Quantization for Physical Layer Security

Oana Graur, Nazia Islam, and Werner Henkel
Jacobs University Bremen
Electrical Engineering and Computer Science
Bremen, Germany
Emails: {o.graur, n.islam}@jacobs-university.de, werner.henkel@ieee.org

***Abstract*—We propose a multi-level CSI quantization and key reconciliation scheme for physical layer security. The noisy wireless channel estimates obtained by the users first run through a transformation, prior to the quantization step. This enables the definition of guard bands around the quantization boundaries, tailored for a specific efficiency and not compromising the uniformity required at the output of the quantizer. Our construction results in an better key disagreement and initial key generation rate trade-off when compared to other level-crossing quantization methods.**

I. Introduction and Motivation

Due to the inherently random nature of the broadcast wireless channel, extensive research efforts have been directed, over the last decade, towards the generation of encryption keys at the physical layer. As opposed to cryptographic security that relies on limited computational resources of potential eavesdroppers, as well as a key exchange mechanism, physical layer security aims at providing users sharing a wireless channel with symmetric keys that can be used for encryption/decryption, without relying on a preexistent key distribution infrastructure. The original principle dates back to the one-time pad, described by Vernam [1] in 1926, where a plaintext is encrypted with a previously known secret key through modular addition. If the key is truly random and as long as the plaintext message, an eavesdropper without access to the key cannot decrypt the message. Shannon, later on, formulated this finding in information-theoretic terms [2], i.e., the availability of the ciphertext at the eavesdropper does not provide any aid in guessing the plaintext message if the entropy of the key is larger or equal to the entropy of the message. Although this finding has been widely known, the key distribution, along with the requirement of the large key length, constituted the practical limitations for which much of the research focus has shifted towards classic cryptographic schemes over the last century. The interest in information-theoretic security has risen again, along with the advancements in ad-hoc networks, such as wireless sensor networks (WSN), and Internet of Things (IoT), where the assumption of a key distribution infrastructure, on which computational security relies, is unfeasible. A thorough survey on recent physical layer key generation advancements can be found in [3].

Our contribution in this paper focuses on the quantization and reconciliation of correlated channel estimates obtained by two users. Unlike other works [4], [5], we use the complex channel state information (CSI) for key generation, and quantize the real and imaginary parts jointly. In obtaining the complex CSI, a parasitic antenna array is used at one of the users, in order to generate artificial fading and to ensure a high degree of channel randomness, even in line-of-sight (LOS) or static environments. We also propose a transformation that maps the complex channel estimates to the unit square, prior to a vector quantization step, whose purpose is multifold. First, the transformation we propose facilitates the use of well-known, low-complexity vector quantizers, such as Linde-Buzo-Grey (LBG) [6], by providing a uniformly distributed quantizer output, even for higher level quantization. Second, we show how such a transformation enables the straightforward construction of guard bands around the quantization boundaries, without sacrificing the uniformity of the quantizer output. Such guard bands are introduced as a key reconciliation method, with the purpose of excluding the measurement samples most likely to be erroneous due to independent noise on both sides or circuitry imperfections. Our findings show that in the case of a very strong correlation between the legitimate user measurements, for a fixed key generation rate, a higher level quantization with wider guard bands is preferred to lower level quantization with narrow guard bands. Section IV show the performance improvement of our scheme to previous methods described in literature.

A. Requirements for Physical Layer Key Generation

Three main requirements need to be fulfilled for physical layer key generation, channel reciprocity, randomness, and spatial decorrelation.

If we denote by h_{AB} the forward channel from Alice to Bob, and by h_{BA} the reverse channel from Bob to Alice, as shown in Fig. 1, the *channel reciprocity* principle implies $h_{AB} = h_{BA} = c$. This is true to some extent for TDD systems, such as 802.11, WiMAX, LTE, etc.. As long as the coherence time of the channel is larger than the measurement time, the two users, Alice and Bob, can send previously known pilot signals in consecutive time slots in order to obtain their vectors of channel estimates, $\hat{\mathbf{a}} = \mathbf{c} + \mathbf{n_a}$, $\hat{\mathbf{b}} = \mathbf{c} + \mathbf{n_b}$, where $\hat{\mathbf{a}}$ and $\hat{\mathbf{b}}$ denote the estimate vectors at Alice, and Bob, respectively. $\mathbf{n_a}$, and $\mathbf{n_b}$ represent the independent noise vectors affecting the user estimates, arising from different transceiver circuitry, and possible variations of the channel during the non-simultaneous measurement slots. Although they are correlated, a straightforward quantization of the measurement vectors will likely result in key mismatch between the users, and an additional step of key reconciliation needs to be performed.

The channel measurements can represent either channel state information (CSI), or received signal strength information (RSSI). The CSI measurements can refer to either the channel impulse response or frequency response, containing both amplitude and phase information. RSSI, in contrast, refers to an average of the received power for the whole packet and can be seen as more coarse-grained, compared to the instantaneous CSI values. Although CSI-based key generation has been shown to significantly outperform RSSI-based key generation [7], RSSI data has been used in most of the previously proposed key generation schemes based on its availability from most off-the-shelf WiFi cards.

Spatial decorrelation. If a passive eavesdropper, Eve, is located a few wavelengths away from any of the legitimate users, the channel samples estimated by Eve, $\hat{\mathbf{e}}$, will exhibit a low correlation to the forward and reverse channel samples estimated by Alice and Bob. Hence, most of the randomly generated key bits will be secure with respect to Eve. In order to support this claim, we refer the readers to the work in [8]–[10], where theoretical and experimental approaches have been taken in deriving the amount of key information that leaks to the eavesdropper, depending on its separation distance. Even a small amount of information leaked is of serious concern and is highly dependent on Eve's position and relative distance to the legitimate users, thus further processing methods such as advantage distillation and privacy amplification [11], [12], are required. An initial key $\mathbf{K}^N$ of length N, obtained by Alice and Bob, is reduced to a shorter key of length R, i.e., $\mathbf{K}^R$, through the use of a hash function g, known by all parties, such that the leakage $H(\mathbf{K}^R|\hat{\mathbf{e}}, g)$ is diminished. In here, we hence ignore the effect of a passive Eve, by assuming sufficient eavesdropper separation, as well as privacy amplification after the quantization step. We are also not concerned here with the possibility of active jamming attacks.

Randomness. A large degree of randomness ensures the existence of a large key pool after quantization, making it more computationally prohibitive for the eavesdropper to resort to brute-force attacks. If the reciprocal wireless channel does not exhibit a high degree of fading, artificial fading can be induced through the use of parasitic antenna arrays, as we discuss in Section II-A. It should be noted that the uncertainty at the eavesdropper is maximum when the key is uniformly distributed over its alphabet.

For comparing different approaches, we follow the framework of [13], with the following metrics.

1) Correlation Coefficient: We use the Pearson correlation coefficient, $0 \leq \rho \leq 1$, as a measure of the degree of reciprocity of two sequences, $\hat{\mathbf{a}} = [\hat{a}_1 \cdots \hat{a}_N]^T$ and $\hat{\mathbf{b}} = [\hat{b}_1 \cdots \hat{b}_N]^T$.

2) Key Disagreement Rate (KDR): The key disagreement rate is defined as the average ratio between the key symbols found in disagreement between Alice and Bob to the overall number of symbols. We shall distinguish accordingly between symbol and bit disagreement rate in subsequent sections.

3) Initial Key Generation Rate (IKGR): We define the symbol IKGR as the average of the ratio between the number of symbols used for key generation after quantization to the total number of symbols fed to the quantizer. For multilevel quantizations, i.e., $N_q \geq 2$, the bit IKGR is obtained by multiplying the symbol IKGR with the number of bits per symbol.

II. System Description

A. RECAP Antennas for Channel Randomization

The wireless channel between the users does not only include the propagation channel, but also the radiation characteristics of the transmit/receive antennas. The channel can be seen as time-varying if the propagation channel is multipath rich and one of the nodes is moving. However, in the case of a line-of-sight (LOS) channel, reconfigurable aperture antenna arrays (RECAPs) can be used. A RECAP antenna consists of reconfigurable elements (REs), confined to a physical aperture [8], [14]. Each RE can be in a number of states, e.g., by varying capacitive loads.

B. System Model

Figure 1 depicts the system model. We consider one of the legitimate users, e.g., Alice, to be equipped with a RECAP antenna with 24 parasitic reconfigurable elements (REs), and one feed element, shown in orange. Bob and Eve are each equipped with a single dipole antenna. The perceived channel distribution, as seen by the users, when a RECAP antenna is used, depends on the number of REs that are active, as well as on the number of states.

Although using RECAP antennas for creating artificial fading does not always lead to a normal channel distribution, when the number of reconfigurable elements of the array is large, the number of states is large, and the reflection coefficient is controlled, as discussed in [15], the distribution is very close to a complex Gaussian, with the real and imaginary parts i.i.d.. The channel distributions obtained for the RECAP configurations in Fig. 2, are shown subsequently, in Fig. 3. For the rest of this work, we assume the channel to follow a normalized complex Gaussian distribution, with the real and imaginary parts i.i.d., as obtained for the $N_{RE} = 24$ RECAP configuration. Additional details on how the channel measurements used in this work were obtained, along with a study on the number of secure bits as a function of multipath and eavesdropper antenna separation, can be found in [16], [17].

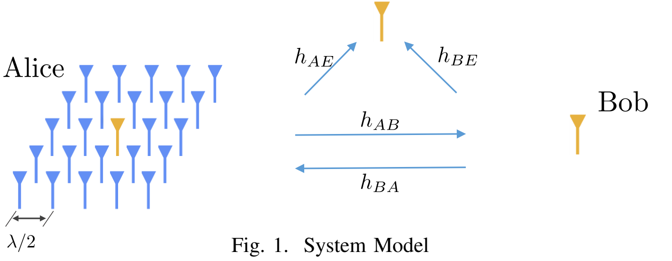

Fig. 1. System Model

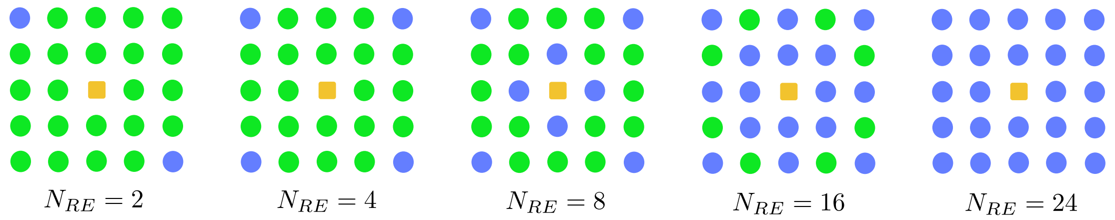

Fig. 2. RECAP configurations; 2, 4, 8, 16, 24 active reconfigurable elements (REs); feed element in orange, active REs in blue, inactive REs in green

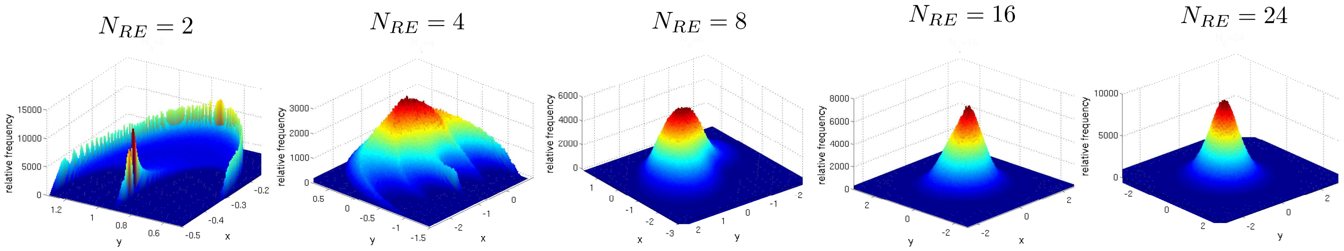

Fig. 3. Complex channel pdfs given different RECAP configurations; 2, 4, 8, 16, 24 active reconfigurable elements (REs)

The first step in the key generation and reconciliation process is the channel probing phase, in which both Alice and Bob obtain their length N vectors of complex CSI estimates, namely $\hat{\mathbf{a}}$ and $\hat{\mathbf{b}}$. Note that throughout this paper, bold lowercase notations are used for vectors, while the noisy estimates are indicated by the ˆ symbol.

If $c = x + jy$ denotes a complex channel sample, $\hat{a} = \hat{x}_A + j\hat{y}_A$ and $\hat{b} = \hat{x}_B + j\hat{y}_B$ represent the noisy estimates of the channel sample c at Alice, and Bob, respectively, with $\hat{x}_A$, $\hat{y}_A$, $\hat{x}_B$, $\hat{y}_B$ denoting the estimates of the real and imaginary components. All notations are summarized in Table I, for convenience.

TABLE I
NOTATIONS

Notation	Description
$\mathbf{c} = \mathbf{x} + j\mathbf{y}$	vector of channel samples (complex)
$\mathbf{x} = [x_1 \cdots x_N]^T$	vector of channel samples (real part)
$\mathbf{y} = [y_1 \cdots y_N]^T$	vector of channel samples (imaginary part)
$\hat{\mathbf{a}} = \hat{\mathbf{x}}_\mathbf{A} + j\hat{\mathbf{y}}_\mathbf{A}$	vector of complex channel estimates at Alice, $\hat{\mathbf{a}} = [\hat{a}_1 \cdots \hat{a}_N]^T$
$\hat{\mathbf{b}} = \hat{\mathbf{x}}_\mathbf{B} + j\hat{\mathbf{y}}_\mathbf{B}$	vector of complex channel estimates at Bob, $\hat{\mathbf{b}} = [\hat{b}_1 \cdots \hat{b}_N]^T$
$\hat{\mathbf{x}}_\mathbf{A} = \mathbf{x} + \mathbf{n}_\mathbf{xa}$	measurement estimates of $\mathbf{x}$ at Alice
$\hat{\mathbf{y}}_\mathbf{A} = \mathbf{y} + \mathbf{n}_\mathbf{ya}$	measurement estimates of $\mathbf{y}$ at Alice
$\hat{\mathbf{x}}_\mathbf{B} = \mathbf{x} + \mathbf{n}_\mathbf{xb}$	measurement estimates of $\mathbf{x}$ at Bob
$\hat{\mathbf{y}}_\mathbf{B} = \mathbf{y} + \mathbf{n}_\mathbf{yb}$	measurement estimates of $\mathbf{y}$ at Bob
$\hat{\mathbf{u}}_\mathbf{a} = \hat{\mathbf{u}}_{xa} + j\hat{\mathbf{u}}_{ya}$	transformed vector $\hat{\mathbf{a}}$ (uniform domain)
$\hat{\mathbf{u}}_\mathbf{b} = \hat{\mathbf{u}}_{xb} + j\hat{\mathbf{u}}_{yb}$	transformed vector $\hat{\mathbf{b}}$ (uniform domain)
σ^2	variance of $\mathbf{x}$, $\mathbf{y}$ (channel variance)
$\sigma^2_{n_a}$	noise variance at Alice
$\sigma^2_{n_b}$	noise variance at Bob
$\sigma^2_a = \sigma^2 + \sigma^2_{n_a}$	variance of $\mathbf{a}$ (at Alice)
$\sigma^2_b = \sigma^2 + \sigma^2_{n_b}$	variance of $\mathbf{b}$ (at Bob)
N_q	number of quantization regions
$\mathcal{R}_i$	ith quantization region
$(\hat{u}_{xa}, \hat{u}_{ya})$	real and imaginary components of Alice's sample $\hat{a}$ after transformation
$(\hat{u}_{xb}, \hat{u}_{yb})$	real and imaginary components of Bob's sample $\hat{b}$ after transformation to uniform domain
(n_{ux}, n_{uy})	random variables describing the real and imaginary noise components, respectively, affecting a complex sample $c = x + jy$, after transformation to uniform domain

C. Uniform Transformation

Having obtained their sequences of analog complex channel estimates, both Alice and Bob first apply a transformation of the data, before quantizing, as follows:

$$\hat{u}_{xa} = \frac{1}{2}\text{erfc}\left(-\frac{\hat{x}_A}{\sqrt{2(\sigma^2 + \sigma^2_{na})}}\right); \hat{u}_{ya} = \frac{1}{2}\text{erfc}\left(-\frac{\hat{y}_A}{\sqrt{2(\sigma^2 + \sigma^2_{na})}}\right). \tag{1}$$

$\hat{u}_{xa}$ and $\hat{u}_{ya}$ correspond to the real and imaginary components of sample $\hat{a}$ after the transformation, at Alice, likewise $\hat{u}_{xb}$ and $\hat{u}_{yb}$ for Bob. Since the estimates $\hat{x}_A$ and $\hat{y}_A$ are each distributed according to a zero-mean Gaussian pdf with variance $\sigma^2_a = \sigma^2 + \sigma^2_{na}$, the transformed samples $\hat{u}_{xa}$ and $\hat{u}_{ya}$ will each follow a uniform distribution in $(0, 1)$. Thus, the vector of complex estimates $\hat{\mathbf{a}}$, in the original domain, will now be mapped into vector $\hat{\mathbf{u}}_a$, uniformly distributed in the unit square, after transformation. We refer to the domain after transformation as the uniform domain. Performing such a transformation of the data before quantization is motivated by the reduced complexity of the vector quantization, as well as the computation of the guard band widths.

Our goal now is to find an equal-area partitioning of the unit square into N_q quantization regions, while maintaining a low probability that a channel sample is quantized to different regions by Alice and Bob, due to independent noise effects. The equal-area constraint is required to ensure a uniform distribution of the quantized key symbols.

We first turn our attention to the noise distribution after transformation. Since n_{x_a} and n_{y_a} were normally distributed before transformation with means x and y, and variances $\sigma^2_{nx_a} = \sigma^2_{ny_a} = \sigma^2_{n_a}$, their marginal pdfs after transformation are found to be

$$f(n_{ux}|x) = \frac{\sigma_a}{\sigma_{n_a}} e^{\left(\text{erfc}^{-1}(2n_{ux})\right)^2 - \frac{\left(x + \sigma_a\sqrt{2}\text{erfc}^{-1}(2n_{ux})\right)^2}{2\sigma^2_{n_a}}} \tag{2}$$

The marginal pdf for the imaginary noise component is similar to the one in (2). The noise at Alice, around the point of coordinates (x, y) will have a distribution, after the transformation, which will depend on the (x, y) positions in the original domain. The real and imaginary noise pdfs at Bob are obtained by substituting σ_a with σ_b in (2). Figure 4 shows the marginal pdf of the noise after transformation (real dimension only), from (2), for various positions of (x, y) in the original domain. As (x, y) vary from the inside of the circularly symmetric Gaussian towards the periphery, the marginal noise pdfs after transformation have a narrower variance towards the edges of the unit square.

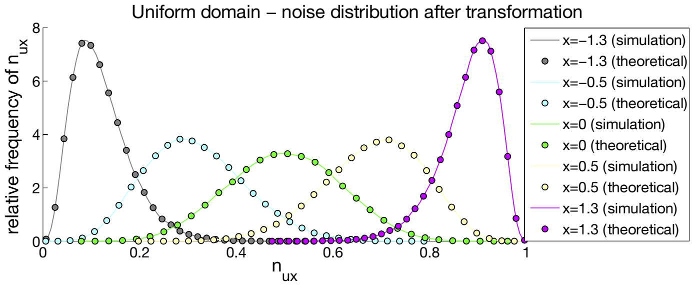

Fig. 4. Marginal PDF of the noise after transformation to uniform domain; real component only. The circular markers correspond to the theoretical curves, as given in (2), while the lines correspond to the pdf estimates from simulations.

After the transformation phase, both Alice and Bob are ready to proceed with the vector quantization. We will first proceed with describing the vector quantization scheme chosen and then describe the computation of the guard bands.

III. Quantization

One of the most widely used vector quantization schemes is the Linde-Buzo-Gray (LBG) algorithm [6]. Its widespread is a consequence of the fact that is has very low implementation complexity and it outperforms other vector quantizers in practical situations. LBG is the discrete version of the Lloyd-Max quantizer, and, unlike Lloyd-Max, it does not require a closed form expression of the input density, but an initial training vector that is iteratively partitioned into N_q clusters.

We show in Fig. 5 the difference in output distribution when we apply the LBG quantization to a circularly symmetric Gaussian input and when we apply it to a uniformly distributed input, as the one obtained after our transformation in (1). With an increase in the number of quantization regions, the uniformity of the output is not preserved when LBG quantization is applied directly to the estimate vectors, without first performing the transformation. Hence, the proposed transformation is important for key generation.

A. Guard Band Construction

The second argument for such a transformation is that once the coordinates of the vertices of the Voronoi cells are obtained, the computation of the guard bands is straightforward. Since the quantization cells are now equal-area polygons tessellating the unit square, we can design guard bands around the quantization boundaries starting from a certain efficiency. We define efficiency $0 \leq \eta \leq 1$ to represent the ratio of points that fall outside the guard bands to the overall number of points. Due to the uniform distribution of the samples after transformation, the efficiency $\eta = \frac{A_{\text{useful}}}{A_{\text{square}}} = 1 - A_{\text{gb}}$, where A_{gb} is the total area of the guard bands. Since we are interested in preserving the uniformity of the output symbols, even after the construction of the guard bands, we require that an area of $\frac{1-\eta}{N_q}$ is assigned to the guard bands within each quantization region. It should be noted, however, that although the quantization regions should have equal areas in the unit square, this does not imply equal widths of the guard bands across the regions. If we let $(\mathbf{v}_x, \mathbf{v}_y)$ denote the vectors holding the real and imaginary coordinates of the vertices of a certain region $\mathcal{R}_i$, the coordinates of the inner polygon representing the useful region of cell $\mathcal{R}_i$ can be computed using the theorem of similar polygons, as follows:

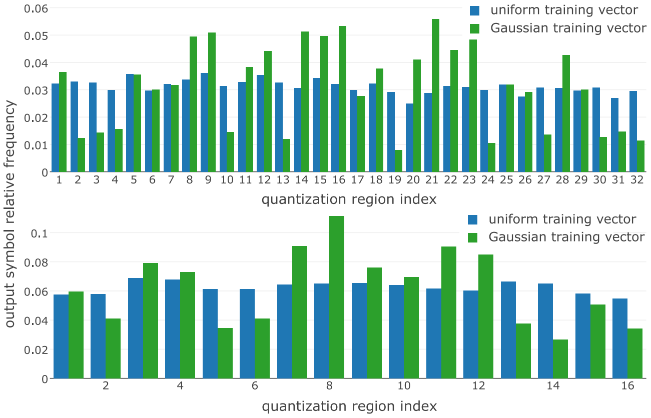

Fig. 5. Output distribution across quantization regions for uniform and normally distributed LBG training sets; (a) $N_q = 32$; (b) $N_q = 16$

$$\begin{aligned}\mathbf{v}_{x_{\text{rescaled}}} &= \sqrt{\eta}(\mathbf{v}_x - \mu_{\mathbf{v}_x}) + \mu_{\mathbf{v}_x} \ , \\ \mathbf{v}_{y_{\text{rescaled}}} &= \sqrt{\eta}(\mathbf{v}_y - \mu_{\mathbf{v}_y}) + \mu_{\mathbf{v}_y} \ , \end{aligned} \tag{3}$$

where $\mu_{\mathbf{v}}$ is the mean of vector $\mathbf{v}$. For illustration purposes, we show in Fig. 6 (a) the LBG quantization regions, along with the corresponding guard bands, for $N_q = 8$, and an efficiency $\eta = 0.8$. Fig. 6 (b) shows the same points that have been quantized in the uniform domain, after being transformed back to the original domain. This is shown to illustrate the fact that an equivalent quantization in the original domain would have non-linear guard bands. Note that our method does not require such an inverse transformation of the points, and both Alice and Bob generate their keys by quantizing their transformed complex vectors $\hat{\mathbf{u}}_a$ and $\hat{\mathbf{u}}_b$, respectively.

The guard band construction is also possible in the original domain, however, more complicated. For the simplest case of the binary quantization, when the data is quantized in the original domain, with the quantization boundary consisting of a straight line going through the origin, the guard bands of width $2r$ around the quantization line are computed by solving

$$1 - \eta = \frac{1}{2\pi(\sigma^2 + \sigma_{na}^2)} \int_{-\infty}^{\infty} \int_{-r}^{r} e^{-\frac{\hat{x}_A^2 + \hat{y}_A^2}{2(\sigma^2 + \sigma_{na}^2)}} d\hat{x}_A d\hat{y}_A \ . \tag{4}$$

However, for a larger number of Voronoi cells, with arbitrary quantization boundaries, (4) becomes much more complex, making even individual numerical solutions for the guard band widths in the original domain practically unfeasible. Note that regardless of the domain chosen, neither the quantization nor the guard band reconciliation should affect the uniformity at the output of the quantizer. Previous quantization and reconciliation schemes have taken different approaches. We briefly describe some of the more relevant previous results, since we will use them as a basis of comparison to our method in Section IV. However, most of the results available in the literature discuss binary quantization schemes and do not take advantage of quantizing the real and imaginary components of the complex channel jointly, as we propose.

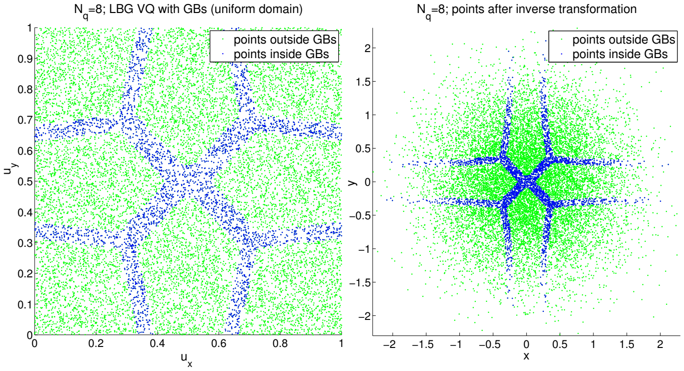

Fig. 6. (a) Linde-Buzo-Gray (LBG) quantization of the uniformly distributed square; points that fall in the guard bands in blue, points outside guard bands in green. This plot was generated for an efficiency $\eta = .8$; (b) equivalent positions in the original domain.

Aono [14] drops RSSI values below a threshold, chosen as the median, and communicates the positions of the discarded samples to the other party. In [18], Tope computes the difference in RSSI values and relies on two thresholds to exclude points that will likely result in a key mismatch. Similarly, in the work of Mathur et al. [5], Alice and Bob check for successive blocks of m samples that fall above or below two thresholds, q_+, and q_-. Jana et al. [4] proposed both a multibit and single bit adaptive secret bit generation (ASBG) algorithm, which is a modification of the work of Mathur [5]. In contrast, the quantizer proposed by Jana, however, divides the measurements into smaller block lengths and calculates the thresholds for each block separately, resulting in a faster adaptation to shifts in the RSSI mean value over time.

Unlike all of the above methods, we start from fine-grained CSI measurements, following a complex circularly symmetric distribution, as explained in Section II-A.

B. Key Disagreement Rates

The symbol mismatch probability[1] $P(\hat{a} \in \mathcal{R}_i | \hat{b} \notin \mathcal{R}_i)$ between Alice and Bob can be computed as follows:

$$P_{\hat{a}\neq\hat{b}} = \sum_{i=1}^{N_q} \sum_{j=1, j\neq i}^{N_q} P(\hat{b} \in \mathcal{R}_j, \hat{a} \in \mathcal{R}_i) \tag{5}$$

$$\begin{aligned} P_{\hat{a}\neq\hat{b}} &= \int_c \sum_{i=1}^{N_q} \sum_{j=1, j\neq i}^{N_q} p(\hat{b} \in \mathcal{R}_j, \hat{a} \in \mathcal{R}_i, c) dc \\ &= \int_c \sum_{i=1}^{N_q} \sum_{j=1, j\neq i}^{N_q} P(\hat{b} \in \mathcal{R}_j, \hat{a} \in \mathcal{R}_i | c) p(c) dc \\ &= \int_c \sum_{i=1}^{N_q} \sum_{j=1, j\neq i}^{N_q} P(\hat{b} \in \mathcal{R}_j | c) P(\hat{a} \in \mathcal{R}_i | c) p(c) dc \end{aligned}$$

For the simplest case, with two quantization regions, with the quantization boundary at $x = 0$, the bit mismatch probability, or bit disagreement rate (BDR), is derived in (6)-(9), where $\mathcal{R}_1$ is from $(-\infty, 0)$, $\mathcal{R}_2$ is from $(0, \infty)$, and $\mathcal{R} = \mathcal{R}_1 \cup \mathcal{R}_2$. Note that $\hat{a}$, $\hat{b}$, and c are all complex variables, so any integration is in real and imaginary dimensions. For binary quantization, $N_q = 2$, due to the symmetry of the quantization, it is sufficient to integrate only the along the real components of the variables, namely $\hat{x}_A$, $\hat{x}_B$, and x, as shown in (9).

$$P_{\hat{a}\neq\hat{b}_{N_2}} = P(\hat{a} \in \mathcal{R}_1, \hat{b} \in \mathcal{R}_2) + P(\hat{a} \in \mathcal{R}_2, \hat{b} \in \mathcal{R}_1) \tag{6}$$

$$P_{\hat{a}\neq\hat{b}_{N_2}} = 2 \int_{c\in\mathcal{R}} P(\hat{a} \in \mathcal{R}_1 | c) P(\hat{b} \in \mathcal{R}_2 | c) p(c) dc \tag{7}$$

$$P_{\hat{a}\neq\hat{b}_{N_2}} = 2 \int_{c\in\mathcal{R}} \int_{\hat{b}\in\mathcal{R}_2} \int_{\hat{a}\in\mathcal{R}_1} p(\hat{a}|c) p(\hat{b}|c) p(c) d\hat{a}\, d\hat{b}\, dc \tag{8}$$

IV. Results

For a fair evaluation of the quantization and reconciliation performances, we show simulation results for the bit disagreement rate (BDR) versus the correlation coefficient. We provide results for both the binary quantization, $N_q = 2$, as well as multibit quantization, $N_q = 4$ and $N_q = 8$. One interesting aspect is whether any advantage can be achieved by using a higher level quantization, e.g., extracting multiple bits from a single CSI sample, while fixing the initial key generation rate.

In Fig. 7, we show the bit disagreement rates (BDR) versus correlation for various efficiency curves, for two quantization regions, and the same BDR plotted against the SNR in Fig. 8. For binary quantization we investigate three scenarios: Method 1 quantizes the user estimates with a line through the middle of the original domain, i.e., no transformation is applied. Method 2 splits the original domain into two equally probable regions by using a circle of appropriate radius. Method 3 transforms the user estimates to the unit square, before quantizing[2] with a line at $u_x = 0.5$. A maximum key generation rate of 1, for the binary quantization case, is achieved for the case when the guard band widths are zero. As confirmed by simulations, for the binary quantization, methods 1 and 3 have, of course, the same performance, and surpass Method 2. For four quantization regions, $N_q = 4$, we have considered four options. Method 1 quantizes the original data by splitting the original domain with four squares intersecting in the origin. Method 2 uses 4 concentric circles to quantize the Gaussian estimates. The radii of the concentric

[1] Note that P denotes a probability, while the lowercase p refers to a probability density function.

[2] This is equivalent to LBG quantization in the uniform domain for $N_q = 2$

$$P_{\hat{a}\neq\hat{b}_{N_q=2}} = \frac{1}{\sqrt{2}\sigma_{n_a}\sigma_{n_b}\sigma}\int_{-\infty}^{\infty}\int_{-\infty}^{0}\int_{0}^{\infty} e^{-\frac{(\hat{x}_A-x)^2}{2\sigma_{n_a}^2}}\, e^{-\frac{(\hat{x}_B-x)^2}{2\sigma_{n_b}^2}}\, e^{-\frac{x^2}{2\sigma^2}}\, d\hat{x}_A d\hat{x}_B dx \quad (9)$$

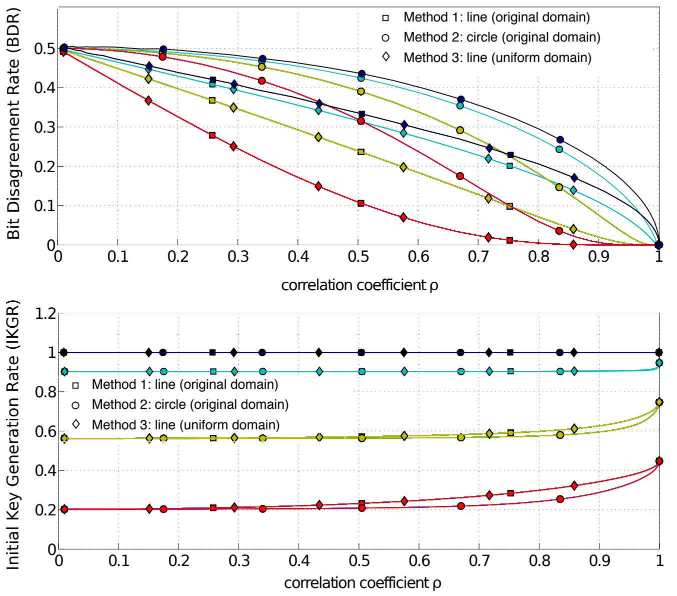

Fig. 7. Bit disagreement rate versus correlation for different initial key generation rates; $N_q = 2$

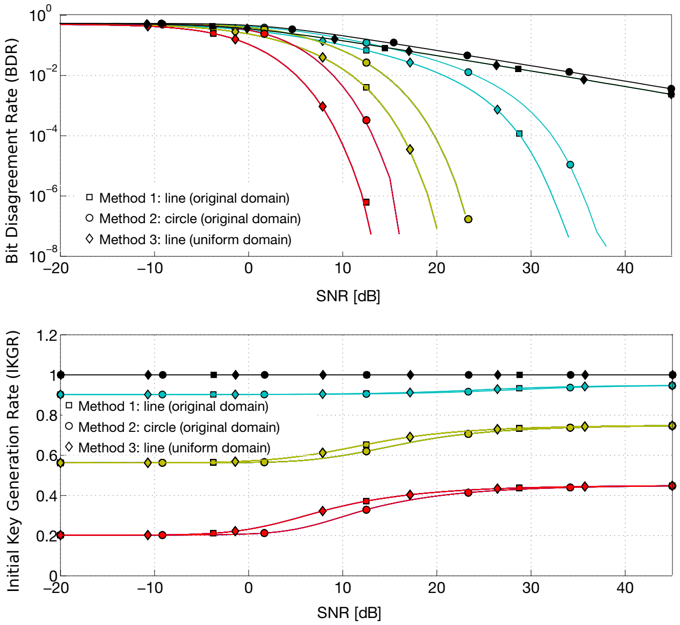

Fig. 8. Bit disagreement rates and the corresponding IKGRs for $N_q = 2$

circles are computed such that the output of the quantization is uniformly distributed. Methods 3 and 4 first transform the data to the uniform domain. Method 3 is similar to Method 1, however, the quantization with four squares is done in the uniform domain, instead of the original one. Method 4 is the LBG quantization in the uniform domain, that we have described in the previous sections. Figure 9 shows the BDR versus the correlation coefficient for different key generation rates. Note that since we now consider 2 bits/symbol, an IKGR of 2 corresponds to an efficiency $\eta = 1$ when no points are discarded, i.e., guard band widths are zero. Our findings show identical performance for the quantization with four squares, whether it is done in the uniform domain, and the Linde-Buzo-Gray quantization case. Again, the concentric quantization shows the worst performance. Figure 10 shows the BDR versus the SNR for $N_q = 4$ for different key generation rates.

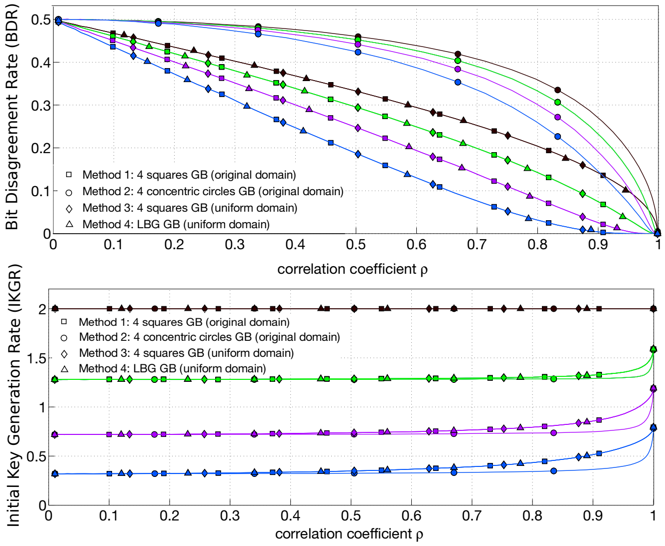

Fig. 9. Bit disagreement rates versus correlation for different initial key generation rates; $N_q = 4$

We illustrate, in Fig. 11, a performance comparison between our work and previous quantization and reconciliation schemes, following the framework discussed in [13]. We compare our LBG results for the case of $N_q = 2$ and $N_q = 3$ with the multibit scheme proposed by Jana [4]. As shown in Fig. 11, with the initial key generation fixed, IKGR=2, our 2-bit LBG quantization shows an improvement over the corresponding 2-bit quantization of Jana, regardless of the value of the correlation coefficient. However, by increasing the number of bits extracted per CSI symbol, i.e., 3 bits/symbol, a performance increase in terms of BDR is achievable only for high correlation values, compared to the case of extracting only 2 bits/symbol. The schemes proposed by Tope and Maurer exhibit a low BDR, however, they also have very low initial key generation rates. Nevertheless, if we fix our IKGR to similar values as shown of the other schemes in Fig. 11, our LBG methd is advantageous is terms of BDR when compared to all the other quantization schemes.

V. Conclusion

Instead of simply applying the quantization to the CSI estimate vectors that Alice and Bob obtain, we first apply a transformation of the data that leads to a uniform distribution. The advantage of performing such a transformation

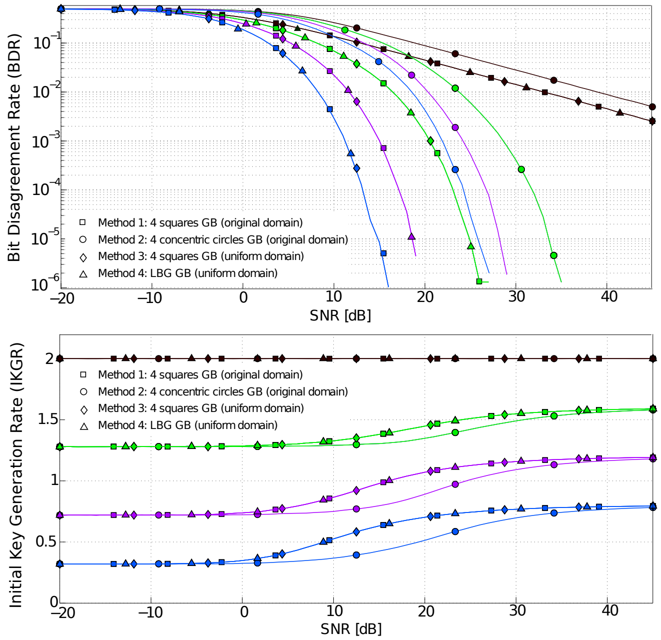

Fig. 10. Bit disagreement rates versus SNR for different initial key generation rates; $N_q = 4$

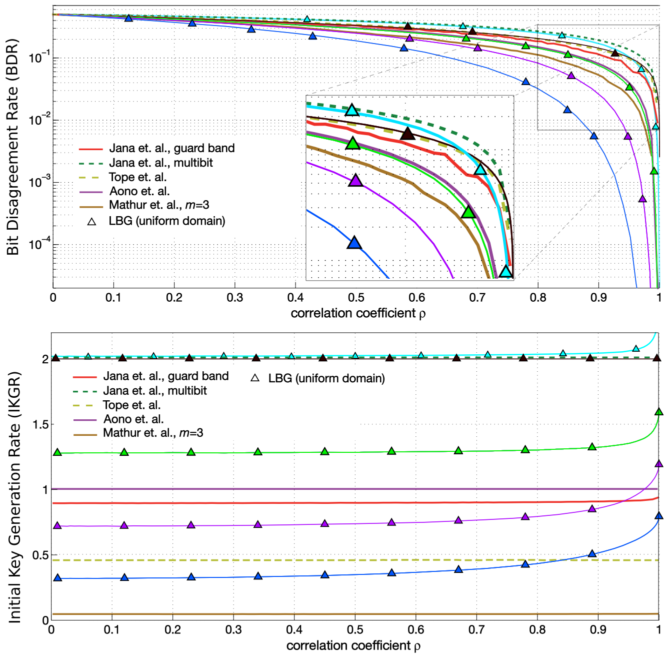

Fig. 11. Bit disagreement Rate (BDR) and Initial Key Generation Rate (IKGR) versus correlation - comparison to previous works

of the complex data, enables us a to use a well known vector quantizer, such as Linde-Buzo-Gray [6], to partition the uniform domain into equal-area regions and to easily construct the guard bands around the quantization boundaries, for a fixed key generation rate. Our proposed method takes advantage of the joint quantization of the real and complex CSI components and discards the samples that are most likely to result in key mismatches, without disturbing the uniformity requirement at the output of the quantizer. Our method shows a better performance in terms of bit disagreement and initial key generation rates compared to other previous quantization and reconciliation schemes currently available, while also benefiting from a low implementation complexity.

References

[1] G. Vernam, "Cipher Printing Telegraph Systems for Secret Wire and Radio Telegraphic Communications," *Journal of the AIEE*, vol. 45, p. 295, 1926.

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

[3] J. Zhang, T. Duong, A. Marshall, and R. Woods, "Key Generation from Wireless Channels: A Review," *IEEE Access*, vol. 4, pp. 1–1, 2016.

[4] S. Jana, S. N. Premnath, M. Clark, S. Kasera, N. Patwari, and S. Krishnamurthy, "On the Effectiveness of Secret Key Extraction from Wireless Signal Strength in Real Environments," in *Mobile Communications (MobiCom09)*, (Beijing), pp. 1–2, 2009.

[5] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-Telepathy: Extracting a Secret Key from an Unauthenticated Wireless Channel," *Proceedings of the 14th ACM international conference on Mobile computing and networking - MobiCom '08*, p. 128, 2008.

[6] Y. Linde, A. Buzo, and R. M. Gray, "An Algorithm for Vector Quantizer Design," *IEEE Transactions on Communications*, vol. 28, pp. 84–95, jan 1980.

[7] Y. Liu, S. C. Draper, and A. M. Sayeed, "Exploiting Channel Diversity in Secret Key Generation from Multipath Fading Randomness," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 5, pp. 1484–1497, 2012.

[8] R. Mehmood and J. W. Wallace, "Experimental Assessment of Secret Key Generation using Parasitic Reconfigurable Aperture Antennas," *Proceedings of 6th European Conference on Antennas and Propagation, EuCAP 2012*, no. 1, pp. 1151–1155, 2012.

[9] R. Mehmood, J. W. Wallace, and M. A. Jensen, "Experimental Characterization of Channel-Based Key Establishment using Reconfigurable Antennas," *8th European Conference on Antennas and Propagation, EuCAP 2014*, no. EuCAP, pp. 447–448, 2014.

[10] A. J. Pierrot, R. a. Chou, and M. R. Bloch, "Experimental Aspects of Secret Key Generation in Indoor Wireless Environments," in *IEEE 14th Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, pp. 669–673, 2013.

[11] U. Maurer and S. Wolf, "Secret-Key Agreement over Unauthenticated Public Channels- Part III: Privacy Amplification," *IEEE Transactions on Information Theory*, vol. 49, pp. 839–851, 2003.

[12] C. H. Bennett, G. Brassard, C. Crkpeau, U. M. Maurer, and S. Member, "Generalized Privacy Amplification," vol. 41, no. 6, pp. 1915–1923, 1995.

[13] R. Guillaume, C. Zenger, A. Mueller, C. Paar, and A. Czylwik, "Fair Comparison and Evaluation of Quantization Schemes for PHY-based Key Generation," *OFDM 2014, 19th International OFDM Workshop 2014 (InOWo'14); Proceedings of*, pp. 1–5, 2014.

[14] 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, pp. 3776–3784, nov 2005.

[15] R. Mehmood and J. W. Wallace, "Wireless Security Enhancement using Parasitic Reconfigurable Aperture Antennas," in *2011 European Antennas Propagation Conference*, (Rome, Italy), pp. 2761–2765, apr 2011.

[16] J. W. Wallace and R. K. Sharma, "Automatic Secret Keys From Reciprocal MIMO Wireless Channels: Measurement and Analysis," *IEEE Transactions on Information Forensics and Security*, vol. 5, pp. 381–392, sep 2010.

[17] R. Mehmood, J. W. Wallace, and M. A. Jensen, "Key Establishment Employing Reconfigurable Antennas: Impact of Antenna Complexity," *IEEE Transactions on Wireless Communications*, vol. 13, pp. 6300–6310, nov 2014.

[18] M. A. Tope and J. C. Mceachen, "Unconditionally Secure Communications over Fading Channels," *Military Communications Conference*, vol. 00, no. c, pp. 54–58, 2001.