symmetry

MDPI

Article

IRS-Assisted Hybrid Secret Key Generation

Meixiang Zhang [1,†], Ziyue Zhuang [1,2,†] and Sooyoung Kim [2,*,†]

[1] College of Information Engineering, Yangzhou University, Yangzhou 225009, China; mxzhang@yzu.edu.cn (M.Z.); mz120210954@stu.yzu.edu.cn (Z.Z.)
[2] Division of Electronics Engineering, IT Convergence Research Center, Jeonbuk National University, Jeonju 54896, Republic of Korea
* Correspondence: sookim@jbnu.ac.kr
† These authors contributed equally to this work.

Abstract: Physical layer secret key (SK) generation is known to be an efficient means to achieve a high secrecy rate, on the condition that dynamic channel state information (CSI) is provided. For this reason, the secrecy performance is highly degraded in a static environment. The intelligent reflecting surface (IRS) is a promising solution to create dynamic randomness, and thus lead to enhanced secrecy performance regardless of the user environments. This paper proposes an IRS-assisted physical layer SK generation scheme, by efficiently combining phase information of the direct and reflected channel information in a hybrid way. In particular, the initial SKs are obtained by adopting an efficient phase quantization method with symmetric bit allocation to complex numbered channel estimates. Simulation results show that the proposed hybrid phase quantization (PQ) can improve the SK generation rate and the key disagreement probability in a static environment.

Keywords: secret key generation; intelligent reflecting surface; phase quantization

Citation: Zhang, M.; Zhuang, Z.; Kim, S. IRS-Assisted Hybrid Secret Key generation. *Symmetry* **2023**, *15*, 1906. https://doi.org/10.3390/sym15101906

Academic Editors: Jia Hou, Jun Li, Xueqin Jiang and Antonio Palacios

Received: 7 August 2023
Revised: 7 September 2023
Accepted: 6 October 2023
Published: 12 October 2023

1. Introduction

Physical layer secret key (SK) generation technology is a promising technique for achieving a one-time-pad encryption approach in wireless communication systems. This is possible due to the reciprocity, space-time uniqueness, and fast time-varying nature of the wireless channel. With this approach, both legitimate communication parties can independently generate SKs in real-time using the wireless channel features as a random source, without the need for key transmission [1]. SK generation techniques rely on time-varying characteristics of the wireless channel. Therefore, in static environments, the keys cannot be updated quickly, which can eventually result in lower security protection. Examples of such cases can be found in static line-of-sight (LOS) scenarios such as those encountered in drone-enabled multi-hop wireless networks [2], or indoor Internet of Things (IoT) applications. Specifically, the study in [2] provides extensive analysis on mutual information between legitimate parties when they exchange SKs in the LOS condition.

The intelligent reflecting surface (IRS) has received a lot of attention in recent years, due to its capability of ameliorating the wireless channel environment through software-controlled reflections [3]. Specifically, the IRS consists of a large number of low-cost passive reflecting elements, each can independently make changes to the incident signal [3,4], and thus it has great potential to increase the SK generation rate in real time [5–8]. Most of the current research works on IRS-assisted SK generation focused on optimization problems to maximize the SK generation rate or SK capacity at the legitimate user by optimizing the phase shift coefficients or using random phase shifting of IRS [6–8].

For example, an IRS-assisted SK generation scheme was proposed in order to overcome the problem of low SK rate in a static environment, by using discrete phase shift [6]. This scheme maximized the SK rate by optimizing the IRS phase switching time, but there was no implementation details such as quantization method for the estimated channel

state information (CSI). On the other hand, phase shift optimization schemes for the IRS were proposed [7,8]. A lower bound on the SK capacity was derived for an IRS-assisted wireless network with multiple eavesdroppers, and an IRS reflection coefficient optimization framework was introduced [7]. The design principle of IRS-assisted SK generation was proposed, and its performance improvement in SK rate was verified [8].

However, both of the above two schemes incurred complexity compared with the random phase shifting scheme. Furthermore, a technique to maximize the SK capacity was introduced for the SK-generation process based on CSI, by adjusting the layout of the IRS elements [9]. It also proposed the process of SK generation based on CSI, but there was no detailed description for each step.

On the other hand, a number of studies reported quantization methods used during the SK generation process [10–15]. Although binary quantization method is simple and easy to implement [10], it can only generate a single SK bit. Multi-level equiprobable quantization methods were utilized to increase the bit generation rate [11,12]. In this case, selecting the appropriate quantization levels and interval partitioning are crucial issues that require a trade-off between information preservation and SK length. For example, previous studies presented multi-level phase quantization (PQ) methods to increase SK generation rate [13–15]. However, the complexity of quantization process is also increasing as the number of quantized bits redincreases. This is because the number of quantization levels is exponentially increasing with the number of quantized bits.

As a solution to the above mentioned problems of the existing works, this paper proposes an efficient IRS-assisted SK generation scheme with a computationally efficient PQ method. The first novelty of the proposed scheme lies in the hybrid method of extracting CSI for initial key generation. Phase information is first extracted from the direct channel, and then extracted from the combined channels with the IRS. This is because the IRS usually changes the phase of the reflecting signals almost without amplitude variations.

This way of hybrid extraction of CSI from different channels will contribute to increasing the randomness of key generation, and eventually lead to the increment in SK generation rate. The second novelty of the proposed scheme is utilization of a new and computationally efficient PQ method to generate SK from the extracted CSI. We first form a new complex number by using the amplitude and phase information extracted from the proposed hybrid method, and then quantize the phase in the complex plane. This paper presents the details of extracting phase information from the estimated CSI of the proposed hybrid method. The proposed method is universally applicable to any m-level quantization method, and the quantization level can be adaptively regulated.

The remainder of this paper is organized as follows. Section 2 describes the related works including the system model for an IRS-assisted SK generation and the conventional quantization methods. Section 3 first presents the hybrid way of extracting CSI, and then details the proposed PQ method. In order to verify the merits of the proposed scheme, Section 4 first presents a number of performance measures, and then provides the simulation results. Finally, the paper is concluded in Section 5.

2. Conventional IRS-Assisted SK Generation and Quantization

2.1. System Model for an IRS-Assisted SK Generation

Figure 1 shows a system model for a conventioanl IRS-assisted wireless communication system, where data transmission is encrypted with SK generated with the aid of IRS in order to achieve secure communications [5]. A typical scenario where IRS is required is in indoor IoT applications, where the channel changes slowly. In this case, the block fading channel remains constant during a long coherence time. An IRS can increase randomness by configuring its phase shift. Furthermore, the study in [5] introduced an application of using random phase shifts of IRS elements, with consideration of multiple eavesdroppers.

In these previous studies, the legitimate communication parties Alice and Bob send probe signals to each other in time-division duplex (TDD) mode, and extract SK from their correlated measurements before encrypted data transmission. Each of N reflecting elements

receives a superimposed multipath signal from the sender and then reflects the signal in random phase, with a diagonal IRS phase shifting matrix $\mathbf{\Theta} = \text{diag}(e^{j\theta_1}, e^{j\theta_2}, \cdots, e^{j\theta_N})$, where $\theta_n \in [0, 2\pi)$ is the phase shift of the n-th element. Additionally, a passive eavesdropper Eve was assumed to be positioned a few wavelengths away from the legitimate users [6,9,16,17]. As a result, she passively taps into an eavesdropping channel that is independent of the legitimate channel, without engaging in active attacks. Finally, all parties are equipped with a single antenna each.

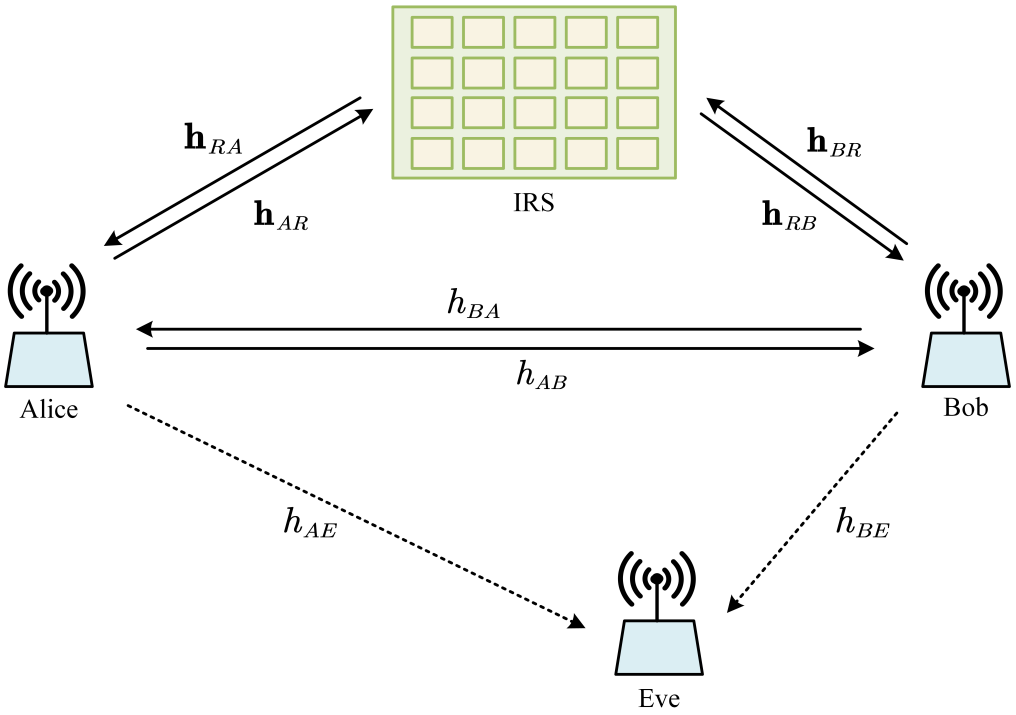


Figure 1. System model for an IRS-assisted wireless communication system.

In each block, Alice and Bob send the probe pilots alternatively to generate the SK during the first L time slots of the coherence time. After key generation, the data are encrypted with the generated keys before its transmission during the remaining coherence time. The received signals at Alice and Bob in each probe round can be expressed as follows, respectively [5,18]:

$$\begin{aligned} \mathbf{y}_A &= (h_{BA} + \mathbf{h}_{RA}^H \mathbf{\Theta} \mathbf{h}_{BR})\mathbf{x} + \mathbf{n}_A, \\ \mathbf{y}_B &= (h_{AB} + \mathbf{h}_{RB}^H \mathbf{\Theta} \mathbf{h}_{AR})\mathbf{x} + \mathbf{n}_B, \end{aligned} \tag{1}$$

where $h_{AB} \in \mathbb{C}^{1\times 1}$ and $h_{BA} \in \mathbb{C}^{1\times 1}$ are the CSIs of the direct channel from Alice to Bob and Bob to Alice, respectively, $\mathbf{h}_{AR}$ and $\mathbf{h}_{BR} \in \mathbb{C}^{N\times 1}$ are the CSI vectors from Alice and Bob to the IRS, and $\mathbf{h}_{RA}$ and $\mathbf{h}_{RB} \in \mathbb{C}^{N\times 1}$ are the reflected CSI vectors from the IRS to Alice and Bob, respectively. In addition, $\mathbf{x} \sim \mathcal{CN}(0, \mathbf{I})$ is the probing signal vector sent by Bob and Alice, and $\mathbf{n}_A \sim \mathcal{CN}(0, \sigma_A^2 \mathbf{I})$ and $\mathbf{n}_B \sim \mathcal{CN}(0, \sigma_B^2 \mathbf{I})$ denote the complex additive white Gaussian noise (AWGN) at Alice and Bob, where $\mathbf{I}$ is the identity matrix.

In this case, the channel estimates at Alice and Bob can be calculated from their reciprocally combined channels of the direct and reflected channels as follows:

$$\begin{aligned} \hat{h}_A &= h_{BA} + \mathbf{h}_{RA}^H \mathbf{\Theta} \mathbf{h}_{BR} + \hat{n}_A, \\ \hat{h}_B &= h_{AB} + \mathbf{h}_{RB}^H \mathbf{\Theta} \mathbf{h}_{AR} + \hat{n}_B, \end{aligned} \tag{2}$$

where $\hat{n}_A = \mathbf{x}^H \mathbf{n}_A / \|\mathbf{x}\|^2$ and $\hat{n}_B = \mathbf{x}^H \mathbf{n}_B / \|\mathbf{x}\|^2$ denote the estimation errors at Alice and Bob, respectively. Specifically, the initial two time slots are dedicated to the estimation of

the direct channel, while the remaining slots are only allocated for the estimation of the reflected channel and SK generation [18]. These channel estimates are used to generate SK at the quantization process, and the generated keys are used for information reconciliation as shown in Figure 2. Finally, the privacy amplification algorithm based on hash function is applied to avoid information leakage [9]. Through the above process, both communication parties complete the same key establishment.

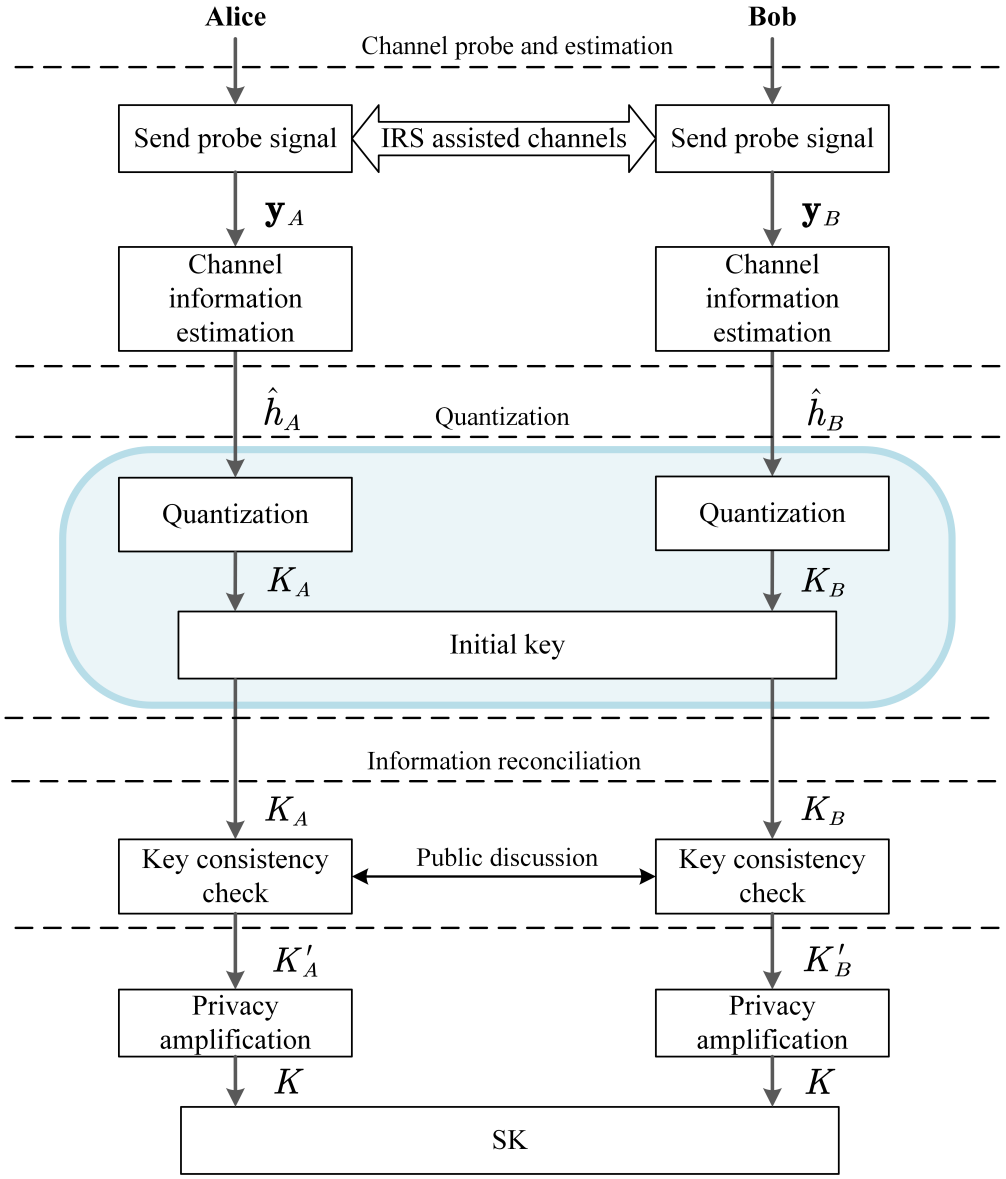


Figure 2. Conventional SK-generation protocol with IRS.

2.2. Conventional Quantization Methods

Based on the above channel estimates of $\hat{h}_A$ and $\hat{h}_B$, the initial key value is generated by converting the estimated value to binary bits. There have been binary quantization methods, namely absolute-value-based quantization (AVQ) and difference-value-based quantization (DVQ) [10]. Since these methods converts the channel estimates in to a single bit, the SK rate becomes low.

Multi-level quantization methods can be used to increase the SK rate [11–15]. For example, an equiprobable quantization method was proposed [11], given the probability density function (PDF) of the input signal x, the decision thresholds for the m-level quantization method were determined as follows:

$$\int_{-\infty}^{\bar{q}_i} p(x)dx = \frac{i}{m}, \tag{3}$$

where $p(x)$ is the PDF of x, $\bar{q}_i$ is the i-th decision threshold, $i = 1, 2, \cdots, m-1$. By this way, each of the m quantization regions, i.e., $(-\infty, \bar{q}_1], (\bar{q}_1, \bar{q}_2], \cdots, (\bar{q}_{m-1}, \infty)$ is selected with equal probability, and it is mapped to $\log_2 m$ bits using Gray coding. Furthermore, a method to improve the bit agreement ratio was proposed by inserting guard bands between two consecutive quantization levels [12]. We note that the complex numbered CSI does not have a uniform distribution, and thus $\bar{q}_i$ cannot be simply determined. This eventually leads to a complex quantization problem.

Since the phase information of the CSI has uniform PDF, quantization of the phase may lead to a simple quantization process. A PQ method was proposed by using a uniform quantization method for phase information of the channel estimates [13]. Furthermore, a phase shift quantization method, which is similar to the phase shift keying (PSK) demodulation method, was proposed [14]. This method quantized the phase value, ϕ with a m-level uniform quantizer as follows [15]:

$$f(\phi) = j \quad \text{if} \quad \phi \in \left[\frac{2\pi(j-1)}{m}, \frac{2\pi j}{m}\right), \tag{4}$$

for $j = 1, 2, \cdots, m$. Therefore, the quantization of each phase value generates $\log_2 m$ secret bits. In order to extract $\log_2 m$ bits, the above quantization method requires of 1 to m comparison operations, and thus average $m/2$ operations per extracted CSI.

3. Proposed Methods

3.1. SK Generation Protocol

In order to fully exploit the randomness, we propose a hybrid approach to extracting CSI in order to generate the SK, as shown in Figure 3. In each block, there are total L time slots, and we assume that the channel does not change within a block. In addition, Alice and Bob alternatively send probe signals every two time slots, and thus there are a total $L/2$ probe rounds in each block. Specifically, in the first probe round, Alice and Bob alternatively send probe signals while the IRS is turned off. Then, the received signals at Alice and Bob can be expressed as follows, respectively:

$$\begin{aligned} \mathbf{y}_A &= h_{BA}\mathbf{x} + \mathbf{n}_A, \\ \mathbf{y}_B &= h_{AB}\mathbf{x} + \mathbf{n}_B. \end{aligned} \tag{5}$$

Upon receiving $\mathbf{y}_A$ and $\mathbf{y}_B$ in (5) at Alice and Bob, respectively, channel estimations are conventionally performed using the least square (LS) method, and the channel estimates at Alice and Bob can be presented as follows [7]:

$$\begin{aligned} \hat{h}_A &= h_{BA} + \hat{n}_A, \\ \hat{h}_B &= h_{AB} + \hat{n}_B. \end{aligned} \tag{6}$$

The phase information of these channel estimates will be jointly quantized to form the initial key bit sequence.

Afterwards, Alice and Bob alternatively extract the channel estimates from the combined channels, which are composed of the direct and reflected channels, using (2) during the subsequent $L-2$ time slots. In this case, $\mathbf{\Theta}$ is randomly switched at every two time slots to impose randomness. Similarly, the phase information of these channel estimates with linear normalization will be jointly quantized to generate the initial key bit sequence. The detailed process of the quantization for the proposed method is explained in the next section.

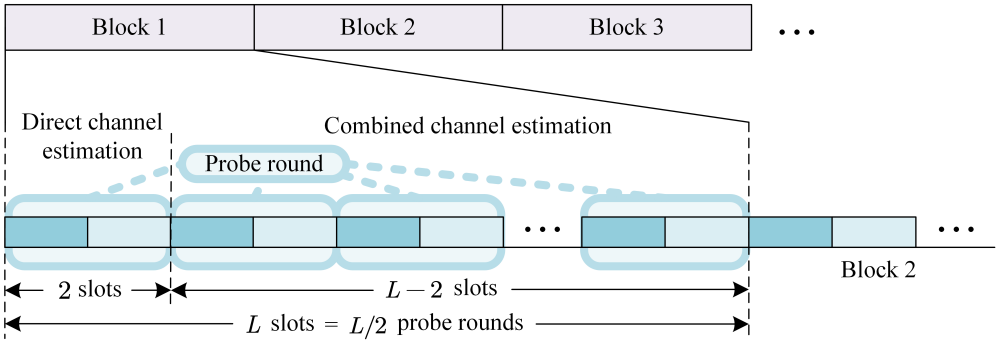


Figure 3. Channel probing stage of IRS-assisted SK generation.

3.2. Compact Phase Quantization Method

We propose a new efficient 2^p-level PQ method using the phase information of $\hat{h}_A$ and $\hat{h}_B$ in (2) and (6) to generate p quantized bits, respectively, as shown in Figure 4. We set quantization thresholds that equally divide the complex plane into 2^p regions, and allocate p bits in each region by using the Gray coding, which allows us to extract p bits from the phase information. Therefore, this process can be interpreted as the demodulation process of a PSK modulation symbol. There have been extensive works on developing efficient demodulation schemes, especially focusing on soft demapping [19,20]. Among them, we choose the most efficient one and tailor it to our application.

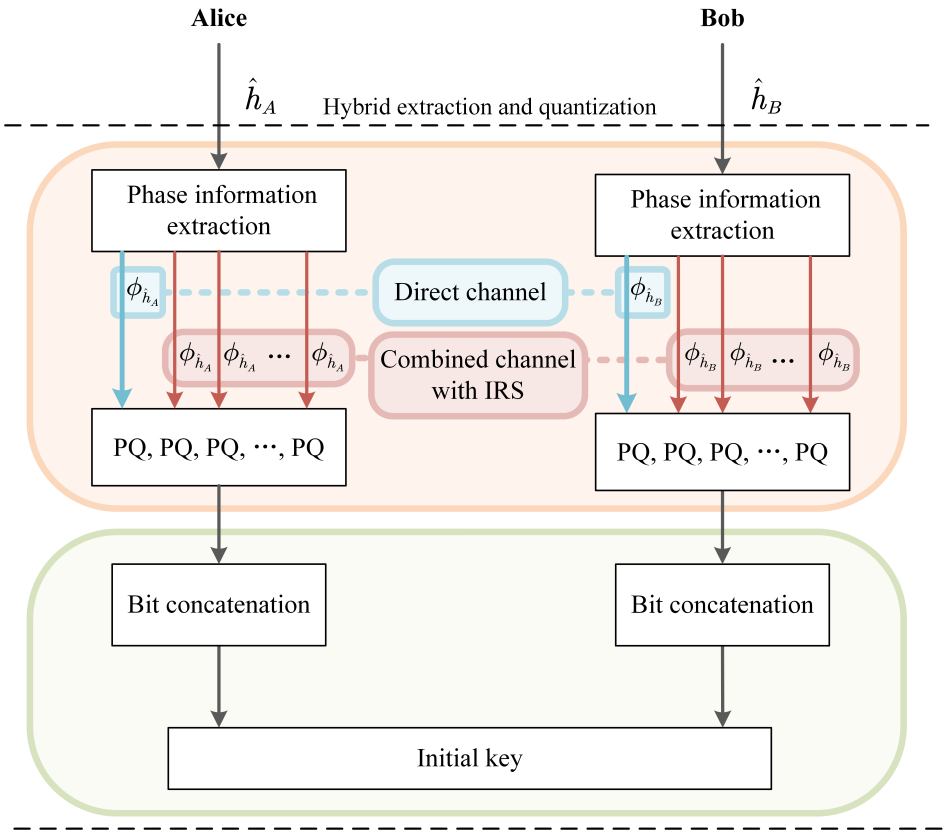


Figure 4. Proposed hybrid quantization with IRS.

We note that the main purpose of the proposed hybrid CSI extraction is to compensate low SK rate during the static environment, by using an efficient quantization method. Since we assume low amplitude variation of h_{AB}, the IRS is activated to impose phase dynamics of the CSI. This implies that it is not necessary to allocate multiple bits to amplitude in the channel probing stage. Instead, multiple bit allocation to phase information obtained from

IRS would contribute to increase the dynamics of the CSI. In addition, phase information is uniformly distributed from 0 to 2π, PQ would provide better randomness than AQ to secrete key information. Therefore, we extract phase information in the total time slots. It is also important to have computationally efficient quantization methods, i.e., a compact and easily extendable method. Considering the above facts, we refer to the constellation diagrams of the PSK modulation scheme with Gray coding and its soft demapping principle introduced in [20], and tailor them for our purpose.

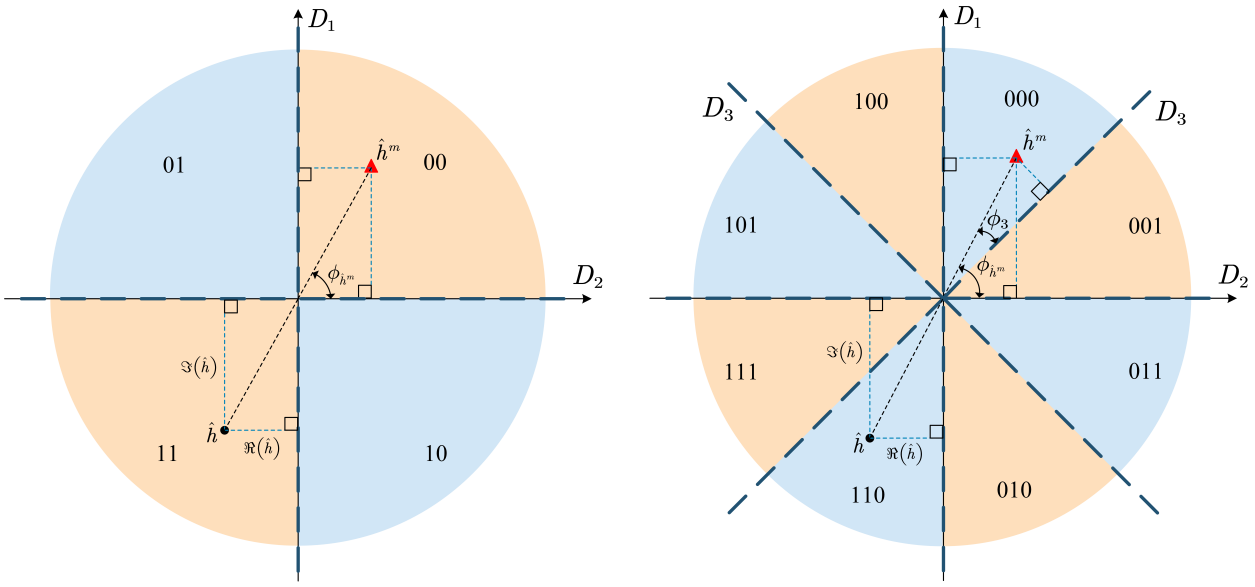
In order to visualize the PQ, we represent the extracted CSI of $\hat{h}_A$ and $\hat{h}_B$ as $\hat{h}_A = |\hat{h}_A|e^{j\phi_{\hat{h}_A}} = \Re(\hat{h}_A) + j\Im(\hat{h}_A)$ and $\hat{h}_B = |\hat{h}_B|e^{j\phi_{\hat{h}_B}} = \Re(\hat{h}_B) + j\Im(\hat{h}_B)$, respectively, where $|x|$ is the amplitude, ϕ_x is the phase, $\Re(x)$ is the real part, and $\Im(x)$ is the imaginary part of the complex number x, respectively. We equally divide the complex plane into 2^p separated phase regions. In the following sections, we present the proposed PQ examples of 4 to 32 levels, and this can be extendable to any 2^p-level schemes.

3.3. Examples of 4 to 32 Level PQ

For a 2^p-level PQ, the quantization bit mapping is made by the Gray coding principle. For convenience, here we denote the estimated CSI of either Alice or Bob as $\hat{h}$, because the quantization processes for $\hat{h}_A$ and $\hat{h}_B$ are the same. Figure 5 shows the bit mapping and decision threshold lines for 2^2- and 2^3-level PQ methods for the estimated CSI, $\hat{h}$ in the complex plane, where D_i redwith a dotted line indicates the decision threshold redline for the i-th quantized bit $b_i, i = 1, \cdots, p$.

Referring to Figure 5, we can find that the first and second bits can be estimated by taking the signs of real and imaginary parts of $\hat{h}$, i.e., $b_1 = \text{sign}(\Re(\hat{h}))$ and $b_2 = \text{sign}(\Im(\hat{h}))$. Then, these b_1 and b_2 provide sufficient information on in which quadrant of the complex plain $\hat{h}$ locates. By using this, we map $\hat{h}$ redrepresented by red triangle in the first quadrant of the complex plain, that is $\hat{h}^m = |\hat{h}|e^{j\phi_{\hat{h}^m}}$, where $\phi_{\hat{h}^m} = \tan^{-1}(|\Im(\hat{h})/\Re(\hat{h})|)$, so that its phase value is in the region of 0 to $\pi/2$. This means the third bit of 2^3-level PQ can be estimated by taking the sign of the distance between the threshold line D_3 to $\hat{h}^m$ located in the first quadrant, that is,

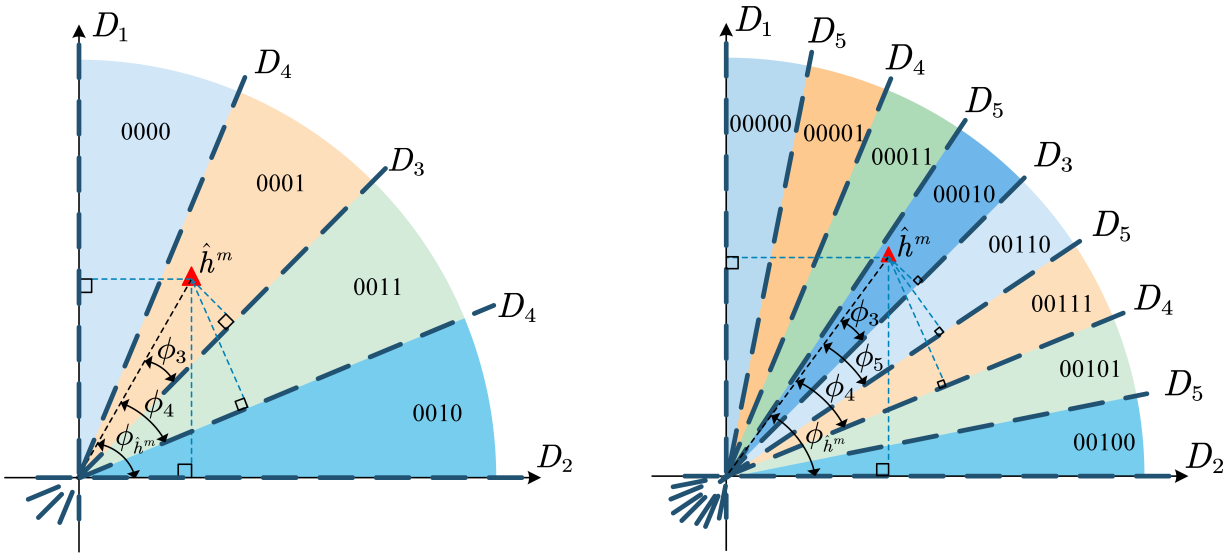
$$\begin{aligned} b_3 &= \text{sign}(|\hat{h}^m| \sin(-(\phi_{\hat{h}^m} - \pi/4))) \\ &= \text{sign}(-(\phi_{\hat{h}^m} - \pi/4)). \end{aligned} \tag{7}$$



(a) 2^2-level PQ (b) 2^3-level PQ

Figure 5. Bit mapping and decision thresholds for 2^2-level PQ and 2^3-level PQ.

The above principle, then can be extended to any 2^p-level PQ. Figure 6 shows the bits mapping with Gary coding and decision threshold lines for 2^4 and 2^5-level PQ methods, where $\hat{h}^m$ is redthe mapped version of $\hat{h}$ in the first quadrant of the complex plane. It is clear that b_1 to b_3 can be estimated exactly the same way as in the above 2^2 and 2^3-level PQ method. In addition, the remaining bits can be estimated recursively by using the previously estimated information. For example, $b_4 = \text{sign}(|-(\phi_{\hat{h}^m} - \pi/4)| - \pi/8)$.



(a) 2^4-level PQ (b) 2^5-level PQ

Figure 6. Bit mapping and decision thresholds for 2^4-level PQ and 2^5-level PQ.

By generalizing the above principle to 2^p-level PQ, we can have the following recursive equation:

$$\begin{aligned} b_1 &= \text{sign}(\Re(\hat{h})), \\ b_2 &= \text{sign}(\Im(\hat{h})), \\ b_i &= \text{sign}(-\phi_i), \\ \phi_i &= (-1)^i(|\phi_{i-1}| - \pi/2^{i-1}), \quad 2 < i \leq p, \end{aligned} \tag{8}$$

where $\phi_2 = \phi_{\hat{h}^m}$. The following Algorithm 1 describes the proposed PQ method. After the quantization process, the quantized bits are concatenated together to obtain the initial key bit sequence for Alice and Bob, respectively.

Algorithm 1 Proposed PQ.

Input: $\hat{h}$ % Estimated CSI
Output: **b** % Initial key bit vector
1: $\phi_{\hat{h}^m} = \tan^{-1}(|\Im(\hat{h})/\Re(\hat{h})|)$
2: $\phi_2 = \phi_{\hat{h}^m}$
3: $b_1 = \text{sign}(\Re(\hat{h}))$
4: $b_2 = \text{sign}(\Im(\hat{h}))$
5: **for** $i \leftarrow 3$ *to* p **do**
6: $\quad \phi_i = (-1)^i(|\phi_{i-1}| - \pi/2^{i-1})$
7: $\quad b_i = \text{sign}(-\phi_i)$
8: **end for**

We note that the proposed PQ in Algorithm 1 can be applied to any p bit PQ scheme, and thus a single quantizer can be universally applied to various multi-level quantization systems. In particular, when we adopt an adaptive quantization scheme to generate a

time-varying p bits, the proposed scheme may have a strong advantage for its universal applicability. Different quantization levels offer distinct performance advantages. Employing a quantization scheme with a smaller number of levels often results in lower initial key disagreement probability. However, the generated key sequence will also be shorter. Conversely, when employing a quantization scheme with a higher level, a longer key sequence can be obtained, albeit with a trade-off of potentially introducing multiple inconsistent bits in a string of key sequences. As such, the selection of quantization levels should be approached with careful consideration.

4. Secrecy Performance

The fundamental assumption made in this paper is that Eve is positioned a few wavelengths away from the legitimate users, as is common in many previous studies [6,9,16,17]. Under these circumstances, Bob and Eve will experience independent channels. Consequently, the CSI of the legitimate channel remains undisclosed to Eve, ensuring the perfect security of the SK generated from the legitimate CSI. Therefore, the primary performance metric in this scenario is the efficiency of key generation, which can be assessed using various performance measures as outlined below.

4.1. Performance Measures

We evaluate the proposed SK generation scheme in terms of a number of secrecy performance measures including the SK capacity, SK randomness, initial key disagreement probability, and effective key length. All of the above performance measures of the proposed schemes are compared with those of the conventional schemes.

The SK capacity, C is defined as $C = \min\{I(\hat{h}_A;\hat{h}_B), I(\hat{h}_A;\hat{h}_B \mid \hat{h}_E)\}$, where $\hat{h}_E$ denotes the estimated CSI at Eve. Since the channel estimates in different probe rounds are independent random variables [5], the SK capacity in the s-th probe round, C_s is also a random variable. Assuming the eavesdropper, Eve is a wavelength or more away from either Alice or Bob, the SK capacity in the first probe round without IRS, C_1 is upper bounded by the mutual information [11,21]:

$$\begin{aligned} C_1 &\le I(\hat{h}_A;\hat{h}_B \mid \hat{h}_E) = I(\hat{h}_A;\hat{h}_B) \\ &= \log_2\left(1 + \frac{\sigma^2_{\hat{h}_{BA}}}{\sigma^2_{\hat{n}_A} + \sigma^2_{\hat{n}_B} + \frac{\sigma^2_{\hat{n}_A}\sigma^2_{\hat{n}_B}}{\sigma^2_{\hat{h}_{BA}}}}\right). \end{aligned} \tag{9}$$

In this case, due to the channel reciprocity within the coherent time, we have $\sigma^2_{h_{BA}} = \sigma^2_{h_{AB}}$. In addition, we can assume that $\hat{n}_A$ and $\hat{n}_B$ are independent and identically distributed random variables without loss of generality, and thus $\sigma^2_{\hat{n}_A} = \sigma^2_{\hat{n}_B}$. Therefore, (9) can be simplified as

$$C_1 \le \log_2\left(1 + \frac{\sigma^4_{h_{BA}}/\sigma^4_{\hat{n}_A}}{1 + 2\sigma^2_{h_{BA}}/\sigma^2_{\hat{n}_A}}\right). \tag{10}$$

The SK capacity in the remaining probe rounds with IRS, $C_s, s = 2, 3, \cdots, S$, $S = L/2$, is upper bounded by the conditional mutual information [11,21]. In this case, we have $\sigma^2_{h_{BA}} + \sum_{n=1}^{N} \sigma^2_{h^n_{BRA}}$, where $\sigma^2_{h^n_{BRA}}$ is the variance of the n-th reflected channel. Thus, C_s can be derived as follows [9]:

$$\begin{aligned} C_s &\le I(\hat{h}_A;\hat{h}_B \mid \hat{h}_E) = I(\hat{h}_A;\hat{h}_B) \\ &= \log_2\left(1 + \frac{(\sigma^2_{h_{BA}} + \sum_{n=1}^{N} \sigma^2_{h^n_{BRA}})^2/\sigma^4_{\hat{n}_A}}{1 + 2(\sigma^2_{h_{BA}} + \sum_{n=1}^{N} \sigma^2_{h^n_{BRA}})/\sigma^2_{\hat{n}_A}}\right), \\ 2 &\le s \le S. \end{aligned} \tag{11}$$

The above derivation result shows that the SK capacity of the proposed system is certainly dependent on $\sigma^2_{h^n_{BRA}}$, and it is proportional to N. Therefore, we can expect the enhanced SK capacity in the proposed system due to the increased randomness introduced by the IRS. Finally, the SK capacity of the proposed scheme, C_p across all L slots is upper bounded as follows [18]:

$$\begin{aligned} C_p &\leq \frac{1}{S}\sum_{s=1}^{S} C_s \\ &= \frac{1}{S}\left[C_1 + \sum_{s=2}^{S} C_s\right] \\ &= \frac{1}{S}[C_1 + (S-1)C_s]. \end{aligned} \tag{12}$$

On the other hand, the SK capacity of the conventional scheme without IRS, is upper bounded by $C_c = C_1$.

The second performance measure to be investigated is the SK randomness, which is defined as the proportion of '1' in the generated binary initial key bit sequence, thus we have:

$$r = \frac{\sum^{n_q}\sum_{i=1}^{p}[b_i = 1]}{n_q p}, \tag{13}$$

where n_q is the total number of investigated probe rounds for the estimation. The closer to 0.5 the r, the better the randomness of the key. In other word, when the proportion of '1' and '0' in the key sequence is uniform, the randomness of the key is better.

The third performance measure is the initial key disagreement probability. Suppose that Alice and Bob convert each of their estimations $\hat{h}_A$ and $\hat{h}_B$ to $(b_{A,1}, b_{A,2}, \cdots, b_{A,p})$ and $(b_{B,1}, b_{B,2}, \cdots, b_{B,p})$, respectively, then the initial key disagreement probability, p_d is the probability of inconsistent bits between Alice and Bob. Therefore, it is defined as the ratio of the number of inconsistent bits to the key sequence length as follows:

$$p_d = \frac{\sum^{n_q}\sum_{i=1}^{p} b_{A,i} \oplus b_{B,i}}{n_q p}. \tag{14}$$

The last performance measure is effective key length K_l (bits/block). It describes the length of error-free SK that can be generated per block, and it can be represented as follows:

$$K_l = p(1 - p_d)\frac{L}{2}. \tag{15}$$

4.2. Simulation Results and Discussions

Before we compare the secrecy performance measures presented in the previous section, the computational complexities of the proposed and conventional PQ methods are compared in terms of the number of the required operations for PQ. As shown in Table 1, the proposed method requires linearly increasing complexity by p, and it requires a constant number of operations regardless of the estimated CSI value. On the other hand, the conventional PQ method requires exponentially increasing complexity by p, and it requires one to maximum of 2^p comparisons, resulting in $(2^p/2)$ comparisons on average. Figure 7 illustrates this.

Table 1. Comparisons of computations required for quantization.

2^p**-Level PQ Methods**	**Required Operations (Average, Maximum)**
Conventional PQ [15]	comparisons $((2^p/2), 2^p)$
Proposed PQ	p linear operations in (8) (p,p)

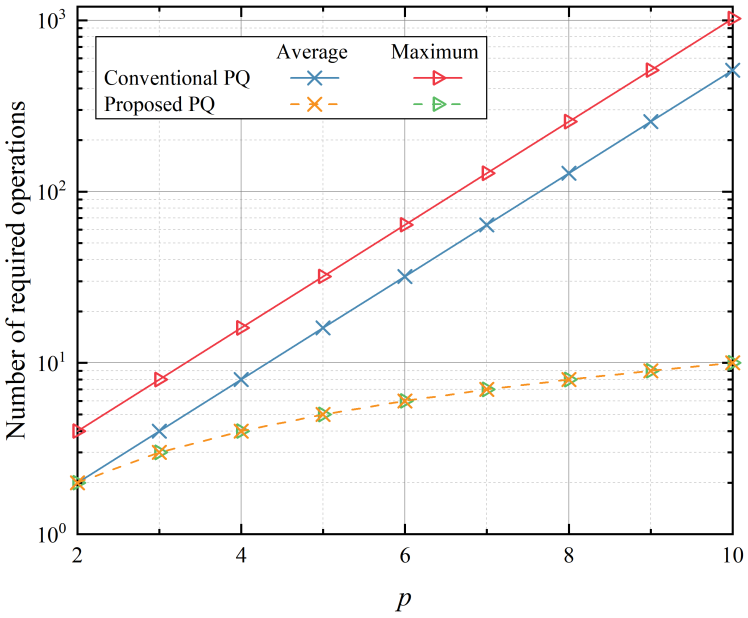


Figure 7. Comparison of computations for quantization in terms of the number of required operations.

Next, we compare performance simulation results of the proposed scheme to that of the conventional schemes. First, Figure 8 shows the SK capacity variation by signal-to-noise ratio (SNR), and the number of probe rounds is set to $L = 20$. It is evident that the SK capacity of the proposed scheme with IRS assistance is higher than the conventional one, and the SK capacity increases with an increase in the number of IRS elements N. This highlights the positive aspects of using IRS in wireless communication systems, which boosts the SK capacity and makes transmission more efficient.

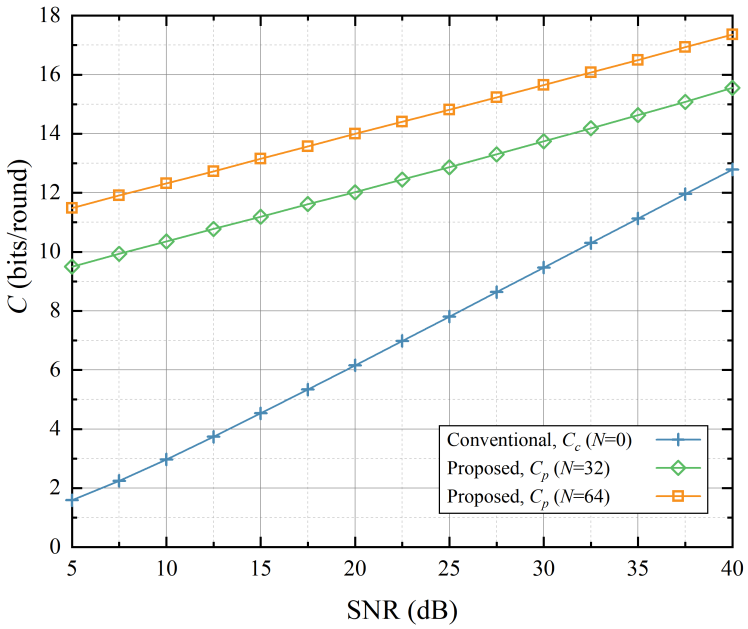


Figure 8. Comparison of SK capacity, C.

Second, Figure 9 compares the SK randomness, r, $L = 20$. We can see that the SK randomness of all PQ methods remains stable, showing almost a constant value of about 0.5 across all the investigated SNR ranges. In other words, the assistance of IRS in the proposed method does not alter randomness performance. This is primarily due to the property of PQ having a uniform PDF and its quantization regions being equally probable

and uniformly distributed. Consequently, both '1' and '0' are uniformly quantized, leading to the preservation of SK randomness.

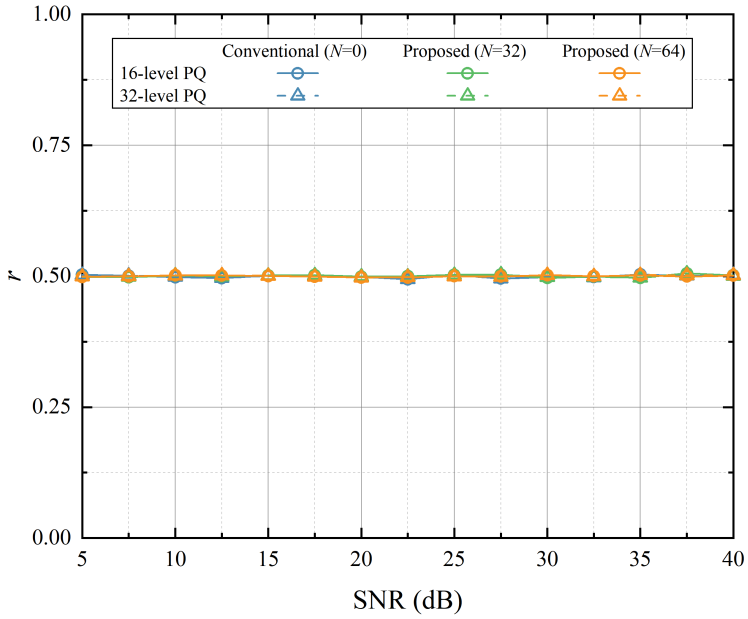


Figure 9. Comparison of SK randomness, r.

Figure 10 compares the initial key disagreement probabilities, $L = 20$. As shown in the figure, when the quantization level is lower, the initial probability of disagreement becomes smaller due to the increased area of each quantization region. Consequently, this decrease in the likelihood of mismatching quantization regions between Alice and Bob ultimately leads to fewer inconsistent bits within the sequence. redGiven the quantization level, the proposed PQ outperforms the conventional PQ method without IRS. It can also be seen that as the number of IRS elements N increases, the disagreement probability decreases. This illustrates the role of IRS in significantly enhancing channel reliability as well.

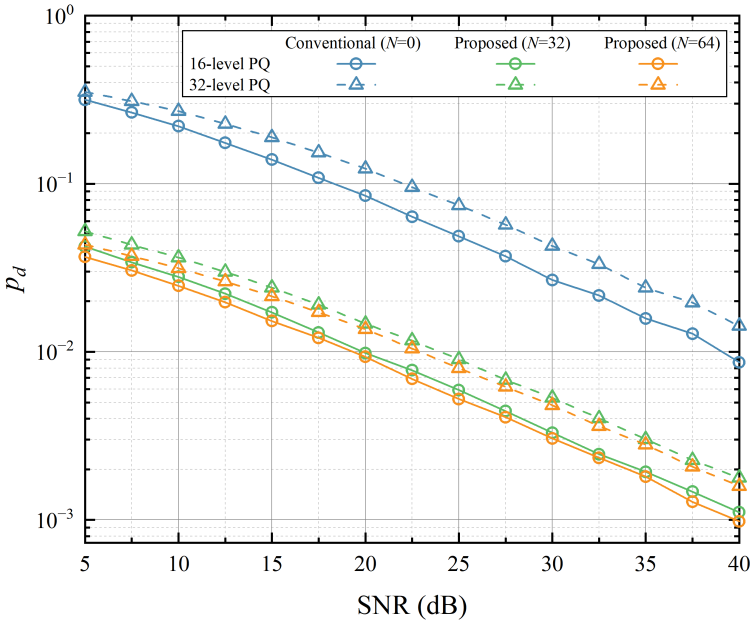


Figure 10. Comparison of initial key disagreement probability, p_d.

Figure 11 compares the effective key length, K_l of the proposed method with that of the conventional method, when the number of probe rounds is set to 10 and 20, i.e., $L = 20$ and $L = 40$. It is evident that higher quantization levels result in longer effective key length. Furthermore, when compared to the conventional PQ without IRS, as L increases, our proposed scheme with IRS demonstrates superior performance, with its effective key length increasing with the rise of N. While the increase in quantization levels leads to higher initial key disagreement probability, higher level quantization allows for the generation of longer effective key length in a single quantization process, thereby enhancing transmission speed and efficiency. In the static environment, the channel features extracted by Alice and Bob have low correlation and high initial key disagreement rate, thus affecting the effectiveness of the subsequent information reconciliation stage. Configuring the IRS as a new random source and extracting phase information means that our proposed scheme can obtain initial keys with a lower key disagreement probability, making information reconciliation easier to achieve during SK generation.

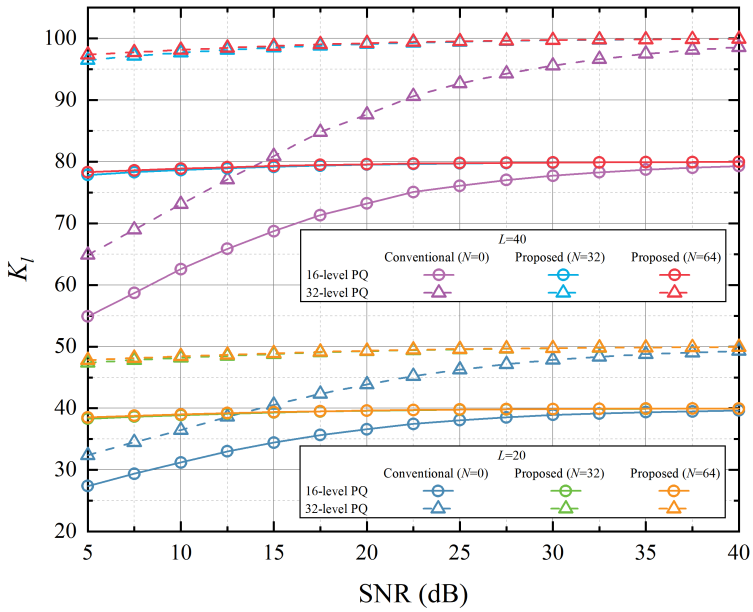


Figure 11. Comparison of effective key length, K_l.

5. Conclusions

In this paper, we proposed an efficient IRS-assisted physical layer SK generation scheme with random phase shifts in static environment. By extracting the phase information from the combined channel estimation from both sides of the legitimate communication parties, a better random key sequence can be generated. Specifically, this paper proposed a simple and computationally efficient PQ method by using a symmetric bit allocation, which can be easily extended to any 2^p-level quantization scheme and can be universally applied. Simulation results demonstrated that the proposed scheme can improve various performance measures including the SK capacity, effective key length, and the SK disagreement probability, without sacrificing the randomness. By adopting the IRS-assisted hybrid approach, we can achieve about 21% of enhancement in SK capacity, and an order of enhancement of initial key disagreement probability performance. Specifically, our proposed scheme could be able to generate almost constant effective key lengths regardless of SNR, being an attractive solution for low SNR conditions.

Author Contributions: Conceptualization, S.K. and M.Z.; methodology, Z.Z.; validation, S.K., M.Z. and Z.Z.; formal analysis, Z.Z.; data curation, Z.Z.; writing—original draft preparation, Z.Z.; writing—review and editing, S.K. and M.Z.; supervision, S.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (NRF-2021R1A2C1003121).

Data Availability Statement: Not applicable.

Acknowledgments: The authors extend their appreciation to the Yangzhou University Graduate International Academic Exchange Fund Project (YZUF2022204) and the Young Backbone Teachers Project of Yangzhou University.

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

Abbreviations

The following abbreviations are used in this manuscript:

SK	Secret key
LOS	Line-of-sight
IoT	Internet of Things
IRS	Intelligent reflecting surface
CSI	Channel state information
PQ	Phase quantization
TDD	Time-division duplex
AWGN	Additive white Gaussian noise
AVQ	Absolute value-based quantization
DVQ	Difference value-based quantization
PDF	Probability density function
PSK	Phase shift keying
LS	Least square
SNR	Signal-to-noise ratio

References

1. Maurer, U.M. Secret key agreement by public discussion from common information. *IEEE Trans. Inf. Theory* **1993**, *39*, 733–742. [CrossRef]
2. Matthé, M.; Chorti, A. Analysis of the mutual information of channel phase observations in line-of-sight scenarios. *Entropy* **2023**, *25*, 1038. [CrossRef] [PubMed]
3. Wu, Q.; Zhang, R. Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network. *IEEE Commun. Mag. Jan.* **2019**, *58*, 106–112. [CrossRef]
4. Wu, Q.; Zhang, R. Beamforming optimization for wireless network aided by intelligent reflecting surface with discrete phase shifts. *IEEE Trans. Commun.* **2019**, *68*, 1838–1851. [CrossRef]
5. 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]
6. 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]
7. Ji, Z.; Yeoh, P.L.; Zhang, D.; Chen, G.; Zhang, Y.; He, Z.; Yin, H. Secret key generation for intelligent reflecting surface assisted wireless communication networks. *IEEE Trans. Veh. Technol.* **2021**, *70*, 1030–1034. [CrossRef]
8. 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.
9. Lu, X.; Lei, J.; Shi, Y.; Li, W. Intelligent reflecting surface assisted secret key generation. *IEEE Signal Process. Lett.* **2021**, *28*, 1036–1040. [CrossRef]
10. Zhang, J.; Rajendran, S.; Sun, Z.; Woods, R.; Hanzo, L. Physical layer security for the Internet of Things: Authentication and key generation. *IEEE Wirel. Commun.* **2019**, *26*, 92–98. [CrossRef]
11. Ye, C.; Reznik, A.; Shah, Y. Extracting secrecy from jointly Gaussian random variables. In Proceedings of the 2006 IEEE International Symposium on Information Theory, Seattle, WA, USA, 9–14 July 2006; pp. 2593–2597.
12. Zeng, K.; Wu, D.; Chan, A.; Mohapatra, P. Exploiting multiple-antenna diversity for shared secret key generation in wireless networks. In Proceedings of the 2010 Proceedings IEEE INFOCOM, San Diego, CA, USA, 14–19 March 2010; pp. 1–9.
13. Sayeed, A.; Perrig, A. Secure wireless communications: Secret keys through multipath. In Proceedings of the 2008 IEEE International Conference on Acoustics, Speech and Signal Processing, Las Vegas, NV, USA, 31 March–4 April 2008; pp. 3013–3016.

14. Shehadeh, Y.E.H.; Alfandi, O.; Tout, K.; Hogrefe, D. Intelligent mechanisms for key generation from multipath wireless channels. In Proceedings of the 2011 Wireless Telecommunications Symposium (WTS), New York, NY, USA, 13–15 April 2011; pp. 1–6.
15. Wang, Q.; Su, H.; Ren, K.; Kim, K. Fast and scalable secret key generation exploiting channel phase randomness in wireless networks. In Proceedings of the 2011 Proceedings IEEE INFOCOM, Shanghai, China, 10–15 April 2011; pp. 1422–1430.
16. Xiao, S.; Guo, Y.; Huang, K.; Jin, L. Cooperative group secret key generation based on secure network coding. *IEEE Commun. Lett.* **2018**, *22*, 1466–1469. [CrossRef]
17. Aldaghri, N.; Mahdavifar, H. Physical layer secret key generation in static environments. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 2692–2705.
18. Lu, T.; Chen, L.; Zhang, J.; Cao, K.; Hu, A. Reconfigurable intelligent surface assisted secret key generation in quasi-static environments. *IEEE Commun. Lett.* **2021**, *26*, 244–248.
19. Zhang, M.; Kim, S.; Kim, Y. Universal soft decision demodulator for M-ary adaptive modulation systems. In Proceedings of the 2012 18th Asia-Pacific Conference on Communications (APCC), Jeju, Republic of Korea, 15–17 October 2012; pp. 574–578.
20. Zhang, M.; Kim, S. Universal soft demodulation schemes for M-ary phase shift keying and quadrature amplitude modulation. *IET Commun.* **2016**, *10*, 316–326.
21. Rottenberg, F.; Nguyen, T.; Dricot, J.-M.; Horlin, F.; Louveaux, J. CSI-based versus RSS-based secret-key generation under correlated eavesdropping. *IEEE Trans. Commun.* **2021**, *69*, 1868–1881. [CrossRef]