iCoding: Countermeasure Against Interference and Eavesdropping in Wireless Communications

Yicheng Liu, Zhao Li, *Member, IEEE*, Kang G. Shin, *Life Fellow, IEEE*, Zheng Yan, *Fellow, IEEE*, and Jia Liu, *Senior Member, IEEE*

***Abstract*— With the rapid development of wireless communication technologies, interference management (IM) and security/privacy in data transmission have become critically important. On one hand, due to the broadcast nature of wireless medium, the interference superimposed on the desired signal can destroy the integrity of data transmission. On the other hand, malicious receivers (Rxs) may eavesdrop a legitimate user's transmission and thus breach the confidentiality of communication. To counter these threats, we propose a novel encoding method, called *immunizing coding* (iCoding), which handles both IM and physical-layer security simultaneously. By exploiting both channel state information (CSI) and data carried in the interference, an iCoded signal is generated and sent by the legitimate transmitter (Tx). The iCoded signal interacts with the interference at the desired/legitimate Rx, so that the intended data can be recovered without the influence of disturbance, i.e., immunity to interference. In addition, since the data carried in the iCoded signal which is obtained via encoding the desired data and interference cooperatively, is different from the original desired data, the eavesdropper cannot access unauthorized information by wiretapping the desired signal, thus achieving immunity to eavesdropping. Our theoretical analysis, experimental and numerical evaluation have shown iCoding to effectively manage interference while preventing potential eavesdropping, hence enhancing the legitimate user's transmission and secrecy thereof.**

***Index Terms*— Interference, secure communication, coding, interference management, channel capacity, spectral efficiency.**

I. Introduction

DUE to the broadcast nature of wireless channels, wirelessly transmitted signals overlap with each other [1], risking the integrity and confidentiality of wireless transmissions as compared to wired communication [2]. On one hand, interference is superimposed on the desired signal at the intended receiver (Rx), impeding the recovery of the user's data and hence harming the integrity of communication [3]. On the other hand, owing to the broadcast nature of wireless medium, eavesdroppers within the coverage area of the legitimate transmission can hear and decode the signal to get the transmitted information, thus risking the confidentiality of communication. To mitigate/counter the above-mentioned risks, techniques such as interference management (IM) [4], [5], [6], [7], [8], [9], [10], secure communication (SC) [11], [12], [13], [14], [15], [16], and mechanisms incorporating both together [17], [18], [19] have been proposed and receiving an increasing attention in recent years.

There have been numerous IM methods, including ZF reception [4] and interference alignment (IA) [5], [6], which exploit channel state information (CSI); and interference neutralization (IN) [7], [8] and interference steering (IS) [9], [10], which exploit both CSI and data of the interference. With IA, interferences are adjusted at the interfering transmitter (Tx) so that multiple interfering signals are mapped into a finite subspace, that is, the overall interference space at the interfered/desired receiver (Rx) is minimized, while the desired signal(s) may be sent through a subspace without attenuation [5]. However, since IA adjusts spatial characteristics of the signals at the interfering Tx, the adjusted transmissions no longer match their channel, thus degrading the quality of the received signals at the interfering Rx (i.e., the Rx served by the interfering Tx). IN generates a neutralizing signal with respect to (w.r.t.) the disturbance, then the interference propagated through the wireless channel is canceled out by the neutralizing signal at the desired/interfered Rx, hence achieving interference-free reception of the desired signal [7], [8]. However, IN needs to consume additional transmit power of the desired Tx for generating neutralizing signal, thus yielding reduction of power for the intended signal's transmission. Considering the power overhead for IN, the authors of [9] and [10] proposed IS. IS employs a steering signal based on the interference information similarly to IN, but only manages the effective portion of the interference, i.e., the projection of interference on the desired signal. With IS, interference perceived by the interfered Rx is adjusted to a subspace orthogonal to the desired transmission. Compared to IN, IS reduces the power overhead for IM at the cost of consuming spatial

Received 23 April 2024; revised 27 August 2024; accepted 11 September 2024. Date of publication 26 September 2024; date of current version 4 October 2024. This work was supported in part by the National Natural Science Foundation of China under Grant 62072351, Grant U23A20300, and Grant 62202359; in part by the Key Research Project of Shaanxi Natural Science Foundation under Grant 2023-JC-ZD-35; in part by the 111 Center under Grant B16037; in part by JSPS KAKENHI under Grant JP23K16877; in part by the Project of Cyber Security Establishment with Inter-University Cooperation; and in part by the U.S. National Science Foundation under Grant 2245223. The associate editor coordinating the review of this article and approving it for publication was Dr. Dusit Niyato. *(Corresponding author: Zhao Li.)*

Yicheng Liu, Zhao Li, and Zheng Yan are with the School of Cyber Engineering, Xidian University, Xi'an, Shaanxi 710126, China (e-mail: ycliuxdu@stu.xidian.edu.cn; zli@xidian.edu.cn; zyan@xidian.edu.cn).

Kang G. Shin is with the Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, MI 48109 USA (e-mail: kgshin@umich.edu).

Jia Liu is with the Center for Strategic Cyber Resilience Research and Development, National Institute of Informatics, Tokyo 101-8430, Japan (e-mail: jliu@nii.ac.jp).

Digital Object Identifier 10.1109/TIFS.2024.3468902

degree-of-freedom (DoF), and is shown to yield good spectral efficiency (SE) performance and power-efficiency [10].

Aiming to defend against the breach of confidentiality from potential eavesdroppers in wireless communication systems, traditional SC addresses the security at upper layers of the protocol stack by using secret keys. With the increasing compute power of eavesdroppers, the effectiveness of traditional SC is facing a great challenge, yielding physical-layer security technologies, such as key encryption [11], [12], artificial noise (AN) [13], [14], cooperative jamming (CJ) [15] and beamforming (BF) [16], receiving widespread attention in recent years. Physical-layer key generation technique exploits reciprocity and randomness of wireless fading channels to generate security keys, providing protection against potential eavesdropping. In [11], a novel key generation scheme using random probing signals to hide CSI and combining both user generated randomness and channel randomness to generate a shared key, was proposed as a countermeasure against active attacks. This scheme can avoid the risks originated from CSI distribution where CSI acts as the security key. The authors of [12] introduced a wireless key establishment method that allows the Tx to specify arbitrary content as the key and manipulate the wireless channel to enable the Rx to obtain the same key without the need for information reconciliation. However, the methods in [11] and [12] require the Tx and Rx to perform channel estimation separately within the coherent time, which increases the power overhead and complexity of the system. The authors of [13] proposed for the first time that AN can be used for achieving SC. By imposing AN on the null subspace w.r.t. the desired signal, the influence of AN on the desired transmission can be avoided while the eavesdropper's signal-to-interference-plus-noise ratio (SINR) is deteriorated. In [14], AN is injected by the legitimate Tx. Without the knowledge of the eavesdropper's CSI, secure transmission can be realized by appropriately allocating the transmit power used for legitimate transmission and AN. The authors of [15] proposed a CJ strategy by employing legitimate source and destination as jammers in a half-duplex two-hop wireless relay network. However, this scheme requires the knowledge of eavesdropper's CSI. Reference [16] uses semi-definite programming relaxation to jointly design CJ and BF at the base station (BS). By optimizing the spatial autocorrelation matrix of the transmitted signal and adjusting its spatial distribution, the legitimate Rx can only receive the signal in a specific direction, thus limiting the maximum available SINR at the eavesdropper. However, the complexity of this method is very high and its extension to other system settings, e.g., eavesdropper and legitimate Rx are equipped with various numbers of antennas, is limited.

The above-mentioned IM and SC schemes are designed to address the risk of interference or eavesdropping. In practice, however, both risks may exist simultaneously. Therefore, it is important to design a comprehensive solution by integrating countermeasures of both IM and eavesdropping together. In [17], an IA-aided SC method was proposed. It lets the legitimate Tx send AN, so as to disrupt ZF-reception-based eavesdropping. However, this scheme degrades legitimate data rate and cannot guarantee security when the eavesdropper is equipped with multiple antennas. In [18], an unmanned aerial vehicle (UAV) assisted secure transmission scheme was proposed. In this work, UAVs exploit the idea of IA and cooperate with small-cell BSs (SBSs) to design precoding matrices, so that UAVs can act as SBSs and replace some idle ones. Meanwhile, in order to realize secure transmission, those idle SBSs replaced by the UAVs generate jamming signals to disrupt potential eavesdropping. The authors of [19] combined IA with CJ, in which AN is generated not only by the legitimate destination, but also the legitimate source and relay, thus degrading eavesdroppers' SINR severely. By carefully designing the precoding matrices, interferences from different Txs can be aligned within the same subspace at the legitimate destination, but not aligned at the eavesdroppers due to the randomness of wireless channels. However, this method incurs high cooperation overhead. Based on the above descriptions, to the best of our knowledge, the existing integration of IM and eavesdropping prevention [17], [18], [19] always eliminates the risks of interference and eavesdropping separately via two independent operations, i.e., no real integration is available.

To mitigate/overcome the above-mentioned deficiencies of existing schemes, we propose a novel scheme, called *immunizing coding* (iCoding), to achieve IM and SC in one operation. With this scheme, the original desired data is encoded at the legitimate Tx based on CSI and data information carried in the interference; the encoded data (i.e., iCoded data) is then sent to the desired/legitimate Rx. On one hand, the iCoded data is different from the original data, hence achieving the confidentiality of communication. On the other hand, the iCoded data interacts with interference at the legitimate Rx, so that the impact of interference on the desired transmission can be eliminated. In the design of iCoding, we present an 8-shaped mapping rule to meet the power constraint at the legitimate Tx. According to this rule, the iCoded data symbols to be sent can be confined to the original standard constellation map.

The contributions of this paper are three-fold:

- Proposal of *immunizing coding* (iCoding). By exploiting both CSI and data carried in the interference, an iCoded signal is generated and then sent by the legitimate Tx. iCoding can eliminate the disturbance at the legitimate Rx, hence realizing immunity to the interference, i.e., I2I. In addition, by exploiting both the randomness of wireless channel and interference, the iCoded data is no longer the same as the original desired data, thus achieving immunity to eavesdropping, namely, I2E.
- Design of constellation extension and 8-shaped mapping rule. First, by extending the constellation map, the iCoded data symbol exceeding the range of the original standard constellation can be represented and then be mapped back to the original constellation map to meet the power constraint at the legitimate Tx. Accordingly, the legitimate Rx performs inverse mapping on its decoded data to recover the original desired data correctly.
- Development of a supplement to guarantee the I2E property of iCoding. Since the iCoded data may be identical to the original desired data which incurs I2E loss, we employ a virtual coding component, namely

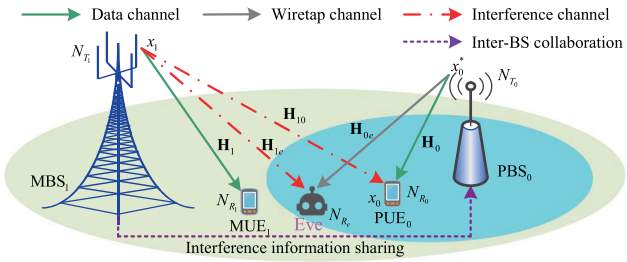


Fig. 1. System model.

escaping data to pre-attenuate the iCoded data in the encoding process so as to produce a data symbol different from the original desired data, hence regaining I2E. Correspondingly, the legitimate Tx should send an *artificial interference* (AI) to its serving Rx to counter the influence of escaping data carried in the received signal, and the original desired data can then be recovered.

The remainder of this paper is organized as follows. Section II describes the system model. Section III details the design of iCoding, while Section IV discusses the realization of iCoding under non-ideal situations. In Section V, we present a method to avoid I2E loss. In Section VI, we evaluate the performance of iCoding. Finally, we conclude the paper in Section VII.

Throughout this paper, we use the following notations. The set of complex numbers is denoted as $\mathbb{C}$, while vectors and matrices are represented by bold lower-case and upper-case letters, respectively. Let $\mathbf{X}^H$, $\mathbf{X}^T$ and $\mathbf{X}^{-1}$ be the Hermitian, transpose and inverse of matrix $\mathbf{X}$. $\|\cdot\|$ and $|\cdot|$ indicate the Euclidean norm and the absolute value. $\mathbb{E}(\cdot)$ denotes statistical expectation. Re$(\cdot)$ and Im$(\cdot)$ represent taking the real and imaginary part of a complex number.

II. System Model

We consider downlink transmission in heterogeneous cellular networks (HCNs) composed of overlapping macro and pico cells. As Fig. 1 shows, both macro BS (MBS$_1$) and pico BS (PBS$_0$) are equipped with N_{T_1} and N_{T_0} antennas, while macro user equipment (MUE$_1$) and pico user equipment (PUE$_0$) have N_{R_1} and N_{R_0} antennas, respectively. The eavesdropper (Eve) located in the coverage of pico-cell is equipped with N_{R_e} antennas. Let P_{T_1} and P_{T_0} denote the transmit power of MBS$_1$ and PBS$_0$, respectively. Let $\mathbf{H}_0 \in \mathbb{C}^{N_{R_0}\times N_{T_0}}$, $\mathbf{H}_1 \in \mathbb{C}^{N_{R_1}\times N_{T_1}}$, and $\mathbf{H}_{0e} \in \mathbb{C}^{N_{R_e}\times N_{T_0}}$ be the channel matrices from PBS$_0$ to PUE$_0$, MBS$_1$ to MUE$_1$, and PBS$_0$ to Eve, while CSI from MBS$_1$ to PUE$_0$ and Eve are denoted as $\mathbf{H}_{10} \in \mathbb{C}^{N_{R_0}\times N_{T_1}}$ and $\mathbf{H}_{1e} \in \mathbb{C}^{N_{R_e}\times N_{T_1}}$, respectively. We assume PBS$_0$ operates in an open mode [20] — i.e., users in the coverage of PBS$_0$ can access it, so that users' traffic can be offloaded from a heavily-loaded macro-cell to a pico-cell. Therefore, Eve may act as a legitimate user of PBS$_0$ to eavesdrop on the information transmitted from PBS$_0$ to PUE$_0$. Since PUE$_0$ and Eve are usually not at the same location, $\mathbf{H}_0$ and $\mathbf{H}_{0e}$ are statistically independent of each other [21]. We adopt a spatially uncorrelated Rayleigh flat fading channel to model the elements of the above channel matrices as independent and identically distributed (i.i.d.) zero-mean unit-variance complex Gaussian random variables. We assume that all Rxs experience block fading, i.e., channel parameters remain constant in a block consisting of several successive time slots and vary randomly between successive blocks. MUE$_1$ and PUE$_0$ can accurately estimate CSI from MBS$_1$ and PBS$_0$ to them, respectively, and feed it back to their associated BS via a low-rate, error-free link (e.g., X2 interface [22]). We assume reliable links for the delivery of CSI and signaling. The delivery delay is negligible relative to the time scale at which the channel state varies [23].

We let $\mathbf{x}_1$ and $\mathbf{x}_0$ denote the desired data vectors from MBS$_1$ and PBS$_0$ to their serving subscribers. $\mathbb{E}(\|\mathbf{x}_1\|^2) = \mathbb{E}(\|\mathbf{x}_0\|^2) = 1$ holds. For clarity of presentation, we assume both macro- and pico-transmissions employ beamforming (BF), i.e., only one data stream is sent from MBS$_1$ to MUE$_1$, and PBS$_0$ to PUE$_0$, respectively. Then, $\mathbf{x}_1$ and $\mathbf{x}_0$ become scalars x_1 and x_0. According to Fig. 1, transmission from MBS$_1$ to MUE$_1$ interferes with that from PBS$_0$ to PUE$_0$. Nevertheless, due to the limited coverage of pico-cell, PBS$_0$ will not cause too much interference to MUE$_1$, and thus the disturbance from PBS$_0$ to MUE$_1$ will be omitted in the rest of this paper.

Since pico-cells are deployed to improve the capacity and coverage of existing cellular systems, each pico-cell, unlike the macro-cell, has subordinate features, and hence the transmission in the macro-cell is given priority over that in the pico-cell. Specifically, MBS$_1$ will not adjust its transmission for the pico-users. However, we assume that PBS$_0$ can acquire the information of x_1 via inter-BS collaboration [24], [25]. With the above CSI and data information, iCoded data x_0^* can be generated at, and sent by PBS$_0$. Since the transmission from MBS$_1$ to MUE$_1$ only depends on $\mathbf{H}_1$ and is free from interference, we mainly focus on the pico user's transmission performance (including its secure capacity).

III. Design of Immunizing Coding

The received signal at PUE$_0$ is expressed as:

$$\mathbf{y}_0 = \sqrt{P_{T_0}}\mathbf{H}_0\mathbf{p}_0x_0^* + \sqrt{P_{T_1}}\mathbf{H}_{10}\mathbf{p}_1x_1 + \mathbf{z}_0 \quad (1)$$

where $\mathbf{p}_0$ represents the precoding vector for the iCoded data x_0^* at PBS$_0$ and $\mathbf{p}_1$ is the precoder for the interfering data x_1 at MBS$_1$. The first term on the right-hand side (RHS) of Eq. (1) denotes the iCoded signal sent from PBS$_0$ and the second term is the interference from MBS$_1$. $\mathbf{z}_0$ denotes the additive white Gaussian noise (AWGN) vector whose elements have zero-mean and variance σ_n^2. Note that in Eq. (1), PBS$_0$ sends an iCoded signal (carrying x_0^*) instead of its desired signal (carrying data x_0).

PUE$_0$ employs filter vector $\mathbf{w}_0$ to obtain the estimated signal $\hat{s}_0$ as:

$$\hat{s}_0 = \sqrt{P_{T_0}}\mathbf{w}_0^H\mathbf{H}_0\mathbf{p}_0x_0^* + \sqrt{P_{T_1}}\mathbf{w}_0^H\mathbf{H}_{10}\mathbf{p}_1x_1 + \mathbf{w}_0^H\mathbf{z}_0. \quad (2)$$

According to Eq. (2), the maximum gain of x_0^* is achieved as long as the precoder $\mathbf{p}_0$ and the receiving filter $\mathbf{w}_0$ match $\mathbf{H}_0$. We adopt the singular value decomposition (SVD) based precoding and receive filtering as an example, i.e., we apply SVD to $\mathbf{H}_0$ to obtain $\mathbf{H}_0 = \mathbf{U}_0\Lambda_0\mathbf{V}_0^H$. Then, we employ

$\mathbf{p}_0 = \mathbf{v}_0^{(1)}$ and $\mathbf{w}_0 = \mathbf{u}_0^{(1)}$ at PBS_0 and PUE_0, respectively, where $\mathbf{v}_0^{(1)}$ and $\mathbf{u}_0^{(1)}$ represent the first column vectors of the right and left singular matrices $\mathbf{V}_0$ and $\mathbf{U}_0$. In practice, there are other signal processing options which can be used for designing $\mathbf{p}_0$ and $\mathbf{w}_0$.

Let the iCoded data x_0^* be determined by the original desired data x_0 and x_c where x_c indicates virtual immunizing data. Then, Eq. (3) can be obtained as:

$$x_0^* = x_0 + x_c. \tag{3}$$

Substituting $\mathbf{p}_0 = \mathbf{v}_0^{(1)}$, $\mathbf{w}_0 = \mathbf{u}_0^{(1)}$ and Eq. (3) into Eq. (2), we have:

$$\hat{s}_0 = \sqrt{P_{T_0}}\lambda_0^{(1)}x_0 + \sqrt{P_{T_0}}\lambda_0^{(1)}x_c + \sqrt{P_{T_1}}[\mathbf{u}_0^{(1)}]^H\mathbf{H}_{10}\mathbf{p}_1x_1 + [\mathbf{u}_0^{(1)}]^H\mathbf{z}_0 \tag{4}$$

where $\lambda_0^{(1)}$ is the largest singular value of $\mathbf{H}_0$. The first term on the RHS of Eq. (4) contains PUE_0's desired data x_0 and the second term has the immunizing data x_c.

For accurate recovery of the desired data x_0 at PUE_0, the second and third terms on the RHS of Eq. (4) must satisfy:

$$\sqrt{P_{T_0}}\lambda_0^{(1)}x_c + \sqrt{P_{T_1}}[\mathbf{u}_0^{(1)}]^H\mathbf{H}_{10}\mathbf{p}_1x_1 = 0. \tag{5}$$

From Eq. (5) we can get Eq. (6) as:

$$x_c = -\sqrt{P_{T_1}/P_{T_0}}[\lambda_0^{(1)}]^{-1}[\mathbf{u}_0^{(1)}]^H\mathbf{H}_{10}\mathbf{p}_1x_1. \tag{6}$$

Note that in Eq. (6) x_c is related to the interfering data x_1, but not to x_0. By substituting Eq. (6) into Eq. (4), we can get:

$$\hat{s}_0 = \sqrt{P_{T_0}}\lambda_0^{(1)}x_0 + [\mathbf{u}_0^{(1)}]^H\mathbf{z}_0. \tag{7}$$

Therefore, according to Eq. (7), the interference is eliminated, thus leaving only the desired signal and noise. Based on the above analysis, the average spectral efficiency (SE) of PUE_0 can be calculated as:

$$\mathbb{E}(r_0) = \mathbb{E}\left\{\log_2\left\{1 + P_{T_0}[\lambda_0^{(1)}]^2/\sigma_n^2\right\}\right\} \tag{8}$$

where σ_n^2 denotes the noise power.

For clarity of presentation, we take square-16QAM (Quadrature Amplitude Modulation) as an example to illustrate the basic principle of iCoding, as shown in Fig. 2. We denote the desired signal component as $s_0 = \sqrt{P_{T_0}}\lambda_0^{(1)}x_0$, the immunizing signal as $s_c = \sqrt{P_{T_0}}\lambda_0^{(1)}x_c$, the received signal component from PBS_0 as $\tilde{s}_0^* = \sqrt{P_{T_0}}\lambda_0^{(1)}x_0^*$, and the interference from MBS_1 as $s_1 = \sqrt{P_{T_1}}[\mathbf{u}_0^{(1)}]^H\mathbf{H}_{10}\mathbf{p}_1x_1$, respectively. Then, the estimated/filtered signal in Eq. (4) (ignoring noise) can be rewritten as $\hat{s}_0 = \tilde{s}_0^* + s_1$. Similarly, the iCoded signal sent by PBS_0 is expressed as $\mathbf{s}_0^* = \sqrt{P_{T_0}}\mathbf{p}_0x_0^*$. According to Eqs. (2)–(4), we define operator $\mathcal{J}(\cdot)$ to represent extraction of the effective portion of a signal component, i.e., equivalent data symbol carried in the signal. By applying $\mathcal{J}(\cdot)$ to various signals, the inter-signal relationship can be mapped into the constellation map and represented by inter-equivalent-symbol relationship. It should be noted that $\mathcal{J}(\cdot)$ may involve different signal processing for various signal components. Specifically, we define the operators at PBS_0 and PUE_0 as $\mathcal{J}_T(\cdot) = \frac{1}{\sqrt{P_{T_0}}}\mathbf{p}_0^\dagger$ where $\mathbf{p}_0^\dagger = (\mathbf{p}_0^T\mathbf{p}_0)^{-1}\mathbf{p}_0^T$ is the pseudo-inverse of $\mathbf{p}_0$ and $\mathcal{J}_R(\cdot) = \frac{1}{\sqrt{P_{T_0}}\lambda_0^{(1)}}$, respectively. Then, we can have $\mathcal{J}_T(\mathbf{s}_0^*) = x_0^*$, $\mathcal{J}_R(s_0) = x_0$, $\mathcal{J}_R(s_c) = x_c$, $\mathcal{J}_R(\tilde{s}_0^*) = x_0^*$ and $\mathcal{J}_R(\hat{s}_0) = x_0$. As for $\mathcal{J}_R(s_1)$, it should be noticed that $\mathcal{J}_R(s_1) = \frac{s_1}{\sqrt{P_{T_0}}\lambda_0^{(1)}} = \frac{\sqrt{P_{T_1}}[\mathbf{u}_0^{(1)}]^H\mathbf{H}_{10}\mathbf{p}_1}{\sqrt{P_{T_0}}\lambda_0^{(1)}}x_1$, i.e., $\mathcal{J}_R(s_1) \neq x_1$. Based on the above discussion, we can use a two-dimensional vector to express the equivalent data symbol carried in a signal in the constellation map, the vector starts at the origin and ends at the constellation point corresponding to the equivalent data symbol.

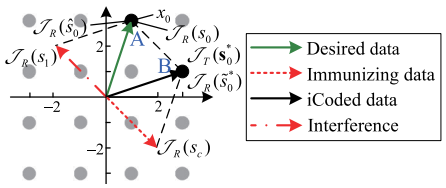


Fig. 2. Illustration of the basic principle of iCoding.

As Fig. 2 shows, PBS_0 first calculates the immunizing data x_c ($\mathcal{J}_R(s_c)$) according to interference s_1 in terms of Eq. (6), and then encodes the original desired data x_0 (point A in Fig. 2) with x_c to obtain the iCoded data x_0^* ($\mathcal{J}_T(\mathbf{s}_0^*)$, point B). Next, PBS_0 sends the iCoded signal $\mathbf{s}_0^*$ to PUE_0. Likewise, PUE_0 applies $\mathbf{w}_0 = \mathbf{u}_0^{(1)}$ to the received signal $\mathbf{y}_0$ and extracts the estimated data symbol, denoted as $\mathcal{J}_R(\hat{s}_0)$, from the post-processed signal $\hat{s}_0$. $\mathcal{J}_R(\hat{s}_0) = \mathcal{J}_R(\tilde{s}_0^* + s_1)$ holds. According to Eq. (7), $\mathcal{J}_R(\hat{s}_0)$ is the same as $\mathcal{J}_R(s_0)$ (point A), i.e., PUE_0 can accurately recover original desired data x_0 from $\tilde{s}_0^* + s_1$. Based on the above discussion, iCoding can mitigate s_1 at PUE_0, hence realizing I2I. Moreover, since $\mathcal{J}_T(\mathbf{s}_0^*) \neq x_0$, Eve's eavesdropping on x_0 is crippled.

It should be noticed that Fig. 2 only shows the realization of iCoding in an ideal situation, i.e., x_0^* ($\mathcal{J}_T(\mathbf{s}_0^*)$) and $\mathcal{J}_R(\hat{s}_0)$ exactly locate at standard constellation points in the square-16QAM constellation map. However, in practice, due to the randomness of interference, x_0^* may be out of the range of the original constellation, or even be in the surrounding area of a standard constellation point. Similarly, due to channel randomness and the influence of noise, such non-ideal situations may occur in obtaining $\mathcal{J}_R(\hat{s}_0)$ at PUE_0. In what follows, we will present the design of iCoding under above-mentioned non-ideal situations in Section IV.

IV. Design of iCoding Under Non-Ideal Situations

A. Constellation Extension and 8-Shaped Mapping

Due to the randomness of interference, the iCoded data x_0^* may be out of the range of the original constellation map. In such a case, if x_0^* is directly sent, PBS_0's power range needs to be extended; this will not only incur more transmit power consumption, but also increase PBS_0's hardware cost. In what follows, we will first present the constellation extension so that the iCoded symbol exceeding the original constellation can be represented; and then, under the constraints of transmit power and its dynamic range at PBS_0, we propose a 8-shaped mapping rule according to which the iCoded data x_0^* in the extended constellation is mapped back to the original

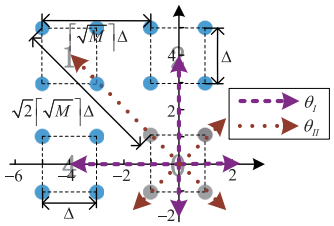


Fig. 3. Illustration of constellation extension.

constellation map before being transmitted. Likewise, the decoded data at PUE_0 is inversely mapped to the original constellation, so that the original desired data x_0 can be accurately recovered.

The constellation extension rule can be expressed as:

$$\begin{cases} d_{\theta_I} = 3^{k-1}\lceil\sqrt{M}\rceil\Delta \\ d_{\theta_{II}} = \sqrt{2}\cdot 3^{k-1}\lceil\sqrt{M}\rceil\Delta \end{cases} \tag{9}$$

where d_{θ_I} and $d_{\theta_{II}}$ represent the distances from the origin to the center of the duplicated constellations along directions determined by $\theta_I \in \{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$ and $\theta_{II} \in \{\frac{\pi}{4}, \frac{3\pi}{4}, \frac{5\pi}{4}, \frac{7\pi}{4}\}$, respectively, in the k^{th} round extension. M denotes the modulation order. Δ is the horizontal (or vertical) distance between two adjacent constellation points. The notation $\lceil\cdot\rceil$ denotes rounding up to the nearest integer. Note, in practice, that the iCoded symbol may still be out of the range of the 1^{st} round extended constellation. In such a case, we can duplicate the 1^{st} round extended constellation according to Eq. (9) to obtain the 2^{nd} round extended constellation, and continue this process repeatedly. Then, we take the 1^{st} round extension of square-4QAM (Quadrature Amplitude Modulation) as an example in Fig. 3.

As the figure shows, we index the original constellation map with 0, then we duplicate it along two directions determined by phase angle θ_I. Since $k = 1$, the center of the duplicated constellation is $\lceil\sqrt{M}\rceil\Delta$ away from the origin (i.e., the center of original constellation). We can thus obtain the first-stage duplicated constellation map by adding two constellations indexed with 2 and 4, respectively, to 0. Next, we copy the original constellation along the other directions determined by θ_{II}. The center of the duplicated constellation is $\sqrt{2}\lceil\sqrt{M}\rceil\Delta$ away from the origin. Then, one constellations indexed with 1 is added to the first-stage duplicated constellation map. For space limitations, we only plot the constellation extension in the second quadrant in Fig. 3. The other duplicated constellations along θ_I and θ_{II} can be obtained in the same manner.

Based on the above discussion, the iCoded data can be represented by the constellation point in the extended constellation map. However, direct transmission of such an extended symbol requires a high dynamic range of transmit power at the Tx, incurring an increase of equipment's complexity and cost. To solve this problem, we propose an 8-shaped mapping rule which is applied to the Tx and Rx, respectively. For simplicity, we consider the case of iCoded symbol coinciding with standard constellation point. As for the case of existence of deviation from the iCoded/estimated data to standard constellation point, we will elaborate it in the next subsection.

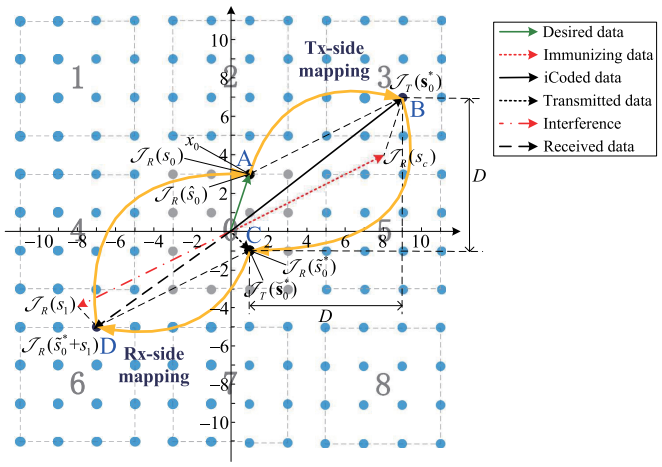


Fig. 4. Realization of iCoding in extended constellation and with 8-shaped mapping rule.

Fig. 4 shows the realization of iCoding in the 1^{st} round extended square-16QAM constellation where the 8-shaped mapping rule is applied. At the Tx-side, PBS_0 calculates x_c ($\mathcal{J}_R(s_c)$) according to s_1 and then encodes x_0 (point A in Fig. 4) with it so as to obtain x_0^*. When x_0^* ($\mathcal{J}_T(\mathbf{s}_0^*)$, point B) exceeds the range of original constellation, $\mathcal{J}_T(\mathbf{s}_0^*)$ is mapped back to $\check{x}_0^*$ ($\mathcal{J}_T(\check{\mathbf{s}}_0^*)$, point C), $\check{\mathbf{s}}_0^*$ is the actual transmitted signal of PBS_0. $\mathcal{J}_T(\mathbf{s}_0^*) = \check{x}_0^*$ indicates removing $\sqrt{P_{T_0}}\mathbf{p}_0$ in the expression of $\check{\mathbf{s}}_0^*$. As Fig. 4 shows, the relative position of $\mathcal{J}_T(\check{\mathbf{s}}_0^*)$ in constellation 0 is the same as that of $\mathcal{J}_T(\mathbf{s}_0^*)$ in constellation 3. In this way, an arbitrary iCoded symbol can be limited to the range of original constellation. Then, $\mathcal{J}_T(\check{\mathbf{s}}_0^*)$ is sent by PBS_0.

Noting that an arbitrary symbol can be represented by its amplitude (ρ) and phase (ϕ), an iCoded data x_0^* can be expressed as $x_0^* = \rho_0^* e^{j\phi_0^*}$. Then, we can get $\text{Re}(x_0^*) = \rho_0^*\cos\phi_0^*$ and $\text{Im}(x_0^*) = \rho_0^*\sin\phi_0^*$. So, the 8-shaped mapping rule can be expressed as:

$$\begin{cases} \text{Re}(\check{x}_0^*) = \rho_0^*\cos\phi_0^* - D\cdot\text{Rd}\left(\frac{\rho_0^*\cos\phi_0^*}{D}\right) \\ \text{Im}(\check{x}_0^*) = \rho_0^*\sin\phi_0^* - D\cdot\text{Rd}\left(\frac{\rho_0^*\sin\phi_0^*}{D}\right) \end{cases} \tag{10}$$

where $\text{Rd}(\cdot)$ denotes the rounding-off operation. D is the horizontal mapping distance between $\mathcal{J}_T(\mathbf{s}_0^*)$ (point B) and $\mathcal{J}_T(\check{\mathbf{s}}_0^*)$ (point C). D is determined by the number of extending times k, the modulation order M, and the horizontal (vertical) distance between two adjacent standard constellation points Δ. $D = 3^{k-1}\lceil\sqrt{M}\rceil\Delta$ holds. Consider Fig. 4 as an example, in which $k = 1$, $M = 16$ and $\Delta = 2$, so that we can get $D = 8$. We use $\mathcal{R}_8(\cdot)$ to denote the 8-shaped mapping operation, by substituting $D = 8$, $\text{Re}(x_0^*) = 9$ and $\text{Im}(x_0^*) = 7$ into Eq. (10), we can see that $\mathcal{R}_8(x_0^*) = \check{x}_0^*$ holds.

At the Rx-side, PUE_0 extracts $\mathcal{J}_R(\tilde{s}_0^* + s_1)$ (point D) from the post-processed mixed signal $\tilde{s}_0^* + s_1$, and then inversely maps $\mathcal{J}_R(\tilde{s}_0^* + s_1)$ to obtain the estimated data $\mathcal{J}_R(\hat{s}_0)$ in the original constellation. As the figure shows, $\mathcal{J}_R(\hat{s}_0) = \mathcal{J}_R(s_0) = x_0$ holds; that is, x_0 is accurately decoded. The expression of inverse mapping rule at PUE_0 is the same as that at PBS_0, we only need to substitute the amplitude and phase of $\mathcal{J}_R(\tilde{s}_0^* + s_1)$ instead of ρ_0^* and ϕ_0^*, into Eq. (10).

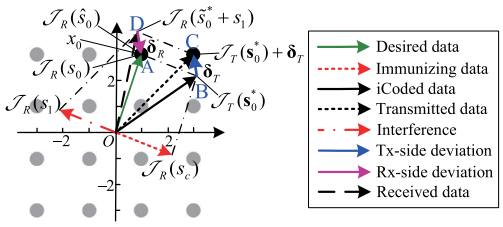


Fig. 5. Realization of iCoding under the existence of deviation from x_0^* and $\mathcal{J}_R(\hat{s}_0)$ (or $\mathcal{J}_R(\tilde{s}_0^* + s_1)$) to standard constellation point (w/o constellation extension).

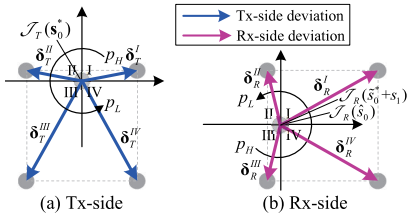


Fig. 6. Illustration of prioritized maximum likelihood.

In Fig. 4, we use yellow arrowed arcs to depict the 8-shaped mapping at PBS_0 and PUE_0. Specifically, start from x_0 (point A) to $\mathcal{J}_T(\mathbf{s}_0^*)$ (point B) via arc $\overset{\frown}{\text{AB}}$; next, along $\overset{\frown}{\text{BC}}$ to $\mathcal{J}_T(\tilde{\mathbf{s}}_0^*) = x_0^*$ (point C); and then, from point C via $\overset{\frown}{\text{CD}}$ to $\mathcal{J}_R(\tilde{s}_0^* + s_1)$ (point D); finally, along $\overset{\frown}{\text{DA}}$ to $\mathcal{J}_R(\hat{s}_0)$ (point A). Since the shape of $\overset{\frown}{\text{ABCDA}}$ is similar to that of number 8, we call the proposed mapping rule as 8-shaped mapping.

Figs. 2 and 4 have presented the design principle of iCoding graphically. However, the relation of the original desired data x_0 and the recovered $\hat{x}_0$ ($\mathcal{J}_R(\hat{s}_0)$) still needs to be verified quantitatively. We provide a theorem as follows.

Theorem 1: In the case of the iCoded data coincides with a standard constellation point, the desired data x_0 is iCoded (and mapped according to the 8-shaped mapping rule) and sent by the Tx. At the desired Rx, after applying matched filter to the received mixed signal (and inversely mapping the estimated $\mathcal{J}_R(\tilde{s}_0^* + s_1)$ in terms of the 8-shaped mapping rule), x_0 can be recovered correctly.

Since the proof of Theorem 1 can be referred in that of Theorem 2, as provided in the Appendix, we do not explicitly present the proof of Theorem 1.

B. Design of iCoding Under the Existence of Deviation From the iCoded/Estimated Data to Standard Constellation Point

As aforementioned, due to the randomness of interference, the iCoded data x_0^* may not be exactly at the standard constellation point. That is, x_0^* deviates from standard constellation point at the source. Similarly, at the destination, the estimated data may also be away from standard constellation point. To address such non-ideal situation, we employ maximum likelihood (ML) criterion to obtain the standard constellation point with minimum Euclidean distance from x_0^* at the Tx-side and $\mathcal{J}_R(\hat{\mathbf{s}}_0)$ (or $\mathcal{J}_R(\tilde{s}_0^* + s_1)$) at the Rx-side, respectively.

Fig. 5 takes square-16QAM as an example to show the coding and decoding process at PBS_0 and PUE_0, respectively, under the existence of deviation from x_0^* ($\mathcal{J}_T(\mathbf{s}_0^*)$) and estimated data $\mathcal{J}_R(\hat{s}_0)$ (or $\mathcal{J}_R(\tilde{s}_0^* + s_1)$) to standard constellation point. As the figure shows, at PBS_0, although $\mathcal{J}_T(\mathbf{s}_0^*)$ does not exceed the range of original constellation, it is not at any standard constellation point. According to the ML criterion, we approximate $\mathcal{J}_T(\mathbf{s}_0^*)$ to $\mathcal{J}_T(\mathbf{s}_0^*) + \boldsymbol{\delta}_T$ so as to obtain standard constellation point. $\boldsymbol{\delta}_T$ represents the deviation vector from $\mathcal{J}_T(\mathbf{s}_0^*)$ to its nearest standard constellation point. Then, PBS_0 sends the iCoded data $\mathcal{J}_T(\mathbf{s}_0^*) + \boldsymbol{\delta}_T$. At PUE_0, $\mathcal{J}_R(\hat{s}_0)$ (or $\mathcal{J}_R(\tilde{s}_0^* + s_1)$) is extracted from the post-processed signal $\tilde{s}_0^* + s_1$; then, according to ML, PUE_0 can obtain the estimated data $\mathcal{J}_R(\hat{s}_0) + \boldsymbol{\delta}_R$ (or $\mathcal{J}_R(\tilde{s}_0^* + s_1) + \boldsymbol{\delta}_R$) where $\boldsymbol{\delta}_R$ is the deviation vector from $\mathcal{J}_R(\hat{s}_0)$ (or $\mathcal{J}_R(\tilde{s}_0^* + s_1)$) to its nearest constellation point. As Fig. 5 shows, $\mathcal{J}_R(\hat{s}_0) + \boldsymbol{\delta}_R = \mathcal{J}_R(\tilde{s}_0^* + s_1) + \boldsymbol{\delta}_R = \mathcal{J}_R(s_0) = x_0$ holds, i.e., PUE_0 can correctly recover the original desired data x_0. When considering constellation extension, a similar analysis can be conducted, leading to the same conclusion regarding the feasibility of iCoding. For conciseness, we have omitted the details here.

Theorem 2: In the case of there exists deviation from the iCoded/estimated data to standard constellation point, the desired/legitimate Tx and Rx can employ ML to obtain the transmitted and recovered data, respectively, locating at standard constellation point, and realize correct desired data transmission.

The proof of Theorem 2 is given in Appendix.

From the proof of Theorem 2, we can see that the deviation vectors at PBS_0 and PUE_0 should have the same length and opposite direction, i.e., $\boldsymbol{\delta}_R = -\boldsymbol{\delta}_T$ should hold, so that PUE_0 can recover x_0. However, when the iCoded data lies in the mid-vertical line of two adjacent standard constellation points, using ML cannot determine the unique constellation point to which the iCoded data approximates. In such a case, PBS_0 may randomly select one of the constellation points with the same minimum distance to $\mathcal{J}_T(\mathbf{s}_0^*)$ and send it to PUE_0. However, without the information of $\boldsymbol{\delta}_R$, PUE_0 cannot determine the unique standard constellation point. If the estimated data $\mathcal{J}_R(\hat{s}_0)$ is selected mistakenly, i.e., $\boldsymbol{\delta}_R = -\boldsymbol{\delta}_T$ does not hold, erroneous decoding is incurred. To solve this problem, we can employ *prioritized maximum likelihood* (PML) by establishing a coordinate system centered at $\mathcal{J}_T(\mathbf{s}_0^*)$ and specifying the priority order of the four quadrants (see in Fig. 6). Each quadrant contains a standard constellation point obtained by applying ML to $\mathcal{J}_T(\mathbf{s}_0^*)$ at Tx (Fig. 6(a)) and to $\mathcal{J}_R(\tilde{s}_0^* + s_1)$ at Rx (Fig. 6(b)), respectively, so that the transmitted and estimated data can be uniquely determined. In this way, there is no need to send $\boldsymbol{\delta}_T$ to PUE_0 for assisting its data recovery.

Specifically, as Fig. 6(a) shows, at the Tx-side the first quadrant has the highest priority and the fourth quadrant has the lowest priority, whereas in Fig. 6(b) it is shown that at the Rx-side the third quadrant has highest priority and the second quadrant has the lowest priority. In subfigure (a), the coordinate system is centered at the iCoded data $\mathcal{J}_T(\mathbf{s}_0^*)$; we can find four standard constellation points which are closest to $\mathcal{J}_T(\mathbf{s}_0^*)$ in four quadrants, denoted by I, II, III and IV, respectively. As the figure shows, $\boldsymbol{\delta}_T^I = \boldsymbol{\delta}_T^{II}$ and $\boldsymbol{\delta}_T^{III} = \boldsymbol{\delta}_T^{IV}$, since $|\boldsymbol{\delta}_T^I| < |\boldsymbol{\delta}_T^{III}|$ and the standard point in quadrant I

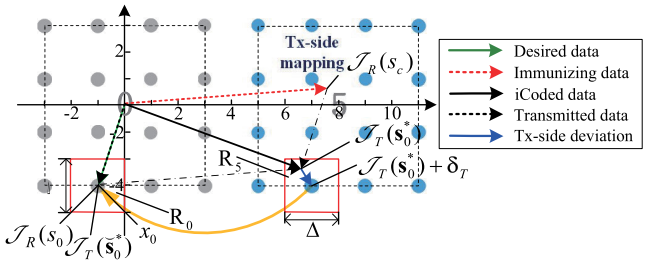


Fig. 7. An example of I2E loss (w/ constellation extension).

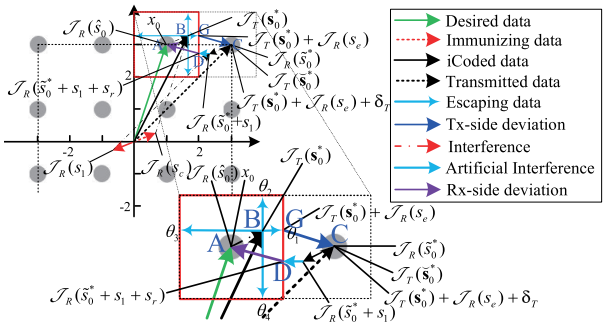


Fig. 8. Realization of iCoding with I2E+ (w/o constellation extension).

has higher priority than that in quadrant II, $\mathcal{J}_T(\mathbf{s}_0^*) + \boldsymbol{\delta}_T^I$ will be sent instead of $\mathcal{J}_T(\mathbf{s}_0^*)$. Similarly, in subfigure (b), a coordinate system centered at $\mathcal{J}_R(\tilde{s}_0^* + s_1)$ is established, and then data corresponding to $\mathcal{J}_R(\tilde{s}_0^* + s_1) + \boldsymbol{\delta}_R^{III}$ is sent instead of $\mathcal{J}_R(\tilde{s}_0^* + s_1)$.

V. Design of I2E Reinforcement

As discussed so far, the realization of immunity-to-eavesdropping (I2E) of iCoding lies in the fact that the iCoded data $\mathcal{J}_T(\mathbf{s}_0^*)$ (or $\mathcal{J}_T(\mathbf{s}_0^*) + \boldsymbol{\delta}_T$, or $\mathcal{J}_T(\tilde{\mathbf{s}}_0^*)$) is different from the original desired data x_0. However, in practice, the randomness of interference may yield the transmitted data being identical to x_0, hence incurring I2E loss. To remedy this deficiency, we propose an I2E reinforcement method, called *I2E+*, to ensure the secrecy of iCoding.

Before delving into the details of I2E+, we first present an example of I2E loss in Fig. 7. Due to the symmetry of constellation, we only plot the original constellation (indexed with 0) and one of its extensions (indexed with 5). As the figure shows, the iCoded data $\mathcal{J}_T(\mathbf{s}_0^*)$ lies in the red square region marked as R_5, which is centered at a standard constellation point in the #5 constellation. The edge-length of region R_5 is Δ. Then, according to ML, any $\mathcal{J}_T(\mathbf{s}_0^*)$ falls in R_5 will be an approximate to the standard point at the square's center. In this example, PBS_0 calculates $\mathcal{J}_R(s_c)$ and then encodes it with the desired data x_0 to obtain the iCoded data $\mathcal{J}_T(\mathbf{s}_0^*)$. Since $\mathcal{J}_T(\mathbf{s}_0^*)$ is not a standard constellation point, we apply ML to $\mathcal{J}_T(\mathbf{s}_0^*)$ to get its closest standard constellation point $\mathcal{J}_T(\mathbf{s}_0^*) + \boldsymbol{\delta}_T$. As $\mathcal{J}_T(\mathbf{s}_0^*) + \boldsymbol{\delta}_T$ is in the #3 constellation, we then apply an 8-shaped mapping to obtain the transmitted data $\mathcal{J}_T\left(\check{\mathbf{s}}_0^*\right)$ which is in the original constellation. As Fig. 7 shows, $\mathcal{J}_T\left(\check{\mathbf{s}}_0^*\right)$ coincides with the desired data x_0, thus incurring I2E loss. Therefore, we call such a red square area *forbidden coding region* (FCR); while as FCR's counterpart, we call the remaining part of the (extended) constellation *permitting coding region* (PCR). Moreover, as Fig. 7 shows, there are multiple FCRs w.r.t. a specific desired data in the extended constellation, and the number of FCRs is the same as that of the constellations. Clearly, in order to realize I2E, the encoded data should not be in FCR. It is worth noting that the likelihood of the iCoded data x_0^* being the same with the desired data x_0 (lies in the FCR) is influenced by the interference, especially the interference power. For instance, if the power of interference is zero, the iCoded data will certainly be the same as the desired data, thereby necessitating I2E+. On the contrary, if the power of interference is sufficiently strong to enable of iCoding to produce data that differs from the desired data with high probability, I2E+ is deactivating. However, there remains a non-zero probability that the iCoded data will be identical to the desired data even under strong interference. This can occur if the iCoded data falls within the FCR of the extended constellation and is subsequently mapped back to the FCR of the original constellation after applying 8-shaped mapping rule. In summary, I2E+ can significantly enhance the confidentiality of iCoding, particularly in scenarios with weak interference.

Based on the above observations, we will next present the design of I2E+ without constellation extension in Fig. 8. For simplicity, we only plot one quadrant at the Tx- and Rx-side, in which the encoding and decoding are realized. The basic idea of I2E+ is to employ an *escaping data* x_e (in addition to the iCoded data x_c) carried in a virtual coding component s_e (i.e., $\mathcal{J}_R(s_e) = x_e$ holds), in the encoding process, so as to let the iCoded data escape from FCR. Then, we can get an escaped iCoded data lying in PCR, so that the transmitted data can differ from the original desired data x_0, hence realizing I2E. It should be noted that x_e ($\mathcal{J}_R(s_e)$) is only a virtual component used during the encoding process which is similar to x_c, and thus there is no need of a physical signal to carry x_e and be sent by PBS_0. However, PBS_0 needs to send PUE_0 an *artificial interference* (AI) whose post-processed version at PUE_0 is denoted as s_r, carrying *recovering data* x_r (i.e., $\mathcal{J}_R(s_r) = x_r$ holds), along with the escaped iCoded signal, so that $\mathcal{J}_R(s_e)$ can be counteracted by $\mathcal{J}_R(s_r)$ and only the desired data is left for PUE_0. Since generating such AI consumes the transmit power of PBS_0, I2E+ should find the shortest path along which the encoded data escapes from the FCR, so that the power consumption for I2E+ can be minimized.

One can easily see that the shortest path along which the iCoded data escapes from the FCR should be one of the vectors starting from B, being vertical to and reaching the four edges of the FCR. We denote the four candidate escaping directions as θ_1, θ_2, θ_3 and θ_4, respectively. By comparing the distances from point B to the four edges of the FCR along the four candidate directions, we can determine x_e ($\mathcal{J}_R(s_e)$) with the shortest escaping path. We define φ_e as the phase of x_e and can have four different φ_es corresponding to θ_1, θ_2, θ_3 and θ_4, respectively. Then, the amplitude of x_e, denoted by ρ_e, under various φ_es can be computed as:

$$\rho_e = \begin{cases} \Delta - (\mathrm{Re}\left(x_0^*\right) \bmod \Delta), & \theta_1;\ \mathrm{Re}\left(x_0^*\right) \bmod \Delta, \quad \theta_3 \\ \Delta - (\mathrm{Im}\left(x_0^*\right) \bmod \Delta), & \theta_2;\ \mathrm{Im}\left(x_0^*\right) \bmod \Delta, \quad \theta_4 \end{cases} \tag{11}$$

where mod denotes modulus operator, Δ represents the edge-length of FCR, and Re$(\cdot)$ and Im$(\cdot)$ denote the real and imaginary part of a constellation point, respectively. Then, the escaping data x_e can be expressed as $x_e = \rho_e e^{j\varphi_e}$. As Fig. 8 shows, due to the effect of $\mathcal{J}_R(s_e)$, the iCoded data is steered from FCR into PCR. Then, we can apply ML to approximate the escaped data $\mathcal{J}_T(\mathbf{s}_0^*) + \mathcal{J}_R(s_e)$ (point G) to a nearby constellation point $\mathcal{J}_T(\mathbf{s}_0^*) + \mathcal{J}_R(s_e) + \boldsymbol{\delta}_T$ (point C). Therefore, the final transmitted iCoded data $\mathcal{J}_T(\check{\mathbf{s}}_0^*) = \mathcal{J}_T(\mathbf{s}_0^*) + \mathcal{J}_R(s_e) + \boldsymbol{\delta}_T$ is different form x_0, realizing I2E.

After performing the Tx-side process, PBS_0 sends the escaped iCoded signal and AI to PUE_0. Then, PUE_0 can perceive a mixed signal containing both interference and the above-mentioned components. The superimposed data carried in the mixed signal can be decoded as $\mathcal{J}_R(\tilde{s}_0^* + s_1 + s_r)$ (point D). Note that $\mathcal{J}_T(\mathbf{s}_0^*) = \mathcal{J}_R(\tilde{s}_0^*)$ (without constellation extension) holds as the signal components on both sides of the equation contain the same data x_0^* (this is similar to the case shown in Fig. 2). By applying ML, PUE_0 can get the desired data as $\mathcal{J}_R(\hat{s}_0) = \mathcal{J}_R(\tilde{s}_0^* + s_1 + s_r) + \boldsymbol{\delta}_R = x_0$ (point A).

We use $P_{T_0}^{(r-)}$ and $P_{T_0}^{(r)}$ to denote the transmit power for the iCoded signal under the influence of x_e, and AI, respectively. Then, the received mixed signal of PUE_0 can be expressed as:

$$\mathbf{y}_0 = \sqrt{P_{T_0}^{(r-)}}\mathbf{H}_0\mathbf{p}_0\tilde{x}_0^* + \sqrt{P_{T_0}^{(r)}}\mathbf{H}_0\mathbf{p}_0 x_r + \sqrt{P_{T_1}}\mathbf{H}_{10}\mathbf{p}_1 x_1 + \mathbf{z}_0 \tag{12}$$

where $\tilde{x}_0^* = x_0 + x_c + x_e$ is the iCoded data obtained by employing I2E+. In this case, x_c can be calculated according to Eq. (6) by replacing P_{T_0} with $P_{T_0}^{(r-)}$.

At PUE_0, we post-process $\mathbf{y}_0$ with $\mathbf{u}_0^{(1)}$, and can get the estimated signal $\hat{s}_0$ as:

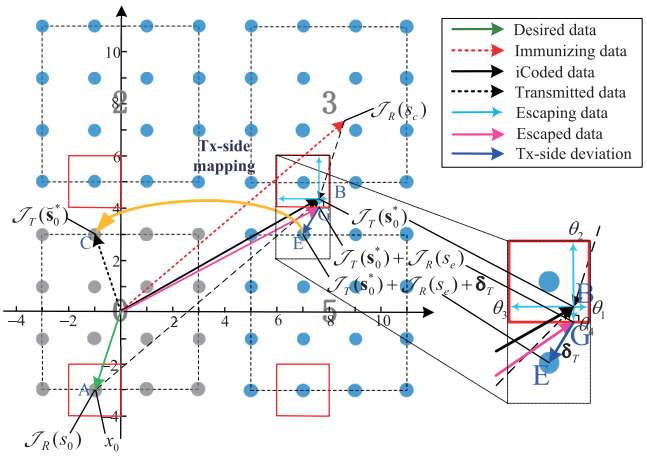
$$\begin{aligned}\hat{s}_0 = &\sqrt{P_{T_0}^{(r-)}}\lambda_0^{(1)}(x_0 + x_c) - \sqrt{P_{T_0}^{(r-)}}\lambda_0^{(1)}x_e + \sqrt{P_{T_0}^{(r)}}\lambda_0^{(1)}x_r \\ &+ \sqrt{P_{T_1}}[\mathbf{u}_0^{(1)}]^H\mathbf{H}_{10}\mathbf{p}_1 x_1 + [\mathbf{u}_0^{(1)}]^H\mathbf{z}_0.\end{aligned} \tag{13}$$

According to Eq. (13), in order to completely counter the influence of x_e, x_r should satisfy:

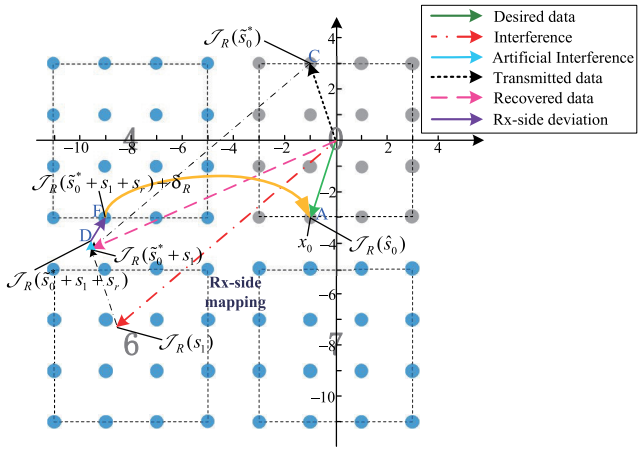
$$\sqrt{P_{T_0}^{(r)}}x_r = -\sqrt{P_{T_0}^{(r-)}}x_e. \tag{14}$$

Since $x_e = \rho_e e^{\varphi_e}$ and $x_r = \rho_r e^{\varphi_r}$ where ρ_r and φ_r denote the amplitude and phase of x_r, respectively, we can have $\varphi_r = -\varphi_e$ and $\sqrt{P_{T_0}^{(r)}}\rho_r = \sqrt{P_{T_0}^{(r-)}}\rho_e$. Note that φ_e and ρ_e have been determined by Eq. (11); and $P_{T_0}^{(r-)}$ is computed according to Eq. (6) so as to eliminate the interference component $\sqrt{P_{T_1}}[\mathbf{u}_0^{(1)}]^H\mathbf{H}_{10}\mathbf{p}_1 x_1$ in Eq. (13). Therefore, the strength of AI can be determined by $\sqrt{P_{T_0}^{(r-)}}\rho_e$. This way, we can have the recovering signal sent by PBS_0 as $\sqrt{P_{T_0}^{(r-)}}\mathbf{p}_0\rho_e e^{-j\varphi_e}$.

Based on the above discussion, we can also realize iCoding with I2E+ in an extended constellation as shown in Fig. 9. As Fig. 9(a) shows, upon the iCode data $\mathcal{J}_T(\mathbf{s}_0^*)$ (point B) escaping from FCR in the #3 constellation to PCR in the #5 constellation (the escaped data is represented by point G), ML is applied to obtain a standard constellation point $\mathcal{J}_T(\mathbf{s}_0^*) + \mathcal{J}_R(s_e) + \boldsymbol{\delta}_T$ (point E). Then, by applying 8-shaped mapping, we can have the final iCoded transmitted data



(a) Realization of iCoding with I2E+ at the Tx-side.



(b) Realization of iCoding with I2E+ at the Rx-side.

Fig. 9. Realization of iCoding with I2E+ (w/ constellation extension).

$\mathcal{J}_T(\check{\mathbf{s}}_0^*) = \mathcal{R}_8(\mathcal{J}_T(\mathbf{s}_0^*) + \mathcal{J}_R(s_e) + \boldsymbol{\delta}_T)$ (point C). It is shown that $\mathcal{J}_T(\check{\mathbf{s}}_0^*) \neq x_0$, so I2E is realized. Fig. 9(b) plots the Rx-side processing of iCoding with I2E+. As the figure shows, PUE_0 perceives a mixed signal composing of the escaped iCoded signal, interference and AI. By applying matched filtering, we can obtain the estimated data as $\mathcal{J}_R(\tilde{s}_0^* + s_1 + s_r)$ (point D). Recall that $\mathcal{J}_T(\mathbf{s}_0^*) = \mathcal{J}_R(\tilde{s}_0^*)$ (without constellation extension) or $\mathcal{J}_T(\check{\mathbf{s}}_0^*) = \mathcal{J}_R(\tilde{s}_0^*)$ (with constellation extension) holds as signal components on both sides of the two equations carry the same data x_0^*. Then, we use ML to approximate $\mathcal{J}_R(\tilde{s}_0^* + s_1 + s_r)$ to its nearby constellation point $\mathcal{J}_R(\tilde{s}_0^* + s_1 + s_r) + \boldsymbol{\delta}_R$ (point F) with deviation $\boldsymbol{\delta}_R$. Finally, we employ the inverse mapping to $\mathcal{J}_R(\tilde{s}_0^* + s_1 + s_r) + \boldsymbol{\delta}_R$ and can obtain the estimated desired data $\mathcal{J}_R(\hat{s}_0)$ being identical to x_0 (point A). This way, correct decoding is realized.

We now briefly discuss the power consumption of iCoding with constellation extension and iCoding with I2E+. The power consumption of the former is determined by the power of the iCoded data alone, while the latter is determined jointly by the power of the iCoded data and AI. By exploiting the randomness of both wireless channel and interference, the iCoded data is no longer the same as the original desired data, thus achieving I2E. However, the iCoded data may fall

TABLE I
PARAMETER SETTINGS OF THE EXPERIMENT

Parameter	Carrier freq.	Symbol rate	Interpolation factor	Sampling rate (baseband)	Roll-off factor of filter	Transmit gain
Value	915MHz	0.2MBaud	2	0.4MHz	0.5	[5dB, 15dB]

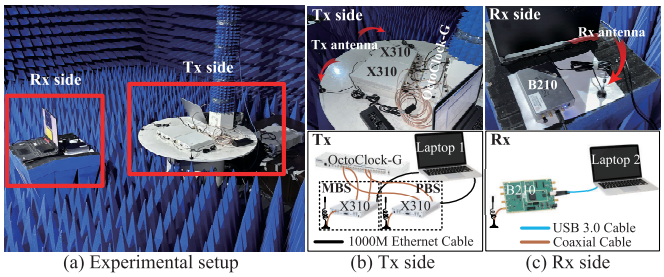
outside the range of the original constellation map, thereby incurring extra power consumption and PBS_0's hardware cost. To address this deficiency, we propose constellation extension and 8-shape mapping rule. Specifically, we first extend the original constellation to represent any iCoded data exceeding the range of the original constellation, then, we apply 8-shaped mapping rule to map the iCoded data back to the original constellation before transmission. Therefore, the iCoded data transmitted by PBS_0 are within the original constellation map, which shares the same mathematical expectation power as the data transmitted without iCoding. As a result, there is no additional power consumption at the PBS_0 when iCoding is applied. As for iCoding with I2E+, PBS_0 needs to send PUE_0 an AI carrying recovering data x_r along with the escaped iCoded signal so as to counteract the influence introduced by the escaping data x_e. This transmission of AI will incur additional power consumption. In the next section, we will show the simulation result of the average power cost for AI, from which employing I2E+ in iCoding is found to incur only a small amount of power overhead, thus making it practical useful.

VI. EVALUATION

In this section, we first use the universal software radio peripheral (USRP) platform to implement iCoding and demonstrate its validity, and then use MATLAB simulation to evaluate the performance of iCoding and iCoding with I2E+.

A. Hardware Implementation of iCoding

We use QPSK for the desired transmission, with amplitude 1 and phases $\{\frac{\pi}{4}, \frac{3\pi}{4}, \frac{5\pi}{4}, \frac{7\pi}{4}\}$, and BPSK for the interference, with amplitude $\sqrt{2}$ and phases $\{0, \pi\}$. Fig. 10 shows the experimental setup of iCoding. To mitigate the influence of multipath, environmental interference from human motion, unexpected RF signal transmission, and background noise on the experimental results, we conducted the experiment in an anechoic chamber, thereby facilitating the validation of iCoding. However, it should be noted that our method can be applied to practical communication scenarios where the aforementioned factors are present. As illustrated in Fig. 10(a), the prototype system includes two Txs representing MBS_1 and PBS_0, respectively, and a Rx. Note that the Rx can serve as either the PUE_0 or the eavesdropper, depending on its location (the details can be referred to Fig. 11). As subfigures (b) and (c) show, the Tx-side consists of two USRP X310 devices, each equipped with a single antenna. The two Txs are connected to a host computer (called laptop1) through 1000M Ethernet cables and synchronized with an OctoClock-G clock source. The Rx is implemented using a USRP B210 with a single antenna, connected to a host computer (called laptop2). In the experiment, laptop1 controls MBS_1 and



(a) Experimental setup (b) Tx side (c) Rx side

Fig. 10. Experimental setup of iCoding.

PBS_0 to simultaneously transmit interference and the iCoded signal to the Rx. Note that in the generation of the iCoded signal, the interference data x_1 is available at the PBS_0 via the centralized control of laptop1. The main parameters used in the experiment are shown in Table I.

As plotted in Fig. 10(b), we utilize one X310 as MBS_1, while the other serves as PBS_0. It should be noticed that the transmit power of USRP device, denoted as P_T, is determined by the transmit gain, G_T, at the USRP device, and the amplitude of transmitted symbol, A_S, cooperatively. $[P_T] = [G_T] + [A_S^2]$ holds where $[P_T]$ and $[A_S^2]$ are in dBm and $[G_T]$ is in dB. In the experiment, we set the range of $[G_T]$ for PBS_0 to be [5dB, 15dB], and for MBS_1 to be [8dB, 18dB]. The iCoded data and interference data have the same A_S. As a result, P_{T_1} is twice (a.k.a., 3dB higher than) that of P_{T_0}. Consequently, the amplitude of the signal sent from MBS_1 and received by the PUE_0 is $\sqrt{2}$ times that of the signal from PBS_0.

Fig. 11 shows various deployments of the eavesdropper in the iCoding experiment. As the figure shows, we deploy the legitimate Rx on the mid-perpendicular of the line connecting MBS_1 and PBS_0. We categorize the location of the eavesdropper in the anechoic chamber into three types based on the strength of interference and iCoded signal: strong interference region, strong iCoded signal region, and comparable mixed signal region. In the strong interference and strong iCoded signal regions, the reception of the eavesdropper (denoted by Eve_2 and Eve_1) is dominated by the interference and the iCoded signal, respectively, while in the comparable mixed signal region, the reception of the eavesdropper (denoted by Eve_3) is determined by the interaction of both signal components. It should be noted that in the case of Eve_3, the iCoded signal and interference arrive at the eavesdropper asynchronously, which can cause interference to eavesdropping.

According to Fig. 11, we can infer that the iCoded signal and interference will undergo similar fading before reaching the legitimate Rx, i.e., the CSI from MBS_1 and PBS_0 to PUE_0 (i.e., h_{10} and h_0) satisfy $h_{10} = h_0 = h$.[1] With this

[1]As MBS_1, PBS_0, and PUE_0 are equipped with a single antenna in the experiment, $\mathbf{H}_{10}$ and $\mathbf{H}_0$ become scalars.

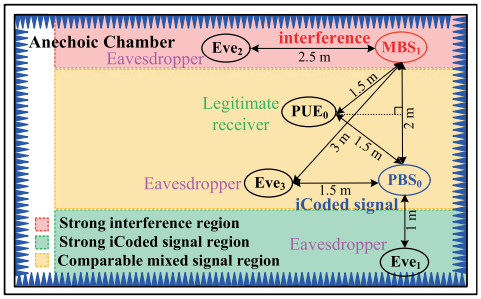


Fig. 11. Various deployments of the eavesdropper.

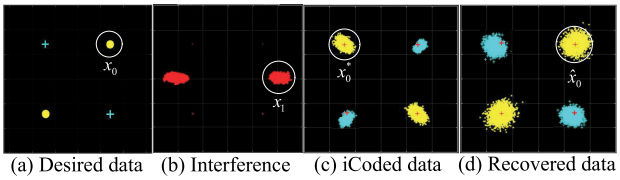


Fig. 12. Validation of iCoding based on the constellation map.

simplification, Eq. (2) can be rewritten as:

$$\hat{s}_0 = \sqrt{P_{T_0}} h x_0 + \sqrt{P_{T_0}} h x_c + \sqrt{P_{T_1}} h x_1 + z_0. \tag{15}$$

Then, similarly to the derivation of Eqs. (3)–(5), and noting that we adopt $P_{T_1}/P_{T_0} = 2$ in the experiment, we can have $\sqrt{P_{T_0}} h x_c + \sqrt{P_{T_1}} h x_1 = 0$ and $x_c = -\sqrt{2} x_1$. In this setup, there is no need to estimate h_{10} and h_0, hence simplifying the implementation of iCoding.

In the case of Eve_1, the iCoded signal from PBS_0 is dominant, while Eve_2 suffers from strong interference since her location is adjacent to MBS_1. As for Eve_3, the iCoded signal and interference arrive asynchronously, and the CSI of the two transmission links is unavailable for channel fading compensation, resulting in severe destructive influence for eavesdropping.

B. Experimental Result

To verify the validation and evaluate the performance of iCoding, we first present the experimental results of the constellation map at the legitimate source, interferer, and legitimate receiver with iCoding in Fig. 12.

As depicted in Fig. 12, we use two different colors to represent the QPSK constellation points for clarity. In iCoding, since the desired data only participates in the coding process at the legitimate Tx instead of being directly transmitted, we employ a standard QPSK constellation to present the constellation of the desired data in Fig. 12(a). Fig. 12(b) plots the constellation of a BPSK modulated interference with amplitude $\sqrt{2}$ and phases $\{0, \pi\}$. Following the principle of iCoding, we can obtain the iCoded constellation in terms of the interference and desired data, as depicted in Fig. 12(c). Consequently, the legitimate Rx processes the received mixed signal and obtains the estimated constellation as plotted in Fig. 12(d). In subplot (a), we take the desired data x_0 and in subplot (b), we use the interference data x_1 as examples. Using iCoding, an iCoded data x_0^* is obtained, from which the estimated data $\hat{x}_0$ can be recycled. By comparing subplots

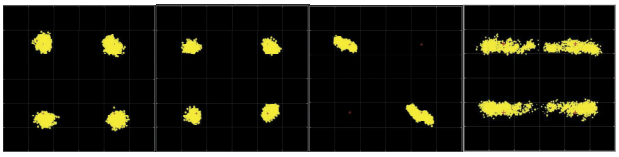


Fig. 13. The estimated constellations of the legitimate Rx and eavesdropper at their respective locations.

(c) and (a) we can observe that the iCoded data differs from the original desired data. In contrast, the estimated data $\hat{x}_0$ at the legitimate Rx, as illustrated in subplot (d), is identical to the desired data. Fig. 12 verifies that the iCoded signal carries distinct data information from the original desired data, and is capable of completely mitigating the influence of interference at the legitimate Rx. In other words, immunity to both interference and eavesdropping is achieved.

Then, we plot in Fig. 13 the constellations observed by both legitimate Rx and eavesdropper at their respective locations specified in Fig. 11.

Fig. 13(a) shows the constellation at the legitimate Rx (i.e., PUE_0). In this case, the interference and the iCoded signal both experience approximately the same channel fading before reaching the legitimate Rx. As a result, the Rx can observe a clear and concentrated QPSK constellation. In subfigure (b), the eavesdropper can perceive a strong iCoded signal from PBS_0. As the iCoded signal is still QPSK modulated, the estimated constellation at Eve appears in QPSK form. However, since the iCoded data is distinct from the original desired data, the eavesdropper cannot extract the legitimate information by decoding the received mixed signal. When Eve is deployed in the strong interference region, as shown in subfigure (c), the interference from MBS_1 is strong. Since the interference is a BPSK modulated signal in our experiment, the eavesdropper observes a distorted and rotated BPSK constellation with phases differing from that of the original interference. This is because in the experiment, we let Eve employ QPSK demodulation. Then, according to the maximum likelihood criterion, a rotated BPSK constellation aligning with part of the QPSK template is yielded. Moreover, due to the impact of a relatively weak iCoded signal, we can observe that the rotated BPSK constellation is somewhat distorted. In this scenario, the eavesdropping can be effectively crippled. In subfigure (d), the strength of the iCoded signal is comparable to that of the interference. However, the two signals undergo different channel fading before reaching the eavesdropper. In this case, the observed constellation at Eve appears as a distorted QPSK constellation, effectively thwarting eavesdropping.

To verify the IM and secrecy performance of iCoding, we evaluate the BER performance of both the legitimate Rx and the eavesdropper at their respective locations as plotted in Fig. 14. For ease of comparison, we also plot the BER of PUE_0 without interference (denoted as PUE_0 w/o intf.), which can serve as an upper bound of the BER performance of the legitimate Rx.

As depicted in the figure, PUE_0 can achieve a lower BER than Eve, and the BER curves of PUE_0 decrease significantly

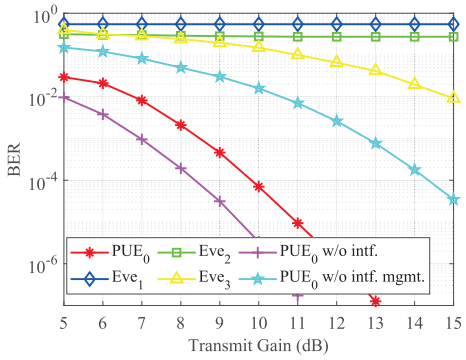


Fig. 14. BER performance of the legitimate Rx and eavesdropper.

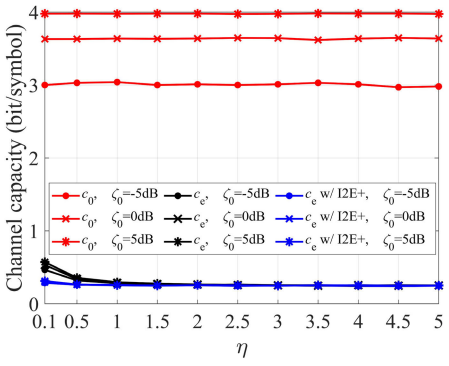
as the transmit gain increases. With iCoding, the influence of interference can be mitigated, resulting in a BER to, but still inferior to, the upper bound.[2] In contrast, when the interference is left unmanaged (denoted as PUE_0 w/o intf. mgmt.), PUE_0's BER is noticeably degraded. As for the eavesdropper deployed at various locations, his/er BER performance is poor. This is because: 1) the iCoded signal and the interference interact asynchronously with each other, thereby hindering the eavesdropper from obtaining an accurate constellation map (e.g., in the cases of Eve_2 and Eve_3), and 2) even if a standard constellation is available (e.g., in the case of Eve_1), the decoded data information still contains numerous errors due to the I2E capability of iCoding.

C. MATLAB Simulation of iCoding

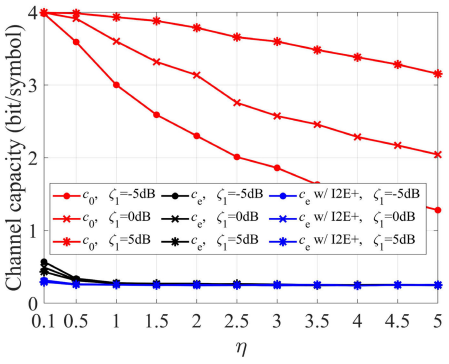
We now evaluate the performance of iCoding and iCoding with I2E+ using MATLAB simulation. We employ channel capacity to demonstrate the efficiency and secrecy of the proposed methods. According to information theory, channel capacity of PUE_0 and Eve, denoted as c_0 and c_e, respectively, are the maximum amount of mutual information that can be achieved in the communications from PBS_0 to them. Besides iCoding, we also simulate some other typical methods, including IS, IN, ZF reception, point-to-point multiple-input multiple-output (p2pMIMO) and non-interference management (non-IM) (i.e., the PUE_0 employs matched filtering (MF) to decode its desired data while leaving the interference unmanaged) for comparison.

We set $N_{T_i} = N_{R_i} = N_{R_e} = 2$ where $i \in \{0, 1\}$ and assume SVD based precoding and receive filtering is employed. We let both MBS_1 and PBS_0 adopt square-16QAM to generate 10^3 symbols i.e., x_1 and x_0, in each sample. We obtain the simulation results by averaging over 5×10^4 samples. Moreover, we utilize gray coding criterion to ensure better symbol error rate. x_0 is randomly selected from the sixteen 16QAM symbols with equal probability. The generation of x_1 satisfies random distribution, since the interference sent form MBS_1 to PUE_0 is random after passing through channel.

[2]This is because our experimental setup could not ensure strict identity of the channel fading experienced by the iCoded signal and interference, as described in the derivation related to Eq. (15). Consequently, the two signal components cannot interact with each other as expected, resulting in some loss compared to the upper bounded BER.



(a) $\zeta_0 \in \{-5, 0, 5\}$ dB.



(b) $\zeta_1 \in \{-5, 0, 5\}$ dB.

Fig. 15. Variation of c_0 and c_e vs. η under different ζ_0s and ζ_1s.

Under iCoding with I2E+, we first encode x_0 with x_c to promote iCoding and then exam whether the coding result obtains I2E, if I2E of this sample is lost, we calculate escaping data and code it with iCoded data. In this simulation, We can obtain the marginal distribution functions of x_0 as $p(x_0)$ at PBS_0 and the estimated $\hat{x}_0$ as $p(\hat{x}_0)$ at PUE_0, as well as their joint distribution function $p(x_0, \hat{x}_0)$, respectively, so that c_0 can be calculated as:

$$\begin{aligned} c_0 &= \max_{p(x_0)} \{I(X_0; \hat{X}_0)\} \\ &= \max_{p(x_0)} \left\{ \sum_{x_0 \in X} \sum_{\hat{x}_0 \in \hat{X}_0} p(x_0, \hat{x}_0) \log_2 \frac{p(x_0, \hat{x}_0)}{p(x_0) p(\hat{x}_0)} \right\} \end{aligned} \tag{16}$$

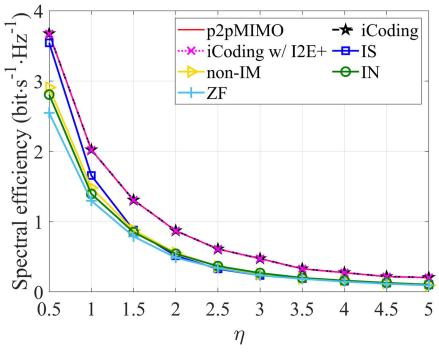
where X and $\hat{X}_0$ denote the symbol sets at PBS_0 and PUE_0, respectively, to which x_0 and $\hat{x}_0$ belong, i.e., $x_0 \in X_0$ and $\hat{x}_0 \in \hat{X}_0$ hold, $I(X_0; \hat{X}_0)$ represents the average mutual information. Similarly, Eve's eavesdropping capacity c_e is computed as $c_e = \max I(X_0; \hat{X}_e)$ where $\hat{X}_e$ is the estimated symbol set at Eve.

We use $\bar{P}_{T_1}$ and $\bar{P}_{T_0}$ to denote the effective power of received signals sent from MBS_1 and PBS_0, at PUE_0 [8]. Then, we define the transmit power of MBS_1 and PBS_0 normalized by noise power as $\zeta_1 = 10 \lg \frac{\bar{P}_{T_1}}{\sigma_n^2}$ and $\zeta_0 = 10 \lg \frac{\bar{P}_{T_0}}{\sigma_n^2}$, respectively. We also use η to denote the ratio of $\bar{P}_{T_1}$ to $\bar{P}_{T_0}$, i.e., $\eta = \frac{\bar{P}_{T_1}}{\bar{P}_{T_0}}$. We set $\eta \in [0.1, 5]$ in the simulation.

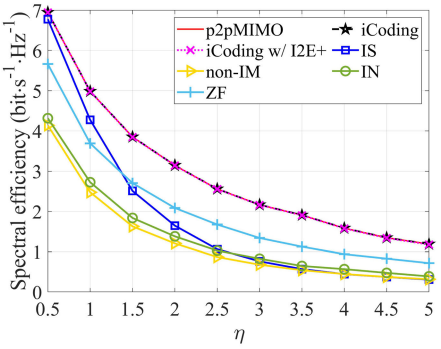
Fig. 15 shows the variation of c_0 and c_e along with η under different ζ_0s and ζ_1s. Since given ζ_0, ζ_1 can be determined

based on η, and vice versa, we plot two subfigures under $\zeta_0 \in \{-5, 0, 5\}$dB and $\zeta_1 \in \{-5, 0, 5\}$dB, respectively. Since the use of I2E+ does not affect c_0, both iCoding and iCoding with I2E+ output the same c_0, hence for simplicity we only plot iCoding's c_0 in the figure. As for c_e, since I2E+ can ensure the secrecy of transmission, c_e of iCoding with I2E+ excels that of iCoding. As Fig. 15(a) shows, since Eve is subject to the interference from MBS_1 whereas PUE_0 is free from interference due to the use of iCoding and iCoding with I2E+, clearly c_0 outperforms c_e. When $\zeta_0 = 5$dB, c_0 can be as high as 4bit/symbol, i.e., reaching the upper bound of the channel capacity of 16QAM-based transmission [26]. In addition, given fixed ζ_0, c_0 is independent of η; while under medium to high η, c_e is independent of η. This is because SNR/SINR at PUE_0 and Eve can be expressed as $\gamma_0 = \frac{\bar{P}_{T_0}}{\sigma_n^2} = 10^{0.1\zeta_0}$ and $\gamma_e = \frac{\bar{P}_{T_0}}{\bar{P}_{T_1}+\sigma_n^2} = \frac{1}{\eta+10^{-0.1\zeta_0}}$, respectively. Then, we can see from the expression of γ_0 that c_0 is independent of η and increases as ζ_0 grows. As for c_e, we can see that when η is quite small, ζ_0 dominates both γ_e and c_e, and c_e slightly increases as ζ_0 grows; while as η grows larger, η becomes dominant compared to $10^{-0.1\zeta_0}$ in calculating γ_e, so that c_e becomes less dependent on the variation of ζ_0. Moreover, since iCoding and iCoding with I2E+ can realize I2E, Eve's eavesdropping is further destroyed, incurring c_e as low as 0.25bit/symbol, i.e., the lower bound of the channel capacity of 16QAM-based transmission. Under very small η, the probability that I2E is lost under iCoding is non-negligible, yielding a slightly better c_e than 0.25bit/symbol; as a comparison, iCoding with I2E+ can ensure that the transmitted data differs from the desired one, hence its c_e is lower/better than iCoding's. Moreover, iCoding with I2E+ outputs the same c_e under various ζ_0. This is because by employing I2E+, we can guarantee that the transmitted iCoded data is different from the desired one in regardless of the value of ζ_0.

Fig. 15(b) plots the variation of c_0 and c_e along with η under different ζ_1s. Since both iCoding and iCoding with I2E+ can yield the same c_0, we only plot one curve for simplicity. Given fixed ζ_1, c_0 is shown to decrease as η grows; while for c_e, it decreases with an increase of η when η is low and becomes invariant under medium to high η. This is because SNR/SINR at PUE_0 and Eve can be computed as $\gamma_0 = \frac{\bar{P}_{T_0}}{\sigma_n^2} = \frac{10^{0.1\zeta_1}}{\eta}$ and $\gamma_e = \frac{\bar{P}_{T_0}}{\bar{P}_{T_1}+\sigma_n^2} = \frac{1}{\eta(1+10^{-0.1\zeta_1})}$, respectively. Then, one can see from the expression of γ_0 that c_0 is in inverse proportional to η, so that γ_0 and c_0 reduce as η grows. Given fixed η, since higher ζ_1 yields larger $10^{0.1\zeta_1}$, c_0 enhances as ζ_1 grows. c_e decreases as ζ_1 grows under fixed and small η. This is because when η is quite small, η can dominate and yield a large γ_e, making c_e slightly higher than 0.25bit/symbol, and decreases as γ_e declines (or ζ_1 increases) under $\eta < 1$. As η grows larger, interference deteriorates the eavesdropper so badly that a c_e as small as 0.25bit/symbol (i.e., the lower bound of 16QAM-based channel capacity) is yielded (following Eq. (16)). Therefore, given $\eta > 1$, c_e becomes constant and does not vary with ζ_1. Since iCoding with I2E+ can ensure the secrecy of legitimate transmission, it outputs lower/better c_e than iCoding, especially under small ζ_1 and



(a) $\zeta_1 = 0$dB.



(b) $\zeta_1 = 10$dB.

Fig. 16. PUE_0's SE vs. η with various IM schemes under different ζ_1s.

η. Moreover, iCoding with I2E+ outputs the same c_e under various ζ_1. This is because by employing I2E+, the transmitted iCoded data is different from the desired data with probability 1 no matter what value ζ_1 is taken.

Fig. 16 plots the variation of PUE_0's average spectral efficiency (SE) along with η under $\zeta_1 \in \{0, 10\}$dB and different IM schemes. Although iCoding with I2E+ incurs power cost for AI, since such power cost is negligible, iCoding with I2E+ yields almost the same SE as iCoding. Given fixed ζ_1, $\bar{P}_{T_0}$ decreases as η grows, hence decreasing PUE_0's SE. Since both iCoding (iCoding with I2E+) and p2pMIMO realize interference-free data reception at PUE_0, they can achieve the highest SE. In Fig. 16(a), we set $\zeta_1 = 0$dB, the strength of interference is weak relative to noise. In such a case, noise dominates the SE performance, so that the contribution of IM to SE is limited, incurring ZF and IN be inferior to non-IM. In Fig. 16(b), ζ_1 is set to be 10dB, the strength of interference is relatively stronger than that of the noise. So, IM can contribute more to PUE_0's SE, yielding SE of IS, IN and ZF reception higher than that of non-IM. Moreover, given fixed η, $\zeta_1 = 10$dB yields higher $\bar{P}_{T_0}$ than $\zeta_1 = 0$dB does, hence SE performance with various methods in Fig. 16(b) outperforms that in Fig. 16(a). When η is small, IS outperforms ZF. This is because ZF reception incurs more desired signal's power loss while nullifying interference at PUE_0; for IS, only the effective portion of interference imposing on the desired transmission of PUE_0 is mitigated, thus decreasing IM cost and preserving the performance of intended transmission. As η grows larger, $\bar{P}_{T_1}$ becomes strong relative to $\bar{P}_{T_0}$, thus ZF can mitigate more interference with the same desired signal's power loss,

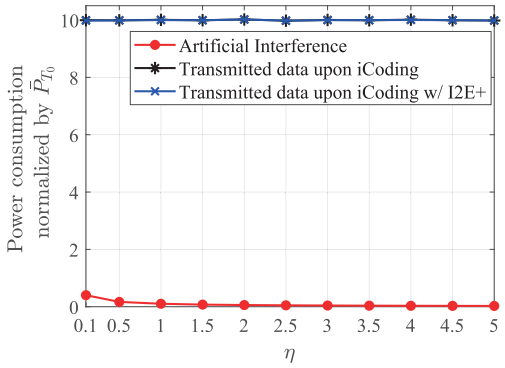


Fig. 17. Power consumption for AI and transmitted data obtained under iCoding and iCoding with I2E+ vs. η.

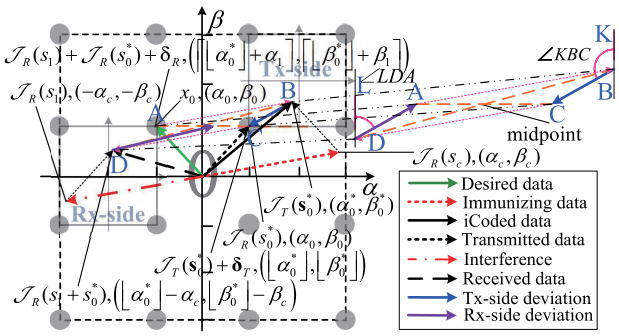


Fig. 18. Proof of Theorem 2 in a square-16QAM without constellation extension.

whereas for IS, more transmit power at PBS_0 is consumed for generating the steering signal. Hence, ZF outperforms IS as η increases. Compared to IS, iCoding does not incur transmit power cost at PBS_0, thus outperforming IS in PUE_0's SE. Compared to ZF reception, iCoding does not incur any desired signal's power loss, and hence yielding higher SE.

Fig. 17 plots the variation of average power consumption normalized by $\bar{P}_{T_0}$, for AI and transmitted data obtained using iCoding and iCoding with I2E+, along with η. As the figure shows, the power used for transmitting the iCoded data with iCoding is statistically the same as that under iCoding with I2E+, which confirms the transmitted data of iCoding and iCoding with I2E+ shares the same power consumption. Moreover, both methods' average power curves remain unchanged regardless of the variation of η. This is because although iCoding and iCoding with I2E+ may output data symbol in an extended constellation, the 8-shaped mapping can convert the symbol to the original constellation, thus yielding constant average power consumption as η varies. In addition, the power cost of AI decreases as η grows and approaches zero as η gets large enough, as explained in the following analysis. When η is small, the interference is relatively weak compared to the desired transmission, resulting in a high probability of I2E loss. This triggers the activation of I2E+, which incurs additional power cost for generating AI. As η grows, interference becomes strong enough to enable iCoding to produce data that differs from the original desired data with high probability, leading to the deactivation of I2E+ and resulting in no additional power cost for AI. However, there remains a non-zero probability that the iCoded data is identical to the desired data even when interference is strong. In such cases, I2E+ is used, resulting in some power overhead. It is worth noting that the power required for sending AI is relatively small compared to the power used for data transmission, which facilitates the use of I2E+.

VII. Conclusion

In this paper, we proposed a novel method, called *immunizing coding* (iCoding), to achieve IM and physical-layer security simultaneously. By exploiting both CSI and data information carried in the interference, an iCoded signal is generated and sent by the legitimate/desired Tx. Such a signal interacts with the interference at the intended Rx and can mitigate the effect of disturbance, hence achieving interference-free desired transmission. Moreover, since the iCoded data differs from the original desired data, the eavesdropper cannot access legitimate information via wiretapping the desired signal, achieving immunity to eavesdropping. Our theoretical analysis and numerical evaluation have shown that the proposed scheme can effectively improve a legitimate user's transmission efficiency and secrecy.

Appendix A
Proof of Theorem

Here we will present the proof of Theorem 2 under square-16QAM without and with constellation extension. Before delving into details, we first provide two Properties as follows.

Property 1: Both $\lceil \chi+\gamma \rceil = \chi+\lceil \gamma \rceil$ and $\lfloor \chi+\gamma \rfloor = \chi+\lfloor \gamma \rfloor$ hold where χ is a real integer and γ is an arbitrary real number.

Property 2: 8-shaped mapping operation satisfies:

$$\mathcal{R}_8(\omega) = \omega - D \cdot \text{Rd}(\frac{\omega}{D}) = \begin{cases} \omega - D, & \omega \in [\frac{D}{2}, \frac{3D}{2}) \\ \omega + D, & \omega \in (-\frac{3D}{2}, -\frac{D}{2}] \end{cases} \tag{17}$$

where ω is an arbitrary real number.

A. Proof of Theorem 2 Without Constellation Extension

We use Fig. 18 to illustrate the proof of Theorem 2. As the figure shows, at the Tx-side, the iCoded data $\mathcal{J}_T(\mathbf{s}_0^*)$ (point B) is not at standard constellation point, so that a deviation vector $\boldsymbol{\delta}_T$ is introduced to approximate $\mathcal{J}_T(\mathbf{s}_0^*)$ to its nearby standard constellation point $\mathcal{J}_T(\mathbf{s}_0^*) + \boldsymbol{\delta}_T$ (point C) according to ML criterion. For clarity, we define a temporary coordinate system whose origin is at the center of the square determined by the four closest standard constellation points surrounding $\mathcal{J}_T(\mathbf{s}_0^*)$. This way, $\mathcal{J}_T(\mathbf{s}_0^*)$ lies in the third quadrant of the temporary coordinate system, then $\mathcal{J}_T(\mathbf{s}_0^*) + \boldsymbol{\delta}_T$'s, i.e., point C's, coordinate can be expressed as $(\lfloor \alpha_0^* \rfloor, \lfloor \beta_0^* \rfloor)$.

At the Rx-side, the received data $\mathcal{J}_R(s_1 + \tilde{s}_0^*)$ (point D) is not at the standard constellation point, so we need to apply ML again to approximate it to a nearby standard constellation point (point A). We connect points A, B, C and D to form a quadrilateral which has two diagonals $\overline{BD}$ and $\overline{AC}$. Then, the coordinates of the midpoints of line segments $\overline{BD}$

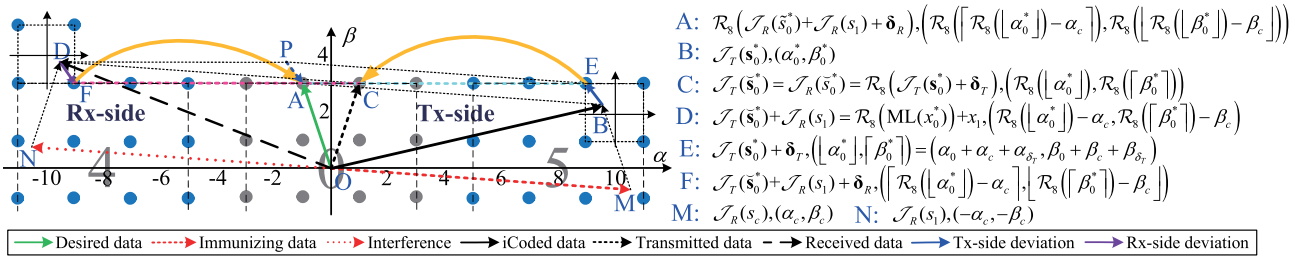


Fig. 19. Proof of Theorem 2 in a square-16QAM with constellation extension.

and $\overline{AC}$ can be represented by $\left(\frac{\alpha_0^*+\lfloor\alpha_0^*\rfloor-\alpha_c}{2}, \frac{\beta_0^*+\lfloor\beta_0^*\rfloor-\beta_c}{2}\right)$ and $(\frac{\lfloor\alpha_0^*\rfloor+\lceil\lfloor\alpha_0^*\rfloor+\alpha_1\rceil}{2}, \frac{\lfloor\beta_0^*\rfloor+\lceil\lfloor\beta_0^*\rfloor+\beta_1\rceil}{2})$, respectively. Since $\alpha_0^* = \alpha_0 + \alpha_c$ and $\beta_0^* = \beta_0 + \beta_c$ hold, the midpoint of line segment $\overline{BD}$ can be rewritten as $\left(\frac{\alpha_0+\lfloor\alpha_0^*\rfloor}{2}, \frac{\beta_0+\lfloor\beta_0^*\rfloor}{2}\right)$. Moreover, as the coordinates of x_0, i.e., α_0 and β_0, are integers, by applying Property 1 to α_0^* and β_0^*, we get $\lfloor\alpha_0^*\rfloor = \lfloor\alpha_0+\alpha_c\rfloor = \alpha_0 + \lfloor\alpha_c\rfloor$ and $\lfloor\beta_0^*\rfloor = \lfloor\beta_0+\beta_c\rfloor = \beta_0 + \lfloor\beta_c\rfloor$, so that the midpoint of $\overline{AC}$ can be rewritten as $(\frac{\lfloor\alpha_0^*\rfloor+\lceil\alpha_0+\lfloor\alpha_c\rfloor+\alpha_1\rceil}{2}, \frac{\lfloor\beta_0^*\rfloor+\lceil\alpha_0+\lfloor\beta_c\rfloor+\beta_1\rceil}{2})$, which can be further simplified to $(\frac{\lfloor\alpha_0^*\rfloor+\alpha_0+\lfloor\alpha_c\rfloor+\lceil\alpha_1\rceil}{2}, \frac{\lfloor\beta_0^*\rfloor+\alpha_0+\lfloor\beta_c\rfloor+\lceil\beta_1\rceil}{2})$. According to the design principle of immunizing data x_c, we have $\alpha_c = -\alpha_1$ and $\beta_c = -\beta_1$; therefore, $\lfloor\alpha_c\rfloor + \lceil\alpha_1\rceil = 0$ and $\lfloor\alpha_c\rfloor + \lceil\alpha_1\rceil = 0$ hold and $\overline{AC}$'s midpoint can be finally expressed as $\left(\frac{\alpha_0+\lfloor\alpha_0^*\rfloor}{2}, \frac{\beta_0+\lfloor\beta_0^*\rfloor}{2}\right)$ which is identical to $\overline{BD}$'s midpoint. Thus, we proved ABCD to be a parallelogram.

From the above discussion, we know that the Tx-side deviation vector $\boldsymbol{\delta}_T$ (i.e., vector $\overrightarrow{BC}$) has the same length as the Rx-side deviation vector $\boldsymbol{\delta}_R$ (i.e., vector $\overrightarrow{DA}$). Moreover, the phase angles of $\boldsymbol{\delta}_T$ and $\boldsymbol{\delta}_R$ representing by $\angle KBC$ and $\angle LDA$, respectively, satisfy $\angle KBC + \angle LDA = \pi$. That is, $\boldsymbol{\delta}_T$ and $\boldsymbol{\delta}_R$ are of the opposite directions.

Based on the above analysis, $\boldsymbol{\delta}_T = -\boldsymbol{\delta}_R$ holds. Therefore, Theorem 2 follows. ■

B. Proof of Theorem 2 With Constellation Extension

We now prove Theorem 2 in an extended constellation as shown in Fig. 19. Due to space limitations, we will only present the proof in terms of the x-coordinate, while omitting the proof for y-coordinate.

As the figure shows the x-coordinate of $\mathcal{J}_T(\mathbf{s}_0^*) + \boldsymbol{\delta}_T$ (point E) can be expressed as α_E. Since in this example, the iCoded data (point B) lies in the #4 extended constellation, we apply the 8-shaped mapping to obtain the transmitted data $\mathcal{J}_T(\breve{\mathbf{s}}_0^*)$ (point C) whose x-coordinate $(\breve{\alpha}_0^*)$ can be computed by substituting the coordinate of $\mathcal{J}_T(\mathbf{s}_0^*)+\boldsymbol{\delta}_T$ into Eq. (10) as:

$$\breve{\alpha}_0^* = \alpha_E - D \cdot \mathrm{Rd}(\frac{\alpha_E}{D}). \tag{18}$$

At the Rx-side, the received data $\mathcal{J}_R(\tilde{s}_0^* + s_1)$ (point D) is not at standard constellation point, so that a deviation vector $\boldsymbol{\delta}_R$ is required to approximate it to a standard constellation point $\mathcal{J}_R(\tilde{s}_0^* + s_1) + \boldsymbol{\delta}_R$ (point F) following the ML criterion. Then, by applying inverse mapping to $\mathcal{J}_R(\tilde{s}_0^*+s_1)+\boldsymbol{\delta}_R$, $\mathcal{J}_R(\hat{s}_0)$ (point A) in the original constellation is yielded. $\mathcal{J}_R(\hat{s}_0)$'s x-coordinate $\hat{\alpha}_0$ can be calculated according to Eq. (19) below:

$$\begin{aligned}\hat{\alpha}_0 = \alpha_E - D \cdot \mathrm{Rd}\left(\frac{\alpha_E}{D}\right) + \alpha_1 + \alpha_{\delta_R} \\ - D \cdot \mathrm{Rd}\left[\frac{\alpha_E - D \cdot \mathrm{Rd}\left(\frac{\alpha_E}{D}\right) + \alpha_1 + \alpha_{\delta_R}}{D}\right]\end{aligned} \tag{19}$$

where α_{δ_R} and α_1 represent the x-coordinates of $\boldsymbol{\delta}_R$ and $\mathcal{J}_R(s_1)$, respectively.

We simplify Eq. (19) as:

$$\hat{\alpha}_0 = \alpha_E + \alpha_1 + \alpha_{\delta_R} - D \cdot \mathrm{Rd}\left(\frac{\alpha_E + \alpha_1 + \alpha_{\delta_R}}{D}\right). \tag{20}$$

Recall that $\alpha_c + \alpha_1 = 0$, and x_0 is a standard point in the original constellation, we can have $\mathrm{Rd}\left(\frac{\alpha_0}{D}\right) = 0$. Then, as long as $\alpha_{\delta_T} + \alpha_{\delta_R} = 0$, $\hat{\alpha}_0 = \alpha_0$ can hold; that is, $\mathcal{J}_R(\hat{s}_0) = \mathcal{J}_R(s_0) = x_0$ is satisfied, indicating the correct decoding at the intended Rx. In what follows, we will verify $\alpha_{\delta_T} + \alpha_{\delta_R} = 0$.

According to the discussion in subsection A, we have known that EBAP can form a parallelogram, thus vectors $\overrightarrow{BE}$ (i.e., $\boldsymbol{\delta}_T$) and $\overrightarrow{PA}$ have the same amplitude and opposite directions. In order to prove $\boldsymbol{\delta}_R = -\boldsymbol{\delta}_T$, we need to verify $\overrightarrow{PA} = \overrightarrow{DF}$ where $\overrightarrow{DF}$ is $\boldsymbol{\delta}_R$. We draw auxiliary lines $\overline{EA}$ and $\overline{CF}$ in Fig. 19, then the proof of $\overrightarrow{PA} = \overrightarrow{DF}$ can be equivalent to the verification of congruence of triangles ΔEAP and ΔCFD.

As plotted in Fig. 19, $\overrightarrow{EP}$ has the same amplitude and opposite direction w.r.t. the immunizing data vector $\overrightarrow{AB}$, while $\overrightarrow{CD}$ has the same amplitude and phase as the interference vector $\overrightarrow{ON}$. Since $\overrightarrow{AB} = \overrightarrow{OM}$ and $\overrightarrow{AB} = -\overrightarrow{EP}$ hold; base on the design principle of iCoding. i.e., $\mathcal{J}_R(s_1) = -\mathcal{J}_R(s_c)$ or equivalently $\overrightarrow{ON} = -\overrightarrow{OM}$, we can get $\overrightarrow{EP} = \overrightarrow{ON}$ and $\overrightarrow{EP} = \overrightarrow{CD}$.

Next, we prove $\overrightarrow{EA} = \overrightarrow{CF}$. We can write the x-coordinates of $\mathcal{J}_T(\mathbf{s}_0^*) + \boldsymbol{\delta}_T$ (point E) and $\mathcal{R}_8\left(\mathcal{J}_R(\tilde{s}_0^* + s_1) + \boldsymbol{\delta}_R\right)$ (point A) as $\lfloor\alpha_0^*\rfloor$ and $\mathcal{R}_8\left(\lceil\mathcal{R}_8\left(\lfloor\alpha_0^*\rfloor\right) - \alpha_c\rceil\right)$, respectively. Then, $\overrightarrow{EA}$ can be expressed by Eq. (21):

$$\mathrm{Re}\left(\overrightarrow{EA}\right) = \left(\lfloor\alpha_0^*\rfloor - \left(\mathcal{R}_8\lceil\mathcal{R}_8\left(\lfloor\alpha_0^*\rfloor\right) - \alpha_c\rceil\right)\right. . \tag{21}$$

Similarly, $\overrightarrow{CF}$ can be represented by points C's and F's coordinates as Eq. (22):

$$\begin{aligned}\mathrm{Re}\left(\overrightarrow{CF}\right) &= \mathcal{R}_8\left(\mathcal{J}_T(\breve{\mathbf{s}}_0^*) + \boldsymbol{\delta}_T\right) - \left(\mathcal{J}_T(\breve{\mathbf{s}}_0^*) + \mathcal{J}_R(s_1) + \boldsymbol{\delta}_R\right) \\ &= \mathcal{R}_8\left(\lfloor\alpha_0^*\rfloor\right) - \lceil\mathcal{R}_8\left(\lfloor\alpha_0^*\rfloor\right) - \alpha_c\rceil.\end{aligned} \tag{22}$$

Then, we prove the $x-$coordinate of $\overrightarrow{EA}$ is identical to that of $\overrightarrow{CF}$. First, we apply Property 1 to $\alpha_0^* = \alpha_0+\alpha_c$ and can have $\lfloor\alpha_0^*\rfloor = \alpha_0+\lfloor\alpha_c\rfloor$. Then, by substituting $\lfloor\alpha_0^*\rfloor = \alpha_0+\lfloor\alpha_c\rfloor$ into Eq. (21), we can simplify the expression of its $x-$coordinate as:

$$\begin{aligned}&\lfloor\alpha_0^*\rfloor - \mathcal{R}_8\left(\lceil\mathcal{R}_8\left(\lfloor\alpha_0^*\rfloor\right) - \alpha_c\rceil\right)\\ =&\alpha_0 + \lfloor\alpha_c\rfloor - \mathcal{R}_8\left(\lceil\mathcal{R}_8(\alpha_0 + \lfloor\alpha_c\rfloor) - \alpha_c\rceil\right).\end{aligned} \tag{23}$$

Since the iCoded data lies in the 1^{st} round extended constellation and its $x-$coordinate is positive as shown in Fig. 19, $\alpha_0 + \lfloor\alpha_c\rfloor \in [\frac{D}{2}, \frac{3D}{2})$ holds. Otherwise, if the iCoded data's $x-$coordinate is negative, $\alpha_0 + \lfloor\alpha_c\rfloor \in [-\frac{3D}{2}, -\frac{D}{2})$ is yielded. Then, we can apply Property 2 to Eq. (23) and get:

$$\begin{aligned}&\lfloor\alpha_0^*\rfloor - \mathcal{R}_8\left(\lceil\mathcal{R}_8\left(\lfloor\alpha_0^*\rfloor\right) - \alpha_c\rceil\right)\\ =&\alpha_0 + \lfloor\alpha_c\rfloor - \mathcal{R}_8\left(\lceil\alpha_0 + \lfloor\alpha_c\rfloor - \alpha_c - D\rceil\right).\end{aligned} \tag{24}$$

Moreover, as $\lfloor\alpha_c\rfloor-\alpha_c \in (-1, 0)$ and $\alpha_0 \in [-\frac{D}{2}+1, \frac{D}{2}-1]$ (i.e., the desired data x_0 lies in the original constellation), we can have $\alpha_0 + \lfloor\alpha_c\rfloor - \alpha_c - D \in (-\frac{3D}{2}, -\frac{D}{2} - 1)$. Then, $\lceil\alpha_0 + \lfloor\alpha_c\rfloor - \alpha_c - D\rceil \in [-\frac{3D}{2} + 1, -\frac{D}{2}]$ holds. Since $[-\frac{3D}{2} + 1, -\frac{D}{2}] \in (-\frac{3D}{2}, -\frac{D}{2}]$, by applying Property 2 to $\mathcal{R}_8\left(\lceil\alpha_0 + \lfloor\alpha_c\rfloor - \alpha_c - D\rceil\right)$, we can further simplify Eq. (24) as:

$$\begin{aligned}&\lfloor\alpha_0^*\rfloor - \mathcal{R}_8\left(\lceil\alpha_0 + \lfloor\alpha_c\rfloor - \alpha_c - D\rceil\right)\\ =&\alpha_0 + \lfloor\alpha_c\rfloor - \left(\lceil\alpha_0 + \lfloor\alpha_c\rfloor - \alpha_c - D\rceil + D\right).\end{aligned} \tag{25}$$

This way, since $\lfloor\alpha_0^*\rfloor = \lfloor\alpha_0+\alpha_c\rfloor \in [\frac{D}{2}, \frac{3D}{2})$ holds, we can rewrite the expression of $\overrightarrow{CF}$'s $x-$coordinate in Eq. (22) as:

$$\begin{aligned}&\mathcal{R}_8(\lfloor\alpha_0^*\rfloor) - \left(\lceil\mathcal{R}_8\left(\lfloor\alpha_0^*\rfloor\right) - \alpha_c\rceil\right)\\ =&\alpha_0 + \lfloor\alpha_c\rfloor - D - \left(\lceil\alpha_0 + \lfloor\alpha_c\rfloor - \alpha_c - D\rceil\right).\end{aligned} \tag{26}$$

By comparing Eqs. (25) and (26), we can verify that $\overrightarrow{EA}$ and $\overrightarrow{CF}$ have the same $x-$coordinate. Similarly, we can also prove these two vectors' $y-$coordinates are the same.

Upon the proof of $\overrightarrow{EP} = \overrightarrow{CD}$, $\overrightarrow{EA} = \overrightarrow{CF}$, i.e., vectors on both sides of the equations have the same amplitude and phase features, we can easily get $\angle DCF = \angle PEA$. So, ΔEAP and ΔCFD are congruent triangles. Therefore, $\overrightarrow{DF} = \overrightarrow{PA}$ holds. Since $\overrightarrow{PA}$ has the same amplitude and opposite direction w.r.t. $\overrightarrow{BE}$, we have $\overrightarrow{DF} = -\overrightarrow{BE}$, i.e., $\boldsymbol{\delta}_R = -\boldsymbol{\delta}_T$. Thus, Theorem 2 under constellation extension follows.

Based on subsections A and B, the proof of Theorem 2 is done. ■

REFERENCES

[1] Z. Li, J. Ding, X. Dai, K. G. Shin, and J. Liu, "Exploiting interactions among signals to decode interfering transmissions with fewer receiving antennas," *Comput. Commun.*, vol. 136, pp. 63–75, Feb. 2019.

[2] P. Angueira et al., "A survey of physical layer techniques for secure wireless communications in industry," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 810–838, 2nd Quart., 2022.

[3] L. Hu et al., "Interference alignment for physical layer security in multi-user networks with passive eavesdroppers," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 3692–3705, 2023.

[4] A. Goldsmith, "On the optimality of multiantenna broadcast scheduling using zero-forcing beamforming," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 3, pp. 528–541, Mar. 2006.

[5] A. Ghasemi, A. S. Motahari, and A. K. Khandani, "Interference alignment for the K-user MIMO interference channel," *IEEE Trans. Inf. Theory*, vol. 68, no. 3, pp. 1401–1411, Mar. 2022.

[6] V. Ntranos, M. A. Maddah-Ali, and G. Caire, "Cellular interference alignment," *IEEE Trans. Inf. Theory*, vol. 61, no. 3, pp. 1194–1217, Mar. 2015.

[7] Z. Li, J. Chen, L. Zhen, S. Cui, K. G. Shin, and J. Liu, "Coordinated multi-point transmissions based on interference alignment and neutralization," *IEEE Trans. Wireless Commun.*, vol. 18, no. 7, pp. 3347–3365, Jul. 2019.

[8] Z. Li, K. G. Shin, and L. Zhen, "When and how much to neutralize interference?" in *Proc. IEEE INFOCOM Conf. Comput. Commun.*, May 2017, pp. 1–9.

[9] Z. Li, Y. Liu, K. G. Shin, J. Li, F. Guo, and J. Liu, "Design and adaptation of multi-interference steering," *IEEE Trans. Wireless Commun.*, vol. 18, no. 7, pp. 3329–3346, Jul. 2019.

[10] Z. Li, Y. Liu, K. G. Shin, J. Liu, and Z. Yan, "Interference steering to manage interference in IoT," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10458–10471, Dec. 2019.

[11] J. Zhang, S. Rajendran, Z. Sun, R. Woods, and L. Hanzo, "Physical layer security for the Internet of Things: Authentication and key generation," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 92–98, Oct. 2019.

[12] S. Fang, I. Markwood, and Y. Liu, "Wireless-assisted key establishment leveraging channel manipulation," *IEEE Trans. Mobile Comput.*, vol. 20, no. 1, pp. 263–275, Jan. 2021.

[13] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. VTC–Fall. IEEE 62nd Veh. Technol. Conf.*, vol. 3, Oct. 2005, pp. 1906–1910.

[14] S. Fang, T. Wang, Y. Liu, S. Zhao, and Z. Lu, "Entrapment for wireless eavesdroppers," in *Proc. IEEE INFOCOM Conf. Comput. Commun.*, Apr. 2019, pp. 2530–2538.

[15] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[16] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1202–1216, Mar. 2011.

[17] N. Zhao, F. R. Yu, M. Li, and V. C. M. Leung, "Anti-eavesdropping schemes for interference alignment (IA)-based wireless networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5719–5732, Aug. 2016.

[18] N. Zhao et al., "Caching UAV assisted secure transmission in hyper-dense networks based on interference alignment," *IEEE Trans. Commun.*, vol. 66, no. 5, pp. 2281–2294, May 2018.

[19] Z. Ding, M. Peng, and H.-H. Chen, "A general relaying transmission protocol for MIMO secrecy communications," *IEEE Trans. Commun.*, vol. 60, no. 11, pp. 3461–3471, Nov. 2012.

[20] T. Quek, D. Guillaume, and I. Guvenc, *Small Cell Networks: Deployment, PHY Technologies, and Resource Management*. Cambridge, U.K.: Cambridge Univ. Press, 2013.

[21] J. Luo, F. Wang, S. Wang, H. Wang, and D. Wang, "Reconfigurable intelligent surface: Reflection design against passive eavesdropping," *IEEE Trans. Wireless Commun.*, vol. 20, no. 5, pp. 3350–3364, May 2021.

[22] G. S. Park and H. Song, "Cooperative base station caching and X2 link traffic offloading system for video streaming over SDN-enabled 5G networks," *IEEE Trans. Mobile Comput.*, vol. 18, no. 9, pp. 2005–2019, Sep. 2019.

[23] C. Song, "Leakage rate analysis for artificial noise assisted massive MIMO with non-coherent passive eavesdropper in block-fading," *IEEE Trans. Wireless Commun.*, vol. 18, no. 4, pp. 2111–2124, Apr. 2019.

[24] W. Nie, F.-C. Zheng, X. Wang, W. Zhang, and S. Jin, "User-centric cross-tier base station clustering and cooperation in heterogeneous networks: Rate improvement and energy saving," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 5, pp. 1192–1206, May 2016.

[25] V. Jungnickel et al., "Backhaul requirements for inter-site cooperation in heterogeneous LTE-advanced networks," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC)*, Jun. 2013, pp. 905–910.

[26] B. Liu et al., "Performance comparison of PS star-16QAM and PS square-shaped 16QAM (square-16QAM)," *IEEE Photon. J.*, vol. 9, no. 6, pp. 1–8, Dec. 2017.

Yicheng Liu is currently pursuing the Ph.D. degree with the School of Cyber Engineering, Xidian University. His research interests include wireless communication, physical layer security, and interference management.

Zhao Li (Member, IEEE) received the B.S. degree in telecommunications engineering and the M.S. and Ph.D. degrees in communication and information systems from Xidian University, Xi'an, China, in 2003, 2006, and 2010, respectively. He was a Visiting Scholar and then a Research Scientist with the Real-Time Computing Laboratory, Department of Electrical Engineering and Computer Science, University of Michigan, from 2013 to 2015. He is currently an Associate Professor with the School of Cyber Engineering, Xidian University. He has published over 60 technical papers at premium international journals and conferences, such as IEEE TRANSACTIONS ON MOBILE COMPUTING, IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, IEEE INTERNET OF THINGS JOURNAL, IEEE INFOCOM, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, *Computer Communications*, and *Wireless Networks*. His research interests include wireless communication, 5G communication systems, resource allocation, interference management, the IoT, and physical layer security.

Kang G. Shin (Life Fellow, IEEE) received the B.S. degree in electronics engineering from Seoul National University, Seoul, South Korea, in 1970, and the M.S. and Ph.D. degrees in electrical engineering from Cornell University, Ithaca, NY, USA, in 1976 and 1978, respectively. He is currently the Kevin and Nancy O'Connor Professor of computer science and the Founding Director of the Real-Time Computing Laboratory, Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, MI, USA. At Michigan, he has supervised the completion of 82 Ph.D. students and also chaired the Computer Science and Engineering Division for three years starting in 1991. From 1978 to 1982, he was a Faculty Member of the Rensselaer Polytechnic Institute, Troy, NY, USA. He has authored/co-authored more than 900 technical articles (more than 330 of which are published in archival journals) and more than 30 patents or invention disclosures. His current research interests include QoS-sensitive computing and networks and embedded real-time and cyber-physical systems. He is a fellow of ACM. He received numerous institutional awards and best paper awards.

Zheng Yan (Fellow, IEEE) received the B.Eng. degree in electrical engineering and the M.Eng. degree in computer science and engineering from Xi'an Jiaotong University, Xi'an, China, in 1994 and 1997, respectively, the M.Eng. degree in information security from the National University of Singapore, Singapore, in 2000, and the Lic.Sc. and D.Sc. (Tech.) degrees in electrical engineering from Helsinki University of Technology, Helsinki, Finland, in 2005 and 2007, respectively. She is currently a Distinguished Professor with Xidian University, Xi'an. She has published over 400 papers in prestigious journals and conferences worldwide, including IEEE SECURITY AND PRIVACY, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, IEEE INFOCOM, and ACM/ICCC ICSE. She is the inventor and the co-inventor of over 110 patents and 50 PCT patent applications. Her research interests include trust, security and privacy, social networking, cloud computing, networking systems, and data mining. She serves as an Executive Editor-in-Chief of Information Sciences and Area Editor/Associate Editor/Editorial Board Member of over 60 journals, including *ACM Computing Surveys, Information Fusion*, IEEE INTERNET OF THINGS JOURNAL, and IEEE *Network Magazine*. She has served as a General Chair or Program Committee Chair for over 40 international conferences and has delivered over 30 keynote and invited talks at international conferences and renowned enterprises.

Jia Liu (Senior Member, IEEE) received the B.E. degree from the School of Telecommunications Engineering, Xidian University, Xi'an, China, in 2010, and the Ph.D. degree from the School of Systems Information Science, Future University Hakodate, Hakodate, Japan, in 2016. He has published over 60 academic papers in premium international journals and conferences, such as IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, and IEEE INFOCOM. His research interests include wireless systems security, space-air-ground integrated networks, the Internet of Things, and 6G. He received the 2016 and 2020 IEEE Sapporo Section Encouragement Award.