

# On the RIS Manipulating Attack and Its Countermeasures in Physical-layer Key Generation

Lei Hu\*, Guyue Li\*<sup>†</sup>, Hongyi Luo\*, Aiqun Hu<sup>†‡</sup>

\*School of Cyber Science and Engineering, Southeast University, Nanjing, 210096, China

<sup>†</sup>Purple Mountain Laboratories for Network and Communication Security, Nanjing, 210096, China

<sup>‡</sup>National Mobile Communications Research Laboratory, Southeast University, Nanjing, 210096, China

Corresponding author: Guyue Li, Email: guyuelee@seu.edu.cn

**Abstract**—Reconfigurable Intelligent Surface (RIS) is a new paradigm that enables the reconfiguration of the wireless environment. Based on this feature, RIS can be employed to facilitate Physical-layer Key Generation (PKG). However, this technique could also be exploited by the attacker to destroy the key generation process via manipulating the channel features at the legitimate user side. Specifically, this paper proposes a new RIS-assisted Manipulating attack (RISM) that reduces the wireless channel reciprocity by rapidly changing the RIS reflection coefficient in the uplink and downlink channel probing step in orthogonal frequency division multiplexing (OFDM) systems. The vulnerability of traditional key generation technology based on channel frequency response (CFR) under this attack is analyzed. Then, we propose a slewing rate detection method based on path separation. The attacked path is removed from the time domain and a flexible quantization method is employed to maximize the Key Generation Rate (KGR). The simulation results show that under RISM attack, when the ratio of the attack path variance to the total path variance is 0.17, the Bit Disagreement Rate (BDR) of the CFR-based method is greater than 0.25, and the KGR is close to zero. In addition, the proposed detection method can successfully detect the attacked path for SNR above 0 dB in the case of 16 rounds of probing and the KGR is 35 bits/channel use at 23.04MHz bandwidth.

**Index Terms**—Physical layer security, Reconfigurable Intelligent Surface, OFDM, secret key generation, active attack.

## I. INTRODUCTION

The rapid development of the fifth-generation (5G) communication system has greatly increased the amount of data transmitted in the air interface. However, due to the broadcast characteristics of the wireless media, a large amount of confidential information may be eavesdropped on by unauthorized users. The Physical-layer Key Generation (PKG) uses the reciprocity of the wireless channel to generate a pair of symmetric secret key to encrypt data. Due to the time-varying and spatial uncorrelation of the channel, the eavesdropper cannot predict the channel of the legitimate user and secure one-time pad communication can be realized [1].

However, the performance of PKG is limited by channel reciprocity and time-varying. Recently, Reconfigurable Intelligent Surface (RIS) emerges as a new technology that can realize the regulation of electromagnetic waves and thus change the wireless propagation environment [2]. Due to the passive characteristics and low hardware cost of RIS, RIS-assisted wireless communication system has been studied extensively.

Based on the above features, little existing literature has studied RIS-assisted PKG. Ji *et al.* [3] randomly change the phase of RIS to introduce artificial randomness and increase the key generation rate (KGR). In their other work [4], RIS reflecting coefficients are optimized to maximize the lower bound of secret key rate in multiple eavesdroppers scenario. Moreover, Lu *et al.* [5] adjusted the placement of RIS to maximize the key rate capacity. The above literature is all based on the single antenna scenario. Recently, [6] studies optimization of RIS beamforming to maximize key rate in MISO system. However, these works are based on the assumption that RIS is controlled by the legitimate party, e.g. BS, ignoring the fact that it could also be controlled by the attacker.

As far as we know, it is the first time to investigate the RIS in secret key generation from the aspect of active attack. In this paper, we propose a new RIS-assisted Manipulating attack (RISM) in the orthogonal frequency division multiplexing (OFDM) system and give the RISM detection method and key generation method based on path separation. The main contributions of this paper are summarized as follows.

- An RISM method is proposed to reduce the KGR, in which the active attacker Eve rapidly changes the phase of RIS to manipulate the wireless environment. The vulnerability of traditional key generation technology using the channel frequency response (CFR) coefficient under this attack is analyzed.
- A slewing rate detection method based on path separation and multiple channel probing is proposed. Then, we adopt a flexible quantization method based on the separated paths to improve the KGR.
- Simulation results show that the KGR of CFR coefficient under RISM is close to zero when the ratio of the variance of the attacked path is 0.17. The success rate of detection is close to 1 for SNR above 0 dB. Also, the KGR is improved significantly.

## II. THE OFDM-BASED PKG SYSTEM

We first consider a general key generation model in OFDM system. It is assumed that Alice and Bob are equipped with single antenna. To leverage the channel reciprocity of time-division duplex (TDD) mode, Alice and Bob take turns to estimate channels within coherence time. During the channel probing stage, the OFDM symbol transmitted by Alice is

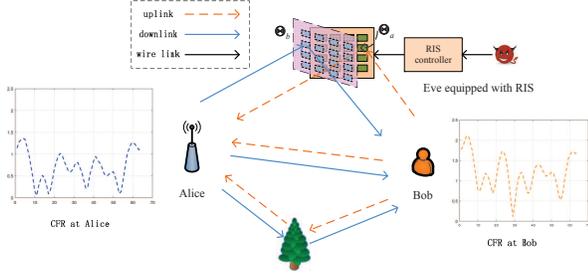


Fig. 1. The proposed RISM attack model.

denoted as  $\mathbf{X} = \text{diag}(x_1, x_2, \dots, x_L)$ , where  $L$  is the number of subcarriers. The received signal at Bob side after removing cyclic prefix is represented as

$$\mathbf{Y}_b = \mathbf{X}\mathbf{H}_d + \mathbf{N}_b \quad (1)$$

where  $\mathbf{H}_d \in \mathbb{C}^{L \times 1}$  denotes the direct channel from Alice to Bob,  $\mathbf{N}_b \sim \mathcal{N}_c(\mathbf{0}, \sigma_n^2 \mathbf{I}_L)$  is the complex additive white Gaussian noise. Then, the least-square (LS) estimation is performed at Bob and the estimated channel is given by

$$\bar{\mathbf{H}}_b = \mathbf{H}_d + \tilde{\mathbf{N}}_b \quad (2)$$

where the noise component  $\tilde{\mathbf{N}}_b = \mathbf{X}^{-1}\mathbf{N}_b$  and  $\tilde{\mathbf{N}}_b \sim \mathcal{N}_c(\mathbf{0}, \sigma_n^2 \mathbf{X}^{-1})$ . For the purpose of exposition, we assume  $x_1 = x_2 = \dots = x_L = 1$ . Since uplink and downlink channel probing is completed within coherence time, the channel reciprocity holds between channel probing. Similarly, Alice estimates the channel as

$$\bar{\mathbf{H}}_a = \mathbf{H}_d + \tilde{\mathbf{N}}_a \quad (3)$$

Then, in the quantization step, Cumulative Distribution Function (CDF) based quantization method can be used to convert channel coefficients into bits [7]. Due to the existence of noise, there will be a small amount of inconsistent bits between Alice's and Bob's quantization results, which can be corrected through information reconciliation step. Finally, the information leaked in the information reconciliation step can be eliminated through the privacy amplification.

### III. RISM ATTACK SCHEME

In this section, we propose a novel RIS-assisted attack method, RISM, which reduces the channel reciprocity by changing the reflection coefficient of the uplink and downlink channel probing and thus reduces the KGR. We then give the change of channel correlation coefficient and the influence on CDF based quantization after RISM.

#### A. RISM Attack Model

Fig. 1 shows an RISM attack in PKG system, wherein a malicious attacker Eve employs an RIS to destroy the reciprocal channel between Alice and Bob. The RIS controlled by Eve has  $M$  passive reflection elements, and the phase of each element in the uplink channel probing stage is different from that of the downlink stage. We consider an active attack scheme where Eve doesn't require extra hardware to eavesdrop

and doesn't need to know the time slot of the channel probing. Particularly, Eve randomly and rapidly changes the reflection coefficient of each element in both uplink and downlink. The time interval of change is much smaller than the coherence time. Thus, the channel estimated by Bob in RISM is

$$\hat{\mathbf{H}}_b = \mathbf{H}_d + \sum_{m=1}^M \theta_{b,m} \mathbf{H}_{ar,m} \odot \mathbf{H}_{rb,m} + \tilde{\mathbf{N}}_b \quad (4)$$

$$= \mathbf{H}_d + \mathbf{H}_r \Theta_b + \tilde{\mathbf{N}}_b \quad (5)$$

where  $\odot$  denotes the Hadamard product,  $\mathbf{H}_{ar,m} \in \mathbb{C}^{L \times 1}$  and  $\mathbf{H}_{rb,m} \in \mathbb{C}^{L \times 1}$  are the links from Alice to  $m$ -th sub-surface of RIS and from the  $m$ -th sub-surface to Bob, respectively.  $\mathbf{H}_r \Theta_b$  is the equivalent cascaded channel matrix and  $\mathbf{H}_r = [\mathbf{H}_{r,1}, \mathbf{H}_{r,2}, \dots, \mathbf{H}_{r,M}]$ , where  $\mathbf{H}_{r,m} \triangleq \mathbf{H}_{ar,m} \odot \mathbf{H}_{rb,m}$ ,  $m = 1, 2, \dots, M$ . The RIS reflection vector is  $\Theta_b = [\theta_{b,1}, \theta_{b,2}, \dots, \theta_{b,M}]^T$ . Similarly, the channel estimation at Alice in RISM can be expressed as

$$\hat{\mathbf{H}}_a = \mathbf{H}_d + \mathbf{H}_r \Theta_a + \tilde{\mathbf{N}}_a \quad (6)$$

where the reflection coefficient  $\theta_{u,m} = e^{j\phi_{u,m}}$ ,  $u = a, b$  and the phase  $\phi_{u,m}$  follows a independent and identically distributed (i.i.d.) uniform distribution over  $[0, 2\pi)$ .

#### B. Evaluation of RISM Effect

To evaluate the impact of RISM on channel reciprocity, Pearson's cross-correlation coefficient of CFR can be calculated. The  $\ell$ -th element of  $\hat{\mathbf{H}}_u$  is expressed as  $\hat{H}_{u,\ell} = H_{d,\ell} + \sum_{m=1}^M \theta_{u,m} H_{r,m}^\ell + \tilde{N}_{u,\ell}$ . Hence, the correlation coefficient of  $\ell$ -th channel estimation in the frequency domain is

$$\rho_\ell = \frac{\mathbb{E}\{(\hat{H}_{a,\ell} - \mu_{a,\ell})(\hat{H}_{b,\ell} - \mu_{b,\ell})^*\}}{\sqrt{\mathbb{E}\{|\hat{H}_{a,\ell} - \mu_{a,\ell}|^2\} \mathbb{E}\{|\hat{H}_{b,\ell} - \mu_{b,\ell}|^2\}}} \quad (7)$$

$$= \frac{\sigma_{d,\ell}^2 + G_1}{\sigma_{d,\ell}^2 + G_2 + \xi_\ell + \sigma_{n,\ell}^2} \quad (8)$$

$$= \frac{\sigma_{d,\ell}^2}{\sigma_{d,\ell}^2 + \xi_\ell + \sigma_{n,\ell}^2} \quad (9)$$

where  $\sigma_{d,\ell}^2$  and  $\sigma_{n,\ell}^2$  denote the variance of direct channel and noise in the  $\ell$ -th subcarrier, respectively. Since the reflection phase is uniformly distributed, we have

$$G_1 = \mathbb{E}\{(\hat{H}_{d,\ell} - \mu_{d,\ell}) \left( \sum_{m=1}^M \theta_{b,m} H_{r,m}^\ell \right)^*\} \quad (10)$$

$$+ \mathbb{E}\{(\hat{H}_{d,\ell} - \mu_{d,\ell})^* \left( \sum_{m=1}^M \theta_{a,m} H_{r,m}^\ell \right)\} \\ + \mathbb{E}\{ \left( \sum_{m=1}^M \theta_{b,m} H_{r,m}^\ell \right)^* \left( \sum_{m=1}^M \theta_{a,m} H_{r,m}^\ell \right) \} = 0$$

$$G_2 = \mathbb{E}\{2\Re((\hat{H}_{d,\ell} - \mu_{d,\ell}) \left( \sum_{m=1}^M \theta_{a,m} H_{r,m}^\ell \right)^*)\} = 0 \quad (11)$$

Also,  $\xi_\ell = \sum_{m=1}^M \sigma_{r,m,\ell}^2$  is the sum of the cascaded channel variances. Since the variance  $\xi_\ell > 0$ , RISM will inevitably lead

to a decrease in the CFR correlation coefficient. As the  $\xi_\ell$  increases, the correlation coefficient tends to zero, resulting in low channel reciprocity.

In addition, to reflect the impact of RISM on quantization step in PKG, we analyze the CDF based bit disagreement rate (BDR) of CFR under this attack, where Alice and Bob use the CDF of channel coefficient to divide its range into  $2^{m_i}$  equally spaced regions and gray code is used to encode  $\widehat{H}_{u,\ell}$  into  $m$  bit(s). The BDR after RISM can be approximated as formula (12) in the case of low bit disagreement, where  $A = \sigma_{d,\ell}^2 + \xi_\ell + \sigma_{n,\ell}^2$ ,  $\Phi$  is the CDF of a Gaussian distribution with zero mean unit variance,  $\alpha_a$  and  $\beta_a$  are the upper and lower bounds of  $\widehat{H}_{a,\ell}$  in the agreement area when  $\widehat{H}_{a,\ell}$  is given, i.e.

$$\alpha_a = \min\{1, \lceil F(\widehat{H}_{a,\ell})2^{-m_i} \rceil 2^{-m_i}\} \quad (13)$$

$$\beta_a = \max\{0, \lfloor F(\widehat{H}_{a,\ell})2^{-m_i} \rfloor 2^{-m_i}\} \quad (14)$$

According to the results of literature [7] and formula (12), the BDR will increase with the increase of variance of the cascaded channel. Considering that the error-correcting ability of information reconciliation is limited, when the BDR is beyond the reconciliation capability, the users have to discard the generated bits, indicating the failure of this round of secret key generation.

#### IV. RISM DETECTION AND COUNTERMEASURES

In this section, we propose a slewing rate detection method and a flexible quantization method to resist RISM attack. In addition, we give the theoretical key rate performance loss when the OFDM bandwidth is insufficient to distinguish each path.

##### A. Path Separation and Detection Method

We consider that in a multi-path environment, only the paths through the RIS change rapidly, while others remain the same during the coherence time. Motivated by this, by separating the attacked paths, the impact of the attack can be eliminated and we can reconstruct the reciprocal channel for key generation. In OFDM system, each path can be obtained via an  $L$ -point inverse discrete Fourier transform (IDFT) [8]. Given the proximity of adjacent elements of the RIS, it is often difficult to distinguish multiple paths through different elements. Therefore, it can be assumed that only one path passes through the RIS<sup>1</sup>. The matrix form of the path separation can be described as

$$\mathbf{h}_u = \frac{1}{L} \mathbf{F}_L^H (\mathbf{H}_d + \mathbf{H}_r \mathbf{\Theta}_u + \tilde{\mathbf{n}}_u) \quad (15)$$

$$= \mathbf{h}_d + \mathbf{h}_{r,u} + \tilde{\mathbf{n}}_u \quad (16)$$

where  $\mathbf{F}_L$  refers to the  $L$  order discrete Fourier transform (DFT) matrix. Since the number of paths is small in the multipath channel, it is generally considered sparse. Therefore, the direct channel and the cascade channel can be characterized as  $\mathbf{h}_d = [\bar{h}_1, \dots, \bar{h}_{L_d}, \mathbf{0}_{1 \times (L-L_d)}]^T$  and  $\mathbf{h}_{r,u} =$

$[0, \dots, 0, \bar{h}_{u,k}, \mathbf{0}_{1 \times (L-k)}]^T$ , respectively. The  $k$ -th element of  $\mathbf{h}_{r,u}$  is the attacked path.

Then, we distinguish which paths are available for key generation and which path is attacked by Eve. We propose to detect RISM by sounding the channel multiple times in a coherence time, which can also reduce noise on unattacked paths. Specifically, according to the time chart of proposed key generation based on IEEE 802.11a Data frame, a round of channel probing can be carried out every 2.8ms, providing the possibility of attack detection. In order to minimize the impact of noise, the detection method is shown in (17)

$$\frac{\sum_{q=1}^Q h_{i,q} h_{i,q}^*}{Q} - \frac{1}{L_d + 1} \sum_{\ell=1}^{L_d+1} \frac{\sum_{q=1}^Q h_{\ell,q} h_{\ell,q}^*}{Q} \underset{\mathcal{H}_1}{\overset{\mathcal{H}_0}{\gtrless}} \alpha \quad (17)$$

where  $h_{i,q}$  is the  $q$ -th round channel probing on  $i$ -th path and  $Q$  is the number of probing.  $\mathcal{H}_0$  indicates the  $i$ -th path is attacked by RISM and  $\mathcal{H}_1$  indicates the RISM is absent on  $i$ -th path. Note that  $\alpha$  depends on the variance of the attacked path and is set to be an empirical value. With the increase of the number of probes, the estimation of the variance will be more accurate. However, the channel probing will result in the increase of pilot overhead and the number of channel probing rounds is limited in the coherence time. Therefore, a tradeoff should be made between the number of channel probing and the success rate. Finally, Alice and Bob will discard the attacked path, and the remaining paths are perfectly satisfied channel reciprocity and can be used for key generation.

##### B. Path Separation based Flexible Quantization

Considering that after IDFT is performed, different paths will have different signal-to-noise ratios (SNR). To make full use of high SNR paths and reduce the BDR of low SNR paths, we use a flexible quantization method to maximize the generated key bits. The SNR in the frequency domain is defined as

$$\text{SNR} = \frac{\mathbb{E}\{(\mathbf{H}_d + \mathbf{H}_r \mathbf{\Theta}_u)^H (\mathbf{H}_d + \mathbf{H}_r \mathbf{\Theta}_u)\}}{\mathbb{E}\{\tilde{\mathbf{N}}_u^H \tilde{\mathbf{N}}_u\}} \quad (18)$$

$$= \frac{\mathbb{E}\{\mathbf{H}_d^H \mathbf{H}_d\} + M \mathbb{E}\{\mathbf{H}_r^H \mathbf{H}_r\}}{L \sigma_n^2} \quad (19)$$

After the RISM attack detection, the path through RIS is removed. Then, the SNR of the  $i$ -th path is [1]

$$\text{SNR}_i = \frac{\mathbf{f}_i / L \mathbb{E}\{\mathbf{H}_d \mathbf{H}_d^H\} \mathbf{f}_i^H / L}{\sigma_n^2 / L} \quad (20)$$

$$= \frac{\mathbf{f}_i / L \mathbf{F}_L \mathbb{E}\{\mathbf{h}_d \mathbf{h}_d^H\} \mathbf{F}_L^H \mathbf{f}_i^H / L}{\sigma_n^2 / L} \quad (21)$$

$$= \frac{L \mathbb{E}\{|\bar{h}_i|^2\}}{\sigma_n^2}, \quad i \neq k \quad (22)$$

where  $\mathbf{f}_i$  is the  $i$ -th row of the DFT matrix  $\mathbf{F}$ . In the practical system, in order to ensure the key consistency, the key error rate (KER) needs to be below  $10^{-3}$ . To meet this requirement, we set quantization levels according to the SNR of each path. Particularly, each path will use higher quantization bits to increase the key rate when it is lower than a given KER.

<sup>1</sup> Assuming a bandwidth of  $B = 20$  MHz in IEEE 802.11a, paths can only be distinguished if the distance between them is greater than  $d = c/B = 15$  m. However, most RIS sizes are much smaller than  $d$ .

$$\begin{aligned}
P'_{BD} &\approx \frac{1}{m_i} \{1 - P_{CA}\} \\
&= \frac{1}{m_i} \left\{ 1 - \int_{v=-\infty}^{\infty} \left\{ \Phi \left[ \frac{(\sigma_{d,\ell}^2 + A)\Phi^{-1}[\alpha_a] - \sigma_{d,\ell}^2 v}{\sqrt{(2\sigma_{d,\ell}^2 + A)A}} \right] - \Phi \left[ \frac{(\sigma_{d,\ell}^2 + A)\Phi^{-1}[\beta_a] - \sigma_{d,\ell}^2 v}{\sqrt{(2\sigma_{d,\ell}^2 + A)A}} \right] \right\} \frac{e^{-v^2/2}}{\sqrt{2\pi}} dv \right\}
\end{aligned} \tag{12}$$

### C. Performance Analysis of Key Generation

Due to the finite bandwidth, the resolution to estimate the delay of every path is finite as well. Particularly, under bandwidth  $B$ , the path delay resolution is expressed as  $\Delta\tau = \frac{1}{B}$ . As a result, when the bandwidth is insufficient to resolve each path, paths that are in the same tap as the attack path will be discarded after the attack detection, which affects the KGR.

In order to measure the impact of the discarded available paths on the KGR, we assume that there are  $N$  discarded paths in the total path  $L_d$ , and  $N$  increases with the reduction of bandwidth. We assume that  $\tilde{\mathbf{h}}_u \in \mathbb{C}^{N \times 1}$  denotes the discarded paths. At this point, the theoretically reduced key rate is

$$R_{reduced} = I(\tilde{\mathbf{h}}_a; \tilde{\mathbf{h}}_b) \tag{23}$$

$$= \log_2 \frac{|\mathbf{R}_a| |\mathbf{R}_b|}{|\mathbf{R}_a| |\mathbf{R}_b - \mathbf{R}_{ab} \mathbf{R}_a^{-1} \mathbf{R}_{ba}|} \tag{24}$$

$$= \log_2 \frac{|\mathbf{\Lambda}_h + \frac{\sigma_n^2}{L} \mathbf{I}|}{|\mathbf{\Lambda}_h + \frac{\sigma_n^2}{L} \mathbf{I} - \mathbf{\Lambda}_h (\mathbf{\Lambda}_h + \frac{\sigma_n^2}{L} \mathbf{I})^{-1} \mathbf{\Lambda}_h^H|} \tag{25}$$

$$= \sum_{i=1}^N \log_2 \frac{1}{1 - \left( \frac{L\lambda_i/\sigma_n^2}{1+L\lambda_i/\sigma_n^2} \right)^2} \tag{26}$$

where the covariance matrix

$$\mathbf{R}_b = \mathbb{E}\{\tilde{\mathbf{h}}_b \tilde{\mathbf{h}}_b^H\} = \mathbf{\Lambda}_h + \sigma_n^2 \mathbf{I} / L \tag{27}$$

$$\mathbf{R}_{ab} = \mathbb{E}\{\tilde{\mathbf{h}}_a \tilde{\mathbf{h}}_b^H\} = \mathbf{\Lambda}_h \tag{28}$$

where  $\lambda_i = [\mathbf{\Lambda}_h]_{i,i}$  is the variance of  $i$ -th discarded path. We notice that the reduced key rate depends on the path variance and the number of paths discarded. Hence, higher bandwidth is needed to improve KGR.

## V. NUMERICAL RESULTS

In this section, we evaluate the performance of our proposed RISM attack and countermeasures via numerical results. The geometry-based channel model 3GPP Spatial Channel Model (SCM) is adopted for simulation. In the simulation of the broadband multipath environment, the number of paths before being attacked is set to 7, and each path has 20 subpaths. The number of RIS reflection elements  $M$  is 30, and the distance between adjacent elements is  $\lambda/2$ . The positions of Alice, Bob, and RIS are randomly distributed, and the distance between them is evenly distributed within [35, 200] m. In OFDM system, the Carrier frequency  $f_c = 2$  GHz and 64 subcarriers are implemented. The bandwidth  $B$  is set to be 23.04 MHz and each path can be resolved.

Considering that as the number of RIS reflection elements increases, the subpath of the attacked path increases,

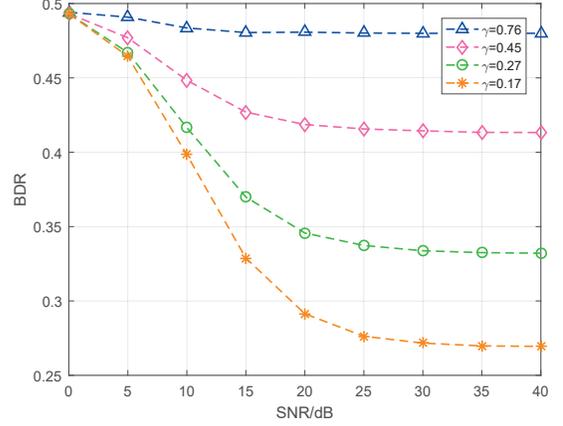


Fig. 2. BDR of CFR amplitude quantization after RISM.

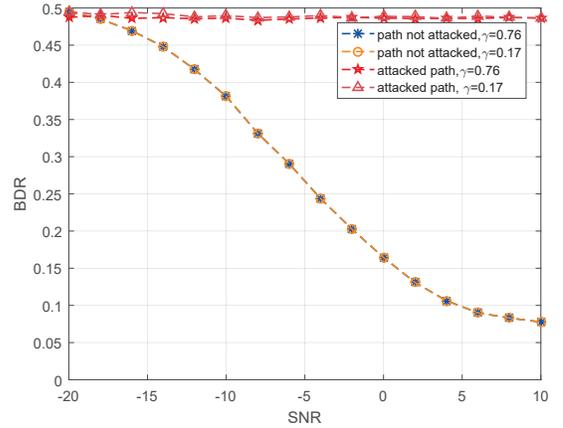


Fig. 3. BDR of different path versus SNR.

increasing the variance of the attacked path. Define  $\gamma = \frac{\mathbb{E}\{|\tilde{h}_{u,k}|^2\}}{\sum_{i=1}^{L_d} \mathbb{E}\{|\tilde{h}_i|^2\} + \mathbb{E}\{|\tilde{h}_{u,k}|^2\}}$  as the ratio of the variance of the attacked path to the variance of the total paths. Fig. 2 compares the BDR of the CFR v.s. different  $\gamma$  after the RISM, where the quantization bit  $m = 1$ . We can find that as the SNR increases, the BDR corresponding to different  $\gamma$  gradually decreases and tends to a constant value. However, we note that the BDR increases with the increase of  $\gamma$ . When  $\gamma$  is small and equal to 0.17, the final BDR tends to 0.27. According to the literature [9], the maximum tolerable BDR is 0.11 and the generated bits in RISM will be discarded.

Fig. 3 shows the BDR of different paths after the attack,

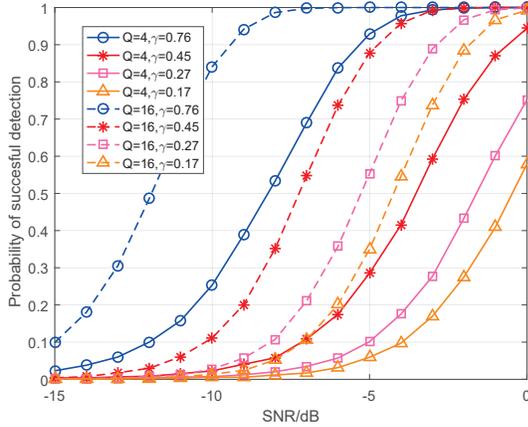


Fig. 4. Probability of successful detection versus SNR and probing times.

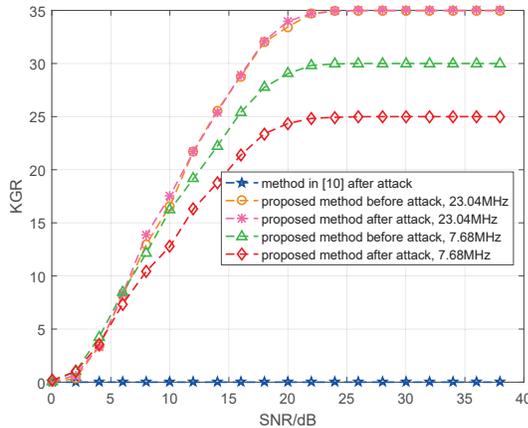


Fig. 5. KGR comparison between the CFR method and the proposed method.

where the BDR of the attacked path is around 0.5 at different  $\gamma$ , which means that the path is completely non-reciprocal. Besides, the path that does not go through RIS decreases with the increase of SNR, providing conditions for the reconstruction of the reciprocal channel.

Fig. 4 shows the probability of successful detection. As the variance of noise decreases, the probability increases. In addition, the success rate increases with the increase of attacked path variance ratio  $\gamma$ . Also, as the number of probes increases, a higher detection probability can be obtained. In the simulation setup, assume the speed  $v = 1m/s$ , then the Doppler spread  $D_s$  is about 6.7 Hz. Thus, the coherence time is  $T_c = \frac{1}{2D_s} = 75ms$ . Since multiple probing rounds increase the pilot overhead, we set the round of probing  $Q = 16$  to achieve a tradeoff between the success rate and the overhead.

Fig. 5 presents the practical key rate after channel probing, CDF-based quantization, and low-density parity-check code (LDPC) bit-flipping-based information reconciliation. We notice that the BDR of traditional key generation method [10] based on CFR is high, resulting in low KGR. With the increase

of SNR, the number of quantization bits of each path increases, leading to the increase of total key bits generated. At the same time, at 7.68MHz bandwidth, one available path and the attacked path are in the same tap. Therefore, a reciprocal path is discarded and the KGR after the attack is lower than that before the attack. In contrast, with high bandwidth of 23.04MHz, the path resolution is high enough that the attacked path can be removed independently. Therefore, the nearly perfect key rate can be achieved.

## VI. CONCLUSION

In this paper, an RISM scheme aiming to reduce the rate of key generation was proposed and analyzed. In traditional CFR-based method, we showed its vulnerability on the channel reciprocity and quantization step of key generation under RISM. Therefore, the CFR-based method cannot generate effective key bits due to its high BDR. For more, the slewing rate detection method and flexible quantization were proposed to remove the attacked path and improve the KGR. Numerical results showed that a high success rate of detection can be obtained for SNR above 0 dB and a high KGR can be achieved.

## ACKNOWLEDGMENT

This work was supported in part by the National Natural Science Foundation of China under Grant 61941115 and Grant 61801115, in part by the Jiangsu key R & D plan BE2019109, and in part by the Zhishan Youth Scholar Program of SEU (3209012002A3).

## REFERENCES

- [1] G. Li, A. Hu, J. Zhang, L. Peng, C. Sun, and D. Cao, "High-agreement uncorrelated secret key generation based on principal component analysis preprocessing," *IEEE Transactions on Communications*, vol. 66, no. 7, pp. 3022–3034, 2018.
- [2] Q. Wu and R. Zhang, "Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming," *IEEE Transactions on Wireless Communications*, vol. 18, no. 11, pp. 5394–5409, 2019.
- [3] Z. Ji, P. L. Yeoh, G. Chen, C. Pan, Y. Zhang, Z. He, H. Yin, and Y. Li, "Random shifting intelligent reflecting surface assisted data transmission," *IEEE Wireless Communications Letters*, pp. 1–1, 2021.
- [4] Z. Ji, P. L. Yeoh, D. Zhang, G. Chen, Y. Zhang, Z. He, H. Yin, and Y. Li, "Secret key generation for intelligent reflecting surface assisted wireless communication networks," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 1, pp. 1030–1034, 2021.
- [5] X. Lu, J. Lei, Y. Shi, and W. Li, "Intelligent reflecting surface assisted secret key generation," *IEEE Signal Processing Letters*, pp. 1–1, 2021.
- [6] Y. Chen, G. Li, C. Pan, L. Hu, and A. Hu, "Intelligent Reflecting Surface-Assisted Secret Key Generation In Multi-antenna Network," *arXiv e-prints*, p. arXiv:2105.00511, May 2021.
- [7] N. Patwari, J. Croft, S. Jana, and S. K. Kaser, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Transactions on Mobile Computing*, vol. 9, no. 1, pp. 17–30, 2010.
- [8] G. Li, A. Hu, C. Sun, and J. Zhang, "Constructing reciprocal channel coefficients for secret key generation in fdd systems," *IEEE Communications Letters*, vol. 22, no. 12, pp. 2487–2490, 2018.
- [9] D. Elkouss, A. Leverrier, R. Alleaume, and J. J. Boutros, "Efficient reconciliation protocol for discrete-variable quantum key distribution," in *2009 IEEE International Symposium on Information Theory*, 2009, pp. 1879–1883.
- [10] S. Yasukawa, H. Iwai, and H. Sasaoka, "Adaptive key generation in secret key agreement scheme based on the channel characteristics in ofdm," in *2008 International Symposium on Information Theory and Its Applications*, 2008, pp. 1–6.