

New Bounds on the Information-Theoretic Key Agreement of Multiple Terminals

Amin Aminzadeh Gohari
EECS Department
University of California Berkeley
Berkeley, CA 94720
aminzade@eecs.berkeley.edu

Venkat Anantharam
EECS Department
University of California Berkeley
Berkeley, CA 94720
ananth@eecs.berkeley.edu

Abstract— We study the problem of Information-theoretically secure secret key agreement under the well-known *source model* and *channel model*. In both of these models the parties wish to create a shared secret key that is secure from an eavesdropper with unlimited computational resources. In the channel model, the first party can choose a sequence of inputs to a discrete memoryless channel, which has outputs at the other parties and at the eavesdropper. After each channel use, the parties can engage in arbitrarily many rounds of interactive authenticated communication over a public channel. At the end, each party should be able to generate the key. In the source model, the parties wishing to generate a secret key (as well as the eavesdropper) receive a certain number of independent identically distributed copies of jointly distributed random variables after which the parties are allowed interactive authenticated public communication, at the end of which each party should be able to generate the key. We derive new lower and upper bounds on the secret key rate under the source model and the channel model, and introduce a technique for proving that a given expression bounds the secrecy rate from above in the channel model. Our lower bounds strictly improve what is essentially the best known lower bound in both the source model and the channel model. Our upper bound in the channel model strictly improves the current state of art upper bound. We do not know whether our new upper bound in the source model represents an strict improvement but we have included the bound for completeness.

I. INTRODUCTION

A fundamental problem in cryptography is the generation of a common secret key between a set of parties in the presence of an eavesdropper. This secret key can then be, for instance, used in private communication. Information theoretic security is the most stringent form of security since it does not make any assumptions on the computational power of the adversary. Shannon was the first who precisely formulated the problem of information-theoretically secure secret key generation [12]. Since then, the work of Shannon has been much developed and modified (for example see [11], [10], [7], [3], [4]). In an early work, Maurer considered the model in which Alice can send a message to Bob (which is also heard by the eavesdropper Eve) through a broadcast channel [7]. He made the interesting observation that even if the channel from Alice to Eve is stronger than the channel from Alice to Bob, Alice and Bob may still be able to generate a common secret key that is asymptotically information-theoretically secure from Eve if we allow Bob to send authenticated but public messages to Alice.

This observation led to the formulation of the two main models in this area, introduced by the works of Ahlswede and Csiszár [3], Csiszár and Narayan [1] and Maurer [7], called the *source model* and *channel model*. In both models there are m parties interested in secret key generation against an adversary Eve. In the channel model, the m parties and Eve have access to n independently and identically distributed (i.i.d.) repetitions of jointly distributed random variables X_i ($i = 1, \dots, m$), and Z . Following the reception of the n i.i.d. repetitions of $(X_1, X_2, \dots, X_m, Z)$, in the traditional source model the m parties are allowed to have interactive authenticated public communication. In the channel model, a secure DMC channel $q(x_2, x_3, \dots, x_m, z|x_1)$ exists from the first terminal to all other terminals (including Eve). The input of the DMC is governed by the first party while the other parties (including Eve) observe the outputs of the broadcast channel at their end. In the traditional channel model, after each use of the channel by the first party, all the m parties are allowed to engaged in arbitrary many rounds of interactive authenticated communication over a public channel. We generalize both models somewhat by allowing the communication only among the first u ($1 \leq u \leq m$) of the parties; parties $u + 1, \dots, m$ can listen and have to participate in secret key generation, but do not talk. This generalization has the technical advantage of putting one-way secret key generation and interactive secret key generation on the same footing and includes the standard model as a special one.

Following the communication, in both models, each party generates random variable S_i as its secret key ($i = 1, 2, \dots, m$). All S_i 's should with high probability be equal to each other and they should be approximately independent of Eve's whole information after the communication (e.g. the n i.i.d repetitions of Z and the public discussion in the source model). The achieved secret key rate would then be roughly $\frac{1}{n}H(S_1)$. The highest achievable secret key rate (asymptotic in n) is called the secrecy capacity (for a precise formulation see section 2).

Calculation of the exact secrecy capacity remains an unsolved problem, although some lower and upper bounds on this quantity are known. In the source model and for the case of $m = 2$, the best know upper bound due to Gohari and Anantharam equals $\inf_J [I(X_1; X_2|J) + I(X_1X_2; J|Z)]$ [4]. In the channel mode, the best know upper bound ex-

explicitly mentioned in the literature, as far as we are aware, is $\min\{\sup_{p(x_1)} I(X_1; X_2), \sup_{p(x_1)} I(X_1; X_2|Z)\}$ proposed by Maurer [7]. This can however be easily generalized to $\inf_{\bar{Z}-Z-X_1X_2} [\sup_{p(x_1)} I(X_1; X_2|\bar{Z})]$. In the source model, the essentially best known lower bound, proved using random binning arguments, is due to Ahlswede and Csiszár [3]: the maximum of $\sup_{V-U-X-YZ} (I(U; Y|V) - I(U; Z|V))$ and $\sup_{V-U-Y-XZ} (I(U; X|V) - I(U; Z|V))$ (Maurer provided a different technique for deriving lower bounds on the secret key rate in [7]. More specifically, he proved that even when the maximum of the two one-way communications vanishes, the secret key rate may be positive. This technique however seems to give us a rather low secrecy rate.) In the channel model, the essentially best known lower bound as far as we are aware is $\sup_{p(x_1)} \max\{\sup_{V-U-X_1-X_2Z} [I(U; X_2|V) - I(U; Z|V)], \sup_{V-U-X_2-X_1Z} [I(U; X_1|V) - I(U; Z|V)]\}$ where (X_1, X_2, Z) inside the supremum has joint distribution $p(x_1)q(x_2, z|x_1)$ [7] [1].

In this paper we develop a new single letter lower bound for the secrecy rate under both the source model and the channel model. Our bounds, in the case of two terminals, strictly improve the above mentioned results. Roughly speaking our bound in the source model is proved by following the interactive communication stage by stage, however we have to do some careful bookkeeping of the buildup of the secret-key rate by controlling the amount of reduction of secret key rate built-up in earlier stages due to the communication in later stages. The lower bound in source model is exploited for deriving a new lower bound on the secrecy rate in the channel model. An example is provided to show that the new bound represents an strict improvement of better than $\sup_{p(x_1)} \max\{\sup_{V-U-X_1-X_2Z} [I(U; X_2|V) - I(U; Z|V)], \sup_{V-U-X_2-X_1Z} [I(U; X_1|V) - I(U; Z|V)]\}$. In this paper, we also improve the above mentioned upper bound on secret key rate in the channel model. Our proof technique is similar to the one for proving upper bounds in our previous paper [4]. The idea is to define a potential function and show that for any valid secret key generating protocol, the potential function starts from the upper bound and decreases as we move along the protocol, and eventually becomes equal to the gain of the protocol. Finally, we propose a new upper bound in the source model that generalizes the upper bound of [4] and may improve it. We have included this bound for completeness.

The outline of this paper is as follows. In section II, we introduce the basic notations and definitions used in this paper. Section III contains the main results of this paper followed by section IV which gives brief heuristic sketch of the proofs for the results.

II. DEFINITIONS AND NOTATIONS

Throughout this paper we assume X_1, X_2, \dots, X_m and Z are $m + 1$ possibly dependent random variables each taking values from a finite set.

Our model is similar to the multi-terminal source and channel models as in [1] and [2] except that we relax the uniformity condition on the generated secret key i.e. equation (2) in [1]

(Maurer in [7] argued that the assumption of uniformity could always be added without loss of generality). We study the weak notion of secrecy throughout this paper and assume that all m parties are interested in secret key generation. (It is known that the weak and strong secret key rates are equal [8])

A. Source Model

Given n i.i.d. repetitions of a random variable X , we denote the i^{th} of these by $X(i)$. We write $X^{1:i}$ for $(X(1), X(2), \dots, X(i))$. For $X^{1:n}$ we will often instead write X^n .

Definition 1: Given n i.i.d repetitions of the random variables $(X_1, X_2, \dots, X_m, Z)$ having the joint distribution $p(x_1, x_2, x_3, \dots, x_m, z)$, the pair (n, \vec{C}) , where $\vec{C} = (C_1, C_2, \dots, C_r)$ is a finite set of discrete random variables is considered a “valid communication” if:

- $H(C_i|C_1, C_2, \dots, C_{i-1}, X_j^n) = 0 \forall j : 1 \leq j \leq m, i - j \equiv_m 0$
- For all $r > u$, we have $C_i = 0 \forall i : i - r \equiv_m 0$ (r -th terminal is not allowed to participate in the communication)

Please note that if (n, \vec{C}) is valid, then one has $H(\vec{C}|X_1^n, X_2^n, \dots, X_m^n) = 0$.

Definition 2. Let $p(x_1, x_2, x_3, \dots, x_m, z)$ be a joint distribution, n be a natural number, $X_1^n, X_2^n, \dots, X_m^n$ and Z^n be n i.i.d. repetitions of random variables X_1, \dots, X_m and Z having the joint distribution $p(x_1, x_2, x_3, \dots, x_m, z)$, ϵ be a positive real number, $\vec{C} = (C_1, C_2, \dots, C_r)$ be a finite set of discrete random variables and S_1, \dots, S_m be m discrete random variables.

The data typing condition $SK(n, \epsilon, S_1, S_2, S_3, \dots, S_m, \vec{C})$ is said to hold iff the following conditions are satisfied:

- 1) the pair (n, \vec{C}) is a valid communication.
- 2) $H(S_i|C_1, C_2, \dots, C_r, X_i^n) = 0$ for all $1 \leq i \leq m$
- 3) $P(S_1 = S_2 = S_3 = \dots = S_m) > 1 - \epsilon$
- 4) $\frac{1}{n} I(S_1; Z^n, C_1, C_2, \dots, C_r) < \epsilon$

To any SK data type, we assign a number called the “gain” of the SK data type which is defined as $\frac{1}{n} H(S_1)$.

Definition 3: $S(X_1; X_2; X_3; \dots; X_u; X_{u+1}^{(s)}; \dots; X_m^{(s)} || Z)$, the secret key rate when the terminals can randomize, is defined as the supremum over all (M_1, M_2, \dots, M_u) satisfying: $p(M_1, \dots, M_u, X_1, \dots, X_m, Z) = p(M_1) \cdot p(M_2) \cdot \dots \cdot p(M_u) \cdot p(X_1, \dots, X_m, Z)$ of $\lim_{\epsilon \rightarrow 0} \limsup_{n \rightarrow \infty} \sup_{SK(n, \epsilon, S_1, S_2, S_3, \dots, S_m, \vec{C})} Gain(SK)$.

The data typing $SK(n, \epsilon, S_1, S_2, S_3, \dots, S_m, \vec{C})$ inside the supremum is defined for $(X_1 M_1, X_2 M_2, \dots, X_u M_u, X_{u+1}, \dots, X_m)$.

Please note that the superscript “(s)” is used to denote the silent parties.

B. Channel Model

Given an ordered sequence of n random variables taking values from the set X , we denote the i^{th} of these by $X(i)$. We write $X^{1:i}$ for $(X(1), X(2), \dots, X(i))$. For $X^{1:n}$ we will often instead write X^n .

III. STATEMENT OF THE RESULTS

A. Source Model

Theorem 1. $S(X_1; X_2; \dots; X_u; (X_{u+1})^{(s)} \dots; (X_m)^{(s)} \| Z)$ is lower bounded by $\sum_{j=q}^p [\min_{1 \leq r \leq m} I(U_j; X_r | U_{1:j-1}) - I(U_j; Z | U_{1:j-1})]$ for every $q \leq p$, and (U_1, \dots, U_p) satisfying the following constraints:

- U_i ($i = 1, \dots, p$) takes values from a finite set.
- $p(U_1, \dots, U_p | X_1 X_2, X_3, \dots, X_m, Z) = \prod_{i=1}^p p(U_i | U_{1:i-1} X_{i \bmod m})$
- For all $r > u$, we have $U_i = 0 \forall i : i - r \equiv m \pmod{0}$

This lower bound strictly improves the known lower bound given by the maximum of the two one-way secrecy rates.

Theorem 2. $S(X_1; X_2; \dots; X_u; X_{u+1}^{(s)} \dots; X_m^{(s)} \| Z)$ is upper bounded by $\inf_{f, J} f^{-1} \{f(S(X_1; X_2; \dots; X_u; (X_{u+1})^{(s)} \dots; (X_m)^{(s)} \| J)) + S_{f\text{-one-way}}(X_1 X_2 \dots X_m; J^{(s)} \| Z)\}$. where $f : \mathfrak{R} \geq 0 \mapsto \mathfrak{R} \geq 0$ is a strictly increasing convex function and the f-one-way secrecy rate is defined as be

$$S_{f\text{-one-way}}(X; Y^{(s)} \| Z) = \sup_{V-U-X-Y} [f(H(U|ZV)) - f(H(U|YV))].$$

This upper bound is in turn upper bounded by $\inf_{f, J} f^{-1} (f(S(X_1 J; X_2 J; \dots; X_u J; (X_{u+1} J)^{(s)} \dots; (X_m J)^{(s)} \| J)) + S_{f\text{-one-way}}(X_1 X_2 \dots X_m; J^{(s)} \| Z))$ whose single letter characterization could be computed using Theorem 3.

Remark. This upper bound reduces to our previous upper bound given in the [4] (section V) for the special case of $f(x) = x$. We don't know if this bound strictly improves that of [4].

Theorem 3. Let $[m]$ and $[u]$ respectively denote the sets $\{1, 2, \dots, m\}$ and $\{1, 2, \dots, u\}$. The following formula on the secret key rate in the presence of silent parties holds:

$$S(X_1 Z; X_2 Z; \dots; X_u Z; (X_{u+1} Z)^{(s)} \dots; (X_m Z)^{(s)} \| Z) = H(X_1 \dots X_u | Z) - \min_{(R_1, \dots, R_u) \in \mathfrak{R}} (\sum_{i=1}^u R_i), \text{ where:}$$

$$\mathfrak{R} = \{(R_1, \dots, R_u) : \forall B : B \subset [m], B \cap [u] \neq \emptyset, B \neq [m] : \sum_{j \in B \cap [u]} R_j \geq H(X_B \cap [u] | X_{B^c} Z)\}.$$

B. Channel Model

Theorem 4. Assume that $q \leq p$ are two arbitrary natural numbers, (U_1, \dots, U_p) are arbitrary random variables satisfying the following properties:

- U_i ($i = 1, \dots, p$) takes values from a finite set.
- $p(U_1, \dots, U_p | X_1 X_2, X_3, \dots, X_m, Z) = \prod_{i=1}^p p(U_i | U_{1:i-1} X_{i \bmod m})$
- For all $r > u$, we have $U_i = 0 \forall i : i - r \equiv m \pmod{0}$

$C_{CH}(u, q(x_2, x_3, \dots, x_m, z | x_1))$ is lower bounded by $\sup_{p(x_1)} \sum_{j=q}^p [\min_{1 \leq r \leq m} I(U_j; X_r | U_{1:j-1}) - I(U_j; Z | U_{1:j-1})]$ where $(X_1, \dots, X_m, Z, U_1, \dots, U_p)$ inside the supremum has joint distribution $p(x_1) q(x_2, x_3, \dots, x_m, z | x_1) p(U_1, \dots, U_p | X_1 X_2, X_3, \dots, X_m, Z)$.

In the case of $m = 2$, the new lower bound on $C_{CH}(2, q(y, z | x))$ derived by taking supremum over all valid (q, p, U_1, \dots, U_p) strictly improves the $\sup_{p(x)} [\max(S(X; Y^{(s)} \| Z), S(X^{(s)}; Y \| Z))]$ lower bound. In this expression, $S(X; Y^{(s)} \| Z)$ is the source-model one way secrecy rate from X to Y in the presence of Z .

Definition 4. Let $q(x_2, x_3, \dots, x_m, z | x_1)$ be a conditional distribution, n be a natural number, ϵ be a positive real number, $\vec{C} = (\vec{C}_1, \vec{C}_2, \dots, \vec{C}_n)$ be a collection of n finite sets of discrete random variables $\vec{C}_i : i = 1..n$. Each \vec{C}_i is a finite set of discrete random variables: $\vec{C}_i = (C_i^1, C_i^2, \dots, C_i^{r(i)})$. Let $M_1, \dots, M_u, X_1^n, X_2^n, \dots, X_m^n, Z^n$ and S_1, \dots, S_m be $u + (m + 1)n + m$ discrete random variables.

Consider the following conditions:

- 1) For $i = 1, \dots, n$: $p(X_2(i) = x_2(i), X_3(i) = x_3(i), \dots, X_m(i) = x_m(i), Z(i) = z(i) | X_1^{1:i} = x_1^{1:i}, X_2^{1:i-1} = x_2^{1:i-1}, \dots, X_m^{1:i-1} = x_m^{1:i-1}, Z^{1:i-1} = z^{1:i-1}, M_1 = m_1, \dots, M_u = m_u) = q(x_2(i), x_3(i), \dots, x_m(i), z(i) | x_1(i))$
- 2) For $i = 2, \dots, n$: $H(X_1(i) | \vec{C}_1, \vec{C}_2, \dots, \vec{C}_{i-1}, M_1, X_1^{1:i-1}) = 0$
- 3) $p(M_1 \dots M_u X_1(1), X_2(1), \dots, X_m(1), Z(1)) = p(M_1) \dots p(M_u) p(X_1(1), X_2(1), \dots, X_m(1), Z(1))$
- 4) $H(\vec{C}_i^j | \vec{C}_1, \vec{C}_2, \dots, \vec{C}_{i-1} \vec{C}_i^{1:j-1} X_s^{1:i} M_s) = 0 \forall s : 1 \leq s \leq u, s - j \equiv m \pmod{0}$
 $\vec{C}_i^j = 0 \forall i, j, s : j - s \equiv m \pmod{0}$ and $s > u$ (meaning that s -th terminal is not allowed to participate in the communication)
- 5) $H(S_i | \vec{C}_i, X_i^n M_i) = 0$ for $1 \leq i \leq u$
 $H(S_i | \vec{C}_i, X_i^n) = 0$ for $u + 1 \leq i \leq m$
- 6) $P(S_1 = S_2 = S_3 = \dots = S_m) > 1 - \epsilon$
- 7) $\frac{1}{n} I(S_1; Z^n, \vec{C}) < \epsilon$

Intuitively, n represents the number of communication rounds; \vec{C}_i communications at the i -th stage; M_1, \dots, M_u external randomness provided to the first u parties.

The data typing condition $SK_C(n, \epsilon, S_1, S_2, S_3, \dots, S_m, \vec{C}, (M_1, M_2, \dots, M_u), X_1^n, X_2^n, \dots, X_m^n, Z^n)$ is said to hold iff all above-mentioned conditions are satisfied. To any SK_C data type, we assign a number called the "gain" of the SK_C data type which is defined as $\frac{1}{n} H(S_1)$.

Definition 5: $C_{CH}^\epsilon(u, q(x_2 \dots x_m z | x_1))$, the ϵ secret key rate, is defined as:

$$\limsup_{n \rightarrow \infty} \sup_{SK_C(n, \epsilon, \dots)} \text{Gain}(SK)$$

Definition 6: $C_{CH}(u, q(x_2 \dots x_m z | x_1))$, the channel model secret key rate, is defined as the limit of $C_{CH}^\epsilon(u, q(x_2 \dots x_m z | x_1))$ as ϵ goes to zero.

Note that we have allowed the first user to participate in the public discussion and to randomize. The assumption on the participation of the first party in the public discussion can be removed but this party must be allowed to randomize. Otherwise, the inputs to the broadcast channel will be always a deterministic function of the public communication and thus known to the eavesdropper, resulting in zero secret key rate. It is legitimate to differentiate between the ability to randomize and the ability to participate in the public discussion as long as the first user is concerned. For the sake of notational simplicity, however, we allow the first user to participate in the public discussion.

Theorem 5. Let $\varphi_j(p(x_1, \dots, x_m, z))$ ($j = 1, 2, \dots$) be a function from the set of probability distributions defined on finite sets to real numbers. For any conditional distribution $q(x_2, x_3, \dots, x_m, z|x_1)$, $\phi(q(x_2, x_3, \dots, x_m, z|x_1)) = \sup_{q(x_1)} \varphi_1(q(x_1) \cdot q(x_2, x_3, \dots, x_m, z|x_1))$ would be an upper bound on $C_{CH}(u, q(x_2, x_3, \dots, x_m, z|x_1))$, the channel model secrecy rate (assuming that only the first u terminals are permitted to talk), if φ_j ($j = 1, 2, \dots$) satisfy the following:

Take some arbitrary j and $p(x_1, \dots, x_m, z)$. $\varphi_j(X_1; X_2; X_3; \dots; X_m \| Z)$ should satisfy the following properties (we sometimes use the notation $\varphi_j(X_1; X_2; X_3; \dots; X_m \| Z)$ to refer to $\varphi_j(p(x_1, \dots, x_m, z))$ when (X_1, \dots, X_m, Z) has the law $p(x_1, \dots, x_m, z)$)

1) Whenever

$H(X'_1|X_1) = 0$ and
 $X_1 X_2 \dots X_m Z - X_1 - X'_1 - X'_1 X'_2 \dots X'_m Z'$ and
 $p(x'_2, x'_3, \dots, x'_m, z'|x'_1) = q(x_2, x_3, \dots, x_m, z|x_1)$
are true, we have:

$$\varphi_{j+1}(X_1 X'_1; X_2 X'_2; \dots; X_m X'_m \| Z Z') \leq \varphi_j(X_1; X_2; \dots; X_m \| Z) + \phi(q(x_2, x_3, \dots, x_m, z|x_1))$$

2) For any random variable F such that $\exists i \leq u$:

$$H(F|X_i) = 0, \text{ we have:}$$

$$\varphi_j(X_1; X_2; \dots; X_m \| Z) \geq \varphi_j(X_1 F; X_2 F; \dots; X_m F \| Z F)$$

3) For any random variables X'_1, X'_2, \dots, X'_m such that $\forall i$:

$$H(X'_i|X_i) = 0, \text{ we have:}$$

$$\varphi_j(X_1; X_2; \dots; X_m \| Z) \geq \varphi_j(X'_1; X'_2; \dots; X'_m \| Z).$$

4) $\varphi_j(X_1; X_2; \dots; X_m \| Z) \geq H(X_1|Z) - \sum_{i=2}^m H(X_1|X_i)$

5) Whenever for random variables M_1, M_2, \dots, M_u

$$p(M_1, M_2, \dots, M_u, X_1, X_2, X_3, \dots, X_m, Z) = p(M_1)p(M_2)\dots p(M_u)p(X_1, X_2, X_3, \dots, X_m, Z)$$

is true, we have:

$$\varphi_j(X_1; X_2; \dots; X_m \| Z) \geq \varphi_j(M_1 X_1; M_2 X_2; \dots; M_u X_u; X_{u+1}; \dots; X_m \| Z)$$

Furthermore there exists $\varphi_j(p(x_1, \dots, x_m, z))$ ($j = 1, 2, \dots$) satisfying the above properties such that $C_{CH}(u, q(x_2, x_3, \dots, x_m, z|x_1)) = \sup_{q(x_1)} \varphi_1(q(x_1) \cdot q(x_2, x_3, \dots, x_m, z|x_1))$.

Theorem 6. Let $[m]$ and $[u]$ respectively denote the sets $\{1, 2, \dots, m\}$, $\{1, 2, \dots, u\}$. For every $\Lambda = (\lambda_B, B \subseteq [m])$ satisfying the following equation for all u -tuple (R_1, \dots, R_u) of real numbers

$$\sum_{B: B \subseteq [m], B \cap [u] \neq \emptyset, B \neq [m]} \lambda_B \sum_{j \in B \cap [u]} R_j = \sum_{j=1 \dots u} R_j.$$

, the following inequality holds:

$$C_{CH}(u, q(x_2, x_3, \dots, x_m, z|x_1)) \leq \sup_{p(x_1)} \{ \inf_{p(J|X_1, \dots, X_m, Z)} ([H(X_1 \dots X_u | J) - \tau^\Lambda(X_1, X_2, \dots, X_u, X_{u+1}^{(s)}, \dots, X_m^{(s)} \| J) + I(X_1 X_2 \dots X_m; J | Z)]) \}.$$

In this expression (X_1, \dots, X_m, J, Z) have the law $p(X_1)q(x_2, \dots, x_m, z|x_1)p(J|X_1, \dots, X_m, Z)$ and Λ is the mnemonic for $(\lambda_B, B \subseteq [m])$.

And τ^Λ is defined as $\sum_{B: B \subseteq [m], B \cap [u] \neq \emptyset, B \neq [m]} \lambda_B H(X_B \cap [u] | X_{B^c} J)$.

Remark. The above upper bound can be written as the infimum over the set of all valid Λ of

$\sup_{p(x_1)} \{ \inf_{p(J|X_1, \dots, X_m, Z)} ([H(X_1 \dots X_u | J) - \tau^\Lambda(X_1, X_2, \dots, X_u, X_{u+1}^{(s)}, \dots, X_m^{(s)} \| J) + I(X_1 X_2 \dots X_m; J | Z)]) \}$. If the infimum over Λ is swaped with the supremum over $p(x_1)$, one gets the following lower bound on our upper bound by applying theorem 3:

$\sup_{p(x_1)} \{ \inf_{p(J|X_1, \dots, X_m, Z)} ([S(X_1 J; X_2 J; \dots; X_u J; (X_{u+1} J)^{(s)} \dots; (X_m J)^{(s)} \| J) + I(X_1 X_2 \dots X_m; J | Z)]) \}$. We were not able to prove that this smaller expression is an upper bound on $C_{CH}(u, q(x_2, x_3, \dots, x_m, z|x_1))$.

Theorem 7. In the case of $m = 2$, the new upper bound on $C_{CH}(2, q(y, z|x))$ equals $\sup_{p(x)} \inf_J [I(X; Y|J) + I(XY; J|Z)]$. This bound strictly improves the $\max_{p(x)} [\min(I(X; Y), I(X; Y|Z))]$ bound proposed by Maurer [7].

IV. PROOFS OF THEOREMS 1-7

In this section, we give brief heuristic sketch of the proofs for the results.

Proof of Theorem 1. The second property of (U_1, \dots, U_p) is equivalent to the following condition: $I(U_i; X_{[m]-\{j\}} | U_{1:i-1} X_j) = 0 \forall i, j : 1 \leq j \leq m, i-j \equiv m \pmod{0}$. Intuitively, assuming that all the X_i 's and Z have learnt $U_{1:i-1}$, the $(i \bmod m)^{th}$ party can create U_i . This random variable is then communicated to all other parties using a random binning algorithm. If all the $m-1$ good parties have more information about U_i than the Eavesdropper, i.e. $\min_{1 \leq r \leq m} I(U_j; X_r | U_{1:j-1}) > I(U_j; Z | U_{1:j-1})$, the parties can exploit this advantage and increase their shared secret key by $\min_{1 \leq r \leq m} I(U_j; X_r | U_{1:j-1}) - I(U_j; Z | U_{1:j-1})$ bits. On the other hand, if $\min_{1 \leq r \leq m} I(U_j; X_r | U_{1:j-1}) < I(U_j; Z | U_{1:j-1})$, U_i can be communicated to all other parties while making sure that this would not destroy more than $I(U_j; Z | U_{1:j-1}) - \min_{1 \leq r \leq m} I(U_j; X_r | U_{1:j-1})$ bits from the previously generated secret key.

In order to prove that the new lower bound strictly improves the maximum of the two one way lower bounds, we use the example and proof technique provided by Ahlswede and Csiszár in [3].

Proof of Theorem 2. In order to prove that $\inf_{f, J} f^{-1}(f(S(X_1; X_2; \dots; X_u; (X_{u+1})^{(s)} \dots; (X_m)^{(s)} \| J))) + S_{f-one-way}(X_1 X_2 \dots X_m; J^{(s)} \| Z)$ is an upper bound on $S(X_1; X_2; \dots; X_u; X_{u+1}^{(s)} \dots; X_m^{(s)} \| Z)$, it is sufficient to verify the five conditions of Theorem 1 of [4]. The following facts were used in the proof: 1. The convexity of f implies that it is continuous and that $f(x+a) - f(x)$ is an increasing function in x for any fixed a 2. Without loss of generality we can assume $f(0) = 0$, because $S_{f-one-way}(X; Y^{(s)} \| Z)$ and $f^{-1}(f(a) + b)$ (for any non-negative a and b) are invariant with respect to shifts in f .

Proof of Theorem 3. The proof techniques are very similar to the ones used in Lemma 2 and appendix A of [1].

Proof of Theorem 4. $C_{CH}(u, q(x_2, x_3, \dots, x_m, z|x_1))$ is lower bounded by

$\sup_{p(x_1)} S(X_1; X_2; \dots; X_u; (X_{u+1})^{(s)} \dots; (X_m)^{(s)} \| Z)$ because the first party can always insert i.i.d. repetitions of any $p(x_1)$ at the input of the broadcast channel [7]. We then apply theorem 1 to lower bound $S(X_1; X_2; \dots; X_u; (X_{u+1})^{(s)} \dots; (X_m)^{(s)} \| Z)$ by $\sum_{j=q}^p [\min_{1 \leq r \leq m} I(U_j; X_r | U_{1:j-1}) - I(U_j; Z | U_{1:j-1})]$.

In order to prove that the new lower bound is strictly better than the maximum of the two one way, we designed an example in which the expression $\sup_{p(x_1)} \max\{\sup_{V-U-X_1-X_2-Z} [I(U; X_2|V) - I(U; Z|V)], \sup_{V-U-X_2-X_1-Z} [I(U; X_1|V) - I(U; Z|V)]\}$ uniquely achieves its supremum at a certain $p(x_1)$, and thereby proved that this expression is strictly smaller than $\sup_{p(x_1)} I(X_1; X_2 \| Z)$ which is achievable by the new lower bound.

Proof of Theorem 5. Fix a probability distribution $q(x_2, \dots, x_m, z|x_1)$ and assume that X_1, X_2, \dots, X_m, Z are taking values from the discrete finite sets Δ_i , $i = 1..m + 1$. For every $\delta > 0$ and $\epsilon > 0$, one can find valid data type $SK_C(n, \epsilon, S_1, S_2, S_3, \dots, S_m, \vec{C}, (M_1, M_2, \dots, M_u), X_1^n, X_2^n, \dots, X_m^n, Z^n)$ whose Gain is within δ interval of $C_{CH}^\epsilon(u, q(x_2, \dots, x_m, z|x_1))$. We have: $n\phi(q(x_2, x_3, \dots, x_m, z|x_1)) \geq (n - 1)\phi(q(x_2, x_3, \dots, x_m, z|x_1)) + \varphi_1(X_1^1; X_2^1; \dots; X_m^1 \| Z^1) \geq (n - 1)\phi(q(x_2, x_3, \dots, x_m, z|x_1)) + \varphi_1(M_1 X_1^1; M_2 X_2^1; \dots; M_u X_u^1; X_{u+1}^1 \dots X_m^1 \| Z^1) \geq (n - 1)\phi(q(x_2, x_3, \dots, x_m, z|x_1)) + \varphi_1(M_1 X_1^1 \vec{C}_1; M_2 X_2^1 \vec{C}_1; \dots; M_u X_u^1 \vec{C}_1; X_{u+1}^1 \vec{C}_1 \dots X_m^1 \vec{C}_1 \| Z^1 \vec{C}_1) \geq i (n - 2)\phi(q(x_2, x_3, \dots, x_m, z|x_1)) + \varphi_2(M_1 X_1^{1:2} \vec{C}_1; M_2 X_2^{1:2} \vec{C}_1; \dots; M_u X_u^{1:2} \vec{C}_1; X_{u+1}^{1:2} \vec{C}_1 \dots X_m^{1:2} \vec{C}_1 \| Z^{1:2} \vec{C}_1) \geq \dots \varphi_n(M_1 X_1^{1:n} \vec{C}_{1:n}; M_2 X_2^{1:n} \vec{C}_{1:n}; \dots; M_u X_u^{1:n} \vec{C}_{1:n}; X_{u+1}^{1:n} \vec{C}_{1:n} \dots X_m^{1:n} \vec{C}_{1:n} \| Z^{1:n} \vec{C}_{1:n}) \geq \varphi_n(S_1; S_2; \dots; S_m \| Z^{1:n} \vec{C}_{1:n}) \geq H(S_1 | Z^{1:n} \vec{C}_{1:n}) - \sum_{j=2}^m H(S_j | S_j) \geq nC_{CH}^\epsilon(u, p(x_2, \dots, x_m, z|x_1)) - n\delta - (m - 1)[h(\epsilon) + \epsilon \cdot n \log \prod_{i=1}^m |\Delta_i|]$

The inequality i is valid because φ satisfies property number 1. The theorem is proved by taking the limit as ϵ and δ go to zero.

Proof of Theorem 6. In order to prove that the suggested expression bounds the secrecy rate from above, it suffices to show that it satisfies all the required properties of Theorem 5. The details are suppressed.

Proof of Theorem 7. The only possible value for $\lambda_{\{1\}}$ and $\lambda_{\{2\}}$ in the case of $m = u = 2$ is one. The upper bound, therefore reduces to $\sup_{p(x)} \inf_J [I(X; Y | J) + I(XY; J | Z)]$. In order to prove that this bound strictly improves the $\max_{p(x)} [\min(I(X; Y), I(X; Y \| Z))]$ bound proposed by Maurer [7], we need to find a conditional distribution $p(yz|x)$ for which the new upper bound is less than Maurer's upper bound. For this, we use the example of Renner and Wolf in [9]. X and Y are taking values from the set $\{0, 1, 2, 3\}$. Assuming that $P(X = i) = p_i$, Table (I) characterizes the conditional probability distribution of Y given X . The conditional distribution of Z given X and Y is specified by

TABLE I
JOINT PROBABILITY DISTRIBUTION OF X AND Y

X					
Y		0	1	2	3
0		$\frac{1}{2}p_0$	$\frac{1}{2}p_1$	0	0
1		$\frac{1}{2}p_0$	$\frac{1}{2}p_1$	0	0
2		0	0	p_2	0
3		0	0	0	p_3

the following equation:

$$Z = \begin{cases} X + Y \pmod{2} & \text{if } X, Y \in \{0, 1\} \\ X & \pmod{2} & \text{if } X \in \{2, 3\} \end{cases}$$

V. CONCLUSION

We derived new lower bounds on the secret key rate that generalize and improve the essentially best lower bound on the secrecy rate. We have provided new upper bounds on the secrecy rate in the general multi-user case. In the case of channel model, this bound strictly improves the currently best upper bound on the secrecy rate. In the source model, the proposed upper bound may improve our previous bound in [4].

ACKNOWLEDGMENT

The authors would like to thank TRUST (The Team for Research in Ubiquitous Secure Technology), which receives support from the National Science Foundation (NSF award number CCF-0424422) and the following organizations: Cisco, ESCHER, HP, IBM, Intel, Microsoft, ORNL, Pirelli, Qualcomm, Sun, Symantec, Telecom Italia and United Technologies for their support of this work. The research was also partially supported by NSF grant numbers CCF-0500023 and CCF-063537.

REFERENCES

- [1] I. Csiszár and P. Narayan, *Secrecy Capacities for Multiple Terminals*, IEEE Trans. Inform. Theory, Vol. 50, No. 12, Dec 2004.
- [2] I. Csiszár and P. Narayan, *Secrecy Capacities for Multiterminal Channel Models*, IEEE International Symposium on Information Theory, pp.2138 - 2141, 2005.
- [3] R. Ahlswede and I. Csiszár, *Common randomness in information theory and cryptography. Part I: Secret sharing*, IEEE Trans. Inform. Theory, Vol. 39, No. 4, pp. 1121 -1132, 1993.
- [4] Amin A. Gohari and V. Anantharam, *Communication for omniscience by a neutral observer and information-theoretic key agreement of multiple terminals*, Proceedings of International Symposium on Information Theory (ISIT), 2007.
- [5] Ueli M. Maurer and S. Wolf, *Unconditionally secure key agreement and the intrinsic conditional information*, IEEE Trans. Inform. Theory, Vol. 45, No.2, pp. 499-514, 1999.
- [6] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, John Wiley and Sons, 1991.
- [7] Ueli M. Maurer, *Secret Key Agreement by Public Discussion From Common Information*, IEEE Trans. Inform. Theory, Vol. 39, pp. 733-742, 1993.
- [8] Ueli M. Maurer and S. Wolf *From Weak to Strong Information-Theoretic Key Agreement*, Proceedings of International Symposium on Information Theory (ISIT), 2000.

- [9] R. Renner and S. Wolf, *New Bounds in Secret-Key Agreement: The Gap Between Formation and Secrecy Extraction*, Proceedings of EUROCRYPT 2003, LNCS, Springer-Verlag, 2003
- [10] I. Csiszár and J. Körner, *Broadcast channels with confidential messages*, IEEE Trans. Inform. Theory, Vol. 24, No. 3, pp. 339-348, 1978.
- [11] A. D. Wyner, *The Wiretap Channel*, Bell System Technical Journal, Vol. 54, No. 8, pp. 1355-1387, 1975.
- [12] C.E. Shannon, *Communication theory of secrecy*, Bell System Technical Journal, Vol. 28, pp. 656-715, Oct 1949.