Secret Key Agreement Using Correlated Sources over the Generalized Multiple Access Channel

Somayeh Salimi, Mikael Skoglund
School of Electrical Engineering and ACCESS Linnaeus Center
KTH Royal Institute of Technology, Stockholm, Sweden
{somayen,skoglund}@ee.kth.se

Abstract—A secret key agreement setup between 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. The three users observe i.i.d. outputs of correlated sources and there is a generalized discrete memoryless multiple access channel (GDMMAC) from users 1 and 2 to user 3 for communication between the users. The secret key agreement is established using the correlated sources and the GDMMAC. In this setup, inner and outer bounds of the secret key capacity region are investigated. Moreover, for a special case where the channel inputs and outputs and the sources form Markov chains in some order, the secret key capacity region is derived. Also a Gaussian case is considered in this setup.

I. INTRODUCTION

Secret key sharing between two legitimate users in the presence of an eavesdropper was considered in [1] and [2] in the source and the channel model. In the source model, all the three users could observe i.i.d. outputs of correlated sources and there was a noiseless public channel with unlimited capacity for communication between the two legitimate users, through which all communications could be intercepted by the eavesdropper. In [1], secret key capacity is characterized in the source model when the noiseless public channel is one-way. In [3], secret key sharing in a source model with public channel of limited capacity is investigated in which there is a helper with access to source observations correlated with the others observations. In [4], the same problem of sharing a secret key is investigated in the source model where instead of the public channel, there is a noisy broadcast channel from the transmitter to the receiver and the eavesdropper. In [5], secret key sharing was considered in a framework where two users intended to share secret keys with a base station and the two users were eavesdroppers of each other’s key. In [5], all the three users can observe i.i.d. outputs of correlated sources and there is a noiseless public channel with unlimited capacity from users 1 and 2 to user 3.

Motivated by the above works, we consider secret key sharing in a framework similar to [5] but in more conformity with real communication scenarios since the realization of public channel with unlimited capacity is not compatible with the noisy nature of wireless networks. Hence, instead of public channels with unlimited capacity, we consider noisy channels for communication between the users. Each of the users 1 and 2, as network users, intends to share a secret key with user 3, as a base station, and users 1 and 2 are the eavesdroppers with respect to each other. The three users have access to correlated sources and there is a generalized discrete memoryless multiple access channel (GDMMAC) to transmit the required information from users 1 and 2 to user 3. Users 1 and 2 govern the channel inputs of the GDMMAC and each of the three users receives his corresponding output from the channel. Each of the users 1 and 2 generates a secret key from his observations and sends the required information via the GDMMAC to user 3. Users 1 and 2 use the channel outputs to eavesdrop each other’s key. For this setup, we derive an inner bound of the secret key capacity region in which a combination of wiretap codebook and secret key generation codebook along with Wyner-Ziv codebook is used. Furthermore, an explicit outer bound of the secret key capacity region is given and for a special case, the secret key capacity region is derived. Also, the problem is discussed in a Gaussian case.

The rest of the paper is organized as follows: in Section II, the proposed model is described. In Section III, our main results are given. A special case is investigated in Section IV. A Gaussian example is discussed in Section V. Conclusion and suggestions for future works are given in Section VI. Proofs of the theorems are presented in Appendices. Throughout the paper, a random variable is denoted with an upper case letter (e.g. $X$) and its realization is denoted with the corresponding lower case letter (e.g., $x$). We use $X_i^N$ to indicate vector $(X_{i,1}, X_{i,2}, ..., X_{i,N})$ and $X_{i,j}^k$ to indicate vector $(X_{i,j}, X_{i,j+1}, ..., X_{i,k})$, where $i$ denotes the index of the corresponding user.

II. PRELIMINARIES

Users 1, 2 and 3 observe correlated discrete memoryless sources $S_1, S_2$ and $S_3$, respectively, with joint distribution $P_{S_1,S_2,S_3}$ in an i.i.d. manner. Furthermore, there is a GDMMAC with probability distribution $P_{Y_1,Y_2|X_1,X_2}$ independent of the sources, where users 1 and 2 govern the inputs $X_1$ and $X_2$, and then, outputs $Y_1, Y_2$ and $Y_3$ are seen by users 1, 2 and 3, respectively. Each of users 1 and 2 intends to share a secret keys with user 3 where user 1 is the eavesdropper of user 2’s secret key and vice versa.

For the secret key agreement, users 1 and 2 generate secret keys $K_1$ and $K_2$ as stochastic functions of the information available at them, i.e., $S_1^N$ and $S_2^N$, respectively. For $i = 1, 2, ..., N$, the $i$-th channel inputs $X_{1,i}$ and $X_{2,i}$ are determined as stochastic mappings $X_{1,i} = f_{1,i}(S_1^i)$ and
Now, we state the main result of the paper. We impose the separation strategy as in \cite{4} to the GDMMAC.

**Theorem 1:** In the described model, all rate pairs in the closure of the convex hull of the set of all key rate pairs $(R_1, R_2)$ that satisfy the following region are achievable:

\[ R_1 > 0, R_2 > 0 \]
\[ R_1 \leq I(U_1; S_1 \mid U_2) + I(U_2; S_2 \mid U_1) \]
\[ R_2 \leq I(U_2; S_1 \mid U_1) + I(V_1; V_2; Y_1) - I(U_2; Y_2; V_2) \]
\[ R_1 + R_2 \leq I(U_1, U_2; S_1 - U_1; S_2 | U_2) + I(V_1; V_2; Y_1) - I(U_2; Y_2; V_2) - I(V_1; V_2; Y_1; X_1) \]

subject to the constraints:

\[ I(U_1; S_1 | U_2, S_3) \leq I(V_1; V_2 | V_1) \]
\[ I(U_2; S_2 | S_1, S_3) \leq I(V_2; V_3 | V_1) \]

for random variables taking values in sufficiently large finite sets according to the distributions:

\[ p_1(u_1, u_2, s_1, s_2, s_3) = p(u_1 | s_1) p(u_2 | s_2) p(s_1, s_2, s_3) \]
\[ p_2(v_1, v_2, x_1, y_1, y_2, x_2) = p(v_1 | x_1) p(v_2 | x_2) p(y_1 | y_2) p(y_2 | y_1) \]

The proof of Theorem 1 is given in Appendix I. Here, the sketch of the proof is given. To derive this inner bound, a part of the keys between the users is generated by using the source common randomness and the other part is generated by exploiting the channel common randomness. For this purpose, we impose the separation strategy as in \cite{4} to the GDMMAC.

**III. MAIN RESULTS**

Now, we state the main result of the paper.

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

**IV. SPECIAL CASE**

In this section, we consider a special case of the general problem discussed in the previous sections. This special case arises when the channel inputs and outputs and the sources form Markov chains as:

\[ (X_1, X_2) \rightarrow Y_1 - Y_3, \quad (X_1, X_2) \rightarrow Y_2 - Y_3, \quad S_1 - S_3 - S_2. \]

Also, we constrain a special condition to the channel such that each of the channel inputs can be specified with access to the receiver’s channel output and the other transmitter’s input or in other words:

\[ H(X_1 | X_2, Y_3) = 0, \quad H(X_2 | X_1, Y_3) = 0. \]

In this case, the GDMMAC cannot itself provide secrecy; due to the Markov chains between the inputs and outputs, however, it can be used by users 1 and 2 to transmit the required information of the source common randomness. The secret key capacity region is given in the following theorem.

**Theorem 2:** In the mentioned special case of the described setup, the secret key capacity region is the set of all rate pairs $(R_1, R_2)$ that satisfy:

\[ R_1 \leq I(U_1; S_1 | S_2), \quad R_2 \leq I(U_2; S_2 | S_1), \]

subject to the constraints:

\[ I(U_1; S_1 | S_2) \leq I(X_1; X_2), I(U_2; S_2 | S_1) \leq I(X_2; X_3 | X_1), I(U_1; S_1 | S_3) + I(U_2; S_2 | S_3) \leq I(X_1, X_2; Y_3), \]
for random variables taking values in sufficiently large finite sets according to the distributions:

\[
p(u_1, u_2, s_1, s_2, s_3) = p(u_1|s_1)p(u_2|s_2)p(s_1, s_2, s_3), \]

\[
p(x_1, x_2, y_1, y_2, y_3) = p(x_1)p(x_2)p(y_1, y_2, y_3|x_1, x_2).
\]

The achievability can be deduced from Theorem 1 by substituting \( V_1 = X_1, V_2 = X_2 \) and employing the Markov chains. The outer bound is proved in Appendix III. In this example, the GDMMAC is used just to transmit the required source common randomness information and hence, the problem can be treated as a pure source model with rate limited public channels. When the channel rates satisfy:

\[
H(S_1|S_3) \leq I(X_1;Y_3|X_2), H(S_2|S_3) \leq I(X_2;Y_3|X_1),
\]

\[
H(S_1, S_2|S_3) \leq I(X_1, X_2;Y_3),
\]

the case is similar to the special case of the forward source model of \([5]\) where the secret key capacity is the union of all rate pairs that satisfy:

\[
R_1 \leq I(S_1;S_3 | S_2), \quad R_2 \leq I(S_2;S_3 | S_1).
\]

\section{A Gaussian Example}

As a scalar Gaussian example, we consider the case where the source observations at the users are according to Markov chain \( S_1 - S_3 - S_2 \). Then, without loss of generality, we can model them as \( S_1 = S_3 + E_{c,1}, S_2 = S_3 + E_{c,2} \) where \( S_3, E_{c,1} \) and \( E_{c,2} \) are independent zero mean Gaussian variables with variances \( P_3, N_{s,1} \) and \( N_{s,2} \), respectively. The GDMMAC is described by:

\[
Y_3 = X_1 + X_2 + E_{c,3}, Y_2 = X_1 + X_2 + E_{c,2}, Y_1 = X_1 + X_2 + E_{c,1},
\]

in which \( E_{c,i} \sim \mathcal{N}(0, N_{c,i}) \) for \( i = 1, 2, 3 \) with the input power constraints \( P_1 \) and \( P_2 \) at users 1 and 2, respectively. By the standard arguments as the discrete channel arguments, the results can be extended to Gaussian case. We consider:

\[
V_1 = X_1, V_2 = X_2, S_1 = U_1 + D_1, S_2 = U_2 + D_2,
\]

in Theorem 1 where \( U_i \sim \mathcal{N}(0, P_i), D_i \sim \mathcal{N}(0, P_3 + N_{s,1} - P_u) \) and \( U_1 \) is independent of \( D_i \) for \( i = 1, 2 \).

By substituting the random variables as above in Theorem 1, the following proposition for secret key rate region can be deduced for which the proof is relinquished due to space limitation.

**Proposition 2:** \((R_1, R_2)\) is an achievable key rate pair if it satisfies the equations at the top of the next page.

For the values \( P_1 = P_2 = P_3 = 1, N_{s,1} = N_{s,2} = N_{c,3} = 0.5 \), the rate region is shown in Fig. 2 where \( N_{c,1} = N_{c,2} \) and they vary from 0.5 to 0.9. When \( N_{c,1} = N_{c,2} = 0.5 \), no secret key can be generated through GDMMAC and the second terms of the secret key rates bound in Proposition 2 will be zero. In this case, the region is the secret key rate region of a pure source model with rate limited public channels. When these noises increase, the key rate region enlarges however the sum rate boundary remains fixed since the sum rate term related to channel common randomness is zero until these noises amount to about \( N_{c,1} = N_{c,2} = 0.75 \). At this point, the term related to the channel common randomness in the sum rate bound would be positive and hence, the sum rate bound increases. For \( N_{c,1} = N_{c,2} = 0.8 \), the rate region is rectangular since each user’s rate bound in proposition 2 will exceed the total sum rate bound.

**VI. Conclusion**

The problem of secret key sharing in a combined framework with both source and the channel common randomness was studied. For this problem, the inner bound and the explicit outer bound of the secret key capacity region were derived. The separation strategy used to achieve the inner bound was not optimal in general, however, for the especial case where the channel inputs and outputs and the sources form Markov chains in some order, the secret key capacity region was derived. It was shown that this case can be simulated as the source model of key agreement with public channels of limited capacity. As future work, the joint source channel coding can be investigated instead of the separation strategy. In addition, in a more practical scenario, some types of dependency between the source and the channel can be supposed.

**Appendix I**

**Proof of Theorem 1**

We fix the distribution to be the same as in Theorem 1. Users 1 and 2 independently and randomly generate typical sequences \( u_1^N \) and \( u_2^N \), respectively, each with probability:

\[
p(u_1^N) = \prod_{i=1}^{N} p(u_{1,i}), p(u_2^N) = \prod_{i=1}^{N} p(u_{2,i}).
\]

The number of the sequences \( u_1^N \) and \( u_2^N \) are \( 2^{N(I(U_1;S_1)+\epsilon')} \) and \( 2^{N(I(U_2;S_2)+\epsilon')} \), respectively, in which \( \epsilon' > 0 \) can be chosen arbitrarily small. Using two-layered random binning, they are labeled as:

\[
u_1^N(k_1S, k_2S, k_3S),
\]

\[
k_1S \in \{1, ..., 2^{N(r_1S)}\}, k_2S \in \{1, ..., 2^{N(r_2S)}\}, k_3S \in \{1, ..., 2^{N(r_3S)}\}
\]

\[
u_2^N(k_2S, k_2S, k_3S),
\]

\[
k_2S \in \{1, ..., 2^{N(r_1S)}\}, k_2S \in \{1, ..., 2^{N(r_2S)}\}, k_3S \in \{1, ..., 2^{N(r_3S)}\}
\]

where:

\[
r_{1S} + r_{1S}' = I(U_1;S_1) - I(U_1;S_2) + 2\epsilon', \quad r_{1S}'' = I(U_1;S_1) - \epsilon',
\]

\[
r_{2S} + r_{2S}' = I(U_2;S_2) - I(U_2;S_1) + 2\epsilon', \quad r_{2S}'' = I(U_2;S_1) - \epsilon'.
\]

It is obvious that \( r_{1S} + r_{1S}' + r_{1S}'' = I(U_1;S_1) + \epsilon' \) and so, each sequence \( u_1^N \) can be determined if the indices \( (k_1S, k_2S, k_3S) \) are known. The same is true for \( u_2^N \).
In addition to the secret key codebooks, the wiretap channel codebooks are generated. Users 1 and 2 generate independent sequences \(v_1^N\) and \(v_2^N\), respectively, each with probability:

\[
p(v_1^N) = \prod_{i=1}^{N} p(v_{1i}), p(v_2^N) = \prod_{i=1}^{N} p(v_{2i}).
\]

The number of sequences \(v_1^N\) and \(v_2^N\) is \(2^{N(r_1 + r_1')}\) and \(2^{N(r_2 + r_2')}\), respectively, which are labeled as:

\[
v_1^{N}(k_1C, k'_1C), k_1C \in \{1, \ldots, 2^{N r_1C}\}, k'_1C \in \{1, \ldots, 2^{N r_1'C}\}
v_2^{N}(k_2C, k'_2C), k_2C \in \{1, \ldots, 2^{N r_2C}\}, k'_2C \in \{1, \ldots, 2^{N r_2'C}\}
\]

where:

\[
r_1'C = I(V_1; X_2, Y_2|V_2) - \epsilon''', r_2'C = I(V_2; X_1, Y_1|V_1) - \epsilon'''' (8)
\]

Two functions \(f_1\) and \(f_2\) are defined as:

\[
f_1 : V_1 \rightarrow K'_1S, \quad f_2 : V_2 \rightarrow K'_2S,
\]

where \(V_1\) and \(V_2\) are the set of \(2^{N(r_1 + r_1')}\) and \(2^{N(r_2 + r_2')}\) codewords \(v_1^N\) and \(v_2^N\), respectively. Mapping \(f_1\) is a random partitioning of codewords \(v_1^N\) into \(2^{r_1'}\) equal-sized parts. Elements of part \(i\) are labeled as \((V_1)_i\). Mapping \(f_2\) is similarly defined. In the definition of \(f_1\), we assume that \(r_1C + r_1'\geq r_1'S\) and as we would see in the decoding step, this can be deduced from the constraint of Theorem 1. The same is true for \(f_2\).

For encoding, when typical sequences \(s_1^N\) and \(s_2^N\) are observed at users 1 and 2, respectively, sequences \(u_1^N\) and \(u_2^N\) are chosen at the corresponding users such that \((s_1^N, u_1^N)\) and \((s_2^N, u_2^N)\) are \(\epsilon''\)-jointly typical. It can be seen that these sequences are unique with high probability for arbitrarily small \(\epsilon''\). For the sequences \(u_1^N(k_{1S}, k'_{1S}, k''_{1S})\) and \(u_2^N(k_{2S}, k'_{2S}, k''_{2S})\), the indices \(k_{1S}\) and \(k_{2S}\) are chosen by users 1 and 2, respectively, to share with user 3 as the secret keys due to the source observations. For this purpose, the indices \(k'_{1S}\) and \(k'_{2S}\) are the required information to be sent by users 1 and 2 to user 3. User 1 encodes \(k'_{1S}\) in such a way that he returns \(v_1^N\) randomly chosen from \((V_1)_{k'_{1S}}\) using the mapping \(f_1\). User 2 acts in the same way using mapping \(f_2\) and returns \(v_2^N\). For the selected \(v_1^N(K_{1C}, k'_{1C})\) and \(v_2^N(k_{2C}, k'_{2C})\), user 1 and 2, respectively, consider \(k_{1C}\) and \(k_{2C}\) to share with user 3 as the secret keys due to the channel common randomness. Then, the channel inputs \(x_1^N\) and \(x_2^N\) are sent over GDMMAC according to the distributions \(p(x_1|v_1)\) and \(p(x_2|v_2)\).

For decoding, user 3, first, chooses the sequences \(v_1^N\) and \(v_2^N\) which are \(\epsilon_1\)-jointly typical with the received \(y_3^N\) when \(\epsilon_1 = \frac{\epsilon}{3}\). User 3 decodes key pair \((k_{1C}, k_{2C})\) if \((v_1^N(k_{1C}, k'_{1C}), v_2^N(k_{2C}, k'_{2C}), y_3^N) \in A_{\epsilon_1}(P_{V_1}, y_3\mid V_3)\), when such \((v_1^N(k_{1C}, k'_{1C}), v_2^N(k_{2C}, k'_{2C}))\) exists and is unique. Otherwise, it declares error. It can be shown that the decoding error probability of this step is bounded as:

\[
P_{e_1}^{(N)} \leq \epsilon_1 + 2^{N(-2\epsilon'' + 4\epsilon_1)} + 2^{N(-\epsilon'' + 3\epsilon_1)} + 2^{N(-\epsilon'' + 3\epsilon_1)}.
\]

By setting \(\epsilon'' > 3\epsilon_1\), for example \(\epsilon'' = 4\epsilon_1 = \frac{4\epsilon}{3}\), we choose \(N\) so large that \(2^{N(-\epsilon'' + 3\epsilon_1)} \leq \epsilon_1\), and then \(P_{e_1}^{(N)} \leq 4\epsilon_1 = \frac{4\epsilon}{3}\). After correct decoding \((k_{1C}, k'_{1C})\) and \((k_{2C}, k'_{2C})\), user 3 considers \(k_{1C}\) and \(k_{2C}\) to share with users 1 and 2, respectively, as the secret keys due to the channel common randomness. Then, using functions \(f_1\) and \(f_2\), user 3 finds the mappings \((V_1)_{k'_{1S}}\) of the codeword \(v_1^N\) and \((V_2)_{k'_{2S}}\) of the codeword \(v_2^N\) and sets \(k_{1S} = i, k_{2S} = j\). Now, user 3 decodes sequences \(u_1^N(k_{1S}, k'_{1S}, k''_{1S})\) and \(u_2^N(k_{2S}, k'_{2S}, k''_{2S})\) such that:

\[
u_1^N(k_{1S}, k'_{1S}, k''_{1S}) \in A_{\epsilon_2}(P_{U_1, u_2, S_3})
\]

when such \((u_1^N(k_{1S}, k'_{1S}, k''_{1S}), u_2^N(k_{2S}, k'_{2S}, k''_{2S}))\) exists and is unique. Otherwise, it declares error. For \(\epsilon_2 = \frac{\epsilon_1}{3}\), according to Wyner-Ziv problem for multiple sources in [7], the decoding error probability of this step is bounded as:

\[
P_{e_2}^{(N)} \leq \epsilon_2 + 2^{N(4\epsilon_2 + I(U_1; U_2; S_1, S_2 | S_3) - (r_1S + r_2S))} + 2^{N(7\epsilon_2 + I(U_1, S_1; U_2, S_2) - r_1S)} + 2^{N(7\epsilon_2 + I(U_2; S_2 | U_1, S_3) - r_2S)}.
\]
If we set:

\[ r_{1S} < I(U_1; S_1 | U_2) - I(U_1; S_2 | U_2), \]
\[ r_{2S} < I(U_2; S_1) - I(U_2; S_1 | U_1), \]
\[ r_{1S} + r_{2S} < I(U_1; S_2) - I(U_1; S_1) - I(U_1; U_2), \]

then by substituting \( r_{1S} \) and \( r_{2S} \) from (6) and (7), we have:

\[ P_e^{(N)} \leq \varepsilon + 2^{-N(\rho - \varepsilon)} + 2^{-N(\tau - \varepsilon)} + 2^{-\varepsilon}. \]

By setting \( \varepsilon' = \frac{7}{2}\varepsilon \), and for example \( \varepsilon' = 4\varepsilon_2 = \frac{3}{4} \), we choose \( N \) so large that \( 2^{N(\rho - \varepsilon)} \leq \varepsilon \), and then \( P_e^{(N)} \leq 4\varepsilon_2 = \frac{3}{4} \).

After this step of decoding, user 3 considers \( k_{1S} \) and \( k_{2S} \) to share with users 1 and 2, respectively, as the secret keys due to the source observations.

By the above arguments, the total decoding error probability is bounded as \( P_e^{(N)} \leq P_e^{(N)} + P_e^{(N)} \leq \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon. \)

For correct decoding in the first step, according to \( P_e^{(N)} \) equation, it is necessary that:

\[ r_{1C} + r_{1C} < I(V_1; Y_3 | V_2), \quad r_{2C} + r_{2C} < I(V_2; Y_3 | V_1) \]

and hence, considering the rate constraints in Theorem 1, the functions \( f_1 \) and \( f_2 \) can be defined.

Now, we should check the security conditions of definition 1 and show that the indices \( (k_{1S}, k_{1C}) \) can be shared as secret keys between user 1 and user 2 and \( (k_{2S}, k_{2C}) \) can be shared as secret keys between user 2 and user 3. We give the proof of (3) and by symmetry, (4) can be deduced. We have:

\[ I(K_{1S}, K_{1C}; S_{1}^N, X_2^N, Y_2^N) = I(K_{1S}; S_{1}^N, X_2^N, Y_2^N | K_{1C}) + I(K_{1C}; S_{2}^N, X_2^N, Y_2^N | A) \]

Now, we analyze each term separately. We consider \( \varepsilon_3 = \varepsilon_4 = \varepsilon_5 = \varepsilon_6 = \frac{\varepsilon}{6} \). Some Markov chains useful in the security analysis are given in continue. These Markov chains arise from the coding scheme.

\[ (U_1^N, U_2^N) \rightarrow (K_{1S}, K_{2S}) \rightarrow (V_1^N, V_2^N) \rightarrow (X_1^N, X_2^N, Y_1^N, Y_2^N) \]

\[ U_1^N = S_1^N - S_2^N - U_2^N \]
\[ V_1^N - V_2^N = K_{2S} - U_2^N - S_2^N \]

For term A, we have:

\[ I(K_{1S}; S_{1}^N, X_2^N, Y_2^N | K_{1C}) \leq I(K_{1S}; S_{1}^N, X_2^N, Y_2^N, K_{1C}) \]

\[ \leq I(K_{1S}; S_{1}^N, X_2^N, Y_2^N, S_{1}^N, K_{1C}, K_{1S}, K_{1S}^N) \]

\[ \leq I(K_{1S}; S_{1}^N, X_2^N, Y_2^N, S_{1}^N, K_{1C}, K_{1S}, K_{1S}^N) + I(K_{1S}; S_{1}^N, X_2^N, Y_2^N, K_{1C}) \]

\[ \leq I(K_{1S}; S_{1}^N, X_2^N, Y_2^N, S_{1}^N, K_{1C}, K_{1S}) + I(K_{1S}; S_{1}^N, X_2^N, Y_2^N, K_{1C}) + I(K_{1S}; S_{1}^N, X_2^N, Y_2^N, K_{1C}) \]

\[ \leq I(K_{1S}; S_{1}^N, X_2^N, Y_2^N, S_{1}^N, K_{1C}, K_{1S}) + N\varepsilon \]

In above equations, (a) and (b) follow from Markov chains (9) and (10), respectively. (c) can be deduced from the same approach as lemma 2 in [6] to show \( H(U_1^N | S_{1}^N, M_1', M_1') \leq N\varepsilon_3 \). (d) follows from the fact that \( k_{1S}^N \) is one of the indices of \( \varepsilon_3 \). To prove (e), the same approach as lemma 3 in [6] is exploited to show \( N I(U_1^N | S_{2}^N) \leq I(U_1^N | S_{2}^N) + N\varepsilon_4 \).

For term B, we have:

\[ I(K_{1C}; S_{1}^N, X_2^N, Y_2^N) \leq I(K_{1C}; S_{1}^N, X_2^N, Y_2^N) - I(H(K_{1C}) - H(K_{1C}) - H(K_{1C}) - H(K_{1C}) + H(V_1^N | K_{1C}, S_{1}^N, X_2^N, Y_2^N)) + N\varepsilon_5 \]

\[ \leq H(K_{1C}) - H(V_2^N | X_2^N, Y_2^N) + N\varepsilon_5 \]

\[ \leq -NH(V_1^N | Y_1^N, V_2^N) + N\varepsilon_5 + N\varepsilon_5 \]

\[ \leq N\varepsilon_5 \]

In the above equations, (a) can be deduced from the same approach as lemma 2 in [6] to show \( H(V_1^N | K_{1C}; X_2^N, Y_2^N) \leq N\varepsilon_5 \). (b) follows from the fact that \( k_{1C} \) is one of the indices of \( v_1^N (c) \) can be followed from Markov chain (11). The same approach as lemma 3 in [6] can be exploited to show \( NH(V_1^N | X_2^N, Y_2^N) + N\varepsilon_6 \). (c) is a direct consequence of reliable decoding at user 3.

Hence, the security condition (3) is satisfied as:

\[ I(K_{1S}, K_{1C}; S_{1}^N, X_2^N, Y_2^N) \leq N \left( \frac{3\varepsilon}{4} + \frac{\varepsilon}{4} \right) = N\varepsilon. \]

To show that the total rate of user 1’s key is sum of \( r_{1S} \) and \( r_{1C} \), we should prove the independency of the keys of the two steps. When analyzing term A of the security condition, we show that \( I(K_{1S}; S_{1}^N, X_2^N, Y_2^N, K_{1C}) \leq \frac{N\varepsilon}{3} \) and hence \( I(K_{1S}; K_{1C}) \leq N\varepsilon \), and this completes the proof of theorem 1.

APPENDIX II

Proof of the explicit outer bound in Lemma 1

First, users 1 and 2 generate secret keys \( K_1 \) and \( K_2 \), respectively, as stochastic functions \( K_1 = f_1(S_{1}^N) \) and \( K_2 = f_2(S_{1}^N) \). Then, they determine the channel inputs as stochastic functions \( X_1^N = f_3(S_{1}^N) \) and \( X_2^N = f_4(S_{2}^N) \) and send them via The GDMMAC. Consequently, \( Y_1^N, Y_2^N \) and \( Y_3^N \) are received by user 1, user 2 and user 3, respectively. User 3 should be able to reconstruct the secret keys and according to Fano’s inequality for an arbitrary small \( \varepsilon > 0 \):

\[ H(K_1, K_2 | Y_3^N, S_3^N) \leq \frac{N}{N}(\frac{H(\varepsilon)}{N} + \varepsilon \log |K_1| |K_2| - 1) \]

where \( \varepsilon_1 \rightarrow 0 \) if \( \varepsilon \rightarrow 0 \). Also, the following security conditions should be satisfied as:

\[ I(K_1; S_{1}^N, X_2^N, Y_2^N) < N\varepsilon, \quad I(K_2; S_{1}^N, X_1^N, Y_1^N) < N\varepsilon. \]
Now, we show that for the secret keys satisfying the reliability outer bound of $Y^c$, we have

$$\frac{1}{N} H(K_1 | S_1^N, X_2^N, Y_2^N) + \epsilon \leq \frac{1}{N} H(K_1 | S_1^N, X_2^N, Y_2^N) + \epsilon$$

where (a) results from the security condition, (b) from the fact that $H(X_1|X_2) = 0$, (c) from Fano’s inequality, and (d) from the reliability outer bound of $Y^c$. Thus, the explicit outer bound of Lemma 1 and the outer bound on $R_1$ (symmetry can be used for $R_2$).

$$R_1 = \frac{1}{N} H(K_1 | S_1^N, X_2^N, Y_2^N) + \epsilon \leq \frac{1}{N} H(K_1 | S_1^N, X_2^N, Y_2^N) + \epsilon$$

where (a) results from the security condition, (b) from the fact that $H(X_1|X_2) = 0$, (c) from Fano’s inequality, and (d) from the reliability outer bound of $Y^c$. Thus, the explicit outer bound of Lemma 1 and the outer bound on $R_1$ (symmetry can be used for $R_2$).

$$R_1 = \frac{1}{N} H(K_1 | S_1^N, X_2^N, Y_2^N) + \epsilon \leq \frac{1}{N} H(K_1 | S_1^N, X_2^N, Y_2^N) + \epsilon$$

where (a) results from the security condition, (b) from the fact that $H(X_1|X_2) = 0$, (c) from Fano’s inequality, and (d) from the reliability outer bound of $Y^c$. Thus, the explicit outer bound of Lemma 1 and the outer bound on $R_1$ (symmetry can be used for $R_2$).

$$R_1 = \frac{1}{N} H(K_1 | S_1^N, X_2^N, Y_2^N) + \epsilon \leq \frac{1}{N} H(K_1 | S_1^N, X_2^N, Y_2^N) + \epsilon$$

where (a) results from the security condition, (b) from the fact that $H(X_1|X_2) = 0$, (c) from Fano’s inequality, and (d) from the reliability outer bound of $Y^c$. Thus, the explicit outer bound of Lemma 1 and the outer bound on $R_1$ (symmetry can be used for $R_2$).

$$R_1 = \frac{1}{N} H(K_1 | S_1^N, X_2^N, Y_2^N) + \epsilon \leq \frac{1}{N} H(K_1 | S_1^N, X_2^N, Y_2^N) + \epsilon$$

where (a) results from the security condition, (b) from the fact that $H(X_1|X_2) = 0$, (c) from Fano’s inequality, and (d) from the reliability outer bound of $Y^c$. Thus, the explicit outer bound of Lemma 1 and the outer bound on $R_1$ (symmetry can be used for $R_2$).

$$R_1 = \frac{1}{N} H(K_1 | S_1^N, X_2^N, Y_2^N) + \epsilon \leq \frac{1}{N} H(K_1 | S_1^N, X_2^N, Y_2^N) + \epsilon$$

where (a) results from the security condition, (b) from the fact that $H(X_1|X_2) = 0$, (c) from Fano’s inequality, and (d) from the reliability outer bound of $Y^c$. Thus, the explicit outer bound of Lemma 1 and the outer bound on $R_1$ (symmetry can be used for $R_2$).

$$R_1 = \frac{1}{N} H(K_1 | S_1^N, X_2^N, Y_2^N) + \epsilon \leq \frac{1}{N} H(K_1 | S_1^N, X_2^N, Y_2^N) + \epsilon$$

where (a) results from the security condition, (b) from the fact that $H(X_1|X_2) = 0$, (c) from Fano’s inequality, and (d) from the reliability outer bound of $Y^c$. Thus, the explicit outer bound of Lemma 1 and the outer bound on $R_1$ (symmetry can be used for $R_2$).

$$R_1 = \frac{1}{N} H(K_1 | S_1^N, X_2^N, Y_2^N) + \epsilon \leq \frac{1}{N} H(K_1 | S_1^N, X_2^N, Y_2^N) + \epsilon$$

where (a) results from the security condition, (b) from the fact that $H(X_1|X_2) = 0$, (c) from Fano’s inequality, and (d) from the reliability outer bound of $Y^c$. Thus, the explicit outer bound of Lemma 1 and the outer bound on $R_1$ (symmetry can be used for $R_2$).

$$R_1 = \frac{1}{N} H(K_1 | S_1^N, X_2^N, Y_2^N) + \epsilon \leq \frac{1}{N} H(K_1 | S_1^N, X_2^N, Y_2^N) + \epsilon$$

where (a) results from the security condition, (b) from the fact that $H(X_1|X_2) = 0$, (c) from Fano’s inequality, and (d) from the reliability outer bound of $Y^c$. Thus, the explicit outer bound of Lemma 1 and the outer bound on $R_1$ (symmetry can be used for $R_2$).

$$R_1 = \frac{1}{N} H(K_1 | S_1^N, X_2^N, Y_2^N) + \epsilon \leq \frac{1}{N} H(K_1 | S_1^N, X_2^N, Y_2^N) + \epsilon$$

where (a) results from the security condition, (b) from the fact that $H(X_1|X_2) = 0$, (c) from Fano’s inequality, and (d) from the reliability outer bound of $Y^c$. Thus, the explicit outer bound of Lemma 1 and the outer bound on $R_1$ (symmetry can be used for $R_2$).

$$R_1 = \frac{1}{N} H(K_1 | S_1^N, X_2^N, Y_2^N) + \epsilon \leq \frac{1}{N} H(K_1 | S_1^N, X_2^N, Y_2^N) + \epsilon$$

where (a) results from the security condition, (b) from the fact that $H(X_1|X_2) = 0$, (c) from Fano’s inequality, and (d) from the reliability outer bound of $Y^c$. Thus, the explicit outer bound of Lemma 1 and the outer bound on $R_1$ (symmetry can be used for $R_2$).

$$R_1 = \frac{1}{N} H(K_1 | S_1^N, X_2^N, Y_2^N) + \epsilon \leq \frac{1}{N} H(K_1 | S_1^N, X_2^N, Y_2^N) + \epsilon$$

where (a) results from the security condition, (b) from the fact that $H(X_1|X_2) = 0$, (c) from Fano’s inequality, and (d) from the reliability outer bound of $Y^c$. Thus, the explicit outer bound of Lemma 1 and the outer bound on $R_1$ (symmetry can be used for $R_2$).

$$R_1 = \frac{1}{N} H(K_1 | S_1^N, X_2^N, Y_2^N) + \epsilon \leq \frac{1}{N} H(K_1 | S_1^N, X_2^N, Y_2^N) + \epsilon$$

where (a) results from the security condition, (b) from the fact that $H(X_1|X_2) = 0$, (c) from Fano’s inequality, and (d) from the reliability outer bound of $Y^c$. Thus, the explicit outer bound of Lemma 1 and the outer bound on $R_1$ (symmetry can be used for $R_2$).

$$R_1 = \frac{1}{N} H(K_1 | S_1^N, X_2^N, Y_2^N) + \epsilon \leq \frac{1}{N} H(K_1 | S_1^N, X_2^N, Y_2^N) + \epsilon$$

where (a) results from the security condition, (b) from the fact that $H(X_1|X_2) = 0$, (c) from Fano’s inequality, and (d) from the reliability outer bound of $Y^c$. Thus, the explicit outer bound of Lemma 1 and the outer bound on $R_1$ (symmetry can be used for $R_2$).
\[
H(S_N^1, S_N^2 | S_N^3) - H(S_N^1 | X_N^2, Y_N^3, S_N^3) - \\
H(S_N^2 | K_2, X_N^1, Y_N^3, S_N^3)
\]
\[
= H(S_N^1, S_N^2 | S_N^3) - H(S_N^1 | K_1, Y_N^3, S_N^3) - H(S_N^2 | K_2, Y_N^3, S_N^3)
\]
\[
\leq I(S_N^1, S_N^2; K_1, K_2, Y_N^3 | S_N^3)
\]
\[
= H(K_1, K_2, Y_N^3 | S_N^3) - H(K_1, K_2, Y_N^3 | S_N^3, S_N^1, S_N^2)
\]
\[
\leq H(Y_N^3 | S_N^3) - H(Y_N^3 | S_N^3, S_N^1, S_N^2) + N\varepsilon_1
\]
\[
\leq H(Y_N^3) - H(Y_N^3 | X_N^1, X_N^2, S_N^3, S_N^1, S_N^2) + N\varepsilon_1
\]
\[
= H(Y_N^3) - H(Y_N^3 | X_N^1, X_N^2) + N\varepsilon_1 = I(X_N^1, X_N^2; Y_N^3) + N\varepsilon_1
\]
\[
\leq NI(X_N^1, X_N^2; Y_N^3) + N\varepsilon_1
\]

In the above equations, (a) results from the Markov chain 
\((S_N^1, K_1, X_N^1) - S_N^3 - (S_N^2, K_2, X_N^2)\) and (b) from Fano’s inequality.

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] I. Csiszar, P. Narayan, “Common randomness and secret key generation with a helper,” IEEE Trans. Inf. Theory, vol. 46, no. 2, pp.344-366, Mar 2000.
[4] A. Khisti, S. Diggavi, G. Wornell, “Secret key generation using correlated sources and noisy channels,” IEEE Int.Symp. Inf. Theory, Toronto, Canada, pp. 1005-1009, Jul. 2008.
[5] S. Salimi, M. Salmasizadeh, M. R. Aref, “Secret Key Sharing in a New Source Model: Rate Regions,” IET Communications, Vol. 5, Issue 4, pp. 443-455, March 2011.
[6] Y. Liang and V. Poor, “Multiple access channels with confidential messages,” IEEE Trans. Inf. Theory, vol. 54, no. 3, pp. 976-1002, Mar. 2008.
[7] M. Gastpar, “The Wyner-Ziv problem with multiple sources,” IEEE Trans. Inf. Theory, vol. 50, no. 11, pp. 2762 - 2768, Nov. 2004.