The survey and analysis on Physical Layer Encryption techniques

Xingxin Yu *

Coventry University 2 Handy Road, 05-01 The Cathay, Singapore 229233

* Corresponding Author Email: 1332931767@qq.com

Abstract. Physical Layer Key Generation (PKG) has evolved as a promising technique to circumvent the problems faced by the classical symmetric key production schemes. It exploits channel reciprocity and spatial decorrelation provided by wireless medium. This paper systematically reviews the evolution of PKG technologies, discussing their working principles, performance metrics, and implementations under various scenarios such as slow-fading channels, low SNR, and multi-user environments. With recent advancements introduced—intelligent reflecting surfaces (RIS/STAR-RIS), optimization powered by AI/ML, and their integration with massive MIMO and terahertz communications—chaos, robustness, and scalability enhancements are investigated. Further exploration involves application domains from IoT and healthcare to Industry 4.0 and 6G networks, this focus shifting from proof of feasibility to full-fledged implementation. The concluded findings show that PKG is inclined to become a key security primitive for next-generation wireless systems to enjoin lightweight and efficient friendly key management schemes.

Keywords: Physical Layer Key Generatio, Physical Layer Security, Machine Learning-Assisted Key Generation, Machine Learning-Enhanced Key Generation Scheme.

1. Introduction

For ages, channel eavesdropping on air interfaces due to the public nature of common channels has posed a challenge to security. Common methods of securing communication are based upon symmetric encryption at the link and application layers. But these methods have their disadvantages, such as complicated key distribution schemes or the risk of key leakage. To solve these shortcomings, the emerging Physical Layer Key Generation (PKG) techniques use channel reciprocity, thus sidestepping the need for pre-distributed keys and making it more difficult for an unauthorized device to listen for the encryption keys, which then enhances the security of the communication channel. Nevertheless, significant technical problems yet confront the existing KPG paradigms.

Common ones employed by the existing PKG schemes-auctioning the physical layer are RSS, CSI, and phase information. These features discriminate channel information inefficiently; i.e., they provide coarse-grained data that further reduce the rate of key generation and can degrade the randomness of the keys. Moreover, existing physical layer features are highly noise sensitive and thus suffer from a significant degradation in performance under low signal-to-noise ratio scenarios and from a drastic increase in key mismatch rate. From the standpoint of technical heterogeneity, existing physical layer features request baseband chips to furnish an external interface output to the extraction module after the demodulation of the signals.

Slow fading of channels constitutes yet another problem for PKG schemes. Keys would be updated dynamically based on CSI sampling as these channels have the nature of varying with time. The channel sampling should therefore be done at a rate equal to the maximum Doppler frequency. However, in environments where user mobility is quite low (wireless sensor networks, for instance), Doppler frequencies become low and the time necessary for producing longer keys becomes high; key sequences with substantial repeated patterns exist in the final quantized cryptographic sequence, considerably lowering the computational complexity of an exhaustive brute-force attack and consequently exposing the system to compromises.

This review paper focuses on analyzing technical challenges more systematically, covering different research approaches, achievements, functional performance metrics, application scenarios,

and technical teams in PKG at both domestic and international levels. Based on this review, some future trends are outlined for supporting the development and applications of PKG technology [1].

2. Physical Layer Key Generation Model

ALICE and BOB are legitimate communicators, while EVE acts as an attacker. ALICE and BOB exchange messages using a symmetric encryption algorithm, where the channel response is estimated based on their communication signals, and a secret key is generated accordingly. EVE, being located far from both ALICE and BOB, attempts a key eavesdropping attack by intercepting the communication signals between ALICE and BOB. She estimates the channel responses to infer the channel characteristics shared by ALICE and BOB, thereby attempting to derive their communication key. After the key estimation, EVE uses fraudulent messages to deceive either ALICE or BOB. (Figure 1).

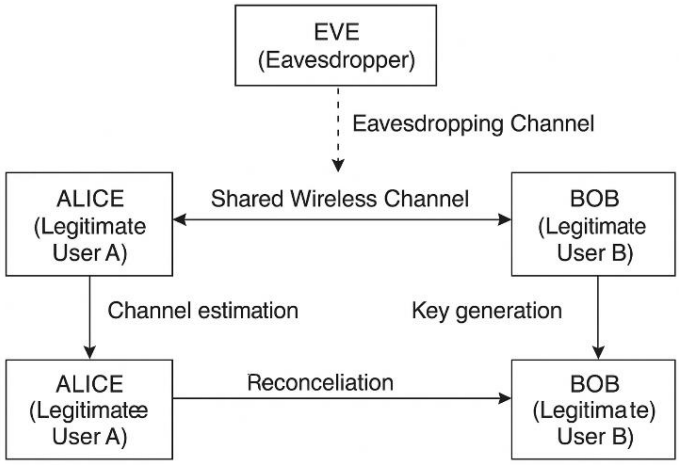

Figure 1. Physical Layer Key Generation Model involving Alice, Bob, and Eve

Before the conversation commences, EVE already has the following knowledge: 1. The communication protocol between ALICE and BOB; 2. Channel response used between ALICE and BOB for key generation, including the method of key generation; 3. Communication frequency band and time during communication between ALICE and BOB.

Channel Estimation – Both communicating parties (ALICE and BOB) measure the wireless channel characteristics, such as Channel State Information (CSI), to obtain correlated random values that are unique to their link.

Feature Extraction – The obtained channel measurements are processed to extract stable and distinguishable features (e.g., amplitude, phase, or received signal strength) suitable for key generation.

Information Reconciliation – This step corrects bit mismatches caused by noise, interference, or fading, ensuring that both ALICE and BOB hold identical key sequences.

Privacy Amplification – Finally, cryptographic hash functions are applied to compress and randomize the reconciled key, minimizing any partial information that may have been exposed to an eavesdropper (EVE).

These steps collectively ensure that the generated key is highly random, mutually consistent, and resilient to eavesdropping attacks, forming the foundation of secure physical-layer key generation.

3. Analysis of the Current State of Physical Layer Key Generation Technologies

3.1. Evolution of Physical Layer Key Generation

The physical layer key generation technique was born in 2008. Its traumas revolve around exploiting the reciprocal wireless multipath channel response functions as a doorway for an unsolicited key distribution method to be established between the chosen communicating entities. The mainth security advantage being the channel responses disappearing into their own variant forms as time increases with distance from each communication terminal. It is having this in theory that at any distance greater than half-a-wavelength, any channel response so measured by some device is independent from the original channel response. This makes it quite difficult for a passive eavesdropper or active adversary attempting a deception attack to glean the shared key. The initial experimental demonstration was based on RSS on an 802.11 platform where it was shown that the system did generate key bits at a certain rate with no errors while eavesdroppers shared very limited mutual information with the legitimate users and thus secured an effective protection from interception [2].

Wireless keying methods are envisioned to be applied on wearable wireless devices that may be moved or shaken. This takes RSS trajectories of two moving wireless devices as keying material, rather than the RSS itself. In addition, motivated by channel reciprocity in channel-based key establishment mechanisms, the key scheme proposes the novel notion of RSS trajectory reciprocity, guaranteeing a successful key generation when two devices have identical RSS values but their RSS trajectories are identical. To take full advantage of the RSS trajectories, considering the entropy and efficiency of the key generation process, this scheme then designs a file quantization scheme. Besides, here, we also analyze the security of the establishment of the key during eavesdropping and monitoring. The proposed scheme is tested to generate 64-, 128-, 192-, and 256-bit keys under indoor and outdoor environments, with timing results of 0.22/0.33, 0.61/0.74, 0.95/1.02, and 1.28/1.46 seconds, respectively.

In recent years, the development of physical layer key generation techniques has aimed to overcome the challenges caused by noise, low signal correlation, and synchronization issues in wireless channels. Research efforts have primarily focused on improving key generation efficiency, reducing bit mismatches, and enhancing the randomness and entropy of the generated keys. To achieve this, various adaptive quantization and signal processing methods—such as entropy-based quantization, machine-learning-assisted adaptive thresholding, and IRS-induced channel randomization techniques—have been introduced to extract more reliable and stable secret bits from wireless signals [3]. These advancements have greatly improved the robustness and practicality of physical layer key generation, providing a strong foundation for secure key establishment in next-generation wireless communication systems.

3.2. Challenges in PKG Technology for Slow-Changing Channel Scenarios

In slow-changing or static wireless channel environments, physical layer key generation (PKG) encounters severe limitations. Since the channel characteristics vary very little over time, the extracted key bits exhibit low randomness and weak entropy, which makes them unsuitable for secure key generation. As a result, the generated keys become more predictable, increasing the risk of key leakage and vulnerability to eavesdropping attacks. Moreover, insufficient channel variation leads to highly correlated channel measurements between consecutive samples, reducing the uniqueness of the shared keys. Synchronization errors and environmental noise further introduce bit mismatches between legitimate users, which degrade the overall key generation rate and reliability. Consequently, in static or low-mobility environments, PKG systems struggle to maintain both high entropy and stable key generation performance, limiting their practical deployment in real-world scenarios.

To overcome the limitations of slow-changing channels, several adaptive physical layer key generation (PKG) schemes have been proposed to enhance entropy, stability, and robustness. These

solutions aim to introduce artificial randomness, increase spatial diversity, or exploit multi-domain features to improve the quality of generated keys. Among the most representative approaches are environment-adaptive protocols based on Received Signal Strength (RSS) variation, MIMO-assisted extraction, relay-assisted key generation, and Intelligent Reflecting Surface (IRS)-based enhancement techniques [3]. Each approach targets specific performance goals such as higher key generation rate, lower bit mismatch rate, improved entropy, and resistance to predictable channel attacks. (Table 1)

Table 1. Comparison of Representative Physical Layer Key Generation Methods

Method	Core Idea	Main Advantage	Main Limitation
RSS-based	Utilizes small RSS fluctuations to extract random bits	Simple and easy to implement	Low entropy in static environments
MIMO-assisted	Exploits multi-antenna spatial diversity	High entropy and scalability	Requires complex hardware
Relay-assisted	Adds relay nodes to introduce extra randomness	Improves key rate and entropy	Increases communication overhead
TDS Scheme	Generates time-domain randomness through substitution	Strong against predictable channel attacks	Needs accurate synchronization
IRS-based	Uses intelligent reflecting surfaces to vary propagation	Effective in static channels	Higher implementation cost

3.3. Challenges of PKG Technology in MIMO Scenarios

In multiple-input multiple-output (MIMO) systems, physical layer key generation (PKG) faces several technical challenges. The presence of multiple antennas introduces high-dimensional channel characteristics and complex spatial correlation, which increase the difficulty of channel estimation and synchronization. In addition, hardware mismatches between transmit and receive chains may destroy channel reciprocity, resulting in inconsistent key bits. The coexistence of multiple users in massive MIMO networks also leads to pilot contamination and inter-beam interference, which can cause information leakage and degrade the reliability of key generation.

To address these challenges, various research teams have proposed MIMO-specific PKG enhancement schemes. For example, a research group developed the MAKE (Multi-Antenna Key Extraction) technique using IEEE 802.11n multi-antenna devices to construct a multi-antenna key generator. The MAKE approach exploits RSSI-based common randomness, and experimental results in indoor and outdoor environments demonstrated that it could increase the bit generation rate by nearly four times compared to single-antenna systems. This verified the feasibility of multi-level quantization to enhance key extraction efficiency. The basic communication structure of TDD-based physical layer key generation in a MIMO system — involving Alice, Bob, the base station, and an eavesdropper — is illustrated in Figure 2.

Another research team designed a CSI-based PKG approach that fully utilizes the channel state information to exploit spatial diversity, yielding higher key generation rates than RSSI-based schemes. To further improve reliability, an LDPC-coded PKG system was introduced, where quaternary LDPC coding outperformed the binary version under higher signal-to-noise ratio (SNR) conditions by providing better error correction and bit consistency.

In addition, a multi-user OFDMA-based PKG protocol was proposed to enable simultaneous key establishment between a base station and multiple users. This design allows parallel uplink and downlink key generation, effectively reducing channel probing overhead while maintaining low interference.

For millimeter-wave (mmWave) massive MIMO systems, researchers proposed exploiting virtual Angle of Arrival (AoA) and Angle of Departure (AoD) features as new sources of channel randomness. These parameters are sparse, stable, and resistant to noise, enabling bit agreement rates above 99% even at −10 dB SNR.

To further reduce pilot overhead and inter-user interference in large-scale MIMO, another team introduced a Channel Dimension Reduction (CDR) method. This technique utilizes the sparse beam-domain channel model to estimate only a few dominant channels along the main beam directions. The approach significantly reduces pilot signaling requirements and minimizes spatial correlation between users, allowing secure and efficient key generation in parallel non-overlapping beams [4].

Overall, these studies demonstrate that through adaptive quantization, channel diversity utilization, coding enhancement, and spatial beam-domain optimization, PKG technology in MIMO scenarios can achieve improved entropy, higher key generation rates, and better resilience against eavesdropping attacks.

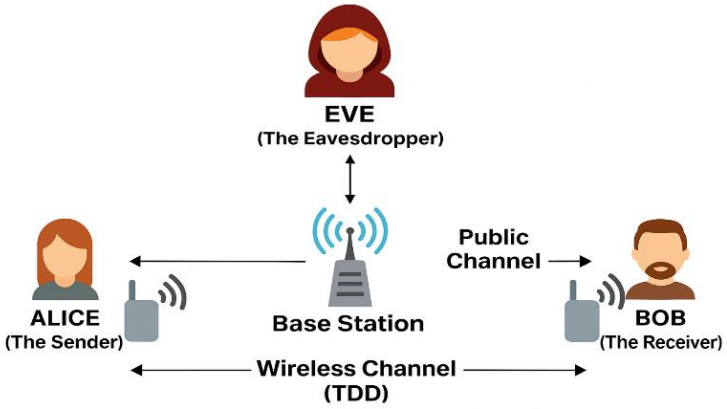

Figure 2. Communication Model of Physical Layer Key Generation under TDD MIMO System

4. PKG Development Trends and Application Scenarios

After the past decade, some fundamental issues, common research scenarios, or applications in physical layer key generation had mostly been clarified. The main challenges confronted root into three different measures for evaluating schemes for key generation: the key generation rate, key mismatch rate, and key randomness. Common application scenarios include: low-power IoT security scenarios, high-speed communication scenarios such as 6G networks, and slow fading, and mmWave-MIMO. The trends in physical layer key generation research point to maximizing the key generation rate, minimizing the key mismatch rate, and enhancing the randomness of generated keys in these scenarios.

4.1. Key Generation Assisted by Reconfigurable Intelligent Surfaces (RIS/STAR-RIS)

One of the most active research trends of the past few years has been introducing reconfigurable intelligent surfaces to inject active randomness in slow-fading/static channels to improve bit consistency and key rates [5]. A systematic review in 2024 classified RIS-assisted PKG into three kinds: introduction of randomness by RIS, optimization of reflection coefficients, and design of detection/pilot protocols while also comparing multiple optimization techniques. Meanwhile, STAR-RIS allows attainers to obtain sufficient independent degrees of freedom even in quasi-static environments. Experiments showed significant improvements in matching rates and throughput in slow-fading scenarios and thus open new feasible avenues for industrial IoT and indoor deployments [5].

4.2. Systematic Security for 6G: Integration with PLS/JCS/ISAC and Policy Promotion

At the system level, 6G security research advances the physical layer, connection layer, and service layer together in parallel, where the physical layer is the “first line of defense” from eavesdropping and interference. Both the 2025 comprehensive review and NIST perspectives emphasize that in 6G-where latency and synchronization demands are more stringent-the security implications of physical layer events are tremendously amplified. Therefore, the joint design of PKG with other key

technologies such as JCS/ISAC, massive MIMO/THz, and RIS has to be included in the industrial standards and evaluation framework. This means that future PKG will possess more of a system role within design than an "add-on module" of traditional wireless systems.[8]

4.3. AI/ML-Driven Intelligent PKG

The presence of AI/Machine Learning in PKG is getting more and more highlighted [6]. Particularly, its role is evident in three specific respects.

Channel Estimation and Non-Reciprocity Compensation [7]: Conventional methods result in reduced key agreement rate in FDD systems or when hardware imperfections make the channel non reciprocal. The study in 2024 shows that the "mapping learning" through deep neural networks on the FDD uplink and downlink channels can recover symmetric features from different frequency bands and hence restore PKG performance.

An adaptive quantization method serves this purpose: traditionally, fixed thresholds have been used, making them vulnerable to noise or environmental conditions. Using machine learning, it is possible to adaptively adjust the quantization boundaries and predict bit inconsistencies in the information coordination phase, thus minimizing the overhead of retransmission and error correction.

Adversarial Security and Attack Detection: An attacker might exaggerate machine learning to deduce channel characteristics and to strengthen eavesdropping capabilities. To deal with such intelligent attacks, researchers propose "adversarial sample training"—using generative adversarial networks (GANs) to simulate possible attacker signals and create resistance in PKG. This trend indicates that future PKG security will not be based on "the assumption of unintelligent attackers" but rather on defenses against "AI-empowered eavesdroppers [8]."

5. Conclusion

Through this survey and analysis, it is concluded that physical layer key generation (PKG) has evolved from conceptual validation to a mature, system-oriented security paradigm. By leveraging channel reciprocity and spatial randomness, PKG effectively addresses the limitations of traditional symmetric key schemes. Research progress across slow-fading, MIMO, and multi-user environments has demonstrated that integrating techniques such as RIS/STAR-RIS, AI-driven optimization, and beam-domain modeling significantly enhances key entropy, robustness, and scalability. The continuous convergence of PKG with 6G, IoT, and intelligent network frameworks indicates its growing role as a foundational security primitive, enabling lightweight and adaptive key management for future wireless communication systems.

References

[1] Petrov, V., Guerboukha, H., Shaikhanov, Z., Knightly, E. W., Mittleman, D. M., & Jornet, J. M. (2025). Physical Layer Security for Terahertz Communications in massive IOT. DIVA. https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1927849&dswid=851.

[2] Kumar, R., & Arnon, S. (2024). Review of physical layer security in Integrated Satellite–Terrestrial Networks. MDPI. https://www.mdpi.com/2079-9292/13/22/4414.

[3] Ma, Y., Chen, L., Lu, T., Song, Y., & Cao, K. (2024). Star-ris-assisted key generation method in quasi-static environment - EURASIP journal on Wireless Communications and networking. Springer Open. https://jwcn-eurasipjournals.springeropen.com/articles/10.1186/s13638 - 024 - 02388 - y.

[4] Chai, M., Liu, Y., Zhao, S., & Deng, H. (2025). Enhancing physical-layer security in UAV-assisted communications: A UAV-mounted reconfigurable intelligent surface scheme for secrecy rate optimization. MDPI. https://www.mdpi.com/2504 - 446X/9/3/208.

[5] Gao, N., Han, Y., Li, N., Jin, S., & Matthaiou, M. (2024). When physical layer key generation meets ris: Opportunities, challenges, and Road ahead | ieee journals & magazine | ieee xplore. IEEE Xplore. https://ieeexplore.ieee.org/document/10475842/.

[6] Liu, K., Li, M., Huang, K., Wan, Z., Li, Q., Sun, X., Xu, X., & Jin, L. (2024). Object-based attention: Saliency detection using contrast via background prototypes - zhou - 2014 - electronics letters - wiley online library. The Institution of Engineering and Technology. https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/el.2014.0903.

[7] Torshizi, E. O., & Henkel, W. (2024). Pairwise physical layer secret key generation for FDD systems. IEEE Xplore. https://ieeexplore.ieee.org/document/10693595/.

[8] Gan, C., Wang, W., Hu, Y., Zhao, X., Dun, S., Xiao, Q., Wang, W., & Huang, H. (2025). Coupling secret sharing with decentralized server-aided encryption in encrypted deduplication. MDPI. https://www.mdpi.com/2076 - 3417/15/3/1245.