AUT Journal of Modeling and Simulation

AUT J. Model. Simul., 56(1) (2024) 117-126
DOI: 10.22060/miscj.2023.22720.5342

# Channel Phase Based Secret Key Generation: Untrusted Relaying or Not?

Mohammadreza Keshavari[1], Hadi Zayyani[2], Ali Kuhestani[2]*, and Hossein Ahmadi[3]

[1] Iran Telecommunication Research Center (ITRC), Tehran, Iran.
[2] Faculty of Electrical and Computer Engineering, Qom University of Technology, Qom, Iran.
[3] Department of Electronic and Telecommunications, Polytechnic University of Turin, Italy.

**ABSTRACT:** Compared to traditional cryptography methods, physical layer secret key generation (PLSKG) can be more efficient and well-suited for Internet-of-Things (IoT) owing to its lightweight nature and scalability. In PLSKG, schemes utilizing local random generators are employed to achieve a high key generation rate. In this study, it is proposed a high-rate PLSKG in the presence of an untrusted relay. This untrusted relay assists the PLSKG process but cannot determine the secret key. We select channel probe signals from PSK signals and adopt a multi-bit quantizer at the receiver to enhance practicality. Additionally, we utilize quantization with guard bands (GB) to decrease the key error rate. We calculate the performance and security of the proposed PLSKG scheme under these conditions. Our results indicate that the relay, receiving superimposed signals from Alice and Bob, cannot ascertain the secret key. Finally, we compare the proposed PLSKG with a direct scenario where the relay is omitted during key generation.

**Review History:**

Received: Oct. 01, 2023
Revised: Oct. 31, 2023
Accepted: Nov. 02, 2024
Available Online: Sep. 05, 2024

**Keywords:**

Secret Key Generation
Untrusted Relay
Direct Transmission
Channel Phase

## 1- Introduction

Given the extensive number of point-to-point communications on the Internet of Things (IoT), conventional security techniques have become increasingly inadequate [1]. Lightweight and secure security methods, like physical layer secret key generation (PLSKG), emerge as promising alternatives to computationally intensive methods, especially in 6G networks [2], [3]. Recently, both academic [3-5] and industrial researchers [6], [7] have focused on PLSKG. This method leverages a shared random source, to generate keys between end parties. Key generation can be based on various channel characteristics, including the phase of the communication channel, received signal power (RSS), the whole channel state information (CSI), and other features [8-10]. While RSS commonly exist in commercial communication instruments and has been the focus of numerous studies [3], it tends to yield low key generation rates in static or near-to-static environments. Moreover, RSS is susceptible to several attacks, including wiretapping [11], man-in-the-middle [12], and predictable channel attacks [13]. Conversely, the channel phase offers a robust alternative, providing high entropy due to its significant variations.

For scenarios like short-range communications, satellite communications, and communications over millimeter wave bands, the signal-to-noise ratio (SNR) is closely linked to line-of-sight (LoS) paths, eliminating fading. Here, a high entropy common source is crucial. For example, prior work [14] has utilized the Doppler frequency shift inspired by spacecraft mobility to generate the secret keys. Another enhancement technique for PLSKG is cooperative relaying, which is particularly beneficial when there is a considerable distance between the transmitter and receiver. An intriguing area of study is the untrusted relaying scenario, where a relay, acting as a legal node, aids source-to-destination communications but may also passively eavesdrop [15]. This situation is common in large-scale wireless networks like wireless sensor networks (WSN). As an example, the previous research [15] proposed a PLSKG scheme using the CSI of Alice-relay and Bob-relay channels. Notably the performance metrics of key generation, like key mismatch rate (KMR) and key discarding rate (KDR) were not thoroughly examined in [15].

In this paper, we design and analyze a novel PLSKG scheme for cooperative communications utilizing an untrusted relay applicable to free-space environments. Unlike the new paper [15], our scheme utilizes the phase of the channel as the common random source among Alice, Bob, and the relay to extract the key. To enhance the entropy, Alice and Bob inject discrete random phases, which are practical and straightforward to implement. Specifically, we employ PSK modulation to inject discrete random phases. To minimize KMR, different quantization techniques [16], [17] could be adopted, while we use the guard band (GB) method with a

*Corresponding author's email: kuhestani@qut.ac.ir

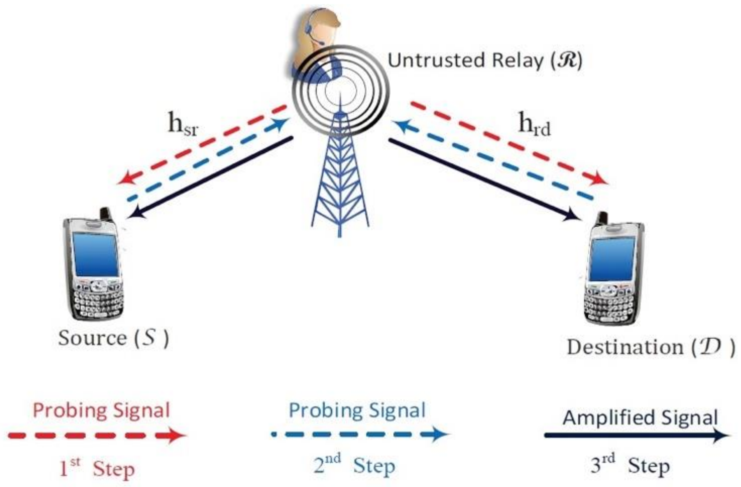

**Fig. 1. The proposed key generation scheme**

multi-bit quantizer. For this system model, a new closed-form solution for the KMR is calculated. In the GB-based approach, only samples located within quantization regions (QRs) are used for key generation, excluding those in GBs. Based on this approach, we also calculate the KDR criterion. Furthermore, we extend our proposed PLSKG to a multi-hop untrusted relay scenario and compare it with a direct scenario where the relay is omitted from the key generation process. Numerical examples provide valuable insights for implementing a practical PLSKG for communication systems.

## 2- System Model

As illustrated in Fig.1, the system model under investigation is a two-hop relaying system. In this network, confidential data is sent from a source (Alice, S) to a destination (Bob, D) with the assistance of an amplify-and-forward (AF) untrusted relay (R). The nodes in this system model are equipped with a single antenna and also they communicate in a half-duplex mode. There is no powerful direct link between S and D due to the considerable distance between the legitimate nodes, necessitating the use of cooperative relaying despite the relay being untrusted. Protecting the key from potential attacks by the untrusted relay is crucial, even as it assists in key generation.

Our focus is on key generation from the phase of the channel. In this scenario, it is assumed that the source and destination choose a symbol by random from an *M*-PSK modulation scheme, where *M* is the modulation order. For $u \in \{S, D\}$, the phase of the sent symbol is given by $\Phi_{u,i} = \frac{2\pi}{M} i_u$, where $i_u = 0, 1, ..., M-1$ and $i_u$ as the index of the symbol, chosen stochastically from a uniform distribution. The loss and the phase of the source-relay link are illustrated by $\alpha_{sr}$, and $\Phi_{sr}$, respectively, $\alpha_{rd}$ and $\Phi_{rd}$ represent the corresponding measures for the relay-destination channel. It is assumed that the noise is white Gaussian with zero mean and variance $\sigma_n^2$ across all nodes.

Direct quantization typically produces a high error rate, necessitating robust forward error correction channel codes to adjust the phases. We employ *M*-PSK quantization with GBs to mitigate the probability of key error. Generally, the *i*'th guard bound $\mathrm{GB}_i$ and the *i*'th quantization region $QR_i$, defined as:

$$GB_i = \left[\frac{2\pi}{M}i + \frac{\pi}{M} - \frac{\Psi}{2}, \frac{2\pi}{M}i + \frac{\pi}{M} + \frac{\Psi}{2}\right] \tag{1}$$

$$QR_i = \left[\frac{2\pi}{M}i - \frac{\pi}{M} + \frac{\Psi}{2}, \frac{2\pi}{M}i + \frac{\pi}{M} - \frac{\Psi}{2}\right] \tag{2}$$

in which $\varnothing$ is the width of GBs. The necessity for GBs comes from the fact that phases near boundaries have the potential to provide incorrect decisions. Consequently, an effective quantization method involves discarding phase samples located in the boundary regions.

From the security perspective, a critical question is how each node (source or destination) informs the other (destination or source) about discarding a sample without compromising security. We note that the GBs are also equiprobable because the quantization regions are equiprobable. During the public discussion phase, each node can specify which probings are quantized and which are discarded. Performance-wise, larger GBs reduce the key error probability by discarding more suspicious channel probings. As such, a trade-off between performance and efficiency has appeared. The goal is to achieve the maximum number of secret keys while targeting a specific $P_{SKD}$.

## 3- Proposed PLSKG Scheme

For the proposed PLSKG scheme, *M*-PSK quantization is utilized. The usually used grey coding method is employed to convert the quantized symbols into binary strings for both the source and destination. The keys generated in each probing instance are denoted as $k_S$ and $k_D$ For the source and destination, respectively. After *L* probing instances, the key segments are combined, resulting in each node's final keys, $k_S$ and $k_D$ .

The key generation process, illustrated in Fig. 1, proceeds as what follows:

1) ***First phase***: The relay transmits a high-power pilot, enabling the source and destination to capture their respective channels accurately.

2) ***Second phase***: The source and destination concurrently send signals with the amplitudes of $\sqrt{P_S}$ and $\sqrt{P_D}$ and the random phases of $\Phi_S$ and $\Phi_D$ , respectively.

3) ***Third phase***: The AF relay broadcasts its received message with the gain of G. Subsequently, the source cancels its self-interference. The SNR of the received signal at the source is then given by:

$$\gamma_S = \frac{\mathrm{G}^2 \alpha_{sr}^2 \alpha_{rd}^2 P_D}{\sigma_{T,S}^2} \tag{3}$$

where $\sigma_{T,S}^2 = \sigma_n^2 \left(1 + G^2 \alpha_{sr}^2\right)$. According to [14], the estimated phase at the source for high SNR conditions is:

$$\widehat{\Phi}_S = \Phi_\mathrm{D} + \Phi_{sr} + \Phi_{rd} + \epsilon_S \tag{4}$$

where $\in_S$ is Gaussian with zero mean and variance $\sigma_{\in_S}^2 = \sqrt{\frac{2}{2\gamma_S + 1}}$. Given $\Phi_{sr}$ , the source has access to $\Phi_\mathrm{D} + \Phi_{rd} + \in_S$ . Thus, the source can access both $\Phi_S + \Phi_{sr}$ and $\Phi_\mathrm{D} + \Phi_{rd} + \in_S$ . A similar analysis applies to the destination node, which can access both. $\Phi_S + \Phi_{sr} + \in_D$ and $\Phi_\mathrm{D} + \Phi_{rd}$ , where $\in_D$ is Gaussian with zero mean and variance $\sigma_{\in_D}^2 = \sqrt{\frac{2}{2\gamma_D + 1}}$ The SNR at the destination is given by $\gamma_D = \frac{G^2 \alpha_{sr}^2 \alpha_{rd}^2 P_S}{\sigma_{T,D}^2}$ where $\sigma_{T,D}^2 = \sigma_n^2 \left(1 + G^2 \alpha_{rd}^2\right)$. After quantizing the aforementioned quantities and combining them, the equal key for the source and destination can be represented by:

$$\begin{aligned} k_S &= Q_{MPSK}\left(Q_S^{(1)}\right) \| Q_{MPSK}\left(Q_S^{(2)}\right) = k_S^{(1)} \| k_S^{(2)} \\ k_D &= Q_{MPSK}\left(Q_D^{(1)}\right) \| Q_{MPSK}\left(Q_D^{(2)}\right) = k_D^{(1)} \| k_D^{(2)} \end{aligned} \tag{5}$$

where $\Phi_S^{(1)} = \Phi_S + \Phi_{sr}$ , $\Phi_S^{(2)} = \Phi_D + \Phi_{rd} + \in_S$ , $\Phi_D^{(1)} = \Phi_S + \Phi_{sr} + \in_D$ , and $\Phi_D^{(2)} = \Phi_D + \Phi_{rd}$ . The quantization function can be described as

$$Q_{MPSK}(x) = \frac{x}{\frac{2\pi}{M}} + \frac{1}{2}$$

The key segments $k_S^{\cdot(1)}$ , $k_S^{(2)}$ , $k_D^{(1)}$ , and $k_D^{(2)}$ are binary strings with $\log_2 M$ bits each. The concatenated keys $k_S$ or $k_D$ are binary ones with $K = 2\log_2 M$ bits. It is evident that for phase noises $\in_S$ and $\in_D$ equal to zero, the source and destination achieve an equal key.

A necessary consideration is that, when GBs exist, the source and destination must compute the quantities mentioned below:

$$k_m^{(i)} \triangleq \frac{\Phi_m^{(i)}}{\frac{2\pi}{M}} + \frac{1}{2}, k_m^{+(i)} \triangleq \frac{\Phi_m^{(i)} + \frac{\Psi}{2}}{\frac{2\pi}{M}} + \frac{1}{2}, k_m^{-(i)} \triangleq \frac{\Phi_m^{(i)} - \frac{\Psi}{2}}{\frac{2\pi}{M}} + \frac{1}{2}$$

where $i \in \{0, 1, ..., M-1\}$ and $m \in \{\mathrm{S}, \mathrm{D}\}$. After that, the source and destination obtain their keys as follows:

$$k_m^{(i)} = \begin{cases} k_m^{(i)} & if \quad k_m^{+(i)} = k_m^{-(i)} \\ \emptyset & \quad otherwise \end{cases} \tag{6}$$

where $\phi$ indicates that the nodes ignore the obtained sequences. As mentioned earlier, for the case of $\phi$, the obtained phase within the GBs are not used for PLSKG.

## 4- Performance Study of the Proposed PLSKG Scheme

In this section, the probability of discarding $P_{dis}$ and the probability of key mismatch $P_{km}$ are analytically studied.

### A. Derivation of the discarding probability

We define the total GB as $\mathrm{GB} = \bigcup_{i=0}^{M-1} GB$ . The probability of discarding is then given by:

$$\begin{aligned} P_{dis} = Pr\Big\{ &\left(\Phi_S^{(1)}\ or\ \Phi_D^{(1)} \in GB\right) \\ or\ &\left(\Phi_S^{(2)}\ or\ \Phi_D^{(2)} \in GB\right)\Big\} \end{aligned} \tag{7}$$

Let $A = \left(\Phi_S^{(1)}\, or\, \Phi_D^{(1)} \in GB\right)$ and $B = \left(\Phi_S^{(2)}\, or\, \Phi_D^{(2)} \in GB\right)$ , then we have $P_{dis} = P(A) + P(B) - P(A)P(B)$, where P(A) and P(B) are achieved similarly due to the similar nature of the phases, and P(A ∩ B) = P(A)P(B) because the events A and B are independent. Thus,

$$\begin{aligned}&\mathrm{P(A)} = \mathrm{Pr}\left\{\Phi_S^{(1)}\ or\ \Phi_D^{(1)}\ \in GB\right\} = \\ &Pr\left\{\Phi_S^{(1)} \in GB\right\} + Pr\left\{\Phi_D^{(1)}\ \in GB\right\} \\ &-Pr\left\{\Phi_S^{(1)}, \Phi_D^{(1)}\ \in GB\right\}\end{aligned} \tag{8}$$

The first probability $Pr\left\{\Phi_S^{(1)} \in GB\right\}$ is given by:

$$\begin{aligned}&Pr\left\{\Phi_S^{(1)} \in GB\right\} = Pr\left\{\Phi_S^{(1)} \in \bigcup_{i=0}^{M-1} GB\right\} = \\ &\sum_{i=0}^{M-1} Pr\left\{\Phi_S^{(1)} \in GB_i\right\} = \frac{M\Psi}{2\pi}\end{aligned} \tag{9}$$

since the GBs are disjoint and $\Phi_S^{(1)} = \Phi_S + \Phi_{sr}$ is uniformly distributed. Additionally, the second probability in (8), $Pr\left\{\Phi_D^{(1)} \in GB\right\}$, is equal to:

$$\sum_{i=0}^{M-1} Pr\left\{\Phi_D^{(1)} \in GB_i\right\} = MPr\left\{\Phi_D^{(1)} \in GB_0\right\} = MP_0 \tag{10}$$

because the GBs are symmetric and the $\Phi_D^{(1)}$ follows a uniform plus Gaussian distribution. Thus,

$$\begin{aligned}&P_0 \triangleq Pr\left\{\Phi_D^{(1)} \in GB_0\right\} = \\ &Pr\left\{\frac{\pi}{M} - \frac{\Psi}{2} \le \Phi_S + \Phi_{sr} + \epsilon_D \le \frac{\pi}{M} + \frac{\Psi}{2}\right\}\end{aligned} \tag{11}$$

To calculate this probability, we find the generalized probability $F(\alpha,\beta) = Pr\{\alpha \le X + Y \le \beta\}$ where $X = \Phi_S + \Phi_{sr} \sim$ Uniform$(0, 2\pi)$, $Y = \in_D \sim$ N$(0, \sigma_\in^2)$, and X and Y are independent. Therefore, $P_0 = F\left(\frac{\pi}{M} - \frac{Ø}{2}, \frac{\pi}{M} + \frac{Ø}{2}\right)$. To find $F(\alpha,\beta)$, we have:

$$F(\alpha,\beta) = Pr\{\alpha \le Z = X + Y \le \beta\} = F_Z(\beta) - F_Z(\alpha) \tag{12}$$

where $F_Z(\alpha)$ is the cumulative distribution function (CDF) of Z = X + Y. Now, to compute the CDF,

$$\begin{aligned}F_Z(\alpha) &= Pr\{Z \le \alpha\} = Pr\{X + Y \le \alpha\} \\ &= \int_{-\infty}^{+\infty}\int_{-\infty}^{\alpha - x} f_X(u) f_Y(v)\, dv du \\ &= \int_0^{2\pi}\int_{-\infty}^{\alpha - x} \frac{1}{2\pi} f_Y(v)\, dv du \\ &= \frac{1}{2\pi}\int_0^{2\pi} G_Y(\alpha - x)\, dx\end{aligned} \tag{13}$$

where $G_Y(.)$ is the CDF of $Y = \in_D \sim N(0, \sigma_\in^2)$, a known function in the probability theory. Specifically, $G_Y(r) = G_Y\left(\frac{r}{\sigma_{\grave{o}}}\right)$, where $G_Y(.)$ is the CDF of a normalized gaussian disttribution $N(0, 1)$.

To compute the third probability term in (8), $\mathrm{Pr}\left\{\Phi_S^{(1)}, \Phi_D^{(1)} \in GB\right\}$,

$$\begin{aligned}&\mathrm{Pr}\left\{\Phi_S^{(1)}, \Phi_D^{(1)}\ \in GB\right\} \\ &= \sum_{i=0}^{M-1} \mathrm{Pr}\left\{\Phi_S^{(1)}, \Phi_D^{(1)}\ \in GB_i\right\} \\ &= MPr\left\{\Phi_S^{(1)}, \Phi_D^{(1)}\ \in GB_0\right\} = MP_1\end{aligned} \tag{14}$$

where $P_1 = Pr\left\{\Phi_S^{(1)}, \Phi_D^{(1)} \in GB_0\right\}$. To calculate $P_1$,

$$P_1 = Pr\{(\Phi_S + \Phi_{sr}) \in GB_0, (\Phi_S + \Phi_{sr} + \epsilon_D) \in GB_0\} \tag{15}$$

To obtain $P_1$, we calculate the joint probability $Pr\{\alpha \le X \le \beta, \alpha \le Z = X + Y \le \beta\}$. Thus,

$$\begin{aligned}P_1 = F_{XZ}(\beta,\beta) - F_{XZ}(\beta,\alpha) - F_{XZ}(\alpha,\beta) \\ + F_{XZ}(\alpha,\alpha)\end{aligned} \tag{16}$$

where $F_{XZ}(\alpha,\beta)$ is the joint CDF of X and Z. To obtain this joint CDF, one can write

$$\begin{aligned}F_{XZ}(\alpha,\beta) &= Pr\{X \le \alpha, Z = X + Y \le \beta\} \\ &= \int_{-\infty}^{\alpha}\int_{-\infty}^{\beta - x} f_X(x) f_Y(y)\, dy dx \\ &= \frac{1}{2\pi}\int_0^{\alpha} G_Y(\beta - \alpha)\, dx\end{aligned} \tag{17}$$

where $G_Y(.)$ is the CDF of a Gaussian $Y \sim N(0, \sigma_{\epsilon}^2)$. Putting it all together, P(A) in (8) can be expressed as:

$$P(A) = \frac{M\Psi}{2\pi} + MP_0 - MP_1 \tag{18}$$

where $P_0$ and $P_1$ are obtained implicitly. To calculate a closed-form expression for $P_0$ and $P_1$, we define

$$\begin{aligned} h(\alpha, \beta, \sigma_\epsilon) &= \frac{1}{2\pi}\int_0^\alpha G_Y(\beta - \alpha)dx \\ &= \frac{1}{2\pi}\int_0^\alpha G_n\left(\frac{\beta - x}{\sigma_\epsilon}\right)dx \end{aligned} \tag{19}$$

For simplicity, we can omit the dependency on $\sigma_{ò}$. Then, $F_Z(\alpha) = h(2\pi, \alpha)$.
So,

$$P_0 = F_Z(\beta_0) - F_Z(\alpha_0) = h(2\pi, \beta_0) - h(2\pi, \alpha_0) \tag{20}$$

where $\alpha_0 = \frac{\pi}{M} - \frac{Ø}{2}$ and $\beta_0 = \frac{\pi}{M} + \frac{Ø}{2}$. Also,

$$P_1 = h(\beta_0, \beta_0) - h(\alpha_0, \beta_0) - h(\beta_0, \alpha_0) + h(\alpha_0, \alpha_0) \tag{21}$$

Thus, the probability P(A) in (18) is:

$$\begin{aligned} P(A) = \frac{M\Psi}{2\pi} &+ Mh(2\pi, \beta_0, \sigma_{\epsilon_D}) - Mh(2\pi, \alpha_0, \sigma_{\epsilon_D}) \\ &- Mh(\beta_0, \beta_0, \sigma_{\epsilon_D}) - Mh(\alpha_0, \beta_0, \sigma_{\epsilon_D}) \\ &- Mh(\beta_0, \alpha_0, \sigma_{\epsilon_D}) + Mh(\alpha_0, \alpha_0, \sigma_{\epsilon_D}) \end{aligned} \tag{22}$$

Similarly, the probability P(B) is:

$$\begin{aligned} P(B) = \frac{M\Psi}{2\pi} &+ Mh(2\pi, \beta_0, \sigma_{\epsilon_S}) - Mh(2\pi, \alpha_0, \sigma_{\epsilon_S}) \\ &- Mh(\beta_0, \beta_0, \sigma_{\epsilon_S}) - Mh(\alpha_0, \beta_0, \sigma_{\epsilon_S}) \\ &- Mh(\beta_0, \alpha_0, \sigma_{\epsilon_S}) + Mh(\alpha_0, \alpha_0, \sigma_{\epsilon_S}) \end{aligned} \tag{23}$$

Finally, the discarding probability is obtained using these values of P(A) and P(B).

### B. Derivation of the key mismatch probability

To obtain the key mismatch probability $P_{km}$, we first compute the key agreement probability $P_{ka}$. Thus,

$$P_{km} = 1 - P_{dis} - P_{ka} \tag{24}$$

The key agreement probability $P_{ka}$ is the probability that the phases are placed in equal quantization regions, and can be obtained as follows:

$$\begin{aligned} P_{ka} &= Pr\left\{\Phi_S^{(1)}, \Phi_D^{(1)} \in Same - QR, \Phi_D^{(2)} \in ame - QR\right\} \\ &= \sum_{i=0}^{M-1}\sum_{j=0}^{M-1} Pr\left\{\Phi_S^{(1)}, \Phi_D^{(1)} \right. \\ &\left. \in QR_i, \Phi_S^{(2)}, \Phi_D^{(2)} \in QR_j\right\} = \sum_{i=0}^{M-1}\sum_{j=0}^{M-1} \tilde{P}_i\tilde{P}_j \end{aligned} \tag{25}$$

where $\widetilde{P}_i \triangleq Pr\left\{\Phi_S^{(1)}, \Phi_D^{(1)} \in QR_i\right\}$. To calculate $\tilde{P}_i$, given the discontinuity of phases around 2π, we compute $\tilde{P}_0 = Pr\left\{\Phi_S^{(1)}, \Phi_D^{(1)} \in QR_0\right\}$ and $\widetilde{P}_i, i \neq 0$, separately. To obtain $\tilde{P}_0$, we divide the $QR_0$ to two disjoint regions of $QR_{01}$ and $QR_{02}$, shown in Fig. 3. Thus,

$$\begin{aligned} \widetilde{P}_0 &= Pr\left\{\Phi_S^{(1)} \in QR_0, \Phi_D^{(1)} \in QR_0\right\} \\ &= Pr\left\{\left(\Phi_S^{(1)} \in QR_{01} \middle| \Phi_S^{(1)} \in QR_{02}\right), \left(\Phi_D^{(1)}\right.\right. \\ &\left.\left. \in QR_{01} \middle| \Phi_D^{(1)} \in QR_{02}\right)\right\} \end{aligned} \tag{26}$$

If we denote the events $A_1 = \left\{\Phi_S^{(1)} \in QR_{01}\right\}$, $A_2 = \left\{\Phi_S^{(1)} \in QR_{02}\right\}$, $B_1 = \left\{\Phi_D^{(1)} \in QR_{01}\right\}$, and $B_2 = \left\{\Phi_D^{(1)} \in QR_{02}\right\}$, then,

$$\begin{aligned} \widetilde{P}_0 &= P[(A_1 \cup A_2) \cap (B_1 \cup B_2)] \\ &= P(A_1B_1) + P(A_1B_2) \\ &+ P(A_2B_1) + P(A_2B_2) \end{aligned} \tag{27}$$

Next, we calculate the probabilities in (27):

$$\begin{aligned} P_{11} &= P(A_1B_1) \\ &= Pr\left\{\Phi_S^{(1)} \in QR_{01}, \Phi_D^{(1)} \in QR_{01}\right\} \\ &= Pr\left\{0 \le \Phi_S^{(1)} \le \alpha_0, 0 \le \Phi_D^{(1)} \le \alpha_0\right\} \\ &= h(\alpha_0,\alpha_0) - h(\alpha_0,0) - h(0,\alpha_0) \\ &+ h(0,0) = h(\alpha_0,\alpha_0) - h(\alpha_0,0) \end{aligned} \tag{28}$$

where $h(0,x)=0$. For the next probability,

$$\begin{aligned} P_{12} &= P(A_1B_2) \\ &= Pr\left\{\Phi_S^{(1)} \in QR_{01}, \Phi_D^{(1)} \in QR_{02}\right\} \\ &= Pr\left\{0 \le \Phi_S^{(1)} \le \alpha_0, 2\pi - \alpha_0 \le \Phi_D^{(1)} \le 2\pi\right\} \\ &= h(\alpha_0,2\pi) - h(0,2\pi-\alpha_0) - h(\alpha_0,2\pi-\alpha_0) \\ &+ h(0,\alpha_0) = h(\alpha_0,2\pi) - h(\alpha_0,2\pi-\alpha_0) \end{aligned} \tag{29}$$

For the next probability,

$$\begin{aligned} P_{21} &= P(A_2B_1) = Pr\left\{\Phi_S^{(1)} \in QR_{02}, \Phi_D^{(1)} \in QR_{01}\right\} \\ &= Pr\left\{2\pi - \alpha_0 \le \Phi_S^{(1)} \le 2\pi, 0 \le \Phi_D^{(1)} \le \alpha_0\right\} \\ &= h(2\pi,\alpha_0) - h(2\pi-\alpha_0,\alpha_0) - h(0,2\pi) \\ &+ h(2\pi-\alpha_0,\alpha_0) = \\ &h(2\pi,\alpha_0) - h(2\pi-\alpha_0,\alpha_0) + h(2\pi-\alpha_0,\alpha_0) \end{aligned} \tag{30}$$

For the last probability,

$$\begin{aligned} P_{22} &= P(A_2B_2) = \\ &Pr\left\{\Phi_S^{(1)} \in QR_{02}, \Phi_D^{(1)} \in QR_{02}\right\} = \\ &Pr\left\{2\pi - \alpha_0 \le \Phi_S^{(1)} \le 2\pi, 2\pi - \alpha_0 \le \Phi_D^{(1)} \le 2\pi\right\} = \\ &h(2\pi,2\pi) - h(2\pi-\alpha_0,2\pi) - h(2\pi-\alpha_0,2\pi) \\ &+ h(2\pi-\alpha_0,2\pi-\alpha_0) \end{aligned} \tag{31}$$

Thus, from (27), the final probability is:

$$\widetilde{P}_0 = P_{11} + P_{12} + P_{21} + P_{22} \tag{32}$$

For $\widetilde{P}_i$ where $i \ne 0$,

$$\begin{aligned} \widetilde{P}_i\Big|_{i\ne0} &= Pr\left\{\Phi_S^{(1)} \in QR_i, \Phi_D^{(1)} \in QR_i\right\} \\ &= Pr\left\{\Phi_S^{(1)} \in QR_i\right\}. Pr\left\{\Phi_D^{(1)} \in QR_i \middle| \Phi_S^{(1)} \in QR_i\right\} \end{aligned} \tag{33}$$

For high SNR regime, the noise term can be neglected, and hence, the second conditional probability in (33) approaches one:

$$\widetilde{P}_i\Big|_{i\ne0} = \frac{\Psi}{2\pi} \tag{34}$$

Following (25) and after some computations,

$$P_{ka} = \left(\frac{\Psi(\mathrm{M}-1)}{2\pi} + \widetilde{P}_0\right)^2 \tag{35}$$

where $\widetilde{P}_0$ is obtained from (32).

*Note:* To compare the proposed untrusted relaying with direct key generation ignoring the relay, our scheme generates $2\log_2 M$ bits per key generation round, leading to $\frac{2\log_2 M}{3}$ bits, while the direct scenario generates $\frac{\log_2 M}{2}$ bits per round. This highlights the improved key generation rate of our proposed untrusted relaying scheme. From a security perspective, the untrusted relay cannot obtain information about the injected and channel phases due to the reception of superimposed signals from the source and destination. In contrast, an external eavesdropper in the direct scenario captures separate signals from the source and destination, increasing the risk of information extraction. Therefore, our proposed untrusted relaying PLSKG offers better security than the direct scenario.

## 5- Numerical Examples and Discussions

This part provides some engineering insights into the proposed key generation scheme using various figures. For all simulations, BPSK modulation with one-bit quantization is employed. The noise power is set to $\sigma_n^2 = 1$, and the relay gain is $G$ = 1. Additionally, we assume the relay is positioned equidistantly between Alice and Bob.

In Figure 2, the probability of KMR is plotted against the transmitted power ($P$) by Alice and Bob. The distances between Alice and Bob are set to $d$ = 5 and $d$ = 10. As observed, the KMR increases with the distance between Alice and Bob, since the received SNRs at the nodes are decreased and consequently, the key errors increase. The figure also

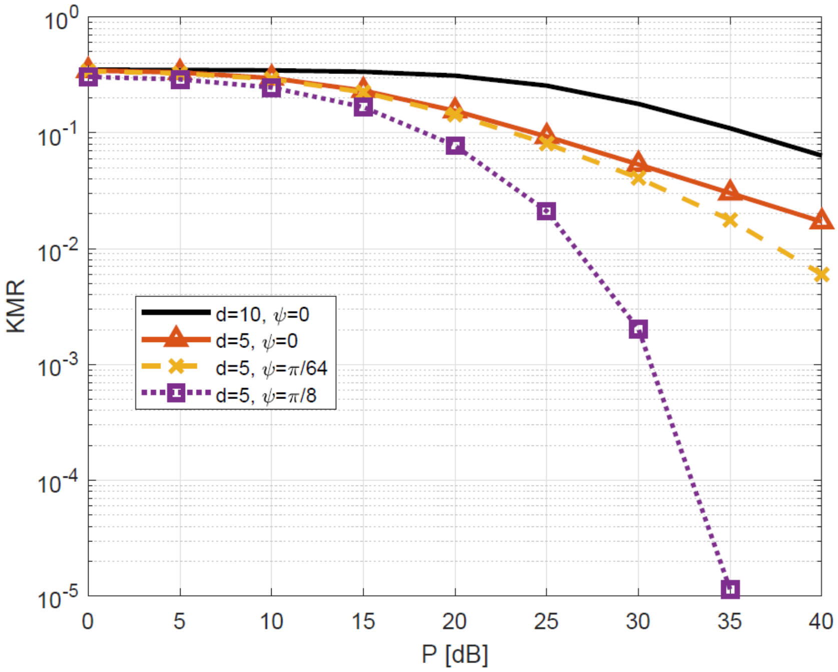

**Fig. 2. Key mismatch rate versus the source and destination transmit power**

illustrates the impact of the GB Ø . The presence of Ø in the key generation protocol reduces the KMR by discarding samples around decision boundaries. However, this also reduces the KGR because more samples are discarded. A critical design insight from this figure is that if the channel coding applied in the key generation can correct an error rate of, for instance, 0.1, and the nodes can transmit up to $P = 23$ dBW, a receiver with Ø $= \pi/64$ is preferable (compared to Ø $= \pi/8$). This choice offers a higher KGR while maintaining a bit error rate below 0.1, which can be compensated by coding.

We also note that growing the GB Ø , decreases the KMR and the required key rate. Therefore, selecting a proper Ø is crucial to balance these two requirements. As an example, in a cellular system, the base station with high error correction capabilities and a high key generation rate requirement, a smaller Ψ is preferred as KMR is not a primary concern. In applications like IoT nodes that have low data processing capabilities with the requirement of a low key rate, the KMR efficiency must be prioritized. As such, the GB Ψ should be enlarged accordingly.

Figure 3 plots the probability of discarding against $P$ for different values of Ψ. It is evident that the discarding rate increases with larger GB values. The figures suggest that even with increased power ($P$), the discarding rate does not significantly decrease.

Figure 4 compares the KMR of phase and amplitude features for obtaining secret keys. This figure is plotted for a direct communication scenario, excluding the untrusted relay for key generation. Here, the GB is set to zero. As seen, the channel phase outperforms the amplitude channel regarding KMR. Specifically, for KMR$=0.04$, approximately 1 dB is saved when using the channel phase feature.

## 6- Conclusion

In this study, a PLSKG method was suggested in the existence of an untrusted relay. The probing signals were designed using PSK signals, and a multi-bit quantizer was employed at the receiving nodes. To decrease the KMR, we incorporated quantization with GBs for extracting the key. We derived expressions for key agreement rate, KMR, and KDR per channel probe for this scenario. Our simulation results provided valuable insights behind the proposed GB-limited PLSKG method, highlighting its effectiveness and practicality for secure communication in the existence of untrusted relays.

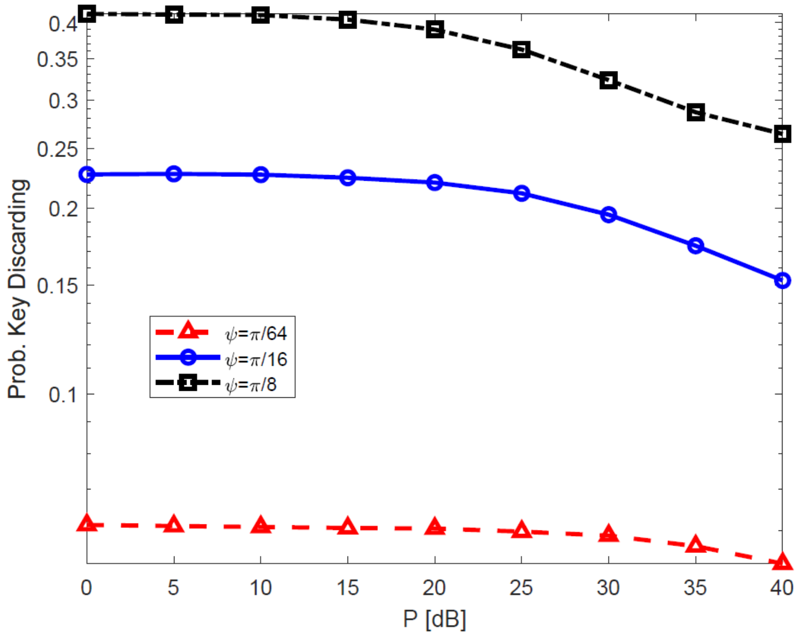

**Fig. 3. Key discarding rate versus the source and destination transmit power.**

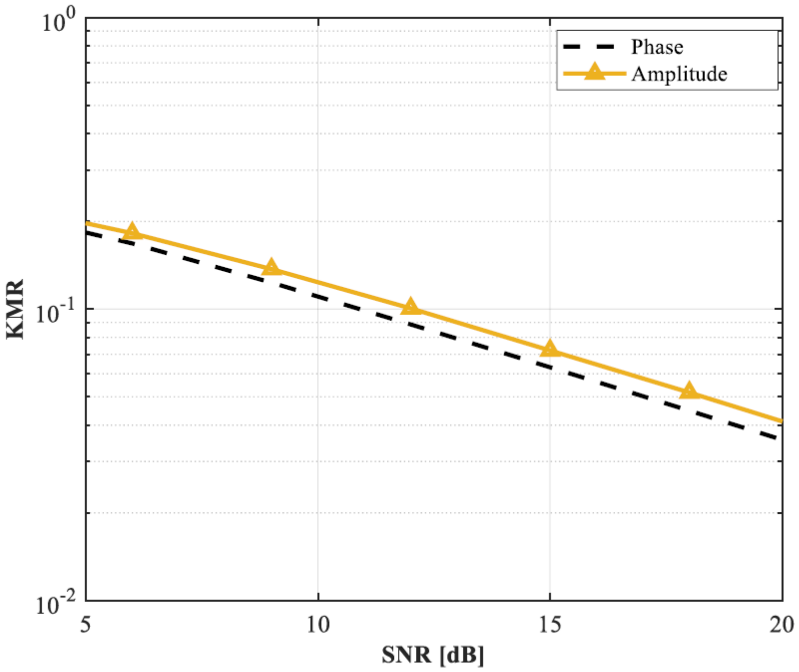

**Fig. 4. Key mismatch rate versus the source and destination transmit power for direct communication.**

## References

[1] W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," IEEE network, vol. 34, no. 3, pp. 134-142, 2019.

[2] A. Chorti et al., "Context-aware security for 6G wireless: The role of physical layer security," IEEE Communications Standards Magazine, vol. 6, no. 1, pp. 102-108, 2022.

[3] J. Zhang, G. Li, A. Marshall, A. Hu, and L. Hanzo, "A new frontier for IoT security emerging from three decades of key generation relying on wireless channels," IEEE Access, vol. 8, pp. 138406-138446, 2020.

[4] J. Zhang, S. Rajendran, Z. Sun, R. Woods, and L. Hanzo, "Physical layer security for the Internet of Things: Authentication and key generation," IEEE Wireless Communications, vol. 26, no. 5, pp. 92-98, 2019.

[5] G. Li, C. Sun, J. Zhang, E. Jorswieck, B. Xiao, and A. Hu, "Physical layer key generation in 5G and beyond wireless communications: Challenges and opportunities," Entropy, vol. 21, no. 5, p. 497, 2019.

[6] J. Zhang, A. Marshall, and L. Hanzo, "Channel-envelope differencing eliminates secret key correlation: LoRa-based key generation in low power wide area networks," IEEE Transactions on Vehicular Technology, vol. 67, no. 12, pp. 12462-12466, 2018.

[7] C. Zenger, H. Vogt, J. Zimmer, A. Sezgin, and C. Paar, "The passive eavesdropper affects my channel: Secret-key rates under real-world conditions," in 2016 IEEE Globecom Workshops (GC Wkshps), 2016: IEEE, pp. 1-6.

[8] M. Letafati, A. Kuhestani, K.-K. Wong, and M. J. Piran, "A lightweight secure and resilient transmission scheme for the Internet of Things in the presence of a hostile jammer," IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4373-4388, 2020.

[9] M. Letafati, H. Behroozi, B. H. Khalaj, and E. A. Jorswieck, "Hardware-impaired PHY secret key generation with man-in-the-middle adversaries," IEEE Wireless Communications Letters, vol. 11, no. 4, pp. 856-860, 2022.

[10] G. Epiphaniou, P. Karadimas, D. K. B. Ismail, H. Al-Khateeb, A. Dehghantanha, and K.-K. R. Choo, "Nonreciprocity compensation combined with turbo codes for secret key generation in vehicular ad hoc social IoT networks," IEEE Internet of Things Journal, vol. 5, no. 4, pp. 2496-2505, 2017.

[11] M. Edman, A. Kiayias, and B. Yener, "On passive inference attacks against physical-layer key extraction?," in Proceedings of the Fourth European Workshop on System Security, 2011, pp. 1-6.

[12] S. Eberz, M. Strohmeier, M. Wilhelm, and I. Martinovic, "A practical man-in-the-middle attack on signal-based key generation protocols," in Computer Security–ESORICS 2012: 17th European Symposium on Research in Computer Security, Pisa, Italy, September 10-12, 2012. Proceedings 17, 2012: Springer, pp. 235-252.

[13] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," IEEE Transactions on Mobile Computing, vol. 9, no. 1, pp. 17-30, 2009.

[14] O. A. Topal, G. K. Kurt, and H. Yanikomeroglu, "Securing the inter-spacecraft links: Physical layer key generation from Doppler frequency shift," IEEE Journal of Radio Frequency Identification, vol. 5, no. 3, pp. 232-243, 2021.

[15] M. Letafati, A. Kuhestani, H. Behroozi, and D. W. K. Ng, "Jamming-resilient frequency hopping-aided secure communication for Internet-of-Things in the presence of an untrusted relay," IEEE Transactions on Wireless Communications, vol. 19, no. 10, pp. 6771-6785, 2020.

[16] C. Feng and L. Sun, "Physical Layer Key Generation from Wireless Channels with Non-ideal Channel Reciprocity: A Deep Learning Based Approach," in 2022 IEEE 95th Vehicular Technology Conference:(VTC2022-Spring), 2022: IEEE, pp. 1-6.

[17] X. Guan, N. Ding, Y. Cai, and W. Yang, "Wireless key generation from imperfect channel state information: Performance analysis and improvements," in 2019 IEEE International Conference on Communications Workshops (ICC Workshops), 2019: IEEE, pp. 1-6.

**HOW TO CITE THIS ARTICLE**

*M. R. Keshavari, H. Zayyani, A. Kuhestani, H. Ahmadi, Channel Phase Based Secret Key Generation: Untrusted Relaying or Not?, AUT J. Model. Simul., 56(1) (2024) 117-126.*

**DOI:** 10.22060/miscj.2023.22720.5342