Quantization and LLR Computation for Physical Layer Security

Oana Graur, Nazia Islam, Alexandra Filip, and Werner Henkel

Jacobs University Bremen
Electrical Engineering and Computer Science
Bremen, Germany
Emails: o.graur@jacobs-university.de, n.islam@jacobs-university.de, alexandra.filip@dlr.de, w.henkel@jacobs-university.de

***Abstract*—The problem of key reconciliation based on Low-Density Parity-Check (LDPC) codes and Slepian-Wolf coding for physical layer key generation is investigated. When using the channel-state-information (CSI) of a reciprocal wireless channel for key generation between two legitimate users, independent noise components, quantization, and synchronization errors at the end nodes give rise to key differences that need to be corrected by sending side information. We provide a comparison of three different quantization schemes in terms of key disagreement rate and output probability distributions and present the log-likelihood formulations required by a soft decision LDPC decoder to perform key reconciliation, for the investigated quantization methods.**

I. Introduction

While computational security algorithms usually reside in upper protocol layers and rely on the assumption of limited processing capabilities of a potential eavesdropper, physical-layer key generation aims at providing secrecy in the more information-theoretic sense, as introduced by Shannon [1]. Thus, by sharing a previously known secret key, such as a one-time pad, two legitimate users, Alice and Bob, are able to exchange an encrypted message through an unsafe public channel, without leaking any information to a potential eavesdropper, Eve. As long as Alice and Bob share a secret common source of randomness from which they can generate a long uniformly distributed secret key, perfect secrecy is achieved, meaning that Eve has the same chances of guessing the original message with or without the ciphertext, or, in more theoretical terms, the eavesdropper's equivocation is equal to the entropy of the message. It soon became clear that such a common source of randomness could be provided by the fluctuating and reciprocal nature of the wireless medium and that the channel-state information (CSI) can be measured by both Alice and Bob and used to generate one-time pads, thus eliminating the problem of previous key distribution.

Since most wireless transmission standards, such as 802.11, Bluetooth, WiMAX, ZigBee, employ time division duplexing (TDD), probing in consecutive short time slots the forward and the reverse channel provides the possibility of obtaining nearly identical CSI on both sides. Such a method of key generation, solely based on the reciprocity property of wireless TDD systems, besides solving the problem of key distribution, comes with the significant benefit that it does not require the legitimate channel between Alice and Bob to have an SNR advantage over the eavesdropper's channels, such as [8], [9], nor does it assume Alice and Bob to have information about the channels to Eve. However, one important aspect that we address here is that due to independent noise on both ends, different transceiver circuitry, and quantization errors, key mismatches are very likely to occur, leading to the necessity of a key reconciliation scheme.

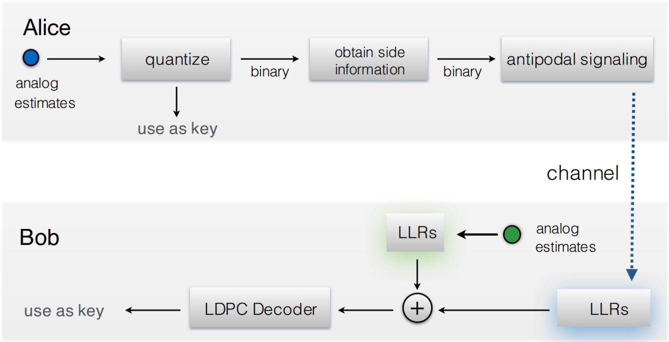

Fig. 1. System model - key reconciliation based on LDPC codes

The current paper is structured as follows: Section II offers an overview of the system model along with channel characterization aspects. In Section III, the impact of codebook sizes and possible quantization schemes is discussed in terms of key disagreement rates for the case when no key reconciliation takes place between the users. An exact formulation of the log-likelihood ratios as required, e.g., by LDPC decoding, is detailed in Section IV, for the quantization schemes analyzed in the previous section.

II. System Description

A point from the channel distribution is measured by both Alice and Bob, disturbed by different noise components. The analog value obtained by Alice, is quantized and assumed to be correct. Employing Slepian-Wolf coding [13], Alice compresses her vector of quantized key symbols and sends Bob additional side information (parity or syndrome bits), as illustrated in Fig. 1. Bob obtains his own vector of channel estimates, along with the side information, possibly corrupted, sent by Alice, and proceeds to computing the log-likelihood ratios required, e.g., for an LDPC decoder, in order to obtain the exact same key Alice generated after her quantization step. Although the reconciliation scheme presented in Fig. 1 shows an implementation with LDPC codes, the log-likelihood ratios presented in Section IV can be utilized by any soft decision non-binary decoder.

For key generation based on the channel-state information (CSI), a few conditions must be ensured. First, the channel has to be *reciprocal*, that is, if we denote by h_B a forward channel sample from Alice to Bob, and by h_A the corresponding reverse channel sample from Bob to Alice, then $h_A = h_B$. However, their estimates of the channel, $\hat{h}_A$ and $\hat{h}_B$, might differ due to independent noise. Reciprocity can be assumed in the case of TDD systems when the channel is quasi-static, i.e., the coherence time of the channel is larger than the measurement time. Thus, the vectors of estimates, $\hat{\mathbf{h}}_A$ and $\hat{\mathbf{h}}_B$ can be obtained during an initial measurement phase by sending pilot signals in consecutive TDD time slots.

A second assumption is that the channel follows a bivariate normal distribution. A Gaussian channel distribution, as shown in [2], [3], minimizes the number of vulnerable bits. If the wireless channel is static or a line-of-sight (LOS) channel, the randomness present is not sufficient such that the central limit theorem holds, leading to a normal distribution of the CSI, which would be ideal for key generation. However, since the wireless channel is also dependent on the radiation patterns of the antennas, random variations in the channel can be induced by using reconfigurable aperture antennas (RECAPs) and changing the capacitive loads at the reconfigurable elements. It has been shown that for a high number of RECAP antenna elements (e.g. 24), and a large number of states as discussed in [2], [7], the channel distribution is very close to a complex Gaussian, with the real and imaginary parts independent and identically distributed. Further details on the the validity of this assumption, RECAP configuration, as well as measurements description can be found in [4], [5]. For the rest of this paper, we will assume a circular symmetric Gaussian channel distribution with zero mean and variance σ^2_{ch}.

A third assumption refers to the antenna separation. Herein, we assume a sufficient separation between Eve and Alice and Bob such that the legitimate and the eavesdropper channels are not correlated. Recent studies [12] have shown that an antenna separation of half a wavelength is not sufficient, and that for the rate of the number of vulnerable key bits to the total number of key bits to go to zero, an eavesdropper separation of several wavelengths is necessary [15].

III. Quantization

In order to study the effects of different quantization methods on the overall key disagreement rate, we first consider the case when no reconciliation is performed, and each legitimate user obtains a key by independently quantizing its own analog noisy CSI measurements. We will refer here to the symbol mismatch rate as the probability that given one sample measurement $\hat{h}_A$ at Alice and the corresponding measurement $\hat{h}_B$ at Bob, they are not quantized to the same region by both users.

Points from the channel distribution that are very close to quantization boundaries are very likely to result in a key mismatch. If a channel value h falls within a certain region $\mathcal{R}_i$, but very close to a quantization boundary, its noisy measurements $\hat{h}_A$ and $\hat{h}_B$ might simply jump across the quantization threshold to a neighboring region. Both the quantization algorithm and the size of the codebook N_q, greatly impact the overall symbol agreement rate between Alice and Bob.

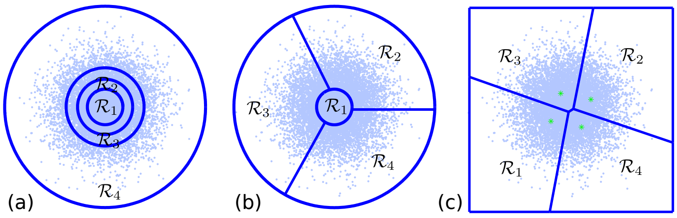

Fig. 2. Three quantization methods - (a) concentric quantization regions; (b) circles and slices; (c) Linde-Buzo-Gray algorithm, $N_q = 4$

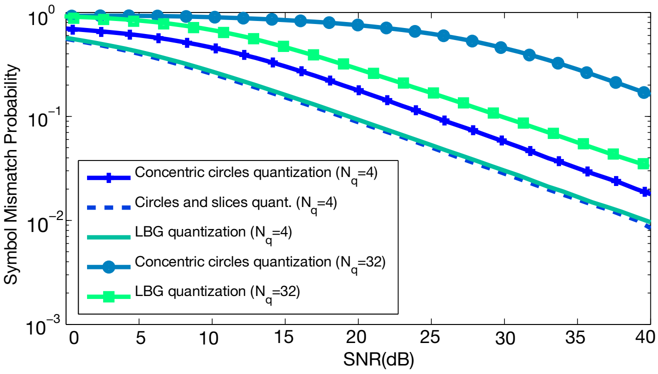

Fig. 3. Symbol mismatch probability between Alice and Bob for different quantization methods (no reconciliation)

We consider three vector quantizations schemes, the first based on concentric circles, as illustrated in Fig. 2-(a), the second based on concentric circles and slices, as shown in Fig. 2-(b), and the third based on the Linde-Buzo-Gray algorithm [5], [14], leading to the quantization areas shown in Fig. 2-(c), all for a codebook size of $N_q = 4$. The radii of the concentric circles in the first method are computed such that the number of measurement points end up uniformly distributed across all regions. The exact values are provided in Table I. While such a method leads to a simplification of the LLR formulation, as it will be explained in Section IV, when the codebook size is increased, a severe performance degradation in terms of symbol-error-ratio (SER), or symbol mismatch rate, is noticed. This is a direct consequence of the shape of the quantization regions. The narrower a region is, the more likely it is that noisy measurements will end up quantized to neighboring regions. Increasing the number of regions N_q in the first quantization example will lead to even narrower regions, thus, such quantization method will be highly sensitive in terms of noise, leading to a high number of errors even at high signal-to-noise (SNR) ratios.

TABLE I
QUANTIZATION LIMITS; $N_q = 4$; $\sigma = \sqrt{\sigma_{ch}^2 + \sigma_A^2}$

	METHOD	(a)		METHOD	(b)	
Region	r_{min_i}	r_{max_i}	r_{min_i}	r_{max_i}	θ_{min_i}	θ_{max_i}
$\mathcal{R}_1$	0	$0.758\ \sigma$	0	$0.758\ \sigma$	0	2π
$\mathcal{R}_2$	$0.758\ \sigma$	$1.177\ \sigma$	$0.758\ \sigma$	∞	0	$\frac{2\pi}{3}$
$\mathcal{R}_3$	$1.177\ \sigma$	$1.665\ \sigma$	$0.758\ \sigma$	∞	$\frac{2\pi}{3}$	$\frac{4\pi}{3}$
$\mathcal{R}_4$	$1.665\ \sigma$	∞	$0.758\ \sigma$	∞	$\frac{4\pi}{3}$	2π

The second quantization method introduces the so-called "slices" as a way to mitigate this effect and counteract the error performance degradation. This quantization method also leads to a uniform distribution of the key symbols, which is desirable for secrecy concerns, i.e., not to provide any redundancy to a potential eavesdropper. The boundaries for the four regions $\mathcal{R}_i$ illustrated in Fig. 2-(c) are also provided in Table I, in terms of radii (r_{min_i}, r_{max_i}) and angles $(\theta_{min_i}, \theta_{max_i})$, in polar coordinates. As seen in Fig. 3, this method shows a better performance in terms of symbol mismatch probability, as compared to the previous one, with an error reduction from 17% to 9% at an SNR of 20 dB, and from 1.78% to 0.95% at 40 dB, for the case of four quantization regions.

The third algorithm for channel quantization is the Linde-Buzo-Gray (LBG) vector quantization scheme, as described in [14]. The LBG algorithm is a sample version of the Lloyd-Max quantizer that does not require a closed form pdf of the channel distribution, but only the measurement samples. Given a length M sequence of 2-dimensional channel samples and the desired number of code vectors N_q, the algorithm delivers the final codebook and the corresponding quantization region for each codeword vector.

The difference in mismatch rate between the first and third quantization method also becomes much more significant when increasing the size of the codebook vector. For an SNR of 20 dB and $N_q = 32$ quantization regions, we notice a probability of 75% that Alice and Bob quantize to different regions when using first method (concentric circles), as compared to 24% when using the LBG algorithm.

Once such partitioning boundaries have been determined, a Gray-like bit mapping can be assigned to the regions.

A. Key Probability Distribution

The one-time pad perfect secrecy is achieved under two important assumptions, namely that the pad length is at least the size of the message to be encrypted, and that the key is selected at random with a uniform distribution. Thus, achieving a low SER is not sufficient, provided the uniform distribution requirement is not entirely satisfied. Since the key distribution is a parameter that is assumed to be known to the eavesdropper, a non-uniform distribution will result in some keys being more probable than others, facilitating potentially successful analytical attacks. When the output distribution provided by the quantizer is not uniform, the perfect secrecy condition requiring the eavesdroppers equivocation to be equal to the entropy of the message is not satisfied. While the first two quantization methods are constructed with a circularly symmetric zero-mean Gaussian input distribution in mind, with variance σ, and, by construction, deliver a uniform output distribution of the symbols, regardless of the codebook size[1], the LBG algorithm can be used for any arbitrary distribution. However, we show in Fig. 5 that the LBG quantization fails to deliver an exact uniform output distribution, even for small codebook lengths, i.e., $N_q = 4$. The non-uniformity of the distribution becomes even more pronounced for higher alphabets. Figure 4 shows the distribution of measurement points across 32 Voronoi regions delivered by the LBG algorithm. The non-uniformity can be expressed as a rate loss which we have taken into account in Fig. 3 by a corresponding right shift of the LBG curves. The rate loss corresponds to ideal source coding to make the distribution uniform. Overall, the best error performance among the three cases analyzed is provided by the second quantization method for the case of four regions, with only a slight advantage over the LBG algorithm.

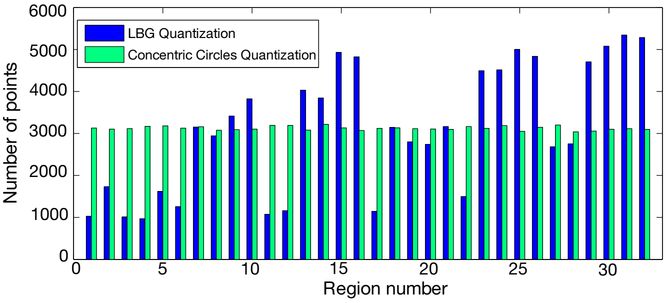

Fig. 4. Distribution of measurement points across $N_q = 32$ Voronoi regions resulting from concentric circles quantization and LBG quantization

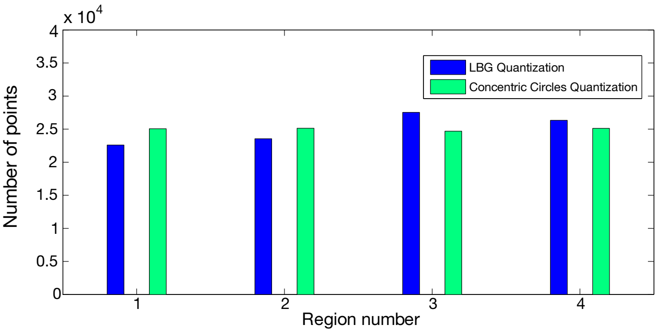

Fig. 5. Distribution of measurement points across $N_q = 4$ Voronoi regions resulting from concentric circles quantization and LBG quantization

IV. KEY RECONCILIATION

For notation simplicity, we will denote an analog complex measurement estimate at Alice, $\hat{h}_A$, by $a = x_A + jy_A$, and a channel estimate at Bob, $\hat{h}_B$, by $b = x_B + jy_B$, where (x, y) denote the real and imaginary parts, respectively. These values represent the AWGN-disturbed measurements of the ideal channel sample $c = x_{ch} + jy_{ch}$, at Alice and Bob, respectively. The input to the LDPC decoder consists of two sets of log-likelihood ratios (LLRs), one for the parity symbols received from Alice, and one for Bob's own estimates of the channel, assuming Alice's key bits as "correct" reference. In general,

[1] We only provide here a table of quantization boundaries for four quantization regions, although the limits for higher codebook sizes can be easily computed by integrating the complex Gaussian input distribution and imposing equal "volumes" in each region, i.e, uniform output distribution.

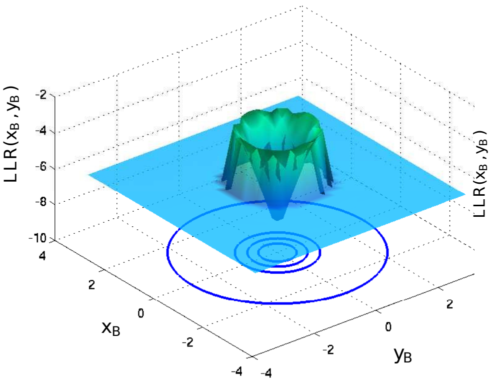

Fig. 6. Method (a): LLR(b)=ln $\frac{P(a\in\mathcal{R}_3|b)}{P(a\notin\mathcal{R}_3|b)}$

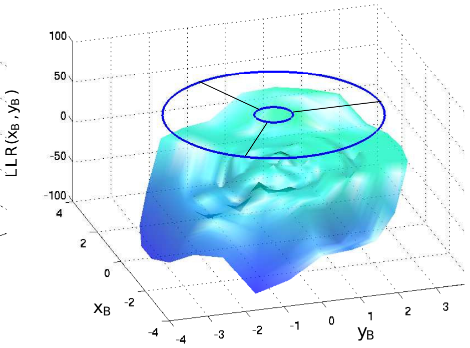

Fig. 7. Method (b): LLR(b)=ln $\frac{P(a\in\mathcal{R}_2|b)}{P(a\notin\mathcal{R}_2|b)}$

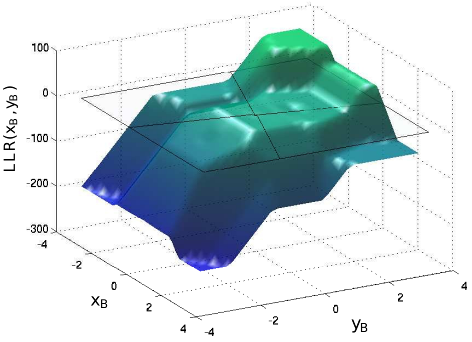

Fig. 8. LBG quant: LLR(b)=ln $\frac{P(a\in\mathcal{R}_3|b)}{P(a\notin\mathcal{R}_3|b)}$

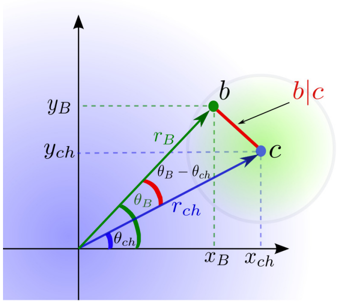

Fig. 9. Polar coordinates transformation; Given channel measurement c, b represents Bob's noisy measurement of c. In polar coordinates c is represented by (r_{ch}, θ_{ch}).

the LLR for a measurement value at Bob can be computed according to (1), where $p(b|a \in \mathcal{R}_i)$ is the probability density function of Bob's measurement b given that Alice quantized its corresponding value a to region $\mathcal{R}_i$.

$$LLR(b) = \ln \frac{p(b|a \in \mathcal{R}_i)}{p(b|a \notin \mathcal{R}_i)} \qquad (1)$$

Previous works, such as [13], consider a noiseless environment for the transmission of side information, or simply consider the same formulation for the information bits, as for the parity (syndrome) bits that are transmitted over the physical channel. This is, however, inaccurate, and leads to sub-optimum decoding.

While the LLR computation for the parity bits is trivial (2), since they might just experience a standard AWGN channel with variance σ_B^2, the calculation of the LLRs for Bob's information bits is much more problematic, due to the fact that Bob's decoding of the information bits is subject to what Alice quantized to.

$$LLR_{parity}(b) = \ln\left(\frac{e^{-\frac{(b-1)^2}{2\sigma_B^2}}}{e^{-\frac{(b+1)^2}{2\sigma_B^2}}}\right) = \frac{2b}{\sigma_B^2} \; . \qquad (2)$$

The LLR formulation for the information bits at Bob has to account for the fact that Alice measures the channel with error determined by σ_A^2, and then quantizes. Nevertheless, Bob assumes that whatever Alice quantized to represents the correct key and it has to reconcile with her values. In [6], we have shown that the general formula for the LLR for the information symbols, assuming a uniform distribution of the quantized measurements across N_q regions, to be as follows

$$LLR(b) = \ln \frac{(N_q-1)P(a \in \mathcal{R}_i|b)}{P(a \notin \mathcal{R}_i|b)} \; , \qquad (3)$$

where $P(a \in \mathcal{R}_i|b)$ represents the probability that Alice quantized its value a to region $\mathcal{R}_i$, given current measurement value b at Bob. In more intuitive terms, Eq. (3) is a measure of the log-likelihood that given a noisy value of the channel at Bob, Alice quantized her noisy counterpart to a certain region $\mathcal{R}_i$ and not the others. Now, by iterating through all the possible regions and computing LLRs for b, a vector of LLRs is produced for every variable node of the LDPC decoder that is associated with the channel measurements (information symbols). In [6] we provide a complete derivation of the exact LLR formulation when the channel distribution is a circularly symmetric Gaussian.

Equation (4) shows the LLR expression when the concentric circles quantization is used. For this specific quantization method, a transformation to polar coordinates, such as the one shown in Fig. 9, allows us to express parts of the LLR expression with modified Bessel functions of the first kind (J_0) as given by (4). Such a simplification leads to a significant reduction in the number of numerical integrations. However, this is only possible for the concentric circles quantization, which comes with the disadvantage of a worse SER performance than any of the other two methods. The LLR for the slices quantization is given in (5), while the one for arbitrary Voronoi regions is given by (6). The LLRs in (4) – (6) are functions of b that can be viewed as resulting from the convolution of the noise and channel densities, and can be computed in advance by numerical integration, and stored, for a wide range of values of b values and SNRs, in order to speed up the LDPC decoder.

V. Numerical Results

In this section, we provide some numerical results for the intrinsic LLRs required by the LDPC decoder on Bob's side, necessary for key reconciliation, given the three different types of quantization discussed.

We show in Fig. 6 the numerical results obtained for the log-likelihood ratios for the first type of quantization, for an SNR=14 dB, where the SNR is defined as σ_{ch}^2/σ_B^2. Figure 6 shows for every possible value of b, in Cartesian coordinates, (x_B, y_B), the probability that Alice quantized to region $\mathcal{R}_3$ and not to any other regions. As expected, for values of b that would be also in region $\mathcal{R}_3$ and fall sufficiently far away

$$LLR_{\text{(a)}}(r_B) = \ln \frac{(N_q-1)\int\limits_{0}^{\infty}\int\limits_{r_{min_i}}^{r_{max_i}} r_A r_{ch} e^{-\frac{r_{ch}^2+r_A^2}{2\sigma_A^2}-\frac{r_{ch}^2+r_B^2}{2\sigma_B^2}-\frac{r_{ch}^2}{2\sigma_{ch}^2}} \cdot J_0(-\frac{r_{ch}r_A}{\sigma_A^2}) \cdot J_0(-\frac{r_{ch}r_B}{\sigma_B^2}) dr_A dr_{ch}}{\sum\limits_{\mathcal{R}_k, k\neq i}\int\limits_{0}^{\infty}\int\limits_{r_{min_k}}^{r_{max_k}} r_A r_{ch} e^{-\frac{r_{ch}^2+r_A^2}{2\sigma_A^2}-\frac{r_{ch}^2+r_B^2}{2\sigma_B^2}-\frac{r_{ch}^2}{2\sigma_{ch}^2}} \cdot J_0(-\frac{r_{ch}r_A}{\sigma_A^2}) \cdot J_0(-\frac{r_{ch}r_B}{\sigma_B^2}) dr_A dr_{ch}} \tag{4}$$

$$LLR_{\text{(b)}}(r_B, \theta_B) = \ln \frac{(N_q-1)\int\limits_{0}^{\infty}\int\limits_{0}^{2\pi}\int\limits_{r_{min_i}}^{r_{max_i}}\int\limits_{\theta_{min_i}}^{\theta_{max_i}} r_A r_{ch} e^{-\frac{r_{ch}^2+r_A^2-2r_{ch}r_A\cos(\theta_{ch}-\theta_A)}{2\sigma_A^2}-\frac{r_{ch}^2+r_B^2-2r_{ch}r_B\cos(\theta_{ch}-\theta_B)}{2\sigma_B^2}-\frac{r_{ch}^2}{2\sigma_{ch}^2}} d\theta_A dr_A d\theta_{ch} dr_{ch}}{\sum\limits_{\mathcal{R}_k, k\neq i}\int\limits_{0}^{\infty}\int\limits_{0}^{2\pi}\int\limits_{r_{min_k}}^{r_{max_k}}\int\limits_{\theta_{min_k}}^{\theta_{max_k}} r_A r_{ch} e^{-\frac{r_{ch}^2+r_A^2-2r_{ch}r_A\cos(\theta_{ch}-\theta_A)}{2\sigma_A^2}-\frac{r_{ch}^2+r_B^2-2r_{ch}r_B\cos(\theta_{ch}-\theta_B)}{2\sigma_B^2}-\frac{r_{ch}^2}{2\sigma_{ch}^2}} d\theta_A dr_A d\theta_{ch} dr_{ch}} \tag{5}$$

$$LLR_{\text{(c)}}(x_B, y_B) = \ln \frac{(N_q-1)\int\limits_{-\infty}^{\infty}\int\limits_{-\infty}^{\infty}\int\limits_{\mathcal{R}_{i_y}}\int\limits_{\mathcal{R}_{i_x}} e^{-\frac{(x_A-x_{ch})^2+(y_A-y_{ch})^2}{2\sigma_A^2}-\frac{(x_{ch}-x_B)^2+(y_{ch}-y_B)^2}{2\sigma_B^2}-\frac{(x_{ch}^2+y_{ch}^2)}{2\sigma_{ch}^2}} dx_A\, dy_A\, dx_{ch}\, dy_{ch}}{\sum\limits_{\mathcal{R}_k, k\neq i}\int\limits_{-\infty}^{\infty}\int\limits_{-\infty}^{\infty}\int\limits_{\mathcal{R}_{k_y}}\int\limits_{\mathcal{R}_{k_x}} e^{-\frac{(x_A-x_{ch})^2+(y_A-y_{ch})^2}{2\sigma_A^2}-\frac{(x_{ch}-x_B)^2+(y_{ch}-y_B)^2}{2\sigma_B^2}-\frac{(x_{ch}^2+y_{ch}^2)}{2\sigma_{ch}^2}} dx_A\, dy_A\, dx_{ch}\, dy_{ch}} \tag{6}$$

from any quantization boundaries, the LLR is maximum. As b takes values closer to the quantization thresholds and into other regions, the LLR decreases to a minimum. This is the case for regions $\mathcal{R}_1, \mathcal{R}_2$, and $\mathcal{R}_4$. For the second quantization method (b), Fig. 7 shows the log-likelihood plot for one of the external slices. Figure 8 shows the log-likelihood for $\mathcal{R}_3$, for the case of the arbitrary Voronoi quantization regions, as provided by the LBG algorithm. The numbering of the regions is the one provided in Fig. 2. For our simulations, we used a discrete grid for b with incremental values of 0.05 between $[-3.5, 3.5]$ for both axes.

VI. Conclusion

We have investigated the problem of physical-layer key generation and reconciliation with Slepian-Wolf coding and Low-Density Parity-Check (LDPC) codes in a wireless scenario when two users measure a reciprocal channel with independent noise on both sides. We offered an analysis on the effect of different quantization schemes on the overall error rate performance, or key disagreement rate, assuming imperfect channel measurements. Our results show that for higher codebook sizes, the Linde-Buzo-Gray quantizer does not output a uniform distribution of key symbols, which is of paramount importance for the secrecy aspect, and show a possible quantization scheme that guarantees a uniform output distribution and also provides a slightly lower key disagreement rate than the LBG quantizer. We have further shown the log-likelihood (LLR) formulation required by a soft-decision LDPC decoder for key reconciliation, for each of the quantization schemes analyzed and a circularly symmetric complex Gaussian channel distribution.

Acknowledgment

This work is supported by the German Research Foundation (Deutsche Forschungsgemeinschaft – DFG).

References

[1] C. E. Shannon, “Communication Theory of Secrecy Systems,” *Bell System Technical Journal*, 28:656–715, 1949.

[2] R. Mehmood and J. Wallace, “Wireless Security Enhancement Using Reconfigurable Aperture Antennas,” *European Conference on Antennas and Propagation (EuCAP’11)*, Rome, Italy, Apr. 12-16, 2011, pp. 1-5.

[3] R. Mehmood and J. Wallace, “MIMO Capacity Enhancement Using Parasitic Reconfigurable Aperture Antennas (RECAPs),” *IEEE Transactions on Antennas and Propagation*, vol. 60, pp. 665-673, Feb. 2012.

[4] J. Wallace, R. Kurma, “Automatic Secret Keys From Reciprocal MIMO Wireless Channels: Measurement and Analysis,” *IEEE Transactions on Information Forensics and Security*, vol. 5, pp. 381-392, Sept. 2010.

[5] A. Filip, R. Mehmood, J. Wallace, and W. Henkel, “Variable Guard Band Construction to Support Key Reconciliation,” *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2014)*, Florence, Italy, May. 4-9, 2014.

[6] O. Graur, N. Islam, A. Filip, and W. Henkel, “Quantization Aspects in LDPC Key Reconciliation for Physical Layer Security” *10th International ITG Conference on Systems, Communications and Coding (SCC)*, Hamburg, Germany, February 2-5, 2015.

[7] A. Filip, R. Mehmood, J. Wallace, and W. Henkel, “Physical-Layer Key Generation Supported by RECAP Antenna Structures,” proc. *9th International ITG Conference on Source and Channel Coding (SCC)*, Munich, Germany, 2013.

[8] M. Bloch, J. Barros, “Physical-Layer Security: From Information Theory to Security Engineering,” *Cambridge University Press*, 2011.

[9] X. Zhou, L. Song, Y. Zhang, “Physical Layer Security in Wireless Communications,” *CRC Press Inc.*, 2013.

[10] R. Wilson, D. Tse, R. .A. Scholz, “Channel Identification: Secret Sharing using Reciprocity in Ultrawideband Channels,” *IEEE Transactions on Information Forensics and Security*, 2:364-375, Sept. 2007.

[11] C.Y. William Lee, “Mobile Communications Design Fundamentals,” *John Wiley & Sons, Inc.,*, New York, NY, USA, 1992, pp. 227-240.

[12] A. J. Pierrot, R. A. Chou, M. R. Bloch, “Experimental Aspects of Secret Key Generation in Indoor Wireless Environments,” in *2013 IEEE 14th Workshop on. Signal Processing Advances in Wireless Communications (SPAWC)*, 2013, pp. 669673.

[13] X. Sun, X. Wu, C. Zhao, M. Jiang, and W. Xu, “Slepian-Wolf Coding for Reconciliation of Physical Layer Secret Keys,” proc. *IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1-6, 18-21 Apr. 2010.

[14] Y. Linde, A. Buzo, R. M. Gray, “An Algorithm for Vector Quantizer Design,”*IEEE Transactions on Communications*, 28:84-95, 1980.

[15] J.W. Wallace and R.K. Sharma, “Automatic Secret Keys from Reciprocal MIMO Wireless Channels: Measurement and Analysis,” *IEEE Trans. Inf. Forensics and Security*, vol. 5, no. 3, pp. 381-392, Sep. 2010.