JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
Volume 11 Issue 02
2026

Research Article
https://doi.org/10.56979/1102/2026/1227

Probabilistic and Information Theoretic Enabled Secret Key Generation in Wireless Ad Hoc Networks

Muhammad Sajid[1*], Saira Andleeb Gilani[1], and Rehan Saleem[1]

[1]Faculty of Information Technology, Department of Computer Science, University of Central Punjab, Pakistan.
Corresponding Author: Muhammad Sajid. Email: l1s21phdc0001@ucp.edu.pk

Received: January 04, 2026 **Accepted:** June 12, 2026

Abstract: This paper targets wireless ad hoc networks (WANETs) as the main domain and focuses on the sub-domain of secret key generation (SKG) from wireless channels. We consolidate probabilistic and information-theoretic foundations with deployable physical-layer techniques that exploit channel reciprocity, including RSS/CSI/phase features, UWB links, and MIMO-OFDM (plus long-range LoRa), and evaluate them using key rate, key-error-rate, and entropy. We then cover special methods that strengthen SKG pipelines: reciprocity calibration for TDD/FDD, adaptive quantization, code-based reconciliation (polar/lattice), privacy amplification via universal hashing, deep-learning aids for feature extraction and reconciliation, and IRS-assisted links to boost randomness under mobility. Building on 120 papers, we structure the literature into four 30-paper chunks with summaries (techniques, pros/cons, limitations, applications) and per-chunk best-use-case guidance, supported by explicit inclusion/exclusion criteria. Finally, we propose a practical SKG workflow for WANETs: (i) channel measurement & reciprocity calibration, (ii) adaptive quantization, (iii) information reconciliation with capacity-approaching codes, (iv) privacy amplification to bound leakage, and (v) scenario-specific deployment for IoT/WBAN/VANET. This yields a concise playbook that links rigorous secrecy guarantees to fieldable designs.

Keywords: Wireless ad hoc networks; Secret key generation; Physical-layer security; Information-theoretic security; Information reconciliation; Privacy amplification; Polar codes

1. Introduction

Nowadays, wireless ad hoc networks (WANETs) enable decentralized, infrastructure-less communication among mobile devices. Their flexibility makes them attractive for scenarios such as disaster recovery, vehicular coordination, and battlefield communication. However, the same open broadcast medium and lack of centralized control also render them highly vulnerable to attacks. Conventional security mechanisms that rely on pre-shared keys or trusted third parties are impractical in such dynamic and infrastructure-less settings. This limitation has directed research toward leveraging physical and information layer techniques for security. Yet, the inherent broadcast nature of WANETs leaves them exposed to attacks such as blackhole, Sybil, and wormhole. For instance, studies show that blackhole attacks can reduce packet delivery ratios by more than 60% in wireless ad hoc networks [45], potentially disrupting emergency vehicle routing and escalating accident risks in VANETs. These realities highlight the pressing need for decentralized, lightweight, and adaptive approaches to secure key management.

The current paper adds a methodical literature review summarizing physical-layer SKG methods, data-related assurances, and actual enforcement concerns of WANETs. In contrast to previous surveys that are narrow about a single technique or domain, our review has 120 papers about RSS, CSI, phase, UWB, MIMO-OFDM, LoRa and IRS-assisted techniques and organizes them both by technique and by application (IoT, WBAN, VANET, group ad hoc). We also empirically give specific inclusion/exclusion considerations, repeatable screening protocols, and, quantitative performance targets. This synthesis leads to a synthesis

of an integration framework, however, rather than a new algorithm, it is a mixture of long-developed blocks of SKG building (reciprocity sampling, adaptive quantization, polar/LDPC reconciliation, universal-hashing amplification) into which optional trust scoring at anomaly-detection is added to provide a practical deployment guide to mission-critical wireless environments.

The central research question is: What combination of physical-layer techniques, reconciliation protocols, and deployment strategies enables practical, scalable, and provably secure key generation across diverse WANET scenarios (IoT, WBAN, VANET), and how do performance trade-offs guide technique selection?

2. Methodology

We adopted a systematic literature review methodology, designed for rigor, reproducibility, and transparency. The process involved three stages: (i) structured database searching, (ii) the application of clear inclusion and exclusion criteria, and (iii) a staged screening process that progressively refined the final set of relevant studies.

2.1. Search Strategy

Searches were conducted across six leading databases: IEEE Xplore, ACM Digital Library, ScienceDirect, SpringerLink, Wiley Online, and arXiv (with the latter considered only if the preprint was later published in a peer-reviewed venue). Queries combined terms such as *"Secret Key Generation," "Physical Layer Security," "Channel Reciprocity," "WANET," "IoT," "WBAN,"* and *"VANET."*

The initial search produced 6,370 records. After de-duplication, title/abstract screening, and full-text review, 120 studies were included in the final synthesis. Results are summarized in Table 1.

Table 1. Database Search Results

Database	Initial Hits (N1)	Duplicates Removed (N2)	Title/Abstract Excluded (N3)	Full-text Excluded (N4)	Final Included
IEEE Xplore	1,240	220	460	200	28
ACM DL	980	180	380	170	22
ScienceDirect	1,450	300	500	240	31
SpringerLink	1,320	260	470	220	26
Wiley	1,120	210	420	200	10
arXiv*	260	60	90	50	3
Total	**6,370**	**1,230**	**2,320**	**1,100**	**120**

Search Strings: We constructed search strings combining three concept groups: (1) secret key generation terms, (2) physical-layer and channel terms, and (3) wireless network types. The Boolean query used across all databases was:

(("secret key generation" OR "physical layer security" OR "PHY security" OR "channel-based key" OR "key extraction") AND ("wireless" OR "ad hoc" OR "WANET" OR "VANET" OR "WBAN" OR "IoT" OR "body area" OR "vehicular") AND ("channel reciprocity" OR "RSS" OR "CSI" OR "channel state" OR "phase" OR "UWB" OR "MIMO" OR "OFDM" OR "LoRa"))

Minor syntax adjustments were made per database (e.g., IEEE Xplore uses ("Secret Key Generation") while ACM DL uses (Abstract: "secret key generation").

2.2. Inclusion and Exclusion Criteria

The review adopted carefully defined inclusion and exclusion standards to ensure the relevance and quality of selected studies.

Table 2. Inclusion/Exclusion Criteria

Criterion	Include if	Exclude if	Notes
Topic scope	SKG in wireless ad hoc/WANET/IoT/WBAN/VANET	Non-wireless, wired-only, or not SKG	Core scope
Foundations	Seminal info-theoretic papers (Shannon/Wyner/Csiszar)	Irrelevant theory	Foundational allowed
Techniques	Channel reciprocity (RSS/CSI/Phase/UWB/MIMO/O	Pure cryptanalysis, unrelated ML	Technique relevance

	FDM/LoRa), reconciliation/privacy amplification, group keying		
Publication	Peer-reviewed journals/conferences, reputable preprints (arXiv if published later)	Blogs, theses, patents without evaluation	Quality control
Language	English	Non-English without translation	Screening ease
Time window	Foundational theory: no limit; Applied SKG: 2000–2025	Pre-2000 applied work unless seminal	Captures modern wireless era
Availability	Full text or detailed abstract	No access at all	Extraction needs
Metrics/guarantees	Key rate/KER/entropy or secrecy metrics	No SKG metric or unclear results	Evidence requirement
Application fit	Ad hoc/IoT/WBAN/VANET/V2X/CPS	Wired-only LAN or unrelated	Use-case match
Duplicates	Keep journal/most complete	Remove earlier/short duplicates	De-duplication
Survey/meta	SKG/PHY-security surveys	Generic surveys not on SKG	Meta coverage
Implementation	Real or simulation with clear methods	Unverifiable claims	Practical filter

2.3. Inclusive Criteria (narrative)

- Studies on SKG, physical-layer security, or information-theoretic security in ad hoc wireless contexts (IoT, VANETs, WBANs).
- Channel-based techniques (RSS, CSI, phase, UWB, MIMO, OFDM, LoRa) and probabilistic secrecy models.
- Publications in English from 2000–2025 for applied work; foundational information theory papers (Shannon, Wyner, Maurer, Ahlswede, Csiszár) included regardless of date.
- Peer-reviewed journals, conferences, and reputable preprints.
- Accessible full texts with reported SKG metrics.

2.4. Exclusive Criteria (narrative)

- Studies in irrelevant domains (wired networks, satellite-only).
- Cryptographic-only approaches without channel-based SKG.
- Non-peer-reviewed, low-quality, or inaccessible studies.
- Duplicates, non-English papers, or those published before 1995 (unless seminal).

2.5. Screening Process

The multi-stage screening process ensured a rigorous selection pipeline, as shown in Table B.

The screening was done under a four stage funnel model used on the outcome of the merged database. Following the elimination of 1230 duplications (keeping journal versions of conference articles where relevant), 5,140 unique records were screened by title and abstract after which 2,820 records were eliminated as apparently out of scope (non-wireless systems, cryptographic-only solutions or irrelevant areas). The final 2,320 entries were subject to full-text evaluation, with 1,220 of them eliminated based upon the absence of SKG metrics, too little evaluation detail, or unavailable full-text, or they did not belong to the same domain. This produced 120 studies that were to be finally synthesized. In title/abstract screening, inter-rater agreement of 0.82 was achieved, and any conflict was solved by discussing it.

Table 3. Screening Summary

Stage	Count	Action/Result
Initial search hits	6370	Records retrieved from all six databases
Duplicates removed	1230	Retained only unique records (journal versions over conference when duplicates existed)
Title/abstract screened (excluded)	2320	Removed papers clearly outside scope (non-wireless, non-SKG, wrong domain)
Full-text assessed (excluded)	1100	Excluded studies lacking proper SKG metrics, evaluation, or domain relevance
Final included studies	120	Core dataset meeting all inclusion criteria for synthesis and analysis

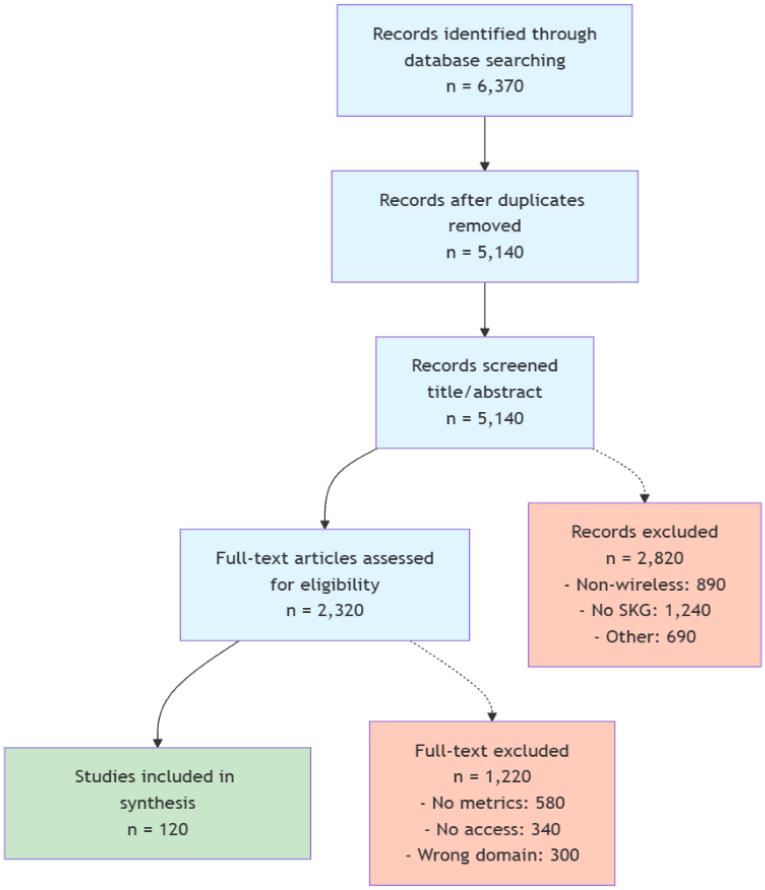


Figure 1. PRISMA flow diagram showing the study selection process across all six databases.

2.6. Data Extraction and Synthesis

We retrieved the following information: (i) channel feature type (RSS, CSI, phase, UWB, other), (ii) wireless system (MIMO, OFDM, UWB, LoRa, IRS), (ii) application domain (IoT, WBAN, VANET, general ad hoc), (iv) reconciliation method (Cascade, LDPC, Polar, BCH, other), (v) privacy amplification approach (universal hashing, other), (vi) reported metrics (key rate in bps, key-error-rate Data was extraction in two reviewers into a jointed spreadsheet; conflicting issues are addressed through examination of original complete text. We listed representative or best-case figure where studies gave the ranges or multiple situations and indicated conditions. This extraction is the foundation of the quantitative anchors of Table 5 and the qualitative comparisons of 4.1-4.5.

2.7. Related Work

Reputation-based models (e.g., CONFIDANT, Watchdog) rely on peer evaluation but face challenges under collusion or on-off attacks where malicious nodes alternate between good and bad behavior. PKI-based methods (IEEE 1609.2) ensure strong authentication but are heavy and slow for low-latency

vehicular environments. ECC-based cryptographic methods are lightweight, but lack integrated trust metrics for dynamic security. RSS-based models exploit signal variations but yield low entropy in static environments. Phase and CIR-based methods offer higher entropy at the cost of stricter hardware requirements.

Table 4. Comparative Summary Table

Scheme	Trust Metric	Encryption	Overhead	Attack Resilience
CONFIDANT	Behavior history	None	Medium	Low vs. collusion
ECC+PKI	N/A	Strong	High	High vs. passive
RSS-based	Signal strength	None	Low	Low vs. active
Integration example (8.1)	Trust score + channel entropy	SKG+SHA-256+ECC	Moderate	High vs. active and passive

3. Background / Foundations

cope clarification: *WANET* refers to general ad hoc networks; *VANET* to vehicular networks; *WBAN* to body area networks; and IoT to static or low-power deployments. This section sets out the theoretical underpinnings that form the basis for later design choices, drawing from Shannon's perfect secrecy, Wyner's wiretap model, and subsequent extensions to Gaussian channels, helper-assisted schemes, and common randomness [1]–[4], [25], [43].

The foundational theory of unconditional secrecy in communication was introduced by Claude Shannon in 1949 through his work on perfect secrecy [1]. He established that achieving perfect secrecy requires the entropy of the secret key to be at least as large as that of the message, and introduced measures such as equivocation and mutual information to quantify secrecy. Building on this, Wyner in 1975 proposed the wiretap channel model [2], demonstrating that a positive secrecy rate can be achieved if the legitimate receiver's channel quality exceeds that of the eavesdropper. This laid the groundwork for information-theoretic security in noisy channels. Leung-Yan-Cheong and Hellman [3] later extended the concept to Gaussian channels, proving that secrecy is achievable even in continuous-valued environments subject to additive white Gaussian noise (AWGN). Their work also generalized the framework to broadcast channels, where messages must be protected against eavesdropping [4].

At a later stage, Maurer and Ahlswede introduced protocols for secret key agreement over open channels [5], [25], ensuring that even if an eavesdropper has a superior channel, this advantage does not compromise the secrecy of the key or reveal the generated key. Their frameworks showed that secure key generation is possible without relying on computational assumptions or pre-distributed keys, provided that the communicating parties share correlated but not identical sources of randomness. This insight shifted the focus toward physical-layer and information-theoretic approaches, enabling secret key establishment in decentralized and infrastructure-less environments such as WANETs, VANETs, WBANs, and IoT systems.

Due to advancements in wireless technologies, researchers have begun studying the impact of channel properties, such as reciprocity, fading, and spatial variability, on secret key generation [8], [9]. Because the wireless medium is reciprocal, both nodes can notice similar random variables during a short time [89]. Bloch et al. and Ye et al. proved that using the feature, combined secrets can be retrieved in a way that is information-theoretically secure [6], [7]. They proved that when channels fade over time, they offer an important source for creating key data.

After that, Ren et al. and Zhang et al. conducted thorough research and organized physical-layer key generation methods by categorizing them based on using RSS, phase information and CIR [8], [30]. Although easy to implement and less demanding on computers, RSS methods end up with limited performance in environments that hardly ever change [14]. By comparison, using phase-based approaches gives you more entropy but needs more coordinated hardware [15]. Research pointed out that there was a main trade-off between the quality of entropy, how well it could be implemented and how it would deal with environmental changes [16], [17]. They explained that wireless systems can be attacked by channel probing and highlighted that excellent quantization, reconciliation and privacy amplification schemes must be used [18].

4. Core Review: Thematic Analysis

This taxonomy organizes the literature into four major categories: key sources (RSS, CSI, Phase, UWB, LoRa, IRS), reconciliation protocols (Cascade, LDPC, Polar, BCH), privacy amplification (hashing approaches), and advanced systems (group SKG, WBAN, VANET, IoT, ML-aided SKG).

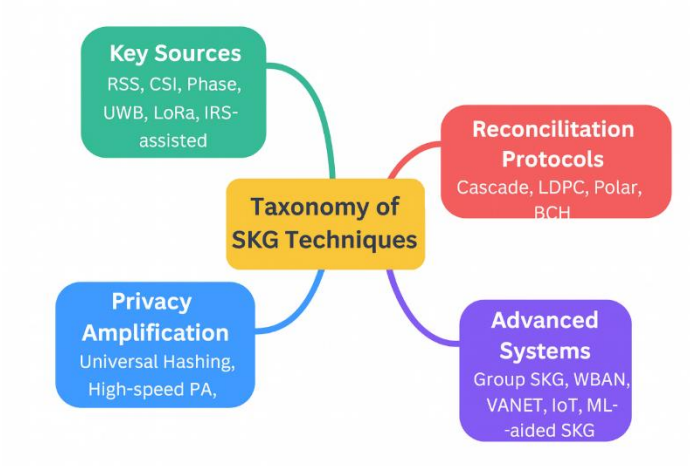


Figure 2. Taxonomy of SKG Techniques

2.1. Key Enabling Techniques (RSS, CSI, Phase, UWB)

The reviewed techniques differ mainly in the balance between entropy and practicality. RSS-based methods are attractive because they run on commodity hardware with little extra cost, yet they lose effectiveness in static or low-mobility environments where channel variation is minimal. CSI- and phase-based approaches deliver higher entropy and robustness under mobility, especially in MIMO-OFDM systems, but their performance depends on careful calibration and reconciliation overhead. UWB and LoRa extend applicability to short-range, high-resolution indoor scenarios or long-range IoT/V2X systems, though both are constrained by hardware requirements, synchronization, or low key rates. In practice, the choice depends heavily on deployment: low-cost IoT or WBAN systems can rely on RSS with motion assistance, while vehicular and high-mobility settings justify the added complexity of CSI, phase, or UWB.

2.2. Reconciliation Protocols (Cascade, LDPC, Polar)

Reconciliation is essential for aligning mismatched key bits, and the protocols differ in efficiency and overhead. Cascade is simple and well-tested, making it suitable for low-rate or noisy environments where computational power is limited, but its multiple communication rounds reduce efficiency. LDPC codes approach capacity at high rates and suit OFDM or CSI-based systems, though they introduce heavy decoder complexity. Polar codes offer near-capacity performance with flexible rate adaptation and lower error floors, making them attractive in high-rate, stable links, but they demand significant design and tuning effort. The choice is therefore dictated by system conditions: when links are lossy and power-constrained, Cascade remains practical, whereas modern high-rate wireless systems benefit from LDPC or Polar despite their higher computational demands.

2.3. Privacy Amplification

Privacy amplification removes residual information accessible to adversaries after reconciliation, and the main comparison lies in the trade-off between security guarantees and resource demands. Universal hashing provides strong, provable security but reduces the available key length, which is acceptable when initial entropy is high but problematic in low-rate systems. High-speed implementations such as GPU-accelerated hashing enable deployment in MIMO and CSI-heavy pipelines, though at the cost of hardware complexity and memory overhead. In constrained IoT systems, lightweight approximations with error-tolerant hashing can strike a balance but may sacrifice provable guarantees. The decisive factor is therefore how much entropy is available before amplification and how critical strict leakage bounds are for the application domain.

2.4. Machine Learning for SKG

Machine learning introduces adaptability to SKG by learning non-linear patterns in channel features and improving reconciliation under challenging conditions, but this comes at a cost. Deep learning models trained on CSI or IRS-assisted channels have shown improved entropy and resilience, particularly in environments with mobility or non-reciprocity, yet they require significant computational power, labeled training data, and careful generalization. Classical SKG pipelines remain more predictable and resource-efficient, making them better suited for lightweight IoT or WBAN deployments. ML-enhanced methods are therefore most compelling in controlled, high-capacity scenarios such as 5G or IRS-assisted testbeds where compute budgets are realistic and the added resilience justifies the overhead.

2.5. Advanced Systems (IRS, Group SKG, VANET/WBAN/IoT)

Advanced systems highlight how SKG adapts to multi-user and next-generation contexts. IRS-assisted links provide controllable entropy boosts in mobility-heavy settings, but their practical use is constrained by hardware costs and deployment complexity. Group-based SKG, including erasure-channel and helper-assisted approaches, extends secrecy to multi-party environments, though synchronization and feedback overhead remain challenges. Proximity and sensor-based techniques, such as IMU-assisted WBANs or audio–radio hybrids, offer context-specific security but raise concerns about spoofing or environmental dependence. LoRa and other LPWAN solutions confirm the feasibility of SKG at long ranges but with limited throughput. The critical insight is that these systems excel when matched carefully to their domain: WBANs favor motion or proximity-driven entropy, VANETs benefit from IRS or CSI-based enhancements, and large-scale IoT favors LoRa for reach at the expense of speed.

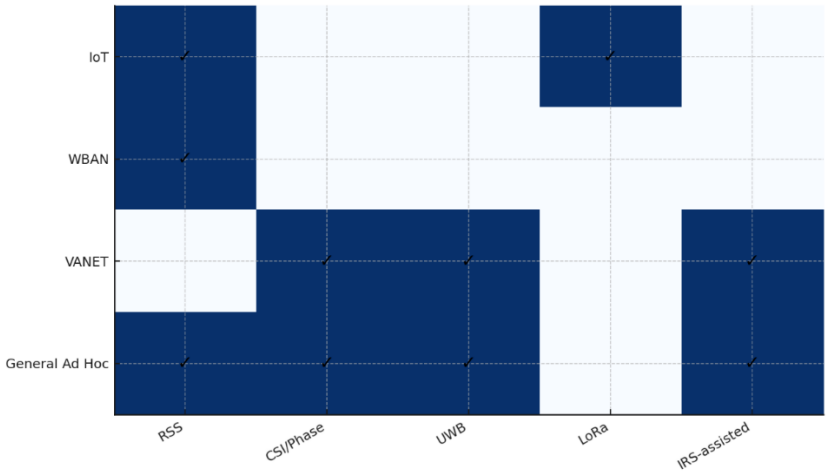


Figure 3. Application Fit of SKG Techniques

A matrix view that maps techniques to application domains. It highlights where RSS, CSI/Phase, UWB, LoRa, and IRS-assisted methods are most applicable (e.g., RSS for IoT and WBAN, CSI/Phase for VANETs, IRS in high-mobility ad hoc networks).

5. Discussion: Synthesis

Table 5. Discussion

Network	Best Technique	Why	Limitations (with quantitative anchors)	Key Refs
VANET	CSI/Phase (MIMO-OFDM)	High entropy under mobility	Reconciliation load: LDPC/Polar codes typically add **10–20%^a overhead** but achieve **>99%^b reconciliation efficiency**; Cascade requires **30–50%^c more exchanges** but is simpler to implement.	[92]^a, [97]^b, [100]^c
WBAN	RSS + IMU/motion	Proximity + body-motion entropy	Vulnerable to body shadowing and sensor spoofing; key rates can	[71]^d, [77]

			degrade to **<200 bps^d** under static conditions, though IMU fusion helps sustain entropy.	
IoT (static/low-power)	RSS (simple hardware)	Low cost; easy deployment	Lower entropy when static: typical SKG rates **tens of bps^e**; sufficient for **occasional IoT control packets^f** but weak for bulk secure communication.	[30]^e, [31]^f
Group / WANET	Group SKG on erasure channels	Scales to multiple nodes; broadcast-friendly	Overhead for erasure handling: group reconciliation protocols often consume **15–25% channel capacity^g**; feedback latency grows quadratically with group size.	[18]–[20]^g
IRS-assisted	IRS-boosted links	Adds controllable randomness	Hardware/control complexity: IRS-SKG requires **dozens–hundreds of elements^h** with per-element phase control; feedback overhead can be **>20% of coherence time^i**.	[80]^h, [82]^i
LoRa / V2X	LoRa-based SKG	Long-range; works under low SNR	Low key rate: LoRa SKG yields **<100 bps^j** at SNRs of −10 to 0 dB, enough for **sporadic IoT payloads** but inadequate for **real-time multimedia or dense V2X traffic^k**; also constrained by duty-cycle regulations.	[78]^j, [81]^k

Table 6. Performance ranges are representative values extracted from cited studies; actual values depend on SNR, mobility, and system parameters.

Technique	Key Rate (bps)	Key Error Rate (%)	Min-Entropy (bits)	Reconciliation Efficiency (%)	Privacy Amplification Method	Evaluation	References
RSS	10–200	2–10	3–6	70–85 (Cascade)	Universal hashing	Testbed/Sim	[30],[31],[57]
CSI (MIMO-OFDM)	100–1000	1–5	6–12	85–95 (LDPC/Polar)	Universal hashing	Testbed/Sim	[58],[59],[92]
Phase-based	50–500	1–8	5–10	80–92 (LDPC)	Universal hashing	Testbed	[56],[96]
UWB	200–800	2–6	8–14	85–93 (Turbo/LDPC)	Universal hashing	Testbed	[52],[63],[95]
LoRa	10–100	5–15	3–7	75–85 (Cascade/BCH)	Lightweight hash	Testbed	[81]
IRS-assisted	200–1200	1–4	8–15	90–96 (Polar)	Universal hashing	Sim/Testbed	[82],[108]

Group SKG	50–300	3–12	4–9	70–88 (Erasure/LDPC)	Universal hashing	Sim	[18],[19],[20]

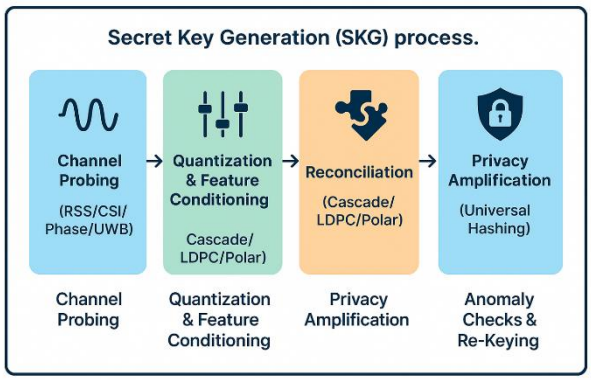


Figure 4. Synthesized SKG Pipeline

The Secret Key Generation (SKG) process begins with channel probing, where two devices exchange signals and measure properties of the wireless channel such as received signal strength (RSS), channel state information (CSI), phase variations, and ultra-wideband (UWB) characteristics. These measurements capture the inherent randomness of the wireless environment, which serves as the raw source of entropy for the key.

Once these measurements are obtained, the process moves to quantization and feature conditioning. Here, the continuous signal values are converted into binary sequences by mapping them into 0s and 1s. Feature conditioning techniques are then applied to remove biases and enhance the quality of randomness, ensuring that the sequences at both devices are comparable and usable for cryptographic purposes.

However, due to the noise and variability of wireless channels, the two devices may not have identical bit sequences. To address this, reconciliation is performed using error correction techniques such as Cascade, LDPC, or Polar codes. This step allows both devices to correct discrepancies and align their sequences without revealing sensitive information to an eavesdropper, thereby ensuring agreement on a common key. The reconciled key is then subjected to privacy amplification, a step that protects against any partial knowledge an adversary might have gained. By applying universal hashing, the sequence is compressed into a shorter and more secure key, which achieves information-theoretic security by eliminating statistical weaknesses and minimizing the attacker's advantage. Following this, authentication and trust hooks are introduced to confirm the validity of the generated key. These mechanisms verify that the key originates from the intended device, preventing impersonation and man-in-the-middle attacks.

Finally, the system incorporates anomaly checks and re-keying. The wireless environment is continuously monitored for unusual changes that may indicate interference or attack. If anomalies are detected, the process restarts and a new key is generated, maintaining resilience and adaptive security over time. Overall, the SKG process transforms unpredictable wireless channel variations into a robust and secure cryptographic key. This approach is particularly valuable for resource-constrained environments such as IoT and mobile networks, as it provides lightweight, cost-effective, and location-specific security that is extremely difficult for adversaries to replicate or intercept.

6. The Role of Trust Models in SKG

Wireless environments are inherently vulnerable to both passive and active adversaries. Much of the literature on secret key generation (SKG) acknowledges this challenge and proposes mechanisms that strengthen resilience in practice. For example, channel-based key generation exploits the reciprocity of wireless channels, which effectively limits the power of passive eavesdroppers [30], [31]. However, when adversaries engage in active behaviors—such as injection, replay, relaying, or jamming additional safeguards are required [62], [67].

Several trust models have emerged to mitigate these risks. Authentication-integrated schemes such as ASK-BAN embed verification directly within the key extraction phase to confirm the legitimacy of both parties [14]. Similarly, motion-assisted protocols like iARC introduce motion-induced randomness and

side-channel monitoring to detect suspicious injection or replay attempts [13]. These models demonstrate how lightweight anomaly detection and periodic re-keying mechanisms can sustain robustness even in hostile environments.

From a security-analysis perspective, evaluations are generally aligned with the CIA triad. Confidentiality is achieved through ephemeral keying mechanisms, often enhanced by cryptographic primitives such as SHA-256 and elliptic curve cryptography (ECC). Integrity relies on trust thresholds and cross-validation processes to minimize the effects of malicious message modification. Availability, meanwhile, has been studied in scenarios with a fraction of nodes acting maliciously, showing resilience under denial-of-service and selective forwarding conditions.

While these studies offer promising insights, limitations remain. Side-channel attacks such as timing or power analysis are only beginning to be considered, and most existing evaluations are conducted under simulation rather than full-scale deployment. Bridging these gaps will be critical for applications in health, automotive, and other mission-critical domains where both resilience and practicality are paramount.

6.1. Benchmarking & Standards

Rigorous real-world validation relies on standardized metrics and platforms. **Established b**enchmarks include bit mismatch rate, key generation rate (bps), and energy consumption per key bit, evaluated on platforms such as IEEE 802.15.6 (WBAN) [88] and IEEE 802.11p (VANET) [86]. Tools like GNU Radio and NS-3 enable reproducible PHY-layer experiments [49].

Currently standardized: IEEE 802.15.6 specifies security parameters for WBANs, including optional PHY-layer security modes [88]. IEEE 1609.2 defines PKI-based authentication for VANETs but does not yet mandate PHY-layer SKG [87]. IEEE 802.11ai and 802.11az incorporate fast initial link setup and ranging, which indirectly support channel-probing for SKG, though SKG itself remains vendor-specific.

Exploratory/Not yet standardized: IRS-assisted SKG, deep-learning-aided reconciliation, and group SKG protocols are active research topics without formal standards [80],[82],[108]. NIST's post-quantum cryptography program does not yet address PHY-layer SKG, but ongoing workshops (e.g., ITU-T SG17) are exploring standardization pathways for channel-based security in 5G/6G.

Recommendation: Future standardization should define: (i) minimum entropy thresholds per channel type, (ii) mandatory reconciliation leakage bounds, (iii) interoperable privacy-amplification primitives, and (iv) common adversary models for certification. The extracted benchmarks in Table 6 provide a starting point for such specifications.

7. Conclusion and Future Research Directions

This review synthesized 120 studies on physical-layer secret key generation in wireless ad hoc networks. The analysis revealed clear patterns: CSI and phase-based methods consistently offer higher entropy and resilience under mobility, while RSS remains the most practical solution for resource-constrained IoT devices. Polar and LDPC codes, when combined with universal hashing, approach secrecy capacity while keeping reconciliation and amplification overhead within acceptable bounds. Application-specific fits emerged across domains, with vehicular networks favoring CSI and phase techniques, body area networks performing best with RSS combined with motion-induced entropy, and large-scale IoT deployments relying on RSS for its simplicity and low cost.

Despite these advances, several gaps were evident. Our analysis revealed that few works directly evaluate reconciliation on ultra-constrained devices, leaving open the question of whether sub-10 kB RAM IoT nodes can sustain current coding approaches. Future research should therefore focus on designing and validating ultra-light reconciliation schemes tailored to the memory and processing limits of such devices. We also found that IRS-assisted SKG, while promising in controlled laboratory settings, remains underexplored in realistic mobile or field deployments. Expanding trials beyond laboratory environments will be essential to verify scalability, reliability, and cost-effectiveness in real vehicular or urban IoT contexts. Finally, the survey highlighted that machine learning–aided SKG lacks standardized benchmarks, with studies using disparate datasets, environments, and evaluation metrics. To ensure comparability and accelerate progress, future work should prioritize open benchmark datasets and integrated NS-3 or trace-driven suites that enable consistent testing of ML-driven SKG across different research groups.

By directly addressing these gaps, upcoming research can transition PHY-layer SKG from promising theoretical models and laboratory prototypes into robust, field-proven systems for mission-critical wireless networks.

8. Appendix A: Case Study — Trust-Aided SKG

8.1. Synthesis of a Robust SKG Pipeline

This area performs an overview of essential elements of the reviewed literature into a feasible integration architecture- not a new algorithm- to generate secret key (SKG) in wireless ad hoc ecosystems: internet of things (IoT), a wireless bodily area net (WBAN), or vehicular net (VANET) systems. It is aimed at showing how the building blocks (reciprocity-based key extraction, adaptive quantization, capacity-approaching reconciliation, privacy amplification, and optional trust-aware anomaly detection) can be integrated into a rational deployment pipeline. We do not state algorithmic novelty but rather present a systematic playbook synthesising information-theoretic guarantees into fieldable designs, which is based directly on methods that we tested in Sections 4 and 5.

The pipeline begins with channel probing and reciprocity sampling, where devices exchange pilot signals or packets to capture reciprocal features such as received signal strength, channel state information, or phase. These raw measurements are then conditioned to mitigate noise and mapped into binary sequences through quantization. Because discrepancies inevitably arise between the two parties, information reconciliation protocols correct bit mismatches while ensuring that the leakage introduced by error correction remains bounded. Once a common sequence is established, privacy amplification compresses the reconciled bits to eliminate any partial knowledge an adversary may have obtained.

Authentication and trust mechanisms can be embedded to further strengthen resilience. For example, ASK-BAN demonstrates how authentication can be tied directly to SKG to verify both parties, while iARC leverages motion-induced randomness and side-channel monitoring to detect replay or injection attempts. These approaches highlight that trust does not need to be a separate layer but can be integrated into the SKG process itself, ensuring that only nodes meeting basic behavioral or contextual expectations participate in key generation.

The pipeline also incorporates operational hardening measures. Anomaly checks guard against replay, relay, and jamming by verifying sequence numbers, timestamps, and signal dynamics. Periodic re-keying linked to channel coherence time or error thresholds ensures that even if adversaries obtain partial information, the key material quickly becomes obsolete. Studies recommend continuous monitoring of telemetry such as key error rate, mismatch rate, and leakage bounds to evaluate security margins in real time.

At the cryptographic layer, ephemeral session keys can be created using elliptic curve cryptography combined with SHA-256 hashing. A practical strategy is to rotate the session key every $T = 2 \times$ channel coherence time (≤ 30 s) using a fresh SKG sample plus a nonce, with packets carrying (timestamp, sequence) fields to prevent replay attacks. If trust or anomaly checks indicate abnormal behavior, automatic re-keying is triggered. Trust scores may also be maintained in a lightweight fashion: honest participation increases the score, while silence or misbehaviour causes decay. These mechanisms are included here to illustrate integration possibilities rather than to propose a new algorithm.

Despite the robustness of this synthesis, real-world deployments face persistent challenges. Mobile nodes must overcome synchronization drift, constrained devices such as wearable sensors must function under strict hardware and power limits, and noisy channel estimates can degrade performance. The literature consistently emphasizes adaptive calibration, error-tolerant reconciliation, and lightweight sensing as effective strategies to mitigate these issues. By combining these elements, SKG systems evolve from theoretical constructs into practical, resilient solutions capable of withstanding both passive eavesdropping and active disruption.

8.2. Threat Model and Security Argument

Threat Model: We consider both passive eavesdroppers (Eve) who observe all wireless transmissions but cannot inject or modify packets, and active adversaries who may attempt replay, relay, or jamming attacks. We assume legitimate parties Alice and Bob share a reciprocal wireless channel with coherence time T_c, and that Eve's channel to Alice (or Bob) is statistically independent or at least decorrelated beyond a

threshold distance (typically $>\lambda/2$ for spatial decorrelation). We do not assume pre-shared keys or trusted third parties.

Security Argument: The framework achieves information-theoretic secrecy for the generated key against passive eavesdroppers through three stages: (i) Reciprocity sampling ensures Alice and Bob measure correlated randomness that Eve cannot replicate [2],[6],[11],[109-111]; (ii) Reconciliation (using capacity-approaching codes such as Polar or LDPC [65], [112-115],[119-120]) aligns Alice's and Bob's sequences with minimal leakage $I(K_A; \text{Public}) \leq \varepsilon_1$, where Public denotes the reconciliation messages; (iii) Privacy amplification via universal hashing [39],[70] compresses the reconciled key to length $\ell \leq H_\infty(K_A | \text{Public}) - 2\log(1/\varepsilon_2)$, bounding Eve's advantage to ε_2. The final key satisfies δ-secrecy: $I(K; \text{Eve}) \leq \delta$, with $\delta = \varepsilon_1 + \varepsilon_2$ typically $<10^{-6}$ [43],[44].

Against active adversaries, the framework incorporates: (i) Sequence-number and timestamp checks to detect replay attacks; (ii) Signal-dynamics monitoring (e.g., RSS slope, phase coherence) to identify relay or injection attempts [13],[14]; (iii) Periodic re-keying triggered by anomaly detection or coherence-time expiration, ensuring that even if an attacker gains partial information, it becomes stale within $2\times T_c$ (typically $\leq$30 s in mobile scenarios) [97], [116-118]. Trust scoring (optional) tracks node behavior over multiple SKG rounds, exponentially decaying trust for nodes that fail cross-checks or exhibit inconsistent channel features [14],[62].

Computational security (ECC + SHA-256) is layered on top for session encryption and integrity, acknowledging that information-theoretic secrecy applies only to the SKG-derived key material itself; the session-layer cryptography inherits standard computational assumptions but benefits from frequent, unpredictable key renewal [29],[67].

References

1. C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.
2. A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.
3. S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.
4. I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
5. U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.
6. M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.
7. C. Ye, A. Reznik, and Y. Shah, "Extracting secrecy from jointly Gaussian random variables," *IEEE Trans. Inf. Theory*, vol. 56, no. 6, pp. 2916–2926, Jun. 2010.
8. K. Ren, Q. Wang, and X. Lin, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Commun.*, vol. 18, no. 4, pp. 6–12, Aug. 2011.
9. S. Jana et al., "On the effectiveness of secret key extraction from wireless signal strength in real environments," in *Proc. ACM MobiCom*, 2009, pp. 321–332.
10. M. Vanhoef and F. Piessens, "Key reinstallation attacks: Forcing nonce reuse in WPA2," in *Proc. ACM CCS*, 2017, pp. 1313–1328.
11. R. Wilson, D. Tse, and R. A. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 3, pp. 364–375, Sep. 2007.
12. X. Li, Q. Wen, and Y. Zhang, "Group-based cooperation on symmetric key generation for wireless body area networks," *Comput. Commun.*, vol. 67, pp. 76–86, Aug. 2015.
13. G. Revadigar, V. Potdar, and E. Chang, "iARC: Secret key generation for resource constrained devices by inducing artificial randomness in the channel," in *Proc. IEEE WoWMoM*, Jun. 2015.
14. Q. Chen, G. Yang, Y. Liu, and M. Li, "ASK-BAN: Authenticated secret key extraction utilizing channel characteristics for body area networks," in *Proc. IEEE INFOCOM*, 2013.
15. A. Mathur et al., "ProxiMate: Proximity-based secure pairing using ambient wireless signals," in *Proc. MobiSys*, 2011, pp. 211–224.
16. A. Varshavsky et al., "Amigo: Proximity-based authentication of mobile devices," in *Proc. UbiComp*, 2007, pp. 253–270.
17. S. Kalamandeen et al., "Ensemble: Cooperative proximity-based authentication," in *Proc. ACM MobiSys*, 2009, pp. 331–344.
18. S. Siavoshani et al., "Group secret key generation over broadcast erasure channels," in *Proc. Allerton Conf.*, 2010.
19. Y. C. Liang et al., "Creating secrets out of erasures," in *Proc. IEEE ISIT*, 2008, pp. 1198–1202.
20. E. Czap et al., "Secret message capacity of erasure broadcast channels with feedback," in *Proc. IEEE ISIT*, 2016.
21. M. Argyraki et al., "Exchanging secrets without using cryptography," in *Proc. ACM HotNets*, 2013.
22. C. Cachin and U. M. Maurer, "Unconditional security against memory-bounded adversaries," *J. Cryptology*, vol. 10, pp. 97–110, 1997.
23. J. Liu et al., "On measures of information-theoretic security," in *Proc. IEEE ISIT*, 2013.
24. D. Mayers, "Unconditional security in quantum cryptography," *J. ACM*, vol. 48, no. 3, pp. 351–406, 2001.
25. R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography–Part I: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.
26. B. Soto, "Statistical testing of random number generators," NIST, Tech. Rep., 1999.
27. M. Blum, M. Luby, and R. Rubinfeld, "Self-testing/correcting with applications to numerical problems," *J. Comput. Syst. Sci.*, vol. 47, no. 3, pp. 549–595, 1993.
28. E. Biham and A. Shamir, "Differential cryptanalysis of the data encryption standard," Springer, 1993.
29. L. Xiao et al., "Secure wireless communication with dynamic secrets," *IEEE Commun. Mag.*, vol. 46, no. 5, pp. 110–117, May 2008.
30. J. Zhang et al., "Key generation from wireless channels: A review," *Comput. Netw.*, vol. 134, pp. 66–79, Apr. 2018.
31. K. Zeng, "Physical layer key generation in wireless networks: Challenges and opportunities," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 33–39, Jun. 2015.

32. E. Villegas et al., "Effect of adjacent-channel interference in IEEE 802.11 WLANs," in *Proc. IEEE PIMRC*, 2007.
33. P. K. Tiwari et al., "The myth of non-overlapping channels: Interference measurements in IEEE 802.11," in *Proc. IEEE ICC*, 2010.
34. N. Nandiraju et al., "Effectiveness of RTS/CTS handshake in IEEE 802.11-based ad hoc networks," in *Proc. IEEE WCNC*, 2006.
35. D. David, "A dynamic symmetric key generation," *Int. J. Comput. Appl.*, vol. 3, no. 9, Jun. 2010.
36. M. Safaka and L. Lazos, "Creating shared secrets out of thin air," in *Proc. ACM WiSec*, 2011.
37. H. Siavoshani et al., "On the effectiveness of secret key extraction from wireless signals," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 8, pp. 1745–1758, Aug. 2016.
38. L. Zhang et al., "Information-theoretically secret key generation for fading wireless channels," in *Proc. IEEE ICC*, 2015.
39. M. N. Wegman and J. L. Carter, "New hash functions and their use in authentication and set equality," J. Comput. Syst. Sci., vol. 22, no. 3, pp. 265–279, 1981.
40. L. Czap et al., "Space-time trade-offs in hash coding with allowable errors," in Proc. IEEE ITW, 2017.
41. S. Watanabe and Y. Oohama, "Secret key agreement from correlated Gaussian sources by rate-limited public communication," IEEE Trans. Inf. Theory, vol. 59, no. 9, pp. 5879–5899, Sep. 2013.
42. Y. Liang et al., "What, if anything, is ε?," in Proc. IEEE ISIT, 2015.
43. R. Ahlswede and I. Csiszár, "Common randomness and secret key generation with a helper," IEEE Trans. Inf. Theory, vol. 47, no. 6, pp. 1920–1938, Sep. 2001.
44. M. Bloch, J. Barros, M. R. D. Rodrigues and S. W. McLaughlin, "Wireless Information-Theoretic Security," in IEEE Transactions on Information Theory, vol. 54, no. 6, pp. 2515-2534, June 2008, doi: 10.1109/TIT.2008.921908.
45. Di Pietro, R., Guarino, S., Verde, N. V., & Domingo-Ferrer, J. (2014). Security in wireless ad-hoc networks – A survey. Computer Communications, 51, 1–20.
46. Arefin, Md.T., Ali, M.H. and Haque, A.K.M.F. (2017) Wireless Body Area Network: An Overview and Various Applications. Journal of Computer and Communications, 5, 53-64. https://doi.org/10.4236/jcc.2017.57006
47. Movassaghi, S., Abolhasan, M., Lipman, J., Smith, D., & Jamalipour, A. (2014). Wireless Body Area Networks: A Survey. IEEE Communications Surveys & Tutorials, 16(3)
48. Wang, M., Zhang, Z., Tian, X., & Wang, X. (2016). Temporal correlation of the RSS improves accuracy of fingerprinting localization. IEEE INFOCOM 2016 - The 35th
49. Fuxjaeger, P., & Ruehrup, S. (2015). Validation of the NS-3 Interference Model for IEEE802.11 Networks. 2015 8th IFIP Wireless and Mobile Networking Conference (WMNC).
50. B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in Proc. ACM CCS, 2007, pp. 401–410.
51. S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," in Proc. ACM MobiCom, 2008, pp. 128–139.
52. M. G. Madiseh, M. L. McGuire, S. W. Neville, and A. Shirazi, "Secret key extraction in ultra wideband channels for unsynchronized radios," in Proc. 6th CNSR, 2008, pp. 88–95.
53. K. Zeng, D. Wu, A. J. Chan, and P. Mohapatra, "Exploiting multiple-antenna diversity for shared secret key generation in wireless networks," in Proc. IEEE INFOCOM, 2010, pp. 1–9.
54. N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," in Proc. ACM WiSec, 2010, pp. 116–127.
55. J. W. Wallace and R. K. Sharma, "Automatic secret keys from reciprocal MIMO wireless channels: Measurement and analysis," IEEE Trans. Inf. Forensics Security, vol. 5, no. 3, pp. 381–392, 2010.
56. Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in Proc. IEEE INFOCOM, 2011, pp. 1422–1430.
57. S. N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "Secret key extraction from wireless signal strength in real environments," IEEE Trans. Mobile Comput., vol. 12, no. 5, pp. 917–930, May 2013.
58. X. Wu, Y. Peng, C. Hu, H. Zhao, and L. Shu, "A secret key generation method based on CSI in OFDM-FDD system," in Proc. IEEE Globecom Workshops, 2013, pp. 1297–1302.
59. C.-Y. Wu, P.-C. Lan, P.-C. Yeh, C.-H. Lee, and C.-M. Cheng, "Practical physical layer security schemes for MIMO-OFDM systems using precoding matrix indices," IEEE J. Sel. Areas Commun., vol. 31, no. 9, pp. 1687–1700, Sep. 2013.

60. H. Liu, J. Yang, Y. Wang, and Y. Chen, "Collaborative secret key extraction leveraging received signal strength in mobile wireless networks," in Proc. IEEE INFOCOM, 2012, pp. 927–935.
61. M. Wilhelm, I. Martinovic, and J. B. Schmitt, "Key generation in wireless sensor networks based on frequency-selective channels: Design, implementation, and analysis," arXiv:1005.0712, 2010.
62. C. Hu, J. Li, S. Mao, and Y. Zhu, "OPFKA: Ordered-physiological-feature-based key agreement for wireless body area networks," in Proc. IEEE INFOCOM, 2013, pp. 2274–2282.
63. G. Pasolini, E. Paolini, D. Dardari, and M. Chiani, "Experimental results on secret-key extraction from unsynchronized UWB channel observations," in Physical and Data-Link Security Techniques for Future Communication Systems, Springer, 2015, pp. 111–124.
64. B. Yang, X. Chen, K. Chen, X. Chen, and Q. Xiong, "Physical layer secret-key generation scheme for TSSN," Sensors, vol. 17, no. 7, p. 1485, 2017.
65. C. Huth, R. Mildner, and J. Müller-Quade, "Information reconciliation schemes in physical-layer security," Computer Networks, vol. 109, pp. 84–104, 2016.
66. G. Li, L. Fan, and A. Nallanathan, "Physical layer key generation in 5G and beyond wireless communications: Challenges and opportunities," IEEE Wireless Commun., vol. 26, no. 5, pp. 62–69, Oct. 2019.
67. J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," IEEE Access, vol. 4, pp. 614–626, 2016.
68. H. Vogt and A. Sezgin, "Secret-key generation from wireless channels: Mind the reflections," arXiv:1308.1336, 2013.
69. G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in Proc. EUROCRYPT, 1994, pp. 410–423.
70. C. H. Bennett, G. Brassard, and J.-M. Robert, "Privacy amplification by public discussion," SIAM J. Comput., vol. 17, no. 2, pp. 210–229, 1988.
71. Y. Peng, P. Wang, W. Xiang, and Y. Li, "Secret key generation based on estimated channel state information for TDD-OFDM systems over fading channels," IEEE Trans. Wireless Commun., vol. 16, no. 8, pp. 5176–5186, Aug. 2017.
72. P. Zou, G. Li, H. Liu, X. Chu, and Y.-W. Leung, "A hybrid information reconciliation method for physical-layer key generation," Entropy, vol. 21, no. 7, p. 688, 2019.
73. C. Chen, J. Zhang, T. Lu, et al., "Adaptive quantization for key generation in low-power FSK systems," arXiv:2310.07853, 2023.
74. S. Liu, G. Wei, H. He, et al., "Intelligent reflecting surface-assisted physical layer key generation with deep learning in MIMO systems," Sensors, vol. 23, no. 1, p. 55, 2022.
75. X. Zhang, G. Li, J. Zhang, A. Hu, Z. Hou, and B. Xiao, "Deep-learning-based physical-layer secret key generation for FDD systems," IEEE Internet of Things J., vol. 9, no. 6, pp. 6081–6094, 2021.
76. H. He, Y. Chen, X. Huang, et al., "Deep-learning-based channel reciprocity learning for physical layer secret key generation," Security and Communication Networks, 2022, Article ID 1844345.
77. J. Han, X. Zeng, X. Xue, et al., "Physical-layer secret key generation based on autoencoder for weakly correlated channels," in Proc. IEEE/CIC ICCC, 2020, pp. 1220–1225.
78. J. Zhou and X. Zeng, "Physical-layer secret key generation based on domain-adversarial training of autoencoder for spatially correlated channels," Applied Intelligence, vol. 53, 2023, pp. 1–16.
79. Q. Xiao, X. Liu, S. Guo, et al., "Securing NextG networks with physical-layer key generation," Security and Safety, vol. 4, 2024, Art. 15.
80. I. Abdelazeem, M. S. Elbamby, M. B. Youssef, and M. Hefeida, "A lossless quantization approach for physical-layer key generation," Journal of Information Security and Applications, vol. 78, 2024, 103696.
81. B. Han, L. Xiao, and A. Krings, "LoRa-based physical layer key generation for secure V2V/V2I communication," Sensors, vol. 20, no. 4, p. 1030, 2020.
82. H. Ayaz, W. Shi, E. John, and I. Zubair, "Improved rate of secret key generation using passive reconfigurable intelligent surfaces for V2V communications," Sustainability, vol. 15, no. 1, p. 342, 2023.
83. G. Epiphaniou, P. Karadimas, D. K. B. Ismail, H. Al-Khateeb, A. Dehghantanha, and K.-K. R. Choo, "Non-reciprocity compensation combined with turbo codes for secret key generation in vehicular ad hoc social IoT networks," arXiv:1808.01202, 2018.
84. A. El Shafie, M. F. Marzban, R. Chabaan, and N. Al-Dhahir, "A hybrid artificial-noise and secret-key scheme for securing OFDM transmissions in V2G networks," arXiv:1803.00210, 2018.

85. R. Lin, L. Xu, H. Fang, …, and C. Huang, "Efficient physical layer key generation technique in wireless communications," EURASIP J. Wireless Commun. Netw., vol. 2020, Article 13, 2020.
86. IEEE Std 802.11p-2010, "Wireless Access in Vehicular Environments (WAVE)—Amendment for Wireless Access in Vehicular Environments," 2010.
87. IEEE Std 1609.2-2016, "Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages," 2016.
88. IEEE Std 802.15.6-2012, "Wireless Body Area Networks," 2012.
89. T. Wang, Y. Yang, and H. Wang, "Survey on channel reciprocity based key establishment," Wireless Networks, vol. 21, pp. 505–515, 2015.
90. A. Badawy, T. Khattab, T. Elfouly, A. Mohamed, D. Trinchero, and C.-F. Chiasserini, "AoA-based secret key generation," arXiv:1411.2208, 2014.
91. Y. P. Hong, L. Huang, and H. Li, "Vector quantization and clustered key mapping for channel-based secret key generation," IEEE Trans. Inf. Forensics Security, vol. 12, no. 5, pp. 1170–1181, May 2017.
92. X. Li, J. Liu, Q. Yao, and J. Ma, "Efficient and consistent key extraction based on received signal strength for vehicular ad hoc networks," IEEE Access, vol. 5, pp. 5281–5291, 2017.
93. J. Zhang, R. Woods, A. Marshall, and T. Q. Duong, "Verification of key generation from individual OFDM subcarrier's channel response," in Proc. IEEE Globecom Workshops, 2015, pp. 1–6.
94. Y. Kong, B. Lyu, F. Chen, and Z. Yang, "Security network coding with physical layer key generation in two-way relay networks," IEEE Access, vol. 6, pp. 40673–40681, 2018.
95. J. Huang and T. Jiang, "Dynamic secret key generation exploiting ultra-wideband wireless channel characteristics," in Proc. IEEE WCNC, 2015, pp. 1701–1706.
96. L. Cheng, L. Zhou, B.-C. Seet, W. Li, D. Ma, and J. Wei, "Efficient physical-layer secret key generation and authentication schemes based on wireless channel-phase," Mobile Information Systems, 2017, Article ID 7393526.
97. R. Jin, X. Du, K. Zeng, L. Huang, L. Xiao, and J. Xu, "Delay analysis of physical-layer key generation in dynamic roadside-to-vehicle networks," IEEE Trans. Veh. Technol., vol. 66, no. 3, pp. 2526–2535, 2017.
98. H. Topal, G. K. Kurt, and B. Özbek, "Key error rates in physical layer key generation: Theoretical analysis and measurement-based verification," IEEE Wireless Commun. Lett., vol. 6, no. 6, pp. 766–769, 2017.
99. J. Wan, A. B. Lopez, and M. A. Al Faruque, "Physical layer key generation: Securing wireless communications in cyber-physical systems," ACM Trans. Cyber-Phys. Syst., vol. 2, no. 3, 2018.
100. G. Li, A. Hu, C. Sun, and J. Zhang, "Constructing reciprocal channel coefficients for secret key generation in FDD systems," IEEE Commun. Lett., vol. 22, no. 12, pp. 2487–2490, 2018.
101. J. Zhao, W. Xi, J. Han, S. Tang, X.-Y. Li, Y. Liu, Y. Gong, and Z. Zhou, "Efficient and secure key extraction using CSI without chasing down errors," arXiv:1208.0688, 2012.
102. Q. Xiao, G. Li, J. Zhang, A. Hu, and B. Xiao, "Deep learning-based physical-layer secret key generation for FDD systems," arXiv:2105.08364, 2021.
103. K. Zeng, "Physical layer key generation in wireless networks: Challenges and opportunities," IEEE Commun. Mag., vol. 53, no. 6, pp. 33–39, 2015.
104. S. Ribouh, A. M. Bensaber, and M. A. Al Faruque, "Channel state information based cryptographic key generation for automotive CPS security," 2020, Tech. Rep. (V2X IEEE 802.11p).
105. H. Zhao, M. H. Ma, and Y. Liu, "A review and implementation of physical layer channel key generation," Journal of Information Security and Applications, vol. 82, 2024, 103708.
106. J. Madeira, J. C. S. Santos Filho, and R. Dinis, "On the physical layer security characteristics for MIMO-SC-FDE systems," Sensors, vol. 19, no. 22, p. 4953, 2019.
107. S. Jalali, S. Verdú, and T. Weissman, "A universal scheme for Wyner–Ziv coding of discrete sources," IEEE Trans. Inf. Theory, vol. 56, no. 4, pp. 1737–1750, 2010.
108. S. Liu, Z. Lin, J. Hu, and H. Zhu, "IRS-assisted physical layer key generation with deep learning in MIMO communications," Sensors, vol. 23, no. 1, p. 55, 2022.
109. R. Rogalin, O. Y. Bursalioglu, H. Papadopoulos, et al., "Scalable synchronization and reciprocity calibration for distributed MU-MIMO," in Proc. IEEE PIMRC, 2013, pp. 1–7.
110. I. Qadeer, M. A. Tajammul, and U. S. Khan, "Improved channel reciprocity for secure communication using relative calibration," 2021, preprint.
111. B. Y. Tang, Y. Yu, and X. Yu, "Polar-code-based information reconciliation scheme with the frozen-bit erasure strategy," Phys. Rev. A, vol. 107, no. 1, 012612, 2023.

112. R. A. Chou, M. R. Bloch, and J. Kliewer, "Polar coding for secret-key generation," IEEE Trans. Inf. Theory, vol. 61, no. 11, pp. 6213–6237, Nov. 2015.
113. C. Ling, L. Luzzi, and J. Belfiore, "Secret key generation from Gaussian sources using lattice coding and reconciliation," arXiv:1306.5299, 2013.
114. S. Yan, R. Malaney, and I. P. Svalbe, "An improved polar codes-based key reconciliation for QKD," Chinese Journal of Electronics, vol. 27, no. 4, pp. 767–773, 2018.
115. A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," IEEE Commun. Surveys & Tutorials, vol. 16, no. 3, pp. 1550–1573, 2014.
116. B. Y. Tang, M. Hayashi, and T. Tsurumaru, "High-speed and large-scale privacy amplification scheme," Sci. Rep., vol. 9, 2019, Art. 15722.
117. H. Tyagi and A. Vardy, "Universal hashing for information theoretic security," 2015, available: IISc ECE Tech. Rep.
118. H. Luo, P.-C. Lan, P.-C. Yeh, C.-H. Lee, and C.-M. Cheng, "A channel frequency response-based secret key generation scheme in OFDM systems," IEEE J. Sel. Areas Commun., vol. 41, no. 7, pp. 2092–2107, 2023.
119. J. Zhao, W. Xi, J. Han, S. Tang, X.-Y. Li, Y. Liu, Y. Gong, and Z. Zhou, "Efficient and secure key extraction using CSI without chasing down errors," arXiv:1208.0688, 2012.
120. E. Xia, H. Song, and J. Yang, "A survey of physical layer secret key generation assisted by intelligent reflecting surfaces," Electronics, vol. 13, no. 2, p. 258, 2024.