Unitary Modulation for Secrecy Enhancement in Multi-antenna Wireless Systems with Only CSIT

Pang-Chang Lan[†], Y.-W. Peter Hong[⋆], Tze-Ping Low[+], and C.-C. Jay Kuo[†]

[†]Ming Hsieh Department of Electrical Engineering, University of Southern California, Los Angeles, CA 90089-2564, USA
[⋆]Institute of Communications Engineering, National Tsing Hua University, Hsinchu, Taiwan 30013
[+]MediaTek USA Inc., Woburn, MA 01801-1130, USA
Emails: pangchal@usc.edu; ywhong@ee.nthu.edu.tw; tze-ping.low@mediatek.com; cckuo@sipi.usc.edu

***Abstract*—This work proposes the use of a unitary modulation scheme to enhance physical layer secrecy in multi-antenna wireless systems. The proposed scheme takes advantage of having only channel state information at the transmitter (CSIT) but not at the receiver and the eavesdropper. With CSIT, the transmitter can first take the LQ or singular value decomposition of the channel matrix and then replace its unitary component by an information-bearing unitary matrix symbol. When the SNR is sufficiently high, the legitimate receiver is able to extract the unitary matrix by exploiting the uniqueness of the matrix decomposition. But the eavesdropper is incapable of doing so due to the ambiguity caused by the unknown unitary rotation on its channel, which ensures zero information leakage to the eavesdropper when the channels are independent. A detection scheme based on the chordal distance is proposed, and the achievable secrecy rate is derived and shown to depend only on the mutual information of the main channel. The simulation results demonstrate the effectiveness and secrecy advantages of our proposed unitary modulation scheme.**

I. Introduction

Security in wireless communication systems has received much attention in recent years due to the increasing emphases on providing user privacy and data confidentiality. In addition to conventional cryptographic approaches, recent studies on physical layer secrecy, mainly originating from the pioneering works by Wyner in [1] and Csiszár and Körner in [2], demonstrated the possibility and effectiveness of using channel coding and signal processing techniques to provide secure communication links between legitimate terminals. The performance is often measured by the so-called secrecy rate, which is defined as the rate that can be achieved on the secure link subject to asymptotically zero error probability at the legitimate receiver and vanishing information rate at the eavesdropper as the codeword length increases. These techniques complement conventional cryptographic approaches and help resolve issues regarding key distribution and user authentication in the initialization stage of symmetric-key cryptosystems.

Knowledge of the channel state information (CSI) has a deciding factor on the physical layer secrecy performance. In practice, CSI at the receiver and the eavesdropper (CSIRE) is typically obtained through pilot-assisted training from the transmitter, and CSI at the transmitter (CSIT) is obtained through feedback from the receiver and/or the eavesdropper. Many works in the literature, e.g., [3]–[6], assumed the availability of CSI at all terminals and showed that positive secrecy rates can be achieved by encoding over spatial and temporal dimensions in which the main channel (i.e., the channel between the transmitter and the legitimate receiver) is more favorable than the eavesdropper channel. Interestingly, it was shown more recently in [7] that higher secrecy rates can, in fact, be achieved in wiretap channels with only main-channel CSIT and no CSIRE. In reciprocal channels, this channel knowledge assumption can be achieved by having the receiver emit the pilot signal and the transmitter directly estimate the channel. In non-reciprocal channels, an additional round-trip training is required [8], [9]. However, the proposed schemes in [7] focus on cases with the single-antenna receiver and eavesdropper and demonstrate the secrecy advantages based on Gaussian input, which may not be the best choice.

In this paper, we propose the use of unitary modulation to exploit the advantages of having only main-channel CSIT (and no CSIRE) in multi-antenna wireless systems. With main-channel CSIT, the transmitter can first take the LQ or singular value decomposition (SVD) of the main-channel channel matrix and then replace the right unitary component of the channel by an information-bearing unitary matrix symbol. Due to the uniqueness of the matrix decompositions, the receiver is able to extract the information-bearing matrix by carrying out a similar decomposition when the SNR is sufficient high. A detection method is proposed for the receiver based on the chordal distance metric. However, the eavesdropper will be hindered from obtaining secret information due to ambiguities caused by the unknown unitary rotation embedded in its own channel matrix. It is interesting to note that when the main channel is independent of the eavesdropper channel, the mutual information on the eavesdropper channel becomes zero. The achievable secrecy rate is then equal to the achievable rate of a point-to-point channel. This implies that no wiretap code is needed to ensure secrecy against the eavesdropper, making it easier to incorporate the proposed scheme into existing systems and to avoid challenges in the wiretap code design. The secrecy rate performance then also becomes independent of the eavesdropper channel quality. We derive achievable secrecy rate with uniformly random unitary

Part of the work by Y.-W. Peter Hong is supported by Industrial Technology Research Institute, Taiwan, under grant E301AR2900.

978-1-4673-6305-1/15/$31.00 ©2015 IEEE

matrices as the channel input. Computer simulations based on the Spatial Channel Model Extended (SCME) [10] is provided to demonstrate the effectiveness of the proposed scheme.

Notation: We use bold uppercase and bold lowercase alphabets to denote matrices and vectors, respectively, and let $\mathbf{A}_{ij}$ denote the (i, j)-th of $\mathbf{A}$. Let $\mathbb{R}^{m\times n}$ and $\mathbb{C}^{m\times n}$ denote respectively the $m \times n$ real and complex matrix spaces. Let $V_k(\mathbb{C}^n)$ denote the complex Stiefel manifold of orthonormal k frames in $\mathbb{C}^n$, i.e., $\mathbf{T} \in V_k(\mathbb{C}^n)$ is a $n \times k$ matrix with orthonormal columns. For the matrix operations, $(\cdot)^T$ stands for transpose, $(\cdot)^H$ stands for conjugate transpose, $(\cdot)^\dagger$ stands for pseudo-inverse, $\mathrm{tr}(\cdot)$ denotes the trace operation, $\otimes$ denotes the Kronecker product, $\mathrm{vec}(\cdot)$ denotes the vectorization operation (i.e., $\mathrm{vec}(\begin{bmatrix}\mathbf{t}_1 & \cdots & \mathbf{t}_n\end{bmatrix}_{m\times n}) = \begin{bmatrix}\mathbf{t}_1^T & \cdots & \mathbf{t}_n^T\end{bmatrix}^T_{1\times mn}$), $\mathrm{diag}(\cdots)$ denotes the diagonalization operation, $\|\cdot\|_2$ denotes the induced matrix 2 norm, and $\|\cdot\|_F$ denotes the Frobenius norm. Let $\mathbf{I}_n$ be the identity matrix with dimension $n \times n$. $\mathcal{CN}(\mathbf{m}, \mathbf{\Sigma})$ denotes the circularly complex Gaussian distribution with mean $\mathbf{m}$ and covariance $\mathbf{\Sigma}$. The matrix distribution $\mathbf{X} \sim \mathcal{CN}(\mathbf{M}, \mathbf{A} \otimes \mathbf{B})$ with $\mathbf{X} \in \mathbb{C}^{m\times n}$, $\mathbf{A} \in \mathbb{C}^{m\times m}$, and $\mathbf{B} \in \mathbb{C}^{n\times n}$ is equivalent to $\mathrm{vec}(\mathbf{X}^T) \sim \mathcal{CN}(\mathrm{vec}(\mathbf{M}^T), \mathbf{A}\otimes\mathbf{B})$ and its pdf is given by [11]

$$f_{\mathbf{X}}(\vec{X}) = \frac{\exp(-\operatorname{tr}(\mathbf{A}^{-1}(\vec{X}-\mathbf{M})\mathbf{B}^{-1}(\vec{X}-\mathbf{M})^H))}{\pi^{mn}\det(\mathbf{A})^n\det(\mathbf{B})^m}. \quad (1)$$

Similar definitions are applied to the real Gaussian random vectors and matrices with the notation $\mathcal{N}(\cdot, \cdot)$.

II. Unitary Modulation Scheme with Only Main-Channel CSIT

Consider a multiple-input multiple-output multi-antenna eavesdropper (MIMOME) wiretap fading channel consisting of a transmitter, a receiver, and an eavesdropper with respectively N, M, and K antennas as shown in Fig. 1. The transmitter modulates the secret information into space-time symbols, denoted by $\mathbf{X} \in \mathbb{C}^{N\times T}$, which spans T time slots and satisfies the average power constraint $\frac{1}{T}E[||\mathbf{X}||_F^2] \leqslant P$. We consider a block fading channel where the channel remains constant during the transmission of a symbol and varies independently from one symbol to another. The received signals at the receiver and the eavesdropper can be written as

$$\begin{aligned}\mathbf{Y} &= \mathbf{HX} + \mathbf{W}\\ \mathbf{Z} &= \mathbf{GX} + \mathbf{W}'\end{aligned} \quad (2)$$

where $\mathbf{H} \in \mathbb{C}^{M\times N}$ and $\mathbf{G} \in \mathbb{C}^{K\times N}$ are independent fading channel matrices with entries that are i.i.d. $\mathcal{CN}(0, \sigma_H^2)$ and $\mathcal{CN}(0, \sigma_G^2)$ respectively (i.e., $\mathbf{H} \sim \mathcal{CN}(\mathbf{0}, \sigma_H^2\mathbf{I}_M \otimes \mathbf{I}_N)$ and $\mathbf{G} \sim \mathcal{CN}(\mathbf{0}, \sigma_G^2\mathbf{I}_K\otimes\mathbf{I}_N)$), and $\mathbf{W} \in \mathbb{C}^{M\times T}$ and $\mathbf{W}' \in \mathbb{C}^{K\times T}$ are additive Gaussian noise matrices with i.i.d. $\mathcal{CN}(0, 1)$ entries (i.e., $\mathbf{W} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_M\otimes\mathbf{I}_T)$ and $\mathbf{W}' \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_K\otimes\mathbf{I}_T)$). Assume that there is only main-channel CSIT and no CSIRE, which can be realized by reversed training in reciprocal channels and with an additional round-trip training in non-reciprocal channels [8].

In the proposed unitary modulation scheme, the transmitter exploits CSIT to precompensate for the unitary rotation on the main channel and enable coherent detection of the information-bearing unitary matrix symbols at the legitimate receiver. However, the symbols must be chosen such that the eavesdropper will not be able to decode the message when the unitary rotation embedded of its own channel is unknown. This is different from the work in [12] where unitary space-time modulation is designed to allow for noncoherent detection at the receiver (i.e., detection without knowledge of the channel). From their perspective, it is necessary to have $T \neq N$. However, this choice of unitary modulation allows for noncoherent detection at the eavesdropper as well. To avoid information leakage, we instead choose input matrices $\mathbf{X}$ with $T = N$ as follows.

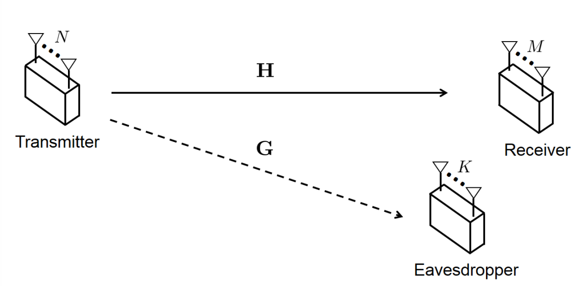

Fig. 1. MIMOME Wiretap Fading Channel

More specifically, with the main-channel CSIT, the transmitter first decomposes the channel matrix into $\mathbf{H} = \mathbf{SQ}$, where $\mathbf{Q} \in \mathbb{C}^{N\times N}$ is a unitary matrix and $\mathbf{S} \in \mathbb{C}^{M\times N}$. Notice that we assume $N > 1$. The decomposition is chosen such that the following criterion is satisfied.

Criterion 1. *For* $\mathbf{H}$ *that is full rank, the decomposition should yield* $\mathbf{Q}$ *whose first* $R \triangleq \min(M, N)$ *rows are unique up to a phase rotation on each row.*

This criterion ensures that the modulated unitary symbol can be reliably restored at the receiver, as to be clear in the following sections. It turns out that both the LQ decomposition and SVD satisfy this criterion. In the following, we focus our discussions on the LQ-based approach, but the procedures can be done similarly with the SVD. In particular, when using the LQ decomposition, $\mathbf{S}$ is simply a lower triangular matrix.

Let $\mathcal{F} = \{\mathbf{F}_1, \cdots, \mathbf{F}_{2^J}\} \subset V_N(\mathbb{C}^N)$ be the set of 2^J N-by-N unitary matrix symbols, which is revealed to all terminals. In practice, the set $\mathcal{F}$ can be chosen as the DFT or householder codebooks already existing in LTE systems or can be specially designed to have the desired distance properties. To modulate the secret message, the transmitter partitions its secret information into binary sequences of length-J and maps each sequence to its corresponding unitary matrix symbol in $\mathcal{F}$. Suppose that $\mathbf{F}$ is the unitary matrix chosen from $\mathcal{F}$ and is to be transmitted. Let the channel input be $\mathbf{X} = \sqrt{P}\mathbf{Q}^H\mathbf{F}$ to precompensate for the right unitary matrix $\mathbf{Q}$ of the main channel. It can be shown that $\mathbf{X}$ indeed satisfies the average power constraint since $\mathbf{Q}^H\mathbf{F}$ is unitary. The corresponding received signal matrices can, thus, be written as

$$\mathbf{Y} = \sqrt{P}\mathbf{S}\mathbf{F} + \mathbf{W}$$
$$\mathbf{Z} = \sqrt{P}\mathbf{G}\mathbf{Q}^H\mathbf{F} + \mathbf{W}'. \tag{3}$$

In the following section, we propose a detection scheme that relies on the uniqueness of the matrix decomposition and on the chordal distance metric. Also, we show that the eavesdropper will not be able to obtain any secret information.

III. Detection of Unitary Matrices based on the Chordal Distance Metric

To retrieve the secret message, the receiver performs the same decomposition on the received signal $\mathbf{Y}$ to obtain $\hat{\mathbf{S}}\hat{\mathbf{F}}$. The estimated symbol $\hat{\mathbf{F}}$ is then mapped to a unitary matrix in the codebook $\mathcal{F}$ according to the shortest distance criterion, i.e., by finding the index $\hat{j}$ such that

$$\hat{j} = \arg\min_{i\in\{1,\cdots,2^J\}} d(\hat{\mathbf{F}}, \mathbf{F}_i) \tag{4}$$

where $d(\cdot,\cdot)$ is a distance metric to be chosen properly. By Criterion 1, the estimated symbol $\hat{\mathbf{F}}$ should be unique up to a phase rotation on each of the first R rows if the channel is noiseless. That is, for the first R rows, each row of $\hat{\mathbf{F}}$ should span the same one-dimensional subspace as the corresponding row in $\mathbf{F}$ if $\mathbf{W} = \mathbf{0}$. Hence, it is necessary to define a distance metric that allows the distance between two matrices to be zero when they differ by only a phase rotation on each row. This property is satisfied with the proposed vector-wise chordal distance metric, which is defined as

$$\mathrm{d_v}(\hat{\mathbf{F}}, \mathbf{F}_i) \triangleq \sqrt{\sum_{n=1}^{R} d_c^2([\hat{\mathbf{F}}^T]_n, [\mathbf{F}_i^T]_n)} \tag{5}$$

where $d_c(\mathbf{v},\mathbf{w}) \triangleq \sqrt{1 - |\mathbf{v}^H\mathbf{w}|^2}$ is the chordal distance between two unit norm vectors $\mathbf{v}$ and $\mathbf{w}$ [13], [14], and $[\mathbf{A}]_n$ represents the n-th column of the matrix $\mathbf{A}$. Note that a good codebook should ensure that for arbitrary R, the distance between every two unitary matrices in the codebook is as large as possible according to the distance metric $\mathrm{d_v}(\cdot,\cdot)$.

In the absence of noise, the vector-wise chordal distance and Criterion 1 ensures perfect reconstruction of the unitary modulation symbol $\mathbf{F}$ at the receiver. In the presence of noise, if the noise $\mathbf{W}$ is sufficiently small and also satisfies $\|\tilde{\mathbf{X}}^\dagger\|_2\|\mathbf{W}\|_2 < 1$ or, equivalently, $\frac{\sigma_{\max}(\mathbf{W})}{\sqrt{P}\sigma_{\min}(\mathbf{H})} < 1$ where $\tilde{\mathbf{X}} \triangleq \sqrt{P}\mathbf{S}\mathbf{F}$ is the signal component, and $\sigma_{\min}(\cdot)$ and $\sigma_{\max}(\cdot)$ denote the maximum and minimum singular values, the error $\Delta\mathbf{F} \triangleq \hat{\mathbf{F}} - \mathbf{F}$ can be bounded by [15]

$$\|\Delta\mathbf{F}\|_F \leqslant \sqrt{2}\|\tilde{\mathbf{X}}^\dagger\|_2\|\mathbf{W}\|_F + O(\frac{\|\mathbf{W}\|_F^2}{\|\tilde{\mathbf{X}}\|_2^2}) \tag{6}$$

$$= \sqrt{\frac{2\sum_{i=1}^R \sigma_i^2(\mathbf{W})}{P\sigma_{\min}^2(\mathbf{H})}} + O(\frac{\sum_{i=1}^R \sigma_i^2(\mathbf{W})}{P\sigma_{\max}^2(\tilde{\mathbf{H}})}). \tag{7}$$

Therefore, $\hat{\mathbf{F}}$ can be made arbitrarily close to $\mathbf{F}$ as the SNR goes to infinity, i.e., as $\frac{NP}{\|\mathbf{W}\|_F^2} \to \infty$. This shows that the unitary modulation is reliable in delivering information to the desired receiver when the SNR is sufficiently high.

In contrast to the reliability at the receiver, the eavesdropper cannot obtain any secret information under the assumption that the main channel and the eavesdropper channel are independent. This is due to the fact that the distribution of $\mathbf{G}$ is invariant to the right-multiplication of an independent unitary matrix. That is, for any unitary matrix $\mathbf{U}$ independent of $\mathbf{G}$, the matrix $\mathbf{G}\mathbf{U}$ has the same distribution as $\mathbf{G}$. Hence, the distributions of $\mathbf{G}\mathbf{Q}^H\mathbf{F}$ (and $\mathbf{Z}$) remains the same regardless of the value of $\mathbf{F}$ being given or not. The mutual information at the eavesdropper then turns out to be

$$I(\mathbf{Z};\mathbf{F}) = h(\mathbf{Z}) - h(\mathbf{Z}|\mathbf{F}) = 0. \tag{8}$$

As a result, the non-coherent detection at the eavesdropper can fail completely because of the unitary modulation.

IV. Achievable Secrecy Rate of the Proposed Unitary Modulation Scheme

In this section, we characterize the achievable secrecy rate of the MIMOME fading wiretap channel in (2) with the proposed LQ-based unitary modulation scheme. To derive the achievable secrecy rate, it is necessary to first obtain, in the following lemmas, the distributions of the matrices obtained from the LQ decomposition of the normalized channel matrix $\tilde{\mathbf{H}} \triangleq \frac{1}{\sigma_H}\mathbf{H} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_M \otimes \mathbf{I}_N)$.

Lemma 1. *A random matrix $\tilde{\mathbf{H}} \in \mathcal{CN}(\mathbf{0}, \mathbf{I}_M \otimes \mathbf{I}_N)$ can be decomposed into the product of* 1) *a lower triangular matrix $\mathbf{L} \in \mathbb{C}^{M\times N}$ with independent entries and* 2) *a uniformly random unitary matrix (a Haar matrix) $\mathbf{Q} \in V_N(\mathbb{C}^N)$ independent of $\mathbf{L}$. In particular, $\sqrt{2}\mathbf{L}_{rr}$ for $r \in \{1,\cdots,R\}$ are independently Chi-distributed with $2(N-r+1)$ degrees of freedom, and $\mathbf{L}_{mn}$ for $m > n$, $m \in \{1,\cdots,M\}$, and $n \in \{1,\cdots,N\}$ are i.i.d. as $\mathcal{CN}(0,1)$.*

For brevity, we omit the proof of the lemma and refer the interested readers to distribution results of real-valued thin QR decomposition in [11], [16] which our proof is closely related to. Lemma 1 implies the distribution of the product of a lower triangular matrix and a unitary matrix with the above distributions. This is described in the following lemma.

Lemma 2. *Suppose that $\mathbf{L} \in \mathbb{C}^{M\times N}$ is a lower triangular matrix with the distribution specified in Lemma 1. Then, for a uniformly random unitary matrix $\mathbf{F} \in V_N(\mathbb{C}^N)$ independent of $\mathbf{L}$, the distribution of $\mathbf{L}\mathbf{F}$ is $\mathcal{CN}(\mathbf{0}, \mathbf{I}_M \otimes \mathbf{I}_N)$.*

The above lemmas show that the LQ decomposition of the channel matrix $\mathbf{H} = \sigma_H\mathbf{H}$ yields matrices $\mathbf{S} = \sigma_H\mathbf{L}$ and $\mathbf{Q}$ with the distributions of $\mathbf{L}$ and $\mathbf{Q}$ described by Lemma 1. Then, by choosing $\mathcal{F}$ to be a set of i.i.d. uniformly random unitary matrices, the effective signal component $\mathbf{S}\mathbf{F}$, where $\mathbf{F} \in \mathcal{F}$, will have distribution that is the same as $\mathbf{H}$. The achievable secrecy rate of the proposed unitary modulation scheme in the MIMOME wiretap channel in (2) can then be bounded in the following theorem.

Theorem 1. *With $\mathcal{F}$ being generated by i.i.d. uniformly random unitary matrices, the achievable secrecy rate of the proposed unitary modulation in the MIMOME wiretap channel in* (6) *and* (7) *can be lower bounded by*

$$R_s \geqslant \begin{cases} \frac{1}{N}\log\left((1+P\sigma_H^2)^{MN-\frac{M(M-1)}{2}}\bar{P}^{-\frac{1}{2}}\right), & \textit{if } N \geqslant M \\ \frac{1}{N}\log\left((1+P\sigma_H^2)^{\frac{N(N-1)}{2})}\bar{P}^{-\frac{1}{2}}\right), & \textit{if } N < M \end{cases} \tag{9}$$

where $\bar{P} \triangleq \prod_{r=1}^{R}\left(1+P\sigma_H^2\left[N-r+1-\frac{\Gamma(N-r+\frac{3}{2})^2}{\Gamma(N-r+1)^2}\right]\right)$.

Proof. According to [2], the achievable secrecy rate can be expressed as

$$R_s = \frac{1}{N}\Big(I(\mathbf{Y};\mathbf{F}) - I(\mathbf{Z};\mathbf{F})\Big) \tag{10}$$

where the $1/N$ factor is for normalization by transmission time since the unitary coded symbol spreads across N slots. Similar to (8), $I(\mathbf{Z};\mathbf{F}) = 0$ since the knowledge of the random unitary matrix $\mathbf{F}$ does not change the distribution of $\mathbf{Z}$. The task is to compute $I(\mathbf{Y};\mathbf{F}) = h(\mathbf{Y}) - h(\mathbf{Y}|\mathbf{F})$.

By Lemma 2, $\mathbf{Y} \in \mathcal{CN}\left(\mathbf{0},(1+P\sigma_H^2)\mathbf{I}_M \otimes \mathbf{I}_N\right)$ and, thus,

$$h(\mathbf{Y}) = h(\mathrm{vec}(\mathbf{Y})) = \log\left(\left[\pi e(1+P\sigma_H^2)\right]^{MN}\right). \tag{11}$$

Given $\mathbf{F}$, on the other hand, we have

$$\begin{aligned} h(\mathbf{Y}|\mathbf{F}) &= h(\sqrt{P}\sigma_H\,\mathrm{diag}(\mathbf{F}^H,\overset{M}{\cdots},\mathbf{F}^H)\mathrm{vec}(\mathbf{L}^H)+\mathrm{vec}(\mathbf{W}^H)|\mathbf{F}) \\ &= h(\sqrt{P}\sigma_H\,\mathrm{vec}(\mathbf{L}^H)+\mathrm{vec}(\mathbf{W}^H)) \\ &= h(\sqrt{P}\sigma_H\,\mathrm{vec}(\mathbf{L})+\mathrm{vec}(\mathbf{W})) \end{aligned} \tag{12}$$

since $\mathrm{diag}(\mathbf{F}^H,\overset{M}{\cdots},\mathbf{F}^H)$ is an unitary matrix, $\mathrm{vec}(\mathbf{W})$ is unitary invariant, and the differential entropy is unchanged by multiplying a known unitary matrix. Note that the diagonal terms in $\mathbf{L}$ are Chi-distributed by Lemma 1. We can upper-bound the entropy by

$$h(\mathbf{Y}|\mathbf{F}) \leqslant h(\sqrt{P}\sigma_H\,\mathrm{vec}(\tilde{\mathbf{L}})+\mathrm{vec}(\mathbf{W})) \tag{13}$$

where $\tilde{\mathbf{L}}$ is $\mathbf{L}$ with diagonal terms $\mathbf{L}_{rr}$ for $r \in \{1,\cdots,R\}$ replaced by real Gaussian random variables $\tilde{\mathbf{L}}_{rr}$ with the same mean and variance as

$$\tilde{\mathbf{L}}_{rr} \sim \mathcal{N}\Big(\frac{\Gamma(N-r+\frac{3}{2})}{\Gamma(N-r+1)}, N-r+1-\frac{\Gamma(N-r+\frac{3}{2})^2}{\Gamma(N-r+1)^2}\Big). \tag{14}$$

Let $\tilde{\mathbf{y}} \triangleq \sqrt{P}\sigma_H \cdot \mathrm{vec}(\tilde{\mathbf{L}}) + \mathrm{vec}(\mathbf{W})$. Then the real and imaginary parts of $\tilde{\mathbf{y}}$, denoted by $\tilde{\mathbf{y}}_R, \tilde{\mathbf{y}}_I \in \mathbb{R}^{MN}$, are independent real Gaussian vectors with independent elements. The respective variance of the elements is given by

$$\sigma^2(\tilde{\mathbf{y}}_{R,i+(j-1)N}) = \begin{cases} 1/2, & \text{if } i > j, \\ \frac{1+P\sigma_H^2\left[N-i+1-\frac{\Gamma(N-i+\frac{3}{2})^2}{\Gamma(N-i+1)^2}\right]}{2}, & \text{if } i = j, \\ (1+P\sigma_H^2)/2, & \text{otherwise;} \end{cases}$$

$$\sigma^2(\tilde{\mathbf{y}}_{I,i+(j-1)N}) = \begin{cases} 1/2, & \text{if } i \geqslant j, \\ (1+P\sigma_H^2)/2, & \text{otherwise} \end{cases} \tag{15}$$

for $i \in \{1,2,\cdots,N\}$ and $j \in \{1,\cdots,M\}$. Therefore, the achievable secrecy rate has the lower bound given by

$$R_s = \frac{h(\mathbf{Y}) - h(\mathbf{Y}|\mathbf{F})}{N} \geqslant \frac{h(\mathbf{Y}) - h(\tilde{\mathbf{y}})}{N} \tag{16}$$

which is exactly (9). □

Assume that M fixed and $N \to \infty$. The diagonal elements of $\mathbf{L}$ can be approximated by real Gaussian as [17]

$$\left(2\mathbf{L}_{rr} - \sqrt{4(N-r+1)-1}\right) \to_d \mathcal{N}(0,1) \tag{17}$$

for $r \in \{1,\cdots,R\}$. This implies that the upper bound in (13) is asymptotically tight with fixed M and increasing N and that asymptotically $\sigma^2(\tilde{\mathbf{L}}_{rr}) \to \frac{1}{4}$. The asymptotic lower bound of achievable secrecy rate can then be written as

$$Rs \geqslant \log(1+P\sigma_H^2)^M \tag{18}$$

as $N \to \infty$. Comparing the result with the point-to-point MIMO channel capacity under constant power allocation with only CSIR and no CSIT, we have

$$\begin{aligned} C_{\text{MIMO}} &= \mathrm{E}[\log\det(\mathbf{I}_M + \frac{P}{N}\mathbf{H}\mathbf{H}^H)] \\ &\leqslant \log\det(\mathbf{I}_M + \frac{P}{N}\mathrm{E}[\mathbf{H}\mathbf{H}^H]) \\ &\leqslant \log(1+P\sigma_H^2)^M \underset{N\to\infty}{\leqslant} R_s \end{aligned} \tag{19}$$

where the inequality is owing to the concavity of the $\log\det$ function. Here the eavesdropper is absent in the point-to-point MIMO channel. Note that the point-to-point MIMO channel capacity with only CSIR is, in fact, the upper bound of the secrecy capacity of the MIMOME wiretap channel with only CSIRE since the existence of the eavesdropper will lower the transmission rate. We conclude this result in the following corollary.

Corollary 1. *As M fixed and $N \to \infty$, the achievable secrecy rate for the MIMOME wiretap channel with only main-channel CSIT and no CSIRE is greater than that with only CSIRE and no CSIT.*

V. Simulation Results

In this section, we show simulation results to support the proposed unitary modulation scheme. The results are divided into two parts, experiments on achievable secrecy rates and those on link level simulations based on SCME.

A. Experiments on Achievable Secrecy Rates

Consider the MIMOME wiretap channel defined in Section II. Let $\sigma_H^2 = \sigma_G^2 = 1$ and the numbers of antennas be $M = N = K = 4$. Fig. 2 shows the achievable secrecy rates of 1) the unitary modulation scheme with only main-channel CSIT and 2) the full CSIRE scheme with main-channel CSIT and full CSIRE. By full CSIRE, the receiver and the eavesdropper are supposed to have their respective CSI $\mathbf{H}$ and $\mathbf{G}$. In the full CSIRE scheme, we assume that the transmitter chooses the best MIMO subchannel to transmit the information bearing signals while putting artificial noises

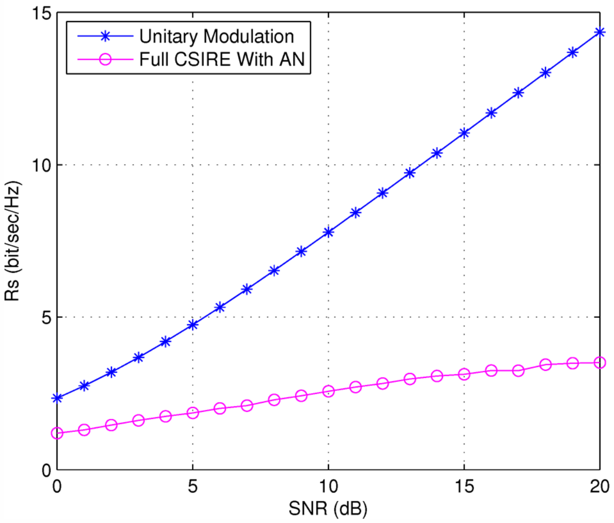

Fig. 2. Achievable secrecy rate R_s versus SNR P.

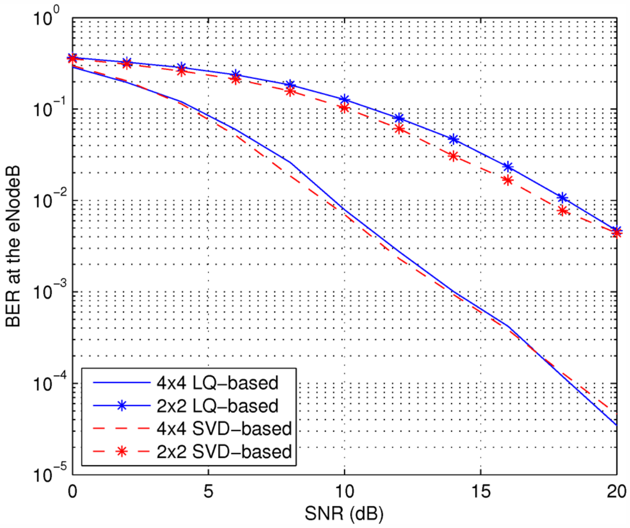

Fig. 3. eNodeB's BER versus SNR P under SCME.

Parameter	Value
Channel Model	SCME
Channel Scenario	Urban Macro
MIMO	2×2 and 4×4
Center Frequency	2 GHz
Subcarrier Bandwidth	15 kHz
Precoding Codebook	DFT for 2×2 MIMO Householder for 4×4 MIMO
UE Speed	8.3 m/s
Antenna Pattern	Two Dual-polarized Elements for 4 Antennas One Dual-polarized Element for 2 Antennas
Antenna Spacing	4 Wavelengths Spacing for eNodeB 2 Wavelengths Spacing for UE
Antenna Slanted Dipole	45 and -45 Degree for eNodeB 0 and 90 Degree for UE

TABLE I
SIMULATION SETTINGS

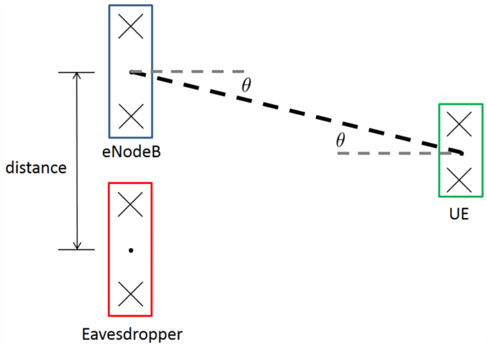

Fig. 4. Illustration of the UE-to-eNodeB angle and the eavesdropper-to-eNodeB distance for 4×4 MIMO.

(AN) on the rest of the subchannels. This is a special case of the MIMO antenna selection [18]. The receiver is assumed to know the subchannels carrying AN. The result demonstrates that the unitary modulation scheme provides a much higher secrecy rate than the full CSIRE scheme.

B. Link Level Experiments based on SCME

Consider the uplink scenario in LTE where a UE sends secret messages such as secret keys and user authentication data to a eNodeB in the initiation stage of the symmetric cryptosystems. Assume that the UE and eNodeB apply the unitary modulation and detection scheme introduced in Section II and III to complement the cryptographic approaches. Simulation settings are provided in Table I based on LTE TS36.211 [19] and TR25.996 [20]. As illustrated in Fig. 4 for the 4×4 MIMO, the broadsides of the antenna arrays of the eNodeB and the UE are set parallel, and the angle θ is set to 30 degrees. Similar assumptions are made for the 2×2 MIMO case except that there is only one dual-dipole antenna pair at each terminal. Note that the 2×2 MIMO system uses 2-bit (4 indices) DFT codebooks while the 4×4 MIMO system uses 4-bit (16 indices) Householder codebook. By such a codebook setting, the transmission rates of the 2×2 and 4×4 unitary modulation schemes are the same as one bit per resource element. We use the simulator, MATLAB implementation of the 3GPP Spatial Channel Model Extended (SCME) provided by [10].

In Fig. 3, we investigate the reliability of the unitary modulation scheme at the legitimate receiver, the eNodeB, without considering the eavesdropper. A BER as low as 10^{-4} can be achieved with SNR about 18dB. It can be seen that the 4×4 unitary modulation scheme has a comparatively low BER with respective to the 2×2 scheme. This shows that adding more antennas can provide the unitary modulation scheme a better tolerance for noises under the same transmission rate.

Next, we examine the eavesdropper's capability of breaking the proposed unitary modulation scheme. Assume that the eavesdropper has the same detector and antenna settings as the eNodeB. If the eavesdropper channel is highly correlated to the main channel, the eavesdropper will then have a better opportunity to obtain the secret message. We focus on the

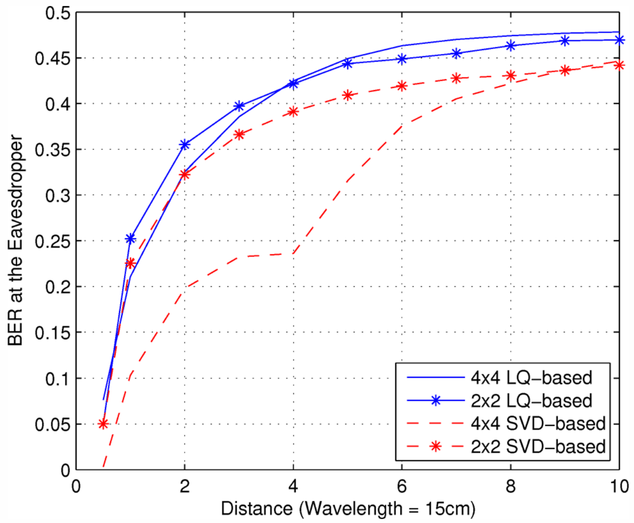

Fig. 5. Eavesdropper's BER versus the eavesdropper-to-eNodeB distance under SCME.

influence of the channel correlation caused by the distance between the eNodeB and the eavesdropper and assume that the received signals at the eavesdropper do not experience any noises, i.e., $\mathbf{W}' = \mathbf{0}$. The eavesdropper-to-eNodeB distance is illustrated in Fig. 4 for the 4×4 MIMO case. The 2×2 MIMO case follows a similar setting with only one dual-dipole antenna pair at each terminal. Fig. 5 shows the BER at the eavesdropper with respect to the distance in wavelengths between the eavesdropper and the eNodeB. Note that for a $2\mathrm{GHz}$ center frequency, the wavelength is approximately $15\mathrm{cm}$. It can be observed that the 2×2 MIMO system provides worse BER at the eavesdropper than the 4×4 system. The reason is that the eNodeB and the eavesdropper in the 4×4 MIMO system have two dual-polarized elements separated by 4 wavelengths. In comparison with the 2×2 case, the antenna separation in the 4×4 MIMO results in higher correlation between the main channel and the eavesdropper channel given the same eavesdropper-to-eNodeB distance. The overall BER at the eavesdropper with a distance over 10 wavelengths or $1.5\mathrm{m}$ approaches 0.5. We argue that within such a short distance, the eavesdropper may expose its position to the eNodeB which can take corresponding actions to prevent eavesdropping. This demonstrate that the unitary modulation scheme is an effective technique to enhance secrecy.

VI. Conclusions

In this work, we proposed a unitary modulation scheme to enhance secrecy in multi-antenna systems by exploiting CSIT in the absence of CSIRE. With CSIT, the transmitter first takes the LQ decomposition of the channel matrix and precompensates for the unitary component in its transmit signal. Then, the secret message is embedded in an information-bearing unitary matrix symbol that is transmitted to the legitimate receiver over the precompensated channel. The receiver will be able to reconstruct the symbol by taking the same matrix decomposition, but the eavesdropper will not due to the ambiguity caused by the unknown unitary rotation of its own channel. A detector based on the chordal distance metric was proposed and a lower-bound on the achievable secrecy rate was derived. The achievable secrecy rate of the proposed scheme was shown to asymptotically approach the point-to-point MIMO capacity with CSIR only. The simulation results validated the theoretical claims and also showed the robustness of the proposed scheme to correlations on the main and the eavesdropper channels.

References

[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[2] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.

[3] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Info. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[4] Y. Liang, H. Poor, and S. Shamai(Shitz), "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[5] A. Khisti and G. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[6] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[7] P.-C. Lan, Y.-W. P. Hong, and C.-C. J. Kuo, "Enhancing secrecy in fading wiretap channels with only transmitter-side channel state information," in *Proceedings of IEEE Global Communications Conference (Globecom) Workshop*, 2014.

[8] C.-W. Huang, T.-H. Chang, X. Zhou, and Y.-W. P. Hong, "Two-way training for discriminatory channel estimation in wireless MIMO systems," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2724–2738, May 2013.

[9] L. P. Withers, R. M. Taylor, and D. M. Warme, "Echo-MIMO: A two-way channel training method for matched cooperative beamforming," *IEEE Trans. Signal Process.*, vol. 56, no. 9, pp. 4419–4432, Sep. 2008.

[10] J. Salo, G. Del Galdo, J. Salmi, P. Kyösti, M. Milojevic, D. Laselva, and C. Schneider, "MATLAB implementation of the interim channel model for beyond-3G systems (SCME)," Online, May 2005, http://www.tkk.fi/Units/Radio/scm/.

[11] R. B. Muirhead, *Aspects of Multivariate Statistical Theory*. NY, USA: John Wiley & Sons, 1982.

[12] B. M. Hochwald and T. L. Marzetta, "Unitary space-time modulation for multiple-antenna communication in Rayleigh flat fading," *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 543–564, Mar. 2000.

[13] J. H. Conway, R. H. Hardin, and N. J. A. Sloane, "Packing lines, planes, etc.: Packings in Grassmannian spaces," *Experiment Math*, vol. 5, no. 2, pp. 139–159, 1996.

[14] A. Barg and D. Y. Nogin, "Bounds on packings of spheres in the grassmann manifold," *IEEE Trans. Inf. Theory*, vol. 48, no. 9, pp. 2450–2454, Sep. 2002.

[15] X. Chang, C. Paige, and G. Stewart, "Perturbation analyses for the QR factorization," *SIAM Journal on Matrix Analysis and Applications*, vol. 18, no. 3, pp. 775–791, 1997.

[16] A. K. Gupta and D. K. Nagar, *Matrix Variate Distributions*. FL, USA: Chapman & Hall/CRC, 2000.

[17] G. A. Korn and T. M. Korn, *Mathematical Handbook for Scientists and Engineers*. NY, USA: McGraw-Hill, Inc, 1968.

[18] S. Sanayei and A. Nosratinia, "Antenna selection in MIMO systems," *IEEE Commun. Mag.*, vol. 42, no. 10, pp. 68–73, Oct. 2004.

[19] *3GPP TS 36.211 V9.0.0*, 3GPP RAN1 RP-60, 3rd Generation Partnership Project Std., 2013.

[20] *3GPP TR 25.996 V9.0.0*, 3GPP RAN1 SP-46, 3rd Generation Partnership Project Std., 2009.