Common randomness for physical-layer key generation in powerline transmission

Werner Henkel, Abderraheem M. Turjman, Hisham K. H. Qanadilo, and Uwe Pagel

Jacobs University Bremen
Email: werner.henkel@ieee.org

***Abstract*—Physical layer key generation is based on common randomness at both ends of a legitimate link, safe from eavesdropping. We show that powerline channels not only show the desired reciprocity of the channel, but also can be randomized to be able to create more and more key bits. We show a simulation of a simplified network element with only a single bridge tap, which already shows the required behavior. Additionally, we show measurement results from inside a room between outlets to outline that practically, transfer functions can also be modified. Simulations and measurements indicate the reciprocity together with the possibility to randomize the transfer function by operations using random terminations at another outlet or at another line at one of the outlets of the legitimate link.**

I. Introduction

Reciprocity of every two-port network is given by

$$Z_{12} = Z_{21}\,,\; Y_{12} = Y_{21}\,,\; \det \mathbf{A} = 1\,,\; S_{12} = S_{21}\,. \quad (1)$$

In contrast to a dedicated twisted pair (TP and UTP phone wires, Ethernet cables), a powerline network has branching connections, so-called bridge taps, leading to notches at certain frequencies and non-homogeneous and non-symmetric properties, also of terminations, lead to coupling effects between pairs, much stronger than the NEXT and FEXT (Near/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} and are location dependent, can be utilized for key generation by quantizing the frequency scale within a certain range.

We will show that transfer functions can be modified using terminations at unused pairs or terminating the line at a bridge tap with arbitrary impedances. Randomly changing those loads will lead to randomly changing transfer functions.

One should note that a powerline cable has at least three wires, L, N, and PE, which means that the description will require to have two ports on both sides, meaning a 4×4 S-parameter matrix. We measured those parameters of sockets and switches with a 2-port vector network analyzer (VNA) using baluns and terminating unused ports with 75 Ohms.

II. Simulation results for a bridge-tap configuration

Using the simulation package by Gruber and Lampe [1], [2], after some adjustment of ϵ_r to ensure the correct characteristic impedance, we studied a powerline link including a branching to another socket with or without an appliance connected or with intentional terminations at that location.

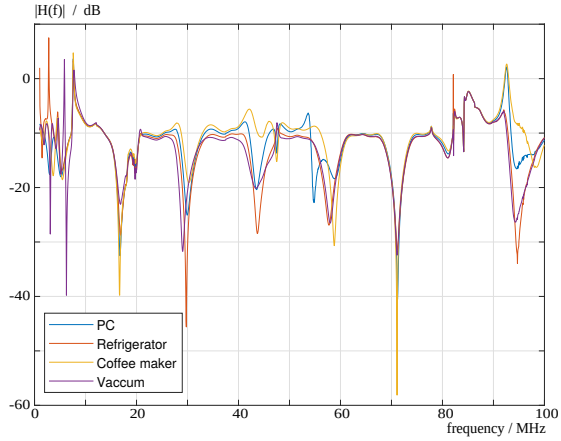

Fig. 1. Transfer functions with different appliances at a branching line

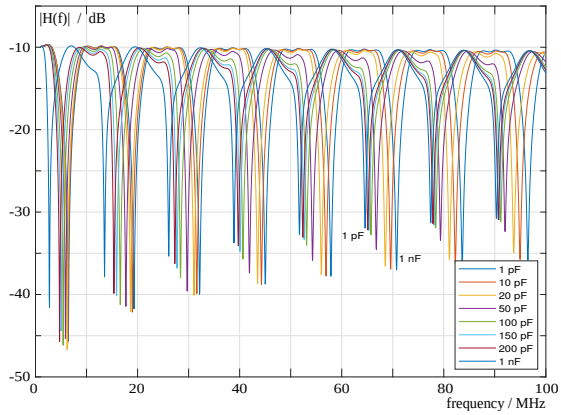

Fig. 2. Transfer functions with different capacitive loads at the branch end

At the branch end, we added a socket and cable connection to different appliances like PC, refrigerator, coffee maker, and vacuum cleaner [3]. Figure 1 shows that actually the socket itself has a stronger influence than the appliances. Nevertheless, local minima are shifting in certain frequency ranges. Figure 2 shows results with different capacitors connected to the end of the branch.

Without showing here, an eavesdropper experiences different transfer functions.

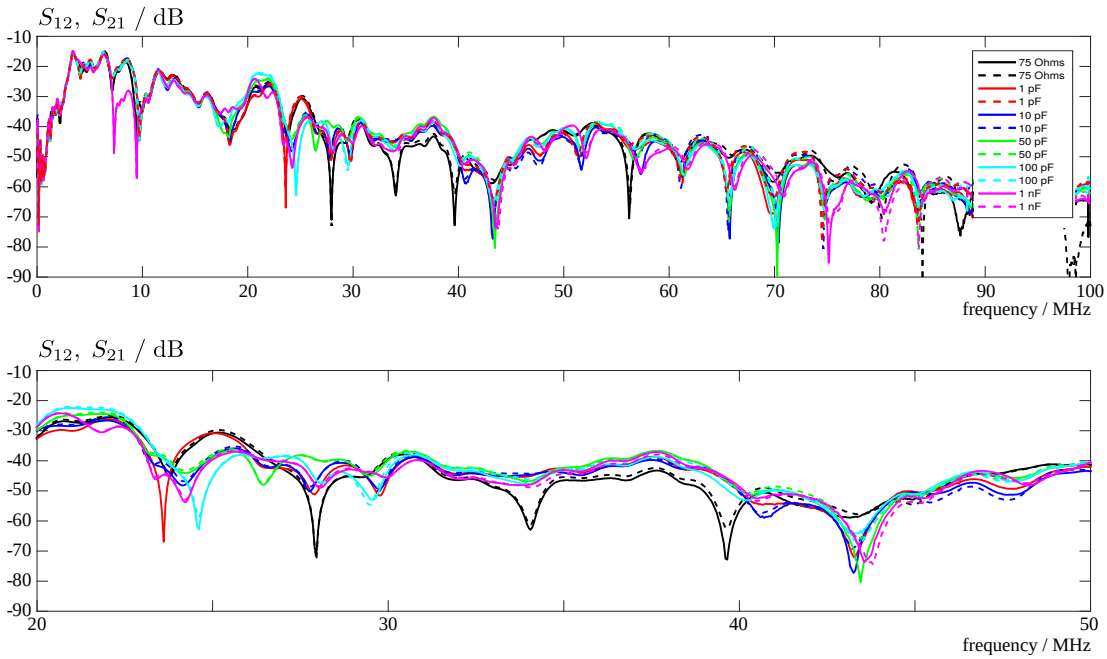

Fig. 3. Modifying the transfer characteristics on the L-N loop by one-sided termination at N-PE with 75 Ohms or different capacities; A-B and B-A directions are shown as solid or dashed, respectively.

III. 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 while measuring the L-N loop. This allows to change minima positions to some extent in certain frequency ranges. Figure 3 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.

At not too distant further sockets, we terminated a bridge tap at L-N with different capacitors. Figure 4 shows the corresponding results.

We recognize the shift of minima especially in a certain frequency range (marked in Fig. 4 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 powerline connections.

Also in measurements, the eavesdropper channels are significantly different.

IV. Conclusions

We could show that indeed common randomness can be obtained in powerline connections using the reciprocity $S_{12} = S_{21}$ together with random (reactive) loads at bridge taps or at the end of other loops in the same cable.

We envisage determining keys by quantizing the frequencies in certain ranges and determine the location of notches, i.e., map regions of notch locations to key bit patterns. Key reconciliation can be obtained very easily by a shift of the quantization thresholds such that the notches do not end up close to quantization boundaries. This shift can be communicated over the public channel without jeopardizing secrecy.

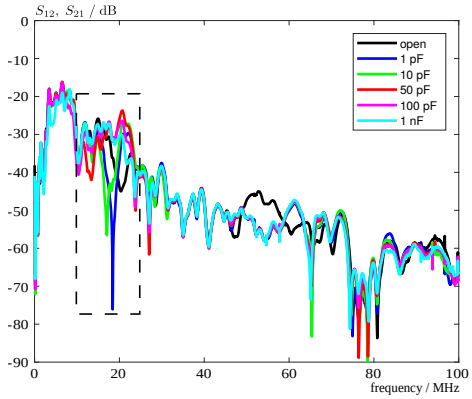

Fig. 4. S_{21} between Alice and Bob with different terminations at another socket 1.4 m from Alice

Acknowledgment

This work was funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – HE 3654/27-1. We thank Lutz Lampe at UBC for his support regarding his simulation tool.

References

[1] F. Gruber and L. Lampe, "On PLC channel emulation via transmission line theory," in *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] J.-C. Le Bunetel, C. Dhia, 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, Aug. 2012.