Pairwise secret key agreement based on location-derived common randomness

Conference Paper

Author(s):
Salimi, Somayeh; Papadimitratos, Panos

Publication date:
2016

Permanent link:
https://doi.org/10.3929/ethz-a-010646726

Pairwise Secret Key Agreement based on Location-derived Common Randomness

Somayeh Salimi, Panos Papadimitratos
Networked Systems Security Group, School of Electrical Engineering, KTH, Stockholm, Sweden
somayen@kth.se, papadim@.kth.se

***Abstract*—A source model of key sharing between three users is considered in which each pair of them wishes to agree on a secret key hidden from the remaining user. There are rate-limited public channels for communications between the users. We give an inner bound on the secret key capacity region in this framework. Moreover, we investigate a practical setup in which localization information of the users as the correlated observations are exploited to share pairwise keys between the users. The inner and outer bounds of the key capacity region are analyzed in this setup for the case of i.i.d. Gaussian observations.**

I. Introduction

Secret key sharing at the physical layer is a promising approach for deriving shared secret keys. Ahlswede and Csiszar [1] and Maurer [2] introduced source and channel models of key sharing between two legitimate users in the presence of an eavesdropper using source and channel common randomness along with an unlimited public channel. Various extensions considered a limited public channel [3], sharing of one secret key in a network of users [4], and more than one secret key in different scenarios [5]– [11].

Pairwise key sharing first introduced in [11], is a specific problem in this area, requiring that each pair of users shares a secret key concealed from the remaining user(s). In a basic setup including three users with access to correlated source observations and communication over an unlimited public channel, inner and outer bounds on the secret key capacity region were derived. In this paper, we extend the pairwise key sharing framework in [11] to the rate-limited public channel for communications. The public channel is full duplex and each of the users can simultaneously send/receive information over/from the public channel. Based on the correlated observations, users communicate over the rate-limited public channel. Then, each user generates the respective keys as functions of its source observations and the information received over the rate-limited public channel. We derive an inner bound on the key capacity region in this framework; the explicit outer bound given in [11] holds here for the rate-limited public channel case.

We consider location-derived common randomness here because it is a promising, towards practical applications, approach. This is so because a multitude of emerging wireless systems are location-aware and devices can and need to perform distance measurements over RF communication, notably for security reasons, for example [12], [13].

Location-derived common randomness was considered in [14] in a different setup, with a key established between a mobile node and a wireless infrastructure. In a setup closer to the one considered here, [15] considered two users that move according to a discrete time stochastic mobility model and measure their respective distance, after exchanging messages, in the presence of an eavesdropper. In this paper, leveraging the latter approach, we generalize location-derived key sharing to the "pairwise secret key"setting, notably with three users. We present inner bounds of the pairwise key capacity region for both unlimited and limited public channels. Furthermore, the explicit outer bound in [11] is analyzed in this i.i.d. Gaussian setup. Some numerical results are given for the Gaussian setup as well.

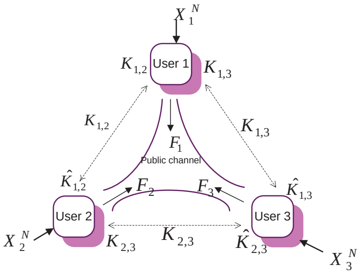

Fig. 1: Pairwise secret key sharing in the source model

The proposed scheme can be extended to the case of more than three users as the future work in which collusion of curious users needs to be investigated. Here we consider simply users curious about the keys their peers derive. But they do not otherwise deviate from the specification and disrupt the protocol.

The rest of the paper is organized as follows: in Section II, the preliminaries of the key sharing setup are given. An inner bound of the pairwise key capacity region with rate-limited public channel is given in Sections III. Deriving pairwise keys from localization information along with the respective inner and outer bounds are presented in Section IV. Numerical results and concluding remarks are given in Sections V and VI, respectively. Proofs of the results are presented in Appendices.

II. Preliminaries

Users 1, 2 and 3, respectively, have access to n i.i.d. observations X_1, X_2 and X_3 according to Fig. 1. The observations are correlated according to distribution $P_{X_1X_2X_3}$. The random variable X_i takes values from the finite set $\mathcal{X}_i$ for $i = 1, 2, 3$. Furthermore, there exists a noiseless public channel of limited capacity for communication between the three users where user i is subject to rate constraint R_i for its transmission. Each pair of the three users intends to share a secret key concealed from the remaining user. $K_{i,j}$ denotes the shared key between users i and j, hidden from user m, for $i, j, m \in \{1, 2, 3\}$, $i < j$, $m \neq i, j$.

We represent the formal definition of the described secret key sharing setup.

User i sends stochastic function $F_i = f_i(X_i^n)$ over the rate-limited public channel for $i = 1, 2, 3$ subject to

$$\frac{1}{n}H(F_i) \leq R_i \tag{1}$$

Upon receiving the information over the public channel, key generation is performed at the users. Key generation function g_i is used by user i for $i = 1, 2, 3$ as:

$$g_1 : \mathcal{F}_2 \times \mathcal{F}_3 \times \mathcal{X}_1^n \rightarrow \mathcal{K}_{1,2} \times \mathcal{K}_{1,3} \tag{2}$$
$$g_2 : \mathcal{F}_1 \times \mathcal{F}_3 \times \mathcal{X}_2^n \rightarrow \mathcal{K}_{1,2} \times \mathcal{K}_{2,3} \tag{3}$$
$$g_3 : \mathcal{F}_1 \times \mathcal{F}_2 \times \mathcal{X}_3^n \rightarrow \mathcal{K}_{1,3} \times \mathcal{K}_{2,3}. \tag{4}$$

Thus, user 1 calculates $K_{1,2}$ and $K_{1,3}$ to share with users 2 and 3, respectively. Similarly, user 2 calculates $\hat{K}_{1,2}$ and $K_{2,3}$ to share with users 1 and 3 and user 3 calculates $\hat{K}_{1,3}$ and $\hat{K}_{2,3}$ to share with users 1 and 2.

Definition 1: In the pairwise secret key sharing over public channels of limited rates (R_1, R_2, R_3) at the respective users 1, 2, 3, the rate triple (R_{12}, R_{13}, R_{23}) is an achievable key rate pair if for every $\varepsilon > 0$ and sufficiently large n, we have:

$$\forall i < j \in \{1,2,3\} \quad \frac{1}{n}H(K_{i,j}) \geq R_{ij} - \epsilon \tag{5}$$
$$\forall i < j \in \{1,2,3\} \quad \Pr\{K_{i,j} \neq \hat{K}_{i,j}\} < \varepsilon \tag{6}$$
$$\forall i{<}j, m{\in}\{1,2,3\}, m \notin \{i,j\} \quad I(K_{i,j}; F_i, F_j, X_m^n) < \varepsilon \tag{7}$$
$$\forall i{\in}\{1,2,3\} \quad \frac{1}{n}H(F_i) \leq R_i. \tag{8}$$

Equation (5) means that rate R_{ij} is the rate of the secret key between users i and j. Equation (6) means that each user can correctly estimate the respective keys. Equation (7) means that each user effectively has no information about the remaining users' secret key. Equation (8) denotes that the key sharing is subject to the constraint of the public channel.

Definition 2: The region containing the entire achievable secret key rate triples (R_{12}, R_{13}, R_{23}) is the secret key capacity region.

III. Main Result

In the following, an inner bound on the pairwise key capacity region of the source model with rate-limited public channel is given. First, we define:

$$\begin{aligned}
&\mathbf{r_{12}} = [I(S_{12}; X_2 \,|S_{23}S_{32}) - I(S_{12}; X_3, S_{13} \,|S_{23}, S_{32})]^+,\\
&\mathbf{r_{21}} = [I(S_{21}; X_1 \,|S_{13}S_{31}) - I(S_{21}; X_3, S_{23} \,|S_{13}, S_{31})]^+,\\
&\mathbf{r_{13}} = [I(S_{13}; X_3 \,|S_{23}S_{32}) - I(S_{13}; X_2, S_{12} \,|S_{23}, S_{32})]^+,\\
&\mathbf{r_{31}} = [I(S_{31}; X_1 \,|S_{12}S_{21}) - I(S_{31}; X_2, S_{32} \,|S_{12}, S_{21})]^+,\\
&\mathbf{r_{23}} = [I(S_{23}; X_3 \,|S_{13}S_{31}) - I(S_{23}; X_1, S_{21} \,|S_{13}, S_{31})]^+,\\
&\mathbf{r_{32}} = [I(S_{32}; X_2 \,|S_{12}S_{21}) - I(S_{32}; X_1, S_{31} \,|S_{12}, S_{21})]^+,\\
&\mathbf{I_{12}} = I(S_{12}; S_{21} \,|X_3, S_{13}, S_{23}),\\
&\mathbf{I_{13}} = I(S_{13}; S_{31} \,|X_2, S_{12}, S_{32}),\\
&\mathbf{I_{23}} = I(S_{23}; S_{32} \,|X_1, S_{21}, S_{31}), \mathbf{I_1} = I(S_{21}; S_{31} \,|X_1),\\
&\mathbf{I_2} = I(S_{12}; S_{32} \,|X_2), \mathbf{I_3} = I(S_{13}; S_{23} \,|X_3).
\end{aligned}$$

Theorem 1: In the described setup, all rates in the closure of the convex hull of the set of all key rate triples (R_{12}, R_{13}, R_{23}) that satisfy the following region, are achievable:

$$\begin{aligned}
&R_{12} > 0, R_{13} > 0, R_{23} > 0,\\
&R_{12} \leq \mathbf{r_{12}} + \mathbf{r_{21}} - \mathbf{I_{12}},\\
&R_{13} \leq \mathbf{r_{13}} + \mathbf{r_{31}} - \mathbf{I_{13}},\\
&R_{23} \leq \mathbf{r_{23}} + \mathbf{r_{32}} - \mathbf{I_{23}},\\
&R_{12} + R_{13} \leq \mathbf{r_{12}} + \mathbf{r_{21}} + \mathbf{r_{13}} + \mathbf{r_{31}} - \mathbf{I_{12}} - \mathbf{I_{13}} - \mathbf{I_1},\\
&R_{12} + R_{23} \leq \mathbf{r_{12}} + \mathbf{r_{21}} + \mathbf{r_{23}} + \mathbf{r_{32}} - \mathbf{I_{12}} - \mathbf{I_{23}} - \mathbf{I_2},\\
&R_{13} + R_{23} \leq \mathbf{r_{13}} + \mathbf{r_{31}} + \mathbf{r_{23}} + \mathbf{r_{32}} - \mathbf{I_{13}} - \mathbf{I_{23}} - \mathbf{I_3},\\
&R_{12} + R_{13} + R_{23} \leq \mathbf{r_{12}} + \mathbf{r_{21}} + \mathbf{r_{13}} + \mathbf{r_{31}} + \mathbf{r_{23}} + \mathbf{r_{32}} -\\
&\qquad \mathbf{I_{12}} - \mathbf{I_{13}} - \mathbf{I_{23}} - \mathbf{I_1} - \mathbf{I_2} - \mathbf{I_3}
\end{aligned} \tag{9}$$

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

$$p(s_{12}, s_{13}, s_{21}, s_{23}, s_{31}, s_{32}, x_1, x_2, x_3) = p(x_1, x_2, x_3).$$
$$p(s_{12}|x_1)p(s_{13}|x_1)p(s_{21}|x_2)p(s_{23}|x_2)p(s_{31}|x_3)p(s_{32}|x_3)$$

and subject to the constraints:

$$I(S_{12};X_1|X_2,S_{32}) + I(S_{13};X_1|X_3,S_{23}) \leq R_1, \tag{10}$$
$$I(S_{21};X_2|X_1,S_{31}) + I(S_{23};X_2|X_3,S_{13}) \leq R_2, \tag{11}$$
$$I(S_{31}; X_3|X_1,S_{21}) + I(S_{32};X_3|X_2,S_{12}) \leq R_3, \tag{12}$$
$$\begin{aligned}&I(S_{12};X_1|X_2,S_{32}) + I(S_{21};X_2|X_1,S_{31}) + I(S_{13},S_{23};X_1,X_2|X_3)\\ &\leq R_1 + R_2,\end{aligned} \tag{13}$$
$$\begin{aligned}&I(S_{13};X_1|X_3,S_{23}) + I(S_{31};X_3|X_1,S_{21}) + I(S_{12},S_{32};X_1,X_3|X_2)\\ &\leq R_1 + R_3,\end{aligned} \tag{14}$$
$$\begin{aligned}&I(S_{23};X_2|X_3,S_{13}) + I(S_{32};X_3|X_2,S_{12}) + I(S_{21},S_{31};X_2,X_3|X_1)\\ &\leq R_2 + R_3.\end{aligned} \tag{15}$$
$$\begin{aligned}&I(S_{21},S_{31};X_2,X_3|X_1) + I(S_{12},S_{32};X_1,X_3|X_2) + I(S_{13},S_{23};X_1,X_2|X_3)\\ &\leq R_1 + R_2 + R_3.\end{aligned} \tag{16}$$

Proof: The proof of Theorem 1 is given in Appendix A in the extended version [18]. ■

The rate region in Theorem 1 is achieved by double random binning as well as Wyner-Ziv coding [16] and rate splitting. In the achievability scheme, the rate of the key between users i and j consists of two parts. A part is rate of the key generated by user i to share with user j ($\mathbf{r}_{ij}$) and the other part is the rate of the key generated by user j to share with user i ($\mathbf{r}_{ji}$). The auxiliary random variable S_{ij} stands for the former key while S_{ji} is associated with the latter key. The total rate of the key between users i and j is the sum of $\mathbf{r}_{ij}$ and $\mathbf{r}_{ji}$ in which term $\mathbf{I}_{ij}$ is subtracted to avoid revealing any information about one of the key to the remaining user (as the eavesdropper) in the case that the other key is disclosed. The limitation of the public channel at the users is reflected in (10)-(16).

Remark 1: The region in Theorem 1 reduces to key rate regions in [7] by considering subset of keys and assuming unlimited public channel. It also reduces to the key rate region in [11] by removing public channel limitations.

We do not present a new outer bound on the key capacity region. The explicit outer bound in [11] with unlimited public channel holds in this new setup.

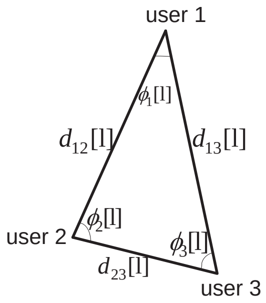

Fig. 2: Using location information for Pairwise secret key sharing

IV. A Real-World Example of the Pairwise Key Sharing

In this section, we consider pairwise key sharing between three users who move in two-dimensional space according to a discrete time stochastic mobility model. The idea of using localization information to share a secret key between two users in the presence of an eavesdropper was first introduced in [15]. Here, we extend this idea to the pairwise key sharing between three users. The users are mobile in continuous space according to a discrete time stochastic mobility model, independent of each other. Each pair of the three mobile users exploits the distance between themselves as a source of common randomness to share a key while the remaining user tries to make an estimate of that distance as precise as possible. We borrow some notations from [15]. We assume the considered time is divided into n discrete time slots where time slot l includes the time interval $[lT,(l+1)T]$. The users' locations are assumed constant during a time slot. As shown in Fig. 2, at time slot l, the distance between users i and j is $d_{ij}[l] = |x_i[l] - x_j[l]|$ in which $x_i[l] \in \mathbb{R}^2$ is the random variable which denotes user i location at time slot l. In the same figure, $\phi_i[l]$ shows the angle of the triangle at user i at time slot l. Each pair first exchanges beacon signals (e.g., using propagation delay) to make correlated observations and then, they communicate over the (limited) public channel to share a key hidden from the remaining user. This is performed in two phases as follow.

Localization phase: User i broadcast some beacons (as a short signal bearing localization information on the initiating node) at the beginning of time slot l and users j and m obtain noisy observations of $d_{ji}[l]$ and $d_{mi}[l]$, respectively, for $i \in \{1,2,3\}, j \neq m \in \{1,2,3\} - i$. We assume the users are equipped to directional antenna and hence, user i obtain $\hat{\phi}_i[l]$ as the noisy version of the angle between the remaining two users. The same as in [15], we assume the sent information by the users is corrupted by Gaussian noises. We have:

$$\tilde{d}_{ij}[l] = d_{ij}[l] + N_{ij}[l] \tag{17}$$

$$\tilde{\phi}_i[l] = \phi_i[l] + N_i[l] \tag{18}$$

where $N_{ij}[l]$ and $N_i[l]$ are zero-mean Gaussian noises with variances σ^2_{ij} and σ^2_i, respectively. All the noises are independent of each other. In the rest of the paper, we consider the case of i.i.d. locations and additive noises. Thus, we drop index l in equations (17)-(18). If the number of broadcast beacons by each user is $J \geq 1$, then σ^2_{ij} and σ^2_i are divided by J [15]. We assume that users are perfectly clock synchronized (it is shown in [15] that clock mismatch does not affect the theoretical bounds of secret key rates).

Key generation by public channel communications: At the beginning of this phase, user i has access to its observations

$$\mathbf{o}_i = \{\tilde{\mathbf{d}}_{ij} = \{\tilde{d}_{ij}[l]\}_{l=1}^{n}, \tilde{\mathbf{d}}_{im} = \{\tilde{d}_{im}[l]\}_{l=1}^{n}, \tilde{\boldsymbol{\phi}}_i = \{\tilde{\phi}_i[l]\}_{l=1}^{n}\} \tag{19}$$

The users communicate over a (rate-limited) public channel to share secret keys in the pairwise manner. Users i and j exploit the reciprocity of the distance between themselves to share a key based on their noisy observations $\tilde{\mathbf{d}}_{ij}$ and $\tilde{\mathbf{d}}_{ji}$, respectively:

$$\tilde{d}_{ij} = d_{ij} + N_{ij} \tag{20}$$

$$\tilde{d}_{ji} = d_{ji} + N_{ji}, \tag{21}$$

where $d_{ij} = d_{ji}$ is the real distance and $N_{ij} \sim \mathcal{N}(0, \sigma^2_{ij}/J)$, $N_{ji} \sim \mathcal{N}(0, \sigma^2_{ji}/J)$ assuming each user broadcasted J beacons at the localization phase. On the other hand, the remaining user m tries to estimate d_{ij} to obtain information about the key between users i and j as much as possible with access to $(\tilde{d}_{mi}, \tilde{d}_{mj}, \tilde{\phi}_m)$.

Due to simplicity, we assume $\sigma_{ij} = \sigma_{ji}$ between each pair i and j. In continue, we consider unlimited and rate-limited public channels separately.

A. unlimited public channel

Since the observation between pair i and j is symmetric (because of $\sigma_{ij} = \sigma_{ji}$) and the public channels at both sides are unlimited, we choose one-way communication between each pair. Without loss of generality, it is assumed that user 1 communicates to user 2, user 2 communicates to user 3 and user 3 communicates to user 1. According to the directions of communications between users, we choose $S_{12} = \tilde{d}_{12}, S_{23} = \tilde{d}_{23}, S_{31} = \tilde{d}_{31}, S_{21} = S_{32} = S_{13} = \phi$ in Theorem 1. Then the rate region in Theorem 1 is reduced to:

$$R_{12} > 0, R_{13} > 0, R_{23} > 0, \tag{22}$$

$$R_{12} \leq I(\tilde{d}_{12};\tilde{d}_{21}) - I(\tilde{d}_{12};\tilde{d}_{31},\tilde{d}_{32},\tilde{\phi}_3) \tag{23}$$

$$R_{13} \leq I(\tilde{d}_{31};\tilde{d}_{13}) - I(\tilde{d}_{31};\tilde{d}_{21},\tilde{d}_{23},\tilde{\phi}_2) \tag{24}$$

$$R_{23} \leq I(\tilde{d}_{23};\tilde{d}_{32}) - I(\tilde{d}_{23};\tilde{d}_{12},\tilde{d}_{13},\tilde{\phi}_1) \tag{25}$$

Each potential eavesdropper combines its available observations to estimate the distance between the other two users to enlarge the subtracted mutual information terms in (23)-(25). Thus, user m as a potential eavesdropper of the key between users i and j makes estimate of d_{ij} as:

$$\hat{d}_{ij} = \sqrt{\tilde{d}^2_{mi} + \tilde{d}^2_{mj} - 2\tilde{d}_{mi}\tilde{d}_{mj}\cos(\tilde{\phi}_m)} \tag{26}$$

where the parameters inside the square root are defined as (17) and (18). For $J \gg 1$, $\sigma^2_{ij}/J \ll d^2_{ij}$ and $\sigma^2_i/J \approx 0$, $\forall i \neq j \in \{1,2,3\}$ with high probability and (26) can be approximated as [15]:

$$\hat{d}_{ij} = d_{ij} + \mathcal{N}(0, \frac{\hat{\sigma}^2_{ij}}{J}) \tag{27}$$

Substituting (27) as the estimate of d_{ij} in (23)-(25) results in the following rate region (it can be shown that this is the best that each potential eavesdropper can do):

Theorem 2: Using unlimited public channel in the pairwise key sharing from the localization information, all rates in the closure of the convex hull of the set of all key rate triples (R_{12}, R_{13}, R_{23}) that satisfy the following region, are achievable:

$$R_{12} > 0, R_{13} > 0, R_{23} > 0, \tag{28}$$

$$R_{12} \leq \frac{1}{2}\mathbb{E}([\log(1 + \frac{d_{12}^4 J^2(\hat{\sigma}_{12}^2 - \sigma_{12}^2)}{(d_{12}^2 J + \hat{\sigma}_{12}^2)(2d_{12}^2 J\sigma_{12}^2 + \sigma_{12}^4)})]^+) \tag{29}$$

$$R_{13} \leq \frac{1}{2}\mathbb{E}([\log(1 + \frac{d_{13}^4 J^2(\hat{\sigma}_{13}^2 - \sigma_{13}^2)}{(d_{13}^2 J + \hat{\sigma}_{13}^2)(2d_{13}^2 J\sigma_{13}^2 + \sigma_{13}^4)})]^+)) \tag{30}$$

$$R_{23} \leq \frac{1}{2}\mathbb{E}([\log(1 + \frac{d_{23}^4 J^2(\hat{\sigma}_{23}^2 - \sigma_{23}^2)}{(d_{23}^2 J + \hat{\sigma}_{23}^2)(2d_{23}^2 J\sigma_{23}^2 + \sigma_{23}^4)})]^+) \tag{31}$$

in which $\mathbb{E}$ is the expectation with respect to (d_{12}, d_{13}, d_{23}) and

$$\hat{\sigma}_{ij}^2 \triangleq \sigma_{im}^2 + \sigma_{jm}^2 + \text{Const}_{d_{12},d_{13},d_{23}}(\frac{\sigma_m^2}{4d_{ij}^2} - \frac{\sigma_{im}^2}{4d_{ij}^2 d_{im}^2} - \frac{\sigma_{jm}^2}{4d_{ij}^2 d_{jm}^2}) \tag{32}$$

for $\text{Const}_{d_{12},d_{13},d_{23}} = (d_{12} + d_{13} + d_{23})(d_{12} + d_{13} - d_{23})(d_{13} + d_{23} - d_{12})(d_{12} + d_{23} - d_{13})$.

Proof: The proof is given in Appendix B in [18]. ■

In the following, we give an outer bound on the key capacity region in the described setup for unlimited public channel based on the explicit outer bound in [11].

Corollary 1: Using unlimited public channel in the pairwise key agreement from localization information, the following is an outer bound on the pairwise key capacity region:

$$R_{12} > 0, R_{13} > 0, R_{23} > 0, R_{12} \leq \frac{1}{2}\log(1 + \frac{\mathbb{E}(\hat{\sigma}_{12}^2)}{\sigma_{12}^2}) \tag{33}$$

$$R_{13} \leq \frac{1}{2}\log(1 + \frac{\mathbb{E}(\hat{\sigma}_{13}^2)}{\sigma_{13}^2}) \tag{34}$$

$$R_{23} \leq \frac{1}{2}\log(1 + \frac{\mathbb{E}(\hat{\sigma}_{23}^2)}{\sigma_{23}^2}) \tag{35}$$

in which $\mathbb{E}$ is expected value with respect to (d_{12}, d_{13}, d_{23}) and $\hat{\sigma}_{ij}^2$ is defined as (32).

Proof: The proof is given in Appendix C [18]. ■

B. rate-limited public channel

In this case, the information sent by the users over the public channel should be subject to the respective rate constraints. In particular, a noisy version of the observation at each user can be considered for the key generation. To apply this constraint, we set:

$$S_{ij} = \tilde{d}_{ij} + D_{ij} \tag{36}$$

in Theorem 1 where $D_{ij} \sim \mathcal{N}(0, \sigma_{ij}'^2)$. The noises D_{ij} are independent of each other and of all the observations. In fact S_{ij} is a noisy version of $\tilde{d}_{ij}$ where its related information can be sent by user i through the public channel with rate constraint R_i. It should be noted that in the case of rate-limited public channel, we can not assume one-way communication between each pair and we need to consider the general two-way communications to derive the largest rate region. By considering all the auxiliary random variables of Theorem 1 as (36) and applying the rate constraints in (10)-(16) in Theorem 1, we deduce:

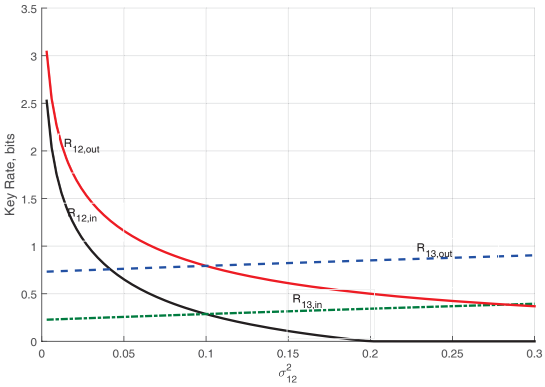

Fig. 3: inner and outer bounds on R_{12} and R_{13}

Theorem 3: Using public channels with rates (R_1, R_2, R_3), respectively, at users 1,2,3 in the pairwise key sharing from localization information, the pairwise key rate region on the top of the next page is achievable which is subject to the constraints:

$$\begin{aligned}
&\frac{1}{2}\mathbb{E}(\log(1 + \frac{(2d_{12}^2 J + \sigma_{12}^2)\sigma_{12}^2}{(d_{12}^2 J + \sigma_{12}^2)\sigma_{12}'^2}) + \log(1 + \frac{(2d_{13}^2 J + \sigma_{13}^2)\sigma_{13}^2}{(d_{13}^2 J + \sigma_{13}^2)\sigma_{13}'^2})) \leq R_1 \\
&\frac{1}{2}\mathbb{E}(\log(1 + \frac{(2d_{12}^2 J + \sigma_{12}^2)\sigma_{12}^2}{(d_{12}^2 J + \sigma_{12}^2)\sigma_{21}'^2}) + \log(1 + \frac{(2d_{23}^2 J + \sigma_{23}^2)\sigma_{23}^2}{(d_{23}^2 J + \sigma_{23}^2)\sigma_{23}'^2})) \leq R_2 \\
&\frac{1}{2}\mathbb{E}(\log(1 + \frac{(2d_{13}^2 J + \sigma_{13}^2)\sigma_{13}^2}{(d_{13}^2 J + \sigma_{13}^2)\sigma_{31}'^2}) + \log(1 + \frac{(2d_{23}^2 J + \sigma_{23}^2)\sigma_{23}^2}{(d_{23}^2 J + \sigma_{23}^2)\sigma_{32}'^2})) \leq R_3
\end{aligned} \tag{37}$$

Proof: The proof is given in Appendix B in [18]. ■

V. Numerical Results

In this section, numerical evaluation of the results in Sections IV-A and IV-B is given. We assume that at each time slot, all users' locations are characterized by i.i.d. circularly symmetric zero mean, unit variance Gaussian random variables. First we consider unlimited public channel case. We set $\sigma_{13}^2 = \sigma_{23}^2 = \sigma_1^2 = \sigma_2^2 = \sigma_3^2 = 0.1$ and plot the key rates as functions of σ_{12}^2. Because of symmetry, the bounds on the rates R_{13} and R_{23} are the same and hence, we analyse one of them. In Fig. 3, the inner and outer bounds on key rates R_{12} and R_{13} are shown as functions of σ_{12}^2. Clearly the bounds on R_{12} decrease as σ_{12}^2 increases, while the bounds on R_{13} increase with the growth of σ_{12}^2. However, for small values of σ_{12}^2, the bounds on R_{12} are more affected compared to the bounds on R_{13}.

Then, we analyse the key rate region in the rate-limited public channel case. We set $R_1 = .5$, $R_2 = .2$, $R_3 = .8$ and $\sigma_{12}^2 = \sigma_{13}^2 = \sigma_{23}^2 = \sigma_1^2 = \sigma_2^2 = \sigma_3^2 = 0.1$. In order to clarify the rate region, we project the 3-D region into three 2-D regions. As we discussed in Section IV-B, in the case of rate-limited pubic channel, we have two-way communication between each pair. Each user splits its available public channel rate to share keys with the other users while the public channel rates of the other users affect this splitting. As shown in Fig. 4–6, the rate regions are not necessarily rectangular in contrast to the case of unlimited public channel. Obviously, the achievable rates are significantly smaller than the corresponding values in Fig. 3 where unlimited public channel is assumed (respective rates at Fig. 3 for $\sigma_{12}^2 = 0.1$).

$$R_{12} > 0,\, R_{13} > 0,\, R_{23} > 0, \tag{38}$$

$$\begin{aligned}
R_{12} &\leq \frac{1}{2}\mathbb{E}([\log(1+\frac{d_{12}^4 J^2(\hat{\sigma}_{12}^2-\sigma_{12}^2)}{(d_{12}^2 J+\hat{\sigma}_{12}^2)(d_{12}^2 J(2\sigma_{12}^2+\sigma_{12}'^2)+(\sigma_{12}^2+\sigma_{12}'^2)\sigma_{12}^2)})]^+ + [\log(1+\frac{d_{12}^4 J^2(\hat{\sigma}_{12}^2\sigma_{12}'^2-\sigma_{12}^2(\sigma_{12}^2+\sigma_{12}'^2))}{(d_{12}^2 J(\hat{\sigma}_{12}^2+\sigma_{12}^2+\sigma_{12}'^2)+\hat{\sigma}_{12}^2(\sigma_{12}^2+\sigma_{12}'^2))(d_{12}^2 J(2\sigma_{12}^2+\sigma_{21}'^2)+(\sigma_{12}^2+\sigma_{21}'^2)\sigma_{12}^2)})]^+)\\
R_{13} &\leq \frac{1}{2}\mathbb{E}([\log(1+\frac{d_{13}^4 J^2(\hat{\sigma}_{13}^2-\sigma_{13}^2)}{(d_{13}^2 J+\hat{\sigma}_{13}^2)(d_{13}^2 J(2\sigma_{13}^2+\sigma_{13}'^2)+(\sigma_{13}^2+\sigma_{13}'^2)\sigma_{13}^2)})]^+ + [\log(1+\frac{d_{13}^4 J^2(\hat{\sigma}_{13}^2\sigma_{13}'^2-\sigma_{13}^2(\sigma_{13}^2+\sigma_{13}'^2))}{(d_{13}^2 J(\hat{\sigma}_{13}^2+\sigma_{13}^2+\sigma_{13}'^2)+\hat{\sigma}_{13}^2(\sigma_{13}^2+\sigma_{13}'^2))(d_{13}^2 J(2\sigma_{13}^2+\sigma_{32}'^2)+(\sigma_{13}^2+\sigma_{31}'^2)\sigma_{13}^2)})]^+)\\
R_{23} &\leq \frac{1}{2}\mathbb{E}([\log(1+\frac{d_{23}^4 J^2(\hat{\sigma}_{23}^2-\sigma_{23}^2)}{(d_{23}^2 J+\hat{\sigma}_{23}^2)(d_{23}^2 J(2\sigma_{23}^2+\sigma_{23}'^2)+(\sigma_{23}^2+\sigma_{23}'^2)\sigma_{23}^2)})]^+ [\log(1+\frac{d_{23}^4 J^2(\hat{\sigma}_{23}^2\sigma_{23}'^2-\sigma_{23}^2(\sigma_{23}^2+\sigma_{23}'^2))}{(d_{23}^2 J(\hat{\sigma}_{23}^2+\sigma_{23}^2+\sigma_{23}'^2)+\hat{\sigma}_{23}^2(\sigma_{23}^2+\sigma_{23}'^2))(d_{23}^2 J(2\sigma_{23}^2+\sigma_{32}'^2)+(\sigma_{23}^2+\sigma_{32}'^2)\sigma_{23}^2)})]^+)
\end{aligned} \tag{39}$$

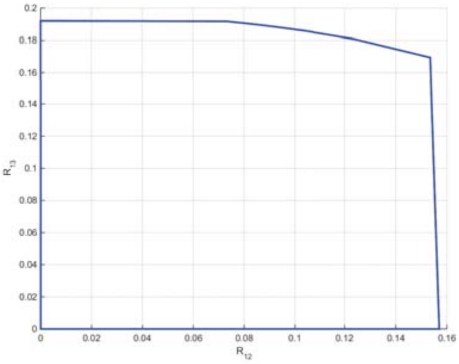

Fig. 4: $R_{12} - R_{13}$ with $R_1 = .5$, $R_2 = .2$,$R_3 = .8$

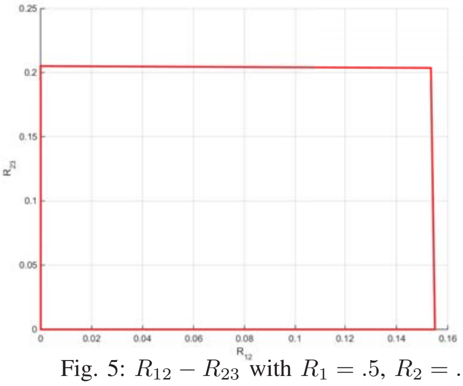

Fig. 5: $R_{12} - R_{23}$ with $R_1 = .5$, $R_2 = .2$,$R_3 = .8$

VI. Conclusion

The source model of pairwise secret key sharing was investigated with rate-limited pubic channel between three users. An inner bound on the key capacity region was derived for the general case of discrete memoryless source observations. We considered a setup in which the users exploited the distance between themselves as correlated observations to generate keys. Inner and outer bounds on the key capacity region were analyzed for the case of i.i.d. Gaussian observations. As a future work, we analyze the problem of pairwise key sharing between arbitrary number of users who access to limited public channel.

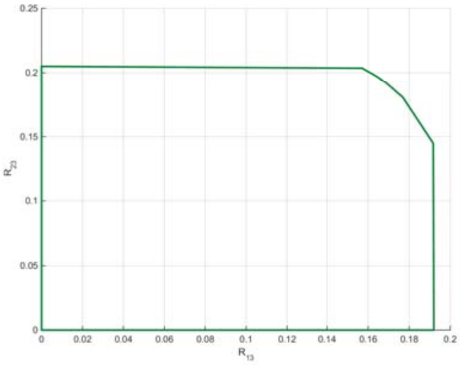

Fig. 6: $R_{13} - R_{23}$ with $R_1 = .5$, $R_2 = .2$,$R_3 = .8$

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] I. Csiszr and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3047–3061, Dec. 2004.

[5] C. Ye, P. Narayan, "The secret key-private key capacity region for three terminals," *IEEE Int .Symp. Inf. Theory*, Adelaide, Australia, pp. 2142–2146, Sep. 2005.

[6] S. Nitinawarat, C. Ye, A. Barg, P. Narayan, A. Reznik, "Secret Key Generation for a Pairwise Independent Network Model," *IEEE Int. Symp. Inf. Theory (ISIT)*, Toronto, Canada, pp. 1015–1019, Jul. 2008.

[7] S. Salimi, M. Salmasizadeh, M. R. Aref, "Rate Regions of Secret Key Sharing in a New Source Model," *IET Communications*, Vol. 5, Issue 4, pp. 443–455, March 2011.

[8] S. Salimi, M. Salmasizadeh, M. R. Aref, J. Dj Golić, "Key Agreement over Multiple Access Channel," *IEEE Trans. on Information Forensics and Security*, vol. 6, Issue 3, pp. 775-790, Sep. 2011.

[9] 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.

[10] S. Salimi, M. Skoglund, J. Dj Golić, M. Salmasizadeh, M. R. Aref, "Key Agreement over a Generalized Multiple Access Channel Using Noiseless and Noisy Feedback," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1765–1778, Sep. 2013.

[11] S. Salimi, M. Skoglund, M. Salmasizadeh, M. R. Aref, "Pairwise Secret Key Agreement Using the Source Common Randomness," *Int. Sym. on Wireless Communication Systems (ISWCS)*, pp. 751–755 , Paris, France, Aug. 2012.

[12] P. Papadimitratos, M. Poturalski, P. Schaller, P. Lafourcade, D. Basin, S. Čapkun, J.-P. Hubaux, "Secure Neighborhood Discovery: A Fundamental Element for Mobile Ad-Hoc Networking," *IEEE Communications Magazine*, vol. 46, no. 2, pp. 132–139, Feb. 2008.

[13] M. Fiore, C. Casetti, C.-F. Chiasserini, P. Papadimitratos, "Discovery and Verification of Neighbor Positions in Mobile Ad Hoc Networks," *IEEE Transactions on Mobile Computing*, vol. 12, no. 2, pp. 289 – 303, Feb. 2013.

[14] C. Neuberg, P. Papadimitratos, C. Fragouli, R. Urbanke, "A Mobile World of Security - The Model," *IEEE Conference on Information Sciences and Systems (CISS)*, Baltimore, MD, USA, Mar. 2011.

[15] O. Gungor, F. Chen, C. E. Koksal, "Secret Key Generation From Mobility," *GLOBECOM Workshop on Physical Layer Security*, pp. 874–878 , Texas, US, Dec. 2011.

[16] 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.

[17] G.B. Dantzig, and B.C. Eaves, "Fourier-Motzkin Elimination and its Dual," *Journal of Combinatorial Theory*, Ser. A, 14:288-297, 1973.

[18] S. Salimi, P. Papadimitratos, "Pairwise Secret Key Agreement based on Location-derived Common Randomness,"Extended version, Available at http://www.arxiv.org