User-Independent Randomized Pilot Activation for Secure Key Generation

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

***Abstract*—In this paper, we propose a novel physical-layer secret key generation (SKG), which randomly activates a pilot sequence during the channel probing phase. Each legitimate user interpolates the received signals to recover the full channel state information (CSI). Due to the random reduction of the pilot sequence, the proposed scheme can degrade the eavesdropping performance regardless of the correlation between legitimate users and eavesdroppers, thereby improving the secret key capacity (SKC). Furthermore, low power consumption during the channel probing phase can be achieved. Our simulation results demonstrate that the proposed scheme exhibits superior performance in the presence of eavesdroppers.**

***Index Terms*—eavesdropping channel, low power consumption, pilot design, secrecy outage probability, secret key capacity, secret key generation.**

I. Introduction

Securing communications will be crucial in the Internet of Things; automated driving and telemedicine are expected to be realized with 6G [1]. However, guaranteeing security is a severe issue in wireless communications due to its broadcasting nature. Historically, key-based encryption schemes, such as symmetric and asymmetric key cryptography, have been widely used in conventional wireless communications [2]. A symmetric key cryptosystem uses a secret key shared between the transmitter and receiver to encrypt and decrypt with the same key. Note that asymmetric key cryptography uses a public key for encryption and a secret key for decryption, where security is guaranteed due to its computational complexity.

The recent development of quantum computing technology threatens computationally secure encryption schemes. In [3], it is indicated that secret key encryption may be broken by a quantum brute force attack with Grover's quantum algorithm. Furthermore, Shor's quantum algorithm is proved to potentially break asymmetric key cryptography in polynomial time [4]. While lattice- and code-based resistant quantum asymmetric key cryptography has been investigated [4], the assumption that no quantum algorithm can solve NP-hard problems and the computational complexity issue is shaking the foundations of encryption security.

Preprint (Accepted Version). DOI: 10.1109/TWC.2024.3383868.

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.*)

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

To tackle the above-mentioned security challenges, physical-layer secret key generation (SKG), which generates a secret key from reciprocal wireless channels [5–7], has attracted attention as an alternative to conventional cryptography. The SKG relies on the channel reciprocity between legitimate users and channel fluctuations as a random source of a secret key. If the eavesdropper is positioned more than a coherence distance away from the legitimate users under fading, the correlation between the legitimate channel and the eavesdropper's channel becomes sufficiently low, and the secret key shared among the legitimate users cannot be extracted. The SKG has the benefits of lightweight, flexible, and scalable characteristics compared to conventional encryption-based key exchange schemes [8].

In SKG implementation, there are four steps, i.e., channel probing, quantization, information reconciliation, and privacy amplification [9]. Channel probing is the most important step since it determines the success of SKG and the secrecy key rate. More specifically, the legitimate users send pilot signals to each other through a reciprocal channel to obtain the same channel state information (CSI). The design of the pilot signal used for channel probing is crucial for its practical SKG application. In [10], increasing the number of pilot signals allows for highly accurate CSI acquisition. Additionally, in [11], it is suggested that the secret key rate increases upon increasing the transmit power. The authors in [12] show that there is a trade-off between total power consumption and total bandwidth in SKG for wireless sensor networks. Furthermore, in [13], the secret key capacity in multiple antenna systems is analyzed in terms of transmit power. However, to the best of our knowledge, no works have addressed improving the power efficiency in SKG. A further challenge is that if the eavesdropper is positioned close to either of the legitimate users, the correlation between the eavesdropping channel and the legitimate channel becomes high, hence suffering from the increased possibility of information leakage [14].

Against the above-mentioned background, in this paper, we propose a novel SKG scheme using random pilot activation. More specifically, in the preliminary stage of channel probing, the random subset of pilot symbols is independently deactivated to zeros at each legitimate user. Then, the received pilot signals are interpolated to achieve full CSI. This improves power efficiency as the benefit of reduced pilot overhead. While the interpolation allows the channel reciprocity between the legitimate users to be maintained, it prevents an eavesdropper from specifying the reduced portions correctly, degrading eavesdropping performance. Our major contributions can be summarized as follows.

1) We present a novel SKG scheme that improves power efficiency and suppresses information leakage by randomly reducing pilot signals at the transmitter and interpolating the received CSI at the receiver. The idea of enhancing confidentiality to eavesdroppers by deactivating the pilot signal is new, which also reduces power consumption.
2) We provide a detailed analysis of the proposed SKG and implement a comprehensive framework for the practical SKG process. Additionally, we derive a theoretically achievable SKC that takes into account the influence of the eavesdropper.
3) We numerically evaluate the performance of the proposed SKG algorithm in a practical fading channel. Simulation results demonstrate that the proposed scheme outperforms the conventional SKG in terms of mutual information (MI), SKC, key disagreement rate (KDR), secrecy outage probability (SOP), and randomness tests.

The remainder of this paper is organized as follows. In Section II, we review the related SKG studies. Section III introduces the system model of the proposed SKG scheme. In Section IV, we propose our SKG scheme with generalized random pilot activation. In Section V, our simulation results are provided, and finally, Section VI concludes this paper.

II. Related Work

In this section, we review the related studies, which aim to improve SKG performance. Some schemes focused on preprocessing to enhance secrecy performance by improving the reciprocity among legitimate users [15–18]. In [15], the curve fitting method was proposed, where a measured channel is preprocessed to reduce the number of discrepancies and improve the secrecy SKG performance. Lin *et al.* [16] proposed preprocessing the received signal strength (RSS) measurements using the wavelet shrinkage based on rigrsure, which is an adaptive threshold selection algorithm. In [17], the SKG scheme with moving average filtering was proposed to achieve reliable and efficient SKG. Moreover, in [18], the SKG involving multiple users, using the Savitzky Golay filter preprocessing, was proposed to enhance the RSS reciprocity for legitimate users. The schemes of [15–18] improve the correlation of channel measurements between legitimate users, hence enhancing the reliability of SKG. However, the effects of eavesdroppers are not considered despite the fact that eavesdroppers may also improve eavesdropping performance with the aid of such preprocessing methods.

Several methods based on artificial randomness have been studied to improve the confidentiality of SKG [19–25]. In [19], the SKG scheme superimposing artificial noise was developed in the presence of a passive eavesdropper. Chen *et al.* [20] presented the SKG with known artificial interference in a narrowband fading channel, where the resultant increased channel variation enhances the randomness of the secret key. In [21], the eavesdropping-resilient OFDM system based on sorted subcarrier interleaving was proposed. Here, interleaving is carried out at the transmitter based on CSI of the reciprocal legitimate channel, while deinterleaving is used at the receiver. Li *et al.* [22] proposed the artificial randomness scheme for high-rate SKG in a slow-fading environment. In this scheme, one legitimate user generates a random sequence and combines it with the obtained slow-fading channel, which increases the randomness of SKG. In [23], the channel-based random subcarrier selection and artificial signal design were proposed. Using uncorrelated subcarriers provides increased randomness and alleviates the temporal correlation issue of adjacent subcarriers. In [24], the low-complexity artificial randomness scheme was proposed to achieve a high secret key rate in static environments, where artificial randomness is added independently at the legitimate users to generate secret keys. The authors in [25] proposed the pilot randomization scheme to mitigate the injection attack by converting them to jamming attacks, which constitute a less severe threat. This artificial randomness scheme achieves a superior performance against eavesdroppers at the sacrifice of decreased power efficiency and increased information leakage due to the need for CSI feedback.

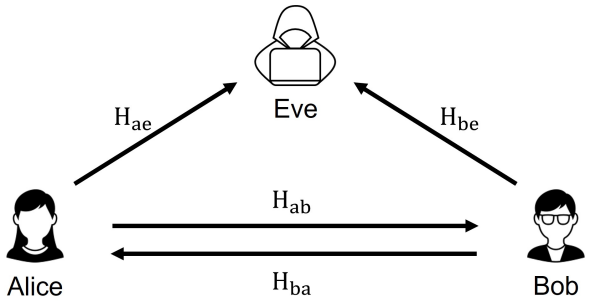


Fig. 1. System model in the presence of an eavesdropper.

In this paper, we focus on reducing information leakage to eavesdroppers and maintaining high SKC while improving power efficiency. The definitive difference compared to [15–18] is that the proposed scheme recovers CSI from the randomly reduced pilot signal, while the conventional methods aim at smoothing acquired CSI and improving the channel correlation. Furthermore, in contrast, to [19–25], the proposed scheme introduces artificial random reduction of the pilot signal to reduce information leakage by itself and improve the power efficiency of channel probing.

III. System Model

This paper considers two legitimate users, Alice and Bob, and a passive eavesdropper, Eve, as shown in Fig. 1. Although Eve does not launch active attacks, she can eavesdrop on signals from Alice and Bob to obtain their respective CSIs. In addition, Eve is assumed to know all protocols and parameters of key generation between Alice and Bob.

A. Channel Model

We assume the frequency-selective channels, which are widely used in SKG. The complex-valued baseband representation of channel impulse response is given by

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

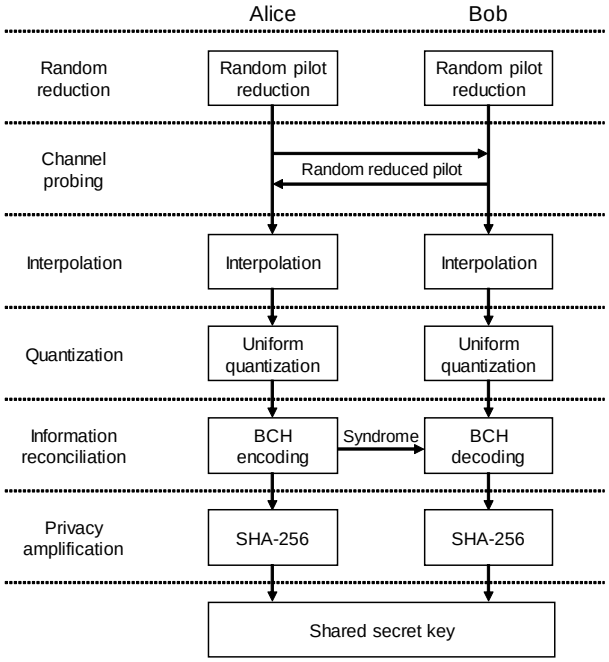


Fig. 2. Proposed SKG scheme.

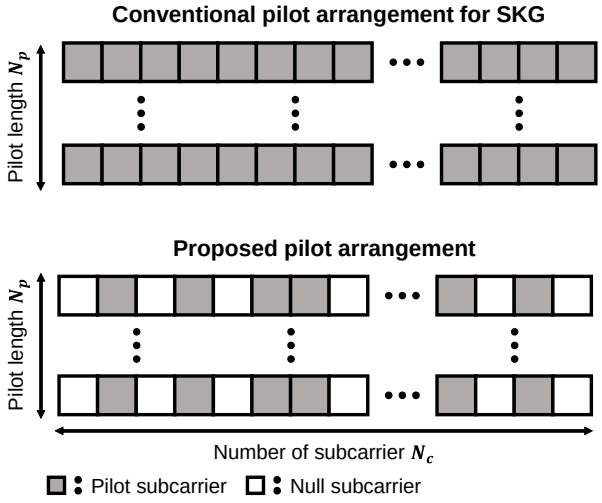


Fig. 3. Comparison of the pilot arrangement between conventional and proposed scheme.

where L, $h_l(t)$, and τ_l indicate the number of paths, corresponding complex-valued attenuation coefficient, and delay of the l-th path, respectively. $\delta(\cdot)$ represents the Dirac delta function. Here, the channel frequency response of the Fourier transformed $h(t,\tau)$ is expressed as

$$H(t,f) = \int_0^\infty h(t,\tau)e^{-j2\pi f\tau}d\tau. \tag{2}$$

The received signal in the time domain can be represented by

$$r(t) = \int_{-\infty}^{\infty} h(t,\tau)s(t-\tau)d\tau + n(t), \tag{3}$$

where $s(t)$ and $n(t)$ denote the transmitted signal and additive white Gaussian noise (AWGN), which is a zero-mean normal distribution with variance σ_n^2, represented by $\mathcal{CN}(0,\sigma_n^2)$. Similar to (2), the frequency-domain representation of the received signal by Fourier transform is expressed as

$$R(t,f_n) = H(t,f_n)S(f_n) + N(t,f_n), \tag{4}$$

where f_n indicates the n-th subcarrier frequency.

B. Legitimate and Eavesdropping Channel

As illustrated in Fig. 1, this paper assumes Eve is close to the legitimate user and correlated with the legitimate channel. Here, we consider a time-division duplex (TDD) system generally used in SKG. CSI obtained by each legitimate user has reciprocity, assuming in the coherence time. Since the channel assumed in (2) is time-varying Rayleigh fading, the channel gain H_{ab} from Alice to Bob and H_{ba} from Bob to Alice are $H_{ab} = H_{ba} \sim \mathcal{CN}(0,\sigma_h^2)$. The correlation coefficient between legitimate users can be expressed as

$$\rho_{ba} = \frac{E\{{H_{ab}}^\dagger H_{ba}\}}{\sigma_h^2}, \tag{5}$$

where $E\{\cdot\}$ indicates the expectation operation and $(\cdot)^\dagger$ means the conjugate transpose. The eavesdropping channel H_{ae} and H_{be} are also a Rayleigh fading channel, $H_{ae} = H_{be} \sim \mathcal{CN}(0,\sigma_e^2)$. The correlation coefficients between legitimate and eavesdropping channels are represented as

$$\rho_{ae} = \frac{E\{{H_{ab}}^\dagger H_{ae}\}}{\sigma_h\sigma_e} \tag{6}$$

$$\rho_{be} = \frac{E\{{H_{ab}}^\dagger H_{be}\}}{\sigma_h\sigma_e}. \tag{7}$$

IV. Proposed scheme

This section proposes our SKG scheme, which utilizes randomized pilot activation. The proposed SKG procedure is shown in Fig. 2. Our proposed scheme consists of the following six steps: 1) random reduction of the pilot sequence, 2) channel probing from the reduced pilot sequence, 3) reconstructing the CSI by interpolation, 4) quantization, 5) information reconciliation, and 6) privacy amplification.

A. Random Reduction of Pilot Sequence

In the proposed scheme, the pilot signals per frame are randomly reduced. Fig. 3 shows the pilot arrangement of the conventional and proposed schemes to obtain CSI for SKG. In conventional SKG, a large number of pilot signals have been required to share accurate keys based on channel reciprocity, which poses challenges regarding power efficiency and information leakage to eavesdroppers. Therefore, the proposed scheme uses a randomly reduced pilot sequence of that signal as opposed to the conventional pilot arrangement, which has the effect of reducing power consumption and inhibiting correct decoding by the eavesdropper due to its

randomness. Assuming an OFDM pilot sequence consisting of N_c subcarriers, it can be represented as

$$\mathbf{S_p} = \{s_i\}_{i=0}^{N_c-1}, \quad s_i \in \{0,1\}, \tag{8}$$

where i indicates the index of the subcarriers, and s_i represents which subcarriers are activated or deactivated. Here, the reduction ratio Pr is expressed as

$$P_r = \frac{|\{i \,|\, s_i = 0\}|}{|\{i \,|\, s_i = 1\}|}. \tag{9}$$

In the proposed scheme, Alice and Bob independently carry out the random reduction of the pilot sequence based on the reduction rate P_r. The random reduced pilot sequence for Alice and Bob, respectively, can be expressed as

$$\mathbf{S}_{ba} = \{s_a\}_{a=0}^{N_c-1}, \quad s_a \in \{0,1\} \tag{10}$$

$$\mathbf{S}_{ab} = \{s_b\}_{b=0}^{N_c-1}, \quad s_b \in \{0,1\}. \tag{11}$$

B. Channel Probing

In the TDD-OFDM system assumed in this paper, Alice and Bob alternately transmit pilot sequences (10) and (11) after insertion of the cyclic prefix (CP) with each other. We assume that the time and frequency synchronization between Alice and Bob is also perfect. Meanwhile, the received signal at Alice and Bob after removing the CP is expressed as

$$\mathbf{R}_{ba} = H_{ba}\mathbf{S}_{ba} + \mathbf{n}_{ba} \tag{12}$$

$$\mathbf{R}_{ab} = H_{ab}\mathbf{S}_{ab} + \mathbf{n}_{ab}, \tag{13}$$

where $\mathbf{n}_{ba}$, $\mathbf{n}_{ab}$ are AWGN with variance of $\sigma_{n_0}^2$. At the receiver side, the channel is estimated by least square (LS) estimation, which is expressed as

$$\hat{H}_{ba} = \frac{\mathbf{S}_{ba}^{\dagger}}{\|\mathbf{S}_{ba}\|^2}\mathbf{R}_{ba} = H_{ba} + \frac{\mathbf{S}_{ba}^{\dagger}}{\|\mathbf{S}_{ba}\|^2}\mathbf{n}_{ba} \tag{14}$$

$$\hat{H}_{ab} = \frac{\mathbf{S}_{ab}^{\dagger}}{\|\mathbf{S}_{ab}\|^2}\mathbf{R}_{ab} = H_{ab} + \frac{\mathbf{S}_{ab}^{\dagger}}{\|\mathbf{S}_{ab}\|^2}\mathbf{n}_{ab}, \tag{15}$$

where $\|\cdot\|$ denotes the Euclidean norm. Here, the estimated legitimate channel gains are random Gaussian variables with zero mean and variance $\sigma_h^2 + \frac{\sigma_{n_0}^2}{\|\mathbf{S}_{ba}\|^2}$ and $\sigma_h^2 + \frac{\sigma_{n_0}^2}{\|\mathbf{S}_{ab}\|^2}$. These processes are assumed to be carried out within a coherence time T_c. Let Δt be the time required for these processes, expressed by

$$\Delta t < T_c \approx \frac{1}{f_m}. \tag{16}$$

where f_m is the maximum Doppler spread of the channel.

C. Interpolation

Since the CSI obtained by (14) and (15) are estimates based on randomly reduced pilot sequences, interpolation is required to compensate for channel reciprocity. In this paper, we use spline cubic interpolation to interpolate the obtained CSI [26]. The CSI applying spline cubic interpolation and restoring the reduced portions is expressed as

$$\begin{aligned}\tilde{H}_{uv}(i+\delta_{uv}(i)) = \epsilon_0\hat{H}_{uv}(i) + \epsilon_1\hat{H}_{uv}(i+1) \\ -\Delta_p\epsilon_0\hat{H}'_{uv}(i) + \Delta_p\epsilon_1\hat{H}'_{uv}(i+1), \\ i = 0, 1, ..., N_cP_r - 1\end{aligned} \tag{17}$$

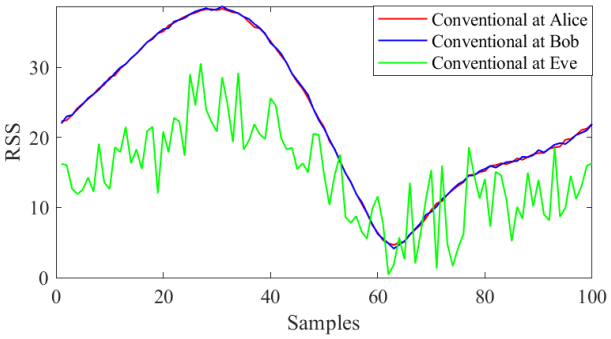
where

$$\epsilon_0 = 3\frac{\delta_{uv}(i)^2}{{\Delta_p}^2} - 2\frac{\delta_{uv}(i)^3}{{\Delta_p}^3} \tag{18}$$

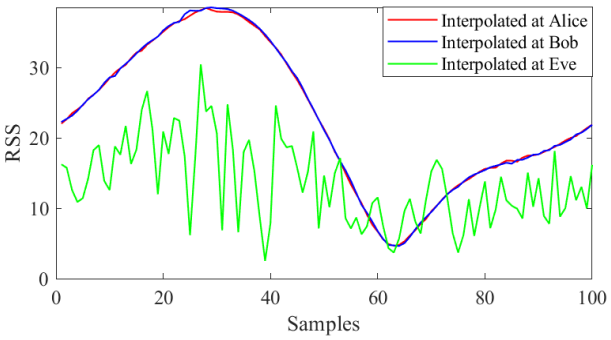
$$\epsilon_1 = 3\frac{(\Delta_p - \delta_{uv}(i))^2}{{\Delta_p}^2} - 2\frac{(\Delta_p - \delta_{uv}(i))^3}{{\Delta_p}^3}. \tag{19}$$

Here, we have $\{u, v\} = \{a, b, e\}$ while $\hat{H}'_{uv}$ indicates the first order derivative of $\hat{H}_{uv}$. $\delta_{uv}(i)$ and Δ_p represent the index of the randomly reduced portion and frequency interval of the active pilot, respectively.

In this method, the reduced portions have to be identified at the receiver side. However, these portions are randomly determined at the transmitter side. Therefore, based on the P_r shared among users, the index $\delta_{uv}(i)$ is determined by selecting a smaller received power as the reduction portion. Fig. 4 compares received signal strength (RSS) values at Alice, Bob, and Eve for the conventional and proposed scheme, which employs random pilot reduction and interpolation. Fig. 4(a) shows the RSS using the conventional scheme, where the RSS for Alice and Bob are almost identical, whereas Eve has a different RSS. In contrast, using the proposed scheme in Fig. 4(b), the RSS of Alice and Bob are almost the same



(a) Conventional RSS



(b) Proposed RSS

Fig. 4. RSS measurements of Alice, Bob, and Eve with or without proposed random pilot reduction and interpolation. Here, the correlation of legitimate users is $\rho_{ba} = 1.0$, that of eavesdroppers is $\rho_{be} = 0.6$, the reduction ratio P_r is 0.75, and Eb/No is 30 dB.

despite the random reduction of the pilot signal, while the RSS of Eve is different from that of Fig. 4(a). More specifically, in the conventional scheme (Fig. 4(a)), the RSS of Eve has a more similar peaked shape to those of Alice and Bob, especially between 0 and 40 samples than in the proposed scheme (Fig. 4(b)) This confirms that the proposed scheme makes it more difficult for Eve to access CSI of the legitimate users.

D. Quantization

The analog CSI value obtained in (17) has to be converted to a binary value to generate a secret key that can be shared among legitimate users. In SKG, there are two general schemes of quantization: RSS-based quantization [27] and phase information-based quantization schemes [28]. In this paper, we adopt an RSS-based scheme, which is easy to acquire at the receiver and has a high affinity with the proposed scheme, compensating for the reduced portions by interpolation. Furthermore, in the proposed scheme, the reciprocity of CSI shared by Alice and Bob may be lower due to the random reduction of pilot sequences and interpolation. Therefore, a quantization scheme that can improve the key agreement using a guard band gap is adopted [27].

To be specific, assuming $\tilde{H}_{uv}$ to be the CSI acquired and interpolated at the receiver side, the threshold for quantization is expressed using the mean $\mu_{\tilde{H}_{uv}}$ and standard deviation $\sigma_{\tilde{H}_{uv}}$ of $\tilde{H}_{uv}$ as

$$\xi_{upper} = \mu_{\tilde{H}_{uv}} + \sigma_{\tilde{H}_{uv}} \Delta_q \tag{20}$$

$$\xi_{lower} = \mu_{\tilde{H}_{uv}} - \sigma_{\tilde{H}_{uv}} \Delta_q. \tag{21}$$

Here, ξ_{upper} and ξ_{lower} represent the upper and lower boundaries of the quantization interval. Also, Δ_q indicates the quantization guard band. Considering a 1-bit quantizer using these thresholds, the quantized bit can be expressed as

$$K_{uv} = \begin{cases} 1 & |\tilde{H}_{uv}(i)| > \xi_{upper} \\ 0 & |\tilde{H}_{uv}(i)| \leq \xi_{lower} \\ \text{none} & \xi_{lower} < |\tilde{H}_{uv}(i)| \leq \xi_{upper}, \end{cases} \tag{22}$$

To meet the constraint of $\xi_{lower} > 0$, the upper bound has to be in the range of

$$\Delta_q < \frac{\mu_{\tilde{H}_{uv}}}{\sigma_{\tilde{H}_{uv}}} = \sqrt{\frac{\pi}{4-\pi}}. \tag{23}$$

Note that estimated CSI that fall into the guard band gap are excluded from the generated secret key because of their unreliability. There is a trade-off in quantization performance where a higher Δ_q value shortens the key length while improving the key agreement rate.

E. Information Reconciliation

From (22), the quantized bits obtained by Alice and Bob may be inconsistent due to noise and imperfect reciprocity. To enhance the agreement rate, the process of information reconciliation is imperative. In this paper, we adopt the Bose Chaudhuri Hocquenghem (BCH) codes as the information reconciliation for SKG. While high channel reciprocity between legitimate users is assumed, the potential key mismatches are corrected by BCH error correction codes. Furthermore, BCH codes are based on a simple algebraic method, referred to as syndrome decoding [9]. Hence, flexible adjustment of block length and error correction capability is achievable. The BCH code is given by (n, k, t), where $n = 2^m - 1$ indicates the code length, k is the information bit length, and t denotes the error correction capability. In BCH codes, k information bits are turned into n codewords containing $n - k$ parity bits to correct a maximum of t errors.

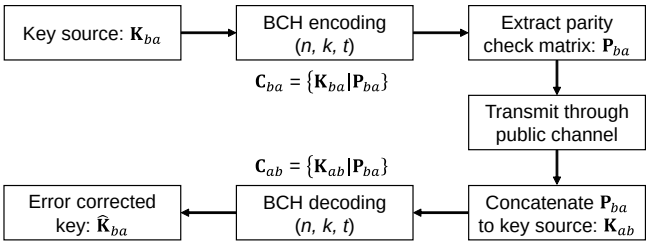


Fig. 5. Information reconciliation using BCH codes.

The procedure for information reconciliation using BCH codes is shown in Fig. 5. Alice first encodes the quantization values $\mathbf{K}_{ba}$ obtained in (22) with BCH encoding. The encoded signal is represented as

$$\mathbf{C}_{ba} = \{\mathbf{K}_{ba} \mid \mathbf{P}_{ba}\}, \tag{24}$$

where $\{\cdot|\cdot\}$ indicates the concatenation of row vectors. $\mathbf{K}_{ba} \in \mathbb{R}^{k\times 1}$ and $\mathbf{P}_{ba} \in \mathbb{R}^{(n-k)\times 1}$ denote the quantized values at Alice and parity check matrix, respectively. Then, to correct the error on Bob's side, Alice transmits $\mathbf{P}_{ba}$ as the syndrome through the public channel. Meanwhile, on Bob's side, the obtained quantization values and the received syndrome are used to generate the corresponding BCH codewords expressed as

$$\mathbf{C}_{ab} = \{\mathbf{K}_{ab} \mid \mathbf{P}_{ba}\}, \tag{25}$$

where $\mathbf{K}_{ab} \in \mathbb{R}^{k\times 1}$ is the quantized values at Bob. Using this codeword to perform BCH decoding, the difference between $\mathbf{K}_{ba}$ and $\mathbf{K}_{ab}$ is reconciled, and $\hat{\mathbf{K}}_{ab}$ with a high agreement rate can be obtained.

F. Privacy Amplification

In information reconciliation, the syndrome has to be shared through a public channel, raising the risk of information leakage to eavesdroppers. Thus, privacy amplification is needed to inhibit the effects of this leakage and enhance the security of shared keys. In this paper, secure hash algorithm 2 (SHA-2) is applied for privacy amplification [29]. SHA-2 has the characteristics of a one-way function, which is extremely difficult to reconstruct, as well as robustness to attacks.

G. Assumption of Eavesdropping

This paper assumes a passive eavesdropper who can eavesdrop on all communications between legitimate users. The

eavesdropper can obtain the signal from Alice and Bob due to the broadcasting nature of the radio wave,

$$\mathbf{R}_{ue} = H_{ue}\mathbf{S} + \mathbf{n}_{ue}, \quad u \in \{a, b\}. \tag{26}$$

Eve performs the procedure in (14)–(22) using this received signal to obtain the quantized value of the eavesdropping CSI, which can be expressed as $\mathbf{K}_{ue}$. Here, the eavesdropped syndrome P_{ba} generates the BCH codeword represented by

$$\mathbf{C}_{ue} = \{\mathbf{K}_{ue} \mid \mathbf{P}_{ba}\}, \quad u \in \{a, b\}. \tag{27}$$

Then, BCH decoding is performed to obtain the information-reconciled $\hat{\mathbf{K}}_{ue}$ at Eve.

H. Theoretical Secrecy Rate

In this subsection, we derive the SKC in the proposed scheme to evaluate the achievable SKC, considering the influence of Eve. The mutual information between legitimate users and that between a legitimate user and Eve can be represented as

$$I(\tilde{H}_{ba}, \tilde{H}_{ab}) = H(\tilde{H}_{ba}) + H(\tilde{H}_{ab}) - H(\tilde{H}_{ab}, \tilde{H}_{ba}) \tag{28}$$
$$I(\tilde{H}_{ba}, \tilde{H}_{be}) = H(\tilde{H}_{ba}) + H(\tilde{H}_{be}) - H(\tilde{H}_{be}, \tilde{H}_{ba}), \tag{29}$$

where $H(\cdot)$ means the entropy. Thus, the SKC, taking into account Eve, can be expressed using the mutual information as

$$C_S = I(\tilde{H}_{ba}, \tilde{H}_{ab}) - I(\tilde{H}_{ba}, \tilde{H}_{be}). \tag{30}$$

Since obtaining the closed-form expression of SKC is an open problem, this paper attempts to obtain it by directly calculating the mutual information. We utilize the mutual information estimation method based on k-nearest neighbor distances [30]. The estimate of MI can be represented as

$$I(X, Y) = \psi(k) + \psi(N) - \langle \psi(n_x + 1) + \psi(n_y + 1) \rangle, \tag{31}$$

where k is the number of nearest neighbors and N is the length of the input measurements, $X = [x_1, x_2, ..., x_N]$ and $Y = [y_1, y_2, ..., y_N]$. $\langle \cdot \rangle$ means the average over all elements. n_x indicates the number of points x_j with a distance from x_i less than $\epsilon(i)/2$, and n_y is similar to n_x. Here, the distance from x_i and y_i to their k-th nearest neighbors are $\epsilon_x(i)/2$ and $\epsilon_y(i)/2$, thus $\epsilon(i) = \max\{\epsilon_x(i), \epsilon_y(i)\}$. $\psi(\cdot)$ denotes the digamma function, which can be represented as

$$\psi(x) = \frac{d}{dx} \ln \Gamma(x) = \lim_{n \to \infty} \left\{ \ln n - \frac{1}{x} - \sum_{j=1}^{n} \frac{1}{x + j} \right\}. \tag{32}$$

For $x = 1$,

$$\psi(1) = \lim_{n \to \infty} \left\{ \ln n - \sum_{j=1}^{n} \frac{1}{j} \right\} = -\gamma, \tag{33}$$

where γ is the Euler's constant. Furthermore, the digamma function satisfies the following recurrence relationship:

$$\psi(x + 1) = \psi_x + \frac{1}{x}. \tag{34}$$

Then, the SKC is computed according to (30).

V. Performance Results

In this section, we provide a comprehensive numerical analysis of the proposed SKG with the randomized pilot activation. The effectiveness of the proposed scheme is intensively evaluated from the viewpoint of MI, SKC, and SOP in the presence of an eavesdropper compared to the conventional benchmark. Here, we use SKG without pilot signal reduction as the conventional benchmark. Additionally, the generated keys are validated through the randomness test. In our simulations, we consider TDD-OFDM systems and assume that the processes in the proposed SKG are carried out in coherence time. Here, the channel bandwidth is 2.4 GHz, $L = 15$ paths are generated to represent each multipath fading channel with exponential attenuation, and the Doppler frequency is given by 10 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 $\Delta_q = 0.1$. It is assumed that the pilot reduction ratio and the procedure of the proposed scheme are shared by all users in advance. For a fair comparison with respect to power efficiency, energy per bit to noise power spectral density ratio (Eb/No) is employed in our evaluations. More specifically, Eb/No of the pilot sequence is defined using signal-to-noise ratio (SNR) and P_r as follows:

$$\text{Eb/No} = \text{SNR} + 10 \log_{10}(P_r) \text{ in dB}. \tag{35}$$

A. Key Disagreement Rate

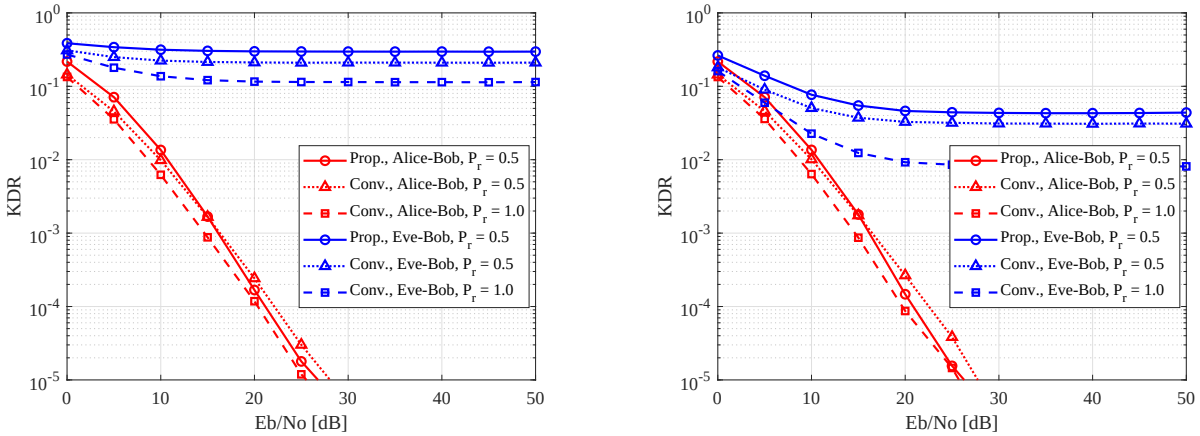
Firstly, to investigate the reliability of the proposed scheme, we compared the KDR. The KDR between the legitimate users and the eavesdropper are represented, respectively, by

$$P_k^{ba} = \frac{\sum_{j=1}^{N_k} |K_{ba}(j) - \hat{K}_{ab}(j)|}{N_k}, \tag{36}$$

$$P_k^{be} = \frac{\sum_{j=1}^{N_k} |K_{ba}(j) - \hat{K}_{be}(j)|}{N_k}. \tag{37}$$

where N_k denotes the key length, and $K_{ba}(j)$ is the j-th element of the generated key at Alice. Also, $\hat{K}_{ba}(j)$ and $\hat{K}_{be}(j)$ are the j-th element of the generated key at Bob and Eve, respectively. Note that each quantization value K_{uv} is calculated in (22).

Fig. 6(a) compares the KDRs of the legitimate user and Eve for $\rho_{ba} = 1.0$ and $\rho_{be} = 0.6$. The conventional scheme without pilot reduction $P_r = 1.0$ is considered a benchmark. We also show another conventional scheme where the pilot signal is reduced to half ($P_r = 0.5$), where the quantization level is doubled to achieve the same key length as those of other schemes. As shown in Fig. 6(a), the KDR of the conventional scheme with $P_r = 0.5$ is higher than the conventional scheme with $P_r = 1.0$ in each scenario. By contrast, the proposed scheme is close to the conventional one without pilot signal reduction in the high Eb/No region between Alice and Bob. Furthermore, the KDR performance between Eve and Bob is the worst as the benefits of our pilot reduction and interpolation.



(a) Correlation between the legitimate user and eavesdropper is $\rho_{be} = 0.6$

(b) Correlation between the legitimate user and eavesdropper is $\rho_{be} = 0.9$

Fig. 6. RSS measurements of Alice, Bob, and Eve with or without proposed random pilot reduction and interpolation. Here, the correlation of legitimate users is $\rho_{ba} = 1.0$, the reduction ratio P_r is 0.75, and Eb/No is 30 dB.

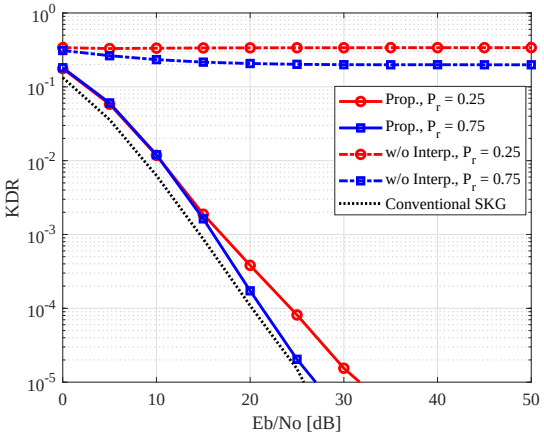


Fig. 7. The effect of the proposed CSI interpolation with $\rho_{ba} = 1.0$.

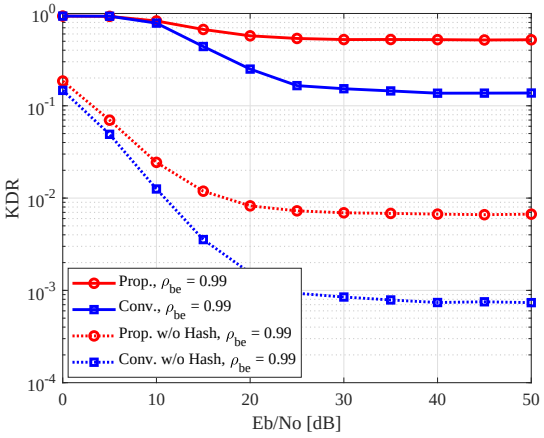


Fig. 8. Comparison of eavesdropper's KDR with and without Hash function.

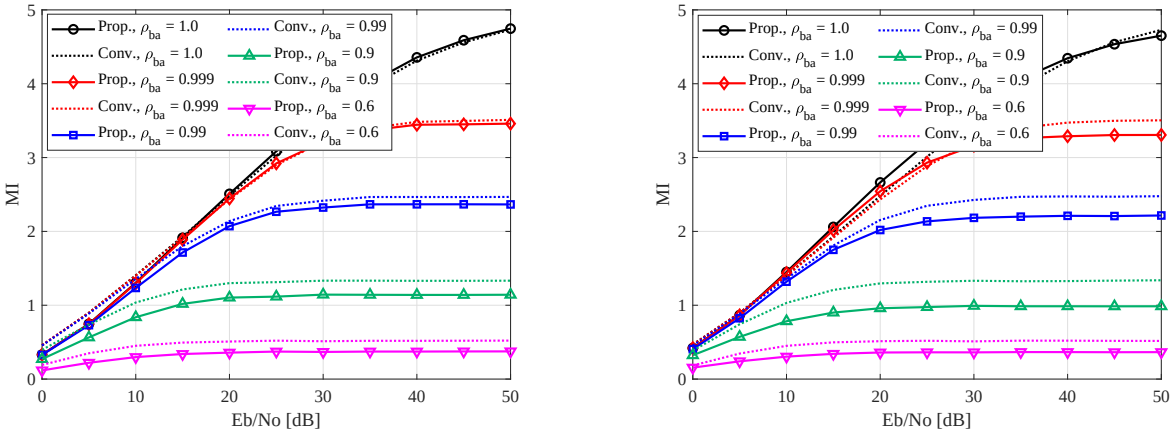
Fig. 6(b) shows the KDRs for $\rho_{ba} = 1.0$ and $\rho_{be} = 0.9$ while other parameters are the same as those in Fig. 6(a). Similar to Fig. 6(a), in the proposed scheme, the KDR of the legitimate users coincides with the conventional scheme without pilot reduction as Eb/No increases, whereas the KDR of the eavesdropper tends to decrease. This confirms that the proposed scheme prevents key information leakage to eavesdroppers while maintaining the key agreement among legitimate users.

Fig. 7 shows the effects of our CSI interpolation on the KDR performance. The correlation between the legitimate users is $\rho_{ba} = 1$, and the presence of the eavesdropper is not considered. While the conventional SKG without the pilot signal reduction exhibits the best KDR performance, a 25% reduction of the pilot signal is achieved in the proposed scheme, and the proposed scheme's KDR is close to that of the conventional SKG. In the case without CSI interpolation, the KDR is as high as 1 in the entire Eb/No regions, which confirms that it is impossible to share a key.

In Fig. 8, the privacy amplification with and without the Hash function in the KDR of the eavesdropper is investigated, where we focus on the KDR of the eavesdropper and assume that the correlation between the legitimate user and the eavesdropper is $\rho_{be} = 0.99$. In the case of conventional SKG without the Hash function, the KDR of the eavesdropper is lower than 10^{-3}, which increases the probability of the key leakage. By contrast, the Hash function makes it possible to degrade the KDR to approximately 10^{-1}. Furthermore, the effectiveness of the proposed scheme can be maintained regardless of the use of the Hash function.

B. Secret Key Capacity

Fig. 9(a) compares the MI performance of the proposed scheme of $P_r = 0.75$ with the various channel correlations. Also, the conventional scheme that does not use the proposed random reduction scheme is employed as a benchmark. In the case where the correlation is 1.0, the proposed scheme has almost the same MI as the conventional one in the region where Eb/No is sufficiently high. This is because the power efficiency improves by reducing the number of pilot



(a) $P_r = 0.75$ (b) $P_r = 0.375$

Fig. 9. MI versus Eb/No in the proposed scheme with the various channel correlations ρ_{ba}. The full-pilot SKG scheme is also plotted as a conventional benchmark.

symbols, and the interpolation can achieve almost perfect reconstruction. On the other hand, it is challenging to select the exact reduction portion in regions where Eb/No is small due to noise effects, and interpolation does not work well, resulting in degradation. When the correlation is less than 1.0, the proposed scheme is degraded in the entire Eb/No region, while the conventional scheme is not. Furthermore, upon decreasing the correlation from 1.0 to 0.9, the difference becomes larger. When the correlation is 0.6, the range of degradation is smaller than that of 0.9. The proposed scheme reduces MI by adding artificial randomness due to the effect of random reduction, but when the correlation becomes lower than a certain level, this effect is weakened.

Fig. 9(b) compares the MI of the proposed scheme of $P_r = 0.375$ with the same parameters as those used in Fig. 9(a). In contrast to Fig. 9(a), the proposed scheme exhibits higher MI with a correlation of 1.0 than the conventional full-pilot scheme in the entire Eb/No region. This shows that reducing the pilot symbols to 37.5% is still almost completely decodable with perfect correlation while benefiting from power efficiency. MI of the proposed scheme deteriorates as the correlation decreases, as shown in Fig. 9(a). The deterioration becomes higher as the reduction rate is reduced.

Fig. 10(a) shows the SKC performance of the proposed scheme of $P_r = 0.75$ with the various correlations between Bob and Eve ρ_{be}. The SKC with $\rho_{be} = 0$ is plotted as an upper bound. Note that since we assume $\rho_{ba} = 1.0$, where the legitimate channels are reciprocal. It can be confirmed that the proposed scheme, which randomly reduces pilot symbols and reconstructs by interpolation, outperforms the conventional benchmark, regardless of ρ_{be}. This is because the proposed scheme improves power efficiency by reducing the pilot symbols (75% in this case) and also by using interpolation to smooth the acquired RSS, thus suppressing noise effects.

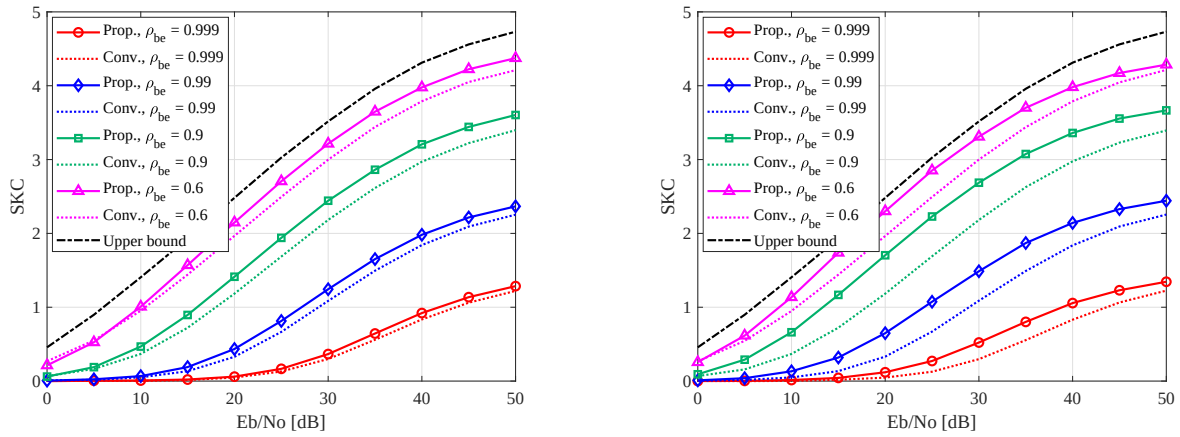
Fig. 10(b) shows the SKC of the proposed scheme with $P_r = 0.375$. Observe in Fig. 10(b) that in each scenario, the proposed scheme outperforms the conventional full-pilot benchmark scheme. More specifically, compared to Fig. 10(a), the improvement in SKC by the proposed scheme is more significant. As expressed in (30), SKC can be represented by the difference between the MI of legitimate users and eavesdroppers. Therefore, in the proposed scheme, legitimate users with a high correlation can maintain high MI, while eavesdroppers with a low correlation degrade MI, resulting in an increase in SKC. [1-4] It can also be observed that in the absence of the eavesdropper, the gain of the proposed scheme diminishes.

Fig. 11(a) shows the SKC of the proposed scheme with various pilot reduction ratios P_r. Here, the correlation values are set as $\rho_{ba} = 1.0$ and $\rho_{be} = 0.6$. The conventional full-pilot SKG is also plotted as a benchmark. In Fig. 11(a), it is found that in each scenario, the SKC performance significantly improves upon decreasing P_r from 1.0 to 0.375. Especially in the Eb/No of 25 dB, the maximum improvement of the proposed scheme is approximately 14%. By contrast, the SKC deteriorates in the case of $P_r = 0.25$ compared to the conventional scheme. The reduction of pilot symbols to more than 25% results in significant degradation, particularly in the high Eb/No region, because it cannot be completely reconstructed by interpolation due to the lack of an exact pilot portion.

Fig. 11(b) shows the SKC with the correlation values as $\rho_{ba} = 1.0$ and $\rho_{be} = 0.9$. In contrast to Fig. 10(b), it can be observed that the gains from the proposed scheme are greater in cases where the eavesdropper correlation is high; the maximum improvement is approximately 33%. Even at $P_r = 0.25$, different from Fig. 11(a), which is significantly degraded, the SKC in Fig. 11(b) is almost equivalent to the conventional benchmark at Eb/No of 50 dB. As shown in Fig. 10(b), comparing the eavesdropper's correlation of 0.9 and 0.6, it is reasonable that the 0.9 case provides a higher gain.

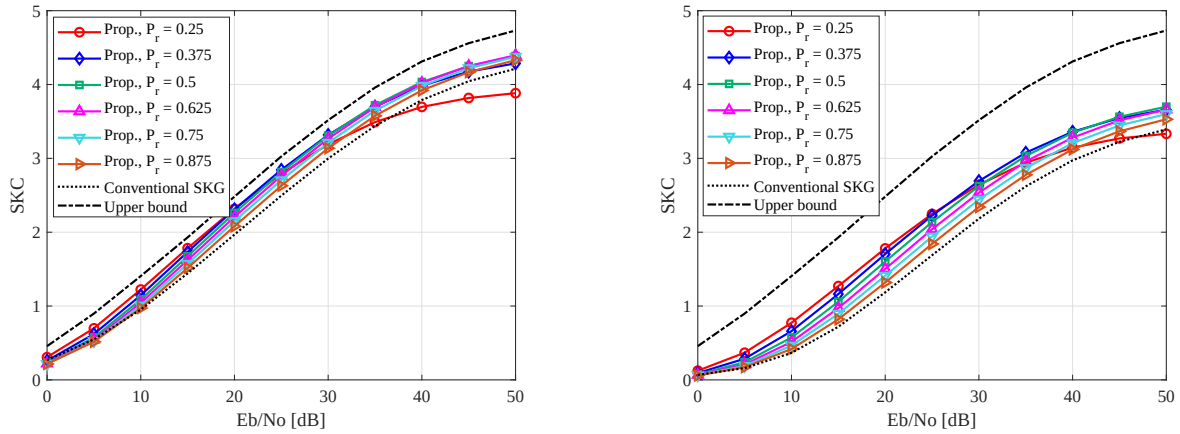
C. Secrecy Outage Probability

To elaborate a little further, we evaluate the achievable SOP performance of the proposed scheme. More specifically, the



(a) $P_r = 0.75$ (b) $P_r = 0.375$

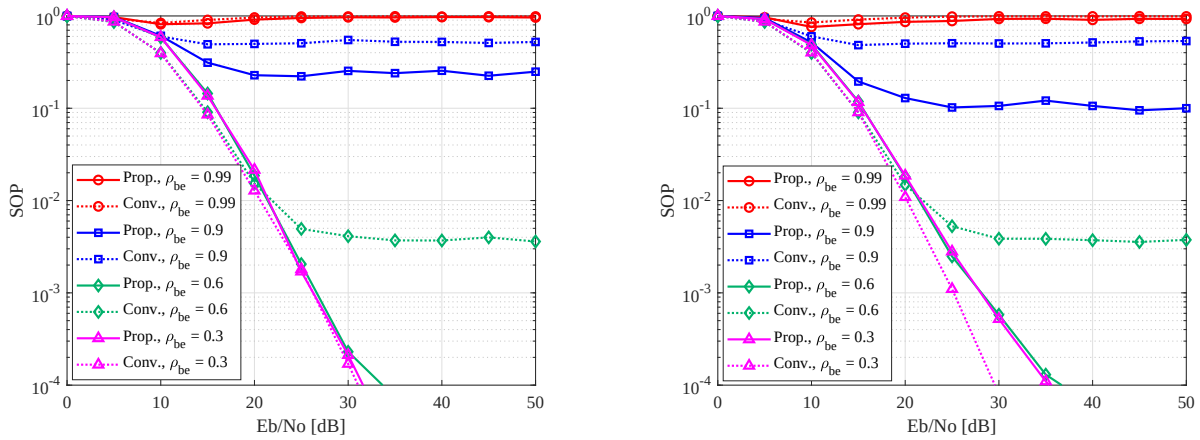
Fig. 10. SKC versus Eb/No in the proposed scheme with the various correlations between Bob and Eve ρ_{be}. The full-pilot SKG scheme is also plotted as a conventional benchmark.



(a) Correlation between the legitimate user and eavesdropper is $\rho_{be} = 0.6$

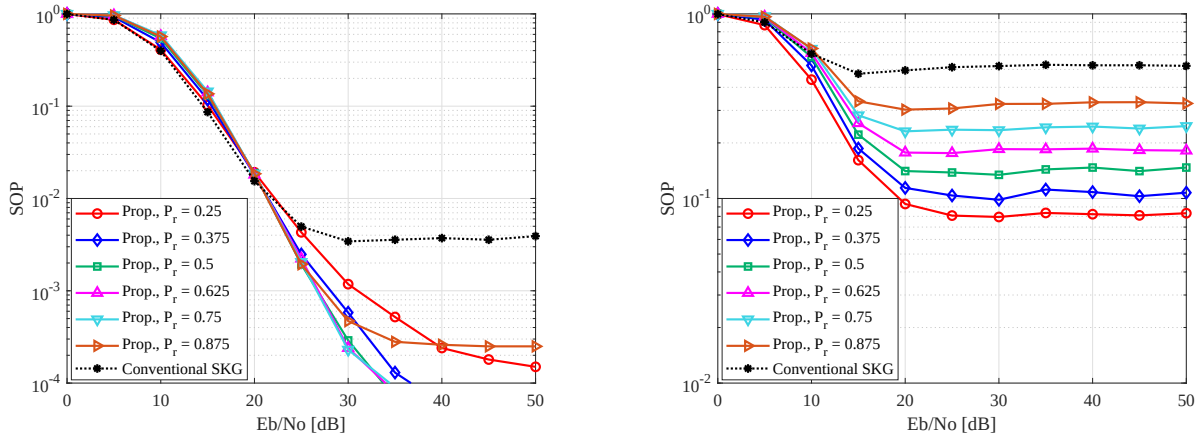
(b) Correlation between the legitimate user and eavesdropper is $\rho_{be} = 0.9$

Fig. 11. SKC versus Eb/No in the proposed scheme with the various reduction ratios P_r. Here, the correlation of legitimate users is $\rho_{ba} = 1.0$. The full-pilot SKG scheme is also plotted as a conventional benchmark.



(a) $P_r = 0.75$ (b) $P_r = 0.375$

Fig. 12. SOP versus Eb/No in the proposed scheme with the various correlations of Eve ρ_{be}. The full-pilot SKG scheme is also plotted as a benchmark.



(a) Correlation between the legitimate user and eavesdropper is $\rho_{be} = 0.6$

(b) Correlation between the legitimate user and eavesdropper is $\rho_{be} = 0.9$

Fig. 13. SOP versus Eb/No in the proposed scheme with the various reduction rates P_r and the correlations are set as $\rho_{ba} = 1.0$ and $\rho_{be} = 0.6$. The full-pilot SKG scheme is also plotted as a benchmark.

SOP P_{out} consists of two factors, the KDR between legitimate users (36) and that of the eavesdropper (37), which can be expressed as

$$P_{out} = P(\{P_k^{ba} \neq 0\} \cup \{P_k^{be} = 0\}). \tag{38}$$

Thus, the SOP is a metric that can evaluate the accuracy of the generated keys being shared in a secret manner.

Fig. 12(a) shows the SOP of the proposed scheme with the various correlations of Eve ρ_{be}. Here, $\rho_{ba} = 1.0$ and $P_r = 0.75$ are employed. In the case of a high correlation of $\rho_{be} = 0.99$ for eavesdroppers, the SOP is almost 1 in all Eb/No regions, confirming that secure key sharing is challenging. On the other hand, when the eavesdropper correlation is less than, i.e., $\rho_{be} < 0.9$, the proposed scheme outperforms the conventional scheme, especially in the high Eb/No region. In this paper, P_k^{ba}, which means successfully sharing the key, becomes dominant in the region where Eb/No is low, and conversely, P_k^{be}, which means breaking the key by the eavesdropper, becomes dominant in the region where Eb/No is high. Hence, when Eb/No is high, the probability of the key being stolen by an eavesdropper is increased, thus triggering an error floor.

Moreover, Fig. 12(b) shows the SOP of the proposed scheme $P_r = 0.375$ with the various correlations while setting $\rho_{ba} = 1.0$ and $P_r = 0.75$. As shown in Fig. 12(b), the trend is the same as in Fig. 12(a), but it is clear that the improvement is superior, especially in a high Eb/No region. This is because the increasing reduction of pilot symbols leads to strongly induced randomness, making eavesdropping difficult. However, as mentioned in the previous section, the effect of inducing randomness on the resistance to eavesdropping is limited, and the improvement is marginal when $\rho_{be} < 0.6$.

Fig. 13(a) shows the SOP with the various P_r and the correlations are set as $\rho_{ba} = 1.0$ and $\rho_{be} = 0.6$. As seen in Fig. 11(a), the SOP improves as the reduction rate decreases to 0.375. On the other hand, when P_r becomes 0.25, the SOP deteriorates in the high Eb/No region. This is because the proposed scheme is reaching the limit of its effectiveness in degrading eavesdropping performance, and the probability of successful eavesdropping by the eavesdroppers becomes high.

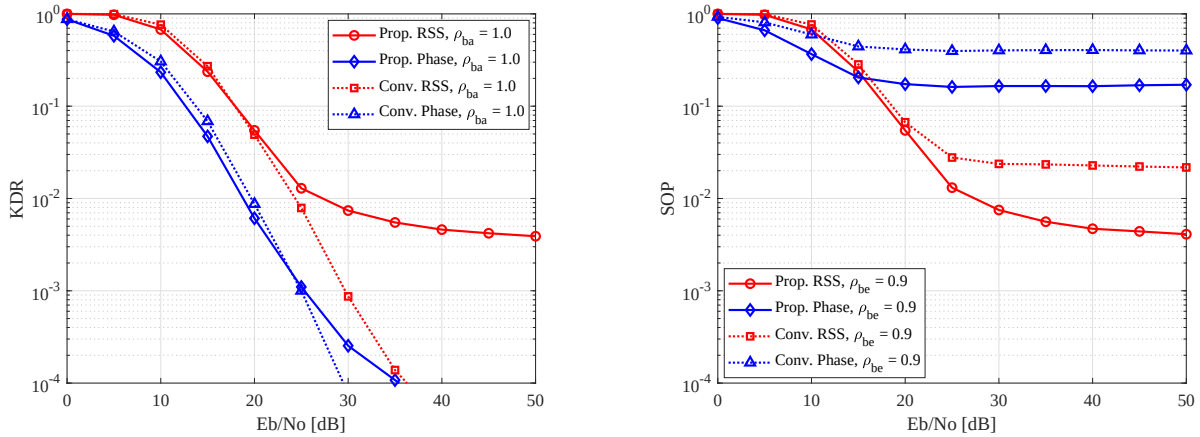
Finally, Fig. 13(b) shows the SOP with the various P_r and the correlations are set as $\rho_{ba} = 1.0$ and $\rho_{be} = 0.9$. In the case of the higher correlation of Eve, the SOP degrades significantly overall compared to Fig. 13(a). Note that SOP does not deteriorate even when P_r is decreased to 0.25. The reason for this, especially in the high Eb/No region, is that the possibility of stealing the key is high due to the high correlation of the eavesdroppers, which exceeds the gain from the proposed scheme.

D. Effect of Quantization

Figs. 14 compares the KDRs between the RSS-based [27] and phase-based [28] quantization methods. Here, the proposed scheme's pilot reduction ratio is set at 0.25. Fig. 14(a) represents the KDR without taking into account the eavesdropper. In both the conventional and proposed schemes, the phase-based quantization exhibits a superior KDR. Note that the proposed scheme suffers from a slightly increased KDR due to the random pilot reduction, and both RSS-based and phase-based quantization methods have error floors.

Fig. 14(b) demonstrates the SOP performance in the presence of the eavesdropper. In contrast to Fig. 14(a), the proposed scheme outperforms the conventional SKG in both RSS- and phase-based methods. This is because the effects of the KDR degradation due to random pilot reduction is more prominent in the eavesdropper than in the legitimate user. Also, the RSS-based method exhibits a superior SOP in the high Eb/No region.

Fig. 15 shows the KDRs of the proposed and conventional schemes using RSS-based quantization with various quantization levels. The KDR degrades upon increasing the quantization level. Additionally, the performance of the proposed scheme is comparable to that of the conventional SKG in the low Eb/No region due to improved power utilization efficiency.



(a) KDR with $\rho_{ba} = 1.0$ (b) SOP with $\rho_{ba} = 1.0$ and $\rho_{be} = 0.9$

Fig. 14. Performance comparison results by RSS-based and phase-based quantization methods. The proposed pilot reduction ratio is set at $P_r = 0.25$.

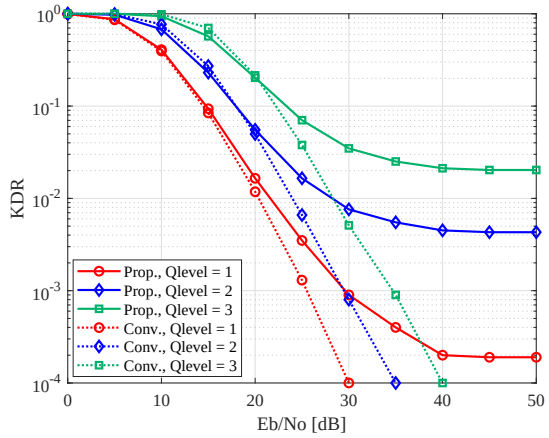


Fig. 15. Comparison result of KDR by quantization level. The full-pilot conventional SKG scheme is also plotted as a benchmark.

TABLE I
NIST TEST RESULTS

Parameters	Conv.	Prop.
Approximate Entropy	0.639	0.9239
Cumulative Sums	0.1250	0.1566
Discrete Fourier Transform	0.8883	0.3993
Frequency Block	0.1367	0.4585
Frequency Monobit	1.0000	1.0000
Runs	0.9593	0.3282
Serial	0.4449, 0.1471	0.7670, 0.4840

However, in the high Eb/No region, it deteriorates due to the discrepancy effect caused by the random pilot reduction.

E. Randomness Test

To evaluate the validity of the generated keys, we performed the NIST randomness test [31]. The randomness tests are composed of 15 tests, and the output of each test is the p-value, which is guaranteed to be random in cases more than 0.01. We use a 1536-bit key with a quantization level of 3 bits to ensure a sufficiently long key length for the test and perform 7 NIST tests at the Eb/No of 20 dB. Table I lists the randomness test results of the conventional and proposed SKG. The conventional one does not reduce the pilot signal, and the proposed one has a reduction ratio of 0.75. Both the conventional and the proposed schemes pass the randomness test, which shows that our scheme can generate keys with randomness comparable to the conventional one.

VI. Conclusions

In this paper, we proposed the novel physical-layer SKG with random pilot activation for enhancing SKC and confidentiality against eavesdroppers. More specifically, our random pilot activation induces artificial randomness and decreases the potential information leakage to the eavesdropper. In our evaluations of MI, SKC, and SOP, we developed a comprehensive SKG process, including information reconciliation and privacy amplification. Our simulation results demonstrated that the proposed SKG scheme exhibits high performance, regardless of the channel correlation between the legitimate and eavesdropper channels and even when the pilot symbols are reduced to as low as 37.5% of the full-pilot sequence.

References

[1] A. Chorti, A. N. Barreto, S. Kopsell, M. Zoli, M. Chafii, P. Sehier, G. Fettweis, and H. V. Poor, "Context-aware security for 6G wireless: The role of physical layer security," *IEEE Communications Standards Magazine*, vol. 6, no. 1, pp. 102–108, 2022.

[2] E. Mahalal, M. Ismail, Z.-Y. Wu, and M. M. Fouda, "Characterization of secret key generation in 5G+ indoor mobile LiFi networks," in *GLOBECOM 2022 - 2022 IEEE Global Communications Conference*, 2022, pp. 01–06.

[3] S. P. Jordan and Y.-K. Liu, "Quantum cryptanalysis: Shor, Grover, and beyond," *IEEE Security & Privacy*, vol. 16, no. 5, pp. 14–21, 2018.

[4] F. Borges, P. R. Reis, and D. Pereira, "A comparison of security and its performance for key agreements in post-quantum cryptography," *IEEE Access*, vol. 8, pp. 142 413–142 422, 2020.

[5] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

[6] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 240–254, 2010.

[7] 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.
[8] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Communications*, vol. 18, no. 4, pp. 6–12, 2011.
[9] M. Adil, S. Wyne, S. J. Nawaz, and B. Muhammad, "Average contiguous duration (ACD)-based quantization for secret key generation in generalized gamma fading channels," *IEEE Access*, vol. 9, pp. 110 435–110 450, 2021.
[10] Z. Xu, G. Y. Li, C. Yang, S. Zhang, Y. Chen, and S. Xu, "Energy-efficient power allocation for pilots in training-based downlink OFDMA systems," *IEEE Transactions on Communications*, vol. 60, no. 10, pp. 3047–3058, 2012.
[11] B. Yang, W. Wang, and Q. Yin, "Secret key generation from multiple cooperative helpers by rate unlimited public communication," in *2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, May 2014, pp. 8183–8187.
[12] U. Altun, S. T. Basaran, G. K. Kurt, and E. Ozdemir, "Scalable secret key generation for wireless sensor networks," *IEEE Systems Journal*, vol. 16, no. 4, pp. 6031–6041, Dec 2022.
[13] Y. Hua, "Generalized channel probing and generalized pre-processing for secret key generation," *IEEE Transactions on Signal Processing*, vol. 71, pp. 1067–1082, 2023.
[14] 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, 2017.
[15] F. Zhan, N. Yao, Z. Gao, and H. Yu, "Efficient key generation leveraging wireless channel reciprocity for MANETs," *Journal of Network and Computer Applications*, vol. 103, pp. 18–28, 2018.
[16] R. Lin, L. Xu, H. Fang, and C. Huang, "Efficient physical layer key generation technique in wireless communications," *EURASIP J. Wirel. Commun. Netw.*, vol. 2020, no. 1, pp. 1–15, 2020.
[17] D. Guo, K. Cao, J. Xiong, D. Ma, and H. Zhao, "A lightweight key generation scheme for the Internet of things," *IEEE Internet of Things Journal*, vol. 8, no. 15, pp. 12 137–12 149, 2021.
[18] M. Yuliana, Suwadi, and W. Wirawan, "Performance evaluation of Savitzky Golay filter method that implement within key generation," in *2021 IEEE 5th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE)*, 2021, pp. 343–348.
[19] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, 2008.
[20] D. Chen, Z. Qin, X. Mao, P. Yang, Z. Qin, and R. Wang, "SmokeGrenade: An efficient key generation protocol with artificial interference," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 11, pp. 1731–1745, 2013.
[21] H. Li, X. Wang, and J.-Y. Chouinard, "Eavesdropping-resilient OFDM system using sorted subcarrier interleaving," *IEEE Transactions on Wireless Communications*, vol. 14, no. 2, pp. 1155–1165, 2015.
[22] G. Li, A. Hu, J. Zhang, and B. Xiao, "Security analysis of a novel artificial randomness approach for fast key generation," in *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, 2017, pp. 1–6.
[23] S. Naderi, D. B. da Costa, and H. Arslan, "Joint random subcarrier selection and channel-based artificial signal design aided PLS," *IEEE Wireless Communications Letters*, vol. 9, no. 7, pp. 976–980, 2020.
[24] 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, 2020.
[25] T. M. Pham, M. Mitev, A. Chorti, and G. P. Fettweis, "Pilot randomization to protect MIMO secret key generation systems against injection attacks," *IEEE Wireless Communications Letters*, vol. 12, no. 7, pp. 1234–1238, 2023.
[26] A. M. Khan, V. Jeoti, and M. A. Zakariya, "Improved pilot-based LS and MMSE channel estimation using DFT for DVB-T OFDM systems," in *2013 IEEE Symposium on Wireless Technology & Applications (ISWTA)*, 2013, pp. 120–124.
[27] 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, pp. 1–6.
[28] 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, 2023.
[29] R. Chaves, G. Kuzmanov, L. Sousa, and S. Vassiliadis, "Improving SHA-2 hardware implementations," in *Cryptographic Hardware and Embedded Systems - CHES 2006*, L. Goubin and M. Matsui, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 298–310.
[30] A. Kraskov, H. Stögbauer, and P. Grassberger, "Estimating mutual information," *Physical review E*, vol. 69, no. 6, p. 066138, 2004.
[31] 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, 2012.

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. In 2019, he was recognized as The University of Tokyo Excellent Young Researcher. 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.

Dr. Sugiura was a recipient of numerous awards, including the 18th JSPS Prize in 2022, the Fifth Yasuharu Suematsu Award in 2019, the Sixth RIEC Award from the Foundation for the Promotion of Electrical Communication in 2016, the Young Scientists' Prize by the Minister of Education, Culture, Sports, Science and Technology of Japan in 2016, the 14th Funai Information Technology Award (First Prize) from the Funai Foundation in 2015, the 28th Telecom System Technology Award from the Telecommunications Advancement Foundation in 2013, the Sixth IEEE Communications Society Asia-Pacific Outstanding Young Researcher Award in 2011, the 13th Ericsson Young Scientist Award in 2011, and the 2008 IEEE Antennas and Propagation Society Japan Chapter Young Engineer Award. He has served as an Editor for IEEE WIRELESS COMMUNICATIONS LETTERS (2019–), as an Associate Editor for IEEE TRANSACTIONS ON COMMUNICATIONS (2023–), and as an Editor for SCIENTIFIC REPORTS (2021–2024). He was certified as 2021 IEEE WIRELESS COMMUNICATIONS LETTERS Exemplary Editor.