

A Scalable and Lightweight Physical Layer Key Generation Protocol for Multi-User Wireless Systems

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

Abstract—This paper presents a novel group secret key generation (GSKG) protocol for multi-user wireless systems with a star topology. In contrast to conventional methods relying on pairwise key derivation followed by reconciliation, the proposed approach enables the central node to directly select a group secret key uniformly at random across the full quantization space. This eliminates the need for intermediate pairwise keys, significantly reducing computational complexity, communication overhead, and latency. To ensure consistent group key reconstruction, we introduce two lightweight, non-coding reconciliation techniques: One-Sided Centering (OSC) and Quantization Pattern Alternation (QPA). Unlike coding-based reconciliation in conventional schemes, OSC and QPA allow the central node to transmit helper data – derived from adjusted measurements or shifted quantization grids – to peripheral nodes. This helper data not only aligns their channel observations with the selected quantization region, but also implicitly distributes the group key. Thus, reconciliation and distribution are seamlessly integrated into a unified protocol. The proposed GSKG framework supports both fully and partially cooperative scenarios and remains robust against unreliable or compromised nodes by selectively omitting or perturbing helper data. Furthermore, a concatenation-based group key construction method exploits existing bidirectional channel measurements to generate multiple key segments, enhancing throughput without additional channel probing. Extensive simulations validate the scheme's performance in terms of key disagreement rate, key generation rate, computational efficiency, and robustness against eavesdropping. The results confirm that the protocol offers high scalability and security, making it a practical and efficient solution for group key establishment in IoT and other resource-constrained wireless applications.

Index Terms—Group secret key generation, channel quantization, key reconciliation, randomization, key disagreement ratio, Multi-user, reciprocity, ray-tracing, IoT.

I. INTRODUCTION

Secure key exchange remains a foundational challenge in modern wireless communications, particularly in resource-constrained environments. Classical cryptographic protocols, such as Diffie-Hellman (D-H), rely on computational hardness assumptions to establish symmetric keys. However, the advent of quantum computing threatens these schemes, as quantum algorithms (e.g., Shor's) can efficiently solve the underlying mathematical problems, rendering conventional approaches vulnerable [1]. Furthermore, the computational and energy demands of such protocols limit their applicability in low-power devices, including embedded sensors, Internet of Things (IoT) nodes, and RFID tags. However, due to three defining characteristics of 5G IoT networks – namely, high mobility,

massive deployment of resource-constrained devices, and a heterogeneous hierarchical architecture – traditional cryptographic mechanisms encounter significant challenges. These include difficulties in key distribution, excessive dependence on computational complexity, and overall inefficiency, making classical cryptographic protocols unsuitable for such environments [2].

Physical Layer Key Generation (PLKG) has emerged as a promising approach to establishing shared secret keys by exploiting the reciprocity and randomness of wireless channels, thus avoiding reliance on computational complexity. In Time Division Duplex (TDD) systems, extensive research has utilized channel state information (CSI) and received signal strength (RSS) to extract highly correlated observations between legitimate transceivers [3], [4]. Surveys have summarized the theoretical foundations and research challenges of these approaches [5]–[7]. Subsequent studies have refined the schemes through improved quantization, reconciliation, and robustness under practical conditions [8], [9]. More recent efforts exploit multidimensional diversity [10], employ neural network-based prediction for IoT applications [11], [12], and demonstrate the feasibility of PLKG in low-power wide-area networks [13]. By contrast, Frequency Division Duplex (FDD) systems face additional challenges due to the absence of strict reciprocity. To overcome this, earlier studies have exploited the continuity of phase differences across adjacent frequency bands by modeling the channel as a two-port network [14]. High-resolution direction-of-arrival (DoA) estimation techniques such as MUSIC and ESPRIT [15], [16], as well as reciprocity reconstruction methods [17], [18], have also been investigated. More recently, machine learning techniques have been employed to enable robust FDD key generation [19].

Despite these advances, most studies remain focused on pairwise key generation, while secure group communication is increasingly critical in domains such as ad hoc networks, industrial automation, and IoT ecosystems. These applications demand Group Secret Key Generation (GSKG) protocols that enable multiple users to derive a common cryptographic key, ensuring end-to-end confidentiality and integrity. Prior work has explored GSKG in star, ring, and mesh topologies [20]–[24], building on the foundational results of Csizsár and Narayan [25] and advancing toward practical implementations such as those by Ye and Reznik [26]. Nonetheless, GSKG in multiuser settings is inherently more complex than pairwise approaches due to coordination, synchronization, and error resilience among distributed nodes. Centralized distribution must also address channel asymmetries, noise, and device heterogeneity, while scalability introduces further challenges of latency, overhead, and energy consumption, particularly in

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

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

adversarial environments.

Conventional GSKG schemes designed for star topologies [24] typically involve the establishment of individual pairwise keys between a central node and each peripheral node, which are subsequently combined to derive a common group key. Although this approach is widely adopted, it imposes substantial overhead in terms of both computation and communication, leading to scalability challenges. More recent alternatives, such as cooperative GSKG scheme [27], aim to mitigate reconciliation complexity by reducing the number of rounds required. However, these methods often suffer from degraded key rates as the group size increases and encounter more significant challenges in channel estimation and coordination. In this work, we propose an efficient GSKG scheme specifically designed for star-topology wireless networks. In contrast to conventional methods [20]–[24], [27]–[29], our approach eliminates the need for pairwise key generation, relying solely on the direct channel observations between a central node (Alice) and multiple peripheral nodes (Bobs). Furthermore, we propose an integrated framework that unifies non-coding key reconciliation and group key distribution into a single stage, thereby substantially reducing communication overhead, computational burden, and overall system complexity. Critically, the proposed scheme ensures information-theoretic security against passive eavesdroppers (e.g., Eve), facilitating scalable and secure group communication in next-generation wireless networks. The key contributions of this paper are summarized as follows:

- 1) We propose a lightweight, scalable, and efficient physical-layer GSKG framework for star-topology wireless networks that eliminates the need for conventional pairwise key generation and aggregation. Instead, the central node randomly selects a group key from a quantized key space, significantly reducing system complexity, communication overhead, and latency. Simulation results demonstrate up to a 65% reduction in communication overhead and a 99% decrease in computational complexity compared to LDPC-based schemes. The flexible key selection process ensures a uniform key distribution, thereby enhancing secrecy against potential eavesdroppers. Furthermore, the statistical randomness of the generated keys is validated using the NIST test suite.
- 2) We introduce two novel, low-complexity, non-coding reconciliation strategies – *One-Sided Centering* (OSC) and *Quantization Pattern Alternation* (QPA) – as efficient alternatives to conventional coding-based techniques. These approaches achieve a group key disagreement rate below 10^{-5} at SNRs ≥ 20 dB using lightweight helper data such as quantization shifts or pattern indices. By combining measurement alignment and group key distribution in a unified process, OSC and QPA achieve significant reductions in both complexity and latency.
- 3) We propose a novel concatenation-based group key construction method that replaces conventional XOR-based aggregation to enhance the practical key throughput per channel use. Multiple key segments are independently selected from a shared Gray-coded codebook, with

lightweight helper data transmitted to peripheral nodes. By reusing bidirectional channel measurements, the method increases the amount of usable key material without requiring additional channel probing. It should be noted that while concatenation extends the group key length and improves practical key utilization, the overall entropy remains fundamentally bounded by the mutual information between Alice’s and Bob’s channel observations.

- 4) We conduct extensive simulations and ray-tracing validations confirm that the proposed scheme ensures high key uniformity ($e_u \leq 0.005$), strong randomness (passing all NIST statistical tests), and high resilience against eavesdropping, making it well-suited for secure, real-time group communication in IoT systems.

The remainder of this paper is organized as follows. Section II introduces the system model, adversary model, channel model, and channel reciprocity assumptions. Section III provides an overview of conventional group key generation schemes, followed by the conceptual framework and detailed formulation of the proposed GSKG protocol, together with the non-coding QPA reconciliation algorithm. Sections IV and V present the performance evaluation metrics and validate the proposed scheme through extensive simulations, respectively. Section VI discusses key aspects, including eavesdropping resilience, channel dynamics, entropy limitations, and potential application scenarios. Finally, Section VII concludes the paper.

II. SYSTEM OVERVIEW

A. System Model

We consider a physical-layer GSKG framework based on a star-topology wireless network. A trusted central node – referred to as *Alice* (e.g., a base station or access point) – coordinates the key establishment process for M legitimate end users, denoted as *Bobs* $B_1, B_2, \dots, B_M$, where $M \geq 2$. Key generation is performed over wireless fading channels in the presence of one or more passive eavesdroppers. All nodes are assumed to lie within mutual communication range and to exhibit either quasi-static behavior or slow mobility, resulting in quasi-static channel conditions. Although this assumption is realistic for many indoor IoT deployments, it may limit channel entropy, particularly in fully static scenarios. This limitation, along with potential mitigation strategies, is further addressed in Section VI. Each terminal is equipped with a single antenna and operates in half-duplex mode, alternating between transmission and reception using time-division multiplexing. This configuration reflects practical deployment scenarios in resource-constrained networks, such as IoT and sensor systems.

B. Adversary Model

In line with standard assumptions in the physical-layer key generation literature [14], [30], [31], we adopt a passive adversary model. All legitimate users are assumed to be fully trusted, and this study does not address threats such as insider attacks, device compromise, or active man-in-the-middle (MITM) attacks. Extending the proposed framework to detect and mitigate insider threats remains a promising direction for future research. The passive eavesdropper, referred to as *Eve*, is

assumed to be located at least half a wavelength away from any legitimate node. In rich multipath environments, this spatial separation ensures that Eve's wireless channels are uncorrelated with those of the legitimate users, preventing her from inferring channel measurements from her own observations. Moreover, Eve is assumed to have full access to all public messages exchanged during key generation and complete knowledge of the protocol, in accordance with Kerckhoffs's principle. This establishes a conservative and robust security model under the strongest reasonable passive adversary assumption.

C. Channel Model and Reciprocity

In TDD systems, uplink and downlink transmissions share the same frequency band but are separated in time. The time-domain channel impulse response between Alice and a given Bob (or Eve) is modeled using a tapped-delay line representation:

$$h(t, \tau) = \sum_{\ell=0}^{L-1} \alpha_{\ell} \delta(t - \tau_{\ell}), \quad (1)$$

where $\alpha_{\ell} \in \mathbb{C}$ and $\tau_{\ell} \in \mathbb{R}$ represent the complex gain and propagation delay of the ℓ -th multipath component, respectively, and $\delta(\cdot)$ denotes the Dirac delta function. Assuming channel reciprocity and temporal coherence over a coherence interval T_c , the forward and reverse channel impulse responses between Alice and the i -th Bob satisfy

$$h_{AB_i}(t) \approx h_{B_iA}(t), \quad \text{for } t \in T_c. \quad (2)$$

Let $h(t)$ denote the true reciprocal channel within this interval. In practice, the channel estimates obtained at Alice and Bob are corrupted by thermal noise and hardware imperfections, which are commonly modeled as additive noise:

$$\tilde{h}_A(t) = h(t) + w_A(t), \quad (3)$$

$$\tilde{h}_{B_i}(t) = h(t) + w_{B_i}(t), \quad (4)$$

where $\tilde{h}_A(t)$ and $\tilde{h}_{B_i}(t)$ denote the noisy channel estimates at Alice and the i -th Bob, respectively. The noise terms $w_A(t)$ and $w_{B_i}(t)$ are modeled as independent complex Gaussian random variables:

$$w_A(t), w_{B_i}(t) \sim \mathcal{CN}(0, \sigma^2). \quad (5)$$

In frequency-selective environments – especially in multicarrier systems – the channel is typically estimated in the frequency domain across N subcarriers. The frequency-domain channel response at the n -th subcarrier, indexed by frequency f_n , is given by

$$h[n] = \sum_{\ell=0}^{L-1} \alpha_{\ell} e^{-j2\pi f_n \tau_{\ell}}, \quad n = 1, 2, \dots, N, \quad (6)$$

and the corresponding noisy estimates at Alice and Bob are modeled as

$$\tilde{h}_A[n] = h[n] + w_A[n], \quad (7)$$

$$\tilde{h}_B[n] = h[n] + w_B[n]. \quad (8)$$

with $w_A[n], w_B[n] \sim \mathcal{CN}(0, \sigma^2)$ are independent complex Gaussian noise components associated with each subcarrier.

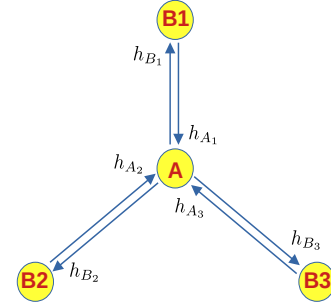


Fig. 1: Star topology wireless system comprising a central node (Alice) and three peripheral nodes (Bobs)

III. PROPOSED GSKG PROTOCOL

This section formalizes the design of the proposed GSKG protocol for star-topology wireless networks. We begin by systematically reviewing conventional GSKG approaches, which rely on pairwise key generation, coding-based reconciliation, and XOR-based aggregation – highlighting their fundamental limitations in scalability, computational complexity, and effective key generation rate. Motivated by these shortcomings, we introduce a novel GSKG framework that eliminates the need for pairwise key establishment and reconciliation by directly selecting the group key from a structured Gray-coded codebook. At the heart of the proposed method lies a unified, lightweight strategy for non-coding reconciliation and group key distribution. This approach employs shift-based helper data to align each peripheral node's channel measurement with a target quantization interval preselected by the central node. The section concludes with a comprehensive algorithmic framework that rigorously defines the procedures for group key selection, helper data generation, and group key reconstruction.

A. Conventional GSKG Schemes

Consider a star-topology network comprising a central node, denoted as *Alice*, and M peripheral nodes, labeled $B_1, B_2, \dots, B_M$ (collectively referred to as *Bobs*). During the channel probing phase, Alice independently conducts bidirectional channel measurements with each Bob. Specifically, Alice and the i -th peripheral node (Bob _{i}) independently measure their reciprocal channel coefficients, denoted as h_{A_i} and h_{B_i} , respectively. From these measurements, each node extracts a relevant reciprocal channel feature – such as amplitude, phase, phase difference, or angle-of-arrival/departure – represented as m_{A_i} and m_{B_i} , as observed by Alice and Bob, respectively. A wireless system comprising a central node, Alice, and three peripheral nodes – Bob₁, Bob₂, and Bob₃ – arranged in a star topology, is illustrated in Fig. 1. Following channel measurement, both Alice and each Bob quantize their observations using a lossless quantization scheme. The quantizer divides the dynamic range into 2^n equal-width intervals, each assigned a unique n -bit Gray code. This transforms the continuous-valued observations into discrete binary sequences. The resulting key segments derived from the i -th Alice–Bob channel are given by

$$K_{A_i} = \mathcal{GC}(\mathcal{Q}(m_{A_i})), \quad K_{B_i} = \mathcal{GC}(\mathcal{Q}(m_{B_i})), \quad (9)$$

where $\mathcal{Q}(\cdot)$ denotes the quantization function, and $\mathcal{GC}(\cdot)$ denotes the Gray coding operation. This process yields candidate

pairwise keys between Alice and each Bob. However, due to hardware imperfections and channel noise, discrepancies may arise between the initial key versions K_{A_i} and K_{B_i} following the quantization stage. To reconcile the mismatched bits while preserving secrecy, a Slepian-Wolf coding-based reconciliation protocol – typically implemented using low-density parity-check (LDPC) codes [32] – is employed. LDPC-based reconciliation efficiently corrects these mismatches with minimal information leakage, and has been adopted in practical systems, such as those following the IEEE 802.15.4z standard for Ultra-Wideband (UWB) communication. After successful reconciliation, the shared key between Alice and the i -th Bob is denoted as

$$K_i = K_{A_i}^r = K_{B_i}^r, \quad (10)$$

where the superscript r indicates the reconciled version. This pairwise reconciliation process is independently performed between Alice and each of the M peripheral nodes.

To generate the group key, Alice computes the bitwise XOR of all reconciled pairwise keys:

$$\mathcal{K}_G^A = \bigoplus_{i=1}^M K_i = K_1 \oplus K_2 \oplus \dots \oplus K_M. \quad (11)$$

She then distributes the group key to each Bob by broadcasting a masked version, $\mathcal{K}_G^A \oplus K_{A_i}^r$, for $i = 1, 2, \dots, M$. Each Bob subsequently reconstructs the group key by performing

$$\mathcal{K}_G^{B_i} = (\mathcal{K}_G^A \oplus K_{A_i}^r) \oplus K_{B_i}^r, \quad (12)$$

which yields $\mathcal{K}_G^{B_i} = \mathcal{K}_G^A$ if reconciliation has been successfully completed.

It is important to note that while we refer to this as the “conventional GSKG scheme” for benchmarking purposes, it essentially reflects the architecture adopted by the majority of state-of-the-art protocols [20]–[24], [27]–[29]. While this protocol ensures secrecy against passive eavesdropping, it imposes substantial computational complexity and communication overhead. Specifically, the requirement to independently establish and reconcile M pairwise keys introduces significant complexity. As the number of peripheral nodes increases, the resulting demands on energy, bandwidth, and latency become increasingly prohibitive – particularly in resource-constrained or latency-sensitive environments. Moreover, the reliance on coding-based reconciliation further intensifies the processing burden at the peripheral nodes. In addition, the XOR-based group key construction fundamentally limits the length of generated keys. For an n -bit quantization scheme with M Bobs, although a total of $M \cdot n$ bits are initially derived from all pairwise keys, the final group key contains only n bits. This substantial reduction in effective key yield reveals a critical inefficiency of XOR-based group key construction, particularly in high-throughput or real-time applications.

B. Conceptual Overview

To address the scalability, complexity, and overhead limitations inherent associated with conventional group key generation frameworks, the proposed scheme introduces a more efficient and streamlined paradigm. Instead of establishing and reconciling M individual pairwise keys, the central node,

Alice, selects a group key uniformly at random from the key space defined by the underlying quantization scheme. This selected key corresponds to a valid codeword within an n -bit binary Gray codebook and serves as the shared group key among all legitimate nodes. The core innovation lies in leveraging the algebraic structure of the binary representation inherent to Gray codes. By operating in this binary domain, the scheme enables XOR combinations of codewords to remain within the valid codebook space. This property allows Alice to sample a valid group key directly while preserving essential cryptographic attributes such as uniformity and unpredictability, without requiring additional post-processing. By eliminating explicit pairwise key generation and subsequent aggregation, the proposed approach achieves substantial reductions in both computational complexity and communication overhead. Additionally, the inherent uniformity of the selected group key strengthens its resistance to inference attacks, making the scheme both efficient and robust.

To ensure practical applicability in resource-constrained environments, the proposed framework incorporates a lightweight, non-coding reconciliation mechanism. This approach enables each peripheral node to align its local channel observation with the designated quantization region using helper data transmitted by the central node. Notably, the reconciliation and group key distribution processes are seamlessly unified into a single communication round: by transmitting a unique shift value or quantization pattern index to each Bob, Alice simultaneously reconciles their shared channel measurements and distributes the group key. This streamlined design substantially reduces system complexity, communication overhead, and latency – thereby enhancing overall efficiency. These attributes make the proposed scheme particularly well-suited for deployment in IoT and other low-power wireless applications.

C. Proposed GSKG Protocol Description

In our proposed GSKG protocol, after completing the channel probing phase and extracting the corresponding RSS or CSI values – denoted as m_{A_i} and m_{B_i} for each link between Alice and Bob $_i$, $i = 1, 2, \dots, M$ – Alice randomly selects one of the predefined quantization intervals and adopts the corresponding Gray codeword as the group key:

$$\mathcal{K}_G^A = \mathcal{G}_C(q_G) = \mathcal{G}_C(\text{rand}(q_1, q_2, \dots, q_{2^n})), \quad (13)$$

where $\text{rand}(\cdot)$ denotes a uniform random selector over the set of 2^n quantization intervals, and $\mathcal{G}_C(\cdot)$ represents the Gray encoding function.

To distribute the group key, Alice transmits individualized helper data in the form of a shift value, enabling each Bob to reconstruct the key from his local channel observation. This mechanism draws inspiration from the OSC non-coding reconciliation scheme introduced in [14], [15]. The core principle is that, after selecting a group key, Alice shifts her channel measurement to align precisely with the midpoint of the corresponding quantization interval. It should be noted that, the midpoint of the destination quantization interval is selected to maximize the correction of the mismatch between Alice’s and Bob’s key measurements. The required shift value is then communicated to the respective Bob, who applies it to his

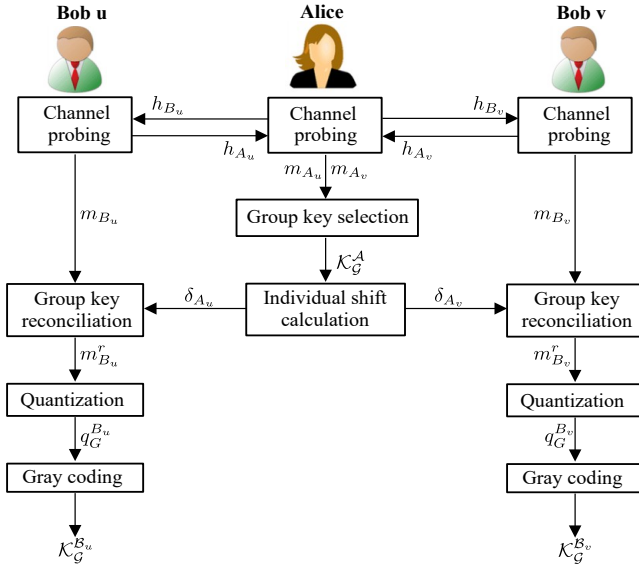


Fig. 2: Group key reconstruction process at the peripheral nodes

own channel measurement. Provided that Bob's measurement is sufficiently correlated with Alice's, the adjusted value falls within the same quantization interval, ensuring successful and reliable group key reconstruction.

Formally, let $q_G \in \{1, 2, \dots, 2^n\}$ denote the index of the selected quantization interval, and let L represent the dynamic range of the channel feature. The center of the q_G -th quantization interval is located at

$$c_{q_G} = \Delta \cdot (\mathcal{Q}^{-1}(\mathcal{K}_G^A) - \frac{1}{2}) = \frac{L(2q_G - 1)}{2^n}, \quad (14)$$

where n and Δ are the number of quantization bits and the quantization step size, respectively, and $\mathcal{Q}^{-1}(\cdot)$ denotes the inverse quantization mapping.

To align the i -th Bob's measurement m_{B_i} with the target interval, Alice computes a shift value δ_{A_i} such that her measurement m_{A_i} is relocated to c_{q_G} . The shift value is given by

$$\delta_{A_i} = c_{q_G} - m_{A_i} = \frac{L(2q_G - 1)}{2^n} - m_{A_i}. \quad (15)$$

This shift value effectively maps each Bob's local observation to align with the selected quantization region, ensuring correct decoding of the group key across all legitimate participants.

Alice then broadcasts the computed shift value δ_{A_i} to the i -th Bob over a public channel. Upon reception, each Bob computes his reconciled measurement by applying the received shift value from Alice to his own channel observation as

$$m_{B_i}^r = m_{B_i} + \delta_{A_i}, \quad i = 1, 2, \dots, M, \quad (16)$$

and then performs quantization and Gray encoding to reconstruct the group key

$$\mathcal{K}_G^{B_i} = \mathcal{GC}(\mathcal{Q}(m_{B_i}^r)), \quad i = 1, 2, \dots, M. \quad (17)$$

Only those Bobs whose channel measurements are sufficiently correlated with Alice's can align with the correct quantization interval and successfully recover the group key. This inherently filters out unreliable or adversarial users.

Figure 2 illustrates this group key reconstruction process for two peripheral nodes (Bob u and Bob v , where $u, v \in \{1, 2, \dots, M\}$) in a star topology. In this illustration, the ideal case assumes $m_{A_u} \approx m_{B_u}$ and $m_{A_v} \approx m_{B_v}$, while the shift values differ, i.e., $\delta_{A_u} \neq \delta_{A_v}$. As a result, both Bobs successfully reconstruct the same group key, satisfying $\mathcal{K}_G^A = \mathcal{K}_G^{B_u} = \mathcal{K}_G^{B_v}$, using their respective local measurements and individualized helper data from Alice.

To enhance system security and robustness, Alice may adopt a selective cooperation policy during the shift transmission phase, wherein she may intentionally broadcast incorrect shift values to selected peripheral nodes. Utilizing indicators such as signal reliability or channel quality, Alice can introduce localized perturbations into the group key distribution process. This strategy mitigates risks associated with spoofing or node compromise – without adding additional authentication overhead. A fundamental information-theoretic measure of pairwise link reliability is the *key generation rate* R_{A_i, B_i} , defined as

$$R_{A_i, B_i} = \frac{I_{A_i, B_i}}{T}, \quad (18)$$

where T denotes the duration of the channel measurement window, and I_{A_i, B_i} represents the mutual information (in nats) between the reciprocal channel observations m_{A_i} and m_{B_i} . This mutual information is expressed as

$$I_{A_i, B_i} = -\frac{1}{2} \log(1 - \rho^2), \quad (19)$$

where ρ denotes the correlation coefficient between m_{A_i} and m_{B_i} , and the squared correlation coefficient ρ^2 is given by

$$\rho^2 = \frac{1}{\left(1 + \frac{\delta^2}{\delta_{A_i, B_i}^2 P_{T_{A_i}}}\right) \left(1 + \frac{\delta^2}{\delta_{A_i, B_i}^2 P_{T_{B_i}}}\right)}, \quad (20)$$

where $P_{T_{A_i}}$ and $P_{T_{B_i}}$ denote the transmit powers of Alice and the i -th Bob, respectively, δ^2 is the noise variance, and δ_{A_i, B_i}^2 represents the channel gain for the $A_i \leftrightarrow B_i$ link. Higher values of R_{A_i, B_i} indicate stronger channel reciprocity and improved reliability for key generation. This statistical model effectively captures the behavior of reciprocal measurements in rich multipath environments and enables tractable analysis of the mutual information between the observations. Equation (19) assumes that the reciprocal channel features m_{A_i} and m_{B_i} are jointly Gaussian – a widely adopted approximation in the PLKG literature, particularly under quasi-static multipath fading when using the real and imaginary parts of CSI in rich multipath environments, where central limit effects induce Gaussian-like behavior. However, we note that other commonly used features such as amplitude and phase are not Gaussian – with amplitude often modeled as Rayleigh or Rician distributed, and phase approximated as uniformly distributed. In such cases, Equation (19) serves as an analytical approximation. If higher fidelity is needed, the mutual information can be estimated empirically from measured data using non-parametric estimation techniques. Additional modeling details can be found in prior works [33]–[35]. By integrating this metric into the shift decision logic, Alice can selectively exclude or downweight nodes with weak or untrustworthy links, thereby enhancing the integrity and resilience of the group key agreement protocol.

To enhance the practical group key throughput per channel use, we propose a novel group key construction scheme based on key segment concatenation. In this approach, Alice constructs an extended group key by selecting multiple quantization intervals and concatenating the corresponding Gray-coded key segments. Specifically, following a single channel probing session with all Bobs, Alice randomly selects l target quantization intervals, denoted by $q_{G_1}, q_{G_2}, \dots, q_{G_l}$, and forms the group key as

$$\mathcal{K}_G^A = \mathcal{K}_{G_1}^A \parallel \mathcal{K}_{G_2}^A \parallel \dots \parallel \mathcal{K}_{G_l}^A, \quad (21)$$

where $\mathcal{K}_{G_j}^A$ represents the Gray code associated with the j -th selected interval. It should be noted that the base case of our proposed scheme considers $l = 1$; however, the protocol is flexible and can concatenate additional key segments to generate longer group keys and increase the amount of usable key material per channel use. To enable correct key reconstruction at the Bobs' side, Alice transmits l distinct shift values to each peripheral node, aligning their measurements with the corresponding target intervals. This strategy allows the GSKG scheme to generate longer group keys while maintaining the same entropy, as all key segments originate from a single channel observation.

A key advantage of this scheme lies in its efficiency: Alice requires only a single probing session per node to generate the necessary shift values for multiple key segments. Consequently, the overall group key length is extended to $l \cdot n$ bits, increasing the key space from 2^n to 2^{ln} . It is important to note that this concatenation-based extension increases the bit-length of the generated group key but does not necessarily enhance its entropy. When all segments are derived from the same reciprocal measurement, the total entropy is fundamentally limited by the mutual information between Alice's and Bob's observations,

$$H(\mathcal{K}_G) \leq \min_{i=1,2,\dots,M} I(m_{A_i}; m_{B_i}). \quad (22)$$

Therefore, the increased key length may introduce redundancy unless the segments are extracted from statistically independent components, such as multiple subcarriers, antennas, or channel realization.

Algorithm 1 outlines the complete step-by-step procedure of the proposed group key generation and distribution protocol, providing a clear pseudocode representation of the underlying method. To further illustrate the proposed approach, consider the wireless system depicted in Fig. 1. The system employs a linear quantization scheme with 2^3 intervals, each represented by a 3-bit Gray code. Suppose Alice selects two key segments ($l = 2$) to construct the group key. Let these segments be $\mathcal{K}_{G_1}^A = 101$ and $\mathcal{K}_{G_2}^A = 001$, resulting in the final group key $\mathcal{K}_G^A = 101001$.

To enable key reconstruction at each Bob's side, Alice transmits two shift values per Bob, corresponding to the quantization intervals q_{G_1} and q_{G_2} associated with the selected key segments. Figure 3 provides an illustrative example of the required shift values for each Bob individually, ensuring that Alice's measurements align precisely with the center of the

Algorithm 1 Proposed Group Key Generation and Distribution

Require:

- Channel coefficients at Alice: $\{h_{A_i}\}_{i=1}^M$;
- Channel coefficients at Bobs: $\{h_{B_i}\}_{i=1}^M$;
- Number of quantization bits: n ;
- Number of key segments: l

Ensure: Group key generation and securely distribution among high-correlation Bobs

1. Channel Probing

- Alice and each Bob perform bidirectional channel probing to estimate reciprocal channel coefficients h_{A_i} and h_{B_i} for $i = 1, \dots, M$.

2. Feature Extraction

- Alice and each Bob extract robust features (CSI or RSSI) from channel estimates, obtaining m_{A_i} and m_{B_i} for i -th user pair.

3. Group Key Selection and Distribution

for $j = 1$ **to** l **do**

3.1 Group Key Segment Selection:

- Alice randomly selects a quantization index $q_{G_j} \in \{1, \dots, 2^n\}$.
- The corresponding Gray codeword is assigned as the j -th segment of the group key:

$$\mathcal{K}_{G_j}^A \leftarrow \mathcal{GC}(q_{G_j})$$

3.2 Shift Value Computation:

- For each Bob $_i$, Alice computes the required shift value:

$$\delta_{A_i}^j = \frac{L(2q_{G_j} - 1)}{2^n + 1} - m_{A_i}$$

- The shift value $\delta_{A_i}^j$ is publicly transmitted to the i -th Bob.

3.3 Group Key Reconciliation at Bobs:

- Each Bob $_i$ aligns its measurement for j -th group key segment:

$$m_{B_i}^{r_j} \leftarrow m_{B_i}^j + \delta_{A_i}^j$$

3.4 Quantization and Encoding:

- The aligned values are quantized and mapped to Gray codewords to reconstruct the j -th part of group key:

$$\mathcal{K}_{G_j}^{B_i} \leftarrow \mathcal{GC}(q(m_{B_i}^{r_j}))$$

End

4. Group Key Formation

- Each Bob forms the complete group key by concatenating all l key segments:

$$\mathcal{K}_G^{B_i} = \mathcal{K}_{G_1}^{B_i} \parallel \mathcal{K}_{G_2}^{B_i} \parallel \dots \parallel \mathcal{K}_{G_l}^{B_i}$$

target quantization intervals. The shift value for the i -th Bob and the j -th key segment is denoted as $\delta_{A_i}^j$ in the figure.

Moreover, the black circles represent the original measurements between Alice and Bob $_1$, Bob $_2$, and Bob $_3$, taken at Alice's side. The red and blue circles indicate the positions of

Alice's measurements after applying the required shifts, such that they fall exactly at the center of the selected quantization intervals corresponding to the first and second key segments, respectively, for each Bob.

D. Discretization via Quantization Pattern Alternation

Instead of explicitly computing and transmitting shift values to each peripheral node, group key reconciliation and distribution can be efficiently realized by dynamically adapting the quantization map to local channel observations. This approach, referred to as *Quantization Pattern Alternation* (QPA), provides a lightweight and secure alternative to the previously introduced OSC scheme.

Consider a reciprocal feature space with dynamic range L , quantized using a uniform linear scheme into 2^n primary intervals, each of width $\Delta = \frac{L}{2^n}$. To enable fine-grained adaptation, each primary interval is further subdivided into m uniform subintervals. This measurement-adaptive structure supports reconciliation based on localized channel observations. During the reconciliation phase, Alice identifies the index s_i of the subinterval into which her observation m_{A_i} falls. This index is calculated as:

$$s_i = \left\lfloor \frac{m \cdot \text{mod}(m_{A_i}, \Delta)}{\Delta} \right\rfloor, \quad (23)$$

where $\text{mod}(m_{A_i}, \Delta)$ returns the offset of m_{A_i} within its primary interval. Alice then transmits the subinterval index $s_i \in \{0, 1, \dots, m-1\}$ to the i -th Bob.

Using this compact helper data, the receiver dynamically selects the quantization pattern that aligns Alice's measurement with the central subinterval. This pattern adaptation significantly reduces the probability of quantization mismatch, thereby increasing the likelihood of successful key reconstruction. Notably, the transmitted value s_i incurs minimal overhead – typically requiring only a few bits – and does not compromise the secrecy of the shared key. Since s_i conveys only the relative offset within a known quantization region, it reveals no useful information to a passive adversary. As an illustrative example, Fig. 4 shows a scenario in which reciprocal channel features are derived from phase measurements spanning the angular domain $[0, 2\pi)$, which is uniformly quantized into $2^3 = 8$ primary intervals. Each primary interval is further divided into $m = 5$ subintervals, yielding subinterval indices $s_i \in \{0, 1, 2, 3, 4\}$. To encode s_i , a 2-bit representation is employed: “00” for $s_i = 0$, “01” for $s_i = 1$, “10” for $s_i = 3$, and “11” for $s_i = 4$. In the default case $s_i = 2$, no transmission is required, and the receiver retains the baseline quantization pattern.

IV. PERFORMANCE ANALYSIS OF THE PROPOSED GSKG SCHEME

This section presents a comprehensive evaluation of the proposed GSKG scheme in comparison with conventional approaches, focusing on communication overhead and computational complexity. We refer to the *conventional GSKG scheme* not as a single method, but as a representative model for a broad class of state-of-the-art group secret key generation algorithms. These conventional approaches are typically characterized by three key features: (i) generating pairwise keys between

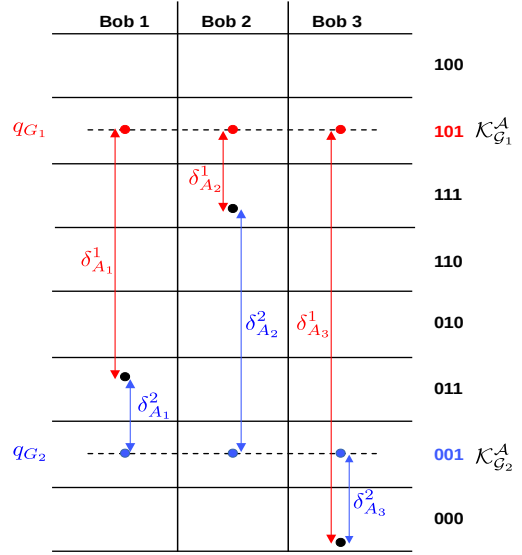


Fig. 3: Segment-wise shift mapping from Alice to the Bobs to enable group key reconstruction

Alice and each peripheral node, (ii) applying coding-based reconciliation – often utilizing techniques such as Slepian–Wolf coding – for each pairwise key, and (iii) deriving the final group key by XORing all reconciled pairwise keys. To distinguish this category in our analysis, we denote it using the superscript c . In contrast, the *proposed GSKG scheme*, denoted by the superscript p , eliminates the need for generating pairwise keys and leverages the introduced QPA or OSC methods – non-coding reconciliation techniques. The analysis is conducted within a star-topology network comprising a central node and M peripheral nodes. Both schemes quantize channel measurements using Gray coding with n -bit resolution. In the proposed approach, the number of bits required to encode each shift value is denoted by s , and the total number of concatenated segments forming the complete group key is denoted by l . It is worth noting that the proposed scheme, in its basic form, does not require key concatenation; concatenation is an optional extension to produce longer group keys and increase the total number of generated key bits. These parameters form the basis of the comparative analysis that follows, highlighting the trade-offs among communication load, computational complexity, efficiency, and overall performance.

A. Communication Overhead

In the conventional schemes, Alice independently performs one-way key reconciliation with each of the M peripheral nodes using LDPC-based Slepian-Wolf coding. For a group key of length n , she transmits a syndrome of length $n(1 - R_c)$ to each Bob, where R_c denotes the code rate of the employed LDPC code. The resulting total reconciliation overhead at this stage is expressed as

$$\text{Overhead}_{\text{Rec}}^{(c)} = M \cdot n \cdot (1 - R_c), \quad (24)$$

Following reconciliation, Alice locally computes the group key K_G^A by performing a bitwise XOR of all reconciled version of pairwise keys, which does not incur additional communication cost. To distribute K_G^A to the Bobs, she transmits $K_G^A \oplus K_{A_i}^r$

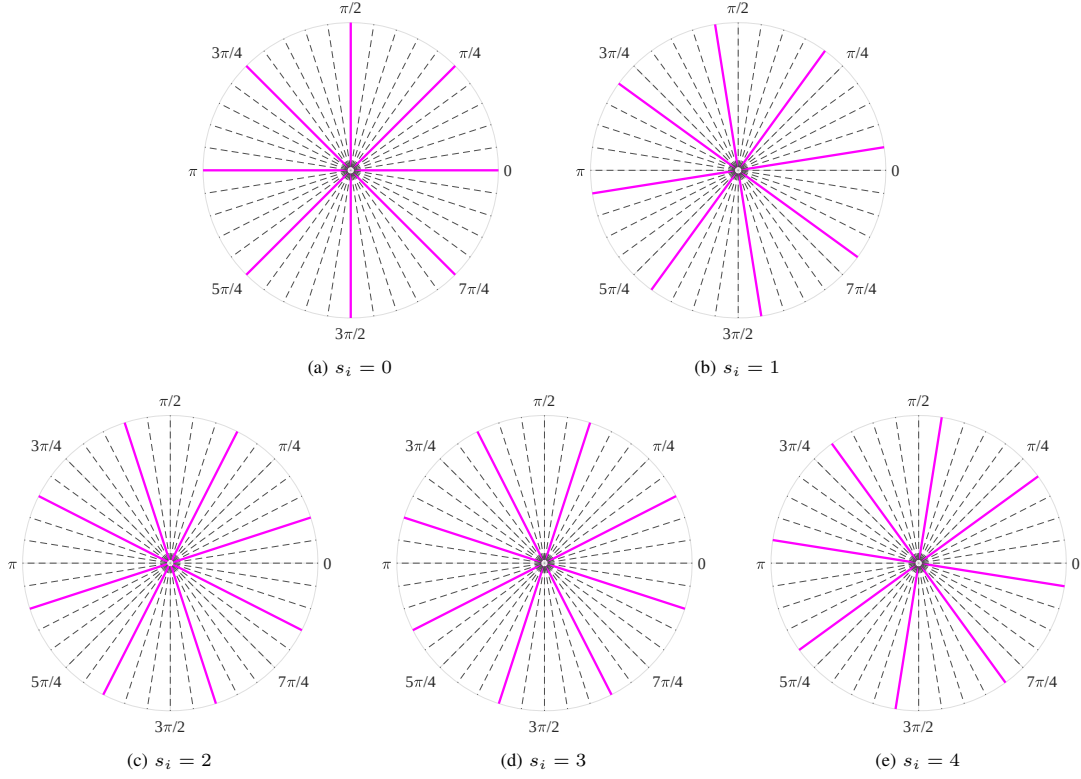


Fig. 4: Illustration of the quantized phase domain in polar QPA with 8 primary intervals and 5 subintervals per segment

to each Bob i , where $K_{A_i}^r$ is the individual pairwise key shared with that Bob. Each of these M transmissions consists of n bits, resulting in a total distribution overhead given by

$$\text{Overhead}_{\text{Dist}}^{(c)} = M \cdot n. \quad (25)$$

Consequently, the total communication overhead of the conventional schemes, normalized per group key bit (with $L = n$), is

$$\text{Overhead}_{\text{Total}}^{(c)} = \frac{M \cdot n \cdot (2 - R_c)}{L} = M \cdot (2 - R_c). \quad (26)$$

In contrast, under the proposed scheme, Alice transmits s -bit helper data per segment to each Bob – representing either a shift value (in OSC) or a quantization pattern (in QPA). These helper data simultaneously enable reconciliation and facilitate group key distribution, thereby eliminating the need for a separate key dissemination phase. Consequently, the total communication overhead per group key bit for the proposed scheme is given by

$$\text{Overhead}_{\text{Total}}^{(p)} = \frac{M \cdot l \cdot s}{L} = \frac{M \cdot s}{n}, \quad (27)$$

where $L = l \cdot n$ denotes the total group key length composed of l segments, each of n -bit resolution. While both conventional and proposed schemes exhibit linear scaling with the number of peripheral nodes, the proposed method achieves a significantly lower per-user overhead factor. This is because the helper data length s is typically much smaller than $n(1 - R_c) + n$, which accounts for both the LDPC syndrome and XOR-based key distribution in conventional schemes. Moreover, the helper data in our scheme simultaneously supports both reconciliation and group key distribution, thereby improving overall efficiency.

Specifically, the ratio of the overheads between the conventional and proposed schemes is given by

$$\frac{\text{Overhead}_{\text{Total}}^{(c)}}{\text{Overhead}_{\text{Total}}^{(p)}} = \frac{n(2 - R_c)}{s}, \quad (28)$$

This expression is generally greater than 1 and illustrates that the reduction in communication overhead becomes increasingly significant when $s \ll n(2 - R_c)$. Under such conditions, the proposed scheme achieves a substantial and consistent overhead reduction. Figure 5 provides a comparative analysis of the communication overhead associated with the proposed and conventional schemes. The evaluation considers QPA-based reconciliation with $s = 2$ bits per segment for the proposed method, and LDPC-based Slepian–Wolf coding with a code rate of $R_c = 1/2$ for the conventional approach. The comparison is conducted across varying numbers of peripheral nodes to highlight scalability and overhead efficiency.

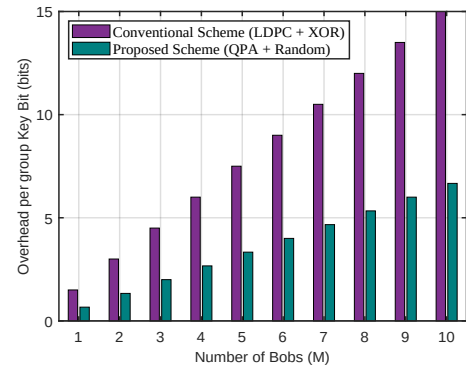


Fig. 5: Comparison of communication overhead between the proposed and conventional schemes as a function of the number of peripheral nodes

TABLE I: Stage-wise computational complexity of the proposed ($l = 1$) and conventional GSKG schemes

Operation	Conventional Scheme	Proposed Scheme
Key Reconciliation (Alice)	LDPC Encoding: $\mathcal{O}(M \cdot n_c \cdot d)$	—
Key Reconciliation (Bobs)	LDPC Decoding: $\mathcal{O}(M \cdot n_c \cdot d \cdot I)$	—
Group Key Forming (Alice)	XOR-based: $\mathcal{O}(M \cdot n)$	Randomly Selecting: $\mathcal{O}(n)$
Group Key Preparation (Alice)	Masking: $\mathcal{O}(M \cdot n)$	Shift Calculation: $\mathcal{O}(M)$
Group Key Extraction (Bobs)	XOR: $\mathcal{O}(M \cdot n)$	Shift Applying: $\mathcal{O}(M \cdot n)$

B. Computational Complexity

In the conventional schemes, which employs pairwise key generation followed by LDPC-based Slepian–Wolf reconciliation, the computational workload is distributed between the central node and the peripheral nodes. At the central node, Alice encodes a syndrome for each pairwise key using an LDPC encoder, incurring a per-user complexity of $\mathcal{O}(n_c \cdot \bar{d}_c)$, where n_c denotes the LDPC block length – typically much larger than the group key length n – and $\bar{d}_c$ is the average check node degree. For M users, the total encoding complexity scales as

$$\mathcal{O}_{\text{Enc}}^{(C)} = \mathcal{O}(M \cdot n_c \cdot \bar{d}_c) . \quad (29)$$

Group key distribution additionally involves XOR masking of the final key for each user, a lightweight operation with an overall complexity of $\mathcal{O}(M \cdot n)$.

On the receiver side, each Bob performs iterative LDPC decoding to recover the corresponding pairwise key. The decoding complexity per user is $\mathcal{O}(n_c \cdot \bar{d}_c \cdot I)$, where I denotes the number of decoding iterations, resulting in a total system-wide complexity of

$$\mathcal{O}_{\text{Dec}}^{(C)} = \mathcal{O}(M \cdot n_c \cdot \bar{d}_c \cdot I) . \quad (30)$$

While LDPC encoding at the central node imposes a moderate computational burden, the decoding process at the peripheral nodes constitutes the dominant cost – particularly when high reliability requires longer codes or increased iteration counts.

In contrast, the proposed scheme leverages lightweight alignment-based techniques – OSC or QPA – that substantially reduce computational complexity at both the central and peripheral nodes by replacing iterative decoding processes with simple, constant-time arithmetic operations. At the central node, Alice computes helper data for each of the l key segments and each of the M peripheral nodes. For OSC, this involves calculating a shift value that aligns her observation with the center of a quantization interval. For QPA, it entails determining the optimal quantization pattern index from a predefined set of m subintervals. In both cases, each segment-wise computation involves only basic arithmetic operations (e.g., subtraction, modulo, rounding), each with constant complexity $\mathcal{O}(1)$. Accordingly, the total complexity at the central node scales as:

$$\mathcal{O}_{\text{Enc}}^{(P)} = \mathcal{O}(M \cdot l) . \quad (31)$$

On the receiver side, each Bob uses the received helper data to align and quantize their local observations. In the case of OSC, this involves applying a scalar shift followed by uniform quantization; for QPA, the observation is mapped according

to the indicated quantization pattern. Both procedures are computationally efficient, with per-user complexity $\mathcal{O}(l)$ and negligible variation between the two schemes. Linear scalability of the proposed approach with respect to both the number of users and key segments, coupled with the inherent simplicity of its operations, makes it particularly suitable for low-latency, energy-efficient, and resource-constrained deployment scenarios. Table I provides a stage-by-stage comparison of the computational complexity for the proposed scheme – evaluated in its base case with a single key segment ($l = 1$) – against that of conventional schemes.

V. SIMULATION RESULTS

A. Simulation Setup

To rigorously evaluate the performance of the proposed GSKG scheme, extensive simulations are conducted using MATLAB’s 5G Toolbox with the 3GPP-compliant Tapped Delay Line A (TDL-A) channel model. The simulation setup features a star-topology wireless network consisting of a central node (Alice), multiple peripheral nodes (Bobs), and one or more passive eavesdroppers (Eves). The signal-to-noise ratio (SNR) is varied from 0 to 30 dB. For each SNR value, 10^6 independent channel realizations are simulated between Alice and each Bob to ensure statistically robust results. This large dataset captures the variability of realistic wireless propagation conditions. The carrier frequency is fixed at 3.5 GHz, aligning with the mid-band spectrum commonly used in 5G networks. To emulate low-mobility indoor environments, Doppler shifts are randomly varied in the range of 1–5 Hz. The TDL-A channel profile is chosen to represent typical urban indoor scenarios characterized by dense multipath propagation. The proposed framework supports key extraction from various reciprocal channel features, including amplitude, phase, and direction-of-arrival (DoA). Key reconciliation is carried out using an n -bit quantization scheme, where $n \in \{1, 2, 3\}$. The quantized values are subsequently followed by n -bit Gray coding to enhance key consistency by reducing the likelihood of bit-flip errors during reconstruction.

In addition to stochastic simulations, the proposed scheme is further validated using deterministic channel realizations generated with Remcom’s Wireless InSite. Custom floor plans were designed to emulate a typical indoor environment, explicitly accounting for multipath propagation, path loss, and Doppler effects to simulate complex wireless signal behavior in built environments. The layout includes multiple rooms with a mix of reflective and absorptive surfaces, supporting up to 25 multipath components per Alice–Bob link. Each Bob is placed in a different room, while Alice is centrally located. The resulting

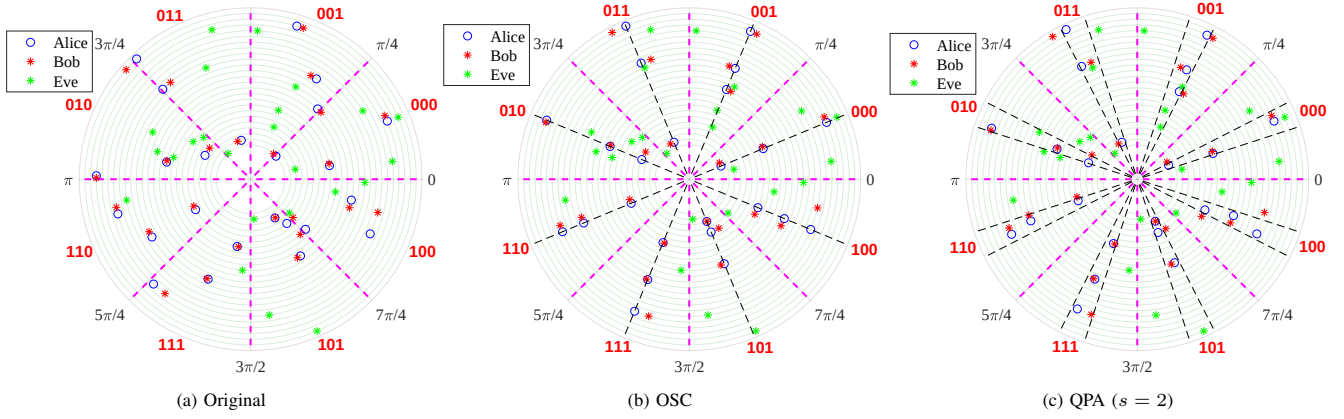


Fig. 6: Spatial distribution of measurement positions between Alice, the 24 Bobs, and Eve in a group key generation scenario. **Left:** Before key reconciliation; **Middle:** After reconciliation using OSC; **Right:** After reconciliation using QPA

ray-tracing data is exported and imported into MATLAB to compute channel coefficients and extract reciprocal channel features. These configurations emulate realistic IoT network deployments and enable rigorous performance evaluation of the proposed scheme under diverse and practical propagation conditions.

B. Performance Metrics

1) *Group Key Disagreement Rate:* The *Group Key Disagreement Rate (GKDR)* is defined as the average fraction of bit mismatches between the group key generated by the central node and the group keys recovered by the peripheral nodes after the group key distribution phase.

Let $\mathcal{K}_G^A \in \{0,1\}^n$ represent the group key generated by Alice, and let $\mathcal{K}_G^{B_i} \in \{0,1\}^n$ denote the reconstructed group key at the i -th peripheral node Bob _{i} . The GKDR is computed as the average bit-wise error rate across all M peripheral nodes.

$$\text{GKDR} = \frac{1}{M} \sum_{i=1}^M \frac{1}{n} \sum_{j=1}^n \mathbb{I}[\mathcal{K}_G^A[j] \neq \mathcal{K}_G^{B_i}[j]], \quad (32)$$

where n is the group key length in bits, and $\mathbb{I}[\cdot]$ denotes the indicator function, which evaluates to 1 if the argument is true, and 0 otherwise. A lower GKDR indicates higher consistency and reliability in group key agreement across the network.

2) *Group Key Generation Rate:* The *Group key generation rate (GKGR)* quantifies the efficiency of generating a consistent and secure group key among multiple users by measuring the average number of successfully agreed-upon key bits per channel use. It is defined as

$$\text{GKGR} = \frac{n \cdot (1 - \text{GKDR})}{N_c}, \quad (33)$$

where n denotes the total number of raw key bits generated during the process, $\text{GKDR} \in [0,1]$ is the GKDR and N_c is the number of channel uses consumed during the group key generation and distribution process. A lower GKDR (i.e., higher agreement among users) results in a higher GKGR, indicating more efficient use of the wireless medium for secure group key establishment.

3) *Uniformity:* The *average relative uniformity error* [36] quantifies the deviation of the empirical symbol distribution from an ideal uniform distribution. Let n_i denote the number of occurrences of the i -th quantization symbol, where $i = 1, 2, \dots, 2^n$, and let n_{avg} be the expected count per symbol under a perfectly uniform distribution. The uniformity error is defined as

$$e_u = \frac{1}{2^n} \sum_{i=1}^{2^n} \frac{|n_i - n_{\text{avg}}|}{n_{\text{avg}}}, \quad (34)$$

where lower values of e_u indicate higher uniformity. This metric provides a useful measure of the balance and entropy of the generated key symbols, and is particularly relevant in evaluating the statistical quality of the group key across all users.

4) *Randomness:* Randomness characterizes the statistical unpredictability of the generated group key sequences. To evaluate it rigorously, we employ the NIST Statistical Test Suite [37], which comprises multiple hypothesis tests designed to assess various aspects of randomness. Each test produces a p -value representing the probability that a truly random sequence would exhibit a deviation as extreme as the observed one. In accordance with standard criteria [37], a key sequence is considered random with 99% confidence if its p -value exceeds 0.01. Larger p -values suggest stronger conformity to the null hypothesis of randomness. For group-wise key generation, these tests are applied to concatenated or individual key streams from multiple users to ensure that group-level entropy is preserved.

C. Results and Analysis

1) *GKDR:* To evaluate the group key disagreement rate performance of the proposed GSKG method, simulations were conducted using two non-coding reconciliation techniques – OSC and QPA – and compared against a conventional scheme based on LDPC coding. The SNR was varied from 0 to 30 dB. Phase measurements extracted from channel probing between Alice and each of the peripheral nodes served as the raw input for group key generation. Figure 6(a) represents the raw spatial phase measurements obtained from Alice, the 24 peripheral nodes (Bobs), and a passive eavesdropper (Eve) during a single channel probing instance at an SNR of 10 dB. Figures 6(b) and 6(c) illustrate the reconciled observations after applying the

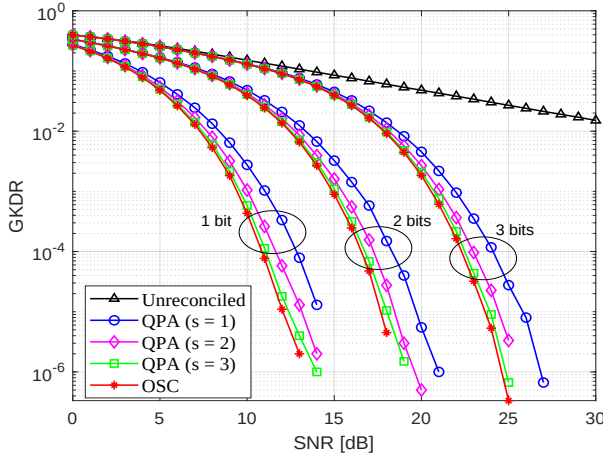


Fig. 7: GKDR performance versus SNR for the proposed GSKG scheme using both QPA and OSC techniques under various quantization resolutions

OSC and QPA techniques, respectively. While these methods do not affect the physical reciprocity of the channels between Alice and each Bob, they enhance functional reciprocity at the quantization stage, resulting in better alignment of key bits. Consequently, strong agreement is observed between Alice and each Bob after reconciliation, whereas Eve's measurements remain uncorrelated. This contrast clearly demonstrates the effectiveness of both reconciliation schemes in aligning legitimate users' observations and preserving the secrecy of reciprocal channel features against passive eavesdropping.

Figure 7 illustrates the GKDR performance of the proposed scheme across a range of SNR values for both the OSC and QPA schemes. The evaluation is conducted under varying quantization resolutions ($n = 1, 2, 3$ bits) within a star-topology network comprising eight peripheral nodes. For the QPA scheme, multiple subinterval configurations are considered, specifically $s = 1, 2, 3$. The results are presented on a logarithmic scale, with the pre-reconciliation GKDR included as a baseline reference. As expected, increasing the subinterval numbers yields improved GKDR performance. Notably, the QPA scheme with $s = 3$ subintervals closely approaches the performance of the OSC method, demonstrating its effectiveness as a lightweight alternative.

To benchmark performance, Fig. 8 presents a comparison of the GKDR between the proposed scheme – incorporating OSC and QPA techniques – and conventional GSKG approach based on an irregular LDPC code with a rate of 1/2 in the binary domain. The code is constructed using the following variable node (VN) and check node (CN) degree distribution polynomials:

$$\lambda(x) = 0.28286x + 0.39943x^2 + 0.31771x^7,$$

$$\rho(x) = 0.6x^5 + 0.4x^6.$$

with a codeword length of $n_c = 2048$. Two LDPC decoding configurations are considered with $I = 10$ and $I = 100$ iterations.

The figure clearly illustrates that the proposed GSKG scheme achieves nearly equivalent GKDR performance to that of the conventional scheme employing 100 decoding iterations, while substantially reducing computational complexity. For instance,

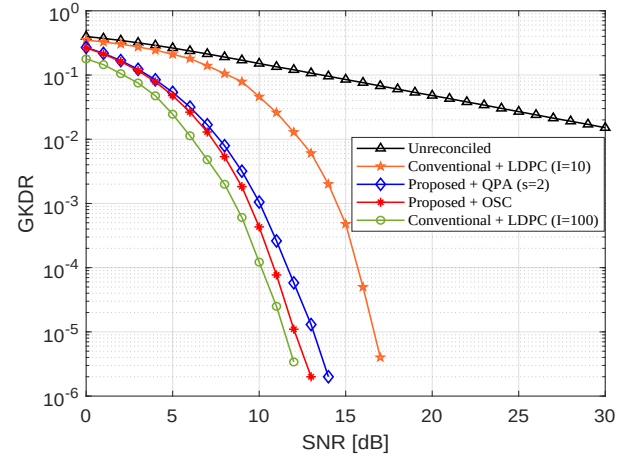


Fig. 8: Comparison of GKDR performance between the proposed scheme (using OSC and QPA) and conventional scheme based on an irregular LDPC code with rate 1/2.

considering $l = 1$, $n = 3$, $M = 10$, and $I = 100$, the computational complexity of the proposed scheme employing OSC/QPA is only $\mathcal{O}(43)$, compared to $\mathcal{O}(12,410,970)$ for the conventional LDPC-based approach. This highlights the practical advantages of the proposed low-complexity reconciliation approach in real-time and resource-constrained environments.

Given the challenging and time-intensive nature of real-world measurements, ray-tracing (RT) simulations were employed to evaluate the performance of the proposed scheme under realistic propagation conditions. Various indoor environments – such as angles of arrival and departure, path delays, and path gains – at each simulation point. These parameters were exported as text files and subsequently processed in *MATLAB* to generate coherent channel realizations. Figure 9 depicts one of the baseline RT simulation scenarios, consisting of eight peripheral nodes (Bobs), each represented by a red antenna placed in a separate room, and a central node (Alice) positioned in the main hall, denoted by a green antenna. For visual clarity, only the three strongest propagation paths between Alice and each Bob are illustrated in the figure.

To rigorously assess the performance of the proposed GSKG framework in complex, multipath-rich environments, a total of 10^4 independent simulation runs were conducted for the considered layout. In each run, the positions of all antennas were randomly varied within the indoor environment while preserving the overall spatial structure. Figure 10(a) presents representative examples of antenna placements across different simulation rounds. Furthermore, four passive eavesdroppers were positioned at fixed locations, each situated at a minimum distance of $\lambda/2$ from the legitimate nodes, and are indicated by black stars in Figure 10(a). These adversaries attempt to intercept the communication and infer the group key shared among the legitimate participants. To more accurately capture the richness and complexity of indoor wireless propagation, the simulation campaign incorporated the maximum number of multipath components per link. These components were coherently combined to produce a composite signal, whose amplitude was subsequently used for key generation. Figure 10(b) compares the GKDR performance of the proposed scheme for

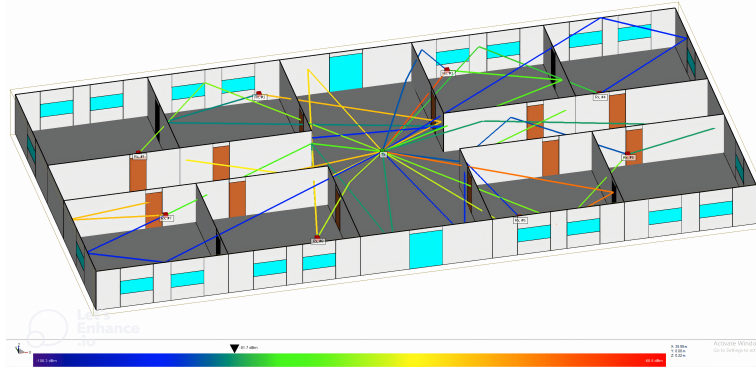


Fig. 9: Baseline RT scenario with one central node and eight peripheral nodes, each linked by three dominant propagation paths

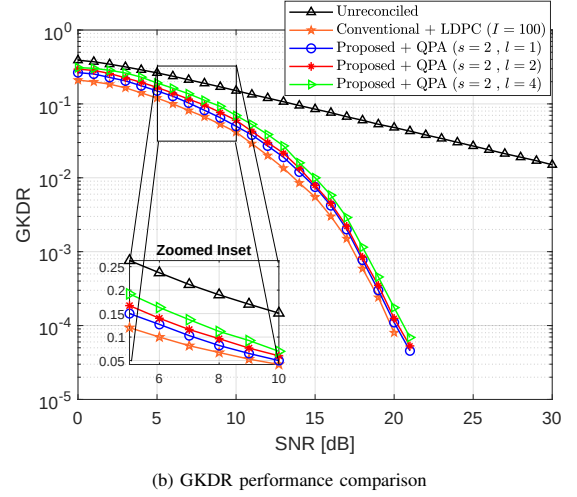
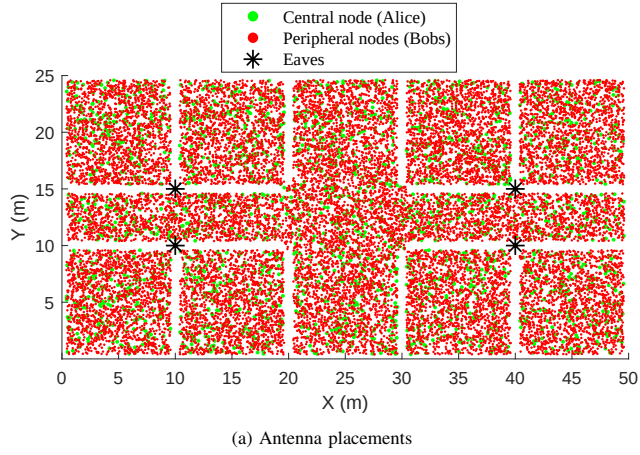


Fig. 10: RT simulations: **Left:** Representative antenna placements across simulation rounds with four fixed passive eavesdroppers; **Right:** GKDR performance of the proposed scheme for different key segment lengths ($l = 1, 2, 4$) compared with conventional approaches

different key segment lengths ($l = 1, 2, 4$) against conventional scheme.

Simulation results in Figure 10(b) demonstrate that the GKDR remains largely stable across varying numbers of key segments, with only a slight increase observed as l grows. This minor degradation may be attributed to the larger block size, which increases the likelihood of key mismatches. Moreover, the results demonstrate highly competitive performance compared to the conventional scheme employing LDPC with 100 decoding iterations for key reconciliation, highlighting the robustness and scalability of the proposed OSC/QPA techniques, even for longer group keys. In contrast to conventional methods that require multiple pairwise reconciliations and decoding steps, the proposed approach achieves efficient key expansion using a single probing round, linear helper data overhead, and no decoding complexity – resulting in up to a 99% reduction in computational cost. It is important to reiterate that key concatenation is an optional extension, intended to demonstrate the trade-off between key length and performance. The fundamental contribution of the proposed scheme lies in generating one key segment per observation.

2) *GKGR*: Figure 11 presents a comparison of the GKGR as a function of SNR for both the conventional scheme and the proposed scheme, evaluated using a single key segment ($l = 1$) under the OSC and QPA methods. The analysis

accounts for various quantization resolutions. The results clearly indicate that the proposed scheme achieves competitive GKGR performance relative to conventional approaches, even in the single-segment configuration. Notably, as the number of concatenated segments increases ($l > 1$), the proposed concatenation-based framework produces longer group keys per channel probe compared to conventional XOR-based schemes. This improvement stems from the framework's ability to efficiently aggregate high-entropy key material across multiple independently reconciled segments. As l increases, the total key length scales proportionally, highlighting the scheme's scalability and practical throughput benefits – making it particularly well-suited for high-performance and resource-constrained wireless environments.

3) *Uniformity and Randomness*: The proposed randomization strategy significantly enhances the uniformity of the generated group key distribution. The randomized key distribution exhibits a substantially lower deviation from the ideal uniform distribution, with a uniformity error (e_u) of 0.005, compared to 0.147 in the non-randomized case, thereby satisfying the criterion $e_u \leq 0.01$. This improvement ensures an approximately uniform symbol distribution across the entire key alphabet. Figure 12 illustrates the empirical key distributions for both the proposed and conventional schemes, clearly highlighting the enhancement achieved by the proposed

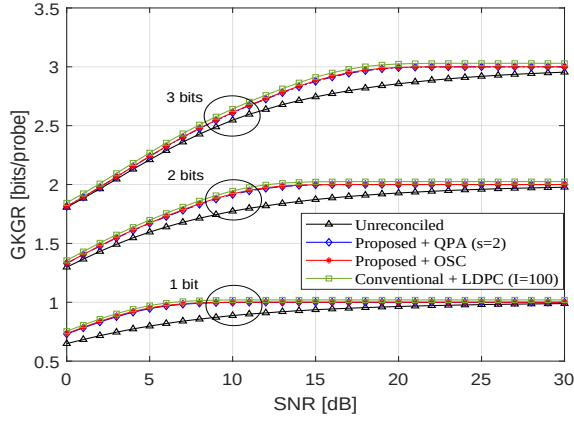


Fig. 11: GSKGR comparison of the proposed GSKG scheme using OSC and QPA techniques versus a conventional GSKG approach employing irregular LDPC codes

approach. Notably, this uniformity improvement is attained without introducing any additional computational overhead, in contrast to alternative post-processing methods such as non-linear quantization [36] or applying arithmetic coding [38].

To further assess the statistical randomness of the final group key sequences, the NIST statistical test suite [37] is applied. The analysis is performed at an average SNR of 15 dB, comparing the conventional and the proposed schemes, evaluated using a single key segment ($l = 1$). Due to sequence length limitations, a representative subset of nine NIST tests is selected for execution. The resulting p -values are visualized in the spider plot shown in Fig. 13, offering a comparative perspective on the statistical quality of the generated keys. As illustrated, the proposed scheme yields a marked improvement, with all tests consistently passed at the 99% confidence level. These results validate the cryptographic strength and unpredictability of the proposed group key sequences, demonstrating their robustness against statistical inference attacks. Additionally, we have extended the NIST analysis to configurations with higher key segment counts ($l = 2$ and $l = 4$). The results show minor declines in p -values – 1.1% and 1.9%, respectively – reflecting the increased redundancy introduced by correlations among segments derived from the same channel observation.

VI. DISCUSSION

A. Eavesdropping Resilience and Spatial Decorrelation

In our setup – consistent with established practices in the physical-layer key generation literature – Eve is positioned at a distance of at least $\lambda/2$ from both Alice and each Bob. This spatial separation ensures that the wiretap channel remains uncorrelated with the legitimate channels, thereby preventing Eve from obtaining useful information about the secret key. In both the OSC and QPA – unified reconciliation and group key distribution schemes – the helper information – specifically, the grid shift in OSC and the quantization pattern index in QPA – is transmitted over a public channel. Although a passive eavesdropper (Eve) may intercept this information and attempt to replicate the transformation using her own channel observations, such attempts are fundamentally ineffective. Owing to the spatial decorrelation characteristic of wireless propagation, Eve’s channel remains statistically

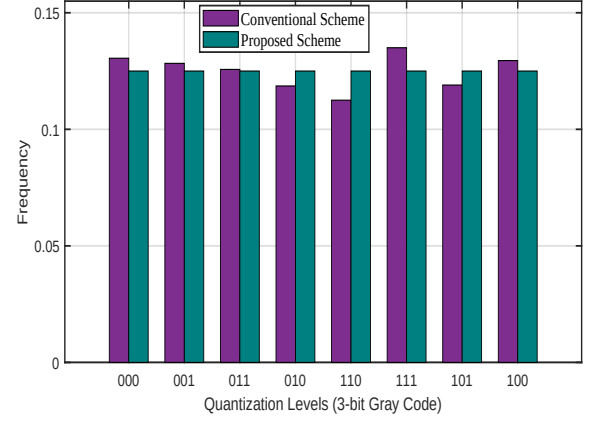


Fig. 12: Comparison of normalized empirical codeword distributions between the proposed and conventional schemes

uncorrelated with those of the legitimate users, precluding her from extracting any meaningful insights about the final key.

B. Information-Theoretic Security

The proposed GSKG scheme aims to provide strong information-theoretic security against passive adversaries. It avoids the use of traditional redundancy-bearing reconciliation mechanisms, such as LDPC-based Slepian-Wolf encoding, which are known to leak partial information about the secret key. In typical pairwise LDPC-based reconciliation schemes, such as the syndrome approach, each helper message is computed as $S_i = K_i \cdot H^T$, where H is a parity-check matrix. This helper data confines the possible values of K_i to a specific coset of the LDPC code, thereby reducing the key entropy from the eavesdropper’s perspective. In contrast, the proposed scheme transmits only shift values or quantization pattern indices designed to assist legitimate users in aligning with a preselected group key $\mathcal{K}_G^A$, without revealing significant structural information about $\mathcal{K}_G^A$ itself. This design reduces helper data leakage and supports information-theoretic secrecy, provided the helper information is statistically independent of $\mathcal{K}_G^A$ from the adversary’s viewpoint.

Although the helper data (e.g., the shift value δ_{A_i}) is deterministically computed based on the selected group key and Alice’s private observation m_{A_i} , it does not reduce the entropy of the group key from the adversary’s perspective. Since Eve lacks access to m_{A_i} , she cannot infer the group key from the helper data alone. Under this assumption, the mutual information $I(\mathcal{K}_G^A; \delta_{A_i})$ remains negligible, and the helper data does not compromise the secrecy of $\mathcal{K}_G^A$. This implies that the entropy of $\mathcal{K}_G^A$ is largely preserved and that its confidentiality remains protected even against a computationally unbounded passive eavesdropper. As a result, the transmission of helper data for group key alignment and distribution leaks negligible information to Eve, preserving the information-theoretic security of the proposed scheme. Revisiting Fig. 6(b), we evaluate a scenario in which Eve applies the same grid shift as the Bobs. The resulting effect is illustrated in Fig. 14, which clearly shows that Eve’s quantized values remain incoherent with those of the legitimate nodes.

The observed average KDR between the group keys shared by Alice and the Bobs, and those estimated by Eve, is 0.4793,

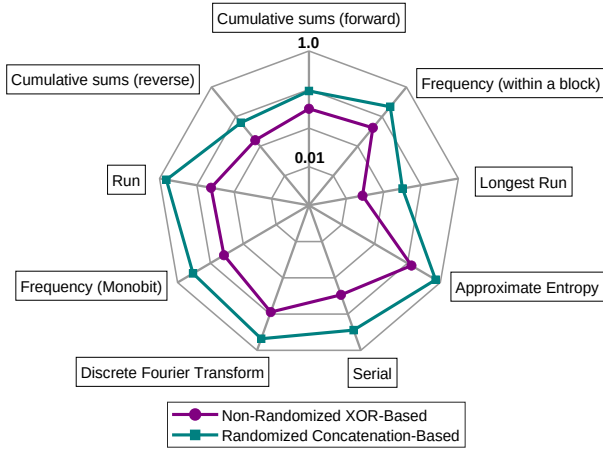


Fig. 13: NIST test p -values for group keys generated using the proposed and conventional schemes

which closely approximates the theoretical ideal of 0.5. This suggests that Eve's ability to infer the key is effectively equivalent to random guessing — akin to flipping a fair coin for each bit, with no significant information advantage. Furthermore, the near-uniform distribution of the generated group keys, as illustrated in Fig. 12, enhances the entropy and unpredictability of the key material, thereby strengthening its resistance to inference-based key recovery attacks.

C. Channel Dynamics and Entropy Limitations

We acknowledge that when multiple key segments are derived from a single channel observation, the entropy of the resulting concatenated key is not strictly additive due to inherent temporal or spatial correlations. While the publicly shared shift values do not directly reveal key material, they may inadvertently assist an adversary if the underlying channel observations are partially or fully exposed. This reflects a fundamental trade-off: concatenation extends key length and supports integration with standardized symmetric-key cryptographic algorithms (e.g., 128-bit AES), but must be applied cautiously to avoid overestimating the true entropy.

The proposed GSKG scheme exploits the temporal variability of reciprocal channel features to ensure adequate entropy for secure key generation. Nevertheless, in fully static environments, the mutual observations between Alice and the Bobs may exhibit high correlation and reduced randomness, which in turn lowers the effective key entropy, diminishes the key generation rate, and degrades the statistical uniformity of the resulting keys. To address performance degradation in fully static environments, a variety of entropy-enhancement strategies have been proposed in the literature. These include the introduction of artificial randomness through local perturbations or synthetic sequences, exploitation of multipath propagation and fading characteristics, advanced channel probing techniques, and helper-assisted methods — such as reconfigurable intelligent surfaces (RIS) — that induce channel dynamics via random beamforming or phase shifting. Notably, the KGPT framework [39] employs controlled power-level variations at the transmitter to generate artificial channel fluctuations, thereby enabling robust key extraction even under static fading conditions. In our proposed scheme, this challenge is mitigated

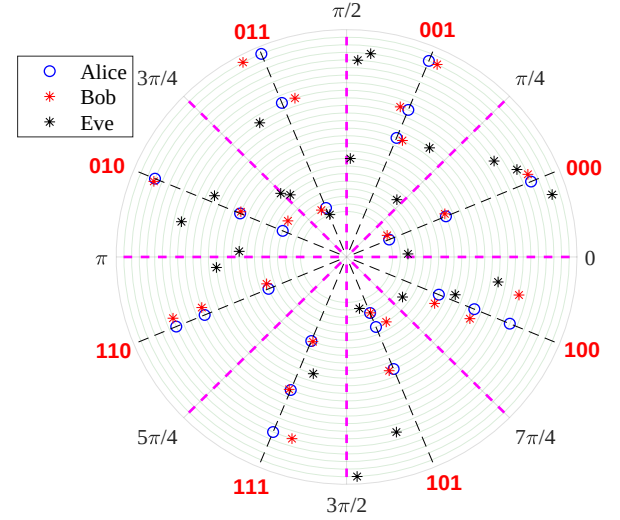


Fig. 14: Eve's reconciled output after applying the same reconciliation shift as Bob, compared to the original measurements of Alice and Bob

through a random group key selection mechanism, wherein Alice randomly selects a quantization region from the full quantization space. This randomness enhances the statistical uniformity of the generated keys, even in scenarios with limited channel variability. Simulations demonstrate that, under low-mobility conditions — modeled by periodically relocating Alice and the Bobs — natural temporal variations in the channel persist across successive frames. In such settings, the random key selection performed by Alice effectively maintains both the entropy and uniformity of the generated keys, thereby supporting reliable key generation despite reduced channel dynamics.

D. Applications and Deployment Scenarios

The findings of this study have broad applicability across domains where secure communication, low latency, and scalable key management are critical. In particular, IoT networks, vehicular ad-hoc networks (VANETs), and drone swarms stand to benefit significantly from the proposed group-wise key generation mechanism implemented in a star topology. In IoT networks — characterized by constrained power resources, dynamic and heterogeneous topologies, and high device density — the ability to securely establish cryptographic keys with minimal computational and communication overhead is crucial for scalability and energy efficiency. The proposed scheme meets these demands by enabling lightweight and distributed group key generation, specifically tailored to the operational constraints of IoT devices. In VANETs, where ultra-low latency and high reliability are essential for real-time decision-making and cooperative safety applications, rapid and decentralized group key establishment is essential. The proposed method facilitates dynamic and on-the-fly group key updates without incurring excessive overhead, thereby supporting secure inter-vehicle communication in highly mobile environments. Similarly, drone swarms — deployed in mission-critical operations such as surveillance, reconnaissance, and search-and-rescue — require robust coordination and strong security guarantees. The proposed key generation protocol ensures the confidentiality,

integrity, and freshness of communications among multiple autonomous aerial agents, reinforcing their resilience against eavesdropping and manipulation. Across all these domains, minimizing power consumption and reducing latency during key generation are paramount, particularly as systems scale in size and complexity. The proposed approach addresses these requirements by offering a low-complexity, scalable, and secure group key establishment framework suitable for resource-constrained and latency-sensitive environments. A detailed adaptation and optimization of the protocol for each application-specific setting (e.g., mobility models, traffic patterns, and hardware capabilities) represents a promising avenue for future research.

VII. CONCLUSION

This paper has presented a novel and efficient GSKG framework designed for wireless networks operating in a star topology. The proposed approach addresses the scalability, complexity, and latency challenges inherent in conventional pairwise key establishment methods. By allowing the central node to directly select a group key uniformly from the quantization space – thus eliminating the need for intermediate pairwise key establishment – the scheme significantly reduces both computational complexity and communication overhead. To ensure consistent and reliable key reconstruction at the peripheral nodes, we proposed QPA, a lightweight and non-coding reconciliation technique. Unlike conventional methods based on error-correcting codes, QPA achieves high alignment accuracy with minimal complexity, making it well-suited for dynamic and resource-constrained wireless environments. QPA circumvents the complexities of conventional channel coding while achieving high alignment accuracy, thereby streamlining the overall protocol. Its seamless integration into the group key distribution process makes the approach particularly suitable for dynamic and resource-constrained wireless environments. Furthermore, a concatenation-based key construction strategy was employed to enhance key throughput by leveraging bidirectional channel measurements. This technique enables the extraction of multiple independent key segments without requiring additional probing, thereby improving overall efficiency. Simulation results demonstrate the effectiveness of the proposed scheme in terms of key disagreement rate, key generation rate, and resilience against passive eavesdropping. In particular, the near-ideal randomness and uniformity of the generated keys validate the information-theoretic security of the approach.

REFERENCES

- [1] T. M. Fernández-Caramés, “From pre-quantum to post-quantum IoT security: A survey on quantum-resistant cryptosystems for the internet of things,” *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6457–6480, 2020.
- [2] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, “Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities,” *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8169–8181, 2019.
- [3] Y. Peng, P. Wang, W. Xiang, and Y. Li, “Secret key generation based on estimated channel state information for TDD-OFDM systems over fading channels,” *IEEE Transactions on Wireless Communications*, vol. 16, no. 8, pp. 5176–5186, 2017.
- [4] S. Zhang, L. Jin, Y. Lou, and Z. Zhong, “Secret key generation based on two-way randomness for TDD-SISO system,” *China Communications*, vol. 15, no. 7, pp. 202–216, 2018.
- [5] J. M. Hamamreh, H. M. Furqan, and H. Arslan, “Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1773–1828, 2019.
- [6] Y. Liu, H.-H. Chen, and L. Wang, “Physical layer security for next generation wireless networks: Theories, technologies, and challenges,” *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 347–376, 2016.
- [7] H. V. Poor and R. F. Schaefer, “Wireless physical layer security,” *Proceedings of the National Academy of Sciences*, vol. 114, no. 1, pp. 19–26, 2017.
- [8] N. Aldaghri and H. Mahdavi, “Physical layer secret key generation in static environments,” *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2692–2705, 2020.
- [9] N. Patwari, J. Croft, S. Jana, and S. K. Kasper, “High-rate uncorrelated bit extraction for shared secret key generation from channel measurements,” *IEEE Transactions on Mobile Computing*, vol. 9, no. 1, pp. 17–30, 2010.
- [10] Z. Ji, Y. Zhang, Z. He, P. L. Yeoh, B. Li, H. Yin, Y. Li, and B. Vucetic, “Wireless secret key generation for distributed antenna systems: A joint space-time-frequency perspective,” *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 633–647, 2021.
- [11] A. Alashqar, E. O. Torshizi, R. Mesleh, and W. Henkel, “Shared cross-prediction neural network for efficient key generation in IoT networks,” in *2025 14th International ITG Conference on Systems, Communications and Coding (SCC)*, 2025, pp. 1–6.
- [12] —, “Secret key generation driven by attention-based convolutional autoencoder and quantile quantization for IoT security in 5G and beyond,” *IEEE Access*, vol. 13, pp. 131 744–131 756, 2025.
- [13] H. Ruotsalainen, J. Zhang, and S. Grebeniuk, “Experimental investigation on wireless key generation for low-power wide-area networks,” *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 1745–1755, 2020.
- [14] E. Olyaei Torshizi and W. Henkel, “Pairwise physical layer secret key generation for FDD systems,” *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 9518–9533, 2024.
- [15] —, “Exploiting FDD channel reciprocity for physical layer secret key generation in IoT networks,” *IEEE Communications Letters*, vol. 28, no. 6, pp. 1268–1272, 2024.
- [16] E. O. Torshizi, U. Upreti, and W. Henkel, “Highly efficient FDD secret key generation using ESPRIT and jump removal on phase differences,” in *2022 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2022, pp. 1–6.
- [17] G. Li, A. Hu, C. Sun, and J. Zhang, “Constructing reciprocal channel coefficients for secret key generation in FDD systems,” *IEEE Communications Letters*, vol. 22, no. 12, pp. 2487–2490, 2018.
- [18] W. Wang, H. Jiang, X. Xia, P. Mu, and Q. Yin, “A wireless secret key generation method based on chinese remainder theorem in FDD systems,” *Science China Information Sciences*, vol. 55, pp. 1605–1616, 2012.
- [19] X. Zhang, G. Li, J. Zhang, A. Hu, Z. Hou, and B. Xiao, “Deep-learning-based physical-layer secret key generation for FDD systems,” *IEEE Internet of Things Journal*, vol. 9, no. 8, pp. 6081–6094, 2021.
- [20] Q. Wang, H. Su, K. Ren, and K. Kim, “Fast and scalable secret key generation exploiting channel phase randomness in wireless networks,” in *2011 Proceedings IEEE INFOCOM*, 2011, pp. 1422–1430.
- [21] C. D. T. Thai, J. Lee, J. Prakash, and T. Q. S. Quek, “Secret group-key generation at physical layer for multi-antenna mesh topology,” *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 1, pp. 18–33, 2019.
- [22] H. Liu, J. Yang, Y. Wang, Y. Chen, and C. E. Koksall, “Group secret key generation via received signal strength: Protocols, achievable rates, and implementation,” *IEEE Transactions on Mobile Computing*, vol. 13, no. 12, pp. 2820–2835, 2014.
- [23] P. Xu, K. Cumanan, Z. Ding, X. Dai, and K. K. Leung, “Group secret key generation in wireless networks: Algorithms and rate optimization,” *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 8, pp. 1831–1846, 2016.
- [24] Y. Wei, C. Zhu, and J. Ni, “Group secret key generation algorithm from wireless signal strength,” in *2012 Sixth International Conference on Internet Computing for Science and Engineering*, 2012, pp. 239–245.
- [25] I. Csizsar and P. Narayan, “Secrecy capacities for multiple terminals,” *IEEE Transactions on Information Theory*, vol. 50, no. 12, pp. 3047–3061, 2004.
- [26] C. Ye and A. Reznik, “Group secret key generation algorithms,” in *2007 IEEE International Symposium on Information Theory*. IEEE, 2007, pp. 2596–2600.

- [27] S. Xiao, Y. Guo, K. Huang, and L. Jin, "Cooperative group secret key generation based on secure network coding," *IEEE Communications Letters*, vol. 22, no. 7, pp. 1466–1469, 2018.
- [28] L. Jiao, P. Wang, N. Wang, S. Chen, A. Alipour-Fanid, J. Le, and K. Zeng, "Efficient physical layer group key generation in 5G wireless networks," in *2020 IEEE Conference on Communications and Network Security (CNS)*, 2020, pp. 1–9.
- [29] T. Tang, T. Jiang, and W. Zou, "Group secret key generation in physical layer, protocols and achievable rates," in *2017 17th International Symposium on Communications and Information Technologies (ISCIT)*, 2017.
- [30] R. Guillaume, F. Winzer, A. Czylik, C. T. Zenger, and C. Paar, "Bringing PHY-based key generation into the field: An evaluation for practical scenarios," in *2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall)*, 2015, pp. 1–5.
- [31] G. Li, A. Hu, J. Zhang, L. Peng, C. Sun, and D. Cao, "High-agreement uncorrelated secret key generation based on principal component analysis preprocessing," *IEEE Transactions on Communications*, vol. 66, no. 7, pp. 3022–3034, 2018.
- [32] J. Etesami and W. Henkel, "LDPC code construction for wireless physical-layer key reconciliation," in *2012 1st IEEE International Conference on Communications in China (ICCC)*, 2012, pp. 208–213.
- [33] L. Lai, Y. Liang, and H. V. Poor, "A unified framework for key agreement over wireless fading channels," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 480–490, 2012.
- [34] H. Zhou, L. M. Huie, and L. Lai, "Secret key generation in the two-way relay channel with active attackers," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 3, pp. 476–488, 2014.
- [35] L. Lai, Y. Liang, and W. Du, "Cooperative key generation in wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 8, pp. 1578–1588, 2012.
- [36] E. O. Torshizi and W. Henkel, "Reciprocity and secret key generation for FDD systems using non-linear quantization," in *2022 IEEE Globecom Workshops (GC Wkshps)*, 2022, pp. 927–932.
- [37] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Booz-allen and hamilton inc mclean va, Tech. Rep., 2001.
- [38] A. Said, "Introduction to arithmetic coding-theory and practice," *arXiv preprint arXiv:2302.00819*, 2023.
- [39] X. Huan, K. Miao, J. Liu, C. Wu, W. Chen, R. Pei, and H. Hu, "KGPT: Wireless key generation based on power tuning for static Internet-of-Things," *IEEE Transactions on Industrial Informatics*, vol. 21, no. 3, pp. 2610–2619, 2025.



Anas Alashqar earned his B.Sc. in Communication and Software Engineering from Al-Balqa Applied University, Jordan, in 2012, followed by an M.Sc. in Electrical Engineering with a focus on Wireless Networks from Princess Sumaya University for Technology, Jordan, in 2020. He is currently pursuing a Ph.D. in Electrical Engineering at Constructor University, Germany. He has served as a Teaching and Research Assistant, as well as a Quality Coordinator, at the School of Electrical Engineering and Information Technology at the German Jordanian University, Jordan. Mr. Alashqar's research interests include physical layer security (PLS), deep learning, the Internet of Things (IoT), wireless communications networks, and software-defined radio (SDR).



Werner Henkel (Senior Member, IEEE) received his Diploma and Dr.-Ing. (Ph.D.) degree from Darmstadt University of Technology (TUD) in May 1984 and June 1989, respectively. Thereafter, stages were: Deutsche Telekom's R&D Labs in Darmstadt, sabbatical at AT&T Bell Laboratories (later Lucent), Telecommunications Research Center Vienna, City University Bremen. Earlier teaching was at the universities of Kaiserslautern and Vienna. Since September 2003 he is a professor for electrical engineering at Constructor University, formerly Jacobs University

and International University of Bremen chairing the ECE program from its existence until 2022. He was elected Dean from April 2012 to June 2014. He was adjunct faculty at ODU, Norfolk, VA in 2015. Courses taught are: Coding Theory; Information Theory; Data Compression, Compressive Sensing, and Modern Coding; Digital Signal Processing; Signals & Systems; Wireline Communications (DSL); Measurement automation; Circuits; and Statistical Analysis and Simulation. Dr. Henkel was involved in organizing or serving on the TPC for: ISIT 1997, IEEE J-SAC, June 2002, International Zurich Seminar 2004, EUSIPCO 2004 and 2007, ICC 2006, 2017 - 2026, Turbo Symposia (ISTC) 2008, 2010, 2014, 2016, 2018, 2020/21, 2023, IWCMC 2022 Sec. Symp., GC 2022 WS '5GBeyond', INFOCOM Wireless-Sec 2023, Globecom 2024 IEEE NExtG Wisec, and SampTA 2013. Publications are in the areas of coding, iterative decoding, unequal error protection, coded modulation, joint source-channel coding, network coding, frame synchronization, channel modeling, impulse noise, DSL, Power Line, single- and multicarrier transmission, multi-user communication, MIMO, DNA analysis, physical-layer security, and TEMPEST.



Ehsan Olyaei Torshizi (Member, IEEE) received his B.Sc. degree with distinction in 2009 and his M.Sc. degree with honors in 2012, both in communications engineering in Iran. From 2013 to 2021, he held various positions in industry as a wireless communications and signal processing engineer. In December 2021, he joined the Transmission Systems Group at Constructor University Bremen (formerly Jacobs University Bremen), Germany, as a Research Associate and Lecturer. He was awarded the DAAD (German Academic Exchange Service) Prize 2025 by

Constructor University in recognition of his outstanding academic achievements. He has served as a Technical Program Committee (TPC) member for the IEEE PIMRC 2025 – Fundamentals and PHY Track and has reviewed over 100 papers for top-tier IEEE and ACM journals and conferences. His research interests include physical-layer security (PLS), secret key generation, LDPC codes, compressed sensing, signal processing, power line communications, multiuser communications, MIMO systems, deep learning, the Internet of Things (IoT), and TEMPEST.