path.

The proof of Theorem 1 is presented in Section IV. Here to illustrate the idea, we give two examples. For the first one, the half-rate feasibility condition is satisfied and rate $1/2$ is achievable.

Example 1: Consider the CDS instance in Fig. 3.1, where the characteristic graph G_f has two qualified components. Within qualified component $a.$, there are 3 unqualified paths and none of them has an internal qualified edge (see the blue circles in Fig. 3.2). Note that a vertex that is not connected to any unqualified edge is a (trivial) unqualified path/component (e.g., vertex B_2 in qualified component $a.$). Qualified component $b.$ only has two nodes that are connected by one qualified edge. Therefore, the half-rate feasibility condition in Theorem 1 is satisfied and the scheme that achieves rate $1/2$ is shown in Fig. 3.2.

For the scheme, every vertex in a qualified component uses the same noise variable and different qualified components use independent noise variables (e.g., qualified components $a.$ and $b.$ use z_1 and z_2, respectively). Within a qualified component, we consider each unqualified component (a maximal set of vertices where any two vertices are connected by an unqualified path) sequentially, and assign each vertex in the unqualified component a linearly independent combination of the secret and noise (e.g., the 3 unqualified components in $a.$ are assigned $s + z_1, s + 2z_1, s + 3z_1$ respectively).

The correctness constraint (3) holds because 1) any qualified edge belongs to a qualified component (e.g., $\{A_2, B_2\}$), 2) the two vertices belong to different unqualified components (note that there is no internal qualified edge, e.g., consider A_2, B_2), and 3) any distinct unqualified components are assigned a linearly independent combination of secret and noise, from which the secret can be successfully recovered (e.g., $A_2 = s + 2z_1, B_2 = s + 3z_1$). We show that the security constraint (4) is guaranteed as well. There are two cases. First, for unqualified edges within a qualified component (e.g., $\{B_1, A_3\}$), they belong to the same unqualified component so that the same signal is assigned and no information about the secret is revealed (e.g., $B_1 = A_3 = s + z_1$). Second, for unqualified edges across two qualified components (e.g., $\{B_2, A_4\}$), different noise variables are used so that again nothing about the secret is leaked (e.g., $B_2 = s + 3z_1, A_4 = s + 2z_2$).

For the second example, the condition in Theorem 1 is violated such that rate $1/2$ is not achievable. We use the CDS instance in Fig. 1 as the second example (reproduced in Fig. 4).

Example 2: Consider the CDS instance in Fig. 4, where the characteristic graph G_f is a qualified component. The unqualified path (B_2, A_1, B_3, A_2) contains an internal

[7]Note that a degenerate setting can be converted to a non-degenerate one. Consider any vertex v that is connected to only qualified edges. In other words, this vertex has no security constraint. Then we may set the signal v to be the secret S and eliminate v. Repeating the same procedure for all such vertices, we have a non-degenerate setting.

qualified edge $\{B_2, A_2\}$, so the half-rate feasibility condition in Theorem 1 is violated and rate $1/2$ is not achievable. An intuitive explanation by contradiction is as follows.

Suppose rate $1/2$ is achievable, then the size of each signal A_x, B_y that is connected to a qualified edge must be $N = L$ symbols (we omit $o(L)$ terms in this explanation) and the noise appeared in the signal has size L symbols as well (see Lemma 1 in Section IV-A). For any qualified edge, the noise variables for the two signals must be the same to ensure that the secret can be decoded, i.e., the noise space must fully overlap (see Lemma 2 for a proof). For example, in Fig. 4 A_2, B_2 must use the same noise. Then by submodularity, full noise alignment must hold for any qualified component, i.e., all signals in a qualified component must use the same noise variables (see Lemma 3). For example, in Fig. 4 $A_1, A_2, A_3, B_1, B_2, B_3$ must use the same noise. Next, consider any unqualified edge, given that the noise space is fully overlapped, the signal space must fully overlap to avoid leaking information about the secret (see Lemma 4). For example, B_2 must be equal to A_1 in Fig. 4. Similarly by submodularity, for any unqualified path within a qualified component, the signal spaces must fully overlap (see Lemma 5). For example, in Fig. 4 we must have $B_2 = A_1 = B_3 = A_2$ for the unqualified path (B_2, A_1, B_3, A_2). Finally, the presence of an internal qualified edge $\{B_2, A_2\}$ results in a contradiction, because $B_2 = A_2$ and B_2 is independent of the secret so that the edge $\{B_2, A_2\}$ cannot be qualified.

Remark 1: From the computational complexity perspective, there are efficient algorithms to test if the condition in Theorem 1 is satisfied. It is well known (refer to Section 22.5 of [43]) that finding connected components of a graph has a linear time (in the number of nodes and edges of G_f) algorithm, based on which the algorithm to test the condition in Theorem 1 can be easily constructed without increasing the order of the computational complexity.

Note that rate $1/2$ is the highest for all non-degenerate settings as each vertex v has at least one unqualified edge and the size of v cannot be smaller than the secret size, i.e., $N \geq L$ and $R = L/(2N) \leq 1/2$. As the half-rate feasibility condition is fully settled, we proceed to scenarios where rate $1/2$ is not achievable. Interestingly, the simplest such instance is that in Fig. 4. This 6-node CDS instance is the simplest in the sense that for any 5-node non-degenerate CDS instance, half-rate feasibility condition is satisfied (because with only 5 nodes, there are not sufficient edges to produce an internal qualified edge). Our second main result is the linear capacity characterization of the CDS instance in Fig. 4, stated in Theorem 2.

Theorem 2: The linear capacity of the CDS instance shown in Fig. 4 is $2/5$.

The achievable scheme is shown in Fig. 4, where the secret has $L = 4$ bits, $S = (s_1, s_2, s_3, s_4)$, and the noise has $L_Z = 9$ independent uniform bits, $Z = (z_0, z_1, \cdots, z_8)$. Each signal has $N = 5$ bits and is shown in Fig. 4. Note that along the qualified path $(A_1, B_1, A_2, B_2, A_3, B_3)$, every two connected vertices share 4 noise bits in a consecutive manner, i.e., A_1 uses z_0, z_1, z_2, z_3, z_4, and B_1 uses z_1, z_2, z_3, z_4, z_5 etc. The secret bits are assigned such that for any unqualified edge, the same noise bits are combined with the same secret bits (e.g., see the blue circles with the same shape in Fig. 4. For the unqualified edge $\{B_1, A_3\}$, both vertices use z_4, z_5 so that the same signal bits $s_4 + z_4, z_5$ are present).

The rate achieved is $R = L/(2N) = 2/5$. Both correctness and security constraints are easy to verify. For example, consider the qualified edge $\{B_1, A_2\}$. Considering the part of the signal that uses the same noise z_2, z_3, z_4, z_5, we may recover $(s_1 + s_2, s_2 + s_3, s_3 + s_4, s_4)$, from which we can decode $S = (s_1, s_2, s_3, s_4)$. Consider the unqualified edge $\{A_2, B_3\}$. As distinct independent noise bits $z_2, z_3, z_4, z_7, z_8, z_0$ will not reveal anything and the common noise bits z_5, z_6 carry the same secret bits, security is guaranteed.

The converse proof for all linear schemes is presented in Section V. We give an intuitive explanation of the idea here. A finer argument of the contradiction in Example 2 is required. For this explanation, let us assume the noise space of any two vertices from a qualified edge share exactly L dimensions in common (relaxation of this assumption is deferred to the full proof in Section V). That is, the noise spaces of A_1 and B_1 share L dimensions (this space is denoted as γ_1), and B_1 and A_2 share L dimensions (denote this space as γ_2). Now how many dimensions do A_1, B_1, A_2 have in common? γ_1 and γ_2 are two subspaces of the noise space of B_1 such that $\dim(\gamma_1 \cap \gamma_2) \geq \dim(\gamma_1) + \dim(\gamma_2) - N = 2L - N$. Proceeding with this argument along the qualified path $(A_1, B_1, A_2, B_2, A_3, B_3)$, we find that the noise spaces of $A_1, B_1, A_2, B_2, A_3, B_3$ must share $5L - 4N$ dimensions. We argue that such a common overlap cannot exist, so $5L - 4N \leq 0$ and $R_{linear} = L/(2N) \leq 2/5$. To set up the proof by contradiction, let us assume that all 6 noise spaces share a common dimension (denoted as γ). As the path (B_2, A_1, B_3, A_2) is unqualified, the signal space of γ must fully overlap as otherwise information about the secret will be revealed. This means that in the noise overlap of $\{A_2, B_2\}$, some signal is overlapped and does not contribute useful information of the secret. As the noise space of A_2, B_2 shares exactly L dimensions and in the overlap γ is useless, we cannot decode the L-symbol secret from $\{A_2, B_2\}$, arriving at the contradiction that $\{A_2, B_2\}$ is a qualified edge. The intersections of more than 2 spaces have no correspondence to entropy terms such that the above linear argument may not hold in the information theoretic sense (i.e., non-linear codes might achieve a higher rate). Note that the achievable scheme in Fig. 4 is designed following the overlap insights provided by the linear converse idea.

IV. Proof of Theorem 1

A. Only If Part

Consider any non-degenerate CDS instance, described by the characteristic graph $G_f(V, E)$. We show that if the half-rate feasibility condition in Theorem 1 is violated, then rate $1/2$ is not achievable. To set up the proof by contradiction, let us assume that $R = \lim_{L \to \infty} \frac{L}{2N} = 1/2$ is achievable, i.e., $N = L + o(L)$. As a result, each signal that is connected to a qualified edge and the noise used in such a signal must have entropy $L + o(L)$. This result is stated in Lemma 1.

Lemma 1 (Signal and Noise Size): When $R = 1/2$, for any signal $v \in V$ such that there exists $u \in V$ such that $\{v, u\}$ is a qualified edge, we have

$$H(v) = H(v|S) = L + o(L). \quad (6)$$

Proof: First, consider the "$\leq$" direction.

$$H(v|S) \leq H(v) \leq N = L + o(L). \quad (7)$$

Second, consider the "$\geq$" direction. As the CDS instance is non-degenerate, for any vertex w, there exists a vertex w' such that $\{w, w'\}$ is unqualified. From the security constraint (4), we have

$$I(w, w'; S) = 0 \Rightarrow I(w; S) = 0 \quad (8)$$

$$(w \text{ can by any vertex}) \Rightarrow I(v; S) = I(u; S) = 0. \quad (9)$$

Consider now the qualified edge $\{v, u\}$. From the correctness constraint (3), we have

$$\begin{aligned} H(S|v, u) &= 0 \\ \Rightarrow L &\overset{(1)}{=} H(S) = I(v, u; S) \overset{(9)}{=} I(v; S|u) \\ &\leq H(v) \overset{(9)}{=} H(v|S). \end{aligned} \quad (10)$$

The proof is thus complete. ■

Next, we consider any qualified edge and show that the noise appeared in both end vertices of the qualified edge has joint entropy $L + o(L)$, roughly the same as the entropy of the noise appeared in each vertex by itself. In other words, the noise must fully align.

Lemma 2 (Noise Alignment for Qualified Edge): When $R = 1/2$, for any qualified edge $\{v, u\}$,

$$H(v, u|S) = L + o(L). \quad (11)$$

Proof: On the one hand, we have

$$\begin{aligned} H(v, u|S) &= H(v, u, S) - H(S) \\ &\overset{(3)}{=} H(v, u) - H(S) \quad (12) \\ &\overset{(1)}{\leq} H(v) + H(u) - L \\ &\overset{(6)}{=} L + L - L + o(L) = L + o(L). \quad (13) \end{aligned}$$

On the other hand, we have

$$H(v, u|S) \geq H(v|S) \overset{(6)}{=} L + o(L). \quad (14)$$

The proof is now complete. ■

In the following lemma, we generalize the noise alignment phenomenon from qualified edges to (any induced subgraph of) qualified components.

Lemma 3 (Noise Alignment for Qualified Component): When $R = 1/2$, for any qualified component Q with vertex set $V_Q \subset V$, we have

$$\forall V_q \subset V_Q,\ H(V_q|S) = H(V_Q|S) = L + o(L). \quad (15)$$

Proof: We first prove the "$\geq$" direction.

$$\begin{aligned} H(V_Q|S) &\geq H(V_q|S) \geq H(v|S) \\ \text{for any } v \in V_q &\overset{(6)}{=} L + o(L). \end{aligned} \quad (16)$$

Second, we prove the "$\leq$" direction and complete the proof. Denote $V_Q = \{v_1, v_2, \cdots, v_Q\}$. Start with any qualified edge $\{v_{i_1}, v_{i_2}\}, i_1, i_2 \in \{1, 2, \cdots, Q\}$ in the qualified component Q. As Q is a qualified component, there must exist a vertex $v_{i_3} \in V_Q$ and a vertex from v_{i_1}, v_{i_2} (suppose it is v_{i_2} without loss of generality) such that $\{v_{i_2}, v_{i_3}\}$ is a qualified edge. From the sub-modularity property of entropy functions, we have

$$\begin{aligned} &H(v_{i_1}, v_{i_2}|S) + H(v_{i_2}, v_{i_3}|S) \\ &\geq\ H(v_{i_1}, v_{i_2}, v_{i_3}|S) + H(v_{i_2}|S) \quad (17) \\ &\overset{(6)(11)}{\Longrightarrow}\ L + L \geq H(v_{i_1}, v_{i_2}, v_{i_3}|S) + L + o(L) \quad (18) \\ &\overset{(16)}{\Rightarrow}\ H(v_{i_1}, v_{i_2}, v_{i_3}|S) \leq L + o(L). \quad (19) \end{aligned}$$

Then similarly, as Q is a qualified component, there must exist a vertex $v_{i_4} \in V_Q$ such that $\{v, v_{i_4}\}$ is a qualified edge, where v is one vertex from $v_{i_1}, v_{i_2}, v_{i_3}$. With a similar proof as above, we have

$$\begin{aligned} &H(v_{i_1}, v_{i_2}, v_{i_3}, v_{i_4}|S) \leq L + o(L) \Rightarrow \cdots \\ &\Rightarrow H(V_q|S) \leq H(V_Q|S) \leq L + o(L). \end{aligned} \quad (20)$$

■

We now proceed to the signal alignment phenomenon. We show that within a qualified component, any two vertices v, u that form an unqualified edge must produce exactly the same signal, i.e., the joint entropy of v, u is $L + o(L)$, the same as that of any individual v or u.

Lemma 4 (Signal Alignment for Unqualified Edge Within Qualified Component): When $R = 1/2$, for any unqualified edge $\{v, u\}$ that is within a qualified component Q, we have

$$H(v, u) = L + o(L). \quad (21)$$

Proof: Note that both end vertices of the unqualified edge $\{v, u\}$ belong to the vertex set of the qualified component Q. Combining the security constraint (4) and (15), we have

$$H(v, u) \overset{(4)}{=} H(v, u|S) \overset{(15)}{=} L + o(L). \quad (22)$$

■

In the following lemma, we generalize the signal alignment phenomenon from unqualified edges to unqualified paths.

Lemma 5 (Signal Alignment for Unqualified Path Within Qualified Component): When $R = 1/2$, for any unqualified path within a qualified component Q, $(\{v_1, v_2\}, \{v_2, v_3\}, \cdots, \{v_{P-1}, v_P\})$, we have

$$H(v_1, v_P) \leq L + o(L). \quad (23)$$

Proof: Equipped with what has been established, the proof follows from a simple recursive application of the sub-modularity property of entropy functions.

$$\begin{aligned} &H(v_1, v_2) + H(v_2, v_3) + \cdots H(v_{P-1}, v_P) \\ &\geq\ H(v_1, v_2, \cdots, v_P) + H(v_2) + H(v_3) + \cdots + H(v_{P-1}) \\ &\overset{(21)(6)}{\Rightarrow}\ (P-1)L \geq H(v_1, v_P) + (P-2)L + o(L) \\ &\Rightarrow\ H(v_1, v_P) \leq L + o(L). \end{aligned} \quad (24)$$

■

After establishing the above lemmas, we are ready to present where is the contradiction. As the half-rate feasibility condition is violated, there must exist an internal qualified edge (denoted as $\{v_1, v_P\}$) in an unqualified path

$(\{v_1, v_2\}, \{v_2, v_3\}, \cdots, \{v_{P-1}, v_P\})$ and the unqualified path is within a qualified component Q. From the correctness constraint (3) of the qualified edge $\{v_1, v_P\}$, we have

$$\begin{aligned} L + o(L) &\overset{(23)}{\geq} H(v_1, v_P) \overset{(3)}{=} H(v_1, v_P, S) \\ &= H(S) + H(v_1, v_P|S) \\ &\overset{(1)(11)}{=} L + L + o(L). \end{aligned} \tag{25}$$

So normalizing (25) by L and letting L approach infinity, we have $1 \geq 2$, and the contradiction is arrived. The proof of the only if part is thus complete.

Remark 2: The above proof is based on assuming that $R = 1/2$ and then arguing by contradiction. We may bound the terms appeared more carefully and obtain a stronger bound on R, $R \leq \overline{R}$, where $\overline{R}$ is strictly smaller than $1/2$, i.e., $\overline{R} = 1/2 - \delta$ for a positive constant δ (that is only a function of f and in particular, it does not depend on L).

B. If Part

We show that if the half-rate feasibility condition in Theorem 1 is satisfied, then the CDS capacity is 1/2. We first prove that $R \leq 1/2$ and then show that $R = 1/2$ is achievable.

The proof of $R \leq 1/2$ is as follows. Consider any CDS instance that contains at least one qualified edge $\{v, u\}$; otherwise all edges are unqualified, the problem is meaningless as the secret is never disclosed. Further, the CDS instance is non-degenerate, so there exists an unqualified edge $\{u, w\}$. From the security constraint (4), we have

$$I(u, w; S) = 0 \Rightarrow I(u; S) = 0. \tag{26}$$

From the correctness constraint (3), we have

$$L \overset{(1)}{=} H(S) \overset{(3)}{=} I(S; v, u) \overset{(26)}{=} I(S; v|u) \leq H(v) \leq N \tag{27}$$

$$\Rightarrow R = L/(2N) \leq 1/2. \tag{28}$$

We now present the coding scheme that achieves rate $1/2$. The scheme is a generalization of that presented in Example 1.

Consider any non-degenerate CDS instance, described by the characteristic graph $G_f(V, E)$. Suppose $G_f(V, E)$ has M qualified components. A single vertex that is not connected to any qualified edge is a (trivial) qualified component. Suppose within the $m^{th}, m \in \{1, 2, \cdots, M\}$ qualified component, there are U_m unqualified components. Choose p as a prime number that is no fewer than $\max(U_1, U_2, \cdots, U_M)$. The secret S contains $L = 1$ symbol from the finite field $\mathbb{F}_p$, denoted as $S = (s)$ and the noise Z contains $L_Z = M$ symbols from $\mathbb{F}_p$, denoted as $Z = (z_1, z_2, \cdots, z_M)$. Note that $z_1, \cdots, z_M$ are i.i.d. uniform symbols over $\mathbb{F}_p$.

The signals are assigned as follows. Consider the m^{th} qualified component Q_m. We set

any signal v in the $i^{th}, i \in \{1, 2, \cdots, U_m\}$ unqualified component within Q_m as $s + iz_m$. (29)

To complete the proof of the achievable scheme, we show that the scheme is both correct and secure. Consider the correctness constraint (3) first. A qualified edge must belong to one qualified component. As the half-rate feasibility condition in Theorem 1 is satisfied, there is no internal qualified edge, i.e., any qualified edge must belong to different unqualified components within a qualified component. Consider any qualified edge $\{v, u\}$ that is from qualified component Q_m and within Q_m, suppose v belongs to the i^{th} unqualified component and u belongs to the j^{th} unqualified component. Note that j is not equal to i. From (29), we have

$$v = s + iz_m, u = s + jz_m \tag{30}$$

$$\begin{aligned} &\Rightarrow H(S|v, u) = H(s|s + iz_m, s + jz_m) \\ &\overset{j \neq i}{=} H(s|s, z_m) = 0 \end{aligned} \tag{31}$$

so that the scheme is always correct.

Next consider the security constraint (4). Consider any unqualified edge $\{v, u\}$. We have the following two cases.

1) $\{v, u\}$ is from the same qualified component, say Q_m. Note that any unqualified edge must belong to the same unqualified component within Q_m, say the i^{th} unqualified component. From (29), we have

$$v = u = s + iz_m \tag{32}$$

$$\begin{aligned} \Rightarrow H(S|v, u) &= H(s|s + iz_m) \\ &= H(s, s + iz_m) - H(s + iz_m) \\ &= 1 = H(S) \end{aligned} \tag{33}$$

so that security is guaranteed.

2) $\{v, u\}$ is from different qualified components. Suppose v is from Q_m and u is from $Q_{m'}$, where $m \neq m'$. Further assume that v belongs to the i^{th} unqualified component in Q_m, and u belongs to the j^{th} unqualified component in $Q_{m'}$. From (29), we have

$$v = s + iz_m, u = s + jz_{m'} \tag{34}$$

$$\Rightarrow H(S|v, u) = H(s|s + iz_m, s + jz_{m'}) \tag{35}$$

$$\begin{aligned} &= H(s, s + iz_m, s + jz_{m'}) \\ &\quad - H(s + iz_m, s + jz_{m'}) \end{aligned} \tag{36}$$

$$\begin{aligned} &= H(s, z_m, z_{m'}) \\ &\quad - H(s + iz_m, s + jz_{m'}) \end{aligned} \tag{37}$$

$$\geq H(s, z_m, z_{m'}) - 2 = 1 = H(S) \tag{38}$$

so that $H(S|v, u) = H(S)$ and security is guaranteed.

Randomness Cost Reduction

The above scheme uses M noise symbols in total. We show that 2 noise symbols are sufficient, i.e., we save $M - 2$ noise symbols and the randomness rate is improved from $R_Z = 1/M$ to $R_Z = 1/2$. This reduction is made possible by the following simple observation - each unqualified edge only involves two vertices and each vertex only contains 1 noise symbol, so we only need to guarantee these two noise symbols appeared (if different) are linearly independent and for this purpose, two base noise symbols are sufficient as all other noise symbols can be generic linear combinations of these two noise symbols. The detailed proof is presented next.

Choose p as a prime number such that $p > \max(U_1, U_2, \cdots, U_M, M-2)$. The remaining proof is the same as that above, except that $z_1, z_2. \cdots, z_M$ are linear combinations of two base independent uniform symbols z_1, z_2 (instead of being mutually independent).

$$z_3 = z_1 + z_2, z_4 = z_1 + 2z_2, \cdots, z_M = z_1 + (M-2)z_2. \tag{39}$$

The correctness constraint is not influenced as only the noise assignment is changed. The security constraint continues to hold as we may easily verify that every step in (32) - (38) goes through after we set (39).

Remark 3: While the characteristic graph of a CDS instance is bipartite, a closer inspection of the proof of both the only if part and the if part reveals that the bipartite property is not used in the proof. Therefore Theorem 1 holds also for non-bipartite characteristic graphs.

V. Proof of Theorem 2: Linear Converse

We show that for the CDS instance in Fig. 4, the rate for all linear schemes cannot be higher than $2/5$. For a linear scheme, the signal v is a linear function of the secret $S \in \mathbb{F}_p^{L\times 1}$ and the noise $Z \in \mathbb{F}_p^{L_Z\times 1}$. All secret and noise symbols are i.i.d. and uniform. $v = \mathbf{F}_v S + \mathbf{H}_v Z$, where $\mathbf{F}_v$ is an $N \times L$ matrix over $\mathbb{F}_p$, and $\mathbf{H}_v$ is an $N \times L_Z$ matrix over $\mathbb{F}_p$.

We first establish two general properties that hold for all linear schemes. The first property states that for any qualified edge, the overlap of the noise spaces cannot be fewer than L dimensions. This property is stated in Lemma 6.

Lemma 6 (Noise Alignment): For any linear scheme and for any qualified edge $\{v, u\}$,

$$\dim(\textit{rowspan}(\mathbf{H}_v) \cap \textit{rowspan}(\mathbf{H}_u)) \geq L. \tag{40}$$

Proof: For any non-degenerate setting, we know from (26) that any vertex must be independent of the secret.

$$\begin{aligned} 0 &= I(S; v) = I(S; \mathbf{F}_v S + \mathbf{H}_v Z) \\ \Rightarrow 0 &= I(S; \mathbf{F}_v(\mathcal{J}, :)S + \mathbf{H}_v(\mathcal{J}, :)Z) \end{aligned} \tag{41}$$

where $\mathcal{J}$ is an arbitrary subset of $\{1, 2, \cdots, N\}$ and for a matrix A, we use $A(\mathcal{J}, :)$ to denote the sub-matrix of A formed by rows in the index set $\mathcal{J}$. In words, (41) means that for linear schemes the secret space must be fully covered by the noise space.

Denote $\dim(\text{rowspan}(\mathbf{H}_v) \cap \text{rowspan}(\mathbf{H}_u))$ by α. As $\mathbf{H}_v$ and $\mathbf{H}_u$ overlap in α dimensions, we may assume without loss of generality (by a change of basis operation) that the first α rows of $\mathbf{H}_u$ and $\mathbf{H}_v$ are the same, i.e., $\mathbf{H}_v(1:\alpha, :) = \mathbf{H}_u(1:\alpha, :) \triangleq \mathbf{H}_\alpha$. Further, we have that

$$\begin{aligned} &\text{The row vectors of } \mathbf{H}_\alpha, \mathbf{H}_v(\alpha+1:N, :) \text{ and} \\ &\mathbf{H}_u(\alpha+1:N, :) \text{ are linearly independent.} \end{aligned} \tag{42}$$

To simplify the notation, we define

$$\begin{aligned} &\mathbf{F}_v(1:\alpha, :) \triangleq \mathbf{F}_{v_1}, \mathbf{F}_v(\alpha+1, N, :) \triangleq \mathbf{F}_{v_2}, \\ &\mathbf{H}_v(\alpha+1, N, :) \triangleq \mathbf{H}_{v_2}. \end{aligned} \tag{43}$$

For the qualified edge $\{v, u\}$, the correctness constraint (3) requires that

$$\begin{aligned} L &\overset{(1)}{=} H(S) \\ &= I(S; v, u) && (44) \\ &= I(S; \mathbf{F}_{v_1}S + \mathbf{H}_\alpha Z, \mathbf{F}_{u_1}S + \mathbf{H}_\alpha Z, \\ &\quad \mathbf{F}_{v_2}S + \mathbf{H}_{v_2}Z, \mathbf{F}_{u_2}S + \mathbf{H}_{u_2}Z) && (45) \\ &= I(S; (\mathbf{F}_{v_1} - \mathbf{F}_{u1})S, \mathbf{F}_{u_1}S + \mathbf{H}_\alpha Z, \\ &\quad \mathbf{F}_{v_2}S + \mathbf{H}_{v_2}Z, \mathbf{F}_{u_2}S + \mathbf{H}_{u_2}Z) && (46) \\ &= I(S; \mathbf{F}_{u_1}S + \mathbf{H}_\alpha Z, \mathbf{F}_{v_2}S + \mathbf{H}_{v_2}Z, \mathbf{F}_{u_2}S + \mathbf{H}_{u_2}Z) \\ &\quad + I(S; (\mathbf{F}_{v_1} - \mathbf{F}_{u_1})S | \mathbf{F}_{u_1}S + \mathbf{H}_\alpha Z, \cdots \\ &\qquad \mathbf{F}_{v_2}S + \mathbf{H}_{v_2}Z, \mathbf{F}_{u_2}S + \mathbf{H}_{u_2}Z) && (47) \\ &\leq H((\mathbf{F}_{v_1} - \mathbf{F}_{u_1})S) && (48) \\ &\leq \alpha && (49) \end{aligned}$$

where (48) follows from the property that the first term of (47) is zero (proved in the following), and the last step follows from the fact that $(\mathbf{F}_{v_1} - \mathbf{F}_{u_1})S$ has at most α symbols.

To complete the proof of $\alpha \geq L$, we show that $I(S; \mathbf{F}_{u_1}S + \mathbf{H}_\alpha Z, \mathbf{F}_{v_2}S + \mathbf{H}_{v_2}Z, \mathbf{F}_{u_2}S + \mathbf{H}_{u_2}Z) = 0$.

$$\begin{aligned} &I(S; \mathbf{F}_{u_1}S + \mathbf{H}_\alpha Z, \mathbf{F}_{v_2}S + \mathbf{H}_{v_2}Z, \mathbf{F}_{u_2}S + \mathbf{H}_{u_2}Z) \\ = \;& H(\mathbf{F}_{u_1}S + \mathbf{H}_\alpha Z, \mathbf{F}_{v_2}S + \mathbf{H}_{v_2}Z, \mathbf{F}_{u_2}S + \mathbf{H}_{u_2}Z) \\ &\quad - H(\mathbf{F}_{u_1}S + \mathbf{H}_\alpha Z, \mathbf{F}_{v_2}S + \mathbf{H}_{v_2}Z, \cdots \\ &\quad \mathbf{F}_{u_2}S + \mathbf{H}_{u_2}Z | S) && (50) \\ \leq \;& H(\mathbf{F}_{u_1}S + \mathbf{H}_\alpha Z) + H(\mathbf{F}_{v_2}S + \mathbf{H}_{v_2}Z) \\ &+ H(\mathbf{F}_{u_2}S + \mathbf{H}_{u_2}Z) \\ &- H(\mathbf{H}_\alpha Z, \mathbf{H}_{v_2}Z, \mathbf{H}_{u_2}Z) \\ \overset{(41)(42)}{=} \;& H(\mathbf{H}_\alpha Z) + H(\mathbf{H}_{v_2}Z) + H(\mathbf{H}_{u_2}Z) \\ &- H(\mathbf{H}_\alpha Z) - H(\mathbf{H}_{v_2}Z) - H(\mathbf{H}_{u_2}Z) = 0. && (51) \end{aligned}$$

As mutual information is non-negative, the proof of Lemma 6 is now complete. ■

The second property states that for any unqualified edge, within the noise overlapping space, the signal space must fully overlap. This property is stated in Lemma 7.

Lemma 7 (Signal Alignment): For any linear scheme and for any unqualified edge $\{v, u\}$,

$$\begin{aligned} &\forall \mathcal{J} \subset \{1, 2, \cdots, N\}, \\ &\mathbf{H}_v(\mathcal{J}, :) = \mathbf{H}_u(\mathcal{J}, :) \Rightarrow \mathbf{F}_v(\mathcal{J}, :) = \mathbf{F}_u(\mathcal{J}, :). \end{aligned} \tag{52}$$

Proof: For the unqualified edge $\{v, u\}$, the security constraint (4) imposes that

$$\begin{aligned} 0 &= I(S; v, u) \\ &= I(S; \mathbf{F}_v S + \mathbf{H}_v Z, \mathbf{F}_u S + \mathbf{H}_u Z) \\ &\geq I(S; \mathbf{F}_v(\mathcal{J}, :)S + \mathbf{H}_v(\mathcal{J}, :)Z, \\ &\qquad \mathbf{F}_u(\mathcal{J}, :)S + \mathbf{H}_u(\mathcal{J}, :)Z) && (53) \\ &\geq I(S; (\mathbf{F}_v(\mathcal{J}, :) - \mathbf{F}_u(\mathcal{J}, :))S \\ &\qquad + (\mathbf{H}_v(\mathcal{J}, :) - \mathbf{H}_u(\mathcal{J}, :))Z). && (54) \end{aligned}$$

Now suppose. $\mathbf{H}_v(\mathcal{J}, :) = \mathbf{H}_u(\mathcal{J}, :)$. Plugging this condition into the equality above, we have

$$0 \geq I(S; (\mathbf{F}_v(\mathcal{J}, :) - \mathbf{F}_u(\mathcal{J}, :))S)$$

$$\Rightarrow \mathbf{F}_v(\mathcal{J},:) = \mathbf{F}_u(\mathcal{J},:) \tag{55}$$

and the proof is complete. ■

Equipped with the above two lemmas, we are ready to consider the CDS instance in Fig. 4. We first consider the qualified path $P = (\{A_1, B_1\}, \{B_1, A_2\}, \{A_2, B_2\}, \{B_2, A_3\}, \{A_3, B_3\})$ and see what is the dimension of the common overlap for the noise spaces of $A_1, B_1, A_2, B_2, A_3, B_3$. For any given linear scheme, we find the noise overlap of every qualified edge in P and simplify the notation as follows.

$$\dim(\text{rowspan}(\mathbf{H}_v) \cap \text{rowspan}(\mathbf{H}_u)) \triangleq \alpha_{vu},$$
$$\text{e.g., } \dim(\text{rowspan}(\mathbf{H}_{A_1}) \cap \text{rowspan}(\mathbf{H}_{B_1})) = \alpha_{A_1B_1} \tag{56}$$

and we identify 5 constants $\alpha_{A_1B_1}, \alpha_{B_1A_2}, \alpha_{A_2B_2}, \alpha_{B_2A_3}, \alpha_{A_3B_3}$. Similarly, we denote

$$\dim(\text{rowspan}(\mathbf{H}_v) \cap \text{rowspan}(\mathbf{H}_u) \cap \text{rowspan}(\mathbf{H}_w)) = \alpha_{vuw}, \text{ etc.} \tag{57}$$

and wish to characterize $\alpha_{A_1B_1A_2B_2A_3B_3}$, i.e., the overlap of 6 noise spaces. Consider $\alpha_{A_1B_1A_2}$.

$$\begin{aligned}
&\alpha_{A_1B_1A_2}\\
&= \dim\big(\text{rowspan}(\mathbf{H}_{A_1}) \cap \text{rowspan}(\mathbf{H}_{B_1}) \cap \text{rowspan}(\mathbf{H}_{A_2})\big)\\
&= \dim\big((\text{rowspan}(\mathbf{H}_{A_1}) \cap \text{rowspan}(\mathbf{H}_{B_1})) \cap \cdots\\
&\quad (\text{rowspan}(\mathbf{H}_{B_1}) \cap \text{rowspan}(\mathbf{H}_{A_2}))\big) &(58)\\
&\geq \dim\big((\text{rowspan}(\mathbf{H}_{A_1}) \cap \text{rowspan}(\mathbf{H}_{B_1}))\big)\\
&\quad + \dim\big((\text{rowspan}(\mathbf{H}_{B_1}) \cap \text{rowspan}(\mathbf{H}_{A_2}))\big)\\
&\quad - \dim(\text{rowspan}(\mathbf{H}_{B_1})) &(59)\\
&= \alpha_{A_1B_1} + \alpha_{B_1A_2} - N &(60)
\end{aligned}$$

where (59) follows from the fact that both the overlap of the row span of $\mathbf{H}_{A_1}$, $\mathbf{H}_{B_1}$ and the overlap of the row span of $\mathbf{H}_{B_1}, \mathbf{H}_{A_2}$ are subspaces of $\mathbf{H}_{B_1}$, and within a vector space of dimension α, two subspaces of dimension α_1, α_2 must overlap in a space of dimension at least $\alpha_1 + \alpha_2 - \alpha$. (60) is due to the fact that we may assume without loss of generality $\dim(\text{rowspan}(\mathbf{H}_{B_1})) = N$, i.e., the noise space has full rank. This is argued as follows. Suppose the matrix $\mathbf{H}_{B_1}$ does not have full row rank, i.e., there exists a row of $\mathbf{H}_{B_1}$ that is a linear combination of other rows, say $\mathbf{H}_{B_1}(1,:)$. From (41), we know that B_1 is independent of S, so the precoding vector of the secret $\mathbf{F}_{B_1}(1,:)$ must also be the same linear combination of other rows of $\mathbf{F}_{B_1}$. In other words, the first row of the signal B_1 is a deterministic function of the other rows of B_1 and contributes no entropy to B_1 (thus can be eliminated without loss). So we may only consider achievable schemes so that for any signal, the precoding matrix for the noise has full rank,[8] N.

We proceed similarly to the overlap of 4 noise spaces, $\alpha_{A_1B_1A_2B_2}$. Interpreting this overlap as the overlap of two spaces, i.e., the row span of $\mathbf{H}_{A_1}, \mathbf{H}_{B_1}, \mathbf{H}_{A_2}$ and the row space of $\mathbf{H}_{A_2}, \mathbf{H}_{B_2}$, within one space, i.e., the row space of $\mathbf{H}_{A_2}$, we have

$$\begin{aligned}
\alpha_{A_1B_1A_2B_2} &\geq \alpha_{A_1B_1A_2} + \alpha_{A_2B_2} - N &(61)\\
&\overset{(60)}{\geq} \alpha_{A_1B_1} + \alpha_{B_1A_2} + \alpha_{A_2B_2} - 2N &(62)
\end{aligned}$$

Similarly,

$$\begin{aligned}
&\alpha_{A_1B_1A_2B_2A_3}\\
&\geq \alpha_{A_1B_1} + \alpha_{B_1A_2} + \alpha_{A_2B_2} + \alpha_{B_2A_3} - 3N &(63)\\
&\quad \alpha_{A_1B_1A_2B_2A_3B_3}\\
&\geq \alpha_{A_1B_1} + \alpha_{B_1A_2} + \alpha_{A_2B_2} + \alpha_{B_2A_3} + \alpha_{A_3B_3} - 4N\\
&\triangleq \alpha^*. &(64)
\end{aligned}$$

In other words, the 6 noise spaces overlap in a space of dimension at least α^* so that we may assume without loss of generality that the first α^* rows of the noise precoding matrix of $A_1, B_1, A_2, B_2, A_3, B_3$ are the same.

$$\begin{aligned}
&\mathbf{H}_{A_1}(1:\alpha^*,:) = \mathbf{H}_{B_1}(1:\alpha^*,:) = \mathbf{H}_{A_2}(1:\alpha^*,:)\\
&\quad = \mathbf{H}_{B_2}(1:\alpha^*,:) = \mathbf{H}_{A_3}(1:\alpha^*,:) = \mathbf{H}_{B_3}(1:\alpha^*,:). &(65)
\end{aligned}$$

We next consider the unqualified path $P_u = (\{B_2, A_1\}, \{A_1, B_3\}, \{B_3, A_2\})$, where every vertex belongs to the qualified path P considered above. The overlap of the 6 noise spaces must be a subspace of the overlap of the noise space of any unqualified edge. Applying Lemma 7, i.e., (52) to the 3 unqualified edges in P_u, we have

$$\begin{aligned}
&\mathbf{H}_{B_2}(1:\alpha^*,:) = \mathbf{H}_{A_1}(1:\alpha^*,:)\\
&\Rightarrow \mathbf{F}_{B_2}(1:\alpha^*,:) = \mathbf{F}_{A_1}(1:\alpha^*,:) &(66)\\
&\mathbf{H}_{A_1}(1:\alpha^*,:) = \mathbf{H}_{B_3}(1:\alpha^*,:)\\
&\Rightarrow \mathbf{F}_{A_1}(1:\alpha^*,:) = \mathbf{F}_{B_3}(1:\alpha^*,:) &(67)\\
&\mathbf{H}_{B_3}(1:\alpha^*,:) = \mathbf{H}_{A_2}(1:\alpha^*,:)\\
&\Rightarrow \mathbf{F}_{B_3}(1:\alpha^*,:) = \mathbf{F}_{A_2}(1:\alpha^*,:) &(68)\\
&\Rightarrow \mathbf{H}_{B_2}(1:\alpha^*,:) = \mathbf{H}_{A_2}(1:\alpha^*,:),\\
&\quad \mathbf{F}_{B_2}(1:\alpha^*,:) = \mathbf{F}_{A_2}(1:\alpha^*,:). &(69)
\end{aligned}$$

The final step is to consider the internal qualified edge $\{A_2, B_2\}$, where we have the noise and signal alignment constraint (69). The correctness constraint (3) requires that

$$L \overset{(1)}{=} H(S) = I(S; A_2, B_2). \tag{70}$$

Following the proof of (48), we have

$$\begin{aligned}
L &\leq H((\mathbf{F}_{A_2}(1:\alpha_{A_2B_2},:) - \mathbf{F}_{B_2}(1:\alpha_{A_2B_2},:))S) &(71)\\
&\overset{(69)}{=} H((\mathbf{F}_{A_2}(\alpha^*+1:\alpha_{A_2B_2},:)\\
&\quad -\mathbf{F}_{B_2}(\alpha^*+1:\alpha_{A_2B_2},:))S) &(72)\\
&\leq \alpha_{A_2B_2} - \alpha^* &(73)\\
&\overset{(64)}{=} \alpha_{A_2B_2} - (\alpha_{A_1B_1} + \alpha_{B_1A_2} + \alpha_{A_2B_2}\\
&\quad + \alpha_{B_2A_3} + \alpha_{A_3B_3} - 4N) &(74)\\
&= 4N - (\alpha_{A_1B_1} + \alpha_{B_1A_2} + \alpha_{B_2A_3} + \alpha_{A_3B_3}) &(75)\\
&\overset{(40)}{\leq} 4N - 4L &(76)\\
\Rightarrow R &= L/(2N) \leq 4N/5 \times 1/(2N) = 2/5. &(77)
\end{aligned}$$

The linear converse proof is thus complete.

[8]The noise precoding matrix has size $N \times L_Z$, where $N \leq L_Z$. Note that if otherwise $N > L_Z$, then the rows of the noise cannot be linearly independent, and we have a similar situation where some row is a linear combination of other rows and we can follow the same line to argue that this row of signal is redundant.

Remark 4: The information theoretic capacity of the CDS instance in Fig. 4 is an interesting open problem, which might be challenging. While the linear capacity is characterized in Theorem 2 to be $2/5$, the best information theoretic converse with all Shannon type information inequalities [44] is $5/12$, found by computer programs[9] *[45], [46]. Therefore, if the linear scheme of Theorem 2 is information theoretically optimal, then we need non-Shannon type information inequalities to establish the converse; if the best converse with only Shannon-type information inequalities is information theoretically optimal, then we need non-linear codes to achieve it. Therefore, for the CDS instance in Fig. 4 with only 6 nodes and defined by only 8 variables, either non-linear codes are necessary for achievability schemes or non-Shannon inequalities are necessary for converse arguments; further it is possible that both are required to establish the capacity.*

VI. Conclusion

The conditional disclosure of secrets problem is studied from an information theoretic capacity perspective. A noise and signal alignment approach is used to identify all best case scenarios where the capacity is the highest, and the linear capacity of the scenario that minimally violates the best case criterion. In the context of secret sharing, a matroid approach is used to characterize extremal rate scenarios called ideal secret sharing [47]. In principle, the matroid view of [47] can be applied to our setting (with some modification to account for sets of nodes that have no correctness or security constraints) to produce the same necessary and sufficient condition for highest extremal rate. But we find our alignment view more intuitive and more importantly, beyond extremal rate scenarios, our approach can be refined to provide an explicit tighter converse, which is presented in Theorem 2 for one instance and further generalized to arbitrary instances in our follow-up work [48]. A number of interesting related questions remain open, among which a few are mentioned below. The achievable scheme of Theorem 1 uses scalar codes (the secret has only 1 symbol) while if block codes are used, the field size required can be reduced and the tradeoff between block-length and field size is an interesting problem. As another example, while the best case scenarios are fully characterized, we know very little about the worst case scenarios, i.e., for which problem instances, the capacity is small and how small can it be? It is desirable to establish capacity approximations and exact capacity results for various classes of problem instances (e.g., in terms of the characteristic graphs). Along this line, achievable rates of conditional disclosure of secrets have been studied in [23], [29] under the title of 'amortization' (typical in computer science community), where it is shown that rate of $1/6$ is always achievable for any f in our three user setting [29]. Therefore, compared to the best rate scenarios of capacity $1/2$ studied in this work, at most the rate is reduced by a factor of 3 for general f. In a follow-up work, we have characterized the linear capacity of a class of graphs [48]. We have focused exclusively on the metric of capacity in this work, while other metrics are also interesting, e.g., the capacity region, the maximum randomness rate and the randomness constrained capacity. Extensions to include a larger number of users (beyond 2 users holding the secret) and more secrets (beyond a single secret) look fertile. To sum up, this work represents an interesting initial step towards using signal overlap analysis and tools in information theory to understand the fundamental limits of multi-user primitives in cryptography, for which the potential remains promising while the topic is widely under-explored.

[9]This bound will also hold under vanishing error and/or leakage because the computer aided proofs are based on a finite number of linear combinations of Shannon type information inequalities (sub-modularity inequalities) so that the $o(L)$ terms will disappear after normalizing by L and letting $L \to \infty$.

Appendix

We show that the capacity, C, defined as the supremum of achievable rates $R = \frac{L}{2N}$, is equal to the limit of the supremum of R when $L \to \infty$.

Note that $C = \sup_L R = \sup_L \frac{L}{2N}$. Then by the definition of supremum, for any $\epsilon > 0$, we can choose L so that $\frac{L}{2N} > C - \epsilon$, i.e., $N < \frac{L}{2(C-\epsilon)}$. Any CDS scheme of secret size L and signal size N can be applied when the secret size is an integer multiple of L, say qL for some integer q (by repeating the scheme q times), and the signal size is qN. Now consider any secret size $L' = qL + r$, where $0 \le r < L$, we have a scheme of signal size $N' = (q+1)N$ (we can append zeros to the secret to make its length $(q+1)L$). Then

$$R = \frac{L'}{2N'} = \frac{qL + r}{2(q+1)N} > \frac{qL + r}{(q+1)L}(C - \epsilon) \to C \quad \text{as } q \to \infty \tag{78}$$

where we apply $N < \frac{L}{2(C-\epsilon)}$. So as $q \to \infty$ and the secret size $L' \to \infty$, we have that $R \to C$.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1948.

[2] M. Bloch *et al.*, "An overview of information-theoretic security and privacy: Metrics, limits and applications," *IEEE J. Sel. Areas Inf. Theory*, vol. 2, no. 1, pp. 5–22, Mar. 2021.

[3] S. Ulukus, S. Avestimehr, M. Gastpar, S. Jafar, R. Tandon, and C. Tian, "Private retrieval, computing and learning: Recent progress and future challenges," 2021, *arXiv:2108.00026*.

[4] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*. Boca Raton, FL, USA: CRC Press, 2014.

[5] C. Devet and I. Goldberg, "The best of both worlds: Combining information-theoretic and computational PIR for communication efficiency," in *Proc. Int. Symp. Privacy Enhancing Technol. Symp.* Cham, Switzerland: Springer, 2014, pp. 63–82.

[6] R. Cramer, I. B. Damgård, and J. B. Nielsen, *Secure Multiparty Computation and Secret Sharing*. Cambridge, U.K.: Cambridge Univ. Press, 2015.

[7] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information theoretic security," *Found. Trends Commun. Inf. Theory*, vol. 5, nos. 4–5, pp. 355–580, 2009.

[8] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[9] A. Yener and S. Ulukus, "Wireless physical-layer security: Lessons learned from information theory," *Proc. IEEE*, vol. 103, no. 10, pp. 1814–1825, Oct. 2015.

[10] H. Sun and S. A. Jafar, "The capacity of private information retrieval," *IEEE Trans. Inf. Theory*, vol. 63, no. 7, pp. 4075–4088, Jul. 2017.

[11] K. Banawan and S. Ulukus, "The capacity of private information retrieval from coded databases," *IEEE Trans. Inf. Theory*, vol. 64, no. 3, pp. 1945–1956, Mar. 2018.

[12] E. J. Lee and E. Abbe, "Two Shannon-type problems on secure multi-party computations," in *Proc. 52nd Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Sep. 2014, pp. 1287–1293.

[13] D. Data, V. M. Prabhakaran, and M. M. Prabhakaran, "Communication and randomness lower bounds for secure computation," *IEEE Trans. Inf. Theory*, vol. 62, no. 7, pp. 3901–3929, Jul. 2016.

[14] Y. Zhou, H. Sun, and S. Fu, "On the randomness cost of linear secure computation: (Invited Presentation)," in *Proc. 53rd Annu. Conf. Inf. Sci. Syst. (CISS)*, Mar. 2019, pp. 1–6.

[15] Y. Zhao and H. Sun, "Expand-and-randomize: An algebraic approach to secure computation," *Entropy*, vol. 23, no. 11, p. 1461, Nov. 2021.

[16] Q. Yu, S. Li, N. Raviv, S. M. M. Kalan, M. Soltanolkotabi, and S. A. Avestimehr, "Lagrange coded computing: Optimal design for resiliency, security, and privacy," in *Proc. 22nd Int. Conf. Artif. Intell. Statist.*, 2019, pp. 1215–1225.

[17] W.-T. Chang and R. Tandon, "On the capacity of secure distributed matrix multiplication," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2018, pp. 1–6.

[18] H. Sun, "The capacity of anonymous communications," *IEEE Trans. Inf. Theory*, vol. 65, no. 6, pp. 3871–3879, Jun. 2019.

[19] B. Tahmasebi and M. A. Maddah-Ali, "Private sequential function computation," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2019, pp. 1667–1671.

[20] Z. Wang, K. Banawan, and S. Ulukus, "Private set intersection: A multi-message symmetric private information retrieval perspective," *IEEE Trans. Inf. Theory*, vol. 68, no. 3, pp. 2001–2019, Mar. 2022.

[21] Y. Gertner, Y. Ishai, E. Kushilevitz, and T. Malkin, "Protecting data privacy in private information retrieval schemes," in *Proc. 13th Annu. ACM Symp. Theory Comput. (STOC)*, 1998, pp. 151–160.

[22] R. Gay, I. Kerenidis, and H. Wee, "Communication complexity of conditional disclosure of secrets and attribute-based encryption," in *Proc. Annu. Cryptol. Conf.* Berlin, Germany: Springer, 2015, pp. 485–502.

[23] B. Applebaum, B. Arkis, P. Raykov, and P. N. Vasudevan, "Conditional disclosure of secrets: Amplification, closure, amortization, lower-bounds, and separations," in *Proc. Annu. Int. Cryptol. Conf.* Cham, Switzerland: Springer, 2017, pp. 727–757.

[24] V. Vaikuntanathan, "Some open problems in information-theoretic cryptography," in *Proc. 37th IARCS Annu. Conf. Found. Softw. Technol. Theor. Comput. Sci. (FSTTCS)*, 2018, pp. 5:1–5:7.

[25] A. Beimel, "Secret-sharing schemes: A survey," in *Proc. Int. Conf. Coding Cryptol.* Berlin, Germany: Springer, 2011, pp. 11–46.

[26] S. Laur and H. Lipmaa, "A new protocol for conditional disclosure of secrets and its applications," in *Proc. Int. Conf. Appl. Cryptogr. Netw. Secur.* Berlin, Germany: Springer, 2007, pp. 207–225.

[27] T. Liu, V. Vaikuntanathan, and H. Wee, "Conditional disclosure of secrets via non-linear reconstruction," in *Proc. Annu. Int. Cryptol. Conf.* Cham, Switzerland: Springer, 2017, pp. 758–790.

[28] B. Applebaum and P. N. Vasudevan, "Placing conditional disclosure of secrets in the communication complexity universe," in *Proc. 10th Innov. Theor. Comput. Sci. Conf. (ITCS)*, 2018, pp. 4:1–4:14.

[29] B. Applebaum and B. Arkis, "On the power of amortization in secret sharing: D-uniform secret sharing and CDS with constant information rate," in *Proc. Theory Cryptogr. Conf.* Cham, Switzerland: Springer, 2018, pp. 317–344.

[30] S. A. Jafar, "Interference alignment: A new look at signal dimensions in a communication network," *Found. Trends Commun. Inf. Theory*, vol. 7, no. 1, pp. 1–134, 2011, doi: 10.1561/0100000047.

[31] V. Cadambe and S. Jafar, "Interference alignment and degrees of freedom of the K-user interference channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3425–3441, Aug. 2008.

[32] M. A. Maddah-Ali, A. S. Motahari, and A. K. Khandani, "Communication over MIMO x channels: Interference alignment, decomposition, and performance analysis," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3457–3470, Aug. 2008.

[33] Y. Wu and A. G. Dimakis, "Reducing repair traffic for erasure coding-based storage via interference alignment," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2009, pp. 2276–2280.

[34] N. B. Shah, K. V. Rashmi, P. V. Kumar, and K. Ramchandran, "Interference alignment in regenerating codes for distributed storage: Necessity and code constructions," *IEEE Trans. Inf. Theory*, vol. 58, no. 4, pp. 2134–2158, Apr. 2012.

[35] V. Cadambe, S. Jafar, H. Maleki, K. Ramchandran, and C. Suh, "Asymptotic interference alignment for optimal repair of MDS codes in distributed storage," *IEEE Trans. Inf. Theory*, vol. 59, no. 5, pp. 2974–2987, May 2013.

[36] C. Meng, A. K. Das, A. Ramakrishnan, S. A. Jafar, A. Markopoulou, and S. Vishwanath, "Precoding-based network alignment for three unicast sessions," *IEEE Trans. Inf. Theory*, vol. 61, no. 1, pp. 426–451, Jan. 2015.

[37] J. Han, C.-C. Wang, and N. B. Shroff, "Analysis of precoding-based intersession network coding and the corresponding 3-unicast interference alignment scheme," in *Proc. 49th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Sep. 2011, pp. 1033–1040.

[38] H. Maleki, V. Cadambe, and S. Jafar, "Index coding—An interference alignment perspective," *IEEE Trans. Inf. Theory*, vol. 60, no. 9, pp. 5402–5432, Sep. 2014.

[39] H. Sun and S. A. Jafar, "Index coding capacity: How far can one go with only Shannon inequalities?" *IEEE Trans. Inf. Theory*, vol. 61, no. 6, pp. 3041–3055, Jun. 2015.

[40] H. Sun and S. A. Jafar, "Blind interference alignment for private information retrieval," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2016, pp. 560–564.

[41] Z. Jia, H. Sun, and S. A. Jafar, "Cross subspace alignment and the asymptotic capacity of X-secure T-private information retrieval," *IEEE Trans. Inf. Theory*, vol. 65, no. 9, pp. 5783–5798, Sep. 2019.

[42] A. Schrijver, *Combinatorial Optimization: Polyhedra and Efficiency*, vol. 24. Berlin, Germany: Springer, 2003.

[43] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to Algorithms*. Cambridge, MA, USA: MIT Press, 2009.

[44] R. W. Yeung, *Information Theory and Network Coding*. Boston, MA, USA: Springer, 2008.

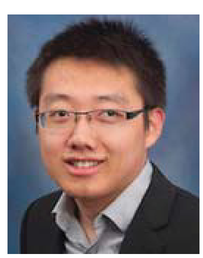
[45] (2007). *Xitip: Information Theoretic Inequalities Prover*. [Online]. Available: http://xitip.epfl.ch/

[46] C. Tian, J. S. Plank, and B. Hurst. (Oct. 2019). *An Open-Source Toolbox for Computer-Aided Investigation on the Fundamental Limits of Information Systems, Version 0.1*. [Online]. Available: https://github.com/ct2641/CAI/releases/tag/0.1

[47] E. F. Brickell and D. M. Davenport, "On the classification of ideal secret sharing schemes," *J. Cryptol.*, vol. 4, no. 2, pp. 123–134, Jan. 1991.

[48] Z. Li and H. Sun, "On the linear capacity of conditional disclosure of secrets," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2021, pp. 3202–3207.

Zhou Li received the B.E. degree in communications engineering from the Beijing University of Posts and Telecommunications, Beijing, China, in 2014. He is currently pursuing the Ph.D. degree with the University of North Texas. His research interests include information theory and privacy.



Hua Sun (Member, IEEE) received the B.E. degree in communications engineering from the Beijing University of Posts and Telecommunications, China, in 2011, and the M.S. degree in electrical and computer engineering and the Ph.D. degree in electrical engineering from the University of California at Irvine, Irvine, CA, USA, in 2013 and 2017, respectively. He is currently an Assistant Professor with the Department of Electrical Engineering, University of North Texas, Denton, TX, USA. His research interests include information theory and its applications to communications, privacy, security, and storage. He was a recipient of the NSF CAREER Award in 2021 and the UNT College of Engineering Distinguished Faculty Fellowship in 2021. His coauthored papers received the IEEE Jack Keil Wolf ISIT Student Paper Award in 2016 and an IEEE GLOBECOM Best Paper Award in 2016.