Capacity Results for the Wiretapped Oblivious Transfer

Tianyou Pei, Wei Kang$^\text{©}$, Member, IEEE, and Nan Liu$^\text{©}$, Member, IEEE

Abstract—In this paper, we study the problem of the 1-of-2 string oblivious transfer (OT) between Alice and Bob in the presence of a passive eavesdropper Eve. The eavesdropper Eve is not allowed to get any information about the private data of Alice or Bob. When Alice and Bob are honest-but-curious users, we propose a protocol that satisfies 1-private (neither Alice nor Bob colludes with Eve) OT requirements for the binary erasure symmetric broadcast channel, in which the channel provides dependent erasure patterns to Bob and Eve. We find that when the erasure probabilities of the channel are within a certain range, the derived lower and upper bounds on the wiretapped OT capacity meet. Our results generalize and improve upon the results on 1-private wiretapped OT capacity by Mishra et al. Finally, we propose a protocol for a larger class of wiretapped channels and derive a lower bound on the wiretapped OT capacity.

Index Terms—Oblivious transfer (OT), wiretap channel.

I. INTRODUCTION

OBLIVIOUS transfer (OT) is a fundamental research problem in cryptography. It was first introduced in [1] and [2] as a two-party protocol between Alice and Bob to achieve the following function: Alice has a bit Z as the input of the protocol. At the end of the protocol, Bob receives either the bit Z or an erased constant E, each with probability 1/2, while Alice remains ignorant whether the bit Z is erased or not at Bob. This model is later proven to be equivalent [3] to a variant of OT called the 1-of-2 bit oblivious transfer [4]. Crépeau and Savvides later showed that with multiple uses of 1-of-2 bit oblivious transfer protocol, we can construct a 1-of-2 string oblivious transfer protocol [5], which is described as follows. In the 1-of-2 string OT, Alice has two independent binary strings with the same length, denoted as $K_0$ and $K_1$. Bob is interested in retrieving one of the two strings from Alice, say $K_{\Theta}$, while keeping his preference $\Theta$ secret from Alice. We call the random variable $\Theta$ as Bob’s bit, which takes its value in $\{0, 1\}$. At the same time, Alice wishes that Bob knows nothing about the other string, denoted as $K_{\bar{\Theta}}$, where $\bar{\Theta} = 1 - \Theta$. OT is cryptographically important because a secure two-party computation with any function can be constructed from a 1-of-2 string OT protocol [6]. It has been shown that OT can be achieved with noisy resources, either a discrete memoryless multiple source (DMMS) or a noisy discrete memoryless channel (DMC), in addition to the noiseless interactions between Alice and Bob [7], [8], [9], [10], [11].

The 1-of-m string OT problem, which is generalized from 1-of-2 string OT, was first studied from an information theoretic perspective by Nascimento and Winter in [12] and [13]. The purpose of this information theoretical approach is to study how to achieve OT in the optimal way given unlimited computational power at Alice and Bob, rather than just studying whether it is possible to attain OT with a given channel or correlated sources. The authors proposed the concept of OT capacity, which was defined as the minimum amount of noisy resources, e.g., channel uses of the DMC or correlated sources, to achieve OT. In this information theoretic setting, Alice and Bob are assumed to possess unlimited computational power and can conduct unlimited amount of interactive communications through a noiseless public channel. The reason why the amount of noisy resources should be minimized while the noiseless interactive communication can be unlimited, is two fold according to [13]. Firstly, the noisy resources are deemed more expensive and therefore it is desirable to minimize the use of the noisy resource in OT protocol. Secondly, the noiseless interactive communication is given for free, so that we may be more focused on studying the benefit the noise in the channels and correlated sources brings, because it is impossible to achieve OT without noisy resources [14]. The assumption of unlimited and free noiseless interactions can also be found in the problem of secret key generation [15, Definition 2.1], [16, Definition 17.16].

Later on, Ahlswede and Csiszár derived an upper bound on the 1-of-2 string OT capacity for a generic DMC or DMMS [17]. Furthermore, under the setting that the DMC is a binary erasure channel (BEC) and that the users are honest-but-curious, the authors proposed a protocol, which works in the following way [17, Theorem 2]: Alice sends an i.i.d. binary uniform sequence $X^n$ through the BEC $n$ times. Bob receives $Y^n$ and generates a set $G$ consisting of the non-erased positions and a set $B$ of the erased positions and sends $(G, B)$ or $(B, G)$ into the public channel depending
on Bob’s bit. The erasure pattern of Bob, i.e., the positions at which Bob received erasures, is unknown to Alice and therefore is used to conceal Bob’s bit. On the other hand, \(X_B\), the symbols with positions in set \(B\), is erased by the BEC channel, and hence, unknown to Bob, and therefore, can be used by Alice to encrypt \(K_{\Theta}\). The authors showed that the above protocol achieves the upper bound and therefore, they obtained the OT capacity with BEC channel \([17]\). In \([17]\), the authors also studied the OT problem for a class of generalized erasure channels, which introduces noise in the non-erased symbols. The authors proposed a protocol which achieves capacity when erasure probability is greater than or equal to 0.5. This protocol firstly inflates both \(G\) and \(B\), and then applies the technique of random binning on both \(X_G\) and \(X_B\) to generate secret keys to conceal the strings \(K_{\Theta}\) and \(K_{\bar{\Theta}}\), respectively.

The wiretapped OT problem was introduced by Mishra et al. in \([18]\), which includes an eavesdropper Eve in addition to the original Alice and Bob setting, see Fig. 1. The legitimate user Bob and the eavesdropper Eve connect to Alice through a broadcast channel, characterized by transition probability \(P(y, z|x)\), where the input to the channel from Alice is denoted as \(X\), and the outputs received by Bob and Eve are denoted as \(Y\) and \(Z\), respectively. Eve can passively overhear all the communications in the public channel. On top of the OT requirements of Alice and Bob, it is required that Eve can not get any information about the two strings of Alice (\(K_0, K_1\)), nor Bob’s bit \(\Theta\). In this three-party setup, two problems have been proposed in \([18]\). One is 1-privacy, which assumes that neither Alice nor Bob colludes with Eve. The other is 2-privacy, which assumes that Alice or Bob may collude with Eve to obtain more private information. In this paper, we focus on the 1-privacy problem.

For the 1-privacy problem, Mishra et al. \([18]\) mainly studied two special classes of broadcast channels. The first class is where the broadcast channel consists of two independent BECs, which we call independent erasure broadcast channel (IEBC), i.e.,

\[
p(y, z|x) = W(y|x)V(z|x),
\]

where both \(W(y|x)\) and \(V(z|x)\) are BECs. For this class, Mishra et al. obtained the wiretapped OT capacity. The second class is the physically degraded broadcast channel made up of a cascade of two independent BECs, which we call degraded erasure broadcast channel (DEBC), i.e., Alice connects to Bob via a BEC and Bob connects to Eve via another BEC. In other words,

\[
p(y, z|x) = W(y|x)V(z|y),
\]

where both \(W(y|x)\) and \(V(z|y)\) are BECs. In this case, they proposed both lower and upper bounds for the OT capacity for 1-privacy, however, the proposed lower and upper bounds do not meet.

In the wiretapped OT problem, under the setting of IEBC, Eve, like Alice, has no knowledge about the erasure pattern at Bob, and therefore will be ignorant of Bob’s bit \(\Theta\), when \(\Theta\) is concealed by the erasure pattern at Bob \([18, \text{Theorem } 2]\). However, with correlated erasures, such as the DEBC considered in \([18, \text{Theorem } 5]\), Eve can know something about the erasure pattern of Bob from her own erasure pattern, which eventually will leak Bob’s bit to Eve, if Bob chooses to use his erasure pattern to conceal his bit \(\Theta\). To overcome this problem, Mishra et al. \([18, \text{Theorem } 5]\) proposed to utilize the noisy channel \(p(y, z|x)\) to establish some common randomness between Alice and Bob, which is secret from Eve, and then use this common randomness to encrypt the erasure pattern of Bob. By doing so, Eve will be totally ignorant of the erasure pattern of Bob, and therefore Bob’s bit is kept private from Eve. However, a rather large amount of channel resources are needed to generate enough common randomness between Alice and Bob to encrypt the erasure pattern at Bob, and as a result, the protocol in \([18, \text{Theorem } 5]\) achieves a lower bound on the wiretapped OT capacity, which does not meet with the upper bound.

Compared with the non-wiretapped OT problem, another difficulty that arises in the wiretapped OT is that, \(X_G\) and/or \(X_B\) can be partially seen by Eve through the BEC channel, which compromises the security of \(K_{\Theta}\) and \(K_{\bar{\Theta}}\), as they are encrypted directly by \(X_G\) and \(X_B\), respectively. To overcome this difficulty, it is proposed in \([18]\) to adopt the inflation-binning method, which originated from \([17, \text{Remark } 7]\). More specifically, Bob inflates the size of the set \(G\) and \(B\), and Alice uses binning method to obtain secret keys from \(X_G\) and \(X_B\), which are secret from Eve. In applying the inflation-binning method, \([18]\) replaced binning by universal_2 hash functions. Under the IBEC and DBEC model considered in \([18]\), we note that the size of the inflated sets \(G\) and \(B\) will not exceed \(\frac{q}{2}\).

In this paper, we focus on the 1-privacy wiretapped OT problem under the binary erasure symmetric broadcast channel (BESBC). The set of channels under consideration is more general and contains the IEBC and DEBC studied in \([18]\) as special cases. Our novelty compared to the results of 1-privacy in \([18]\) is two-fold. First, we utilize a 1-bit common randomness between Alice and Bob, which is unknown to Eve, to control the order of Alice’s transmission of the encrypted versions of the two strings over the public channel. As a result, Bob’s bit is concealed from Eve even when the erasure pattern of Bob is leaked to Eve. Since the cost of establishing 1 bit common randomness is negligible when the length of the strings are sufficiently large, we find a tighter lower bound on the wiretapped OT capacity. We further show that within a certain range of channel parameters, the proposed lower bound meets the upper bound, and the wiretapped OT capacity is established. Second, given that the BESBC is more general
than the IEBC and DEBC, we may encounter the cases where we need to inflate \( G \) and \( B \) to a size larger than \( \frac{n}{2} \) before feeding them into the universal hash functions. Note that this difficulty does not exist in the IEBC or DEBC studied in [18]. We propose a protocol which reuses part of the non-erased positions at Bob and create some overlap between the sets \( G \) and \( B \). We show that this protocol will not violate the security and privacy constraints due to the observations in [17, Remark 6]. Finally, we utilize the technique of the double random binning and generalize the protocol proposed for the BESBC to the erasure-like broadcast channels, and obtain the corresponding lower bound on the wiretapped OT capacity.

II. System Model

In this paper, we study the 1-of-2 string wiretapped OT problem with 1-privacy, as shown in Fig 1. In this model, there are three entities, namely the database owner Alice, the user Bob and the eavesdropper Eve. We assume that Alice has two strings, each consisting of \( k \) bits, in the database. The two strings, denoted as \( K_0, K_1 \), are independent and uniformly distributed in \( \{0, 1\}^k \). Bob is interested in retrieving one of the string \( K_0, \Theta \), where \( \Theta \) is a binary random variable, uniformly distributed in \( \{0, 1\} \). Eve is interested in the value of \( (K_0, K_1) \) and \( \Theta \). We assume a broadcast channel \( p(y, z|x) \) connecting Alice, Bob and Eve. Alice sends a sequence of \( X^n \) into the broadcast channel and Bob receives \( Y^n \) and Eve receives \( Z^n \). We also assume that through a public channel, Alice and Bob can conduct bounded but arbitrarily large amount of noiseless interactive communications, which will be overheard by Eve. More specifically, Alice and Bob may conduct one round of noiseless communications before the use of broadcast channel, and conduct one round of noiseless communications after each use of the broadcast channel. We assume that in each round of noiseless communications, Bob initiates the transmission and Alice responds with her own transmission. We denote Alice’s transmission before the noisy channel use as \( F_{0a} \) and Bob’s transmission as \( F_{0b} \). The noiseless transmission after the \( i \)-th use of broadcast channel from Alice and Bob are denoted as \( F_{ia} \) and \( F_{ib} \), respectively, for \( i = 1, 2, \ldots, n \). We define

\[
F_a \equiv (F_{0a}, F_{1a}, \ldots, F_{na}),
\]

\[
F_b \equiv (F_{0b}, F_{1b}, \ldots, F_{nb}),
\]

\[
F \equiv (F_a, F_b).
\]

We assume that Alice, Bob and Eve have unlimited computational power. Furthermore, Alice and Bob can perform random experiments independently of each other to provide the required private randomness. Let random variables \( M \) and \( N \) represent the private randomness of Alice and Bob, respectively.

The final knowledge of the two legitimate users and the eavesdropper are

\[
V_A = (K_0, K_1, X^n, M, F),
\]

\[
V_B = (\Theta, Y^n, N, F),
\]

\[
V_E = (Z^n, F).
\]

The functional relations between the above random variables are defined as follows. For \( i = 0, 1, \ldots, n \), we have

\[
X_i = g_i(K_0, K_1, M, F_a^{i-1}, F_b^{i-1}),
\]

\[
F_{ia} = f_{ia}(K_0, K_1, M, F_a^{i-1}, F_b^i),
\]

\[
F_{ib} = f_{ib}(\Theta, N, Y^i, F_a^{i-1}, F_b^i),
\]

where

\[
F_a^{i-1} \equiv (F_{ia}, \ldots, F_{(i-1)a}),
\]

\[
F_b^{-1} \equiv (F_{ib}, \ldots, F_{(i-1)b}).
\]

The decoding function at Bob is

\[
K_{\Theta} = h(N, \Theta, Y^n, F).
\]

Definition 1: Assume a pair of messages \( K_0, K_1 \) with length \( k \) and Bob’s bit \( \Theta \). An \((n, k)\) protocol includes \( n \) uses of noisy channel from Alice to Bob with input \( X^n \) and output \( Y^n \), interactive noiseless communications between Alice and Bob and a decoding function \( h \) at Bob.

We assume that Alice and Bob are honest-but-curious users, which means that they comply with the given protocol but may infer forbidden information from the available information.

Definition 2: A positive rate \( R \) is an achievable wiretapped OT rate with 1-privacy for honest-but-curious users if for every \( \tau, \delta > 0 \), and every sufficiently large \( n \), there exists a \((n, k)\) protocol with \( \frac{k}{n} \geq R - \delta \), such that the following requirements are satisfied.

\[
Pr(K_{\Theta} \neq \hat{K_{\Theta}}) \leq \tau, \quad \text{(Correctness in decoding)},
\]

\[
I(\Theta; V_A) \leq \tau, \quad \text{(Privacy at Alice)},
\]

\[
I(K_{\Theta}; V_B) \leq \tau, \quad \text{(Security at Bob)},
\]

\[
I(\Theta, K_{\Theta}, \hat{K_{\Theta}}; V_E) \leq \tau, \quad \text{(Privacy and Security at Eve)}.
\]

The supremum of achievable wiretapped OT rate with 1-privacy is defined as the wiretapped OT capacity with 1-privacy, denoted as \( C \).

In this paper, we first focus on the case where the noisy channel is a BESBC, i.e.,

\[
Pr(Y = y, Z = z | X = x) = W(y|x)V(z|y, x),
\]

where the input and output alphabets are \( X = \{0, 1\}, Y = Z = \{0, 1, E\} \), and the symbol \( E \) denotes the erasure. \( W(y|x) \) is a BEC with the probability of erasure being \( \epsilon_1 \), denoted as BEC(\( \epsilon_1 \)). \( V(z|y, x) \) is a symmetric channel in the sense that no matter \( x = 0 \) or \( 1 \),

\[
V(Z = E|Y = E, X = x) = \epsilon_2,
\]

\[
V(Z = E|Y = x, X = x) = \epsilon_3.
\]

Therefore, the joint probability of the erasures at \( Y \) and \( Z \) is,

\[
Pr(Y = E, Z = E|X = x) = \epsilon_1 \epsilon_2, \quad \text{(22)}
\]

\[
Pr(Y = E, Z \neq E|X = x) = \epsilon_1 (1 - \epsilon_2), \quad \text{(23)}
\]

\[
Pr(Y \neq E, Z = E|X = x) = (1 - \epsilon_1) \epsilon_3, \quad \text{(24)}
\]

\[
Pr(Y = E, Z = E|X = x) = (1 - \epsilon_1)(1 - \epsilon_3), \quad \text{(25)}
\]

as given in Fig. 2.
In other words, $\epsilon_2$ represents the probability that $Z$ is erased given that $Y$ is erased, no matter the input $X$, and $\epsilon_3$ represents the probability that $Z$ is erased given $Y$ is not erased, no matter the input $X$. The above implies that for $x = 0, 1$, we have

$$V(Z = x|Y = E, X = x) = 1 - \epsilon_2,$$  \hspace{1cm} (26)

$$V(Z = x|Y = E, X = x) = 0,$$  \hspace{1cm} (27)

$$V(Z = x|Y = x, X = x) = 1 - \epsilon_3,$$  \hspace{1cm} (28)

$$V(Z = 1 - x|Y = x, X = x) = 0.$$  \hspace{1cm} (29)

Note that the IEBC and DEBC studied in [18] can be viewed as special cases of our model where by setting $\epsilon_2 = \epsilon_3$, we obtain the IEBC [18], and by setting $\epsilon_2 = 1$, we obtain the DEBC [18].

In addition to BESBC, we also investigate a more general class of erasure-like broadcast channel as follows. In [17], a more general class of erasure-like memoryless channels are studied, where the channel can be represented as a mixture of two channels with identical input alphabet $\mathcal{X}$ and disjoint output alphabets $\mathcal{Y}_0$ and $\mathcal{Y}_1$, namely as

$$W(y | x) = \begin{cases} 
(1 - \epsilon) W_0(y | x), & x \in \mathcal{X}, y \in \mathcal{Y}_0, \\
\epsilon W_1(y | x), & x \in \mathcal{X}, y \in \mathcal{Y}_1.
\end{cases}$$  \hspace{1cm} (30)

In the later sections, we will study the wiretapped OT problem, where the channel from Alice to Bob and the channel from Alice to Eve are both of the form (30). More specifically, with disjoint sets $\mathcal{Y}_0, \mathcal{Y}_1, \mathcal{Z}_0, \mathcal{Z}_1$, we have that for every $x \in \mathcal{X}$

$$\Pr[Y = y, Z = z | X = x] = \begin{cases} 
(1 - \epsilon_1)(1 - \epsilon_3) W_0(y | x) V_0(z | x), & y \in \mathcal{Y}_0, z \in \mathcal{Z}_0, \\
(1 - \epsilon_1) \epsilon_3 W_0(y | x) V_1(z | x), & y \in \mathcal{Y}_0, z \in \mathcal{Z}_1, \\
\epsilon_1(1 - \epsilon_2) W_1(y | x) V_0(z | x), & y \in \mathcal{Y}_1, z \in \mathcal{Z}_0, \\
\epsilon_1 \epsilon_2 W_1(y | x) V_1(z | x), & y \in \mathcal{Y}_1, z \in \mathcal{Z}_1,
\end{cases}$$  \hspace{1cm} (31)

for some channels $W_0$ defined on $\mathcal{X} \times \mathcal{Y}_0$, $W_1$ defined on $\mathcal{X} \times \mathcal{Y}_1$, $V_0$ defined on $\mathcal{X} \times \mathcal{Z}_0$, and $V_1$ defined on $\mathcal{X} \times \mathcal{Z}_1$.

III. CAPACITY RESULTS FOR THE WIRETAPPED OT FOR THE BESBC

A. Main Results

We first propose a converse result in the following theorem, which provides an upper bound on the capacity of the wiretapped OT in the case of a BESBC.

**Theorem 1:** The wiretapped OT capacity with 1-privacy for honest-but-curious users for the BESBC satisfies

$$C \leq \min \left( \epsilon_3(1 - \epsilon_1), \epsilon_1, \frac{1}{2}(\epsilon_1 \epsilon_2 + \epsilon_3(1 - \epsilon_1)) \right).$$  \hspace{1cm} (32)

Theorem 1 will be proven in Section III-B. The proof follows similar ideas as those in [17, Theorem 1] and [18, Lemma 4].

The next theorem states an achievability result, which is a lower bound on the wiretapped OT capacity of the BESBC. However it is only valid for $\epsilon_2 \geq \epsilon_3$.

**Theorem 2:** A lower bound on the wiretapped OT capacity with 1-privacy for honest-but-curious users for the BESBC is

$$C \geq \min \left( \epsilon_3(1 - \epsilon_1), \epsilon_1, \frac{1}{2}(\epsilon_1 \epsilon_2 + \epsilon_3(1 - \epsilon_1)) \right),$$  \hspace{1cm} (33)

if $\epsilon_2 \geq \epsilon_3$.

**Remark 1:** It is straightforward to see that the upper bound in Theorem 1 and the lower bound in Theorem 2 meet if $\epsilon_2 \geq \epsilon_3$, which means that we have obtained the wiretapped OT capacity of the BESBC under the condition $\epsilon_2 \geq \epsilon_3$.

Furthermore, we can see that the condition $\epsilon_2 \geq \epsilon_3$, under which we have obtained the OT capacity, includes the two cases studied in [18]:

1) In the case of IEBC, i.e., $\epsilon_2 = \epsilon_3$, our capacity result collapses to [18, Theorem 1].

2) In the case of DEBC, i.e., $\epsilon_2 = 1$, our capacity result coincides with the upper bound given in [18, Theorem 5], and is strictly better than the lower bound in [18, Theorem 5].

Therefore, the improvement of our capacity results over the results of 1-privacy in [18] are:

1) We propose an upper bound on the wiretapped OT capacity for general $\epsilon_1, \epsilon_2$ and $\epsilon_3$, while [18] has an upper bound on the wiretapped OT capacity in the two special cases of $\epsilon_2 = \epsilon_3$ and $\epsilon_2 = 1$.

2) We propose a lower bound on the wiretapped OT capacity when $\epsilon_2 \geq \epsilon_3$, while [18] has lower bounds on the wiretapped OT capacity in the two special cases of $\epsilon_2 = 1$ and $\epsilon_2 = \epsilon_3$.

3) For $\epsilon_2 = 1$: we propose a protocol that performs strictly better than the protocol proposed in [18]. Moreover, our protocol is shown to be capacity-achieving.

4) For $1 \geq \epsilon_2 > \epsilon_3$: we found the capacity of this case, which is not studied in [18].

B. Proof of Theorem 1

For Theorem 1, we need to prove that the 1-private OT rate $R$ for the binary broadcast symmetric erasure channel is bounded above by

$$\min \left( (1 - \epsilon_1) \epsilon_3, \epsilon_1, \frac{1}{2}(\epsilon_1 \epsilon_2 + \epsilon_3(1 - \epsilon_1)) \right),$$  \hspace{1cm} (34)

which is equivalent to

$$R \leq \min_{p_X} \max_{p_Y} I(X; Y | Z), \max_{p_X} H(Y | X), \max_{p_X} \frac{1}{2} H(X | Z).$$  \hspace{1cm} (35)

Firstly, we view $K_0$ as common randomness established between Alice and Bob, given eavesdropper Eve observing $F$ and $Z^n$. Then, $I(X; Y | Z)$, which is the upper bound on the capacity of the corresponding secret key generation problem [15, Theorem 1], [19, Theorem 22.6], can serve as an upper
bound on the OT capacity. This same argument is also used in [17] and [18].

Secondly, $H(X|Y)$, which is an upper bound on OT capacity without eavesdropper [17, Theorem 1], also serves as an upper bound on OT capacity with eavesdropper.

For the third term, i.e., $R \leq \max_{P_X} \frac{1}{2} H(X|Z)$, we follow the similar steps as those in [18, Lemma 4] as follows

$$2k = H(K_0, K_1)$$

$$= I(K_0, K_1; X^n, F) + H(K_0, K_1|X^n, F)$$

$$\leq I(K_0, K_1; X^n, F) + n\delta$$

$$\leq I(K_0, K_1; Z^n, F) + n\delta$$

$$= I(K_0, K_1; Z^n, F) + I(K_0, K_1; X^n|Z^n, F) + n\delta$$

$$\leq H(X^n|Z^n, F) - H(X^n|Z^n, F, K_0, K_1) + 2n\delta$$

$$\leq H(X^n|Z^n, F) + 2n\delta$$

$$\leq n(\epsilon_1\epsilon_2 + \epsilon_3(1 - \epsilon_1)) + 2n\delta,$$

(36)

where (a) is due to [18, Lemma 5], and (b) is because of the condition (18). Note that the property $H(K_0, K_1|X^n, F) \leq n\delta$ follows directly from [18, Lemma 5] because the proof of [18, Lemma 5] is based on the decoding requirement at Bob and the privacy requirement at Alice, and it does not involve the observation of the eavesdropper Eve. Therefore this lemma is valid no matter what Eve observes. In other words, this lemma can be applied to not only IEBC as in [18, Theorem 1], but also the wiretapped OT with any BESBC channels as in Theorem 1 in this paper.

C. Proof of Theorem 2

1) Motivations: We first note the general idea of the proof of Theorem 2 here. To motivate our scheme, we briefly review the existing achievability schemes proposed for the OT under the setting of the BEC by Ahlswede and Csiszar [17] and the wiretapped OT under the setting of the IEBC and DEBC by Mishra et al. [18, Theorem 1 and 5].

Review of the scheme by Ahlswede-Csiszar: We begin with the scheme by Ahlswede and Csiszar [17]. Alice sends an i.i.d. binary uniform sequence $X^n$ through a binary erasure channel. Bob receives the sequence perfectly in some positions and erasures in others. Bob forms a set $G \subset \{1, \ldots, n\}$ which is a subset of the positions of the non-erased $Y^n$, and another set $B \subset \{1, \ldots, n\}$ which is a subset of the positions of the erased $Y^n$. It is required that $|G| = |B|$ and they are both equal to the length of the strings at Alice, i.e., $k$. If Bob wants to retrieve $K_0$, then define $(L_0, L_1) = (G, B)$, otherwise define $(L_0, L_1) = (B, G)$. Bob sends $(L_0, L_1)$ to Alice via the noiseless public channel. Alice retrieves the corresponding parts from $X^n$, i.e., $X_{L_0}, X_{L_1}$. These two parts are used as secret keys to encrypt the strings $K_0, K_1$, and then Alice sends $K_0 \oplus X_{L_0}$ and $K_1 \oplus X_{L_1}$ to Bob via the public channel. The privacy of Bob’s bit at Alice hinges on the fact that Alice has no knowledge about the erasure pattern at Bob, i.e., $B$ or $G$, and therefore could not tell whether $(L_0, L_1) = (G, B)$ or $(L_0, L_1) = (B, G)$. Security at Bob is guaranteed because Bob only has the knowledge of $X_G$ and no knowledge at all about $X_B$.

Review of the scheme by Mishra et al.: For the wiretapped OT problem, in IEBC, i.e., $\epsilon_2 = \epsilon_3$, Eve naturally has no knowledge about Bob’s bit, because Eve, like Alice, has no knowledge about the erasure pattern at Bob. However, for correlated erasures, i.e., $\epsilon_2 \neq \epsilon_3$, such as the DEBC studied in [18, Theorem 2] with $\epsilon_2 = 1$, Eve can determine $(L_0, L_1) = (G, B)$ or $(L_0, L_1) = (B, G)$ with certainty if the sequence length $n$ is sufficiently large, and this leaks Bob’s bit $\Theta$ to Eve. To cope with this problem, Mishra et al. [18, Theorem 5] proposed to utilize the noisy channel to establish some common randomness between Alice and Bob, which is secret from Eve, and then use this common randomness to encrypt $(L_0, L_1)$. By doing so, Eve will be totally ignorant of $(L_0, L_1)$, and therefore can not tell if it is $(G, B)$ or $(B, G)$. Thus, Bob’s bit is kept private from Eve.

We note the following two points in the protocol designed in [18, Theorem 5]:

1) It requires a large amount of channel resources, i.e., $2|L_0|$ bits of common information between Alice and Bob to generate two secret keys to encrypt $L_0$ and $L_1$. As a result, the rate of the protocol in [18, Theorem 5] does not meet the upper bound.

2) Fundamentally, it is only required that Eve be ignorant of Bob’s bit $\Theta$, but not the values of $(L_0, L_1)$.

Therefore, in this paper, we design a protocol that allows Eve to gain the knowledge of $(L_0, L_1)$ but prevents Eve from learning the value of Bob’s bit $\Theta$.

Proof sketch of Theorem 2: We note that in the protocols by both Ahlswede and Csiszar [17] and Mishra et al. [18, Theorem 5], Alice is supposed to send the encrypted versions of $K_0, K_1$ into the public channel in the fixed order, i.e, $K_0$ first and then $K_1$. This fixed order directly connects $(G, B)$ and Bob’s bit $\Theta$. More specifically, if we know $(L_0, L_1) = (G, B)$, then we know $\Theta = 0$; otherwise, $\Theta = 1$. With the above understanding, we propose to change the fixed order to a random order. We design a binary random variable $S$ to control the order. If $S = 0$, we send the encrypted version of $K_0, K_1$ in this order into the public channel, and if $S = 1$, we send encrypted $K_1, K_0$ in this order into the public channel. As long as Bob knows the value of $S$, the protocol still works. At the same time, Eve knows nothing about $\Theta$ even with the knowledge of $(L_0, L_1)$ equal to $(G, B)$ or $(B, G)$. It is obvious that, in this setting, we only need to establish 1 bit of common randomness between Alice and Bob, that is secret to Eve. The burden of doing so is negligible in terms of the rate.

Another problem in the wiretapped OT is that with the presence of eavesdropper Eve, Alice and Bob need to use universal2 hash functions (or random binning from the information theoretic perspective) to establish some common randomness, which is secret to Eve, to encrypt $K_0, K_1$. To establish a common randomness with length $nR$, we need to form sets $G$ and $B$ from the non-erased and erased coordinates with length $n\beta \approx \frac{nR}{\epsilon_2}$. When $\beta > \frac{1}{2}$, we face the problem of not having enough separate coordinates to place into the sets $G$ and $B$. Note that $\beta > \frac{1}{2}$ will not occur in
the IEBC or DEBC studied in [18], i.e., $\epsilon_2 = \epsilon_3$, or $\epsilon_2 = 1$. However, when we generalize the model to $\epsilon_2 \geq \epsilon_3$, we will face this difficulty. As pointed out in [17, Remark 6], the correlation between $X_G$ and $X_B$ does not matter as long as $X_G$ has the same distribution as $X_B$. Therefore, we propose to allocate part of the non-erased coordinates to both sets $G$ and $B$, which results in some overlap between $G$ and $B$. By doing so, our proposed protocol attains security and privacy when $\beta > \frac{1}{2}$. Next, we will propose a protocol, which achieves the wiretapped OT rate in this theorem.

2) Protocol: Our protocol includes the following 8 steps.

In Step 1, Alice sends an i.i.d binary uniform sequence $X^n$ into the broadcast channel. Bob observes $Y^n$ and Eve observes $Z^n$.

In Step 2, Alice and Bob use universal2 hash functions to establish a 1-bit common randomness $S$, which is concealed against Eve. More specifically, Bob randomly picks $n\alpha$ bits from the non-erased coordinates, called $L$, and $n\alpha$ is a natural number. Then, Bob uniformly picks a function $F_\alpha$ from a family $F$ of universal2 hash functions [20] (see Appendix A for details):

$$F_\alpha : \{0,1\}^{n\alpha} \rightarrow \{0,1\}^{n(\epsilon_3-\delta)n},$$

(37)

where $\delta \in (0,1)$, and $\alpha(\epsilon_3-\delta)n$ is a natural number. Bob applies the function $F_\alpha$ on $X_{L,\alpha}$ and retrieves the first bit of $F_\alpha(X_{L,\alpha})$, denoted by $K_\alpha$, and independently generates a uniform bit $S$. Bob sends $L, F_\alpha, K_\alpha \oplus S$ into the public channel. Upon receiving $L, F_\alpha, K_\alpha \oplus S$, Alice locates the positions $L, F_\alpha$ and finds the corresponding channel inputs $X_{L,\alpha}$. Alice then applies the function $F_\alpha$ on $X_{L,\alpha}$ and retrieve the first bit of the output of the function, which is $K_\alpha$. Then Alice recovers $S$ from $K_\alpha$ and $K_\alpha \oplus S$.

In Step 3, Bob generates sets $G$ and $B$ as follows. Define $\beta = \frac{R - \epsilon_1 - 1}{\epsilon_1}$ such that $n\beta$ is a natural number, and

$$R < \min \left( \epsilon_3(1-\epsilon_1), \epsilon_1, \frac{1}{2}(\epsilon_1 \epsilon_2 + \epsilon_3(1-\epsilon_1)) \right).$$

(38)

Bob uniformly selects $n\beta$ coordinates from the non-erased coordinates except the set $L,\alpha$ defined in Step 2 and names the set of the corresponding locations as $G$.

Next Bob will form the set $B$, which falls into one of the following three cases:

1) If $\beta < \epsilon_1$ and $\beta < \frac{1}{2}$, Bob uniformly selects $n\beta$ coordinates from the erased coordinates and name the set of corresponding locations as $B$, see Subfigure 3(a) and 3(b) for two sub-cases, $\beta < \frac{1}{2} < \epsilon_1$ and $\beta < \epsilon_1 \leq \frac{1}{2}$. The choice of $B$ in this case is similar to [17, Theorem 2].

2) If $\epsilon_1 \leq \beta < \frac{1}{2}$. Bob collects all erased coordinates, and we denote the number of the erased coordinates as $n_e$. Bob then uniformly selects $n\beta - n_e$ coordinates from the unused non-erased coordinates, which are the non-erased coordinates that are not in sets $G$ or $L,\alpha$. Bob names the set of corresponding locations as $B$, see Subfigure 3(c). The choice of $B$ in this case is similar to [17, Remark 7] and [18, Theorem 1].

3) If $\beta \geq \frac{1}{2}$, Bob first collects all the coordinates, which are not included in $G$ or $L,\alpha$. Bob then uniformly selects $n(2\beta - 1)$ coordinates from $G$. Bob names the set of locations corresponding to the above two parts of coordinates as $B$, see Subfigure 3(d), where the grey area indicates the part in $B$, chosen from $G$. The choice of $B$ overlapping with $G$ in this case is a novel step that we propose in this paper.

In Step 4, Bob checks the value of $\Theta$ and $S$, or more specifically, the value of $\Theta \oplus S$, and define the set $(L_0, L_1)$ as

$$L_0 \oplus S = G,$$

(39)

$$L_0 \oplus S = B,$$

(40)

or more specifically,

$$(L_0, L_1) = \begin{cases} (G, B), & \text{if } \Theta \oplus S = 0, \\ (B, G), & \text{if } \Theta \oplus S = 1. \end{cases}$$

(41)

Bob then sends $(L_0, L_1)$ to Alice through the public channel.

In Step 5, Alice randomly and independently chooses functions $F_0, F_1$ from a family $F$ of universal2 hash functions:

$$F_0, F_1 : \{0,1\}^{\beta n} \rightarrow \{0,1\}^{n(R-\delta)},$$

(42)
where \( \delta \in (0, R) \), and \( n(R - \delta) \) is a natural number. Alice then applies functions \( F_0 \) and \( F_1 \) on \( X_{L_0} \) and \( X_{L_1} \), respectively, and obtains \( \tilde{X}_{L_0} \) and \( \tilde{X}_{L_1} \).

In Step 6, Alice checks the value of the 1 bit common information \( S \) and uses \( \tilde{X}_{L_0} \) and \( \tilde{X}_{L_1} \) to encrypt \( K_S \) and \( K_{\tilde{S}} \) and obtain \((\tilde{X}_{L_0} \oplus K_S, \tilde{X}_{L_1} \oplus K_{\tilde{S}})\), where \( \tilde{S} = 1 - S \).

In Step 7, Alice sends \((F_0, F_1, \tilde{X}_{L_0} \oplus K_0, \tilde{X}_{L_1} \oplus K_1)\) into the public channel. More specifically,

1. If \( S = 0 \), then send \((F_0, F_1, K_0, \tilde{X}_{L_1} \oplus K_1)\) into the public channel in this order.
2. If \( S = 1 \), then send \((F_0, F_1, K_0, \tilde{X}_{L_1} \oplus K_0)\) into the public channel in this order.

In Step 8, upon receiving \((F_0, F_1, \tilde{X}_{L_0} \oplus K_0, \tilde{X}_{L_1} \oplus K_0)\), Bob, with the knowledge of \( S, \Theta \), will recover \( K_0 \) as follows. Let us assume \( S = 0 \) and \( \Theta = 0 \). Then Bob can determine that \( L_{S \Theta} = \tilde{L}_0 = G \). With the knowledge of \( S = 0 \), Bob can locate \( F_0, \tilde{X}_{L_0} \oplus K_0 \) from the received information from Alice in Step 7. Bob then applies \( F_0 \) to \( X_{L_0} = X_G \), which is not-erased at Bob according to the generation of \( G \) in Step 3, and obtain \( \tilde{X}_{L_0} \). Bob thus decodes \( K_0 \) from \( \tilde{X}_{L_0} \oplus K_0 \), which is received from the public channel, and \( \tilde{X}_{L_0} \), which is calculated according to above procedure. For the other values of \( S \) and \( \Theta \), the decoding procedure at Bob can be derived in a similar manner.

3. \textbf{Performance Analysis:} We assume positive quantities \( \alpha, \delta, \bar{\delta}, \tilde{\delta} \) satisfying \( \bar{\delta} > \epsilon_3 \delta + \epsilon_3 \alpha + \delta \) and \( \epsilon_3 > \bar{\delta} > \delta \). By letting \( \delta \) be arbitrarily small, which implies arbitrarily small \( \alpha \) and \( \delta \), we show that the rate 

   \[
   \text{min}\{\epsilon_3(1 - \epsilon_1), \epsilon_1, \frac{1}{2}(\epsilon_1 \epsilon_2 + \epsilon_3 (1 - \epsilon_1))\}
   \]

   is achievable in the following lemma, where we will prove that the correctness, security and privacy constraints in (15)-(18) are satisfied.

   \textbf{Lemma 1:} The above proposed protocol achieves any wiretapped OT rate

   \[
   R < \text{min}\left(\epsilon_3(1 - \epsilon_1), \epsilon_1, \frac{1}{2}(\epsilon_1 \epsilon_2 + \epsilon_3 (1 - \epsilon_1))\right),
   \]

   with 1-privacy for the BESBC where the users are honest-but-curious and \( \epsilon_2 \geq \epsilon_3 \).

   \textbf{Lemma 1} is proved in Appendix A.

IV. EXTENSIONS BEYOND BESBC

In the previous section, we focused on the wiretapped OT problem for BESBC. In this section, we will follow [17, Theorem 4] and generalize our results to a larger class of broadcast channels as defined in (31).

We first define the following quantities:

\[
R_0 \triangleq I(X; Y_0) - I(X; Y_1),
\]

\[
R_{00} \triangleq I(X; Y_0) - I(X; Z_0),
\]

\[
R_{10} \triangleq I(X; Y_1) - I(X; Z_0),
\]

\[
R_{11} \triangleq I(X; Y_1) - I(X; Z_1),
\]

\[
R_{G} \triangleq (1 - \epsilon_3)R_{00} + \epsilon_3 R_{01},
\]

\[
R_B \triangleq (1 - \epsilon_2)R_{10} + \epsilon_2 R_{11},
\]

where random variables \((X, Y_0, Y_1, Z_0, Z_1)\) satisfy the following joint distribution

\[
P_{X,Y_0,Y_1,Z_0,Z_1}(x, y_0, y_1, z_0, z_1) = P_{X}(x)W_0(y_0|x)W_1(y_1|x)V_0(z_0|x)V_1(z_1|x),
\]

for \( x \in X, y_0 \in Y_0, y_1 \in Y_1, z_0 \in Z_0, z_1 \in Z_1. \) (51)

Then, we have the following theorem.

\textbf{Theorem 3:} A lower bound on the wiretapped OT capacity with 1-privacy, for honest-but-curious users when the broadcast channel is of the form (31), is

\[
\max_{X} \max_{\gamma_1, \gamma_2, \tau_1, \tau_2} \min_{\gamma_1 R_G + (\gamma_1 - \gamma_2)R_0^+} \left\{ (\gamma_1 - \gamma_2)R_0^+ \right\},
\]

where the parameters \( \gamma_1, \gamma_2, \tau_1, \tau_2 \) satisfy

\[
\gamma_1 + \tau_1 = \gamma_2 + \tau_2 = \beta,
\]

\[
0 \leq \beta \leq 1,
\]

\[
\gamma_1, \gamma_2 \leq 1 - \epsilon_1,
\]

\[
\tau_1, \tau_2 \leq \epsilon_1,
\]

and

\[
\tilde{R} \triangleq \min[\gamma_1 + \gamma_2, (1 - \epsilon_1)]R_G + \min[\gamma_1 + \gamma_2, \epsilon_1]R_B + (\gamma_1 - \gamma_2)R_0.
\]

\textbf{Proof:} We first briefly overview the general idea of our scheme, then we will present the protocol, and at the end, we will analyze the performance of the protocol in Lemma 2.

\textbf{Overview of scheme:} We first use a negligible amount of the uses of the noisy channel to establish 1 bit of common randomness \( S \) between Alice and Bob, which is secret from Eve. We will use this random bit to ensure Bob’s privacy at Eve.

We then assume that Bob forms the sets \( G \) and \( B \) such that the set \( G \) consists of around \( n\gamma_1 \) coordinates from the symbols in \( Y_0 \) and \( n\gamma_2 \) coordinates from the symbols in \( Y_1 \), and similarly the set \( B \) contains around \( n\tau_2 \) coordinates from the symbols in \( Y_0 \) and \( n\tau_2 \) coordinates from the symbols in \( Y_1 \).

The novelty here is that we allow the reuse of coordinates from both \( Y_0 \) and \( Y_1 \), in contrast to reusing only non-erased coordinates in Theorem 2. We also allow \( G \) to contain coordinates from both \( Y_0 \) and \( Y_1 \), while in Theorem 2, only non-erased coordinates are included in \( G \).

Then we will not use the universal2 hash function, but use the schemes of the secret key generation, i.e., double binning, as suggested by [17, Proposition 1], to generate common randomness between Alice and Bob.

\textbf{Protocol:} Formally, our protocol includes the following steps. Assume a given distribution \( P_X \)

In Step 1, Alice sends an i.i.d. sequence \( X^n \) according to distribution \( P_X \) into the broadcast channel. Bob observes \( Y^n \) and Eve observes \( Z^n \).

In Step 2, Alice and Bob generates a secret key, which is concealed against Eve. More specifically, Bob randomly pick
Symbols from his received symbols $Y_i$ for $i = 1, \ldots, n$, which fall in $\mathcal{Y}_0$. We denote the locations of the picked symbols as $\mathcal{L}_n$. Then Bob applies the secret key generation scheme on $Y_{\mathcal{L}_n}$ to obtain a binary function $K_n = \phi(Y_{\mathcal{L}_n})$, which is shared with Alice with probability $1$. Bob generates a binary random variable $S$ and sends $K_n \oplus S$ to Alice through the public channel. Alice can recover $S$ from $K_n \oplus S$ and $K_n$.

In Step 3, Bob generates sets $G$ and $B$ as follows. For each coordinate $i$, define four events as follows.

$$
A_i \triangleq \{ i \in G \text{ and } i \notin B \}, \\
B_i \triangleq \{ i \notin G \text{ and } i \in B \}, \\
C_i \triangleq \{ i \in G \text{ and } i \in B \}, \\
D_i \triangleq \{ i \notin G \text{ and } i \notin B \}.
$$

For $i$ such that $Y_i \in \mathcal{Y}_0 \setminus \mathcal{Y}_{\mathcal{L}_n}$, if $\gamma_1 + \gamma_2 \leq 1 - \epsilon_1 - \alpha$, we have

$$
Pr(A_i) = \frac{\gamma_1}{1 - \epsilon_1 - \alpha}, \\
Pr(B_i) = \frac{\gamma_2}{1 - \epsilon_1 - \alpha}, \\
Pr(C_i) = 0, \\
Pr(D_i) = 1 - \frac{\alpha - \gamma_1 - \gamma_2}{1 - \epsilon_1 - \alpha},
$$

and if $\gamma_1 + \gamma_2 > 1 - \epsilon_1 - \alpha$, we have

$$
Pr(A_i) = \frac{1 - \epsilon_1 - \alpha - \gamma_2}{1 - \epsilon_1 - \alpha}, \\
Pr(B_i) = \frac{1 - \epsilon_1 - \alpha - \gamma_1}{1 - \epsilon_1 - \alpha}, \\
Pr(C_i) = \frac{\gamma_1 + \gamma_2 - 1 + \epsilon_1}{1 - \epsilon_1 - \alpha}, \\
Pr(D_i) = 0.
$$

Similarly, for $i$ such that $Y_i \in \mathcal{Y}_1$, if $\tau_1 + \tau_2 \leq \epsilon_1$, we have

$$
Pr(A_i) = \frac{\tau_1}{\epsilon_1}, \\
Pr(B_i) = \frac{\tau_2}{\epsilon_1}, \\
Pr(C_i) = 0, \\
Pr(D_i) = \frac{\epsilon_1 - \tau_1 - \tau_2}{\epsilon_1},
$$

and if $\tau_1 + \tau_2 > \epsilon_1$, we have

$$
Pr(A_i) = \frac{\epsilon_1 - \tau_2}{\epsilon_1}, \\
Pr(B_i) = \frac{\epsilon_1 - \tau_1}{\epsilon_1}, \\
Pr(C_i) = \frac{\tau_1 + \tau_2 - \epsilon_1}{\epsilon_1}, \\
Pr(D_i) = 0.
$$

We observe that

$$
Pr(i \in G) = Pr(i \in B) = \beta = \gamma_1 + \tau_1 = \gamma_2 + \tau_2.
$$

In Step 4, Bob defines the set $(\mathcal{L}_0, \mathcal{L}_1)$ as

$$
(\mathcal{L}_0, \mathcal{L}_1) = \begin{cases} 
(G, B), & \text{if } \Theta \oplus S = 0, \\
(B, G), & \text{if } \Theta \oplus S = 1.
\end{cases}
$$

Bob then sends $(\mathcal{L}_0, \mathcal{L}_1)$ to Alice through the public channel.

In Step 5, Alice applies the secret key generation schemes on both $X_{\mathcal{L}_0}$ and $X_{\mathcal{L}_1}$, and obtains secret keys $\hat{X}_{\mathcal{L}_0}$ and $\hat{X}_{\mathcal{L}_1}$, respectively.

In Step 6, Alice checks the value of the 1 bit common information $S$ and uses $\hat{X}_{\mathcal{L}_0}$ and $\hat{X}_{\mathcal{L}_1}$ to encrypt $K_S$ and $\bar{K}_S$ and obtain $(\hat{X}_{\mathcal{L}_0} \oplus K_S, \hat{X}_{\mathcal{L}_1} \oplus K_S)$, where $S = 1 - S$. In Step 7, Alice sends $(\hat{X}_{\mathcal{L}_0} \oplus K_S, \hat{X}_{\mathcal{L}_1} \oplus K_S)$ into the public channel. More specifically,

1) If $S = 0$, then send $(\hat{X}_{\mathcal{L}_0} \oplus K_0, \hat{X}_{\mathcal{L}_1} \oplus K_1)$ into the public channel in this order.

2) If $S = 1$, then send $(\hat{X}_{\mathcal{L}_0} \oplus K_1, \hat{X}_{\mathcal{L}_1} \oplus K_0)$ into the public channel in this order.

In Step 8, upon receiving $(\hat{X}_{\mathcal{L}_0} \oplus K_S, \hat{X}_{\mathcal{L}_1} \oplus K_S)$, Bob, with the knowledge of $S, \Theta$, will recover $K_\Theta$ as follows. Let us assume $S = 0$ and $\Theta = 0$. Then Bob can determine that $\mathcal{L}_S \oplus \Theta = \mathcal{L}_0 = G$. Bob thus decodes $K_0$ from $\hat{X}_{\mathcal{L}_0} \oplus K_0$, which is received from the public channel, and $\hat{X}_{\mathcal{L}_1}$, which is calculated according to the secret key generation scheme as in Step 5. For the other values of $S$ and $\Theta$, the decoding procedure at Bob can be derived in a similar manner.

**Performance analysis:** We will show that the above proposed protocol satisfies the correctness, security and privacy constraints in (15)-(18) if the rate does not violate (52)-(56) in Theorem 3. The result is presented in the following lemma.

**Lemma 2:** The above proposed protocol achieves any wiretapped OT rate specified in (52)-(56) with 1-privacy for the broadcast channel of the form (31) where the users are honest-but-curious.

Lemma 2 is proved in Appendix B.

When we specialize the result of Theorem 3 to the BESBC model, we have the following corollary.

**Corollary 1:** For the wiretapped OT problem with BESBC, the following rate is achievable.

$$
\min \left( \epsilon_1, (1 - \epsilon_1) \epsilon_3, \frac{1}{2} [(1 - \epsilon_1) \epsilon_3 + \epsilon_1 \epsilon_2] \right), \quad \text{if } \epsilon_2 \geq \epsilon_3,
$$

$$
\min \left( \epsilon_1, (1 - 2 \epsilon_1) \epsilon_3 + \epsilon_1 \epsilon_2, \frac{1}{2} [(1 - \epsilon_1) \epsilon_3 + \epsilon_1 \epsilon_2] \right), \quad \text{if } \epsilon_2 \leq \epsilon_3, \epsilon_1 \leq \frac{1}{2},
$$

$$
(1 - \epsilon_1) \epsilon_2, \quad \text{if } \epsilon_2 \leq \epsilon_3, \epsilon_1 \geq \frac{1}{2}.
$$

The proof of the corollary can be found in Appendix C.

We note that the achievable rate in the above corollary collapses to the achievable rate in Theorem 2 if we assume $\epsilon_2 \geq \epsilon_3$. On the other hand, if $\epsilon_2 < \epsilon_3$, the achievable rate in Corollary 1 does not meet the upper bound in Theorem 1. Therefore, the wiretapped OT capacity for the BESBC in the case of $\epsilon_2 < \epsilon_3$ is still unknown.

**V. CONCLUSION**

We proposed a protocol that achieves the 1-of-2 string wiretapped OT capacity for the BESBC when $\epsilon_2 \geq \epsilon_3$. Our result is tighter and more general compared with the state-of-the-art result of [18, Theorem 5]. We further propose a new protocol which is applicable to a larger class of broadcast.
channels and obtain a novel lower bound on the wiretapped OT capacity.

**APPENDIX A**

**PROOF OF LEMMA 1**

We first list basic definitions and properties regarding universal hash functions, Rényi entropy and privacy amplification as follows, which can also be found in [18, Appendix A].

**Definition 3:** A class $\mathcal{F}$ of functions mapping $A \to B$ is universal if, for $F \sim \text{Unif}(\mathcal{F})$ and for any $a_0, a_1 \in A$, $a_0 \neq a_1$, we have

$$P[F(a_0) = F(a_1)] \leq \frac{1}{|B|}. \quad (83)$$

The class of all linear maps from $\{0, 1\}^n$ to $\{0, 1\}^r$ is a universal class.

**Definition 4:** Let $A$ be a random variable with alphabet $A$ and distribution $p_A$. The collision probability $P_c(A)$ of $A$ is defined as the probability that $A$ takes the same value twice in two independent experiments. That is,

$$P_c(A) = \sum_{a \in A} p_A^2(a). \quad (84)$$

**Definition 5:** The Rényi entropy of order two of a random variable $A$ is

$$R(A) = \log_2 \left( \frac{1}{P_c(A)} \right). \quad (85)$$

For an event $E$, the conditional distribution $p_{A|E}$ is used to define the conditional collision probability $P_{c}(A|E)$ and the conditional Rényi entropy of order 2, $R(A|E)$.

**Lemma 3 (Corollary 4 of [21]):** Let $P_{AB}$ be an arbitrary probability distribution, with $A \in \mathcal{A}, D \in \mathcal{D}$, and let $d \in D$. Suppose $R(A|D = d) \geq c$. Let $\mathcal{F}$ be a universal class of functions mapping $A \to \{0, 1\}^l$ and $F \sim \text{Unif}(\mathcal{F})$. Then,

$$H(F(A)|F, D = d) \geq l - \log(1 + 2^{l-c}) \geq \frac{l - 2^{l-c}}{\ln 2}. \quad (86)$$

To proof Lemma 1, we follow the similar proof steps as those in [18, lemma 9] and prove that (15)-(18) are satisfied for our protocol.

Suppose that when the length of the erased coordinates received by Bob is less than $n(\epsilon_1 - \delta)$ or the length of the non-erased coordinates is less than $n(1 - \epsilon_1 - \delta)$, the protocol will fail. We use $\#(e(Y^n))$ and $\#(\bar{e}(Y^n))$ to represent the number of erased and non-erased coordinates of $Y^n$, respectively. From [16, Lemma 2.6], we have that the probabilities

$$\Pr[\#(e(Y^n)) \geq n(\epsilon_1 - \delta)] \geq 1 - K(n) \exp(-nD(\epsilon_1 - \delta)|\epsilon_1)), \quad (87)$$

$$\Pr[\#(\bar{e}(Y^n)) \geq n(1 - \epsilon_1 - \delta)] \geq 1 - K(n) \exp(-nD(1 - \epsilon_1 - \delta)|1 - \epsilon_1)), \quad (88)$$

where $K(n)$ is a polynomial of $n$, and for $0 \leq p, q \leq 1$

$$D(p|q) \triangleq p \log \frac{p}{q} + (1 - p) \log \frac{1 - p}{1 - q}. \quad (89)$$

We can see that with sufficiently large $n$, the probabilities in (87) and (88) are arbitrarily close to 1.

**Correctness:** We prove that (15) is satisfied for our protocol. Bob knows the values of $S$, and Bob also knows $X_{\bar{\Theta}} = X_{\bar{\Theta} \oplus s}$ and $F_{\bar{\Theta} \oplus s}$, then Bob can compute the key $\tilde{X}_{\bar{\Theta} \oplus s} = F_{\bar{\Theta} \oplus s}(X_{\bar{\Theta} \oplus s})$. As a result, Bob can learn the value of $K_{\bar{\Theta}}$ from $K_{\bar{\Theta}} \oplus X_{\bar{\Theta} \oplus s}$ sent by Alice and the key $X_{\bar{\Theta} \oplus s}$. The above analysis is based on the assumption that we have enough non-erased symbols in $Y^n$ to form the set $\mathcal{A}_0$ and $\mathcal{G}$ with size $n\alpha$ and $n(\frac{R}{\epsilon_2} - \delta - \alpha)$, respectively. Hence, from (88) we have

$$\Pr[K_{\bar{\Theta}} \neq K_{\bar{\Theta}}] = \Pr[\#(\bar{e}(Y^n)) \leq n(1 - \epsilon_1 - \delta)]$$

$$\leq K(n) \exp(-nD(1 - \epsilon_1 - \delta)|1 - \epsilon_1)). \quad (90)$$

**Security at Bob:** We prove that (17) is satisfied for our protocol.

$$I(K_{\bar{\Theta}}; \overline{V_B}) = I(K_{\bar{\Theta}}; \Theta, Y^n, N, F)$$

$$= I(K_{\bar{\Theta}}; \Theta, Y^n, N, \mathcal{L}_0, \mathcal{L}_1, \mathcal{L}_r, S \oplus K_{\bar{\Theta}}, F_{\bar{\Theta}}, F_0, F_1, K_{\bar{\Theta}} \oplus \tilde{X}_{\bar{\Theta} \oplus s}, K_{\bar{\Theta}} \oplus \tilde{X}_{\bar{\Theta} \oplus s})$$

$$= I(K_{\bar{\Theta}}; \Theta, Y^n, N, \mathcal{L}_0, \mathcal{L}_1, \mathcal{L}_r, S, F_{\bar{\Theta}}, F_0, F_1, K_{\bar{\Theta}} \oplus \tilde{X}_{\bar{\Theta} \oplus s}, K_{\bar{\Theta}} \oplus \tilde{X}_{\bar{\Theta} \oplus s})$$

$$\leq (a) I(K_{\bar{\Theta}}; \Theta, Y^n, N, \mathcal{L}_0, \mathcal{L}_1, \mathcal{L}_r, S, F_{\bar{\Theta}}, F_0, F_1, K_{\bar{\Theta}} \oplus \tilde{X}_{\bar{\Theta} \oplus s}, K_{\bar{\Theta}} \oplus \tilde{X}_{\bar{\Theta} \oplus s})$$

$$\leq (b) I(K_{\bar{\Theta}}; \Theta, Y^n, N, \mathcal{L}_0, \mathcal{L}_1, \mathcal{L}_r, S, F_{\bar{\Theta}}, F_0, F_1, K_{\bar{\Theta}} \oplus \tilde{X}_{\bar{\Theta} \oplus s}, K_{\bar{\Theta}} \oplus \tilde{X}_{\bar{\Theta} \oplus s})$$

$$\leq (c) I(K_{\bar{\Theta}}; \Theta, Y^n, N, \mathcal{L}_0, \mathcal{L}_1, \mathcal{L}_r, S, F_{\bar{\Theta}}, F_0, F_1, K_{\bar{\Theta}} \oplus \tilde{X}_{\bar{\Theta} \oplus s}, K_{\bar{\Theta}} \oplus \tilde{X}_{\bar{\Theta} \oplus s})$$

$$\leq (d) I(K_{\bar{\Theta}}; K_{\bar{\Theta}} \oplus \tilde{X}_{\bar{\Theta} \oplus s}; \Theta, Y^n, N, \mathcal{L}_0, \mathcal{L}_1, \mathcal{L}_r, S, F_{\bar{\Theta}}, F_0, F_1)$$

$$\leq H(\tilde{X}_{\bar{\Theta} \oplus s}|K_{\bar{\Theta}}, \Theta, Y^n, N, \mathcal{L}_0, \mathcal{L}_1, \mathcal{L}_r, S, F_{\bar{\Theta}}, F_0, F_1)$$

$$\leq H(\tilde{X}_{\bar{\Theta} \oplus s}) \leq n(R - \delta)$$

$$= n(R - \delta)$$

$$\leq H(\tilde{X}_{\bar{\Theta} \oplus s}|K_{\bar{\Theta}}, \Theta, Y^n, N, \mathcal{L}_0, \mathcal{L}_1, \mathcal{L}_r, S, F_{\bar{\Theta}}, F_0, F_1)$$

$$\leq n(R - \delta) - H(\tilde{X}_{\bar{\Theta} \oplus s}|Y_{\bar{\Theta} \oplus s}, F_{\bar{\Theta}}) \quad (91)$$

where

(a) holds since $K_{\bar{\Theta}}$ is a function of $(F_{\bar{\Theta}}, Y^n, \mathcal{L}_0)$.

(b) holds since $F_{\bar{\Theta} \oplus s}(X_{\bar{\Theta} \oplus s})$ is a function of $(F_{\bar{\Theta} \oplus s}, Y^n, \mathcal{L}_0 \oplus s)$.

(c) holds since $K_{\bar{\Theta}}$ is independent of all other random variables in the mutual information term, which is because $K_{\bar{\Theta}}$ is not involved in our protocol until Step 6 and thus it is independent of every random variable appearing in the protocol before Step 6.

(d) holds since $K_{\bar{\Theta}}$ is independent of $(\Theta, Y^n, N, \mathcal{L}_0, \mathcal{L}_1, \mathcal{L}_r, S, F_{\bar{\Theta}}, F_0, F_1)$ for the same reason as in step (c).

(e) holds since the length of the sequence $F_{\bar{\Theta}}(X_{\bar{\Theta}})$ is $n(R - \delta)$. 

Authorized licensed use limited to the terms of the applicable license agreement with IEEE. Restrictions apply.
(f) holds because of the following Markov chain
\[
X_{\Theta: S} \rightarrow (Y_{\Theta: S}, F_{\Theta: S}) \\
\rightarrow (K_{\Theta}, \Theta, Y^n, N, L_{\Theta}, L_{\Theta}, \alpha, S, F_\alpha, F_\Theta, F_\Theta).
\]
which is valid because $X_{\Theta: S}$ is a function of $(X_{\Theta: S}, F_{\Theta: S})$ and
\[
\Pr(X_{\Theta: S} | Y_{\Theta: S}, F_{\Theta: S}, K_{\Theta}, \Theta, Y^n, N, L_{\Theta}, L_{\Theta}, \alpha, S, F_\alpha, F_\Theta, F_\Theta) = \Pr(X_{\Theta: S} | Y_{\Theta: S}),
\]
due to the memoryless channel.

We note that $\bar{L}_{\Theta: S} = \mathcal{B}$ from (40) in Step 4 of our protocol, which represents the operation of assigning $\mathcal{B}$ to $L_1$ or $L_2$ according to the value of $\Theta$ and $S$. Then we have
\[
R(X_{\mathcal{B}} | Y_{\mathcal{B}} = y_{\mathcal{B}}) = \#(e(y_{\mathcal{B}})),
\]
where $\#(e(y_{\mathcal{B}}))$ represents the number of coordinates, at which $y_{\mathcal{B}}$ are erased. We note that
\[
\Pr[\#(e(Y_{\mathcal{B}})) \geq n(\beta \epsilon_3 - \delta)] \\
\geq \Pr[\#(e(Y^n)) \geq n(\epsilon_1 - \delta)] \\
\geq 1 - K(n) \exp(-nD(\epsilon_1 - \delta | \epsilon_1)).
\]
By defining $\xi_1 = K(n) \exp(-nD(\epsilon_1 - \delta | \epsilon_1))$, we have
\[
H(\bar{X}_{\mathcal{B}} | Y_{\mathcal{B}}, F_{\Theta: S}) \\
\geq H(\bar{X}_{\mathcal{B}} | Y_{\mathcal{B}}, F_{\Theta: S}, \#(e(Y_{\mathcal{B}})) \geq n(\beta \epsilon_3 - \delta)) \\
= \Pr[\#(e(Y_{\mathcal{B}})) \geq n(\beta \epsilon_3 - \delta)] \\
H(\bar{X}_{\mathcal{B}} | Y_{\mathcal{B}}, F_{\Theta: S}, \#(e(Y_{\mathcal{B}})) \geq n(\beta \epsilon_3 - \delta)) \\
\geq 1 - \xi_1 \left( \frac{n(R - \delta)}{\ln 2} \right)
\]
where the third inequality is because of (95) and Lemma 3. Thus, we have
\[
I(K_{\Theta}; V_{\mathcal{B}}) \leq n(R - \delta) - H(\bar{X}_{\mathcal{B}} | Y_{\mathcal{B}}, F_{\Theta: S}) \\
\leq n(R - \delta) - (1 - \xi_1) \left( \frac{n(R - \delta)}{\ln 2} \right)
\]
Therefore, $I(K_{\Theta}; V_{B})$ converges to zero exponentially as $n \rightarrow \infty$ if we assume $\delta - \epsilon_3 \delta - \epsilon_3 \alpha - \delta > 0$.

Privacy at Alice: We prove that (16) is satisfied for our protocol.
\[
I(\Theta; V_A) = I(\Theta; K_0, K_1, X^n, M, F) \\
\leq I(\Theta; K_0, K_1, X^n, M, S, F)
\]
where (a) follows because of the following Markov chain
\[
\Theta \rightarrow (S, L_0, L_1) \\
\rightarrow (K_0, K_1, X^n, M, L_0, L_0, \alpha, F_0, F_1, K_\Theta, X_{\Theta: S}, K_\Theta, \bar{X}_{\Theta: S})
\]
which is valid because from our protocol, we can see that $\Theta$ is only related to other random variables in Step 4 where $L_{\Theta: S} = \mathcal{G}$ and $L_{\Theta: S} = \mathcal{B}$.

(c) follows since given $S, \Theta$, the distribution of $(L_0, L_1)$ is uniform in $\{1, 2, \ldots, n\}$, which is same as the distribution of $(L_0, L_1)$ given $S$.

Security and Privacy at Eve: We prove that (18) is satisfied for our protocol.
\[
I(K_0, K_1; \Theta; V_E) = I(K_\Theta, K_\Theta, \Theta; V_E) \\
= I(\Theta; V_E) + I(K_\Theta; V_E | \Theta) + I(K_\Theta; V_E | \Theta, K_\Theta)
\]
(100)
For the first term, we have
\[
I(\Theta; V_E) = I(\Theta; Z^n, F) \\
= I(\Theta; Z^n, L_0, S \oplus K_0, F_0, L_0, L_1, F_0, F_1, K_\Theta \oplus \bar{X}_{\Theta: S}, K_\Theta \oplus \bar{X}_{\Theta: S}) \\
\leq I(\Theta; Z^n, L_0, S \oplus K_0, F_0, L_0, L_1, F_0, F_1, K_\Theta, K_\Theta \oplus \bar{X}_{\Theta: S}, K_\Theta, K_\Theta \oplus \bar{X}_{\Theta: S}) \\
= I(\Theta; Z^n, L_0, S \oplus K_0, F_0, L_0, L_1, F_0, F_1, K_\Theta, K_\Theta \oplus \bar{X}_{\Theta: S}, K_\Theta \oplus \bar{X}_{\Theta: S})
\]
(100)
\begin{align}
F_0, F_1, \bar{X}_{\Theta \oplus S}, \bar{X}_{\Theta \oplus S}, (\Theta \oplus S) &\rightarrow H(S \oplus K_\alpha | S, Z^n, \bar{L}_\alpha, F_0, \bar{L}_0, L_1, \\
F_0, F_1, \bar{X}_{\Theta \oplus S}, \bar{X}_{\Theta \oplus S}, (\Theta \oplus S) &\leq |S \oplus K_\alpha| - H(K_\alpha | S, Z^n, \bar{L}_\alpha, F_0, \bar{L}_0, L_1, \\
F_0, F_1, \bar{X}_{\Theta \oplus S}, \bar{X}_{\Theta \oplus S}, (\Theta \oplus S) &\leq |S \oplus K_\alpha| - H(K_\alpha | S, Z^n, \bar{L}_\alpha, F_0, \bar{L}_0, L_1, \\
F_0, F_1, \bar{X}_{\Theta \oplus S}, \bar{X}_{\Theta \oplus S}, (\Theta \oplus S) &\leq |F_0(X_{\bar{L}_\alpha}) - H(F_0(X_{\bar{L}_\alpha}), K_\alpha | S, Z^n, \bar{L}_\alpha, F_0, \bar{L}_0, L_1, \\
F_0, F_1, \bar{X}_{\Theta \oplus S}, \bar{X}_{\Theta \oplus S}, (\Theta \oplus S) &\leq |F_0(X_{\bar{L}_\alpha}) - H(F_0(X_{\bar{L}_\alpha}), K_\alpha | S, Z^n, \bar{L}_\alpha, F_0, \bar{L}_0, L_1, \\
F_0, F_1, \bar{X}_{\Theta \oplus S}, \bar{X}_{\Theta \oplus S}, (\Theta \oplus S) &\leq |F_0(X_{\bar{L}_\alpha}) - H(F_0(X_{\bar{L}_\alpha}), K_\alpha | S, Z^n, \bar{L}_\alpha, F_0, \bar{L}_0, L_1, \\
F_0, F_1, \bar{X}_{\Theta \oplus S}, \bar{X}_{\Theta \oplus S}, (\Theta \oplus S) &\leq (n(\alpha(\epsilon_3 - \delta)) - (1 - \xi_3) \left(n(\alpha(\epsilon_3 - \delta)) - \frac{2^{-n(\delta - \delta)}}{\ln 2}\right),
\end{align}

where

(a) \((K_{\Theta}, K_{\Theta})\) is independent of all the other random variables in the mutual information term, because \((K_{\Theta}, K_{\Theta})\) are not involved in our protocol until Step 6 and thus they are independent of every random variable appearing in the protocol before Step 6.
(b) follows since \(\Theta\) is independent of \(\Theta \oplus S\).
(c) follows due to the Markov chain
\begin{align}
S &\rightarrow \Theta \oplus S \\
&\rightarrow (Z^n, \bar{L}_\alpha, F_0, \bar{L}_0, L_1, F_0, F_1, \bar{X}_{\Theta \oplus S}, \bar{X}_{\Theta \oplus S}),
\end{align}

which is valid because from our protocol, we can see that \(S\) is only related to other random variables in the above Markov chain in Step 4 where \(S\) is used to encrypt \(\Theta\) to obtain \(\Theta \oplus S\).
(d) follows because
\begin{align}
H(F_0(X_{\bar{L}_\alpha}) | K_\alpha, S, Z^n, \bar{L}_\alpha, F_0, \bar{L}_0, L_1, \\
F_0, F_1, \bar{X}_{\Theta \oplus S}, \bar{X}_{\Theta \oplus S}, (\Theta \oplus S) &\leq H(F_0(X_{\bar{L}_\alpha}) | K_\alpha) - 1,
\end{align}

where the last inequality because \(K_\alpha\) is the first bit of \(F_0(X_{\bar{L}_\alpha})\).
(e) follows since \(K_\alpha\) is a function of \(F_0(X_{\bar{L}_\alpha})\).
(f) follows because of the Markov chain
\begin{align}
F_0(X_{\bar{L}_\alpha}) &\rightarrow (Z_{\bar{L}_\alpha}, F_0) \\
&\rightarrow (S, Z^n, \bar{L}_\alpha, L_0, L_1, F_0, F_1, \bar{X}_{\Theta \oplus S}, \bar{X}_{\Theta \oplus S}, (\Theta \oplus S),
\end{align}

which is valid because \(F_0(X_{\bar{L}_\alpha})\) is a function of \((X_{\bar{L}_\alpha}, F_0)\) and
\begin{align}
\Pr[X_{\bar{L}_\alpha} | Z_{\bar{L}_\alpha}, F_0, S, Z^n, \bar{L}_\alpha, L_0, L_1, \\
F_0, F_1, \bar{X}_{\Theta \oplus S}, \bar{X}_{\Theta \oplus S}, (\Theta \oplus S) &\rightarrow \Pr(X_{\bar{L}_\alpha} | Z_{\bar{L}_\alpha}),
\end{align}

\(\text{due to the memoryless channel.}\)

(g) follows because \(R(X_{\bar{L}_\alpha} | Z_{\bar{L}_\alpha} = \#(e(Z_{\bar{L}_\alpha}))\)
\begin{align}
H(F_0(X_{\bar{L}_\alpha}) | Z_{\bar{L}_\alpha}, F_0) &\geq H(F_0(X_{\bar{L}_\alpha}) | Z_{\bar{L}_\alpha}, F_0, \#(e(Z_{\bar{L}_\alpha}))) \\
&= \Pr[\#(e(Z_{\bar{L}_\alpha})) \geq (\epsilon_3 - \delta)|L_\alpha] \\
&+ \Pr[\#(e(Z_{\bar{L}_\alpha})) < (\epsilon_3 - \delta)|L_\alpha] \\
&\geq \Pr[\#(e(Z_{\bar{L}_\alpha})) \geq (\epsilon_3 - \delta)|L_\alpha].
\end{align}

We note that
\begin{align}
\Pr[\#(e(Z_{\bar{L}_\alpha})) &\geq (\epsilon_3 - \delta)|L_\alpha] \geq 1 - \xi_3, \\
\xi_3 &\triangleq K(n \exp (-nD(\epsilon_3) | \epsilon_3 - \delta)).
\end{align}

We note that if \(R(X_{\bar{L}_\alpha} | Z_{\bar{L}_\alpha}) = \#(e(Z_{\bar{L}_\alpha})) \geq n(\alpha(\epsilon_3 - \delta))\), we have
\begin{align}
H(F_0(X_{\bar{L}_\alpha}) | Z_{\bar{L}_\alpha}, F_0, \#(e(Z_{\bar{L}_\alpha}))) &\geq (\epsilon_3 - \delta)|L_\alpha| \\
&\geq n(\alpha(\epsilon_3 - \delta)) - \frac{2^{-n(\delta - \delta)}}{\ln 2}.
\end{align}

Then,
\begin{align}
H(F_0(X_{\bar{L}_\alpha}) | Z_{\bar{L}_\alpha}, F_0) &\geq (1 - \xi_3) \left(n(\alpha(\epsilon_3 - \delta)) - \frac{2^{-n(\delta - \delta)}}{\ln 2}\right).
\end{align}

From above derivation, we have
\begin{align}
I(\Theta; V_F) &\leq \xi_3 n(\alpha(\epsilon_3 - \delta)) + (1 - \xi_3) \frac{2^{-n(\delta - \delta)}}{\ln 2},
\end{align}

which converges to zero exponentially with \(n \to \infty\) for any finite positive \(\alpha, \delta\) and \(\delta\) with \(\epsilon_3 > \delta > \delta\).

For the second term, we have
\begin{align}
I(K_{\Theta}; \Theta, V_F) &\leq I(K_{\Theta}; \Theta, Z^n, F) \\
&= I(K_{\Theta}; \Theta, Z^n, L_0, L_1, L_\alpha, S \oplus K_\alpha, \\
&\quad F_0, F_1, K_\Theta \oplus \bar{X}_{\Theta \oplus S}, \bar{X}_{\Theta \oplus S}, (\Theta \oplus S)) \\
&\leq I(K_{\Theta}; \Theta, Z^n, S, L_\Theta \oplus S, L_\Theta, L_\Theta, L_\Theta, S \oplus K_\alpha, \\
&\quad F_0, F_0, F_1, K_\Theta \oplus \bar{X}_{\Theta \oplus S}, \bar{X}_{\Theta \oplus S}, (\Theta \oplus S)) \\
&\leq I(K_{\Theta}; \Theta, Z^n, S, L_\Theta \oplus S, L_\Theta, L_\Theta, L_\Theta, K_\Theta, \\
&\quad F_0, F_0, F_1, K_\Theta \oplus \bar{X}_{\Theta \oplus S}, \bar{X}_{\Theta \oplus S}, (\Theta \oplus S)) \\
&= I(K_{\Theta}; \Theta, Z^n, S, L_\Theta \oplus S, L_\Theta, L_\Theta, L_\Theta, K_\Theta, \\
&\quad F_0, F_0, F_1, K_\Theta \oplus \bar{X}_{\Theta \oplus S}, \bar{X}_{\Theta \oplus S}, (\Theta \oplus S)) \\
&\leq I(K_{\Theta}; \Theta, Z^n, S, L_\Theta \oplus S, L_\Theta, L_\Theta, L_\Theta, L_\Theta, K_\Theta, \\
&\quad F_0, F_0, F_1, K_\Theta \oplus \bar{X}_{\Theta \oplus S}, \bar{X}_{\Theta \oplus S}, (\Theta \oplus S)) \\
&\leq 0.
\end{align}
where $K \beta < \epsilon$

due to the memoryless channel.

(b) holds because of the Markov chain

$$X_{\Theta, S} \rightarrow (Z_{\Theta, S}, F_{\Theta, S}, X_{\Theta}, L_{\Theta, S}, L_{\Theta}, K_{\Theta}, F_{\Theta, S}, F_{\Theta, S}, X_{\Theta, S})$$

where $L_{\Theta} = L_{\Theta, S} \cap L_{\Theta, S}$ is the overlapping part between $L_{\Theta}$ and $L_{\Theta}$. The above Markov chain is valid because $X_{\Theta, S}$ is a function of $(X_{\Theta, S}, F_{\Theta, S})$ and

$$\Pr(X_{\Theta, S} | K_{\Theta}, \Theta, Z_{\Theta, S}, L_{\Theta, S}, L_{\Theta}, K_{\Theta}, F_{\Theta, S}, F_{\Theta, S}, X_{\Theta, S}) = \Pr(X_{\Theta, S} | Z_{\Theta, S}, X_{\Theta})$$

due to the memoryless channel.

(c) holds because

$$R(X_{\Theta, S}, X_{\Theta, S}, Z_{\Theta, S})$$

$$= z_{\Theta, S}$$

$$= \#(e(z_{\Theta, S} \setminus \mathcal{L}_{\Theta}))$$

$$= \#(e(y_{\Theta, S} \setminus \mathcal{L}_{\Theta}) \cap e(z_{\Theta, S} \setminus \mathcal{L}_{\Theta})) +$$

$$\#(e(y_{\Theta, S} \setminus \mathcal{L}_{\Theta}) \cap e(z_{\Theta, S} \setminus \mathcal{L}_{\Theta}))$$

where $\cap$ represents the “and” operation.

We consider the following three cases:

(i) If $\beta < \epsilon_1$ and $\beta \leq \frac{1}{2}$, Bob uniformly selects $n\beta$ coordinates from the erased coordinates and name the set of corresponding locations as $B$. In this case

$$Y_{\Theta, S} \setminus L_{\Theta, S} = Y_B$$

$$\Pr(\#(e(Z_{\Theta, S} \setminus \mathcal{L}_{\Theta})) \geq n(\beta e_2 - \delta))$$

$$\geq \Pr\left[ \#(e(Z_{\Theta, S} \setminus \mathcal{L}_{\Theta})) \geq n(\beta e_2 - \delta) \right]$$

$$\geq \Pr\left[ \#(e(Y_{\Theta, S} \setminus \mathcal{L}_{\Theta})) = n \beta \right]$$

$$\geq \Pr\left[ \#(e(Z_{\Theta, S} \setminus \mathcal{L}_{\Theta})) \geq n(\beta e_2 - \delta) \right]$$

$$\geq (1 - K(n) \exp(-nD(\beta | e_1)))$$

$$\geq (1 - K(n) \exp(-n\beta D(e_2 - \frac{\delta}{\beta} | e_2)))$$

$$\geq 1 - \xi_2$$

(ii) If $\epsilon_1 < \beta < \frac{1}{2}$, Bob collects all erased coordinates and uniformly selects $n\beta - n\epsilon_2$ coordinates from the non-erased coordinates, but not in $G$ or $L_{\Theta}$. Bob names the set of corresponding locations as $B$. In this case $L_{\Theta, S} \setminus L_b = L_B \triangleq L_{B_1} \cup L_{B_2}$ where $L_{B_1}$ represents the coordinates in $L_B$, which are erased at Bob with $|L_{B_1}| = n\epsilon_2$ and similarly, $L_{B_2}$ represents the coordinates in $L_B$, which are non-erased at Bob

$$\Pr(\#(e(Z_{\Theta, S} \setminus \mathcal{L}_{\Theta})) \geq n(\beta e_3 - \delta))$$

$$\geq \Pr(\#(e(Z_{\Theta, S} \setminus \mathcal{L}_{\Theta})) \geq n(\epsilon_1, \epsilon_2))$$

$$\geq (1 - K(n) \exp(-n \min(D(\beta | e_1),\beta D(e_2 - \frac{\delta}{\beta} | e_2))))$$

(iii) If $\beta > \frac{1}{2}$, Bob collects all the coordinates not in $G$ or $L_{\Theta}$ and uniformly selects $n(2\beta - 1)$ coordinates from $G$. Bob names the set of corresponding locations as $B$. In this case

$$L_{\Theta, S} \setminus L_b = L_B \triangleq L_{B_1} \cup L_{B_2}$$

$$\Pr(\#(e(Z_{\Theta, S} \setminus \mathcal{L}_{\Theta})) \geq n(\beta e_3 - \delta))$$

$$\geq \Pr(\#(e(Z_{\Theta, S} \setminus \mathcal{L}_{\Theta})) \geq n(\epsilon_1, \epsilon_2) + (1 - \epsilon_1 - \beta - \epsilon_3) - 2\epsilon_3 \delta - 2\epsilon_3 \alpha - \delta)$$

$$\geq (1 - K(n) \exp(-n \min(D(\epsilon_1 - \delta | e_1), (\epsilon_1 - \beta - \epsilon_3)(\epsilon_2 - \delta | e_2), (\beta - 1 - \delta | e_3 - \delta | e_3)))$$
\[ x \left( 1 - K(n) \right) \exp(-n(\epsilon_1 - \delta')) D(\epsilon_2 - \delta' || \epsilon_2) \times \left( 1 - K(n) \right) \exp(-n(1 - \epsilon_1 - \beta - \delta')) D(\epsilon_3 - \delta' || \epsilon_3) \geq 1 - \xi_4, \]
\[ \xi_4 \triangleq \frac{2 \epsilon_3 \delta + 2 \epsilon_3 \alpha + \delta}{4 \max(\epsilon_1, \epsilon_2, \epsilon_3, 1 - \epsilon_1 - \beta)}, \]
\[ \Delta_2 \triangleq 3 K(n) \exp(-n \Delta_2), \]
\[ \Delta_2 \triangleq \min(D(\epsilon_1 - \delta' || \epsilon_1), D(\epsilon_1 + \delta' || \epsilon_1), (\epsilon_1 - \delta') D(\epsilon_2 - \delta' || \epsilon_2), (1 - \epsilon_1 - \beta - \delta') D(\epsilon_3 - \delta' || \epsilon_3)), \]

where \((a)\) is because of
\[ (\beta + \alpha + \delta) \epsilon_3 = R \leq \frac{1}{2} (\epsilon_1 \epsilon_2 + \epsilon_3 (1 - \epsilon_1)). \]

By defining \(\xi_5 = \max(\xi_2, \xi_3, \xi_4)\), we have
\[ \Pr[\#(e(Z_{\Theta,\Theta} \setminus \mathcal{L}_0)) \geq n(\beta \epsilon_3 - \delta)] \geq 1 - \xi_5. \]

Therefore, we have
\[ H(X_{\Theta,\Theta} | X_{\Theta}, \mathcal{L}_{\Theta,\Theta}, Z_{\Theta,\Theta}, F_{\Theta,\Theta}) \geq \Pr[\#(e(Z_{\Theta,\Theta} \setminus \mathcal{L}_0)) \geq n(\beta \epsilon_3 - \delta)] \]
\[ = (1 - \xi_5) \left( n(R - \delta) - \frac{2^{n(R - \delta) - n(\beta \epsilon_3 - \delta)}}{\ln 2} \right), \]
\[ = (1 - \xi_5) \left( n(R - \delta) - \frac{2^{-n(\delta - \epsilon_3 \delta - \epsilon_3 \alpha - \delta)}}{\ln 2} \right). \]

From above derivation, we have
\[ I(K_{\Theta}; \Theta, V_E) \leq \xi_5 \left( n(R - \delta) + (1 - \xi_5) \frac{2^{-n(\delta - \epsilon_3 \delta - \epsilon_3 \alpha - \delta)}}{\ln 2} \right), \]

which converges to zero exponentially with \(n \to \infty\) for any finite positive \(\alpha, \delta\) and \(\delta\) with \(\delta - \epsilon_3 \delta - \epsilon_3 \alpha - \delta > 0\).

For the third term, we have
\[ I(K_{\Theta}; \Theta, K_{\Theta}, V_E) \]
\[ = I(K_{\Theta}; \Theta, K_{\Theta}, Z^n, F) \]
\[ = I(K_{\Theta}; \Theta, K_{\Theta}, Z^n, \mathcal{L}_0, L_1, L_\alpha, S \oplus K_\alpha, F_\alpha, F_0, F_1, K_{\Theta} \oplus X_{\Theta,\Theta,\Theta}, K_{\Theta} \oplus X_{\Theta,\Theta,\Theta}) \]
\[ \leq I(K_{\Theta}; \Theta, K_{\Theta}, Z^n, S, \mathcal{L}_0, L_1, L_\alpha, S \oplus K_\alpha, F_\alpha, F_0, F_1, K_{\Theta} \oplus X_{\Theta,\Theta,\Theta,\Theta}, K_{\Theta} \oplus X_{\Theta,\Theta,\Theta,\Theta}) \]
\[ = I(K_{\Theta}; \Theta, K_{\Theta}, Z^n, S, \mathcal{L}_{\Theta,\Theta}, \mathcal{L}_{\Theta,\Theta}, \mathcal{L}_\alpha, \mathcal{L}_\alpha, \alpha, F_\alpha, F_0, F_1, K_{\Theta} \oplus X_{\Theta,\Theta,\Theta,\Theta}, K_{\Theta} \oplus X_{\Theta,\Theta,\Theta,\Theta}) \]
\[ = I(K_{\Theta}; \Theta, K_{\Theta}, Z^n, S, \mathcal{L}_{\Theta,\Theta}, \mathcal{L}_{\Theta,\Theta}, \mathcal{L}_\alpha, \mathcal{L}_\alpha, K_{\Theta}, F_\alpha, F_0, F_1, X_{\Theta,\Theta,\Theta,\Theta}, X_{\Theta,\Theta,\Theta,\Theta}) \]
\[ \leq I(K_{\Theta}; \Theta, K_{\Theta}, Z^n, S, \mathcal{L}_{\Theta,\Theta}, \mathcal{L}_{\Theta,\Theta}, \mathcal{L}_\alpha, \mathcal{L}_\alpha, K_{\Theta}, F_\alpha, F_0, F_1, X_{\Theta,\Theta,\Theta,\Theta}, X_{\Theta,\Theta,\Theta,\Theta}) \]
\[ = I(K_{\Theta}; \Theta, K_{\Theta}, Z^n, S, \mathcal{L}_{\Theta,\Theta}, \mathcal{L}_{\Theta,\Theta}, \mathcal{L}_\alpha, \mathcal{L}_\alpha, K_{\Theta}, F_\alpha, F_0, F_1, X_{\Theta,\Theta,\Theta,\Theta}, X_{\Theta,\Theta,\Theta,\Theta}) \]
\[ = I(K_{\Theta}; \Theta, Z^n, S, \mathcal{L}_{\Theta,\Theta}, \mathcal{L}_{\Theta,\Theta}, \mathcal{L}_\alpha, \mathcal{L}_\alpha, K_{\Theta}, F_\alpha, F_0, F_1, X_{\Theta,\Theta,\Theta,\Theta}, X_{\Theta,\Theta,\Theta,\Theta}) \]
\[ = I(K_{\Theta}; \Theta, Z^n, S, \mathcal{L}_{\Theta,\Theta}, \mathcal{L}_{\Theta,\Theta}, \mathcal{L}_\alpha, \mathcal{L}_\alpha, K_{\Theta}, F_\alpha, F_0, F_1, X_{\Theta,\Theta,\Theta,\Theta}, X_{\Theta,\Theta,\Theta,\Theta}) \]

where \((a)\) holds since \(K_{\Theta}\) is independent of all other random variables in the mutual information term, due to the fact that \(K_{\Theta}\) is not involved in our protocol until Step 6 and thus it is independent of every random variable appearing in the protocol before Step 6.

(b) holds because of the following Markov chain
\[ X_{\Theta,\Theta,\Theta,\Theta} \rightarrow (Z_{\Theta,\Theta,\Theta,\Theta}, \mathcal{L}_{\Theta,\Theta,\Theta,\Theta}, \mathcal{L}_{\Theta,\Theta,\Theta,\Theta}, F_{\Theta,\Theta,\Theta,\Theta}) \rightarrow (K_{\Theta}, \Theta, Z^n, S, \mathcal{L}_\alpha, F_\alpha(X_{\Theta,\Theta,\Theta,\Theta}), F_\alpha). \]
(c) holds because of the following Markov chain
\[
\tilde{X}_{\Theta \oplus S} \rightarrow (Z_{\Theta \oplus S}, F_{\Theta \oplus S}, L_{\Theta \oplus S})
\rightarrow (Z_{\Theta \oplus S}, L_{\Theta \oplus S}, F_{\Theta \oplus S}, X_{\Theta \oplus S}),
\]
which follows the same logic as in step (b).
(d) holds because of the following Markov chain
\[
\tilde{X}_{\Theta \oplus S} \rightarrow (X_{\Theta}, Z_{\Theta \oplus S}, L_{\Theta \oplus S}, F_{\Theta \oplus S})
\rightarrow (Z_{\Theta \oplus S}, L_{\Theta \oplus S}, F_{\Theta \oplus S}, X_{\Theta \oplus S}),
\]
which follows the same logic as in step (b).
(e) is due to the following derivation. We note that \(L_{\Theta \oplus S} = \mathcal{G}\)
\[
R(X_{\Theta} | Z_{\mathcal{G}} = z_{\mathcal{G}}) = \#(e(z_{\mathcal{G}})),
\]
where \(\#(e(z_{\mathcal{G}}))\) represents the number of coordinates, at which \(z_{\mathcal{G}}\) are erased. We note that
\[
\Pr[\#(e(Z_{\mathcal{G}})) \geq n(\beta \epsilon_3 - \delta)]
\geq \Pr[|\mathcal{G}| = n \beta \wedge \#(e(Z_{\mathcal{G}})) \geq n(\beta \epsilon_3 - \delta)]
\geq (1 - K(n) \exp(-nD(\beta + \alpha||(1 - \epsilon_1))))
\geq (1 - K(n) \exp(-n\beta D(\epsilon_3 - \delta / \beta||\epsilon_3))
\geq 1 - \xi_0,
\]
\[
\xi_0 \triangleq 2K(n) \exp(-n \min(D(\beta + \alpha||(1 - \epsilon_1)),
\beta D(\epsilon_3 - \delta / \beta||\epsilon_3))).
\]
By using Lemma 3, we have
\[
H(X_{\Theta \oplus S} | Z_{\Theta \oplus S}, F_{\Theta \oplus S})
\geq \Pr[\#(e(Z_{\mathcal{G}})) \geq n(\beta \epsilon_3 - \delta)]H(X_{\Theta \oplus S})
\geq (1 - \xi_0) \left( n(R - \tilde{\delta}) - \frac{2n(1 - \tilde{\delta})-n(\beta \epsilon_3 - \delta)}{\ln 2} \right)
\geq (1 - \xi_0) \left( n(R - \tilde{\delta}) - \frac{2n(1 - \epsilon_3 \delta - \epsilon_3 \alpha - \delta)}{\ln 2} \right).
\]
From (128), we have
\[
H(X_{\Theta \oplus S} | X_{\Theta}, L_{\Theta \oplus S}, Z_{\Theta \oplus S}, F_{\Theta \oplus S})
\geq (1 - \xi_0) \left( n(R - \tilde{\delta}) - \frac{2n(1 - \epsilon_3 \delta - \epsilon_3 \alpha - \delta)}{\ln 2} \right).
\]
From above derivation, we have
\[
I(K_{\Theta}; \Theta, K_{\Theta}, V_E)
\leq (\xi_0 + \xi_6) \left( n(R - \tilde{\delta}) + (2 - \xi_5 - \xi_6) \frac{2n(1 - \epsilon_3 \delta - \epsilon_3 \alpha - \delta)}{\ln 2} \right),
\]
which converges to zero exponentially with \(n \rightarrow \infty\) for any finite positive \(\alpha, \delta\) and \(\tilde{\delta}\) with \(\tilde{\delta} - \epsilon_3 \delta - \epsilon_3 \alpha - \delta > 0\).

**APPENDIX B**

**PROOF OF Lemma 2**

**Definition 6 ([16, Section 17.1]):** We define security index of \(K\) against \(Z\) as
\[
S(K | Z) \triangleq \log |K| - H(K) + I(K; Z).
\]
We can see that \(S(K | Z)\) going to zero means that \(K\) is almost uniformly distributed and \(K\) and \(Z\) are almost independent. For two random variables \(K_1\) and \(K_2\), we have
\[
S(K_1, K_2 | Z)
\geq \log |K_1| + \log |K_2| - H(K_1, K_2) + I(K_1, K_2; Z)
\geq \log |K_1| + \log |K_2| - H(K_1) - H(K_2 | K_1) +
\geq S(K_1 | Z) + S(K_2 | Z, K_1).
\]

**Lemma 4 (Secrecy Lemma for i.i.d Sources [16, Corollary 17.5]):** For i.i.d. sources \((X^n, Y^n)\),
1) to any \(\delta > 0\), there exists \(\xi > 0\) such that for any \(k \leq \exp(nH(X | Y - \delta))\), a randomly selected mapping \(\kappa: \mathcal{X}^n \mapsto \{1, 2, \ldots, k\}\) satisfies
\[
S(\kappa(X^n) | Y^n) < \exp(-n\xi),
\]
double exponentially surely (meaning that the probability of not satisfying the above property is not larger than \(\exp(-\exp(nc))\) if \(n > n_0\), for some \(c > 0\) and \(n_0 > 0\).
2) Let \(U\) be any random variable with at most \(\exp(nr)\) possible values, with \(r < H(X | Y)\). Then if \(k \leq \exp(nH(X | Y - r - \delta))\), a randomly selected mapping \(\kappa: \mathcal{X}^n \mapsto \{1, 2, \ldots, k\}\) satisfies
\[
S(\kappa(X^n) | Y^n, U) < \exp(-n\xi),
\]
double exponentially surely.

For secret key generation scheme, we use the technique of double random binning as follows. Assume a pair of i.i.d. sources \(X^n \in \mathcal{X}^n\) and \(Y^n \in \mathcal{Y}^n\) satisfying joint distribution \(P(x, y)\). We define a randomly selected mapping \(\varphi\) as
\[
\varphi: \mathcal{X}^n \mapsto \{1, 2, \ldots, M_1\} \times \{1, 2, \ldots, M_2\},
\]
We can obtain the following two functions from \(\varphi\), which can also be viewed as randomly selected mappings,
\[
\kappa: \mathcal{X}^n \mapsto \{1, 2, \ldots, M_1\},
\]
\[
\phi: \mathcal{X}^n \mapsto \{1, 2, \ldots, M_2\},
\]
such that
\[
\varphi(x^n) = (\kappa(x^n), \phi(x^n)).
\]
From the result of Slepian-Wolf [16, Lemma 13.13] [19, Theorem 10.3], we can see that if \(M_1 \geq \exp(nH(X | Y) + \delta)\), then \(X^n\) can be recovered from \(Y^n\) and \(\kappa(X^n)\) with probability of error less than \(\epsilon\). Assume a wiretapper obtains an i.i.d. observation \(Z^n\), which is correlated with \(X^n\) with joint distribution \(P(x, z)\). Apply the second part of the above secrecy lemma by letting \(k = M_2\) and \(U = \kappa(X^n)\), we have that if \(M_2 \leq \exp(nH(X | Z - \frac{1}{n} \log M_1 - \delta))\), then
\[
S(\phi(X^n) | Z^n, \kappa(X^n)) < \exp(-n\xi),
\]
doubly exponentially surely, which leads to the existence of a deterministic mapping with parameters \((M_1, M_2)\) satisfying security index requirement (149).

In our proposed protocol, we use the above secret key generation scheme in two different steps.

In step 2, Bob applies a secret key generation scheme on \(Y_{\mathcal{L}_\alpha}\) to obtain one bit of shared information \(K_\alpha = \phi_\alpha(Y_{\mathcal{L}_\alpha})\). In this case, we set \(M_1 \geq \exp(n\alpha(H(Y|X) + \delta))\) and \(M_2 = 2\), then Alice can recover \(Y_{\mathcal{L}_\alpha}\) and consequently \(K_\alpha\) with probability of error less than \(\epsilon\) and

\[
S(K_\alpha|Z_{\mathcal{L}_\alpha}, \kappa_\alpha(Y_{\mathcal{L}_\alpha})) < \exp(-n\alpha x),
\]

which will leads to the privacy at Eve.

In step 5, Alice applies secret key generation schemes on \(X_{\mathcal{L}_\alpha}\) and \(X_{\mathcal{L}_\beta}\), or equivalently \(X_B\) and \(X_B\), respectively. We assume that the secret key generation scheme on \(X_\beta\) is a randomly selected mapping \(\varphi_\beta = (\kappa_\beta, \phi_\beta)\) with size of alphabets \((M_1, M_2)\). Similarly, the secret key generation scheme on \(X_B\) is a randomly selected mapping \(\varphi_B = (\kappa_B, \phi_B)\) with size of alphabets \((M_1, M_2)\). We define the set of coordinates

\[
\mathcal{O} \triangleq \mathcal{G} \cap \mathcal{B}.
\]

The assumption that Alice could not distinguish between the sets \(\mathcal{G}\) and \(\mathcal{B}\) implies that Bob should be able to recover \(X_B\) from the secret key generation scheme if \(X_B\) goes through the same channel as \(X_B\) to reach Bob. We define the corresponding channel output as \(\bar{Y}_B\). For the coordinates \(i\) such that \(i \in \mathcal{O}\), we assume that \(Y_i = \bar{Y}_i\).

For the convenience of the presentation, we define the following random variables

\[
X_G = X_i, \text{ with probability } \frac{1}{|\mathcal{G}|}, \text{ for } i \in \mathcal{G},
\]

\[
Y_G = Y_i, \text{ with probability } \frac{1}{|\mathcal{G}|}, \text{ for } i \in \mathcal{G},
\]

\[
Z_G = Z_i, \text{ with probability } \frac{1}{|\mathcal{B}|}, \text{ for } i \in \mathcal{B},
\]

\[
X_B = X_i, \text{ with probability } \frac{1}{|\mathcal{B}|}, \text{ for } i \in \mathcal{B},
\]

\[
Y_B = Y_i, \text{ with probability } \frac{1}{|\mathcal{B}|}, \text{ for } i \in \mathcal{B},
\]

\[
\bar{Y}_B = \bar{Y}_i, \text{ with probability } \frac{1}{|\mathcal{B}|}, \text{ for } i \in \mathcal{B},
\]

\[
Z_B = Z_i, \text{ with probability } \frac{1}{|\mathcal{B}|}, \text{ for } i \in \mathcal{B},
\]

\[
X_O = X_i, \text{ with probability } \frac{1}{|\mathcal{O}|}, \text{ for } i \in \mathcal{O},
\]

\[
X'_G = X_i, \text{ with probability } \frac{1}{|\mathcal{G}\setminus\mathcal{O}|}, \text{ for } i \in \mathcal{G}\setminus\mathcal{O},
\]

\[
X'_B = X_i, \text{ with probability } \frac{1}{|\mathcal{B}\setminus\mathcal{O}|}, \text{ for } i \in \mathcal{B}\setminus\mathcal{O},
\]

\[
Y_O = \bar{Y}_O = Y_i = \bar{Y}_i, \text{ with probability } \frac{1}{|\mathcal{O}|}, \text{ for } i \in \mathcal{O},
\]

\[
Y'_G = Y_i, \text{ with probability } \frac{1}{|\mathcal{G}\setminus\mathcal{O}|}, \text{ for } i \in \mathcal{G}\setminus\mathcal{O},
\]

\[
Y'_B = Y_i, \text{ with probability } \frac{1}{|\mathcal{B}\setminus\mathcal{O}|}, \text{ for } i \in \mathcal{B}\setminus\mathcal{O},
\]

\[
Y'_B = Y_i, \text{ with probability } \frac{1}{|\mathcal{B}\setminus\mathcal{O}|}, \text{ for } i \in \mathcal{B}\setminus\mathcal{O}.
\]

\[
\begin{align*}
Y'_B &= Y_i, \text{ with probability } \frac{1}{|\mathcal{B}\setminus\mathcal{O}|}, \text{ for } i \in \mathcal{B}\setminus\mathcal{O}, \\
Y'_B &= Y_i, \text{ with probability } \frac{1}{|\mathcal{B}\setminus\mathcal{O}|}, \text{ for } i \in \mathcal{B}\setminus\mathcal{O}, \quad (164)
\end{align*}
\]

\[
\begin{align*}
Y'_B &= Y_i, \text{ with probability } \frac{1}{|\mathcal{B}\setminus\mathcal{O}|}, \text{ for } i \in \mathcal{B}\setminus\mathcal{O}, \\
T_G &= \begin{cases} O, & \text{if } i \in \mathcal{O}, \\
G', & \text{if } i \in \mathcal{G}\setminus\mathcal{O}, \quad (165)
\end{cases}
\end{align*}
\]

\[
\begin{align*}
T_B &= \begin{cases} O, & \text{if } i \in \mathcal{O}, \\
B', & \text{if } i \in \mathcal{B}\setminus\mathcal{O}. \quad (166)
\end{cases}
\end{align*}
\]

\[
\begin{align*}
W_G(y|x) &\triangleq \Pr(Y_G = y|X_G = x) \\
&= \frac{\gamma_1}{\gamma_1 + \tau_1}W_0(y|x) + \frac{\tau_1}{\gamma_1 + \tau_1}W_1(y|x), \quad (170)
\end{align*}
\]

The above random variables satisfy the following distributions

\[
\begin{align*}
W_B(y|x) &\triangleq \Pr(Y_B = y|X_B = x) \\
&= \frac{\gamma_2}{\gamma_2 + \tau_2}W_0(y|x) + \frac{\tau_2}{\gamma_2 + \tau_2}W_1(y|x), \quad (171)
\end{align*}
\]

\[
\begin{align*}
V_G(z|x) &\triangleq \Pr(Z_G = z|X_G = x) \\
&= \left(\frac{\gamma_1(1 - \epsilon_1) + \tau_1(1 - \epsilon_2)}{\gamma_1 + \tau_1}\right)V_0(z|x) + \left(\frac{\gamma_1\epsilon_1 + \tau_1\epsilon_2}{\gamma_1 + \tau_1}\right)V_1(z|x), \quad (172)
\end{align*}
\]

\[
\begin{align*}
V_B(z|x) &\triangleq \Pr(Z_B = z|X_B = x) \\
&= \left(\frac{\gamma_2(1 - \epsilon_1) + \tau_2(1 - \epsilon_2)}{\gamma_2 + \tau_2}\right)V_0(z|x) + \left(\frac{\gamma_2\epsilon_1 + \tau_2\epsilon_2}{\gamma_2 + \tau_2}\right)V_1(z|x), \quad (173)
\end{align*}
\]

\[
\begin{align*}
W'_B(y|x) &\triangleq \Pr(Y'_B = y|X'_B = x) \\
&= \Pr(Y_B = y|X_B = x, T_B = B') \\
&= \min(1 - \epsilon_1 - \alpha - \gamma_1, \gamma_2) - \frac{\min(1 - \epsilon_1 - \alpha - \gamma_1, \gamma_2) + \min(\epsilon_1 - \tau_1, \tau_2)}{W_0(y|x) + W_1(y|x)}, \quad (174)
\end{align*}
\]

\[
\begin{align*}
W'_B(y|x) &\triangleq \Pr(Y'_B = y|X'_B = x) \\
&= \Pr(Y_B = y|X_B = x, T_B = B') \\
&= \min(1 - \epsilon_1 - \alpha - \gamma_1, \gamma_2) - \frac{\min(1 - \epsilon_1 - \alpha - \gamma_1, \gamma_2) + \min(\epsilon_1 - \tau_1, \tau_2)}{W_0(y|x) + W_1(y|x)}. \quad (175)
\end{align*}
\]

We consider the following two cases:

1) If \(X_G\) and \(X_B\) do not overlap, the probability of error in the above recovery is upper bounded by \(\epsilon\) when

\[
M_1 = \exp(n\beta(R + \delta)), \quad \text{for } i \in \mathcal{B}\setminus\mathcal{O}, \quad (176)
\]

\[
R = H(X_G|Y_G) = H(X_B|\bar{Y}_B). \quad (177)
\]
2) If $X_G$ and $X_B$ overlap, we need to modify the protocol in the following way. Alice is aware of the set $O$ as the overlap between $L_1$ and $L_2$. Alice will replace the random mapping $\kappa_G$ by the following two random mappings.

\[
\kappa_{OG}: X_O \mapsto \{1, 2, \ldots, M_{1o}\}, \tag{178}
\]

\[
\kappa'_G: X_{G\setminus O} \mapsto \{1, 2, \ldots, M_{1r}\}, \tag{179}
\]

such that

\[
M_1 = M_{1o}M_{1r}, \tag{180}
\]

\[
M_{1o} = \exp(n\beta(R + \delta)), \tag{181}
\]

\[
M_{1r} = \exp(n\beta(R' + \delta)), \tag{182}
\]

\[
R = \frac{1}{2} (H(X_G|Y_G, T_G) + H(X_B|Y_B, T_B)) - H(X_G, X_B|Y_G, Y_B, T_G, T_B), \tag{183}
\]

\[
R' = H(X_G, X_B|Y_G, Y_B, T_G, T_B) - H(X_G|Y_G, T_G) = H(X_G, X_B|Y_G, Y_B, T_G, T_B) - H(X_B|Y_B, T_B). \tag{184}
\]

Similar, we replace $\kappa_B$ by $\kappa_{OB}$ and $\kappa'_B$ with the same setting as $\kappa_{OG}$ and $\kappa'_G$.

It is easy to see, from the result of Slepian-Wolf, that

a) The probability of error of recovering $X_G$ from the observation of $Y_G$, $\kappa'_G(X_G)$, $\kappa_{OG}(X_O)$, $\kappa_{OB}(X_O)$ is upper bounded by $\epsilon$.

b) The probability of error of recovering $X_B$ from the observation of $Y_B$, $\kappa'_B(X_B)$, $\kappa_{OG}(X_{O\setminus G})$, $\kappa_{OB}(X_{O\setminus G})$ is upper bounded by $\epsilon$.

c) The probability of error in recovery of both $X_G$ and $X_B$ from the observation of $Y_G$, $Y_B$, $\kappa'_G(X_G)$, $\kappa'_B(X_B)$, $\kappa_{OG}(X_O)$, $\kappa_{OB}(X_O)$ is upper bounded by $\epsilon$.

For the security requirement at Bob, we consider the following two cases

1) If $X_G$ and $X_B$ do not overlap, then if

\[
\frac{1}{n\beta} \log M_2 \leq [H(X_B|Y_B) - \frac{1}{n\beta} \log M_1]^+ - \delta
\]

\[
= [H(X_B|Y_B) - H(X_B|Y_B)]^+ - 2\delta
\]

\[
= [H(X_G|Y_G) - H(X_G|Y_G)]^+ - 2\delta
\]

\[
= [I(X_G; Y_G) - I(X_B; Y_B)]^+ - 2\delta
\]

\[
= [I(X_G; Y_G|T_G) - I(X_B; Y_B|T_B)]^+ - 2\delta, \tag{185}
\]

where (a) follows because $T_G$ and $T_B$ are constants here. Secrecy lemma implies

\[
S(\phi_B(X_B)|Y_B, \kappa_B(X_B), Y_G, \kappa_G(X_G))
\]

\[
= S(\phi_B(X_B)|Y_B, \kappa_B(X_B)) < \exp(-n\beta\xi), \tag{186}
\]

doubly exponentially surely.

2) If $X_G$ and $X_B$ overlap, then if

\[
\frac{1}{n\beta} \log M_2 \leq [H(X_B|Y_B, T_B) - \frac{1}{n\beta} \log(M_1M_{1o}^2)]^+ - \delta
\]

\[
= [H(X_B|Y_B, T_B) - (H(X_G|Y_G, T_G) + H(X_B|Y_B) - H(X_G, X_B|Y_G, Y_B, T_G, T_B)]^+ - 2\delta
\]

\[
= [I(X_G; Y_G, T_G) - I(X_B; Y_B, T_B)]^+ - 2\delta
\]

\[
= [I(X_G; Y_G|T_G) - I(X_B; Y_B|T_B)]^+ - 2\delta, \tag{187}
\]

where (a) is because $X_G$ is independent of $T_G$ and $X_B$ is independent of $T_B$.

Secrecy lemma implies

\[
S(\phi_B(X_B)|Y_B, \kappa_B(X_B), Y_G, \kappa_G(X_G))
\]

\[
= S(\phi_B(X_B)|Y_B, \kappa_B(X_B)) < \exp(-n\beta\xi), \tag{188}
\]

doubly exponentially surely.

Therefore, no matter $X_G$ and $X_B$ overlap or not, as long as

\[
\frac{1}{n\beta} \log M_2 \leq [I(X_G; Y_G|T_G) - I(X_B; Y_B|T_B)]^+ - 2\delta,
\]

we have

\[
S(\phi_B(X_B)|Y_B, \kappa_B(X_B), Y_G, \kappa_G(X_G)) < \exp(-n\beta\xi), \tag{189}
\]

doubly exponentially surely.

For the security at Eve, we consider the following two cases.

1) If $X_G$ and $X_B$ do not overlap, then if

\[
\frac{1}{n\beta} \log M_2 \leq [H(X_G|Z_G) - \frac{1}{n\beta} \log M_1]^+ - \delta
\]

\[
= [H(X_G|Z_G) - H(X_G|Y_G)]^+ - 2\delta
\]

\[
= [I(X_G; Y_G) - I(X_G; Z_G)]^+ - 2\delta
\]

\[
= [I(X_G; Y_G|T_G) - I(X_G; Z_G|T_G)]^+ - 2\delta, \tag{191}
\]

secrecy lemma implies

\[
S(\phi_B(X_B)|Z_B, \kappa_B(X_B), Z_G, \kappa_G(X_G))
\]

\[
= S(\phi_B(X_B)|Z_B, \kappa_B(X_B)) < \exp(-n\beta\xi), \tag{192}
\]

doubly exponentially surely. Similarly, if

\[
\frac{1}{n\beta} \log M_2 \leq [H(X_B|Z_B) - \frac{1}{n\beta} \log M_1]^+ - \delta
\]

\[
= [H(X_B|Z_B) - H(X_G|Y_G)]^+ - 2\delta
\]

\[
= [I(X_G; Y_G) - I(X_B; Z_B)]^+ - 2\delta
\]

\[
= [I(X_G; Y_G|T_G) - I(X_B; Z_B|T_B)]^+ - 2\delta, \tag{193}
\]

secrecy lemma implies

\[
S(\phi_B(X_B)|Z_B, \kappa_B(X_B), Z_G, \kappa_G(X_G))
\]

\[
= S(\phi_B(X_B)|Z_B, \kappa_B(X_B)) < \exp(-n\beta\xi), \tag{194}
\]
doubly exponentially surely, where the first equality is due to the fact that $X_B$ is independent of $X_G$, when they do not overlap. From the above analysis, we have

$$S(\phi_G(X_G), \phi_B(X_B)|Z_B, \kappa_B(X_B), Z_B, \kappa_G(X_G), \phi_B(X_G)) = S(\phi_G(X_G)|Z_B, \kappa_B(X_B), Z_B, \kappa_G(X_G)) + S(\phi_B(X_B)|\phi_G(X_G), Z_B, \kappa_B(X_B), Z_B, \kappa_G(X_G), \phi_B(X_G)) \leq 2 \exp(-n\beta\xi), \quad (195)$$

doubly exponentially surely

2) If $X_G$ and $X_B$ overlap, we need to go back to the extractor lemma [16, Lemma 17.3], which leads to the secrecy lemma. In the proof of extractor lemma, it is shown that a random selected mapping $\kappa: \mathcal{X} \mapsto \{1, 2, \ldots, k\}$ satisfies that the following probability

$$\Pr \left( |\Pr(\kappa^{-1}(i)) - \frac{1}{k}| \geq \frac{\epsilon}{k} \right), \quad i = 1, \ldots, k, \quad (196)$$
is exponentially small. In our case here, we are working with two random selected mappings $\phi_G$ and $\phi_B$, therefore, we need to prove that the probability

$$\Pr \left( |\Pr(\phi_G^{-1}(i)) - \frac{1}{M_2}| \geq \frac{\epsilon}{M_2} \right)
\text{ or } |\Pr(\phi_B^{-1}(j)) - \frac{1}{M_2}| \geq \frac{\epsilon}{M_2} \right), \quad i = 1, \ldots, M_2, \text{ and } j = 1, \ldots, M_2, \quad (197)$$
is exponentially small. To show this, we need to make the following three probabilities

$$\Pr \left( |\Pr(\phi_G^{-1}(i)) - \frac{1}{M_2}| \geq \frac{\epsilon}{M_2} \right)
\text{ and } |\Pr(\phi_B^{-1}(j)) - \frac{1}{M_2}| \leq \frac{\epsilon}{M_2} \right) \leq \Pr \left( |\Pr(\phi_G^{-1}(i)) - \frac{1}{M_2}| \geq \frac{\epsilon}{M_2} \right), \quad (198)$$

$$\Pr \left( |\Pr(\phi_G^{-1}(i)) - \frac{1}{M_2}| \leq \frac{\epsilon}{M_2} \right)
\text{ and } |\Pr(\phi_B^{-1}(j)) - \frac{1}{M_2}| \geq \frac{\epsilon}{M_2} \right) \leq \Pr \left( |\Pr(\phi_B^{-1}(j)) - \frac{1}{M_2}| \geq \frac{\epsilon}{M_2} \right), \quad (199)$$

$$\Pr \left( |\Pr(\phi_G^{-1}(i)) - \frac{1}{M_2}| \geq \frac{\epsilon}{M_2} \right)
\text{ and } |\Pr(\phi_B^{-1}(j)) - \frac{1}{M_2}| \geq \frac{\epsilon}{M_2} \right) \leq \Pr \left( |\Pr(\phi_B^{-1}(j)) - \frac{1}{M_2}| \geq \frac{\epsilon}{M_2} \right), \quad (200)$$
exponentially small. Therefore, we will follow the arguments from Lemma 17.3 to Corollary 17.5 in [16, Section 17.1] and work on all of the above three probabilities separately. Then we have if the following three conditions are all satisfied,

$$\frac{1}{n\beta} \log M_2 \leq [H(X_G|Z_G, T_G) - \frac{1}{n\beta} \log(M_1 M_1^2)]^+ - \delta$$

$$= [H(X_G|Z_B, T_G) - \frac{1}{n\beta} \log(M_1 M_1^2)]^+ - \delta$$

$$= [H(X_G|Y_G, T_G) + H(X_B|Y_B, T_B)] - [H(X_G, X_B|Y_G, Y_B, T_G, T_B)] - [H(X_G, X_B|Y_G, Y_B, T_G, T_B)] + [H(X_G|Y_G, T_G)] + [H(X_B|Y_B, T_B)]^+ - 2\delta$$

$$= [I(X_G; Y_G, T_G) - I(X_G; Z_G|T_G)]^+ + 2\delta$$

$$= [I(X_G; Y_G|T_G) - I(X_G; Z_G|T_G)]^+ + 2\delta,$$ \quad (201)

$$\frac{1}{n\beta} \log M_2 \leq [H(X_B|Z_B, T_B) - \frac{1}{n\beta} \log(M_1 M_1^2)]^+ - \delta$$

$$= [H(X_G|Z_G, T_G) - \frac{1}{n\beta} \log(M_1 M_1^2)]^+ - \delta$$

$$= [I(X_G; Y_G|T_G) - I(X_G; Z_G|T_G)]^+ + 2\delta$$

$$= [I(X_G; Y_G|T_G) - I(X_G; Z_G|T_G)]^+ + 2\delta,$$ \quad (202)

secrecy lemma implies

$$S(\phi_G(X_G), \phi_B(X_B)|Z_B, \kappa_B(X_B), Z_G, \kappa_G(X_G), \phi_G(X_G)) < \exp(-n\beta\xi), \quad (205)$$
doubly exponentially surely.

Therefore, no matter $X_G$ and $X_B$ overlap or not, as long as

$$\frac{1}{n\beta} \log M_2 \leq [I(X_G; Y_G|T_G) - I(X_G; Z_G|T_G)]^+ - 2\delta,$$ \quad (206)

$$\frac{1}{n\beta} \log M_2 \leq [I(X_G; Y_G|T_G) - I(X_G; Z_G|T_G)]^+ - 2\delta,$$ \quad (207)
\[
\frac{1}{n^*} \log M \leq \frac{1}{2} \left[ I(X_G, X_B; Y_G, \tilde{Y}_B| T_G, T_B) - I(X_G, X_B; Z_G, Z_B| T_G, T_B) \right]^+ - \delta),
\]
we have
\[
S(\phi_G(X_G), \phi_B(X_B)| Z_B, \kappa_B(X_B), Z_G, \kappa_G(X_G), \phi_G(X_G)) < \exp(-n/\beta),
\]
doubly exponentially surely.

In conclusion, there exists a pair of deterministic secret key generation schemes \((\phi_G(X_G), \phi_B(X_B))\) satisfying security index requirement \((190)\) and \((209)\). Next, we prove that the proposed protocol satisfies the conditions in \((15)-(18)\).

**Correctness:** We prove that \((15)\) is satisfied for our protocol. In our protocol, an error occurs in decoding \(K_{\Theta}\) if secret key \(K_{\alpha}\) is recovered incorrectly or the secret key \(\phi_G(X_G)\) is recovered incorrectly. We have shown that the probabilities of above two errors, i.e., errors of \(K_{\alpha}\) and errors of \(\phi_G(X_G)\), are both less than \(\epsilon\). Therefore, the probability of decoding error is upper bounded by \(2\epsilon\).

**Security at Bob** We prove that \((17)\) is satisfied for our protocol. We know that
\[
V_B = (\Theta, Y^n, N, L_G, L_B, L_\alpha, S, K_{\alpha}, \kappa_G(X_L), K_B(X_L), K_{\Theta} \oplus \phi_G(X_L), K_{\Theta} \oplus \phi_B(X_L)).
\]
We define
\[
V_B \setminus (K_{\Theta} \oplus \phi_B(X_L)) = (\Theta, Y^n, N, L_G, L_B, L_\alpha, S, K_{\alpha}, \kappa_G(X_L), K_B(X_L), K_{\Theta} \oplus \phi_G(X_L)),
\]
in other words, \(V_B \setminus (K_{\Theta} \oplus \phi_B(X_L))\) contains all the random variables in \(V_B\), except \(K_{\Theta} \oplus \phi_B(X_L)\).

The information leakage at Bob is
\[
\begin{align*}
I(K_{\Theta}; V_B) &\leq I(K_{\Theta}; V_B \setminus (K_{\Theta} \oplus \phi_B(X_L)))+ \delta) \\
&= H(K_{\Theta} \oplus \phi_B(X_L)| V_B \setminus (K_{\Theta} \oplus \phi_B(X_L)))- H(K_{\Theta} \oplus \phi_B(X_L)| K_{\Theta}, V_B \setminus (K_{\Theta} \oplus \phi_B(X_L))) \\
&\leq |K_{\Theta} \oplus \phi_B(X_L)| - H(K_{\Theta} \oplus \phi_B(X_L)| K_{\Theta}, V_B \setminus (K_{\Theta} \oplus \phi_B(X_L))) \\
&= |K_{\Theta} \oplus \phi_B(X_L)| - H(K_{\Theta} \oplus \phi_B(X_L)| V_B \setminus (K_{\Theta} \oplus \phi_B(X_L))) \\
&= |K_{\Theta} \oplus \phi_B(X_L)| - |\phi_B(X_L)| + S(\phi_B(X_L)| Y_L, X_L, \kappa_G(X_L), \kappa_B(X_L)) \\
&\leq |K_{\Theta} \oplus \phi_B(X_L)| - |\phi_B(X_L)| + \exp(-n/\beta)
\end{align*}
\]
where \((a)\) is due to the Markov chain
\[
K_{\Theta} \rightarrow K_{\Theta} \oplus \phi_B(X_L) \rightarrow V_B \setminus (K_{\Theta} \oplus \phi_B(X_L)),
\]
\((b)\) is due to the Markov chain
\[
\phi_B(X_L) \rightarrow (Y_L, \kappa_G(X_L), \kappa_B(X_L)) \rightarrow (K_{\Theta}, V_B \setminus (K_{\Theta} \oplus \phi_B(X_L))),
\]
and \((c)\) follows because of \((190)\).

**Privacy at Alice:** We prove that \((16)\) is satisfied for our protocol. We follow the same argument as \((98)\) in the proof of Lemma A and obtain \(I(\Theta, \tilde{V}_A) = 0\).

**Security and Privacy at Eve:** We prove that \((18)\) is satisfied for our protocol. We know that
\[
V_E = (Z^n, L_0, L_1, L_\alpha, S \oplus K_{\alpha}, \kappa_G(X_L), \kappa_B(X_L), K_{\Theta} \oplus \phi_G(X_L), K_{\Theta} \oplus \phi_B(X_L)).
\]
We define
\[
V_E \setminus (S \oplus K_{\alpha}) = (Z^n, L_0, L_1, L_\alpha, \kappa_G(X_L), \kappa_B(X_L), K_{\Theta} \oplus \phi_G(X_L), K_{\Theta} \oplus \phi_B(X_L))
\]
i.e., \(V_E \setminus (S \oplus K_{\alpha})\) contains all the random variables in \(V_E\), except \(S \oplus K_{\alpha}\) and \(K_{\Theta} \oplus \phi_G(X_L), K_{\Theta} \oplus \phi_B(X_L))\) contains all the random variables in \(V_E\), except \((K_{\Theta} \oplus \phi_G(X_L), K_{\Theta} \oplus \phi_B(X_L))\).

We have
\[
I(K_{\Theta}, K_{\Theta}, \Theta; V_E) = I(K_{\Theta}, \Theta; V_E) = I(\Theta; V_E) + I(K_{\Theta}, \Theta; V_E | \Theta).
\]
For the first term, we have
\[
I(\Theta; V_E) \leq I(\Theta; V_E | \Theta \oplus S) + I(\Theta; \Theta \oplus S) \\
= I(\Theta; V_E | \Theta \oplus S) = I(S; \tilde{V}_E | \Theta \oplus S) = I(S; \tilde{V}_E | \Theta \oplus S)
\]
\((a)\)
\[
I(S; S \oplus \kappa_{\alpha}, \tilde{V}_E | (S \oplus \kappa_{\alpha}), \Theta \oplus S) = H(S \oplus \kappa_{\alpha}, \tilde{V}_E | (S \oplus \kappa_{\alpha}), \Theta \oplus S) - H(S \oplus \kappa_{\alpha}, \tilde{V}_E | (S \oplus \kappa_{\alpha}), \Theta \oplus S) - H(K_{\Theta} | S, \tilde{V}_E | (S \oplus \kappa_{\alpha}), \Theta \oplus S)
\]
\((b)\)
\[
\leq \log |S \oplus \kappa_{\alpha}| - H(K_{\Theta} | Z_L, \kappa_{\alpha}(Y_L)) = \log |S \oplus \kappa_{\alpha}| - \log |K_{\Theta}| + S(K_{\Theta} | Z_L, \kappa_{\alpha}(Y_L))
\]
\((c)\)
\[
\leq \exp(-na/\beta)
\]
where \((a)\) is due to the Markov chain
\[
S \rightarrow (S \oplus K_\alpha, \Theta \oplus S) \rightarrow V_E \backslash (S \oplus K_\alpha),
\] (220)

\((b)\) is due to the Markov chain
\[
K_\alpha \rightarrow (Z_{L_\alpha}, \kappa_\alpha(Y_{L_\alpha})) \rightarrow (S, V_E \backslash (S \oplus K_\alpha), \Theta \oplus S),
\] (221)

and \((c)\) follows because of (150).

For the second term, we have
\[
\log I_{K_\Theta, K_\Theta; E|\Theta} = \log I_{K_\Theta, K_\Theta; E|\Theta} - \log I_{K_\Theta, K_\Theta; E|\Theta} = \log I_{K_\Theta, K_\Theta; E|\Theta} - \log I_{K_\Theta, K_\Theta; E|\Theta} = \log I_{K_\Theta, K_\Theta; E|\Theta}.
\]

From (170)-(173), we have
\[
\beta I(X_G; Y_G|T_G) - I(X_B; Y_B|T_B) = \gamma_1 I(X; Y_0) + \tau_1 I(X; Y_1) - \gamma_2 I(X; Y_0) - \tau_2 I(X; Y_1) - \gamma_1 I(Y_0) - \gamma_2 I(Y_1)
\]
\[
= (\gamma_1 - \gamma_2) R_0,
\]

\[
\beta I(X_G; Y_G|T_G) - I(X_G; Z_G|T_G)
\]
\[
= \gamma_1 I(Y_0) + \gamma_2 I(Y_1) - \gamma_1 I(Y_0) - \gamma_2 I(Y_1) - \gamma_1 \epsilon_3 R_{00} + \gamma_2 \epsilon_3 R_{01} + (\gamma_1 - \gamma_2) R_{10} + \gamma_1 \epsilon_2 R_{11} + \gamma_2 \epsilon_2 R_{10} + \gamma_1 R_G + \gamma_2 R_B,
\]

\[
\beta I(X_B; Y_B|T_B) = \beta I(X_B; Y_B|T_B) - I(X_B; Z_B|T_B) + \beta I(X_B; Y_G|T_G) - I(X_B; Z_G|T_G) + \beta I(X_B; Y_G|T_G) - I(X_B; Z_G|T_G) + \beta I(X_B; Y_G|T_G) - I(X_B; Z_G|T_G) + \beta I(X_B; Y_B|T_B)
\]

\[
= \gamma_1 I(Y_0) + \gamma_2 I(Y_1) - \gamma_1 I(Y_0) - \gamma_2 I(Y_1) - \gamma_1 \epsilon_3 R_{00} + \gamma_2 \epsilon_3 R_{01} + (\gamma_1 - \gamma_2) R_{10} + \gamma_1 \epsilon_2 R_{11} + \gamma_2 \epsilon_2 R_{10} + \gamma_1 R_G + \gamma_2 R_B,
\]

\[
\beta I(X_G; Y_G|T_G) - I(X_G; Z_G|T_G) = \beta I(X_G; Y_G|T_G) - I(X_G; Z_G|T_G)
\]

\[
= \gamma_1 I(Y_0) + \gamma_2 I(Y_1) - \gamma_1 I(Y_0) - \gamma_2 I(Y_1) - \gamma_1 \epsilon_3 R_{00} + \gamma_2 \epsilon_3 R_{01} + (\gamma_1 - \gamma_2) R_{10} + \gamma_1 \epsilon_2 R_{11} + \gamma_2 \epsilon_2 R_{10} + \gamma_1 R_G + \gamma_2 R_B,
\]

\[
\beta I(X_B; Y_B|T_B) = \beta I(X_B; Y_B|T_B) - I(X_B; Z_B|T_B) + \beta I(X_B; Y_G|T_G) - I(X_B; Z_G|T_G) + \beta I(X_B; Y_G|T_G) - I(X_B; Z_G|T_G) + \beta I(X_B; Y_B|T_B)
\]

\[
= \gamma_1 I(Y_0) + \gamma_2 I(Y_1) - \gamma_1 I(Y_0) - \gamma_2 I(Y_1) - \gamma_1 \epsilon_3 R_{00} + \gamma_2 \epsilon_3 R_{01} + (\gamma_1 - \gamma_2) R_{10} + \gamma_1 \epsilon_2 R_{11} + \gamma_2 \epsilon_2 R_{10} + \gamma_1 R_G + \gamma_2 R_B.
\]
\[ R = \min \left\{ \min(\epsilon_1, 1 - \epsilon_1), (1 - \epsilon_1) \epsilon_3, \frac{1}{2} \left[ (1 - \epsilon_1) \epsilon_3 + \min(\epsilon_1, 1 - \epsilon_1) \epsilon_2 \right] \right\}. \]
If we assume $\epsilon_2 < \epsilon_3$, we have that the second term is larger than the third term in the lower bound in (235). Therefore,

$$R = \min(\min(\epsilon_1, 1 - \epsilon_1), \max(1 - 2\epsilon_1, 0))\epsilon_3 +$$

$$+ \min(\epsilon_1, 1 - \epsilon_1)\epsilon_2, \frac{1}{2}(1 - \epsilon_1)\epsilon_3 + \min(1 - \epsilon_1, \epsilon_1)\epsilon_2)$$

$$= \begin{cases} 
\min(\epsilon_1, (1 - 2\epsilon_1)\epsilon_3 + \epsilon_1\epsilon_2, \\
\frac{1}{2}(1 - \epsilon_1)\epsilon_3 + \epsilon_1\epsilon_2) 
\end{cases} \text{if } \epsilon_1 \leq \frac{1}{2},$$

$$= (1 - \epsilon_1)\epsilon_2 \quad \text{if } \epsilon_1 \geq \frac{1}{2}$$

(246)

which concludes the proof of Corollary 1.

REFERENCES

[1] D. V. Forney J. D. Jr., “The reliability function of a code over an arbitrary alphabet,” in Proc. IEEE Int. Symp. Inf. Theory, 1966, pp. 157–166.

[2] J. V. Levenshtein, “The weight distribution of binary linear codes,” Probl. Pereda. Inform., vol. 10, pp. 3–18, 1966.

[3] R. Ahlswede and I. Csiszar, “Common randomness in information theory and cryptography, Part I: Secret sharing,” IEEE Trans. Inf. Theory, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[4] A. E. Gamal and Y.-H. Kim, Network Information Theory. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[5] C. Crépeau, “Efficient unconditional oblivious transfer,” in Information Theory, Combinatorics, and Search Theory, Cham, Switzerland: Springer, 2013, pp. 145–166.

[6] M. Mishra, B. K. Dey, V. M. Prabhakaran, and S. N. Diggavi, “Wire-tapped oblivious transfer,” IEEE Trans. Inf. Theory, vol. 63, no. 4, pp. 2560–2595, Apr. 2017.

[7] I. Csiszar and J. Körner, Information Theory: Coding Theorems for Discrete Memoryless Systems. Cambridge, U.K.: Cambridge Univ. Press, 11.

[8] A. L. Carter and M. N. Wegman, “Universal classes of hash functions,” J. Comput. Syst. Sci., vol. 18, no. 2, pp. 143–154, Apr. 1979. [Online]. Available: https://www.sciencedirect.com/science/article/pii/0022000079900448

[9] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, “Generalized privacy amplification,” IEEE Trans. Inf. Theory, vol. 41, no. 6, pp. 1915–1923, Jun. 1995.

[10] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, “Generalized privacy amplification,” IEEE Trans. Inf. Theory, vol. 41, no. 6, pp. 1915–1923, Jun. 1995.

[11] Tianyou Pei received the B.Eng. degree in communications engineering from Qingdao University, Qingdao, China, in 2020, and the M.Eng. degree in information and communication engineering from Southeast University, Nanjing, China, in 2023. He joined Nanjing Research and Development Center, Huawei Technology Company Ltd., Nanjing, in 2023. His main research interests include information theoretical security.

[12] Wei Kang (Member, IEEE) received the B.Eng. degree in electrical engineering from Beijing University of Posts and Telecommunications, Beijing, China, in 2001, the M.Eng. degree in electrical engineering from McGill University, Montreal, Canada, in 2003, and the Ph.D. degree in electrical engineering from the University of Maryland, College Park, MD, USA, in 2008. He joined the School of Information Science and Engineering, Southeast University, Nanjing, China, in 2009, where he is currently a Professor. His main research interests include network information theory.

[13] Nan Liu (Member, IEEE) received the B.Eng. degree in electrical engineering from Beijing University of Posts and Telecommunications, Beijing, China, in 2001, and the Ph.D. degree in electrical and computer engineering from the University of Maryland, College Park, MD, USA, in 2007. From 2007 to 2008, she was a Post-Doctoral Scholar with the Wireless Systems Laboratory, Department of Electrical Engineering, Stanford University. In 2009, she became a Professor with the National Mobile Communications Research Laboratory, School of Information Science and Engineering, Southeast University, Nanjing, China. Her research interests include information theory and communication theory. She is currently an Associate Editor of IEEE TRANSACTIONS ON COMMUNICATIONS.