Decoding-Order-Aware Secrecy Rate Maximization in IRS-Assisted Untrusted NOMA Under Imperfect SIC

Ankit Kumar[1], Kaneez Khatoon[1], Deepak Mishra[2], and Ravikant Saini[1]
[1]Indian Institute of Technology Jammu, India
[2]University of New South Wales, Australia

***Abstract*—This work investigates an IRS-assisted downlink NOMA system with untrusted users under imperfect SIC, where internal eavesdropping—users intercepting each other's messages—poses distinct security challenges absent in conventional external-eavesdropper models. A key contribution is the systematic analysis of all possible decoding orders, proving that the $(2, 2)$ order yields the largest feasible power allocation region satisfying simultaneous secrecy and QoS constraints. The joint optimization of decoding order, power allocation, and IRS reflection coefficients is decomposed into two tractable subproblems: closed-form power allocation under perfect SIC and semidefinite relaxation (SDR)-based IRS phase optimization, solved via an alternating framework. Numerical results demonstrate performance improvements of 14.6% at low power (10 W) and 12.7% at high power (80 W) over benchmark schemes, validating the effectiveness of the proposed approach in balancing secrecy and service quality under practical SIC imperfections.**

***Index Terms*—Intelligent reflecting surface, non-orthogonal multiple access, physical layer security, untrusted users, secrecy rate maximization, QoS-aware optimization, imperfect successive interference cancellation.**

I. INTRODUCTION

NON-ORTHOGONAL multiple access (NOMA) has emerged as a key enabling technology for 5G and beyond wireless networks due to its ability to support multiple users on the same resource block, significantly improving spectral efficiency. However, NOMA's broadcast nature and reliance on successive interference cancellation (SIC) introduce significant security vulnerabilities. In practical deployments, SIC is inherently imperfect due to channel estimation errors, hardware impairments, and decoding failures [1], resulting in residual interference that degrades both system performance and security [2]. Physical layer security (PLS) techniques have been explored to safeguard NOMA transmissions against both external and internal threats [3].

Intelligent reflecting surfaces (IRS) offer energy-efficient improvements in coverage and throughput for next-generation wireless systems [4]. By deploying large arrays of low-cost passive reflecting elements, IRS can intelligently manipulate electromagnetic wave propagation to create favorable channel conditions [5]. Unlike active relaying or multi-antenna beamforming, IRS operates passively, consuming minimal power while providing substantial performance gains. The synergy between IRS and NOMA has been extensively investigated [6], [7], demonstrating superior performance in terms of both spectral efficiency and coverage enhancement.

A. Literature Review and Problem Motivation

Most prior work on secure IRS-NOMA systems assumes external eavesdroppers [6], [7]. However, internal eavesdropping-where legitimate users intercept each other's messages-fundamentally alters the secrecy formulation, as the same channel conditions used for data transmission also enable eavesdropping. This untrusted-user scenario has been studied in NOMA systems [3], [8], but extending to imperfect SIC while jointly addressing QoS constraints remains an open challenge. Secure transmission under internal eavesdropping in cooperative NOMA has been investigated in [8], while decoding order critically determines secrecy performance [3]. Imperfect SIC has been modeled in various NOMA contexts [1], [2], [9], but not specifically for untrusted IRS-assisted scenarios with joint decoding order optimization.

Imperfect hardware and SIC imperfections in NOMA have been recently characterized [10], and secure IRS-aided NOMA under imperfect CSI investigated [11]. However, these works do not jointly address QoS constraints, secrecy guarantees under internal eavesdropping, imperfect SIC modeling, IRS phase optimization, and systematic decoding order selection—the comprehensive framework we develop in this paper.

This work fills this gap by developing a comprehensive framework that jointly optimizes decoding order, power allocation, and IRS reflection coefficients to maximize secrecy rates while guaranteeing QoS under practical imperfect SIC conditions.

B. Novel Contributions

The main contributions are:

1) We develop a system model for IRS-assisted downlink NOMA with untrusted users under imperfect SIC, incorporating both direct and reflected links under Rayleigh fading and path loss.
2) We systematically investigate all four possible decoding orders and prove that $\mathcal{O}_4 = (2, 2)$ yields the largest feasible power allocation region under imperfect SIC when $\zeta \geq 2^{-R_{\text{th}}}$, providing key design insights for practical NOMA deployments.
3) We propose a joint resource allocation framework that decouples power allocation and IRS phase optimization.

D. Mishra's participation has been supported in part by the Australian Research Council Discovery Early Career Researcher Award (DECRA) – DE230101391

For perfect SIC ($\zeta = 0$), a Closed-form solution for power allocation is derived. When SIC is imperfect ($\zeta > 0$), bisection search is used instead. For IRS phase optimization, semidefinite relaxation (SDR) [12] with Gaussian randomization is applied in both cases.

4) We develop an alternating optimization algorithm that iteratively updates power allocation and IRS reflection coefficients, solved via bisection search and convex optimization tools, achieving monotonic convergence to a stationary point.
5) Numerical results demonstrate performance improvements of 14.6% at $P_s = 10$ W and 12.7% at $P_s = 80$ W over benchmark schemes.

II. SYSTEM MODEL

We consider an IRS-assisted downlink NOMA system as illustrated in Fig. 1, where a single BS communicates with two untrusted users U_1 and U_2, aided by an IRS of Q reflecting elements. A two-user model captures the fundamental secrecy-QoS tradeoff while avoiding severe inter-user interference and receiver complexity inherent in larger NOMA systems [3], [8], [13].

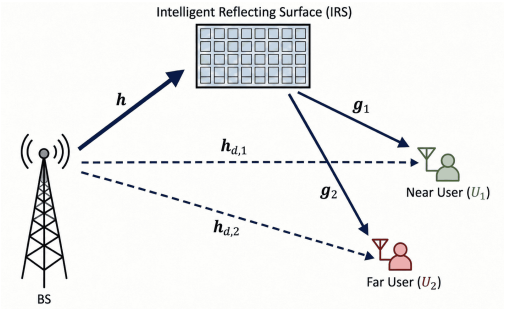


Fig. 1: IRS-assisted NOMA system with untrusted users. Near user U_1 requires secrecy while far user U_2 requires QoS.

Both direct BS-user and reflected BS-IRS-user links experience quasi-static Rayleigh fading with channel power gains following an exponential distribution with mean $L_p d^{-n}$, where L_p, n, and d denote the path-loss constant, path-loss exponent, and distance between nodes, respectively.

Remark 1: Perfect CSI at the BS is assumed for tractability, following standard practice in IRS-NOMA works [5], [8], [11]. Extending this to imperfect or statistical CSI is left for future work.

We assume $\lambda_2(\theta)\rho_t > \gamma_{\text{th}}$, ensuring the weak user's received SNR exceeds the QoS threshold-necessary for any feasible power allocation. The BS-IRS, IRS-U_k, and direct BS-U_k channels are $\mathbf{h} \in \mathbb{C}^{1\times Q}$, $\mathbf{g}_k \in \mathbb{C}^{Q\times 1}$, and $h_{d,k} \in \mathbb{C}$, $\forall k \in \mathcal{K} \triangleq \{1,2\}$, respectively.

The qth IRS element reflects with amplitude $\delta_q \in [0,1]$ and phase shift $\theta_q \in [0, 2\pi)$, $\forall q \in \mathcal{Q} \triangleq \{1,\ldots,Q\}$. The IRS phase-shift vector and matrix are $\boldsymbol{f}_p = [e^{j\theta_1},\ldots,e^{j\theta_Q}]^T$ and $\boldsymbol{\Theta} = \text{diag}(e^{j\theta_1},\ldots,e^{j\theta_Q})$, following [4]. The BS transmits the superimposed signal $\sqrt{\alpha P_s}s_1 + \sqrt{(1-\alpha)P_s}s_2$, where $\alpha \in (0,1)$ is the power allocation coefficient and P_s is the total transmit power. The received signal at U_k is

$$y_k = \left(\mathbf{g}_k^H \boldsymbol{\Theta}\mathbf{h} + h_{d,k}\right)\left(\sqrt{\alpha P_s}s_1 + \sqrt{(1-\alpha)P_s}s_2\right) + n_k \quad (1)$$

where n_k denotes AWGN with zero mean and variance σ^2. The end-to-end effective channel power gain is $\lambda_k(\theta) = |\mathbf{g}_k^H \boldsymbol{\Theta}\mathbf{h} + h_{d,k}|^2$, with $\lambda_1(\theta) > \lambda_2(\theta)$ corresponding to near and far users, respectively. Imperfect SIC leaves residual interference scaled by $\zeta \in [0,1]$, obtainable via [1], where $\zeta = 0$ is perfect SIC and $\zeta = 1$ represents complete SIC failure.

III. DECODING ORDER ANALYSIS AND SELECTION

In NOMA systems with untrusted users, the choice of decoding order significantly impacts both secrecy performance and quality-of-service (QoS) guarantees. This section analyzes all possible decoding orders and establishes the optimal choice for joint secrecy and QoS objectives.

We consider a two-user untrusted NOMA system with effective IRS-assisted channel gains $\lambda_k(\theta)$ for user U_k, $k \in \{1,2\}$, where $\lambda_1(\theta) \geq \lambda_2(\theta)$ so that U_1 is the strong user and U_2 is the weak user. The BS allocates power αP_s to U_1 and $(1-\alpha)P_s$ to U_2, where $\alpha \in (0,1)$, $\rho_t = P_s/\sigma^2$ is the transmit SNR, and $\zeta \in [0,1]$ models SIC imperfection.

A. SINR and Secrecy Rate Definitions

Let Γ_{ij} denote the SINR when U_j decodes the signal for U_i, and $R_{ij} = \log_2(1+\Gamma_{ij})$ be the corresponding rate. The strong user's secrecy rate is $R_{s,1} = \{R_{11} - R_{12}\}^+$, where $\{x\}^+ = \max(0,x)$. The weak user U_2 must satisfy the QoS constraint $R_{22} \geq R_{\text{th}}$, equivalent to $\Gamma_{22} \geq \gamma_{\text{th}} \triangleq 2^{R_{\text{th}}} - 1$.

A decoding order $\mathcal{O} = (i,j)$ indicates the user decoded first at U_1 and U_2, respectively. Four possible orders are [14]:

$$O_1 = (1,1),\ O_2 = (1,2),\ O_3 = (2,1),\ O_4 = (2,2). \quad (2)$$

B. Analysis of Decoding Order $O_4 = (2,2)$

In O_4, both users decode the weak user's message 2 first and the strong user's message 1 second after SIC. The SINRs are

$$\Gamma_{11} = \frac{\alpha\lambda_1(\theta)}{\lambda_1(\theta)(1-\alpha)\zeta + \frac{1}{\rho_t}}, \quad \Gamma_{12} = \frac{\alpha\lambda_2(\theta)}{\lambda_2(\theta)(1-\alpha)\zeta + \frac{1}{\rho_t}}, \quad (3)$$

$$\Gamma_{21} = \frac{(1-\alpha)\lambda_1(\theta)}{\alpha\lambda_1(\theta) + \frac{1}{\rho_t}}, \quad \Gamma_{22} = \frac{(1-\alpha)\lambda_2(\theta)}{\alpha\lambda_2(\theta) + \frac{1}{\rho_t}}. \quad (4)$$

Strong-user secrecy requires $\Gamma_{11} > \Gamma_{12}$, which gives $\lambda_1(\theta) > \lambda_2(\theta)$ (satisfied by definition). The QoS constraint $\Gamma_{22} \geq \gamma_{\text{th}}$ yields

$$\alpha \leq \alpha_{\max}^{(4)} \triangleq \frac{\lambda_2(\theta) - \frac{\gamma_{\text{th}}}{\rho_t}}{\lambda_2(\theta)(1+\gamma_{\text{th}})}. \quad (5)$$

Feasible region: $\mathcal{F}_4 = (0, \alpha_{\max}^{(4)}]$.

C. Analysis of Decoding Order $O_1 = (1,1)$

In O_1, both users decode message 1 first and message 2 second. The SINRs are

$$\Gamma_{11} = \frac{\alpha\lambda_1(\theta)}{(1-\alpha)\lambda_1(\theta) + \frac{1}{\rho_t}}, \quad \Gamma_{12} = \frac{\alpha\lambda_2(\theta)}{(1-\alpha)\lambda_2(\theta) + \frac{1}{\rho_t}}, \quad (6)$$

$$\Gamma_{21} = \frac{(1-\alpha)\lambda_1(\theta)}{\alpha\lambda_1(\theta)\zeta + \frac{1}{\rho_t}}, \quad \Gamma_{22} = \frac{(1-\alpha)\lambda_2(\theta)}{\alpha\lambda_2(\theta)\zeta + \frac{1}{\rho_t}}. \quad (7)$$

TABLE I: Feasible Power Allocation Regions

Order	Secrecy Constraint	Feasible Region
O_1	$\lambda_1(\theta) > \lambda_2(\theta)$	$(0, \alpha_{\max}^{(1)}]$
O_2	$\alpha > \alpha_{\min}^{(2)}$	$(\alpha_{\min}^{(2)}, \alpha_{\max}^{(2)}]$
O_3	non-binding	$(0, \alpha_{\max}^{(3)}]$
O_4	$\lambda_1(\theta) > \lambda_2(\theta)$	$(0, \alpha_{\max}^{(4)}]$

Secrecy depends only on channel ordering. The QoS constraint gives

$$\alpha \le \alpha_{\max}^{(1)} = \frac{\lambda_2(\theta) - \frac{\gamma_{\text{th}}}{\rho_t}}{\lambda_2(\theta)[\gamma_{\text{th}} + \zeta(1+\gamma_{\text{th}})]}. \tag{8}$$

For $\zeta \ge 2^{-R_{\text{th}}}$, we have $\alpha_{\max}^{(1)} \le \alpha_{\max}^{(4)}$, i.e., $\mathcal{F}_4 \supseteq \mathcal{F}_1$.

D. Analysis of Decoding Orders O_2 and O_3

For $O_2 = (1, 2)$, the SINRs are

$$\Gamma_{11} = \frac{\alpha\lambda_1(\theta)}{(1-\alpha)\lambda_1(\theta) + \frac{1}{\rho_t}}, \quad \Gamma_{12} = \frac{\alpha\lambda_2(\theta)}{(1-\alpha)\lambda_2(\theta)\zeta + \frac{1}{\rho_t}}, \tag{9}$$

$$\Gamma_{21} = \frac{(1-\alpha)\lambda_1(\theta)}{\alpha\lambda_1(\theta)\zeta + \frac{1}{\rho_t}}, \quad \Gamma_{22} = \frac{(1-\alpha)\lambda_2(\theta)}{\alpha\lambda_2(\theta) + \frac{1}{\rho_t}}. \tag{10}$$

Secrecy requires $\alpha > \alpha_{\min}^{(2)} = 1 - \frac{\lambda_1(\theta)-\lambda_2(\theta)}{(1-\zeta)\lambda_1(\theta)\lambda_2(\theta)\rho_t}$, and QoS gives $\alpha \le \alpha_{\max}^{(2)} = \alpha_{\max}^{(4)}$. Feasible region: $\mathcal{F}_2 = (\alpha_{\min}^{(2)}, \alpha_{\max}^{(2)}]$ (empty if $\alpha_{\min}^{(2)} \ge \alpha_{\max}^{(2)}$).

For $O_3 = (2, 1)$, secrecy constraint is non-binding since $\lambda_1(\theta) > \lambda_2(\theta)$ and $\zeta < 1$ ensure the added fraction is positive. QoS gives

$$\alpha \le \alpha_{\max}^{(3)} = \frac{\lambda_2(\theta) - \frac{\gamma_{\text{th}}}{\rho_t}}{\lambda_2(\theta)[\zeta + \gamma_{\text{th}}(1+\zeta)]}. \tag{11}$$

Feasible region: $\mathcal{F}_3 = (0, \alpha_{\max}^{(3)}]$.

E. Optimal Decoding Order Selection

Proposition 1: For $\zeta \ge 2^{-R_{\text{th}}}$, decoding order $O_4 = (2, 2)$ yields the largest feasible power-allocation region among all four orders.

Proof 1: Since $\zeta \ge 2^{-R_{\text{th}}}$ implies $\gamma_{\text{th}} + \zeta(1+\gamma_{\text{th}}) \ge 1 + \gamma_{\text{th}}$, and both $\alpha_{\max}^{(4)}$ and $\alpha_{\max}^{(1)}$ share identical numerators, we have $\alpha_{\max}^{(4)} \ge \alpha_{\max}^{(1)}$, giving $\mathcal{F}_4 \supseteq \mathcal{F}_1$. Since $\alpha_{\max}^{(2)} = \alpha_{\max}^{(4)}$ but O_2 has additional lower bound $\alpha_{\min}^{(2)} > 0$, we have $\mathcal{F}_4 \supset \mathcal{F}_2$. Similarly, $\alpha_{\max}^{(3)} \le \alpha_{\max}^{(4)}$ gives $\mathcal{F}_4 \supseteq \mathcal{F}_3$.

Remark 2: For perfect SIC ($\zeta = 0$), $\alpha_{\max}^{(1)} > \alpha_{\max}^{(4)}$.

Physical Intuition: Order $O_4 = (2, 2)$ dominates under imperfect SIC because both users decode the weak signal first, minimizing residual interference exposure. When U_2's message is decoded first, residual interference $\zeta\alpha P_s$ is manageable since α can be kept small for QoS. Conversely, in $O_1 = (1, 1)$, residual $\zeta(1-\alpha)P_s$ when decoding U_2 is larger and harmful. In O_4, the strong user decodes its own message last, experiencing minimal eavesdropping risk, naturally balancing secrecy and QoS under practical SIC imperfections.

IV. SUM SECURE RATE MAXIMIZATION

Based on Proposition 1, we adopt decoding order $O_4 = (2, 2)$ for the remainder of this paper, assuming $\lambda_1(\theta) > \lambda_2(\theta)$ throughout.

Under decoding order O_4, the sum secrecy rate is:

$$R_s = R_{s,1} + R_{22} = (R_{11} - R_{12}) + R_{22}. \tag{12}$$

The joint optimization problem is:

$$\begin{aligned} \mathcal{P}_1 : \max_{\alpha, \boldsymbol{\Theta}} \quad & R_s \\ \text{s.t.} \quad & (C_1) : 0 \le \alpha \le 1, \quad (C_2) : |[\boldsymbol{\Theta}]_{qq}| = 1, \forall q \in \mathcal{Q}, \\ & (C_3) : R_{22} \ge R_{\text{th}}. \end{aligned} \tag{13}$$

SDR Relaxation Rationale: Problem $\mathcal{P}_1$ is non-convex due to the unit-modulus constraint (C_2) and the rank-one structure of $\boldsymbol{\Theta}$. To obtain a tractable solution, we employ semidefinite relaxation (SDR) [12]. By lifting the optimization variable from $\boldsymbol{f}_p \in \mathbb{C}^{Q\times 1}$ to the matrix $\boldsymbol{\mathcal{F}} = \boldsymbol{f}_p \boldsymbol{f}_p^H \in \mathbb{C}^{Q\times Q}$, the unit-modulus constraints become diagonal constraints $\boldsymbol{\mathcal{F}}_{qq} = 1$, and the objective becomes concave in $\boldsymbol{\mathcal{F}}$. The non-convex rank-one constraint $\text{rank}(\boldsymbol{\mathcal{F}}) = 1$ is relaxed to $\boldsymbol{\mathcal{F}} \succeq 0$, yielding a convex SDP. If the optimal $\boldsymbol{\mathcal{F}}^*$ has rank one, the solution is exact; otherwise, Gaussian randomization recovers a near-optimal rank-one solution.

Defining $\boldsymbol{f}_p = [f_1, \ldots, f_Q]^H$ where $f_q = e^{j\theta_q}$, $\boldsymbol{H}_1 = \text{diag}(\boldsymbol{h})\boldsymbol{g}_1^H$, $\boldsymbol{H}_2 = \text{diag}(\boldsymbol{h})\boldsymbol{g}_2^H$, $\boldsymbol{\mathcal{F}} = \boldsymbol{f}_p \boldsymbol{f}_p^H$, $\boldsymbol{G}_{iu1} = \boldsymbol{H}_1 \boldsymbol{H}_1^H$, and $\boldsymbol{G}_{iu2} = \boldsymbol{H}_2 \boldsymbol{H}_2^H$. The simplified sum secrecy rate is given by (14) below.

Quadratic Transform: To handle the fractional form in (15), we employ the quadratic transform technique [12], which introduces auxiliary variables y_1, y_2, y_3 to convert each log-fraction into a difference-of-convex (DC) form. This enables iterative optimization via the concave-convex procedure (CCCP), where auxiliary variables are updated in lines 7–12 of Algorithm 1. The transformed sum rate is:

$$\bar{R}_s = \log_2(1+M_1^+) + \log_2\big(1 - 1/M_2^-\big) + \log_2(1+M_3^+), \tag{18}$$

where

$$M_1^+ = 2y_1\sqrt{\text{Tr}(\boldsymbol{\mathcal{F}}\boldsymbol{G}_{iu1})\alpha} - y_1^2\left(\text{Tr}(\boldsymbol{\mathcal{F}}\boldsymbol{G}_{iu1})(1-\alpha)\zeta + \frac{1}{\rho_t}\right),$$

$$M_2^- = 2y_2\sqrt{(1-\alpha)\text{Tr}(\boldsymbol{\mathcal{F}}\boldsymbol{G}_{iu2}) + \frac{1}{\rho_t}} - y_2^2(\alpha\text{Tr}(\boldsymbol{\mathcal{F}}\boldsymbol{G}_{iu2})),$$

$$M_3^+ = 2y_3\sqrt{(1-\alpha)\text{Tr}(\boldsymbol{\mathcal{F}}\boldsymbol{G}_{iu2})} - y_3^2\left(\text{Tr}(\boldsymbol{\mathcal{F}}\boldsymbol{G}_{iu2})\alpha\zeta + \frac{1}{\rho_t}\right),$$

and y_1, y_2, y_3 are given in (17).

The equivalent simplified optimization problem is:

$$\begin{aligned} \mathcal{P}_2 : \max_{\boldsymbol{\mathcal{F}}} \quad & \bar{R}_s \\ \text{s.t.} \quad & (C_4) : \boldsymbol{\mathcal{F}}_{q,q} = 1, \quad \forall q = 1, 2, \ldots, Q, \\ & (C_5) : \text{Tr}(\boldsymbol{\mathcal{F}}\boldsymbol{G}_{iu1}) \ge \text{Tr}(\boldsymbol{\mathcal{F}}\boldsymbol{G}_{iu2}), \\ & (C_6) : \boldsymbol{\mathcal{F}} \succeq 0, \quad (C_7) : \text{rank}(\boldsymbol{\mathcal{F}}) = 1. \end{aligned} \tag{19}$$

$\mathcal{P}_2$ is a standard convex SDP solvable via CVX. When $\text{rank}(\boldsymbol{\mathcal{F}}) \ne 1$, Gaussian randomization extracts a rank-one solution: $\boldsymbol{f}_p = \boldsymbol{U}\boldsymbol{\Sigma}^{1/2}\boldsymbol{r}$, where $\boldsymbol{\mathcal{F}} = \boldsymbol{U}\boldsymbol{\Sigma}\boldsymbol{U}^H$ is the eigenvalue decomposition and $\boldsymbol{r} \in \mathcal{CN}(\boldsymbol{0}, \mathbf{I}_Q)$.

$$R_s = \log_2\left(1+\frac{\alpha\lambda_1(\theta)}{\lambda_1(\theta)(1-\alpha)\zeta+\frac{1}{\rho_t}}\right)+\log_2\left(\frac{\lambda_2(\theta)(1-\alpha)\zeta+\frac{1}{\rho_t}}{\lambda_2(\theta)[\zeta+\alpha(1-\zeta)]+\frac{1}{\rho_t}}\right)+\log_2\left(1+\frac{(1-\alpha)\lambda_2(\theta)}{\lambda_2(\theta)\alpha\zeta+\frac{1}{\rho_t}}\right) \tag{14}$$

$$\bar{R}_s = \log_2\left(1+\frac{\mathrm{Tr}(\boldsymbol{\mathcal{F}}\boldsymbol{G}_{iu1})\,\alpha}{\mathrm{Tr}(\boldsymbol{\mathcal{F}}\boldsymbol{G}_{iu1})(1-\alpha)\zeta+\frac{1}{\rho_t}}\right)+\log_2\left(\frac{\mathrm{Tr}(\boldsymbol{\mathcal{F}}\boldsymbol{G}_{iu2})(1-\alpha)\zeta+\frac{1}{\rho_t}}{\mathrm{Tr}(\boldsymbol{\mathcal{F}}\boldsymbol{G}_{iu2})[\zeta+\alpha(1-\zeta)]+\frac{1}{\rho_t}}\right)+\log_2\left(1+\frac{(1-\alpha)\,\mathrm{Tr}(\boldsymbol{\mathcal{F}}\boldsymbol{G}_{iu2})}{\mathrm{Tr}(\boldsymbol{\mathcal{F}}\boldsymbol{G}_{iu2})\,\alpha\zeta+\frac{1}{\rho_t}}\right) \tag{15}$$

$$\begin{aligned}\frac{dR_s}{d\alpha} = \frac{1}{\ln 2}\Bigg[&\frac{\lambda_1(\theta)\left(\lambda_1(\theta)\zeta+\frac{1}{\rho_t}\right)}{\left(\lambda_1(\theta)(1-\alpha)\zeta+\frac{1}{\rho_t}\right)\left(\lambda_1(\theta)[\zeta+\alpha(1-\zeta)]+\frac{1}{\rho_t}\right)}-\frac{\lambda_2(\theta)\left(\lambda_2(\theta)\zeta+\frac{1}{\rho_t}\right)}{\left(\lambda_2(\theta)(1-\alpha)\zeta+\frac{1}{\rho_t}\right)\left(\lambda_2(\theta)[\zeta+\alpha(1-\zeta)]+\frac{1}{\rho_t}\right)}\\&-\frac{\lambda_2(\theta)\left(\lambda_2(\theta)\zeta+\frac{1}{\rho_t}\right)}{\left(\lambda_2(\theta)\alpha\zeta+\frac{1}{\rho_t}\right)\left(\lambda_2(\theta)[\zeta+(1-\alpha)(1-\zeta)]+\frac{1}{\rho_t}\right)}\Bigg]=0\end{aligned} \tag{16}$$

$$y_1=\sqrt{\frac{\mathrm{Tr}(\boldsymbol{\mathcal{F}}\boldsymbol{G}_{iu1})\,\alpha}{\mathrm{Tr}(\boldsymbol{\mathcal{F}}\boldsymbol{G}_{iu1})(1-\alpha)\zeta+\frac{1}{\rho_t}}},\quad y_2=\sqrt{\frac{(1-\alpha)\,\mathrm{Tr}(\boldsymbol{\mathcal{F}}\boldsymbol{G}_{iu2})+\frac{1}{\rho_t}}{\alpha\,\mathrm{Tr}(\boldsymbol{\mathcal{F}}\boldsymbol{G}_{iu2})}},\quad y_3=\sqrt{\frac{(1-\alpha)\,\mathrm{Tr}(\boldsymbol{\mathcal{F}}\boldsymbol{G}_{iu2})}{\mathrm{Tr}(\boldsymbol{\mathcal{F}}\boldsymbol{G}_{iu2})\,\alpha\zeta+\frac{1}{\rho_t}}} \tag{17}$$

For α, we set $dR_s/d\alpha = 0$ as given in (16). A closed-form solution exists only for $\zeta = 0$ (perfect SIC), as shown in Remark 3. For $\zeta > 0$ (imperfect SIC), the transcendental nature of (16) necessitates numerical root-finding methods such as Newton-Raphson or bisection search.

Remark 3: For perfect SIC ($\zeta = 0$), setting $dR_s/d\alpha = 0$ yields a quadratic equation in α with roots:

$$\alpha_{1,2} = \frac{\sqrt{\lambda_1(\theta)}\,[\pm\sqrt{(\lambda_1(\theta)-\lambda_2(\theta))(\lambda_2(\theta)\rho_t+2)}]-\lambda_1(\theta)}{\lambda_1(\theta)\lambda_2(\theta)\rho_t}, \tag{20}$$

Only α_1 (taking the $+$ sign) lies in $(0, 1)$ and is feasible.

Remark 4: After obtaining the optimal power allocation coefficient, QoS constraint (C_3) must be verified. If α violates $R_{22} \geq R_{\text{th}}$, then α is set to $\alpha^{(4)}_{\max}$ from (5).

Algorithm 1 Alternating Optimization Scheme

Input: $Q, P_s, \sigma^2, \boldsymbol{g}_k, \boldsymbol{h}, \zeta, R_{\text{th}}$, tolerance $\epsilon \ll 1$
Output: $\alpha^*, R_s^*, \boldsymbol{f}_p^*$
Initialize: $i = 1$, $\boldsymbol{f}_p = \exp(j \cdot \mathbf{0})$ ▷ Coherent combining baseline
Compute initial R_s using (14)
while true **do**
  $i = i + 1$; $j = 1$;
  while true **do**
    Compute y_1, y_2, y_3 by substituting current α and $\boldsymbol{f}_p$ into (17)
    $j = j + 1$
    Evaluate R_s^j using (18) with updated y_1, y_2, y_3
    if $R_s^j - R_s^{j-1} < \epsilon$ **then break**
    end if
  end while
  Solve SDP $\mathcal{P}_2$ in (19) using CVX to find $\boldsymbol{\mathcal{F}}^*$
  Extract rank-one solution: If $\mathrm{rank}(\boldsymbol{\mathcal{F}}^*) = 1$, set $\boldsymbol{f}_p = \mathrm{eig}_{\max}(\boldsymbol{\mathcal{F}}^*)$; else apply Gaussian randomization
  if $\zeta = 0$ **then**
    Compute α using closed-form (20)
  else
    Solve $dR_s/d\alpha = 0$ in (16) via bisection search
  end if
  Check QoS: If $R_{22}(\alpha) < R_{\text{th}}$, set $\alpha = \alpha^{(4)}_{\max}$ from (5)
  Compute R_s^i using (14) with updated $\alpha, \boldsymbol{f}_p$
  if $R_s^i - R_s^{i-1} < \epsilon$ **then break** ▷ Outer loop converged
  end if
end while
Return $\alpha^* = \alpha^i$, $\boldsymbol{f}_p^* = \boldsymbol{f}_p^i$, $R_s^* = R_s^i$

V. NUMERICAL RESULTS

In this section, numerical experiments evaluate the performance of the proposed IRS-assisted untrusted NOMA system. Unless stated otherwise, system parameters are: $K = 2$, $Q = 16$, $P_s = 40$ W, BS-to-IRS distance $d_1 = 35$ m, IRS-to-near-user $d_2 = 28$ m, and IRS-to-far-user $\sqrt{d_2^2 + y^2}$ with $y = 20$ m. A distance scaling factor β replaces each link distance d_i with βd_i to assess varying path-loss conditions. All links undergo quasi-static Rayleigh fading with noise variance $\sigma^2 = -110$ dBm, SIC imperfection factor $\zeta = 0.2$, and QoS threshold $R_{\text{th}} = 0.5$ bps/Hz. Each result is obtained by averaging over 10^3 independent channel realizations.

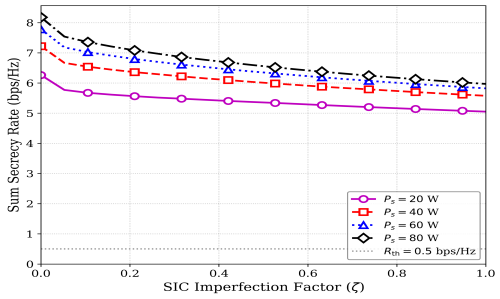
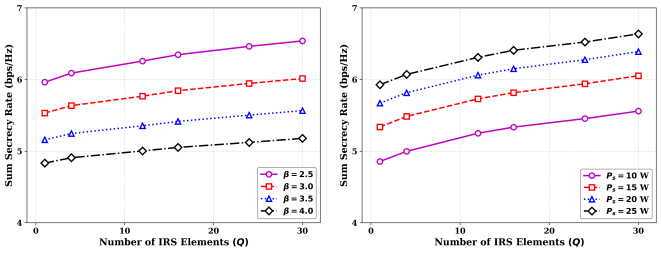


Fig. 2: Impact of SIC imperfection on sum secrecy rate.

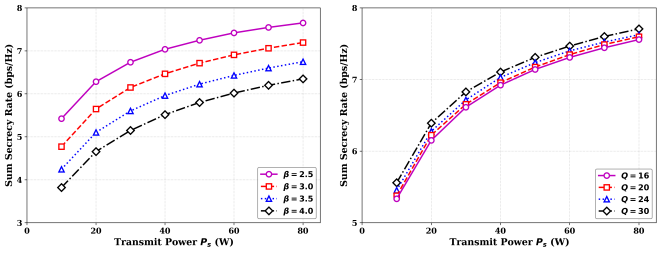
Fig. 2 quantifies performance degradation under imperfect SIC. As ζ increases from 0 to 1, relative loss grows from 19.0% to 26.8% across power levels, with higher degradation at elevated P_s due to residual interference in high-SNR regimes. All curves remain above the QoS threshold.

Fig. 3 shows secure rate variation with the number of IRS elements Q. In Fig. 3(a), secure rate increases with Q as more IRS elements provide greater beamforming diversity. As β increases, channel gains reduce, leading to lower rates; at $Q = 30$, rates span 5.2–6.7 bps/Hz as β varies from 4.0 to 2.5. In Fig. 3(b), the sum secrecy rate increases with P_s, with 15.7% improvement when power increases from 10 W to 25 W at $Q = 30$.



(a) (b)

Fig. 3: Sum secrecy rate vs. Q: (a) various β (b) various P_s.



(a) (b)

Fig. 4: Sum secrecy rate vs. P_s: (a) various β (b) various Q.

Fig. 4 presents secure rate variation with P_s. Fig. 4(a) shows concave growth reflecting NOMA's interference-limited nature; for $\beta = 2.5$, rate increases from 5.4 to 7.65 bps/Hz as P_s rises from 10 to 80 W. Fig. 4(b) confirms that larger IRS arrays provide greater gains in noise-limited (low P_s) than interference-limited (high P_s) regimes.

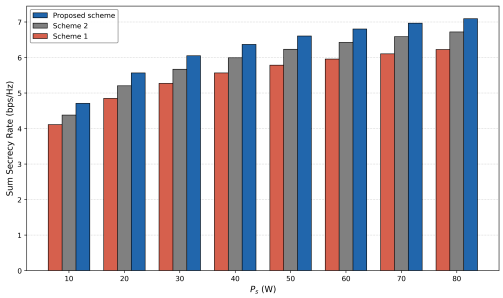


Fig. 5: Performance comparison of joint optimization scheme.

The performance comparison with two benchmark schemes is shown in Fig. 5. In Scheme 1, $\mathbf{\Theta} = \mathbf{I}$ is used with optimal closed-form α from (20). In Scheme 2, a fixed $\mathbf{\Theta}$ is used with α optimized via (16). The proposed scheme jointly optimizes both α and $\mathbf{\Theta}$ through Algorithm 1, exploiting the interdependence between power allocation and IRS phase design to maximize secrecy rates. The proposed method achieves 14.6% and 6.8% gains over the two baselines at $P_s = 10$ W, and 12.7% and 6.0% at $P_s = 80$ W, validating that neither power allocation nor IRS phase optimization alone achieves the performance of joint optimization.

VI. CONCLUSION

This paper investigated sum secrecy rate maximization in an IRS-assisted downlink NOMA system with untrusted users and imperfect SIC. A key insight is that decoding order fundamentally determines the feasible secrecy-QoS region under imperfect SIC: decoding order $O_4 = (2, 2)$ was proven optimal for $\zeta \geq 2^{-R_{\text{th}}}$, maximizing the power allocation region satisfying simultaneous near-user secrecy and far-user QoS constraints. The practical takeaway is that joint IRS phase design and power allocation is essential—neither can be optimized independently without significant performance loss. An alternating optimization algorithm efficiently decoupled these interdependent subproblems. Numerical results confirmed monotonic rate growth with Q and P_s, achieving 14.6% and 12.7% gains at 10 W and 80 W respectively over benchmarks that optimize only one dimension.

Future work includes: (1) extension to multi-antenna BSs with transmit beamforming, (2) robust optimization under imperfect/statistical CSI, (3) multi-user NOMA with $K > 2$ users and mixed trust levels, and (4) integration with rate-splitting multiple access (RSMA) for enhanced fairness and security.

REFERENCES

[1] N. S. Mouni, A. Kumar, and P. K. Upadhyay, "Adaptive user pairing for NOMA systems with imperfect SIC," *IEEE Wireless Commun. Lett.*, vol. 10, no. 7, pp. 1547–1551, Jul. 2021.

[2] S. S. Chauhan, S. Kumar, A. Bhardwaj, and B. Deka, "RIS partition-assisted non-orthogonal multiple access (NOMA) and quadrature-NOMA with imperfect SIC," *IEEE Trans. Wireless Commun.*, vol. 22, no. 7, pp. 4371–4386, Jul. 2023.

[3] K. Cao, B. Wang, H. Ding, T. Li, J. Tian, and F. Gong, "Secure transmission designs for NOMA systems against internal and external eavesdropping," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2930–2943, Jan. 2020.

[4] C. Pan, H. Ren, K. Wang, J. F. Kolb, M. Elkashlan, M. Chen, M. Di Renzo, Y. Hao, J. Wang, A. L. Swindlehurst, X. You, and L. Hanzo, "Reconfigurable intelligent surfaces for 6G systems: Principles, applications, and research directions," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 2, pp. 1388–1422, 2021.

[5] Q. Wu and R. Zhang, "Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming," *IEEE Trans. Wireless Commun.*, vol. 18, no. 11, pp. 5394–5409, Nov. 2019.

[6] X. Wang, W. Hao, P. Zhu, G. Sun, and P. Xiao, "Beamforming and jamming optimization for IRS-aided secure NOMA networks," *IEEE Trans. Wireless Commun.*, vol. 21, no. 3, pp. 1557–1569, Mar. 2022.

[7] S.-P. Le, H.-N. Nguyen, N.-T. Nguyen, C. H. Van, A.-T. Le, and M. Voznak, "Physical layer security analysis of IRS-based downlink and uplink NOMA networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2023, no. 1, Art. no. 105, Oct. 2023.

[8] B. Su, W. Yu, H. Liu, A. Chorti, and H. V. Poor, "Secure transmission design for cooperative NOMA in the presence of internal eavesdropping," *IEEE Wireless Commun. Lett.*, vol. 11, no. 5, pp. 878–882, May 2022.

[9] J. Gu, M. Wang, W. Duan, L. Zhang, and H. Zhang, "RIS-NOMA communications over Nakagami-m fading with imperfect successive interference cancellation," *Comput. Commun.*, vol. 226–227, p. 107926, 2024.

[10] X. Yue, M. Song, C. Ouyang, Y. Liu, T. Li, and T. Hou, "Exploiting active RIS in NOMA networks with hardware impairments," *IEEE Trans. Veh. Technol.*, vol. 73, no. 6, pp. 8207–8221, Jun. 2024.

[11] X. Li, M. Liu, C. Deng, X. Guan, Z. Ding, and H. V. Poor, "Secure RIS-aided NOMA: Joint beamforming and phase shift optimization under imperfect CSI," *IEEE Trans. Commun.*, vol. 73, no. 2, pp. 845–860, Feb. 2025.

[12] K. Shen and W. Yu, "Fractional programming for communication systems—Part I: Power control and beamforming," *IEEE Trans. Signal Process.*, vol. 66, no. 10, pp. 2616–2630, May 2018.

[13] K. Khatoon, D. Mishra, and R. Saini, "Irs assisted secure noma for untrusted users," in *2024 IEEE International Conference on Acoustics, Speech, and Signal Processing Workshops (ICASSPW)*, 2024, pp. 356–360.

[14] ——, "Joint optimization of decoding order, power allocation and reflection coefficients in an irs assisted untrusted secure noma," *IEEE Wireless Communications Letters*, vol. 14, no. 4, pp. 1069–1073, 2025.