

# A PHY-Based Secret Sharing Scheme in MIMO Systems

Zhuoru Jian<sup>1,2(✉)</sup>, Hai Huang<sup>1</sup>, Xiaojun Jing<sup>1,2</sup>, and Jia Li<sup>3</sup>

<sup>1</sup> School of Information and Communication Engineering,  
Beijing University of Posts and Telecommunications, Beijing, China  
jzr@bupt.edu.cn

<sup>2</sup> Key Laboratory of Trustworthy Distributed Computing and Service (BUPT),  
Ministry of Education, Beijing University of Posts and Telecommunications,  
Beijing, China

<sup>3</sup> School of Engineering and Computer Science, Oakland University,  
Rochester, USA

**Abstract.** A secure secret sharing scheme distributes a secret among a group of participants and only when a sufficient number of shares are combined together can the secret be reconstructed. In this paper, we present a secure PHY-based secret sharing (PSS) scheme exploiting radio channel fading coefficients in multiple-input multiple-output (MIMO) systems.  $(n, n)$  threshold secret sharing scheme is considered and there is no need for the third party to distribute keys in PSS scheme. A two-step randomness sharing is designed, which reduces the time overhead significantly compared to one-by-one randomness sharing when the number of participants increases. Furthermore, we derive a power allocation scheme under power constraints based on particle swarm optimization (PSO) algorithm. Numerical results demonstrate the efficiency of our power allocation strategies on secret key rates.

**Keywords:** PHY-based secret sharing · Two-step randomness sharing  
Power allocation

## 1 Introduction

Secret sharing is proposed to distribute a secret among a group of participants, each of whom is allocated a share of the secret. Individual shares are of no use on their own and only when a specified number of shares are combined together can the secret be read out. The purpose of secret sharing is to prevent secrets from being excessively concentrated as well as to prevent a copy of an encryption key falling into the wrong hands. In one type of secret sharing schemes which is called  $(t, n)$  threshold scheme [1], a secret is divided into  $n$  shares and every  $t$  shareholders out of  $n$  can reconstruct the secret while shareholders less than  $t$  should not be able to gain any information about the secret.

Security of classic cryptographic-based key generation in secret sharing schemes usually depends on the computational hardness of some mathematical problems. And most key distribution strategies assume that there may exist a safe wireless transmitting

channel, which, however, is highly challenging in wireless systems. Besides, with the development of hardware technology, these schemes may be compromised. To enhance the security of wireless communications, PHY-based key generation has attracted much attention in recent years.

There have been extensive researches on key generation based on the wireless physical layer. Instead of exploiting the computationally secure nature of the public key cryptography and symmetric encryption schemes, wireless physical layer based key generation is information-theoretically secure. The concept of the secret key agreement exploiting wireless channel characteristics was first proposed in [2]. Key generation schemes such as received signal strength (RSS) based schemes and channel state information (CSI) based schemes have been studied in [3–6]. Secret key agreement in two-way wireless relaying systems was studied in [7, 8]. Group secret key generation was discussed in [9], where one-by-one randomness sharing was exploited, i.e., each participant took turns to broadcast training sequences to estimate channel gains. In general, the secret key generation procedures are usually divided into four stages, i.e., channel probing, quantization, information reconciliation and privacy amplification [10]. Channel reciprocity, which provides similar wireless channel characteristics for the two communication parties within coherence time, is exploited in most systems.

In this paper, we propose a PHY-based secret sharing (PSS) scheme based on fading channel characteristics in multiple-input multiple-output (MIMO) systems. The main contributions are summarized as follows.

- A two-step randomness sharing is designed. Different from letting participants take turns to broadcast training sequences, we divide the coherence time into two time slots in which all the participants transmit signals to reduce the time overhead.
- The status of each participant in the group is equal and anyone within the group can encrypt a file using the obtained key while the others need to decrypt the file jointly, thus can prevent secrets falling into the wrong hands.
- A power allocation scheme based on particle swarm optimization (PSO) algorithm is presented to improve the secret key rates under power constraints.

The rest of this paper is organized as follows. Section 2 introduces the system model. Section 3 presents the proposed PSS scheme in details and provides our power allocation algorithm. The numerical results are shown in Sect. 4 and conclusions are given in Sect. 5.

## 2 System Model

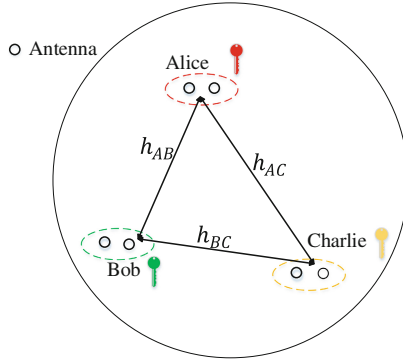
In this paper, we are mainly concerned with  $(n, n)$  threshold secret sharing schemes, when all shares are necessary to recover the secret. Without loss of generality, we consider a secret sharing scheme for a group including three participants named Alice, Bob and Charlie. The system model is depicted in Fig. 1, where the three participants wish to generate a set of secret keys through fading wireless channels in the presence of a potentially dishonest one who may act as a passive eavesdropper. In this model, we assume that the fading channel is a slow fading channel, which means the fading channel remains constant within the channel coherence time, thus the reciprocity of the

channel holds. Let  $h_{i,j}$  denotes channel between antenna  $i$  and  $j$ , and it is assumed to be Gaussian random variables, i.e.,  $h_{i,j} \sim \mathcal{N}(0, \sigma_{i,j}^2)$ . We also assume the noise at each antenna is *i.i.d* complex Gaussian random variable with zero mean and variance  $\sigma^2$ . Moreover, we assume all the participants can communicate with each other and work in a half-duplex system. Each participant is equipped with two antennas and in each time slot in the proposed scheme, one antenna is used to transmit signals while the other is used to receive signals. Considering channel estimation between antenna  $i$  and  $j$ , the received signals after the training process at antenna  $i$  and  $j$  can be written as  $\mathbf{y}_{i,j} = h_{i,j}\mathbf{s}_i + \mathbf{n}_j$  and  $\mathbf{y}_{j,i} = h_{j,i}\mathbf{s}_j + \mathbf{n}_i$ , where  $\mathbf{s}_i$  and  $\mathbf{s}_j$  are probe signals transmitted from antenna  $i$  and  $j$ , respectively. Then node  $j$  and  $i$  can obtain the following estimated channel gains

$$\tilde{h}_{i,j} = \frac{\mathbf{s}_i^T}{\|\mathbf{s}_i\|^2} \mathbf{y}_{i,j} = h_{i,j} + \frac{\mathbf{s}_i^T}{TP_i} \mathbf{n}_j, \quad (1)$$

$$\tilde{h}_{j,i} = \frac{\mathbf{s}_j^T}{\|\mathbf{s}_j\|^2} \mathbf{y}_{j,i} = h_{j,i} + \frac{\mathbf{s}_j^T}{TP_j} \mathbf{n}_i, \quad (2)$$

where  $\|\mathbf{s}_i\|^2 = TP_i$  and  $\|\mathbf{s}_j\|^2 = TP_j$ .  $P_i, P_j$  are transmission power of antenna  $i$  and  $j$ , respectively.  $T$  is the duration of the signal transmitted by each antenna.



**Fig. 1.** System model.

After the channel estimation, each antenna pair  $(i,j)$  can agree on a nearly uniformly distributed pairwise secret key with arbitrarily small error probability [8], the secret key rate between antenna  $i$  and  $j$  is  $R_{i,j} = I_{i,j}/2T$  where

$$I_{i,j} = I(\tilde{h}_{i,j}, \tilde{h}_{j,i}) = -\frac{1}{2} \log \left( 1 - \frac{\sigma_{i,j}^2 TP_i}{\sigma_{i,j}^2 TP_i + \sigma^2} \cdot \frac{\sigma_{j,i}^2 TP_j}{\sigma_{j,i}^2 TP_j + \sigma^2} \right). \quad (3)$$

### 3 PHY-Based Secret Sharing and Power Allocation

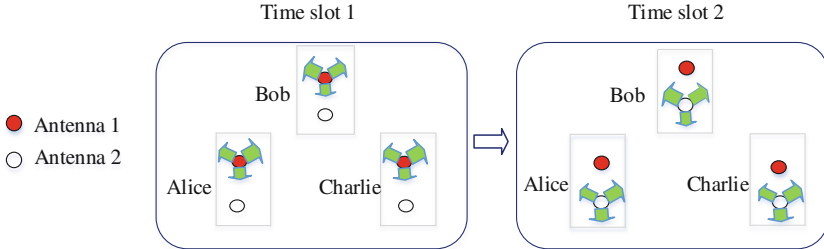
#### 3.1 PSS Scheme

In our scheme, the duration of each channel estimation requires two time slots  $T_1$  and  $T_2$ . It is reasonable to assume  $T_1 = T_2 = T/2$ , where  $T$  represents the channel coherence time. Our scheme includes two major components: two-step point-to-point randomness sharing and secret key generation. Let  $\mathcal{B}$  represents the group, i.e.,  $\mathcal{B} = \{A, B, C\}$ , the details can be described as follows.

- **Two-step point-to-point randomness sharing.** As is illustrated in Fig. 2, this phase consists of two time slots. In the first time slot  $T_1$ , each participant  $n, n \in \mathcal{B}$  transmits probe signals  $\mathbf{s}_n$  with length  $L$  using their antenna 1. At the same time, their antenna 2 are used to receive all the signals. Assuming all transmitted sequences are orthogonal to each other, the received signal at each participant can be written as

$$\mathbf{y}_{k_2} = \sum_{n \in \mathcal{B}, n \neq k} h_{k_2, n_1} \mathbf{s}_n + \mathbf{n}_{k_2}, \quad (4)$$

where  $k$  denotes the participant  $k$  and the subscript 1, 2 denote antenna 1 and 2.  $\mathbf{n}_{k_2}$  is additive white Gauss noise at antenna  $k_2$  and  $\mathbf{s}_n = [s_{n1}, s_{n2}, \dots, s_{nL}]$  is the probe signal. We assume the three parties are at least half of wavelength away, thus all the channel gains are independent of each other, which indicates that Charlie can get no information about  $h_{B_2, A_1}$ , so it is with Alice and Bob.



**Fig. 2.** Two-step randomness sharing in PSS where each participant is equipped with two antennas.

In the second time slot  $T_2$ , each participant  $n$  transmits probe signals  $\mathbf{s}_n$  using their antenna 2, respectively. At the same time, their antenna 1 are used to receive all the signals. Similar to the first time slot, the received signal at each participant can be written as

$$\mathbf{y}_{k_1} = \sum_{n \in \mathcal{B}, n \neq k} h_{k_1, n_2} \mathbf{s}_n + \mathbf{n}_{k_1}. \quad (5)$$

Due to the channel reciprocity, we have  $h_{i,j} = h_{j,i}$ . Consequently the shared randomness among Alice, Bob and Charlie can be given as  $\tilde{\mathbf{h}}_{BA} = (\tilde{h}_{B_2,A_1}, \tilde{h}_{B_1,A_2})$ ,  $\tilde{\mathbf{h}}_{CA} = (\tilde{h}_{C_2,A_1}, \tilde{h}_{C_1,A_2})$ ,  $\tilde{\mathbf{h}}_{BC} = (\tilde{h}_{B_2,C_1}, \tilde{h}_{B_1,C_2})$ .

- **Secret key generation.** Based on the two-step randomness sharing, each participant within the group can obtain the corresponding estimated channel gains, i.e., Alice gets  $\tilde{\mathbf{h}}_{BA}$  and  $\tilde{\mathbf{h}}_{CA}$ , Bob gets  $\tilde{\mathbf{h}}_{BC}$  and  $\tilde{\mathbf{h}}_{BA}$  and Charlie gets  $\tilde{\mathbf{h}}_{CA}$  and  $\tilde{\mathbf{h}}_{BC}$ . Then according to the pairwise key agreement schemes in [6, 9], the cumulative distribution function (CDF) based quantizer maps  $\tilde{\mathbf{h}}_{BA}$ ,  $\tilde{\mathbf{h}}_{CA}$ ,  $\tilde{\mathbf{h}}_{BC}$  to the corresponding Gray code. After information reconciliation and privacy amplification, three pairwise keys  $\tilde{\mathbf{h}}_{BA}^\Delta$ ,  $\tilde{\mathbf{h}}_{CA}^\Delta$  and  $\tilde{\mathbf{h}}_{BC}^\Delta$  are generated. Next, all the three participants calculate the XOR of the pairwise keys they possess. Thus the final secret keys  $(K_A, K_B, K_C)$  can be easily obtained by  $K_A = \tilde{\mathbf{h}}_{BA}^\Delta \oplus \tilde{\mathbf{h}}_{CA}^\Delta$ ,  $K_B = \tilde{\mathbf{h}}_{BA}^\Delta \oplus \tilde{\mathbf{h}}_{BC}^\Delta$ ,  $K_C = \tilde{\mathbf{h}}_{CA}^\Delta \oplus \tilde{\mathbf{h}}_{BC}^\Delta$  with the key rate  $R_{key}$ .

As the channel between any two participants consists of two sub-channels, concatenating the pairwise secret keys from each sub-channel, the key rates for each channel  $\mathbf{h}_{BA}$ ,  $\mathbf{h}_{CA}$ ,  $\mathbf{h}_{BC}$  can be written as  $R_{BA} = R_{B_2,A_1} + R_{B_1,A_2}$ ,  $R_{CA} = R_{C_2,A_1} + R_{C_1,A_2}$ ,  $R_{BC} = R_{B_2,C_1} + R_{B_1,C_2}$ . Since the shorter key is protected by the longer key in XOR operation, the group key rate is limited by the smallest pairwise key rate. Therefore the final keys  $(K_A, K_B, K_C)$  in this scheme are obtained with the key rate

$$R_{key} = \min\{R_{BA}, R_{CA}, R_{BC}\}. \quad (6)$$

### 3.2 Power Allocation

Here we design an algorithm to search for the optimal power allocation for the PSS scheme under total power constraint. The problem we solve can be given as

$$\begin{aligned} & \text{maximize} && R_{key} \\ & \text{s.t.} && P = \sum_{d \in Q} P_d, \\ & && P_d > 0 \end{aligned} \quad (7)$$

where  $P$  is the total power of the group and  $Q$  is the set of all the antennas within the group.  $P_d$  is the transmission power of antenna  $d$ . Exploiting the penalty function method, we can rewrite the problem as

$$\begin{aligned} & \text{maximize} && R_{key} + \lambda \left[ P, \sum_{d \in Q} P_d \right]^+, \\ & \text{s.t.} && P_d > 0 \end{aligned} \quad (8)$$

where  $\lambda$  is a inertial weight coefficient for the penalty function.  $[a, b]^+$  means that  $[a, b]^+ = 0$  if  $a \geq b$ , otherwise  $[a, b]^+ = a - b$ .

---

**Algorithm 1. PSO algorithm for power allocation**


---

1. Set  $n = 0$ , and generate the initial position  $\{x_{i,d}^n, d \in Q\}$  and velocity  $\{v_{i,d}^n, d \in Q\}$  for each particle.  $x_{i,d}^n \in [x_{min}, x_{max}]$ ,  $v_{i,d}^n \in [v_{min}, v_{max}]$ .
  2. Calculate the fitness  $F_i^n$  for each particle. Then we get  $\mathbf{P}_i = [x_{i,A_1}^0, x_{i,A_2}^0, \dots, x_{i,C_2}^0]$  and  $\mathbf{P}_b = [x_{b,A_1}^0, x_{b,A_2}^0, \dots, x_{b,C_2}^0]$ .
  3. Let  $n = n + 1$ , and update the value of  $v_i^n$  and  $x_i^n$  according to Eq.(9) and Eq.(10). If  $v_{i,d}^n < v_{min}$ , set  $v_{i,d}^n = v_{min}$ , else if  $v_{i,d}^n > v_{max}$ , set  $v_{i,d}^n = v_{max}$ . If  $x_{i,d}^n < x_{min}$ , set  $x_{i,d}^n = x_{min}$ , else if  $x_{i,d}^n > x_{max}$ , set  $x_{i,d}^n = x_{max}$ .
  4. Calculate the new fitness  $F_i^n$ . If  $F_i^n > F_i^{n-1}$ , set  $\mathbf{P}_i = [x_{i,A_1}^n, x_{i,A_2}^n, \dots, x_{i,C_2}^n]$ . Meanwhile, if  $F_i^n > F_b^{n-1}$ , set  $b = i$ , and  $\mathbf{P}_b = [x_{b,A_1}^n, x_{b,A_2}^n, \dots, x_{b,C_2}^n]$ .
  5. If the number of iterations reaches to the predetermined value, stop and get the optimal power allocation  $\mathbf{P}_b$ , otherwise return to step 3.
- 

We design the power allocation based on the proposed PSO algorithm to maximize the key rate. PSO is inspired by the birds flocking behaviors and is a population-based optimization method. In Algorithm 1,  $\mathbf{x}_i^n = \{x_{i,d}^n, d \in Q\}$  is the position of bird  $i$  at time  $n$ , and  $x_{i,d}^n$  means the transmission power of antenna  $d$ .  $\mathbf{v}_i^n = \{v_{i,d}^n, d \in Q\}$  is the velocity of bird  $i$ .  $\mathbf{P}_i = [x_{i,A_1}^n, x_{i,A_2}^n, \dots, x_{i,C_2}^n]$  is the personal best position of bird  $i$  and  $\mathbf{P}_b = [x_{b,A_1}^n, x_{b,A_2}^n, \dots, x_{b,C_2}^n]$  represents the global best position of the group, where  $b$  indicates bird  $b$ . Moreover, according to Eq. (8), the fitness  $F$  can be given as  $F = R_{key} + \lambda \left[ P, \sum_{d \in Q} P_d \right]^+$ . The purpose is to find the best position where the fitness  $F$  is maximum through iteration. The position and speed update model is

$$\mathbf{v}_i^{(n+1)} = \mathbf{v}_i^n + c_1 \boldsymbol{\beta}_1 \diamond (\mathbf{P}_i - \mathbf{x}_i^n) + c_2 \boldsymbol{\beta}_2 \diamond (\mathbf{P}_b - \mathbf{x}_i^n), \quad (9)$$

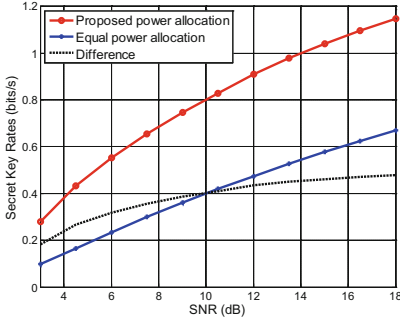
$$\mathbf{x}_i^{(n+1)} = \mathbf{x}_i^n + \omega \mathbf{v}_i^{(n+1)}, \quad (10)$$

where  $\diamond$  represents the element-by-element (Hadamard) product operation.  $\omega$  is the inertial weight coefficient and  $c_1$  and  $c_2$  are the learning factors. We set  $\omega = 0.5$ ,  $c_1 = c_2 = 2$ .  $\boldsymbol{\beta}_1$  and  $\boldsymbol{\beta}_2$  are vectors which obey uniform distributions over  $[0,1]$ . Using Algorithm 1, we update the power allocation and when the number of iterations reaches to a predetermined value, we can get the optimal power allocation.

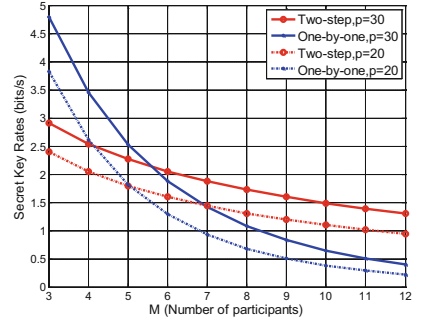
## 4 Numerical Results and Analysis

In order to estimate the performance of our proposed scheme, some numerical examples are provided in this section. For simplicity, all additive noise variance are assumed to be 1 (i.e.,  $\sigma^2 = 1$ ).

Figure 3(a) compares the secret key rates of our proposed power allocation with the equal power allocation. We assume the variances of each channel gain are set as  $\sigma_{A_1,B_2} = 2.7$ ,  $\sigma_{A_2,B_1} = 1.3$ ,  $\sigma_{B_2,C_1} = 1.1$ ,  $\sigma_{B_1,C_2} = 0.09$ ,  $\sigma_{A_1,C_2} = 5.7$ ,  $\sigma_{A_2,C_1} = 4$  and  $\sigma_{i,j} = \sigma_{j,i}$ . The inertial weight coefficient is set as  $\lambda = 4$ . It is obvious that our power allocation scheme using PSO algorithm outperforms equal power allocation. We can also see that the secret key rate difference between the two allocations increases with the increased SNR at the low SNR region. However, when the SNR is higher, the difference tends to be a stable value. This phenomenon occurs because the proposed power allocation algorithm tends to assign more power to channels with worse channel quality. When SNR is low, the secret key rate is mainly limited by noise, so with SNR increasing the improvement of the power allocation algorithm can be more significant. However, when SNR is high, the secret key rate is mainly limited by the variances of channel coefficients, thus the improvement of the power allocation algorithm can become stable.



(a)



(b)

**Fig. 3.** (a). Comparison of key rates with proposed power allocation and key rates with equal power distribution under total power constraint. (b). Secret key rates using two-step randomness sharing and one-by-one randomness sharing versus the number of participants, the variances of all channel gains are 2.7.

Moreover, Fig. 3(b) shows the secret key rates using two-step randomness sharing and one-by-one randomness sharing as a function of the number of participants (i.e.,  $M$ ) during the coherence time. The variances of all channel gains are 2.7, and the power  $P = 20$  or 30. The results indicate that our two-step randomness sharing can reduce the time overhead when the number of participants gets large.

## 5 Conclusions

In this paper, we have investigated the  $(n, n)$  threshold secret sharing scheme based on physical layer in MIMO systems. In our PSS scheme, three legitimate participants within a group employ the two-step randomness sharing scheme to establish keys with

each other exploiting the fading channel coefficients. Once the group secret keys generated, any participant in the group can encrypt confidential message and let the rest of the group work together to restore the message. Moreover, a PSO algorithm based power allocation scheme was derived for total power constraint. Numerical results show that our proposed power allocation is efficient on the secret key rates.

**Acknowledgment.** Project 61471066 supported by NSFC.

## References

1. Lin, C.C., Tsai, W.H.: Secret image sharing with steganography and authentication. *J. Syst. Softw.* **73**(3), 405–414 (2004)
2. Hershey, J.E., Hassan, A.A., Yarlagadda, R.: Unconventional cryptographic keying variable management. *IEEE Trans. Commun.* **43**(1), 3–6 (1995)
3. Liu, H., Yang, J., Wang, Y., Chen, Y.J., Koksai, C.E.: Group secret key generation via received signal strength: Protocols, achievable rates, and implementation. *IEEE Trans. Mob. Comput.* **13**(12), 2820–2835 (2014)
4. Liu, H., Wang, Y., Yang, J., Chen, Y.: Fast and practical secret key extraction by exploiting channel response. In: 2013 Proceedings of the IEEE INFOCOM, pp. 3048–3056 (2013)
5. Wang, Q., Su, H., Ren, K., Kim, K.: Fast and scalable secret key generation exploiting channel phase randomness in wireless networks. In: 2011 Proceedings of the IEEE INFOCOM, pp. 1422–1430 (2011)
6. Chen, K., Natarajan, B.: MIMO-based secret key generation strategies: rate analysis. *Int. J. Mob. Comput. Multimedia Commun.* **6**(3), 22–55 (2014)
7. Shimizu, T., Iwai, H., Sasaoka, H.: Physical-layer secret key agreement in two-way wireless relaying systems. *IEEE Trans. Inf. Forensics Secur.* **6**(3), 650–660 (2011)
8. Zhou, H., Huie, L.M., Lai, L.: Secret key generation in the two-way relay channel with active attackers. *IEEE Trans. Inf. Forensics Secur.* **9**(3), 476–488 (2014)
9. Xu, P., Cumanan, K., Ding, Z., Dai, X., Leung, K.K.: Group secret key generation in wireless networks: algorithms and rate optimization. *IEEE Trans. Inf. Forensics Secur.* **11**(8), 1831–1846 (2016)
10. Zhang, J., Duong, T.Q., Marshall, A., Woods, R.: Key generation from wireless channels: A review. *IEEE Access* **4**, 614–626 (2016)

Signal and Information Processing, Networking and  
Computers

Proceedings of the 3rd International Conference on  
Signal and Information Processing, Networking and  
Computers (ICSINC)

Sun, S.; Chen, N.; Tian, T. (Eds.)

2018, XIV, 511 p. 265 illus., Hardcover

ISBN: 978-981-10-7520-9