Cooperative Key Generation in Wireless Networks

Lifeng Lai, *Member, IEEE*, Yingbin Liang, *Member, IEEE*, and Wenliang Du, *Member, IEEE*

***Abstract*—The impact of relay nodes on the secret key generation via the physical layer resources is investigated. A novel relay-assisted strategy is proposed to improve the generated secret key rate. The main idea is to exploit the random channels associated with relay nodes in the network as additional random sources for the key generation. This approach is particularly useful when the channels between legitimate nodes change slowly. Four increasingly sophisticated yet more practical scenarios are studied, for which relay-assisted key generation protocols are proposed and are shown to be optimal or order-optimal in terms of the key rate. It is also shown that the multiplexing gain in the key rate scales linearly with the number of relays, which demonstrates that relay-assisted schemes substantially increase the key rate. This is in sharp contrast to scenarios with relays helping information transmission, in which the multiplexing gain does not scale with the number of relays. Furthermore, a cooperative scheme is also proposed in which relays help key generation but the generated keys are kept secure from these relays.**

***Index Terms*—Information theoretic security, key generation, key rate, multiplexing gain, relay-oblivious.**

I. Introduction

RECENTLY, a physical layer (PHY) approach to generate symmetric keys based on wireless channel reciprocity has attracted considerable attentions [2]–[10]. Here, the channel reciprocity refers to the case in which the channel response of the forward channel (from the transmitter to the receiver) is the same as the channel response of the backward channel (from the receiver to the transmitter) in time-division duplex (TDD) systems. Such a random channel serves as a common randomness source for the parties to generate secret keys. Eavesdroppers experience physical channels independent from the legitimate user's channel as long as they are a few wavelengths away from these legitimate nodes, which is generally the case in wireless networks [11]. Thus, the keys are provably secure with an information theoretic guarantee due to the nature of the key generation scheme, as opposed to the crypto keys whose security depends on the assumption of intractability of certain mathematical problems. We also note that the key generated using such a PHY approach can be made uniformly distributed [12], and can hence be used for encryption using the one-time pad scheme. Furthermore, two major properties of such keys greatly facilitate one-time pad encryption using these keys: (1) these keys are already shared by two legitimate terminals via the generation process, which overcomes the typical challenge of key distribution in using the one-time pad encryption; and (2) these keys can be replenished dynamically as wireless channels vary over time, and the key rate can be improved via relay-assisted schemes proposed in this paper, which greatly improves the transmission rate via the one-time pad encryption. Thus, the PHY approach not only produces information theoretically secure keys, but also facilitates information theoretically secure encryption.

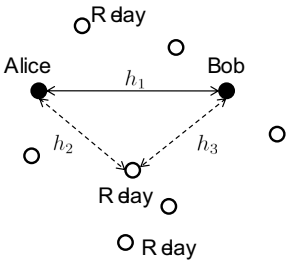


Fig. 1. A network with multiple terminals.

Since the generated key rate via the PHY approach depends critically on how fast the channel between the legitimate parties changes, the key generation rate can be limited in slowly changing wireless environments. In these cases, additional random sources need to be exploited to improve the key rate. In this paper, we propose a novel approach to substantially improve the key rate that can be generated from wireless channels. The main idea is to exploit the presence of multiple relay nodes in wireless networks and use the random channels associated with these relay nodes as additional random sources for the key generation. As illustrated in Figure 1, besides the direct fading link connecting the legitimate users Alice and Bob, the fading channels between Alice and relays and between Bob and relays (depicted as dotted lines in Figure 1) can also serve as additional random sources for key generation.

In this paper, we consider the following adversary model. It is assumed that Eve (i.e., any eavesdropper) listens to transmissions over wireless channels and also has full access to the public channel over which legitimate nodes exchange information. Eve obtains a noisy version of transmissions over wireless channels, and a noiseless version of transmissions over the public channel. Eve is passive, and does not send signals to interfere with legitimate transmissions. Relays are assumed to follow the designed transmission protocols, and not to leak information to Eve (i.e., not to cooperate with Eve). We study two system requirements: one requires the generated key to be secret only from Eve, the other one requires the generated key to be secret not only from Eve, but also from relays. Hence, for the second requirement, relays are assumed to be curious and try to infer as much information about the

Manuscript received 1 August 2011; revised 1 May 2012. The work of L. Lai was supported by the National Science Foundation CAREER Award under Grant CCF-10-54338 and by the National Science Foundation under Grant CNS-11-16534. The work of Y. Liang was supported by the National Science Foundation CAREER Award under Grant CCF-10-26565 and by the National Science Foundation under Grant CNS-11-16932. The work of W. Du was supported by the National Science Foundation under Grant CNS-11-16932. Parts of this paper have been presented at the Forty-Ninth Annual Allerton Conference on Communication, Control, and Computing Sept./Oct. 2011, Monticello, Illinois [1].

L. Lai is with Department of Systems Engineering, University of Arkansas, Little Rock, AR 72204, USA. (e-mail: lxlai@ualr.edu).

Y. Liang and W. Du are with Department of Electrical Engineering and Computer Science, Syracuse University, Syracuse, NY 13244, USA. (e-mail: {yliang06,wedu}@syr.edu).

Digital Object Identifier 10.1109/JSAC.2012.120924.

generated key as possible, but relays do not collude with each other and do not collude with Eve. The privacy of the key (from relays) needs to be guaranteed here in addition to the security of the key (from Eve). The models considered here can be viewed as the first step towards more advanced and practical models.

In this paper, we study four wireless scenarios. In the first scenario, we illustrate our main idea using a simple network consisting of Alice, Bob and a relay node. In this scenario, in addition to the wireless channels, we assume that Alice and Bob can also communicate over a noiseless public channel which is observable to the eavesdropper for key generation. In the second scenario, we consider a more practical system in which there is no public channel. Hence, any information needed for the key agreement should be transmitted over the wireless channels. In the third scenario, we extend our study to general networks with multiple relays. In the fourth scenario, we further impose an additional constraint that the relay nodes should not obtain any information about the generated keys. Our main contributions and results are summarized as follows.

1) Relay schemes are traditionally used to improve the network throughput [13] or the communication reliability [14] for information transmission. This paper develops novel protocols that demonstrate a critical role that relays can play in helping secret key generation.
2) Based on the information theoretic measure of security, we show analytically that the proposed approach is optimal (i.e., maximizes the key rate) for networks with one relay, and is asymptotically optimal as the signal-to-noise ratio (SNR) increases for networks with multiple relays.
3) We use the *multiplexing gain*, defined as the ratio of the key rate with relay cooperation to that without relay cooperation, to quantify the gain in the key rate due to relay cooperation. Interestingly, we show that the multiplexing gain with relay cooperation increases linearly as the number of relays increases, which demonstrates a tremendous gain in the key rate due to relay cooperation. This is also in sharp contrast to the case of information transmission using relays, in which the multiplexing gain does not scale with the number of relays.

The proposed relay-assisted key generation approach enjoys several advantages. First, the key rate scales linearly with the number of relay nodes. Such scalability property is very important for consistently replenishing large-size keys for securing wireless transmissions of large packs. Second, the proposed scheme can be adapted to enjoy the help from relays but keep the generated key secure from relays, thus improving the robustness to node compromise. Third, the proposed approach does not require precise synchronization among nodes, which is often required by cooperation schemes for the information transmission [14].

The remainder of the paper is organized as follows. In Section II, we review the existing results for the PHY-based key generation approach via wireless fading channels without relay cooperation. This section provides necessary background for the developments in the following sections. In Section III, we present our scheme for the relay-assisted key generation for a single-relay network with a public discussion channel. In Section IV, we study the scenario without a public discussion channel. We then extend our study to a general network with multiple relays in Section V. We study the scenario in which the relay is oblivious to the generated keys in Section VI. Finally, we present numerical examples in Section VII and concluding remarks and future directions in Section VIII.

II. Review: Key Generation over Point-to-Point Wireless Channels

In this section, we review the basic ideas of the PHY based key generation by exploiting the channel reciprocity [2]–[8]. This will provide necessary background for further developments in the remainder of the paper, and will also provide the baseline for performance comparison. Suppose two terminals Alice (A) and Bob (B) wish to agree on a key via a wireless fading channel between them in the presence of an eavesdropper Eve (E). Both Alice and Bob can transmit over the wireless channel. They can also send information using the public channel as generally assumed in the literature. (As we discuss in Section IV, we can still establish a key without this public channel). It is assumed that Eve listens to transmissions of Alice and Bob over wireless channels, and also has full access to the information transmitted over the public channel. It is also assumed that Eve is passive, and does not send signals to interfere with legitimate transmissions. The key generation process is not covert, i.e., Eve knows that there is a key agreement process going on, although it does not learn any information about the generated key.

If Alice transmits a signal X_A over the wireless channel, Bob and Eve receive

$$\begin{aligned} Y_B &= h_1 X_A + N_B, \\ Y_E &= h_{AE} X_A + N_E \end{aligned} \tag{1}$$

respectively, in which h_1 and h_{AE} are the random (fading) channel gains from Alice to Bob and Eve, N_B and N_E are zero mean additive Gaussian noises with variance σ^2. Alternatively, if Bob transmits a signal X_B, Alice and Eve receive

$$\begin{aligned} Y_A &= h_1^* X_B + N_A, \\ Y_E &= h_{BE} X_B + N_E \end{aligned} \tag{2}$$

respectively, in which h_1^* and h_{BE} are the channel gains from Bob to Alice and Eve, N_A and N_E are zero mean additive Gaussian noises with variance σ^2. It is reasonable to assume that all additive Gaussian noises are independent of each other. For practical considerations, we consider the half-duplex model, in which neither Alice nor Bob can transmit and receive at the same time. We assume that the channel is reciprocal, i.e., $h_1 = h_1^*$. The protocols developed in this paper are still applicable even this reciprocity does not hold perfectly, as long as the forward channel and backward channel are correlated. Since the signals arriving at different wireless receivers experience different transmission paths, and hence different random phases, the channel gain h_1 is independent of h_{AE} and h_{BE}. We consider an ergodic block fading model, in which the channel gains are fixed for a block of T symbols and change randomly to other values at the beginning of the next block. For simplicity, in this paper, we assume that h_1 is a Gaussian random variable with zero mean and variance σ_1^2, i.e., $h_1 \sim \mathcal{N}(0, \sigma_1^2)$. The results can be easily extended to other fading models. *It is assumed that none of the terminals knows the value of the fading gains initially.*

There are two steps in the key generation via wireless fading channel reciprocity: (1) channel estimation, in which Alice and Bob estimate the common channel gain h_1 via training

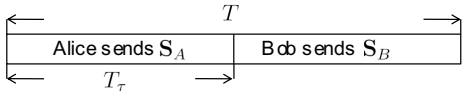


Fig. 2. Training based scheme.

symbols; (2) key agreement, in which Alice and Bob agree on a common random key based on their correlated but imperfect estimations of the channel gain by employing Slepian-Wolf source coding. We next describe these two steps in more detail.

Let T_τ denote the amount of time spent by Alice on training, and let $T - T_\tau$ denote the amount of time used by Bob on training, as depicted in Figure 2. Suppose Alice sends a known sequence $\mathbf{S}_A$ with T_τ components, then Bob receives $\mathbf{Y}_B = h_1\mathbf{S}_A + \mathbf{N}_B$. After that, Bob sends a known sequence $\mathbf{S}_B$ with $T - T_\tau$ components, then Alice receives $\mathbf{Y}_A = h_1\mathbf{S}_B + \mathbf{N}_A$. The observations at Eve during this process are independent of the observations at both Alice and Bob due to its independent channel gains from the transmitters.

To generate a key from these observations, Alice first generates an estimate of the channel gain h_1

$$\tilde{h}_{1,A} = \frac{\mathbf{S}_B^T}{||\mathbf{S}_B||^2}\mathbf{Y}_A = h_1 + \frac{\mathbf{S}_B^T}{||\mathbf{S}_B||^2}\mathbf{N}_A, \tag{3}$$

in which $||\cdot||$ denotes the norm of its argument. Similarly, Bob computes an estimate $\tilde{h}_{1,B}$ of the channel gain h_1

$$\tilde{h}_{1,B} = \frac{\mathbf{S}_A^T}{||\mathbf{S}_A||^2}\mathbf{Y}_B = h_1 + \frac{\mathbf{S}_A^T}{||\mathbf{S}_A||^2}\mathbf{N}_B. \tag{4}$$

Note that $\tilde{h}_{1,A}$ is a zero mean Gaussian random variable with variance $\sigma_1^2 + \frac{\sigma^2}{||S_B||^2}$, and similarly $\tilde{h}_{1,B}$ is a zero mean Gaussian random variable with variance $\sigma_1^2 + \frac{\sigma^2}{||S_A||^2}$. Assuming that Alice and Bob transmit with power P during the training period, we have $||\mathbf{S}_B||^2 = (T - T_\tau)P$ and $||\mathbf{S}_A||^2 = T_\tau P$.

Based on data processing lemma [15], it is easy to see that the following Markovian relationship is true [16]:

$$\tilde{h}_{1,A} \longleftrightarrow \mathbf{Y}_A \longleftrightarrow h_1 \longleftrightarrow \mathbf{Y}_B \longleftrightarrow \tilde{h}_{1,B}, \tag{5}$$

which implies $I(\tilde{h}_{1,A};\tilde{h}_{1,B}) \leq I(\mathbf{Y}_A;\mathbf{Y}_B)$. Similarly, from the Markovian relationship

$$\mathbf{Y}_A \longleftrightarrow \tilde{h}_{1,A} \longleftrightarrow h_1 \longleftrightarrow \tilde{h}_{1,B} \longleftrightarrow \mathbf{Y}_B, \tag{6}$$

we have $I(\tilde{h}_{1,A};\tilde{h}_{1,B}) \geq I(\mathbf{Y}_A;\mathbf{Y}_B)$. As the result, $I(\tilde{h}_{1,A};\tilde{h}_{1,B}) = I(\mathbf{Y}_A;\mathbf{Y}_B)$, which implies that $\tilde{h}_{1,A}$ and $\tilde{h}_{1,B}$ retain the mutual information between $\mathbf{Y}_A$ and $\mathbf{Y}_B$; i.e., they are sufficient for the key generation purpose. From $(\tilde{h}_{1,A},\tilde{h}_{1,B})$, one can generate a key with rate [12]

$$\begin{aligned} R_s &= \frac{1}{T}I(\tilde{h}_{1,A};\tilde{h}_{1,B}) \qquad (7)\\ &= \frac{1}{2T}\log\left(\frac{(\sigma^2+\sigma_1^2PT_\tau)(\sigma^2+\sigma_1^2(T-T_\tau)P)}{\sigma^4+\sigma^2\sigma_1^2PT}\right), \end{aligned}$$

in which the normalization factor $1/T$ is due to the fact that the channel gain is fixed for T symbols, and hence the communication parties can observe *only one* value of the channel statistics for every T symbols. It is obvious that the optimal value of T_τ that maximizes (7) is $T/2$, with which (7) is simplified to

$$R_s = \frac{1}{T}I(\tilde{h}_{1,A};\tilde{h}_{1,B}) = \frac{1}{2T}\log\left(1+\frac{\sigma_1^4P^2T^2}{4(\sigma^4+\sigma^2\sigma_1^2PT)}\right). \tag{8}$$

It is easy to see that the key rate depends on the power P and the coherence time T. As the available power P increases, the key rate increases at an order of $\frac{1}{2T}\log P$. However, as the coherence time T increases (meaning that the channel changes slowly), the key rate decreases at an order of $\frac{1}{2T}\log T$, which approaches to zero.

To generate a uniformly distributed key with the rate in (8), one needs to employ the Slepian-Wolf coding [12] to send helper information from Alice to Bob through the public channel [1] in order to reconciliate the effects of noise in their channel estimates. Somewhat remarkably, the helper data, although observable to Eve, do not leak any information about the generated key to Eve. More specifically, for every N symbol times, which is as large as a number of blocks of symbol times, Alice has $m = \lfloor N/T \rfloor$ observations of the random variable $\tilde{h}_{1,A}$, where $\lfloor\cdot\rfloor$ denotes the largest integer that is smaller than its argument. These observations are collected into a vector $\tilde{\mathbf{h}}_{1,A} = [\tilde{h}^{\Delta}_{1,A}(1),\cdots,\tilde{h}^{\Delta}_{1,A}(m)]^T$, where $\tilde{h}^{\Delta}_{1,A}(i)$ is a quantized version of $\tilde{h}_{1,A}(i)$ with quantization interval being Δ. $\tilde{h}^{\Delta}_{1,A}(i)$'s are independent of each other. Similarly, Bob has a vector of observations $\tilde{\mathbf{h}}_{1,B} = [\tilde{h}^{\Delta}_{1,B}(1),\cdots,\tilde{h}^{\Delta}_{1,B}(m)]^T$. Alice randomly divides the typical $\tilde{h}^{\Delta}_{1,A}$ sequences into non-overlapping bins, with each bin having $2^{mI(\tilde{h}^{\Delta}_{1,A};\tilde{h}^{\Delta}_{1,B})}$ typical $\tilde{h}^{\Delta}_{1,A}$ sequences. Hence, each sequence has two indices: bin number and index within the bin. Now, after observing the vector $\tilde{\mathbf{h}}_{1,A}$, Alice sets the key to be the index of this sequence within its bin. Alice then sends the bin number as the helper data to Bob through the public channel. That is, Alice needs to send $H(\tilde{h}^{\Delta}_{1,A}|\tilde{h}^{\Delta}_{1,B})$ bits of information through the public channel, where $H(X|Y)$ denotes the conditional entropy of X given Y. After combining the information observed from the public channel with $\tilde{\mathbf{h}}_{1,B}$, it can be shown that Bob can recover the value of $\tilde{\mathbf{h}}_{1,A}$ with the probability arbitrarily close to 1. Then Bob can recover the key. It can also be shown that the bin number and index within each bin are independent of each other. Hence, even though the eavesdropper can observe the bin number transmitted over the public channel, it learns no information about the generated key. Now, by letting the quantization level Δ go to zero, one achieve the key rate (8). We note that the key generated using this approach can be shown to be uniformly distributed [12], and can hence be used for encryption using the one-time pad scheme.

III. Relay-Assisted Key Generation With a Public Channel

It is easy to see from (8) that the main limitation on the key rate is the normalization factor $1/T$, due to the fact that there is only one fading realization over T symbol times, i.e., the channel between legitimate nodes change only every T symbol times. When T is large, the generated key rate can be small. We thus propose a relay-assisted scheme for key generation that increases the key rate by exploiting relay nodes in networks.

[1]The case without a public discussion channel will be discussed in Section IV.

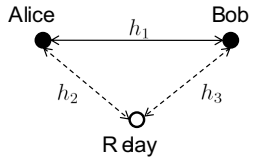


Fig. 3. Key generation with the assistance of one relay.

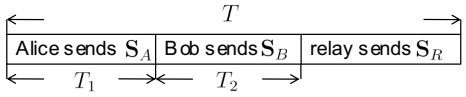


Fig. 4. Time frame for the training based scheme with a relay.

In this section, we consider a simple network with one relay (see Figure 3) to illustrate our basic idea. We then study more general networks with multiple relays in Section V. The relay is assumed to follow the designed transmission protocols, and not to leak information to Eve (i.e., not to cooperative with Eve). The generated key is required to be secure only from Eve, not necessarily from the relay. We assume that the channel gain between Alice and the relay is h_2 and the channel gain between the relay and Bob is h_3. We assume $h_2 \sim \mathcal{N}(0, \sigma_2^2)$ and $h_3 \sim \mathcal{N}(0, \sigma_3^2)$, i.e., they both are Gaussian distributed with means zero and variances σ_2^2 and σ_3^2, respectively. We note that the schemes presented in this paper are also applicable to models with fading coefficients taking other distributions.

In the sequel, we first propose our relay-assisted algorithm for key generation, and then explain the idea of the algorithm in more detail, after which we justify that the proposed algorithm is optimal. The time frame of the scheme is shown in Figure 4.

Algorithm of Key Generation with One Relay

Step 1: Channel Estimation:

- Alice sends a known sequence $\mathbf{S}_A$, from which Bob and the relay obtain estimates $\tilde{h}_{1,B}$ and $\tilde{h}_{2,R}$ respectively.
- Bob sends a known sequence $\mathbf{S}_B$, from which Alice and the relay obtain estimates $\tilde{h}_{1,A}$ and $\tilde{h}_{3,R}$ respectively.
- The relay sends a known sequence $\mathbf{S}_R$, from which Alice and Bob obtain estimates $\tilde{h}_{2,A}$ and $\tilde{h}_{3,B}$ respectively.

Step 2: Key Agreement:

- Alice and Bob agree on a key K_1 from the correlated observations $(\tilde{h}_{1,A}, \tilde{h}_{1,B})$ using the public channel.
- Alice and the relay agree on a key K_2 from the correlated observations $(\tilde{h}_{2,A}, \tilde{h}_{2,R})$ using the public channel.
- Bob and the relay agree on a key K_3 from the correlated observations $(\tilde{h}_{3,B}, \tilde{h}_{3,R})$ using the public channel.
- The relay broadcasts $K_2 \oplus K_3$[2].
- If the size of K_2 is smaller than the size of K_3, Alice and Bob set (K_1, K_2) as the key, otherwise set (K_1, K_3) as the key, where (K_i, K_j) denotes the concatenation of K_i and K_j.

In the channel estimation step of the above algorithm, we adopt a three-way training approach. First, Alice sends a known sequence $\mathbf{S}_A$ with T_1 components (see Figure 4), and Bob and the relay receive

$$\mathbf{Y}_B = h_1 \mathbf{S}_A + \mathbf{N}_B, \quad \mathbf{Y}_R = h_2 \mathbf{S}_A + \mathbf{N}_R, \tag{9}$$

from which Bob obtains an estimate $\tilde{h}_{1,B}$ of h_1 and the relay obtains an estimate $\tilde{h}_{2,R}$ of h_2 via

$$\tilde{h}_{1,B} = \frac{\mathbf{S}_A^T}{||\mathbf{S}_A||^2}\mathbf{Y}_B = h_1 + \frac{\mathbf{S}_A^T}{||\mathbf{S}_A||^2}\mathbf{N}_B, \tag{10}$$

$$\tilde{h}_{2,R} = \frac{\mathbf{S}_A^T}{||\mathbf{S}_A||^2}\mathbf{Y}_R = h_2 + \frac{\mathbf{S}_A^T}{||\mathbf{S}_A||^2}\mathbf{N}_R. \tag{11}$$

After that, Bob sends a known sequence $\mathbf{S}_B$ with T_2 components over the wireless channel, and Alice and the relay receive

$$\mathbf{Y}_A = h_1 \mathbf{S}_B + \mathbf{N}_A, \quad \mathbf{Y}_R = h_3 \mathbf{S}_B + \mathbf{N}_R, \tag{12}$$

from which Alice obtains an estimates $\tilde{h}_{1,A}$ of h_1 and the relay obtains an estimate $\tilde{h}_{3,R}$ of h_3 via

$$\tilde{h}_{1,A} = \frac{\mathbf{S}_B^T}{||\mathbf{S}_B||^2}\mathbf{Y}_A = h_1 + \frac{\mathbf{S}_B^T}{||\mathbf{S}_B||^2}\mathbf{N}_A, \tag{13}$$

$$\tilde{h}_{3,R} = \frac{\mathbf{S}_B^T}{||\mathbf{S}_B||^2}\mathbf{Y}_R = h_3 + \frac{\mathbf{S}_B^T}{||\mathbf{S}_B||^2}\mathbf{N}_R. \tag{14}$$

After these two training steps, Alice has $\tilde{h}_{1,A}$, Bob has $\tilde{h}_{1,B}$ and the relay has $(\tilde{h}_{2,R}, \tilde{h}_{3,R})$. The observations of Alice and Bob are correlated, and hence can be used to generate keys for these parties via public discussion as described in Section II. However, the observations at the relay are independent of the observations at Alice and Bob and hence are not yet useful for the key generation purpose. To solve this issue, the relay sends a training sequence $\mathbf{S}_R$ in the remaining $T - T_1 - T_2$ portion of each coherence interval, and Alice and Bob receive

$$\mathbf{Y}_A = h_2 \mathbf{S}_R + \mathbf{N}_A, \quad \mathbf{Y}_B = h_3 \mathbf{S}_R + \mathbf{N}_A. \tag{15}$$

Alice and Bob can then obtain estimates

$$\tilde{h}_{2,A} = \frac{\mathbf{S}_R^T}{||\mathbf{S}_R||^2}\mathbf{Y}_A = h_2 + \frac{\mathbf{S}_R^T}{||\mathbf{S}_R||^2}\mathbf{N}_A, \tag{16}$$

$$\tilde{h}_{3,B} = \frac{\mathbf{S}_R^T}{||\mathbf{S}_R||^2}\mathbf{Y}_B = h_3 + \frac{\mathbf{S}_R^T}{||\mathbf{S}_R||^2}\mathbf{N}_B. \tag{17}$$

After the relay sends the training sequence, the observations at Alice are $(\tilde{h}_{1,A}, \tilde{h}_{2,A})$, at Bob are $(\tilde{h}_{1,B}, \tilde{h}_{3,B})$, and at the relay are $(\tilde{h}_{2,R}, \tilde{h}_{3,R})$. The observations of each node at the end of training are shown in Figure 5. Now, the observations at the relay are correlated with the observations at Alice and Bob. This correlation can hence be exploited to increase the key rate at Alice and Bob.

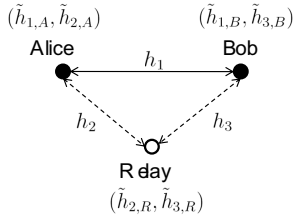


Fig. 5. The observations at the nodes after the training stage.

In the key generation step of the above algorithm, Alice and Bob first agree on a key K_1 with a rate $I(\tilde{h}_{1,A}; \tilde{h}_{1,B})/T$ using

[2]In practice, the relay first reduces the key with a larger size to equalize the sizes of the two keys, and then perform "$\oplus$" operation between the two keys.

the correlated information $(\tilde{h}_{1,A}, \tilde{h}_{1,B})$ via the approach as described in Section II. Similarly, Alice and the relay generate a key K_2 with a rate $I(\tilde{h}_{2,A}; \tilde{h}_{2,R})/T$ using the correlated information $(\tilde{h}_{2,A}, \tilde{h}_{2,R})$, and Bob and the relay generate a key K_3 with a rate $I(\tilde{h}_{3,B}; \tilde{h}_{3,R})/T$ using the correlated information $(\tilde{h}_{3,B}, \tilde{h}_{3,R})$. Finally, the relay sends $K_2 \oplus K_3$ over the public channel. The steps are shown in Figure 6. After these steps, both Alice and Bob know (K_1, K_2, K_3). If the size of K_2 is smaller than the size of K_3, Alice and Bob set (K_1, K_2) as the key, otherwise set (K_1, K_3) as the key. The resulting key rate is given by

$$R_{co} = \frac{1}{T}\Big\{\min\{I(\tilde{h}_{2,R}; \tilde{h}_{2,A}), I(\tilde{h}_{3,R}; \tilde{h}_{3,B})\} + I(\tilde{h}_{1,A}; \tilde{h}_{1,B})\Big\}. \quad (18)$$

Remark 1: We note that K_2 and K_3 cannot simultaneously serve in the final key since the eavesdroppers learn $K_2 \oplus K_3$ from the public channel.

The following theorems state that the key generated in the above algorithm is secure and the protocol is optimal.

Theorem 2: The generated key is provably secure from any eavesdropper that experiences an independent wireless channel from the legitimate nodes.

We note that Theorem 2 applies only if the relays are trusted and do not collude with the eavesdropper.

Proof: In the proof, we assume that the generated key is (K_1, K_2). The case of (K_1, K_3) is similar. We use M_i to denote the public information used to establish the key K_i. From Section II, we know that M_i does not leak any information about K_i, that is $\frac{1}{n} I(K_i; M_i) \leq \epsilon$ for any $\epsilon > 0$. In our relay-assisted key agreement protocol, the eavesdroppers observe $(M_1, M_2, M_3, K_2 \oplus K_3)$ from the public channel. Although the eavesdropper can also estimate their channel gains, these channels gains are independent of the channel gains used for the key generation and do not contain any information about the keys, and hence are omitted in the mutual information calculation below. To show that the key (K_1, K_2) is secure, we compute

$$\begin{aligned}
&\frac{1}{n} I(K_1, K_2; M_1, M_2, M_3, K_2 \oplus K_3) \\
&= \frac{1}{n}\big(I(K_1; M_1) + I(K_2; M_2, M_3, K_2 \oplus K_3)\big) \\
&= \frac{1}{n}\big(I(K_1; M_1) + I(K_2; M_2) + I(K_2; M_3, K_2 \oplus K_3)\big) \\
&\leq 2\epsilon, \quad (19)
\end{aligned}$$

where ϵ can be arbitrarily small as the length of the codes increases. The above equations follow from the independence of the random variables involved and the basic properties of mutual information. This means that the observations at the eavesdroppers provide negligible information about the generated keys, and hence the keys are information theoretically secure. ∎

Theorem 3: Among the training-based approaches for key generation, the above algorithm generates a key with the largest possible key rate, and is hence optimal.

Proof: The problem of key generation with a helper that possesses correlated observations has been considered in [17] for the discrete memoryless model. Based on correlated observations obtained from our training strategy, the optimal key rate with unlimited public discussion is given by

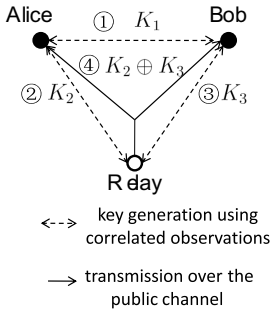


Fig. 6. The key agreement protocol.

$$R_{co,op} = \frac{1}{T}\Big\{I(\tilde{h}_{1,A}, \tilde{h}_{2,A}; \tilde{h}_{1,B}, \tilde{h}_{3,B} | \tilde{h}_{2,R}, \tilde{h}_{3,R}) + \min\{I(\tilde{h}_{2,R}, \tilde{h}_{3,R}; \tilde{h}_{1,A}, \tilde{h}_{2,A}), I(\tilde{h}_{2,R}, \tilde{h}_{3,R}; \tilde{h}_{1,B}, \tilde{h}_{3,B})\}\Big\}. \quad (20)$$

Due to the unique information structure in the problem under consideration, we can simplify this expression as follows. Firstly, we have

$$\begin{aligned}
I(\tilde{h}_{2,R}, \tilde{h}_{3,R}; \tilde{h}_{1,A}, \tilde{h}_{2,A}) &= I(\tilde{h}_{2,R}; \tilde{h}_{2,A}), \\
I(\tilde{h}_{2,R}, \tilde{h}_{3,R}; \tilde{h}_{1,B}, \tilde{h}_{3,B}) &= I(\tilde{h}_{3,R}; \tilde{h}_{3,B}). \quad (21)
\end{aligned}$$

Secondly, we have

$$\begin{aligned}
&I(\tilde{h}_{1,A}, \tilde{h}_{2,A}; \tilde{h}_{1,B}, \tilde{h}_{3,B} | \tilde{h}_{2,R}, \tilde{h}_{3,R}) \\
&= I(\tilde{h}_{1,A}, \tilde{h}_{2,A}; \tilde{h}_{1,B}, \tilde{h}_{3,B}, \tilde{h}_{2,R}, \tilde{h}_{3,R}) \\
&\quad - I(\tilde{h}_{1,A}, \tilde{h}_{2,A}; \tilde{h}_{2,R}, \tilde{h}_{3,R}) \\
&= I(\tilde{h}_{1,A}, \tilde{h}_{2,A}; \tilde{h}_{1,B}, \tilde{h}_{2,R}) - I(\tilde{h}_{2,A}; \tilde{h}_{2,R}) \\
&= I(\tilde{h}_{2,A}; \tilde{h}_{1,B}, \tilde{h}_{2,R}) + I(\tilde{h}_{1,A}; \tilde{h}_{1,B}, \tilde{h}_{2,R} | \tilde{h}_{2,A}) \\
&\quad - I(\tilde{h}_{2,A}; \tilde{h}_{2,R}) \\
&= I(\tilde{h}_{2,A}; \tilde{h}_{2,R}) + I(\tilde{h}_{1,A}; \tilde{h}_{1,B}) - I(\tilde{h}_{2,A}; \tilde{h}_{2,R}) \\
&= I(\tilde{h}_{1,A}; \tilde{h}_{1,B}). \quad (22)
\end{aligned}$$

Hence, in our problem setup, (20) can be simplified to

$$R_{co,op} = \frac{1}{T}\Big\{\min\{I(\tilde{h}_{2,R}; \tilde{h}_{2,A}), I(\tilde{h}_{3,R}; \tilde{h}_{3,B})\} + I(\tilde{h}_{1,A}; \tilde{h}_{1,B})\Big\}, \quad (23)$$

which is the same as the key rate (18) generated using our simple protocol. Hence, our key generation algorithm results the key rate that achieves this capacity, and is optimal. ∎

In order to analyze the impact of a relay on the gain of the key rate, we introduce the following definition of the *multiplexing gain* as a performance measure.

Definition 4: The multiplexing gain of the key rate is the limit of the ratio of the key rate with relay cooperation to the key rate without the relay cooperation as the SNR approaches the infinity. Hence, it is equal to $\lim_{P \to \infty} R_{co}/R_s$, where R_{co} and R_s denote the key rates with and without relay cooperation, respectively.

The following proposition provides the multiplexing gain for our proposed relay-assisted scheme.

Proposition 5: The multiplexing gain of the proposed scheme is 2.

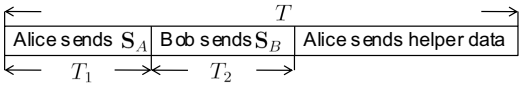


Fig. 7. One coherence time block for the case without a public channel.

Proof: We first compute (23) by applying $h_2 \sim \mathcal{N}(0, \sigma_2^2)$ and $h_3 \sim \mathcal{N}(0, \sigma_3^2)$,

$$R_{co} = \frac{1}{2T}\left[\min\left\{\log\left(\frac{(\sigma^2+\sigma_2^2PT_1)(\sigma^2+\sigma_2^2(T-T_1-T_2)P)}{\sigma^4+\sigma^2\sigma_2^2P(T-T_2)}\right)\right.\right. \left.\left. \log\left(\frac{(\sigma^2+\sigma_3^2PT_2)(\sigma^2+\sigma_3^2(T-T_1-T_2)P)}{\sigma^4+\sigma^2\sigma_3^2P(T-T_1)}\right)\right\} + \log\left(\frac{(\sigma^2+\sigma_1^2PT_1)(\sigma^2+\sigma_1^2T_2P)}{\sigma^4+\sigma^2\sigma_1^2P(T_1+T_2)}\right)\right]. \quad (24)$$

It is then easy to verify that each term in (24) scales with $\log P$, and hence

$$\lim_{P\to\infty} R_{co}/R_s = 2. \quad (25)$$

■

It is interesting to note that in the normal relay channel in which the relay helps to transmit information, the multiplexing gain is equal to one [18]. However, the multiplexing gain for secret key generation is two, which indicates that it is crucially important to exploit the presence of a relay in key generation (as opposed to information transmission), which provides a significant gain that doubles the rate of the key that can be generated from the wireless channel.

It is also interesting to note that for a given amount of power P, we achieve a performance gain

$$\lim_{T\to\infty} R_{co}/R_s = 2. \quad (26)$$

This suggests that our relay-assisted key generation scheme doubles the key rate even when the channel changes very slowly and does not provides much dynamics in randomness.

IV. Relay-Assisted Key Generation Without Public Discussion

In this section, we study a more realistic scenario in which there is no additional public channel available. All other assumptions about the model are the same as in Section III. As discussed in Section II, the public channel affects only the key agreement step, during which Alice sends $H(\tilde{Y}_A|\tilde{Y}_B)$ bits of information (more precisely, the bin number of its observations) to Bob by the Slepian-Wolf coding. Due to the absence of the public channel, we first modify the point-to-point key agreement process, and then present our relay-assisted key generation algorithm based on this modified key agreement process.

A. Modified Point-to-Point Key Agreement Process

We now describe the key generation algorithm without a public channel for the point-to-point case. In this case, the entire coherence time slot of the wireless channel is used not only for the channel estimation but also for transmitting the helper data, i.e., the bin number. An illustration of a coherence time block is depicted in Figure 7, in which Alice spends T_1 symbols to send the training sequence $\mathbf{S}_A$, Bob spends T_2 symbols to send training sequence $\mathbf{S}_B$, and Alice uses the remaining $T - T_1 - T_2$ symbols to send the bin number to Bob. Moreover, the helper data, which were transmitted over a noiseless public channel, now needs to be transmitted over the noisy (unreliable) wireless channel. Hence, a new scheme needs to be devised for transmitting the helper data reliably. More specifically, since the real-valued information on the bin number can be sent only over the unreliable wireless channel with a limited capacity, it cannot be sent perfectly any more. In this case, we adapt the transmission strategy proposed in [17]. We let Alice first compress the channel estimate and then transmit the bin number of this compressed version of the channel estimate to Bob to establish the key. More precisely, we use U to denote a compressed version of $\tilde{h}_{1,A}$. We first generate $2^{mI(U;\tilde{h}_{1,A})}$ typical U sequences. We then divide these typical sequences into bins, each bin containing $2^{mI(U;\tilde{h}_{1,B})}$ sequences. Hence, each U^m sequence can be specified by two indices: the bin number (ranging from 1 to $2^{m(I(U;\tilde{h}_{1,A})-I(U;\tilde{h}_{1,B}))}$), and the index of the sequence within each bin. Now, after observing $\tilde{\mathbf{h}}_{1,A} = [\tilde{h}_{1,A}(1), \cdots, \tilde{h}_{1,A}(m)]^T$, Alice finds a U^m sequence that is jointly-typical with $\tilde{\mathbf{h}}_{1,A}$. (This step can be shown to be successful with high probability.) Alice sets the key value as the index of the sequence in the bin and sends the bin number to Bob, which requires a rate of $I(U;\tilde{h}_{1,A}) - I(U;\tilde{h}_{1,B})$. This rate should be lower than the capacity of the wireless channel from Alice to Bob, and hence information on the bin number can be successfully received by Bob. With the bin number, Bob obtains an estimate $\tilde{U}^m$ by looking for a unique sequence in the bin specified by the bin number that is jointly typical with its observation $\tilde{\mathbf{h}}_{1,B}$. The sequence $\tilde{U}^m$ is equal to U^m with probability 1, thus Bob can then recover the key value.

Typically, we set the compressed $U = \tilde{h}_{1,A} + Z$, in which Z is a zero mean Gaussian random variable with variance σ_z^2 and is independent of other random variables considered in this problem. The variance represents how accurate the compressed version is from the original channel estimate, and is chosen to satisfy the condition that the wireless channel is able to support the rate of the bin number necessary for the key generation from the correlated noisy observations.

B. Relay-Assisted Key Generation without a Public Channel

Our algorithm for relay-assisted key generation without a public channel is based on the scheme we develop in the preceding section. A coherence time frame is split into seven time slots as illustrated in Figure 8. In the first three time slots (with each spanning over $T/8$), Alice, Bob and the relay takes turns to transmit a training sequence and the other two nodes obtain the estimates of the corresponding channel. In the following three time slots (with each spanning over $T/8$), based on the modified key agreement process as described in Section IV-A, Alice sends helper data to Bob, and the relay sends helper data to Alice and Bob, respectively, so that Alice and Bob agree on a key K_1, Alice and the relay agree on a key K_2, and Bob and the relay agree on a key K_3. In the remaining $T/4$, the relay sends $K_2 \oplus K_3$ to Bob via the wireless channel. Finally, both Alice and Bob set (K_1, K_2) as the generated key. The proof of the security of the generated key is similar to the proof of Theorem 2, and is hence omitted here.

We now analyze how the relay-assisted key rate grows as the available power grows, and analyze the multiplexing gain obtained by having an additional relay node.

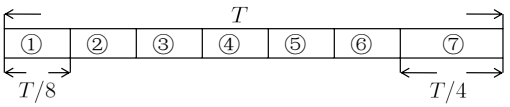


Fig. 8. Time frame for the relay-assisted key generation without a public channel. Phases 1) to 6) occupy $T/8$ each, phase 7) occupies $T/4$.

Theorem 6: The multiplexing gain of the proposed relay-assisted key generation algorithm due to a relay for the case without a public channel is 2.

Proof: Please refer to Appendix A. ∎

Remark 7: By comparing Proposition 5 and Theorem 6, we conclude that even without the public channel, we do not lose the multiplexing gain.

V. Relay-Assisted Key Generation with Multiple Relays

In this section, we study general networks with multiple relays. Our studies in Sections III and IV suggest that exploiting multiple relays may substantially improve the key rate. We note that it is possible to modify the scheme to make it robust to the compromise of some relays, which is the case studied in Section VI.

More specifically, we study a network with N relays available for helping to generate a common key between Alice and Bob. Similarly to Section III, relays are assumed to follow the designed transmission protocols, and not to leak information to Eve (i.e., not to collude with Eve). The generated key is required to be secure only from Eve, not necessarily from relays. For the easiness of the presentation, we assume that a public channel is available for the key agreement process as in Section III. The results can be extended to the case without a public channel similarly as in Section IV.

As in Sections III and IV, the key generation protocol includes channel estimation and key agreement steps. In the channel estimation step, Alice, Bob and the relays take turns to broadcast their training sequences, and all other nodes estimate their corresponding channel gains. In the key agreement step, each pair of nodes agree on one key based on their channel estimation using the Slepian-Wolf coding as illustrated in Figure 9. More specifically, Alice sends helper data to Bob, via which Alice and Bob agree on a key K_1. Then, each relay sends helper data to Alice and Bob, respectively, via which the relay agrees on a key $K_{A,i}$ with Alice and agrees on a key $K_{B,i}$ with Bob for $i = 1, \ldots, N$. Finally, each relay sends $K_{A,i} \oplus K_{B,i}$ to both Alice and Bob to allow them to recover all the keys. In the end, Alice and Bob concatenate $(K_1, (K_{A,1} \wedge K_{B,1}), \ldots, (K_{A,N} \wedge K_{B,N}))$ as the key, where $(K_i \wedge K_j)$ denotes either K_i or K_j that has a smaller key rate.

Using this approach, the achieved key rate is given by

$$\begin{aligned} R_{co,N} = \frac{1}{T}\Big\{ & I(\tilde{h}_{1,A}; \tilde{h}_{1,B}) \\ & + \min\{I(\tilde{h}_{A1,A}; \tilde{h}_{A1,R}), I(\tilde{h}_{B1,B}; \tilde{h}_{B1,R})\} \\ & + \cdots \\ & + \min\{I(\tilde{h}_{AN,A}; \tilde{h}_{AN,R}), I(\tilde{h}_{BN,B}; \tilde{h}_{BN,R})\} \Big\}. \end{aligned} \quad (27)$$

Theorem 8: The multiplexing gain of having N relays is $N + 1$, i.e.,

$$\lim_{P \to \infty} R_{co,N}/R_s = N + 1, \quad (28)$$

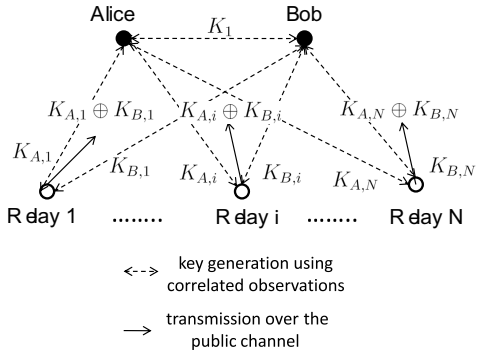


Fig. 9. The key agreement protocol for N relays case.

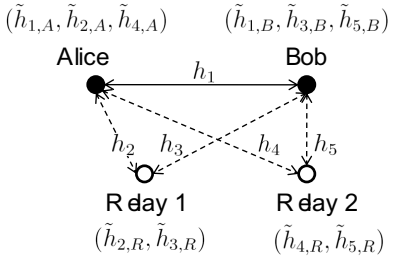


Fig. 10. Observations at the nodes after the training.

and this multiplexing gain is order-optimal.

Proof: See Appendix B. ∎

Remark 9: The above theorem implies that the multiplexing gain of key generation scales linearly with the number of relay nodes.

VI. Relay-oblivious Key Generation

In this section, we study an interesting scenario in which not only eavesdroppers but also relays are prevented from gaining any information about generated keys. That is we wish to generate a relay-oblivious key while still benefiting from the relays. In this case, relays are still assumed to follow the designed transmission protocols, i.e., not to leak information to Eve (i.e., not to cooperative with Eve), and not to collude with each other, but are assumed to be curious and try to infer as much information about the generated key as possible.

We first study the case with two relays (see Figure 10) as an example to illustrate the idea. The relay-oblivious key generation process has two main steps. In the first step, Alice, Bob, and the two relays follow the same protocol as developed in Section V to generate keys, as if there is no security constraint on the relays. In the second step, Alice and Bob distill a key that is oblivious from the relays based on the keys already generated. The key generation protocol is described in more detail below.

Relay-oblivious Key Generation with Two Relays

Step 1: Follow the same protocol as that in Section V:

- Alice and Bob agree on a key K_1 from the correlated observations $(\tilde{h}_{1,A}, \tilde{h}_{1,B})$
- Alice and relay 1 agree on a key K_2 from the correlated observations $(\tilde{h}_{2,A}, \tilde{h}_{2,R})$
- Bob and relay 1 agree on a key K_3 from the correlated observations $(\tilde{h}_{3,B}, \tilde{h}_{3,R})$

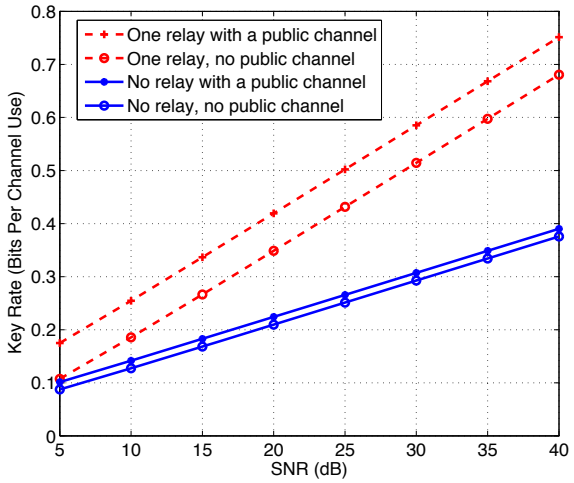


Fig. 11. Comparison of key rates for four network scenarios.

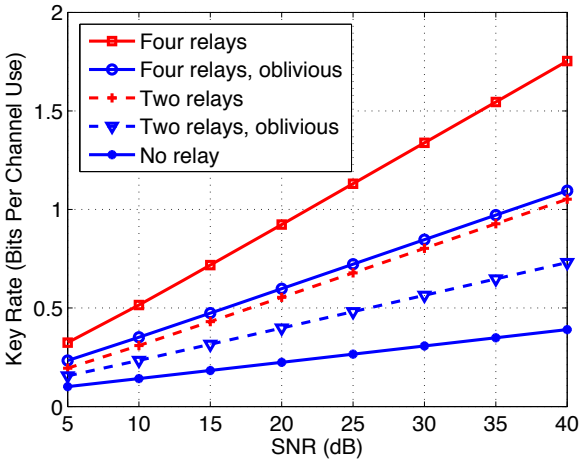


Fig. 12. Comparison of key rates with and without secrecy constraint at relays.

- Alice and relay 2 agree on a key K_4 from the correlated observations $(\tilde{h}_{4,A}, \tilde{h}_{4,R})$
- Bob and relay 2 agree on a key K_5 from the correlated observations $(\tilde{h}_{5,B}, \tilde{h}_{5,R})$
- Relay 1 broadcast $K_2 \oplus K_3$ using the public channel.
- Relay 2 broadcast $K_4 \oplus K_5$ using the public channel.

Step 2: Key Distillation:

- Without loss of generality, assuming the length of K_2 is less than the length of K_3, and the length of K_4 is less than the length of K_5, Alice and Bob concatenate $(K_1, K_2 \oplus K_4)$ as the key.

We note that if we do not need to keep the key secret from each relay, we can use (K_1, K_2, K_4) as the key.

Lemma 1: Each relay gains negligible information about the generated key $(K_1, K_2 \oplus K_4)$.

Proof: It is sufficient to show that relay 1 has negligible information about the key. The same arguments are applicable for relay 2. From the protocol, one can see that relay 1 knows (K_2, K_3) and $M_i, i = 1, \cdots, 5$ from the public channel. Here, again, M_i is the helper data used in generating key K_i.

$$\begin{aligned} & I(K_2, K_3, M_1, \cdots, M_5; K_1, K_2 \oplus K_4) \\ &= I(K_2, K_3, M_1, \cdots, M_5; K_1) \\ &\quad + I(K_2, K_3, M_1, \cdots, M_5; K_2 \oplus K_4 | K_1) \\ &= I(M_1; K_1) + I(M_2, M_4; K_2 \oplus K_4) \\ &\leq I(M_1; K_1) + I(M_2; K_2) + I(M_4; K_4) \\ &\leq 3\epsilon \end{aligned} \tag{29}$$

where ϵ can be arbitrarily small as the codeword length increases. ■

The extension to the general case with N relays is simple. Assuming that N is an even number, we then divide these N relays into $N/2$ pairs. Now, each pair of relays can run the same protocol as discussed above, and contribute a key that is oblivious from the relays. A final key is obtained by concatenating these keys together. Based on this approach, the following corollary on the multiplexing gain in this case can be obtained.

Corollary 10: The multiplexing gain of the rate of the key that is secure from relays is $\lfloor N/2 \rfloor + 1$.

VII. Numerical Results

In this section, we demonstrate the impact of relays on the key rate via a few numerical examples. In Figure 11, we compare the key rates as a function of the SNR corresponding to four scenarios with one relay in the system. We set the coherence blocklength to be $T = 20$, and set the variances of the channel estimation errors respectively to be $\sigma^2 = \sigma_1^2 = \sigma_2^2 = 1$. It can be seen from the figure that the gain in the secret key rate due to the relay increases as the SNR increases for both cases with and without a public channel. It can also be seen that the key rate generated without a public channel is smaller than that generated with a public channel. However, the gap between the two is a bounded by a constant. Furthermore, the key rate generated without a public channel also grows logarithmically with P.

In Figure 12, we plot the key rate for the case with and without secrecy constraint on the relays for a different number of relay nodes. From the figure, we can see that when we impose secrecy constraint on the relays, the key rate is roughly half of that of the case without secrecy constraint on the relays. However, even with a strict secrecy constraint, the presence of relay nodes significantly increase the key rate.

Figure 13 shows the relationship between the key rate and the number of relay nodes when SNR= 20dB. From the figure, it is clear that the key rate increases linearly with the number of relays for both the case with and without secrecy constraint on the relay nodes. This confirms our analysis that the key rate increase linearly with the number of relay nodes. Hence the presence of relay nodes can significantly increase the size of the generated keys.

VIII. Conclusions

In this paper, we have proposed a PHY-based relay-assisted key generation approach, which exploits the presence of multiple relays in wireless networks for improving the generated secret key rate. We have designed a simple relay-assisted scheme that is optimal for single relay case, and is asymptotically optimal for more general networks with multiple relays. We have shown that if the multiplexing gain of the generated key rate grows linearly with the number of relay nodes. This is in sharp contrast to scenarios in which relays help for data

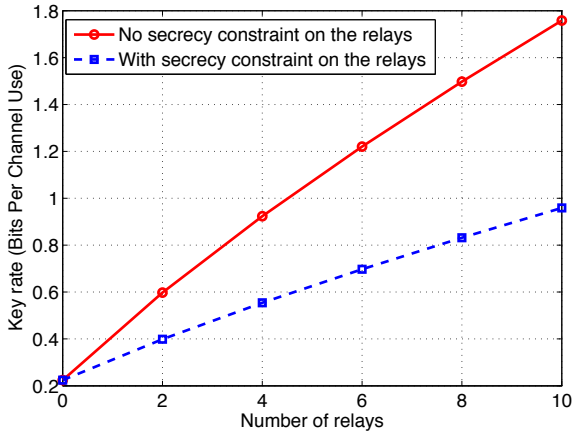


Fig. 13. Key rates vs the number of relays.

transmission, and in which the multiplexing gain is limited to be 1. We have also propose a scheme that exploits relays to generate keys but keeps the keys secure from the relays. For this case, the multiplexing gain of the relay-oblivious key is $\lfloor N/2 \rfloor + 1$.

Appendix A
Proof of Theorem 6

We first analyze how the point-to-point key rate $R_{s,np}$ without a public channel scales with the power P. Following [17], if the wireless channel for transmitting the bin number has a rate constraint R, then the following secret key rate can be generated from the correlated observations $(\tilde{h}_{1,A}, \tilde{h}_{1,B})$:

$$\begin{aligned} R_s = & I(U;\tilde{h}_{1,B}) \\ & \text{s.t.} \quad U \to \tilde{h}_{1,A} \to \tilde{h}_{1,B}, \\ & \text{and} \quad I(U;\tilde{h}_{1,A}) - I(U;\tilde{h}_{1,B}) \le R, \end{aligned} \tag{30}$$

where U is an auxiliary random variable subject to the Markov chain relationship given in (30).

As discussed in Section IV-A, we let $U = \tilde{h}_{1,A} + Z$, where Z is a zero mean Gaussian random variable with variance σ_z^2 and is independent of other random variables considered in this problem. It is clear that $U \to \tilde{h}_{1,A} \to \tilde{h}_{1,B}$. In this case, the key rate can be computed to be

$$\begin{aligned} R_{s,np} &= \frac{1}{T} I(U;\tilde{h}_{1,B}) \\ &= \frac{1}{2T} \log \left(\frac{(\sigma_1^2 + \frac{\sigma^2}{PT_1} + \sigma_z^2)(\sigma_1^2 + \frac{\sigma^2}{PT_2})}{(\sigma_1^2 + \frac{\sigma^2}{PT_1} + \sigma_z^2)(\sigma_1^2 + \frac{\sigma^2}{PT_2}) - \sigma_1^4} \right). \end{aligned} \tag{31}$$

where the normalization term $1/T$ is due to the fact that the channel gain remains fixed for T symbol times.

To achieve the above key rate, one needs to transmit helper data at the rate

$$\begin{aligned} & \frac{1}{T}(I(U;\tilde{h}_{1,A}) - I(U;\tilde{h}_{1,B})) \\ & = \frac{1}{2T} \log \left(1 + \frac{\sigma_1^2 \sigma^2}{\sigma_z^2(\sigma^2 + \sigma_1^2 PT_1)} + \frac{\sigma^2}{\sigma_z^2 PT_2} \right) \end{aligned} \tag{32}$$

over the wireless channel. However, in the remaining $T - T_1 - T_2$ symbol times reserved for transmission of the helper data, one can transmit at the rate

$$\frac{T - T_1 - T_2}{2T} \mathbb{E} \left\{ \log \left(1 + \frac{h_1^2 P}{\sigma^2} \right) \right\}, \tag{33}$$

in which $\mathbb{E}\{\cdot\}$ denotes the average over the corresponding random variables. Hence, the value of σ_z^2 should be chosen such that

$$(32) \le (33). \tag{34}$$

We set $T_1 = T_2 = T/4$. Although such a choice of the parameters may not be optimal, it does not affect the order of the key rate as the SNR increases. In the high SNR regime, we have

$$\mathbb{E} \left\{ \log \left(1 + \frac{h_1^2 P}{\sigma^2} \right) \right\} \doteq \log P,$$

where $\doteq$ denotes the equality in the order sense. Now, if we choose $\sigma_z^2 = P^{-2}$, the condition given in (34) is satisfied. Now, we plug these choices of parameters into (31) and obtain

$$\begin{aligned} R_{s,np} &= \frac{1}{2T} \log \left(\frac{(\sigma_1^2 + \frac{4\sigma^2}{PT} + P^{-2})(\sigma_1^2 + \frac{4\sigma^2}{PT})}{(\sigma_1^2 + \frac{4\sigma^2}{PT} + P^{-2})(\sigma_1^2 + \frac{4\sigma^2}{PT}) - \sigma_1^4} \right) \\ &\sim \frac{1}{2T} \log P. \end{aligned} \tag{35}$$

Hence, $R_{s,np} \sim \frac{1}{2T} \log P$ in the high SNR regime, which is the same as that in the case with a public channel.

We now derive the key rate $R_{co,np}$ for the case with a relay and without a public channel, and analyze its asymptotic behavior based on the result discussed above. Firstly, using (35), it is easy to see that the rate of the key K_1 is

$$R_{s,1} = \frac{1}{2T} \log \left(\frac{(\sigma_1^2 + \frac{8\sigma^2}{PT} + \sigma_{z,1}^2)(\sigma_1^2 + \frac{8\sigma^2}{PT})}{(\sigma_1^2 + \frac{8\sigma^2}{PT} + \sigma_{z,1}^2)(\sigma_1^2 + \frac{8\sigma^2}{PT}) - \sigma_1^4} \right), \tag{36}$$

with $\sigma_{z,1}^2$ chosen to satisfy

$$\begin{aligned} & \frac{1}{2T} \log \left(1 + \frac{\sigma_1^2 \sigma^2}{\sigma_{z,1}^2(\sigma^2 + \sigma_1^2 PT/8)} + \frac{\sigma^2}{\sigma_{z,1}^2 PT/8} \right) \\ & \le \frac{1}{16} \mathbb{E} \left\{ \log \left(1 + \frac{h_1^2 P}{\sigma^2} \right) \right\}. \end{aligned} \tag{37}$$

In (37), the left-hand-side is the rate of the helper data needed for key generation, while the right-hand-side is the rate that can be transmitted via the wireless channel in the modified key agreement process. The rates of K_2 and K_3 can be derived similarly and are given by

$$R_{s,2} = \frac{1}{2T} \log \left(\frac{(\sigma_2^2 + \frac{8\sigma^2}{PT} + \sigma_{z,2}^2)(\sigma_2^2 + \frac{8\sigma^2}{PT})}{(\sigma_2^2 + \frac{8\sigma^2}{PT} + \sigma_{z,2}^2)(\sigma_2^2 + \frac{8\sigma^2}{PT}) - \sigma_2^4} \right), \tag{38}$$

$$R_{s,3} = \frac{1}{2T} \log \left(\frac{(\sigma_3^2 + \frac{8\sigma^2}{PT} + \sigma_{z,3}^2)(\sigma_3^2 + \frac{8\sigma^2}{PT})}{(\sigma_3^2 + \frac{8\sigma^2}{PT} + \sigma_{z,3}^2)(\sigma_3^2 + \frac{8\sigma^2}{PT}) - \sigma_3^4} \right), \tag{39}$$

with $\sigma_{z,2}^2$ and $\sigma_{z,3}^2$ chosen to satisfy

$$\begin{aligned} & \frac{1}{2T} \log \left(1 + \frac{\sigma_2^2 \sigma^2}{\sigma_{z,2}^2(\sigma^2 + \sigma_2^2 PT/8)} + \frac{\sigma^2}{\sigma_{z,2}^2 PT/8} \right) \\ & \le \frac{1}{16} \mathbb{E} \left\{ \log \left(1 + \frac{h_2^2 P}{\sigma^2} \right) \right\}, \end{aligned} \tag{40}$$

$$\text{and} \quad \frac{1}{2T}\log\left(1+\frac{\sigma_3^2\sigma^2}{\sigma_{z,3}^2(\sigma^2+\sigma_3^2PT/8)}+\frac{\sigma^2}{\sigma_{z,3}^2PT/8}\right) \le \frac{1}{16}\mathbb{E}\left\{\log\left(1+\frac{h_3^2P}{\sigma^2}\right)\right\}, \tag{41}$$

respectively.

We finally require that phase 7) is successful, i.e., the relay can broadcast an XOR of the keys to Alice and Bob. Hence, in addition to (40) and (41), $\sigma_{z,2}^2$ and $\sigma_{z,3}^2$ should also satisfy

$$\max\{R_{s,2},R_{s,3}\} \le \frac{1}{8}\mathbb{E}\left\{\log\left(1+\frac{h_3^2P}{\sigma^2}\right)\right\}. \tag{42}$$

Here, $\max\{R_{s,2},R_{s,3}\}$ is the rate of $K_2 \oplus K_3$ and $\frac{1}{8}\mathbb{E}\left\{\log\left(1+\frac{h_3^2P}{\sigma^2}\right)\right\}$ is the rate that the wireless channel can support in the remaining $T/4$ part of a coherence block.

In summary, the key agreement rate without a public channel is given by

$$R_{co,np} = R_{s,1} + \min\{R_{s,2},R_{s,3}\}, \tag{43}$$

where $R_{s,1}$, $R_{s,2}$ and $R_{s,3}$ are given in (36), (38) and (39) respectively.

We set $\sigma_{z,1}^2=\sigma_{z,2}^2=\sigma_{z,3}^2=P^{-2}$. It is easy to verify that all requirements (37), (40), (41) and (42) are satisfied. With these choices of the parameters, by comparing (8) and (43) we obtain $\lim_{P\to\infty} R_{op,np}/R_s = 2$, which concludes the proof.

APPENDIX B
PROOF OF THEOREM 8

Following the same steps in the proof of Proposition 5, it is easy to verify that $\lim_{P\to\infty} R_{co,N}/R_s = N+1$.

In the following, we show that the pair-wise approach is order-optimal. To this end, we first derive an upper-bound on the generated key rate using N relays. We then show that the multiplexing gain of this upper-bound is $N+1$, which then implies that our scheme is order optimal. We start with the proof for $N=2$, and then generalize it for more general cases. We first construct a genie-aided upper-bound by assuming that relay 1 and relay 2 can combine their observations. It is clear that this does not decrease the key rate. In this case, the problem is converted to the case with one relay observing $(\tilde{h}_{2,R},\tilde{h}_{3,R},\tilde{h}_{4,R},\tilde{h}_{5,R})$. The key capacity for this scenario is

$$R_{co,ge} = \frac{1}{T}\Big\{\min\{I(\tilde{h}_{2,R},\tilde{h}_{3,R},\tilde{h}_{4,R},\tilde{h}_{5,R};\tilde{h}_{1,A},\tilde{h}_{2,A},\tilde{h}_{4,A}), I(\tilde{h}_{2,R},\tilde{h}_{3,R},\tilde{h}_{4,R},\tilde{h}_{5,R};\tilde{h}_{1,B},\tilde{h}_{3,B},\tilde{h}_{5,B})\} + I(\tilde{h}_{1,A},\tilde{h}_{2,A},\tilde{h}_{4,A};\tilde{h}_{1,B},\tilde{h}_{3,B},\tilde{h}_{5,B}|\tilde{h}_{2,R},\tilde{h}_{3,R},\tilde{h}_{4,R},\tilde{h}_{5,R})\Big\}$$

Next, we can show that

$$I(\tilde{h}_{1,A},\tilde{h}_{2,A},\tilde{h}_{4,A};\tilde{h}_{1,B},\tilde{h}_{3,B},\tilde{h}_{5,B}|\tilde{h}_{2,R},\tilde{h}_{3,R},\tilde{h}_{4,R},\tilde{h}_{5,R}) = I(\tilde{h}_{1,A};\tilde{h}_{1,B}),$$

$$I(\tilde{h}_{2,R},\tilde{h}_{3,R},\tilde{h}_{4,R},\tilde{h}_{5,R};\tilde{h}_{1,A},\tilde{h}_{2,A},\tilde{h}_{4,A}) = I(\tilde{h}_{2,R},\tilde{h}_{4,R};\tilde{h}_{2,A},\tilde{h}_{4,A}) = I(\tilde{h}_{2,R};\tilde{h}_{2,A}) + I(\tilde{h}_{4,R};\tilde{h}_{4,A}),$$

$$\text{and} \quad I(\tilde{h}_{2,R},\tilde{h}_{3,R},\tilde{h}_{4,R},\tilde{h}_{5,R};\tilde{h}_{1,B},\tilde{h}_{3,B},\tilde{h}_{5,B}) = I(\tilde{h}_{3,R},\tilde{h}_{5,R};\tilde{h}_{3,B},\tilde{h}_{5,B}) = I(\tilde{h}_{3,R};\tilde{h}_{3,B}) + I(\tilde{h}_{5,R};\tilde{h}_{5,B}).$$

Hence,

$$R_{co,ge} = \frac{1}{T}\Big\{I(\tilde{h}_{1,A};\tilde{h}_{1,B}) + \min\{I(\tilde{h}_{2,R};\tilde{h}_{2,A}) + I(\tilde{h}_{4,R};\tilde{h}_{4,A}), I(\tilde{h}_{3,R};\tilde{h}_{3,B}) + I(\tilde{h}_{5,R};\tilde{h}_{5,B})\}\Big\},$$

from which we can derive $\lim_{P\to\infty} R_{co,ge}/R_s = 3$. This implies that our proposed pair-wise approach for the two-relay case achieves the same multiplexing gain as that of the genie-aided bound, and hence it is order-optimal.

Following the steps similar to the above, we can show that for the general case with N relays, we have

$$\lim_{P\to\infty} R_{co,ge}/R_s = N+1, \tag{44}$$

which implies that the proposed pair-wise approach achieves the same multiplexing gain as that of the genie-aided bound for the case with N relays, and hence is order-optimal.

REFERENCES

[1] L. Lai, Y. Liang, and K. Du, "PHY-Based cooperative key generation in wireless networks,," in *Proc. Allerton Conf. on Communication, Control, and Computing*, (Monticello, IL), Sept. 2011.

[2] L. Lai and H. V. Poor, "A unified framework for key agreement over wireless fading channels," in *Proc. IEEE Inform. Theory Workshop*, (Taormina, Sicily, Italy), Oct. 2009.

[3] L. Lai, Y. Liang, and H. V. Poor, "Key agreement over wireless fading channels with an active attacker," in *Proc. Allerton Conf. on Communication, Control, and Computing*, (Monticello, IL), Sept. 2010.

[4] R. Wilson, D. Tse, and R. A. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *IEEE Trans. Inf. Forens. Security*, vol. 2, pp. 364–375, Sept. 2007.

[5] T.-H. Chou, A. M. Sayeed, and S. C. Draper, "Minimum energy per bit for secret key acquisition over multipath wireless channels," in *Proc. IEEE Intl. Symposium on Inform. Theory*, (Seoul, Korea), Jun. 2009.

[6] T.-H. Chou, A. M. Sayeed, and S. C. Draper, "Impact of channel sparsity and correlated eavesdropping on secret key generation from multipath channel randomness," in *Proc. IEEE Intl. Symposium on Inform. Theory*, (Austin, TX), Jun. 2010.

[7] A. Sayeed and A. Perrig, "Secure wireless communications: Secret keys through multipath," in *Proc. IEEE Intl. Conf. on Acoustics, Speech, and Signal Processing*, (Las Vegas, NV), Apr. 2008.

[8] C. Ye, S. Mathur, A. Reznik, W. Trappe, and N. Mandayam, "Information-theoretic key generation from wireless channels," *IEEE Trans. Inf. Forens. Security*, vol. 5, pp. 240–254, Jun. 2010.

[9] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radiotelephathy: Extracting a secret key from an unauthenticated wireless channel," in *Proc. ACM International Conference on Mobile Computing and Networking*, (San Francisco, CA), 2008.

[10] K. Zeng, D. Wu, A. Chan, and P. Mohapatra, "Exploiting multiplean-tenna diversity for shared key generation in wireless networks," in *Proc. IEEE Conf. Computer Communications (Infocom)*, (San Diego, CA), Mar. 2010.

[11] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge, UK: Cambridge University Press, May 2005.

[12] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography, Part I: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, pp. 1121–1132, July 1993.

[13] G. Kramer, M. Gastpar, and P. Gupta, "Cooperative strategies and capacity theorems for relay networks," *IEEE Trans. Inf. Theory*, vol. 51, pp. 3037–3063, Sep. 2005.

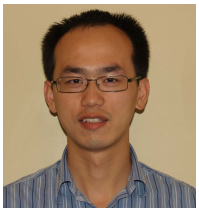
[14] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Inf. Theory*, vol. 50, pp. 3062–3080, Dec. 2004.

[15] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York: Wiley, 1991.

[16] L. Lai, Y. Liang, and H. V. Poor, "A unified framework for key agreement over wireless fading channels," *IEEE Trans. Inf. Forens. Security*, vol. 7, pp. 480–490, Apr. 2012.

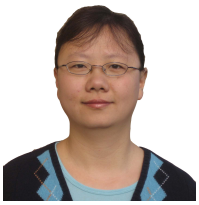
[17] I. Csiszár and P. Narayan, "Common randomness and secret key generation with a helper," *IEEE Trans. Inf. Theory*, vol. 46, pp. 344–366, Mar. 2000.

[18] K. Azarian, H. El Gamal, and P. Schniter, "On the achievable diversity-multiplexing tradeoff in half-duplex cooperative channels," *IEEE Trans. Inf. Theory*, vol. 51, pp. 4152–4172, Dec. 2005.



Lifeng Lai (M'07) received the B.E. and M. E. degrees from Zhejiang University, Hangzhou, China in 2001 and 2004 respectively, and the PhD degree from The Ohio State University at Columbus, OH, in 2007. He was a postdoctoral research associate at Princeton University from 2007 to 2009. He is now an assistant professor at University of Arkansas, Little Rock. Dr. Lai's research interests include wireless communications, information security, and information theory.

Dr. Lai was a Distinguished University Fellow of the Ohio State University from 2004 to 2007. He is a co-recipient of the Best Paper Award from IEEE Global Communications Conference (Globecom), 2008, the Best Paper Award from IEEE Conference on Communications (ICC), 2011. He received the National Science Foundation CAREER Award in 2011, and Northrop Young Researcher Award in 2012.



Yingbin Liang (S'01-M'05) received the Ph.D. degree in Electrical Engineering from the University of Illinois at Urbana-Champaign in 2005. In 2005-2007, she was working as a postdoctoral research associate at Princeton University. In 2008-2009, she was an assistant professor at the Department of Electrical Engineering at the University of Hawaii. Since December 2009, she has been an assistant professor at the Department of Electrical Engineering and Computer Science at the Syracuse University. Dr. Liang's research interests include communications, wireless networks, information theory, and machine learning.

Dr. Liang was a Vodafone Fellow at the University of Illinois at Urbana-Champaign during 2003-2005, and received the Vodafone-U.S. Foundation Fellows Initiative Research Merit Award in 2005. She also received the M. E. Van Valkenburg Graduate Research Award from the ECE department, University of Illinois at Urbana-Champaign, in 2005. In 2009, she received the National Science Foundation CAREER Award, and the State of Hawaii Governor Innovation Award.

Wenliang (Kevin) Du (M'01) received the B.S. degree in Computer Science from the University of Science and Technology of China, Hefei, China, in 1993, the M.S. degree and the Ph.D degree from the Computer Science Department at Purdue University, West Lafayette, Indiana, USA, in 1999 and 2001, respectively. Dr. Du is currently a professor in the Department of Electrical Engineering and Computer Science at Syracuse University, Syracuse, New York, USA. His research background is in computer and network security. His current research interests include web security and mobile system security. He is also interested in developing instructional laboratories for security education, and the labs he developed have been used by over a hundred universities worldwide. His research has been sponsored by grants from National Science Foundation, Army Research Office, JP Morgan Chase, and Google.