Power-Line Physical-Layer Key Generation Study Based on Low Complexity 3-Wire 4-Port Modeling

1st Werner Henkel, *senior member, IEEE*
werner.henkel@ieee.org

2nd Tai Him Yim
yimtaihim@gmail.com

3rd Aditya Ojha
nraditya2057@gmail.com

4th Sumit Giri
sumit123768@gmail.com

5th Ehsan Olyaei Torshizi
eolyaei@constructor.university

Computer Science and Engineering
Constructor University Bremen
Bremen, Germany

***Abstract*—We first present a simplified full ABCD or S-matrix model for a 3-wire powerline grid connection to support our simulations of physical-layer security to finally be able to obtain statically significant results. Typical in-house power-line cables consist of three wires labeled L (Line), N (Neutral), and PE (Protective Earth). 4×4 ABCD or S-parameter matrices are derived from the well-known 2×2 ABCD matrix known for 2-conductor transmission lines including a FEXT (Far-End CrossTalk) model for 8 of the 16 ABCD matrix elements. For a point-to-point ABCD matrix, bridge taps with loads over L and N are represented by their corresponding Δ circuit and its ABCD matrix to finally allow for simple matrix multiplication of the cascade of such line and bridge taps elements between two end points.**

As a first application that promises secret key generation we study transfer functions when introducing randomly changing reactive loads at the legitimate terminals. We observe that the phase response at a certain frequency is very suitable to be mapped to key elements. The resulting key distribution is close to uniform and the key disagreement rates for legitimate and eavesdropping channels are almost ideal, i.e., close to zero for the first and close to 0.5 for the latter.

I. Introduction

The computation of the transfer function between two terminals in a multi-pair arrangement has nicely been addressed by Gruber and Lampe [1], [2] in 2013. However, the corresponding Matlab package relies on field computations, making it relatively complex and time-consuming. Moreover, it is based on the assumption of homogeneity, and it is necessary to adjust the relative permittivity to account for the fact that plastic materials like PVC are not rigid but foamed. Additionally, there are air-filled gaps between wires that need to be considered. This adjustment is essential to align the characteristic impedance of the actual cable with that in the simulation.

Our physical layer key generation requires fast simulations to analyze performances of different scenarios and obtain a statistically meaningful amount of data.

This work was funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – HE 3654/27-1.

In power-line communications with multicarrier modulation, the transfer function is inherently determined, primarily for equalization. In contrast to the mentioned Matlab package, we require the overall four-port matrix, not only the transfer function, between two terminals, e.g., two sockets. This means transferring branching components to the direct connection between the two points, which one may see as the backbone. This entails the product of ABCD matrices, be it from backbone elements or bridge taps. Based on the Gruber/Lampe package, we have already done some of such works described in [3] by simply using the transfer function replacing the scattering parameters $S_{12} = S_{21}$, since they would be ideally the same for perfect termination.

Both approaches cannot fully replace measurements, such as in [4], since practically, FEXT functions show statistical variations that are due to the production process and the cable layout. Those can only be modeled by the mean (or 90 % worst-case) FEXT function.

The remainder of this paper is organized as follows. Section II introduces 4×4 four-port matrices that are needed for a 3-wire power-line cable, which we selected as the most common installation cable in our country. Section III compares ABCD matrices derived from full two-sided scattering parameters or one-sided open/short impedance (or S_{11}) measurements. A FEXT response model is proposed for inclusion into the parameters relating two different wire pairs. This leads to a simplified model consisting of secondary line parameters and the FEXT model. A bridge tap with a load (e.g., and appliance) is handled in Section IV. Section V discusses our actual application for physical layer key generation. Here we show, how common randomness is obtained and which results for legitimate users and an eavesdropper can be achieved quantizing phase responses. We conclude with Section VI.

II. Matrix descriptions of a 3-wire transmission line

A 3-wire four-port, as illustrated in Fig. 1, involves four voltages and four currents, likewise four incident and four

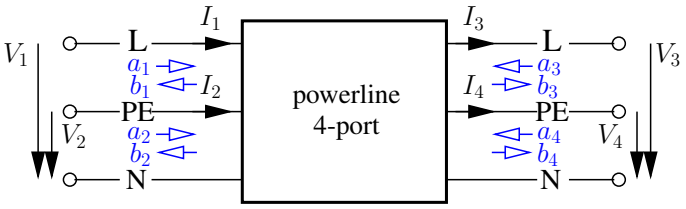

Fig. 1. Power line four-port

reflected wave components a_i and b_i, $i = 1, ..., 4$, respectively. Note that for the current directions and ABCD matrix equation, we have selected the non-symmetric option in line with Matlab routines.

Accordingly, we obtain the matrices

$$\begin{bmatrix} V_1 \\ V_2 \\ I_1 \\ I_2 \end{bmatrix} = \begin{bmatrix} A_1 & A_2 & B_1 & B_2 \\ A_3 & A_4 & B_3 & B_4 \\ C_1 & C_2 & D_1 & D_2 \\ C_3 & C_4 & D_3 & D_4 \end{bmatrix} \begin{bmatrix} V_3 \\ V_4 \\ I_3 \\ I_4 \end{bmatrix}, \quad (1)$$

$$\begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{bmatrix} = \begin{bmatrix} S_{11} & S_{12} & S_{13} & S_{14} \\ S_{21} & S_{22} & S_{23} & S_{24} \\ S_{31} & S_{32} & S_{33} & S_{34} \\ S_{41} & S_{42} & S_{43} & S_{44} \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{bmatrix}. \quad (2)$$

Figure 2 shows all measurement combinations required to determine the complete set of S-parameters, resulting in a total of $4 \cdot 6 = 24$ parameters

$$\begin{bmatrix} S_{11} & S_{13} \\ S_{31} & S_{33} \end{bmatrix}, \begin{bmatrix} S_{11} & S_{14} \\ S_{41} & S_{44} \end{bmatrix}, \begin{bmatrix} S_{22} & S_{23} \\ S_{32} & S_{33} \end{bmatrix},$$

$$\begin{bmatrix} S_{22} & S_{24} \\ S_{42} & S_{44} \end{bmatrix}, \begin{bmatrix} S_{11} & S_{12} \\ S_{21} & S_{22} \end{bmatrix}, \begin{bmatrix} S_{33} & S_{34} \\ S_{43} & S_{44} \end{bmatrix},$$

while only 16 are required. Some are determined repeatedly and one may take the mean of such measurements.

By employing the transformation relations outlined in [5], one can move from **S** to ABCD representation. They are also readily available in Matlab as "s2abcd" and "abcd2s".

A usual 2-conductor transmission line is described by the well-known ABCD formulation

$$\begin{bmatrix} \cosh \gamma l & Z_w \sinh \gamma l \\ \frac{1}{Z_w} \sinh \gamma l & \cosh \gamma l \end{bmatrix}. \quad (3)$$

The secondary line parameters, consisting of the characteristic (wave) impedance Z_w and the propagation constant $\gamma = \alpha + j\beta$, can be measured by open and short terminations, despite some virtual length extension for open termination. This extension may result in small length deficiencies, causing inaccuracies at higher frequencies.

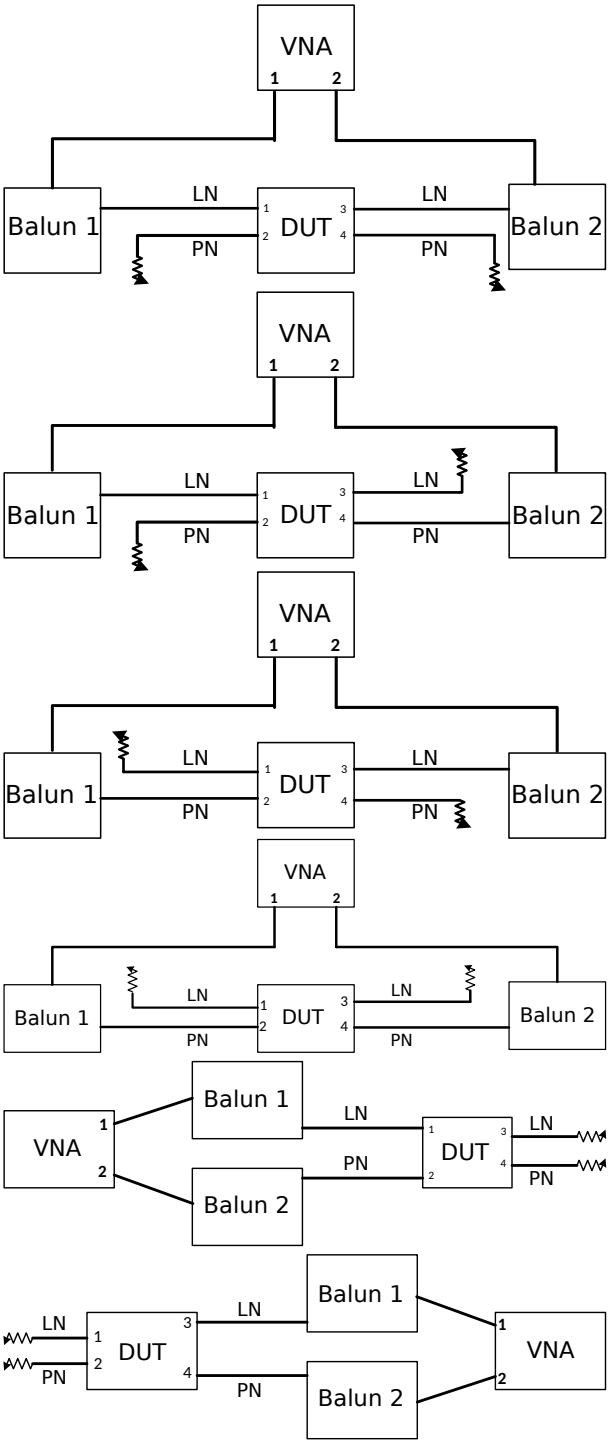

Fig. 2. S-parameter measurements for a DUT (VNA: vector network analyzer, balun for balanced matching of the 50 Ohm VNA connectors to wire pairs with a characteristic impedance of roughly 75 Ohm)

III. Model for the 4×4 ABCD matrix

In the first and fourth arrangements in Fig. 2, it is evident that they represent standard 2-wire pairs with some terminations at the other pairs added. The resulting parameters are easily described by (3), hence obtaining 8 parameters of the 4×4 ABCD matrix directly. This results in a checkerboard arrangement at positions 11, 13, 22, 24, 31, 33, 42, and 44, using row and column indices. The remaining parameters represent FEXT (Far-End CrossTalk) terms such as the one at position 12 referring to V_1/V_4 or position 41 referring to I_2/V_3. From DSL standards [6], [7], we know a model for

FEXT in the form of

$$H_{\mathrm{FEXT}} = H_{\mathrm{TR}} \cdot \sqrt{l/l_0} \cdot f \cdot k \tag{4}$$

with the transfer function H_{TR}, length l, reference length l_0, frequency f, and a constant k[1]. For that constant, we simply used the mean of the fraction of the absolute values of the measured FEXT and the model function. In the DSL case, there is an additional factor attributed to the larger arrangement with, for instance, 50 pairs.

Dividing H_{FEXT} in (4) by H_{TR} is shown in Fig. 3 compared to a FEXT measurement with the same normalization to the transfer function. Additionally, we show a dependency proportional to $\sqrt{f}$, which we found more suitable for our 4×4 ABCD matrix design. One should note that in contrast to the DSL case, the two loops are not independent, but one conductor is common to the two loops, e.g., L-N and N-PE, having N in common. Regarding the ordinate scale in dB, note that for the comparison, we just determine the constant k to make the model functions fit, but we did not exactly normalize to the length of the cable, since this is just another factor, not changing the frequency behavior.

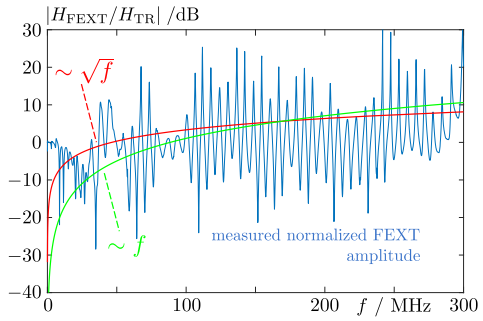

Fig. 3. Sample FEXT response and model options

When adopting such dependencies, we can, e.g., formulate the two mentioned components using

$$\frac{V_1}{V_4} \approx \frac{V_2}{V_4}\sqrt{l/l_0} \cdot \sqrt{f} \cdot k \text{ and } \frac{I_2}{V_3} \approx \frac{I_1}{V_3}\sqrt{l/l_0} \cdot \sqrt{f} \cdot k\,. \tag{5}$$

The constant k is determined comparing the component obtained from the full scattering matrix and the one through this model, i.e., again as the mean of the fractions of the two components. The intuitive reasoning for the FEXT model is that independent of the coupling location, the overall transfer function has to be part of it, assuming identical transfer functions on both pairs. In power terms, the coupling should grow with the length, explaining $\sqrt{l/l_0}$. The original DSL-FEXT model with a linear frequency dependency results from seeing two independent loops as a "transformer" and there the mutual inductance comes with $j\omega$. One should note that all these models are, of course, a rough estimate of the FEXT behavior. In reality, it is a very randomly oscillating function that cannot be described analytically. However, the subsequently described steps allow the simulation of indoor power-line arrangements much quicker than field-oriented programs such as the one by Gruber and Lampe [1], [2]. The actual FEXT function depends significantly on the wire layout inside the cable and the layout of the overall cable, which again depends on the manufacturing process and the installation, as well as on materials around the cable. This is practically impossibly to model. Although twisted pairs in telephone cables are much more homogeneous than power-line cables, also there, a trend model was found to be the only possibility.

In the following equations (6) to (9), we are listing all the relations for the 16 ABCD parameters. We abbreviate $k\sqrt{l/l_0 f}$ as H_{mod}.

$$\begin{aligned} A_1 &= \left.\frac{V_1}{V_3}\right|_{V_4,I_3,I_4=0} \\ B_1 &= \left.\frac{V_1}{I_3}\right|_{\ldots} \\ C_1 &= \left.\frac{I_1}{V_3}\right|_{\ldots} \\ D_1 &= \left.\frac{I_1}{I_3}\right|_{\ldots} \end{aligned} \tag{6}$$

$$\begin{aligned} A_2 &= \left.\frac{V_1}{V_4}\right|_{\ldots} \approx H_{\mathrm{mod}} \cdot A_4 \approx H_{\mathrm{mod}} \cdot A_1 \\ B_2 &= \left.\frac{V_1}{I_4}\right|_{\ldots} \approx H_{\mathrm{mod}} \cdot B_4 \approx H_{\mathrm{mod}} \cdot B_1 \\ C_2 &= \left.\frac{I_1}{V_4}\right|_{\ldots} \approx H_{\mathrm{mod}} \cdot C_4 \approx H_{\mathrm{mod}} \cdot C_1 \\ D_2 &= \left.\frac{I_1}{I_4}\right|_{\ldots} \approx H_{\mathrm{mod}} \cdot D_4 \approx H_{\mathrm{mod}} \cdot D_1 \end{aligned} \tag{7}$$

$$\begin{aligned} A_3 &= \left.\frac{V_2}{V_3}\right|_{\ldots} \approx A_2 \\ B_3 &= \left.\frac{V_2}{I_3}\right|_{\ldots} \approx B_2 \\ C_3 &= \left.\frac{I_2}{V_3}\right|_{\ldots} \approx C_2 \\ D_3 &= \left.\frac{I_2}{I_3}\right|_{\ldots} \approx D_2 \end{aligned} \tag{8}$$

$$\begin{aligned} A_4 &= \left.\frac{V_2}{V_4}\right|_{\ldots} \approx A_1 \\ B_4 &= \left.\frac{V_2}{I_4}\right|_{\ldots} \approx B_1 \\ C_4 &= \left.\frac{I_2}{V_4}\right|_{\ldots} \approx C_1 \\ D_4 &= \left.\frac{I_2}{I_4}\right|_{\ldots} \approx D_1 \end{aligned} \tag{9}$$

For clarification, we mark the direct insertion of single-pair ABCD parameters in color for the two pairs in Eq. (10).

$$\begin{bmatrix} V_1 \\ V_2 \\ I_1 \\ I_2 \end{bmatrix} = \begin{bmatrix} A_1 & A_2 & B_1 & B_2 \\ A_3 & A_4 & B_3 & B_4 \\ C_1 & C_2 & D_1 & D_2 \\ C_3 & C_4 & D_3 & D_4 \end{bmatrix} \begin{bmatrix} V_3 \\ V_4 \\ I_3 \\ I_4 \end{bmatrix} \tag{10}$$

Entries expected to be identical due to an assumed symmetry of the cable are highlighted with color markings in Eq. (11). They could be averaged to enforce the symmetry if there are small deviations due to measurement errors and inhomogeneous cable layout. It may be argued that practical scenarios might not exhibit the exact symmetry. Nevertheless, our goal was to create a model for fast simulations, acknowledging that not all properties of a practical situation can be fully captured.

One may note that the FEXT model introduction within (7) and (8) would destroy reciprocity, which is, of course,

[1]Note, in this formulation, k carries a unit [s=1/Hz].

a key property of every passive M-port network. We recover this symmetry by moving to S-parameters, mirroring the lower triangular part to the upper one and then returning to ABCD parameters. In this way, the amplitudes shown in Fig. 8 were almost identical to results without S-mirroring, which we cannot show due to space limitations.

$$\begin{bmatrix} V_1 \\ V_2 \\ I_1 \\ I_2 \end{bmatrix} = \begin{bmatrix} A_1 & A_2 & B_1 & B_2 \\ A_3 & A_4 & B_3 & B_4 \\ C_1 & C_2 & D_1 & D_2 \\ C_3 & C_4 & D_3 & D_4 \end{bmatrix} \begin{bmatrix} V_3 \\ V_4 \\ I_3 \\ I_4 \end{bmatrix} \tag{11}$$

In Fig. 8, we present results obtained from measuring a $3 \times 1.5\,\mathrm{mm}^2$ cable with a length of 28 m. Blue curves are ABCD entries derived from full S-parameter measurements through [5]. The red curves in green frames are the 2×2 ABCD matrices from wire pairs derived from secondary line parameters. The counterpart with blue frames were obtained from modifications using Eq. (5). Some deviations are attributed to the frequency range of the baluns, despite full 2-port calibration.

IV. Bridge-tap 4×4 ABCD matrix

To be able to obtain overall ABCD and S matrices of a point-to-point connection, we first represent a bridge tap by its input admittances in the form of a Δ arrangement, where we assume admittances Y_1 between L and N, Y_2 between PE and N, and Y_3 between L and PE. The load we assume between L and N. Load appliances have, e.g., been modeled in [8]. For our load at L and N, only, we can assume I_4 to be zero, leading to

$$\begin{aligned} V_1 &= A_1 V_3 + A_2 V_4 - B_1 Y_L V_3 \\ I_1 &= C_1 V_3 + C_2 V_4 - D_1 Y_L V_3 \\ V_2 &= A_3 V_3 + A_4 V_4 - B_3 Y_L V_3 \\ I_2 &= C_3 V_3 + C_4 V_4 - D_3 Y_L V_3 \end{aligned} \tag{12}$$

To obtain Y_{1-3}, we additionally set $V_2 = 0$, leading to $Y_1||Y_3 = Y_1 + Y_3$. Likewise, choosing $V_1 = 0$ leads to $Y_2||Y_3 = Y_2 + Y_3$, and finally, $V_1 = V_2$ means $Y_1||Y_2 = Y_1 + Y_2$. Together with the ABCD matrix in (12), one can then obtain with some trivial but lengthy math,

$$\begin{aligned} Y_1 = {} & [(Y_1 + Y_3) - (Y_2 + Y_3) + (Y_1 + Y_2)]/2 \\ = {} & [A_1C_2 - A_2C_1 - 2A_3C_2 + 2A_4C_1 - A_3C_4 + A_4C_3 \\ & + A_2D_1Y_L - B_1C_2Y_L - 2A_4D_1Y_L + 2B_3C_2Y_L \\ & - A_4D_3Y_L + B_3C_4Y_L] \,/\, [2(A_1A_4 - A_2A_3 \\ & + A_2B_3Y_L - A_4B_1Y_L)] \end{aligned} \tag{13}$$

$$\begin{aligned} Y_2 = {} & [-(Y_1 + Y_3) + (Y_2 + Y_3) + (Y_1 + Y_2)]/2 \\ = {} & [A_1C_2 + 2A_1C_4 - A_2C_1 - 2A_2C_3 + A_2D_1Y_L \\ & + 2A_2D_3Y_L - A_3C_4 + A_4C_3 - A_4D_3Y_L \\ & - B_1C_2Y_L - 2B_1C_4Y_L + B_3C_4Y_L] \,/\, [2(A_1A_4 \\ & - A_2A_3 + A_2B_3Y_L - A_4B_1Y_L)] \end{aligned} \tag{14}$$

$$\begin{aligned} Y_3 = {} & [(Y_1 + Y_3) + (Y_2 + Y_3) - (Y_1 + Y_2)]/2 \\ = {} & [-A_1C_2 + A_2C_1 - A_2D_1Y_L + A_3C_4 - A_4C_3 \\ & + A_4D_3Y_L + B_1C_2Y_L - B_3C_4Y_L] \,/\, [2(A_1A_4 \\ & - A_2A_3 + A_2B_3Y_L - A_4B_1Y_L)] \end{aligned} \tag{15}$$

The Z-matrix for the Δ admittance 4-port is given by

$$\begin{bmatrix} V_1 \\ V_2 \\ V_3 \\ V_4 \end{bmatrix} = \frac{1}{Y_1Y_2 + Y_2Y_3 + Y_1Y_3} \cdot \cdot \begin{bmatrix} Y_2 + Y_3 & Y_3 & Y_2 + Y_3 & Y_3 \\ Y_3 & Y_1 + Y_3 & Y_3 & Y_1 + Y_3 \\ Y_2 + Y_3 & Y_3 & Y_2 + Y_3 & Y_3 \\ Y_3 & Y_1 + Y_3 & Y_3 & Y_1 + Y_3 \end{bmatrix} \begin{bmatrix} I_1 \\ I_2 \\ I_3 \\ I_4 \end{bmatrix}, \tag{16}$$

which can be turned into an ABCD matrix by the corresponding Matlab command "z2abcd" or consulting [5].

V. Physical-layer key generation from transfer factors for Alice-Bob and Alice-Eve connections

From practical measurements and also simulations with the Gruber/Lampe package, we know that having Eve close to either Alice or Bob is critical, just as in the wireless case. Likewise, we found that for obtaining the desired *common randomness* for physical-layer key generation, variable reactive loads should be placed not too far from Alice or Bob to lead to sufficient changes in the transfer function. The most convenient and implementation-wise most practical solution appears to equip the legitimate end with a varying reactive load, which we chose to be capacitive or inductive, i.e., lossless. Additionally, we are still assuming the (almost) ideal ohmic termination (75 Ohm) everywhere, in parallel to the reactive loads at the legitimate ends. The capacitive and inductive loads were selected in the ranges 1 pF to 1 nF and 1 nH to 1 μH (in log steps), respectively.

Figure 4 shows a simple situation with 9 wire segments (1.83, 0.47, 2.33, 2.20, 2.10, 2.03, 3.10, 1.13, 0.97 m) and arbitrary appliances, where we had coffee maker, PC, vacuum cleaner, and fridge to randomly choose. During the simulations, the segments lengths were chosen randomly up to 3.3 m. The terminations at Bob's end shows the parallel 75 Ohm and random reactive loads. Alice and Eve's loads were chosen to be 75 Ohm. In a practical setup, one would, of course, also equip Alice with random reactive loads, since Eve could be close to her, too.

Results for $S_{13} = S_{31}$ for the Alice-Bob link are shown in Fig. 5. Note that the reciprocity holds for every passive 4-port (M-port in general; also for arbitrary passive termination in the fuse box) and one can show [9] that these transfer factors are identical to the transfer functions under ideal termination with the characteristic impedance. Practically, one will, of course,

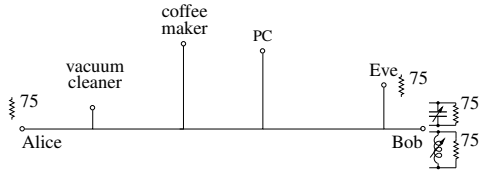

Fig. 4. Sample powerline network, segment lengths in meters

not use a vector network analyzer (VNA) to determine S-parameters, but will measure the transfer function as, e.g., every multicarrier (OFDM/DMT) modem does.

The transfer function changes nicely with the different reactive loads, as also already observed from measurements. This provides the required common randomness. Similar modifications can also in practice be achieved by connecting the reactive loads to unused pairs at the sides of Alice or Bob. However, this cannot be simulated when assuming homogeneous wire pairs.

Implementing the random reactive loads into the end units conveniently allows to change them triggered by Alice and/or Bob.

In our earlier publications [3], [4], [10], [11], we concentrated on using the amplitude response for key generation, since maxima and minima are modified in amplitude and location with varying reactive terminations. However, using the phase seems more suitable, since one can just quantize the phase in equal steps and map phases to a bit pattern using a Gray code labeling. We show such a mapping in Fig. 6 for $M = 16$ quantization steps. We picked the frequency bin (here 1801 from a total of 2001), which had the biggest variance for a short run with random length configuration and terminations to make use of the full $[-\pi, \pi)$ range. For the variance computation, one has to, of course, take the 2π periodicity into account. The data used for localizing a suitable frequency was later not included in the actual statistics. This means, we do not match to the actual scenario, which would then be done in a practical implementation, which could even further improve the results. Another selection criterion may be to look for the maximum SNR location.

In both figures, solid lines show the Alice-Bob link, where dashed ones are for Alice-Eve. They are better visible in the zoom-in plot Fig. 6.

As analog key reconciliation step, we have chosen a simple procedure, which publicly announces a shift of data (or equivalently the quantization grid) to the middle of the corresponding quantization interval (say, at Alice), which ensures that the measurement at the other side (Bob) will also likely be in the same interval. This will work, as long as the difference between the two measurements is less than half of the quantization interval width apart. This shift procedure is, e.g., also described in [9]. Let us assume Alice to communicate the shift for the measured phases. The quantization value $Q(\phi_A)$

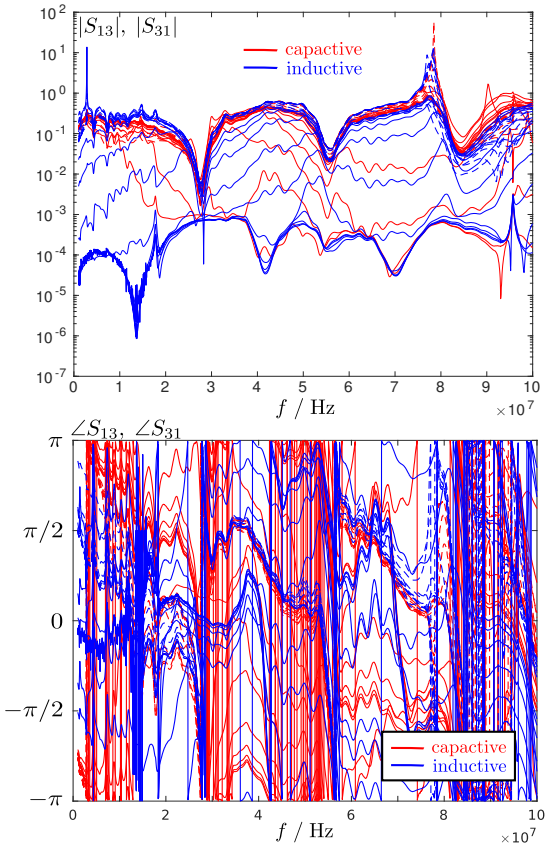

Fig. 5. $S_{13} = S_{31}$ in amplitude and phase for the Alice-Bob (solid lines) and Alice-Eve (dashed lines) links and varying reactive load (red: capacitive, blue: inductive,)

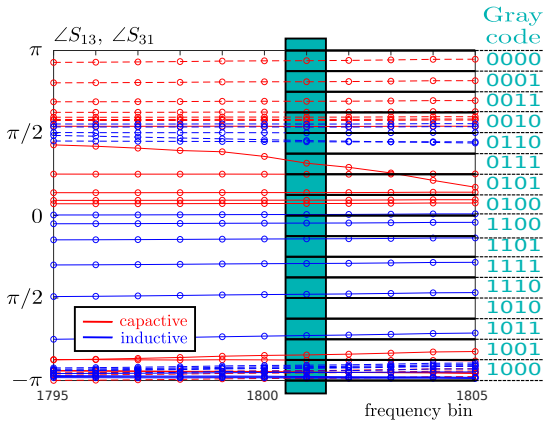

Fig. 6. Zoom-in of the phase of $S_{13} = S_{31}$ for the Alice-Bob solid lines) and Alice-Eve (dashed lines) and mapping to quantization intervals with Gray labeling

is given by

$$\mathrm{Q}(\phi_\mathrm{A}) = \mathcal{Q}_\mathrm{A} \quad \text{if} \quad \mathrm{mod}\,(\phi_\mathrm{A}, 2\pi) \in \left[\frac{2\pi(\mathcal{Q}_\mathrm{A} - 1)}{2^M} \ , \ \frac{2\pi\ \mathcal{Q}_\mathrm{A}}{2^M} \right) . \quad (17)$$

mod(...) stands for moving the phase into a $[0, 2\pi)$ interval.

The shift is then determined by

$$S_{\mathrm{A}} = \phi_{\mathrm{A}} - \frac{\pi(2\mathcal{Q}_{\mathrm{A}} - 1)}{2^M} \tag{18}$$

Subsequently, the data is updated according to

$$\phi_{\mathrm{A}} := \phi_{\mathrm{A}} - S_{\mathrm{A}} \ , \ \phi_{\mathrm{B}} := \phi_{\mathrm{B}} - S_{\mathrm{A}} \ . \tag{19}$$

Likewise, the procedure can also initiated by Bob. Further key reconciliation can be based on Slepian-Wolf coding, just as in [12], [13].

In the noise-free situation shown in figures 5 and 6 the resulting bit-wise key disagreement rate (KDR) was zero for the legitimate link and 0.503 for the link to the eavesdropper (for 12.000 random segments, appliances, and reactive loads), which is almost ideal. With some uncorrelated noise, naturally, the KDR of the legitimate link will also increase, but it just naturally depends on the noise variance relative to the quantization interval width. One may adjust the number of quantization intervals as appropriate.

Figure 7 shows a histogram over the quantization intervals for the legitimate and eavesdropping links. The probabilities are not yet completely uniform. Arithmetic coding may be used to further flatten the distribution. We are working on another option to ensure the distribution to be perfectly flat.

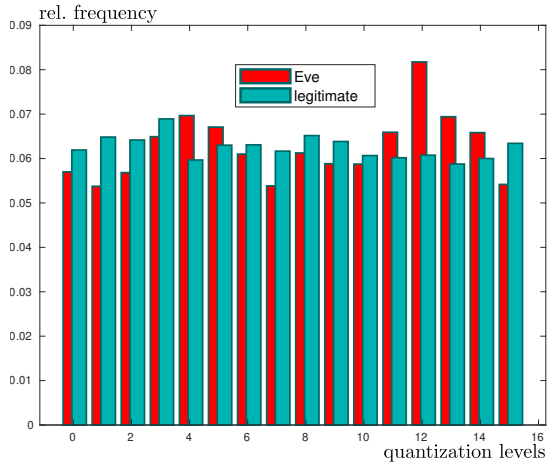

Fig. 7. Histogram for legitimate and eavesdropping key segments

VI. Conclusions

For extensive and statistically reliable simulations of physical layer secret key generation on power lines, we have presented a possibility for designing a simplified 4×4 ABCD-matrix formulation for a 3-wire power-line cable. This formulation is based on standard single-pair secondary line parameters along with a modified FEXT model utilized to design the ABCD entries at positions, where the sums of row and column indices are odd, representing functions relating to two different pairs. Our findings indicate that a decent match is achieved for lengths suitable for in-room cable arrangements. Such a model assumes some symmetry and cannot represent all the variations of a real far-end crosstalk function, nor the effects of arbitrary cable layouts, since in practice, the way wires are laid out and how the interconnections are realized, has quite some influence on the transfer characteristics. We showed an exemplary network layout with Alice, Bob, and Eve, some home appliances and varying reactive loads at one of the legitimate ends. We could show that especially the phase of the transfer factor (or transfer function) can nicely serve as a basis for physical layer key generation. Almost perfect KDR results are obtained for the legitimate and eavesdropping links, indicating almost ideal secrecy.

In further works, we will investigate different network topologies and and add noise to show the KDR dependent on the noise and the number of quantization intervals (number of bits of key segments). This will again show the capabilities of our key reconciliation schemes, already outlined in our publications for wireless key generation. Estimates of secret key rate and NIST tests will also follow.

References

[1] 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)*. IEEE, 2015, pp. 178–183.

[2] ——, *MIMO PLC Channel Emulator Release License*. University of British Columbia, 2013. [Online]. Available: http://www.ece.ubc.ca/~lampe/MIMOPLC/

[3] W. Henkel, H. Y. Kim, A. M. Turjman, and M. Bode, "A simple physical-layer key generation scheme for power-line transmission," in *2021 IEEE International Symposium on Power Line Communications and its Applications (ISPLC)*, 2021, pp. 13–18.

[4] W. Henkel, A. M. Turjman, H. K. H. Qanadilo, and U. Pagel, "Common randomness for physical-layer key generation in powerline transmission," in *13th Workshop on Power Line Communication (WSPLC)*, Hammamet, Tunesia, 2019.

[5] T. Reveyrand, "Multiport conversions between S, Z, Y, H, ABCD, and T parameters," in *2018 International Workshop on Integrated Nonlinear Microwave and Millimetre-wave Circuits (INMMIC)*. IEEE, 2018, pp. 1–3.

[6] "Test procedures for digital subscriber line (DSL) transceivers," G. 996.1.

[7] E. Liu, Y. Gao, G. Samdani, O. Mukhtar, and T. Korhonen, "Broadband characterization of indoor powerline channel and its capacity consideration," in *IEEE International Conference on Communications, 2005. ICC 2005. 2005*, vol. 2, 2005, pp. 901–905.

[8] D. Chariag, M. J-C. Le Bunetel, and Y. Raingeaud, "A method to construct equivalent circuit from input impedance of household appliances," *International Journal on Communications Antenna and Propagation*, vol. 2, no. 4, Aug. 2012.

[9] E. Olyaei Torshizi and W. Henkel, "Exploiting FDD channel reciprocity for physical layer secret key generation in IoT networks," *IEEE Communications Letters*, vol. 28, no. 6, pp. 1268–1272, 2024.

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

[11] 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*. IEEE, 2018, pp. 1–6.

[12] 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)*, 2015, pp. 1–7.

[13] O. Graur, N. Islam, A. Filip, and W. Henkel, "Quantization aspects in LDPC key reconciliation for physical layer security," in *SCC 2015; 10th International ITG Conference on Systems, Communications and Coding*, 2015, pp. 1–6.

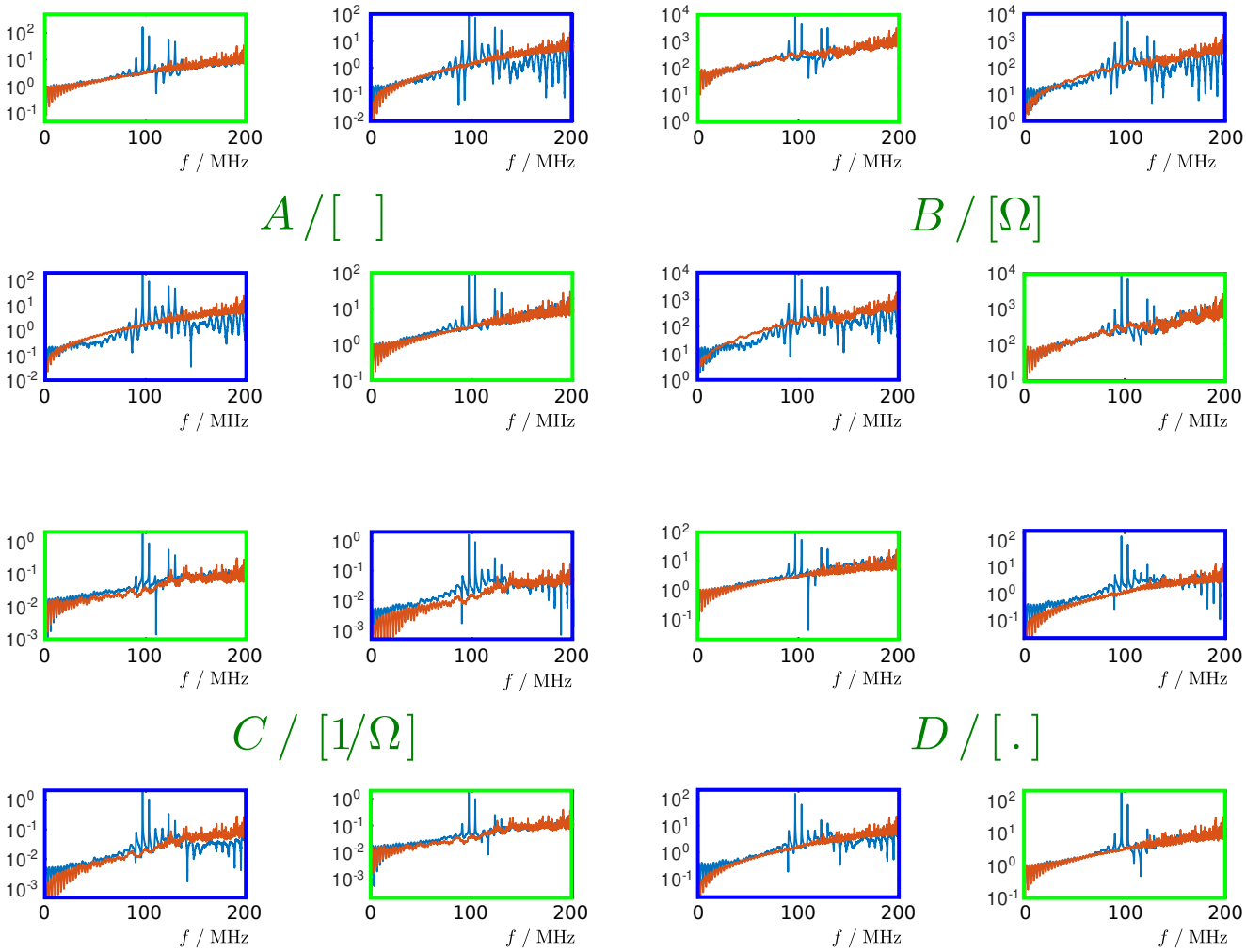

Fig. 8. Absolute values of 4×4 ABCD parameters from scattering parameters and modeled ones, having incorporated FEXT and S-matrix mirroring Green frames: direct wire pairs; blue frames: pairings involving FEXT coupling; blue curves: ABCD parameters derived from full S-parameter measurements according to Fig. 2 using [5]; red curves: ABCD parameters determined by Eq. (3) including FEXT as in Eq. (5) in blue-framed figures