# Random Pilot Activation and Interpolated Channel Estimation for Physical-Layer Secret Key Generation in Correlated Eavesdropping Channel

Shun Kojima, *Member, IEEE,* and Shinya Sugiura, *Senior Member, IEEE*

***Abstract*—In this paper, we propose a novel physical-layer secret key generation (SKG) scheme, which is based on reduced random pilot selection at a legitimate transmitter and channel interpolation at a legitimate receiver. As a result, the proposed scheme is capable of reducing pilot overhead and increasing secret key capacity (SKC) while suppressing information leakage to an eavesdropper in a correlated eavesdropping channel. More specifically, a subset of full pilot sequence is activated based on the legitimate channels at the legitimate transmitter, and the full channel coefficients are estimated from the received pilot symbol subset at the legitimate receiver with the aid of our channel interpolation. Additionally, despite the non-reciprocal channel due to the presence of a Doppler shift and an additive noise, our scheme achieves high SKG reliability in comparison to that without our reduced pilot selection or channel interpolation. We also derive the theoretical SKC for the proposed scheme. Our simulation results demonstrate that the proposed SKG scheme exhibits a higher performance in terms of both the SKC and key disagreement ratio.**

***Index Terms*—Channel interpolation, correlated channel, eavesdropping channel, physical layer security, pilot reduction, secrecy capacity, secret key generation.**

## I. Introduction

INTERNET of Things (IoT) has been highlighted as a promising concept developed on top of wireless communication technology, which typically requires low latency, low power consumption, and a high number of supported terminals [2]. Additionally, security and privacy are also of primary concern in IoT systems. Due to the broadcast nature of wireless channels, it is essential to address the issue of unintended eavesdroppers. The public key method is commonly utilized to exchange secret keys between legitimate users for data encryption. However, its high computational complexity and power consumption make it unsuitable for low-cost IoT devices [3].

In contrast to the public-key-based upper-layer secret key exchange, physical-layer secret key generation (SKG) has been extensively investigated as a means to achieve information-theoretic security, low complexity, and low power consumption [4]. The physical-layer SKG relies on the inherent randomness of a fading channel between two legitimate users, Alice and Bob, and does not require any third party to share secret keys. Furthermore, the physical layer SKG has proven to be information-theoretically secure because it exploits unpredictable channel properties that vary depending on a myriad of sources, thus guaranteeing channel reciprocity only among legitimate users and making eavesdroppers inaccessible [5, 6]. Most previous studies of physical-layer SKG assume a time-division duplex (TDD)-based system to satisfy the channel reciprocity condition. However, even in the TDD scenario, it is challenging to attain perfect channel reciprocity due to the reduction of a channel correlation by the additive noise, Doppler shift, carrier frequency offset, synchronization error, and hardware impairment [7]–[9]. Imperfect channel reciprocity tends to result in a higher key disagreement ratio (KDR) between Alice and Bob.

Physical-layer SKG is typically performed by estimation [16] and quantization [10]–[14] of reciprocal channel state information (CSI) at each legitimate user. In general, pilot symbols are sent from Alice and Bob to each other to share the identical CSI, which is then quantized to generate a secret key. The pilot symbols may be interrupted by an eavesdropper, Eve, due to the open frame structure and the broadcast nature of wireless channels, hence suffering from the leakage of secret keys. In terms of channel quantization, SKG is classified into two categories, i.e., the received signal strength (RSS)-based SKG [10]–[12] and the phase-based SKG [13]–[15]. The RSS-based SKG has the advantage of allowing simple low-power hardware while suffering from weak randomness due to its continuity, the performance degradation caused by additive noises, and the vulnerability to active attacks from eavesdroppers. By contrast, the phase-based improves randomness and suppresses noise, hence generating a practical secret key even in a stationary environment. However, the risk of eavesdropping is high, especially when the channel correlation between the legitimate and eavesdropping channels is high.

Against the above-mentioned background, the novel contributions of this paper are as follows. We propose a novel physical-layer SKG scheme that is based on a random reduction of pilot symbols at the legitimate transmitter and a channel interpolation at the legitimate receiver. More specifically, one of the predefined random pilot patterns is selected based on the legitimate channel to reduce the pilot symbols at the legitimate transmitter, and the full channel coefficients are estimated from the partial pilot signals received at the

Preprint (Accepted Version). DOI: 10.1109/TVT.2024.3386597. 

The authors are with the Institute of Industrial Science, The University of Tokyo, Tokyo 153-8505, Japan, (e-mail: {skojima,sugiura}@iis.u-tokyo.ac.jp). (*Corresponding author: Shinya Sugiura.*)

The work was supported in part by National Institute of Information and Communications Technology (NICT), Japan, under Grant JPJ12368C00801.

legitimate receiver with the aid of our interpolation. As a result, the proposed pilot reduction and channel interpolation schemes allow us to achieve reduced power consumption, reduced pilot overhead, and increased secrecy performance against the passive eavesdropper. These are achieved as the explicit benefits of improved channel reciprocity and reduced pilot leakage. We evaluate the achievable performance of the proposed scheme in terms of the secret key capacity (SKC), KDR, and randomness test to demonstrate that the proposed scheme outperforms the conventional SKG benchmark.

The remainder of this paper is organized as follows. Section II reviews the related work. In Section III, our system model of the legitimate and eavesdropping channels is presented. Section IV introduces the proposed random pattern selection for pilot reduction and channel interpolation, and Section V analyzes the SKC. Numerical results are provided in Section VI, and our conclusions are given in Section VII.

## II. Related Work

In this section, we review the previous studies related to the proposed physical-layer SKG scheme. More specifically, we focus our attention on the conventional physical-layer SKG schemes assuming the presence of an eavesdropper. Zhang *et al.* [17] were the first to introduce a detailed analysis of physical-layer SKC in the presence of an eavesdropper. It is revealed that SKC performance is affected by a cross-correlation between the legitimate and eavesdropper channel. In [18], the analytical SKC performance of the RSS-based SKG and full-CSI-based SKG was compared in a correlated eavesdropping channel.

The artificial randomness is introduced into the physical-layer SKG to improve the secrecy performance [19]–[22][1]. In [19], beamforming and jamming weights are designed as artificial noise based on the eavesdropper channel to increase the SKC. Chen *et al.* [20] proposed SKG that superimposes artificial noises on the pilot signal to degrade the eavesdropper channel under the realistic assumption that legitimate and eavesdropping channels are correlated. In [21], SKG employing local independent randomness is proposed in the context of static channels. Moreover, in [22], an efficient dual-permutation SKG was developed to match the randomly permuted channel measurements between a pair of users by minimizing their discrepancy holistically. However, the schemes superimposed the artificial noise [19], [20] are imposed by the increased transmission power associated with artificial noises further than those of pilot symbols. Furthermore, perfect knowledge of the eavesdropper's CSI is typically assumed at the legitimate transmitter. Moreover, the artificial randomness methods of [21] and [22] may increase delay and information leakage due to additional processing.

In [23], Qin and Ding proposed the pilot-assisted physical-layer SKG scheme for non-reciprocal channels. Additionally, in [23], the authors also proposed the eigenvalue-based physical-layer SKG scheme, which is effective even when the eavesdropper is located close to the legitimate users. Note that due to the bi-directional channel estimation in [23], information leakage associated with the pilot transmission is inhabited. In [24], the SKC of the physical-layer SKG is analyzed under the presence of information leakage to eavesdroppers, and the secure channel estimation is proposed, by relying on the secret pilot sequence unknown to eavesdroppers. By repeatedly sending secret pilot symbols between Alice and Bob, which are only identified by the legitimate transmitter, a secret key is shared while avoiding information leakage to eavesdroppers. By contrast to the explicit benefits, both the schemes of [23], [24] have to rely on information fed back between Alice and Bob, and impose the additional processing delay and power consumption.

In [25], [26], the effects of quantization on the physical-layer SKG are investigated. Zenger *et al.* [25] compared the achievable secrecy performance of physical-layer SKG between several quantization schemes, where the effects of eavesdroppers are evaluated in a rigorous manner based on the online entropy estimation. In [26], the two-layer secure quantization scheme for physical-layer SKG is proposed to guarantee secrecy in the presence of correlation between the legitimate and eavesdropper channels. Here, the bit sequence achieved by channel quantization is divided into two layers, depending on the probability of eavesdropping, where the first-layer bit sequence is used for error-checking, while the second-layer bit sequence is employed for generating a secret key. Note that the benefits of [26] are achieved at the sacrifice of decreased SKG efficiency.

As mentioned above, several methods have been proposed to improve the secrecy performance of physical-layer SKG in the presence of eavesdroppers. However, most of them are imposed by increased power consumption. To the best of our knowledge, for the first time in this paper, the proposed scheme achieves both reduced power consumption and improved confidentiality with the aid of the novel concepts of reduced random pilot activation and channel interpolation.

## III. Channel Model

### A. Channel Statistics

In a multipath channel, each path is delayed, phase-rotated, and attenuated due to the surrounding objects and movement velocity. The overlapping receptions of the multiple paths induce frequency-selective fading. Here, the channel impulse response consisting of $L$ paths is expressed as follows:

$$h(\tau, t) = \sum_{l=0}^{L-1} h_l(t)\ \delta(\tau - \tau_l), \tag{1}$$

where

$$L = \lfloor BT_m \rfloor + 1, \tag{2}$$

while $h_l$ and $\tau_l$ represent the complex-valued channel coefficient and the delay of the $l$-th path, respectively. Also, $\delta(\cdot)$ is Dirac's delta function, and $\lfloor . \rfloor$ is the floor function.

[1]Unlike [19]–[22], our proposed scheme does not rely on using artificial randomness as a source of entropy. Hence, the combination of the proposed scheme and artificial randomness may improve the secrecy performance, which is left for future study.

Furthermore, $B$ and $T_{\mathrm{m}}$ denote the bandwidth and the delay spread. Each channel tap is represented by

$$h_l(t) = \frac{a_l}{\sqrt{L}} \sum_{l=0}^{L-1} \exp\Big(j\left(2\pi f_d t \cos\theta_l + \phi_l\right)\Big), \tag{3}$$

where $a_l$ and $f_d$ indicate the amplitude of the $l$-th path and the maximum Doppler frequency, respectively. $\theta_l$ and $\phi_l$ are the angle of arrival and its initial phase of the $l$-th path, respectively. Here, we have the relationship of $\sum_{l=0}^{L-1} E\left[\left|h_l^2\right|\right] = 1$, where $E[\cdot]$ represents the expectation operation. In this paper, we employ Jake's model to represent the time-varying channel [27].

Let $H(f,t)$ denote the Fourier transform of the channel transfer function $h(\tau,t)$, which is expressed by

$$H(f,t) = \int_0^{\infty} h(\tau,t)\exp\left(-j2\pi f\tau\right)d\tau \tag{4}$$

$$= \sum_{l=0}^{L-1} h_l(t)\exp\left(-j2\pi f\frac{l}{B}\right). \tag{5}$$

From (5), for $L > 1$, the channel's spectral response $H(f,t)$ does not tend to be flat, thus exhibiting frequency selectivity.

### B. Channel Estimation

The signal received at each receiver is given by

$$r(t) = \int_{-\infty}^{\infty} h(\tau,t)s(t-\tau)d\tau + n(t)$$
$$= h(t) \otimes s(t) + n(t), \tag{6}$$

where $h(t)$, $s(t)$, and $n(t)$ represent the channel impulse response, the transmitted signal, and the additive white Gaussian noise (AWGN). After the fast Fourier transform of (6), the block model of the received samples can be represented by

$$\mathbf{r} = \mathbf{h}^T \mathrm{diag}\{\mathbf{s}\} + \mathbf{n} \tag{7}$$

$$= \mathbf{h}^T\mathbf{S} + \mathbf{n}, \tag{8}$$

where $\mathbf{r} \in \mathbb{C}^{N_c}$ indicates the received frequency-domain samples, and $N_c$ is the number of subcarriers. Also, $\mathbf{s} \in \mathbb{C}^{N_c}$ are the transmitted symbols, and we have the relationship of $\mathbf{S} = \mathrm{diag}\{\mathbf{s}\}$. $\mathbf{h} \in \mathbb{C}^{N_c}$ and $\mathbf{n} \in \mathbb{C}^{N_c}$ denote the channel frequency responses and AWGNs, respectively.

In this paper, the least squares (LS) algorithm is employed for carrying out low-complexity frequency-domain channel estimation [28]. We consider a real-valued pilot block defined by $\mathbf{P} \in \mathbb{R}^{N_p \times N_c}$. In SKG, all subcarriers are generally allocated as pilot signals to obtain accurate CSI. The pilot signals can be represented by

$$\mathbf{P} = \{P^{(i)} = 1\}. \tag{9}$$

The channel frequency responses and the frequency-domain AWGNs, corresponding to pilot subcarriers, are expressed by [28]

$$\mathbf{h}_p = \mathbf{P}\mathbf{h} \in \mathbb{C}^{N_p} \tag{10}$$

$$\mathbf{n}_p = \mathbf{P}\mathbf{n} \in \mathbb{C}^{N_p}, \tag{11}$$

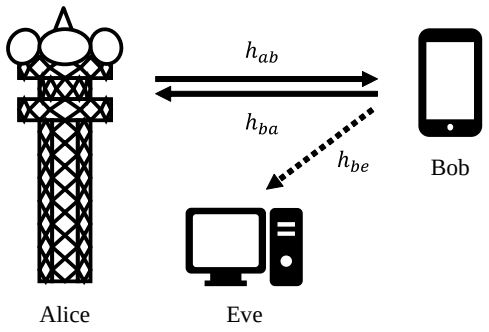


Fig. 1. The channel model, comprising of Alice and Bob as legitimate users and of Eve as an eavesdropper.

and the diagonal matrix of the pilot symbols can be expressed by

$$\mathbf{S}_p = \mathbf{P}\mathbf{S}\mathbf{P}^T. \tag{12}$$

Similar to (8), the received model of the pilot symbols is given by

$$\mathbf{r}_p = \mathbf{h}_p^T\mathbf{S}_p + \mathbf{n}_p. \tag{13}$$

In the LS algorithm, the frequency channel response is estimated as follows:

$$\hat{\mathbf{h}}_p = \mathbf{S}_p^H\mathbf{r}_p$$
$$= \mathbf{h}_p + \mathbf{S}_p^H\mathbf{n}_p. \tag{14}$$

### C. System Model

Fig. 1 shows the channel model considered in our physical-layer SKG scheme, where Alice and Bob are legitimate users, and Eve is a passive eavesdropper. Each user is equipped with a single antenna, according to most of the previous SKG studies [29], while the use of multiple antennas improves the achievable SKG performance [30], [31]. In this paper, under the assumption of the TDD mode, each pilot symbol is transmitted at a specific frequency. For simplicity, assume that Eve is located near Alice and is eavesdropping on the signal from Bob[2]. This means that the channel correlation between Eve and legitimate users is high, and the potential for eavesdropping is relatively high [26]. The channel coefficient from Bob to Alice and that from Alice to Bob are represented, respectively, by

$$h_{ba}^{(i)} = \rho_{ba}h_{ab}^{(i)} + \sqrt{1-\rho_{ba}^2}\omega_{ba}^{(i)} \tag{15}$$

$$h_{be}^{(i)} = \rho_{be}h_{ab}^{(i)} + \sqrt{1-\rho_{be}^2}\omega_{be}^{(i)}, \tag{16}$$

where $i = 0, \cdots, N_c - 1$ is the index of subcarriers. Similarly, $h_{be}^{(i)}$ is the eavesdropping channel from Bob to Eve. Also, $\omega_{ba}^{(i)}$ and $\omega_{be}^{(i)}$ represent the circularly symmetric complex-valued Gaussian random variables at Alice and Eve, respectively. Furthermore, $\rho_{ba}$ and $\rho_{be}$ denote the cross correlation coefficient between $h_{ab}^{(i)}$ and $h_{ba}^{(i)}$ and that between $h_{ab}^{(i)}$ and $h_{be}^{(i)}$.

[2]Of course, it is also reversible in situations where Eve's location is close to Bob, and she is eavesdropping on signals from Alice.

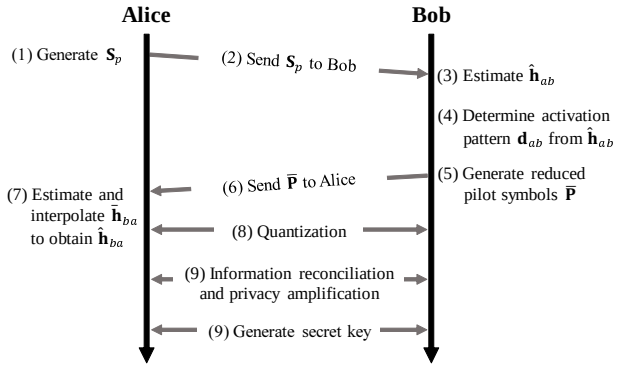


Fig. 2. Signaling procedures of the proposed physical-layer SKG scheme.

Hence, we have the relationships of $h_{ba}^{(i)} \sim \mathcal{CN}(0, \sigma_{h_{ba}}^2)$ and $h_{be}^{(i)} \sim \mathcal{CN}(0, \sigma_{h_{be}}^2)$, $\rho_{ba}$ and $\rho_{be}$ can be expressed by

$$\rho_{ba} = \frac{E[h_{ba}^{\dagger} h_{ab}]}{\sigma_{h_{ba}}^2} = J_0(2\pi f_d^{ba} \tau_d^{ba}) \tag{17}$$

$$\rho_{be} = \frac{E[h_{ba}^{\dagger} h_{be}]}{\sigma_{h_{ba}} \sigma_{h_{be}}} = J_0(2\pi f_d^{be} \tau_d^{be}), \tag{18}$$

where $(\cdot)^{\dagger}$ denotes the conjugate transpose operation. $f_d^{ba}$ and $f_d^{be}$ are the maximum Doppler frequency of the link from Bob to Alice and that from Bob to Eve, respectively. Moreover, $\tau_d^{ba}$ and $\tau_d^{be}$ denote the time difference between the actual and estimated channel coefficients at Alice and Eve, respectively, and $J_0(\cdot)$ indicates a zero-order Bessel function of the first kind. From these equations, spatial uncorrelations of the channel can be modeled, and correlations between channel coefficients can be considered [17].

## IV. Proposed Method

In this section, we propose a novel physical-layer SKG scheme based on two concepts, i.e., reduce pilot pattern selection at the legitimate transmitter and channel interpolation at the legitimate receiver. Fig. 2 shows the overview of our SKG scheme, where secret keys are generated from the CSI of the legitimate channel for the sake of simplicity.

In the proposed scheme, Alice first sends a complete pilot sequence to Bob; then, Bob estimates $\mathbf{h}_{ab} = [h_{ab}^{(0)}, \cdots, h_{ab}^{(N_c-1)}]^T$ from the received pilot sequence as $\hat{\mathbf{h}}_{ab} = [\hat{h}_{ab}^{(0)}, \cdots, \hat{h}_{ab}^{(N_c-1)}]^T$. Next, Bob selects the predefined random pilot activation pattern, by deactivating a subset of the full pilot sequence to zeros, based on the first-$D$ and the last-$D$ entries of $\hat{\mathbf{h}}_{ab}$, where $D$ indicates the length of the channel used to determine the activation pattern $\mathbf{d}_{ab}$. Here, the predefined pattern is assumed to be shared among all users in advance. Then, the reduced pilot sequence $\bar{P}$ is sent from Bob to Alice. After that, Alice first estimates the channel coefficients $\bar{\mathbf{h}}_{ba} = [\bar{h}_{ba}^{(0)}, \cdots, \bar{h}_{ba}^{(N_c-1)}]^T$ from the received partial pilot symbols. From these values, $\mathbf{d}_{ba}$ is identified, and interpolation is applied to estimate the complete channel coefficients $\hat{\mathbf{h}}_{ba} = [\hat{h}_{ba}^{(0)}, \cdots, \hat{h}_{ba}^{(N_c-1)}]^T$. Finally, Alice and Bob quantize $\hat{\mathbf{h}}_{ab}$ and $\hat{\mathbf{h}}_{ba}$ to generate a secret key, respectively.

Typically, in physical-layer SKG, information reconciliation is exploited for improving the key agreement ratio after the quantization process. More specifically, Cascade protocol [33] and forward error-correction codes, such as LDPC codes [34], are used to enhance the cross-correlation between the secret keys generated at Alice and Bob. Since, in the information reconciliation process, redundant information is exchanged through a public channel, privacy amplification is employed to strengthen security after the information reconciliation process. This is carried out based on the universal hash function [35] at Alice and Bob. Although the information reconciliation and privacy amplification processes have the benefits of increasing the key agreement rate while maintaining security, the key generation efficiency and SKC are not improved. Therefore, in this paper, we do not consider information reconciliation and privacy amplification while focusing on channel estimation and quantization.

As above-mentioned, the proposed scheme consists of two processes, i.e., the reduced pilot pattern selection and channel interpolation, which are introduced as follows.

### A. Reduced Pilot Pattern Selection Algorithm

We consider the scenario where Eve tries to interrupt the signals sent from Bob to Alice. Hence, we focus our attention on improving the secrecy of the legitimate channel from Bob to Alice. More specifically, in the proposed SKG scheme, the subset of the $N_p$–length full pilot sequence is randomly deactivated at Bob in order to minimize the possibility that the eavesdropper steals the secret key while decreasing the pilot overhead and power consumption[3]. Here, the transmitted pilot activation pattern has to be obtained at the legitimate users while maintained to be unpredictable at the eavesdropper. To this end, Bob uses highly correlated legitimate channel information to activate the partial pilot sequence. Our pilot pattern selection algorithm is robust against the interception of eavesdroppers which are sufficiently apart from the legitimate users under the assumption of the presence of small-scale fading.

To be more specific, our pilot activation pattern selection is illustrated in Fig. 3, where we assume that Eve is positioned close to Alice, as shown in Fig. 1, and tries to intercept the pilot symbols transmitted from Bob. First, Bob estimates the channels $\mathbf{h}_{ab}$ from the pilot symbols transmitted from Alice. Then, Bob calculates $D_1$ and $D_2$, which correspond to the average absolute values of the first-$D$ and last-$D$ channel coefficients as follows:

$$D_1 = \frac{1}{D} \sum_{d=0}^{D-1} |h_{xy}^{(d)}| \tag{19}$$

$$D_2 = \frac{1}{D} \sum_{d=N_c-D}^{N_c} |h_{xy}^{(d)}|, \tag{20}$$

[3]To elaborate a little further, the proposed scheme is readily applicable to multi-user scenarios in combination with the conventional orthogonal multiple access protocols, such as time division multiple access (TDMA) and orthogonal frequency-division multiple access (OFDMA).

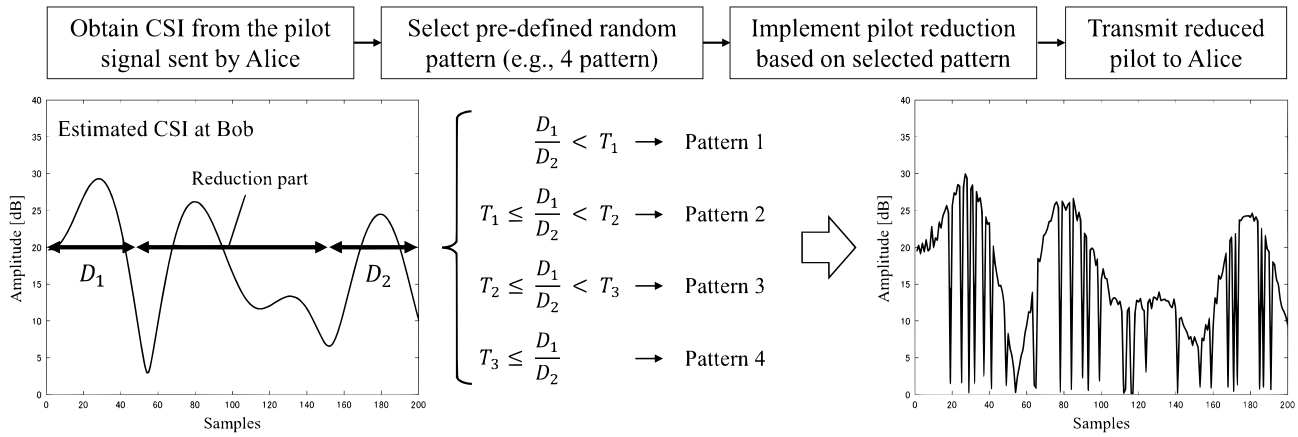


Fig. 3. The overview of the proposed reduced pilot pattern selection.

where $\{x, y\} = \{a, b, e\}$. From (19) and (20), the ratio of $D_1$ to $D_2$ is represented by

$$\frac{D_1}{D_2} = \frac{\sum_{d=0}^{D-1} |h_{xy}^{(d)}|}{\sum_{d=N_c-D}^{N_c} |h_{xy}^{(d)}|}. \tag{21}$$

Now let us introduce thresholds $T_n$ $(n = 0, \cdots, N-1)$ to select a single out of the $N$ predefined active pilot patterns. $T_n$ is determined by the number of predefined pilot patterns to make $\frac{D_1}{D_2}$ equally spaced, which is given by

$$\mathbf{d}_{xy} = \begin{cases} \text{Pattern } 1 & (\frac{D_1}{D_2} < T_1) \\ \text{Pattern } 2 & (T_1 \leq \frac{D_1}{D_2} < T_2) \\ \quad \vdots & \\ \text{Pattern } N & (T_{N-1} \leq \frac{D_1}{D_2}), \end{cases} \tag{22}$$

where $\mathbf{d}_{xy} = [d_{xy}^{(0)}, \cdots, d_{xy}^{N_c-2D-1}] \in \mathbb{Z}^{N_c-2D}$ is an $(N_c - 2D)$–length binary sequence, and $P_r = \sum_{i=0}^{N_c-2D-1} d_{xy}^{(i)}/N_c$ is the pilot activation ratio. To be more specific, the $(N_c-2D)P_r$ active pilot symbols are used for generating the full secret key at Alice.

In our scheme, $\mathbf{d}_p$ is determined based on the legitimate channel between Alice and Bob. In general, the eavesdropping channel between Bob and Eve is less correlated with the legitimate channel when Eve is more than several wavelengths apart from Bob under the presence of fading. This tends to prevent Eve from obtaining the accurate $\mathbf{d}_p$. Therefore, the proposed algorithm can easily add computational security in addition to the information theoretical security. Note that the deactivated pilot positions may be used for sending additional information symbols to increase the data rate.

The pilot symbol with the insertion of the null subcarrier by applying the pilot pattern $\mathbf{d}_p$, defined by $\bar{\mathbf{P}} = \{\bar{P}^{(i)}\}$, can be expressed as

$$\bar{P}^{(i)} = [i \in \mathbf{d}_p]. \tag{23}$$

Here, from (11)–(14) and (23), we obtain the estimated CSI by the partially deactivated pilot symbols at Alice and Eve,

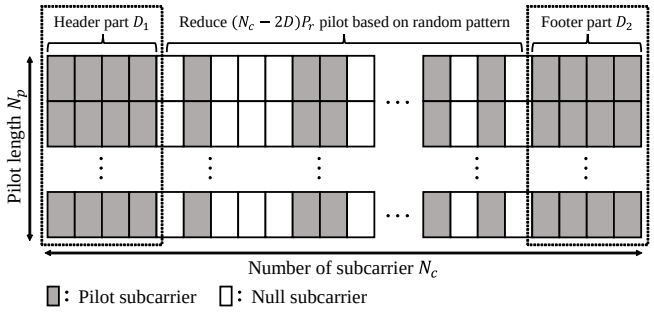


Fig. 4. The arrangement of activated pilot sequence in the proposed scheme.

respectively.

$$\bar{\mathbf{h}}_{ba} = \mathbf{h}_{ba} + \bar{\mathbf{S}}_p^H \mathbf{n}_{ba} \tag{24}$$

$$\bar{\mathbf{h}}_{be} = \mathbf{h}_{be} + \bar{\mathbf{S}}_p^H \mathbf{n}_{be}, \tag{25}$$

where $\bar{\mathbf{S}}_p^H = \bar{\mathbf{P}}\mathbf{S}\bar{\mathbf{P}}^{\mathbf{T}}$, $n_{ba}$ and $n_{be}$ indicate the associated AWGN components at Alice and Eve, respectively.

### *B. Channel Interpolation*

Alice receives the pilot sequence reduced by our pilot pattern selection algorithm of Section IV-A, as shown in Fig. 4. At the channel interpolation stage, Alice first estimates the reduced random pilot pattern $\mathbf{d}_{ba}$ from the estimated ratio $D_1/D_2$ of (21) in order to identify the active pilot positions. Eve also obtains $\mathbf{d}_{be}$; however, the accuracy depends on the correlation with $h_{ab}$, thus making it challenging to ascertain accurate values in eavesdroppers, who generally have lower correlations. Then, the channel coefficients associated with the active pilot symbols are estimated, while the rest of the channel coefficients are interpolated from the estimated channel coefficients. In the proposed scheme, we consider three interpolation schemes, i.e., linear interpolation, spline interpolation, and Akima interpolation.

*1) Linear Interpolation:* Linear interpolation is a regression method using linear polynomial equations to make linear approximations from adjacent signals. Consider that the pilot spacing in the frequency domain in the proposed random

pattern selection is $\Delta'_p$. Then, the interpolated channel of the $u$-th subcarrier ($v\Delta'_p < u < (v+1)\Delta'_p$) by linear interpolation is formulated by

$$\begin{aligned}\hat{h}_{xy}^{(u)} &= \hat{h}_{xy}^{(v\Delta'_p+w)} \\ &= \bar{h}_{xy}^{(v)} + \frac{w}{\Delta'_p}\big(\bar{h}_{xy}^{(v+1)} - \bar{h}_{xy}^{(v)}\big),\end{aligned} \tag{26}$$

where $v$ and $w$ satisfy $0 \le v \le N_p - 1$ and $0 \le w \le \Delta'_p - 1$. From (26), linear interpolation operates with low complexity and typically exhibits a good approximation in a slow fading scenario rather than in the complicated channels with a high time variation.

*2) Spline Interpolation:* Spline interpolation accurately reflects a curve variation propensity by fitting with a series of unique third-order polynomials between each subcarrier. Here, the interpolated channel coefficient at the $u$-th subcarrier is represented by

$$\hat{h}_{xy}^{(u)} = \gamma_0 \bar{h}_{xy}^{(v)} + \gamma_1 \bar{h}_{xy}^{(v+1)} + \gamma_0 \Delta'_p \bar{h}'^{(v)}_{xy} + \gamma_1 \Delta'_p \bar{h}'^{(v+1)}_{xy} \tag{27}$$

where $\bar{h}'_{xy}$ denotes the first-order derivative, while $\gamma_0$ and $\gamma_1$ are the constants determined by $w/\Delta'_p$ as follows:

$$\gamma_0 = 3\frac{w^2}{{\Delta'_p}^2} - 2\frac{w^3}{{\Delta'_p}^3} \tag{28}$$

$$\gamma_1 = 3\frac{(\Delta'_p - w)^2}{{\Delta'_p}^2} - 2\frac{(\Delta'_p - w)^3}{{\Delta'_p}^3}. \tag{29}$$

*3) Akima Interpolation:* Akima interpolation is a cubic interpolation, similar to spline interpolation, and generates a piecewise polynomial by the successive first-order derivative [36]. Since Akima interpolation preserves the gradient, it is resistant to overshooting and is capable of achieving good interpolation performance when the characteristics of the original function are known. However, Akima interpolation has the disadvantage that the continuity of derivatives is not guaranteed, similar to spline interpolation, which makes it challenging to interpolate data that drastically deviates from the original data.

### C. Quantization

In the physical-layer SKG, the estimated analog channel coefficients are quantized to generate a binary secret key. In the proposed scheme, Alice estimates the full channel coefficients from the reduced pilot sequence with the aid of channel interpolation, which may result in an unstable match to the channel coefficients estimated by Bob. Therefore, we employ a quantization scheme having a guard band gap for the sake of improving the key agreement ratio [37], [38].

More specifically, let us consider that an estimated channel coefficient $\hat{h}_{xy}(t)$ is quantized by a one-bit quantizer to generate one bit $\kappa$ as follows:

$$\kappa = \begin{cases} 1 & |\hat{h}_{xy}(t)| > \Lambda_{upper} \\ 0 & |\hat{h}_{xy}(t)| \le \Lambda_{lower} \\ \text{none} & \Lambda_{lower} < |\hat{h}_{xy}(t)| \le \Lambda_{upper}, \end{cases} \tag{30}$$

where

$$\Lambda_{upper} = \mu_{\hat{h}_{xy}} + \sigma_{\hat{h}_{xy}}\Delta_Q \tag{31}$$

$$\Lambda_{lower} = \mu_{\hat{h}_{xy}} - \sigma_{\hat{h}_{xy}}\Delta_Q. \tag{32}$$

Here, $\Lambda_{upper}$ and $\Lambda_{lower}$ indicate the quantized upper and lower thresholds, respectively. Also, $\mu_{\hat{h}_{xy}}$ and $\sigma_{\hat{h}_{xy}}$ are the expectation and the standard deviation of $\hat{h}_{xy}(t)$, respectively, and $\Delta_Q$ denotes the quantization guard band. To satisfy the constraint of $\Lambda_{lower} > 0$, the upper bound has to be in the range of

$$\Delta_Q < \frac{\mu_{\hat{h}_{xy}}}{\sigma_{\hat{h}_{xy}}} = \sqrt{\frac{\pi}{4-\pi}} \tag{33}$$

Note that the estimated channel coefficients that fall into the guard band gap are excluded from the generated secret key due to low reliability. There is the quantization performance trade-off where a high $\Delta_Q$ value improves the key agreement rate while decreasing the key length.

## V. Secret Key Capacity

In this section, we derive the SKC of the proposed scheme to evaluate the achievable secrecy bound for securely sharing a secret key between two legitimate terminals in the presence of the eavesdropper with the independent channel. Based on the transmitted pilot sequence, the channel is estimated according to (14), (24), and (25), which can be expressed by

$$\hat{\mathbf{h}}_{ab} = \mathbf{h}_{ab} + \mathbf{S}_p^H \mathbf{n}_{ab} \tag{34}$$

$$\hat{\mathbf{h}}_{ba} = f(\bar{\mathbf{h}}_{ba}) = f(\mathbf{h}_{ba} + \bar{\mathbf{S}}_p^H \mathbf{n}_{ba}) \tag{35}$$

$$\hat{\mathbf{h}}_{be} = f(\bar{\mathbf{h}}_{be}) = f(\mathbf{h}_{be} + \bar{\mathbf{S}}_p^H \mathbf{n}_{be}). \tag{36}$$

and

$$\sigma^2_{\hat{h}_{ab}} = \sigma^2_{h_{ab}} + \frac{\sigma^2_{n_{ab}}}{N_p P_t}, \tag{37}$$

$$\sigma^2_{\hat{h}_{ba}} = \sigma^2_{h_{ba}} + \frac{\sigma^2_{n_{ba}}}{N_p \bar{P}_t}, \tag{38}$$

$$\sigma^2_{\hat{h}_{be}} = \sigma^2_{h_{be}} + \frac{\sigma^2_{n_{be}}}{N_p \bar{P}_t}. \tag{39}$$

where $f(\cdot)$ denotes the interpolation operations. $\sigma_{\hat{h}_{ab}}$, $\sigma_{\hat{h}_{ba}}$, and $\sigma_{\hat{h}_{be}}$ represent the variances of $\hat{h}_{ab}$, $\hat{h}_{ba}$, and $\hat{h}_{be}$, respectively. $\mathbf{n}_{ab}$, $\mathbf{n}_{ba}$, and $\mathbf{n}_{be}$ indicate the associated AWGN components at Bob, Alice, and Eve with the variances of $\sigma^2_{n_{ab}}$, $\sigma^2_{n_{ba}}$, and $\sigma^2_{n_{be}}$, respectively. Also, $N_p$ denotes the length of the pilot sequence $\mathbf{s}$. $P_t$ is the transmit power of Alice, and $\bar{P}_t$ is the transmit power applying the proposed reduction algorithm, which can be expressed by

$$\bar{P}_t = P_r P_t. \tag{40}$$

Here, the signal-to-noise ratios (SNRs) for each user are given by

$$\gamma_{ab} = \frac{P_t \sigma_{h_{ab}}^2}{\sigma_{n_{ab}}^2} \tag{41}$$

$$\gamma_{ba} = \frac{\bar{P}_t \sigma_{h_{ba}}^2}{\sigma_{n_{ba}}^2} \tag{42}$$

$$\gamma_{be} = \frac{\bar{P}_t \sigma_{h_{be}}^2}{\sigma_{n_{be}}^2}. \tag{43}$$

From these equations, the mean-square error (MSE) of the LS algorithm is represented by

$$\epsilon_{ab} = \frac{1}{N_p \gamma_{ab}} \tag{44}$$

$$\epsilon_{ba} = \frac{1}{N_p \gamma_{ba}} \tag{45}$$

$$\epsilon_{be} = \frac{1}{N_p \gamma_{be}}. \tag{46}$$

Furthermore, the cross-correlation between $\hat{h}_{ab}$ and $\hat{h}_{ba}$, and that between $\hat{h}_{ab}$ and $\hat{h}_{be}$ are given by [17].

$$\rho(\hat{h}_{ab}, \hat{h}_{ba}) = \frac{\rho_{ba}}{\sqrt{(1+\epsilon_{ab})(1+\epsilon_{ba})}}, \tag{47}$$

$$\rho(\hat{h}_{ba}, \hat{h}_{be}) = \frac{\rho_{be}}{\sqrt{(1+\epsilon_{ba})(1+\epsilon_{be})}}. \tag{48}$$

From (47) and (48), mutual information (MI) is formulated by

$$I(\hat{h}_{ab}, \hat{h}_{ba}) = -\frac{1}{2}\log_2(1-\rho(\hat{h}_{ab}, \hat{h}_{ba})^2) \tag{49}$$

$$I(\hat{h}_{ba}, \hat{h}_{be}) = -\frac{1}{2}\log_2(1-\rho(\hat{h}_{ba}, \hat{h}_{be})^2). \tag{50}$$

Hence, the SKC of the proposed scheme can be represented by

$$\begin{aligned} C_{SK} &= I(\hat{h}_{ab}, \hat{h}_{ba}) - I(\hat{h}_{ba}, \hat{h}_{be}) \\ &= \frac{1}{2}\log_2\left(\frac{1-\rho(\hat{h}_{ba}, \hat{h}_{be})^2}{1-\rho(\hat{h}_{ab}, \hat{h}_{ba})^2}\right). \end{aligned} \tag{51}$$

The proposed scheme increases MSEs of channel estimation because of the randomly reduced pilot sequence. Observe in (51) that SKC is a function of the channel estimation MSEs of the legitimate user and eavesdropper, as well as the channel correlations.

## VI. Simulation Results

In this section, we carry out Monte Carlo simulations, and provide our performance results for the proposed physical-layer SKG scheme, which is evaluated in terms of the MSE, derived SKC, KDR, and the randomness test in the presence of an eavesdropper.

We consider the TDD-based orthogonal frequency-division multiplexing (OFDM) system, where our physical-layer SKG process between Alice and Bob is carried out during the channel coherence time. We also consider Eve positioned near Alice to intercept the signal transmitted from Bob. To evaluate the achievable SKG performance in the presence of the eavesdropping channel, we consider the practical scenario where Eve knows all information used by legitimate users. Here, $L = 15$ paths are generated to represent each multipath fading channel with exponential attenuation, and the Doppler frequency is given by 1 Hz. The length of the full pilot sequence is set to $N_p = 10$, and the number of subcarriers is given by $N_c = 512$. Also, the quantization guard band is set as $\Delta_Q = 0.25$. Unless otherwise noted, we employ the basic system parameters of $(\rho_{ba}, \rho_{be}) = (0.99, 0.90)$, $D = 32$, $P_r = 0.75$, and $N = 4$. In order to provide fair comparisons in the power consumption reduction between the proposed and conventional schemes, the energy per bit to noise power spectral density ratio (Eb/No) is considered.

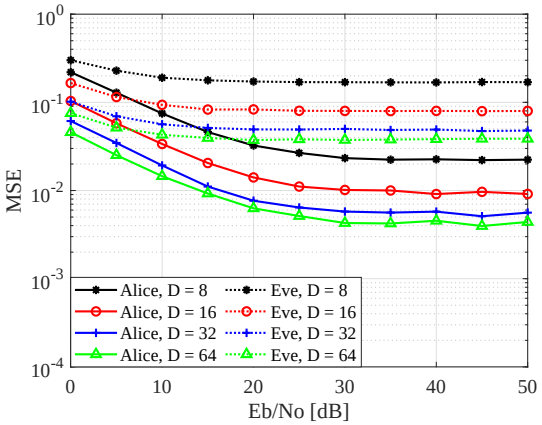


Fig. 5. MSEs of the proposed reduced pilot pattern selection at Alice and Eve with the correlation of $\rho_{ba} = 0.99$ and $\rho_{be} = 0.64$.

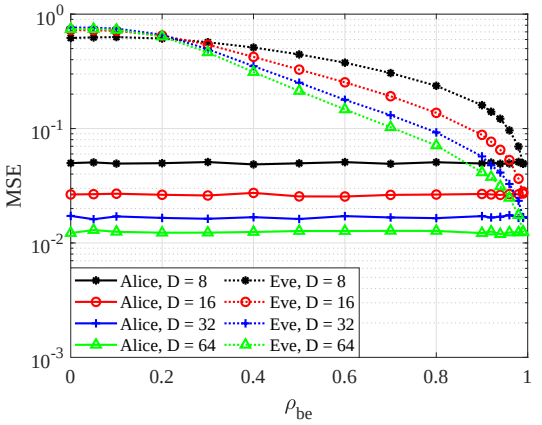


Fig. 6. Effects of $D$ on the MSE versus $\rho_{be}$ at Alice and Eve.

### A. Effects of Proposed Reduced Pilot Pattern Selection

Fig. 5 shows the MSEs of the reduced pilot patterns, which are estimated at Alice and Eve, respectively. The channel correlations are given by $\rho_{ba} = 0.99$ and $\rho_{be} = 0.64$. Observe in Fig. 5 that upon increasing $D$, each MSE tends to decrease and induce an error floor. More specifically, the advantage of Alice over Eve increases with the increase of Eb/No. This implies that the legitimate users have the benefit

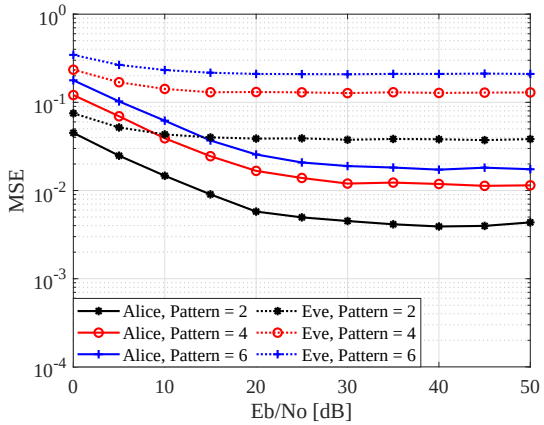


Fig. 7. Effects of the number of reduced pilot patterns $N$ on the MSE versus Eb/No at Alice and Eve.

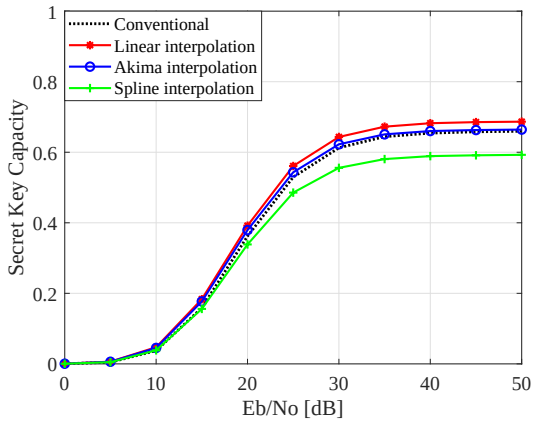


Fig. 9. SKC comparisons between the three interpolation schemes with $\rho_{ba} = 0.99$ and $\rho_{be} = 0.90$. Also, the conventional scheme that does not use the proposed reduced pilot pattern selection is employed as a benchmark.

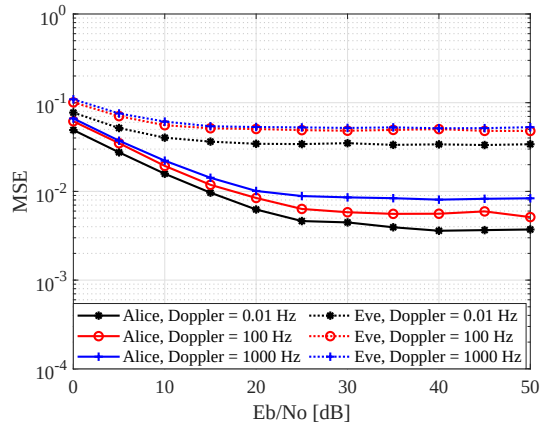


Fig. 8. Effects of the Doppler frequency on the MSE versus Eb/No at Alice and Eve.

of estimating the reduced pilot pattern more accurately than the eavesdropper, especially in the high Eb/No region.

Fig. 6 compares the MSEs of the estimated partial pilot pattern at Alice and Eve, where the $\rho_{be}$ value is varied while fixing $\rho_{ba} = 0.99$. As shown in Fig. 6, upon decreasing $\rho_{be}$, the MSE at Eve increases while the MSE at Alice remains almost unchanged. It is found that the proposed reduced pilot pattern selection algorithm has the robustness to information leakage to the eavesdropper for $\rho_{be} < 0.95$.

Fig. 7 shows the MSE of the estimated partial pilot pattern at Alice and Eve, where the number of pilot patterns is given by $N = 2$, 4, and 6. As seen in Fig. 7, for both Alice and Eve, the MSE improves when the number of pilot patterns $N$ decreases.

Fig. 8 shows the effects of the Doppler frequency on the MSE at Alice and Eve, respectively. As shown in Fig. 8, the MSE degrades at Alice and Eve as the Doppler frequency increases. On the other hand, the degradation of the MSE due to the Doppler frequency is insignificant and thus has a negligible impact on the proposed scheme.

### *B. Secret Key Capacity Analysis*

Fig. 9 compares the SKC performance between the three interpolation schemes of Section IV-B. Also, the conventional scheme that does not use the proposed reduced pilot pattern selection is employed as a benchmark. As shown in Fig. 9, the proposed schemes with linear interpolation and Akima interpolation outperform the conventional benchmark scheme despite the reduced pilot symbols. Note that since we assume $\rho_{ba} = 0.99$, the legitimate channel is not reciprocal. Our channel interpolation reduces the effects of the non-reciprocity and exhibits a higher SKC than the conventional full-pilot benchmark[4]. Additionally, the proposed scheme with linear interpolation achieves the best performance over the entire Eb/No region with a maximum 4 % gain, regardless of $\rho_{be}$. This is because the channel variation assumed in this paper can be linearly approximated if a sufficient number of samples is available. While inferior to linear interpolation, Akima interpolation also outperforms the conventional scheme at each Eb/No with a maximum 0.7 % gain. The SKC curve of the proposed scheme with spline interpolation is the worst due to the overfitting effects of the channel reciprocity.

Fig. 10 shows the SKC of the proposed scheme employing linear interpolation, where the $D$ value is varied from 4 to 32. As expected from Figs. 5 and 6, upon increasing $D$, the SKC performance improves with a maximum 5% gain than the conventional scheme. A high $D$ value leads to the reduction of activated pilot signals. Then, this degrades channel estimation while improving pilot activation pattern estimation, thus increasing the SKC.

Fig. 11 shows the SKC of the proposed scheme employing linear interpolation, where the pilot activation ratio is given by $P_r = 0.5$, 0.625, 0.75, and 0.875. Observe in Fig. 11 that all the curves of the proposed scheme outperform that of the conventional full-pilot benchmark scheme. More specifically, the curve with $P_r = 0.625$ exhibits the best SKC performance with a maximum 6.1 % gain. Note that the SKC performance

[4]Naturally, if the channel reciprocity is perfect, i.e., $\rho_{ba} = 1.0$, the SKC of the proposed scheme does not attain any performance gain.

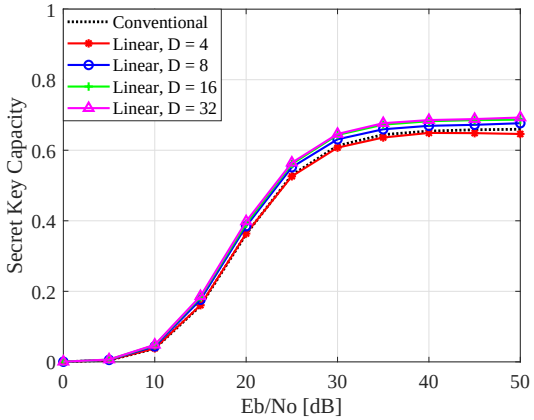


Fig. 10. Effects of $D$ on the SKC performance of the proposed scheme using linear interpolation at $\rho_{ba} = 0.99$ and $\rho_{be} = 0.90$.

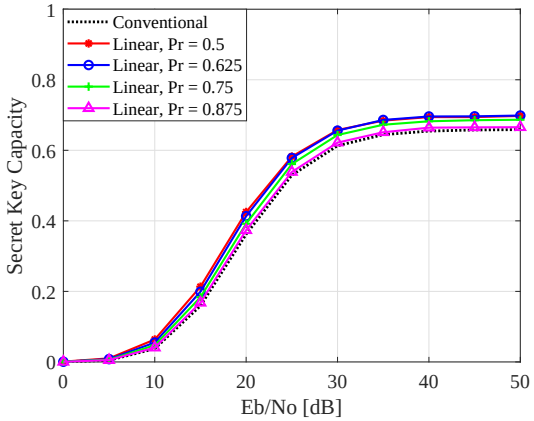


Fig. 11. Effects of the pilot activation ratio $P_r$ on the SKC performance of the proposed scheme employing linear interpolation for $\rho_{ba} = 0.99$ and $\rho_{be} = 0.90$.

of the proposed scheme deteriorates for a low $P_r$ value due to insufficient pilot symbols used for interpolation at Alice. By contrast, for a high $P_r$, the performance improvement owing to our channel interpolation becomes minimal.

Fig. 12 compares MI of the legitimate channel, MI of the eavesdropper channel, and SKC in the proposed and conventional benchmark schemes. As seen in Fig. 12, the proposed scheme exhibits higher MI of the legitimate channel and higher SKC than the conventional full-pilot scheme with a maximum 2.7 % gain, which is achieved as the benefits of our linear interpolation. More specifically, this is because the potential disagreement of the estimated channels at Alice and Bob due to imperfect reciprocity $\rho_{ba} = 0.99$ can be recovered owing to our interpolation with smoothing. Furthermore, the proposed scheme attained a higher MI of the legitimate channel and a lower MI of the eavesdropper channel than the conventional scheme. This is because, in the proposed scheme, estimation of the reduced pilot pattern is essential, and the eavesdropper channel with a low $\rho_{be}$ value causes errors in estimating the pilot patterns. Thus, the proposed scheme achieved higher SKC than the conventional scheme.

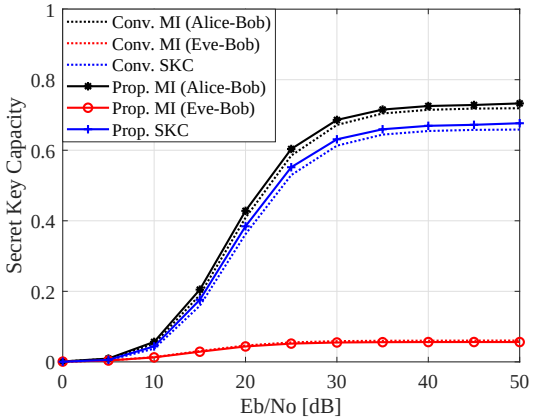


Fig. 12. Comparisons between MI of the legitimate channel, MI of the eavesdropper channel, and SKC in the proposed and conventional benchmark schemes.

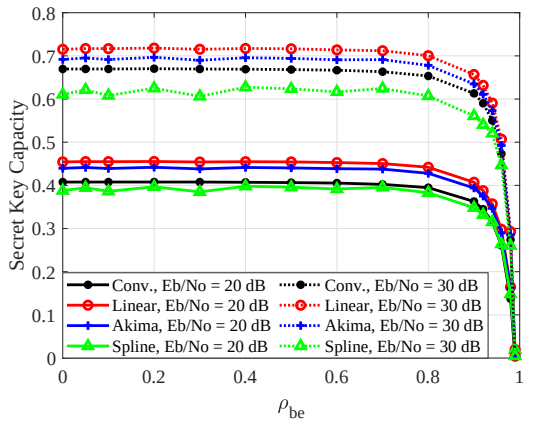


Fig. 13. SKC versus $\rho_{be}$ in the proposed scheme with the three interpolation methods at Eb/No = 20 and 30 dB. The full-pilot SKG scheme is also plotted as a benchmark.

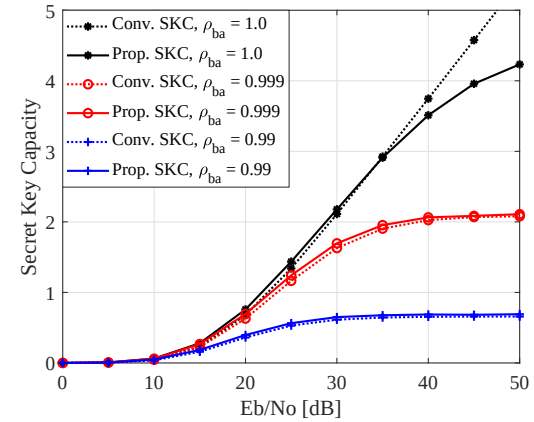


Fig. 14. Comparisons of SKC between the proposed scheme for $\rho_{ba} = 1.0$, 0.999, and 0.99. The full-pilot SKG scheme is also plotted as a benchmark.

Fig. 13 compares the three interpolation methods in terms of the SKC versus $\rho_{be}$ at Eb/No = 20 and 30 dB. The conventional full-pilot SKG is also plotted as a benchmark.

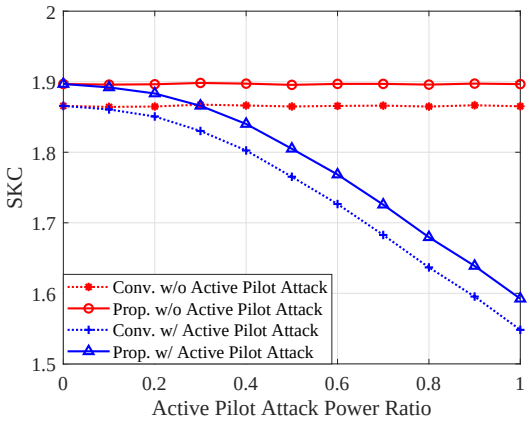


Fig. 15. Effects of the active pilot attack on the SKC performance of the proposed scheme for $\rho_{ba} = 0.99$ and $\rho_{be} = 0.64$. The full-pilot SKG scheme is also plotted as a benchmark.

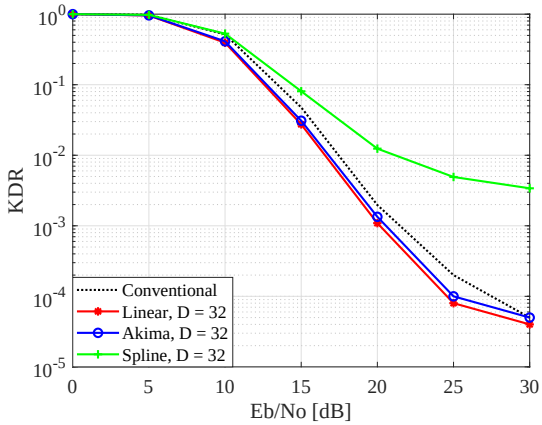


Fig. 16. KDR of the proposed scheme employing the three interpolation methods. The full-pilot SKG scheme is also plotted as a benchmark.

In Fig. 13, it is found that in each scenario, the SKC performance significantly improves upon decreasing $\rho_{be}$ from 1 to approximately 0.8. By contrast, the SKC remains almost constant for $\rho_{be} < 0.8$. Note that from (51), the effect of $\rho_{be}$ on the SKC is on the logarithmic scale since MI of the eavesdropper channel is substantially low for $\rho_{be} < 0.8$.

Fig. 14 shows the SKC of the proposed scheme for $\rho_{ba} = 1.0$, 0.999, and 0.99. In Fig. 14, it is observed that for $\rho_{ba} = 1$, the SKC of the conventional full-pilot benchmark scheme linearly increases with Eb/No. The proposed scheme outperforms the conventional scheme in the range of Eb/No $< 30$ dB. For $\rho_{ba} = 0.999$ and 0.99, the proposed scheme achieves better performance with a maximum of 1.4 % and 5.0 %, respectively, than the conventional scheme. Therefore, the proposed scheme is especially beneficial for the scenario with reciprocal imperfection.

Fig. 15 shows the effect of the active pilot attack on the SKC performance. We assume an active attack in which one adversary sends a pilot signal of a specific pattern to each of Alice and Bob to cause a desired change to the legitimate channel [40][41]. Here, the active pilot attack power ratio (APAPR) represents the ratio of the power of the signal transmitted as an active attack to that of the legitimate pilot signal. As shown in Fig. 15, SKC deteriorates as APAPR increases for both the proposed and conventional schemes in the presence of the active attack. Meanwhile, the proposed scheme exhibits superior SKC to the conventional scheme with a gain of 1.7 % under all APAPR active attacks.

### C. The Performance of Key Disagreement Ratio

To elaborate a little further, we evaluate the achievable KDR performance of the proposed scheme, where the effect of the eavesdropper channel is not taken into account. Here, the KDR represents how accurate the secret key shared among legitimate users is. It is assumed that SKG is successful only if the keys generated by Alice and Bob in (30) match; otherwise, the key disagreement event occurs. Note that in the ideal scenario with no channel estimation errors, the KDR becomes zero.

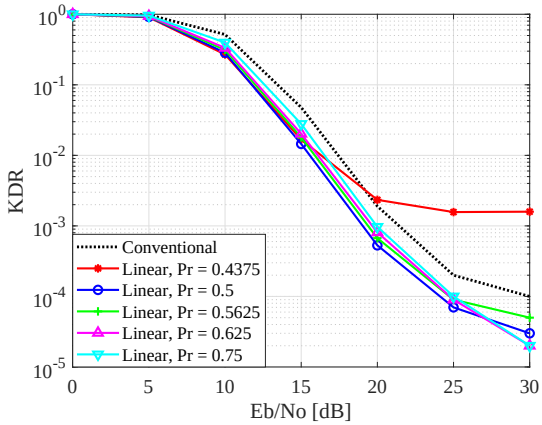


Fig. 17. KDR performance of the proposed scheme employing linear interpolation, where the pilot activation ratio is given by $P_r = 0.4375$, 0.5, 0.5625, 0.625, and 0.75.

Fig. 16 shows the KDR of the proposed scheme with the three interpolation methods. Similar to Fig. 9, the proposed schemes employing linear interpolation and Akima interpolation attain better KDR performance than the conventional scheme in the entire Eb/No region. As expected, the spline interpolation significantly deteriorates and exhibits an error floor due to the effects of overfitting.

Moreover, Fig. 17 shows the KDR performance of the proposed method employing linear interpolation, where the pilot activation ratio is given by $P_r = 0.4375$, 0.5, 0.5625, 0.625, and 0.75. As shown in Fig. 17, in the proposed scheme, upon reducing $P_r$, the KDR tends to improve while outperforming the conventional scheme except for the $P_r = 0.4375$ case. This is because the low pilot symbols lead to the reduction of power consumption, hence increasing the power efficiency.

Fig. 18 shows the KDR while varying the number of subcarriers. It can be seen that the proposed scheme exhibits a power reduction effect regardless of the number of subcarriers, especially in the low Eb/No region, and outperforms the conventional scheme. On the other hand, in the high Eb/No region, the proposed scheme causes an error floor, and performance

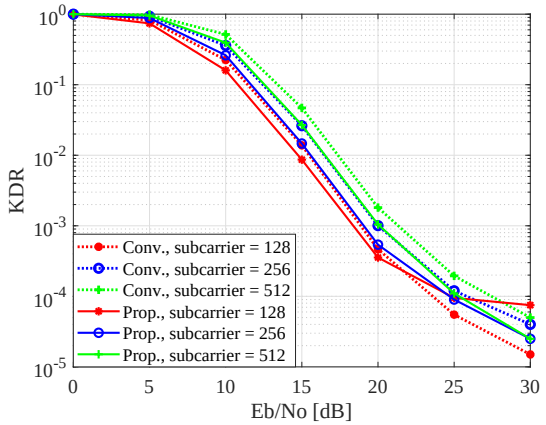


Fig. 18. KDR performance of the conventional and proposed scheme with various numbers of subcarriers.

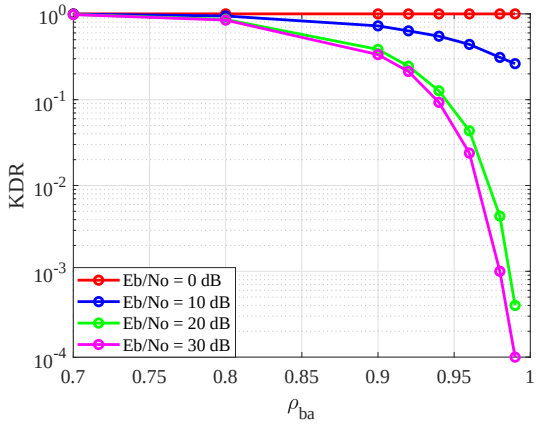


Fig. 19. KDR versus $\rho_{ba}$ of the proposed scheme employing linear interpolation at Eb/No = 0 dB, 10 dB, 20 dB, and 30 dB.

TABLE I
NIST RANDOMNESS TEST RESULTS

| Test | p-value |
|---|---|
| Frequency Monobit | 0.9296 |
| Frequency Block | 0.9289 |
| Runs | 0.4261 |
| Longest Run | 0.7431 |
| Discrete Fourier Transform | 0.2561 |
| Serial | 0.3963, 0.2142 |
| Approximate Entropy | 0.7678 |
| Cumulative Sums | 0.7375 |

degrades upon decreasing the number of subcarriers. This is because $D$ must be maintained above a certain level to preserve the selection of the reduction pattern.

Finally, Fig. 19 shows the relationship between the KDR and $\rho_{ba}$ in the proposed scheme with linear interpolation at $E_b/N_0 = 0$ dB, 10 dB, 20 dB, and 30 dB. As shown in Fig. 19, upon increasing $E_b/N_0$, the KDR performance significantly improves.

### D. Randomness test

We evaluate the randomness of the generated keys by the NIST randomness test [39]. There are 15 tests to verify randomness, and the output of these tests is a p-value where randomness is guaranteed if this value is greater than 0.01. In our simulations, the generated keys are 512 bits; thus, we perform 8 tests that can be sufficiently verified with a small number of bits. Table I shows the NIST test results of the proposed generated keys. The keys pass the randomness test, confirming that it has sufficient randomness.

## VII. Conclusions

In this paper, we proposed a novel physical-layer SKG scheme for improving SKC in the presence of an eavesdropper. The proposed scheme consists of the reduced pilot pattern selection algorithm that decreases the information leakage to the eavesdropper, as well as of the channel interpolation algorithm to estimate accurate full channel coefficients from the reduced pilot sequence. Also, we derived the SKC bound for the proposed scheme to evaluate the achievable performance. Our simulation results demonstrate that the proposed SKG scheme exhibits high performance, regardless of the channel correlation between the legitimate and eavesdropper channels, and maximizes the SKC even when the pilot length is reduced to as low as 62.5% of the original full-pilot one.

## 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, May/June 2020.

[2] S. J. Nawaz, S. K. Sharma, S. Wyne, M. N. Patwary, and M. Asaduzzaman, "Quantum machine learning for 6G communication networks: State-of-the-art and vision for the future," *IEEE Access*, vol. 7, pp. 46317-46350, 2019.

[3] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469-472, July 1985.

[4] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550-1573, 2014.

[5] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. I. Secret sharing," *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1121-1132, July 1993.

[6] K. Zeng, "Physical layer key generation in wireless networks: challenges and opportunities," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 33-39, June 2015.

[7] F. Kaltenberger, H. Jiang, M. Guillaud, and R. Knopp, "Relative channel reciprocity calibration in MIMO/TDD systems," *Proc. of the 2010 Future Network & Mobile Summit*, Florence, Italy, pp. 1-10, June 2010.

[8] Z. Gu, N. Wei, and Z. Zhang, "Timing synchronization reciprocity error cancellation in OFDM/TDD coordinated multi-point transmission system," *Proc. of 2012 IEEE Global Communications Conference (GLOBECOM)*, pp. 4752-4757, Dec. 2012.

[9] X. Jiang, M. Cirkic, F. Kaltenberger, E. G. Larsson, L. Deneire, and R. Knopp, "MIMO-TDD reciprocity under hardware imbalances: Experimental results," *Proc. of 2015 IEEE International Conference on Communications (ICC)*, pp. 4949-4953, June 2015.

[10] H. Liu, J. Yang, Y. Wang, Y. Chen, and C. E. Koksal, "Group secret key generation via received signal strength: Protocols, achievable rates, and implementation," *IEEE Transactions on Mobile Computing*, vol. 13, no. 12, pp. 2820-2835, Dec. 2014.

[11] Y. Luo, L. Pu, Z. Peng, and Z. Shi, "RSS-based secret key generation in underwater acoustic networks: Advantages, challenges, and performance improvements," *IEEE Communications Magazine*, vol. 54, no. 2, pp. 32-38, February 2016.

[12] H. Zhao, Y. Zhang, X. Huang, and Y. Xiang, "An adaptive secret key establishment scheme in smart home environments," *Proc. of 2019 IEEE International Conference on Communications (ICC)*, pp. 1-6, May 2019.

[13] Q. Wang, K. Xu and K. Ren, "Cooperative secret key generation from phase estimation in narrowband fading channels," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 9, pp. 1666-1674, October 2012.

[14] L. Wang, H. An, H. Zhu, and W. Liu, "MobiKey: Mobility-based secret key generation in smart home," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 7590-7600, Aug. 2020.

[15] Y. Matsuzaki, S. Kojima, and S. Sugiura, "Deep-learning-based physical-layer lightweight authentication in frequency-division duplex channel," *IEEE Communications Letters*, vol. 27, no. 8, pp. 1969-1973, Aug. 2023.

[16] N. K. Kundu, S. P. Dash, M. R. Mckay, and R. K. Mallik, "Channel estimation and secret key rate analysis of MIMO terahertz quantum key distribution," *IEEE Transactions on Communications*, vol. 70, no. 5, pp. 3350-3363, May 2022.

[17] J. Zhang, B. He, T. Q. Duong, and R. Woods, "On the key generation from correlated wireless channels," *IEEE Communications Letters*, vol. 21, no. 4, pp. 961-964, Apr. 2017.

[18] F. Rottenberg, T. -H. Nguyen, J. -M. Dricot, F. Horlin, and J. Louveaux, "CSI-based versus RSS-based secret-key generation under correlated eavesdropping," *IEEE Transactions on Communications*, vol. 69, no. 3, pp. 1868-1881, Mar. 2021.

[19] T. -Y. Liu, P. -H. Lin, S. -C. Lin, Y. -W. P. Hong, and E. A. Jorswieck, "To avoid or not to avoid CSI leakage in physical layer secret communication systems," *IEEE Communications Magazine*, vol. 53, no. 12, pp. 19-25, Dec. 2015.

[20] Y. Chen, K. Huang, Y. Zhou, K. Ma, H. Jin, and X. Xu, "Physical layer key generation scheme through scrambling the correlated eavesdropping channel," *IEEE Access*, vol. 8, pp. 48982-48990, 2020.

[21] N. Aldaghri and H. Mahdavifar, "Physical layer secret key generation in static environments," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2692-2705, Feb. 2020.

[22] H. Liu, Y. Wang, Y. Ren, and Y. Chen, "Bipartite graph matching based secret key generation," *Proc. of IEEE INFOCOM 2021*, pp. 1-10, May 2021.

[23] D. Qin, and Z. Ding, "Exploiting multi-antenna non-reciprocal channels for shared secret key generation," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 12, pp. 2693-2705, Dec. 2016.

[24] H. Jin, K. Huang, L. Jin, Z. Zhong, and Y. Chen, "Physical-layer secret key generation with correlated eavesdropping channel," *Proc. of 2018 IEEE 4th International Conference on Computer and Communications (ICCC)*, pp. 226-231, Dec. 2018.

[25] C. Zenger, J. Zimmer, and C. Paar, "Security analysis of quantization schemes for channel-based key extraction," *Proc. of Workshop Wireless Commun. Secur. Phys. Layer*, pp. 267-272, Jul. 2015.

[26] H. Jin, K. Huang, S. Xiao, Y. Lou, X. Xu, and Y. Chen, "A two-layer secure quantization algorithm for secret key generation with correlated eavesdropping channel," *IEEE Access*, vol. 7, pp. 26480-26487, 2019.

[27] P. Dent, G. Bottomley, and T. Croft, "Jakes fading model revisited," *Electron. Lett.*, vol. 29, no. 3, pp. 1162-1163, Jun. 1993.

[28] K. Polonen and V. Koivunen, "Iterative interpolation method for multiband-OFDM channel estimation," *Proc. of 2007 IEEE International Conference on Ultra-Wideband*, pp. 225-228, Sep. 2007.

[29] 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, Dec. 2018.

[30] M. Zorgui, Z. Rezki, B. Alomair and M. -S. Alouini, "The diversity-multiplexing tradeoff of secret-key agreement over multiple antenna channels," *IEEE Transactions on Wireless Communications*, vol. 15, no. 2, pp. 1562-1574, Feb. 2016.

[31] M. Sandell, "Secret key generation with multiantenna relays," *IEEE Access*, vol. 11, pp. 8387-8396, 2023.

[32] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, pp. 614-626, 2016.

[33] Y. Wei, K. Zeng, and P. Mohapatra, "Adaptive wireless channel probing for shared key generation based on PID controller," *IEEE Transactions on Mobile Computing*, vol. 12, no. 9, pp. 1842-1852, Sept. 2013.

[34] Y. Liu, S. C. Draper, and A. M. Sayeed, "Exploiting channel diversity in secret key generation from multipath fading randomness," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 5, pp. 1484-1497, Oct. 2012.

[35] S. N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "Secret key extraction from wireless signal strength in real environments," *IEEE Transactions on Mobile Computing*, vol. 12, no. 5, pp. 917-930, May 2013.

[36] H. Akima, "A new method of interpolation and smooth curve fitting based on local procedures," *Journal of the Association for Computing Machinery*, vol. 17, no. 4, pp. 589-602, Oct. 1970.

[37] Y. Peng, P. Wang, W. Xiang, and Y. Li, "Secret key generation based on estimated channel state information for TDD-OFDM systems over fading channels," *IEEE Transactions on Wireless Communications*, vol. 16, no. 8, pp. 5176-5186, Aug. 2017.

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

[39] F. Pareschi, R. Rovatti, and G. Setti, "On statistical tests for randomness included in the NIST SP800-22 test suite and based on the binomial distribution," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 491-505, Apr. 2012.

[40] A. Bereyhi, S. Asaad, R. R. M 端 ller, R. F. Schaefer, and H. V. Poor, "Secure transmission in IRS-assisted MIMO systems with active eavesdroppers," *Proc. of 54th Asilomar Conf. Signals, Syst., Comput.*, pp. 718-725, Nov. 2020.

[41] J. Li, P. Wang, L. Jiao, Z. Yan, K. Zeng, and Y. Yang, "Security analysis of triangle channel-based physical layer key generation in wireless backscatter communications," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 948-964, 2023.

**Shun Kojima** (Member, IEEE) received the B.E., M.E., and Ph.D. degrees in electrical and electronics engineering from Chiba University, Japan, in 2017, 2018, and 2021, respectively. From 2021 to 2022, he was an Assistant Professor with the Department of Fundamental Engineering, Utsunomiya University, Tochigi, Japan. He is currently a Project Research Associate with the Institute of Industrial Science, The University of Tokyo, Tokyo, Japan. His research interests include adaptive modulation and coding, visible light communications, physical layer security, and machine learning. He received the Best Paper Award at the 26th International Conference on Software, Telecommunications and Computer Networks in 2018, the Best Poster Award at the 3rd Communication Quality Student Workshop in 2019, the IEEE VTS Tokyo/Japan Chapter 2020 Young Researcher's Encouragement Award, the RISP Best Paper Award in 2021, the Institute of Electronics, Information and Communication Engineers (IEICE) Radio Communication Systems Active Researcher Award in 2021, the IEICE Young Researchers Award in 2023, and the Takayanagi Research Encouragement Award in 2023.

**Shinya Sugiura** (M'06–SM'12) received the B.S. and M.S. degrees in aeronautics and astronautics from Kyoto University, Kyoto, Japan, in 2002 and 2004, respectively, and the Ph.D. degree in electronics and electrical engineering from the University of Southampton, Southampton, U.K., in 2010.

From 2004 to 2012, he was a Research Scientist with Toyota Central R&D Labs., Inc., Nagakute, Japan. From 2013 to 2018, he was an Associate Professor with the Department of Computer and Information Sciences, Tokyo University of Agriculture and Technology, Koganei, Japan. Since 2018, he has been an Associate Professor with the Institute of Industrial Science, The University of Tokyo, Tokyo, Japan, where he heads the Wireless Communications Research Group. His research has covered a range of areas in wireless communications, networking, signal processing, and antenna technology. He authored or coauthored over 100 IEEE journal and magazine papers.