Secret Key Exchange using Private Random Precoding in MIMO FDD and TDD Systems

DOI:
10.1109/TVT.2016.2611565

Document Version
Accepted author manuscript

Secret Key Exchange using Private Random Precoding in MIMO FDD and TDD Systems

Hasan Taha, *Student Member, IEEE,* Emad Alsusa, *Senior Member, IEEE*

***Abstract*—Along with the ongoing evolution of multiple antennas communication systems, new physical layer security techniques are continuing to achieve higher levels of secrecy. Most physical layer approaches, however, concern time division duplex (TDD) channels which rely on using the channel reciprocity feature as a shared randomness, and tend to be associated with a large computational burden. In this paper, we propose a new physical layer method which utilizes private random precoding for exchanging the secret key bits in multiple-input multiple-output (MIMO) systems. The principle of this method is to exploit the precoding matrix index (PMI) in a manner that produces low correlation at the adversary. A robust key exchange between the transmitter and the receiver is established by uniquely relating the secret key bits to the channel precoding matrix using a private version of the universal codebooks. What's more is that the proposed method is applicable in, both, frequency division duplex (FDD) and TDD channels. The results demonstrate that the proposed method can offer superior performance in terms of the key agreement, secrecy level and computational load.**

***Index Terms*—FDD, MIMO precoding, physical layer security, TDD, secret key exchange.**

I. Introduction

CRYPTOGRAPHY concerns preserving data integrity and includes two main secure transmission schemes, namely the asymmetric (also known as the public key cryptography) and the symmetric ciphers. Asymmetric ciphers rely on the use of the exponential data exchange method that raises a set of prime numbers to specific powers to make the mathematical attack overwhelming [1]. The main drawback of this method however is the required additional resources for the potential complex computations if the eavesdropper's hardware gain is much higher than that of the legitimate node. In this case, symmetric ciphers with private shared keys are preferred [2], but the exchange of the secret key is done by the public key exchange with a third party authenticator [3], [4]. The presence of a third party is limited, or may not exist in the decentralized network topologies, such as the vehicular networks (vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V)), not to mention that the the transmitted power is also relatively low. For this reason, it is more practical to employ physical layer security techniques to equip each node with a higher secrecy level without the burden of excessive complexity relative to the public key cryptography.

A. Related Work

Physical layer security utilizes the open air characteristics particularly in point-to-point models to establish a secure link. Motivated by the results of the theoretical analysis, [5]-[8], practical models focused on examining the possibility to use the reciprocal radio channel variation to effectively create a secure data exchange. It was shown that the channel coefficients between two nodes operating at the same frequency, as in the case of time division duplex (TDD) systems, are highly correlated random variables and can be easily used by symmetric ciphers to establish a secret key. Many researchers have proposed methods for establishing a secret key based on quantizing different aspects of the channel coefficients, such as the magnitude, phase, or both [9]-[11]. Recent works have included some techniques for multiple-input multiple-output (MIMO) systems with increased secret key length and lower key bits disagreement which is commonly known as the key error rate (KER), [12]-[14]. Moreover, in [15], secret bits are generated using a probabilistic channel quantization approach (CQA) of the real and imaginary parts with channel decorrelation process to generate independent sequential quantized values. Another popular approach is based on establishing security measures through exploiting the MIMO precoding matrix index (PMI) [16], [17]. In [17], the authors have demonstrated good KER improvements through a PMI based method called the MIMO-OFDM physical-layer rotated reference technique (MOPRO), which relied on using the singular value decomposition (SVD) for precoding and the minimum mean square error (MMSE) criterion for the PMI detection. In general, the drawback of such techniques is that they require relatively high computations per byte per secret key especially for the channel decomposition stage. The authors in [18] proposed two methods for secret key generation that utilize the differential and channel-hopping algorithms. However, the strong reliance on the reciprocal channel concept will generate correlated secret bit sequences that may degrade the randomness of the secret bits and the secrecy level in low mobility as proved later. The authors in [19] proposed a parasitic antenna array technique to exchange the secret key. Techniques like this however require the availability of more than eight multiple antennas on the same terminal and high signal-to-noise ratio (SNR) values to ensure good KER performance.

In frequency division duplex (FDD) systems the channel reciprocity assumption is no longer valid because the uplink and downlink channels operate at far-spaced radio frequencies. However, since the electromagnetic waves are assumed to experience similar propagation paths, reciprocity will still exist in terms of the signal's time of arrival (ToA), angle of departure (AoD) and angle of arrival (AoA) [20], [21]. Nonetheless, a successful time and phase estimation of the ToA and AoD are possible only with clock synchronization

The authors are with the School of Electrical and Electronic Engineering, University of Manchester, Manchester M13 9PL, U.K. (e-mail: hasan.taha@manchester.ac.uk; emad.alsusa@manchester.ac.uk).

schemes and specially configured antennas. With this in mind, in [22], a secret key generation method was proposed based on the Chinese remainder theorem (CR) applied on the angle of the received signal path where complex extraction of a shared reciprocal delay profile is highly related to the mobility effect of the transmitter and/or the receiver. In [23], the authors proposed pilot transmission in a feed back scheme to estimate a combination of the uplink (UL) and downlink (DL) channels in order to share the random secret basis. In this method, the transmitter sends a pilot and the intended receiver feeds the pilot signal back. The same procedure is repeated at the receiver. The difficulty of placing these pilots in a narrow time period less than the coherence time is constrained by the multiple user scheduling process and the mobility rate. Besides, longer lengths of random secret bits require repeating the estimation process with a time gap larger than the coherence time, which degrades the spectral efficiency especially in low mobility conditions. Considering the same concept, in [24], a simplified version of the latter method was proposed, but the computations to enhance the estimation process and reduce the accumulated noise increase the computational burden due to larger power deviations which can potentially worsen the channel estimation error.

B. Main Contribution

For a time varying channel, such as the V2I model, to secure the communication link with a shared secret key established using the channel characteristics at both sides of the communication link requires constant update whenever there is a change. As a result, the feedback overhead increases as a function of the product of the number of antennas at both communicating nodes. Therefore, establishing secret key exchange based on full channel knowledge is not practical especially for systems with a limited channel capacity. It is desirable to design a secret key exchange technique that can achieve the potential gains of physical layer security in TDD and FDD time varying channels without significantly compromising the link capacity.

To this end, we propose a new physical layer method that uses Private Random Precoding (PRP) to achieve a secure communication link. The proposed scheme manipulates conventional MIMO precoding to establish a successful secret key exchange by collecting the private indexes of the precoding codewords within three major procedural phases. The first phase is responsible of finding a shared randomness between the transmitter and the receiver which can be done through sending private preambles that are assigned to each of the possible precoding matrices of the codebook. Based on the receiver's feedback, the second phase is used to produce a private secure version of the public codebook by rotating the index assignments in the codebook. The third phase generates a random seed of a full length secret key and transmits each chunk of bits as an assignment of the precoder index. The receiver collects the secret key bits of each successful index detection and concatenates the assigned index after translating it to its private version. Moreover, we propose two maximum likelihood (ML) methods for the *Soft* and *Hard* precoding index detection. Soft detection is used at the receiver when it has a good link quality and low physical path perturbation, which tends to be the case exist with line of sight communications or low path-loss environment. On the other hand, Hard detection is used for the receivers located far apart from the transmitter and/or have low SNR where the additive noise components widen the Soft detection boundary. For the best achievable performance gain, the receiver decides to switch between the two detectors with each received signal SNR value as a threshold indicator, in order to calibrate its KER performance with the desired level of interest.

We investigate the practical aspects of the proposed PRP method and compare it with other existing benchmarks. It will be shown that the PRP method can achieve good KER performance with very low computational burden and higher secrecy level at different mobile speeds. The results show that the PRP method provides better secrecy levels of randomness and smaller number of vulnerable bits in the case of the correlated wiretap channel with low complexity relative to the aforementioned benchmark techniques. Overall we show that our technique performs well under various system scenarios and that it is also applicable in devices supported only with low Open System Interconnection (OSI) layers. Furthermore, it will be shown that the technique benefits from MIMO spatial diversity with higher orders of antenna systems and is also applicable in FDD and TDD systems alike.

C. Organization and Notations

The rest of the paper is organized as follows. Section II, introduces the system model while Section III presents the proposed algorithm. Section IV includes an information theoretic analysis. Simulation results are discussed in Section V and conclusions in Section VI.

Table I shows the given notations that will be used in this paper.

TABLE I
NOTATIONS CONVENTION

Symbol	Description
x	Scalar
$\mathbf{x}$, $\mathbf{X}$	Vector and matrix
x_i	Vector/Matrix component
$(\cdot)^*$	Complex conjugate
$\mathbf{x} \cdot \mathbf{x}$	Element-wise product of two vectors
$(\cdot)^T$	Matrix transpose
$(\cdot)^\dagger$	Matrix conjugate transpose (Hermitian)
$\mathbf{I}$	Identity matrix (size is deduced from the context)
$h(\cdot)$	Differential entropy
$h(X,Y)$	Differential entropy of jointly distributed random variables
$h(X\|Y)$	Conditional differential entropy
$I(X;Y)$	Mutual information of X and Y
$I(X;Y\|Z)$	Conditional mutual information given Z
$\|\mathbf{X}\|$	determinant of $\mathbf{X}$
$\mathrm{E}\{\cdot\}$	Expectation

II. System Model

A. Basic Principles

Let us consider a linear MIMO system with a uniform linear array (ULA) in which M antennas are equally spaced apart with a distance greater than half a wavelength to avoid the reduction of spatial diversity and the impact of mutual coupling [25]. MIMO precoding enables the transmitter to accommodate its signal pattern in definite paths to enhance the system performance through exploiting the strongest channel mode. At the transmitter, a modulation symbol, s, is mapped using an $M_T \times 1$ precoding codeword matrix, $\mathbf{f}$, where M_T corresponds to the number of transmit antennas, forming the transmit data vector $\mathbf{x} = \mathbf{f}s$. Assuming an orthogonal frequency division multiplexing (OFDM) system, the received Rayleigh fading signal can be expressed as

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{n}, \tag{1}$$

where $\mathbf{H}$ is an $M_R \times M_T$ channel matrix of independent identically distributed (i.i.d) random variables and $\mathbf{n}$ is the additive white Gaussian noise vector of length M_R, distributed as i.i.d random variables according to $\mathcal{CN}(0, N_0)$. In conventional MIMO precoding, choosing the appropriate precoding codeword requires the downlink channel state information (CSI) at the transmitter. In TDD systems, the transmitter and the receiver decompose the reciprocal channel matrix using singular value decomposition (SVD) which produces three matrices $\mathbf{U}, \Lambda$ and $\mathbf{V}^\dagger$. $\mathbf{U}$ and $\mathbf{V}$ are unitary matrices ($\mathbf{U}^\dagger\mathbf{U}= \mathbf{I}$, and $\mathbf{V}^\dagger\mathbf{V}= \mathbf{I}$), whereas Λ is a real-diagonal matrix. The transmitter precodes the data using $\mathbf{V}$, in (1) as

$$\mathbf{y} = \mathbf{H}\mathbf{V}s + \mathbf{n} = \left(\mathbf{U}\Lambda\mathbf{V}^\dagger\right)\mathbf{V}s + \mathbf{n}. \tag{2}$$

The receiver in turn decodes using $\mathbf{U}^\dagger$, such that we get the estimated value of the transmitted signal at the receiver

$$\begin{aligned} \hat{\mathbf{y}} &= \mathbf{U}^\dagger\mathbf{U}\Lambda s + \mathbf{U}^\dagger\mathbf{n}, \\ &= \underbrace{\Lambda s}_{\substack{\text{desired} \\ \text{symbol}}} + \underbrace{\mathbf{U}^\dagger\mathbf{n}}_{\substack{\text{noise} \\ \text{component}}} . \end{aligned} \tag{3}$$

In FDD systems, providing the CSI by the receiver is commonly considered impractical because it significantly degrades the bandwidth efficiency as the feedback overhead increases with the number of antenna elements. In limited feedback precoding, to reduce the CSI overhead, we use a codebook, $\mathcal{F}$, which consists of L unitary precoding matrices (or codewords) such that, [26],

$$\mathcal{F}_{\text{public}} = \left\{\mathbf{f}_0, \mathbf{f}_1, \ldots, \mathbf{f}_{L-1} \mid \mathbf{f}_l^\dagger\mathbf{f}_l = \mathbf{I},\ \forall 0 \le l \le L-1\right\}. \tag{4}$$

The receiver selects one of the codewords from the codebook and feeds back the index to the transmitter. The index selection follows the receiver's decision of which codeword is able to map the transmitted symbols across the spatial channel to augment the system performance. It is worth mentioning that the number of codewords, L, affects the network performance since larger sizes of codebooks will reduce the interference in the multi-user downlink signals. The optimal decision of the codewords distribution is out of the scope of this paper. Finally, Fig. 1 shows a basic schematic of a codebook based MIMO precoding system.

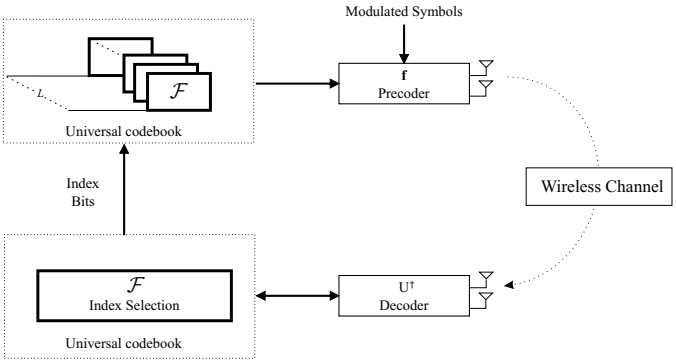

Fig. 1. MIMO codebook based precoding block diagram.

B. Precoding Codebooks

Precoding codebooks have been well studied for MIMO beamforming and spacial multiplexing. The most commonly used codebooks are the Discrete Fourier Transform (DFT), Grassmannian Line Package (GLP) and Kerdock codebooks. These codebooks performances are approximately similar and only differ in terms of the application where they are used and the available hardware [27], [28].

Since the codewords are independent of the instantaneous CSI, they can be generated offline and distributed to all communication nodes. Instead of needing a whole CSI transmission, the receiver appoints the optimum codeword, $\mathbf{f}_{\text{opt.}}$, from the codebook based on a selection criteria that enhances the system throughput such as capacity or error performance. In the case of maximizing the receiver's capacity, [26],

$$C\left(\mathbf{f}\right) = \log_2\left(\det\left(\mathbf{I}_{M_R} + \gamma\left(\mathbf{H}\mathbf{f}\right)^\dagger\left(\mathbf{H}\mathbf{f}\right)\right)\right), \tag{5}$$

where γ is the normalized SNR and the optimal precoder, $\mathbf{f}_{\text{opt.}}$, is, [29],

$$\mathbf{f}_{\text{opt.}} = \underset{\mathbf{f}_i \in \mathcal{F}_{\text{public}}}{\text{argmax}} C(\mathbf{f}_i). \tag{6}$$

C. Adversary Model

We consider a confidential communication link between a base station (BS) and a mobile station (MS) each equipped with multiple antennas of size M_{BS} and M_{MS}, respectively. A nearby eavesdropper, Eve, has M_{Eve} antennas and is closer to the MS than the BS. Therefore, we assume two wireless MIMO downlink channels $\mathbf{H}_{\text{BS-MS}}$ (between BS and MS) and $\mathbf{H}_{\text{BS-Eve}}$ (between BS and Eve), as shown in Fig. 2, with

$$M_{\text{BS}} \ge M_{\text{MS}}. \tag{7}$$

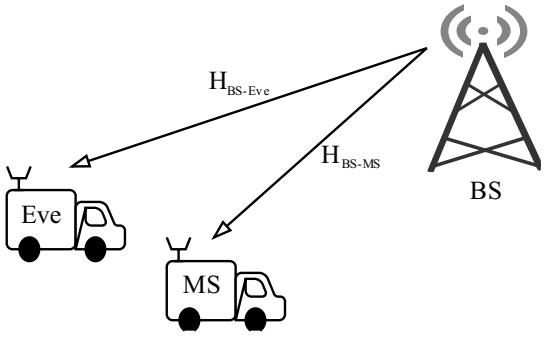

Fig. 2. BS and MS communication in the presence of Eve.

The wiretap channel assumes a passive attack by Eve through her ability to move closer to the MS to get a correlated version of the downlink channel and thus Eve now applies her attack on the collected key with the same system as MS

$$M_{\text{Eve}} = M_{\text{MS}}. \tag{8}$$

The practical BS-Eve downlink channel is expressed as, [30]-[32],

$$\mathbf{H}_{\text{BS-Eve}} = \rho \mathbf{H}_{\text{BS-MS}} + \sqrt{1-\rho^2}\mathbf{H}_{\text{i.i.d}}. \tag{9}$$

where $\mathbf{H}_{\text{BS-Eve}}$ and $\mathbf{H}_{\text{BS-MS}}$ are i.i.d Rayleigh fading channels which are correlated with a wide sense of a correlation coefficient ρ, $0 \leq \rho \leq 1$. $\mathbf{H}_{\text{i.i.d}}$ will be used to represent an i.i.d. Rayleigh fading channel with zero correlation with $\mathbf{H}_{\text{BS-MS}}$. Hence, the received signal in (1) can be expressed as

$$\begin{aligned} \mathbf{y}_{\text{MS}} &= \mathbf{H}_{\text{BS-MS}}\mathbf{x} + \mathbf{n}_{\text{MS}}, & (10)\\ \mathbf{y}_{\text{Eve}} &= \mathbf{H}_{\text{BS-Eve}}\mathbf{x} + \mathbf{n}_{\text{Eve}}. & (11) \end{aligned}$$

III. The Proposed Algorithm

The proposed PRP algorithm generates the secret key from collecting consecutive transmissions of the precoding codewords' indexes. Before the transmission starts, we assume that the codebook is distributed to all nodes. In the attack scenario we assume that Eve has a knowledge of the codebook, thus that direct precoding is susceptible to an illegitimate adversary action. Here we detail the procedural steps to increase the gain of the conventional precoding using the proposed private random precoding to exchange the secret key.

A. Phase 1: Private Common Random Value

We use the same initialization step used by the security community in their physical layer based algorithms which is finding a shared random value. In TDD systems, the reciprocal channels are considered as the common source of shared randomness where both the transmitter and the receiver can estimate their private shared random value that corresponds to the intermediate channel. On the other hand, in the case of FDD systems, the synchronized CSI estimation of the downlink channel is not available at the transmitter. Hence we propose the transmitter to carry out a self training of the optimal precoder of the downlink channel. The strategy of this training works as follows:

1) BS⟶MS (DL signal): The BS generates random private symbols, that are not shared even with the legitimate receiver, then assigns random codewords to precode it and sends it to the receiver. The received signal, referred to here as *case 1*, at the MS is

$$\mathbf{Y}_{\text{MS}} = [\mathbf{y}_0, \mathbf{y}_1, \ldots, \mathbf{y}_{L-1}], \tag{12}$$

where,

$$\begin{aligned} \mathbf{y}_0 &= \mathbf{H}_{0,\text{BS-MS}}\mathbf{f}_{p_0} \cdot \mathbf{s}_0 + \mathbf{n}_{0,\text{MS}},\\ \mathbf{y}_1 &= \mathbf{H}_{1,\text{BS-MS}}\mathbf{f}_{p_1} \cdot \mathbf{s}_1 + \mathbf{n}_{1,\text{MS}},\\ &\vdots \quad \vdots \quad \vdots\\ \mathbf{y}_{L-1} &= \underbrace{\mathbf{H}_{L-1,\text{BS-MS}}}_{\text{known at MS}}\mathbf{f}_{p_{L-1}} \cdot \mathbf{s}_{L-1} + \mathbf{n}_{L-1,\text{MS}}, \end{aligned} \tag{13}$$

such that, $0 \leq p \leq L-1$ in the set, $\mathbf{p} = \{p_0, p_1, \ldots, p_{L-1}\}$, which is the random vector of indexes assigned to each private preamble vector, $\mathbf{s}$, that is known only at the BS.

2) MS⟶BS (UL signal): The MS decodes the received signals in (12) by applying its optimal decoder, $\mathbf{U}_{\text{opt.}}$, and forwards the signal back to the BS.

3) UL Equalization: At the transmitter side a zero-forcing UL equalizer has a perfect channel knowledge where the equalizer matrix, $\mathbf{Q}$, is defined as [33], [34]

$$\mathbf{Q} = \left[\mathbf{H}^{\dagger}_{\text{MS-BS}}\mathbf{H}_{\text{MS-BS}}\right]^{-1}\mathbf{H}^{\dagger}_{\text{MS-BS}}. \tag{14}$$

Thus the signal received at the BS (*case 2*), $\bar{\mathbf{Y}}_{\text{BS}} = [\bar{\mathbf{y}}_0, \bar{\mathbf{y}}_1, \ldots, \bar{\mathbf{y}}_{L-1}]$, is given by (16, 17, 18, and after applying the uplink channel equalizer (*case 3*), 19).

4) DL-Optimal Precoder Detection: From the fact that in the noiseless environment, when the precoding codeword ($\mathbf{f}_{\mathbf{p}_i}$, in case 1) matches its corresponding decoder ($\mathbf{U}^{\dagger}_{\text{opt.}}$, in case 2) this generates a real diagonal matrix multiplied by the private preamble ($\mathbf{s}$, used at case 1) and the BS can consider ($\mathbf{f}_{\mathbf{p}_i}$=$\mathbf{f}_{\text{opt.}}$, in case 3) as in (3). Due to the additive noise components in the optimal precoder detection, the BS calculates the minimum Euclidean distance of the private phase of the private symbols (in case 1) relative to the received signal (in case 3) using a maximum likelihood modular reduction method as

$$D_{\text{Euclidean},\hat{l}} = \underset{0\leq l\leq L-1}{\text{argmin}} \left(|\text{mod}(\measuredangle\bar{\mathbf{y}}_l, \measuredangle\mathbf{s}_l)|\right). \tag{15}$$

At this moment, both BS and MS have the same knowledge of the optimal precoder index and Eve is left puzzled of this process due to the private preambles used by the BS.

B. Phase 2: Codebook Private Indexing

Recall the assumption that the codebook can be available at all nodes including the eavesdropper, thus the vulnerability of the secret key increases when equal antenna elements and SNR exist at the MS and Eve. Hence, the more correlation between $\mathbf{H}_{\text{BS-MS}}$ and $\mathbf{H}_{\text{BS-Eve}}$ the lower the secrecy rate achieved. In order to overcome this problem and to make the wiretap

$$\bar{\mathbf{y}}_{0,\text{BS}} = \mathbf{H}_{0,\text{MS-BS}}\left(\mathbf{U}^{\dagger}_{\text{opt.}}\mathbf{H}_{0,\text{BS-MS}}\mathbf{f}_{\mathbf{p}_0}\mathbf{s}_0 + \mathbf{U}^{\dagger}_{opt.}\mathbf{n}_{0,\text{MS}}\right) + \mathbf{n}_{0,\text{BS}}, \tag{16}$$

$$\bar{\mathbf{y}}_{1,\text{BS}} = \mathbf{H}_{1,\text{MS-BS}}\left(\mathbf{U}^{\dagger}_{\text{opt.}}\mathbf{H}_{1,\text{BS-MS}}\mathbf{f}_{\mathbf{p}_1}\mathbf{s}_1 + \mathbf{U}^{\dagger}_{opt.}\mathbf{n}_{1,\text{MS}}\right) + \mathbf{n}_{1,\text{BS}}, \tag{17}$$

$$\vdots \quad \vdots \quad \vdots$$

$$\bar{\mathbf{y}}_{L-1,\text{BS}} = \underbrace{\mathbf{H}_{L-1,\text{MS-BS}}}_{\text{known at BS}}\left(\mathbf{U}^{\dagger}_{\text{opt.}}\mathbf{H}_{L-1,\text{BS-MS}}\mathbf{f}_{\mathbf{p}_{L-1}}\mathbf{s}_{L-1} + \mathbf{U}^{\dagger}_{opt.}\mathbf{n}_{L-1,\text{MS}}\right) + \mathbf{n}_{L-1,\text{BS}}, \tag{18}$$

$$\hat{\mathbf{y}}_{L-1,\text{BS}} = \underbrace{\mathbf{U}^{\dagger}_{\text{opt.}}\mathbf{H}_{L-1,\text{BS-MS}}\mathbf{f}_{\mathbf{p}_{L-1}}}_{(\text{real-diagonal}|opt.=L-1)} \underbrace{\mathbf{s}_{L-1}}_{\text{private pointer}} + \underbrace{\mathbf{U}^{\dagger}_{\text{opt.}}\mathbf{n}_{L-1,\text{MS}} + \mathbf{Q}\mathbf{n}_{L-1,\text{BS}}}_{\text{noise components}}. \tag{19}$$

channel correlation less dependent on the optimal precoder, we propose to create a private version of the codebook, $\mathcal{F}_{\text{Private}}$, for the BS and MS. In fact, changing the codeword index in relation to the other codewords will not alter the codebook characteristics means no change will occur to the codebook performance. Therefore the private codebook has the same codewords possibilities available in the public version but with different indexes using the link capacity criteria as follows:

1) TDD systems: using the reciprocal channel measurements, the transmitter and the receiver apply a new indexing procedure, based on the channel capacity, and re-sort the indexes of the codebook progressively to create a new private version $\mathcal{F}_{\text{Private, TDD}} = [\mathbf{f}_{(0)}, \mathbf{f}_{(1)}, \cdots, \mathbf{f}_{(L-1)}]$, where

$$\mathbf{f}_{(0)} = \underset{\mathbf{f}_i \in \mathcal{F}_{\text{public}}}{\text{argmax}} C(\mathbf{f}_i), \tag{20}$$

$$\mathbf{f}_{(L-1)} = \underset{\mathbf{f}_i \in \mathcal{F}_{\text{public}}}{\text{argmin}} C(\mathbf{f}_i). \tag{21}$$

2) FDD systems: as previously discussed the only private random shared value is the index of the optimal precoder; therefore, we can apply index rotation to the subspace indexes starting from $\mathbf{f}_{\text{opt.}}$ as shown in Fig. 3, such that $\overline{\mathcal{F}}_{\text{Private, FDD}} = \left\{\bar{\mathbf{f}}_{(0)}, \mathbf{f}_{(1)}, \ldots, \mathbf{f}_{(L-1)}\right\}$.

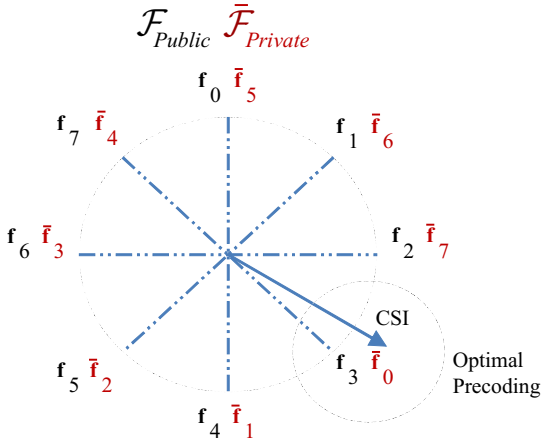

Fig. 3. 3-bit Private Codebook Subspace.

C. Phase 3: Secret Key Algorithm

Here we summarize the secret key exchange between BS and MS. Fig. 4 shows a schematic of the secret key bits generation and exchange, which can be outlined as follows:

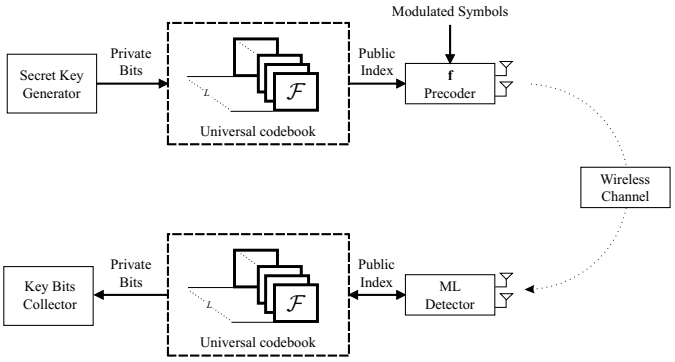

Fig. 4. Proposed private random precoding block diagram.

1) BS generates random secret key bits of length k, and groups each w-bits, $2^w = L$, then maps these to an index of the provided codewords.
2) BS precodes the public random modulated symbols and sends them to the MS.
3) MS in-turn receives, $\mathbf{H}_{\text{BS-MS}}\mathbf{f}_{\text{BS}}$, then apply the appropriate ML method to estimate the transmitted precoder, $\mathbf{f}_{\hat{l}}$, through finding the minimum subspace distance from the other precoders using either:

- Soft detection

$$\mathbf{f}_{\hat{l}} = \underset{0 \le l \le L-1}{\text{argmin}} \left(|\mathbf{H}_{\text{BS-MS}}\mathbf{f}_{\text{BS}}| - |\mathbf{H}_{\text{BS-MS}}\mathbf{f}_l|\right). \tag{22}$$

- Hard detection

$$\mathbf{f}_{\hat{l}} = \underset{0 \le l \le L-1}{\text{argmin}} \left(\text{Imag}\left\{\mathbf{U}^{\dagger}_l\mathbf{H}_{\text{BS-MS}}\mathbf{f}_{\text{BS}}\right\}\right). \tag{23}$$

In other words, MS uses a designed threshold value of the instantaneous SNR to decide on the proper detection method that achieves its desired KER. It will be shown later in Section V how switching between the Soft and Hard detector affects the overall performance. After this, MS locates the private index that yields the secret key as

$$\bar{\mathbf{f}}_{l,private} \triangleq \mathbf{f}_{\hat{l},\text{public}}, \tag{24}$$

$$K_{secret} = \left[l_1 \parallel l_2 \parallel \ldots \parallel l_{k/w}\right]. \tag{25}$$

4) Optionally, MS transmits another secret key bits on the uplink using the previous steps.

5) Both BS and MS exchange their collected key bits using any type of a universal Hash function for a private acknowledgement [2].

Algorithm 1 summarizes the overall steps of the initial setup and key exchange.

Algorithm 1 Secret Key Exchange Algorithm.

Step 1: Initialization by BS and MS

1: **Require**: $\mathcal{F}$
2: **for** $l = 0$ **to** $L-1$
3: BS signal = $\mathbf{f}_l s_l$
4: MS decode-relay signal = $\mathbf{U}_{opt.}^{\dagger}\mathbf{H}_{\text{BS-MS}}\mathbf{f}_l s_l + \mathbf{n}_{l,\text{MS}}$
5: **end for**
6: **Return**: $\mathbf{f}_{opt.}$
7: $\overline{\mathcal{F}}_{\text{Private}}$ =**Rotate** $\mathcal{F}_{\text{Public}}$ from $\mathbf{f}_{opt.}$

Step 2: Secret Key transmission and detection

BS:

1: Generate secret key, K_{secret} = random (k-bits)
2: **for** $i = 0$ **to** $k - w$ **step** w
3: l = binary-to-decimal $(K_{i:i+w})$
4: Map $\mathbf{f}_l \triangleq \bar{\mathbf{f}}_l$, precode using $\mathbf{f}_l$

MS:

5: Estimate $\mathbf{f}_{\hat{l}}$ using ML detection, (22) or (23)
6: Map $\bar{\mathbf{f}}_l \triangleq \mathbf{f}_{\hat{l}}$
7: **end for**
8: **Return**: Secret key, K_{secret} = $[l_1 \| l_2 \| \ldots \| l_{k/w}]$

End

IV. Information Theoretic Analysis

It was shown in the analysis of the channel quantization approach that the achievable mutual information resulted from quantifying the two way channels is identical to the jointly quantized random variables $I(X;Y)$, [35], as $I_{\text{bits}} = I\left(\mathbf{H}_{\text{BS-MS}}; \mathbf{H}_{\text{MS-BS}}\right)$, given that $\mathbf{H}_{\text{MS-BS}} = \left(\mathbf{H}_{\text{BS-MS}}\right)^T$. In our case, we will analyse the mutual secret information bounds as:

A. The Upper Bound

For simplicity, denote $\mathbf{H}_{\text{BS-MS}}$, $\mathbf{H}_{\text{MS-BS}}$, $\mathbf{H}_{\text{BS-Eve}}$, and $\mathbf{H}_{\text{MS-Eve}}$ as $\mathbf{H}_{\text{B}}$, $\mathbf{H}_{\text{M}}$, $\mathbf{H}_{\text{BE}}$, and $\mathbf{H}_{\text{ME}}$ respectively. The secrecy bit rate can be defined as the mutual information of the observed channels on the downlink and the uplink given the knowledge of Eve's channel. With very low channel estimation errors, the achievable secrecy rate of the secret key is bounded by, [36], [13],

$$I_{\text{secret}} = I\left(\mathbf{H}_{\text{B}}\mathbf{f}_{l_{\text{B}}}; \mathbf{H}_{\text{M}}\mathbf{f}_{l_{\text{M}}} \mid \mathbf{H}_{\text{BE}}\mathbf{f}_{l_{\text{B}}}, \mathbf{H}_{\text{ME}}\mathbf{f}_{l_{\text{M}}}\right). \quad (26)$$

The *upper bound* of the mutual information for exchanging the secret key bits can be expressed as $I_{\text{secret}} \leq I_{\text{bits}}$. The best case scenario, i.e. the highest achievable secrecy, is when Eve is far from the BS and MS, that is $\mathbf{H}_{\text{B}}, \mathbf{H}_{\text{M}} \perp \mathbf{H}_{\text{BE}}, \mathbf{H}_{\text{ME}}$ and all the information bits are considered secure, $I_{\text{secret}} = I_{\text{bits}}$, [13].

B. The Lower Bound

The more interesting situation is when Eve is closer and quasi stationary in a wide sense with the MS moving at the same speed with less scattering and connected to a distant roof mounted BS. We will denote $\mathbf{H}_{\text{E}}$ as a representation of either ($\mathbf{H}_{\text{BE}}$, or $\mathbf{H}_{\text{ME}}$), since the downlink and the uplink key exchange signals are not synchronized and the existence of both is not valid, then the rate of secret bits is $I_{\text{secret}} = I\left(\mathbf{H}_{\text{B}}; \mathbf{H}_{\text{M}} \mid \mathbf{H}_{\text{E}}\right)$, [13]. Also since we proposed the channel independent precoding matrix indexes, we rewrite I_{secret} to fit the PRP technique as an equivocation argument between the BS, MS, and Eve, all equipped with the same number of antennas, M, as

$$I_{\text{secret}} = h\left(\mathbf{H}_{\text{B}}\mathbf{f}_{l_{\text{B}}}; \mathbf{H}_{\text{M}}\mathbf{f}_{l_{\text{M}}} \mid \mathbf{H}_{\text{E}}\mathbf{f}_{l_{\text{B,M}}}\right), 0 \leq l \leq L-1. \quad (27)$$

The secret information can be expressed as the equivocation of the downlink, $h\left(\mathbf{H}_{\text{B}}\mathbf{f}_{l_{\text{B}}} \mid \mathbf{H}_{\text{E}}\mathbf{f}_{l_{\text{B}}}\right)$, multiplexed with the uplink, $h\left(\mathbf{H}_{\text{M}}\mathbf{f}_{l_{\text{M}}} \mid \mathbf{H}_{\text{E}}\mathbf{f}_{l_{\text{M}}}\right)$, and considering the joint probability in the presence of Eve. For better understanding of the *lower bound* of the mutual information about the secret key, Fig. 5 shows a simple space of the random variables held together by the BS, MS and Eve.

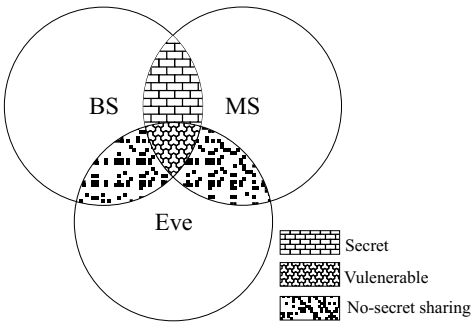

Fig. 5. Random variables expressed as the Venn diagram.

The secret key can be expressed as

$$\begin{aligned} I_{\text{secret}} &= I\left(\mathbf{H}_{\text{B}}\mathbf{f}_l; \mathbf{H}_{\text{M}}\mathbf{f}_l \mid \mathbf{H}_{\text{E}}\mathbf{f}_l\right), & (28)\\ &= h\left(\mathbf{H}_{\text{B}}\mathbf{f}_l \mid \mathbf{H}_{\text{E}}\mathbf{f}_l\right) + h\left(\mathbf{H}_{\text{M}}\mathbf{f}_l \mid \mathbf{H}_{\text{E}}\mathbf{f}_l\right) \\ &- h\left(\mathbf{H}_{\text{B}}\mathbf{f}_l, \mathbf{H}_{\text{M}}\mathbf{f}_l, \mathbf{H}_{\text{E}}\mathbf{f}_l\right) + h\left(\mathbf{H}_{\text{E}}\mathbf{f}_l\right). & (29) \end{aligned}$$

Proposition 1. The downlink signal equivocation term in (29), $h\left(\mathbf{H}_{\text{B}}\mathbf{f}_l \mid \mathbf{H}_{\text{E}}\mathbf{f}_l\right)$, can be quantified as in (31) to yield an equivocation rate greater than that achieved in direct channel quantization, $h\left(\mathbf{H}_{\text{B}}\mathbf{f}_l \mid \mathbf{H}_{\text{E}}\mathbf{f}_l\right)$, given in (32).

$$h\left(\mathbf{H}_{\mathrm{B}}\mathbf{f}_{l_{\mathrm{B}}} \mid \mathbf{H}_{\mathrm{E}}\mathbf{f}_{l_{\mathrm{B}}}\right)$$
$$= \log_2(\pi e)^M \prod_{i=1}^{M}\left(1-\mathbf{R}_{\mathrm{BE}(i,i)}\right), \quad (30)$$
$$\simeq \log_2(\pi e)^M \left(1-\left(\sum_{m=1}^{M}\frac{1}{M}E\{\mathbf{H}_{\mathrm{B},m}(\mathbf{H}_{\mathrm{E},m})^*\}\right)^2\right)^M. \quad (31)$$

$$h\left(\mathbf{H}_{\mathrm{B}} \mid \mathbf{H}_{\mathrm{E}}\right)$$
$$\simeq \log_2(\pi e)^M \left(1-\sum_{b=1}^{M}\sum_{e=1}^{M}\frac{1}{M}\left(E\{\mathbf{H}_{\mathrm{B},b}(\mathbf{H}_{\mathrm{E},e})^*\}\right)^2\right)^M. \quad (32)$$

Proof: The proof for Proposition 1 is provided in Appendix A. ∎

It is worth mentioning that in the worst case scenario, when Eve is moving towards Alice to enhance her channel correlation to the best level as $\rho \approx 1$, the equivocation is reduced to the lowest value compared with the uncorrelated case. Nevertheless, this correlation has larger influence on the equivocation of the direct channel quantization technique and thus the proposed algorithm still offers higher equivocation as will be shown later in this paper. On the other hand, the number of multiple antennas has a notable effect on the equivocation rates, that is a larger number of antennas can dramatically affect the performance of the attacker by reducing the number of vulnerable bits of the secret key.

Proposition 2. Using a similar way as in Proposition 1, we find the uplink signal equivocation, $h\left(\mathbf{H}_{B}\mathbf{f}_{l} \mid \mathbf{H}_{M}\mathbf{f}_{l}\right)$, term as

$$h\left(\mathbf{H}_{\mathrm{M}}\mathbf{f}_{l_{\mathrm{M}}} \mid \mathbf{H}_{\mathrm{E}}\mathbf{f}_{l_{\mathrm{M}}}\right) \quad (33)$$
$$\simeq \log_2(\pi e)^M \left(1-\left(\sum_{m=1}^{M}\frac{1}{M}E\{\mathbf{H}_{\mathrm{M},m}(\mathbf{H}_{\mathrm{E},m})^*\}\right)^2\right)^M. \quad (34)$$

Proof: The proof for Proposition 2 is provided in Appendix B. ∎

Proposition 3. The joint covariance of the BS, MS and Eve in the lower bound equation in (29) results in the expression

$$h\left(\mathbf{H}_{\mathrm{B}}\mathbf{f}_{l}, \mathbf{H}_{\mathrm{M}}\mathbf{f}_{l}, \mathbf{H}_{\mathrm{E}}\mathbf{f}_{l}\right) = \log_2(\pi e)^{M_T}\left(\mathbf{R}_{\mathrm{BME}}\right), \quad (35)$$

where $\mathbf{R}_{\mathrm{BME}}$ is in (36) shown at the top of the next page, and

$$\bar{\mathbf{R}}_1 = \mathbf{R}_1^{\dagger}\mathbf{R}_1;\ \mathbf{R}_1 = \mathbf{R}_{\mathrm{BM}}, \quad (37)$$
$$\bar{\mathbf{R}}_2 = \mathbf{R}_2^{\dagger}\mathbf{R}_2;\ \mathbf{R}_2 = \mathbf{R}_{\mathrm{BE}}, \quad (38)$$

$$\mathbf{R}_3 = \mathbf{R}_{\mathrm{ME}}. \quad (39)$$

Proof: The proof for Proposition 3 is provided in Appendix C. ∎

V. Result and Analysis

A. Simulation Setup and Complexity

In this section, we assess the performance of the proposed PRP method using computer simulation with a realistic setup that is normally adopted in the Long Term Evolution (LTE) [37], [38], as summarized in Table II. Table III shows the computational comparison after channel estimation stage for a single byte of the secret key, where the suppression of the channel decomposition yields an interesting reduction of the number of computations which can be seen from Fig. 6.

TABLE II
Simulation Setup.

Channel model	SCME, Vehicular A
MIMO system	3×3, 4×4, 6×6, and 8×8, single user
Modulation	QPSK
Fading	Small scale Rayleigh fading
Centre frequency	1.8/2 GHz (UL/DL)
Vehicle velocity	3, 30, 60, 120 km/h
Codebook	DFT
Codebook Size	2, 3, 4 and 5-bits
Key length	128 bits

TABLE III
Methods Comparison, w-bits codebook of rank-1 and $M_R\times M_T$ MIMO.

Computational Process	Proposed Soft, Hard	MOPRO	CQA
Multiplication and Division	$2^{w+1}(M_RM_T)$, $2^{w+1}M_R^2$	$2M_TM_R^2+$ $2^{w+1}(M_R+1)$	$2M_RM_T(5M_R+1)$
Channel decomposition	nil, $2^{w+1}M_RM_T^2$	$4M_RM_T^2$	$\frac{128(M_RM_T)^3}{(M_RM_T)^3+2}$
Addition and Subtraction	$2^{w+1}(M_RM_T)$, $2^{w+1}(M_R^2+M_T)$	$2M_R^2(M_T-1)+$ $2^{w+2}(M_R-\frac{1}{2})$	$2M_R(5M_R+M_T)$

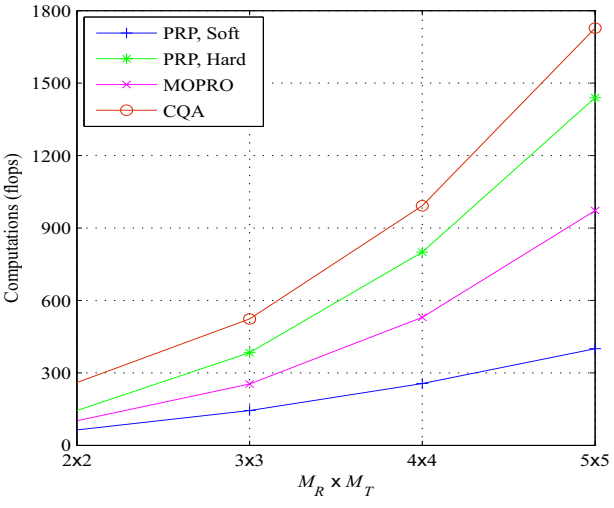

Fig. 6. Computational complexity comparison to others with $w=2$ bits and variable $M_R\times M_T$ MIMO systems.

$$\left|\mathbf{R}_{\mathrm{BME}}\right| = \left|\mathbf{I}-\mathbf{R}\mathbf{R}_1\right|\left|\left(\mathbf{I}-\mathbf{R}\mathbf{R}_2\right)-\left(\left(\mathbf{R}_3^{\dagger}-\mathbf{R}_2^{\dagger}\mathbf{R}_1\right)\left(\mathbf{I}-\mathbf{R}\mathbf{R}_1\right)^{-1}\left(\mathbf{R}_3-\mathbf{R}_1^{\dagger}\mathbf{R}_2\right)\right)\right|, \quad (36)$$

B. PRP Performance

Fig. 7 illustrates a good KER performance at 3 km/h in comparison with the quantization based (CQA [15], CR [22]) methods and MOPRO [17]. Two main points can be highlighted from this figure. First, using a larger codebook size generates longer key bits and enhances the generation rate at the expense of the KER performance. This is due to the fact that minimizing the Euclidean distance in the subspace distribution between the codewords will minimize the corresponding Euclidean distance at the ML detector. Second, Hard detection compared to Soft detection is more appropriate in the lower SNR region that practically ranges between 5-10 dB. At higher mobility speed (120 km/h), for a key exchange error rate that is lower than 10^{-2}, key generation requires a trade-off between the error rate and the length of the correct bits per transmitted signal as depicted in Fig. 8.

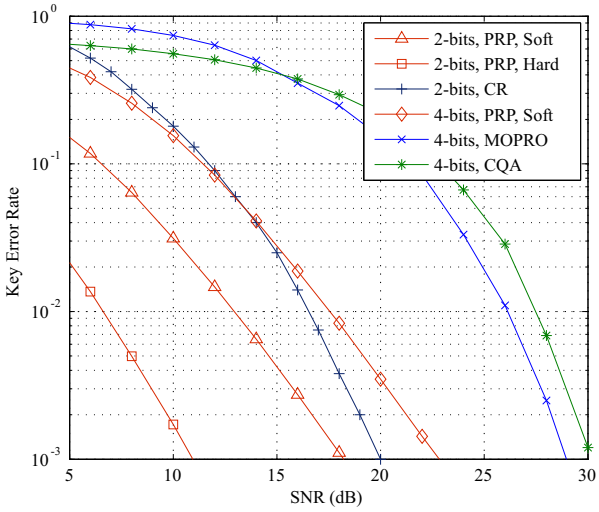

Fig. 7. PRP versus others performances at 3 km/h with 4×4 MIMO.

Fig. 9a shows clearly the subspace distance effect for different codebook sizes. Increasing the spatial diversity gain, over higher orders of MIMO channels, will eventually lead to better performance since the codewords in-between distances can be distributed on wider dimensions and thus have better correct detection probability. A comparison as a function of the number of antenna elements is depicted in Fig. 9b.

The codebook size as shown earlier is a very critical factor to be determined before transmitting the secret key. In fact, if we consider the case of fixed codebook size during the whole key transmission, it may degrade the performance of the secret key bits throughput. In this case, we propose a dynamic change of the codebook size based on setting a threshold SNR that targets 10^{-2} KER to lower the disagreement rate between the BS and MS and increase the system throughput. As a result,

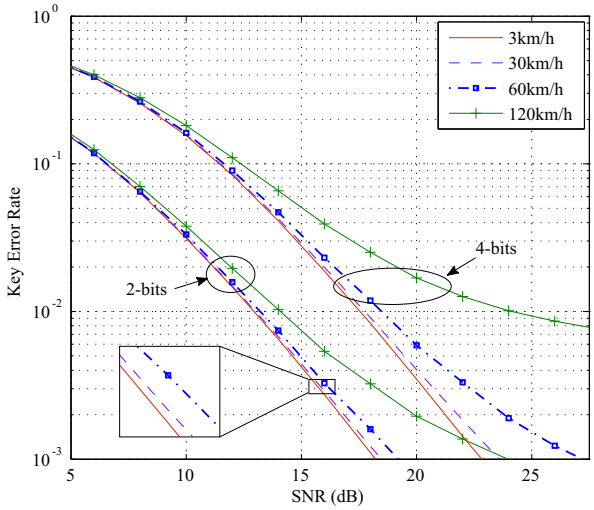

Fig. 8. KER performance with 4×4 MIMO single user and different codebook sizes at different MS velocity.

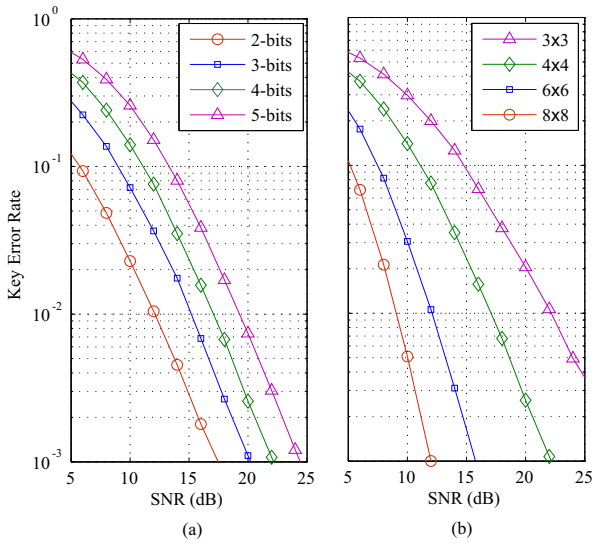

Fig. 9. Subspace distance effect (at 3 km/h, Soft detector) on the codebook performance with different codebook sizes in 4×4 MIMO system in (a), and (b) 4-bits codebook with different antenna sizes.

the exchange of the secret key is set to start with the smallest size and can be extended if the SNR allows larger sizes subject to satisfying a certain KER. The performance of the proposed method using an adaptive codebook size is depicted in Fig. 10.

C. Nearby Adversary Performance

During the key exchange process, it is highly expected that Eve could run the same procedure but the proposed private in-

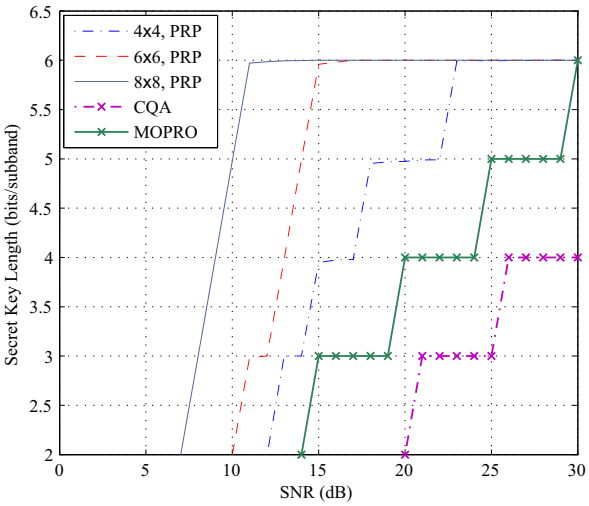

Fig. 10. Dynamic secret key exchange (at 3 km/h) to achieve 10^{-2} KER using Soft detector.

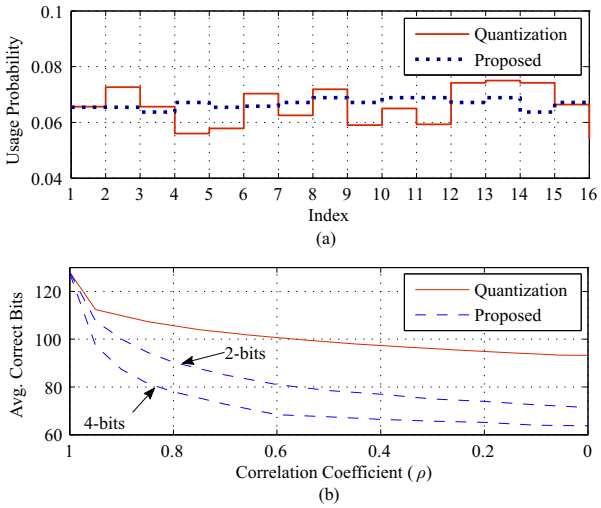

Fig. 11. Security performance with 4×4 MIMO system at (3 km/h, and SNR=20dB). (a) Codeword index usage probability, and (b) Average number of correct secret key bits detected by Eve with different correlation.

dexing will prevent her from guessing the correct indexes without a prior knowledge of the optimum precoder. In fact, for the direct channel quantization method the correlated quantization levels will generate a correlated secret key bits and hence the security level is decreased due to Eve's ability to retrieve the secret key bits based on the index excitation processing. As mentioned earlier, the decorrelation processing that was proposed in previous related works will eventually increase the computational complexity with considerable information feedback. In Fig. 11a we show that our proposed random secret key generator is able to generate random consecutive sequences of secret bits even at low mobility, based on the observation of its decimal corresponding value, with no need for the time gap between the temporal probes that are used in the quantization approaches, [15], [22]. Fig. 11b represents the average number of bits that can be detected by Eve when having an identical system to the MS. It is evident that our proposed random indexing and precoding can achieve better performance than other quantization methods at lower velocity with a difference of approximately 30 bits. Moreover, this can be verified through tracking the channel correlation between the MS and Eve that is observed at different correlation levels which can be gained when Eve is trying to move closer towards the MS as depicted in Fig. 12. Using our proposed algorithm we can decorrelate the BS-MS and BS-Eve channels with simple physical displacement in the order of a few centimeters for the downlink channel which operates at GHz frequencies. Therefore, Eve will be no longer be capable of reconstructing her downlink channel into a similar version to that of the legitimate downlink channel and hence the security of the random indexing is preserved.

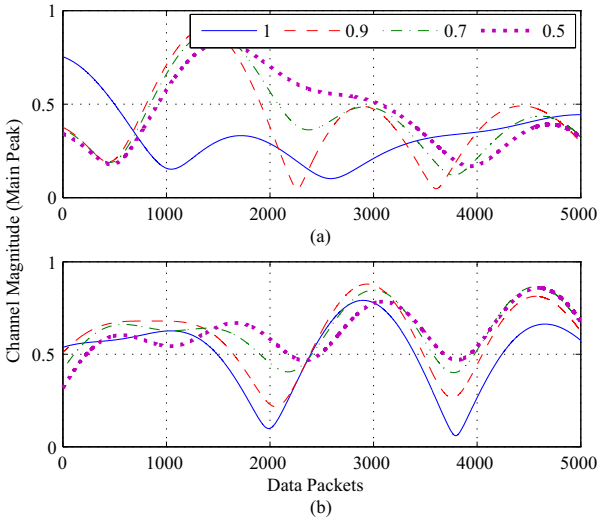

Fig. 12. Eve's Channel at different correlation with MS (at 3 km/h) using (a) the proposed algorithm and (b) the quantization method.

VI. Conclusion

This paper presented a versatile method for establishing the secret key in MIMO FDD and TDD systems based on private randomized precoding in a closed loop decode-and-forward relay mode. The simulation results have shown that the proposed method has superior KER performance and low computational burden at the expense of a modest increase in memory requirement. Although Eve may have a chance to attack the key exchange process, this assumption is considered highly unlikely especially for the Gigahertz frequency bands where the minimum distance required to have a correlated version of the downlink channel is in the order of centimetres. Furthermore, it was demonstrated that the proposed technique provides better security performance even when the channels are highly correlated.

APPENDIX A
PROOF OF EXPRESSION $h\left(\mathbf{H}_{\mathrm{B}}\mathbf{f}_l \mid \mathbf{H}_{\mathrm{E}}\mathbf{f}_l\right)$

Proof: The conditional differential entropy of the *downlink signal* can be written as

$$h\left(\mathbf{H}_{\mathrm{B}}\mathbf{f}_l \mid \mathbf{H}_{\mathrm{E}}\mathbf{f}_l\right) = h\left(\mathbf{H}_{\mathrm{B}}\mathbf{f}_l, \mathbf{H}_{\mathrm{E}}\mathbf{f}_l\right) - h\left(\mathbf{H}_{\mathrm{E}}\mathbf{f}_l\right). \tag{40}$$

In (40) , the joint correlation can be computed as, [39],

$$h\left(\mathbf{H}_{\mathrm{B}}\mathbf{f}_l, \mathbf{H}_{\mathrm{E}}\mathbf{f}_l\right) = E\left\{\left[\begin{array}{cc}\mathbf{H}_{\mathrm{B}}\mathbf{f}_l & \mathbf{H}_{\mathrm{E}}\mathbf{f}_l\end{array}\right]\left[\begin{array}{cc}\mathbf{H}_{\mathrm{B}}\mathbf{f}_l & \mathbf{H}_{\mathrm{E}}\mathbf{f}_l\end{array}\right]^{\dagger}\right\}, \tag{41}$$

$$= \log_2(\pi e)^{M}\left|\begin{array}{cc}\mathbf{R}_{\mathrm{B}} & \mathbf{R}_{\mathrm{BE}} \\ \mathbf{R}_{\mathrm{BE}}^{\dagger} & \mathbf{R}_{\mathrm{E}}\end{array}\right|, \tag{42}$$

$$= \log_2(\pi e)^{M}\det\left(\mathbf{R}_{\mathrm{B}}\left(\mathbf{R}_{\mathrm{E}} - \mathbf{R}_{\mathrm{BE}}\left(\mathbf{R}_{\mathrm{B}}\right)^{-1}\mathbf{R}_{\mathrm{BE}}^{\dagger}\right)\right), \tag{43}$$

where $\mathbf{R}_{\mathrm{B}}$ and $\mathbf{R}_{\mathrm{E}}$ are symmetric semi-definite positive matrices of the covariance of the BS and Eve given as

$$\mathbf{R}_{\mathrm{B}} = E\left\{\left(\mathbf{H}_{\mathrm{B}}\mathbf{f}_l\right)\left(\mathbf{H}_{\mathrm{B}}\mathbf{f}_l\right)^{\dagger}\right\}, \tag{44}$$

$$\mathbf{R}_{\mathrm{E}} = E\left\{\left(\mathbf{H}_{\mathrm{E}}\mathbf{f}_l\right)\left(\mathbf{H}_{\mathrm{E}}\mathbf{f}_l\right)^{\dagger}\right\}. \tag{45}$$

Substituting (43) in (40) results in the conditional covariance of, $\mathbf{H}_{\mathrm{B}}\mathbf{f}_l$, given the existence of Eve, $\mathbf{H}_{\mathrm{E}}\mathbf{f}_l$, as the Schur complement of $\mathbf{R}_{\mathrm{E}}$ found in $h\left(\mathrm{BS,Eve}\right)$ which is expressed as the following conditional differential entropy, [40],

$$h\left(\mathbf{H}_{\mathrm{B}}\mathbf{f}_l \mid \mathbf{H}_{\mathrm{E}}\mathbf{f}_l\right) = \log_2(\pi e)^{M}\det\left(\mathbf{R}_{\mathrm{B}} - \mathbf{R}_{\mathrm{BE}}\left(\mathbf{R}_{\mathrm{E}}\right)^{-1}\mathbf{R}_{\mathrm{BE}}^{\dagger}\right) \tag{46}$$

$$= \log_2(\pi e)^{M}\det\left(\mathbf{I} - \mathbf{R}_{\mathrm{BE}}\mathbf{R}_{\mathrm{BE}}^{\dagger}\right). \tag{47}$$

In (47), suppose that the precoding matrix is a unitary matrix generated randomly and is independent of the measurement of $\mathbf{H}_{\mathrm{B}}$, hence the conditional covariance under multiple antennas of higher order will satisfy that, [17],

$$\mathbf{R}_{\mathrm{B}} = E\left[\left(\mathbf{H}_{\mathrm{B}}\mathbf{f}_l\right)\left(\mathbf{H}_{\mathrm{B}}\mathbf{f}_l\right)^{\dagger} \mid \mathbf{f}_l\right] = \mathbf{I}_{\mathrm{B}}, \tag{48}$$

$$\mathbf{R}_{\mathrm{M}} = E\left[\left(\mathbf{H}_{\mathrm{M}}\mathbf{f}_l\right)\left(\mathbf{H}_{\mathrm{M}}\mathbf{f}_l\right)^{\dagger} \mid \mathbf{f}_l\right] = \mathbf{I}_{\mathrm{M}}, \tag{49}$$

$$\mathbf{R}_{\mathrm{E}} = E\left[\left(\mathbf{H}_{\mathrm{E}}\mathbf{f}_l\right)\left(\mathbf{H}_{\mathrm{E}}\mathbf{f}_l\right)^{\dagger} \mid \mathbf{f}_l\right] = \mathbf{I}_{\mathrm{E}}, \tag{50}$$

The $\mathbf{R}_{\mathrm{BE}}$ in (47) is simplified as

$$\mathbf{R}_{\mathrm{BE}(m,n)} = \sum_{m=1}^{M}\sum_{n=1}^{M} E\left\{\left(\mathbf{H}_{\mathrm{B},m}\mathbf{f}_{l,\mathrm{B},m}\right)\left(\mathbf{H}_{\mathrm{E},n}\mathbf{f}_{l,\mathrm{E},n}\right)^{*}\right\}, \tag{51}$$

$$= \sum_{m=1}^{M}\sum_{n=1}^{M} E\left\{\mathbf{f}_{l,\mathrm{B},m}\left(\mathbf{f}_{l,\mathrm{E},n}\right)^{*}\right\} E\left\{\mathbf{H}_{\mathrm{B},m}\left(\mathbf{H}_{\mathrm{E},n}\right)^{*}\right\}. \tag{52}$$

Since $\mathbf{f}_{l,\mathrm{B}}$ and $\mathbf{f}_{l,\mathrm{E}}$ are orthogonal unitary matrices, it follows that $\mathbf{f}_l\,\mathbf{f}_l^{*} = \mathbf{I}$ and $\mathbf{f}_l\mathbf{f}_j^{*} = 0$ for $l \neq j$ then a diagonal matrix is generated from solving (52) while keeping in mind the power constraint of multiple antennas, [41],

$$\mathbf{R}_{\mathrm{BE}} = \begin{cases}\sum\limits_{m=1}^{M}\frac{1}{M}E\left\{\mathbf{H}_{\mathrm{B},m}\left(\mathbf{H}_{\mathrm{E},m}\right)^{*}\right\} & , \text{ if } \mathbf{f}_{l,\mathrm{B}} = \mathbf{f}_{l,\mathrm{E}}, \\ 0 & , \text{ otherwise.}\end{cases} \tag{53}$$

$h\left(\mathbf{H}_{\mathrm{B}}\mathbf{f}_l \mid \mathbf{H}_{\mathrm{E}}\mathbf{f}_l\right)$ term results from simplifying (47) and substituting (53) to address the downlink equivocation of the secret key as in (31). ■

APPENDIX B
PROOF OF EXPRESSION $h\left(\mathbf{H}_{\mathrm{M}}\mathbf{f}_l \mid \mathbf{H}_{\mathrm{E}}\mathbf{f}_l\right)$

Proof: The proof is similar to the proof of $h\left(\mathbf{H}_{\mathrm{B}}\mathbf{f}_l \mid \mathbf{H}_{\mathrm{E}}\mathbf{f}_l\right)$, so we omit it here. ■

APPENDIX C
PROOF OF EXPRESSION $h\left(\mathbf{H}_{\mathrm{B}}\mathbf{f}_l, \mathbf{H}_{\mathrm{M}}\mathbf{f}_l, \mathbf{H}_{\mathrm{E}}\mathbf{f}_l\right)$

Proof: The joint covariance of the BS, MS and Eve in the lower bound equation in (29) is solved by computing the Schur complement of a 3×3 block matrix which is

$$h\left(\mathbf{H}_{\mathrm{B}}\mathbf{f}_l, \mathbf{H}_{\mathrm{M}}\mathbf{f}_l, \mathbf{H}_{\mathrm{E}}\mathbf{f}_l\right) = E\left\{\left[\begin{array}{ccc}\mathbf{H}_{\mathrm{B}}\mathbf{f}_l & \mathbf{H}_{\mathrm{M}}\mathbf{f}_l & \mathbf{H}_{\mathrm{E}}\mathbf{f}_l\end{array}\right]\left[\begin{array}{ccc}\mathbf{H}_{\mathrm{B}}\mathbf{f}_l & \mathbf{H}_{\mathrm{M}}\mathbf{f}_l & \mathbf{H}_{\mathrm{E}}\mathbf{f}_l\end{array}\right]^{\dagger}\right\},$$

$$= \log_2(\pi e)^{M_T}\left[\begin{array}{ccc}\mathbf{R}_{\mathrm{B}} & \mathbf{R}_{\mathrm{BM}} & \mathbf{R}_{\mathrm{BE}} \\ \mathbf{R}_{\mathrm{MB}} & \mathbf{R}_{\mathrm{M}} & \mathbf{R}_{\mathrm{ME}} \\ \mathbf{R}_{\mathrm{EB}} & \mathbf{R}_{\mathrm{EM}} & \mathbf{R}_{\mathrm{E}}\end{array}\right],$$

$$= \log_2(\pi e)^{M_T}\left(\mathbf{R}_{\mathrm{BME}}\right), \tag{54}$$

where $\mathbf{R}_{\mathrm{BME}}$ is writen as in (55). Applying the assumption (48, 49, and 50) in (55), yields the term in (36). Finally, $\mathbf{R}_{\mathrm{BM}}$ and $\mathbf{R}_{\mathrm{ME}}$ can be calculated with the assumption used for (52) and (53). ■

REFERENCES

[1] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-key Cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978. [Online]. Available: http://doi.acm.org/10.1145/359340.359342

[2] W. Stallings, *Cryptography and Network Security: Principle and Practice*, 6th ed. Pearson, 2014.

[3] B. Arazi, "Vehicular Implementations of Public Key Cryptographic Techniques," *Vehicular Technology, IEEE Transactions on*, vol. 40, no. 3, pp. 646–653, Aug 1991.

[4] J.-L. Huang, L.-Y. Yeh, and H.-Y. Chien, "ABAKA: An Anonymous Batch Authenticated and Key Agreement Scheme for Value-Added Services in Vehicular Ad Hoc Networks," *Vehicular Technology, IEEE Transactions on*, vol. 60, no. 1, pp. 248–262, Jan 2011.

[5] C.E.Shannon, "Communication Theory of Secrecy Systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, April 1949.

[6] A. Wyner, "The Wire-tap Channel," *Bell System Technical Journal*, vol. 54, pp. 1355–1387, 1975.

[7] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian Wiretap Channel," *IEEE Transaction on Information Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[8] I. Csiszár and J. Körner, "Broadcast Channels with Confidential Messages," *IEEE Transaction on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.

$$\mathbf{R}_{\mathrm{BME}} = \left| \mathbf{R}_{\mathrm{B}} \right| \left| \mathbf{R}_{\mathrm{M}} - \mathbf{R}_{\mathrm{MB}} \mathbf{R}_{\mathrm{B}}^{-1} \mathbf{R}_{\mathrm{BM}} \right| \left| \left(\mathbf{R}_{\mathrm{E}} - \mathbf{R}_{\mathrm{EB}} \mathbf{R}_{\mathrm{B}}^{-1} \mathbf{R}_{\mathrm{BE}} \right) - \left(\left(\mathbf{R}_{\mathrm{EM}} - \mathbf{R}_{\mathrm{EB}} \mathbf{R}_{\mathrm{B}}^{-1} \mathbf{R}_{\mathrm{BM}} \right) \left(\mathbf{R}_{\mathrm{M}} - \mathbf{R}_{\mathrm{MB}} \mathbf{R}_{\mathrm{B}}^{-1} \mathbf{R}_{\mathrm{BM}} \right)^{-1} \left(\mathbf{R}_{\mathrm{ME}} - \mathbf{R}_{\mathrm{MB}} \mathbf{R}_{\mathrm{B}}^{-1} \mathbf{R}_{\mathrm{BE}} \right) \right) \right|. \quad (55)$$

[9] C. Ye, A. Reznik, and Y. Shah, "Extracting Secrecy from Jointly Gaussian Random Variables," in *Information Theory, 2006 IEEE International Symposium on*, July 2006, pp. 2593–2597.

[10] N. Patwari, J. Croft, S. Jana, and S. Kasera, "High-Rate Uncorrelated Bit Extraction for Shared Secret Key Generation from Channel Measurements," *Mobile Computing, IEEE Transactions on*, vol. 9, no. 1, pp. 17–30, Jan 2010.

[11] A. Sayeed and A. Perrig, "Secure Wireless Communications: Secret Keys Through Multipath," in *Acoustics, Speech and Signal Processing, 2008. ICASSP 2008. IEEE International Conference on*, March 2008, pp. 3013–3016.

[12] K. Zeng, D. Wu, A. Chan, and P. Mohapatra, "Exploiting Multiple-Antenna Diversity for Shared Secret Key Generation in Wireless Networks," in *INFOCOM, 2010 Proceedings IEEE*, March 2010, pp. 1–9.

[13] J. W. Wallace and R. K. Sharma, "Automatic Secret Keys From Reciprocal MIMO Wireless Channels: Measurement and Analysis," *IEEE Transaction on Information Forensics and Security*, vol. 5, no. 3, pp. 381–392, Sept. 2010.

[14] B. Quist and M. Jensen, "Bound on the Key Establishment Rate for Multi-Antenna Reciprocal Electromagnetic Channels," *Antennas and Propagation, IEEE Transactions on*, vol. 62, no. 3, pp. 1378–1385, March 2014.

[15] C. Chen and M. Jensen, "Secret Key Establishment Using Temporally and Spatially Correlated Wireless Channel Coefficients," *Mobile Computing, IEEE Transactions on*, vol. 10, no. 2, pp. 205–215, Feb 2011.

[16] J.-P. Cheng, Y.-H. Li, P.-C. Yeh, and C.-M. Cheng, "MIMO-OFDM PHY Integrated MOPI Scheme for Confidential Wireless Transmission," in *Wireless Communications and Networking Conference (WCNC), 2010 IEEE*, April 2010, pp. 1–6.

[17] P.-C. Y. C.-H. L. Chih-Yao Wu, Pang-Chang Lan and C.-M. Cheng, "Practical Physical Layer Security Schemes for MIMO-OFDM Systems Using Precoding Matrix Indices," *IEEE journal on selected areas in communications*, vol. 31, no. 9, pp. 1687–1700, Sept. 2013.

[18] B. Zan, M. Gruteser, and F. Hu, "Key Agreement Algorithms for Vehicular Communication Networks Based on Reciprocity and Diversity Theorems," *Vehicular Technology, IEEE Transactions on*, vol. 62, no. 8, pp. 4020–4027, Oct 2013.

[19] D. Pinchera and M. Migliore, "Effectively Exploiting Parasitic Arrays for Secret Key Sharing," *Vehicular Technology, IEEE Transactions on*, vol. PP, no. 99, pp. 1–1, 2015.

[20] L. Mailaender, "On the Geolocation Bounds for Round-trip Time-of-Arrival and All Non-Line-of-Sight Channels," *EURASIP J. Adv. Signal Process*, vol. 2008, Jan. 2008. [Online]. Available: http://dx.doi.org/10.1155/2008/584670

[21] A. Badawy, T. Khattab, T. El-Fouly, A. Mohamed, D. Trinchero, and C.-F. Chiasserini, "Secret Key Generation Based on AoA Estimation for Low SNR Conditions," in *Vehicular Technology Conference (VTC Spring), 2015 IEEE 81st*, May 2015, pp. 1–7.

[22] W. Wang, H. Jiang, X. Xia, P. Mu, and Q. Yin, "A Wireless Secret Key Generation Method Based on Chinese Remainder Theorem in FDD Systems," *Science China Information Sciences*, vol. 55, no. 7, pp. 1605–1616, 2012.

[23] S. Goldberg, Y. Shah, and A. Reznik, "Method and Apparatus for Performing JRNSO in FDD, TDD and MIMO Communications," Mar. 19 2013, uS Patent 8,401,196. [Online]. Available: http://www.google.co.uk/patents/US8401196

[24] X. Wu, C. Hu, Y. Peng, H. Zhao, and H. Duan, "Secret Key Extraction Based on Uplink CFR Estimation for OFDM-FDD System," in *Communication Technology (ICCT), 2013 15th IEEE International Conference on*, Nov 2013, pp. 37–41.

[25] A. Mahmood and M. Jensen, "Impact of Array Mutual Coupling on Multi-Antenna Propagation-Based Key Establishment," *Antennas and Propagation, IEEE Transactions on*, vol. PP, no. 99, pp. 1–1, 2015.

[26] C. Jiang, M. Wang, C. Yang, F. Shu, J. Wang, W. Sheng, and Q. Chen, "MIMO Precoding Using Rotating Codebooks," *Vehicular Technology, IEEE Transactions on*, vol. 60, no. 3, pp. 1222–1227, March 2011.

[27] V. Prabhu, S. Karachontzitis, and D. Toumpakaris, "Performance Comparison of Limited Feedback Codebook-Based Downlink Beamforming Schemes for Distributed Antenna Systems," in *Wireless Communication, Vehicular Technology, Information Theory and Aerospace Electronic Systems Technology, 2009. Wireless VITAE 2009. 1st International Conference on*, May 2009, pp. 171–176.

[28] D. Yang, L.-L. Yang, and L. Hanzo, "DFT-Based Beamforming Weight-Vector Codebook Design for Spatially Correlated Channels in the Unitary Precoding Aided Multiuser Downlink," in *Communications (ICC), 2010 IEEE International Conference on*, May 2010, pp. 1–5.

[29] L. T. C.-C. Jay Kuo, Shang-Ho Tsai and Y.-H. Chang, *Precoding Techniques for Digital Communication Systems*. Springer US, 2008. [Online]. Available: http://www.springer.com/us/book/9780387717685

[30] T.-H. Chou, S. Draper, and A. Sayeed, "Secret Key Generation from Sparse Wireless Channels: Ergodic Capacity and Secrecy Outage," *Selected Areas in Communications, IEEE Journal on*, vol. 31, no. 9, pp. 1751–1764, September 2013.

[31] N. Ferdinand, D. da Costa, A. de Almeida, and M. Latva-aho, "Physical Layer Secrecy Performance of TAS Wiretap Channels with Correlated Main and Eavesdropper Channels," *Wireless Communications Letters, IEEE*, vol. 3, no. 1, pp. 86–89, February 2014.

[32] E. Jorswieck, S. Tomasin, and A. Sezgin, "Broadcasting Into the Uncertainty: Authentication and Confidentiality by Physical-Layer Processing," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1702–1724, Oct 2015.

[33] C.-J. Chen and L.-C. Wang, "Performance Analysis of Scheduling in Multiuser MIMO Systems with Zero-Forcing Receivers," *Selected Areas in Communications, IEEE Journal on*, vol. 25, no. 7, pp. 1435–1445, September 2007.

[34] C. Siriteanu, Y. Miyanaga, S. Blostein, S. Kuriki, and X. Shi, "MIMO Zero-Forcing Detection Analysis for Correlated and Estimated Rician Fading," *Vehicular Technology, IEEE Transactions on*, vol. 61, no. 7, pp. 3087–3099, Sept 2012.

[35] C. Ye, A. Reznik, and Y. Shah, "Extracting Secrecy from Jointly Gaussian Random Variables," in *Information Theory, 2006 IEEE International Symposium on*, July 2006, pp. 2593–2597.

[36] U. Maurer and S. Wolf, "Unconditionally Secure Key Agreement and The Intrinsic Conditional Information," *Information Theory, IEEE Transactions on*, vol. 45, no. 2, pp. 499–514, Mar 1999.

[37] 3GPP, "Spatial Channel Model for Multiple Input Multiple Output (MIMO) Simulations, Version 12.0.0 Release 12," 3rd Generation Partnership Project (3GPP), TR 25.996, Sep. 2014.

[38] 3GPP, "Measurement of Radiated Performance for Multiple Input Multiple Output (MIMO) and Multi-Antenna Reception for High Speed Packet Access (HSPA) and LTE Terminals, Version 12.0.0 Release 12," 3rd Generation Partnership Project (3GPP), TR 37.976, Oct. 2014.

[39] R. B. Arellano-Valle, J. E. Contreras-Reyes, and M. G. Genton, "Shannon Entropy and Mutual Information for Multivariate Skew-Elliptical Distributions," *Scandinavian Journal of Statistics*, vol. 40, no. 1, pp. 42–62, 2013. [Online]. Available: http://dx.doi.org/10.1111/j.1467-9469.2011.00774.x

[40] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004. [Online]. Available: https://books.google.co.uk/books?id=mYm0bLd3fcoC

[41] T. Marzetta and B. Hochwald, "Capacity of a Mobile Multiple-Antenna Communication Link in Rayleigh Flat Fading," *Information Theory, IEEE Transactions on*, vol. 45, no. 1, pp. 139–157, Jan 1999.