Comments On "Information-Theoretic Key Agreement of Multiple Terminals—Part I"

Amin Gohari and Venkat Anantharam

***Abstract*— Theorem 5 of A. Gohari, V. Anantharam, *IEEE Transactions on Information Theory*, vol. 56, no. 8, pp. 3973-3996, 2010, states an upper bound on the secrecy capacity for the source model problem. It has a three page proof given in Appendix B of the paper. Unfortunately, we show that this bound does not provide any improvement over the simpler bound given in Corollary 1 of the paper. We also provide an example of a family of two agent source model problems where the one-way secrecy rate in each direction is zero, but the secrecy rate is nonzero and can be determined exactly as a conditional mutual information.**

THE paper [1] studies the source model problem for the general case of key agreement between multiple legitimate parties. For clarity of exposition, we restrict the presentation here to the special case of two legitimate parties, but our comments apply to the general case as well.

The classical source model problem with two legitimate parties, Alice and Bob, and an eavesdropper, Eve, is defined as follows: Alice, Bob and Eve respectively observe n i.i.d. repetitions of random variables X, Y and Z, distributed according to some given $p(x, y, z)$. Alice and Bob engage in authenticated and public discussion as follows: Alice creates message F_1 using some $p(f_1|x^n)$ and sends it to Bob. Bob generates message F_2 using some $p(f_2|f_1 y^n)$ and sends it to Alice; then Alice generates F_3 according to $p(f_3|f_{1:2}x^n)$ etc. Assuming k rounds of communication, Alice creates a key K_A according to some $p(k_A|x^n f_{1:k})$ and Bob creates key K_B according to $p(k_B|y^n f_{1:k})$. In an (n, ϵ) code, we demand that the keys be equal to each other with high probability:

$$p(K_A = K_B) \geq 1 - \epsilon.$$

We also require the keys to be almost independent of Eve's information[1]

$$\frac{1}{n} I(K_A; Z^n F_{1:k}) \leq \epsilon.$$

The rate of the generated key is $\frac{1}{n}H(K_A)$.[2] We say that a key rate R_s is achievable if, for every $\epsilon > 0$, there is an (n, ϵ) code whose key rate is at least $R_s - \epsilon$. The supremum of the achievable key rates is called the secret key capacity and denoted by $S(X; Y\|Z)$.

The secret key capacity is known for the following few distributions $p(x, y, z)$. It is shown in [2] that if $X \to Y \to Z$ form a Markov chain then $S(X; Y\|Z) = I(X; Y|Z)$. Furthermore, the capacity is achievable via one-way communication from Alice to Bob. It is also known that $S(X; Y\|Z) = I(X; Y|Z)$ holds for the product of reversely degraded sources, *i.e.* when $X = (X_1, X_2)$, $Y = (Y_1, Y_2)$ and $Z = (Z_1, Z_2)$ where (X_1, Y_1, Z_1) is independent of (X_2, Y_2, Z_2) and $X_1 \to Y_1 \to Z_1$ and $Y_2 \to X_2 \to Z_2$ hold. The idea is to achieve a secrecy rate $I(X_1; Y_1|Z_1)$ by a one-way communication from Alice to Bob, and to achieve a secrecy rate $I(X_2; Y_2|Z_2)$ by a one-way communication from Bob to Alice. This gives a total of $I(X_1; Y_1|Z_1) + I(X_2; Y_2|Z_2) = I(X; Y|Z)$. The above are the only cases where the secret key capacity is known, and both cases are based on the one-way key rate. In the Appendix, we provide a simple example in which the one-way secrecy rate in either direction, of Alice to Bob, or Bob to Alice, is zero, but the secrecy capacity can be exactly found to be equal to $S(X; Y\|Z) = I(X; Y|Z) > 0$.[3] See also [7]–[10] for some recent studies of the source model problem.

We need a definition before stating [1, Thm. 5]. Given a function $f : \mathbb{R} \mapsto \mathbb{R}$, let $S_{f-one-way}$ be defined as follows:

$$S_{f-one-way}(X; Y\|Z) = \sup_{V-U-X-YZ} f(H(U|YV)) - f(H(U|ZV)). \quad (1)$$

Theorem 1 [1, Thm. 5]: For any arbitrary strictly increasing convex function $f : \mathbb{R}_{\geq 0} \mapsto \mathbb{R}_{\geq 0}$, and for any finite random variable J, arbitrarily jointly distributed with X and Y, the secret key capacity $S(X; Y\|Z)$ is bounded from above by

$$f^{-1}\Big(f(S(X; Y\|J)) + S_{f-one-way}(XY; J\|Z)\Big).$$

When $f(x) = kx$ for some constant k, the above upper bound reduces to a simpler bound given in [1, Corollary 1]. Herein, we show that the above bound does not provide any better upper bound than the one obtained by setting $f(x) = kx$. Thus, the bound of [1, Thm. 5] reduces to the bound of Corollary 1 of the paper.

Consider equation (1). Having some $V - U - X - YZ$, take some T independent of all previously defined variables, and define $\tilde{U} = (U, T)$. Then, we have $V - \tilde{U} - X - YZ$. We have

$$f(H(\tilde{U}|YV)) - f(H(\tilde{U}|ZV)) = f(H(U|YV) + H(T)) - f(H(U|ZV) + H(T)).$$

Manuscript received October 10, 2016; revised January 19, 2017; accepted March 4, 2017. Date of current version July 12, 2017. The work of A. Gohari was supported by the Sharif University of Technology under Grant QB950607. The work of V. Anantharam was supported in part by the NSF Science and Technology Center under Grant CCF-0939370: Science of Information, in part by NSF under Grant ECCS-1343398, Grant CNS-1527846, Grant CCF-1618145, and in part by CTLC, Berkeley.

A. Gohari is with the Department of Electrical Engineering, Sharif University of Technology, Tehran 11365, Iran (email: aminzadeh@sharif.edu).

V. Anantharam is with the Department of Electrical Engineering and Computer Sciences, University of California at Berkeley, Berkeley, CA 94720 USA (e-mail: ananth@eecs.berkeley.edu).

Communicated by A. Khisti, Associate Editor for Shannon Theory.

Digital Object Identifier 10.1109/TIT.2017.2685579

[1] This is the weak notion of secrecy. There are stronger notions of secrecy that turn out to give secret key rates equal to that under the weak notion, for the source model problem [3].

[2] Equivalently, we may restrict K_A to be almost uniform, and look at the normalized log of its cardinality as the key rate [1].

[3] Maurer and Wolf [4] construct an example in which the two one-way secrecy rates from Alice to Bob, and from Bob to Alice are both zero, while $S(X; Y\|Z) > 0$. On the other hand, [5, Figs. 4 and 5] gives two examples in which $S(X; Y\|Z)$ is equal to $I(X; Y|Z)$, and $S(X; Y\|Z)$ is strictly greater than both of the one-way secrecy rates, but the two one-way secrecy rates are non-zero. Finally, Orlitsky and Wigderson [6] show that $S(X; Y\|Z) > 0$ if and only if the secrecy capacity with just two rounds of communication is positive.

Given an increasing convex function f, the difference $x \mapsto f(x+d) - f(x)$ is non-decreasing in x for all $d \geq 0$. Therefore, the supremum of $f(H(U|YV)) - f(H(U|ZV))$ over all $V - U - X - YZ$ occurs when we let $H(T)$ go to infinity.

Let

$$g(d) = \lim_{x\to\infty} f(x+d) - f(x), \qquad \forall d \geq 0.$$

According to Lemma 1 given below, one of the following will occur: $g(d) = \infty$ for all $d > 0$, or $g(d) = kd$ for some constant k and all $d \geq 0$. If $g(d) = \infty$, the upper bound from Theorem 5 is infinity. If $g(d) = kd$ is the bound of [1, Thm. 5] is one we can get with a linear function $f(x)$. Therefore, the f aspect of the bound is not giving anything new. We are done.

Lemma 1: For any arbitrary strictly increasing convex function $f : \mathbb{R}_{\geq 0} \mapsto \mathbb{R}_{\geq 0}$, let

$$g(d) = \lim_{x\to\infty} f(x+d) - f(x), \qquad \forall d \geq 0.$$

Then, either $g(d) = \infty$ for all $d > 0$, or $g(d) = kd$ for some constant k and all d.

Proof: Since $f(\cdot)$ is increasing, the function $g(\cdot)$ is non-decreasing. Furthermore,

$$\begin{aligned} &f(x+d_1+d_2) - f(x) \\ &\quad = f(x+d_1+d_2) - f(x+d_1) + f(x+d_1) - f(x). \end{aligned}$$

Hence $g(d_1+d_2) = g(d_1) + g(d_2)$.

Assume that $g(d_0) = \infty$ for some d_0. Then $g(d_0/\ell) = g(\ell d_0) = \infty$ for $\ell \in \mathbb{N}$. From the fact that $g(\cdot)$ is non-decreasing, we get that $g(d) = \infty$ for all $d > 0$. If $g(d) < \infty$ for all d, then from the additivity and non-decreasing properties of $g(\cdot)$ we conclude that $g(\cdot)$ is linear. ∎

As a result of the above discussion, two explicit upper bounds on $S(X;Y\|Z)$ are given in [1]:

$$\begin{aligned} B_1(X;Y\|Z) &= \inf_{p_{J|XYZ}} I(X;Y|J) + I(XY;J|Z), \\ B_2(X;Y\|Z) &= \inf_{p_{J|XYZ}} \sup_{V\to U\to XY\to ZJ} I(X;Y|J) + I(U;J|V) \\ &\qquad - I(X;Y|J). \end{aligned}$$

Observe that $B_2(X;Y\|Z) \leq B_1(X;Y\|Z)$ because for any $V \to U \to XY \to ZJ$ we have

$$\begin{aligned} I(U;J|V) - I(U;Z|V) &\leq I(U;J|ZV) \\ &\leq I(UV;J|Z) \\ &\leq I(XY;J|Z). \end{aligned} \tag{2}$$

There is no discussion of cardinality bounds on the alphabet of auxiliary variables in [1]. The cardinality of J in $B_1(X;Y\|Z)$ can be bounded by $|\mathcal{X}||\mathcal{Y}||\mathcal{Z}|$ using Fenchel's extension of the Carathéodory theorem. For $B_2(X;Y\|Z)$, the cardinality of U and V can be bounded from above by $|\mathcal{U}| \leq |\mathcal{X}|^2|\mathcal{Y}|^2$ and $|\mathcal{V}| \leq |\mathcal{X}||\mathcal{Y}|$ (see [11, Thm. 22.4]). However, it is not clear if one can find a bound on the cardinality of J in $B_2(X;Y\|Z)$. Therefore, we can replace infimum with minimum and supremum with maximum wherever cardinality bounds are available:

$$\begin{aligned} B_1(X;Y\|Z) &= \min_{p_{J|XYZ}} I(X;Y|J) + I(XY;J|Z), \\ B_2(X;Y\|Z) &= \inf_{p_{J|XYZ}} \max_{V\to U\to XY\to ZJ} I(X;Y|J) + I(U;J|V) \\ &\qquad - I(U;Z|V). \end{aligned}$$

Therefore, while B_1 is computable, B_2 cannot be computed explictly. This is not to say that upper bound B_2 is useless. Any arbitrary choice of J does give us a valid upper bound. We simply cannot find the best possible upper bound that we can obtain using $B_2(X;Y\|Z)$.

A different upper bound was recently proposed in [12], wherein it is shown that $S(X;Y\|Z)$ is bounded from above by

$$B_3(X;Y\|Z) = \inf_{\rho^J_{xyz}} I(X;Y|J) + I(XY;J|Z). \tag{3}$$

Here the infimum is over all quantum systems J with an arbitrary joint state with classical variables X, Y, Z according to some ρ^J_{xyz} as follows:

$$\rho_{XYZJ} = \sum_{x,y,z} p(x,y,z)|x,y,z\rangle\langle x,y,z| \otimes \rho^J_{x,y,z}.$$

As argued in [12], while the auxiliary random variable J in $B_1(X;Y\|Z)$ computes a lower convex envelope, the "quantum convexification" by an auxiliary system J is not well understood (see [13]). Finally, we point out that a one-shot version of B_1 is given in [15, Corollary 8].

I. Conclusion

Only two upper bounds $B_2(X;Y\|Z)$ and $B_3(X;Y\|Z)$ remain as the best known upper bounds on the secret key capacity. Unfortunately, $B_2(X;Y\|Z)$ and $B_3(X;Y\|Z)$ cannot be calculated explicitly.

Appendix

Let R be a uniform Bernouli random variable. We pass R through three independent erasure channels with parameter ϵ to obtain X, Y and Z. Thus, $p(x,y,z,r) = p(r)p_{BEC}(x|r)p_{BEC}(y|r)p_{BEC}(z|r)$. This joint pmf is similar to the one considered in [3], except that in [3] random variable R is passed through independent BSC channels. Observe that because of the symmetry $p_{X,Y}(a,b) = p_{X,Z}(a,b) = p_{Y,Z}(a,b)$ for all $a, b \in \{0,1,e\}$. Therefore, the one-way secrecy rates are zero. Furthermore, X, Y and Z do not form a Markov chain in any order. Since we always have $S(X;Y\|Z) \leq I(X;Y|Z)$ [2], [14], we obtain $S(X;Y\|Z) \leq \epsilon(1-\epsilon)^2$. The proof sketch for showing that $\epsilon(1-\epsilon)^2$ is an achievable secrecy rate is as follows. Take some $\delta > 0$. Assuming that Alice, Bob and Eve observe X^n, Y^n and Z^n respectively, Alice and Bob reveal the location of their erasures on the public channel. The number of locations where neither Alice nor Bob's bits are erased is at least $n((1-\epsilon)^2 - \delta)$ with probability tending to one as n tends to infinity. Observe that the location of erasures of Alice and Bob is independent of the bits observed by Alice and Bob in the non-erased locations. Thus, Alice and Bob can agree on $n((1-\epsilon)^2 - \delta)$ bits, which are independent of the communication used to reveal the erasure locations. However, each of these bits is observed by Eve with probability $1-\epsilon$, and we need to apply privacy amplification on the common bits to produce secure bits. If we let $A = B$ denote the common bit of Alice and Bob, and Z denote Eve's observation, the conditional entropy $H(A|Z)$ is equal to ϵ, which gives the rate at which we can extract bits from A that are secure from Z. If Alice and Bob create a random hash (or random binning) of output size $n((1-\epsilon)^2 - \delta)(\epsilon - \delta)$ of the $n((1-\epsilon)^2 - \delta)$ bits, the hash index will be almost independent of Eve's observation.

References

[1] A. Gohari and V. Anantharam, "Information-theoretic key agreement of multiple terminals—Part I," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3973–3996, Aug. 2010.

[2] R. Ahlswede and I. Csiszàr, "Common randomness in information theory and cryptography. I. Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[3] U. M. Maurer and S. Wolf, "From weak to strong information-theoretic key agreement," in *Proc. Int. Symp. Inf. Theory (ISIT)*, 2000, p. 18.

[4] U. Maurer and S. Wolf, "Towards characterizing when information-theoretic secret key agreement is possible," in *Advances in Cryptology—ASIACRYPT*. Berlin, Germany: Springer, 1996, pp. 196–209.

[5] E. Chitambar, B. Fortescue, and M. H. Hsieh, "Distributions attaining secret key at a rate of the conditional mutual information," in *Proc. Annu. Cryptol. Conf.*, Berlin, Germany, 2015, pp. 443–462.
[6] A. Orlitsky and A. Wigderson, "Secrecy enhancement via public discussion," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*. Jan. 1993, p. 155.
[7] S. Nitinawarat and P. Narayan, "Secret key generation for correlated Gaussian sources," *IEEE Trans. Inf. Theory*, vol. 58, no. 6, pp. 3373–3391, Jun. 2012.
[8] S. Watanabe and Y. Oohama, "Secret key agreement from vector Gaussian sources by rate limited public communication," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 541–550, Sep. 2011.
[9] C. Chan, "Linear perfect secret key agreement," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Oct. 2011, pp. 723–726.
[10] C. Chan, M. Mukherjee, N. Kashyap, and Q. Zhou, "When is omniscience a rate-optimal strategy for achieving secret key capacity?" in *Proc. IEEE Inf. Theory Workshop (ITW)*, Sep. 2016, pp. 354–358.
[11] A. El Gamal and Y.-H. Kim, *Network Information Theory*. Cambridge, U.K.: Cambridge Univ. Press, 2011.
[12] K. Keykhosravi, M. Mahzoon, A. Gohari, and M. R. Aref, "From source model to quantum key distillation: An improved upper bound," in *Proc. Iran Workshop Commun. Inf. Theory (IWCIT)*, May 2014, pp. 1–6.
[13] S. Beigi and A. Gohari, "On dimension bounds for auxiliary quantum systems," *IEEE Trans. Inf. Theory*, vol. 60, no. 1, pp. 368–387, Jan. 2014.
[14] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.
[15] H. Tyagi and S. Watanabe, "Converses for secret key agreement and secure computing," *IEEE Trans. Inf. Theory*, vol. 61, no. 9, pp. 4809–4827, Sep. 2015.

Amin Gohari received the M.Sc. and Ph.D. degrees in electrical engineering from the University of California, Berkeley, in 2010, and the B.Sc. degree from the Sharif University of Technology, Iran, in 2014. He is an Associate Professor at the Sharif University of Technology, Tehran, Iran. He was a recipient of the 2010 Eli Jury Award from the Department of Electrical Engineering, UC Berkeley, for "outstanding achievement in the area of communication networks," and the 2009–2010 Bernard Friedman Memorial Prize in Applied Mathematics from the Department of Mathematics, UC Berkeley, for demonstrated ability to do research in applied mathematics. He was also a recipient of the Gold Medal from the 41st International Mathematical Olympiad (IMO 2000) and the First Prize from the 9th International Mathematical Competition for University Students (IMC 2002). He is also a co-author of a paper that received the 2013 Jack Keil Wolf ISIT Student Paper Award. He was selected as an Exemplary Reviewer for TRANSACTIONS ON COMMUNICATIONS in 2016.

Venkat Anantharam received the B.Tech. in electrical engineering (electronics) from the Indian Institute of Technology, Madras, in 1980, and the M. A. and C.Phil. degrees in mathematics and the M.S. and Ph.D. degrees in electrical engineering from the University of California, Berkeley, in 1983, 1984, 1982, and 1986 respectively. He is on the faculty of the EECS Department at the University of California, Berkeley. He was a recipient of the Philips India Medal and the President of India Gold Medal from IIT Madras in 1980 and an NSF Presidential Young Investigator award in 1988. He is a co-recipient of the 1998 Prize Paper Award of the IEEE Information Theory Society, and a co-recipient of the 2000 Stephen O. Rice Prize Paper Award of the IEEE Communications Theory Society. He received the Distinguished Alumnus Award from IIT Madras in 2008.