

Physical Layer Secret Key Generation for FDD-OTFS Systems

Aoba Morimoto* and Shun Kojima

Graduate School of Engineering, Chiba University, Chiba, Japan

Email: 25wm4311@student.gs.chiba-u.jp*

Abstract—This paper proposes a physical-layer secret key generation (SKG) scheme for frequency-division duplex orthogonal time frequency space (FDD-OTFS) systems. Conventional SKG relies on channel reciprocity, which cannot be directly exploited in FDD systems because uplink and downlink responses are observed at different carrier frequencies. To address this limitation, we introduce a bidirectional channel-probing protocol for multiple-input multiple-output FDD-OTFS, in which legitimate terminals exchange training signals precoded with locally generated random unitary matrices. By leveraging the delay-Doppler representation, the proposed protocol extracts highly correlated channel coefficients for raw key generation while reducing the correlation between the eavesdropper's observations and legitimate channel features. Simulation results show that the proposed scheme achieves a lower bit-disagreement ratio than FDD-OFDM and direct FDD-OTFS quantization baselines, maintains robustness under different mobility conditions, and improves the mutual-information-based secret-key capacity.

Index Terms—Frequency division duplex, OTFS, physical-layer security, secret key generation.

I. INTRODUCTION

Recent advances in IoT networks have increased the demand for secure wireless communications [1]. Conventional wireless security relies on symmetric-key and public-key cryptography [2]. However, key distribution and cryptographic computations impose considerable overhead [3]. Moreover, since these cryptographic mechanisms generally rely on computational hardness assumptions, their long-term security may be threatened by advances in quantum algorithms [4]. To address these issues, physical-layer secret key generation (SKG) has attracted significant attention as a lightweight and secure technique for secret key establishment [5]. SKG exploits the randomness of wireless channels to generate shared secret keys between Alice and Bob. Since it can be implemented with low computational complexity and does not require key distribution by a trusted third party, SKG is a promising solution for resource-constrained devices and latency-sensitive wireless applications [6]–[8].

Most existing SKG schemes rely on channel reciprocity between legitimate users, Alice and Bob [5], [9], [10]. In time division duplex (TDD) systems, the uplink and downlink share the same frequency band. Therefore, Alice and Bob can obtain highly correlated channel observations within the coherence time. However, the reciprocity does not hold in frequency division duplex (FDD) systems, where the uplink and downlink use different carrier frequencies [11], [12]. To enable SKG in

FDD systems, prior studies have exploited multi-antenna non-reciprocal channels [10], [13]. Qin *et al.* [10] propose pilot-assisted secret key generation, which constructs key-generation features by applying random matrices to non-reciprocal FDD channel coefficients. Matsuzaki *et al.* [13] propose a deep learning-based SKG scheme for the FDD system to realize lightweight and reliable security.

Meanwhile, orthogonal time frequency space (OTFS) modulation has attracted considerable attention for next-generation mobile communication systems, particularly in high-mobility scenarios. OTFS maps information symbols onto the delay-Doppler (DD) domain and represents time-varying multipath channels in terms of delay and Doppler components [14]. Owing to this DD-domain representation, OTFS can provide stable channel characteristics even under severe Doppler conditions. Consequently, OTFS-based SKG, which exploits DD-domain channel estimates for key generation, has emerged as a promising secure solution for high-mobility wireless environments [15], [16]. Saeed *et al.* [15] propose spike-location and entropy-coding methods that generate keys from OTFS DD-domain channel estimates for TDD-OTFS systems. Kawoya *et al.* [16] introduce an efficient SKG scheme that utilizes OTFS channel state information for secure vehicular communication. However, these existing OTFS-based SKG schemes cannot be directly applied to FDD-OTFS links, which are attractive for continuous and low-latency key establishment owing to separate uplink and downlink frequency bands.

To bridge these gaps, this paper proposes a pilot-assisted SKG scheme for FDD-OTFS systems. In the proposed scheme, Alice and Bob perform bidirectional channel probing by exchanging training signals weighted by locally generated random unitary matrices and construct key-generation features from DD-domain multiple-input multiple-output (MIMO) channel responses. The bidirectional channel probing enables the legitimate terminals to construct highly correlated features, and the random unitary matrices suppress reconstruction of the randomly rotated coefficients by the eavesdropper. Simulation results demonstrate that the proposed scheme achieves a lower bit-disagreement rate (BDR) and higher secret key capacity (SKC) than the conventional FDD-OFDM and a direct FDD-OTFS quantization baseline under different mobility conditions.

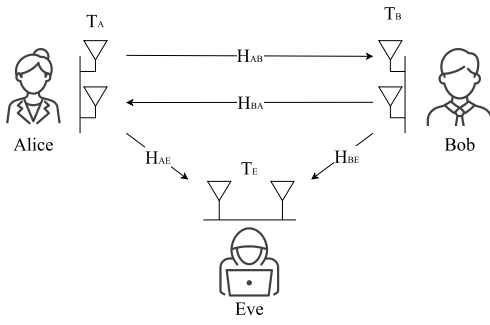


Fig. 1: FDD-OTFS MIMO channel model in the presence of an eavesdropper.

II. SYSTEM MODEL

A. FDD-OTFS Channel Model

We consider a MIMO transmission system in the presence of an eavesdropper, Eve, as shown in Fig. 1. Alice, Bob, and Eve are equipped with T_A , T_B , and T_E antennas, respectively. In FDD systems, the Alice–Bob and Bob–Alice links operate at carrier frequencies f_{AB} and f_{BA} , respectively. When the two carrier frequencies are placed symmetrically around the center frequency f_c with an FDD spacing of Δf_{FDD} , f_{AB} and f_{BA} can be written as

$$f_{AB} = f_c + \frac{\Delta f_{FDD}}{2}, \quad f_{BA} = f_c - \frac{\Delta f_{FDD}}{2}. \quad (1)$$

For the p -th path, the spatial response matrix of each link is defined as

$$\mathbf{A}_p^{XY} = \mathbf{a}_r^{XY}(\theta_{r,p}^{XY}) [\mathbf{a}_t^{XY}(\theta_{t,p}^{XY})]^H. \quad (2)$$

Here, $XY \in \{AB, BA\}$ denotes a legitimate link, where X and Y represent the transmitter and receiver, respectively. Also, $\mathbf{a}_r^{XY}(\cdot)$ and $\mathbf{a}_t^{XY}(\cdot)$ are the receive and transmit array response vectors of link XY , respectively, and $\theta_{r,p}^{XY}$ and $\theta_{t,p}^{XY}$ denote the angle of arrival and angle of departure of the p -th path, respectively.

An OTFS frame is represented on an $M \times N$ DD grid [14]. Let $\mathbf{X}_{DD}$ and $\mathbf{Y}_{DD}$ denote the transmitted and received DD-domain symbol matrices, respectively. The ISFFT and SFFT operations are expressed as

$$\mathbf{X}_{TF} = \mathbf{F}_M \mathbf{X}_{DD} \mathbf{F}_N^H, \quad \mathbf{Y}_{DD} = \mathbf{F}_M^H \mathbf{Y}_{TF} \mathbf{F}_N, \quad (3)$$

where $\mathbf{F}_M$ and $\mathbf{F}_N$ are unitary DFT matrices.

Let Δf_{sc} denote the subcarrier spacing, and define the OTFS symbol duration as $T_{sym} = 1/\Delta f_{sc}$. Defining the baseband frequency of the m -th subcarrier as $f_m = (m - M/2)\Delta f_{sc}$ and the time instant of the n -th OTFS symbol as $t_n = nT_{sym}$, the TF-domain MIMO channel response of link XY is expressed as

$$\mathbf{H}_{XY}^{TF}[m, n] = \sum_{p=1}^P \alpha_p^{XY}[m, n] \mathbf{A}_p^{XY}. \quad (4)$$

Here, $\alpha_p^{AB}[m, n]$ is the scalar TF-domain coefficient of the p -th path and is given by

$$\alpha_p^{XY}[m, n] = g_p^{XY} e^{-j2\pi(f_m + f_{XY} - f_c)\tau_p} e^{j2\pi\nu_p^{XY}t_n}, \quad (5)$$

where g_p^{XY} , τ_p , and ν_p^{XY} denote the complex path gain, delay, and Doppler frequency of the p -th path, respectively.

The discrete DD-domain MIMO channel response of link XY obtained at the OTFS receiver is defined as

$$\mathbf{H}_{XY}^{DD} = \text{SFFT}_{M,N} \{ \mathbf{H}_{XY}^{TF} \}. \quad (6)$$

Here, $\text{SFFT}_{M,N}\{\cdot\}$ denotes the SFFT operation over an $M \times N$ TF grid. Accordingly, the DD-domain MIMO channel matrix of link XY at delay index l and Doppler index k has dimensions $\mathbf{H}_{XY}^{DD}[l, k] \in \mathbb{C}^{T_Y \times T_X}$, where T_X and T_Y denote the numbers of antennas at transmitter X and receiver Y , respectively. In this paper, $\mathbf{H}_{AB}^{DD}[l, k]$ and $\mathbf{H}_{BA}^{DD}[l, k]$ serve as the underlying channel responses for constructing key-generation features.

B. Eavesdropper Model

Eve is assumed to be a passive eavesdropper that does not interfere with the Alice–Bob communication link. Eve knows the proposed protocol, public system parameters, and quantization rules, but does not know the random unitary matrices generated at the legitimate terminals. Eve cannot directly observe the legitimate DD-domain MIMO channel coefficients in (4) and instead observes the Alice–Eve and Bob–Eve links, whose DD-domain MIMO channel coefficients are denoted by $\mathbf{H}_{AE}^{DD}[l, k]$ and $\mathbf{H}_{BE}^{DD}[l, k]$, respectively.

Let $\mathcal{S} = \{(l_i, k_i)\}_{i=1}^{|S|}$ denote the set of DD cells used for key generation, which is selected from high-energy DD-domain channel components. The DD cells are vectorized according to the ordering of $\mathcal{S}$. The channel feature vector associated with link $\xi \in \{AB, BA, AE, BE\}$ is defined as

$$\mathbf{h}_\xi = \left[\text{vec}(\mathbf{H}_\xi^{DD}[l_1, k_1])^T, \dots, \text{vec}(\mathbf{H}_\xi^{DD}[l_{|S|}, k_{|S|}])^T \right]^T, \quad (7)$$

where $\text{vec}(\cdot)$ denotes the vectorization of each DD-domain MIMO channel matrix. Let $\bar{\mathbf{h}}_{AB}$ and $\bar{\mathbf{h}}_{BA}$ denote the normalized and dimension-aligned reference vectors derived from $\mathbf{h}_{AB}$ and $\mathbf{h}_{BA}$, respectively. Following the channel-correlation-based eavesdropper evaluation in [10], the correlation between the Eve-side channel vectors and the corresponding legitimate reference vectors is controlled by the target correlation parameter ρ_E , where $0 \leq \rho_E \leq 1$. Specifically, the Alice–Eve and Bob–Eve channel vectors are generated using a Gaussian correlation model [17] as

$$\begin{aligned} \mathbf{h}_{AE} &= \rho_E \bar{\mathbf{h}}_{AB} + \sqrt{1 - \rho_E^2} \mathbf{w}_{AE}, \\ \mathbf{h}_{BE} &= \rho_E \bar{\mathbf{h}}_{BA} + \sqrt{1 - \rho_E^2} \mathbf{w}_{BE}, \end{aligned} \quad (8)$$

where $\mathbf{w}_{AE}$ and $\mathbf{w}_{BE}$ are circularly symmetric complex Gaussian random vectors that are independent of the corresponding reference vectors and normalized to have the same average power as those vectors. A larger ρ_E represents stronger

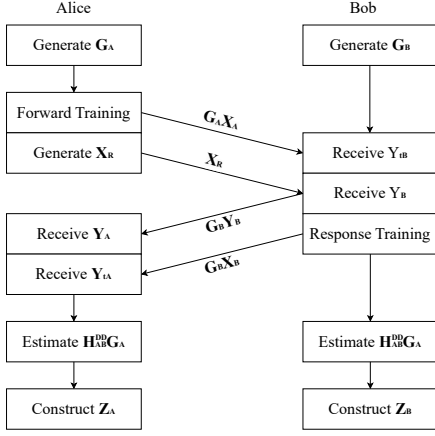


Fig. 2: Proposed training procedure for obtaining the randomly rotated DD-domain MIMO coefficient $\mathbf{H}_{AB}^{\text{DD}}[l, k]\mathbf{G}_A$.

correlation between $\mathbf{h}_{AE}$ and $\bar{\mathbf{h}}_{AB}$ and between $\mathbf{h}_{BE}$ and $\bar{\mathbf{h}}_{BA}$. Thus, ρ_E is used as an evaluation parameter that controls the correlation strength of Eve's candidate features, rather than specifying a particular Eve location or propagation geometry. Based on the generated Alice–Eve and Bob–Eve channel vectors, Eve constructs candidate features for key generation.

III. PROPOSED SYSTEM

A. Randomly Rotated DD-MIMO Feature Extraction

As shown in Fig. 2, the proposed scheme performs bidirectional channel probing, where Alice and Bob exchange training signals weighted by locally generated random unitary matrices and obtain randomly rotated DD-domain MIMO channel coefficients at both terminals.

We first describe the process by which both Alice and Bob obtain $\mathbf{H}_{AB}^{\text{DD}}[l, k]\mathbf{G}_A$. Alice and Bob locally generate random unitary matrices $\mathbf{G}_A \in \mathbb{C}^{T_A \times T_A}$ and $\mathbf{G}_B \in \mathbb{C}^{T_B \times T_B}$ satisfying $\mathbf{G}_A^H \mathbf{G}_A = \mathbf{I}_{T_A}$ and $\mathbf{G}_B^H \mathbf{G}_B = \mathbf{I}_{T_B}$, respectively. Alice transmits the training signals $\mathbf{G}_A \mathbf{X}_A$ and $\mathbf{X}_R$, where $\mathbf{X}_A \in \mathbb{C}^{T_A \times N_f}$ and $\mathbf{X}_R \in \mathbb{C}^{T_A \times N_f}$ are normalized training matrices satisfying $\mathbf{X}_A \mathbf{X}_A^H = \mathbf{I}_{T_A}$ and $\mathbf{X}_R \mathbf{X}_R^H = \mathbf{I}_{T_A}$, and N_f denotes the training sequence length. For a DD cell $(l, k) \in \mathcal{S}$, the received signals at Bob are given by

$$\mathbf{Y}_{tB}[l, k] = \mathbf{H}_{AB}^{\text{DD}}[l, k]\mathbf{G}_A \mathbf{X}_A + \mathbf{W}_{tB}[l, k], \quad (9)$$

and

$$\mathbf{Y}_B[l, k] = \mathbf{H}_{AB}^{\text{DD}}[l, k]\mathbf{X}_R + \mathbf{W}_B[l, k], \quad (10)$$

where $\mathbf{W}_{tB}[l, k]$ and $\mathbf{W}_B[l, k]$ denote additive white Gaussian noise (AWGN) matrices whose entries are independent and identically distributed as $\mathcal{CN}(0, \sigma_w^2)$. Bob then obtains

$$\hat{\mathbf{Z}}_{AB,A}[l, k] = \mathbf{Y}_{tB}[l, k]\mathbf{X}_A^\dagger \simeq \mathbf{H}_{AB}^{\text{DD}}[l, k]\mathbf{G}_A. \quad (11)$$

Here, $(\cdot)^\dagger$ denotes the Moore–Penrose pseudoinverse.

To enable Alice to obtain $\mathbf{H}_{AB}^{\text{DD}}[l, k]\mathbf{G}_A$, Bob applies $\mathbf{G}_B$ to $\mathbf{Y}_B[l, k]$ and transmits it back to Alice. Bob also transmits

$\mathbf{G}_B \mathbf{X}_B$, where $\mathbf{X}_B \in \mathbb{C}^{T_B \times N_f}$ is a normalized training matrix satisfying $\mathbf{X}_B \mathbf{X}_B^H = \mathbf{I}_{T_B}$. The received signals at Alice are then given by

$$\mathbf{Y}_A[l, k] = \mathbf{H}_{BA}^{\text{DD}}[l, k]\mathbf{G}_B \mathbf{H}_{AB}^{\text{DD}}[l, k]\mathbf{X}_R + \tilde{\mathbf{W}}_A[l, k], \quad (12)$$

and

$$\mathbf{Y}_{tA}[l, k] = \mathbf{H}_{BA}^{\text{DD}}[l, k]\mathbf{G}_B \mathbf{X}_B + \mathbf{W}_{tA}[l, k]. \quad (13)$$

Then, Alice estimates

$$\hat{\mathbf{E}}[l, k] = \mathbf{Y}_A[l, k]\mathbf{X}_R^\dagger \simeq \mathbf{H}_{BA}^{\text{DD}}[l, k]\mathbf{G}_B \mathbf{H}_{AB}^{\text{DD}}[l, k], \quad (14)$$

and

$$\hat{\mathbf{F}}[l, k] = \mathbf{Y}_{tA}[l, k]\mathbf{X}_B^\dagger \simeq \mathbf{H}_{BA}^{\text{DD}}[l, k]\mathbf{G}_B. \quad (15)$$

For the selected DD cells, $\hat{\mathbf{F}}[l, k] \in \mathbb{C}^{T_A \times T_B}$ is assumed to have full column rank, i.e., $\text{rank}(\hat{\mathbf{F}}[l, k]) = T_B$. This condition ensures that the Moore–Penrose pseudoinverse can be used to recover the randomly rotated coefficient. Alice obtains the corresponding randomly rotated DD-domain MIMO coefficient as

$$\hat{\mathbf{Z}}_{AB,A}[l, k] = \hat{\mathbf{F}}^\dagger[l, k]\hat{\mathbf{E}}[l, k]\mathbf{G}_A \simeq \mathbf{H}_{AB}^{\text{DD}}[l, k]\mathbf{G}_A. \quad (16)$$

Similarly, by exchanging the roles of Alice and Bob, both terminals obtain the corresponding estimates $\hat{\mathbf{Z}}_{BA,A}[l, k]$ and $\hat{\mathbf{Z}}_{BA,B}[l, k]$ of $\mathbf{H}_{BA}^{\text{DD}}[l, k]\mathbf{G}_B$. The complex feature vectors at Alice, Bob, and Eve are defined as

$$\mathbf{z}_A = \begin{bmatrix} \text{vec}(\{\hat{\mathbf{Z}}_{AB,A}[l, k]\}_{(l,k) \in \mathcal{S}}) \\ \text{vec}(\{\hat{\mathbf{Z}}_{BA,A}[l, k]\}_{(l,k) \in \mathcal{S}}) \end{bmatrix}, \quad (17)$$

$$\mathbf{z}_B = \begin{bmatrix} \text{vec}(\{\hat{\mathbf{Z}}_{AB,B}[l, k]\}_{(l,k) \in \mathcal{S}}) \\ \text{vec}(\{\hat{\mathbf{Z}}_{BA,B}[l, k]\}_{(l,k) \in \mathcal{S}}) \end{bmatrix}, \quad (18)$$

and

$$\mathbf{z}_E = \begin{bmatrix} \text{vec}(\{\hat{\mathbf{Z}}_{AE,E}[l, k]\}_{(l,k) \in \mathcal{S}}) \\ \text{vec}(\{\hat{\mathbf{Z}}_{BE,E}[l, k]\}_{(l,k) \in \mathcal{S}}) \end{bmatrix}. \quad (19)$$

Here, $\hat{\mathbf{Z}}_{AE,E}[l, k]$ and $\hat{\mathbf{Z}}_{BE,E}[l, k]$ denote Eve's candidate coefficient matrices constructed from the Alice–Eve and Bob–Eve links, respectively. For performance evaluation, these candidate matrices are arranged to have the same feature order and number of components as the corresponding legitimate feature components.

B. Coefficient Quantization and Key Generation

The proposed scheme first converts each complex feature vector into a real-valued feature vector by stacking its real and imaginary parts, and then applies scalar quantization to the resulting real-valued features. For Alice, the real-valued quantization input is defined as

$$\mathbf{r}_A = [\Re\{\mathbf{z}_A\}^T \quad \Im\{\mathbf{z}_A\}^T]^T. \quad (20)$$

The quantization inputs for Bob and Eve, denoted by $\mathbf{r}_B$ and $\mathbf{r}_E$, respectively, are defined in the same manner by replacing $\mathbf{z}_A$ with $\mathbf{z}_B$ and $\mathbf{z}_E$.

Let q denote the number of bits generated from each real-valued feature, and let $Q = 2^q$ denote the number of quantization levels. The quantization thresholds satisfy

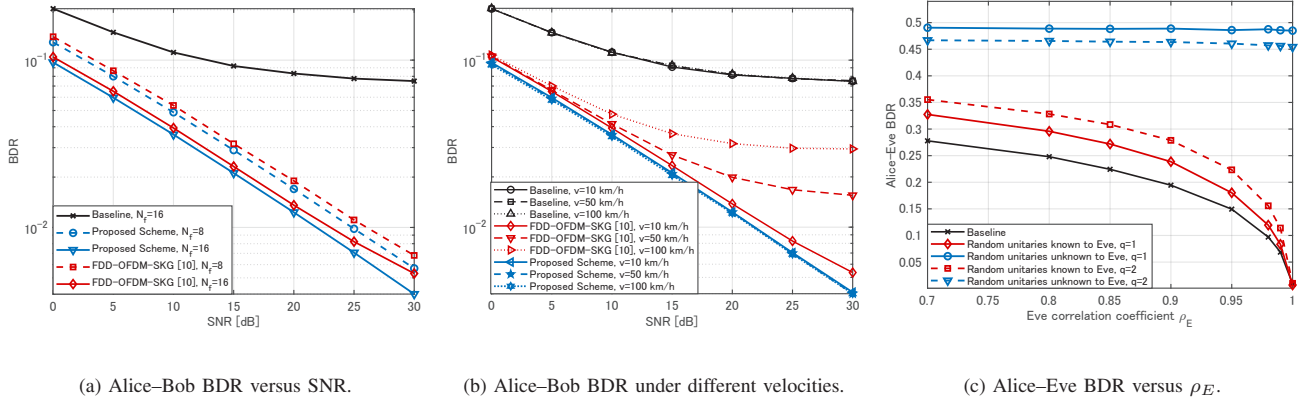


Fig. 3: BDR performance of the proposed scheme, the FDD-OFDM-SKG benchmark [10], and the baseline.

$-\infty = \eta_0 < \eta_1 < \dots < \eta_{Q-1} < \eta_Q = +\infty$ and are determined from Alice's empirical distribution as

$$\eta_i = F_A^{-1}(i/Q), \quad i = 1, 2, \dots, Q-1, \quad (21)$$

where $F_A^{-1}(\cdot)$ denotes the inverse empirical cumulative distribution function of the elements of $\mathbf{r}_A$. The quantization thresholds $\{\eta_i\}_{i=1}^{Q-1}$, rather than Alice's raw feature vector, are shared through an authenticated public channel and are treated as public side information available to Eve. Using Alice's empirical distribution defines a single public quantization rule, which is commonly applied to Alice, Bob, and Eve.

When a real-valued feature r satisfies $\eta_j \leq r < \eta_{j+1}$ for $j = 0, 1, \dots, Q-1$, its quantization index is defined as j . The index is then encoded using a q -bit Gray encoding map $\mathcal{G}_q(\cdot)$ as

$$\mathbf{b}(r) = \mathcal{G}_q(j). \quad (22)$$

Let D_z denote the common length of the complex feature vectors before quantization. Since both the Alice-Bob and Bob-Alice DD-domain MIMO coefficients are used, this length is given by

$$D_z = 2|\mathcal{S}|T_A T_B. \quad (23)$$

For Alice, the raw bit sequence is generated by concatenating the quantized bits as

$$\mathbf{K}_A = [\mathbf{b}(r_{A,1})^T, \dots, \mathbf{b}(r_{A,2D_z})^T]^T. \quad (24)$$

The raw bit sequences for Bob and Eve, denoted by $\mathbf{K}_B$ and $\mathbf{K}_E$, respectively, are defined in the same manner by replacing $\mathbf{r}_A$ with $\mathbf{r}_B$ and $\mathbf{r}_E$. Therefore, the generated raw bit length is

$$L = 2qD_z = 4q|\mathcal{S}|T_A T_B. \quad (25)$$

The obtained bits are raw keys before information reconciliation and privacy amplification. In practical SKG, Alice and Bob apply these post-processing to correct residual bit disagreements and obtain the final secret key. In this paper, BDR is evaluated using the raw bit sequences, whereas SKC is evaluated using the pre-quantization real-valued feature vectors.

TABLE I: Simulation Parameters

Parameter	Value
Carrier frequency f_c	2.0 GHz
Subcarrier spacing Δf_c	15 kHz
Number of subcarriers (OFDM)	256
OFDM symbols per frame	128
OTFS grid size	$M = 256, N = 128$
FDD spacing Δf_{FDD}	5 MHz
Antenna configuration	$T_A = 4, T_B = T_E = 2$
Number of trials	5000

IV. PERFORMANCE EVALUATION

In this section, we evaluate the proposed SKG for FDD-OTFS through computer simulations. The simulation parameters are listed in Table I. The signal-to-noise ratio (SNR) is defined as the average received training-signal power divided by the AWGN power. The evaluation uses two metrics: BDR and mutual-information-based SKC. BDR measures the mismatch ratio between raw key bit sequences, whereas SKC evaluates the mutual-information advantage of the legitimate features over Eve's features. Let $\mathbf{K}_A$, $\mathbf{K}_B$, and $\mathbf{K}_E$ denote the raw bit sequences of Alice, Bob, and Eve, respectively. The Alice-Bob and Alice-Eve BDRs are defined as

$$\text{BDR}_{AB} = \frac{1}{L} d_H(\mathbf{K}_A, \mathbf{K}_B), \quad \text{BDR}_{AE} = \frac{1}{L} d_H(\mathbf{K}_A, \mathbf{K}_E), \quad (26)$$

where L is the number of compared bits and $d_H(\cdot, \cdot)$ denotes the Hamming distance. The mutual-information-based SKC is evaluated using the pre-quantization real-valued feature vectors $\mathbf{r}_A$, $\mathbf{r}_B$, and $\mathbf{r}_E$ as

$$R_{\text{SKC}} = [I(\mathbf{r}_A; \mathbf{r}_B) - I(\mathbf{r}_A; \mathbf{r}_E)]^+, \quad (27)$$

where $I(\cdot; \cdot)$ denotes mutual information and $[x]^+ = \max(x, 0)$. In this paper, mutual information is estimated from correlation coefficients between real-valued feature vectors using a Gaussian correlation model and is expressed in bits per real-valued source sample [17]. As a benchmark, we consider FDD-OFDM-SKG, in which OFDM is used to observe the same time-varying channel, and pilot-assisted processing is applied to the channel frequency response coefficients [10]. In

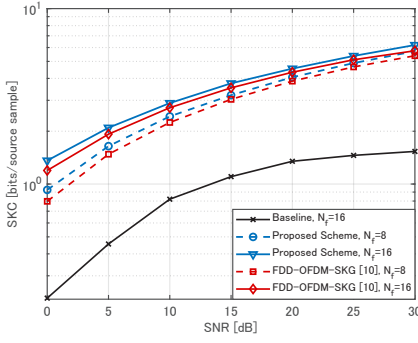


Fig. 4: Mutual-information-based SKC versus SNR.

addition, the baseline directly quantizes the DD-domain FDD-OTFS MIMO channel obtained by Alice and Bob without using the bidirectional channel probing. Eve observes the Alice–Eve and Bob–Eve channels generated according to the target correlation parameter ρ_E and generates a candidate bit using the same rule as Alice and Bob. The case where Eve knows the random unitary matrices is included as a worst-case, whereas the independent-unitary case models the practical situation in which Eve cannot reproduce the random unitary matrix.

Fig. 3(a) shows the Alice–Bob BDR as a function of SNR, where N_f denotes the training sequence length. The proposed scheme achieves a lower BDR than the baseline across the entire SNR range and provides an improvement of one order of magnitude in the high-SNR region. Increasing N_f reduces the BDR by improving estimation accuracy. Fig. 3(b) shows the Alice–Bob BDR under different velocities. The proposed scheme maintains a BDR on the order of 10^{-3} in the high-SNR region, whereas the FDD-OFDM-SKG benchmark exhibits a BDR floor on the order of 10^{-2} as the velocity increases. These results indicate the robustness of DD-domain features in high-mobility environments. Fig. 3(c) shows the BDR between Alice and Eve as a function of the Eve target correlation parameter ρ_E . When Eve knows the random unitary matrices, the Alice–Eve BDR decreases as ρ_E increases. In contrast, when Eve uses independent random unitary matrices, the Alice–Eve BDR remains close to 0.5 regardless of ρ_E . This result indicates that local random rotation makes reconstruction of the randomly rotated coefficients difficult even for a highly correlated Eve.

Fig. 4 shows the mutual-information-based SKC as a function of SNR. The proposed scheme achieves a higher SKC than FDD-OFDM-SKG and the baseline, especially in the high-SNR region. These results demonstrate that the proposed scheme is effective in terms of key agreement, secrecy, and secret key capacity.

V. CONCLUSION

This paper proposed a physical-layer SKG scheme for FDD-OTFS systems. The proposed scheme performs bidirectional channel probing with locally generated random unitary matrices to obtain randomly rotated DD-domain MIMO channel

coefficients, and generates raw key bits by quantizing their real and imaginary parts. Simulation results showed that the proposed scheme reduces the BDR compared with the direct FDD-OTFS quantization baseline and achieves more stable key agreement than the FDD-OFDM-SKG benchmark in high-mobility environments. The SKC results further confirmed its effectiveness in terms of the capability.

ACKNOWLEDGMENTS

This work was supported in part by JSPS KAKENHI (25K01227), Toyota Physics and Chemistry Research Institute, and Japan Keirin Autorace (JKA) foundation.

REFERENCES

- [1] E. Illi *et al.*, “Physical layer security for authentication, confidentiality, and malicious node detection: A paradigm shift in securing IoT networks,” *IEEE Commun. Surveys Tuts.*, vol. 26, no. 1, pp. 347–423, First Quart. 2024.
- [2] Q. Xiao, J. Zhao, S. Feng, G. Li, and A. Hu, “Securing NextG networks with physical-layer key-generation: A survey,” *Security and Safety*, vol. 3, Art. no. 2023021, 2024.
- [3] H. Zhao, E. Guo, Z. Lian, Y. Zhao, X. Huang, and C. Su, “A review and implementation of physical layer security techniques in the Internet of Things,” *J. Inf. Security Appl.*, vol. 83, Art. no. 103779, 2024.
- [4] J. M. Hamamreh, H. M. Furqan, and H. Arslan, “Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey,” *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1773–1828, Second Quart. 2019.
- [5] S. Kojima and S. Sugiura, “User-independent randomized pilot activation for secure key-generation,” *IEEE Trans. Wireless Commun.*, vol. 23, no. 9, pp. 11624–11635, Sept. 2024.
- [6] U. M. Maurer, “Secret key agreement by public discussion from common information,” *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.
- [7] 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. 12978–12990, Sept. 2024.
- [8] S. Kojima and S. Sugiura, “Non-orthogonal multiple access based physical-layer group secret key distribution,” *IEEE Trans. Veh. Technol.*, Early Access, Dec. 2025.
- [9] J. Zhang, G. Li, A. Marshall, A. Hu, and L. Hanzo, “A new frontier for IoT security emerging from three decades of key-generation relying on wireless channels,” *IEEE Access*, vol. 8, pp. 138406–138446, 2020.
- [10] D. Qin and Z. Ding, “Exploiting multi-antenna non-reciprocal channels for shared secret key generation,” *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 12, pp. 2693–2705, Dec. 2016.
- [11] X. Zhang, G. Li, J. Zhang, A. Hu, Z. Hou, and B. Xiao, “Deep-learning-based physical-layer secret key generation for FDD systems,” *IEEE Internet Things J.*, vol. 9, no. 8, pp. 6081–6094, Apr. 2022.
- [12] M. A. Ayg  l, H. M. Furqan, H. A. C  rpan, and H. Arslan, “FDD secret key generation: Identifying vulnerabilities and a novel defensive method,” *IEEE Wireless Commun. Lett.*, vol. 14, no. 5, pp. 1446–1450, May 2025.
- [13] Y. Matsuzaki, S. Kojima, and S. Sugiura, “Deep-learning-based physical-layer lightweight authentication in frequency-division duplex channel,” *IEEE Commun. Lett.*, vol. 27, no. 8, pp. 1969–1973, Aug. 2023.
- [14] R. Hadani *et al.*, “Orthogonal time frequency space modulation,” in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, San Francisco, CA, USA, Mar. 2017, pp. 1–6.
- [15] U. Saeed, R. Calderbank, K. Zeng, E. S. Bentley, L. Huie-Seversky, K. Said, and L. Liu, “Key generation and secrecy analysis using OTFS for TDD systems,” *IEEE Trans. Wireless Commun.*, vol. 24, no. 8, pp. 6275–6289, Aug. 2025.
- [16] A. F. Kawoya, H. Wang, and M. S. Abood, “Efficient key extraction for secure vehicular communication through OTFS,” *IEEE Commun. Lett.*, vol. 28, no. 3, pp. 468–472, Mar. 2024.
- [17] J. Zhang, B. He, T. Q. Duong, and R. Woods, “On the key-generation from correlated wireless channels,” *IEEE Commun. Lett.*, vol. 21, no. 4, pp. 961–964, Apr. 2017, doi: 10.1109/LCOMM.2017.2649496.