Secret Key Generation Using Channel Quantization with SVD for Reciprocal MIMO Channels

Haji M. Furqan*, *Student Member, IEEE*, Jehad M. Hamamreh* and Huseyin Arslan*§, *Fellow, IEEE*
*School of Engineering and Natural Sciences, Istanbul Medipol University, Istanbul, Turkey, 34810
§Department of Electrical Engineering, University of South Florida, Tampa, FL, 33620

Abstract—**The generation of secret keys from reciprocal wireless channel by exploiting their randomness nature, is an emerging area of interest to provide secure communication. One of the main challenges in this domain is to increase the secret key length, extracted from the shared channel coefficients between two legitimate communication parties, while maintaining its randomness and uniformity. In this work, we develop a practical key generation method, based on channel quantization with singular value decomposition (CQSVD), which is capable of significantly increasing the generated secret key in MIMO systems. This is achieved through quantizing the phases and amplitudes of the estimated MIMO channel coefficient's matrix by using an alternative form of SVD, where the key sequence is extracted from the orthogonal basis functions of the decomposed channel. In this method, it is shown that for an $M \times M$ antenna system, with M^2 independent channel fading coefficients, a secret key sequence of length $2M^3$ can be generated. The extracted key sequence is transformed to a random phase sequence, which is then used to manipulate the transmitted data on a symbol level basis rather than bit level-basis, to provide more secure communication. The comparative simulation results show that the proposed CQSVD method outperforms the state of the art secret key generation methods.**

I. Introduction

Due to the broadcast nature of wireless signals, the security of wireless devices is becoming more challenging than before. Traditional security techniques are mainly based on cryptographic keys [1] to fulfill the security requirements [2]. However, key establishment, management and distribution processes in wireless networks, are challenging, especially with current and future heterogeneous and de-centralized networks. Recently, physical layer security has drawn great research interest because of its capability in eliminating the requirement of an authenticated communication channel, to manage and distribute keys, by using channel and noise measurement as a source of randomness to generate secret keys [2], [3].

In physical layer-based key generation, the transmitter and receiver extract random sequences, called secret keys, from the random variations of the reciprocal wireless channel between them, and then use them to encrypt and decrypt the data by performing similar processing at their sides [4], [5]. The fundamental theoretical work behind this direction can be traced back to [6], which is very similar to the work independently done in [7], [8]. The secret key generation analysis made in [6], was extended to account for the presence of an active eavesdropper in [9]-[11]. In [12], researchers proposed a technique that uses the short term reciprocity of the radio channel to secure information, in which, the exchange of information does not require the availability of a common secure key between two users since the phase of the fading coefficients are used as a secret key. The proposed technique in [12] can also be used for cryptographic key agreement between two users. In [13], a technique, which directly quantizes the complex channel coefficients, was suggested. In [14], discretizing the extracted coefficients of some practical and standardized multipath components, was investigated. In [15], level crossing rates of the fading processes are exploited for key generation. In [16], channel estimates are used as correlated random variable for information reconciliation. Quantization of channel phases to generate longer keys for a multi-tone communication system was studied in [17]-[19]. On the other hand, the authors of [20], [21] used time-varying frequency characteristics of OFDM wireless systems to explore channel based key generation and key agreement.

Multiple-antenna based devices are capable of significantly increasing the randomness of channel, which can be used for secret key generation and agreement. Recently, multiple antenna links and the corresponding secrecy and secret key rates are studied in [22], [27]. In [23], the secret key rate for the basic source model with a MIMO channel was studied. In [24], a practical multiple-antenna based key generation technique is presented, in which the randomness is extracted from the measured received signal strength indicator (RSSI). It was shown that the increase in the number of antennas at Eve could not infer more information to her about the secret keys generated from the main channel. In [25], the author proposed two practical key generation techniques for the MIMO-OFDM systems. The first is based on using precoding matrix indicator (PMI) for secret key generation, while the second matrix is based on channel quantization for increasing the length of the secret key. In RSSI and channel quantization-based key generation techniques [27], the length of the generated key is not only affected by the channel randomness, but also by the quantization method applied on the estimated channel coefficients.

In this work, we develop and propose a key generation method based on channel quantization with SVD (CQSVD), for increasing the generated key length in MIMO systems. In specific, the amplitudes and phases of the complex MIMO channel coefficients, are quantized using the proposed CQSVD method. By using this method, it is shown that a key vector of length $2M^3$ can be generated from a block fading $M \times M$ MIMO channel. To achieve key renewal process, the generated

978-1-5090-2061-4/16/$31.00 ©2016 IEEE

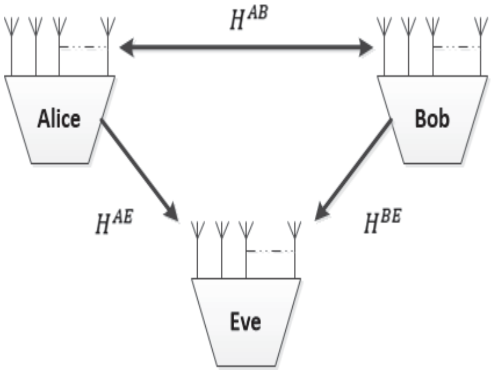

Fig. 1. The wireless communications scenario considered in this work.

key vector can be updated over each fading block or after several blocks. Moreover, in this work, encryption is performed on a symbol level basis rather than bit level-basis to provide more secure communication, since in this case brute force attack cannot easily be performed on the application layer without using specific devices to capture the data symbols. The obtained results prove that the employment of such method can significantly increase the key length, without causing high key mismatch probability or breaking its uniformity and randomness. Additionally, since the operation of this method highly depends on the channel, the key performance is tested against the effect of imperfect channel estimation and imperfect reciprocity.

The rest of the paper is organized as follows. In Section II, the system model is presented. Then, the proposed method is explained in Section III. In Section IV, the simulation results are discussed, while the conclusion is drafted in Section V.

II. SYSTEM MODEL AND PRELIMINARIES

We consider a spatial multiplexing MIMO communication system model as presented in Fig. 1. In particular, a legitimate source (Alice) and a legitimate user (Bob), that are equipped with multiple antennas denoted by M_t and M_r, respectively, want to generate a shared secret key vector by using the channel related information, i.e., amplitude and phase. The antenna spacing at each terminal is at least have wavelength $(\frac{\lambda}{2})$ to provide sufficiently de-correlated signals. Also, there is a passive adversary, Eve, who tries to eavesdrop on the communication between Alice and Bob. Eve is equipped with multiple antennas (M_e) and can listen to all the communication between Alice and Bob, and she also knows the key extraction algorithm. We also assume that Eve cannot be very close to legitimate nodes, i.e., Eve's distance to legitimate nodes cannot be less than few multiples of the wavelength [26]. This will ensure that Bob and Eve experience independent channel realizations [6]. Under these assumptions, Alice first transmits a reference signal to Bob for channel estimation and then Bob sends back a reference signal to Alice and after that they apply CQSVD method, which will be explained in detail in the next section. After that, Alice applies symbol level encryption on the transmitted data symbol vector $\mathbf{x_n} \in C^{M_t \times 1}$ using a phase randomization (PR) vector, made from the extracted key. Alice then transmits the resulting encrypted data symbol vector $\mathbf{x} \in C^{M_t \times 1}$ to Bob. The baseband received signal at Bob's side in a matrix form is given by

$$\mathbf{y^b} = \sqrt{\frac{E_x}{M_t}}\mathbf{H^b}\mathbf{x} + \mathbf{z^b} \tag{1}$$

where, E_x is the symbol energy, M_t is the number of transmit antennas, $\mathbf{H^b} \in C^{[M_r \times M_t]}$ and $\mathbf{z_b} \in C^{M_r \times 1}$ are the complex channel response and the zero-mean complex additive white Gaussian noise (AWGN) of Bob's channel, respectively. The baseband received signal at Eve's side in matrix form is given by

$$\mathbf{y^e} = \sqrt{\frac{E_x}{M_t}}\mathbf{H^e}\mathbf{x} + \mathbf{z^e} \tag{2}$$

Where $\mathbf{H^e}$ and $\mathbf{z^e}$ are the complex channel response, and AWGN of the Eve's channel, respectively. It should be noted that in this system we assume that each antenna (independent of the others) experiences a one-tap Rayleigh fading channel with constant channel gain over one packet length, but independent and identically distributed (i.i.d) from one packet to another. Accordingly, the minimum mean square error (MMSE) signal detection at Bob's and Eve's side is given by [28] as follows

$$\begin{aligned} \hat{\mathbf{x}}^{b/e}_{MMSE} &= \hat{\mathbf{W}}^{b/e}_{MMSE}\mathbf{y}^{\mathbf{b/e}} && (3)\\ &= (\mathbf{H}^{*\mathbf{b/e}}\mathbf{H}^{\mathbf{b/e}} + \sigma_z^2\mathbf{I})^{-1}\mathbf{H}^{*\mathbf{b/e}}\mathbf{y}^{\mathbf{b/e}} && (4)\\ &= \hat{\mathbf{x}}_{b/e} + (\mathbf{H}^{*\mathbf{b/e}}\mathbf{H}^{\mathbf{b/e}} + \sigma_z^2\mathbf{I})^{-1}\mathbf{H}^{*\mathbf{b/e}}\mathbf{z}^{\mathbf{b/e}} && (5)\end{aligned}$$

Where $\mathbf{H}^*$ is the hermitian transpose of the channel, while $\hat{\mathbf{x}}_{MMSE}$ is the estimated signal by using MMSE detection method. After this step, the receiver, Bob will apply symbol based decryption to get the original version of the signal, while Eve will receive a degraded version of the signal.

III. PROPOSED CQSVD METHOD

In this section, we explain our proposed CQSVD method to generate a PR vector for symbol level encryption as presented in Fig. 2. Under the assumption of channel reciprocity, $H^{AB} = (H^{BA})^T$, where H^{AB} and H^{BA} are the channels between Alice and Bob and between Bob and Alice, respectively, and $(.)^T$ stands for the transposition. In this way, Alice and Bob are able to compute similar information for key generation, but Eve is unable to generate similar key [27]. Hence, channels between Alice and Eve H^{AE} and between Bob and Eve H^{BE} are independent to H^{AB} and H^{BA}, respectively. To generate shared secret key vector (PR vector) in the multiple antenna system by using CQSVD method, Alice and Bob perform the following main steps:

(A) Estimation of the complex channel coefficient's matrix.
(B) Decomposition of the channel matrix.
(C) Generation of random matrices.
(D) Reshaping to generate PR vector.

Each of the main step has further small sub-steps. The detail of the main steps and their sub-steps is as follows:

A. Estimation of the complex channel coefficient's matrix

1) In the first step, Alice sends a reference signal $\mathbf{ref} \in C^{M_t \times 1}$ to Bob for channel estimation.
2) Bob estimates the channel $H^{AB} \in C^{[M_r \times M_t]}$ and sends a reference signal to Alice (within coherence time).
3) Alice also estimates the channel $H^{BA} \in C^{[M_r \times M_t]}$ from reference signal.

B. Decomposition of channel matrix

After estimating the channel matrix {H} at both Alice and Bob, each node will do the following steps:

1) Finding magnitudes and phases of the matrix {H}.
2) In order to generate PR vector for encryption, the channel magnitude matrix and phase matrix are decomposed by using simple SVD or alternative SVD, and then step (C) and (D) are performed. Firstly, we will explain matrix decomposition by using simple SVD and then by using alternative SVD. In linear algebra, SVD states that a rectangular matrix $\mathbf{G} \in C^{[M_r \times M_t]}$ can be factorized into product of three matrices [29] as follows:

$$SVD\{\mathbf{G}\} = \mathbf{USV^T}, \tag{6}$$

where $\mathbf{S}$ is a diagonal matrix, $\mathbf{U}$ is a unitary matrix and $\mathbf{V^T}$ is the transpose of another unitary matrix. Firstly, We apply simple form of SVD on the channel's magnitude and phase matrix and then implement step (C) and (D) to generate PR vector for encryption. Since applying SVD on the channel's magnitude and phase matrix gives 6 matrices, each has size of ($M \times M$), where four of them are unitary matrices, while the other two are diagonal matrices, the total length of resulting PR vector by using simple SVD is $4M^2 + 2M$ as presented in Fig. 2. However, the length can further be increased by using an alternative form of SVD as presented in Fig. 2. The alternative form of SVD can be used to decompose any matrix $\mathbf{G} \in C^{[M_r \times M_t]}$ into a weighted, ordered sum of M separable matrices [29] as follows:

$$\mathbf{G} = \sum_{i=1}^{M} \mathbf{A_i} = \sum_{i=1}^{M} \sigma_\mathbf{i} \mathbf{u_i} \otimes \mathbf{v_i} \tag{7}$$

where $\mathbf{u_i}$ and $\mathbf{v_i}$ are the i^{th} columns of the corresponding SVD matrices $\mathbf{U}$ and $\mathbf{V}$, respectively, and $\sigma_\mathbf{i}$ is the i^{th} ordered singular values from $\mathbf{S}$, and each $\mathbf{A_i}$ is $M \times M$ matrix. Note that the number of non-zero σ_i is exactly the rank of the matrix. So, by using this alternative form of SVD both the channel amplitude matrix as well as channel phase matrix are decomposed into M matrices, each of which contains $M \times M$ elements. In this way, we get total $2M$ quantized matrices per MIMO channel observation, and from which PR vector of length $2M^3$ can be obtained by applying steps (C) and (D), which is much more longer than the length of PR vector by simple SVD case that is $4M^2 + 2M$ as presented in Fig. 2. So, we prefer to use alternative form of SVD in CQSVD method.

C. Generation of PR matrices

After getting matrices from alternate form of SVD, both Alice and Bob will apply the following procedure on each matrix to generate PR matrices.

1) Take the mean p of each matrix and compare it with every entry of matrix A. If the value of any element is greater than p assign one to that index, else assign zero. With this procedure the resultant matrix will contain random values of 1's and 0's.
2) As explained earlier that our scheme is based on symbol level encryption, so we have to convert 1's and 0's into phases. We achieve this task by multiplying each element in the matrix by 2, subtracting 1 and then multiplying by "j", $(2 \times A - 1) \times 1j$, where j is an imaginary number. The resultant matrix is called PR matrix. We apply the above mentioned procedure on each of the remaining matrices.

D. Reshaping to generate PR vector

1) Finally, we concatenate these PR matrices into one vector called PR vector of length $2M^3$.
2) In the literature of channel-based secret key generation methods, data encryption is usually applied on a bit level basis. However, in our method, the extracted secret key is applied on a symbol level basis as it is composed of random phases instead of random bits. This feature increases the security level against eavesdroppers as compared to bit level encryption.

After generating PR vector, Alice generates a signal, modulates it and divides modulated symbols into M_t streams, in such a way that each frame contains $2M^3$ symbols, and then encrypt these symbols by multiplying each symbol with an element of PR vector, for example, encryption of any symbol x_n is given by

$$r_k = Ae_k^\phi \tag{8}$$

$$x = x_n r_k \tag{9}$$

where r_k is an element in PR vector, $A = 1$ and $\phi_k \in j, -j$ are amplitude and phase of r_k, respectively, x_n is the original data symbol and x is the encrypted symbol. The process of decryption x is performed at Bob by dividing output of MMSE detector by r_k.

$$\hat{x_n} = \hat{x}/r_k = Ae_k^\phi \tag{10}$$

In this way, Bob will get the original symbol. It is mentioned in [27] that theoretical results predict M^2 growth of key generation rates, without channel quantization, for a MIMO system. However, key of length longer than M^2 can be generated by using different method of quantization [27]. Hence, by using SVD, at high SNR, we can generate a key vector of length $4M^2 + 2M$. This length can further be enlarged by using alternate SVD, which can generate a key vector of length $2M^3$. It should be emphasized that unlike the quantization techniques in [5], [17] and [27], which require public sharing of information about the used quantization

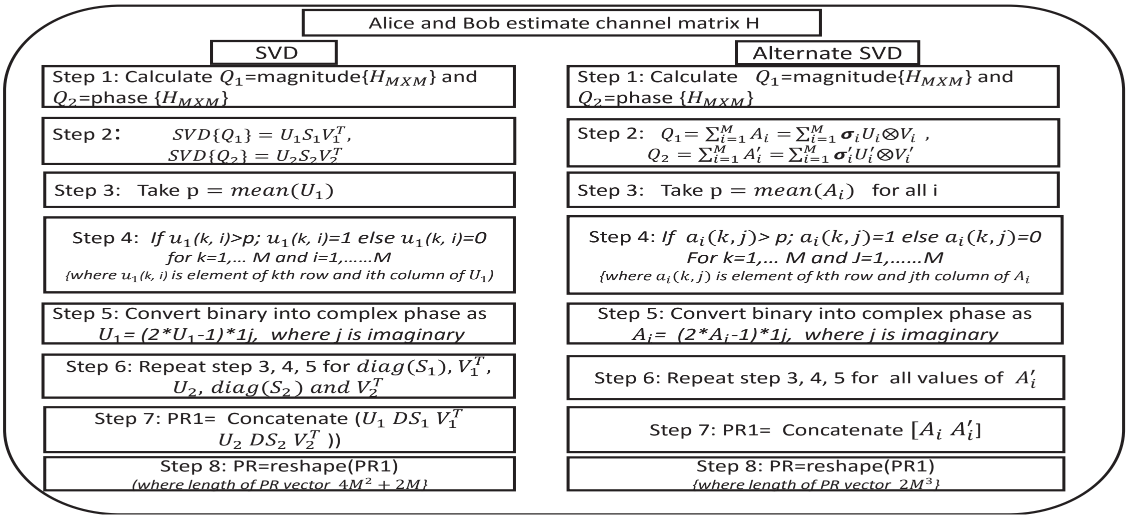
Alice and Bob estimate channel matrix H
SVD
Step 1: Calculate Q_1=magnitude$\{H_{MXM}\}$ and Q_2=phase $\{H_{MXM}\}$
Step 2: $SVD\{Q_1\} = U_1 S_1 V_1^T$, $SVD\{Q_2\} = U_2 S_2 V_2^T$
Step 3: Take p $= mean(U_1)$
Step 4: If u_1(k, i)>p; u_1(k, i)=1 else u_1(k, i)=0 for k=1,... M and i=1,......M {where u_1(k, i) is element of kth row and ith column of U_1)
Step 5: Convert binary into complex phase as U_1= (2*U_1-1)*1j, where j is imaginary
Step 6: Repeat step 3, 4, 5 for $diag(S_1), V_1^T$, U_2, $diag(S_2)$ and V_2^T
Step 7: PR1= Concatenate (U_1 DS_1 V_1^T U_2 DS_2 V_2^T))
Step 8: PR=reshape(PR1) (where length of PR vector $4M^2 + 2M$}
Alternate SVD
Step 1: Calculate Q_1=magnitude$\{H_{MXM}\}$ and Q_2=phase $\{H_{MXM}\}$
Step 2: $Q_1 = \sum_{i=1}^{M} A_i = \sum_{i=1}^{M} \boldsymbol{\sigma}_i U_i \otimes V_i$, $Q_2 = \sum_{i=1}^{M} A_i' = \sum_{i=1}^{M} \boldsymbol{\sigma}_i' U_i' \otimes V_i'$
Step 3: Take p $= mean(A_i)$ for all i
Step 4: If $a_i(k,j)$> p; $a_i(k,j)$=1 else $a_i(k,j)$=0 For k=1,... M and J=1,......M {where $a_i(k,j)$ is element of kth row and jth column of A_i
Step 5: Convert binary into complex phase as A_i= (2*A_i-1)*1j, where j is imaginary
Step 6: Repeat step 3, 4, 5 for all values of A_i'
Step 7: PR1= Concatenate $[A_i\ A_i']$
Step 8: PR=reshape(PR1) {where length of PR vector $2M^3$}

Fig. 2. SVD and Alternate SVD based channel quantization method.

level, the proposed CQSVD method does not require sending any public messages about quantization. To reduce the key mismatch probability between the estimated keys and increase its robustness, we propose using powerful estimators, whose training data symbols are long enough and have sufficient power.

It should be noted that in our algorithm due to the comparison with the mean in the process of key generation (Step C), the key is expected to be uniform and it will be shown in the next section. The randomness of our key is verified by using Run test function for randomness provided by MATLAB Statistics Toolbox (2015) as h=runstest($\mathbf{r}$), where $\mathbf{r}$ is our generated key vector (Step C). This function returns a test decision for the null hypothesis that the values in the data vector $\mathbf{r}$ come in random order, against the alternative that they do not. The test is based on the number of runs of consecutive values above or below the mean of $\mathbf{r}$. The value of result h is 1 if the test rejects the null hypothesis at the 5 % significance level, or the value is 0 otherwise [30], where $h = 0$ means random and $h = 1$ means not random. In our case, several tests are carried out for different channel and all of them have given a result of zero, which means the key is random.

IV. Simulation Results

In this section, simulation results are presented to analyze the effectiveness of the proposed secret key generation scheme based on CQSVD method. In order to fully assess the performance of the generated key, two main metrics, which reflect the effect of the estimated channel and the adopted quantization method, are evaluated. These metrics include key mismatch probability (error rate) and key rate (efficiency) per matrix of MIMO channel coefficients. Moreover, the CQSVD is compared with the state of the art channel quantization alternating (CQA) method for key generation from reciprocal MIMO channels [31]. In all the simulations, imperfect channel estimation and imperfect channel reciprocity due to possible realistic synchronization, interference and noise errors are taken into account. This is performed by introducing intentional independent estimation errors to both Alice and Bob. Thus, the estimated erroneous channels at Alice and Bob can be modeled as $\mathbf{\hat{H}^a} = \mathbf{H} + \mathbf{\Delta H^a}$ and $\mathbf{\hat{H}^b} = \mathbf{H} + \mathbf{\Delta H^b}$, respectively, where $\mathbf{H}$ is the true channel. $\mathbf{\Delta H^a}$ and $\mathbf{\Delta H^b}$ are modeled as independent complex Gaussian noise vectors with zero mean and error variance $\sigma^{\mathbf{2}} = e \times 10^{\frac{-SNR_{dB}}{10}}$. It should be emphasized that the error variance value of the estimated channel depends on the quality of the adopted estimator, which is highly affected by the length of the training sequence and its power. Thus, three variances with different e's, corresponding to three different estimators, are considered.

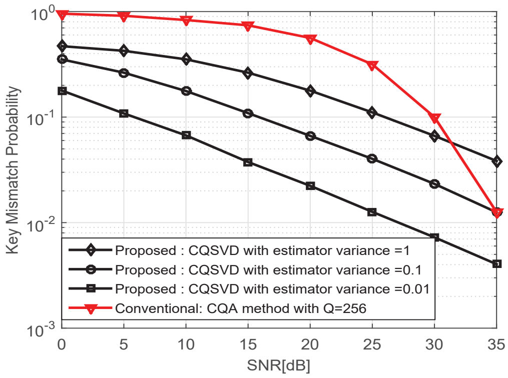

Fig. 3. Secret key mismatch probability (key error rate) under imperfect channel estimation and imperfect channel reciprocity.

Fig. 3 shows the key mismatch probability (KMP) between the generated key sequences at Alice and Bob, whose estimated erroneous channels are independent, but have equal variance value since the same estimators are considered at both sides. It is clear that as $\sigma^{\mathbf{2}}$ decreases by reducing e

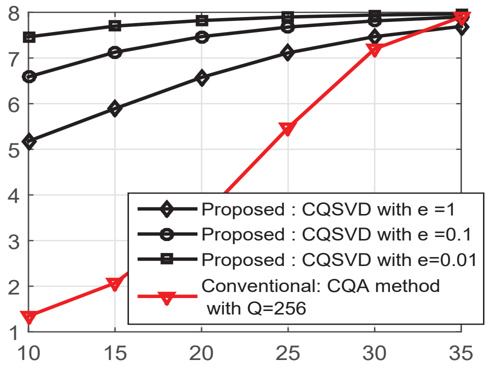

Fig. 4. Secret key rate (efficiency= Bits/channel coefficient) vs SNR, under imperfect channel estimation and imperfect channel reciprocity.

from 1 to 0.01, the KMP of the proposed method (CQSVD) also decreases. Also, it is shown that CQSVD outperforms CQA method with a quantization level Q equals to 256, at SNRs less than 30. It should be mentioned that CQA method can have different Q values. However, for fair comparison, Q=256 is selected for comparison since CQA with Q=256 can generate the same key rate as that of CQSVD at high SNR, as it can be shown in Fig. 4 at SNR=35 dB. For more details about CQA, readers can refer to [27]. Fig. 4 presents the possible key rate measured in terms of bits per single estimated channel coefficient and is defined as the average identical number of bits that can be extracted from a single channel coefficient. It is evident from Fig. 4 that CQSVD exceeds CQA at low SNRs since the channel quantization process in CQSVD exploits the orthogonality property brought by SVD, instead of sector segmentation process employed by CQA, which is more sensitive to noise than CQSVD. However, at high SNRs, it is noticed that both CQSVD and CQA have the same key rate as both methods become noise-error free. In general, for a block fading $M \times M$ MIMO system with M^2 channel degree of freedom (coefficients), the length (L) of the generated key can be defined as $L = M^2(1-KMP)c$, where $c = 2M$ is the maximum number of generated bits per estimated channel coefficient. Furthermore, the secrecy rate (SR) can be defined as $SR = (1 - KMP)c$. In Fig. 5, we show the distribution of the key before conversion into complex phase (Section III, Step C). It is clear that our key vector is approximately uniform. Fig. 6 presents the phases of the complex RP vector (Section III, Step D). It is clear that key is approximately random. The randomness is also verified by run test function, provided by MATLAB Statistics Toolbox (2015) (as explained earlier in Section III).

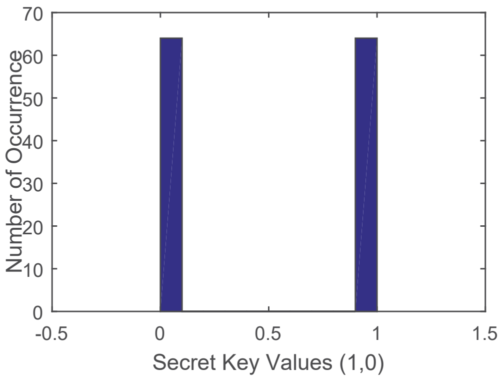

Fig. 5. Distribution of elements of PR key vector (step D1) (uniformity).

Now, since the proposed scheme implements symbol level encryption by using the generated PR vector, it is of importance to test the effect of the developed technique on data communication. This can be characterized by calculating the BER performance versus SNR [2]. The simulation parameters of the considered spatial multiplexing MIMO system are presented in Table I. In the simulation, in order to check the robustness of the method, both imperfect channel estimation (ICE) and imperfect channel reciprocity (ICR) are considered at all communication parties [32]. In specific, channel estimation errors are modeled as mentioned before and we will show performance for $e = 0.01$ and $e = 0.001$. Fig. 7 presents the effect of employing secret key generation using CQSVD method on the BER performance of the considered spatial multiplexing MIMO system. It is shown that ICE and ICR lead to a small degradation in the BER, due to the mismatch between the generated PR vectors at both sides. It should be noted that the resulting small degradation can be overcome by

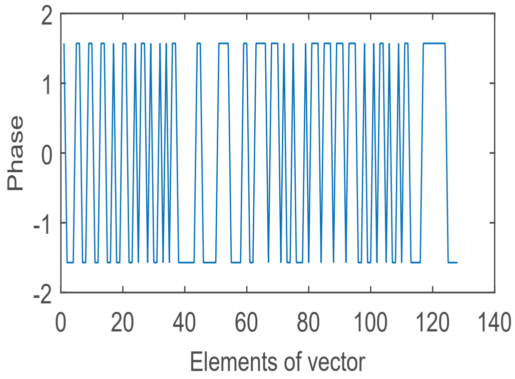

Fig. 6. Phase of final PR key vector (randomness).

TABLE I
Simulation Parameters

No of antenna at Tx	4
No of antenna at Rx	4
Block (Packet) length	128
Modulation	4-QAM
No. of Packets/frame	1000
No. of frames	128
Equalization type	MMSE
Fading type	Raleigh fading channel

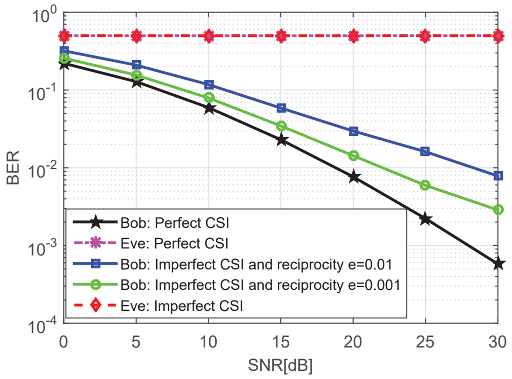

Fig. 7. BER performance of RP method with QPSK under imperfect channel estimation and imperfect channel reciprocity.

increasing the training sequence length and its power, where better channel estimation can be obtained.

V. Conclusion

This paper has provided a secret key generation method, called CQSVD, which exploits the reciprocity of $M \times M$ MIMO channel. In this method, a phase randomization (PR) key vector for symbol level encryption is generated by applying alternative form of SVD on channel's phase and magnitude matrices. It was shown that for $M \times M$ MIMO channel, a key length of $(2M^3)$ can be generated. Simulations with a simple 4×4 MIMO channel have been presented. The scheme has been analyzed for perfect and imperfect channel estimation as well as for perfect and imperfect channel reciprocity.

Acknowledgment

This work has been supported by The Scientific Research Council of Turkey (TUBITAK) under grant No. 114E244.

References

[1] C. E. Shannon, "Communication theory of secrecy systems", Bell Syst. Tech. J., vol. 28, pp. 656–715, Oct. 1949.

[2] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey", IEEE Commun. Surv. Tutorials, vol. 16, no. 3, pp. 1550–1573, 2014.

[3] H. Liu , J. Yang , Y. Wang and Y. Chen, "Collaborative secret key extraction leveraging received signal strength in mobile wirelessnetworks", Proc. IEEE INFOCOM, pp. 927–935, 2012.

[4] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust Key Generation from Signal Envelopes in Wireless Networks", Proc. 14th ACM Conf. Computer and Comm. Security (CCS), 2007.

[5] S. Mathur, W. Trappe, N.B. Mandayam, C. Ye and A. Reznik, "Radio-Telepathy: Extracting a Secret Key from an Unauthenticated Wireless Channel", Proc. ACM MobiCom, 2008.

[6] U. M. Maurer, "Secret key agreement by public discussion from common information", IEEE Trans. Inf. Theory, vol. 39, no. 3, pp. 733–742, May 1993.

[7] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. I. Secret sharing", IEEE Trans. Inf. Theory, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[8] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. II. CR capacity", IEEE Trans. Inf. Theory, vol. 44, no. 1, pp. 225–240, 1998.

[9] U. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels-part I: definitions and a completeness result", IEEE Trans. Inf. Theory, vol. 49, no. 4, pp. 822–831, Apr. 2003.

[10] U. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels-part II: the simulatability condition", IEEE Trans. Inf. Theory, vol. 49, no. 4, pp. 832–838, Apr. 2003.

[11] U. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels-part III: privacy amplification", IEEE Trans. Inf. Theory, vol. 49, no. 4, pp. 839–851, Apr. 2003.

[12] H. Koorapaty, A. A. Hassan and S. Chennakeshu, "Secure information transmission for mobile radio", IEEE Commun. Lett., vol. 4, no. 2, pp. 52–55, Feb. 2000.

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

[14] C. Ye, A. Reznik, G. Sternburg and Y. Shah, "On the Secrecy Capabilities of ITU Channels", in 2007 IEEE 66th Vehicular Technology Conference, pp. 2030–2034, 2007.

[15] C. Ye, "Information-theoretically secret key generation for fading wireless channels", IEEE Trans. Inf. Forensics Security, vol. 5, no. 2, pp. 240–254, 2010.

[16] T. Shimizu, H. Iwai and H. Sasaoka, "Reliability-Based Sliced Error Correction in Secret Key Agreement from Fading Channel," 2010 IEEE Wireless Communication and Networking Conference, Sydney, NSW, pp. 1–6, 2010.

[17] A. Sayeed and A. Perrig, "Secure wireless communications: Secret keys through multipath", Proc. Int. Conf. Acoust. Speech, Signal Processing, pp. 3013–3016, Mar. 2008.

[18] S. C. Draper and A. M. Sayeed, "Secret key generation through OFDM multipath channel", in 2011 45th Annual Conference on Information Sciences and Systems, pp. 1–6, 2011.

[19] Y. Liu, S. C. Draper, and A. M. Sayeed, "Exploiting Channel Diversity in Secret Key Generation From Multipath Fading Randomness", IEEE Trans. Inf. Forensics Secur., vol. 7, no. 5, pp. 1484–1497, 2012.

[20] Y. El Hajj Shehadeh, O. Alfandi, K. Tout, and D. Hogrefe, "Intelligent mechanisms for key generation from multipath wireless channels", in 2011 Wireless Telecommunications Symposium (WTS), pp. 1–6, 2011.

[21] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks", in 2011 Proceedings IEEE INFOCOM, pp. 1422–1430, 2011.

[22] F. Renna, M. Bloch, and N. Laurenti, "Semi-Blind Key-Agreement over MIMO Fading Channels", IEEE Transactions on Communications, vol. 61, no. 2, pp. 620–627, 2013.

[23] E. A. Jorswieck, A. Wolf and S. Engelmann, "Secret key generation from reciprocal spatially correlated MIMO channels", Proc. IEEE Global Telecommun. Conf., pp. 1245–1250, 2013.

[24] 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, pp. 1–9, 2010.

[25] C.-Y. Wu, P.-C. Lan, P.-C. Yeh, C.-H. Lee and C.-M. Cheng, "Practical Physical Layer Security Schemes for MIMO-OFDM Systems Using Precoding Matrix Indices", IEEE J. Sel. Areas Commun., vol. 31, no. 9, pp. 1687–1700, Sep. 2013

[26] A. Kraskov, H. Stogbauer, and P. Grassberger, "Estimating mutual information", Phys. Rev. E, vol. 69, no. 6, p. 066138, Jun 2004.

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

[28] Y. S. Cho, J. kim, W. Y. Yang, C. G. kang, "MIMO-OFDM Wireless Communication with MATLAB", John Wiley & Sons, Asia, 20 10, pp319–330.

[29] J. W. Demmel, Applied Numerical Linear Algebra. SIAM, Philadelphia, PA, 1997

[30] MATLAB and Statistics Toolbox Release 2015a The MathWorks, Inc., Natick, Massachusetts, United States.

[31] C. Chen and M. Jensen, "Secret key establishment using temporally and spatially correlated wireless channel coefficients", IEEE Trans. Mobile Computing, vol. 10, pp. 205–215, Feb 2011.

[32] J. M. Hamamreh, E. Guvenkaya, T. Baykas and H. Arslan, "A Practical Physical-Layer Security Method for Precoded OSTBCBased Systems", in 2016 IEEE Wireless Communications and Networking Conference (WCNC), Doha, Qatar, 3-6 April 2016.