H2020-MSCA-IF-2020

Secure Indoor Communication empowered by Intelligent reflecting Surface (SICIS)

D3.1

Report on evaluating the overall secrecy performance by using IRS-based microwave QR code

Authors(s)	Sai Xu, Jie Zhang
Author(s) Affiliation	University of Sheffield, UK
Editor(s):	Sai Xu
Status-Version:	V1.0
Project Number:	101032170
Project Title:	Secure Indoor Communication empowered by Intelligent reflecting Surface
Project Acronym:	SICIS
Work Package Number	3

Abstract

This report presents communication security of intelligent reflecting surface (IRS)-based microwave quick response (QR) code. Specifically, the confidential information at a low- cost low-power Internet-of-Things device (Alice) is encoded as a microwave QR code on its associated IRS. To acquire the microwave QR code, a radio frequency signal is transmitted by an authorized user (Bob) and then received by itself through the reflection at the IRS. Meanwhile, a passive eavesdropper (Eve) attempts to intercept the reflected signal from the IRS and decode the carried confidential information. To enhance security, the transmitted signal and the receiving beamforming at Bob are jointly designed while the receiving beamforming vector at Eve is also optimized to capture the worse case of eavesdropping. Based on this, the average bit error probabilities at Bob and Eve are derived for phase shift keying (PSK). The simulation results demonstrate the secrecy performance of the considered system.

The results presented in this deliverable have addressed the requirement of Task 3.1 in the SICIS project.

Keywords: Microwave quick response code, radio frequency two-dimensional code, intelligent reflecting surface, backscatter, physical layer security.

Table of Contents

1. INTRODUCTION

Security is one of the most important issues for Internet- of-Things (IoT) networks [1]. Traditionally, wireless communications are protected by adopting cryptography methods that are embedded in the upper layers of networks. However, cryptographic technologies often require a high complexity, which may be unaffordable for many low-cost IoT devices [2]. As an alternative, physical-layer security (PLS) technologies have also been investigated to realize confidential communication [3], [4]. The fundamental of PLS is to enlarge the gap of signal-to-noise ratio (SNR) or signal-to-interference-plus-noise ratio (SINR) between the authorized user and the unauthorized user, by exploiting the difference of their physical channels and designing beamforming, interference and artificial noise [2]. Owing to a lower complexity than the cryptographic technologies, PLS has tremendous potential to secure communication of low-cost IoT devices.

With the aid of PLS technologies, the security of backscatter communication (BackCom) [5] that is frequently used at low- power IoT devices can be improved. BackCom is a passive communication technology, through which a device can send its own information by modulating and reflecting the incoming signal from an external radio frequency (RF) source [6]. In recent years, intelligent reflecting surface (IRS) has been developed to act as a backscatter device [7]. For example, in [7], [8], [9], modulation schemes at an IRS were studied, such as phase shift keying (PSK), quadrature amplitude modulation (QAM) and star-QAM. In [10], [11], IRS-BackCom was applied to cognitive radio and computational data offloading, respectively. In the aspect of PLS, some initial investigations on IRS-BackCom have also started [12],[13],[14].

As a new derivative of IRS-BackCom, microwave quick response (QR) code or RF two-dimensional code (RF2C) has been recently proposed to realize passive communication for low-cost low-power IoT devices in [15]. The key idea of microwave QR code is to map the information to an adjustable or unadjustable information metasurface [16], [17] in the form of QR code. Once electromagnetic (EM) waves illuminate the metasurface, the information of QR code will be modulated to the incoming signal. With the signal reflection, the information is disseminated. Considering that IRS is a well-developed metasurface, it is an excellent choice to integrate it with microwave QR code. Up to now, the security of IRS-based microwave QR code as a newly-proposed communication paradigm has not been investigated.

This report will focus on communication security of IRS-based microwave QR code. Our major contributions are outlined as follows. 1) A secure transmission system model of IRS-based microwave QR code is established and an optimization problem of dissemination security of the microwave QR code is formulated. 2) The transmitted signal and the receiving beamforming at the authorized and unauthorized users are jointly designed. Based on this, their average bit error probabilities (ABEPs) are given. 3) Simulations are conducted to show the secrecy performance of the considered system.

2. SYSTEM MODEL

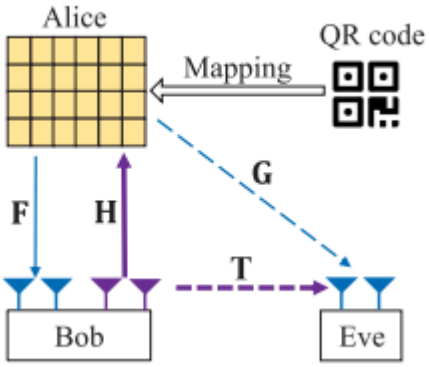

Fig. 1. An illustration of secure transmission of IRS-based microwave QR code.

Fig. 1 depicts a secure transmission system of IRS-based microwave QR code, consisting of an L-element IRS acting as an information source (Alice), an authorized user (Bob) equipped with Nt transmitting antennas and Nr receiving antennas, and a passive eavesdropper (Eve) equipped with N receiving antennas. In this system, the confidential information is mapped to the complex reflection coefficient of IRS elements, aiming to form a microwave QR code. To acquire the microwave QR code, Bob emits an RF signal towards the IRS. With the reflection at the IRS, the information of microwave QR code is modulated onto the RF signal, which can be received by Bob and overheard by Eve. Assume that the channels of Bob-Alice, Alice-Bob, Bob, Eve, and Alice-Eve link undergo quasi-static flat fading, and that the channel state information (CSI) for designing the transmitted signal at Bob is fully available. 1 Another assumption is that self-interference at Bob can be perfectly eliminated. When Bob radiates EM wave towards the IRS in a time slot, the signals received by Bob and Eve are respectively given by

$$\mathbf{y}_{\mathrm{b}} = \mathbf{F}\Theta\mathbf{H}\mathbf{x} + \mathbf{n}_{\mathrm{b}}, \quad \mathbf{y}_{\mathrm{e}} = \mathbf{G}\Theta\mathbf{H}\mathbf{x} + \mathbf{T}\mathbf{x} + \mathbf{n}_{\mathrm{e}}.$$

Where $\mathbf{x}$ denotes the transmitted signal by Bob. $\boldsymbol{\Theta}$ is the reflection coefficient matri $\mathbf{x}$ at the IRS. $\mathbf{n}_{\mathrm{b}}$ and $\mathbf{n}_{\mathrm{e}}$ are white Gaussian random vectors at Bob and Eve, with $\mathbf{n}_{\mathrm{b}} \sim (\mathbf{0}, \sigma_{\mathrm{b}}^2\mathbf{I})$ and $\mathbf{n}_{\mathrm{e}} \sim (\mathbf{0}, \sigma_{\mathrm{e}}^2\mathbf{I})$,respectively. Letting $\boldsymbol{\theta}$ denote the reflection coefficient vector at the IRS with $\boldsymbol{\Theta} = \mathrm{diag}\{\boldsymbol{\theta}\}$, the signals received by Bob and Eve are further expressed as

$$\mathbf{y}_{\mathrm{b}} = \mathbf{F}\mathrm{diag}\{\mathbf{H}\mathbf{x}\}\boldsymbol{\theta} + \mathbf{n}_{\mathrm{b}},$$
$$\mathbf{y}_{\mathrm{e}} = \mathbf{G}\mathrm{diag}\{\mathbf{H}\mathbf{x}\}\boldsymbol{\theta} + \mathbf{T}\mathbf{x} + \mathbf{n}_{\mathrm{e}}.$$

In the considered system, θ represents the information vector bearing confidential data instead of a passive beamformer. Adopting the normalized receiving beamforming wb and we, the outputs at Bob and Eve are respectively given by

$$r_{\mathrm{b}} = \mathbf{w}_{\mathrm{b}}^H\mathbf{F}\mathrm{diag}\{\mathbf{H}\mathbf{x}\}\boldsymbol{\theta} + \mathbf{w}_{\mathrm{b}}^H\mathbf{n}_{\mathrm{b}},$$
$$r_{\mathrm{e}} = \mathbf{w}_{\mathrm{e}}^H\mathbf{G}\mathrm{diag}\{\mathbf{H}\mathbf{x}\}\boldsymbol{\theta} + \mathbf{w}_{\mathrm{e}}^H\mathbf{T}\mathbf{x} + \mathbf{w}_{\mathrm{e}}^H\mathbf{n}_{\mathrm{e}}.$$

Accordingly, the SNR at Bob and the SINR at Eve are respectively given by

$$\gamma_{\mathrm{b}} = \frac{|\mathbf{w}_{\mathrm{b}}^H\mathbf{F}\mathrm{diag}\{\mathbf{H}\mathbf{x}\}|^2}{\sigma_{\mathrm{b}}^2|\mathbf{w}_{\mathrm{b}}|^2}, \quad \gamma_{\mathrm{e}} = \frac{|\mathbf{w}_{\mathrm{e}}^H\mathbf{G}\mathrm{diag}\{\mathbf{H}\mathbf{x}\}|^2}{|\mathbf{w}_{\mathrm{e}}^H\mathbf{T}\mathbf{x}|^2 + \sigma_{\mathrm{e}}^2|\mathbf{w}_{\mathrm{e}}|^2},$$

To improve the dissemination security of the microwave QR code at Alice, the SINR at Eve is minimized under the constraints of the transmit power at Bob and the allowable minimum SNR at Bob by optimizing the transmitted signal design and the receiving beamforming vector at Bob, which is formulated as

$$\begin{aligned} (\text{P0}) \quad & \min_{\mathbf{x},\mathbf{w}_\text{b}} \quad \gamma_\text{e}, \\ s.t. \quad & \text{C1}: \gamma_\text{b} \geq \Gamma_\text{b}, \\ & \text{C2}: \text{Tr}\left(\mathbf{x}\mathbf{x}^H\right) \leq P, \\ & \text{C3}: \text{Tr}\left(\mathbf{w}_\text{b}\mathbf{w}_\text{b}^H\right) = 1, \end{aligned}$$

where P denotes the transmit power budget at Bob and Γ_b is the threshold value of γ_b

3. MINIMIZATION OF SINR AT EVE

Due to coupling of the optimization variables $\mathbf{x}$ and $\mathbf{w}_\text{b}$, the non-convex optimization problem (P0) is challenging to $\mathbf{w}_\text{e}$ Eve is assumed to be also a system user that has no permission to access the microwave QR code for Bob. For example, Bob and Eve are both users in a time-division system, where Eve attempts to passively intercept and decode the microwave QR code in Bob's time slot. In this case, the CSI of Eve can be acquired. Additionally, the considered system is still secure even though the CSI of Eve is unknown, which can be verified by Section V solve directly. Furthermore, we is contained in the objective function. To handle the optimization problem (P0), we need to be estimated firstly. Based on this, a method of alternative optimization can be employed to minimize γ_e. After the optimization problem (P0) is solved, the computational complexity analysis is presented.

In the considered system, Bob and Eve do not exchange $\mathbf{x}$, $\mathbf{w}_\text{b}$s and $\mathbf{w}_\text{e}$ with each other. As a passive eavesdropper, the optimal strategy of designing $\mathbf{w}_\text{e}$ for Eve is to maximize γ_e under the assumption that the adopted $\mathbf{x}$ and $\mathbf{w}_\text{b}$ can maximize γb without security protection. Mathematically, we can be estimated by Bob through the following optimization problem.

$$\begin{aligned} (\text{P1}) \quad & \max_{\mathbf{w}_\text{e}} \quad \gamma_\text{e}, \\ s.t. \quad & \text{C4}: \text{Tr}\left(\mathbf{w}_\text{e}\mathbf{w}_\text{e}^H\right) = 1. \end{aligned}$$

The optimization problem (P1) can be solved by semi-definite relaxation (SDR), followed by the recovery of the rank-one solution. Specifically, define $\mathbf{W}_\text{e} = \mathbf{w}_\text{e}\mathbf{w}_\text{e}^H$ with We $\mathbf{W}_\text{e} \pm \mathbf{0}$ and $\text{rank}\left(\mathbf{W}_\text{e}\right) = 1$ The optimization problem (P1) is equivalently formulated as

$$\begin{aligned} (\text{P2}) \quad & \max_{\mathbf{W}_\text{e}} \quad \frac{\text{Tr}\left(\mathbf{W}_\text{e}\mathbf{G}\text{diag}\{\mathbf{H}\mathbf{x}\}(\text{diag}\{\mathbf{H}\mathbf{x}\})^H\mathbf{G}^H\right)}{\text{Tr}\left(\mathbf{W}_\text{e}\mathbf{T}\mathbf{x}\mathbf{x}^H\mathbf{T}^H\right)+\sigma_\text{e}^2}, \\ s.t. \quad & \text{C5}: \text{Tr}\left(\mathbf{W}_\text{e}\right) = 1, \\ & \text{C6}: \mathbf{W}_\text{e} \pm \mathbf{0}, \\ & \text{C7}: \text{rank}\left(\mathbf{W}_\text{e}\right) = 1. \end{aligned}$$

Letting $\mathbf{S} = \mathbf{W}_\text{e} / \zeta$ with $\zeta > 0$ the optimization problem (P2) is rewritten as

$$\begin{aligned}
(\text{P3}) \quad \max_{\mathbf{S},\zeta} \quad & \mathrm{Tr}\left(\mathbf{SG}\mathrm{diag}\{\mathbf{Hx}\}(\mathrm{diag}\{\mathbf{Hx}\})^H\mathbf{G}^H\right), \\
s.t. \quad & \mathrm{C8}: \mathrm{Tr}\left(\mathbf{STxx}^H\mathbf{T}^H\right)+\zeta\sigma_{\mathrm{e}}^2 \le 1, \\
& \mathrm{C9}: \mathrm{Tr}\left(\mathbf{S}\right)=\zeta, \\
& \mathrm{C10}: \mathbf{S} \succeq \mathbf{0}, \zeta \ge 0 \\
& \mathrm{C11}: \mathrm{rank}\left(\mathbf{S}\right)=1.
\end{aligned}$$

Dropping the rank-one constraint C11, the optimization problem (P3) is relaxed as

$$\begin{aligned}
(\text{P4}) \quad \max_{\mathbf{S},\zeta} \quad & \mathrm{Tr}\left(\mathbf{SG}\mathrm{diag}\{\mathbf{Hx}\}(\mathrm{diag}\{\mathbf{Hx}\})^H\mathbf{G}^H\right), \\
s.t. \quad & \mathrm{C8}-\mathrm{C10}.
\end{aligned}$$

The optimization problem (P4) is convex and easily addressed by existing CVX tools. Once the optimal solution $\mathbf{S}^*$ to the optimization problem (P4) is obtained, its maximum eigenvector is used to compute the sub-optimal solution $\mathbf{w}_{\mathrm{e}}^*$ to the optimization problem (P1).

In the optimization problem (P0), $\mathbf{w}_{\mathrm{e}}^*$ is selected as the estimation of the receiving beamforming vector at Eve. Then, the variables $\mathbf{x}$ and $\mathbf{w}_{\mathrm{b}}$ are alternatively optimized, which is divided into two steps.

Step-1 (Optimizing $\mathbf{x}$): Given $\mathbf{w}_{\mathrm{b}}$, the optimization problem (P0) is simplified as

$$\begin{aligned}
(\text{P5}) \quad \min_{\mathbf{x}} \quad & \gamma_{\mathrm{e}}, \\
s.t. \quad & \mathrm{C1}, \mathrm{C2}.
\end{aligned}$$

The optimization problem (P5) can be solved by SDR, followed by the recovery of the rank-one solution. Specifically, define $\mathbf{X}=\mathbf{xx}^H$ with $\mathbf{X} \succeq \mathbf{0}$ and rank $\mathrm{rank}\left(\mathbf{X}\right)=1$ The optimization problem (P5) is equivalently formulated as

$$\begin{aligned}
(\text{P6}) \quad \min_{\mathbf{X}} \quad & \frac{\mathrm{Tr}\left(\mathbf{X}^T\mathbf{H}^H\mathrm{diag}\{\mathbf{w}_{\mathrm{e}}^H\mathbf{G}\}(\mathrm{diag}\{\mathbf{w}_{\mathrm{e}}^H\mathbf{G}\})^H\mathbf{H}\right)}{\mathrm{Tr}\left(\mathbf{XT}^H\mathbf{w}_{\mathrm{e}}\mathbf{w}_{\mathrm{e}}^H\mathbf{T}\right)+\sigma_{\mathrm{e}}^2}, \\
s.t. \quad & \mathrm{C12}: \mathrm{Tr}\left(\mathbf{X}^T\mathbf{H}^H\mathrm{diag}\{\mathbf{w}_{\mathrm{b}}^H\mathbf{F}\}(\mathrm{diag}\{\mathbf{w}_{\mathrm{b}}^H\mathbf{F}\})^H\mathbf{H}\right) \\
& \qquad \ge \sigma_{\mathrm{b}}^2\Gamma_{\mathrm{b}}, \\
& \mathrm{C13}: \mathrm{Tr}\left(\mathbf{X}\right) \le P, \\
& \mathrm{C14}: \mathbf{X} \succeq \mathbf{0}, \\
& \mathrm{C15}: \mathrm{rank}\left(\mathbf{X}\right)=1.
\end{aligned}$$

Letting $\mathbf{Q}=\mathbf{X}/\xi$ with $\xi>0$ the optimization problem (P6) is rewritten as

$$\begin{aligned}
(\text{P7}) \quad \min_{\mathbf{Q},\xi} \quad & \mathrm{Tr}\left(\mathbf{Q}^T\mathbf{H}^H\mathrm{diag}\{\mathbf{w}_{\mathrm{e}}^H\mathbf{G}\}(\mathrm{diag}\{\mathbf{w}_{\mathrm{e}}^H\mathbf{G}\})^H\mathbf{H}\right), \\
s.t. \quad & \mathrm{C16}: \mathrm{Tr}\left(\mathbf{QT}^H\mathbf{w}_{\mathrm{e}}\mathbf{w}_{\mathrm{e}}^H\mathbf{T}\right)+\xi\sigma_{\mathrm{e}}^2 \ge 1 \\
& \mathrm{C17}: \mathrm{Tr}\left(\mathbf{Q}^T\mathbf{H}^H\mathrm{diag}\{\mathbf{w}_{\mathrm{b}}^H\mathbf{F}\}(\mathrm{diag}\{\mathbf{w}_{\mathrm{b}}^H\mathbf{F}\})^H\mathbf{H}\right) \\
& \qquad \ge \xi\sigma_{\mathrm{b}}^2\Gamma_{\mathrm{b}}, \\
& \mathrm{C18}: \mathrm{Tr}\left(\mathbf{Q}\right) \le \xi P, \\
& \mathrm{C19}: \mathbf{Q} \succeq \mathbf{0}, \xi \ge 0, \\
& \mathrm{C20}: \mathrm{rank}\left(\mathbf{Q}\right)=1.
\end{aligned}$$

Dropping the rank-one constraint C20, the optimization problem (P7) is relaxed as

$$\text{(P8)} \quad \min_{\mathbf{Q},\xi} \quad \mathrm{Tr}\left(\mathbf{Q}^T\mathbf{H}^H \mathrm{diag}\{\mathbf{w}_e^H\mathbf{G}\}(\mathrm{diag}\{\mathbf{w}_e^H\mathbf{G}\})^H\mathbf{H}\right),$$
$$s.t. \quad \text{C16}-\text{C19}.$$

It is difficult to find that the optimization problem (P8) is convex and easily addressed by existing CVX tools. Once the optimal solution $\mathbf{Q}^*$ to the optimization problem (P8) and its maximum eigenvector are obtained, the optimal or sub-optimal solution $\mathbf{x}^*$ to the optimization problem (P5) can be obtained.

Step-2 (Optimizing $\mathbf{w}_b$):From the optimization problem (P0), it is found that γ_e can be indirectly reduced by optimizing $\mathbf{w}_b$ to increase γ_b. That is because the value of γ_b is determined by the combination of two variables $\mathbf{x}$ and $\mathbf{w}_b$ Once γ_b becomes larger by the optimization of $\mathbf{w}_b$, $\mathbf{x}$ has a wider feasible region to satisfy the constraint C1. Thus, given $\mathbf{x}$, the optimization problem (P0) is simplified as

$$\text{(P9)} \quad \max_{\mathbf{w}_b} \quad \gamma_b,$$
$$s.t. \quad \text{C3}.$$

Due to the constraint C3, the objective function maximization of the problem is equivalent to using spectral decomposition, it is derived that the Hermitian matrix

$$\max_{\mathbf{w}_b} \quad \gamma_b \Leftrightarrow \max_{\mathbf{w}_b} \quad |\mathbf{w}_b^H\mathbf{F}\mathrm{diag}\{\mathbf{Hx}\}|^2.$$

can be rewritten as $\mathbf{\Omega} = \mathbf{U}\mathbf{\Lambda}\mathbf{U}^H$, where $\mathbf{\Lambda}$ is a diagonal matrix consisting of the eigenvalues of $\mathbf{\Omega}$. Defining $\mathbf{v}_b = \mathbf{U}^H\mathbf{w}_b$, the optimization problem (P9) is reformulated as

$$\text{(P10)} \quad \max_{\mathbf{v}_b} \quad \mathbf{v}_b^H\mathbf{\Lambda}\mathbf{v}_b,$$
$$s.t. \quad \text{C21}: |\mathbf{v}_b| = 1.$$

For the optimization problem (P10), the optimal objective value is equal to the maximum eigenvalue of $\mathbf{\Omega}$. Based on this, it can be derived that the optimal $\mathbf{w}_b^*$ is the maximum eigenvector of $\mathbf{\Omega}$.

Algorithm 1 The Overall Algorithm for (P0)

1: **Initialization**: Set $t = 0$, ε, $\gamma_e^{(0)}$, $\mathbf{w}_b$.
2: Solve (P4) and employ rank-one recovery to obtain $\mathbf{w}_e^*$.
3: **repeat**
4: Set $t = t + 1$.
5: Solve (P10) to obtain $\mathbf{w}_b^{(t)}$.
6: Solve (P8) and employ rank-one recovery to obtain $\mathbf{x}^{(t)}$.
7: **until** $\frac{|\gamma_e^{(t)} - \gamma_e^{(t-1)}|}{\gamma_e^{(t)}} < \varepsilon$.
8: **return** $\gamma_e^{(t)}$.

The procedure for solving the optimization problem (P0) is outlined in Algorithm 1. The optimization problem (P0) can be addressed by the optimization of (P4) and the alternative optimization of (P8) and (P10), where the optimization problems (P4) and (P8) have much higher computational complexities than (P10).

4. ABEPS AT BOB AND EVE

Based on the design of the transmitted signal at Bob and the receiving beamforming vectors at Bob and Eve in the previous section, the ABEPs of PSK2 at Bob and Eve will be computed for the considered secure transmission system. Adopting a signal constellation diagram of size M, denoted by $\mathrm{X} = \{x_1, x_2, \cdots, x_M\}$ the closed-form expression of average symbol error probability (ASEP) for the l-th IRS element is given by

$$\mathrm{P}_{\mathrm{ASEP}}(l) = \sum_{m=1}^{M} \sum_{\hat{m}=1, \hat{m} \neq m}^{M} \frac{\Pr\left\{\boldsymbol{\theta}(l) = x_{\hat{m}} \mid \boldsymbol{\theta}(l) = x_m\right\}}{M},$$

where $\boldsymbol{\theta}(l)$ is the estimated vector of $\boldsymbol{\theta}(l)$ Based on this, the closed-form expression of the corresponding ABEP can be acquired. Particularly, the ABEPs of BPSK for the l-th IRS element at Bob and Eve are respectively given by

$$\mathrm{P}_{\mathrm{ABEP,\ BPSK,\ b}}(l) = Q\left(\sqrt{\frac{2}{\mathbf{C}_{\mathrm{b},ll}}}\right),$$

$$\mathrm{P}_{\mathrm{ABEP,\ BPSK,\ e}}(l) = Q\left(\sqrt{\frac{2}{\mathbf{C}_{\mathrm{e},ll}}}\right),$$

where $\mathbf{C}_{\mathrm{b},ll}$ is the (l,l)-th element of $\mathbf{C}_{\mathrm{b}} = \sigma_{\mathrm{b}}^2 \mathbf{U}_{\mathrm{b}} \mathbf{U}_{\mathrm{b}}^H$ with $\mathbf{V}_{\mathrm{b}} = \mathbf{F}\mathrm{diag}\{\mathbf{Hx}\}$ and $\mathbf{U}_{\mathrm{b}} = [\mathbf{V}_{\mathrm{b}}^H \mathbf{V}_{\mathrm{b}}]^{-1} \mathbf{V}_{\mathrm{b}}^H$; $\mathbf{C}_{\mathrm{e},ll}$ is the (l,l)-th element of $\mathbf{C}_{\mathrm{e}} = \mathbf{U}_{\mathrm{e}} \mathbf{T}\mathbf{x}\mathbf{x}^T \mathbf{T}^T \mathbf{U}_{\mathrm{e}}^H + \sigma_{\mathrm{e}}^2 \mathbf{U}_{\mathrm{e}} \mathbf{U}_{\mathrm{e}}^H$ with $\mathbf{V}_{\mathrm{e}} = \mathbf{G}\mathrm{diag}\{\mathbf{Hw}\}$ and $\mathbf{U}_{\mathrm{e}} = [\mathbf{V}_{\mathrm{e}}^H \mathbf{V}_{\mathrm{e}}]^{-1} \mathbf{V}_{\mathrm{e}}^H$. The ABEPs of QPSK for the l-th IRS element at Bob and Eve are approximately given by

$$\mathrm{P}_{\mathrm{ABEP,\ QPSK,\ b}}(l) \approx Q\left(\sqrt{\frac{1}{\mathbf{C}_{\mathrm{b},ll}}}\right),$$

$$\mathrm{P}_{\mathrm{ABEP,\ QPSK,\ e}}(l) \approx Q\left(\sqrt{\frac{1}{\mathbf{C}_{\mathrm{e},ll}}}\right).$$

When $\mathrm{M} > 4,$, the ABEPs for the l-th IRS element are approximately given by

$$\begin{aligned}
\mathrm{P}\ ABEP, M-PSK, b(l) &\approx \frac{2}{\log_2 M}\left[Q\left(\sqrt{\frac{1-\cos(2\pi/M)}{\mathbf{C}_{\mathrm{b},ll}}}\right)\right. \\
&\left. + Q\left(\sqrt{\frac{1-\cos(4\pi/M)}{\mathbf{C}_{\mathrm{b},ll}}}\right)\right], M > 4, \\
\mathrm{P}\ ABEP, M-PSK, e(l) &\approx \frac{2}{\log_2 M}\left[Q\left(\sqrt{\frac{1-\cos(2\pi/M)}{\mathbf{C}_{\mathrm{e},ll}}}\right)\right. \\
&\left. + Q\left(\sqrt{\frac{1-\cos(4\pi/M)}{\mathbf{C}_{\mathrm{e},ll}}}\right)\right], M > 4.
\end{aligned}$$

5. NUMERICAL RESULTS

In this section, numerical simulations are carried out to evaluate the secrecy performance of the considered secure transmission system of IRS-based microwave QR code. In simulations, the

channels $\mathbf{H},\mathbf{F},\mathbf{T}$ and $\mathbf{G}$ are assumed to fol low the Rician distribution and their path loss is given by $\mathrm{PL}=-30-25\lg(d)dB$ at the transmission distance d. The noise variances σ_b^2 and σ_e^2 at Bob and Eve are both set to be the same as the square of the path loss at $\mathrm{d}=50\mathrm{m}$。, aiming to normalize the round-trip path loss of signal propagation. The legend Security represents the proposed optimization scheme for the considered system. The legends Non-security and Active represent two counterparts. To be specific, Non-security denotes the optimization scheme

without regard to the eavesdropping. In Active, a large intelligent surface (LIS) [19] is employed instead of the passive IRS to show microwave QR code in an active manner, while Bob does not radiate EM wave. The legends PSK, Theo and Simu denote the modulation schemes of PSK, the theoretical results and the simulation results, respectively.

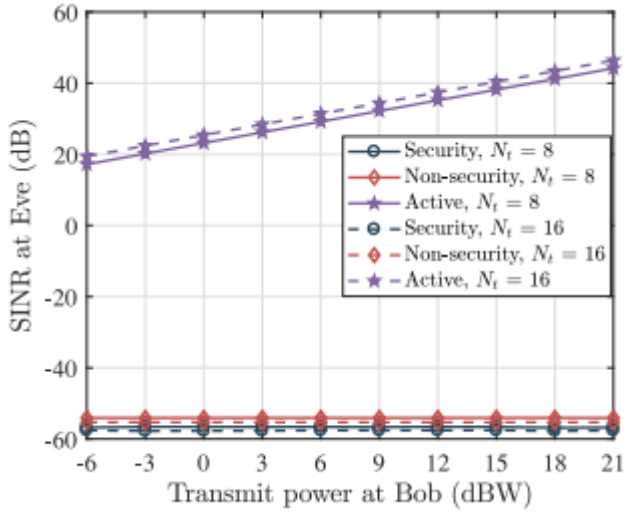

Fig. 2. SINR at Eve vs transmit power at Bob.

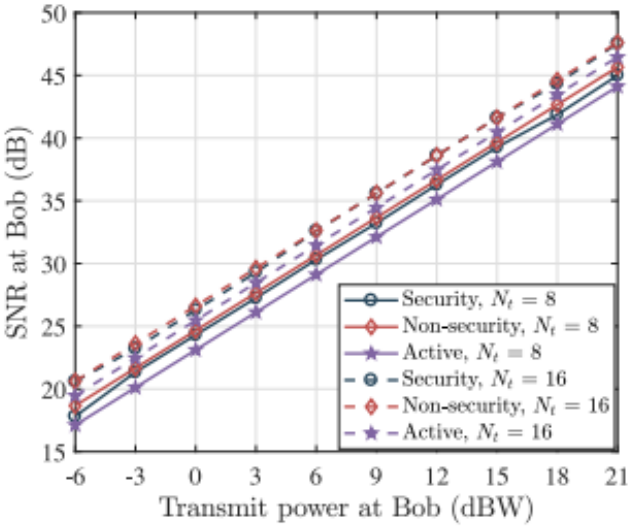

Fig. 3. SNR at Bob vs. transmit power at Bob.

Figs. 2 and 3 depict how the transmit power at Bob affects the SINR at Eve and the SNR at Bob, respectively, where the number of IRS elements L = 19; the number of transmitting antennas at Bob $N_t=16 or 8$ the numbers of receiving antennas at Bob and Eve $N_t=19 and N_e=19$,the distances from Bob to Alice $d_{\mathbf{H}}$=50m, from Bob to Eve $d_{\mathbf{T}}$=90m, from Alice to Eve $d_{\mathbf{G}}\sim[d_{\mathbf{H}}-6\mathrm{m},d_{\mathbf{H}}+6\mathrm{m}]$; the

threshold value $\gamma_{\mathrm{b}}=\dfrac{0.81^{H}\,\mathrm{diag}(\mathbf{F1})}{\sigma_{\mathrm{b}}^{2}}$; the Rician factor κ=0.5 The distance between Bob and Eve is set as 90 m, aiming to present the secrecy performance in the case that Eve suffers low interference from Bob. In Active, the SNR constraint at Bob is set to be the same as Security. From

Figs. 2 and 3, it can be seen that the schemes of Security and Non-security both achieve high secrecy. Compared to Non-security, the scheme of Security has a better secrecy but has a lower SNR at Bob. In the scheme of Active, the security is not guaranteed. These results indicate that the considered system has a good secrecy performance inherently.

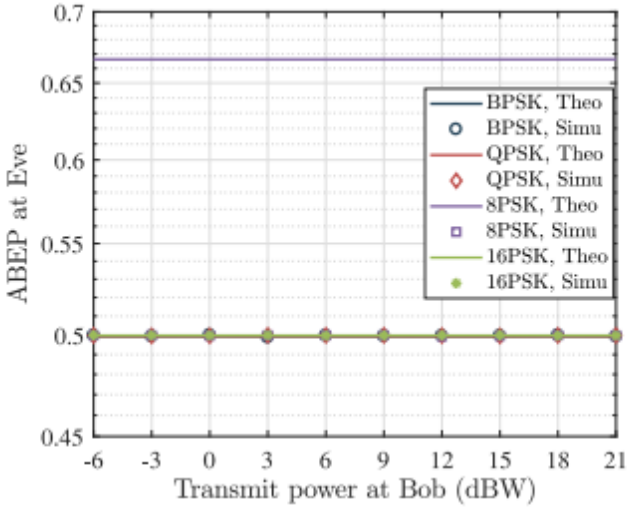

Fig. 4. ABEP at Eve vs. transmit power at Bob.

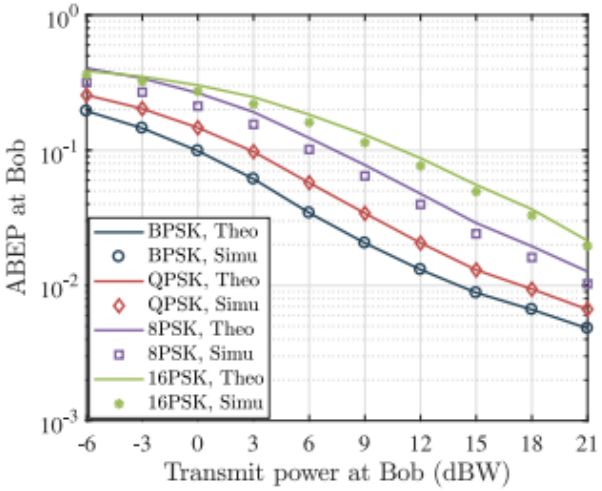

Fig. 5. ABEP at Bob vs. transmit power at Bob.

Figs. 4 and 5 show how the transmit power at Bob affects the ABEPs at Eve and Bob, respectively, where most simulation parameters are the same as the above setting values except for $N_{\mathrm{t}}=16$. It can be observed that the theoretical results of BPSK, QPSK and 16-PSK schemes almost coincide with the simulations, while those of the 8-PSK scheme at a low SINR/SNR do not match well. That is because the approximation of (1) and (2) is not good enough at a low SINR/SNR, especially for the 8-PSK scheme.

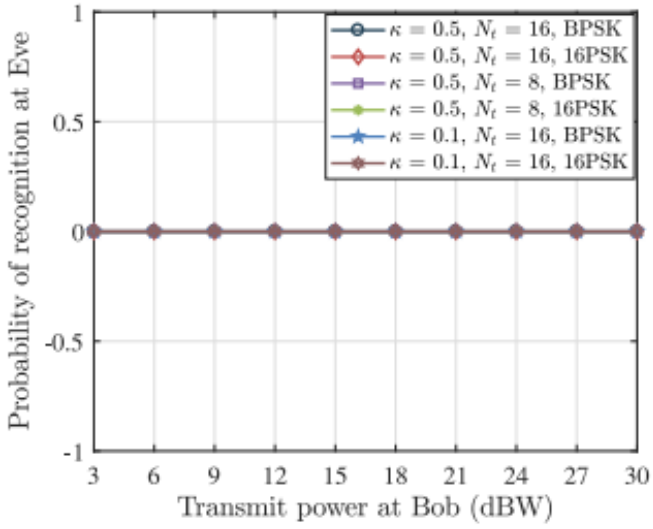

Fig. 6. Recognition probability at Eve vs. transmit power at Bob.

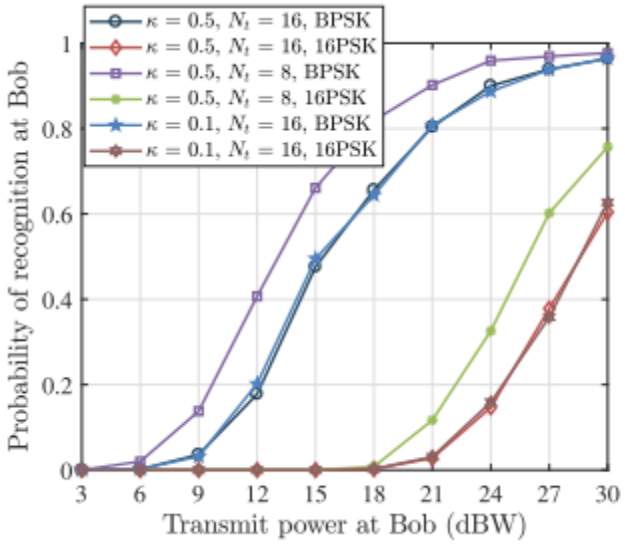

Fig. 7. Recognition probability at Bob vs. transmit power at Bob.

Figs. 6 and 7 plot how the transmit power at Bob affects the recognition probabilities at Eve and Bob, respectively, where the number of QR modules n=38×38 the numbers of receiving antennas at Bob and Eve $N_{\mathrm{r}} = 38$ and $N_{\mathrm{e}} = 38$ for BPSK and $N_{\mathrm{r}} = 19$ and $N_{\mathrm{e}} = 19$ for 16-PSK. Note that the IRS is fabricated from 38 or 19 different frequency-selective materials, aiming to realize the signal detection with much fewer receiving antennas than IRS elements. It can be seen that an increase in the transmit power at Bob and the Rician factor is beneficial to the recognition probability at Bob. Moreover, the recognition probability at Eve is almost zero, which verifies that the considered system has a good secrecy in disseminating the microwave QR code.

6. CONCLUSION

This report investigated communication security of IRS based microwave QR code. Based on the established model, the secrecy performance was optimized and the ABEPs at Bob and Eve were given. According to the simulations, it can be concluded that: 1) The proposed optimization scheme can improve the secrecy performance of system. 2) For the ABEPs at Bob and Eve, the theoretical

expression of PSK is a close approximation to the truth except for 8-PSK at a low SINR/SNR. 3) The considered system has a satisfactory secrecy performance, whether the transmitted signal and the receiving beamforming at Bob are or not jointly designed to prevent passive eavesdropping. That means that the security can still be guaranteed in the case of unknown eavesdropping CSI.

REFERENCES

1. Y. Liu, Z. Su, and Y. Wang, "Energy-efficient and physical layer secure computation offloading in blockchain-empowered Internet of Things," IEEE Internet Things J., early access, Mar. 14, 2022
2. Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," IEEE Commun. Surveys Tuts., vol. 19, no. 1, pp. 347–376, 1st Quart., 2017.
3. N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical layer security of 5G wireless networks for IoT: Challenges and opportunities," IEEE Internet Things J., vol. 6, no. 5, pp. 8169–8181, Oct. 2019.
4. S. Xu, J. Liu, Y. Cao, J. Li, and Y. Zhang, "Intelligent reflecting surface enabled secure cooperative transmission for satellite-terrestrial integrated networks," IEEE Trans. Veh. Technol., vol. 70, no. 2, pp. 2007–2011, Feb. 2021.
5. R. Duan, X. Wang, H. Yigitler, M. U. Sheikh, R. Jantti, and Z. Han, "Ambient backscatter communications for future ultra-low◎power machine type communications: Challenges, solutions, opportunities, and future research trends," IEEE Commun. Mag., vol. 58, no. 2, pp. 42–47, Feb. 2020.
6. N. V. Huynh, D. T. Hoang, X. Lu, D. Niyato, P. Wang, and D. I. Kim, "Ambient backscatter communications: A contemporary survey," IEEE Commun. Surveys Tuts., vol. 20, no. 4, pp. 2889–2922, 4th Quart., 2018.
7. M. Wu, X. Lei, X. Zhou, Y. Xiao, X. Tang, and R. Q. Hu, "Reconfigurable intelligent surface assisted spatial modulation for symbiotic radio," IEEE Trans. Veh. Technol., vol. 70, no. 12, pp. 12918–12931, Dec. 2021.
8. S. Guo, S. Lv, H. Zhang, J. Ye, and P. Zhang, "Reflecting modulation," IEEE J. Sel. Areas Commun., vol. 38, no. 11, pp. 2548–2561, Nov. 2020.
9. W. Tang et al., "MIMO transmission through reconfigurable intelligent surface: System design, analysis, and implementation," IEEE J. Sel. Areas Commun., vol. 38, no. 11, pp. 2683–2699, Nov. 2020.
10. X. Guan, Q. Wu, and R. Zhang, "Joint power control and passive beamforming in IRS-assisted spectrum sharing," IEEE Commun. Lett., vol. 24, no. 7, pp. 1553–1557, Jul. 2020.
11. S. Xu, Y. Du, J. Liu, and J. Li, "Intelligent reflecting surface based backscatter communication for data offloading," IEEE Trans. Commun., vol. 70, no. 6, pp. 4211–4221, Jun. 2022.
12. C. Wang, Z. Li, T.-X. Zheng, D. W. K. Ng, and N. Al-Dhahir, "Intelligent reflecting surface-aided secure broadcasting in millimeter wave symbiotic radio networks," IEEE Trans. Veh. Technol., vol. 70, no. 10, pp. 11050–11055, Oct. 2021.
13. S. Xu, J. Liu, and J. Zhang, "Resisting undesired signal through IRS◎based backscatter communication system," IEEE Commun. Lett., vol. 25, no. 8, pp. 2743–2747, Aug. 2021.
14. S. Xu, J. Liu, and Y. Cao, "Intelligent reflecting surface empowered physical-layer security: Signal cancellation or jamming?" IEEE Internet Things J., vol. 9, no. 2, pp. 1265–1275, Jan. 2022.
15. S. Xu, Y. Du, J. Zhang, and J. Zhang, "Microwave QR code: An IRS◎based solution," IEEE Trans. Veh. Technol., early access, doi: 10.1109/TVT.2022.3229955.
16. Q. Ma and T. J. Cui, "Information metamaterials: Bridging the physical world and digital world," PhotoniX, vol. 25, no. 1, pp. 1–32, Mar. 2020.
17. L. L. Li, H. T. Zhao, C. Liu, L. Li, and T. J. Cui, "Intelligent meta◎surfaces: Control, communication and computing," eLight, vol. 2, no. 1, pp. 1–24, May 2022.
18. A. Goldsmith, Wireless Communications. New York, NY, USA: Cambridge Univ. Press, 2005.
19. S. Hu, F. Rusek, and O. Edfors, "Beyond massive MIMO: The potential of data transmission with large intelligent surfaces," IEEE Trans. Signal Process., vol. 66, no. 10, pp. 2746–2758, May 2018