Group Secret Key Distribution Based on Physical-Layer Key Generation and NOMA-Assisted Downlink

Shun Kojima and Shinya Sugiura*
Institute of Industrial Science, The University of Tokyo
E-mail: {skojima, sugiura}@iis.u-tokyo.ac.jp

***Abstract*—In this paper, we propose a novel non-orthogonal multiple access (NOMA)-based physical-layer group secret key distribution (GSKD) for a star network in the presence of an eavesdropper. In the proposed scheme, a random group secret key generated at a base station (BS) is distributed to legitimate users in an information-theoretically secure manner. More specifically, the BS and each user share a secret key from the associated channel state information (CSI), which is then used to encrypt the group secret key with a one-time pad. Then, each of the encrypted group secret keys is superimposed and efficiently broadcast to the users in the NOMA downlink. Moreover, we derive the theoretical group key rate bound of the proposed scheme. Our performance results demonstrate that the proposed NOMA-based GSKD scheme outperforms the conventional benchmark schemes.**

I. Introduction

Wireless security is typically achieved in the upper layer based on public key cryptography (PKC), which allows us to share secret keys confidentially among legitimate nodes. PKC is an encryption scheme with computational security rather than information-theoretical security, which may not be unbreakable in polynomial time; however, it is susceptible to decryption by quantum algorithms [1]. Furthermore, the computational complexity of exchanging a sufficiently long quantum-resistant key is intensive and unsuitable. It was demonstrated that Shor's quantum algorithm has the potential to break asymmetric key cryptography in polynomial time [2], while Simon's algorithm may be capable of breaking symmetric key cryptography [3]. Moreover, in [4], secret key encryption by a key exchanged with PKC is susceptible to being broken by a quantum brute force attack employing Grover's algorithm.

To address the above-mentioned confidentiality issue, physical-layer secret key generation (SKG) has been attracting attention [5]. By assuming the channel reciprocity between two legitimate nodes, channel state information (CSI) is exploited as the random source of a secret key without requiring any third party. Under the presence of fading, an eavesdropper located more than half a wavelength away from the legitimate uses may not access the CSI between the legitimate users, thus making it information-theoretically secure [6]. Note that since channel reciprocity is established between each two-node pair, it is challenging to directly carry out the conventional SKG among more than two nodes.

While most previous SKG studies focused their attention on a pairwise SKG scenario between two users, the recent extensions to group secret key distribution (GSKD) among multiple nodes are found in [7–11]. In [7], Liu *et al.* proposed the collaborative SKG for a group of wireless nodes, which relies on the difference of signal strength (DOSS). Also, Xiao *et al.* [8] presented the cooperative GSKD based on secure network coding (SNC) to reduce the associated overhead. Furthermore, Xu *et al.* [9] proposed the GSKD that combines the multi-segmentation and one-time pad with pairwise SKG. In [10], the GSKD that utilizes pairwise keys and leverages non-reconciled received signal strength was investigated, while in [11], the orthogonal frequency-division multiple access (OFDMA)-based GSKD protocol was conceived.

To improve the efficiency of SKG, various non-orthogonal multiple access (NOMA)-based key-sharing schemes have been proposed [12–14]. In [12], Chamkhia *et al.* presented the SKG-based secure NOMA-enabled IoT network. Further, Jacob *et al.* [13] proposed the NOMA-based SKG to ensure resistance against internal eavesdropping. These methods consider only two-user scenarios, making applying them to group key sharing challenging. On the other hand, in [14], the GSKD scheme using NOMA was proposed. However, the information reconciliation, which is essential for group key sharing, has not been performed, and the analysis of key generation efficiency remains insufficient.

Against this background, the novel contribution of this paper is to propose a comprehensive NOMA-based GSKD scheme for star network topology and provide a detailed performance analysis for the first time. The base station (BS) generates a random group secret key, which is distributed to multiple legitimate users. More specifically, our proposed scheme is divided into two phases: an SKG phase for generating a secret

Preprint for publication in *IEEE International Conference on Communications (ICC) Workshop*, Montreal, Canada, 2025, DOI: 10.1109/ICCWorkshops67674.2025.11162189.

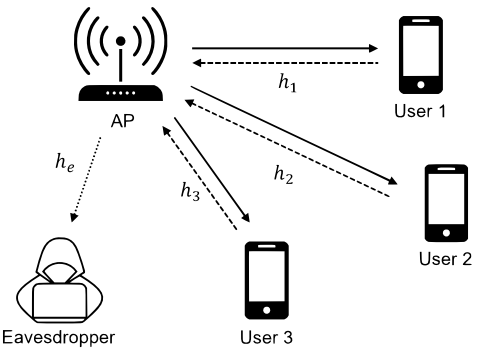

Fig. 1. System model of our GSKD in the presence of an eavesdropper.

key between the BS and each user from the associated CSI and a GSKD phase for distributing a group secret key from the BS to the legitimate users. The group secret key is encrypted by each user's secret key generated in the SKG phase with a one-time pad, and each of the encrypted group secret keys is superimposed and efficiently broadcast to the users in the NOMA downlink. Furthermore, we derive the theoretical group key rate (GKR) bound of the proposed GSKD scheme. We evaluate the achievable performance of the proposed scheme in terms of the group key error rate (GKER), GKR, and NIST randomness tests while showing that the proposed scheme outperforms the conventional GSKD schemes. Also, we investigate the effects of information reconciliation based on Bose-Chaudhuri-Hocquenghem (BCH) codes, as well as channel coding based on polar codes.

II. System Model

This paper considers the GSKD among the BS and a group of N_u legitimate users with the aid of user-specific SKG and NOMA-downlink transmission in the presence of an eavesdropper, as shown in Fig. 1.

A. Channel Model

We consider the time-division duplex (TDD)-based orthogonal frequency-division multiplexing (OFDM) transmission of pilot symbols and group secret key over the multipath fading channels. Also, we assume a star network topology [11] where the N_u legitimate users are distributed around the BS. Here, the u-th user's channel frequency response (CFR) associated with the k-th subcarrier of the n-th OFDM symbol is expressed as

$$H_u^d(n,k) = \frac{1}{\sqrt{K}} \sum_{m=0}^{K-1} h_u^d(n,m) e^{-j2\pi\left(\frac{km}{K} - \frac{v_u n}{P}\right)}, \quad (1)$$

where $d = \{ul, dl\}$ indicates the uplink and downlink, respectively, while K is the number of subcarriers. Also, v is the normalized Doppler shift, which is defined as $v \triangleq f_u^d P T_s$, where P denotes a positive integer with Doppler shift precision to be $1/PT_s$. Also, T_s is the OFDM symbol duration with a sampling interval of t_s, where we have the relationship of $T_s = Kt_s$. Furthermore, f_u^d represents the Doppler shift of each user, which is given by $f_u^d = v_u f_c / c$, where v_u, f_c, and c indicate the moving speed of the u-th user, the center carrier frequency, and the speed of light, respectively. Here, the associated channel impulse response (CIR) is represented as

$$h_u^d(v,\tau) = \sum_{l=0}^{L-1} \beta_l e^{-j2\pi f_u^d \tau} \delta(v - v_l t_s), \quad (2)$$

where L, β_l, and v_l denote the number of paths, the fading coefficient, and the delay of the l-th path, respectively. Note that $\delta(\cdot)$ is the Dirac delta function. For simplicity, we assume that the path delays represent the sampling interval, and hence, the sampled CIR tap is defined by

$$h_u^d(m,n) \triangleq h_u^d(\tau = nT_s, v = mt_s) \quad (3)$$

$$= \begin{cases} \beta_l & m = v_l, \\ 0 & \text{otherwise.} \end{cases} \quad (4)$$

Here, we assume $E\left[|H(n,k)|^2\right] = 1$ for all n and k, where $E[\cdot]$ indicates the expectation operation. Also, we assume a static channel within the coherence time; thus, each pair of uplink and downlink channels has a reciprocal relationship.

B. NOMA-Based Transmission in Downlink

In this paper, NOMA-based transmission is considered in the downlink from the BS to the users, as illustrated in Fig. 1, where each user is located at a different distance from the BS and uses the same bandwidth. Here, d_j is defined as the distance from the BS to the j-th user. Since the channel condition tends to deteriorate upon increasing the distance, we allocate more power to a far user in the NOMA transmission. Then, the BS broadcasts the superimposed signal to N_u users, and each user extracts its information with the aid of successive interference cancellation (SIC). More specifically, the transmitted signal in each time slot $t \in \{1, 2, ..., T\}$ is represented as

$$x(t) = \sum_{j=1}^{N_u} \alpha_j x_j(t), \quad (5)$$

where x_j indicates the signal associated with the j-th user, and $\alpha_j > 0$ is the allocation factor corresponding to the j-th user, which is given by $\alpha_j = \sqrt{p_j P_{BS}}$. Furthermore, $p_j > 0$ indicates the associated power coefficient of the user, and P_{BS} is the average transmission power of the BS. We have the transmitted power constraints of $\sum_{j=1}^{N_u} p_j = 1$ and $\sum_{j=1}^{N_u} \alpha_j^2 = P_{BS}$. The signal received at the j-th user y_j can be expressed by $y_j(t) = \alpha_j \hat{h}_j x_j(t) + \sum_{k=1, k\neq j}^{N_u} \alpha_k \hat{h}_k x_k(t) + n_k(t)$, where $\hat{h}_j = h_j \cdot L_{path}(d_j)$. Here, h_j represents the channel coefficient between the BS and the j-th user and $L_{path}(d_j)$ indicates the path loss function regarding d_j, which is the distance between the BS and the j-th user [15]. Let n_j be the additive white Gaussian noise (AWGN) with zero mean and variance σ_j^2. In the NOMA signal, modulated symbols for the multiple

users are superimposed, and the average received signal-to-interference-plus-noise ratio (SINR) of the j-th user can be expressed as $\gamma_j = p_j|\hat{h}_j|^2/(\sigma_j^2 + \sum_{k=1,k\neq j}^{N_u} p_k|\hat{h}_k|^2)$.

To suppress interference in the superimposed signal, SIC is carried out. Without loss of generality, we consider that the absolute values of the N_u users' channels are ordered as follows:

$$|\hat{h}_1| \geq |\hat{h}_2| \geq \cdots \geq |\hat{h}_{N_u}|. \tag{6}$$

By assuming that SIC can be carried out correctly, the average SINR of the j-th user with SIC can be upper-bounded by $\tilde{\gamma}_j = p_j|\hat{h}_j|^2/(\sigma_j^2 + \sum_{k=1}^{j-1} p_k|\hat{h}_k|^2)$.

III. Proposed NOMA-Based GSKD Algorithm

In this section, we describe the proposed NOMA-based GSKD scheme. In the SKG phase, all the users first transmit a pilot symbol to the BS in different time slots, and then, the BS estimates the CSI of each user. The BS quantizes the estimated CSI of each user to generate a secret key and to perform information reconciliation [6], the BS sends syndromes to each user. Subsequently, in the GSKD phase, the BS randomly generates a group secret key, encrypts it with the secret key of each user, and modulates the encrypted group secret key to information symbols. The modulated symbols are superimposed on a NOMA signal. Finally, the BS broadcasts the signal to the users.

At each user, in the SKG phase, similar to the BS, CSI estimation and quantization are first performed based on the pilot symbol sent from the BS to generate a secret key. Then, information reconciliation is carried out to remove the potential error imposed on the secret key. In the GSKD phase, the encrypted group key is extracted from the received superimposed signal through SIC, and the group key is obtained by decrypting it with the secret key generated in the SKG phase.

A. SKG Phase at BS: Channel Probing and Information Reconciliation

First, the j-th user transmits a pilot symbol to the BS, and the signal received at the BS in the t-th time slot is expressed as

$$Y_j^{BS}(t) = H_j^{BS}(t)X_j^P(t) + N^{BS}(t), \tag{7}$$

where $H_j^{BS}(t)$, $X_j^P(t)$, and $N^{BS}(t)$ indicate the CFR between the BS and the j-th user, the predefined pilot signal transmitted from the j-th user, and the associated AWGN component at the BS. From (7), the BS estimates CSI between the BS and the j-th user as follows:

$$\bar{H}_j^{BS}(t) = Y_j^{BS}(t)/X_j^P(t), \tag{8}$$

Subsequently, the BS retrieves phase information ϕ_j from CSI $\bar{H}_j^{BS}(t)$, quantizes it, and acquires the secret key as follows:

$$k_j(t) = \begin{cases} 1 & \text{if } \phi_j(t) > 0, \\ 0 & \text{if } \phi_j(t) \leq 0. \end{cases} \tag{9}$$

Let us define the secret key associated with the j-th user as $\mathbf{k}_j = [k_j(1), k_j(2), \cdots, k_j(T)]^T$. Then, the information reconciliation is carried out with the BCH codes to calculate the encoded secret key of $\mathbf{c}_j = \begin{bmatrix} \mathbf{k}_j^T & \mathscr{S}_j^T \end{bmatrix}^T$, where $\mathscr{S}_j$ indicates the syndrome vector of $\mathbf{k}_j$. The syndrome is transmitted to each user through a public channel and used for information reconciliation.

B. GSKD Phase at BS: One-Time Pad Encryption, Channel Coding, and Superimposition

As mentioned above, the BS generates an independent random group secret key, which is given by

$$\mathbf{k}^g = [k^g(1), k^g(2), \cdots, k^g(T)]^T, \tag{10}$$

where $k^g(t) \in \{0, 1\}$. To achieve information-theoretic security in the GSKD phase, the BS encrypts the group secret key $\mathbf{k}^g$ using the secret key $\mathbf{k}_j$ generated from CSI as

$$\mathbf{s}_j^g = \mathbf{k}^g \oplus \mathbf{k}_j, \tag{11}$$

which corresponds to the one-time pad encryption. Here, $\oplus$ denotes the exclusive OR (XOR) operation.

Further to information reconciliation imposed on the secret key generated from CSI, polar coding is used for the FEC of the group secret key. The symbols, which are encoded by polar coding and phase-shift keying (PSK)-modulated onto the encrypted group secret key associated with the j-th user, are represented as

$$\tilde{\mathbf{x}}_j^g = \left[\tilde{x}_j^g(1), \tilde{x}_j^g(2), \cdots, \tilde{x}_j^g(T)\right]^T = \mathscr{E}(\mathbf{s}_j^g). \tag{12}$$

Here, $\mathscr{E}$ denotes the function of polar encoding and PSK modulation.

Using power-domain NOMA as specified in (5), a multiplexed transmit signal can be represented as

$$X^U(t) = \sum_{j=1}^{N_u} \alpha_j \tilde{x}_j^g(t), \tag{13}$$

which is broadcast to all the users together with a predefined pilot signal $X^P(t)$, which is denoted by

$$\hat{X}^U(t) = \left[X^P(t)\ X^U(t)\right]^T. \tag{14}$$

C. SKG and GSKD Phases at Users

Upon the broadcast of the signal (14) from the BS, the signal received at the j-th user can be represented as $Y_j^U(t) = H_j^U(t)\hat{X}^U(t) + N_j^U(t)$, where $H_j^U(t)$ and $N_j^U(t)$ denote the CFR between the j-th user and the BS and the AWGN component at the j-th user, respectively. Similarly to the SKG phase at the BS in (8), the j-th user first estimates CSI between the BS and the j-th user as follows: $\bar{H}_j^U(t) = H_j^U(t)X^P(t) + N_j^U(t)/X^P(t)$, while assuming the channel reciprocity. Then, the CIR is quantized in the same manner as (refquantization) to obtain the user-specific secret key as

follows:

$$\hat{\mathbf{k}}_j = \left[\hat{k}_j(1), \hat{k}_j(2), \cdots, \hat{k}_j(T)\right]^T. \tag{15}$$

Each user utilizes the syndrome $\hat{\mathscr{S}}_j$ received from the BS to the BCH-encoded secret key in information reconciliation as follows: $\mathbf{c}'_j = \left[\hat{\mathbf{k}}_j^T \ \hat{\mathscr{S}}_j^T\right]^T$, where $\hat{\mathbf{k}}'_j = \mathscr{B}(\mathbf{c}'_j) = \left[\hat{k}'_j(1), \hat{k}'_j(2), \cdots, \hat{k}'_j(T)\right]^T$. Here, $\mathscr{B}$ indicates the function of BCH decoding. After the j-th user receives the superimposed signal $X_U(t)$, SIC and PSK-demodulation are carried out to calculate the symbols $\bar{\mathbf{x}}_j^g$, which correspond to the transmitted PSK symbols $\tilde{\mathbf{x}}_j^g$, as follows: $\hat{\mathbf{s}}_j^g = \mathscr{D}(\bar{\mathbf{x}}_j^g)$, where $\mathscr{D}$ represents the function of PSK demodulation and polar decoding. Finally, to decrypt the group secret key, each user performs the XOR operation as

$$\hat{\mathbf{k}}_j^g = \hat{\mathbf{s}}_j^g \oplus \hat{\mathbf{k}}'_j. \tag{16}$$

IV. Achievable Group Key Rate

In this section, we derive the achievable GKR, which takes into account the impact of superimposed signal and SIC. In the proposed algorithm, each user obtains the user-specific secret key and group secret key according to (15) and (16), while the eavesdropper tries to calculate both of them. More specifically, the eavesdropper attempts to eavesdrop on the CSI between the BS and each user by estimating the CSI between the BS and the eavesdropper, which is given by

$$\mathbf{h}^e = \left[H^e(1), H^e(2), \cdots, H^e(T)\right]^T. \tag{17}$$

Additionally, the eavesdropper estimates the group secret key of each user from the signal received from the BS in the GSKD phase, which is represented by $\mathbf{G}^e \triangleq \left[\mathbf{g}_1^e, \mathbf{g}_2^e, \cdots, \mathbf{g}_{N_u}^e\right]$, where $\mathbf{g}_j^e$ corresponds to $\hat{\mathbf{k}}_j^g$. Based on the results of [7, 8], the GKR is formulated by

$$R_g = \min_{1\le j\le N_u} \lim_{T\to\infty} \frac{1}{TN} I\left(\mathbf{k}^g; \hat{\mathbf{k}}_j^g \mid \mathbf{h}^e, \mathbf{G}^e\right), \tag{18}$$

where $1/N$ is the normalization factor for time symbols and frequency utilization efficiency, and $I(X;Y|Z)$ indicates the conditional mutual information. In contrast to [7, 8], the proposed algorithm includes the effects of SIC, making it impossible to assume that the group secret key of each user is independently identically distributed. Considering that power allocation factors are calculated according to each user's CSI, (18) is rewritten by

$$R_g = \lim_{T\to\infty} \frac{1}{TN} I\left(\mathbf{k}^g; \hat{\mathbf{k}}_{N_u}^g \mid \mathbf{h}^e, \mathbf{G}^e\right). \tag{19}$$

Using the relationship of $I(X;Y|Z) = I(X;Y,Z) - I(X;Z)$, the part (19) is modified to

$$I\left(\mathbf{k}^g; \hat{\mathbf{k}}_{N_u}^g \mid \mathbf{h}^e, \mathbf{G}^e\right) = I\left(\mathbf{k}^g; \hat{\mathbf{k}}_{N_u}^g, \mathbf{h}^e, \mathbf{G}^e\right) - I\left(\mathbf{k}^g; \mathbf{h}^e, \mathbf{G}^e\right).$$

For simplicity, assuming that the eavesdropper is located apart beyond the coherence distance from any legitimate user and that the channel between the BS and the eavesdropper is uncorrelated to the channels between the BS and the legitimate users, the mutual information has the following relationships:

$$I\left(\mathbf{k}^g; \hat{\mathbf{k}}_{N_u}^g, \mathbf{h}^e, \mathbf{G}^e\right) = I\left(\mathbf{k}^g; \hat{\mathbf{k}}_{N_u}^g, \mathbf{G}^e\right), \tag{20}$$

$$I\left(\mathbf{k}^g; \mathbf{h}^e, \mathbf{G}^e\right) = I\left(\mathbf{k}^g; \mathbf{G}^e\right). \tag{21}$$

Hence, (19) is further simplified to

$$\begin{aligned} R_g &= \lim_{T\to\infty} \frac{1}{TN} \left[I\left(\mathbf{k}^g; \hat{\mathbf{k}}_{N_u}^g, \mathbf{G}^e\right) - I\left(\mathbf{k}^g; \mathbf{G}^e\right)\right] \\ &= \lim_{T\to\infty} \frac{1}{TN} I\left(\mathbf{k}^g; \hat{\mathbf{k}}_{N_u}^g \mid \mathbf{g}_{N_u}^e\right). \end{aligned} \tag{22}$$

Note that the relationship among $\mathbf{k}^g$, $\hat{\mathbf{k}}_{N_u}^g$, and $\mathbf{g}_{N_u}^e$ are given by $\hat{\mathbf{k}}_{N_u}^g = \mathbf{g}_{N_u}^e \oplus \hat{\mathbf{k}}_{N_u}$ and $\mathbf{g}_{N_u}^e = \mathbf{k}^g \oplus \mathbf{k}_{N_u}$. Given that $\mathbf{k}^g$ and $\mathbf{k}_{N_u}$ are identically distributed Gaussian random variables, we have

$$I\left(\mathbf{k}^g; \mathbf{g}_{N_u}^e\right) = I\left(\mathbf{k}^g; \mathbf{g}_{N_u}^e \mid \hat{\mathbf{k}}_{N_u}^g\right) = 0. \tag{23}$$

Considering the chain rule for mutual information, we can utilize the relationship of $I(X;Y|Z) = I(X;Y) - (I(X;Z) - I(X;Z|Y))$. Then, by substituting (23) into (22), we arrive at

$$I\left(\mathbf{k}^g; \hat{\mathbf{k}}_{N_u}^g \mid \mathbf{g}_{N_u}^e\right) = I\left(\mathbf{k}^g; \hat{\mathbf{k}}_{N_u}^g\right). \tag{24}$$

Finally, we can obtain the achievable GKR bound as

$$R_g = \lim_{T\to\infty} \frac{1}{TN} I\left(\mathbf{k}^g; \hat{\mathbf{k}}_{N_u}^g\right). \tag{25}$$

TABLE I
System Parameters

Bandwidth	20 MHz
Number of symbols	2
FFT size	$T = 128$
Number of users	$N_u = 3$
Sampling rate	20 MHz
Noise power density	-152 dBm
Path loss exponent	3.5
Number of paths	$L = 15$
Maximum Doppler shift	$f_d = 10$ Hz
Distance between BS and users	1000 m, 500 m, 250 m
Distance between BS and eavesdropper	250 m
FEC of information reconciliation	BCH code
FEC of group secret key	Polar code

V. Performance Results

In this section, we provide our performance results to characterize the proposed NOMA-based GSKD scheme. For simplicity, we consider that each of the BS, the $N_u = 3$ users, and the eavesdropper is equipped with a single antenna. The detailed system parameters employed in our simulations are listed in Table I. The BCH codes, having the codeword length of 31 and the message length of 16, are employed for information reconciliation of each user's secret key in the SKG phase. Also, polar codes with a coding rate of 1/2 are used for FEC

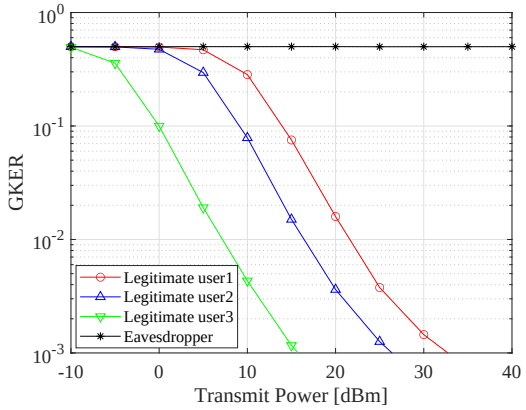

Fig. 2. Comparison of the GKER with each legitimate user and the eavesdropper.

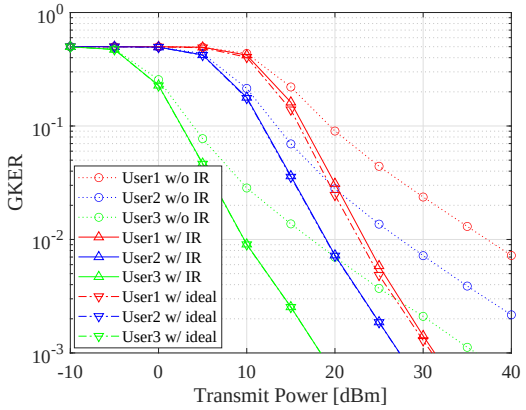

Fig. 3. Comparison of the GKER performance under various patterns of each user's key.

in the GSKD phase. The eavesdropper has access to all the system parameters and is located near the user closest to the BS. We considered the fixed power allocation scheme in the NOMA transmission [16], where a higher power is assigned to a user with a poorer channel condition (farther user). Under the assumption of the channel conditions of (6), we consider the power allocation of $(\alpha_1, \alpha_2, \alpha_3) = (0.7, 0.2, 0.1)$. To verify the effectiveness of the proposed algorithm, we carry out the Monte Carlo simulations, repeating each simulation 100,000 times. To compute the mutual information, we utilized the calculation approach provided in [17].

To investigate the accuracy of the decoded group secret key at each user, we evaluate the GKER, which is defined as $\sum_{i=1}^{T} |k^g(i) - \hat{k}_j^g(i)|/T$. Fig. 2 shows the GKERs at each of the legitimate users and the eavesdropper. The GKER of user 1 shows the worst performance among the users, and a higher performance is observed for users 2 and 3. However, the results of Fig. 2 reflect the impact of NOMA-based transmission, SIC, and polar codes. As expected, the eavesdropper fails to steal the group secret key, exhibiting the GKER as high as 0.5 in the entire transmit power regime.

Fig. 3 illustrates the GKER performance at each user for three different information reconciliation scenarios, i.e., no information reconciliation, BCH-based information reconciliation, and the ideal perfect information reconciliation. The GKER for the scenario without information reconciliation is found to deteriorate. Furthermore, the GKERs for the scenarios of BCH-based and ideal information reconciliation are nearly identical. This implies that the BCH-based information reconciliation is sufficiently powerful for our GSKD scheme.

Next, we evaluate the proposed scheme in terms of the achievable GKR of (25), where we consider the three GSKD benchmarks using DOSS [7], SNC [8], and OFDMA [11]. In the OFDMA benchmark, the same number of subcarriers is allocated to each user, while the power allocation of each subcarrier is deactivated.

Fig. 4 compares the achievable GKRs of the proposed

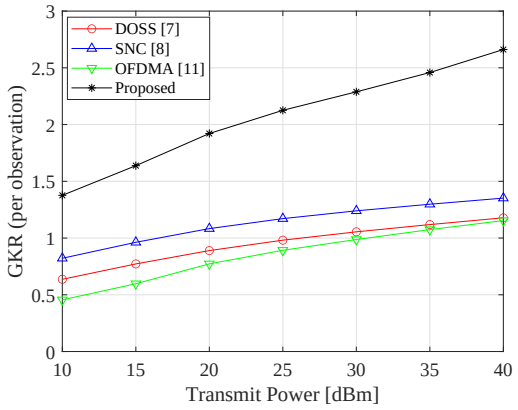

Fig. 4. Comparison of achievable GKR with conventional GSKD methods.

scheme and the three benchmarks. Owing to the benefits of a high efficiency associated with the superimposed signal, the proposed scheme outperforms the benchmark schemes. Note that since the OFDMA benchmark of [11] does not rely on subcarrier-wise power allocation, its achievable performance is limited. Furthermore, the benchmarks of [7] and [8] require a higher overhead between the BS and each user, resulting in performance degradation.

Fig. 5 shows the achievable GKRs while varying the number of users from $N_u = 2$ to 5 in the proposed scheme and the three benchmarks. Here, the transmit power is given by 25 dBm and 35 dBm. Similar to Fig. 4, it is observed that the proposed scheme exhibits the best performance regardless of the number of users, while the proposed scheme's performance advantage is higher in the lower number of users.

A. *Randomness Test*

Finally, to evaluate the randomness of the group secret key shared among the legitimate users. We perform the NIST randomness tests [18]. More specifically, the randomness tests consist of 15 tests, where a p-value is generated for each

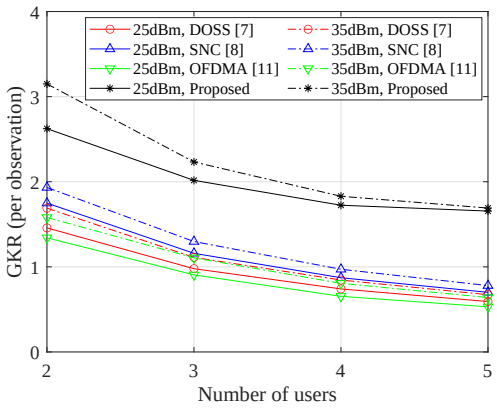

Fig. 5. Achievable GKR versus the number of users with transmit power of 30 dBm.

TABLE II
NIST TEST RESULTS

Parameters	DOSS [7]	SNC [8]	OFDMA [11]	Proposed
Freq. Mono.	0.0801	–	0.9005	0.2606
Freq. Block	0.0468	0.0102	0.0341	0.0842
Long. Runs	–	0.0320	0.9450	0.9290
Runs	–	–	–	0.4399
Serial	0.0312	–	0.2750	0.1555
DFT	0.4220	0.9354	0.1359	0.3588
Cum. Sums	0.1054	–	0.1830	0.2672
Approx. Ent.	0.0394	0.0027	0.2471	0.4862

test. The generated key is considered random if the p-value is greater than 0.01. Table II lists the results for four GSKD schemes. Here, we use the 256-bit group secret key with the quantization level of 1 bit at the transmit power of 25 dBm. As shown in Table II, the proposed scheme successfully passes all the tests, while each of the three benchmark schemes fails the part of the tests.

VI. Conclusions

In this paper, we proposed the NOMA-based GSKD algorithm applicable to a star network in the presence of an eavesdropper. The BS encrypted a group secret key with a secret key generated from the CSI of each user, and the encrypted group secret keys are modulated and superimposed for transmitting NOMA signals to legitimate users. Furthermore, we exploit the BCH codes for the information reconciliation and the polar codes for the FEC of GSKD to improve reliability. We derived the theoretical GKR bound of the proposed NOMA-based GSKD scheme. Our simulation results demonstrated the proposed scheme outperforms the conventional GSKD benchmarks.

Acknowledgement

This work was supported in part by National Institute of Information and Communications Technology (NICT), Japan (Grant JPJ12368C00801), in part by the Japan Science and Technology Agency (JST) FOREST (Grant JPMJFR2127), in part by JST ASPIRE (Grant JPMJBS2345), and in part by the Japan Society for the Promotion of Science (JSPS) KAKENHI (Grant 23K22752).

References

[1] Z. Ji, Y. Zhang, Z. He, P. L. Yeoh, B. Li, H. Yin, Y. Li, and B. Vucetic, "Wireless secret key generation for distributed antenna systems: A joint space-time-frequency perspective," *IEEE Internet Things J.*, vol. 9, no. 1, pp. 633–647, 2022.

[2] 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.

[3] M. Kaplan, G. Leurent, A. Leverrier, and M. Naya-Plasencia, "Breaking symmetric cryptosystems using quantum period finding," in *Advances in Cryptology*. Springer Berlin Heidelberg, 2016, pp. 207–237.

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

[5] S. Kojima and S. Sugiura, "Random pilot activation and interpolated channel estimation for physical-layer secret key generation in correlated eavesdropping channel," *IEEE Trans. Veh. Technol.*, vol. 73, no. 9, pp. 12 978–12 990, 2024.

[6] ——, "User-independent randomized pilot activation for secure key generation," *IEEE Trans. Wireless Commun.*, vol. 23, no. 9, pp. 11 624–11 635, 2024.

[7] 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 Trans. Mobile Comput.*, vol. 13, no. 12, pp. 2820–2835, 2014.

[8] S. Xiao, Y. Guo, K. Huang, and L. Jin, "Cooperative group secret key generation based on secure network coding," *IEEE Commun. Lett.*, vol. 22, no. 7, pp. 1466–1469, 2018.

[9] P. Xu, K. Cumanan, Z. Ding, X. Dai, and K. K. Leung, "Group secret key generation in wireless networks: Algorithms and rate optimization," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 8, pp. 1831–1846, 2016.

[10] G. Li, L. Hu, and A. Hu, "Lightweight group secret key generation leveraging non-reconciled received signal strength in mobile wireless networks," in *IEEE International Conference on Communications Workshops*, 2019, pp. 1–6.

[11] J. Zhang, M. Ding, D. López-Pérez, A. Marshall, and L. Hanzo, "Design of an efficient OFDMA-based multi-user key generation protocol," *IEEE Trans. Veh. Technol.*, vol. 68, no. 9, pp. 8842–8852, 2019.

[12] H. Chamkhia, A. Al-Ali, A. Mohamed, M. Guizani, A. Erbad, and A. Refaey, "Performance analysis of pls key generation-based secure noma-enabled iot networks in the presence of untrusted users," in *2021 IEEE 7th World Forum on Internet of Things (WF-IoT)*, 2021, pp. 633–638.

[13] L. M. Jacob, P. Sreelakshmi, and P. Deepthi, "Physical layer security in power domain noma through key extraction," in *2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, 2021, pp. 1–7.

[14] T. Alshamaseen, S. Althunibat, M. Qaraqe, and H. Alashaary, "Phase-assisted noma based key distribution for iot networks," *Trans. Emerg. Telecommun. Technol.*, vol. 34, no. 4, p. e4738, 2023.

[15] J. Shi, W. Yu, Q. Ni, W. Liang, Z. Li, and P. Xiao, "Energy efficient resource allocation in hybrid non-orthogonal multiple access systems," *IEEE Trans. Commun.*, vol. 67, no. 5, pp. 3496–3511, 2019.

[16] A. Benjebbovu, A. Li, Y. Saito, Y. Kishiyama, A. Harada, and T. Nakamura, "System-level performance of downlink NOMA for future lte enhancements," in *2013 IEEE Globecom Workshops*, 2013, pp. 66–70.

[17] H. Peng, F. Long, and C. Ding, "Feature selection based on mutual information criteria of max-dependency, max-relevance, and min-redundancy," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 27, no. 8, pp. 1226–1238, 2005.

[18] 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 Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 491–505, 2012.