Physical-Layer Key Generation Supported by RECAP Antenna Structures

Alexandra Filip, Rashid Mehmood, Jon Wallace, and Werner Henkel

Jacobs University Bremen
Electrical Engineering and Computer Science
Center for Advanced Systems Engineering (CASE)
Bremen, Germany
Emails: a.filip@jacobs-university.de, {r.mehmood, wall, werner.henkel}@ieee.org

Abstract— **Physical-layer key generation makes use of the reciprocity of wireless time-division duplex (TDD) channels. Both transmission directions experience the same channel, apart from independent noise and quantization effects. The randomness of a mobile channel ensures a certain regeneration rate of keys. Reconfigurable antennas, so-called RECAPs, offer a possibility to also provide randomness in the extreme case when both transmitter and receiver are not moving, even have a line-of-sight connection. RECAP structures and the steps for obtaining a reliably identical and secure key on both sides are discussed.**

I. Introduction and Motivation

Physical-layer security follows Shannon's notion of perfect secrecy [1] and essentially discusses Wyner's wiretap channel [2] (Csiszár and Körner [3]), whereas we do not use the concept of secrecy capacity in the sense that the SNR between the legitimate link should be superior to the ones to the adversary. Instead, we use properties of the channel itself to generate keys.

Our physical layer key generation requires the channel to be reciprocal, 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. Channel measurements and subsequent quantization can directly be used for key generation, ensuring that both sides (Alice and Bob) will almost obtain the same key. Almost, since independent noise on both sides together with the quantization will lead to slight differences that will require reconciliation measures or other means as part of the quantization pattern. The number of common key bits is determined by the mutual information

$$\begin{aligned} I_{\mathrm{K}} &= I(\hat{\mathbf{h}}_a;\hat{\mathbf{h}}_{a'}) \\ &= h(\hat{\mathbf{h}}_a)+h(\hat{\mathbf{h}}_{a'})-h(\hat{\mathbf{h}}_a,\hat{\mathbf{h}}_{a'}) \ , \end{aligned} \tag{1}$$

where $\hat{\mathbf{h}}_a$ is the estimated channel between Alice and Bob, $\hat{\mathbf{h}}_{a'}$ the one between Bob and Alice.

An eavesdropper (Eve) will ideally experience completely different channels and hence would be unable to recover the same key. A mobile environment will ensure new keys to be generated frequently. Nevertheless, one may encounter cases with no movement and even with a line-of-sight transmission, possibly even with an eavesdropper in this line-of-sight path. The number of secure key bits is determined by the conditional mutual information [4], [5]

$$I_{\mathrm{SK}} = I(\hat{\mathbf{h}}_a;\hat{\mathbf{h}}_{a'}|\hat{\mathbf{h}}_b,\hat{\mathbf{h}}_c) \ . \tag{2}$$

$\hat{\mathbf{h}}_b$ and $\hat{\mathbf{h}}_c$ denote the channels Alice – Eve and Bob – Eve, respectively. In the line-of-sight stationary situation, a randomization of the channel is required, which may be possible with reconfigurable antennas, so-called RECAPs, which may change its properties in a more or less random fashion, preserving the reciprocity of the duplex channel between Alice and Bob and providing a different channel to the eavesdropper.

The paper is structured as follows. In the next section, we introduce the RECAP concept, followed by some basics on Lloyd-Max quantization (scalar and vector quantization). The achievable statistics for different RECAP constellations together with corresponding quantization results are presented in Section III. A short section on key reconciliation will outline that a finer quantization will result in higher costs for reconciliation. The paper is concluded in Section V.

II. RECAP antennas for randomizing a stationary channel

The term reconfigurable aperture antenna (RECAP) [6] refers to a regular array of reconfigurable elements (REs) confined to a physical aperture, representing a generalization of the reconfigurable antenna concept. RECAPs are advantageous in a wide variety of applications, such as beamforming, interference suppression, frequency agility, and channel capacity enhancement [7], [8].

The idea of using reconfigurable antennas for key generation was first presented in [9]. However, that work only demonstrated proof-of-concept using a single antenna topology. Our work focuses on obtaining a detailed understanding of the channel statistics that are generated using reconfigurable antennas, studying the role of antenna complexity for security, and optimizing channel quantization to approach theoretical limits of key generation [10]. We consider using a RECAP at one of the nodes to generate synthetic fading in a stationary line-of-sight (LOS) scenario. Specifically, we consider the case

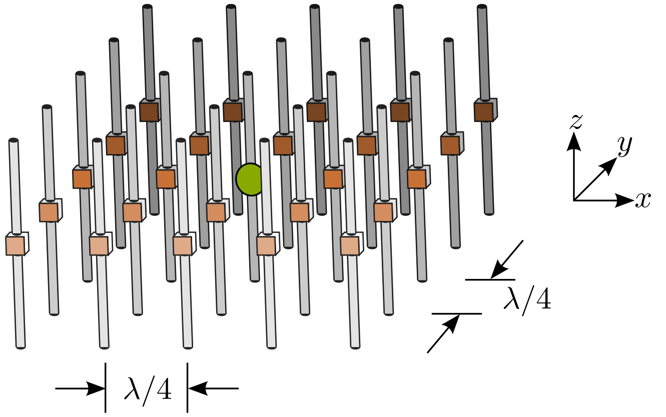

Fig. 1. Perspective view of dipole array RECAP

when Alice has a parasitic RECAP and Bob is equipped with a single dipole.

The parasitic RECAP considered in this work 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 plane as shown in Figure 1. The center element acts as a feed element while others are parasitic antennas loaded with REs. In order to study the effect of variable complexity in terms of the number of reconfigurable elements (N_{RE}), we consider $N_{\mathrm{RE}} = [2, 4, 8, 16, 24]$ as shown in Figure 2. We have assumed REs 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 $[-180°, 0]$.

A. RECAP Simulation

Since many thousand possible RECAP states need to be simulated for the analysis herein, performing a full-wave simulation in order to compute the radiation characteristics of the aperture (radiation pattern and input impedance) corresponding to each configuration is computationally prohibitive. This problem is avoided by following a hybrid approach, where full wave simulation is combined with network analysis, providing fast yet accurate simulation results [11].

For this purpose the structure is analyzed using the Numerical Electromagnetic Code (NEC), in which a unit voltage excitation is applied at the kth port while others are terminated with a short-circuit condition, allowing the short-circuit embedded radiation pattern $e_k^{\mathrm{sc}}(\theta, \phi)$ to be obtained. Also the current flowing at the middle of all other elements is recorded. This procedure is repeated for all the ports in order to compute the admittance matrix $\mathbf{Y}$ and the complete set of short circuit radiation patterns $\mathbf{E}^{\mathrm{sc}}(\theta, \phi)$.

It is more convenient to work in terms of reflection coefficients of the REs than impedances, and for this purpose the admittance matrix and short-circuit patterns are converted to S-parameters and matched (Z_0-terminated) patterns according to

$$\mathbf{S} = (\mathbf{I} + Z_0\mathbf{Y})^{-1}(\mathbf{I} - Z_0\mathbf{Y}) \ , \tag{3}$$

and

$$\mathbf{E}^{\mathrm{mc}}(\theta, \phi) = \frac{\mathbf{E}^{\mathrm{sc}}(\theta, \phi)}{\sqrt{Z_0}}\mathbf{Z}(\mathbf{I} - \mathbf{S}) \ , \tag{4}$$

respectively, where $\mathbf{I}$ is the identity matrix and Z_0 is the normalizing impedance which is assumed to be 72 Ω in our analysis.

Network analysis is employed to compute the radiation pattern and input reflection coefficient of the structure for any arbitrary loading of RE ports according to

$$\underbrace{\begin{bmatrix} b_{\mathrm{F}} \\ \mathbf{b}_{\mathrm{R}} \end{bmatrix}}_{\mathbf{b}} = \underbrace{\begin{bmatrix} S_{\mathrm{FF}} & \mathbf{S}_{\mathrm{FR}} \\ \mathbf{S}_{\mathrm{RF}} & \mathbf{S}_{\mathrm{RR}} \end{bmatrix}}_{\mathbf{S}} \underbrace{\begin{bmatrix} a_{\mathrm{F}} \\ \mathbf{a}_{\mathrm{R}} \end{bmatrix}}_{\mathbf{a}} \ , \tag{5}$$

where a_{F} and b_{F} is the incident and reflected wave on the feed port, respectively, $\mathbf{a}_{\mathrm{R}}$ and $\mathbf{b}_{\mathrm{R}}$ are $N_{\mathrm{R}} \times 1$ vectors corresponding to RE ports, and $\mathbf{S}$ has been partitioned according to feed and REs. Terminating RE ports with loads having reflection matrix $\mathbf{\Gamma}_{\mathrm{R}}$, we have $\mathbf{a}_{\mathrm{R}} = \mathbf{\Gamma}_{\mathrm{R}}\mathbf{b}_{\mathrm{R}}$, where $\mathbf{\Gamma}_{\mathrm{R}}$ is a diagonal matrix with $\Gamma_{\mathrm{R},kk} = \Gamma_{\mathrm{R},k}$. Combined with (5), we have

$$\mathbf{a}_{\mathrm{R}} = \mathbf{\Gamma}_{\mathrm{R}}(\mathbf{I} - \mathbf{S}_{\mathrm{RR}}\mathbf{\Gamma}_{\mathrm{R}})^{-1}\mathbf{S}_{\mathrm{RF}}a_{\mathrm{F}} \ . \tag{6}$$

The radiation pattern of the RECAP with a specific RE termination is computed as

$$\mathbf{E}_{\mathrm{RX}}^{\mathrm{mc}}(\theta, \phi) = \begin{bmatrix} \mathbf{E}_{\mathrm{F}}^{\mathrm{mc}}(\theta, \phi) & \mathbf{E}_{\mathrm{R}}^{\mathrm{mc}}(\theta, \phi) \end{bmatrix} \begin{bmatrix} a_{\mathrm{F}} \\ \mathbf{a}_{\mathrm{R}} \end{bmatrix} \ , \tag{7}$$

where $\mathbf{E}_{\mathrm{F}}^{\mathrm{mc}}(\theta, \phi)$ and $\mathbf{E}_{\mathrm{R}}^{\mathrm{mc}}(\theta, \phi)$ represent the matched patterns corresponding to the feed and the REs, respectively, and $\mathbf{E}_{\mathrm{RX}}^{\mathrm{mc}}(\theta, \phi)$ represents the matched pattern of the feed port with the RE port termination $\mathbf{\Gamma}_{\mathrm{R}}$. The network analysis technique presented here has been tested extensively by comparison with unified full wave simulations and virtually an exact agreement is found for the parameters considered in this paper.

B. Channel Measurement

In our analysis we have considered the azimuthal radiation pattern ($\phi = \pi/2$) only. Furthermore, we are considering only a line-of-sight (LOS) scenario ($\theta = 0$). Hence, the channel between Bob and Alice can be written as

$$h_{\mathrm{a,raw}} = \mathbf{E}_{\mathrm{RX}}^{\mathrm{mc}}(0, \pi/2) \ \alpha \ \mathbf{E}_{\mathrm{TX}}^{\mathrm{mc}}(0, \pi/2) \ , \tag{8}$$

where the path gain α and Bob's radiation pattern $\mathbf{E}_{\mathrm{TX}}^{\mathrm{mc}}$ are 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 each RE in Alice's RECAP to one of N_{RE} different states, which in return changes $\mathbf{E}_{\mathrm{RX}}^{\mathrm{mc}}$ and $h_{\mathrm{a,raw}}$.

In order to compute the histograms of the channel data and apply quantization schemes, we normalize the channel with respect to its mean power and remove the effect of the complex channel mean.

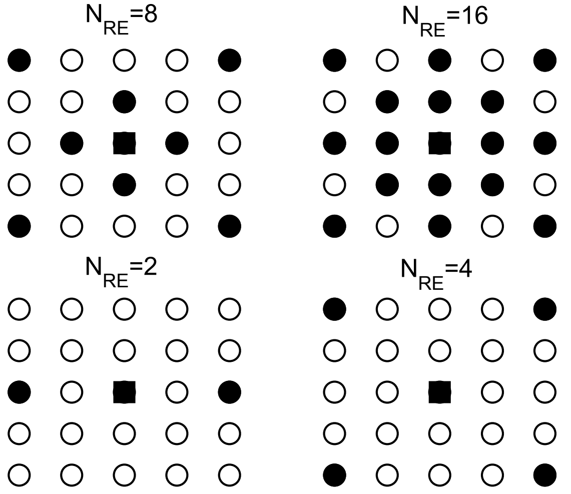

Fig. 2. RECAP structure consisting of a 5×5 dipole array, where N_{RE} elements are terminated with REs (filled circles) and the center element is the feed. Dipoles are aligned along the z axis (extend out of the page).

III. Complex Channel Distributions and Quantization

For the rest of this work we focus on the RECAP line-of-sight reciprocal channel between Alice and Bob. Details regarding the eavesdropper (Eve) will be presented at a later point when introducing the key reconciliation measures. Our main interest is the key generation process which is to be modeled as a vector quantization operation. Furthermore, to correct or limit the number of key differences between Alice and Bob, which can arise as a consequence of independent noise, we introduce possible key reconciliation techniques.

A. Lloyd-Max Quantizer

For quantization, we use a 2-dimensional vector quantizer applying a variant of a 2D Lloyd-Max algorithm [12]. The 1D version is easily described as follows:

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 $\mathcal{J}_i$.

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

Our channel data are available as 2D complex measured values, where we do not even have a density readily available, although for a big number of reconfigurable elements, the central limit theorem will grant us an almost ideal complex Gaussian distribution. In the general case, fitting some model density does not appear feasible. Instead, the alternative of a directly data-driven version of the Lloyd-Max quantizer, the Linde-Buzo-Gray (LBG) algorithm [13], is used. It starts from a single point as the average of all the measured values, which is then split with some spacing, optimizing the two points and corresponding regions followed by more splitting steps. Our description follows [14].

We regard the channel data as a vector random variable in a 2-dimensional space and use the vector quantizer to quantize the real and imaginary parts of the data jointly.

Given a length M sequence of k-dimensional data vectors, $\mathbf{T} = \{\mathbf{x}_1, \mathbf{x}_2, \cdots, \mathbf{x}_M\}$, the desired number of code vectors N, and a distortion measure, the algorithm delivers the final codebook, $\mathbf{C} = \{\mathbf{c}_1, \mathbf{c}_2, \cdots, \mathbf{c}_N\}$ and the encoding (Voronoi) region S_n corresponding to each code vector. A source vector, $\mathbf{x}_m$, is therefore approximated according to its associated region by the corresponding code vector, such that $Q(\mathbf{x}_m) = \mathbf{c}_n$ given that $\mathbf{x}_m \in S_n$. The distortion resulting from approximating $\mathbf{x}_m$ by $Q(\mathbf{x}_m)$ is evaluated using the squared-error distortion. The average distortion formula is

$$D_{\text{a}} = \frac{1}{Mk} \sum_{m=1}^{M} \|\mathbf{x}_m - Q(\mathbf{x}_m)\|^2 , \tag{9}$$

and the final codebook is chosen such that this quantity is minimized. Furthermore, to guarantee an optimum quantization, two conditions have to be met.

1) The nearest neighbor condition ensures that the encoding region S_n, associated with code vector $\mathbf{c}_n$, contains all the source vectors $\mathbf{x}_m$ that are closest to $\mathbf{c}_n$ when compared to all the other code vectors

$$S_n = \left\{\mathbf{x}_m : \|\mathbf{x}_m - \mathbf{c}_n\|^2 \leq \|\mathbf{x}_m - \mathbf{c}_{n'}\|^2 \ \forall n' \neq n\right\} , \tag{10}$$

2) The centroid condition requires that the code vectors are updated such that they represent the average of all the data vectors included in the associated region

$$\mathbf{c}_n = \frac{\sum_{\mathbf{x}_m \in S_n} \mathbf{x}_m}{\sum_{\mathbf{x}_m \in S_n} 1} \ \forall n = 1, 2, \cdots, N . \tag{11}$$

The iterative LBG algorithm solves the two conditions in an alternating fashion. The first code vector is chosen to be the average of the available channel data and the first codebook is obtained by splitting this code vector into two other code vectors given an initial measure ϵ. Next, the vector quantization design algorithm is presented.

1) $\mathbf{T}$, k and $\epsilon > 0$ are given and fixed.
2) Start with one initial code vector, $N = 1$, and compute

$$\mathbf{c}_1^* = \frac{1}{M} \sum_{m=1}^{M} \mathbf{x}_m \text{ and } D_a^* = \frac{1}{Mk} \sum_{m=1}^{M} \|\mathbf{x}_m - \mathbf{c}_1^*\|^2 . \tag{12}$$

3) For $l = 1, 2, \cdots, N$ split $\mathbf{c}_l^*$ to obtain

$$\mathbf{c}_l^{(0)} = (1+\epsilon)\mathbf{c}_l^* \text{ and } \mathbf{c}_{N+l}^{(0)} = (1-\epsilon)\mathbf{c}_l^* , \tag{13}$$

and update number of current code vectors to $N = 2N$.

4) Set iteration index $i = 0$ and initialize $D_a^{(0)} = D_a^*$.
   a) For each $m = 1, 2, \cdots, M$, find minimum value of $\left\|\mathbf{x}_m - \mathbf{c}_n^{(i)}\right\|^2$ among all $n = 1, 2, \cdots, N$. Set

index of closest code vector to n^* and

$$Q(\mathbf{x}_m) = \mathbf{c}_{n^*}^{(i)} \; . \tag{14}$$

b) Update code vectors

$$\mathbf{c}_n^{(i+1)} = \frac{\sum_{Q(\mathbf{x}_m)=\mathbf{c}_n^{(i)}} \mathbf{x}_m}{\sum_{Q(\mathbf{x}_m)=\mathbf{c}_n^{(i)}} 1} \; . \tag{15}$$

c) Update iteration index $i = i + 1$ and compute

$$D_{\mathrm{a}}^{(i)} = \frac{1}{Mk} \sum_{m=1}^{M} \left\| \mathbf{x}_m - Q(\mathbf{x}_m) \right\|^2 \; . \tag{16}$$

d) If $(D_a^{(i-1)} - D_a^{(i)})/D_a^{(i-1)} > \epsilon$ further optimize code vectors, go back to Step 4a.

e) Set $D_a^* = D_a^{(i)}$ and final code vectors $\mathbf{c}_n^* = \mathbf{c}_n^{(i)}$.

5) If number of code vectors needed is greater than current N, repeat steps 3 and 4.

B. RECAP Channel Statistics and Quantization Results

Figure 3 shows results obtained from a simulated antenna configuration with one feed and 2, 4, and 24 reconfigurable additional antenna elements according to Fig. 2. In the simulation, the capacitive coupling is assumed to provide equally distributed angles in the lower half-plane of the S-domain (purely capacitive). We opted for the simulation instead of also available hardware, since the amount of data required for statistics would have required a very long measurement campaign.

The line-of-sight path was selected to face the middle of the wide side / side of the square.

Figure 3 outlines very non-symmetric, non-Gaussian histograms for 2 and 4 reconfigurable antennas and a nicely Gaussian-like symmetric shape with 24 such elements. On the right, we show obtained quantization results for 16 and 32 points. The Gaussian circularly symmetric case, of course, leads to more regular codebook point locations with densities decreasing to the outside.

IV. Key reconciliation

Due to statistically independent noise at both sides of the legitimate channel, i.e., at Bob's and Alice's location, one has to expect differences in the keys if no further measures are taken. One possibility is to introduce guard bands instead of the given Voronoi cell boundaries. These guard bands can be made narrower at places of lower occurrence probability, e.g., in the case of the complex Gaussian channel, for the bigger outside regions, the guard band could be narrower than at the center. Without a modification of the vector quantizer, the inner points will become less useful. To a large extent, their regions will be covered by guard bands not generating keys, even more so, since the guard bands should be larger at higher densities, i.e., in the center. This means the number of key bits will be limited by the noise, i.e., by necessary guard measures for key matching.

Another option is to use Slepian-Wolf joint source coding [15], which is source coding with side information. One of the legitimate users compresses his/her key information $\mathbf{x}$ and sends side information to the other side, where he/she decodes the key information $\mathbf{y}$ with the help of that side information.

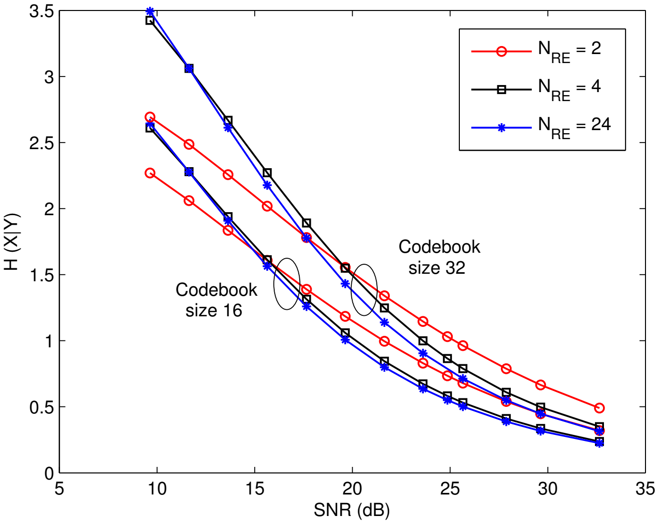

Fig. 4. $H(\mathbf{x}|\mathbf{y})$ for RECAP LOS channels with different number of REs and different codebook sizes

The number of bits that have to be transmitted for key reconciliation is given by the Slepian-Wolf lower bound [16],

$$M \geq M_p = H(\mathbf{x}|\mathbf{y}) = nH(x|y) \; . \tag{17}$$

Figure 4 shows the conditional entropy between the channel estimates of Alice and Bob dependent on the signal-to-noise ratio, the number of reconfigurable elements, and the codebook size. From (17) it can be seen that the conditional entropy represents an indicator for the required number of reconciliation bits. As with guard intervals, also here, it becomes obvious that higher alphabets require more effort in reconciliation. Moreover, for a fixed codebook size, we can observe that while high values of SNR require more reconciliation bits for channels with a small number of reconfigurable elements, this trend does not apply for small SNR values. In the latter case, channels with fewer reconfigurable elements require in fact less redundancy and, in addition, higher alphabets are characterized by bigger differences between channels with different numbers of REs.

Furthermore, to ensure that Eve gets only an exponentially small part of the parities, *Privacy Amplification* can be applied. For this purpose, it has been shown in [17] (Corollary 4) that at most twice the number of reconciliation bits are needed for the final key generation.

There are two Slepian-Wolf coding methods [18] that can be used.

The **parity approach** treats the source $\mathbf{x}$ with length k as an information sequence and encodes it systematically into a length n codeword then punctures all systematic information.

The **syndrome approach** treats the source $\mathbf{x}$ with length[1] n as a point in the standard array of a linear code. The cosets

[1] intentionally renamed!

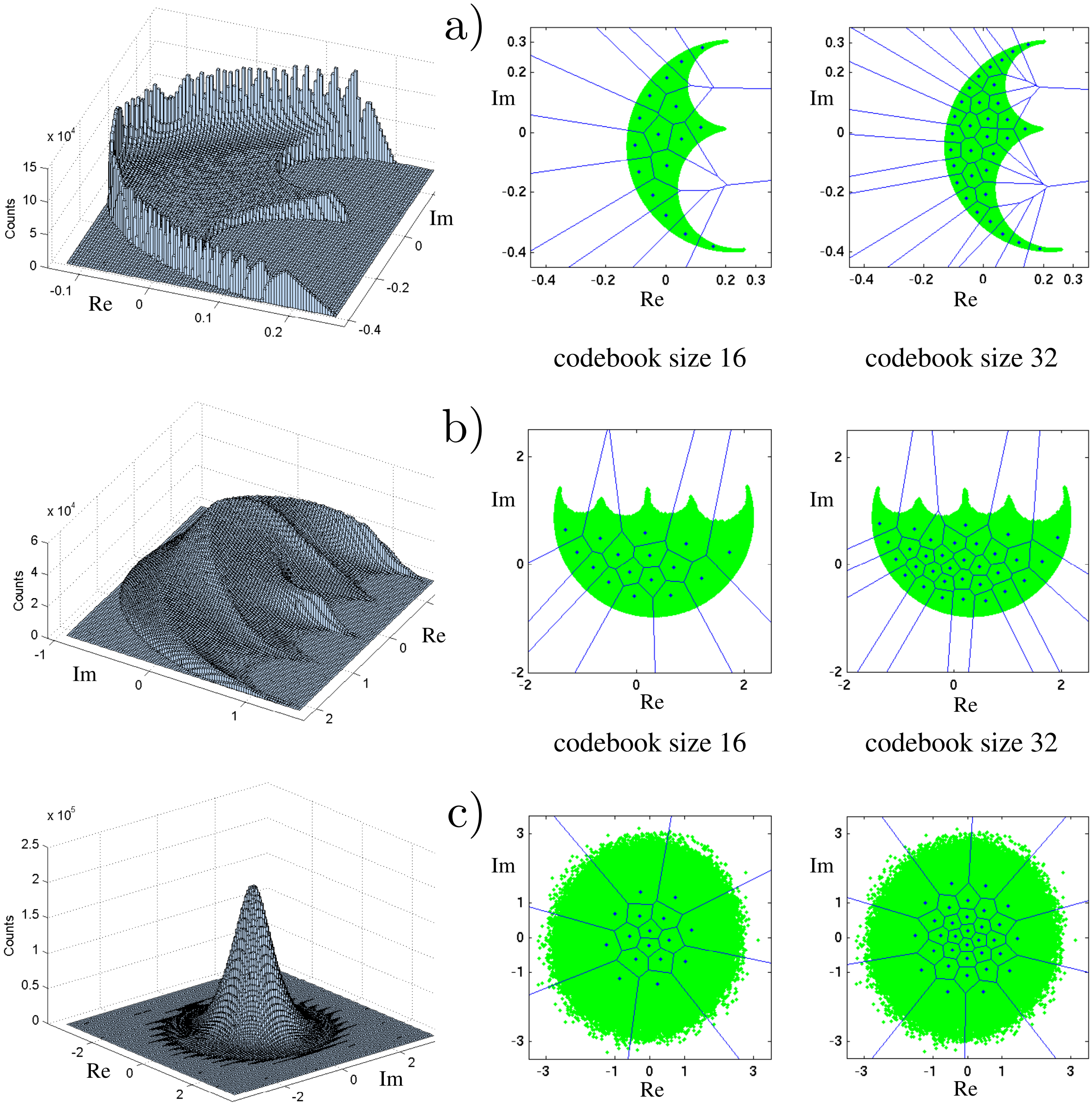

Fig. 3. Statistics and exemplary quantization results for RECAP line-of-sight channels with one seed and 2, 4, and 24 (a, b, and c, respectively) reconfigurable antenna elements with equally distributed random states (The histograms are shown based on 10^8 values, whereas only 10^7 were used to obtain the quantization results. ϵ was chosen to be 0.001.)

form syndromes, then each sequence **x** is compressed to its syndrome of length $(n-k)$.

For Slepian-Wolf coding, one should note that the redundancy is transmitted over a real physical channel, whereas the key estimates **x** and **y** are resulting from a virtual channel. When assuming that either **x** or **y** represent the 'correct' key, the other would then experience twice the noise variance in case of an i.i.d. physical channel (e.g. AWGN).

V. Conclusions

RECAP antenna structures were shown to be usable to randomize a channel for physical-layer key generation, which would otherwise be unsecure, since a regeneration of keys would be dependent on a channel change, i.e., a mobile environment. We investigated the distributions that can be obtained in extreme line-of-sight scenarios and corresponding quantization patterns usable for key generation. Further work will adapt guard intervals and LDPC codes to the given scenarios.

Acknowledgment

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

References

[1] C.E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656-715, 1948.

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

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] R. Mehmood and J. Wallace, "Diminishing returns with increasing complexity in reconfigurable aperture antennas," *IEEE Antennas Wireless Propag. Lett.*, pp. 299-302, 2010.

[9] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *IEEE Transactions on Antennas and Propagation*, vol. 53, pp. 3776-3784, Nov. 2005.

[10] 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.

[11] J. Wallace and R. Mehmood, "On the accuracy of equivalent circuit models for multi-antenna systems," *IEEE Transactions on Antennas and Propagation*, vol. 60, pp. 540-547, Feb. 2012.

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

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

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

[15] 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.

[16] 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.

[17] C. Cachin and U.M. Maurer, "Linking information reconciliation and privacy amplification," *Journal of Cryptology*, vol. 10, no. 2, pp. 97-110, 1997.

[18] J. Etesami and W. Henkel, "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.