Fundamentals of Physical Layer Anonymous Communications: Sender Detection and Anonymous Precoding

Zhongxiang Wei, *Member, IEEE,* Fan Liu, *Member, IEEE,* Christos Masouros, *Senior Member, IEEE,* and H. Vincent Poor, *Life Fellow, IEEE*

***Abstract*—In the era of big data, anonymity is recognized as an important attribute in privacy-preserving communications. The existing anonymous authentication and routing designs are applied at higher layers of networks, ignoring the fact that physical layer (PHY) also contains privacy-critical information. In this paper, we introduce the concept of PHY anonymity, and reveal that the receiver can unmask the sender's identity by only analyzing the PHY information, i.e., the signaling patterns and the characteristics of the channel. We investigate two scenarios, where the receiver has more antennas than the sender in the strong receiver case, and vice versa in the strong sender case. For each scenario, we first investigate sender detection strategies at the receiver, and then we develop anonymous precoding to address anonymity while guaranteeing high signal-to-interference-plus-noise-ratio (SINR) for communications. In particular, an interference suppression anonymous precoder is first proposed, assisted by a dedicated transmitter-side phase equalizer for removing phase ambiguity. Afterwards, a constructive interference anonymous precoder is investigated to utilize inter-antenna interference as a beneficial element without loss of the sender's anonymity. Simulations demonstrate that the anonymous precoders are able to preserve the sender's anonymity and simultaneously guarantee high SINR, opening a new dimension on PHY anonymous designs.**

***Index Terms*—Anonymous Communications, Physical Layer, Sender Detection, Anonymous Precoding, Semi-Definite Relaxation, Constructive Interference**

I. Introduction

In the era of cloud computing, storage and communications, the misuse of confidential data has attracted much attention in both commercial and military applications. Due to the inherent broadcast nature of wireless communications, threats arise from two main aspects, namely security and privacy. The aim of security is to prevent the confidential signal from being eavesdropped upon by potential adversaries. There has been extensive research on cryptography, authentication [1], covert communication [2], multiple-input and multiple-output (MIMO) beamforming plus artificial noise design [3], and cooperative jamming [4], from the upper layer to the physical layer (PHY) of networks. These extensive works enable confidential communications among the legitimate parities, while ensuring the signal is not breakable or decodable at adversaries [5]. In contrast, the aim of privacy is mask data itself or part of it, or conceal the users' identities for the intended receiver. The former line of research seeks to control information leakage, and strike a compromise between privacy and utility [6] [7] [8]. A separate line of research focuses on guaranteeing the communication quality towards legitimate parties, while concealing the identities of communication parties or the specific users' participation during the communications, also defined as anonymous communications [9].

There are three categories of anonymity, namely sender anonymity, receiver anonymity and bi-directional anonymity. Sender anonymity means the receiver cannot trace the sender's identity; receiver anonymity means the sender can contact the receiver without knowing its identity; while bi-directional anonymity means both the sender and receiver communicate without knowing each other's identities [10]. In this paper, we are interested in sender anonymity design. That is, it is required that the signal can be correctly demodulated and decoded by an access point (AP) for communication purpose, and meanwhile the users try to mask their participation against the AP's sender detection. A typical example of sender anonymity comes from remote healthcare, where patients wish to anonymously send their bio-information to APs for medical signal processing, analysis or E-recording, whereas the patients' identities must be kept unknown at the AP side. Another example arises from the upcoming vehicle-to-infrastructure communications, where vehicles report local road and traffic information to a road-side AP, and meanwhile the vehicles wish to mask their participation during the signal transmission. Otherwise, the AP may be able to use sender detection to unmask the sender, and then the location and trajectory of the vehicles.

Researchers have unveiled various ways to enhance anonymity at high layers of networks, such as anonymous authentication/encryption and anonymous routing protocols. Anonymous authentication and encryption schemes have been proposed for cellular networks [11], wireless body area networks [12], wireless local area networks [13], device-to-device (D2D) communications [14], Radio Frequency Identification

Zhongxiang Wei is with the College of Electronic and Information Engineering, Tongji University, Shanghai, China. Email: z_wei@tongji.edu.cn

Fan Liu (corresponding author) is with the Department of Electical and Electronic Engineering, Southern University of Science and Technology, Shenzhen, China. Email: liuf6@sustech.edu.cn

Christos Masouros is with the Department of Electronic and Electrical Engineering at the University College London, London, UK. Email: c.masouros@ucl.ac.uk

H. Vincent Poor is with the Department of Electrical and Computer Engineering, Princeton University, Princeton, NJ 08544 USA (e-mail: poor@princeton.edu).

This work was supported in part by the Engineering and Physical Sciences Research Council under project EP/R007934/1, and in part by the U.S. National Science Foundation under Grant CCF-1908308.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2021.3093722, IEEE Transactions on Wireless Communications

[15], vehicle-to-infrastructure communications [16] and prototype design [17]. The design principle is to use group signature, ring signature [18], or anonymous account index [12] for authentication and encryption. Since the users' real IDs are not exposed during the authentication and encryption processes, potential adversaries are unable to leverage the users' real IDs to unmask the communication participants. Note that while the existing PHY location verification and identity authentication techniques [19] leverage the physical properties of the wireless medium as a source of domain-specific information to complement security mechanisms, they aim at preventing legitimate transceivers from being spoofed/attacked by external eavesdroppers. Since they do not provide anonymity for legitimate communication parties, they fall within the set of traditional PHY security rather than anonymity solutions. On the other hand, a great deal of efforts have been invested in designing anonymous routing for the Internet and ad hoc networks [20] [21]. The fundamental is to preserve the privacy of end hosts as well as routing paths by a number of encrypted layers, where routers serve as proxies and any intermediate nodes are unaware of where the source and sink of the message are located. Note that private information retrieval techniques allow a user to retrieve an element of a database without the owner of that database being able to determine which element was selected. Nevertheless, the target of private information retrieval is to make the data anonymous, but not to make the communication participants anonymous [22]. Random privacy mapping is used to perturb the users' real data locally, before it is transmitted to the receiver. The randomness generated by the mapping mechanism introduces a trade-off between privacy protection and data accuracy, which is further extended into trading-off privacy and other measures of utility. Nevertheless, the aim of privacy mapping is not to mask the participation of the communication users, and thus is not among set of anonymity techniques [7].

There are still issues left to be addressed by the existing anonymizing techniques. First, since existing anonymous authentication and encryption schemes are generally designated based on public-key encryption, asymmetric encryption, identity-based encryption, fully homomorphic encryption, cryptographic primitive, etc., they generally require additional key distribution, agreement and maintenance processes, which may be restrictive in many emerging scenarios of 5G-beyond networks due to the high computational requirement and latency. Although smaller key sizes have been proposed based on elliptic curve cryptosystems, the users still need extra computation to verify the certificates of others, and a pool of certificates is generally required for the certification authority for maintaining keys. Second, the existing anonymous routing protocols are only applicable for large-scale networks, where cooperative agents are involved to guarantee anonymity. Hence, none of the agents could be offline during the underlying process, and it is also vulnerable to internal malicious attacks that can easily break the anonymity. Third, existing anonymizing techniques and associated protocols are employed at the upper layers of networks, assuming PHY provides a privacy-preserving link. In fact, the PHY also contains information that can be used to extract the nodes' identities. When an anonymously authenticated/encrypted sender transmits a signal via its wireless channel, the recipient can analyze the signaling patterns based on the characteristics of channel fading, and then is able to unmask the origin of the received signal at the PHY directly. Thus, privacy threats start from the acquisition of data, which necessitates complementary privacy techniques that reside at the PHY.

Motivated by the aforementioned open challenges, in this paper, we present a first attempt to exploit PHY sender detection schemes and their counterpart anonymous precoding techniques. Our contributions are summarized as follows.

1) This is the first work to unveil that PHY information, i.e., the signaling pattern and the inherent characteristics of channel fading, can be judiciously analyzed to unmask senders' identities and this incurs an unprecedented vulnerability by anonymity-violating behavior at the receiver. Focusing on different antenna configurations, we further propose two novel sender detection strategies that only exploit the PHY information to break the sender's anonymity. For the strong receiver case where the number of receive antennas is larger than the transmit antenna of the sender, a maximum likelihood estimation (MLE) based sender detector is proposed. While in the strong sender case with the reduced receive degrees-of-freedom (DoF) in detection, we further propose a maximum norm (M-Norm) based sender detector, with lower computational complexity than the MLE based detector.
2) For both antenna configurations, a series of corresponding anonymous PHY precoding techniques is proposed against the sender detection schemes. We first propose an interference suppression based anonymous (ISA) precoder that maximizes per-antenna SINR performance while simultaneously addressing the sender's anonymity, assisted by a dedicated transmitter-side phase equalization design for eliminating phase ambiguity. We also prove that the applied semi-definite relaxation (SDR) in optimization is tight and the optimality of the precoder is always maintained.
3) Then, we further propose a constructive-interference (CI) based anonymous (CIA) precoder, which is able to utilize inter-antenna interference as a beneficial element for further enhancing receiver quality without loss of the sender's anonymity. Importantly, the CI based anonymous precoder enables multiplexing more data streams than the number of transmit antennas, and hence is also applicable to the strong receiver case.

Our study also reveals a number important properties of the anonymous precoding designs.

1) As discussed in Section IV-A, the receiver may not correctly unmask the real sender as its detection is jammed by the anonymous precoder. Hence, the conventional receiver-side equalizer that relies on acknowledging the correct propagation channel becomes inapplicable. As a result, sender anonymity is achieved at the cost of reduced receiver SINR.
2) Since receiver-side phase equalization, typically em-

© 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

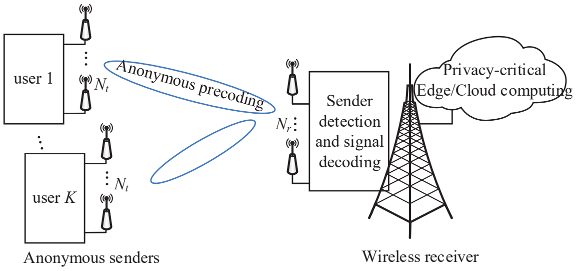


Fig. 1. Illustration of system model, where K users transmit data to the receiver with QoS and sender's anonymity requirements.

ployed in classical optimization-based precoders, becomes inapplicable in anonymous communications, transmitter-side phase equalization is essential for correct demodulation at the receiver.

3) As reflected by the optimization problems P1-P3, introducing additional anonymity constraints inevitably reduces DoF in the precoding design, which further reduces the value of the receiver SINR. Hence, the two aims of optimizing quality-of-service (QoS) and preserving PHY layer anonymity are conflicting and therefore there exists a non-trivial trade-off between improving receiver SINR quality and guaranteeing sender anonymity.

Notation: Matrices and vectors are represented by boldface capital and lower case letters, respectively. $|\cdot|$ denotes the absolute value of a complex number. $||\cdot||$ denotes the Euclidean norm. $\boldsymbol{A}^T$, $\boldsymbol{A}^H$ and $\mathrm{Tr}(\boldsymbol{A})$ denote the transpose, Hermitian transpose and trace of a matrix $\boldsymbol{A}$. $\mathrm{Rank}(\boldsymbol{A})$ denotes the rank of a matrix $\boldsymbol{A}$. $\boldsymbol{A} \succeq 0$ means $\boldsymbol{A}$ is a positive semi-definite matrix. $\Re$ and $\Im$ denote the real and imaginary parts of a complex variable. $\boldsymbol{I}_n$ means an n-by-n identity matrix.

II. System Model and Anonymity Performance Metrics

In this section, the system model and anonymity performance metric are presented in subsections II-A and II-B, respectively.

A. System Model

We consider an uplink multiuser MIMO system depicted in Fig. 1, and in particular a sender anonymity scenario, where users anonymously transmit data to an AP receiver without leaking their identities. Assume the user set $\mathbb{K}$ consists of K users ($|\mathbb{K}| = K$), and there is one user communicating (denote $\mathbb{S}$ as the sender) with the receiver at each time slot in a time-division-multiple-access (TDMA) fashion. In the training phase, all the active users send pilot signals to the AP and channel estimation is performed at the receiver side; then the channel state information (CSI) is fed back to the users for use in precoding design, as that in generic MIMO communications. It is important to note however that this conventional CSI estimation process does not jeopardize the anonymity aims of our work. Indeed, during channel estimation the AP can collect all the IDs and map these to the CSI estimated for all the users in its cell. Nevertheless, the aim of our work is to obstruct the AP, that has all users' IDs, from mapping the data received to the correct user ID and CSI. Accordingly, even though the AP has a set of the users' IDs, it cannot recognize the ID that the data was sent from, thus maintaining anonymity. Multiuser access control can be performed among the users in either a contested or non-contested manner without notifying the AP. In particular, via the contested manner, the users access the channel based on particular sensing or back-off strategies [23], which has been widely used in ad-hoc networks and cognitive radios. While, via the non-contested manner, the users can coordinate by themselves for channel access, where time slots are scheduled to avoid channel access collisions [24]. It is important to note however, that during access control in a multiuser access scenario, the uplink users could potentially share their sender IDs in a group manner, without obstructing the anonymous communication advocated in this paper. That is, the AP can have knowledge of all the users' IDs in its cell, but still, through the anonymous precoding proposed here the AP cannot correctly map the received data to a sender ID therefore maintaining anonymity of the transmitted data. The receiver is equipped with N_r receive antennas, while each user is equipped with N_t transmit antennas. Define $\boldsymbol{H}_k \in \mathbb{C}^{N_r \times N_t}$ as the MIMO channel between the user k and receiver, $\forall k \in K$. Define $\boldsymbol{W}_k$ as the precoding matrix and $\boldsymbol{s}_k$ as the symbol vector to be transmitted by the k-th user. The received signal at the receiver is written as

$$\boldsymbol{y} = \boldsymbol{H}_k \boldsymbol{W}_k \boldsymbol{s}_k + \boldsymbol{n}, \tag{1}$$

where $\boldsymbol{n} \in \mathbb{C}^{N_r \times 1}$ denotes the circularly symmetric complex Gaussian (CSCG) noise at the receiver, and its r-th element follows $[\boldsymbol{n}]_r \sim \mathcal{CN}(0, \sigma^2)$, $\forall r \in N_r$.

B. Performance Metric of Anonymity

Higher layer anonymity is typically quantified by an entropy based metric [25]. It is because the entropy exactly measures the uncertainty of a system, and a larger value of anonymity entropy contains more possibilities, where the receiver is not able to explicitly estimate which user is the real sender. Considering the set $\mathbb{K}$, let p_k denote the probability that the receiver estimates the k-th user as the real sender. Hence, the anonymity entropy can be calculated as $\mathcal{A}(\mathbb{K}) = -\sum_{k\in\mathbb{K}} p_k \log_2 p_k$, where the maximum anonymity entropy $\mathcal{A}_{\max}(\mathbb{K}) = \log_2(K)$ is achieved when $p_k = \frac{1}{K}, \forall k \in \mathbb{K}$, i.e., the users are equally likely senders. Detection error rate (DER) is another metric to measure anonymity. Without loss of generality, assuming multiuser access and sender detection are operated at the block level, the DER is then defined as the percentage of blocks whose origins are mis-detected relative to the total number of blocks received in a transmission period, written as $\mathrm{DER} = \frac{N_{B,mis}}{N_{B,tot}}$, where $N_{B,mis}$ denotes the numbers of the blocks that their origin is mis-detected, and $N_{B,tot}$ denotes the total number of received blocks. As suggested above, the sender detection strategy (denoted as $\mathcal{D}$) for the receiver is to estimate the real sender k as the one with the highest probability p_k of being the sender, i.e.,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2021.3093722, IEEE Transactions on Wireless Communications

$\mathcal{D}^* = \underset{k \in \mathbb{K}}{\operatorname{argmax}}\, p_k$. On the other hand, a favorable sender's anonymity-preserving design at the user is to deteriorate the sender detection performance, while guaranteeing reasonable receiver quality for communication signal. In the following, we will first reveal the sender detection design at the receiver in Section III, and then the anonymous design at the sender is designed in Section IV.

III. Sender Detection Strategy

In this section, we study the sender detection schemes at the receiver. Since the receiver only analyzes the PHY information, i.e., the received signal and the inherent characteristics of the wireless channels to disclose the identity of the sender, under the TDMA premise the sender detection can be formulated as a multiple hypotheses testing (MHT) problem

$$\boldsymbol{Y} = \begin{cases} \mathcal{H}_0: & \boldsymbol{n}, \\ \mathcal{H}_1: & \boldsymbol{H}_1 \boldsymbol{W}_1 \boldsymbol{s}_1 + \boldsymbol{n}, \\ & \vdots \\ \mathcal{H}_K: & \boldsymbol{H}_K \boldsymbol{W}_K \boldsymbol{s}_K + \boldsymbol{n}, \end{cases} \tag{2}$$

where the hypothesis $\mathcal{H}_0$ means no data is transmitted from the user set $\mathbb{K}$ and only noise appears at the receiver. In comparison, hypothesis $\mathcal{H}_k$ means there is a signal coming from the k-th sender. Hence, the receiver attempts to detect the correct hypothesis from the $1+K$ MHT candidates. Apparently, to handle the MHT problem, the receiver can first detect whether the hypothesis $\mathcal{H}_0$ is true or false, and only turns to detect the origin of the signal (the hypotheses $\mathcal{H}_1$ to $\mathcal{H}_K$) when $\mathcal{H}_0$ is decided as a false hypothesis.

The detection of $\mathcal{H}_0$ leads to the classic energy detection that has been extensively researched in the context of cognitive radios [26] [27], which is briefly discussed for the sake of completeness. Based on the received signal $\boldsymbol{y}$, the test statistic for the energy detector is given by $\mathcal{T}(\boldsymbol{y}) = \frac{1}{N_r}\sum_{n=1}^{N_r} ||\boldsymbol{y}(n)||^2 = \frac{||\boldsymbol{y}||^2}{N_r}$. Under hypothesis $\mathcal{H}_0$, the test statistic $\mathcal{T}(\boldsymbol{y})$ follows chi-square distribution with $2N_r$ DoF. Define the probability of false alarm as the probability of the receiver falsely declaring the presence of an incoming signal. Assuming a detection threshold β, the probability of false alarm is given by $\mathrm{P_{FA}}(\beta|\mathcal{H}_0) = \Pr(\mathcal{T}(\boldsymbol{y}) > \beta|\mathcal{H}_0) = \int_{\beta}^{\infty} \psi_{(2N_r)}(x)\, \mathrm{d}x$, where $\psi_{(2N_r)}(x)$ denotes the probability density function (pdf) of a chi-square random variable with $2N_r$ DoF. It can be further written in the form of $\mathrm{P_{FA}}(\beta|\mathcal{H}_0) = 1 - F_{(2N_r)}(\frac{2\beta N_r}{\sigma^2})$, where $F_{(2N_r)}(\cdot)$ denotes the cumulative distribution function (cdf) of a chi-square random variable with $2N_r$ DoF. Note that there is a multitude of advanced detection schemes, such as eigenvalue-based detection [27] and feature detection [28]. Since energy detection has been extensively researched and is not our main contribution, we refer readers to [27] [28] for details. Once the receiver has sensed the presence of an incoming signal, it turns to detect the origin of the received signal, and we have the following Remark 3.1 for the sender detector design at the PHY.

Remark 3.1: The detection of the user's identity in the TDMA scenario is equivalent to the identification of the propagation channel (which is also the unique and unchangeable PHY identity of the user) from the received signal. Hence, the receiver is able to utilize the characteristics of the MIMO channel to disclose the sender. □

Since the characteristics of the MIMO channel (i.e., the dimension and transmit/receive diversity) depend on the configurations of N_r and N_t, in the following we consider the strong receiver ($N_r > N_t$) and strong sender ($N_r \leq N_t$) cases and design specific detector for each.

A. The Case of a Strong Receiver ($N_r > N_t$)

This configuration is a common scenario at uplink transmission since an AP or base station is normally equipped with more antennas than a user. Recalling the MHT in (2), since the receiver has sensed the received signal $\boldsymbol{y}$ and has the knowledge of CSI set $\boldsymbol{H}_k, \forall k \in \mathbb{K}$, it is easy for the receiver to apply the maximum likelihood estimation (MLE) to disclose the estimate of the transmitted vector $\boldsymbol{x}_k = \boldsymbol{W}_k \boldsymbol{s}_k \in \mathbb{C}^{N_t \times 1}$ as

$$\hat{\boldsymbol{x}}_k = \boldsymbol{H}_k^{\dagger} \boldsymbol{y} = \boldsymbol{W}_k \boldsymbol{s}_k + \boldsymbol{H}_k^{\dagger} \boldsymbol{n}, \tag{3}$$

where $\boldsymbol{H}_k^{\dagger} = (\boldsymbol{H}_k^H \boldsymbol{H}_k)^{-1} \boldsymbol{H}_k^H$ denotes the pseudo-inverse of the channel $\boldsymbol{H}_k$. Then, the estimated vector $\hat{\boldsymbol{x}}_k$ is multiplied by $\boldsymbol{H}_k$ to imitate that it propagates through $\boldsymbol{H}_k$, and a re-constructed signal $\hat{\boldsymbol{y}}_k$ is obtained as $\hat{\boldsymbol{y}}_k = \boldsymbol{H}_k \hat{\boldsymbol{x}}_k = \boldsymbol{H}_k \boldsymbol{W}_k \boldsymbol{s}_k + \boldsymbol{H}_k \boldsymbol{H}_k^{\dagger} \boldsymbol{n}$. Note that, if the received signal indeed comes from the k-th user (which propagates through the channel $\boldsymbol{H}_k$), there is a high probability that the re-constructed signal $\hat{\boldsymbol{y}}_k$ built on $\boldsymbol{H}_k$ leads to the smallest Euclidean distance to the actual received signal $\boldsymbol{y}$, i.e., $||\boldsymbol{y} - \hat{\boldsymbol{y}}_k||^2 = \min_{j \in \mathbb{K}} ||\boldsymbol{y} - \hat{\boldsymbol{y}}_j||^2$. Inspired by the above observations, the sender detection strategy can be interpreted form the perspective of the generalized likelihood ratio test (GLRT) [29], written as

$$\begin{aligned} &\mathrm{P}(\boldsymbol{Y}|\mathcal{H}_1) = \frac{\exp\{-\frac{1}{2\sigma^2}(\boldsymbol{y} - \hat{\boldsymbol{y}}_1)^H (\boldsymbol{y} - \hat{\boldsymbol{y}}_1)\}}{\sigma\sqrt{2\pi^{N_r}}}, \\ &\vdots \\ &\mathrm{P}(\boldsymbol{Y}|\mathcal{H}_K) = \frac{\exp\{-\frac{1}{2\sigma^2}(\boldsymbol{y} - \hat{\boldsymbol{y}}_K)^H (\boldsymbol{y} - \hat{\boldsymbol{y}}_K)\}}{\sigma\sqrt{2\pi^{N_r}}}, \end{aligned} \tag{4}$$

where the hypothesis with the highest probability (the maximal likelihood) will be considered as the real sender. Since the likelihood function in (4) is primarily determined by its numerator, where a smaller value of $(\boldsymbol{y} - \hat{\boldsymbol{y}}_k)^H (\boldsymbol{y} - \hat{\boldsymbol{y}}_k)$ leads to a larger value of the likelihood function. Hence, finding the minimal value of $||\boldsymbol{y} - \boldsymbol{H}_k \boldsymbol{H}_k^{\dagger} \boldsymbol{y}||^2 = ||(\boldsymbol{I}_{N_r} - \boldsymbol{H}_k \boldsymbol{H}_k^{\dagger})\boldsymbol{y}||^2$ among all the candidates yields the MLE-based detection strategy as

$$\begin{aligned} &\mathcal{D}^*_{\mathrm{MLE}} = \\ &\underset{k \in \mathbb{K}}{\operatorname{argmin}} \{||(\boldsymbol{I}_{N_r} - \boldsymbol{H}_1 \boldsymbol{H}_1^{\dagger})\boldsymbol{y}||^2, ..., ||(\boldsymbol{I}_{N_r} - \boldsymbol{H}_K \boldsymbol{H}_K^{\dagger})\boldsymbol{y}||^2\}, \end{aligned} \tag{5}$$

where $\boldsymbol{I}_{N_r} - \boldsymbol{H}_k \boldsymbol{H}_k^{\dagger}$ denotes the equivalent detector. Note that $\boldsymbol{H}_k \boldsymbol{H}_k^{\dagger} \neq \boldsymbol{I}_{N_r}$ in strong receiver case with $N_r > N_t$.

B. The Case of a Strong Sender ($N_r \leq N_t$)

In the case of a strong sender, the detection DoFs at the receiver are reduced. The multiplication of matrices $\boldsymbol{H}_k^H \boldsymbol{H}_k$

© 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

is rank-insufficient and thus the detector in (5) becomes infeasible. A possible solution is to employ the well-known minimum mean square error (MMSE) estimator to estimate $\hat{\boldsymbol{x}}_k$, where the sender detector becomes $\left|\left|\left(\boldsymbol{I}_{N_r} - \boldsymbol{H}_k(\boldsymbol{H}_k^H\boldsymbol{H}_k + \frac{\sigma^2 N_t}{p}\boldsymbol{I}_{N_t})^{-1}\boldsymbol{H}_k^H\right)\boldsymbol{y}\right|\right|$ with p denoting the transmission power at the sender. Since the term $\frac{\sigma^2 N_t}{p}\boldsymbol{I}_{N_t}$ adds regularization effect for the matrix inverse operation, it makes the detector still feasible for the $N_r \leq N_t$ configuration. Nevertheless, for the MMSE based detector, the receiver needs the knowledge of the instantaneous transmission power p at the sender, which could be difficult in practice and also the sender can simply keep varying its power to deteriorate the receiver's detection performance. Hence, a more practical detection strategy is required for the strong sender case. In this section, we alternatively propose a maximum norm (M-Norm) based detector, as detailed below.

Starting from the fact that the norm of $\boldsymbol{H}_k^H\boldsymbol{H}_k$ is more likely to be larger than the norm of $\boldsymbol{H}_j^H\boldsymbol{H}_k$, $\forall j \neq k, j \in \mathbb{K}$, it is safe to conclude that with high probability it holds that $||\boldsymbol{H}_k^H\boldsymbol{H}_k\boldsymbol{W}_k\boldsymbol{s}_k||^2 \geq ||\boldsymbol{H}_j^H\boldsymbol{H}_k\boldsymbol{W}_k\boldsymbol{s}_k||^2$. Since the term $\boldsymbol{H}_k\boldsymbol{W}_k\boldsymbol{s}_k$ is the received signal excluding noise, it is intuitive to multiply the received signal $\boldsymbol{y}$ with different $\boldsymbol{H}_j^H$ and calculate the norm of $\boldsymbol{H}_j^H\boldsymbol{y}$, $\forall j \in \mathbb{K}$. If the signal indeed comes from the channel $\boldsymbol{H}_k$, the resulting norm has a high probability of presenting the largest among all the candidates. Finally for the strong sender case, we reach a so-called M-Norm based sender detector as

$$\mathcal{D}^*_{\mathrm{M-Norm}} : \underset{k\in\mathbb{K}}{\operatorname{argmax}}\{||\boldsymbol{H}_1^H\boldsymbol{y}||^2, ..., ||\boldsymbol{H}_K^H\boldsymbol{y}||^2\}. \tag{6}$$

C. Type-k Error Probability Analysis

Define type-k error probability as the probability of, under hypothesis $\mathcal{H}_k$, the receiver falsely declaring either that no one sends, or that a user other than user k sends. For the M-Norm detector, its type-k error probability can be written as $\mathrm{P}_{\mathrm{type-k}}(\mathcal{H}_k) = \Pr(\mathcal{T}(\boldsymbol{y}) < \beta|\mathcal{H}_k) + \sum_{j,j\neq k}^{K}\Pr(\mathcal{T}(\boldsymbol{y}) > \beta|\mathcal{H}_k)\Pr(||\boldsymbol{H}_k^H\boldsymbol{y}||^2 \leq ||\boldsymbol{H}_j^H\boldsymbol{y}||^2|\mathcal{H}_k)$. Without loss of generality, we still assume the k-th user as the real sender and $\boldsymbol{x}_k$ as the transmitted vector. The first term equals to $\mathcal{F}_{(2N_r, 2||\boldsymbol{H}_k\boldsymbol{x}_k||^2/\sigma^2)}(\frac{2\beta N_r}{\sigma^2})$, which is the cdf of a non-central chi-square random variable with $2N_r$ DoF and non-centrality parameter $2||\boldsymbol{H}_k\boldsymbol{x}_k||^2/\sigma^2$. Now, we turn to the term $\Pr(||\boldsymbol{H}_k^H\boldsymbol{y}||^2 \leq ||\boldsymbol{H}_j^H\boldsymbol{y}||^2|\mathcal{H}_k)$. We first compute the value of $||\boldsymbol{H}_j^H\boldsymbol{y}||^2$. The received signal $\boldsymbol{y} = [y_1, y_2, \ldots, y_{Nr}]$ is a multi-dimensional Gaussian vector, distributed as $\boldsymbol{y} \sim \mathcal{CN}(\boldsymbol{u}, \boldsymbol{\Sigma})$. Define $\boldsymbol{c} = \boldsymbol{\Sigma}^{\frac{-1}{2}}\boldsymbol{y}$. Then $\boldsymbol{z} = \boldsymbol{c} - \boldsymbol{\Sigma}^{\frac{-1}{2}}\boldsymbol{u}$ has $\boldsymbol{0}$ mean and identity covariance matrix. Now the matrix $\boldsymbol{y}^H\boldsymbol{H}_j^H\boldsymbol{H}_j\boldsymbol{y} = (\boldsymbol{z}+\boldsymbol{\Sigma}^{\frac{-1}{2}}\boldsymbol{u})^H\boldsymbol{\Sigma}^{\frac{1}{2}}\boldsymbol{H}_j^H\boldsymbol{H}_j\boldsymbol{\Sigma}^{\frac{1}{2}}(\boldsymbol{z}+\boldsymbol{\Sigma}^{\frac{-1}{2}}\boldsymbol{u})$. We use the spectral theorem and write $\boldsymbol{\Sigma}^{\frac{1}{2}}\boldsymbol{H}_j^H\boldsymbol{H}_j\boldsymbol{\Sigma}^{\frac{1}{2}} = \boldsymbol{P}_j^H\boldsymbol{\Lambda}\boldsymbol{P}_j$, where $\boldsymbol{P}_j$ is an orthogonal matrix (so that $\boldsymbol{P}_j^H\boldsymbol{P}_j = \boldsymbol{P}_j\boldsymbol{P}_j^H = \boldsymbol{I}$) and $\boldsymbol{\Lambda}_j$ is diagonal with positive elements $\lambda_{j,1}, ..., \lambda_{j,N_r})$. Write $\boldsymbol{u}_j = \boldsymbol{P}_j\boldsymbol{z}$ so that $\boldsymbol{u}_j$ is a multivariate Gaussian vector with identity co-variance matrix and mean $\boldsymbol{0}$. It is easy to obtain that $\boldsymbol{y}^H\boldsymbol{H}_j^H\boldsymbol{H}_j\boldsymbol{y} = (\boldsymbol{u}_j + \boldsymbol{b}_j)^H\boldsymbol{\Lambda}_j(\boldsymbol{u}_j + \boldsymbol{b}_j) = \sum_{n=1}^{N_r}\lambda_{j,n}(u_{j,n}+b_{j,n})^2$, where $\boldsymbol{b}_j = \boldsymbol{P}_j\boldsymbol{\Sigma}^{\frac{-1}{2}}\boldsymbol{u}_j$. $u_{j,n}$ and $b_{j,n}$ are the n-th elements of $\boldsymbol{u}_j$ and $\boldsymbol{b}_j$, respectively. Indeed, this means the $\boldsymbol{y}^H\boldsymbol{H}_j^H\boldsymbol{H}_j\boldsymbol{y}$ is a linear combination of non-central chi-square variables. Similarly, it is easy to obtain $||\boldsymbol{H}_k^H\boldsymbol{y}||^2 = \sum_{n=1}^{N_r}\lambda_{k,n}(u_{j,n} + b_{j,n})^2$, where $\boldsymbol{\Sigma}^{\frac{1}{2}}\boldsymbol{H}_k^H\boldsymbol{H}_k\boldsymbol{\Sigma}^{\frac{1}{2}} = \boldsymbol{P}_k^H\boldsymbol{\Lambda}_k\boldsymbol{P}_k$ and $\boldsymbol{b}_k = \boldsymbol{P}_k\boldsymbol{\Sigma}^{\frac{-1}{2}}\boldsymbol{u}_k$. Now the type-$k$ error probability can be written as $\mathrm{P}_{\mathrm{type-k}}(\mathcal{H}_k) = \mathcal{F}_{(2N_r, 2||\boldsymbol{H}_k\boldsymbol{x}_k||^2/\sigma^2)}(\frac{2\beta N_r}{\sigma^2}) + (1 - \mathcal{F}_{(2N_r, 2||\boldsymbol{H}_k\boldsymbol{x}_k||^2/\sigma^2)}(\frac{2\beta N_r}{\sigma^2}))\sum_{j\neq k}^{K}\Pr(\lambda_{j,n}(u_{j,n} + b_{j,n})^2 \geq \lambda_{k,n}(u_{k,n} + b_{k,n})^2)$. The type-$k$ error probability of the MLE-based detector can be similarly obtained; details are omitted due to space limitations.

D. Complexity Analysis of the Sender Detection Schemes

Now we calculate the complexities of the detectors. For the MLE based detector, its complexity is dominated by generating the pseudo-inverse matrices of the different MIMO channels. A pseudo-inverse matrix can be obtained by the singular value decomposition (SVD) approach or Cholesky decomposition [30], which have been shown to offer similar complexity results, and the complexity is calculated as $16N_r^2N_t + 24N_rN_t^2 + 29N_t^3$. Afterwards, it reconstructs the estimated version of the received signal and calculates the Euclidean distance to the real received signal $\boldsymbol{y}$, whose complexity is $8N_rN_t + 8N_r$. Hence, the overall complexity of the MLE based detector is computed as $K(16N_r^2N_t + 24N_rN_t^2 + 29N_t^3 + 8N_rN_t + 8N_r)$. On the other hand, the M-Norm based detector multiplies the received signal with the different $\boldsymbol{H}_j^H$ and compares the norm of $\boldsymbol{H}_j^H\boldsymbol{y}$ in sequence. Its overall complexity is given as $K(8N_tN_r + 8N_t)$, which is evidently lower than that of the MLE based detector.

IV. Anonymous Precoding Design

In section III, we have presented two novel sender detectors that analyze the received signal together with the characteristics of MIMO channel to unmask the sender. In this section, on the contrary we investigate anonymous precoder design at the sender end, which judiciously manipulates the pattern of the received signal to inhibit the receiver's detection. Again, we investigate anonymous precoding designs for strong receiver and strong sender cases, respectively.

A. Anonymous Precoder for a Strong Sender Case ($N_r \leq N_t$)

Since the aim of sender anonymity is to guarantee receiver quality for communications and meanwhile to conceal the sender's identity, a reasonable anonymous precoder needs to strike a good trade-off between these two metrics. Before we give problem formulation, we first present Proposition 4.1 for the anonymous precoding design.

Proposition 4.1: Implementing sender's anonymity conflicts with the design of receiver-side equalizer. Since receiver-side equalizer is not applicable in anonymous communications, anonymity is achieved at the cost of the reduced receiver SINR quality. □

Proposition 4.1 can be proved by a counter example. If the receive performance can be enhanced by a channel equalizer at the receiver, no anonymity can be achieved as the equalizer is built on acknowledging the real sender's MIMO channel. On the other hand, if anonymity is maintained and the identity of

This article has been accepted for publication in IEEE Transactions on Wireless Communications. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TWC.2021.3093722

the sender is concealed, the receiver fails to know the exact channel that the signal comes from, further indicating that a correct equalizer would be impossible. Since the receiver's equalizer design conflicts with the anonymity requirement, Proposition 4.1 essentially indicates that we need to treat each receive antenna as an individual receiver and impose per-antenna SINR constraint for multiplexing streams. In the following, two anonymous precoders are proposed for the strong sender case, respectively.

1) Interference-suppression based anonymous (ISA) Precoder: Without loss of generality, assume the k-th user as the sender $\mathbb{S}$ at uplink. For ease of expression, we simply write $\boldsymbol{s}$ as the intended symbol vector and $\boldsymbol{W}$ as the associated precoder matrix. Since at most N_r streams can be multiplexed in the strong sender case, we have $\boldsymbol{s} \in \mathbb{C}^{N_r \times 1}$ and $\boldsymbol{W} \in \mathbb{C}^{N_t \times N_r}$. As revealed by Proposition 4.1, each receive antenna is treated as an individual receiver, and thus we assume the i-th receive antenna's desired symbol as s_i from the vector $\boldsymbol{s}$, $\forall i \in N_r$. Denote $\boldsymbol{q}_i \in \mathbb{C}^{N_t \times 1}$ as the i-th column of a precoding matrix $\boldsymbol{W}$ (i.e., $\boldsymbol{W} = [\boldsymbol{q}_1, ..., \boldsymbol{q}_{N_r}]$), which corresponds to the precoder vector for the symbol s_i. Denote $\boldsymbol{h}_i \in \mathbb{C}^{1 \times N_t}$ as the channel between the i-th receive antenna and sender (i.e., $\boldsymbol{H}_k = [\boldsymbol{h}_1^T, ..., \boldsymbol{h}_{N_r}^T]^T$). To scramble the proposed M-Norm detector in section III, the anonymous precoder should guarantee the norm of $\boldsymbol{H}_k^H \boldsymbol{y}$ small enough to combat the norm test. Since the exact value of the receive noise is not known by the sender, we can alternatively suppress the value of $||\boldsymbol{H}_k^H \boldsymbol{H}_k \boldsymbol{W}||^2$, which has the same effect of manipulating the norm of $||\boldsymbol{H}_k^H \boldsymbol{y}||^2$ and guarantees the real sender hiding in the user set $\mathbb{K}$. Now, we are able to present problem formulation, where we aim to maximize the minimal per-antenna SINR threshold Γ under the power budget and anonymity constraints, such as

$$\begin{aligned} \text{P1}: &\max_{\boldsymbol{W}=[\boldsymbol{q}_1,\cdots,\boldsymbol{q}_{N_r}]} \Gamma, \\ \text{s.t. } &(\text{C1}): \frac{||\boldsymbol{h}_i \boldsymbol{q}_i||^2}{\sigma^2 + \sum_{i'=1,i'\neq i}^{N_r} ||\boldsymbol{h}_i \boldsymbol{q}_{i'}||^2} \geq \Gamma, \forall i \in N_r, \\ &(\text{C2}): \sum_{i=1}^{N_r} ||\boldsymbol{q}_i||^2 \leq p_{\max}, \\ &(\text{C3}): ||\boldsymbol{H}_k^H \boldsymbol{H}_k [\boldsymbol{q}_1, ..., \boldsymbol{q}_{N_r}]||^2 \leq \epsilon, \end{aligned} \tag{7}$$

where (C1) denotes that the per-antenna SINR should be higher than the lower-bound Γ, which is the objective to be optimized. It is also observed that each receive antenna is impaired by inter-antenna interference, which acts as multi-user interference in multiple-input and single-output (MISO) systems. Constraint (C2) guarantees the dissipated transmission power lower than a budget $p_{\max}$. Constraint (C3) suppresses the norm to be lower than a threshold ϵ to scramble the sender detector at the receiver.

The optimization P1 belongs the class of non-convex second-order cone programming (SOCP), where the coupling of the objective Γ and inter-antenna interference makes the optimization intractable. However, it is straightforward to show that the inequality power constraint (C2) will be achieved with equality at the optimum. Otherwise, if there is power left, we can simply increase the transmission power to further improve the value of Γ under constraint (C3), thus contradicting optimality [31]. Hence, we begin with the dual power minimization problem as

$$\begin{aligned} \text{P1(a)}: \min \;& f_{\Gamma^{(j)}}([\boldsymbol{q}_1, ..., \boldsymbol{q}_{N_r}]) \triangleq \sum_{i=1}^{N_r} ||\boldsymbol{q}_i||^2 \\ \text{s.t. } (\text{C4}): &\frac{||\boldsymbol{h}_i \boldsymbol{q}_i||^2}{\sigma^2 + \sum_{i'=1,i'\neq i}^{N_r} ||\boldsymbol{h}_i \boldsymbol{q}_{i'}||^2} \geq \Gamma^{(t)}, \forall i \in N_r, \\ (\text{C5}): &||\boldsymbol{H}_k^H \boldsymbol{H}_k [\boldsymbol{q}_1, ..., \boldsymbol{q}_{N_r}]||^2 \leq \epsilon, \end{aligned} \tag{8}$$

where $\Gamma^{(t)}$ serves as the per-antenna minimum SINR requirement and superscript t denotes the index of iteration as detailed later. Let $f^*_{\Gamma^{(t)}}$ represent the optimal value of P1(a) with minimum SINR requirement $\Gamma^{(t)}$. In fact, solving P1 with (C2) upper bounded by $f^*_{\Gamma^{(t)}}$ yields an optimal objective value of $\Gamma^{(t)}$. Furthermore, the optimal objective values of problems P1(a) and P1 are strictly monotonic increasing. Therefore, considering $\Gamma^{(t)}$ as a variable of optimization, the optimal solution of P1 can be obtained by alternatively solving P1(a) for a given $\Gamma^{(t)}$ and searching over different $\Gamma^{(t)}$. Since P1(a) is still a non-convex SOCP problem, we define $\boldsymbol{Q}_i = \boldsymbol{q}_i \boldsymbol{q}_i^H \in \mathbb{C}^{N_t \times N_t}, \forall i \in N_r$, and transform P1(a) into a semi-definite programming (SDP) as

$$\begin{aligned} \text{P1(b)}: \;& \min \sum_{i=1}^{N_r} \text{Tr}(\boldsymbol{Q}_i) \\ \text{s.t. } &(\tilde{C4}): \text{Tr}(\boldsymbol{h}_i \boldsymbol{Q}_i \boldsymbol{h}_i^H) - \\ &\qquad \Gamma^{(t)}(\sigma^2 + \sum_{i'=1,i'\neq i}^{N_r} \text{Tr}(\boldsymbol{h}_i \boldsymbol{Q}_{i'} \boldsymbol{h}_i^H)) \geq 0, \forall i \in N_r, \\ &(\tilde{C5}): \text{Tr}(\boldsymbol{H}_k^H \boldsymbol{H}_k (\sum_{i=1}^{N_r} \boldsymbol{Q}_i) \boldsymbol{H}_k \boldsymbol{H}_k^H) \leq \epsilon, \\ &(\text{C6}): \boldsymbol{Q}_i \succeq \boldsymbol{0}, \forall i \in N_r, (\text{C7}): \text{Rank}(\boldsymbol{Q}_i) = 1, \forall i \in N_r, \end{aligned} \tag{9}$$

where $(\tilde{C4})$ and $(\tilde{C5})$ are linear matrix inequalities (LMI)s transformed from (C4) and (C5). (C6) and (C7) are the SDR version of $\boldsymbol{Q}_i = \boldsymbol{q}_i \boldsymbol{q}_i^H$, $\forall i \in N_r$. Neglecting the rank-one constraint (C7), the problem P1(b) is defined as a "separable SDP" (SSDP) problem [32], which can be readily solved by convex optimization solvers. Hence, the procedure starts with an initial value of $\Gamma^{(t)}$, and we solve P1(b) to obtain the $\boldsymbol{Q}_i^*$, $\forall i \in N_r$. If the consumed power, i.e., $\sum_{i=1}^{N_r} \text{Tr}(\boldsymbol{Q}_i)$, is smaller than the budget p_{max}, we can increase the value of $\Gamma^{(t)}$, otherwise decrease the value of $\Gamma^{(t)}$. The iteration is operated until convergence, as summarized in Algorithm 1. After performing Algorithm 1, a non-trivial question is whether the obtained optimal solution $\boldsymbol{Q}_i^*$ is of rank 1. Apparently, if it is, then the SDR relaxation is tight and the optimal beamformer $\boldsymbol{q}_i^*$ can be simply obtained from the principal eigen-vector of $\boldsymbol{Q}_i^*$. Regarding the rank of the optimal solution $\boldsymbol{Q}_i^*$, $\forall i \in N_r$, we then have the following Proposition 4.2.

Proposition 4.2: Under the condition of independently distributed MIMO channels, the optimal solution of P1(b) satisfies $\text{Rank}(\boldsymbol{Q}_i) = 1, \forall i \in N_r$, with probability one. □

Proof: Please refer to APPENDIX A. ■

© 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

Algorithm 1 The Equivalence between non-convex SOCP P1 and convex SDP P1(b)

```
Input: MIMO channel $\boldsymbol{H}_k$, power budget $p_{\max}$, symbol vector $\boldsymbol{s}$,
    initial left bound $\Gamma_l$, right bound $\Gamma_r$, anonymity threshold $\epsilon$, and
    tolerance $\tau$.
1: Initialize $\Gamma^{(t)} = (\Gamma_l + \Gamma_r)/2$.
2: while $|\Gamma_r - \Gamma_l| \geq \tau$ do
3:     Solve P1(b) with $\Gamma^{(t)}$. Let $f^*_{\Gamma^{(t)}} = \sum_{i=1}^{N_r} \mathrm{Tr}(\boldsymbol{Q}_i)$. Calculate
       the power reward factor $R = p_{\max} - f^*_{\Gamma^{(t)}}$.
4:     if $R \geq 0$ then
5:         update $\Gamma_l = \Gamma^{(t)}$, else update $\Gamma_r = \Gamma^{(t)}$.
6:     end if
7:     Update the iteration index $t = t + 1$; Update $\Gamma^{(t)} = \frac{\Gamma_l + \Gamma_r}{2}$.
8: end while
Output: Optimal SDP matrices $\boldsymbol{Q}^*_i$, $\forall i \in N_r$.
```

It is interesting that when the channels happen to be not independently distributed (e.g., in the case of line-of-sight or channel correlation), the tightness of the SDRs can still be guaranteed in P1(b) by applying the rank reduction results in [33], as summarized in Proposition 4.3.

Proposition 4.3: Consider a SSDP [33] such as

$$
\begin{aligned}
&(\text{SSDP}):\ \min_{\boldsymbol{X}_1,\ldots,\boldsymbol{X}_L} \sum_{l=1}^{L} \mathrm{Tr}(\boldsymbol{B}_l \boldsymbol{X}_l) \\
&\text{s.t.} \sum_{l=1}^{L} \mathrm{Tr}(\boldsymbol{A}_{ul}\boldsymbol{X}_l) \trianglerighteq_u b_u, u = 1, \ldots, U, \text{and } \boldsymbol{X}_l \succeq \boldsymbol{0}, l = 1, \ldots, L,
\end{aligned}
\tag{10}
$$

where $\boldsymbol{B}_l$ and $\boldsymbol{A}_{ul}$, $\forall l \in L, \forall u \in U$, are Hermitian matrices (but not necessarily positive semi-definite). $b_u \in \mathbb{R}$ and $\trianglerighteq_u \in \{\leq, \geq, =\}$ $\forall u \in U$. Suppose that the SSDP is feasible and bounded, and the optimal value is attained. There always exists an optimal solution $(\boldsymbol{X}^*_1, \ldots, \boldsymbol{X}^*_L)$ such that $\sum_{l=1}^{L} \mathrm{Rank}^2(\boldsymbol{X}^*_l) \leq U$ [33]. □

By applying this result in our context, it can be verified that $\sum_{1}^{N_r} \mathrm{Rank}^2(\boldsymbol{Q}^*_i) \leq N_r + 1$. Also, it is evident from the per-antenna SINR constraint that $\mathrm{Rank}(\boldsymbol{Q}^*_i) \neq 0$, denoting that $\mathrm{Rank}(\boldsymbol{Q}^*_i) \geq 1$, $\forall i \in N_r$. Hence, it is safe to include that there still exists a rank-1 solution such as $\mathrm{Rank}(\boldsymbol{Q}^*_i) = 1$, $\forall i \in N_r$, which makes the SDRs of the Algorithm 1 still tight. That is, if the obtained optimal result $\boldsymbol{Q}^*_i$ happens to have a high rank, the rank-reduction techniques in [33] can be applied to obtain rank-one solutions.

Now the tightness of the SDRs has been confirmed by Propositions 4.2 and 4.3. Nevertheless, while the receiver SINR and sender's anonymity can always be guaranteed, the received signal propagating through the equivalent channel $\boldsymbol{H}_k\boldsymbol{W}$ may have phase ambiguity, which impairs the demodulation at the receiver. A conventional method is to adopt receiver side phase equalization to align the phase of the received signal with the desired symbol. However, since the sender's identity is concealed by the anonymous precoder and the receiver may not be able to declare a correct channel, the conventional receiver side phase equalization is disabled in anonymous communications. To this end, we further propose Proposition 4.4 for a novel transmit phase equalization.

Proposition 4.4: With the optimal precoder $\boldsymbol{q}^*_i$ for the intended symbol s_i, the desired signal at the i-th receive antenna is calculated as $\boldsymbol{h}_i\boldsymbol{q}^*_i s_i$, which should have the same phase to that of the desired symbol s_i for de-modulation purpose. Write $\boldsymbol{h}_i\boldsymbol{q}^*_i = |\boldsymbol{h}_i\boldsymbol{q}^*_i| e^{j\varphi_i}$, where φ_i denotes the angle of the complex number $\boldsymbol{h}_i\boldsymbol{q}^*_i$. Thus, the transmit phase equalization is given as $\boldsymbol{q}^*_i = \boldsymbol{q}^*_i e^{-j\varphi_i}$, which makes the desired signal have exactly same phase to the desired symbol s_i to avoid phase ambiguity without violating anonymity and per-antenna SINR performance. □

Proof: Recalling (C4), the power of the desired signal remains unchanged after the equalization such as $||\boldsymbol{h}_i\boldsymbol{q}^*_i e^{-j\varphi_i}||^2 = ||\boldsymbol{h}_i\boldsymbol{q}^*_i||^2$. Also, based on the trigonometry of norm operation, the power of the inter-antenna interference after equalization is upper bounded by $\sum_{i'=1,i'\neq i}^{N_r} ||\boldsymbol{h}_i\boldsymbol{q}^*_{i'} e^{-j\varphi_{i'}}||^2 = \sum_{i'=1,i'\neq i}^{N_r} ||\boldsymbol{h}_i\boldsymbol{q}^*_{i'}||^2$, denoting the optimal per-antenna SINR remained unchanged. On the other hand, the sender's anonymity is also maintained after transmitter side phase equalization, as phase rotation of $\boldsymbol{q}_i$ has no impact on the trace of $\boldsymbol{Q}_i$, $\forall i \in N_r$. ■

Now we are able to devise the whole ISA precoder, as summarized in Algorithm 2. We first run Algorithm 1 to obtain the optimal matrix $\boldsymbol{Q}^*_i$, and $\boldsymbol{q}^*_i$ is immediately obtained with $\mathrm{Rank}(\boldsymbol{Q}^*_i) = 1$, otherwise matrix reduction is conducted based on Propositions 4.2 and 4.3, $\forall i \in N_r$. Afterwards, transmitter side phase equalization is applied for removing the receiver's phase ambiguity without loss of the optimality of the SINR and anonymity performance.

Algorithm 2 The Overall ISA Precoder Design

```
Input: MIMO channel $\boldsymbol{H}_k$ and symbol vector $\boldsymbol{s}$.
1: Perform Algorithm 1 to obtained the SDR matrices $\boldsymbol{Q}^*_i, \forall i \in N_r$.
2: for $i = 1 : N_r$ do
3:     Decompose $\boldsymbol{Q}^*_i$ to obtain the $\boldsymbol{q}^*_i$ if Rank($\boldsymbol{Q}^*_i$) = 1;
4:     Otherwise do rank reduction for $\boldsymbol{Q}^*_i$ and then decompose $\boldsymbol{Q}^*_i$.
5: end for
6: Do transmitter-side phase equalization $\boldsymbol{q}^*_i = \boldsymbol{q}^*_i e^{-j\varphi_i}$, $\forall i \in N_r$,
   to remove phase ambiguity.
Output: Optimal precoding design $[\boldsymbol{q}^*_1, \ldots, \boldsymbol{q}^*_{N_r}]$.
```

2) Constructive-Interference based Anonymous (CIA) Precoding: In part 1), we have proposed a SDR based anonymous precoding design, where the inter-antenna interference is strictly suppressed to guarantee the per-antenna SINR constraint. That is, the inter-antenna interference is treated as a harmful element, and any interference adds perturbation to the received signal. Following this principle, one needs to perform transmitter side phase equalization to constrain the per-antenna's symbol within a region around the nominal point in the modulated signal constellation, as illustrated in Fig. 2(a). Nevertheless, since the transmitted symbols are known by the sender, it is judicious to jointly utilize the spatial correlation among the channels and the symbols to be transmitted, based on the concept of constructive interference (CI) [34]. That is, the inter-antenna interference has potential to be utilized as a desired element to push the per-antenna desired signals away from the detection thresholds of the signal constellation, where the increased distance to the detection threshold of demodulation benefits the per-antenna receiving performance. Let us start by demonstrating the concept of CI in the following Lemma 4.1, and then we elaborate CI for addressing

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2021.3093722, IEEE Transactions on Wireless Communications

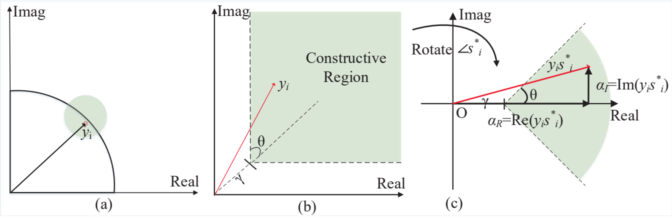


Fig. 2. The geometrical interpretation of CI precoding, where the intended symbol is $\frac{1+i}{\sqrt{2}}$ with QPSK modulation for illustration. By CI design shown in Fig. 1(b), the received signal y_i can be pushed into a constructive region (green area), rather than being strictly located in the proximity region around the constellation point. To guarantee the constructive effect of the interference, geometric interpretation can be exploited as shown in Fig. 1(c).

anonymous precoding design. For notation simplicity we assume PSK modulation, nevertheless the following is applicable to multi-level modulations [34].

Lemma 4.1: Without loss of generality, write the intended symbol of the i-th receive antenna as $s_i = de^{j\phi_i}$ by M-PSK modulation, which can be further expressed as a rotated version of another symbol, such that $s_i = s_{i'}e^{j(\phi_i - \phi_{i'})}$. Hence, the received signal of the i-th receive antenna is written as $y_i = \boldsymbol{h}_i \sum_{i'=1}^{N_r} \boldsymbol{q}_{i'} s_i e^{j(\phi_{i'} - \phi_i)} + n_i$. Taking s_1 as a reference symbol, it is re-expressed as $y_i = \boldsymbol{h}_i e^{j(\phi_1 - \phi_i)} \sum_{i=1}^{N_r} (\boldsymbol{q}_{i'} e^{j(\phi_{i'} - \phi_1)}) s_i + n_i$. Note that the reference symbol can be arbitrary. The reformulation indicates that by exploiting the correlation among the channels and symbols rather than treating the input as a Gaussian signal, the original inter-antenna interference channel reduces to a virtual multicast channel with common messages s_i to all receive antennas [35]. □

As suggested by Lemma 4.1, inter-antenna interference can be utilized as a constructive element to benefit system performance, achieved by exploiting geometrical interpretation shown in Fig. 2. Explicitly, we first rotate the signal y_i by the angle $\angle s_i^*$, and then the rotated signal can be mapped onto real axis $\alpha_I = \Im\{y_i s_i^*\}$ and imaginary axis $\alpha_R = \Re\{y_i s_i^*\}$, respectively. As can be seen, the received signal falls into a constructive region (in Fig. 1 (b)) if and only if the trigonometry $|\alpha_I| \leq (\alpha_R - \gamma)\tan\theta$ (in Fig. 1(c)) holds, where $\theta = \frac{\pi}{M}$ and M represents constellation size. In particular, γ physically represents the Euclidean distance in the signal constellation between the constructive region and the decision thresholds, which also relates to SINR performance of the received signal, as depicted in Fig. 1(c). The above discussion can be extended into any order M-PSK and multi-level modulations [36]. For brevity we refer the readers to [34] for details. Hence, the inter-antenna interference can be made constructive when the following inequality is satisfied.

$$\begin{aligned} &|\Im\{\boldsymbol{h}_i[\boldsymbol{q}_1, ..., \boldsymbol{q}_{N_r}]\boldsymbol{s}s_i^*\}| \leq \\ &\qquad (\Re\{\boldsymbol{h}_i[\boldsymbol{q}_1, ..., \boldsymbol{q}_{N_r}]\boldsymbol{s}s_i^*\}) - \gamma)\tan\theta, \forall i \in N_r, \end{aligned} \tag{11}$$

which guarantees that the inter-antenna interference acts as a beneficial element to push the per-antenna received signal into constructive regions. Nevertheless, when implementing CI with sender's anonymity, it is essential to impose additional anonymous constraint to manipulate the pattern of the received signal. Since the receiver adopts the M-Norm detector to unmask the sender, the following constraint is imposed to hide the sender in the user set.

$$||\boldsymbol{H}_k^H \boldsymbol{H}_k [[\boldsymbol{q}_1, ..., \boldsymbol{q}_{N_r}]]\boldsymbol{s}||^2 \leq \zeta. \tag{12}$$

where ζ serves as an anonymity-related threshold. Now we are able to present the problem formulation for CI-based anonymous precoder. We target to maximize the value of γ, subject to multiple constraints. As discussed, maximizing γ equivalently optimizes the per-antenna receive performance, given as

$$\begin{aligned} \text{P2}: &\max_{[\boldsymbol{q}_1,\dots,\boldsymbol{q}_{N_r}]} \gamma, \\ \text{s.t. } &(\text{C8}): ||[\boldsymbol{q}_1, ..., \boldsymbol{q}_{N_r}]\boldsymbol{s}||^2 \leq p_{max}, \\ &(\text{C9}): ||\boldsymbol{H}_k^H \boldsymbol{H}_k [[\boldsymbol{q}_1, ..., \boldsymbol{q}_{N_r}]]\boldsymbol{s}||^2 \leq \zeta, \\ &(\text{C10}): |\Im\{\boldsymbol{h}_i[\boldsymbol{q}_1, ..., \boldsymbol{q}_{N_r}]\boldsymbol{s}s_i^*\}| \leq \\ &\qquad (\Re\{\boldsymbol{h}_i[\boldsymbol{q}_1, ..., \boldsymbol{q}_{N_r}]\boldsymbol{s}s_i^*\}) - \gamma)\tan\theta, \forall i \in N_r. \end{aligned} \tag{13}$$

Note that the standard convex optimization P2 can be solved directly, without the need of iteration. The whole algorithm is summarized in Algorithm 3. More importantly, the transmitter side phase equalization is not required as the per-antenna received signal has been designed to exactly fall into the constructive regions of the constellation, as summarized in the Remark 4.1.

Remark 4.1: Based on the CIA precoder, the received signal of each antenna has been directly located into constructive regions of the constellation. Hence, the receiver can demodulate the received signal directly, according to the amplitude and phase of the received signal. As a result, the proposed CIA precoder removes the need for receiver or transmitter equalization, while utilizing inter-antenna interference as a beneficial element without loss of anonymity. □

B. Anonymous Precoder for a Strong Receiver ($N_r > N_t$)

In this subsection, we further investigate the anonymous precoding for a strong receiver case. With the configuration of $N_r > N_t$, the SDR formulation is not feasible due to the insufficient transmit DoFs. Nevertheless, by the CI-based precoder, more streams can still be multiplexed than the number of transmit antennas [36], and hence in the strong receiver case all the N_r antennas can be efficiently utilized. On the other hand, as mentioned in Section III, in the strong receiver case the receiver employs the MLE sender detector in (5) to unmask the sender, which considers the user with the minimum value of $||(\boldsymbol{I}_{N_r} - \boldsymbol{H}_k(\boldsymbol{H}_k^H \boldsymbol{H}_k)^{-1}\boldsymbol{H}_k^H)\boldsymbol{y}||^2$ as the real sender. Similar to the anonymous strategy applied in section IV-A, one may design the precoder to manipulate the norm higher than a threshold, i.e., $||(\boldsymbol{I}_{N_r} - \boldsymbol{H}_k(\boldsymbol{H}_k^H \boldsymbol{H}_k)^{-1}\boldsymbol{H}_k^H)\boldsymbol{y}||^2 \geq \zeta$. However, this anonymous constraint confines a non-convex set. More importantly, with the unknown deterministic value of noise, the above constraint reduces to an alternative constraint $||(\boldsymbol{I}_{N_r} - \boldsymbol{H}_k(\boldsymbol{H}_k^H \boldsymbol{H}_k)^{-1}\boldsymbol{H}_k^H)(\boldsymbol{H}_k[\boldsymbol{q}_1, ..., \boldsymbol{q}_{N_r}]\boldsymbol{s})||^2 \geq \zeta$, where the left hand boils down to 0 and the constraint makes no sense. As discussed above, the receiver calculates the norm in (5) in sequence and considers the one with the minimum

© 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

value as the real sender. Hence, we can select a user j from the set $\mathbb{K}$ as an alias, and confines the following inequality as

$$||(\boldsymbol{H}_j\boldsymbol{H}_j^{\dagger}-\boldsymbol{H}_k\boldsymbol{H}_k^{\dagger})\boldsymbol{H}_k[\boldsymbol{q}_1,...,\boldsymbol{q}_{N_r}]\boldsymbol{s}||^2\leq\delta,\forall j\neq k,j\in\mathbb{K},\quad(14)$$

which physically denotes that the k-th and j-th users are equally suspicious to the receiver by setting a small valued threshold δ. Note that the above constraint physically makes the alias j and the real sender k equally suspicious, from the perspective of the receiver. It does not let the alias j transmit artificial noise to jam the receiver. However, imposing $K-1$ constraints in (14) significantly reduces the DoFs of precoder design and thus may result in poor per-antenna SINR performance. To make a good trade-off between the per-antenna SINR and anonymity, the sender can randomly select one user from $\mathbb{K}$ as the alias sender. As a result, there will be only 1 constraint in (14) without significantly degrading DoFs of precoder design. Also, the receiver still fails to declare the correct sender, as the real sender k and the alias j are equally suspicious.

Similar to P2, while we maximize the effect of γ to exploit the beneficial effect of inter-antenna interference, anonymity constraint is also imposed against the MLE based sender detector.

$$\begin{aligned}\text{P3}:&\max_{[\boldsymbol{q}_1,...,\boldsymbol{q}_{N_r}]}\ \gamma,\ \text{ s.t. (C11)}:||[\boldsymbol{q}_1,...,\boldsymbol{q}_{N_r}]\boldsymbol{s}||^2\leq p_{max},\\&\text{(C12)}:|\Im\{\boldsymbol{h}_i[\boldsymbol{q}_1,...,\boldsymbol{q}_{N_r}]\boldsymbol{s}s_i^*\}|\leq\\&\qquad(\Re\{\boldsymbol{h}_i[\boldsymbol{q}_1,...,\boldsymbol{q}_{N_r}]\boldsymbol{s}s_i^*\})-\gamma)\tan\theta,\forall i\in N_r,\\&\text{(C13)}:||(\boldsymbol{H}_j\boldsymbol{H}_j^{\dagger}-\boldsymbol{H}_k\boldsymbol{H}_k^{\dagger})\boldsymbol{H}_k[\boldsymbol{q}_1,...,\boldsymbol{q}_{N_r}]\boldsymbol{s}||^2\leq\delta,j\in\mathbb{K},\end{aligned}\quad(15)$$

where (C11) denotes the power constraint, while constraints (C12) and (C13) are imposed for SINR and anonymity requirements. Since P3 maximizes a linear variable under convex constraints, it is a standard SOCP problem, which can be directly solved without the need of iteration. The whole algorithm is included Algorithm 3.

Algorithm 3 The CIA Precoder Design

```
Input: MIMO channel $\boldsymbol{H}_k$, power budget $p_{max}$, symbol vector $\boldsymbol{s}$.
1: Solve the standard convex optimization P2 (strong sender case).
2: Or solve the standard convex optimization P3 with a random alias
   sender (strong receiver case).
Output: Optimal precoding design $[\boldsymbol{q}_1^*,...,\boldsymbol{q}_{N_r}^*]$.
```

Remark 4.2: Assuming that the real sender (user k) is strongly correlated with another user j ($\forall j\in\mathbb{K}$), the features of the channel $\boldsymbol{H}_k$ approaches those of the $\boldsymbol{H}_j$, and the test results of the k-th user become analogous to those of the j-th user. As a result, the detection results obtained by MLE-based detection and M-norm detection are impaired, and the two users (j and k) are equally suspicious from the perspective of the receiver. On the other hand, when designing anonymous precoding, it becomes easier to satisfy the anonymity constraints with strong channel correlation among the real sender and other users. For example, the anonymity constraint by the CIA precoder is written by (C10) and (C13). When $\boldsymbol{H}_k$ is strongly correlated to $\boldsymbol{H}_j$, the term $(\boldsymbol{H}_j\boldsymbol{H}_j^{\dagger}-\boldsymbol{H}_k\boldsymbol{H}_k^{\dagger})$ approaches 0. Hence, it becomes easier to satisfy the inequalities above. □

Remark 4.3: A promising extension of this work is to consider anonymous communications where multiple users transmit signals simultaneously. The difficulty lies in how to guarantee the multiple users' signals can be correctly decoded when they anonymously transmit to an AP, and it is further related to the centralized or decentralized algorithm design. In particular, by the centralized manner, there is a central unit for precoding design, and in this case anonymous precoding makes no difference to the design presented in this paper. For example, each user's signal is multiplexed onto a subgroup of the receiver's antennas under an individual user's anonymity constraint. Based on the received signal on each receiver antenna, the AP can directly decode the data. In a decentralized setting, as each user calculates its own precoding without a central unit, the key point of designing anonymous precoding is to control the effect of multiuser interference at the AP side. A possible solution is to let users share their wireless channels with others at low overhead. Though the users still design their precoding without notifying others, the receiver SINR can be better controlled by suppressing the multiuser interference, which is similar to mitigating the inter-cell interference of coordinated beamforming systems. □

C. Complexity Analysis for the Anonymous Precoders

In this subsection we investigate the complexities of the proposed precoders. We first consider the strong sender case [1]. For the ISA precoder, it first iteratively solves P1(b) to obtain the optimal SDR matrices $\boldsymbol{Q}_i$, $\forall i\in N_r$. Since P1(b) is subject to N_r LMI constraints (trace) in ($\tilde{C}$4) with size 1, 1 LMI constraint (trace) in ($\tilde{C}$5) with size 1, N_r LMI constraints in (C6) with size N_t (and (C7) is removed by SDR operation), the complexity for iteratively optimizing P1(b) is given as $l_i\sqrt{N_r+1+N_rN_t}\ln(\frac{1}{\tau})\big(n_1(N_r+1+N_rN_t^3)+n_1^2(N_r+1+N_rN_t^2)+n_1^3\big)$, where l_i denotes the number of iterations for convergence and will be further demonstrated in simulations. τ represents the tolerance of accuracy. Afterwards, eigenvalue decomposition for $\boldsymbol{Q}_i$ is computed for obtaining $\boldsymbol{q}_i$ with complexity $23N_t^3$, followed by transmitter side phase equalization with complexity $8N_t$. Hence, the overall complexity of the ISA anonymous precoder is given as $l_i\sqrt{N_r+1+N_rN_t}\ln(\frac{1}{\tau})\big(n_1(Nr+1+N_rN_t^3)+n_1^2(N_r+1+N_rN_t^2)+n_1^3\big)+N_r(23N_t^3+8N_t)$. On the other hand, the CIA precoder (strong sender case) in (P2) is subject to 1 SOC constraint in (C8), N_r linear constraints in (C9), and 1 SOC constraint in (C10). Hence, its overall complexity is given as $\sqrt{4+N_r}\ln(\frac{1}{\tau})\big(n_2N_r+n_2^2Nr+n_2(N_t^2+N_t^2)+n_2^3\big)$. Now we consider the complexity of the CIA precoder in the strong receiver case (P3). It is subject to 1 SOC constraint

[1] For convex formulations that involve linear matrix inequality (LMI) and SOC constraints, their complexities can be evaluated as $\ln(\frac{1}{\tau})\sqrt{c_b}(c_{form}+c_{fact})$ [37]. Specifically, $\ln(\frac{1}{\tau})$ relates to the accuracy setup. $\sqrt{c_b}$ represents the barrier parameter measuring the geometric complexity of the conic constraints. c_{form} and c_{fact} represent the complexities cost on forming and factorization of $n\times n$ matrix of the linear system. We refer readers to [37] for details.

TABLE I. Complexity analysis with accuracy factor τ, where $n_1 = \mathcal{O}(KN_t^2)$ and $n_2 = \mathcal{O}(N_tN_r)$.

Anonymous Precoder	Strong sender	ISA precoder	$l_i\sqrt{N_r+1+N_rN_t}\ln(\frac{1}{\tau})\big(n_1(N_r+1+N_rN_t^3)+ n_1^2(N_r+1+N_rN_t^2)+n_1^3\big)+N_r(23N_t^3+8N_t)$
		CIA precoder	$\sqrt{4+N_r}\ln(\frac{1}{\tau})\big(n_2N_r+n^2N_r+2n_2N_t^2+n_2^3\big)$
	Strong receiver	CIA precoder	$\sqrt{4+N_r}\ln(\frac{1}{\tau})(n_2N_r+n_2^2N_r+n_2(N_t^2+N_r^2)+n_2^3)$
Comparisons	/	MMSE precoder [39]	$16N_r^2N_t+24N_rN_t^2+29N_t^3$
		SVD MIMO [38]	$16N_r^2N_t+24N_rN_t^2+16N_rN_t^2+24N_t^3$
		CI precoder [36]	$\sqrt{2+N_r}\ln(\frac{1}{\tau})(n_2N_r+n_2^2N_r+n_2N_t^2+n_2^3)$

in (C11), N_r linear constraints in (C12), and 1 SOC constraint in (C13). Hence, its overall complexity is given as $\sqrt{4+N_r}\ln(\frac{1}{\tau})(n_2N_r+n_2^2N_r+n_2(N_t^2+N_r^2)+n_2^3)$. By comparing the complexities of the precoders, we have the following observation.

Remark 4.4: Since the per-antenna SINR constraint of the ISA precoder is imposed by the fractional-structured SOC constraints in (C1) of P1, it is further transformed into LMI constraints in P1(b). In comparison, by the CIA precoder, the per-antenna SINR constraint is imposed in the form of linear constraints ((C9) in P2 or (C12) in P3), which generally requires lower computational complexity than the LMI constraint in P1(b). Also, the CIA precoder directly locates the received signal at the receiver into constructive regions, and hence the subsequent matrix decomposition and transmitter-side phase equalization are not required. □

V. Simulation Results

We present the Monte-Carlo simulation results in this section. Without loss of generality, power budget is set to as $p_{\max} = 1$ Watt. QPSK is adopted as modulation scheme and the symbol vector is randomly generated. Assume that each block consists of 50 symbols. There are $K = 5$ senders, and the communication sender in each time slot (block) is randomly generated. We consider a Rayleigh block fading MIMO channel, and without loss of practicality, the proposed design can be straightforwardly extended into a multi-carrier configuration that is suitable for wideband communications. The antenna configuration is set to as $N_r = N_t = 10$ in the strong sender case, while it is assumed that $N_r = 10$ and $N_t = 9$ in the strong receiver case. The energy detection threshold in is set to as $\beta = 10^{-2}$. As revealed in section III, the receiver attempts to identify the real sender from the K candidates, by employing the MLE/M-Norm sender detectors at the strong receiver/sender cases, respectively. In addition, the following classic precoders are selected as comparison algorithms: 1) SVD precoder [38], where the receiver first detects the origin of the received signal and then calculates its receive equalizer based on the declared hypothesis. 2) MMSE [39] and 3) CI precoder [36], where each receive antenna is treated as an individual receiver for multiplexing and hence no equalizer is required at the receiver.

In Fig. 3(a), the sender detection error rate (DER) performance of different precoders is demonstrated. It is observed that both the proposed anonymous ISA and CIA precoders achieve strong anonymity performance, where the receiver's DER performance is maintained at up to 0.8 even with high receiver SNR. For the ISA precoder, its anonymity constraint is guaranteed by (C3) in P1, which is further transformed into a LMI constraint ($\tilde{C5}$). It can be seen that the anonymity is well guaranteed after the SDR operation of P1(b) and transmitter phase equalization, confirming the analysis in Proposition 4.4. Also for the CIA precoder, the anonymity constraint (C10) in P2 manipulates the pattern of the received signal to scramble the sender detection, which makes the receiver have a high probability of mis-clarifying the real sender. In comparison, the SVD MIMO demonstrates the worst anonymity performance, where the receiver is able to unmask the correct sender with below 10^{-2} DER at 10 dB SNR. With the MMSE precoder, the receiver's DER demonstrates a U-shape when the receiver SNR increases. It is because at low SNR regime, its detection performance is impaired by the receive noise. While at high SNR regime, the structure of the MMSE precoder approaches that of the ZF precoder such as $\boldsymbol{H}^H(\boldsymbol{H}\boldsymbol{H}^H)^{-1}$, and thus the received signal tends to be $\boldsymbol{y} = \boldsymbol{s} + \boldsymbol{n}$, where the sender's channel information is removed. As a result, the DER by MMSE precoder is occasionally maintained at a high receiver SNR regime. Also for the CI precoder, its target is to maximize the receiver SINR performance without the consideration of sender's anonymity. In particular, since it has been reported that the CI precoder is reduced to the ZF precoder when occasionally no interference can be exploited [40], a higher DER is achieved over the SVD precoder but is still less-anonymous to the proposed CIA precoder. Last but not least, a smaller value of ϵ and ζ leads to a higher probability of misdetection at the receiver, and hence it is difficult for the receiver to correctly identify the real sender. In other words, the receiver is less likely to estimate a large value for p_k, and anonymity entropy is also enhanced. Also, with the reduced detrimental impact of noise at higher SNR regimes, the accuracy of the sender detector of the receiver is improved (except MMSE) and hence the receiver's detection becomes more accurate, resulting a decreased DER.

In Fig. 3(b), the symbol error rate (SER) performance under different precoders is demonstrated. Since the CI precoder is able to utilize the inter-antenna interference without anonymous constraints, the high DoFs at the sender side endorse the lowest SER performance among all the precoders [40]. However, it can be seen that the proposed CIA precoder achieves a close SER performance to the CI precoder, and significantly outperforms the SVD and MMSE at moderate/high SNR regimes. For the ISA precoder, although its DoF of the precoder design is constrained by the anonymity constraint, it still demonstrates a close SER to the SVD precoder at 0-12 dB SNR regimes, and outperforms the SVD precoder with above 12 dB SNR. Hence, the two anonymous precoders indeed strike a good trade-off between guaranteeing high communication quality and addressing sender's anonymity.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2021.3093722, IEEE Transactions on Wireless Communications

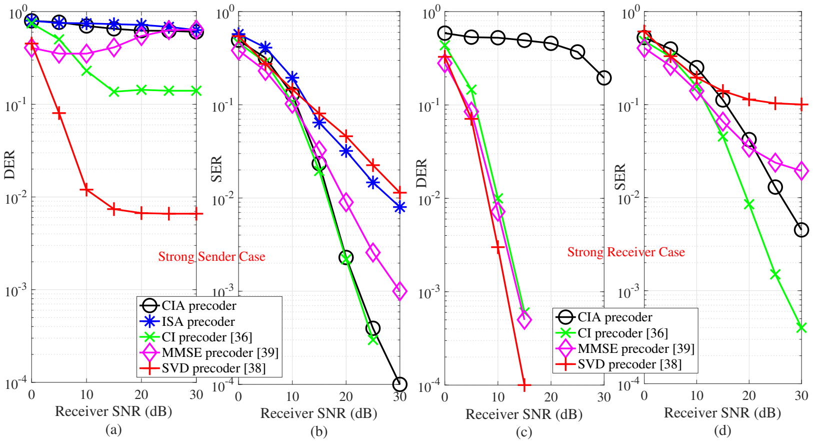


Fig. 3. The impact of receiver SNR on the DER and SER by different precoders. Strong sender case: $N_t = N_r = 10$. The anonymity-related thresholds imposed for constraints (C3) and (C10) are set to as $\epsilon = 20$ and $\zeta = 8$, respectively. Strong receiver case: $N_t = 9$, $N_r = 10$, and $\delta = 0.03$.

In Fig. 3(c), the DER performance of different precoders is presented for the strong receiver case. First, since the DoF of the receiver is improved with the strong receiver configuration, the MLE detector can be employed, which helps the receiver obtain a more accurate detection performance compared to the strong sender case. Importantly, it can be seen that the proposed CIA precoder still guarantees the DER above 0.5 at 0-15 dB SNR, above 0.4 at 15-25 SNR, and above 0.2 at 30 dB SNR regimes. In comparisons, by the CI, MMSE and SVD precoders, the receiver can correctly identify the real sender with 10^{-1}-10^{-2} DER at 5-10 dB SNR regimes, which further decreases to 10^{-3} with above 12 dB SNR regimes. In particular, with the strong receiver case $N_r > N_t$, the multiplication of the MIMO channel and MMSE precoder does not lead to an identity matrix such that $\boldsymbol{H}\boldsymbol{H}^H(\boldsymbol{H}\boldsymbol{H}^H + \frac{N_r\sigma^2}{p}\boldsymbol{I}_{N_r})^{-1} \neq \boldsymbol{I}_{N_r}$ due to the rank-insufficient property of $\boldsymbol{H}\boldsymbol{H}^H$. As a result, the channel information is not null-ed as that in the strong sender case, and thus the sender's anonymity is leaked to the receiver by the MMSE precoder. In Fig. 3(d), the SER performance of different precoders is presented. It is shown that the proposed CIA precoder outperforms the SVD precoder with above 11 dB receiver SNR and the MMSE precoder with above 15 dB receiver SNR, respectively. Also, although anonymity constraint limits the DoFs of the anonymous precoding design, the CIA precoder still provides a comparable SER performance to the CI precoder, and it demonstrates 5 dB SNR gain between the two precoders at 10^{-2} SER level. Furthermore, it is worth mentioning the SVD precoder only supports N_t streams in the strong receiver case, while the CIA precoder enables more data streams (N_r) than the number of the transmit antennas (N_t), confirming its applicability in both strong receiver/sender cases.

In Fig. 4, the DER and SER performances with different antenna configurations are demonstrated. For the DER performance in Fig. 4(a), it is first observed that with more antennas, the DER of the anonymous precoders are improved. It is because with the increased dimension of a channel matrix, the impact of the anonymity threshold ϵ in (C5) and ζ in (C10) becomes stricter, which leads to a more stringent anonymity requirement. Also, a similar trend can be observed by the comparison algorithms with distinct reasons. To be specific, with more transmit antennas, the spatial orthogonality of the MIMO channel between the sender and receiver is increased, and thus the structures of MMSE, SVD and CI precoders slightly tend to that of the ZF precoder. As a result, the DER performance of the comparison algorithms is increased with more transmit antennas, whereas the receiver is still able to declare the correct sender with high probability. Second, with different antenna configurations, the proposed precoders always endorse a stricter anonymity compared to the comparison algorithms, where the receiver is able to declare the correct sender with a DER lower than 0.03 using an SVD precoder, with a DER lower than 0.3 using a CI precoder, and with a DER lower than 0.6 using an MMSE precoder. For the SER performance Fig. 4(b), the CIA precoder shows a close performance to that of the CI precoder, while the ISA precoder always outperforms the SVD precoder. This is because with the increased transmit DoF, it is easier for the anonymous precoder to satisfy the anonymity constraint without sacrificing much per-antenna SINR performance. In addition, it is worth noting that since the SVD's combiner is based on the sender detection, its SER first decreases due to the high transmit DoF but begins to increase with $N_t \geq 12$ due to the improved DER.

In Figs. 4(c) and (d), the DER and SER performance with different antenna configurations is demonstrated in the strong receiver case. In Fig. 4(c), the DER of the CI, MMSE and SVD precoders is reduced to 0, where the MLE based sender detector can perfectly identify the real sender. As a comparison, the proposed anonymous precoder maintains the DER at 0.2-0.8 with different numbers of transmit antennas. An interesting observation is that, with a fixed anonymity threshold, the DER is reduced if the number of the transmit antennas increases. As shown in equation (4), the estimation of the transmitted vector has a size of $\boldsymbol{H}_k^\dagger \boldsymbol{y} \in \mathbb{C}^{N_t \times 1}$. Hence, with a larger number of transmit antennas, the difference between $\boldsymbol{H}_k^\dagger \boldsymbol{y}$ and $\boldsymbol{H}_j^\dagger \boldsymbol{y}$ ($\forall j \neq k$) is increased and it becomes easier for the receiver

© 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Wireless Communications. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TWC.2021.3093722

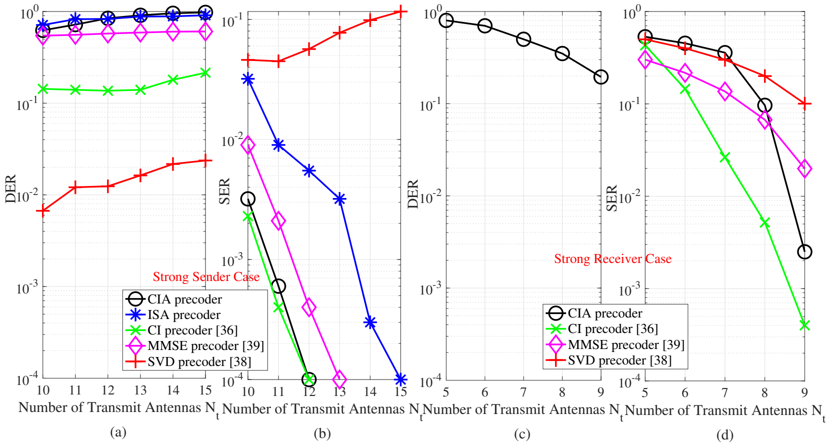


Fig. 4. The impact of different antenna configurations on the DER and SER performance, where $N_r = 10$. Strong sender case: $N_t = 10 - 15$, $\epsilon = 20$, $\zeta = 8$, and SNR is fixed at 20 dB. Strong receiver case: $N_t = 5 - 9$, $\delta = 0.03$. SNR is fixed at 30 dB.

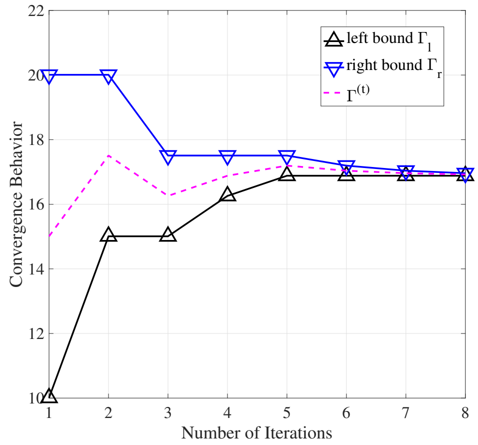


Fig. 5. The convergence behavior on finding $\Gamma^{(t)}$ by P1(b), where tolerance factor $\tau = 0.1$, $N_t = N_r = 10$, and $\epsilon = 20$.

to distinguish the real sender and its alias. It indicates that one needs to also correspondingly set a stricter anonymity threshold in this case. On the other hand, Fig. 4(d) shows that the SER of the proposed CIA precoder is superior to the SVD and MMSE precoders if N_t approaches N_r, while the comparison algorithms fail to address the anonymity as observed in Fig. 4(c). In particular, in the strong receiver case, since we need to multiplex N_r data streams in the case of $N_t < N_r$, the SER performance may not be acceptable when N_t is significantly smaller than N_r. In this case, a possible solution is to consider diversity MIMO where only one single data stream is transmitted by the sender. A key point here is as the receiver may not correctly clarify the real sender, the combiner design at the receiver needs to be independent from the CSI, such as equal gain combiner. Since in this paper we are interested in the multiplexing MIMO design, diversity based MIMO anonymous communication is beyond its scope.

Fig. 5 shows the number of iterations by the ISA precoder for achieving convergence, with initial right bound $\Gamma_r = 20$ and left bound $\Gamma_l = 0$. Since the bisection search requires at most $\ln(\frac{\Gamma_r - \Gamma_l}{\tau})$ iterations for convergence, it is seen that the algorithm converges to a stationary point with around 6-7 iterations, confirming the low complexity of the ISA design.

In Fig. 6, the DER and SER performances with different variance of the channel estimation error are demonstrated, where SNR is fixed at 30 dB. In particular, we consider a worst-case scenario where the receiver has perfect CSI for sender detection while the users have imperfect CSI for anonymous precoding design. It is observed that though the SER performance is increased with a coarse estimation quality, the proposed CIA precoder still outperforms the SVD and MMSE precoders, and the ISA precoder is also superior to the SVD precoder. On the other hand, since the anonymity threshold may not be perfectly guaranteed due to the estimation error, it becomes easier for the receiver to unmask the real sender and hence the DER performance is slightly reduced with a high value of the estimation error. As a comparison, the DER of the comparison precoders is 0 where the receiver can always unmask the real sender in the strong receiver case.

It is observed in Fig. 7 that for the proposed CIA and ISA precoders, there exists a tradeoff between the DER and SER performance. That is, the DER can be increased to a high level by setting stricter anonymity thresholds, while it is achieved by sacrificing the SER performance. Also, it is observed that the tradeoff curve by the ISA precoder is more critical than that of the CIA precoder. This is because the CIA precoder has a linear structure as demonstrated in P2 and P3, and it locates the received signal into construction regions. Hence, a stricter anonymity threshold does not significantly constrain the DoF in the precoder design, where the tradeoff curve is almost flat. In contrast, the ISA precoder strictly constrains the received signal in a proximity region around the constellation point. Hence, with a smaller value of the anonymity threshold, the DoF reduction of the ISA precoder leads to a sharper tradeoff curve.

In Fig. 8, the DER performance is demonstrated with a small number of antennas. It is observed that both the proposed

© 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

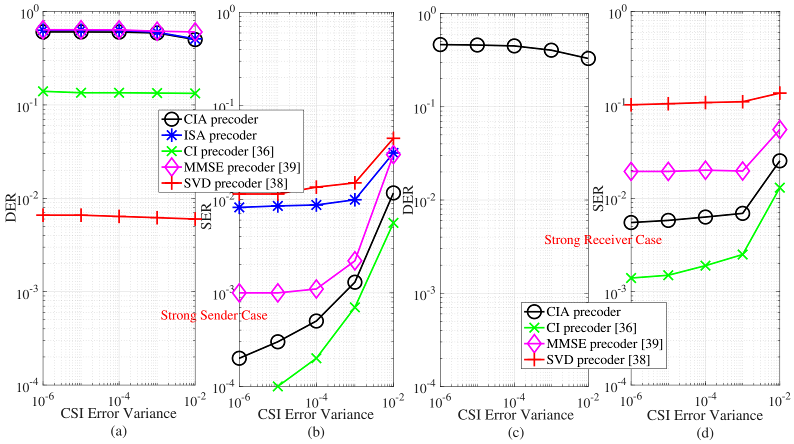


Fig. 6. The impact of imperfect channel estimation on the DER and SER performance, where $N_t = N_r = 10$ in the strong sender case, $N_t = 9$ and $N_r = 10$ in the strong receiver case. The anonymity thresholds are set to as $\epsilon = 20, \zeta = 8$, and $\delta = 0.01$.

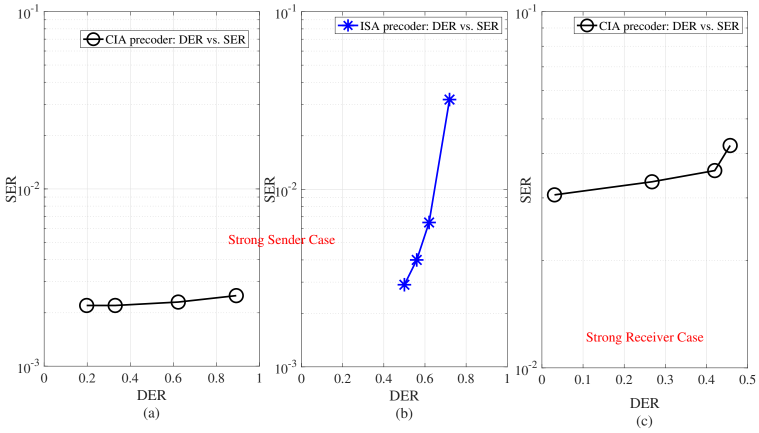


Fig. 7. DER VS. SER curve by the proposed CIA and ISA precoders, where $N_t = N_r = 10$ in the strong sender case, $N_t = 9$ and $N_r = 10$ in the strong receiver case. SNR is fixed at 20 dB.

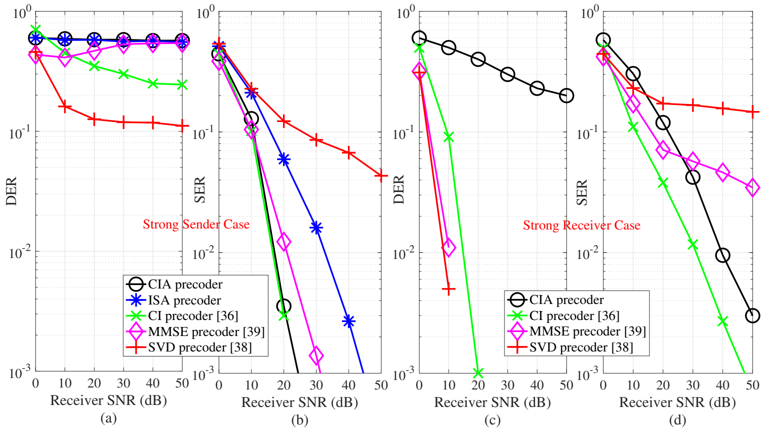


Fig. 8. The impact of receiver SNR on the DER and SER by different precoders. Strong sender case: $N_t = N_r = 5$. Strong receiver case: $N_t = 5$ and $N_r = 6$.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2021.3093722, IEEE Transactions on Wireless Communications

anonymous ISA and CIA precoders achieve strong anonymity performance, where the DER performance is maintained at up to 0.6 in the strong sender case, and around 0.2-0.6 in the strong receiver case. Also, reasonable SER performance is provided by the proposed anonymous precoders, proving that the CIA and ISA precoders strike a good tradeoff between the anonymity and the communication quality.

VI. CONCLUSIONS

In this paper, we have proposed the concept of PHY anonymity, and revealed that by only analyzing PHY information, the receiver is able to unmask the sender's identity. With different antenna configurations, we have proposed two sender detection strategies for the receiver, one MLE detector for the strong receiver case and one M-Norm detector for the strong sender case. Subsequently, we have investigated anonymous precoding design to guarantee the sender's anonymity while maximizing per-antenna SINR performance. Hence, we have further proposed an ISA precoder with tight SDR, assisted by a dedicated transmitter side phase equalizer for removing phase ambiguity, and a CIA precoder with the ability of utilizing inter-antenna interference as an useful source for improving SINR performance. Furthermore, the CIA precoder is also applicable to the strong receiver case, where more streams can be multiplexed than the number of transmit antennas without losing the sender's anonymity. Compared to the comparison algorithms, the proposed anonymous precoders are able to mask the sender's identity, while simultaneously providing high per-antenna SINR for anonymous communications.

APPENDIX A
PROOF OF PROPOSITION 4.2

The relaxed version of transformed problem P1(b) in (9) is jointly convex with respect to the optimization variables and satisfies the Slater's constraint qualification (without (C7)). Hence, strong duality holds and solving the dual problem is equivalent to solving the primal problem [41]. For obtaining the dual problem, we write the Lagrangian function of (9) as $\mathcal{L} = \sum_{i=1}^{N_r} \mathrm{Tr}(\boldsymbol{Q}_i) + \mu(\mathrm{Tr}(\boldsymbol{\Pi} \sum_{i=1}^{N_r} \boldsymbol{Q}_i) - \epsilon) - \sum_{i=1}^{N_r} \boldsymbol{P}_i \boldsymbol{Q}_i + \sum_{i=1}^{N_r} \lambda_i \big(\Gamma^{(j)} \sigma^2 + \Gamma^{(j)} \sum_{i' \neq i, i'=1}^{N_r} \mathrm{Tr}(\boldsymbol{G}_i \boldsymbol{Q}_{i'}) - \mathrm{Tr}(\boldsymbol{G}_i \boldsymbol{Q}_i)\big)$, where $\boldsymbol{\Pi} = \boldsymbol{H}_k^H \boldsymbol{H}_k \boldsymbol{H}_k^H \boldsymbol{H}_k$ and $\boldsymbol{G}_i = \boldsymbol{h}_i^H \boldsymbol{h}_i$ for brevity. μ and λ_i are the Lagrange multipliers associated with constraints ($\tilde{\mathrm{C}}5$) and ($\tilde{\mathrm{C}}4$), respectively, while matrix $\boldsymbol{P}_i \in \mathbb{C}^{N_t \times N_t}$ is the Lagrange multiplier matrix for the positive semi-definite constraint (C6). Hence, the dual problem for the optimization in (9) is written as $\max_{\mu \geq 0, \lambda_i \geq 0, \boldsymbol{P}_i \succeq \boldsymbol{0}} \min_{\boldsymbol{Q}_i} \mathcal{L}(\mu, \lambda_i, \boldsymbol{P}_i, \boldsymbol{Q}_i)$. We reveal the structure of the optimal $\boldsymbol{Q}_i$ of (14) by studying the Karush-Kuhn-Tucker (KKT) conditions, which includes the dual constraints: $\mu^* \geq 0, \lambda_i^* \geq 0, \boldsymbol{P}_i^* \succeq \boldsymbol{0}, \forall i \in N_r$; and complementary slackness: $\boldsymbol{P}_i^* \boldsymbol{Q}_i^* \succeq \boldsymbol{0}, \forall i \in N_r$; and the gradient of Lagrange function with respect to $\boldsymbol{Q}_i$ vanishing to 0: $\frac{\partial \mathcal{L}}{\partial \boldsymbol{Q}_i}|_{\boldsymbol{Q}_i^*} = 0$: $\frac{\partial \mathcal{L}}{\partial \boldsymbol{Q}_i}|_{\boldsymbol{Q}_i^*} = \boldsymbol{I}_{N_t} + \Gamma^{(j)} \sum_{i' \neq i}^{N_r} \lambda_{i'}^* \boldsymbol{G}_{i'} + \mu^* \boldsymbol{\Pi} - \boldsymbol{P}_i - \lambda_i^* \boldsymbol{G}_i = 0, \forall i \in N_r$, which further yields $\boldsymbol{P}_i^* = \boldsymbol{R}_i^* - \lambda_i^* \boldsymbol{G}_i$, where $\boldsymbol{R}_i^* = \boldsymbol{I}_{N_t} + \Gamma^{(j)} \sum_{i' \neq i}^{N_r} \lambda_{i'}^* \boldsymbol{G}_{i'} + \mu^* \boldsymbol{\Pi}$. Indeed, it can be verified that in order to meet the per-antenna SINR constraints, it must hold that $\mathrm{rank}(\boldsymbol{Q}_i^*) \geq 1$ with $\boldsymbol{Q}_i^* \neq \boldsymbol{0}$. Hence, the complementary slackness $\boldsymbol{P}_i \boldsymbol{Q}_i = \boldsymbol{0}$ indicates $\mathrm{Rank}(\boldsymbol{P}_i^*) \leq N_t - 1$.

If $\mathrm{Rank}(\boldsymbol{P}_i^*) = N_t - 1$, then the optimal beamforming matrix $\boldsymbol{Q}_i^*$ must be a rank-one matrix. In order to further reveal the structure of $\boldsymbol{P}_i^*$, we first show by contradiction that $\boldsymbol{R}_i^*$ is a positive-definite matrix with probability one under the condition stated in the Proposition 4.2. For a given set of optimal dual variables, i.e., $\mu^*, \lambda_i^*, \boldsymbol{P}_i^*$, the dual problem can be written as $\min_{\boldsymbol{Q}_i} \mathcal{L}(\boldsymbol{Q}_i, \mu^*, \lambda_i^*, \boldsymbol{P}_i^*)$. Suppose $\boldsymbol{R}_i^*$ is not positive-definite. In this case, we can choose $\boldsymbol{Q}_i = \beta \boldsymbol{r}_i \boldsymbol{r}_i^H$ as one of the optimal solution of the dual problem, where $\beta > 0$ is a scaling parameter and $\boldsymbol{r}_i$ is the eigenvector corresponding to a non-positive eigenvalue $\rho_i < 0$ of $\boldsymbol{R}_i^*$, i.e., $\boldsymbol{R}_i^* \boldsymbol{r}_i = \rho_i \boldsymbol{r}_i$. Then, substituting $\boldsymbol{Q}_i = \beta \boldsymbol{r}_i \boldsymbol{r}_i^H$ and $\boldsymbol{R}_i^* \boldsymbol{r}_i = \rho_i \boldsymbol{r}_i$ into the dual problem yields $\sum_{i=1}^{N_r} \mathrm{Tr}(\beta \boldsymbol{r}_i \boldsymbol{r}_i^H) - \rho \sum_{i=1}^{N_r} \mathrm{Tr}(\boldsymbol{r}_i \boldsymbol{r}_i^H (\boldsymbol{P}_i^* + \lambda_i \boldsymbol{G}_i))$, where the first term is not positive. For the second term, since the channel vector $\boldsymbol{h}_i$ is statistically independent, and based on $\boldsymbol{P}_i^* \succeq \boldsymbol{0}$, we have the second term $\rho \sum_{i=1}^{N_r} \mathrm{Tr}(\boldsymbol{r}_i \boldsymbol{r}_i^H (\boldsymbol{P}_i^* + \lambda_i \boldsymbol{G}_i))$ is greater than 0. Setting $\rho \rightarrow \infty$, we have the term $-\rho \sum_{i=1}^{N_r} \mathrm{Tr}(\boldsymbol{r}_i \boldsymbol{r}_i^H (\boldsymbol{P}_i^* + \lambda_i \boldsymbol{G}_i)) \rightarrow -\infty$, where the dual optimal value becomes unbounded from below. However, the optimal value of the primal problem (9) is non-negative. Thus, strong duality cannot hold which leads to a contradiction [41]. Therefore, $\boldsymbol{R}_i^*$ is a positive-definite matrix with probability one, i.e., $\mathrm{Rank}(\boldsymbol{R}_i^*) = N_t$. By applying $\boldsymbol{P}_i^* = \boldsymbol{R}_i^* - \lambda_i^* \boldsymbol{G}_i$ and the sub-additivity property of the rank operation, we have $\mathrm{Rank}(\boldsymbol{P}_i^*) + \mathrm{Rank}(\lambda_i \boldsymbol{G}_i) \geq \mathrm{Rank}(\boldsymbol{P}_i^* + \lambda_i \boldsymbol{G}_i) = \mathrm{Rank}(\boldsymbol{R}_i^*) = N_t \Rightarrow \mathrm{Rank}(\boldsymbol{P}_i^*) = N_t - 1$.. Finally, we obtain that $\mathrm{Rank}(\boldsymbol{P}_i^*) = N_t - 1$. Thus, $\mathrm{Rank}(\boldsymbol{Q}_i^*) = 1$ holds with probability one.

REFERENCES

[1] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Efficient key generation by exploiting randomness from channel responses of individual OFDM subcarriers," *IEEE Trans. Commun.*, vol. 64, no. 6, pp. 2578-2588, Jun. 2016

[2] J. Hu, *et al.,* "Covert communication achieved by a greedy relay in wireless networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 7, pp. 4766-4779, Jul. 2018.

[3] Z. Wei and C. Masouros, "Device-centric distributed antenna transmission: Secure precoding and antenna selection with interference exploitation," *IEEE Internet Things J.,* vol. 7, no. 3, pp. 192-203, Mar. 2020.

[4] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Wireless Commun.*, vol. 58, no. 3, pp. 1875-1888, Mar. 2010.

[5] M. S. Herfeh, A. Chorti and H. V. Poor, "Physical layer security: Authentication, integrity and confidentiality," Chapter in *Physical Layer Security*, Khoa N. Le, Ed. Cham, Switzerland: Springer Nature, to appear.

[6] L. Sankar, S. R. Rajagopalan, and H. V. Poor, "Utility-privacy tradeoffs in databases: an information-theoretic approach," *IEEE Trans. Inf. Foren. Sec.*, vol. 8, no. 6, pp. 838-852, Jun. 2013.

[7] K. Kalantari, L. Sankar, and A. D. Sarwate, "Robust privacy-utility tradeoffs under differential privacy and hamming distortion," *IEEE Trans. Inf. Foren. Sec.*, vol. 13, no. 11, pp. 2816-2830, Nov. 2018.

[8] J. Liao, L. Sankar, V. Y. Tan, and F. D. Pin Calmon, "Hyphthesis testing under mutual information privacy constraints in the high privacy regime," *IEEE Trans. Inf. Foren. Sec.*, vol. 13, no. 4, pp. 1508-1071, Apr. 2018.

[9] A. Serjantov and G. Danezis, "Towards an information theoretic metric for anonymity," *in Proc. Privacy Enhancing Technologies Workshop'02,* San Francisco, USA, Apr. 2002.

[10] G. Danezis, "Introducing anonymous communications properties, threat models, systems and attack," [Online] http://www0.cs.ucl.ac.uk/staff/G.Danezis/talks/AnonTalk.pdf, 2006.

© 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

[11] T. Y. Youn, Y. H. Park, and J. Lim, "Weaknesses in an anonymous authentication scheme for roaming service in global mobility networks," *IEEE Commun. Lett.*, vol. 13, n0. 7, pp. 471-473, Jul. 2009.

[12] J. Liu, Z. Zhang, X. Chen, and K. S. Kwak, "Certificateless remote anonymous authentication schemes for wireless body area networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 332-342, Feb. 2014.

[13] R. Lu *et al.,* "A novel anonymous mutual authentication protocol with provable link-layer location privacy," *IEEE Trans. Veh. Technol.,* vol. 58, no. 3, pp. 1454-1466, Mar. 2009.

[14] P. Gope, J. Lee, R. H. Hsu, and T. Q. S. Quek, "Anonymous communications for secure device-to-device-aided fog computing," *IEEE Consumer Electron. Maga.*, vol. 15, pp. 10-16, May 2019.

[15] J. Ren and L. Harn, "An efficient threshold anonymous authentication scheme for privacy-preserving communications," *IEEE Trans. Wireless Comm.*, vol. 12, no. 3, pp. 1018-1025, Mar. 2013.

[16] K. Emura and T. Hayashi, "Road to vehicle communications with time-dependent anonymity, a lightweight construction and its experimental results," *IEEE Trans. Veh. Tech.*, vol. 67, no. 2, pp. 1582-1597, Feb. 2018.

[17] K. Emura, A. Kanaoka, S. Ohta, K. Omote, and T. Takahashi, "Secure and anonymous communication technique: formal model and its prototype implementation," *IEEE Trans. Emerging Topics Comput.,* vol. 4, no. 1, pp. 88-101, Mar. 2016.

[18] M. F. Ezerman, H. T. Lee, S. Ling, K. Nguyen, and H. Wang, "Provable secure group signature schemes from code-based assumption," *IEEE Trans. Inf. Theory,* vol. 66, no. 9, pp. 5754-5773, Sep. 2020.

[19] H. Fang, X. Wang, and S. Tomasin, "Machine learning for intelligent authentication in 5G and beyond wireless networks," *IEEE Wireless Commun.,* vol. 26, no. 5, pp. 55-61, Oct. 2019.

[20] K. Sakai, M. T. Sun, W. S. Ku, and J. Wu, "On anonymous routing in delay tolerant networks," *IEEE Trans. Mobile Comput.,* vol. 18, no. 12, pp. 2926-2940, Dec. 2019.

[21] M. Yang, J. Luo, Z. Ling, X. Fu, and W. Yu, "De-anonymizing and countermeasures in anonymous communication networks," *IEEE Commu. Mag.*, vol. 53, no. 4, pp. 60-66, Apr. 2015.

[22] Y. Wei and S. Ulukus, "The capacity of private information retrieval with private side information under storage constraints," *IEEE Trans. Inf. Theory*, vol. 66, no. 4, pp. 2023–2031, Apr. 2020.

[23] Y. Wu, X. Gao, S. Zhou, W. Yang, Y. Polyanskiy, and G. Caire, "Massive access for future wireless communication systems," *IEEE Wireless Commun.*, vol. 27, issue. 4, pp. 148-156, Aug. 2020.

[24] S. Ali, N. Rajatheva, and W. Saad, "Fast uplink grant for machine type communications: challenges and opportunities," *IEEE Commun. Mag.*, vol. 57, no. 3, pp. 97-103, Mar. 2019.

[25] C. Chou, D. Wei, C. J, Kuo, and K. Naik, "An efficient anonymous communication protocol for peer-to-peer applications over mobile ad-hoc networks," *IEEE J. Sel. Areas Commun.,* vol. 25, no. 1, pp. 192-203, Jan. 2007.

[26] Y. C. Liang, Y. Zeng, E. C. Y. Peh, and A. T. Hoang, "Sensing-throughput trade-off for cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 4, pp. 1326-1337, Apr. 2008.

[27] Y. Zeng and Y. C. Liang, "Eigenvalue-based spectrum sensing algorithms for cognitive radio," *IEEE Trans. Commun.*, vol. 57, no. 6, pp. 1784-1793, Jun. 2009.

[28] M. Kosunen, V. Turunen, K. Kokkinen, and J. Ryynanen, "Survey and analysis of cyclostationary signal detector implementations on FPGA," *IEEE J. Emerg. Sel. Topic Circuits Syst.*, vol. 3, no. 4, pp. 541-551, Dec. 2013.

[29] H. V. Poor, *An Introduction to Signal Detection and Estimation-2nd Edition*. Springer-Verlag: New York NY, 1994.

[30] M. Arakawa, Computational workloads for commonly used signal processing kernels, project report ESC-TR-2006-071, MIT, U.S.A., 2006.

[31] A. Shaverdian and M. R. Nakhai, "Robust distributed beamforming with interference coordination in downlink cellular networks," *IEEE Trans. Commun.*, vol. 62, no. 7, pp. 2411-2421, Jul. 2014.

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

[33] Y. Huang and Daniel P. Palomar, "Rank-constrained separable semidefinite programming with applications to optimal beamforming," *IEEE Trans. Signal Process.*, vol. 58, no. 2, pp. 664-678, Feb. 2010.

[34] C. Masouros, T. Rntnarajah, and A. K. S. Qinetiq, "Known interference in the cellular downlink: a performance limiting factor or a source of green signal power?" *IEEE Commun. Mag.*, vol. 51, no. 10, pp. 162-171, Oct. 2013.

[35] Z. Wei, C. Masouros, K. Wong, and X. Kang, "Multi-cell interference exploitation: enhancing the power efficiency in cell coordination," *IEEE Trans. Wireless Commun.*, vol. 19, no. 1, pp. 547-562, Jan. 2020.

[36] C. Masouros and G. Zheng, "Exploiting known interference as green signal power for downlink beamforming optimization," *IEEE Trans. Sig. Proc.*, vol. 63, no. 14, pp. 3668-3680, Jul. 2015.

[37] K. Wang, W. Ma, and C. Chi, "Outage constrained robust transmit optimization for multiuser MISO downlinks: tractable approximations by conic optimization," *IEEE Trans. Antenna Propagat.*, vol. 62, no. 21, pp. 5690-5715, Nov. 2014.

[38] D. Tse and P. Viswanath, *Fundamentals of Wireless Communications,* Cambridge University Press: Cambridge, UK, 2005.

[39] C. B. Peel *et al.*, "A vector-perturbation technique for near-capacity multi-antenna multiuser communication—part I: channel inversion and regularization," *IEEE Trans. Wireless Commun.*, vol. 53, no. 1, pp. 195-202, Jan. 2005.

[40] A. Li and C. Masouros, "Interference exploitation precoding made practical: optimal closed-form solution for PSK modulations," *IEEE Trans. Wireless Commun.*, vol. 17, no. 11, pp. 7661-7676, Sept. 2018.

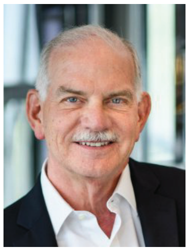
[41] Y. Sun, D. W. K. Ng, J. Zhu, and R. Schober, "Multi-objective optimization for robust power efficient and secure full-duplex wireless communication systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5511-5526, Aug. 2016.

Zhongxiang Wei (S'15–M'17) received the Ph.D. degree in electrical and electronics engineering from the University of Liverpool, Liverpool, U.K., in 2017. From March 2016 to March 2017, he was with the Institution for Infocomm Research, Agency for Science, Technology and Research, Singapore, as a Research Assistant. From March 2017 to October 2017, he was a Visiting Student with the Wireless Networks and Communications Group, Harbin Institute of Technology (HIT), Shenzhen, China. From March 2018 to March 2021, he was with the department of electrical and electronics engineering, University College London, as a research associate. He is currently an associate professor at Tongji University, China. He has authored and co-authored more than 50 research papers published on top-tier journals and international conferences. His research interests include anonymous communications, constructive interference design, millimeter-wave communications, and algorithm design. He has acted as a TPC member or the Session Chair of various international conferences. He was a recipient of an Exemplary Reviewer of the IEEE TWC in 2016, the Outstanding Self-Financed Students Abroad in 2018, and the A*STAR Research Attachment Programme (ARAP) in 2016.

Fan Liu (Member, IEEE) is currently an Assistant Professor of the Department of Electrical and Electronic Engineering, Southern University of Science and Technology (SUSTech). He received the Ph.D. and the BEng. degrees from Beijing Institute of Technology (BIT), Beijing, China, in 2018 and 2013, respectively. He has previously held academic positions in the University College London (UCL), firstly as a Visiting Researcher from 2016 to 2018, and then as a Marie Curie Research Fellow from 2018 to 2020. He was the recipient of the Best Ph.D. Thesis Award of Chinese Institute of Electronics in 2019, the Marie Curie Individual Fellowship in 2018, and has been named as an Exemplary Reviewer for several IEEE Journals. He is an Associate Editor of the IEEE Communications Letters, a Lead Guest Editor of the IEEE Journal on Selected Areas in Communications (JSAC) Special Issue on "Integrated Sensing and Communications (ISAC)", and Academic Chair of the IEEE ComSoc ISAC Emerging Technology Initiative (ISAC-ETI). He has served as the organizer and Co-Chair for several workshops, special sessions and tutorials in flagship IEEE conferences. His research interests include ISAC, vehicular network and intelligent transportation, and mmWave communications.

Christos Masouros (SMIEEE, MIET) received the Diploma degree in Electrical and Computer Engineering from the University of Patras, Greece, in 2004, and MSc by research and PhD in Electrical and Electronic Engineering from the University of Manchester, UK in 2006 and 2009 respectively. In 2008 he was a research intern at Philips Research Labs, UK. Between 2009-2010 he was a Research Associate in the University of Manchester and between 2010-2012 a Research Fellow in Queen's University Belfast. In 2012 he joined University College London as a Lecturer. He has held a Royal Academy of Engineering Research Fellowship between 2011-2016.

Since 2019 he is a Full Professor of Signal Processing and Wireless Communications in the Information and Communications Engineering research group, Dept. Electrical and Electronic Engineering, University College London. His research interests lie in the field of wireless communications and signal processing with particular focus on Green Communications, Large Scale Antenna Systems, Integrated Sensing and Communications, interference mitigation techniques for MIMO and multicarrier communications. He was the recipient of the Best Paper Awards in the IEEE GlobeCom 2015 and IEEE WCNC 2019 conferences, and has been recognized as an Exemplary Editor for the IEEE Communications Letters, and as an Exemplary Reviewer for the IEEE Transactions on Communications. He is an Editor for IEEE Transactions on Communications, IEEE Transactions on Wireless Communications, the IEEE Open Journal of Signal Processing, and Editor-at-Large for IEEE Open Journal of the Communications Society. He has been an Associate Editor for IEEE Communications Letters, and a Guest Editor for a number of IEEE Journal on Selected Topics in Signal Processing issues. He is a founding member and Vice-Chair of the IEEE Emerging Technology Initiative on Integrated Sensing and Communications, Vice Chair of the IEEE Special Interest Group on Integrated Sensing and Communications, and Chair of the IEEE Special Interest Group on Energy Harvesting.



H. Vincent Poor (S'72, M'77, SM'82, F'87) received the Ph.D. degree in EECS from Princeton University in 1977. From 1977 until 1990, he was on the faculty of the University of Illinois at Urbana-Champaign. Since 1990 he has been on the faculty at Princeton, where he is currently the Michael Henry Strater University Professor. During 2006 to 2016, he served as the dean of Princeton's School of Engineering and Applied Science. He has also held visiting appointments at several other universities, including most recently at Berkeley and Cambridge. His research interests are in the areas of information theory, machine learning and network science, and their applications in wireless networks, energy systems and related fields. Among his publications in these areas is the forthcoming book Machine Learning and Wireless Communications. (Cambridge University Press, 2021).

Dr. Poor is a member of the National Academy of Engineering and the National Academy of Sciences and is a foreign member of the Chinese Academy of Sciences, the Royal Society, and other national and international academies. Recent recognition of his work includes the 2017 IEEE Alexander Graham Bell Medal and a D.Eng. honoris causa from the University of Waterloo awarded in 2019.