The Oblivious Transfer Capacity of the Wiretapped Binary Erasure Channel

Manoj Mishra and Bikash Kumar Dey
IIT Bombay, India
Email: {mmishra,bikash}@ee.iitb.ac.in

Vinod M. Prabhakaran
TIFR, Mumbai, India
Email: vinodmp@tifr.res.in

Suhas Diggavi
UCLA, USA
Email: suhas@ee.ucla.edu

Abstract—We consider oblivious transfer between Alice and Bob in the presence of an eavesdropper Eve when there is a broadcast channel from Alice to Bob and Eve. In addition to the secrecy constraints of Alice and Bob, Eve should not learn the private data of Alice and Bob. When the broadcast channel consists of two independent binary erasure channels, we derive the oblivious transfer capacity for both 2-privacy (where the eavesdropper may collude with either party) and 1-privacy (where there are no collusions).

I. INTRODUCTION

The goal of secure multiparty computation (MPC) is for mutually distrusting parties to collaborate in computing functions of their data, but without revealing anything more about their data to others than what they can infer from the function outputs and data. Useful applications of secure MPC include voting, auctions and data-mining amongst several others, see e.g., [4, Chap. 1]. It is well known that information theoretically (unconditionally) secure computation is not possible, in general (i.e. for arbitrary functions), between two parties with noiseless communication and only common and private randomness. A combinatorial characterization of functions that can be securely computed by two parties is given in [7]. Two-party secure computation, in general, requires additional stochastic resources. Specifically, a noisy channel between the parties provides a means to achieve secure computation [4].

Oblivious Transfer (OT) has been proposed as a basic primitive (which can be derived from noisy channels) on which secure computation can be founded [5, 6]. One-out-of-two (1-of-2) string OT is a secure 2-party primitive computation, where one party, Alice, has two strings of equal lengths out of which, the other party, Bob, obtains exactly one string of his choice without Alice finding out the identity of the string selected by Bob. The (string) OT capacity of a discrete memoryless channel is the largest string-length-per-channel-use that can be supported. OT capacity of discrete memoryless channels has been studied in [1, 8, 9]. In [8], a lower bound on the string OT capacity of noisy channels and source distributions was obtained for honest-but-curious participants (i.e., the parties do not deviate from the prescribed protocol, but attempt to derive information about the other party’s input that they are not allowed to know from everything they have access to at the end of the protocol). [1] characterizes the string OT capacity for generalized erasure channels, when the two parties are honest-but-curious. [9] shows that this honest-but-curious string OT capacity of generalized erasure channels can, in fact, be achieved even when the two parties are malicious.

A natural consideration when using noisy channels is the presence of third parties who may derive useful information about the computation. For example, consider the noisy resource as a wireless channel. In this case, an eavesdropper who receives partial information about the transmissions can use it to deduce the output or data of the parties. Motivated by this, we study the OT capacity of an erasure channel in the presence of an eavesdropper (Figure 2). To the best of our knowledge, this problem has not been studied before. We limit our study to the case of honest-but-curious parties Alice and Bob and a passive eavesdropper Eve. We consider secrecy regimes where Eve may collude with Alice or Bob (2-privacy) and where there is no such collusion (1-privacy). These requirements are made more precise in the next section. We derive the 1-of-2 string OT capacity, for both 1-privacy and 2-privacy, in the setup of Figure 2 when Bob and Eve receive independently erased versions of Alice’s transmissions.

The rest of the paper is organized as follows. Section II gives the precise problem definition and states the capacity results that have been proved. Section III gives the achievability part of the proof of our results, by describing protocols achieving any 2-private and 1-private rate below their respective capacities, for the setup of Figure 2. The converse part for our results are proved in Section IV. Most of the rate upper bounds we have hold for the general case of Figure 1 except for one regime in 1-privacy case where the upper bound is specific to the setup of Figure 2.

II. PROBLEM DEFINITION AND STATEMENT OF RESULTS

In the setup of Figure 1 Alice has two independent, uniformly distributed $m$-length bit strings $K_0, K_1$ and Bob has a uniformly distributed choice bit $C$ independent of $K_0, K_1$. Alice is connected to Bob and Eve by a discrete memoryless broadcast channel defined by the conditional distribution $p_Y|Z,X$. Further, Alice and Bob can communicate over an error-free public channel of unlimited capacity, with Eve able to receive every message sent on this public channel. Alice, Bob and Eve are honest-but-curious participants in the protocols that run in this setup.

Definition 1: An $(m, n, k)$ protocol uses the broadcast channel at some instances $i_1, i_2, ..., i_n \in \{1, \ldots, k\}$ and the
The protocol computes \( \hat{K}_C = \hat{K}(C, N, F^k, Y^n) \) as Bob’s string at the end.

We define the views of Alice, Bob and Eve at the end of the protocol to be, respectively,

\[
U_k = (K_0, K_1, M, F^k), \quad V_k = (C, N, F^k, Y^n), \quad W_k = (F^k, Z^n).
\]

Definition 2: A non-negative number \( R_{2P} \) is said to be an achievable 2-private rate if there exists a sequence of \((m, n, k)\) protocols, with \( \frac{m}{n} \rightarrow R_{2P} \) as \( n \rightarrow \infty \), such that

\[
\begin{align*}
P[\hat{K}_C \neq K_C] & \rightarrow 0, \quad (1) \\
I(K_{\overline{C}}; V_k, W_k) & \rightarrow 0, \quad (2) \\
I(C; U_k, W_k) & \rightarrow 0, \quad (3) \\
I(K_0, K_1, C; W_k) & \rightarrow 0, \quad (4)
\end{align*}
\]

where \( \overline{C} = C \oplus 1 \).

Definition 3: The 2-private capacity, \( C_{2P} \), is defined as the supremum of all achievable 2-private rates.

Definition 4: A non-negative number \( R_{1P} \) is said to be an achievable 1-private rate if there exists a sequence of \((m, n, k)\) protocols, with \( \frac{m}{n} \rightarrow R_{1P} \) as \( n \rightarrow \infty \), such that

\[
\begin{align*}
P[\hat{K}_C \neq K_C] & \rightarrow 0, \quad (5) \\
I(K_{\overline{C}}; V_k) & \rightarrow 0, \quad (6) \\
I(C; U_k) & \rightarrow 0 \quad (7)
\end{align*}
\]

where \( \overline{C} = C \oplus 1 \).

Definition 5: The 1-private capacity, \( C_{1P} \), is defined as the supremum of all achievable 1-private rates.

Our main result is the characterization of \( C_{2P} \) and \( C_{1P} \) for the setup of Figure 2. In this specific version of the setup of Figure 1 the broadcast channel is made up of two independent binary erasure channels (BECs). A BEC with erasure probability \( \epsilon_1 (\text{BEC}(\epsilon_1)) \) connects Alice to Bob and a BEC(\( \epsilon_2 \)) connects Bob to Eve. BEC(\( \epsilon_1 \)) acts independently of BEC(\( \epsilon_2 \)) and no assumption is made on the relative values of \( \epsilon_1 \) and \( \epsilon_2 \).

We prove the following theorems for the setup of Figure 2

**Theorem 1:**

\[
C_{2P} = \epsilon_2 \cdot \min\{\epsilon_1, 1 - \epsilon_1\}.
\]

**Theorem 2:**

\[
C_{1P} = \begin{cases} 
\epsilon_1, & \epsilon_1 < \frac{\epsilon_2}{2} \\
\frac{\epsilon_2}{2}, & \frac{\epsilon_2}{2} \leq \epsilon_1 < \frac{1}{2} \\
\epsilon_1 \geq \frac{1}{2} & \end{cases}
\]

### III. PROOF OF ACHIEVABILITY

We begin by briefly reviewing the achievable protocol for a BEC(\( \epsilon_1 \)) given in [1]. We note that the setup of Figure 2 for \( \epsilon_2 = 1 \), reduces to the setup in [1]. Suppose Bob wishes to obtain one of the strings of length \( m \) from Alice. Alice transmits an i.i.d. uniform sequence of bits \( X^n \) over the broadcast channel. Bob receives an erased version \( Y^n \) of \( X^n \). Bob will choose two sets of \( m \) distinct indices (bit locations) each, a set \( B \) (bad set) from the erased indices and a set \( G \) (good set) from the unerased indices. Bob chooses these sets uniformly at random from among the possible choices. In this sketch we ignore the possibility that sufficient number of erased and unerased locations are not present; the probability of such an event will be made small enough by an appropriate choice of \( m \) and \( n \) in the sequel. For \( C = 0 \), Bob assigns \((L_0, L_1) = (G, B)\); otherwise \((L_0, L_1) = (B, G)\). Bob sends \((L_0, L_1)\) to Alice. Alice will form the OT keys, \( T_0 = X^n|_{L_0} \) and \( T_1 = X^n|_{L_1} \), where \( X^n|_{L_0} \) denotes the sequence \( X^n \) restricted to the locations in \( L_0 \). Alice sends \( K_0 \oplus T_0 \) and...
Bob. Alice uses these secret keys to further encrypt the strings before sending them over the public channel. Specifically, Alice and Bob will create (as explained later) two independent secret keys $S_0, S_1$ (each of length approximately $m(1 - \epsilon_2)$), neither of which is known to Eve and only one of which, namely $S_C$, is known to Bob. Notice that Alice will remain unaware of the identity of the secret key known to Bob. Alice uses these secret keys to further encrypt the strings before sending them over the public channel. Specifically, $S_0$ is used to further encrypt $K_0 \oplus T_0$ and $S_1$ for $K_1 \oplus T_1$. This is done by Alice expanding $S_0, S_1$ (each of length approximately $m(1 - \epsilon_2)$) to $S_0, S_1$ respectively (each of length $m$ bits), using a binary code (obtained using random coding argument) of rate about $(1 - \epsilon_2)$. Alice sends $K_0 \oplus T_0 \oplus S_0$ and $K_1 \oplus T_1 \oplus S_1$ to Bob over the public channel.

To generate $S_0, S_1$, Alice and Bob use the secret key agreement scheme of [10], which shows that Alice and Bob can agree upon a secret key which is almost perfectly secret from Eve (i.e. $I(S_i; W_k) \rightarrow 0$ as $n \rightarrow \infty$, $i = 1, 2$), at rate $\epsilon_2$, if Bob received unerased transmissions from Alice. So, to generate $S_0, S_1$, Bob will uniformly at random choose sets of indices $G_S$ (good secret key set) and $B_S$ (bad secret key set), of length approximately $m(1 - \epsilon_2)$ each, from, respectively, unerased and erased indices which were unused for OT key generation. As before, $G_S, B_S$ are sent to Alice in an order determined by $C$. Alice uses $X^n|_{G_S}, X^n|_{B_S}$ to generate the secret keys.

For 1-privacy, Bob may choose $B_S$ randomly from the erased and unerased indices it has leftover after creating $G, B$ and $G_S$. The rest of the protocol remains the same as that for 2-privacy. Clearly, Bob may now know some or all of the bad secret key. Since this secret key is meant to provide security against Eve with whom Bob does not collude now, the secrecy condition is unaffected.

### A. Protocol for a achieving any 2-private rate $r < C_{2P}$

We now present a protocol which achieves any 2-private rate less than $C_{2P}$, for the setup of Figure 2. For any $\delta \in (0, 1)$, we define

$$\tilde{\epsilon}_2 := \epsilon_2(1 - \delta).$$

In a protocol where Alice transmits $n$ bits over the BEC, let $E, E', E''$ be, respectively, the set of indices where Bob sees erasures, Bob sees non-erasures, and Eve sees erasures.

$$E := \{ i \in \{1, \ldots, n\} : Y_i = \text{erasure} \},$$

$$E' := \{ i \in \{1, \ldots, n\} : Y_i = \text{erasure} \},$$

$$E'' := \{ i \in \{1, \ldots, n\} : Y_i \neq \text{erasure} \}.$$

Let $U(A)$ denotes a uniformly random choice from the set $A$. The following lemma says that, with high probability, Eve will see at least $\tilde{\epsilon}_2$ fraction of its received sequence erased.

**Lemma 1:**

$$P \left[ \frac{|E'|}{n} \geq \frac{\tilde{\epsilon}_2}{2} \right] \longrightarrow 1 \text{ exponentially in } n.$$  

**Proof:** The claim follows from Chernoff bound. □

The following lemma says that for any rate $r < C_{2P}$ and a suitably low $\delta$ (to define $\tilde{\epsilon}_2$), Bob will have enough erased and unerased $Y_i$’s with which to run the protocol and achieve rate $r$.

**Lemma 2:** Suppose $r < C_{2P}$ and $\delta < (1 - \epsilon_2)$. Then

$$P \left[ |E| \geq \frac{nr}{\epsilon_2} \right] \longrightarrow 1 \text{ exponentially in } n,$$

$$P \left[ |E'| \geq \frac{nr}{\epsilon_2} \right] \longrightarrow 1 \text{ exponentially in } n.$$  

**Proof:** The claims follow from Chernoff bound. □

### Protocol 1: (Protocol for achieving any 2-private rate $r < C_{2P}$, for the setup in Figure 2)

**Protocol parameters** (known to all parties): rate $r, \delta$ (suitably low, as per Lemma 2), $\tilde{\epsilon}_2$, a binary $(nr, nr(1 - \tilde{\epsilon}_2))$-code $\Lambda_{nr}$ chosen via a random coding argument

**Alice** Transmits an i.i.d. sequence $X^n$, where $\forall i, \ X_i \sim U(\{0, 1\})$, over the BEC.

**Bob** Receives the $Y^n$ from $\text{BEC}(\epsilon_1)$. Let $r < C_{2P}$. Bob now creates the following sets:

$$G \sim U \left( \{ A \subset \overline{Y} : |A| = nr \} \right),$$

$$G_S \sim U \left( \{ A \subset \overline{Y} : |A| = \frac{nr(1 - \tilde{\epsilon}_2)}{\tilde{\epsilon}_2} \} \right),$$

$$B \sim U \left( \{ A \subset E : |A| = nr \} \right),$$

$$B_S \sim U \left( \{ A \subset E : |A| = |G_S| \} \right).$$

Bob has sufficiently many erased and unerased $Y_i$’s (with high probability) to create these sets, as a consequence of Lemma 2. Then, depending on the value of $C$, Bob further creates the sets $L_{00}, L_{01}, L_{10}, L_{11}$ as follows.

$$C = 0 : \quad L_{00} = G, \quad L_{01} = G_S \quad L_{10} = B, \quad L_{11} = B_S$$

$$C = 1 : \quad L_{00} = B, \quad L_{01} = B_S \quad L_{10} = G, \quad L_{11} = G_S$$

Bob sends $L_{00}, L_{01}, L_{10}, L_{11}$ to Alice over the public channel.

**Alice** computes the following keys

$$T_0 = X^n|_{L_{00}},$$

$$T_1 = X^n|_{L_{11}}.$$  

Alice generates secret key $S_0$ from $X^n|_{L_{01}}$, assuming Bob knows $X^n|_{L_{01}}$. Alice also generates secret
key $S_1$ from $X^n|_{L_{11}}$, assuming Bob knows $X^n|_{L_{11}}$. $S_0, S_1$ are $nr(1 - \epsilon_2)$ bits each.

Alice expands the secret keys $S_0, S_1$, to get $\tilde{S}_0, \tilde{S}_1$ of $nr$ bits each

$$\tilde{S}_0 = \Lambda_{nr}(S_0),$$
$$\tilde{S}_1 = \Lambda_{nr}(S_1).$$

Alice finally sends the following two strings to Bob over the public channel:

$$K_0 \oplus T_0 \oplus \tilde{S}_0,$$
$$K_1 \oplus T_1 \oplus \tilde{S}_1.$$

Bob has the pair $(T_C, \tilde{S}_C)$, thus he can get $K_C$.

**Lemma 3:** Any $r < C_{2P}$ is an achievable 2-private rate.

**Proof:**

A sequence of instances $\{P_n\}_{n \in \mathbb{N}}$ of Protocol [1] will be used. Let $J := \lfloor (|E|n(1 - \epsilon_2))/n \rfloor$ be the random variable to indicate the event that Bob has seen enough erasures and non-erasures. By Lemma [2] $P_r[|J| = 1] \rightarrow 1$ exponentially fast.

For ease of notation, we denote:

$$C = (G, B, G_S, B_S)$$
$$L = (L_{00}, L_{01}, L_{10}, L_{11})$$
$$K_C = K_C \oplus T_C \oplus \tilde{S}_C$$
$$K_C = K_C \oplus T_C \oplus \tilde{S}_C$$

We note that for our achievable scheme,

$$U_k = (K_0, K_1, X^n|L, \tilde{K}_0, \tilde{K}_1)$$
$$V_k = (C, Y^n, \tilde{C}, \tilde{K}_0, \tilde{K}_1)$$
$$W_k = (Z^n, L, \tilde{K}_0, \tilde{K}_1)$$

1) To show that (1) is satisfied for $\{P_n\}_{n \in \mathbb{N}}$, we note that

$$P[K_C \neq K_C] = P[|J| = 0]P[K_C \neq K_C| |J| = 0] + P[|J| = 1]P[K_C \neq K_C| |J| = 1]$$

Since $P_r[|J| = 0] \rightarrow 0$ exponentially fast, it is sufficient to show that $P[K_C \neq K_C| |J| = 1] \rightarrow 0$ as $n \rightarrow \infty$. Now, when Bob does have sufficient erasures and non-erasures, Bob knows $T_C$ since $T_C = X^n|G$. Similarly, Bob knows $\tilde{C}_C$ since $\tilde{S}_C$ is a function of $S_C$ which, in turn, is a function of $X^n|G_S$. Thus, when Bob receives $K_C$ from Alice, Bob learns $K_C$ with zero error. Hence, $P[K_C \neq K_C| |J| = 1] = 0$.

2) To show that (2) is satisfied for $\{P_n\}_{n \in \mathbb{N}}$, we note that

$$I(K_C; V_k, W_k) \leq I(K_C; V_k, W_k, |J|)$$
$$= \sum_{j=0}^{1} P_r[|J| = j] I(K_C; V_k, W_k, |J| = j)$$
$$+ I(K_C; |J|).$$

Since $P_r[|J| = 0] \rightarrow 0$ exponentially fast and $I(K_C; |J|) = 0$, it is sufficient to show that $I(K_C; V_k, W_k, |J| = 1) \rightarrow 0$ as $n \rightarrow \infty$. Now,

$$I(K_C; V_k, W_k| |J| = 1)$$
$$= I(K_C; C, Y^n, Z^n, \tilde{G}, \tilde{L}, \tilde{K}_0, \tilde{K}_1| |J| = 1)$$
$$= I(K_C; C, Y^n, Z^n, \tilde{G}, \tilde{K}_C, \tilde{K}_C| |J| = 1)$$
$$= I(C, \tilde{K}_C, C, Y^n, Z^n, \tilde{G}, \tilde{K}_C, J = 1)$$

[since $K_C$ is indep. of $(C, Y^n, Z^n, \tilde{G}, \tilde{K}_C, J)$]

$$= H(\tilde{K}_C| C, Y^n, Z^n, \tilde{G}, \tilde{K}_C, J = 1)$$

$$= H(\tilde{K}_C| C, Y^n, Z^n, \tilde{G}, \tilde{K}_C, J = 1)$$

[as $T_C, \tilde{S}_C - C, Z^n, \tilde{G} - C, K_C, Y^n$ is a Markov chain conditioned on $J = 1$]

$$= H(\tilde{T}_C| C, Z^n, \tilde{C}, I, J = 1)$$

[as $T_{\tilde{C}, T}$ is uniform over its alphabet]

$$= H(\tilde{T}_C| C, Z^n, \tilde{C}, I, J = 1)$$

[since $X^n|B_S - I$ is a Markov chain conditioned on $J = 1$ and $T_{\tilde{C}, T}$ is uniform over its alphabet]

$$\leq n(1 - \epsilon_2) - \sum_{|i| < nr(1 - \epsilon_2 - \frac{\epsilon_2}{4})} p_I(i)H(\tilde{T}_{C,I}| I = i, J = 1)$$

[using Lemma 10]

$$= nr(1 - \epsilon_2) + \sum_{|i| < nr(1 - \epsilon_2 - \frac{\epsilon_2}{4})} p_I(i)2^{-nr(1 - \epsilon_2 - \frac{\epsilon_2}{4})} - E(|I|)$$

$$= nr(1 - \epsilon_2) + \sum_{|i| < nr(1 - \epsilon_2 - \frac{\epsilon_2}{4})} p_I(i)2^{-nr(1 - \epsilon_2 - \frac{\epsilon_2}{4})} - E(|I|)$$


\[+ \sum_{|i| \geq nr(1-\epsilon_2 - \frac{\epsilon_3}{2})} p_{i}(i) |i| + I(\tilde{S}_{C, I}; Z^n, G_{C, I, J = 1}) \]
\[\leq nr(1-\epsilon_2) + \overline{p}_{n} 2^{-n r(1-\epsilon_2 - \frac{\epsilon_3}{2})} - nr(1-\epsilon_2) + \sum_{|i| \geq nr(1-\epsilon_2 - \frac{\epsilon_3}{2})} p_{i}(i) \cdot nr + I(\tilde{S}_{C, I}; Z^n, G_{C, I, J = 1}) \]
\[p_{n} = Pr(|I| \geq nr(1-\epsilon_2 - \frac{\epsilon_3}{2})), \overline{p}_{n} = 1 - p_{n}, \]
\[p_{n} \rightarrow 0 \text{ exp. as } n \rightarrow \infty \text{ by Lemma } [1] \]
\[= \overline{p}_{n} 2^{-n r(1-\epsilon_2 - \frac{\epsilon_3}{2})} + p_{n} \cdot nr + I(\tilde{S}_{C, I}; Z^n, G_{C, I, J = 1}) \]
\[\leq \overline{p}_{n} 2^{-n r(1-\epsilon_2 - \frac{\epsilon_3}{2})} + p_{n} \cdot nr + I(\tilde{S}_{C, I}; Z^n, G_{C, I, J = 1}) \]
\[= \overline{p}_{n} 2^{-n r(1-\epsilon_2 - \frac{\epsilon_3}{2})} + p_{n} \cdot nr + I(\tilde{S}_{C, I}; Z^n, G_{C, I, J = 1}) \]
\[\text{[since } I \text{ is indep. of (} \tilde{S}_{C, I} \text{), conditioned on } J = 1] \]
\[= \overline{p}_{n} 2^{-n r(1-\epsilon_2 - \frac{\epsilon_3}{2})} + p_{n} \cdot nr + I(\tilde{S}_{C, I}; Z^n, G_{C, I, J = 1}) \]
\[= \overline{p}_{n} 2^{-n r(1-\epsilon_2 - \frac{\epsilon_3}{2})} + p_{n} \cdot nr + I(\tilde{S}_{C, I}; Z^n, G_{C, I, J = 1}) \]
\[= \overline{p}_{n} 2^{-n r(1-\epsilon_2 - \frac{\epsilon_3}{2})} + p_{n} \cdot nr + I(\tilde{S}_{C, I}; Z^n, G_{C, I, J = 1}) \]
\[= \overline{p}_{n} 2^{-n r(1-\epsilon_2 - \frac{\epsilon_3}{2})} + p_{n} \cdot nr + I(\tilde{S}_{C, I}; Z^n, G_{C, I, J = 1}) \]
\[= \overline{p}_{n} 2^{-n r(1-\epsilon_2 - \frac{\epsilon_3}{2})} + p_{n} \cdot nr + I(\tilde{S}_{C, I}; Z^n, G_{C, I, J = 1}) \]
\[\text{[since } (K_{0}, K_{1}) \text{ is indep. of (} C, X^n, L \text{),} \]
\[= H(\tilde{L}|X^n, J = 1) - H(\tilde{L}|X^n, C, J = 1) \]
\[= H(\tilde{L}|J = 1) - H(\tilde{L}|C, J = 1) \]
\[= H(\tilde{L}|J = 1) - H(\tilde{L}|C, J = 1) \]
\[\text{[since } X^n \text{ is indep. of (} \tilde{L}, J \text{),} \]
\[= H(\tilde{L}|J = 1) - H(\tilde{L}|C, J = 1) \]
\[\text{[since } C \text{ is indep. of (} \tilde{L}, J \text{)]} \]
\[= 0 \]
\[4) \text{ To show that eqn. (4) is satisfied for } \{P_{n}\}_{n \in \mathbb{N}} \text{, we will use the proofs already seen for Part (2) and Part (3), as follows:} \]
\[I(K_{0}, K_{1}, C; W_{k}) \]
\[= I(K_{0}, K_{1}; W_{k}|C) + I(C; W_{k}) \]
\[= I(K_{C}, K_{\tilde{C}}; C, Z^n, L, K_{0}, K_{1}|C) + I(C; W_{k}) \]
\[= I(K_{C}, K_{\tilde{C}}; \tilde{C}, K_{C}, Z^n, L) + I(C; W_{k}) \]
\[\text{[since } (K_{C}, K_{\tilde{C}}) \text{ is indep. of (} Z^n, L \text{),} \]
\[= I(K_{C}, \tilde{K}_{C}; C, Z^n, L) + I(C; W_{k}) \]
\[= I(K_{C}, \tilde{K}_{C}; C, Z^n, L, K_{0}, K_{1}) + I(C; W_{k}) \]
\[= I(K_{C}, \tilde{K}_{C}; C, Z^n, L, K_{0}, K_{1}) + I(C; W_{k}) \]
\[+ I(K_{C}, T_{C} \oplus \tilde{S}_{C}; C, Z^n, L, K_{C}, \tilde{K}_{C}) + I(C; W_{k}) \]
\[\text{[since } \tilde{K}_{C} \text{ is indep. of (} C, Z^n, L, \tilde{C}, K_{C}) \]
\[= I(K_{C}, \tilde{K}_{C}; C, Z^n, L) + I(K_{C}, \tilde{K}_{C}; C, Z^n, L, \tilde{K}_{C}) + I(C; W_{k}) \]
\[+ I(C; W_{k}) \]
\[\text{[since } T_{C}, \tilde{S}_{C} - C, Z^n, L - K_{C}, \tilde{K}_{C}, T_{C}, \tilde{S}_{C} \]
\[\text{is a Markov chain] \]
\[= I(K_{C}, \tilde{K}_{C}; C, Z^n, L) + I(K_{C}, \tilde{K}_{C}; C, Z^n, L, \tilde{K}_{C}) \]
\[+ I(C; W_{k}) \]
\[\text{[since } K_{C} \text{ is indep. of (} C, Z^n, L, \tilde{K}_{C}, K_{C}) \]

The first two terms above go to zero following the exact same arguments as in the proof of Part (2). The last term above goes to zero as a consequence of the proof of Part (3).

B. Protocol for achieving any 1-private rate \( r < C_{1P} \)

The difference in this protocol, compared to Protocol [1], is in the way the set \( B_{S} \) is chosen.

- \( \epsilon_1 < \frac{r}{2} \): Bob chooses \( B_{S} \) randomly out of leftover unerased indices and, thus, fully knows the corresponding secret key.
- \( \frac{r}{2} \leq \epsilon_1 < \frac{1}{2} \): Bob chooses \( B_{S} \) randomly out of all indices left after creating \( G, B \) and \( G_{S} \) and may know the corresponding secret key partially.
• \( \epsilon_1 \geq \frac{1}{2} \): Bob chooses \( B_S \) randomly out of leftover erased indices and knows nothing about the corresponding secret key.

Just as in Lemma 2 we can show that for a suitably low \( \delta \) and sufficiently large \( n \), Bob will have enough erased and unerased \( Y_i \)'s with which to run the protocol and achieve any rate \( r < C_{1p} \).

**Lemma 4:** Any \( r < C_{1p} \) is an achievable 1-private rate.

The proof of this lemma is similar to the proof of Lemma 3.

IV. PROOF OF CONVERSE

The converses hold even under a weaker sense of security where conditions (2), (4), (6), and (8) hold only with a \( \frac{1}{n} \) factor on the left-hand-side.

**Lemma 5:** For the setup of Figure 2

\[
C_{2p} \leq \epsilon_2 \cdot \min \{ \epsilon_1, 1 - \epsilon_1 \}
\]

Proof: We first state a general upperbound on \( C_{2p} \): For the setup of Figure 1

\[
C_{2p} \leq \min \left\{ \max_{p_X} I(X;Y|Z), \max_{p_X} H(X|Y, Z) \right\}.
\]  
(1)

\( C_{2p} \leq \max_{p_X} I(X;Y|Z) \) follows from the observation that operating the protocol with Bob setting \( C = 0 \) allows Alice and Bob to agree on the secret key \( K_0 \) which is secret from Eve. Since \( \max_{p_X} I(X;Y|Z) \) is an upperbound on secret key capacity of the broadcast channel \( p_Y;Z|X \) (with public discussion) [2], the bound follows.

It is easy to verify that the 2-private protocol can be viewed as a (two-party) OT protocol between the parties Alice and Bob-Eve (combined). Hence, by invoking an outerbound on OT capacity in [1], we have \( C_{2p} \leq \max_{p_X} H(X|Y, Z) \). Evaluating these upper bounds in (1) for the specific setup in Figure 2

\[
C_{2p} \leq \max_{p_X} I(X;Y|Z) = \epsilon_2 (1 - \epsilon_1),
\]

\[
C_{2p} \leq \max_{p_X} H(X|Y, Z) = \epsilon_2 \epsilon_1.
\]  

**Lemma 6:** For the setup of Figure 2

\[
C_{1p} \leq \min \left\{ \epsilon_1, \frac{\epsilon_2}{2}, \epsilon_2 (1 - \epsilon_1) \right\}
\]

Proof: We first show that \( C_{1p} \leq \min \{ \epsilon_1, \epsilon_2 (1 - \epsilon_1) \} \) by means of the following more general statement: For the setup of Figure 1

\[
C_{1p} \leq \left\{ \max_{p_X} I(X;Y|Z), \max_{p_X} H(X|Y) \right\}.
\]  
(2)

Proof of \( C_{1p} \leq \max_{p_X} I(X;Y|Z) \) is identical to the one for 2-private case (3), \( C_{1p} \leq \max_{p_X} H(X|Y) \) follows from observing that a 1-private protocol is also a protocol for OT between Alice and Bob over the channel \( p_Y|X \) for which \( \max_{p_X} H(X|Y) \) is an upperbound on OT capacity [1]. Evaluating (2) for the specific setup in Figure 2

\[
C_{1p} \leq \max_{p_X} H(X|Y) = \epsilon_1.
\]

$$C_{1p} \leq \max_{p_X} I(X;Y|Z) = \epsilon_2 (1 - \epsilon_1).$$

It only remains to show that \( C_{1p} \leq \frac{\epsilon_2}{2} \). For this, we need the following lemma which states that \( (X^n, F^k) \) must together carry nearly all the information about \( (K_0, K_1) \).

**Lemma 7:** \( \frac{1}{n} H(K_0, K_1|X^n, F^k) \rightarrow 0 \) as \( n \rightarrow \infty \).

The proof is deferred to the appendix. The lemma can be interpreted as follows: Bob’s privacy against Alice (eqn. 7) implies that Alice is unaware of which string is required by Bob. This forces that both the strings be decodable from observing the interface of Alice to the system (i.e. observing \( (X^n, F^k) \)). If this were not the case and \( K_0, K_1 \), say, could not be fully decoded from \( (X^n, F^k) \), then Alice can infer that Bob wanted \( K_1 \) (i.e., \( C = 1 \)) violating the requirement of (7).

To convert this into an upperbound on the rate, intuitively, Eve has access to all of \( (X^n, F^k) \) except those bits of \( X^n \) erased by her channel. Since the erased fraction of bits is about \( \epsilon_2 \), and we require both strings to be secret from Eve, each string has a rate of at most \( \epsilon_2/2 \). We make this argument more formally below. Let \( I = \{ i_1, \ldots, i_n \} \) be the instances where the channel is used and the (random) set of indices at which Eve saw erasures be \( E' := \{ i \in I : Z_i \text{ erasure} \} \). Let \( e' \) denote a realization of \( E' \) and \( \bar{e'} = I \setminus e' \) its complement.

\[
2m = H(K_0, K_1) = I(K_0, K_1; X^n, F^k) + H(K_0, K_1|X^n, F^k)
\]
\( \overset{(a)}{=} I(K_0, K_1; X^n, F^k) + o(n) \)
\( \overset{(b)}{=} I(K_0, K_1; X^n, F^k|E') + o(n) \)
\( = \sum_{e' \subseteq I} p_{E'}(e') I(K_0, K_1; X^n, F^k|E' = e') + o(n) \)
\( = \sum_{e' \subseteq I} p_{E'}(e') I(K_0, K_1; X^n|\bar{e'}, F^k, E' = e') + o(n) \)
\( \leq \sum_{e' \subseteq I} p_{E'}(e') I(K_0, K_1; X^n|\bar{e'}, F^k, E' = e') + o(n) \)
\( + \sum_{e' \subseteq I} p_{E'}(e') H(X^n|\bar{e'}, E' = e') + o(n) \)
\( \overset{(c)}{=} n e_2 + o(n) \),

where (a) follows from Lemma 7, (b) from the independence of Eve’s channel, and (c) from (8). Therefore, \( C_{1p} \leq \frac{\epsilon_2}{2} \).

ACKNOWLEDGMENT

The work was supported in part by the Bharti Centre for Communication, IIT Bombay, a grant from the Information Technology Research Academy, Media Lab Asia, to IIT Bombay and TIFR, a grant from the Department of Science and Technology, Government of India, to IIT Bombay, and a Ramanujan Fellowship from the Department of Science and Technology, Government of India, to V. Prabhakaran. S. Diggavi was supported in part by NSF awards 1136174, 1321120 and MURI award AFOSR FA9550-09-064.
We need two lemmas from [11], which are stated here for completeness.

**Lemma 8:** Let $U, V, Z$ denote random variables with values in finite sets $U$, $V$ and $Z$ respectively. Suppose $z_1, z_2 \in Z$ with $P[Z = z_1] = p > 0$ and $P[Z = z_2] = q > 0$. Then,

$$|H(U|V, Z = z_1) - H(U|V, Z = z_2)| \leq 3\sqrt{\frac{(p+q)^2}{2pq} I(UV; Z) \log |U|} + 1.$$

**Proof:** See [11].

**Lemma 9:** $I(K_0, K_1; N, Y^n|X^n, F_k) = 0$.

**Proof:** See [11] or Lemma 2.2 of [2].

Note that (7) and Lemma 8 together imply

$$H(K_0|X^n, F_k, C = 0) - H(K_0|X^n, F_k, C = 1) = o(n),$$

$$H(K_1|X^n, F_k, C = 0) - H(K_1|X^n, F_k, C = 1) = o(n).$$

Multiplying both equations by $\frac{1}{2}$ and subtracting, we get

$$H(K_C|X^n, F_k, C) - H(K_C|X^n, F_k, C) = o(n). \quad (11)$$

**Lemma 9** implies that $I(K_0, K_1; C|X^n, F_k) = 0$. Hence,

$$H(K_0, K_1|X^n, F_k) = H(K_0, K_1|X^n, F_k, C) = H(K_C, K\tilde{C}|X^n, F_k, C, K) = H(K_C|X^n, F_k, C) + H(K_{\tilde{C}}|X^n, F_k, C, K) \leq H(K_C|X^n, F_k, C) + H(K_{\tilde{C}}|X^n, F_k, C).$$

In light of (11), this lemma will be proved if we show either $H(K_C|X^n, F_k, C)$ or $H(K_{\tilde{C}}|X^n, F_k, C)$ to be $o(n)$.

For this we note that Lemma 9 implies

$$I(K_0, K_1; N, Y^n|X^n, F_k, C) = 0.$$

This, in turn, implies that

$$I(K_C, K\tilde{C}; N, Y^n|X^n, F_k, C) = 0.$$

Hence, $I(K_C; N, Y^n|X^n, F_k, C) = 0$. Therefore,

$$H(K_C|X^n, F_k, C) = H(K_C|X^n, F_k, C, N, Y^n) \leq H(K_C|\tilde{K}_C) \leq o(n),$$

where (a) follows from the fact that since $\tilde{K}_C$ is a function of $(C, N, Y^n, F_k)$, and (b) from (5) and Fano’s inequality.

**APPENDIX A**

**A USEFUL LEMMA**

In the following, for $r' < 1$, we consider the construction of a random $(n, nr')$ binary code $C$, generated with i.i.d. $Ber(\frac{1}{2})$ components. For any code $C$, let $X^C$ be a random codeword picked uniformly from the code. For any set $J \subseteq [1:n]$, let $X^C_J$ denote the components of $X^C$ in $J$. $H(X^C_J)$ is the entropy of the vector $X^C_J$. This is a function of the code, and so $H(X^C_J)$ is a random variable under the above random code construction. The following lemma states that for any $r' < r$, $\beta < r' - r$, and $|J| \geq nr$, then with high probability over the code, $H(X^C_J) \geq nr - 2^{-n\beta}$.

**Lemma 10:** Let $r' < 1$, and $C$ be a random $(n, nr')$ binary code generated with i.i.d. $Ber(\frac{1}{2})$ components. Let $X^C_J$ be as defined above. Then for any $\beta$, $0 < \beta < (r'-r)$, with high probability, the code satisfies the following property: for any set $J \subseteq [1:n]$ with $|J| \geq nr$, $H(X^C_J) \geq nr - 2^{-n\beta}$.

**Proof:** Wlog, let us assume $|J| = nr$. Let the $N = 2^{nr}$ random codewords be denoted by $X_i; i = 1, 2, \ldots, N$. Let us denote the codeword components in $J$ by $Y_i := X_i|_J$. By assumption, clearly $Y_i$ are independent and uniformly distributed over the $2^{nr'}$ binary strings in $\{0,1\}^{nr'}$. Let us denote the empirical distribution of $Y_i; i = 1, 2, \ldots, N$ as $\hat{p}_J$. We are interested in the entropy $H(\hat{p}_J)$.

By Sanov’s theorem,

$$Pr[H(\hat{p}_J) < nr - 2^{-n\beta}] \leq (N+1)^{2^{nr} - 2^{ND(p^*||u)}}$$

where $u$ denotes the uniform distribution over $\{0,1\}^{nr}$, and

$$p^* = \arg\min_{p: H(p) < nr - 2^{-n\beta}} D(p||u).$$

Clearly,

$$D(p^*||u) = nr - H(p^*) > 2^{-n\beta}.$$

So

$$Pr[H(\hat{p}_J) < nr - 2^{-n\beta}] < (2^{nr'} + 1)^{2^{nr} - 2^{nr'} - 2^{-n\beta}} < 2^{n(r'-1/n)} - 2^{nr'} - 2^{-n\beta} \leq 2^{-2nr'(2^{n(r'-r-\beta)} - n(r'+1/n))}.$$
By union bound,
\[ \Pr[H(p_J) < nr - 2^{-n\beta} \text{ for some } J] \]
\[ \leq \left( \frac{n}{nr} \right) 2^{-2^n r (2^{n(r' - r - \beta)} - n(r' + 1/n))} \]
\[ \leq 2^{nH(r')} \cdot 2^{-2^n r (2^{n(r' - r - \beta)} - n(r' + 1/n))}. \]

Since \( \beta < r' - r \), the above upper bound goes to zero as \( n \to \infty \).