A Lightweight and Efficient Key Generation Scheme From OFDM Subcarriers' Channel Responses

Agnes Francis Kawoya, Hua Wang, *Member, IEEE*, and Dongxuan He

***Abstract*—This letter presents a physical layer secret key generation (PLSKG) protocol utilizing the amplitude of channel frequency response (CFR) of Orthogonal Frequency Division Multiplexing (OFDM) subcarriers. Firstly, least squares estimation estimates the CFR. Next, a partition moving average (PMA) algorithm encodes the CFR. PMA re-uses the CFR within a partition by encoding at different overlap sizes, thus increasing the key generation rate (KGR). Then, a 2-bit differential-based quantization at every overlap for each partition is followed for an improved KGR and randomness. Finally, a cyclic redundancy check is performed to select strings with consistent results as candidate key, eliminating streams from less correlated measurements, thus ensuring a 0-bit mismatch. Simulation results have verified that our scheme achieves random 0-bit disagreement keys with a high average key length and reduced complexity compared to the other existing lightweight schemes.**

***Index Terms*—Physical layer security, key generation, quantization.**

I. Introduction

THE FEASIBILITY of using OFDM subcarriers' channel responses for key generation was studied in [1]. It was further employed for lightweight key generation in [2]. PLSKG is based on three principles, namely channel reciprocity, temporal variation, and spatial decorrelation [2], [3]. Channel reciprocity allows the nodes to obtain highly correlated channel measurements and generate identical keys. Temporal variation of the signal induces randomness for the extraction of cryptographic keys. Spatial decorrelation ensures that an eavesdropper situates more than a few wavelengths from either legitimate node can hardly get the observation of a legitimate channel and thus can not guess the key.

A typical PLSKG protocol consists of four stages: 1) channel probing; 2) quantization; 3) information reconciliation; and 4) privacy amplification [2], [3], [4]. In the channel probing stage, nodes extract a physical property of the channel. Through quantization, the nodes convert the channel measurements into consistent binary sequences, i.e., initial keys. Key mismatch between nodes after the quantization is expected due to the channel variation, hardware asymmetry, and noise. Information reconciliation is thus employed to remove the mismatch. Finally, privacy amplification is implemented to eliminate the information leaked during the previous process. The core stages that differentiate the implementation complexity of PLSKG protocols are quantization and information reconciliation.

Quantization may be absolute value-based, where measurements are compared to thresholds for binary assignment, or differential-based, which captures the relative change of channel measurements. The latter is much more lightweight for implementation [5]. Differential quantization was first introduced in [6]. It has been implemented for lightweight key generation in [2], [5], [7], [8]. In [2], channel measurements are pre-processed with a moving average filter (MAF). They develop a cascade information reconciliation with fewer information interactions to lower implementation complexity. In [5], the differential-based quantization (DBQ) algorithm introduces a resolution parameter of the channel measurements such that channel measurements having variation smaller than the threshold are thus dropped for an improved key agreement rate (KAR). They employ an error correcting code (ECC) for a secure sketch information reconciliation, particularly the BCH(15,3,5), which can correct up to 20% mismatch. In [7], the quantization and information reconciliation is similar to [5] but without a resolution parameter. Privacy amplification is adopted in all works to remove information leakage through a hash function. Finally, [8] includes a pre-processing of channel measurements, moving average coding (MAC) algorithm, before developing a fuzzy extractor during a 2-bit DBQ scheme for a secure sketch information reconciliation. Unlike existing PLSKG protocols, our proposed protocol only contains channel probing and quantization stages. Authors in [2] adopt a pre-process that decreases the number of measurements for an increased KAR, which is at the cost of KGR. Our proposed pre-process aims to keep the same number of measurements and thus have a higher KGR. Likewise in [5], the DBQ drops channel measurements, which decreases KGR, and they quantize them to one bit per measurement. Our proposed scheme is a 2-bit DBQ and inherits higher KGR and KAR. The work in [8] uses quantization as a fuzzy extractor for information reconciliation stage, it has increased processing compared to our proposed scheme.

In this letter, we propose a lightweight PLSKG protocol. The proposed protocol eliminates the information reconciliation cost by generating keys that match after the quantization stage, and privacy amplification is not required, making it more lightweight. The main contributions are summarized as follows: 1) A novel partition moving average

Manuscript received 27 July 2024; accepted 7 September 2024. Date of publication 11 September 2024; date of current version 8 November 2024. This work was supported in part by the State Key Laboratory of Wireless Mobile Communications, China Academy of Telecommunications Technology (CATT); in part by Datang Linktester Technology Company Ltd; and in part by the National Natural Science Foundation of China under Grant 62101306. The associate editor coordinating the review of this article and approving it for publication was T. Xu. *(Corresponding author: Agnes Francis Kawoya; Hua Wang.)*

Agnes Francis Kawoya is with the School of Information and Electronics, Beijing Institute of Technology, Beijing 100081, China, and also with the Department of Electronics and Telecommunications Engineering, University of Dodoma, Dodoma 490, Tanzania (e-mail: agneskawoya@gmail.com).

Hua Wang and Dongxuan He are with the School of Information and Electronics, Beijing Institute of Technology, Beijing 100081, China (e-mail: wanghua@bit.edu.cn; hedongxuan@bit.edu.cn).

Digital Object Identifier 10.1109/LWC.2024.3457752

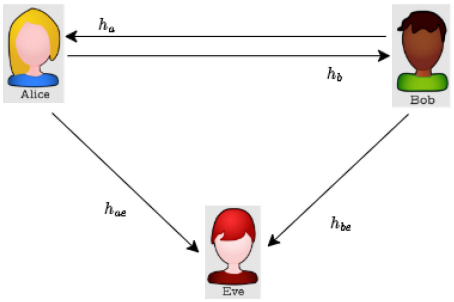

Fig. 1. Wireless communication model with eavesdropping.

(PMA) pre-processing algorithm is proposed to isolate highly correlated regions of the channel measurements. 2) The pre-processing algorithm allows the estimated CFR within a partition to be re-used for key generation, thus increasing the KGR. 3) a cyclic redundancy check (CRC) step is included in the quantization, which has a two-fold advantage. Firstly, it ensures 0-bit disagreement keys by selecting bit streams from highly correlated partitions. Secondly, if the CRC calculated by Alice and Bob are inconsistent, then different parameters are selected for the PMA to re-quantize, and nodes do not return to the first stage of channel probing, as is the case with schemes of [2], [5], [7].

The rest of this letter is organized as follows. Section II describes the system model. We introduce the proposed PLSKG protocol in Section III, discuss the performance in Section IV, and conclude in Section V.

II. System Model

A. Eavesdropping Model

We consider a time-division duplexing (TDD)-based OFDM wireless communication system over multipath fading channels. As shown in the wireless eavesdropping model Fig. 1, Alice (A) and Bob (B) are legitimate nodes which communicate with each other in the presence of a passive eavesdropper, Eve (E). Eve is assumed to obey the following assumptions common to most key generation schemes based on physical layer methods [2], [9]. Eve remains passive to avoid exposure to the legitimate nodes. She locates a few wavelengths away from Alice or Bob to avoid being noticeable, thus ensuring the spatial decorrelation requirement of PLSKG. Eve can measure the channel of the Alice-Eve and Bob-Eve links.

B. Channel Representation

Assuming a tapped-delay-line (TDL) model, the complex low-pass equivalent channel impulse response characterized by delay, τ, and with P delayed multipaths, $h(\tau, t)$ can be written as

$$h(\tau, t) = \sum_{p=1}^{P} h_p(\tau_p, t)\delta(\tau - \tau_p) \tag{1}$$

where $\delta(.)$ denotes the Dirac delta function, and h_p and τ_p are the attenuation coefficient and delay of the p-th path at time t, respectively. The CFR, $\mathbf{H}(f_k, t)$, of the k-th ($k \in \{0, 1, \ldots, K-1\}$ with K being the total number of subcarriers) subcarrier with frequency f_k is obtained by applying IFFT operation to $h(\tau, t)$

$$\mathbf{H}(f_k, t) = \sum_{p=1}^{P} h_p(\tau_p, t)\exp(-j2\pi f_k \tau_p). \tag{2}$$

The frequency-domain representation of the received signal can be given by

$$\mathbf{Y}(f_k, t) = \mathbf{H}(f_k, t)\mathbf{X}(f_k) + \mathbf{Z}(f_k, t) \tag{3}$$

where $\mathbf{X}(f_k)$ is the pilot signal and $\mathbf{Z}(f_k, t)$ is additive white Gaussian noise (AWGN) of a zero mean normal distribution of variance σ^2. We get the least square estimation of CFR as [2], [9]

$$\hat{\mathbf{H}}(f_k, t) = \frac{\mathbf{Y}(f_k, t)}{\mathbf{X}(f_k)} = \mathbf{H}(f_k, t) + \hat{\mathbf{Z}}(f_k, t) \tag{4}$$

where

$$\hat{\mathbf{Z}}(f_k, t) = \frac{\mathbf{Z}(f_k, t)}{\mathbf{X}(f_k)} \tag{5}$$

is the channel estimation error. Details of the modulation scheme may be referenced in [1], they have been omitted from this letter for brevity.

C. Channel Estimation

Generally, Alice is the initiator of channel probing. Let Alice send the pilot signal to Bob at time t_a, and within the coherence time of the channel, T_c, Bob responds to Alice at time t_b. From (4), their CFR estimates can be obtained as

$$\hat{\mathbf{H}}_a(f_k, t_a) = \mathbf{H}(f_k, t_a) + \hat{\mathbf{Z}}(f_k, t_a) \tag{6}$$

$$\hat{\mathbf{H}}_b(f_k, t_b) = \mathbf{H}(f_k, t_b) + \hat{\mathbf{Z}}(f_k, t_b). \tag{7}$$

$\hat{\mathbf{Z}}(f_k, t_a)$ and $\hat{\mathbf{Z}}(f_k, t_b)$ are independent and identically distributed (i.i.d) Gaussian variables.

III. Key Generation Protocol

Our protocol only has channel probing and quantization stages. The quantization includes a pre-processing step, a 2-bit DBQ and a CRC checksum step. This section details each stage separately and concludes with a security analysis.

A. Channel Probing

Channel probing is done to estimate the OFDM subcarriers' CFR amplitude, as explained in Section II. The interval between the signals sent by Alice and Bob, Δt, is less than T_c, i.e., $\Delta t < \frac{1}{f_d}$, where f_d is the Doppler spread of the channel.

B. Quantization

1) PMA algorithm: Before quantization, a pre-processing step is added to isolate highly correlated regions of the measured CFR estimates. Alice and Bob perform the same operation. We take Alice as an example for illustration. The estimated CFR, $\hat{\mathbf{H}}_a(f_k, t_a) = [\hat{\mathbf{H}}_a(f_0, t_a), \hat{\mathbf{H}}_a(f_1, t_a), \ldots, \hat{\mathbf{H}}_a(f_{K-1}, t_a)]^T$, are divided

sequentially to l equal partitions. Let $\hat{\mathbf{H}}_a^q[i]$ be a vertical concatenation of $\hat{\mathbf{H}}_a(f_k, t_a)[q]$, given by

$$\hat{\mathbf{H}}_a^q[i] = \begin{bmatrix} \hat{\mathbf{H}}_a(f_k, t_a)[q] \\ \hat{\mathbf{H}}_a(f_k, t_a)[q] \\ \vdots \\ \hat{\mathbf{H}}_a(f_k, t_a)[q] \end{bmatrix}_{z(w-v+1)\times 1}, \tag{8}$$

where $i = 1, 2, \ldots, z(w-v+1)$, $q = 1, 2, \ldots, l$. $\hat{\mathbf{H}}_a^q[i]$ is the i-th estimate of the q-th partition and z is the total number of estimated CFR within a partition.

The PMA pre-processing can be described as

$$\tilde{\mathbf{H}}_a^{q,v}[m] = \frac{\sum_{i=(m-1)(w-v)+1}^{(m-1)(w-v)+w} \hat{\mathbf{H}}_a^q[i]}{w}, m = 1, 2, 3, \ldots, M \tag{9}$$

where $\tilde{\mathbf{H}}_a^{q,v}[m]$ is the m-th measurement of the q-th partition and overlap v after PMA, w and v are the window and overlap sizes of the cyclic moving average, respectively. M is the length of the PMA output, $M = z$, PMA does not decrease the number of measurements available for quantization. Eq. (9) describes a cyclic overlapping sliding window operation where w and v are bounded. The window size must be less than z, the overlap size must be greater than half the window size to allow cycling the partition to obtain distinct groups of the same number as the partition size, i.e., $w < z$ and $\frac{w}{2} < v < w$ [8]. For a selected w, the PMA operation is performed for several values of $v = \{v_1, v_2, \ldots, v_n\}$, where $n = |v|$, $|\cdot|$ denotes the cardinality, thus allowing the same data to be re-used for key generation. The PMA output $[\tilde{\mathbf{H}}_a^{q,v}[1], \tilde{\mathbf{H}}_a^{q,v}[2], \ldots, \tilde{\mathbf{H}}_a^{q,v}[M]]^T$ may be represented by matrix $\mathbf{A} \in \mathbb{R}^{z\times 1}$ as

$$\mathbf{A} = \frac{1}{\lambda} \times \mathbf{I_p C W} \tag{10}$$

where the circulant matrix $\mathbf{C} \in \mathbb{R}^{z\times z}$ is a Toeplitz matrix having the form,

$$\mathbf{C} = \begin{bmatrix} \hat{\mathbf{H}}_a(f_0, t_a)[q] & \hat{\mathbf{H}}_a(f_1, t_a)[q] & \ldots & \hat{\mathbf{H}}_a(f_{z-1}, t_a)[q] \\ \hat{\mathbf{H}}_a(f_{z-1}, t_a)[q] & \hat{\mathbf{H}}_a(f_0, t_a)[q] & \ldots & \hat{\mathbf{H}}_a(f_{z-2}, t_a)[q] \\ \vdots & \ddots & \ddots & \vdots \\ \hat{\mathbf{H}}_a(f_1, t_a)[q] & \hat{\mathbf{H}}_a(f_2, t_a)[q] & \ldots & \hat{\mathbf{H}}_a(f_0, t_a)[q] \end{bmatrix} \tag{11}$$

$\mathbf{I_p}^{z\times z}$ is the matrix whose rows are selected from the identity matrix, $\mathbf{I}^{\mathbf{z}\times\mathbf{z}}$, as described in Algorithm 1. λ is the window size w, while $\mathbf{W}^{\mathbf{z}\times\mathbf{1}}$ is the block matrix of the form

$$\mathbf{W} = \begin{bmatrix} \mathbf{1}^{w\times 1} \\ \mathbf{0}^{(z-w)\times 1} \end{bmatrix} \tag{12}$$

Observed in Fig. 2, the 3^{rd} partition is the most uncorrelated while the 2^{nd} has the most correlated measurements. Keys generated from the 2^{nd} partition will have higher KAR compared to those generated from the 3^{rd}. It would be beneficial to avoid the 3^{rd} partition.

2) 2-bit DBQ: The differential-based quantization method is adopted. $\tilde{\mathbf{H}}_a^{q,v}[m]$ is quantized according to the following rule,

$$K_m^{q,v} = \begin{cases} 1, \text{ if } \tilde{\mathbf{H}}_a^{q,v}[m] \geq \tilde{\mathbf{H}}_a^{q,v}[m-1], \\ 0, \text{ otherwise.} \end{cases}$$

Algorithm 1 $\mathbf{I_p}$ Matrix Assignment

Require: w, v, z % window, overlap and partition sizes
Ensure: $\mathbf{I_p}$ interchanges rows of $\mathbf{C}$ according to PMA parameters
1: Cycle the rows of identity matrix $\mathbf{I}$ to assign rows to $\mathbf{I_p}$
2: **for** j=1:z **do**
3: $\quad \mathbf{I_p}(j,:) \leftarrow \mathbf{I}(1 + (j-1)(z+v-w),:)$
4: **end for**

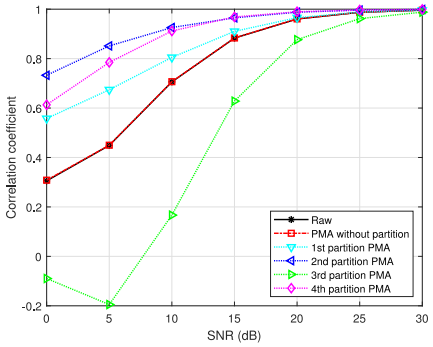

Fig. 2. Correlation comparison of Alice and Bob with $l = 4$.

$$K_{m+1}^{q,v} = \begin{cases} 1, \text{ if } \tilde{\mathbf{H}}_a^{q,v}[m] \geq \tilde{\mathbf{H}}_a^{q,v}[m-2], \\ 0, \text{ otherwise.} \end{cases}$$

$K_m^{q,v}$ and $K_{m+1}^{q,v}$ $(m \in \{1, 2, \ldots, 2z\})$ are the two quantized bits of $\tilde{\mathbf{H}}_a^{q,v}[m]$ at partition q for overlap size v. The current measurement is compared to two previous measurements. For $m = 1$, it is compared with $m = z$ and $m = z-1$, and for $m = 2$ compared with $m = 1$ and $m = z$. Each $\tilde{\mathbf{H}}_a^{q,v}[m]$ generates two bits. The number of generated streams, N, is given by $l \times n$. We have N streams to select from to generate the candidate key. CRC selection is performed for key generation.

3) CRC selection: Assuming that the output streams of the 2-bit DBQ for Alice or Bob is $\mathbf{B}_F = \{\mathbf{B}_F[1], \mathbf{B}_F[2], \ldots, \mathbf{B}_F[N]\}$, $F \in \{A, B\}$, Algorithm 2 describes the CRC selection. Alice sends the CRC check sum to Bob who compares with his own one. Bob selects streams with consistent check results to generate the candidate key, K_B. Bob sends the corresponding codeword to Alice which is the vector $\mathbf{C}^{N\times 1} \in \{0, 1\}^*$ notifying Alice of the streams that form the candidate key, Alice generates K_A. The selected bit stream is represented by a 1 in $\mathbf{C}$, and 0 otherwise.

C. Security Analysis

In the channel probing stage, Eve can estimate the Alice-Eve and Bob-Eve links by observing the channel-probing frames sent by Alice or Bob. However, Eve is more than a half-wavelength away from Alice or Bob and fulfils the spatial decorrelation principle of PLSKG. Her estimates will be different from Alice and Bob's. Experimental studies in [10] for IoT prove the spatial decorrelation principle. If Eve eavesdrops on the codeword, she does not have the streams generated by Alice. Therefore, she cannot generate the candidate key.

Algorithm 2 Quantization CRC Step

Require: $\mathbf{B}_A$, $\mathbf{B}_B$ % bit streams after 2-bit DBQ of Alice and Bob
Ensure: $K_A = K_B$ % Candidate key
Alice and Bob perform CRC
for F $\in \{A, B\}$ **do**
  $j \leftarrow 1$
  while $(j \leq N)$ **do**
    CRC($\mathbf{B}_F[j]$)
    $j \leftarrow j + 1$
  end while
end for
Alice sends CRC($\mathbf{B}_A$) to Bob
Bob checks, selects candidate key and updates codeword $\mathbf{C}$
$n \leftarrow 0$
for p=1:N **do**
  for q=1:N **do**
    if CRC($\mathbf{B}_A[p]$)=CRC($\mathbf{B}_B[q]$) **then**
      $K_B[1 + (n \times length\mathbf{B}_B[q]) : length\mathbf{B}_B[q] + (n \times length\mathbf{B}_B[q])] \leftarrow \mathbf{B}_B[q]$ (generate K_B)
      $\mathbf{C}[p] \leftarrow 1$
      $n \leftarrow n + 1$
    else
      $\mathbf{C}[p] \leftarrow 0$
    end if
  end for
end for
if $\mathbf{C}$ = zero matrix **then**
  Quantization has failed. Re-do with new PMA parameters
end if
Bob sends $\mathbf{C}$ to Alice, Alice generates key
$n \leftarrow 0$
for p=1:N **do**
  if $\mathbf{C}[p]$=1 **then**
    $K_A[1 + (n \times length\mathbf{B}_A[p]) : length\mathbf{B}_A[p] + (n \times length\mathbf{B}_A[p])] \leftarrow \mathbf{B}_A[p]$ (generate K_A)
    $n \leftarrow n + 1$
  end if
end for

TABLE I
PARAMETER SETTINGS

Parameter	Value
Number of FFT point	64
Number of data subcarriers	52
Baseband sampling frequency	$20MHz$
Channel spacing	$20MHz$
Doppler spread	$6Hz$
Root mean square delay spread	$50ns$
Channel probing rate	$10s^{-1}$
Total running time	$200s$

IV. PERFORMANCE EVALUATION

We implement a time-variant multipath channel model and an IEEE 802.11 OFDM transceiver to test the performance of the proposed protocol [1], [2]. The simulation parameters are detailed in Table I. Alice first sends a probing frame, $\Delta t = 0.1ms$. Each completes 2000 rounds of channel measurement. In each round, an estimated CFR with 52 subcarriers is obtained. For the convenience of data processing, key generation operation is done for every four channel estimates completed, i.e., an estimated CFR with 208 samples is collected. We compare our scheme with the proposed schemes in [2], [5], [8]. Reference [7] is very similar to [5]. We adopt the following metrics for performance evaluation.

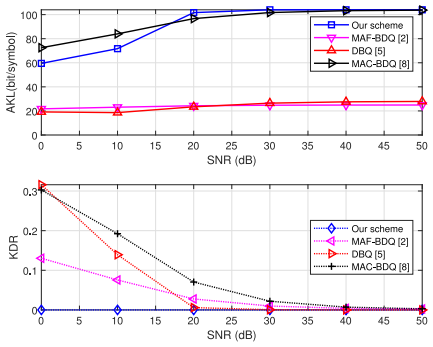

Fig. 3. AKL and KDR results.

1) Key disagreement rate (KDR): KDR indicates the key mismatch between Alice and Bob, defined as [3], given by

$$KDR = \frac{\sum_i |K_A(i) - K_B(i)|}{l_k}, \tag{13}$$

where l_k denotes the key length, $K_A(i)$ and $K_B(i)$ denotes the i-th key bit of Alice and Bob, respectively.
2) Randomness: Randomness of key by p-value tests with the National Institute of Standards and Technology (NIST) test suit as described in [11]. A p-value > 0.01 renders the sequence random.
3) Average key length (AKL): AKL is defined as the average key length generated from one OFDM symbol. Since the channel measurements of four OFDM symbols are collected to generate an initial key, AKL can be expressed as [2]

$$AKL = \frac{\sum_{i=1}^{N} L_i(1 - KDR_i)}{4N}, \tag{14}$$

where N is the number of generated initial keys, and L_i and KDR_i are the length and KDR of the ith pair of generated initial key, respectively.
4) Implementation Complexity: Analyzed from two aspects: 1) computational complexity according to mathematical operations and 2) resource consumption according to communication overhead of quantization and information reconciliation stages [2].

For our protocol, we make four partitions, i.e., $l = 4$, $q = \{1, 2, 3, 4\}$. We select the window $w = 51$ with overlaps $v = \{26, 34, 42, 50\}$. We choose four streams to generate the key at most. As for the MAF-BDQ scheme of [2], we select a window of 24 and step 8 as this reports the best performance in terms of KDR and AKL. While for the DBQ scheme of [5], the tuning parameter $\epsilon = 0.1 \times standard\ deviation$. For MAC-BDQ [8], we set $w = 206$ and $v = \{110, 130, 160, 180\}$.

Fig. 3 shows the ability of our quantization scheme to produce 0-bit mismatched keys with the highest KGR observed from the AKL. It is slightly lower than that of MAC-BDQ [8] at lower SNR because a few streams match. Without PMA, our scheme will be the same as MAC-BDQ. The excellent performance of our scheme in terms of KDR is explained by Fig. 4. PMA can discriminate partitions of low correlation for key generation. No stream is selected from the 3^{rd} partition at

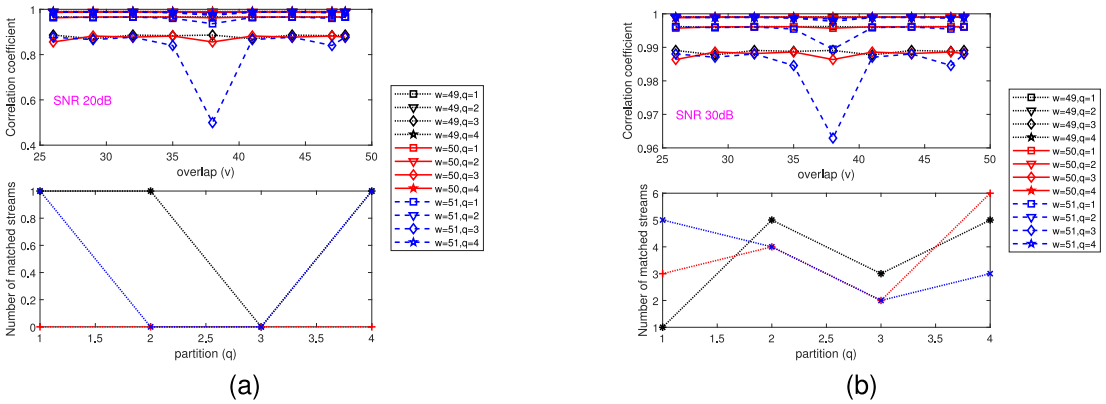

Fig. 4. Comparison of performance with PMA parameters w = {49, 50, 51}, v = {26, 29, 32, 35, 38, 41, 44, 47, 48} and q ={1, 2, 3, 4} at (a)SNR 20dB (b)SNR 30dB.

TABLE II
NIST RANDOMNESS TEST RESULTS

Test	p-value
Frequency	0.2024
Block Frequency	0.1958
Cummulative sums forward, reverse	0.4045, 0.2113
Serial	0.7316, 0.8499
Non-overlapping	0.5174, 0.0224, 0.5394, 0.0486
Runs	0.0370
Longest runs of ones	0.7251
Rank	0.0852
Approximate Entropy	0.8525
Discrete Fourier Transform	0.5164

TABLE III
IMPLEMENTATION COMPLEXITY

Quantization	Computational complexity	Information interactions
Our scheme	O(N)	1
MAF-BDQ [2]	O(N)	N/A
DBQ [5]	O(N)	N/A
MAC-BDQ [8]	O(N)	N/A
Reconciliation	Computational complexity	Information interactions
Our scheme	N/A	N/A
Improved cascade [2]	O(L)	2
ECC-based [5]	O(L^2)	1
Secure sketch [8]	O(L^2)	1

lower SNR, exemplified by Fig. 4(a). DBQ [5] can not correct the errors at very low SNR with KDR above 20%. At this SNR, when $w = 50$, the quantization will fail. Therefore, PMA parameter w may be changed to 49 or 51. Longer keys may be generated for higher SNR, exemplified by 30dB in Fig. 4(b), as more streams match. The randomness of the key is reported in Table II. It shows a p-value > 0.01 for all tests.

For the implementation complexity, if we assume that the length of the channel measurements to be quantized is N, they all have a computational complexity of $O(N)$. The quantization of our scheme involves Alice sending CRC, and Bob responds with a codeword, which is a single information interaction. Information reconciliation implementation complexity is analyzed as in [2]. Assuming that the length of the initial key is L, then the computational complexity of the improved cascade [2] is $O(L)$, while that of ECC [5] and secure sketch [8] is $O(L^2)$. The specific implementation complexity is shown in Table III, where N/A is *not applicable*. According to the above analysis, the proposed key protocol is more lightweight. It is important to note that increasing overlaps will slightly change computational load.

V. CONCLUSION

This letter proposes a lightweight novel PLSKG protocol that has only two stages. Moreover, the quantization of OFDM subcarriers' channel responses includes a pre-processing that detects regions of the estimated CFR with higher channel reciprocity for a 0-bit mismatch key generation. The results show that our protocol can achieve reliable and efficient key generation with lower implementation complexity.

REFERENCES

[1] J. Zhang et al., "Secure key generation from OFDM subcarriers' channel responses," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, 2014, pp. 1302–1307.
[2] D. Guo et al., "A lightweight key generation scheme for the Internet of Things," *IEEE Internet Things J.*, vol. 8, no. 15, pp. 12137–12149, Aug. 2021.
[3] W. Xu et al., "Key generation for Internet of Things: A contemporary survey," *ACM Comput. Surv.*, vol. 54, no. 1, pp. 1–37, Jan. 2021.
[4] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 347–376, 1st Quart., 2016.
[5] J. Zhang, A. Marshall, and L. Hanzo, "Channel-envelope differencing eliminates secret key correlation: LoRa-based key generation in low power wide area networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 12, pp. 12462–12466, Dec. 2018.
[6] B. Zan, M. Gruteser, and F. Hu, "Key agreement algorithms for vehicular communication networks based on reciprocity and diversity theorems," *IEEE Trans. Veh. Technol.*, vol. 62, no. 8, pp. 4020–4027, Oct. 2013.
[7] J. Zhang et al., "H2K: A heartbeat-based key generation framework for ECG and PPG signals," *IEEE Trans. Mobile Comput.*, vol. 22, no. 2, pp. 923–934, Feb. 2023.
[8] A. F. Kawoya, H. Wang, and M. S. Abood, "Efficient key extraction for secure vehicular communication through OTFS," *IEEE Comm. Lett.*, vol. 28, no. 3, pp. 468–472, Mar. 2024.
[9] Y. Peng et al., "Secret key generation based on estimated channel state information for TDD-OFDM systems over fading channels," *IEEE Trans. Wireless Commun.*, vol. 16, no. 8, pp. 5176–5186, Aug. 2017.
[10] C. Zenger et al., "The passive eavesdropper affects my channel: Secret-key rates under real-world conditions," in *Proc. IEEE GlobeCom Workshops (GC Wkshps)*, 2016, pp. 1–6.
[11] L. Bassham et al., "A statistical test suite for random and pseudorandom number generators for cryptographic applications," U.S. Dept. Comm., Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, Rep. SP 800-22, 2010.