A Simple Physical-Layer Key Generation for Frequency-Division Duplexing (FDD)

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

2nd Maria Namachanja
Electrical Engineering
Jacobs University Bremen
Bremen, Germany
m.namachanja@jacobs-university.de

***Abstract*—Common randomness of channels offers the possibility to create cryptographic keys without the need for a key exchange procedure. Channel reciprocity for TDD (time-division duplexing) systems has been used for this purpose many times. FDD (frequency-division duplexing) systems, however, were long considered to not provide any usable symmetry. However, since the scattering transmission parameters S_{12} and S_{21} would ideally be the same due to reciprocity, when using neighboring frequency ranges for both directions, they would just follow a continuous curve when putting them next to each other. To not rely on absolute phase, we use phase differences between antennas and apply a polynomial curve fitting, thereafter, quantize the midpoint between the two frequency ranges with the two measurement directions. This is shown to work even with some spacing between the two bands.**

For key reconciliation, we force the measurement point from one direction to be in the midpoint of the quantization interval by a grid shift (or likewise measurement data shift). Since the histogram over the quantization intervals does not follow a uniform distribution, some source coding / hashing will be necessary. The key disagreement rate toward an eavesdropper was found to be close to 0.5. Additionally, when using an antenna array, a random permutation of antenna measurements can even further improve the protection against eavesdropping.

***Index Terms*—Physical-layer security, physical-layer key generation, frequency-division duplexing, FDD, secret-key capacity, key reconciliation**

I. Introduction

Physical-layer key generation is based on common randomness, where a channel should be reciprocal and additionally changing randomly. A mobile channel application with time-division duplexing (TDD) was long known to nicely provide this property, as long as the mobile is moving or a randomly reconfigurable antenna array randomizes the channel.

Overview works on physical layer security, especially related to TDD, are available in [1]–[4]. Reconfigurable antennas for channel randomization have been studied in [5]–[10].

Practically, the reciprocity is not perfect, due to independent noise on both sides of the channel and imperfect circuitry. After quantization to obtain key sequence patterns [11], this requires key reconcilation procedures. Those are typically based on guard bands and/or coding schemes, just as Slepian-Wolf coding [11]–[17].

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

Reciprocity is, of course, a general principle, not only for TDD wireless [18], but already known from two-port matrices, where $Z_{12} = Z_{21}$ in case of the impedance matrix, $Y_{12} = Y_{21}$ in case of the admittance matrix, and det(**A**)=1 in case of the ABCD matrix **A**. Note, the ABCD matrix links voltages and currents on the left to the ones on the right as

$$\begin{bmatrix} V_1 \\ I_1 \end{bmatrix} = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \begin{bmatrix} V_2 \\ -I_2 \end{bmatrix} .$$

When moving to RF (radio-frequency engineering), using scattering parameters instead, reciprocity means $S_{12} = S_{21}$ or for the so-called T-matrix, det(**T**)=1. S-parameters relate wave parameters (incident: $a_{1/2}$, reflected: $b_{1/2}$ in the form

$$\begin{bmatrix} b_1 \\ b_2 \end{bmatrix} = \begin{bmatrix} S_{11} & S_{12} \\ S_{21} & S_{22} \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \end{bmatrix} .$$

For further details on two-port matrices, the reader is referred to introductory ECE text books and likewise, standard RF text books introduce scattering parameters and related descriptions.

We find reciprocity in many channels, not only in wireless. However, when moving to frequency-division duplexing (FDD), the channels are, of course, not reciprocal, since one is operating in different frequency ranges. Nevertheless, what is still symmetrical are the angles of arrival [18], and since reciprocity holds for the same frequency range, we can assume some continuity between the FDD bands when they are close to each other. In here, we make use of that continuity through polynomial curve fitting, quantization of mid-points, quantization grid shift for key reconciliation, and possibly additional permutation for further protection against eavesdropping.

Maurer, Ahlswede, and Csiszár provided bounds for the secret key capacity [19]–[21] as

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

where A and B denote the legitimate users Alice and Bob, respectively, and E is the eavesdropper Eve. We will, for convenience, compute the key disagreement rates (KDR),

defined as the ratio of deviating bits $K_A(i)$ and $K_{B/E}(i)$, at Alice's and Bob's/Eve's ends, respectively, to the total number,

$$R_{\mathrm{KDR}} = \frac{1}{N_k} \sum_{i=1}^{N_k} K_A(i) \oplus K_{B/E}(i) \tag{2}$$

for the legitimate and the eavesdropping channels to evaluate the key generation and protection quality.

In Section II, we will describe the system setup and measurements taken. Section III shows the procedure to obtain the midpoint of phase differences between neighboring antennas linking neighboring frequency responses for S_{12} and S_{21}. Here, we apply polynomial curve fitting of the phase differences between antennas, quantizing that phase difference, and shift the quantization grid as a means for key reconciliation. When investigating the histogram over the quantization regions, this does not show a uniform distribution. This behavior will be derived and discussed in Section IV. Eavesdropping will be discussed in Section V, providing KDRs to a possible eavesdropper and proposing a simple additional measure. Results will be summarized in Section VI, discussing the KDR for the legitimate channels. Furthermore, dependencies on the spacing between the two FDD bands are outlined. The effect of antenna permutations is shown in terms of the KDR and histogram. We conclude with Section VII.

II. System and Measurement Setup

We were measuring S_{12} and S_{21} in two neighboring frequency ranges, 2.1875 to 2.1925 and 2.1925 to 2.1975 GHz, respectively. Alice was realized as a linear circular antenna array with a radius of 14,568 cm and 40 antennas. This circular array could be rotated in a remotely controlled fashion thereby allowing for 40 automatic S_{12} and S_{21} measurements. In earlier works, we had used measurements with the array to, e.g., apply the MUSIC algorithm for direction of arrival estimation and use the locations of maxima of the MUSIC spectra for key generation [18]. Here, we simplify the key generation by just assuming a certain continuity of the phase differences between two antenna measurements between the two frequency ranges. The reciprocity is only indirectly used namely by knowing that it should not matter, if one considers S_{12} or S_{21}. We are then counting on the continuity of those functions. From one measurement cycle, we obtain phase differences of 40 neighboring antenna pairs, but one can also use other antenna pairings, which is then used to generate more key sequences and additionally protect against eavesdropping as will be discussed later.

For the results presented in here, we measured in house in very different environments like lab, corridor, regular home environments, basement, garage, sometimes even with walls or doors blocking transmission, even to the point, where a steel door was in between transmit and receive antennas. A part of the measurements was ensuring the same height of transmit and received antennas, i.e., without elevation, others had a totally random placement. In total we had 13 major locations, where the antenna array ("Alice") was fixed and the single antenna ("Bob" or "Eve") was randomly placed at 10 to 13 different positions. At the same major locations, Bob and Eve were randomly taken from the individual single antenna locations.

III. Key Generation by Curve-Fitting, Quantization, and Grid Shift for Key Reconciliation

Our intention was to come up with a low complexity approach for key generation that would work for directly neighboring FDD frequency ranges. Anyhow, also our results applying direction-of-arrival (DoA) estimation [18] showed that also there, frequency bands should not be too far apart. Investigating measurements of S_{12} and S_{21} in neighboring 5 MHz bands showed that one can approximate the frequency behavior of the phase difference between the transmission characteristics of neighboring antennas with a 2nd-order polynomial curve fitting. In [22], some curve fitting approach was also used, but there to improve results for TDD-based key generation.

Some exemplary curve fitting result are shown in figures 1 to 3 as green curves for both segments. One would assume a direct continuation between the S_{12} and S_{21} phase difference segments as in Fig. 2, due to reciprocity. Despite of having calibrated the VNA (vector network analyzer), occasional non-ideal behavior like in Fig. 1 is possible and within the tolerance range of the instrument.

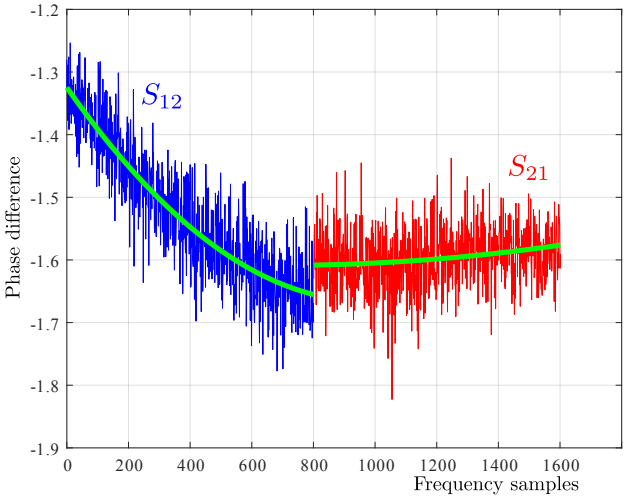

Fig. 1. Phase difference between neighboring antennas and curve fitting for S_{12} and S_{21} in neighboring frequency ranges (Example 1)

From the polynomial curve fit, we determine the phase difference at the merging point of the two FDD bands. The phase difference is quantized, where, as an example in Fig. 4 we used 8 intervals, i.e., a linear quantizer with 3 Bits. In that figure, one can realize that, by moving the quantization grid (or equivalently, the data), one of the measurements is moved into the middle of a quantization interval. This amount of shift is publicly communicated, such that especially the legitimate counterpart can likewise adjust the quantization grid

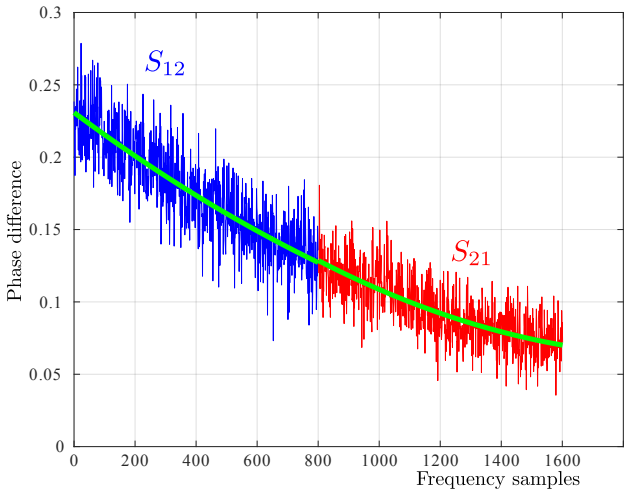

Fig. 2. Phase difference between neighboring antennas and curve fitting for S_{12} and S_{21} in neighboring frequency ranges (Example 2)

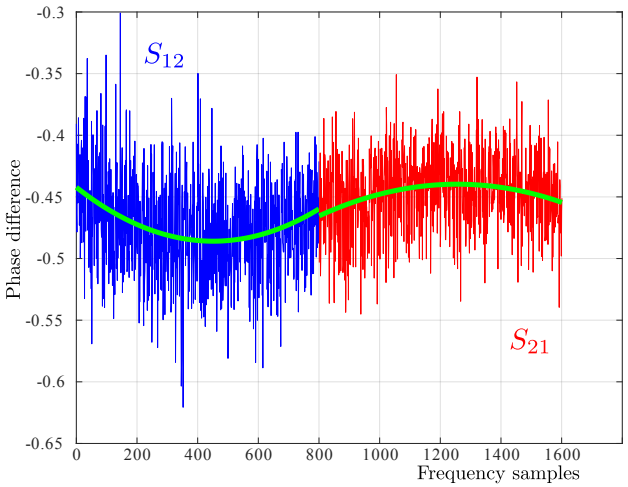

Fig. 3. Phase difference between neighboring antennas and curve fitting for S_{12} and S_{21} in neighboring frequency ranges (Example 3)

(or measurement data). This is already the first stage of key reconciliation to reduce the key disagreement rate. On the right of the figure, Gray-coded key bit patterns are listed. The Gray coding ensures single-bit changes when crossing quantization boundaries.

Unusable measurements we conclude from too low received amplitude and correspondingly very noisy phase measurements. We rejected measurements when the received amplitude was below a certain threshold or when the variance of the phase relative to the fitted polynomial exceeded a certain value. There is a trade-off between efficiency, i.e., the share of valid keys, and the key disagreement rate.

Further key reconciliation steps and possibly following privacy amplification [19]–[21] are out of the scope of this paper. One may use Slepian-Wolf coding based approaches like in [14] for further key reconciliation. To avoid leakage to an eavesdropper, especially, due to communicated redundancy

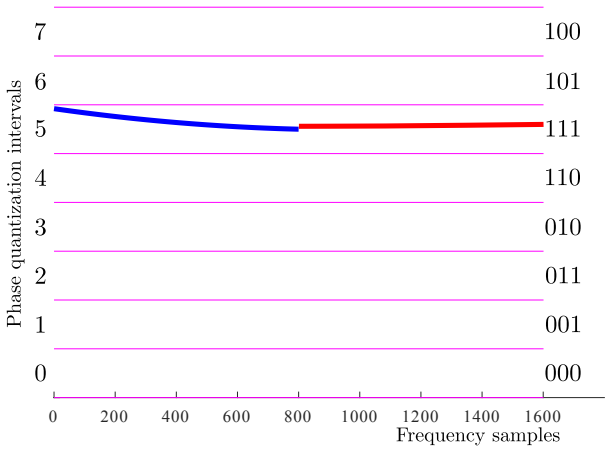

Fig. 4. Grid shift for key reconciliation and Gray labeling

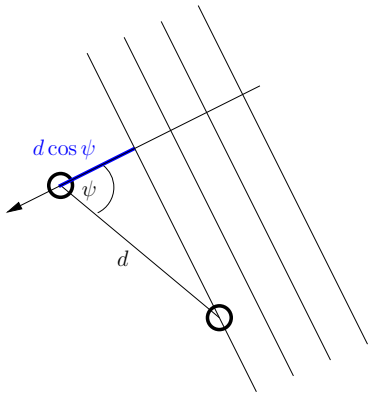

Fig. 5. Antenna pair in wave front

in Slepian-Wolf coding, some hashing / source coding can be applied [21].

IV. Expected Distribution

Although we practically used a circular array to collect many measurements at once and allow for eavesdropping countermeasures discussed in the following section, let us here consider one antenna pair and the distribution of possible phase differences that will also lead to a corresponding non-uniform distribution over the quantization regions.

Let the distance between the two antennas be d. The maximum phase difference is then given by

$$\Delta\phi_{\max} = \frac{\omega_0}{c} d = \frac{2\pi f_0}{c} d = 2\pi \frac{d}{\lambda_0} \tag{3}$$

for a carrier frequency (mid frequency between the two FDD bands) f_0, the corresponding wavelength λ_0, and the speed of light c. For our measurements, we had $f_0 = 2.19$ GHz and $d = 22.859$ mm, which leads to an interval of possible phase differences $\Delta\phi \in [-\pi/3, +\pi/3]$.

When defining an angle ψ of the wave front direction from the connecting line between the antennas according to Fig. 5, the phase difference becomes

$$\Delta\phi_{\max} = \frac{\omega_0}{c} d \cos\psi \ . \tag{4}$$

We assume a uniform distribution of ψ in the interval $[0, \pi]$, where we already take into account that the corresponding interval on the negative side will lead to the same phase differences. The density is hence $f_\Psi(\psi) = 1/\pi$ for $0 \leq \psi \leq \pi$. With

$$\frac{d\{\Delta\phi\}}{d\psi} = -\frac{\omega_0}{c} d \sin(\psi) \ , \tag{5}$$

we obtain

$$\begin{aligned} f_{\Delta\Phi}(\Delta\phi) &= \frac{1}{\pi} \frac{c}{\omega_0 d} \frac{1}{|\sin\psi|} \\ &= \frac{1}{\pi} \frac{c}{\omega_0 d} \frac{1}{|\sin\cos^{-1}\left[\Delta\phi \frac{c}{\omega_0 d}\right]|} \\ &= \frac{1}{\pi} \frac{c}{\omega_0 d} \frac{1}{\left|\sqrt{1 - \left[\Delta\phi \frac{c}{\omega_0 d}\right]^2}\right|} \ . \end{aligned} \tag{6}$$

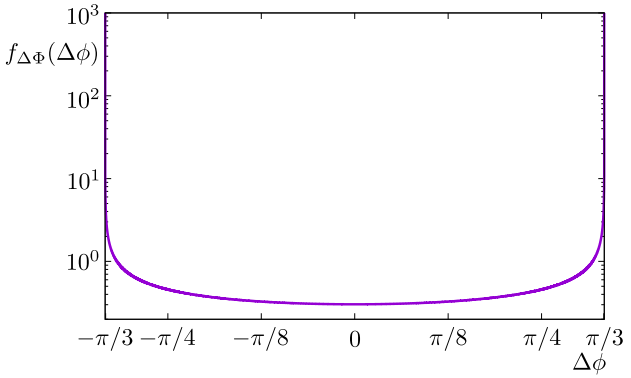

Fig. 6. Density of phase differences between two antennas

Figure 6 shows the resulting distribution, which is indeed far from the desired uniform distribution, which will either ask for a non-uniform quantization or later source coding (hashing), e.g., arithmetic coding. In here, we will just show the results with linear quantization. We do not yet discuss leveling out the distribution apart from the effect of additional antenna permutations.

V. Eavesdropping and Countermeasures

We are considering passive eavesdropping, only. The legitimate and eavesdropping channels are shown in Fig. 7.

Eavesdropping had, e.g., been studied by He et al. in [23], [24] with the conclusion that one can assume independent channels at distances of, at least, around 6λ, which was in earlier times considered to be only in the order of λ. In our case, the shift of the quantization grid (or equivalently, the phase measurements) is communicated publicly. Hence, Eve can likewise apply the same grid shift, but it does not help her in any way. She will measure a different phase, anyhow. We found that even without any additional measures, the bit-error ratio, i.e., the KDR toward Eve ranges from 0.45 to 0.496, i.e., is close to 0.5 for all locations. An eavesdropper is hence almost left with coin-tossing. One might still consider 0.45 as not sufficient, asking, e.g., for privacy amplification [25],

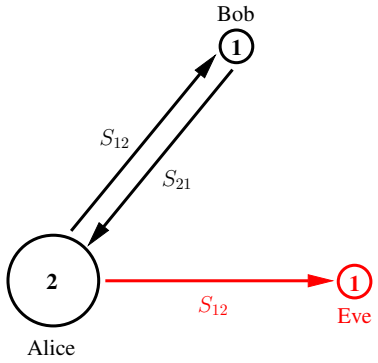

Fig. 7. Legitimate and eavesdropping channels

[26]. Especially critically observed would be the situation of a low-entropy channel, like a line-of-sight stationary situation, where eventually, information could be collected over time. Since we did measurements with an antenna array, we were able to obtain new key bits by simply permuting the antennas (assumed to be located at Alice). This offers $N!$ configurations for N antennas. As a side effect of generating new key bits also in a stationary situation, this achieves additional security with respect to eavesdropping. The eavesdropper would additionally have to estimate the permutation pattern used when Alice is probing the channel to Bob.

Other options to solve both issues, the creation of new key bits in a stationary situation and the avoidance of eavesdropping, can be realized by reconfigurable antennas to change directional properties [6]. They could also be located at Bob's end. Randomly controlled reconfigurable intelligent surfaces [27]–[29], e.g., placed at walls or in the vicinity of the antennas, are another option to randomize the channel.

VI. Results

Excluding low amplitude and high-variance phase measurements, we obtained an efficiency of 92.3 %. Using all available measurements, the key disagreement rate over all measurements was $1.85 \cdot 10^{-2}$ with 8 quantization intervals, which is not yet at a possibly desired range of 10^{-5} or better, however, is is a good starting point for other key reconciliation methods, like Slepian-Wolf coding based approaches. We should note that intentionally, not the most favorable antenna positions were chosen, often blocking line of sight. In figures 8 and 9, we clearly observe that the distribution is by far not uniform as already indicted in Section IV. This is clearly not a suitable distribution for secret key applications. A uniform distribution can be obtained by a nonlinear quantizer which will then also lead to a nonuniform distribution of key mismatches. Alternatively, source-coding methods, like Arithmetic Coding may be applied. Another problem is the limited number of key bits especially in case of a low-entropy channel situation, in the extreme, a steady line-of-sight channel. One option to solve both problems is to randomly permute the antennas, hence probe in a permuted order. With our antenna array of 40 antennas, this would allow for 40! permutations. Further

possibilities were already mentioned in Section V. Here, we will concentrate on results obtained with a certain number of permutations. In Fig. 10, we show histograms for a different number of permutations and realize that a growing number of permutations will level out the distribution a lot, however, not finally becoming totally uniform. The KDR is only insignificantly affected. For this measurements location (big garage), we received KDRs of $6.9 \cdot 10^{-3}$, $7.9 \cdot 10^{-3}$, $7 \cdot 10^{-3}$, $6.7 \cdot 10^{-3}$, for 0, 3, 10, and 100 permutations, respectively. Hence, almost no change. At some locations, however, one could recognize a small increase in KDR for permuted measurements.

Permutations, just as other randomization approaches with reconfigurable antennas or surfaces also protect against active Man-in-the-Middle attacks [30].

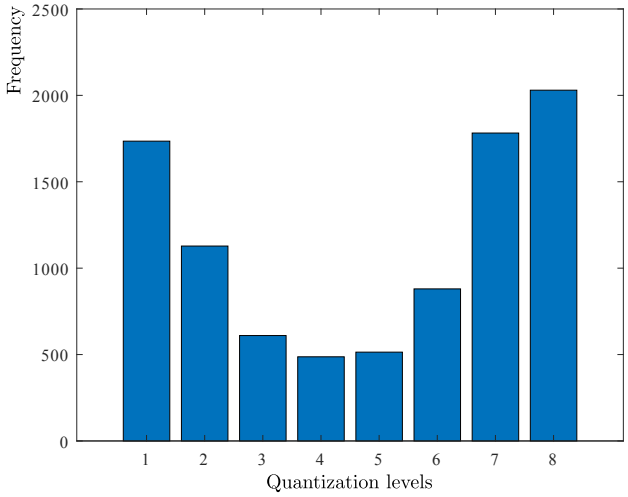

Fig. 8. Histogram over 8 quantization intervals

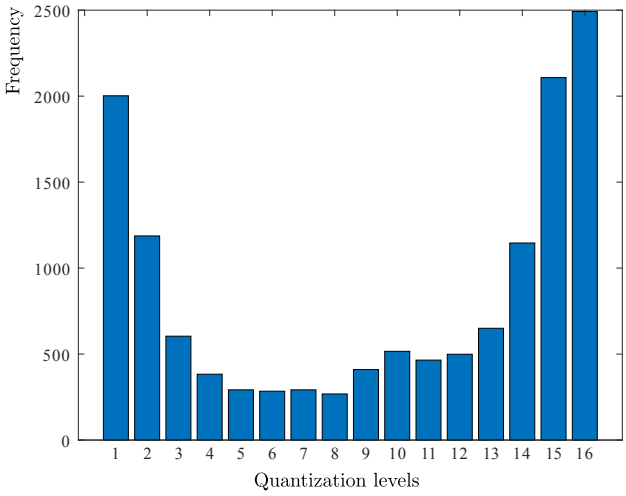

Fig. 9. Histogram over 16 quantization intervals

So far, we assumed adjacent frequency bands without a guard band. We also investigated the behavior, if we introduce a spacing between the two bands. This means, to not perform more measurements, we narrowed the used frequency bands

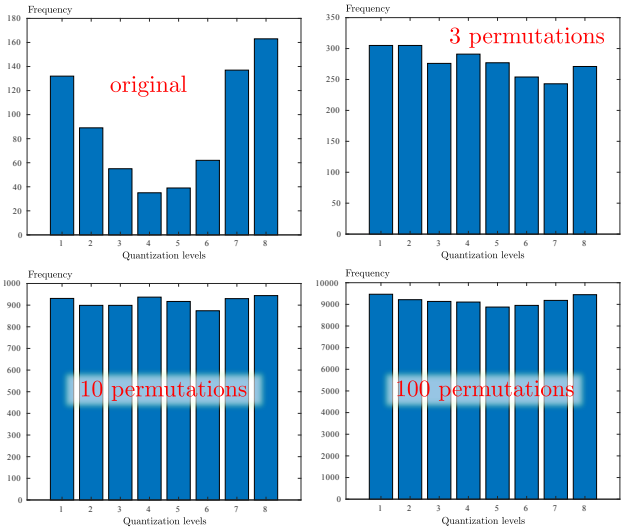

Fig. 10. Histograms with 0, 3, 10, and 100 antenna permutations

to create a gap in between the two FDD bands. Hence, apart from the gap, it also shows results for narrower frequency ranges. Figure 11 shows the to be expected deterioration of the KDR, which is almost linear with the gap size. A gap of 800 frequency samples meant to leave a spacing of 5 MHz and two bands of only 2.5 MHz for the two directions. It should already be obvious from figures 1 to 4 that the deterioration of the KDR is more due to the gap between the active FDD bands than the width of the bands.

For all the given KDR values, however, we should note that we were not too restrictive in rejecting measurements which resulted in a relatively high efficiency. Being more restrictive, will lead to an improvement in KDR, but sacrificing efficiency. There is a trade-off between the two.

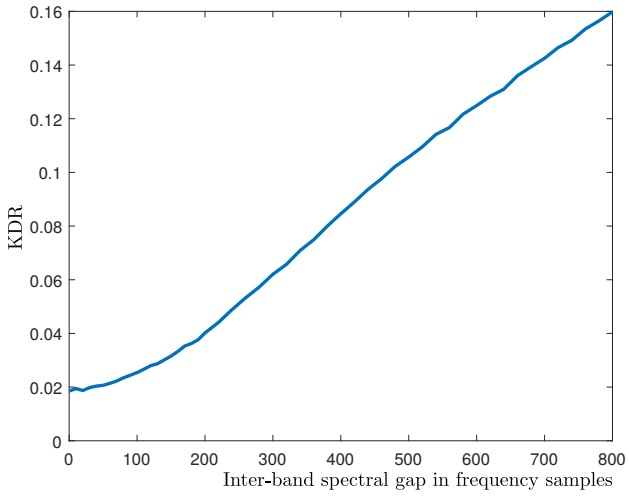

Fig. 11. KDR dependent on a frequency gap in between the two FDD bands

VII. Conclusions

We proposed a very low complexity physical-layer key generation scheme, just using curve fitting for the phase difference between two antennas. An antenna array applying a random pair selection will allow for higher numbers of independent keys, improve statistics (uniformity of key generation), and enhance protection against eavesdropping. The security against eavesdropping is, however, anyhow shown to be very high, even without such measures. The KDR rate was found to be in the 10^{-2} range for high efficiency of more than 90 %. The KDR toward an eavesdropper was already close to 0.5 without any random permutation. Further work on eavesdropping issues is currently done. Future publications with then also contain estimates of the secret key capacity and discuss possible attacks.

A band separation can be permitted, but, of course, the method relies on neighboring FDD bands.

Further work will investigate the trade-off between efficiency and KDR and will improve the detection of unreliable measurements to be excluded. So far, very simple threshold decisions for the amplitude and phase variance were applied. The reliability of the detection can certainly be improved by more elaborate analysis of the phase, e.g., directly based on the curve fitting results.

References

[1] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, pp. 614–626, 2016.

[2] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Communications Surveys Tutorials*, vol. 19, no. 1, pp. 347–376, 2017.

[3] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," *Proceedings of the National Academy of Sciences*, vol. 114, no. 1, pp. 19–26, 2017.

[4] A. Hyadi, Z. Rezki, and M.-S. Alouini, "An overview of physical layer security in wireless communication systems with csit uncertainty," *IEEE Access*, vol. 4, pp. 6121–6132, 2016.

[5] 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.

[6] R. Mehmood and J. W. Wallace, "Experimental assessment of secret key generation using parasitic reconfigurable aperture antennas," in *2012 6th European Conference on Antennas and Propagation (EUCAP)*, pp. 1151–1155, March 2012.

[7] R. Mehmood and J. W. Wallace, "Experimental assessment of secret key generation using parasitic reconfigurable aperture antennas," *Proceedings of 6th European Conference on Antennas and Propagation, EuCAP 2012*, no. 1, pp. 1151–1155, 2012.

[8] R. Mehmood, J. Wallace, and M. Jensen, "Key establishment employing reconfigurable antennas: Impact of antenna complexity," *IEEE Transactions on Wireless Communications*, vol. 13, pp. 6300–6310, Nov 2014.

[9] A. Filip, R. Mehmood, J. Wallace, and W. Henkel, "Physical-layer key generation supported by RECAP antenna structures," in *Proceedings of 2013 9th International ITG Conference on Systems, Communication and Coding (SCC)* , pp. 1–6, 2013.

[10] R. Mehmood, J. Wallace, and M. Jensen, "Optimal array signaling for key establishment in static multipath channels," *Antennas and Propagation (EuCAP), 2015 9th European Conference on*, pp. 1–2, 2015.

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

[12] J. Wallace, "Secure physical layer key generation schemes: Performance and information theoretic limits," in *2009 IEEE International Conference on Communications, ICC '09.*, (Dresden, Germany), pp. 1–5, June 2009.

[13] 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.

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

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

[16] 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.

[17] O. Graur, N. Islam, A. Filip, and W. Henkel, "Quantization and LLR Computation for Physical Layer Security," in *International Zurich Seminar on Communications*, 2016.

[18] 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 (GC Wkshps)*, pp. 1–6, 2018.

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

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

[21] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[22] M. Yuliana, Wirawan, Suwadi, Endroyono, and T. Suryani, "Enhancing channel reciprocity of secret key generation scheme by using modified polynomial regression method," in *2018 International Conference on Computer Engineering, Network and Intelligent Multimedia (CENIM)*, pp. 35–40, 2018.

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

[24] 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.

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

[26] 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, 2003.

[27] C. Liaskos, S. Nie, A. Tsioliaridou, A. Pitsillides, S. Ioannidis, and I. Akyildiz, "A new wireless communication paradigm through software-controlled metasurfaces," *IEEE Communications Magazine*, vol. 56, no. 9, pp. 162–169, 2018.

[28] E. Basar, M. Di Renzo, J. De Rosny, M. Debbah, M.-S. Alouini, and R. Zhang, "Wireless communications through reconfigurable intelligent surfaces," *IEEE Access*, vol. 7, pp. 116753–116773, 2019.

[29] Q. Wu and R. Zhang, "Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network," *IEEE Communications Magazine*, vol. 58, no. 1, pp. 106–112, 2020.

[30] Y. Pan, Z. Xu, M. Li, and L. Lazos, "Man-in-the-middle attack resistant secret key generation via channel randomization," *Proceedings of the Twenty-second International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing*, Jul 2021.