electronics

MDPI

Review

A Survey of Physical Layer Secret Key Generation Enhanced by Intelligent Reflecting Surface

Enjun Xia, Bin-Jie Hu * and Qiaoqiao Shen

School of Electronic and Information Engineering, South China University of Technology, Guangzhou 510641, China; 201810102017@mail.scut.edu.cn (E.X.); 201910101872@mail.scut.edu.cn (Q.S.)
* Correspondence: eebjiehu@scut.edu.cn

Abstract: As wireless communication scenarios grow more complicated, security issues are becoming increasingly prominent and severe. In the Internet of Things and vehicle-to-everything scenarios, conventional cryptographic technology faces numerous challenges. These include difficulties in secret key distribution and management, low update rates of secret keys, and vulnerability to quantum attacks. Physical layer secret key generation is considered a promising solution to security issues. The perfect secrecy proposed by Shannon can be achieved by combining secret key generation and the one-time pad when the length of secret keys is equal to that of plaintext. Hence, it is important to increase secret key generation rates. Intelligent reflecting surfaces demonstrate great advantages in improving the secret key generation performance. This paper provides a comprehensive review of current research efforts related to secret key generation assisted by intelligent reflecting surfaces, which is divided into three main categories: introducing the randomness of intelligent reflecting surfaces, optimizing the reflecting coefficients, and designing probing protocols. Comparative results of existing optimization approaches are provided and discussed. Furthermore, we emphasize the significance of selecting a random source of secret key generation from the perspective of information theory. Finally, two significant application scenarios, the Industrial Internet of Things and vehicle-to-everything, are discussed, and some challenges and opportunities are presented.

Keywords: physical layer secret key generation; intelligent reflecting surfaces; optimization; communication security

Citation: Xia, E.; Hu, B.-J.; Shen, Q. A Survey of Physical Layer Secret Key Generation Enhanced by Intelligent Reflecting Surface. *Electronics* **2024**, *13*, 258. https://doi.org/10.3390/electronics13020258

Academic Editor: Hung-Yu Chien

Received: 14 November 2023
Revised: 20 December 2023
Accepted: 4 January 2024
Published: 5 January 2024

1. Introduction

From the first-generation (1G) to fifth-generation (5G) mobile communication systems, there has been continuous improvement in system performance in terms of coverage, data rates, connections, and latency. Meanwhile, the security problems of communication systems are becoming increasingly serious. The sixth-generation (6G) mobile communication system faces more security risks and potential attacks [1,2]. Therefore, 6G requires stronger security mechanisms. Classical cryptography has gone from an art to a science since the 1980s. The field of cryptography is becoming more and more widespread, encompassing secret communications, message authentication, digital signatures, protocols for exchanging secret keys, authentication protocols, and more. Symmetric encryption and decryption algorithms, along with asymmetric encryption and decryption algorithms, are the cornerstone of modern security systems [3]. The premise of classical cryptographic technology to ensure security is that attackers cannot crack highly complex mathematical problems, such as discrete logarithm problems, using the current computing power available. However, with the emergence of quantum computers, this assumption may no longer hold in the future, and conventional cryptographic technology faces challenges. With the emergence of the Internet of Things (IoT), the number of devices connected to the Internet has increased significantly. In scenarios such as vehicle-to-everything (V2X) and Industrial Internet of Things (IIoT), secret key distribution and management based on authoritative

third parties present challenges in terms of high communication overhead and computational complexity [4]. Physical layer security technologies [5] have the advantages of being lightweight and decentralized, with low communication overhead. They are especially suitable for resource-constrained devices in IoT scenarios, as well as in V2X scenarios where the high-speed movement of vehicles brings the burden of key distribution management. From the perspective of endogenous security [6], wireless communication systems take advantage of the convenience of wireless connections to enable terminals to connect to the Internet from any location and at any time. However, the side effects of this openness of wireless connections bring potential security risks, such as eavesdropping attacks. These security problems that originate from within the system are called endogenous security problems. Physical layer security technologies are endogenous security technologies, which effectively solve the endogenous security problems.

Physical layer security, which consists mainly of securing transmitting, secret key generation, and authentication, may be a part of the whole security mechanism, along with classic cryptographic mechanisms. Securing transmitting uses security coding technologies to protect the confidentiality of data rather than relying on secret keys [7]. Nevertheless, it is challenging to acquire a positive secrecy capacity or to design effective security codes. Physical layer authentication extracts "fingerprints" from wireless links or hardware devices to identify users [8]. The aim of physical layer secret key generation (PLSKG) is for two parties, Alice and Bob, to acquire shared secret keys, knowing dependent random variables, but who do not share a secret key initially [9]. In time division duplex (TDD) mode, owing to the reciprocity of the channel, Alice and Bob observe a highly correlated channel parameter, such as received signal strength (RSS) or channel state information (CSI), which is regarded as a common random source. After quantization [10], information reconciliation [11], and privacy amplification [12], Alice and Bob can generate the same secret key.

An intelligent reflecting surface (IRS) is a two-dimensional surface consisting of an array of discrete elements that can change the phases and amplitudes of incident electromagnetic waves [13,14]. An IRS can create a virtual line-of-sight link between two parties blocked by an obstacle to improve the signal-to-noise ratio (SNR). An IRS is emerging as a promising technology owing to its ability to modify wireless channels in data transmitting and physical layer security [15,16]. Intuitively, the SNR's increase improves the performance of data transmitting, securing transmitting, and PLSKG, which can be achieved by optimizing the IRS's reflecting coefficients. Nevertheless, maximizing the SNR cannot acquire the optimal secret key generation rate (SKGR) of PLSKG because the entropy rate of a legitimate channel and the SNR of an eavesdropper also have an effect on the SKGR. There are three major directions of IRS-assisted PLSKG. One is to increase the entropy rate of a legitimate channel by randomly changing the phases of the IRS's elements after every two-way channel probing [17–20]. The second is maximizing the SKGR by optimizing the phases or amplitudes of the IRS's elements [21–27], which usually is achieved by solving a complicated optimization problem. The third is designing channel probing methods, which affect the entropy of a common random source [28–30].

Xiao et al. [31] provided a comprehensive overview of the application of PLSKG in the next communication systems and discussed some positive and negative effects of massive multiple-input–multiple-output (MIMO), IRSs, artificial intelligence (AI), integrated space–air–ground networks, and quantum communications on PLSKG. Li et al. [32] discussed in detail PLSKG combined with duplex modes, massive MIMO, and millimeter wave (mmWave) communications, and demonstrated the feasibility of PLSKG in practical communication systems. Li et al. [33] analyzed the constructive and destructive effects of IRSs on PLSKG. In static environments or wave-blockage scenarios, IRSs can improve the performance of PLSKG significantly. However, malicious users can launch attacks assisted by an IRS when they control the IRS, which can result in the failure or leakage of secret keys. Zhang et al. [34] provided a comprehensive overview of the principles, generation process, performance optimization, and application scenarios of PLSKG. Zeng et al. [35] focused

on several challenges in PLSKG. (1) How to estimate the amount of leaked information. (2) The overhead of information reconciliation is high when the SNR of a legitimate user is low. (3) How to decorrelate a generated bit sequence to obtain a truly random sequence. Jiao et al. [36] first pointed out three problems with existing PLSKG, and then introduced the 5G enabling technologies to solve the existing problems. Specifically, highly directional beams are used to block eavesdroppers in adjacent locations, mmWave channels are used to attain a high SNR, and hybrid precoding is used to reduce the temporal correlation of channel samples.

There are few articles [31,33] surveying the related works of IRS-assisted PLSKG. Although the studies [31,33] discussed some aspects of IRS-assisted PLSKG, it is necessary to extend them to promote the study of PLSKG. Existing reviews have not specifically analyzed the advantages and disadvantages of the IRS-assisted PLSKG research works within a unified framework. These motivate us to provide a survey of IRS-assisted PLSKG. This paper focuses on the topic of IRS-assisted PLSKG that includes related principles, research contents, and application scenarios. We provide detailed discussions on optimization complexity, training overheads, SKGRs, etc. Based on the limitations of existing studies, possible further extensions and research directions are discussed. Our major contributions can be summarized as follows.

- To provide readers with a more comprehensive and objective understanding of IRS-assisted PLSKG, we divide this field into three main categories: introducing the IRS's randomness, optimizing the IRS's reflecting coefficients, and designing probing protocols. We focus on the fundamental principles of the related works. Furthermore, the limitations of existing studies are discussed, which can inspire directions for further improvements.
- From an information-theoretic perspective, we carefully consider how to leverage the advantages of IRSs to improve SKGRs. We analyze the advantages and disadvantages of several methods for optimizing the IRS's reflecting coefficients within the same framework. Furthermore, we emphasize the importance of selecting a random source and propose the optimal method for acquiring the largest SKGR among the existing methods.
- Some application scenarios of PLSKG are discussed. Theoretically, PLSKG can be used for the majority of communication scenarios. We focus on the IIoT and V2X scenarios because they face the types of serious security risks that cannot be effectively addressed by conventional cryptographic schemes. We identify existing issues with PLSKG and provide potential solutions. Some future research directions are also given.

Notation: X^T, X^*, X^H, $tr\{X\}$, and X^{-1} denote the transposition, conjugating, conjugate transpose, trace, and inverse of a matrix, respectively. $diag(x)$ denotes a diagonal matrix whose i-th diagonal element is the i-th element of the vector x. $vec(X)$ denotes converting a matrix into a vector in column-major order. $\| x \|$ denotes the Euclidean norm of x. $A \otimes B$ and $A \diamond B$ denote the Kronecker and Khatri–Rao product, respectively. $\mathbb{C}^N$ denotes the N dimension vector space of complex numbers. Similarly, $\mathbb{C}^{N \times M}$ denotes the matrix space of complex numbers with N rows and M columns. $I(X;Y)$ denotes the mutual information of X and Y. $H(X)$ denotes the entropy of the random variable X. $log()$ is a function of the base 2 logarithm. $Pr\{B\}$ denotes the probability of the event B. $\mathcal{O}()$ denotes the computational complexity of an algorithm.

The rest of this article is structured as follows. Section 2 explains the fundamental concepts of PLSKG. Section 3 specifically introduces the state-of-the-art research on IRS-assisted PLSKG from different aspects. The application scenarios and challenges are discussed. Section 4 concludes the whole paper.

2. Preliminaries

In the pioneering work of information-theoretic security by Shannon in 1949 [37], the concept of perfect secrecy was introduced. Perfect secrecy can be guaranteed only if a secret key has at least as much entropy as the message to be encrypted, generally equivalent

to the key and plaintext being of equal length, which is difficult to achieve because the length of the key is usually less than that of the plaintext in practical situations. In 1993, Maurer [9] studied generating a secret key shared by two parties under the condition that the enemy obtains at most a negligible amount of information about the key. Ahlswede and Csiszar [38] also studied the same problem. The definition of the key capacity [38], also called the secrecy capacity in [9], is given below. For every $\epsilon > 0$, there exists a protocol for a sufficiently large n satisfying

$$Pr\{K \neq K'\} < \epsilon, \tag{1}$$

$$\frac{1}{n} I\left(\Phi^k, \Psi^k, Z^n; K\right) < \epsilon, \tag{2}$$

$$R < \frac{1}{n} H(K) + \epsilon, \tag{3}$$

$$\frac{1}{n} log|\mathcal{K}| < \frac{1}{n} H(K) + \epsilon, \tag{4}$$

where K, K' denote the keys generated by Alice and Bob, respectively, Φ^k, Ψ^k denote the information exchanged between Alice and Bob, Z^n denotes the sequence observed by an eavesdropper, Eve, $\mathcal{K}$ denotes the set from which K, K' take values, and $|\mathcal{K}|$ denotes the cardinality of the set $\mathcal{K}$. n is the length of the sequences observed by Alice, Bob, and Eve. The definition of the entropy is $H(K) = -\sum_{x \in \mathcal{K}} p(x) log(p(x))$, where $p(x)$ is the probability of the event that the key generated by Alice is x. The definition of the mutual information is $I(\Phi^k, \Psi^k, Z^n; K) = H(\Phi^k, \Psi^k, Z^n) + H(K) - H(\Phi^k, \Psi^k, Z^n, K)$, where $H(\Phi^k, \Psi^k, Z^n) = -\sum_{\varphi \in \Phi^k, \phi \in \Psi^k, z \in Z^n} p(\varphi, \phi, z) log(p(\varphi, \phi, z))$, $p(\varphi, \phi, z)$ denotes the probability of the event that the exchanged information between Alice and Bob is φ, ϕ and the observed sequence by Eve is z. $H(\Phi^k, \Psi^k, Z^n, K)$ has a similar definition to $H(\Phi^k, \Psi^k, Z^n)$. The maximum achievable R is called the key capacity. The first constraint (1) guarantees that Alice and Bob acquire the same key. The second constraint (2) ensures that Eve obtains at most a negligible amount of information about the key. The third (3) is the limitation of the entropy. The fourth constraint (4) ensures that the key follows a uniform distribution.

In general, it is difficult to acquire the expression of the key capacity except in a few special cases [38]. Luckily, Maurer [9] gave the upper and lower bounds of the key capacity.

$$R \leq min\{I(X;Y), I(X;Y|Z)\}, \tag{5}$$

$$R \geq max\{I(X;Y) - I(X;Z), I(X;Y) - I(Y;Z)\}, \tag{6}$$

where X, Y, and Z denote the random variables observed by Alice, Bob, and Eve, respectively, and the definition of the conditional mutual information is $I(X;Y|Z) = H(X|Z) - H(X|Y,Z)$. $R = I(X;Y)$ when Z is independent of X, Y. When $X \rightarrow Y \rightarrow Z$ forms a Markov chain, $R = I(X;Y) - I(X;Z)$. When $Y \rightarrow X \rightarrow Z$ forms a Markov chain, $R = I(X;Y) - I(Y;Z)$.

Maurer [9] demonstrated the feasibility of PLSKG by using a satellite as a random source, and three-party terminals on land as receivers on binary symmetric channels. At present, the majority of the literature uses wireless channel parameters as random sources for the following reasons. (1) The wireless channel exhibits spatial variation: in a rich scattering environment, the received signals at two locations that are more than half an electromagnetic wave distance apart are independent of each other, preventing eavesdroppers from obtaining legitimate channel information. (2) The wireless channel has time variation: within a coherent time, the channel state is unchanged, and, beyond the coherent time, the channel states are independent of each other. Therefore, it can be used as a random source that is not controlled by any third party, as proposed by Ahlswede and Csiszar [38]. (3) The wireless channel has reciprocity: the state of the channel remains unchanged during forward transmission and reverse transmission. The legitimate parties can obtain highly correlated channel information. The above characteristics make it advantageous to use wireless channels as the random source to extract the key.

A general protocol of PLSKG consists of four phases: channel probing [39], quantization [10], information reconciliation [11], and privacy amplification [12]. Some articles have the phase of preprocessing such as denoising, decorrelated, and increasing reciprocity. Mathur et al. [40] proposed a protocol using channel impulse response or receiving signal strength as a random source. They conducted experiments using off-the-shelf 802.11 hardware, which achieved approximately 1 bit/second SKGR in a real indoor environment. Chen et al. [41] used temporally and spatially correlated wireless channel coefficients as the random source to acquire high SKGRs. The reasons for their approach of acquiring high SKGRs were the increased dimension of the random source and the improved SNRs of legitimate users after denoising preprocessing. To increase SKGRs further, MIMO [42] and orthogonal frequency division multiplexing (OFDM) [43,44] are used to improve the performance of PLSKG. IRSs, as one of the 6G enabling technologies, can improve the performance of PLSKG significantly. Hence, there have been numerous studies on IRS-assisted PLSKG in recent years [17–26,28–30].

Unlike MIMO systems with higher complexity and higher power consumption, the consumed power of each element of an IRS is only 15, 45, and 60 mW for 3-bit, 4-bit, and 5-bit resolution phase shifting [45]. In addition, the received power increases in the order of N_r^2 in an IRS-assisted single-user system, where N_r denotes the number of reflecting elements. In the theoretical study, the control ways of IRSs are divided into three categories: continuous amplitudes and phase shifts, constant amplitudes and continuous phase shifts, and constant amplitudes and discrete phase shifts [13]. The control way of continuous amplitudes and phase shifts has a tractable constraint in IRS-related optimization problems. The control way of constant amplitudes and discrete phase shifts is consistent with practical applications. IRSs have great potential to improve the performance of data transmission and PLSKG.

3. IRS-Assisted PLSKG

How can IRSs improve the PLSKG's performance? IRSs improve the PLSKG's performance in two significant aspects: the SNR and the entropy rate of the wireless channel. If the entropy rate of the wireless channel is low, the SKGR is small, even if the SNR is high. This usually happens in static or sparse multipath environments. Note that the reason why we use the entropy rate rather than entropy is that the wireless channel is modeled as a stochastic process. Certainly, if the SNR is low, the SKGR is also small, even if the entropy rate is high. Therefore, IRSs are mainly used to increase the entropy rate of the wireless channel in static indoor environments. In wave-blockage or cell-edge scenarios, the focus should be on improving the SNR. We need to consider the two aspects simultaneously when they are equally important. This can be achieved by optimizing the IRS's reflecting coefficients to maximize the SKGR. The formulated optimization problems are usually complex. In the following, we present and discuss the research progress from three aspects: introducing the IRS's randomness, optimizing the IRS's reflecting coefficients, and designing probing protocols.

3.1. Introducing the IRS's Randomness

In static and sparse multipath environments, the entropy rate of the wireless channel is low, which limits the SKGR. To deal with the problem, a feasible method is to introduce the IRS's randomness [17–20]. This method uses the random reflecting coefficients of an IRS as the random source. The general process is divided into three steps. (1) An IRS randomly selects reflecting coefficients according to some probability distribution. (2) Alice and Bob probe their channel in turn to acquire samples of the channel parameters. Note that the probing period must be smaller than the coherence time of the channel. (3) Repeat steps 1 and 2 until a sufficient number of samples are obtained.

As shown in Figure 1, T_{up}, T_p denote the update period of an IRS and the probing period of Alice and Bob, respectively. $t_i, s_i (i = 1, 2, \ldots, L)$ denote the time of transmitting signals by Alice and Bob, respectively. L denotes the oversampling factor within a channel coherence time. It is important to calculate the SKGR of this scheme, and the theoretical

analysis is given by Hu et al. [19]. They considered a system consisting of a single antenna, Alice, a single antenna, Bob, and an IRS with N_r reflecting elements. The estimated channel of Alice and Bob can be expressed as

$$h_a = \sum_{n=1}^{N_r} \varphi_n h_{ar,n} h_{rb,n} + n_a, \tag{7}$$

$$h_b = \sum_{n=1}^{N_r} \varphi_n h_{ar,n} h_{rb,n} + n_b, \tag{8}$$

$$h_e = \sum_{n=1}^{N_r} \varphi_n h_{ar,n} h_{re,n} + n_e, \tag{9}$$

where $h_{ar,n}, h_{rb,n}, h_{re,n}$ denote the channels of Alice and the n-th element of the IRS, Bob and the n-th element, and Eve and the n-th element, respectively, φ_n denotes the n-th reflecting coefficient, and n_a, n_b denote additive white Gaussian noise (AWGN) with 0 means and σ_a^2, σ_b^2 variances of Alice and Bob, respectively. It is difficult to obtain the closed form of the SKGR, but it has an approximate form when N_r is large [19]

$$R = \frac{1}{T_{up} + T_p} I(h_a; h_b) \approx \frac{1}{T_{up} + T_p} log\left(1 + \frac{1}{\frac{2}{\gamma_{eq}} + \frac{1}{\gamma_{eq}^2}}\right), \tag{10}$$

where $\gamma_{eq} = \frac{\sigma_h^2(1+N_r\sigma_h^2)}{\sigma^2}$, $\sigma_a^2 = \sigma_b^2 = \sigma^2$, and σ_h^2 denotes the power of the channel. Equation (10) is a rewritten form of the original formula [19] to see more clearly the effect of N_r on the SKGR. It is observed that R is directly proportional to γ_{eq}. It is in line with the expectation that the SKGR increases as N_r increases. Another important factor is the duration of acquiring a pair of samples (h_a, h_b). As shown in Figure 1, it is equal to $T_{up} + T_p$ when L is equal to 1. The smaller $T_{up} + T_p$ is, the better.

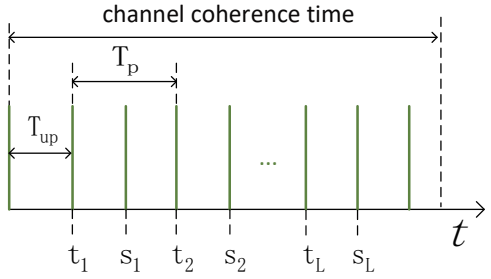

Figure 1. Time domain diagram of the channel probing.

The experimental results were given and discussed by Staat et al. [18]. Assuming extracting one bit from one downsampled sample, the SKGR is upper bounded by $(T_{up} + LT_p)^{-1}$. Note that downsampling is implemented by averaging L samples within a channel coherence time. T_{up} and T_p are approximately equal to 2ms, and N_r is 128 in their experiments. The SKGR is 237.45 bits/s and the SKDR is 0.26 when $L = 1$. The SKGR is 97.39 bits/s and the SKDR is 0.083 when $L = 4$. It is concluded that selecting L requires a tradeoff between the SKGR and SKDR. Only one subcarrier of the OFDM and one antenna are used; the SKGR will increase further if using all subcarriers and multiple antennas.

The goal of oversampling is to decrease the power of noise by averaging the data samples with noise. The IRS uses 1-bit resolution to control phases, which means it takes values from the set $\{1, -1\}$. It is not necessary to use a higher resolution, because the random source $\sum_{n=1}^{N_r} \varphi_n h_{ar,n} h_{rb,n}$ approximately follows a Gaussian distribution when N_r is large, resulting in the SKGRs of different phase control approaches being approximately equal.

The primary risk of random phase shifting [17–19] is the potential for an eavesdropping attack when Eve is in close proximity to Bob or Alice. As indicated in Equations (8) and (9),

the observation results of Bob and Eve are correlated only if the channels $h_{rb,n}$ and $h_{re,n}$ are correlated. Owing to the static environment, $h_{rb,n}$ and $h_{re,n}$ change slowly, which makes them vulnerable to inference attacks. What is the upper bound of the SKGR of the random phase shifting? Correlated eavesdroppers need to be considered, and the synchronization error also has an effect on the SKGR when the update period of the IRS is short.

As mentioned before, the IRS randomly selects reflecting coefficients according to some probability distribution. Which distribution is the best? There are no conclusions about this question. The articles [18,19] use a uniform distribution by default. Liu et al. [17] pointed out that their approach [18,19] reduced the entropy of the random source because the distribution of the random source is not a uniform distribution. This motivated Liu et al. [17] to make sure that the distribution of the random source is uniform by controlling the IRS's reflecting coefficients. They proposed two methods: phase shifting control of heuristic and deep reinforcement learning. Requiring training data for learning is the burden of this method. The benefit is that the SKGR of their proposed method is much larger than that of the other methods [18,19]. Some remarks on the study [17] are listed as follows.

- The use of uniform multi-level quantization in the study [17] limits the selection of the random shifting control approach. It means that the random source $\sum_{n=1}^{N_r} \varphi_n h_{ar,n} h_{rb,n}$ must follow a uniform distribution to achieve maximum entropy. In fact, the maximum entropy can be achieved for arbitrary distributions using the existing quantization method [10].
- The optimal selection of the random shifting control approach should maximize the SKGR subject to the constraints of the IRS's reflecting coefficients. Will the SKGR increase significantly if the amplitudes of the reflecting coefficients can change? The optimal probability distribution for the reflecting coefficients is not easy to obtain. Nevertheless, some experience and intuition might be worth considering. For example, select φ_n to maximize the variance of the random source. Furthermore, ensure that φ_n follows a Gaussian distribution with maximum variance.

Are the schemes of random phase shifting [17–19] as secure as conventional PLSKG schemes? This problem was studied by Mehmood et al. [20]. In their model, both Alice and Bob were equipped with an IRS. Eve was one wavelength away from Alice. The experimental results demonstrated that the greater the number of reflecting elements and multipaths there were, the higher was the level of secrecy. In sparse multipath environments, a large number of the reflecting elements are required to guarantee the secrecy of PLSKG.

3.2. Optimizing the IRS's Reflecting Coefficients

For consistency of representation, the symbols used in this section are included in Table 1. Different from introducing the randomness of the IRS, optimizing the IRS's reflecting coefficients is finished before the process of PLSKG. The IRS's reflecting coefficients do not change during the process. Generally, the statistical information of channels, such as covariance matrices, is required before the optimization. The optimization of the reflecting coefficients can increase the SKGR because the reflecting coefficients are included in the statistical information.

Table 1. The definitions of symbols.

Symbols	Definitions
N_a	The number of Alice's antennas.
N_b	The number of Bob's antennas.
N_r	The number of the IRS's elements.
N_e	The number of Eve's antennas.
K_e	The number of Eves.
K_u	The number of users (multiple user scenarios).
ϵ	The accuracy of the algorithm solution.
I_{SCA}	The iteration number of SCA.

Different optimization problems are formulated based on different system models, which may include single or multiple antennas, the presence or absence of eavesdroppers, and different control methods for IRSs. A basic system consists of single-antenna users, Alice and Bob, one eavesdropper, Eve, and an IRS having N_r reflecting coefficients. The IRS can change the amplitudes and phases continuously. The optimization problem is formulated as

$$\max_{\varphi} \quad R \tag{11}$$

$$s.t. \quad |\varphi_n| \leq 1, n = 1, 2, ..., N_r, \tag{12}$$

where φ_n denotes the n-th reflecting coefficient, and R denotes the SKGR. In the study [21], $R = log\left(\frac{f(\varphi)}{g(\varphi)}\right)$, where $f(\varphi) = c_1 + c_2\varphi^H A_1\varphi + c_3\varphi^H A_2\varphi\varphi^H A_3\varphi$, and $g(\varphi) = d_1 + d_2\varphi^H B_1\varphi + d_3\varphi^H B_2\varphi\varphi^H B_3\varphi$. Observe that $f(\varphi)$ consists of three different terms: a constant, a quadratic term $\varphi^H A_1\varphi$, and a quartic term $\varphi^H A_2\varphi\varphi^H A_3\varphi$. $g(\varphi)$ has a similar expression to $f(\varphi)$. It is not difficult to see that the objective function is not convex. Semidefinite relaxation (SDR) is used to transform $\varphi^H A_1\varphi$ into $tr\{A_1V\}$ and $\varphi^H A_2\varphi\varphi^H A_3\varphi$ into $tr\{A_2VA_3V\}$, where $V = \varphi\varphi^H$. Therefore, $f(\varphi) = f(V) = c_1 + c_2tr\{A_1V\} + c_3tr\{A_2VA_3V\}$ is a convex function of V, because A_2 and A_3 are positive semidefinite matrices. An auxiliary variable, C, is introduced, and let $f(V) \geq Cg(V)$. The original problem is then transformed into maximizing C by jointly optimizing C and V. Due to variable coupling, alternatively optimizing methods are used to solve the problem. To reduce the complexity of the algorithm, the successful convex approximation (SCA) is used. Assuming there are K_e Eves in the system model, the objective function is changed to $R = min\left\{log\left(\frac{f(\varphi)}{g(\varphi)}\right), k = 1, 2, ..., K_e\right\}$, which only increases the number of constraints and does not change the structure of the optimization problem.

Li et al. [23] considered a multi-user scenario in which Alice intended to generate secret keys with K_u users. All parties, Alice and the users, were equipped with a single antenna. When Alice extracted keys with the k-th user, the remaining users were regarded as potential eavesdroppers. The formulated optimization problem has a more complex structure than that of the study [21]. The solving method of [23] is a little different from that of [21]. The logarithm of the product is converted into the sum of logarithms. An effective algorithm combining the SDR and SCA was proposed.

The studies [21,23] only considered a single-input–single-output (SISO) system model. It is necessary to expand it into a multiple-input–single-output (MISO) model. Hu et al. [24] assumed that Alice and Bob were equipped with N_a and single antennas, respectively. A joint transmitting and reflecting beamforming optimization was formulated as

$$\max_{\varphi, w} \quad R \tag{13}$$

$$s.t. \quad |\varphi_n| \leq 1, n = 1, 2, ..., N_r, \tag{14}$$

$$\| w \|^2 \leq P_A, \tag{15}$$

where w denotes the transmitting beamforming and P_A denotes the transmitting power. The alternating optimization method is a common method to solve this variable coupling problem, and transforms the original problem into the optimizing problem of φ and the optimizing problem of w. Owing to no eavesdroppers, the original problem is equivalent to two sub-optimizing problems, and the closed-form solutions of the sub-optimizing problems are acquired.

The random source in the study [24] was a scalar, which limits the SKGR. Liu et al. [22] used a N_a-dimensional channel as a random source, which increased the SKGR significantly. Further, a $N_a(N_r + 1)$-dimensional channel was used as a random source by probing the channel multiple times within a coherence time [26]. The randomness of the direct and cascaded channel was explored fully, which increased the SKGR considerably. The probing method proposed by Lu et al. [26] included the precoding of signals, the control of the IRS's reflecting coefficients, and the channel estimation. Hence, an optimization of the

joint of the precoding matrix and the reflecting coefficients was formulated. By variable substitution and mathematical operations, the original problem was transformed into an equivalent problem that had a simpler form and was effectively solved. Although Hu et al. [27] considered a MIMO system, the receiver acquired the preprocessing signal by taking an inner product of the receiving signal and an all-one vector, which resulted in the system model degenerating into a MISO situation. The major contribution was that they proposed a low-complexity algorithm to solve a joint transmitting and reflecting beamforming optimization problem.

The comparative results of various studies on the optimization of the IRS's reflecting coefficients are presented in Table 2. The algorithm of [24] has minimal computational complexity because there are no eavesdroppers, and the form of the covariance matrix of the channel becomes simpler by using the Kronecker correlation model. The algorithms [21–23] using the Kronecker correlation model have lower complexity than those [24,26,27] not using the Kronecker model. For multi-dimensional channels used as the random source [22,26], the SKGR is large and the SKDR is high. For one-dimensional channels used as the random source [21,23,24,27], the SKGR is small and the SKDR is low. The increase in the dimension of the random source is a crucial factor in increasing the SKGR because it fully explores the randomness of the channel. On the other hand, the SNR is low because the multiple antennas are not used to obtain diversity gain. Similar to the communication theory of traditional data transmission, the trade-off between multiplexing and diversity gain should be considered.

Table 2. Comparative results of different optimization methods.

References	Antenna Model	Eavesdropping Model	Joint Optimization	IRS's Constraints	Training Overhead	Performance	Complexity
[21]	SISO	K_e single-antenna Eves	No	$\|\varphi_n\| \leq 1$	2	Small SKGR, high SKDR.	$\mathcal{O}\big((N_r^{6.5}K_e^{3.5} + N_r^{5.5}K_e^{2.5})\, log^2(1/\epsilon)\big) I_{SCA}$
[22]	MISO	K_e single-antenna Eves	No	$\|\varphi_n\| \leq 1$	$1 + N_a$	Large SKGR, high SKDR.	$\mathcal{O}\big((N_r^{6.5}K_e^{3.5} + N_r^{5.5}K_e^{2.5})\, log^2(1/\epsilon)\big) I_{SCA}$
[23]	SISO, K_u users	$K_u - 1$ single-antenna Eves	No	$\|\varphi_n\| \leq 1$	$2K_u$	Small SKGR, high SKDR.	$\mathcal{O}\big((N_r^9 K_u^3 + N_r^7 K_u^5 + N_r^5 K_u^7)\, log(1/\epsilon)\big) I_{SCA}$
[24]	MISO	No	Yes	$\|\varphi_n\| = 1$	2	Small SKGR, low SKDR.	$\mathcal{O}(1)$
[26]	MISO	No	Yes	Discrete phases	$(1 + N_a)$ $(1 + N_r)$	Large SKGR, high SKDR.	$\mathcal{O}\big(N_a^3/\epsilon^2 + N_a(1 + N_r) log(1/\epsilon)\big)$
[27]	MIMO	K_e single-antenna Eves	Yes	$\|\varphi_n\| \leq 1$	2	Small SKGR, low SKDR.	$\mathcal{O}\big(K_e(N_a + N_r)/\epsilon\big)$

Different optimization methods acquire different SKGRs based on different system models. We provide an explanation from the perspective of information theory. As shown in Figure 2, assume that Alice and Bob are equipped with N_a and N_b antennas, respectively. An IRS has N_r reflecting elements. Bob transmits the training symbol s_b and Alice receives the signals [46]

$$y_a = \sqrt{P_b}(H_{ba} + H_{ra}\Phi H_{br})s_b + n_a, \tag{16}$$

where $H_{ba} \in \mathcal{C}^{N_a \times N_b}$, $H_{ra} \in \mathcal{C}^{N_a \times N_r}$, $H_{br} \in \mathcal{C}^{N_r \times N_b}$, denote the channels between Bob and Alice, between the IRS and Alice, and between Bob and the IRS, respectively, $\Phi = diag(\varphi)$

denotes the reflecting coefficients matrix, and n_a denotes the additive white Gaussian noise (AWGN). Equation (16) is rewritten as [46]

$$\begin{aligned} y_a =& vec\left(\sqrt{P_b}(H_{ba} + H_{ra}\Phi H_{br})s_b\right) + n_a \\ =& \sqrt{P_b}\left(s_b^T \otimes I_{N_a}\right) vec(H_{ba}) + \sqrt{P_b}\left(s_b^T \otimes I_{N_a}\right)\left(H_{br}^T \diamond H_{ra}\right)\varphi + n_a \\ =& \sqrt{P_b}\left(s_b^T \otimes I_{N_a}\right) H_c\bar{\varphi} + n_a \\ =& \sqrt{P_b}\left(\bar{\varphi}^T \otimes s_b^T \otimes I_{N_a}\right) h_c + n_a, \end{aligned} \tag{17}$$

where P_b denotes the transmitting power of Bob, $s_b^T \otimes I_{N_a}$ denotes the Kronecker product between s_b^T and I_{N_a}, and $H_{br}^T \diamond H_{ra}$ denotes the Khatri–Rao product between H_{br}^T and H_{ra}, $\bar{\varphi} = [1, \varphi^T]^T$, $H_c = [vec(H_{ba}), H_{br}^T \diamond H_{ra}]$, and $h_c = vec(H_c)$.

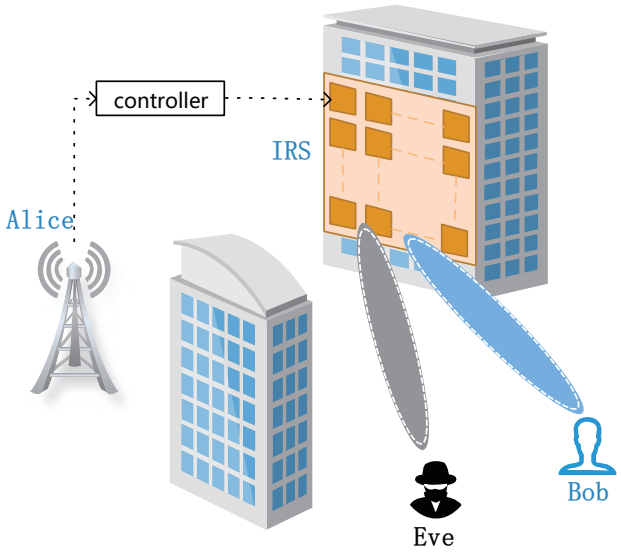

Figure 2. IRS-assisted PLSKG.

To estimate the channel h_c, Bob transmits the training sequence with the length of $T \geq N_b(N_r + 1)$ and Alice stacks T received signals [46]

$$\bar{y}_a = \begin{bmatrix} y_a(1) \\ \vdots \\ y_a(T) \end{bmatrix} = \begin{bmatrix} X_a(1) \\ \vdots \\ X_a(T) \end{bmatrix} h_c + \begin{bmatrix} n_a(1) \\ \vdots \\ n_a(T) \end{bmatrix} = X_a h_a + \bar{n}_a, \tag{18}$$

where $X_a(t) = \sqrt{P_b}\bar{\varphi}^T(t) \otimes s_b^T(t) \otimes I_{N_a}$. Provided that X_a is full rank, the method of least squares (LS) can be used to estimate h_c. The estimated channels of Alice and Bob can be expressed as [47]

$$h_a = X_a^H \bar{y}_a = h_c + n'_a, \tag{19}$$

$$h_b = X_b^H \bar{y}_b = h_c + n'_b. \tag{20}$$

Lu et al. [26] used Ah_c as the random source and acquired the mathematical model

$$z_a = Ah_a = Ah_c + \tilde{n}_a, \tag{21}$$

$$z_b = Ah_b = Ah_c + \tilde{n}_b, \tag{22}$$

where $A = \bar{\Phi}^T \otimes P^T$, $\bar{\Phi}$ denotes the reflecting coefficient matrix and P denotes the precoding matrix. According to the data-processing inequality of information theory, $I(h_a; h_b) \geq$

$I(Ah_a; h_b) \geq I(Ah_a; Ah_b) = I(z_a; z_b)$. Because A is a column full rank matrix, $I(z_a; z_b) \geq I((AA^H)^{-1}A^H z_a; z_b) \geq I((AA^H)^{-1}A^H z_a; (AA^H)^{-1}A^H z_b) = I(h_a; h_b)$. We conclude that there is no information loss because $I(h_a; h_b) = I(z_a; z_b)$. This is also the reason why the SKGR of [26] is the largest among the existing methods.

Similar to Equation (21), Liu et al. [22] used $A_1 h_c$ as the random source and $A_1 = \varphi^T \otimes I_{N_a}$. There is information loss because A_1 is not a column full rank matrix, which results in $I(h_a; h_b) \geq I(A_1 h_a; A_1 h_b)$.

Hu et al. [24] used $w^T A_1 h_c$ as the random source, and the transmitting beamforming w^T is not a column full rank matrix. We conclude that the SKGR of [24] is smaller than that of [22] according to the data-processing inequality. Hence, the SKGR of the work [26] is larger than that of the work [22] for the MISO system model, and the SKGR of the work [22] is larger than that of the work [24].

Although the SKGR decreases by preprocessing h_c with a matrix whose columns are not of full rank, it can improve the SNR and reduce the training overhead. As shown in Table 2, the training overhead of the work [26] is larger than that of the work [22], and the training overhead of the work [22] is larger than that of the work [24]. It is known that optimizing the transmitting and reflecting beamforming can improve the SNR. For instance, the SNR is improved by optimizing the transmitting beamforming, w, and reflecting beamforming, φ, in the study [24], and by optimizing the reflecting beamforming, φ, in the study [22].

Based on the model of estimated channels shown in Equation (19), we propose to use the channel h_c as the random source to acquire the largest SKGR among the existing methods. Alice and Bob can use state-of-the-art channel estimation techniques to acquire channel samples, which are then used to generate secret keys. The whole process of PLSKG has no optimization problems. Nevertheless, the dimension of h_c is $N_a N_b (N_r + 1)$ and the SNR corresponding to a certain dimension may be low. In addition, there are challenges in quantizing high-dimensional vectors. These shortcomings prevent the practical application of this probing protocol, but it can be used as a reference value for comparing the performance of other PLSKG methods.

3.3. Designing Probing Protocols

Channel probing is the first phase of PLSKG, and different probing protocols or methods have a significant effect on the performance of PLSKG. It is observed that the method of random phase shifting [17–20] only explores the randomness of the IRS's reflecting coefficients and does not use the randomness of the channel itself. To solve this problem, Lu et al. [28] proposed a probing protocol fully exploiting the randomness from the channel and the IRS. Specifically, the whole process can be divided into four steps. The first step is that Alice and Bob estimate the direct channel when the IRS is turned off. The second step involves estimating the reflecting channel by configuring orthogonal reflecting coefficients in N_r rounds of channel probing. In the third step, Alice uses the way of random phase shifting [17–19] to control the IRS, and Bob estimates the cascaded channel. The final step is for Alice to reconstruct the reciprocal channel of step 3. It is obvious that the SKGR contributes from three random sources: the direct channel, the reflecting channel, and the IRS. Some remarks on the study [28] are listed as follows.

- The randomness of the wireless channel and the IRS is exploited. The channel coherence time is divided into three parts assigned to direct channel estimation, reflecting channel estimation, and random phase shifting, respectively.
- The SKGR does not always increase as the number of reflecting elements increases. Estimating the reflecting channels requires a large number of time slots when the number of reflecting elements is large, which reduces the available slots for random phase shifting. It is necessary to reduce the overhead of estimating the reflecting channels.
- The attack model only includes one eavesdropper and can be expanded to include additional cases of non-colluding multiple eavesdroppers. This probing protocol can be expanded to include systems with multiple antennas to increase the SKGR.

One of the interesting applications of PLSKG is to achieve perfect secrecy [37] by combining the one-time pad. Ji et al. [29] divided one channel coherence time into two parts. The first part is used to extract secret keys using random phase shifting [17–19]. The second part is used to transmit data encrypted by the extracting keys and the one-time pad. It is critical to make sure that the SKGR is approximately equal to the transmitting rate due to the requirement of perfect secrecy. The optimal time slot allocation for the two parts is obtained by their proposed optimizing algorithm.

Most studies concentrate on sub-6GHz communications, and PLSKG of mmWave channels is prone to blockage effects. IRSs can solve this problem. Lu et al. [30] investigated PLSKG in the IRS-assisted mmWave system. The major difference is that the random source is the virtual beam-domain channel instead of the actual physical channel. There are two advantages of using the beam-domain channel. One is reducing the training overhead by exploiting the sparsity of the mmWave channel. The other is that different virtual channels of the beam domain are independent of each other. In their protocol, the virtual spatial angles need to be estimated first, and then Alice and Bob estimate the channel gains in the beam domain. The channels are re-estimated after one channel coherence block, but the virtual spatial angles are re-estimated after several coherent blocks. From a signal processing perspective, transforming the original channels into virtual beam-domain channels is similar to the idea of principal component analysis. Both methods achieve the goal of reducing the dimensionality of the data. The dimension discussed in the study [30] is the virtual spatial angle. Since the channels of different beams are independent of each other, Eve only acquires information about the secret key when the beams of Bob and Eve overlap. Narrower beams offer enhanced security. The main contribution is proposing a probing protocol to estimate the beam-domain channel. Interestingly, this idea can be applied to MIMO PLSKG in sparse multipath environments. It is worth further study in the future.

3.4. Application Scenarios

IIoT, commonly referred to as Industry 4.0, improves the efficiency of production and manufacturing through the use of large numbers of networked embedded sensing devices. These devices are often poorly secured and vulnerable to cyber-attacks. This brings huge challenges to IIoT security [48]. Conventional cryptographic schemes such as public key infrastructure (PKI) have high complexity, making them unsuitable for resource-constrained IIoT devices. The complexity increases as the number of devices increases owing to the centralized architecture model of conventional security systems. PLSKG is a promising solution to the security of IIoT due to it being lightweight and its provision of information-theoretical security. Certainly, PLSKG cannot meet all the requirements of IIoT. A more practical conclusion is that PLSKG enhances security as part of an overall security system. Specifically, PLSKG can tackle the issue of key generation, and the generated key can be used to provide confidentiality and authentication services.

Owing to dynamic changes in network topology and open connectivity, V2X communications face serious and complex security challenges [4]. A V2X security system must prevent broadcast messages from being falsified, protect privacy data such as vehicles' positions, and prevent information from being eavesdropped. Conventional cryptographic technologies are well-established and have been used for an extended period. However, there are still challenges when applying them directly to V2X. Public-key cryptosystems, such as those proposed by Rivest–Shamir–Adleman (RSA), Diffie–Hellman (DH), and elliptic curve cryptography (ECC), are associated with high communication and computation overhead, which cannot meet the requirement of low latency for V2X. PLSKG can rapidly and efficiently generate symmetric secret keys for V2X communications, which overcomes the shortcomings of conventional methods. Some details of PLSKG in V2X communications scenarios are listed as follows.

- The reciprocity, temporal variation, and spatial variation of wireless channels are important foundations of PLSKG. The coherence time is only hundreds of microseconds

in typical V2X scenarios. This property of rapid change is beneficial for obtaining a large SKGR. In general, the SKGR is inversely proportional to the coherence time. In urban scattering-rich environments, channel responses are independent between one transmit–receive link and another, if the links are separated by an order of half a wavelength or more. This makes it difficult for eavesdroppers to acquire information about the generated key.

- Users of symmetric encryption algorithms must share a secret key before any secure communications. This is achieved by asymmetric algorithms in classical cryptographic schemes. Nevertheless, it may not be appropriate for resource-limited and time-critical V2X devices, as asymmetric algorithms have high computational complexity. Wan et al. [49] proposed a PLSKG protocol for generating a pre-shared key in V2X communications. The length of the pre-shared key is optimized under timing constraints for the V2X application. They compared their work with cryptographic algorithms to evaluate the security strength, performance, and overhead. The results indicate that their PLSKG protocol is a low-cost and efficient security mechanism.
- Figure 3 depicts a schematic diagram illustrating the combination of PLSKG and V2X public key infrastructure. The Certificate Authority (CA) issues certified public–private key pairs to vehicles. The CA communicates with vehicles through a 5G cellular base station (gNB) and roadside units (RSUs). After the initial stage, vehicles can authenticate others using their private key and attach the corresponding certificate. Then, two vehicles start a PLSKG protocol assisted by an IRS to generate keys to enable secure communications over an insecure channel. Compared with traditional cryptography, the update rate of the secret key of PLSKG is much faster, which improves the security of communication systems.

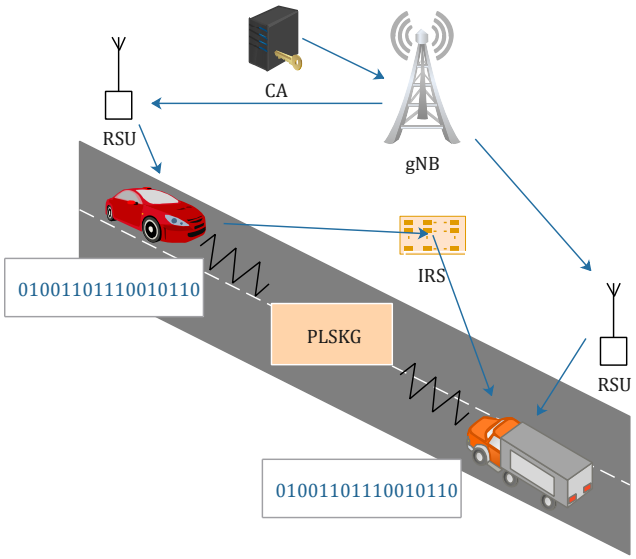

Figure 3. The V2X application scenario.

3.5. Challenges and Opportunities

- Correlation channel models
  The Kronecker correlation channel model simplifies the form of the covariance matrix of the channel and simplifies the optimization problem. Nevertheless, the Kronecker model only applies to Rayleigh-fading environments [50]. An alternative approach is to assume that there is no prior knowledge [21–23] about the spatial correlation model of the channel. The PLSKG based on this assumption can be applied to any channel environment. Its disadvantage is increasing the complexity of the optimization problems [21–23]. How to balance the advantages and disadvantages of these two methods is a question that is worthy of study.

- High SKDRs
  The existing works [21–24,26,27] on optimizing the IRS's reflecting coefficients only focus on maximizing the SKGR, without considering the constraint of the SKDR. The overhead in the information reconciliation phase is high when the SKDR is large. Hence, it is necessary to consider the constraint of the SKDR in optimization problems. In the presence of jamming attackers, there may be no feasible solution to the optimization problem including the constraint of the SKDR.
- The attack's model
  In the studies of PLSKG, existing attack models are simple and ideal. Specifically, most works only considered passive eavesdropping attacks and did not consider active attacks such as pilot contaminations [51], jamming attacks [52], injection attacks [53], and man-in-the-middle attacks [54]. The main issue is the complexity and analytically intractability if the model includes many attack modes. It is one of the key factors limiting the development of PLSKG. A scheme is needed to evaluate the security of a PLSKG protocol.
- A tractable system framework
  Most studies only focus on one or two phases of PLSKG, such as the probing phase [17–24,26–30], and few works [41] include all phases of PLSKG. The SKGR calculated according to Equation (6) is a theoretical value, and the actual value will be affected by other factors such as quantization, the SKDR, information reconciliation, and privacy amplification. A tractable system framework must include all phases of PLSKG, have reliable output such as the SKGR, and can be optimized.
- A trade-off between PLSKG and data transmission
  The probing process of PLSKG requires communication resources. Hence, it is necessary to study both simultaneously [55] when communication resources are limited. Both data transmission and PLSKG require channel estimation. As a result, the estimated channels in the PLSKG can be used to demodulate the signals in the data transmission. It is a feasible approach to integrate PLSKG into existing communication systems. Relevant research is still lacking.

4. Conclusions

The classical cryptographic technology exhibits high computational complexity, high communication overhead, and the risk of being cracked by quantum computing in complex and severe communication scenarios. PLSKG, one of the technologies of physical layer security, is a promising solution to the problems faced by conventional cryptographic approaches due to its characteristics of being lightweight and highly efficient, and its ability to provide information-theoretical security. Recently, there have been numerous studies on IRS-assisted PLSKG because the IRS is capable of manipulating wireless channels to create an intelligent environment.

We present a comprehensive survey of IRS-assisted PLSKG, which is divided into three aspects: introducing the IRS's randomness, optimizing the IRS's reflecting coefficients, and designing probing protocols. From the perspective of information theory, the selection of the random source has a significant effect on the SKGR. We compare the advantages and disadvantages of existing optimization methods [21–24,26,27] and present the results in Table 2.

It has been observed that IRSs can significantly improve the performance of PLSKG in static and dynamic environments. Random phase shifting [17–19] is effective and easy to achieve, and it is mainly used in static environments. Optimizing the IRS's reflecting coefficients can significantly increase the SKGR. Nevertheless, the optimization problems of the reflecting coefficients usually are difficult to solve and have high computational complexity. Some assumptions of system models, such as the Kronecker correlation model, can reduce the complexity of optimization problems. The protocols of channel probing have a significant impact on PLSKG. A well-designed protocol can increase the SKGR and improve the efficiency of the PLSKG. There are some challenges and issues that need to be addressed to promote the development of PLSKG.

Author Contributions: Conceptualization, E.X. and B.-J.H.; methodology, E.X. and B.-J.H.; software, E.X.; validation, E.X. and B.-J.H.; formal analysis, E.X. and B.-J.H.; investigation, E.X. and B.-J.H.; resources, E.X. and B.-J.H.; data curation, E.X.; writing—original draft preparation, E.X.; writing—review and editing, E.X., B.-J.H. and Q.S.; visualization, E.X., B.-J.H. and Q.S.; supervision, B.-J.H.; project administration, B.-J.H.; funding acquisition, B.-J.H. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the National Natural Science Foundation of China (NSFC) under Grant 61871193, in part by the R&D Program of key science and technology fields in Guangdong province under Grant 2019B090912001, and in part by the Guangzhou Key Field R&D Program under Grant 202206030005.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data sharing not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

PLSKG	Physical layer secret key generation
IRS	Intelligent reflecting surface
SKGR	Secret key generation rate
SKDR	Secret key disagreement ratio
SCA	Successive convex approximation
SDR	Semidefinite relaxation
V2X	Vehicle-to-everything
IoT	Internet of Things
IIoT	Industrial Internet of Things
MIMO	Multiple-input–multiple-output
SNR	Signal-to-noise ratio
PKI	Public key infrastructure

References

1. Porambage, P.; Gür, G.; Osorio, D.P.M.; Liyanage, M.; Gurtov, A.; Ylianttila, M. The Roadmap to 6G Security and Privacy. *IEEE Open J. Commun. Soc.* **2021**, *2*, 1094–1122. [CrossRef]
2. Nguyen, V.L.; Lin, P.C.; Cheng, B.C.; Hwang, R.H.; Lin, Y.D. Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges. *IEEE Commun. Surv. Tutorials* **2021**, *23*, 2384–2428. [CrossRef]
3. Katz, J.; Lindell, Y. *Introduction to Modern Cryptography: Principles and Protocols*, 1st ed.; Chapman and Hall/CRC: Boca Raton, FL, USA, 2007.
4. Lu, R.; Zhang, L.; Ni, J.; Fang, Y. 5G Vehicle-to-Everything Services: Gearing Up for Security and Privacy. *Proc. IEEE* **2020**, *108*, 373–389. [CrossRef]
5. Zou, Y.; Zhu, J.; Wang, X.; Hanzo, L. A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends. *Proc. IEEE* **2016**, *104*, 1727–1765. [CrossRef]
6. Jin, L.; Hu, X.; Lou, Y.; Zhong, Z.; Sun, X.; Wang, H.; Wu, J. Introduction to wireless endogenous security and safety: Problems, attributes, structures and functions. *China Commun.* **2021**, *18*, 88–99. [CrossRef]
7. Wu, Y.; Khisti, A.; Xiao, C.; Caire, G.; Wong, K.K.; Gao, X. A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead. *IEEE J. Sel. Areas Commun.* **2018**, *36*, 679–695. [CrossRef]
8. Xiao, L.; Greenstein, L.J.; Mandayam, N.B.; Trappe, W. Using the physical layer for wireless authentication in time-variant channels. *IEEE Trans. Wirel. Commun.* **2008**, *7*, 2571–2579. [CrossRef]
9. Maurer, U.M. Secret key agreement by public discussion from common information. *IEEE Trans. Inf. Theory* **1993**, *39*, 733–742. [CrossRef]
10. Patwari, N.; Croft, J.; Jana, S.; Kasera, S.K. High-Rate Uncorrelated Bit Extraction for Shared Secret Key Generation from Channel Measurements. *IEEE Trans. Mob. Comput.* **2010**, *9*, 17–30. [CrossRef]
11. Brassard, G.; Salvail, L. Secret-Key Reconciliation by Public Discussion. In Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques, Lofthus, Norway, 23–27 May 1993; pp. 410–423. [CrossRef]
12. Bennett, C.H.; Brassard, G.; Crepeau, C.; Maurer, U.M. Generalized privacy amplification. *IEEE Trans. Inf. Theory* **1995**, *41*, 1915–1923. [CrossRef]

13. Liu, Y.; Liu, X.; Mu, X.; Hou, T.; Xu, J.; Di Renzo, M.; Al-Dhahir, N. Reconfigurable Intelligent Surfaces: Principles and Opportunities. *IEEE Commun. Surv. Tutorials* **2021**, *23*, 1546–1577. [CrossRef]
14. Wu, Q.; Zhang, R. Towards Smart and Reconfigurable Environment: Intelligent Reflecting Surface Aided Wireless Network. *IEEE Commun. Mag.* **2020**, *58*, 106–112. [CrossRef]
15. Hong, S.; Pan, C.; Ren, H.; Wang, K.; Chai, K.K.; Nallanathan, A. Robust Transmission Design for Intelligent Reflecting Surface-Aided Secure Communication Systems with Imperfect Cascaded CSI. *IEEE Trans. Wirel. Commun.* **2021**, *20*, 2487–2501. [CrossRef]
16. Guo, H.; Yang, Z.; Zou, Y.; Lyu, B.; Jiang, Y.; Hanzo, L. Joint Reconfigurable Intelligent Surface Location and Passive Beamforming Optimization for Maximizing the Secrecy-Rate. *IEEE Trans. Veh. Technol.* **2023**, *72*, 2098–2110. [CrossRef]
17. Liu, Y.; Wang, M.; Xu, J.; Gong, S.; Hoang, D.T.; Niyato, D. Boosting Secret Key Generation for IRS-Assisted Symbiotic Radio Communications. In Proceedings of the 2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring), Helsinki, Finland, 25–28 April 2021; pp. 1–6. [CrossRef]
18. Staat, P.; Elders-Boll, H.; Heinrichs, M.; Kronberger, R.; Zenger, C.; Paar, C. Intelligent Reflecting Surface-Assisted Wireless Key Generation for Low-Entropy Environments. In Proceedings of the 2021 IEEE 32nd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Helsinki, Finland, 13–16 September 2021; pp. 745–751. [CrossRef]
19. Hu, X.; Jin, L.; Huang, K.; Sun, X.; Zhou, Y.; Qu, J. Intelligent Reflecting Surface-Assisted Secret Key Generation with Discrete Phase Shifts in Static Environment. *IEEE Wirel. Commun. Lett.* **2021**, *10*, 1867–1870. [CrossRef]
20. Mehmood, R.; Wallace, J.W. Wireless security enhancement using parasitic reconfigurable aperture antennas. In Proceedings of the 5th European Conference on Antennas and Propagation (EUCAP), Rome, Italy, 11–15 April 2011; pp. 2761–2765.
21. Ji, Z.; Yeoh, P.L.; Zhang, D.; Chen, G.; Zhang, Y.; He, Z.; Yin, H.; Li, Y. Secret Key Generation for Intelligent Reflecting Surface Assisted Wireless Communication Networks. *IEEE Trans. Veh. Technol.* **2021**, *70*, 1030–1034. [CrossRef]
22. Liu, Y.; Huang, K.; Sun, X.; Yang, S.; Wang, L. Intelligent Reflecting Surface-Assisted Wireless Secret Key Generation against Multiple Eavesdroppers. *Entropy* **2022**, *24*, 446–460. [CrossRef]
23. Li, G.; Sun, C.; Xu, W.; Renzo, M.D.; Hu, A. On Maximizing the Sum Secret Key Rate for Reconfigurable Intelligent Surface-Assisted Multiuser Systems. *IEEE Trans. Inf. Forensics Secur.* **2022**, *17*, 211–225. [CrossRef]
24. Hu, L.; Li, G.; Qian, X.; Ng, D.W.K.; Hu, A. Joint Transmit and Reflective Beamforming for RIS-assisted Secret Key Generation. In Proceedings of the 2022 IEEE Global Communications Conference, Rio de Janeiro, Brazil, 4–8 December 2022; pp. 2352–2357. [CrossRef]
25. Wei, Z.; Li, B.; Guo, W. Adversarial Reconfigurable Intelligent Surface Against Physical Layer Key Generation. *IEEE Trans. Inf. Forensics Secur.* **2023**, *18*, 2368 – 2381. [CrossRef]
26. Lu, T.; Chen, L.; Zhang, J.; Chen, C.; Hu, A. Joint Precoding and Phase Shift Design in Reconfigurable Intelligent Surfaces-Assisted Secret Key Generation. *IEEE Trans. Inf. Forensics Secur.* **2023**, *18*, 3251–3266. [CrossRef]
27. Hu, L.; Li, G.; Qian, X.; Hu, A.; Ng, D.W.K. Reconfigurable Intelligent Surface-Assisted Secret Key Generation in Spatially Correlated Channels. *IEEE Trans. Wirel. Commun.* **2023**, *early access*. [CrossRef]
28. Lu, T.; Chen, L.; Zhang, J.; Cao, K.; Hu, A. Reconfigurable Intelligent Surface Assisted Secret Key Generation in Quasi-Static Environments. *IEEE Commun. Lett.* **2022**, *26*, 244–248. [CrossRef]
29. Ji, Z.; Yeoh, P.L.; Chen, G.; Pan, C.; Zhang, Y.; He, Z.; Yin, H.; Li, Y. Random Shifting Intelligent Reflecting Surface for OTP Encrypted Data Transmission. *IEEE Wirel. Commun. Lett.* **2021**, *10*, 1192–1196. [CrossRef]
30. Lu, T.; Chen, L.; Zhang, J.; Chen, C.; Duong, T.Q. Reconfigurable Intelligent Surface-Assisted Key Generation for Millimeter Wave Communications. In Proceedings of the 2023 IEEE Wireless Communications and Networking Conference (WCNC), Glasgow, UK, 26–29 March 2023; pp. 1–6. [CrossRef]
31. Xiao, Q.; Zhao, J.; Feng, S.; Li, G.; Hu, A. Securing NextG networks with physical-layer key generation: A survey. *Secur. Saf.* **2024**, *3*, 2023021. [CrossRef]
32. Li, G.; Sun, C.; Zhang, J.; Jorswieck, E.; Xiao, B.; Hu, A. Physical Layer Key Generation in 5G and Beyond Wireless Communications: Challenges and Opportunities. *Entropy* **2019**, *21*, 497. [CrossRef] [PubMed]
33. Li, G.; Hu, L.; Staat, P.; Elders-Boll, H.; Zenger, C.; Paar, C.; Hu, A. Reconfigurable Intelligent Surface for Physical Layer Key Generation: Constructive or Destructive? *IEEE Wirel. Commun.* **2022**, *29*, 146–153. [CrossRef]
34. Zhang, J.; Duong, T.Q.; Marshall, A.; Woods, R. Key Generation From Wireless Channels: A Review. *IEEE Access* **2016**, *4*, 614–626. [CrossRef]
35. Zeng, K. Physical layer key generation in wireless networks: challenges and opportunities. *IEEE Commun. Mag.* **2015**, *53*, 33–39. [CrossRef]
36. Jiao, L.; Wang, N.; Wang, P.; Alipour-Fanid, A.; Tang, J.; Zeng, K. Physical Layer Key Generation in 5G Wireless Networks. *IEEE Wirel. Commun.* **2019**, *26*, 48–54. [CrossRef]
37. Shannon, C.E. Communication Theory of Secrecy Systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715. [CrossRef]
38. Ahlswede, R.; Csiszar, I. Common randomness in information theory and cryptography. I. Secret sharing. *IEEE Trans. Inf. Theory* **1993**, *39*, 1121–1132. [CrossRef]
39. Walkenhorst, B.T.; Harper, A.D.; Baxley, R.J. Channel model and sounding method effects on wireless secret key rates. In Proceedings of the 2012 IEEE Conference on Technologies for Homeland Security (HST), Waltham, MA, USA, 13–15 November 2012; pp. 597–602. [CrossRef]

40. Mathur, S.; Trappe, W.; Mandayam, N.; Ye, C.; Reznik, A. Radio-Telepathy: Extracting a Secret Key From an Unauthenticated Wireless Channel. In Proceedings of the 14th ACM International Conference on Mobile Computing and Networking, New York, NY, USA, 14–19 September 2008; pp. 128–139. [CrossRef]
41. Chen, C.; Jensen, M.A. Secret Key Establishment Using Temporally and Spatially Correlated Wireless Channel Coefficients. *IEEE Trans. Mob. Comput.* **2011**, *10*, 205–215. [CrossRef]
42. Jorswieck, E.A.; Wolf, A.; Engelmann, S. Secret key generation from reciprocal spatially correlated MIMO channels. In Proceedings of the 2013 IEEE Globecom Workshops, Atlanta, GA, USA, 9–13 December 2013; pp. 1245–1250. [CrossRef]
43. Zhang, J.; Marshall, A.; Woods, R.; Duong, T.Q. Efficient Key Generation by Exploiting Randomness From Channel Responses of Individual OFDM Subcarriers. *IEEE Trans. Commun.* **2016**, *64*, 2578–2588. [CrossRef]
44. Peng, Y.; Wang, P.; Xiang, W.; Li, Y. Secret Key Generation Based on Estimated Channel State Information for TDD-OFDM Systems Over Fading Channels. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 5176–5186. [CrossRef]
45. Méndez-Rial, R.; Rusu, C.; González-Prelcic, N.; Alkhateeb, A.; Heath, R.W. Hybrid MIMO Architectures for Millimeter Wave Communications: Phase Shifters or Switches? *IEEE Access* **2016**, *4*, 247–267. [CrossRef]
46. Swindlehurst, A.L.; Zhou, G.; Liu, R.; Pan, C.; Li, M. Channel Estimation with Reconfigurable Intelligent Surfaces—A General Framework. *Proc. IEEE* **2022**, *110*, 1312–1338. [CrossRef]
47. Steven, M.K. *Fundumentals of Statistical Signal Processing: Estimation Theory*; Prentice Hall PTR: New Jersey, NJ, USA, 1993.
48. Tange, K.; De Donno, M.; Fafoutis, X.; Dragoni, N. A Systematic Survey of Industrial Internet of Things Security: Requirements and Fog Computing Opportunities. *IEEE Commun. Surv. Tutorials* **2020**, *22*, 2489–2520. [CrossRef]
49. Wan, J.; Lopez, A.; Faruque, M.A.A. Physical Layer Key Generation: Securing Wireless Communication in Automotive Cyber-Physical Systems. *ACM Trans. Cyber-Phys. Syst.* **2018**, *3*, 1–26. [CrossRef]
50. Chuah, C.N.; Tse, D.N.C.; Kahn, J.M.; Valenzuela, R.A. Capacity scaling in MIMO wireless systems under correlated fading. *IEEE Trans. Inf. Theory* **2002**, *48*, 637–650. [CrossRef]
51. Im, S.; Jeon, H.; Choi, J.; Ha, J. Secret Key Agreement with Large Antenna Arrays Under the Pilot Contamination Attack. *IEEE Trans. Wirel. Commun.* **2015**, *14*, 6579–6594. [CrossRef]
52. Belmega, E.V.; Chorti, A. Protecting Secret Key Generation Systems Against Jamming: Energy Harvesting and Channel Hopping Approaches. *IEEE Trans. Inf. Forensics Secur.* **2017**, *12*, 2611–2626. [CrossRef]
53. Jin, R.; Zeng, K. Physical layer key agreement under signal injection attacks. In Proceedings of the 2015 IEEE Conference on Communications and Network Security, Florence, Italy, 28–30 September 2015; pp. 254–262. [CrossRef]
54. Mitev, M.; Chorti, A.; Belmega, E.V.; Reed, M. Man-in-the-Middle and Denial of Service Attacks in Wireless Secret Key Generation. In Proceedings of the 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 9–13 December 2019; pp. 1–6. [CrossRef]
55. Lai, L.; Liang, Y.; Poor, H.V. A Unified Framework for Key Agreement Over Wireless Fading Channels. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 480–490. [CrossRef]