International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

A Novel Hybrid Protocol and Code Related Information Reconciliation Scheme for Physical Layer Secret Key Generation

Sujata Kadam
Dept.of Electronics and Telecommunication
R.A.I.T
Navi Mumbai, India
sujatakadam7890@gmail.com

Joanne Gomes
Dept.of Information Technology
S.F.I.T
Mumbai, India
jgomes@sfit.ac.in

Abstract— Wireless networks are vulnerable to various attacks due to their open nature, making them susceptible to eavesdropping and other security threats. Eavesdropping attack takes place at the physical layer. Traditional wireless network security relies on cryptographic techniques to secure data transmissions. However, these techniques may not be suitable for all scenarios, especially in resource-constrained environments such as wireless sensor networks and adhoc networks. In these networks having limited power resources, generating cryptographic keys between mobile entities can be challenging. Also, the cryptographic keys are computationally complex and require key management infrastructure. Physical Layer Key Generation (PLKG) is an emerging solution to address these challenges. It establishes secure communication between two users by taking advantage of the wireless channel's inherent features. PLKG process involves channel probing, quantization, information reconciliation (IR) and privacy amplification to generate symmetric secret key. The researchers have used various PLKG techniques to get the secret key, still they face problems in the IR scheme to obtain symmetric keys between the users who share the same channel for communication. Both the code based and protocol based methods proposed in the literature have advantages and limitations related to their performance parameters such as information leakage, interaction delay and computation complexity. This research work proposes a novel IR mechanism that combines the protocol and code-based error correction methods to obtain reduced Bit Mismatch Rate (BMR), reduced information leakage, reduced interaction delay, and reduced computational time to enhance physical layer secret key's quality. In the proposed research work, the channel samples are generated using the Received Signal Strength (RSS) and Channel Impulse Response (CIR) parameters. These samples are quantized using Vector Quantization with Affinity Propagation Clustering (VQAPC) method to generate the preliminary key. The samples collected by the two users who wish to communicate, (for example Alice and Bob) will be different due to noise in the channel and hardware limitations. Hence their preliminary keys will be different. Removing this discrepancy between Bob's and Alice's initial keys, using novel Hybrid Protocol and Code related Information Reconciliation (HPC-IR) scheme to generate error corrected key, is the most important contribution of this research work. This key is further encoded by the MD5 hash function to generate a final secret key for exchanging information between two users over the wireless channel. It is observed that the proposed HPC-IR scheme achieves BMR of 19.4%, information leakage is 0.002, interaction delay is 0.001 seconds and computation time is 0.02 seconds.

Keywords- Physical layer, vector quantization, information reconciliation, information leakage, symmetric secret key.

I. INTRODUCTION

The use of wireless communication is increasing day by day thereby supporting a high data rate. Parallel to this, the data transfer rate's security is degrading. To safeguard the data, cryptographic schemes are used by sharing the public or private key [1, 2]. On a wireless channel, an intruder can intrude or leak the data transfer or communication made by the wireless channel users. This attack happens on the information exchange layer named the physical layer, and it is noted as jamming and eavesdropping [3, 4]. In eavesdropping, the confidential information shared between the two legitimate users can be overheard by the intruder. This leakage of sensitive information can prove to be dangerous. Hence safeguarding the data at physical layer, during transmission through a wireless medium is necessary. The question at this point is how to generate an identical key between the authorized users, which is non-vulnerable to the intruder. Traditional cryptographic techniques consisting of the symmetric and asymmetric cryptographic methods demand key management infrastructure and are computationally complex. Furthermore, the current cryptographic methods are no longer reliable due to the emergence of quantum computers that may quickly execute a difficult and huge factorization [5]. Physical Layer key generation (PLKG) has been emerging as a cutting-edge substitute for the upper layer key distribution technique [6].

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

PLKG is a method of achieving secure communication between users sharing a wireless channel by exploiting the properties of the physical transmission medium. It seeks to offer symmetric keys that can be utilized independently of an existing key distribution infrastructure for encryption and decryption. This is especially crucial in situations where standard key distribution techniques would not be possible or practical, such as ad hoc networks, wireless sensor networks (WSNs), and the Internet of Things (IOT). Vernam's description of the one-time pad serves as the foundation for the original idea [7] where a plaintext is encrypted using modular addition and a previously known secret key. An eavesdropper without the key cannot decrypt the message if the key is really random and the message is plaintext. The concept of information-theoretic security, as formulated by Shannon [8], ensures that even if an eavesdropper intercepts the cipher text, they cannot gain any information about the plaintext without knowledge of the secret key, provided that the entropy of the key is at least as large as the entropy of the message. This means that the security is based on the inherent uncertainty in the wireless channel and not solely on the complexity of cryptographic algorithms. For PLKG three main requirements need to be satisfied. They are channel reciprocity, temporal variations and spatial decorrelation [9, 10]. PLKG process is as shown in Fig. 1. The two legitimate users (Alice and Bob) probe the wireless channel using a channel probing method. The probed channel samples are converted in the form of bits using a quantization method. It provides Alice and Bob with an initial preliminary key as the output. By using an error correction procedure, the difference in the key that was received by each user is further eliminated. The reconciled keys are applied to privacy amplification which makes the key secure [11]. The quality of the generated key is measured by parameters such entropy, secrecy, key generation rate, length of the key and so on. The fundamental components

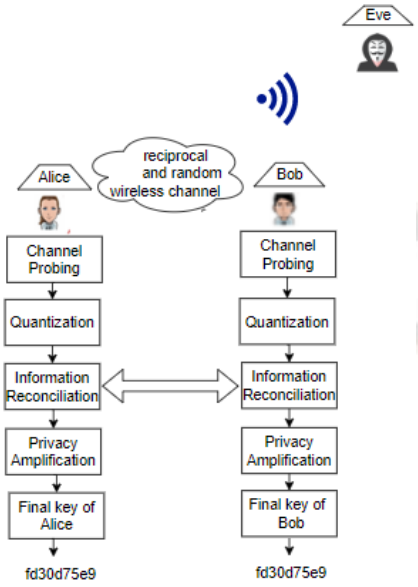

Fig. 1: PLKG system [11]

of PLKG system have been extensively researched and widely incorporated in the existing literature.

Channel Probing: In the process of PLKG, the two legitimate users (Alice and Bob) probe the wireless channel between them in order to gather signal samples, as illustrated in Fig 1. These signal samples are obtained by measuring different parameters of the channel such as Received Signal Strength (RSS), Channel Frequency Response (CFR), Angle of arrival (AOA), Channel Impulse Response (CIR) etc. which are quantized to generate the preliminary keys. These preliminary keys are processed further to get final secret key. An ideal secret key should have high Key Generation Rate (KGR), high entropy and more security. The wireless channel is probed in [12] using an Electronic Steered Parasitic Array Radiator (ESPAR) smart antenna. Secret keys are agreed upon by Access point A with its ESPAR antenna and user terminal B with its traditional omnidirectional antenna. As with B, Eavesdropper C is a user terminal. A and B can use a technique like time division duplex (TDD) to communicate at the same frequency. The reactance vector of an m-element ESPAR antenna is the expression for the reactance values established at each parasitic element. The reactance vector series is an expression for a set of N-units of reactance vectors .The only device that can regulate the beam pattern of an ESPAR antenna is the access point itself. As a result, a very high level of security can be achieved using this approach. An eavesdropper close to the access point might be able to infer information by near-field probing the ESPAR antenna if there aren't many beam patterns. On the other hand, there are 248 beam patterns, and each beam pattern has a few milliseconds of existence time. As so, it would be far too challenging for the eavesdropper listening in to infer the transmitted information. In [13] the importance of multiple antenna systems over single antenna system is highlighted using Multiple Antenna Key Generator (MAKE). In comparison to a single antenna system, it demonstrated a significant increase in key generation rate. In order to achieve a desired KGR and optimize the probing process, an adaptive channel probing system based on Lempel Ziv complexity (LZ76) and Proportional-integral-derivative (PID) controller is proposed in [14]. The KGR depends on the conditional mutual information between Alice and Bob. Mutual information obtained is 72.34 bits/sec for mobile scenarios and 58.96 bits/sec for static scenarios. It was also proved that while the entropy rate decreases with the increasing probing rate, the KGR also rises. In papers [15-18] authors have implemented PLKG methods probing various channel parameters mentioned above.

Quantization: The quantization methods play an important role in PLKG. The samples obtained after channel probing are quantized to get preliminary key. The main goal of quantization method is to generate preliminary key which will have high entropy for security, reduced Bit Mismatch Rate (BMR) between two users using same quantization method so that both the users will have an identical secret key, and higher KGR. Researchers have used lossy and lossless quantizers to convert the probed channel samples into bits [11]. Lossless quantizers are discussed in [12], 19], [21], [23], 24], [25] and lossy quantizers are discussed in [20], [22]. In [12] a lossless binary quantizer is used to get the preliminary key. The threshold is determined by taking the median value of the RSS values from the channel. If the probed RSS value lies above the threshold, the quantizer output is 1 else the quantizer output is 0. From 384

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

measured RSS values of signal, a 128-bit secret key is produced. In [19] deep fades in the RSS measurements is considered as the threshold to get the preliminary key. In [20] a level crossing algorithm which uses two thresholds for quantization is used. Pre-processing methods are applied in [21] to improve the channel reciprocity as it improves BMR and High Rate Uncorrelated Bit Extraction (HRUBE) method is implemented which gives KGR of 10 to 22 bits/second (typical value of KGR is 16-200 bits/sec) corresponding to BMR of 0.54% to 2.2% (typical value of BMR is 0.5 to 15.85%). In [13] extra bands are inserted between two neighbouring quantization levels which further reduces the BMR to improve symmetry of the secret key of the two users. [22] uses Adaptive Secret Bit Generation (ASBG) quantization to achieve maximum entropy by splitting RSS values into lower subblocks and obtaining the threshold for each subblock independently. The Lloyd-max based quantizer is adopted to minimize the quantization error in [23], which helps to reduce the BMR wherein the RSS samples are pre-processed by using Moving Window Averaging (MWA). In [24], Modified Kalman (MK) pre-processing technique along with the multi-level quantization is used which generates key with low randomness. To obtain secure secret key, randomness of the key should be high in order to achieve high entropy. By considering the multi-path Rayleigh fading channel, Improved Channel Quantization Alternating (ICQA) algorithm is proposed in [25] where the samples are measured using the CFR parameter. Authors claim that, BMR of their proposed system decreases by 31.5% than Channel Quantization Algorithm (CQA) and 20.4% than Channel Quantization Guard band (CQG) algorithm. The different quantization methods such as Traditional Amplitude Quantization (TAQ), Traditional Phase Quantization (TPQ), Regular Vector Partitioning Quantization (RVPQ) have been discussed in [26] by Han et al. Here the quantization is performed by the vector partitioning quantization in which the vector space is divided into several non-overlapping regions based on the requirement. Each region is mapped to corresponding bits. Then the algorithm is extended by the k-means clustering method where two k-means algorithms are adopted, namely, lossy k-means and compensation k-means for the quantized samples to move towards the cluster centers. Considering the gamma fading channels, the average contiguous duration based quantization method is developed in [27]. The method measured the envelope of the channel samples for performing the quantization. A non-uniform quantization method is applied for the secret key generation from the channel samples. The quantization is performed by considering the RSS on the Nakagami-m fading channel under multi-level considerations. The correlation coefficient evaluated the guard strip width through the analytical model. The performance in terms of key agreement probability, bit mismatch probability, and key generation rate is examined. Initially, the wavelet transform is used for physical layer secret key generation, which is defined by Zhan et al. [28]. For that, the authors used discrete wavelet transform, and the output of the transform is quantized by the multi-level quantization method. The said quantization converted the decomposed vectors into compressed bits. Then to tolerate the bit mismatch the gray code is applied.

Information Reconciliation: The result of the quantization is the preliminary key generated by both Alice and Bob. In the channel, noise and interference may get added [29,30], thus making the key to be different for both the users. The similar key generation between the end users is a tedious task. Different quantization techniques strive to optimize this process to the fullest extent by reducing quantization error. To further reduce the dissimilarity between keys i.e. to reduce the initial BMR, information reconciliation methods are developed. Error correction between Alice's and Bob's key bits is known as information reconciliation, or IR for short. Its primary aim is to make the two users agree upon the same key. IR methods consist of protocol based approaches [31-35] and code based approaches [36-41]. A protocol based approach is a two-way scheme in which communication takes place between Alice and Bob for error correction of key bits, until they agree upon a common key. In this process, multiple rounds of two-way communication take place. The protocol-based approaches reduce the mismatch by concerning the multi-round interaction with parity checks, thereby having the delay and complexity issues. Many protocol based IR methods have been proposed in the literature such as Cascade protocol, Winnow protocol, Optimal IR, and Optimal IR with Pre-distillation [31-35]. In the code based IR method, only one round of communication takes place between Alice and bob for error correction of key bits. The code-based IR methods effectively reduce the key mismatch in simple manner, with or without the interaction delay. Also in code based IR methods, the efficiency of key generation is better than the protocol based IR methods. Examples of code based IR methods are Bose Chaudhuri Hocquenghem (BCH) codes, Reed Solomon (RS) codes, Turbo codes, Polar codes, Low Density Parity Check (LDPC) codes. This classification of the IR methods is illustrated in Fig. 2.

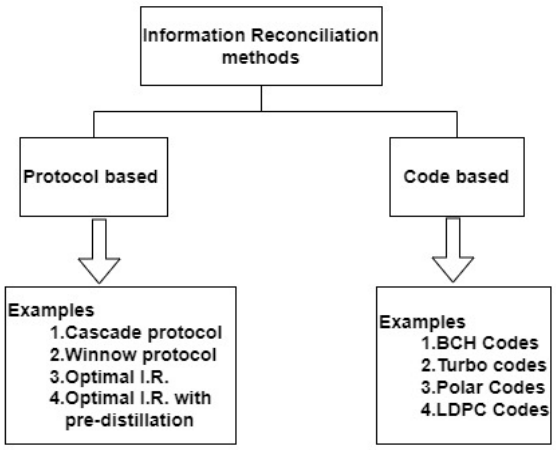

Fig. 2. Information Reconciliation methods

In [31] a cascade protocol for interactive IR is proposed. It corrects errors by calculating parity checks of the respective blocks. The protocol is run for a predetermined number of passes which is determined based on initial BMR which is calculated before execution. The first step in the protocol is a random permutation which is agreed by both Alice and Bob by discussion over the public channel. Cascade protocol is known for its ease of implementation. But it needs atleast $1+\log_2 N$ communications in one iteration where N is the number of blocks. The efficiency of cascade protocol is 0.906 for an error rate of 0.01. In [32] Winnow protocol for IR is proposed which aims to reduce the interactivity between communicating parties by making use of hamming codes for error correction. It offers better throughput, lower interactivity but similar efficiency as cascade protocol. It is based on the exchange of parity and

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

Hamming's syndrome. Winnow protocol has faster implementation speed. It is capable of correcting an initial BMR of up to 13.22%. In the Winnow protocol, new errors can get added to a block having multiple errors thereby increasing the BMR. The information rate of an IR scheme is the ratio of the reconciled key string to the initial key string. In an efficient IR scheme, the information rate should be high. In Winnow protocol, to maintain the privacy, m syndrome bits are eliminated from each block, which reduces the information rate. In [33] an optimal IR protocol is proposed to improve the efficiency and information rate of Winnow protocol. In this, BMR decreases to 0.39 and the information rate increases to 0.42 with respect to winnow protocol with BMR of 0.5 and information rate of 0.42. In [34] pre-processing method is used which is valid when the BMR is greater than 0.1. The data rate is improved more than 37 times when the original BMR = 0.3. To solve the issue of a very large initial BMR and increase the efficiency of the system, [35] uses pre-distillation to ensure whether BMR is lowered so that IR protocol effectively corrects the key bit differences. After predistillation, the initial BMR drops rapidly, facilitating subsequent IR and privacy amplification. When the initial BMR is more than 0.15, pre-distillation and optimal IR work well together, and when the initial BMR = 0.3, the information rate increases by more than 49 times. Many code based IR methods proposed in literature exhibit better performance in improving efficiency of PLKG at reduced cost. Quantum key reconciliation method by applying BCH based slepian wolf coding with feedback syndrome decoding is proposed in [36]. Reconciliation efficiency of 1.55 is obtained for an entropy of 0.1. The Polar codes are discussed in [37]. They use the channel polarization property using which the bit channels are divided into noiseless bit channels or pure noise bit channels. Only the noiseless bit channels are selected to transmit information between the users. Polar codes exhibit better performance than LDPC codes when peak signal to noise ratio is greater than 3.5dB. In [38] a new protocol for error correction using rate adaptive LDPC codes is proposed. LDPC codes are known for the sparseness (and therefore low density) of their parity check matrices. They have performance which is near to the theoretical Shannon limit. Reconciliation efficiency of the IR process using the proposed protocol is 1.1 which is considerably better than the efficiency of its non-interactive version with an efficiency of 1.09. Graphical representation of the LDPC codes by a bipartite graph called as Tanner graph is provided in [39]. Tanner graph provides a complete representation of the code and it helps in the description of decoding algorithm. LDPC codes are known to achieve coding rates near the capacity of several channels under belief propagation decoding. These codes can be used to encode near the theoretical limit for source coding. Two strategies i.e. puncturing and shortening which are able to adapt the rate of a channel code are discussed in [40]. It is seen that the proposed algorithm gives better performance in terms of Frame Error Rate (FER). For a FER of 10^{-3} significant improvement is seen in Binary Symmetric Channel (BSC) for a mother code of code rate 0.3 punctured a 10 %, in Binary Erasure Channel (BEC) for a mother code of rate 0.6 punctured a 5% and in the Additive White Gaussian Noise (AWGN) channel for a mother code of rate 0.6 punctured a 10% respectively. In vehicle to vehicle communication, Turbo codes are used with non- reciprocity compensation as proposed in [41]. This method gives BMR as low as 0.02. KGR obtained for 128-bit key is 35 keys /minute.

Protocol based error correction methods require multiple round-trip communications. They cause high interaction delay. Also as the number of passes increases their efficiency decreases. Code based error correction methods need only single round of one-way communication. They have less interaction delay but large information leakage. Both protocol based and code based IR methods have different impact on the output performance parameters of IR block in PLKG process. The high level comparison of performance parameters between protocol based and code based IR methods is given in Table I.

TABLE I. PROTOCOL BASED AND CODE BASED IR METHODS

Performance parameters	Typical values	Protocol based IR methods	Code based IR methods
Interaction delay	0.1 – 2.1	High	Low
Computational Complexity	0.04-0.47	Low	High
Information Leakage	0.005-0.2	Low	High

For an efficient IR method, interaction delay, computational complexity and information leakage should be low. Hence by combining the advantages of both protocol based and code based methods, hybrid information reconciliation schemes have been proposed in the literature which correct the errors in the key generated by the end users effectively. This research work proposes one such novel hybrid IR mechanism. Survey of existing hybrid IR methods is presented in the next section as it is related to the proposed research work.

Privacy Amplification: As the information during the IR stage is heard by the eavesdropper, partial or even complete information about the key may be exposed. To ensure perfect secrecy, the aligned keys are now subjected to privacy amplification [42,43] where a hash function or more general, a randomness extractor is applied to the keys to obtain a cryptographic secret key. Hash functions widely used are the message digest and the secure hash functions. The output of privacy amplification block is a hexadecimal key which should be same for both Alice and Bob. This is the final secret key.

The existing PLKG methods can be improved in terms of BMR, entropy and KGR, by employing innovative quantization methods and advanced error correction codes. In the proposed research work, for generation of the secret key, the end users obtain the RSS and CIR samples from the channel. Quantization is performed on these samples using Vector quantization with Affinity propagation clustering (VQAPC) [44]. The research work presented in this paper proposes a novel hybrid, protocol and code related information reconciliation scheme (HPC-IR) by combining the advantages of both cascade protocol and LDPC code. This scheme is applied to the preliminary key obtained by VQAPC. The error corrected key is encoded using the MD5 hash function which generates the final secret key.

The remaining paper is structured as follows: Section II gives related work comprising recent hybrid IR methods. Section III explains the proposed architecture for Secret key generation for error reduction in generated key for physical layer security.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

Section IV provides the results and discussion. At last, section V concludes by reporting the benefits of the work along with future scope.

II. RELATED WORK

The different blocks of the PLKG method have been surveyed and discussed earlier. This section reviews the recent hybrid IR methods.

Review of hybrid information reconciliation methods

For information reconciliation, a hybrid method is adopted by Li et al. [45]. This method combines the BBBSS protocol based and BCH code based error correction method. The designed model is tested by considering one input, one output, and single eavesdropper based system design for validation. The reconciliation efficiency was improved from individual BBBSS and BCH codes as 2.48 and 22.36, respectively. Error correction for Quantum key distribution is explained in [46]. In this Winnow algorithm with high speed parity and hamming error correction based on FPGA is used which has better performance in processing bandwidth and error correction efficiency. With the Shannon limit approached (SLA) IR, Tang et al. [47] utilized the polar code, thereby having the quantized BMR of 2%, having efficiency and correctness of 1.055. To achieve correctness, cyclic redundancy check length and sub-block of the information are taken into consideration thereby having the forward reconciliation. While in the acknowledgement phase, the Shannon limit approach was applied. Table II summarizes the recent hybrid IR methods.

TABLE II. RECENT HYBRID INFORMATION RECONCILIATION METHODS

Research Publication and Year	IR Method	Performance parameters	
		BMR (%)	Reconciliation efficiency
Li et al. [45] Entropy 2019	Hybrid of BBBSS protocol and BCH code	0.5-11.5	2.48 & 22.36
Tang et al.[46] IJQI 2019	Winnow algorithm with parity and hamming codes	0.88	-
Tang et al. [47] QIP 2021	Polar codes with (SLA) I.R scheme is used.	2	1.055

III. SYSTEM MODEL OF PLKG

A shared key is established between the users (Bob and Alice) concerning the wireless channel reciprocity, which means the transceiver of a wireless link can take the same channel simultaneously. But due to the noise and interference in the wireless channel, probing of similar samples by both the users becomes difficult. Hence there is discrepancy in the shared secret key. This discrepancy can be removed by using proper quantization and error correction method. In the proposed research work this discrepancy is removed by using VQAPC and HPC-IR scheme to obtain secret symmetric key.

The wireless physical layer communication system model as shown in Fig. 3, involves two legitimate users, Alice and Bob, who want to establish a shared key using an unauthenticated wireless channel. But Eve is able to listen in on all of Alice and Bob's conversations since she is an eavesdropper. Since Alice and Bob's observations are not associated with Eve's, it is assumed that Eve can't be that close to either of them.

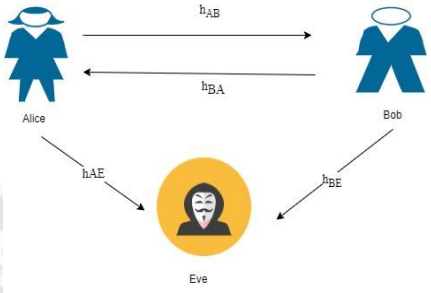

Fig. 3. Wireless physical layer communication System model

Both Alice and Bob probe the wireless channel during channel measurements.

$$y_A = h_{BA}x + n_a,$$
$$y_B = h_{AB}x + n_b \quad (1)$$

where,

during a probing procedure, the valid channel from Bob to Alice is represented by the complex number h_{BA}, and the legal channel from Alice to Bob is represented by h_{AB}. x is the common probe signal, y_A is the received signal of Alice, and y_B is the received signal of Bob. Also, n_a and n_b denote the complex additive white gaussian noise and both of them obey the distribution of $CN(0,\sigma^2_n)$.Alice and Bob obtain the samples by channel estimation as shown in (2)

$$ma = \frac{yA}{\sqrt{P}\,x} = h_{BA} + n_a$$

$$mb = \frac{yB}{\sqrt{P}\,x} = h_{AB} + n_b \quad (2)$$

where m_a and m_b denote the samples of Alice and Bob during the probing process. Both Alice and Bob probe Nakagami-m fading channel. The Nakagami-m fading channel is a mathematical model used to describe the behavior of wireless communication channels, in scenarios where multipath propagation and fading are significant factors. It offers several advantages over the existing fading models. As m increases, the fading becomes less severe and approaches a non-fading channel. Nakagami-m fading is often considered more realistic than the simple Rayleigh fading model. It accounts for the fact that in real-world environments, the strength of multipath components can vary, leading to variations in signal amplitude. This makes it a valuable tool for modeling and simulating real-world channels. Nakagami-m fading can be efficiently simulated using random number generators and statistical techniques. Fig.4a shows the basic secret key generation system explained earlier, which consists of channel probing, quantization, information reconciliation and privacy amplification blocks. Fig.4 b depicts the proposed architecture for secret key generation. The samples that Bob and Alice collected are different because of the noise and interference in the channel. This leads to the generation of a dissimilar key at the end. But for communication, they both need to generate a similar key. This can be achieved by using innovative quantization and IR methods. In the proposed architecture in the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

first stage of quantization similar samples of both the users are grouped into different clusters using APC. The samples within a particular cluster are then subjected to vector quantization.

This lowers the Assignment disagreement rate (ADR) obtained after quantization by Alice and Bob. ADR can be defined as the amount of disagreement between the two users. This happens when the samples are assigned to different quantization regions. The resulting ADR was 0.0019. The output of VQAPC is the preliminary key generated for two users. This preliminary key further undergoes error correction in the IR stage which is the second stage of the proposed architecture as shown in Fig. 4b. A hybrid IR method consisting of cascade protocol and LDPC code is used for information reconciliation. During this stage the key is exchanged between the two users. The key generated at Alice and Bob's end is then encoded by using MD5 hash function to generate the final secured secret key.

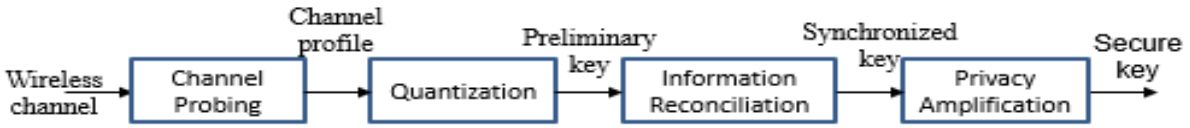

Fig. 4 a. Basic secret key generation system

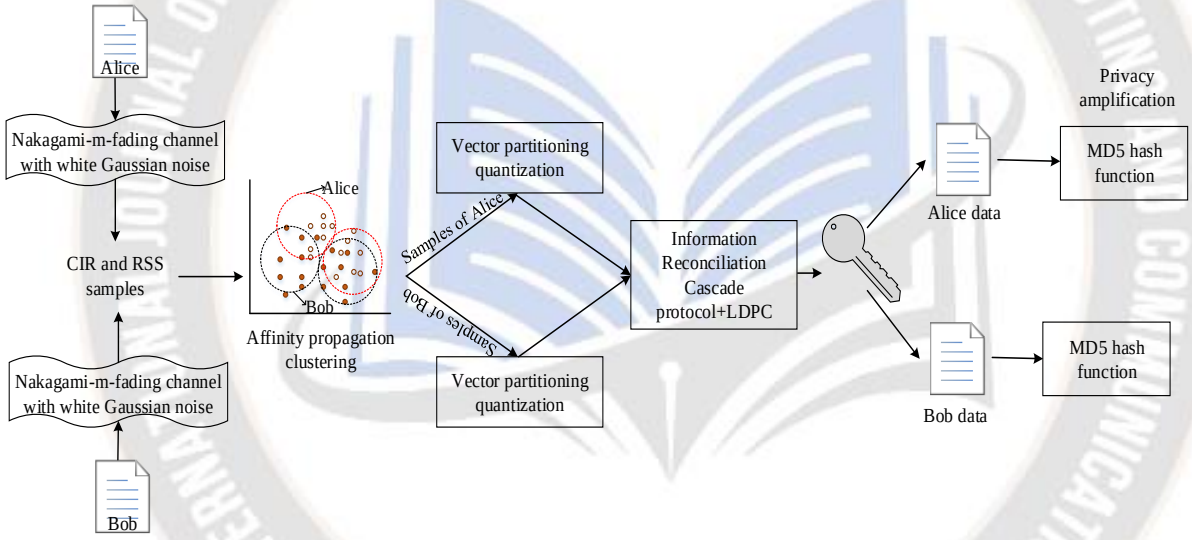

Fig. 4 b. Proposed architecture for secret key generation

Hybrid-Protocol and Code related information reconciliation (HPC-IR) scheme

Both protocol and code based methods have their advantages and limitations. Protocol based methods require many passes and many rounds of backward and forward communications. There is a fairly noticeable interaction delay when Alice and Bob are far apart. Additionally, when the pass number rises, protocol-based approaches become less effective. On the positive side protocol based methods are less complex and leak less amount of information. On the other hand, code based methods have only single pass, single round and single communication. Hence it has less interaction delay. But it has costly computation overhead and high information leakage. It is possible to combine the good features of both protocol and code based methods to obtain a hybrid information reconciliation scheme. In this research work, a HPC-IR scheme by combining the advantages of both cascade protocol and LDPC code is proposed.

Cascade protocol is the block based error correction scheme that uses two parameters for setting the block of quantized samples. One is block size, and another one is block growth size. The protocol divides the block based on the error rate. The error rate is found by the error estimation and is denoted as $\mathcal{E}$. The preliminary key with bit strings on Alice and Bob is represented as $KA_1, KA_2, ...KA_n$ and $KB_1, KB_2, ...KB_n$ respectively having the bits within the set $\{0,1\}$.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

Initially, the bit string from Alice and Bob is scrambled to evenly spread the error. Then in the first round, the bit strings are divided into blocks of b_1 where, $b_1 = \phi / \varepsilon$

- ϕ indicates the initial block size. The k^{th} block in the initial round is given as,

$$B_k^1 = \{m \mid (k-1)b_1 < m < kb_1\} \quad (3)$$

- Alice will calculate the similarity bits on all her blocks and find the parity bits. The parity bits are sent to the bob to verify his blocks. Bob will compare the parity with his parity bits. If any changes have been encountered, the LDPC based error correction is performed. This will correct the error by using different parity in each block. At this session, Alice and Bob have a similar count of errors (nullified error); hence no information is deleted in this protocol based scheme.
- In the proceeding round, the block size growth is indicated as φ. The length of each block in the proceeding round is given as $b_i = \varphi b_{i-1} (i > 1)$, where i is the total round involved. When φ is high, then the growth rate is also high. For this considered block, the scrambling function is performed, which is similar to the function that was previously performed. In this instance, the block of l can be written as,

$$B_l^i = \{m \mid f_i(m) = l\} \quad (4)$$

Here, $f_i : [1,2,....n] \rightarrow [1,2,...[n/b_i]]$. m and n indicates the total errors in the initial and i[th] round. Again Alice send the parity bit for the above mentioned block. Similarly, bob also computes the same. If both parties are not-identical, then LDPC will be performed.

- Now all these unsymmetrical blocks from Alice and Bob are considered on the set S. In this set, Alice and Bob will choose a block of the smallest one and repeat the process to correct the errors. Let m' is the error on the block that is chosen for correcting errors. Those blocks are stored on the set X.
- The condition to check an even number of errors is $S' = (S \cup X) \setminus (S \cap X)$ (zero). If $S' \neq \Theta$ then there is an odd number of errors. Due to this chaining process, more errors are detected and corrected by the cascade protocol. The process ends when the total number of rounds is over. Fig. 5 shows the proposed hybrid model's structure.

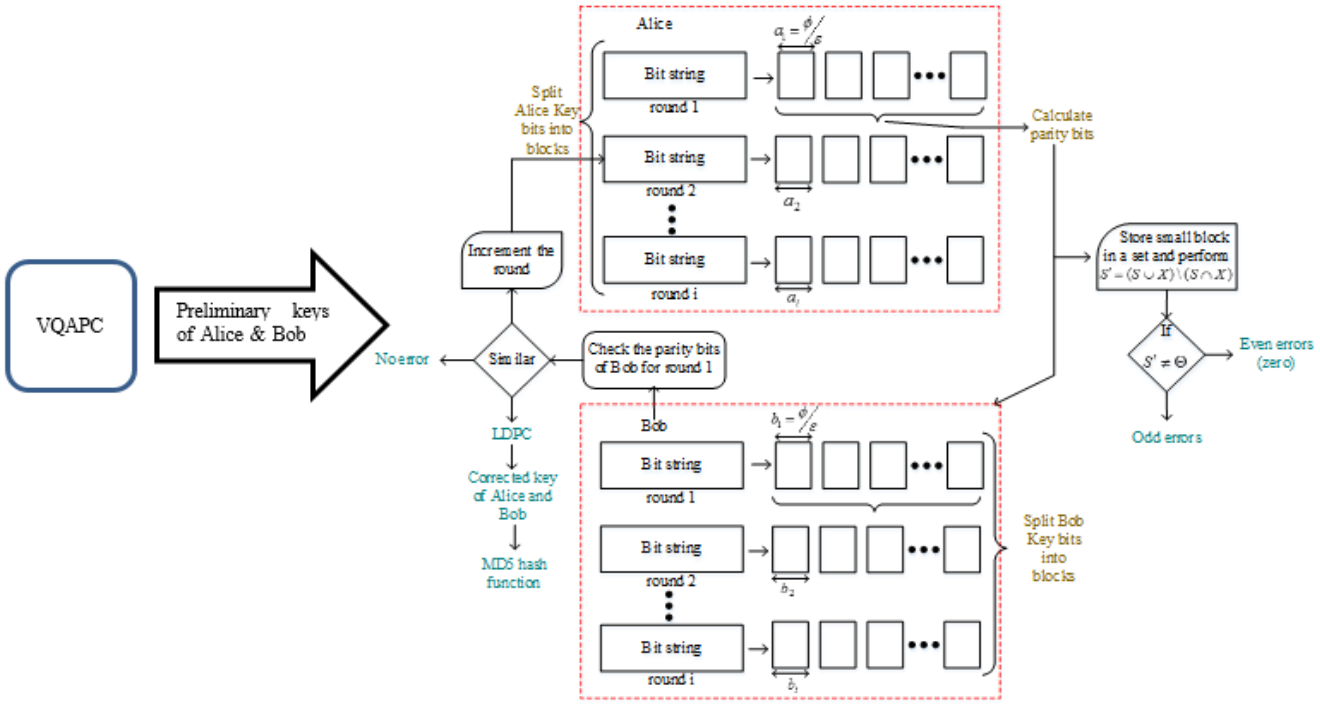

Fig. 5. Structure of HPC-IR scheme

LDPC is a linear error correcting code mostly used on the noisy transmission channel. Here two channel codes are used, one for protecting the additional bits C_a and the other for Slepian-wolf coding C_w. The generator matrix and parity matrix for Slepian wolf coding and additional bits code is denoted by G_w, G_a and H_w, H_a respectively. The parity between the users should satisfy the Slepian-wolf approach as,

$$q = H_w K_b \quad (5)$$

The obtained bits are the key bits (K) in the secondary code of the block b. Then the generated codeword is,

$$g = G_a^T q \quad (6)$$

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

$$g = G_a^T H_w K_b \tag{7}$$

For the vector of block H_w the generator matrix is $G = [I\ H_w^T\ G_a]$, while transmitting the key bits through the quantization channel with the white Gaussian noise. The degree of distribution to the variable and check node on LDPC code is expressed as,

$$\nu(t) = \sum_j \sum_{i\geq 2} \nu_i^{(j)} t^{i-1} \tag{8}$$

$$\vartheta(t) = \sum_{i\geq 2} \vartheta_i\, t^{i-1} \tag{9}$$

where, $\nu_i^{(j)}$ denotes the variable node with a degree i on the subset j and ϑ_i is the check node on the same degree. For multi-edge type, the check and variable node is described as,

$$\sum_{i\geq 2} \vartheta_i = \sum_{j=1}^{2} \sum_{i\geq 2} \nu_i^{(j)} = 1 \tag{10}$$

With b_1 be the length of K_b, then,

$$\sum_{i\geq 2} \frac{\nu_i^{(1)}}{i} = \frac{b_1}{E'} \tag{11}$$

where, E' is the edge of the Tanner graph. It is a fact that the additional bits should be higher than the value of M, then

$$\sum_{i\geq 2} \frac{\nu_i^{(2)}}{i} = \frac{M}{E'}(1+\beta), \qquad \beta \geq 0 \tag{12}$$

The number of parity bits g is $M(1+\beta)$, then the rate of LDPC code is,

$$R = \frac{b_1}{b_1 + M(1+\beta)} \tag{13}$$

The output of the LDPC is error corrected key which is encoded by MD5 hash function to obtain the secret key. For any communication among Alice and Bob they need to exchange this secret key.

IV. RESULT AND DISCUSSION

MATLAB 2021a is used in the proposed research work to implement a method for creating the shared key from the Nakagami-m fading wireless channel samples. The results are compared with other models that are currently in use. The simulation parameters are given in Table III.

TABLE III. SIMULATION PARAMETERS

Parameters	*Values*
Preliminary Key Length	500
Blocks	5
Block size	100
Block growth rate	100
Number of round	5
Number of iterations	10
Number of block at first round	5

The RSS and CIR based samples are obtained by Alice and Bob. The error rate between these samples, which causes the generated key bits to be in error, is **0.0988%**. For the proposed design methodology, the number of clusters formed is two having a total samples of 500 for each user.

A preliminary key is generated at the output of VQAPC for both Alice and Bob. This preliminary key is the input to the IR stage. IR is an essential step in PLKG to align the secret key between two communicating parties. At the input of the IR stage initial BMR is obtained. The number of bits in error at the output of VQAPC is 240. Hence an initial BMR of 240/500 =0.48 (48%) is obtained. This initial BMR is further reduced by the IR scheme. The preliminary key obtained by VQAPC is subjected to HPC-IR scheme to obtain a symmetric secret key. The performance of information reconciliation algorithms can be evaluated using various metrics such as BMR, information leakage, computation time and so on. The different performance metrics of HPC-IR scheme are discussed with their comparative analysis with other schemes.

a) Bit Mismatch Rate (BMR)

In IR schemes used for PLKG, BMR is a metric that quantifies the discrepancy between the reconciled keys of two communicating parties. During the IR process, both Alice and Bob compare their respective versions of the key and exchange information to align the bits that do not match. The goal is to minimize the BMR by iteratively exchanging information until both parties achieve a high level of agreement. BMR is typically computed as the ratio of the number of mismatched bits to the total number of bits in the reconciled keys. It is often expressed as a percentage or a fraction between 0 and 1, where a lower BMR indicates a higher level of agreement and a more successful reconciliation process. Reducing the BMR is crucial for ensuring the accuracy and reliability of the generated secret key. A lower BMR signifies a higher level of consistency between the keys of the communicating parties, indicating a successful information reconciliation process.

$$BMR = \frac{Ne}{N} \tag{14}$$

where N_e= No. of bits in error and N is the total No. of bits

The number of bits in mismatch of the proposed model and the BMR is given in Fig.6 and Table IV

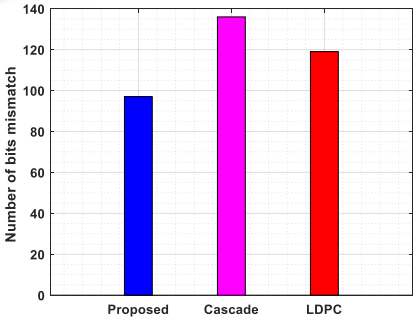

Fig. 6. Total Mismatch bits

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

TABLE IV. BIT MISMATCH RATE

Approaches	Bits in mismatch	BMR
HPC-IR	97	19.4 %
Cascade	136	27.2%
LDPC	119	23.8%

The total number of bits in error at the output of HPC-IR is 97. For the cascade protocol method, the error bit is 136, and for the LDPC method, the error is 119. Thus it is proved that the error on the proposed HPC-IR is very low compared to the other models as shown in Fig. 6.

The other performance parameters such as information leakage, interaction delay and computation time are as discussed below. These parameters are compared with the existing IR methods such as cascade [31], LDPC [39], BBBSS, BCH and Hybrid Information Reconciliation Protocol (HIRP)which is a combination of BBBSS and BCH [45].

b) Information Leakage

Information leakage, in a sense is the information retrieved by the intruder during the communication from the reconciliation.

$$L = \frac{I(V_k, r)}{K_l} \tag{15}$$

where, K_l is the length of the reconciled key V_k , r is the information revealed during the interaction between Alice and Bob. The information that the intruder perceived is $I(V_k, r)$ To ensure that the generated key is secure, atleast L amount of the corrected keys need to be removed in the final stage. The leakage information by the HPC-IR, cascade protocol, LDPC code, hybrid BBBSS and BCH is represented in Fig. 7.

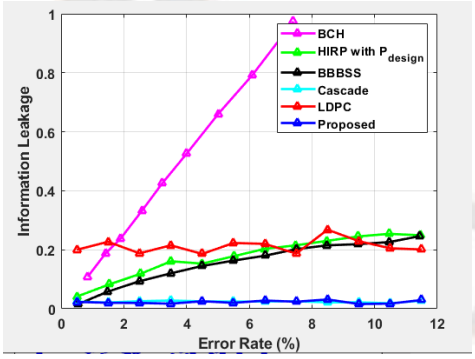

Fig. 7. Information leakage

It shows information leakage versus error rate. BCH exhibits maximum information leakage ratio that increases rapidly along the increasing error rate. LDPC has the next highest information leakage. HIRP has a similar leakage ratio to that of BBBSS and they grow slowly. Cascade has almost similar leakage ratio as of the proposed HPC-IR method which is very less as compared to the existing information reconciliation methods.

c) Interaction delay

It defines the amount of time the end user takes to share their information. In protocol based approaches, having multiple round interactions this delay is significant. This includes data transmission time and data propagation time on the channel.

$$T_{del} = T_{data} + T_{chan} \tag{16}$$

$$T_{del} = \frac{L_r}{BW} + 2\sum_{bf=1}^{h} I(bf)\left(d/\upsilon + comm_o\right) \tag{17}$$

Here, the first term is the transmission parameters, and the second is the channel parameters. L_r is the length of r and BW is the system bandwidth. Then the channel parameters are, $\sum_{bf=1}^{h} I(bf)$ denotes the number of backward and forward interactions happening in the channel with the maximum interaction limit on the channel as h , $comm_o$ is the communication overhead on the channel and d and υ are the transmission distance and light velocity.
The obtained result for the different IR schemes is depicted in Fig. 8 BBBSS has the highest interaction delay as compared to the other methods. HIRP has less delay as compared to both BCH and BBBSS. The proposed HPC-IR method has the least delay of all the methods including cascade and LDPC.

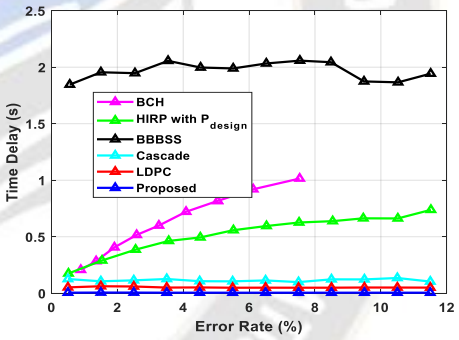

Fig. 8. Interaction Delay

d) Computation time

Computation time shortly defines the complexity of the models used. In certain resource constrained systems where the decoding process needs many round iterations, the performance of the error correcting schemes will be limited. Hence it is needed to calculate the time required for computation. This computation time is defined as,

$$C_\tau = TC.N_{eqioper} \tag{18}$$

where, TC is the time cost of an equivalent addition and $N_{eqioper}$ represent the number of equivalent additions. C_τ is obtained by finding the BMR of the initial keys. More the BMR is higher is the Computation time.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

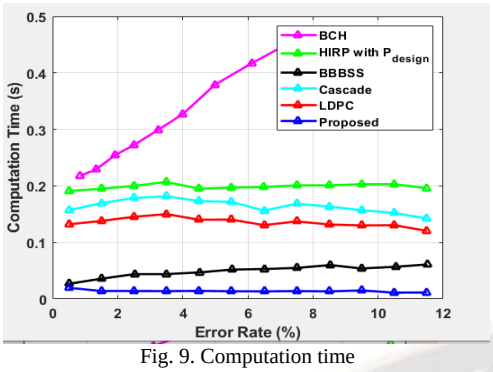

Fig. 9. Computation time

Generally, protocol based error correction methods have lower computation time as compared to the code based methods. The comparison of the computation time for error correction is presented in Fig.9. BCH shows highest computation time that increases in large BMR regions. The proposed HPC-IR method requires the least computation time.

V. CONCLUSION

In order to accurately fetch the channel samples by Alice and Bob, the RSS and CIR parameters are measured by both the users. Analysis of Alice and Bob's samples is done for error rate and have obtained an error rate of 0.0988%. They are further subjected to VQAPC algorithm which generates the preliminary keys of both Alice and Bob. The ADR obtained was 0.0019 for SNR of 40 dB. The initial BMR obtained after quantization was 48%. This mismatch in the preliminary key bits was further reduced to 19.4% by the novel HPC-IR scheme which is very low when compared to LDPC (23.8%) and cascade (27.2%). For 4% of the considered error rate the novel HPC-IR scheme achieves minimum information leakage of 0.002, minimum interaction delay of 0.001 seconds, minimum computation time of 0.02 seconds as compared to the other IR schemes.

Future Work

Future research should focus on group key generation and the multiuser domain because the majority of the physical layer key generation schemes now in use are based on point-to-point schemes. It is needed to focus more on developing techniques which make PLKG methods more robust to noise, fading and other environmental factors. Machine learning and advanced signal processing algorithms can be implemented to enhance the accuracy and efficiency of PLKG systems. Integrating PLKG methods with the existing cryptographic techniques used in wireless networks, IOT devices and vehicular networks can be of great advantage. Conducting real-world experiments and trials in different environments (urban, rural, indoor, outdoor) is crucial for validating the effectiveness of PLKG methods and understanding their limitations. Designing of energy efficient PLKG techniques is important, especially for battery constrained devices used in IOT applications. HPC-IR scheme can be extended further considering more protocol and code related IR methods to further improve the performance of PLKG system

REFERENCES

[1] Al-Shabi, M. A. "A survey on symmetric and asymmetric cryptography algorithms in information security" ,International Journal of Scientific and Research Publications (IJSRP) 9.3 (2019): 576-589.
[2] Henriques, Michelle S., and Nagaraj K. Vernekar. "Using symmetric and asymmetric cryptography to secure communication between devices in IoT", 2017 International Conference on IoT and Application (ICIOT), IEEE, (2017)
[3] Huo, Y., Tian, Y., Ma, L., Cheng, X., and Jing, T.: Jamming strategies for physical layer security. IEEE Wireless Communications 25(1), 148-153 (2017).
[4] Zhu, J., Zou, Y., and Zheng, B.: Physical-layer security and reliability challenges for industrial wireless sensor networks. IEEE access 5, 5313-5320 (2017).
[5] Khammassi, Nader, et al. "QX: A high-performance quantum computer simulation platform." Design, Automation & Test in Europe Conference & Exhibition (DATE), IEEE(2017).
[6] Li, Guyue, et al. "Physical layer key generation in 5G and beyond wireless communications: Challenges and opportunities." Entropy 21.5 (2019): 497.
[7] G. Vernam, "Cipher Printing Telegraph Systems for Secret Wire and Radio Telegraphic Communications," Journal of the AIEE, vol. 45, p. 295, (1926)
[8] C. Shannon, "Communication Theory of Secrecy Systems," Bell System Technical Journal, vol. 28, no. 4, pp. 656–715, (1949)
[9] Zeng, Kai. "Physical layer key generation in wireless networks: challenges and opportunities." IEEE Communications Magazine 53.6 (2015): 33-39.
[10] A. Ambekar, M. Hassan, and H. D. Schotten, "Improving Channel Reciprocity For Effective Key Management Systems", in Proc. International Symposium on Signals, Systems and Electronics , Potsdam, Germany, (2012)
[11] S.Kadam, and J.Gomes. "Comparative Analysis of Quantization Schemes for Physical Layer Key generation",IEEE 5th International Conference on Advances in Science and Technology (ICAST) , (2022)
[12] Aono, Tomoyuki, et al. "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels." IEEE Transactions on Antennas and Propagation 53.11 (2005): 3776-3784.
[13] Zeng, Kai, et al. "Exploiting multiple-antenna diversity for shared secret key generation in wireless networks." 2010 Proceedings IEEE INFOCOM. IEEE,(2010).
[14] Wei, Yunchuan, Kai Zeng, and Prasant Mohapatra. "Adaptive wireless channel probing for shared key generation based on PID controller." IEEE Transactions on Mobile Computing 12.9 (2012): 1842-1852.
[15] Zhang, J., Marshall, A., and Hanzo, L.: Channel-envelope differencing eliminates secret key correlation: LoRa-based key generation in low power wide area networks. IEEE Transactions on Vehicular Technology 67(12), 12462-12466 (2018).
[16] Sudarsono, A., Yuliana, M., and Kristalina, P.: A reciprocity approach for shared secret key generation extracted from received signal strength in the wireless networks. In 2018 International Electronics Symposium on Engineering Technology and Applications (IES-ETA), IEEE, 170-175 (2018).
[17] Shen, C., Li, H., Sahin, G., Choi, H-A., and Shah, Y.: Golay code based bit mismatch mitigation for wireless channel impulse response based secrecy generation. IEEE Access 7, 2999-3007 (2018).
[18] Zhang, Xinwei, et al. "Deep-learning-based physical-layer secret key generation for FDD systems." IEEE Internet of Things Journal 9.8 (2021): 6081-6094.
[19] Azimi-Sadjadi, Babak, et al. "Robust key generation from signal envelopes in wireless networks." Proceedings of the 14th ACM conference on Computer and communications security (2007)

[20] Mathur, Suhas, et al. "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel." Proceedings of the 14th ACM international conference on Mobile computing and networking (2008)
[21] Patwari, Neal, et al. "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements." IEEE Transactions on Mobile Computing 9.1 (2009): 17-30.
[22] Premnath, Sriram Nandha, et al. "Secret key extraction from wireless signal strength in real environments." IEEE Transactions on mobile Computing 12.5 (2012): 917-930.
[23] Soni, A., Upadhyay, R., and Kumar, A.: Wireless physical layer key generation with improved bit disagreement for the internet of things using moving window averaging. Physical Communication 33, 249-258 (2019).
[24] Yuliana, M.: A simple secret key generation by using a combination of pre-processing method with a multi-level quantization. Entropy 21(2), 192 (2019).
[25] Huang, L., Guo, D., Xiong, J., and Ma, D.: An improved CQA quantization algorithm for physical layer secret key extraction. In 2020 International Conference on Wireless Communications and Signal Processing (WCSP), IEEE, 829-834 (2020).
[26] Han, Q., Liu, J., Shen, Z., Liu, J., and Gong, F.: Vector partitioning quantization utilizing K- means clustering for physical layer secret key generation. Information Sciences 512, 137-160 (2020).
[27] Adil, M., Wyne, S., and Nawaz, S.J.: On quantization for secret key generation from wireless channel samples. IEEE Access 9, 21653-21668 (2021).
[28] Zhan, F., and Yao, N.: On the using of discrete wavelet transform for physical layer key generation. Ad Hoc Networks 64, 22-31 (2017).
[29] Li, G., Hu, A., Sun, C., and Zhang, J.: Constructing reciprocal channel coefficients for secret key generation in FDD systems,IEEE Communications Letters 22(12), 2487-2490 (2018).
[30] Zhang, J., Rajendran, S., Sun, Z., Woods, R., and Hanzo, L.: Physical layer security for the Internet of Things: Authentication and key generation. IEEE Wireless Communications 26(5), 92-98 (2019).
[31] G. Brassard and L. Salvail, "Secret Key Reconciliation by Public Discussion," Proc. Workshop Theory and Application of Cryptographic Techniques on Advances in Cryptology, pp. 410-423, (1994).
[32] Buttler, William T., Steven K. Lamoreaux, Justin R. Torgerson, G. H. Nickel, C. H. Donahue, and Charles G. Peterson. "Fast, efficient error reconciliation for quantum cryptography." Physical Review A 67, no. 5 (2003): 052303.
[33] Q. Wang, X. Wang, Q. Lv, X. Ye, L. You and R. Zeng, "A New Information Reconciliation Protocol in Information Theoretically Secret Key Agreement", Journal of Computational Information Systems, vol.10, no. 21, pp. 9413–9420, (2014).
[34] Wang, Qiuhua, Xiaojun Wang, Qiuyun Lv, Lin You, and Wangke Yu. "Pre-process method for reducing initial bit mismatch rate in secret key generation based on wireless channel characteristics." In Communication Technology (ICCT), pp. 888-891 ,(2015).
[35] Wang, Qiuhua, Xiaojun Wang, Qiuyun Lv, and Jianrong Bao. "Methods for improving the rate of secret key generation based on wireless channel characteristics." Journal of Networks 11, no. 2 , 46-56,(2016).
[36] Treeviriyanupab, Patcharapong, "BCH-based Slepian-Wolf coding with feedback syndrome decoding for quantum key reconciliation", Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), 9th International Conference on. IEEE, (2012)
[37] Shi, Peng, Wenjuan Tang, Shengmei Zhao, and Bei Wang. "Performance of polar codes on wireless communication channels." In Communication Technology (ICCT), 14th International Conference on, pp. 1134-1138. IEEE, (2012).
[38] Martinez-Mateo, Jesus, David Elkouss, and Vicente Martin, "Interactive Reconciliation with Low-density Parity-check Codes." Turbo Codes and Iterative Information Processing (ISTC), 2010 6th International Symposium on. IEEE, (2010).
[39] Bonello, Nicholas, Sheng Chen, and Lajos Hanzo. "Low-density parity-check codes and their rateless relatives." IEEE Communications Surveys & Tutorials 13.1 (2010): 3-26.
[40] Elkouss, David, Jesus Martinez-Mateo, and Vicente Martin. "Untainted puncturing for irregular low-density parity-check codes." *IEEE Wireless Communications Letters* 1.6 (2012): 585-588.
[41] Epiphaniou, G., Karadimas, P., Ismail, D.K.B., Al-Khateeb, H., Dehghantanha, A., and Choo, K-K.R.: Nonreciprocity compensation combined with turbo codes for secret key generation in vehicular ad hoc social IoT networks. IEEE Internet of Things Journal 5(4), 2496-2505 (2017).
[42] S. Watanabe and M. Hayashi, "Non-asymptotic Analysis Of Privacy Amplification Via Rényi Entropy And Inf-spectral Entropy", in Proc. IEEE International Symposium of Information Theory, Istanbul, Turkey, pp. 2715–2719, (2013).
[43] M.Hayashi and T.Tsurumaru, "More efficient privacy amplification with less random seeds via dual universal hash function", IEEE Transactions on Information Theory ,vol.62, no.4, pp. 2213-2232, (2016).
[44] Kadam, Sujata, and Joanne Gomes. "Quantization at the Physical layer using Affinity Propagation Clustering." 2023 World Conference on Communication & Computing (WCONF). IEEE, (2023).
[45] Li, G., Zhang, Z., Yu, Y., and Hu, A.: A hybrid information reconciliation method for physical layer key generation. Entropy 21(7), 688 (2019).
[46] Tang, Shi-Biao, and Jie Cheng. "Research on error-correction algorithm of high-speed QKD system based on FPGA." *International Journal of Quantum Information* 17.02 (2019): 1950013..
[47] Tang, B-Y., Liu, B., Yu, W-R., and Wu, C-Q.: Shannon-limit approached information reconciliation for quantum key distribution. Quantum Information Processing 20(3), 1-16 (2021).

.