Reciprocity for Physical Layer Security with Wireless FDD and in Wireline Communications

Werner Henkel, *senior member, IEEE*, Oana A. Graur, Nazia S. Islam, Uwe Pagel, Navdeep Manak, Onur Can

Jacobs University Bremen
Bremen, Germany
Emails: werner.henkel@ieee.org, {o.graur, n.islam}@jacobs-university.de

***Abstract*—The reciprocity of the channel transfer functions between legitimate users changing randomly delivers the common randomness used in physical-layer key generation. Time-Division Duplexing (TDD) provides this symmetry of the bidirectional channel measurements, despite of uncorrelated noise on both sides and possible hardware imperfections. We now show that also Frequency-Division Duplexing (FDD) yields a usable symmetry as far as the direction of arrival is concerned. Even in wireline communications, be it over power lines or twisted pairs, transfer and far-end crosstalk functions provide useful symmetries, where especially key generation for power line communication may become important for IoT applications.**

I. Introduction

Physical layer security comes in two flavors, one known as Wyner's wiretap channel [1] making use of differences in the channel capacities (secrecy capacity) of the legitimate relative to the eavesdropper channels. We instead use physical properties for key generation that provide a so-called common randomness. This common randomness was known from Time-Division Duplexing (TDD) [2]–[5] assuming the channel probing in the two directions to be within the coherence time. The reciprocity of the channel results in similar measurements of the transfer function, in case of flat fading, a complex channel gain per carrier. The measurements are not exactly the same due to uncorrelated noise and hardware imperfections. Quantization schemes [6] leading to parts of a key sequence have to be combined with key reconciliation schemes, such as the introduction of guard bands [7] or Slepian-Wolf coding [8], [9]. Finally, privacy amplification [10] will be required to counteract leakage to possible eavesdroppers.

Maurer, Ahlswede, and Csiszár describe bounds for the secret key capacity [11] as

$$I(A;B) - \min\{I(A;E), I(B;E)\} \leq C_s \leq \qquad (1)$$
$$\leq \min\{I(A;B), I(A;B|E)\} \ ,$$

where A and B denote the legitimate users Alice and Bob, respectively, and E is the eavesdropper Eve.

Although we also contributed to TDD physical layer key generation and reconciliation, the topic here is devoted to other opportunities, namely addressing FDD and also wireline communications, especially, power line communications and also showing possibilities for twisted pairs, although power lines appear to be an interesting medium for the Internet of Things (IoT) and also production control (Industry 4.0).

So far, FDD was considered not to provide the required symmetry, since definitely, the frequency response will not be identical in different frequency bands. However, triggered by works of Palleit and Weber [12], we looked into the directions of arrival (DoA) as a possible candidate. They tried to determine the frequency response in the opposite channel in another frequency band by estimating the incident wave components, i.e., their directions of arrival (DoA) and times of arrival (ToA). The DoA seemed to show the necessary symmetry. Wave components are reflected at the same objects independent of the direction, hence follow the same paths in both directions. Surfaces might change the amplitudes, which is less the case when the considered duplex bands are close. We found that indeed the DoA seems to show a decent reciprocity and could be quantized to deliver key components.

Power lines, at first sight, appear too deterministic to use them for key generation. However, inhouse, a power line network is not just a straight cable connection between two outlets, but has bridge taps to appliances and sockets that might be connected or left open. Open-ended bridge taps yield, of course, periodic notches in the transfer function. Overall, power line transfer functions are very irregular and due to switched appliances, might also offer some degree of randomness. However, in here, we do not yet randomize the channel, which will be a future topic. We just show that transfer functions between two outlets are almost the same in both directions and sufficiently different to other outlets, which might be used for eavesdropping.

Twisted pairs are much more homogeneous than power lines, especially, without bridge taps. The transfer function follows a very deterministic model, hence, not usable for key generation purposes. There, the far-end crosstalk (FEXT) function will be shown to provide the desired symmetries and protection again eavesdropping.

This paper is not to be seen as final treatment for all those channels, but it outlines that other communication channels likewise provide symmetries that can be used for physical layer key generation. For FDD and the power line case, we also shortly discuss quantization, guard intervals, and the mapping to key bit patterns.

The structure of the paper is as follows. Section II discusses FDD DoA estimation using the MUSIC (MUltiple SIgnal Classification) algorithm, followed by a treatment of the power line case in Section III and twisted pairs in Section IV. As an example based on a power line transfer function, Section V outlines how simple quantization and

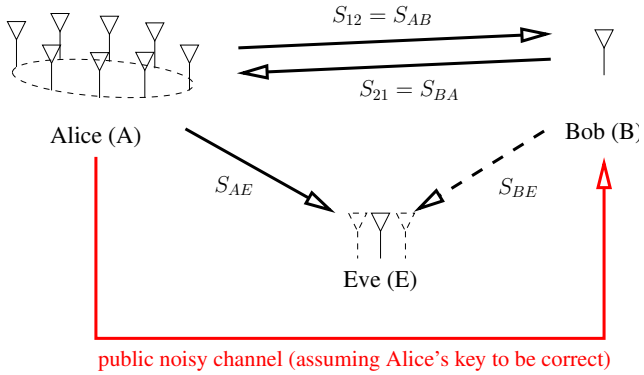

Fig. 1. Key generation and reconciliation setup where Alice uses an antenna array (circular) for angle estimation and Bob uses a single dipole. Eve might have a single dipole, too, not excluding multiple antennas, as well. The channel BE is dashed, since it would not allow for determining angles of arrival. The public channel to exchange reconciliation information is shown in red.

guard intervals and also the mapping to key bit patters can be realized. We conclude with Section VI.

II. Common randomness through DoA estimation using the MUSIC algorithm

Figure 1 shows our setup for key generation, eavesdropping, and key reconciliation, where the latter is not discussed in here, but in already mentioned earlier publications on Slepian-Wolf coding with LDPC codes, e.g., [9], where parities or syndromes are provided through a public channel.

The wireless channel is known to be reciprocal. This also means that DoA estimation leads to the same result regardless in which direction the measurements are carried out. The DoA estimations will also roughly be the same, even if the frequency bands are not the same. However, they should be close, not to encounter frequency dependencies of reflectors and antennas.

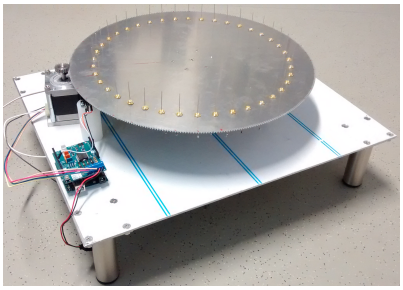

Fig. 2. Circular antenna array

We use a circular array (see Fig. 2) for the measurements with 40 antennas spaced at roughly $\lambda/3$ and first use neighboring 5 MHz channels around 2.3 GHz. We chose a circular array (against a single dipole) to avoid ambiguities that one would encounter in a linear array, limiting the angular range to 180 degrees. The circular array is a "virtual" one, since only one antenna is actually connected and the other antenna positions will be measured by moving the antenna disc by the corresponding angle. The only drawback of the "virtual" arrangement is that positions have to be measured one after another and the room situation should not change during the measurement cycle. Hence, this requires remote control from another room. Otherwise, it is suitably providing results that would also be obtained with an actual multi-antenna system. We measure scattering matrix parameters S_{12} and S_{21} (forward and reverse gains, respectively) to realize the two directions using a standard vector network analyzer.

For DoA estimation we used the MUSIC algorithm [13]. Other alternatives would be standard beam-forming, ESPRIT [14], or SAGE [15], where the latter was also used in [12] that we have already mentioned. ESPRIT usually uses two submatrices of the steering matrix and with it two subsets of the antenna sets as, e.g., shown in [16]. This is problematic with a circular array due to a different steering matrix structure. [17] provides a kind of spatial interpolation to obtain the desired components. MUSIC does not require such steps. In the following, we will shortly sketch the MUSIC algorithm.

The received signal E_s of one source component $s(t)$ can be written as

$$E_s(\mathbf{r}, t) = s(t) e^{j(\omega t - \mathbf{r}^T \mathbf{k})} , \tag{2}$$

where $\mathbf{r}$ denotes the position of the receiving antenna (also transmitting antenna due to reciprocity) and $\mathbf{k}$ is the wave number. We express $\mathbf{k}$ by

$$\mathbf{k} = k(\cos\theta, \sin\theta^T) , \quad k = \frac{\omega}{c} . \tag{3}$$

In case of a circular array with L antennas and the antenna index l, we express

$$\mathbf{r}_l = R \cdot (\cos(2\pi(l-1)/L), \sin(2\pi(l-1)/L))^T . \tag{4}$$

Multiplying $\mathbf{r}_l^T$ and $\mathbf{k}$ from (4) and (3) according to (2) yields the exponential function

$$a_l = e^{-j\frac{2\pi}{\lambda} \cdot R \cdot \cos(\theta - 2\pi\frac{l-1}{L})} , \quad l = 0, ..., L-1 . \tag{5}$$

This is a component of the so-called steering vector $\mathbf{a}$. When computing a spatial correlation matrix

$$\begin{aligned} \mathbf{R} &= E\left\{\mathbf{x}(t)\mathbf{x}^H(t)\right\} && (6)\\ &= \mathbf{A}E\left\{\mathbf{s}(t)\mathbf{s}^H(t)\right\}\mathbf{A}^H + E\left\{\mathbf{n}(t)\mathbf{n}^H(t)\right\} && (7)\\ &= \mathbf{U}\mathbf{\Lambda}\mathbf{U}^H \\ &= \mathbf{U}_S\mathbf{\Lambda}_S\mathbf{U}_S^H + \mathbf{U}_N\mathbf{\Lambda}_N\mathbf{U}_N^H , && (8) \end{aligned}$$

it is split it into signal "S" and noise "N" components. Here, $\mathbf{x}(t)$ is the received vector of length L, $\mathbf{A}$ is an $L \times M$ matrix, $\mathbf{s}$ the source vector of M components and $\mathbf{n}$ a noise vector of length L.

The so-called MUSIC spectrum is then computed as

$$p_{\text{MUSIC}}(\theta) = \frac{1}{\mathbf{a}^H(\theta) \cdot \mathbf{U}_N \, \mathbf{U}_N^H \cdot \mathbf{a}(\theta)} \tag{9}$$

or alternatively as

$$p_{\text{MUSIC}}(\theta) = \frac{\mathbf{a}^H\mathbf{a}}{\mathbf{a}^H(\theta) \cdot \mathbf{U}_N \, \mathbf{U}_N^H \cdot \mathbf{a}(\theta)} \tag{10}$$

The steering vector $\mathbf{a}$ in (9), (10) is dependent on the angle θ, which is varied between 0 and 360 degrees. Maxima are obtained at those angles where the steering vector is orthogonal to the noise eigenvectors. The signal and noise eigenvectors can, e.g., be separated according to the corresponding eigenvalues or estimating the number of signal components according to [18]–[22].

Figures 3 to 5 show examples of MUSIC spectra obtained by measuring S_{12} and S_{21} in neighboring frequency bands.

Figures 4 and 5 differ by moving the single dipole antenna to another location, thereby representing an eavesdropper position. The MUSIC spectra show some rough relation, due to the same reflectors being present. However, the eavesdropper will not be able to easily predict the behavior. If necessary, reconfigurable antenna approaches [2], [23] can be used to further randomize the channel.

For figures 3 to 5, we used directly neighboring 5 MHz bands. It is expected that the relation between the MUSIC spectra for both directions becomes less pronounced with more distant bands. Figures 6 and 7 show two examples with a spacing of 20 MHz in between the two FDD 5 MHz bands. The relation is still visible, but, as expected, the use of distant FDD spectra seems less suited for key generation.

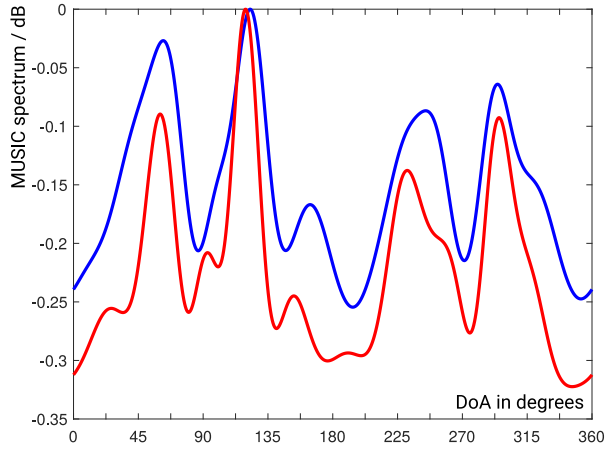

Fig. 3. MUSIC spectra determined from scattering parameters S_{12} and S_{21}, measurements taken in neighboring frequency bands at 2327-2332 MHz and 2332-2337 MHz, respectively

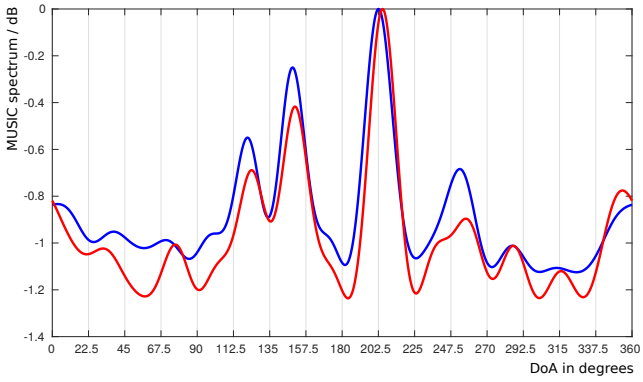

Fig. 4. MUSIC spectra obtained as in the previous figure, but different environment

We observe the maxima representing the angles of arrival. We limited ourselves to the azimuth, but one can, of course, extend the treatment with the elevation. The spatial correlation function was directly computed in frequency domain.

III. Reciprocal Power Line Transfer Functions

Power line inhouse networks come in very different topologies with bridge taps to appliances or simply to open sockets. Open-ended bridge taps, of course, mean shorts at periodic frequencies. Hence, one expects very different transfer functions with lots of variation over frequency between power outlets. Eavesdropping devices will experience different transfer functions to legitimate devices. With

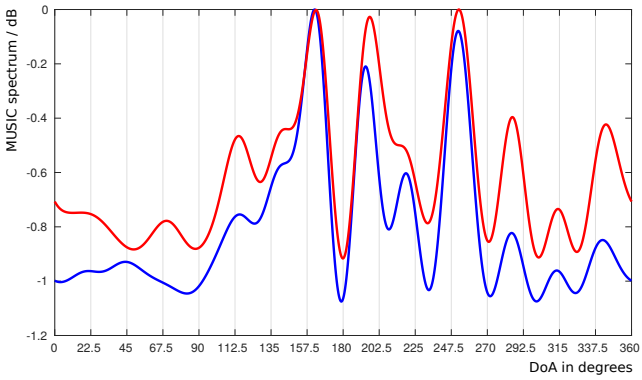

Fig. 5. MUSIC spectra obtained as in the previous figure, with different location of the single dipole to realize an eavesdropper measurement, keeping Alice's position

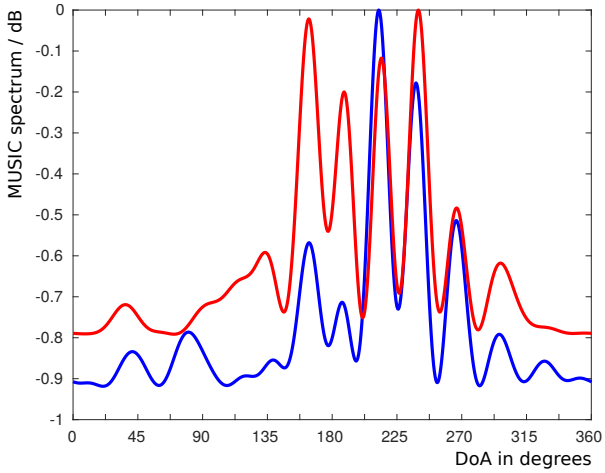

Fig. 6. MUSIC spectra from measurements taken at frequency bands with a 20 MHz spacing, 2317-2322 MHz and 2342-2347 MHz

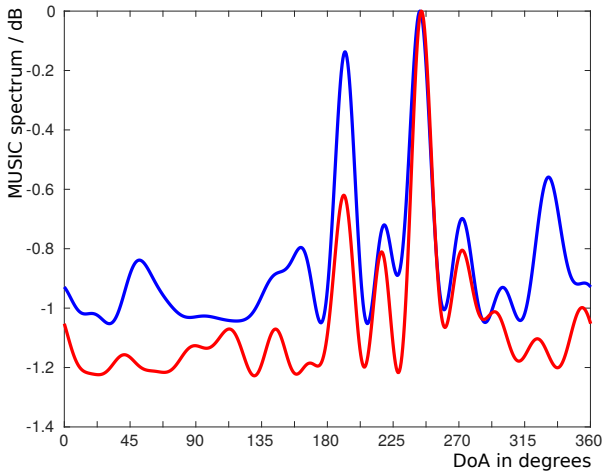

Fig. 7. MUSIC spectra from measurements taken at frequency bands with a 20 MHz spacing, 2317-2322 MHz and 2342-2347 MHz

dedicated coupling devices blocking the mains frequency and adapting to the characteristic impedance we measured between different power outlets. In the paper, we only show the N-PE pairing, but the L-N pair delivers likewise usable results. We did so far not measure between different L lines in a three-phase system, but those pairings can, of course, as well be used. Figure 8 shows that the transfer functions are very related for the two directions offering the desired reciprocity. In Fig. 9, we applied a special

smoothing and equalization (leveling) function and limited the frequency range to up to 30 MHz, which typically shows good symmetries. We recognize that after such a modification, one could use the positions of maxima for key generation just as in the MUSIC spectrum of the previous section. One might first think of using minima, but they are more vulnerable to interference. From the figures, where A, B, E denote different sockets, one clearly recognizes the symmetries of the bidirectional transfer functions, e.g., A→B and B→A and the differences to transfer functions to other (eavesdropping) sockets, A→E. This ensures that an eavesdropper experiences a sufficiently different transfer function compared to a legitimate channel between a pair of different sockets, making attacks difficult, if not impossible. In our measurements, selecting one socket to be E is, of course, arbitrary. That's why we also show the transfer function $E \rightarrow A$, which is, of course, not the channel direction of a passive eavesdropper. If sockets are closely located on the same cable, just as in the wireless case, differences will become smaller. Figure 10 shows results at outlets along the same cable spaced by roughly one meter.

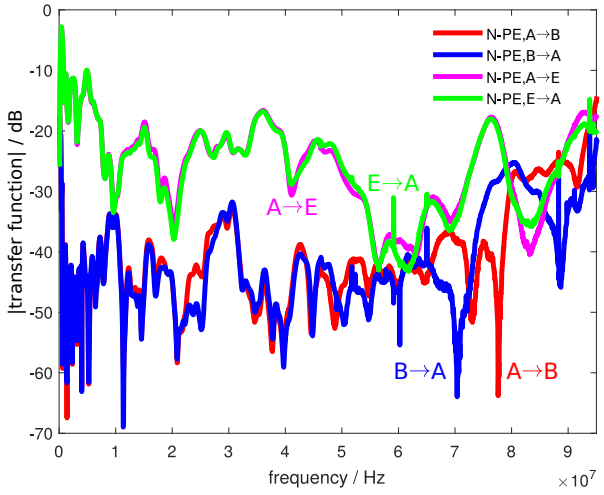

Fig. 8. Transfer functions to and from different outlets (100 kHz - 95 MHz)

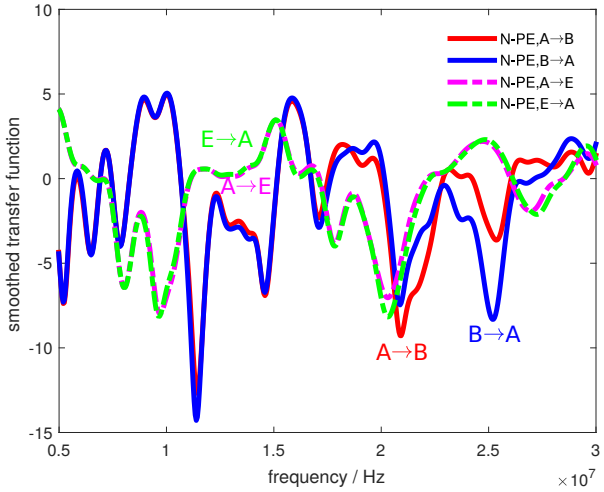

Fig. 9. Transfer functions to and from different outlets (100 kHz - 30 MHz) after smoothing and leveling

For physical-layer key generation, not just reciprocity is required, but also randomness ("common randomness").

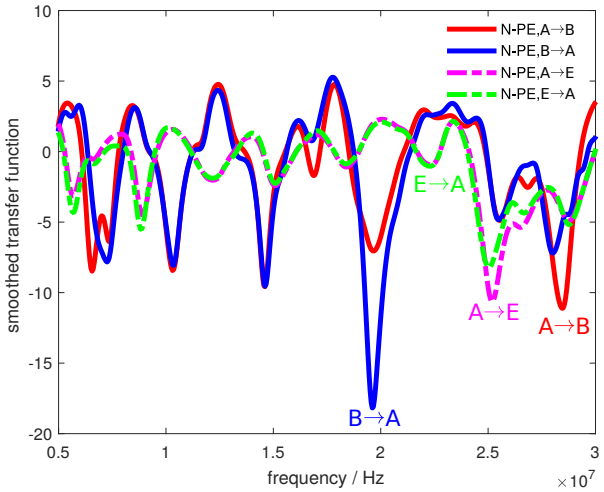

Fig. 10. Transfer functions between closely located outlets (100 kHz - 30 MHz) after smoothing and leveling

Switched appliances and artificial changes certainly allow for some randomization, which will require further studies.

IV. Reciprocal FEXT

The FEXT function is another option for reciprocity in case of an isolated wire pair, be it twisted pairs (unshielded or shielded, UTP, TP), Ethernet, or power lines. Power line installations, however, typically have bridge taps and then, the FEXT function is not as symmetric any more. Apart from the reciprocity, we would also require that the overall FEXT function cannot easily be computed from partial knowledge of an eavesdropper.

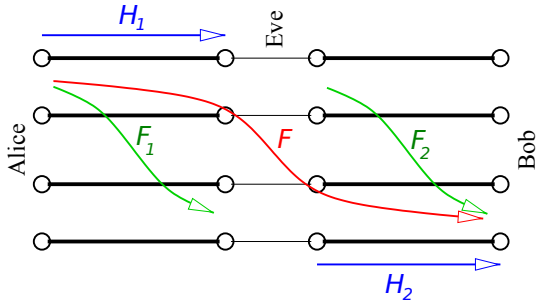

Fig. 11. Arrangement and measured functions of loop segments

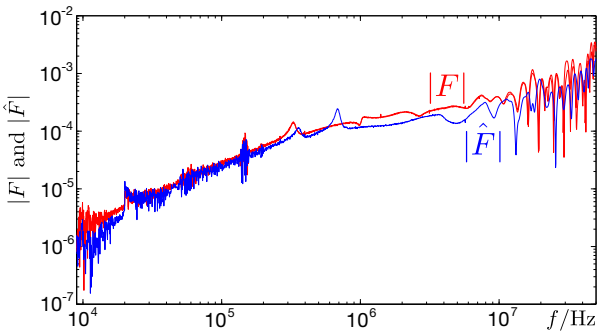

Fig. 12. FEXT function and an eavesdropper's estimate (CAT 5)

For convenience and to illustrate the principle, we show FEXT functions measured at a 25 m / 50 m twisted pair arrangement (CAT 5) shown in Fig. 12. Note, since the measurements and eavesdropper estimates are very symmetric, the plotted two curves in the same color are exactly

onto each other. In red, two-sided FEXT-measurements are shown, while the blue $\hat{F}$ curves are closest estimates of a wiretapping eavesdropper. The estimate of the overall FEXT function results from

$$F \approx \hat{F} = F_1 \cdot H_2 + H_1 \cdot F_2 \ , \tag{11}$$

making use of the segment transfer functions H_1 and H_2 and the segment FEXT functions F_1 and F_2 (see Fig. 11) that the eavesdropper might have access to, when examining the transfer and FEXT functions of the segments. The assumption for Eq. (11) is that the FEXT-coupled component through F_1 has to traverse the transfer function H_2 and likewise, the F_2-coupled component passes through H_1 and both together make up the overall FEXT coupling function F.

It is clearly visible that the estimate shows the rough trend, but definitely not the same fluctuations and notches, thereby allowing secure key generation. FEXT functions are stronger in power cables, since they are not as symmetric and not twisted as their telephone and Ethernet counterparts. Although we do not show the corresponding measurements, they are almost perfectly reciprocal, as well.

Although this paper is not yet discussing randomization in detail, in the case of FEXT, randomly modifying coupling/grounding of/to other loops in the neighborhood is an option thereby modifying FEXT.

V. Quantization, Key Reconciliation, and Mapping

Figure 13 sketches the quantization in case of a power line measurement. The white spaces indicate guard bands instead of thresholds that can be used to realize some key reconciliation that can be combined with Slepian-Wolf coding. The maxima are marked and the crossed-out marking indicates a maximum falling inside a guard interval.

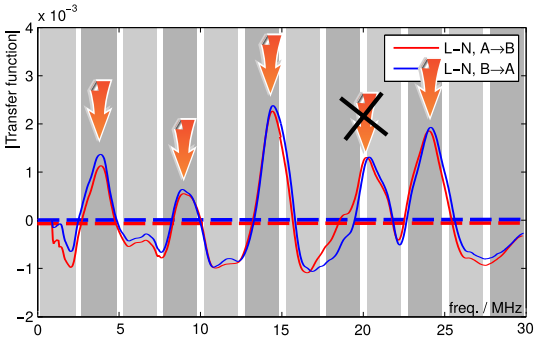

Fig. 13. Quantization of maxima positions with guard bands

For mapping the maxima positions to bit patterns of key sequences, one will have $\binom{n}{k}$ possible maxima positions, where n denotes the number of quantization intervals, k the number of maxima that result from the given thresholds. $\binom{n}{k}$ is typically not a power of 2, hence, one cannot directly tabulate the maxima pattern to a bit pattern of fixed length. We list all $\binom{n}{k}$ possible maxima patterns according to a binary representation of $\binom{n}{k}$,

$$\binom{n}{k} = \sum_{i=0}^{L} b_i 2^i \equiv b_L b_{L-1} ... b_1 b_0 \tag{12}$$

with b_L denoting the highest nonzero component (MSB) of the binary representation. For the conversion table, we concatenate lists of binary patterns of lengths $2^{b_i} \forall b_i \neq 0$. By doing so, we obtain the list length that is actually required for patterns of weight k to map it into a binary format. Those binary words do then, of course, have different lengths, which yields a somewhat irregular mapping table. However, the procedure ensures equal probability of all binary key sequences which is essential for cryptographic applications.

VI. Conclusions

We showed that wireless TDD transmission is not the only channel suitably providing a reciprocity usable for physical-layer key generation. For FDD, we used the direction of arrival estimated by means of the so-called MUSIC spectrum derived from S_{12} and S_{21} bidirectional measurements of a circular antenna array against a single dipole that we found is only slightly dependent on the direction of the measurements. The maxima of the MUSIC spectrum indicate the directions.

For the power line application, we measured the transfer function between power outlets, with some smoothing routine also leading to maxima whose location can be used for key generation purposes just as with the MUSIC spectrum in the FDD case. In case of a homogeneous cable, the far-end crosstalk function is fully reciprocal, too.

In all cases, given a certain distance [24]–[26] in the wireless case and also not at close vicinity along a power line cable, an eavesdropper would experience different channel properties, hence, different keys. In case of a homogeneous cable, an eavesdropper on the cable would also not be able to determine the exact FEXT function.

Quantization and the introduction of guard intervals for key reconciliation have been shown to be simple. Mapping the maxima locations in the MUSIC spectrum or power line transfer functions has been realized by tables with binary key vectors of different lengths determined by the binary representation of the number of combinations of maxima.

To optimize the procedures and determine the key-disagreement rate with and without guard intervals, many more measurements and simulations of the wireless channel (e.g. ray tracing) and also simulations of the power line inhouse network will follow. With the limited number of measurements, unfortunately, we are not yet able to determine key disagreement rates and leakage to eavesdroppers, quantitatively. Measurements with a network analyzer are time consuming and can hence only deliver an indication for the reciprocity properties. A transition to simulation is essential to collect the amount of data required to do statistics for quantitative evaluation. Such simulations and measurements with automated location changes of antennas and/or reflectors will be next steps.

Randomization of the channels has not been discussed much in this paper. Nevertheless, wireless randomization is either given by mobility itself or using randomly reconfigurable antennas. Randomization in power line or other wireline connections is certainly given by switched appliances, loads, random bridge taps, random coupling between wires or ground. Those aspects will be dealt with in later works, too.

REFERENCES

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

[2] J. Wallace, W. Henkel, O. Graur, N. Islam, R. Mehmood, R. Sharma, and A. Filip, "Physical-layer key generation and reconciliation," in *Communications in Interference Limited Networks*, Springer, 2016.

[3] A. Sayeed and A. Perrig, "Secure Wireless Communications: Secret Keys Through Multipath," in *2008 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP 2008)*, (Las Vegas), pp. 3013–3016, March 2008.

[4] J. Hershey, A. Hassan, and R. Yarlagadda, "Unconventional Cryptographic Keying Variable Management," *IEEE Transactions on Communications*, vol. 43, pp. 3–6, Jan 1995.

[5] R. D. Wilson, D. Tse, and R. A. Scholtz, "Channel Identification: Secret Sharing Using Reciprocity in Ultrawideband Channels," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 3-1, pp. 364–375, 2007.

[6] O. Graur, N. Islam, and W. Henkel, "Quantization for physical layer security," in *IEEE International Global Communications Conference (Globecom 2016)*, 2016.

[7] A. Filip, R. Mehmood, J. Wallace, and W. Henkel, "Variable guard band construction to support key reconciliation," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 8173–8177, May 2014.

[8] J. Etesami and W. Henkel, "LDPC code construction for wireless physical-layer key reconciliation," in *1st IEEE International Conference on Communications in China (ICCC)*, pp. 208–213, Aug 2012.

[9] 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, Dec 2015.

[10] U. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels- Part III: Privacy amplification," *IEEE Transactions on Information Theory*, vol. 49, pp. 839–851, Apr. 2003.

[11] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. No. August, Cambridge University Press, 2011.

[12] N. Palleit and T. Weber, "Frequency shift of the channel impulse response in MIMO-FDD systems," in *1st COST2100 Workshop "MIMO and Cooperative Communications"*, (Trondheim), June 2008.

[13] R. Schmidt, "Multiple emitter location and signal parameter estimation," *IEEE Transactions on Antennas and Propagation*, vol. 34, pp. 276–280, Mar 1986.

[14] R. Roy, A. Paulraj, and T. Kailath, "Estimation of signal parameters via rotational invariance techniques - ESPRIT," in *Military Communications Conference - Communications-Computers: Teamed for the 90's, 1986. MILCOM 1986. IEEE*, vol. 3, pp. 41.6.1–41.6.5, Oct 1986.

[15] B. H. Fleury, D. Dahlhaus, R. Heddergott, and M. Tschudin, "Wideband angle of arrival estimation using the SAGE algorithm," in *Spread Spectrum Techniques and Applications Proceedings, 1996., IEEE 4th International Symposium on*, vol. 1, pp. 79–85 vol.1, Sep 1996.

[16] R. Adve, "Direction of Arrival Estimation." https://www.comm.utoronto.ca/~rsadve/Notes/DOA.pdf.

[17] C. P. Mathews and M. D. Zoltowski, "Eigenstructure techniques for 2-d angle estimation with uniform circular arrays," *IEEE Transactions on Signal Processing*, vol. 42, pp. 2395–2407, Sept 1994.

[18] M. Wax and T. Kailath, "Detection of signals by information theoretic criteria," *IEEE Transactions on Acoustics, Speech, and Signal Processing*, vol. 33, pp. 387–392, Apr 1985.

[19] H. Akaike, *Information Theory and an Extension of the Maximum Likelihood Principle*, pp. 199–213. New York, NY: Springer New York, 1973.

[20] G. Schwarz, "Estimating the dimension of a model," *The Annals of Statistics*, vol. 6, pp. 461–464, Mar 1978.

[21] J. Rissanen, "Modeling by shortest data description," *Automatica*, vol. 14, pp. 465–471, 1978.

[22] H. van Trees, *Optimum Array Processing: Part IV of Detection, Estimation, and Modulation Theory*. Detection, Estimation, and Modulation Theory, Wiley, 2004.

[23] R. Mehmood and J. W. Wallace, "Wireless security enhancement using parasitic reconfigurable aperture antennas," in *European Antennas Propagation Conference*, (Rome, Italy), pp. 2761–2765, Apr 2011.

[24] W. Trappe, "The challenges facing physical layer security," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 16–20, 2015.

[25] X. He, H. Dai, W. Shen, and P. Ning, "Is link signature dependable for wireless security?," in *IEEE INFOCOM*, pp. 200–204, April 2013.

[26] X. He, H. Dai, Y. Huang, D. Wang, W. Shen, and P. Ning, "The security of link signature: A view from channel models," in *2014 IEEE Conference on Communications and Network Security (CNS)*, pp. 103–108, Oct 2014.