Parameters Optimization of Quantization Schemes for Channel-Based Key Extraction

Yuhong Wang, Sumei Sun, Min Li Huang, Peng Hui Tan, Boon Shyang Lim and Yonghong Zeng
Institute for Infocomm Research, A*STAR, Singapore

***Abstract*— We propose a scheme which generates shared secret keys from the amplitude of frequency domain channel state information (CSI) of individual orthogonal frequency-division multiplexing (OFDM) subcarrier. A unique quantization scheme is proposed, with the use of two parameters, α and β, to set the quantization threshold. Based on multivariate Rayleigh distribution, we derive the analytical expressions for key bit disagreement rate (BDR) and key length. The theoretical analysis of BDR and key length aligns with the simulation results. We also present a mathematical model to optimize the parameters of our proposed quantization scheme and a guideline to set α and β. Our proposed method for iterative tuning of β can balance the number of zeros and ones in the generated key sequences so that the randomness requirement is met.**

Keywords— Physical layer security; Key extraction, OFDM; quantization;

I. INTRODUCTION

Physical-layer security has emerged as a new approach to enhance the security of wireless communication. It is generally viewed as a complementary measure to the existing classic authentication and cryptography mechanisms, rather than a replacement for them. By utilizing the wireless channel reciprocity property, we can extract randomness from the channels between legitimate users, resulting in highly unique and mutually agreeable secret keys. Key generation systems are typically assessed based on three key performance metrics: randomness, key generation rate (KGR), and key bit disagreement rate (BDR) [10]. However, as noted in [3] and [4], there is often a trade-off between these metrics.

A channel-based secret key extraction scheme typically comprises of three key steps [11]: (1) channel estimation, involving probing and estimation of the physical channel; (2) key bit extraction, which involves obtaining similar features between legitimate users, and (3) key reconciliation, which involves eliminating any differences between the extracted keys. In the key bit extraction step, the primary processing block is quantization, which involves mapping the channel measurements into binary (random) values.

A number of quantization techniques were developed and analyzed in literature [3][4][5][12][13]. Fundamentally, designing the quantizer involves adjusting the quantization threshold to strike a balance between randomness, KGR, and BDR. The quantization threshold can be determined in various ways, depending on the approach adopted. For example, [5] proposes to use the cumulative distribution function for the determination of the quantization threshold, while [15] utilizes a QAM demodulator quantizer to map the complex value channel estimation into secret key bits. On the other hand, [3] and [4] suggest determining the threshold based on the mean value μ and standard deviation σ, where the thresholds are computed as and $q_+ = \mu + \alpha\sigma$, $q_- = \mu - \alpha\sigma$, with $\alpha \geq 0$. Sample values that are above q_+ or below q_- are then converted to 1 or 0, respectively. While this quantization method can reduce BDR, as demonstrated in [3], it can also lead to a reduction in KGR. In order to further reduce key BDR and to reduce the redundancy, [3] proposes an excursion-based quantization scheme that replaces successive sequences of m sample values that lie on one side of a threshold with a single binary value (either 1 or 0).

In addition to [3][4], there are other literatures which have evaluated the performance of channel-based key extraction scheme [1] [2] [6]. [1] presents a framework to evaluate and compare channel-based key extraction schemes. [2] proposes a source model that evaluates known quantization methods, using the correlation coefficient as a metric to quantitatively measure the degree of reciprocity between legitimated users. [6] investigates the reliability of secret key generation under realistic estimation conditions, providing an analytical expression that relates channel signal-to-noise ratio (SNRs) and channel correlation coefficient to BDR.

Generally speaking, most of existing secret key generation methods exploit either received signal strength (RSS) [4][13] or channel state information (CSI) [14] [15] [16]. CSI-based key generation systems offer a higher KGR than RSS-based methods [14]. In [14], the CSI of multiple orthogonal frequency-division multiplexing (OFDM) subcarriers is exploited, resulting in higher KGR for both stationary and mobile scenarios. To further enhance the KGR, multiple antenna systems have been utilized in [17].

Although previous literatures have presented theoretical analyses, simulations, and experimental work on channel-based key extraction schemes, there are still several issues that remain unexplored. Our goal is to address two of these issues. Firstly, assuming that we use a quantization scheme that determines the threshold based on the mean value μ and standard deviation σ [3], we aim to determine the optimal quantization parameter α. This will allow us to maximize the key length (efficiency) of the channel-based key extraction scheme under the condition that BDR (robustness) requirement is met. Secondly, we investigate how to achieve a balanced number of zeros and ones in the generated key sequences after quantization. This is necessary in order to preserve their randomness property.

In this paper, we propose a scheme which generates shared secret keys from the amplitude of frequency domain CSI of OFDM signal. A unique quantization scheme is proposed, with the use of two parameters, α and β, to set the quantization

threshold. We analyze the BDR and key length in theory. The theoretical analysis of the BDR and key length aligns with the simulation results. We also present a mathematical model to optimize the parameters of our proposed quantization scheme and a guideline to set α and β in order to achieve randomness, robustness, and efficiency of the generated key bits.

The following are the main contributions of our work:

1) We propose a novel quantization scheme, which involves determining the thresholds as $q_+ = \mu + \alpha\sigma$ and $q_- = \mu - \alpha\beta\sigma$, with $\alpha >= 0$, $\beta>0$.
   We generate shared secret keys from the amplitude of frequency domain CSI of OFDM signal, which follows Rayleigh distribution. Since the probability density function of Rayleigh distribution is not symmetric about mean, the quantization scheme proposed by [3] can not guarantee that number of zeros and ones are balanced in the generated key sequences. We therefore introduce the parameter β to address the above issue. By tuning β we can achieved balanced number of zeros and ones in the generated key sequence so that the randomness requirement is met.
2) Based on multivariate Rayleigh distribution, we derive analytical expression which relates parameter α and β to BDR and key length. The theoretical analysis of the BDR and key length aligns with the simulation results.
3) We propose a mathematic model for the optimization of parameter α and β. Since BDR and key length are both function of α and β, our target is to maximize key length under the constraint that BDR requirement is met.
4) We propose a guideline which sets the value of α based on the correlation coefficient and BDR requirement, ensuring both efficiency and robustness. Furthermore we propose an iterative algorithm to automatically adjust β, guaranteeing its randomness properties.

The remainder of the paper is structured as follows. Section 2 outlines the system model used for key bit extraction. Section 3 details our proposed channel-based secret key extraction scheme. Section 4 provides the derivation of expressions for BDR and key length, while Section 5 introduces a mathematical model for parameter optimization and presents guidelines for setting α and β. Our work is concluded in Section 6.

II. System Model

We consider extracting a secret key in an OFDM system by utilizing the CSI values of individual sub-carriers as the basis of randomness. As shown in Fig.1, the wireless communication setup comprises of legitimate users, namely Alice (A) and Bob (B), as well as a possible eavesdropper, Eve. Assuming the wireless channel experienced at Alice and Bob are $H_{A,B}(f)$ and $H_{B,A}(f)$ respectively, where $f = k/T$ for k-th subcarrier and T is duration of OFDM symbol (not including cyclic prefix (CP)). The frequency domain signal received by Bob and Alice can be expressed as:

$$y_B(f) = H_{A,B}(f)S(f) + w_B(f) \quad (1a)$$

$$y_A(f) = H_{B,A}(f)S(f) + w_A(f) \quad (1b)$$

where, $S(f)$ is the known signal (such as preamble or pilot signal) transmitted by Alice and Bob, and $w_A(f)$ and $w_B(f)$ are the additive noise at Alice and Bob, respectively.

Based on received signal, Alice and Bob calculate channel estimates of $H_{A,B}(f)$ and $H_{B,A}(f)$ as follows:

$$\widehat{H}_{B,A}(f) = H_{B,A}(f) + w_B(f)/S(f) \quad (2a)$$

$$\widehat{H}_{A,B}(f) = H_{A,B}(f) + w_A(f)/S(f) \quad (2b)$$

The goal of key extraction is to facilitate the creation of two identical secret keys between Alice and Bob. To achieve this, probe packets are sent by both parties to probe the channel. Firstly, Bob sends a probe request, Alice receives the probe request and performs channel estimation. Then Alice sends a probe response, Bob receives the probe response and performs channel estimation. The time interval between the receiving of probe request and sending of probe response by Alice is Δt. If Δt is within the channel's coherence time, and Alice and Bob use the same carrier frequency to transmit signal, $\widehat{H}_{B,A}(f)$ and $\widehat{H}_{A,B}(f)$ should be highly correlated in theory. For system with Doppler frequency f_m, the coherence time T_c is approximately $T_c = 9/(16\pi f_m)$ [8]. Channel based-secret key extraction exploits the wireless channel reciprocity property, which is quantified by the channel correlation coefficient.

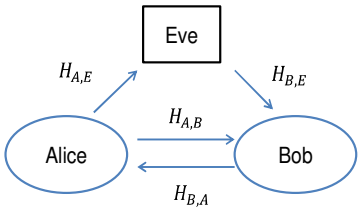

Fig. 1. Wireless Communication Setup Between Legitimate Users Alice (A) and Bob (B) with a possible eavesdropper Eve

According to [21], channel correlation coefficient is a function of time interval Δt, Doppler frequency f_m and SNR. Fig. 2 plots the channel correlation coefficient against the time interval Δt for TDL-B and TDL-C channels (as defined in [18]), with RMS delay spreads of 200 ns and 300 ns, respectively. The simulation is carried out using a carrier frequency of 5.2 GHz, and a moving speed of 3 km/hr, resulting in a corresponding Doppler frequency f_m of 14.45 Hz. We generated 5000 CSI packets for Alice and Bob, respectively, for each channel type and each time interval. Subsequently, we computed the Pearson correlation coefficient [2] of the CSI amplitude between Alice and Bob. The simulation results indicate that when the time interval is 12.5 ms and SNR is 20dB, the channel correlation coefficient is approximately 0.5, which is consistent with the theoretical analysis that predicts a correlation coefficient of 0.5 for a time interval of 12.4 ms. The graphs show that at the same time interval, as the SNR decreases, the channel correlation coefficient also decreases.

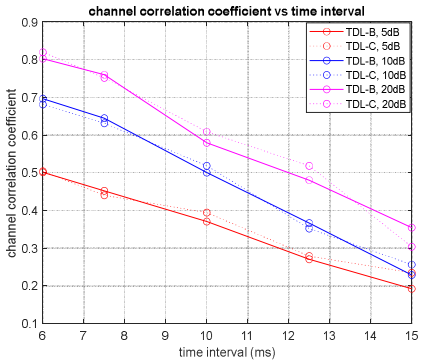

Fig. 2. Channel Correlation Coefficient vs time interval between Alice and Bob transmission time for TDL-B and TDL-C channels

III. OUR PROPOSED CHANNEL-BASED KEYEXTRACTION SCHEME

In theory, the wireless channel between Alice and Bob exhibits a property known as channel reciprocity, which allows for secret key bits to be extracted from CSI estimation $H_{A,B}(f)$ and $H_{B,A}(f)$. However, in practice, the carrier frequency offset (CFO) and differences in the analog-to-digital converter (ADC) sampling clock frequency between Alice and Bob can cause variations in the CSI estimates, which can result in the loss of channel reciprocity. [19] demonstrates that if the ADC sampling clock frequency offset between Alice and Bob is Δf, then there will be an additional phase rotation θ_m^k for k-th subcarrier of m-th OFDM symbol. Due to the additional phase rotation in channel estimation, the phase of $\hat{H}_{B,A}(f)$ and $\hat{H}_{A,B}(f)$ will not be correlated, however, the amplitude of $\hat{H}_{B,A}(f)$ and $\hat{H}_{A,B}(f)$ will still be correlated. Thus we will use $|\hat{H}_{B,A}(f)|$ and $|\hat{H}_{A,B}(f)|$ for key bit extraction.

As shown in Fig. 3, we propose to generate shared secret keys from the amplitude of frequency domain CSI of individual OFDM subcarriers. For each CSI packet, we evaluate the subcarrier amplitude correlation coefficient and choose subcarriers whose frequency intervals exceed the channel's coherent bandwidth. We then combine the selected subcarriers from multiple CSI packets and concatenate them into a CSI amplitude vector, which is then normalized. The resulting normalized CSI amplitude vector is fed to a CSI amplitude quantization block that converts the analog CSI amplitude into binary key bits.

Fig. 3. Our Proposed Key Bit Extraction Scheme

A. Evaluate the amplitude correlation coefficient and Subcarrier Selection

The coherence bandwidth in a multipath fading channel is determined by the multipath channel's delay spread. When the coherence bandwidth exceeds the subcarrier interval, adjacent subcarriers become correlated. If we use correlated subcarriers to extract key bits, the randomness of the extracted key bits may be compromised. As stated in [20], it is possible to derive keys from multiple subcarriers that are separated by G subcarriers.

Denote $\Lambda_{A,B}(n) = |\hat{H}_{A,B}(n/T)|$ and $\Lambda_{B,A}(n) = |\hat{H}_{B,A}(n/T)|$ as the amplitude of frequency domain CSI for subcarrier n, the amplitude correlation coefficient between subcarrier i and j can be expressed as,

$$\rho_{sc}(i,j) = \frac{\{\boldsymbol{x}(i)-\mu_i\}^T\{\boldsymbol{x}(j)-\mu_j\}}{\sigma_i\sigma_j} \quad (3)$$

where, $\boldsymbol{x}(i)$ and $\boldsymbol{x}(j)$ are amplitude vector for subcarrier i and j, respectively. μ_i and μ_j represent the mean values of subcarrier i and j, while σ_i and σ_j represent their standard deviation. $\boldsymbol{x}(l)(l = i,j)$ can be written as,

$$\boldsymbol{x}(l) = \left[\Lambda_{A,B}^{(1)}(l), \Lambda_{A,B}^{(2)}(l), \cdots, \Lambda_{A,B}^{(k)}(l), \cdots, \Lambda_{A,B}^{(P)}(l)\right]^T, l = i,j \quad (4)$$

where, $\Lambda_{A,B}^{(k)}(n)$ is the amplitude of frequency domain CSI for subcarrier n of k-th packet sent from Alice to Bob.

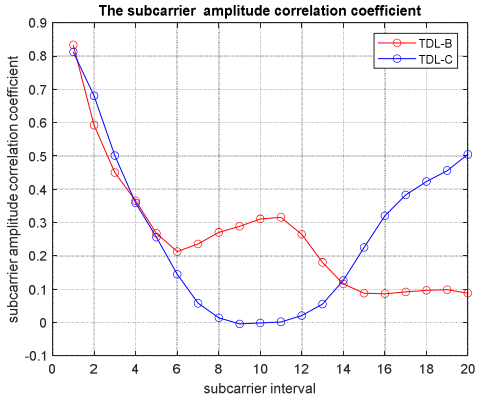

Fig. 4. Subcarrier amplitude correlation coefficient for TDL-B and TDL-C channels

Fig.4 shows subcarrier amplitude correlation coefficient for TDL-B and TDL-C channels. The graph shows that for TDL-B and TDL-C channels, when the subcarrier interval is 5, the subcarrier amplitude correlation coefficient is only 0.25. This suggests that these two subcarriers are not correlated with each other when the subcarrier interval G is 5. By analyzing the subcarrier amplitude correlation coefficient, we can determine the subcarrier interval G at which two subcarriers become uncorrelated. Our subcarrier selection method involves selecting one subcarrier from every G subcarriers. Despite having N subcarriers in the OFDM system, after subcarrier selection, we will only select $M = \lfloor N/G \rfloor$ subcarriers from each CSI packet.

B. Concatenation of CSI Amplitude and Normalizaiton

Denote $\{\gamma_{A,B}^{(k)}(1), \gamma_{A,B}^{(k)}(2), \cdots, \gamma_{A,B}^{(k)}(M)\}$ as the CSI amplitude vector of k-th CSI packet after subcarrier selection for Alice, then the concatenation of CSI amplitude vector from P packets can be written as:

$$\boldsymbol{\Omega_A} = [\gamma_{A,B}^{(1)}(1), \cdots, \gamma_{A,B}^{(1)}(k), \cdots, \gamma_{A,B}^{(1)}(M), \gamma_{A,B}^{(2)}(1), \cdots, \gamma_{A,B}^{(2)}(k), \cdots, \gamma_{A,B}^{(2)}(M), \cdots, \gamma_{A,B}^{(P)}(1), \cdots, \gamma_{A,B}^{(P)}(k), \cdots, \gamma_{A,B}^{(P)}(M)]^T \quad (5)$$

The cardinality of set $\boldsymbol{\Omega_A}$ is MP. It is important to note that the CSI amplitude vector $\boldsymbol{\Omega_A}$ must be normalized prior to quantization, such that every element $\gamma_{A,B}^{(k)}(l)$ in $\boldsymbol{\Omega_A}$ falls within the range [0, 1]. Similarly, we can define a normalized concatenated amplitude of the CSI vector for Bob, denoted as $\boldsymbol{\Omega_B}$, which also comprises of MP elements.

C. Quantization

Alice selects two threshold values $q_{A,+}$, $q_{A,-}$, which can be expressed as

$$q_{A,+} = \mu_A + \alpha\sigma_A \ , \quad (6a)$$

$$q_{A,-} = \mu_A - \alpha\beta\sigma_A \quad (6b)$$

where, μ_A and σ_A denote the mean value and standard deviation of all elements of $\boldsymbol{\Omega_A}$. Parameters α and β can be adjusted to satisfy the requirements for BDR, key length and randomness requirement. Similarly, Bob will choose two threshold values, $q_{B,+}$ and $q_{B,-}$, which can be expressed as,

$$q_{B,+} = \mu_B + \alpha\sigma_B \ , \quad (7a)$$

$$q_{B,-} = \mu_B - \alpha\beta\sigma_B \quad (7b)$$

where, μ_B and σ_B denote the mean value and standard deviation of all elements of $\boldsymbol{\Omega_B}$.

Once the quantization threshold has been established, Alice and Bob must come to a consensus on the indices that will be used to extract the secret key bits. Both Alice and Bob set a parameter known as the indexing window, denoted as w. The window size w may be predetermined or communicated through a public channel. Alice and Bob employ the following procedure to reach an agreement on the indices [3]:

1) Alice finds all disjoint subset of indexes $\{m_s, m_e\}$ that satisfy $\boldsymbol{\Omega_A}(m) \geq q_{A,+}$ or $\boldsymbol{\Omega_A}(m) < q_{A,-}$,$\forall\, m \in \{m_s, m_s+1, \cdots, m_e\}$. Alice sends the index $l_{A,x} = \{\left\lfloor \frac{m_s+m_e}{2} \right\rfloor\}$ to Bob through a public channel.

2) For every received index m_r, Bob checks whether $\boldsymbol{\Omega_B}(m) \geq q_{B,+}$ or $\boldsymbol{\Omega_B}(m) < q_{B,-}$, $\forall\, m \in \{m_r - \left\lfloor \frac{w-2}{2} \right\rfloor, \cdots, m_r + \left\lceil \frac{w-2}{2} \right\rceil\}$. Bob sends all feasible index values $l_{B,x} = \{m_r\}$ to Alice through a public channel.

After Alice receives the index set $l_{B,x}$ from Bob, Alice creates the key bits according to threshold values $q_{A,+}$, $q_{A,-}$,

$$\kappa_{A_m} = \begin{cases} 1 & \Omega_A(m) \geq q_{A,+} \\ 0 & \Omega_A(m) < q_{A,-} \end{cases}, m \in l_{B,x} \quad (8)$$

In a similar manner, Bob generates the key bits vector $\{\kappa_{B_m}\}$. As a result of channel reciprocity, the key bits vectors $\{\kappa_{A_m}\}$ and $\{\kappa_{B_m}\}$ generated using the aforementioned steps should be similar. If there is any differences between $\{\kappa_{A_m}\}$ and $\{\kappa_{B_m}\}$, key reconciliation can eliminate discrepancies between $\{\kappa_{A_m}\}$ and $\{\kappa_{B_m}\}$. Even if Eve intercepts the channel, she is incapable of creating the identical secret key because the channel coefficients $H_{A,E}$ and $H_{B,E}$ are uncorrelated with $H_{A,B}$ and $H_{B,A}$ when Eve is positioned half a wavelength away from Alice and Bob.

IV. Analysis of BDR and Key Length

The selection of parameters w, α, and β involves a fundamental trade-off between BDR and key length. In this section, we will demonstrate how BDR and key length can be calculated as functions of α and β. BDR represents the probability that a single bit generated by Alice and Bob will be different at each end. Let us consider the scenario where Alice generates the bit '1' at a specific index, and we want to determine the likelihood that Bob will generate the bit '0' at that same index. Assuming that the amplitude of CSI adheres to a Rayleigh distribution, we can express BDR as:

$$BDR(\alpha,\beta) = P(B=0|A=1) = \frac{P(B=0,A=1)}{P(A=1)} \quad (9)$$

$$P(B=0,A=1) = \underbrace{\int_{q_{A,+}}^{1}\int_{0}^{q_{B,-}}\cdots\int_{q_{A,+}}^{1}}_{L\ terms} f(\boldsymbol{u})du_1\cdots du_L \quad (10)$$

where, $L = (2w-1)$, $f(\boldsymbol{u})$ is multivariate Rayleigh probability density function derived from correlated Gaussian random variables [22]. $f(\boldsymbol{u})$ can be written as,

$$f(\boldsymbol{u}) = \frac{\prod_{i=1}^{L} u_i}{(2\pi)^L(\det(\boldsymbol{K}))^{\frac{1}{2}}}\int_{-\pi}^{\pi}\cdots\int_{-\pi}^{\pi}\exp(-g(\boldsymbol{u},\boldsymbol{\phi})d\phi_1\cdots d\phi_L \quad (12)$$

where, $\boldsymbol{u} = [u_1\, u_2 \cdots u_L]^T$, $\boldsymbol{\phi} = [\phi_1\, \phi_2 \cdots \phi_L]^T$,

$$g(\boldsymbol{u},\boldsymbol{\phi}) = \sum_{i=1}^{L}\sum_{j=1}^{L}[\boldsymbol{E}_{i,j}\cos(\phi_i)\cos(\phi_j) + \boldsymbol{D}_{i,j}\sin(\phi_i)\sin(\phi_j) + 2\boldsymbol{C}_{i,j}\cos(\phi_i)\sin(\phi_j)]u_iu_j \quad (13)$$

In (12), $\boldsymbol{K}$ is $2L \times 2L$ covariance matrix, derived from correlated Gaussian vector [22], matrices $\boldsymbol{E}$, $\boldsymbol{D}$ and $\boldsymbol{C}$ are sub-matrices of $\boldsymbol{K}^{-1}$. $\boldsymbol{K}$ and $\boldsymbol{K}^{-1}$ can be respectively written as [22],

$$\mathbf{K} = \begin{bmatrix} \boldsymbol{K_{cc}} & \boldsymbol{K_{cs}} \\ \boldsymbol{K_{cs}^T} & \boldsymbol{K_{ss}} \end{bmatrix} \quad (14a)$$

$$\boldsymbol{K}^{-1} = \begin{bmatrix} \boldsymbol{E} & \boldsymbol{C} \\ \boldsymbol{C}^T & \boldsymbol{D} \end{bmatrix} \quad (14b)$$

In (9), $P(A=1)$ can be written as,

$$P(A=1) = \underbrace{\int_{q_{A,+}}^{1}\int_{q_{A,+}}^{1}\cdots\int_{q_{A,+}}^{1}}_{(w)\ terms} f(\boldsymbol{v})dv_1\cdots dv_w \quad (15)$$

where, $\boldsymbol{v} = [v_1\, v_2 \cdots v_w]^T$ is a Rayleigh vector consisting of w CSI amplitude of Alice, denoted as $[\gamma_{A,B}(1), \cdots, \gamma_{A,B}(2), \cdots \gamma_{A,B}(w)]^T$. $\boldsymbol{u} = [u_1\, u_2 \cdots u_L]^T$ is a Rayleigh vector consisting of w CSI amplitude of Alice and $w-1$ CSI amplitude of Bob in chronological order, denoted as $[\gamma_{A,B}(1), \gamma_{B,A}(1), \gamma_{A,B}(2), \cdots, \gamma_{B,A}(w-1), \gamma_{A,B}(w)]^T$. Similarly, key length can be written as,

$$KL(\alpha,\beta) = \frac{MP}{w}(P(A=1,B=1) + P(A=0,B=0)) \quad (16)$$

where,

$$P(A=1,B=1) = \underbrace{\int_{q_{A,+}}^{1}\int_{q_{B,+}}^{1}\cdots\int_{q_{A,+}}^{1}}_{L\ terms} f(\boldsymbol{u})du_1\cdots du_L \quad (17)$$

$$P(A=0,B=0) = \underbrace{\int_{0}^{q_{A,-}}\int_{0}^{q_{B,-}}\cdots\int_{0}^{q_{A,-}}}_{L\ terms} f(\boldsymbol{u})du_1\cdots du_L \quad (18)$$

Fig. 5 and Fig. 6 compare the theoretical and simulated BDR and key length for TDL-B and TDL-C channels, as a function of the channel correlation coefficient. To obtain these results, we utilized our wireless local area network (WLAN) 11ac simulation platform to generate 5000 CSI packets for each time interval in the set of [7 ms, 8 ms, 10 ms, 11.5 ms] and [7 ms, 8 ms, 10 ms, 11.5 ms, 11.75 ms] for TDL-B and TDL-C channels, respectively. We set w to 2, G to 5, the carrier frequency to 5.2 GHz, SNR to 20 dB, and moving speed to 3

km/hr, resulting in a corresponding Doppler frequency of 14.45 Hz. After subcarrier selection, each CSI packet consists of 12 subcarriers. We then computed $\boldsymbol{K}$ using the generated CSI dataset and calculated the theoretical BDR and key length using equations (9) and (16), respectively. Utilizing the same 5000 CSI packets, we also extract key bits using our proposed scheme, shown in Fig. 3, we compare the key bits obtained by Alice and Bob, and record the simulated BDR and key length results. As shown in Fig. 5 and Fig. 6, the simulated BDR and key length close to the theoretical BDR and key length.

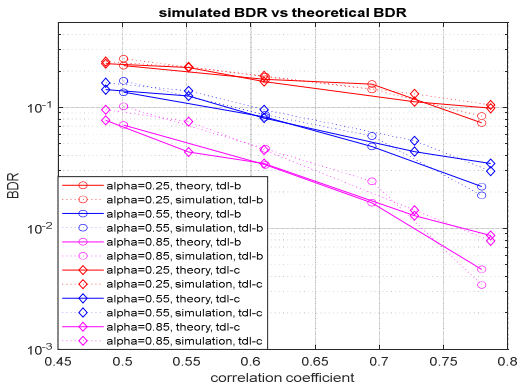

Fig. 5. Theoretical and simulated BDR vs correlation coefficient in TDL-B and TDL-C channels

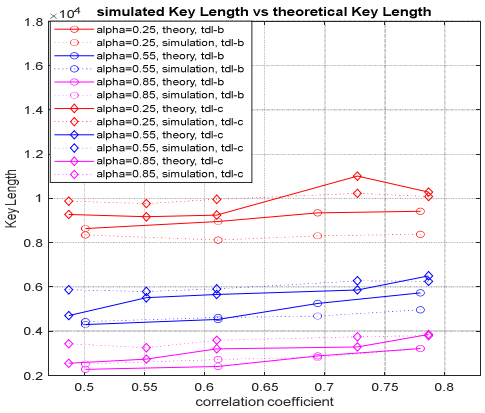

Fig. 6. Theoretical and simulated key length vs correlation coefficient in TDL-B and TDL-C channels

V. PARAMETER OPTIMIZAITON OF QUANTIZATION SYSTEM

A. *Mathematic model of parameter optimizaiton*

In this section we present a mathematical model for optimizing the parameters α and β. Assuming the key reconciliation scheme chosen can correct up to t errors within a Q-bit information block, then BDR requirement is $\varepsilon \le \frac{t}{Q}$. Given that both the BDR and key length are dependent on α and β, our objective is to maximize the key length $KL(\alpha,\beta)$ while ensuring that the $BDR(\alpha,\beta)$ requirement is satisfied. This can be expressed as:

$$\begin{aligned} &min \quad -KL(\alpha,\beta) \\ &s.t. -BDR(\alpha,\beta) - \varepsilon \ge 0 \end{aligned} \tag{19}$$

Introducing a variable z, the above problem can be written as,

$$\begin{aligned} &min \quad -KL(\alpha,\beta) \\ &s.t. -BDR(\alpha,\beta) - \varepsilon - z^2 = 0 \end{aligned} \tag{20}$$

Define the following Lagrange function,

$$\begin{aligned} L(\alpha,\beta,z,\lambda,\sigma) = &-KL(\alpha,\beta) - \lambda \cdot (BDR(\alpha,\beta) - \varepsilon - z^2) \\ &+\frac{\sigma}{2}(BDR(\alpha,\beta) - \varepsilon - z^2)^2 \end{aligned} \tag{21}$$

Using mathematical manipulation, problem (21) can be converted into,

$$\begin{aligned} L(\alpha,\beta,\lambda,\sigma) = &-KL(\alpha,\beta) \\ &+\frac{1}{2\sigma}\{[\max(0,\lambda - \sigma(-BDR(\alpha,\beta) - \varepsilon))]^2 - \lambda^2\} \end{aligned} \tag{22}$$

Problem (22) is an unconstrained optimization problem. Let $\nabla_\alpha L(\alpha,\beta,\lambda,\sigma) = 0$, $\nabla_\beta L(\alpha,\beta,\lambda,\sigma) = 0$, optimal value of α and β can be iteratively obtained.

B. *Guideline for setting α and β*

While solving problem (22) can help us find the optimal values of α and β, it should be noted that solving (22) is not trivial. To assist in setting the values of α and β, we have proposed a guideline as follows:

1) During the channel probing stage, Alice and Bob keep the time interval Δt less than the coherence time and adjust the transmission power to ensure that SNR is large enough so that the channel correlation coefficient between Alice and Bob is larger than 0.5.

2) Assuming the key reconciliation scheme chosen can correct up to t errors within a Q-bit information block, the BDR requirement is $\varepsilon \le t/Q$. Assume that channel coefficient is 0.75 and $w = 2$, if BDR requirement ε is around 4e-2, we shall choose larger α (i.e., α =0.55); if BDR requirement ε is around 1e-1, then can choose smaller α (i.e., α =0.25);

3) Initial value of β can set to 1, then use iterative algorithm to tune β so that in the generated key bits the number of zeros and ones are balanced.

C. *Iterative tuning of parameter β*

The value of α affects both the number of zeros and ones, while the value of β only affects the number of zeros. If the resulting key bit sequence is unbalanced with respect to the number of zeros and ones, it can affect the randomness performance. To address this issue, we propose using an iterative algorithm to tune the parameter β. Fig. 7 illustrates the diagram of the iterative algorithm for tuning β. Initially we set $\beta = 1$, and after generating the key bit sequence $\{\kappa_{A_m}\}$, Alice checks the number of zeros and number of ones in the key bit sequence, denoted as N_0 and N_1, respectively. The unbalance ratio ρ_u is defined as $\rho_u = (N_0 - N_1)/N_1$. If $|\rho_u| > 0.1$, it indicates that the number of zeros and ones is not balanced, and we need to tune the parameter β. The parameter β can be automatically tuned as,

$$\beta \leftarrow \beta\,(1 + \rho_u) \quad if |\rho_u| > 0.1 \tag{23}$$

By tuning the parameter β according to (23), we can balance the number of zeros and ones in the generated key sequence, thereby improving the randomness performance. Fig. 8 displays the relationship between the unbalance ratio and the iteration number as a result of tuning parameter β (the channel

used in simulation is TDL-C channel). The plot demonstrates that, after two round of β tuning, the resulting unbalance ratio falls within the range of ±0.05.

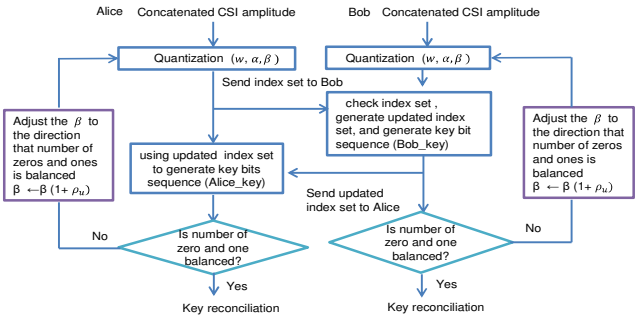

Fig. 7. Iterative tuning of parameter β

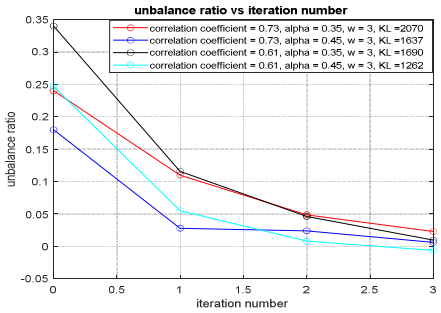

Fig. 8. Unbalance ratio vs iteration number as result of tuning parameter β

VI. CONCLUSION

In this paper, we have proposed a scheme which generates shared secret keys from the amplitude of frequency domain CSI of OFDM signal. A unique quantization scheme is proposed, with the use of two parameters, α and β, to set the quantization threshold. We analyze the BDR and key length in theory. The theoretical analysis of the BDR and key length aligns with the simulation results. We also present a mathematical model to optimize the parameters of our proposed quantization scheme and a guideline to set α and β. Our proposed method for iterative tuning of β can balance the number of zeros and ones in the generated key sequences so that the randomness requirement is met.

ACKNOWLEDGMENT

The research is supported by National Research Foundation, Singapore, jointly with Energy Market Authority and Keppel Offshore & Marine Limited under the Energy Programme "EMA-KOM Joint RFP (EMA-EP007-EKOM)" with Envision Digital International Pte. Ltd. as main Host Institution.

REFERENCES

[1] C. T. Zenger, J. Zimmer, and C. Paar, "Security analysis of quantization schemes for channel-based key extraction", in Workshop Wireless Commun. Security at the Physical Layer, Coimbra, Portugal, Jul. 2015.

[2] R. Guillaume, A. Mueller, C. T. Zenger, C. Paar, and A. Czylwik, "Fair comparison and evaluation of quantization schemes for PHY-based key generation", in Proc. 18th Int. OFDM Workshop (InOWo'14), pp. 1–5, Aug. 2014.

[3] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radiotelepathy: Extracting a secret key from an unauthenticated wireless channel," in Proc. 14th Annu. Int. Conf. Mobile Computing and Networking (MobiCom), pp. 128–139, Sep. 2008.

[4] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments," in Proc. 15th Annu. Int. Conf. Mobile Computing and Networking (MobiCom), pp. 321–332, Sep. 2009.

[5] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," IEEE Trans. Mobile Comput., vol. 9, no. 1, pp. 17–30, 2010.

[6] S Primak, K Liu, and X Wang, "Secret key generation using physical channels with imperfect CSI", 2014 IEEE 80th Vehicular Technology Conference (VTC2014-Fall), Sep 2014.

[7] N. Patwari, J. Croft, S. Jana, and S. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements", IEEE Transactions on Mobile Computing, vol. 9, no. 1, pp. 17–30, Jan 2010.

[8] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks", in Proc. of the 14th ACM Conference on Computer and Communications Security, CCS '07, (New York, NY, USA), pp.401– 410, Oct. 2007.

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

[10] Junqing Zhang, Trung Q. Duong, Alan Marshall, and Roger Woods, "Key generation from wireless channels: A review", IEEE Access, vol 4, Jan. 2016.

[11] S. Sun, Y. Wu, B. S. Lim, and H. D. Nguyen, "A high bit-rate shared key generator with time-frequency features of wireless channels", in Proc. IEEE Globecom, Dec. 2017.

[12] M. A. Tope, and J. C. McEachen, "Unconditionally secure communications over fading channels", in Military Communications Conference (MILCOM) 2001, Oct. 2001.

[13] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels", IEEE Transactions on Antennas and Propagation, vol. 53, No. 11, pp. 3776–3784, Nov. 2005.

[14] H. Liu, Y. Wang, J. Yang, and Y. Chen, "Fast and practical secret key extraction by exploiting channel response", in Proc. IEEE 2013 Infocom, Apr. 2013.

[15] S. Ribouh, K. Phan, A. V. Malawade, Y. Elhillali, A. Rivenq, and M. A. A. Faruque, "Channel state information-based cryptographic key generation for intelligent transportation systems", IEEE Transactions on Intelligent Transport Systems, vol. 22, no. 12, pp. 7496-7507, Dec. 2021.

[16] X. Wu, Y. Peng, C. Hu, H. Zhao, and L. Shu, "A secret key generation method based on CSI in OFDM-FDD system", in Proc. IEEE Globecom Workshops (GC Workshps), pp. 1297–1302, Dec. 2013.

[17] K. Zeng, D. Wu, A. Chan, P. Mohapatra, "Exploiting multiple-antenna diversity for shared secret key generation in wireless networks", in Proc. IEEE Infocom 2010, Mar. 2010.

[18] 3GPP TR 38.901 (Version 14.3.0, Release 14), "Study on channel model for frequencies from 0.5 to 100 GHz", 2018.

[19] T. Pollet, P. Spruyt and M. Moeneclaey, "The BER performance of OFDM systems using non-synchronized sampling", in Proc. IEEE Globecom 94, vol.1, Nov. 28-Dec. 2.

[20] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Efficient key generation by exploiting randomness From channel responses of Individual OFDM Subcarriers", IEEE Transactions on Comm., Vol. 64, No. 6, pp. 2578- 2588, Jun. 2016.

[21] G. L. Stüber, "Principles of mobile communication", Springer, Second Edition, Jan. 2000.

[22] R. K. Mallik, On multivariate Rayleigh and exponential distributions, IEEE Trans. on Information Theory, Vol. 49, No.6, pp.1499-1515, June 2003.