Joint Optimization for Secure and Reliable Communications in Finite Blocklength Regime

Mintaek Oh\textsuperscript{a}, Graduate Student Member, IEEE, Jeonghun Park\textsuperscript{b}, Member, IEEE, and Jinseok Choi\textsuperscript{c}, Member, IEEE

Abstract—To realize ultra-reliable low latency communications with high spectral efficiency and security, we investigate a joint optimization problem for downlink communications with multiple users and eavesdroppers in the finite blocklength (FBL) regime. We formulate a multi-objective optimization problem to maximize a sum secrecy rate by developing a secure precoder and to minimize a maximum error probability and information leakage rate. The main challenges arise from the complicated multi-objective problem, non-tractable back-off factors from the FBL assumption, non-convexity and non-smoothness of the secrecy rate, and the intertwined optimization variables. To address these challenges, we adopt an alternating optimization approach by decomposing the problem into two phases: secure precoding design, and maximum error probability and information leakage rate minimization. In the first phase, we obtain a lower bound of the secrecy rate and derive a first-order Karush-Kuhn-Tucker (KKT) condition to identify local optimal solutions with respect to the precoders. Interpreting the condition as a generalized eigenvalue problem, we solve the problem by using a power iteration-based method. In the second phase, we adopt a weighted-sum approach and derive KKT conditions in terms of the error probabilities and leakage rates for given precoders. Simulations validate the proposed algorithm.

Index Terms—Physical layer security, finite blocklength, secure precoding, error probability and information leakage rate minimization, alternating optimization.

I. INTRODUCTION

ULTRA-RELIABLE low latency communications (URLLC) have inevitably become one of the primary usage scenarios in realizing 5G and 6G communications [2], [3], [4]. To support delay-sensitive communications, a short-packet transmission is often taken into account [5], [6], [7], [8]. Unlike conventional communications that mainly consider the infinite blocklength coding regime, the finite blocklength (FBL) based communications is more suitable to leverage the benefit of short data packet transmission [9]. The communication in the FBL regime, however, is limited by a back-off factor determined by non-negligible decoding error probability and blocklength [10]. Accordingly, the existing transmission strategies with infinite blocklength becomes far less optimal in the FBL regime and thus, delay-constrained applications need to carefully consider the reliability issue as well as the latency; optimizing the per-user error probability plays a key role in achieving the high throughput with low latency in the FBL regime [11].

In addition, information security has become a critical issue for future wireless networks to protect confidential information from eavesdroppers. Since the wireless communication systems are highly likely to be vulnerable to eavesdropping due to the broadcast nature of wireless communications [12], the importance of security has been gaining more attention [13], [14]. Considering the complexity issues, physical layer security (PLS) has been considered as a promising solution for secure communications [12], [15]. The maximal secret communication rate called the secrecy rate has been characterized at which information can be transmitted securely and reliably over a wiretap channel [16], [17]. In spite of the broad investigation on the PLS methods, it is inappropriate to directly apply the existing solutions when communication systems operate in the FBL regime due to the additional back-off factor from the FBL penalty in PLS [18], [19], [20]. In this regard, we investigate PLS for downlink FBL-based communications.

A. Prior Work

PLS has been widely studied in wireless communication systems. For the case of multiple users and a single eavesdropper in multiple-input single-output (MISO) wireless networks, suboptimal precoding solutions were proposed in previous works. A secure precoding that maximizes a sum secrecy spectral efficiency (SE) with suboptimal scheduling was proposed in [21]. In [22], a secrecy rate optimization was proposed for maximizing the MISO network’s energy efficiency in terms of users’ quality-of-service (QoS). For a multiple-input multiple-output (MIMO) system, the secrecy SE with multiple eavesdroppers equipped with multiple antennas was...
investigated in [23]. Furthermore, in [24], a secure precoding algorithm was proposed in MIMO broadcasting channels for a simultaneous wireless information and power transfer system. For a multi-user multi-eavesdropper network, a secure transmission strategy was proposed in [25]. Specifically, in [25], an artificial noise (AN)-aided secure precoding was considered to maximize the secrecy throughput by addressing the leakage signal from non-colluding eavesdroppers. Moreover, there exists prior work incorporating a scenario of colluding eavesdroppers [26].

Based on the analytical finding of the maximal channel coding rate at the FBL [10], there have been several works that analyzed accurate information-theoretic approximations of the achievable rates in the FBL regime [27], [28], [29]. Leveraging the results in the FBL regime, in [30] and [31], resource allocation was investigated to maximize the sum rate and to assist the short-packet communication subject to QoS constraints for URLLC users. In addition, the decoding error probability also needs to be considered in advanced wireless communication techniques incorporating reliable and real-time services. In this regard, the joint optimization of SE and error probability in the FBL regime is needed to cope with the stringent requirements of URLLC. The joint optimization problem in [32] was solved by using an alternation optimization framework between the sum SE maximization and error probability minimization.

Recent studies have also analyzed PLS in the FBL regime [18], [19]. In [19], the maximal secret communication rate over a wiretap channel in the FBL regime, i.e., the secrecy rate, was derived. According to the fundamental results, it was observed that there exist tradeoffs among delay, reliability, and security. In this regard, the wireless communication techniques need to be further investigated for improving the secrecy rate in the FBL regime [33]. To find the optimal tradeoff, state-of-the-art precoding methods were proposed to improve the secrecy rate under the reliability and security constraints. For the case of a single user and eavesdropper, analytical frameworks of the FBL-based secure communications were investigated in [34] and [35]. Specifically, in [34], the performance of FBL-based communications in the presence of an eavesdropper was investigated, and the optimal block-length in maximizing secrecy throughput was also analyzed by using the AN-aided maximum ratio transmission precoding. For full-duplex MIMO short-packet systems, [36] proposed the secure precoding method based on zero-forcing (ZF) to maximize the sum secrecy rate. Extension to a single-user and multi-eavesdropper scenario in the FBL regime, the optimal blocklength maximizing the secrecy throughput and the AN allocation eliminating the wiretap effect were considered in [37]. From [38], an outage probability considering both reliability and security was proposed according to the characteristics of FBL-based secure communications. In our previous work [1], we proposed an efficient secure precoding algorithm for downlink communications with multiple users and a single eavesdropper.

Although the prior works investigated the secure communications in the FBL regime, the single-eavesdropper scenario is mainly considered. In addition, the prior work provided theoretical analysis and made an effort of maximizing the achievable secrecy rate with the conventional linear precoders. In this regard, thorough optimization of transmission for FBL-based secure communications under the reliability and security constraints for the general multi-user multi-eavesdropper MIMO network is still missing. It is, however, challenging to solve the optimization problem for such sophisticated networks. In addition, we note that solving the sum secrecy rate optimization problem is already non-convex and difficult to solve [39], and the back-off factors entangled with the secrecy rate make the problem more challenging [19]. Besides, it is infeasible to find direct solutions with the multi-objectives [32]. Overcoming the aforementioned challenges, we put forth a novel secure precoding method that brings the optimal tradeoff among rate, reliability, and security in the FBL regime.

B. Contributions

In this paper, we consider the FBL-based downlink secure communication systems where an access point (AP) with multiple antennas serves multiple users while multiple eavesdroppers attempt to wiretap the user messages. Our contributions are summarized as follows:

- Based on the characteristics of FBL-based communications, we adopt the secrecy rate as our key performance metric. Using the secrecy rate, we formulate a sum secrecy rate maximization problem to jointly optimize (i) a precoding matrix, and (ii) error probability and information leakage rate. However, there exist several challenges in solving the formulated optimization problem. First, the problem is inherently non-convex and thus, finding a global optimal solution is infeasible. Second, the formulated problem is a multi-objective optimization, and also each user has error probability and information leakage constraints determined by the system reliability requirements. Third, the secrecy rate is not tractable due to the back-off factors which are functions of optimization variables intertwined with each other. Finally, the sum secrecy rate is non-smooth since the secrecy rate under the presence of multiple eavesdroppers is determined by the maximum wiretap channel rate.

- To resolve aforementioned difficulties, we first decompose the problem into two phases adopting alternating optimization: the secrecy rate maximization precoding design and the maximum error probability and information leakage rate minimization. In the first phase, for given error probability and leakage rate, we apply a smooth approximation to a non-smooth objective function. Then, we make the problem a more tractable form by deriving a lower bound of the secrecy rate. Due to non-convexity of the problem, we derive a first-order KKT condition which can be interpreted as a generalized eigenvalue problem and hence, the best local optimal precoder can be found by finding its principal eigenvector. It can be solved by a power iteration-based precoding method. In the second phase, we reformulate the multi-objective optimization problem into a single-objective optimization problem by using a
weighted-sum approach for a given precoder. Since the problem is still not tractable due to the maximum function in the secrecy rate, we further consider the lower bound of the objective function and optimize the maximum error probability and information leakage rate by solving KKT conditions.

- We note that obtaining the instantaneous channel state information at a transmitter (CSIT) of eavesdroppers is challenging. Hence, we consider the case of the partial CSIT of wiretap channels which is regarded as a more practical scenario. Assuming that only the wiretap channel covariance is available at the AP, we reformulate the problem by deriving an approximated lower bound of the secrecy rate which can be handled by using the channel covariance. Then, we follow similar steps as for the perfect CSIT case and develop a joint precoder, error probability and information leakage rate optimization algorithm under the partial CSIT of wiretap channels.
- Via simulations, we verify the rate, reliability, and security performances of the proposed joint optimization methods. In particular, we demonstrate that the proposed algorithm achieves the highest secrecy rate while keeping the lowest maximum error probability and information leakage rate in various scenarios compared to baseline methods. Therefore, it is concluded that the proposed algorithms are beneficial to the FBL-based secure communications under the strict requirement of the reliability and security for future wireless applications.

**Notation:** $A$ is a matrix and $a$ is a column vector. The superscripts $(\cdot)^T$, $(\cdot)^H$, and $(\cdot)^{-1}$ denote the transpose, Hermitian, and matrix inversion, respectively. The blackboard bold symbols $\mathbb{C}$, $\mathbb{R}_+$, and $\mathbb{N}_+$ denote the complex, nonnegative real, and nonnegative integer domains, respectively. $I_N$ is the identity matrix with size $N \times N$. Assuming that $A_1, \ldots, A_N \in \mathbb{C}^{K \times K}$, $A = \text{blkdiag}(A_1, \ldots, A_N) \in \mathbb{C}^{KN \times KN}$ is a block diagonal matrix. $\|A\|$ represents L2 norm. We use $\text{tr}(\cdot)$ for trace operator, $\text{vec}(\cdot)$ for vectorization, and $I(a, b)$ is a uniform distribution with two boundaries $a$ and $b$. We also follow MATLAB style notation.

II. SYSTEM MODEL

We consider a downlink network in which the 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, we assume the FBL channel coding, i.e., the coding length is $L \ll \infty$. We denote a user set and an eavesdropper set as $\mathcal{K} = \{1, \ldots, K\}$ and $\mathcal{M} = \{1, \ldots, M\}$, respectively. The data symbol for user $k$, $s_k$, is drawn from a Gaussian distribution with a zero mean and variance of $\mathbb{E}[|s_k|^2] = P$, $\forall k \in \mathcal{K}$. The AP broadcasts the data symbols $s_k, \forall k \in \mathcal{K}$ to each legitimate user through a linear precoder $F = [f_1, \ldots, f_K] \in \mathbb{C}^{N \times K}$, where $f_k \in \mathbb{C}^{N}$ indicates a precoding vector for $s_k$. Then a transmitted signal vector $x \in \mathbb{C}^N$ is

$$x = \sum_{k=1}^{K} f_k s_k = Fs,$$

where $s = [s_1, \ldots, s_K]^T \in \mathbb{C}^K$. After transmission, a received signal of user $k$ is given by

$$y_k = \sqrt{\gamma_k} h_k^H f_k s_k + \sum_{\ell \neq k, \ell = 1}^{K} \sqrt{\gamma_{\ell}} h_\ell^H f_\ell s_\ell + n_k,$$

where $\gamma_k$ and $h_k \in \mathbb{C}^N$ are the large-scale channel fading term and small-scale channel fading vector between the AP and user $k$, respectively, and $n_k$ is an additive white Gaussian noise (AWGN) at user $k$ with a zero mean and variance of $\sigma_n^2$. Similarly, the large-scale channel fading term and small-scale channel fading vector between the AP and eavesdropper $m$ are represented as $\gamma_m^e$ and $g_m \in \mathbb{C}^N$, respectively. Then, the received signal at eavesdropper $m$ is

$$y_m^e = \sum_{\ell = 1}^{K} \sqrt{\gamma_m^e g_m^H f_\ell} s_\ell + n_m^e,$$

where $n_m^e$ is the AWGN noise at the eavesdropper $m$ with a zero mean and variance of $\sigma_e^2$. We assume the perfect CSIT for both the legitimate users and eavesdroppers. We then extend our method to a partial CSIT case.

III. PROBLEM FORMULATION

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

$$R_k = \log_2 (1 + \rho_k^f),$$

where $\rho_k^f$ is the signal-to-interference-plus-noise ratio (SINR) of user $k$ defined as

$$\rho_k^f = \frac{\gamma_k |h_k^H f_k|^2}{\sum_{\ell \neq k, \ell = 1}^{K} \gamma_\ell |h_\ell^H f_\ell|^2 + \sigma^2 / P}.$$

The achievable rate of eavesdropper $m$ for $s_k$ is

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

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

$$\rho_{m,k}^e = \frac{\gamma_m^e |g_m^H f_k|^2}{\sum_{\ell \neq m, \ell = 1}^{K} \gamma_\ell |g_\ell^H f_k|^2 + \sigma_e^2 / P}.$$

According to [18] and [19], the secrecy rate which measures the maximum rate transmission of the confidential information that any eavesdropper cannot decode in the FBL regime is given as

$$R_k^{sec}(F, \epsilon_k, \delta_m; L) = R_k - \sqrt{\frac{V_k}{L}} Q^{-1} (\epsilon_k) - \max_{m \in \mathcal{M}} \left\{ R_{m,k}^e + \sqrt{\frac{V_{m,k}}{L}} Q^{-1} (\delta_m) \right\},$$

where $V_{m,k}$ and $V_k$ are channel dispersion factors that depend on the stochastic variations of the legitimate and the wiretap channels, respectively [10], [19]. $Q^{-1}(\cdot)$ denotes an inverse Q-function defined as $Q(x) = \frac{1}{\sqrt{2\pi}} \int_{x}^{\infty} e^{-t^2} dt$, $\epsilon_k$ is the decoding error probability of user $k$, and $\delta_m$ is the secrecy constraint on the information leakage of $s_k$ from eavesdropper $m$ [19]. Note that if the blocklength $L$ goes to infinity, then the
secrecy rate in (8) is sufficiently close to the classic secrecy SE. Thus, back-off factors in (8), i.e., $\sqrt{\frac{L}{Q}Q^{-1}(\epsilon_k)}$ and $\sqrt{\frac{m_kL}{Q}Q^{-1}(\delta_{m,k})}$, play as a drawback which reduces 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 [40], [41], the channel dispersion factors become

$$\mathcal{N}_k = \mathcal{N}^{i.i.d.}(\rho_k) = \frac{2\rho_k}{1 + \rho_k} (\log_2 e)^2,$$

$$\mathcal{N}^{i.i.d.}(\rho^{e}_{m,k}) = \frac{2\rho^{e}_{m,k}}{1 + \rho^{e}_{m,k}} (\log_2 e)^2.$$  

(9) (10)

Now, we let the predetermined maximum error probability and information leakage constraints as $\epsilon_k$ and $\delta_{m,k}, \forall k \in \mathcal{K}$, respectively. Defining $\epsilon = [\epsilon_1, \cdots, \epsilon_K]^T \in \mathbb{R}_+^K$ and $\Delta = [\delta_1, \cdots, \delta_K] \in \mathbb{R}_+^{M \times K}$, where $\delta_k = [\delta_{1,k}, \cdots, \delta_{M,k}]^T \in \mathbb{R}_+^{M \times K}$, we formulate a joint optimization problem to maximize the sum secrecy rate and to minimize the maximum error probability and information leakage rate as

$$\max_{\mathcal{F}, \epsilon, \Delta} \sum_{k=1}^{K} R^{sec}_k(\mathcal{F}, \epsilon, \Delta; L)$$

subject to

$$\epsilon_k \leq \epsilon_k, \forall k \in \mathcal{K},$$

$$\delta_{m,k} \leq \delta_{m,k}, \forall m \in \mathcal{M}, \forall k \in \mathcal{K},$$

(11) (12) (13) (14) (15) (16)

where (12) and (13) are the error probability and information leakage rate constraints, and (14) is a transmit power constraint at the AP, respectively. The main challenges in solving the optimization problem are: 1) the problem is the multi-objective optimization, 2) the objective function in (11) is not tractable due to the maximum function which is non-smooth, 3) the problem is inherently non-convex, and 4) the error probability and information leakage need to be considered in the constraints and they are intertwined with the secrecy rate as parameters of the back-off factors. A reasonable solution to the multi-objective problem investigates a set of solutions, each of which satisfies the objectives at an acceptable level without being dominated by any other solution [42]. Therefore, we propose a joint optimization method to solve the multi-objective problem with a reasonable tradeoff.

IV. PROPOSED JOINT OPTIMIZATION METHOD

In this section, we develop a novel optimization method for solving the problem in (11) by employing an alternating optimization approach. We first begin with obtaining the secure precoder that maximizes the sum secrecy rate for given error probabilities and information leakage rates, and then solve the minimization problem in terms of the maximum error probability and information leakage rate for the obtained precoder.

A. Phase I: Sum Secrecy Rate Maximization

In this phase, we find the optimal precoder that maximizes the sum secrecy rate while fixing $\epsilon_k$ and $\delta_{m,k}, \forall k \in \mathcal{K}, \forall m \in \mathcal{M}$. Since the objective function in (11) is not smooth, it is necessary to make (8) smooth to find a more tractable form. To this end, we first adopt a LogSumExp technique [43] to approximate the maximum function with a parameter $\alpha$ as

$$\max_{i=1, \cdots, N} \{ x_i \} \approx \frac{1}{\alpha} \ln \left( \sum_{i=1}^{N} \exp(\alpha x_i) \right), \quad (17)$$

where the approximation becomes tight as $\alpha \to \infty$. Applying (17) to (8), we have

$$\max_{m \in \mathcal{M}} R^{sec}_{m,k} + \frac{\sqrt{\mathcal{N}_{m,k}}}{L} Q^{-1}(\delta_{m,k}) \log_2 e$$

$$\approx \frac{1}{\alpha} \ln \left( \sum_{m=1}^{M} (1 + \rho^{e}_{m,k}) \right)$$

$$\times \exp \left( \alpha \log_2 e + \frac{2\rho^{e}_{m,k}}{L(1 + \rho^{e}_{m,k})} Q^{-1}(\delta_{m,k}) \log_2 e \right)$$

$$= \tilde{R}^{\epsilon}_{k}.$$  

(18) (19)

Now, we introduce the following lemma [32]:

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

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

(20)

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

Proof: Refer to the proof of Lemma 2 in [32].

Based on Lemma 1 with (19), we can obtain the lower bound of the approximated secrecy rate. For given $\tilde{\rho}_k$ and $\tilde{\rho}^{e}_{m,k}$, the lower bound of (8) is obtained as

$$R^{sec}_{k} \approx \tilde{R}^{\epsilon}_{k} - \sqrt{\frac{2\rho_k}{L(1 + \rho_k)} Q^{-1}(\epsilon_k) \log_2 e} - \tilde{R}^{\epsilon}_{k}$$

$$\geq \log_2 (1 + \rho_k) + Q^{-1}(\epsilon_k) q(\tilde{\rho}_k) \ln(1 + \rho_k) \log_2 e - \psi_k$$

$$- \frac{1}{\alpha} \ln \left( \sum_{m=1}^{M} (1 + \rho^{e}_{m,k}) \frac{\rho^{e}_{m,k}}{Q^{-1}(\delta_{m,k})} \right)$$

$$\times \exp \left( \ln(1 + \rho^{e}_{m,k}) + \frac{\psi^{\epsilon}_{m,k}}{Q^{-1}(\delta_{m,k})} \right)$$

$$= \log_2 (1 + \rho_k)^{\omega_{k}} - \psi_k - \frac{1}{\alpha} \ln \left( \sum_{m=1}^{M} \beta_{m,k} (1 + \rho^{e}_{m,k}) \omega^{\epsilon}_{m,k} \right)$$

$$= \tilde{R}^{sec,lb}_{k},$$

(21) (22)
where (a) comes from (19), (b) follows from Lemma 1, and
\[
\psi_k = \frac{Q^{-1}(\epsilon_k)}{\sqrt{L}} \log_2 e \cdot r(\tilde{\rho}_k),
\]
\[
\psi_{\epsilon, m, k} = \frac{Q^{-1}(\delta_{m, k})}{\sqrt{L}} \log_2 e \cdot r(\tilde{\rho}_{\epsilon, m, k}),
\]
\[
\omega_k = 1 - \frac{Q^{-1}(\epsilon_k)}{\sqrt{L}} \cdot q(\tilde{\rho}_k),
\]
\[
\omega_{\epsilon, m, k} = \frac{\alpha}{\ln 2} \left( 1 + \frac{Q^{-1}(\delta_{m, k})}{\sqrt{L}} \cdot q(\tilde{\rho}_{\epsilon, m, k}) \right),
\]
\[
\beta_{m, k} = \exp \left( \alpha \psi_{\epsilon, m, k} \right).
\]

Since we pursue to solve (11) for given \( \epsilon \) and \( \Delta \) with the lower bound in (22), our problem is transformed to the single-objective maximization problem as
\[
\text{maximize } \sum_{k=1}^{K} R_{k, \text{sec, lb}}(F),
\]
subject to \( \text{tr} (FF^H) \leq 1 \). (23)

Next, to further obtain a compact rate expression with respect to the precoder, we vectorize the precoding matrix as
\[
\tilde{f} = \text{vec}(F) = [f_1^T, f_2^T, \ldots, f_K^T]^T \in \mathbb{C}^{NK}. \quad (25)
\]

It has been observed in previous works on secrecy rate that increasing the transmit power in general improves the secrecy rate [44]. In addition, it is obvious that the channel capacity increases with the transmit power for a given channel coding blocklength. In this regard, we set \( \|\tilde{f}\|^2 = 1 \), i.e., transmission with the maximum power to maximize the secrecy rate. Then, we can finally reformulate the problem in (23) as the product of Rayleigh quotients:
\[
\text{maximize } \sum_{k=1}^{K} \log_2 \left( \frac{\tilde{f}^H A_k \tilde{f}}{\tilde{f}^H B_k \tilde{f}} \right) \omega_k - \ln \left( \sum_{m=1}^{M} \beta_{m, k} \left( \frac{\tilde{f}^H C_m \tilde{f}}{\tilde{f}^H D_m \tilde{f}} \right)^{\omega_{\epsilon, m, k}} \right)^{\frac{1}{\omega_k}},
\]
(26)

where
\[
A_k = \text{blkdiag}(\gamma_0 h_k h_k^H, \ldots, \gamma_{L-1} h_k h_k^H) + I_{NK} \frac{\sigma^2}{P} \in \mathbb{C}^{NK \times NK},
\]
\[
B_k = A_k - \text{blkdiag}(0, \ldots, \gamma_0 h_k h_k^H, \ldots, 0) \in \mathbb{C}^{NK \times NK},
\]
\[
C_m = \text{blkdiag}(\gamma_{\ell} g_m g_m^H, \ldots, \gamma_{L-1} g_m g_m^H) + I_{NK} \frac{\sigma^2}{P} \in \mathbb{C}^{NK \times NK},
\]
\[
D_{m, k} = C_m - \text{blkdiag}(0, \ldots, \gamma_{\ell} g_m g_m^H, \ldots, 0) \in \mathbb{C}^{NK \times NK}.
\]

The second terms in both (28) and (30) have nonzero blocks which are located at the \( k \)th diagonal block. We note that the product of Rayleigh quotient forms in (26) is derived under the assumption \( \|\tilde{f}\|^2 = 1 \), and the problem in (26) is invariant up to the scaling of \( \tilde{f} \). Accordingly, the power constraint in (24) is removed in the reformulated problem.

Now, we focus on identifying the local points of the problem in (26). For simplicity, we define the objective function in (26) as
\[
L_1(\tilde{f}) = \log_2 \prod_{k=1}^{K} \left( \frac{\tilde{f}^H A_k \tilde{f}}{\tilde{f}^H B_k \tilde{f}} \right) \omega_k \left( \sum_{m=1}^{M} \beta_{m, k} \left( \frac{\tilde{f}^H C_m \tilde{f}}{\tilde{f}^H D_m \tilde{f}} \right)^{\omega_{\epsilon, m, k}} \right)^{-\frac{\ln 2}{\omega_k}}
\]
(31)
\[
\omega = \log_2 \lambda(\tilde{f}). \quad (32)
\]

Then, we derive Lemma 2 to find the condition of stationary points of (31).

Lemma 2: The first-order KKT condition of the problem (26) is satisfied if
\[
B_{\text{KKT}}(\tilde{f}) A_{\text{KKT}}(\tilde{f}) \tilde{f} = \lambda(\tilde{f}) \tilde{f},
\]
(33)
where
\[
A_{\text{KKT}}(\tilde{f}) = \lambda_{\text{num}}(\tilde{f}) \cdot \sum_{k=1}^{K} \left[ \frac{\omega_k}{\ln 2} \left( \frac{A_k}{\tilde{f}^H A_k \tilde{f}} \right) \right] - \frac{1}{\alpha} \sum_{m=1}^{M} \left( \frac{\omega_{\epsilon, m, k}}{\ln 2} \left( \frac{C_m}{\tilde{f}^H D_m \tilde{f}} \right) \right) \tilde{f}^H D_m \tilde{f},
\]
(34)
\[
B_{\text{KKT}}(\tilde{f}) = \lambda_{\text{den}}(\tilde{f}) \cdot \sum_{k=1}^{K} \left[ \frac{\omega_k}{\ln 2} \left( \frac{B_k}{\tilde{f}^H B_k \tilde{f}} \right) \right] + \frac{1}{\alpha} \sum_{m=1}^{M} \left( \frac{\omega_{\epsilon, m, k}}{\ln 2} \left( \frac{C_m}{\til{f}^H D_m \til{f}} \right) \right) \til{f}^H D_m \til{f},
\]
(35)
\[
\lambda_{\text{num}}(\til{f}) = \prod_{k=1}^{K} \left( \frac{\til{f}^H A_k \til{f}}{\til{f}^H B_k \til{f}} \right)^{\omega_k},
\]
(36)
\[
\lambda_{\text{den}}(\til{f}) = \prod_{k=1}^{K} \left( \sum_{m=1}^{M} \beta_{m, k} \left( \frac{\til{f}^H C_m \til{f}}{\til{f}^H D_m \til{f}} \right)^{\omega_{\epsilon, m, k}} \right)^{-\frac{\ln 2}{\omega_k}}.
\]
(37)

Proof: See Appendix A. \( \blacksquare \)

We note that the first-order KKT condition in (33) can be interpreted as a generalized eigenvalue problem \( B_{\text{KKT}}^{-1}(\til{f}) A_{\text{KKT}}(\til{f}) \til{f} = \lambda(\til{f}) \til{f} \). Here, \( \lambda(\til{f}) \) is an eigenvalue of \( B_{\text{KKT}}^{-1}(\til{f}) A_{\text{KKT}}(\til{f}) \) with \( \til{f} \) as a corresponding eigenvector. As a result, maximizing the objective function \( L_1(\til{f}) \) is equivalent to maximizing \( \lambda(\til{f}) \). Therefore, it is desirable to find the principal eigenvalue of (33) to maximize (32), which is equivalent to finding the best local optimal solution of (26).

Based on (33), we propose the sum secrecy rate maximization precoding algorithm by adopting the generalized power iteration (GPI) method [45]. As described in Algorithm 1, we initialize \( \til{f}^{(0)} \) and update \( \til{f}^{(t)} \) at each iteration; with the given \( L, \epsilon, \) and \( \Delta \), the algorithm builds \( A_{\text{KKT}}(\til{f}^{(t-1)}) \) and \( B_{\text{KKT}}(\til{f}^{(t-1)}) \) according to (34) and (35). Then, the algorithm updates \( \til{f}^{(t)} \) by computing \( \til{f}^{(t)} = B_{\text{KKT}}^{-1}(\til{f}^{(t-1)}) A_{\text{KKT}}(\til{f}^{(t-1)}) \til{f}^{(t-1)} \) and normalizing as
Algorithm 1 Sum Secrecy Rate Maximization

1. initialize: $\tilde{f}^{(0)}$, $t = 1$.
2. while $\|\tilde{f}^{(t)} - \tilde{f}^{(t-1)}\| > \varepsilon$ & $t \leq t_{\text{max}}$ do
3. Build $A_{\text{KKT}}(\tilde{f}^{(t-1)})$ and $B_{\text{KKT}}(\tilde{f}^{(t-1)})$ according to (34) and (35) for given $\epsilon_k$ and $\delta_{m,k}$.
4. Compute $\tilde{f}^{(t)} = B_{\text{KKT}}^{-1}(\tilde{f}^{(t-1)}) A_{\text{KKT}}(\tilde{f}^{(t-1)}) \tilde{f}^{(t-1)}$.
5. Normalize $\tilde{f}^{(t)} = \tilde{f}^{(t)}/\|\tilde{f}^{(t)}\|$.
6. $t \leftarrow t + 1$.
7. if $\tilde{f}^{(1)} < \tilde{f}^{(t-1)}$ then $\tilde{f}^{*} = [\tilde{f}_1^{(t)}, \tilde{f}_2^{(t)}, \ldots, \tilde{f}_K^{(t)}]^T$.

The complexity of Algorithm 1 is dominated by the inversion in $B_{\text{KKT}}^{-1}(\tilde{f})$. Since $B_{\text{KKT}}^{-1}(\tilde{f})$ is a block-diagonal and symmetric matrix, we implement the inversion by exploiting a divide-and-conquer method so that we only need a computational complexity order of $O\left(\frac{1}{4}TKN^3\right)$ [45] instead of $O\left(K^3N^3\right)$. In this regard, the total complexity is $O\left(\frac{1}{4}TKN^3\right)$, where $T$ is the number of iterations. We note that the complexity of Algorithm 1 is same as a representative low-complexity framework in sum rate maximization (not even secrecy rate), namely, the weighted minimum mean square error (WMMSE) method [46]. In [47], a AN-aided transmission method was proposed based on a sequence of semi-definite programs (SDP) needs a computational complexity order of $O\left(N^{6.5}\right)$ for a single confidential message. In [48], the SDP-based algorithm was also proposed for a single user and multiple eavesdroppers with a complexity order of $O\left(N^{5.5}\right)$. In addition, a jamming noise-aided precoding algorithm was developed for multiple users and eavesdroppers, which needs a complexity order of $O\left((N + K)^3\right)$ [49]. Thus, we emphasize that the complexity of Algorithm 1 is low compared to the existing algorithms.

Remark 1 (Secure Precoding in the FBL Regime): Since Algorithm 1 maximizes the secrecy rate in the FBL regime under given $\epsilon$ and $\Delta$ with low complexity, it can be considered as a computationally efficient secure precoding algorithm in the FBL-based communications.

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

We find the optimal $\epsilon$ and $\Delta$ for fixed $F$. To this end, we transform the multi-objective problem to a single-objective form and derive a solution for the transformed problem. Adopting the weighted-sum approach [11], the multi-objective problem in (11) for given $F$ is converted to

$$
\max_{\epsilon, \Delta} \frac{w}{R_{\infty}} \sum_{k=1}^{K} R_{\text{sec}}^{\epsilon}(\epsilon, \Delta) + (1 - w) \left(\frac{\hat{\epsilon}_{\text{max}} - \max\{\epsilon\}}{\hat{\epsilon}_{\text{max}}} + \frac{\hat{\Delta}_{\text{max}} - \max\{\Delta\}}{\hat{\Delta}_{\text{max}}}\right) \tag{38}
$$

subject to $\epsilon_k \leq \hat{\epsilon}_k$, $\forall k \in \mathcal{K}$,

$$
\delta_{m,k} \leq \hat{\delta}_{m,k}$, $\forall m \in \mathcal{M}$, $\forall k \in \mathcal{K}$,

where $R_{\infty}$ indicates a normalization constant that can be obtained as the sum secrecy rate in the infinite blocklength regime computed with a state-of-the-art secure precoder, $\epsilon_{\text{max}} = \max\{\epsilon_1, \cdots, \epsilon_K\}$, $\hat{\delta}_{\text{max}} = \max\{\delta_{1,1}, \cdots, \delta_{M,K}\}$, and the weight is $w \in [0, 1]$. To solve (38), we need to handle the maximum function in $R_{\text{sec}}^{\epsilon}(\epsilon_k, \hat{\delta}_{m,k})$. We consider the upper bound by adding the wiretap rates as

$$
\sum_{m=1}^{M} \left( \hat{R}_{m,k}^{e} + \sqrt{\frac{P}{L}}Q^{-1}(\hat{\delta}_{m,k}) \right),
$$

where the bound is not tight and the gap increases with the number of eavesdroppers, the proposed method based on the bound will show high performance for many eavesdroppers in Section IV-A. Subsequently, letting $\tau = \max\{\epsilon\}$ and $\xi = \max\{\Delta\}$ and removing the terms that are not a function of either $\epsilon_k$ or $\delta_{m,k}$, the problem in (38) is further transformed to the minimization problem as

$$
\min_{\epsilon, \Delta} \frac{w}{R_{\infty}} \sum_{k=1}^{K} \sqrt{\frac{P}{L}}Q^{-1}(\epsilon_k) + \frac{M}{\sum_{m=1}^{M} \sqrt{\frac{P}{L}}Q^{-1}(\delta_{m,k})}
$$

subject to $\epsilon_k \leq \tau$, $\xi$,

$$
0 \leq \epsilon_k \leq \hat{\epsilon}_k, \quad 0 \leq \tau \leq \epsilon_{\text{max}}, \quad 0 \leq \delta_{m,k} \leq \hat{\delta}_{m,k}, \quad 0 \leq \xi \leq \hat{\delta}_{\text{max}}, \quad \hat{\epsilon}_{\text{max}} = \max\{\epsilon_1, \cdots, \epsilon_K\}, \quad \hat{\Delta}_{\text{max}} = \max\{\delta_{1,1}, \cdots, \delta_{M,K}\}, \quad w \in [0, 1].
$$

where (43) and (46) are the error probability and information leakage rate constraints, and (44) and (47) indicate the maximum error probability assumption and information leakage assumptions. We note that the first term in (41) is monotonically increasing while the second term in (41) is monotonically decreasing with decreasing error probability and information leakage. Therefore, the optimal tradeoff exists among the backoff factors, error probability, and information leakage rate which is found by solving the KKT conditions [50] of (41).

Lemma 3: The optimal upper decoding error probability and information leakage rate for (41) with $\ell, j(k) \in \mathbb{N}_+$ are derived as

$$
\tau^* = Q \left( 2 \ln \left( \frac{\sqrt{L(1-w)R_{\infty}}}{\epsilon_{\text{max}}w\sqrt{2\pi} \sum_{k=1}^{K} \sqrt{V_k}} \right) \right), \tag{48}
$$

$$
\xi^* = Q \left( 2 \ln \left( \frac{\sqrt{L(1-w)R_{\infty}}}{\delta_{\text{max}}w\sqrt{2\pi} \sum_{m=1}^{M} \sum_{j(k)=1}^{K} \sqrt{V_{m,k}}} \right) \right). \tag{49}
$$

Then, without loss of generality, we can assume that $\epsilon_{\ell-1} < \tau < \epsilon_{\ell}$ for some $\ell$ and $\delta_{j(k-1),k} < \xi < \delta_{j(k),k}$ for some $j(k)$.
Algorithm 2 Joint Optimization Based on Alternating Approach

1) initialize: $\hat{f}(0), e(0), \delta(0), \forall k \in K$, and $t = 1$.
2) while increment of $t > e^{\text{out}}$ & $t \leq t_{\text{max}}$ do
3) $\hat{f}(t) \leftarrow$ Algorithm 1 $\left( e^{(t-1)}, \Delta^{(t-1)} \right)$.
4) Compute $R_{\infty}$ by using Algorithm 1 with $L = \infty$.
5) Find $\tau^*$ and $\epsilon^*$ according to (48) and (49) for $\hat{f}(t)$.
6) Set $\epsilon^{(t)} = [\epsilon_1, \cdots, \epsilon_{t-1}, \tau^*, \cdots, \tau^*]'$ and $\delta^{(t)} = [\delta_{1,k}, \cdots, \delta_{j(k)-1,k}, \epsilon^*, \cdots, \epsilon^*]'$, $\forall k \in K$.
7) $t \leftarrow t + 1$.
8) $\hat{f}^* \leftarrow \hat{f}(t), e^* \leftarrow e^{(t)}$, and $\Delta^* \leftarrow \Delta^{(t)}$.
9) return $\hat{f}^* = [f_1^T, f_2^T, \cdots, f_K^T]'$, $e^*$, and $\Delta^*$.

Then, the optimal solution of the problem in (41) is

\[ e^* = [\hat{e}_1, \cdots, \hat{e}_{t-1}, \tau^*, \cdots, \tau^*]' \in \mathbb{R}^K, \]
\[ \Delta^* = [\delta_{1,k}, \cdots, \delta_{j(k)-1,k}, \epsilon^*, \cdots, \epsilon^*]' \in \mathbb{R}^{M \times K}, \]

where

\[ \delta_{k}^* = [\delta_{1,k}, \cdots, \delta_{j(k)-1,k}, \epsilon^*, \cdots, \epsilon^*]' \in \mathbb{R}^M, \forall k \in K. \]

If $\epsilon^*_K < \tau^*$, the optimal error probability becomes

\[ e^* = [\hat{e}_1, \cdots, \hat{e}_t]'. \]

Similarly, if $\delta_{m,k} < \epsilon^*, \forall k \in K$, the optimal information leakage rate becomes

\[ \delta_{k}^* = [\delta_{1,k}, \cdots, \delta_{j(k)-1,k}, \epsilon^*, \cdots, \epsilon^*]' \in \mathbb{R}^M, \forall k \in K. \]

Proof: See Appendix B.

Remark 2 (Optimality of Solutions): Based on the proof of Lemma 3, it is concluded that the derived error probabilities $e^*$ are optimal for both the problem in (38) and its bounded problem in (41) since the derivation of $\tau^*$ does not involve the upper bounding of the wiretap rate. However, due to the upper bound, the derived leakage rates $\Delta^*$ are optimal only for the reformulated problem in (41) and suboptimal for the problem in (38). In addition, when there exists a single eavesdropper, i.e., $m = 1$, the equality in the upper bound of the wiretap rate holds and thus, the derived leakage rates $\Delta^*$ in this case is optimal for both the problems.

C. Joint Secure Precoding Algorithm

From the results in Section IV-A and Section IV-B, we finally design our proposed algorithm, which is described in Algorithm 2. First, Algorithm 2 initializes the precoding vector $\hat{f}(0)$, $e(0)$, and $\delta(0), \forall k \in K$. To find the best local optimal precoding vector $\hat{f}(0)$, Algorithm 1 is used for given $e^{(t-1)}$ and $\delta^{(t-1)}$. Then, $R_{\infty}$ is computed by finding $\hat{f}$ from Algorithm 1 in the infinite blocklength regime. The optimal $\tau^*$ and $\epsilon^*$ are computed based on (48) and (49), and we set $e^{(t)}$ and $\Delta^{(t)}$ accordingly. We repeat these steps until either the objective function in (38) increases smaller than $e^{\text{out}}$ compared to the previous iteration, where $e^{\text{out}} > 0$ denotes a tolerance threshold for the outer loop, or the algorithm reaches a maximum iteration count $t_{\text{max}}$. Since the solutions in (48) and (49) are closed-form, the complexity order of Algorithm 2 is $\mathcal{O} (\frac{1}{4} T_{\text{tot}} K N^3)$, where $T_{\text{tot}}$ is the number of total iterations of Algorithm 1.

V. EXTENSION TO PARTIAL CSIT OF WIRETAP CHANNELS

Since it is hard to obtain the perfect CSIT of eavesdroppers, we consider the case of the partial CSIT of wiretap channels in which only the long-term channel statistics of eavesdroppers, i.e., the channel covariance $R_{\text{wiretap}}$, is available. Since the instantaneous CSI of eavesdroppers is not known, it is infeasible to consider the instantaneous wiretap rate. Accordingly, we consider the ergodic wiretap rate to exploit the partial CSIT similarly to [51]. In [51], the ergodic rate is used as an optimization objective function to deal with the imperfect channel knowledge in the average sense. Then, instead of the secrecy rate in (8), we have

\[ R_{k}^{\text{sec}} = R_k - \sqrt{\frac{V_{\ell}}{L}} Q^{-1}(\epsilon_k) - \max_{m \in M} \left\{ E_g \left[ R_{m,k}^e + \sqrt{\frac{V_{m,k}}{L}} Q^{-1}(\delta_{m,k}) \right] \right\}, \]

where $E_g[\cdot]$ indicates the expectation with respect to wiretap channels. The key difference from [51] is that we do not average the user rate since the user channel knowledge is available, which would indeed lead to better optimization performance. Then, we can rewrite (55) by using the following proposition.

Proposition 1: The approximated upper bound of the ergodic wiretap secrecy rate in (55) is obtained as

\[ E_g \left[ R_{m,k}^e + \sqrt{\frac{V_{m,k}}{L}} Q^{-1}(\delta_{m,k}) \right] \]

\[ \leq R_{\text{m,k}}^e + \sqrt{\frac{V_{m,k}}{L}} Q^{-1}(\delta_{m,k}), \]

where

\[ R_{\text{m,k}}^e = \log_2 \left( 1 + \frac{\gamma_m e^{f_{m,k}} R_{m,k}^e f_k}{\sum_{\ell \neq k} \gamma_m e^{f_{m,\ell}} R_{m,\ell}^e f_\ell + \sigma_\ell^2 / P} \right), \]

\[ V_{m,k}^e = \sqrt{\frac{V_{m,k}^e}{2} \sum_{\ell = 1}^K \gamma_m e^{f_{m,\ell}} R_{m,\ell}^e f_\ell + \sigma_\ell^2 / P} \log_2 e. \]

Proof: The ergodic wiretap rate in (6) is approximated as

\[ E_g [R_{m,k}^e] = E_g \left[ \log_2 \left( 1 + \frac{\gamma_m e^{f_{m,k}} R_{m,k}^e f_k}{\sum_{\ell \neq k} \gamma_m e^{f_{m,\ell}} R_{m,\ell}^e f_\ell + \sigma_\ell^2 / P} \right) \right] \]

\[ \approx \log_2 \left( 1 + \frac{\gamma_m e^{f_{m,k}} R_{m,k}^e f_k}{\sum_{\ell \neq k} \gamma_m e^{f_{m,\ell}} R_{m,\ell}^e f_\ell + \sigma_\ell^2 / P} \right) \]

\[ = R_{\text{m,k}}^e, \]
where \((a)\) comes from Lemma 1 in [52]. We also have
\[
\mathbb{E} \left[ \sum_{m,k} \right] \leq \sqrt{\mathbb{E} \left[ \sum_{m,k} \right]} \leq \frac{2}{\mathbb{E} \left[ \sum_{m,k} \right] + 1} \log_2 e \tag{62}
\]
\[
\sum_{m,k} \leq \frac{2g_2^e f^P R_c f_k}{\sum_{k=1}^K g_2^e f^P R_c f_k + \sigma_e^2 / P} \log_2 e \tag{63}
\]
\[
\sum_{m,k} \leq \frac{2g_2^e f^P R_c f_k}{\sum_{k=1}^K g_2^e f^P R_c f_k + \sigma_e^2 / P} \log_2 e \tag{64}
\]
where \((b)\) and \((c)\) follow from Jensen’s inequality, and \((d)\) comes from the first-order Taylor expansion based on statistical linearization [53].

Applying (56) to (55), we have the lower bound of secrecy rate approximated as
\[
R_k^{sec,p} \geq R_k - \frac{\sqrt{V_k}}{L} Q^{-1}(\delta_m) \leq R_k^{sec,p}.
\]
Replacing \(R_k^{sec}\) in (11) with \(R_k^{sec,p}\), we can also develop the joint secure precoding algorithm with minimizing the maximum error probability and information leakage rate. In particular, as in Section IV-A, we formulate the sum secrecy rate maximization problem with \(R_k^{sec,p}\) as
\[
\max_{\mathbf{F}} \sum_{k=1}^K R_k^{sec,p}(\mathbf{F}) \tag{66}
\]
subject to \(\text{tr}(\mathbf{F}\mathbf{F}^H) \leq 1\). \tag{67}

We note that the formulated problem in (66) consists of the eavesdropper’s channel covariance matrix \(R_e^{m}\). As in Section IV-A, we also derive the first-order KKT condition for (66) as
\[
\mathbf{B}_{KKT}(\mathbf{f}) \mathbf{A}_{KKT}(\mathbf{f}) \mathbf{f} = \lambda(\mathbf{f}) \mathbf{f}, \tag{68}
\]
where
\[
\mathbf{A}_{KKT}(\mathbf{f}) = \lambda_{num}(\mathbf{f}) \cdot \sum_{k=1}^K \left[ \frac{\omega_k}{\ln 2} \left( \mathbf{A}_k + \mathbf{D}_m \mathbf{f} \right) \right] + \frac{1}{\alpha} \sum_{m=1}^M \left[ \frac{\omega_m^e \beta_m}{\ln 2} \left( \mathbf{D}_m \mathbf{f} \right) \right], \tag{69}
\]
\[
\mathbf{B}_{KKT}(\mathbf{f}) = \lambda_{den}(\mathbf{f}) \cdot \sum_{k=1}^K \left[ \frac{\omega_k}{\ln 2} \left( \mathbf{B}_k \mathbf{f} \right) \right] + \frac{1}{\alpha} \sum_{m=1}^M \left[ \frac{\omega_m^e \beta_m}{\ln 2} \left( \mathbf{C}_m \mathbf{f} \right) \right], \tag{70}
\]
\[
\mathbf{C}_m = \text{blkdiag}(\gamma_m^e \mathbf{R}_m, \ldots, \gamma_m^e \mathbf{R}_m) + \frac{\sigma_e^2}{P}, \tag{71}
\]
\[
\mathbf{D}_m = \mathbf{C}_m - \text{blkdiag}(0, \ldots, \gamma_m^e \mathbf{R}_m, \ldots, 0) \in \mathbb{C}^{NK \times NK}, \tag{72}
\]
\[
\lambda(\mathbf{f}) = \lambda_{num}(\mathbf{f}) / \lambda_{den}(\mathbf{f}), \tag{73}
\]
\[
\lambda_{num}(\mathbf{f}) = \prod_{k=1}^K \left( \frac{\mathbf{f}^H \mathbf{A}_k \mathbf{f}}{\mathbf{f}^H \mathbf{B}_k \mathbf{f}} \right)^{\omega_k}, \tag{74}
\]
\[
\lambda_{den}(\mathbf{f}) = \prod_{k=1}^K \left( \sum_{m=1}^M \left( \frac{\mathbf{f}^H \mathbf{C}_m \mathbf{f} \omega_m^e}{\mathbf{f}^H \mathbf{D}_m \mathbf{f}} \right) \right)^{\omega_k}, \tag{75}
\]
Recall that \(\mathbf{A}_k\) and \(\mathbf{B}_k\) are derived in (27) and (28), respectively. Replacing \(\mathbf{A}_{KKT}\) and \(\mathbf{B}_{KKT}\) with \(\mathbf{A}_{KKT}\) and \(\mathbf{B}_{KKT}\) in Algorithm 1, we 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 IV-B based on \(R_k^{sec,p}\) as
\[
\tilde{R}_k = \mathcal{Q} \left( \frac{\sqrt{\ln 2 (1 - w) \tilde{R}_k}}{\xi_{\text{max}} w \sqrt{2 \pi \sum_{k=1}^K \sqrt{V_k}}} \right), \tag{76}
\]
\[
\tilde{\xi}_k = \mathcal{Q} \left( \frac{\sqrt{\ln 2 (1 - w) \tilde{R}_k}}{\xi_{\text{max}} w \sqrt{2 \pi \sum_{k=1}^K \sqrt{V_k}}} \right), \tag{77}
\]
where \(\tilde{R}_k\) is the normalization constant based on \(\tilde{R}_k\) for \(L = \infty\). Then, the joint secure precoding algorithm is proposed with Algorithm 2 by replacing \(\mathbf{A}_k\), \(\mathbf{B}_k\), \(\tau^*\), and \(\xi^*\) with \(\mathbf{A}_k\), \(\mathbf{B}_k\), \(\tilde{\tau}^*\), and \(\tilde{\xi}^*\), respectively.

VI. NUMERICAL RESULTS

In this section, we evaluate the performance of our proposed algorithms and deliver key insights. In the simulations, considered algorithms are: (1) Algorithm 1 (or Algorithm 2), (2) Algorithm 1 (or Algorithm 2) with the partial CSIT of wiretap channel (partial) in Section V, (3) a FBL-based SE maximization algorithm (FBL-SE-MAX) [32], (4) WMMSE [51], (4) ZF, (6) a ZF-based secure precoding algorithm (ZF-EVE), (5) regularized ZF (RZF), and (8) RZF-EVE. The WMMSE-based algorithm uses the sample average approximation and solved by a CVX toolbox [51]. Specifically, FBL-SE-MAX focuses on maximizing the SE with finite coding length, but the security is not considered. In addition, RZF-EVE and ZF-EVE are used to nullify wiretap channels by constructing an effective channel matrix with the \(N - K\) strongest eavesdroppers’ channel vectors. When \(N > K\), ZF-EVE and RZF-EVE exploit the wiretap channels as \(\mathbf{H}_i = [\mathbf{h}_1, \ldots, \mathbf{h}_K, \mathbf{g}_1, \ldots, \mathbf{g}_{N - K}], i.e., \ ZF-EVE and RZF-EVE precoders are
\[
\mathbf{F}_{ZF-EVE} = \left( \mathbf{H} \left( \mathbf{H}^H \mathbf{H} \right)^{-1} \right)^{1:1:K}, \tag{78}
\]
\[
\mathbf{F}_{RZF-EVE} = \left( \mathbf{H} \left( \mathbf{H}^H + \frac{\sigma_e^2}{P} \mathbf{I} \right)^{-1} \right)^{1:1:K}. \tag{79}
\]
To generate the channel vectors \(\mathbf{h}_k\) and \(\mathbf{g}_m\), we adopt a one-ring model [54] based on its spatial covariance matrices \(\mathbf{R}_k = \mathbb{E} [\mathbf{h}_k \mathbf{h}_k^H]\) and \(\mathbf{R}_m = \mathbb{E} [\mathbf{g}_m \mathbf{g}_m^H]\). In addition, we consider
that the geometric location of each eavesdropper is correlated with a particular legitimate user. Accordingly, the channel angle of departure (AoD) of eavesdropper $m$ follows $\theta_m \sim \theta_k + \mathcal{U}(-\Delta, \Delta)$ for randomly selected user $k$ with a scalar weight $0 < \Delta < 1$, where $\theta_k$ represents the AoD of user $k$. We generate $e_k$ and $\delta_{m,k}$ uniformly spaced from $10^{-6}$ to $2 \times 10^{-6}$ for all users and eavesdroppers. For simplicity, we consider $\delta_{m,k} = \delta_{m,k'}, \forall m \in \mathcal{M}$. We set the scalar weight, coding length, optimization weight, iteration thresholds, and maximum iteration counts as $\Delta = 0.1$, $L = 200$, $w = 0.01$, $\epsilon = \epsilon_{\text{out}} = 0.01$, and $t_{\max} = 15$ and $t_{\text{out}}^{\max} = 5$ unless mentioned otherwise.

Additionally, to generate the large-scale channel fading terms $\gamma_k$ and $\gamma_{m,k}^e$, we adopt the ITU-R indoor pathloss model [55] which considers a non-line-of-sight pathloss environment by setting bandwidth, carrier frequency, distance power-loss coefficient, and noise figure to be 10 MHz, 5.2 GHz, 31 (equivalent to the pathloss exponent of 3.1), and 5 dB, respectively. We assume the noise power spectral density of legitimate users and eavesdroppers is the same as $-174$ dBm/Hz. The users are randomly generated around the AP with the maximum distance of $50 \, m$ and minimum distance of $5 \, m$ from the AP. The eavesdroppers are randomly distributed around random users with the maximum distance of $5 \, m$ from the users.

A. Secure Precoding for Given Error and Leakage in FBL Regime

We first investigate the precoders that maximize the sum secrecy rate with respect to the transmit power $P$ for given $e_k$ and $\delta_{m,k}$ as $e_k$ and $\delta_{m,k}$, respectively. We remark that the considered transmit power range is wider than the practical range for comprehensive evaluation of the proposed algorithms. In Fig. 1, Algorithm 1 achieves the highest rate performance for any transmit power regime. In addition, we observe that Algorithm 1 (partial) provides better performance than the benchmark schemes without the perfect wiretap CSIT. This is because unlike the baseline algorithms the proposed methods jointly optimize the sum secrecy rate maximization problem with back-off factors as well as user and wiretap rates. We observe that the secure precoders such as the RZF-EVE and ZF-EVE waste their extra dimension in nullifying the leakage from the wiretap channels rather than increasing legitimate users’ channel gains, showing poor performance in Fig. 1.

In Fig. 2, we evaluate the secrecy rate performance versus the blocklength $L$ for $N = 8$, $K = 4$, $M = 8$, and $P = 20$ dBm. We note that all algorithms reveal an increasing trend of the sum secrecy rate with $L$ as theoretically shown in (8). Fig. 2 shows that the proposed algorithms maintain the highest secrecy rate performance regardless of $L$. Accordingly, the proposed algorithm is effective in the general blocklength. Thus, the proposed secure precoder is preferable in supporting the conventional as well as FBL-based communication systems.

B. Joint Secure Precoding With Error and Leakage Minimization in FBL Regime

Now, we evaluate the proposed method in Algorithm 2. For comparison, the baseline algorithms utilize the second phase (Phase II in Section IV-B) of the proposed optimization framework for minimizing the maximum error probability and information leakage rate in Section IV-B. Fig. 3 shows that the performance of the sum secrecy rate, the maximum error probability, and information leakage rate with respect to the transmit power $P$ for $N = 8$, $K = 4$, and $M = 8$. The benchmark algorithms with the proposed minimization method provide the significant reduction in the maximum error probability and information leakage rate. We note that the proposed algorithm achieves the highest secrecy rate performance while maintaining the lowest maximum error probability and information leakage rate for the most signal-to-noise ratio (SNR). FBL-SE-MAX with Phase II attains the lowest maximum error probability in most SNR regimes. The security rate of FBL-SE-MAX, however, reveals an increasing gap from the proposed algorithm due to ignoring the wiretap channels. We observe that the proposed algorithm provides the significant gain of SNR to fulfill the stringent requirements of URLLC in the FBL regime. For instance, if the system requirements of the sum secrecy rate, maximum error probability, and maximum information leakage are $\sum_{k=1}^{K} R_k^{\text{sec}} > 35$ bits/sec/Hz, $\max\{\epsilon_k\} < 4.0 \times 10^{-11}$, and $\max\{\delta_{m,k}\} < 4.0 \times 10^{-11}$, the proposed algorithm can satisfy...
the requirements with 25.7 dBm transmit power, whereas FBL-SE-MAX and WMMSE equipped with Phase II require 40 dBm, i.e., more than $27 \times$ the transmit power is needed, and even the others cannot meet the requirements in the feasible transmit power regime.

To provide the numerical analysis in terms of the number of AP antennas $N$, we show the performance of the sum secrecy rate, the maximum error probability, and information leakage rate with respect to the number of AP antennas for $P = 20$ dBm, $K = 4$, and $M = 8$ in Fig. 4. It is shown that the proposed algorithms also achieve the highest secrecy rate performance regardless of $N$. As observed in Fig. 4(a), RZF-EVE and ZF-EVE reveal a unique trend of the sum secrecy rate as $N$ increases. Since there exists the optimal tradeoff between increasing the legitimate channel gain and nullifying the wiretap channels, the rates do not monotonically increase with $N$ for RZF-EVE and ZF-EVE. Specifically, Fig. 4(a) shows that since the spare dimension of $N - K$ is small, it would be more beneficial to use the extra degree-of-freedom (DoF) for increasing the legitimate users’ signal gain. Consequently, when $N - K$ is small, ZF-EVE and RZF-EVE present poorer rates than ZF and RZF. When $N - K$ is large, however, the extra DoF can be utilized both to increase user signal gains and to nullify wiretap channels. In this regard, as $N$ increases, ZF-EVE and RZF-EVE show smaller gaps from ZF and RZF, and they outperform ZF and RZF when $N$ is sufficiently large, i.e., sufficient DoF. Regarding the information leakage rate, ZF-EVE that utilizes its extra DoF to fully nullify the wiretap channels is a nearly optimal solution with the enough DoF as shown in Fig. 4(b). Considering the entire performance, however, the proposed algorithms show the most balanced performance.

We further evaluate the proposed algorithms with respect to the number of legitimate users $K$ for $N = 8$, $M = 8$, and $P = 20$ dBm. Overall, Fig. 5 shows that the algorithms reveal similar ordering in the sum secrecy rate as in Fig. 3. Comparing RZF-EVE with RZF, we conjecture that when DoF margin is small compared to the number of users, focusing on maximizing the legitimate users’ sum rate is more beneficial than allocating resources on mitigating information leakage, which is also observed in Fig. 4. In addition, Fig. 5(a) shows that the sum secrecy rate of RZF firstly increases and then decreases with the number of users because there exists the optimal number of users in terms of the sum secrecy rate, which was also noticed in several works [56]. In Fig. 5(b), the proposed algorithm provides the lowest maximum error probability and information leakage rate regardless of $K$. Therefore, the proposed algorithm provides improvement in rate, reliability, and security for the considered system environment.
Fig. 5. (a) The sum secrecy rate and (b) maximum error and information leakage versus the number of users $K$ for $P = 20$ dBm transmit power, $N = 8$ AP antennas, and $M = 8$ eavesdroppers.

In Fig. 6, we assess the sum secrecy rate in terms of the number of eavesdroppers $M$ for $P = 20$ dBm, $N = 8$, and $K = 4$. Fig. 6(a) shows that the proposed algorithms still achieve the highest secrecy rates. As $M$ increases, the relative gaps between the proposed and the other algorithms become larger, which demonstrate the performance of the proposed algorithms. We note that for RZF-EVE and ZF-EVE, decreasing the spatial DoF margin leads to the poor performance of the secrecy rate. As shown in Fig. 6(b), the proposed algorithms offer good and robust performance in minimizing the maximum error probability and leakage rate over $M$.

Although ZF-EVE shows the lowest maximum leakage rate for $M \leq 4$ by fully nullifying the wiretap channels, the achieved secrecy rate is significantly lower and the leakage rate becomes higher than the proposed algorithms for $M > 4$. In this regard, the proposed algorithm is considered to be a potential PLS solution that is robust to the number of eavesdroppers.

Now, we verify convergence of the proposed algorithm: inner and outer loops of Algorithm 2 for $P \in \{-10, 0, 10, 20\}$ dBm, $N = 8$, $K = 4$, and $M = 4$. We first evaluate the convergence results for the inner loop which corresponds to Algorithm 1 in terms of the approximated objective function $\log_2 \lambda(f)$ in (32). In Fig. 7(a), shows that the proposed algorithm converges within $t_{\text{max}}^\text{int} = 5$ iterations for any transmit power regime. Next, we assess the convergence results for the outer loop of Algorithm 2 with respect to the increment of (41). As shown in Fig. 7(b), the outer loop of the proposed algorithm converges within $t_{\text{max}}^\text{out} = 2$ outer iterations. Therefore, it is considered that the proposed algorithm guarantees the fast convergence in the practical transmit power regime and demonstrates high potential for the practical communications compared to other high-complexity precoding algorithms in the FBL regime.

For comprehensiveness, we evaluate CPU time for $N = 4$ AP antennas, $K = 2$ users, and $M = 2$ eavesdroppers in MATLAB. Here, we simulate Algorithm 2 in terms of the secrecy rate, error probability, and information leakage rate with respect to transmit power $P$ together with the benchmark schemes who are applied with Phase II except RZF. In the simulation, the workstation equipped with i9-10900K CPU, RTX 3090 GPU, and 64GB RAM is used. In Table I, we observe that the proposed algorithm performs within a few milliseconds whereas the CVX-based WMMSE algorithm requires the significantly high CPU time which is 3741 times more than that of Algorithm 2. Algorithm 2 and FBL-SE-MAX present a similar time order as they all can be conducted in a few milliseconds. We note that the conventional linear precoders show less computing time than Algorithm 2. Considering the performance in the sum secrecy rate, error probability, and leakage rate, however, Algorithm 2 provides...
reasonable computation time with the highest performance as observed in this section.

Overall, the proposed algorithms offer significant improvement in the secrecy rate, error probability, and information leakage rate, and thus enhance the data rate, security, and reliability with low complexity in the FBL regime.

C. Analysis With Channel Estimation Error

In this subsection, we further evaluate the impact of channel estimation error. To this end, we define legitimate and wiretap channels under the premise that the AP has imperfect CSIT as

\[ h_k = \hat{h}_k + e_k, \]  
\[ g_m = \hat{g}_m + \tilde{e}_m, \]

where \( \hat{h}_k \) and \( \hat{g}_m \) are estimated channels, and \( e_k \) and \( \tilde{e}_m \) are channel estimation errors at user \( k \) and eavesdropper \( m \), respectively. According to [51], using linear minimum mean square estimation (LMMSE) approach in time division duplex (TDD) systems, the channel estimation errors of users and eavesdroppers are obtained as

\[ \mathbb{E}[e_k e_k^H] = \Phi_k = \mathbf{R}_k - (\mathbf{R}_k + \frac{\sigma^2}{\tau_{UL} p_{UL}})^{-1} \mathbf{R}_k, \]  

\[ \mathbb{E}[\tilde{e}_m \tilde{e}_m^H] = \Phi_m = \mathbf{R}_m - \mathbf{R}_m \left( \mathbf{R}_m + \frac{\sigma^2}{\tau_{UL} p_{UL}} \right)^{-1} \mathbf{R}_m, \]

where \( \tau_{UL} \) and \( p_{UL} \) are uplink training length and uplink training transmit power. As the uplink training length and power increase to infinity, the error covariance becomes \( \Phi_k = \Phi_m = 0 \); thereby the estimation errors vanish, i.e., the perfect CSIT.

In the simulation, we consider \( N = 4 \), \( K = 2 \), and \( M = 2 \) with \( \tau_{UL} p_{UL} = 8 \). In Fig. 8, it is observed that the proposed algorithm still maintains the best tradeoff between the sum secrecy rate and the error and information leakage rates, providing the highest the sum secrecy rate, which is a similar trend as the perfect CSIT case. In addition, since FBL-SE-MAX (imperfect) focuses on maximizing the SE, it has difficulty in securing the secrecy rate against eavesdroppers for both perfect and imperfect CSIT scenarios. Moreover, due to the channel estimation errors, RZF-EVE (imperfect) struggles in nullifying both the interference and the wiretap channels, and thus it has the lowest performance. Via the simulations, we validate that the proposed algorithm is able to perform with significant improvement in the imperfect channel environment.
we take the partial derivative of \( L \) for the imperfect CSIT for both legitimate users and eavesdroppers realizing the URLLC under high information security. Therefore, the proposed methods can play a key role in existing methods with fast convergence and high robustness.

In this paper, we proposed secure precoding algorithms that jointly optimize rate, reliability, and security in the finite blocklength regime. To this end, we formulated a joint optimization problem for the sum secrecy rate and error probability, and information leakage rate according to the characteristics of finite blocklength channel coding-based communications. To resolve the key challenges in solving the problem, we first decompose the problem into two subproblems. Then, for the first problem, we designed the precoding algorithm that maximizes the sum secrecy rate for the given error probability and information leakage rate by identifying stationary points. For the second problem, we also reformulated the multi-objective optimization problem into the single-objective optimization problem for a given precoder and solved the KKT conditions to derive the optimal error probability and information leakage rate. Through the alternating optimization, we developed the joint optimization algorithm that provides the significantly improved tradeoff among the security, the error probability, and information leakage rate.

We further extended the algorithms for the case in which only the partial CSI of wiretap channels is available. Via simulations, we validated the secrecy rate, error probability, and information leakage performances of the proposed algorithms. In particular, we demonstrated that the proposed methods achieve the highest secrecy performance while satisfying the stringent reliability and security requirements compared to the existing methods with fast convergence and high robustness. Therefore, the proposed methods can play a key role in realizing the URLLC under high information security.

For a future research direction, it is desirable to consider the imperfect CSIT for both legitimate users and eavesdroppers and to further reduce the complexity of the proposed algorithm.

### APPENDIX A

**PROOF OF LEMMA 1**

We first define the Lagrangian function of the problem (26) as

\[
\mathcal{L}_1(\bar{f}) = \sum_{k=1}^{K} \left[ \log_2 \left( \frac{\bar{f}^H A_k \bar{f}}{\bar{f}^H B_k \bar{f}} \right) \omega_k \right] - \ln \left( \sum_{m=1}^{M} \left( \frac{\bar{f}^H C_m \bar{f}}{\bar{f}^H D_{m,k} \bar{f}} \right) \right) \right]^+.
\]

(84)

According to the first-order KKT condition, the stationary points need to satisfy zero-gradient, i.e., \( \partial \mathcal{L}_1(\bar{f}) / \partial \bar{f} = 0 \). Thus, we take the partial derivative of \( \mathcal{L}_1(\bar{f}) \) with respect to \( \bar{f} \) and set it to zero. Next, we denote the first and second part of (84) as \( \mathcal{L}_{1,\text{use}}(\bar{f}) \) and \( \mathcal{L}_{1,\text{eve}}(\bar{f}) \), thereby

\[
\mathcal{L}_{1,\text{use}}(\bar{f}) - \mathcal{L}_{1,\text{eve}}(\bar{f}).
\]

Then, employing the derivative of the Rayleigh quotient form

\[
\frac{\partial}{\partial \bar{f}} \left( \bar{f}^H A_k \bar{f} \right) = \left( \bar{f}^H A_k \bar{f} \right) - \frac{A_k \bar{f}}{\bar{f}^H A_k \bar{f}} B_k \bar{f},
\]

(85)

we can calculate the partial derivative of \( \mathcal{L}_{1,\text{use}}(\bar{f}) \) with respect to \( \bar{f} \) as

\[
\frac{\partial \mathcal{L}_{1,\text{use}}(\bar{f})}{\partial \bar{f}} = \sum_{k=1}^{K} \left[ \frac{1}{\ln 2} \left( \frac{C_m e}{\bar{f}^H C_m \bar{f}} - \frac{D_{m,k} e}{\bar{f}^H D_{m,k} \bar{f}} \right) \right] \bar{f}.
\]

(86)

Subsequently, we take the partial derivative of \( \mathcal{L}_{1,\text{eve}}(\bar{f}) \) with respect to \( \bar{f} \) as

\[
\frac{\partial \mathcal{L}_{1,\text{eve}}(\bar{f})}{\partial \bar{f}} = \sum_{k=1}^{K} \left[ \frac{1}{\ln 2} \left( \frac{C_m e}{\bar{f}^H C_m \bar{f}} - \frac{D_{m,k} e}{\bar{f}^H D_{m,k} \bar{f}} \right) \right] \bar{f}.
\]

(87)

Then, using (86) and (87), the first-order KKT condition holds if

\[
\sum_{k=1}^{K} \left[ \frac{1}{\ln 2} \frac{A_k}{\bar{f}^H A_k \bar{f}} \right] + \left[ \frac{1}{\ln 2} \frac{B_k}{\bar{f}^H B_k \bar{f}} \right] = \sum_{k=1}^{K} \left[ \frac{1}{\ln 2} \frac{C_m e}{\bar{f}^H C_m \bar{f}} - \frac{D_{m,k} e}{\bar{f}^H D_{m,k} \bar{f}} \right] \bar{f}.
\]

(88)

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

\[
A_{KKT}(\bar{f}) \bar{f} = \lambda(\bar{f}) B_{KKT}(\bar{f}) \bar{f}.
\]

(89)

Since \( B_{KKT}(\bar{f}) \) is Hermitian, it is invertible. This completes the proof.

### APPENDIX B

**PROOF OF LEMMA 3**

We note that \( Q^{-1}(x) \) is convex if \( x < \frac{1}{2} \), so that the problem in (41) becomes a convex problem. To solve the problem, we define the Lagrangian function of the problem in (41) as

\[
\mathcal{L}_2 = \frac{w}{K} \sum_{k=1}^{K} \left[ \sqrt{V e} Q^{-1}(\epsilon_k) \right] + \left( 1 - w \right) \left( \frac{\tau}{\epsilon_{\text{max}}} + \frac{\xi}{\delta_{\text{max}}} \right)
\]

(90)

Authorized licensed use limited to the terms of the applicable license agreement with IEEE. Restrictions apply.
$$-\sum_{k=1}^{K} \lambda_k (\tau - \epsilon_k) - \sum_{k=1}^{K} \nu_k (\epsilon_k - \xi_k) - \mu (\epsilon_{\text{max}} - \tau)$$
$$- \sum_{m=1}^{M} \sum_{k=1}^{K} \lambda_{m,k}^* (\xi - \delta_{m,k}) - \sum_{m=1}^{M} \sum_{k=1}^{K} \nu_{m,k}^* (\delta_{m,k} - \delta_{m,k})$$
$$- \mu^* (\delta_{\text{max}} - \xi_k)$$ \hspace{1cm} (90)

where \(\lambda_k, \nu_k, \mu, \lambda_{m,k}^*, \nu_{m,k}^*, \) and \(\xi^*\) indicate Lagrangian multipliers. For a feasible solution, we assume \(\lambda_k \geq 0, \nu_k \geq 0, \mu \geq 0, \mu^* \geq 0, \lambda_{m,k}^* \geq 0, \) and \(\nu_{m,k}^* \geq 0, \forall k \in \mathcal{K}, \forall m \in \mathcal{M}.\)

According to the KKT conditions, the optimal solution for the problem in (41) should satisfy the following:

$$\frac{\partial \mathcal{L}_2}{\partial \xi} = -\frac{w}{\lambda_{\text{max}}} \frac{\lambda_{m,k}^* + \nu_{m,k}^*}{L} \right) = 0, \hspace{1cm} (95)$$

$$\frac{\partial \mathcal{L}_2}{\partial \epsilon_k} = \frac{1 - w}{\delta_{\text{max}}} - \sum_{m,k} \lambda_{m,k}^* + \mu^* = 0, \hspace{1cm} (96)$$

$$\frac{\partial \mathcal{L}_2}{\partial \delta_{m,k}} = \frac{w}{\lambda_{\text{max}}} \frac{\lambda_{m,k}^* + \nu_{m,k}^*}{L} \right) = 0, \hspace{1cm} (97)$$

$$\frac{\partial \mathcal{L}_2}{\partial \xi_k} = \frac{1 - w}{\delta_{\text{max}}} - \sum_{m,k} \lambda_{m,k}^* + \mu^* = 0, \hspace{1cm} (98)$$

$$\newcommand{\epsilon}{}$$

where (91) and (93) come from that \(\partial Q^{-1}(x)/\partial x = -\sqrt{2\pi} \exp \left( (Q^{-1}(x))^2 / 2 \right) \). Now, we obtain the optimal points \(\epsilon_k^*\) and \(\delta_{m,k}^*\) by using the derived KKT conditions. From (91), (95), and (96), \(\epsilon_k^*\) should be equal to \(\tau^*\) or \(\epsilon_k\). In the same manner, \(\delta_{m,k}^*\) should be equal to \(\xi_k^*\) or \(\delta_{m,k}\) from (93), (98), and (99). Assuming that \(\tau^* < \epsilon_{\text{max}}\) and \(\xi^* < \delta_{\text{max}}\), we obtain \(\mu^* = \mu_{\epsilon^*}^* = 0.\) Since we can assume that \(\epsilon_{\ell-1} < \tau^* < \epsilon_{\ell}\) for some \(\ell\) and \(\delta_{j(k)-1,k} < \xi_k^* < \delta_{j(k),k}\) for some \(j(k)\), the optimal error probability and information leakage are obtained as

$$\epsilon^* = [\epsilon_1, \epsilon_{\ell-1}, \tau^*, \epsilon_{\ell}, \tau^*] \right), \hspace{1cm} (101)$$

$$\delta_k^* = [\delta_{1,k}, \ldots, \delta_{j(k)-1,k}, \delta_{j(k),k}^*, \xi_k^*, \ldots, \xi_k^*] \right). \hspace{1cm} (102)$$

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

$$\Delta^* = [\delta_1^*, \ldots, \delta_K^*]. \hspace{1cm} (103)$$

Assuming \(\epsilon_{\ell-1} < \tau^* < \epsilon_{\ell}\) for some \(\ell, \nu_k^* = 0\) and \(\mu^* = 0\) for \(k \geq \ell.\) Combining (91) and (92),

$$\frac{w}{\lambda_{\text{max}}} \sum_{k=1}^{K} \sqrt{\mathcal{V}_k} \frac{\sqrt{2\pi} \exp \left( (Q^{-1}(\epsilon_k^*))^2 / 2 \right)}{\frac{1 - w}{\epsilon_{\text{max}}}}, \hspace{1cm} \text{for } k \geq \ell. \hspace{1cm} (104)$$

We solve (104) with respect to \(\epsilon_k^*\) and have \(\epsilon_k^* = \tau^*\) which is in (48) for \(k \geq \ell.\) Similarly, we assume \(\delta_{j(k)-1,k} < \xi_k^* < \delta_{j(k),k}\), then \(\nu_{m,k}^* = 0\) and \(\mu^* = 0\) for \(m \geq j(k).\) From (93) and (94),

$$\frac{w}{\delta_{\text{max}}} \sum_{m=j(k)}^{M} \sum_{k=1}^{K} \sqrt{\mathcal{V}_{m,k}} \frac{\sqrt{2\pi} \exp \left( (Q^{-1}(\delta_{m,k})^2 / 2 \right)}{\frac{1 - w}{\delta_{\text{max}}}}, \hspace{1cm} \text{for } m \geq j(k). \hspace{1cm} (105)$$

Solving (105) with respect to \(\delta_{m,k}^*\), we have \(\delta_{m,k}^* = \xi_k^*\) in (49) for \(m \geq j(k).\)

REFERENCES

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

[2] P. Popovski et al., “Wireless access in ultra-reliable low-latency communication (URLLC),” IEEE Trans. Commun., vol. 67, no. 8, pp. 5783–5801, Aug. 2019.

[3] L. Hoberg, A. Festag, I. Llatser, L. Altomare, F. Visintainer, and A. Kovacs, “Enhancements of V2X communication in support of cooperative autonomous driving,” IEEE Commun. Mag., vol. 53, no. 12, pp. 64–70, Dec. 2015.

[4] 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, Sep. 2020.

[5] G. Durisi et al., “Toward massive, ultra-reliable, and low-latency wireless communication with short packets,” Proc. IEEE, vol. 104, no. 9, pp. 1711–1726, Sep. 2016.

[6] G. Durisi, T. Koch, J. Ostman, Y. Polyanskiy, and W. Yang, “Short-packet communications over multiple-antenna Rayleigh-fading channels,” IEEE Trans. Commun., vol. 64, no. 2, pp. 618–629, Feb. 2016.

[7] Q. Zhang, P. P. Liang, Y. -D. Huang, Y. Pei, and Y.-C. Liang, “Label-assisted transmission for short packet communications: A machine learning approach,” IEEE Trans. Veh. Technol., vol. 67, no. 9, pp. 8846–8859, Sep. 2018.

[8] J. Chen, Z. Zhang, Y.-C. Liang, X. Kang, and R. Zhang, “Resource allocation for wireless-powered IoT networks with short packet communication,” IEEE Trans. Wireless Commun., vol. 18, no. 2, pp. 1447–1461, Feb. 2019.

[9] Y. Yu, H. Chen, Y. Li, Z. Ding, and B. Vucetic, “On the performance of non-orthogonal multiple access in short-packet communications,” IEEE Commun. Lett., vol. 22, no. 3, pp. 590–593, Mar. 2018.

[10] 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, May 2010.

[11] 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. 4, pp. 726–729, Dec. 2017.

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

[13] Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, and S. Shieh, “IoT security: Ongoing challenges and research opportunities,” in Proc. IEEE 7th Int. Conf. Service-Oriented Comput. Appl., Nov. 2014, pp. 230–234.

[14] M. B. M. Noor and W. H. Hasssan, “Current research on Internet of Things (IoT) security: A survey,” Comput. Netw., vol. 148, pp. 283–294, Jan. 2018.
[15] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, “A survey of physical layer security techniques for 5G wireless networks and challenges ahead,” IEEE J. Sel. Areas Commun., vol. 36, no. 4, pp. 679–695, Apr. 2018.

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

[17] I. Csiszar and J. Korner, “Broadcast channels with confidential messages,” IEEE Trans. Inf. Theory, vol. IT-24, no. 3, pp. 339–348, May 1978.

[18] W. Yang, R. F. Schaefer, and H. V. H. V. Poor, “Finite-blocklength bounds for wiretap channels,” in Proc. IEEE Int. Symp. Inf. Theory, Jul. 2016, pp. 3087–3091.

[19] 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, Jul. 2019.

[20] C. Feng and H.-M. Wang, “Secure short-packet communications at the physical layer for 5G and beyond,” IEEE Commun. Standards Mag., vol. 5, no. 3, pp. 96–102, Sep. 2021.

[21] I. Krikidis and B. Ottersten, “Secrecy sum-rate for orthogonal random beamforming with opportunistic scheduling,” IEEE Signal Process. Lett., vol. 20, no. 2, pp. 141–144, Feb. 2013.

[22] Z. Sheng, H. D. Tuan, T. Q. Duong, and H. V. Poor, “Beamforming optimization for physical layer security in MISO wireless networks,” IEEE Trans. Signal Process., vol. 66, no. 14, pp. 3710–3723, Jul. 2018.

[23] A. Khisti and G. Womell, “Secure transmission with multiple antennas—Part II: The MIMOME wiretap channel,” IEEE Trans. Inf. Theory, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[24] Q. Shi, W. Xu, J. Wu, E. Song, and Y. Wang, “Secure beamforming for MIMO broadcasting with wireless information and power transfer,” IEEE Trans. Wireless Commun., vol. 14, no. 5, pp. 2841–2853, May 2015.

[25] W. Wang, K. C. Teh, and K. H. Li, “Secrecy throughput maximization for MISO multi-antenna beamforming in MIMO communication systems,” IEEE Commun. Theory Workshop, Sep. 2012, pp. 572–576.

[26] W. Yang, G. Durisi, T. Koch, and Y. Polyanskiy, “Diversity versus channel knowledge at finite block-length,” in Proc. IEEE Inf. Theory Workshop, Oct. 2014.

[27] W. Yang, G. Durisi, T. Koch, and Y. Polyanskiy, “Quasi-static multiple-antenna fading channels at finite blocklength,” IEEE Trans. Inf. Theory, vol. 60, no. 7, pp. 4232–4265, Jun. 2014.

[28] Y. Hu, J. Gross, and A. Schmeink, “On the capacity of relaying with finite blocklength,” IEEE Trans. Veh. Technol., vol. 65, no. 3, pp. 1790–1794, Mar. 2016.

[29] J. Chen, L. Zhang, Y.-C. Liang, and S. Ma, “Optimal resource allocation for multiuser NOMA in short packet communications,” IEEE Trans. Veh. Technol., vol. 69, no. 2, pp. 2141–2156, Feb. 2020.

[30] W. R. Ghanem, V. Jamali, Y. Sun, and R. Schober, “Resource allocation for multi-user downlink MISO OFDMA-UURLC systems,” IEEE Trans. Commun., vol. 68, no. 11, pp. 7184–7200, Nov. 2020.

[31] 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 Things J., vol. 8, no. 20, pp. 15512–15521, Oct. 2021.

[32] C. She et al., “A tutorial on ultra reliable and low-latency communications in 6G: Integrating domain knowledge into deep learning,” Proc. IEEE, vol. 109, no. 3, pp. 204–246, Mar. 2021.

[33] H. Wang et al., “Secure short-packet communications for mission-critical IoT applications,” IEEE Trans. Wireless Commun., vol. 18, no. 5, pp. 2565–2578, May 2019.

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

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

[36] N. Ari, N. Thomas, and L. Musavian, “Performance analysis of short packet communications with multiple eavesdroppers,” IEEE Trans. Commun., vol. 70, no. 10, pp. 6778–6789, Oct. 2022.

[37] 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, Mar. 2022.

[38] M. Zhang et al., “Artificial noise aided secrecy information and power transfer in OFDMA systems,” IEEE Wireless Commun., vol. 15, no. 4, pp. 3085–3096, Apr. 2016.

[39] J. Scarlett, V. Y. F. 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, Jan. 2017.

[40] A. Adhikary, J. Nam, J.-Y. Ahn, and G. Caire, “Joint user selection, power allocation, and precoding design with imperfect CSIT for multi-cell MIMO downlink systems,” IEEE Trans. Wireless Commun., vol. 19, no. 1, pp. 162–176, Jan. 2020.

[41] S. S. Christensen, R. Agarwal, E. De 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. Ji, F. Fang, and S. Li, “On artificial-noise-aided transmit design for multi-user MISO systems with integrated services,” IEEE Trans. Veh. Technol., vol. 66, no. 9, pp. 8179–8195, Sep. 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, 2021.

[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 Security, vol. 11, no. 11, pp. 2609–2623, Nov. 2016.

[45] S. Boyd and L. Vandenberghe, Convex Optimization, Cambridge, U.K.: Cambridge Univ. Press, 2004.

[46] 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, Aug. 2016.

[47] 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, May 2014.

[48] 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. Sci. Technol., Trans. Electr. Eng., vol. 43, no. S1, pp. 121–132, Jul. 2019.

[49] 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, Oct. 2013.

[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 Trans. Antennas Propag., vol. 55, no. 3, pp. 217–223, Jun. 2013.

[51] J. Choi, J. Park, and B. L. Evans, “Spectral efficiency bounds for interference-limited SVD-MIMO cellular communication systems,” IEEE Wireless Commun. Lett., vol. 6, no. 1, pp. 46–49, Jan. 2017.
Jeonghun Park (Member, IEEE) received the B.S. and M.S. degrees in electrical and electronic engineering from Yonsei University, Seoul, South Korea, in 2010 and 2012, respectively, and the Ph.D. degree in electrical and computer engineering from The University of Texas at Austin, TX, USA, in 2017. He is currently an Assistant Professor with the School of Electrical and Electronic Engineering, Yonsei University. Prior to Yonsei University, he worked with Qualcomm Wireless Research and Development, San Diego, USA, and Kyungpook National University, Daegu, South Korea. His research interests include developing and analyzing future wireless communication systems using tools of optimization, information theory, and machine learning.

Jinseok Choi (Member, IEEE) received the B.S. degree from the Department of Electrical and Electronic Engineering, Yonsei University, Seoul, South Korea, in 2014, and the M.S. and Ph.D. degrees in electrical and computer engineering from The University of Texas at Austin, TX, USA, in 2016 and 2019, respectively. He was a Student Member of the Wireless Networking and Communications Group (WNCG) under the supervision of Prof. Brian L. Evans. He was a Senior System Engineer with Wireless Research and Development, Qualcomm Inc., San Diego, CA, USA, and an Assistant Professor with the Ulsan National Institute of Science and Technology (UNIST). He is currently an Assistant Professor with the School of Electrical Engineering, Korea Advanced Institute of Science and Technology (KAIST). His research interests include developing and analyzing future wireless communication systems and to develop algorithms for intelligent devices that require ultra high-speed, high-reliability, and low-latency communications.