EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

# A powerful adversary model and corresponding OTP time slot allocation scheme in RIS-assisted physical layer key generation

Liquan Chen[1,2*], Yufan Song[1], Wanting Ma[1], Tianyu Lu[1], Peng Zhang[1] and Liang Chen[1]

*Correspondence:
lqchen@seu.edu.cn

[1] School of Cyber Science and Engineering, Southeast University, Nanjing 210096, Jiangsu, China
[2] Network and Communication Security, Purple Mountain Laboratories, Nanjing 211111, Jiangsu, China

## Abstract

Physical layer key generation (PLKG) is a technique of information-theoretic security to tackle the problem of key distribution between resource-constrained legitimate users and is a promising candidate for the one time pad (OTP) technique. However, in quasi-static, the key rate is greatly limited due to low entropy. Reconfigurable intelligent surface (RIS) is introduced to adaptively reconfigure the radio environment. However, how to allocate time slots in the OTP to counter the increasingly powerful adversary model is an urgent problem to be solved. In this paper, we propose a very powerful adversary model and give an attack strategy called eavesdropping channel search, which allows Eve to use its search and eavesdropping capabilities to maximize the probability of successful attacks. Meanwhile, we propose a time slot allocation algorithm in the OTP to ensure the security of the key. Simulations validate that our proposed attack strategy is more powerful than any existing adversary model and our proposed time slot allocation algorithm does not have any security loss.

**Keywords:** Physical layer key generation, One time pad, Reconfigurable intelligent surface, Adversary model

## 1 Introduction

The exponential growth of connectivity and widespread adoption of wireless communications in the Internet of Things (IoT) have resulted in an unprecedented acknowledgment of the importance of data confidentiality [1]. Consequently, a multitude of encryption schemes have been suggested for enhancing wireless network security. These can be broadly classified into symmetric encryption and asymmetric encryption [2]. The secure distribution and management of keys in the former pose a considerable challenge, especially in network environments of significant scale. The security of the latter is contingent upon the intricacy of the asymmetric encryption algorithm, which directly affects the efficacy of encryption and decryption in resource-constrained IoT environments. Furthermore, the emergence of formidable quantum computers presents a risk to the integrity of cryptographic methods, as they possess the capability to solve elliptic curve discrete logarithm problems in polynomial time [3].

Luckily, the issue of key distribution between two legitimate users, Alice and Bob, has been effectively addressed through the introduction of physical layer key generation (PLKG). This technique provides a cost-effective approach while maintaining information-theoretic security and lightweight properties [4]. PLKG exploits the inherent randomness and reciprocity of wireless channels to facilitate the establishment of symmetric keys between Alice and Bob [5]. The time-varying wireless channels serve as a source of randomness for generating physical layer keys. The reciprocal nature of channels within the coherence time enables Alice and Bob to acquire nearly identical channel state information (CSI). With the utilization of these attributes, Alice and Bob can successfully accomplish physical layer key generation schemes independently, devoid of any external node involvement [6].

Moreover, PLKG is a promising candidate for the one time pad (OTP) technique [7]. And OTP is commonly acknowledged as the holy grail of cryptography which provides information-theoretic security [8]. However, only a higher key rate can provide enough random keys for OTP. This is difficult to achieve in a quasi-static environment [9, 10]. To solve the problem, reconfigurable intelligent surface (RIS) is usually used to improve the key rate [11–14]. RIS is able to change the amplitude and phase of the reflected signals to reconfigure the radio environment [15].

In the OTP process, channel probing, information reconciliation and encrypted packet transmission all need to occupy channel time [16]. Therefore, time slot allocation is also a key issue. The work in [17] designs an optimal algorithm for allocating time slots for channel probing and encrypted packet transmission. The work in [18] designs a time slot allocation algorithm to maximize the transmission rate. However, the time slot cost of information reconciliation is ignored in the above schemes. At the same time, these schemes lack security against a robust adversary model.

To evaluate the security of the OTP, a robust adversary model needs to be designed. Some studies [17, 19] assume that Eve has a powerful yet finite computational capability and uses the incomplete randomness of the channel to search for keys. Some studies [20–23] assume that Eve can get the CSI correlated with the legitimate channel. But no adversary model considers Eve to have all of the above capabilities. In other words, none of the adversary models in these studies are powerful enough.

In this paper, we propose a very powerful adversary model. Meanwhile, we propose a time slot allocation algorithm in the OTP against the adversary model. Our main technical contributions are as follows:

- We propose a very powerful adversary model. We assume that Eve has a powerful yet finite computational capability and Eve can get the reconciliation information and the CSI correlated with the legitimate channel. We give an attack strategy called eavesdropping channel search, which allows Eve to use its search and eavesdropping capabilities to maximize the probability of successful attacks.
- In order to resist the adversary model, we propose a time slot allocation algorithm to ensure the security of the key.

- Monte Carlo simulation proves that our attack strategy is more powerful than any existing adversary model. At the same time, our proposed time slot allocation algorithm does not have any security loss, which is superior to the existing schemes.

The remainder of this paper is organized as follows. Section 2 describes the methods. Section 3 describes a detailed system model. Section 4 presents the details of our proposed adversary model. Section 5 presents the details of our proposed time slot allocation algorithm. The performance evaluation of the proposed scheme is introduced in Sect. 6. At last, this paper is concluded in Sect. 7.

*Notations:* Italic letters ($A, B, a, b, \ldots$), boldface lower-case letters ($\mathbf{a}, \mathbf{b}, \ldots$) and boldface upper-case letters ($\mathbf{A}, \mathbf{B}, \ldots$) denotes scalars, vectors and matrices, respectively. $(\cdot)^T$ is the transpose. $\circ$ is the Hadamard product. $[\mathbf{a}]_m$ denotes the $m$-th element of vector $\mathbf{a}$. $[\mathbf{A}]_{m,n}$ denotes the $(m, n)$-th element of matrix $\mathbf{A}$. $\mathcal{CN}(\mu, \sigma^2)$ denotes the circularly symmetric complex Gaussian distribution with mean $\mu$ and variance $\sigma^2$. $Re(\cdot)$ is the function of the real part, $Im(\cdot)$ is the function of the imaginary part. $\mathrm{erf}(\cdot)$ is the Gaussian error function. $\mathrm{erfc}^{-1}(\cdot)$ is the inverse complementary error function. $E(\cdot)$ denotes the statistical expectation. $Pr[\cdot]$ represents the probability function. $H(\cdot)$ is the entropy function. $f(\cdot)$ is the probability density function.

## 2 Methods

This article uses PLKG to implement OTP. The security of OTP is a key issue. To ensure the security of our OTP scheme, we first build a powerful adversary model. The adversary model not only has a strong computing power to search, but also can eavesdrop to obtain the relevant channel state information. We give an attack strategy called eavesdropping channel search, which allows Eve to use its search and eavesdropping capabilities to maximize the probability of successful attacks. In order to resist the adversary model, we propose a time slot allocation algorithm to ensure the security of OTP. By increasing the number of channel probes, the probability of the key being breached is reduced. Monte Carlo simulation proves that our attack strategy is more powerful than any existing adversary model. At the same time, our proposed time slot allocation algorithm does not have any security loss, which is superior to the existing schemes.

## 3 System model

In this section, we first give the channel model of this paper and then explain the whole process from channel state information to key generation.

### 3.1 Channel model

Our proposed system consists of legitimate nodes (Alice and Bob), a RIS, and an eavesdropper (Eve), as shown in Fig. 1. All communication nodes are equipped with a single antenna. Key generation works in time-division duplex (TDD) mode. In this system, a RIS equipped with $R$ passive reflecting elements is deployed to enhance the key generation rate so that Alice and Bob can extract a long key and achieve OTP. We assume the RIS is controlled by Alice through a reliable and low delay channel. We consider a passive eavesdropper Eve located around Bob who wants to get the same key as the legitimate nodes based on her own channel observations.

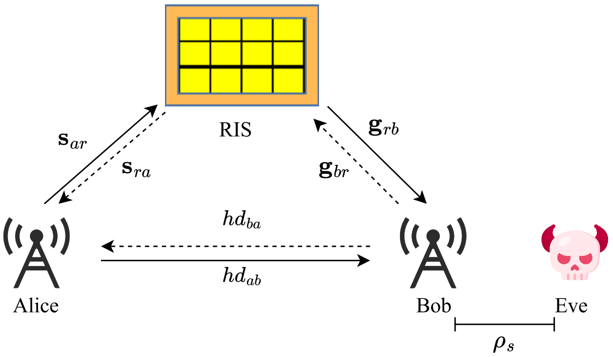

**Fig. 1** System model of a RIS-assisted physical key generation. The system consists of two legitimate nodes (Alice and Bob), a RIS, and an eavesdropper (Eve). $\rho_s$ represents the space correlation coefficient between the legitimate channel and eavesdropping channel. $hd_{uv}(t) \sim \mathcal{CN}(0, \sigma_{hd}^2)$ denotes the direct channel, $\mathbf{s}_{ur}(t) \in \mathbb{C}^{R\times 1}$ denotes the channel from the transmitter $u$ to RIS, $\mathbf{g}_{rv}(t) \in \mathbb{C}^{R\times 1}$ denotes the channel from RIS to the receiver $v$, where $u, v \in \{a, b, e\}$, and $\{a, b, e\}$ denote Alice, Bob and Eve, respectively

We consider a narrow-band and slow-fading channel. The RIS-modified channel from the transmitter $u$ to the receiver $v$ consists of the direct channel and the RIS reflecting channel, where $u, v \in \{a, b, e\}$, and $\{a, b, e\}$ denote Alice, Bob and Eve, respectively. At the $t$-th time instant, the channel from the transmitter $u$ to the receiver $v$ can be expressed as

$$h_{uv}(t) = hd_{uv}(t) + \Phi^T(t)(\mathbf{g}_{rv}(t) \circ \mathbf{s}_{ur}(t)), \tag{1}$$

where $h_{uv}(t) \sim \mathcal{CN}(0, \sigma_h^2)$ denotes the received channel including the direct channel and the reflecting channel, $hd_{uv}(t) \sim \mathcal{CN}(0, \sigma_{hd}^2)$ denotes the direct channel, $\Phi^T(t)(\mathbf{g}_{rv}(t) \circ \mathbf{s}_{ur}(t))$ denotes the reflecting channel, $\mathbf{s}_{ur}(t) \in \mathbb{C}^{R\times 1}$ denotes the channel from the transmitter $u$ to RIS, $\mathbf{g}_{rv}(t) \in \mathbb{C}^{R\times 1}$ denotes the channel from RIS to the receiver $v$, and $\Phi(t) = [\phi_1(t), \ldots, \phi_R(t)]^T$ indicates the reflecting coefficient vector of the RIS where $\phi(t) = e^{j\theta_r(t)}\beta_r(t)$ is the reflecting coefficient of $r$-th element. The range of each passive element is given as $\beta_r(t) \in [0, 1]$ and $\theta_r(t) \in [0, 2\pi]$.

In the slow-fading scenario, there is a time correlation between the two adjacent channel probe values. The time correlation coefficient of the channel gain is given as

$$\rho_t = J_0(2\pi f_d T_s), \tag{2}$$

where $J_0(\cdot)$ is a zeroth-order Bessel function of the first kind, $T_s$ is the sampling period, $f_d$ is the maximum Doppler shift [24]. Allowing for time correlation, channels at the next time instant is given as

$$hd_{ur}(t+1) = \rho_t hd_{ur}(t) + \sqrt{1-\rho_t^2}\,\omega_{hd}, \tag{3}$$

$$\mathbf{s}_{ur}(t+1) = \rho_t \mathbf{s}_{ur}(t) + \sqrt{1-\rho_t^2}\,\omega_s, \tag{4}$$

$$\mathbf{g}_{ur}(t+1) = \rho_t \mathbf{g}_{ur}(t) + \sqrt{1-\rho_t^2}\,\omega_g, \tag{5}$$

where $\omega_{hd} \sim \mathcal{CN}(0, \sigma_{hd}^2)$ is independent of $hd_{ur}(t)$, $\omega_s$ and $\mathbf{s}_{ur}(t)$ are independently and equally distributed, $\omega_g$ and $\mathbf{g}_{ur}(t)$ are equally distributed independently.

Without loss of generality, we only consider the case that Eve eavesdrops on the data transmission from Alice to Bob. The relationship between $h_{ab}(t)$ and $h_{ae}(t, k)$ in the correlated channel model can be presented as

$$h_{ae}(t) = \rho_s h_{ab}(t) + \sqrt{1 - \rho_s^2}\omega_h, \tag{6}$$

where $\omega_h \sim \mathcal{CN}(0, \sigma_h^2)$ is independent of $h_{ab}(t)$, $\rho_s$ represents the space correlation coefficient between the legitimate channel and eavesdropping channel. The space correlation coefficient is given as

$$\rho_s = J_0\left(2\pi \frac{d}{\lambda}\right), \tag{7}$$

where $d$ is the distance between Eve and Bob and $\lambda$ is the length of waveform [20].

Considering the channel reciprocity in the coherent time, we have $hd_{uv} = hd_{vu}$, $\mathbf{g}_{rv} = \mathbf{g}_{vr}$ and $\mathbf{s}_{ur} = \mathbf{s}_{ru}$. Alice configures the $\Phi(t)$ same for every channel bidirectional probing to ensure the reciprocity of the uplink and downlink channels.

## 3.2 Key generation process

As shown in Fig. 2, key generation protocol comprises four stages, namely channel probing, quantization, information reconciliation, privacy amplification. Randomness test (RT) should be carried out before privacy amplification after information reconciliation to ensure that the key can be used.

### *3.2.1 Channel probing*

The received channel can be estimated by sending a public pilot sequence. At the $t$-th time instant, the estimated channel at node $v$ can be expressed as

$$\hat{h}_v(t) = h_{uv}(t) + \varepsilon_v(t), \tag{8}$$

where $\varepsilon_v(t) \sim \mathcal{CN}(0, 2\sigma_n^2/P_u L_P)$ is the channel estimation error by employing zero forcing channel estimation, $P_u$ is the pilot power of the transmitter $u$, $L_P$ is the length of

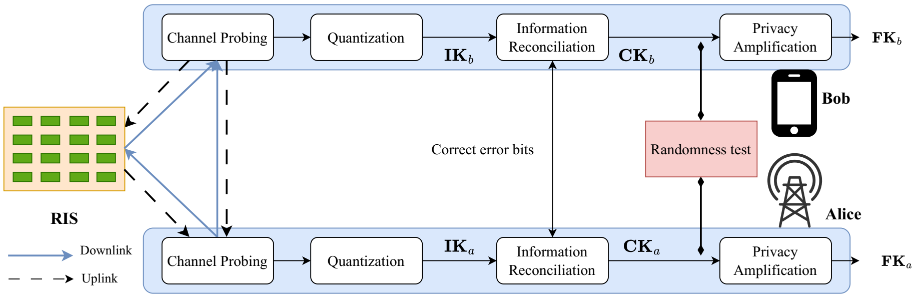

**Fig. 2** Key generation process. Key generation protocol comprises four stages, namely channel probing, quantization, information reconciliation, privacy amplification. Randomness test (RT) should be carried out before privacy amplification after information reconciliation to ensure that the key can be used. $\mathbf{IK}_u$, $\mathbf{CK}_u$ and $\mathbf{FK}_u$ denote the initial key, the common key and the final key, respectively

pilot sequences. $\gamma_v = P_u L_p \sigma_h^2 / \sigma_n^2$ is the normalized signal-to-noise ratio (SNR) of pilot signals.

#### 3.2.2 Quantization

After the channel probing, the communicators put the channel estimate into the quantizer to get the initial key $\mathbf{IK}_u$, where $u \in \{a, b, e\}$. We use a 1-bit quantizer with real part uniform quantization, which is applied in [20, 25] and is expressed as

$$IK_u(t) = \begin{cases} 0, & \text{if} \quad Re(\hat{h}_u(t)) < 0 \\ 1, & \text{others} \end{cases} \tag{9}$$

where $IK_u(t)$ represents the bit quantized by the channel estimate of the $t$-th time.

#### 3.2.3 Information reconciliation

However, it can be seen that due to the noise contained in the two legitimate nodes, the initial key may not be exactly the same and cannot be directly used to encrypt information. Information reconciliation is the final step to correct the inconsistency of the initial key. In this paper, we implement the well-known interactive Cascade protocol [26]. In the information reconciliation process, the legitimate nodes exchange partial information over a public channel, which can be obtained by the eavesdropper.

We denote the bit disagreement ratio (BDR) between $\mathbf{IK}_a$ and $\mathbf{IK}_b$ as $P_{ab}$. Thus, the mutual information [21] of $\mathbf{IK}_a$ and $\mathbf{IK}_b$ can be expressed as

$$I(\mathbf{IK}_a; \mathbf{IK}_b) = H(\mathbf{IK}_a) - H(\mathbf{IK}_a | \mathbf{IK}_b) = L(1 - H(P_{ab})), \tag{10}$$

where $L$ is the length of initial key.

During information reconciliation, Alice and Bob exchange information which can allow Bob to compute the value of $\mathbf{IK}_a$. It follows from the noiseless coding theorem that the minimum amount of information which Alice and Bob need to exchange is $H(\mathbf{IK}_a | \mathbf{IK}_b)$ [27]. However, in a practical implementation of IR, Alice and Bob need exchange more than $H(\mathbf{IK}_a | \mathbf{IK}_b)$ bits of information. This means that legitimate nodes can extract less information than $I(\mathbf{IK}_a; \mathbf{IK}_b)$ when IR succeeds. We assume that Alice and Bob can extract $\beta I(\mathbf{IK}_a; \mathbf{IK}_b)$ bits, where $\beta \in [0, 1]$ is the efficiency of the IR protocol. Thus, the amount of information exchanged can be calculated as

$$L_E = H(\mathbf{IK}_a) - \beta I(\mathbf{IK}_a; \mathbf{IK}_b) = L(1 - \beta + \beta P_{ab}). \tag{11}$$

#### 3.2.4 Randomness test

After information reconciliation, the legitimate nodes obtain the common key **CK** with the same length as the initial key. Next, the common key needs to be tested for randomness to ensure that the generated key has sufficient randomness. A common practice is to adapt the NIST randomness tests to evaluate whether the common key generated from the wireless channel exhibit randomness properties [28]. The common key that passes the randomness test goes to the next step, otherwise it is discarded.

#### *3.2.5 Privacy amplification*

In the process of channel probing, the eavesdropper can obtain the relevant channel information. In the process of information reconciliation, the eavesdropper can obtain the information exchanged on the open letter channel. The information leaked during these two processes puts the key at risk of being cracked by Eve. Thus, Alice and Bob apply the privacy amplification methods to map the results of both nodes to a fixed-length key bit string in order to eliminate part of the information that may be leaked. After privacy amplification, the legitimate nodes get the final key **FK** of length $M$ ($M \leq L$) that can be used for encryption. The common methods used in privacy amplification contain the leftover hash lemma, the cryptographic hash functions, and the Merkle–Damgard hash function [29]. Here, we use the 2-universal hash family which is applied in [30].

## 4 Formal adversary model

In this section, we propose and analyze the adversary model. We first give the hypothesis about the capabilities of the eavesdropper, then analyze the secret bits extracted from the wireless channel, and then give all the possible attack strategies of the eavesdropper, and analyze the success rate of different strategies.

### 4.1 Assumptions about Eve's capabilities

We consider a wireless channel randomness based design scenarios in Sect. 3. We assume that all design specifications and parameters in the wireless key generation process (e.g., bandwidth, carrier frequency, quantization methods and privacy amplification methods) are known to the public. An adversary Eve can hear all communications between Alice and Bob. We assume that Eve can neither actively affect the wireless channel between Alice and Bob, nor modify the content of any communication. We also assume that Eve has a powerful yet finite computational capability. This enables Eve to perform intensive computations to search for the secret between Alice and Bob.

**Definition 1** (Eve's Capabilities):

- Eve and Bob are located close enough to get the CSI correlated with the legitimate channel.
- Eve can get the reconciliation information that Alice and Bob exchanged on the open letter channel.
- Eve has a powerful yet finite computational capability to search for the secret between Alice and Bob.

### 4.2 Analyzing secrets generated from wireless channel

#### *4.2.1 Equivalent channel model*

In order to facilitate the subsequent analysis, we first simplify the channel model. According to the channel model in (1), the received channel consists of a slow-fading direct channel and a reflected channel controlled by a phase shift matrix. By randomly changing the phase shift matrix, the reflecting channel can be regarded as a fast-fading channel with complex Gaussian distribution [18]. Therefore, the receiving channel at the next time instant is simplified as

$$h_{ab}(t+1) = \rho_1\omega_0 + \sqrt{1-{\rho_1}^2}\omega_1, \tag{12}$$

where $\omega_0 = h_{ab}(t)$, $\omega_1 \sim \mathcal{CN}(0, \sigma_h^2)$ is independent of $\omega_0$ and $\rho_1 = \rho_t\sigma_{hd}/\sigma_h$ is the time correlation coefficient of the equivalent channel.

The eavesdropping channel at the current time instant cannot be simplified, but for the sake of symbolic unity and to distinguish it from the expression in Sect. 3, it is reformulated as

$$h_{ae}(t) = \rho_2\omega_0 + \sqrt{1-{\rho_2}^2}\omega_2, \tag{13}$$

where $\rho_2 = \rho_s$ and $\omega_2 \sim \mathcal{CN}(0, \sigma_h^2)$ is independent of $\omega_0$.

Given that the eavesdropping channel at the next time instant $h_{ae}(t+1)$ is both time dependent on $h_{ae}(t)$ and space dependent on $h_{ab}(t+1)$, it can be expressed as

$$h_{ae}^{t+1} = \rho_1\rho_2\omega_0 + \rho_2\sqrt{1-{\rho_1}^2}\omega_1 + \rho_1\sqrt{1-{\rho_2}^2}\omega_2 + \sqrt{1-{\rho_1}^2}\sqrt{1-{\rho_2}^2}\omega_3, \tag{14}$$

where $\omega_3 \sim \mathcal{CN}(0, \sigma_h^2)$ and $\omega_0, \omega_1, \omega_2, \omega_3$ are independent of each other.

#### *4.2.2 Calculation of statistical correlation of the initial key*

Since the measurements from the wireless channel are correlated in time, the initial key generated from the measurements is also statistically correlated. Using this statistical correlation, Eve can effectively increase the probability of a successful attack [19]. In addition, the statistical correlation will be used to calculate the probability of the key passing the randomness test in Sect. 4.4.

The initial key is modeled as a binary correlated sequence with correlation coefficient $\rho_I \in [-1, 1]$ for consecutive bits $IK(t)$ and $IK(t+1)$, which is written as

$$\rho_I = \frac{cov(IK(t), IK(t+1))}{\sigma(IK(t))\sigma(IK(t+1))}, \tag{15}$$

where $cov(IK(t), IK(t+1)) = E((IK(t) - E(IK(t)))(IK(t+1) - E(IK(t+1))))$ is the covariance between $IK(t)$ and $IK(t+1)$, $\sigma(IK(t))$ is the standard deviation of $IK(t)$ and the subscript $u = \{a, b\}$ is dropped for clarity.

Given that $Pr(IK(t) = 0) = Pr(IK(t) = 1) = 1/2$, $E(IK(t)) = 1/2$. Thus, the standard deviation is calculated as

$$\sigma(IK(t)) = \sqrt{E((IK(t) - E(IK(t)))^2)} = \frac{1}{2}, \tag{16}$$

the covariance is calculated as

$$cov(IK(t), IK(t+1)) = E\left(IK(t) - \frac{1}{2}\right)\left(IK(t+1) - \frac{1}{2}\right) = E(IK(t)IK(t+1)) - \frac{1}{4}, \tag{17}$$

where $E(IK(t)IK(t+1))$ is calculated as

$$\begin{aligned}
&E(IK(t)IK(t+1)) = Pr[IK(t)=1, IK(t+1)=1] \\
=&\iint\limits_{D} Pr[Re(\varepsilon(t)) > -s_0, Re(\varepsilon(t+1)) > -\left(\rho_1 s_0 + \sqrt{1-\rho_1{}^2}s_1\right)|Re(\omega_0,\omega_1) = s_0, s_1] \\
=&\frac{1}{8\pi}\iint\limits_{D}[1+\mathrm{erf}\left(\sqrt{\frac{\gamma}{2}}s_0\right)]\left[1+\mathrm{erf}\left(\sqrt{\frac{\gamma}{2}}(\rho_1 s_0 + \sqrt{1-\rho_1{}^2}s_1)\right)\right]\exp\left(-\frac{s_0{}^2+s_1{}^2}{2}\right)ds_1 ds_0,
\end{aligned} \tag{18}$$

where the integral region D is $-\infty < s_0 < +\infty, -\infty < s_1 < +\infty$.

#### 4.2.3 Analysis of the BDR of the legitimate channel

According to (11), the BDR between legitimate communicators affects the amount of information exchanged during the reconciliation phase and thus the amount of information that Eve can obtain. We need to calculate the BDR for subsequent strategy.

We can derive the BDR between Alice and Bob based on [25], which is

$$P_{ab} = \frac{1}{2} - \frac{1}{\sqrt{2\pi}}\int_0^{\infty}\mathrm{erf}\left(\sqrt{\frac{\gamma_a s^2}{2}}\right)\mathrm{erf}\left(\sqrt{\frac{\gamma_b s^2}{2}}\right)\exp\left(\frac{-s^2}{2}\right)\mathrm{d}s. \tag{19}$$

#### 4.2.4 Analysis of the BDR of the eavesdropping channel

Eve and Bob are located close enough to get the CSI associated with the legitimate channel. Eve can use her own CSI to generate the initial key $\mathbf{IK}_e$. Given the proximity of Bob and Eve, it is reasonable to assume that they have the same SNR.

We can derive the BDR between Alice and Eve based on [25], which is

$$P_0 = P_{ae} = \frac{1}{2} - \frac{1}{\sqrt{2\pi}}\int_0^{\infty}\mathrm{erf}\left(\sqrt{\frac{\gamma_b s^2}{2}}\right)\mathrm{erf}\left(\sqrt{\frac{\gamma_a \rho_2{}^2 s^2}{2(\gamma_a - \rho_2{}^2\gamma_a + 1)}}\right)\exp\left(\frac{-s^2}{2}\right)\mathrm{d}s. \tag{20}$$

In fact, due to the effect of time correlation, the BDR of each bit of Alice and Eve is not independent. When $IK_a(t) \neq IK_e(t)$, the probability of $IK_a(t+1) \neq IK_e(t+1)$ is greatly increased. Conversely, if $IK_a(t) = IK_e(t)$, the probability of $IK_a(t+1) \neq IK_e(t+1)$ is greatly decreased [21]. We can calculate the conditional probability based on [21], which is

$$\begin{aligned}
&P_1 = Pr[IK_a(t+1) \neq IK_e(t+1)|IK_a(t) \neq IK_e(t)] \\
=&\frac{Pr[IK_a(t) \neq IK_e(t), IK_a(t+1) \neq IK_e(t+1)]}{Pr[IK_a(t) \neq IK_e(t)]},
\end{aligned} \tag{21}$$

and

$$\begin{aligned}
&Pr[IK_a(t) \neq IK_e(t), IK_a(t+1) \neq IK_e(t+1)] \\
&= \frac{1}{16\pi^2}\int\limits_{-\infty}^{+\infty}\int\limits_{-\infty}^{+\infty}\int\limits_{-\infty}^{+\infty}\int\limits_{-\infty}^{+\infty}[1-\mathrm{erf}_1\mathrm{erf}_2][1-\mathrm{erf}_3\mathrm{erf}_4] \\
&\exp\left(-\frac{s_0{}^2+s_1{}^2+s_2{}^2+s_3{}^2}{2}\right)ds_3 ds_2 ds_1 ds_0,
\end{aligned} \tag{22}$$

where $\mathrm{erf}_1 = \mathrm{erf}(\sqrt{\gamma_a/2}s_0)$, $\mathrm{erf}_2 = \mathrm{erf}(\sqrt{\gamma_b/2}(\rho_2 s_0 + \sqrt{1-\rho_2{}^2}s_2))$, $\mathrm{erf}_3 = \mathrm{erf}(\sqrt{\gamma_a/2}(\rho_1 s_0 + \sqrt{1-\rho_1{}^2}s_1))$, $\mathrm{erf}_4 = \mathrm{erf}(\sqrt{\gamma_b/2}(\rho_1\rho_2 s_0 + \rho_2\sqrt{1-\rho_1{}^2}s_1 + \rho_1\sqrt{1-\rho_2{}^2}s_2 + \sqrt{1-\rho_1{}^2}\sqrt{1-\rho_2{}^2}s_3))$, $s_1, s_2, s_3, s_4$ are the integral variables. Thus, $Pr[IK_a(t+1) = IK_e(t+1)|IK_a(t) \neq IK_e(t)] = 1 - P_1$.

Similarly, $Pr[IK_a(t+1) \neq IK_e(t+1)|IK_a(t) = IK_e(t)] = P_2$ and $Pr[IK_a(t+1) = IK_e(t+1)|IK_a(t) = IK_e(t)] = 1 - P_2$. These conditional probabilities will come into play in the Eve's strategies in Sect. 4.3.

Moreover, according to the Markov chain in Fig. 3, $P_0$, $P_1$, $P_2$ are satisfied

$$P_0 = P_0 P_1 + (1 - P_0)P_2. \tag{23}$$

### 4.3 Eve's strategies

In this section, we give corresponding attack strategy for each link of key generation and propose an attack strategy named eavesdropping channel search (ECS).

The whole process of key generation can be expressed as

$$\hat{\mathbf{h}}_a \rightarrow \mathbf{IK}_a \rightarrow \mathbf{CK}_a \rightarrow \mathbf{FK}_a. \tag{24}$$

As Eve knows the process, there are three straightforward strategies:

#### *4.3.1 Random guess (RG)*

Search for the final key $\mathbf{FK_a}$ in the $\{0,1\}^M$ space. Since the final key is completely random with equal probability distribution, Eve has to rely on random guess to crack it.

#### *4.3.2 Eavesdropping channel search without reconciliation information (ECSwo)*

Search for the initial key $\mathbf{IK_a}$ in the $\{0,1\}^L$ space. Eve uses her own initial key $\mathbf{IK}_e$ without reconciliation information to search for $\mathbf{IK}_a$. According to (20), if the space correlation coefficient is larger than 0, it means that the initial key generated by Eve is more likely to have the same value of the initial key generated by Alice, i.e., $P_0$ should be smaller than 0.5. If the space correlation is smaller than 0, $P_0$ should be larger than 0.5, respectively. This helps Eve because she can search for $\mathbf{IK}_a$ by her own $\mathbf{IK}_e$.

As shown in Fig. 4, when $\rho_2 > 0$, $\mathbf{IK}_e = 01101$ and $\mathbf{IK}_a = 01110$ will be very similar. Eve first tests $\mathbf{IK}_a$ with the original initial key 01101. If the test does not pass, Eve will change a

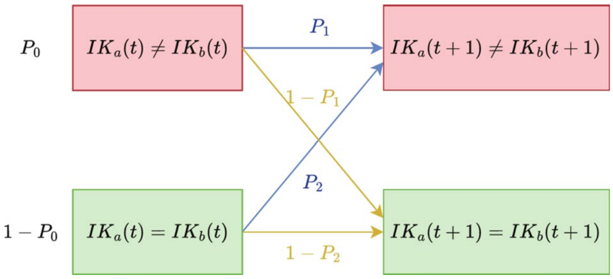

**Fig. 3** The Markov chain of $P_{ae}$. $P_0$ denotes the BDR between Alice and Eve. $P_1 = Pr[IK_a(t+1) \neq IK_e(t+1)|IK_a(t) \neq IK_e(t)]$. $P_2 = Pr[IK_a(t+1) \neq IK_e(t+1)|IK_a(t) = IK_e(t)]$

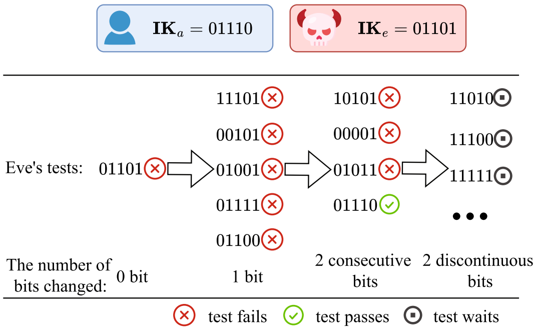

**Fig. 4** The process of Eve's tests when $\rho_2 > 0$. When $\rho_2 > 0$, $\mathbf{IK}_e = 01101$ and $\mathbf{IK}_a = 01110$ will be very similar. Eve first tests $\mathbf{IK}_a$ with the original initial key 01101. If the test does not pass, Eve will change a bit in the $\mathbf{IK}_e$ $(11101, 00101, \ldots)$ and test again. If the test still fails, Eve will change the two bits in the $\mathbf{IK}_e$ $(10101, 00001, \ldots)$ and test again. And so on until the test is passed

bit in the $\mathbf{IK}_e$ $(11101, 00101, \ldots)$ and test again. If the test still fails, Eve will change the two bits in the $\mathbf{IK}_e$ $(10101, 00001, \ldots)$ and test again. And so on until the test is passed.

Furthermore, according to Sect. 4.2.4, when $IK_a(t) \neq IK_e(t)$, the probability of $IK_a(t+1) \neq IK_e(t+1)$ is greatly increased. Therefore, when changing more than one bit, Eve will preferentially change consecutive bits. As shown in Fig. 4, when two bits are changed, Eve will first test $10101, 00001, \ldots$ and then $11010, 11100, \ldots$.

On the contrary, when $\rho_2 < 0$, the BDR between Alice and Eve will be larger than 0.5. Therefore, Eve will first change all of her bits to test. For example, if $\mathbf{IK}_e = 01101$, Eve will first test 10010. If the test fails, Eve will reserve one bit and change the rest of the bits $(00010, 11010, \ldots)$, and then test again. If the test still fails, Eve will reserve the two bits and test again. Similar to when $\rho_2 > 0$, Eve will first reserve consecutive bits when reserving multiple bits.

#### *4.3.3 Eavesdropping channel search with reconciliation information (ECSw)*

Search for the common key $\mathbf{CK_a}$ in the $\{0,1\}^{L-L_E}$ space. Considering that Alice and Bob will leak $L_E$ bits in the information reconciliation phase, this compresses the search space. At this point, Eve's efficiency in using her own initial key $\mathbf{IK}_e$ to search for the common key will be greatly improved.

### 4.4 The attack success probability of Eve

In this section, we will calculate the attack success probability (ASP) for each of Eve's strategies in Sect. 4.3. We use N to represent Eve's search capability. This means that Eve can guess or test the key N times.

#### *4.4.1 The attack success probability of RG*

After privacy amplification, each bit of the final key is randomly distributed with equal probability. This means that Eve has a 1/2 chance of guessing each bit correctly. In addition, the final key is generated, indicating that it has passed the randomness test. Thus, the attack success probability of RG is expressed as

$$Pr[\mathrm{RG}] = \frac{N}{2^M}. \tag{25}$$

#### *4.4.2 The attack success probability of ECSwo*

Since the search is for the initial key, Eve's successful attack requires that the correct initial key is searched and that the key passes the randomness test.

First, we introduce the probability of the generated key passing frequency test in RT [19], which is given as

$$Pr[\mathrm{RT}_{\mathrm{freq}}] = \mathrm{erf}\left( erfc^{-1}(\alpha)\sqrt{\frac{1-|\rho_I|}{1+|\rho_I|}} \right), \tag{26}$$

where $\alpha$ is the P-value threshold in RT, and other modules in RT are defined in [19] Appendix C.

Then, given the fact that RT has been passed, we calculate the attack success probability of ECSwo. Since Eve does not know Alice's CSI, she cannot know the correlation coefficient $\rho_2$ exactly. Thus, Eve need to consider the positive and negative correlation simultaneously. Because Eve cannot know the correlation is positive or not, she needs to search from her original initial key and the initial key in which all bits are changed simultaneously. ECSwo searches for $\mathbf{IK}_a$ from the most likely bit sequence toward the least likely one in $\{0,1\}^L$. Given the fact that RT has been passed, the ECSwo success probability searching for $\mathbf{IK}_a$ is expressed as

$$\begin{aligned}
&Pr[\mathrm{ECSwo}|\mathrm{RT}] = P_{ECS}(L, P_1, P_2) \\
&= \binom{L}{0}(1-P_2)^L + \binom{L}{1}(1-P_2)^{L-2}P_2(1-P_1) + \binom{L-1}{1}(1-P_2)^{L-3}P_2P_1(1-P_1) \\
&+ \left(\binom{L}{2} - \binom{L-1}{1}\right)(1-P_2)^{L-4}P_2^2(1-P_1)^2 + \cdots \\
&+ \binom{L}{0}(P_1)^L + \binom{L}{1}(P_1)^{L-2}(1-P_1)P_2 + \binom{L-1}{1}(P_1)^{L-3}(1-P_1)(1-P_2)P_2 \\
&+ \left(\binom{L}{2} - \binom{L-1}{1}\right)(P_1)^{L-4}(1-P_1)^2P_2^2 + \cdots
\end{aligned} \tag{27}$$

When the time correlation coefficient $\rho_1 = 0$, whether $IK_a(t)$ is equal to $IK_e(t)$ does not affect whether $IK_a(t+1)$ is equal to $IK_e(t+1)$. In this case, $P_0 = P_1 = P_2$ and (27) can be simplified as

$$\begin{aligned}
P_{ECS}(L, P_0, P_0) =& \sum_{i=0}^{n/2} \binom{L}{i} P_0^i(1-P_0)^{L-i} + \sum_{i=0}^{n/2} \binom{L}{i} (1-P_0)^i(P_0)^{L-i} \\
=& I_{P_0}\left(L-\frac{n}{2}, \frac{n}{2}+1\right) + I_{1-P_0}\left(L-\frac{n}{2}, \frac{n}{2}+1\right),
\end{aligned} \tag{28}$$

where $I_x(a,b)$ is the regularized incomplete beta function and $n$ satisfies

$$N = \sum_{i=0}^{n/2} \binom{L}{i} + \sum_{j=0}^{n/2} \binom{L}{j}. \tag{29}$$

As a result, the attack success probability of ECSwo is calculated as

$$Pr[\text{ECSwo}] = Pr[\text{ECSwo}|\text{RT}] \cdot Pr[\text{RT}]. \tag{30}$$

#### 4.4.3 The attack success probability of ECSw

Like ECSwo, ECSw uses the same search method, but ECSw uses reconciliation information to compress the search space. Thus, the attack success probability of ECSw is calculated as

$$Pr[\text{ECSw}] = Pr[\text{ECSw}|\text{RT}] \cdot Pr[\text{RT}], \tag{31}$$

where $Pr[\text{ECSw}|\text{RT}] = P_{ECS}(L', P_1, P_2)$ and $L' = L - L_E$.

Because the search space of ECSw is smaller than that of ECSwo, the success probability of ECSw is higher than that of ECSwo.

## 5 The proposed OTP scheme

In this section, we propose a time slot allocation algorithm in the OTP against the adversary model. We first analyze the defense strategy against Eve. Then, we propose a three-stage OTP scheme. Finally, we propose a time slot allocation algorithm to ensure the security of the key.

### 5.1 The defense strategy against Eve

We assume that legitimate communicators cannot restrict Eve's search capability. In addition, we assume that the length of the final key will not change, because the commonly used encryption keys are 128 bits or 256 bits.

For RG, since neither $N$ nor $M$ can be changed, the probability of success of RG is fixed. This means that Eve has at least a probability of $Pr[\text{RG}]$ attack success. For ECSwo, in order to reduce $Pr[\text{ECSwo}]$, Alice can increase the number of channel probing to increase the initial key length $L$. In addition, Alice can reduce the time correlation by increasing the sampling period or using RIS. For ECSw, in addition to the above strategy, Alice can also reduce the BDR of Alice and Bob by increasing the signal power to reduce the information leakage during the information reconciliation. However, increasing signal power also allows Eve to gain more relevant CSI to Alice, which in turn increases $Pr[\text{ECSw}]$. Based on the above analysis, the most effective strategy is to increase the number of channel probing, that is, to increase the length of the initial key $L$.

With the increase of $L$, the probability that the key is successfully attacked by ECSw and ECSwo decreases. However, when $L$ is too large, it will greatly reduce the efficiency of key generation, which may cause Alice to have no key available for a period of time. So we need to set $L$ to an appropriate size. Given that Eve has at least a probability of $Pr[\text{RG}]$ attack success, we just need to set L to satisfy

$$Pr[\text{ECSw}] \leq Pr[\text{RG}]. \tag{32}$$

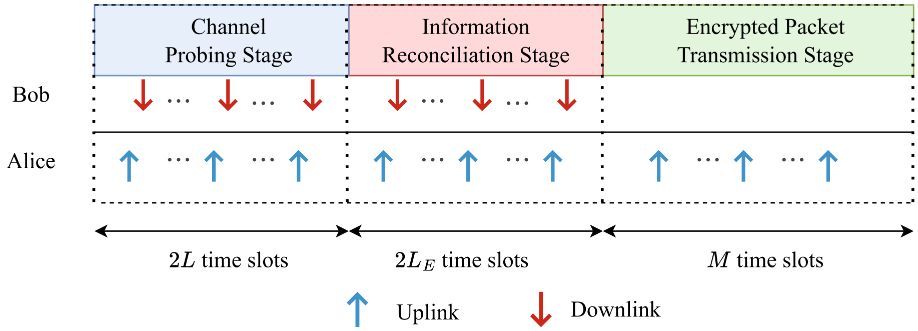

**Fig. 5** Time slot allocation for three-stage OTP scheme. Our proposed scheme consists of three stages: channel probing, information reconciliation and encrypted packet transmission

### 5.2 Three-stage OTP scheme

Our proposed scheme consists of three stages: channel probing, information reconciliation and encrypted packet transmission in Fig. 5. We assume that Alice and Bob have performed two-way authentication before generating the physical layer key.

In Stage 1, Alice and Bob probe the channel $L$ times, which occupies total $2L$ time slots. In Stage 2, Alice and Bob send the parity checks to realize information reconciliation. According to (11), Alice and Bob send reconciliation information $L_E$ times, which occupies total $2L_E$ time slots. In Stage 3, Alice or Bob uses the remaining time slots to transmit the encrypted data. Each time slot transmits 1 bit of encrypted data. Because OTP needs to be given a key of the same length as the message, the length of the encrypted data is the same as that of the final key. Therefore, Alice or Bob spends $M$ time slots to transmit the encrypted information.

### 5.3 Time slot allocation algorithm

Our time slot allocation algorithm will follow the guideline that guarantees both enough security strength and high efficiency. We want the total time slot from key generation to encrypted transmission to be minimal, while ensuring security. Thus, we can formulate the time slot allocation as the following problem:

$$\min_{L} 2L + 2L_E + M \tag{33a}$$

$$\text{s.t. } Pr[\text{ECSw}] \le Pr[\text{RG}], \tag{33b}$$

$$Pr[\text{ECSw}] = Pr[\text{ECSw}|\text{RT}] \cdot Pr[\text{RT}], \tag{33c}$$

$$Pr[\text{ECSw}|\text{RT}] = P_{ECS}(L - L_E, P_1, P_2), \tag{33d}$$

$$L_E = L(1 - \beta + \beta P_{ab}). \tag{33e}$$

**Algorithm 1** Proposed optimal time slot allocation algorithm.

```
Set $L_0 = M$ and $loop = 1$.
while $loop <$ max number of loop && $Pr[\mathrm{ECSw}] \leq Pr[\mathrm{RG}]$ do
    $L_{loop} = L_{loop-1} - \frac{Pr[\mathrm{ECSw}] - Pr[\mathrm{RG}]}{\frac{\partial Pr[\mathrm{ECSw}]}{\partial L}}$
    Update $loop = loop + 1$.
end while
Obtain $L_{opt}$.
```

In (33a), the objective function is the number of total time slots. (33b) is for security constraint. Variables used in the security constraint are given in (33c), (33d) and (33e).

According to (33b) and (33e), $L$ is positively correlated with $L_e$, and $L$ is negatively correlated with $Pr$[ECSw]. Thus, the problem formulation of (33) is to find the minimum value of $L$ under the security constraint. And we can solve it by Algorithm 1.

## 6 Results and discussion

In this section, numerical results are given to illustrate the effectiveness of the proposed attack strategy and the security of the proposed OTP scheme.

### 6.1 Set up

We consider an RIS-assisted wireless system. Unless otherwise stated, the experimental parameters are set in this section.

A RIS, equipped with $M = 16$ elements, is deployed between Alice and Bob. The signal power of the direct channel is equal to the signal power of the reflecting channel.

The attacker Eve aims to obtain the secret key through ECS with reconciliation information. Given that a realistically powerful capability for Eve is $2^{63.1}$ [31], we consider a powerful capability of Eve with $N = 2^{64}$ such that the attack success probability of cracking a 128-bit key by random guess is $2^{-64}$.

For ease of analysis, we assume that $\gamma_a = \gamma_b = \gamma_e = 20$ dB. The length of the final key is set to $M = 128$ and the length of the initial key is set to $L = 180$. The time correlation coefficient is set to $\rho_t = 0.4$ and the space correlation coefficient is set to $\rho_s = 0.5$. Thus, $\rho_1 = 0.2$ and $\rho_2 = 0.5$. The efficiency of the IR protocol is set to $\beta = 0.9$. The P-value threshold in RT is set to $\alpha = 0.01$ [11].

### 6.2 Benchmark schemes

#### *6.2.1 Benchmarks for attack strategies*

Four benchmarks are as follows, and their ASPs are calculated in Appendix A.

**(1) Maximum-Likelihood tree search without reconciliation information (MLTSwo)**: Eve uses the statistical correlation to search for the initial key without reconciliation information, which is applied in [17, 19]. Statistical correlation results in the probability of the initial key not being completely random, and Eve can search for the initial key in order of probability from maximum to minimum.

**(2) Maximum-Likelihood tree search with reconciliation information (MLTSw)**: Eve uses the statistical correlation to search for the common key without reconciliation information. Considering that Alice and Bob will leak some bits in the information reconciliation phase, this compresses the search space. At this point, Eve's efficiency in using statistical correlation to search for the common key will be greatly improved.

**(3) Eavesdropping channel attack without reconciliation information(EAwo)**: Eve uses her own CSI to crack the key but does not search, which is applied in [20, 21]

**(4) Eavesdropping channel attack with reconciliation information(EAw)** Eve uses reconciliation information to get some bits, and uses her own CSI to crack the rest.

#### *6.2.2 Benchmarks for time slot allocation*

Four benchmarks based on RIS are present:

**(1)** [17]**'s scheme**: This case is to protect the key against MLTSwo attack.

**(2)** [18]**'s scheme**: This case is to maximize the transmission rate.

**(3)** [22]**'s scheme**: This case is to maximizes the minimum secret key capacity for the worst-case eavesdropper channel.

**(4)** [32]**'s scheme**: This case is to maximizes key generation rate.

### 6.3 Metrics

The performance of the attack strategy is evaluated by the attack success probability (ASP). The performance of the OTP scheme is evaluated by the security loss (SL).

**(1) The attack success probability**: The ASP refers to the probability of cracking a key using a certain attack strategy. A higher ASP indicates that the attack strategy is more threatening and effective.

**(2) The security loss**: The SL describes the loss of security during key generation [19]. The SL is calculated as

$$\mathrm{SL} = \log_2 \frac{Pr[\text{Eve succeeds}]}{Pr[\text{RG}]}, \tag{34}$$

where $Pr[\text{Eve succeeds}]$ is the maximum probability that Eve will break the key by any attack strategies. If SL=0, the ASP without any attack strategies will be higher than the ASP of RG, which means that there is no security loss. If SL>0, this indicates that there is a strategy that can crack the key more efficiently than RG. The smaller the SL, the more secure the key generation process is.

### 6.4 Results

#### *6.4.1 Evaluation of ASP*

We evaluate the ASP of the attack strategies against the length of the initial key, the time correlation coefficient of the equivalent channel, the space correlation coefficient of the equivalent channel and the SNR.

Figure 6 illustrates the ASP versus the length of the initial key $L$. From this figure, we can clearly observe that the ASP of all schemes except RG decreases with the increase of the $L$. This is because as $L$ increases, the search space for these schemes becomes larger. This verifies the correctness of our proposed OTP scheme. However, the search space of RG scheme is always $2^M$, so the ASP of RG does not change. Our proposed OTP scheme is to find the smallest $L$ to satisfy that the ASP of ECSw is smaller than the ASP of RG. In addition, the ASP of our proposed ECS strategy is always larger than that of MLTS

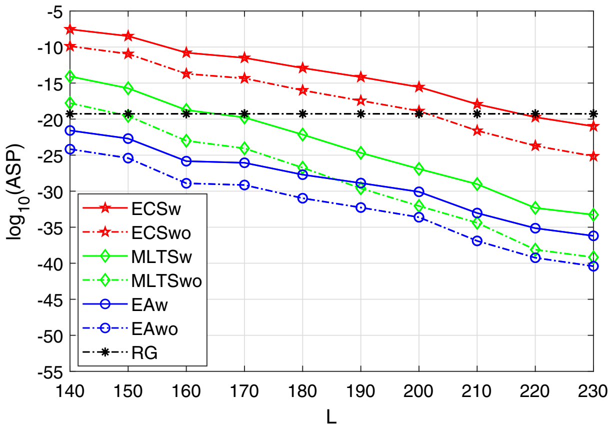

**Fig. 6** ASP versus *L*. We present the ASP of our and benchmarks' attack strategies versus the length of the initial key *L*. We can clearly observe that the ASP of all schemes except RG decreases with the increase of the *L*. In addition, the ASP of our proposed ECS strategy is always larger than that of MLTS strategy and EA strategy. This illustrates the effectiveness of our proposed attack strategy

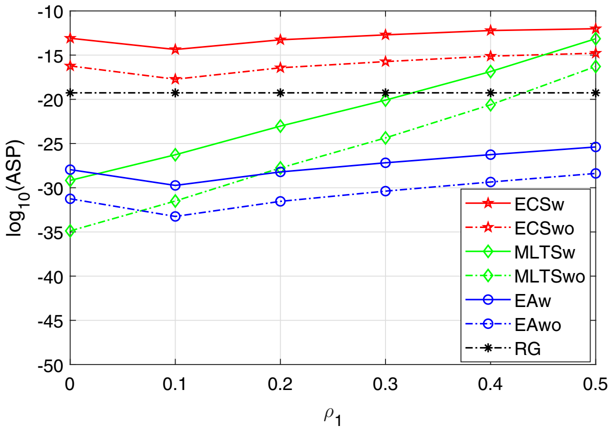

**Fig. 7** ASP versus $\rho_1$. We present the ASP of our and benchmarks' attack strategies versus the $\rho_1$. We find that the ASP of all schemes except RG generally increases with the increase of $\rho_1$. The ASP of our proposed ECS strategy is larger than that of MLTS strategy and EA strategy. This means that in a slow-fading environment, the key is more vulnerable to attack

strategy and EA strategy. At the same time, we can also see that the use of leaked reconciliation information can effectively compress the search space and improve ASP.

In Fig. 7, we present the impact of the $\rho_1$. We find that the ASP of all schemes except RG generally increases with the increase of $\rho_1$. The MLTS strategy is the most affected because it only exploits $\rho_1$ for attacks. When $\rho_1 = 0$, the MLTS strategy is even worse than the RG strategy because in this case the MLTS strategy is completely a random guess and the search space for the MLTS strategy is larger. In addition, when $\rho_1$ changes from 0 to 0.1, the ASP of ECS and EA has an abnormal decline. This is because the probability of the initial key passing RT is reduced. In addition, the ASP of our proposed ECS strategy is larger than that of MLTS strategy and EA strategy.

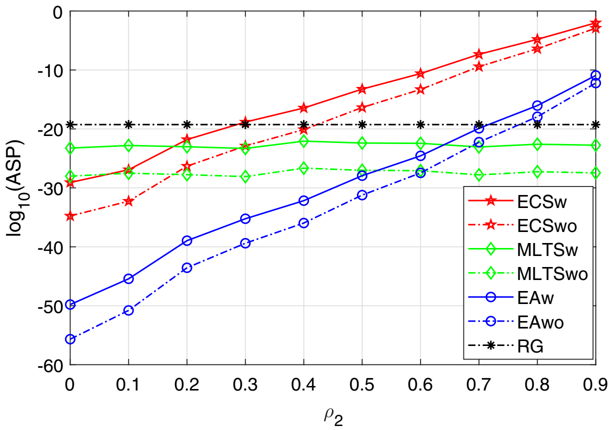

**Fig. 8** ASP versus $\rho_2$. We present the ASP of our and benchmarks' attack strategies versus the $\rho_2$. We find that the ASP of ECS and EA increases with the increase of $\rho_2$. When $\rho_2 \geq 0.2$, ECS strategy is superior to MLTS strategy. This means that even if Eve and Alice have only a small correlation, our proposed attack strategy is superior to the others

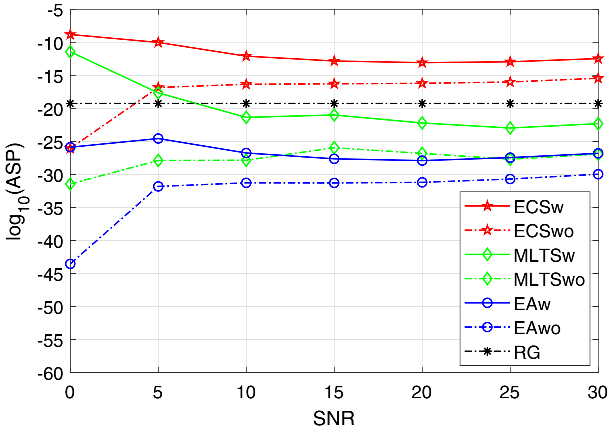

**Fig. 9** ASP versus SNR. We present the ASP of our and benchmarks' attack strategies versus the SNR. The ASP of our proposed ECS strategy is always larger than that of MLTS strategy and EA strategy. When SNR changes from 0 dB to 15 dB, the ASP of the strategies those use leaked reconciliation information decreases, but the ASP of the strategies those do not use leaked reconciliation information increases. As SNR increases further, the ASP of each strategy tends to stabilize

Figure 8 presents the influence of the $\rho_2$. We find that the ASP of ECS and EA increases with the increase of $\rho_2$. This is because the larger $\rho_2$, the more similar the CSI of Eve and Alice will be, and the greater the probability that the initial keys generated will be the same. When $\rho_2 \geq 0.2$, ECS strategy is superior to MLTS strategy. This means that even if Eve and Alice have only a small correlation, our proposed attack strategy is superior to the others.

In Fig. 9, we illustrate the performance of the ASP with different SNR. The ASP of our proposed ECS strategy is always larger than that of MLTS strategy and EA

**Table 1** Comparison of our time slot allocation algorithm with some other schemes

| | $\rho_1 = 0.25, \rho_2 = 0.3$ | | | $\rho_1 = 0.25, \rho_2 = 0.5$ | | |
|---|---|---|---|---|---|---|
| **Ref.** | $L$ | $2L + 2L_E + M$ | **SL** | $L$ | $2L + 2L_E + M$ | **SL** |
| Our | 182 | 2*182+2*19+128 | 0 | 222 | 2*222+2*23+128 | 0 |
| [17] | 164 | 2*164+2*17+128 | 3.64 | 164 | 2*164+2*17+128 | 8.65 |
| [18] | 173 | 2*173+2*18+128 | 2.09 | 173 | 2*173+2*18+128 | 7.19 |
| [22] | 174 | 2*174+2*18+128 | 1.70 | 174 | 2*174+2*18+128 | 7.14 |
| [32] | 177 | 2*177+2*19+128 | 1.40 | 177 | 2*177+2*19+128 | 5.64 |

strategy. When SNR changes from 0 dB to 15 dB, the ASP of the strategies those use leaked reconciliation information decreases, but the ASP of the strategies those do not use leaked reconciliation information increases. This is because $P_{ab}$ is reduced, less reconciliation information is leaked, and the search space is larger. At the same time, $P_{ae}$ decreases, and the probability of single search success increases. As SNR increases further, the ASP of each strategy tends to stabilize, because the $P_{ab}$ and $P_{ae}$ change little at this time.

#### *6.4.2 Evaluation of LS*

We evaluate the security loss of our and other time slot allocation schemes. Table 1 shows the number of channel probing and the number of information reconciliation required by our algorithm with no security risk compared to other schemes. The length of both final key and ciphertext is set to 128 bits, so the time slots occupied by encrypted packet transmission is 128. Our algorithm has no security loss against any of the listed attacks in Sect. 4.3 and 6.2.1, whereas the others have varying degrees of security loss. In addition, when $\rho_2$ changes from 0.3 to 0.5, the SL of benchmark schemes increases significantly. This means that in cases where Eve has access to the relevant CSI, the benchmark schemes have a greater security loss.

### 6.5 Discussion

This paper mainly designs a powerful adversary model and proposes an OTP scheme to counter this model. We found that Eve, after obtaining a CSI correlated with the legitimate channel, can generate a key similar to that of a legitimate communicator. And in a slow-changing environment, Eve is more likely to continuously guess the key. Based on this, we designed Eve's attack strategy and calculated the probability of success. Compared with the adversary model in [17, 19–21], our adversary model has a higher attack success probability. In addition, we designed an OTP scheme to counter our adversary model. Compared with the OTP scheme in [17, 18, 22, 32], our OTP has no security loss.

However, the OTP scheme in this paper needs to know the specific correlation of the eavesdropping channel. How to obtain the correlation is not considered in this paper, but it can be solved by radar sensing and other methods.

## 7 Conclusion

In this paper, we propose a very powerful adversary model. We assume that Eve has a powerful yet finite computational capability and Eve can get the reconciliation information and the CSI correlated with the legitimate channel. We give an attack strategy called eavesdropping channel search, which allows Eve to use its search and eavesdropping capabilities to maximize the probability of successful attacks. Meanwhile, we propose a time slot allocation algorithm in the OTP against the adversary model. Simulations validate that our proposed attack strategy is more powerful than any existing adversary model and our proposed time slot allocation algorithm does not have any security loss.

## Appendix A The ASP of benchmarks

### A.1 The attack success probability of MLTSwo

Since the search is for the initial key, Eve's successful attack requires that the correct initial key is searched and that the key passes the randomness test. According to [19], given the fact that RT has been passed, the attack success probability of MLTSwo can be expressed as

$$\begin{aligned} &Pr[\text{MLTSwo}|\ \text{RT}]\\ =&I_{\frac{1-\rho_I}{2}}\left(L-\frac{n}{2},\frac{n}{2}+1\right)+I_{\frac{1+\rho_I}{2}}\left(L-\frac{n}{2},\frac{n}{2}+1\right), \end{aligned} \tag{A1}$$

where $I_x(a,b)$ is the regularized incomplete beta function and $n$ satisfies (29).

### A.2 The attack success probability of MLTSw

Like MLTSwo, MLTSw uses the same search method, but MLTSw uses reconciliation information to compress the search space. Given the fact that RT has been passed, the attack success probability of MLTSw is calculated as

$$\begin{aligned} &Pr[\text{MLTSw}|\ \text{RT}]\\ =&I_{\frac{1-\rho_I}{2}}\left(L'-\frac{n}{2},\frac{n}{2}+1\right)+I_{\frac{1+\rho_I}{2}}\left(L'-\frac{n}{2},\frac{n}{2}+1\right). \end{aligned} \tag{A2}$$

### A.3 The attack success probability of EAwo

Eve uses her own initial key to crack the key. Given the fact that RT has been passed, the attack success probability of EAwo is calculated as

$$Pr[\text{EAwo}|\text{RT}]=(1-P_2)^L. \tag{A3}$$

### A.4 The attack success probability of EAw

Like EAwo, EAw uses the same search method, but EAw uses reconciliation information to compress the search space. Given the fact that RT has been passed, the attack success probability of EAw is calculated as

$$Pr[\text{EAw}|\ \text{RT}]=(1-P_2)^{L'}. \tag{A4}$$

### Abbreviations

| | |
|---|---|
| IoT | Internet of Things |
| PLKG | Physical layer key generation |
| OTP | One time pad |
| RIS | Reconfigurable intelligent surface |
| CSI | Channel state information |
| RT | Randomness test |
| TDD | Time-division duplex |
| SNR | Signal-to-noise ratio |
| BDR | Bit disagreement ratio |
| ECS | Eavesdropping channel search |
| RG | Random guess |
| ECSwo | Eavesdropping channel search without reconciliation information |
| ECSw | Eavesdropping channel search with reconciliation information |
| ASP | Attack success probability |
| SL | Security loss |
| MLTSwo | Maximum-likelihood tree search without reconciliation information |
| MLTSw | Maximum-likelihood tree search with reconciliation information |
| EAwo | Eavesdropping channel attack without reconciliation information |
| EAw | Eavesdropping channel attack with reconciliation information |

**Acknowledgements**
Not applicable.

### Author contributions
All authors contributed to this work and approved the final manuscript.

**Funding**
This work is supported by National Natural Science Foundation of China (No.U22B2026).

### Data availability
The datasets used during the current study are available from the corresponding author on reasonable request.

## Declarations

### Ethics approval and consent to participate
Not applicable.

### Consent for publication
Not applicable.

### Competing interests
The authors have no competing interests to declare.

Received: 15 March 2024 Accepted: 28 June 2024
Published online: 11 July 2024

### References

1. G. Li, C. Sun, W. Xu, M.D. Renzo, A. Hu, On maximizing the sum secret key rate for reconfigurable intelligent surface-assisted multiuser systems. IEEE Trans. Inf. Forensics Secur. **17**, 211–225 (2022). https://doi.org/10.1109/TIFS.2021.3138612
2. Y. Chen, Z. Chen, Y. Zhang, Z. Luo, Y. Li, B. Xing, B. Guo, L. Chen, Physical layer key generation scheme for MIMO system based on feature fusion autoencoder. IEEE Internet Things J. **10**(16), 14886–14895 (2023). https://doi.org/10.1109/JIOT.2023.3288641
3. M. Ylianttila, R. Kantola, A. Gurtov, L. Mucchi, I. Oppermann, Z. Yan, T.H. Nguyen, F. Liu, T. Hewa, M. Liyanage, A. Ijaz, J. Partala, R. Abbas, A. Hecker, S. Jayousi, A. Martinelli, S. Caputo, J. Bechtold, I. Morales, A. Stoica, G. Abreu, S. Shahabuddin, E. Panayirci, H. Haas, T. Kumar, B.O. Ozparlak, J. Röning, 6G White paper: Research challenges for Trust. Security and Privacy (2020)
4. U.M. Maurer, Secret key agreement by public discussion from common information. IEEE Trans. Inf. Theory **39**(3), 733–742 (1993). https://doi.org/10.1109/18.256484
5. J. Zhang, G. Li, A. Marshall, A. Hu, L. Hanzo, A new frontier for IoT security emerging from three decades of key generation relying on wireless channels. IEEE Access **8**, 138406–138446 (2020). https://doi.org/10.1109/ACCESS.2020.3012006
6. J. Zhang, A. Marshall, R. Woods, T.Q. Duong, Efficient key generation by exploiting randomness from channel responses of individual OFDM subcarriers. IEEE Trans. Commun. **64**(6), 2578–2588 (2016). https://doi.org/10.1109/TCOMM.2016.2552165
7. G. Li, Z. Zhang, J. Zhang, A. Hu, Encrypting wireless communications on the fly using one-time pad and key generation. IEEE Internet Things J. **8**(1), 357–369 (2021). https://doi.org/10.1109/JIOT.2020.3004451

8. C.E. Shannon, Communication theory of secrecy systems. The Bell Syst. Tech. J. **28**(4), 656–715 (1949). https://doi.org/10.1002/j.1538-7305.1949.tb00928.x
9. J. Jiao, L. Chen, Stochastic perturbation-based physical-layer secret key generation in quasi-static scene. In: 2021 7th International Conference on Computer and Communications (ICCC), pp. 544–548 (2021). https://doi.org/10.1109/ICCC54389.2021.9674489
10. L. Hu, Y. Chen, G. Li, A. Hu, Exploiting artificial randomness for fast secret key generation in quasi-static environments. In: 2021 IEEE 6th International Conference on Signal and Image Processing (ICSIP), pp. 985–989. (2021) https://doi.org/10.1109/ICSIP52628.2021.9688810
11. T. Lu, L. Chen, J. Zhang, C. Chen, A. Hu, Joint precoding and phase shift design in reconfigurable intelligent surfaces-assisted secret key generation. IEEE Trans. Inf. Forensics Secur. **18**, 3251–3266 (2023). https://doi.org/10.1109/TIFS.2023.3268881
12. L. Jiao, G. Sun, J. Le, K. Zeng, Machine learning-assisted wireless PHY key generation with reconfigurable intelligent surfaces. In: Proceedings of the 3rd ACM Workshop on Wireless Security and Machine Learning. WiseML '21, pp. 61–66. Association for Computing Machinery, New York, NY, USA (2021). https://doi.org/10.1145/3468218.3469042
13. V. Shahiri, H. Behroozi, A. Kuhestani, K.-K. Wong, Reconfigurable intelligent surface-assisted secret key generation under spatially correlated channels in quasi-static environments. IEEE Internet of Things Journal, 1–1 (2024) https://doi.org/10.1109/JIOT.2023.3349354
14. Z.-M. Jiang, M. Rihan, P. Zhang, L. Huang, Q. Deng, J. Zhang, E.M. Mohamed, Intelligent reflecting surface aided dual-function radar and communication system. IEEE Syst. J. **16**(1), 475–486 (2022). https://doi.org/10.1109/JSYST.2021.3057400
15. M.D. Renzo, M. Debbah, D.-T. Phan-Huy, A. Zappone, M.-S. Alouini, C. Yuen, V. Sciancalepore, G.C. Alexandropoulos, J. Hoydis, H. Gacanin, Smart radio environments empowered by reconfigurable AI meta-surfaces: an idea whose time has come. EURASIP J. Wirel. Commun. Netw. **2019**(1), 1–20 (2019)
16. Y. Song, L. Chen, W. Ma, T. Lu, P. Zhang, Time slot allocation for RIS-assisted physical layer key generation in OTP. In: 2023 IEEE 98th Vehicular Technology Conference (VTC2023-Fall), pp. 1–5 (2023). https://doi.org/10.1109/VTC2023-Fall60731.2023.10333784
17. L. Chen, K. Cao, T. Lu, Y. Lu, A. Hu, A one-time pad encryption scheme based on efficient physical-layer secret key generation for intelligent IoT system. China Commun. **19**(7), 185–196 (2022)
18. Z. Ji, P.L. Yeoh, G. Chen, C. Pan, Y. Zhang, Z. He, H. Yin, Y. Li, Random shifting intelligent reflecting surface for OTP encrypted data transmission. IEEE Wirel. Commun. Lett. **10**(6), 1192–1196 (2021). https://doi.org/10.1109/LWC.2021.3061549
19. Z. Qu, S. Zhao, J. Xu, Z. Lu, Y. Liu, How to test the randomness from the wireless channel for security? IEEE Trans. Inf. Forensics Secur. **16**, 3753–3766 (2021)
20. L. Jin, X. Hu, X. Sun, Y. Lou, K. Huang, Z. Zhong, X. Xu, Native security scheme based on physical layer chain key for encryption and authentication. In: 2021 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), pp. 1–7 (2021). IEEE
21. L. Chen, Y. Song, T. Lu, P. Zhang, Machine learning assisted physical layer secret key generation in the one-time-pad encryption scheme. In: Proceedings of the 2023 ACM Workshop on Wireless Security and Machine Learning. WiseML'23, pp. 45–50. Association for Computing Machinery, New York, NY, USA (2023)
22. Z. Ji, P.L. Yeoh, D. Zhang, G. Chen, Y. Zhang, Z. He, H. Yin, Y. li, Secret key generation for intelligent reflecting surface assisted wireless communication networks. IEEE Trans. Veh. Technol. **70**(1), 1030–1034 (2021) https://doi.org/10.1109/TVT.2020.3045728
23. X. Gu, W. Duan, G. Zhang, Q. Sun, M. Wen, P.-H. Ho, Physical layer security for RIS-aided wireless communications with uncertain eavesdropper distributions. IEEE Syst. J. **17**(1), 848–859 (2023). https://doi.org/10.1109/JSYST.2022.3153932
24. J. Zhang, B. He, T.Q. Duong, R. Woods, On the key generation from correlated wireless channels. IEEE Commun. Lett. **21**(4), 961–964 (2017)
25. X. Hu, L. Jin, K. Huang, K. Ma, C. Song, S. Xiao, A secure communication scheme based on equivalent interference channel assisted by physical layer secret keys. Secur. Commun. Netw. **2020**, 1–15 (2020)
26. G. Brassard, L. Salvail, Secret-key reconciliation by public discussion, in *Advances in Cryptology – EUROCRYPT '93*. ed. by T. Helleseth (Springer, Berlin, Heidelberg, 1994), pp.410–423
27. T.B. Pedersen, M. Toyran, High performance information reconciliation for QKD with CASCADE (2013)
28. L.E. Bassham III, A.L. Rukhin, J. Soto, J.R. Nechvatal, M.E. Smid, E.B. Barker, S.D. Leigh, M. Levenson, M. Vangel, D.L. Banks, et al.: Sp 800-22 rev. 1a. a statistical test suite for random and pseudorandom number generators for cryptographic applications. National Institute of Standards & Technology (2010)
29. A. Dey, S. Nandi, M. Sarkar, Security measures in IoT based 5G networks. In: 2018 3rd International Conference on Inventive Computation Technologies (ICICT), pp. 561–566 (2018). https://doi.org/10.1109/ICICT43934.2018.9034365
30. S. Jana, S.N. Premnath, M. Clark, S.K. Kasera, N. Patwari, S.V. Krishnamurthy, On the effectiveness of secret key extraction from wireless signal strength in real environments. In: Proceedings of the 15th Annual International Conference on Mobile Computing and Networking. MobiCom '09, pp. 321–332. Association for Computing Machinery, New York, NY, USA (2009)
31. M. Stevens, E. Bursztein, P. Karpman, A. Albertini, Y. Markov, The first collision for full sha-1, in *Advances in Cryptology - CRYPTO 2017*. ed. by J. Katz, H. Shacham (Springer, Cham, 2017), pp.570–596
32. Y. Liu, M. Wang, J. Xu, S. Gong, D.T. Hoang, D. Niyato, Boosting secret key generation for irs-assisted symbiotic radio communications. In: 2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring), pp. 1–6 (2021). https://doi.org/10.1109/VTC2021-Spring51267.2021.9448719

## Publisher's Note