Quantization Aspects in LDPC Key Reconciliation 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*—For physical-layer security, key reconciliation procedures are needed to correct key differences that can arise as a consequence of independent noise at the two ends of a reciprocal link. We assume either a random link in a mobile environment or use reconfigurable antenna elements to randomize the channel, such that it allows for frequent key generation. We apply LDPC codes to reconcile the keys on both sides. In here, we derive the LLRs taking into account the underlying quantization.**

I. Introduction and Motivation

Secrecy can be attained at the physical layer in a time division duplex (TDD) wireless environment by exploiting the mutual channel-state-information (CSI) in order to generate shared keys between legitimate users [1]–[6]. Nevertheless, quantization errors and independent noise might eventually lead to key mismatches. For this reason, a mechanism that ensures key reconciliation is needed. Further effects, such as differences in amplifier non-linearities and quantization boundaries or synchronization effects are ignored for the treatment in here. We focus on developing two key reconciliation procedures which employ binary and non-binary LDPC codes.

Due to the randomness of wireless channels, an eavesdropper located further away than the minimum coherence distance[1] will likely experience a completely different channel, being left with the option of brute force attacks. Paired with a frequent key generation and privacy amplification, such an attempt would be rendered infeasible. We assume a flat fading channel for the sake of simplicity.

In the case of mobile terminals, the changing channel will allow for frequent generation of new keys. In the case of a stationary line-of-sight channel, we use reconfigurable antenna elements to randomize the channel to mimic a mobile environment. The paper is structured as follows, the next section gives a brief system description. Section III introduces the key reconciliation techniques used. In Section IV, the specific LLR formulation problem is addressed. Two approaches are compared and analyzed in Section V. Section VI concludes the paper.

II. System Description

For our analysis, a few assumptions have been made. The wireless channel between Alice and Bob is *reciprocal*, i.e., channel amplitude and phase are identical in both directions. Both Alice and Bob obtain channel-state information (CSI) by sending pilot signals previously known to all parties. Since we consider a TDD system, it is further assumed that Alice and Bob obtain their estimates in consecutive time slots and that the channel has not changed during both their measurements, i.e., the coherence time is larger than the measurement time. In order to emulate a mobile channel environment (a time-variant channel), we use reconfigurable aperture antennas (RECAPs). After the channel measurement data is obtained, we use vector quantization to discretize the channel for key generation. We consider a parasitic RECAP at Alice to generate artificial fading in a line of sight channel to simulate the mobile environment. Further design specifications can be found in [8].

In order to obtain channel characteristics, a hybrid approach which employs full wave simulation is combined with network analysis to provide fast and accurate channel statistics. When a 24-RECAP is used for randomization, the measured channel is found to approximately have a complex Gaussian shape [9].

III. Key Reconciliation Methods

The key reconciliation method detailed in this paper employs Slepian-Wolf coding with Low Density Parity Check (LDPC) codes. The choice of using LDPC codes is motivated by their ability to achieve performances close to the Shannon capacity [10]. Since LDPC codes themselves have been thoroughly analyzed and discussed in other reference works, we will limit our description here to the context of our key-reconciliation scheme.

A. Slepian-Wolf Coding

The CSI measurements of both Alice and Bob lead to the generation of two correlated keys. Further exchange of information is thus required between Alice and Bob in order to ensure that the keys both of them generate are not only correlated, but identical. This, however, needs to be performed in such a way that secrecy is not compromised, implying that neither Alice nor Bob send actual CSI information to each other. The solution to this problem is offered by Slepian-Wolf coding which is a type of source coding with side information.

◇ A. Filip is now with DLR, Oberpfaffenhofen, Germany.

[1]For 802.11 at 2.4 GHz, the coherence distance is $\frac{\lambda}{2} \approx 6$ cm. Further recent results supporting this assumption can be found in [7].

ISBN 978-3-8007-3659-1

There are two equivalent approaches to Slepian-Wolf coding, the parity approach and the syndrome approach[2]. As shown in Fig. 1, both legitimate users, Alice and Bob, measure the same reciprocal physical channel but obtain slightly different estimates, $\mathbf{a} = [a_1, a_2, \ldots, a_N]^T$ and $\mathbf{b} = [b_1, b_2, \ldots, b_N]^T$, due to independent noise with variances σ_A^2, and σ_B^2, respectively. Alice compresses her quantized key information $\mathbf{a}$ to a syndrome $\mathbf{s} = [s_1, s_2, \ldots s_M]$ and sends it over the physical channel to Bob. Regardless of the method used to generate the parities, BPSK signalling can be used for transmission over the physical channel.

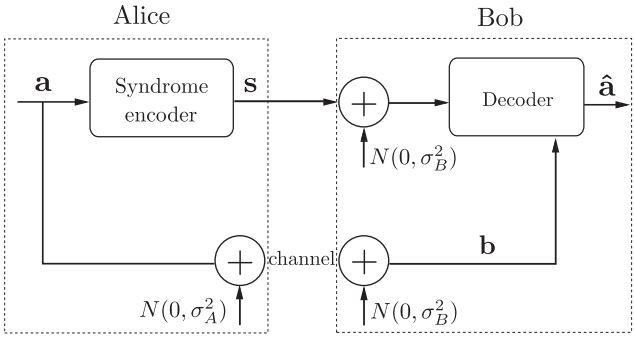

Fig. 1. Syndrome method for Slepian-Wolf decoding

Bob uses both the noisy side information received from Alice, along with his noisy measurement values in order to decode the correlated information.

B. Encoding: LDPC Codes

Here, multi-edge type irregular Low-Density Parity-Check Codes (LDPC) are chosen for the implementation of Slepian-Wolf coding. The whole system can be seen as using two concatenated LDPC codes, one to generate the syndrome, as shown in (1), and one to add redundancy for sending it over the noisy physical channel. Further details on the construction of the concatenated LDPC code can be found in [11]. The syndrome vector to be sent to Bob over the physical channel is computed according to

$$\mathbf{s} = \mathbf{Ha}\,, \tag{1}$$

where $\mathbf{H}$ is the sparse parity check matrix of the first LDPC code used to generate the syndrome, of size $M \times N$, with $M = N - K$.

C. Decoding: LDPC Codes

The decoding process is depicted in Fig. 2. For the soft-value LDPC decoding on Bob's side, we use an efficient message passing decoding algorithm called Belief-Propagation (BP).

The inputs to the LDPC decoder are log-likelihood ratios (LLR) values defined as in (2) for a binary codebook,

$$L(b) = \ln \frac{P(b|a=+1)}{P(b|a=-1)}\,, \tag{2}$$

where a represents Alice's quantized value and b is Bob's analog measurement, assuming Alice's key bits as "correct" reference. $P(b|a=+1)$ stands for the probability of

[2]The syndrome approach was employed for the current work, although throughout the paper we also use the term "parity" bits interchangeably to refer to the syndrome bits sent by Alice to Bob.

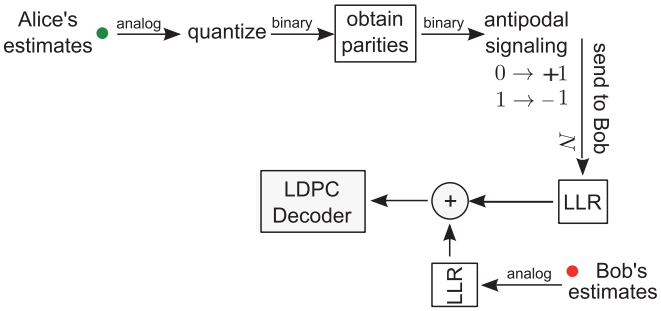

Fig. 2. Decoding steps

Bob to measure b, given that Alice quantized to $a = +1$. Throughout the rest of the paper we will use upper case P to denote probabilities and lowercase p to denote probability density functions (pdfs).

For our key reconciliation system, it is imperative to distinguish between two classes of variable nodes of the multi-edge LDPC decoder: the set of variable nodes whose inputs are LLRs corresponding to the information symbols obtained by Bob from his own measurements of the channel, and the set of variable nodes whose inputs deal with the parity (syndrome) symbols received from Alice. As it will become evident in the following section, different ways of calculating the LLR values are required, one for the information bits and one for the parity bits.

There has been some independent experimental work in [7] that analyzes the secrecy capacity, but, like many other relevant works found in literature, assumes the side information is transmitted over a noiseless physical channel, which is not realistic. The analysis we provide here takes into account the noise effect on both the independent measurements of the legitimate users Alice and Bob, as well as on the transmission of parities (side information) over the physical channel.

IV. LLR Formulation for Belief Propagation (BP) Decoding in the LDPC Decoder

A. LLR for Parity Bits

The parity bits just experience a standard AWGN physical channel with variance σ_B^2, hence

$$p(b|a=\pm 1) = \frac{1}{\sqrt{2\pi\sigma_B^2}} e^{\frac{-(b\mp 1)^2}{2\sigma_B^2}}\,.$$

The corresponding LLR for the parity bits is given by

$$LLR_{\,parity} = \ln\left(\frac{e^{-\frac{(b-1)^2}{2\sigma_B^2}}}{e^{-\frac{(b+1)^2}{2\sigma_B^2}}}\right) = \frac{2b}{\sigma_B^2}\,. \tag{3}$$

B. LLR for Information Bits

While the computation of LLRs in the case of the parity bits is trivial, this is not the case for the information bits. Furthermore, for the information bits, we will offer a comparison between an accurate but more complex method of computing LLRs, in Section IV-B2, and an approximation of lower complexity, presented in Section IV-B1.

1) Modeling quantization effects by increased Gaussian noise in the LLR computation - Approximate LLR Computation: As previously mentioned, due to independent noise contributions at both ends of our channel, the resulting quantization regions for a specific symbol might not coincide for Alice and Bob.

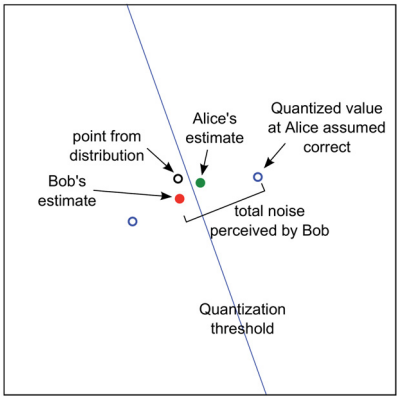

Fig. 3. Decoding scenario for quantized values at Alice assumed to be correct

A point from the channel distribution is measured by both Alice and Bob, disturbed by different noise contributions, σ_A^2 and σ_B^2, respectively. For simplicity, we assume here that $\sigma_A^2 = \sigma_B^2$. The analog value at Alice is then quantized and assumed to be correct. Due to this assumption, the total noise in effect perceived by Bob is marked in Fig. 3. In the LLR computation of the information bits, to model this increased noise, we increase the AWGN variance at Bob to at least twice that of the actual variance, namely $\sigma^2 = 2\sigma_B^2$. For the LLR calculation of the information bits, we use $p(b|a = c_{+1})$ and $p(b|a = c_{-1})$, where c_{+1} and c_{-1} represent our codebook vectors. Using the 2D Gaussian pdf we obtain,

$$p(b|a = c_{\pm 1}) = \frac{1}{2\pi\sigma^2} e^{\frac{-d(b,c_{\pm 1})}{2\sigma^2}} .$$

Here, $d(b, c_{\pm 1})$ denotes the squared Euclidean distance between the received value b and the codebook entries $c_{\pm 1}$. Thus, the intrinsic LLR is

$$LLR_{\,intrinsic} = \frac{d(b, c_{-1}) - d(b, c_{+1})}{2\sigma^2} . \quad (4)$$

This method is an approximation and leads to errors. The Euclidean distance measure is not robust when Bob's estimate point is close to the threshold since the distance is subject to the position of the codebook vectors inside their respective quantization regions.

2) Exact LLR Computation for Information Bits: Let us again assume Alice's key (quantization region) to be correct and Bob's to be reconciled.

The undisturbed complex value $c = x_{ch} + jy_{ch}$ from the channel distribution is disturbed by AWGN to $a = x_A + jy_A$ on Alice's side before quantization and to $b = x_B + jy_B$ on Bob's side, as shown in Fig. 4. The complex channel distribution is given by (5),

$$p(c) = \frac{1}{2\pi\sigma_{ch_x}\sigma_{ch_y}} e^{-\frac{1}{2}\left(\frac{(x_{ch}-\mu_{ch_x})^2}{\sigma_{ch_x}^2} + \frac{(y_{ch}-\mu_{ch_y})^2}{\sigma_{ch_y}^2}\right)} . \quad (5)$$

Assuming that the channel means are zero, $\mu_{ch_x} = \mu_{ch_y} = 0$, and the variances $\sigma_{ch_x}^2 = \sigma_{ch_y}^2 = \sigma_{ch}^2$, we can further simplify Eq. (5) to

$$p(c) = \frac{1}{2\pi\sigma_{ch}^2} e^{-\frac{(x_{ch}^2 + y_{ch}^2)}{2\sigma_{ch}^2}} . \quad (6)$$

The disturbance at Bob, $p(b|c)$ is written as

$$p(b|c) = \frac{1}{2\pi\sigma_B^2} e^{-\frac{(x_B - x_{ch})^2 + (y_B - y_{ch})^2}{2\sigma_B^2}} . \quad (7)$$

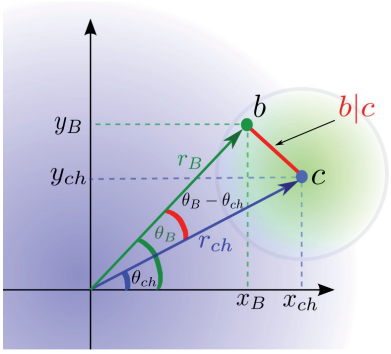

Fig. 4. Polar coordinates transformation; Given channel measurement c, b represents Bob's noisy measurement of c. In polar coordinates c is represented by (r_{ch}, θ_{ch}).

Similarly, the disturbance at Alice, $p(a|c)$, given the ideal channel measurement c, is given by

$$p(a|c) = \frac{1}{2\pi\sigma_A^2} e^{-\frac{(x_A - x_{ch})^2 + (y_A - y_{ch})^2}{2\sigma_A^2}} , \quad (8)$$

where σ_A^2 and σ_B^2 are the variances of the independent AWGN noise present at Alice and Bob, respectively. Again, the means (μ_{A_x}, μ_{A_y}) and (μ_{B_x}, μ_{B_y}) of the independent complex noise, at both Alice and Bob, are assumed to be zero.

Using Bayes' rule, we obtain

$$p(c|b) = \frac{1}{2\pi\sigma_B^2} e^{-\frac{|c-b|^2}{2\sigma_B^2}} \cdot \frac{p(c)}{p(b)} ,$$
$$p(c|a) = \frac{1}{2\pi\sigma_A^2} e^{-\frac{|c-a|^2}{2\sigma_A^2}} \cdot \frac{p(c)}{p(a)} ,$$

where $p(a)$ and $p(b)$ are given by (9) and (10) as

$$p(a) = \frac{1}{2\pi(\sigma_{ch}^2 + \sigma_A^2)} e^{-\frac{(x_A^2 + y_A^2)}{2(\sigma_{ch}^2 + \sigma_A^2)}} , \quad (9)$$

$$p(b) = \frac{1}{2\pi(\sigma_{ch}^2 + \sigma_B^2)} e^{-\frac{(x_B^2 + y_B^2)}{2(\sigma_{ch}^2 + \sigma_B^2)}} . \quad (10)$$

We assume N quantization regions $\mathcal{R}_i$, $i \in [1, N]$, $N = 2^m$. Notation $\mathcal{R}$ is employed to denote the union of all quantization regions $\mathcal{R}_i$. On Bob's side, having received a value b, we need to determine the probability of what Alice may have quantized to, i.e., $P(a \in \mathcal{R}_i|b)$ and $P(a \notin \mathcal{R}_i|b)$.

$$P(a \in \mathcal{R}_i|b) = \int_{\mathcal{R}_i} \int_{\mathcal{R}} p(a|c) \cdot p(c|b)\, dc\, da ,$$
$$P(a \notin \mathcal{R}_i|b) = \int_{\mathcal{R} \setminus \mathcal{R}_i} \int_{\mathcal{R}} p(a|c) \cdot p(c|b)\, dc\, da .$$

Note, c and a are, of course, complex and also the corresponding integrals are complex. Exploiting Bayes' rule again, we obtain,

$$p(b|a \in \mathcal{R}_i) = P(a \in \mathcal{R}_i|b) \cdot \frac{p(b)}{P(a \in \mathcal{R}_i)} ,$$
$$p(b|a \notin \mathcal{R}_i) = P(a \notin \mathcal{R}_i|b) \cdot \frac{p(b)}{P(a \notin \mathcal{R}_i)} .$$

Thus, we can finally write down the equation for the intrinsic LLR that is needed as an input to the LDPC decoder. Since the LLR is given by the ratio of two quadruple integrals as in (11), for our simulations we resort to the two examples in Fig. 5 and the binary case. The LLR for the intrinsic information might be precomputed replacing the integrals by sums and doing this over a discrete valued grid. However, a discrete sum over the entire space is computationally very extensive and practically unrealistic. In order to use the expression for real time computations, we need to simplify. By employing polar coordinates (r, θ), the limits of the quantization regions are easily computed, requiring a uniform distribution of the regions. Note that a good key sequence should have equally distributed values. Tables I and II present the quantization area limits for the examples in Fig. 5. Given a quantization region $\mathcal{R}_i$, we employ the notation (R_i, Θ_i) to denote the sets of radii and angles of every point belonging to the region. For our simulations we use a discretized grid for b with incremental values of 0.05 between -3.5 and 3.5 for both real and imaginary axis. For the case of two quantization regions, $+1$ and -1, the LLR in (11) reduces to (13). The LLR in (11) applies to a general case where the quantization regions are circles and slices, as shown in Fig. 5-a. For the second case, where the quantization regions are concentric circles only, given the Gray mapping in Fig. 5-b, we distinguish at the input of the LDPC decoder between the first bit (in green) and the second bit (in blue). Thus, we switch between two sets of LLR values, one corresponding to each bit. This enables us to simplify the quadruple integrals to double integrals by using Bessel functions of the first kind, as in (12). This simplification is only possible if the quantization regions are concentric circles, as depicted in Fig. 5-b. Equation (12) gives the LLR for the first bit (in green). In the numerator, we integrate over the regions where the first bit has a value of 0, in our example $\mathcal{R}_1$ and $\mathcal{R}_2$, while in the denominator we consider the regions where the first bit has a value of 1, $\mathcal{R}_3$ and $\mathcal{R}_4$. We omit the explicit formula for the second bit here due to space limitations, nevertheless it follows the same principle, given the corresponding integration limits. In the binary case, when presented with two quantization regions, the LLR in (11) reduces to (13), due to symmetry properties. Hence, we use Eq. (13) to calculate the LLR value for the information bits. For the parity bits, Eq. (3) is used.

V. Results

This section presents the results of a BER comparison when using the two different LLR options presented in Sections IV-B1 and IV-B2 for the binary case, along with the likelihood ratios for the example in Fig. 5-b. Figures 6-7 show the likelihood ratios for the first and second bit, respectively, for the quantization regions in Fig. 5-b.

For the binary case, as can be seen from Fig. 8, when using the approximate approach described in Section IV-B1, at high SNR, an unexpected drop in performance is observed. This is because, at high SNR, the points that still cross the quantization threshold are now quantized with a higher error value, thus the quantization effect becomes more dominant. With the correctly derived LLR (Eq. (13)), this error effect is eliminated. In Fig. 9, we show the LLR curves for different SNR values. For high SNRs, the absolute value of the LLR increases, reflecting the expected increase in reliability.

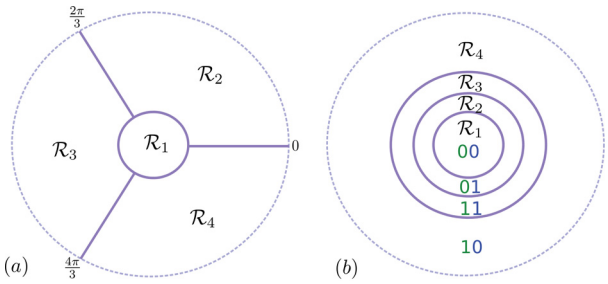

Fig. 5. Two examples of quantization regions; LLR for Fig. 5-a is given by (11), while the LLR for (b) is given by (12), given the shown Gray mapping.

TABLE I
Quantization limits for Example (a)

Region $\mathcal{R}_i$	r_{min_i}	r_{max_i}	θ_{min_i}	θ_{max_i}
$\mathcal{R}_1$	0	$0.758\ \sigma_{ch}$	0	2π
$\mathcal{R}_2$	$0.758\ \sigma_{ch}$	∞	0	$\frac{2\pi}{3}$
$\mathcal{R}_3$	$0.758\ \sigma_{ch}$	∞	$\frac{2\pi}{3}$	$\frac{4\pi}{3}$
$\mathcal{R}_4$	$0.758\ \sigma_{ch}$	∞	$\frac{4\pi}{3}$	2π

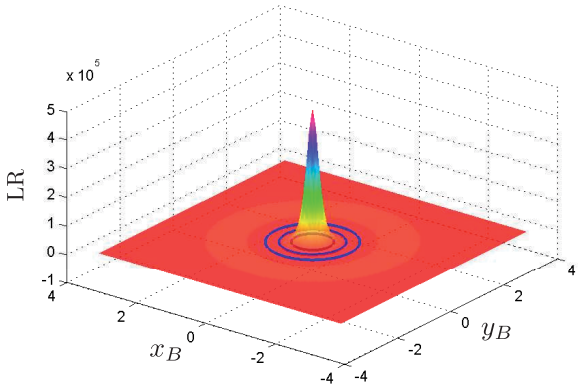

Fig. 6. Likelihood ratio (not logarithmic!) for the first bit

TABLE II
Quantization limits for Example (b)

Region $\mathcal{R}_i$	r_{min_i}	r_{max_i}
$\mathcal{R}_1$	0	$0.758\ \sigma_{ch}$
$\mathcal{R}_2$	$0.758\ \sigma_{ch}$	$1.177\ \sigma_{ch}$
$\mathcal{R}_3$	$1.177\ \sigma_{ch}$	$1.665\ \sigma_{ch}$
$\mathcal{R}_4$	$1.665\ \sigma_{ch}$	∞

ISBN 978-3-8007-3659-1

$$LLR = \ln \frac{p(b|a \in \mathcal{R}_i)}{p(b|a \notin \mathcal{R}_i)} = \ln \frac{P(r_B, \theta_B | a \in (R_i, \Theta_i))}{P(r_B, \theta_B | a \notin (R_i, \Theta_i))} = \ln \frac{(N-1) P(a \in (R_i, \Theta_i) | r_B, \theta_B)}{P(a \notin (R_i, \Theta_i) | r_B, \theta_B)}$$

$$= \ln \frac{(N-1) \int_0^\infty \int_0^{2\pi} \int_{r_{min_i}}^{r_{max_i}} \int_{\theta_{min_i}}^{\theta_{max_i}} p(a \in (R_i, \Theta_i) | r_B, \theta_B) d\theta_A dr_A d\theta_{ch} dr_{ch}}{\sum_{\mathcal{R}_k, k \neq i} \int_0^\infty \int_0^{2\pi} \int_{r_{min_k}}^{r_{max_k}} \int_{\theta_{min_k}}^{\theta_{max_k}} p(a \in (R_k, \Theta_k) | r_B, \theta_B) d\theta_A dr_A d\theta_{ch} dr_{ch}}$$

$$= \ln \frac{(N-1) \int_0^\infty \int_0^{2\pi} \int_{r_{min_i}}^{r_{max_i}} \int_{\theta_{min_i}}^{\theta_{max_i}} r_A r_{ch} e^{-\frac{r_{ch}^2 + r_A^2 - 2 r_{ch} r_A \cos(\theta_{ch} - \theta_A)}{2\sigma_A^2} - \frac{r_{ch}^2 + r_B^2 - 2 r_{ch} r_B \cos(\theta_{ch} - \theta_B)}{2\sigma_B^2} - \frac{r_{ch}^2}{2\sigma_{ch}^2}} d\theta_A dr_A d\theta_{ch} dr_{ch}}{\sum_{\mathcal{R}_k, k \neq i} \int_0^\infty \int_0^{2\pi} \int_{r_{min_k}}^{r_{max_k}} \int_{\theta_{min_k}}^{\theta_{max_k}} r_A r_{ch} e^{-\frac{r_{ch}^2 + r_A^2 - 2 r_{ch} r_A \cos(\theta_{ch} - \theta_A)}{2\sigma_A^2} - \frac{r_{ch}^2 + r_B^2 - 2 r_{ch} r_B \cos(\theta_{ch} - \theta_B)}{2\sigma_B^2} - \frac{r_{ch}^2}{2\sigma_{ch}^2}} d\theta_A dr_A d\theta_{ch} dr_{ch}} \tag{11}$$

$$LLR_{\,first\ bit} = \ln \frac{\int_0^\infty \int_{r_{min_1}}^{r_{max_2}} r_A r_{ch} e^{-\frac{r_{ch}^2 + r_A^2}{2\sigma_A^2} - \frac{r_{ch}^2 + r_B^2}{2\sigma_B^2} - \frac{r_{ch}^2}{2\sigma_{ch}^2}} \cdot J_0(-\frac{r_{ch} r_A}{\sigma_A^2}) \cdot J_0(-\frac{r_{ch} r_B}{\sigma_B^2}) dr_A dr_{ch}}{\int_0^\infty \int_{r_{min_3}}^{r_{max_4}} r_A r_{ch} e^{-\frac{r_{ch}^2 + r_A^2}{2\sigma_A^2} - \frac{r_{ch}^2 + r_B^2}{2\sigma_B^2} - \frac{r_{ch}^2}{2\sigma_{ch}^2}} \cdot J_0(-\frac{r_{ch} r_A}{\sigma_A^2}) \cdot J_0(-\frac{r_{ch} r_B}{\sigma_B^2}) dr_A dr_{ch}} \tag{12}$$

$$LLR_{\,binary} = \ln \frac{\int_{-\infty}^{0} \int_{-\infty}^{+\infty} e^{-\frac{(x_A - x_{ch})^2}{2\sigma_A^2}} \cdot e^{-\frac{(x_{ch} - x_B)^2}{2\sigma_B^2}} \cdot e^{-\frac{x_{ch}^2}{2\sigma_{ch}^2}} dx_{ch}\, dx_A}{\int_{0}^{+\infty} \int_{-\infty}^{+\infty} e^{-\frac{(x_A - x_{ch})^2}{2\sigma_A^2}} \cdot e^{-\frac{(x_{ch} - x_B)^2}{2\sigma_B^2}} \cdot e^{-\frac{x_{ch}^2}{2\sigma_{ch}^2}} dx_{ch}\, dx_A} \tag{13}$$

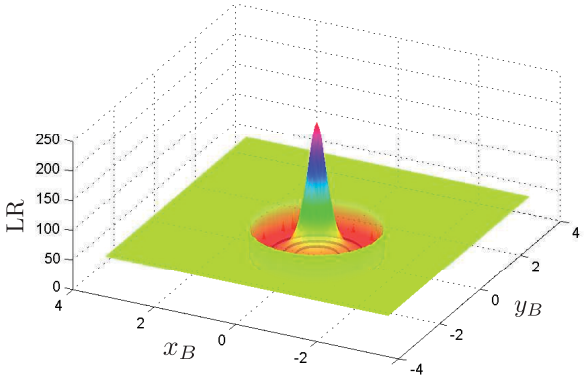

Fig. 7. Likelihood ratio (not logarithmic!) for the second bit

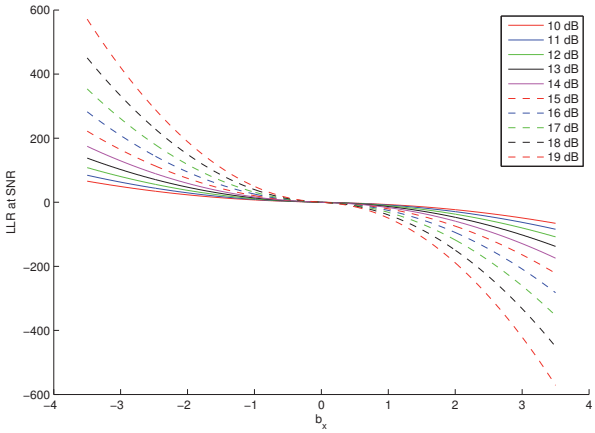

Fig. 9. LLR for different SNR values - binary case

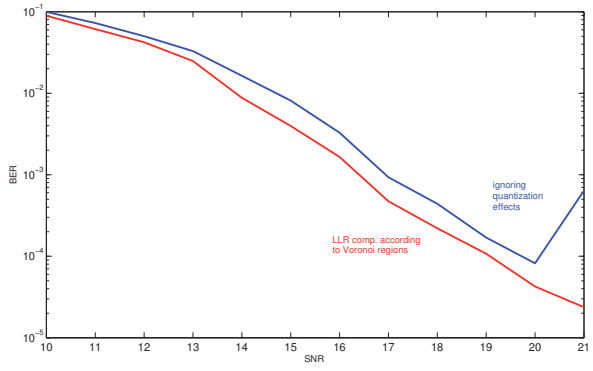

Fig. 8. BER using LLR obtained through noise modeling

VI. Conclusion

In an Alice-Bob wireless scenario, where both sides measure the reciprocal channel with independent noise in order to obtain a shared key, it is of paramount importance to ensure proper key reconciliation. We presented such a method in which we make use of Slepian-Wolf coding and Low Density Parity Check (LDPC) codes. Hence, we derived the LLRs for Slepian-Wolf encoded key reconciliation, found that expressions simplify for concentric quantization regions in the Gaussian case, allowing for reducing the computations to half the number of numerical integrations.

ISBN 978-3-8007-3659-1

ACKNOWLEDGMENT

This work is funded by the German Research Foundation (Deutsche Forschungsgemeinschaft, DFG).

REFERENCES

[1] J. W. Wallace, "Secure Physical Layer Key Generation Schemes: Performance and Information Theoretic Limits.," in *ICC*, pp. 1–5, IEEE, 2009.

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

[3] M. Wilhelm, I. Martinovic, and J. Schmitt, "Secure Key Generation in Sensor Networks Based on Frequency-Selective Channels," *Selected Areas in Communications, IEEE Journal on*, vol. 31, pp. 1779–1790, September 2013.

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

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

[6] C. Ye, A. Reznik, G. Sternberg, and Y. Shah, "On the Secrecy Capabilities of ITU Channels," in *Vehicular Technology Conference, 2007. VTC-2007 Fall. 2007 IEEE 66th*, pp. 2030–2034, Sept 2007.

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

[8] A. Filip, R. Mehmood, J. Wallace, and W. Henkel, "Variable Guard Band Construction to Support Key Reconciliation," in *Acoustics, Speech and Signal Processing (ICASSP), 2014 IEEE International Conference on*, pp. 8173–8177, May 2014.

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

[10] T. Richardson and R. Urbanke, "The Capacity of Low-Density Parity-Check Codes under Message-Passing Decoding," *Information Theory, IEEE Transactions on*, vol. 47, pp. 599–618, Feb 2001.

[11] J. Etesami and W. Henkel, "LDPC Code Construction for Wireless Physical-Layer Key Reconciliation," in *Communications in China (ICCC), 2012 1st IEEE International Conference on*, pp. 208–213, Aug 2012.

