Variable Guard Band Construction to Support Key Reconciliation

Alexandra Filip[◇], Rashid Mehmood[†], Jon Wallace[‡], and Werner Henkel

Jacobs University Bremen
Electrical Engineering and Computer Science
Bremen, Germany
Emails: alexandra.filip@dlr.de, r.mehmood@ieee.org, wall@ieee.org, w.henkel@jacobs-university.de

Abstract— **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 a line-of-sight channel and use reconfigurable antenna elements to randomize it, such that it allows for key generation. The Linde-Buzo-Gray algorithm is employed to quantize the complex channel transfer characteristic, and adaptive guard bands, symmetric to the quantization thresholds, are further constructed. To limit the number of key errors, we ensure that only the points that fall outside the guard band interval are accepted for key generation. The steps for constructing the guard bands are presented.**

I. Introduction and Motivation

We consider a type of physical layer key generation requiring the channel to be reciprocal [1]–[6], meaning that both directions of a duplex channel will observe the same channel characteristics in amplitude and phase, assuming a flat fading channel for simplicity. Quantized measurements of the complex channel gain are almost identical at Alice's and Bob's end, only different due to statistically independent noise and resulting differences of the quantization results, ignoring differences in the analog circuitry.

An eavesdropper (Eve) will ideally experience completely different channels to Alice and Bob making it impossible to recover the same key.[1] In case of a mobile environment, the changing channel properties will enable frequent generation of new keys. Under stationary line-of-sight conditions, other measures have to be taken to randomize the channel. Reconfigurable antenna arrays allow for such randomization even achieving almost complex Gaussian properties in case of bigger antenna arrays. In this work, we make use of simulated data for such an antenna array, for space limitations concentrating on the almost Gaussian case, only.

Since the uncorrelated noise on both sides may lead to different keys, a key reconciliation procedure will be essential for the practical use of such physical layer key generation. One possible approach is the use of guard bands instead of quantization thresholds, wherein measured data is discarded. In here, we design such guard bands and study bit-error ratios and efficiencies.

The paper is structured as follows. The next section introduced reconfigurable antennas, followed by a short introduction to vector quantization with the Linde-Buzo-Gray algorithm in Section III. The guard band construction process is introduced in Section IV while the results and their interpretation are discussed in Section V. The paper is concluded in Section VI.

II. RECAP antennas for channel randomization

The term reconfigurable aperture antenna (RECAP) [8] refers to a regular array of reconfigurable elements (REs) confined to a physical aperture. RECAPs can be used in a wide variety of applications, such as beamforming, interference suppression, and channel capacity and security enhancement [9], [10].

In this work, we consider using a parasitic RECAP at one of the communicating nodes (Alice) to generate artificial fading in a stationary line-of-sight (LOS) environment, i.e., it creates a time-variant "mobile" environment also during times, when this cannot be guaranteed by the channel itself. The parasitic RECAP consists of a 5×5 square array of half-wave dipoles confined to an area of $1\lambda \times 1\lambda$ in the xy plane and height of $\lambda/2$ in the z direction as shown in Fig. 1. The center element acts as a feed element while others are parasitic antennas loaded with REs. REs are assumed to consist of variable capacitances, such that the reflection coefficient presented at the k^{th} RE port is $\Gamma_k = \exp(j\alpha_k)$, where α_k is continuously distributed over $[-180°, 0]$. The other node (Bob) is equipped with a single dipole.

A. RECAP Simulation

In order to characterize RECAP channel statistics, we need to simulate thousands of possible RECAP states, which is computationally expensive using full-wave simulation. Instead, a hybrid approach is used, where full wave simulation is combined with network analysis, providing fast as well as accurate simulation results [11].

B. Channel Characterization

In our analysis, we have considered the azimuthal radiation pattern ($\phi = \pi/2$) and a line-of-sight scenario ($\theta = 0$). The

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

[†] R. Mehmood is now with Brigham Young University, UT, USA.

[‡] J. Wallace is now with Wavetronics, Provo, and Brigham Young University, UT, USA.

[1] A man-in-the-middle attack is discussed in [7].

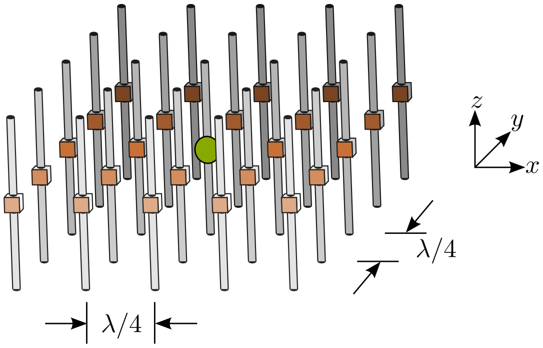

Fig. 1. Perspective view of dipole array RECAP

channel between Bob and Alice can be written as

$$h_{\mathrm{a,raw}} = \mathbf{E}^{\mathrm{mc}}_{\mathrm{RX}}(0,\pi/2)\ \alpha\ \mathbf{E}^{\mathrm{mc}}_{\mathrm{TX}}(0,\pi/2)\ , \tag{1}$$

where α is the path gain, $\mathbf{E}^{\mathrm{mc}}_{\mathrm{RX}}$ is the matched (Z_0-terminated) radiation pattern of Alice's RECAP obtained using the hybrid analysis, and $\mathbf{E}^{\mathrm{mc}}_{\mathrm{TX}}$ is the Bob's matched radiation pattern which is assumed to be constant. Note that the channel $h_{\mathrm{a,raw}}$ does not take the effect of noise into account. Synthetic fading is created by randomly changing the state of each RE in Alice's RECAP, which in return changes $\mathbf{E}^{\mathrm{mc}}_{\mathrm{RX}}$ and $h_{\mathrm{a,raw}}$.

In order to apply quantization schemes, we normalize the channel with respect to its mean power and remove the effect of the complex channel mean, which can be expressed as

$$\mathbf{h}_{\mathrm{a}} = \frac{\mathbf{h}_{\mathrm{a,raw}} - \mathrm{E}\{\mathbf{h}_{\mathrm{a,raw}}\}}{\sqrt{\mathrm{E}|\mathbf{h}_{\mathrm{a}}|^2}}\ , \tag{2}$$

where $\mathrm{E}\{.\}$ denotes expectation, and $\mathbf{h}_{\mathrm{a,raw}}$ and $\mathbf{h}_{\mathrm{a}}$ represent vectors of raw and processed channels between Alice and Bob.

III. Vector Quantization

Having obtained the channel measurement data, the next step is the quantization process. We opted for the Linde-Buzo-Gray (LBG) algorithm [12], a 2-dimensional vector quantizer which represents a sample version of the Lloyd-Max quantizer [13]. One might also go for two scalar quantizers for circularly symmetric distributions as in [14], albeit suboptimum. For very irregular distributions resulting from a small number of REs, this is not an option.

Just as the Lloyd-Max quantizer, the LBG algorithm reduced the Euclidean distortion measure and is centered around two steps, namely a nearest-neighbor step that leads to the Voronoi regions and a centroid step that determines the representative code-book vectors. Hence, to just shortly provide the steps, they are given by

$$S_n = \left\{\mathbf{x}_m : \|\mathbf{x}_m - \mathbf{c}_n\|^2 \leq \|\mathbf{x}_m - \mathbf{c}_{n'}\|^2\ \forall n' \neq n\right\}\ , \tag{3}$$

for the Voronoi regions and the given code-book vectors $\mathbf{c}_n$. The code-book vectors themselves are determined as the average of the data with a Voronoi region (conditional mean)

$$\mathbf{c}_n = \frac{\sum_{\mathbf{x}_m \in S_n} \mathbf{x}_m}{\sum_{\mathbf{x}_m \in S_n} 1} \quad \forall\, n = 1, 2, \cdots, N\ . \tag{4}$$

The vector quantization is described in more detail in [15].

IV. Construction of Guard Bands

As already mentioned previously, the reciprocity of the channel between Alice and Bob allows the two to have access to the same magnitude and phase of the channel. This comes with a great advantage since it ensures that generating keys using vector quantization based on the channel measurements will permit both Alice and Bob to have almost the same key. The only factor that can intervene and lead to slightly different keys on the two sides of the channel is the noise, independent at the two ends. In here, we ignore non-symmetries of the circuitry at Alice and Bob as a further possible source of inconsistencies and possible countermeasures, just as corrections of different non-linearities etc.. Measures that need to be taken to avoid the difference in keys are addressed as key reconciliation techniques.

For this paper, we study the possibility of introducing guard bands instead of just the normal quantization thresholds that delimit the different encoding regions to support key reconciliation. To this end, any point that will end up in the guard band region will not be used for generating keys. We consider variable-width guard bands, such that, at regions with a small probability of occurrence, the guard bands will be narrower than at regions with high probability. For a complex Gaussian channel this strategy would lead to larger guard bands toward the center and narrow ones toward the outside of the distribution.

To obtain the variable guard bands, we first approximate the probability of traversing the guard band of width g as a function of the a-priori probability near the border[2]where $p(x)$ is the channel density. From this equation, we can solve for the width g to obtain

$$P_{\text{trav}} \sim p(x) \cdot \frac{1}{2}\mathrm{erfc}\frac{g}{\sqrt{2}\sigma_n}\ , \tag{5}$$

$$g \sim \sqrt{2}\sigma_n \mathrm{erfc}^{-1}\left[k \cdot \frac{P_{\text{trav}}}{p(x)}\right]\ , \tag{6}$$

where k is a constant which will be modified to obtain different widths. Since k is only a constant, we can incorporate P_{trav} in it and simplify the expression above to find

$$g \sim \sqrt{2}\sigma_n \mathrm{erfc}^{-1}[k/p(x)]\ . \tag{7}$$

This depends on the noise variance and the channel density. One might realize that we ignored the effect of the number of nearest neighbors. The reason for ignoring the effect is similar to error performance curves in general. In the region of interest, they are so steep that a small factor of two to four will not have an effect on the SNR. Here, we also have the erfc function in (5) which has this behavior and hence the influence on the guard band width g is negligible in the range of interest.

For our practical implementation, for the complex channel gain measurements, we used a discretization to a two-dimensional discrete grid from -3.5 to 3.5 in I and Q with

[2] $\sqrt{2}$ results from assuming one side to be noise-free and hence the other to experience twice the variance.

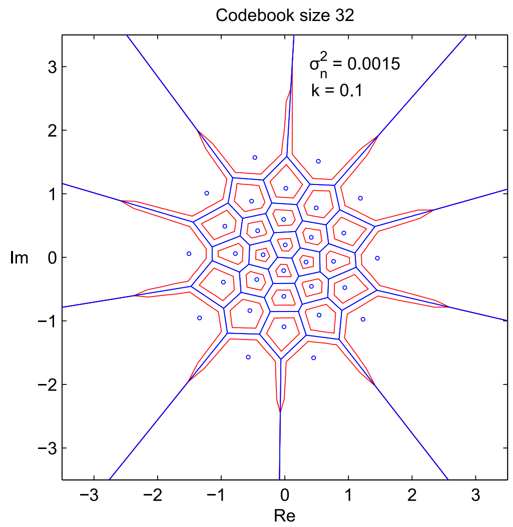

Fig. 2. Guard band construction for codebook size 32, wide bands

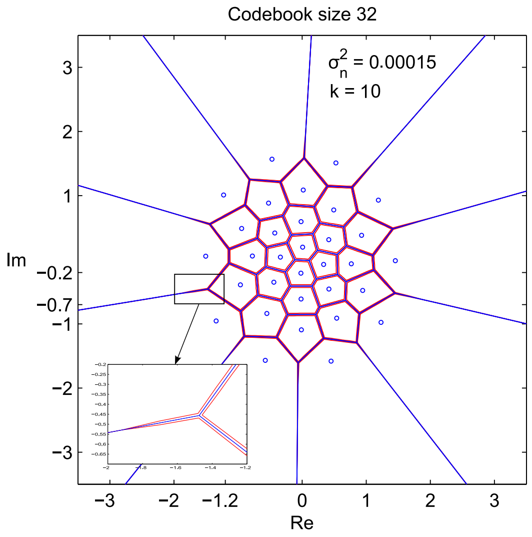

Fig. 3. Guard band construction for codebook size 32, narrow bands

a bin-size of 0.005. We refer to these scales throughout this paper.
For each limiting threshold, we choose 10 equally spaced points at which we computed the guard band widths.

For simplicity, in (7), we used the absolute count within bins for $p(x)$ which is easily possible, since k is chosen accordingly. Hence, the later specified values for k should be regarded in a relative sense, only. Note that a bigger k means a narrower guard band.
For too small values of the count of samples near to the quantization limits, we chose to set the guard band width to zero, which is visible from figures 2 and 3.

V. Results

This section presents the results obtained for the RECAP scenario with one seed and 24 reconfigurable elements, which has been shown in [15] to result in a Gaussian-like channel distribution. Figures 2 and 3 show the result obtained for the guard bands construction for a size 32 codebook[3]. The values for the noise variance and for k are chosen such that two extreme scenarios are depicted: very wide guard bands, covering to a great extent the encoding regions in the center of the distribution, and very narrow guard bands close to the actual Voronoi boundaries.

Intuitively, each encoding region occupies a smaller area and the high probability center regions become to a great extent unusable for very wide guard bands. Moreover, considering that the guard band width is proportional to the standard deviation, the maximum value of allowed noise variance is more limited for larger codebook sizes. However, one should, of course, note, that for bigger codebook sizes N also result in higher number of key bits $\log_2 N$.
We can observe the contraction of the guard band width at low densities of the complex channel gain, which is even nearer to the center of the distribution for higher values of k. This is visible from Fig. 3 [4].

To evaluate the performance for different noise variances as well as for different widths (controlled by k), we performed simulations to obtain the error probability and the efficiency. While the error probability represents the probability to cross the guard band and end up in another quantization region, the efficiency is defined by the probability to obtain valid keys. To determine the error probability, we consider the data points defining our distribution and disturb each one of them by two independent AWGN values with zero-mean and desired noise variance. This allows us to simulate the exact scenarios describing Alice and Bob. The received quantized values are further compared and either accounted for hitting the guard bands, if either one of the received values belongs to the guard band region, or counted for the error probability, if the two received values are different. The efficiency can then be obtained after subtracting the probability to end up in the guard band and the error probability from the maximum probability of 1.

Figures 4 and 5 provide the efficiency and the error probability results for a codebook of size 32, for different noise variances and the allowed range of k for each scenario. As one could already anticipate, higher noise levels together with small k lead to very broad guard bands, finally starting to cover the inner area with high probabilities completely, essentially making some codebook entries disappear. This is, of course, more predominantly the case for larger codebook sizes.

Furthermore, we observe that for constant σ_n^2, decreasing k results in lower efficiency as well as lower probability of error. This is to be understood since, as we decrease k, we increase the guard band width, which ensures on the one hand that there is a lower probability to have a key error and, on the other hand, that as the area covered by guard bands increases, the efficiency decreases. This trade-off can be seen in figures

[3] For space limitations, results for other codebook sizes cannot be included.
[4] One might zoom into the color pdf to recognize it well!

4 and 5; a very high efficiency is achieved at the expense of a very high error probability. A somewhat irregular behavior at low error probabilities in Fig. 5 is due to limiting the number of investigated samples.

Examining the same plots, another important observation can be made. When the value of k is fixed and the noise variance changes, the probability of success changes quite noticeably while the probability of error does not change so much. For example, increasing σ_n^2 results in visibly lower efficiency and slowly increasing error probability. This behavior can be understood when arguing the impact that the guard band width increase has on the two performance indicators. While the efficiently is directly affected by the guard-band width g proportional to σ_n according to (7), the guard bands are constructed to roughly preserve the error probability (P_{trav} in Eq. (6)). However, the simplified derivation only considers areas near to the boundary, which causes a slight dependence on the noise level.

Overall, we realize a significant drop in efficiency when requiring low error rates. Assuming an error rate of 10^{-7}, from Fig. 5, one would obtain a k of around $3 \cdot 10^{-4}$. Picking the $\sigma_n^2 = 5 \cdot 10^{-4}$ curve in Fig. 4 would result in an efficiency of slightly above 0.4. The corresponding SNR is around 33 dB, which is already pretty high.

The error rate can only be reduced or the efficiency increased by choosing smaller codebook sizes (leading to less bits per channel measurement) or, possibly, by moving to Slepian-Wolf type LDPC coding schemes [14], [16], which also requires more redundancy for reconciliation with larger codebook sizes. One should, however, note that the quantization causes adverse channel conditions that are not yet taken into account in [14]. One has to, at least, modify the intrinsic information or better take the quantization effect already into account in the code design.

VI. Conclusions

In this paper, we analyzed the possibility to introduce adaptive guard bands instead of quantization thresholds to support the key reconciliation process. We investigated scenarios with different codebook sizes, for different noise conditions, and width realizations. The evaluation has been done using the efficiency and the error probability as performance indicators. We realized that the efficiency is, of course, reduced for low error rates and bigger codebook sizes. Depending on the actual relation between channel gain measurements and noise/crosstalk environment, one may possibly go for codebook sizes smaller than 32 that was shown as an example in this paper. Another option is available through Slepian-Wolf coding [14] or making use of the Chinese Remainder Theorem [17].

Future works will provide results for guard band concept and Slepian-Wolf coding for RECAP line-of-sight channels with also fewer numbers of reconfigurable elements and therefore different non-Gaussian distributions.

Acknowledgment

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

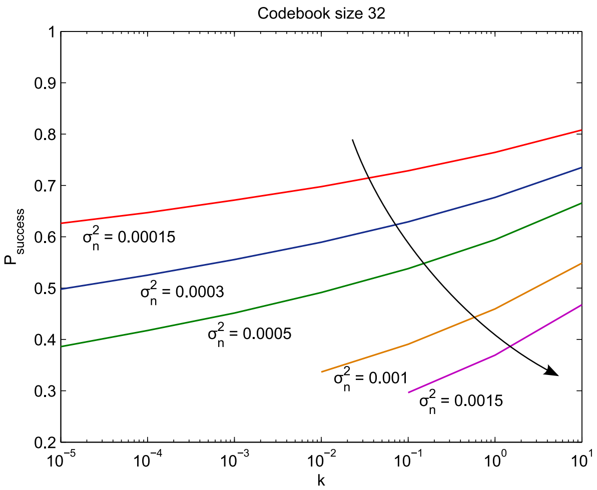

Fig. 4. Efficiency for codebook size 32

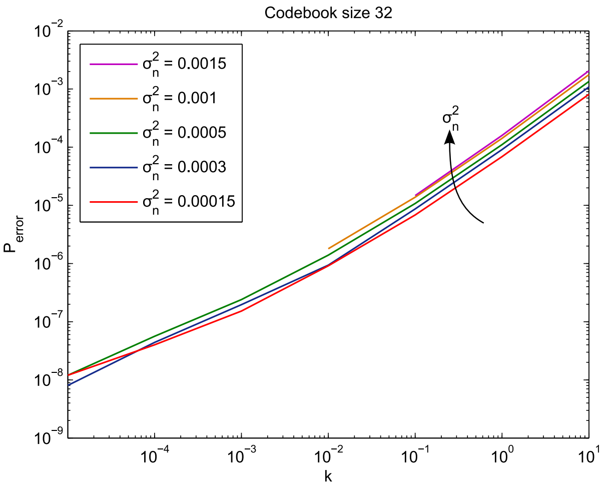

Fig. 5. Error probability for codebook size 32

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] M. Wilhelm, I. Martinovic, and J.B. Schmitt, “Secure key generation in sensor networks based on frequency-selective channels,” *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1779-1790, September 2013.

[4] A. Sayeed and A. Perrig, “Secure wireless communications: Secret keys through multipath,” in *Proc. 2008 IEEE Intl. Conf. Acoustics, Speech, and Signal Processing*, Las Vegas, NV, Mar. 31–Apr. 4, 2008, pp. 3013-3016.

[5] C. Ye, A. Reznik, and Y. Shah, “Extracting secrecy from jointly Gaussian random variables,” in *Proc. 2006 IEEE Intl. Symp. on Information Theory*, Seattle, WA, July 9-14, 2006, pp. 2593-2597.

[6] C. Ye, A. Reznik, G. Sternberg, and Y. Shah, “On the secrecy capabilities of ITU channels,” in *Proc. 2007 IEEE 66th Veh. Technol. Conf.*, Baltimore, MD, Sep. 30-Oct. 3, 2007.

[7] S. Eberz, M. Strohmeier, M. Wilhelm, and I. Martinovic, “A practical man-in-the-middle attack on signal-based key generation protocols,” *Springer Lecture Notes in Computer Science, Computer Security – ESORICS 2012*, pp. 235-252, 2012.

[8] L. Pringle, P. Harms, S. Blalock, G. Kiesel, E. Kuster, P. Friederich, R. Prado, J. Morris, and G. Smith, “A reconfigurable aperture antenna based on switched links between electrically small metallic patches,” *IEEE Trans. Antennas Propag.*, vol. 52, pp. 1434-1445, June 2004.

[9] R. Mehmood and J. Wallace, “Channel security enhancement using reconfigurable aperture antennas,” *European Conference on Antennas and Propagation (EuCAP’11)*, Rome, Italy, Apr. 12-16, 2011, pp. 1-5.

[10] 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 Trans. Antennas Propag.*, vol. 53, pp. 3776-3784, Nov. 2005.

[11] 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.

[12] Y. Linde, A. Buzo, and R. M. Gray, “An algorithml for vector quantizer design,” *IEEE Trans. on Comm.* , vol. com-28, no. 1, pp. 84-95, 1980.

[13] S. Lloyd, “Least squares quantization in PCM,” *IEEE Trans. on Inf. Th.*, vol. 28, no. 2, pp. 129-137, Mar. 1982.

[14] J. Etesami, W. Henkel, and A. Wakeel, “LDPC Code Construction for Wireless Physical-Layer Key Reconciliation,” *First IEEE International Conference on Communications in China (ICCC 12)*, Beijing, China, Aug. 15-18, 2012.

[15] A. Filip, R. Mehmood, J. Wallace, and W. Henkel, “Physical-Layer Key Generation Supported by RECAP Antenna Structures,” *Submitted to SCC*, 2013.

[16] 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.

[17] W. Wang, HY Jiang, XG Xia, PG Mu, and QY Yin, “A wireless secret key generation method based on Chinese remainder theorem in FDD systems,” *Science China Information Sciences*, SP Science China Press, vol. 55, no. 7, pp. 1605-1616, 2012.

[18] http://www.data-compression.com/vq.shtml