A Simple Physical-Layer Key Generation Scheme for Power-Line Transmission

1st Werner Henkel, *senior member, IEEE*
Electrical Engineering
Jacobs University Bremen
Bremen, Germany
werner.henkel@ieee.org

2nd Ha Young Kim
Electrical Engineering
Jacobs University Bremen
Bremen, Germany
hkim@jacobs-alumni.de

3rd Abderraheem M. Turjman
Hochschule Bremen
now with Müller Engineering, Berlin

4th Mathias Bode
Electrical Engineering
Jacobs University Bremen
Bremen, Germany
m.bode@jacobs-university.de

***Abstract*—We have already shown in earlier publications that reciprocity of power-line channels, expressed by, e.g., $S_{12} = S_{21}$ using scattering parameters, can provide the desired common randomness for physical layer key generation. We had used minima or maxima of those transfer S-parameters to select possible keys. The tree-like power-line topology with bridge taps that are imperfectly terminated, possibly just left open, provide the means to create deep notches and, of course, local maxima in between. Using those positions, however, does not work well under noise conditions and power-line channels are known for their stationary and non-stationary disturbances. Minima will just be filled by noise, maxima that are wider than the minima experience a ripple thereby making it difficult to obtain identical positions under uncorrelated noise at the legitimate users' ends. To solve this issue, in here, we propose to instead use the amplitude values at maxima positions. Disturbances there are directly related to the noise amplitudes. High maxima and corresponding key sequences resulting from amplitude quantization of the transfer characteristic are then less error-prone. Further improvements to reduce noise effects are obvious, just like averaging measurements, smoothing over frequency, or just only accepting measurements above certain thresholds.**
Quantization of amplitudes is carried out in log domain and mapping to bit patterns is realized in a cyclic fashion together with Gray coding. Key reconciliation is realized by shifting measurements into the middle of quantization intervals.

***Index Terms*—Physical-layer security, physical-layer key generation, power-line communication, key reconciliation**

I. Introduction

There are two totally different approaches to make use of physical channel properties for security applications. One builds on SNR advantages, i.e., channel capacity advantages between legitimate users and to eavesdroppers. This was once introduced by Wyner in [1]. Our application, however, is physical-layer key generation making use of channel symmetries and random changes. Channel symmetries, i.e., channel reciprocity, is a standard property already of passive two-ports, expressed, e.g., as det(**A**) = 1, with an ABCD matrix **A**. This is equivalently described by $S_{12} = S_{21}$ using scattering parameters that are more commonly used in radio-frequency engineering. There, the counterpart of the ABCD matrix is the so-called T-matrix, which has the same property, namely det(**T**) = 1. We are making use of S-parameters, where S_{12} and S_{21} describe the transmission from point 2 to 1 and 1 to 2, respectively.

Wireless time-division duplexing was known for its reciprocity since long and there only the coherence time has to exceed the ping-pong channel measurement duration and the reciprocity is obvious since the channel is characterized by waves traveling between reflection points or directly, where rays combine at an antenna. Since the attenuation and reflection properties do not depend on the direction of transmission, very naturally, the transfer function between Alice and Bob is the same as from Bob to Alice to make use of the standard naming convention of the two legitimate users. This property is, of course, fully in line with $\mathbf{S}_{12}$ being equal to $\mathbf{S}_{21}$, which is easily visible when the two-directional measurements are displayed on a vector network analyzer.

An eavesdropper Eve that is located more than 6 wavelengths away from one of the legitimate users experiences completely uncorrelated channel properties and hence, when quantizing the channels in one or the other way, the key results of the pairings Alice-Eve or Bob-Eve lead to unrelated key sequences to the legitimate one, Alice-Bob.

In the power-line case, an eavesdropper could be located at another socket and our earlier investigations in [2]–[4] show that just like in the wireless case, the eavesdropper should be located sufficiently apart from Alice or Bob to experience different notch locations. Distances of a bit more than 1 meter were found to be sufficient. Since in here, we will not use the frequency location of notches or maxima any more, the protection towards Eve is considered to be even stronger.

What needs to be discussed as well is that the channel is required to change randomly, still, of course, preserving the reciprocity, but this is ensured, anyhow. In wireless, this

Funded by the Deutsche Forschungsgemeinschaft (DFG – German Research Foundation) - HE 3654/27-1

change is realized by mobility of a terminal, where for realization of the TDD ping-pong measurements, the channel should not change much, but to the next measurements it should change significantly. This means, mobility has some constraints. Other options in wireless are reconfigurable antennas or reconfigurable intelligent surfaces.

In the power-line situation, however, mobility is not possible. The cable connections to appliances and sockets are, of course, fixed. Appliances themselves can change, by, e.g., turning them on or off. In here, we use random reactive (lossless) loads at one branch end in the vicinity of Alice or Bob. This was also seen as an effective possibility in practical measurements. There is another possibility, which we have also already studied practically. This is terminating an unused pair with random reactive loads. When using the L-N pair for transmission and key generation, e.g., N-PE would be available for such random terminations. In this paper, we study the first option by simulations to obtain a suitable number of measurements to do statistics. The other termination option will be later studied in more detail, too, but the effects are determined by non-ideal cable properties that are not well represented in a simulation program where cables are considered to be homogeneous. Coupling properties between wire-pairs inside the same cable depend on the production process and, in the power-line case, a lot on the layout of the cables on or inside walls and, of course, the distribution points will play a crucial role, too. Hence, we are well aware that a simulation program cannot easily forecast the behavior here and, at best, can give some impression under idealizing assumptions, where the reality will provide even better conditions, especially, also as far as eavesdropping is concerned.

Further steps in physical-layer key generation are, of course, quantization, key reconciliation, leveling of the key probability distribution, and finally, privacy amplification by some source coding/hashing. We will describe a simple quantization and key reconciliation scheme, where the latter should bring the key-disagreement rate (KDR) into a range from which coding schemes could effectively be used. The KDR R_{KDR} is defined as

$$R_{\mathrm{KDR}} = \frac{1}{N_k} \sum_{i=1}^{N_k} K_A(i) \oplus K_B(i) \qquad (1)$$

where K_A and K_B denote Alice's and Bob's key bits, respectively, and N_k denotes the total number of collected key bits. A typical coding scheme for key reconciliation is, e.g., Slepian-Wolf coding as described in [5]. Depending on the signal probability distribution and the chosen quantization, the key sequences will not necessarily be equally distributed, which is a requirement for a suitable key sequence. One may adjust the quantization regions accordingly or apply arithmetic encoding to achieve equally distributed key symbols without statistical bindings. When applying Slepian-Wolf coding schemes, parity or syndrome information has to be communicated over the public channel. A proper hashing has to be applied which reduces the number of usable key bits by the amount of transmitted parity / syndrome bits. Also, any other possible key leakage has to be counteracted by privacy amplification [6].

In the following section, we will describe the simulation setup followed by the procedures for quantization, a first step for key reconciliation, and the labeling to key sequence segments outlined in Section III. Simulation results will be shown in Section IV, and Section V concludes the paper.

II. Simulation Setup

To be able to do statistics, we had to refrain to simulations of the power-line network. We used a simulation package once set up by Gruber and Lampe[1] [7], [8]. The simulation package allows to determine transfer functions from per-unit length parameters derived from a numerical solver. We idealized assuming $S_{12} = S_{21}$ in the noise-free case to be equal to the computed transfer function. The package allows multi-pair arrangements and in a tree-like configuration, a carry back of terminations to branch points allows to determine the overall source-sink behavior. We will not give details here and refer the reader to Gruber and Lampe's original works or a short summary in [4]. We may however mention that we had to modify the relative permittivity ϵ_r to 1.5, which should ideally be 4 for PVC. Otherwise, the characteristic impedance of the cable would not have matched the actual measured one. This is explained by the fact that the cable is not tightly filled and the insulators are also foamed, not consisting of rigid pure PVC.

We selected a small 6-node network with the legitimate user ends Alice and Bob plus additional end points BE1-BE4 as shown in Fig. 1. BP labels the branch points, BE the end end points, numbers at edges specify the length in meters. BE2-BE4 were terminated randomly with appliances such as PC, fridge, coffeemaker, and vacuum cleaner, where we took their properties from [9] extended by socket connections with short cables that we had measured ourselves.

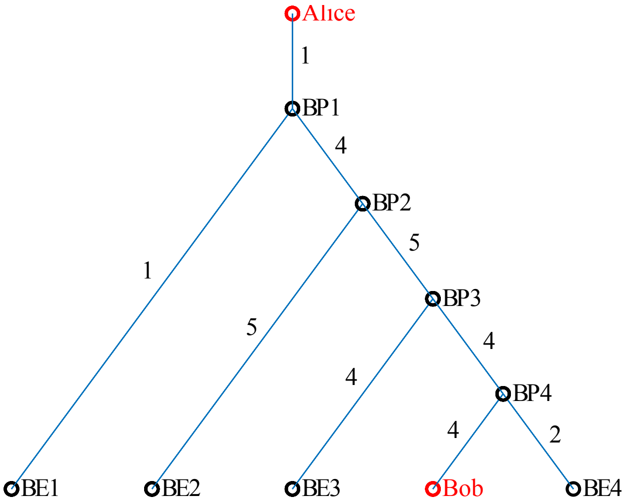

Fig. 1. Tree structure of an exemplary power-line segment network

[1] We gratefully acknowledge the support by Lutz Lampe at UBC

BE1 at a distance of only 2 m from Alice was used to place random reactive loads, i.e., capacitances and inductances with values from 1 pF to 50 pF and 1 nH to 1 μH, respectively. The latter, we chose in a log-scale fashion to bridge the larger range. Those value ranges were chosen to be practically realizable and also lead to a corresponding amplitude spread to ensure a suitable variation of the resulting quantization outcomes.

III. Quantization, Key Reconciliation, and Labeling

To improve noise tolerance, we are only considering the global maximum position, which depends on the chosen reactive load. We scanned the range of those loads and determined the global maxima of all, which we denote as f_{allmax}. One may for the actual key generation, only consider maxima in a range around f_{allmax}, e.g., $[f_{\text{allmax}} - \frac{c}{2l_{\text{typ}}}, f_{\text{allmax}} + \frac{c}{2l_{\text{typ}}}]$. c is the speed of light and l_{typ} a typical length of the powerline cable arrangement. This is to limit the search to around the interesting area where the reactive load changes the local behavior. For this paper, we used global maxima over the complete measurement range.

We decided for quantizing the log-scale of the transmission coefficients, i.e., in dB scale, where so far, we linearly quantize in arbitrarily choosable steps. This can simply be realized by, e.g., a floor function after proper scaling, leading to integers as a label for the quantization intervals. For mapping those intervals to bit patterns, we number them in a modular fashion, i.e., for a certain number of bits n, we periodically label them with 0 to $2^n - 1$. This is realized as the remainder of a modulo division. The resulting label is then mapped to a bit pattern according to Gray mapping. This ensures to only have a one bit mismatch, if uncorrelated noise would lead to different but neighboring quantization intervals for both directions.

A first step of key reconciliation can be realized by translating one of the maxima measurements, e.g., of S_{12} to the middle of the quantization interval. This minimizes the key disagreement ratio, which is defined as the ratio of the number of different key bits relative to all generated ones. When moving values to the middle of the interval, the values resulting from the opposite direction, i.e., S_{21}, would be close to that value and the chance to cross the quantization threshold would be minimized.

The advantage of this translation method is that the translation can be publicly communicated without jeopardizing secrecy at all. Additionally, it does not reduce the key generation rate, i.e., the rate of usable key bits. Other simple approaches like introducing guard bands at quantization thresholds would reduce the key generation rate according to the share of guard bands.

Figures 2 to 5 illustrate the procedure, where the centering of quantization results are shown in Fig. 2 and zoomed-in as Fig. 4. What is visible is that the chosen range of inductances leads to less variability than for capacitance terminations.

The described translation procedure is considered as a first step of key reconciliation, only. It will, as we can recognize from our simulation results in the following section, not yet achieve desired very low key disagreement ratios. However, it brings it into a range that is a good starting point for Slepian-Wolf coding (see the options in Fig. 6) to finally match keys with a high probability.

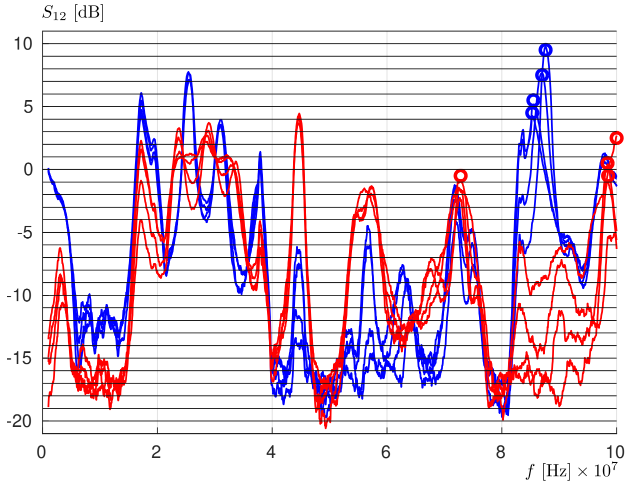

Fig. 2. Quantization intervals shown with S_{12} including centering of quantization results shown as circles; blue: capacitive terminations, red: inductive terminations

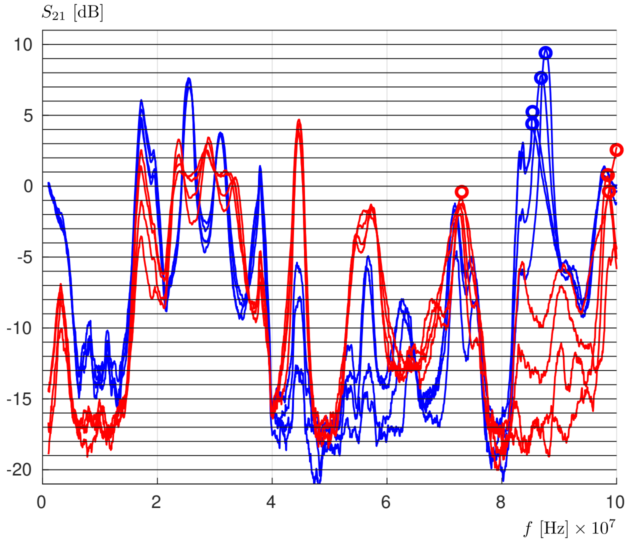

Fig. 3. Quantization intervals shown with S_{21} using the shift from S_{12} quantization centering

We investigated LDPC code design for Slepian-Wolf coding in [5]. One has to note that additionally to the structure shown in Fig. 6, the transmitted redundancy in the form of the syndrome or parity has to go through a physical (public) channel which is additionally disturbed and requires some additional error correction. Hence, the redundancy is not just given by the conditional entropy $H(\mathbf{X}_{12}|\mathbf{X}_{21})$, but has to additionally provide protection again channel errors. The decoder has then to process parities and parities of parities experiencing noise from the physical channel which might be modeled as AWGN.

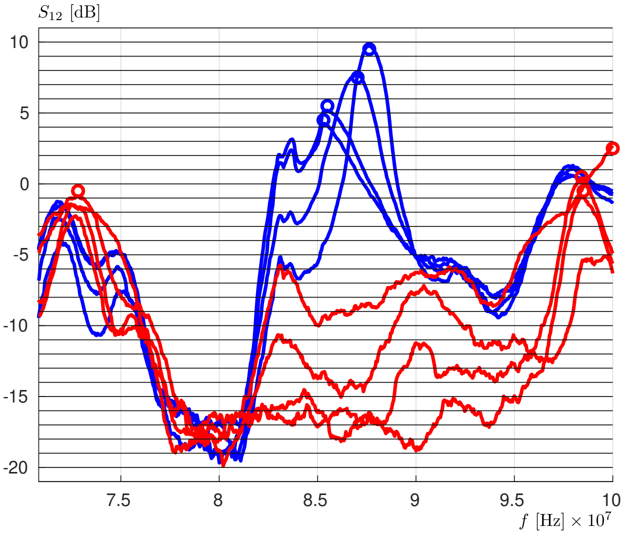

Fig. 4. Zoom-in of Fig. 2

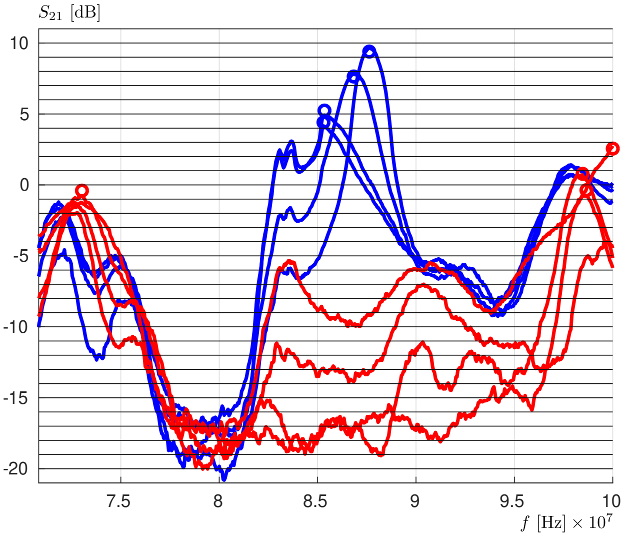

Fig. 5. Zoom-in of Fig. 3

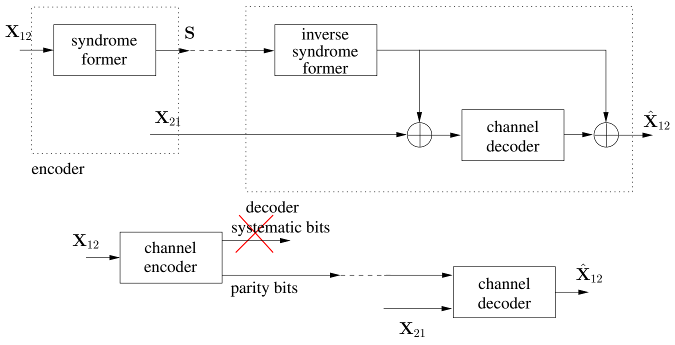

Fig. 6. Slepian-Wolf coding as syndrome and parity approaches

The density for the noisy measured $\mathbf{X}_{21}$ is different and leads to also non-consistent densities of log-likelihood ratios. The code design ideally takes those differences into account, leading to multi-edge-type code constructions in case of LDPC codes. We are about to publish more elaborate studies on such codes.

IV. Simulation results

For the KDR results shown in Fig. 7, we selected quantization interval widths (Q in dB) and a number of key bits per quantization and corresponding mapping cycle (I) for bit patterns according to the following table.

Interval width	Number of bits	no. of intervals
Q / dB	$\log_2 I$	I
1	3	8
1	4	16
2	3	8
0.5	3	8

AWGN was added, no averaging of measurements performed. Averaging will, of course, move key-disagreement rate curves to the left. For power-line applications, due to non-stationary noise, some averaging has to be performed, anyhow.

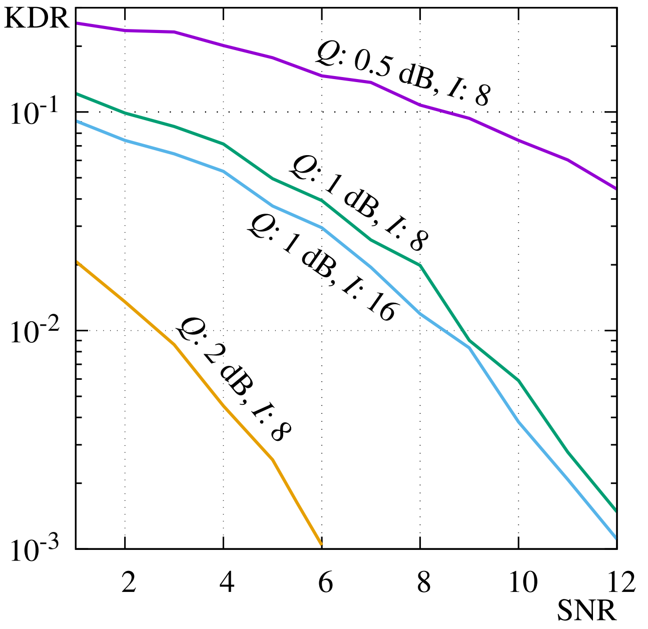

Fig. 7. Key disagreement ratio for 1 and 2 dB quantization interval width and cyclic Gray code mapping repeating mapping of 16 and 8 intervals, respectively

Since the quantization steps, number of intervals, and the selection of reactive terminations was not yet optimized in any form (just chosen such that they could be easily implemented) it was expected that the distribution of quantization results and hence resulting key segments are not at all uniformly distributed. In figures 8 to 11, we show exemplary histograms for the four cases.

Indeed, frequency distributions are far from uniform. One may use arithmetic coding or other approaches to obtain a uniform distribution, but in future work, we will optimize the quantization and termination options jointly.

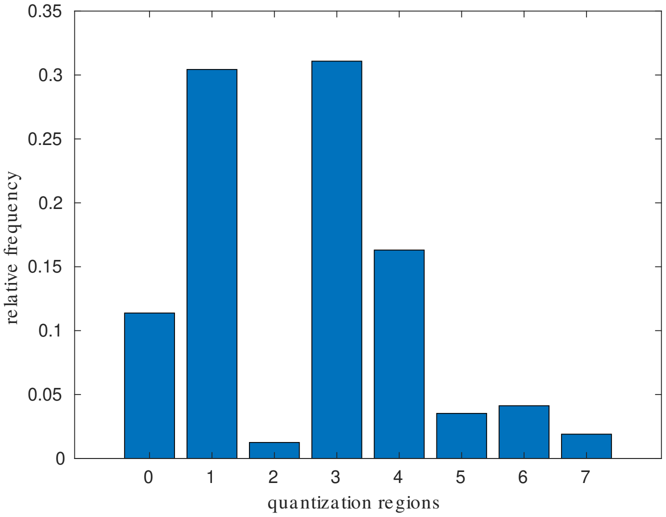

Fig. 8. Frequency distribution over quantization intervals for an interval width of 1 dB and 3 bit segment size

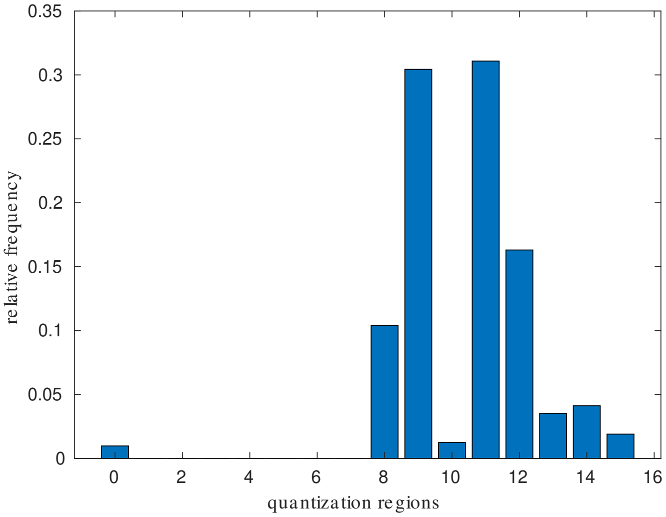

Fig. 9. Frequency distribution over quantization intervals for an interval width of 1 dB and 4 bit segment size

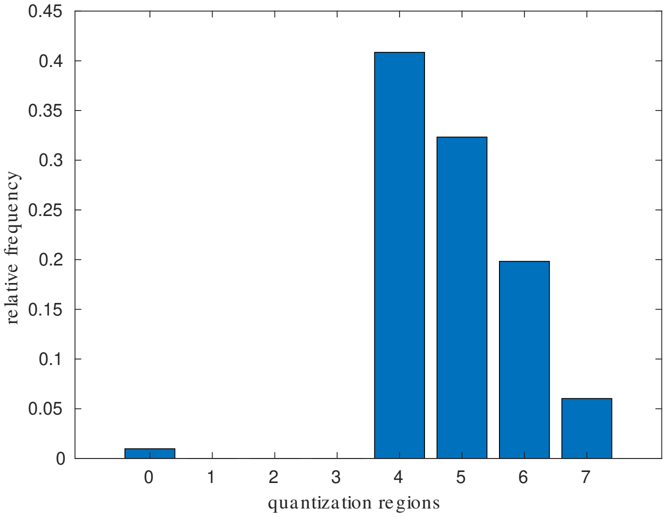

Fig. 10. Frequency distribution over quantization intervals for an interval width of 2 dB and 3 bit segment size

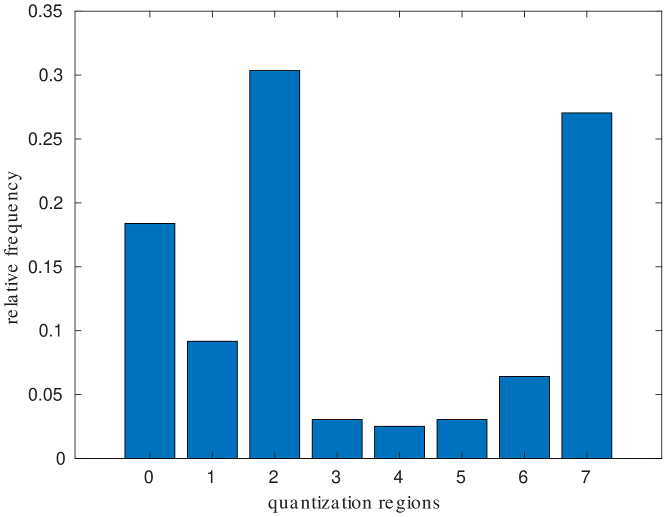

Fig. 11. Frequency distribution over quantization intervals for an interval width of 0.5 dB and 3 bit segment size

V. Conclusions

The reciprocity of transfer scattering parameters was used as a basis for key generation and reactive terminations at some branch end were used for randomly changing them.

We showed that instead of frequency locations of notches or maxima as the basis for key generation discussed in our earlier papers, using the value of the maximum could be more suitable. The key disagreement ratio can easily be improved by averaging measurements thereby making the scheme practically applicable at given SNRs. An averaging is anyhow necessary in power-line environments due to non-stationary noise conditions.

Randomly chosen reactive, i.e., lossless terminations at some branch end not too far form one of the legitimate users allowed to randomly change produced key segments. To make the distribution of key segments uniform, a joint optimization of quantization and terminations will follow. So far, the range selection, quantization, and termination choices were guided by simplicity and practical issues.

We have not discussed eavesdropper issues much, since we already showed in earlier works that a little distance from the legitimate nodes will already ensure that the frequency locations of notches and maxima are different, since the tree structure that an eavesdropper sees is very different from the one of the legitimate users. In the given scheme now, additionally, the amplitude of the maximum, not only the frequency location, would have to be estimated, which seems impossible.

As an alternative to reactive terminations at some branch end, we are confident that likewise, terminations at unused wire pairs at one of the legitimate nodes leads to similar effects, possibly requiring a different search procedure for a suitable frequency range. We have not yet simulated this case, knowing that practically, non-ideal cable properties define the coupling between wire pairs a lot and hence will influence the effect of reactive terminations at unused pairs. Non-ideal cable properties cannot easily be simulated, but we have seen the effects of such terminations from practical measurements.

References

[1] A. D. Wyner, “The wire-tap channel,” *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[2] W. Henkel, “Wireline physical-layer key generation,” in *11th Workshop on Power Line Communication (WSPLC)*, (Prague), IEEE, Sept. 2017.

[3] W. Henkel, O. A. Graur, N. S. Islam, U. Pagel, N. Manak, and O. Can, “Reciprocity for physical layer security with wireless FDD and in wireline communications,” in *2018 IEEE Globecom Workshops*, pp. 1–6, IEEE, 2018.

[4] W. Henkel, A. M. Turjman, H. Kim, and H. K. H. Qanadilo, “Common randomness for physical-layer key generation in power-line transmission,” in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, pp. 1–6, 2020.

[5] N. Islam, O. Graur, A. Filip, and W. Henkel, “LDPC code design aspects for physical-layer key reconciliation,” in *2015 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–7, 2015.

[6] U. M. Maurer, “Secret key agreement by public discussion from common information,” *IEEE Transactions on Information Theory*, vol. 39, pp. 733–742, May 1993.

[7] F. Gruber and L. Lampe, “On PLC channel emulation via transmission line theory,” in *2015 IEEE International Symposium on Power Line Communications and Its Applications (ISPLC)*, pp. 178–183, IEEE, 2015.

[8] F. Gruber and L. Lampe, *MIMO PLC Channel Emulator Release License*. University of British Columbia, 2013.

[9] C. Dhia, J.-C. Le Bunetel, and Y. Raingeaud, “A method to construct equivalent circuit from input impedance of household appliances a method to construct equivalent circuit from input impedance of household-appliances,” *International Journal on Communications Antenna and Propagation*, vol. 2, Aug. 2012.