On the Robustness of AFDM and OTFS Against Passive Eavesdroppers

Vincent Savaux, *Senior Member, IEEE*, Hyeon Seok Rou, *Member, IEEE*, Zeping Sui, *Member, IEEE*, Giuseppe Thadeu Freitas de Abreu, *Senior Member, IEEE*, Zilong Liu, *Senior Member, IEEE*

***Abstract*—We investigate the robustness of affine frequency division multiplexing (AFDM) and orthogonal time frequency space (OTFS) waveforms against passive eavesdroppers performing brute-force demodulation to intercepted signals, under the assumption that eavesdroppers have no knowledge of chirp parameters (in AFDM) or the delay–Doppler grid configuration (in OTFS), such that they must search exhaustively over possible demodulation matrices. Analytical results show that the brute-force complexity scales as $\mathcal{O}(\sqrt{N})$ for OTFS and $\mathcal{O}(N^2)$ for AFDM, where N is the number of subcarriers, indicating that AFDM has superior resilience over OTFS. Simulation results demonstrate that AFDM is capable of preventing reliable demodulation at the eavesdropper side with a bit error rate (BER) of 0.5, while OTFS allows partial signal recovery under equivalent conditions.**

***Index Terms*—AFDM, OTFS, physical layer security, eavesdropper, parameter hopping, robustness.**

I. Introduction

Network security has often been restricted to complex key-based encryption schemes. However, keyless techniques, generally based on the signal-to-interference-plus-noise ratio (SINR) optimization, have recently emerged as promising approaches [1], [2], complementing traditional key-based methods. These methods usually rely on the use of spatial diversity, and relatively few studies address physical layer security (PLS) inherent to the waveform itself. As a parallel development, there has been a growing interest in affine frequency division multiplexing (AFDM) [3], [4] and orthogonal time frequency space (OTFS) [5], [6] over the past few years as two alternatives to orthogonal frequency division multiplexing (OFDM) for next-generation communication systems, as they better cope with doubly dispersive channels [7], [8]. The performance of both modulation schemes has been extensively compared in terms of bit error rate (BER), peak-to-average power ratio (PAPR), and capability of supporting integrated sensing and communication (ISAC) [9], [10], in addition to among other functionalities such as index modulation [11]–[13]. However, their robustness against threats in the context of physical layer (PHY) security remains a largely open topic.

For example, in AFDM, by leveraging permutations over the chirp sequences [14], a novel PHY security approach was presented in [15], which was shown to be virtually perfectly secure even against quantum-accelerated eavesdroppers due to the immense complexity in the combinatorial space. Alternatively, techniques to realize PHY security over the conventional AFDM parameters (usually denoted as c_1 and c_2) are reported in [16]–[19], via parameter hopping of (c_1,c_2). In [16], a pseudo-random sequence is selected for the pre-chirp parameter c_2 from a codebook, whereas in [17], c_2 is securely generated at both the legitimate transmitter and receiver sides based on their common hidden communication channel. In both studies, the security enhancement is based on the parameter c_2 only. Nevertheless, c_1 can also play a crucial role in PLS. In [18], [19], the authors analyzed the range of (c_1,c_2) to guarantee security and then evaluated the robustness of AFDM through simulations only. Similarly, based on the modulation parameters of the OTFS waveform, delay-Doppler precoding was proposed in [20] for enhancing the security of OTFS. However, to the best of our knowledge, beyond methods that improve the PHY security of AFDM and OTFS [16]–[20], no study has evaluated the intrinsic robustness of these waveforms against eavesdropping to date.

Therefore, in this paper, we analyze and compare the robustness of AFDM and OTFS modulations against eavesdroppers attempting to brute-force demodulate the leaked signals they receive from legitimate users. We consider a malicious user who performs blind demodulation by exhaustively testing all the possible modulation parameters, *i.e.* the delay-Doppler grid size (K,L) in OTFS, and the chirp parameters (c_1,c_2) in AFDM, given that the number N of subcarriers is known. We then assess the robustness in terms of the maximum number of attempts an eavesdropper has to perform to demodulate the signal properly, focusing on the parameter c_1. We show that the brute-force complexity of OTFS and AFDM scales as $\mathcal{O}(\sqrt{N})$ and $\mathcal{O}(N^2)$, respectively.

The analysis proves that AFDM is significantly more robust than OTFS against brute-force demodulation, because the chirp parameters (c_1,c_2) are chosen within a continuous subset of $\mathbb{R}^2$. In contrast, the delay-Doppler grid size (K,L) in OTFS corresponds to the limited number of divisors of N. It should be noted that the proposed study may serve as a reference for all parameter hopping-based methods [16]–[18] to assess their robustness, in addition to providing theoretical numerical results. Furthermore, simulation results validate the theoretical developments on the robustness and show the superiority of AFDM over OTFS, showing that the BER of AFDM at the eavesdropper remains flat and undecodable for any SNR range, while it converges to a moderate signal recovery for OTFS, given the same number of demodulation attempts.

The rest of the paper is organized as follows: Section II presents both the AFDM and OTFS signal models, as well as the eavesdropping scenario. The theoretical robustness analysis is developed in Section III. Simulation results are provided in Section IV, and conclusions are drawn in Section V.

II. System Model

This section introduces the signal models of both AFDM and OTFS modulations, with our considered scenarios which involve

V. Savaux is with the Institute of Research and Technology b<>com, 35510 Cesson Sévigné, France (email: vincent.savaux@b-com.com).

H. S. Rou and G. T. F. de Abreu are with the School of Computer Science and Engineering, Constructor University Bremen, Campus Ring 1, 28759 Bremen, Germany (email: [hrou, gabreu]@constructor.university).

Z. Sui and Z. Liu are with the School of Computer Science and Electronics Engineering, University of Essex, Colchester CO4 3SQ, U.K. (email: zeping-sui@outlook.com, zilong.liu@essex.ac.uk). The work of Z. Liu was supported in part by the UK Engineering and Physical Sciences Research Council under Grants EP/X035352/1 ('DRIVE'), EP/Y000986/1 ('SORT'), and EP/Y037243/1 ('REVOL6G'), by the Royal Society under Grants IEC\NSFC\233292 and IES\R1\241212.

legitimate users and eavesdroppers attempting to demodulate the communications of the former.

A. AFDM and OTFS Signals Models

Let us consider a multicarrier AFDM or OTFS signal consisting of N subcarriers. Inspired by [21], [22], both waveforms can be interpreted as a precoded OFDM modulation scheme, whose transmitted signal can be expressed as

$$\mathbf{x} = \boldsymbol{\mathcal{F}}_N^H \mathbf{Q} \mathbf{d}, \tag{1}$$

where the vector $\mathbf{d} \in \mathbb{C}^N$ contains the data randomly taken from a constellation, and the matrix $\boldsymbol{\mathcal{F}}_N^H$ is the IDFT matrix of size $N \times N$ containing the element $\frac{1}{\sqrt{N}} e^{2j\pi \frac{mn}{N}}$ at entry (n,m). Then, the expression of the recoding matrix $\mathbf{Q}$ depends on the considered modulation. For instance, we simply have $\mathbf{Q} = \mathbf{I}_N$ in OFDM. In AFDM, it is given by

$$\mathbf{Q} = \boldsymbol{\mathcal{F}}_N \boldsymbol{\Lambda}_{c_1} \boldsymbol{\mathcal{F}}_N^H \boldsymbol{\Lambda}_{c_2}, \tag{2}$$

where $\boldsymbol{\Lambda}_{c_i} = \text{diag}([e^{2j\pi c_i 0^2}, .., e^{2j\pi c_i (N-1)^2}]) \in \mathbb{C}^{N \times N}$, $i = 1,2$, with $c_1, c_2 \in \mathbb{R}$ the so-called chirp parameters which can be set to achieve full diversity in time and frequency selective channels [3], [7], as described in the following.

In OTFS, the matrix $\mathbf{Q}$ is given by

$$\mathbf{Q} = \boldsymbol{\mathcal{F}}_N (\boldsymbol{\mathcal{F}}_L^H \otimes \mathbf{I}_K), \tag{3}$$

where $K \times L$ is the size of the delay-Doppler grid the data is mapped on. Interestingly, note that in OTFS, the delay-Doppler diversity is directly dependent on K and L, and in turn on N since $N = K \times L$. In contrast, it is related to c_1 and c_2 in AFDM, independently of N.

Omitting the cyclic prefix (CP) or chirp-periodic prefix (CPP) addition and removal, the general input-output relation in SISO systems can be expressed as

$$\mathbf{y} = \underbrace{\sum_{l=0}^{L_c - 1} h_l \boldsymbol{\Delta}_{\theta_l} \boldsymbol{\Pi}^l \mathbf{x}}_{\mathbf{H}\mathbf{x}} + \mathbf{w}, \tag{4}$$

where $\mathbf{y} \in \mathbb{C}^{N \times 1}$ is the vector of the received signal, and $\mathbf{w} \in \mathbb{C}^{N \times 1}$ is the vector of the additive white Gaussian noise with independent and identically distributed samples $w_n \sim \mathbb{C}\mathcal{N}(0, \sigma^2)$. In turn, $\mathbf{H} \in \mathbb{C}^{N \times N}$ is the channel matrix, where h_l is the lth channel path coefficient (possibly null if the channel is sparse), and L_c is the channel length. Moreover, $\boldsymbol{\Delta}_{\theta_l} \in \mathbb{C}^{N \times N}$ is the diagonal matrix containing the samples $e^{2j\pi \frac{\theta_l n}{N}}$, where $\theta_l \in [0, \theta_{\max}]$ is the normalized Doppler shift (integer of fractional component), and $\theta_{\max}$ the maximum normalized Doppler shift. Then, $\boldsymbol{\Pi}$ is the forward cyclic-shift matrix. Note that the full-diversity property of AFDM holds if [3], [7], [23]:

$$\frac{2\theta_{\max} + 1}{2N} \leq c_1, \qquad c_2 << \frac{1}{N}. \tag{5}$$

Furthermore, according to [3], to ensure both proper channel estimation and data transmission, c_1 should satisfy $c_1 < \frac{1}{4L_c}$, which is not proved in this paper for the sake of conciseness. Note that more details on how c_1 should be chosen in the context of PLS can be found in [18], [19].

B. Scenario

We consider a scenario in which base stations (BSs) communicate with legitimate UEs of the network, while malicious eavesdroppers attempt to brute-force demodulate the leaked signals. These signals are assumed to be modulated using AFDM or OTFS, as previously described, and the eavesdropper is aware of the waveform it receives. Note that, even though we consider a cellular system comprising BS and UEs, the model is general enough to be extended to any type of communication, such as cell-free, device-to-device (D2D), vehicular-to-everything (V2X), side link, or multiple-input multiple-output (MIMO) systems.

We deliberately assume a worst-case scenario (from the point of view of the legitimate stakeholders of the network) in which the eavesdropper is synchronized with the leaked signals it receives, and has a perfect knowledge of the channel $\mathbf{H}$ between the transmitter (*e.g.* a BS or a UE) and itself, as well as the number of subcarriers N. Note that this therefore limits CSI-based PHY security approaches [17], which depend on the hidden CSI from the eavesdroppers. It results in the capability of perfect equalization, such that the equalized signal at the eavesdropper can be expressed as:

$$\hat{\mathbf{x}} = \mathbf{G}\mathbf{y} = \mathbf{x} + \mathbf{G}\mathbf{w}, \tag{6}$$

where $\mathbf{G} \in \mathbb{C}^{N \times N}$ is the equalization matrix such as $\mathbf{G}\mathbf{H} = \mathbf{I}_N$.

The demodulator then performs data recovery expressed as $\hat{\mathbf{d}} = \mathbf{Q}^{-1} \boldsymbol{\mathcal{F}}_N \hat{\mathbf{x}}$. In contrast, it is assumed that the modulation parameters (*i.e.* c_1 and c_2 in AFDM, and K and L in OTFS), and in turn the decoding matrix $\mathbf{Q}^{-1}$, are unknown to the eavesdropper. Consequently, a brute-force demodulation strategy is adopted to estimate the transmitted data $\mathbf{d}$, which means that it exhaustively tests all the possible values of the modulation parameters until it recovers the data. Despite the exhaustive search may seem to be an oversimplified method, it is optimal in the sense of the maximum likelihood in blind estimation of unknown parameters. In the following, we analyze the robustness of OTFS and AFDM against such a brute-force demodulation.

III. Robustness Analysis

In this section, we evaluate the robustness of the OTFS and AFDM modulation schemes in terms of the maximum number of attempts, denoted by M_a, that an eavesdropper should carry out to recover the transmitted data $\hat{\mathbf{d}}$ from $\hat{\mathbf{x}}$ in (6). It is worth emphasizing that we assess the robustness of the waveforms, independently of additional secure methods as presented in [16]–[20], or independently of any other techniques that aim to secure the transmission at the data level, *e.g.* by applying a pseudo-random matrix to $\mathbf{d}$ directly. Since we focus on the robustness of the waveform against brute-force demodulation, we can deliberately omit the noise in this section, *i.e.* $\mathbf{w} \to \mathbf{0}$ in (6). In other words, M_a corresponds to the maximum attempts the eavesdropper should make to find the decoding matrix $\mathbf{Q}'^{-1}$ such as $\mathbf{Q}'^{-1}\mathbf{Q} = \mathbf{I}_N$, with a probability of 1, given that N is known. The larger the number M_a, the stronger the waveform.

A. OTFS

In OTFS, the brute-force strategy consists in testing all the possible decoding matrices $\mathbf{Q}^{-1}$ according to K (or L equivalently), and keep the set of matrices $\mathbf{Q}'^{-1}$ (parametrized by (K', L')) leading to $\mathbf{Q}'^{-1}\mathbf{Q} = \mathbf{I}_N$. The robustness of OTFS is given in Proposition 1.

Proposition 1. *Given an OTFS signal composed of N subcarriers and parametrized by (K, L), its robustness against brute-force demodulation is given by*

$$M_a = \sigma(N) \leq 2\sqrt{N}, \tag{7}$$

where $\sigma(N)$ is the number of integer divisors of N.

Proof. Note that this result is a direct consequence of the so-called Dirichlet divisor problem, whose more precise upper bounds can be found in [24]. First, we can readily show from (3) that the solution to $\mathbf{Q'}^{-1}\mathbf{Q}=\mathbf{I}_N$ is unique and is given by $(K',L')=(K,L)$. Thus, the number of attempts performed by an eavesdropper directly depends on the number of integer divisors of $N=K\times L$, due to the rectangular delay-Doppler grid structure of OTFS. Then, since the number of divisors of N is twice the number of divisors of N between 1 and $\sqrt{N}$, M_a can be upper-bounded by $2\sqrt{N}$, which concludes the proof. □

We deduce from (7) that the robustness of OTFS exhibits an inverse quadratic growth with respect to the number of subcarriers, which then becomes weak for low N values. Furthermore, in practice, M_a in (7) largely overestimates the possible number of solutions for $\mathbf{Q}^{-1}$ because: i) we know from Dirichlet that the average number of divisors $\sigma(N)$ of N is rather asymptotically equal to $\ln(N)+2\gamma-1\leq 2\sqrt{N}$, where γ is the Euler-Mascheroni constant i.e., $M_a=2\sqrt{N}$ is a loose upper bound, and ii) we know from [15] that only a subset of all possible values (K,L) should be considered to guarantee delay-Doppler diversity (*e.g.* we know that if $K=1$, OTFS is exactly equivalent to OFDM).

B. AFDM

In AFDM, the brute-force demodulation involves an exhaustive joint search of (c_1,c_2) in a continuous subset $\Omega_c\in\mathbb{R}^2$, which is theoretically impractical within a reasonable time. In fact, M_a tends to infinity due to the continuous nature of Ω_c. However, it can be assumed that the brute-force demodulation is made possible regardless of a small error $(c_1+\Delta_1,c_2+\Delta_2)$. Then, M_a becomes finite and corresponds to the ratio of the area defined by Ω_c and the area $(2\cdot|\Delta_1|\times 2\cdot|\Delta_2|)$ (more details are provided in Theorem 1 below). More precisely, M_a depends on whether c_1 and c_2 can be tested independently or not. In a pure blind demodulation process, c_1 and c_2 must be tested together, and then $M_a=M_{c_1}\cdot M_{c_2}$, where M_{c_1} and M_{c_2} are the maximum numbers of attempts an eavesdropper should carry out to reach $c_1\pm|\Delta_1|$ (resp. $c_2\pm|\Delta_2|$) given that c_2 is known (resp. c_1 is known). In a scenario where c_1 and c_2 can be tested sequentially (*e.g.*, if the constellation is known then the samples of $\mathbf{\Lambda}_{c_2}\mathbf{d}$ appears as rotated constellation elements given that c_1 is tested correctly), then $M_a=M_{c_1}+M_{c_2}$.

An overall analysis of PLS in AFDM based on jointly (c_1,c_2) design should be undertaken. However, despite not being extensive, interesting PLS solutions based on c_2 in AFDM have already been proposed in [16]–[19]. In contrast, to the best of our knowledge, no study on c_1 has been proposed to date. In general, an error on c_1 prevents the possible demodulation, even in a sequential test of c_1 and c_2. Thus, c_1 is the most limiting parameter in the exhaustive search of (c_1,c_2) allowing for a brute-force demodulation by an eavesdropper. For this reason, we focus on the robustness of AFDM with respect to (w.r.t.) c_1 in this paper. It can be considered as a preliminary result for a more general study involving both c_1 and c_2.

To evaluate M_{c_1}, we characterize the distance between c_1 and a given value c_1' tested by the eavesdropper, resulting in the failure of demodulation. To this end, the eavesdropper should arbitrarily restrict the possible range of c_1' as $c_1'\in[D_{\min},D_{\max}]$, where $D_{\min}=\frac{2\theta_{\max}+1}{2N}$ according to the full-diversity condition in (5), and $\frac{2\theta_{\max}+1}{2N}<D_{\max}\leq\frac{1}{4L_c}$. In practice, from the eavesdropper perspective, the lower the value of $D_{\max}$, the lower the complexity, with the risk of missing the actual c_1 value. Then, we express the robustness of AFDM in Theorem 1.

Theorem 1. *Let us consider an AFDM signal composed of N subcarriers and parametrized by (c_1,c_2). Given that c_2 is known or can be tested sequentially after c_1, the robustness of AFDM w.r.t. c_1 against brute-force demodulation is given by*

$$M_{c_1}=\frac{\pi}{2N}\big(2ND_{\max}-(2\theta_{\max}-1)\big)(N-1)^2. \tag{8}$$

Proof. First, we express the samples x_n of $\mathbf{x}$ in (1) for any $n=0,1,N-1$ as

$$x_n=\frac{1}{\sqrt{N}}\sum_{m=0}^{N-1}d_m e^{2j\pi(c_1n^2+c_2m^2+\frac{mn}{N})}, \tag{9}$$

where m is the subcarrier index, and d_m is the mth element of the vector $\mathbf{d}$.

By assuming that the eavesdropper attempts to brute force the received AFDM signal using (c_1',c_2'), the sample $\hat{d}_k$ of $\hat{\mathbf{d}}$, $k=0,1,..,N-1$, is given by the DAFT of x_n as

$$\hat{d}_k=\frac{1}{\sqrt{N}}\sum_{n=0}^{N-1}x_n e^{-2j\pi(c_1'n^2+c_2'k^2+\frac{kn}{N})}. \tag{10}$$

Then, by substituting (9) into (10), and defining $\Delta_1=c_1-c_1'$ and $\Delta_2=c_2-c_2'$, we obtain:

$$\begin{aligned}\hat{d}_k&=\frac{1}{N}\sum_{n=0}^{N-1}\sum_{m=0}^{N-1}d_m e^{2j\pi((c_1-c_1')n^2+c_2m^2-c_2'k^2+\frac{(m-k)n}{N})} \\ &=\frac{e^{2j\pi\Delta_2k^2}}{N}\sum_{m=0}^{N-1}d_m e^{2j\pi c_2(m^2-k^2)}\overbrace{\sum_{n=0}^{N-1}e^{2j\pi(\Delta_1n^2+\frac{(m-k)n}{N})}}^{S_1},\end{aligned} \tag{11}$$

where S_1 is defined for clarity.

It must be noted that S_1 simplifies only for integer Δ_1 values, since it reduces to the sum of the Nth roots of unity. In that case $S_1=N\delta_{m,k}$ where $\delta_{m,k}$ is the Kronecker delta, and hence $\hat{d}_k=e^{2j\pi\Delta_2k^2}d_k$, where the term $e^{2j\pi\Delta_2k^2}$ corresponds to a phase rotation, which could be tested afterward. However, the equality $S_1=N\delta_{m,k}$ corresponds to either the perfect match $c_1'=c_1$, which is unattainable because c_1 is a continuous variable, or $\Delta_1\in\mathbb{N}^*$ and then $c_1'\notin[\frac{2\theta_{\max}+1}{2N},D_{\max}]$, which is inconsistent with the assumption $c_1'\in[\frac{2\theta_{\max}+1}{2N},D_{\max}]$. Despite the equality $c_1'=c_1$ (*i.e.* $\Delta_1=0$) cannot theoretically be achieved, the eavesdropper can demodulate the received signal with an acceptable error $|\Delta_1|<<1$, which can be characterized by:

$$\left|e^{2j\pi\Delta_1n^2}-1\right|\leq|\varepsilon|, \tag{12}$$

where $|\varepsilon|<<1$ highlights the acceptable error level, depending on other modulation parameters, but not dealt with in this paper (*e.g.* we can reasonably assume that $|\varepsilon|$ can take a higher value for a low modulation and coding schemes (MCS) than high MCS). Since (12) should hold for any $n=0,1,..,N-1$, and $\Delta_1<<1$, we use the series expansion of the exponential function to derive the upper bound of Δ_1 with $n=N-1$ as

$$(12)\Leftrightarrow|\Delta_1|\leq\frac{|\varepsilon|}{2\pi(N-1)^2}\leq\frac{1}{2\pi(N-1)^2}, \tag{13}$$

TABLE I
BRUTE-FORCE DEMODULATION COMPLEXITY OF DIFFERENT WAVEFORMS BY AN EAVESDROPPER.

Waveform	**Complexity**	
	Attempts	Demodulation
OFDM	1	$\mathcal{O}(N\log N)$
OTFS	$\sigma(N)$	$\mathcal{O}(KL\log L)$
AFDM	$M_{c_1}.M_{c_2}$ or $M_{c_1}+M_{c_2}$	$\mathcal{O}(N\log N)$

where "1" can replace $|\varepsilon|$ to obtain an upper bound that only depends on N.

Notice that in this case, the demodulated data becomes $\hat{d}_k = e^{2j\pi\Delta_2 k^2} d_k(1+\varepsilon)$. In AFDM, the brute-force strategy w.r.t. c_1 then consists in testing all possible values c_1' within $[\frac{2\theta_{\max}+1}{2N}, D_{\max}]$ with a step of $2|\Delta_1| = \frac{1}{\pi(N-1)^2}$. Then, the maximum number of attempts M_{c_1} corresponds to the ratio of the range of the search set $[\frac{2\theta_{\max}+1}{2N}, D_{\max}]$ and the step $2|\Delta_1|$, leading to (8), which concludes the proof. □

We deduce from (8) that the robustness of AFDM is quadratically proportional to the number of subcarriers N and also linearly proportional to the size of the search set through $D_{\max}$. Thus, AFDM should be much stronger than OTFS against passive eavesdroppers, therefore limiting a brute-force demodulation of a leaked signal in real-time. The complexity order of brute-force demodulation in OFDM, OTFS, and AFDM is summarized in Table I. It is expressed in terms of the number of attempts and the corresponding flops for demodulation per attempt. Unlike OTFS, M_{c_1} in (8) is independent of chirp parameters c_1 and c_2, hence AFDM achieves both robustness against eavesdroppers and full delay-Doppler diversity. Furthermore, note that c_2 must also be dechirped on top of c_1 in AFDM to complete the demodulation, thus strengthening the waveform, as addressed in [16]–[18].

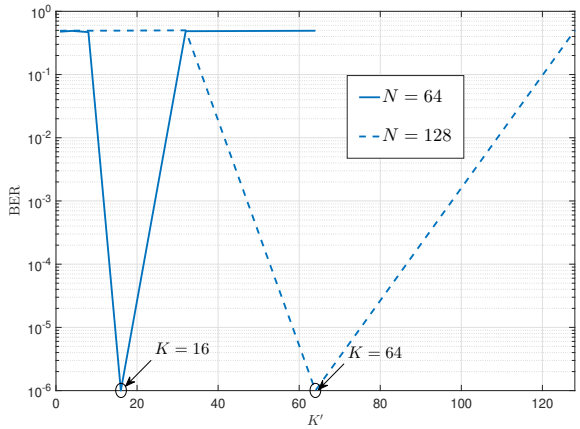
IV. SIMULATION RESULTS

In this section, we validate the theoretically derived results through simulations and we evaluate the performance of the AFDM and OTFS waveforms in terms of the achievable BER at the eavesdropper. The parameters used in all simulations are summarized in Table II. Simulations have been performed using MATLAB, and the results have been averaged over at least 10^3 independent Monte-Carlo runs.

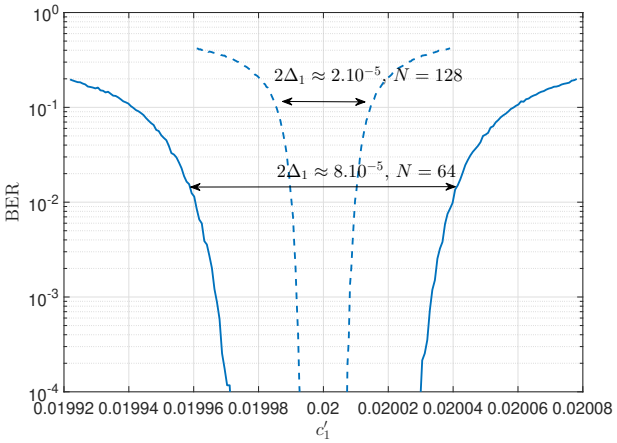
Fig. 1 shows the BER versus the demodulation parameters K' in OTFS (a), and c_1' in AFDM (b), for $N \in \{64, 128\}$ and $K \in \{16, 64\}$, and in an additive white Gaussian noise (AWGN) environment such as SNR$=25$ dB. In Fig. 1(a), the OTFS parameter K is set to $K=16$. The cardinality of the set to be tested by the eavesdropper to properly demodulate the OTFS signal is $\sigma(\{64,128\})=\{7,8\}$. We observe that the only solution that minimizes the BER is $K'=K$, which confirms the weakness of OTFS against brute-force demodulation. We assume

TABLE II
SIMULATION PARAMETERS.

Parameter	**Value**
Modulation	QPSK
N	$\{64,128\}$
(c_1,c_2)	$(0.02,10^{-3})$
L_c	4
$\theta_{\max}$	0.3
h_l (Eq. (4))	$\mathcal{CN}(0,\sigma_h^2=\frac{1}{4})$
$D_{\max}$	0.1



(a) BER versus K' in OTFS, for $N=\{64,128\}$ and $K=\{16,64\}$. It can be observed that the BER is minimum for $K'=K$.



(b) AFDM BER versus c_1' for $N=\{64,128\}$ and $c_1=0.02$. It can be observed that the value of Δ_1 matches the theoretical one.

Fig. 1. BER versus demodulation parameters K' in (a) OTFS and (b) c_1' in AFDM, for $N=\{64,128\}$, where we set SNR=25 dB and QPSK modulation.

that the eavesdropper *a priori* knows c_2 or can properly estimate this pre-chirp parameter, so it is omitted in the simulations.

Thus, it focuses on brute-force demodulation by testing c_1' values. The range of c_1' values has been arbitrarily restricted around $c_1 \pm 8.10^{-5}$ in Fig. 1(b) for the sake of clarity. We can observe that the BER reaches a minimum value that spans over $2\Delta_1$ defined in (13). Moreover, other series of simulations show that: i) no other local minimum is achieved when c_1' varies in a wider range of values, and ii) the BER variations become sharper as the constellation size increases. This validates the analysis leading to the upper-bound in (13) and in turn (8).

To further validate the robustness analysis, Fig. 2 shows the BER versus SNR (dB) achieved at the eavesdropper for OFDM, AFDM, and OTFS modulations, using $N = 128$ subcarriers. A four-tap channel (see parameters in Table II) is considered, which is equalized at the receiver side using the MMSE equalizer, before the brute-force demodulation. To compare OTFS and AFDM against brute-force demodulation, we assume that the eavesdropper can test $M_a=\sigma(128)=8$ values of K' in OTFS, and in AFDM, it can test 8 (same attempts number as OTFS) and 10^4 different c_1' values. The BER of OFDM, considering only 1 attempt, is also shown as a benchmark. In AFDM, c_1'

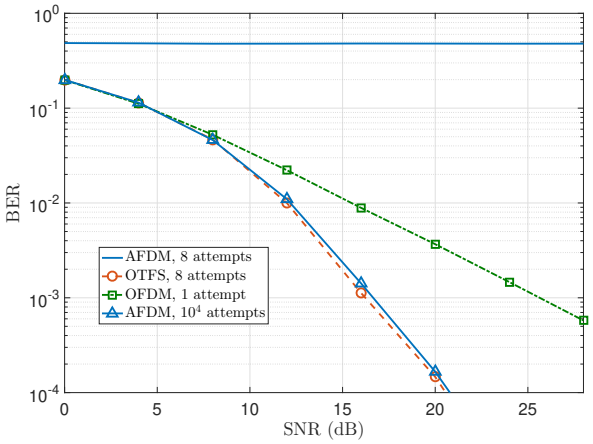


Fig. 2. BER versus SNR (dB) achieved at eavesdropper considering OFDM (1 attempt), OTFS (8 attempts), and AFDM (8 and 10^4 attempts), with $N=128$ in multipath channel.

is randomly chosen within the set $[\frac{\theta_{\max}}{N},0.1]$, with a minimum spacing of $2\Delta_1$ between two attempts.

It can be observed that the BER of OFDM (1 attempt), OTFS (8 attempts), and AFDM (10^4 attempts) decreases to zero when the SNR increases, validating that the exhaustive possible values of K' and c_1', respectively, work well. It implies that the eavesdropper can demodulate the OTFS and AFDM signals. Moreover, both OTFS and AFDM outperform OFDM, since they are more robust than OFDM against a doubly dispersive channel. In contrast, the BER of AFDM using 8 attempts keeps a value of about 0.5, which shows that 8 attempts are largely insufficient to brute-force demodulate the AFDM signal. This ultimately proves that AFDM is much stronger than OTFS against passive eavesdropping.

V. Conclusion

We investigated the robustness of both AFDM and OTFS modulations against eavesdropping, in terms of the maximum number of attempts required for a passive eavesdropper to demodulate the signals via brute-force search, in the absence of any additional PLS method. It was shown that, for a signal composed of N subcarriers, the corresponding complexity scales as $\mathcal{O}(\sqrt{N})$ and $\mathcal{O}(N^2)$ for OTFS and AFDM, respectively. This result is due to the nature of the modulation parameters: in OTFS, the delay-Doppler size (K,L) is chosen within the divisors of N, whereas in AFDM, the chirp parameters (c_1,c_2) are selected within a continuous subset of $\mathbb{R}^2$. The analysis, which can also be used to assess the robustness performance of PLS techniques in AFDM and OTFS, indicates that AFDM has an advantage over OTFS in terms of privacy. Simulation results validated the theoretical analysis through the BER, which showed that AFDM significantly outperforms OTFS in terms of PHY security.

References

[1] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and Applications of Physical Layer Security Techniques for Confidentiality: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, p. 1773–1828, Secondquarter 2019.

[2] D. Wang, B. Bai, W. Zhao, and Z. Han, "A Survey of Optimization Approaches for Wireless Physical Layer Security," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1878–1911, 2019.

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

[4] H. S. Rou, K. R. R. Ranasinghe, V. Savaux, G. T. F. de Abreu, D. G. G., and C. Masouros, "Affine Frequency Division Multiplexing (AFDM) for 6G: Properties, Features, and Challenges," 2025. [Online]. Available: https://arxiv.org/abs/2507.21704

[5] Z. Wei, W. Yuan, S. Li, J. Yuan, G. Bharatula, R. Hadani, and L. Hanzo, "Orthogonal time-frequency space modulation: A promising next-generation waveform," *IEEE wireless communications*, vol. 28, no. 4, pp. 136–144, 2021.

[6] R. Hadani, S. Rakib, M. Tsatsanis, A. Monk, A. J. Goldsmith, A. F. Molisch, and R. Calderbank, "Orthogonal Time Frequency Space Modulation," in *proc of 2017 IEEE Wireless Communications and Networking Conference (WCNC)*, March 2017, pp. 1–6.

[7] H. S. Rou *et al.*, "From Orthogonal Time–Frequency Space to Affine Frequency-Division Multiplexing: A comparative study of next-generation waveforms for integrated sensing and communications in doubly dispersive channels," *IEEE Signal Processing Magazine*, vol. 41, no. 5, pp. 71–86, September 2024.

[8] Z. Sui *et al.*, "Multi-functional chirp signalling for next-generation multi-carrier wireless networks: Communications, sensing and ISAC perspectives," *arXiv preprint arXiv:2508.06022*, 2025.

[9] W. Yuan, Z. Wei, S. Li, R. Schober, and G. Caire, "Orthogonal time frequency space modulation—Part III: ISAC and potential applications," *IEEE Communications Letters*, vol. 27, no. 1, pp. 14–18, 2022.

[10] K. R. R. Ranasinghe, H. S. Rou, G. T. F. De Abreu, T. Takahashi, and K. Ito, "Joint channel, data and radar parameter estimation for AFDM systems in doubly-dispersive channels," *IEEE Transactions on Wireless Communications*, 2024.

[11] Z. Sui, Z. Liu, L. Musavian, L.-L. Yang, and L. Hanzo, "Generalized spatial modulation aided affine frequency division multiplexing," *IEEE Transactions on Wireless Communications*, pp. 1–1, 2025.

[12] Z. Sui, H. Zhang, Y. Xin, T. Bao, L.-L. Yang, and L. Hanzo, "Low Complexity Detection of Spatial Modulation Aided OTFS in Doubly-Selective Channels," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 10, pp. 13 746–13 751, 2023.

[13] H. S. Rou, K. Yukiyoshi, T. Mikuriya, G. T. F. De Abreu, and N. Ishikawa, "AFDM chirp-permutation-index modulation with quantum-accelerated codebook design," in *2024 58th Asilomar Conference on Signals, Systems, and Computers*. IEEE, 2024, pp. 817–821.

[14] H. S. Rou and G. T. F. de Abreu, "Chirp-permuted AFDM: A new degree of freedom for next-generation versatile waveform design," *arXiv preprint arXiv:2507.20825*, 2025.

[15] ——, "Chirp-Permuted AFDM: A Versatile Waveform Design for ISAC in 6G," 2025. [Online]. Available: https://arxiv.org/abs/2507.20825

[16] P. Wang, Z. Wang, Y. Ma, X. Tian, and Y. Ni, "A Secure Affine Frequency Division Multiplexing for Wireless Communication Systems," in *Proc. IEEE ICC*, 2025, pp. 2701–2706.

[17] Y. I. Tek and E. Basar, "A Novel and Secure AFDM System for High Mobility Environments," *IEEE Transactions on Vehicular Technology*, pp. 1–6, 2025.

[18] H. Chen *et al.*, "Chirp Parameters Hopping over Time for Affine Frequency Division Multiplexing with Physical Layer Security," in *Proc. IEEE ICC*, 2025, pp. 2120–2125.

[19] D. Zhang, Z. Wang, Y. Tang, D. Wu, and M. Yuan, "Parameter Design for Secure Affine Frequency Division Multiplexing Waveform," 2025. [Online]. Available: https://arxiv.org/abs/2503.19364

[20] Q. Liu, Q. Xu, C. Li, Z. Wei, X. Yang, and L. Wang, "Secure OTFS Transmission via Joint Delay-Doppler Precoding and Time-Domain Noise Injection," in *Proc. IEEE ICCC*, August 2024, pp. 569–574.

[21] A. A. Boudjelal, R. Y. Bir, and H. Arslan, "Toward a Common Transceiver Framework for 6G: Orthogonal Coexistence and Structural Unification of DFT Waveforms," *IEEE Transactions on Communications*, pp. 1–15, 2025.

[22] V. Savaux, S. Sawadogo, H. S. Rou, and G. T. F. de Abreu, "On the Noise Robustness of Affine Frequency Division Multiplexing: Analysis and Applications," 2025. [Online]. Available: https://arxiv.org/abs/2510.03901

[23] A. Bemani, N. Ksairi, and M. Kountouris, "AFDM: A Full Diversity Next Generation Waveform for High Mobility Communications," in *Proc. IEEE ICC*, 2021, pp. 1–6.

[24] M. N. Huxley, "Exponential sums and lattice points III," *Proceedings of the London Mathematical Society*, vol. 87, no. 3, pp. 591–609, 2003. [Online]. Available: https://londmathsoc.onlinelibrary.wiley.com/doi/abs/10.1112/S0024611503014485