The Capacity of Anonymous Communications

Hua Sun, *Member, IEEE*

***Abstract*— We consider the communication scenario where K transmitters are each connected to a common receiver with an orthogonal noiseless link. One of the transmitters has a message for the receiver, who is prohibited from learning anything in the information theoretic sense about which transmitter sends the message (transmitter anonymity is guaranteed). The capacity of anonymous communications is the maximum number of bits of desired information that can be anonymously communicated per bit of total communication. For this anonymous communication problem over a parallel channel with K transmitters and one receiver, we show that the capacity is $1/K$, i.e., to communicate 1 bit anonymously, each transmitter must send a 1 bit signal. Furthermore, it is required that each transmitter has at least 1 bit correlated randomness (that is independent of the messages and is not available to the receiver) per message bit and the size of correlated randomness at all K transmitters is at least $K-1$ bits per message bit.**

***Index Terms*— Capacity, anonymous communications.**

I. Introduction

TRADITIONAL studies in information theoretic security and cryptography focus on efficient coding techniques for protecting the information contents. There is much recent interest in shifting the objective to hide user behaviors. For example, private information retrieval (PIR) aims to pursue communication efficient methods for hiding the identity of the desired message that the user wants to retrieve from a set of distributed replicated databases. The fundamental capacity limits of PIR and several of its variants are characterized recently in [1]–[3].

In this work, we consider the anonymous communication problem, where the goal is to hide the identity of the transmitters, receivers and the association between the two in a network. This problem of anonymous communications has been studied extensively in cryptography and computer science communities [4]–[6], where typically the objective is to provide scalable solutions over large networks while information theoretic optimality guarantees are not considered or treated in the approximate order sense. Specifically, a central goal in cryptography and computer science is to construct a modular anonymous communication protocol over the Internet. Starting from the seminal work by Chaum [7], the idea of using a set of auxiliary relays (called 'mix' server) for random forwarding and routing has been developed further as the onion routing technique [8] and finally to the widely used software - Tor [9]. The anonymous guarantee provided by this line of research is limited to computationally bounded adversaries [7]–[12]. Information theoretic anonymous protocols (achievability results) have been proposed in [13]–[15] over broadcast based networks, although optimality is not known (converse results). For further details on related works in cryptography and computer science, we refer to the excellent tutorials in [5], [6], and references therein.

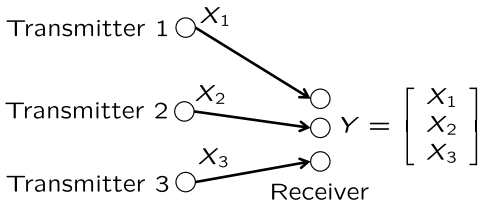

Fig. 1. Network topology: transmitters are connected to a single receiver with parallel interference-free noiseless links.

In this work, we focus on transmitter anonymity and consider an elemental model where K transmitters want to communicate to a common receiver anonymously with interference-free noiseless parallel channels.[1] This communication scenario appears naturally in the context of gossiping (where the gossip source does not want to be revealed), course or job evaluation (where the evaluation person is anonymized), and auction and voting (where the bidder or voter does not want to be identified). Our goal is to identify the exact information theoretic limits on the rate and common randomness for anonymous communications. For example, consider the case where we have $K = 3$ transmitters. As each transmitter is connected to the receiver with a parallel channel, the received signal Y is the collection of all transmitted signals, X_1, X_2, X_3 (see Figure 1).

One of the transmitters wishes to send a desired message to the receiver without being identified, i.e., the receiver decodes the message correctly, but has no knowledge about which transmitter sends the message. This anonymity constraint requires that no matter which transmitter wants to send the message, the received signal must be identically distributed and the decoding mapping can not depend on the desired transmitter index. To accomplish the task of keeping the transmitter identity anonymous, we assume that the transmitters share some *secret* correlated random variables that are not available to the receiver and are independent of the messages. In this

Manuscript received April 4, 2018; revised September 10, 2018; accepted October 29, 2018. Date of publication November 9, 2018; date of current version May 20, 2019. This paper was presented in part at the 2018 IEEE International Symposium on Information Theory.

The author is with the Department of Electrical Engineering, University of North Texas, Denton, TX 76203 USA (e-mail: hua.sun@unt.edu).

Communicated by N. Devroye, Associate Editor for Communications.
Digital Object Identifier 10.1109/TIT.2018.2880235

[1] Separate and perfect communication links are the least favorable channel conditions for anonymity because this assumption eliminates the possibility of hiding over direct interactions between the signals and noise.

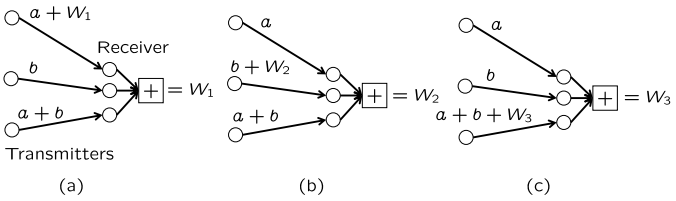

Fig. 2. The anonymous coding scheme with $K = 3$ transmitters. (a). $\theta = 1$. (b). $\theta = 2$. (c). $\theta = 3$. Note that no matter which message is sent, the receiver sees 3 uniform random bits and the decoding rule is always an addition.

case, we assume that Transmitter 1 holds a, Transmitter 2 holds b and Transmitter 3 holds $a + b$, where a, b are 2 i.i.d. uniform random bits (that form the correlated random variables). Then a simple scalar linear coding scheme that guarantees transmitter anonymity is presented next. Suppose the desired transmitter index is $\theta \in \{1, 2, 3\}$. The transmitted signals are

$$X_1 = a + \mathbb{1}(\theta = 1)W_1 \tag{1}$$

$$X_2 = b + \mathbb{1}(\theta = 2)W_2 \tag{2}$$

$$X_3 = a + b + \mathbb{1}(\theta = 3)W_3 \tag{3}$$

where $\mathbb{1}(x)$ is the indicator function that takes value 1 if the event x is true and 0 otherwise. Each message is assumed to be 1 independent uniform bit as well.

Correctness is easy to see as for all cases, the randomness cancels with each other after the addition operation. Anonymity holds because regardless of the value of θ, the received signal consists of 3 uniform random bits and the decoding mapping is always an addition. As such, the receiver learns nothing about which transmitter is the source of the message. We see that in order to communicate 1 bit anonymously, each transmitter needs to send 1 bit out. It is not hard to see that this is information theoretically optimal as even if there is no anonymity constraint, each transmitter will send out the desired message bit. What is non-trivial is the requirement on the correlated randomness. In this context, we show that for all linear schemes, each transmitter must hold a correlated random variable whose size is at least the size of the message and the total amount of randomness available at all transmitters must be at least as large as the size of $K - 1$ messages. Further, when the scheme is capacity achieving, both the individual and total randomness sizes are optimal information theoretically (i.e., for all non-linear schemes as well). A scheme of similar nature appears in a different context in [13] and [15], where coded randomness is not allowed and optimality on the communications and randomness is not considered.

Notation: For integers $Z_1, Z_2, Z_1 \leq Z_2$, we use the compact notation $[Z_1 : Z_2] = \{Z_1, Z_1 + 1, \cdots, Z_2\}$. The notation $X \sim Y$ is used to indicate that random variables X and Y are identically distributed.

II. Problem Statement

Consider a network with K transmitters and 1 receiver. Each transmitter is connected to the receiver with an orthogonal noiseless link. Each link can carry one symbol from a finite field $\mathbb{F}_p$ per channel use for a prime p.

Transmitter $k, k \in [1 : K]$ has a message W_k. The messages $W_1, \cdots, W_K$ are independent and are each comprised of L i.i.d. uniform symbols from $\mathbb{F}_p$. In p-ary units,

$$H(W_1) = \cdots = H(W_K) = L, \tag{4}$$

$$H(W_1, \cdots, W_K) = H(W_1) + \cdots + H(W_K). \tag{5}$$

The transmitters wish to communicate with the receiver anonymously. The transmitters privately generate θ uniformly over $[1 : K]$ (without loss of generality) and wish to communicate W_θ to the receiver while keeping θ a secret to the receiver. Depending on θ, there are K strategies that the transmitters employ to privately communicate the desired message.[2] For example, if $\theta = k$, then in order to communicate W_k, Transmitter i sends a signal $X_i^{[k]}$ over N channel uses. To fulfill the task of communicating anonymously, we assume that Transmitter i holds a correlated random variable Z_i. The correlated random variables are generated offline, i.e., before the realizations of the messages are known, so that the correlated random variables are independent of the messages.

$$H(Z_1, \cdots, Z_K, W_1, \cdots, W_K) = H(Z_1, \cdots, Z_K) + H(W_1, \cdots, W_K) \tag{6}$$

The correlated random variables are not available to the receiver (these random variables are the only information that the receiver does not know). The transmitted signal, $X_i^{[k]}$, is a function of the information available to the transmitter (i.e., the message and the correlated random variable),

$$H(X_i^{[k]} | W_i, Z_i) = 0 \tag{7}$$

The received signal at the receiver is a collection of the K transmitted signals.

$$Y^{[k]} = [X_1^{[k]}, \cdots, X_K^{[k]}]^T \tag{8}$$

From $Y^{[k]}$, the receiver decodes the desired message W_k according to a decoding mapping g. Note that the receiver is not allowed to learn anything about the index of the desired transmitter, so the decoding rule does not depend on k. The decoding mapping g is fixed and known at every node (including the transmitters).[3]

$$W_k = g(Y^{[k]}) \tag{9}$$

To ensure transmitter anonymity, the K strategies must be indistinguishable (identically distributed) from the perspective

[2] It turns out that for our achievable scheme, the transmitters do not need to know the exact value of the desired transmitter index θ. It suffices for each transmitter to know that whether he is the desired or not.

[3] The encoding and decoding functions are globally known (akin to codebooks). g is the mapping that is agreed a priori and will produce the correct estimate of the desired message. In general g is allowed to be random as long as it is independent of the desired message index. It is easy to see that randomized g does not help as we could pick any choice of g (and then fix it) such that the same constraint (10) must be satisfied. The receiver is allowed to try arbitrary other operations to infer the desired message index. However, because the received signals are identically distributed, so the outcome of any operation by the receiver does not depend on the desired message index (thus such inference will reveal no information and does not violate anonymity).

of the receiver, i.e., the following anonymity constraint must be satisfied $\forall k \in [1:K]$,

$$\text{[Anonymity]} \quad (Y^{[1]}, g) \sim (Y^{[k]}, g)$$
$$\text{i.e.,} \quad (X_1^{[1]}, \cdots, X_K^{[1]}, g) \sim (X_1^{[k]}, \cdots, X_K^{[k]}, g) \quad (10)$$

The anonymous communication *rate* characterizes how many symbols of desired information are communicated per symbol of total communication, and is defined as

$$R \triangleq \frac{L}{KN} \quad (11)$$

Note that by symmetry,[4] the number of channel uses for each transmitter does not depend on the transmitter indices. A rate R is said to be achievable if there exists an anonymous communication scheme of rate greater than or equal to R, for which zero error decoding is guaranteed. The supremum of achievable rates is called the capacity C.

The individual randomness size ρ measures the amount of correlated randomness at each transmitter relative to the message size (by symmetry, without loss of generality, we assume that each transmitter holds the same amount of correlated randomness, i.e., $H(Z_1) = \cdots = H(Z_K)$). The total randomness size η measures the total amount of correlated randomness at all transmitters relative to the message size.

$$\rho = \frac{H(Z_1)}{L} \quad (12)$$

$$\eta = \frac{H(Z_1, \cdots, Z_K)}{L} \quad (13)$$

III. Capacity of Anonymous Communications

Theorem 1 states our main result.

Theorem 1: The capacity of anonymous communications over a parallel channel with K transmitters and 1 receiver is $C = 1/K$. To achieve capacity, the minimum requirement on randomness size is $\rho = 1$ individually and $\eta = K - 1$ in total.

Remark 1: Theorem 1 settles the capacity of anonymous communications, while the requirement on the randomness is fully understood only at the capacity point. It is an interesting open problem to characterize the tradeoff region between the anonymous communication rate and the randomness size (i.e., if the communicate rate is lower, can we lower the normalized randomness size?). If we have further restrictions on the schemes used (e.g., linear schemes as proved in Section VI and some other special cases of non-linear schemes discussed in Remark 8), then the randomness size in Theorem 1 is indeed information theoretically optimal for any positive rate.

The achievability proof appears in Section IV, where we provide a scalar linear anonymous coding scheme. The converse proof on the rate appears in Section V. The converse proof on the randomness appears in Section VI for linear schemes and Section VII for all possible schemes (i.e., the information theoretic converse).

[4]Given any (asymmetric) achievable scheme that might employ a different number of channel uses for each transmitter, a symmetric scheme with the same rate (defined as the message size over the total number of channel uses by all transmitters) is obtained by repeating the original scheme K times, and in the i-th repetition shifting the transmitter indices cyclicly by i.

When there is no anonymity constraint, the capacity is trivially 1 (only the desired transmitter sends its message) and no common randomness is needed. Therefore, in order to obtain anonymity among a set of K transmitters, the price for anonymity in communication cost is K times of that with no anonymity constraint and we further need $K - 1$ bits of common randomness overall and 1 bit per transmitter, to communicate 1 bit anonymously.

IV. Proof of Theorem 1: Achievabiliy

The achievable scheme with K transmitters is an immediate generalization of that when $K = 3$, presented in the introduction section. We show that to communicate 1 bit anonymously, each transmitter uses its channel once, so that the rate achieved is $1/K$.

We present the scheme over the binary field (any field will work in general). Denote $a_1, \cdots, a_{K-1}$ as $K-1$ i.i.d. uniform bits, that are independent of the messages. The correlated random variables are assigned as follows.

$$Z_i = a_i, \quad i \in [1:K-1]$$
$$Z_K = a_1 + \cdots + a_{K-1} \quad (14)$$

The transmitted signals are

$$\begin{aligned} X_i &= a_i + \mathbb{1}(\theta = i) W_i \\ &= Z_i + \mathbb{1}(\theta = i) W_i, \ i \in [1:K-1] \\ X_K &= a_1 + \cdots + a_{K-1} + \mathbb{1}(\theta = K) W_K \\ &= Z_K + \mathbb{1}(\theta = K) W_K \end{aligned} \quad (15)$$

from which we can easily identify $X_i^{[k]}, \forall i, k \in [1:K]$.

The decoding mapping is the addition operation.

$$g(Y) = X_1 + X_2 + \cdots + X_K \quad (16)$$
$$\text{i.e.,} \quad g(Y^{[k]}) = X_1^{[k]} + X_2^{[k]} + \cdots + X_K^{[k]} = W_k \quad (17)$$

Correctness is easy to verify as the K correlated random variables lie in a $K-1$ dimensional space (in fact, any $K-1$ dimensional space will work) and the decoding mapping is along the null space of the correlated random variables. Anonymity is guaranteed because for all possible values of θ, the received signal is comprised of K uniform i.i.d. bits and the decoding mapping does not depend on θ. That is, when $\theta = k$, $\forall k \in [1:K]$:

$$H(Y^{[k]}) = H(X_1^{[k]}, \cdots, X_K^{[k]}) \quad (18)$$
$$= H(a_1, a_2, \cdots, a_{K-1}, W_k) \quad (19)$$
$$= K \quad (20)$$

Remark 2 (Coded Randomness): In our coding scheme, the common randomness variables are correlated in coded form at the transmitters. Combining with the converse, we know that coded randomness[5] is necessary to minimize the randomness size (i.e., if we do not allow randomness to be mixed, then we must use more randomness).

Remark 3 (Collusion): Our achievable scheme is resilient to user collusions (colluded users will share both the messages

[5]By uncoded randomness, we refer to *raw* independent bits (e.g., a_1, a_2), while coded randomness allows raw bits to be *mixed* (e.g., $a_1 + a_2$).

and correlated random variables with the receiver. Equivalently, the receiver has the prior knowledge to preclude a set of non-desired transmitters) in the following sense. Suppose each transmitter only knows he is desired or not, then any collusion of $K-2$ non-desired transmitters with the receiver can not identify the desired transmitter index (i.e., the transmitters that are not in the colluding set are equally likely to be the desired).

Remark 4: (Security): Our achievable scheme is perfectly secure in that the receiver obtains absolutely no information about all other messages beyond the desired one.

V. Proof of Theorem 1: Converse on Rate

We show that to transmit L symbols anonymously, each transmitter must use the channel at least $N \geq L$ times. Then the rate bound $R = \frac{L}{NK} \leq 1/K$ follows.

We first show that $H(X_i^{[i]}) \geq L$, i.e., when Transmitter i is the desired transmitter, he must send a signal that contains at least as much information as that contained in his message, from the correctness constraint. Define $W_{\bar{i}} = (W_1, \cdots, W_{i-1}, W_{i+1}, \cdots, W_K)$.

$$\begin{aligned} L &\overset{(4)}{=} H(W_i) && (21)\\ &\overset{(9)}{=} I(W_i; Y^{[i]}) && (22)\\ &\overset{(8)}{\leq} I(W_i; X_1^{[i]}, \cdots, X_K^{[i]}, Z_1, \cdots, Z_K, W_{\bar{i}}) && (23)\\ &\overset{(6)(5)}{=} I(W_i; X_1^{[i]}, \cdots, X_K^{[i]} | Z_1, \cdots, Z_K, W_{\bar{i}}) && (24)\\ &\overset{(7)}{=} I(W_i; X_i^{[i]} | Z_1, \cdots, Z_K, W_{\bar{i}}) && (25)\\ &\leq H(X_i^{[i]}) && (26) \end{aligned}$$

Next, we show that $H(X_i^{[k]}) \geq L, k \neq i$, i.e., when Transmitter i is not the desired transmitter, he must send a statistically equivalent signal so that the entropy is also not less than the message size, from the anonymity constraint.

$$\begin{aligned} H(X_i^{[k]}) &\overset{(10)}{=} H(X_i^{[i]}) && (27)\\ &\overset{(26)}{\geq} L, \ k \neq i && (28) \end{aligned}$$

Combining with the fact that $H(X_i^{[k]}) \leq N, \forall k$, we arrive at the desired rate bound.

VI. Proof of Theorem 1: Converse on Randomness for Linear Schemes

We present the proof on randomness separately for linear schemes and all possible schemes (non-linear schemes included), because our result for linear schemes holds for any rate while that for non-linear schemes works only for capacity achieving schemes (see Section VII). Specifically, we show that unconditionally, the individual randomness size $\rho \geq 1$ and sum randomness size $\eta \geq K-1$ for all linear schemes (with arbitrary positive rate). Otherwise, anonymous communication is not feasible, i.e., the capacity is 0.

A proof outline is as follows. We first use the anonymity constraint (i.e., regardless of the desired message index, the decoding mapping must be the same linear combination for linear schemes) to show that for non-desired transmitters, the transmitted signals can not contain their messages (undesired). Then combining with the property that any set of transmitted signals must contain as much information as L times the cardinality of the set (this follows from the uncertainty of the desired message index. For a statement, see Lemma 1), we arrive at the desired randomness size bounds.

We first present the proof when $K = 3$.

A. Proof for Scalar Linear Case When $K = 3$

To illustrate the main idea in a simpler setting, we first consider the $K = 3$ setting and assume the scheme is scalar linear, i.e., each message and each correlated random variable is only 1 symbol. We show that each correlated random symbol must be uniformly random, $H(Z_i) \geq L, i \in \{1, 2, 3\}$ and any two random symbols are independent, $H(Z_i, Z_j) \geq 2L$, $i \neq j, i, j \in \{1, 2, 3\}$.

For a linear scheme, the transmitted signal is a linear combination of the message symbol and the correlated random variable, and the decoding mapping is also a linear combination of the received signal symbols (so the only operation allowed is taking linear combinations). Note that we define a linear scheme to be one where both encoding and decoding mappings must be linear (this is a standard definition for linear schemes, see e.g., [16, Sec. III]). Specifically, the transmitted signals are

$$X_i^{[k]} = V_i^{[k]} W_i + U_i^{[k]} Z_i, \quad i, k \in \{1, 2, 3\} \tag{29}$$

where $V_i^{[k]}, U_i^{[k]}$ are deterministic scalars over $\mathbb{F}_p$ (and are globally known). The decoding coefficients are denoted as $G_1, G_2, G_3 \in \mathbb{F}_p$ (note that the constants G_1, G_2, G_3 do not depend on the desired transmitter index k) and the decoding works as follows.

$$\begin{aligned} W_k &= G_1 X_1^{[k]} + G_2 X_2^{[k]} + G_3 X_3^{[k]} && (30)\\ &= G_1 V_1^{[k]} W_1 + G_2 V_2^{[k]} W_2 + G_3 V_3^{[k]} W_3 \\ &\quad + G_1 U_1^{[k]} Z_1 + G_2 U_2^{[k]} Z_2 + G_3 U_3^{[k]} Z_3 && (31) \end{aligned}$$

As such, for any $k \in \{1, 2, 3\}$, the undesired messages can not appear. It follows from the equality (31) (note that (31) holds for all realizations of the messages) that

$$\begin{aligned} & G_1 V_1^{[1]} \neq 0, G_2 V_2^{[1]} = 0, G_3 V_3^{[1]} = 0 && (32)\\ & G_1 V_1^{[2]} = 0, G_2 V_2^{[2]} \neq 0, G_3 V_3^{[2]} = 0 && (33)\\ & G_1 V_1^{[3]} = 0, G_2 V_2^{[3]} = 0, G_3 V_3^{[3]} \neq 0 && (34)\\ & \Rightarrow G_1 \neq 0, G_2 \neq 0, G_3 \neq 0, V_1^{[1]} \neq 0, V_2^{[2]} \neq 0, \\ & \quad V_3^{[3]} \neq 0, V_2^{[1]} = V_3^{[1]} = 0, V_1^{[2]} = V_3^{[2]} = 0, \\ & \quad V_1^{[3]} = V_3^{[3]} = 0 && (35) \end{aligned}$$

Consider now $X_1^{[2]} = U_1^{[2]} Z_1$. From (28), we have

$$\begin{aligned} L &\overset{(28)}{\leq} H(X_1^{[2]}) && (36)\\ &\overset{(29)(35)}{=} H(U_1^{[2]} Z_1) && (37)\\ &= H(Z_1) && (38)\\ &\overset{(12)}{=} \rho L && (39) \end{aligned}$$

where (38) follows from the observation that $U_1^{[2]}$ is not zero, i.e.,

$$U_1^{[2]} \neq 0, \tag{40}$$

as otherwise $H(X_1^{[2]}) = 0$, contradicting (28). Therefore, we have proved that the individual randomness size $\rho \geq 1$. Symmetrically, from (38) and (40), we have

$$L \leq H(Z_2), \quad L \leq H(Z_3), \tag{41}$$

$$U_i^{[k]} \neq 0, \quad k \neq i \tag{42}$$

Next, we consider $(X_1^{[1]}, X_2^{[1]}) = (V_1^{[1]}W_1 + U_1^{[1]}Z_1, U_2^{[1]}Z_2)$.

$$\begin{aligned} &H(X_1^{[1]}, X_2^{[1]}) \\ &\overset{(29)(35)}{=} H(U_2^{[1]}Z_2) + H(V_1^{[1]}W_1 + U_1^{[1]}Z_1 | U_2^{[1]}Z_2) && (43)\\ &\overset{(42)}{\geq} H(Z_2) + H(V_1^{[1]}W_1 + U_1^{[1]}Z_1 | Z_2, Z_1) && (44)\\ &\overset{(41)}{\geq} L + H(V_1^{[1]}W_1 | Z_2, Z_1) && (45)\\ &\overset{(6)}{=} L + H(V_1^{[1]}W_1) && (46)\\ &\overset{(35)(4)}{=} 2L && (47) \end{aligned}$$

Then we consider $H(X_1^{[3]}, X_2^{[3]}) \overset{(29)(35)}{=} H(U_1^{[3]}Z_1, U_2^{[3]}Z_2)$, as follows.

$$\begin{aligned} \eta L &\overset{(13)}{=} H(Z_1, Z_2, Z_3) && (48)\\ &\geq H(Z_1, Z_2) && (49)\\ &\overset{(29)(35)(42)}{=} H(X_1^{[3]}, X_2^{[3]}) && (50)\\ &\overset{(10)}{=} H(X_1^{[1]}, X_2^{[1]}) && (51)\\ &\overset{(47)}{\geq} 2L && (52) \end{aligned}$$

Therefore we have proved that the sum randomness size $\eta \geq 2 = K - 1$.

Remark 5: From (31), we know that the correlated random variables must satisfy some linear equation, i.e., they must lie in a lower dimensional space (rank deficient) for successful decoding.

B. General Proof for Vector Linear Case With Arbitrary K

We generalize the above proof to the vector linear case with arbitrary number of transmitters, K. We show that $H(Z_1) \geq L$ and $H(Z_1, \cdots, Z_{K-1}) \geq (K-1)L$.

The vector linear scheme is represented as follows.

$$X_i^{[k]} = \mathbf{V}_i^{[k]} W_i + \mathbf{U}_i^{[k]} Z_i, \quad i, k \in [1:K] \tag{53}$$

where $\mathbf{V}_i^{[k]}, \mathbf{U}_i^{[k]}$ are $N \times L$ constant encoding matrices, over $\mathbb{F}_p$ (and are globally known). Note that there is no loss of generality in assuming that Z_i contains L symbols over $\mathbb{F}_p$, as we do not impose any statistical properties on the L symbols (e.g., they are not necessarily independent). For any $i, k \in [1:K]$,

$$\begin{aligned} W_k &= \sum_{i=1}^{K} \mathbf{G}_i X_i^{[k]} && (54)\\ &= \sum_{i=1}^{K} \mathbf{G}_i \mathbf{V}_i^{[k]} W_i + \sum_{i=1}^{K} \mathbf{G}_i \mathbf{U}_i^{[k]} Z_i && (55) \end{aligned}$$

The decoding mapping is specified by the constant filtering matrices $\mathbf{G}_i$, each of which has dimension $L \times N$ over $\mathbb{F}_p$. Then we have

$$\operatorname{rank}(\mathbf{G}_k \mathbf{V}_k^{[k]}) = L, \quad k \in [1:K] \tag{56}$$

$$\mathbf{G}_k \mathbf{V}_k^{[i]} = 0, \quad k \neq i, \ i, k \in [1:K] \tag{57}$$

Following the proof presented in the previous section, we proceed to consider $\mathbf{G}_1 \ X_1^{[2]} \overset{(53)(57)}{=} \mathbf{G}_1 \mathbf{U}_1^{[2]} Z_1$.

$$\begin{aligned} L &\overset{(4)}{=} H(W_1) && (58)\\ &\overset{(56)}{=} H(\mathbf{G}_1 \mathbf{V}_1^{[1]} W_1) && (59)\\ &\overset{(6)}{=} H(\mathbf{G}_1 \mathbf{V}_1^{[1]} W_1 | Z_1) && (60)\\ &\overset{(53)}{=} H(\mathbf{G}_1 X_1^{[1]} | Z_1) && (61)\\ &\leq H(\mathbf{G}_1 X_1^{[1]}) && (62)\\ &\overset{(10)}{=} H(\mathbf{G}_1 X_1^{[2]}) && (63)\\ &\overset{(53)(57)}{=} H(\mathbf{G}_1 \mathbf{U}_1^{[2]} Z_1) && (64)\\ &\leq H(Z_1) && (65)\\ &\overset{(12)}{=} \rho L && (66) \end{aligned}$$

where (59) follows from the fact that $\mathbf{G}_1 \mathbf{V}_1^{[1]}$ is invertible such that entropy is preserved. Therefore, we have proved that the individual randomness size $\rho \geq 1$. As a byproduct, from (64), we obtain that

$$\operatorname{rank}(\mathbf{G}_1 \mathbf{U}_1^{[2]}) = L \tag{67}$$

as otherwise we have the contradiction that $H(\mathbf{G}_1 \mathbf{U}_1^{[2]} Z_1) < L$. Symmetrically, from (67), we have

$$\operatorname{rank}(\mathbf{G}_k \mathbf{U}_k^{[i]}) = L, \quad k \neq i \tag{68}$$

Next, we consider the total randomness size. We first prove a lemma.

Lemma 1: For all $i \in [1:K-1]$, we have

$$H(\mathbf{G}_1 X_1^{[i+1]}, \mathbf{G}_2 X_2^{[i+1]}, \cdots, \mathbf{G}_i X_i^{[i+1]}) \geq iL \tag{69}$$

Proof: The proof is based on induction. Note that the basis case where $i = 1$ is proved in (63). Suppose now (69) holds when $i = j$, $j \in [1:K-2]$, i.e.,

$$H(\mathbf{G}_1 X_1^{[j+1]}, \mathbf{G}_2 X_2^{[j+1]}, \cdots, \mathbf{G}_j X_j^{[j+1]}) \geq jL \tag{70}$$

Now consider the case where $i = j + 1$.

$$\begin{aligned} &H(\mathbf{G}_1 X_1^{[j+2]}, \mathbf{G}_2 X_2^{[j+2]}, \cdots, \mathbf{G}_{j+1} X_{j+1}^{[j+2]}) \\ &\overset{(10)}{=} H(\mathbf{G}_1 X_1^{[j+1]}, \mathbf{G}_2 X_2^{[j+1]}, \cdots, \mathbf{G}_{j+1} X_{j+1}^{[j+1]}) && (71)\\ &= H(\mathbf{G}_1 X_1^{[j+1]}, \mathbf{G}_2 X_2^{[j+1]}, \cdots, \mathbf{G}_j X_j^{[j+1]}) \\ &\quad + H(\mathbf{G}_{j+1} X_{j+1}^{[j+1]} | \mathbf{G}_1 X_1^{[j+1]}, \cdots, \mathbf{G}_j X_j^{[j+1]}) && (72)\\ &\overset{(70)(53)(57)}{\geq} jL + H(\mathbf{G}_{j+1} X_{j+1}^{[j+1]} | Z_1, \cdots, Z_j, Z_{j+1}) && (73)\\ &\overset{(53)(57)}{=} jL + H(\mathbf{G}_{j+1} \mathbf{V}_{j+1}^{[j+1]} W_{j+1} | Z_1, \cdots, Z_{j+1}) && (74)\\ &\overset{(6)(56)}{=} jL + H(W_{j+1}) && (75)\\ &\overset{(4)}{=} (j+1)L && (76) \end{aligned}$$

where in (71), we have used the anonymity constraint to change the desired message index from $j+2$ to $j+1$ so that we may proceed with the induction assumption (70). Since both the basis and the inductive steps have been performed, by mathematical induction, we have proved that (69) holds for all $i \in [1 : K-1]$. The proof for Lemma 1 is complete. ∎

Finally, consider (69) and set $i = K-1$. We have

$$(K-1)L \overset{(69)}{\leq} H(X_1^{[K]}, \cdots, X_{K-1}^{[K]}) \tag{77}$$

$$\overset{(53)(57)(68)}{\leq} H(Z_1, \cdots, Z_{K-1}) \tag{78}$$

$$\overset{(13)}{\leq} \eta L \tag{79}$$

where (78) is due to the observation that non-desired signals (from Transmitters 1 to $K-1$ when Transmitter K is the desired) are deterministic functions of the correlated random variables (derived from the properties of the encoding and decoding matrices, see (53)(57)(68)). Therefore we have proved that the sum randomness size $\eta \geq K-1$, for any rate $R = \frac{L}{NK}$.

VII. Proof of Theorem 1: Information Theoretic Converse on Randomness for Capacity Achieving Schemes

We show that when the scheme is capacity achieving, i.e., the rate achieved is $1/K$, i.e., $H(X_i^{[k]}) = N = L, \forall i, k \in [1 : K]$, then the randomness sizes $\rho = 1$ and $\eta = K-1$ are both information theoretically optimal.

A proof outline is as follows. We first show that when the scheme is capacity achieving, the transmitted signals must be uniform (see Lemma 2). Next, combining anonymity and correctness, we prove that for any received signal tuple that differs in one element, the decoded message values must be different as well. This distinctness observation leads to the property that the transmitted signals from non-desired transmitters are deterministic functions of the correlated random variables (see Lemma 3). Finally, this deterministic property for non-desired transmit signals gives us the desired bounds on the size of correlated randomness.

We start with the $K = 3$ setting to illustrate the proof.

A. Proof for Binary Scalar Case When $K = 3$

Before presenting the general proof for arbitrary K, we first consider the $K = 3$ case and assume that each message is one bit, to illustrate the idea. Then in this case, $L = 1$ and the field is $\mathbb{F}_2$. In this case, we need to show that $H(Z_i) \geq 1$ and $H(Z_1, Z_2, Z_3) \geq 2$.

First, for capacity achieving schemes, i.e.,

$$H(X_i^{[k]}) = 1, \quad \forall i, k \in \{1, 2, 3\} \tag{80}$$

the received signal is uniformly random. The proof is deferred to Lemma 2 for the general case. That is, for any k,

$$X_1^{[k]}, X_2^{[k]}, X_3^{[k]} \text{ is uniformly distributed.} \tag{81}$$

Next, consider $X_1^{[2]}, X_2^{[2]}, X_3^{[2]}, W_2$. Note that

$$H(W_2|X_1^{[2]}, X_3^{[2]}) \overset{(5)(6)(7)}{=} H(W_2) \overset{(4)}{=} L \tag{82}$$

$$H(X_2^{[2]}|X_1^{[2]}, X_3^{[2]}) \overset{(81)}{=} L \tag{83}$$

$$H(W_2|X_1^{[2]}, X_2^{[2]}, X_3^{[2]}) \overset{(9)}{=} 0 \tag{84}$$

where (82) follows from the observation that W_2 is only available at Transmitter 2, so it is independent of the transmitted signals from Transmitter 1 and Transmitter 3 (i.e., $X_1^{[2]}, X_3^{[2]}$). (82) and (83) indicate that conditioned on $X_1^{[2]}, X_3^{[2]}$, W_2 and $X_2^{[2]}$ are 2 uniform random variables. Further, (84) states that the uniform random variable W_2 is a deterministic function of the uniform random variable $X_2^{[2]}$ (conditioned on $X_1^{[2]}, X_3^{[2]}$). Then we have the observation that for any realization of $X_1^{[2]}, X_3^{[2]}$, W_2 has a one-to-one mapping to $X_2^{[2]}$, i.e.,

$$H(X_2^{[2]}|W_2, X_1^{[2]}, X_3^{[2]}) = 0 \tag{85}$$

Repeating the argument for W_1 and W_3, we have

$$H(X_1^{[1]}|W_1, X_2^{[1]}, X_3^{[1]}) = 0 \tag{86}$$

$$H(X_3^{[3]}|W_3, X_1^{[3]}, X_2^{[3]}) = 0 \tag{87}$$

From the anonymity constraint (10) and the correctness constraint (9), we know that

$$(X_1^{[1]}, X_2^{[1]}, X_3^{[1]}, g, W_1) \sim (X_1^{[k]}, X_2^{[k]}, X_3^{[k]}, g, W_k) \tag{88}$$

We now consider the individual randomness size. Combining (85) and (88), we have the second element in the tuple of both sides of (88) is deterministic after conditioned on the first, third and last element, i.e.,

$$H(X_2^{[1]}|W_1, X_1^{[1]}, X_3^{[1]}) = 0 \tag{89}$$

Then

$$I(X_2^{[1]}; W_2)$$

$$\leq I(X_2^{[1]}, W_1, X_1^{[1]}, X_3^{[1]}; W_2) \tag{90}$$

$$= I(W_1, X_1^{[1]}, X_3^{[1]}; W_2) + I(X_2^{[1]}; W_2|W_1, X_1^{[1]}, X_3^{[1]}) \tag{91}$$

$$\overset{(89)}{\leq} I(W_1, X_1^{[1]}, Z_1, X_3^{[1]}, W_3, Z_3; W_2) + 0 \tag{92}$$

$$\overset{(5)(6)(7)}{=} 0 \tag{93}$$

and

$$1 \overset{(80)}{=} H(X_2^{[1]}) \tag{94}$$

$$\overset{(7)}{=} I(X_2^{[1]}; W_2, Z_2) \tag{95}$$

$$\overset{(93)}{=} I(X_2^{[1]}; Z_2|W_2) \tag{96}$$

$$\leq H(Z_2) \tag{97}$$

$$\overset{(12)}{=} \rho \tag{98}$$

Therefore the individual randomness size satisfies that $\rho \geq 1$.

We proceed next to consider the sum randomness size. Combining (85), (86), (87) and (88), we have obtained the structure of the decoding mapping, i.e., for any 3-tuple of the received signal, if 2 elements are fixed, the remaining

element has a one-to-one mapping with the desired message. For example, when $Y^{[k]} = (0,0,0)$, suppose that $W_k = g(Y^{[k]}) = g(0,0,0) = w, w \in \{0,1\}$, then $g(0,0,1) = g(0,1,0) = g(1,0,0) = 1-w$. Proceeding along this line, the decoding mapping is uniquely identified as follows.

$Y^{[k]}$	$W_k = g(Y^{[k]})$
$(0,0,0)$	w
$(0,0,1)$	$1-w$
$(0,1,0)$	$1-w$
$(0,1,1)$	w
$(1,0,0)$	$1-w$
$(1,0,1)$	w
$(1,1,0)$	w
$(1,1,1)$	$1-w$

(99)

We are now ready to show that

$$H(X_2^{[1]}, X_3^{[1]} | Z_1, Z_2, Z_3) = 0. \tag{100}$$

Consider an arbitrary realization of $(W_1, Z_1, Z_2, Z_3) = (w_1, z_1, z_2, z_3)$, drawn according to the correct joint distribution (W_1 is independent of Z_1, Z_2, Z_3). Then $X_1^{[1]}$ is a constant (denoted as x_1) as $X_1^{[1]}$ is a function of W_1 and Z_1. We now show that $X_2^{[1]}, X_3^{[1]}$ are now constants as well. Note that the only variables that are random now are W_2, W_3. Suppose $X_2^{[1]}$ is still random, depending on the value of W_2. Then consider two realizations of $X_2^{[1]}$, denoted as $x_2, x_2', x_2 \neq x_2'$ and the received signal realizations

$$y_1 = (x_1, x_2, X_3^{[1]}) \tag{101}$$

$$y_2 = (x_1, x_2', X_3^{[1]}) \tag{102}$$

Note that y_1 and y_2 differ in only one element (i.e., x_2 and x_2') so that from the decoding mapping table, we have $g(y_1) \neq g(y_2)$. However, from the correctness constraint, we know that $g(y_1) = g(y_2) = w_1$. Therefore, we arrive at the contradiction and $X_2^{[1]}, X_3^{[1]}$ are deterministic functions of the correlated random variables. Then we have

$$\eta \overset{(13)}{=} H(Z_1, Z_2, Z_3) \tag{103}$$

$$\overset{(100)}{=} H(X_2^{[1]}, X_3^{[1]}, Z_1, Z_2, Z_3) \tag{104}$$

$$\geq H(X_2^{[1]}, X_3^{[1]}) \tag{105}$$

$$\overset{(81)}{=} 2 \tag{106}$$

Therefore the sum randomness size $\eta \geq 2$ and the proof is complete.

B. Proof for Arbitrary K

We follow the steps of the proof for $K = 3$ binary case and show $H(Z_i) \geq L, H(Z_1, Z_2, \cdots, Z_K) \geq (K-1)L$.

First, we present a lemma, which says that the received signals are uniformly random, when the scheme is capacity achieving.

Lemma 2:

$$H(X_i^{[k]}) = N = L, \quad \forall i, k \in [1:K] \tag{107}$$

$$\Rightarrow H(X_1^{[k]}, \cdots, X_K^{[k]}) = KL, \quad \forall k \in [1:K] \tag{108}$$

Proof: Note that (107) implies that $H(X_1^{[k]}, \cdots, X_K^{[k]}) \leq KL$. It suffices to prove only the other direction. Define $X_{\bar{i}}^{[i]} = (X_1^{[i]}, \cdots . X_{i-1}^{[i]}, X_{i+1}^{[i]}, \cdots, X_K^{[i]})$.

$$H(X_1^{[k]}, \cdots, X_K^{[k]})$$

$$= \sum_{i=1}^{K} H(X_i^{[k]} | X_1^{[k]}, \cdots, X_{i-1}^{[k]}) \tag{109}$$

$$\overset{(10)}{=} \sum_{i=1}^{K} H(X_i^{[i]} | X_1^{[i]}, \cdots, X_{i-1}^{[i]}) \tag{110}$$

$$\geq \sum_{i=1}^{K} H(X_i^{[i]} | X_{\bar{i}}^{[i]}) \tag{111}$$

$$\geq \sum_{i=1}^{K} I(W_i; X_i^{[i]} | X_{\bar{i}}^{[i]}) \tag{112}$$

$$\overset{(9)}{=} \sum_{i=1}^{K} H(W_i | X_{\bar{i}}^{[i]}) \tag{113}$$

$$\geq \sum_{i=1}^{K} H(W_i | X_{\bar{i}}^{[i]}, W_{\bar{i}}, Z_1, \cdots, Z_K) \tag{114}$$

$$\overset{(7)(6)(4)}{=} KL \tag{115}$$

where the last step follows from the fact that the transmitted signal is a deterministic function of the message and the correlated randomness so that the transmitted signal can be eliminated, and then we invoke the independence of the messages and correlated randomness. ■

Next, note that

$$H(W_i | X_{\bar{i}}^{[i]}) \overset{(113)}{=} L, \tag{116}$$

$$H(X_i^{[i]} | X_{\bar{i}}^{[i]}) \overset{(108)}{=} L, \tag{117}$$

$$H(W_i | X_{\bar{i}}^{[i]}, X_i^{[i]}) \overset{(9)}{=} 0 \tag{118}$$

Note that W_i is independent of $X_{\bar{i}}^{[i]}$. Then we have the observation that for any realization of $X_{\bar{i}}^{[i]}$, W_i has a one-to-one mapping to $X_i^{[i]}$, i.e.,

$$H(X_i^{[i]} | W_i, X_{\bar{i}}^{[i]}) = 0 \tag{119}$$

From the anonymity constraint (10) and the correctness constraint (9), we know that for any $i \in [1:K]$,

$$(X_i^{[i]}, X_{\bar{i}}^{[i]}, g, W_i) \sim (X_i^{[1]}, X_{\bar{i}}^{[1]}, g, W_1) \tag{120}$$

Combining (119) and (120), we have

$$H(X_i^{[1]} | W_1, X_{\bar{i}}^{[1]}) = 0 \tag{121}$$

Then for $i \neq 1$,

$$I(X_i^{[1]}; W_i)$$

$$\leq I(X_i^{[1]}, W_1, X_{\bar{i}}^{[1]}; W_i) \tag{122}$$

$$= I(W_1, X_{\bar{i}}^{[1]}; W_i) + I(X_i^{[1]}; W_i | W_1, X_{\bar{i}}^{[1]}) \tag{123}$$

$$\overset{(121)}{\leq} I(W_1, X_{\bar{i}}^{[1]}, Z_{\bar{i}}, W_{\bar{i}}; W_i) + 0 \tag{124}$$

$$\overset{(6)(7)}{=} 0 \tag{125}$$

where $Z_{\bar{i}} = (Z_1, \cdots, Z_{i-1}, Z_{i+1}, \cdots, Z_K)$.

For the individual randomness size, we have

$$L \overset{(107)}{=} H(X_i^{[1]}) \tag{126}$$
$$\overset{(7)}{=} I(X_i^{[1]}; W_i, Z_i) \tag{127}$$
$$\overset{(125)}{=} I(X_i^{[1]}; Z_i|W_i) \tag{128}$$
$$\leq H(Z_i) \tag{129}$$
$$\overset{(12)}{=} \rho L \tag{130}$$

Therefore $\rho \geq 1$.

For the sum randomness size, as (119) holds for all $i \in [1:K]$ and from (120), we know that if any $K-1$ elements of the received signal are determined, the remaining element has a one-to-one mapping with the desired message, which means that

$$\begin{aligned}&\text{For 2 received signal tuples that differ in 1 element,}\\ &\text{i.e., } y_1 = (x_1, \cdots, x_k, \cdots, x_K),\\ &\qquad y_2 = (x_1, \cdots, x_k', \cdots, x_K),\\ &\text{we have } g(y_1) \neq g(y_2).\end{aligned} \tag{131}$$

Then we claim that $X_2^{[1]}, \cdots, X_K^{[1]}$ are functions of $Z_1, \cdots, Z_K$, stated in the following lemma.

Lemma 3:

$$H(X_2^{[1]}, \cdots, X_K^{[1]}|Z_1, \cdots, Z_K) = 0 \tag{132}$$

Proof: Consider an arbitrary realization of $W_1, Z_1, \cdots, Z_K$, denoted as $(W_1, Z_1, \cdots, Z_K) = (w_1, z_1, \cdots, z_K)$. As W_1, Z_1 are fixed, then $X_1^{[1]}$ is a constant, denoted as x_1. We show that $X_2^{[1]}, \cdots, X_K^{[1]}$ are constants now. To set up the proof by contradiction, suppose there exists one $X_k^{[1]}$ that can take multiple values. Denote two such values as $x_k, x_k', x_k \neq x_k'$. The other $X_i^{[1]}, i \neq k$ are assumed to be constants and denoted as x_i. Note that for fixed $z_2. \cdots, z_k$, $X_2^{[1]}, \cdots, X_K^{[1]}$ are conditionally independent as now the randomness only comes from the messages $W_2, \cdots, W_K$ and the messages are independent. We now have two different received signal tuples

$$y_1 = (x_1, \cdots, x_k, \cdots, x_K) \tag{133}$$
$$y_2 = (x_1, \cdots, x_k', \cdots, x_K) \tag{134}$$

From (131), we know that $g(y_1) \neq g(y_2)$. However, this contradicts with the fact that $g(y_1) = g(y_2) = w_1$. Therefore we have arrived at the contradiction and $X_2^{[1]}, \cdots, X_K^{[1]}$ are functions of $Z_1, \cdots, Z_K, W_1$. Further $X_2^{[1]}, \cdots, X_K^{[1]}$ are independent of W_1 so that we only need to condition on $Z_1, \cdots, Z_K$ in (69) (i.e., the conditioning on W_1 is omitted). Therefore we have proved the lemma. ∎

From Lemma 3, we have

$$\eta L \overset{(13)}{=} H(Z_1, \cdots, Z_K) \tag{135}$$
$$\overset{(132)}{=} H(X_2^{[1]}, \cdots, X_K^{[1]}, Z_1, \cdots, Z_K) \tag{136}$$
$$\geq H(X_2^{[1]}, \cdots, X_K^{[1]}) \tag{137}$$
$$\overset{(107)}{=} (K-1)L \tag{138}$$

Therefore the desired sum randomness size bound follows and the proof is complete.

Remark 6: The above proof relies on the assumption that the scheme is capacity achieving. Otherwise, Lemma 2 and Lemma 3 may not hold (i.e., the transmitted signals may not be uniformly random and the non-desired transmitted signals may not be deterministic functions of the correlated randomness, because we may inject useless correlated randomness when the rate is not maximized).

Remark 7: The individual randomness size bound holds without the constraint that the achieved rate is equal to the capacity, i.e., we have $\rho \geq 1$ for any positive rate (the total randomness size bound, however, hinges on the assumption of capacity achieving schemes). A sketch of proof idea is as follows (the above proof is more informative in that the combinatoric structure of the decoding mapping is revealed). We first note that the transmitted signal from Transmitter i, $i \neq 1$ is independent of W_1, i.e., $I(X_i^{[1]}; W_1) = 0$. Next, from the anonymity constraint, the same relation on the mutual information must hold when W_i is desired, i.e., $I(X_i^{[i]}; W_i) = 0$, meaning that the transmitted signal from Transmitter i does not contain any information about W_i. To guarantee this, the randomness needed must be at least as large as the message size.

Remark 8: A more general condition where the bound on the total randomness size holds unconditionally for arbitrary positive rates is when we require the transmitted signal to be deterministic functions of the correlated random variable when he is not desired, i.e., $H(X_i^{[k]}|Z_i) = 0, i \neq k$ (in other words, the messages do not play a role when they are not desired. As the messages are independent among themselves and of the correlated random variables, it will be interesting if they help to reduce total randomness size). Lemma 3 proves that this deterministic condition holds for capacity achieving schemes. After we assume this deterministic condition to be satisfied, the proof is the same as that presented above after Lemma 3.

VIII. Conclusion

We consider the problem of anonymous communications from an information theory perspective. We have characterized the capacity of anonymous communications over a parallel channel with K transmitters and 1 receiver, to be $C = 1/K$. Further, the minimum randomness sizes required are $\rho = 1$ per transmitter and $\eta = K-1$ for all transmitters.

This work represents a step towards using information theoretic tools to understand the fundamental limits of anonymous network communications. Characterizing the capacity of anonymous communication networks under general network topology (beyond one hop), general message setting (beyond one desired message and independent messages) and general transmitter and/or receiver anonymity constraints (beyond only transmitter anonymity) is a promising research avenue. For example, a recent work has considered the generalization to anonymous information delivery over replication based distributed storage systems [17].

References

[1] 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.

[2] H. Sun and S. A. Jafar, "The capacity of robust private information retrieval with colluding databases," *IEEE Trans. Inf. Theory*, vol. 64, no. 4, pp. 2361–2370, Apr. 2018.
[3] 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.
[4] K. Peng, *Anonymous Communication Networks: Protecting Privacy on the Web*. Boca Raton, FL, USA: CRC Press, 2014.
[5] J. Ren and J. Wu, "Survey on anonymous communications in computer networks," *Comput. Commun.*, vol. 33, no. 4, pp. 420–431, 2010.
[6] G. Danezis and C. Diaz, "A survey of anonymous communication channels," Microsoft, Cambridge, U.K., Tech. Rep. MSR-TR-2008-35, 2008.
[7] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Commun. ACM*, vol. 24, no. 2, pp. 84–90, 1981.
[8] D. M. Goldschlag, M. G. Reed, and P. F. Syverson, "Hiding routing information," in *Proc. Int. Workshop Inf. Hiding*. Berlin, Germany: Springer-Verlag, 1996, pp. 137–150.
[9] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second-generation onion router," Naval Res. Lab., Washington, DC, USA, Tech. Rep. 03-1221.1-2602, 2004.
[10] L. V. Ahn, A. Bortz, and N. J. Hopper, "K-anonymous message transmission," in *Proc. 10th ACM Conf. Comput. Commun. Secur.*, 2003, pp. 122–130.
[11] M. K. Reiter and A. D. Rubin, "Crowds: Anonymity for Web transactions," *ACM Trans. Inf. Syst. Secur.*, vol. 1, no. 1, pp. 66–92, 1998.
[12] A. Beimel and S. Dolev, "Buses for anonymous message delivery," *J. Cryptol.*, vol. 16, no. 1, pp. 25–39, 2003.
[13] D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *J. Cryptol.*, vol. 1, no. 1, pp. 65–75, 1988.
[14] M. Waidner and B. Pfitzmann, "The dining cryptographers in the disco: Unconditional sender and recipient untraceability with computationally secure serviceability," in *Advances in Cryptology—EUROCRYPT*. Berlin, Germany: Springer-Verlag, 1989.
[15] S. Dolev and R. Ostrobsky, "Xor-trees for efficient anonymous multicast and reception," *ACM Trans. Inf. Syst. Secur.*, vol. 3, no. 2, pp. 63–84, 2000.
[16] S. A. Jafar, "Topological interference management through index coding," *IEEE Trans. Inf. Theory*, vol. 60, no. 1, pp. 529–568, Jan. 2014.
[17] H. Sun. (2018). "Anonymous information delivery." [Online]. Available: https://arxiv.org/abs/1806.05601

Hua Sun (S'12–M'17) received his B.E. in Communications Engineering from Beijing University of Posts and Telecommunications, Beijing, China, in 2011, M.S. in Electrical and Computer Engineering from University of California Irvine, USA, in 2013, and Ph.D. in Electrical Engineering from University of California Irvine, USA, in 2017. He is an Assistant Professor in the Department of Electrical Engineering at the University of North Texas, USA. His research interests include information theory and its applications to communications, privacy, networking, and storage.

Dr. Sun received the IEEE Jack Keil Wolf ISIT Student Paper Award in 2016, an IEEE GLOBECOM Best Paper Award in 2016, and the University of California Irvine CPCC Fellowship for the year 2011-2012.