Security and Safety, Vol. 3, 2023021 (2024)
https://doi.org/10.1051/sands/2023021
sands.edpsciences.org

Security and Safety in Physical Layer Systems

Review

Open Access

Information Network

Securing NextG networks with physical-layer key generation: A survey

Qingjiang Xiao, Jinrong Zhao, Sheng Feng, Guyue Li*, and Aiqun Hu

School of Cyber Science and Engineering, Southeast University, Nanjing 211189, China

Received: 24 April 2023 / Revised: 2 July 2023 / Accepted: 11 July 2023 / Published online: 18 September 2023

Abstract As the development of next-generation (NextG) communication networks continues, tremendous devices are accessing the network and the amount of information is exploding. However, with the increase of sensitive data that requires confidentiality to be transmitted and stored in the network, wireless network security risks are further amplified. Physical-layer key generation (PKG) has received extensive attention in security research due to its solid information-theoretic security proof, ease of implementation, and low cost. Nevertheless, the applications of PKG in the NextG networks are still in the preliminary exploration stage. Therefore, we survey existing research and discuss (1) the performance advantages of PKG compared to cryptography schemes, (2) the principles and processes of PKG, as well as research progresses in previous network environments, and (3) new application scenarios and development potential for PKG in NextG communication networks, particularly analyzing the effect and prospects of PKG in massive multiple-input multiple-output (MIMO), reconfigurable intelligent surfaces (RISs), artificial intelligence (AI) enabled networks, integrated space-air-ground network, and quantum communication. Moreover, we summarize open issues and provide new insights into the development trends of PKG in NextG networks.

Keywords NextG networks, PKG, massive MIMO, RIS, AI, space-air-ground integrated network, quantum technology

Citation Xiao Q, Zhao J and Feng S et al. Securing NextG networks with physical-layer key generation: A survey. Security and Safety 2024; **3**: 2023021. https://doi.org/10.1051/sands/2023021

1 Introduction

The next-generation (NextG) communication networks are expected to achieve a new network paradigm of "global coverage, full spectrum, full application, strong security" [1]. To achieve this goal, researchers have carried out a lot of research and proposed new technologies, as shown in Figure 1.

To meet the demand for global coverage, the NextG communication networks need to be effectively supplemented by non-terrestrial networks, such as satellite networks, unmanned aerial vehicles (UAV) networks and marine communication networks, and so on, for building an integrated space-air-ground network. For example, satellite communication networks can provide communication with wider coverage and higher transmission rate, which is an effective complement to the terrestrial network and suitable for areas that cannot be covered by traditional communication means, such as aviation, ocean, and desert. Moreover, with the increasing maturity of UAV networks, many high-risk jobs in harsh environments

* Corresponding author (email: guyuelee@seu.edu.cn)

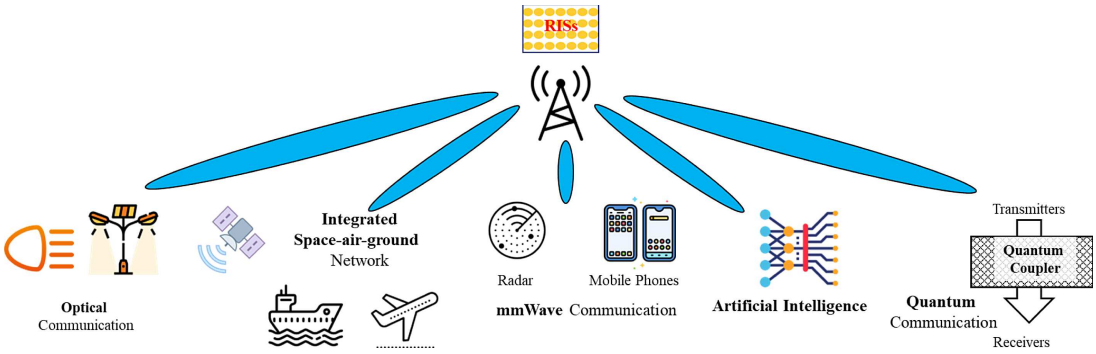


Figure 1. New technologies and potential applications of NextG networks

can be remotely operated through drones, and areas that are difficult for humans to reach during disaster search and rescue can also be explored through drones. However, with the global coverage of NextG wireless communication, an increasing number of devices will access the network through wireless communication, and available spectrum resources have become scarce, for which the full use of the full spectrum has become an important component of the paradigm of the NextG networks. To make all spectrum to be fully developed to meet the requirements of massive devices, various spectrum resources (*e.g.*, millimeter wave (mmWave) and optical frequency bands) have been extensively explored [1], especially the optical wireless communication has developed into a significant complement to the traditional spectrum [2, 3]. In the NextG networks, various devices will connect to the network worldwide, and diversified spectra resources will be explored, people expect NextG networks to have higher energy efficiency, higher data transmission rates, better network throughput, and more intelligent applications compared to previous networks. Therefore, several technologies have been further integrated and developed. For example, massive MIMO or even ultra-massive MIMO technology has received attention and is considered one of the most efficient methods to increase the network throughput of wireless communication systems [4–6]. Additionally, reconfigurable intelligent surfaces (RISs) intelligently reconfigure the propagation environment for mobile users in a cost-effective, energy-efficient, and spectrally efficient manner, which ensures that the data rate and transmission reliability of users can be dramatically improved [7–11]. Besides, the NextG network will enable a new set of smart applications with the use of artificial intelligence (AI) and big data technologies in order to deal with the vast datasets produced by the use of large devices, different communication situations, large numbers of antennas, and high data rates [1]. Finally, strong security is the prerequisite for ensuring the correct functioning of NextG networks. At present, security technologies based on cryptography have been widely applied, and physical-layer key generation (PKG), as another potential technology, has also been widely studied, which will be introduced in more detail in the following.

1.1 Security risks and traditional solutions of NextG networks

Wireless networks are easy to suffer from multiple potential attacks [12] due to the natural characteristics of their transmission medium, including but not limited to eavesdropping attacks [13], impersonation attacks [14], Denial-of-Service (DoS) attacks [15], message falsification attacks [16], *etc.* The security of user privacy and the integrity, confidentiality, and dependability of data communications are all seriously threatened by each of these threats. Especially in the NextG networks, with the frequent interaction between devices and the participation of AI technologies, the risk of data leakage in the process of collection and transmission will be further amplified. And because the service provider needs to collect a large amount of data to train the AI model, once the data set is leaked, it will cause more serious consequences than previous networks. For instance, implantable and wearable medical devices in NextG networks will be prevalently used to monitor the physical health of the elderly. These devices store historical data about physical health indicators (such as heart rate, blood oxygen levels, and sleep duration), which is sensitive personal information that requires strict confidentiality [17]. However, an attacker can use impersonation attacks to pass as a legitimate user and get access to the system and network without

authorization, which will compromise the data's confidentiality. Additionally, attackers can furthermore violate the integrity and authenticity of information transmission between devices through active attacks such as information falsification attacks. Once the data transmission security of NextG network systems cannot be guaranteed, many wireless network-based applications will experience a crisis of confidence and suffer significant losses, including the deterioration of service quality and the leakage of commercial secrets and personal information.

There has already been considerable research done to help secure wireless communications. Existing solutions are typically based on cryptography to develop cryptographic models with high computational complexity [18–20] that render it impossible for an attacker to obtain the message content while the message is still valid, which is under the assumption that the attacker's computational power is insufficient to obtain the plaintext in a finite amount of time [21, 22]. It can be seen that the cryptography-based system makes use of the mismatch between the computing resources controlled by the attacker and the computing cost necessary to crack the key to access information, thereby creating a barrier to ensure the security of information transmission. However, there is no quantitative security evidence for this, and this security guarantee could be revoked at any time as a result of the development of efficient algorithms and hardware iterations. To this end, while cryptography-based methods have successfully protected wireless network transmission in the past, they will experience more difficulties in NextG wireless communication due to the explosive proliferation of wireless network access points and the sharp rise in computing ability in recent years. The difficulties can be concluded as follows:

- First, the assumption that the encryption model is sufficiently complex and the computational power of the attacker is insufficient to break the message within the effective time is the foundation for the security of cryptography-based schemes. However, given the expeditious advancement of hardware technology [22] and the emergence of new computational techniques (*e.g.*, quantum computing [23, 24]), this assumption may be falsified and its security is hard to guarantee.
- Second, cryptography-based methods are built on convoluted mathematical protocols and issues. For devices with powerful capabilities, like smartphones, these methods work effectively. However, some low-overhead, battery-constrained lightweight devices find it difficult to match the demands of cryptography-based schemes [17], rendering them useless in these situations.
- Third, the traditional cryptography scheme relies on a key management infrastructure to manage and distribute keys, which makes it challenging to update keys on time in the face of massive devices [25] and further compromises security, and is unattractive to many distributed networks and networks with a constrained computational capacity [22].

Considering the difficulties encountered by cryptography-based schemes in facing NextG networks, there is an urgent need for security schemes with perfect security, low computing power requirements for devices, and adaptability to distributed scenarios to secure NextG networks, to overcome the new risks brought by algorithm evolution and hardware iteration, and further guarantee the security of lightweight devices and distributed networks.

1.2 Advantages of PKG

Compared to cryptographic schemes that lack sufficient theoretical proofs to guarantee security, physical layer security (PLS) techniques have attracted a great deal of attention from researchers for their solid information-theoretic security proofs. Additionally, the challenges that the cryptography scheme is encountering are anticipated to be resolved by the key generation technology based on the PLS mechanism. The PKG is to generate keys according to physical-layer characteristics, such as channel fading, noise, or device features, to realize specific security functions [26]. The PKG uses the randomness and unpredictability of the wireless channel to generate the key [22] required for information transmission between the sender and the receiver and frequently updates the key in accordance with the wireless channel's time-varying characteristics to further improve security performance.

Since the key generation process does not consume a lot of computational resources, it is also applicable in some networks consisting of low-overhead, battery-constrained lightweight devices [27]. Moreover, its information-theoretic security is achieved, for which PKG does not need to worry about being vulnerable to hardware iterations or the emergence of effective algorithms. PKG does not require a key

management infrastructure to manage and distribute keys, so they can also be widely used in many distributed networks, further expanding the application scenarios. Additionally, PLS solutions can be easily implemented and changed without almost any upper-layer protocol adjustment needed [27].

Due to the advantages mentioned above, some researchers aggressively proposed PKG protocols to meet the practical needs of various scenarios and implement real prototypes for adequate performance evaluation [28–31]. For example, Wu *et al.* [28] proposed a dynamic PKG scheme for OFDM passive optical network (OFDM-PON) systems and set up a real-time intensity modulation direct detection (IMDD) OFDM-PON system using Virtex-6 FPGA from Xilinx with fully pipelined DSP architecture. Cao *et al.* [30] built a cheap and moderately complex testbed with ESP32 and a PKG prototype is implemented on the proposed testbed.

It is worth noting that the quantum key distribution (QKD), which is based on the Heisenberg uncertainty principle and quantum entanglement, can keep the security of the keys and overcome the problems of quantum computing in the face of the improvement of the attacker's computing power and efficiency. However, the application of QKD will bring complex challenges. The most intuitive ones are the lack of suitable interfaces in the real environment and the high cost of quantum node construction, making it difficult to have enough quantum nodes to provide access services for massive user terminals. Compared to PKG which uses existing wireless network equipment for security protection, the cost of QKD is extremely high. More detailed challenges and related work on QKD are presented in Section 3.5.

1.3 Related work

Given the above advantages, PKG has received unprecedented attention for NextG network applications and various PKG schemes have been proposed to protect the network security. The existing surveys and tutorials can be mainly grouped into two categories. The first one focuses on investigating the PKG techniques themselves, as in [22, 32, 33]. In [22, 33], the authors present the fundamentals of PKG, including principles, performance metrics, channel parameters, and specific steps, where [22] briefly introduces some applications of PKG for wireless local area networks (WLANs) and wireless sensor networks (WSNs), while [33] describes the applications and implementations of the protocols on IEEE 802.11, IEEE 802.15.4, and explores potential pitfalls and future research. In [32], the authors review the existing research works on channel reciprocity-based key establishment from different perspectives, exhaustively investigate and present the works related to each step of PKG, and also discuss the feasibility, security issues, and emerging technologies in this area.

The other category starts from network security requirements, analyzes which PLS technologies need to be adopted in the network, and introduces PKG technologies in conjunction with network application scenarios, such as [34–37]. This type of review tends to present PKG as a subset of PLS, with a more abbreviated introduction, but with the benefit of being able to analyze them in the context of the needs of NextG network technologies. Li *et al.* [34] reviewed channel reciprocity-based key generation (CRKG) for 5G and beyond networks with three candidate technologies (*i.e.*, duplex mode, massive MIMO, and mmWave communications), identified opportunities and challenges for CRKG, and discusses the corresponding solutions. In [36], the authors present recent advances in PLS and security requisites for the sixth-generation (6G) networks and analyze security features and practical implementations in the context of novel applications (such as optical wireless communication and massive MIMO). In [37], the authors discuss the security and privacy of 6G networks in terms of different layers in the network architecture and analyze the impact of AI applications on 6G security. In [35], the authors provide a thorough analysis of the security challenges faced by 6G networks and discuss the possible security implications of distributed and scalable AI or machine learning (ML) security, distributed ledger technology, quantum security, visible light communication, and other applications that may encounter security and privacy issues.

Due to the lack of literature that simultaneously provides an in-depth introduction to the field of PKG and an analysis of the specific applications of PKG combined with NextG, we wrote this paper to make up for the gap, and the summary and comparison between this paper and the above-mentioned related papers are shown in Table 1.

Table 1. Comparison with available reviews in recent years

Paper	Zhang *et al.* [22]	Wang *et al.* [32]	Zhang *et al.* [33]	Li *et al.* [34]	Porambage *et al.* [35]	Mucchi *et al.* [36]	Nguyen *et al.* [37]	Our survey
Year	2016	2015	2020	2019	2021	2021	2021	2023
History	✓		✓					✓
Principle	✓	✓	✓					✓
Protocol	✓	✓	✓					✓
Parameters	✓		✓					✓
Metrics	✓	✓	✓					✓
Massive MIMO			✓	✓		✓	✓	✓
Millimeter-wave				✓			✓	✓
Quantum					✓		✓	✓
AI-enabled					✓	✓	✓	✓
RIS-assisted						✓	✓	✓
Space-air-ground								✓

1.4 Contributions and organization

In our paper, we provide a comprehensive survey of existing PKG technologies conjugated with NextG networks to help the reader better understand the prospects and applications of PKG in NextG networks. The following is a summary of our contributions:

- We provide a description and analysis of the new paradigm of NextG networks from a high-level perspective, introduce state-of-the-art technologies that are likely to be widely used in NextG networks, analyze possible security hazards and drawbacks of traditional resistance schemes, and illustrate the superior advantages of PKG in securing NextG networks.
- We introduce the initial knowledge of PKG from five aspects: the development history of the PKG field, the principles on which the effectiveness of PKG relies, the general steps of the PKG protocol, the channel parameters often utilized by PKG protocols, and the important metrics for measuring the effectiveness of PKG, and in which the challenges faced and the solutions that have been proposed are presented to help the reader gain a comprehensive understanding of the basic principles and methods of PKG.
- Combining the latest technologies of NextG, such as massive MIMO, RIS, quantum computing, AI-enabled technology, and space-air-ground integrated network. We analyze the impact of the NextG network on PKG applications and the role of PKG on NextG security, introduce the challenges and existing solutions respectively, and finally discuss the open issues and future work in depth for each technology.

The rest of this paper is structured as follows. Section 2 introduces the basics of PKG, including the development history, principles, key generation protocols, channel parameters, and performance metrics, to provide readers with a succinct overview of PKG. Section 3 introduces the application of PKG in NextG communication networks. The last section concludes this survey, the structure of our paper can be shown in Figure 2.

2 The overview of PKG

In this section, we provide a comprehensive and detailed perspective to further understand PKG, including the historical evolution of PKG, the working principle, the general stages of the protocol, common channel parameters, and performance evaluation metrics. At the same time, we analyze the difficulties that may be encountered in the implementation of the PKG protocols and extensively investigate the schemes proposed in the near years to improve the performance of PKG, introduce their core ideas, and analyze their advantages and disadvantages.

2.1 History

We provide a succinct overview of the development of PKG technology. In 1949, Shannon first proposed the idea of complete secrecy [38]. Based on Shannon, Wyner [39] developed the eavesdropping channel

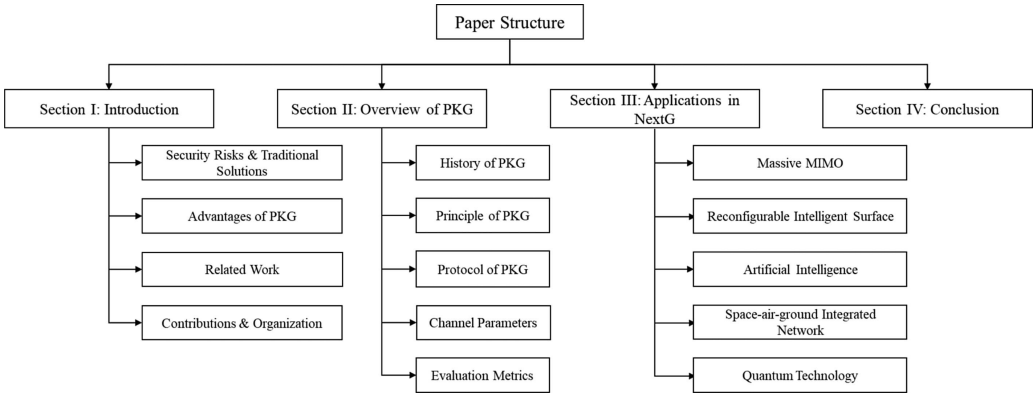


Figure 2. The structure of our paper

model, which demonstrates that channel coding can increase the secrecy transmission rate of information when the condition of the channel between the parties engaging in legitimate communication is better than the eavesdropper's channel condition. To achieve the objective of secret communication, Maurer *et al.* [40] discovered in 1993 that the two parties in a legal communication can use a random signal source known only to the two parties to produce a key. A useful key generation protocol was presented forth by Hershey [41] in 1995 and was based on the three properties of wireless channels—reciprocity, uniqueness, and randomness. Since then, many researchers have further studied the PKG in various scenarios from different angles [28, 42–45], which will be introduced later.

2.2 Principle

The principle of PKG can be summarized as three points: spatial decorrelation, temporal variation, and channel reciprocity.

- **Spatial decorrelation.** Spatial decorrelation indicates that eavesdroppers will experience uncorrelated multipath fading when they are located more than half a wavelength away from legitimate users [22, 33, 46]. For this reason, the key generated by both parties using the state information of the legal channel as a common source is difficult to be obtained by the eavesdropper, and the security is extremely high. Moreover, spatial decorrelation is a common situation because the wavelength of radio signals at frequencies commonly used for wireless communication (such as wireless fidelity (WiFi) and cellular) is very small.
- **Temporal variation.** Temporal variation means that the communication environment of the wireless channel changes obviously with time, which is caused by unpredictable random movement of transceivers and any object in the environment because the movement will change the reflection, refraction, and scattering of the channel path. Temporal variation is conducive to the frequent generation and update of physical-layer keys and strengthens the security of communication systems.
- **Channel reciprocity.** Channel reciprocity means that the transceivers at both ends of the wireless link experience the same multipath fading and observe the same channel state, which is a prerequisite for enabling the transceivers to generate the same key. It is noteworthy that a time-division duplex (TDD) communication system has better channel reciprocity than a frequency-division duplex (FDD) system generally, which is due to the fact that in TDD systems, the same frequency is used for the uplink and downlink, while in FDD systems two different frequencies are used. For this reason, the uplink and downlink signals in TDD systems are more likely to be received and transmitted in the same way, resulting in better channel reciprocity.

2.3 Protocol

In recent years, there are many practical protocols have been proposed to optimize the performance of PKG and meet the constraints of different scenarios, such as maximizing the sum key generation rate

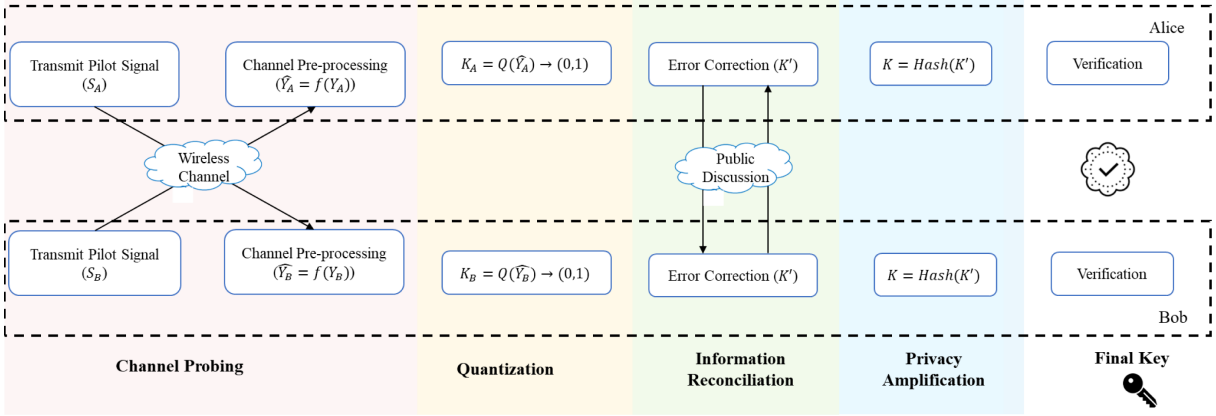


Figure 3. The general procedures of PKG protocols

(KGR) and reducing the pilot overhead. However, they are generally composed of four steps: channel probing, quantization, information reconciliation, and privacy amplification [25, 29, 42, 47, 48], which are portrayed in Figure 3.

As depicted in Figure 3, there are two legitimate users, namely Alice and Bob, and their PKG process can be summarized as follows: Alice and Bob perform channel probing firstly to obtain channel information, such as obtaining Y_{A} and Y_{B} by sending pilot signals S_{A} and S_{B} to the other party respectively and performing channel estimation based on the received signals, and often a preprocessing method is used to eliminate interference from non-reciprocal factors. They then converted the measurements into digital binaries by quantization to get the raw keys K_{A} and K_{B}. Since there may be a mismatch between K_{A} and K_{B}, information reconciliation is applied to resolve any inconsistency that might be present. Considering the possible information leakage in the past steps, privacy amplification is employed to remove the leaked information. Finally, key verification terminates the PKG process. We will describe each of the four main steps in detail later.

2.3.1 Channel probing

Both communication parties need to use the same random source as input to generate the identical key, which generally requires channel probing to obtain the reciprocal information. Due to the random and reciprocal nature of the wireless channel, channel characteristics such as the received signal strength (RSS), channel state information (CSI), and angle of arrival are widely used random sources [49]. As shown in Figure 3, Alice and Bob first send pilot signals S_{A} and S_{B} to each other for obtaining channel characteristics. Through the transmission of the wireless channel, the signals they receive can be given as

$$Y_{\mathrm{A}} = h_{\mathrm{BA}} S_{\mathrm{B}} + N_{\mathrm{A}} \tag{1}$$

$$Y_{\mathrm{B}} = h_{\mathrm{AB}} S_{\mathrm{A}} + N_{\mathrm{B}} \tag{2}$$

where the h_{BA} and h_{AB} are the channel responses from Bob to Alice and from Alice to Bob respectively, N_{A} and N_{B} are the zero-mean complex white Gaussian additive noise at Alice and Bob. Significantly, the time t_{A} and t_{B} of Alice and Bob transmitting the pilot signals are not synchronized. Considering the reciprocity of the channel, the time difference $\Delta t = |t_{\mathrm{A}} - t_{\mathrm{B}}|$ must be less than the channel coherence time for which the channel can be considered constant during the two probes [22].

Consider that in real-world applications, the reciprocity of wireless communication systems is affected by the environment and equipment, including hardware fingerprint differences between devices produced by different manufacturers and external additive noise [22, 50]. Such non-reciprocal factors will make the values of channel characteristics measured by adjacent probes correlated and further reduce the reliability of the PKG schemes [49]. Therefore, it is necessary to preprocess the acquired channel characteristic measurements before the subsequent steps to reduce the correlation between the characteristic measurements. Several preprocessing methods have been developed to eliminate the correlation [22, 49], such as principal component analysis (PCA) [49, 51], discrete cosine transform (DCT) [52, 53], filtering-based algorithms

[50, 54–57] and weighted sliding window smoothing [58]. Li *et al.* [51] proposed a preprocessing method based on PCA to solve the non-reciprocity and correlation issues in key generation from orthogonal frequency division multiplexing (OFDM) channel measurement. In [49], a general mathematical model for several preprocessing strategies was proposed and the preprocessing performance was compared by numerical simulations. The results demonstrated that enhanced key generation by PCA using common eigenvectors can obtain keys with a high KGR, low key error rate, and good randomness. In [56], Zhang *et al.* designed a low pass filter for the key generation system which is based on OFDM subcarriers' channel responses to have better channel reciprocity and less noise, and ultimately reduce the key disagreement rate (KDR). In [55], authors preprocess the channel measurements before quantization with simple moving average filtering to improve channel reciprocity. In [58], authors proposed weighted sliding window smoothing to reduce noise, which can smooth out local noise, and also make up for the mismatched sensing time caused by the half-duplex nature.

2.3.2 Quantization

After doing the aforementioned channel probing, Alice and Bob acquire preprocessed channel measurements $\hat{Y_{\mathrm{A}}}$ and $\hat{Y_{\mathrm{B}}}$, respectively, which are analog values that cannot be utilized directly by PKG schemes. For this reason, the objective of quantization is to map the preprocessed channel characteristic measurements $\hat{Y_{\mathrm{A}}}$ and $\hat{Y_{\mathrm{B}}}$ into binary sequences K_{A} and K_{B} (also the raw keys).

Recent research [32] shows that the performance of the quantization has a direct impact on the KGR and the KDR, which depends on the selection of the quantization levels and quantization thresholds. In general, a multi-level quantization will lead to a higher KGR while being more vulnerate to non-reciprocity factors and further cause a higher KDR.

The number of quantization levels is affected by the signal-to-noise ratio (SNR) of the channel [22] and the thresholds are usually determined according to the mean, standard deviation, and distribution of the measured values [22, 33, 46]. Taking the dual-threshold quantization scheme as an example, the quantization function expression is shown in the formula:

$$Q(x) = \begin{cases} 1, & x > q^+, \quad q^+ = \mu(x) + \alpha\sigma(x) \\ 0, & x < q^-, \quad q^- = \mu(x) - \alpha\sigma(x) \end{cases} \tag{3}$$

where $\mu(x)$ and $\sigma(x)$ represent the mean and stand deviation of x, and α is the quantization factor used to control the quantization threshold position. The measured values between q^+ and q^- will be dropped and others will be mapped into one or zero. In addition, to improve quantization performance and deal with active attacks, several quantization schemes adjust the threshold adaptively [59, 60] and multi-bit quantization schemes [41, 61, 62] were proposed.

2.3.3 Information reconciliation

There might have a small number of inconsistent bits in the keys K_{A} and K_{B} generated by Alice and Bob through quantization due to the non-reciprocity factors [32], for which information reconciliation is applied to find and correct the mismatch bits in raw keys, and finally get the same key K'. The workflow of information reconciliation based on error correction code (ECC) is shown in Figure 4. The communicating parties, Alice and Bob, first divide the raw keys K_{A} and K_{B} generated during the quantization process into blocks. Next, Alice encodes the blocks of K_{A} and sends the calculated syndrome to Bob, who employs the corresponding decoder to obtain the desired codebook, consisting of K_{B} and the received syndrome. Bob performs error correction by the ECC, and Alice and Bob then apply CRC to determine whether the keys agree or not. If the check values of Alice and Bob are the same, *i.e.*, $C^A = C^B$, then the key agreement is reached and the process proceeds to the privacy amplification step, otherwise, it goes back to the channel probing.

Recently, various information reconciliation protocols have been proposed over the years, such as Cascade [63], low-density parity-check (LDPC) [64], Turbo codes [65], and Polar code [66], which enable the keys to achieve agreement by error detection or error correction. In [63], the authors proposed an efficient protocol where the amount of information leaked during reconciliation is close to the minimum possible amount of information for a sufficiently reliable secret channel. Many PKG protocols have adopted

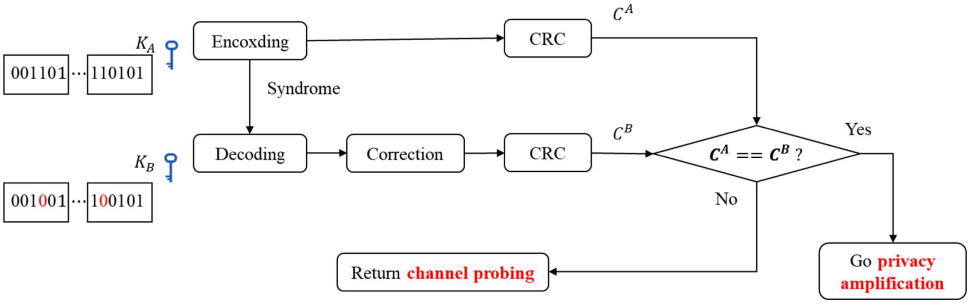


Figure 4. The workflow of ECC-based information reconciliation

this scheme for information reconciliation, such as [60, 67, 68]. In [64], the authors describe in detail two algorithms based on binary and quadratic LDPC codes, the latter of which is more suitable for high SNR environments. Epiphaniou *et al.* [65] generate random and symmetric encryption keys by utilizing the properties of dynamic propagation channels and innovatively integrating time-variable properties into the key generation process, the experimental results show that the use of Turbo codes has a substantial boost in KDR and KGR. In [66], the authors design a protocol for generating keys in correlated Gaussian random variables based on polar codes and prove that the protocol based on polar codes outperforms similar protocols that use LDPC codes instead of polar codes.

2.3.4 Privacy amplification

During information reconciliation, some information may be obtained by eavesdroppers in public discussions, which can jeopardize the security of the generated keys. Privacy amplification is then adopted [22] to reduce the information leakage about the generated keys to eavesdroppers, such that the final key is secure against attacks. Common privacy amplification protocols are mainly implemented based on extractor [69, 70], or hash functions [70–74].

2.4 Channel parameters

PKG relies on channel parameters for extracting secret keys from the wireless channel, which is the random source to generate identical keys and characterized by several physical properties such as multipath, fading, and noise. In this subsection, we will discuss the key channel parameters used in PKG and their impact on the security and performance of the generated keys. Common channel parameters include channel impulse response (CIR), channel frequency response (CFR), phase information, RSS, precoding matrix index (PMI), and so on.

RSS is widely used as the channel parameter for PKG because they are easy to measure [32] and can be obtained without additional hardware, making it a cost-effective solution. Moreover, RSS-based PKG protocols can be implemented in various wireless communication systems, such as 802.11 systems [59, 75–78] and 802.15.4 systems [79–81]. Another widely used channel parameter is CSI, including channel phase [82–84], CIR [85, 86], and CFR [87], which provides more accurate information than RSS and can reduce errors when extracting keys. In addition, CSI can model the effect of frequency-selective channels more accurately, and therefore can better resist interference. Besides, CSI can also improve the efficiency and reliability of key extraction by using the information of multipath propagation. However, there are drawbacks to obtaining the key using the CSI as well. For instance, it is expensive and requires high-quality hardware equipment to get the CSI, and obtaining CSI demands sophisticated algorithms for complex signal processing. Moreover, CSI may be forged by an attacker, which will compromise the security of PKG. In addition, PMI-based key extraction schemes [88, 89] are explored. Considering the correlated MIMO channel, Wu *et al.* [88] proposed PMI-based secret key generation with rotation matrix (MOPRO), and the experimental results show that the KDR is dramatically reduced and the communication overhead is greatly decreased. In [89], Taha *et al.* proposed a new physical layer approach to exchange keys in MIMO channels using private random precoding (PRP), which is applicable to both TDD and FDD systems and has an excellent performance in computational overhead and key agreement.

It is worth mentioning that in recent years, there have also been some schemes that use other channel parameters to generate keys, such as the angles of arrival and departure [90], signal envelopes [91], *etc.* Overall, the selection of channel parameters for key generation will be mainly determined by the wireless technology used, and the randomness, stability, repeatability, and acquisition difficulty of channel parameters should be considered comprehensively.

2.5 Evaluation metrics

To evaluate the performance of PKG, several metrics are widely used. In this subsection, we will discuss some of the most commonly used metrics.

- **KGR.** KGR is an important performance metric, referring to the speed at which a secure key can be generated by utilizing the inherent randomness in the wireless channel. The KGR is typically measured in bits per second (bps), which can be given as

$$\mathrm{KGR} = \frac{L}{T} \quad (\text{bits/s}) \tag{4}$$

  where L represents the length of the key and T is the time taken.
- **KDR.** KDR is a critical performance metric in PKG that quantifies the probability of different bits between the raw keys generated by Alice and Bob after quantization, which can be defined as

$$\mathrm{KDR} = \frac{\sum_{i=1}^{L} |K_{\mathrm{A}}(i) - K_{\mathrm{B}}(i)|}{L} \tag{5}$$

  where L represents the length of keys, $K_{\mathrm{A}}(i)$ and $K_{\mathrm{B}}(i)$ are the ith bits of K_{A} and K_{B} respectively, which is the raw key generated by Alice and Bob after quantization.
- **Randomness.** Similar to KDR and KGR, randomness is also an important metric used to evaluate PKG performance. With higher randomness, the key is more unpredictable and has better security. The randomness test suite developed by the National Institute of Standards and Technology (NIST) is a set of statistical tests used to evaluate the quality of randomness in digital data. And the NIST randomness test suite is often used to evaluate the quality of the keys generated by PKG and verify whether the keys meet certain statistical properties.

3 The applications of PKG in the NextG networks

In this section, we explore the impact of NextG networks on the PKG field and the potential of PKG for ensuring NextG security. Moreover, we provide in-depth analysis from five aspects (*e.g.*, massive MIMO, quantum technology, AI, RIS, and space-air-ground integrated network). In each subsection, the faced challenges and existing research work will be introduced in detail, and urgent open issues and future work are discussed as well.

3.1 Massive MIMO

Massive MIMO is one of the key technologies to improve 5G NR frequency efficiency. In Massive MIMO systems, large-scale antenna arrays are formed by simultaneously utilizing tens to hundreds of antennas at a base station (BS). Numerous antennas can be used to spatially multiplex many user terminals (UTs). Therefore, users can be flexibly selected to receive at any given time, significantly improving spatial resolution and degree of freedom [92]. To go further, in order to achieve higher bandwidth and faster wireless communication, researchers in [93] introduced the idea of ultra-massive (UM) MIMO (1024×1024). UM MIMO technology employs hundreds or thousands of antennas on the BS side to greatly enhance the throughput, energy efficiency, and robustness of wireless communication systems. Massive MIMO and UM MIMO will still be the focus of NextG mobile communication research and will not only be limited to the ground mobile communication systems but also be applied to the satellite communication systems,

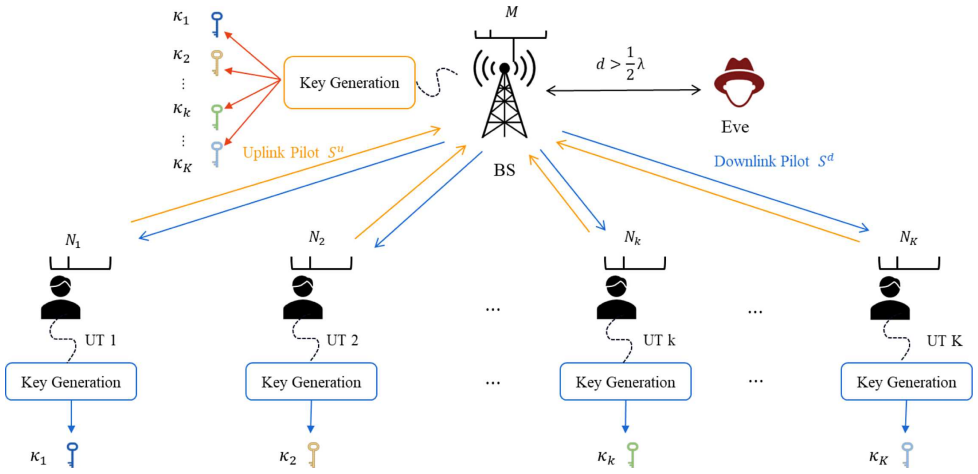


Figure 5. System model of massive MIMO for PKG

ocean communication systems, and high-altitude platform communication systems, which is one of the core technologies to form full-scene communication in the near future [94].

While the massive MIMO technology has brought great advantages in improving the spectrum efficiency and scheduling complexity of the system, it is also faced with communication security problems in diversified multi-service scenarios. At present, traditional upper-layer encryption technology has been widely used to ensure information security. However, with the huge increase in wireless devices, key distribution between massive devices has become complex and even impractical, and traditional encryption techniques may not be sufficient to guarantee information security [95].

3.1.1 Massive MIMO for PKG: Advantages and challenges

PKG has provided a new paradigm for information theory secure key sharing. In massive MIMO systems, PKG technology can solve the shortcomings of traditional key distribution schemes and provide security for communication. Meanwhile, massive MIMO technology also brings many benefits to PKG and boosts the key generation performance. In massive MIMO scenarios, the BS generates a narrow and directional beam aimed at different users. Narrow beams and directional beams increase the received SNR and KGR, while significantly weakening the received SNR of eavesdroppers [34]. Simultaneously, the key generation rate increases linearly with the number of antennas [96]. In addition, if the number of antennas is greater than the number of propagation paths, the wireless channel will exhibit sparsity. This sparsity can contribute to obtaining channel reciprocity information such as CSI. To this extent, massive MIMO technology is more conducive to the realization of PKG. Figure 5 shows a massive MIMO model that the BS is provided with M antennas and the kth UT is provided with N_k antennas. The BS generates secret keys $\kappa = \{\kappa_1, \kappa_2, \cdots, \kappa_K\}$ with K UTs concurrently, where κ_k is the pairwise key generated by BS and the kth user. In traditional PKG protocols, the BS and the user send orthogonal pilot signals to estimate CSI. Considering passive eavesdropping, it is assumed that the distance from Eve to BS and all UTs is greater than half wavelength. As a result, we regard the channel observations between BS and UTs are independent of Eve's channel observations. Because of the open nature of the wireless channel, all UTs can receive signals. Consequently, in addition to Eve, other UTs are also regarded as potential eavesdroppers [97].

Even though the extensive number of antennas benefits the communication systems, massive MIMO for PKG imposes new challenges that can be categorized as:

- **Difficult channel probing.** Most of the research on PKG is in the TDD mode, where the BS and users alternately send pilots to probe the channel. When the sampling time difference between them is within the channel coherence time, both parties can estimate the CSI with a high correlation. However, in the multi-user system with orthogonal pilots, an enormous number of pilots are introduced to distinguish different users. The pilot length and the number of antennas have a linear relationship, so

it becomes difficult to complete channel probing in the coherence time when there are a large number of antennas or users [98].

- **Inter-user interference.** When different users communicate using non-orthogonal pilot signals (or shared pilot signals between BSs), significant inter-user interference will occur. This interference will affect the reciprocity of channel measurement, resulting in the failure of both parties to obtain the same key. Additionally, the interference will cause some correlation between different users, which may result in secret key leakage.
- **High dimension of the channel matrix.** Because of the spatial correlation of antennas, the channel probing results often exhibit high auto-correlation characteristics, resulting in long 0 and 1 in the quantized bit sequence. Traditionally, preprocessing algorithms can be used to reduce correlation, such as PCA [49, 51] and DCT [52, 53]. However, in massive MIMO systems, the number of antennas at the BS and UTs side is extremely large. The complexity of executing preprocessing algorithms such as PCA will increase as the dimension of the channel matrix increases.
- **Pilot contamination attack.** The eavesdropper can launch a pilot contamination attack by sending BS the pilot signal that is identical to that of legitimate users. Then the CSI estimated by the BS is not the legitimate user, but the sum of users and eavesdroppers. Therefore, the channel probing results of BS and users may not be reciprocal, so both parties cannot generate a consistent secret key.

To sum up, the problems of implementing PKG in massive MIMO systems mainly focus on the difficulty of calculating high-dimensional channel matrices and large pilot overhead leading to excessive channel probing time.

3.1.2 Solution methods

Currently, the issues of PKG in massive MIMO scenarios have attracted extensive research. Fortunately, some preliminary solutions have been proposed, including beam domain-based channel dimensionality reduction algorithms and utilizing new channel features. Below are some measures presently being proposed to address the above issues.

- **Reduce pilot overhead.** The large pilot overhead caused by multiple antennas makes the time delay exceed the coherence time, which leads to the key generation failure. At present, there has been some research on reducing pilots. An optimization method was proposed in [97] to achieve maximum sum KGR with pilot reuse which means that different users transmit the same pilot signal. By designing appropriate precoding and receiving matrices, interference between different UTs will be reduced. This method can achieve nearly perfect channel CSI and significantly reduce the pilot overhead caused by the increase in UTs quantity. Chen *et al.* [98] introduced an interference neutralization-based multi-user beam allocation (IMBA) algorithm for pilot multiplexing. The algorithm designs precoding and receiving matrices to assist key generation. Compared to using orthogonal signals, this method can greatly reduce pilot overhead.
- **Optimize computational complexity.** Research has also been launched on the computational complexity of channel high-dimensional matrix. Li *et al.* [99] proposed a key generation method based on loop-back, called two-band multiple-antenna loop-ack key generation (TB-MALA), to address the high auto-correlation problem in MIMO systems. The method also effectively reduced the effective channel auto-correlation by making use of the rotation matrix. In view of the computational complexity and time consumption resulting from high dimensional matrices in massive MIMO wireless communications, the optimization problems of the multi-user secret key generation are studied in [43]. The power allocation algorithm and the beam scheduling algorithm are presented to achieve the optimal solution. This method can obviously decrease the channel matrix dimension and reduce inter-user interference. Jiao *et al.* [90] suggested utilizing novel channel characteristics to generate a consistent secret key in massive MIMO systems, for instance, virtual angle of arrival (AoA) and angle of departure (AoD). Employing virtual sparse channel estimation methods to estimate at low overhead is relatively easy, and greatly reduces complexity compared to estimating high-dimensional CSI.
- **Resist pilot contamination attack.** Regarding pilot contamination attacks, in [100], authors proposed a secret key agreement (SKA) protocol that can detect pilot contamination attacks. There is a complementary relationship between the received signal strength of eavesdroppers and legitimate users, so this relationship can be used to measure the amount of information leaked to eavesdroppers.

Specifically, if the pilot contamination attack detector declares the presence of a pilot contamination attack multiple times, the SKA protocol will suspend the key generation process to prevent eavesdroppers from obtaining information. The numerical results indicate that the SKA protocol can effectively constrain the impact of the pilot contamination attack on the SKA by adjusting the pause threshold, which ensures the performance of key generation between BS and users.

3.1.3 Future works

Massive MIMO technology will continue to develop in NextG networks. The mmWave massive MIMO and UM MIMO are also considered potential technologies for future communication. The following are some research opportunities and future directions.

- **PKG in mmWave massive MIMO.** In the future wireless network, mmWave is expected to improve the network capacity and data rate, and massive MIMO is used to overcome the high propagation path loss of the mmWave channel. Higher frequency and more antennas bring new channel characteristics, such as fewer propagation paths, greater attenuation, *etc.*, which pose new challenges to PKG.
- **Multi-cell and multi-user key generation.** Cellular networks usually contain multiple BSs. Cellular communication involves a large-scale connection on a limited wireless spectrum, and the pilot resources between cells are multiplexed. High-frequency pilot reuse makes users at the edge of the cell suffer from co-frequency interference from adjacent cells, and there is inter-user interference among users in the cell. BSs and users may not be able to generate symmetric keys because interference affects channel estimation results. How to solve the impact of interference on PKG is a problem to be further studied.
- **PKG in UM MIMO system.** The ultra-massive antenna provides NextG with richer communication resources and higher degrees of freedom. And UM MIMO can be combined with other key technologies, such as terahertz and high-speed rail communication. More antennas also bring more opportunities and challenges to PKG. More research and exploration are needed on how to apply PKG in UM MIMO scenarios.

3.2 Reconfigurable intelligent surface

A RIS consists of a large number of passive reflecting elements, each element can independently change the propagation characteristics of the signal, such as amplitude and phase, in an expected or random way. Unlike traditional relay stations, it only controls the reflection of the signal and does not consume extra power, making it low-power and environmentally friendly, which is very attractive to some resource limited networks, such as sensor networks. The low power consumption brings about a low cost and easy implementation, which means it can be used with a wide range of wireless network types. Finally, it can be flexibly deployed according to communication requirements [101]. These features make it a key technology in the future network technology revolution [102]. For example, in 5G, massive MIMO, and mmWave communication play important roles. The former improves communication quality and expands signal coverage range, and the latter has fast data transmission speed and strong anti-interference ability. However, these technologies still face many difficulties and challenges in practical scenarios. RIS can effectively compensate for these shortcomings. On the one hand, the energy consumption of massive MIMO systems is very high, while the power required by RIS is much lower than that of traditional relay nodes. Moreover, RIS can be used to optimize the energy efficiency of the MIMO system [103–105] so that the power or energy needed can be further reduced; on the other hand, the signal propagation path of mmWave communication is easily blocked by objects, using RIS to reflect the signal is a feasible solution to the issue [106].

As it can help to build a controllable signal propagation environment, RIS has also been widely studied in the field of PKG. Below, we will introduce the research work on RIS into two kinds, which correspond to the two kinds of influences that RIS brings to PKG: positive and negative.

3.2.1 Positive impact: RIS-assisted PKG

At present, in RIS-assisted PKG, two issues have attracted much attention, *i.e.*, how to generate randomness for PKG by exploiting RIS in a static environment, and how to design schemes of RIS configuration in a dynamic environment to optimize the performance of PKG, such as KGR.

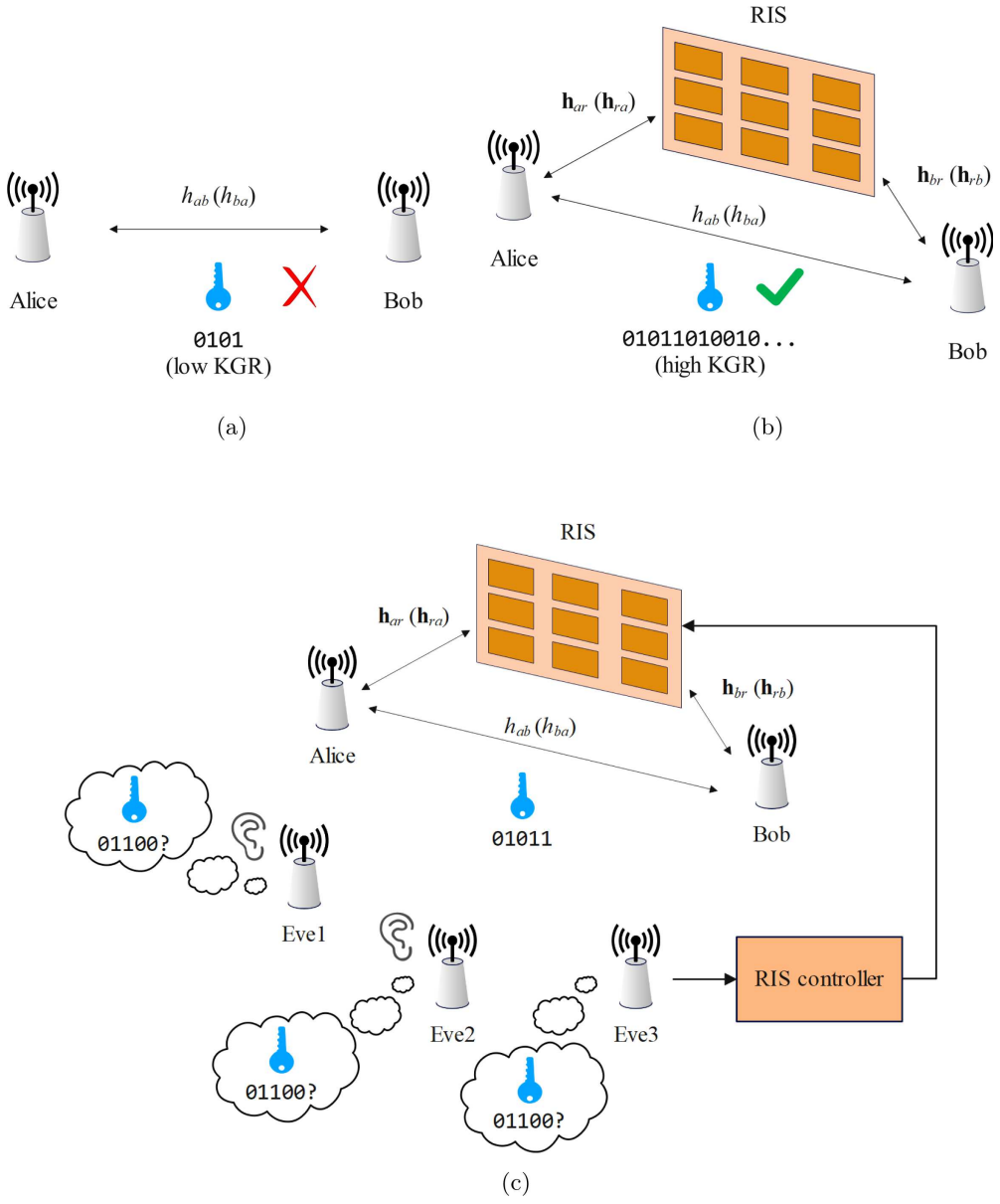


Figure 6. Positive and negative impacts of RIS on PKG. (a) The KGR is very low in static environments. (b) Positive impacts: RIS provides (i) more randomness for PKG in static environments, and (ii) more possibilities for KGR optimization in dynamic environments. (c) Negative impacts: RIS may be exploited by active attackers

Static environment refers to the environment, such as the communication environment between devices with fixed indoor positions, where the channel characteristic parameters lack change. However, we cannot directly extract secret keys from the channel that lacks change, otherwise, as shown in Figure 6a, it will lead to extremely low KGR or a large number of consecutive repeated bits, which poses a great threat to communication security. As shown in Figure 6b, by deploying RIS in static environments, a new solution to increase randomness has been found.

The greater KGR, the more secret key bits can be obtained per unit of time or a single channel measurement period, and the more secure communication requirements between communication nodes can be met. The optimization of the coefficient matrix for RIS to improve KGR is a hot topic of research in dynamic environments, as shown in Figure 6b. However, under most circumstances, the expression of KGR may be very complex, so the optimization problem is difficult to solve, we can only find its sub-optimal solution.

- **PKG in static environment.** In [107–109], Random RIS phase configuration schemes are used to simulate the dynamic time-varying channel. Specifically, in [107], the remote controller of RIS calculates the optimal phase switching time immediately after Alice and Bob send the pilot signal, and then switches the RIS phase randomly. It is very hard to derive a closed form of the KGR expression for RIS channel coefficients with discrete phase shifts, in contrast to studies based on Gaussian channel coefficients. Therefore, in [107], only two extreme conditions, *i.e.*, high SNR and massive RIS elements are analyzed. The analysis of the condition of massive RIS elements is meaningful because the numerical results show that when the number of elements is 20, the KGR is very close to the theoretical upper limit. Moreover, the KGR of the proposed scheme is higher than the other two benchmarks based on the artificial random signal. In [108], Alice and Bob first estimate the direct channel and then remove the direct channel estimation from the signal observed by the receiver in each time slot to obtain the sub-reflecting channel estimation, respectively. Different from the two-way probing (TWP), in the one-way probing (OWP) used in this scheme, Bob measures the channel in downlink slots, and then Alice reconstructs the CSI based on the direct channel estimation and the sub-reflecting channel estimation. But the study did not propose an algorithm to optimize the achievable KGR. In [109], a PKG scheme using RIS for channel phase probing was proposed, which uses RIS to randomize the phase of the probing signal to generate randomness. In the quantization stage, Bob divides $[0, 2\pi)$ equally into 2^W sub-intervals, where W is a positive integer. Each sub-interval represents a sequence of binary bits, and the initial KGR is the set of the bit sequences corresponding to all sub-channel phase estimation. Uncommon in other studies, this research analyzed the impact of deployment locations of RIS on PKG performance. Currently, most of the research on RIS remains in the theoretical stage, but some studies have delved further into the research. In [110, 111], the authors implemented a prototype system using commodity Wi-Fi transceivers and a low-cost RIS in a low-entropy environment to assist the PKG of the OFDM system, respectively.
- **PKG performance optimization.** In the single-user scenario, the authors of the study [112] regarded the RIS as a passive beamformer and then derived the minimum achievable secret key capacity under the condition that multiple eavesdroppers are nearby, Finally, an optimization algorithm to improve the performance of PKG protocols was proposed. In [113], a multiple-input single-output (MISO) system was considered, and the authors deduced the minimum achievable secret key capacity. Then, an optimization algorithm was proposed to maximize it by configuring the reflecting coefficient matrix of RIS. In short, this study used RIS to improve the lower limit of the secret key capacity and enhance the security of the system. In the multi-user scenario, Li *et al.* [114] considered a multi-user channel model, and gave the optimization algorithms to maximize the sum KGR of multi-users when the channels between users are independent and correlated respectively. To deal with the non-convexity of constraints, the above articles apply the semi-definite relaxation (SDR) method to relax the constraints. The complexity of the optimization algorithms is reduced by applying the successive convex approximation (SCA) technique which can obtain a sub-optimal solution.

3.2.2 Negative impact: RIS-based attacks in PKG

While RIS has brought positive impacts, security issues have also arisen. As shown in Figure 6c, active eavesdroppers may exploit the RIS to design attack schemes. Some attackers may even seize control of the RIS. Currently, much research has been done on RIS-based attacks. Designing attacks against RIS is beneficial to attract research on designing corresponding countermeasures, which will make the RIS technology more mature.

Wei *et al.* [115] pointed out the serious impact of the pilot spoofing attack (PSA). Eve and Alice send amplified pilot sequences at the same time. Eve can increase the possibility of obtaining legal channel probing samples by increasing the amplifying factor. The study first analyzes how RIS can improve the performance of PKG under PSA. The results show that with the increase of spoofing factor, the upper bound of KGR quickly approaches 0, which means that RIS has limited effect on defending against powerful PSA. Secondly, the influence of RIS on legitimate communication after it is controlled by attackers is analyzed. The spoofing KGR increases with the increase of the spoofing factor, and if it is optimized, the spoofing effect will be significantly strengthened. The study points out that the traditional scheme of optimizing RIS phase configuration is difficult to work against PSA. The authors of [116] proved that colluded Eves are able to obtain secret keys according to the globally known pilot sequence. They

replaced the pilot sequence with a random Gaussian matrix to cope with the challenge. The secret key is generated according to the fact that the singular values of probability distribution functions (PDF) of legitimate nodes' received signal matrices are very similar. The scheme does not need legal channel estimation, because the channel used for PKG is not required in the subsequent wireless communication. A muti-Eve attack scheme is also designed [117]. In the proposed scheme, Eves estimated the legal channel by making the entropy of the legal channel conditioned on Eves' signals approached zero. In [111], two kinds of attacks against RIS were proposed, namely the RIS jamming (RISJ) attack and the RIS leakage (RISL) attack, respectively. RISJ attack is an active attack, which prevents Alice and Bob from agreeing on the shared secret key by adjusting the RIS reflection matrices. Unless separating the direct channel and the RIS-induced channel in a system with a high multipath resolution, it is still challenging to find a strategy to resist this attack. In the RISL attack, the secret key will be obtained by Eve. RISL attacks can be divided into two kinds, in the first kind of RISL, Eve controls the configuration of RIS elements in a predetermined way, such as controlling their switching state, to make the channel measurement results of Alice and Bob meet Eve's expectations. In the second RISL type, Eve attempts to speculate on the legal channel. But this kind of attack imposes a high requirement for Eve and is more possible to succeed in some specific environments. Works in [118] are instances of RISL attack. The study features in that the RIS only plays a malicious role in the PKG system. Specifically, the RIS is controlled by Eve and is used to reconstruct the secret key to a certain extent.

3.2.3 Future works

As a potential technology, the research and application prospect of RIS is very broad, but there are still many key problems that have not been solved, which deserve more research in the future. Here are some examples:

- **Consider security issues when optimizing RIS configuration.** At present, most research on RIS mainly focuses on performance optimization, effective and low-complexity channel estimation, *etc.* Moreover, it is usually assumed that RIS is friendly, but the actual situation is that RIS may be exploited by attackers. So future work should pay attention to the coexistence of friendly RIS and malicious RIS, and the role of RIS in minimizing the secret information leaked to Eve, that is, optimizing the configuration of RIS to improve the communication security of the system. In addition to defending against active and passive RIS-based attacks, we are also faced with the challenge of how to detect and locate attackers.
- **RIS-assisted mmWave massive MIMO system.** The mmWave communication has abundant available frequency band resources because of its short signal wavelength, but mmWave signals are more easily blocked by obstructions, so they mainly propagate in line-of-sight (LoS) environments, which leads to serious path loss. Combining it with a massive MIMO system can effectively alleviate this problem, which has become one of the key technologies of 5G and NextG communication networks. However, the current challenge is to solve the resulting high power consumption problem. The emergence of RIS technology provides a feasible solution to it. It is believed that combining RIS with mmWave massive MIMO system [119, 120] will improve the performance and enhance the security of communication systems, and reduce power consumption and cost.
- **RIS deployment location, multi-RIS scheme, and cooperation between RISs.** Currently, most research in the field focuses on optimizing the configuration of the elements and the reflection coefficient matrices of RIS to improve data transmission speed, secrecy rate, or KGR, *etc.*, while fixing the RIS in a certain position. However, there is no reason given for the selection of the deployment location of the RIS. In other words, there is still a lack of research on the impact of the deployment location of the RIS on system performance. Moreover, the spatial position of RIS can be used as a new degree of freedom. For example, RIS can be deployed on a drone to enhance channel randomness through the drone's random movement, thereby assisting secret key generation. In addition, there is currently almost no research discussing the scheme of multiple RISs and how they collaborate. Generally speaking, multiple RISs can bring more randomness. As the number of RISs increases, the computational overhead caused by optimizing the reflection coefficients also increases. Therefore, how to reduce the computational complexity and secret key generation delay is also worth studying.
- **RIS authorization and countermeasures against adversarial RIS.** In PLS, there have been a lot of meaningful studies utilizing RIS to enhance the security of wireless communication networks.

However, the characteristic of RIS being able to only reflect signals and not actively transmit signals is a double-edged sword. On one hand, it helps reduce power consumption and simplify design; on the other hand, it poses a serious obstacle to the authorization of legitimate RIS. Almost all the research assumes that the RIS is the authorized one, in other words, the RIS itself is reliable. However, there is currently no widely adopted mechanism to ensure this, and only a few works have explored such a problem so far. For example, in [118], the authors utilized RIS controlled by Eve to attack CSI-based and two-way cross multiplication-based PKG systems, respectively. Hu *et al.* [121] proposed a new RIS-assisted manipulation attack that reduces wireless channel reciprocity by rapidly changing the RIS reflection coefficients and further proposed a path separation-based slewing rate detection method to remove the attacked paths and defend against this attack. Li *et al.* [122] proposed a RIS jamming attack that disrupts channel reciprocity by deploying an adversarial RIS and further designed a countermeasure that exploits wideband signals for multipath separation to distinguish adversarial RIS paths from all separated channel paths to resist RIS jamming attacks. To this end, more work is needed in the future to discover and defend against adversarial RIS attacks. It is worth noting that in addition to the above-mentioned attacks, adversarial RIS is likely to bring other hazards, which are worth extensive research to explore and design corresponding defense solutions, and how to ensure that the used RIS is authenticated, is also an urgent problem to be solved.

3.3 Artificial intelligence

In future wireless communications, AI technology, especially deep learning (DL) methods, will be applied to improve the efficiency and quality of wireless communication in various fields. The NextG networks are expected to have faster data rates, lower transmission delay, and more connected devices. These requirements also present new challenges. First, because of the complexity of NextG communication networks, it is hard to accurately describe networks with mathematical models. Secondly, new performance challenges increase hardware devices' complexity, so new implementation techniques are needed to make the algorithms more suitable for practical applications. AI is considered one of the solutions to improve the performance and robustness of NextG communication networks. The data-driven nature is one of the advantages of AI [123]. AI can learn features from massive data to increase network efficiency and reduce delay. AI's excellent performance will lead the intelligent development trend of NextG communication.

Some preliminary studies have demonstrated that AI and ML have great potential in wireless channel measurement and modeling. AI can leverage clustering, classification, and regression algorithms for channel multipath clustering and channel feature prediction. Wireless channel modeling has begun to apply ML algorithms, for example, convolutional neural networks (CNN). In addition, AI and ML can predict the wireless channel characteristics of unknown scenes, unknown frequency bands, and future moments [1]. AI can also solve problems that may be difficult to model or accurately solve by traditional methods. In recent years, some researchers combine DL with channel coding, channel estimation [124], channel CSI feedback [125], modulation classification [126], *etc.*, and use AI technology to help optimize the physical layer. The direct input deep neural network (DI-DNN) proposed by Gao *et al.* employs signals received by all antennas to estimate the channel [127]. Wen *et al.* [125] designed CSINet using DL technology, which is a novel CSI sensing and recovery mechanism. CSInet can efficiently learn how to use channel structures from the training set. In addition, the current communication systems are characterized by high capacity and high density, and a large amount of data will be generated during wireless transmission, which provides sufficient samples for DL model training.

3.3.1 Challenges of traditional PKG and advantages of AI for PKG

Because of the powerful capabilities of AI in channel estimation, feature extraction, and other aspects, researchers have attempted to apply AI to solve the shortcomings of PKG technology. Specifically, the DL algorithms are used to model and predict channels to extract the information needed for the key. For example, DL algorithm can be used to model the frequency response of a channel and generate a key by predicting CFR. The AI-based PKG scheme is shown in Figure 7. The traditional PKG methods still have limitations in the actual implementation process, and currently, there are many works that use AI to assist PKG to overcome difficulties. The following problems are faced by traditional PKG methods and are expected to be solved through AI combined with PKG.

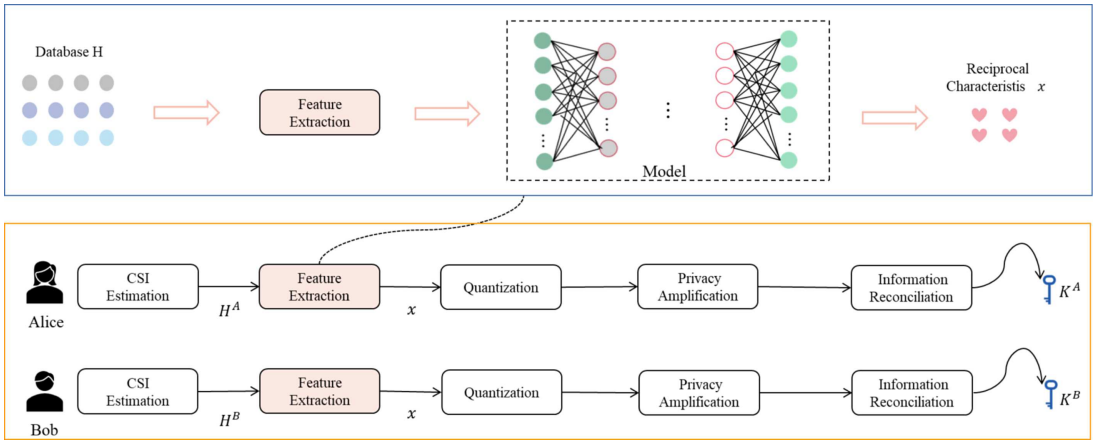


Figure 7. AI-based PKG scheme

- **PKG in TDD systems.** The feasibility of PKG technology mainly depends on the characteristics of the wireless channel, *i.e.*, spatial decorrelation and short-term reciprocity. However, in the TDD system, the reciprocity can be affected by non-simultaneous sampling and noise factors, which may lead to high KDR. Existing PKG approaches capture reciprocity features in the channel by designing some feature extraction methods. Most of the studies employ traditional linear transformation (*e.g.*, PCA [49, 51] and DCT [52, 53] algorithms) to extract reciprocity features, these methods may suffer from limitations like low KGR or high feedback overhead. Some nonlinear feature extraction methods are better than linear transformation [128]. In the channel simulation environment, most of these methods show good performance, but the robustness is poor in the actual environment.
- **PKG in FDD systems.** For FDD systems, the uplink and downlink channels use different carrier frequencies to transmit information. The reciprocity parameters in TDD are completely different in FDD [34]. Therefore, finding reciprocal channel characteristics in FDD systems is challenging. To address this issue, some research has been conducted. Recently, many researchers try to find new frequency-independent reciprocity features (such as angle and delay) based on the uplink and downlink CSIs to generate the key. Nevertheless, accurate acquisition of angles and delays requires significant resource overhead, and there are limitations on the number of antennas that are not suitable for low-power terminals [129]. Some researchers focus on generating keys through path separation. But in complex multipath environments, it is hard to accurately separate paths.
- **Third party threats.** Most current PKG protocols are based on spatial decorrelation, *i.e.*, if the eavesdropper is positioned at a distance exceeding half a wavelength from the legitimate correspondents, it is considered that the eavesdropper is unable to accurately estimate the channel probing between legitimate correspondents. Under this assumption, it will be difficult to obtain the reciprocity characteristics for PKG for the eavesdropper. Nevertheless, certain research shows that in some environments, the spatial correlation of channels still exists between eavesdroppers and legitimate correspondents [130]. Besides, the eavesdropper may be closer to the legitimate party, which can lead to information disclosure.

PKG technology based on AI can improve the performance of PKG and solve the problems faced by traditional PKG technology applications. Firstly, AI technology can enhance the efficiency of PKG protocols. AI-based methods can automatically learn channel characteristics from large amounts of data through ML algorithms, thereby achieving fast and accurate key generation. Secondly, AI technology can improve the security of PKG protocols. For example, AI-based methods can leverage the excellent fitting and discrimination capabilities of DL algorithms to effectively identify and filter out noise and interference. In addition, AI technology can also monitor the key generation process, detect and handle abnormalities in a timely manner, thereby further enhancing the stability and reliability of key generation.

3.3.2 Solution methods: applying AI in PKG

In the past few years, there have been a number of successful studies that use AI technology to address the above-mentioned issues related to traditional PKG schemes. Specifically, we will introduce the relevant AI and PKG combination solutions for the above-mentioned challenges.

- **Reciprocal feature extraction.** Channel reciprocity in actual TDD systems is affected by various environmental factors, limiting the practical application of PKG. It is essential to establish reciprocity features in non-ideal wireless channels. To address this problem, DL technology offers attractive solutions. DL is a powerful feature extraction technology and does not require statistical information of predefined channel models. By applying DL technology to channel estimation, the performance of existing channel estimation technology can be improved, with lower complexity in practical applications [124]. Han *et al.* [131] proposed an efficient PKG scheme based on an autoencoder to extract reciprocity features from weakly correlated channel estimation and obtain better performance results than the PCA-based method. He *et al.* [132] designed a multi-branch autoencoder neural network based on prior knowledge of channel measurement models, called a channel reciprocity learning network (CRLNet). This model uses collected CSI data for training to adaptively learn reciprocity features in weakly correlated channels and can achieve higher KGR.
- **DL assisted PKG in FDD system.** At present, researchers have begun to combine DL with PKG to reduce costs and improve efficiency in FDD systems. Zhang *et al.* [133] employed feature mapping to construct reciprocity features in FDD systems and proposed a key generation neural network (KGNet) for constructing interactive channel features. This method solves the problem of mathematically representing feature mapping between different frequency bands. In [134], two-channel feature mapping methods based on deep transfer learning (DTL) and meta-learning respectively for FDD system key generation were proposed to address the issue of the inapplicability of DL models due to environmental changes. The feature mapping algorithm based on DTL first uses data samples from the original environment to train the network, and then applies a few data from the new environment to fine-tune the trained initial network model. The model can be effective in new environments through this approach. The other feature mapping algorithm based on meta-learning carries out intra-task and cross-task learning across multiple tasks, where each task represents a key generation in a specific scenario. Through this process, the optimal model initialization parameters for generating keys in the new environment can be obtained.
- **Eavesdropping prevention.** The difference between the keys generated by legitimate users and eavesdroppers can be increased by applying neural networks. In [135], a method based on the automatic encoder and neural network domain confrontation (DANN) was proposed to assist in PKG, called automatic encoder domain confrontation training (DAAE). This method can estimate the reciprocal channel characteristics of legitimate communication parties and maximize the difference between the channel features and those of eavesdroppers. The weak correlation channel CSI in the form of amplitude and phase is sent to the neural network for training, and the main components of the reciprocal channel information between legitimate parties are obtained through the DAAE feature extractor. Compared with other PKG methods, it reduces the correlation between legitimate communication parties and eavesdroppers. Compared to PKG using only automatic encoders, it achieves better security.
- **Cooperation with RIS.** RIS is also an emerging technology and has been used to assist PKG research. At the same time, in massive MIMO scenarios, PKG may have serious overhead issues. To address this issue, Liu *et al.* [136] proposed a low-cost RIS-assisted PKG method based on DL. Firstly, the channel CSI is constructed by using RIS. Then, the channel reciprocity features are extracted through the designed neural network (RIS CRNet). This method can extract highly anisotropic channel features without any prior information, and the overhead is small. In [137], ML is used to resolve the high-dimensional non-convex optimization problem of PKG in RIS-assisted multi-antenna systems. They proposed a new algorithm based on the unsupervised deep neural network (DNN) with a simple structure, which uses DNN to obtain the optimal configuration of BS and coding and RIS phase shifts. Simulation results reveal that this method achieves a higher KGR.

3.3.3 Future works

The research on AI-enabled PKG technology is still in the developmental stage. Although some AI-based PKG schemes have been proposed and applied in practical communication systems, these schemes still

face many challenges and limitations. Therefore, in the future, further research is needed to explore more efficient, secure, and reliable AI-enabled PKG technology. The following are some further potential research directions:

- **Reliable common dataset.** DL networks require a large amount of data for parameter training. These data often need to be obtained under specific channel conditions. Therefore, many studies presently rely on mathematically simulated data samples, ignoring the impact of actual environments. The static data obtained from specific channel conditions may conflict with the diversity and temporal variability of the actual wireless channel. In order to obtain more practical research results, the collected actual data should be used for network training and validation. However, obtaining trustworthy channel data in practice is challenging. The actual data sampling environment is complex, and there are many false alarms and misjudgments in the data. In addition, the acquisition and classification of data also pose significant challenges.
- **Generalized scene model.** Currently, the DL models applied to PKG are mostly data-driven, and trained on channel data from a single scene, which limits their application to hypothetical single scenarios. The transformation of the scene may lead to the inapplicability of the DL model. Therefore, exploring a generalized DL model that can be applied to various scenes is a challenging research area. Additionally, the employ of DL models for PKG has some uncertainty due to the instability of the wireless channel environment, resulting in overfitting or underfitting issues. Hence, developing more stable DL models is also a challenging task.
- **Low complexity models.** Some DL models used for PKG may generate high computational complexity, which makes them difficult to apply to small terminals. So far, most DL model frameworks have been designed based on DNN and CNN. Nevertheless, these models can cause high complexity in memory and time, and lead to ultra-high parameters. Therefore, designing better-performance DL models while reducing their complexity is also a challenging research direction [138].

3.4 Space-air-ground integrated network

The space-air-ground integrated network is aimed at integrating space-based, air-based, and ground-based networks, which can make up for their respective shortcomings. The advantages of ground networks are low latency, high data rate, powerful computing ability, *etc.* However, it is difficult to connect ground networks to remote areas, and inefficient for temporary network construction and load balancing. Non-ground networks have wide coverage, and large transmission capacity, and are not limited by the geographical environment, but the communication delay is high. Various components in the space-air-ground integrated network have currently attracted extensive research interest [139]. Below we will introduce three typical networks, *i.e.*, the Internet of Vehicles (IoV), UAV network, and satellite network.

3.4.1 IoV network

The development of the automobile industry and communication technology makes our life more convenient, and the interconnection between automobiles and other network devices has also become a rapidly developing technology, which aims to provide a guarantee for the better operation of the road traffic system. The IoV is a huge network for information exchange between vehicles and other communication devices, which can make traffic management more information-based, improve the quality of vehicle user experience and make vehicle control more intelligent. Figure 8a illustrates different components of communication in IoV, including vehicle-to-vehicle (V2V), vehicle-to-roadside (V2R), vehicle-to-human (V2H), and vehicle-to-infrastructure (V2I) communication.

Whether the security issues of IoV be valued is the key to its further development. In fact, IoV communication is vulnerable to attacks such as eavesdropping, forward, interception, *etc.* The data transmission rate of long-distance vehicle communication is usually very low and the mobility of vehicles is very high. These two problems will reduce channel reciprocity, and some common short-distance wireless communication technologies become unsuitable, which deepens the security risk of IoV communication. In addition, to achieve a high key agreement rate, it is significant to study how to improve the correlation of RSS values between vehicles.

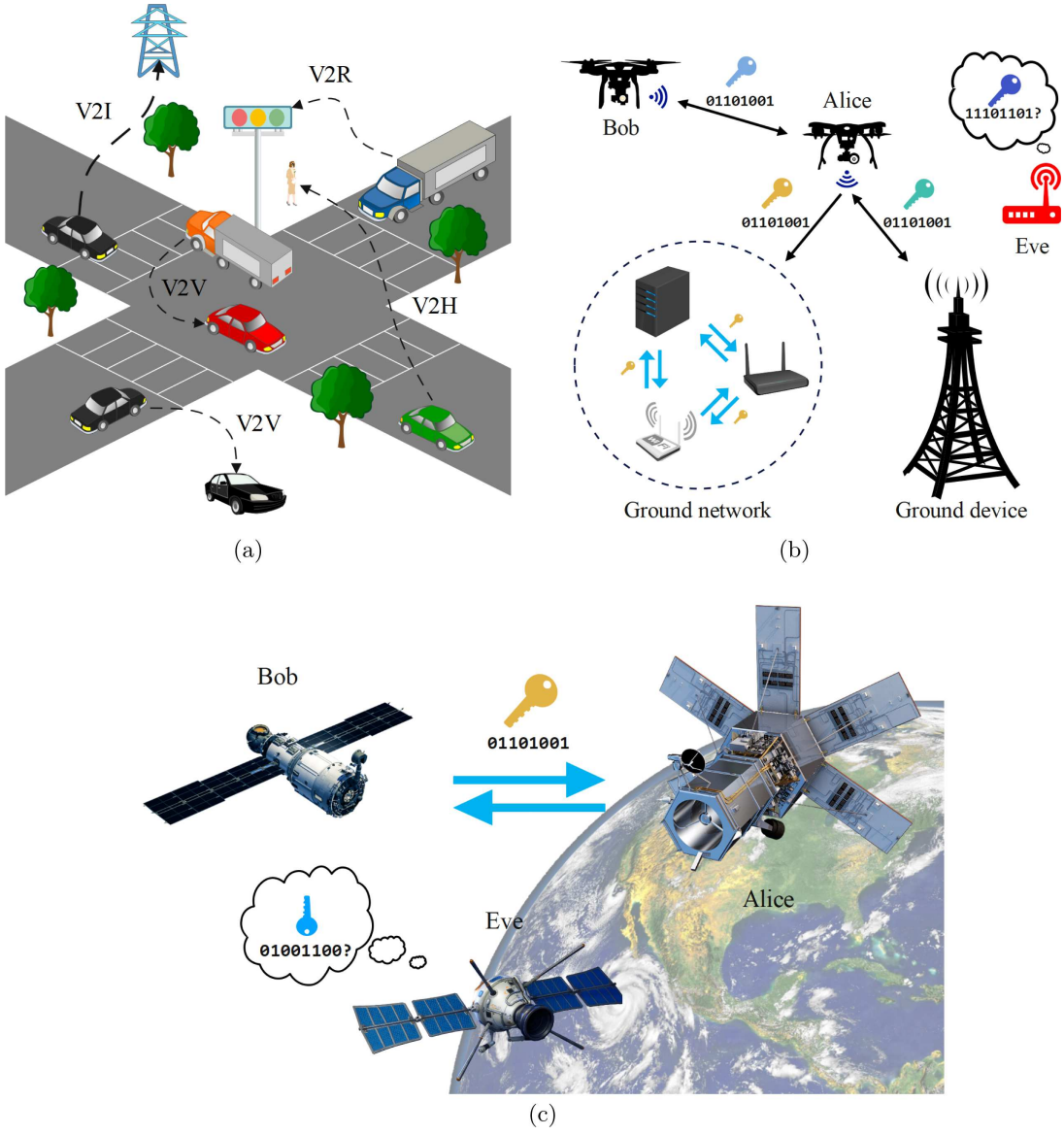


Figure 8. Three typical networks in the space-air-ground integrated network. (a) IoV network. (b) UAV network. (c) Satellite network

Chen *et al.* [140] proposed a PKG scheme that extracts secret keys from RSS in V2R communication. The RSS values are improved by using polynomial interpolation to improve the correlation between the vehicle and roadside unit (RSU). However, when the speed of the vehicle is a little high, the performance of the proposed quantization method is unacceptable, which means an expensive error correction cost. Bottarelli *et al.* [141] proposed a PKG algorithm for V2V communications by introducing a novel channel response quantization method. To solve the non-reciprocity issue of channel responses and improve KGR, the research introduced a quantization optimization block, named as perturb-observe (PO) algorithm. A PKG scheme derived from RSS in the V2V communication was proposed by the authors in [142]. Doppler effect is considered in channel probing as it can influence the channel coherence time. Different from [140], the similarity of RSS values between vehicles is enhanced by using the Kalman filter in [142]. However, the study did not propose a method to improve the KGR. In [143], the authors proposed Vehicle-Key to ensure the security of LoRa-enabled IoV communications. LoRa's long-distance communication decreases channel reciprocity, the study proposed a deep-learning model to address this issue and improve the key agreement rate. In the model, the channel measurement of a communication node can be predicted by

the other one. Moreover, the authors performed four different IoV-based PKG experiments outdoors to evaluate the theoretical results.

3.4.2 UAV network

UAVs have played an important role in air-based network communications in recent years. As small air crafts, UAVs have been crucial in achieving deep network coverage in three-dimensional space, especially in some special scenarios where their flexibility and importance in assisting communications are evident, such as temporary network reconstruction in disaster areas and network resource allocation in crowded areas. Specifically, UAV communication has the following characteristics: (i) *LoS channel dominated*. UAVs typically hover or circle in the air, with few obstacles in the communication link. Since the signal can propagate through the direct link without reflection or scattering, the signal transmission is generally considered to be in LoS environments [144], and the channel condition between the UAV and ground communication device is of high quality. (ii) *High mobility and flexibility*. Due to their controllable three-dimensional maneuverability, UAVs can maintain quasi-static or cruise to a designated location according to the requirements of the system. The motion of UAVs provides a new degree of freedom to provide efficient communication. Additionally, UAVs can adjust their hovering position to maintain communication quality or adjust their deployment position to achieve emergency communication. Moreover, UAV is also very suitable for some temporary communication scenarios. (iii) *Fast and low-cost network construction*. The size of a UAV is usually small, which enables flexible deployment and application in complex and variable environments. A cluster of UAVs can form a communication network in various scenarios. In emergency situations where ground-based communication infrastructure is damaged or non-existent, UAVs can serve as temporary communication infrastructure for disaster relief, remote sensing, firefighting, and other purposes. The deployment of UAVs helps to reduce communication costs and achieve uninterrupted communication.

As small mobile devices, UAVs first use energy to maintain their own flight, resulting in limited energy allocated to communication processes such as signal transmission and reception, signal power amplification, computational expenses, and so on. Moreover, like LoS communication, UAV communication is vulnerable to eavesdropping attacks. Therefore, both the data link and the control link of UAV communication require high levels of confidentiality. Moreover, in terms of PKG, LoS channel results in low randomness, which means low KGR. Figure 8b shows the application of PKG in three different types of UAV communication scenarios.

The following are some examples of research on PKG in UAV communication, which can be mainly divided into three types: UAV air-to-ground communication, UAV air-to-air communication, and UAV-assisted ground communication.

- **PKG in UAV air-to-ground communication.** Lin *et al.* [145] considered UAV MIMO communication and proposed a PKG scheme that can be implemented in FDD systems. In this work, the three-dimension (3D) spatial angle of the UAV is used as a new channel parameter to generate the secret key, which can also combat an active eavesdropping attack called Environment reconstruction based attack for secret keys (ERASE). In the process of PKG, the stage of angle information extraction and angle data processing is added, which is used to make the extracted angle information with uneven distribution follow a near-uniform distribution, thus avoiding a series of repeated bits in the secret key. However, this scheme needs to balance the KGR and the randomness of the key.
- **PKG in UAV air-to-air communication.** In UAV air-to-air communication. Pham *et al.* [146] proposed that the rotation of the UAV antennas be regarded as a randomness source which is reflected by the channel phases. The two-dimensional (2D) case is analyzed first, *i.e.*, the rotation axis l of the antennas is perpendicular to the plane Σ formed by Alice, Bob, and Eve. Then the authors extend it to the 3D case, *i.e.*, l is not perpendicular to Σ. Finally, numerical results of achievable KGR are given under different SNRs, without analyzing their theoretical values and upper bounds on KGR, nor involving specific quantization and information reconciliation stages. Assaf *et al.* [147] combined physically unclonable functions (PUFs) with PKG technology. Specifically, the study addressed the problem of the static channel in UAV communication using PUFs to generate equivalent channel randomness. The randomness was then enhanced with artificial fading (AF), and a new bit extraction scheme was proposed by modifying the adaptive secret bit extraction (ASBE), reducing the number of

transmissions between the nodes and reducing the required number of side-information bits. However, the study only considers UAVs with a single antenna at present. In the future, the study can be extended to multiple UAV scenarios, but the cost of PUF emulators needs to be addressed. Nagubandi *et al.* [148] proposed the relay-assisted selective inversion (RASI) protocol, which uses a ground relay to assist PKG between UAVs. The idea of this protocol stems from the fact that the channel from UAV to ground relay has more randomness than that from UAV to UAV. In this protocol, the two UAVs send pilot signals with a length of 1 successively, assuming that the channel coefficients of UAV A and UAV B to the ground relay are h_{ar} and h_{br}. After receiving the pilot signals, the ground relay sends different broadcast signals based on the relative magnitudes of h_{ar} and h_{br}, and then the two UAVs determine their final form of the received signal according to this broadcast signal respectively. This scheme performs better than another relay-based scheme in the case of low SNR. However, since the UAVs determine the form of their received signal based on the relative magnitudes of h_{ar} and h_{br}, it is possible for there to be a sequence of h_{ar} greater than h_{br}, or *vice versa*. As a result, the randomness of PKG in the proposed RASI protocol may be affected. However, the study did not consider the presence of attackers, an active attacker may interfere with the ground relay to send broadcast signals. In [149], the authors constructed a UAV-assisted relay network outdoors, and implemented RSS-based PKG between UAVs and ground nodes, respectively.

- **PKG in UAV-assisted communication.** Han *et al.* [150] proposed DroneKey, which is a UAV-assisted group-key generation (GKG) scheme for large-scale IoT networks. In the proposed scheme, a UAV flies in a predetermined 3D trajectory and keeps broadcasting wireless signals to ensure that the secret key in the network is updated. Every device in the network receives the signals. To express how the channel between the device and the UAV changes, the CSI stream is extracted. Then the inherent correlation between the CSI streams is obtained by using DL. Finally, the group keys are generated. The scheme considered the situation that the flight trajectory of the UAV is obtained by attackers, and used fuzzy function to address the issue to enhance the security of DroneKey.

3.4.3 Satellite network

With the continuous increase in global communication demand, the limitations of ground communication have gradually become insufficient to meet the rapidly growing needs. Satellite networks can expand the application scope of ground networks and overcome the limitations of current network coverage and spectrum utilization. Specifically, it has a large transmission capacity, the signal transmission cost is independent of the transmission distance, and it is not limited by the geographical environment [151]. As a kind of ultra-long-distance communication, satellite communication can theoretically achieve global coverage with only three satellites. Using the vast coverage range of satellites, the collaboration between satellite and ground networks can connect rural and remote areas that are currently beyond the coverage of existing network infrastructures. In addition, the utilization of the current spectrum is already very high and it is difficult to continue to meet the needs of high-bandwidth applications. Therefore, spectrum sharing between satellite and ground networks enables effective spectrum utilization and provides reliable communication.

Satellite communication often involves important areas at the national level, such as the military, making its security particularly important. Therefore, at the current stage, we are more focused on the security and reliability of satellite communication. In satellite communication, the LoS channel typically dominates, making it difficult to extract sufficient randomness directly from the channel characteristic parameters for high KGR. Moreover, satellite communication, unlike most ground wireless communication, has the characteristic of broadcasting over a large range, making signals easier to be received by unauthorized users. Therefore, satellite communication is more vulnerable to active or passive attacks. Passive attacks mainly involve eavesdropping, where the eavesdropper intercepts the signal transmitted by the satellite and attempts to decipher the information, leading to information leakage. Active attacks include spoofing attacks, jamming attacks, *etc.*, where attackers may disguise themselves as legitimate receivers to obtain secret information or send jamming signals, disrupting satellite communication. These attacks could cause serious damage to communication and result in unpredictable economic losses. So it is important to study how to generate the secret key in satellite communication. Figure 8c shows PKG in satellite communication tersely.

Due to the reason mentioned above, many researchers have done extensive exploration. The authors of [152] proposed a PKG scheme for communication between spacecraft. They utilize the reciprocal Doppler frequency shift measurements between spacecraft as a randomness source to generate the secret key. More specifically, the spacecraft uses measurements of the nominal power spectral density samples (NPSDSs), which preserves the effects of Doppler frequency shift. Firstly, the communication nodes send pilot signals, respectively, then use the maximum likelihood estimation to estimate the NPSDS. Finally, quantize the estimation to generate the secret key. As an extension of [152], the authors model the mobility of the spacecraft in [153]. Specifically, in order to obtain high-security capacity, the authors use a specific Brownian motion model to simulate the random motion component of the spacecraft. The maximum achievable KGR is provided. The method proposed in [154] is also appropriate to be applied to satellite communication. It exploits the reciprocal carrier frequency offset (CFO) between the communication nodes to extract randomness. The communication nodes first exchange binary phase-shift keying (BPSK) signals to estimate the CFO, and then quantize their individual CFO estimations by using equiprobable or uniform quantization. Finally, they reconcile information using linear block codes. Zhang *et al.* [155] proposed the reconciliation efficiency index (CREI) and the adaptive information reconciliation scheme selection (AIRSS) protocol. The CREI is maximized in the protocol to reduce the disagreements caused by channel non-reciprocity in PKG. The simulation results showed the CREI of different protocols in satellite communication scenarios. In [156], the authors reduced the correlation between the legal channel and the wiretap channel by leveraging the advantage of the multi-satellite scheme in space-to-ground satellite PKG.

3.4.4 Future works

The space-air-ground integrated network will be more and more valuable in the future, and the development and application of PKG technology can enhance its security. Next, we will introduce promising directions that lack sufficient research as future works.

- **Adaptive PKG quantization threshold setting in IoV communication.** Because the vehicular communication environment is complex and variable, in the quantization stage of PKG, the fixed threshold currently commonly used may have a great impact on the secret KDR, which will lead to higher expenses in the negotiation stage. Adaptive threshold setting based on DL or other methods can be applied so the threshold can be adjusted adaptively according to the situation, which is helpful to improve the key agreement rate.
- **Make full use of the mobility of UAV.** UAVs have the characteristic of flexible mobility, while most current research assumes that UAVs are in a hovering state. Although this simplifies the system model, it is believed that programming their flight trajectory can significantly improve communication security. Firstly, the dynamic spatial position of UAVs can provide new channel parameters to assist with PKG in static environments. Secondly, due to their non-fixed positions and the ability to optimize flight trajectories for legitimate devices, this can increase the difficulty and cost of eavesdropping attacks. However, UAV mobility also complicates trajectory design and system models. The usual approach is to assume that UAV states are static during each small time slot, but the actual problem is how to appropriately select the length of each time slot to improve system accuracy. Furthermore, it is worth further research on how to combine UAV flight trajectory programming with counteracting eavesdropping attacks and optimizing KGR. Finally, when modeling channels, the LoS and NLoS mixed channel scenario should be considered to fit more practical situations [157].
- **Considering orbital randomness and multi-satellite scheme.** The orbit of a satellite is mainly determined by the gravity of the earth and Newton's laws of mechanics, but strictly speaking, the gravity of the moon, the influence of the atmosphere, and the gravity of the sun are all factors that affect the orbit. Even though the satellite orbit data is open, these factors, which are extremely weak and random, can't be predicted by attackers, so they can be used as random sources to generate secret keys. In addition, multiple satellites will bring more randomness than a single satellite, so more research should be carried out on schemes of PKG through multi-satellite cooperation.
- **Considering the non-reciprocity of legal channels and the correlation of wiretap channels in PKG of satellite communications.** Satellite communication, due to its characteristic of long signal propagation distance and long communication delay, has led to some challenging problems. On

one hand, because of the time-varying environment and the long propagation delay [158], the reciprocal channel is difficult to be established; on the other hand, generally, from the satellite's perspective, the eavesdropper and legitimate user are closely located, and the LoS channel is dominant [159], which leads to that the correlation between legitimate and wiretap channel cannot be ignored. There are not many solutions at present. However, addressing these issues is crucial for advancing the practical implementation of PKG in satellite communications.

3.5 Quantum technology

Quantum information technology (QIT) has become an emerging technology to enable and boost future wireless communication systems from several key perspectives such as computing, communication, security, and intelligence. The future communication technology based on quantum will bring many advantages, including quantum security, improved privacy protection, using secure quantum communication like quantum key distribution to improve the security of future communication, and real-time optimization based on quantum to improve communication efficiency and capacity. QIT is regarded as one of the essential technologies for realizing efficient, safe, and intelligent wireless networks. Quantum computing is mainly applied in unstructured search, optimization, and quantum simulation. Additionally, it can be coupled with other emerging technologies to enhance precision and accelerate processing speeds. Quantum computing utilizes the advantage of quantum parallelism to make the computing speed far higher than the classical computing technology, and ultimately achieve quantum supremacy on some types of problems such as optimization problems [160].

In classical cryptographic schemes, the legitimate communication parties typically rely on the public key cryptosystem (PKC) to complete key distribution. PKC relies on complex mathematical problems used in the encryption algorithm, which makes it impossible for attackers to calculate the private key. They are called computational security. However, the ability of quantum computing poses a serious risk to this encryption scheme [161]. Quantum computers have faster search and factorization capabilities than classical computers. Attackers can use quantum computing to destroy any cryptographic system and algorithm based on integer factoring and discrete logarithm mathematical complexity [162].

3.5.1 QKD technology and application challenges on mobile devices

In order to solve the security issues caused by the development of quantum technology, researchers have been exploring post-quantum cryptography (PQC). PQC aims to find quantum secure cryptographic solutions to resist the attacks of quantum computers and classical computers [160]. PQC develops keys based on mathematical problems, which are hard to solve by quantum computers. However, PQC is not only difficult to study but also a challenging task to integrate into communication systems. In this context, researchers pay much attention to QKD technology. Among all the emerging quantum information technologies, QKD technology is one of the technologies that developed the fastest [163].

QKD is based on a few basic quantum mechanics principles, such as the Heisenberg uncertainty principle and quantum entanglement, to ensure that the increase of computing power cannot and will not affect the security of the key [164]. QKD technology can be implemented with different photon degrees of freedom, such as frequency, phase, polarization, time, and trajectory angular momentum. QKD leverages the authenticated classical channel and the quantum communication channel to solve the problem of exchanging keys between communication parties on the insecure channel [163]. Quantum physics principles can be utilized to monitor eavesdroppers in the process of key generation to prevent them from obtaining keys or messages.

However, when QKD technology is applied to mobile devices, there are still the following challenges and limitations.

- **No suitable security interface.** It is difficult for terminal users to securely access key distribution services in QKD networks in quantum computing environments. Because of the high construction cost of quantum nodes, it is unrealistic for each terminal user to have a dedicated quantum node to access the services of the QKD network. Therefore, several terminal users must share a quantum node in a real-time environment, but this poses security risks.

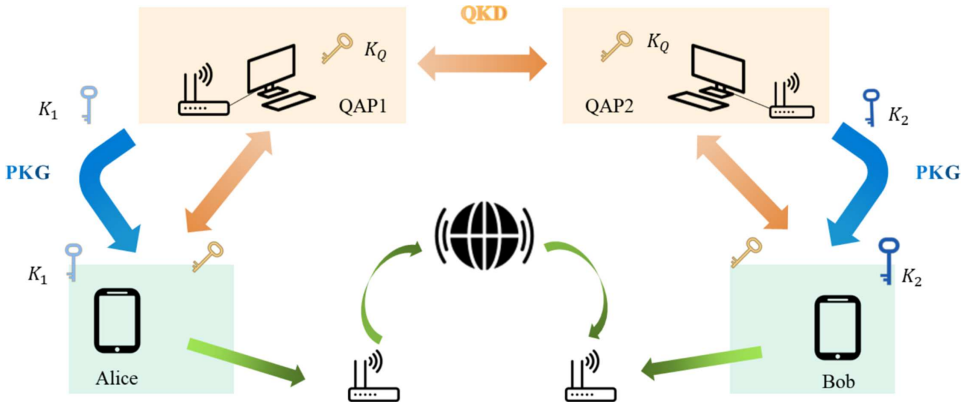


Figure 9. Communication between two remote users using a combination of QKD and PKG

- **Man in the middle attack.** Mobile devices typically rely on software to implement the QKD protocol, and software may have security vulnerabilities, such as a lack of identity authentication and encryption protection mechanisms. These vulnerabilities present opportunities for third parties to exploit. The third party can impersonate a legitimate user and deceive both parties of the legal communication. For example, Eve masquerades as Bob in front of Alice, and masquerades as Alice in front of Bob.
- **Long distance transmission.** The development of QKD research mainly focuses on the use of long-distance optical fiber transmission to ensure the security of large-scale infrastructure [165]. But long-distance quantum communication faces many problems. Fiber loss will limit the transmission distance. With the increase in transmission distance, signal loss and SNR decline will seriously affect KGR. At present, some researchers are studying quantum repeaters to solve this problem. These repeaters rely on the transmission of entangled quantum states between repeater nodes, but it is very hard to build such a system, and the required technology is difficult to achieve in a short time [166]. Satellite links can also be used for long-distance quantum communication, but the cost is too high.

3.5.2 Solution methods combination of QKD and PKG

The physical layer is the first line of defense for communication security. The physical layer employs the unique characteristics of the wireless channel to ensure communication security without assuming the computing ability of the attacker. The correctly implemented PLS scheme should be quantum-safe. PLS has the advantages of absolute security, endogenous integration of communication and security, and independence of complex mathematical operations. In the future communication systems where quantum computing is rapidly developing, PLS technology can effectively cope with the communication security problems caused by quantum computing [167]. The PKG technology uses the wireless channel as the random source of key generation. By reason of the time-varying, uniqueness, and randomness of the wireless channel, CSI changes with time and is difficult to predict. Similar to quantum cryptography, the third party is also hard to measure, reconstruct, and copy, ensuring the security of the key. Moreover, PKG has the same problems as QKD. It is hard to maintain the high reciprocity of signals in long distance transmission, so the conditions for generating the reciprocity key may not be met. A new scheme was proposed to cope with the problem that QKD and PKG are not applicable to remote IoT, *i.e.*, combining the emerging technologies of QKD and PKG to achieve key sharing [168]. PKG can be utilized to accomplish the final stage of secret key distribution from a quantum access point (QAP) to IoT users. Figure 9 illustrates the system model that integrates QKD and PKG. Alice and Bob are two remote wireless users without direct contact. QAP1 and QAP2 are two quantum access nodes with wireless links to Alice and Bob respectively.

In order to achieve secure key distribution between Alice and Bob, first of all, the physical layer key is generated between Alice and QAP1, Bob and QAP2 by employing PKG technology. Next, use QKD technology to distribute quantum keys between QAP1 and QAP2. Then QAP1 and QAP2 employ their physical layer keys to encrypt and pass the quantum keys to Alice and Bob respectively. Thus Alice and Bob have a unified key and can use the key for encrypted communication. In summary, the entire

process is divided into three stages: QKD, PKG, and edge forwarding. The following will elaborate on these stages in detail.

- **QKD phase.** QKD usually includes two stages: the key-sharing stage and the post-processing stage. Firstly, in the key sharing phase, QAP1 transmits a group of random qubits selected from a group of four states with two bases to QAP2 through a quantum channel such as fiber optics. Then QAP2 selects one of the two bases on a random measurement basis. QAP1 and QAP2 keep these bits consistently and discard the remaining ones. Secondly, in the post-processing stage, QAP1 will send some bits to QAP2 to avoid eavesdropping attacks. QAP2 compares the detected content with the content sent by QAP1. These shared bits will be invalid if the error rate is higher than the set threshold. Otherwise, QAP1 and QAP2 implement information coordination to correct errors and privacy amplification to reduce privacy disclosure. The post-processing phase is usually done through an authenticated classical channel. Finally, QAP1 and QAP2 obtain the quantum key K_Q.
- **PKG phase.** PKG protocols mainly include four stages: channel probing, quantization, information reconciliation, and privacy amplification. Alice and QAP1 perform PKG protocol between them to generate channel key K_1. Bob and QAP2 also go through all phases of PKG protocol to perform channel key K_2.
- **Edge forwarding phase.** QAP1 and QAP2 forward the shared quantum keys to Alice and Bob based on the channel keys generated by them respectively to complete the key sharing. With the help of the channel key, the edge can encrypt the quantum key using the One-TimePad (OTP) encryption algorithm. Then the edge forwards the cipher text to the user.

Li *et al.* [168] also show how to extend the method to multi-user scenarios by optimizing and designing edge-forwarding strategies. In addition, in order to improve practicality, some methods were proposed to reduce time delays and improve key generation rates.

3.5.3 Future works

Although combining QKD and PKG can enhance communication security, this technology still faces many challenges in future communication. Moreover, research in this area is relatively scarce at present. The following are some open issues that we believe need to be addressed urgently:

- **Device authentication.** Considering the hybrid architecture of QKD and PKG, both QKD and PKG cannot authenticate the transmission source, making them very vulnerable to spoofing attacks. Identity authentication can be further enhanced through emerging PLS technologies, such as radio frequency fingerprint technology [169].
- **Untrusted intermediate QAP.** The combination system of PKG and QKD relies on the trust of the intermediate QAP. When QAP is not trusted, how to implement the solution is also a good research direction. In this case, it may be beneficial to use multiple QAPs so that they can verify and monitor each other's behavior. Additionally, other security mechanisms can be explored to ensure the security of the system. Ultimately, further research and development of alternative solutions are needed to ensure system security in situations where QAPs cannot be trusted.
- **Security risks of hybrid architecture.** The security of existing PKG schemes mainly depends on changes in the environment. When the environment changes slowly, PKG schemes may encounter security vulnerabilities. The current research on addressing PKG in slowly changing channels is challenging [170].
- **Extension to Point to Multipoint (P2M) mechanisms.** Existing QKD services can only support point-to-point (P2P) key distribution, which means that a separate key distribution channel needs to be established for each node when establishing QKD communication. The system becomes more complex and costly as a result. As a consequence, the practical application of the P2M mechanism in QKD networks still needs further research and development.

4 Conclusion

In this survey, we reviewed recent trends in utilizing the advantages of PKG to enhance network security by implementing secure key generation through wireless channel properties such as spatial decorrelation,

time variation, and channel reciprocity. At the same time, new technologies that are expected to be widely applied in the NextG networks will also be in favor of the application of PKG in the NextG networks. We first analyzed the challenges faced by traditional key generation schemes in NextG network scenarios, analyzed the possibility of PKG overcoming corresponding difficulties, and emphasized the differences between previous investigations and our work. Then, the preliminary knowledge of PKG was summarized, including its development history, principles, protocols, channel parameters, and evaluation metrics, to help target readers have a more comprehensive understanding of PKG. Finally, we conducted an in-depth analysis of the five new technologies widely adopted in the NextG networks and provided a detailed explanation of the background, advantages and disadvantages, challenges, solutions, and open issues that still need to be addressed when combining each technology with PKG.

Conflict of Interest

The author declares no conflict of interest.

Data Availability

No data are associated with this article.

Authors' Contributions

Qingjiang Xiao mainly investigated the research progress of PKG in the previous network and participated in writing the abstract, Sections 1, 2, and the conclusion of the manuscript. Jinrong Zhao mainly discusses the application of PKG in NextG network scenarios such as massive MIMO, AI, and quantum technology, and participates in the writing of Section 3. Feng Sheng mainly studied the application of PKG in RIS and space-air-ground integrated networks and participated in the writing of Section 3 of the manuscript. Guyue Li and Aiqun Hu were responsible for the framework design and writing guidance of the survey. All authors read and approved the final manuscript.

Acknowledgements

We thank the anonymous reviewers for their helpful comments.

Funding

This work was supported in part by the National Key R&D Program of China under Grant 2022YFB2902202, in part by the National Natural Science Foundation of China (No. U22A2001, No. 62171121), in part by the Natural Science Foundation of Jiangsu Province under Grant BK20211160.

References

[1] You X, Wang C-X, Huang J and Gao X et al. Towards 6G wireless communication networks: vision, enabling technologies, and new paradigm shifts. Sci Chin Inf Sci 2021; **64**: 1–74.
[2] Sevincer A, Bhattarai A and Bilgi M et al. LIGHTNETs: smart LIGHTing and mobile optical wireless NETworks – a survey. IEEE Commun Surv Tutorials 2013; **15**: 1620–41.
[3] Memedi A and Dressler F. Vehicular visible light communications: a survey. IEEE Commun Surv Tutorials 2021; **23**: 161–81.
[4] Jiang L, Luo C and Li X et al. RIS-assisted downlink multi-cell communication using statistical CSI. In: 2022 International Symposium on Wireless Communication Systems (ISWCS). IEEE, 2022, 1–6.
[5] Matthaiou M, Yurduseven O and Ngo HQ et al. The road to 6G: ten physical layer challenges for communications engineers. IEEE Commun Mag 2021; **59**: 64–9.
[6] Zhang J, Björnson E and Matthaiou M, et al. Prospective multiple antenna technologies for beyond 5G. IEEE J Sel Areas Commun 2020; **38**: 1637–60.
[7] Ding Z, Lv L and Fang F et al. A state-of-the-art survey on reconfigurable intelligent surface-assisted non-orthogonal multiple access networks. Proc IEEE 2002; **110**: 1358–79.
[8] Wu Q and Zhang R. Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming. IEEE Trans Wireless Commun 2019; **18**: 5394–409.
[9] Wu Q and Zhang R. Beamforming optimization for wireless network aided by intelligent reflecting surface with discrete phase shifts. IEEE Trans Commun 2020; **68**: 1838–51.
[10] Zainud-Deen SH. Reconfigurable intelligent surfaces for wireless communications. In: 2022 39th National Radio Science Conference (NRSC). Vol 1. IEEE, 2022, 342.
[11] Pan C, Ren H and Wang K et al. Reconfigurable intelligent surfaces for 6G systems: principles, applications, and research directions. IEEE Commun Mag 2021; **59**: 14–20.
[12] Zou Y, Zhu J and Wang X et al. A survey on wireless security: technical challenges, recent advances, and future trends. Proc IEEE 2016; **104**: 1727–65.
[13] Han Y, Duan L and Zhang R. Jamming-assisted eavesdropping over parallel fading channels. IEEE Trans Inf Forensics Secur 2019; **14**: 2486–99.
[14] Xu Y, Liu M and Peng L et al. Colluding RF fingerprint impersonation attack based on generative adversarial network. In: ICC 2022 – IEEE International Conference on Communications. IEEE, 2022, 3220–5.

[15] Kim D and An S. PKC-based DoS attacks-resistant scheme in wireless sensor networks. IEEE Sensors J 2016; **16**: 2217–8.
[16] Ohigashi T and Morii M. A practical message falsification attack on WPA. Proc JWIS 2009; **54**: 66.
[17] Zhang J, Rajendran S and Sun Z et al. Physical layer security for the internet of things: authentication and key generation. IEEE Wireless Commun 2019; **26**: 92–8.
[18] Mukherjee A, Ali S and Fakoorian A et al. Principles of physical layer security in multiuser wireless networks: a survey. IEEE Commun Surv Tutorials 2014; **16**: 1550–73.
[19] Stamp M. Information Security: Principles and Practice. New York; John Wiley & Sons, 2011.
[20] Whitman ME and Mattord HJ. Principles of Information Security. Boston, MA: Cengage Learning, 2021.
[21] Jorswieck E, Tomasin S and Sezgin A. Broadcasting into the uncertainty: authentication and confidentiality by physical-layer processing. Proc IEEE 2015; **103**: 1702–24.
[22] Zhang J, Duong TQ and Marshall A et al. Key generation from wireless channels: a review. IEEE Access 2016; **4**: 614–26.
[23] Cheng C, Lu R and Petzoldt A et al. Securing the internet of things in a quantum world. IEEE Commun Mag 2017; **55**: 116–120.
[24] Suhail S, Hussain R and Khan A. On the role of hash-based signatures in quantum-safe internet of things: current solutions and future directions. IEEE Internet Things J 2021; **8**: 1–17.
[25] Li G, Sun C and Jorswieck EA et al. Sum secret key rate maximization for TDD multi-user massive MIMO wireless networks. IEEE Trans Inf Forensics Secur 2021; **16**: 968–82.
[26] Xie N, Zhang JH and Zhang QH. Security provided by the physical layer in wireless communications. In: IEEE Network. IEEE, 2022, 1–7.
[27] Wang Y, Miao Z and Jiao L. Safeguarding the ultra-dense networks with the aid of physical layer security: a review and a case study. IEEE Access 2016; **4**: 9082–92.
[28] Wu Y, Yu Y and Hu Y et al. Channel-based dynamic key generation for physical layer security in OFDM-PON systems. IEEE Photonics J 2021; **13**: 1–9.
[29] Yuliana M, Wirawan and Suwadi. Performance evaluation of the key extraction schemes in wireless indoor environment. In: 2017 International Conference on Signals and Systems (ICSigSys). IEEE, 2017, 138–44.
[30] Cao G, Zhang Y and Ji Z. ESP32-driven physical layer key generation: a low-cost, integrated, and portable implementation. In: 2022 IEEE 96th Vehicular Technology Conference (VTC2022-Fall). IEEE, 2022, 1–5.
[31] Chen C, Zhe Y and Siyu Y et al. Research on key distribution and encryption control system of optical network physical layer. In: 2021 World Conference on Computing and Communication Technologies (WCCCT). IEEE, 2021, 1–5.
[32] Wang T, Liu Y and Vasilakos AV. Survey on channel reciprocity based key establishment techniques for wireless systems. Wireless Networks 2015; **21**: 1835–46.
[33] Zhang J, Li G and Marshall A et al. A new frontier for IoT security emerging from three decades of key generation relying on wireless channels. IEEE Access 2020; **8**: 138406–46.
[34] Li G, Sun C and Zhang J et al. Physical layer key generation in 5G and beyond wireless communications: challenges and opportunities. Entropy 2019; **21**: 497.
[35] Porambage P, Gür G and Moya Osorio DP et al. 6G security challenges and potential solutions. In: 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit). IEEE, 2021, 622–7.
[36] Mucchi L, Jayousi S and Caputo S et al. Physical-layer security in 6G networks. IEEE Open J Commun Soc 2021; **2**: 1901–14.
[37] Nguyen V-L, Lin P-C and Cheng B-C et al. Security and privacy for 6G: a survey on prospective technologies and challenges. IEEE Commun Surv Tutorials 2021; **23**: 2384–2428.
[38] Shannon CE. Communication theory of secrecy systems. Bell Syst Tech J 1949; **28**: 656–715.
[39] Wyner AD. The wire-tap channel. Bell Sys Tech J 1975; **54**: 1355–87.
[40] Maurer UM. Secret key agreement by public discussion from common information. IEEE Trans Inf Theory 1993; **39**: 733–42.
[41] Hershey JE, Hassan AA and Yarlagadda R. Unconventional cryptographic keying variable management. IEEE Trans Commun 1995; **43**: 3–6.
[42] Zhang J, Ding M and López-Pérez D et al. Design of an efficient OFDMA-based multi-user key generation protocol. IEEE Trans Veh Technol 2019; **68**: 8842–52.
[43] Sun C and Li G. Power allocation and beam scheduling for multi-user massive MIMO secret key generation. IEEE Access, 8:164580–164592, 2020.
[44] Hu L, Chen Y and Li G et al. Exploiting artificial randomness for fast secret key generation in quasi-static environments. In: 2021 IEEE 6th International Conference on Signal and Image Processing (ICSIP). IEEE, 2021, 985–9.
[45] Renna F, Bloch MR and Laurenti N. Semi-blind key-agreement over MIMO fading channels. IEEE Trans Commun 2013; **61**: 620–7.
[46] Ren K, Su H and Wang Q. Secret key generation exploiting channel characteristics in wireless communications. IEEE Wireless Commun 2011; **18**: 6–12.
[47] Cheng W, Xu A and Jiang Y et al. The realization of key extraction based on USRP and OFDM channel response. In: 2017 IEEE Conference on Communications and Network Security (CNS). IEEE, 2017, 374–5.
[48] Mathur S, Trappe W and Mandayam N et al. Radio-Telepathy: extracting a secret key from an unauthenticated wireless channel. In: Proceedings of the 14th ACM International Conference on Mobile Computing and Networking, MobiCom '08. New York, NY, USA: Association for Computing Machinery, 2008, 128–39.
[49] Li G, Hu A and Zhang J et al. High-agreement uncorrelated secret key generation based on principal component analysis preprocessing. IEEE Trans Commun 2018; **66**: 3022–34.

[50] Zhang J, Marshall A and Woods R et al. Efficient key generation by exploiting randomness from channel responses of individual OFDM subcarriers. IEEE Trans Commun 2016; **64**: 2578–88.
[51] Li G, Hu A and Peng L et al. The optimal preprocessing approach for secret key generation from OFDM channel measurements. In: 2016 IEEE Globecom Workshops (GC Wkshps). IEEE, 2016, 1–6.
[52] Margelis G, Fafoutis X and Oikonomou G et al. Physical layer secret-key generation with discreet cosine transform for the internet of things. In: 2017 IEEE International Conference on Communications (ICC). IEEE, 2017, 1–6.
[53] Goel A and Vishwakarma VP. Efficient feature extraction using DCT for gender classification. In: 2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT). IEEE, 2016, 1925–28.
[54] Liu H, Wang Y and Yang J et al. Fast and practical secret key extraction by exploiting channel response. In: 2013 Proceedings IEEE INFOCOM. IEEE, 2013, 3048–56.
[55] Guo D, Cao K and Xiong J et al. A lightweight key generation scheme for the internet of things. IEEE Internet Things J 2021; **8**: 12137–49.
[56] Zhang J, Woods R and Marshall A et al. An effective key generation system using improved channel reciprocity. In: 2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, 2015, 1727–31.
[57] Ali ST, Sivaraman V and Ostry D. Eliminating reconciliation cost in secret key generation for body-worn health monitoring devices. IEEE Trans Mob Comput 2014; **13**: 2763–76.
[58] Zhu X, Xu F and Novak E et al. Extracting secret key from wireless link dynamics in vehicular environments. In: 2013 Proceedings IEEE INFOCOM. IEEE, 2013, 2283–91.
[59] Premnath SN, Jana S and Croft J et al. Secret key extraction from wireless signal strength in real environments. IEEE Trans Mob Comput 2013; **12**: 917–30.
[60] Jana S, Premnath SN and Clark M et al. On the effectiveness of secret key extraction from wireless signal strength in real environments. In: Proceedings of the 15th Annual International Conference on Mobile Computing and Networking. ACM, 2009, 321–332.
[61] Wu Y, Xia H and Cheng C. Improved mult-bit adaptive quantization algorithm for physical layer security based on channel charscteristics. In: 2018 5th International Conference on Systems and Informatics (ICSAI). IEEE, 2018, 807–11.
[62] Patwari N, Croft J and Jana S et al. High-rate uncorrelated bit extraction for shared secret key generation from channel measurements. IEEE Trans Mob Comput 2010; **9**: 17–30.
[63] Brassard G and Salvail L. Secret-key reconciliation by public discussion. In: Advances in Cryptology – EUROCRYPT'93: Workshop on the Theory and Application of Cryptographic Techniques Lofthus, Norway, May 23–27, 1993 Proceedings 12. Springer, 1994, 410–423.
[64] Liu Y, Draper SC and Sayeed AM. Exploiting channel diversity in secret key generation from multipath fading randomness. IEEE Trans Inf Forensics Secur 2012; **7**: 1484–97.
[65] Epiphaniou G, Karadimas P and Ismail DKB et al. Nonreciprocity compensation combined with turbo codes for secret key generation in vehicular Ad Hoc social IoT networks. IEEE Internet Things J 2018; **5**: 2496–2505.
[66] Hentilä H, Shkel YY and Koivunen V. Secret key generation over wireless channels using short blocklength multilevel source Polar coding. In: ICASSP 2021 – 2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, 2021, 2615–19.
[67] Zhu X, Xu F and Novak E et al. Extracting secret key from wireless link dynamics in vehicular environments. In: 2013 Proceedings IEEE INFOCOM. IEEE, 2013, 2283–91.
[68] Wei Y, Zeng K and Mohapatra P. Adaptive wireless channel probing for shared key generation based on PID controller. IEEE Trans Mob Comput 2012; **12**: 1842–52.
[69] Wang Q, Su H and Ren K et al. Fast and scalable secret key generation exploiting channel phase randomness in wireless networks. In: 2011 Proceedings IEEE INFOCOM. IEEE, 2011, 1422–30.
[70] Maurer U and Wolf S. Secret-key agreement over unauthenticated public channels. II. Privacy amplification. IEEE Trans Inf Theory 2003; **49**: 839–51.
[71] Wegman MN and Carter JL. New hash functions and their use in authentication and set equality. J Comput Syst Sci 1981; **22**: 265–79.
[72] Bennett CH, Brassard G and Crépeau C et al. Generalized privacy amplification. IEEE Trans Inf Theory 1995; **41**: 1915–23.
[73] Zhang J, Kasera SK and Patwari N. Mobility assisted secret key generation using wireless link signatures. In: 2010 Proceedings IEEE INFOCOM. IEEE, 2010, 1–5.
[74] Ambekar A, Hassan M and Schotten HD. Improving channel reciprocity for effective key management systems. In: 2012 International Symposium on Signals, Systems, and Electronics (ISSSE). IEEE, 2012, 1–4.
[75] Guillaume R, Winzer F and Czylwik A et al. Bringing PHY-based key generation into the field: an evaluation for practical scenarios. In: 2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall). IEEE, 2015, 1–5.
[76] Zeng K, Wu D and Chan A et al. Exploiting multiple-antenna diversity for shared secret key generation in wireless networks. In: 2010 Proceedings IEEE INFOCOM. IEEE, 2010, 1–9.
[77] Guillaume R, Winzer F and Czylwik A et al. Bringing PHY-based key generation into the field: an evaluation for practical scenarios. In: 2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall). IEEE, 2015, 1–5.
[78] Sudarsono A and Yuliana M. An anonymous authentication with received signal strength based pseudonymous identities generation for VANETs. IEEE Access 2023; **11**: 15637–54.
[79] Van der Elst V, Wilssens R and Jocqué J et al. Platform for multi-user channel-based encryption of speech communication with AES on 2.45 GHz. In: 2022 16th European Conference on Antennas and Propagation (EuCAP). IEEE, 2022, 1–5.
[80] Liu H, Yang J and Wang Y et al. Group secret key generation via received signal strength: protocols, achievable rates, and implementation. IEEE Trans Mob Comput 2014; **13**: 2820–35.

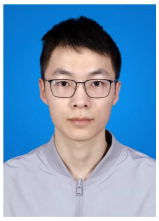
[81] Liu H, Yang J and Wang Y et al. Collaborative secret key extraction leveraging received signal strength in mobile wireless networks. In: 2012 Proceedings IEEE Infocom. IEEE, 2012, 927–35.
[82] Lu X, Lei J and Shi Y et al. Applying intelligent reflective surface to channel phase probing in wireless secret key generation, 2022, doi: 10.21203/rs.3.rs-1468291/v1.
[83] Cheng L, Zhou L and Seet B-C et al. Efficient physical-layer secret key generation and authentication schemes based on wireless channel-phase. Mob Inf Syst 2017; **2017**: 7393526.
[84] Shehadeh YEH, Alfandi O and Hogrefe D. Towards robust key extraction from multipath wireless channels. J Commun Networks 2012; **14**: 385–95.
[85] Linh DV and Yem VV. Key generation technique based on channel characteristics for MIMO-OFDM wireless communication systems. IEEE Access 2023; **11**: 7309–19.
[86] Zhang J, Marshall A and Woods R et al. Secure key generation from OFDM subcarriers' channel responses. In: 2014 IEEE Globecom Workshops (GC Wkshps). IEEE, 2014, 1302–7.
[87] Liu H, Wang Y and Liu J et al. Authenticating users through fine-grained channel information. IEEE Trans Mob Comput 2017; **17**: 251–64.
[88] Wu C-Y, Lan P-C and Yeh P-C et al. Practical physical layer security schemes for MIMO-OFDM systems using precoding matrix indices. IEEE J Sel Areas Commun 2013; **31**: 1687–1700.
[89] Taha H and Alsusa E. Secret key exchange using private random precoding in MIMO FDD and TDD systems. IEEE Trans Veh Technol 2017; **66**: 4823–33.
[90] Jiao L, Tang J and Zeng K. Physical layer key generation using virtual AoA and AoD of mmWave massive MIMO channel. In: 2018 IEEE Conference on Communications and Network Security (CNS). IEEE, 2018, 1–9.
[91] Badawy A, Elfouly T and Khattab T et al. Robust secret key extraction from channel secondary random process. Wireless Commun Mob Comput 2016; **16**: 1389–1400.
[92] Borges D, Montezuma P and Dinis R et al. Massive MIMO techniques for 5G and beyond – opportunities and challenges. Electronics 2021; **10**: 1667.
[93] Akyildiz IF and Jornet JM. Realizing ultra-massive MIMO (1024×1024) communication in the (0.06–10) terahertz band. Nano Commun Networks 2016; **8**: 46–54.
[94] Lu AA and Gao XQ. Prospects and overview of massive MIMO transmission. Bull Natl Nat Sci Found Chin 2020; **34**: 186–92.
[95] Zhang J, Duong TQ and Woods R et al. Securing wireless communications of the internet of things from the physical layer, an overview. Entropy 2017; **19**: 420.
[96] Zeng K. Physical layer key generation in wireless networks: challenges and opportunities. IEEE Commun Mag 2015; **53**: 33–9.
[97] Li G, Sun C and Jorswieck EA et al. Sum secret key rate maximization for TDD multi-user massive MIMO wireless networks. IEEE Trans Inf Forensics Secur 2020; **16**: 968–82.
[98] Chen Y, Li G and Sun C et al. Beam-domain secret key generation for multi-user massive MIMO networks. In: ICC 2020-2020 IEEE International Conference on Communications (ICC). IEEE, 2020, 1–6.
[99] Li G, Xu Y and Xu W et al. Robust key generation with hardware mismatch for secure MIMO communications. IEEE Trans Inf Forensics Secur 2021; **16**: 5264–78.
[100] Im S, Jeon H and Choi J et al. Robustness of secret key agreement protocol with massive MIMO under pilot contamination attack. In: 2013 International Conference on ICT Convergence (ICTC). IEEE, 2013, 1053–8.
[101] Zhou T, Xu K and Xia X et al. Achievable rate maximization for aerial intelligent reflecting surface-aided cell-free massive MIMO system. In: 2020 IEEE 6th International Conference on Computer and Communications (ICCC). IEEE, 2020, 623–8.
[102] Dang J, Zhang Z and Wu L. Joint beamforming for intelligent reflecting surface aided wireless communication using statistical CSI. Chin Commun 2020; **17**: 147–57.
[103] Elganimi TY, Elmajdub RI and Nauryzbayev G et al. IRS-assisted beamspace millimeter-wave massive MIMO with interference-aware beam selection. In: 2022 IEEE 96th Vehicular Technology Conference (VTC2022-Fall). IEEE, 2022, 1–6.
[104] Lu C, Fang Y and Qiu L. Energy-efficient beamforming design for cooperative double-IRS aided multi-user MIMO. In: GLOBECOM 2022 – 2022 IEEE Global Communications Conference. IEEE, 2022, 4619–24.
[105] You L, Xiong J and Ng DWK et al. Energy efficiency and spectral efficiency tradeoff in RIS-aided multiuser MIMO uplink transmission. IEEE Trans Signal Process 2021; **69**: 1407–21.
[106] Qiao J and Alouini M-S. Secure transmission for intelligent reflecting surface-assisted mmWave and terahertz systems. IEEE Wireless Commun Lett **9** (2020) 1743–1747.
[107] Hu X, Jin L and Huang K et al. Intelligent reflecting surface-assisted secret key generation with discrete phase shifts in static environment. IEEE Wireless Commun Lett 2021; **10**: 1867–70.
[108] Lu T, Chen L and Zhang J et al. Reconfigurable intelligent surface assisted secret key generation in quasi-static environments. IEEE Commun Lett 2022; **26**: 244–8.
[109] Lu X, Lei J and Shi Y et al. Applying intelligent reflective surface to channel phase probing in wireless secret key generation. 2022, doi: 10.21203/rs.3.rs-1468291/v1.
[110] Staat P, Elders-Boll H and Heinrichs M et al. Intelligent reflecting surface-assisted wireless key generation for low-entropy environments. In: 2021 IEEE 32nd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC). IEEE, 2021, 745–51.
[111] Li G, Hu L and Staat P et al. Reconfigurable intelligent surface for physical layer key generation: constructive or destructive? IEEE Wireless Commun 2022; **29**: 146–53.
[112] Ji Z, Yeoh PL and Zhang D et al. Secret key generation for intelligent reflecting surface assisted wireless communication networks. IEEE Trans Veh Technol 2021; **70**: 1030–4.

[113] Liu Y, Huang K and Yang S et al. Secret key generation for intelligent reflecting surface assisted wireless communication networks with multiple eavesdroppers. In: 2021 International Conference on Advanced Computing and Endogenous Security. IEEE, 2022, 1–6.
[114] Li G, Sun C and Xu W et al. On maximizing the sum secret key rate for reconfigurable intelligent surface-assisted multiuser systems. IEEE Trans Inf Forensics Secur 2022; **17**: 211–25.
[115] Wei Z, Wang L and Guo W. Secret key rate upper-bound for reconfigurable intelligent surface-combined system under spoofing. In: 2022 IEEE 96th Vehicular Technology Conference (VTC2022-Fall). IEEE, 2022, 1–6.
[116] Wei Z and Guo W. Random matrix based physical layer secret key generation in static channels. Preprint: arXiv:2110.12785, 2021.
[117] Wei Z, Guo W and Li B. A multi-eavesdropper scheme against RIS secured LoS-dominated channel. IEEE Commun Lett 2022; **26**: 1221–5.
[118] Wei Z, Li B and Guo W. Adversarial reconfigurable intelligent surface against physical layer key generation. IEEE Trans Inf Forensics Secur 2023; **18**: 2368–81.
[119] Bakşi S and Popescu DC. Secret key generation with precoding and role reversal in MIMO wireless systems. IEEE Trans Wireless Commun 2019; **18**: 3104–3112.
[120] Manjappa NC, Wimmer L and Maletic N et al. Enhanced physical layer secure key generation using mm Wave beamforming. In: 2022 International Symposium on Wireless Communication Systems (ISWCS). IEEE, 2022, 1–6.
[121] Hu L, Li G and Luo H et al. On the RIS manipulating attack and its countermeasures in physical-layer key generation. In: 2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall). IEEE, 2021, 1–5.
[122] Li G, Staat P and Li H et al. RIS-Jamming: breaking key consistency in channel reciprocity-based key generation. Preprint: arXiv:2303.07015, 2023.
[123] Wang T, Wang S and Zhou Z-H. Machine learning for 5G and beyond: from model-based to data-driven mobile wireless networks. China Commun **16** (2019) 165–175.
[124] Yang Y, Gao F and Ma X et al. Deep learning-based channel estimation for doubly selective fading channels. IEEE Access 2019; **7**: 36579–89.
[125] Wen C-K, Shih W-T and Jin S. Deep learning for massive MIMO CSI feedback. IEEE Wireless Commun Lett 2018; **7**: 748–51.
[126] Lin Y, Tu Y and Dou Z. An improved neural network pruning technology for automatic modulation classification in edge devices. IEEE Trans Veh Technol 2020; **69**: 5703–6.
[127] Gao S, Dong P and Pan Z. Deep learning based channel estimation for massive MIMO with mixed-resolution ADCs. IEEE Commun Lett 2019; **23**: 1989–93.
[128] Wu X, Peng Y and Hu C et al. A secret key generation method based on CSI in OFDM-FDD system. In: 2013 IEEE Globecom Workshops (GC Wkshps). IEEE, 2013, 1297–302.
[129] Wan Z, Huang K and Chen L. Secret key generation scheme based on deep learning in FDD MIMO systems. IEICE Trans Inf Syst 2021; **104**: 1058–62.
[130] He X, Dai H and Huang Y et al. The security of link signature: a view from channel models. In: 2014 IEEE Conference on Communications and Network Security. IEEE (2014) 103–8.
[131] Han J, Zeng X and Xue X et al. Physical layer secret key generation based on autoencoder for weakly correlated channels. In: 2020 IEEE/CIC International Conference on Communications in China (ICCC). IEEE, 2020, 1220–5.
[132] He H, Chen Y and Huang X et al. Deep learning-based channel reciprocity learning for physical layer secret key generation. Secur Commun Networks 2022; **2022**: 1844345.
[133] Zhang X, Li G and Zhang J et al. Deep-learning-based physical-layer secret key generation for FDD systems. IEEE Internet Things J 2021; **9**: 6081–94.
[134] Zhang X, Li G and Zhang J et al. Enabling deep learning-based physical-layer secret key generation for FDD-OFDM systems in multi-environments. Preprint: arXiv:2211.03065, 2022.
[135] Zhou J and Zeng X. Physical-layer secret key generation based on domain-adversarial training of autoencoder for spatial correlated channels. Appl Intell 2023; **53**: 1–16.
[136] Liu S, Wei G and He H et al. Intelligent reflecting surface-assisted physical layer key generation with deep learning in MIMO systems. Sensors 2022; **23**: 55.
[137] Chen C, Zhang J and Lu T et al. Machine learning-based secret key generation for IRS-assisted multi-antenna systems. Preprint: arXiv:2301.08179, 2023.
[138] Huang H, Guo S and Gui G et al. Deep learning for physical-layer 5G wireless techniques: opportunities, challenges and solutions. IEEE Wireless Commun 2019; **27**: 214–22.
[139] Qu H, Xu X and Zhao J et al. An SDN-based space-air-ground integrated network architecture and controller deployment strategy. In: 2020 IEEE 3rd International Conference on Computer and Communication Engineering Technology (CCET). IEEE, 2020, 138–42.
[140] Sudarsono A, Yuliana M and Kristalina P. A shared secret key generation between vehicle and roadside based preprocessing method. In: 2019 International Conference on Computer Engineering, Network, and Intelligent Multimedia (CENIM). IEEE, 2019, 1–8.
[141] Bottarelli M, Karadimas P and Epiphaniou G et al. Adaptive and optimum secret key establishment for secure vehicular communications. IEEE Trans Veh Technol 2021; **70**: 2310–21.
[142] Sudarsono A and Yuliana M. An implementation of secure vehicle-to-vehicle communication using shared key generation with Kano method. In: 2021 International Electronics Symposium (IES). IEEE, 2021, 67–72.
[143] Yang H, Liu H and Luo C et al. Vehicle-Key: a secret key establishment scheme for LoRa-enabled IOV communications. In: 2022 IEEE 42nd International Conference on Distributed Computing Systems (ICDCS). IEEE, 2022, 787–97.
[144] Watanabe T and Nishimori K. Evaluation of channel capacity characteristics for asymmetric LoS-MIMO. In: 2021 International Symposium on Antennas and Propagation (ISAP). IEEE, 2021, 1–2.

[145] Lin K, Ji Z and Zhang Y et al. Secret key generation based on 3D spatial angles for UAV communications. In: 2021 IEEE Wireless Commun and Networking Conference (WCNC). IEEE, 2021, 1–6.
[146] Pham TM, Barreto AN and Mitev M et al. Secure communications in line-of-sight scenarios by rotation-based secret key generation. In: 2022 IEEE International Conference on Communications Workshops (ICC Workshops). IEEE, 2022, 1101–5.
[147] Assaf T, Al-Dweik A and Iraqi Y. High-rate secret key generation using physical layer security and physical unclonable functions. IEEE Open J Commun Soc 2023; **4**: 209–25.
[148] Nagubandi H and Harshan J. RASI: relay-assisted physical-layer key generation in unmanned aerial vehicles. In: 2018 IEEE 87th Vehicular Technology Conference (VTC Spring). IEEE, 2018, 1–5.
[149] Li K, Lu N and Zheng J et al. A practical secret key management for multihop drone relay systems based on bluetooth low energy. In: 2021 18th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON). IEEE, 2021, 1–2.
[150] Han D, Li A and Li J et al. DroneKey: a drone-aided group-key generation scheme for large-scale IoT networks. In: Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, CCS '21. New York, NY, USA: Association for Computing Machinery, 2021, 1306–19.
[151] Chen S, Sun S and Kang S. System integration of terrestrial mobile communication and satellite communication – the trends, challenges and key technologies in B5G and 6G. China Commun 2020; **17**: 156–71.
[152] Topal OA, Kurt GK and Yanikomeroglu H. Securing the inter-spacecraft links: doppler frequency shift based physical layer key generation. In: 2020 IEEE International Conference on Wireless for Space and Extreme Environments (WiSEE). IEEE, 2020, 112–117.
[153] Topal OA, Kurt GK and Yanikomeroglu H. Securing the inter-spacecraft links: physical layer key generation from doppler frequency shift. IEEE J Radio Freq Ident 2021; **5**: 232–43.
[154] Aman W, Ijaz A and Mahboob Ur Rahman M et al. Shared secret key generation via carrier frequency offsets. In: 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring). IEEE, 2019, 1–5.
[155] Zhang Z, Li G and Hu A. An adaptive information reconciliation protocol for physical-layer based secret key generation. In: 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring). IEEE, 2019, 1–5.
[156] Hao Y, Mu P and Wang H et al. Key generation method based on multi-satellite cooperation and random perturbation. Entropy 2021; **23**: 1653.
[157] Jin R, Yang L and Zhang H. Performance analysis of temporal correlation in finite-area UAV networks with LoS/NLoS. In: 2020 IEEE Wireless Commun and Networking Conference (WCNC). IEEE, 2020, 1–6.
[158] Zhang Y, Liu A and Li P et al. Deep learning (DL)-Based channel prediction and hybrid beamforming for LEO satellite massive MIMO system. IEEE Internet Things J 2022: **9**: 23705–15.
[159] Yun S, Kim I-M and Ha J. Artificial noise scheme for correlated MISO wiretap channels. IEEE Trans Veh Technol 2019; **68**: 9323–7.
[160] Wang C and Rahman A. Quantum-enabled 6G wireless networks: opportunities and challenges. IEEE Wireless Commun 2022; **29**: 58–69.
[161] Imre S. Quantum communications: explained for communication engineers. IEEE Commun Mag 2013; **51**: 28–35.
[162] Mavroeidis V, Vishi K and Zych MD et al. The impact of quantum computing on present cryptography. Preprint: arXiv:1804.00200, 2018.
[163] Elmabrok O and Razavi M. Wireless quantum key distribution in indoor environments. JOSA B 2018; **35**: 197–207.
[164] Chamola V, Jolfaei A and V Chanana et al. Information security in the post quantum era for 5G and beyond networks: threats to existing cryptography, and post-quantum cryptography. Comput Commun 2021; **176**: 99–118.
[165] Tsai C-W, Yang C-W and Lin J et al. Quantum key distribution networks: challenges and future research issues in security. Appl Sci 2021; **11**: 3767.
[166] Bedington R, Arrazola JM and Ling A. Progress in satellite quantum key distribution. NPJ Quant Inf 2017; **3**: 30.
[167] Shakiba-Herfeh M, Chorti A and Poor HV. Physical layer security: authentication, integrity, and confidentiality. In: Le KN (ed.). Physical Layer Security. Springer, Cham, 2021, 129–150.
[168] Li G, Luo H and Yu J et al. Information-theoretic secure key sharing for wide-area mobile applications. IEEE Wireless Commun 2023. doi: 10.1109/MWC.012.2200289.
[169] Sood K, Yu S and Nha Nguyen DD et al. A tutorial on next generation heterogeneous IoT networks and node authentication. IEEE Internet Things Mag 2021; **4**: 120–6.
[170] Aldaghri N and Mahdavifar H. Physical layer secret key generation in static environments. IEEE Trans Inf Forensics Secur 2020; **15**: 2692–2705.

Qingjiang Xiao received the B.Eng. degree from the College of Computer and Data Science, Fuzhou University. He is currently pursuing the M.Sc. degree with the School of Cyber Science and Engineering, Southeast University. His current research interests include physical layer security and secret key generation.

Jinrong Zhao received the B.Sc. degree in computer science and technology from Shenyang Aerospace University, Shenyang, China, in 2021. She is currently pursuing the M.S. degree in electronic information with Southeast University, Nanjing, China. Her research interests include physical layer security and secret key generation



Sheng Feng received the B.Eng. degree in electronic information from the School of Information and Communication Engineering, Nanjing Institute of Technology, Nanjing, China, in 2022. He is currently working toward the M.Eng. degree in the School of Cyber Science and Engineering, Southeast University, Nanjing, China. His research interests include physical layer security and secret key generation.

Guyue Li received the B.Sc. degree in Information Science and Technology and the Ph.D. degree in Information Security from Southeast University, Nanjing, China, in 2011 and 2017, respectively. From June 2014 to August 2014, she was a Visiting Student with the Department of Electrical Engineering, Tampere University of Technology, Finland. She is currently an associate professor with the School of Cyber Science and Engineering, Southeast University. Her research interests include physical layer security, secret key generation, radio frequency fingerprint and link signature.

Aiqun Hu received the B.Sc. (Eng.), the M.Sc. (Eng.) and Ph.D. degrees from Southeast University in 1987, 1990, and 1993 respectively. He was invited as a post-doc research fellow in The University of Hong Kong from 1997 to 1998, and TCT fellow in Nanyang Technological University in 2006. He is currently a Professor at the National Mobile Communications Research Laboratory, Southeast University. His research interests include data transmission and secure communication technology.