LDPC Code Construction for Wireless Physical-Layer Key Reconciliation

Jalal Etesami and Werner Henkel

Jacobs University Bremen
Transmission Systems Group (TrSyS)
Center for Advanced Systems Engineering
Bremen, Germany
(Jalal Etesami is now with the University of Illinois at Urbana-Champaign)
Emails: etesami2@illinois.edu, w.henkel@jacobs-university.de

***Abstract*— The paper describes a reconciliation procedure for physical key generation based on specially designed LDPC codes using Slepian-Wolf-type coding. The LDPC codes are optimized for intrinsic information with two different noise variances within the same codeword.**

I. Introduction and Motivation

Physical layer security strategies exploit the randomness of wireless channels, which can highly strengthen the security of wireless communications. The approach, we are focusing on, is an information-theoretic one [1], [2], which builds on Shannon's notion of perfect secrecy [3], where the adversary is assumed to have unlimited computational resources and the cipher object is to ensure that absolutely no information is released to the adversary, was laid by Wyner [4] and later by Csiszár and Körner [5], who proved in several papers that there exist channel codes guaranteeing both robustness to transmission errors and data confidentiality.

In this paper, we consider the problem of designing channel codes for sharing and protecting trustful information between the legitimate users based on low density parity check (LDPC) codes. Practically, sharing information is performed via noisy channels which means the receiver has to apply some error-correcting procedures. In the context of secret key generation, this error-correction is called *reconciliation*. For this purpose, the legitimate user needs some additional bits from the transmitter side but in earlier works [6], [7] such additional bits were assumed to be available via a noiseless channel which is not realistic. In here, we design suitable LDPC codes for error-prone channels.

The rest of the paper is organized as follows. In Section II, we introduce the model. In Section III, we study Slepian-Wolf coding, the Lloyd-Max quantizer, and a procedure to calculate a lower bound for the number of necessary additional informations for reconciliation, and the linear programming algorithm for designing adequate LDPC codes and finally, Section IV represents the simulation results.

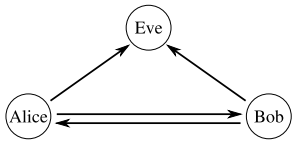

Fig. 1. An example of a wireless network with potential eavesdropping

II. System Model

Consider the secure wireless communication system depicted in Fig. 1. The channels can be regarded as independent for antenna separation distances of more than half a wavelength λ and it is also assumed that both the main channels (Alice-Bob) and the eavesdropper's channels are quasi-static channels, i.e., the fading coefficients are random but constant during the transmission of an entire codeword. To estimate channels, Alice and Bob transmit pilot sequences (for our purposes simplified as known complex value $\underline{t}$), which are known to all parties and are eliminated at the receivers (division). They are solely used to measure the channel characteristic, simplified as complex factors $\underline{H}_m$ and $\underline{H}_e$ for the legitimate and the eavesdropper channel, respectively. The opposite (almost reciprocal) channel from Bob to Alice is measured in the same way, where we assume that the channel, although measured at two different times, has not changed. Bob and Alice receive two slightly different channel estimates

$$\underline{x} = \underline{H}_m + \underline{z}_1 \quad \text{and} \quad \underline{y} = \underline{H}_m + \underline{z}_2 \,, \tag{1}$$

respectively. $\underline{z}_1$ and $\underline{z}_2$ denote the statistically independent noise contributions on both sides (Fig. 2). We assume the complex channel gain H_m, and also $\underline{z}_1$, $\underline{z}_2$ to be zero mean complex Gaussian random variables with variances P, N_1, and N_2, respectively. We simplify $N = N_1 = N_2$. Postulating either Bob or Alice to have obtained the 'correct' $\underline{H}_m$, the other side would then be thought to be facing twice the variance, i.e., $N_v = 2N$. This means, we regard the channel information as linked by a virtual channel with the variance N_v. The key follows from a quantization leading to vectors $\mathbf{x}$, $\mathbf{y}$. Due to the uncorrelated noise on both sides, for *reconciliation*,

978-1-4673-2815-9/12/$31.00 ©2012 IEEE

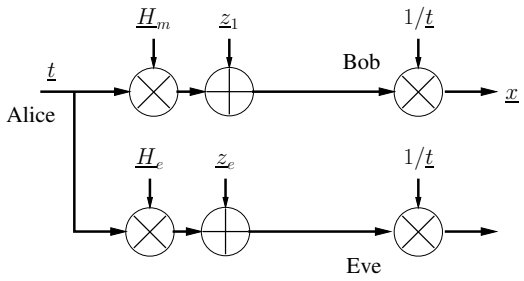

Fig. 2. Wireless channel model

additional protection data needs to be transmitted along the actual physical channel with the variance N.

In order to calculate the number of extra bits for reconciliation, M_p, we need to compute $H(\underline{x}|\underline{y})$, which is given by $\log_2\sqrt{2\pi eN_v}$. Unfortunately, this differential conditional entropy comes with a unit and we can hence not interpret it as the number of extra bits. Fortunately, we anyhow quantize the signal, which solves this issue, too.

A. Lloyd-Max Quantizer

In order to obtain the lowest possible distortion, we apply the Lloyd-Max algorithm [15], which finds an optimum quantization constellation, iteratively. For one dimension, the algorithm is simply described by the following two steps:

1) Finding the ending points by dividing the region between the constellation points equally. For instance, if we assume that c_{i-1}, c_i, and c_{i+1} are three consequent constellation points, then their region will be, $\mathcal{J}_i = [d_{i-1} = \frac{c_{i-1}+c_i}{2}, d_i = \frac{c_i+c_{i+1}}{2}]$.
2) Modifying the constellation points by taking the conditional mean of our random variable, for example X, given that it lies within the region $\mathcal{J}_i$.

$$c_i^m = \mathbb{E}[X|d_{i-1} < X < d_i] = \frac{\int_{\mathcal{J}_i} x f_X(x)dx}{\int_{\mathcal{J}_i} f_X(x)dx} .$$

For simplicity, we applied the one-dimensional algorithm separately for each coordinate (assuming independence).

III. Reconciliation

The reconciliation can be seen as a special case of source coding with side information, *Slepian-Wolf coding*, where, e.g., Alice compresses her source symbols x and sends side information to Bob, then Bob will decode his sequence y with the help of the side information.
Based on the Slepian-Wolf lower bound [8], one can infer the total number of bits, M, which have to be exchanged for reconciliation, is

$$M \geq M_p = H(\mathbf{x}|\mathbf{y}) = nH(x|y) . \quad (2)$$

There are two approaches for implementing Slepian-Wolf coding, the parity and the syndrome approach [9].

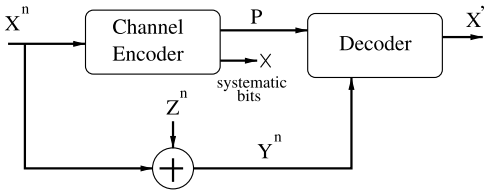

Fig. 3. The parity approach

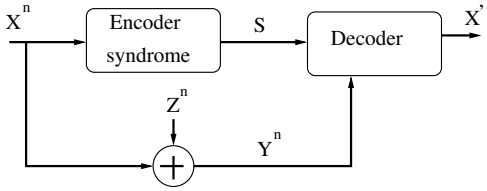

Fig. 4. The syndrome approach

A. Parity Approach

Let $\mathcal{C}(n+m, n)$ be a linear channel code. This method treats the source $\mathbf{x}$ with length n as an information sequence and encodes it systematically into a length $n+m$ codeword $\begin{bmatrix}\mathbf{x}_{n\times 1}\\ \mathbf{p}_{m\times 1}\end{bmatrix}$, then punctures all the systematic bits $\mathbf{x}$.[1] For a linear code, one can write the generator matrix as $\mathbf{G}_{n\times(n+m)} = \begin{bmatrix}\mathbf{I}_n & \mathbf{Q}_{n\times m}\end{bmatrix}^T$. Hence, the resulting parity will be

$$\mathbf{p} = \mathbf{Q}^T\mathbf{x} .$$

B. Syndrome Approach

Let $\mathcal{C}(n,k)$ be a linear channel code. The syndrome approach treats the source $\mathbf{x}$ with length n as a point in the standard array of $\mathcal{C}$. The cosets form syndromes, then each sequence $\mathbf{x}$ is compressed to its syndrome with length $(n-k)$. One may consider an (n,k)-LDPC code with parity check matrix $\mathbf{H}_{(n-k)\times n}$, then the syndrome of $\mathbf{x}$ would be

$$\mathbf{s} = \mathbf{H}\mathbf{x} .$$

C. LDPC Code Design

The main goal here is designing an LDPC code and implementing one of the Slepian-Wolf coding schemes for reconciliation. We know that the shared information between Alice and Bob are transmitted via a noisy virtual channel with the noise power N_v, and the additional bits for reconciliation are transmitted via another channel (the physical one) with the noise power N. We would in principle need two channel codes, one for Slepian-Wolf coding and the other one for protecting additional bits during the actual transmission of the parities or syndrome positions.
Let $\mathcal{C}_m$ be an LDPC code for Slepian-Wolf coding with the generator matrix $\mathbf{G}_m$ and the parity matrix $\mathbf{H}_m$ and $\mathcal{C}_s$ be another LDPC code for additional bits with the generator

[1] All lowercase bold letter denote column vectors, all bold capital letters denote matrices

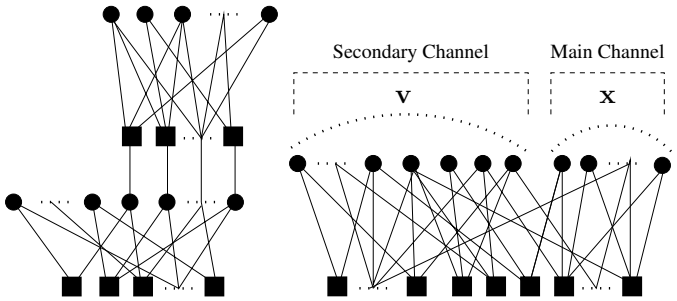

Fig. 5. Left: Tanner graph of the LDPC codes for the syndrome approach, right: equivalent Tanner graph; circles: variable nodes, squares: check nodes

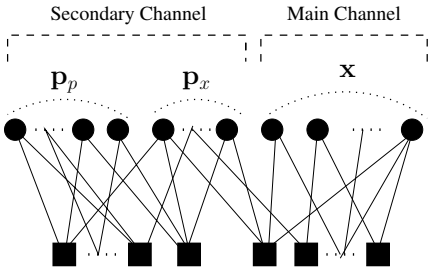

Fig. 6. Tanner graph of the LDPC code for the parity approach

matrix $\mathbf{G}_s$ and the parity matrix $\mathbf{H}_s$. In the following, we will develop the design algorithm for constructing an optimum algorithm for both codes $\mathcal{C}_m$ and $\mathcal{C}_s$.

We implemented the syndrome approach (the parity approach is similar; see Fig. 6). Hereto, we need an (n, k)-LDPC code as $\mathcal{C}_m$ such that the number of syndromes satisfies the Slepian-Wolf bound. Hence,

$$\mathbf{s} = \mathbf{H}_m \mathbf{x} \, . \tag{3}$$

These bits will be the information bits for the secondary code $\mathcal{C}_s$, hence, $k_s = M_p$ and the generated codeword is

$$\mathbf{v} = \mathbf{G}_s^T \mathbf{s} \, . \tag{4}$$

Therefore, by combining (3) and (4), we obtain

$$\mathbf{v} = \mathbf{G}_s^T \mathbf{H}_m \mathbf{x} \, . \tag{5}$$

The above equation tells us, that the whole procedure is equivalently encoding a vector $\mathbf{x}$ by the generator matrix $\mathbf{G} = [\mathbf{I} \;\; \mathbf{H}_m^T \mathbf{G}_s]$ of an LDPC code $\mathcal{C}$, systematically and transmitting the information bits $\mathbf{x}$ through the virtual quantization channel with the noise power N_v and the rest over the channel with the noise power N.

This notion allows us to design one LDPC code with two different subsets of variable nodes, where each of these subsets senses different signal-to-noise ratios. A two edge type LDPC code will be considered, likewise proposed in [11], however, not for a wireless key generation mechanism, but for Wyner's wiretap channel with an actual information leakage to the eavesdropper and addressing binary erasure channels.

Suppose $\lambda(x) = \sum_j \sum_{i \geq 2} \lambda_i^{(j)} x^{i-1}$ and $\rho(x) = \sum_{i \geq 2} \rho_i x^{i-1}$ are the variable and check node degree distributions of the desired LDPC code $\mathcal{C}$, where $\lambda_i^{(j)}$ represents the proportion of edges connected to variable nodes of degree i that belong to the subset j and ρ_i is defined as the proportion of edges connected to check nodes of degree i. This is a description that follows the multi-edge type description of [10]. Hence,

$$\sum_{i \geq 2} \rho_i = \sum_{j=1}^{2} \sum_{i \geq 2} \lambda_i^{(j)} = 1 \, . \tag{6}$$

With n being the length of $\mathbf{x}$, we obtain

$$\sum_{i \geq 2} \frac{\lambda_i^{(1)}}{i} = \frac{n}{E'} \, , \tag{7}$$

where E' is the total number of edges in the Tanner graph. Based on the fact that the number of additional bits must be greater than M_p, we have

$$\sum_{i \geq 2} \frac{\lambda_i^{(2)}}{i} = \frac{M_p}{E'}(1+\beta) \, , \quad \beta \geq 0 \, . \tag{8}$$

Combining (7) and (8), we obtain

$$\sum_{i \geq 2} \frac{\lambda_i^{(2)}}{i} = \frac{M_p}{n}(1+\beta) \sum_{i \geq 2} \frac{\lambda_i^{(1)}}{i} \, , \quad \beta \geq 0 \, . \tag{9}$$

Based on Eq. (8), the number of parity bits $\mathbf{v}$ is $M_p(1+\beta)$, which means the rate of the desired LDPC code $\mathcal{C}$ is

$$R = \frac{n}{n + M_p(1+\beta)} \, . \tag{10}$$

Now, we are seeking for an LDPC code that has the maximum overall rate or equivalently minimum β. This leads us to find a variable degree distribution that satisfies equations (6), (9), the *stability condition*, [12], the *convergence condition*, [13], and also has the maximum overall rate, when the check node degree distribution $\rho(x)$, signal-to-noise ratios of both channels, and the maximum degree of the variable nodes in each class are given. These all lead us to the following optimization problem.

$$\min_{\beta \in \mathbb{R}^+} (1+\beta) \, , \tag{11}$$

subject to

$$\sum_{j=1}^{2} \sum_{i=2}^{d_{max_j}} \lambda_i^{(j)} = 1 \, , \tag{12}$$

$$\frac{M_p}{n}(1+\beta) \sum_{i=2}^{d_{max_1}} \frac{\lambda_i^{(1)}}{i} = \sum_{i=2}^{dc_{max}} \frac{\rho_i}{i} \, , \quad \beta \geq 0 \, , \tag{13}$$

$$\sum_{i=2}^{d_{max_2}} \frac{\lambda_i^{(2)}}{i} = \sum_{i=2}^{dc_{max}} \frac{\rho_i}{i} \, , \tag{14}$$

$$e^{-r} < \frac{1}{\lambda'(0)\rho'(1)} \, , \tag{15}$$

$$\Psi(\boldsymbol{\mu}_0, \lambda, \rho, x_v) > x_v \, , \quad \forall x_v \, . \tag{16}$$

The last equation describes the development (convergence) of the mutual information x_v. Otherwise, d_{max_j} is the maximum

degree of the variable nodes in class j and $\boldsymbol{\mu}_0$ is the vector of the means of the intrinsic channel L-values of the two channels. In our case, we have two different signal-to-noise ratios, hence e^{-r} will be modified as follows [14],

$$e^{-r} = \frac{ne^{-\frac{1}{2N_v}} + M_p(1+\beta)e^{-\frac{1}{2N}}}{n + M_p(1+\beta)} \tag{17}$$

and $\lambda'(0)$ and $\rho'(1)$ are given by

$$\lambda'(0) = \lambda_2^{(1)} + \lambda_2^{(2)} \ , \ \rho'(1) = \sum_{i=2}^{dc_{max}} (i-1)\rho_i \ . \tag{18}$$

D. Slepian-Wolf Bound

Let us represent a signal point in a desired constellation by $\underline{\mathbf{c}}_{ij} = (c_{x_j}, c_{y_i})$, $j \in \{1, ..., t+1\}$ and $i \in \{1, ..., r+1\}$, where $c_{x_j} \in (l_{j-1}, l_j) \subset \mathbb{R}$, $c_{y_i} \in (s_{i-1}, s_i) \subset \mathbb{R}$ and $l_0 = s_0 = -\infty$ and $l_{t+1} = s_{r+1} = \infty$. Then, by the definition of the conditional entropy, we have

$$\begin{aligned} H(\underline{\mathbf{x}}|\underline{\mathbf{y}}) \quad = \quad & -\sum_{\underline{\mathbf{c}}_{ij} \in \mathcal{L}} \int_{\mathbb{R}} f(\underline{\mathbf{x}} = \underline{\mathbf{c}}_{ij}|\underline{\mathbf{y}}) f(\underline{\mathbf{y}}) \\ & \log_2 f(\underline{\mathbf{x}} = \underline{\mathbf{c}}_{ij}|\underline{\mathbf{y}}) d\mathbf{y} \ , \end{aligned}$$

where $\mathcal{L}$ is the set of all points from the constellation and $\underline{x} = (x_1, x_2)$, $\underline{y} = (y_1, y_2)$.
By the independence assumption between the elements or equivalently $f(\underline{\mathbf{y}}) = f(y_1)f(y_2)$, $f(\underline{\mathbf{x}} = \underline{\mathbf{c}}_{ij}|\underline{\mathbf{y}}) = f(x_1 = c_{x_j}|y_1)f(x_2 = c_{y_i}|y_2)$, and after some simplification, one obtains

$$\begin{aligned} H(\underline{\mathbf{x}}|\underline{\mathbf{y}}) \quad = \quad & \sum_{\underline{\mathbf{c}}_{ij} \in \mathcal{L}} \{P(x_1 = c_{x_j}) \mathcal{H}(x_2 = c_{y_i}|y_2) \\ & + P(x_2 = c_{y_i}) \mathcal{H}(x_1 = c_{x_j}|y_1)\} \ , \end{aligned}$$

where $P(x_1 = c_{x_j}) = \int_{l_{j-1}}^{l_j} f(x_1) dx_1$ and

$$\mathcal{H}(x_1 = c_{x_j}|y_1) := -\int_{\mathbb{R}} f(y_1) \left(\int_{l_{j-1}}^{l_j} f(x_1|y_1) dx_1 \right)$$

$$\log_2 \left(\int_{l_{j-1}}^{l_j} f(x_1|y_1) dx_1 \right) dy_1 \ . \tag{19}$$

By combining above equations and since $\sum_{j=1}^{t+1} P(x_1 = c_{x_j}) = \sum_{i=1}^{r+1} P(x_2 = c_{y_i}) = 1$, we obtain

$$H(\underline{\mathbf{x}}|\underline{\mathbf{y}}) = \sum_{i=1}^{r+1} \mathcal{H}(x_2 = c_{y_i}|y_2) + \sum_{j=1}^{t+1} \mathcal{H}(x_1 = c_{x_j}|y_1) \ . \tag{20}$$

Figure 7 illustrates the results of calculating $H(\underline{\mathbf{x}}|\underline{\mathbf{y}})$ for different SNR and different modulation constellations, when $P = 1$ and $N_1 = N_2 = N$, $N_v = 2N$. It shows results with fixed constellations drawn from different QAM pattern and with those optimized by Lloyd-Max (L-M) quantization.

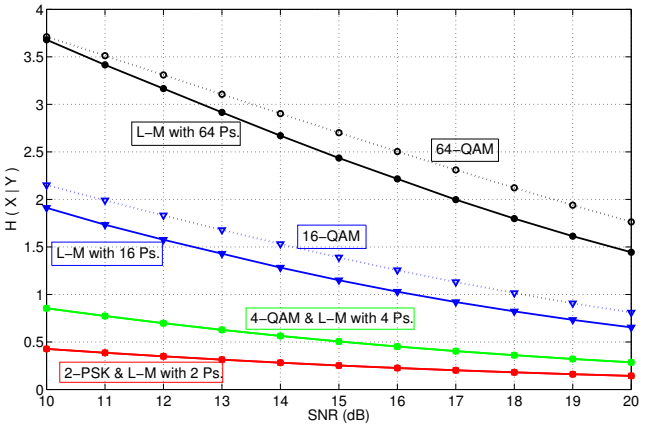

Fig. 7. $H(\mathbf{x}|\mathbf{y})$ for different quantization schemes

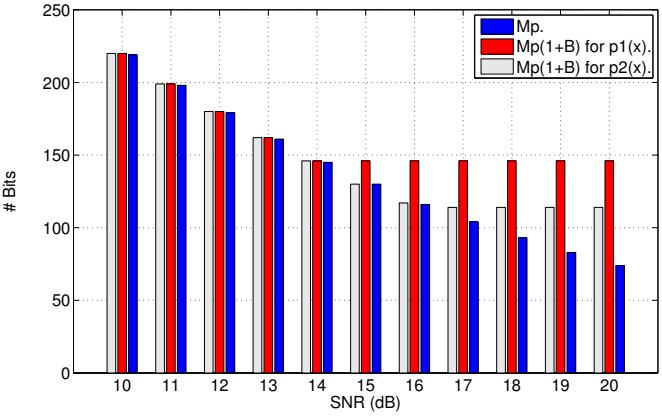

Fig. 8. Blue bars are the number of extra bits (M_p) and red and grey ones are the total number of bits for protecting the main bits ($M_p(1+\beta)$), when $n = 512$ with a BPSK constellation and $\rho_1(x) = 0.98x^8 + 0.02x^9$ and $\rho_2(x) = 0.98x^{10} + 0.02x^{11}$, respectively.

IV. Simulation Results

In this section, we assumed that the number of bits through the main channel is 512 bits, i.e., $n = 2^9$ and the check degree distribution investigated are $\rho_1(x) = 0.98x^8 + 0.02x^9$ and $\rho_2(x) = 0.98x^{10} + 0.02x^{11}$; the SNR is between 10 and 20 dB. In these cases, it is possible to check that the stability condition is always fulfilled for every variable node degree distribution $\lambda(x)$. Hence, one can just discard constraint (15). Figure 8 compares the number of extra bits through the secondary channel, M_p, and the total number of bits through the main and secondary channels, $M_p(1+\beta)$. As one can see from the above figures, at high SNRs, the total number of the parity bits, which we need to protect the bits from the main channel, is constant, representing roughly 21 % and 28 % for the studied check node degree distributions. This flooring can be explained by looking at our optimization problem, where we assumed the check node degree distribution to be given. From the second constraint (13), one can easily obtain a lower

bound for the total number of parity bits,

$$M_p(1+\beta) \geq 2n \sum_{i=2}^{dc_{max}} \frac{\rho_i}{i}\,, \tag{21}$$

which is not related to the SNR.

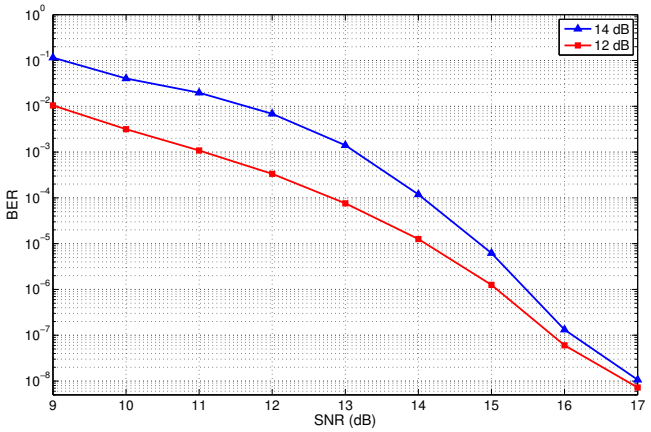

Fig. 9. BER results for $\rho_1(x) = 0.98x^8 + 0.02x^9$, $n = 512$, and BPSK constellation; $\lambda^{(1)}(x) = \sum_{i=2}^{d_{max_1}} \lambda_i^{(1)} x^{i-1} = 0.5976x + 0.0158x^2 + 0.0124x^3 + 0.0105x^4 + 0.0093x^5 + 0.0085x^6 + 0.0079x^7 + 0.0075x^8 + 0.0072x^9 + 0.0069x^{10} + 0.0067x^{11} + 0.0065x^{12} + 0.0064x^{13} + 0.0063x^{14}$, $\lambda^{(2)}(x) = \sum_{i=2}^{d_{max_2}} \lambda_i^{(2)} x^{i-1} = 0.1884x + 0.0151x^2 + 0.0107x^3 + 0.0091x^4 + 0.0081x^5 + 0.0076x^6 + 0.0071x^7 + 0.0068x^8 + 0.0066x^9 + 0.0064x^{10} + 0.0063x^{11} + 0.0061x^{12} + 0.0060x^{13} + 0.0060x^{14}$ (12 dB)[3]

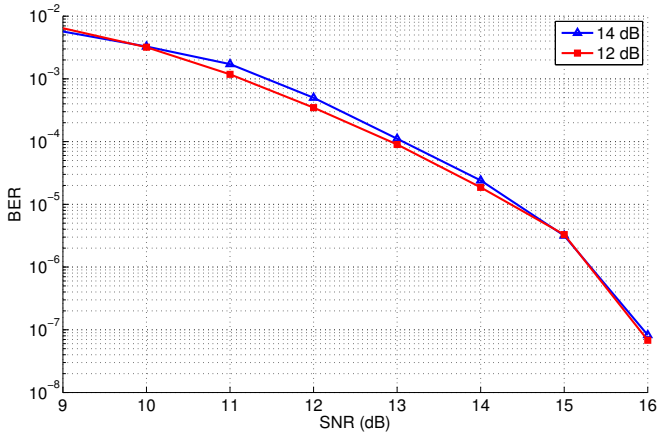

Fig. 10. BER results for $\rho_2(x) = 0.98x^{10} + 0.02x^{11}$, $n = 512$, and BPSK constellation

Figures 9 and 10 show corresponding bit-error ratio results for two different design SNRs of the "virtual" quantization channel[4]. Hereto, we applied the PEG construction algorithm to obtain the actual parity check matrix.

The bits used for reconciliation are, of course, available to Eve, as well. So-called *Privacy Amplification* can be used in this case. From [16] (Corollary 4) can be concluded that at most twice the number of bits are 'lost' for the final key generation from a *universal class of hash functions* leading to an exponentially small information for Eve (for details, see [16], [17]). If we manage to make Eve's information to be i.i.d., this loss can be reduced to the actual number of reconciliation bits.

[3]Other distributions can be obtained from the authors

[4]with twice the variance of the physical channel

V. Conclusions

We presented a study of secure wireless communication based on an information-theoretic security model. Briefly, we studied an LDPC-based reconciliation method and considered a case, when the channel for communicating the extra bits is noisy. For achieving this goal, we proposed an algorithm for designing an LDPC code and we analyzed the performance of these codes, and we proposed a method for calculating the Slepian-Wolf lower bound for the continues case.

We found that roughly 21 % redundancy will be needed in case of simple binary quantization with a higher percentage for higher constellations. Lloyd-Max quantization reduces the required redundancy for higher constellations.

In a follow-up publication, we will present more details for the non-binary case with general two-dimensional vector quantization, and especially also results for the special case when reconfigurable antenna arrays (RECAPs) are used to randomize channels when terminals do not move and would hence otherwise not allow for generating new keys.

Acknowledgment

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

References

[1] J.W. Wallace, "Secure Physical Layer Key Generation Schemes: Performance and Information Theoretic Limits," proc. *IEEE Intl. Conf. Comm.* Dresden, Germany, pp. 1-5, June 14-18, 2009.

[2] 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.

[3] C.E. Shannon, "Communication Theory of Secrecy Systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656-715, 1948.

[4] A.D. Wyner, "The Wire-tap Channel," *Bell Syst. Tech. J.*, vol. 54, no. 8 pp. 1355-1367, Oct. 1975.

[5] I. Csiszár and J. Körner, "Broadcast Channels with Confidential Messages," *IEEE Trans. on Inf. Th.*, vol. IT-24, no. 3, pp. 339-348, May 1978.

[6] 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.

[7] M. Bloch, A. Thangaraj, S.W. McLaughlin, J.-M. Merolla, "LDPC-based Secret Key Agreement over the Gaussian Wiretap Channel," proc. *IEEE ISIT*, Seattle, WA, pp. 1179-1183, July 9-14, 2006

[8] D. Slepian and J.K. Wolf, "Noiseless Coding of Correlated Information Sources," *IEEE Trans. on Inf. Th.*, vol. IT-19, no. 4, pp. 471-480, July 1973.

[9] P. Tan, K. Xie, J. Li, "Slepian-Wolf Coding Using Parity Approach and Syndrome Approach," *41st Annual Conference on Information Sciences and Systems, 2007 (CISS '07)*, pp. 708-713, March 14-16, 2007

[10] T.J. Richardson and R.L. Urbanke, *Modern Coding Theory*, Cambridge University Press, 2008.

[11] V. Rathi, M. Andersson, R. Thobaben, J. Kliewer, M. Skoglund, M., "Two Edge Type LDPC Codes for the Wiretap Channel," proc. *Forty-Third Asilomar Conference on Signals, Systems, and Computers*, pp. 834-838, Nov. 1-4, 2009.

[12] T.J. Richardson, M.A. Shokrollahi, R.L. Urbanke, "Design of Capacity-Approaching Irregular Low-Density Parity-Check Codes," *IEEE Trans. on Inf. Th.*, vol. 47, no. 2, pp. 619-637, Feb. 2001.
[13] A. Ashikhmin, G. Kramer, and S.t. Brink, "Extrinsic Information Transfer Functions: Model and Erasure Channel Properties," *IEEE Trans. on Inf. Th.*, vol. 50, no. 11, pp. 2657-2673, Nov. 2004.
[14] S. Sandberg, N. von Deetzen, "Design of bandwidth-efficient unequal error protection LDPC codes," *IEEE Trans. on Comm.*, vol. 58, no. 3, pp. 802-811, March 2010.
[15] S. Lloyd, "Least squares quantization in PCM," *IEEE Trans. on Inf. Th.*, vol. 28, no. 2, pp. 129- 137, Mar. 1982.
[16] C. Cachin and U.M. Maurer, "Linking Information Reconciliation and Privacy Amplification," *Journal of Cryptology*, vol. 10, no. 2, pp. 97-110, 1997.
[17] C. Cachin, *Entropy Measures and Unconditional Security in Cryptography*, PhD thesis, ETH Zürich, 1997, Hartung-Gorre Verlag, Konstanz, 1997.