A New Upperbound for the Oblivious Transfer Capacity of Discrete Memoryless Channels

K. Sankeerth Rao
Department of Electrical Engineering
Indian Institute of Technology, Bombay
Mumbai, India
Email: sankeerth1729@gmail.com

Vinod M. Prabhakaran
School of Technology and Computer Science
Tata Institute of Fundamental Research
Mumbai, India
Email: vinodmp@tifr.res.in

Abstract—We derive a new upper bound on the string oblivious transfer capacity of discrete memoryless channels (DMC). The main tool we use is the tension region of a pair of random variables introduced in Prabhakaran and Prabhakaran (2014) where it was used to derive upper bounds on rates of secure sampling in the source model. In this paper, we consider secure computation of string oblivious transfer in the channel model. Our bound is based on a monotonicity property of the tension region in the channel model. We show that our bound strictly improves upon the upper bound of Ahlswede and Csiszár (2013).

I. INTRODUCTION

The goal of secure function computation is for users in a network to compute functions of their collective data in such a way that users do not learn any additional information about the data than the output of the functions they are computing. This forms a central theme of modern cryptography under the rubric of Secure Multiparty Computation.

In general, information theoretically secure function computation between two users, who are equipped only with private/common randomness and noiseless communication channels between them, is infeasible except for a class of essentially trivial functions [10]. However, Crépeau and Kilian showed that any function may be computed information theoretically securely if a (nontrivial) noisy channel is available from one of the users to the other [4]. The approach was to show that a certain primitive secure computation called *oblivious transfer* (OT) [16] is feasible given such a noisy channel resource, and then rely on a reduction of of two-party computation to OT by Kilian [9].

OT (more specifically, 1-out-of-2 m-string OT) is the following secure function computation between two users, say, Alice and Bob: Alice is given 2 strings S_0, S_1 picked independently and identically uniformly distributed from $\{0,1\}^m$, Bob is given a uniform binary bit K, independent of S_0, S_1. Alice is required to produce no output and Bob should output S_K. Furthermore, Alice should not learn any information about K and Bob should not learn anything about the string $S_{\bar{K}}$, where $\bar{K} = K + 1 \mod 2$. As must be clear from the discussion above, OT cannot be securely computed when Alice and Bob only have access to noise-free communication channels and private/common randomness.

Motivated by its role in secure computation, several works have addressed the rate at which OT can be obtained from a discrete memoryless channel (DMC). In [12], OT capacity of a DMC was defined as the largest rate of m-over-n, where n is the number of channel uses, achievable when Bob recovers S_K with vanishing probability of error and under vanishing information leakage measured via conditional mutual informations. The paper also characterized noisy resources which provide a strictly positive OT capacity. The OT capacity of erasure channels was obtained in [7] for the honest-but-curious setting, where the users follow the protocol faithfully, but attempt to derive information they are not allowed to know from everything they have access to at the end of the protocol. Ahlswede and Csiszár [1] characterized the OT capacity for a more general class of channels called the generalized erasure channels. In [13], it was shown that the OT capacity of generalized erasure channels remain the same even when the users are allowed to be malicious. The best known upper bounds on the OT capacity of DMCs are due to Ahlswede and Csiszár [1][1]. These bounds, which apply for the case of honest-but-curious users (and therefore, also for malicious users), were obtained by weakening the problem of obtaining OT from a DMC to a secret key agreement problem. In this paper we strictly improve upon these bounds.

The main tool we use is the *tension region* $\mathfrak{T}(U; V)$ of a pair of random variables U, V introduced in [15]. Defined as the increasing hull of the set of all $(I(V; Q|U), I(U; Q|V), I(U; V|Q))$, where Q is some random variables jointly distributed with U, V, it has the interpretation as a rate-information tradeoff region for a distributed common randomness generation problem which generalizes the setting of Gács and Körner [5]. Specifically, consider a genie who has access to $U^n, V^n \sim p(u, v)$ i.i.d., who needs to communicate to a user with only U^n and separately to a user with only V^n such that two users may agree (with vanishing probability of error) on a common random variable W. The "quality" is measured by how small the average "residual information" $I(U^n; V^n|W)/n$ is. It was shown in [15] that the trade-off between the two rates of communication from the genie to

---

[1] The same upper bounds can be inferred from an earlier work by Wolf and Wullschleger [17] for the case of zero-error and perfect privacy.

the users and the quality of the common random variable agreed by the users is given by the tension region.

In [15], properties of tension region were used to derive upper bounds on the rate of a form of secure computation with no inputs, but randomized outputs, called *secure sampling* for the *source model*, i.e., the "noisy" resource available to the two users are observations from a distributed source (rather than a noisy channel as here), and the goal of the secure computation is to produce samples of another distributed source in such a way that neither user can infer any more information about each other's output than can be inferred from their own outputs[2]. The upper bound technique was a monotonicity result for secure sampling protocols which implies that the tension region of the outputs must contain the tension region of the distributed source samples.

In contrast, this paper deals with the *channel model*. The main technical contributions include a version of the monotonicity result for the channel model. It turns out that, unlike in the source model, the whole tension region does not satisfy a useful (i.e., single-letterizable) mononticity property, but its restriction to the $I(V; Q|U) = 0$ plane does. Specifically, we show that the restricted tension region of the inputs-and-outputs of the function being securely computed must contain the (Minkowski) sum of the restricted tension regions of the input and output of the DMC at each channel use. We turn this into an upper bound on the OT capacity by characterizing the restricted tension region of the inputs-and-outputs of the OT function. In the interest of space, we only present the argument required to obtain our upper bound on OT capacity in this paper. The more general monotonicity result is deferred to a full-length version.
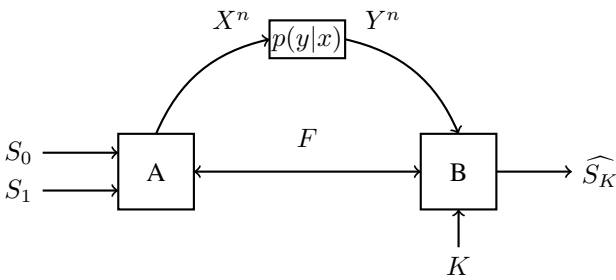
II. PROBLEM STATEMENT

Fig. 1. String Oblivious Transfer

Consider the setup in Fig. 1. Alice's data are two strings S_0, S_1 chosen independently and uniformly from $\{0,1\}^m$. Bob's data is a uniform bit $K \in \{0,1\}$ independent of S_0, S_1. The goal is for Bob to learn S_K. We require that neither user learn any (significant) amount of additional information about the other's data apart from Bob learning

S_K. They have access to unlimited amounts of private randomness (i.e., randomness independent of each other and of the data) and a noiseless discussion channel. There is also a DMC from Alice to Bob: $p(y|x)$ where $x \in \mathcal{X}$, the input alphabet, and $y \in \mathcal{Y}$, the output alphabet. Before each instance of using the DMC and after the last use of the DMC, Alice and Bob may exchange messages with each other over the noiseless discussion channel, potentially over multiple rounds. There are no constraints on the number of rounds of message exchange they may engage in over the discussion channel except that it be finite with probability 1. We assume that the users are honest-but-curious.

Definition 1. *Alice and Bob are said to have followed an* (n, m, ϵ) *secure protocol if, the strings S_0 and S_1 input to Alice have length m each (as above), the protocol makes n uses of the DMC, and at the end of the protocol, Bob can output $\widehat{S_K}$ which agrees with S_K with probability at least $1 - \epsilon$, and if the transcript F of the messages exchanged on the discussion channel and the inputs X^n and outputs Y^n of the DMC satisfy the following privacy constraints[3]:*

$$I(F, X^n; K|S_0, S_1) \leq \epsilon, \tag{1}$$

$$I(F, Y^n; S_{\bar{K}}|K) \leq n\epsilon. \tag{2}$$

Notice that (1) guarantees Bob's privacy against Alice, and (2) guarantees privacy for Alice against Bob.

Definition 2. *A rate R is said to be* achievable *if there is a sequence of (n, nR, ϵ_n) secure protocols such that $\epsilon_n \to 0$ as $n \to \infty$. The supremum of all achievable rates is the OT capacity, C, of the DMC.*

Our main result is the following upper bound on OT capacity.

Theorem 1.

$$C \leq \max_{p(x)} \min_{Q-X-Y} I(X; Q|Y) + I(X; Y|Q), \tag{3}$$

where the the minimization is over random variables Q jointly distributed with X, Y satisfying the Markov chain constraint $Q - X - Y$ and the cardinality bound $|\mathcal{Q}| \leq |\mathcal{X}||\mathcal{Y}| + 2$.

The currently best known upper bound is due to Ahlswede and Csiszár [1]:

$$C \leq \max_{p(x)} \min(I(X; Y), H(X|Y)). \tag{4}$$

It is easy to see that Theorem 1 subsumes this. For a fixed $p(x)$ in (3), notice that choosing $Q = \emptyset$ gives the bound $I(X; Y)$, and choosing $Q = X$ gives the bound $H(X|Y)$. We shall show in Section IV that our bound is a strict improvement on (4).

---

[2]In fact, it is easy to show that secure computation of OT is equivalent to secure sampling of the distribution: $A = (W_0, W_1)$ by Alice and $B = (J, W_J)$ by Bob, where $W_0, W_1 \in \{0,1\}^m$ and $J \in \{0,1\}$ indepedent and uniform. Hence, the results in [15] can be used to derive bounds on OT capacity of discrete memoryless sources. Using a lemma of this paper, we give explicit bounds in Section V.

[3]Notice that we do not need to explicitly bring in the private random variables in defining the privacy conditions since, conditioned F, X^n, S_0, S_1, Alice's private randomness is independent of K and, similarly, conditioned on F, Y^n, K, Bob's private randomness is independent of S_0, S_1.

III. Proof of Theorem 1

Consider an (n, nR, ϵ) secure protocol, let all the random variables that Alice has access to *after* the i-th usage of the DMC be called the *view* of Alice at the i-th stage and be represented by U_i, $i = 0, 1, 2, \ldots, n$, where U_0 denotes Alice's view at the beginning of the protocol, i.e., U_0 is made up of S_0, S_1, and the private randomness of Alice. Similarly, we define the view of Bob till the i-th stage and denote it by V_i. Let U_{final} and V_{final} be the views of Alice and Bob at the termination of the protocol (after Bob outputs). U_{final} consists of S_0, S_1, the transcript F of the discussion over the noisefree channel, the inputs X^n to the DMC and Alice's private randomness. Similarly, V_{final} comprises $K, F, Y^n, \widehat{S}_K$, and Bob's private randomness.

For a pair of jointly distributed random variables U, V, let us define the function $\alpha(U; V)$

$$\alpha(U; V) := \min_{Q - U - V} I(U; Q|V) + I(U; V|Q). \quad (5)$$

This is closely related to the tension region $\mathfrak{T}(U; V)$ of a pair of random variables U, V of [15]. We recall from there the definition of $\mathfrak{T}(U; V)$:

$$\mathfrak{T}(U; V) = i\Big(\Big\{ \big(I(V; Q|U), I(U; Q|V), I(U; V|Q)\big) : $$
$$Q \text{ jointly distributed with } U, V \Big\}\Big),$$

where $i(\mathsf{S})$ denotes the *increasing hull* of $\mathsf{S} \subseteq \mathbb{R}^3_+$, defined as $i(\mathsf{S}) = \{s \in \mathbb{R}^3_+ : \exists s' \in \mathsf{S} \text{ s.t. } s \geq s'\}$. Thus, we have

$$\alpha(U; V) = \min\{s_2 + s_3 : (0, s_2, s_3) \in \mathfrak{T}(U; V)\}.$$

From [15, Theorems 2.3 and 2.4], we know that $\mathfrak{T}(U; V)$ is a closed, convex region and that, without loss of generality, we may assume the cardinality bound $|\mathcal{Q}| \leq |\mathcal{X}||\mathcal{Y}| + 2$ on the alphabet of Q in the definition. This justifies the use of min and the cardinality bound in (3) as well as the use of min in (5).

As we will prove later, α as a function of the two views satisfies the following properties:

(a) $\alpha(U_i; V_i) \leq \alpha(U_{i-1}; V_{i-1}) + \alpha(X_i; Y_i)$, $i = 1, \ldots, n$.
This means that α of the views can increase at most by $\alpha(X_i; Y_i)$ between the $(i-1)$-th and the i-th uses of the DMC. Specifically, we will see that no increase in α can come from the discussion over the noiseless channel, and an increase of at most $\alpha(X_i; Y_i)$ accrues from the i-th use of the DMC. This allows us to upper bound the increase in α of the views as the protocol progresses.

(b) $\alpha(U_0; V_0) = \alpha(S_0 S_1; K) = 0$,
$\alpha(U_{\text{final}}; V_{\text{final}}) = \alpha(U_n; V_n)$.
This means that α of the initial views is 0, and the α of the final views is the same as after the final use of the DMC.

(c) $\alpha(S_0 S_1; K S_K) \leq \alpha(U_{\text{final}}; V_{\text{final}}) + n\delta(\epsilon)$,
where $\delta(\epsilon) \to 0$ as $\epsilon \to 0$. This means that α of the final views must be at least close to the α of the inputs and (ideal) outputs of Alice and Bob for the OT function being securely computed.

(d) $\alpha(S_0 S_1; K S_K) = nR$
This means that α when applied to the inputs and

(ideal) outputs of Alice and Bob gives the length of the input strings to Alice.

(e) $\alpha(X; Y)$ is a concave function of $p(x)$ for a fixed $p(y|x)$. This justifies the use of max instead of sup in (3).

Now applying (a) recursively and using (b), we get

$$\alpha(U_{\text{final}}; V_{\text{final}}) \leq \sum_{i=1}^{n} \alpha(X_i; Y_i).$$

Using (c) and (d), we get

$$nR = \alpha(S_0 S_1; K S_K) \leq \alpha(U_{\text{final}}; V_{\text{final}}) + n\delta(\epsilon).$$

Thus, we have

$$R \leq \frac{1}{n} \sum_{i=1}^{n} \alpha(X_i; Y_i) + \delta(\epsilon) \leq \max_{p(x)} \alpha(X; Y) + \delta(\epsilon).$$

Thus, we may conclude that $\max_{p(x)} \alpha(X; Y)$ is an upper bound on the OT-capacity for the DMC $p(y|x)$.

It only remains to prove (a)-(e).

(a) Let $\widetilde{U}_i$ and $\widetilde{V}_i$ be the views of Alice and Bob right before the i-th use of the DMC. Then, $\widetilde{U}_i = (U_{i-1}, \Delta F_{i-1}, X_i)$ and $\widetilde{V}_i = (V_{i-1}, \Delta F_{i-1})$, where ΔF_{i-1} is the transcript of the messages exchanged over the noiseless discussion channel after the $i-1$-th use of the DMC and before the i-th use. Note that $U_i = \widetilde{U}_i$ and $V_i = (\widetilde{V}_i, Y_i)$. The following can be inferred from [15, Theorem 5.4]:

$$\mathfrak{T}(\widetilde{U}_i; \widetilde{V}_i) \supseteq \mathfrak{T}(U_{i-1}; V_{i-1}),$$

i.e., the tension region of views cannot shrink during the discussion phase, or by Alice doing a private computation of X_i. Hence,

$$\alpha(\widetilde{U}_i; \widetilde{V}_i) \leq \alpha(U_{i-1}, V_{i-1}).$$

In fact, the second line of property (b) also follows similarly, i.e., $\alpha(U_{\text{final}}; V_{\text{final}}) = \alpha(U_n; V_n)$. Property (a) now follows from the following lemma which is proved in the appendix.

Lemma 1.

$$\alpha(U_i; V_i) \leq \alpha(\widetilde{U}_i; \widetilde{V}_i) + \alpha(X_i; Y_i).$$

(b) By choosing Q to be a constant, $\alpha(U_0; V_0) = \alpha(S_0, S_1; K) = 0$ follows. Proof of $\alpha(U_{\text{final}}; V_{\text{final}}) = \alpha(U_n; V_n)$ was already mentioned in (a).

(c) For a pair of random variables U, V, and $0 \leq \epsilon \leq H(V|U)$, we define

$$\alpha_\epsilon(U; V) = \min_{I(Q; V|U) \leq \epsilon} I(U; Q|V) + I(U; V|Q).$$

Note that $\alpha(U; V) = \alpha_0(U; V)$. We will need the following property (proved in the appendix using the fact that $\mathfrak{T}(U; V)$ is closed [15, Theorem 2.4]).

Lemma 2. *For any pair of random variables U, V, the function $\alpha_\epsilon(U; V)$ is right continuous in ϵ at 0.*

Property (c) now follows from the following lemma (also proved in the appendix):

Lemma 3.

$$\alpha_\epsilon(S_0 S_1; K S_k) \leq \alpha(S_0 S_1 F X^n; K S_K F Y^n) + n\delta_1(\epsilon),$$
$$\alpha(S_0 S_1 F X^n; K S_K F Y^n) \leq \alpha(U_{\text{final}}; V_{\text{final}}) + n\delta_2(\epsilon),$$

where $\delta_1(\epsilon) \to 0$ and $\delta_2(\epsilon) \to 0$ as $\epsilon \to 0$.

The proof of the first part relies on the privacy conditions (1)-(2). The second part uses $P(\widehat{S_K} \neq S_K) \leq \epsilon$.

(d) We prove the following lemma in the appendix.

Lemma 4. $I(S_0 S_1; K S_K | Q) + I(S_0 S_1; Q | K S_K) \geq nR$ *for all $Q - S_0 S_1 - K S_K$.*

The property follows by noticing that equality is achieved by $Q = \emptyset$.

(e) For $Q - X - Y$,

$$I(X; Q|Y) + I(X; Y|Q)$$
$$= I(XY : Q) - I(Y; Q) + I(X; Y|Q)$$
$$= I(X; Q) - I(Y; Q) + I(X; Y|Q)$$
$$= H(Q|Y) - H(Q|X) + H(Y|Q) - H(Y|X).$$

For fixed $p(q|x)$ and $p(y|x)$, the above expression is concave in $p(x)$ since $H(Q|X), H(Y|X)$ are linear in $p(x)$, and both $H(Q|Y), H(Y|Q)$ are concave in $p(x)$; the latter can be shown, for instance, using the convexity of relative entropy. i.e., for the DMC $p(y|x)$, if we define

$$f_{p(q|x)}(p(x)) := I(X; Q|Y) + I(X; Y|Q),$$

where the mutual information terms are evaluated using $p(x, y, q) = p(x)p(q|x)p(y|x)$, then, for $0 \leq \lambda \leq 1$,

$$\lambda f_{p(q|x)}(p_1(x)) + (1 - \lambda)f_{p(q|x)}(p_2(x))$$
$$\leq f_{p(q|x)}(\lambda p_1(x) + (1 - \lambda)p_2(x)).$$

Property (e) now follows from noticing that $\alpha(X; Y) = \min_{p(q|x)} f_{p(q|x)}(p(x))$.
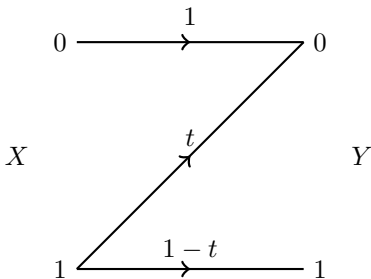
IV. AN EXAMPLE

Fig. 2. The Z-channel (or binary asymmetric channel)

Consider the Z-channel $p(y|x)$ shown in Figure 2. $p(0|0) = 1 - p(1|0) = 1$, and $p(0|1) = 1 - p(1|1) = t$, where $0 \leq t \leq 1$. Figure 3 compares the upper bound (3) on OT capacity from Theorem 1 with the upper bound (4) of Ahlswede and Csiszár [1]. In fact, for ease of numerical
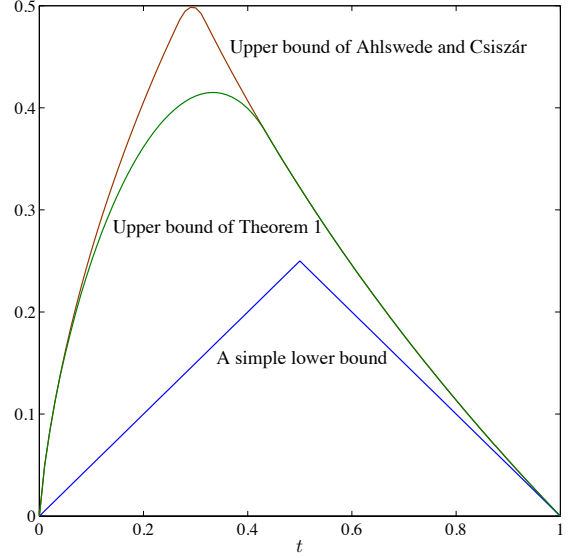

Fig. 3. Bounds on OT capacity of the Z-channel

calculation, what is plotted is (3) optimized over a smaller set of choices for Q; specifically, we restrict to binary Q and $p(q|x)$ of the form $p(0|1) = 0$. Even with this restriction, we observe that for a range of t's the upper bound of (3) strictly improves upon (4).

For comparison, we also plot a simple lower bound to the OT capacity of this channel. Let us consider two channel uses at a time. Now if we only use the input letters from $\{01, 10\}$, then this is a binary erasure channel (erasure symbol 00) with erasure probability t for which the OT capacity was shown in [1] to be $\min(1 - t, t)$. So a lower bound for the OT capacity of the Z-channel is $\frac{\min(1-t,t)}{2}$. We leave the problem of characterizing the OT capacity of the Z-channel as an interesting open problem. We conjecture that at least the lower bound, if not both the bounds, can be improved.

V. DISCUSSION

An analogous upper bound on the OT capacity of the source model can be derived using the results in [15]. Applying Lemma 4 of this paper to [15, Corollary 5.8], the OT capacity C of the discrete memoryless source $p_{X,Y}$ can be shown to satisfy

$$C \leq \min_{Q - X - Y} I(X; Q|Y) + I(X; Y|Q).$$

Details are deferred to a full-length version of this paper..

While this paper focused on deriving an upper bound on OT capacity of DMCs, the technique is more general. In fact, we can derive a general upper bound on the secure sampling capacity of DMCs analogous to the upper bound in [15, Section V] for the source model. The upper bound on OT capacity presented here will follow as a corollary of such a general upper bound. This is deferred to a full-length version.

The definition of OT capacity of DMCs in [12], [7], [1], [13] is in terms of the length of the string (m) per

channel use. A different (not equivalent) possibility is to fix m (say $m = 1$, for 1-bit OT) and consider the number of independent m-string OTs obtained per channel use. This is of interest since, in many secure computation protocols, several independent instances of OT are called for (unlike the one instance of a long string-OT considered in the original definition of OT capacity). We may also consider varying the number of strings given to Alice and the number of strings picked up Bob. The general upper bound mentioned above provides means to derive upper bounds on the rates in all these cases.

The achievability question of how to obtain "high" rates of secure computation/sampling, in general, remains open. The capacity achieving schemes for generalized erasure channels of [1], [13] do not appear to extend to the general case. For the alternative definitions of capacity mentioned above, the best achievability results available for the general case only achieve very low (but non-zero) rates [8]. This is an important problem which requires further research.

Unlike in the two-party setting, information theoretically secure computation, in general, becomes feasible in the multiuser case even when only private randomness at users and private noise-free channels between every pair of users are available, provided the fraction of colluding adversarial users is constrained (less than 1/2 for honest-but-curious and less than 1/3 for malicious) [2], [3]. When such constraints are not satisfied, availability of pairwise OTs, for instance, can enable secure computation in general [6], [14]. Hence, OT capacity of multiuser channels is also of interest [11]. Secure computation in multiuser (noisy) networks is another question which merits further study.

Acknowledgment

References

[1] R. Ahlswede and I. Csiszár, "On oblivious transfer capacity," *Information Theory, Combinatorics, and Search Theory,* Lecture Notes in Computer Science, vol. 7777, pp. 145–166, 2013.

[2] M. Ben-Or, S. Goldwasser, and A. Wigderson, "Completeness theorems for non-cryptographic fault-tolerant distributed computation," 20th Annual ACM Symposium on Theory of Computing, pp. 1–10, 1988.

[3] D. Chaum, C. Crépeau, and I. Damgård, "Multiparty unconditionally secure protocols," 20th Annual ACM Symposium on Theory of Computing, pp. 11–19, 1988.

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

[5] P. Gács and J. Körner, "Common information is far less than mutual information," *Problems of Control and Information Theory*, vol. 2, no. 2, pp. 119–162, 1973.

[6] D. Harnik, Y. Ishai, and E. Kushilevitz, "How many oblivious transfers are needed for secure multiparty computation?" Advances in Cryptology - CRYPTO 2007, Lecture Notes in Computer Science, vol. 4622, pp. 284–302, 2007.

[7] H. Imai, K. Morozov, and A. C. A. Nascimento, "On the oblivious transfer capacity of the erasure channel," 2006 IEEE International Symposium on Information Theory, pp. 1428-1431, 2006.

[8] Y. Ishai, E. Kushilevitz, R. Ostrovsky, Rafail, M. Prabhakaran, A. Sahai, and J. Wullschleger, "Constant-rate oblivious transfer from noisy channels," Advances in Cryptology – CRYPTO 2011, Lecture Notes in Computer Science, vol. 6841, pp. 667–684, 2011.

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

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

[11] M. Mishra, B.K. Dey, V.M. Prabhakaran, and S. Diggavi, "The oblivious transfer capacity of the wiretapped binary erasure channel," to be presented at IEEE International Symposium on Information Theory, 2014. http://arxiv.org/abs/1404.6614

[12] A.C.A. Nascimento and A. Winter, "On the oblivious-transfer capacity of noisy resources," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2572–2581, 2008.

[13] A.C.B. Pinto, R. Dowsley, K. Morozov, A.C.A. Nascimento, "Achieving oblivious transfer capacity of generalized erasure channels in the malicious model," *IEEE Trans. Inform. Theory*, vol. 57, no. 8, pp. 5566–5571, 2011.

[14] M.M. Prabhakaran and V.M. Prabhakaran, "On secure multiparty sampling for more than two parties," 2012 IEEE Information Theory Workshop (ITW), pp. 99–103, Sept. 2012.

[15] V.M. Prabhakaran and M.M. Prabhakaran, "Assisted common information with an application to secure two-party sampling," to appear in *IEEE Trans. Inform. Theory*, vol. 60, no. 6, 2014. http://dx.doi.org/10.1109/TIT.2014.2316011

[16] S. Wiesner, "Conjugate coding," Sigact News, vol. 15, pp. 78–88, 1983.

[17] S. Wolf and J. Wullschleger, "New monotones and lower bounds in unconditional two-party computation," IEEE Trans. Inform. Theory, vol. 54, no. 6, pp. 2792–2797, 2008.

Appendix

Proof of Lemma 1. Note that $U_i = \tilde{U}_i$ which contains X_i as part of it, and $V_i = (\tilde{V}_i, Y_i)$. Suppose we have $\tilde{Q}$ jointly distributed with $\tilde{U}_i, \tilde{V}_i$ such that $\tilde{Q} - \tilde{U}_i - \tilde{V}_i$ is a Markov chain, and Q' is jointly distributed with X_i, Y_i such that $Q' - X_i - Y_i$ a Markov chain. We define a random variable Q with alphabet $\mathcal{Q} = \tilde{\mathcal{Q}} \times \mathcal{Q}'$, where $\tilde{\mathcal{Q}}$ and $\mathcal{Q}'$ are the alphabets of $\tilde{Q}$ and Q' respectively, jointly distributed with U_i, V_i as follows:

$$p_{Q|U_i,V_i}((\tilde{q}, q')|u_i, v_i) = p_{\tilde{Q}|\tilde{U}_i}(\tilde{q}|\tilde{u}_i)p_{Q'|X_i}(q'|x_i),$$

where the $\tilde{u}_i$ on the right hand side is the same as u_i, and x_i is the x_i which is part of u_i. Notice that $Q - U_i - V_i$ is a Markov chain.

To prove the lemma, it is enough to show the following two inequalities

$$I(U_i; Q|V_i) \leq I(\tilde{U}_i; \tilde{Q}|\tilde{V}_i) + I(X_i; Q'|Y_i), \quad (6)$$

$$I(U_i; V_i|Q) \leq I(\tilde{U}_i; \tilde{V}_i|\tilde{Q}) + I(X_i; Y_i|Q'). \quad (7)$$

With come abuse of notation, if we write $Q = (\tilde{Q}, Q')$, then

$$p_{U_i, \tilde{V}_i, X_i, Y_i, Q}(u, \tilde{v}, x, y, (\tilde{q}, q'))$$
$$= p_{\tilde{U}_i, \tilde{V}_i}(u, \tilde{v})p_{\tilde{Q}|\tilde{U}_i}(\tilde{q}|u)p_{X_i|\tilde{U}_i}(x|u)p_{Y|X}(y|x)p_{Q'|X_i}(q'|x), \quad (8)$$

where $p_{Y|X}$ is the DMC and $p_{X_i|\tilde{U}_i}$ is deterministic. We

have

$$
\begin{aligned}
I(U_i; Q|V_i) &= I(U_i; \tilde{Q}Q'|\tilde{V}_i Y_i) \\
&= I(U_i; \tilde{Q}|\tilde{V}_i Y_i) + I(U_i; Q'|\tilde{Q}\tilde{V}_i Y_i) \\
&\leq I(U_i Y_i; \tilde{Q}|\tilde{V}_i) + I(U_i \tilde{Q}\tilde{V}_i; Q'|Y_i) \\
&= [I(U_i; \tilde{Q}|\tilde{V}_i) + I(Y_i; \tilde{Q}|U_i, \tilde{V}_i)] \\
&\quad + [I(X_i; Q'|Y_i) + I(U_i \tilde{Q}\tilde{V}_i; Q'|X_i Y_i)] \\
&= I(\tilde{U}_i; \tilde{Q}|\tilde{V}_i) + I(X_i; Q'|Y_i),
\end{aligned}
$$

where, in the penultimate step, we used the fact that X_i is a part of U_i, and in the last step, we used $U_i = \tilde{U}_i$ and the fact that, for the joint distribution in (8), $\tilde{Q} - (U_i, \tilde{V}_i) - Y_i$ and $Q' - (X_i, Y_i) - (U_i, \tilde{Q}, \tilde{V}_i)$ are Markov chains.

Similarly,

$$
\begin{aligned}
I(U_i; V_i|Q) &= I(U_i; \tilde{V}_i Y_i|\tilde{Q}Q') \\
&= I(U_i; \tilde{V}_i|\tilde{Q}Q') + I(U_i; Y_i|\tilde{V}_i \tilde{Q}Q') \\
&\leq I(U_i Q'; \tilde{V}_i|\tilde{Q}) + I(U_i \tilde{V}_i \tilde{Q}; Y_i|Q') \\
&= [I(U_i; \tilde{V}_i|\tilde{Q}) + I(Q'; \tilde{V}_i|U_i \tilde{Q})] \\
&\quad + [I(X_i; Y_i|Q') + I(U_i \tilde{V}_i \tilde{Q}; Y_i|Q'X_i)] \\
&= I(\tilde{U}_i; \tilde{V}_i|\tilde{Q}) + I(X_i; Y_i|Q'),
\end{aligned}
$$

where the last step follows from the fact that, for the joint distribution in (8), $Q' - (U_i, \tilde{Q}) - \tilde{V}_i$ and $(Q', Y_i) - X_i - (U_i, \tilde{V}_i, \tilde{Q})$ are Markov chains. $\qquad \square$

Proof of Lemma 2. We fix the joint distribution U, V. Below, we will write α_ϵ to mean $\alpha_\epsilon(U; V)$. Note that α_ϵ is a non-increasing function of ϵ. Suppose α_ϵ is not (right) continuous at $\epsilon = 0$, Then there exists a sequence $\epsilon_n \to 0$ such that $\alpha_{\epsilon_n} \nrightarrow \alpha_0$. So there exists a $\delta > 0$ and a monotone subsequence $\epsilon'_n \downarrow 0$ such that $\alpha_0 - \alpha_{\epsilon'_n} \geq \delta, \forall n$. Since $\alpha_{\epsilon'_n}$ is a monotone non-decreasing sequence bounded above it is convergent. Let $l = \sup_n \alpha_{\epsilon'_n}$. Then, $l = \lim_{n \to \infty} \alpha_{\epsilon'_n} \leq \alpha_0 - \delta$. Since $\mathfrak{T}(U; V)$ is a closed region [15, Theorem 2.4], so is

$$
\mathfrak{T}_{1,2+3}(U; V) := \{(s_1, s_2 + s_3) : (s_1, s_2, s_3) \in \mathfrak{T}(U; V)\}.
$$

Hence, all the limit points of $\mathfrak{T}_{1,2+3}(U; V)$ lie in itself. So $(0, l) \in \mathfrak{T}_{1,2+3}(U; V)$. This leads to a contradiction as $l \leq \alpha_0 - \delta$ and, by definition, α_0 is the minimum attainable value of s such $(0, s) \in \mathfrak{T}_{1,2+3}(U; V)$. $\qquad \square$

Proof of Lemma 3. The proof of the first part is along the lines of the proof of property $3'$ of [15, Theorem 5.7]. Consider any Q jointly distributed with S_0, S_1, K, F, X^n, Y^n. We have

$$
\begin{aligned}
&I(KS_K Y^n F; Q|S_0 S_1 F X^n) \\
&= I(KY^n F; Q|S_0 S_1 F X^n) \\
&\geq I(K; Q|S_0 S_1 F X^n) \\
&= I(K; QFX^n|S_0 S_1) - I(K; FY^n|S_0 S_1) \\
&\geq I(K; Q|S_0 S_1) - I(K; FY^n|S_0 S_1) \\
&\geq I(K; Q|S_0 S_1) - \epsilon \quad \text{(by (1))} \\
&= I(KS_K; Q|S_0 S_1) - \epsilon. \tag{9}
\end{aligned}
$$
$$
I(S_0 S_1 X^n F; KS_K Y^n F|Q) \geq I(S_0 S_1; KS_K|Q). \tag{10}
$$

$$
\begin{aligned}
&I(S_0 S_1 X^n F; KS_K Y^n F; Q|KS_K Y^n F) \\
&= I(S_0 S_1 X^n; Q|KS_K Y^n F) \\
&\geq I(S_0 S_1; Q|KS_K Y^n F) \\
&= I(S_0 S_1; QY^n F|KS_K) - I(S_0 S_1; Y^n F|KS_K) \\
&\geq I(S_0 S_1; Q|KS_K) - I(S_0 S_1; Y^n F|KS_K). \tag{11}
\end{aligned}
$$

But,

$$
\begin{aligned}
&I(S_0 S_1; Y^n F|KS_K) \\
&= I(S_{\bar{K}}; Y^n F|KS_K) \\
&= I(S_{\bar{K}}; Y_n F|K) \quad \text{(by indep. of } S_0, S_1, K) \\
&\leq n\epsilon. \quad \text{(by (2))} \tag{12}
\end{aligned}
$$

Substituting (12) in (11),

$$
\begin{aligned}
&I(S_0 S_1 X^n F; KS_K Y^n F; Q|KS_K Y^n F) \\
&\geq I(S_0 S_1; Q|KS_K) - n\epsilon. \tag{13}
\end{aligned}
$$

The first part of the lemma follows from (9),(10), and (13). Specifically,

$$
\alpha_\epsilon(S_0 S_1; KS_K) \leq \alpha(S_0 S_1 X^n F; KS_K Y^n F) + n\epsilon.
$$

To show the second part, let us first observe that U_{final} contains $S_0 S_1 F X^n$ and V_{final} contains $K\widehat{S_K} F Y^n$. Furthermore,

$$
U_{\text{final}} - S_0 S_1 F X^n - K\widehat{S_K} F Y^n - V_{\text{final}}
$$

is a Markov chain, i.e., conditioned on S_0, S_1, F, X^n, Alice's final view (which only additionally contains her private randomness) is conditionally independent of Bob's final view, and similarly, Bob's view is conditionally independent of Alice's view conditioned on $K, \widehat{S_K}, F, Y^n$. Hence, by property 3 of [15, Theorem 5.4], we have

$$
\mathfrak{T}(S_0 S_1 F X^n; K\widehat{S_K} F Y^n) \supseteq \mathfrak{T}(U_{\text{final}}; V_{\text{final}}).
$$

This implies that

$$
\alpha(S_0 S_1 F X^n; K\widehat{S_K} F Y^n) \leq \alpha(U_{\text{final}}; V_{\text{final}}).
$$

It remains to show that

$$
\begin{aligned}
\alpha(S_0 S_1 F X^n; KS_K F Y^n) \\
\leq \alpha(S_0 S_1 F X^n; K\widehat{S_K} F Y^n) + n\delta_2(\epsilon).
\end{aligned}
$$

Let $U := (S_0, S_1, F, X^n)$, $\hat{V} := (K, \widehat{S_K}, F, Y^n)$, and $V := (K, S_K, F, Y^n)$. Since F is part of both U and $\hat{V}$, we have

$$
\begin{aligned}
\alpha(U; \hat{V}) &= \min_{Q - U - \hat{V}} I(U; Q|\hat{V}) + I(U; \hat{V}|Q) \\
&= \min_{Q' - U - \hat{V}} I(U; Q'F|\hat{V}) + I(U; \hat{V}|Q'F)
\end{aligned}
$$

Let $U' := (S_0, S_1, X^n)$, $\hat{V}' := (K, \widehat{S_K}, Y^n)$, and $V' := (K, S_K, Y^n)$. Then,

$$
\alpha(U; \hat{V}) = \min_{Q' - (U'F) - (\hat{V}'F)} I(U'; Q'|\hat{V}'F) + I(U'; \hat{V}'|Q'F).
$$

Similarly,

$$\alpha(U; V)$$
$$= \min_{\tilde{Q}' - (U'F) - (V'F)} I(U'; \tilde{Q}'|V'F) + I(U'; V'|\tilde{Q}'F).$$

For Q' jointly distributed with $(U', F, \hat{V}')$ such that $Q' - (U', F) - (\hat{V}', F)$ is a Markov chain, we will define $\tilde{Q}'$ with the same alphabet as Q' and jointly distributed with (U', F, V') such that $Q' - (U', F) - (V', F)$ is a Markov chain by defining

$$p_{\tilde{Q}'|U',F}(q'|u', f) := p_{Q'|U',F}(q'|u', f).$$

Then, since $P(\hat{V} \neq V) \leq \epsilon$, the total variation distance between $(Q', U', F, \hat{V}')$ and $(\tilde{Q}', U', F, V')$ is at most ϵ, where total variation distance between two random variables W and W' defined over the same alphabet $\mathcal{W}$ is defined as $\Delta(W, W') = \frac{1}{2} \sum_{w \in \mathcal{W}} |p_W(w) - p_{W'}(w)|$.

We will make use [15, Lemma 2.6] to obtain

$$I(U'; \tilde{Q}'|V'F) \leq I(U'; Q'|\hat{V}'F)$$
$$+ 2H_2(\epsilon) + \epsilon n(2R + \log |\mathcal{X}|)$$
$$I(U'; V'|\tilde{Q}'F) \leq I(U'; \hat{V}'|Q'F)$$
$$+ 2H_2(\epsilon) + \epsilon n(2R + \log |\mathcal{X}|),$$

where H_2 is the binary entropy function, and the term $n(2R + \log |\mathcal{X}|)$ is, in fact, the cardinality of U'. From this we may conclude that

$$\alpha(S_0 S_1 F X^n; K S_K F Y^n)$$
$$\leq \alpha(S_0 S_1 F X^n; K\widehat{S_K} F Y^n) + n\delta_2(\epsilon),$$

where $\delta_2(\epsilon) \to 0$ as $\epsilon \to 0$. This completes the proof. $\square$

Proof of Lemma 4. We have,

$$I(S_0 S_1; Q|K S_K)$$
$$= I(S_0 S_1; Q K S_K) - I(S_0 S_1; K S_K)$$
$$= I(S_0 S_1; K S_K|Q) + I(S_0 S_1; Q) - I(S_0 S_1; K S_K).$$

Using this, we can write

$$I(S_0 S_1; K S_K|Q) + I(S_0 S_1; Q|K S_K)$$
$$= 2I(S_0 S_1; K S_K|Q) + [I(S_0 S_1; Q) - I(S_0 S_1; K S_K)]$$
$$= 2[H(K S_K|Q) - H(K S_K|S_0 S_1)]$$
$$+ [H(S_0 S_1|K S_K) - H(S_0 S_1|Q)], \quad (14)$$

where in the last step we used the fact that $Q - S_0 S_1 - K S_K$ is a Markov chain. As we will argue below, under this Markov chain,

$$2H(K S_K|Q) - H(S_0 S_1|Q) \geq 2.$$

Using this, along with $H(K S_K|S_0 S_1) = 1$ and $H(S_0 S_1|K S_K) = nR$ in (14), we can conclude that

$$I(S_0 S_1; K S_K|Q) + I(S_0 S_1; Q|K S_K) \geq nR.$$

It only remains to show that $2H(K S_K|Q) - H(S_0 S_1|Q) \geq 2$ if $Q - S_0 S_1 - K S_K$ is a Markov chain. Since K is independent of (S_0, S_1), it is also independent

of (Q, S_0, S_1). Hence, using the fact that K is a uniform bit,

$$2H(K S_K|Q) = 2H(K) + 2H(S_K|QK)$$
$$= 2 + H(S_0|Q, K = 0) + H(S_1|Q, K = 1)$$
$$= 2 + H(S_0|Q) + H(S_1|Q)$$
$$\geq 2 + H(S_0 S_1|Q).$$

This completes the proof. $\square$