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., [3, 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 charaterization 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 setp 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 $p_{YZ|X}$. 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 pulic 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 public channel at instances $\{1, \ldots, k\} \backslash \{i_1, i_2, .., i_n\}$ and takes the following steps :

1) At the begining of the protocol, Alice and Bob generate private random variables M, N respectively,

978-1-4799-5186-4/14/$31.00 ©2014 IEEE

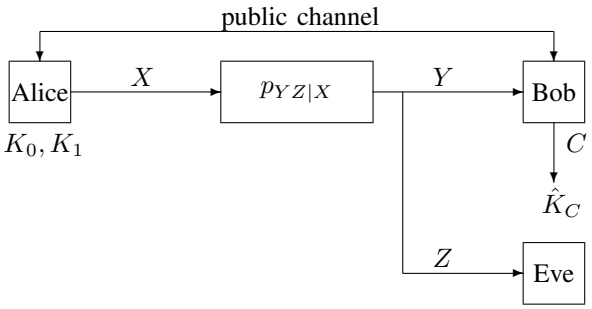

Fig. 1. Setup for obtaining Oblivious Transfer.

which are independent of each other and all other system variables available.

2) $i \notin \{i_1, i_2, .., i_n\}$: $F_i = F_i(K_0, K_1, M, F^{i-1})$ is the public message from Alice, if Alice is the one initiating a public message at time i.
3) $i < i_1$: $F_i = F_i(C, N, F^{i-1})$ is the public message from Bob, if Bob is the one initiating a public message at time i.
4) $i = i_j$: $X_j = X_j(K_0, K_1, M, F^{i-1})$, $F_i = \emptyset$.
5) $i_j < i < i_{j+1}$: $F_i = F_i(C, N, F^{i-1}, Y^j)$ is the public message from Bob, if Bob is the one initiating a public message at time i.

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,

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

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 $\frac{m}{n} \longrightarrow R_{2P}$ as $n \longrightarrow \infty$, such that

$$P[\hat{K}_C \neq K_C] \longrightarrow 0, \quad (1)$$
$$I(K_{\overline{C}}; V_k, W_k) \longrightarrow 0, \quad (2)$$
$$I(C; U_k, W_k) \longrightarrow 0, \quad (3)$$
$$I(K_0, K_1, C; W_k) \longrightarrow 0, \quad (4)$$

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 $\frac{m}{n} \longrightarrow R_{1P}$ as $n \longrightarrow \infty$, such that

$$P[\hat{K}_C \neq K_C] \longrightarrow 0, \quad (5)$$
$$I(K_{\overline{C}}; V_k) \longrightarrow 0, \quad (6)$$
$$I(C; U_k) \longrightarrow 0, \quad (7)$$
$$I(K_0, K_1, C; W_k) \longrightarrow 0, \quad (8)$$

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 ϵ_1 (BEC(ϵ_1)) connects Alice to Bob and a BEC(ϵ_2) connects Alice to Eve. BEC(ϵ_1) acts independently of BEC(ϵ_2) and no assumption is made on the relative values of ϵ_1 and ϵ_2.

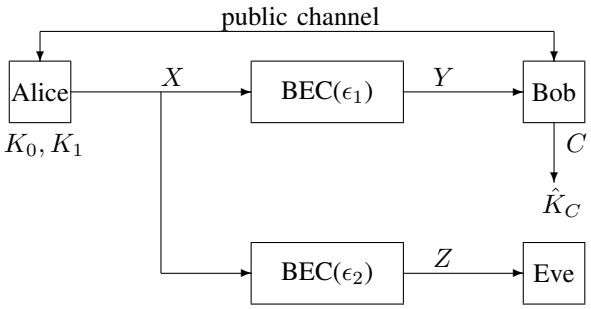

Fig. 2. Setup with the broadcast channel made up of two independent BECs.

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:

$$C_{1P} = \begin{cases} \epsilon_1, & \epsilon_1 < \frac{\epsilon_2}{2} \\ \frac{\epsilon_2}{2}, & \frac{\epsilon_2}{2} \leq \epsilon_1 < \frac{1}{2} \\ \epsilon_2(1 - \epsilon_1), & \epsilon_1 \geq \frac{1}{2} \end{cases}$$

III. Proof of Achievability

We begin by briefly reviewing the achievable protocol for a BEC(ϵ_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 *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 $K_1 \oplus T_1$ to Bob over the public channel. Since Bob knows T_C, he can obtain K_C. It is easy to verify that Alice obtains no information about C and Bob obtains no information about the $K_{\overline{C}}$.

In the setup of Figure 2, privacy against Eve is additionally required. Let us consider the case of 2-privacy first. In the above scheme, Eve will learn approximately a fraction $1 - \epsilon_2$ of both the OT keys T_0 and T_1. Hence, Alice must additionally protect both the strings before sending them over the public

channel. This will be accomplished by setting up additional secret keys (independent of T_0, T_1) which are secret from Eve as follows: 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 $\tilde{S}_0, \tilde{S}_1$ respectively (each of length m bits), using a binary code (obtained using random coding argument) of rate about $(1-\epsilon_2)$. Alice sends $K_0 \oplus T_0 \oplus \tilde{S}_0$ and $K_1 \oplus T_1 \oplus \tilde{S}_1$ 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. $I(S_i; W_k) \longrightarrow 0$ as $n \longrightarrow \infty$, $i = 1, 2$), at rate ϵ_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 $\frac{m(1-\epsilon_2)}{\epsilon_2}$ 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 $E, \overline{E}, E'$ be, respectively, the set of indices where Bob sees erasures, Bob sees non-erasures, and Eve sees erasures.

$$E := \{i \in \{i_1, \ldots, i_n\} : Y_i = \text{erasure}\},$$
$$\overline{E} := \{i \in \{i_1, \ldots, i_n\} : Y_i \neq \text{erasure}\},$$
$$E' := \{i \in \{i_1, \ldots, i_n\} : Z_i = \text{erasure}\}.$$

Let $\mathbb{U}(A)$ 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:

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

Proof: The claim follows from Chernoff bound. ∎

The following lemma says that for any rate $r < C_{2P}$ and a suitably low δ (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 $\delta < (1 - \frac{r}{C_{2P}})$. Then

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

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, δ (suitably low, as per Lemma 2), $\tilde{\epsilon}_2$, a binary $(nr, nr(1-\tilde{\epsilon}_2))$-code Λ_{nr} chosen via a random coding argument

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

Bob Receives the Y^n from BEC(ϵ_1). Let $r < C_{2P}$. Bob now creates the following sets:

$$G \sim \mathbb{U}\left(\left\{A \subset \overline{E} : |A| = nr\right\}\right),$$
$$G_S \sim \mathbb{U}\left(\left\{A \subset \overline{E}\backslash G : |A| = \frac{nr(1-\tilde{\epsilon_2})}{\tilde{\epsilon_2}}\right\}\right),$$
$$B \sim \mathbb{U}\left(\{A \subset E : |A| = nr\}\right),$$
$$B_S \sim \mathbb{U}\left(\{A \subset E\backslash B : |A| = |G_S|\}\right).$$

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.

$$\begin{aligned} C = 0: \quad & L_{00} = G, \quad L_{01} = G_S \\ & L_{10} = B, \quad L_{11} = B_S \\ C = 1: \quad & L_{00} = B, \quad L_{01} = B_S \\ & L_{10} = G, \quad L_{11} = G_S \end{aligned}$$

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

Alice computes the following keys

$$T_0 = X^n|_{L_{00}},$$
$$T_1 = X^n|_{L_{10}}.$$

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 $nr(1-\tilde{\epsilon}_2)$ 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 it can get K_C.

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

A formal proof of this lemma is given in an extended version available at arXiv.org. A sketch of the proof is as follows. A sequence of instances $\{P_n\}_{n\in\mathbb{N}}$ of Protocol 1 will be used. For $\{P_n\}_{n\in\mathbb{N}}$,

1) (1) is satisfied since, whenever the protocol succeeds (which happens with high probability by Lemma 2), Bob recovers K_C.
2) In the protocol, $K_{\overline{C}}$ is encrypted using $T_{\overline{C}} \oplus \tilde{S}_{\overline{C}}$ (all are strings of length nr bits). (2) is satisfied because for a colluding Bob and Eve, the uncertainty of $T_{\overline{C}} \oplus \tilde{S}_{\overline{C}}$ differs from nr by a term that can be made arbitrarily small by choosing suffiiciently large n and suitably small δ.
3) Alice and Eve can learn about C only from the sets of indices Bob sends. (3) holds since erasures are independent across indices and the sets G, G_S and B, B_S are formed by uniformly picking out indices from the unerased and erased locations respectively. Morover, $|G| = |B|$ and $|G_S| = |B_S|$.
4) (4) is satisfied for the following two reasons. Eve obtains no information about C for the same reason as Alice learning nothing about C. Additionally, conditioned on C, Eve will learn very little of (K_0, K_1). More precisely, for Eve, the uncertainty of $(T_0 \oplus \tilde{S}_0, T_1 \oplus \tilde{S}_1)$ differs from $2nr$ by a term that can be made arbitrarily small by choosing suffiiciently large n and suitably small δ.

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.

- $\epsilon_1 < \frac{\epsilon_2}{2}$: Bob chooses B_S randomly out of leftover unerased indices and, thus, fully knows the corresponding secret key.
- $\frac{\epsilon_2}{2} \leq \epsilon_1 < \frac{1}{2}$: 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 δ 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,

$$C_{2P} \leq \min\left\{\max_{p_X} I(X;Y|Z), \max_{p_X} H(X|Y,Z)\right\}. \quad (9)$$

$C_{2P} \leq \max_{p_X} I(X;Y|Z)$ 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 (9) 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,

$$C_{1P} \leq \min\left\{\epsilon_1, \quad \frac{\epsilon_2}{2}, \quad \epsilon_2(1-\epsilon_1)\right\}$$

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,

$$C_{1P} \leq \left\{\max_{p_X} I(X;Y|Z), \max_{p_X} H(X|Y)\right\}. \quad (10)$$

Proof of $C_{1P} \leq \max_{p_X} I(X;Y|Z)$ is identical to the one for 2-private case (9). $C_{1P} \leq \max_{p_X} H(X|Y)$ 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 (10) 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: $\frac{1}{n} H(K_0, K_1 | X^n, F^k) \longrightarrow 0$ as $n \longrightarrow \infty$.

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 the interface of Alice to the system (i.e. observing (X^n, F^k)). If this were not the case and K_0, 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 ϵ_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 $\overline{e}' = I \backslash e'$ its complement.

$$\begin{aligned}
2m &= H(K_0, K_1) \\
&= I(K_0, K_1; X^n, F^k) + H(K_0, K_1 | X^n, F^k) \\
&\overset{(a)}{=} I(K_0, K_1; X^n, F^k) + o(n) \\
&\overset{(b)}{=} I(K_0, K_1; X^n, F^k | E') + o(n) \\
&= \sum_{e' \subseteq I} p_{E'}(e') I(K_0, K_1; X^n, F^k | E' = e') + o(n) \\
&= \sum_{e' \subseteq I} p_{E'}(e') I(K_0, K_1; X^n|_{\overline{e}'}, F^k | E' = e') + o(n) \\
&\quad + \sum_{e' \subseteq I} p_{E'}(e') I(K_0, K_1; X^n|_{e'} | X^n|_{\overline{e}'}, F^k, E' = e') \\
&\leq \sum_{e' \subseteq I} p_{E'}(e') I(K_0, K_1; X^n|_{\overline{e}'}, F^k | E' = e') \\
&\quad + \sum_{e' \subseteq I} p_{E'}(e') H(X^n|_{e'} | E' = e') + o(n) \\
&= I(K_0, K_1; Z^n, F^k) + n\epsilon_2 + o(n) \\
&\overset{(c)}{=} n\epsilon_2 + o(n),
\end{aligned}$$

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.

REFERENCES

[1] R. Ahlswede, I. Csiszár, "On oblivious transfer capacity", *Information Theory, Combinatorics and Search Theory*, Springer Berlin Heidelberg, pp. 145–166, 2013.

[2] R. Ahlswede, I. Csiszár, "Common randomness in information theory and cryptography part I: secret sharing", *IEEE Transactions on Information Theory*, vol. 39, No. 4, pp. 1121–1132, July 1993.

[3] R. Cramer, I. Damgård, J. B. Nielsen, *Secure Multiparty Computation and Secret Sharing - An Information Theoretic Approach*, Online. `http://www.daimi.au.dk/~ivan/MPCbook.pdf`

[4] C. Crépeau, J. Kilian, "Achieving oblivious transfer using weakened security assumptions", *29th Symposium on Foundations of Computer Science*, pp. 42-52, 1988.

[5] J. Kilian, "Founding cryptography on oblivious transfer", *20th Symposium on Theory of Computing*, pp. 20–31, 1988

[6] J. Kilian, "More general completeness theorems for secure two-party computation", *Symposium on Theory of Computing*, pp. 316–324, 2000.

[7] E. Kushilevitz, "Privacy and communication complexity", *SIAM Journal on Discrete Mathematics*, vol. 5, No. 2, pp. 273–284, 1992.

[8] A.C.A. Nascimento, A. Winter, "On the oblivious-transfer capacity of noisy resources", *IEEE Transactions on Information Theory*, vol.54, No.6, pp. 2572–2581, 2008.

[9] A.C. Pinto, R. Dowsley, K. Morozov, A.C.A. Nascimento, "Achieving oblivious transfer capacity of generalized erasure channels in the malicious model", *IEEE Transactions on Information Theory*, vol. 57, No. 8, pp. 5566–5571, 2011.

[10] U. Maurer, S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," *Advances in CryptologyEUROCRYPT 2000*, pp. 351368, Springer, 2000.

APPENDIX A
PROOF OF LEMMA 7

We need two lemmas from [1], which are stated here for completeness.

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

$$\begin{aligned}
&|H(U|V, Z = z_1) - H(U|V, Z = z_2)| \\
&\qquad \leq 3\sqrt{\frac{(p+q)\ln 2}{2pq} I(UV; Z) log|\mathcal{U}|} + 1.
\end{aligned}$$

Proof: See [1]. ■

Lemma 9: $I(K_0, K_1, M; C, N, Y^n | X^n, F^k) = 0$.

Proof: See [1] or Lemma 2.2 of [2]. ■

Note that (7) and Lemma 8 together imply

$$\begin{aligned}
H(K_0|X^n, F^k, C = 0) - H(K_0|X^n, F^k, C = 1) &= o(n), \\
H(K_1|X^n, F^k, C = 0) - H(K_1|X^n, F^k, C = 1) &= o(n).
\end{aligned}$$

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

$$H(K_C|X^n, F^k, C) - H(K_{\overline{C}}|X^n, F^k, C) = o(n). \quad (11)$$

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

$$\begin{aligned}
&H(K_0, K_1|X^n, F^k) \\
&\qquad = H(K_0, K_1|X^n, F^k, C) \\
&\qquad = H(K_C, K_{\overline{C}}|X^n, F^k, C) \\
&\qquad = H(K_C|X^n, F^k, C) + H(K_{\overline{C}}|X^n, F^k, C, K_C) \\
&\qquad \leq H(K_C|X^n, F^k, C) + H(K_{\overline{C}}|X^n, F^k, C).
\end{aligned}$$

In light of (11), this lemma will be proved if we show either $H(K_C|X^n, F^k, C)$ or $H(K_{\overline{C}}|X^n, F^k, C)$ 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

$$I(K_C, K_{\overline{C}}; N, Y^n | X^n, F^k, C) = 0.$$

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

$$\begin{aligned}
H(K_C|X^n, F^k, C) &= H(K_C|X^n, F^k, C, N, Y^n) \\
&\overset{(a)}{=} H(K_C|X^n, F^k, C, N, Y^n, \hat{K}_C) \\
&\leq H(K_C|\hat{K}_C) \\
&\overset{(b)}{=} o(n),
\end{aligned}$$

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