A Novel and Secure AFDM System for High Mobility Environments

Yusuf Islam Tek, *Graduate Student Member, IEEE* and Ertugrul Basar, *Fellow, IEEE*

***Abstract*—This paper introduces a novel and secure affine frequency division multiplexing (AFDM) system designed for high-mobility environments in next-generation wireless networks. Leveraging the reciprocity of wireless channels and the flexibility of the pre-chirp parameter, the system establishes secure communication by generating unique pre-chirp parameters from the shared channel properties between legitimate users, effectively excluding eavesdroppers. A quantization mechanism is incorporated to ensure robustness against noise and channel estimation errors. Simulation results demonstrate that the proposed system achieves comparable error performance to conventional AFDM and outperforms other benchmark schemes while significantly enhancing security, positioning it as a promising solution for 6G wireless communication.**

***Index Terms*—6G networks, AFDM modulation, channel reciprocity, linear time-varying (LTV) channel, physical layer security (PLS), pre-chirp parameter, secure communication.**

I. Introduction

6G technology represents a paradigm shift in wireless communication, offering ultra-high data rates, low latency, and extensive connectivity, particularly in high-mobility scenarios such as high-speed trains, autonomous vehicles, and aerial platforms. These environments pose significant challenges to maintaining secure and reliable communication due to rapid channel variations and increased vulnerability to attacks. In this context, physical layer security (PLS) emerges as a critical enabler, leveraging the inherent characteristics of wireless channels, such as fading and noise, to enhance data confidentiality and integrity. By addressing security threats like eavesdropping and jamming without relying solely on computational cryptography, PLS provides a robust framework for safeguarding 6G networks, ensuring resilience and trustworthiness in highly dynamic environments [1].

Affine frequency division multiplexing (AFDM) is an emerging waveform designed to address the challenges of high-mobility environments, such as those anticipated in 6G networks [2]. Unlike traditional orthogonal frequency division multiplexing (OFDM), which performs well in static or low-mobility scenarios but struggles with high Doppler effects in the linear time-variant (LTV) channels, AFDM leverages the discrete affine Fourier transform (DAFT) to provide resilience against both time and frequency domain impairments. This makes it particularly suited for high-speed vehicular and aerial communications. On the other hand, orthogonal time frequency space (OTFS) is also a suitable waveform for high mobility, and both AFDM and OTFS are innovative waveforms developed to meet the high mobility requirements of 6G. However, there are significant differences when compared in terms of complexity. While OTFS processes signals in the 2D delay-Doppler domain instead of the time-frequency domain, AFDM relies on the 1D DAFT, which provides similar benefits by chirp-like subcarriers. This makes AFDM a suitable candidate for next-generation networks that need to handle heavy complexity and stability requirements.

Moreover, security is also a critical aspect of next-generation communication networks. Mobility significantly complicates secure wireless communication due to rapid channel variations, making conventional security approaches vulnerable to interception or decoding attacks. In order to tackle this security need, many studies have been proposed in the literature. In the study [3], a key generation method exploiting the LTV channel has been proposed for frequency-division duplexing (FDD) systems, while in [4], the authors have proposed a method for the same purpose but in time-division duplexing (TDD) systems. Furthermore, to establish secure communication in aerial networks using OTFS, in [5], a key generation and constellation rotation method has been proposed. Moreover, in [6], a seed extracted from the channel is utilized to generate a sequence based on the Gosudarstvennyi standard, which is subsequently employed to perturb the OTFS modulation, thereby securing the transmitted information. In [7], the authors have introduced a novel resource-hopping mechanism for OTFS systems integrated with delay- or Doppler-partitioned sparse code multiple access. This approach effectively mitigates jamming interference in controlled multiuser uplink communications. In [8], the authors proposed a rotated OTFS (R-OTFS) waveform employing precoding with an orthogonal transformation matrix derived from the equivalent channel of the legitimate users, enabling secure and reliable symbol rotation. The authors in [9] have presented a precoding scheme employing a projection matrix combined with artificial noise to disrupt potential eavesdroppers for downlink OTFS systems.

Considering the significance of security under high mobility, exploiting waveform-specific parameters for enhanced stability and security becomes particularly relevant. Conventional AFDM systems utilize the DAFT as a modulator, with two basic system parameters: c_1 (post-chirp) and c_2 (pre-chirp). By appropriately configuring these parameters, subchannels corresponding to different propagation paths can be effectively separated, resulting in a sparse and quasi-static channel representation within the DAF domain [2]. This enables AFDM systems to achieve full diversity in doubly dispersive channels. c_1 governs the frequency dispersion of the signal and plays a key role in aligning the AFDM basis functions with the Doppler characteristics of the channel, ensuring better separation and

Y. I. Tek is with the Communications Research and Innovation Laboratory (CoreLab), Department of Electrical and Electronics Engineering, Koç University, Sariyer 34450, Istanbul, Turkey. Email: ytek21@ku.edu.tr.

E. Basar is with the Department of Electrical Engineering, Tampere University, 33720 Tampere, Finland, on leave from the CoreLab, Department of Electrical and Electronics Engineering, Koc University, 34450 Sariyer, Istanbul, Turkey. Email: ertugrul.basar@tuni.fi and ebasar@ku.edu.tr.

This work is supported by TUBITAK under Grant Number 124E419.

resilience against time variations. Since the performance of the system is primarily influenced by c_1, it must be carefully optimized to ensure full diversity. In contrast, c_2 serves as a more flexible parameter. It manipulates the dispersion of the signal on the time-frequency plane. The adaptability of c_2 has been extensively explored in the literature to enhance system performance. For instance, studies such as [10] and [11] propose various index modulation schemes that capitalize on the flexibility of c_2 different than subcarrier-based IM as in [12]. Similarly, the work in [13] introduces a peak-to-average power ratio (PAPR) reduction technique by constructing optimized c_2 subsets. Furthermore, a range estimation method proposed in [14] also leverages the malleability of c_2. From the PLS perspective, the authors in [15] have introduced a method involving the permutation of the pre-chirp sequence, rendering it secure against decoding attempts by an eavesdropper, even when equipped with quantum-based computers. Furthermore, [16] presents the weighted affine Fourier transform (WAFT) as an innovative unitary transform that extends AFT to enable a hybrid carrier communication system. The WAFT-based system integrates single-carrier and chirp multi-carrier modulation, offering dynamic control over PAPR and bit error rate (BER) through adjustable parameters. Additionally, its multi-parameter design strengthens encryption by increasing the complexity for eavesdroppers in cases of parameter mismatch.

In this study, we present a novel and secure AFDM system designed to address the security requirements of next-generation wireless networks. The proposed system leverages the reciprocity of wireless channels in TDD systems and the inherent flexibility of the pre-chirp parameter c_2 to implement a parameter generation-based approach. While conventional AFDM systems restrict the pre-chirp parameter c_2 to either a rational number below a specific threshold or an irrational value, [17] has demonstrated that the choice of c_2 does not influence the system performance using a minimum mean-squared error (MMSE) equalizer. Recent studies such as [10] and [14] have exploited this property and showed c_2 can also be configured as a set of values corresponding to individual subcarriers. Also, in [18], the authors have simplified the AFDM system by removing the dependency on c_2. Building on this insight, our system utilizes the shared wireless channel between two legitimate users to dynamically generate an identical pre-chirp parameter set for both parties using the DAFT. Since this parameter is generated according to the unique Alice-Bob channel, the eavesdropper is unable to derive the same pre-chirp parameter set, thereby securing the transmitted information. Additionally, a quantization process is employed on the generated parameter set to facilitate efficient information reconciliation.

Although the existing literature on PLS schemes for OTFS is extensive, research into PLS methods specifically tailored for AFDM remains relatively scarce. The aforementioned AFDM-based PLS schemes inherently offer lower complexity compared to OTFS-based schemes, primarily due to the simpler modulation structure of AFDM versus the grid structure of OTFS. However, unlike other PLS schemes, our design leverages the inherent pre-chirp modulation property of AFDM. Consequently, our proposed scheme requires no additional steps beyond the commonly adopted channel sounding and quantization processes used in most other PLS schemes.

The remainder of the paper is organized as follows. Section II presents the transceiver structure and provides a detailed analysis of the proposed secure AFDM system. Section III discusses the simulation results, and finally, Section IV concludes the paper.

Notations: Scalars, vectors, and matrices are denoted by x, $\mathbf{x}$, and $\mathbf{X}$, respectively. The notation x_i refers to the i-th element of vector $\mathbf{x}$, while $\mathbf{X}[i,j]$ denotes the element at the i-th row and j-th column of matrix $\mathbf{X}$. The identity matrix of size $N \times N$ is denoted by $\mathbf{I}_N$. A diagonal matrix formed by the sequence $[x_0, \ldots, x_M]$ is represented as $\mathbf{X} = \mathrm{diag}([x_0, \ldots, x_M])$. Superscripts $(\cdot)^T$ and $(\cdot)^H$ indicate the transpose and Hermitian transpose operations, respectively. The operators $\mathcal{R}(\cdot)$ and $\lfloor \cdot \rfloor$ stand for the real part of a complex value and the floor function, respectively. A circularly symmetric complex Gaussian random variable X with variance σ^2 is expressed as $X \sim \mathcal{CN}(0, \sigma^2)$, while a uniformly distributed random variable Y over the interval $[a, b]$ is denoted by $Y \sim U(a, b)$. Finally, $\mathbf{F}_N$ represents the normalized N-point discrete Fourier transform (DFT) matrix.

II. Secure AFDM System

In this section, we first present the transceiver model, detailing the AFDM modulation, transmission, and reception under the proposed secure framework. Later, we explain how Alice and Bob obtain their pre-chirp parameter sets by performing channel sounding and extracting key features from their reciprocal channel. Finally, we describe the quantization process.

A. Transceiver Model

In this section, we introduce the transceiver model depicted in Fig. 1 and employed in the proposed system. Let us assume that Alice wants to initiate a secret communication with Bob. Alternatively, Bob may also want to initiate a secret communication with Alice, as the procedural steps remain identical for both parties. We consider an AFDM system with N subcarriers, a sample period of T seconds, $B = 1/T$ Hz bandwidth, and a subcarrier spacing of $\Delta f = B/N$ Hz. It is assumed that this communication system adopts TDD. In the AFDM system, the information symbols are converted into chirp-domain signals by using inverse DAFT (IDAFT) and then transmitted over an LTV channel. Then, the received signal is converted back to the DAF domain information symbols on the receiving end through the DAFT operation.

In order to further express the modulation steps of the proposed AFDM system, firstly, we define the DAFT matrix $\mathbf{A} \in \mathbb{C}^{N \times N}$ and IDAFT matrix $\mathbf{A}^{-1} = \mathbf{A}^H \in \mathbb{C}^{N \times N}$. Since $\mathbf{A}$ is a unitary matrix, performing inverse and Hermitian transpose operations end up with the same results. $\mathbf{A}$ is expressed as

$$\mathbf{A} \triangleq \mathbf{\Lambda}_{\mathbf{c}_2} \mathbf{F}_N \mathbf{\Lambda}_{c_1}, \tag{1}$$

where $\mathbf{\Lambda}_{c_1} \in \mathbb{C}^{N \times N}$ is the post-chirp matrix with parameter c_1 and $\mathbf{\Lambda}_{\mathbf{c}_2} \in \mathbb{C}^{N \times N}$ is the pre-chirp matrix with parameter

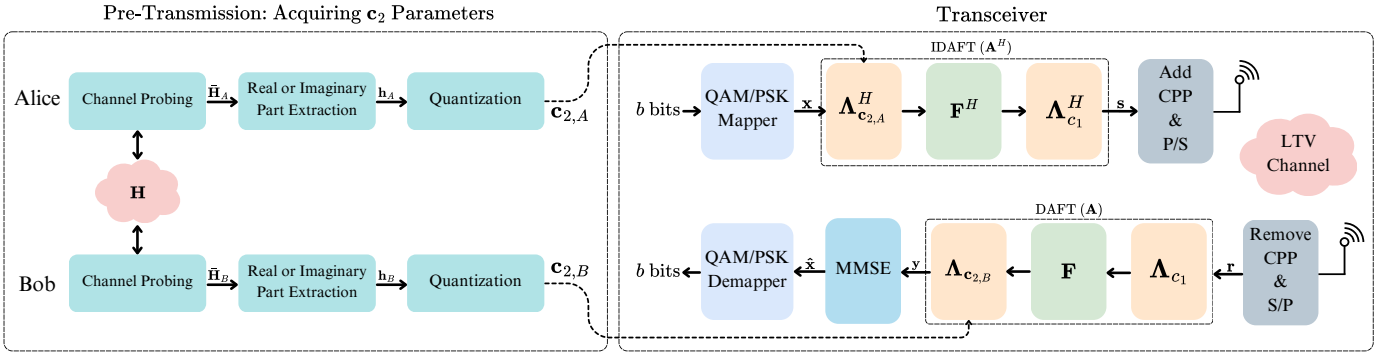

Fig. 1. Pre-transmission and transceiver scheme of the proposed system between two legitimate users. In this figure, matrices and vectors for Alice and Bob are labeled with subscripts A and B, respectively. However, since the operations are identical for both Alice and Bob, these subscripts are omitted in the explanation to avoid notational redundancy.

set $\mathbf{c}_2 = [c_{2,1}, \ldots, c_{2,n}, \ldots, c_{2,N}] \in \mathbb{R}^{N\times 1}, n = 1, \ldots, N$. In the conventional AFDM system, a c_2 value is used in the pre-chirp matrix for each subcarrier. However, in this scheme, we use $\mathbf{c}_2$, which is a parameter set obtained from the channel and will be explained in the following subsection. These chirp matrices are defined as

$$\mathbf{\Lambda}_{c_1} = \text{diag}\left(e^{-j2\pi c_1 n^2}, n = 0, \ldots, N-1\right), \tag{2a}$$

$$\mathbf{\Lambda}_{\mathbf{c}_2} = \text{diag}\left(e^{-j2\pi c_{2,n}(n-1)^2}, n = 1, \ldots, N\right). \tag{2b}$$

Later on, to obtain the transmit vector, first, the information bits are modulated by a Q-ary modulation alphabet, and DAF domain information symbol vector $\mathbf{x} \in \mathbb{C}^{N\times 1}$ is obtained. Subsequently, the time domain transmit signal $\mathbf{s} \in \mathbb{C}^{N\times 1}$ can be obtained by performing IDAFT operation as

$$\mathbf{s} = \mathbf{A}^H\mathbf{x} = \mathbf{\Lambda}^H_{c_1}\mathbf{F}^H_N\mathbf{\Lambda}^H_{\mathbf{c}_2}\mathbf{x}. \tag{3}$$

Before transmitting $\mathbf{s}$, a chirp-periodic prefix (CPP) should be added. CPP serves a purpose similar to that of the cyclic prefix (CP) in OFDM. The CPP ensures that a multipath channel sees the AFDM symbol as if it were periodically extended with matching chirp patterns. Hence, multipath propagation is addressed, and the channel is effectively transformed into a periodic domain. Afterward, the transmit signal $\mathbf{s}$ is sent over a doubly-dispersive channel modeled as

$$h(\tau, \nu) = \sum_{p=1}^{P} h_p \delta(\tau - \tau_p)\delta(\nu - \nu_p), \tag{4}$$

where P is the number of paths and h_p is the channel gain of the p-th path while τ_p and ν_p are the delay time and the Doppler shift of the p-th path, respectively. On the receiver side, the CPP-discarded time domain received signal $\mathbf{r} \in \mathbb{C}^{N\times 1}$ can be expressed as

$$\mathbf{r} = \mathbf{H}\mathbf{s} + \mathbf{w}, \tag{5}$$

where $\mathbf{w} \in \mathbb{C}^{N\times 1} \sim \mathcal{CN}(N_0\mathbf{I}_N)$, and $\mathbf{I}_N$ is the $N \times N$ identity matrix. The true time domain LTV channel matrix between Alice and Bob $\mathbf{H} \in \mathbb{C}^{N\times N}$ is modeled as

$$\mathbf{H} = \sum_{p=1}^{P} h_p \mathbf{\Gamma}_{\text{CPP}_p}\mathbf{\Delta}_{f_p}\mathbf{\Pi}^{l_p}, \tag{6}$$

where $l_p = \frac{\tau_p}{T}$ and $f_p = NT\nu_p$ are the normalized path delay and normalized Doppler shift of the p-th path. Additionally, $l_p \in [0, l_{\max}]$ and $l_{\max}$ is the maximum delay. We define the discrete Doppler shift of the p-th path as $f_p = \alpha_p + \beta_p \in [-f_{\max}, f_{\max}]$, where $f_{\max}$ is the maximum discrete Doppler shift. The term $\alpha_p \in [-\alpha_{\max}, \alpha_{\max}]$ is an integer index, whereas $\beta_p \in (-0.5, 0.5]$ is the fractional component. $\mathbf{\Pi} \in \{0,1\}^{N\times N}$ and $\mathbf{\Delta}_{f_p} = \text{diag}\left(e^{-j2\pi f_p n}, n = 0, \ldots, N-1\right)$ are the forward cyclic-shift matrix and digital frequency shift matrix, respectively. Moreover, $\mathbf{\Gamma}_{\text{CPP}_p} \in \mathbb{C}^{N\times N}$ is the diagonal CPP phase matrix defined as

$$\mathbf{\Gamma}_{\text{CPP}p} = \text{diag}\left(\begin{cases} e^{-j2\pi c_1(N^2-2N(l_p-n))}, & n < l_p \\ 1, & n \geq l_p \end{cases}\right), \tag{7}$$

where $n = 0, \ldots, N-1$. Note that if $2Nc_1$ is an integer and N is even, $\mathbf{\Gamma}_{\text{CPP}p}$ becomes an identity matrix.

The DAF domain received signal $\mathbf{y} \in \mathbb{C}^{N\times 1}$ can be written as

$$\begin{aligned}\mathbf{y} = \mathbf{A}\mathbf{r} &= \sum_{p=1}^{P} h_p \mathbf{A}\mathbf{\Gamma}_{\text{CPP}_p}\mathbf{\Delta}_{f_p}\mathbf{\Pi}^{l_p}\mathbf{A}^H\mathbf{x} + \mathbf{A}\mathbf{w}, \\ &= \mathbf{H}_{\text{eff}}\mathbf{x} + \widetilde{\mathbf{w}},\end{aligned} \tag{8}$$

where $\mathbf{H}_{\text{eff}} \triangleq \mathbf{A}\mathbf{H}\mathbf{A}^H$ is the DAF domain effective channel and $\widetilde{\mathbf{w}} = \mathbf{A}\mathbf{w}$. After obtaining $\mathbf{y}$, by exploiting the MMSE equalizer, the DAF domain received signal is equalized, and estimated information symbol vector $\hat{\mathbf{x}} \in \mathbb{C}^{N\times 1}$ is obtained as

$$\hat{\mathbf{x}} = \mathbf{H}^H_{\text{eff}}\left(\mathbf{H}_{\text{eff}}\mathbf{H}^H_{\text{eff}} + N_0\mathbf{I}_N\right)\mathbf{y}. \tag{9}$$

Finally, a detector is applied to $\hat{\mathbf{x}}$ for decoding the information bits.

B. Acquiring $\mathbf{c}_2$ Parameters

Let us consider that Alice and Bob are communicating with each other through an AFDM system, and there is an eavesdropper, Eve. As illustrated in Fig. 2, since the wireless channel has a reciprocal property, the propagation characteristics of the wireless channel are the same in both directions between Alice and Bob. Reciprocal wireless channels can be exploited to establish a common secret, such as a cryptographic key, without prior coordination or the need for public key exchange. The channel between Alice and Eve (or Bob and Eve) is

This article has been accepted for publication in IEEE Transactions on Vehicular Technology. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TVT.2025.3586731

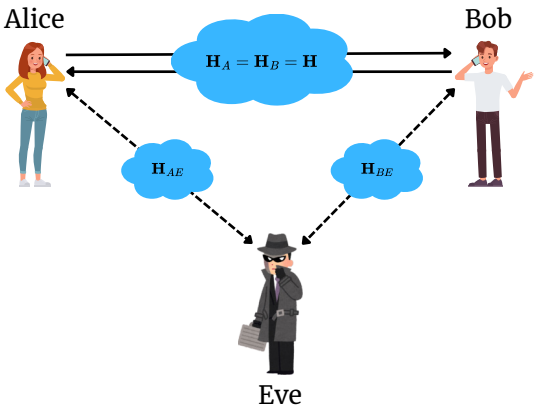

Fig. 2. The reciprocity property of the wireless channel between Alice and Bob. The channels between Alice and Eve ($\mathbf{H}_{\mathrm{AE}}$) and Bob and Eve ($\mathbf{H}_{\mathrm{BE}}$) are fundamentally different from $\mathbf{H}$ due to the distinct physical location of Eve. Also, Eve uses $\mathbf{H}_{\mathrm{AE}}$ or $\mathbf{H}_{\mathrm{BE}}$ to generate its $\mathbf{c}_2$ set.

different from the channel between Alice and Bob because Eve is physically located at a different position. Wireless channels are highly sensitive to spatial changes, meaning even slight differences in Eve's location result in uncorrelated channels.

Moreover, in conventional AFDM systems, there are two main parameters: post-chirp frequency c_1 and pre-chirp frequency c_2. The first chirp frequency c_1 is a key parameter that is carefully optimized based on the statistics of the doubly-selective channel to achieve strong orthogonality of the AFDM subcarriers in the delay-Doppler domain. In contrast, the second chirp frequency c_2 is a more flexible parameter that has negligible influences on the orthogonality of the subcarriers. In order to achieve optimal diversity in the doubly-selective channels with integer Doppler shifts, c_1 must be selected as

$$c_1 = \frac{2f_{\max} + 1}{2N}, \tag{10}$$

and c_2 can be set as a rational number sufficiently smaller than $\frac{1}{2N}$ or any irrational number. However, some studies such as [10] and [14] show that different c_2 values can be used for each subcarrier rather than only a c_2 value for all subcarriers. Taking advantage of this flexibility, we propose a secure AFDM waveform that exploits different c_2 values generated by utilizing the reciprocity property of the wireless channels. We suggest utilizing either the real or imaginary part of the main diagonal elements of the time-domain LTV channel to define the pre-chirp parameter sets to initiate secure transmission. Also, a quantization operation is performed on the real or imaginary coefficients for information reconciliation. These steps are briefly represented in the pre-transmission part of Fig. 1.

In the proposed secure AFDM system, channel sounding is performed as an initial step to estimate the reciprocal wireless channel between Alice and Bob. This phase allows both parties to extract channel characteristics that will be used to derive the $\mathbf{c}_2$, which is the common pre-chirp set. Depending on the coherence time and the bandwidth, sounding signals are sent with each block or every few blocks to maintain fresh channel knowledge for a new $\mathbf{c}_2$ set generation and detection. Specifically, Alice and Bob transmit probing AFDM signals with predefined c_2 parameters, which are processed to estimate

TABLE I
COMPUTATIONAL COMPLEXITY (η^N) OF EVE FOR VARYING N AND η VALUES.

N \ η	4	5	6	7
64	3.403×10^{38}	5.421×10^{44}	6.334×10^{49}	1.220×10^{54}
128	1.158×10^{77}	2.939×10^{89}	4.012×10^{99}	1.488×10^{108}
256	1.341×10^{154}	8.636×10^{178}	1.610×10^{199}	2.214×10^{216}
512	1.798×10^{308}	7.458×10^{357}	2.591×10^{398}	4.900×10^{432}

the LTV channel $\mathbf{H}$. Then, the imperfectly estimated channel $\bar{\mathbf{H}}$ is obtained by Alice or Bob. Since there are reasons for this imperfect estimation, such as noise, $\bar{\mathbf{H}}$ is different than the true channel $\mathbf{H}$. These differences cause mismatches in the pre-chirp parameter sets between Alice and Bob. In order to include imperfect channel estimation effects on the system and examine the results of these mismatches, we use $\bar{\mathbf{H}}$ at the receiver side for equalization and demodulation. For this, instead of h_p, we use

$$\tilde{h}_p = h_p + \epsilon, \; p = 1, \ldots, P \tag{11}$$

in (6), where $\epsilon \sim \mathcal{CN}(0, \sigma_e^2)$ [19]. From these estimates, a feature such as the real or imaginary part of the channel response is extracted and quantized. Since the channel exhibits reciprocity, the quantized values at both Alice and Bob should be highly correlated, enabling them to independently determine a common $\mathbf{c}_2$ without direct exchange of sensitive information.

In the next step, the real parts of the elements in the main diagonal of $\bar{\mathbf{H}}$ is extracted as $\mathbf{h} = [h_1, \ldots, h_n, \ldots, h_N] \in \mathbb{R}^{N \times 1}$ and

$$h_n = \mathcal{R}(\bar{\mathbf{H}}[n, n]), \quad n = 1, \ldots, N. \tag{12}$$

As mentioned earlier, imaginary parts can also be used, yet we have used the real parts here. Afterward, a quantization operation is performed on $\mathbf{h}$. For this operation, step size can be calculated as

$$\alpha = \frac{\rho_{\max} - \rho_{\min}}{\eta - 1}, \tag{13}$$

where $\rho_{\max}$ and $\rho_{\min}$ are the maximum and minimum quantization values, respectively. η is the quantization level. For the n-th element of the $\mathbf{h}_u$, the corresponding quantized chirp vector $\mathbf{c}_2$ is determined using the η-level quantization process as

$$c_{2,n} = \rho_{\min} + \alpha \left\lfloor \frac{h_n - \rho_{\min}}{\alpha} + \frac{1}{2} \right\rfloor, \; n = 1, \ldots, N, \tag{14}$$

Since this $\mathbf{c}_2$ vector is generated using Alice and Bob's common channel, it will be private to Alice and Bob, and Eve cannot obtain it. It can be used in the pre-chirp matrix given in (2b) to establish secure communication over an AFDM system between Alice and Bob. In the quantization process, the coefficients are quantized between η levels. Thus, each $\mathbf{c}_2$ element can take η different values. Therefore, Eve has to generate the pre-chirp matrix and perform demodulation steps for each possible $\mathbf{c}_2$ realization, and there are a total of η^N possible realizations. As shown in Table I, the quantity η^N grows exponentially with both η and N, underscoring the related increase in computational complexity. The system will become computationally secure if the N and η are chosen

This article has been accepted for publication in IEEE Transactions on Vehicular Technology. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TVT.2025.3586731

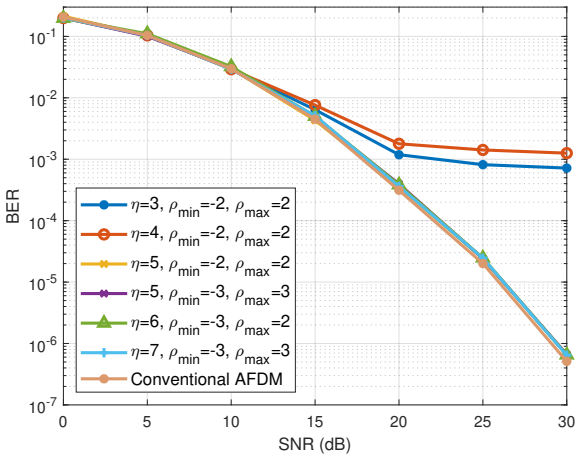

Fig. 3. BER results for varying quantization parameters.

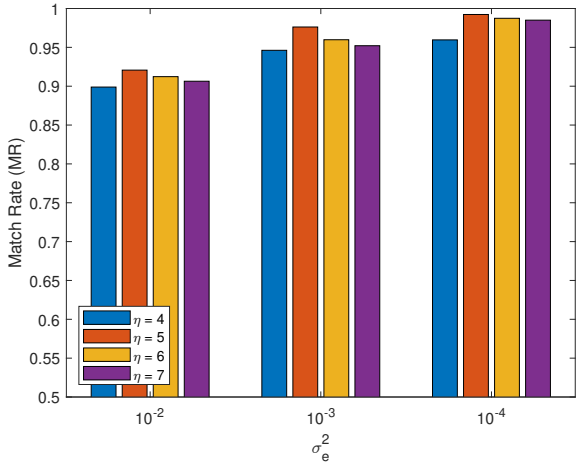

Fig. 4. Match rates for varying η versus channel estimation error variances with $\rho_{\min} = -3$ and $\rho_{\max} = 3$.

large enough. Moreover, since the pre-chirp vector consists of N elements, the whole quantization process involves $3N$ real additions, as well as N real multiplications and divisions.

Furthermore, in our scheme, we only modify the pre-chirp matrix values, which do not affect the subcarriers or frame structure. Consequently, the spectral efficiency of the proposed system remains identical to that of conventional AFDM, which is $\log_2(Q)$ bits/seconds/Hz.

III. Simulation Results

In this section, we show the error performance results of our system obtained by computer simulations. In all simulations, we used $N = 128$ subcarriers. We consider an LTV wireless channel, and the Extended Vehicular A (EVA) model is used as the delay profile [20]. The carrier frequency is $f_c = 4$ GHz, and the subcarrier spacing $\Delta f = 1$ kHz. Each delay path is characterized by a single Doppler shift generated using Jakes' model, $\nu_p = \nu_{\max} \cos(\theta_p)$, where $\nu_{\max}$ is the maximum Doppler shift depending on the user speed, and $\theta_p \sim U(-\pi, \pi)$. The user speed is set at 810 km/h, corresponding to $\nu_{\max} = 1875$ kHz. Pre-chirp parameter c_1 calculated by (10). We define the signal-to-noise ratio (SNR) as $1/N_0$, and QPSK modulation is used. In all conventional AFDM simulations, we set $c_2 = \frac{1}{2N}$ while in the proposed system, we use our specifically generated $\mathbf{c}_2$ set.

In Fig. 3, the error performance of the proposed system with different quantization parameters is given. In this simulation, there is no channel estimation error, $\sigma_e^2 = 0$. When the figure is examined, it is observed that for low η values such as $\eta = 3$ and $\eta = 4$, the error performance of the system approaches the error floor. For higher η values, the system yields results consistent with the classical AFDM system. This situation can be explained by the quantized value being mapped to an incorrect level due to noise when the number of quantization levels is low. Furthermore, we would like to emphasize that higher η values increase the number of possible $\mathbf{c}_2$ realizations.

In order to evaluate the reliability of the proposed reciprocal pre-chirp parameter generation method, we analyze the match rate between the $\mathbf{c}_2$ vectors independently generated by Alice and Bob under channel estimation errors. The match rate measures how often Alice and Bob independently generate the same pre-chirp parameters despite the estimation errors. As

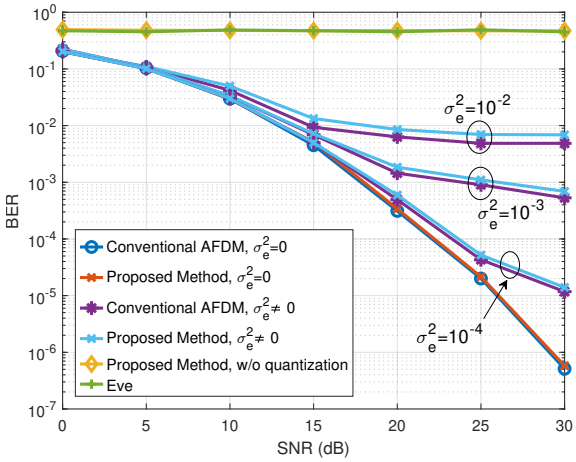

Fig. 5. BER comparison of conventional AFDM and the proposed system under channel estimation error with varying σ_e^2.

shown in Fig. 4, the match rate remains consistently high even at larger estimation error variances when a sufficiently large quantization level η is used. For all η values, the match rate exceeds 90% across all considered σ_e^2 values. This result validates the effectiveness of the quantization step in reconciling minor estimation mismatches and confirms that the system can maintain consistent and secure parameter agreement between legitimate users without requiring additional information exchange. It is also worth mentioning that although the match rates remain high across all η levels, increasing η results in a larger number of possible $\mathbf{c}_2$ combinations. Consequently, Eve must perform significantly more demodulation attempts, which substantially increases her computational burden.

The error performance comparison between the proposed method and the conventional AFDM for varying σ_e^2 values is given in Fig. 5. The quantization parameters are selected as $\eta = 7, \rho_{\min} = -3$ and $\rho_{\max} = 3$. When the results are examined, it is observed that the error performance of the proposed method and the classical AFDM system is similar for different σ_e^2 levels. Thanks to the quantization process, the obtained $\mathbf{c}_2$ sets remain close to optimal even under different noise and channel estimation errors. However, it is seen that the proposed system encounters the worst-case scenario when quantization is not applied. Moreover, since

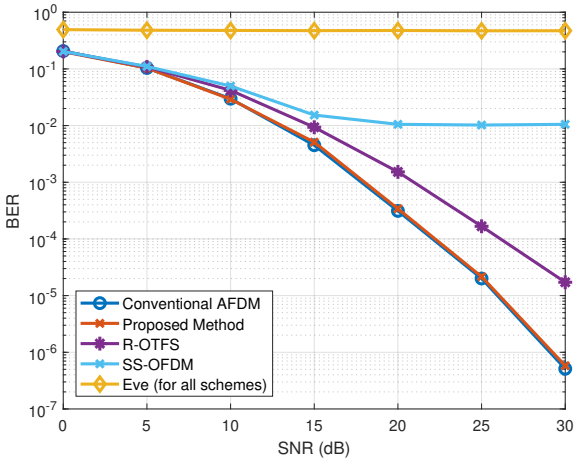

Fig. 6. BER comparison of the proposed system and other schemes proposed in the literature.

Eve cannot access the channel information of Alice and Bob, Eve is unable to generate the correct $\mathbf{c}_2$ set and cannot obtain any information about the transmitted signals. As a result, the BER performance of Eve remains constant at 0.5 across all SNR values. In order to correctly demodulate the transmitted information bits, Eve has to perform 7^{128} distinct demodulation operations, rendering the task computationally infeasible.

In Fig. 6, a comparison of the error performance between the proposed and other methods in the literature is given. In this comparison, we choose R-OTFS proposed in [8] and a subcarrier sorting-based OFDM (SS-OFDM) proposed in [21] as benchmarks. The SS-OFDM system sorts subcarriers by channel quality, sending half of the original bits over the better subcarriers and XOR-ed halves over the poorer ones. For this simulation, the same channel conditions are applied to all schemes. It is assumed there are no channel estimation errors. When we examine the error performance of Eve, it is clear that none of the schemes allow Eve to eavesdrop, as her BER remains at 0.5 for all cases. However, when it comes to the error performance of legitimate users, the proposed method outperforms the others. At a BER level of 10^{-4}, there is approximately a 4 dB SNR gain over the R-OTFS scheme. This gap can be attributed to the matrix inverse-based one-tap equalizer used in R-OTFS, which amplifies noise. As for SS-OFDM, its performance significantly degrades under high mobility due to the nature of OFDM systems, resulting in an error floor around 10^{-2}.

IV. Conclusion

In this study, we have proposed a secure AFDM system leveraging the wireless channel characteristics and inherent properties of AFDM. Specifically, Alice and Bob employ the wireless LTV channel between them to establish a common pre-chirp matrix, which remains unique to their communication link. Consequently, Eve is unable to decode the transmitted signal, even if intercepted over the air. In order to further enhance the system's reliability, a quantization process has been applied to the pre-chirp coefficients. Extensive computer simulations demonstrate that the proposed method achieves comparable error performance to the classical AFDM system under identical channel estimation error variances. Furthermore, our proposed scheme performs well compared to similar benchmark schemes. This confirms that the proposed system ensures secure communication without compromising error performance. These findings position our system as a promising candidate for next-generation wireless systems requiring robust security and reliability. Future research directions include exploring advanced techniques for information reconciliation of $\mathbf{c}_2$ and integrating suitable channel coding methods to further enhance system reliability, particularly in the presence of significant channel estimation errors.

References

[1] W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," *IEEE Netw.*, vol. 34, no. 3, pp. 134–142, 2020.

[2] A. Bemani, N. Ksairi, and M. Kountouris, "Affine frequency division multiplexing for next generation wireless communications," *IEEE Trans. Wireless Commun.*, vol. 22, no. 11, pp. 8214–8229, 2023.

[3] M. S. J. Solaija, S. E. Zegrar, and H. Arslan, "Delay-doppler-based key generation using otfs," *IEEE Wireless Commun. Lett.*, vol. 12, no. 8, pp. 1474–1478, 2023.

[4] U. Saeed *et al.*, "Key generation and secrecy analysis using otfs for tdd systems," *IEEE Trans. Wireless Commun.*, 2024.

[5] J. Chen *et al.*, "A physical encryption scheme for OTFS system," in *Proc. IEEE Int. Conf. Commun. Technol. (ICCT)*, 2022.

[6] W. Liang *et al.*, "Underlying security transmission design for orthogonal time frequency space (OTFS) modulation," *Sensors*, vol. 22, no. 20, 2022.

[7] Q. Deng, Y. Ge, and Z. Ding, "Jamming suppression via resource hopping in high-mobility OTFS-SCMA systems," *IEEE Wireless Commun. Lett.*, vol. 12, no. 12, pp. 2138–2142, 2023.

[8] J. Sun, Z. Wang, and Q. Huang, "Secure precoded orthogonal time frequency space modulation," in *Proc. Int. Conf. Wireless Commun. Signal Process. (WCSP)*, 2021.

[9] Q. Li *et al.*, "Secure precoding design for high-mobility systems with OTFS modulation," *Phys. Commun.*, vol. 61, p. 102179, 2023.

[10] G. Liu *et al.*, "Pre-chirp-domain index modulation for full-diversity affine frequency division multiplexing towards 6g," *IEEE Trans. Wireless Commun.*, 2025, early access.

[11] H. S. Rou *et al.*, "AFDM chirp-permutation-index modulation with quantum-accelerated codebook design," 2024. [Online]. Available: https://arxiv.org/abs/2405.02085

[12] Y. Tao *et al.*, "Affine frequency division multiplexing with index modulation: Full diversity condition, performance analysis, and low-complexity detection," *IEEE J. Sel. Areas Commun.*, vol. 43, no. 4, pp. 1041–1055, 2025.

[13] H. Yuan *et al.*, "Papr reduction with pre-chirp selection for affine frequency division multiplexing," *IEEE Wireless Commun. Lett.*, vol. 14, no. 3, pp. 736–740, 2025.

[14] J. Zhu *et al.*, "A low-complexity range estimation with adjusted affine frequency division multiplexing waveform," 2023. [Online]. Available: https://arxiv.org/abs/2312.11125

[15] H. S. Rou and G. T. F. de Abreu, "Chirp-permuted AFDM for quantum-resilient physical-layer secure communications," 2025. [Online]. Available: https://arxiv.org/abs/2502.03289

[16] Z. Li *et al.*, "A hybrid carrier communication system based on weighted affine Fourier transform," *IEEE Commun. Lett.*, vol. 28, no. 7, pp. 1629–1633, 2024.

[17] Z. Li *et al.*, "Chirp parameter selection for affine frequency division multiplexing with MMSE equalization," *IEEE Trans. Commun.*, 2024, early access.

[18] J. Du *et al.*, "A simplified affine frequency division multiplexing system for high mobility communications," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, 2024.

[19] Y. I. Tek and E. Basar, "Joint delay-Doppler index modulation for orthogonal time frequency space modulation," *IEEE Trans. Commun.*, vol. 72, no. 7, pp. 3985–3993, 2024.

[20] ETSI TS 136 104 V14.3.0, "Evolved Universal Terrestrial Radio Access (E-UTRA); Base Station (BS) radio transmission and reception."

[21] M. Li *et al.*, "Secure transmission algorithm based on subcarrier sorting and XOR operation in OFDM systems," in *Proc. IEEE Int. Conf. Commun. Syst. (ICCS)*, 2018, pp. 147–151.