creative commons

COMMONS DEED

저작자표시-비영리-변경금지 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.

다음과 같은 조건을 따라야 합니다:

저작자표시. 귀하는 원저작자를 표시하여야 합니다.

비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.

변경금지. 귀하는 이 저작물을 개작, 변형 또는 가공할 수 없습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 이용허락규약(Legal Code)을 이해하기 쉽게 요약한 것입니다.

Disclaimer

dCollection

ULSAN NATIONAL INSTITUTE OF
SCIENCE AND TECHNOLOGY

Master’s Thesis

Secure Precoding for
Future Wireless Communication Systems

Mintaek Oh

Department of Electrical Engineering

Ulsan National Institute of Science and Technology

2023

Secure Precoding for
Future Wireless Communication Systems

Mintaek Oh

Department of Electrical Engineering

Ulsan National Institute of Science and Technology

ULSAN NATIONAL INSTITUTE OF
SCIENCE AND TECHNOLOGY

Secure Precoding for Future Wireless Communication Systems

A thesis/dissertation submitted to
Ulsan National Institute of Science and Technology
in partial fulfillment of the
requirements for the degree of
Master of Science

Mintaek Oh

05.23.2023 of submission
Approved by

Sung W. Yoon

Advisor
Sung Whan Yoon

ULSAN NATIONAL INSTITUTE OF
SCIENCE AND TECHNOLOGY

Secure Precoding for
Future Wireless Communication Systems

Mintaek Oh

This certifies that the thesis/dissertation of Mintaek Oh is approved.

05.23.2023 of submission

Signature

Advisor: Sung Whan Yoon

Signature

Jinseok Choi

Signature

Hyoil Kim

ULSAN NATIONAL INSTITUTE OF
SCIENCE AND TECHNOLOGY

Abstract

Physical layer security has emerged a flourishing strategy to protect confidential information from eavesdroppers with lower computational complexity compared to cryptography. Secure precoding is a promising transmission method of physical layer security to improve security by exploiting an intrinsic attribute of wireless communications. The main goal of the secure precoding is to maximize secrecy rate in multi-input and multi-output (MIMO) systems with the presence of eavesdroppers. Unfortunately, there exists no optimal solution, and also solving the secrecy rate maximization problem becomes more challenging as networks involve a multi-user (MU) and multi-eavesdropper (ME) scenario because of its non-smoothness and non-convexity. In this thesis, I proposed a novel secure precoding algorithm for downlink MU-MIMO systems under ME threat to enhance the secrecy rate, and provide subsequent analyses for realizing ultra-reliable low latency communications (URLLC). By incorporating strong security, communication reliability, and latency, a multi-objective optimization problem is investigated in the finite blocklength (FBL) regime. The derived optimization problem aims to maximize the secrecy rate by designing a secure precoder, while simultaneously minimizing both the maximum error probability and the rate of information leakage. The proposed FBL-based optimization algorithm provides the significantly improved tradeoff among the security, the error probability, and information leakage rate. Therefore, the proposed algorithms can offer significantly improved security for future wireless communication systems.

ULSAN NATIONAL INSTITUTE OF
SCIENCE AND TECHNOLOGY

ULSAN NATIONAL INSTITUTE OF
SCIENCE AND TECHNOLOGY

Contents

ULSAN NATIONAL INSTITUTE OF
SCIENCE AND TECHNOLOGY

List of Figures

ULSAN NATIONAL INSTITUTE OF SCIENCE AND TECHNOLOGY

I Introduction

This introductory chapter briefly overviews the background and motivation in this thesis. Section 1.1 and Section 1.2 presents the background and related work in terms of physical layer security such as secure precoding in the finite blocklength regime regarding ultra-reliable low latency communication. Section 1.3 provides the motivation of the proposed research. Section 1.4 summarizes the contributions of the proposed research. The notations are put together in Section 1.5.

1.1 Background

In the forthcoming B5G and 6G communications eras, wireless networks are anticipated to become more increasingly complex and diversified due to the vast number of communication devices. Owing to the broadcast nature of wireless communications, which makes them susceptible to eavesdropping, the significance of security has been gaining attention [1]. In this regard, physical layer security has been considered as a promising solution for enhancing private information security [2]. Especially, the physical layer security has been thriving because of its reduced computational complexity in contrast to cryptography approaches [3]. The maximum secure communication rate, known as the secrecy rate, has been defined as the rate at which information can be securely and reliably transmitted over a wiretap channel [4]. As the volume of transmitted information and the variety of wireless applications grow rapidly, the significance of information security has become increasingly crucial. Consequently, numerous efforts have been made to implement physical layer security to maximize the secrecy rate in 6G applications. In physical layer security, secure precoding is the notable method for addressing the secrecy rate maximization challenge in multiple-input multiple-output (MIMO) systems.

Extension to delay-sensitive and mission-critical applications such as internet-of-things (IoT) and unmanned aerial vehicle (UAV), ultra-reliable low latency communications (URLLC) is the primary requirement of 6G communications [5]. In terms of the latency, a short-packet transmission is often considered to support real-time communications [6]. To this end, the networks take account into finite blocklength (FBL) regime, which are better suited for harnessing the advantages of transmitting brief data packets. However, in contrast to traditional communication systems, the FBL-based communication systems result in diminished performance due to the presence of a back-off factor entangled with the secrecy rate. According to [7], the back-off factor in the FBL regime is determined by blocklength and non-negligible decoding error probability. Incorporating the back-off factor caused by eavesdropping, the secrecy rate over a wiretap channel in the FBL regime was derived in [8]. In other words, information leakage rate entangled in the back-off factor is now non-negligible and affects the security performance due to the FBL as well as wiretap channels.

1.2 Related Work

The field of physical layer security has been thoroughly explored in various contexts. Beginning with Wyner's groundbreaking research [3]. Specifically, numerous endeavors have been made to as-

ULSAN NATIONAL INSTITUTE OF SCIENCE AND TECHNOLOGY

sess the secrecy rate of multi-antenna systems using an information-theoretic methodology [9–11]. To achieve the theoretical secrecy rate region, secret dirty-paper coding (S-DPC) was derived in [12]. In the study presented in [13], it was demonstrated that linear precoding is capable of achieving the equivalent secrecy rate region as that of S-DPC. Numerous previous studies have proposed secure precoding techniques aimed at optimizing the secrecy rate. In [14], a successive convex approximation approach was introduced to alleviate the challenges of maximizing the total secrecy rate. To examine both the secrecy rate and secrecy energy efficiency concurrently, extensive research has been conducted on massive MIMO systems [15], and systems that facilitate simultaneous wireless information and power transfer [16].

The artificial noise (AN) injection strategy is a notable method for attaining secure communication in MIMO systems [17]. Specifically, an AN design centered around the null-space of the legitimate channel matrix is a widely-recognized technique for optimizing the overall secrecy rate [18]. In the context of a multi-user (MU), multi-eavesdropper (ME) network, a secure transmission approach by injecting AN investigated to maximize the secrecy rate so that signal leakage from wiretap channels is mitigated [19]. In addition, by employing the alternating optimization method [15], the power ratio between the secure precoder and the AN covariance matrix was fine-tuned. To find the local optimal solution, in [20], the two-level optimization framework was proposed to investigate AN-assisted secure communication design, utilizing the fixed zero-forcing (ZF) precoding approach. In [21], the optimization method jointly designing the secure precoding and AN under sources and relay transmit power constraints was derived.

Recent research has explored physical layer security in the FBL regime [8]. Based on the essential findings concerning the secrecy rate with the finite coding length, it has been observed that tradeoffs exist among delay, reliability, and security. As a result, further exploration of wireless communication techniques is necessary to enhance the secrecy rate within the FBL regime [22]. To identify the optimal tradeoff, cutting-edge precoding techniques have been proposed to boost the secrecy rate while adhering to reliability and security constraints [23]. In [24], the performance of FBL-based communications with an eavesdropper present was examined, and the optimal blocklength for maximizing secrecy throughput was analyzed by employing AN-assisted maximum ratio transmission (MRT) precoding. In the previous work [25], an efficient secure precoding algorithm was proposed for downlink communications with multiple users and a single eavesdropper considering the FBL regime.

1.3 Motivation

Regarding the URLLC, the previous studies investigated the FBL-based secure precoding algorithms to extremely reduce the latency and improve the reliability of wireless communications. However, the most works have considered the limited communication scenarios such as a single-eavesdropper case, and proposed secure transmission strategies maximizing the secrecy rate based on the conventional linear precoders [24, 26]. In [27, 28], the linear precoding was also investigated to secure networks in non-orthogonal multiple access (NOMA) systems. Additionally, the existing secure precoding techniques are applied to rate splitting multiple access (RSMA) [29, 30] with the presence of wiretap channels. In [31], an outage probability that takes into account both reliability and security was introduced, reflecting the properties of secure communications based on the finite blocklength framework. While previous research has examined secure communication within the FBL regime, it has predominantly focused on scenarios involving a single eavesdropper. Furthermore, these studies have offered theoretical analyses and attempted to maximize achievable secrecy rates using traditional linear precoding techniques. Nevertheless, a comprehensive optimization of FBL-based secure communication, taking into account both reliability and security constraints for complex multi-user, multi-eavesdropper MIMO networks, has yet to be explored. Addressing the optimization problem for such intricate networks is a formidable task. It is worth noting that the sum secrecy rate optimization issue is already non-convex and hard to solve, as evidenced by [32], and the interplay between back-off factors and secrecy rates only adds to the challenge [8]. Moreover, directly finding solutions for multiple objectives is unfeasible [33]. To overcome these challenges, I propose a novel secure precoding technique that achieves an optimal balance among rate, reliability, and security within the FBL regime.

1.4 Thesis Summary

In summary, I have contributed to secure precoding designs and algorithm development by applying the FBL regime. In this thesis, the main contributions are summarized as follows:

- In the FBL-based communication systems, this study prioritizes the secrecy rate as the primary performance criterion. By employing the secrecy rate, the research develops a comprehensive secrecy rate maximization problem aimed at concurrently optimizing 1) the precoder, and 2) the balance between error probability and information leakage rate. However, several obstacles emerge when attempting to resolve the formulated optimization problem. First and foremost, the issue is inherently non-convex, rendering the pursuit of a globally optimal solution impractical. Secondly, the proposed problem encompasses multi-objective optimization, wherein each user faces error probability and information leakage constraints dictated by the system's reliability requirements. Thirdly, the secrecy rate becomes unwieldy due to back-off factors that are determined by interrelated optimization variables. Finally, the overall secrecy rate is non-smooth, as the secrecy rate relies on the maximum wiretap channel rate in situations involving multiple eavesdroppers.

- To address the previously mentioned obstacles, this study adopts a two-phase alternating optimization strategy, consisting of 1) maximizing the secrecy rate via precoding design, and 2) minimizing the maximum error probability and information leakage rate. In the first phase, with given error probability and leakage rate, a smooth approximation is utilized for the non-smooth objective function. This allows for a more manageable problem by setting a lower bound for the secrecy rate. Due to the problem's non-convex nature, a first-order optimality condition is derived, which can be construed as a generalized eigenvalue problem. This facilitates the identification of the optimal local precoder through its principal eigenvector, which can be solved using a power iteration-based precoding technique. In the second phase, the multi-objective optimization problem is transformed into a single-objective optimization problem by employing a weighted-sum method for a given precoder. However, as the problem remains intractable due to the maximum function in the secrecy rate, the lower bound of the objective function is further considered. The optimization of the maximum error probability and information leakage rate is achieved by solving the Karush-Kuhn-Tucker (KKT) conditions.

- Simulations are conducted to verify the reliability and security performance of the recommended joint optimization methods. The findings reveal that, in comparison to baseline techniques, the proposed algorithm achieves the highest secrecy rate while ensuring the lowest maximum error probability and information leakage rate across various scenarios. As a result, it can be concluded that the proposed algorithms provide substantial benefits for FBL-based secure communications, satisfying the rigorous reliability and security demands of upcoming advanced wireless applications.

1.5 Notation

This thesis uses the following notation: $\mathbf{A}$ is a matrix, $\mathbf{a}$ is a column vector, and $\mathscr{A}$ is a set. The superscripts $(\cdot)^{\mathsf{T}}$, $(\cdot)^{\mathsf{H}}$, and $(\cdot)^{-1}$ denote the transpose, Hermitian, and matrix inversion, respectively. $\mathbb{E}[\cdot]$ represents an expectation operator. $\mathbf{0}$ is a matrix that has all zeros in its elements with a proper dimension. The blackboard bold symbols $\mathbb{C}$, $\mathbb{R}_{+}$, and $\mathbb{N}_{+}$ denote the complex, nonnegative real, and nonnegative integer domains, respectively. $\mathbf{I}_N$ is the identity matrix with size $N \times N$. Assuming that $\mathbf{A}_1, \ldots, \mathbf{A}_N \in \mathbb{C}^{K\times K}$, $\mathbf{A} = \mathrm{blkdiag}\left(\mathbf{A}_1, \ldots, \mathbf{A}_N\right) \in \mathbb{C}^{KN\times KN}$ is a block diagonal matrix. $|\cdot|$ indicates an absolute value, and $\|\mathbf{A}\|$ represents ℓ_2 norm. I use $\mathrm{tr}(\cdot)$ for trace operator, $\mathrm{vec}(\cdot)$ for vectorization, and $\mathscr{U}\left(a, b\right)$ to denote a uniform distribution with two boundaries a and b. The MATLAB style notation is used.

ULSAN NATIONAL INSTITUTE OF SCIENCE AND TECHNOLOGY

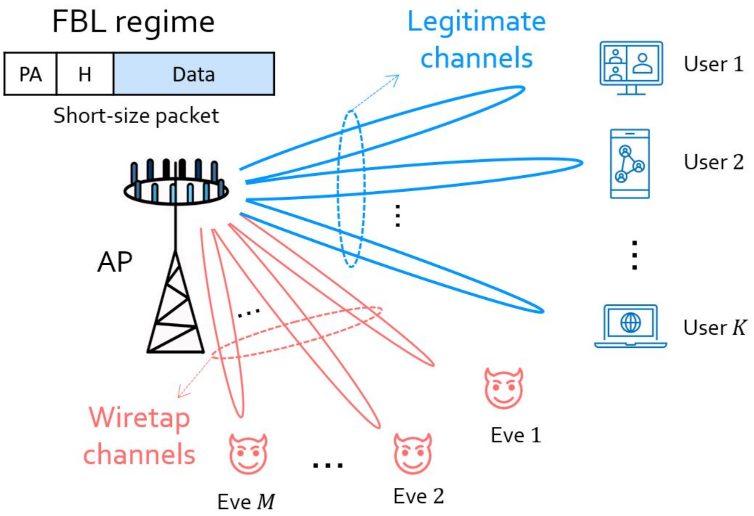


Figure 1: MU-MIMO network with wiretap channels in FBL regime

II FBL-Based Joint Optimization in MU-MIMO Wiretap Channels

2.1 Introduction

In this chapter[1], a joint optimization algorithm is proposed to consider secure and reliable communications in the FBL regime for downlink MU-MIMO systems where multiple eavesdroppers coexist. The sum secrecy rate in the FBL regime is adopted as a key metric which has back-off factor determined by non-negligible decoding error probability and information leakage rate; thereby the problem is multi-objective optimization. The alternating solution reveals that the proposed optimization algorithm provides significantly improved tradeoff among the security, the error probability, and information leakage rate.

2.2 System Model

As shown in Fig. 1, I consider a downlink network in which an access point (AP) equipped with N antennas serves K single-antenna users. The network includes M single-antenna eavesdroppers who attempt to overhear legitimate user messages. In addition, I assume the FBL channel coding, i.e., the coding length is $L \ll \infty$. I denote a user set and an eavesdropper set as $\mathscr{K} = \{1,\cdots,K\}$ and $\mathscr{M} = \{1,\cdots,M\}$, respectively. The data symbol for user k, s_k, is drawn from a Gaussian distribution with a zero mean and variance of $\mathbb{E}[|s_k|^2] = P$, $\forall k \in \mathscr{K}$. The AP broadcasts the data symbols $s_k, \forall k \in \mathscr{K}$ to each legitimate user through a linear precoder $\mathbf{F} = [\mathbf{f}_1,\ldots,\mathbf{f}_K] \in \mathbb{C}^{N\times K}$, where $\mathbf{f}_k \in \mathbb{C}^N$ indicates a

[1] This section is based of the research published in the jornal papaer: M. Oh, J. Park, and J. Choi, "Joint Optimization for Secure and Reliable Communications in Finite Blocklength Regime," in *IEEE Transactions on Wireless Communications*, early access, 2023.

precoding vector for s_k. Then a transmitted signal vector $\mathbf{x} \in \mathbb{C}^N$ is

$$\mathbf{x} = \sum_{k=1}^{K} \mathbf{f}_k s_k = \mathbf{F}\mathbf{s}, \tag{1}$$

where $\mathbf{s} = [s_1, \ldots, s_K]^\mathsf{T} \in \mathbb{C}^K$.

After transmission, the signal received by user k can be expressed as

$$y_k = \mathbf{h}_k^\mathsf{H} \mathbf{f}_k s_k + \sum_{\ell \neq k, \ell=1}^{K} \mathbf{h}_k^\mathsf{H} \mathbf{f}_\ell s_\ell + n_k, \tag{2}$$

where n_k denotes the AWGN noise at user k characterized by zero mean and a variance of σ^2. Additionally, $\mathbf{h}_k \in \mathbb{C}^N$ represents the channel fading vector between the AP and user k, defined as

$$\mathbf{h}_k = \sqrt{\gamma_k} \tilde{\mathbf{h}}_k \tag{3}$$

Here, γ_k and $\tilde{\mathbf{h}}_k$ symbolize the large-scale and small-scale channel fading factors between the AP and user k, respectively. Correspondingly, the channel fading vector from the AP to eavesdropper m is denoted by $\mathbf{g}_m \in \mathbb{C}^N$. This vector incorporates both large-scale and small-scale channel fading components, represented as γ_m^e and $\tilde{\mathbf{g}}_m$, respectively.

$$\mathbf{g}_m = \sqrt{\gamma_m^\mathsf{e}} \tilde{\mathbf{g}}_m. \tag{4}$$

Then, the received signal at eavesdropper m is

$$y_m^\mathsf{e} = \sum_{\ell=1}^{K} \mathbf{g}_m^\mathsf{H} \mathbf{f}_\ell s_\ell + n_m^\mathsf{e}, \tag{5}$$

where n_m^e is the AWGN noise at the eavesdropper m with a zero mean and variance of σ_e^2. In this system model, it is also assumed that the AP has the perfect channel state information at the transmitter (CSIT) for both the legitimate users and eavesdroppers. Further, this analysis is extended to consider a scenario with only partial CSIT.

2.3 Problem Formulation

In this section, I introduce performance metrics that incorporate the effect of FBL in the considered communication system. The achievable rate of user k is

$$R_k = \log_2 (1 + \rho_k), \tag{6}$$

where ρ_k is the SINR of user k defined as

$$\rho_k = \frac{|\mathbf{h}_k^\mathsf{H} \mathbf{f}_k|^2}{\sum_{\ell \neq k, \ell=1}^{K} |\mathbf{h}_k^\mathsf{H} \mathbf{f}_\ell|^2 + \sigma^2 / P}. \tag{7}$$

The achievable rate of eavesdropper m for s_k is

$$R_{m,k}^\mathsf{e} = \log_2 \left(1 + \rho_{m,k}^\mathsf{e}\right), \tag{8}$$

where $\rho^{\mathsf{e}}_{m,k}$ is the SINR of eavesdropper m for s_k defined as

$$\rho^{\mathsf{e}}_{m,k} = \frac{|\mathbf{g}_m^{\mathsf{H}}\mathbf{f}_k|^2}{\sum_{\ell\neq k,\ell=1}^{K}|\mathbf{g}_m^{\mathsf{H}}\mathbf{f}_\ell|^2 + \sigma_{\mathsf{e}}^2/P}. \tag{9}$$

In [8, 34], the secrecy rate, which measures the maximum rate transmission of confidential information that any eavesdropper cannot decode in the FBL regime, is given as

$$R_k^{\mathsf{sec}}(\mathbf{f}_k,\varepsilon_k,\delta_{m,k};L) = R_k - \sqrt{\frac{\mathscr{V}_k}{L}}Q^{-1}(\varepsilon_k) - \max_{m\in\mathscr{M}}\left\{R^{\mathsf{e}}_{m,k} + \sqrt{\frac{\mathscr{V}^{\mathsf{e}}_{m,k}}{L}}Q^{-1}\left(\delta_{m,k}\right)\right\}, \tag{10}$$

where $\mathscr{V}^{\mathsf{e}}_{m,k}$ and $\mathscr{V}k$ are channel dispersion factors that depend on the stochastic variations of the legitimate and wiretap channels, respectively [7, 8]. In addition, $Q^{-1}(\cdot)$ represents an inverse Q-function defined as $Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^\infty e^{\frac{t^2}{2}}dt$, ε_k is the decoding error probability of user k, and $\delta_{m,k}$ is the secrecy constraint on the information leakage of s_k from eavesdropper m [8]. It is important to note that if the blocklength L approaches infinity, the secrecy rate in (10) becomes sufficiently close to the classic secrecy SE. Therefore, the back-off factors in (10), i.e., $\sqrt{\frac{\mathscr{V}_k}{L}}Q^{-1}(\varepsilon_k)$ and $\sqrt{\frac{\mathscr{V}^{\mathsf{e}}_{m,k}}{L}}Q^{-1}\left(\delta_{m,k}\right)$, act as drawbacks that reduce the secrecy rate in the FBL regime.

Considering an interference channel where transmitters use an independent and identically distributed (i.i.d.) Gaussian codebook and receivers employ nearest-neighbor decoding [35,36], the channel dispersion factors become

$$\mathscr{V}_k = \mathscr{V}^{\text{i.i.d.}}(\rho_k) = \frac{2\rho_k}{1+\rho_k}\left(\log_2 e\right)^2, \tag{11}$$

$$\mathscr{V}^{\mathsf{e}}_{m,k} = \mathscr{V}^{\text{i.i.d.}}(\rho^{\mathsf{e}}_{m,k}) = \frac{2\rho^{\mathsf{e}}_{m,k}}{1+\rho^{\mathsf{e}}_{m,k}}\left(\log_2 e\right)^2. \tag{12}$$

Now, I let the predetermined maximum error probability and information leakage constraints as $\hat{\varepsilon}_k$ and $\hat{\delta}_{m,k}, \forall k \in \mathscr{K}, \forall m \in \mathscr{M}$, respectively. Defining $\bar{\varepsilon} = [\varepsilon_1,\cdots,\varepsilon_K]^{\mathsf{T}} \in \mathbb{R}_+^K$ and $\Delta = [\bar{\delta}_1,\cdots,\bar{\delta}_K] \in \mathbb{R}_+^{M\times K}$, where $\bar{\delta}_k = [\delta_{1,k},\cdots,\delta_{M,k}]^{\mathsf{T}} \in \mathbb{R}_+^M, \forall k \in \mathscr{K}$, I formulate a joint optimization problem to maximize the sum secrecy rate and to minimize the maximum error probability and information leakage rate as

$$\underset{\mathbf{F},\bar{\varepsilon},\Delta}{\text{maximize}} \;\; R^{\mathsf{sec}}_{\mathsf{sum}}(\mathbf{F},\bar{\varepsilon},\Delta;L) = \sum_{k=1}^{K} R_k^{\mathsf{sec}} \tag{13}$$

$$\underset{\bar{\varepsilon}}{\text{minimize}} \;\; \max\{\varepsilon_1,\cdots,\varepsilon_K\} \tag{14}$$

$$\underset{\Delta}{\text{minimize}} \;\; \max\{\delta_{1,1},\cdots,\delta_{M,K}\} \tag{15}$$

$$\text{subject to } \; \mathrm{tr}\left(\mathbf{F}\mathbf{F}^{\mathsf{H}}\right) \leq 1, \tag{16}$$

$$\varepsilon_k \leq \hat{\varepsilon}_k, \; \forall k \in \mathscr{K}, \tag{17}$$

$$\delta_{m,k} \leq \hat{\delta}_{m,k}, \; \forall m \in \mathscr{M}, \forall k \in \mathscr{K}, \tag{18}$$

where (14) and (15) are the error probability and information leakage rate constraints, and (16) is a transmit power constraint at the AP, respectively. The main challenges in addressing the optimization problem include: 1) the multi-objective nature of the problem, 2) the intractability of the objective function in (13) due to the non-smooth maximum function, 3) the inherent non-convexity of the problem, and 4) the necessity to consider decoding error probability and information leakage in the constraints, which are closely related to the secrecy rate as back-off factor parameters. A viable approach for tackling the multi-objective problem entails investigating a set of solutions, where each solution achieves the objectives at an acceptable level without being outperformed by any other alternative [37]. As a result, I propose a joint optimization method that effectively addresses the multi-objective challenge while maintaining a reasonable tradeoff.

2.4 Alternating Optimization Framework

In this section, I introduce a new optimization technique to tackle the problem defined in (13) by utilizing an alternating optimization strategy. I initially derive the secure precoder that maximizes the sum secrecy rate, considering given decoding error probability and information leakage rate. Subsequently, I address the minimization problem concerning the maximum error probability and information leakage rate for the acquired precoder.

A. Phase I: Best Secure Precoding Direction

During this phase, the goal is to identify the optimal precoder that enhances the sum secrecy rate, with fixed ε_k and $\delta_{m,k}$, $\forall k \in \mathcal{K}, \forall m \in \mathcal{M}$. Given the non-smooth nature of the objective function in (13), it becomes essential to smooth (10) for achieving a more manageable form. To facilitate this, I initially employ a LogSumExp approach [38] as an approximation to the maximum function, using a parameter α as

$$\max_{i=1,\cdots,N}\{x_i\} \approx \frac{1}{\alpha}\ln\left(\sum_{i=1}^{N}\exp(x_i\alpha)\right), \tag{19}$$

where the approximation becomes tight as $\alpha \to \infty$. Applying (19) to (10), I have

$$\begin{aligned}
&\max_{m\in\mathcal{M}}\left\{R^{\mathsf{e}}_{m,k}+\sqrt{\frac{\mathcal{V}^{\mathsf{e}}_{m,k}}{L}}Q^{-1}(\delta_{m,k})\log_2 e\right\} && (20)\\
&\approx \frac{1}{\alpha}\ln\left[\sum_{m=1}^{M}\exp\left(\alpha R^{\mathsf{e}}_{m,k}+\alpha\sqrt{\frac{2\rho^{\mathsf{e}}_{m,k}}{L(1+\rho^{\mathsf{e}}_{m,k})}}Q^{-1}(\delta_{m,k})\log_2 e\right)\right]\\
&= \frac{1}{\alpha}\ln\left[\sum_{m=1}^{M}(1+\rho^{\mathsf{e}}_{m,k})^{\frac{\alpha}{\ln 2}}\exp\left(\frac{\alpha}{\ln 2}\sqrt{\frac{2\rho^{\mathsf{e}}_{m,k}}{L(1+\rho^{\mathsf{e}}_{m,k})}}Q^{-1}(\delta_{m,k})\right)\right]\\
&= \tilde{R}^{\mathsf{e}}_{k}. && (21)
\end{aligned}$$

Now, I introduce the following lemma [33]:

Lemma 1 *For any given x, $\tilde{x} > 0$, an upper bound of $\sqrt{2x/(1+x)}$ is obtained as*

$$\sqrt{\frac{2x}{1+x}} \le q(\tilde{x})\ln(1+x)+r(\tilde{x}), \tag{22}$$

where $q(\tilde{x}) = \frac{1}{\sqrt{2\tilde{x}(1+\tilde{x})}}$ and $r(\tilde{x}) = \sqrt{\frac{2\tilde{x}}{1+\tilde{x}}} - q(\tilde{x})\ln(1+\tilde{x})$.

ULSAN NATIONAL INSTITUTE OF SCIENCE AND TECHNOLOGY

Proof 1 *Refer to the proof of Lemma 2 in [33].*

Based on Lemma 1 with (21), I can obtain the lower bound of the approximated secrecy rate. For given $\tilde{\rho}_k$ and $\tilde{\rho}^{\mathsf{e}}_{m,k}$, the lower bound of (10) is obtained as

$$\begin{aligned} R_k^{\mathsf{sec}} &\overset{(a)}{\approx} R_k - \sqrt{\frac{2\rho_k}{L(1+\rho_k)}} Q^{-1}(\varepsilon_k)\log_2 e - \tilde{R}_k^{\mathsf{e}} \qquad (23)\\ &\overset{(b)}{\geq} \log_2(1+\rho_k) - \frac{Q^{-1}(\varepsilon_k)}{\sqrt{L}} q(\tilde{\rho}_k)\ln(1+\rho_k)\log_2 e - \psi_k \\ &\quad - \frac{1}{\alpha}\ln\left\{\sum_{m=1}^{M}(1+\rho^{\mathsf{e}}_{m,k})^{\frac{\alpha}{\ln 2}}\exp\left(\ln(1+\rho^{\mathsf{e}}_{m,k})^{\frac{\alpha Q^{-1}(\delta_{m,k})q(\tilde{\rho}^{\mathsf{e}}_{m,k})}{\sqrt{L}\ln 2}} + \alpha\psi^{\mathsf{e}}_{m,k}\right)\right\} \\ &= \log_2(1+\rho_k)^{\omega_k} - \psi_k - \frac{1}{\alpha}\ln\left\{\sum_{m=1}^{M}\beta_{m,k}(1+\rho^{\mathsf{e}}_{m,k})^{\omega^{\mathsf{e}}_{m,k}}\right\} \\ &= R_k^{\mathsf{sec,lb}}, \qquad (24) \end{aligned}$$

where (a) comes from (21), (b) follows from Lemma 1, and

$$\begin{aligned} &\psi_k = \frac{Q^{-1}(\varepsilon_k)\log_2 e}{\sqrt{L}} r(\tilde{\rho}_k),\ \psi^{\mathsf{e}}_{m,k} = \frac{Q^{-1}(\delta_{m,k})\log_2 e}{\sqrt{L}} r(\tilde{\rho}^{\mathsf{e}}_{m,k}), \\ &\omega_k = 1 - \frac{Q^{-1}(\varepsilon_k)}{\sqrt{L}} q(\tilde{\rho}_k),\ \omega^{\mathsf{e}}_{m,k} = \frac{\alpha}{\ln 2}\left(1 + \frac{Q^{-1}(\delta_{m,k})}{\sqrt{L}} q(\tilde{\rho}^{\mathsf{e}}_{m,k})\right), \\ &\beta_{m,k} = \exp\left(\alpha\psi^{\mathsf{e}}_{m,k}\right). \end{aligned}$$

Since I pursue to solve (13) for given $\bar{\varepsilon}$ and Δ with the lower bound in (24), myproblem is transformed to the single-objective maximization problem as

$$\underset{\mathbf{F}}{\text{maximize}} \ \sum_{k=1}^{K} R_k^{\mathsf{sec,lb}}(\mathbf{F}) \qquad (25)$$

$$\text{subject to } \ \text{tr}\left(\mathbf{F}\mathbf{F}^{\mathsf{H}}\right) \leq 1. \qquad (26)$$

Next, to further obtain a compact rate expression with respect to the precoder, I vectorize the precoding matrix as

$$\bar{\mathbf{f}} = \text{vec}(\mathbf{F}) = \left[\mathbf{f}_1^{\top}, \mathbf{f}_2^{\top}, \ldots, \mathbf{f}_K^{\top}\right]^{\top} \in \mathbb{C}^{NK}. \qquad (27)$$

It has been observed in previous works on secrecy rate that, in general, increasing the transmit power improves the secrecy rate [39]. Additionally, it is evident that the channel capacity increases with the transmit power for a given channel coding blocklength. In this regard, I set $||\bar{\mathbf{f}}||^2 = 1$, i.e., transmission with the maximum power to maximize the secrecy rate. Consequently, I can reformulate the problem in (25) as the product of Rayleigh quotients as

$$\underset{\bar{\mathbf{f}}}{\text{maximize}} \ \sum_{k=1}^{K}\log_2\left(\frac{\bar{\mathbf{f}}^{\mathsf{H}}\mathbf{A}_k\bar{\mathbf{f}}}{\bar{\mathbf{f}}^{\mathsf{H}}\mathbf{B}_k\bar{\mathbf{f}}}\right)^{\omega_k} - \ln\left\{\sum_{m=1}^{M}\beta_{m,k}\left(\frac{\bar{\mathbf{f}}^{\mathsf{H}}\mathbf{C}_m\bar{\mathbf{f}}}{\bar{\mathbf{f}}^{\mathsf{H}}\mathbf{D}_{m,k}\bar{\mathbf{f}}}\right)^{\omega^{\mathsf{e}}_{m,k}}\right\}^{\frac{1}{\alpha}}, \qquad (28)$$

where

$$\mathbf{A}_k = \text{blkdiag}\left(\mathbf{h}_k\mathbf{h}_k^{\mathsf{H}}, \cdots, \mathbf{h}_k\mathbf{h}_k^{\mathsf{H}}\right) + \mathbf{I}_{NK}\frac{\sigma^2}{P} \in \mathbb{C}^{NK \times NK}, \tag{29}$$

$$\mathbf{B}_k = \mathbf{A}_k - \text{blkdiag}(\mathbf{0}, \cdots, \underbrace{\mathbf{h}_k\mathbf{h}_k^{\mathsf{H}}}_{k\text{th block}}, \cdots, \mathbf{0}) \in \mathbb{C}^{NK \times NK}, \tag{30}$$

$$\mathbf{C}_m = \text{blkdiag}\left(\mathbf{g}_m\mathbf{g}_m^{\mathsf{H}}, \cdots, \mathbf{g}_m\mathbf{g}_m^{\mathsf{H}}\right) + \mathbf{I}_{NK}\frac{\sigma_{\mathsf{e}}^2}{P} \in \mathbb{C}^{NK \times NK}, \tag{31}$$

$$\mathbf{D}_{m,k} = \mathbf{C}_m - \text{blkdiag}(\mathbf{0}, \cdots, \underbrace{\mathbf{g}_m\mathbf{g}_m^{\mathsf{H}}}_{k\text{th block}}, \cdots, \mathbf{0}) \in \mathbb{C}^{NK \times NK}. \tag{32}$$

The second terms in both (30) and (32) have non-zero blocks, which are located at the kth diagonal block. It is important to note that the product of Rayleigh quotient forms in (28) is derived under the assumption $\|\bar{\mathbf{f}}\| = 1$, and the problem in (28) remains invariant up to the scaling of $\bar{\mathbf{f}}$. As a result, the power constraint in (26) is eliminated in the reformulated problem.

Now, I focus on identifying the local points of the problem in (28). For simplicity, I define the objective function in (28) as

$$\mathscr{L}_1(\bar{\mathbf{f}}) = \log_2 \prod_{k=1}^{K} \left[\left(\frac{\bar{\mathbf{f}}^{\mathsf{H}}\mathbf{A}_k\bar{\mathbf{f}}}{\bar{\mathbf{f}}^{\mathsf{H}}\mathbf{B}_k\bar{\mathbf{f}}} \right)^{\omega_k} \left\{ \sum_{m=1}^{M} \beta_{m,k} \left(\frac{\bar{\mathbf{f}}^{\mathsf{H}}\mathbf{C}_m\bar{\mathbf{f}}}{\bar{\mathbf{f}}^{\mathsf{H}}\mathbf{D}_{m,k}\bar{\mathbf{f}}} \right)^{\omega_{m,k}^{\mathsf{e}}} \right\}^{-\frac{\ln 2}{\alpha}} \right] \tag{33}$$

$$= \log_2 \lambda(\bar{\mathbf{f}}). \tag{34}$$

Then, I derive Lemma 2 to find the condition of stationary points of (33).

Lemma 2 *The first-order KKT condition of the problem* (28) *is satisfied if*

$$\mathbf{B}_{\mathsf{KKT}}^{-1}(\bar{\mathbf{f}})\mathbf{A}_{\mathsf{KKT}}(\bar{\mathbf{f}})\bar{\mathbf{f}} = \lambda(\bar{\mathbf{f}})\bar{\mathbf{f}}, \tag{35}$$

where

$$\mathbf{A}_{\mathsf{KKT}}(\bar{\mathbf{f}}) = \lambda_{\mathsf{num}}(\bar{\mathbf{f}}) \sum_{k=1}^{K} \left[\frac{\omega_k}{\ln 2} \left(\frac{\mathbf{A}_k}{\bar{\mathbf{f}}^{\mathsf{H}}\mathbf{A}_k\bar{\mathbf{f}}} \right) + \frac{1}{\alpha} \sum_{m=1}^{M} \left(\frac{\omega_{m,k}^{\mathsf{e}}\beta_{m,k} \left(\frac{\bar{\mathbf{f}}^{\mathsf{H}}\mathbf{C}_m\bar{\mathbf{f}}}{\bar{\mathbf{f}}^{\mathsf{H}}\mathbf{D}_{m,k}\bar{\mathbf{f}}} \right)^{\omega_{m,k}^{\mathsf{e}}} \frac{\mathbf{D}_{m,k}}{\bar{\mathbf{f}}^{\mathsf{H}}\mathbf{D}_{m,k}\bar{\mathbf{f}}}}{\sum_{\ell=1}^{M} \beta_{m,k} \left(\frac{\bar{\mathbf{f}}^{\mathsf{H}}\mathbf{C}_\ell\bar{\mathbf{f}}}{\bar{\mathbf{f}}^{\mathsf{H}}\mathbf{D}_{\ell,k}\bar{\mathbf{f}}} \right)^{\omega_{\ell,k}^{\mathsf{e}}}} \right) \right], \tag{36}$$

$$\mathbf{B}_{\mathsf{KKT}}(\bar{\mathbf{f}}) = \lambda_{\mathsf{den}}(\bar{\mathbf{f}}) \sum_{k=1}^{K} \left[\frac{\omega_k}{\ln 2} \left(\frac{\mathbf{B}_k}{\bar{\mathbf{f}}^{\mathsf{H}}\mathbf{B}_k\bar{\mathbf{f}}} \right) + \frac{1}{\alpha} \sum_{m=1}^{M} \left(\frac{\omega_{m,k}^{\mathsf{e}}\beta_{m,k} \left(\frac{\bar{\mathbf{f}}^{\mathsf{H}}\mathbf{C}_m\bar{\mathbf{f}}}{\bar{\mathbf{f}}^{\mathsf{H}}\mathbf{D}_{m,k}\bar{\mathbf{f}}} \right)^{\omega_{m,k}^{\mathsf{e}}} \frac{\mathbf{C}_m}{\bar{\mathbf{f}}^{\mathsf{H}}\mathbf{C}_m\bar{\mathbf{f}}}}{\sum_{\ell=1}^{M} \beta_{m,k} \left(\frac{\bar{\mathbf{f}}^{\mathsf{H}}\mathbf{C}_\ell\bar{\mathbf{f}}}{\bar{\mathbf{f}}^{\mathsf{H}}\mathbf{D}_{\ell,k}\bar{\mathbf{f}}} \right)^{\omega_{\ell,k}^{\mathsf{e}}}} \right) \right], \tag{37}$$

$$\lambda_{\mathsf{num}}(\bar{\mathbf{f}}) = \prod_{k=1}^{K} \left(\frac{\bar{\mathbf{f}}^{\mathsf{H}}\mathbf{A}_k\bar{\mathbf{f}}}{\bar{\mathbf{f}}^{\mathsf{H}}\mathbf{B}_k\bar{\mathbf{f}}} \right)^{\omega_k}, \tag{38}$$

$$\lambda_{\mathsf{den}}(\bar{\mathbf{f}}) = \prod_{k=1}^{K} \left\{ \sum_{m=1}^{M} \beta_{m,k} \left(\frac{\bar{\mathbf{f}}^{\mathsf{H}}\mathbf{C}_m\bar{\mathbf{f}}}{\bar{\mathbf{f}}^{\mathsf{H}}\mathbf{D}_{m,k}\bar{\mathbf{f}}} \right)^{\omega_{m,k}^{\mathsf{e}}} \right\}^{\frac{\ln 2}{\alpha}}. \tag{39}$$

Proof 2 *I first define the Lagrangian function of the problem* (28) *as*

$$\mathscr{L}_1(\bar{\mathbf{f}}) = \sum_{k=1}^{K} \left[\log_2 \left(\frac{\bar{\mathbf{f}}^{\mathsf{H}}\mathbf{A}_k\bar{\mathbf{f}}}{\bar{\mathbf{f}}^{\mathsf{H}}\mathbf{B}_k\bar{\mathbf{f}}} \right)^{\omega_k} - \ln \left\{ \sum_{m=1}^{M} \left(\frac{\bar{\mathbf{f}}^{\mathsf{H}}\mathbf{C}_m\bar{\mathbf{f}}}{\bar{\mathbf{f}}^{\mathsf{H}}\mathbf{D}_{m,k}\bar{\mathbf{f}}} \right)^{\omega_{m,k}^{\mathsf{e}}} \right\}^{\frac{1}{\alpha}} \right]. \tag{40}$$

According to the first-order optimality condition, the stationary points need to satisfy zero-gradient, i.e., $\frac{\partial \mathscr{L}_1(\bar{\mathbf{f}})}{\partial \bar{\mathbf{f}}^{\mathsf{H}}} = 0$*. Thus, I take the partial derivative of* $\mathscr{L}_1(\bar{\mathbf{f}})$ *with respect to* $\bar{\mathbf{f}}$ *and set it to zero. Next, I denote the first and second part of* (40) *as* $\mathscr{L}_{1,\mathsf{user}}(\bar{\mathbf{f}})$ *and* $\mathscr{L}_{1,\mathsf{eve}}(\bar{\mathbf{f}})$*, thereby* $\mathscr{L}_1(\bar{\mathbf{f}}) = \mathscr{L}_{1,\mathsf{user}}(\bar{\mathbf{f}}) - \mathscr{L}_{1,\mathsf{eve}}(\bar{\mathbf{f}})$*. Then, I have the partial derivative of* $\mathscr{L}_{1,\mathsf{user}}(\bar{\mathbf{f}})$ *with respect to* $\bar{\mathbf{f}}$ *as*

$$\frac{\partial \mathscr{L}_{1,\mathsf{user}}(\bar{\mathbf{f}})}{\partial \bar{\mathbf{f}}^{\mathsf{H}}} = \sum_{k=1}^{K} \frac{1}{\ln 2} \left(\frac{\mathbf{A}_k \bar{\mathbf{f}}}{\bar{\mathbf{f}}^{\mathsf{H}} \mathbf{A}_k \bar{\mathbf{f}}} - \frac{\mathbf{B}_k \bar{\mathbf{f}}}{\bar{\mathbf{f}}^{\mathsf{H}} \mathbf{B}_k \bar{\mathbf{f}}} \right). \tag{41}$$

Subsequently, I take the partial derivative of $\mathscr{L}_{1,\mathsf{eve}}(\bar{\mathbf{f}})$ *with respect to* $\bar{\mathbf{f}}$ *as*

$$\frac{\partial \mathscr{L}_{1,\mathsf{eve}}(\bar{\mathbf{f}})}{\partial \bar{\mathbf{f}}^{\mathsf{H}}} = \frac{1}{\alpha} \sum_{k=1}^{K} \sum_{m=1}^{M} \left\{ \frac{\omega^{\mathsf{e}}_{m,k} \left(\frac{\bar{\mathbf{f}}^{\mathsf{H}} \mathbf{C}_m \bar{\mathbf{f}}}{\bar{\mathbf{f}}^{\mathsf{H}} \mathbf{D}_{m,k} \bar{\mathbf{f}}} \right)^{\omega^{\mathsf{e}}_{m,k}} \left(\frac{\mathbf{C}_m \bar{\mathbf{f}}}{\bar{\mathbf{f}}^{\mathsf{H}} \mathbf{C}_m \bar{\mathbf{f}}} - \frac{\mathbf{D}_{m,k} \bar{\mathbf{f}}}{\bar{\mathbf{f}}^{\mathsf{H}} \mathbf{D}_{m,k} \bar{\mathbf{f}}} \right)}{\sum_{\ell=1}^{M} \left(\frac{\bar{\mathbf{f}}^{\mathsf{H}} \mathbf{C}_\ell \bar{\mathbf{f}}}{\bar{\mathbf{f}}^{\mathsf{H}} \mathbf{D}_{\ell,k} \bar{\mathbf{f}}} \right)^{\omega^{\mathsf{e}}_{\ell,k}}} \right\}. \tag{42}$$

Then, using (41) *and* (42)*, the first-order optimality condition holds if*

$$\begin{aligned} &\sum_{k=1}^{K} \left[\frac{\omega_k}{\ln 2} \frac{\mathbf{A}_k}{\bar{\mathbf{f}}^{\mathsf{H}} \mathbf{A}_k \bar{\mathbf{f}}} + \frac{1}{\alpha} \left\{ \sum_{m=1}^{M} \left(\frac{\omega^{\mathsf{e}}_{m,k} \left(\frac{\bar{\mathbf{f}}^{\mathsf{H}} \mathbf{C}_m \bar{\mathbf{f}}}{\bar{\mathbf{f}}^{\mathsf{H}} \mathbf{D}_{m,k} \bar{\mathbf{f}}} \right)^{\omega^{\mathsf{e}}_{m,k}} \frac{\mathbf{D}_{m,k}}{\bar{\mathbf{f}}^{\mathsf{H}} \mathbf{D}_{m,k} \bar{\mathbf{f}}}}{\sum_{\ell=1}^{M} \left(\frac{\bar{\mathbf{f}}^{\mathsf{H}} \mathbf{C}_\ell \bar{\mathbf{f}}}{\bar{\mathbf{f}}^{\mathsf{H}} \mathbf{D}_{\ell,k} \bar{\mathbf{f}}} \right)^{\omega^{\mathsf{e}}_{\ell,k}}} \right) \right\} \right] \bar{\mathbf{f}} \\ &= \sum_{k=1}^{K} \left[\frac{\omega_k}{\ln 2} \frac{\mathbf{B}_k}{\bar{\mathbf{f}}^{\mathsf{H}} \mathbf{B}_k \bar{\mathbf{f}}} + \frac{1}{\alpha} \left\{ \sum_{m=1}^{M} \left(\frac{\omega^{\mathsf{e}}_{m,k} \left(\frac{\bar{\mathbf{f}}^{\mathsf{H}} \mathbf{C}_m \bar{\mathbf{f}}}{\bar{\mathbf{f}}^{\mathsf{H}} \mathbf{D}_{m,k} \bar{\mathbf{f}}} \right)^{\omega^{\mathsf{e}}_{m,k}} \frac{\mathbf{C}_m}{\bar{\mathbf{f}}^{\mathsf{H}} \mathbf{C}_m \bar{\mathbf{f}}}}{\sum_{\ell=1}^{M} \left(\frac{\bar{\mathbf{f}}^{\mathsf{H}} \mathbf{C}_\ell \bar{\mathbf{f}}}{\bar{\mathbf{f}}^{\mathsf{H}} \mathbf{D}_{\ell,k} \bar{\mathbf{f}}} \right)^{\omega^{\mathsf{e}}_{\ell,k}}} \right) \right\} \right] \bar{\mathbf{f}}. \end{aligned} \tag{43}$$

Now, the first-order optimality condition can be reorganized as

$$\mathbf{A}_{\mathsf{KKT}}(\bar{\mathbf{f}})\bar{\mathbf{f}} = \lambda(\bar{\mathbf{f}}) \mathbf{B}_{\mathsf{KKT}}(\bar{\mathbf{f}})\bar{\mathbf{f}}. \tag{44}$$

Since $\mathbf{B}_{\mathsf{KKT}}(\bar{\mathbf{f}})$ *is Hermitian, it is invertible. This completes the proof.* ■

I note that the first-order optimality condition in (35) can be interpreted as a generalized eigenvalue problem $\mathbf{B}^{-1}_{\mathsf{KKT}}(\bar{\mathbf{f}})\mathbf{A}_{\mathsf{KKT}}(\bar{\mathbf{f}})\bar{\mathbf{f}} = \lambda(\bar{\mathbf{f}})\bar{\mathbf{f}}$. Here, $\lambda(\bar{\mathbf{f}})$ is as an eigenvalue of $\mathbf{B}^{-1}_{\mathsf{KKT}}(\bar{\mathbf{f}})\mathbf{A}_{\mathsf{KKT}}(\bar{\mathbf{f}})$ with $\bar{\mathbf{f}}$ as a corresponding eigenvector. As a result, maximizing the objective function $\mathscr{L}_1(\bar{\mathbf{f}})$ is equivalent to maximizing $\lambda(\bar{\mathbf{f}})$. Therefore, it is desirable to find the principal eigenvalue of (35) to maximize (34), which is equivalent to finding the best local optimal solution of (28).

According to (35), I propose a sum secrecy rate maximization precoding algorithm by adopting the GPI-based approach [40]. As described in FBL-S-GPIP, I initialize $\bar{\mathbf{f}}^{(0)}$ and update $\bar{\mathbf{f}}^{(t)}$ at each iteration. Given L, $\bar{\varepsilon}$, and Δ, the algorithm constructs $\mathbf{A}_{\mathsf{KKT}}(\bar{\mathbf{f}}^{(t-1)})$ and $\mathbf{B}_{\mathsf{KKT}}(\bar{\mathbf{f}}^{(t-1)})$ according to (36) and (37). Then, the algorithm updates $\bar{\mathbf{f}}^{(t)}$ by computing $\bar{\mathbf{f}}^{(t)} = \mathbf{B}^{-1}_{\mathsf{KKT}}(\bar{\mathbf{f}}^{(t-1)})\mathbf{A}_{\mathsf{KKT}}(\bar{\mathbf{f}}^{(t-1)})\bar{\mathbf{f}}^{(t-1)}$ and normalizing as $\bar{\mathbf{f}}^{(t)} = \bar{\mathbf{f}}^{(t)}/\|\bar{\mathbf{f}}^{(t)}\|$. These steps are repeated until either $\bar{\mathbf{f}}^{(t)}$ converges to a tolerance level ε or the algorithm reaches $t_{\max}$.

The computational complexity of FBL-S-GPIP is primarily determined by the inversion in $\mathbf{B}^{-1}_{\mathsf{KKT}}(\bar{\mathbf{f}})$. By exploiting the block-diagonal and symmetric structure of $\mathbf{B}_{\mathsf{KKT}}(\bar{\mathbf{f}})$, I employ a divide-and-conquer technique for the inversion, resulting in a reduced complexity of $\mathscr{O}\left(\frac{1}{3}KN^3\right)$ [40], instead of the original $\mathscr{O}\left(K^3N^3\right)$. Therefore, the overall complexity of FBL-S-GPIP is $\mathscr{O}\left(\frac{1}{3}TKN^3\right)$, where T represents the number of iterations. It is important to note that the complexity of FBL-S-GPIP is comparable to that

Algorithm 1: FBL-S-GPIP: Best Secure Precoding Direction

```
initialize: $\bar{\mathbf{f}}^{(0)}$, $t = 1$.
while $\left\|\bar{\mathbf{f}}^{(t)} - \bar{\mathbf{f}}^{(t-1)}\right\| > \varepsilon$ & $t \le t_{\max}$ do
    Build $\mathbf{A}_{\mathsf{KKT}}(\bar{\mathbf{f}}^{(t-1)})$ and $\mathbf{B}_{\mathsf{KKT}}(\bar{\mathbf{f}}^{(t-1)})$ according to (36) and (37) for given $\varepsilon_k$ and $\delta_{m,k}$.
    Compute $\bar{\mathbf{f}}^{(t)} = \mathbf{B}^{-1}_{\mathsf{KKT}}(\bar{\mathbf{f}}^{(t-1)})\mathbf{A}_{\mathsf{KKT}}(\bar{\mathbf{f}}^{(t-1)})\bar{\mathbf{f}}^{(t-1)}$.
    Normalize $\bar{\mathbf{f}}^{(t)} = \bar{\mathbf{f}}^{(t)} / \left\|\bar{\mathbf{f}}^{(t)}\right\|$.
    $t \leftarrow t + 1$.
$\bar{\mathbf{f}}^{\star} \leftarrow \bar{\mathbf{f}}^{(t)}$.
return $\bar{\mathbf{f}}^{\star} = \left[\mathbf{f}_1^{\mathsf{T}}, \mathbf{f}_2^{\mathsf{T}}, \ldots, \mathbf{f}_K^{\mathsf{T}}\right]^{\mathsf{T}}$.
```

of a well-known low-complexity sum rate maximization method, namely the weighted minimum mean square error (WMMSE) algorithm [41]. In contrast, other existing methods exhibit higher computational complexities. For instance, the AN-aided transmission approach based on semi-definite programs (SDP) described in [42] requires a complexity order of $\mathscr{O}\left(N^{6.5}\right)$ for a single confidential message. Similarly, the SDP-based algorithm proposed in [43] for a single user and multiple eavesdroppers has a complexity order of $\mathscr{O}\left(N^{8.5}\right)$. Moreover, the jamming noise-aided precoding algorithm developed for multiple users and eavesdroppers in [44] has a complexity order of $\mathscr{O}\left((N+K)^3\right)$. Considering these comparisons, it is evident that FBL-S-GPIP offers a relatively low computational complexity when compared to existing algorithms.

B. Phase II: Maximum Error Probability and Information Leakage Rate Minimization

I determine the optimal values of $\bar{\varepsilon}$ and Δ while keeping $\mathbf{F}$ fixed. This involves transforming the original multi-objective problem into a single-objective problem and finding a solution for the transformed problem. By employing the weighted-sum approach [45], I convert the multi-objective problem stated in (13) into a new formulation:

$$\underset{\bar{\varepsilon},\Delta}{\text{maximize}} \quad \frac{w}{R_\infty}\sum_{k=1}^{K} R_k^{\mathsf{sec}}(\bar{\varepsilon},\Delta) + (1-w)\left(\frac{\hat{\varepsilon}_{\mathsf{max}} - \max\{\bar{\varepsilon}\}}{\hat{\varepsilon}_{\mathsf{max}}} + \frac{\hat{\delta}_{\mathsf{max}} - \max\{\Delta\}}{\hat{\delta}_{\mathsf{max}}}\right) \tag{45}$$

$$\text{subject to} \quad \varepsilon_k \le \hat{\varepsilon}_k, \ \forall k \in \mathscr{K}, \tag{46}$$

$$\delta_{m,k} \le \hat{\delta}_{m,k}, \ \forall m \in \mathscr{M}, \forall k \in \mathscr{K}, \tag{47}$$

where R_∞ can be obtained by calculating the sum secrecy rate in the infinite blocklength regime using a state-of-the-art secure precoder. The values $\hat{\varepsilon}\mathsf{max}$ and $\hat{\delta}\mathsf{max}$ are determined as the maximum values among $\hat{\varepsilon}_1, \ldots, \hat{\varepsilon}_K$ and $\hat{\delta}_{1,1}, \ldots, \hat{\delta}_{M,K}$, respectively. The weight parameter w is chosen from the range $[0,1]$. To solve the multi-objective problem in (45), it is necessary to address the maximum function in $R_k^{\mathsf{sec}}(\varepsilon_k, \delta_{m,k})$. I handle this by introducing an upper bound obtained by adding the wiretap rates:

$$\max_{m\in\mathscr{M}}\left\{R^{\mathsf{e}}_{m,k} + \sqrt{\frac{\mathscr{V}^{\mathsf{e}}_{m,k}}{L}}Q^{-1}\left(\delta_{m,k}\right)\right\} \le \sum_{m=1}^{M}\left(R^{\mathsf{e}}_{m,k} + \sqrt{\frac{\mathscr{V}^{\mathsf{e}}_{m,k}}{L}}Q^{-1}\left(\delta_{m,k}\right)\right). \tag{48}$$

ULSAN NATIONAL INSTITUTE OF SCIENCE AND TECHNOLOGY

It is important to note that although this bound may not be tight and the gap tends to increase with the number of eavesdroppers, the proposed method based on this bound will demonstrate strong performance, especially in scenarios with a large number of eavesdroppers, as discussed in Section 2.4. Subsequently, letting $\tau = \max\{\bar{\varepsilon}\}$ and $\xi = \max\{\Delta\}$ and removing the terms that are not a function of either ε_k or $\delta_{m,k}$, the problem in (45) is further transformed to the minimization problem as

$$\underset{\bar{\varepsilon},\Delta}{\text{minimize}} \ \frac{w}{R_\infty}\sum_{k=1}^{K}\left[\sqrt{\frac{\mathcal{V}_k}{L}}Q^{-1}(\varepsilon_k)+\sum_{m=1}^{M}\left(\sqrt{\frac{\mathcal{V}^{\mathsf{e}}_{m,k}}{L}}Q^{-1}\left(\delta_{m,k}\right)\right)\right]+(1-w)\left(\frac{\tau}{\hat{\varepsilon}_{\mathsf{max}}}+\frac{\xi}{\hat{\delta}_{\mathsf{max}}}\right) \tag{49}$$

$$\text{subject to} \ \ \varepsilon_k \leq \tau, \tag{50}$$

$$0 \leq \varepsilon_k \leq \hat{\varepsilon}_k, \tag{51}$$

$$0 \leq \tau \leq \hat{\varepsilon}_{\mathsf{max}}, \tag{52}$$

$$\delta_{m,k} \leq \xi, \tag{53}$$

$$0 \leq \delta_{m,k} \leq \hat{\delta}_{m,k}, \tag{54}$$

$$0 \leq \xi \leq \hat{\delta}_{\mathsf{max}}, \tag{55}$$

where the constraints (51) and (54) represent the error probability and information leakage rate constraints, respectively. On the other hand, (52) and (55) correspond to the assumptions of maximum error probability and information leakage. In the objective function (49), it can be observed that the first term is monotonically increasing, while the second term is monotonically decreasing with decreasing error probability and information leakage. Consequently, there exists an optimal tradeoff among the back-off factors, error probability, and information leakage rate. This optimal tradeoff can be obtained by solving the KKT conditions [46] associated with (49).

Lemma 3 *The optimal upper decoding error probability and information leakage rate for* (49) *with* $\ell, j(k) \in \mathbb{N}_+$ *are derived as*

$$\tau^\star = Q\left(\sqrt{2\ln\left(\frac{\sqrt{L}(1-w)R_\infty}{\hat{\varepsilon}_{\mathsf{max}}w\sqrt{2\pi}\sum_{k=\ell}^{K}\sqrt{\mathcal{V}_k}}\right)}\right), \tag{56}$$

$$\xi^\star = Q\left(\sqrt{2\ln\left(\frac{\sqrt{L}(1-w)R_\infty}{\hat{\delta}_{\mathsf{max}}w\sqrt{2\pi}\sum_{m=j(k)}^{M}\sum_{k=1}^{K}\sqrt{\mathcal{V}^{\mathsf{e}}_{m,k}}}\right)}\right). \tag{57}$$

Then, without loss of generality, I can assume that $\hat{\varepsilon}_{\ell-1} < \tau < \hat{\varepsilon}_\ell$ *for some* ℓ *and* $\hat{\delta}_{j(k)-1,k} < \xi < \hat{\delta}_{j(k),k}$ *for some* $j(k)$*. Then, the optimal solution of the problem in* (49) *is*

$$\bar{\varepsilon}^\star = [\hat{\varepsilon}_1, \cdots, \hat{\varepsilon}_{\ell-1}, \tau^\star, \cdots, \tau^\star]^{\mathsf{T}} \in \mathbb{R}^K_+, \tag{58}$$

$$\Delta^\star = [\bar{\delta}^\star_1, \cdots, \bar{\delta}^\star_K] \in \mathbb{R}^{M\times K}_+, \tag{59}$$

where

$$\bar{\delta}^\star_k = [\hat{\delta}_{1,k}, \cdots, \hat{\delta}_{j(k)-1,k}, \xi^\star, \cdots, \xi^\star]^{\mathsf{T}} \in \mathbb{R}^M_+, \ \forall k \in \mathcal{K}. \tag{60}$$

ULSAN NATIONAL INSTITUTE OF SCIENCE AND TECHNOLOGY

If $\hat{\varepsilon}_K < \tau^\star$, the optimal error probability becomes

$$\bar{\varepsilon}^\star = [\hat{\varepsilon}_1, \cdots, \hat{\varepsilon}_K]^{\mathsf{T}}. \tag{61}$$

Similarly, if $\hat{\delta}_{M,k} < \xi^\star, \forall k \in \mathscr{K}$, the optimal information leakage rate becomes

$$\bar{\delta}^\star_k = [\hat{\delta}_{1,k}, \cdots, \hat{\delta}_{M,k}]^{\mathsf{T}},\ \forall k \in \mathscr{K}. \tag{62}$$

Proof 3 *I note that $Q^{-1}(x)$ is convex if $x < \frac{1}{2}$, so that the problem in* (49) *becomes a convex problem. To solve the problem, I define the Lagrangian function of the problem in* (49) *as*

$$\begin{aligned}\mathscr{L}_2 = {} & \frac{w}{R_\infty}\sum_{k=1}^{K}\left[\sqrt{\frac{\mathscr{V}_k}{L}}Q^{-1}(\varepsilon_k)+\sum_{m=1}^{M}\left(\sqrt{\frac{\mathscr{V}^{\mathsf{e}}_{m,k}}{L}}Q^{-1}(\delta_{m,k})\right)\right]+(1-w)\left(\frac{\tau}{\hat{\varepsilon}_{\mathsf{max}}}+\frac{\xi}{\hat{\delta}_{\mathsf{max}}}\right)-\sum_{k=1}^{K}\lambda_k(\tau-\varepsilon_k)\\ & -\sum_{k=1}^{K}\nu_k(\hat{\varepsilon}_k-\varepsilon_k)-\mu(\hat{\varepsilon}_{\mathsf{max}}-\tau)-\sum_{m=1}^{M}\sum_{k=1}^{K}\lambda^{\mathsf{e}}_{m,k}(\xi-\delta_{m,k})-\sum_{m=1}^{M}\sum_{k=1}^{K}\nu^{\mathsf{e}}_{m,k}(\hat{\delta}_{m,k}-\delta_{m,k})-\mu^{\mathsf{e}}(\hat{\delta}_{\mathsf{max}}-\xi),\end{aligned} \tag{63}$$

where λ_k, ν_k, μ, $\lambda^{\mathsf{e}}_{m,k}$, $\nu^{\mathsf{e}}_{m,k}$, and μ^{e} indicate Lagrangian multipliers. For a feasible solution, I assume $\lambda_k \geq 0$, $\nu_k \geq 0$, $\mu \geq 0$, $\mu^{\mathsf{e}} \geq 0$, $\lambda^{\mathsf{e}}_{m,k} \geq 0$, and $\nu^{\mathsf{e}}_{m,k} \geq 0, \forall k \in \mathscr{K}, \forall m \in \mathscr{M}$. According to the KKT conditions, the optimal solution for the problem in (49) *should satisfy the followings:*

$$\left.\frac{\partial \mathscr{L}_2}{\partial \varepsilon_k}\right|_{\varepsilon_k=\varepsilon_k^\star} = -\frac{w}{R_\infty}\sqrt{\frac{\mathscr{V}_k}{L}}\sqrt{2\pi}\exp\left(\frac{\left(Q^{-1}(\varepsilon_k^\star)\right)^2}{2}\right)+\lambda_k^\star+\nu_k^\star=0, \tag{64}$$

$$\left.\frac{\partial \mathscr{L}_2}{\partial \tau}\right|_{\tau=\tau^\star} = \frac{1-w}{\hat{\varepsilon}_{\mathsf{max}}}-\sum_k\lambda_k^\star+\mu^\star=0, \tag{65}$$

$$\left.\frac{\partial \mathscr{L}_2}{\partial \delta_{m,k}}\right|_{\delta_{m,k}=\delta_{m,k}^\star} = -\frac{w}{R_\infty}\sqrt{\frac{\mathscr{V}^{\mathsf{e}}_{m,k}}{L}}\sqrt{2\pi}\exp\left(\frac{\left(Q^{-1}(\delta_{m,k}^\star)\right)^2}{2}\right)+\lambda^{\mathsf{e},\star}_{m,k}+\nu^{\mathsf{e},\star}_{m,k}=0, \tag{66}$$

$$\left.\frac{\partial \mathscr{L}_2}{\partial \xi}\right|_{\xi=\xi^\star} = \frac{1-w}{\hat{\delta}_{\mathsf{max}}}-\sum_{m,k}\lambda^{\mathsf{e},\star}_{m,k}+\mu^{\mathsf{e},\star}=0, \tag{67}$$

$$\lambda_k^\star(\tau^\star-\varepsilon_k^\star)=0, \tag{68}$$

$$\nu_k^\star(\hat{\varepsilon}_k-\varepsilon_k^\star)=0, \tag{69}$$

$$\mu^\star(\hat{\varepsilon}_{\mathsf{max}}-\tau^\star)=0, \tag{70}$$

$$\lambda^{\mathsf{e},\star}_{m,k}(\xi^\star-\delta^\star_{m,k})=0, \tag{71}$$

$$\nu^{\mathsf{e},\star}_{m,k}(\hat{\delta}_{m,k}-\delta^\star_{m,k})=0, \tag{72}$$

$$\mu^{\mathsf{e},\star}(\hat{\delta}_{\mathsf{max}}-\xi^\star)=0, \tag{73}$$

where (64) *and* (66) *come from that $\partial Q^{-1}(x)/\partial x = -\sqrt{2\pi}\exp\left(\left(Q^{-1}(x)\right)^2/2\right)$. Now, I obtain the optimal points $\varepsilon_k^\star$ and $\delta^\star_{m,k}$ by using the derived KKT conditions. From* (64), (68), *and* (69), *$\varepsilon_k^\star$ should be equal to $\tau^\star$ or $\hat{\varepsilon}_k$. In the same manner, $\delta^\star_{m,k}$ should be equal to $\xi^\star$ or $\hat{\delta}_{m,k}$ from* (66), (71), *and* (72). *Assuming that $\tau^\star < \hat{\varepsilon}_{\mathsf{max}}$ and $\xi^\star < \hat{\delta}_{\mathsf{max}}$, I obtain $\mu^\star = \mu^{\mathsf{e},\star} = 0$. Since I can assume that $\hat{\varepsilon}_{\ell-1} < \tau^\star < \hat{\varepsilon}_\ell$ for some ℓ and $\hat{\delta}_{j(k)-1,k} < \xi^\star < \hat{\delta}_{j(k),k}$ for some $j(k)$, the optimal error probability and information*

ULSAN NATIONAL INSTITUTE OF SCIENCE AND TECHNOLOGY

Algorithm 2: FBL-JS-GPIP: Joint Optimization based on Alternating Approach

```
initialize: $\bar{\mathbf{f}}^{(0)}, \bar{\varepsilon}^{(0)}, \bar{\delta}_k^{(0)}, \forall k \in \mathscr{K}$, and $t = 1$.
while increment of (49) $> \varepsilon^{\mathrm{out}}$ & $t \le t_{\max}^{\mathrm{out}}$ do
    $\bar{\mathbf{f}}^{(t)} \leftarrow$ FBL-S-GPIP with $\bar{\varepsilon}^{(t-1)}, \Delta^{(t-1)}$.
    Compute $R_\infty$ by using FBL-S-GPIP with $L = \infty$.
    Find $\tau^\star$ and $\xi^\star$ according to (56) and (57) for $\bar{\mathbf{f}}^{(t)}$.
    Set $\bar{\varepsilon}^{(t)} = [\hat{\varepsilon}_1, \cdots, \hat{\varepsilon}_{\ell-1}, \tau^\star, \cdots, \tau^\star]^{\mathsf{T}}$ and $\bar{\delta}_k^{(t)} = [\hat{\delta}_{1,k}, \cdots, \hat{\delta}_{j(k)-1,k}, \xi^\star, \cdots, \xi^\star]^{\mathsf{T}}, \forall k \in \mathscr{K}$.
    $t \leftarrow t + 1$.
$\bar{\mathbf{f}}^\star \leftarrow \bar{\mathbf{f}}^{(t)}$, $\bar{\varepsilon}^\star \leftarrow \bar{\varepsilon}^{(t)}$, and $\Delta^\star \leftarrow \Delta^{(t)}$.
return $\bar{\mathbf{f}}^\star = \left[\mathbf{f}_1^{\mathsf{T}}, \mathbf{f}_2^{\mathsf{T}}, \ldots, \mathbf{f}_K^{\mathsf{T}}\right]^{\mathsf{T}}$, $\bar{\varepsilon}^\star$, and $\Delta^\star$.
```

leakage vectors are obtained as

$$\bar{\varepsilon}^\star = [\hat{\varepsilon}_1, \cdots, \hat{\varepsilon}_{\ell-1}, \tau^\star, \cdots, \tau^\star]^{\mathsf{T}}, \tag{74}$$

$$\bar{\delta}_k^\star = [\hat{\delta}_{1,k}, \cdots, \hat{\delta}_{j(k)-1,k}, \xi^\star, \cdots, \xi^\star]^{\mathsf{T}}. \tag{75}$$

The information leakage matrix builds upon the derived information leakage vectors as

$$\Delta^\star = [\bar{\delta}_1^\star, \cdots, \bar{\delta}_K^\star]. \tag{76}$$

Assuming $\hat{\varepsilon}_{\ell-1} < \tau^\star < \hat{\varepsilon}_\ell$ for some ℓ, $\nu_k^\star = 0$ and $\mu^\star = 0$ for $k \ge \ell$. Combining (64) *and* (65)*,*

$$\frac{w}{R_\infty} \sum_{k=\ell}^{K} \sqrt{\frac{\mathscr{V}_k}{L}} \sqrt{2\pi} \exp\left(\frac{\left(Q^{-1}(\varepsilon_k^\star)\right)^2}{2}\right) = \frac{1-w}{\hat{\varepsilon}_{\mathsf{max}}}, \text{ for } k \ge \ell. \tag{77}$$

I solve (77) *with respect to $\varepsilon_k^\star$ and have $\varepsilon_k^\star = \tau^\star$ which is in* (56) *for $k \ge \ell$. Similarly, I assume $\hat{\delta}_{j(k)-1,k} < \xi^\star < \hat{\delta}_{j(k),k}$, then $\nu_{m,k}^{\mathsf{e},\star} = 0$ and $\mu^{\mathsf{e},\star} = 0$ for $m \ge j(k)$. From* (66) *and* (67)*,*

$$\frac{w}{R_\infty} \sum_{m=j(k)}^{M} \sum_{k=1}^{K} \sqrt{\frac{\mathscr{V}_{m,k}^{\mathsf{e}}}{L}} \sqrt{2\pi} \exp\left(\frac{\left(Q^{-1}(\delta_{m,k}^\star)\right)^2}{2}\right) = \frac{1-w}{\hat{\delta}_{\mathsf{max}}}, \text{ for } m \ge j(k). \tag{78}$$

Solving (78) *with respect to $\delta_{m,k}^\star$, I have $\delta_{m,k}^\star = \xi^\star$ in* (57) *for $m \ge j(k)$. This completes proof.* ■

C. Proposed Joint Secure Precoding Algorithm

Based on the results obtained in Section 2.4 and Section 8, I present my proposed algorithm, referred to as FBL-JS-GPIP. The algorithm follows the following steps: 1) initialization: FBL-JS-GPIP initializes the precoding vector $\bar{\mathbf{f}}^{(0)}$, $\bar{\varepsilon}^{(0)}$, and $\bar{\delta}_k^{(0)}$ for all $k \in \mathscr{K}$, 2) local optimization: To find the best local optimal precoding vector $\bar{\mathbf{f}}^{(t)}$, FBL-S-GPIP is used with the given $\bar{\varepsilon}^{(t-1)}$ and $\bar{\delta}_k^{(t-1)}$, 3) computation of normalized value: R_∞ is computed by finding $\bar{\mathbf{f}}$ using FBL-S-GPIP in the infinite blocklength regime, 4) computation of optimal parameters: The optimal values of $\tau^\star$ and $\xi^\star$ are computed based on (56) and (57), respectively. Then, $\bar{\varepsilon}^{(t)}$ and $\Delta^{(t)}$ are set accordingly, 5) iteration: The above steps are repeated until either the objective function in (45) increases by a value smaller than the tolerance threshold $\varepsilon^{\mathrm{out}}$

ULSAN NATIONAL INSTITUTE OF SCIENCE AND TECHNOLOGY

compared to the previous iteration, where $\varepsilon^{\text{out}} > 0$, or the algorithm reaches the maximum iteration count $t_{\max}^{\text{out}}$. The solutions obtained in (56) and (57) are closed-form, which leads to a complexity order of $\mathscr{O}\left(\frac{1}{3}T_{\text{tot}}KN^3\right)$ for FBL-JS-GPIP. Here, T_{tot} represents the total number of iterations in FBL-S-GPIP.

D. Extension to Partial CSIT of Wiretap Channels

Due to the challenges associated with obtaining perfect CSIT, I consider the scenario where only the long-term channel statistics, represented by the channel covariance matrix $\mathbf{R}_m^{\mathsf{e}}$, are available for the wiretap channels. In this partial CSIT setting, the instantaneous CSI of the eavesdroppers is unknown, making it impractical to consider the instantaneous wiretap rate. Therefore, I adopt the ergodic wiretap rate as the performance metric, following a similar approach as in [47]. The use of ergodic rates as an optimization objective allows for the exploitation of the available partial CSIT in an average sense, effectively addressing the challenge of imperfect channel knowledge. Now, instead of the secrecy rate in (10), I have

$$R_k^{\mathsf{sec,p}} = R_k - \sqrt{\frac{\mathscr{V}_k}{L}}Q^{-1}(\varepsilon_k) - \max_{m\in\mathscr{M}}\left\{\mathbb{E}_{\mathbf{g}}\left[R_{m,k}^{\mathsf{e}} + \sqrt{\frac{\mathscr{V}_{m,k}^{\mathsf{e}}}{L}}Q^{-1}\left(\delta_{m,k}\right)\right]\right\}, \tag{79}$$

where $\mathbb{E}_{\mathbf{g}}[\cdot]$ indicates the expectation with respect to wiretap channels. A notable distinction from [47] is that I do not average the user rates in my approach because I have access to the user channel knowledge, which allows for a more precise optimization and ultimately leads to improved performance. By leveraging the available user channel information, I can directly optimize the individual user rates without the need for averaging, resulting in enhanced optimization outcomes. Then, I can rewrite (79) by using the following proposition.

Proposition 1 *The approximated upper bound of the ergodic wiretap secrecy rate in* (79) *is obtained as*

$$\mathbb{E}_{\mathbf{g}}\left[R_{m,k}^{\mathsf{e}}+\sqrt{\frac{\mathscr{V}_{m,k}^{\mathsf{e}}}{L}}Q^{-1}\left(\delta_{m,k}\right)\right] \lessapprox \bar{R}_{m,k}^{\mathsf{e}}+\sqrt{\frac{\bar{\mathscr{V}}_{m,k}^{\mathsf{e}}}{L}}Q^{-1}\left(\delta_{m,k}\right), \tag{80}$$

where

$$\bar{R}_{m,k}^{\mathsf{e}} = \log_2\left(1+\frac{\mathbf{f}_k^{\mathsf{H}}\mathbf{R}_m^{\mathsf{e}}\mathbf{f}_k}{\sum_{\ell\neq k}^{K}\mathbf{f}_\ell^{\mathsf{H}}\mathbf{R}_m^{\mathsf{e}}\mathbf{f}_\ell+\sigma_{\mathsf{e}}^2/P}\right), \tag{81}$$

$$\bar{\mathscr{V}}_{m,k}^{\mathsf{e}} = \sqrt{\frac{2\mathbf{f}_k^{\mathsf{H}}\mathbf{R}_m^{\mathsf{e}}\mathbf{f}_k}{\sum_{k=1}^{K}\mathbf{f}_\ell^{\mathsf{H}}\mathbf{R}_m^{\mathsf{e}}\mathbf{f}_\ell+\sigma_{\mathsf{e}}^2/P}}\log_2 e. \tag{82}$$

Proof 4 *The ergodic rate of eavesdropper in* (8) *can be approximated as*

$$\mathbb{E}_{\mathbf{g}}[R_{m,k}^{\mathsf{e}}] = \mathbb{E}_{\mathbf{g}}\left[\log_2\left(1+\frac{|\mathbf{g}_m^{\mathsf{H}}\mathbf{f}_k|^2}{\sum_{\ell\neq k}^{K}|\mathbf{g}_m^{\mathsf{H}}\mathbf{f}_\ell|^2+\sigma_{\mathsf{e}}^2/P}\right)\right] \tag{83}$$

$$\overset{(a)}{\approx} \log_2\left(1+\frac{\mathbf{f}_k^{\mathsf{H}}\mathbf{R}_m^{\mathsf{e}}\mathbf{f}_k}{\sum_{\ell\neq k}^{K}\mathbf{f}_\ell^{\mathsf{H}}\mathbf{R}_m^{\mathsf{e}}\mathbf{f}_\ell+\sigma_{\mathsf{e}}^2/P}\right) \tag{84}$$

$$= \bar{R}_{m,k}^{\mathsf{e}}, \tag{85}$$

where (a) comes from Lemma 1 in [48]. Now, it can be obtained by the following procedure:

$$\begin{aligned}
\mathbb{E}\left[\sqrt{\mathscr{V}^{\mathsf{e}}_{m,k}}\right] \overset{(b)}{\leq} \sqrt{\mathbb{E}\left[\mathscr{V}^{\mathsf{e}}_{m,k}\right]} &\overset{(c)}{\leq} \sqrt{\frac{2}{\frac{1}{\mathbb{E}\left[\rho^{\mathsf{e}}_{m,k}\right]}+1}\log_2 e} && (86)\\
&\overset{(d)}{\approx} \sqrt{\frac{2\mathbf{f}_k^{\mathsf{H}}\mathbf{R}^{\mathsf{e}}_m\mathbf{f}_k}{\sum_{k=1}^{K}\mathbf{f}_\ell^{\mathsf{H}}\mathbf{R}^{\mathsf{e}}_m\mathbf{f}_\ell+\sigma_{\mathsf{e}}^2/P}\log_2 e} && (87)\\
&= \sqrt{\bar{\mathscr{V}}^{\mathsf{e}}_{m,k}}, && (88)
\end{aligned}$$

where (b) and (c) follow from Jensen's inequality, and (d) comes from the first-order Taylor expansion in [49]. This completes proof. ■

Applying (80) to (79), I have the lower bound of secrecy rate approximated as

$$\begin{aligned}
R_k^{\mathsf{sec,p}} &\gtrapprox R_k - \sqrt{\frac{\mathscr{V}_k}{L}}Q^{-1}(\varepsilon_k) - \max_{m\in\mathscr{M}}\left\{\bar{R}^{\mathsf{e}}_{m,k}+\sqrt{\frac{\bar{\mathscr{V}}^{\mathsf{e}}_{m,k}}{L}}Q^{-1}\left(\delta_{m,k}\right)\right\}\\
&= \bar{R}_k^{\mathsf{sec,p}}. && (89)
\end{aligned}$$

Replacing R_k^{sec} in (13) with $\bar{R}_k^{\mathsf{sec,p}}$, I can also design the joint optimization framework for finding the precoder, error probability, and information leakage rate. According to Section 2.4, I can also formulate the sum secrecy rate maximization problem with the approximated rate $\bar{R}_k^{\mathsf{sec,p}}$:

$$\begin{aligned}
&\underset{\mathbf{F}}{\text{maximize}} \ \sum_{k=1}^{K}\bar{R}_k^{\mathsf{sec,p}} && (90)\\
&\text{subject to} \ \ \mathrm{tr}\left(\mathbf{F}\mathbf{F}^{\mathsf{H}}\right)\leq 1. && (91)
\end{aligned}$$

I note that the formulated problem in (90) consists of the channel covariance matrix of mth wiretap channel as defined $\mathbf{R}^{\mathsf{e}}_m$. In addition, according to Section 2.4, the first-order optimality condition can be derived for (90) as

$$\bar{\mathbf{B}}_{\mathsf{KKT}}^{-1}(\bar{\mathbf{f}})\bar{\mathbf{A}}_{\mathsf{KKT}}(\bar{\mathbf{f}})\bar{\mathbf{f}} = \bar{\lambda}(\bar{\mathbf{f}})\bar{\mathbf{f}}, \quad (92)$$

where

$$\bar{\mathbf{A}}_{\mathsf{KKT}}(\bar{\mathbf{f}}) = \bar{\lambda}_{\mathsf{num}}(\bar{\mathbf{f}}) \sum_{k=1}^{K} \left[\frac{\omega_k}{\ln 2} \left(\frac{\mathbf{A}_k}{\bar{\mathbf{f}}^{\mathsf{H}} \mathbf{A}_k \bar{\mathbf{f}}} \right) + \frac{1}{\alpha} \sum_{m=1}^{M} \left(\frac{\omega^{\mathsf{e}}_{m,k} \beta_{m,k} \left(\frac{\bar{\mathbf{f}}^{\mathsf{H}} \bar{\mathbf{C}}_m \bar{\mathbf{f}}}{\bar{\mathbf{f}}^{\mathsf{H}} \bar{\mathbf{D}}_{m,k} \bar{\mathbf{f}}} \right)^{\omega^{\mathsf{e}}_{m,k}} \frac{\bar{\mathbf{D}}_{m,k}}{\bar{\mathbf{f}}^{\mathsf{H}} \bar{\mathbf{D}}_{m,k} \bar{\mathbf{f}}}}{\sum_{\ell=1}^{M} \beta_{m,k} \left(\frac{\bar{\mathbf{f}}^{\mathsf{H}} \bar{\mathbf{C}}_\ell \bar{\mathbf{f}}}{\bar{\mathbf{f}}^{\mathsf{H}} \bar{\mathbf{D}}_{\ell,k} \bar{\mathbf{f}}} \right)^{\omega^{\mathsf{e}}_{\ell,k}}} \right) \right], \tag{93}$$

$$\bar{\mathbf{B}}_{\mathsf{KKT}}(\bar{\mathbf{f}}) = \bar{\lambda}_{\mathsf{den}}(\bar{\mathbf{f}}) \sum_{k=1}^{K} \left[\frac{\omega_k}{\ln 2} \left(\frac{\mathbf{B}_k}{\bar{\mathbf{f}}^{\mathsf{H}} \mathbf{B}_k \bar{\mathbf{f}}} \right) + \frac{1}{\alpha} \sum_{m=1}^{M} \left(\frac{\omega^{\mathsf{e}}_{m,k} \beta_{m,k} \left(\frac{\bar{\mathbf{f}}^{\mathsf{H}} \bar{\mathbf{C}}_m \bar{\mathbf{f}}}{\bar{\mathbf{f}}^{\mathsf{H}} \bar{\mathbf{D}}_{m,k} \bar{\mathbf{f}}} \right)^{\omega^{\mathsf{e}}_{m,k}} \frac{\bar{\mathbf{C}}_{m}}{\bar{\mathbf{f}}^{\mathsf{H}} \bar{\mathbf{C}}_{m} \bar{\mathbf{f}}}}{\sum_{\ell=1}^{M} \beta_{m,k} \left(\frac{\bar{\mathbf{f}}^{\mathsf{H}} \bar{\mathbf{C}}_\ell \bar{\mathbf{f}}}{\bar{\mathbf{f}}^{\mathsf{H}} \bar{\mathbf{D}}_{\ell,k} \bar{\mathbf{f}}} \right)^{\omega^{\mathsf{e}}_{\ell,k}}} \right) \right], \tag{94}$$

$$\bar{\mathbf{C}}_m = \mathrm{blkdiag}\left(\mathbf{R}^{\mathsf{e}}_m, \cdots, \mathbf{R}^{\mathsf{e}}_m\right) + \mathbf{I}_{NK} \frac{\sigma^2_{\mathsf{e}}}{P} \in \mathbb{C}^{NK \times NK}, \tag{95}$$

$$\bar{\mathbf{D}}_{m,k} = \bar{\mathbf{C}}_m - \mathrm{blkdiag}(\mathbf{0}, \cdots, \underbrace{\mathbf{R}^{\mathsf{e}}_m}_{k\text{th block}}, \cdots, \mathbf{0}) \in \mathbb{C}^{NK \times NK}, \tag{96}$$

$$\bar{\lambda}(\bar{\mathbf{f}}) = \bar{\lambda}_{\mathsf{num}}(\bar{\mathbf{f}}) / \bar{\lambda}_{\mathsf{den}}(\bar{\mathbf{f}}), \tag{97}$$

$$\bar{\lambda}_{\mathsf{num}}(\bar{\mathbf{f}}) = \prod_{k=1}^{K} \left(\frac{\bar{\mathbf{f}}^{\mathsf{H}} \mathbf{A}_k \bar{\mathbf{f}}}{\bar{\mathbf{f}}^{\mathsf{H}} \mathbf{B}_k \bar{\mathbf{f}}} \right)^{\omega_k}, \tag{98}$$

$$\bar{\lambda}_{\mathsf{den}}(\bar{\mathbf{f}}) = \prod_{k=1}^{K} \left\{ \sum_{m=1}^{M} \beta_{m,k} \left(\frac{\bar{\mathbf{f}}^{\mathsf{H}} \bar{\mathbf{C}}_m \bar{\mathbf{f}}}{\bar{\mathbf{f}}^{\mathsf{H}} \bar{\mathbf{D}}_{m,k} \bar{\mathbf{f}}} \right)^{\omega^{\mathsf{e}}_{m,k}} \right\}^{\frac{\ln 2}{\alpha}}. \tag{99}$$

Recall that $\mathbf{A}_k$ and $\mathbf{B}_k$ are derived in (29) and (30), respectively. Replacing $\mathbf{A}_{\mathsf{KKT}}$ and $\mathbf{B}_{\mathsf{KKT}}$ with $\bar{\mathbf{A}}_{\mathsf{KKT}}$ and $\bar{\mathbf{B}}_{\mathsf{KKT}}$ in FBL-S-GPIP, I can design the secure precoding algorithm by leveraging the partial CSIT of the eavesdroppers. The maximum error probability and information leakage rate can also be optimized by following the same steps in Section 8 based on $\bar{R}^{\mathsf{sec,p}}_k$ as

$$\bar{\tau}^\star = Q\left(\sqrt{2 \ln \left(\frac{\sqrt{L}(1-w)\bar{R}_\infty}{\hat{\varepsilon}_{\mathsf{max}} w \sqrt{2\pi} \sum_{k=\ell}^{K} \sqrt{\mathscr{V}_k}} \right)} \right), \tag{100}$$

$$\bar{\xi}^\star = Q\left(\sqrt{2 \ln \left(\frac{\sqrt{L}(1-w)\bar{R}_\infty}{\hat{\delta}_{\mathsf{max}} w \sqrt{2\pi} \sum_{m=j(k)}^{M} \sum_{k=1}^{K} \sqrt{\bar{\mathscr{V}}^{\mathsf{e}}_{m,k}}} \right)} \right), \tag{101}$$

where $\bar{R}_\infty$ is the normalization constant based on $\bar{R}^{\mathsf{sec,p}}_k$ for $L = \infty$. Then, the joint secure precoding algorithm is proposed with FBL-JS-GPIP by replacing $\mathbf{A}_k$, $\mathbf{B}_k$, $\tau^\star$, and $\xi^\star$ with $\bar{\mathbf{A}}_k$, $\bar{\mathbf{B}}_k$, $\bar{\tau}^\star$, and $\bar{\xi}^\star$, respectively.

2.5 Simulation Results

In this section, I evaluate the performance of myproposed algorithms and deliver key insights. Including the proposed algorithms and benchmark schemes, I evaluate the following cases:

- Proposed algorithms: FBL-S-GPIP, FBL-S-GPIP with the partial CSIT of wiretap channel (partial), FBL-JS-GPIP, FBL-JS-GPIP (partial).

- Benchmark schemes: (1) a FBL-based SE maximization algorithm (FBL-SE-MAX) [33], (2) WMMSE [47], (3) a ZF-based secure precoding algorithm (ZF-EVE), (4) RZF, and (5) RZF-EVE.

The WMMSE-based algorithm, which incorporates a sample average approximation, is solved using the CVX toolbox [47]. While FBL-SE-MAX prioritizes maximizing the spectral efficiency (SE) for a finite coding length, it does not take into account security considerations. On the other hand, RZF-EVE and ZF-EVE aim to nullify the impact of wiretap channels by constructing an effective channel matrix using the $N-K$ strongest eavesdroppers' channel vectors. When $N > K$, ZF-EVE and RZF-EVE exploit the wiretap channels as $\bar{\mathbf{H}} = [\mathbf{h}_1, \ldots, \mathbf{h}_K, \mathbf{g}_1, \ldots, \mathbf{g}_{N-K}]$, i.e., ZF-EVE and RZF-EVE precoders are

$$\mathbf{F}_{\mathsf{ZF-EVE}} = \left[\bar{\mathbf{H}}\left(\bar{\mathbf{H}}^{\mathsf{H}}\bar{\mathbf{H}}\right)^{-1}\right]_{:,1:K}, \tag{102}$$

$$\mathbf{F}_{\mathsf{RZF-EVE}} = \left[\bar{\mathbf{H}}\left(\bar{\mathbf{H}}^{\mathsf{H}}\bar{\mathbf{H}} + \frac{\sigma^2}{P}\mathbf{I}\right)^{-1}\right]_{:,1:K}. \tag{103}$$

To model the large-scale channel fading terms γ_k and $\gamma^{\mathsf{e}}_{m,k}$, I adopt the ITU-R indoor pathloss model [50], which accurately represents the non-line-of-sight pathloss environment. For this model, I set the parameters as follows: a bandwidth of 10 MHz, carrier frequency of 5.2 GHz, distance power-loss coefficient of 31 (equivalent to a pathloss exponent of 3.1), and a noise figure of 5 dB. The noise power spectral density is assumed to be the same for both legitimate users and eavesdroppers, set at -174 dBm/Hz. The users are randomly positioned around the AP, with distances ranging from a minimum of 5 meters to a maximum of 50 meters. The eavesdroppers are randomly distributed around the users, with a maximum distance of 5 meters from each user, allowing them to intercept the transmitted signals.

To generate the channel vectors $\mathbf{h}_k$ and $\mathbf{g}_m$ with the derived pathloss, I adopt the one-ring model [51] based on its spatial covariance matrices $\mathbf{R}_k = \mathbb{E}[\mathbf{h}_k\mathbf{h}_k^{\mathsf{H}}]$ and $\mathbf{R}^{\mathsf{e}}_m = \mathbb{E}[\mathbf{g}_m\mathbf{g}_m^{\mathsf{H}}]$. The AP is equipped with uniform circular array with radius ϕD where ϕ denotes the wavelength and $D = \frac{0.5}{\sqrt{(1-\cos(2\pi/N)^2+\sin^2(2\pi/N))}}$. I consider the angular spreads of the users and the eavesdroppers to be $\pi/12$ and assume that the angles of departures (AoDs) are drawn from the uniform distribution $\theta_k \sim \mathscr{U}(0, 2\pi]$. In addition, I consider that the geometric location of each eavesdropper is correlated with a particular legitimate user. Accordingly, the channel AoDs of eavesdropper m follow $\theta^{\mathsf{e}}_m \sim \theta_k + \mathscr{U}(-\Delta\pi, \Delta\pi)$ for randomly selected user k with a scalar weight $0 < \Delta < 1$, where θ_k represents the AoD of user k. I generate $\hat{\varepsilon}_k$ and $\hat{\delta}_{m,k}$ uniformly spaced from 10^{-6} to 2×10^{-6} for all users and eavesdroppers. For simplicity, I consider $\hat{\delta}_{m,k} = \hat{\delta}_{m,k'}, \forall m \in \mathscr{M}$. I set the scalar weight, coding length, optimization weight, iteration thresholds, and maximum iteration counts as $\Delta = 0.1$, $L = 200$, $w = 0.01$, $\varepsilon = \varepsilon^{\text{out}} = 0.01$, and $t_{\max} = 15$ and $t^{\text{out}}_{\max} = 5$ unless mentioned otherwise.

I begin by examining FBL-S-GPIP, which aims to maximize the sum secrecy rate by optimizing the transmit power P given fixed values of ε_k and $\delta_{m,k}$, denoted as $\hat{\varepsilon}_k$ and $\hat{\delta}_{m,k}$, respectively. It is worth noting that the range of transmit power considered in the evaluation is wider than what is typically used in practice, allowing for a comprehensive assessment of the proposed algorithms. Figure 2 showcases the rate performance of FBL-S-GPIP across various transmit power levels. Notably, FBL-S-GPIP consistently achieves the highest rate performance across the entire transmit power range. Furthermore, it is observed that FBL-S-GPIP (partial) outperforms the benchmark schemes that do not possess perfect wiretap CSIT. This can be attributed to the fact that the proposed methods jointly optimize the sum secrecy rate maximization problem by considering back-off factors, as well as user and wiretap rates. In

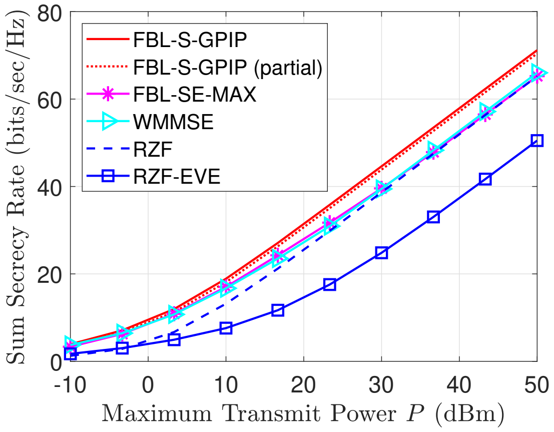


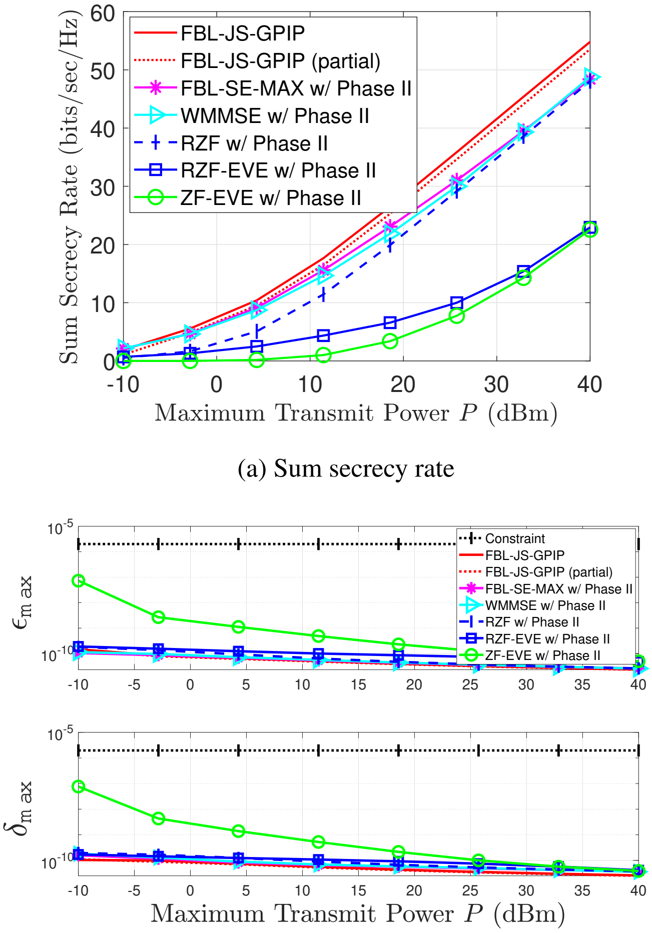
Figure 2: Simulation results of sum secrecy rate with transmit power

contrast, secure precoders such as RZF-EVE and ZF-EVE primarily focus on nullifying leakage from the wiretap channels rather than enhancing the channel gains of legitimate users, resulting in inferior performance as illustrated in Figure 2.

I proceed to evaluate the performance of the proposed method, FBL-JS-GPIP, and compare it with the baseline algorithms that utilize the second phase (Phase II) of the proposed optimization framework, focusing on minimizing the maximum error probability and information leakage rate. Figure 3 illustrates the performance of the sum secrecy rate, maximum error probability, and information leakage rate as a function of the transmit power P for the specific configuration of $N = 8$, $K = 4$, and $M = 8$. It is evident that the benchmark algorithms incorporating the proposed minimization method exhibit a significant reduction in both the maximum error probability and information leakage rate. Notably, the proposed algorithm achieves the highest secrecy rate performance while simultaneously maintaining the lowest maximum error probability and information leakage rate across a wide range of signal-to-noise ratios (SNR). Furthermore, FBL-SE-MAX with Phase II achieves the lowest maximum error probability in most SNR regimes. However, it is observed that the proposed algorithm outperforms FBL-SE-MAX in terms of security rate, indicating a growing gap between the two methods due to FBL-SE-MAX's neglect of the wiretap channels. Overall, the proposed algorithm demonstrates significant SNR improvement, thereby fulfilling the stringent requirements of URLLC in the finite FBL regime.

To provide a numerical analysis based on the number of AP antennas N, the performance of the sum secrecy rate, maximum error probability, and information leakage rate is evaluated in relation to N for a fixed transmit power $P = 20$ dBm, $K = 4$, and $M = 8$, as depicted in Figure 4. The results demonstrate that the proposed algorithms consistently achieve the highest secrecy rate performance across different values of N. However, a distinct trend is observed for RZF-EVE and ZF-EVE in terms of the sum secrecy rate as N increases. This can be attributed to the optimal tradeoff between enhancing legitimate channel gains and nullifying the wiretap channels. Consequently, the rates do not exhibit a monotonic increase with N for RZF-EVE and ZF-EVE. Specifically, Figure 4(a) reveals that when the spare dimension of $N - K$ is small, it is more beneficial to allocate the extra degree-of-freedom (DoF) towards increasing the signal gain of legitimate users. As a result, ZF-EVE and RZF-EVE exhibit lower rates compared to

ULSAN NATIONAL INSTITUTE OF SCIENCE AND TECHNOLOGY



(a) Sum secrecy rate

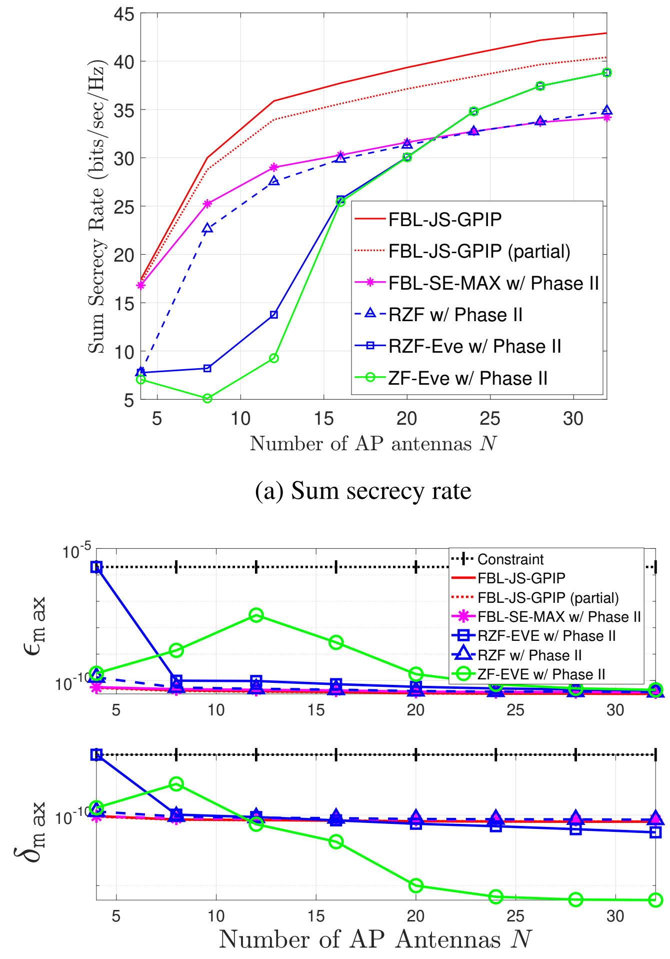
(b) Error probability and information leakage rate

Figure 3: Simulation results of sum secrecy rate, error probability, and information leakage rate with transmit power

ZF and RZF. Conversely, when $N-K$ is large, the additional DoF can be utilized to both enhance user signal gains and nullify wiretap channels. Consequently, as N increases, the performance gap between ZF-EVE/RZF-EVE and ZF/RZF diminishes, and ZF-EVE and RZF-EVE outperform ZF and RZF when there are sufficient DoFs. In terms of the information leakage rate, ZF-EVE, which utilizes its extra DoFs to fully nullify the wiretap channels, is nearly an optimal solution when there are sufficient DoFs, as depicted in Figure 4(b). However, when considering the overall performance, the proposed algorithms exhibit a more balanced and favorable performance.

The sum secrecy rate is evaluated in terms of the number of eavesdroppers M for a fixed transmit power $P=20$ dBm, $N=8$, and $K=4$, as depicted in Figure 5. Figure 5(a) illustrates that the proposed algorithms consistently achieve the highest secrecy rates across different values of M. Furthermore, as the number of eavesdroppers increases, the relative gaps between the proposed algorithms and the other algorithms become larger, highlighting the superior performance of the proposed methods. It is worth noting that for RZF-EVE and ZF-EVE, reducing the spatial DoF margin leads to a decline in secrecy rate performance. This can be observed in Figure 5(b). In terms of minimizing the maximum error

ULSAN NATIONAL INSTITUTE OF
SCIENCE AND TECHNOLOGY



(a) Sum secrecy rate

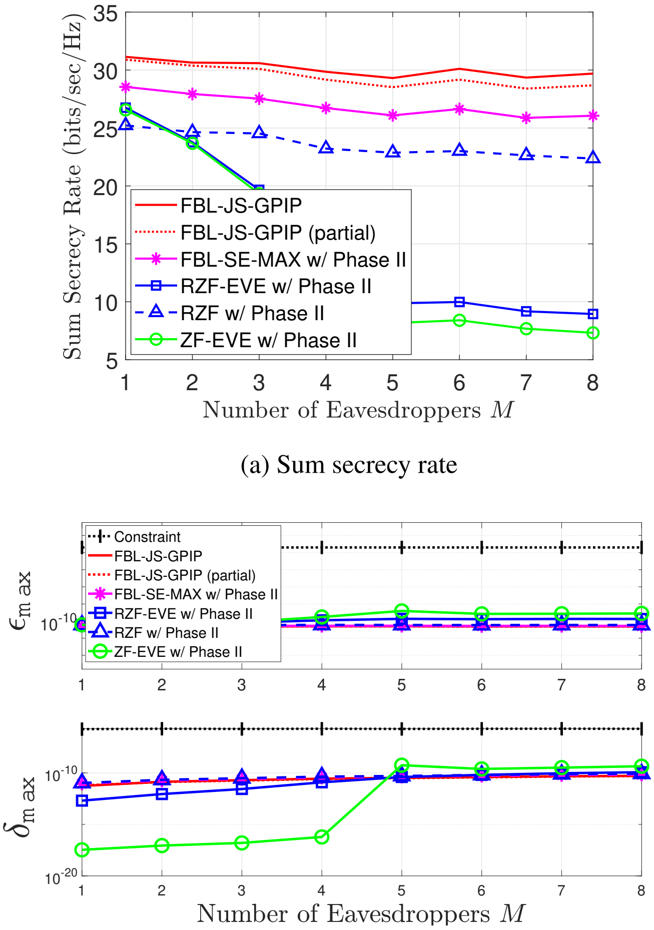
(b) Error probability and information leakage rate

Figure 4: Simulation results of sum secrecy rate, error probability, and information leakage rate with number of AP antennas

probability and leakage rate over M, the proposed algorithms exhibit robust and favorable performance, as shown in Figure 5(b). While ZF-EVE achieves the lowest maximum leakage rate for $M \leq 4$ by fully nullifying the wiretap channels, it suffers from significantly lower secrecy rates and higher leakage rates compared to the proposed algorithms for $M > 4$. In light of these observations, the proposed algorithm is regarded as a potential physical layer security solution that offers robustness in the face of varying numbers of eavesdroppers.

To verify the convergence of the proposed algorithm, both the inner and outer loops of FBL-JS-GPIP are examined using $P \in \{-10, 0, 10, 20\}$ dBm, $N = 8$, $K = 4$, and $M = 4$. The convergence results of the inner loop, corresponding to FBL-S-GPIP, are evaluated based on the approximated objective function $\log_2 \lambda(\bar{\mathbf{f}})$ in (34). Figure 6(a) demonstrates that the proposed algorithm achieves convergence within a maximum of $t_{\max} = 5$ iterations for any transmit power regime. Furthermore, the convergence of the outer loop of FBL-JS-GPIP is assessed in terms of the increment of (49). As depicted in Figure 6(b), the outer loop of the proposed algorithm converges within a maximum of $t_{\max}^{\mathrm{out}} = 2$ outer iterations. Conse-

ULSAN NATIONAL INSTITUTE OF
SCIENCE AND TECHNOLOGY



(a) Sum secrecy rate

(b) Error probability and information leakage rate

Figure 5: Simulation results of sum secrecy rate, error probability, and information leakage rate with number of eavesdroppers

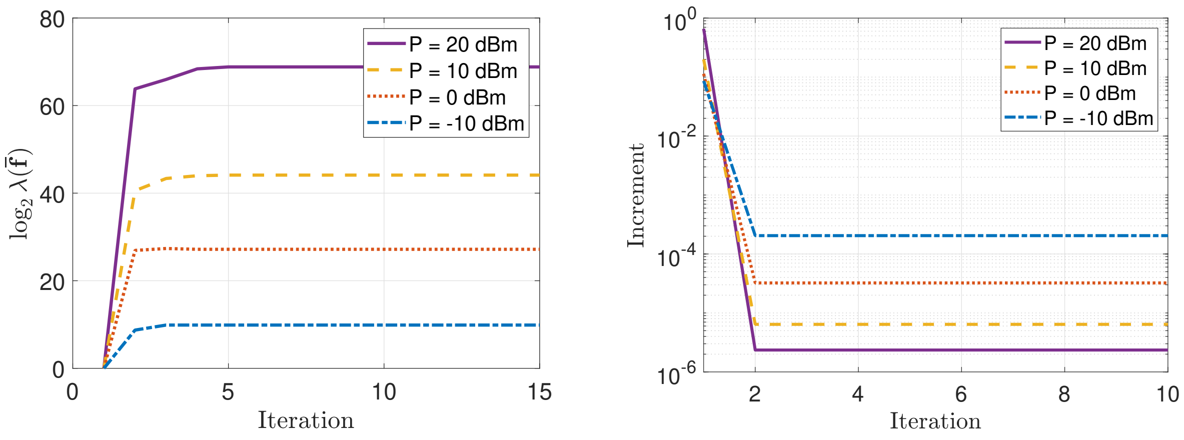


Figure 6: Convergence results of inner and outer loops

quently, it can be concluded that the proposed algorithm ensures fast convergence in practical transmit

ULSAN NATIONAL INSTITUTE OF SCIENCE AND TECHNOLOGY

Table 1: CPU Time in MATLAB for Precoders for $N = 4,\ K = 2,\ M = 2$.

	FBL-JS-GPIP	**WMMSE**	**FBL-SE-MAX**	**RZF-EVE**	**RZF w/o Ph. II**
CPU times (msec)	4.006	14991.797	2.042	0.847	0.428
Comparison (times)	1	3741.869	0.510	0.211	0.107

power regimes. Moreover, it exhibits high potential for practical communications, outperforming other high-complexity precoding algorithms in the FBL regime.

To provide a comprehensive analysis, the CPU time is evaluated using MATLAB for the case of $N = 4$ AP antennas, $K = 2$ users, and $M = 2$ eavesdroppers. The simulation involves FBL-JS-GPIP, benchmark schemes with Phase II (except for RZF), and conventional linear precoders. The simulation is conducted on a workstation equipped with Intel i9-10900K CPU, RTX 3090 GPU, and 64GB RAM. The results are presented in Table 1. As shown in the table, the proposed algorithm, FBL-JS-GPIP, operates within a few milliseconds, demonstrating its computational efficiency. In contrast, the CVX-based WMMSE algorithm requires significantly more CPU time, being approximately 3741 times longer than that of FBL-JS-GPIP. Both FBL-JS-GPIP and FBL-SE-MAX exhibit similar time frames, as they can be executed within milliseconds. It is important to note that conventional linear precoders exhibit shorter computation times compared to FBL-JS-GPIP. However, when considering the performance in terms of sum secrecy rate, maximum error probability, and maximum information leakage rate, FBL-JS-GPIP offers a reasonable computation time while achieving the highest performance, as observed in this simulation.

2.6 Conclusion

In this research, I introduced secure precoding techniques that optimize the sum secrecy rate, decoding error probability, and information leakage within the FBL regime. To address this challenge, I developed a joint optimization framework that considers the finite blocklength channel coding characteristics. To tackle the problem, I divided it into two sub-problems. In the first sub-problem, I proposed a precoding algorithm that maximizes the sum secrecy rate while considering the given error probability and information leakage rate. This was achieved by finding stationary points. For the second sub-problem, I restructured the multi-objective optimization problem into a single-objective problem, focusing on a specific precoder. The ideal error probability and information leakage rate were determined by solving the KKT conditions. By applying alternating optimization, I developed a joint optimization algorithm that significantly improved the tradeoff between security, error probability, and information leakage rate. I also extended the algorithms to handle the scenario where only partial channel knowledge of the wiretap channels is available. Through simulations, I validated the performance of the proposed algorithms in terms of secrecy rate, error probability, and information leakage. The results demonstrated that the proposed methods achieve the highest secrecy performance while meeting the stringent requirements of reliability and security. The algorithms also exhibited fast convergence and high robustness. Overall,

ULSAN NATIONAL INSTITUTE OF SCIENCE AND TECHNOLOGY

the proposed techniques have the potential to play a crucial role in achieving URLLC with high information security. For future research, it would be valuable to explore the impact of imperfect channel state information on both legitimate users and eavesdroppers and to further enhance the computational efficiency of the proposed algorithm.

III Conclusion

This chapter concludes the thesis with a summary of contributions in Section 3.1 and potential future research directions in Section 3.2.

3.1 Summary

In this thesis, I presented the secure transmission strategies to realize upcoming 6G communications. The strategies are based on physical layer security schemes such as beamforming and optimization techniques. To the advanced design for 6G applications, it is also necessary to develop techniques supporting key factors regarding ultra-low latency and ultra-high reliability as well as strong security. To this end, I developed the joint optimization algorithm that offers the optimal balance between the sum secrecy rate and reliability requirements.

Through my thesis, I focused on optimizing the FBL-based secrecy rate maximization problem to mitigate wiretap channel effect and the back-off factor penalty. Due to the fundamentally different consideration in FBL regime, it is important to take into account the non-negligible decoding error probability and information leakage rate. In this regard, I aimed to solve the multi-objective optimization problem with an alternating manner. To this end, I first divided the problem into single-objective optimization problem by employing the weighted-sum approach. Subsequently, I solved each subproblem with reformulation and novel optimization methods. In the first phase, I reformulated the best secure precoding direction problem into a GPI-friendly form with given error probability and information leakage rate. Then, I interpreted the problem as generalized eigenvalue problem, and adopted the generalized power iteration algorithm to find the principal eigenvector which is the best local optimal precoding direction maximizing the sum secrecy rate. In the second phase, for given precoder, I obtained the closed-form solution of error probability and information leakage rate with KKT conditions. The proposed algorithm offers the optimal tradeoff among considered variables while satisfying the stringent reliability and security requirements with fast convergence and high robustness.

3.2 Future Work

In this thesis, I dealt with some of the main critical issues to support MU-MIMO systems with wiretap channels and URLLC. However, there still remain issues that need to be resolved to successfully to realize 6G communication systems. Therefore, I present promising future research directions associated to the topics in this thesis.

- **Imperfect CSIT for both users and eavesdroppers scenario:** Despite of the partial CSIT of wiretap channels in Chapter II, it is desirable to consider the imperfect CSIT for both legitimate users and eavesdroppers. In reality, the channel estimation of eavesdroppers is considered to be generally more difficult than that of legitimate users. Then, the next question would be how to estimate the wiretap channels. I introduce some channel estimation techniques for wiretap channels. (1) Deep learning-based channel estimation: the access point can use deep learning models, such

ULSAN NATIONAL INSTITUTE OF SCIENCE AND TECHNOLOGY

as convolutional neural networks and recurrent neural networks, to estimate both the main channels and the eavesdropper channels. These models can be trained on a large dataset containing various channel realizations and corresponding transmitted and received signals. Once trained, the models can accurately estimate the wiretap channels, enabling the access point to optimize its transmission strategy for secure communication. (2) Blind channel estimation: this approach do not require any known training sequences. Instead, it relies on the statistical properties of the transmitted signal to estimate wiretap channels. However, it can be more complex and computationally demanding than pilot-based techniques. Overall, with these channel estimation methods, it is possible to obtain the high secrecy rate performance, and can further find the optimal tradeoff among precoder, error probability, and information leakage rate in the FBL regime. Therefore, it is necessary to investigate channel estimation for wiretap channels to support MU-MIMO systems under eavesdropping threat.

- **Extension to 6G communication systems:** In relation to various networks, taking account into the multi-beam satellite security scenario presents a promising future research direction. This can be achieved by leveraging the distinct channel characteristics which differ from terrestrial networks. In other non-terrestrial scenarios, UAVs are becoming increasingly popular in various applications. Physical layer security techniques for UAV communications should be carefully selected and designed based on the specific application, communication environment, and potential security threats. Furthermore, reconfigurable intelligent surface (RIS)-aided wireless communication systems are an emerging technology designed to improve the performance and efficiency of wireless networks. By controlling the phase shifts of these elements, the RIS can adaptively shape the propagation environment, enhance the desired signals, and suppress interference or eavesdropping signals, which leads to improved physical layer security. Overall, there still remain crucial to thoroughly consider the physical layer security across diverse scenarios to successfully implement 6G communication systems.

References

[1] Y.-W. P. Hong, P.-C. Lan, and C.-C. J. Kuo, “Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches,” *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 29–40, 2013.

[2] Y. Zou, J. Zhu, X. Wang, and V. C. Leung, “Improving physical-layer security in wireless communications using diversity techniques,” *IEEE Net.*, vol. 29, no. 1, pp. 42–48, 2015.

[3] A. D. Wyner, “The wire-tap channel,” *The Bell Sys. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[4] I. Csiszár and J. Korner, “Broadcast channels with confidential messages,” *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[5] H. Ren, C. Pan, Y. Deng, M. Elkashlan, and A. Nallanathan, “Resource allocation for secure URLLC in mission-critical IoT scenarios,” *IEEE Trans. Commun.*, vol. 68, no. 9, pp. 5793–5807, 2020.

[6] G. Durisi, T. Koch, and P. Popovski, “Toward massive, ultrareliable, and low-latency wireless communication with short packets,” *Proc. IEEE*, vol. 104, no. 9, pp. 1711–1726, 2016.

[7] Y. Polyanskiy, H. V. Poor, and S. Verdú, “Channel coding rate in the finite blocklength regime,” *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2307–2359, 2010.

[8] W. Yang, R. F. Schaefer, and H. V. Poor, “Wiretap channels: Nonasymptotic fundamental limits,” *IEEE Trans. Inf. Theory*, vol. 65, no. 7, pp. 4069–4093, 2019.

[9] Y. Liang and H. V. Poor, “Multiple-access channels with confidential messages,” *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 976–1002, 2008.

[10] A. Khisti, A. Tchamkerten, and G. W. Wornell, “Secure broadcasting over fading channels,” *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2453–2469, 2008.

[11] F. Oggier and B. Hassibi, “The secrecy capacity of the MIMO wiretap channel,” *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, 2011.

[12] R. Liu and H. V. Poor, “Secrecy capacity region of a multiple-antenna Gaussian broadcast channel with confidential messages,” *IEEE Trans. Inf. Theory*, vol. 55, no. 3, pp. 1235–1249, 2009.

ULSAN NATIONAL INSTITUTE OF SCIENCE AND TECHNOLOGY

[13] S. A. A. Fakoorian and A. L. Swindlehurst, “On the optimality of linear precoding for secrecy in the MIMO broadcast channel,” *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1701–1713, 2013.

[14] P. Zhao, M. Zhang, H. Yu, H. Luo, and W. Chen, “Robust beamforming design for sum secrecy rate optimization in MU-MISO networks,” *IEEE Trans. Inf. Forensics and Security*, vol. 10, no. 9, pp. 1812–1823, 2015.

[15] N.-P. Nguyen, H. Q. Ngo, T. Q. Duong, H. D. Tuan, and K. Tourki, “Secure massive MIMO with the artificial noise-aided downlink training,” *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 802–816, 2018.

[16] M. Alageli, A. Ikhlef, and J. Chambers, “SWIPT massive MIMO systems with active eavesdropping,” *IEEE J. Sel. Areas Commun.*, vol. 37, no. 1, pp. 233–247, 2018.

[17] R. Negi and S. Goel, “Secret communication using artificial noise,” in *Proc. IEEE Veh. Technol. Conf.*, vol. 62, no. 3. Citeseer, 2005, p. 1906.

[18] J. Zhu, R. Schober, and V. K. Bhargava, “Linear precoding of data and artificial noise in secure massive MIMO systems,” *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 2245–2261, 2015.

[19] W. Wang, K. C. Teh, and K. H. Li, “Secrecy throughput maximization for MISO multi-eavesdropper wiretap channels,” *IEEE Trans. Inf. Forensics and Security*, vol. 12, no. 3, pp. 505–515, 2016.

[20] H. Qin, X. Chen, Y. Sun, M. Zhao, and J. Wang, “Optimal power allocation for joint beamforming and artificial noise design in secure wireless communications,” in *2011 IEEE Int. Conf. on Commun. Workshops*. IEEE, 2011, pp. 1–5.

[21] Q. Li and L. Yang, “Artificial noise aided secure precoding for MIMO untrusted two-way relay systems with perfect and imperfect channel state information,” *IEEE Trans. Inf. Forensics and Security*, vol. 13, no. 10, pp. 2628–2638, 2018.

[22] C. She, C. Sun, Z. Gu, Y. Li, C. Yang, H. V. Poor, and B. Vucetic, “A tutorial on ultra-reliable and low-latency communications in 6G: Integrating domain knowledge into deep learning,” *arXiv preprint arXiv:2009.06010*, 2020.

[23] D. Xu and H. Zhu, “Proactive eavesdropping via jamming over short packet suspicious communications with finite blocklength,” *IEEE Trans. Commun.*, vol. 70, no. 11, pp. 7505–7519, 2022.

[24] H.-M. Wang, Q. Yang, Z. Ding, and H. V. Poor, “Secure short-packet communications for mission-critical IoT applications,” *IEEE Trans. Wireless Commun.*, vol. 18, no. 5, pp. 2565–2578, 2019.

[25] M. Oh, J. Park, and J. Choi, “Secure Internet-of-Things communications: Joint precoding and power control,” in *IEEE Int. Conf. Commun.*, 2022, pp. 3412–3417.

ULSAN NATIONAL INSTITUTE OF SCIENCE AND TECHNOLOGY

[26] L. Wei, Y. Yang, and B. Jiao, “Secrecy throughput in full-duplex multiuser MIMO short-packet communications,” *IEEE Wireless Commun. Lett.*, vol. 10, no. 6, pp. 1339–1343, 2021.

[27] N. Zhao, D. Li, M. Liu, Y. Cao, Y. Chen, Z. Ding, and X. Wang, “Secure transmission via joint precoding optimization for downlink MISO NOMA,” *IEEE Trans. Veh. Technol.*, vol. 68, no. 8, pp. 7603–7615, 2019.

[28] Z. Xiang, W. Yang, Y. Cai, Z. Ding, Y. Song, and Y. Zou, “NOMA-assisted secure short-packet communications in IoT,” *IEEE Wireless Commun.*, vol. 27, no. 4, pp. 8–15, 2020.

[29] A. Salem, C. Masouros, and B. Clerckx, “Secure rate splitting multiple access: How much of the split signal to reveal?” *IEEE Trans. Wireless Commun.*, 2022.

[30] H. Xia, Y. Mao, X. Zhou, B. Clerckx, S. Han, and C. Li, “Secure beamforming design for rate-splitting multiple access in multi-antenna broadcast channel with confidential messages,” *arXiv preprint arXiv:2202.07328*, 2022.

[31] C. Feng, H.-M. Wang, and H. V. Poor, “Reliable and secure short-packet communications,” *IEEE Trans. Wireless Commun.*, vol. 21, no. 3, pp. 1913–1926, 2021.

[32] M. Zhang, Y. Liu, and R. Zhang, “Artificial noise aided secrecy information and power transfer in OFDMA systems,” *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 3085–3096, 2016.

[33] J. Choi and J. Park, “MIMO design for internet of things: Joint optimization of spectral efficiency and error probability in finite blocklength regime,” *IEEE Internet of Things J.*, vol. 8, no. 20, pp. 15 512–15 521, 2021.

[34] W. Yang, R. F. Schaefer, and H. V. H. Vincent Poor, “Finite-blocklength bounds for wiretap channels,” *IEEE Int. Sym. on Inf. Theory*, pp. 3087–3091, 2016.

[35] J. Scarlett, V. Y. Tan, and G. Durisi, “The dispersion of nearest-neighbor decoding for additive non-Gaussian channels,” *IEEE Trans. Inf. Theory*, vol. 63, no. 1, pp. 81–92, 2016.

[36] S. Schiessl, J. Gross, M. Skoglund, and G. Caire, “Delay performance of the multiuser MISO downlink under imperfect CSI and finite-length coding,” *IEEE J. Sel. Areas Commun.*, vol. 37, no. 4, pp. 765–779, 2019.

[37] R. T. Marler and J. S. Arora, “Survey of multi-objective optimization methods for engineering,” *Structural and multidisciplinary optimization*, vol. 26, no. 6, pp. 369–395, 2004.

[38] C. Shen and H. Li, “On the dual formulation of boosting algorithms,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 32, no. 12, pp. 2216–2231, Mar. 2010.

[39] M. Bloch, J. Barros, M. R. Rodrigues, and S. W. McLaughlin, “Wireless information-theoretic security,” *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

ULSAN NATIONAL INSTITUTE OF
SCIENCE AND TECHNOLOGY

[40] J. Choi, N. Lee, S.-N. Hong, and G. Caire, "Joint user selection, power allocation, and precoding design with imperfect CSIT for multi-cell MU-MIMO downlink systems," *IEEE Trans. Wireless Commun.*, vol. 19, no. 1, pp. 162–176, 2019.

[41] S. S. Christensen, R. Agarwal, E. D. Carvalho, and J. M. Cioffi, "Weighted sum-rate maximization using weighted MMSE for MIMO-BC beamforming design," *IEEE Trans. Wireless Commun.*, vol. 7, no. 12, pp. 4792–4799, Dec. 2008.

[42] W. Mei, Z. Chen, L. Li, J. Fang, and S. Li, "On artificial-noise-aided transmit design for multiuser MISO systems with integrated services," *IEEE Trans. Veh. Technol.*, vol. 66, no. 9, pp. 8179–8195, Dec. 2017.

[43] G. Shi, Y. Li, W. Cheng, X. Gao, and W. Zhang, "An artificial-noise-based approach for the secrecy rate maximization of MISO VLC wiretap channel with multi-eves," *IEEE Access*, vol. 9, pp. 651–659, Dec. 2020.

[44] V.-D. Nguyen, T. Q. Duong, O. A. Dobre, and O.-S. Shin, "Joint information and jamming beamforming for secrecy rate maximization in cognitive radio networks," *IEEE Trans. Inf. Forensics and Security*, vol. 11, no. 11, pp. 2609–2623, 2016.

[45] M. Haghifam, M. R. Mili, B. Makki, M. Nasiri-Kenari, and T. Svensson, "Joint sum rate and error probability optimization: Finite blocklength analysis," *IEEE Wireless Commun. Lett.*, vol. 6, no. 6, pp. 726–729, 2017.

[46] S. Boyd and L. Vandenberghe, *Convex optimization*. Cambridge university press, 2004.

[47] H. Joudeh and B. Clerckx, "Sum-rate maximization for linearly precoded downlink multiuser MISO systems with partial CSIT: A rate-splitting approach," *IEEE Trans. Commun.*, vol. 64, no. 11, pp. 4847–4861, 2016.

[48] Q. Zhang, S. Jin, K.-K. Wong, H. Zhu, and M. Matthaiou, "Power scaling of uplink massive MIMO systems with arbitrary-rank channel means," *IEEE J. Sel. Topics Signal Process.*, vol. 8, no. 5, pp. 966–981, 2014.

[49] A. Dalir and H. Aghaeinia, "Maximizing first-order approximate mean of SINR under imperfect channel state information for throughput enhancement of MIMO interference networks," *Iranian J. of Science and Technol., Trans. Elec. Engineering*, vol. 43, no. 1, pp. 121–132, 2019.

[50] X. Zhao, S. Geng, and B. M. Coulibaly, "Path-loss model including LOS-NLOS transition regions for indoor corridors at 5 GHz [wireless corner]," *IEEE Antennas Propag. Mag.*, vol. 55, no. 3, pp. 217–223, Jun. 2013.

[51] A. Adhikary, J. Nam, J.-Y. Ahn, and G. Caire, "Joint spatial division and multiplexing—The large-scale array regime," *IEEE Trans. Inf. Theory*, vol. 59, no. 10, pp. 6441–6463, 2013.

ULSAN NATIONAL INSTITUTE OF
SCIENCE AND TECHNOLOGY