Common Randomness for Physical-Layer Key Generation in Power-Line Transmission

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

2nd Abderraheem M. Turjman
3rd Hayoung Kim
4th Hisham K. H. Qanadilo

Jacobs University Bremen

***Abstract*—Physical layer key generation is based on reciprocal channels providing common randomness, which was so far known from TDD wireless channels. This paper opens the door to wireline physical-layer security, especially focusing on power-line connections. Additionally to the known reciprocity, we now also provide randomization by terminating idle branching connections (e.g., empty sockets) with random (reactive) loads. Alternatively, unused pairs at the power-line modem's end may be terminated by random (reactive) loads. Simulation and measurement results are shown.**

We also indicate, how the actual key generation can be realized by quantizing a frequency range and using the position of notches of the transfer function or of transmission coefficients selecting a quantization interval and with it a binary label as a key segment. Key reconciliation can simply be realized by a publicly announced shift of the quantization grid.

Applications are seen for in-home and industrial devices required to exchange data over the power-line network securely.

***Index Terms*—Physical-layer security, PLC, power-line communication, IoT, smart grid**

I. Introduction

Physical layer security had its start with Wyner's wiretap channel [1], which is based on signal-to-noise ratio advantages of the legitimate channel compared to the channels to eavesdroppers. We are, however, focusing on key generation from common randomness of channels which originated from works of Ahlswede, Csiszàr [2], and Maurer [3]. "Common" stands for reciprocity properties of a channel between Alice and Bob, allowing for the generation of identical key elements on both sides, without leaking information to an eavesdropper (Eve). This requires to have a different, ideally independent, channel to Eve. "Randomness" is required to generate a growing number of key bits, still requiring to not have significant channel changes during the measurement time of the bidirectional channel probing from Alice to Bob and Bob to Alice.

The common randomness is typically present in case of mobile TDD (time division duplexing) channels when the probing is executed within the coherence time. Mobility allows for randomization, which may be simulated by randomly modified reconfigurable antennas in an antenna array.
For FDD (frequency division duplexing), one can make use of the DoA (Direction of Arrival) as the common variable showing suitable symmetries.

Power-line channels were thought to not allow for the necessary random properties. We now show that power-line connections actually provide the necessary reciprocity and additionally, different measures also allow to randomize the channel. We show a simulation of a simplified network element with only a single bridge tap, which already shows the required behavior. We also provide a glimpse of what measurements are required to include seemingly trivial components like sockets, switches, and alike.
Additionally, we show measurements inside a room between outlets to outline that also practically, transfer functions can be modified. Both, simulations and measurements clearly indicate the reciprocity needed for identical key generation on both sides and the possibility to randomize the transfer function by operations using random terminations at another outlet or at another line at one of the ends of the legitimate link.

The following two sections will first discuss reciprocity properties and then introduce the basic description of a three-wire system and discusses the measurement and calibration issues that come with such 3-wire cabling and components which we typically label with L (Line), N (Neutral), and PE (Protective Earth), where we sometimes abbreviate the latter with P, only. Section IV will then describe a simple simulation model and the use of the simulation package by Gruber/Lampe [4], [5] and our modifications and extensions. This is followed by the actual simulation results in Section V. Practical measurements with different terminations at a different pair and at a bridge tap are described in Section VI. In Section VII, we indicate, how we envisage key generation and also provide a simple procedure for key reconciliation not leaking information. Section VIII concludes the paper.

II. Reciprocity in power-line systems

Seeing a wireline connection as a two-port, reciprocity is, e.g., provided by the well-known relations between the elements of two-port impedance, admittance, or ABCD matrices.

This work was funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – HE 3654/27-1.
The authors are grateful to Uwe Pagel for supporting us in hardware design. We also thank Prof. Lutz Lampe at UBC for his support regarding their simulation tool.

Those symmetries are

$$Z_{12} = Z_{21} \ , \quad Y_{12} = Y_{21} \ , \quad \det \mathbf{A} = 1 \ , \tag{1}$$

respectively. Likewise, when considering scattering parameters, reciprocity is given in the transmission coefficients, i.e.,

$$S_{12} = S_{21} \ . \tag{2}$$

First results on FDD wireless and power-line reciprocity were shown in [6], [7].

In contrast to a dedicated twisted pair (TP), unshielded twisted pair (UTP), inside telephone or Ethernet cables), a power-line network is not a point-to-point connection, but has branching connections, so-called bridge taps, that might be open-ended at a socket or switch or might be terminated with some appliances or with fuses and RCCB (Residual Current Circuit Breaker) with very different impedances. Additionally, inhouse power cables are by far not as homogeneous as telephone or Ethernet cables. The bridge taps lead to notches at certain frequencies and the non-homogeneous and non-symmetric properties, also of terminations, lead to coupling effects between pairs, much stronger than the NEXT and FEXT (Near-End / Far-End CrossTalk) known from twisted pairs.

The frequencies of notches that will be seen to be symmetrically showing up in S_{12} and S_{21} can be utilized for key generation by quantizing the frequency scale within a certain range. We will additionally show that, as to be expected, the notch positions are different at different locations, ensuring security against eavesdropping.

The extreme coupling between wire pairs will allow for varying the transfer function using terminations at unused pairs. Otherwise, the ideal way of modifying the transfer function is terminating the line at a bridge tap with arbitrary impedances, thereby also modifying the transfer function. With purely reactive loads, we will see that we can easily shift the notches. Choosing such terminations randomly can lead to the randomness that is otherwise realized by mobility in wireless communication.

The next section lays the two-port foundation for a typical 3-wire cabling and corresponding other components, like sockets, switches, etc..

III. 3-WIRE TWO-PORT DESCRIPTION

In a 3-wire system, all two-ports, also the cable itself, have 3 connections on each side as shown in Fig. 1, accordingly have two independent voltages and two independent currents on both sides, where we used N as a reference which carries $I_1 + I_2$ or $I_3 + I_4$ on the left and right side, respectively, to fulfill the port conditions.

The ABCD matrix has now 16 components

$$\begin{bmatrix} V_1 \\ V_2 \\ I_1 \\ I_2 \end{bmatrix} = \begin{bmatrix} A_1 & A_2 & B_1 & B_2 \\ A_3 & A_4 & B_3 & B_4 \\ C_1 & C_2 & D_1 & D_2 \\ C_3 & C_4 & D_3 & D_4 \end{bmatrix} \begin{bmatrix} V_3 \\ V_4 \\ I_3 \\ I_4 \end{bmatrix} \tag{3}$$

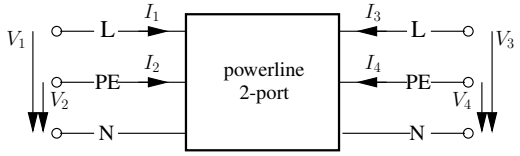

Fig. 1. Power line two-port

or in a more compressed form,

$$\begin{bmatrix} \mathbf{V}_L \\ \mathbf{I}_L \end{bmatrix} = \begin{bmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{C} & \mathbf{D} \end{bmatrix} \begin{bmatrix} \mathbf{V}_R \\ \mathbf{I}_R \end{bmatrix} \ . \tag{4}$$

Likewise, we also have 16 S-parameters describing the relation of incident (a_i) to reflected (b_i) waves.

$$\begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{bmatrix} = \begin{bmatrix} S_{11} & S_{12} & S_{13} & S_{14} \\ S_{21} & S_{22} & S_{23} & S_{24} \\ S_{31} & S_{32} & S_{33} & S_{34} \\ S_{41} & S_{42} & S_{43} & S_{44} \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{bmatrix} \tag{5}$$

We decided to determine S-parameters of sockets and switches with some short power cables using a 2-port vector network analyzer (VNA) together with baluns to realize the coupling between 50 and 75 Ohms, where the latter is roughly the characteristic impedance of the pairs of 3-pair power cables of type 3×1.5 NYM-J. With every measurement, terminating unused ports with 75 Ohms, one can obtain 4 parameters of the 4×4 S-parameter matrix. Possible measurement arrangements are shown in Fig. 2. Those arrangements lead to the submatrices of the 4×4 S-parameter matrix listed as (6) to finally assemble the required 16 entries.

$$\begin{bmatrix} S_{11} & S_{13} \\ S_{31} & S_{33} \end{bmatrix}, \quad \begin{bmatrix} S_{11} & S_{14} \\ S_{41} & S_{44} \end{bmatrix}, \quad \begin{bmatrix} S_{22} & S_{23} \\ S_{32} & S_{33} \end{bmatrix},$$
$$\begin{bmatrix} S_{22} & S_{24} \\ S_{42} & S_{44} \end{bmatrix}, \quad \begin{bmatrix} S_{11} & S_{12} \\ S_{21} & S_{22} \end{bmatrix}, \quad \begin{bmatrix} S_{33} & S_{34} \\ S_{43} & S_{44} \end{bmatrix}. \tag{6}$$

To calibrate measurements, the baluns are specified by a 3-point procedure with open, short, termination to determine their ABCD-matrix. From the measurements of 2×2 S-parameter sub-matrices between different ports Live – Neutral (LN) and Protective-Earth – Neutral (PN) of the DUT (device under test) according to Fig. 2, one would determine the corresponding ABCD matrix by well-known conversation formulas and then on both sides multiply with the inverses of the two balun ABCD matrices.

Our two-port with 3 lines can be seen as a multi-port connection and conversion formulas between matrix representations, especially **S**, **T**, ABCD, **Z** are provided by [8]. As an alternative to S-parameters, the so-called T-matrix offers the description of a cascade of two-ports, but the transition to ABCD-matrices is more commonly applied.

IV. SIMULATION MODEL AND REALIZATION

We made use of a multiple-input, multiple-output (MIMO) power line communication (PLC) channel emulator to determine the per unit length parameters (primary line parameters)

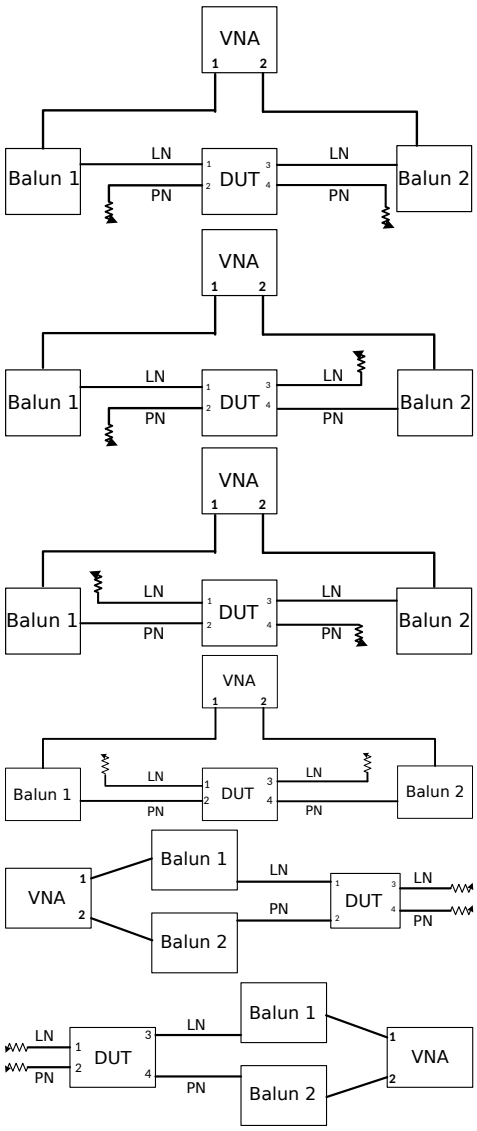

Fig. 2. S-parameter measurements for a DUT

of the multi-conductor transmission line and the transfer function between any two points in a power line network. It is a MATLAB-based tool by Gruber/Lampe [4], [5]. The per unit length parameter computation package uses a numerical solver to obtain the capacitance matrix for a multi-conductor transmission line. We sketch the relations that are used, but refer to the original papers for details. To determine the capacitance matrix,

$$\mathbf{Q} = \mathbf{C}\mathbf{V} \tag{7}$$

is used, where $\mathbf{V}$ and $\mathbf{Q}$ are voltage and charge vectors, respectively. The capacitance matrix $\mathbf{C}$ in (7) should, of course, not be misinterpreted as $\mathbf{C}$ of the ABCD matrix in (4).

The charge Q enclosed in area S can be expressed by the potential function

$$Q = \oiint_S \epsilon \frac{\partial \Phi}{\partial n} \mathbf{a}_n \, ds \, , \tag{8}$$

where ϵ is the permittivity of the medium that is surrounding the conductors and $\mathbf{a}_n$ is the unit vector normal to the surface of the area S.

The potential function $\Phi(x, y)$ at coordinates (x, y) in the area around the conductors, according to Laplace's equation, fulfills

$$\nabla^2 \Phi(x, y) = \frac{\partial^2 \Phi(x, y)}{\partial x^2} + \frac{\partial^2 \Phi(x, y)}{\partial y^2} = 0 \, . \tag{9}$$

The capacitance matrix can be obtained by Eq. (9), then solving Eq. (8). The conductance matrix $\mathbf{G}$ can be obtained by including the losses of the medium that is surrounding the conductors by defining a complex dielectric constant

$$\hat{\epsilon} = \epsilon(1 - j\frac{\sigma}{2\pi f \epsilon}) \, , \tag{10}$$

where σ is the conductivity of the medium and f is the frequency. The introduction of a complex $\hat{\epsilon}$ also yields a complex capacitance matrix $\underline{\mathbf{C}}$. The capacitance and conductance matrices can then be obtained by

$$\mathbf{C} = \Re\{\underline{\mathbf{C}}\} \, , \quad \mathbf{G} = -\omega \, \Im\{\underline{\mathbf{C}}\} \, . \tag{11}$$

It is assumed that the medium around the conductors is not magnetic, i.e., $\mu = \mu_0$. The inductance does not depend on the permittivity of the medium. As a result, the inductance matrix $\mathbf{L}$ can be obtained from the capacitance matrix applying

$$\mathbf{L} = \mu_0 \epsilon_0 \, \mathbf{C}_0^{-1} \, . \tag{12}$$

$\mathbf{C}_0$ is the free space capacitance matrix. ϵ_0 and μ_0 are the free space permittivity and free space permeability, respectively.

We also used the simulation package to compute the transfer function of a transmission line network. One can see the network reaching out to an end point as a tree (see Fig. 3). Starting from the leaves, impedances are combined thereby computing equivalent impedances at vertices. Starting at the root, one would then determine transfer functions at tree segments. This is a very standard approach coined "carry-back method" in [9]. We describe the principle shorty, but have to refer to [9] for more details.

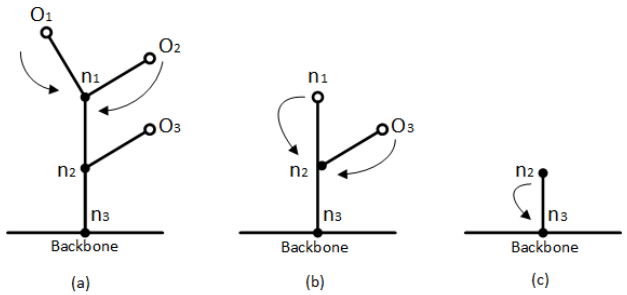

Fig. 3. Impedance carry-back [9]

As illustrated in Fig. 3(a), the load impedance at node n_1 is firstly updated by adding the equivalent admittances from outlets O_1 and O_2 to n_1. The equivalent circuit after first carry back will be in Fig. 3(b). Then, n_1 and O_3 can also be

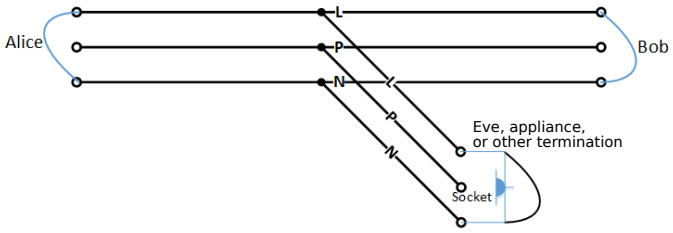

Fig. 4. Test power-line arrangement with a branching to another socket or appliance

carried back to the node n_2. Finally, the backbone (tree root) is reached as shown in Fig. 3(c).

After having defined a backbone connection and doing impedance combinations as just described, the channel transfer function between nodes at that backbone is given as a product of segment transfer functions H_n

$$H = \prod_{n=1}^{N} H_n \ , \tag{13}$$

where H_n is the individual transfer functions of a segment at depth n, and N denotes the number of considered segments.

Note: The relative permittivity ϵ_r for the NYM-J cable, which has the insulator PVC, should be 4. However, to obtain the right characteristic impedance of an actual cable, we had to change ϵ_r to 1.5. This might be due to the fact that an actual cable is not tightly PVC filled.

V. Simulation Results for a Bridge-Tap Configuration

Using Gruber and Lampe's simulation environment [4], [5], we investigated a simplified, but still typical test case providing a power-line link between Alice and Bob plus a branching to another socket with or without an appliance connected or with intentional terminations at that location. The structure is shown in Fig. 4.

At the branch end, we added a socket and cable connection to different appliances like PC, refrigerator, coffee maker, and vacuum cleaner. The model circuits for those devices were taken from [10]. The socket and plug combination ABCD matrix included cable connections of roughly a meter on both sides. Figure 5 shows transfer functions for the different appliances. The different terminations lead to stronger variations in a certain frequency range, which depends on the line configuration. Here, we had a T-structure of 10 plus 10 meter loops plus a 3 m branch to the appliances in the middle. Frequencies of local minima clearly depend on the connected appliance.

Instead of appliances, one can, of course, intentionally put reactive loads to a branching connection (here without the socket for simplicity). This will, of course, shift the minima locations as also known well from bridge taps of different lengths. A lossless cable with an open or shorted end can also be seen as a reactive load. Figure 6 shows results with

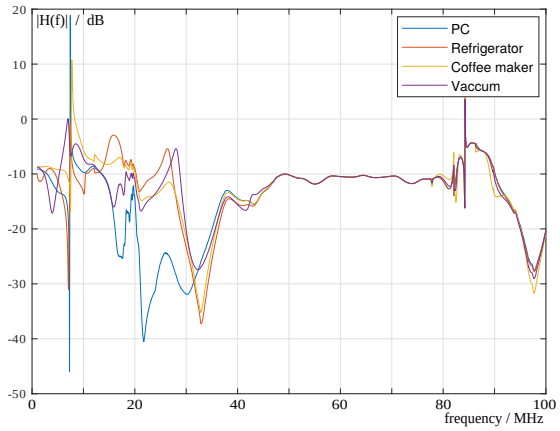

Fig. 5. Transfer functions with different appliances at a branching line

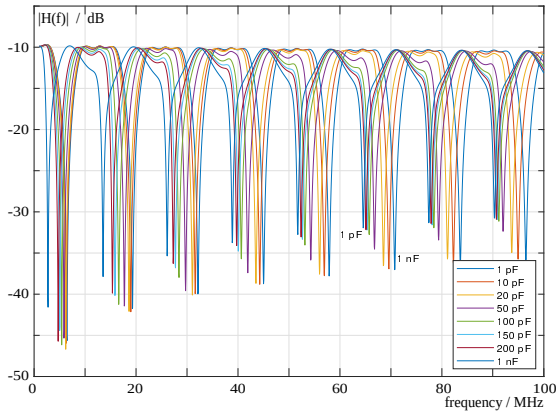

Fig. 6. Transfer functions with different capacitive loads at the branch end

different capacitors connected to the end of the branch and it clearly outlines that, as expected, one can easily shift minima locations. We will see this also practically in the network as described in the next section, but less pronounced. There, we will also see possibilities with terminations at other wire pairs at Alice's or Bob's end. This does not make sense to be simulated, since it depends on the inhomogeneity of the real cables and network, defining the actual crosstalk functions.

What can and should be simulated is the difference in transfer functions between Alice and Bob and, e.g., Alice and Eve. We show this for the same arrangement with the branching connection in Fig. 7. Although we obtain minima at different frequencies in some frequency ranges, we observe a strong correlation in case of this simple T-network.

We are currently extending the simulation to realize random power-line connection graphs with random placement of Alice, Bob, Eve, and appliances to model an actual room scenario to be able to determine secret key capacities. This will yield a quantitative measure to evaluate eavesdropping risks. Furthermore, such simulations can deliver data for the key generation rate and key disagreement ratio for some chosen quantization and reconciliation procedures.

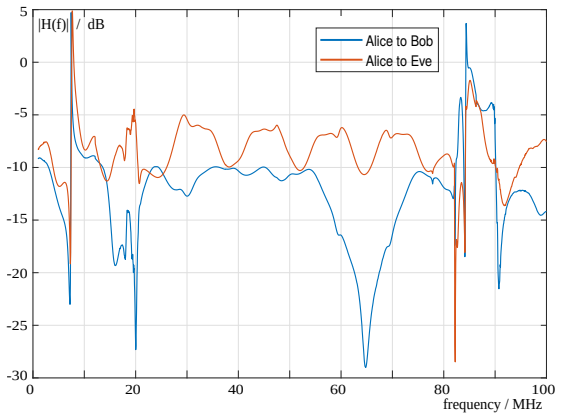

Fig. 7. Transfer functions between Alice and Bob vs. Alice and Eve

VI. Measurements

The following section shows exemplary measurements of S-parameters between sockets where we modify the transfer characteristic by changing terminations at the N-PE connection (behind a coupling capacitor-balun insulating circuit, whose influence can be ignored) while measuring the L-N loop. Due to the strong coupling between loops in a power-line cable, this indeed allows to modify the transfer characteristic. Figure 8 shows the results between 9 kHz and 100 MHz with a zoomed-in figure from 20 to 50 MHz to show the changes more clearly. This allows to change minima positions to some extent in certain frequency ranges.

At not too distant further sockets, one may also just add a termination circuit which is then similar to the simplified circuit with bridge tap termination in Section V. We terminated the L-N connections (again behind a coupling capacitor-balun combination) with different capacitors. Figure 9 shows the corresponding results.

We recognize the shift of minima especially in a certain frequency range (marked in Fig. 9 with a dashed box).

From results with varying terminations either at a separate socket or at another loop, it becomes obvious that the transmission coefficients S_{12} and S_{21} can be modified, especially, minima can be shifted. Since we see the frequencies of minima (or maxima) as the parameter to be quantized to map them to key sequence blocks, results show that the common *randomness* can be achieved in power-line connections.

The most important aspect is, however, that an eavesdropper experiences different channel properties to Alice or Bob. To investigate this, we placed Alice and Bob at sockets opposite of the room, while Eve was only 1.40 m away from Alice on the same cable (same location as used for the bridge tap termination in Fig. 9). The results are shown in Fig. 10. Even with such a close distance, the channel between Bob and Alice and the one between Bob and Eve are already different, although, of course, visibly related still. As in the wireless case, the further away the eavesdropper is placed from the legitimate users, the better.

VII. Some ideas for key generation and reconciliation

From our first results, it is visible that the range of interest with shiftable minima has to be determined in advance. This will require some initialization phase where power-line modems will agree on the range. Thereafter, we can linearly quantize the range and map quantization regions to bit patterns. We have to assume small deviations between the Alice-Bob and Bob-Alice measurements, since hardware imperfections, nonlinearities, and noise can still make S_{12} deviate from S_{21}, slightly. This asks for key reconciliation, ideally without jeopardizing secrecy. One could, e,g., introduce guard bands instead of quantization boundaries, which would mean not accepting measurements where a minimum ends up in a guard interval. Additionally, one can use Slepian-Wolf coding, publicly sending redundancy for key correction. However, in the case here, one could simply publicly announce a shift of the quantization grid, so that minima will always be located in the middle of the quantization interval. These shifts are then restricted to half the quantization interval size. Knowing the shift will not provide any useful information to an eavesdropper, since the actual interval will not be communicated.

VIII. Conclusions

Physical-layer key generation requires common randomness of a legitimate channel, secure from eavesdropping. We have shown via simulation and actual measurements that, as expected, the power-line channel is reciprocal with, e.g., $S_{12} = S_{21}$. Additionally, the channel can be randomized by, e.g., varying (reactive) loads at unused wire pairs or at another (not too distant) socket. Practically, reactive loads have to be realized by active circuitry to enable fast changes. Inside a power-line modem, just putting reactive loads to unused pairs is very simple, just requires a balun coupling with some additional protective measures against high-voltage peaks that every power-line modem has.

We have also shown that the channel to an eavesdropper is significantly different from the legitimate one, even if the eavesdropper access point is just a meter away from Alice or Bob.

Minima of the transfer scattering parameter appear to be usable to be linearly quantized in frequency with a mapping to bit patterns, which will then resemble pieces of a longer cryptographic key. Key reconciliation can just be realized by a publicly communicated shift of the quantization grid, such that minima are located sufficiently far from quantization boundaries.

The results of the paper outline that also power-line connections offer the possibility for physical-layer key generation, which can be realized easily with IoT power-line devices.

References

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

[2] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography – Part I: Secret sharing," *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1121–1132, July 1993.

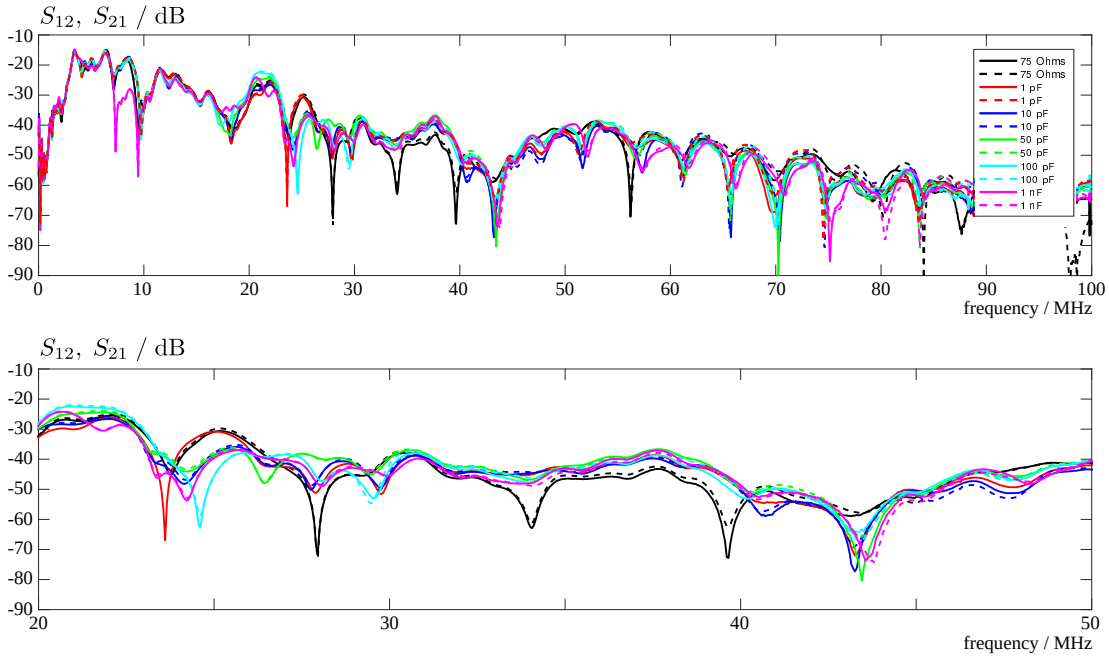

Fig. 8. Modifying the transfer characteristics on the L-N loop by one-sided termination at N-PE with 75 Ohms or different capacities; A-B and B-A directions are shown as solid or dashed, respectively.

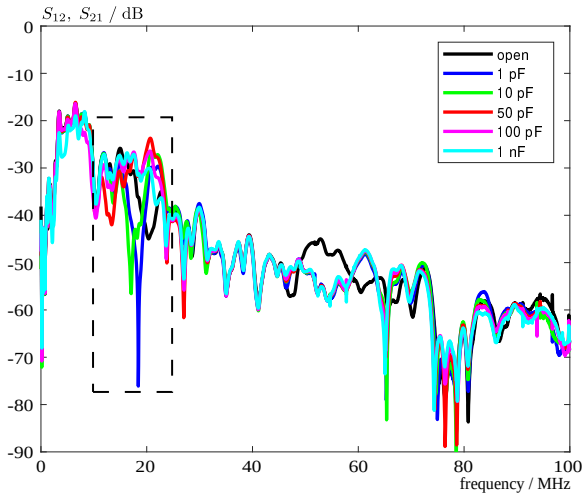

Fig. 9. S_{21} between Alice and Bob with different terminations at another socket 1.4 m from Alice

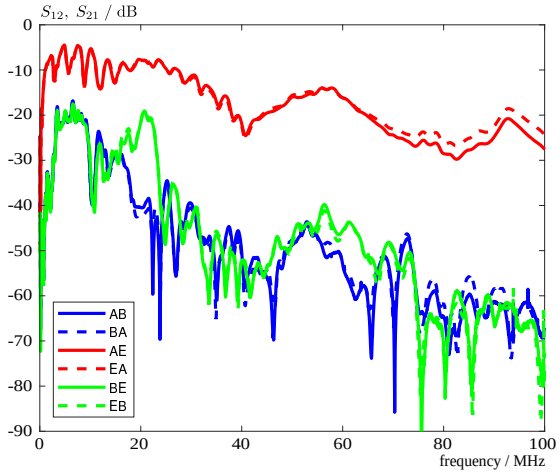

Fig. 10. S_{12} and S_{21} for pairings Alice-Bob, Alice-Eve, and Bob-Eve

[3] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[4] 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.

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

[6] 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.

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

[8] 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.

[9] A. M. Tonello and F. Versolatto, "Bottom-up statistical PLC channel modeling – Part I: Random topology model and efficient transfer function computation," *IEEE Transactions on Power Delivery*, vol. 26, no. 2, pp. 891–898, 2011.

[10] 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.