Key Agreement over a Generalized Multiple Access Channel Using Noiseless and Noisy Feedback

Somayeh Salimi, Mikael Skoglund, Jovan Dj. Golić, Mahmoud Salmasizadeh, and Mohammad Reza Aref

***Abstract*—A secret key agreement framework involving three users is considered in which each of the users 1 and 2 intends to share a secret key with user 3 and users 1 and 2 are eavesdroppers with respect to each other. There is a generalized discrete memoryless multiple access channel (GDMMAC) from users 1 and 2 to user 3 where the three users receive outputs from the channel. Furthermore, there is a feedback channel from user 3 to users 1 and 2 through which user 3 sends information extracted from the received output from the GDMMAC to increase the key rates. We consider both noiseless and noisy feedback. In the case of noiseless feedback, a public channel of unlimited capacity from user 3 to users 1 and 2 is used only once. In the case of noisy feedback, a noisy broadcast channel (BC) from user 3 to users 1 and 2 can be repeatedly used, like GDMMAC. In both setups, inner bounds of the secret key capacity region are derived. The secret key capacity region is derived in some special cases where the channel inputs and outputs form Markov chains in certain orders. For illustration, the corresponding results are also derived and discussed for Gaussian channels. The cases with noiseless feedback, noisy feedback, and no feedback at all are compared with each other.**

***Index Terms*—Secret key agreement, multiple access channel, broadcast channel, wiretap channel, feedback channel, secret key capacity region.**

I. Introduction

AHLSWEDE and Csiszar [1] and Maurer [2] introduced the problem of secret key sharing across the broadcast channel where, in addition to the broadcast channel, there is a noiseless public channel for communication between the transmitter and the receiver through which all communications can be overheard by the eavesdropper. Secret key sharing over a pair of broadcast channels between two legitimate users in the presence of an eavesdropper was investigated in [3]. Furthermore, secrecy has been investigated in other frameworks where a user can be a legitimate user and simultaneously an eavesdropper. The broadcast channel with two confidential messages is investigated in [8] in which the transmitter intends to send independent confidential messages to two receivers where the receivers are eavesdroppers of each other's message. The generalized multiple access channel with two confidential messages is considered in [4] where each of the two transmitters intends to send a message to the receiver and at the same time obtains information about the other transmitter's message through the received output from the channel. Secret key sharing over the generalized multiple access channel has been investigated in [5] where each of the two transmitters wishes to share a secret key with the receiver while keeping it concealed from the other transmitter. In [5], there is a noiseless public channel from the transmitters to the receiver in addition to the generalized multiple access channel.

In this paper, secret key sharing over the generalized multiple access channel is considered in a framework where the receiver can send feedback from the output received over the generalized MAC. It is assumed that there is a generalized discrete memoryless multiple access channel (GDMMAC) in the forward direction from users 1 and 2 to user 3 where all three users receive noisy outputs from the channel. In this framework, users 1 and 2 intend to share secret keys with user 3 while being the eavesdroppers with respect to each other. Users 1 and 2 send information to user 3 over the GDMMAC in the forward direction and user 3 can send them a feedback from the information received over GDMMAC. Two scenarios are considered for transmission of the feedback data in the backward direction.

In the first scenario, there is a noiseless public channel from user 3 to users 1 and 2. In this scenario, which is referred as noiseless feedback, the public channel is of unlimited capacity, but it is insecure and all the information sent by user 3 can be overheard by both users 1 and 2. In the second scenario, referred to as noisy feedback, there is a broadcast channel (BC) in the backward direction from user 3 to users 1 and 2. Due to the noisy nature of the BC, in comparison with the noiseless public channel, less information can be sent back by user 3 compared to the noiseless public channel, but instead, the inherent secrecy of the BC may potentially increase the secret key rates. This scenario can be realized in a wireless network, for example in the case where users 1 and 2 are mobile terminals communicating to a base station (user 3), in uplink mode (the GDMMAC). Furthermore, the base station (user 3) can communicate with users 1 and 2 in downlink mode (public channel or BC), and each of the mobile terminals wishes to share with the base station a secret key hidden from the other user. In the case of noiseless feedback, user 3 exploits a public channel like an Internet connection and in the noisy case, the respective downlink wireless channel is used. Inner bounds of the secret key capacity region for both the scenarios are derived in this paper. For special cases

Manuscript received September 14, 2012; revised March 10, 2013. This work has been supported in part by the Swedish Research Council. The material in this paper was presented in part at the IEEE International Symposium on Information Theory, Saint Petersburg, Russia, Aug. 2011.

S. Salimi and M. Skoglund are with ACCESS Linnaeus Center, School of Electrical Engineering, KTH Royal Institute of Technology, Stockholm, Sweden (e-mail: somayen@kth.se, skoglund@ee.kth.se).

J. Dj. Golić is with the Security Lab., Telecom Italia, Turin 10148, Italy (e-mail: jovan.golic@telecomitalia.it).

M. Salmasizadeh is with Electronics Research Center, Sharif University of Technology, Tehran, Iran (e-mail: salmasi@sharif.edu).

M. R. Aref is with ISSL Lab., Dept. of Electrical Engineering, Sharif University of Technology, Tehran, Iran (email: aref@sharif.edu).

Digital Object Identifier 10.1109/JSAC.2013.130910.

0733-8716/13/$31.00 © 2013 IEEE

where the channel inputs and outputs of the GDMMAC and the BC form Markov chains in certain orders, the secret key capacity region is also obtained. In the first scenario, the effect of using the feedback channel is discussed through a binary-erasure example in which no secret key can be shared between the users without the use of the feedback channel. In the second scenario, another binary example is considered and the bilateral effect of increasing the channel noise from user 3 to user 1 in the backward direction on the secret key capacity region is discussed. Furthermore, the results for the cases with noiseless feedback, noisy feedback, and no feedback at all are compared with each other in the case of Gaussian channels.

The paper is organized as follows. In Section II, the description, results and an example related to the noiseless feedback scenario are presented. The description, results and an example related to the noisy feedback scenario are presented in Section III. The Gaussian case is treated in Section IV. The conclusion and suggestions for future work are given in Section V. Proofs of the main theorems are given in the Appendices. In the paper, a random variable is denoted by an upper case letter and its realization is denoted by the corresponding lower case letter. Also, X_i^N denotes the vector $(X_{i,1}, X_{i,2}, ..., X_{i,N})$, and $X_{i,j}^k$ denotes the vector $(X_{i,j}, X_{i,j+1}, ..., X_{i,k})$, where i denotes the index of the corresponding user.

II. Key Agreement Over GDMMAC Using Noiseless Feedback

A. Preliminaries

There is a GDMMAC with probability distribution $P_{Y_{1f},Y_{2f},Y_{3f}|X_{1f},X_{2f}}$, where users 1 and 2 govern the inputs X_{1f} and X_{2f} and then outputs Y_{1f}, Y_{2f} and Y_{3f} are received by users 1, 2, and 3 respectively. Also, there is an insecure noiseless feedback channel of unlimited capacity from user 3 to users 1 and 2. In this setup, it is assumed that users 1 and 2 are allowed to make n_f uses of the GDMMAC, and then, user 3 is allowed to make one use of the noiseless feedback channel to send back information to users 1 and 2. Using the GDMMAC in the forward direction and the noiseless feedback channel in the backward direction, each of users 1 and 2 intends to share a secret keys with user 3 while keeping it concealed from the other user. For simplicity, like in [4], it is assumed that each of users 1 and 2 uses the outputs of the GDMMAC only to eavesdrop and not as inputs to the encoder. Our results can be easily generalized to the situation where the channel outputs are used by users 1 and 2 as inputs to the encoders of the GDMMAC as in [9], but this is beyond the scope of the present work. We first present the formal definition of the described secret key sharing as shown in Fig.1.

Step 1) n_f uses of the GDMMAC: Users 1 and 2 randomly generate independent keys K_{1f} and K_{2f}, respectively, and then, determine the i-th channel inputs $X_{1f,i}$ and $X_{2f,i}$ to the GDMMAC for $i = 1, 2, ..., n_f$ as stochastic functions of the corresponding keys. Subsequently, the outputs $Y_{1f,i}, Y_{2f,i}$ and $Y_{3f,i}$ are observed by users 1,2, and 3, respectively. User 3 estimates keys $\hat{K}_{1f}$ and $\hat{K}_{2f}$ as a deterministic function of $Y_{3f}^{n_f}$.

Step 2) Noiseless feedback usage: User 3 generates keys K_{1fb} and K_{2fb}, as stochastic functions of $Y_{3f}^{n_f}$ to share with users 1 and 2, respectively, and then, generates F as a stochastic function of $Y_{3f}^{n_f}$ and sends it over the noiseless feedback channel to users 1 and 2. After receiving F over the public channel, estimates $\hat{K}_{1fb}$ and $\hat{K}_{2fb}$ are made by users 1 and 2, respectively, as deterministic functions of the available information.

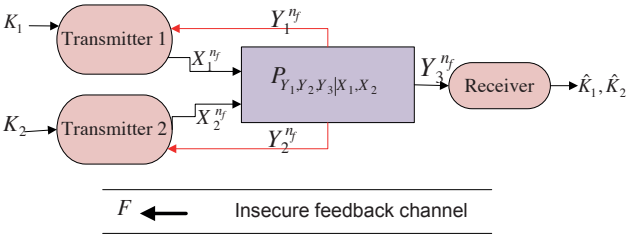


Fig. 1. Secret key sharing over GDMMAC using noiseless feedback channel

After these steps, the key pair (K_{1f}, K_{1fb}) is shared between user l and user 3 and the key pair (K_{2f}, K_{2fb}) is shared between user 2 and user 3. All the above keys take values in some finite sets. Now, we state the conditions that should be met in the described secret key sharing framework.

Definition 1: In the proposed secret key sharing model, (R_1, R_2) is an achievable key rate pair if for every $\varepsilon > 0$ and sufficiently large n_f, there exists a secret key sharing code such that:

$$\tfrac{1}{n_f} H(K_{1f}, K_{1fb}) > R_1 - \varepsilon, \tfrac{1}{n_f} H(K_{2f}, K_{2fb}) > R_2 - \varepsilon \quad (1)$$

$$\Pr\{(K_{if}, K_{ifb}) \neq (\hat{K}_{if}, \hat{K}_{ifb})\} < \varepsilon, i = 1, 2 \quad (2)$$

$$\tfrac{1}{n_f} I(K_{1f}, K_{1fb}; K_{2f}, X_{2f}^{n_f}, Y_{2f}^{n_f}, F) < \varepsilon \quad (3)$$

$$\tfrac{1}{n_f} I(K_{2f}, K_{2fb}; K_{1f}, X_{1f}^{n_f}, Y_{1f}^{n_f}, F) < \varepsilon. \quad (4)$$

Equation (1) means that R_1 and R_2 are the rates of the secret keys shared between user 1 and user 3 and user 2 and user 3, respectively. Equation (2) means that each user can correctly estimate the corresponding keys. Equations (3) and (1) mean that users 1 and 2 effectively have no information about each other's secret keys.

Definition 2: The region containing all the achievable key rate pairs (R_1, R_2) is the secret key capacity region.

B. Main result

Theorem 1: In secret key agreement over the GDMMAC using noiseless feedback, all rate pairs in the closure of the convex hull of the set of all pairs (R_1, R_2) that satisfy the following conditions are achievable:

$$R_1 \geq 0, R_2 \geq 0,$$

$$R_1 \leq [I(T_{1f}; Y_{3f}|T_{2f}) - I(T_{1f}; X_{2f}, Y_{2f}, T_{2fb}, V|T_{2f})]^+ + \overbrace{[I(T_{1fb}; X_{1f}, Y_{1f}|V, T_{1f}) - I(T_{1fb}; X_{2f}, Y_{2f}, T_{2f}, T_{2fb}|V, T_{1f})]^+}^{r_{1fb}},$$

$$R_2 \leq [I(T_{2f}; Y_{3f}|T_{1f}) - I(T_{2f}; X_{1f}, Y_{1f}, T_{1fb}, V|T_{1f})]^+ + \overbrace{[I(T_{2fb}; X_{2f}, Y_{2f}|V, T_{2f}) - I(T_{2fb}; X_{1f}, Y_{1f}, T_{1f}, T_{1fb}|V, T_{2f})]^+}^{r_{2fb}},$$

$$R_1 + R_2 \leq [I(T_{1f}, T_{2f}; Y_{3f}) - I(T_{1f}; X_{2f}, Y_{2f}, T_{2fb}, V|T_{2f}) - I(T_{2f}; X_{1f}, Y_{1f}, T_{1fb}, V|T_{1f})]^+ + r_{1fb} + r_{2fb}$$

for random variables taking values in finite sets according to a distribution of the form:

$$p(t_{1f},t_{2f},x_{1f},x_{2f},y_{1f},y_{2f},y_{3f},t_{1fb},t_{2fb},v)=p(t_{1f})p(t_{2f})\times p(x_{1f}|t_{1f})p(x_{2f}|t_{2f})p(y_{1f},y_{2f},y_{3f}|x_{1f},x_{2f})p(v,t_{1fb},t_{2fb}|y_{3f})$$

The function $[x]^+$ equals x if $x \geq 0$ and 0 if $x < 0$.

The proof of Theorem 1 is not presented since the proof of Theorem 4 includes it as a special case, but intuitive interpretation of Theorem 1 is given below.

In the described setup, secret key agreement between each of the users 1 and 2 with user 3 consists of two steps. In the first step, only the GDMMAC is available and each of the users 1 and 2 agrees on a key with user 3 using the GDMMAC. The first terms on the right-hand side of the bounds on R_1 and R_2 correspond to this step. These terms are obtained using the wiretap codebook by users 1 and 2 and, T_{1f} and T_{2f} are auxiliary random variables relevant to the keys K_{1f} and K_{2f}, respectively. After receiving the GDMMAC outputs by all the users, the public channel is then exploited by user 3 to generate another key with each of the users 1 and 2 through the feedback channel. In this step, the information available to the users can be regarded as correlated sources and, as such, can be used to generate additional secret keys. This step is similar to the source model with a public channel from user 3 to the other two users and the secret sharing codebook for the source model is thus used. The second terms on the right-hand side of the R_1 and R_2 bounds correspond to this step and, T_{1fb} and T_{2fb} are auxiliary random variables relevant to the keys K_{1fb} and K_{2fb}, respectively. The random variable V refers to the common information sent to both users 1 and 2. It should be noted that sending the information over the feedback channel by the user 3 may result in information leakage about the first step keys and hence, the second step keys may affect the first step keys. This fact can be seen in the rates of the first step keys in Theorem 1.

C. Special cases

In the described model, we could not yet derive a general outer bound; however, we investigate some special cases to derive the secret key capacity region.

Theorem 2: When the GDMMAC inputs and outputs form a Markov chain as $(X_{1f},X_{2f})-Y_{2f}-Y_{1f}-Y_{3f}$, the secret key capacity region is as follows:

$$0 \leq R_1 \leq I(Y_{1f};Y_{3f}|Y_{2f}), \qquad R_2 = 0.$$

Achievability can be inferred from Theorem 1 by substituting $T_{1f}=X_{1f},T_{2f}=X_{2f},T_{1fb}=Y_{3f},T_{2fb}=V=\phi$ and using the above Markov chain. The converse is proved in Section VI.A in [6].

Theorem 3: When the GDMMAC inputs and outputs form Markov chains as

$$X_{1f}-(X_{2f},Y_{2f})-Y_{3f}, \quad X_{2f}-(X_{1f},Y_{1f})-Y_{3f}, \quad Y_{1f}-Y_{3f}-Y_{2f},$$

the secret key capacity region is as follows:

$$0 \leq R_1 \leq I(T_{1fb};X_{1f},Y_{1f}|V) - I(T_{1fb};X_{2f},Y_{2f}|V),$$
$$0 \leq R_2 \leq I(T_{2fb};X_{2f},Y_{2f}|V) - I(T_{2fb};X_{1f},Y_{1f}|V).$$

Achievability can be inferred from Theorem 1 by substituting $T_{1f} = T_{2f} = \phi$ and considering random variables T_{1fb}, T_{2fb}, V with the distribution:

$$p(x_{1f},x_{2f},y_{3f},y_{1f},y_{2f},t_{1fb},t_{2fb},v)=p(x_{1f})p(x_{2f})\times p(y_{3f},y_{1f},y_{2f}|x_{1f},x_{2f})p(t_{1fb},t_{2fb}|y_{3f})p(v|t_{1fb},t_{2fb}),$$

which form a Markov chain as $T_{1fb} - Y_{1f} - Y_{2f} - T_{2f}$.

The existence of such random variables T_{1fb} and T_{2fb} can be deduced from the Markov chain $Y_{1f} - Y_{3f} - Y_{2f}$ and is shown in [6]. The converse is proved in Section VI.B in [6].

A practical example of Theorem 3 is presented in the sequel.

Example 1: Consider a situation where the GDMMAC inputs have alphabet $\{-1, 1\}$ and the inputs and outputs relationships at time instant $i = 1, ..., N_f$ are according to:

$$Y_{1f,i} = (X_{2f,i} \times Z_{1,i}), \qquad Y_{2f,i} = (X_{1f,i} \times Z_{2,i}),$$
$$Y_{3f,i} = \{Y_{1f,i} \times E_{1,i}, Y_{2f,i} \times E_{2,i}\},$$

in which $Z_1^{n_f}$ and $Z_2^{n_f}$ are vectors with i.i.d. components over the alphabet $\{-1, 1\}$ with distribution $\Pr(Z_{1,i} = 1) = p_1$ and $\Pr(Z_{2,i} = 1) = p_2$ where $0 < p_1, p_2 \leq 0.5$. $E_1^{n_f}$ and $E_2^{n_f}$ are vectors with i.i.d components over the alphabet $\{0, 1\}$ with distribution $\Pr(E_{1,i} = 0) = p'_1$ and $\Pr(E_{2,i} = 0) = p'_2$ where $0 < p'_1, p'_2 \leq 0.5$. Operation $\times$ has the usual meaning of multiplication and the random variables $(X_{1f,i}, X_{2f,i}, Z_{1,i}, Z_{2,i}, E_{1,i}, E_{2,i})$ are independent of each other. In the above channel, each of the users 1 and 2 receives the other user's input plus a noise from the channel. User 3 receives erased versions of the channel outputs of users 1 and 2 with probabilities p'_1 and p'_2, respectively. The GDMMAC inputs and outputs form Markov chains the same as in Theorem 3. In this example, since user 3 receives degraded versions of the other users' outputs, no secret key can be shared at the first step and the first parts of key rates in Theorem 1 are zero. However, after the channel outputs are received by the users, secret key sharing can be established by user 3 through the noiseless feedback channel. The secret key agreement protocol is such that user 3 considers $Y_{1f,i}$ as the secret key with user 1 when erasure does not happen for the corresponding user, i.e., when $E_{1,i} = 1$ and takes no secret key when erasure happens. Symmetrically, user 3 agrees on a secret key with user 2. User 3 should inform users 1 and 2 whether erasure happens or not so that users 1 and 2 can correctly agree on the secret keys. For this purpose, user 3 sets the random variable V_i to be equal to $(E_{1,i}, E_{2,i})$ and sends it over the public channel. After receiving V_i, user 1 considers $Y_{1f,i}$ as the secret key with user 3 if $E_{1,i} = 1$ and ignores it if $E_{1,i} = 0$. User 2 acts in a symmetric way. By substituting $T_{jfb,i} = Y_{j,i}$ when $E_{j,i} = 1$ and $T_{jfb,i} = \phi$ when $E_{j,i} = 0$ for $j \in \{1, 2\}$ in the second parts of secret key rates in Theorem 1, the following secret key rates are achievable:

$$R_1 \leq (1 - p'_1)h(p_1), \qquad R_2 \leq (1 - p'_2)h(p_2).$$

In this example, the above region is the key capacity region due to an explicit outer bound resulting from Theorem 3 as:

$$R_1 \leq I(T_{1fb};X_{1f},Y_{1f}|V) - I(T_{1fb};X_{2f},Y_{2f}|V)$$
$$\leq I(Y_{3f};X_{1f},Y_{1f}|X_{2f},Y_{2f})$$
$$= I(Y_{3f};Y_{1f}|X_{1f},X_{2f},Y_{2f}) = (1 - p'_1)h(p_1).$$

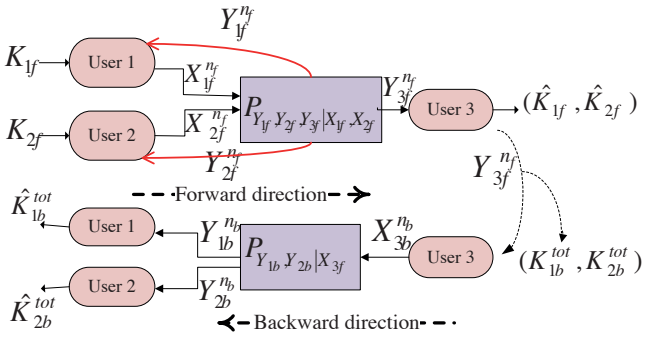


Fig. 2. Secret key sharing using GDMMAC and BC

III. Key Agreement Over GDMMAC Using Noisy Feedback

A. Preliminaries

Users 1, 2 and 3 communicate over a pair of noisy channels. In the forward direction, there is a GDMMAC from users 1 and 2 to user 3 the same as in the previous section. Instead of the noiseless feedback channel, there is a noisy broadcast channel (BC) from user 3 to users 1 and 2 in the backward direction where user 3 governs input X_{3b} of the BC with probability distribution $P_{Y_{1b},Y_{2b}|X_{3b}}$, and outputs Y_{1b} and Y_{2b} are seen by users 1 and 2, respectively. The same as in the previous section, users 1 and 2 intend to share secret keys with user 3 where user 1 is the eavesdropper of user 2's key and vice versa.

We represent the formal definition of the described secret key sharing as shown in Fig.2.

Step 1) n_f uses of the GDMMAC: The same as Step 1 in the noiseless feedback setup.

Step 2) n_b uses of the BC: User 3 generates keys K_{1b}^{tot} and K_{2b}^{tot}, as stochastic functions of $Y_{3f}^{n_f}$ to share with users 1 and 2, respectively, and then, determines the i-th channel input $X_{3b,i}$ to the BC for $i = 1,2,...,n_b$ as a stochastic mapping of $Y_{3f}^{n_f}$. By receiving $Y_{1b}^{n_b}$ and $Y_{2b}^{n_b}$ over the BC by users 1 and 2, estimates $\hat{K}_{1b}^{tot}$ and $\hat{K}_{2b}^{tot}$ are produced as deterministic functions of information available at each of these two users.

After these steps, the key pair (K_{1f}, K_{1b}^{tot}) is shared between user l and user 3 and the key pair (K_{2f}, K_{2b}^{tot}) is shared between user 2 and user 3. All the above keys take values in some finite sets. Now, we state the conditions that should be met in the described secret key sharing framework.

Definition 3: In the proposed secret key sharing model, (R_1, R_2) is an achievable key rate pair if for every $\varepsilon > 0$ and sufficiently large n_f and n_b, there exists a secret key sharing code such that:

$$\frac{1}{n_f+n_b}H(K_{1f}, K_{1b}^{tot}) > R_1 - \varepsilon, \frac{1}{n_f+n_b}H(K_{2f}, K_{2b}^{tot}) > R_2 - \varepsilon \tag{5}$$

$$\Pr\{(K_{if}, K_{ib}^{tot}) \neq (\hat{K}_{if}, \hat{K}_{ib}^{tot})\} < \varepsilon, i = 1, 2 \tag{6}$$

$$\frac{1}{n_f+n_b}I(K_{1f}, K_{1b}^{tot}; K_{2f}, X_{2f}^{n_f}, Y_{2f}^{n_f}, Y_{2b}^{n_b}) < \varepsilon \tag{7}$$

$$\frac{1}{n_f+n_b}I(K_{2f}, K_{2b}^{tot}; K_{1f}, X_{1f}^{n_f}, Y_{1f}^{n_f}, Y_{1b}^{n_b}) < \varepsilon. \tag{8}$$

The above equations have the same meaning as their counterparts in Definition 1.

The secret key capacity region is defined the same way as in Definition 2.

B. Main Results

First, we define parameters with a brief interpretation given after the formulation of Theorem 4:

$$\alpha \triangleq \frac{n_f}{n_f+n_b}, \qquad \bar{\alpha} \triangleq 1-\alpha, \qquad \beta \triangleq \frac{n_b}{n_f} = \frac{1}{\alpha} - 1$$

$$R_{1f} \triangleq \alpha[I(T_{1f}; Y_{3f}|T_{2f}) - I(T_{1f}; X_{2f}, Y_{2f}, T_{2fb}, V|T_{2f})]^+,$$

$$R_{1fb} \triangleq \alpha[I(T_{1fb}; X_{1f}, Y_{1f}|T_{1f}, V) - I(T_{1fb}; X_{2f}, Y_{2f}, T_{2f}, T_{2fb}|T_{1f}, V)]^+,$$

$$R_{2f} \triangleq \alpha[I(T_{2f}; Y_{3f}|T_{1f}) - I(T_{2f}; X_{1f}, Y_{1f}, T_{1fb}, V|T_{1f})]^+,$$

$$R_{2fb} \triangleq \alpha[I(T_{2fb}; X_{2f}, Y_{2f}|T_{2f}, V) - I(T_{2fb}; X_{1f}, Y_{1f}, T_{1f}, T_{1fb}|T_{2f}, V)]^+,$$

$$R_{12f} \triangleq \alpha[I(T_{1f}, T_{2f}; Y_{3f}) - I(T_{1f}; X_{2f}, Y_{2f}, T_{2fb}|T_{2f}) - I(T_{2f}; X_{1f}, Y_{1f}, T_{1fb}|T_{1f})]^+,$$

$$R_{1b} \triangleq \bar{\alpha}[I(T_{1b}; Y_{1b}|U) - I(T_{1b}; Y_{2b}, T_{2b}|U)]^+,$$

$$R_{2b} \triangleq \bar{\alpha}[I(T_{2b}; Y_{2b}|U) - I(T_{2b}; Y_{1b}, T_{1b}|U)]^+ \tag{9}$$

Theorem 4: In the described setup, all key rates in the closure of the convex hull of the set of all pairs (R_1, R_2) that satisfy the following region, are achievable:

$$R_1 \geq 0, R_2 \geq 0$$
$$R_1 \leq R_{1f} + R_{1fb} + R_{1b}, \qquad R_2 \leq R_{2f} + R_{2fb} + R_{2b},$$
$$R_1 + R_2 \leq R_{12f} + R_{1fb} + R_{2fb} + R_{1b} + R_{2b}, \tag{10}$$

subject to the constraints in (11) on the top of the next page, for any $0 < \alpha < 1$ and random variables taking values in finite sets according to a distribution of the form:

$$p(t_{1f}, t_{2f}, x_{1f}, x_{2f}, y_{1f}, y_{2f}, y_{3f}, t_{1fb}, t_{2fb}, v, u, t_{1b}, t_{2b}, x_{3b}, y_{1b}, y_{2b}) = p(t_{1f})p(t_{2f})p(x_{1f}|t_{1f})p(x_{2f}|t_{2f})p(y_{1f}, y_{2f}, y_{3f}|x_{1f}, x_{2f}) \times p(v, t_{1fb}, t_{2fb}|y_{3f})p(u, t_{1b}, t_{2b})p(x_{3b}|t_{1b}, t_{2b}, u)p(y_{1b}, y_{2b}|x_{3b}).$$

The proof of Theorem 4 is given Appendix I. Here, the justification of the above rates is given. As seen in (10), user 1's secret key rate consists of three components. The first term, R_{1f}, is the rate of the key (K_{1f}) that can be generated by user 1 and shared between user 1 and user 3 in the forward direction using only the GDMMAC. The wiretap codebook is used for this step, and the same as in Theorem 1, T_{1f} and T_{2f} are auxiliary random variables related to the keys of this step. The second term, R_{1fb}, is the rate that could be generated from the correlated observations received from GDMMAC; meaning that the channel outputs of the GDMMAC can be regarded as correlated source observations at the users for secret key generation. The secret sharing codebook for the source model is used for this step. For this purpose, user 3 generates K_{1fb} as a function of the received output from GDMMAC for sharing with user 1 and the required information should be sent by user 3 over the BC in the backward direction. The same as in Theorem 1, T_{1fb} and T_{2fb} are auxiliary random variables related to the keys of this step and the random variable V refers to the common information sent to both users 1 and 2. Unlike in Theorem 1, the feedback channel is noisy and the required information sent by user 3 should satisfy the constraints of the BC. The rates of the information

$$\begin{aligned}
&\max\{I(V;Y_{3f}|X_{1f},Y_{1f},T_{1f}),I(V;Y_{3f}|X_{2f},Y_{2f},T_{2f})\}\le\beta\min\{I(U;Y_{1b}),I(U;Y_{2b})\}\\
&\max\{I(V;Y_{3f}|X_{1f},Y_{1f},T_{1f}),I(V;Y_{3f}|X_{2f},Y_{2f},T_{2f})\}+I(T_{1fb};Y_{3f}|V,X_{1f},Y_{1f},T_{1f})\le\beta I(U,T_{1b};Y_{1b}),\\
&\max\{I(V;Y_{3f}|X_{1f},Y_{1f},T_{1f}),I(V;Y_{3f}|X_{2f},Y_{2f},T_{2f})\}+I(T_{2fb};Y_{3f}|V,X_{2f},Y_{2f},T_{2f})\le\beta I(U,T_{2b};Y_{2b}),\\
&\max\{I(V;Y_{3f}|X_{1f},Y_{1f},T_{1f}),I(V;Y_{3f}|X_{2f},Y_{2f},T_{2f})\}+I(T_{1fb};Y_{3f}|V,X_{1f},Y_{1f},T_{1f})+I(T_{2fb};Y_{3f}|V,X_{2f},Y_{2f},T_{2f})+\\
&I(T_{1fb};T_{2fb}|V,Y_{3f})\le\beta[\min\{I(U;Y_{1b}),I(U;Y_{2b})\}+I(T_{1b};Y_{1b}|U)+I(T_{2b};Y_{2b}|U)-I(T_{1b};T_{2b}|U)],
\end{aligned}\tag{11}$$

to be transmitted by user 3 are on the left-hand sides of (11) according to Wyner-Ziv coding for this problem and this information should be subject to rate limitations of the BC with common message in the backward direction which is shown as the Marton-Gelfand-Pinsker region [10] on the right-hand sides of (11). The third component, R_{1b}, is the rate of the key (K_{1b}) that can be shared between users 1 and 3 exploiting the inherent secrecy of the BC and using the wiretap codebook. T_{1b} and T_{2b} are auxiliary random variables relevant to the keys of this step and the random variable U refers to the common message sent to both users 1 and 2. Hence, a combination of secret sharing codebook, Gelfand-Pinsker coding, Wyner-Ziv coding and wiretap codebook is used in the backward direction. In this sense, the total key shared between user 1 and user 3 in the backward direction i.e., K_{1b}^{tot} in Definition 3, constitutes of two keys K_{1fb} and K_{1b}. User 2's key rate and the sum rate can be justified in the same way.

Remark 1: If we cancel the BC by setting $X_{3b}=Y_{1b}=Y_{2b}=T_{1b}=T_{2b}=T_{1fb}=T_{2fb}=U=V=\phi$ in Theorem 4, the region reduces to the secrecy rate region of the GDMMAC with two confidential messages as discussed in [4] where the transmitters are eavesdropper with respect to each other.

Remark 2: If we cancel the GDMMAC by setting $T_{1f}=T_{2f}=X_{1f}=X_{2f}=Y_{1f}=Y_{2f}=Y_{3f}=T_{1fb}=T_{2fb}=V=\phi$ in Theorem 4, the region reduces to the secrecy rate region of the BC with two confidential messages as discussed in [8] where the BC's receivers are eavesdroppers with respect to each other.

Remark 3: If we convert the BC to a noiseless public channel with sufficiently large capacity in the backward direction by setting $T_{1b}=T_{2b}=\phi,U=X_{3b}=Y_{1b}=Y_{2b}$ and considering $H(X_{3b})$ greater than $\max(H(Y_{3f}|X_{1f},Y_{1f}),H(Y_{3f}|X_{2f},Y_{2f}))$ in Theorem 4, the region reduces to the secret key rate region of the GDMMAC with noiseless feedback channel as in Theorem 1. Hence, in the proof of Theorem 4, if we relax Gelfand-Pinsker coding as well as the wiretap codebook related to the BC, then the proof holds for noiseless feedback and thus results in Theorem 1.

C. Special Case

In this section, we derive the secret key capacity region for a special case.

Theorem 5: When the GDMMAC and BC inputs and outputs form Markov chains as $(X_{1f},X_{2f})-Y_{2f}-Y_{1f}-Y_{3f}$ and $X_{3b}-Y_{1b}-Y_{2b}$, the secret key capacity region is the set of all rate pairs (R_1,R_2) that satisfy:

$$R_1\le\alpha I(T_{1fb};Y_{1f}|Y_{2f})+\bar{\alpha}I(X_{3b};Y_{1b}|Y_{2b}),\qquad R_2=0,$$

subject to the constraint:

$$I(T_{1fb};Y_{3f}|Y_{1f})\le\beta I(X_{3b};Y_{1b})$$

for random variables taking values in finite sets according to a distribution of the form:

$$\begin{aligned}
&p(x_{1f},x_{2f},y_{1f},y_{2f},y_{3f},t_{1fb},x_{3b},y_{1b},y_{2b})=p(x_{1f})p(x_{2f})\times\\
&p(y_{1f},y_{2f},y_{3f}|x_{1f},x_{2f})p(t_{1fb}|y_{3f})p(x_{3b})p(y_{1b},y_{2b}|x_{3b})
\end{aligned}$$

Achievability can be inferred from Theorem 4 by substituting $T_{1f}=T_{2f}=T_{2fb}=T_{2b}=U=V=\phi,T_{1b}=X_{3b}$, and using the above Markov chains. The converse is proved in Appendix II.

In this case, due to Markov chains $(X_{1f},X_{2f})-Y_{2f}-Y_{3f}$ and $(X_{1f},X_{2f})-Y_{1f}-Y_{3f}$, none of users 1 and 2 can share a secret key with user 3 in the forward direction using just the GDMMAC. However, after the GDMMAC outputs are received in the forward direction by the three users, secret key sharing can be established by user 3 through the noisy BC. For this purpose, user 3 uses the correlation between the received output from the GDMMAC to share a secret key to user 1. The required information is sent to user 1 over the backward BC by user 3 and the rate constraint in Theorem 5 is due to this fact. It is evident that no secret key can be shared between user 3 and user 2 using the GDMMAC outputs due to Markov chain $Y_{2f}-Y_{1f}-Y_{3f}$. At the same time, user 3 can agree on another secret key with user 1 exploiting the inherent secrecy of the backward BC which is in favor of user 1 due to Markov chain $X_{3b}-Y_{1b}-Y_{2b}$. As none of the channels are in favor of user 2, no secret key can be shared between user 2 and user 3. With these arguments, achievability of the above region is justified.

In the following, a practical example of secret key sharing in our framework is presented.

Example 2: Consider binary GDMMAC and BC with all channels inputs and outputs alphabets over $\{0,1\}$. The GDMMAC and BC input-output relationships at time instant i are according to:

$$\begin{aligned}
&Y_{2f,i}=X_{1f,i}\cdot X_{2f,i},Y_{1f,i}=Y_{2f,i}\oplus E_{1,i},Y_{3f,i}=Y_{1f,i}\oplus E_{2,i},\\
&Y_{2b,i}=X_{3b,i}\oplus E_{3,i},\qquad Y_{1b,i}=Y_{2b,i}\oplus E_{4,i},
\end{aligned}$$

in which $E_{j,i}$ is a binary random variable with the distribution $\Pr(E_{j,i}=1)=p_j$ where $0<p_j\le 0.5$ for $j=1,..,4$. The random variables $E_{j,i}$ for $j=1,..,4$ are independent of each other. In this example, it can be seen that no secret key can be shared using just the GDMMAC in the forward direction due to Markov chain between the channel inputs and outputs of GDMMAC. However, the channel outputs of the GDMMAC can be used by user 3 as source observations and secret key agreement can be established between users 3 and 1 due to the Markov chain $Y_{2f}-Y_{1f}-Y_{3f}$. In fact, the correlation between the noises received by users 1 and 3 from GDMMAC is the potential to generate secrecy and this necessitates sending the required information of the source common randomness through the BC from user 3 to user 1. It should be noted that due to the Markov chain $X_{3b}-Y_{2b}-Y_{1b}$, the backward channel is favorable for user 2 to generate secrecy. Indeed, the backward channel from user 3 to user 1 just serves as

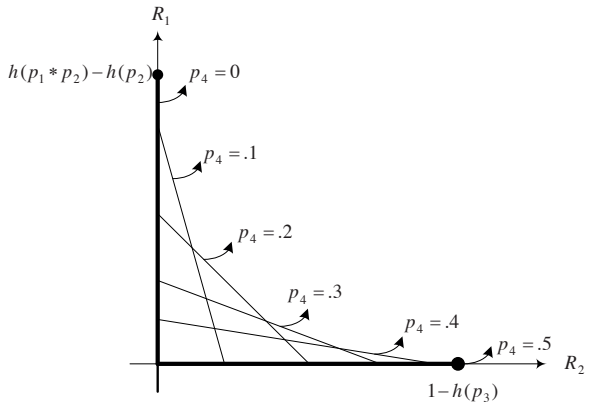


Fig. 3. The secret key rate regions of noisy feedback for different values of noise p_4

a public channel with limited capacity. In this example, we assume fixed value for the parameter p_j for $j=1,2,3$ and investigate the impact of varying p_4 on the secret key rate region. By substituting $T_{1f}{=}T_{2f}{=}T_{2fb}{=}T_{1b}{=}V{=}\phi, T_{2b}{=}X_{3b}$ in Theorem 4, the secret key rate region is shown for six values of p_4 in Fig. 3. For $p_4=0$, the users 1 and 2 receive same outputs from the BC and so no secret key can be shared between users 2 and 3. In this state, the BC serves as a public channel with limited capacity from user 3 to user 1 to send the required information and assuming $h(p_2)+h(p_3)<1$, we have $R_1 \leq h(p_1*p_2)-h(p_2)$ where $p_1{*}p_2{=}p_1{+}p_2{-}2p_1p_2$. As p_4 increases, the secret key rate between users 3 and 2 would increase as user 1 receives a more noisy output from BC with respect to user 2's received output. On the other hand, increment of p_4 worsen the backward channel from user 3 to 1 and hence, less information can be sent from user 3 to user 1 and this results in reducing the secret key rate between users 3 and 1. Therefore, increment of p_4 has a two-side effect on the secret key rate region. As p_4 reaches to 0.5, the backward channel from user 3 to user 1 becomes a completely random channel and the secret key sharing would be possible just between users 3 and 2 and we have $R_2 \leq 1-h(p_3)$.

IV. Gaussian Channels

In this section, we consider secret key sharing in the described setups where the channels are Gaussian. To clarify the effect of using feedback, first, we investigate the Gaussian case where there is a correlation between the noises received by users 1 and 3 over the Gaussian MAC. We examine noiseless and noisy feedback in Examples 3 and 4, respectively. Then the general scenario with independent noises is considered.

Example 3 (noiseless feedback): Consider a Gaussian MAC described by:

$$Y_{3f,i}=X_{1f,i}{+}X_{2f,i}{+}E_{3f,i},$$
$$Y_{1f,i}=X_{1f,i}{+}X_{2f,i}{+}E_{3f,i}{+}E_{1f,i},$$
$$Y_{2f,i}=X_{1f,i}{+}X_{2f,i}{+}E_{2f,i},$$

in which $E_{if} \sim \mathcal{N}(0,N_{if})$ for $i=1,2,3$ and are all i.i.d.. Power constraints P_1 and P_2 hold for users 1 and 2, respectively. This Gaussian MAC can be realized in a wireless environment where user 3, as a base station, receives the output and then sends versions of this output to the other users. The setup between the users is in such a way that user 3 amplifies the received output and retransmits it to user 1. This amplify-and-forward strategy results in correlated noises between users 1 and 3. On the other hand, user 3 computes the sum of the signals sent by users 1 and 2 and sends it to user 2. Hence, by using this compute-and-forward strategy by user 3, user 2 receives an independent noise through the Gaussian MAC.

In this example, user 1 receives a degraded version of user 3's output through the generalized MAC. In other words, there is a Markov chain as $Y_{2f}-(X_{1f},X_{2f})-Y_{3f}-Y_{1f}$ between the channel inputs and outputs of the generalized MAC. The correlation between the output noises of user 1 and 3 can be exploited by user 3 to increase the rate of the secret key shared between them.

By the standard arguments corresponding to the discrete channel arguments, the obtained results can be extended to the Gaussian case. By substituting $T_{1f}{=}X_{1f}, T_{2f}{=}X_{2f}, T_{1fb}{=}Y_{3f}, T_{2fb}=V=\phi$ in Theorem 1 the secret key rate pair $(A_1,0)$ is achievable and by substituting $T_{1f}=X_{1f}, T_{2f}=X_{2f}, T_{1fb}=T_{2fb}=V=\phi$ in Theorem 1 the secret key rate pair $(0,A_2)$ is achievable where:

$$A_1=0.5([\log(1+\tfrac{P_1}{N_{3f}})-\log(1+\tfrac{P_1}{N_{2f}})]^+ + \log(1+\tfrac{(N_{3f}-N_{1f})P_2+N_{2f}}{(P_2+N_{3f})N_{1f}})),$$
$$A_2=0.5\log(1+\tfrac{N_{1f}P_2}{N(P_2+N_{1f}+N_{3f})}).$$

After convexification, the key rate region is obtained as:

$$0\leq R_1, \qquad 0\leq R_2, \qquad \frac{R_1}{A_1}+\frac{R_2}{A_2}\leq 1.$$

In this example, if there is no feedback channel, the key rate region would be the same as above with the difference in equations given as $A_1=0.5([\log(1+\frac{P_1}{N_{3f}})-\log(1+\frac{P_1}{N_{2f}})]^+$.

Example 4 (noisy feedback): Consider the Gaussian MAC as in Example 3 and the BC described by:

$$Y_{1b,i}=X_{3b,i}+E_{1b,i}, \qquad Y_{2b,i}=X_{3b,i}+E_{2b,i},$$

in which $E_{jb}\sim\mathcal{N}(0,N_{jb})$ for $j=1,2$ and are all i.i.d.. We assume that $N_{2b}\leq N_{1b}$. Power constraints P_1, P_2 and P_3 hold for users 1, 2 and 3, respectively. The same Markov chain as in Example 3 holds and due to the correlation between the noises received over the generalized MAC, user 3 sends information through the feedback channel to increase secrecy, but, in this example, the required information sent by user 3 should be subject to the rate constraint of the backward BC from user 3 to user 1. Hence, we cannot set $T_{1fb}{=}Y_{3f}$ anymore as it may exceed the rate of the backward channel from user 3 to user 1. To apply this rate constraint, we take $Y_{3f}=U_{1f}+D_{1f}$ in Theorem 4 where $U_{1f}\sim\mathcal{N}(0,P_{1f}), D_{1fb}\sim\mathcal{N}(0,P_1+P_2+N_{3f}-P_{1f})$ and U_{1f} is independent of D_{1f}. In fact U_{1f} is part of Y_{3f} that can be sent through the BC by user 3 to user 1. On the other hand, the backward BC as a scalar Gaussian broadcast channel can be considered as a degraded broadcast channel and without loss of generality, we take $X_{3b}=U_{1b}+D_{1b}$ in Theorem 4 where $U_{1b}{\sim}\mathcal{N}(0,P_{1b}), D_{1b}{\sim}\mathcal{N}(0,P_3-P_{1b})$ and U_{1b} is independent of D_{1b}. In this degraded BC, U_{1b} is part of X_{3b} that can be decoded by both users 1 and 2 and the required information is sent by user 3 through that. It is obvious that due to $N_{2b}\leq N_{1b}$, no secret key can be shared

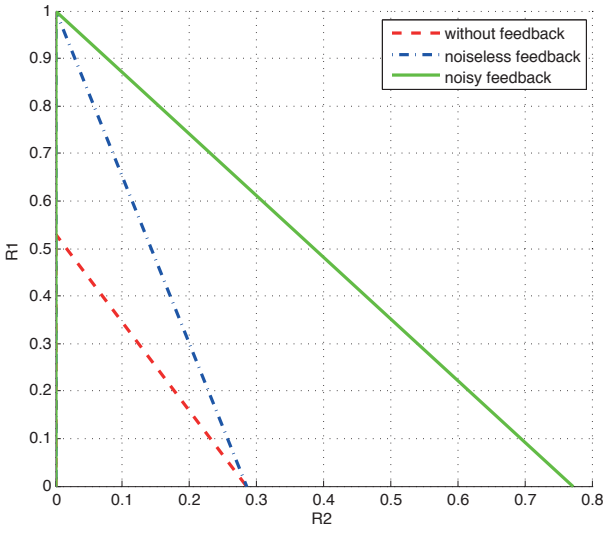


Fig. 4. The effect of feedback for correlated noises over the generalized MAC

between user 3 and user 1 using the inherent secrecy of the BC. By substituting $T_{1f}=X_{1f}, T_{2f}=X_{2f}, V = T_{2fb}= T_{1b}= \phi, T_{1fb} = U_{1f}, U = U_{1b}, T_{2b}=X_{3b}$ in Theorem 4, we deduce Proposition 1.

Proposition 1: Substituting auxiliary random variables as described, the key rate region on the top of the next page is achievable.

For the values $P_1=P_2=P_3=50, N_{1f}=.5, N_{2f}=2, N_{3f}=1, N_{1b}=2, N_{2b}=1$ the rate regions are depicted in Fig. 4 in the cases of no feedback, noiseless feedback and noisy feedback. It can be seen that using the noiseless feedback channel strictly enlarges the secret key rate region when the received noises over the generalized MAC are correlated. When the feedback is noisy, even though the information sent by user 3 to user 1 should satisfy the rate constraint, the inherent secrecy of the noisy BC is useful to increase the rate of the key shared between users 2 and 3. In this example, the noisy nature of the feedback channel almost does not adversely affect the key rate between users 3 and 1 in comparison with the noiseless case and also has a desirable effect on the key rate between users 3 and 2. Although it may seem that the noisy feedback is less useful than the noiseless one, in the case of secret sharing it may be advantageous.

In the following we consider the general Gaussian case where each of the three users receives independent noise through the generalized multiple access channel as in [9].

Example 5 (noiseless feedback): Consider a Gaussian MAC described by:

$$Y_{3f,i}=X_{1f,i}+X_{2f,i}+E_{3f,i}, \quad Y_{1f,i}=X_{1f,i}+X_{2f,i}+E_{1f,i},$$
$$Y_{2f,i} = X_{1f,i}+X_{2f,i}+E_{2f,i},$$

in which the noises distributions and the power constraints are defined similarly to Example 3. In this example, different situations are possible according to the values of the received noises by the users. By substituting the auxiliary random variables in three manners:

$$T_{1fb}=Y_{3f}, T_{1f}= T_{2f}= T_{2fb}=V=\phi,$$
$$T_{2fb}=Y_{3f}, T_{1f}= T_{2f}= T_{1fb}=V=\phi,$$
$$\text{and} \quad T_{1f} = X_{1f}, T_{2f} = X_{2f}, T_{1fb} = T_{2fb} = V = \phi$$

in Theorem 1 and convexifying the region, the following key rate region is achievable:

$$0 \le R_1, \qquad 0 \le R_2, \qquad \frac{R_1}{A_1} + \frac{R_2}{A_2} \le 1.$$

where:

$$A_1 = 0.5 \max([\log(1 + \tfrac{P_1}{N_{3f}}) - \log(1 + \tfrac{P_1}{N_{2f}})]^+,$$
$$\log(1 + [\tfrac{P_1P_2(N_{2f}-N_{1f})+N_{1f}N_{2f}(P_1-P_2)}{(P_1+N_{2f})(P_2(N_{1f}+N_{3f})+N_{1f}N_{3f})}]^+)),$$
$$A_2 = 0.5 \max([\log(1 + \tfrac{P_2}{N_{3f}}) - \log(1 + \tfrac{P_2}{N_{1f}})]^+,$$
$$\log(1 + [\tfrac{P_1P_2(N_{1f}-N_{2f})+N_{1f}N_{2f}(P_2-P_1)}{(P_2+N_{1f})(P_1(N_{2f}+N_{3f})+N_{2f}N_{3f})}]^+)).$$

In this example, if there is no feedback channel, the key rate region would be the same as above with the difference in equations given as $A_1 = 0.5([\log(1 + \frac{P_1}{N_{3f}}) - \log(1 + \frac{P_1}{N_{2f}})]^+$ and $A_2 = 0.5([\log(1 + \frac{P_2}{N_{3f}}) - \log(1 + \frac{P_2}{N_{1f}})]^+$.

Example 6 (noisy feedback): Consider the general Gaussian MAC as in Example 5 and the BC described in Example 4. Even though the received noises over the generalized MAC are independent, using the feedback is useful in the same way as in Example 5, but with the difference that we should consider the rate constraint of the feedback channel. Without loss of generality, we assume $N_{2b} \le N_{1b}$. With the same arguments as in Example 4, we take $Y_{3f} = U_{1f} + D_{1f} = U_{2f} + D_{2f}$ in Theorem 4 where $U_{if} \sim \mathcal{N}(0, P_{if})$, $D_{ifb} \sim \mathcal{N}(0, P_1+P_2+N_{3f}-P_{if})$ and U_{if} is independent of D_{if} for $i = 1, 2$. By substituting the auxiliary random variables in three manners:

$$T_{1fb}=U_{1f}, T_{1b} = X_{3b}, T_{1f}= T_{2f}= T_{2fb}=V= T_{2b} =\phi,$$
$$T_{2fb}=U_{2f}, T_{2b} = X_{3b}, T_{1f}= T_{2f}= T_{1fb}=V= T_{1b} =\phi,$$
$$\text{and} \quad T_{1f}=X_{1f}, T_{2f}=X_{2f}, T_{2b}=X_{3b}, T_{1b}=T_{1fb}=T_{2fb}=V =\phi$$

in Theorem 4 and convexifying the region, we deduce Proposition 2.

Proposition 2: Substituting auxiliary random variables as described before, the key rate region on the next page is achievable.

To numerically analyze the independent noises over the generalized MAC, we consider three cases for Examples 5 and 6. These cases include $N_{3f} < N_{1f} < N_{2f}$, $N_{1f} < N_{3f} < N_{2f}$ and $N_{1f} < N_{2f} < N_{3f}$. In all the three cases, we have $N_{1f} < N_{2f}$. The other three possible cases can be symmetrically analyzed. The values of these noise variances are taken as 1, 1.5 and 2, in the increasing order. The values of the power constraints and the broadcast channel noises are the same as the values considered in Examples 3 and 4. The numerical results are shown in Fig. 5. According to Fig. 5(a), in the case that the noises received by users 1 and 2 over the generalized MAC are greater than the one received by user 3, using the noiseless feedback does not benefit the key rates. In the second case, according to Fig. 5(b), using the noiseless feedback strictly increases the achievable key rate of user 1. In this case, user 2 does not achieve any non-zero key rate unless the noisy feedback is used. In the third case, it is seen that without feedback, any rate pair other than (0,0) would not be

$R_1 > 0, R_2 > 0,$ The rate region of Example 4

$$R_1 \le \tfrac{1}{2}[\log(1+\tfrac{P_1}{N_{3f}}) - \log(1+\tfrac{P_1}{N_{2f}})]^+ + \tfrac{1}{2}\log(1+\tfrac{P_{1f}(P_2(N_{3f}-N_{1f})+N_{3f}^2)}{(P_1+P_2+N_{3f})^2(P_2+N_{1f}+N_{3f})-P_{1f}(P_1N_{1f}+(P_2+N_{3f})(P_1+P_2+N_{3f}))}),$$

$$R_2 \le \tfrac{1}{2}\log(1+\tfrac{P_2N_{1f}(P_1+P_2+N_{3f})(P_1+P_2+N_{3f}-P_{1f})}{N_{3f}[N_{1f}(P_2+N_{3f})(P_1+P_2+N_{3f})+((P_2+N_{3f})^2+P_1(P_2+N_{1f}+N_{3f}))(P_1+P_2+N_{3f}-P_{1f})]})+$$
$$\tfrac{1}{2}\log(1+\tfrac{(P3-P_{1b})(N_{1b}-N_{2b})}{N_{1b}N_{2b}+N_{2b}(P_3-P_{1b})}),$$

$$R_1+R_2 \le \tfrac{1}{2}[\log(1+\tfrac{P_1(N_{2f}-P_2-N_{3f})}{(P_2+N_{3f})(P_1+N_{2f})})+$$
$$\log(1+\tfrac{P_2N_{1f}(P_1+P_2+N_{3f})(P_1+P_2+N_{3f}-P_{1f})}{N_{3f}[N_{1f}(P_2+N_{3f})(P_1+P_2+N_{3f})+((P_2+N_{3f})^2+P_1(P_2+N_{1f}+N_{3f}))(P_1+P_2+N_{3f}-P_{1f})]})]^+ +$$
$$\tfrac{1}{2}\log(1+\tfrac{P_{1f}(P_2(N_{3f}-N_{1f})+N_{3f}^2)}{(P_1+P_2+N_{3f})^2(P_2+N_{1f}+N_{3f})-P_{1f}(P_1N_{1f}+(P_2+N_{3f})(P_1+P_2+N_{3f}))})+\tfrac{1}{2}\log(1+\tfrac{(P3-P_{1b})(N_{1b}-N_{2b})}{N_{1b}N_{2b}+N_{2b}(P_3-P_{1b})}),$$

subject to the constraints:

$$P_{1f} \le P_1+P_2+N_{3f}, \qquad P_{1b} \le P_3,$$

$$P_{1f}N_{1f}(P_2+N_{3f})(P_3+N_{1b}-P_{1b}) \le P_{1b}(P_1+P_2+N_{3f})(P_2+N_{1f}+N_{3f})(P_1+P_2+N_{3f}-P_{1f})$$

$$0 \le R_1, \qquad 0 \le R_2, \qquad \frac{R_1}{B_1}+\frac{R_2}{B_2} \le 1.$$ The rate region of Example 6

Here:

$$B_1 = 0.5\max([\log(1+\tfrac{P_1}{N_{3f}}) - \log(1+\tfrac{P_1}{N_{2f}})]^+,$$
$$\log(1+[\tfrac{P_{1f}(P_1P_2(N_{2f}-N_{1f})+N_{1f}N_{2f}(P_1-P_2))}{(P_1+P_2+N_{3f})(P_1+N_{2f})(P_2+N_{1f})(P_1+P_2+N_{3f}-P_{1f})+P_{1f}(P_1+N_{2f})(P_2(N_{1f}+N_{3f})+N_{1f}N_{3f})}]^+)),$$
$$B_2 = 0.5[\log(1+\tfrac{P_3}{N_{2b}}) - \log(1+\tfrac{P_3}{N_{1b}})]^+ + 0.5\max([\log(1+\tfrac{P_2}{N_{3f}}) - \log(1+\tfrac{P_2}{N_{1f}})]^+,$$
$$\log(1+[\tfrac{P_{2f}(P_1P_2(N_{1f}-N_{2f})+N_{1f}N_{2f}(P_2-P_1))}{(P_1+P_2+N_{3f})(P_1+N_{2f})(P_2+N_{1f})(P_1+P_2+N_{3f}-P_{2f})+P_{2f}(P_2+N_{1f})(P_1(N_{2f}+N_{3f})+N_{2f}N_{3f})}]^+)).$$

and subject to the constraints:

$$P_{1f} \le P_1+P_2+N_{3f} \qquad P_{2f} \le P_1+P_2+N_{3f},$$

$$P_{1f}N_{1b}(P_2(N_{1f}+N_{3f})+N_{1f}N_{3f}) \le P_3(P_2+N_{1f})(P_1+P_2+N_{3f})(P_1+P_2+N_{3f}-P_{1f})$$

$$P_{2f}N_{2b}(P_1(N_{2f}+N_{3f})+N_{1f}N_{3f}) \le P_3(P_1+N_{2f})(P_1+P_2+N_{3f})(P_1+P_2+N_{3f}-P_{2f})$$

---

achievable. According to Fig. 5(c), user 1 can achieve non-zero rate using noiseless feedback, however, noisy feedback should be necessarily used to make possible the key agreement between users 2 and 3.

V. Conclusion

The problem of secret key sharing over a GDMMAC with feedback from the receiver to two transmitters is investigated. Inner bounds of the secret key capacity region are derived for both noiseless and noisy feedback. In some special cases of interest, the outer bound coinciding with the inner bound is also established. In the case of noisy feedback, the inherent secrecy of the BC can increase the key rates, but the constraints on the rates of the feedback information are a deterrent factor. This bilateral effect is discussed through a binary example. In a Gaussian case, the results for the cases of no feedback, noiseless feedback, and noisy feedback are discussed and mutually compared. By using essentially the same coding techniques, the results in Theorems 1 and 4 can be extended to the case where there are more than two network users and each of them intends to share a secret key with the base station hiddenly from the other users.

Appendix I: Proof of Theorem 4

We fix the distribution to be of the form as in Theorem 4. As described in Section III, the secret key sharing is established in two steps; n_f uses of the GDMMAC and n_b uses of the BC. In continue, we describe code construction, encoding and decoding of the two steps separately.

First, we consider using the GDMMAC. Users 1 and 2 independently generate typical sequences $t_{1f}^{n_f}$ and $t_{2f}^{n_f}$, respectively, each with probability $p(t_{jf}^{n_f}) = \prod_{i=1}^{n_f} p(t_{jf,i}), j = 1, 2.$

The numbers of sequences $t_{1f}^{n_f}$ and $t_{2f}^{n_f}$ are $2^{n_f(r_{1f}+r'_{1f})}$ and $2^{n_f(r_{2f}+r'_{2f})}$, respectively, and they are labeled as:

$$t_{1f}^{n_f}(k_{1f},k'_{1f}), k_{1f} \in \mathcal{K}_{1f} = \{1,\ldots,2^{n_f r_{1f}}\}, k'_{1f} \in \mathcal{K}'_{1f} = \{1,\ldots,2^{n_f r'_{1f}}\},$$
$$t_{2f}^{n_f}(k_{2f},k'_{2f}), k_{2f} \in \mathcal{K}_{2f} = \{1,\ldots,2^{n_f r_{2f}}\}, k'_2 \in \mathcal{K}'_{2f} = \{1,\ldots,2^{n_f r'_{2f}}\},$$

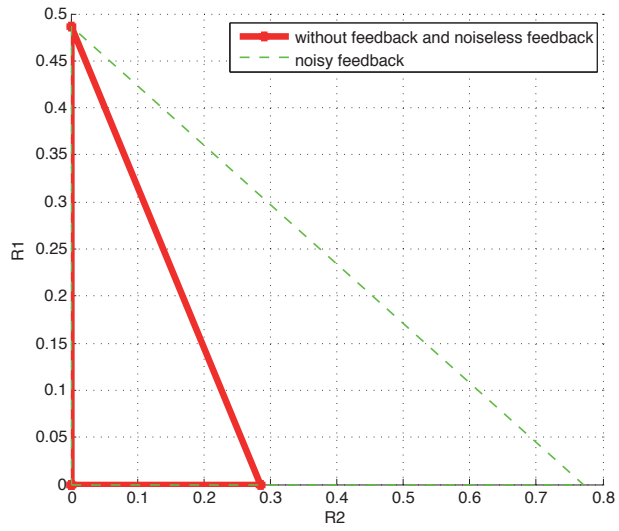
where

$$r'_{1f} = I(T_{1f}; T_{2f}, X_{2f}, Y_{2f}, T_{2fb}) - \varepsilon',$$
$$r'_{2f} = I(T_{2f}; T_{1f}, X_{1f}, Y_{1f}, T_{1fb}) - \varepsilon' \qquad (12)$$

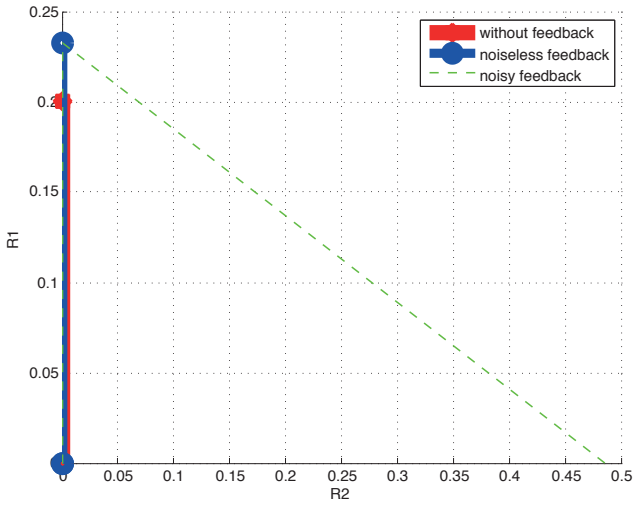
in which $\varepsilon' > 0$ can be arbitrarily small.

For the first step encoding, when a key index k_{1f} is chosen by user 1, an index k'_{1f} is randomly selected and then for $t_{1f}^{n_f}(k_{1f}, k'_{1f})$, the channel input $x_{1f}^{n_f}$ is sent according to the distribution $p(x_{1f}|t_{1f})$. The same is performed by user 2.

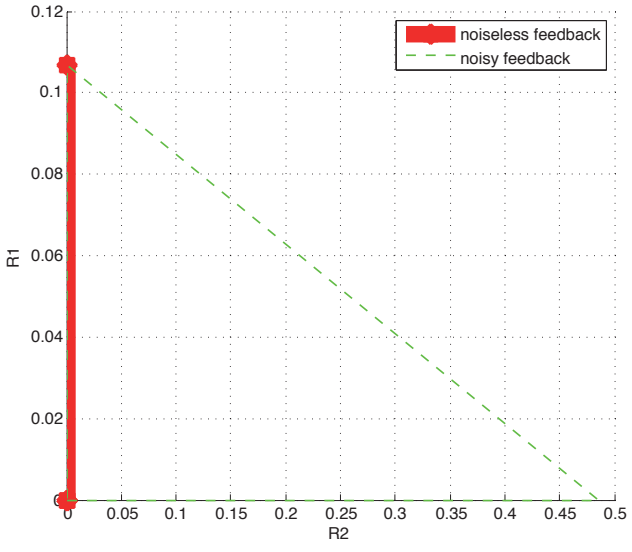
For the first step decoding, user 3 declares error unless there exists a unique $(t_{1f}^{n_f}(k_{1f}, k'_{1f}), t_{2f}^{n_f}(k_{2f}, k'_{2f}))$ such that for the received $y_{3f}^{n_f}$, $(t_{1f}^{n_f}, t_{2f}^{n_f}, y_{3f}^{n_f}) \in A_{\varepsilon_1}^{n_f}(P_{T_{1f},T_{2f},Y_{3f}})$.



(a) $N_{3f}=1, N_{1f}=1.5, N_{2f}=2$



(b) $N_{1f}=1, N_{3f}=1.5, N_{2f}=2$



(c) $N_{1f}=1, N_{2f}=1.5, N_{3f}=2$

Fig. 5. The effect of feedback for independent noises over the generalized MAC

It can be seen that if we set:

$$\begin{aligned}&r_{1f}<I(T_{1f};Y_{3f}|T_{2f})-I(T_{1f};X_{2f},Y_{2f},T_{2fb}|T_{2f}),\\&r_{2f}<I(T_{2f};Y_{3f}|T_{1f})-I(T_{2f};X_{1f},Y_{1f},T_{1fb}|T_{1f}),\\&r_{1f}+r_{2f}<I(T_{1f},T_{2f};Y_{3f})-I(T_{1f};X_{2f},Y_{2f},T_{2fb}|T_{2f})-\\&I(T_{2f};X_{1f},Y_{1f},T_{1fb}|T_{1f}),\end{aligned}\tag{13}$$

then the decoding error probability of this step could be made arbitrarily small.

At the end of the first step, user 3 generates secret keys of the second step as stochastic functions of the channel output y_{3f}^{nf} and sends required information to users 1 and 2 via the backward BC. In this step, secret key codebook for correlated sources as well as wiretap codebook for channel are used. First, user 3 generates $2^{n_f r_{0fb}}$ sequences $v^{nf}(k_{0fb})$ over $A_{\varepsilon''}^{n_f}(V)$ where $k_{0fb}\in\mathcal{K}_{0fb}=\{1,...,2^{n_f r_{0fb}}\}$ and:

$$r_{0fb}=I(V;Y_{3f})+\varepsilon''\tag{14}$$

in which $\varepsilon''>0$ can be chosen arbitrarily small. $2^{n_f r_{0fb}}$ sequences v^{nf} are randomly distributed into $2^{n_f r_{00fb}}$ bins with bin indices $k_{00fb}\in\mathcal{K}_{00fb}=\{1,...,2^{n_f r_{00fb}}\}$. For each v^{nf}, user 3 chooses $2^{n_f r_1}$ sequences t_{1fb}^{nf} over $A_{\varepsilon''}^{n_f}(T_{1fb}|V)$. Similarly $2^{n_f r_2}$ sequences t_{2fb}^{nf} is generated by user 3. These sequences are labeled using two-layered random binning as:

$$\begin{aligned}&t_{1fb}^{n_f}(k_{1fb},k'_{1fb},k''_{1fb}),k_{1fb}\in\mathcal{K}_{1fb}=\{1,...,2^{n_f r_{1fb}}\},\\&k'_{1fb}\in\mathcal{K}'_{1fb}=\{1,...,2^{n_f r'_{1fb}}\},k''_{1fb}\in\mathcal{K}''_{1fb}=\{1,...,2^{n_f r''_{1fb}}\},\\&t_{2fb}^{n_f}(k_{2fb},k'_{2fb},k''_{2fb}),k_{2fb}\in\mathcal{K}_{2fb}=\{1,...,2^{n_f r_{2fb}}\},\\&k'_{2fb}\in\mathcal{K}'_{2fb}=\{1,...,2^{n_f r'_{2fb}}\},k''_{2fb}\in\mathcal{K}''_{2fb}=\{1,...,2^{n_f r''_{2fb}}\},\end{aligned}$$

where:

$$\begin{aligned}r''_{1fb}&=I(T_{1fb};X_{2f},Y_{2f},T_{2f},T_{2fb},T_{1f},V)-\varepsilon'',\\r''_{2fb}&=I(T_{2fb};X_{1f},Y_{1f},T_{1f},T_{1fb},T_{2f},V)-\varepsilon'',\end{aligned}\tag{15}$$

We have $r_{1fb}+r'_{1fb}+r''_{1fb}=r_1$ and hence, for a $v^{nf}(k_{0fb})$, each sequence $t_{1fb}^{n_f}$ can be determined if the indices $(k_{1fb},k'_{1fb},k''_{1fb})$ are known and vice versa. The same is true for $t_{2fb}^{n_f}$. Furthermore, user 3 generates wiretap codebook for the backward BC which is mixture of wiretap codebook along with Gelfand-Pinsker codebook. For a common message rate r_c, user 3 generates $2^{n_b r_c}$ sequences $u^{nb}(k_c)$ over $A_{\varepsilon'''}^{n_b}(U)$ where $k_c\in\mathcal{K}_c=\{1,...,2^{n_b r_c}\}$. For each u^{n_b}, user 3 chooses $2^{n_b(r_{1b}+r'_{1b}+r_{01b})}$ sequences $t_{1b}^{n_b}$ over $A_{\varepsilon''}^{n_b}(T_{1b}|U)$. Similarly $2^{n_b(r_{2b}+r'_{2b}+r_{02b})}$ sequences $t_{2b}^{n_b}$ is generated by user 3. For each u^{n_b}, using two-layered random binning, the sequences $t_{1b}^{n_b}$ and $t_{2b}^{n_b}$ are labeled as:

$$\begin{aligned}&t_{1b}^{n_b}(k_{1b},k'_{1b},k'_{01b}),k_{1b}\in\mathcal{K}_{1b}=\{1,...,2^{n_b r_{1b}}\},\\&k'_{1b}\in\mathcal{K}'_{1b}=\{1,...,2^{n_b r'_{1b}}\},k_{01b}\in\mathcal{K}_{01b}=\{1,...,2^{n_b r_{01b}}\},\\&t_{2b}^{n_b}(k_{2b},k'_{2b},k'_{02b}),k_{2b}\in\mathcal{K}_{2b}=\{1,...,2^{n_b r_{2b}}\},\\&k'_{2b}\in\mathcal{K}'_{2b}=\{1,...,2^{n_b r'_{2b}}\},k_{02b}\in\mathcal{K}_{02b}=\{1,...,2^{n_b r_{02b}}\},\end{aligned}$$

where

$$r'_{1b}=I(T_{1b};Y_{2b}|T_{2b},U)-\varepsilon''',r'_{2b}=I(T_{2b};Y_{1b}|T_{1b},U)-\varepsilon''',\tag{16}$$

in which $\varepsilon'''>0$ can be arbitrarily small. For a $k_c\in\mathcal{K}_c$ and each $k_{1b}\in\mathcal{K}_{1b}$, $k'_{1b}\in\mathcal{K}'_{1b}$, $\mathcal{T}_{1b,k_c}(k_{1b},k'_{1b})$ denotes the set of $2^{n_b r_{01b}}$ sequences $t_{1b}^{n_b}(k_{1b},k'_{1b},k'_{01b})$. Similarly, for each

$k_c \in \mathcal{K}_c$ and each $k_{2b} \in \mathcal{K}_{2b}$ and $k'_{2b} \in \mathcal{K}'_{2b}$, $\mathcal{T}_{2b,k_c}(k_{2b}, k'_{2b})$ represents the set of $2^{n_b r_{02b}}$ sequences $t^{n_b}_{2b}(k_{2b}, k'_{2b}, k'_{02b})$. For a $k_c \in \mathcal{K}_c$ and each $(k_{1b}, k'_{1b}, k_{2b}, k'_{2b})$ it is defined:

$$\mathcal{T}_{b,k_c}(k_{1b}, k'_{1b}, k_{2b}, k'_{2b}) = \mathcal{T}_{1b,k_c}(k_{1b}, k'_{1b}) \times \mathcal{T}_{2b,k_c}(k_{2b}, k'_{2b}) \bigcap A^{n_b}_{\varepsilon'''}(P_{T_{1b},T_{2b}|U}) \quad (17)$$

Furthermore, functions f_0, f_1 and f_2 are defined as:

$$f_0 : \mathcal{K}_c \to \mathcal{K}_{00fb},$$
$$f_1 : \tilde{\mathcal{T}}_{1b} \times \mathcal{K}_c \to \mathcal{K}'_{1fb} \times \mathcal{K}_{00fb},$$
$$f_2 : \tilde{\mathcal{T}}_{2b} \times \mathcal{K}_c \to \mathcal{K}'_{2fb} \times \mathcal{K}_{00fb},$$
$$\mathcal{K}_c = \{1, ..., 2^{n_b r_c}\},$$

where $\tilde{\mathcal{T}}_{1b}$ is the set of $2^{n_b(r_{1b}+r'_{1b})}$ indices pairs (k_{1b}, k'_{1b}). $\tilde{\mathcal{T}}_{2b}$ is symmetrically defined. Mapping f_0 is a random partitioning of sequences $u^{n_b}(k_c)$ into $2^{n_f r_{00fb}}$ equal-sized parts. Elements of part i are labeled as $(\mathcal{K}_c)_i$. For each $k_c \in \mathcal{K}_c$ and the respective $k_{00fb} = f_0(k_c)$, mapping f_1 is $2^{n_f r_{00fb}}$ random partitioning of indices pairs (k_{1b},k'_{1b}) of sequences $t^{n_b}_{1b}(k_{1b},k'_{1b},k'_{01b})$ into $2^{n_f r'_{1fb}}$ equal-sized parts. Elements of part i are labeled as $(\tilde{\mathcal{T}}_{1b})_i$. Mapping f_2 is similarly defined. For these three functions, we implicitly consider the following assumptions and in the decoding step, it is shown that these assumptions hold according to the rate constraints (11) in Theorem 4:

$$n_f r_{00fb} < n_b r_c,$$
$$n_f(r'_{ifb} + r_{00fb}) < n_b(r_{ib} + r'_{ib} + r_c) \ for \ i = 1, 2 \quad (18)$$

Now, we describe the coding scheme of the second step, i.e., using the BC in the backward direction. In this step, user 3 shares two keys with each of users 1 and 2, one derived from the correlation of GDMMAC outputs at the users and the other derived from the inherent secrecy of the BC. With access to sequence $y^{n_f}_{3f}$, user 3 first chooses a sequence $v^{n_f}(k_{0fb})$ which is $\varepsilon''-$jointly typical with $y^{n_f}_{3f}$. Due to the chosen rate r_{0fb} of these sequences in (14), such sequence exists with negligible error probability. For such $v^{n_f}(k_{0fb})$, user 3 looks for a pair $(t^{n_f}_{1fb}, t^{n_f}_{2fb})$ which is $\varepsilon''-$jointly typical with $y^{n_f}_{3f}$ and declares error if there is no such triple. It can be shown that this error probability would be arbitrarily small if we choose:

$$r_1 > I(T_{1fb};Y_{3f}|V), \quad r_2 > I(T_{2fb};Y_{3f}|V),$$
$$r_1 + r_2 > I(T_{1fb};Y_{3f}|V) + I(T_{2fb};Y_{3f}|V) + I(T_{1fb};T_{2fb}|Y_{3f},V) \quad (19)$$

Then, he selects the respective index k_{1fb} of $t^{n_f}_{1fb}$ and k_{2fb} of $t^{n_f}_{2fb}$ as the second parts of the secret keys with user 1 and user 2, respectively. For these sequences, the respective indices k'_{1fb} and k'_{2fb} are the required information to be sent to user 1 and user 2, respectively, along with the index k_{0fb} of $v^{n_f}(k_{0fb})$ to both of them so that each can decode his corresponding key. User 3 encodes k_{0fb}, k'_{1fb} and k'_{2fb} in such a way that first, he returns the bin index k_{00fb} related to that $v^{n_f}(k_{0fb})$ and then he returns k_c, randomly chosen from $(\mathcal{K}_c)_{k_{00fb}}$ using the mappings f_0. Then, for these k_{00fb} and k_c, user 3 finds the respective random partitioning of f_1 and randomly chooses a pair (k_{1b}, k'_{1b}) from $(\tilde{\mathcal{T}}_{1b})_{k'_{1fb}}$. Similarly, using f_2, (k_{2b}, k'_{2b}) is chosen from $(\tilde{\mathcal{T}}_{2b})_{k'_{2fb}}$ by user 3 with the same k_{00fb} and k_c. For the selected $(k_{1b}, k'_{1b}, k_{2b}, k'_{2b})$, user 3 randomly picks up a pair of sequences $(t^{n_b}_{1b}(k_{1b}, k'_{1b}, k_{01b}), t^{n_b}_{2b}(k_{2b}, k'_{2b}, k_{02b}))$ in $\mathcal{T}_{b,k_c}(k_{1b}, k'_{1b}, k_{2b}, k'_{2b})$ (defined in (17)) and declares error if there is no pair. It can be seen that this error probability can be made arbitrarily small if for large enough value of n_b, we have:

$$r_{01b} + r_{02b} > I(T_{1b}; T_{2b}|U) + \epsilon''' \quad (20)$$

User 3 considers the corresponding indices k_{1b} and k_{2b} as the third parts of the keys to be shared with users 1 and 2, respectively. Then the channel input x^{nb}_{3b} is sent over the BC according to the distributions $p(x_{3b}|t_{1b}, t_{2b}, u)$ by user 3.

For the second step decoding, first, both of the users decode the sequence $u^{n_b}(k_c)$. User 1 chooses the sequences u^{n_b} which is ε_2-jointly typical with the received $y^{n_b}_{1b}$. User 2 acts in the symmetric way. It can be seen that both of the users 1 and 2 can decodes the common message (k_c) with negligible probability of error if the common massage rate satisfies [10]:

$$r_c < \min\{I(U; Y_{1b}), I(U; Y_{2b})\}. \quad (21)$$

Then, user 1 decodes key index k_{1b} if $(t^{n_b}_{1b}(k_{1b},k'_{1b},k_{01b}),y^{n_b}_{1b}) \in A^{n_b}_{\varepsilon'_1}(P_{T_{1b},Y_{1b}}|U)$, when such $t^{n_b}_{1b}$ exists and is unique. Otherwise, it declares error. User 2 acts in the same way. According to broadcast channel with common message [10], the probability of error can be made arbitrarily small if in addition to (21), we have:

$$r_c + r_{1b} + r'_{1b} < r_c + r_{1b} + r'_{1b} + r_{01b} < \min\{I(U; Y_{1b}), I(U; Y_{2b})\} + (I(T_{1b}, Y_{1b}|U),$$

$$r_c + r_{2b} + r'_{2b} < r_c + r_{2b} + r'_{2b} + r_{02b} < \min\{I(U; Y_{1b}), I(U; Y_{2b})\} + (I(T_{2b}, Y_{2b}|U),$$
$$r_c + r_{1b} + r'_{1b} + r_{2b} + r'_{2b} \leq r_c + r_{1b} + r'_{1b} + r'_{01b} + r_{2b} + r'_{2b} + r'_{02b} - I(T_{1b}; T_{2b}|U) \leq \min\{I(U; Y_{1b}), I(U; Y_{2b})\} + (I(T_{1b}, Y_{1b}|U) + I(T_{2b}; Y_{2b}|U) - I(T_{1b}; T_{2b}|U). \quad (22)$$

where the first two inequalities results from correct decoding at users 1 and 2, and the third inequality is deduced from small encoding error probability at user 3 as in (20).

According to (16), (20), (21) and (22) the following rates are achievable for the third parts of the total keys:

$$r_{1b} < I(T_{1b}; Y_{1b}|U) - I(T_{1b}; Y_{2b}, T_{2b}|U),$$
$$r_{2b} < I(T_{2b}; Y_{2.b}|U) - I(T_{2b}; Y_{1b}, T_{1b}|U). \quad (23)$$

Now, user 1 finds the index k_{00fb} using mapping f_0 of the index k_c and tries to decode sequence $v^{n_f}(k_{0fb})$ with access to k_{00fb} and the sequences $(x^{n_f}_{1f}, y^{n_f}_{1f}, t^{n_f}_{1f})$. In the symmetric way, user 2 tries to decode $v^{n_f}(k_{0fb})$. It can be shown that both of the users 1 and 2 can correctly estimate $v^{n_f}(k_{0fb})$ if:

$$r_{00fb} > \max\{n_f I(V;Y_{3f}|X_{1f},Y_{1f},T_{1f}), n_f I(V;Y_{3f}|X_{2f},Y_{2f},T_{2f})\} \quad (24)$$

After that, user 1 finds the mapping $(\tilde{\mathcal{T}}_{1b})_i$ of the pair indices (k_{1b}, k'_{1b}) related to the obtained k_{0fb} and sets $k'_{1fb} = i$. With access to index k'_{1fb} and the sequence $(v^{n_f}, x^{n_f}_{1f}, y^{n_f}_{1f}, t^{n_f}_{1f})$, user 1 decodes se-

quence $t_{1fb}^{n_f}$ if $(t_{1fb}^{n_f}(k_{1fb},k'_{1fb},k''_{1fb}),v^{n_f},x_{1f}^{n_f},y_{1f}^{n_f},t_{1f}^{n_f}) \in A_{\varepsilon_3}^{n_f}(P_{T_{1fb},X_{1f},Y_{1f},T_{1f}}|V)$, when such $t_{1fb}^{n_f}$ exists and is unique. Otherwise, it declares error. User 2 acts in the symmetric way. To achieve arbitrarily small decoding error probability of sequences $t_{1fb}^{n_f}$ and $t_{2fb}^{n_f}$ at users 1 and 2, respectively, and to achieve small encoding error probability at user 3 as in (19), according to Wyner-Ziv coding for similar network as in [7], we should have:

$$\begin{aligned}
&r_{00fb}+r'_{1fb}>n_f[\max\{I(V;Y_{3f}|X_{1f},Y_{1f},T_{1f}),\\
&I(V;Y_{3f}|X_{2f},Y_{2f},T_{2f})\}+I(T_{1fb};Y_{3f}|V,X_{1f},Y_{1f},T_{1f})],\\
&r_{00fb}+r'_{2fb}>n_f[\max\{I(V;Y_{3f}|X_{1f},Y_{1f},T_{1f}),\\
&I(V;Y_{3f}|X_{2f},Y_{2f},T_{2f})\}+I(T_{2fb};Y_{3f}|V,X_{2f},Y_{2f},T_{2f})],\\
&r_{00fb}+r'_{1fb}+r'_{2fb}>n_f[\max\{I(V;Y_{3f}|X_{1f},Y_{1f},T_{1f}),\\
&I(V;Y_{3f}|X_{2f},Y_{2f},T_{2f})\}+I(T_{1fb};Y_{3f}|V,X_{1f},Y_{1f},T_{1f})+\\
&I(T_{2fb};Y_{3f}|V,X_{2f},Y_{2f},T_{2f})+I(T_{1fb};T_{2fb}|V,Y_{3f})], \qquad (25)
\end{aligned}$$

and hence, according to (15) and (19), the following rates are achievable for the second parts of the keys:

$$\begin{aligned}
&r_{1fb}=r_1-r'_{1fb}-r''_{1fb}<\\
&I(T_{1fb};X_{1f},Y_{1f}|T_{1f},V)-I(T_{1fb};X_{2f},Y_{2f},T_{2f},T_{2fb}|T_{1f},V),\\
&r_{2fb}=r_2-r'_{2fb}-r''_{2fb}<\\
&I(T_{2fb};X_{2f},Y_{2f}|T_{2f},V)-I(T_{2fb};X_{1f},Y_{1f},T_{1f},T_{1fb}|T_{2f},V),
\end{aligned} \qquad (26)$$

Then, achievability of the secret key rates in Theorem 4 can be deduced according to (13), (23) and (26). It should be noted that the necessary condition (18) in definition of the functions f_0, f_1 and f_2 holds according to the rate constraint (11) in Theorem 4 and equations (21), (22), (24) and (25).

Now, we should check the security conditions of definition 3. We give the proof of (7) and by symmetry, (8) can be deduced. As the keys (K_{1fb},K_{1b}) are shared in the backward direction, equation (7) can be rewritten as:

$$\begin{aligned}
&I(K_{1f},K_{1fb},K_{1b};K_{2f},X_{2f}^{n_f},Y_{2f}^{n_f},Y_{2b}^{n_b})=\\
&\underbrace{I(K_{1f};K_{2f},X_{2f}^{n_f},Y_{2f}^{n_f},Y_{2b}^{n_b})}_{A}+\\
&\underbrace{I(K_{1fb};K_{2f},X_{2f}^{n_f},Y_{2f}^{n_f},Y_{2b}^{n_b}|K_{1f},K_{1b})}_{B}+\\
&\underbrace{I(K_{1b};K_{2f},X_{2f}^{n_f},Y_{2f}^{n_f},Y_{2b}^{n_b}|K_{1f})}_{C}
\end{aligned}$$

We analyze the three terms separately. Some Markov chains useful in the security analysis are given in (27)-(32) on the top of the next page. These Markov chains arise from the coding scheme.

For term A, we have:

$$\begin{aligned}
&I(K_{1f};K_{2f},X_{2f}^{n_f},Y_{2f}^{n_f},Y_{2b}^{n_b}) \overset{(a)}{\leq} I(K_{1f};T_{2f}^{n_f},X_{2f}^{n_f},Y_{2f}^{n_f},Y_{2b}^{n_b})\\
&\leq I(K_{1f};T_{2f}^{n_f},X_{2f}^{n_f},Y_{2f}^{n_f},Y_{2b}^{n_b},K'_{1fb},K'_{2fb},V^{n_f})\\
&\overset{(b)}{=} I(K_{1f};T_{2f}^{n_f},X_{2f}^{n_f},Y_{2f}^{n_f},K'_{1fb},K'_{2fb},V^{n_f})\\
&\overset{(c)}{\leq} I(K_{1f};T_{2f}^{n_f},X_{2f}^{n_f},Y_{2f}^{n_f},K'_{1fb},T_{2fb}^{n_f},V^{n_f})\\
&=I(K_{1f};T_{2f}^{n_f},X_{2f}^{n_f},Y_{2f}^{n_f},T_{2fb}^{n_f},V^{n_f})\\
&\underbrace{+I(K_{1f};K'_{1fb}|T_{2f}^{n_f},X_{2f}^{n_f},Y_{2f}^{n_f},T_{2fb}^{n_f},V^{n_f})}_{I}\\
&=H(K_{1f})-H(K_{1f}|T_{2f}^{n_f},X_{2f}^{n_f},Y_{2f}^{n_f},T_{2fb}^{n_f},V^{n_f})+I\\
&=H(K_{1f})-H(K_{1f},T_{1f}^{n_f}|T_{2f}^{n_f},X_{2f}^{n_f},Y_{2f}^{n_f},T_{2fb}^{n_f},V^{n_f})\\
&+H(T_{1f}^{n_f}|K_{1f},T_{2f}^{n_f},X_{2f}^{n_f},Y_{2f}^{n_f},T_{2fb}^{n_f},V^{n_f})+I\\
&\overset{(d)}{=} H(K_{1f})-H(T_{1f}^{n_f}|T_{2f}^{n_f},X_{2f}^{n_f},Y_{2f}^{n_f},T_{2fb}^{n_f},V^{n_f})\\
&+H(T_{1f}^{n_f}|K_{1f},T_{2f}^{n_f},X_{2f}^{n_f},Y_{2f}^{n_f},T_{2fb}^{n_f},V^{n_f})+I\\
&\overset{(e)}{\leq} H(K_{1f})-n_fH(T_{1f}|T_{2f},X_{2f},Y_{2f},T_{2fb},V)+n_f\varepsilon_4\\
&+H(T_{1f}^{n_f}|K_{1f},T_{2f}^{n_f},X_{2f}^{n_f},Y_{2f}^{n_f},T_{2fb}^{n_f},V^{n_f})+I\\
&\overset{(f)}{\leq} H(K_{1f})-n_fH(T_{1f}|T_{2f},X_{2f},Y_{2f},T_{2fb},V)+n_f\varepsilon_4+n_f\varepsilon_5+I\\
&\overset{(g)}{\leq} -n_fH(T_{1f}|T_{2f},Y_{3f})+n_f\varepsilon_2+n_f\varepsilon_3+I\leq I+n_f\varepsilon_4+n_f\varepsilon_5\\
&\leq I(K'_{1fb};K_{1f},T_{2f}^{n_f},X_{2f}^{n_f},Y_{2f}^{n_f},T_{2fb}^{n_f},V^{n_f})+n_f\varepsilon_4+n_f\varepsilon_5\\
&\leq I(K'_{1fb};T_{1f}^{n_f},T_{2f}^{n_f},X_{2f}^{n_f},Y_{2f}^{n_f},T_{2fb}^{n_f},V^{n_f})+n_f\varepsilon_4+n_f\varepsilon_5\\
&=H(K'_{1fb})-H(K'_{1fb}|T_{1f}^{n_f},T_{2f}^{n_f},X_{2f}^{n_f},Y_{2f}^{n_f},T_{2fb}^{n_f},V^{n_f})+n_f\varepsilon_4+n_f\varepsilon_5\\
&=H(K'_{1fb})-H(K_{1fb},K'_{1fb},K''_{1fb}|T_{1f}^{n_f},T_{2f}^{n_f},X_{2f}^{n_f},Y_{2f}^{n_f},T_{2fb}^{n_f},V^{n_f})\\
&+H(K_{1fb},K''_{1fb}|K'_{1fb},T_{1f}^{n_f},T_{2f}^{n_f},X_{2f}^{n_f},Y_{2f}^{n_f},T_{2fb}^{n_f},V^{n_f})+n_f\varepsilon_4+n_f\varepsilon_5\\
&\overset{(h)}{=} H(K'_{1fb})-H(T_{1fb}^{n_f}|T_{1f}^{n_f},T_{2f}^{n_f},X_{2f}^{n_f},Y_{2f}^{n_f},T_{2fb}^{n_f},V^{n_f})\\
&+H(K_{1fb},K''_{1fb}|K'_{1fb},T_{1f}^{n_f},T_{2f}^{n_f},X_{2f}^{n_f},Y_{2f}^{n_f},T_{2fb}^{n_f},V^{n_f})+n_f\varepsilon_4+n_f\varepsilon_5\\
&\leq H(K_{1fb})+H(K'_{1fb})-H(T_{1fb}^{n_f}|T_{1f}^{n_f},T_{2f}^{n_f},X_{2f}^{n_f},Y_{2f}^{n_f},T_{2fb}^{n_f},V^{n_f})\\
&+H(K''_{1fb}|K'_{1fb},T_{1f}^{n_f},T_{2f}^{n_f},X_{2f}^{n_f},Y_{2f}^{n_f},T_{2fb}^{n_f},V^{n_f})+n_f\varepsilon_4+n_f\varepsilon_5\\
&\overset{(i)}{\leq} H(K_{1fb})+H(K'_{1fb})-n_fH(T_{1fb}|T_{1f},T_{2f},X_{2f},Y_{2f},T_{2fb},V)+n_f\varepsilon_6\\
&+H(K''_{1fb}|K'_{1fb},T_{1f}^{n_f},T_{2f}^{n_f},X_{2f}^{n_f},Y_{2f}^{n_f},T_{2fb}^{n_f},V^{n_f})+n_f\varepsilon_4+n_f\varepsilon_5\\
&\overset{(j)}{\leq} H(K_{1fb})+H(K'_{1fb})-n_fH(T_{1fb}|T_{1f},T_{2f},X_{2f},Y_{2f},T_{2fb},V)\\
&+n_f\varepsilon_6+n_f\varepsilon_7+n_f\varepsilon_4+n_f\varepsilon_5\\
&=n_f(r_1-r''_{1fb})-n_fH(T_{1fb}|T_{1f},T_{2f},X_{2f},Y_{2f},T_{2fb},V)\\
&+n_f\varepsilon_6+n_f\varepsilon_7+n_f\varepsilon_4+n_f\varepsilon_5\\
&\overset{(k)}{=} n_fr_1-n_fI(T_{1fb};T_{1f},T_{2f},X_{2f},Y_{2f},T_{2fb},V)\\
&+n_f\varepsilon''+n_f\varepsilon_4+n_f\varepsilon_5+n_f\varepsilon_6+n_f\varepsilon_7\\
&=n_fr_1-n_fH(T_{1fb})+n_f\varepsilon''+n_f\varepsilon_4+n_f\varepsilon_5+n_f\varepsilon_6+n_f\varepsilon_7\\
&\overset{(l)}{\leq} 2n_f\varepsilon''+n_f\varepsilon_4+n_f\varepsilon_5+n_f\varepsilon_6+n_f\varepsilon_7.
\end{aligned}$$

In the above equations, (a) follows from the fact that index k_{2f} is one of the indices of $t_{2f}^{n_f}$. (b) is due to Markov chain (28), (c) follows from the fact that index k'_{2fb} is one of the indices of $t_{2fb}^{n_f}$ and (d) follows from the fact that index k_{1f} is one of the indices of $t_{1f}^{n_f}$. To prove (e) and (f), respectively, the same approaches as Lemmas 2 and 3 in [8] can be exploited to show $n_fH(T_{1f}|T_{2f},X_{2f},Y_{2f},T_{2fb},V) \leq H(T_{1f}^{n_f}|T_{2f}^{n_f},X_{2f}^{n_f},Y_{2f}^{n_f},T_{2fb}^{n_f},V^{n_f}) + n_f\varepsilon_4$ and $H(T_{1f}^{n_f}|K_{1f},T_{2f}^{n_f},X_{2f}^{n_f},Y_{2f}^{n_f},T_{2fb}^{n_f},V^{n_f}) \leq n_f\varepsilon_5$. (g) is deduced from the reliable decoding condition of k_{1f}. (h) is due to the fact that a sequence $t_{1fb}^{n_f}$ can be determined when the three indices $(k_{1fb},k'_{1fb},k''_{1fb})$ are known. (i) and (j) can be deduced from the same approaches as Lemmas 2 and 3 in [8]. (k) is directly deduced from the rate definition in

$$(K_{1f}, K_{2f}) - (X_{1f}^{n_f}, X_{2f}^{n_f}) - (Y_{1f}^{n_f}, Y_{2f}^{n_f}, Y_{3f}^{n_f}) \tag{27}$$

$$(X_{1f}^{n_f}, X_{2f}^{n_f}, Y_{1f}^{n_f}, Y_{2f}^{n_f}) - Y_{3f}^{n_f} - (T_{1fb}^{n_f}, T_{2fb}^{n_f}) - (K'_{1fb}, K'_{2fb}, V^{n_f}) - (T_{1b}^{n_b}, T_{2b}^{n_b}, U^{n_b}) - (Y_{1b}^{n_b}, Y_{2b}^{n_b}) \tag{28}$$

$$(T_{1b}^{n_b}(k_{1b}, k'_{1b}), U^{n_b}) - (K'_{2fb}, V^{n_f}) - (T_{1f}^{n_f}, X_{1f}^{n_f}, Y_{1f}^{n_f}, T_{2f}^{n_f}, X_{2f}^{n_f}, Y_{2f}^{n_f}) \tag{29}$$

$$(T_{2b}^{n_b}(k_{2b}, k'_{2b}), U^{n_b}) - (K'_{1fb}, V^{n_f}) - (T_{1f}^{n_f}, X_{1f}^{n_f}, Y_{1f}^{n_f}, T_{2f}^{n_f}, X_{2f}^{n_f}, Y_{2f}^{n_f}) \tag{30}$$

$$T_{1b}^{n_b}(k_{1b}, k'_{1b}) - (T_{2b}^{n_b}, U^{n_b}) - K'_{2fb} \tag{31}$$

$$T_{2b}^{n_b}(k_{2b}, k'_{1b}) - (T_{1b}^{n_b}, U^{n_b}) - K'_{1fb} \tag{32}$$

(15) and (l) from the fact that sequences are chosen from $A_{\varepsilon''}^{n_f}(T_{1fb}|V)$.

For term B, we have:

$$\begin{aligned}
&I(K_{1fb}; K_{2f}, X_{2f}^{n_f}, Y_{2f}^{n_f}, Y_{2b}^{n_b}|K_{1f}, K_{1b})\\
&\le I(K_{1fb}; K_{1f}, K_{2f}, K_{1b}, X_{2f}^{n_f}, Y_{2f}^{n_f}, Y_{2b}^{n_b})\\
&\overset{(a)}{\le} I(K_{1fb}; T_{1f}^{n_f}, T_{2f}^{n_f}, T_{1b}^{n_b}, X_{2f}^{n_f}, Y_{2f}^{n_f}, Y_{2b}^{n_b})\\
&\le I(K_{1fb}; K'_{1fb}, K'_{2fb}, T_{1f}^{n_f}, T_{2f}^{n_f}, T_{1b}^{n_b}, X_{2f}^{n_f}, Y_{2f}^{n_f}, Y_{2b}^{n_b})\\
&\overset{(b)}{=} I(K_{1fb}; K'_{1fb}, K'_{2fb}, T_{1f}^{n_f}, T_{2f}^{n_f}, X_{2f}^{n_f}, Y_{2f}^{n_f})\\
&\le I(K_{1fb}; K'_{1fb}, T_{2fb}^{n_f}, T_{1f}^{n_f}, T_{2f}^{n_f}, X_{2f}^{n_f}, Y_{2f}^{n_f})\\
&= H(K_{1fb}) - H(K_{1fb}|K'_{1fb}, T_{2fb}^{n_f}, T_{1f}^{n_f}, T_{2f}^{n_f}, X_{2f}^{n_f}, Y_{2f}^{n_f})\\
&= H(K_{1fb}) + H(K'_{1fb}|T_{2fb}^{n_f}, T_{1f}^{n_f}, T_{2f}^{n_f}, X_{2f}^{n_f}, Y_{2f}^{n_f})\\
&-H(K_{1fb}, K'_{1fb}|T_{2fb}^{n_f}, T_{1f}^{n_f}, T_{2f}^{n_f}, X_{2f}^{n_f}, Y_{2f}^{n_f})\\
&\le H(K_{1fb}) + H(K'_{1fb})\\
&-H(K_{1fb}, K'_{1fb}|T_{2fb}^{n_f}, T_{1f}^{n_f}, T_{2f}^{n_f}, X_{2f}^{n_f}, Y_{2f}^{n_f})\\
&= H(K_{1fb}) + H(K'_{1fb})\\
&-H(K_{1fb}, K'_{1fb}, T_{1fb}^{n_f}|T_{2fb}^{n_f}, T_{1f}^{n_f}, T_{2f}^{n_f}, X_{2f}^{n_f}, Y_{2f}^{n_f})\\
&+H(T_{1fb}^{n_f}|K_{1fb}, K'_{1fb}, T_{2fb}^{n_f}, T_{1f}^{n_f}, T_{2f}^{n_f}, X_{2f}^{n_f}, Y_{2f}^{n_f})\\
&\overset{(c)}{=} H(K_{1fb}) + H(K'_{1fb}) - H(T_{1fb}^{n_f}|T_{2fb}^{n_f}, T_{1f}^{n_f}, T_{2f}^{n_f}, X_{2f}^{n_f}, Y_{2f}^{n_f})\\
&+H(T_{1fb}^{n_f}|K_{1fb}, K'_{1fb}, T_{2fb}^{n_f}, T_{1f}^{n_f}, T_{2f}^{n_f}, X_{2f}^{n_f}, Y_{2f}^{n_f})\\
&\overset{(d)}{\le} 2n_f\varepsilon'' + n_f\varepsilon_6 + n_f\varepsilon_7.
\end{aligned}$$

In the above equations, (a) follows from the fact that indices k_{1f}, k_{2f}, k_{1b} are one of the indices of $t_{1f}^{n_f}, t_{2f}^{n_f}, t_{2b}^{n_b}$, respectively. (b) can be deduced from the Markov chain (28) and (c) due to the fact that (k_{1fb}, k'_{1fb}) are one of the indices of $t_{1fb}^{n_f}$. (d) can be justified with the same arguments as (i), (j), (k) and (l) in term A.

For term C, we have:

$$\begin{aligned}
&I(K_{1b}; K_{2f}, X_{2f}^{n_f}, Y_{2f}^{n_f}, Y_{2b}^{n_b}|K_{1f})\\
&\le I(K_{1b}; K_{1f}, K_{2f}, X_{2f}^{n_f}, Y_{2f}^{n_f}, Y_{2b}^{n_b})\\
&\le I(K_{1b}; T_{1f}^{n_f}, T_{2f}^{n_f}, X_{2f}^{n_f}, Y_{2f}^{n_f}, Y_{2b}^{n_b}, K'_{2fb})\\
&\overset{(a)}{=} I(K_{1b}; Y_{2b}^{n_b}, K'_{2fb}) \le I(K_{1b}; Y_{2b}^{n_b}, K'_{2fb}, T_{2b}^{n_b})\\
&\overset{(b)}{=} I(K_{1b}; Y_{2b}^{n_b}, T_{2b}^{n_b}) \le I(K_{1b}; Y_{2b}^{n_b}, T_{2b}^{n_b}, U^{n_b})\\
&= H(K_{1b}) - H(K_{1b}|Y_{2b}^{n_b}, T_{2b}^{n_b}, U^{n_b})\\
&= H(K_{1b}) - H(K_{1b}, T_{1b}^{n_b}|Y_{2b}^{n_b}, T_{2b}^{n_b}, U^{n_b})\\
&+H(T_{1b}^{n_b}|K_{1b}, Y_{2b}^{n_b}, T_{2b}^{n_b}, U^{n_b})\\
&\overset{(c)}{=} H(K_{1b}) - H(T_{1b}^{n_b}|Y_{2b}^{n_b}, T_{2b}^{n_b}, U^{n_b}) + H(T_{1b}^{n_b}|K_{1b}, Y_{2b}^{n_b}, T_{2b}^{n_b}, U^{n_b})\\
&\overset{(d)}{\le} H(K_{1b}) - n_bH(T_{1b}|Y_{2b}, T_{2b}, U) + n_b\varepsilon_8 + n_b\varepsilon_9\\
&= -n_bH(T_{1b}|Y_{1b}, U) + n_b\varepsilon_8 + n_b\varepsilon_9 \le n_b\varepsilon_8 + n_b\varepsilon_9.
\end{aligned}$$

In the above equations, (a) and (b) can be deduced from the Markov chains (29) and (31), respectively. (c) holds as k_{1b} is one of the indices of $t_{1b}^{n_b}$ sequence. To prove (d), the same approach as Lemmas 2 and 3 in [8] is exploited to show $n_bH(T_{1b}|Y_{2b}, T_{2b}, U) \le H(T_{1b}^{n_b}|Y_{2b}^{n_b}, T_{2b}^{n_b}, U^{n_b}) + n_b\varepsilon_8$ and $H(T_{1b}^{n_b}|K_{1b}, Y_{2b}^{n_b}, T_{2b}^{n_b}, U^{n_b}) \le n_b\varepsilon_9$.

By substituting $\varepsilon'' = \frac{\varepsilon}{12}$,$\varepsilon_i = \frac{\varepsilon}{9}$,$\varepsilon_j = \frac{\varepsilon}{2}$ for $i = 4,..,7$ and $j = 8,9$, the security condition (3) is satisfied as:

$$I(K_{1f}, K_{1fb}, K_{1b}; K_{2f}, X_{2f}^{n_f}, Y_{2f}^{n_f}, Y_{2b}^{n_b}) \le (n_f + n_b)\varepsilon.$$

To show that the total rate of user 1's secret key is the sum of the rates r_{1f}, r_{1fb} and r_{1b}, we should prove the independence of the keys. When analyzing terms B and C of the security condition, we showed that:

$$\begin{aligned}
&I(K_{1fb}; K_{1f}, K_{1b})\\
&\le I(K_{1fb}; K_{1f}, K_{2f}, K_{1fb}, X_{2f}^{n_f}, Y_{2f}^{n_f}, Y_{2b}^{n_b})\\
&\le 2n_f\varepsilon'' + n_f\varepsilon_6 + n_f\varepsilon_7,
\end{aligned}$$

$$\begin{aligned}
&I(K_{1b}; K_{1f}) \le I(K_{1b}; K_{1f}, K_{2f}, X_{2f}^{n_f}, Y_{2f}^{n_f}, Y_{2b}^{n_b})\\
&\le n_b\varepsilon_8 + n_b\varepsilon_9,
\end{aligned}$$

and hence:

$$\begin{aligned}
&H(K_{1f}, K_{1fb}, K_{1b}) \ge H(K_{1f}) + H(K_{1fb}) + H(K_{1b})\\
&-(2n_f\varepsilon'' + n_f\varepsilon_6 + n_f\varepsilon_7 + n_b\varepsilon_8 + n_b\varepsilon_9)\\
&\ge H(K_{1f}) + H(K_{1fb}) + H(K_{1b}) - (n_f + n_b)\varepsilon.
\end{aligned}$$

This completes the proof of Theorem 4.

It should be noted that in the code construction of the second step, we implicitly assume $I(T_{1b}; Y_{1b}) \ge I(T_{1b}; Y_{2b}, T_{2b})$. In the case where $I(T_{1b}; Y_{1b}) < I(T_{1b}; Y_{2b}, T_{2b})$, user 3 randomly maps k'_{1fb} into a space with $2^{n_b(I(T_{1b};Y_{1b})-\varepsilon'_1)}$ elements and no secret key is chosen as k_{1b}. The same is true about user 2's codebook.

Appendix II: Proof of the Converse in Theorem 5

The keys are produced in two steps as discribed in Section 3. Applying Fano's inequality to the corresponding keys at the users, for an arbitrary small$\varepsilon > 0$, we obtain:

$$\begin{aligned}
&H(K_{1f}, K_{2f}|Y_{3f}^{n_f}) \le n_f\left(\tfrac{h(2\varepsilon)}{n_f} + 2\varepsilon\log(|\mathcal{K}_{1f}||\mathcal{K}_{2f}| - 1)\right) \triangleq n_f\varepsilon_1,\\
&H(K_{1b}^{tot}|K_{1f}, X_{1f}^{n_f}, Y_{1f}^{n_f}, Y_{1b}^{n_b}) \le n_b\left(\tfrac{h(\varepsilon)}{n_b} + \varepsilon(\log|\mathcal{K}_{1b}^{tot}| - 1)\right) \triangleq n_b\varepsilon_2,\\
&H(K_{2b}^{tot}|K_{2f}, X_{2f}^{n_f}, Y_2^{n_f}, Y_{2b}^{n_b}) \le n_b\left(\tfrac{h(\varepsilon)}{n_b} + \varepsilon(\log|\mathcal{K}_{2b}^{tot}| - 1)\right) \triangleq n_b\varepsilon_3,
\end{aligned}$$

where $|\mathcal{K}_{1f}|$ is the cardinality of key set $\mathcal{K}_{1f}$ and $\varepsilon_i \to 0$ if $\varepsilon \to 0$ for $i = 1, 2, 3$.

Now, we show that for the secret keys satisfying above reliability conditions and the security conditions (7) and (8) in Definition 3, there exist random variables according to the distribution of Theorem 5 satisfying the mentioned relations. We prove the outer bound of R_1. The outer bound of R_2 can be deduced using the same approaches. The Markov chains (33) and (34) (on the top of the next page) are used in the proof. It is defined $\varepsilon' = \frac{2(n_f+n_b)\varepsilon + n_f\varepsilon_1 + n_b\varepsilon_2}{(n_f+n_b)}$. We have:

$$(K_{1f},K_{2f})-(X_{1f}^{n_f},X_{2f}^{n_f})-Y_{2f}^{n_f}-Y_{1f}^{n_f}-Y_{3f}^{n_f}-(K_{1b}^{tot},K_{2b}^{tot},X_{3b}^{n_b},Y_{2b}^{n_b},Y_{1b}^{n_b}) \tag{33}$$

$$(K_{1b}^{tot},K_{2b}^{tot})-X_{3b}^{n_b}-Y_{1b}^{n_b}-Y_{2b}^{n_b} \tag{34}$$

$$\begin{aligned}
&(n_f+n_b)R_1 \le H(K_{1f},K_{1b}^{tot})+(n_f+n_b)\varepsilon\\
&\overset{(a)}{\le} H(K_{1f},K_{1b}^{tot}|K_{2f},X_{2f}^{n_f},Y_{2f}^{n_f},Y_{2b}^{n_b})+2(n_f+n_b)\varepsilon\\
&\overset{(b)}{\le} H(K_{1f}|K_{2f},X_{2f}^{n_f},Y_{2f}^{n_f},Y_{2b}^{n_b})+H(K_{1b}^{tot}|K_{1f},K_{2f},X_{2f}^{n_f},Y_{2f}^{n_f},Y_{2b}^{n_b})\\
&-H(K_{1f}|K_{2f},Y_{3f}^{n_f})-H(K_{1b}^{tot}|K_{1f},X_{1f}^{n_f},Y_{1f}^{n_f},Y_{1b}^{n_b})+(n_f+n_b)\varepsilon'\\
&\le I(K_{1f};Y_{3f}^{n_f}|K_{2f},X_{2f}^{n_f},Y_{2f}^{n_f})+(n_f+n_b)\varepsilon'\\
&+I(K_{1b}^{tot};X_{1f}^{n_f},Y_{1f}^{n_f},Y_{1b}^{n_b}|K_{1f},K_{2f},X_{2f}^{n_f},Y_{2f}^{n_f},Y_{2b}^{n_b})\\
&\overset{(c)}{\le} I(X_{1f}^{n_f};Y_{3f}^{n_f}|X_{2f}^{n_f},Y_{2f}^{n_f})+(n_f+n_b)\varepsilon'\\
&+I(K_{1b}^{tot};X_{1f}^{n_f},Y_{1f}^{n_f},Y_{1b}^{n_b}|K_{1f},K_{2f},X_{2f}^{n_f},Y_{2f}^{n_f},Y_{2b}^{n_b})\\
&\overset{(d)}{=} 0+I(K_{1b}^{tot};X_{1f}^{n_f},Y_{1f}^{n_f},Y_{1b}^{n_b}|K_{1f},K_{2f},X_{2f}^{n_f},Y_{2f}^{n_f},Y_{2b}^{n_b})\\
&+(n_f+n_b)\varepsilon'\\
&\overset{(e)}{=} I(K_{1b}^{tot};Y_{1f}^{n_f},Y_{1b}^{n_b}|Y_{2f}^{n_f},Y_{2b}^{n_b})+(n_f+n_b)\varepsilon'\\
&=I(K_{1b}^{tot};Y_{1b}^{n_b}|Y_{2f}^{n_f},Y_{2b}^{n_b})+I(K_{1b}^{tot};Y_{1f}^{n_f}|Y_{2f}^{n_f},Y_{2b}^{n_b},Y_{1b}^{n_b})\\
&+(n_f+n_b)\varepsilon'\\
&\overset{(f)}{\le} I(X_{3b}^{n_b};Y_{1b}^{n_b}|Y_{2f}^{n_f},Y_{2b}^{n_b})+I(K_{1b}^{tot};Y_{1f}^{n_f}|Y_{2f}^{n_f},Y_{2b}^{n_b},Y_{1b}^{n_b})\\
&+(n_f+n_b)\varepsilon'\\
&\overset{(g)}{\le} I(X_{3b}^{n_b};Y_{1b}^{n_b}|Y_{2b}^{n_b})+I(K_{1b}^{tot};Y_{1f}^{n_f}|Y_{2f}^{n_f},Y_{2b}^{n_b},Y_{1b}^{n_b})\\
&+(n_f+n_b)\varepsilon'\\
&\overset{(h)}{\le} n_bI(X_{3b};Y_{1b}|Y_{2b})+I(K_{1b}^{tot};Y_{1f}^{n_f}|Y_{2f}^{n_f},Y_{2b}^{n_b},Y_{1b}^{n_b})\\
&+(n_f+n_b)\varepsilon'\\
&\overset{(i)}{\le} n_bI(X_{3b};Y_{1b}|Y_{2b})+I(K_{1b}^{tot};Y_{1f}^{n_f}|Y_{2f}^{n_f},Y_{1b}^{n_b})+(n_f+n_b)\varepsilon'\\
&\le n_bI(X_{3b};Y_{1b}|Y_{2b})+I(K_{1b}^{tot},Y_{1b}^{n_b};Y_{1f}^{n_f}|Y_{2f}^{n_f})+(n_f+n_b)\varepsilon'\\
&\le n_bI(X_{3b};Y_{1b}|Y_{2b})+\textstyle\sum_{i=1}^{n_f}I(K_{1b}^{tot},Y_{1b}^{n_b},Y_{1f,1}^{i-1};Y_{1f,i}|Y_{2f}^{n_f})\\
&+(n_f+n_b)\varepsilon'\\
&\le n_bI(X_{3b};Y_{1b}|Y_{2b})+\textstyle\sum_{i=1}^{n_f}(H(Y_{1f,i}|Y_{2f,i})\\
&-H(Y_{1f,i}|Y_{2f}^{n_f},K_{1b}^{tot},Y_{1b}^{n_b},Y_{1f,1}^{i-1}))+(n_f+n_b)\varepsilon'\\
&\overset{(j)}{=} n_bI(X_{3b};Y_{1b}|Y_{2b})+\textstyle\sum_{i=1}^{n_f}(H(Y_{1f,i}|Y_{2f,i})\\
&-H(Y_{1f,i}|X_{1f}^{n_f},X_{2f}^{n_f},Y_{2f}^{n_f},K_{1b}^{tot},Y_{1b}^{n_b},Y_{1f,1}^{i-1}))+(n_f+n_b)\varepsilon'\\
&\overset{(k)}{=} n_bI(X_{3b};Y_{1b}|Y_{2b})+\textstyle\sum_{i=1}^{n_f}(H(Y_{1f,i}|Y_{2f,i})\\
&-H(Y_{1f,i}|X_{1f,i},X_{2f,i},Y_{2f,i},K_{1b}^{tot},Y_{1b}^{n_b},Y_{1f,1}^{i-1}))+(n_f+n_b)\varepsilon'\\
&\overset{(l)}{=} n_bI(X_{3b};Y_{1b}|Y_{2b})+\textstyle\sum_{i=1}^{n_f}(H(Y_{1f,i}|Y_{2f,i})\\
&-H(Y_{1f,i}|Y_{2f,i},K_{1b}^{tot},Y_{1b}^{n_b},Y_{1f,1}^{i-1}))+(n_f+n_b)\varepsilon'\\
&=n_bI(X_{3b};Y_{1b}|Y_{2b})\\
&+\textstyle\sum_{i=1}^{n_f}I(K_{1b}^{tot},Y_{1b}^{n_b},Y_{1f,1}^{i-1};Y_{1f,i}|Y_{2f,i})+(n_f+n_b)\varepsilon'\\
&\le n_bI(X_{3b};Y_{1b}|Y_{2b})\\
&+\textstyle\sum_{i=1}^{n_f}I(K_{1b}^{tot},Y_{1b}^{n_b},Y_{1f,1}^{i-1},Y_{3f,i+1}^{n_f};Y_{1f,i}|Y_{2f,i})+(n_f+n_b)\varepsilon'\\
&\overset{(m)}{=} n_bI(X_{3b};Y_{1b}|Y_{2b})+\textstyle\sum_{i=1}^{n_f}I(T_{1fb,i};Y_{1f,i}|Y_{2f,i})+(n_f+n_b)\varepsilon'\\
&\overset{(n)}{=} n_bI(X_{3b};Y_{1b}|Y_{2b})+n_fI(T_{1fb};Y_{1f}|Y_{2f})+(n_f+n_b)\varepsilon'
\end{aligned}$$

where (a) results from the security conditions, (b) from Fano's inequalities. (c), (d) and (e) can be deduced as subsets of Markov chain (33), and (f), (g) and (i) from Markov chain (34). (h) is the direct result of the memoryless channel property. (j) and (l) are deduced as subsets of Markov chain (33). (k) is the result of memoryless property in GDMMAC. (m) can be deduced from the definition of the random variable $T_{1fb,i} \triangleq K_{1b}^{tot},Y_{1b}^{n_b},Y_{1f,1}^{i-1},Y_{3f,i+1}^{n_f}$ and (n) by introducing the random variable Q which is uniformly distributed on $1,2,...,n_f$ and independent of all the other variables, and defining $T_{1fb}=T_{1fb,Q},Y_{1f}=Y_{1f,Q}$ and $Y_{2f}=(Y_{2f,Q},Q)$.

With the same approach, it can be shown that $(n_f+n_b)R_2 \le 2(n_f+n_b)\varepsilon+n_f\varepsilon_1+n_b\varepsilon_3$.

In the following, the rate constraint in Theorem 5 is proved.

$$\begin{aligned}
&n_bI(X_{3b};Y_{1b}) \ge I(X_{3b}^{n_b};Y_{1b}^{n_b}) \ge I(Y_{3f}^{n_f};Y_{1b}^{n_b})\\
&\overset{(a)}{\ge} I(Y_{3f}^{n_f};Y_{1b}^{n_b})+H(K_{1b}^{tot}|K_{1f},X_{1f}^{n_f},Y_{1f}^{n_f},Y_{1b}^{n_b})-n_b\varepsilon_2\\
&\overset{(b)}{=} I(Y_{3f}^{n_f};Y_{1b}^{n_b})+H(K_{1b}^{tot}|Y_{1f}^{n_f},Y_{1b}^{n_b})-n_b\varepsilon_2\\
&\ge I(Y_{3f}^{n_f};Y_{1b}^{n_b},K_{1b}^{tot})-I(Y_{1f}^{n_f};Y_{1b}^{n_b},K_{1b}^{tot})-n_b\varepsilon_2\\
&\overset{(c)}{=} I(K_{1b}^{tot},Y_{1b}^{n_b};Y_{3f}^{n_f}|Y_{1f}^{n_f})-n_b\varepsilon_2\\
&=\textstyle\sum_{i=1}^{n_f}I(K_{1b}^{tot},Y_{1b}^{n_b};Y_{3f,i}|Y_{1f}^{n_f},Y_{3f,i+1}^{n_f})-n_b\varepsilon_2\\
&\overset{(d)}{=} \textstyle\sum_{i=1}^{n_f}H(Y_{3f,i}|Y_{1f,i})-\sum_{i=1}^{n_f}H(Y_{3f,i}|Y_{1f}^{n_f},Y_{3f,i+1}^{n_f},K_{1b}^{tot},Y_{1b}^{n_b})-n_b\varepsilon_2\\
&=\textstyle\sum_{i=1}^{n_f}I(K_{1b}^{tot},Y_{1b}^{n_b},Y_{1f,1}^{i-1},Y_{3f,i+1}^{n_f};Y_{3f,i}|Y_{1f,i})-n_b\varepsilon_2\\
&\overset{(e)}{=} n_fI(T_{1fb};Y_{3f}|Y_{1f})-n_b\varepsilon_2
\end{aligned}$$

where (a) results from Fano's inequality, (b) and (c) from the Markov chain (33), (d) from the combination of the memoryless property and Markov chain (33) and (e) from the analogous argument as (m) and (n) in deriving R_1.

REFERENCES

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

[2] 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.

[3] H.Ahmadi, R. Safavi-Naini, "Secret key establishment over a pair of independent broadcast channels," *IEEE Int. Symp. Inf. Theory and its Application (ISITA)*, Taichung, Taiwan, pp. 185-190, Oct. 2011.

[4] Y. Liang and V. Poor, "Multiple access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 976-1002, Mar. 2008.

[5] S. Salimi, M. Salmasizadeh, M. R. Aref, Jovan Dj Golic, "Key Agreement over Multiple Access Channel," *IEEE Trans. Inf. Forens. Security*, vol. 6, Issue 3, pp. 775-790, Sep. 2011.

[6] S. Salimi, M. Salmasizadeh, M. R. Aref, "Key Agreement over Multiple Access Channel Using Feedback Channel," *IEEE Int. Symp. Inf. Theory (ISIT)*, Saint Petersburg, Russia, pp. 1936-1940, Aug. 2011.

[7] S. N. Diggavi, V. A. Vaishampayan "On multiple description source coding with decoder side information," *IEEE Information Theory Workshop (ITW)*, San Antonio, Texas, pp. 1-6, Oct. 2004.

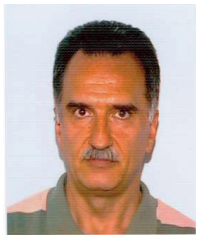
[8] R. Liu, I. Maric, P. Spasojevic, R. D. Yate, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 1–14, Jun. 2008.

[9] E. Ekrem and S. Ulukus, "Effects of Cooperation on the Secrecy of Multiple Access Channels with Generalized Feedback," *Annual Conf. Information Sciences and Systems (CISS)*, Princeton, NJ , pp. 791 – 796, March 2008.

[10] S. I. Gelfand and M. S. Pinsker, "Capacity of a broadcast channel with one deterministic component," *Probl. Inform. Transm.*, vol. 16, no. 1, pp. 1725, Jan. 1980.

Somayeh Salimi received her B.Sc., M.Sc. and Ph.D. from the Electrical Engineering Department of Sharif University of Technology, Iran, in the field of Telecommunications in 2003, 2005 and 2011, respectively. Her Ph.D. research was in the field of Information Theoretic Security under the supervision of Prof. Mohammad Reza Aref and Prof. Mahmoud Salmasizadeh. Since December 2011, she has joined Communication Theory Group, KTH Royal Institute of Technology, Stockholm, Sweden as a postdoctoral researcher. Her research interests include secrecy rates in wiretap channels and information theoretic secret key sharing.

Mikael Skoglund (S'93-M'97-SM'04) received the Ph.D. degree in 1997 from Chalmers University of Technology, Sweden. In 1997, he joined the KTH Royal Institute of Technology, Stockholm, Sweden, where he was appointed to the Chair in Communication Theory in 2003. At KTH, he heads the Communication Theory Lab and he is the Assistant Dean for Electrical Engineering. Dr. Skoglund's research interests are in the theoretical aspects of wireless communications. He has worked on problems in source-channel coding, coding and transmission for wireless communications, Shannon theory and statistical signal processing. He has authored and co-authored more than 300 scientific papers in these areas, and he holds six patents. Dr. Skoglund has served on numerous technical program committees for IEEE conferences. During 2003–08 he was an associate editor with the IEEE Transactions on Communications and he is presently on the editorial board for IEEE Transactions on Information Theory.



Jovan Dj. Golić received the BSc, MSc, and PhD degrees in electrical engineering from the School of Electrical Engineering, University of Belgrade, Belgrade, Yugoslavia, in 1979, 1981, and 1985, respectively. From 1979 to 1993, he worked at the Institute of Applied Mathematics and Electronics, Belgrade, where he was appointed a Department Head in 1986 and a Senior Research Fellow in 1990. In 1987 and 1988, he was a Fulbright Visiting Scientist at the School of Electrical Engineering, Cornell University, Ithaca, NY. Since 1985, he has been a part-time Research Associate at the Mathematical Institute, Serbian Academy of Science and Arts, Belgrade. From 1993 to 1997, he was a Research Scientist at the Information Security Research Centre, Queensland University of Technology, Brisbane, Australia. From 1997 to 2001, he worked as an Associate Professor with the School of Electrical Engineering, University of Belgrade. From 2001 to 2003, he was a chief cryptographer at Rome CryptoDesign Center, Gemplus, Italy. In 2003, he joined Telecom Italia Lab in Turin and, in 2005, he moved to Security Innovation, Telecom Italia, Turin, Italy. In 2012, Security Innovation became Security Lab of Telecom Italia Group. Prof. Golić has taught and developed undergraduate and graduate courses in cryptology, information theory, data compression and error control coding, algebra, numerical analysis, and discrete mathematics. He has been doing research in cryptology for about three decades, both with academic institutions and industry. He has contributed to the areas of stream ciphers and pseudorandom number generators including new cryptanalytic methods and design principles, true random number generation in hardware, secure hardware implementations of cryptographic algorithms, biometric authentication, statistical anomaly detection and intrusion detection, authentication in ad hoc networks, security in information-centric networks, and secret key sharing and agreement protocols. He has published more than a hundred papers in prestigious international journals and book series and a dozen patents or patent applications.

Mahmoud Salmasizadeh received the B. S. and M. S. degrees in Electrical Engineering from Sharif University of Technology in Iran, in 1972 and 1989, respectively. He also received the Ph.D. degree in Information Technology from Queensland University of Technology in Australia, in 1997. Currently he is an associate professor in Electronics Research Institute and adjunct associate professor in Electrical Engineering Department at Sharif University of Technology, Tehran, Iran. His research interests include information theoretic secrecy design and cryptanalysis of cryptographic algorithms and protocols and e-commerce security. He is a founding member of Iranian Society of Cryptology.

Mohammad Reza Aref received the B.S. degree in 1975 from the University of Tehran, Iran, and the M.S. and Ph.D. degrees in 1976 and 1980, respectively, from Stanford University, Stanford, CA, all in electrical engineering. He returned to Iran in 1980 and was actively engaged in academic and political affairs. He was a Faculty member of Isfahan University of Technology from 1982 to 1995. He has been a Professor of electrical engineering at Sharif University of Technology since 1995 and has published more than 230 technical papers in communication and information theory and cryptography in international journals and conferences proceedings. His current research interests include areas of communication theory, information theory and cryptography with special emphasis on network information theory and security for multiuser wireless communications. At the same time, during his academic activities, he has been involved in different political positions. First Vice President of I. R. Iran, Vice President of I. R. Iran and Head of Management and Planning Organization are the most recent ones.