IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 7, 2021, accepted July 5, 2021, date of publication July 28, 2021, date of current version August 12, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3100925

Average Contiguous Duration (ACD)-Based Quantization for Secret Key Generation in Generalized Gamma Fading Channels

MUHAMMAD ADIL[1], SHURJEEL WYNE[1], (Senior Member, IEEE), SYED JUNAID NAWAZ[1], (Senior Member, IEEE), AND BILAL MUHAMMAD[2]

[1]Department of Electrical and Computer Engineering, COMSATS University Islamabad (CUI), Islamabad 45550, Pakistan
[2]CTIF Global Capsule, Department of Business Development and Technology, Aarhus University, 7400 Herning, Denmark

Corresponding author: Muhammad Adil (adil34700@gmail.com)

The work of Muhammad Adil was supported by the Higher Education Commission (HEC), Pakistan, under the Indigenous Ph.D. Fellowship Program. The work of Bilal Muhammad was supported by the project Research Collaboration and Mobility for Beyond 5G Future Wireless Networks (RECOMBINE) through the European Union's Horizon 2020 program under the scheme Marie Skłodowska-Curie Research and Innovation Staff Exchange (RISE) under the grant agreement no. 872857.

ABSTRACT The wireless channel-based Secret Key Generation (SKG) algorithms aim at securing the wireless link against unauthorized eavesdropping by exploiting the channel's randomness for generating matching secret keys at the legitimate nodes for message encryption/decryption. To counter differences in hardware and noise conditions at the legitimate nodes, which can lead to key mismatch, the SKG algorithms typically include the intermediate steps of sampling, quantization, information reconciliation, and privacy amplification. These steps collectively aim to improve the performance trade-offs between Key Generation Rate (KGR), Key Agreement Probability (KAP), and Secret Key Randomness (SKR) properties. This paper derives a closed-form expression for the Average Contiguous Duration (ACD) of Generalized Gamma (GG) fading wireless channels. The ACD is a recently introduced novel quantifier for characterizing the second-order statistics of fading channels, which includes Average Fade Duration (AFD) as its special case. The proposed GG fading ACD expression is shown to include, as its special cases, the ACD for commonly observed fading distributions such as Gamma, Nakagami-*m*, and Rayleigh. By exploiting the derived GG ACD expression, a multi-level quantization scheme for SKG is proposed that determines suitable quantization intervals for identical likelihood of an equal number of consecutive channel samples falling in each quantization interval. A comprehensive comparative analysis of the proposed ACD-based quantization for SKG is conducted in relation to conventional Uniform Quantization (UQ) and Cumulative Distribution Function (CDF)-based Non-Uniform Quantization (NUQ) schemes. The presented numerical results confirm the superior performance trade-off between KGR and KAP offered by the proposed ACD-based quantization in relation to that offered by UQ and CDF-based NUQ.

INDEX TERMS Average contiguous duration, generalized Gamma fading, physical layer security, quantization, secret key generation.

I. INTRODUCTION

The rollout of 5th Generation (5G) communication networks commenced in 2019 with Release-15 of 3rd Generation Partnership Project (3GPP) [1]. Researchers around the globe have recently started articulating the essential needs and requirements that may emerge in the Beyond 5G (B5G) era and Physical Layer Security (PLS) has emerged as a promising solution for augmenting secure wireless communication in B5G and 6th Generation (6G) wireless networks [2].

PLS has found applications in almost all emerging areas of modern wireless communications, such as, Unmanned Aerial Vehicle (UAV) communications [3], [4], Ultra-Reliable Low-Latency Communications (URLLC) [1], [5], and Intelligent Reflecting Surface (IRS) assisted communications [6] to name a few. Symmetric and asymmetric encryption are used

The associate editor coordinating the review of this manuscript and approving it for publication was Ilsun You.

in most modern day wireless communications for securing information against malicious wireless nodes [7]. However, secret key distribution and management infrastructure could become challenging in some modern modes of communications like Device-to-Device (D2D) communications due to limited device resources [8]. This motivates the use of symmetric secret key extraction from the common wireless channel, which requires no assistance from the server.

Secret Key Generation (SKG) is a PLS technique to extract symmetric secret keys at the legitimate nodes. It exploits the wireless propagation channel's randomness and requires channel reciprocity between the legitimate nodes as well as spatial independence between the multipath channel of legitimate nodes, and the multipath channel to the eavesdropping node [9]. The legitimate nodes (termed Alice and Bob in this work) alternately transmit probing signals to one another to independently measure the response of the main channel between them. Due to the underlying channel reciprocity, the channel observations of Alice X^n and those of Bob Y^n are highly correlated, whereas the eavesdropper (termed Eve in this work) measures independent channel observations Z^n and therefore she cannot estimate the key bits extracted by the legitimate nodes [10]–[12]. The SKG algorithms typically consist of channel sampling (legitimate nodes sample the reciprocal channel by alternately exchanging probing signals), channel quantization (Alice and Bob decide on channel-range thresholding scheme for channel observations so that measured channel samples can be transformed to secret key bits), information reconciliation (Alice and Bob minimize mismatch between their extracted key sequences by exchanging samples indices or using parity check codes etc.), and privacy amplification (Alice and Bob use a family of universal hash functions to transform their matched sequences into a final key not known to Eve) [13]. The performance of SKG algorithms is generally evaluated in terms of Key Generation Rate (KGR), Key Agreement Probability (KAP), and Secret Key Randomness (SKR) properties [10], and the quantizer design significantly affects these characteristics.

A. RELEVANT WORK

Suitable quantizer design is of prime significance in the overall design of SKG algorithms as it significantly impacts the desirable SKG performance, i.e., increasing the KGR, SKR, and the KAP between the legitimate nodes [10], [14]. The SKG quantizers can be classified either as a Uniform Quantizer (UQ) or a Non-Uniform Quantizer (NUQ). In the UQ, the observed range of channel samples is divided into equal width quantization intervals and guard-strips of equal interval are placed equidistant from one another, whereas in NUQ the observed channel-range is divided into un-equal width intervals to attain some desirable characteristic such as identical occurrence probability of samples across the quantization intervals. An M-level UQ (M-UQ) divides the channel-range into M uniform quantization intervals, whereas an M-level NUQ (M-NUQ) divides the observed channel-range into M non-uniform qantization intervals. The number M is typically a power of 2. In [15], a 2-NUQ was proposed to exploit the Received Signal Strength (RSS) variations for SKG. The deep fades of the signal's envelope in a Rayleigh fading environment were used to construct a 2-NUQ to increase the SKR of the generated secret key. In [11], an Adaptive Secret Bit Generation (ASBG) quantization strategy was proposed by employing 2-UQ for effective SKG. In [12], a 2-UQ was proposed for Channel Impulse Response (CIR)-based SKG to generate secret key bits with high SKR and KAP at the cost of reduced KGR. In [16], the authors proposed to modify channel quantization for SKG as Channel Quantization with Guard-band (CQG) to effectively increase KAP, and Channel Quantization Alternating (CQA) to avoid the guard-band/guard-strip loss by using a bank of M-NUQ for SKG. In [17], SKG analysis was conducted for wide-band channels and a quantization strategy was proposed that effectively increases KAP of secret keys between the legitimate nodes. In [18], a 2-UQ using vector quantization was proposed to minimize the disagreement between secret key bits extracted from those channel samples that lie on the quantization interval edges. In [19], a 2-UQ based on Lloyd–Max quantizer coupled with RSS pre-processing with sliding window averaging of channel samples was considered for efficient SKG. In [20], a Two Layer Secure (TLS) 2-UQ scheme was proposed with an intent to increase KGR using the correlated phase information of the wireless channel. In [10], an M-NUQ was proposed for Gamma distributed RSS channel samples to extract high entropy secret key bits from the wireless channel. In [21], 2-NUQ was used for Rayleigh channel to extract high entropy secret key bits from the envelope of the wireless channel. Most of the aforementioned quantizer designs have targeted increasing only the KAP of the legitimate nodes and little attention was given to jointly increasing the KAP and SKR. Furthermore, many of these quantizer designs are environment specific and lack generality in their design to be applicable to a wide variety of channel fading conditions.

In the existing literature for SKG, the 2-Level UQ strategy is commonly employed by determining the quantization thresholds from measured channel samples. In [22], the Channel Frequency Response (CFR) is utilized in a deep learning-based system for the Gaussian channel model by applying a 2-level NUQ scheme. An analytical framework for determining quantization intervals for SKG was recently proposed in [10] that employs a multi-level Cumulative Distribution Function (CDF)-based NUQ strategy intending to increase SKR performance in conjunction with KGR and KAP. In [21], a 2-level Average Fade Duration (AFD)-based quantization scheme is proposed for the Rayleigh fading channels. Recently, [14] proposed a novel quantifier named Average Contiguous Duration (ACD) for the characterization of wireless fading channels, and the Nakagami-m, Rice, and Rayleigh fading channels were investigated. The ACD metric can represent AFD as its special case. Multi-level quantization for SKG is one of the prime applications of the ACD metric. Nevertheless, there exists a wide research scope to

TABLE 1. Quantization Techniques for SKG from Wireless Channel Samples.

Research Publication and Year	Channel Model	Channel Parameter	Quantization	Approach
[15], 2005	Measurement Based	RSS	2-UQ	Measurement
[26], 2007	Rayleigh	CIR	2-UQ	Analytical
[12], 2010	Rayleigh	CIR	2-UQ	Analytical, Measurement
[17], 2010	Rayleigh	CIR	M-CDF	Analytical, Measurement
[11], 2014	Measurement Based	RSS	M-UQ	Measurement
[27], 2017	Measurement Based	RSS	2-UQ	Measurement
[18], 2017	Complex Gaussian	RSS	M-UQ	Simulations
[19], 2019	Measurement Based	RSS	2-UQ	Measurement
[20], 2019	Simulation Based	Phase	M-UQ	Analytical
[10], 2021	Gamma	RSS	M-CDF	Analytical
[21], 2021	Rayleigh	Envelope	2-CDF, 2-AFD	Analytical
[14], 2021	Rayleigh, Rice, Nakagami-m	Envelope	2-ACD	Analytical
[22], 2021	Gaussian	CFR	2-NUQ	Analytical
Proposed Work	**Generalized Gamma**	**Envelope**	**M-ACD**	**Analytical**

thoroughly investigate the potential of the ACD metric for the quantization of fading signals for SKG under different practical fading conditions.

The Generalized Gamma (GG) distribution was first proposed by Stacy [23] and later revisited as the $\alpha - \mu$ distribution for modeling wireless fading channels [24]. The GG distribution can not only model a wide variety of channel fading types as its special cases, such as Rayleigh, Nakagami-*m*, Gamma, and Weibull, but it can also compositely model both the small- and large-scale fading [25]. In this context, this work models the wireless channels in the considered system model as GG fading channels. Table 1 summarizes the relevant literature on quantization schemes for SKG from wireless channel samples.

B. CONTRIBUTIONS AND PAPER ORGANIZATION

This work focuses on SKG quantizer design to jointly enhance KAP and SKR for the GG fading channel conditions. This makes the proposed analysis general and applicable to a variety of channel fading conditions. The key contributions are listed as follows.

- A closed-form expression for the ACD of GG fading channels is derived. The derived expression is shown to include the ACD of Gamma, exponential, Rayleigh, and Nakagami-*m* fading as its special cases.
- An ACD-based multi-level non-uniform quantization scheme for GG fading is proposed, which incorporates a mathematical framework to determine the bounding thresholds of guard and quantization intervals to attain identical ACD values across all quantization intervals.
- An improved SKG algorithm is proposed by employing the proposed ACD-based quantization scheme into some notable SKG algorithms.
- A comparative performance analysis of the proposed ACD-based non-uniform quantization scheme is conducted in relation to conventional uniform quantization and CDF-based non-uniform quantization schemes on the basis of the KGR, KAP, and the SKR metrics.

The rest of this paper is organized as follows. Section II describes the considered system and channel model. Section III provides derivations for the proposed ACD-based quantization scheme. Section IV describes the proposed SKG algorithm and related key algorithmic and channel parameters. Section V provides numerical results for performance evaluation of the proposed quantization and SKG strategy. Finally, Section VI concludes this work.

Notational conventions are given in Table 2.

II. SYSTEM MODEL

Consider the wireless communication scenario shown in Fig. 1 in which Alice and Bob are the legitimate nodes who want to communicate securely in the presence of a passive eavesdropping node Eve, who does not disrupt their ongoing communications. Assuming a sufficiently rich scattering environment, the Eavesdropper channel between Alice and Eve will be decorrelated from the main channel between Alice and Bob provided that Eve's spatial separation from either legitimate node is as little as a fraction of the operating wavelength [9], [28].

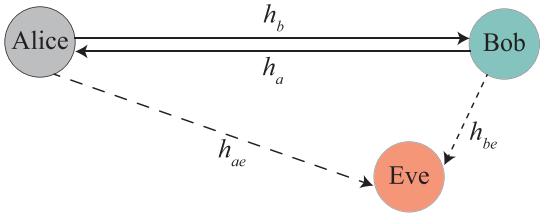


FIGURE 1. System model for secure wireless communications.

The wireless channels between Alice and Bob are ideally considered as reciprocal, i.e., the channel from Alice to Bob is identical to that from Bob to Alice. However, due to the difference in hardware and noise conditions of Alice and Bob, their observation of the common channel between them may differ. Practically, these observations will be correlated random variables with similar statistical properties. Considering that Alice's channel is h_a, Bob's channel can be related to Alice's channel by using the Gauss Markov model [10] as

$$h_b = \rho h_a + \sqrt{1-\rho^2} n_\circ, \tag{1}$$

where $\rho \in [0, 1]$ represents the correlation coefficient between h_a and h_b, which are modeled as correlated GG fading channels in this work. Furthermore, $n_\circ$ is the

TABLE 2. Mathematical Notational Conventions.

Notation	Definition
$h_{(\cdot)}$	Generalized Gamma (GG) fading channel at respective nodes
β	Fading parameter of the GG distribution
c	Inverse of the normalized variance of $h_{(\cdot)}^{\beta}$
ρ	Correlation coefficient between legitimate user's channels
τ^{total}	Total signal duration
$N_{h_{(\cdot)}}(\cdot)$	Level Crossing Rate (LCR)
$\tau_{h_{(\cdot)}}(\cdot)$	Average Fade Duration (AFD)
M	Number of quantization intervals
$M-1$	Number of guard-strip intervals
$\mathcal{Q}_i$	i^{th} quantization interval, $i \in \{1, M\}$
$\mathcal{G}_i$	i^{th} guard-strip interval , $i \in \{1, (M-1)\}$
z	Guard-strip interval
q_i^-	Lower bounding thresholds of i^{th} guard-strip interval, $i \in \{1, (M-1)\}$
q_i^+	Upper bounding thresholds of i^{th} guard-strip interval, $i \in \{1, (M-1)\}$
$\Xi_{q_1}^{q_2}$	Average Contiguous Duration (ACD) between two thresholds q_1 and q_2
$\tau_{q_1}^{q_2}$	Cumulative Contiguous Duration (CCD) between two thresholds q_1 and q_2
τ^{CRD}	Cumulative Rejected Duration (CRD) of $M-1$ guard-strip intervals
τ^{CAD}	Cumulative Accepted Duration (CAD) of M quantization intervals
$\mathcal{L}_{\mathcal{Q}}$	Guard-strip's interval for UQ
R_c	Channel range (Maximum - Minimum of channel values)
$\mathcal{R}_{(\cdot)}$	Channel samples array at respective node
N	Total number of channel samples
$\chi_{(\cdot)}$	Excursions array at respective node
$\mathcal{I}_{(\cdot)}$	Array of channel sample indices at respective node
L	Minimum excursion length for a qualifying excursion
$\nabla_{(\cdot)}$	Array of central excursion's indices at respective node
∇	Array of matching central indices at legitimate nodes
N^{CAS}	Cumulative Accepted Samples (CAS)
N^{CRS}	Cumulative Rejected Samples (CRS)
$\mathcal{P}_{\text{Rj.}}^{\text{UQ}}(M)$	Sample rejection probability under M-level UQ
$\mathcal{P}_{\text{Rj.}}^{\text{CDF-NUQ}}$	Sample rejection probability under M-level CDF-NUQ
$\mathbf{K}_{(\cdot)}$	Generated secret key at respective node
$\mathcal{L}_{\mathcal{K}}$	Secret key length (in bits) at legitimate nodes
$\mathcal{K}_{\mathcal{G}}$	Key Generation Rate (KGR)
$\mathcal{K}_{\mathcal{A}}$	Key Agreement Probability (KAP)
$\mathcal{L}$	Cumulative loss in KGR

difference between Alice and Bob's observation of their common channel h and it can be modeled as $n_\circ \sim \mathcal{N}(0, \sigma_\circ^2)$. The channel from Alice to Eve and Bob to Eve is h_{ae} and h_{be}, respectively, as indicated in Fig 1. The absolute value of channel envelope $|h_{(\cdot)}|$ is used for SKG. However, for mathematical simplicity, we notate $|h_{(\cdot)}|$ as $h_{(\cdot)}$ for the rest of the paper, where the subscript (.) takes label from $\{a, b, ae, be\}$.

The Probability Density Function (PDF) of a GG-distributed channel envelope $h_{(\cdot)}$ can be expressed as [24], [25], [29]

$$p(h_{(\cdot)}) = \frac{\beta}{\Gamma(c)} \left(\frac{c}{\Omega}\right)^c h_{(\cdot)}^{\beta c-1} e^{-\frac{ch_{(\cdot)}^{\beta}}{\Omega}}, \tag{2}$$

where β is a fading parameter, $\Gamma(\cdot)$ is the Gamma function [30], and $\Omega = E[h_{(\cdot)}^{\beta}]$, where $E[\cdot]$ denotes the statistical expectation. The parameter $c > 0$ is the inverse of the normalized variance of $h_{(\cdot)}^{\beta}$, which can be represented as

$$c = \frac{E^2\left[h_{(\cdot)}^{\beta}\right]}{V\left[h_{(\cdot)}^{\beta}\right]}, \tag{3}$$

where $V[\cdot]$ computes the statistical variance. This GG distribution can be used to represent various distribution types as its special case, e.g., Rayleigh ($\beta = 2, c = 1$), Nakagami-m ($\beta = 2$ and $c = m$), and Weibull ($c = 1$). The PDF in (2) can be used to determine CDF of GG fading envelope, which is given as [25]

$$F(h_{(\cdot)}) = \frac{\gamma\left(c, \frac{ch_{(\cdot)}^{\beta}}{\Omega}\right)}{\Gamma(c)}, \tag{4}$$

where $\gamma(\cdot, \cdot)$ is the lower incomplete Gamma function [30]. The joint PDF of the GG fading channels observed by Alice and Bob can be expressed as [25]

$$p(h_a, h_b) = \frac{\beta^2 c^{c+1} h_a^{\beta\frac{c+1}{2}-1} h_b^{\beta\frac{c+1}{2}-1}}{\Gamma(c)\Omega^{c+1}(1-\rho)\rho^{\frac{c-1}{2}}} \times e^{-\frac{c\left(h_a^2+h_b^2\right)}{(1-\rho)\Omega}} I_{c-1}\left(\frac{2c\sqrt{\rho h_a^{\beta} h_b^{\beta}}}{\Omega(1-\rho)}\right). \tag{5}$$

where $I_{c-1}(\cdot)$ is the (c-1)$^{\text{th}}$-order modified Bessel function of first kind and $\rho \in [0, 1]$ is the correlation coefficient. The conditional PDF can be obtained by manipulating (2) and (5), as

$$p(h_a|h_b) = e^{\frac{ch_b^{\beta}}{\Omega} - \frac{c\left(h_a^{\beta}+h_b^{\beta}\right)}{\Omega(1-\rho)}} \frac{\left(\frac{h_a}{\sqrt{\left(h_a^{\beta}+h_b^{\beta}\right)\rho}}\right)^{c-1}}{(1-\rho)\Omega(c\beta)^{-1}} \times I_{c-1}\left(\frac{2c\sqrt{(h_a^{\beta}+h_b^{\beta})\rho}}{(1-\rho)\Omega}\right). \tag{6}$$

The conditional CDF can be obtained by integrating $p(h_a|h_b)$ over h_a with appropriate limits to obtain

$$F(h_a|h_b) = 1 - Q_c\left(\sqrt{\frac{2c\rho h_b^{\beta}}{\Omega(1-\rho)}}, \sqrt{\frac{2ch_a^{\beta}}{\Omega(1-\rho)}}\right), \tag{7}$$

where $Q_c(\cdot, \cdot)$ is the Marcum-Q function of order c [31].

A. SECOND-ORDER FADING STATISTICS

Analytical expression for LCR $N_{h_{(.)}}(q)$ and AFD $\tau_{h_{(.)}}(q)$ of GG fading channels with reference to an arbitrary envelope threshold q can be expressed as [25]

$$N_{h_{(.)}}(q) = \sqrt{2\pi} f_m \frac{2c^{c-\frac{1}{2}}}{\Gamma(c)\Omega^{c-\frac{1}{2}}} q^{\frac{\beta}{2}(2c-1)} e^{-\frac{cq^\beta}{\Omega}}, \tag{8}$$

$$\tau_{h_{(.)}}(q) = \frac{1}{\sqrt{2\pi} f_m} \left(\frac{\Omega}{c}\right)^{c-\frac{1}{2}} \gamma\left(c, \frac{c}{\Omega} q^\beta\right) e^{\frac{cq^\beta}{\Omega}} q^{-\frac{\beta}{2}(2c-1)}, \tag{9}$$

where f_m represents the maximum Doppler shift.

The ACD of a fading signal is defined as the average time duration for which a signal contiguously remains within an interval defined by two bounding thresholds [14]. In Fig. 2, an example signal is illustrated for which computations of ACD for 2 different quantization intervals are shown. For the quantization interval $\mathcal{Q}_1$ defined by the amplitude range from 0 to q_1^-, there are $J = 3$ contiguous duration instances (CDIs) indicated in the figure (i.e., labeled as $\delta_{\mathcal{Q}_1}(1)$, $\delta_{\mathcal{Q}_1}(2)$, and $\delta_{\mathcal{Q}_1}(3)$), which can be used to find ACD for this interval as $\Xi_0^{q_1^-} = \frac{1}{3}\sum_{j=1}^{3} \delta_{\mathcal{Q}_1}(j)$. Similarly, for the quantization interval $\mathcal{Q}_2$ defined from q_1^+ to $q_{\max}$ (peak amplitude), there exist $J = 4$ CDIs labeled as $\delta_{\mathcal{Q}_2}(1), \cdots, \delta_{\mathcal{Q}_2}(4)$, which correspond to the computation of ACD as $\Xi_{q_1^+}^{q_{\max}} = \frac{1}{4}\sum_{j=1}^{4} \delta_{\mathcal{Q}_2}(j)$. For the guard-strip interval $\mathcal{G}_1$ from q_1^- to q_1^+, there exist a total of $J = 6$ CDIs for which the ACD can be computed as $\Xi_{q_1^-}^{q_1^+} = \frac{1}{6}\sum_{j=1}^{6} \delta_{\mathcal{G}_1}(j)$. The ACD $\Xi_{q_1}^{q_2}$ with reference to two arbitrary thresholds q_1 and q_2 (i.e., $q_2 > q_1$) in generic form (for any distribution type) can be defined in a rigorous way as [14]

$$\Xi_{q_1}^{q_2} = \frac{F(q_2) - F(q_1)}{N_{h_{(.)}}(q_1) + N_{h_{(.)}}(q_2)}. \tag{10}$$

By substituting the CDF $F(\cdot)$ given in (4) and LCR $N_{(.)}(.)$ given in (8) into (10), closed-form analytical expression of ACD for the GG fading channels can be derived as

$$\Xi_{q_1}^{q_2} = \frac{\left(\frac{\Omega}{c}\right)^{c-\frac{1}{2}} \left(\gamma\left(c, \frac{cq_2^\beta}{\Omega}\right) - \gamma\left(c, \frac{cq_1^\beta}{\Omega}\right)\right)}{f_m\sqrt{2\pi}\left(q_1^{\frac{\beta}{2}(2c-1)} e^{-\frac{cq_1^\beta}{\Omega}} + q_2^{\frac{\beta}{2}(2c-1)} e^{-\frac{cq_2^\beta}{\Omega}}\right)}. \tag{11}$$

This closed-form expression of the ACD for GG fading channels is one of the main contributions of this work. This analytical expression can represent the ACD of several distribution types as its special case, e.g., by substituting $\beta = 2$ and $c = 1$ in (11) it deduces to the ACD for Rayleigh distribution given in [14]. Table 3 provides further details.

TABLE 3. ACD of notable fading types as a function of the derived equation of ACD for GG fading.

Parameters	Distribution Type	ACD, $\Xi_{q_1}^{q_2}$
$c = 1, \beta = 2$	Rayleigh [14]	$\frac{\sqrt{\Omega}\left(e^{\frac{q_2^2}{\Omega}} - e^{\frac{q_1^2}{\Omega}}\right)}{\sqrt{2\pi} f_m \left(q_1 e^{\frac{q_2^2}{\Omega}} + q_2 e^{\frac{q_1^2}{\Omega}}\right)}$
$c = m, \beta = 2$	Nakagami-m [14]	$\frac{\left(\frac{\Omega}{m}\right)^{m-\frac{1}{2}} \left(\gamma\left(m, \frac{mq_2^2}{\Omega}\right) - \gamma\left(m, \frac{mq_1^2}{\Omega}\right)\right)}{\sqrt{2\pi} f_m \left(q_1^{(2m-1)} e^{-\frac{mq_1^2}{\Omega}} + q_2^{(2m-1)} e^{-\frac{mq_2^2}{\Omega}}\right)}$
$c = 1$	Weibull [Proposed]	$\frac{\sqrt{\Omega}\left(e^{\frac{q_2^\beta}{\Omega}} - e^{\frac{q_1^\beta}{\Omega}}\right)}{\sqrt{2\pi} f_m \left(q_1^{\frac{\beta}{2}} e^{\frac{q_2^\beta}{\Omega}} + q_2^{\frac{\beta}{2}} e^{\frac{q_1^\beta}{\Omega}}\right)}$
$\beta = 1$	Gamma [Proposed]	$\frac{\left(\frac{\Omega}{c}\right)^{c-\frac{1}{2}} \left(\gamma\left(c, \frac{cq_2}{\Omega}\right) - \gamma\left(c, \frac{cq_1}{\Omega}\right)\right)}{\sqrt{2\pi} f_m \left(q_1^{\frac{1}{2}(2c-1)} e^{-\frac{cq_1}{\Omega}} + q_2^{\frac{1}{2}(2c-1)} e^{-\frac{cq_2}{\Omega}}\right)}$

We define *Cumulative Contiguous Duration* (CCD) as the total time duration for which the channel envelope $h_{(.)}$ stays within the amplitude interval of interest (i.e., defined as bounded by q_1 and q_2) as

$$\tau_{q_1}^{q_2} = \tau^{\text{total}} \left(F(q_2) - F(q_1)\right). \tag{12}$$

where τ^{total} is the total observed channel envelope time. This can be represented as a function of ACD, i.e., by multiplying ACD with number of CDIs and τ^{total} as

$$\tau_{q_1}^{q_2} = \tau^{\text{total}}\ \Xi_{q_1}^{q_2} \left(N_{h_{(.)}}(q_1) + N_{h_{(.)}}(q_2)\right). \tag{13}$$

The CCD metric is of significance in conducting the performance analysis of SKG algorithm, e.g., in deriving expression for KGR.

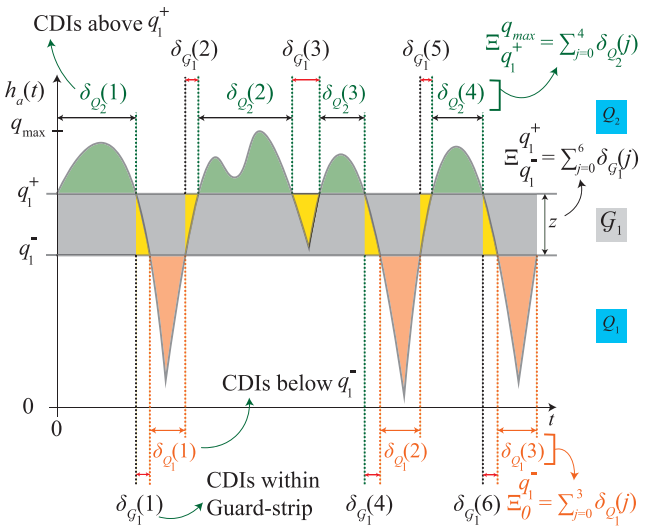


FIGURE 2. 2-Level ACD-based quantization for SKG using fading envelope of some arbitrary signal. The guard strips $\mathcal{G}_1$ of interval z and Contiguous Duration Instances (CDIs) for the quantization intervals $\mathcal{Q}_1$ and $\mathcal{Q}_2$ are also shown.

III. QUANTIZATION FOR SKG

Among the three conventional performance measures of SKG algorithms the SKR, which is quantified in terms of the National Institute of Standards and Technology (NIST) test suite [32], is the most critical. Ideally, an SKG scheme should generate a noise-like bit sequence with each generated bit equally likely to be 0 or 1. This requirement puts restrictions on the design of channel quantization and sample encoding steps of the SKG schemes. Channel quantization is usually performed either based on the PDF [10], the AFD [21], or channel parameters such as the sample mean μ computed from samples collected at Alice and Bob [11]. Recently, [14] has proposed the ACD as another important channel metric to determine suitable quantization thresholds for the channel samples to perform SKG.

Fig. 3 plots the GG fading main channel variations separately for Alice and Bob. The $h_{(\cdot)}$ variations observed at Alice and Bob are highly correlated due to the underlying reciprocity of the main channel. This allows the legitimate nodes to extract a secret key from the channel variations, unknown to Eve, even when their channel strength is weaker than that of Eve. To transform the channel variations such as those shown in Fig. 3 to a secret key sequence, the channel variations are first sampled. This is achieved by alternately sending probe signals between Alice and Bob within a channel coherence time (T_c) for the receiving node to measure its channel response. Since the channel response does not change during one T_c, respective measurements of the main channel at Alice and Bob will be highly correlated and will contribute one channel sample for SKG. This process continues until sufficient channel samples are collected at both legitimate nodes to extract key sequence of the desired length. Let Alice and Bob each collect N channel samples, then the vector of samples $\mathcal{R}_\mathcal{A}$ collected at Alice can be expressed as

$$\mathcal{R}_\mathcal{A} = \left[h_1^\mathcal{A}, h_2^\mathcal{A}, \cdots, h_N^\mathcal{A}\right]^{\mathrm{T}}, \tag{14}$$

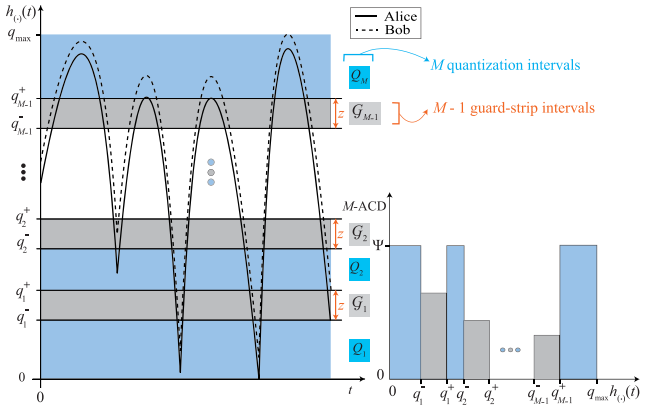


FIGURE 3. *M*-level ACD-based quantization of GG fading envelope by Alice and Bob. An identical Ψ is ensured for the *M* quantization intervals $\mathcal{Q}_1, \mathcal{Q}_2, \cdots, \mathcal{Q}_M$. Also, the $M-1$ guard-strips of identical width z are shown.

Algorithm 1 Proposed Simulation Scheme to Generate Correlated GG Fading Envelope Samples for Alice and Bob

Input: $c, \rho, \beta, \Omega, N$
Output: $\mathcal{R}_\mathcal{A}$ and $\mathcal{R}_\mathcal{B}$
1: **for** $i = 1$ to N **do**
2: $\quad r \leftarrow \text{rand}(1)$
3: $\quad \mathcal{R}_\mathcal{A}(i) \leftarrow \text{solve}\left(r = \frac{\gamma(c, \frac{ch_a^\beta}{\Omega})}{\Gamma(c)}, h_a\right)$
4: $\quad \mathcal{R}_\mathcal{B}(i) \leftarrow \text{solve}\left(r = 1 - Q_m\left(\sqrt{\frac{2c\rho(h_b(i))^\beta}{\Omega(1-\rho)}}, \sqrt{\frac{2c(h_a(i))^\beta}{\Omega(1-\rho)}}\right), h_b(i)\right)$
5: **end for**

where $[\cdot]^{\mathrm{T}}$ represents the matrix transpose operation. Similarly the sample vector collected at Bob can be expressed as

$$\mathcal{R}_\mathcal{B} = \left[h_1^\mathcal{B}, h_2^\mathcal{B}, \cdots, h_N^\mathcal{B}\right]^{\mathrm{T}}. \tag{15}$$

The corresponding array of sample index values for Alice is

$$\mathcal{I}_\mathcal{A} = \left[1^\mathcal{A}, 2^\mathcal{A}, \cdots, N^\mathcal{A}\right]^{\mathrm{T}}, \tag{16}$$

and for Bob the sample index array is

$$\mathcal{I}_\mathcal{B} = \left[1^\mathcal{B}, 2^\mathcal{B}, \cdots, N^\mathcal{B}\right]^{\mathrm{T}}. \tag{17}$$

To assist in simulation-based investigations, a method for generating correlated GG fading channel envelope samples is given in Algorithm 1, where the function rand$(\cdot)$ generates a number r uniformly distributed over the interval [0, 1] and solve$(r = f(x), x)$ solves the equation for the unknown x.

The channel sampling step in SKG is followed by the quantization step, i.e., setting thresholds for transforming the measured channel samples into bit sequences. As shown in Fig. 3, Alice and Bob's estimates of the reciprocal main channel can be different but highly correlated. Alice and Bob then determine suitable threshold values to identify quantization intervals. To avoid the event that slightly differing channel samples near quantization thresholds fall in different quantization intervals at Alice and Bob leading to mismatch in the extracted key bits, a guard-strip of interval z is used between two quantization intervals and any sample that lies within this guard-strip is discarded [10]–[12]. The legitimate nodes can thus extract identical keys despite differing channel observations as long as the absolute difference between their channel samples is less than z. However, this requires determination of z and placement of its thresholds $q_i^\pm$ on the channel-range axis. Fig. 3 shows the quantization by a single node, where the observed channel-range is divided into M quantization intervals $\mathcal{Q}_1$ to $\mathcal{Q}_M$ separated by $M-1$ guard-strips $\mathcal{G}_1$ to $\mathcal{G}_{M-1}$ each of interval z defined as bounded by thresholds q_i^- and q_i^+, $i \in [0, M-1]$.

Based on the quantization and guard-strip intervals determining strategy, the quantization can be classified into following categories.

- Uniform Quantization (UQ)
- Non-uniform Quantization (NUQ)
  - CDF-based NUQ (CDF-NUQ)
  - ACD-based NUQ (ACD-NUQ)

These quantization strategies are described in the following paragraphs.

A. UNIFORM QUANTIZATION (UQ)

For UQ the channel-range is quantized such that the guard-strips are placed at uniform intervals above and below the mean of the channel samples. The UQ strategy has been adopted in most of the measurement-based SKG algorithms [11], [12]. However, this scheme fails to satisfy the SKR requirements of the generated secret key when the underlying channel distribution is not uniform. The channel-range is defined as $R_c = q_{\max}$ - 0, where 0 and $q_{\max}$ represent the minimum and maximum values of the GG fading channel parameter, respectively. For M-level UQ scheme, the channel-range can be divided into M quantization intervals of equal length $\mathcal{L}_\mathcal{Q}$ by defining the M-1 separating guard-strips each of interval z such that

$$R_c = M\mathcal{L}_\mathcal{Q} + (M-1)z, \tag{18}$$

which for given values of R_c, M, and z can be solved for $\mathcal{L}_\mathcal{Q}$ as

$$\mathcal{L}_\mathcal{Q} = \frac{R_c - (M-1)z}{M}. \tag{19}$$

The lower thresholds q_i^- can then be computed as

$$q_i^- = i\mathcal{L}_\mathcal{Q} + (i-1)z; \quad 1 \le i \le M-1, \tag{20}$$

and the corresponding upper thresholds are computed as

$$q_i^+ = q_i^- + z; \quad 1 \le i \le M-1. \tag{21}$$

For an M-UQ, a sample is rejected (Rj.) with probability

$$\mathcal{P}_{\text{Rj.}}^{\text{UQ}}(M) = \sum_{i=1}^{M-1} \int_{q_i^-}^{q_i^+} p(h_{(.)})dh_{(.)}, \tag{22}$$

and accepted (Ac.) with probability $\mathcal{P}_{\text{Ac.}}^{\text{UQ}}(M) = 1 - \mathcal{P}_{\text{Rj.}}^{\text{UQ}}(M)$.

B. NON-UNIFORM QUANTIZATION (NUQ)

In NUQ, the channel-range is divided into quantization intervals of unequal widths (with the exception of uniformly distributed channel envelope) based on statistical knowledge of the wireless channel. Such a NUQ scheme can be based on CDF (or equivalently PDF) of the channel samples [10], [21] or it can be based on the ACD metric [14].

1) CDF BASED NON-UNIFORM QUANTIZATION (CDF-NUQ)

CDF-NUQ is characterized by the division of the channel-range into non-uniform quantization intervals such that the area under each quantization interval is equal. This corresponds to a single channel sample having identical probability of lying in any quantization interval. For M-NUQ, we define the M-CDF function as

$$\Lambda_0^{q_{M-1}^- + z}(M) = \left[F|_{q_0^+=0}^{q_1^-}, F|_{q_1^-+z}^{q_2^-}, \cdots, F|_{q_{M-1}^-+z}^{\infty} \right], \tag{23}$$

where $F|_a^b$ is the area under the PDF curve from a to b, i.e., it represents the likelihood of a channel sample to fall in the quantization interval bounded by a and b. To ensure equal probability for each M quantization intervals, the M non-uniform quantization intervals are determined by setting guard-strip bounding thresholds q_1^- to q_{M-1}^+ such that

$$F|_{q_1^+=0}^{q_1^-} = F|_{q_1^-+z}^{q_2^-} = \cdots = F|_{q_{M-1}^-+z}^{\infty} = \Phi, \tag{24}$$

where $0 \le \Phi \le 1/M$. This can equivalently be expressed by using the distribution's PDF as [10],

$$\begin{aligned} \int_{q_0^+}^{q_1^-} p(h_{(.)})dh_{(.)} &= \int_{q_1^-+z}^{q_2^-} p(h_{(.)})dh_{(.)} \cdots \\ &= \int_{q_{M-1}^-+z}^{\infty} p(h_{(.)})dh_{(.)} = \Phi. \end{aligned} \tag{25}$$

By manipulating $M-1$ pairs of equations representing the PDF area of different quantization intervals, as provided in (24), the $M-1$ thresholds $\{q_1^-, q_2^-, \cdots, q_{M-1}^-\}$ can be computed. The fixed guard-strip interval z is added to lower bounding threshold of each guard-strip to obtain the upper bounding threshold, i.e., $q_{(.)}^+ = q_{(.)}^- + z$.

For M-level CDF-based NUQ, the total probability of rejected samples can be determined by adding the area of PDF curve associated to each guard strip as

$$\mathcal{P}_{\text{Rj.}}^{\text{CDF-NUQ}}(M) = \sum_{i=1}^{M-1} \int_{q_i^-}^{q_i^+} p\left(h_{(.)}\right) dh_{(.)}. \tag{26}$$

Similarly, the total probability of accepted samples can be determined, as $\mathcal{P}_{\text{Ac.}}^{\text{CDF-NUQ}} = 1 - \mathcal{P}_{\text{Rj.}}^{\text{CDF-NUQ}}(M)$.

The 2-CDF-NUQ quantizer with lower threshold q_1^- and upper threshold $q_1^+ = q_1^- + z$ can be expressed using Eq. (4) and Eq. (24) for the GG fading channels as

$$\gamma\left(c, \frac{c(q_1^-)^\beta}{\Omega}\right) = \Gamma\left(c, \frac{c(q_1^+)^\beta}{\Omega}\right), \tag{27}$$

which can be solved given values of c, β, and Ω for the required q_1^- and q_1^+ with guard-strip interval z. For $M = 4$ level CDF-based NUQ, the following equation are numerically solved for q_1^-, q_2^-, and q_3^-

$$\gamma\left(c, \frac{cq_1^{-\beta}}{\Omega}\right) = \gamma\left(c, \frac{cq_2^{-\beta}}{\Omega}\right) - \gamma\left(c, \frac{c(q_1^- + z)^\beta}{\Omega}\right), \tag{28}$$

$$\gamma\left(c, \frac{cq_1^{-\beta}}{\Omega}\right) = \gamma\left(c, \frac{cq_3^{-\beta}}{\Omega}\right) - \gamma\left(c, \frac{c(q_2^- + z)^\beta}{\Omega}\right), \tag{29}$$

$$\gamma\left(c, \frac{mq_1^{-\beta}}{\Omega}\right) + \gamma\left(c, \frac{c(q_2^- + z)^{\beta}}{\Omega}\right) = \gamma\left(c, \frac{cq_3^{-\beta}}{\Omega}\right), \quad (30)$$

$$\gamma\left(c, \frac{cq_3^{-\beta}}{\Omega}\right) - \gamma\left(c, \frac{c(q_2^- + z)^{\beta}}{\Omega}\right) = 1 - \gamma\left(c, \frac{c(q_3^- + z)^{\beta}}{\Omega}\right). \quad (31)$$

and the upper thresholds q_1^+, q_2^+, and q_3^+ are computed by adding guard-strip interval z to each corresponding negative thresholds.

2) ACD BASED NON-UNIFORM QUANTIZATION (ACD-NUQ)

The ACD information can be exploited to perform channel quantization for SKG. The ACD can be used to determine the sample interval (or sample rate) required for ensuring a certain number of contiguous samples falling within a given quantization interval [14]. For example, by setting the sampling interval as $T_s = \Xi_{q_{(\cdot)}^-}^{q_{(\cdot)}^+}/\Upsilon$, on average Υ contiguous samples will fall in the quantization interval spanning from $q_{(\cdot)}^-$ to $q_{(\cdot)}^+$. The contiguous sample count (or excursion length) associated to the ACD can be computed as $\overline{\Xi}_{q_{(\cdot)}^-}^{q_{(\cdot)}^+} = \text{floor}(\Xi_{q_{(\cdot)}^-}^{q_{(\cdot)}^+}/T_s)$.

Fig. 2 depicts the channel profile observed at a legitimate node and the 3 consecutive CDIs below the threshold q_1^- are labelled as $\delta_{\mathcal{Q}_1}(1), \cdots, \delta_{\mathcal{Q}_1}(3)$, whereas those above the threshold q_1^+ are labeled $\delta_{\mathcal{Q}_2}(1), \cdots, \delta_{\mathcal{Q}_2}(4)$. Furthermore, as shown in Fig. 3 for the M-level quantization case, the aim is to set the guard-strip z and thresholds, $q_1^-, q_1^+, \cdots, q_{M-1}^-$, q_{M-1}^+, such that $\Xi_0^{q_1^-}, \Xi_{q_1^+}^{q_2^-}, \cdots, \Xi_{q_{M-1}^+}^{q_{\max}}$ are equal. For M-level ACD-based quantization, the M-ACD functions is defined as

$$\Theta_0^{q_{M-1}^- + z}(M) = \left[\Xi_{q_0^+=0}^{q_1^-}, \Xi_{q_1^- + z}^{q_2^-}, \cdots, \Xi_{q_{M-1}^- + z}^{q_{\max}}\right]. \quad (32)$$

To ensure equal ACD of all the M intervals, out of total $2M$ thresholds $q_{(\cdot)}^{\pm}$, after fixing $q_0^+ = 0$ and $q_M^- = q_{\max}$, the remaining $2(M-1)$ thresholds (see Fig. 3) can be computed such that

$$\Xi_{q_0^+=0}^{q_1^-} = \Xi_{q_1^- + z}^{q_2^-} = \cdots = \Xi_{q_{M-1}^- + z}^{q_M^- = q_{\max}} = \Psi, \quad (33)$$

where Ψ represents the ACD floor.

From the definition proposed in (13), the CCD of channel envelope $h_{(\cdot)}$ for quantization interval $\mathcal{Q}_i$ (defined as bounded by q_{i-1}^+ and q_i^-) can be obtained as

$$\tau_{\mathcal{Q}_i} = \tau_{q_{i-1}^+}^{q_i^-} = \tau^{\text{total}}\, \Xi_{q_{i-1}^+}^{q_i^-}\left(N_{h_{(\cdot)}}(q_{i-1}^+) + N_{h_{(\cdot)}}(q_i^-)\right). \quad (34)$$

Similarly, CCD for the guard-strip interval $\mathcal{G}_i$ (defined as bounded by q_i^- and q_i^+) can be obtained as

$$\tau_{\mathcal{G}_i} = \tau_{q_i^-}^{q_i^+} = \tau^{\text{total}}\, \Xi_{q_i^-}^{q_i^+}\left(N_{h_{(\cdot)}}(q_i^-) + N_{h_{(\cdot)}}(q_i^+)\right). \quad (35)$$

Subsequently, the *Cumulative Accepted Duration (CAD)* can be obtained by adding the CCD of all quantization intervals as

$$\tau^{\text{CAD}} = \sum_{i=1}^{M} \tau_{\mathcal{Q}_i} = \Psi\, \tau^{\text{total}} \sum_{i=1}^{M}\left(N_{h_{(\cdot)}}(q_{i-1}^+) + N_{h_{(\cdot)}}(q_i^-)\right). \quad (36)$$

Similarly, the total time duration for which the channel envelope stays in the guard intervals can be termed as *Cumulative Rejected Duration (CRD)*, which can be obtained as

$$\tau^{\text{CRD}} = \sum_{i=1}^{M-1} \tau_{\mathcal{G}_i} = \tau^{\text{total}} \sum_{i=1}^{M-1} \Xi_{q_i^-}^{q_i^+}\left(N_{h_{(\cdot)}}(q_i^-) + N_{h_{(\cdot)}}(q_i^+)\right). \quad (37)$$

The total observed duration of a signal under consideration can be represented as

$$\tau^{\text{total}} = \tau^{\text{CAD}} + \tau^{\text{CRD}} \quad (38)$$

A simple exposition of the proposed M-level ACD-based quantization can be demonstrated for $M = 2$. The channel-range for $M = 2$ can be divided into two intervals such that

$$\Xi_{q_0^+=0}^{q_1^-} = \Xi_{q_1^- + z}^{q_{\max}}. \quad (39)$$

By substituting $q_{\max} = \infty$ and $q_0^+ = 0$ in (39) for GG fading channels, we get

$$e^{\frac{c}{\Omega}\left(q_1^{-\beta} - q_1^{+\beta}\right)}\left(\frac{q_1^-}{q_1^+}\right)^{\frac{\beta}{2}(1-2c)} \gamma\left(c, \frac{cq_1^{-\beta}}{\Omega}\right) = \Gamma\left(c, \frac{c(q_1^- + z)^{\beta}}{\Omega}\right), \quad (40)$$

Considering the case of exponential distribution (i.e., $\beta = 1$ and $c = 1$) and no guard-strip (i.e., $z = 0$ and $q_1^- = q_1^+ = q$), (40) can be rearranged for the separating threshold q as

$$q = \Omega \ln 2, \quad (41)$$

where the threshold q represents the median value for the considered case of exponential distribution.

Similarly, considering the case of Rayleigh distribution (i.e., $\beta = 2$ and $c = 1$) and no guard-strip (i.e., $z = 0$ and $q_1^- = q_1^+ = q$), (40) can be rearranged for the separating threshold q as

$$q = \sqrt{\Omega \ln 2}. \quad (42)$$

This is consistent with the derivations conducted in [14] for Rayleigh fading channels; thus, it also establishes the validity of the conducted analysis.

After the channel quantization step, the quantized channel samples are mapped to the binary codes associated with each quantization interval, e.g., by using gray coding. These bit strings are sequentially concatenated to form the key sequence that is further processed by the information reconciliation step to generate the sequence of secret key bits. In this work the Bose-Chaudhuri-Hocquenghem (BCH) code [33] has been considered for the information reconciliation between the legitimate nodes.

IV. SECRET KEY GENERATION (SKG)

This section describes the SKG algorithm employing the proposed M-level ACD-based NUQ scheme.

A. QUANTIZATION AND GUARD INTERVALS

$M-1$ guard-strips (i.e., $\mathcal{G}_1, \mathcal{G}_2, \cdots, \mathcal{G}_{M-1}$) of interval z are introduced in the amplitude range (i.e., from 0 to $q_{\max}$) separating M quantization intervals (i.e., $\mathcal{Q}_1, \mathcal{Q}_2, \cdots, \mathcal{Q}_M$). The guard and quantization intervals are defined according to the strategies presented in Sec. III-A, III-B1, and III-B2 for UQ, CDF-based NUQ, and ACD-based NUQ, respectively. The appropriate guard-strip interval z can be determined as a function of the mean squared error $\sigma_\circ$ between sample observations of the legitimate nodes, which is expressed as

$$z = k\sigma_\circ, \tag{43}$$

where k is a control parameter. The samples that fall in the guard-strip interval are termed as *rejected samples*, which are marked as • in Fig. 4. The rejected samples are not considered by the legitimate nodes for SKG. Whereas, the samples that fall in the quantization intervals are referred to as *considered samples*, which are marked as ⊙ and *accepted samples* marked as ⚬ Fig. 4. The considered samples contribute to SKG subject to further processing of the algorithm. *Excursion Qualification Length L:* An excursion is defined by an occurrence of consecutive channel samples within one quantization interval. For example, Fig. 4 shows 4 excursions of different sample lengths in quantization interval $\mathcal{Q}_2$. The minimum excursion length L [12] represents the minimum number of consecutive channel samples required by an excursion to be considered valid for key extraction. Only the channel samples' excursions of length $\geq L$ are valid for SKG, while all the other excursions are discarded. (valid excursions may have more than one qualifying excursions of length L, see e.g., two consecutive excursions shown in Fig. 4). The parameter is pre-determined so that the legitimate nodes can reliably extract secret keys with maximal KAP. Considering Fig. 4 and assuming $L = 3$, 3 out of all 4 excursions (1^{st}, 2^{nd}, and 4^{th}) above q_1^+ shown in this figure will be considered for key extraction as each has length not less than $L = 3$ samples whereas the 3^{rd} excursion will be rejected as it does not qualify minimum excursion length requirement. In this context, in order to optimize the performance trade-off between KGR and SKR, we propose that the minimum excursion length threshold L may be suitably set with reference to the ACD floor value, i.e., $L \propto \text{floor}(\Psi)$.

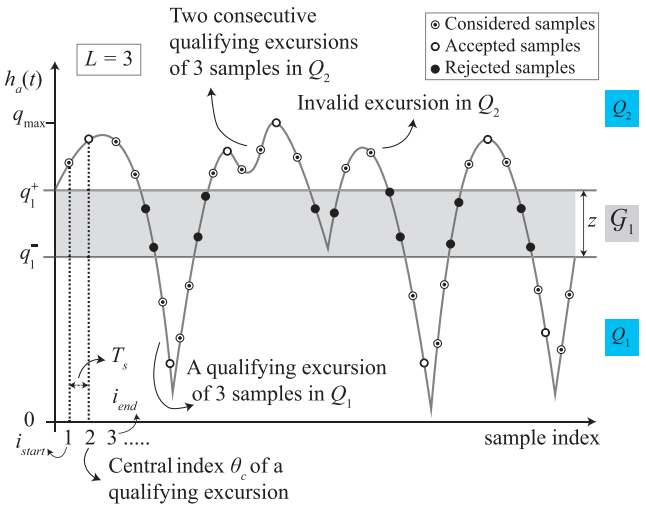


FIGURE 4. 2-level quantization of channel samples at a legitimate node. Four valid excursions (length $\geq L = 3$) above threshold q_1^+ are shown with ⚬ samples used for SKG. The • samples falling in guard-strip are not considered for SKG.

B. CENTRAL INDEX OF A QUALIFYING EXCURSION

This is the index of the centrally-located sample in a qualifying excursion. The central index is calculated as $\theta_c = \lfloor \frac{i_{start}+i_{end}}{2} \rfloor$ where i_{start} is the index of first sample of a qualifying excursion and i_{end} is the index of last sample of the same qualifying excursion. The function $\lfloor \cdot \rfloor$ rounds its argument to the nearest lower integer. In Fig. 4, the indices shown as ⚬ are central indices of their respective qualifying excursions.

C. MATCHING EXCURSION AND ACCEPTED SAMPLES

Due to the main channel being not ideally reciprocal, Alice and Bob may measure different central indices of some of the qualifying excursions. An excursion for which Alice and Bob successfully determine the same central index is termed as a matching excursion. The samples corresponding to the central indices of such matching excursions are termed as accepted samples, which are marked with ⚬) in Fig. 4.

The generic steps for SKG are described below.

- Alice parses her observed channel sample vector $\mathcal{R}_\mathcal{A}$ to identify qualifying excursions of length L samples. Let there are u such excursions $\chi_\mathcal{A}^k$, $k = 1 \ldots u$, which are collected in array $\chi_\mathcal{A}$ expressed as

$$\chi_\mathcal{A} = \left[\chi_\mathcal{A}^1, \chi_\mathcal{A}^2, \cdots, \chi_\mathcal{A}^u\right]. \tag{44}$$

  The array of central indices of these excursions is

$$\nabla_\mathcal{A} = \left[\theta_\mathcal{A}^1, \theta_\mathcal{A}^2, \cdots, \theta_\mathcal{A}^u\right], \tag{45}$$

  where $\theta_\mathcal{A}^k$ is k^{th} central index at Alice.

- Bob repeats the above step to compute his own array of qualifying excursions and their central indices. Let there be v such excursions at Bob that are collected in array $\chi_{\mathcal{B}}$ expressed as

$$\chi_{\mathcal{B}} = \left[\chi_{\mathcal{B}}^{1}, \chi_{\mathcal{B}}^{2}, \cdots, \chi_{\mathcal{B}}^{v}\right]. \tag{46}$$

  The corresponding array of central indices at Bob is given by

$$\nabla_{\mathcal{B}} = \left[\theta_{\mathcal{B}}^{1}, \theta_{\mathcal{B}}^{2}, \cdots, \theta_{\mathcal{B}}^{v}\right], \tag{47}$$

  where $\theta_{\mathcal{B}}^{k}$ represents k^{th} central index at Bob.
- Alice and Bob use indices exchange-based information reconciliation (IR) scheme. Alice first sends $\nabla_{\mathcal{A}}$ to Bob, who compares $\nabla_{\mathcal{A}}$ with $\nabla_{\mathcal{B}}$ and places their common indices in the array ∇ of length w, which can be expressed as

$$\nabla = [\theta_1, \theta_2, \cdots, \theta_w], \tag{48}$$

  where $w \leq \min(u, v)$ and $\min(\cdot)$ returns the minimum of input arguments.
- Bob sends ∇ to Alice so that both have knowledge of central indices of their matching excursions.
- Using the indices in ∇, Alice and Bob transform their relevant channel samples in $\mathcal{R}_{\mathcal{A}}$ and $\mathcal{R}_{\mathcal{B}}$ into length $\mathcal{L}_{\mathcal{K}}$ bit secret key sequences $\hat{\mathbf{K}}_{\mathcal{A}}$ and $\hat{\mathbf{K}}_{\mathcal{B}}$, respectively. This mapping can be expressed as

$$\hat{\mathbf{K}}_i = \mathcal{H}(\nabla), \ i \in (\mathcal{A}, \mathcal{B}) \tag{49}$$

  where the function $\mathcal{H}(\cdot)$ maps the channel sample value at its index argument into a bit sequence according to gray-code bit assignment of quantization intervals. Alice and Bob employ BCH coding-based information reconciliation scheme (BR scheme) as the second step after employing the IR scheme, i.e., the combination of IR and BR schemes is referred to as IBR scheme in Algorithm 2. This is applied on the respective extracted key-bits $\hat{\mathbf{K}}_i$ to obtain matching secret keys $\mathbf{K}_{\mathcal{A}}$ and $\mathbf{K}_{\mathcal{B}}$, i.e., Bob's key is reconciled with the Alice's key.

D. BCH CODES-BASED SECRET KEY RECONCILIATION (BR SCHEME)

To further increase the index-based key agreement probability $\mathcal{K}_{\mathcal{A}}$ between the legitimate nodes, BCH code-based reconciliation is applied. The (n, s, f) BCH code converts blocks of s message bits into n-bit codewords, where each codeword contains $(n - s)$ parity bits to correct up to f errors at the receiver. Alice divides her extracted secret key sequence into $\aleph = \lfloor \frac{\mathcal{L}_{\mathcal{K}}}{s} \rfloor$ message blocks, where a single block is denoted as $\mathbf{K}_{\aleph,s}^{\mathcal{A}}$. At the BCH encoder output, each $\mathbf{K}_{\aleph,s}^{\mathcal{A}}$ provides a BCH codeword $\mathbf{C}_{\aleph,n}^{\mathcal{A}} = [\mathbf{K}_{\aleph,s}^{\mathcal{A}} \mid \mathbf{P}_{\aleph,n-s}^{\mathcal{A}}]$, where $\mathbf{P}_{\aleph,n-s}^{\mathcal{A}}$ denotes the $(n - s)$ parity bits and $[\cdot|\cdot]$ represents concatenation of row vectors. For each $\mathbf{K}_{\aleph,s}^{\mathcal{A}}$, Alice sends the parity block $\mathbf{P}_{\aleph,n-s}$ to Bob. On the other side, Bob divides his sequence of secret key bits into $\aleph$ message blocks of s bits each and appends to them the corresponding received blocks of parity bits to generate $\aleph$ n-bit long codewords $\mathbf{C}_{\aleph,n}^{\mathcal{B}} = [\mathbf{K}_{\aleph,n}^{\mathcal{B}} \mid \mathbf{P}_{\aleph,n-s}^{\mathcal{A}}]$. Then Bob performs BCH decoding of these codewords to correct any discrepancies in his secret key sequence. From the decoded message bits the reconciled key $\mathbf{K}_{\aleph,s}^{\mathcal{B}'}$ is obtained, which is converted to the final key via P/S converter block. This procedure is illustrated in Fig. 5. The joint application of IR and BR schemes is referred to as IBR scheme.

The complete procedure for the proposed ACD-based SKG with M-level quantization is presented as Algorithm 2, which improves the SKG performance relative to the work of [12] as shown later in the numerical results section.

Algorithm 2 Proposed ACD-Based SKG With M-Level NUQ

Parameter Definition:
- Set M and k.
- Estimate c, ρ, β, Ω.

Channel Sample Measurement:
- Measure channel profiles $\mathcal{R}_{\mathcal{A}}$ and $\mathcal{R}_{\mathcal{B}}$ at Alice and Bob, respectively. Algorithm 1 may be used for simulations.

M-ACD-based NUQ:
- Compute bounding thresholds of $M - 1$ guard intervals by following the ACD-based NUQ strategy given in Sec.III-B2.
- Assign unique binary code to each quantization interval, e.g., by using Gray code.

Initial Key Generation:
- Set minimum excursion length to ACD floor (33), i.e, $L = \Psi$.
- Search $\mathcal{R}_{\mathcal{A}}$ and $\mathcal{R}_{\mathcal{B}}$ for qualifying excursions whose central indices are stored in $\nabla_{\mathcal{A}}$ and $\nabla_{\mathcal{B}}$, respectively.

Key Reconciliation:

Step 1 – IR:
- Alice sends $\nabla_{\mathcal{A}}$ to Bob who compares it with $\nabla_{\mathcal{B}}$ and records the matching indices in ∇.
- Bob extracts his secret keys from channel samples in $\mathcal{R}_{\mathcal{A}}$ indexed by ∇ and sends ∇ to Alice.
- Alice extracts her secret keys from channel samples in $\mathcal{R}_{\mathcal{A}}$ indexed by ∇.
- Alice and Bob store their initial secret keys as $\hat{\mathbf{K}}_{\mathcal{A}}$ and $\hat{\mathbf{K}}_{\mathcal{B}}$, respectively.

Step 2 – BR:
- Alice and Bob use the same BCH code of block-length n bits to convert their respective keys $\hat{\mathbf{K}}_{\mathcal{A}}$ and $\hat{\mathbf{K}}_{\mathcal{B}}$ into $\aleph$ message blocks each of length s bits, where $\aleph = \lfloor \frac{\mathcal{L}_{\mathcal{K}}}{s} \rfloor$.
- Alice inputs its $\aleph$ message blocks to a BCH encoder and the parity bits generated for each block are sent over the channel to Bob.
- Bob constructs $\aleph$ BCH codewords by concatenating the received parity bits with its own $\aleph$ message blocks.
- Bob inputs each of the $\aleph$ codewords to a BCH decoder and the corrected message bits from each decoded codeword are concatenated to form final secret key $\mathbf{K}_{\mathcal{B}}$, which is reconciled with the secret key of Alice.

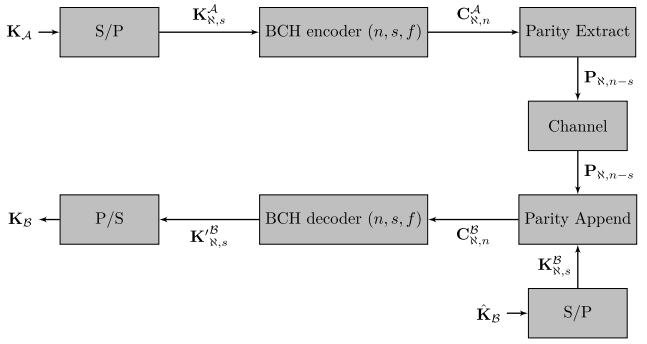


FIGURE 5. BCH Codes-based information reconciliation (BR).

In contrast with lossless quantization in which each channel sample is considered for SKG, the quantizer in Algorithm 2 is a lossy quantizer because every sample is not used for SKG. The benefit gained by this lossy quantization is an increased KAP. The loss incurred by algorithm 2 in terms of number of rejected samples can be further categorized as follows.

- *Guard-strip Loss* ($N^{\text{GS}}_{\text{Rj.}}$): A channel sample that falls inside a guard-strip at one legitimate node is not only itself rejected for SKG, but also its co-indexed sample at the other legitimate node gets rejected even though it may be in a quantization interval. The degree of reciprocity or correlation between observations by the legitimate nodes determines $N^{\text{GS}}_{\text{Rj.}}$, where a stronger correlation results in a smaller guard-strip interval z, and thus smaller $N^{\text{GS}}_{\text{Rj.}}$.
- *Mismatched Excursion Loss* ($N^{\text{MME}}_{\text{Rj.}}$)*:* The SKG algorithm requires that Alice and Bob measure identical lengths of the true excursion in the main channel. If a qualifying excursion is observed simultaneously by Alice and Bob but they both estimate different central index, then that complete excursion is rejected for SKG.
- *Matched Excursion Loss* ($N^{\text{ME}}_{\text{Rj.}}$)*:* Even for those qualifying excursions for which Alice and Bob correctly estimate an identical central index, only the channel sample at central index is used for SKG and all other samples in that qualifying excursion are discarded, i.e., only one sample in each qualifying excursion is used for SKG. For an L sample qualifying excursion accepted for key generation, L - 1 samples are discarded.
- *Invalid Excursion Loss* ($N^{\text{IVE}}_{\text{Rj.}}$)*:* The excursions whose length is $<$ L are rejected/invalid, see Fig. 4. Such excursions are not considered for SKG, therefore they contribute towards loss in KGR.

The *Cumulative Rejected Samples* (CRS) (or sample loss) can be expressed as

$$N^{\text{CRS}} = N^{\text{GS}}_{\text{Rj.}} + N^{\text{ME}}_{\text{Rj.}} + N^{\text{MME}}_{\text{Rj.}} + N^{\text{IVE}}_{\text{Rj.}}, \tag{50}$$

and *Cumulative Accepted Samples* (CAS) as $N^{\text{CAS}} = N - N^{\text{CRS}}$.

In the next section on numerical results, the SKG performance shall be evaluated in terms of KGR, KAP, and SKR, which are numerically defined below.

- *KGR* (in bits/channel sample) is the ratio between the number of extracted secret key bits and total number of channel samples N

$$\mathcal{K}_{\mathcal{G}} = \frac{\left(N - N^{\text{CRS}}\right)\log_2(M)}{N}. \tag{51}$$

The KGR can also be expressed as proportional to the ratio between the CAD and total observed channel envelope duration given in (36) and (38), respectively, as

$$\begin{aligned}\mathcal{K}_{\mathcal{G}} &\propto \frac{\tau^{\text{CAD}}}{\tau^{\text{total}}} \\ &= \mathcal{L}\,\frac{\tau^{\text{CAD}}}{\tau^{\text{total}}}\end{aligned} \tag{52}$$

where $\mathcal{L} < 1$ represents the cumulative loss in KGR imposed by samples rejection of SKG algorithm.

- *KAP* is the ratio between the number of matching key bits $\mathcal{N}_{\mathcal{M}}$ at the legitimate nodes and total length of secret key $\mathcal{L}_{\mathcal{K}}$

$$\mathcal{K}_{\mathcal{A}} = \frac{\mathcal{N}_{\mathcal{M}}}{\mathcal{L}_{\mathcal{K}}}. \tag{53}$$

- *SKR* is quantified in terms of the P-values obtained in different tests of the NIST test suite.

V. NUMERICAL RESULTS AND DISCUSSION

This section presents a comprehensive numerical analysis of the proposed ACD-based NUQ scheme for SKG. The impact of the important channel and algorithmic parameters on the performance of the proposed SKG scheme is intensively evaluated. For the conducted Monte Carlo simulations, 10^6 channel samples are randomly drawn from GG distribution for one legitimate link-end (say Alice) and the correlated channel samples of the other link-end (say Bob) are generated by exploiting Algorithm 1. Multilevel UQ, CDF-based NUQ, and AFD-based NUQ schemes are evaluated by employing the SKG scheme given in Algorithm 2. The number of quantization-levels M, their intervening guard-strips of intervals' z, and other important parameters are set differently for obtaining the different presented results, while the considered settings are explicitly stated in the caption of the corresponding figures. The $\mathcal{K}_{\mathcal{G}}$ and $\mathcal{K}_{\mathcal{A}}$ metrics (defined in the previous section) are studied to investigate the efficiency and robustness of the considered quantization schemes for SKG, while the NIST suite tests namely frequency test, block frequency test, run test, longest run-of-ones test, discrete Fourier transform test, Maurer's test, cumulative sum forward test, cumulative sum reversed test, and binary matrix rank test are employed to evaluate the SKR performance.

A. IMPACT OF CHANNEL PARAMETERS ON KGR

Fig. 6 shows the impact of change in the value of fading parameter β and minimum excursions' qualification

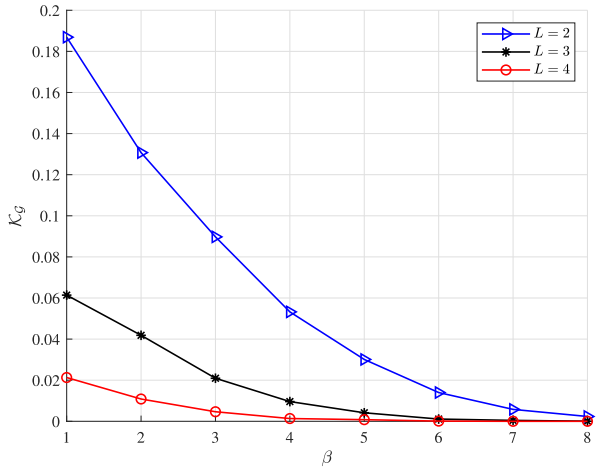


FIGURE 6. $\mathcal{K}_\mathcal{G}$ performance of ACD-NUQ against β for different values of L with $\rho = 0.9$, $M = 2$, $c = 1$, and $\Omega = 4$ with IR scheme.

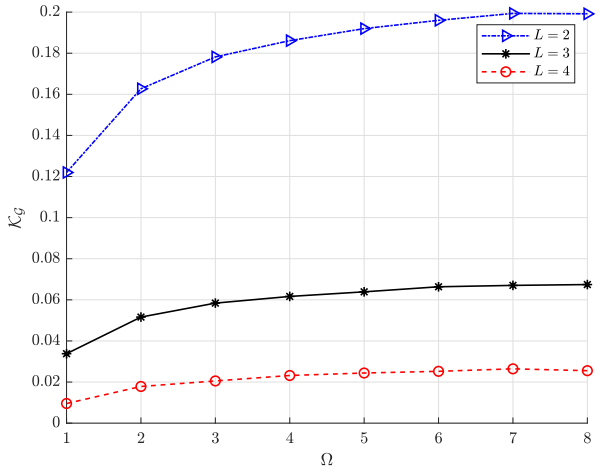


FIGURE 7. $\mathcal{K}_\mathcal{G}$ performance of ACD-NUQ against Ω for different values of L with $\rho = 0.9$, $M = 2$, $c = 1$, and $\beta = 1$ with IR scheme.

threshold L on the KGR $\mathcal{K}_\mathcal{G}$ performance of the proposed ACD-based NUQ scheme. The setting of different channel (i.e., c, ρ, and Ω etc.) and algorithm (e.g., M) parameters for obtaining this plot is given in the caption of the figure. A guard-strip of interval $z = \Omega/8$ is set and the proposed 2-ACD NUQ strategy is employed. As the value of β increases, the variance of the distribution, $(c/\Omega)^{-(2/\beta)}\left(\left(\Gamma(c)\Gamma(c+\frac{2}{\beta}) - \Gamma(c+\frac{1}{\beta})^2\right)\right)/\Gamma(c)^2$, reduces which leads to the increase in amount of rejected samples eventually causing reduction in $\mathcal{K}_\mathcal{G}$. Moreover, increase in L causes both $N_{\text{Rj.}}^{\text{ME}}$ and $N_{\text{Rj.}}^{\text{MME}}$ to increase which leads to reduction in $\mathcal{K}_\mathcal{G}$ performance.

The effect of change in Ω and L on $\mathcal{K}_\mathcal{G}$ performance by employing the proposed ACD-based quantization scheme is shown in Fig. 7. The channel (i.e., c, ρ, and β etc.) and algorithm parameters (i.e. M, and z) set to obtain this plot are indicated in the caption of the figure. The fixed guard-strip of interval $z = 0.5$ is set and 2-ACD quantization scheme is employed to obtain this plot. It can be observed that with the increase in Ω, the $\mathcal{K}_\mathcal{G}$ improves. This is because the increase in Ω effectively reduces the area of the guard-strip which causes reduction in $N_{\text{Rj.}}^{\text{GS}}$. Moreover, it can also be observed that a decrease in L increases the $\mathcal{K}_\mathcal{G}$ which is because of the reduced number of rejected samples or excursions.

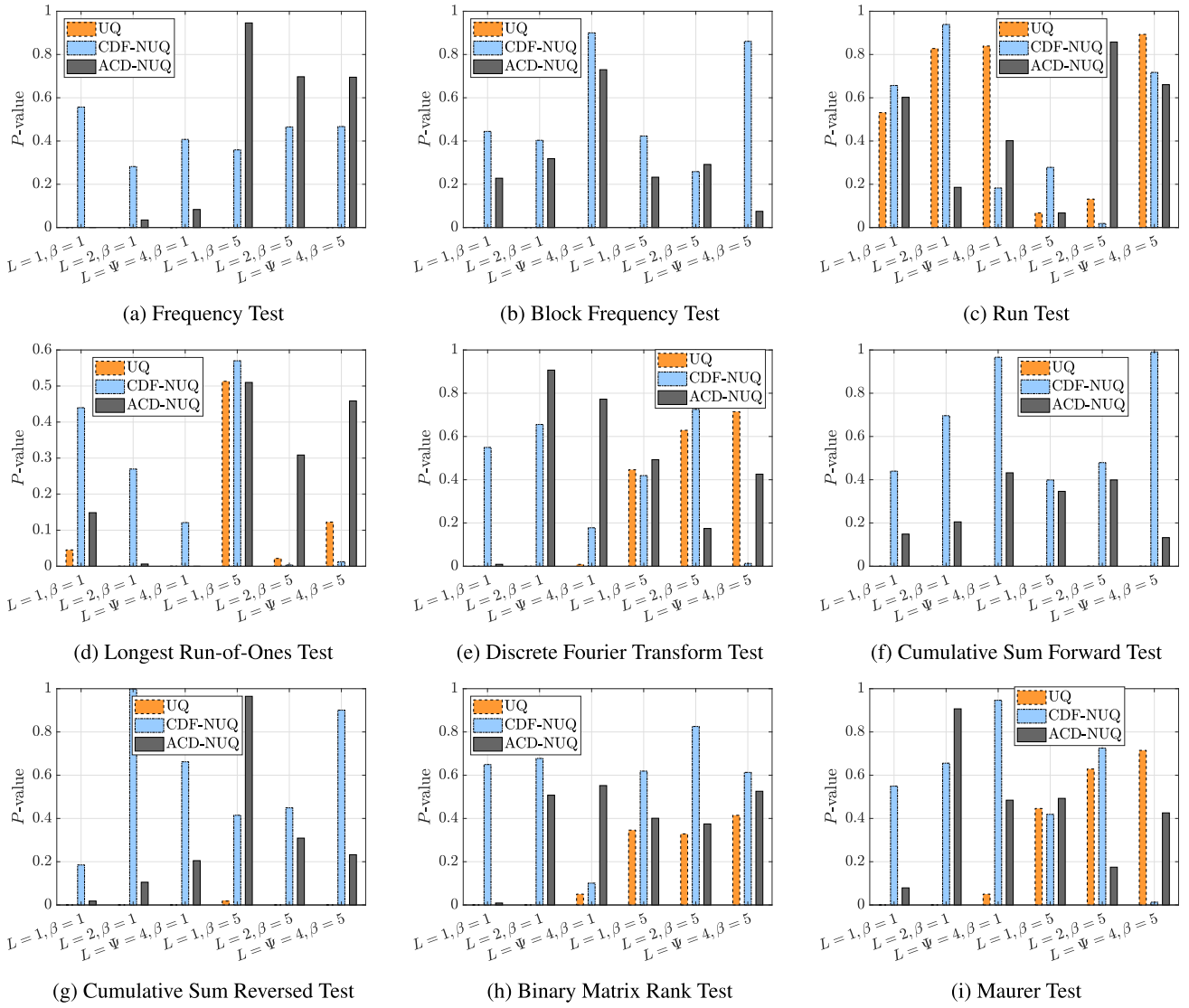
B. COMPARISON OF SKR PROPERTIES FOR UQ, CDF-BASED NUQ, AND ACD-BASED NUQ STRATEGIES

The randomness of the generated key bits is accessed by employing the NIST test suite. The test suite suggests 16 different tests which measure different behavioural aspects of a given sequence. Since some of the NIST tests require a large sample-size (e.g., $> 10^6$ samples), we have conducted 9 suitable tests namely frequency test, block frequency test, run test, longest run-of-ones test, discrete Fourier transform test, cumulative sum forward test, cumulative sum reversed test, binary matrix rank test, and Maurer test for studying the SKR of generated secret key bits, viz: Each test computes P-value, where P-value $\geq$ 0.01 is usually interpreted as a reasonably random sequence and the P-value $\leq$ 0.01 indicates a non-random sequence [32]. The outcome of these tests (i.e., in terms of P-value) is a function of both the channel and algorithm parameters. The impact of these parameters on the SKR for UQ, CDF-based NUQ, and ACD-based NUQ schemes is discussed in this section.

Fig. 8 (a)-(i) show the impact of β, c, and L on the SKR performance of UQ, CDF-NUQ, and ACD-NUQ for fixed value of z. The variance of the fading distribution reduces with the increase in β which also transforms the fading distribution from a non-symmetric to a symmetric distribution about the mean value μ. For the setting of $\beta = 1$ and $c = 1$ (which represents exponential distribution), the area under the distribution curve on both sides of μ becomes equal. For this setting, both the NUQ schemes (i.e., CDF- and ACD-based) outperform UQ in terms of SKR properties, particularly for the NIST tests which emphasise on the proportion of number of 0's and 1's in a given sequence. For a fixed value of c, as the value of β increases from 1 to 2 (i.e., fading typing converging to Rayleigh), the SKR performance of UQ and ACD-based NUQ schemes improves, see e.g., notable improvement in frequency, block frequency, cumulative sum forward, and cumulative sum reversed tests. The SKR performance of CDF-based NUQ is only marginally influenced by the channel parameters, i.e., the CDF-based NUQ performs robustly under different channel conditions as long as the channel samples strictly follow the assumed underlying distribution type. In all the conducted tests, the SKR performance of both ACD-based and CDF-based NUQ schemes is superior to that of UQ. Furthermore, the SKR performance of ACD-based NUQ can be regarded as comparable to that of CDF-based NUQ.

C. PERFORMANCE TRADE-OFF BETWEEN KGR $\mathcal{K}_\mathcal{G}$ AND KAP $\mathcal{K}_\mathcal{A}$ FOR BOTH CDF- AND ACD-BASED NUQ

The trade-off between KGR and KAP is critical in evaluating the performance of SKG algorithms. In Fig. 9 (a)-(c),

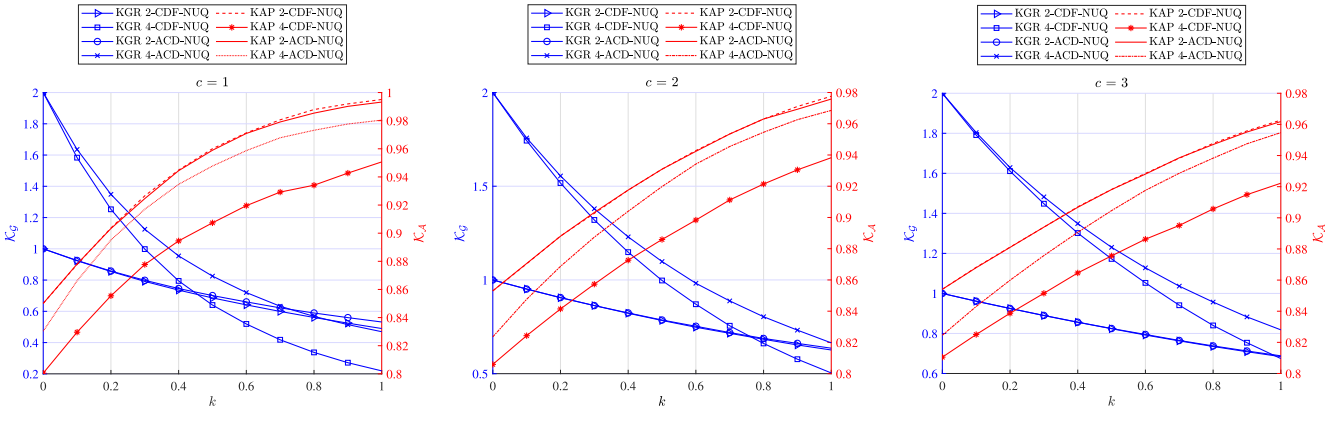


(a) Frequency Test (b) Block Frequency Test (c) Run Test

(d) Longest Run-of-Ones Test (e) Discrete Fourier Transform Test (f) Cumulative Sum Forward Test

(g) Cumulative Sum Reversed Test (h) Binary Matrix Rank Test (i) Maurer Test

FIGURE 8. SKR performance (i.e., quantified by the NIST tests) of UQ, CDF-NUQ, and ACD-NUQ for different value of L, β, and $c = 1$ with IR scheme.



(a) (b) (c)

FIGURE 9. $\mathcal{K}_{\mathcal{G}}$ and $\mathcal{K}_{\mathcal{A}}$ performance of 2-, 4-CDF-NUQ and 2-, 4-ACD-NUQ for increasing guard-strip interval via control parameter k and different values of c. Other parameter values are: $\rho = 0.9$, $L = 1$, $\Omega = 4$, and $\beta = 1$ with IR scheme.

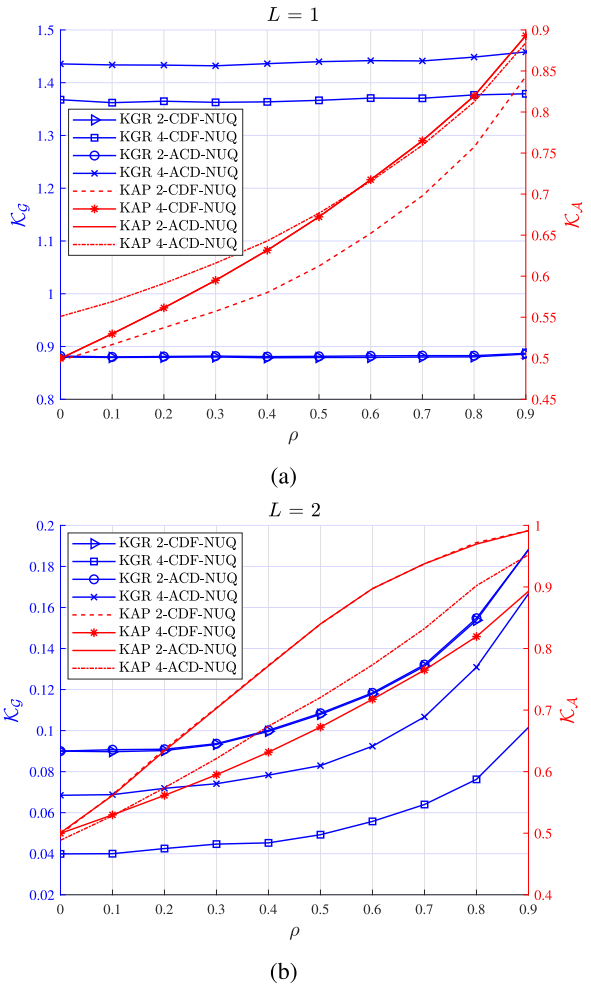


FIGURE 10. $\mathcal{K}_\mathcal{G}$ and $\mathcal{K}_\mathcal{A}$ performance of 2-, 4-CDF-NUQ and 2-, 4-ACD-NUQ for increasing ρ and different values of L. Other parameter values are: $\Omega = 4$, $c = 1$, and $\beta = 1$ with IR scheme.

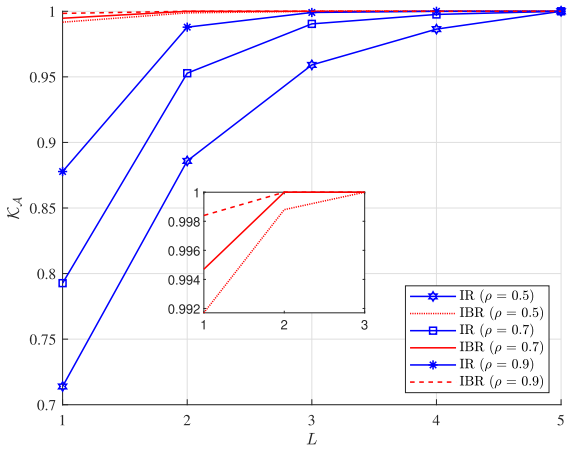


FIGURE 11. $\mathcal{K}_\mathcal{A}$ performance of IR and IBR (i.e., combined IR and BR) for increasing values of L; Other algorithm parameters are: $\beta = 1$, $z = \sigma/10$, $c = 1$, $\Omega = 4$, and different values of ρ.

both the KGR $\mathcal{K}_\mathcal{G}$ and KAP $\mathcal{K}_\mathcal{A}$ are plotted to evaluate the proposed M-ACD NUQ strategy. The impact of change in the guard-strip interval (i.e., controlled by k) and change in c for 2- and 4-level CDF-based and ACD-based NUQ schemes is studied. The $\mathcal{K}_\mathcal{G}$ performance of both the CDF-based and ACD-based NUQ schemes degrades with the increase in k, while on the other hand the $\mathcal{K}_\mathcal{A}$ improves. This is due to increased $N_{\text{Rj.}}^{\text{GS}}$ and reduced likelihood of mismatches around a widening guard-strip. For different values of k, the $\mathcal{K}_\mathcal{G}$ and $\mathcal{K}_\mathcal{A}$ performance of 2-level CDF-based and ACD-based NUQ schemes can be observed as comparable. However, for 4-level quantization strategy, the ACD-based NUQ provides better performance trade-off between $\mathcal{K}_\mathcal{G}$ and $\mathcal{K}_\mathcal{A}$ compared to CDF-based NUQ. This is because the ACD-based NUQ incurs less $N_{\text{Rj.}}^{\text{ME}}$ and $N_{\text{Rj.}}^{\text{MME}}$ compared to CDF-based NUQ for 4-level quantization strategy. Furthermore, the converse comparative performance trend between {2- and 4-level} CDF-based NUQ and {2- and 4-level} ACD-based NUQ can be observed for high values of k. This trend suggests that for the channel conditions represented by high normalized channel variance (i.e., smaller value of c), a low-level (e.g., 2-level) quantization strategy may be preferable over high-level (e.g., 4-level) quantization strategy for all acceptable settings of k.

The impact of correlation coefficient ρ on $\mathcal{K}_\mathcal{G}$ and $\mathcal{K}_\mathcal{A}$ performance is shown in Fig. 10 (a)-(b) for fixed guard-strip interval. Along the increase in ρ from 0 to 1, both $\mathcal{K}_\mathcal{G}$ and $\mathcal{K}_\mathcal{A}$ performance improves, that is because high values of ρ ensure the channel reciprocity assumption.

The grade of improvement offered in terms of KAP performance by the two considered key reconciliation schemes (i.e., IR and IBR), the $\mathcal{K}_\mathcal{A}$ performance is compared in Fig. 11 for different settings of ρ. For both the IR and IBR schemes, as the value of L and ρ increases, the $\mathcal{K}_\mathcal{A}$ performance improves. For different settings of ρ and L, IBR scheme is observed to provide best KAP performance than that provided by IR scheme alone, which is because IBR performs an additional step of key reconciliation which also has an associated cost of required computational complexity.

Determining the optimal value for the minimum excursions qualification threshold L is critical to enhance the overall performance trade-off between $\mathcal{K}_\mathcal{G}$ and $\mathcal{K}_\mathcal{A}$. In this context, the impact of variations in L for different settings of guard-strip interval k on the performance trade-off between $\mathcal{K}_\mathcal{G}$ and $\mathcal{K}_\mathcal{A}$ for 2- and 4-level CDF-based and ACD-based NUQ is shown in the Fig. 12 (a)-(c). The overall $\mathcal{K}_\mathcal{G}$ performance for ACD-based NUQ can be observed better than that offered by CDF-based NUQ. In Fig. 12 (c) corresponding to $L = 4$, the SKG algorithm delivers high $\mathcal{K}_\mathcal{A}$ performance, i.e., key matching stays between 99 and 100% for different quantization schemes and for increasing value of the guard-strip interval k.

Increase in L causes improvement in $\mathcal{K}_\mathcal{A}$ performance and degradation in $\mathcal{K}_\mathcal{G}$ performance, so the optimal setting of L in practical scenarios is critical to achieve a good performance trade-off between $\mathcal{K}_\mathcal{G}$ and $\mathcal{K}_\mathcal{A}$. From the on going analysis, it can be established that by setting $L = 4$, i.e., as equal to the ACD-floor level $L = \text{floor}(\Psi)$, the optimal performance

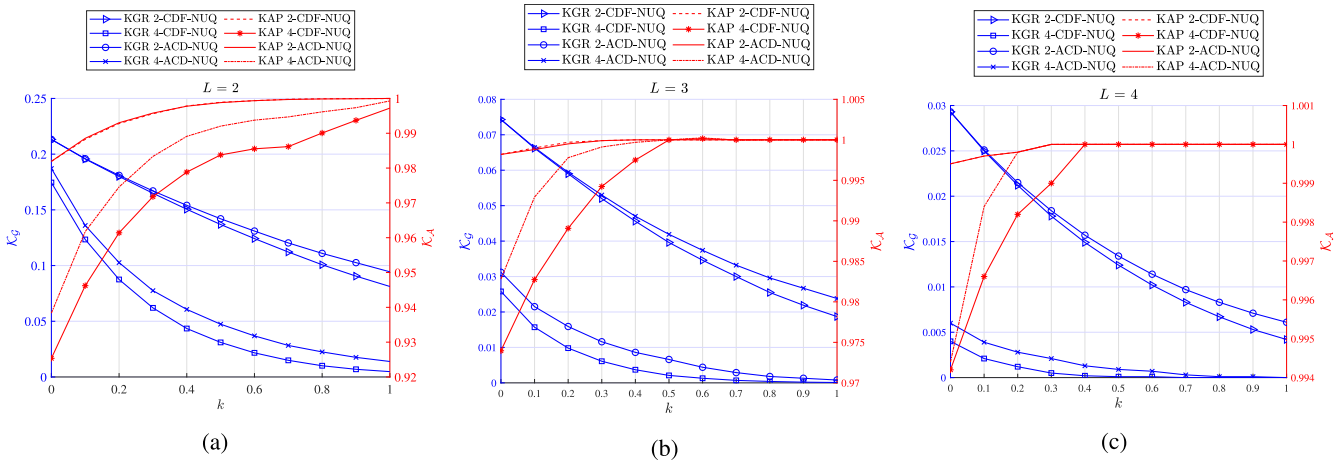


FIGURE 12. $\mathcal{K}_{\mathcal{G}}$ and $\mathcal{K}_{\mathcal{A}}$ performance of 2-, 4-CDF-NUQ and 2-, 4-ACD-NUQ for increasing guard-strip interval via control parameter k and different values of L. Other parameter values are: $\rho = 0.9$, $\Omega = 4$, $c = 1$, and $\beta = 1$ with IR scheme.

trade-off between $\mathcal{K}_{\mathcal{G}}$ and $\mathcal{K}_{\mathcal{A}}$ can be achieved. The proposed M-level ACD-based quantization scheme can be deduced to represent the 2-level AFD-based quantization scheme proposed in [21] by substituting $M = 2$.

VI. CONCLUSION

In this paper, first, a closed-form expression of ACD for GG fading channels has been derived. Next, an ACD-based multi-level NUQ scheme for SKG in GG fading conditions has been proposed. The proposed quantization scheme has been employed with a notable SKG algorithm and performance analysis in terms of KGR, KAP, and SKR metrics has been conducted. Furthermore, a comprehensive comparative analysis of the proposed ACD-based NUQ scheme with conventional UQ and CDF-based NUQ schemes has been conducted. It has been established that ACD-based NUQ delivers a superior performance trade-off between KGR and KAP compared to both the UQ and CDF-based NUQ. Besides, it outperforms UQ and provides comparable performance to that of CDF-based NUQ in terms of SKR properties. This performance gain has been achieved by assuring a matching likelihood of samples falling in each quantization interval and an equal number of contiguous samples falling in each quantization interval.

REFERENCES

[1] S. J. Nawaz, S. K. Sharma, S. Wyne, M. N. Patwary, and M. Asaduzzaman, "Quantum machine learning for 6G communication networks: State-of-the-art and vision for the future," *IEEE Access*, vol. 7, pp. 46317–46350, 2019.

[2] S. J. Nawaz, S. K. Sharma, B. Mansoor, M. N. Patwary, and N. M. Khan, "Non-coherent and backscatter communications: Enabling ultra-massive connectivity in 6G wireless networks," *IEEE Access*, vol. 9, pp. 38144–38186, 2021.

[3] X. Sun, D. W. K. Ng, Z. Ding, Y. Xu, and Z. Zhong, "Physical layer security in UAV systems: Challenges and opportunities," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 40–47, Oct. 2019.

[4] Q. Wu, W. Mei, and R. Zhang, "Safeguarding wireless network with UAVs: A physical layer security perspective," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 12–18, Oct. 2019.

[5] R. Chen, C. Li, S. Yan, R. Malaney, and J. Yuan, "Physical layer security for ultra-reliable and low-latency communications," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 6–11, Oct. 2019.

[6] X. Lu, J. Lei, Y. Shi, and W. Li, "Intelligent reflecting surface assisted secret key generation," *IEEE Signal Process. Lett.*, vol. 28, pp. 1036–1040, 2021, doi: 10.1109/LSP.2021.3061301.

[7] F. Jameel, S. Wyne, S. J. Nawaz, J. Ahmed, and K. Cumanan, "On the secrecy performance of SWIPT receiver architectures with multiple eavesdroppers," *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1–12, Jun. 2018.

[8] O. Hayat, R. Ngah, Z. Kaleem, S. Z. M. Hashim, and J. J. Rodrigues, "A survey on security and privacy challenges in device discovery for next-generation systems," *IEEE Access*, vol. 8, pp. 84584–84603, 2020.

[9] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Commun.*, vol. 18, no. 4, pp. 6–12, Aug. 2011.

[10] M. Adil, S. Wyne, and S. J. Nawaz, "On quantization for secret key generation from wireless channel samples," *IEEE Access*, vol. 9, pp. 21653–21668, 2021.

[11] S. N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "Secret key extraction from wireless signal strength in real environments," *IEEE Trans. Mobile Comput.*, vol. 12, no. 5, pp. 917–930, May 2013.

[12] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 2, pp. 240–254, Jun. 2010.

[13] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[14] S. J. Nawaz, M. Adil, and S. Wyne, "Average contiguous duration—A novel metric for characterizing wireless fading channels," *IEEE Wireless Commun. Lett.*, early access, May 14, 2021, doi: 10.1109/LWC.2021.3080434.

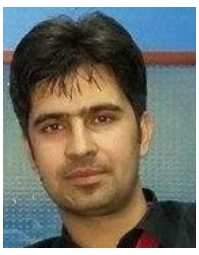
[15] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *IEEE Trans. Antennas Propag.*, vol. 53, no. 11, pp. 3776–3784, Nov. 2005.

[16] A. Sayeed and A. Perrig, "Secure wireless communications: Secret keys through multipath," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process.*, Mar. 2008, pp. 3013–3016.

[17] J. W. Wallace and R. K. Sharma, "Automatic secret keys from reciprocal MIMO wireless channels: Measurement and analysis," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 3, pp. 381–392, Sep. 2010.

[18] Y.-W.-P. Hong, L.-M. Huang, and H.-T. Li, "Vector quantization and clustered key mapping for channel-based secret key generation," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 5, pp. 1170–1181, May 2017.

[19] A. Soni, R. Upadhyay, and A. Kumar, "Wireless physical layer key generation with improved bit disagreement for the Internet of Things using moving window averaging," *Phys. Commun.*, vol. 33, pp. 249–258, Apr. 2019.
[20] H. Jin, K. Huang, S. Xiao, Y. Lou, X. Xu, and Y. Chen, "A two-layer secure quantization algorithm for secret key generation with correlated eavesdropping channel," *IEEE Access*, vol. 7, pp. 26480–26487, 2019.
[21] M. Bottarelli, P. Karadimas, G. Epiphaniou, D. K. B. Ismail, and C. Maple, "Adaptive and optimum secret key establishment for secure vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 70, no. 3, pp. 2310–2321, Mar. 2021.
[22] X. Zhang, G. Li, J. Zhang, A. Hu, Z. Hou, and B. Xiao, "Deep learning-based physical-layer secret key generation for FDD systems," 2021, *arXiv:2105.08364*. [Online]. Available: http://arxiv.org/abs/2105.08364
[23] E. W. Stacy, "A generalization of the gamma distribution," *Ann. Math. Statist.*, vol. 33, no. 3, pp. 1187–1192, Sep. 1962.
[24] H. Lei, C. Gao, Y. Guo, and G. Pan, "On physical layer security over generalized gamma fading channels," *IEEE Commun. Lett.*, vol. 19, no. 7, pp. 1257–1260, Jul. 2015.
[25] S. Primak and V. Kontorovich, "On the second order statistics of generalized gamma process," *IEEE Trans. Commun.*, vol. 57, no. 4, pp. 910–914, Apr. 2009.
[26] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS)*, 2007, pp. 401–410.
[27] X. Li, J. Liu, Q. Yao, and J. Ma, "Efficient and consistent key extraction based on received signal strength for vehicular ad hoc networks," *IEEE Access*, vol. 5, pp. 5281–5291, 2017.
[28] C. Chen and M. A. Jensen, "Secret key establishment using temporally and spatially correlated wireless channel coefficients," *IEEE Trans. Mobile Comput.*, vol. 10, no. 2, pp. 205–215, Feb. 2011.
[29] M. D. Yacoub, "The α-μ distribution: A physical fading model for the stacy distribution," *IEEE Trans. Veh. Technol.*, vol. 56, no. 1, pp. 27–34, Jan. 2007.
[30] G. E. Andrews, R. Askey, and R. Roy, *Special Functions*. Cambridge, U.K.: Cambridge Univ. Press, 1999.
[31] J. G. Proakis and M. Salehi, *Digital Communications*, 5th ed. New York, NY, USA: McGraw-Hill, 2007.
[32] L. E. Bassham, III, A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, E. B. Barker, S. D. Leigh, M. Levenson, M. Vangel, and D. L. Banks, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. Sp 800-22 Rev. 1a, 2010.
[33] Y. Wu, Y. Yu, Y. Hu, Y. Sun, T. Wang, and Q. Zhang, "Channel-based dynamic key generation for physical layer security in OFDM-PON systems," *IEEE Photon. J.*, vol. 13, no. 2, pp. 1–9, Apr. 2021.



MUHAMMAD ADIL received the master's degree in electrical engineering from the Department of Electrical and Computer Engineering, COMSATS University Islamabad (CUI), Islamabad, Pakistan, in 2016, where he is currently pursuing the Ph.D. degree. His current research interests include information theory and physical layer security, optimization in wireless communications, the Internet of Things (IoT), and 5G communications.

SHURJEEL WYNE (Senior Member, IEEE) received the Ph.D. degree from Lund University, Sweden, in March 2009. From April 2009 to April 2010, he was a Postdoctoral Research Fellow with the High-Speed Wireless Center, Lund University. Since June 2010, he has been with the Department of Electrical Engineering, COMSATS University Islamabad (CUI), Islamabad, Pakistan, where he serves as an Associate Professor. His research interests include wireless channel characterization, multi-antenna systems, cooperative communications, physical layer security, and vehicular communications. He was a co-recipient of the Best Paper Award of the antennas and propagation track from the IEEE VTC2013-Spring.

SYED JUNAID NAWAZ (Senior Member, IEEE) received the Ph.D. degree in electronic engineering from Mohammad Ali Jinnah University, Islamabad, in February 2012. Since September 2005, he has been working on several research and teaching positions with COMSATS University Islamabad (CUI), Islamabad, Pakistan, Staffordshire University, U.K., Federal Urdu University, Pakistan, University of York, U.K., and Aristotle University of Thessaloniki, Greece. Since 2012, he has also been working as an Assistant Professor with the Department of Electrical and Computer Engineering, COMSATS University Islamabad (CUI). His current research interests include physical channel modeling, channel estimation and characterization, massive MIMO systems, adaptive signal processing, machine learning, compressed sensing, mm-wave channels, airborne internet, underwater communications, the Internet of Things, and vehicle-to-vehicle communications.

BILAL MUHAMMAD received the master's degree in electrical engineering from Blekinge Tekniska Högskola (BTH), Sweden, in 2008, and the Ph.D. degree in telecommunication engineering from the University of Rome Tor Vergata, Italy, in 2015. He is currently working as an Assistant Professor with the Department of Business Development and Technology, Aarhus University. He is actively participates in EU projects. He has been the WP Leader of SARA and EASY-PV H2020 Innovation Action projects. His research interests include UAV wireless communication for 5G and beyond, GNSS integrity and accuracy for UAV, unmanned traffic management (UTM) systems and services, and UAV business modeling.