Reciprocity and Secret Key Generation for FDD Systems using Non-Linear Quantization

1st Ehsan Olyaei Torshizi
School of Computer Science and Engineering
Jacobs University Bremen
Bremen, Germany
e.olyaei@jacobs-university.de

2nd Werner Henkel, *senior member, IEEE*
School of Computer Science and Engineering
Jacobs University Bremen
Bremen, Germany
werner.henkel@ieee.org

***Abstract*—Secret key generation based on wireless channel reciprocity has received quite some attention, recently. Channel reciprocity as an inherent feature of time division duplexing (TDD) systems leads to creating cryptographic keys without the need for a key exchange procedure. Using different carrier frequencies for the uplink and the downlink, however, means that there is no such symmetry in the frequency response of frequency division duplex (FDD) systems and it makes the key generation for these systems challenging. In this paper, we use the phase differences between neighboring antennas as a frequency-independent channel parameter that provides the required reciprocity in FDD systems. For our studies, we consider neighboring frequency ranges for both directions, which should result in a continuous curve through the two frequency ranges in the two directions. For denoising we use a polynomial curve fitting procedure on the phase differences between antennas. Moreover, we propose a non-linear scheme to quantize the midpoint between the two frequency ranges with the two measurement directions. As a consequence, in contrast to using a linear scheme, the proposed framework would be highly desirable for secret key applications as it gives rise to a more uniform distribution for the resulting histogram over the quantization intervals. Numerical simulation results are shown to verify the effectiveness of the proposed method.**

***Index Terms*—Physical layer security, secret key generation, non-linear quantization, frequency-division duplexing.**

I. Introduction

The rapid development of mobile wireless communication has led to receiving enormous attention to the security of wireless communication. Because of the intrinsically shared nature of the wireless channels, the security of the wireless communication networks could be threatened by eavesdropping. Accordingly, there is a risk of information leakage on both sides of a communication system. Creating secret keys can secure wireless networks and ensure integrity, confidentiality, and authenticity of the communication. Recently, quite some research has shown that the fundamental ability of the physical layer namely the physical layer secret key can provide secure wireless communications [1]. The physical-layer secret key generation (PSKG) utilizes reciprocity of the wireless channel to provide a decently secure physical layer key distribution.

Effective pairwise key generation demands highly similar channel features between two legitimate users. Time-division duplexing (TDD) and frequency-division duplexing (FDD) are the two most conventional duplexing schemes used in wireless communications. In TDD systems, the uplink and downlink transmit over the same frequency band in a ping-pong manner, and the channel responses obtained by legitimate users are reciprocal (if the measurements are done within the coherence time). [2], [3] first presented key generation based on the received signal strength identication (RSSI) and [4]–[7] employed channel state information (CSI) for key generation purposes.

Most wireless systems, especially 5G networks and some current cellular communications, such as Long Term Evolution (LTE) and narrowband Internet of Things (IoT) depend on FDD [8]. Consequently, key generation for such FDD-based systems is important, too. In FDD systems, both the uplink and downlink are simultaneously run in two distinct frequency bands. Hence, one experiences different frequency responses and the channel reciprocity does not hold in the same way as with a TDD system. Therefore, one has to determine reciprocal channel features for key generation in FDD systems. One may use the times of arrival (ToA) and directions of arrival (DoA) as channel parameters to hold the reciprocity in these systems. Secret key generation methods by using the angle and path delay [9] or the channel covariance matrix [10] are proposed to provide the necessary reciprocity in FDD. Moreover, using combinatorial channels with reciprocal channel gains can be realized by employing an additional reverse channel training phase, termed loopback-based protocols [11]–[13]. Since passive eavesdroppers have access to the whole transmissions, there is no guarantee for the security of these protocols [14]. Although accurate estimation of the angle and delay needs a lot of resources including multiple antennas and large bandwidth [15], the results we obtained in our earlier works [16]–[18] which are based on the direction of arrival estimation derived from scattering matrix parameters S_{12} and S_{21} bidirectional measurements, are extremely promising.

Instead of the computational more challenging ToA or DoA computations, in this paper, we directly employ the phase differences between neighboring antennas derived from scattering parameters S_{12} and S_{21} bidirectional measurements between an antenna array and a single dipole counterpart. This does not require absolute phase knowledge. We assume

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

closely located FDD bands. Therefore, we can consider some continuity between them, because reciprocity holds for the same frequency range. Moreover, for denoising, we apply a curve fitting method to the phase differences between each pair of neighboring antennas. It should be mentioned that we utilize a non-linear quantization scheme for the midpoint between the two frequency bands which leads to a more uniform key distribution required for encryption purposes. Finally, as a first key reconciliation step, we force the quantized measurements from one side to be at the midpoint of the quantization intervals, which are not the same due to non-linear quantization. This reduces the key disagreement rate to a range that allows for additional Slepian-Wolf coding as a further key reconciliation step.

The rest of the paper is organized as follows. In Section II, we describe the system setup and also explain how we obtained the measurements at different antenna positions. In Section III, we analyze the distribution of the phase differences and show how we can theoretically reach a uniform distribution over the histogram regions. Furthermore, we propose a practical algorithm to achieve this uniformity for measurements in practice. The secret key generation method, including curve fitting, quantization, and key reconciliation steps, is presented in detail in Section IV. Various numerical simulations are implemented to verify the performance of the proposed method in Section V. Finally, Section VI concludes this paper.

II. System Setup and Measurements

Figure 1 shows the basic model of the key generation and reconciliation setup in which Alice and Bob are legitimate communication partners and Eve acts as a passive attacker who tries to eavesdrop confidential information exchanged between them.

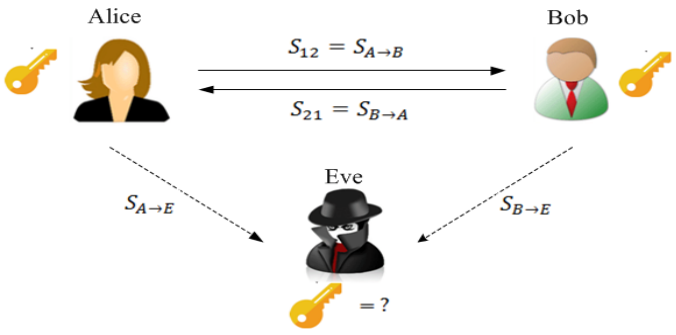

Fig. 1. Basic model of the key generation and reconciliation setup.

In our setup, Alice and Bob use a circular antenna array and a single dipole for angle measurements, respectively, and we consider a single dipole for Eve. The circular array we designed at Alice's end, which is shown in Fig. 2, included a rotating disc with a radius of 14.568 cm and 40 antennas spaced at roughly $\frac{\lambda}{6}$. With each partial rotation of the disc by the corresponding angle (9 degrees), only the parameters of one antenna is measured and this procedure continues until the parameters of all 40 antennas are measured one after another and the disc completes a full 360 degree rotation. We measure scattering matrix parameters S_{12} and S_{21} (known to be reciprocal) using a standard vector network analyzer in a remotely controlled fashion. To avoid encountering frequency dependencies of reflectors and antennas, we measure S_{12} and S_{21} in two closely neighboring 5 MHz frequency ranges on both sides of a central (carrier) frequency of 2.19 GHz.

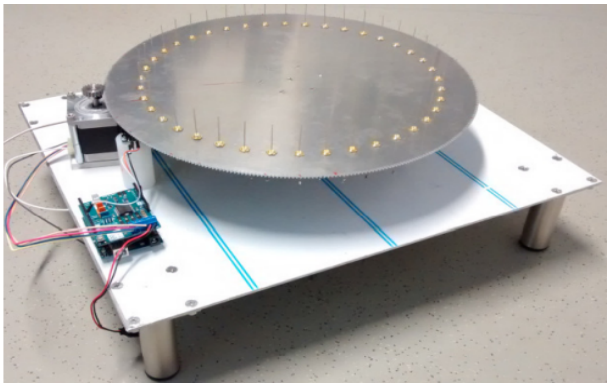

Fig. 2. The circular antenna array.

For our measuring phase, we considered 13 major indoor environments ranging from very low to very high reflection effects including lab, home, basement, corridor, garage, etc. In addition to existing environmental reflective factors, we partly blocked the LOS path between transmit and receive antennas. Moreover, we used cases at the same height (no elevation) or at different heights (nonzero elevation) for both antennas. In total, our data currently consists of 150×40 set of measurements in different environments and at different heights. In line with our earlier work [19], we assume that there is a certain continuity in phase differences between two neighboring antennas in the two frequency bands we considered due to reciprocity between S_{12} and S_{12}.

III. Resulting Frequency Distribution and Non-Linear Quantization

In [19], it is shown that employing linear quantization leads to a non-uniform distribution over the quantization intervals on the corresponding histogram and as a solution to reach a more uniform distribution, using a permutation pattern for antennas is considered. In this section, we analyze the resulting distribution of the possible phase differences and show how a uniform distribution for phase differences can be obtained by using a non-linear quantizer. Let's consider two antennas on the circular array at Alice's end with spacing of d. Then, the maximum possible phase difference will be

$$\Delta\phi_{\max} = \frac{\omega_0}{c} d = \frac{2\pi f_0}{c} d = 2\pi \frac{d}{\lambda_0} \; ; \qquad (1)$$

where f_0, λ_0, and c are the carrier frequency, the corresponding wave length, and the speed of light, respectively. For the circular array we designed, we considered $d = 22.859$ mm and $f_0 = 2.19$ GHz which causes an interval of possible phase differences $\Delta\phi \in [-\pi/3, +\pi/3]$. By considering ψ as an angle

of the wave front direction from the connecting line between the antennas, the phase difference can be expressed by

$$\Delta\phi_{\max} = \frac{\omega_0}{c} d \cos\psi \ . \tag{2}$$

By assuming a uniform distribution for ψ on the interval $[0, \pi]$ and consequently the density function as $f_\Psi(\psi) = 1/\pi$ for $0 \le \psi \le \pi$, we express the density function of the maximum phase difference as

$$\begin{aligned} f_{\Delta\Phi}(\Delta\phi) &= \frac{1}{\pi}\frac{c}{\omega_0 d}\frac{1}{|\sin\psi|} \\ &= \frac{1}{\pi}\frac{c}{\omega_0 d}\frac{1}{|\sin\cos^{-1}\left[\Delta\phi\frac{c}{\omega_0 d}\right]|} \\ &= \frac{1}{\pi}\frac{c}{\omega_0 d}\frac{1}{\left|\sqrt{1-\left[\Delta\phi\frac{c}{\omega_0 d}\right]^2}\right|} \ . \end{aligned} \tag{3}$$

In order to achieve a uniform distribution, we propose a non-linear quantization scheme which is shown as a block diagram in Fig. 3. This idea is based on employing the probability integral transform we adopt as the following theorem.

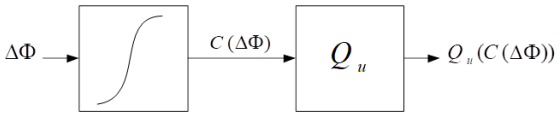

Fig. 3. Non-linear quantization block diagram.

Theorem 1 (Probability integral transformation) [20]: Let X have continuous cumulative distribution function (CDF) $F_X(x)$ and define the random variable Y as $Y = F_X(x)$. Then Y is uniformly distributed on $(0, 1)$, that is, $P(Y \le y) = y$, $0 < y < 1$.

Hence, we select the inverse CDF of phase differences as a non-linear compressor function for the first block of the proposed diagram which could be obtained as follows:

$$\begin{aligned} F_{\Delta\Phi}(\Delta\phi) &= \int_0^{\Delta\phi} \frac{1}{\pi}\frac{c}{\omega_0 d}\frac{1}{\left|\sqrt{1-\left[\frac{c}{\omega_0 d}t\right]^2}\right|}\mathrm{d}t \\ &= \frac{1}{\pi}\sin^{-1}\left[\frac{c}{\omega_0 d}\Delta\phi\right] \ . \end{aligned} \tag{4}$$

and

$$C(\Delta\phi) = F^{-1}_{\Delta\Phi}(\Delta\phi) = \frac{\omega_0 d}{c}\sin\left[\pi\Delta\phi\right] \ . \tag{5}$$

Figures 4 and 5 show the corresponding probability density function (pdf) and CDF of the phase differences, respectively.

In order to implement the proposed non-linear scheme for quantization, with the goal in mind, to keep the complexity low, we introduce a simple algorithm that divides each interval into some sub-intervals. Then, we try to determine the new boundaries in such a way that the amount assigned to each interval on the resulting histogram will be approximately

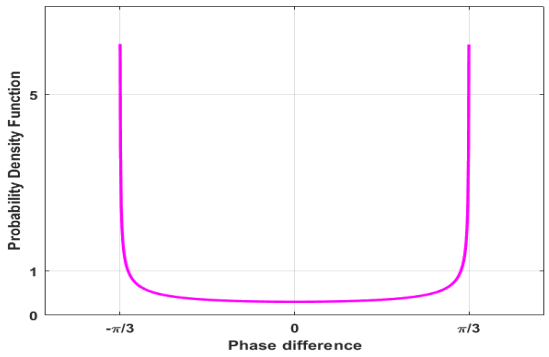

Fig. 4. Ideal PDF of the phase differences between two antennas for a single planar wave front.

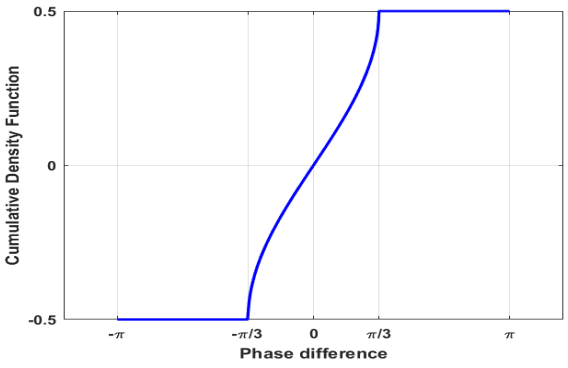

Fig. 5. Ideal CDF of the phase differences between two antennas.

equivalent to the average value over all sub-intervals. If we consider L as the number of quantization intervals, we use $L \times 2^M$ sub-intervals, in which M is considered as an integer greater or equal than 1. The larger we choose M, the more uniform the results in the subsequent histogram will become. The implementation of the algorithm is shown in the following.

IV. Key Generation Procedure

In this section, we employ a simple and low complexity method to generate the keys which are usable for neighboring FDD frequency bands that are not too far apart. As the first step, we approximate the frequency behavior of the phase difference between the transmission characteristics of neighboring antennas for both S_{12} and S_{21}, separately, with an appropriate curve-fitting approach. Prior to this, we need to do some preprocessing on the measurements such as unwrapping the phase differences between each neighboring antenna pair. Moreover, we detect unreliable measurements by using a threshold as a maximum acceptable value for the variance of the phase measurements. There is a trade-off between efficiency and the key disagreement rate (KDR) such that using a stricter threshold on the variance of the measured phase differences leads to lower efficiency. Applying different curve-fitting approaches to our measurements of scattering

Algorithm 1: Finding new boundaries for non-linear quantization

Input:

L (Number of intervals),
M (Number of sub-intervals),
n_{avg} (Average frequency number)

Output:

b (New boundaries)

// over all intervals

for $i = 1 : L$ **do**

  // over all sub-intervals

  while $j <= L \times 2^M$ **do**

    $sum(j) = n(j) + sum(j-1)$

    if $sum(j) >= i \times n_{avg}$ **then**

      $r(i) = sum(j) - i \times n_{avg}$ (compute residue for each interval)

      $b(i) = (j-1) + \frac{n(j)-r(i)}{n(j)}$ (compute new boundaries)

      $i \leftarrow i + 1$

    else

      $j \leftarrow j + 1$

parameters verified that second-order polynomial curve fitting is already a good candidate. Because of reciprocity, by using a calibrated VNA (vector network analyzer), we expect to have a direct continuity between the S_{12} and S_{21} phase difference spectral segments. However, noise and environmental reflection changes (even outside room movements) could disrupt this continuity.

For the next step, we should quantize the determined phase difference at the merging point of the two FDD frequency regions obtained from the polynomial curve fitting, separately, from each side. As we mentioned earlier, we developed a non-linear quantization scheme to reach a better uniformity of the histogram. Moreover, to reduce the key disagreement rate, we force the quantized measurements from one side to be at the midpoint of the resulted quantization intervals from non-linear quantization and consider this as the first stage of key reconciliation. One may employ coding-based approaches like Slepian-Wolf coding based on LDPC codes [21] as a further key reconciliation step.

Two exemplary curve fitting results for phase differences on both sides along with their related non-linear quantized version of measurements are illustrated in figures 6 and 7. The unwrapped version of our phase differences lies between $-\pi$ to $+\pi$ which is specified with dashed lines. The theoretical upper and lower bounds for phase differences, which are specified in figures 6 and 7, are shown with black dashed lines. Furthermore, the second-order polynomial fitted curve is illustrated in green for both frequency ranges. Additionally, to ensure single-bit changes between neighboring quantization intervals, 3-Bit Gray-coded keys are listed on the right side for each quantization interval.

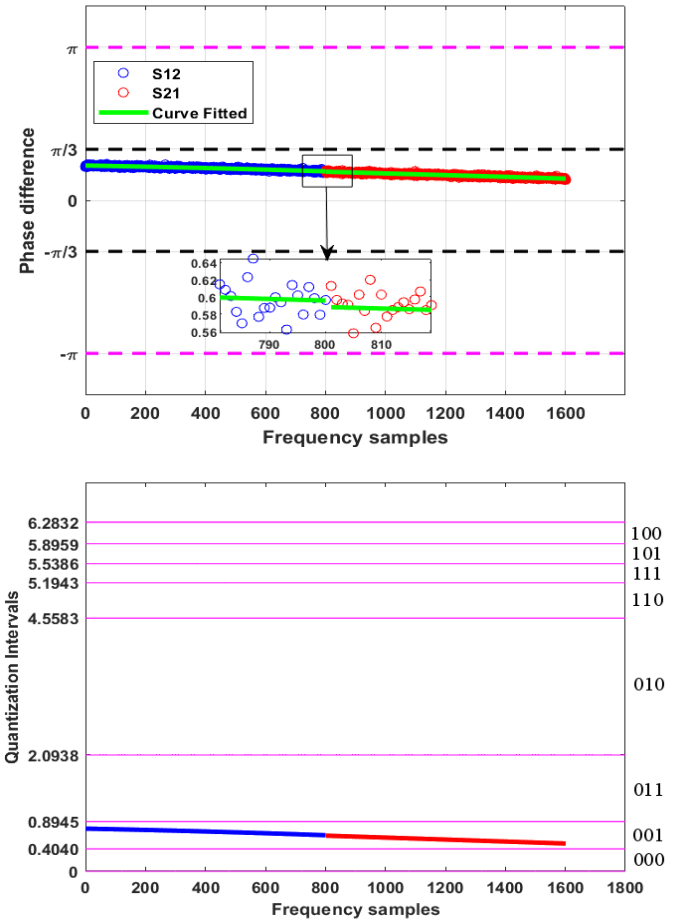

Fig. 6. (Example 1) Top: Curve fitting result for phase differences between two neighboring antennas on both sides. Low: Corresponding non-linearly quantized version of phase differences.

From figures 6 and 7, it can be seen that the phase difference at the merging point (frequency slot 801 for S_{12} or frequency slot 802 for S_{21}) is moved into the middle of the related quantization interval from one side by applying a shift. Since the amount of the shift is publicly communicated, the other legitimate counterpart also can similarly adapt the quantization grid. The continuity we expected at the midpoint is evident.

V. Simulation Results and Discussion

We now provide simulation results first using a linear quantization and then compare them with our proposed non-linear scheme. We consider the variance threshold at 1. After removing unusable measurements with high variance, the resulting histogram using a linear quantizer with 3-Bit Gray-code assignment is presented in Fig. 8. As we expect, the associated histogram is strongly non-uniform. In the case of non-linear quantization, we selected $M = 3$ in our simulations, which means that we divided each quantization interval into 8 sub-intervals. Figure 9 shows the resulting histogram with 64 sub-intervals.

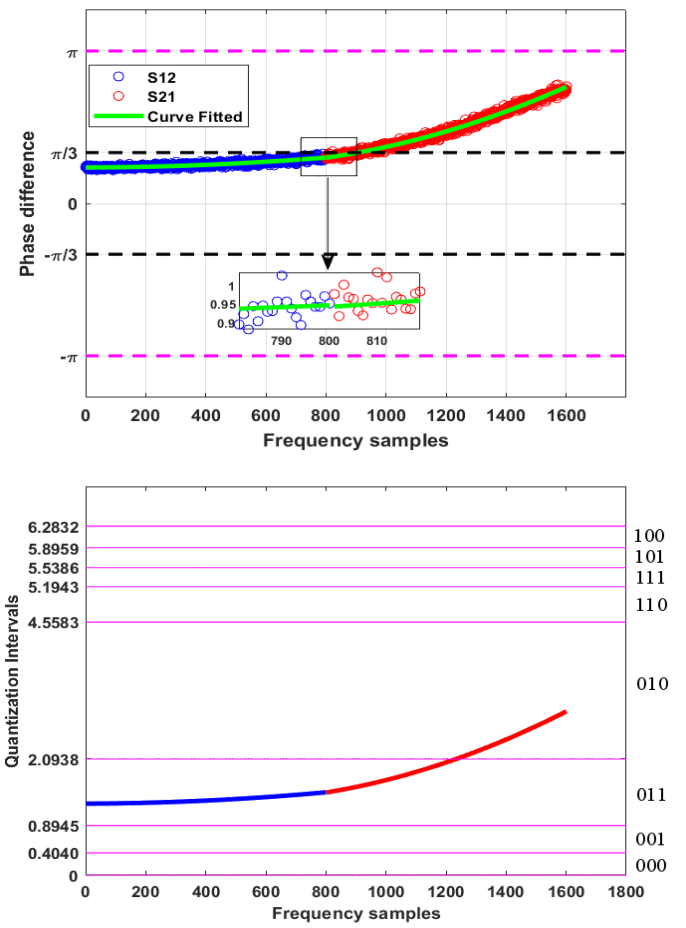

Fig. 7. (Example 2) Top: Curve fitting result for phase differences between two neighboring antennas on both sides. Low: Corresponding non-linearly quantized version of phase differences.

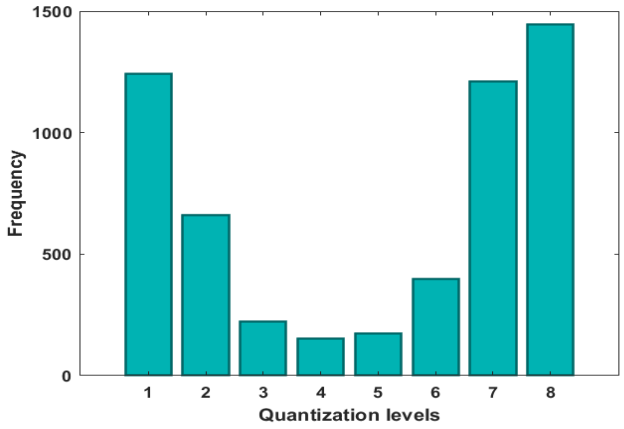

Fig. 8. Histogram over all measurements using linear quantizer with 8 intervals.

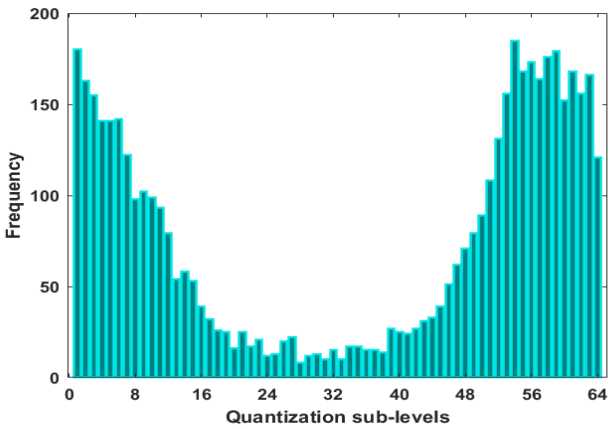

Fig. 9. Histogram over all measurements with 64 sub-intervals.

With the intention of measuring the uniformity of the histogram to have an appropriate metric to compare, we define a relative uniformity error as

$$e_u = \sum_{i=1}^{L} e_i = \sum_{i=1}^{L} \frac{|n_i - n_{avg}|}{n_{avg}} \ . \tag{6}$$

where n_{avg} denotes the average value over all sub-intervals and n_i shows the related value in the ith interval. A result illustrating the uniformity performance of the proposed algorithm for $M = 3$ is shown in Fig. 10. The corresponding relative uniformity error for linear and non-linear quantization schemes were obtained as 5.333 and 0.144, respectively.

To demonstrate the performance of our proposed non-linear scheme compared with the antenna permutation method, the resulting histogram over the same measurements using randomly permuted antennas (channel probing with permuted antennas) for 100 permutations is presented in figure 11. The corresponding value of the relative uniformity error is measured 0.3055.

Comparing figures 10 and 11, we can easily see that the proposed non-linear quantizer provides slightly better performance than the antenna permutation and is hence suitable for secret key applications. It is worth mentioning that we only used the algorithm with a single try. One can develop the algorithm in an iterative manner and consider a convergence criterion on the relative uniformity error and reach a more uniform distribution of the histogram. With consideration of 8 quantization intervals, we obtained an efficiency of 92.5% and KDR of 1.8×10^{-2} in our simulations. As we know, there is a trade-off between KDR and efficiency. Therefore, KDR can be improved by applying a stricter threshold criterion on the variance of the measurements at the cost of decreasing the efficiency.

Based on the studies of He et al. in [22], one can assume independent channels at distances of, at least, around 6λ. In our case, the shift of the quantization grid is communicated in public. Although Eve can apply the same grid shift, it doesn't help her and she will measure a different phase, anyhow. The bit-error ratio, i.e., the KDR toward Eve, even without any additional measures was approximately close to 0.5. Consequently, an eavesdropper is almost left in a heads or tails situation.

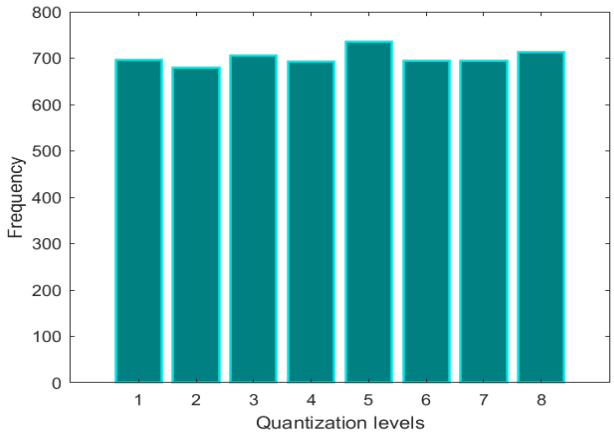

Fig. 10. Histogram over all measurements using non-linear quantization with 8 intervals.

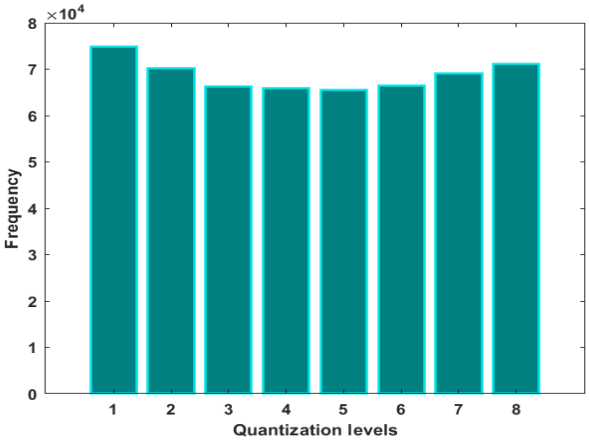

Fig. 11. Histogram over all measurements using linear quantization via 100 antenna permutations.

VI. Conclusions

We developed a low-complexity FDD-based key generation approach by employing a non-linear quantization scheme. Using a non-linear quantizer leads to a uniform distribution on the resulting histogram over the phase differences. Moreover, we proposed a simple algorithm to implement a non-linear quantization scheme. Numerical results demonstrated that compared with the other methods like antenna permutation, our proposed non-linear structure can reach a more uniform distribution. Other approaches such as applying arithmetic coding after linear (or non-linear) quantization and creating more efficient mechanisms to detect the unreliable measurements are planned for further studies.

References

[1] M. Debbah, H. El-Gamal, H. V. Poor, *et al.*, "Wireless physical layer security," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, pp. 1–2, 2010.

[2] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Transactions on Mobile Computing*, vol. 9, no. 1, pp. 17–30, 2009.

[3] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments," in *Proceedings of the 15th annual international conference on Mobile computing and networking*, pp. 321–332, 2009.

[4] T.-H. Chou, S. C. Draper, and A. M. Sayeed, "Impact of channel sparsity and correlated eavesdropping on secret key generation from multipath channel randomness," in *2010 IEEE International Symposium on Information Theory*, pp. 2518–2522, IEEE, 2010.

[5] J. Huang and T. Jiang, "Dynamic secret key generation exploiting ultra-wideband wireless channel characteristics," in *2015 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1701–1706, IEEE, 2015.

[6] R. 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, pp. 364–375, 2007.

[7] F. Marino, E. Paolini, and M. Chiani, "Secret key extraction from a UWB channel: Analysis in a real environment," in *2014 IEEE International Conference on Ultra-WideBand (ICUWB)*, pp. 80–85, IEEE, 2014.

[8] G. Li, A. Hu, C. Sun, and J. Zhang, "Constructing reciprocal channel coefficients for secret key generation in fdd systems," *IEEE Communications Letters*, vol. 22, no. 12, pp. 2487–2490, 2018.

[9] W. Wang, H. Jiang, X. Xia, P. Mu, and Q. Yin, "A wireless secret key generation method based on Chinese Remainder Theorem in FDD systems," *Science China Information Sciences*, vol. 55, no. 7, pp. 1605–1616, 2012.

[10] B. Liu, A. Hu, and G. Li, "Secret key generation scheme based on the channel covariance matrix eigenvalues in FDD systems," *IEEE Communications Letters*, vol. 23, no. 9, pp. 1493–1496, 2019.

[11] S. J. Goldberg, Y. C. Shah, and A. Reznik, "Method and apparatus for performing JRNSO in FDD, TDD and MIMO communications," Mar. 19 2013. US Patent 8,401,196.

[12] A. M. Allam, "Channel-based secret key establishment for FDD wireless communication systems," *Commun. Appl. Electron*, vol. 7, no. 9, pp. 27–31, 2017.

[13] X. Wu, Y. Peng, C. Hu, H. Zhao, and L. Shu, "A secret key generation method based on csi in OFDM-FDD system," in *2013 IEEE Globecom Workshops (GC Wkshps)*, pp. 1297–1302, IEEE, 2013.

[14] P. Linning, G. Li, J. Zhang, R. Woods, M. Liu, and A. Hu, "An investigation of using loop-back mechanism for channel reciprocity enhancement in secret key generation," *IEEE transactions on mobile computing*, vol. 18, no. 3, pp. 507–519, 2018.

[15] D. Vasisht, S. Kumar, H. Rahul, and D. Katabi, "Eliminating channel feedback in next-generation cellular networks," in *Proceedings of the 2016 ACM SIGCOMM Conference*, pp. 398–411, 2016.

[16] 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, IEEE, 2018.

[17] W. Henkel, A. M. Turjman, H. Kim, and H. K. Qanadilo, "Common randomness for physical-layer key generation in power-line transmission," in *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, pp. 1–6, IEEE, 2020.

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

[19] W. Henkel and M. Namachanja, "A simple physical-layer key generation for frequency-division duplexing (FDD)," in *2021 15th International Conference on Signal Processing and Communication Systems (ICSPCS)*, pp. 1–6, IEEE, 2021.

[20] G. Casella and R. L. Berger, *Statistical inference*. Cengage Learning, 2021.

[21] 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, IEEE, 2015.

[22] 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*, pp. 103–108, 2014.