IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 9 May 2024, accepted 5 June 2024, date of publication 10 June 2024, date of current version 19 June 2024.

*Digital Object Identifier 10.1109/ACCESS.2024.3411556*

RESEARCH ARTICLE

# New Dimensions for Physical Layer Secret Key Generation: Excursion Lengths-Based Key Generation

**MUHAMMAD ADIL[1], HABIB ULLAH KHAN[2], MOHAMMAD ARIF[3], MIAN SHAH NAWAZ[1], AND FAHEEM KHAN[3]**

[1]Department of Technology, Abasyn University, Peshawar 25000, Pakistan
[2]Department of Accounting and Information Systems, College of Business and Economics, Qatar University, Doha, Qatar
[3]Department of Computer Engineering, Gachon University, Seongnam-si 13120, South Korea

Corresponding authors: Faheem Khan (faheem@gachon.ac.kr) and Habib Ullah Khan (habib.khan@qu.edu.qa)

This work was supported by Qatar National Library in collaboration with Qatar University under Grant QUHI-CBE-21/22-1.

**ABSTRACT** Physical Layer-based Secret Key Generation (PLSKG) between the legitimate nodes from the reciprocal wireless channel is a vastly studied area of Physical Layer Security (PLS). PLSKG aims to secure the wireless link between the legitimate nodes by symmetrically encrypting the wirelessly transmitted information via a secret key that is extracted from the common randomness of the stochastic wireless channel. PLSKG encompasses the intermediate steps of channel sampling, quantization, information reconciliation, and privacy amplification. The PLSKG algorithms are evaluated in terms of quantifiers such as Key Generation Rate (KGR), Key Agreement Probability (KAP), and randomness. The practical PLSKG algorithms (level-crossing algorithms) extract a secret key by analyzing the channel samples and assigning bit sequences to the channel samples lying in different quantization regions. Level-crossing algorithms are lossy and extract a secret key from the central samples of matched excursions between the legitimate nodes. This results in a reduced KGR as there is a scarcity of such matched excursions considering the fast variations of the wireless link between the legitimate nodes. This paper proposes a Two-Round Channel Parsing (TRCP) algorithm that exploits the correlation between the excursion lengths of the channel samples in addition to the sample correlation. TRCP effectively utilize the channel samples by reducing the sample losses incurred by lossy quantizers exploring a new dimension of correlated excursions of the channel samples between legitimate nodes. Simulation results demonstrate that the proposed TRCP scheme enhances the KGR and KAP performance of the secret key and also passes the National Institute of Standards and Technology (NIST) test suite of randomness.

**INDEX TERMS** Secret key generation, stochastic wireless channel, quantization regions, excursions.

## I. INTRODUCTION

Wireless communication has seen tremendous growth in the last few decades as the 5$^{th}$ Generation (5G) of wireless communications is standardized. Research interest has currently shifted to the 6$^{th}$ Generation (6G) wireless communication which is expected to be hyper-connected (i.e., with no restrictions on data rate, coverage, and computing) via the unification of Artificial Intelligence (AI), Machine Learning (ML), and Virtual Reality (VR) [1], [2]. The 6G of wireless communications, which is now being researched by scientific organizations at commercial and educational centers, is going to advance in a couple of directions: bands with higher frequencies (sub-THz), a greater number of transmitting and receiving antennas (extreme MIMO), and user devices (massive enhancement in the multiple access), and facilitate learning techniques dispersed across every device in the system's infrastructure, involving cutting-edge

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

and user devices. These innovations will enable clients and commercial users to send and receive data at larger speeds, improved reliability, and with a shorter delay [3], [4]. With the exponential increase in both the number of connected devices and data rates, the AI-enabled 6G is expected to suffer from privacy and security challenges [5], [6], [7].

Physical Layer Security (PLS) is proving a promising candidate to provide information security, particularly in scenarios where devices connect on the fly without having an installed infrastructure [8], [9]. PLS can provide services such as information-theoretic security with lightweight coding and can serve as an extra layer of security complementing traditional computational security [10]. The major physical research challenges and issues addressed for 6G and the strategy to overcome those challenges by proposing viable security solutions are presented in [4] and [11]. Moreover, key performance indicators for 6G PLS as well as a preliminary threat picture based on the anticipated PLS network architecture are presented in [12]. Specifically, security solutions addressed for visible light communication, Terahertz (THz) bands, quantum computing, distributed AI, and distributed ledger technologies are analyzed. Furthermore, a comprehensive analysis of issues related to privacy and security in light of key generation technologies to enhance PLS and cutting-edge measures to mitigate the current privacy framework shortcomings are studied in [13].

Physical Layer-based Secret Key Generation (PLSKG) is a PLS technique that exploits the reciprocal[1] stochastic wireless channel variation of the main channel (i.e., the channel between legitimate nodes (e.g., Alice and Bob)) for generating a shared secret key between the respective legitimate nodes [14]. The eavesdropping node (i.e., Eve) overhears the communication via the Eve channel (i.e., the channel between legitimate nodes and Eve). Eve has knowledge of the PLSKG algorithm but the Eve channel is sufficiently decorrelated to the main channel and cannot extract the same key as that of legitimate nodes as long as Eve is spatially separated from the legitimate nodes [15].

PLSKG begins with channel sampling where the legitimate nodes take turns sending probing signals and measuring the corresponding channel response. Channel sampling is followed by quantization where the legitimate nodes divide the channel range into quantization regions so that bit sequences can be assigned to channel samples lying in different quantization regions. Quantization is followed by information reconciliation where the legitimate nodes exchange messages to reduce the discrepancies of their channel samples. Cascade protocol [16] or polar codes-based blind information reconciliation [17] are two of the many schemes that can be used for this purpose. Information reconciliation is followed by privacy amplification where the legitimate nodes randomize the secret key from the perspective of the Eve [18].

[1] In the absence of noise and interference, the wireless propagation channel from Alice to Bob is the same as from Bob to Alice in a Time Division Duplex (TDD) setup.

### A. RELEVANT WORK

PLSKG exploits the correlated stochastic channel variations of the reciprocal main channel for generating a secret key. PLSKG algorithms employ quantizer designs that divide the channel range (i.e., maximum channel value minus minimum channel value) into quantization regions for assigning bit sequences to channel samples lying in those quantization regions. The quantizers are either 2-level, multi-level (i.e., $4, 8, 16, \cdots$), uniform, or non-uniform. In uniform quantizers, the span (i.e., sub-range of channel envelope values) of each quantization region is equal. In non-uniform quantizers, the channel range is divided based on the probability of channel samples falling in different quantization regions (i.e., the span for each quantization region is set so as to make the probability of a sample falling in each quantization region equal). Further, PLSKG algorithms exploit the stochastic channel variations in the time domain by using the Channel Impulse Response (CIR), Received Signal Strength (RSS), channel envelope, phase, and Angle of Arrival (AoA)/Angle of Departure (AoD) or the frequency domain by exploiting the Channel Frequency Response (CFR). PLSKG algorithms are evaluated in terms of metrics namely Key Generation Rate (KGR), Key Agreement Probability (KAP), and randomness assessed via the National Institute of Standards and Technology (NIST) test suite. Each PLSKG scheme tends to improve the tradeoff between KGR, KAP, and the randomness of the generated secret key. A brief discussion of relevant PLSKG algorithms is given below.

In [19], a PLSKG scheme was proposed that exploited the CIR for secret key generation. The channel samples excursions (i.e., consecutive samples falling in a given quantization region) were used for SKG instead of individual samples with the intent to increase the KAP performance of the PLSKG. This, however, resulted in a reduced KGR due to the loss of samples in the PLSKG process. An Adaptive Secret Bit Generation (ASBG) was proposed in [20] to overcome the loss of channel samples and to modify the quantizer design for the varying channel conditions. This resulted in enhanced KGR at the cost of reduced KAP. A similar algorithm was proposed for Multi-Input-Multi-Output (MIMO) channels in [21]. A vector quantization-based PLSKG algorithm was proposed in [22] to increase KGR at the cost of reduced secret key randomness. The channel phase information was exploited using a Two-Layer Secure (TLS) PLSKG scheme in [23] to enhance the KGR performance. To improve the randomness performance of the PLSKG, a multi-level non-uniform quantization strategy was proposed for the Generalized Gamma (GG) fading channels in [24]. The randomness performance was improved but the KGR and KAP remained comparable to other schemes. For the Rayleigh, Rice, and Nakagami Fading channel, a 2-level PLSKG scheme was suggested in [25] that derived analytical

expressions of the Average Contiguous Duration (ACD) (i.e., average excursion length) of the channel envelope residing in a given quantization region. This has improved KGR and randomness with a reduction in KAP performance. The Secret Key Capacity (SKC) for Intelligent Reflecting Surface (IRS)-assisted systems was investigated in [26]. PLSKG algorithms suffer from low KGR when the channel is slow-varying. In [27], the IRS units were deployed for the injection of discrete phase information to enhance the PLSKG performance. To assist multiple Internet-of-Things (IoT) devices by sharing a similar key, a group secret key generation strategy was proposed in [28]. In [29], the SKC for in-band full-duplex (IBFD) MIMO systems was investigated.

All the above-mentioned contributions enhance the tradeoff between KGR, KAP, and randomness. Nevertheless, there exists a wide research scope to thoroughly investigate PLSKG schemes for further enhancing the tradeoff. A summary of different level-crossing-based PLSKG schemes is given in Table 1.

PLSKG exploits the temporal stochastic variations of the reciprocal main channel between the legitimate nodes. For a highly varying stochastic channel and spatial separation of the order of half the wavelength, the eavesdropper channel is considered decorrelated with the main channel (i.e., the mutual information between the main and Eve's channel approaches 0) [15]. This fundamental assumption is also exploited by the link signature-based security mechanisms [30]. For the PLSKG, it allows the legitimate nodes to exploit the main channel as a source of common randomness for extracting a matched secret key. In order to enhance the performance tradeoff between KGR, KAP and the randomness properties, recent studies have explored new dimensions for PLSKG [31].

**TABLE 1. PLSKG schemes from wireless channel samples.**

| Research Publication with Year | Channel Model | Channel Parameter | Technique and Explaination |
|---|---|---|---|
| [19], 2010 | Rayleigh | CIR | Analytical, Measurement-based, uses uniform quantization |
| [21], 2010 | Rayleigh | CIR | Analytical, Measurement-based, exploits CDF for quantization |
| [20], 2014 | RSS | RSS measurements | Measurement-based uniform quantization |
| [32], 2017 | Measurement-based | RSS | Vector quantization |
| [33], 2019 | Measurement-based | RSS | Uniform quantization with moving windows averaging |
| [23], 2019 | Simulation-based | Phase | Analytical and two-layer quantization |
| [24], 2021 | Nakagami-$m$ | RSS | Analytical, used multi-level CDF-based non-uniform quantization |
| [34], 2021 | Rayleigh | Envelope | Analytical CDF-based 2-level non-uniform quantization |
| [25], 2021 | Rayleigh, Rice, Nakagami-$m$ | Envelope | Analytical, proposed ACD as a new quantifier for PLSKG quantization |
| [35], 2021 | Gaussian | CFR | Deep learning-based quantization |
| [36], 2021 | Generalized Gamma | Envelope | Analytical, CDF-based multi-level non-uniform quantization |
| **Proposed TRCP** | **Generalized Gamma** | **Envelope** | **A Two-Round Channel Parsing algorithm** |

### B. CONTRIBUTIONS AND PAPER ORGANIZATION

This work proposes a Two-Round Channel Parsing (TRCP) PLSKG scheme that exploits the reciprocity in both channel samples and full excursion lengths of the stochastic variations of the wireless propagation channel. The key contributions are listed as follows.

- Wireless channel samples are generated from the GG fading channels for the legitimate nodes. The GG fading can model Rayleigh, Nakagami-$m$, Weibull, exponential, and many other channel distributions as its special cases.
- An improved TRCP PLSKG algorithm is proposed that exploits the new dimension of correlation in full excursion lengths for SKG in addition to the correlation in channel samples to enhance the KGR and KAP of the generated secret key.
- A comprehensive comparison of the proposed TRCP scheme with notable PLSKG schemes in terms of KGR and KAP is conducted.
- TRCP algorithm exploits the channel samples in two rounds. For the second round of TRCP, a coding strategy is proposed that ensures the randomness of the key so that the resulting key passes the NIST test suite.
- TRCP enhances the KGR and KAP of the secret key compared with other multi-level PLSKG schemes which not only have less advantage in terms of KGR but also suffer KAP performance degradation.

The rest of this paper is organized as follows. Section II describes the system and channel model for the proposed TRCP PLSKG scheme. Section III discusses the proposed TRCP scheme in detail. Section IV provides detailed numerical results and evaluates TRCP algorithm in terms of different performance metrics and also compares TRCP

**TABLE 2.** Mathematical notational conventions.

| Notation | Definition |
|---|---|
| $h_{(\cdot)}$ | GG fading channel at the respective nodes |
| $p(x)$ | PDF of random variable $x$ |
| $F(x)$ | CDF of random variable $x$ |
| $\rho$ | Correlation coefficient between Alice and Bob's channels |
| $f_m$ | Maximum doppler shift |
| $\mathcal{G}$ | Guard-band |
| $z$ | Guard-band width |
| $q^+$ | The upper threshold of the guard-band |
| $q^-$ | The lower threshold of the guard-band |
| $\mathcal{Q}_i$ | $i^{th}$ quantization region where $i \in \{1, 2\}$ |
| $\Xi_x^y$ | ACD between two thresholds $x$ and $y$ |
| $\mathbf{V}_{(\cdot)}$ | Channel samples array at the respective node |
| $\aleph$ | Total number of channel samples |
| $\mathbf{E}_{(\cdot)}$ | The array of central indices at the respective nodes |
| $\mathbf{F}_{(\cdot)}$ | The matrix of full excursion lengths with central indices at the respective node |
| $L$ | Minimum excursion length for a qualifying excursion |
| $\mathcal{K}_\mathcal{G}$ | Key Generation Rate |
| $\mathcal{K}_\mathcal{A}$ | Key Agreement Probability |
| $\mathfrak{B}_\mathfrak{g}$ | Total number of secret key bits generated |
| $\aleph_b$ | Total number of secret key bits in agreement between the legitimate nodes |
| $\ell_x$ | Full excursion of length $x$ |
| $\mathbf{K}^1{}_{(\cdot)}$ | 1st round key at the respective node |
| $\mathbf{K}^2{}_{(\cdot)}$ | 2nd round key at the respective node |
| $\mathbf{K}_{(\cdot)}$ | Final key at the respective node |
| $p$-value | A value that indicates the strength of the evidence for the null hypothesis |

with other notable schemes. Finally, Section V presents the conclusions.

Notational conventions are given in Table 2.

## II. SYSTEM MODEL

Consider the wireless communication scenario depicted in Fig. 1, where Alice and Bob are the two legitimate nodes who want to communicate secretly in the presence of an eavesdropping node, Eve. Eve is considered passive and can overhear ongoing communication without tempering with the wireless channel between legitimate nodes. The channel between legitimate nodes is the main channel which is reciprocal. The wireless channel from Alice to Bob is $h_{ab}$, Bob to Alice is $h_{ba}$, Alice to Eve is $h_{ae}$, and Bob to Eve is $h_{be}$. We further assume a rapidly varying wireless channel and model all the channels as having a GG distribution [36], [37], [38].

For the channel envelope following the GG distribution, the Probability Density Function (PDF) is given in [38], [39], and [37] as

$$p(h_{(\cdot)}) = \frac{\alpha}{\Gamma(\mu)} \left(\frac{\mu}{\Omega}\right)^{\mu} h_{(\cdot)}^{\alpha\mu-1} e^{-\frac{\mu h_{(\cdot)}^{\alpha}}{\Omega}}, \tag{1}$$

where $\alpha$ is a fading parameter, $\Gamma(\cdot)$ is the Gamma function [40], and $\Omega = E[h_{(\cdot)}^{\alpha}]$, and $E[\cdot]$ is the statistical expectation operation. The parameter $\mu > 0$ is the inverse of the normalized variance of $h_{(\cdot)}^{\alpha}$, which can be represented as

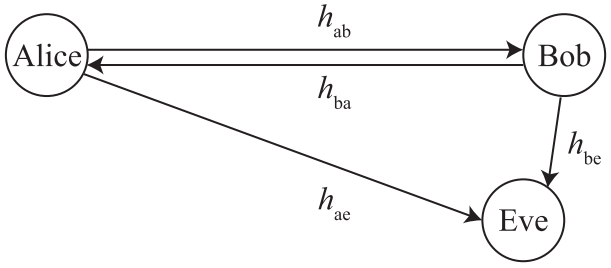


**FIGURE 1.** System model for secure wireless communications.

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

where $V[\cdot]$ is the statistical variance operation. This GG distribution can model various other distributions as its special case, e.g., Rayleigh ($\alpha = 2, \mu = 1$), Nakagami-$m$ ($\alpha = 2$ and $\mu = m$), and Weibull ($\mu = 1$). The above PDF (1) can be integrated over the appropriate limits to compute the expression of CDF as [38]

$$F(h_{(\cdot)}) = \frac{\gamma\left(\mu, \frac{\mu h_{(\cdot)}^{\alpha}}{\Omega}\right)}{\Gamma(\mu)}, \tag{3}$$

where $\gamma(\cdot, \cdot)$ is the lower incomplete Gamma function [40].

The joint GG distribution is exploited to compute the conditional CDF as in [38]

$$F(h_a|h_b) = 1 - Q_\mu\left(\sqrt{\frac{2\mu\rho h_b^{\alpha}}{\Omega(1-\rho)}}, \sqrt{\frac{2\mu h_a^{\alpha}}{\Omega(1-\rho)}}\right), \tag{4}$$

where $Q_\mu(\cdot, \cdot)$ is the Marcum-$Q$ function of order $\mu$ [41] and $\rho$ is the correlation between the legitimate node's channel.

The closed-form analytical expression of ACD between the lower bounding threshold $q^-$ and the upper bounding threshold $q^+$ for the GG fading channels is given in [36]

$$\Xi_{q^-}^{q^+} = \frac{\left(\frac{\Omega}{\mu}\right)^{\mu-\frac{1}{2}} \left(\gamma\left(\mu, \frac{\mu q^{+\alpha}}{\Omega}\right) - \gamma\left(\mu, \frac{\mu q^{-\alpha}}{\Omega}\right)\right)}{f_m\sqrt{2\pi}\left(q^{-\frac{\alpha}{2}(2\mu-1)} e^{-\frac{\mu q^{-\alpha}}{\Omega}} + q^{+\frac{\alpha}{2}(2\mu-1)} e^{-\frac{\mu q^{+\alpha}}{\Omega}}\right)}, \tag{5}$$

where $f_m$ is the maximum Doppler shift.

## III. PROPOSED TRCP SCHEME

The correlated stochastic channel variations of the legitimate nodes where black squared samples correspond to Alice's envelopes and red circled samples correspond to Bob's

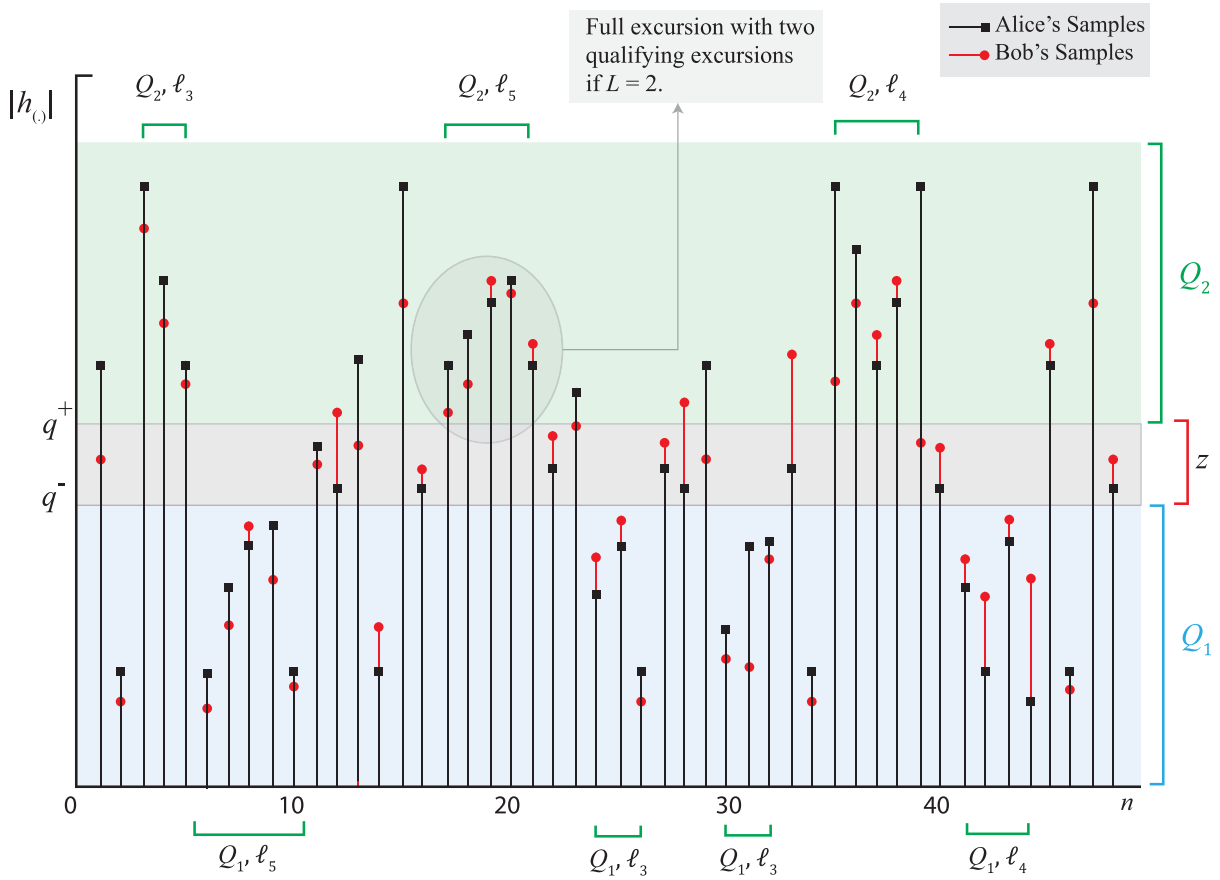


**FIGURE 2.** A depiction of 2-level CDF-based Non-Uniform Quantization (NUQ) and correlated full excursion lengths at the legitimate nodes (i.e., Alice and Bob). Black squares correspond to Alice's channel samples and red dots correspond to Bob's channel samples.

envelopes are shown in Fig. 2. Both the channel envelopes are assumed to follow the GG distribution. Since the main channel is reciprocal in a TDD setup, we assume a high value of correlation coefficient for the main channel. In practice, Alice and Bob transmit probing signals to measure the channel response of the reciprocal channel and store the corresponding envelope values [20]. For testing new algorithms, a technique of generating correlated channel envelope values was proposed in [24]. In this paper, we use the method of [24] for generating correlated channel measurement values at the legitimate nodes as our channel envelope distribution is also GG. This algorithm exploits the conditional CDF of the GG distribution given in (4) to generate wireless channel samples with the desired correlation $\rho$ between the samples of the legitimate nodes. Let the channel envelope samples at Alice be given in a vector $\mathbf{V}_A$ of length $N$, then assuming given channel conditions specified by the parameters $\alpha$, $\Omega$, $\mu$, and $\rho$ and using the inverse CDF method based on (4), correlated channel envelope values $\mathbf{V}_B$ for Bob can be generated using the Algorithm 1 below where the function rand(1) generates a sample from uniform distribution $U[0, 1]$, solve $(y = f(x), x)$ numerically solves the given equation for the unknown $x$. Such measurements may be used to test a number of different SKG algorithms, due to the massive applicability of the

**TABLE 3.** Percentage relative error in the estimated correlation coefficients of the generated sequences for GG distributed channel samples ($\alpha = 2, \Omega = 2$).

| $\rho$ | $\mu = 1$ | | $\mu = 2$ | |
|---|---|---|---|---|
| | $\hat{\rho}$ | $\%Er$ | $\hat{\rho}$ | $\%Er$ |
| 0.1 | 0.0995 | 0.5 | 0.0990 | 1 |
| 0.3 | 0.2950 | 1.66 | 0.3005 | -0.167 |
| 0.5 | 0.4988 | 0.24 | 0.4999 | 0.02 |
| 0.7 | 0.7100 | -1.42 | 0.6995 | 0.071 |
| 0.9 | 0.9008 | -0.09 | 0.8999 | 0.012 |

GG distribution for modelling a wide range of channel conditions corresponding to various correlation coefficients. The accuracy of the proposed scheme is tested by considering different values for the theoretical correlation coefficients $\rho$, generating the GG sequences using the method proposed and computing the estimated correlation coefficients $\hat{\rho}$ using

$$\hat{\rho} = \frac{\sum_{j=1}^{N}(x_j^2 - E[x])(y_j^2 - E[y])}{\sqrt{\sum_{j=1}^{N}(x_j^2 - E[x])^2 \sum_{j=1}^{N}(y_j^2 - E[y])^2}}, \tag{6}$$

where $(x, y) \in (h_a, h_b)$ and $N$ is the total number of samples. Table 3 summarises the results of the algorithm's efficiency in

**Algorithm 1** Generation of Correlated GG Fading Wireless Channel Envelopes [24]

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

terms of the relative percentage error $\frac{\rho-\hat{\rho}}{\rho}100\%$. These results indicate that extremely accurate generation of correlated GG samples is possible using Algorithm 1.

Before discussing TRCP, a few useful terms are defined in the following:

*Channel Range:* The difference between the maximum channel value and the minimum channel value is the channel range. The channel range is divided into two types of regions; quantization regions and guard-bands.

*Quantization Region, $\mathcal{Q}_n$:* The channel range is divided into regions so that secret key bits can be assigned to different channel samples lying in those regions. In Fig. 2, the channel range has two quantization regions (i.e., $\mathcal{Q}_1$ and $\mathcal{Q}_2$).

*Guard-band, $\mathcal{G}$:* To reduce the probability of secret key mismatch, guard-bands are selected and placed in the channel range. The number of guard-bands depends upon the quantization levels used for PLSKG.

*Threshold Values:* The channel values that determine the boundary between different quantization regions (for the case when guard-band width $z$ is 0) or the end values of guard-bands (when guard-band width $z > 0$).

*Lower Threshold Value, $q^-$:* Channel envelope value that corresponds to the lower boundary of the guard-band.

*Upper Threshold Value, $q^+$:* Channel envelope value that corresponds to the upper boundary of the guard-band.

*Guard-band Width, $z$:* The difference between the upper threshold value and the lower threshold value is the guard-band width, $z$. Guard-band width is set proportional to the Mean-Squared Error (MSE, $\sigma$) of the legitimate nodes channels [24].

*Control Parameter, $k$:* The width of the guard-band region is controlled by the parameter $k$ such that $z = k\sigma$ [24].

*Excursion:* An excursion is a consecutive run of channel samples in a given quantization region (see Fig. 2).

*Excursion Length, $\ell$:* The excursion length (in channel samples) is the number of channel samples for which the channel profile stays within a given quantization region.

*Minimum Excursion Length, $L$:* $L$ is an algorithm parameter used in [19], [25], and [36] and specifies the minimum excursion length needed to qualify an excursion for SKG.

*Qualifying Excursion:* An excursion whose length is equal to $L$.

*Matched Qualifying Excursions:* Excursions with the same sample index values and equal lengths $L$ belonging to the same quantization regions at the two legitimate nodes.

*Unmatched Qualifying Excursions:* Excursions with the same sample index values and lengths $L$ belong to the different quantization regions at the legitimate nodes.

*Full Excursion:* The total number of samples for which the channel profile resides within a given quantization region before leaving that quantization region. A full excursion may have more than one qualifying excursions depending on the value of $L$. The length of a full excursion is the number of samples in that excursion and is given by $\ell_s$, where $s$ represents the number of samples in the given full excursion.

*Matched Full Excursions:* Full excursions with the same sample index values where the corresponding channel samples residue in the same quantization region for the legitimate nodes (see Fig. 2).

*Unmatched Full Excursions:* Full Excursions with the same sample index values but channel samples belonging to different quantization regions at the legitimate nodes.

### A. FULL EXCURSION LENGTHS

The striking feature of the TRCP algorithm is the correlation of the lengths of full excursions at the legitimate nodes. Fig. 2 depicts the channel variations at the legitimate nodes where black squares correspond to Alice's channel samples and red dots correspond to Bob's channel sample. It can be clearly seen that Alice and Bob have matched full excursions of $\ell_3$ at indices 3, 4, and 5 in the quantization region $\mathcal{Q}_2$. Similarly, they also have a matched full excursion of $\ell_5$ at indices 6, 7, 8, 9, and 10 in the quantization region $\mathcal{Q}_1$. The legitimate nodes can have full excursions of the same length in different quantization regions and as such different binary code sequences can be assigned to full excursions of the same length belonging to different quantization regions. This guarantees that even if the information of full excursion lengths is shared via the public channel between legitimate nodes, Eve can only guess about the code that will be assigned to these full excursions.

TRCP exploits the channel samples in a two-round PLSKG algorithm where the 1$^{\text{st}}$ round is similar to the algorithms in [19], [25], and [36]. The analysis in [24] indicates that for the quasi-static fading with channel samples having Gamma distribution, the probability of matched excursions reduces with increasing values of length (i.e., longer matched excursions are less probable). Assuming 2-level quantization and no guard-band, the probability of $\ell$ consecutive samples to be found in a quantization interval is given by $2(\frac{1}{2})^{\ell}$ which reduces exponentially with the length $\ell$ and reaches 0.0078125 when $\ell = 8$. When the guard-band is taken into consideration, the probability of longer matched excursions further reduces due to the loss of samples in the guard-band and depends on the guard-band width. This can be computed

solving $2(\int_0^{q^-}\int_0^{q^-} p(h_a, h_b)dh_a dh_b)^{\ell}$. Further, in [24], it can be observed that when temporal correlation is considered between the individual channel samples, the probability of the matched excursion lengths is determined by the sampling interval $T_s$. In this paper, we consider matched excursions of lengths $\ell_m = 8$ or less assuming that matched excursions of lengths higher than 8 with not significantly increase the KGR due to the low probability of such longer excursions and the presence of the guard-band. Therefore, TRCP extracts secret key bits only from those full excursions whose lengths are greater than or equal to $L$ up to $\ell_m$ (i.e., $L$ to $\ell_m$). As such for 2-level quantization, and up to 8 full excursion lengths, we have a 16-level quantization for the 2nd round of TRCP. This is a salient feature of TRCP as in addition to the traditional 2-level quantization in the 1st round, it proposes a 16-level quantization scheme with additional secret key bits exploiting a 2nd dimension of the channel samples for the 2nd round of PLSKG.

Full excursions of different lengths are not equally probable (i.e., the probability of higher-length full excursions is lower) but the probability of a given length full excursion is the same in both $\mathcal{Q}_1$ and $\mathcal{Q}_2$ due to the CDF-based non-uniform quantization. Therefore, TRCP assigns binary codes to a given full excursion length belonging to different quantization regions that are the 1's complements of one another. The 1's complement assignment ensures an equal probability of 0's and 1's in the resulting secret key and the key is more likely to pass the NIST randomness test suite. Further, to reduce the likelihood of repeated 0's and 1's, the code starts with those code sequences which have equal 0's and 1's for high probable full excursion lengths (i.e., 1 0 1 0 and 0 1 0 1 have 2 0's and 1's each.)

We start by generating $h_{ab}$ and $h_{ba}$ having GG distribution and correlation $\rho$ using inverse CDF-based algorithm as in [36]. Let the $\aleph$-sample vector of Alice is $\mathbf{V}_A$ and Bob is $\mathbf{V}_B$.

The proposed TRCP scheme (for 2-level quantization) has two rounds and each parses the channel samples differently.

*Round 1:* Alice parses her channel samples $\mathbf{V}_A$ starting from 1st sample and checks for excursions of length $L$ (i.e., qualifying excursions). Alice places the central indices of all such excursions in a vector $\mathbf{E}_A$. Bob parses her channel samples $\mathbf{V}_B$ starting from 1st sample and checks for excursions of length $L$. Bob places the central indices of all such excursions in a vector $\mathbf{E}_B$. Bob sends $\mathbf{E}_B$ to Alice. Alice compares $\mathbf{E}_A$ and $\mathbf{E}_B$ and places the common entries in $\mathbf{E}_C$. Alice sends $\mathbf{E}_C$ to Bob. Alice assigns secret key bits to channel samples $x$ at the indices in $\mathbf{E}_C$ depending on the quantization regions in which they fall using the 1-bit quantization mapping function as in [20] and [34]

$$R^1(x) = \begin{cases} 0 & x \in \mathcal{Q}_1 \\ 1 & x \in \mathcal{Q}_2 \\ \text{dropped} & x \in \mathcal{G}. \end{cases} \tag{7}$$

$$R^2(y, \ell) = \begin{cases} 1010 & y \in \mathcal{Q}_1 \wedge \ell = \ell_1 \\ 0101 & y \in \mathcal{Q}_2 \wedge \ell = \ell_1 \\ 1100 & y \in \mathcal{Q}_1 \wedge \ell = \ell_2 \\ 0011 & y \in \mathcal{Q}_2 \wedge \ell = \ell_2 \\ 1001 & y \in \mathcal{Q}_1 \wedge \ell = \ell_3 \\ 0110 & y \in \mathcal{Q}_2 \wedge \ell = \ell_3 \\ 0100 & y \in \mathcal{Q}_1 \wedge \ell = \ell_4 \\ 1011 & y \in \mathcal{Q}_2 \wedge \ell = \ell_4 \\ 0010 & y \in \mathcal{Q}_1 \wedge \ell = \ell_5 \\ 1101 & y \in \mathcal{Q}_2 \wedge \ell = \ell_5 \\ 0001 & y \in \mathcal{Q}_1 \wedge \ell = \ell_6 \\ 1110 & y \in \mathcal{Q}_2 \wedge \ell = \ell_6 \\ 1000 & y \in \mathcal{Q}_1 \wedge \ell = \ell_7 \\ 0111 & y \in \mathcal{Q}_2 \wedge \ell = \ell_7 \\ 0000 & y \in \mathcal{Q}_1 \wedge \ell = \ell_8 \\ 1111 & y \in \mathcal{Q}_2 \wedge \ell = \ell_8 \\ \text{dropped} & \text{otherwise} \end{cases} \tag{8}$$

Bob also assigns secret key bits to channel samples at the indices in $\mathbf{E}_C$ depending on the quantization regions in which they fall using (7).

*Round 2:* Alice starts parsing her channel samples $\mathbf{V}_A$ starting from 1st sample and checks for full excursions. Alice places the full excursion lengths and the associated central indices in a different array $\mathbf{F}_A$. Bob also starts parsing her channel samples $\mathbf{V}_B$ starting from 1st sample and checks for full excursions. Bob places the full excursion lengths and the associated central indices in a different array, $\mathbf{F}_B$. Bob sends $\mathbf{F}_B$ to Alice. Alice compares $\mathbf{F}_A$ and $\mathbf{F}_B$ and places the common entries in $\mathbf{F}_C$. Alice sends $\mathbf{F}_C$ to Bob. Alice assigns secret key bits to excursion lengths, $\ell$ in $\mathbf{F}_C$ depending on the quantization regions in which the sample, $y$ at the central index falls using the code assignments given in (8). Similarly, Bob assigns secret key bits to excursion lengths in $\mathbf{F}_C$ depending on the quantization regions in which they fall using the code assignments given in (8). It is pertinent to notice that the 2nd round of TRCP adds only incremental overhead as the same measured channel envelope values are used for extracting additional secret key bits.

This is given in algorithm form as shown below where it is assumed that the legitimate nodes estimate the GG channel parameters $c$, $\rho$, $\alpha$, and $\Omega$.

### B. COMPARISON OF TRCP WITH OTHER PLSKG ALGORITHMS

We compare the proposed TRCP with the following PLSKG algorithm:

- Ye [19].
- Li [32].
- ACD [25].

The above three algorithms differ only in the guard-band placement in the channel range. The Ye et al. [19] is a

**Algorithm 2** Proposed TRCP PLSKG Algorithm

**Parameter Definition:**

- Set $k$, $c$, $\rho$, $\alpha$, $\Omega$.

**Channel Sampling:**

- Legitimate nodes measure the channel profiles by alternately sending probing signals and storing all such measurements in $\mathbf{V}_A$ and $\mathbf{V}_B$. TRCP generates the channel samples using Algorithm 1 in [36].

**Guard-bands and Thresholds Calculation:**

- TRCP calculates the guard-band bounding thresholds $q^-$ and $q^+$ using the CDF-based strategy in [24].
- Binary 0 is assigned to $\mathcal{Q}_1$ and 1 is assigned to $\mathcal{Q}_2$.

**Round 1 of TRCP:**

- Alice and Bob decide on $L$.
- Alice and Bob search $\mathbf{V}_A$ and $\mathbf{V}_B$ independently for qualifying excursions and places the central indices of all such excursions in $\mathbf{E}_A$ and $\mathbf{E}_B$.

**Secret Key Generation/Reconciliation:**

- Bob sends $\mathbf{E}_B$ to Alice who compares $\mathbf{E}_A$ with $\mathbf{E}_B$ and records the matching indices corresponding to the matched excursions in $\mathbf{E}_C$.
- Alice sends $\mathbf{E}_C$ to Bob.
- Alice and Bob extract their secret keys $\mathbf{K}_A^1$ and $\mathbf{K}_B^1$ from the channel samples at the indices in $\mathrm{E}_C$ using (7).

**Round 2 of TRCP:**

- Alice and Bob search $\mathbf{V}_A$ and $\mathbf{V}_B$ independently for full excursions whose lengths are greater than or equal to $L$ and places the central indices of all such excursions in $\mathbf{F}_A$ and $\mathbf{F}_B$.
- Bob sends $\mathbf{F}_B$ to Alice who compares $\mathbf{F}_A$ with $\mathrm{F}_B$ and records the matching indices and lengths in $\mathbf{F}_C$.
- Alice sends $\mathbf{F}_C$ to Bob.
- Alice and Bob extract their secret keys $\mathbf{K}_A^2$ and $\mathbf{K}_B^2$ from the matched excursion lengths in $\mathbf{F}_C$ using (8).
- Alice's final key $\mathbf{K}_A$ is the concatenation of the secret keys $\mathbf{K}_A^1$ and $\mathbf{K}_A^2$.
- Bob's final key $\mathbf{K}_B$ is the concatenation of the secret keys $\mathbf{K}_B^1$ and $\mathbf{K}_B^2$.

uniform quantization strategy and divides the channel range into quantization regions whose channel spans are equal. The Li et al. [32] uses vector quantization to increase the KGR of the legitimate nodes by repeatedly using the channel samples. The guard-band placement is the same as that of Ye et al. [19].

The ACD-NUQ proposed in [25] divides the channel range into quantization regions based on the average time the channel envelope spends in a given quantization interval. For $M$-level quantization, this ensures that the ACD in each quantization region is equal

$$\Theta_0^{q_{M-1}^- + z}(M) = \left[ \Xi_{q_0^+ = 0}^{q_1^-}, \Xi_{q_1^- + z}^{q_2^-}, \cdots, \Xi_{q_{M-1}^- + z}^{q_{\max}} \right]. \quad (9)$$

### C. KEY PERFORMANCE INDICATORS (KPIS) FOR PLSKG

The secret key generated via a PLSKG scheme is used for symmetric encryption of the information exchanged between the legitimate nodes. Since the amount of information exchanged between a pair of nodes is increasing due to the exponential growth in the use of internet and multimedia services, the secret key generated should have the following attributes.

#### 1) KEY GENERATION RATE, $\mathcal{K}_\mathcal{G}$

Key Generation Rate measures on average the number of secret key bits generated from a single channel sample. Assuming the total number of channel samples that the legitimate nodes use for PLSKG be $\aleph$ and the generated secret key bits be $\mathfrak{B}$, then the KGR is given by

$$\mathcal{K}_\mathcal{G} = \frac{\mathfrak{B}_\mathfrak{g}}{\aleph}. \quad (10)$$

#### 2) KEY AGREEMENT PROBABILITY, $\mathcal{K}_\mathcal{A}$

Key Agreement Probability measures on average the number of secret key bits that are in agreement between the legitimate nodes compared to the total number of secret key bits generated. Assuming the number of bits in agreement are $\aleph_a$ and the generated secret key bits be $\mathfrak{B}_\mathfrak{g}$, then the KAP is given by

$$\mathcal{K}_\mathcal{A} = \frac{\aleph_a}{\mathfrak{B}_\mathfrak{g}}. \quad (11)$$

#### 3) RANDOMNESS

The randomness of the generated secret key is assessed via the NIST test suite [42].

## IV. NUMERICAL RESULTS AND DISCUSSION

This section is dedicated to the performance evaluation of the proposed TRCP scheme in comparison to other schemes discussed in Section III. The impact of channel parameters, $\rho$ and algorithm parameters, $k$ and $L$ is discussed on the KGR and KAP performance. $10^6$ channel samples belonging to the GG distribution and exhibiting correlation coefficient, $\rho$ are generated for the legitimate nodes using **Algorithm 1** in [36].

The CDF and ACD equations (9) and (5) are used to determine the threshold values for the quantizer design. TRCP also employ the same quantization thresholds as CDF-based schemes [36]. For a fair comparison, all the schemes employ 2-level quantization and the same channel samples and all schemes are evaluated using the same metrics: $\mathcal{K}_\mathcal{G}$, $\mathcal{K}_\mathcal{A}$, and randomness (assessed via the NIST test suite).

### A. COMPARISON OF KGR AND KAP PERFORMANCE

Fig. 3 depicts the impact of the algorithm parameter, $L$ on the $\mathcal{K}_\mathcal{G}$ performance of the different schemes. It can be clearly observed that the $\mathcal{K}_\mathcal{G}$ reduces as a function of $L$ for all the schemes. This is due to the fact that as the value of $L$ increases, the algorithm tends to rely on longer excursions (excursion length greater than $L$) and shorter excursions are

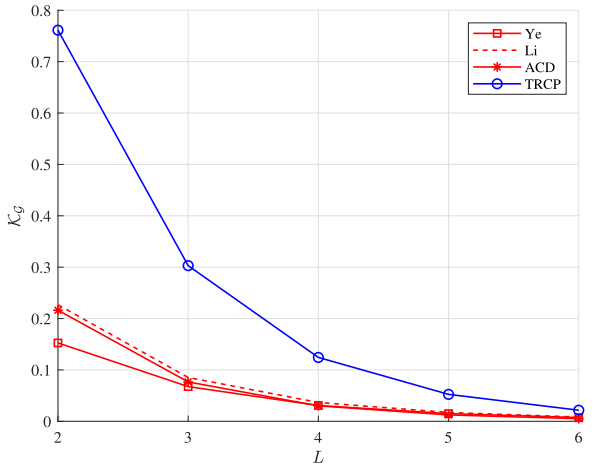


**FIGURE 3.** $\mathcal{K}_\mathcal{G}$ performance of different PLSKG schemes against values of $L$ with $\rho = 0.95$, $\mu = 2$, and $\Omega = 2$.

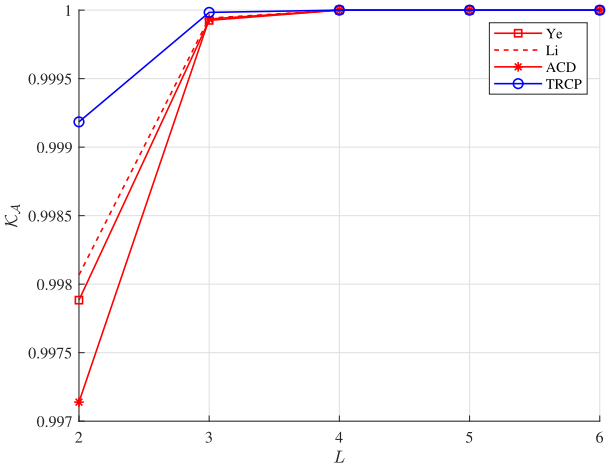


**FIGURE 4.** $\mathcal{K}_\mathcal{A}$ performance of different PLSKG schemes against values of $L$ with $\rho = 0.95$, $\mu = 2$, and $\Omega = 2$.

lost during PLSKG. For a given value of $L$, however, the TRCP outperform all other algorithms. This is due to the 2nd round of TRCP that results in additional secret key bits for the legitimate nodes using the same channel samples. This increase in KGR is larger for smaller values of $L$ and reduces as the value of $L$ increases. This is due to the fact that as the value of $L$ increases, the second round of TRCP is bound to use lesser and lesser full excursion length (i.e., $\ell_L$ to $\ell_8$).

Fig. 4 depicts the impact of the algorithm parameter, $L$ on the $\mathcal{K}_\mathcal{A}$ performance of the different schemes. It can be clearly observed that the $\mathcal{K}_\mathcal{A}$ increases as a function of $L$ for all the schemes. This is due to the fact that as the value of $L$ increases, the algorithms start avoiding smaller excursions which are most likely to be found in different quantization regions for PLSKG. For a given value of $L$, however, the TRCP outperform all other algorithms. This is due to the fact that the ratio of matched secret key bits to the generated secret key bits increases.

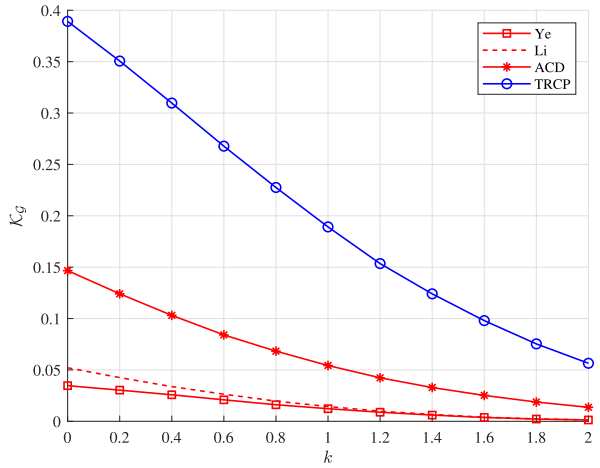


**FIGURE 5.** $\mathcal{K}_\mathcal{G}$ performance of different PLSKG schemes against values of $k$ with $\rho = 0.95$, $\mu = 2$, and $\Omega = 2$.

Fig. 5 depicts the impact of the control parameter $k$ on the $\mathcal{K}_\mathcal{G}$ performance of the different schemes. It can be clearly observed that the $\mathcal{K}_\mathcal{G}$ reduces as a function of $z$ for all the schemes. This is due to the fact that as the value of $k$ increases, the resulting value of the guard-band width (i.e., $z = k\sigma$) also increases and more and more samples tend to fall within the guard-band and are subsequently not considered for PLSKG. For a particular value of $k$, however, TRCP has the best performance and the gap between the KGRs of TRCP and other algorithms reduces as the value of $k$ increases.

Fig. 6 depicts the impact of the control parameter, $k$ on the $\mathcal{K}_\mathcal{A}$ performance of the different schemes. An increasing value of $k$ results in the widening of the guard-band. As channel samples falling in the guard-band are not considered for SKG, it becomes increasingly less probable for the correlated channel samples of the legitimate nodes to be found on the opposite side of the widening guard-band. It can be clearly observed that the $\mathcal{K}_\mathcal{A}$ increases as a function of $k$ for all the schemes. This is due to the fact that as the value of $k$ increases, the resulting value of the guard-band width (i.e., $z = k\sigma$) also increases reducing the likelihood of both the unmatched qualifying excursions (for all algorithms as it becomes less likely for samples to be in different quantization regions when the guard-band is wide) and unmatched full excursions (for TRCP as it exploits full excursion lengths for SKG) and consequently, the likelihood of key mismatch reduces. However, for any given value of $k$, TRCP outperforms all other algorithms.

Fig. 7 depicts the impact of the correlation coefficient, $\rho$ on the $\mathcal{K}_\mathcal{G}$ performance of the different schemes. It can be clearly observed that the $\mathcal{K}_\mathcal{G}$ increases as a function of $\rho$ as expected for all the schemes. This is due to the fact that an increase in $\rho$ results in a reduction of the MSE, bringing the channel samples at the legitimate nodes closer and closer. This results in an increase in matched qualifying excursions (for all algorithms) and matched full excursions (for TRCP) and consequently the KGR of all algorithms

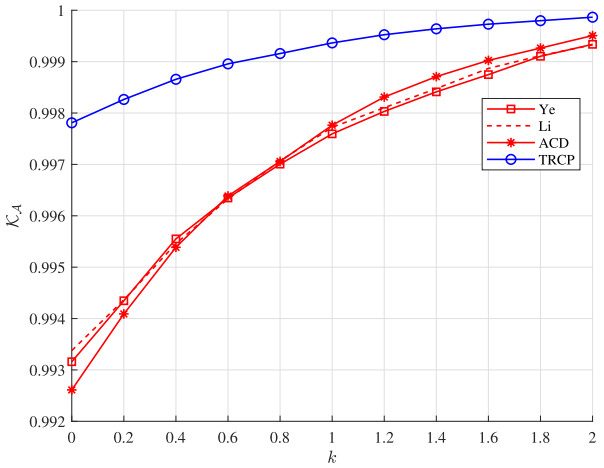


**FIGURE 6.** $\mathcal{K}_{\mathcal{A}}$ performance of different PLSKG schemes against values of $k$ with $\rho = 0.95$, $\mu = 2$, and $\Omega = 2$.

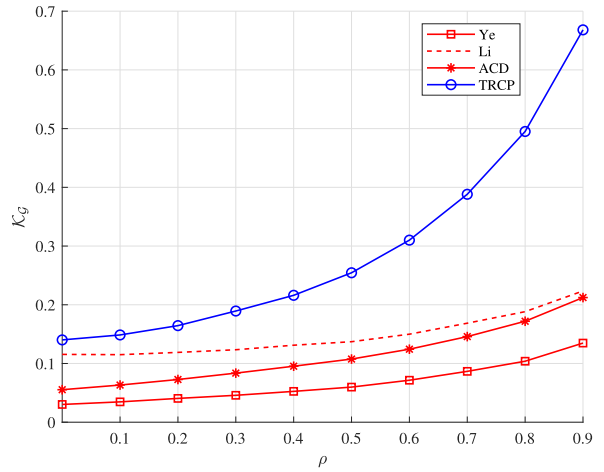


**FIGURE 7.** $\mathcal{K}_{\mathcal{G}}$ performance of different PLSKG schemes against values of $\rho$ with $L = 0.95$, $\mu = 2$, and $\Omega = 2$.

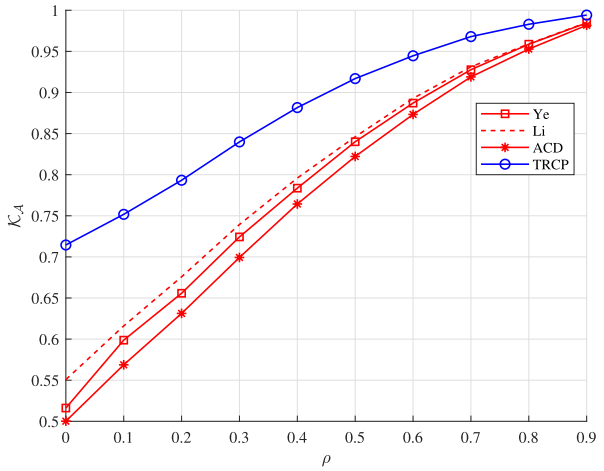


**FIGURE 8.** $\mathcal{K}_{\mathcal{A}}$ performance of different PLSKG schemes against values of $\rho$ with $L = 2$, $\mu = 2$, and $\Omega = 2$.

**TABLE 4.** $p$-value corresponding to different NIST statistical test for the secret key generated by TRCP.

| Test Name | $p$-value ($L = 2$) | $p$-value ($L = 3$) |
|---|---|---|
| Frequency Test | 0.69 | 0.70 |
| Block Frequency Test | 0.99 | 0.99 |
| Run Test | 0.27 | 0.48 |
| Longest-Run-of-Ones Test | 0.31 | 0.42 |
| Cumulative-Sum-Forward Test | 0.87 | 0.81 |
| Cumulative-Sum-Reversed Test | 0.83 | 0.89 |
| Discrete Fourier Transform (DFT) Test | 0.035 | 0.18 |
| Approximate-Entropy Test | 0.44 | 0.32 |
| Maurer Test | 0.84 | 0.83 |

increases. However, the KGR for a given value of $\rho$ is higher for the TRCP algorithm compared to all other algorithms.

Fig. 8 depicts the impact of the correlation coefficient, $\rho$ on the $\mathcal{K}_{\mathcal{A}}$ performance of the different schemes. It can be clearly observed that the $\mathcal{K}_{\mathcal{A}}$ increases as a function of $\rho$ as expected for all the schemes. This is due to the fact that an increase in $\rho$ results in an increased similarity between the channel profiles of the legitimate nodes. This results in an increase in matched qualifying excursions (for all algorithms) and matched full excursions (for TRCP) and consequently the KAP of all algorithms increases. However, the KAP for a given value of $\rho$ is higher for the TRCP algorithm compared to all other algorithms.

These results demonstrate both the efficiency and robustness of the TRCP algorithm compared to other notable PLSKG schemes. TRCP has superior performance compared to both 1-bit quantizers as well as multi-level PLSKG schemes [20], [36]. In addition to higher KGR values, TRCP does not suffer from degradation of KAP as other PLSKG schemes do when the number of quantization regions is increased by adding more guard-bands in the channel range.

### B. RANDOMNESS OF THE SECRET KEY GENERATED BY TRCP ALGORITHM

This subsection is dedicated to the randomness characteristic of the secret key generated by the TRCP algorithm. There is no single metric to quantify the randomness of the generated secret key, however, the NIST test suite comprising 16 tests serves the purpose of assessing the randomness attribute of a sequence. Each test has a sample set requirement and we perform only those tests whose sample requirement can be met by the secret key bits generated via TRCP. Each test results in a $p$-value that determines if the sequence under test is random or not. If the $p$-value corresponding to a given secret key sequence is greater than or equal to 0.01, the sequence is assumed random otherwise it is assumed to be not random and the sequence fails to qualify the corresponding test. The results are depicted in Table 4. These results indicate that the secret key generated by the TRCP algorithm passes all the statistical tests of the NIST test suite.

Symmetric encryption requires Alice and Bob to have the same secret keys. Ideally, both legitimate nodes should encrypt every information bit with a secret key bit (one-time pad cypher). Practical PLSKG algorithms generate secret keys at a rate far less compared to the information rate, however, the secret key $\mathbf{K}$ can be used for the duration of the session of communication to encrypt plain text $\mathbf{m}$ into cyphertext $\mathbf{c}$ ($\mathbf{c} = m \oplus \mathbf{K}$) and can be updated as per the requirement. The Advanced Encryption Standard (AES) is defined for 128-, 192-, and 256-bit secret keys [43]. TRCP operating at KGR of 0.7 bits/channel-sample would require a probing rate of 40 samples/sec to generate 128 bits in 4.5 sec. The legitimate nodes need to exchange pilot signals before the actual exchange of information signals to generate such keys and can use/update the secret key when needed.

TRCP algorithm has improved KGR and KAP (as can be seen from Fig. 3 to Fig. 8) with comparable randomness properties as indicated by the $p$-values of different NIST tests in Table 4. Further, the cost and complexity are similar to other state-of-the-art schemes as it only adds a 2nd layer of processing the same channel envelope values. It is important to notice that the analysis and results of the proposed TRCP algorithm apply to any two communicating nodes that measure channel envelope values for the same transmitted probing signal and extract a secret key via the same algorithm. However, the reciprocal channel between legitimate nodes gives them a higher correlation coefficient value for the main channel compared to the Eve channel.

## V. CONCLUSION

This paper proposed a Two-Round Channel Parsing (TRCP) novel Physical-Layer-based Secret Key Generation (PLSKG) algorithm to better exploit the channel profile of the legitimate nodes for generating a secret key that can be used for symmetric encryption of the information shared between Alice and Bob. TRCP employs a two-layer channel parsing strategy to efficiently exploit the channel samples for secret key generation. It further proposed a coding strategy for the $2^{nd}$ round of the PLSKG that enhances the randomness of the generated secret key. The proposed TRCP scheme was compared with various state-of-the-art schemes in terms of performance metrics namely Key Generation Rate (KGR), Key Agreement Probability (KAP) and randomness. A comprehensive comparative analysis suggests that the proposed TRCP scheme outperforms notable PLSKG schemes both in terms of KGR and KAP and that the resulting secret key sequences pass the NIST test suite. TRCP also outperform multi-level PLSKG schemes and has comparatively better KGR and KAP performance. Future work may consider the mathematical analysis of the sample correlation and excursion lengths correlation for deriving limits of the secret key generation rate and key agreement probability. Further, real-time correlated Generalized Gamma (GG) distributed datasets for channel envelopes in a given coherence time are very rare and we shall consider measurement campaigns for such datasets in future work.

## REFERENCES

[1] Q. Li, Z. Ding, X. Tong, G. Wu, S. Stojanovski, T. Luetzenkirchen, A. Kolekar, S. Bangolae, and S. Palat, "6G cloud-native system: Vision, challenges, architecture framework and enabling technologies," *IEEE Access*, vol. 10, pp. 96602–96625, 2022.

[2] H. Lee, B. Lee, H. Yang, J. Kim, S. Kim, W. Shin, B. Shim, and H. V. Poor, "Towards 6G hyper-connectivity: Vision, challenges, and key enabling technologies," *J. Commun. Netw.*, vol. 25, no. 3, pp. 344–354, Jun. 2023.

[3] A. Chorti, A. N. Barreto, S. Köpsell, M. Zoli, M. Chafii, P. Sehier, G. Fettweis, and H. V. Poor, "Context-aware security for 6G wireless: The role of physical layer security," *IEEE Commun. Standards Mag.*, vol. 6, no. 1, pp. 102–108, Mar. 2022.

[4] E. Jorswieck, P.-H. Lin, and C. Janda, "Physical layer security based enabling technologies for 6G communications values," in *Proc. IEEE Future Netw. World Forum (FNWF)*, Oct. 2022, pp. 550–555.

[5] Q. Xu, Z. Su, and R. Li, "Security and privacy in artificial intelligence-enabled 6G," *IEEE Netw.*, vol. 36, no. 5, pp. 188–196, Sep. 2022.

[6] F. Khan, S. Ahmad, H. Gürüler, G. Cetin, T. Whangbo, and C.-G. Kim, "An efficient and reliable algorithm for wireless sensor network," *Sensors*, vol. 21, no. 24, p. 8355, Dec. 2021.

[7] F. Khan, A. A. Al-Atawi, A. Alomari, A. Alsirhani, M. M. Alshahrani, J. Khan, and Y. Lee, "Development of a model for spoofing attacks in Internet of Things," *Mathematics*, vol. 10, no. 19, p. 3686, Oct. 2022.

[8] A. U. Makarfi, K. M. Rabie, O. Kaiwartya, X. Li, and R. Kharel, "Physical layer security in vehicular networks with reconfigurable intelligent surfaces," in *Proc. IEEE 91st Veh. Technol. Conf. (VTC-Spring)*, May 2020, pp. 1–6.

[9] J. Lansky, A. M. Rahmani, S. M. Zandavi, V. Chung, E. Yousefpoor, M. S. Yousefpoor, F. Khan, and M. Hosseinzadeh, "A Q-learning-based routing scheme for smart air quality monitoring system using flying ad hoc networks," *Sci. Rep.*, vol. 12, no. 1, p. 20184, Nov. 2022.

[10] M. Mitev, A. Chorti, H. V. Poor, and G. P. Fettweis, "What physical layer security can do for 6G security," *IEEE Open J. Veh. Technol.*, vol. 4, pp. 375–388, 2023.

[11] P. Porambage, G. Gür, D. P. M. Osorio, M. Liyanage, A. Gurtov, and M. Ylianttila, "The roadmap to 6G security and privacy," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 1094–1122, 2021.

[12] V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang, and Y.-D. Lin, "Security and privacy for 6G: A survey on prospective technologies and challenges," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2384–2428, 4th Quart., 2021.

[13] M. Bloch, O. Günlü, A. Yener, F. Oggier, H. V. Poor, L. Sankar, and R. F. Schaefer, "An overview of information-theoretic security and privacy: Metrics, limits and applications," *IEEE J. Sel. Areas Inf. Theory*, vol. 2, no. 1, pp. 5–22, Mar. 2021.

[14] 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.

[15] 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.

[16] J. Martinez-Mateo, C. Pacher, M. Peev, A. Ciurana, and V. Martin, "Demystifying the information reconciliation protocol cascade," 2014, *arXiv:1407.3257*.

[17] E. O. Kiktenko, A. O. Malyshev, and A. K. Fedorov, "Blind information reconciliation with polar codes for quantum key distribution," *IEEE Commun. Lett.*, vol. 25, no. 1, pp. 79–83, Jan. 2021.

[18] R. Impagliazzo, L. A. Levin, and M. Luby, "Pseudo-random generation from one-way functions," in *Proc. 21st Annu. ACM Symp. Theory Comput.*, 1989, pp. 12–24.

[19] 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.

[20] 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.

[21] 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.

[22] 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.
[23] 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.
[24] 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.
[25] S. J. Nawaz, M. Adil, and S. Wyne, "Average contiguous duration—A novel metric for characterizing wireless fading channels," *IEEE Wireless Commun. Lett.*, vol. 10, no. 8, pp. 1790–1794, Aug. 2021, doi: 10.1109/LWC.2021.3080434.
[26] 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.
[27] X. Hu, L. Jin, K. Huang, X. Sun, Y. Zhou, and J. Qu, "Intelligent reflecting surface-assisted secret key generation with discrete phase shifts in static environment," *IEEE Wireless Commun. Lett.*, vol. 10, no. 9, pp. 1867–1870, Sep. 2021.
[28] J. Tang, H. Wen, H.-H. Song, L. Jiao, and K. Zeng, "Sharing secrets via wireless broadcasting: A new efficient physical layer group secret key generation for multiple IoT devices," *IEEE Internet Things J.*, vol. 9, no. 16, pp. 15228–15239, Aug. 2022.
[29] H. Luo, N. Garg, and T. Ratnarajah, "A channel frequency response-based secret key generation scheme in in-band full-duplex MIMO-OFDM systems," *IEEE J. Sel. Areas Commun.*, vol. 41, no. 9, pp. 2951–2965, 2023.
[30] X. He, H. Dai, W. Shen, and P. Ning, "Is link signature dependable for wireless security?" in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 200–204.
[31] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "New physical layer key generation dimensions: Subcarrier indices/positions-based key generation," *IEEE Commun. Lett.*, vol. 25, no. 1, pp. 59–63, Jan. 2021.
[32] 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.
[33] 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.
[34] 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.
[35] 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*.
[36] M. Adil, S. Wyne, S. J. Nawaz, and B. Muhammad, "Average contiguous duration (ACD)-based quantization for secret key generation in generalized gamma fading channels," *IEEE Access*, vol. 9, pp. 110435–110450, 2021.
[37] M. D. Yacoub, "The $\alpha$-$\mu$ distribution: A physical fading model for the Stacy distribution," *IEEE Trans. Veh. Technol.*, vol. 56, no. 1, pp. 27–34, Jan. 2007.
[38] 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.
[39] 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.
[40] G. E. Andrews, R. Askey, and R. Roy, *Special Functions*. Cambridge, U.K.: Cambridge Univ. Press, 1999.
[41] J. G. Proakis and M. Salehi, *Digital Communications*. 5th ed. New York, NY, USA: McGraw-Hill, 2007.
[42] 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, D. L. Banks, and N. A. Heckert. *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, Standard Sp 800–22 Rev. 1A, Nat. Inst. Standards Technol., 2010.
[43] N. Ferguson, B. Schneier, and T. Kohno, *Cryptography Engineering: Design Principles and Practical Applications*. Hoboken, NJ, USA: Wiley, 2011.

**MUHAMMAD ADIL** received the Ph.D. degree in electrical engineering from the Department of Electrical and Computer Engineering, COMSATS University Islamabad (CUI), Islamabad, Pakistan, in 2022. He is currently working as an Assistant Professor with the Department of Technology, Abasyn University, Peshawar. His current research interests include information theory and physical layer security, secret key generation, optimization in wireless communications, the Internet-of-Things (IoT), orthogonal time frequency space modulation, and 6G communications.

**HABIB ULLAH KHAN** received the Ph.D. degree in management information systems from Leeds Beckett University, U.K., in 2008. He has nearly 20 years of industry, teaching, and research experience. He is currently working as a Professor with MIS, Department of Accounting and Information Systems, College of Business and Economics, Qatar University, Qatar. His research interests include IT adoption, social media, the internet addiction, mobile commerce, computer mediated communication, IT outsourcing, big data, and IT security.

**MOHAMMAD ARIF** received the B.S. degree in electrical engineering from the University of Engineering and Technology, Peshawar, Pakistan, in 2012, and the M.S. and Ph.D. degrees in electrical engineering from COMSATS University Islamabad, Pakistan, in 2014 and 2021, respectively. Currently, he is working as an Assistant Professor with the Department of Computer Engineering, Gachon University, Seongnam-si, South Korea. He has also served as a Visiting Research Associate with Qatar University, Doha, Qatar, in 2022. His research interests include U-V2X communications, jamming interference, mm-waves communications, C-V2X communications, aerial and terrestrial heterogeneous networks, dual connectivity, decoupled access, interference management, reverse frequency allocation, indoor localization, signal processing, and channel coding.

**MIAN SHAH NAWAZ** received the M.S. degree in telecommunication engineering from the University of Sunderland, U.K., in 2012. He is currently working as an Assistant Professor with the Department of Engineering Technology, Abasyn University, Peshawar. His current research interests include the Internet-of-Things (IoT), physical layer security, and optimization in wireless communications.

**FAHEEM KHAN** received the Ph.D. degree in computer science from the University of Malakand, Khyber Pakhtunkhwa, Pakistan. He was an Assistant Professor in Pakistan for four years and supervised many papers and students. Since April 2021, he has been an Assistant Professor with the Department of Computer Engineering, Gachon University, South Korea. His research interests include computer networking, wireless networking, MANET, sensor networking, the IoT, artificial intelligence, and AI in healthcare systems.