ARTICLE IN PRESS

The Korean Institute of Communications and Information Sciences

Available online at www.sciencedirect.com

ScienceDirect

ICT Express xxx (xxxx) xxx

www.elsevier.com/locate/icte

# Intelligent reflecting surface-aided MIMO secrecy rate maximization

Minsik Kim[a], Daeyoung Park[a,*]

[a] *Department of Information and Communication, Inha University, Republic of Korea*

Received 15 August 2021; received in revised form 19 February 2022; accepted 16 March 2022
Available online xxxx

**Abstract**

This paper considers the intelligent reflecting surface-aided MIMO secrecy rate maximization. We apply the alternating optimization to maximize the secrecy rate of the MIMO wiretap channels. We first provide the closed-form solution to each subproblem of optimizing reflecting unit coefficient and show that the sequence generated by the coordinate descent method converges to a stationary point of the main optimization problem. Numerical results show that the intelligent reflecting surface significantly increases secrecy rates in MIMO wiretap channels.


*Keywords:* Intelligent reflecting surface; MIMO; Secrecy rate

## 1. Introduction

Intelligent reflecting surface (IRS) is a promising solution that can cost-effectively and energy-efficiently improve wireless communication capacity by adjusting a large number of passive reflecting units to appropriately change signal propagation [1]. IRS implemented with conventional reflectarray antennas or software defined metamaterials can achieve passive beamforming for directional signal enhancement or nulling by adjusting reflecting unit phase and amplitude. Recently, IRS has been considered in physical layer security and MISO/MIMO systems to improve wireless communication capabilities [2]. In addition, the benefits of joint non-orthogonal multiple access and IRS were investigated [3]. However, in scenarios where the channels of the legitimate communication link and the channel of the eavesdropping link are spatially highly correlated, the achievable secrecy rate may be very limited.

In the literature, there have been many works that tried to improve achievable secrecy rates in various IRS-aided communication scenarios with an eavesdropper (Eves). Several researches aim to maximize the secrecy rate of the IRS-aided MISO channel by jointly optimizing the source transmit covariance and IRS's phase shift matrix. To improve the achievable secrecy rate, an approximate method based on semidefinite relaxation (SDR) and Gaussian randomization methods was proposed in [4]. Since SDR with Gaussian randomization is computationally heavy, [5] replaced it with a simple neural network at the cost of reduced secrecy rates. The case where the line-of-sight link between the transmitter and user/eavesdropper was blocked was considered in [6,7]. An algorithm using fractional programming and majorization minimization (MM) was proposed in the case of multiple antennas at the eavesdropper [8]. Bisection search (BS) and majorization minimization combined with alternating optimization (AO) algorithm was proposed in the case of the IRS-aided MIMO channel [9].

In this paper, we consider the secure communication from a multi-antenna transmitter to a multi-antenna legitimate user in the presence of a multi-antenna eavesdropper, where an IRS is deployed in the locality of the user and the eavesdropper. First, we can improve the secrecy rate by adjusting the phase shift of the IRS reflecting units. Second, the transmit signal can be designed to balance the signal power towards the IRS and each user/eavesdropper for signal enhancement/cancellation. Thus, by jointly optimizing the active transmit signal at the transmitter and the phase of the IRS reflecting units, the secrecy rate can be maximized. However, this optimization problem is difficult to solve because it has coupled variables and is a non-convex problem. We propose an efficient algorithm to solve this problem based on alternating optimization methods.

Our contributions are summarized as follows: We present a secrecy rate maximization algorithm in IRS-aided MIMO

* Corresponding author.
*E-mail address:* dpark@inha.ac.kr (D. Park).
Peer review under responsibility of The Korean Institute of Communications and Information Sciences (KICS).

https://doi.org/10.1016/j.icte.2022.03.009

wiretap channels. We apply the coordinate descent method and provide the optimal reflection coefficients in closed-form expressions. The proposed closed-form expressions can achieve the maximum secrecy rate faster and more accurately than the conventional method of applying approximation or solving the problem with numerical algorithm. To the best of our knowledge, this paper first provides the closed-form expression for optimal reflection coefficients without resorting to any additional numerical optimization for IRS-aided MIMO secrecy rate maximization.

## 2. IRS-aided secrecy rate maximization

We consider an IRS-aided MIMO wiretap channel, where receiver 1 is a legitimate user and receiver 2 is an eavesdropper. Fig. 1 depicts the system model for IRS-aided MIMO wiretap channels. The transmitter is equipped with $N_t$ antennas and receiver $i$ for $i = 1, 2$ is equipped with $N_{r,i}$ antennas. Let $\mathbf{H}_i \in \mathbb{C}^{N_{r,i}\times N_t}$ denote the direct channel from the transmitter to receiver $i$. An IRS is equipped with $M$ passive reflecting units that can re-scatter the signals with adjustable amplitude and/or phase. We assume the IRS controller adjusts the phase of the reflection coefficient $\alpha_m \in \mathbb{C}$, i.e., $|\alpha_m| = 1$, $m = 1, 2, \ldots, M$. $\mathbf{T} \in \mathbb{C}^{N_t\times M}$ is the channel from the IRS to the transmitter, and $\mathbf{R}_i \in \mathbb{C}^{N_{r,i}\times M}$ is the channel from the IRS to receiver $i$. Due to the channel reciprocity, the channel from the transmitter to IRS is $\mathbf{T}^H \in \mathbb{C}^{M\times N_t}$. Let $\boldsymbol{\Phi} = \operatorname{diag}\{\alpha_1, \alpha_2, \ldots, \alpha_M\}$ denote the diagonal reflection coefficient matrix of the IRS.

The received signals are given by $\mathbf{y}_i = \tilde{\mathbf{H}}_i\mathbf{x} + \mathbf{z}_i$, $i = 1, 2$, where the effective channel from the transmitter to receiver $i$ is given by $\tilde{\mathbf{H}}_i = \mathbf{H}_i + \mathbf{R}_i\boldsymbol{\Phi}\mathbf{T}^H$. $\mathbf{x}$ is the transmitted signal with the power constraint $\operatorname{tr}(\mathbf{Q}) \le P$ with $\mathbf{Q} = \mathbb{E}[\mathbf{x}\mathbf{x}^H] \in \mathbb{C}^{N_t\times N_t}$ and $\mathbf{z}_i \sim \mathcal{CN}(0, \mathbf{I})$ is the Gaussian noise vector. Suppose the IRS reflection coefficients are given. Then, the achievable secrecy rate of the MIMO wiretap channel is given by [10]

$$C(\mathbf{Q}, \boldsymbol{\Phi}) = \log\left|\mathbf{I} + \tilde{\mathbf{H}}_1\mathbf{Q}\tilde{\mathbf{H}}_1^H\right| - \log\left|\mathbf{I} + \tilde{\mathbf{H}}_2\mathbf{Q}\tilde{\mathbf{H}}_2^H\right|, \tag{1}$$

which is a function of $\mathbf{Q}$ and $\boldsymbol{\Phi}$. Here, $|\mathbf{A}|$ denotes the determinant of $\mathbf{A}$. We aim to maximize the secrecy rate of the IRS-aided MIMO wiretap channel by jointly optimizing $\boldsymbol{\Phi}$ and $\mathbf{Q}$

$$\begin{aligned}
\text{(P1)}\ \max_{\mathbf{Q},\boldsymbol{\Phi}}\ & \log\left|\mathbf{I} + \tilde{\mathbf{H}}_1\mathbf{Q}\tilde{\mathbf{H}}_1^H\right| - \log\left|\mathbf{I} + \tilde{\mathbf{H}}_2\mathbf{Q}\tilde{\mathbf{H}}_2^H\right| \\
\text{s.t. } & \boldsymbol{\Phi} = \operatorname{diag}\{\alpha_1, \alpha_2, \ldots, \alpha_M\} \\
& |\alpha_m| = 1, \quad \forall m \\
& \operatorname{tr}(\mathbf{Q}) \le P, \quad \mathbf{Q} \succeq 0.
\end{aligned} \tag{2}$$

Problem (P1) is a non-convex optimization problem, which is hard to solve in general. Thus, we solve Problem (P1) using alternating optimization methods. We first optimize $\mathbf{Q}$ for a fixed $\boldsymbol{\Phi}$. Then, we optimize $\boldsymbol{\Phi}$ for a fixed $\mathbf{Q}$. We repeat this alternating optimization until convergence. Algorithm 1 summarizes how to solve Problem (P1). More detailed descriptions are given in the subsequent subsections.

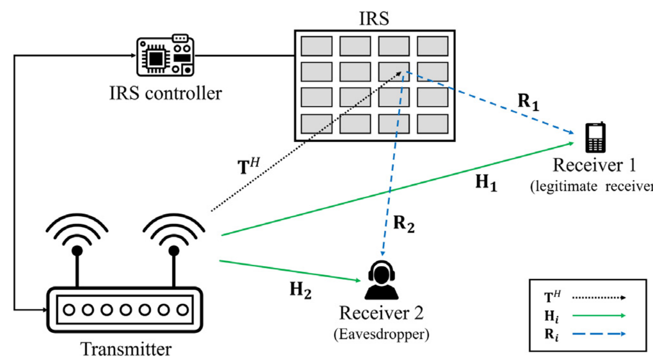


**Fig. 1.** System model for IRS-aided MIMO wiretap channels.

### 2.1. *Optimizing* $\mathbf{Q}$

If $\boldsymbol{\Phi}$ is given, then $\tilde{\mathbf{H}}$ is fixed. In this case, Problem (P1) reduces to the conventional MIMO secrecy rate maximization problem given in (1). In [11], the MIMO secrecy rate maximization problem was solved using the alternating optimization that converges to the KKT point of the problem. In [12], the original problem was reformulated as a minimax problem and its global optimal solution was found using the barrier method to deal with the minimax problem. We can apply either algorithm to optimize $\mathbf{Q}$ for given $\boldsymbol{\Phi}$. Line 5 in Algorithm 1 indicates optimizing $\mathbf{Q}$ for given $\boldsymbol{\Phi}$.

### 2.2. *Optimizing* $\boldsymbol{\Phi}$ *based on the coordinate descent methods*

In this subsection, we focus on how to optimize $\boldsymbol{\Phi}$ for given $\mathbf{Q}$. Since the objective function of Problem (P1) is not a concave function of $\boldsymbol{\Phi}$, the joint optimization is not easy. Thus, we apply the coordinate descent methods to optimize $\{\alpha_m\}_{m=1}^M$ for given $\mathbf{Q}$. More specifically, we express Problem (P1) into a series of optimization problems for given $\mathbf{Q}$ and $\{\alpha_j\}_{j=1, j\neq m}^M$ for $m = 1, 2, \ldots, M$. Then, we apply the coordinate descent method to each subproblem until convergence.

Now we derive a subproblem for the $m$th reflecting unit $\alpha_m$ while $\mathbf{Q}$ and $\{\alpha_j\}_{j=1, j\neq m}^M$ are fixed. We first express the effective MIMO channel as $\tilde{\mathbf{H}}_i = \tilde{\mathbf{H}}_{i,-m} + \alpha_m\mathbf{r}_{im}\mathbf{t}_m^H$, where $\tilde{\mathbf{H}}_{i,-m} = \mathbf{H}_i + \sum_{j=1, j\neq m}^M \alpha_j\mathbf{r}_{ij}\mathbf{t}_j^H$, $\mathbf{R}_i = [\mathbf{r}_{i1}\cdots\mathbf{r}_{iM}]$ and $\mathbf{T} = [\mathbf{t}_1\cdots\mathbf{t}_M]$. $\mathbf{C}_{im} \equiv \mathbf{r}_{im}\mathbf{t}_m^H$ can be considered as a cascaded channel (without taking the effect of IRS reflection yet) that can be estimated using pilot symbols [13]. Note that $\tilde{\mathbf{H}}_{i,-m}$ is independent of $\alpha_m$. For the $m$th subproblem, we fix $\tilde{\mathbf{H}}_{i,-m}$. Then, for $i = 1, 2$, we have

$$\begin{aligned}
&\log\left|\mathbf{I} + \tilde{\mathbf{H}}_i\mathbf{Q}\tilde{\mathbf{H}}_i^H\right| \\
&= \log\left|\mathbf{I} + (\tilde{\mathbf{H}}_{i,-m} + \alpha_m\mathbf{r}_{im}\mathbf{t}_m^H)\mathbf{Q}(\tilde{\mathbf{H}}_{i,-m} + \alpha_m\mathbf{r}_{im}\mathbf{t}_m^H)^H\right| \\
&= \log\left|\mathbf{A}_{im} + \alpha_m\mathbf{B}_{im} + \alpha_m^*\mathbf{B}_{im}^H\right| \\
&= \log\left|\mathbf{I} + \alpha_m\mathbf{A}_{im}^{-\frac{1}{2}}\mathbf{B}_{im}\mathbf{A}_{im}^{-\frac{1}{2}} + \alpha_m^*\mathbf{A}_{im}^{-\frac{1}{2}}\mathbf{B}_{im}^H\mathbf{A}_{im}^{-\frac{1}{2}}\right| \\
&\quad + \log|\mathbf{A}_{im}|,
\end{aligned} \tag{3}$$

where $\mathbf{A}_{im} = \mathbf{I} + \mathbf{r}_{im}\mathbf{t}_m^H\mathbf{Q}\mathbf{t}_m\mathbf{r}_{im}^H + \tilde{\mathbf{H}}_{i,-m}\mathbf{Q}\tilde{\mathbf{H}}_{i,-m}^H$ and $\mathbf{B}_{im} = \mathbf{r}_{im}\mathbf{t}_m^H\mathbf{Q}\tilde{\mathbf{H}}_{i,-m}^H$ for $m = 1, 2, \ldots, M$ and the last equality in (3)

**Algorithm 1** Secrecy Rate Maximization Algorithm for IRS-aided MIMO Wiretap Channels.

1: Input: $\{\mathbf{H}_i\}$, $\{\mathbf{R}_i\}$, $\mathbf{T}$, $P$
2: Initialize $\boldsymbol{\Phi}$
3: Repeat until convergence
4: $\quad\tilde{\mathbf{H}}_i = \mathbf{H}_i + \mathbf{R}_i \boldsymbol{\Phi} \mathbf{T}^H$, $i = 1, 2$
5: $\quad\mathbf{Q} = \arg\max_{\mathbf{Q}\succeq 0:\mathrm{tr}(\mathbf{Q})\leq P} C(\mathbf{Q}, \boldsymbol{\Phi})$
6: $\quad$Repeat until convergence
7: $\quad\quad$for $m = 1 : M$
8: $\quad\quad\quad$Compute $a_{im}$, $i = 1, 2$, in (6)
9: $\quad\quad\quad$Compute $\lambda$ in (8)
10: $\quad\quad\quad\alpha_m = (a_{1m} - \lambda a_{2m})/|a_{1m} - \lambda a_{2m}|$
11: $\quad\quad$end for
12: $\quad$end
13: $\quad\boldsymbol{\Phi} = \mathrm{diag}\{\alpha_1, \alpha_2, \cdots, \alpha_M\}$
14: end

follows from $|\mathbf{XY}| = |\mathbf{X}||\mathbf{Y}|$ and $\mathbf{X} = \mathbf{X}^{1/2}\mathbf{X}^{1/2}$ for $\mathbf{X} \succ 0$. Note that $\mathbf{A}_{im}$ and $\mathbf{B}_{im}$ are independent of $\alpha_m$. For fixed $\mathbf{Q}$ and $\{\alpha_1, \ldots, \alpha_{m-1}, \alpha_{m+1}, \ldots, \alpha_M\}$, the $m$th subproblem for optimizing $\alpha_m$ is given by

$$\begin{aligned} \text{(P1-m)} \quad \max_{\alpha_m\in\mathbb{C}} \; & \log|\mathbf{I} + \alpha_m \mathbf{p}_{1m}\mathbf{q}_{1m}^H + \alpha_m^* \mathbf{q}_{1m}\mathbf{p}_{1m}^H| \\ & - \log|\mathbf{I} + \alpha_m \mathbf{p}_{2m}\mathbf{q}_{2m}^H + \alpha_m^* \mathbf{q}_{2m}\mathbf{p}_{2m}^H| \\ \text{s.t.} \; & |\alpha_m| = 1, \end{aligned} \tag{4}$$

where $\mathbf{p}_{im} = \mathbf{A}_{im}^{-\frac{1}{2}}\mathbf{r}_{im}$ and $\mathbf{q}_{im} = \mathbf{A}_{im}^{-\frac{1}{2}}\tilde{\mathbf{H}}_{i,-m}\mathbf{Q}\mathbf{t}_m$. $\mathbf{p}_{im}$ and $\mathbf{q}_{im}$ are independent of $\alpha_m$ and satisfy $\mathbf{p}_{im}\mathbf{q}_{im}^H = \mathbf{A}_{im}^{-\frac{1}{2}}\mathbf{B}_{im}\mathbf{A}_{im}^{-\frac{1}{2}}$. We focus on the case of nonzero $\mathbf{p}_{im}$ and $\mathbf{q}_{im}$ because it is trivial when either of $\mathbf{p}_{im}$ or $\mathbf{q}_{im}$ is zero.

The $m$th subproblem can be expressed as its equivalent problem. Instead of directly solving Problem (P1-m), we solve its equivalent problem

$$\begin{aligned} \text{(P2-m)} \quad \max_{\alpha_m\in\mathbb{C}} \; & \frac{1 + \mathrm{Re}\{a_{1m}^* \alpha_m\}}{1 + \mathrm{Re}\{a_{2m}^* \alpha_m\}} \\ \text{s.t.} \; & |\alpha_m| = 1, \end{aligned} \tag{5}$$

where

$$a_{im} = 2(\mathbf{q}_{im}^H \mathbf{p}_{im})^* / (1 - (\|\mathbf{p}_{im}\|^2 \|\mathbf{q}_{im}\|^2 - |\mathbf{q}_{im}^H \mathbf{p}_{im}|^2)). \tag{6}$$

for $i = 1, 2$. The equivalence is derived in the following lemma.

**Lemma 1.** *Problem (P1-m) has the same optimal solution with Problem (P2-m). In addition, $a_{im}$ satisfies $|a_{im}| < 1$ for all $i$ and $m$.*

**Proof.** The proof is given in the Appendix. □

If $a_{1m} = a_{2m}$, then any $\alpha_m$ satisfying $|\alpha_m| = 1$ is the optimal solution. Thus, we may exclude the trivial case of $a_{1m} = a_{2m}$. In addition, the event of $a_{1m} = a_{2m}$ has Lebesgue-measure zero when the channel fading has a continuous cumulative distribution function (CDF). Therefore, we can focus on the case of $a_{1m} \neq a_{2m}$, because we have $a_{1m} \neq a_{2m}$ almost surely (i.e., with probability 1) when the channel fading has a continuous CDF.

**Lemma 2.** *For $a_{1m} \neq a_{2m}$ with $|a_{im}| < 1, i = 1, 2$, the optimal solution to Problem (P2-m) is given by*

$$\alpha_m = (a_{1m} - \lambda a_{2m})/|a_{1m} - \lambda a_{2m}| \tag{7}$$

*and the optimal value is $\lambda$, where $\lambda$ is given by*

$$\begin{aligned} \lambda = \frac{1}{1 - |a_{2m}|^2} \Big( & 1 - Re\{a_{1m}^* a_{2m}\} \\ & + \sqrt{(1 - Re\{a_{1m}^* a_{2m}\})^2 - (1 - |a_{1m}|^2)(1 - |a_{2m}|^2)} \Big). \end{aligned} \tag{8}$$

**Proof.** We define $f(\alpha) = (1 + \mathrm{Re}\{a_{1m}^*\alpha\})/(1 + \mathrm{Re}\{a_{2m}^*\alpha\})$ and $\mathcal{S} = \{\alpha \in \mathbb{C} |\, |\alpha| = 1\}$. Let $\bar{\alpha}$ be the optimal solution to Problem (P2-m) and $\lambda = \max_{\alpha\in\mathcal{S}} f(\alpha) = f(\bar{\alpha})$ be the optimal value. According to Lemma 1, we have $|a_{im}| < 1$ for $i = 1, 2$. Thus, we have $1 + \mathrm{Re}\{a_{2m}^*\alpha\} > 0$ for all $\alpha \in \mathcal{S}$. $f(\alpha) \leq \lambda$ for all $\alpha \in \mathcal{S}$ is equivalent to

$$1 - \lambda + \mathrm{Re}\{(a_{1m} - \lambda a_{2m})^*\alpha\} \leq 0, \;\; \forall \alpha \in \mathcal{S}, \tag{9}$$

where the equality holds if and only if $\alpha$ is the optimal solution to Problem (P2-m), i.e., $\alpha = \bar{\alpha}$.

Under the condition $|\alpha| = 1$, Cauchy–Schwartz inequality gives

$$\begin{aligned} 1 - \lambda + \mathrm{Re}\{(a_{1m} - \lambda a_{2m})^*\alpha\} &\leq 1 - \lambda + |a_{1m} - \lambda a_{2m}||\alpha| \\ &= 1 - \lambda + |a_{1m} - \lambda a_{2m}|, \end{aligned} \tag{10}$$

where the equality holds when $\alpha = \frac{a_{1m}-\lambda a_{2m}}{|a_{1m}-\lambda a_{2m}|}$. When $\lambda$ is the optimal value in (9), the upper-bound to $1 - \lambda + \mathrm{Re}\{(a_{1m} - \lambda a_{2m})^*\alpha\}$ is achieved when $\alpha = \bar{\alpha}$. Therefore, $\alpha = \frac{a_{1m}-\lambda a_{2m}}{|a_{1m}-\lambda a_{2m}|}$ is the solution to Problem (P2-m). In addition, since the upper-bound to $1-\lambda+\mathrm{Re}\{(a_{1m} - \lambda a_{2m})^*\alpha\}$ is equal to 0 due to (9), $\lambda$ satisfies $1-\lambda+|a_{1m} - \lambda a_{2m}| = 0$ in (10), i.e., $(1-|a_{2m}|^2)\lambda^2 - 2(1 - \mathrm{Re}\{a_{1m}^* a_{2m}\})\lambda + 1 - |a_{1m}|^2 = 0$ and its largest solution is equal to Eq. (8). Therefore, the lemma follows. □

In summary, combining Lemmas 1–2, we obtain the following optimal solution to Problem (P1-m).

**Theorem 1.** *If $a_{1m} = a_{2m}$, then all $\alpha_m$ satisfying $|\alpha_m| = 1$ is the solution to Problem (P1-m). Otherwise, the optimal solution to Problem (P1-m) is given by*

$$\alpha_m = (a_{1m} - \lambda a_{2m})/|a_{1m} - \lambda a_{2m}|, \tag{11}$$

*where $\lambda$ is given by (8).*

**Proof.** If $a_{1m} = a_{2m}$, the solution is trivially any $\alpha_m$ satisfying $|\alpha_m| = 1$. Otherwise, we apply Lemmas 1–2 to Problem (P1-m) and then the theorem follows. □

Algorithm 1 summarizes the secrecy rate maximization algorithm for IRS-aided MIMO wiretap channels. Line 5 indicates optimizing $\mathbf{Q}$ while $\boldsymbol{\Phi}$ is fixed. In Lines 6–13, the coordinate descent method optimizes $\boldsymbol{\Phi}$ while $\mathbf{Q}$ is fixed.

**Theorem 2** (*Convergence*)**.** *The coordinate descent methods of optimizing* $\mathbf{\Phi}$ *using Theorem 1 converges to a stationary point of Problem (P1).*

**Proof.** If function $f : \mathcal{X}_1 \times \cdots \times \mathcal{X}_M \to \mathbf{R}$ is strict quasiconvex with respect to $\mathbf{x}_m$ on $\mathcal{X}_m$, for each $m = 1, 2, \ldots, M-2$ and $\mathcal{X}_m \in R^{n_m}$ is closed, nonempty, and convex for all $m$, then the sequence $\{\mathbf{x}^{(k)}\}$ generated by $\mathbf{x}_m^{(k+1)} = \arg\min_{\mathbf{x}_m \in \mathcal{X}_m} f(\mathbf{x}_1^{(k+1)}, \ldots, \mathbf{x}_{m-1}^{(k+1)}, \mathbf{x}_m, \mathbf{x}_{m+1}^{(k)}, \ldots, \mathbf{x}_M^{(k)})$ with $\mathbf{x}^{(k+1)} = (\mathbf{x}_1^{(k+1)}, \ldots, \mathbf{x}_M^{(k+1)})$ has limit points and every limit point is a stationary point [14].

Instead of maximizing the objective function of Problem (P1), we equivalently minimize $-E_m(\mathbf{x}_1, \ldots, \mathbf{x}_{m-1}, \mathbf{x}_{m+1}, \ldots, \mathbf{x}_M) + \log \frac{1+\mathbf{a}_{2m}^T \mathbf{x}_m}{1+\mathbf{a}_{1m}^T \mathbf{x}_m}$, $\forall m$, where $E_m(\cdot)$ is independent of $\alpha_m$, $\mathbf{x}_m = [\mathrm{Re}\{\alpha_m\}, \mathrm{Im}\{\alpha_m\}]^T$ and $\mathbf{a}_{im} = [\mathrm{Re}\{a_{im}\}, \mathrm{Im}\{a_{im}\}]^T$. Note $\frac{1+\mathbf{a}_{2m}^T \mathbf{x}_m}{1+\mathbf{a}_{1m}^T \mathbf{x}_m}$ for all $m$ is strictly quasiconvex [15]. In addition, it is continuously differentiable and $\mathcal{X}_m$ is closed, nonempty, and convex. Therefore, the coordinate descent methods of optimizing $\mathbf{\Phi}$ using Theorem 1 converge to a stationary point of Problem (P1) for given $\mathbf{Q}$. □

### 2.3. Algorithm analysis

In this subsection, we analyze the proposed Algorithm 1 and compare with conventional algorithms.

#### 2.3.1. Generalization of IRS-aided MIMO systems

In case of $a_{1m} \neq 0$ and $a_{2m} = 0$ (or equivalently $\mathbf{p}_{2m} = \mathbf{q}_{2m} = 0$), Problem (P1-m) becomes the subproblem of maximizing the IRS-aided MIMO capacity [16]. Theorem 1 generalizes the solutions of the subproblems in IRS-aided MIMO channels to the solutions of subproblems in IRS-aided MIMO wiretap channels.

#### 2.3.2. Comparison with different formulation

One may obtain the optimal $\alpha_m$ in the similar form of (11) and find the optimal $\lambda$ using the Dinkelbach method [9]. OBO method [9] derives optimal $\alpha_m = e^{-j \arg(s_{1m} - \lambda s_{2m})}$, where $s_{im}$ is the only non-zero eigenvalue of $\mathbf{A}_{im}^{-1}\mathbf{B}_{im}$ and $\lambda$ is computed with the bisection search (BS) algorithm. Note that Theorem 1 computes $\lambda$ in a closed form using (8), while OBO [9] finds $\lambda$ using a time-consuming numerical algorithm based on the bisection search. Our closed-form derivation is much better than the numerical method because it is exact and can be computed with much lower complexity. To the best of our knowledge, Theorem 1 first provides the optimal reflection coefficients in a closed-form expression without resorting to any numerical optimization for IRS-aided MIMO secrecy rate maximization.

#### 2.3.3. Computational complexity

We compare the computational complexity per iteration of the alternating optimization algorithm. Optimizing $\mathbf{Q}$ with a fixed $\mathbf{\Phi}$ is the common part for all considered algorithms, where its complexity is $\mathcal{O}(N_t^3)$. In the remaining discussion, we focus on the complexity of optimizing $\mathbf{\Phi}$ of each algorithm. In Algorithm 1, the process of calculating $\alpha_m$, $\forall m$, requires $N_{r,i}^3 + N_{r,i}^2 N_t + N_{r,i} N_t^2 + 2N_{r,i} N_t + 3N_{r,i}^2 + 2N_t^2 + 2N_{r,i} + N_t$ multiplications. Thus, Algorithm 1 has complexity $\mathcal{O}(M(N_r^3 + N_r^2 N_t + N_r N_t^2))$, where $N_r = \max(N_{r,1}, N_{r,2})$. On the other hand, OBO [9] has complexity $\mathcal{O}(M(N_r^3 + N_r^2 N_t + N_r N_t^2 + \log_2 \frac{1}{\epsilon}))$, where $\epsilon$ denotes the required accuracy for the bisection search. If all receiver has one antenna (i.e., $N_{r,i} = 1$, $i = 1, 2$), SDR [4] can optimize $\mathbf{\Phi}$ with complexity of $\mathcal{O}(M^{3.5} + M^2 N_t + M N_t^2)$, while Algorithm 1 and OBO [9] has complexity $\mathcal{O}(M N_t^2)$ and $\mathcal{O}(M(N_t^2 + \log_2 \frac{1}{\epsilon}))$, respectively. Therefore, Algorithm 1 has the lowest computational complexity among considered algorithms. Detailed numerical comparisons will be given in the next section.

## 3. Numerical results

We performed numerical simulations to evaluate the performance of proposed algorithms in IRS-aided MIMO wiretap channels. The distance dependent path loss is $L(d) = \zeta(d/d_0)^{-\beta}$, where $\zeta = -30$ dB is the path loss at reference distance $d_0 = 1$ m, $d$ is the distance between two locations, and $\beta$ denotes the path loss exponent. For small-scale fading, we assume the Rician fading channel model $\mathbf{H} = \sqrt{\kappa/(1+\kappa)}\mathbf{H}^{\mathrm{LoS}} + \sqrt{1/(1+\kappa)}\mathbf{H}^{\mathrm{NLoS}}$, where $\kappa$ is the Rician factor, and $\mathbf{H}^{\mathrm{LoS}}$ and $\mathbf{H}^{\mathrm{NLoS}}$ denote the deterministic LoS and Rayleigh fading components, respectively. We model fading channels by the spatially correlated Rician fading model given in [17]. Unless mentioned otherwise, we set simulation parameters as shown in Table 1. We repeat the updates until the secrecy rate increment in an update is less than $10^{-4}$ bps/Hz and a maximum of 100 iterations. For performance benchmarks, we consider following schemes:

- **CD (Algorithm 1)**: It stands for Algorithm 1 that is the alternating optimization (AO) algorithm with the closed-form solution by optimizing $\mathbf{\Phi}$ based on the coordinate descent (CD) methods. This is our proposed algorithm.
- **OBO (Bisection)** [9]: It stands for the AO algorithm composed of the bisection search and one-by-one (OBO) optimization method in the IRS-aided MIMO wiretap channel. In fact, OBO is nothing but the CD, but we use 'OBO' to distinguish itself from our work.
- **SDR (Gaussian randomization)** [4]: It stands for the AO algorithm obtained by applying SDR and Gaussian randomization in the IRS-aided MISO wiretap channel.
- **Exhaustive method**: It stands for the ideal algorithm that try all possible values for all reflection coefficients to achieve the maximum secrecy rate.
- **Without IRS**: The system 'without IRS' implies that we do not use IRS and optimizes $\mathbf{Q}$ with $\mathbf{\Phi} = 0$.

Fig. 2 depicts the secrecy rate versus SNR performance. We set the bit resolution of $\alpha_m$ is 3 in all methods to make a fair comparison with the exhaustive method. The performance gap between the system with IRS and without IRS increases with the transmit power, which validates the advantages of IRS. SDR achieves nearly the same performance when SNR is low, but its performance degrades in the high SNR. The exhaustive

**Table 1**
The parameters for simulation.

| Parameters | Values |
|---|---|
| The coordinate of node | Tx(0, 0), IRS(10, 10), User(150, 0), Eve($d_{eve}$, 0) |
| The number of antenna | $N_t = 8$<br>$N_{r,1} = N_{r,2} = 1$ for MISO systems<br>$N_{r,1} = N_{r,2} = 4$ for MIMO systems |
| The path loss exponent | $\beta_{TI} = \beta_{IU} = \beta_{IE} = 3$<br>$\beta_{TU} = \beta_{EU} = 1.5$ |
| The Rician factor | $\kappa = 1$ |
| The noise power | −80 dBm |

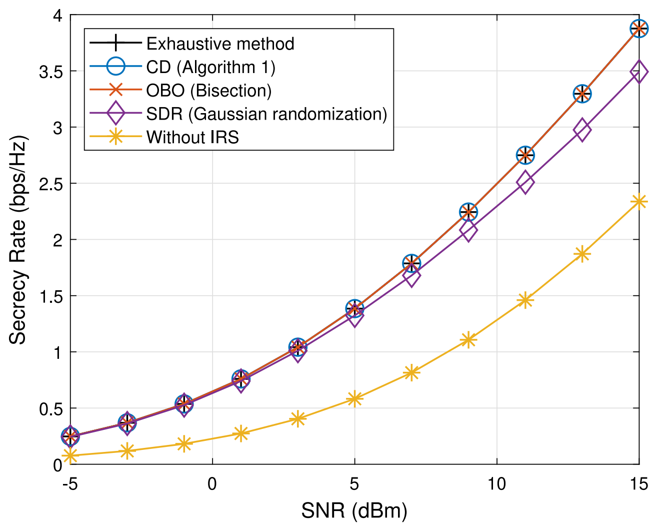


**Fig. 2.** Secrecy rate versus SNR in the IRS-aided MISO wiretap channel ($M = 8$, $d_{eve} = 140$).

method provides the highest secrecy rate and thus it plays the role of the upper bound to the all possible algorithms. CD and OBO achieve nearly the same secrecy rate with the exhaustive method. This numerically validates the optimality of OBO and the proposed algorithm.

Fig. 3 depicts the transmitted rate with respect to the horizontal distance $d_{eve}$ between the transmitter and the eavesdropper in the IRS-aided MISO wiretap channel. We have observed the following: (1) The system without IRS is irrelevant to the eavesdropper's location and has the lowest performance. (2) CD and OBO have only 10% performance degradation when the eavesdropper is close to IRS. Therefore, IRS helps to increase the secrecy rate significantly. In addition, CD and OBO can achieve a high security rate regardless of the location of the eavesdropper.

Fig. 4 shows the secrecy rates versus the number of IRS's reflecting units, $M$. The solid and dashed lines are the secrecy rate in the MIMO system and the MISO system, respectively. We observed that increasing $M$ leads to the significant improvement of secrecy rates. The performance of the SDR is the same as the CD when $M$ is low, however there is performance degradation when $M$ is high because SDR produces a suboptimal solution. In a MIMO channels, as the number of

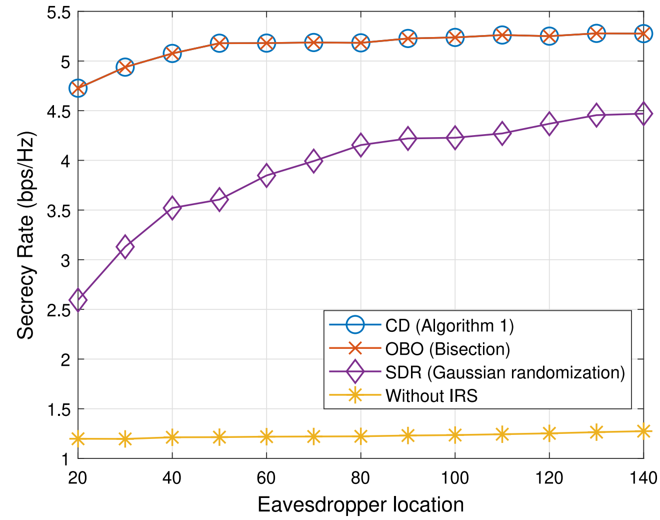


**Fig. 3.** Secrecy rate with respect to the location of eavesdropper $d_{eve}$ ($M = 32$, $P = 10$ dBm).

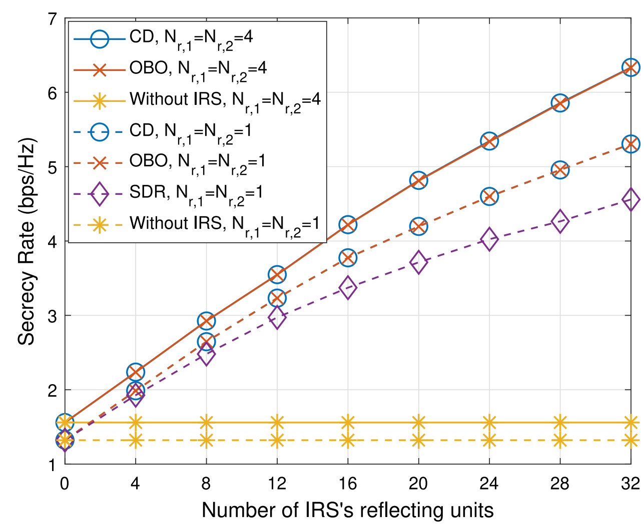


**Fig. 4.** Secrecy rate versus the number of IRS's reflecting units $M$ ($P = 10$ dBm, $d_{eve} = 140$).

**Table 2**
Comparison of average running times.

| Algorithms | $M = 8$ | $M = 32$ |
|---|---|---|
| Exhaustive method | 23 min | Out of memory |
| SDR (Gaussian randomization) | 1.123 s | 2.794 s |
| OBO (Bisection) | 0.057 s | 0.725 s |
| CD (Algorithm 1) | 0.039 s | 0.147 s |
| Without IRS | 0.288 μs | 0.288 μs |

the legitimate user's antennas increases, the sufficient spatial degree of freedom for transmission also increases. Therefore, the MIMO channel with $N_{r,1} = N_{r,2} = 4$ achieves a higher secrecy rates than the MISO channel. We also observe that CD and OBO achieve the same secrecy rate in MIMO/MISO wiretap channels.

Table 2 shows the average running time of different schemes in the IRS-aided MISO wiretap channel. For a fair comparison, we used the same PC with Intel i9 CPU and 32 GB RAM. The average running time is the overall time that algorithms take to optimize $\mathbf{Q}$ and $\mathbf{\Phi}$. The system without IRS is the fastest because optimizing $\mathbf{Q}$ is only performed. If $M$ is large, exhaustive method does not operate due to insufficient memory. According to Remark 3, CD has lower computational complexity than OBO. When $M$ is 8, CD is about 1.5 times faster than OBO. In addition, as $M$ increases, the gap of running time increases. This is because OBO requires computation of bisection search and eigenvalue decomposition in the optimizing $\mathbf{\Phi}$, unlike CD. When $M$ is 32, CD is 5 times and 20 times faster than OBO and SDR, respectively.

## 4. Conclusion

In this paper, we presented closed-form expressions for the optimal IRS coefficient in the IRS-aided MIMO wiretap channel. We transformed the IRS coefficient optimization problem into an equivalent linear-fractional optimization under amplitude constraints, which admits the closed-form optimal solution. In the literature, many IRS optimization problems usually have been numerically solved approximately using semidefinite relaxation or majorization minimization. We first provided the closed-form expression for optimal reflection coefficient without resorting to any numerical optimization for IRS-aided MIMO secrecy rate maximization. Thus, our derived solution is much better in the sense that it is exact and can be computed with much lower complexity and with more numerical stability.

## CRediT authorship contribution statement

**Minsik Kim:** Methodology, Software, Writing. **Daeyoung Park:** Conceptualization, Methodology, Writing, Supervision.

## Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## Acknowledgment

This work was supported by Inha University Research Grant.

## Appendix

We prove Lemma 1 using the Cauchy–Schwartz inequality for $a, x \in \mathbb{C}$, i.e, $-|a||x| \le \mathrm{Re}\{a^* x\} \le |a||x|$, where the first and second equalities hold when $x = -ca$ and $x = ca$ for some $c > 0$, respectively. We define $c_{im} = \|\mathbf{p}_{im}\|\|\mathbf{q}_{im}\|$, $\delta_{im} = \mathbf{q}_{im}^H \mathbf{p}_{im}/c_{im}$, $\bar{\mathbf{p}}_{im} = \frac{1}{\|\mathbf{p}_{im}\|}\mathbf{p}_{im}$, $\bar{\mathbf{q}}_{im} = \frac{1}{\|\mathbf{q}_{im}\|}\mathbf{q}_{im}$ for $i = 1, 2$. Then we have $\delta_{im} = \bar{\mathbf{q}}_{im}^H \bar{\mathbf{p}}_{im}$ and $\mathbf{p}_{im}\mathbf{q}_{im}^H = c_{im}\bar{\mathbf{p}}_{im}\bar{\mathbf{q}}_{im}^H$ and $\alpha_m \mathbf{p}_{im}\mathbf{q}_{im}^H + \alpha_m^* \mathbf{q}_{im}\mathbf{p}_{im}^H = \mathbf{U}_{im}\mathbf{\Lambda}_{im}\mathbf{U}_{im}^H$, where $\mathbf{U}_{im} = [\bar{\mathbf{p}}_{im}, \bar{\mathbf{q}}_{im}]$ and $\mathbf{\Lambda}_{im} = \begin{bmatrix} 0 & c_{im}\alpha_m \\ c_{im}\alpha_m^* & 0 \end{bmatrix}$. Thus, we have

$$
\begin{aligned}
&|\mathbf{I} + \alpha_m \mathbf{p}_{im}\mathbf{q}_{im}^H + \alpha_m^* \mathbf{q}_{im}\mathbf{p}_{im}^H| \\
&= |\mathbf{I} + \mathbf{U}_{im}\mathbf{\Lambda}_{im}\mathbf{U}_{im}^H| = |\mathbf{I} + \mathbf{U}_{im}^H\mathbf{U}_{im}\mathbf{\Lambda}_{im}| \\
&= \left|\mathbf{I} + \begin{bmatrix} 1 & \delta_{im}^* \\ \delta_{im} & 1 \end{bmatrix}\mathbf{\Lambda}_{im}\right| \\
&= \left|\begin{bmatrix} 1 + c_{im}\delta_{im}^*\alpha_m^* & c_{im}\alpha_m \\ c_{im}\alpha_m^* & 1 + c_{im}\delta_{im}\alpha_m \end{bmatrix}\right| \\
&= |1 + c_{im}\delta_{im}\alpha_m|^2 - c_{im}^2 \\
&= 1 - (1 - |\delta_{im}|^2)c_{im}^2 + 2c_{im}\mathrm{Re}\{\delta_{im}\alpha_m\}.
\end{aligned} \tag{12}
$$

Since the covariance matrix $\mathbf{I} + \tilde{\mathbf{H}}_i\mathbf{Q}\tilde{\mathbf{H}}_i^H$ is positive definite for any $\{\alpha_m\}$, the determinants in (3) are strictly positive. This implies that all $\alpha_m \in \mathcal{S} = \{\alpha \in \mathbb{C} \parallel \alpha| = 1\}$ are feasible for Problem (P1-m) in the sense that the determinants in Problem (P1-m) are positive for all $\alpha_m \in \mathcal{S}$. Therefore, $1 - (1 - |\delta_{im}|^2)c_{im}^2 + 2c_{im}\mathrm{Re}\{\delta_{im}\alpha_m\} > 0$ for all $\alpha_m \in \mathcal{S}$. In addition, Cauchy–Schwartz inequality satisfies $2c_{im}\mathrm{Re}\{\delta_{im}\alpha_m\} \ge -2c_{im}|\delta_{im}|$. Thus, we have $\min_{\alpha_m \in \mathcal{S}} 1 - (1 - |\delta_{im}|^2)c_{im}^2 + 2c_{im}\mathrm{Re}\{\delta_{im}\alpha_m\} = 1 - (1 - |\delta_{im}|^2)c_{im}^2 - 2c_{im}|\delta_{im}| > 0$. This implies $1 - (1 - |\delta_{im}|^2)c_{im}^2 > 2c_{im}|\delta_{im}| \ge 0$.

The objective function of Problem (P1-m) is

$$
\begin{aligned}
&\log|\mathbf{I} + \alpha_m \mathbf{p}_{1m}\mathbf{q}_{1m}^H + \alpha_m^* \mathbf{q}_{1m}\mathbf{p}_{1m}^H| \\
&\quad - \log|\mathbf{I} + \alpha_m \mathbf{p}_{2m}\mathbf{q}_{2m}^H + \alpha_m^* \mathbf{q}_{2m}\mathbf{p}_{2m}^H| \\
&= \log(1 - (1 - |\delta_{1m}|^2)c_{1m}^2 + 2c_{1m}\mathrm{Re}\{\delta_{1m}\alpha_m\}) \\
&\quad - \log(1 - (1 - |\delta_{2m}|^2)c_{2m}^2 + 2c_{2m}\mathrm{Re}\{\delta_{2m}\alpha_m\}) \\
&= h_m + \log\frac{1 + \mathrm{Re}\{a_{1m}^*\alpha_m\}}{1 + \mathrm{Re}\{a_{2m}^*\alpha_m\}},
\end{aligned} \tag{13}
$$

where $h_m = \log(1 - (1 - |\delta_{1m}|^2)c_{1m}^2) - \log(1 - (1 - |\delta_{2m}|^2)c_{2m}^2)$, $a_{im} = 2c_{im}\delta_{im}^*/(1 - (1 - |\delta_{im}|^2)c_{im}^2)$, $i = 1, 2$. As mentioned above, we have $1 - (1 - |\delta_{im}|^2)c_{im}^2 > 0$ and $1 - (1 - |\delta_{im}|^2)c_{im}^2 + 2c_{im}\mathrm{Re}\{\delta_{im}\alpha_m\} > 0$ for all $\alpha_m \in \mathcal{S}$. Therefore, Problem (P1-m) has the same solution with Problem (P2-m). In addition, since $1 + \mathrm{Re}\{a_{im}^*\alpha_m\} > 0$ for all $\alpha_m \in \mathcal{S}$, we have $\min_{\alpha_m \in \mathcal{S}} 1 + \mathrm{Re}\{a_{im}^*\alpha_m\} = 1 - |a_{im}| > 0$ due to Cauchy–Schwartz inequality. This implies $|a_{im}| < 1$ for $i$ and $m$.

## References

[1] Q. Wu, R. Zhang, Towards smart and reconfigurable environment: intelligent reflecting surface aided wireless network, IEEE Commun. Mag. 58 (2020) 106–112.

[2] Q. Wu, R. Zhang, Beamforming optimization for intelligent reflecting surface with discrete phase shifts, in: Proc. IEEE ICASSP, 2019, pp. 7830–7833.

[3] A.-T. Le, N.-D.-X. Ha, D.-T. Do, A. Silva, S. Yadav, Enabling user grouping and fixed power allocation scheme for reconfigurable intelligent surfaces-aided wireless systems, IEEE Access 9 (2021) 92263–92275.

[4] M. Cui, G. Zhang, R. Zhang, Secure wireless communication via intelligent reflecting surface, IEEE Wirel. Commun. Lett. 8 (2019) 1410–1414.

[5] Y. Song, M.R.A. Khandaker, F. Tariq, K.-K. Wong, Truly intelligent reflecting surface-aided secure communication using deep learning, arXiv:2004.03056.

[6] X. Yu, D. Xu, R. Schober, Enabling secure wireless communications via intelligent reflecting surfaces, in: Proc. of IEEE Globecom 2019.

[7] B. Feng, Y. Wu, M. Zheng, Secure transmission strategy for intelligent reflecting surface enhanced wireless system, in: Proc. of Int. Conf. Wireless Commun. Sig. Proc. (WCSP) 2019.

[8] H. Shen, W. Xu, S. Gong, Z. He, C. Zhao, Secrecy rate maximization for intelligent reflecting surface assisted multi-antenna communications, IEEE Commun. Lett. 23 (2019) 1488–1492.

[9] L. Dong, H.-M. Wang, Enhancing secure MIMO transmission via intelligent reflecting surface, IEEE Trans. Wirel. Commun. 19 (2020) 7543–7556.

[10] A. Khisti, G.W. Wornell, Secure transmission with multiple antennas–Part II: The MIMOME wiretap channel, IEEE Trans. Inf. Theory 56 (2010) 5515–5532.

[11] Q. Li, M. Hong, H.-T. Wai, Y.-F. Liu, W.-K. Ma, Z.-Q. Luo, Transmit solutions for MIMO wiretap channels using alternating optimization, IEEE J. Sel. Areas Commun. 31 (2013) 1714–1727.

[12] S. Loyka, C.D. Charalambous, An algorithm for global maximization of secrecy rates in Gaussian MIMO wiretap channels, IEEE Trans. Commun. 63 (2015) 2288–2299.

[13] B. Zheng, C. You, R. Zhang, Efficient channel estimation for double-IRS aided multi-user MIMO system, arXiv:2011.00738.

[14] L. Grippo, M. Sciandrone, On the convergence of the block linear Gauss-Seidel method under convex constraint, Oper. Res. Lett. 26 (2000) 127–136.

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

[16] S. Zhang, R. Zhang, Capacity characterization for intelligent reflecting surface aided MIMO communications, IEEE J. Sel. Areas Commun. 38 (2020) 1823–1838.

[17] E. Björnson, L. Sanguinetti, Rayleigh fading modeling and channel hardening for reconfigurable intelligent surfaces, IEEE Wirel. Commun. Lett. 10 (2021) 830–834.