Pairwise Physical Layer Secret Key Generation for FDD Systems

Ehsan Olyaei Torshizi, and Werner Henkel, *Senior Member, IEEE*

***Abstract*—Physical-layer secret key generation (PSKG) stands as a promising privacy protection technique, establishing shared encryption keys through the analysis of highly correlated wireless channel measurements. This approach relies on exploiting reciprocal channel characteristics between uplink and downlink transmissions. Nonetheless, the distinct carrier frequencies employed for uplink and downlink in frequency-division duplexing (FDD) systems pose a challenge in identifying common features. This paper presents a novel approach that exploits the inherent reciprocity between scattering parameters of passive two-port networks within same frequency ranges to overcome this obstacle. By capitalizing this reciprocity and considering closely situated FDD bands, a seamless continuity is anticipated in phase differences extracted form the corresponding S-parameters, between neighboring antennas of an antenna array from both uplink and downlink directions. This continuity, thereby ensures consistency in the generated keys from both transmission ends. Furthermore, a two-stage pre-processing method is proposed to enhance performance effectively. Additionally, the paper suggests the utilization of polynomial curve-fitting through measurement data to improve reciprocity and proposes a non-linear framework for quantizing the merging points of the two FDD bands. A statistical analysis employing multiple linear regression is provided to determine the error probability associated with the generated keys. Empirical results validate the feasibility and effectiveness of the proposed key generation scheme, affirming its attributes in terms of randomness, efficiency, key distribution uniformity, and key disagreement ratio (KDR).**

***Index Terms*—Secret key generation, non-linear quantization, FDD, scattering parameters, Internet-of-Things (IoT), reciprocity**

I. Introduction

The rapid advancement of fifth-generation (5G) mobile communications, engineered to accommodate high transmission rates for various wireless devices, presents an opportunity for accelerating the adoption of the Internet of Things (IoT) across diverse industries [1]. However, the inherently shared nature of the wireless channel renders it susceptible to adversarial eavesdropping and interference, enabling unauthorized parties to intercept communications using finely-tuned receivers within an optimal signal-to-noise ratio (SNR) range [2]. Consequently, the risk of information leakage persists at both ends of the communication system.

To counteract these threats, the concept of wireless physical layer security emerges as a pivotal line of defense against eavesdropping. Its primary objective is to ensure the confidentiality of information exchanged between legitimate entities, preventing unauthorized eavesdropping and intervention. In light of these considerations, the concept of physical-layer secret key generation (PSKG) emerges as a promising solution for fortifying 5G IoT networks. These networks are characterized by their vast scale of IoT devices operating under resource constraints, mobility requirements, and a heterogeneous hierarchical architecture [3].

Effective pairwise key generation requires a significant degree of similarity in channel features between two authorized users [4]. An overview of works on PSKG, specifically related to Time Division Duplex (TDD), is provided in [5]–[9]. In Frequency Division Duplex (FDD) systems, in contrast to TDD systems, uplink and downlink transmissions occur in separate frequency bands and encounter distinct fading. Consequently, many of the mutually attainable channel parameters in TDD systems may not correspond between the uplink and downlink in FDD systems. This discrepancy poses a challenge in identifying frequency-independent reciprocal channel parameters for FDD systems. On the other hand, the majority of wireless systems, particularly 5G networks and certain existing cellular communication technologies such as Long Term Evolution (LTE) and narrowband IoT, rely on FDD [10]. Thus, the necessity to address this open problem is of great importance. Currently, key generation for FDD systems has been studied by only a small number of publications [10]–[27], such that the main methods developed recently being categorized as follows.

1) Employing the prior knowledge of the channel model to construct reciprocal features. In [10], a reciprocal channel construction framework named separating - adjusting - reconstructing (SAR) is proposed based on separating the channel paths, then adjusting them according to the carrier frequency, and finally reconstructing the path amplitude and phase. It should be mentioned that separating the channel paths for the complex multipath environment is not easy.
2) Finding the frequency-independent reciprocal channel features for key generation in FDD systems. One may consider the times of arrival (ToA) and directions of arrival (DoA) as channel parameters to hold the reciprocity in these systems. The secret key generation method by using the angle and path delay is proposed in [11]. We should keep in mind that an accurate estimation of the angle and delay is computationally challenging and needs a lot of resources including multiple antennas and large bandwidth. Moreover, using the reciprocity of channel covariance matrix eigenvalues to generate keys is developed in [12]. Nonetheless, achieving successful time and phase estimation of ToA and DoA is contingent upon employing

E. Olyaei Torshizi and W. Henkel are with the School of Electrical and Computer Engineering, Constructor University, Bremen, 28759, Germany. Emails: eolyaei@constructor.university and werner.henkel@ieee.org (See http://trsys-wh.de/).

The version based on Michael Shell's bare_jrnl.tex version 1.3.

clock synchronization schemes and specially configured antennas [13]. Furthermore, [14] and [15] proposed FDD-based PSKG approaches, leveraging the capabilities of the MUSIC and ESPRIT algorithms, respectively, during the DoA estimation phase of bidirectional measurements.

3) Loopback-based key generation approaches [16]–[18], which try to establish a channel with reciprocal channel gain. They use an additional reverse channel training phase for key generation. Channel impulse response (CIR) estimation of the combination of uplink and downlink channels [16] and only the uplink channel state information (CSI) estimation [17] are developed to generate the key. In addition, in [18], exploiting shared physical channel information on nonreciprocal forward and reverse channels is used for secret key generation. Such methods suffer from high eavesdropping risk plus high channel detection complexity [20].

The aforementioned methods for key generation in FDD systems exhibit certain limitations, including security vulnerabilities, substantial overhead, excessive complexity, and significant bandwidth requirements [16]. Alongside model-based strategies, recent advancements have explored deep learning-based approaches [3], [21]–[24]. However, these approaches are notably dependent on the environment, as the models can only discern the feature mapping function within a particular context. Given that collecting data and training models for individual communication environments require a substantial resources and training data, the practical feasibility of employing such methodologies in real-world scenarios becomes constrained [25].

Our earlier publications [4], [14], [26]–[28] establish the foundation for the current research. In [26], we were the first to demonstrate the usable symmetry of FDD with respect to the direction of arrival. In [27] and [28], we investigated key generation leveraging this reciprocity in FDD wireless and power line applications. Further research into non-linear quantization schemes and pre-processing techniques to enhance key distribution uniformity and address phase discontinuities was presented in [4] and [14], respectively. Building on our earlier works, this paper introduces a novel method to enhance communication system security through a series of effective measures. The approach leverages the inherent reciprocity between forward and reverse transmission factors of the wireless channel, treating it as a two-port network. We use phase differences between adjacent antennas in an array to establish cryptographic keys at both communication ends. Although the method is based on the proximity of narrow FDD bands, empirical results confirm that reciprocity is maintained across both separated and wider FDD bands.

In general, main contributions of the proposed approach are described as follows:

1) Introducing the inherent reciprocity of S-parameters for the wireless channel, modeled as a two-port network, and utilizing phase differences between two adjacent antennas derived from S_{12} and S_{21} within an antenna array, can provide the necessary reciprocity for key generation in FDD systems.
2) Presenting a two-stage pre-processing algorithm that incorporates jump removal and outlier correction for measured phase differences across two FDD bands, with the aim of achieving optimized efficiency. Additionally, introducing polynomial curve-fitting as a denoising technique to enhance the channel reciprocity of the pre-processed measurements across FDD bands.
3) Introducing a novel non-linear quantization scheme aimed at achieving a more uniform distribution for generated keys over all quantization intervals. Additionally, proposing a new, simplistic, and highly effective concept of non-coding one-sided centering key reconciliation, which significantly mitigates the KDR.
4) Attaining a satisfactory KDR, high efficiency levels, requisite randomness, and a more uniform distribution in the resulting key distribution, validated through real measurement data with two antenna configurations.

The remainder of this paper is organized as follows. In Section II, we describe the system model, scattering parameters, and channel reciprocity. Section III provides a comprehensive overview of each stage of our proposed FDD-based PSKG scheme, including two illustrative examples that demonstrate all procedural steps. Sections IV and V present a non-linear quantization method and an in-depth error probability analysis using multiple linear regression, respectively. Section VI introduces our testbed and performance metrics, followed by the validation of the proposed scheme through extensive simulations and experiments. Section VII offers a complementary discussion on some key features, and the paper concludes in Section VIII.

II. System Model and Scattering Parameters

A. System Model Description

As shown in Fig. 1, we consider a basic key generation model that involves two legitimate partners, namely, Alice and Bob, which try to securely transmit encrypted confidential information exclusively between each other.

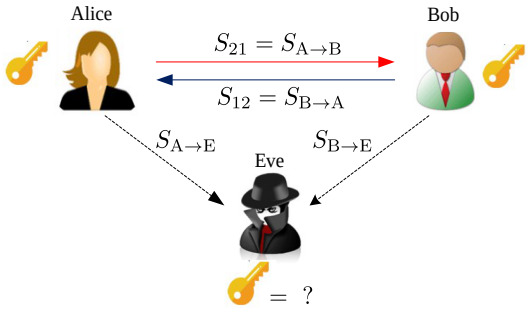


Fig. 1: Basic model of the key generation setup

For this purpose, a matching pair of keys is generated based on the CSI acquired through channel probing by both parties. Moreover, we consider an adversary Eve as a passive attacker who can monitor all the communications during the key generation process and attempts to intercept the generated keys between Alice and Bob. Considering Eve is located sufficiently away from both Alice and Bob, we can ensure uncorrelatedness between the legitimate channel $A \to B$ and wiretap channels $A \to E$ and $B \to E$.

B. Scattering Parameters

Scattering parameters, commonly referred to as S-parameters, constitute the fundamental language of radio-frequency (RF) engineering [29]. They are complex phasor quantities that vary with frequency, essential for describing the electrical behavior of linear electrical networks under various steady-state electrical signal stimuli. Serving as primary descriptors in the frequency domain, particularly at high frequencies where wave-based models are imperative, S-parameters provide comprehensive insights into signal transmission, attenuation, and impedance matching. They form the cornerstone for the efficient analysis, optimization, and design of two-port networks, quantifying both amplitude and phase relationships between incident and reflected waves at each network port.

For a 2-port RF network, the S-parameter matrix describes the relationship between the incident (a_1 and a_2) and reflected (b_1 and b_2) wave parameters as follows:

$$\begin{bmatrix} b_1 \\ b_2 \end{bmatrix} = \begin{bmatrix} S_{11} & S_{12} \\ S_{21} & S_{22} \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \end{bmatrix} , \tag{1}$$

where S_{11} and S_{22} represent the reflection factors, S_{12} and S_{21} signify the forward and reverse transmission factors, respectively. These parameters can be determined as follows:

$$\begin{aligned} S_{11} &= \frac{b_1}{a_1}\Big|_{a_2=0} , \qquad S_{12} = \frac{b_1}{a_2}\Big|_{a_1=0} , \\ S_{21} &= \frac{b_2}{a_1}\Big|_{a_2=0} , \qquad S_{22} = \frac{b_2}{a_2}\Big|_{a_1=0} . \end{aligned} \tag{2}$$

A vector network analyzer (VNA) is a widely used instrument for quantifying scattering matrix parameters, particularly S_{12} and S_{21}, due to its ability to provide simultaneous, precise, and comprehensive evaluations of the complex transmission and reflection characteristics among ports. However, in practical implementations for IoT applications, using VNAs is not feasible. Instead, a multi-carrier transmission approach is often employed, where the transfer function is anyhow measured, serving as a practical alternative. To establish the relationship between the voltage transfer function and S-parameters, the incident and reflected power waves at each port are expressed in terms of the port voltages and currents [29] as follows:

$$a_i = \frac{1}{2}\frac{(V_i + Z_0 I_i)}{\sqrt{|\Re\{Z_0\}|}}, \quad b_i = \frac{1}{2}\frac{(V_i - Z_0^* I_i)}{\sqrt{|\Re\{Z_0\}|}} \tag{3}$$

where, V_i and I_i represent the voltage and current at port i, respectively, while Z_0 denotes the system's characteristic impedance. Under matched conditions, the incident wave at port 2 is zero, simplifying the S-parameter equation to $b_2 = S_{21}a_1$. For the incident wave at port 1 (a_1) under matched conditions, we assume $I_1 = \frac{V_1}{Z_0}$. In our case, assuming $Z_0 = Z_0^*$, it leads to $a_1 = \frac{V_1}{\sqrt{|\Re\{Z_0\}|}}$. Similarly, b_2 is given by $b_2 = \frac{V_2}{\sqrt{|\Re\{Z_0\}|}}$. By substituting a_1 and b_2 into the S-parameter equation, we derive:

$$H(f) = \frac{V_2}{V_1} = \frac{S_{21}(f)}{1 + S_{11}(f)} , \tag{4}$$

In the case where both ports are perfectly matched to their respective characteristic impedances, reflection is nullified, thereby resulting in $H(f) = S_{21}(f)$.

C. Channel Reciprocity

Channel reciprocity, temporal variation, and spatial decorrelation can be considered as the desired propagation characteristics of wireless channels to realize a key generation scheme. It exhibits *common* randomness for secret key generation such that its reciprocity ensures the similarity of generated keys, while temporal decorrelation provides the randomness of resulting keys. In network theory, reciprocity implies that the transmission characteristics between two ports remain unchanged when the source and load are interchanged. Mathematically, reciprocity in a two-port context manifests as $Z_{12} = Z_{21}$, $Y_{12} = Y_{21}$, and $\det(A) = 1$. Furthermore, reciprocity can be expressed in terms of S-parameters, where a two-port network is considered reciprocal if its S-parameter matrix is identical to its transpose, signifying $S_{12} = S_{21}$. These conditions hold for every passive two-port network. A wireless channel, along with connecting cables, can be conceptualized as a two-port system. Reciprocity strictly holds within the same frequency range, making S_{12} and S_{21} interchangeable.

For the first time, we are leveraging this inherent reciprocity for secret key generation in FDD systems. To achieve this, we begin by measuring the scattering parameters, S_{12} and S_{21}, obtained through bidirectional measurements between Alice and Bob. Subsequently, we utilize the phase differences between adjacent antennas directly as parameters to maintain reciprocity at both ends within the same frequency range. The reciprocity of the channel ensures that identical scattering parameters are measured at both ends, thereby guaranteeing consistent phase differences between antennas in Alice's array, which can be measured from either side. Furthermore, utilizing phase differences offers robustness against noise by canceling out shared artifacts, mitigates systematic errors through cancellation during subtraction, and simplifies measurement techniques. It eliminates the need for normalization or calibration by focusing on relative phases rather than absolute values, ultimately enhancing accuracy and practicality.

We employ closely-spaced frequency bands for uplink and downlink in FDD to mitigate excessive frequency dependencies among reflectors and antennas, ensuring a continuum of corresponding phase differences and maintaining requisite reciprocity. Notably, reciprocity is preserved even with separated FDD bands. Although accurate S-parameter measurements with VNAs typically require meticulous calibration, our PSKG method, based on phase differences between adjacent antennas, eliminates this necessity. Nonetheless, we adhere to standard VNA two-port calibration practices as a best practice, despite it not being essential for our method.

III. Proposed FDD-based PSKG Scheme

In this section, we present the proposed PSKG scheme and elaborate in detail on how to employ the phase differences between neighboring antennas derived from scattering matrix parameters S_{12} and S_{21} bidirectional measurements to generate the correlated keys for FDD systems. All the notations used in the model are summarized in Table I.

A. System Configuration

Given that we rely on phase differences between neighboring antennas, derived from bidirectional scattering parameters S_{12}

TABLE I: Notation summary of used symbols

Symbols	Description
$\mathbf{H}_{\mathrm{A}}$, $\mathbf{H}_{\mathrm{B}}$	Alice's and Bob's channel profile
N	Number of frequency samples
$\Delta\phi_l$	l-th phase difference at Alice's $(1 \leq l \leq N)$ and Bob's side $(N+1 \leq l \leq 2N)$
$\mathbf{H}_{\mathrm{A},jr}$, $\mathbf{H}_{\mathrm{B},jr}$	Jump-removed measurements vectors at Alice and Bob
$\mathbf{H}_{\mathrm{A},pp}$, $\mathbf{H}_{\mathrm{B},pp}$	Pre-processed measurements vectors at Alice and Bob
$\mathbf{H}_{\mathrm{A},cf}$, $\mathbf{H}_{\mathrm{B},cf}$	Curve-fitted measurement vectors at Alice and Bob
k	Polynomial curve-fitting order
$\widehat{\Delta\phi}_{\mathrm{A},m}$, $\widehat{\Delta\phi}_{\mathrm{B},m}$	Estimated phase difference of merging point at Alice and Bob
$a_{A,i}$, $a_{B,j}$	Polynomial coefficients for Alice and Bob
$\mathcal{Q}_{\mathrm{A}}$, $\mathcal{Q}_{\mathrm{B}}$	Alice's and Bob's quantization interval
S_{A} , S_{B}	Required shift for Alice and Bob
S_{r}	Reconciliation shift
$\widehat{\Delta\phi}_{\mathrm{A},r}$, $\widehat{\Delta\phi}_{\mathrm{B},r}$	Reconciled version of $\widehat{\Delta\phi}_{\mathrm{A},m}$, $\widehat{\Delta\phi}_{\mathrm{B},m}$
$\mathcal{Q}_{\mathrm{A},r}$, $\mathcal{Q}_{\mathrm{B},r}$	Alice and Bob quantization interval after reconciliation
$\mathbf{K}_{\mathrm{A}}$, $\mathbf{K}_{\mathrm{B}}$	Alice's and Bob's key bits

and S_{21}, as a reciprocal attribute for key generation, the presence of an antenna array comprising at least two antennas is necessary at either Alice's or Bob's side. It is pertinent to note that, owing to the principle of reciprocity, the inclusion of a single antenna array at one side is sufficient. This is because reciprocity dictates that the electromagnetic characteristics of a system remain invariant when the roles of transmitter and receiver are interchanged. Hence, in a scenario featuring a single dipole antenna at Bob's side and an antenna array at Alice's side, reciprocity entails that the channel response between Alice and Bob remains consistent irrespective of whether Alice's array transmits and Bob's dipole receives, or vice versa. In our experimental configuration, Alice is realized as an linear or circular antenna array, while both Bob and Eve are equipped with individual single dipoles.

B. Channel Probing over FDD Bands

First, Alice and Bob use a wireless environment to construct data sets by extracting phase differences between neighboring antennas from measured scattering parameters. In order to construct the channel profiles, we conducted measurements of S_{12} and S_{21} at two distinct dedicated neighboring Δf frequency bands on either side of a central frequency of f_c such that the uplink and downlink frequency width satisfies $\Delta f \ll f_c$. The channel frequency response (CFR) of the l-th frequency sample, $f_l \in [f_c - \Delta f, f_c + \Delta f]$, for $1 \leq l \leq 2N$ can be expressed as

$$H(f_l) = S_{21}(f_l) = |S_{21}(f_l)|e^{j\phi_{21}(f_l)} \ , \tag{5}$$

where $|S_{21}(f_l)|$ and $\phi_{21}(f_l)$ are considered as magnitude and absolute phase of the transmission coefficient at the l-th frequency sample, respectively. Obviously, the absolute phase $\phi_{21}(f_l)$ is directly related to the time delay τ_l experienced by the signal as it travels from one antenna to the other by $\phi_{21}(f_l) = -j2\pi f_l \tau_l$. This can also be formulated dependent on distance d as $\phi_{21}(f_l) = -2\pi d/\lambda$, which clearly explains the difference in absolute phase between antennas.

Specifically, we designate the link from Bob to Alice as Band I and measure the vector $\mathbf{S_{12}}$ within this band, which consists of N frequency samples, where $l \in \{1, 2, \ldots, N\}$. Similarly, Band II is assigned to the link from Alice to Bob, and the

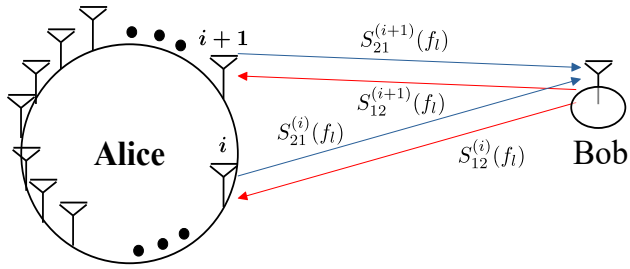


Fig. 2: The antenna system at Alice's and Bob's ends along with the corresponding S-parameters

vector $\mathbf{S_{21}}$ is measured for the same number of frequency samples, where $l \in \{N+1, N+2, \ldots, 2N\}$. Furthermore, let $X_{A,i}(f_l)$ denote the signal transmitted from the i-th antenna at Alice, and $Y_{B,i}(f_l)$ represent the signal received at Bob from the i-th antenna at Alice. Similarly, let $X_{B,i}(f_l)$ denote the signal transmitted from Bob to the i-th antenna at Alice, and $Y_{A,i}(f_l)$ represent the corresponding received signal at the i-th antenna form Bob. Consequently, the signal model in Bands I (uplink) and II (downlink) can be expressed as:

$$Y_{A,i}(f_l) = S_{12}^{(i)}(f_l) \cdot X_{B,i}(f_l), \quad 1 \leq l \leq N \ , \tag{6}$$

$$Y_{B,i}(f_l) = S_{21}^{(i)}(f_l) \cdot X_{A,i}(f_l), \quad N+1 \leq l \leq 2N \ . \tag{7}$$

Considering the measurement of S-parameters for two consecutive antennas within Alice's array, labeled as i and $i+1$, as shown in Fig. 2, we obtain $S_{12}^{(i)}(f_l)$ and $S_{12}^{(i+1)}(f_l)$ at Alice's side, and $S_{21}^{(i)}(f_l)$ and $S_{21}^{(i+1)}(f_l)$ at Bob's side. Consequently, the corresponding absolute phases $\phi_{12}^{(i)}(f_l)$ and $\phi_{12}^{(i+1)}(f_l)$ at Alice's side, and $\phi_{21}^{(i)}(f_l)$ and $\phi_{21}^{(i+1)}(f_l)$ at Bob's side, can be extracted. We then determine the phase differences between two neighboring antennas for all N frequency samples within each FDD band. For the measurements corresponding to antennas i and $i+1$, the phase difference for the l-th frequency sample can be calculated at both Alice's and Bob's sides as

$$\Delta\phi_l^{(i,i+1)} = \begin{cases} \phi_{12}^{(i)}(f_l) - \phi_{12}^{(i+1)}(f_l), & 1 \leq l \leq N \ , \\ \phi_{21}^{(i)}(f_l) - \phi_{21}^{(i+1)}(f_l), & N+1 \leq l \leq 2N \ . \end{cases} \tag{8}$$

Finally, for antennas i and $i+1$, the channel profiles $\mathbf{H}_{\mathrm{A}} = \mathbf{H}(f_{B\to A})$ and $\mathbf{H}_{\mathrm{B}} = \mathbf{H}(f_{A\to B})$ using extracted phase differences from measured S_{12} and S_{21} can be constructed, respectively as

$$\mathbf{H}_{\mathrm{A}} = [\Delta\phi_1^{(i,i+1)}, \Delta\phi_2^{(i,i+1)}, ..., \Delta\phi_N^{(i,i+1)}]^{\mathrm{T}} \ , \tag{9}$$

$$\mathbf{H}_{\mathrm{B}} = [\Delta\phi_{N+1}^{(i,i+1)}, \Delta\phi_{N+2}^{(i,i+1)}, ..., \Delta\phi_{2N}^{(i,i+1)}]^{\mathrm{T}} \ . \tag{10}$$

Furthermore, we designate the N-th and $(N+1)$-th phase differences across both FDD bands as the merging points $\Delta\phi_{\mathrm{A},m} = \Delta\phi_N^{(i,i+1)}$ and $\Delta\phi_{\mathrm{B},m} = \Delta\phi_{N+1}^{(i,i+1)}$ from Alice's and Bob's perspectives, respectively. Ideally, these adjacent phase differences between the two bands should exhibit a continuous transition, assuming the absence of noise and band gaps (which will be addressed subsequently). To enhance continuity, polynomial interpolation will be employed within the bands for denoising purposes. Consequently, the corresponding phase differences at these merging points on both sides should ideally align and will be utilized for key generation at both ends.

Two exemplary measurements related to linear and circular arrays, along with the corresponding measurement environments and antenna positions for Alice, Bob, and Eve, are illustrated in figures 3 and 4, respectively. We have conducted

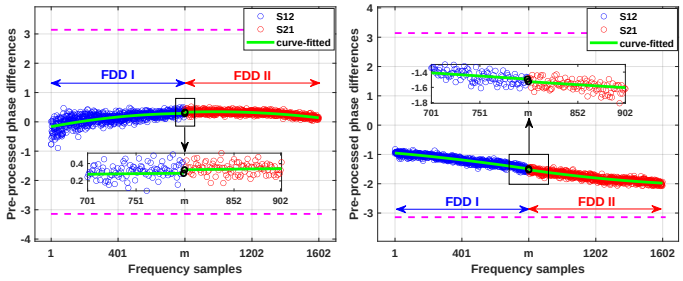


Fig. 3: Two exemplary measurements; Left: UCA, Right: ULA

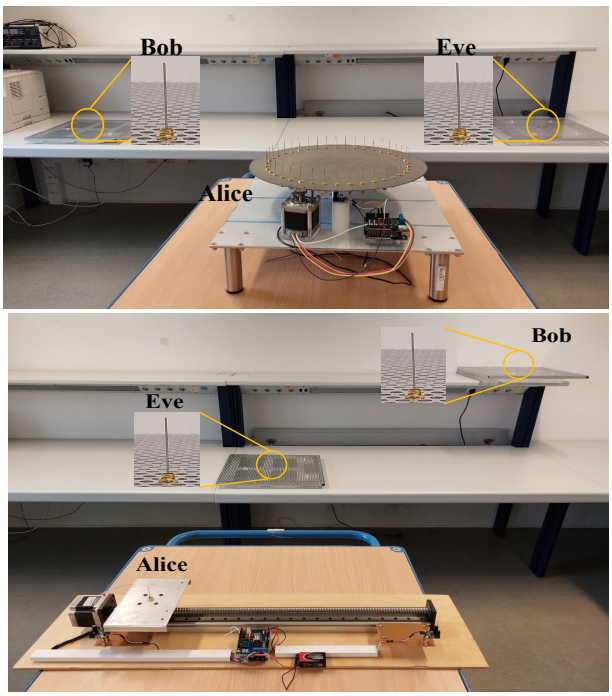


Fig. 4: Exemplary measurement arrangements; Top: UCA, Bottom: ULA

measurements in an averaged-out manner and examined the phase differences for $N = 801$ frequency samples within each FDD band. These phase differences are depicted in radians using blue and red circles. The merging points from the left and right sides are denoted as "m" in the figures. Additionally, purple dashed lines represent the lower and upper bounds of phase difference, which are $-\pi$ and $+\pi$, respectively. Furthermore, the second order fitted curves are presented, highlighting the impact of the proposed pre-processing steps on the curve-fitting outcomes and the positioning of the merging points from both directions.

C. Pre-processing

This section emphasizes the pivotal role of measured data pre-processing in significantly improving key generation performance, particularly in terms of efficiency and KDR. While continuity at merging points from both left and right is typically maintained in measured data, instances arise where discontinuities manifest, particularly within very low SNR regimes. This occurrence is particularly notable when scatterers or obstacles are intentionally positioned along the line-of-sight (LoS) trajectory connecting the transmit and receive antennas. Moreover, phase data may exhibit 2π jumps, causing discontinuities in the original phase differences derived from S_{12} and S_{21}. These discontinuities lead to the generation of dissimilar keys, thereby increasing the KDR. The conventional approach, phase unwrapping, aims to rectify phase differences by adjusting them by integrating multiples of $\pm 2\pi$ until the gap between successive phase differences falls below π. However, our analysis reveals its limited effectiveness, as it not only may fail to provide clean data within the desired interval of $-\pi$ to $+\pi$ but also exacerbates variance, thereby reducing efficiency. We propose an efficient pre-processing approach for removing these jumps, relying on minimizing data variance and adhering to several key principles:

- **Continuity Maintenance:** Ensuring the continuity of phase differences across two FDD bands as distinct curves is essential. In highly noisy environments, the unwrapping process may prove inadequate in achieving this desired continuity.
- **Variance Minimization:** Minimizing variance among phase differences within each FDD band individually is crucial to prevent the exclusion of corresponding data due to failure to meet the variance threshold, which can adversely affect efficiency.
- **Clean Data Provision:** Ensuring the provision of clean data within the correct interval of $-\pi$ and $+\pi$ is imperative. To achieve this, the algorithm must not only detect and remove jumps but also identify and correct potential outliers. Failure to address these issues can compromise the performance of subsequent curve-fitting procedure, resulting in non-compliance of primary generated keys from both sides after quantization.

Therefore, our proposed pre-processing scheme comprises three key steps:

1) Jump Detection / Removal: The proposed method adopts a comparative approach to detect jumps. Initially, it computes the variance of phase differences associated with frequency samples within a specified set. This set is constructed by incrementally adding phase differences, starting from the first one and subsequently incorporating others in sequential order. Throughout this process, it ensures that the variance of the entire collection remains below a predefined threshold after each new sample is included. Simultaneously, the method ensures that the deviation between the newly added sample and the average of all previously processed data does not exceed a predetermined limit. During this process, the method identifies the samples that do not satisfy these two conditions and endeavors to rectify them by applying $\pm 2\pi$ adjustments for jump elimination, thereby facilitating variance minimization.

2) Outlier Detection / Correction: The second stage of the proposed pre-processing scheme focuses on identifying and rectifying any potential remaining outliers in the phase differences after the removal of jumps. It employs another comparative mechanism where each measurement is compared to both the merging point and the mean of all measurements within the corresponding FDD band. If the absolute difference

Algorithm 1 Jump Detection/Removal

Input: Alice's (Bob's) known probing vector $\mathbf{H}_{\mathrm{A}}$ ($\mathbf{H}_{\mathrm{B}}$), Variance threshold V_{th}, predetermined limit L

Output: Jump-removed measurements vector at Alice's (Bob's) side $\mathbf{H}_{\mathrm{A},jr}$ ($\mathbf{H}_{\mathrm{B},jr}$)

$\mathbf{H}_{\mathrm{A},jr} \leftarrow \mathbf{H}_{\mathrm{A}}(1)$
for $i = 2:1:N$ **do**
  $Avg \leftarrow \mathrm{mean}(\mathbf{H}_{\mathrm{A},jr})$
  $\mathbf{H}_{\mathrm{A},jr} \leftarrow [\mathbf{H}_{\mathrm{A},jr}, \mathbf{H}_{\mathrm{A}}(i)]$
  $Var \leftarrow \mathrm{variance}(\mathbf{H}_{\mathrm{A},jr})$
  if $|\mathbf{H}_{\mathrm{A},jr}(i) - Avg| > \pi \quad \&\& \quad Var > V_{th}$ **then**
    $\mathbf{H}_{\mathrm{A},jr}(i) \leftarrow \mathbf{H}_{\mathrm{A}}(i) - 2\pi$
    $Var_{\mathrm{new}} \leftarrow \mathrm{variance}(\mathbf{H}_{\mathrm{A},jr})$
  else
    if $Var_{\mathrm{new}} > Var$ **then**
      $\mathbf{H}_{\mathrm{A},jr}(i) \leftarrow \mathbf{H}_{\mathrm{A}}(i) + 2\pi$
    end
  end
  $i \leftarrow i + 1$
end

between any phase difference and the merging point value, as well as the mean of all measurements, exceeds π, it is flagged as an outlier. Subsequently, the algorithm corrects such outliers by applying a $\pm 2\pi$ shift, ensuring minimized variance. Algorithms 1 and 2, delineated as step-wise pseudo-codes, offer a comprehensive elucidation of the procedural steps involved in jump removal and outlier correction. Applying both proposed schemes result in cleaned measurements, denoted as $\mathbf{H}_{\mathrm{A},pp}$ and $\mathbf{H}_{\mathrm{B},pp}$, at Alice's and Bob's respective ends. This ensures that the midpoints fall within the range of $-\pi$ to $+\pi$, while simultaneously achieving the lowest possible variance across all frequency samples. This alignment significantly augments the assurance in generating identical keys from both ends.

3) Polynomial Curve-Fitting: In this section, we approximate the frequency behavior of jump/outlier-free phase differences between the transmission characteristics of adjacent antennas as obtained from the prior steps. This is achieved through a least-squares polynomial curve fitting. Such an approach enhances channel reciprocity and mitigates noise across the two FDD bands. The corresponding curve-fitted versions of measurements at Alice's and Bob's sides, respectively, within bands I and II can be expressed as

$$\mathbf{H}_{\mathrm{A},cf} = \sum_{i=0}^{k} a_{A,i}\ x^i\ , \quad 1 < x < N\ , \tag{11}$$

$$\mathbf{H}_{\mathrm{B},cf} = \sum_{j=0}^{k} a_{B,j}\ x^j\ , \quad N+1 < x < 2N\ , \tag{12}$$

where k represents the order of the polynomial fitted curve and $a_{A,i}$, $a_{B,j}$ are the corresponding coefficients at Alice's and Bob's sides, respectively. Moreover, x symbolizes the frequency samples belonging to $\{1, 2, ..., N\}$ and $\{N+1, N+2, ..., 2N\}$ for FDD-bands I and II, respectively. Consequently, the estimated phase differences at the merging points can be expressed as

$$\widehat{\Delta\phi}_{\mathrm{A},m} = \mathbf{H}_{\mathrm{A},cf}(N) = \sum_{i=0}^{k} a_{A,i}\ (N)^i\ , \tag{13}$$

Algorithm 2 Outlier Detection/Correction

Input: Jump-removed measurements vector at Alice's (Bob's) side $\mathbf{H}_{\mathrm{A},jr}$ ($\mathbf{H}_{\mathrm{B},jr}$)

Output: Pre-processed measurements vector at Alice's (Bob's) side $\mathbf{H}_{\mathrm{A},pp}$ ($\mathbf{H}_{\mathrm{B},pp}$)

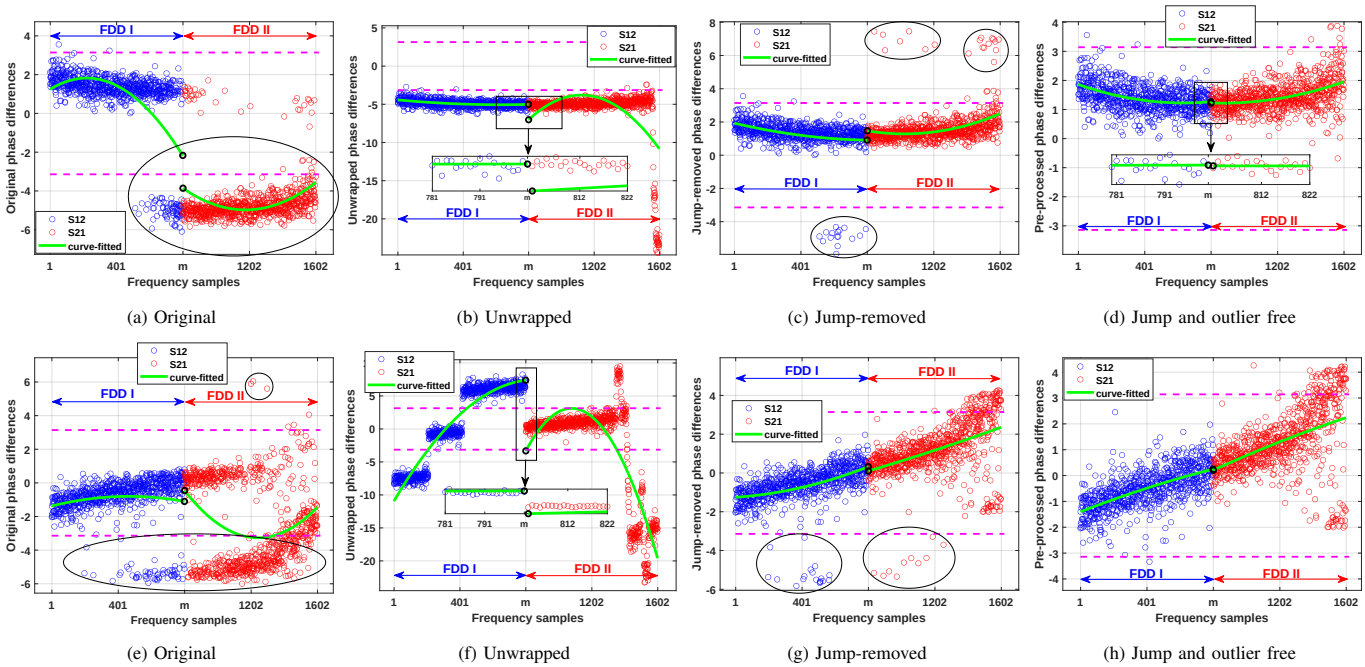
$\mathbf{H}_{\mathrm{A},pp} \leftarrow \mathbf{H}_{\mathrm{A},jr}$
for $i = 1:1:N$ **do**
  if $\mathbf{H}_{\mathrm{A},jr}(i) - \mathbf{H}_{\mathrm{A},jr}(N) > \pi$ **then**
    $\mathbf{H}_{\mathrm{A},pp}(i) \leftarrow \mathbf{H}_{\mathrm{A},jr}(i) - 2\pi$
  else
    if $\mathbf{H}_{\mathrm{A},jr}(i) - \mathbf{H}_{\mathrm{A},jr}(N) < -\pi$ **then**
      $\mathbf{H}_{\mathrm{A},pp}(i) \leftarrow \mathbf{H}_{\mathrm{A},jr}(i) + 2\pi$
    end
  end
  $i \leftarrow i + 1$
end
$Avg \leftarrow \mathrm{mean}(\mathbf{H}_{\mathrm{A},pp})$
for $i = 1:1:N$ **do**
  if $\mathbf{H}_{\mathrm{A},pp}(i) - Avg < -\pi \quad \&\& \quad \mathbf{H}_{\mathrm{A},pp}(i) < \mathbf{H}_{\mathrm{A},pp}(N)$ **then**
    $\mathbf{H}_{\mathrm{A},pp}(i) \leftarrow (\mathbf{H}_{\mathrm{A},pp})(i) + 2\pi$
  else
    if $\mathbf{H}_{\mathrm{A},pp}(i) - Avg > \pi \quad \&\& \quad \mathbf{H}_{\mathrm{A},pp}(i) > \mathbf{H}_{\mathrm{A},pp}(N)$ **then**
      $\mathbf{H}_{\mathrm{A},pp}(i) \leftarrow \mathbf{H}_{\mathrm{A},pp}(i) - 2\pi$
    end
  end
  $i \leftarrow i + 1$
end

$$\widehat{\Delta\phi}_{\mathrm{B},m} = \mathbf{H}_{\mathrm{B},cf}(N+1) = \sum_{j=0}^{k} a_{B,j}\ (N+1)^j\ . \tag{14}$$

Ideally, due to the reciprocity, we expect to have a direct continuity at the merging points between phase difference spectral segments of S_{12} and S_{21} ($\widehat{\Delta\phi}_{\mathrm{A},m} = \widehat{\Delta\phi}_{\mathrm{B},m}$). However, noise and hardware imperfections could disrupt this continuity. As another example, Fig. 5 shows two illustrative phase difference measurements between two adjacent antennas for S_{12} and S_{21} related to designed circular and linear arrays. The original phase difference measurements are depicted in figures 5(a) and 5(e) for the UCA and ULA, respectively. Figures 5(b) and 5(f) reveal how applying a standard unwrapping technique to the initial phase differences yields unsatisfactory outcomes in these cases, dramatically increasing the variance of the measurements and consequently decreasing the curve-fitting performance. Moreover, figures 5(c) and 5(g) show jump-removed phase differences, while figures 5(d) and 5(h) illustrate outlier-corrected versions. They clearly demonstrate that the proposed pre-processing algorithms adeptly detect and remedy jumps and outliers, resulting in nicely matching merging points for both examples.

D. Quantization

At this stage, phase difference estimates obtained from the polynomial fitted curves at the merging points of two FDD regions should be quantized into an M-bit vector ($M = 1, 2, 3, ...$) separately, to generate primary key segments. A linear quantization scheme divides the whole 2π phase range into



(a) Original (b) Unwrapped (c) Jump-removed (d) Jump and outlier free

(e) Original (f) Unwrapped (g) Jump-removed (h) Jump and outlier free

Fig. 5: Phase difference measurements for S_{12} and S_{21} between two antennas; Top: Example I (UCA), Bottom: Example II (ULA)

2^M equal quantization intervals as $[2\pi(i-1)/2^M, 2\pi i/2^M)$, $1 \le i \le 2^M$. Therefore, the first part of the quantization, based on the estimated phase differences to determine corresponding interval numbers $\mathcal{Q}_{\rm A}$ and $\mathcal{Q}_{\rm B}$ for Alice and Bob which are belong to $\{1, 2, ..., 2^M\}$ can be determined by

$$\begin{aligned} &\mathrm{Q}(\widehat{\Delta\phi}_{\mathrm{A},m}) = \mathcal{Q}_{\rm A} \\ &\text{if} \quad \mathrm{mod}\,(\widehat{\Delta\phi}_{\mathrm{A},m}, 2\pi) \in \left[\frac{2\pi(\mathcal{Q}_{\rm A}-1)}{2^M}\ ,\ \frac{2\pi\ \mathcal{Q}_{\rm A}}{2^M}\right) ; \end{aligned} \tag{15}$$

$$\begin{aligned} &\mathrm{Q}(\widehat{\Delta\phi}_{\mathrm{B},m}) = \mathcal{Q}_{\rm B} \\ &\text{if} \quad \mathrm{mod}\,(\widehat{\Delta\phi}_{\mathrm{B},m}, 2\pi) \in \left[\frac{2\pi(\mathcal{Q}_{\rm B}-1)}{2^M}\ ,\ \frac{2\pi\ \mathcal{Q}_{\rm B}}{2^M}\right) ; \end{aligned} \tag{16}$$

To ensure that each quantization level is assigned a unique M-bit binary codeword in such a way that only a single bit alters when crossing quantization boundaries, Gray coding pattern is utilized. As a result of this process, based on the acquired $\mathcal{Q}_{\rm A}$ and $\mathcal{Q}_{\rm B}$, two M-tuple vectors corresponding to S_{12} and S_{21}, respectively, are obtained.

E. Reconciliation

In general, there might be a mismatch between the allocated binary Gray sequences obtained and quantized by Alice and Bob, usually caused by noise and hardware imperfections. Reconciliation involves addressing the key disagreement present in the primary keys generated by Alice and Bob, often employing binary linear codes. To reduce the complexity and computational costs associated with coding schemes, we propose a simple yet effective One-Sided Centering (OSC) approach for key reconciliation. We force the quantized measurements from one side to be at the midpoint of the quantization intervals. Therefore, based on obtained $\mathcal{Q}_{\rm A}$ and $\mathcal{Q}_{\rm B}$, we determine the required shift to relocate one of the merging points into the middle of its quantization interval. This shift is then applied to all frequency samples spanning both FDD bands. The required shift value for each side could be obtained by

$$S_{\rm A} = \widehat{\Delta\phi}_{\mathrm{A},m} - \frac{\pi(2\mathcal{Q}_{\rm A}-1)}{2^M} = \sum_{i=0}^{k} a_{A,i}\,(N)^i - \frac{\pi(2\mathcal{Q}_{\rm A}-1)}{2^M}\ , \tag{17}$$

or

$$S_{\rm B} = \widehat{\Delta\phi}_{\mathrm{B},m} - \frac{\pi(2\mathcal{Q}_{\rm B}-1)}{2^M} = \sum_{j=0}^{k} a_{B,j}\,(N{+}1)^j - \frac{\pi(2\mathcal{Q}_{\rm B}-1)}{2^M}\ , \tag{18}$$

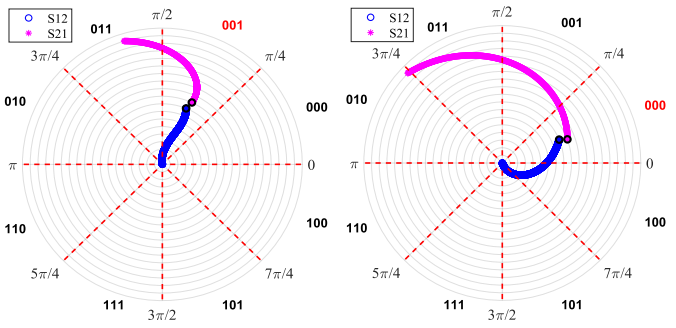
Subsequently, the data could be updated based on the obtained reconciliation shift $S_{\rm r} = S_{\rm A}$ or $S_{\rm r} = S_{\rm B}$, communicated publicly, as

$$\widehat{\Delta\phi}_{\mathrm{A},r} = \widehat{\Delta\phi}_{\mathrm{A},m} - S_{\rm r}\ ,\ \widehat{\Delta\phi}_{\mathrm{B},r} = \widehat{\Delta\phi}_{\mathrm{B},m} - S_{\rm r}\ . \tag{19}$$

Then, the last step of quantization should apply with equations (14) and (15) one more time to reach updated quantization intervals $\mathcal{Q}_{\mathrm{A},r}$ and $\mathcal{Q}_{\mathrm{B},r}$ after reconciliation. Finally, the keys at Alice and Bob result from using an M-bit Gray coding,

$$\mathbf{K}_{\rm A} = \mathrm{GC}\ (\widehat{\Delta\phi}_{\mathrm{A},r})\ ,\quad \mathbf{K}_{\rm B} = \mathrm{GC}\ (\widehat{\Delta\phi}_{\mathrm{B},r}). \tag{20}$$

As previously mentioned, within this PSKG procedure, continuity at the merging points demonstrates the requisite reciprocity necessary to ensure the generation of similar keys by both parties. This continuity is demonstrated effectively in Fig. 3 for measurements that do not require pre-processing, and in Fig. 5(d) and Fig. 5(h) for measurements that necessitate pre-processing. In Fig. 6, polar plots depict the reconciled versions of phase differences, accompanied by the allocated Gray codes for both examples shown in Fig. 5. In this representation, $N = 801$ rings, each, serve as frequency samples to illustrate phase differences at both Alice's and Bob's sides, respectively, and each sector corresponds to one quantization interval. The positions of the merging points, denoted by black circles,



(a) Example I (UCA) (b) Example II (ULA)

Fig. 6: Quantized and reconciled phase differences

indicate the generated keys at both ends. It is important to note that we have implemented this innovative non-coding approach solely for reconciliation as the first step. Simulation results confirm its feasibility and lower complexity compared to coding approaches. Nonetheless, further enhancements to the approach can be achieved by integrating Slepian-Wolf coding based on BCH, Turbo, or LDPC codes [30]. To mitigate the risk of information leakage during probing and reconciliation to potential eavesdroppers, it is imperative to conduct privacy amplification of synchronized keys using appropriate hash functions [31].

IV. Non-linear Quantization

In our comprehensive analysis of numerous measurements, it has been observed that the generated keys do not achieve a perfectly uniform distribution across all quantization intervals. This observation underscores an opportunity for refinement in the key generation process to enhance distribution uniformity. Therefore, we propose the adoption of a non-linear quantization scheme to address this limitation. Figure 7 illustrates the distribution resulting from a complete measurement round, encompassing 40 generated keys for our circular array setup. Initially, it is essential to analyze the resulting distribution of potential phase differences. To facilitate this analysis, let us consider two d-spaced antennas situated on the circular array at Alice's end. The maximum possible phase difference is determined by

$$\Delta\phi_{\max} = \frac{\omega_0}{c} d = \frac{2\pi f_0}{c} d = 2\pi \frac{d}{\lambda_0} , \tag{21}$$

where λ_0, f_0, c, and ω_0 represent the wavelength, central carrier frequency, speed of light, and corresponding angular frequency, respectively. In our case, we had $d = \lambda/2 = 6.841$ cm and $f_0 = 2.1925$ GHz. By defining ψ as an angle of the wave front direction from the connecting line between two consecutive antennas according to Fig. 8, the maximum phase difference can be expressed by

$$\Delta\phi_{\max} = \frac{\omega_0}{c} d \cos\psi . \tag{22}$$

The density function over the phase difference assuming a uniform distribution for ψ on the interval $[0, \pi]$, is given by

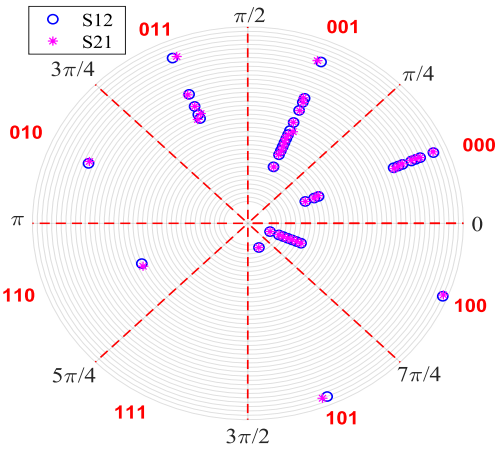


Fig. 7: Distribution of 40 generated keys from linear quantization in UCA

$$f_{\Delta\Phi}(\Delta\phi) = \frac{1}{\pi}\frac{c}{\omega_0 d}\frac{1}{|\sin\psi|} = \frac{1}{\pi}\frac{c}{\omega_0 d}\frac{1}{|\sin\cos^{-1}\left[\Delta\phi\frac{c}{\omega_0 d}\right]|}$$
$$= \frac{1}{\pi}\frac{c}{\omega_0 d}\frac{1}{\left|\sqrt{1-\left[\Delta\phi\frac{c}{\omega_0 d}\right]^2}\right|} . \tag{23}$$

Our proposed nonlinear quantization scheme is founded on the idea of utilizing the probability integral transform, as delineated by the following theorem. The corresponding block diagram is depicted in Fig. 9, as well.

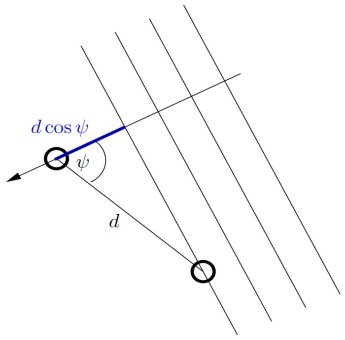


Fig. 8: Two consecutive antennas on the corresponding UCA in wave front

Theorem 1 (Probability integral transformation) [32]: Let X have a 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, $P(Y \leq y) = y$, $0 < y < 1$.

proof: See Appendix I.

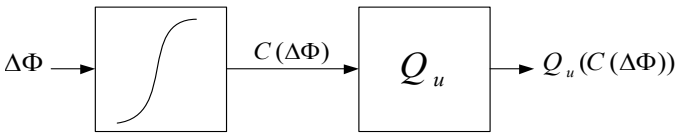
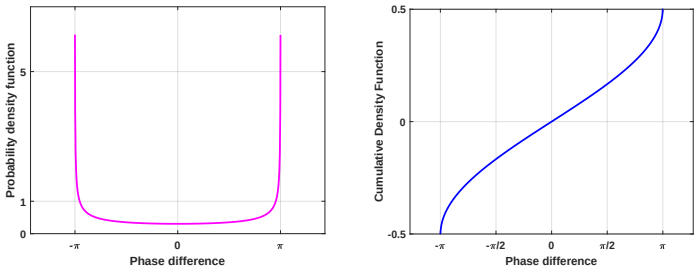


Fig. 9: Proposed non-linear quantization block diagram

Therefore, we employ the inverse CDF of phase differences as a non-linear compression function for the first block of the proposed diagram, which can be derived as follows:

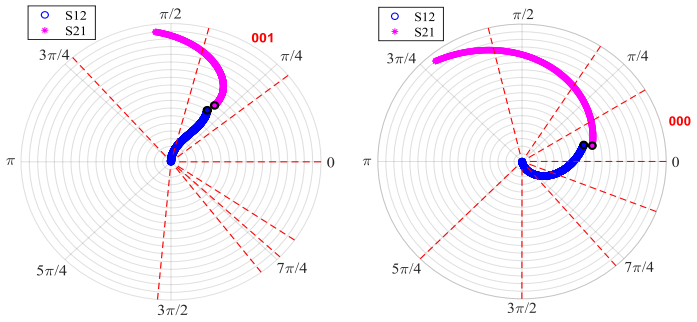
$$C(\Delta\phi) = F^{-1}_{\Delta\Phi}(\Delta\phi) = \frac{\omega_0 d}{c}\sin\left[\pi\Delta\phi\right] . \tag{24}$$



(a) PDF (b) CDF

Fig. 10: Ideal distributions of phase differences between two antennas

Figure 10 illustrates the corresponding CDF and probability density function (PDF) of the maximum possible phase differences. To implement the proposed non-linear quantization scheme, with a focus on minimizing complexity, a new methodology is introduced [4]. The suggested algorithm initially subdivides each quantization interval into multiple sub-intervals based on a predetermined number. Following this, the algorithm engages in an iterative process to define new boundaries and intervals. This iterative procedure aims to ensure that the allocation within each newly determined interval in the resulting histogram approximates the average value across all initial intervals. Let L represent the number of initial quantization intervals; then, the number of sub-intervals is chosen to be $L \cdot 2^n$, where n is an integer greater than or equal to 1. The algorithm terminates either at a predefined number of iterations or by achieving an acceptable threshold for the relative uniformity error. The corresponding non-linear quantization results for both examples of Fig. 6 are presented in Fig. 11. Additionally, Fig. 12 depicts the non-linearly quantized version of the generated keys, corresponding to Fig. 7. Comparing these figures clearly demonstrates how employing the proposed non-linear quantization scheme for just one iteration results in 40 generated keys, uniformly distributed across all unequal quantization intervals.



(a) Example I (UCA) (b) Example II (ULA)

Fig. 11: Non-linearly quantized phase differences

V. Error Probability Analysis

Consider $\widehat{\Delta\phi}_{\mathrm{A},m} \sim \mathcal{N}(\mu_A, \sigma_A^2)$ and $\widehat{\Delta\phi}_{\mathrm{B},m} \sim \mathcal{N}(\mu_B, \sigma_B^2)$ to be approximately two Gaussian random variables, obtained from equations (12) and (13), respectively, which represent the position of the rightmost point of S_{12} and the leftmost point of S_{21}, respectively. We intend to determine the error probability for each pair of keys which signifies the likelihood that $\widehat{\Delta\phi}_{\mathrm{A},m}$ and $\widehat{\Delta\phi}_{\mathrm{B},m}$ are quantized to different intervals. Considering a

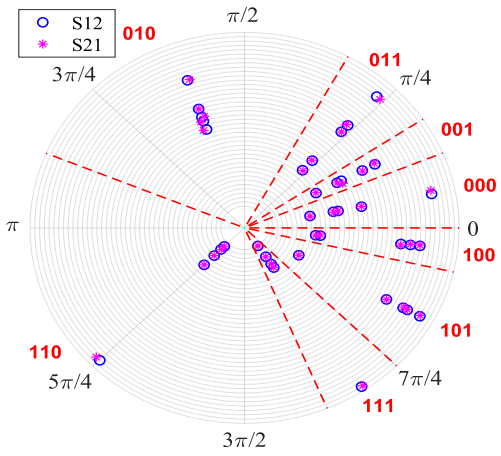


Fig. 12: Distribution of 40 generated keys from non-linear quantization in UCA

non-linear quantization scheme with N quantization levels, the width of the i-th quantization interval is $\widehat{\Delta\phi}_{\mathrm{B},m}$, where this interval is bounded by the two boundaries b_i and b_{i-1}, with i ranging from 1 to N. The probability that the random variable $\widehat{\Delta\phi}_{\mathrm{A},m}$ falls between two consecutive boundaries, b_i and b_{i-1}, can be obtained by

$$P\big(b_{i-1} \leq \widehat{\Delta\phi}_{\mathrm{A},m} \leq b_i\big) = \frac{1}{2}\Big[\mathrm{erf}\Big(\frac{b_i - \mu_A}{\sqrt{2}\sigma_A}\Big) - \mathrm{erf}\Big(\frac{b_{i-1} - \mu_A}{\sqrt{2}\sigma_A}\Big)\Big] . \quad (25)$$

According to equations (14) and (15), the implementation of a Gray-coding scheme results in the allocation of two M-tuple codeword vectors based on the detected quantization intervals for Alice and Bob. Consequently, when $\widehat{\Delta\phi}_{\mathrm{A},m}$ and $\widehat{\Delta\phi}_{\mathrm{B},m}$ fall into two different quantization intervals, it typically indicates a single-bit error between the corresponding keys, $\mathbf{K}_\mathrm{A}$ and $\mathbf{K}_\mathrm{B}$. Hence, the error probability is denoted by $P_{error} = P(\mathbf{K}_\mathrm{A} \neq \mathbf{K}_\mathrm{B})$, with the corresponding Bit Error Ratio (BER) given as P_{error}/M. Considering $\mathcal{K}$ as a set comprising all potential keywords, the error probability can be expressed as:

$$P_{error} = \sum_{\mathbf{K}_\mathrm{A} \in \{\mathcal{K}\}} P(\mathbf{K}_\mathrm{A}) \cdot P(error|\mathbf{K}_\mathrm{A}) = \sum_{\mathbf{K}_\mathrm{A} \in \{\mathcal{K}\}} P(\mathbf{K}_\mathrm{A}) \cdot (1 - P(\mathbf{K}_\mathrm{B} = \mathbf{K}_\mathrm{A})) . \quad (26)$$

Considering all corresponding non-linear quantization boundaries b_i for $i = 1, 2, ..., 2^M$, we have

$$P_{error} = \sum_{i=0}^{2^M} P\big(b_{i-1} \leq \widehat{\Delta\phi}_{\mathrm{A},m} \leq b_i\big) \cdot \Big(1 - P\big(b_{i-1} \leq \widehat{\Delta\phi}_{\mathrm{B},m} \leq b_i\big)\Big) . \quad (27)$$

Inserting Eq. (24) into Eq. (26), the final error probability relation can be expressed as

$$P_{error} = \sum_{i=0}^{2^M} \Big[\mathrm{erf}\Big(\frac{b_i - \mu_A}{\sqrt{2}\sigma_A}\Big) - \mathrm{erf}\Big(\frac{b_{i-1} - \mu_A}{\sqrt{2}\sigma_A}\Big)\Big] \cdot \Big[1 - \frac{1}{2}\Big[\mathrm{erf}\Big(\frac{b_i - \mu_B}{\sqrt{2}\sigma_B}\Big) - \mathrm{erf}\Big(\frac{b_{i-1} - \mu_B}{\sqrt{2}\sigma_B}\Big)\Big]\Big] . \quad (28)$$

To determine the error probability for each pair of generated keys between Alice and Bob, it is necessary to extract the mean and variance of both random variables (RVs) $\widehat{\Delta\phi}_{\mathrm{A},m}$ and $\widehat{\Delta\phi}_{\mathrm{B},m}$. This can be achieved by utilizing a multiple linear regression model [33] (see Appendix II).

VI. Numerical Results

In this section, we commence by introducing our testbed and proceed to perform numerical and statistical analyses based on real measurements to validate the proposed method. Subsequently, we delve into an exploration of key evaluation metrics pertinent to our proposed PSKG approach.

A. Testbed

In our experimental setup, we designed both a Uniform Circular Array (UCA) and a Uniform Linear Array (ULA) configuration at Alice's end. We examined a linear, time-invariant, frequency-selective wireless channel and conducted measurements of S_{12} and S_{21} using a standard VNA in a remotely controlled manner. The measurement process was repeated 10 times and the results were averaged to enhance measurement accuracy and minimize noise. The UCA design incorporates a rotatable disc housing 40 antenna positions, spaced approximately $\lambda/6$ apart, with an antenna array radius of 14.568 cm. Considering $\lambda/6$ as the minimum distance between antennas, it is indeed feasible to explore various distances, including $\lambda/2$, for simulation purposes. The corresponding ULA comprises 20 antenna positions with the same spacing, achieved through linear movement of the antenna plate along a straight path, remotely controlled. For measurement purposes, the active antenna element within Alice's array is connected to Port 1 of the VNA, while Port 2 is connected to Bob's antenna. To streamline the process and avoid the need to connect the VNA to each antenna individually at Alice's side, we conducted measurements in a remotely controlled fashion. This approach utilized a single active antenna that was repositioned to different array locations, thereby eliminating the necessity of switching connections among 20 antennas for the ULA and 40 antennas for the UCA. The measurements were automated using a MATLAB routine, sending SCPI commands to the VNA and interfaced with an Arduino board that controlled stepper motors for precise antenna positioning.

To establish a comprehensive dataset, we meticulously examined diverse indoor scenarios across 13 environments, encompassing offices, homes, labs, garages, basements, and corridors. Our investigations involved nearly 250 measuring scenarios for the UCA and 100 for the ULA, capturing a spectrum of outcomes ranging from minimal to pronounced effects, such as scenarios with blocked paths or obstructed line-of-sight. Additionally, we varied the vertical positioning of Alice and Bob, capturing measurements in scenarios with both zero and nonzero height differences.

B. Performance Metrics

In general, the effectiveness of the proposed PSKG is evaluated from four aspects: efficiency, KDR, key distribution uniformity, and randomness.

1) Efficiency: Efficiency is defined as the percentage of usable to the total number of measurements and our metric to detect usable measurements after pre-processing is the variance of each measurement. Hence, efficiency indicates the ratio of the number of measurements that can pass a selected variance threshold to the total number.

2) KDR: Bitwise KDR, equivalent to BER, is the ratio of deviating key bits between the Gray keys generated independently by Alice and Bob to the total number, which can be defined as

$$\mathrm{KDR} = \frac{1}{N_T}\sum_{N_T}\frac{1}{M}\sum_{i=1}^{M}\left|\mathbf{K}_A(i) - \mathbf{K}_B(i)\right| \ . \tag{29}$$

where M and N_T denote the number of Gray-code bit assignments and the total number of measurements, respectively.

3) Uniformity: The average relative uniformity error [4] can be used as a metric for measuring the deviation from the average value over L quantization intervals for the resulting histogram which can be obtained by

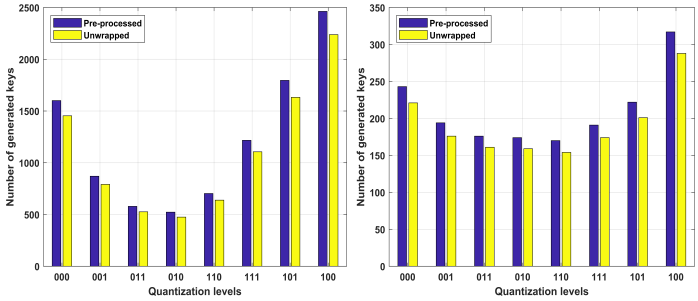
$$e_u = \frac{1}{L}\sum_{i=1}^{L}\frac{|n_i - n_{avg}|}{n_{avg}} \ . \tag{30}$$

where n_i and n_{avg} denote the related value in the i-th interval and the average value over all intervals, respectively.

4) Randomness: The randomness reveals the distribution of generated key streams. A statistical test set is widely used to verify the randomness of the generated keys which is provided by the National Institute of Standards and Technology (NIST) [34]. For each test in this set, test statistics are used to calculate a p-value that summarizes the strength of the evidence against the null hypothesis. A sequence is deemed random with 99% confidence if its corresponding p-value exceeds 0.01, and the larger the p-value, the better the randomness [35].

C. Results

1) Key Generation Distribution: Considering the entirety of measurements collected from the aforementioned diverse scenarios and adopting a $\frac{\lambda}{2}$ spacing between adjacent antennas, along a 3-bit linear quantization scheme, the respective distributions for key generation are compared in Fig. 14. Both unwrapped and pre-processed representations for each array individually are examined. A variance threshold of 1 radian was applied to identify and eliminate unusable measurements displaying higher variance. The figure clearly demonstrates the superior performance of the proposed pre-processing method over unwrapping in preparing measurements. This enhancement results in improved efficiency, whereby the pre-processing method enhances the efficiency to 97.52% compared to 88.61% associated with unwrapping, in the case of UCA. Similarly, this enhancement is observed in the case of ULA, where it improves to 99.36% for pre-processing compared to 90.23% for unwrapping. Moreover, it should be noted that both arrays, when employing the proposed pre-processing scheme, can achieve nearly perfect efficiency for SNR values greater than 12 dB.



(a) UCA (b) ULA

Fig. 13: Key generation distribution with linear quantization

2) Variance of the Measurements: The variance of measurements holds significant importance in determining the efficiency of the key generation method. To provide further clarification, Table II presents a comprehensive comparison of variances for both examples illustrated in Fig. 5, spanning all measurement types, including original, unwrapped, jump-removed, and outliers-corrected data. Pre-processing aims to minimize measurement variance, as highlighted earlier. The values in Table II substantiate the effectiveness of the proposed algorithm in achieving this goal. In contrast, in some instances, the unwrapping process not only fails to mitigate data variance but also exacerbates it, surpassing the predetermined threshold. For a clearer comparison, Fig. 14 compares the resulting variances for all measurement types associated with the 40 previously analyzed measurement sets shown in Fig. 7. This illustration unequivocally demonstrates that employing the unwrapping procedure dramatically increases variance within the sets $\{4, 7, 8, 9, 10, 11, 15, 16, 34, 35\}$ for S_{12} and $\{10, 11, 15, 16, 28, 34, 35\}$ for S_{21}, necessitating their exclusion. Consequently, utilizing this methodology would yield only 29 keys out of the 40 measurement sets. In contrast, the proposed approach effectively attenuates variance across all measurement sets, enabling the generation of all 40 keys.

TABLE II: Variance comparison

	Example 1		Example 2	
	$\mathbf{S_{12}}$	$\mathbf{S_{21}}$	$\mathbf{S_{12}}$	$\mathbf{S_{21}}$
Original	3.7684	1.6086	1.9064	6.5037
Unwrapped	0.2228	12.0211	36.6002	55.5936
Jump-removed	0.9887	0.8893	1.0201	1.9955
Outliers-corrected	0.2228	0.2721	0.5934	0.9614

3) Uniformity and Non-linear Quantization: As depicted in Fig. 13, the respective distributions of keys lack perfect uniformity, characterized by average relative uniformity errors of 0.656 and 0.934 for circular and linear arrays, respectively. Employing the recently proposed non-linear quantization scheme on the same measurements results in a significant reduction in the average relative uniformity error to 0.007 and 0.01 for circular and linear arrays, respectively. This reduction fulfills the condition of $e_u \leq 0.01$, thereby ensuring an almost uniform distribution across all possible keys. Corresponding results for both antenna arrays are presented in Fig. 15. In addition to non-linear quantizers, arithmetic coding [36] presents an alternative approach to achieving uniform distributions. Arithmetic coding is a lossless data compression technique that employs intervals within the [0,1] range of a

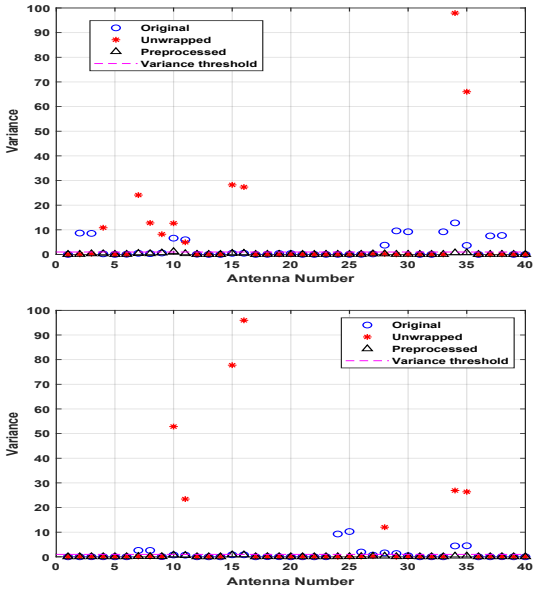
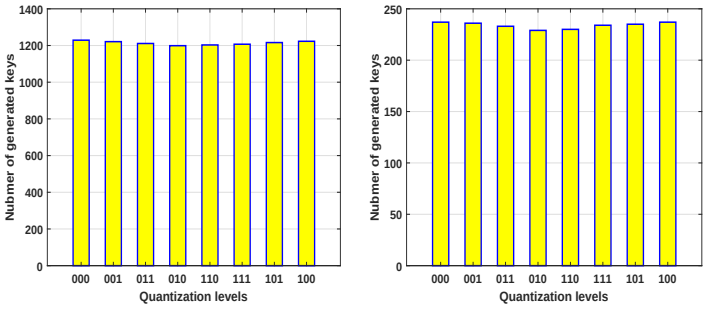


Fig. 14: Variance comparison; Top: S_{12}, Bottom: S_{21}

distribution function, representing probabilities of the original alphabet. As new components are introduced, these intervals are subdivided accordingly. The subdivision process results in stepwise intervals that progressively narrow down to a floating-point value in the limit. Concurrently, as intervals become increasingly smaller, they are encoded with a 0.5/0.5 interval split, representing the binary compressed sequence. As another alternative approach to achieving a uniform distribution of generated keys, the random permutation of antenna measurements [4], [28] serves to not only increase the quantity of generated key segments but also to enhance uniformity among potential key segment outcomes. Antenna permutations were employed to expand the pool of available datasets to $40!$ and $20!$ for the UCA and ULA, respectively. Especially, however, it strengthens protection against eavesdropping and, akin to other randomization techniques involving reconfigurable antennas or surfaces, provides resilience against active Man-in-the-Middle attacks [37].



(a) UCA (b) ULA

Fig. 15: Key generation distribution with non-linear quantization

4) Key Disagreement Ratio: The key disagreement ratio serves as a common metric for evaluating key generation performance. Figure 16 offers a comparison of the KDR against SNR for both ULA and UCA, alongside other methods in [3], [10], [14] and [16]. It is notable that the proposed

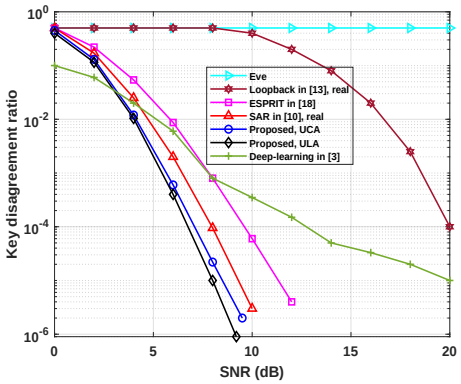


Fig. 16: KDR comparison against SNR

algorithm demonstrates superior performance compared to the other approaches. Furthermore, ULA exhibits marginally better performance than UCA in this regard. To assess the KDR in worst-case scenarios, deliberate obstructions such as steel doors were used along the LoS trajectory connecting the transmit and receive antennas. This intervention led to a deterioration of the KDR to the 10^{-3} range. Furthermore, an average bit-wise KDR of 0.4512 was observed between the generated keys at Alice (or Bob) and the estimated keys at Eve. This value is close to the theoretical ideal value of 0.5, which is equivalent to Eve randomly guessing, akin to flipping a coin for each bit.

5) Randomness: The randomness of the generated final key sequence is subjected to assessment through the NIST statistical test suite [34]. This evaluation is conducted with the method executed at an average SNR of 10 dB for both UCA and ULA. Subsequently, all generated keys are collected, sets of 128-bit keys are extracted, and their corresponding p-values are computed. Due to constraints on bit length, nine out of the sixteen typical tests are executed. Table III compares the corresponding pass rates for both arrays. The data presented in this table unequivocally indicate that the generated key bit sequences successfully pass the NIST test suite, thereby affirming their randomness with 99% confidence.

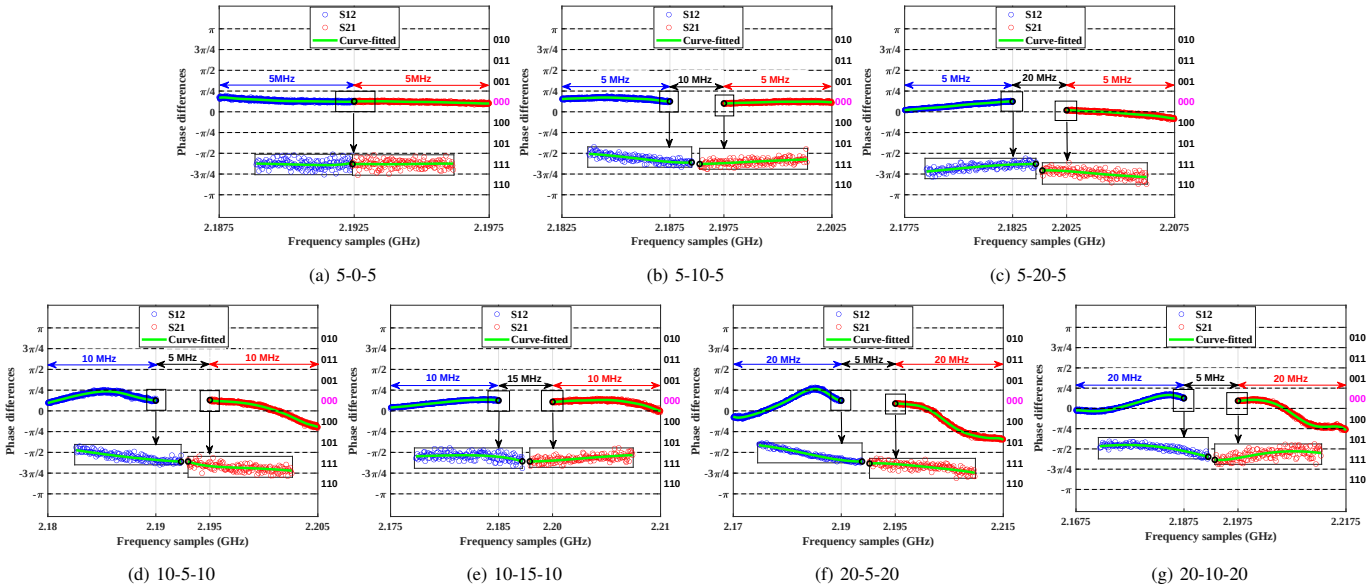
TABLE III: NIST statistical test results

Test	ULA	UCA
Approximate Entropy	0.9129	0.9412
Frequency (Monobit)	0.6491	0.7342
Frequency (within a block)	0.7084	0.7519
Cumulative sums (forward)	0.5413	0.6146
Cumulative sums (reverse)	0.4211	0.4753
Discrete Fourier Transform	0.9102	0.8816
Longest Run	0.1043	0.1257
Run	0.8248	0.8394
Serial	0.69201	0.6501

6) Band Separation: As previously explained, the foundation of our proposed FDD-based SKG approach rests upon the close proximity of the corresponding narrowband FDDs. This reliance is predicated on the utilization of reciprocity within the same frequency range to generate similar keys. Typically, band separation is necessary to prevent interference between uplink and downlink signals. To address this concern, we conducted simulations encompassing various frequency gaps between two active FDD bands to investigate the consistency of the generated keys between Alice and Bob. Furthermore, we aimed to affirm this consistency by conducting simulations that encompassed wider FDD bands. The simulation outcomes, encompassing various scenarios for band separation and employing wider FDD bands are illustrated in Fig. 18. A variance threshold of 1 radian was established, and a second-order polynomial curve fitting was implemented. We employed a linear quantization scheme and refrained from employing any coding scheme. Instead, we exclusively utilized the proposed one-sided centering approach for reconciliation.

Let us consider Fig. 17(a) as the reference for the generated key between Alice and Bob, assuming a 5 MHz bandwidth for each FDD band without any band separation. Figures 17(b) and 17(c) provide robust confirmation that as the separation band increases up to 20 MHz, while maintaining a 5 MHz bandwidth, although there is a slight mismatch in the continuity of the merging points, falling into the same quantization interval still ensures the consistent generation of identical keys from both ends. A similar conclusion can be drawn for the scenario with a 10 MHz bandwidth, as demonstrated in figures 17(d) and 17(e). Furthermore, the presence of symmetry between S_{12} and S_{21}, resulting in the generation of similar keys, is clearly evident in figures 17(d) and 17(f) when the separation between FDD bands widens up to 20 MHz. Figures 17(b) and 17(g) also illustrate this symmetry for a 10 MHz separation. Analysis of the results across the same datasets reveals that enlarging the frequency gap between two operational FDD bands leads to a slightly affected continuity at merging points from left and right. This can potentially impact the efficiency of the proposed SKG method, particularly in low SNR regimes. Specifically, averaging over all measurements for 10 and 20 MHz band separations, the efficiency reached 94.2% and 89.35% respectively for the UCA, compared to 97.52% in the absence of any band separation. Furthermore, employing higher-order polynomial curve fitting offers improved performance by enabling more precise tracking of changes within complex curves across frequency bands. This facilitates the maintenance of continuity at merging points, particularly in scenarios with wider FDD bands.

7) Computational Complexity: Both the jump and outlier detection phases utilize comparison mechanisms for data points, where comparing two numerical values consistently exhibits a time complexity of constant order, typically denoted as $\mathcal{O}(1)$. In the correction phase, it is widely acknowledged that the computational complexity of adding two n-digit numbers is expressed as linear time complexity, denoted as $\mathcal{O}(n)$, where n represents the number of digits in the larger of the two numbers being added. The computational complexity of the Least-Squares method for second-order curve fitting is approximately $\mathcal{O}(N)$, encompassing various stages such as equation setup, matrix formation, and solving linear equations to deduce coefficients, where N represents the number of data points. When considering higher orders, the overall computational complexity is contingent upon both the polynomial degree (n) and the data point count (N). For n-th order polynomial curve fitting via the Least-Squares method, the complexity can vary from $\mathcal{O}(n * N)$ to $\mathcal{O}(n^2 * N)$. The computational complexity of linear quantization depends on its implementation and the data size. Generally, linear quantization is characterized



(a) 5-0-5 (b) 5-10-5 (c) 5-20-5

(d) 10-5-10 (e) 10-15-10 (f) 20-5-20 (g) 20-10-20

Fig. 17: Positions of merging points considering band separation and wider FDD bands in UCA

by constant time complexity $\mathcal{O}(1)$, indicating that the time required to quantize an individual value at merging points remains consistent regardless of its magnitude or other inputs. Our proposed one-sided centering approach for the initial reconciliation stage entails a single subtraction operation to determine the required shift and two addition operations to implement the calculated shift to both merging points. This approach offers significantly lower computational cost compared to conventional coding approaches. Therefore, the proposed algorithm provides competitive linear complexity compared to quadratic or cubic complexity for methods that use the channel covariance matrix [12] and Eigenvalue Decomposition (EVD) [14], [15]. Furthermore, our proposed method eliminates the need for separating channel paths [10], utilizing an additional reverse channel training phase [16]–[18], or training models for individual communication environments [3], [21]–[24], all of which would impose significant complexity on the system.

8) Eavesdropping: In our analysis, we exclusively considered passive eavesdropping scenarios. However, according to existing literature [38] and [39], Eve should ideally be positioned 6λ away from both, Alice and Bob, to ensure the absence of correlation between the legitimate and wiretap channels. In our case, a separation of $\lambda/2$ already resulted in the generation of uncorrelated keys at Eve's side. The required shift of the quantization grid for key reconciliation is communicated publicly. Hence, Eve can apply the same grid shift, but it does not assist her. She will measure a different phase difference. The resulting keys generated by Alice, Bob, and Eve from a complete dataset of the corresponding UCA, comprising 40 measurement sets utilizing a linear quantization scheme, are illustrated in Fig. 18. The comparison between the generated keys emphasizes the robust security of the keys exchanged between Alice and Bob. Furthermore, we examined the distribution of the detected keys from Eve's perspective, derived from the identical key shared between Alice and Bob. The outcomes, as depicted in Fig. 19, demonstrate that the 200

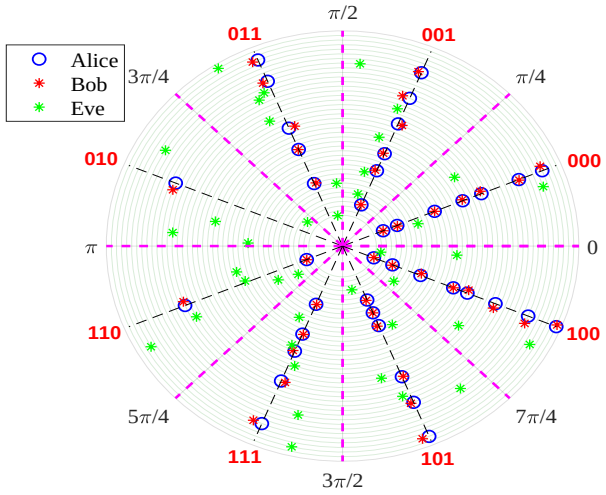


Fig. 18: Generated keys for Alice, Bob, and Eve in UCA

identical keys exchanged between Alice and Bob, exhibit a nearly uniform distribution across all potential keys at Eve's side. Such uniform distribution is required for cryptographic applications.

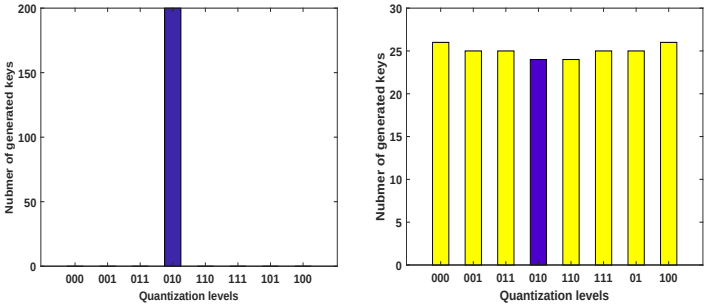


Fig. 19: 200 generated keys in UCA; Left: at Alice's and Bob's side, Right: detected at Eve's side

VII. Discussions

In this study, we examined a key generation strategy designed for FDD systems, evaluating both ULAs and UCAs. We aimed

to demonstrate the feasibility and comparable performance of these configurations, noting that the choice should be based on specific system needs. Both array types utilize channel characteristics to generate the randomness required for key generation, with the main difference being the spatial deployment of circular versus linear arrays.

We demonstrated that the proposed method ensures reciprocity for consistent key generation more efficiently and with less complexity than alternative approaches. It effectively maintains reciprocity across band separation and wider FDD bands, demonstrating its robustness. The use of phase differences enhances this robustness by minimizing noise and systematic errors, and simplifies measurements by focusing on relative phases, thus eliminating the need for normalization and calibration. The method's scalability to FDD multi-user scenarios for shared secret key generation is promising, though exploring this extension is beyond the scope of this paper and represents a potential area for future research. Additionally, we introduced transfer functions as a practical alternative to S-parameters to better suit IoT networks.

While we used a VNA in our laboratory setup for precise S-parameter measurements, this was primarily for controlled experiments to demonstrate that the introduced reciprocity could enable key generation for FDD systems. In real-world deployments, where Alice and Bob are not equipped with a VNA, the transfer function can be obtained using well-established pilot-based channel estimation techniques. These techniques typically involve pilots transmitted according to a specific time-frequency pattern. In our approach, which relies on phase differences, assuming Alice has an antenna array and Bob has a single dipole, the phase differences are measured as follows: from Bob to Alice, phase differences are detected at pilot locations between Alice's two consecutive antennas. For measurements from Alice to Bob, the links are measured sequentially—first from Alice's antenna i to Bob, and then from antenna $i+1$ to Bob. A pilot from one antenna serves as the phase reference for the other, allowing the desired phase difference to be determined.

Any potential impedance mismatch would lead to a non-zero S_{11}, and as shown in Eq. (4), result in changes to the transfer function. However, since the same measurement setup is used for all antennas and the environment remains constant, any mismatches introduced by the setup are insignificant. Additionally, conducting measurements within the same frequency range for consecutive antennas ensures that frequency-dependent mismatches will affect both antennas similarly, making any phase shifts from impedance mismatches negligible for both S_{12} and S_{21} measurements. Therefore, the impact of a non-zero S_{11} on the transfer function is negligible, as it affects both antenna transfer functions equally, and the analysis focuses on phase differences rather than absolute phase values.

VIII. Conclusion

In this paper, we propose a novel approach for physical layer secret key generation in FDD systems. This method leverages the inherent reciprocity between forward and reverse transmission factors of the wireless channel between two legitimate partners. We utilize phase differences between neighboring antennas, derived from corresponding S_{12} and S_{21} parameters, as a reciprocal channel parameter to ensure the required reciprocity for the generating similar keys from both sides. Two antenna arrays, UCA and ULA, are specifically designed to gather actual measurements from diverse scenarios for the proposed PSKG approach. We evaluate the reliability and security of the proposed method using metrics such as efficiency, KDR, uniformity, and randomness. Numerical results, considering various scenarios, validate that the proposed method is simple yet highly effective, capable of generating random key pairs with nearly perfect efficiency and a highly competitive KDR. The feasibility of both antenna arrays is demonstrated through numerical analysis.

Acknowledgments

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

Appendix I: [Proof of Theorem 1]

For $Y = F_X(x)$ and $0 < y < 1$, we have

$$P(Y \leq y) = P(F_X(x) \leq y) = P(F_X^{-1}[F_X(x)] \leq F_X^{-1}(y)) = P(X \leq F_X^{-1}(y)) = F_X(F_X^{-1}(y)) = y\,.$$

Appendix II: [Parameter Estimation]

In order to extract the mean and variance of RVs $\widehat{\Delta\phi}_{\mathrm{A},m}$ and $\widehat{\Delta\phi}_{\mathrm{B},m}$ to determine the error probability, consider the multiple linear regression model in the most general case for our data as follows:

$$\mathbf{H}_{\mathrm{A}} = \mathbf{X}\boldsymbol{\beta} + \boldsymbol{\epsilon}\,. \tag{31}$$

$\mathbf{H}_{\mathrm{A}}$ and $\mathbf{X}$ are a $N \times 1$ vector of N observations of the study variable and a $N \times (k+1)$ matrix of N observations on each of the $k+1$ explanatory variables, which is often referred to as the design matrix, respectively. Moreover, $\beta_i = a_{A,i}$ and $\boldsymbol{\beta}$ is a $(k+1) \times 1$ vector including fixed but unknown model parameters representing regression coefficients and the $N \times 1$ vector $\boldsymbol{\epsilon}$ is related to random error components which can be assumed $\boldsymbol{\epsilon} \sim \mathcal{N}(\mathbf{0}, \sigma^2\mathbf{I}_N)$. Moreover, $\mathbf{X}$ is assumed as a non-stochastic matrix such that $\mathrm{rank}(\mathbf{X}) = k$. Spelling out the components of Eq. (31), this reads

$$\begin{bmatrix} \Delta\phi_1 \\ \Delta\phi_2 \\ \vdots \\ \Delta\phi_N \end{bmatrix} = \begin{bmatrix} 1 & x_1 & \cdots & x_1^k \\ 1 & x_2 & \cdots & x_2^k \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_N & \cdots & x_N^k \end{bmatrix} \begin{bmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \beta_k \end{bmatrix} + \begin{bmatrix} \varepsilon_1 \\ \varepsilon_2 \\ \vdots \\ \varepsilon_N \end{bmatrix}\,. \tag{32}$$

The general procedure for estimating the regression coefficient vector for $k = 2$ results from minimization of a metric M

$$\sum_{i=1}^{N} \mathrm{M}(\varepsilon_i) = \sum_{i=1}^{N} \mathrm{M}(\Delta\phi_i - \beta_0 - x_i\beta_1 - x_i^2\beta_2)\,. \tag{33}$$

Choosing $\mathrm{M}(x) = x^2$ for the above metric leads to the ordinary least-squares method. Let us consider $\mathcal{B}$ as the $(k+1)-$dimensional real Euclidean space consisting of the set of all possible vectors of $\boldsymbol{\beta}$. The objective is to find a $(k+1)$-tuple $\hat{\boldsymbol{\beta}} = (\hat{\beta}_0, \hat{\beta}_1, ..., \hat{\beta}_k)$ from $\mathcal{B}$ that minimizes the sum of squared deviations of $\boldsymbol{\epsilon}$ for given $\mathbf{H}_{\mathrm{A}}$ and $\mathbf{X}$ as

$$\mathrm{S}(\mathbf{b}) = \sum_{i=1}^{N} \varepsilon_i^2 = (\mathbf{H}_\mathrm{A} - \mathbf{X}\mathbf{b})^\mathrm{T}(\mathbf{H}_\mathrm{A} - \mathbf{X}\mathbf{b}) = \mathbf{H}_\mathrm{A}^\mathrm{T}\mathbf{H}_\mathrm{A} + \mathbf{b}^\mathrm{T}\mathbf{X}^\mathrm{T}\mathbf{X}\mathbf{b} - 2\mathbf{b}^\mathrm{T}\mathbf{X}^\mathrm{T}\mathbf{H}_\mathrm{A}. \quad (34)$$

To find the desired vector, we should have $\frac{\partial\ \mathrm{S}(\mathbf{b})}{\partial \mathbf{b}} = 2\mathbf{X}^\mathrm{T}\mathbf{X}\mathbf{b} - 2\mathbf{X}^\mathrm{T}\mathbf{H}_\mathrm{A} = 0$ which implies that $\mathbf{X}^\mathrm{T}\mathbf{X}\mathbf{b} = \mathbf{X}^\mathrm{T}\mathbf{H}_\mathrm{A}$. If $\mathbf{X}$ is full rank, we have $\mathrm{rank}(\mathbf{X}) = k+1$, then $\mathbf{X}^\mathrm{T}\mathbf{X}$ is positive definite and consequently, the unique solution of (33) is given by the pseudo inverse

$$\hat{\boldsymbol{\beta}} = (\hat{\beta}_0, \hat{\beta}_1, ..., \hat{\beta}_k) = (\mathbf{X}^\mathrm{T}\mathbf{X})^{-1}\mathbf{X}^\mathrm{T}\mathbf{H}_\mathrm{A} = \mathbf{b}\ . \quad (35)$$

since $\partial^2\ \mathrm{S}(\mathbf{b})/\partial\mathbf{b}^2 = 2\mathbf{X}^\mathrm{T}\mathbf{X}$, at least, is non-negative definite, the aforementioned obtained $\hat{\boldsymbol{\beta}}$ minimizes $\mathrm{S}(\mathbf{b})$. In case $\mathbf{X}$ is not full rank, the solution of Eq. (33) is as follows:

$$\mathbf{b} = (\mathbf{X}^\mathrm{T}\mathbf{X})^\mathrm{g}\ \mathbf{X}^\mathrm{T}\mathbf{H}_\mathrm{A} + [\ \mathbf{I} - (\mathbf{X}^\mathrm{T}\mathbf{X})^\mathrm{g}\ \mathbf{X}^\mathrm{T}\mathbf{X}\ ]\ \mathbf{w}\ , \quad (36)$$

where $(\mathbf{X}^\mathrm{T}\mathbf{X})^\mathrm{g}$ represents the generalized inverse of $\mathbf{X}^\mathrm{T}\mathbf{X}$ and $\mathbf{w}$ can be considered as an arbitrary vector. If we consider $\mathbf{b}$ as the estimate of $\boldsymbol{\beta}$, then clearly the fitted values are

$$\hat{\mathbf{H}}_\mathrm{A} = \mathbf{X}\mathbf{b}\ , \quad (37)$$

and in the case of $\mathbf{b} = \hat{\boldsymbol{\beta}}$, for the fitted values, we have $\hat{\mathbf{H}}_\mathrm{A} = \mathbf{X}\hat{\boldsymbol{\beta}} = \mathbf{X}(\mathbf{X}^\mathrm{T}\mathbf{X})^{-1}\mathbf{X}^\mathrm{T}\mathbf{H}_\mathrm{A}$. By defining $\mathbf{X}(\mathbf{X}^\mathrm{T}\mathbf{X})^{-1}\mathbf{X}^\mathrm{T}$ as a matrix $\mathbf{H}$, we obtain $\hat{\mathbf{H}}_\mathrm{A} = \mathbf{H}\mathbf{H}_\mathrm{A}$. The $\mathbf{H}$ matrix maps the vector of observed values (dependent variable values) to the vector of fitted values, and its diagonal elements are defined as the leverages, which describe the influence each response value has on the fitted value for that same observation. This matrix is symmetric, idempotent, and

$$\mathrm{trace}(\mathbf{H}) = \mathrm{trace}(\mathbf{X}(\mathbf{X}^\mathrm{T}\mathbf{X})^{-1}\mathbf{X}^\mathrm{T}) = \mathrm{trace}(\mathbf{X}^\mathrm{T}\mathbf{X}(\mathbf{X}^\mathrm{T}\mathbf{X})^{-1}) = \mathrm{trace}(\mathbf{I}_{k+1}) = k+1\ . \quad (38)$$

Moreover, we can define the residuals as difference between the observed and fitted values of the study variable as

$$\mathbf{e} = \mathbf{H}_\mathrm{A} - \hat{\mathbf{H}}_\mathrm{A} = \mathbf{H}_\mathrm{A} - \mathbf{H}\mathbf{H}_\mathrm{A} = (\mathbf{I} - \mathbf{H})\mathbf{H}_\mathrm{A} = \bar{\mathbf{H}}\mathbf{H}_\mathrm{A}\ . \quad (39)$$

The matrix $\bar{\mathbf{H}}$ is symmetric and idempotent, and we have

$$\mathrm{trace}(\bar{\mathbf{H}}) = \mathrm{trace}(\mathbf{I}_N) - \mathrm{trace}(\mathbf{H}) = N - (k+1)\ . \quad (40)$$

Theorem 2: If $\mathbf{X}$ is full rank, then $\mathrm{E}\{\hat{\boldsymbol{\beta}}\} = \boldsymbol{\beta}$ and $Cov(\hat{\boldsymbol{\beta}}) = \sigma^2(\mathbf{X}^\mathrm{T}\mathbf{X})^{-1}$.

proof:

$$\mathrm{E}\{\hat{\boldsymbol{\beta}}\} = \mathrm{E}\{(\mathbf{X}^\mathrm{T}\mathbf{X})^{-1}\mathbf{X}^\mathrm{T}\mathbf{H}_\mathrm{A}\} = (\mathbf{X}^\mathrm{T}\mathbf{X})^{-1}\mathbf{X}^\mathrm{T}E\{\mathbf{H}_\mathrm{A}\} = (\mathbf{X}^\mathrm{T}\mathbf{X})^{-1}\mathbf{X}^\mathrm{T}\mathbf{X}\boldsymbol{\beta} = \boldsymbol{\beta}\ .$$

and

$$\begin{aligned} Cov(\hat{\boldsymbol{\beta}}) &= Cov\big((\mathbf{X}^\mathrm{T}\mathbf{X})^{-1}\mathbf{X}^\mathrm{T}\ \mathbf{H}_\mathrm{A}\big) \\ &= (\mathbf{X}^\mathrm{T}\mathbf{X})^{-1}\mathbf{X}^\mathrm{T}Cov(\mathbf{H}_\mathrm{A})\big((\mathbf{X}^\mathrm{T}\mathbf{X})^{-1}\mathbf{X}^\mathrm{T}\big)^\mathrm{T} \\ &= (\mathbf{X}^\mathrm{T}\mathbf{X})^{-1}\mathbf{X}^\mathrm{T}Cov(\mathbf{H}_\mathrm{A})\mathbf{X}(\mathbf{X}^\mathrm{T}\mathbf{X})^{-1} \\ &= (\mathbf{X}^\mathrm{T}\mathbf{X})^{-1}\mathbf{X}^\mathrm{T}(\sigma^2\mathbf{I})\mathbf{X}(\mathbf{X}^\mathrm{T}\mathbf{X})^{-1} \\ &= \sigma^2(\mathbf{X}^\mathrm{T}\mathbf{X})^{-1}\mathbf{X}^\mathrm{T}\mathbf{X}(\mathbf{X}^\mathrm{T}\mathbf{X})^{-1} = \sigma^2(\mathbf{X}^\mathrm{T}\mathbf{X})^{-1}. \end{aligned}$$

Theorem 3: If $\mathbf{A}$ is an $N \times N$ matrix of constants and $\mathbf{H}_\mathrm{A}$ is an N-dimensional random vector such that $\mathrm{E}\{\mathbf{H}_\mathrm{A}\} = \boldsymbol{\mu}$ and $Cov(\mathbf{H}_\mathrm{A}) = \boldsymbol{\Sigma}$, then $E\{\mathbf{H}_\mathrm{A}^\mathrm{T}\mathbf{A}\mathbf{H}_\mathrm{A}\} = \mathrm{trace}(\mathbf{A}\boldsymbol{\Sigma}) + \boldsymbol{\mu}^\mathrm{T}\mathbf{A}\boldsymbol{\mu}$.

proof: See [40].

Theorem 4: If X is full rank, then $\mathrm{E}\{\mathrm{S}(\hat{\boldsymbol{\beta}})\} = \sigma^2\big(N - (k+1)\big)$.

proof:

$$\begin{aligned} \mathrm{S}(\hat{\boldsymbol{\beta}}) &= (\mathbf{H}_\mathrm{A} - \mathbf{X}\hat{\boldsymbol{\beta}})^\mathrm{T}(\mathbf{H}_\mathrm{A} - \mathbf{X}\hat{\boldsymbol{\beta}}) \\ &= \mathbf{H}_\mathrm{A}^\mathrm{T}\mathbf{H}_\mathrm{A} - 2\hat{\boldsymbol{\beta}}^\mathrm{T}\mathbf{X}^\mathrm{T}\mathbf{H}_\mathrm{A} + \hat{\boldsymbol{\beta}}^\mathrm{T}\mathbf{X}^\mathrm{T}\mathbf{X}\hat{\boldsymbol{\beta}} \\ &= \mathbf{H}_\mathrm{A}^\mathrm{T}\mathbf{H}_\mathrm{A} - 2\hat{\boldsymbol{\beta}}^\mathrm{T}\mathbf{X}^\mathrm{T}\mathbf{H}_\mathrm{A} + \hat{\boldsymbol{\beta}}^\mathrm{T}\mathbf{X}^\mathrm{T}\mathbf{H}_\mathrm{A} \\ &= \mathbf{H}_\mathrm{A}^\mathrm{T}\mathbf{H}_\mathrm{A} - \hat{\boldsymbol{\beta}}^\mathrm{T}\mathbf{X}^\mathrm{T}\mathbf{H}_\mathrm{A} \\ &= \mathbf{H}_\mathrm{A}^\mathrm{T}\mathbf{H}_\mathrm{A} - \mathbf{H}_\mathrm{A}^\mathrm{T}\mathbf{X}(\mathbf{X}^\mathrm{T}\mathbf{X})^{-1}\mathbf{X}^\mathrm{T}\mathbf{H}_\mathrm{A} \\ &= \mathbf{H}_\mathrm{A}^\mathrm{T}\mathbf{H}_\mathrm{A} - \mathbf{H}_\mathrm{A}^\mathrm{T}\mathbf{H}\mathbf{H}_\mathrm{A} = \mathbf{H}_\mathrm{A}^\mathrm{T}\bar{\mathbf{H}}\mathbf{H}_\mathrm{A}. \end{aligned}$$

Using Theorem 2 implies that

$$\begin{aligned} \mathrm{E}\{\mathrm{S}(\hat{\boldsymbol{\beta}})\} &= \mathrm{trace}\big((\mathbf{I}_N - \mathbf{H})\sigma^2\mathbf{I}\big) + (\mathbf{X}\boldsymbol{\beta})^\mathrm{T}(\mathbf{I} - \mathbf{H})\mathbf{X}\boldsymbol{\beta} \\ &= \sigma^2\mathrm{trace}(\mathbf{I}_N - \mathbf{H}) + \boldsymbol{\beta}^\mathrm{T}\mathbf{X}^\mathrm{T}(\mathbf{I} - \mathbf{H})(\mathbf{X}\boldsymbol{\beta}) \\ &= \sigma^2\mathrm{trace}(\mathbf{I}_N - \mathbf{H}) + \boldsymbol{\beta}^\mathrm{T}\big(\mathbf{X}^\mathrm{T}\mathbf{X} - \mathbf{X}^\mathrm{T}\mathbf{X}\big)\boldsymbol{\beta} \\ &= \sigma^2\mathrm{trace}(\mathbf{I}_N - \mathbf{H}) = \sigma^2\big(N - (k+1)\big)\ . \end{aligned}$$

Finally, σ^2 can be estimated employing $\mathrm{E}\{\mathrm{S}(\hat{\boldsymbol{\beta}})\} = \sigma^2\big(N - (k+1)\big)$ as sum of squares of the residuals as follows:

$$\hat{\sigma}^2 = \frac{1}{N - (k+1)}\ \sum_{i=1}^{k} (\Delta\phi_i - \widehat{\Delta\phi}_i)^2\ . \quad (41)$$

In our case, employing second-order polynomial curve fitting at Alice's side, we have $\Delta\phi_i = \beta_0 + \beta_1 x_i + \beta_2 x_i^2$ for $i = 1, 2, ..., N$. Employing Theorem 2, linear regression coefficients would be normal as $\hat{\boldsymbol{\beta}} \sim \mathcal{N}(\boldsymbol{\beta}, \sigma^2(\mathbf{X}^\mathrm{T}\mathbf{X})^{-1})$. Hence, one can determine the required mean and variance of the resulting Gaussian distribution at the merging point for random variable $\widehat{\Delta\phi}_{\mathrm{A},m} \sim \mathcal{N}(\beta_0 + \beta_1 x + \beta_2 x^2\ ,\ \sigma_{\beta_0}^2 + x^2\sigma_{\beta_1}^2 + x^4\sigma_{\beta_2}^2)$ in which $\sigma_{\beta_0}^2$, $\sigma_{\beta_1}^2$, and $\sigma_{\beta_2}^2$ are the first, second, and the third entries on the main diagonal of the covariance matrix of $\hat{\boldsymbol{\beta}}$, respectively. The procedure at Bob's side for random variable $\widehat{\Delta\phi}_{\mathrm{B},m}$ is the same.

REFERENCES

[1] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.

[2] Z. Ji, Y. Zhang, Z. He, P. L. Yeoh, B. Li, H. Yin, Y. Li, and B. Vucetic, "Wireless secret key generation for distributed antenna systems: A joint space-time-frequency perspective," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 633–647, 2021.

[3] 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.

[4] E. O. Torshizi and W. Henkel, "Reciprocity and secret key generation for FDD systems using non-linear quantization," in *2022 IEEE Globecom Workshops (GC Wkshps)*. IEEE, 2022, pp. 927–932.

[5] 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.

[6] 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, 2016.

[7] 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.

[8] 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.

[9] N. Aldaghri and H. Mahdavifar, "Physical layer secret key generation in static environments," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2692–2705, 2020.

[10] 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.

[11] 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, pp. 1605–1616, 2012.

[12] 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.

[13] H. Taha and E. Alsusa, "Secret key exchange using private random precoding in MIMO FDD and TDD systems," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 6, pp. 4823–4833, 2016.

[14] E. O. Torshizi, U. Uprety, and W. Henkel, "Highly efficient FDD secret key generation using ESPRIT and jump removal on phase differences," in *2022 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2022, pp. 1–6.

[15] E. O. Torshizi and W. Henkel, "Exploiting FDD channel reciprocity for physical layer secret key generation in IoT networks," *IEEE Communications Letters, DOI: 10.1109/LCOMM.2024.3388160.*, 2024.

[16] 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.

[17] 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)*. IEEE, 2013, pp. 1297–1302.

[18] 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.

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

[20] 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.

[21] M. Alrabeiah and A. Alkhateeb, "Deep learning for TDD and FDD massive MIMO: Mapping channels in space and frequency," in *2019 53rd asilomar conference on signals, systems, and computers*. IEEE, 2019, pp. 1465–1470.

[22] Z. Wan, K. Huang, and L. Chen, "Secret key generation scheme based on deep learning in FDD MIMO systems," *IEICE TRANSACTIONS on Information and Systems*, vol. 104, no. 7, pp. 1058–1062, 2021.

[23] X. Zhang, G. Li, Z. Hou, and A. Hu, "Secret key generation for FDD systems based on complex-valued neural network," in *2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall)*. IEEE, 2021, pp. 1–6.

[24] Z. Hou and X. Zhang, "Secret key generation scheme based on generative adversarial networks in FDD systems," in *IEEE INFOCOM 2021-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2021, pp. 1–6.

[25] X. Zhang, G. Li, J. Zhang, L. Peng, A. Hu, and X. Wang, "Enabling deep learning-based physical-layer secret key generation for FDD-OFDM systems in multi-environments," *IEEE Transactions on Vehicular Technology*, 2024.

[26] W. Henkel, "Method for physical key generation in frequency division duplexing (FDD)," Aug. 18 2016, DE patent, 102015113730A1.

[27] 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)*. IEEE, 2018, pp. 1–6.

[28] 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)*. IEEE, 2021, pp. 1–6.

[29] D. M. Pozar, *Microwave engineering: theory and techniques*. John wiley & sons, 2021.

[30] 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)*. IEEE, 2015, pp. 1–7.

[31] M. Bloch and J. Barros, *Physical-layer security: from information theory to security engineering*. Cambridge University Press, 2011.

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

[33] E. O. Torshizi and W. Henkel, "Error probability of FDD-based secret key generation using multiple linear regression," in *2023 31st European Signal Processing Conference (EUSIPCO)*. IEEE, 2023, pp. 630–634.

[34] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Booz-allen and hamilton inc mclean va, Tech. Rep., 2001.

[35] K. Lin, Z. Ji, Y. Zhang, G. Chen, P. L. Yeoh, and Z. He, "Secret key generation based on 3d spatial angles for UAV communications," in *2021 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2021, pp. 1–6.

[36] A. Said, "Introduction to arithmetic coding–theory and practice," *arXiv preprint arXiv:2302.00819*, 2023.

[37] Y. Pan, Z. Xu, M. Li, and L. Lazos, "Man-in-the-middle attack resistant secret key generation via channel randomization," in *Proceedings of the Twenty-second International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing*, 2021, pp. 231–240.

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

[39] 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*. IEEE, 2014, pp. 103–108.

[40] A. C. Rencher and G. B. Schaalje, *Linear models in statistics*. John Wiley & Sons, 2008.

Ehsan Olyaei Torshizi (Member, IEEE) was born in Iran in 1986. He received his B.Sc. degree with distinction in 2009 and his M.Sc. degree with honors in 2012, both in communications, from universities in Iran. From 2013 to 2021, he held various roles as a wireless communication and signal processing engineer. In December 2021, he joined the Transmission Systems Group at Constructor University of Bremen (formerly Jacobs University) as a research associate, where he focuses on physical layer secret key generation for wireless and wireline transmission systems. His research interests include physical layer security, secret key generation, LDPC codes, compressed sensing, signal processing, power line communication, multi-user communication, MIMO, and TEMPEST.

Werner Henkel (Senior Member, IEEE) received his Diploma and Dr.-Ing. (Ph.D.) degree from Darmstadt University of Technology (TUD) in May 1984 and June 1989, respectively. Thereafter, stages were: Deutsche Telekom's R&D Labs in Darmstadt, sabbatical at AT&T Bell Laboratories (later Lucent), Telecommunications Research Center Vienna, City University Bremen. Earlier teaching was at the universities of Kaiserslautern and Vienna. Since September 2003 he is a professor for electrical engineering at Constructor University, formerly Jacobs University and International University of Bremen chairing the ECE program from its existence until 2022. He was elected Dean from April 2012 to June 2014. He was adjunct faculty at ODU, Norfolk, VA in 2015. Courses taught are: Coding Theory; Information Theory; Data Compression, Compressive Sensing, and Modern Coding; Digital Signal Processing; Signals & Systems; Wireline Communications (DSL); Measurement automation; Circuits; and Statistical Analysis and Simulation. Dr. Henkel was involved in organizing or serving on the TPC for: ISIT 1997, IEEE J-SAC, June 2002, International Zurich Seminar 2004, EUSIPCO 2004 and 2007, ICC 2006, 2017 - 2024, Turbo Symposia (ISTC) 2008, 2010, 2014, 2016, 2018. 2020/21, 2023, IWCMC 2022 Sec. Symp., GC 2022 WS '5GBeyond', INFOCOM Wireless-Sec 2023, Globecom 2024 IEEE NExtG Wisec, and SampTA 2013. Publications are in the areas of coding, iterative decoding, unequal error protection, coded modulation, joint source-channel coding, network coding, frame synchronization, channel modeling, impulse noise, DSL, Power Line, single- and multicarrier transmission, multi-user communication, MIMO, DNA analysis, physical-layer security, and TEMPEST.