# Highly Efficient FDD Secret Key Generation using ESPRIT and Jump Removal on Phase Differences

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

2nd Utkrist Uprety
*Computer Science and Engineering*
*Jacobs University Bremen*
Bremen, Germany
u.uprety@jacobs-university.de

3rd Werner Henkel, *senior member, IEEE*
*Computer Science and Engineering*
*Jacobs University Bremen*
Bremen, Germany
werner.henkel@ieee.org

***Abstract*—In this study, a highly efficient simple approach to generate secret keys for Frequency-Division Duplexing (FDD) systems is proposed. We use phase differences between neighboring antennas in a linear array to construct the channel profile and the ESPRIT (Estimation of Signal Parameters using Rotational Invariance Techniques) algorithm for estimating the direction of arrival (DOA). In order to increase the channel reciprocity, we approximate the frequency behavior of the phase differences by polynomial curve-fitting. Rather than using unwrapping to prevent jumps, we propose two jump-removing and outlier-correction algorithms which can bring the efficiency to $100$ %. Numerical results verify that the measurements have a minimum variance after using both proposed pre-processing algorithms. Furthermore, the corrected version of measurements has perfect efficiency and better performance on curve-fitting results and key disagreement rate.**

***Index Terms*—Physical layer security, secret key generation, ESPRIT, FDD.**

## I. Introduction

In order to avoid key distribution protocols like the well-known Diffie-Hellman key exchange, especially, for not too powerful IoT devices, physical-layer key generation offers an alternative, which we study in the case of FDD, where reciprocity for common randomness is not as obvious as for time-division duplexing (TDD).

The intrinsically shared nature of the wireless channel is predisposed to adversarial eavesdropping and intervention. This permits eavesdropping by using a tuned receiver within an appropriate SNR range. Hence, secret key generation algorithms play a vital role in the impenetrability of information transmission over wireless networks. They can protect channels against eavesdropping and ensure the confidentiality of transmitted data. Using the reciprocity of the wireless channel, physical layer secret key generation can provide a satisfactorily secure physical layer key distribution [1]. In some current works [2] and [3], it is shown that there are reciprocal channel features not only in TDD but also in FDD systems. There is a wide variety of choices for RF channel-based key generation approaches including channel covariance matrix [4], the angle and delay of path [5], using loop-back mechanisms [6]–[8], received signal strength indicator (RSSI) [9] and deep fades [10] of the received signal. Moreover, [11] and [12] employed deep learning as a data driven method in physical layer. In this paper, in line with our previous works, we directly employ the phase differences between neighboring antennas derived from scattering parameters $S_{12}$ and $S_{21}$ bidirectional measurements between a linear antenna array and a single dipole counterpart. Since we consider FDD bands very close to each other and the reciprocity holds for the same frequency range, we can expect continuity between frequency bands. Moreover, we study the use of ESPRIT for estimating the direction of arrival. In order to reach better results on evaluation metrics, we focus on a pre-processing step as the most important stage in a standard FDD-based secret key generation procedure. For this purpose, first we propose two new mechanisms for jump removal and outlier correction on the phase difference diagrams simultaneously and then employ a polynomial curve-fitting procedure to improve the channel reciprocity.

The remainder of the paper is organized as follows. In Section II, we describe the secret key generation system design and illustrate how the new mechanisms in pre-processing can lead to better results. A brief explanation of the ESPRIT algorithm is presented in Section III. In Section IV, we explain our setup and present the numerical results related to implemented scenarios to verify the performance of the proposed scheme. Finally, Section V concludes this paper.

## II. Secret key generation system design

Figure 1 shows our proposed model for key generation in which Alice and Bob are legitimate communication partners intending to transmit data securely over a wireless channel. Moreover, there is an adversary Eve acting as a passive attacker trying to eavesdrop confidential information exchanged between them. A brief explanation of each step is given below.

### A. Channel Probing Exchange

First, Alice and Bob use a wireless environment to collect channel parameters. As it is mentioned in [3], using the direction of arrival estimation derived from $S_{12}$ and $S_{21}$, bidirectional measurements lead to good results for FDD systems. In our setup in this paper, we use a linear antenna array at Alice's end and a single dipole at Bob's side to measure angles of arrival from $S_{12}$ and $S_{21}$. After measuring the angles at

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

both sides, we compute phase differences between neighboring antennas. The linear antenna array has 20 antenna positions. Hence, after each round of measurements, we have 19 phase differences that can be used.

### *B. Pre-processing*

Pre-processing is the most important stage which plays an essential role in improving key generation performance. Robust preprocessing steps lead to getting better results in terms of efficiency and key disagreement rate (KDR).

*a) Jump detection / removal:* As we know, the presence of $2\pi$ jumps causes discontinuities in the phase diagrams. These jumps can decline the performance of a later curve-fitting procedure which leads to non-compliance of the primary generated keys from both sides after quantization. The routine procedure to prevent such jumps is to unwrap the phases. Our studies on diagrams related to a various ranges of phase difference measurements in different positions for distinct antenna arrays (linear and circular) show that, especially in noisy situations with lots of scatterers, it is not appropriate to unwrap the phase differences alone. In such cases, unwrapping the phase differences not only does not prevent the occurrence of jumps but also causes strange values for the phase difference, which in turn increases the variance of the data. Two examples of the original phase difference measurements for $S_{12}$ and $S_{21}$ measured from circular and linear arrays are illustrated in figures 2 and 3, respectively. The corresponding unwrapped version of the measurements is shown in figures 4 and 5, respectively. From these two figures, we clearly see that using a standard unwrapping procedure on the original phase differences caused a very bad result which can increase the variance of the measurements dramatically and deteriorate curve-fitting performance.

A variance increase in the phase difference of both neighboring antennas will lead to eliminating that set of measurements in constructing the final histogram, because they would be considered as too noisy. Since efficiency is defined as the ratio of usable to the total number of measurements, such measurements could reduce the efficiency. In order to have clean data in the correct interval between $-\pi$ to $\pi$, we propose a new jump detection-removing technique for the

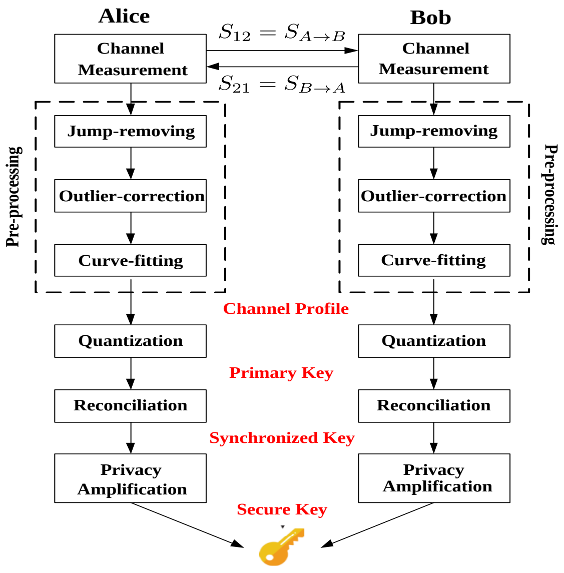

Fig. 1. The proposed model for secret key generation.

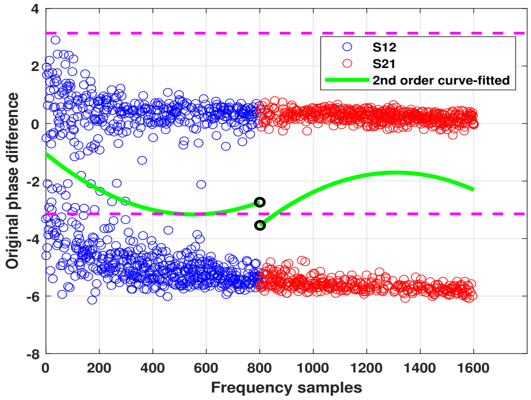

Fig. 2. Phase difference measurements for $S_{12}$ and $S_{21}$ (Example 1).

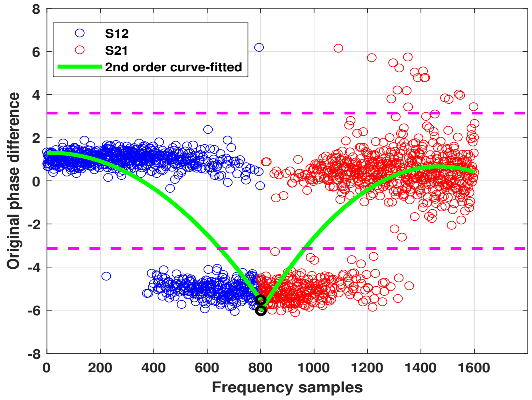

Fig. 3. Phase difference measurements for $S_{12}$ and $S_{21}$ (Example 2).

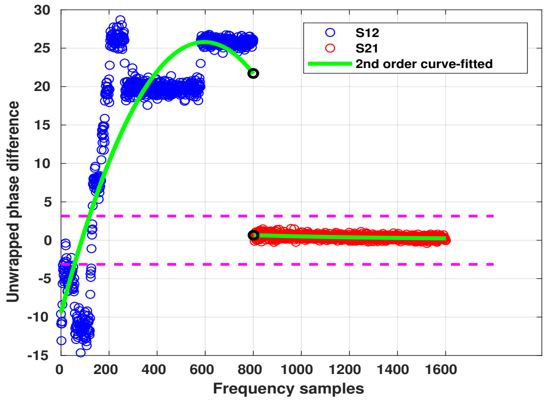

Fig. 4. Unwrapped phase difference measurements for Example 1.

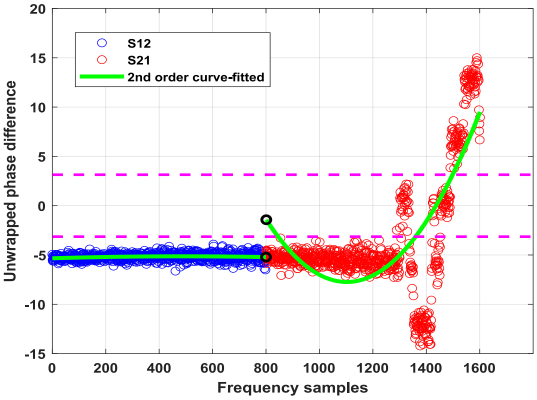

Fig. 5. Unwrapped phase difference measurements for Example 2.

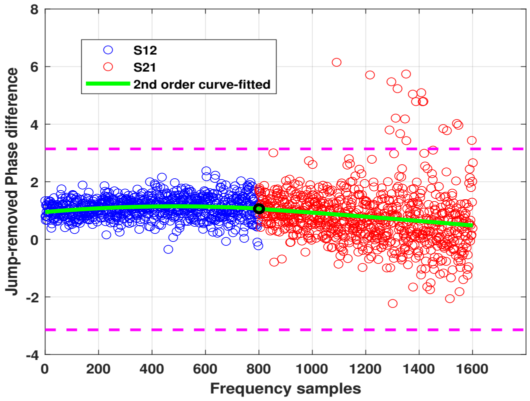

Fig. 7. Jump-removed phase difference measurements for Example 2.

phase differences. The proposed method tries to minimize the variance of the measurements over all frequency samples by applying ± $2\pi$ shifts after detecting a jump. It uses a comparison mechanism between each measurement and the average value related to all cleaned data and following the variance change after applying any shift. The jump-removed version of the phase differences related to figures 2 and 3, are shown in figures 6 and 7, respectively. As we can see from these two figures, the proposed method has been able to detect and eliminate jumps, however, some outliers are still visible outside of the desired range at the top of $+\pi$ and the bottom of $-\pi$.

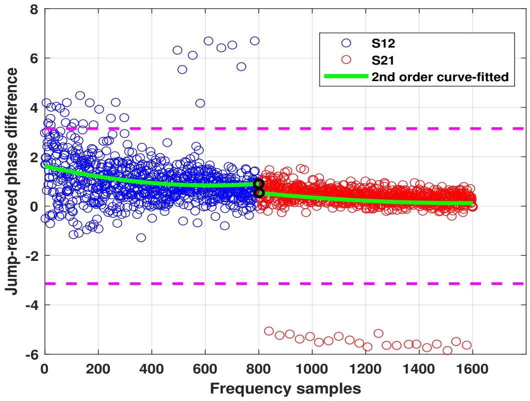

Fig. 6. Jump-removed phase difference measurements for Example 1.

*b) Outlier detection / correction:* As a complementary correction step on the jump-removed phase differences, we propose an outlier-detection method to correct them. For this purpose, we use another comparison mechanism between each measurement with the midpoint values from both left and right sides. Simultaneous use of both proposed jump and outlier correction methods leads to having clean measurements such that the midpoints from both sides are located between $-\pi$ to $+\pi$ with minimum possible variance over all frequency samples. Figures 8 and 9 demonstrate the outlier-corrected version of the phase differences for both examples 1 and 2. Moreover, the variance of the measurements for the original, unwrapped, jump-removed, and outliers-corrected measurements for both examples are reported in Table I. Comparing figures 6 to 9 clearly shows that correcting outliers leads to complete matching for the midpoint from both sides which are specified by black circles.

TABLE I
VARIANCE COMPARISON

| | Example 1 | | Example 2 | |
|---|---|---|---|---|
| | $\mathbf{S_{12}}$ | $\mathbf{S_{21}}$ | $\mathbf{S_{12}}$ | $\mathbf{S_{21}}$ |
| **Original** | 7.3424 | 8.3709 | 8.2285 | 7.8398 |
| **Unwrapped** | 140.7704 | 0.0870 | 0.1322 | 36.7705 |
| **Jump-removed** | 0.9819 | 0.9685 | 0.1322 | 0.9973 |
| **Outliers-corrected** | 0.7071 | 0.0870 | 0.1322 | 0.7614 |

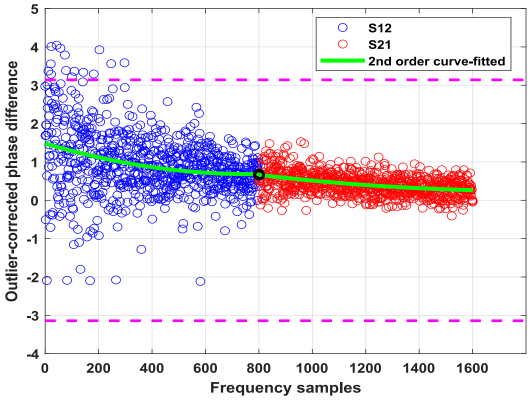

Fig. 8. Outlier-corrected phase difference measurements for Example 1.

*c) Polynomial curve-fitting:* In order to increase the channel reciprocity, we curve fit the jump/outlier-free phase differences resulting from the previous step. For this purpose, we approximate the frequency behavior of the phase difference between the transmission characteristics of the neighboring

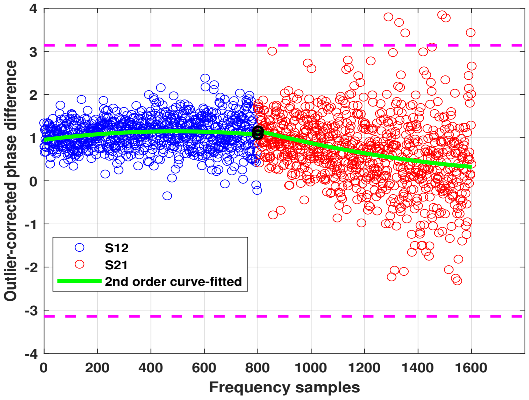

Fig. 9. Outlier-corrected phase difference measurements for Example 2.

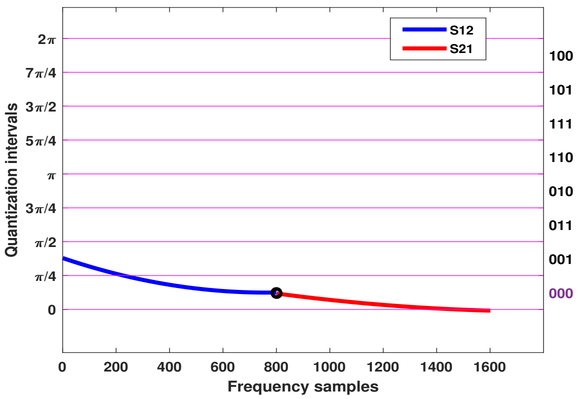

Fig. 10. Quantized phase difference measurements for Example 1.

antennas, using a second-order polynomial least-squares fit. Ideally, due to the reciprocity, we anticipate having a direct continuity between $S_{12}$ and $S_{21}$ phase difference spectral segments ($y_{12}(801) = y_{21}(802)$). However, noise and environmental reflection changes could disrupt this continuity. In order to highlight the effect of our pre-processing steps, curve-fitted results and the position of the midpoint from both sides are shown in all figures 2 to 9 with green curves and black circles.

### C. Quantization

In this stage, the midpoint phase difference estimate is then quantized into an $M$-bit vector ($M = 1, 2, 3, \dots$) to obtain a primary key segment. We use linear quantization to divide the whole $2\pi$ phase range into $2^M$ quantization intervals. Moreover, a Gray coding scheme is used to allocate an $M$-bit binary codeword to each quantization level. Consequently, at the end of this step, depending on which quantization interval the midpoint is at, we have two $M$-tuple vectors from left and right for $S_{12}$ and $S_{21}$, respectively.

### D. Reconciliation

In this step, quantization errors which are usually caused by noise and hardware imperfections must be detected and corrected. The primary keys of Alice and Bob are reconciled by forcing the quantized measurements from one side to be at the midpoint of the quantization intervals to obtain highly synchronized keys. One can further improve this by Slepain-Wolf coding based on BCH, Turbo, or LDPC codes [13]. In order to avoid key leakage, privacy amplification of synchronized keys has then to follow using some hash functions. Figures 10 and 11 show the results of the quantization and reconciliation shift along with allocated Gray codes on the right side for examples 1 and 2, respectively.

Comparing figures 2 to 11 and considering the results of Table I, we can easily see that:

- The curve-fitted results from our proposed jump-removing and outlier-correction methods considerably perform better than standard unwrapping.

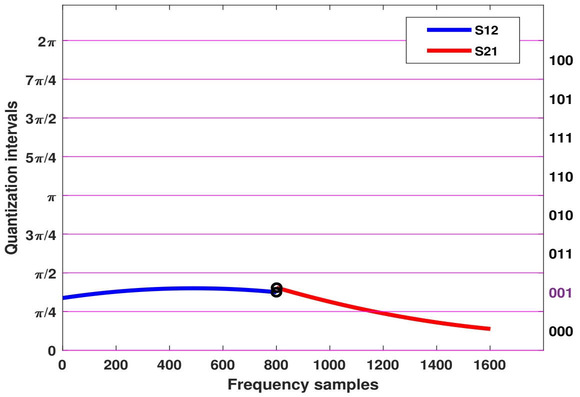

Fig. 11. Quantized phase difference measurements for Example 2.

- A combination of both proposed jump-removing and outlier-correction approaches leads to minimum variance for measurements compared with the original and unwrapped versions.
- Using the presented method, practically none of our own measurement sets had to be deleted due to the non-satisfaction of some variance threshold, hence the efficiency with this method will be 100 %.

## III. ESPRIT Algorithm

In [14], the MUSIC algorithm is used for estimating the direction of arrival of the measurements. In this paper, we employ ESPRIT [15] as a further alternative for key generation. We consider the data model of $M$ signals incident on a linear array, corrupted by noise as below and the goal is to estimate $\phi_{\mathrm{m}}, m = 1, ..., M$.

$$\mathbf{x} = \mathbf{S}\alpha + \mathbf{n} \tag{1}$$

$$\mathbf{S} = [\mathbf{s}(\phi_1)\ \mathbf{s}(\phi_2)\ \dots\ \mathbf{s}(\phi_{\mathrm{M}})] \tag{2}$$

$$\alpha = [\alpha_1\ \alpha_2\ \dots\ \alpha_{\mathrm{M}}]^{\mathrm{T}}, \tag{3}$$

in which the matrix $\boldsymbol{S}$ is an $N \times M$ matrix of the $M$ steering vectors. We can compute the correlation matrix as

$$\begin{aligned} \mathbf{R} &= \mathrm{E}\{\mathbf{x}\mathbf{x}^{\mathrm{H}}\} \qquad (4) \\ &= \mathrm{E}\{\mathbf{S}\alpha\alpha^{\mathrm{H}}\mathbf{S}^{\mathrm{H}}\} + \mathrm{E}\{\mathbf{n}\mathbf{n}^{\mathrm{H}}\} \\ &= \mathbf{S}\mathbf{A}\mathbf{S}^{\mathrm{H}} + \sigma^2\mathbf{I}\,. \qquad (5) \end{aligned}$$

By defining

$$z_m = e^{jkd\cos\phi_{\mathrm{m}}}\,, \tag{6}$$

matrix $\mathbf{S}$ can be written as

$$\mathbf{S} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ z_1 & z_2 & \cdots & z_M \\ \vdots & \vdots & \ddots & \vdots \\ z_1^{N-2} & z_2^{N-2} & \cdots & z_M^{N-2} \\ z_1^{N-1} & z_2^{N-1} & \cdots & z_M^{N-1} \end{bmatrix}. \tag{7}$$

By considering two $(N-1) \times M$ matrices $\mathbf{S_0}$ and $\mathbf{S_1}$ as

$$\mathbf{S_0} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ z_1 & z_2 & \cdots & z_M \\ \vdots & \vdots & \ddots & \vdots \\ z_1^{N-2} & z_2^{N-2} & \cdots & z_M^{N-2} \end{bmatrix}, \tag{8}$$

$$\mathbf{S_1} = \begin{bmatrix} z_1 & z_2 & \cdots & z_M \\ \vdots & \vdots & \ddots & \vdots \\ z_1^{N-2} & z_2^{N-2} & \cdots & z_M^{N-2} \\ z_1^{N-1} & z_2^{N-1} & \cdots & z_M^{N-1} \end{bmatrix}, \tag{9}$$

we can consider $\mathbf{\Phi}$ as an $M \times M$ diagonal matrix whose entries correspond to the phase shift from one element to the next for each individual signal as

$$\mathbf{\Phi} = \begin{bmatrix} z_1 & 0 & \cdots & 0 \\ 0 & z_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & z_M \end{bmatrix}. \tag{10}$$

We have $\mathbf{S_1} = \mathbf{S_0}\mathbf{\Phi}$ and if we can determine $\mathbf{\Phi}$, we can linearly obtain the DOA of all signals using Eq. (6). The ESPRIT algorithm is based on recognizing that the steering vectors inside matrix $\mathbf{S}$ span the same subspace as the matrix of signal eigenvectors $\mathbf{Q_s}$. Since both these matrices span the same subspace, there exists an invertible matrix $\mathbf{C}$ such that

$$\mathbf{Q_s} = \mathbf{S}\mathbf{C}\,. \tag{11}$$

Similarly, as we derived $\mathbf{S_0}$ and $\mathbf{S_1}$ from $\mathbf{S}$, we have $\mathbf{Q}_0 = \mathbf{S}_0\mathbf{C}$ and $\mathbf{Q}_1 = \mathbf{S}_1\mathbf{C} = \mathbf{S}_0\mathbf{\Phi}\mathbf{C}$. By defining

$$\mathbf{\Psi} = \mathbf{C}^{-1}\mathbf{\Phi}\mathbf{C}\,, \tag{12}$$

we have

$$\mathbf{Q_1} = \mathbf{Q_0}\mathbf{\Psi}\,. \tag{13}$$

The last equation implies that the matrix $\mathbf{\Phi}$ is a diagonal matrix of the eigenvalues of $\mathbf{\Psi}$, which itself results from solving Eq. (13) in a least-squares sense.

## IV. Performance Evaluation

### A. Testbed

We have considered a linear antenna array and a single dipole for Alice and Bob, respectively and use a standard vector network analyzer to measure scattering matrix parameters $S_{12}$ and $S_{21}$ in a remotely controlled fashion. We considered many scenarios in wireless indoor environments including office, home, basement, corridor, etc. 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 frequency of $2.19$ GHz.

### B. Simulation Results

We now provide measurement-based simulation results using a linear quantization and second-order polynomial curve-fitting for various locations and positions. In total, we collected 60 sets of measurements with 20 measurements in each set. We set the variance threshold at 1 to detect and remove unusable measurements with high variance for the unwrapped version of measurements. In order to investigate the effect of the polynomial degree of curve-fitting, we also applied curve-fitting with third-order and fourth-order polynomials. Figure 12 compares the resulting histogram for unwrapped version and corrected versions with different polynomial degrees over all measurements for 3-bit quantization, i.e., $8$ equally-sized quantization intervals. Corresponding simulation results show that corrected measurements with the proposed mechanism for $2nd$ order polynomial curve-fitting not only can reach $100$ % efficiency (against $96.1$ % for unwrapped version of measurements) but also leads to better KDR of $1.3 \times 10^{-2}$. Moreover, increasing the degree of the polynomial leads to a slight improvement in the KDR.

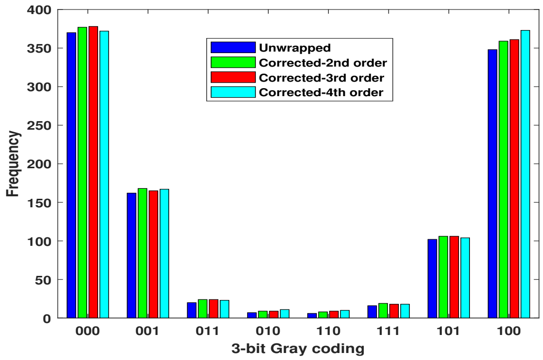

Fig. 12. Histogram over all measurements using linear quantizer with 8 intervals.

As we expected, the corresponding histogram is strongly non-uniform. One solution to overcome the non-uniformity of the resulting histogram is to randomly permute the antennas, hence probing in a permuted order [3]. Figure 13 shows the corresponding histogram with 100 permutations which clearly shows an improvement in uniformity.

It should be mentioned that we use ESPRIT to estimate the absolute phases from the measurements while unwrapping and

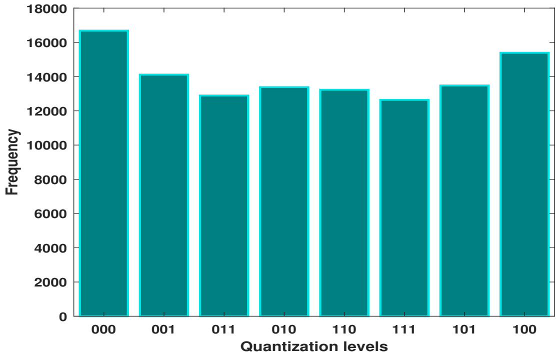

Fig. 13. Histogram over all measurements with 100 permutations and 8 intervals.

the proposed early-mentioned correction mechanisms apply to the phase differences. As an example, the sorted Eigenvalues in a decreasing manner for a measurement set to estimate absolute phases are illustrated in Fig. 14. Moreover, a DoA estimation comparison between $S_{12}$ and $S_{21}$ over all sets of measurements for 4 quantization intervals is provided in Fig. 15. Simulation results verify that in most cases estimated DoAs for $S_{12}$ and $S_{21}$ using ESPRIT are very close to each other.

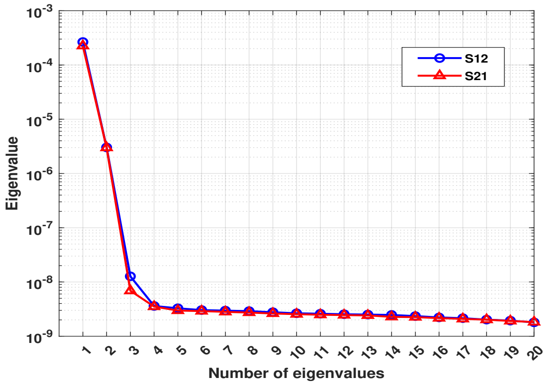

Fig. 14. ESPRIT eigenvalues for one linear array measurement.

## V. Conclusions

We developed a highly efficient key generation approach for FDD systems by employing ESPRIT for estimating the direction of arrivals. Moreover, we addressed more structured mechanisms to detect and correct unreliable measurements. For this purpose, we proposed two new mechanisms for jump removal and outlier correction on phase differences to increase efficiency. We illustrated that using polynomial curve-fitting in pre-processing step leads to increasing the channel reciprocity and compared this effect on performance metrics for different degrees of polynomials. Numerical results demonstrated that our proposed pre-processing steps along with ESPRIT can increase the efficiency to 100 $\%$ and reach competitive values for other metrics compared with unwrapping.

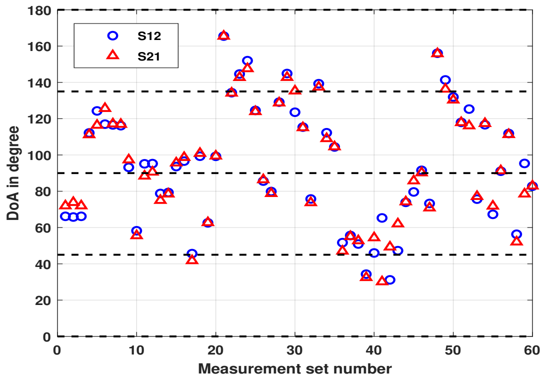

Fig. 15. DoA estimation comparison between $S_{12}$ and $S_{21}$ over 4 quantization intervals.

## 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] 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.

[3] 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.

[4] 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.

[5] 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.

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

[7] 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.

[8] D. Qin and Z. Ding, “Exploiting multi-antenna non-reciprocal channels for shared secret key generation,” *IEEE Transactions on information forensics and security*, vol. 11, no. 12, pp. 2693–2705, 2016.

[9] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, “Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels,” *IEEE Transactions on Antennas and Propagation*, vol. 53, no. 11, pp. 3776–3784, 2005.

[10] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, “Robust key generation from signal envelopes in wireless networks,” in *Proceedings of the 14th ACM conference on Computer and communications security*, pp. 401–410, 2007.

[11] X. Zhang, G. Li, J. Zhang, A. Hu, Z. Hou, and B. Xiao, “Deep learning-based physical-layer secret key generation for FDD systems,” *IEEE Internet of Things Journal*, vol. 9, no. 8, pp. 6081–6094, 2021.

[12] Y. Yang, F. Gao, G. Y. Li, and M. Jian, “Deep learning-based downlink channel prediction for FDD massive MIMO system,” *IEEE Communications Letters*, vol. 23, no. 11, pp. 1994–1998, 2019.

[13] 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.

[14] 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.

[15] R. Adve, “Direction of arrival estimation,” *Online notes available at http://www. comm. utoronto. ca/˜ rsadve/Notes/DOA. pdf*, 2003.