International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 1, Jan-Feb-2026, ISSN (Online): 2395-566X

Beyond Static Secrecy: A Self-Adaptive, Noise-Aware Privacy Amplification Framework for Heterogeneous 6G Quantum-Secured Networks.

Okai Tettey-Antie Samuel
University of Ghana, Ghana

Abstract - Modern Quantum Key Distribution (QKD) often fails in highly dynamic mobile environments due to rigid post-processing architectures. This paper introduces a pioneering self-adaptive privacy amplification (SAPA) framework that replaces traditional static compression with a closed-loop controller. By integrating twelve distinct quantum noise models—including Non-Markovian and Gaussian Bosonic channels—we demonstrate that real-time entropy estimation can reclaim up to 25% of secure key material previously lost in mobile-induced fluctuations. Our results establish a new paradigm for "living" security in future 6G ecosystems.

Keywords - Quantum Key Distribution (QKD), 6G Security, Adaptive Privacy Amplification, Quantum Noise Modeling, Information Theory.

INTRODUCTION

Quantum communication has emerged as a transformative paradigm for secure information exchange, offering security guarantees rooted in the laws of quantum mechanics rather than computational assumptions. Among the most prominent technologies in this domain is Quantum Key Distribution (QKD), which enables two communicating parties to establish a shared secret key while detecting the presence of any eavesdropper. As quantum technologies transition from laboratory demonstrations to real-world deployments, attention has increasingly shifted toward mobile and heterogeneous quantum networks.

Mobile quantum communication environments—such as satellite-based QKD, unmanned aerial platforms, and mobile ground terminals—introduce operational conditions that differ substantially from static fiber-based links. In such environments, quantum channels are subject to rapid fluctuations caused by relative motion, atmospheric effects, environmental interference, and hardware instability. These factors give rise to non-stationary and structured quantum noise that directly affects the reliability and security of key generation processes.

Within the QKD protocol stack, privacy amplification plays a critical role in ensuring that any information potentially leaked to an adversary is eliminated from the final key. Privacy amplification achieves this by compressing the reconciled key according to an estimate of the adversary's information. Traditional privacy amplification mechanisms assume stationary noise behavior and rely on fixed compression parameters derived from worst-case security analyses. While such assumptions simplify protocol design, they become increasingly misaligned with the realities of mobile quantum channels.

When privacy amplification parameters are fixed in dynamic environments, two undesirable outcomes may occur. Over-amplification leads to excessive key shortening, reducing system throughput and practical usability. Under-amplification, on the other hand, risks leaving residual information accessible to an adversary, undermining security guarantees. These issues highlight the need for adaptive mechanisms capable of responding to changing noise conditions.

This work investigates privacy amplification in the context of mobile quantum networks, with a specific focus on how different quantum noise structures influence entropy dynamics and security performance. By examining a diverse set of quantum noise models and introducing an adaptive privacy amplification strategy, this study aims to bridge the gap between theoretical security assumptions and practical deployment realities.

Background

Quantum Key Distribution Fundamentals Quantum Key Distribution enables secure key establishment by encoding information into quantum states whose measurement unavoidably disturbs the system. Protocols such as BB84 exploit this property to detect eavesdropping attempts by monitoring error rates in the quantum channel. Following quantum transmission, classical post-processing steps—including sifting, error correction, and privacy amplification—are applied to produce a secure final key.

The security of QKD relies on bounding the information available to an adversary, typically quantified using entropy measures. Accurate estimation of this entropy is essential for determining how much compression is required during privacy amplification.

Privacy Amplification in QKD

Privacy amplification reduces an adversary's partial knowledge of a key by applying universal hash functions or equivalent compression techniques. The amount of compression required depends on the estimated min-entropy of the reconciled key conditioned on the adversary's information. Finite-key effects, estimation uncertainty, and channel noise all influence this estimation process.

In practice, privacy amplification parameters are often fixed prior to deployment. While conservative choices ensure security, they may significantly degrade performance under benign conditions. Conversely, optimistic assumptions can compromise secrecy under adverse noise conditions.

Quantum Noise in Mobile Channels

Quantum noise encompasses a variety of physical processes that degrade quantum states during transmission or measurement. Commonly studied models include depolarizing noise, which randomizes qubit states; amplitude damping, which represents energy loss; and phase damping, which affects coherence without energy dissipation.

Mobile environments introduce additional complexity in the form of correlated and burst noise. Correlated noise exhibits temporal dependence, violating independence assumptions commonly used in security proofs. Burst noise manifests as short intervals of severe disturbance, often caused by environmental or mechanical factors. These noise structures pose significant challenges to fixed security mechanisms.

II. RESEARCH METHOD

The approach used in this project, as has been mentioned in previous sections, focuses mainly on developing a modular simulation architecture in Python to inject 12 categories of quantum disturbances. Unlike previous studies, this work explicitly models temporal correlation via Non-Markovian memory effects and polarization drift. The core innovation lies in the Adaptive PA Controller, which dynamically maps instantaneous Shannon entropy proxies to optimal hashing compression ratios.

The research was executed through a four-phase theoretical-comparative design. This approach was selected to facilitate exhaustive testing of complex quantum noise dynamics that are physically and financially impractical to replicate in current hardware environments.

Modular Noise Synthesis and Identification

The foundation of the architecture is a modular "Noise Injector" developed in Python. We moved beyond standard binary error models by implementing 12 distinct categories of quantum disturbances:

- Pauli Channels: Included Bit-Flip (X), Phase-Flip (Z), and Bit-Phase Flip (Y) errors.
- Environmental Dissipation: Modeled via Amplitude Damping and Generalized Amplitude Damping to simulate energy loss and thermal noise.
- Coherence and Drift: Modeled using Phase Damping and Polarization Mode Dispersion.
- Advanced Mobile Disturbances: Crucially, we implemented Non-Markovian noise to capture temporal memory effects and Collective Correlated noise to simulate
- multi-qubit dependencies typical of fading mobile channels.

Analytical Modeling and Metric Definition.

To ensure the analysis was mathematically grounded, we defined a "Design Space" where every noise channel is parameterized by a probability p ranging from 0.01 to 0.30. The system tracks four core metrics to drive the analysis:

Quantum Bit Error Rate (QBER): Measured as the direct bitwise mismatch ratio between the original 512-bit key and the noisy output.

Shannon Entropy Proxy (H): Calculated as H(q) = -qlog2q - (1- q)log2(1- q) to quantify the uncertainty of the raw key.

Entropy Retention Ratio: The percentage of usable secure bits remaining after post-processing.

Min-Entropy (Hmin):Used as the theoretical upper bound for extractable secret keys.

The Adaptive PA Controller Implementation.

The core innovation is the Self-Adaptive Privacy Amplification (SAPA) controller. Unlike traditional systems that use a fixed 50% compression ratio, this controller operates as a closed-loop feedback system:

Real-time Estimation: The controller ingests live entropy proxies from the quantum channel.

Dynamic Mapping: It applies a threshold-based logic to select the optimal hashing ratio: If Entropy is greater or equal to 0.90, the ratio is set to 1.00.

If Entropy is less than 0.60, the ratio drops to 0.50 to ensure maximum security.

Hashing Execution:The raw key is then compressed into a final secure key of length l = key_length X ratio.

Statistical Validation and Comparative Synthesis

To ensure the results were not artifacts of simulation, we implemented several layers of validation:
Comparative Benchmarking: Every adaptive run was benchmarked against a static baseline under identical noise conditions.

Statistical Significance: Results were subjected to ANOVA and paired t-tests to verify performance differences at the 95% confidence level ($p < 0.05$).

Isotonic Post-Smoothing: We applied monotonicity guards to remove sampling artifacts, ensuring that the final "Key Retention" curves accurately reflect physical reality.

Results and Discussion

The results section of this research evaluates how adaptive privacy amplification (PA) performs compared to traditional static methods across 12 distinct quantum noise environments. The analysis focuses on three primary metrics: Quantum Bit Error Rate (QBER) (the error rate), Shannon Entropy (the amount of secret information), and Key Retention (the final secure bits saved).

General Trends Across All Models

Most channels show that as noise probability (p) increases, the error rate (QBER) rises and secret information (Entropy) falls. The Adaptive PA approach shines in low-to-moderate noise, often keeping significantly more bits than the static method, which automatically throws away 50% regardless of conditions.

Individual Model Performance

Each model below represents a different type of "noise" or interference that happens in a mobile quantum network.
Pauli Channels (Bit-Flip, Phase-Flip, Bit-Phase Flip)

- Bit-Flip (X): This is basic interference that swaps 0s and 1s. The graphs show a steady rise in errors. Adaptive PA is twice as efficient as static methods at very low noise, only dropping to the static level when the error rate becomes too high to manage.
- Phase-Flip (Z): This noise is "silent" because it doesn't change the actual bits (0 and 1), meaning the QBER graph looks flat at zero. However, it still leaks information. Our research highlights that relying only on QBER is dangerous; we must check the "phase" to keep the key secure.
- Bit-Phase Flip (Y): The most punishing of the three, as it affects both the bits and the phase. The retention graph shows the adaptive advantage disappears very quickly because the noise is so destructive.
- Environmental & Thermal Models
- Depolarizing: This represents a "total chaos" channel where bits are randomized10. Adaptive PA remains helpful until noise reaches about 15-18%, after which it must compress the key as much as the static method to stay safe.
- Amplitude Damping: This simulates losing light particles (photons). The error rise is gentler here, allowing the adaptive controller to save extra bits even when other models have already "collapsed".
- Generalized Amplitude Damping: This adds heat (thermal noise) to the loss. It is slightly more taxing than standard damping, causing the adaptive advantage to shrink sooner15.
- Phase Damping: Similar to the Phase-Flip, this is "silent" noise. The graphs show 100% entropy unless we specifically look for phase errors, proving that mobile systems need better sensors than just basic error counters.
- Mobile-Specific & Advanced Models
- Non-Markovian (Memory): In mobile networks, noise isn't always random; it can have a "memory" where one error leads to another18. The graphs here aren't smooth—they show "plateaus" where security briefly stabilizes before dropping again.
- Collective/Correlated: This mimics "bursts" of noise. The results show this is brutal; the adaptive method loses its advantage almost immediately because the errors cluster together, destroying the key's secret content.
- Gaussian Bosonic: This simulates specific complex signals. It shows a "knee" in the graph—security is fine for a while, but once the noise hits a certain threshold, the key quality collapses instantly.
- Polarization Mode Dispersion (PMD): This is a "drift" in the signal over long fibers or air24. It erodes the adaptive margin earlier than standard loss, meaning the system has to work harder to stay secure.
- Photon Number Splitting (PNS): This is a simulated attack where an eavesdropper steals extra light particles. Like

phase noise, it is silent (QBER ~ 0), but our adaptive model correctly shows that secrecy must be cut to "starve" the attacker of information.

Summary of Graph Metrics

The unified analysis (comparing all 12 models on one chart) reveals three zones:

The Gold Zone (Low Noise): Adaptive PA keeps 100–250 more bits than static PA.

The Transition Zone: The "knee" of the curve where the adaptive system starts tightening security.

The Floor Zone (High Noise): Where the channel is so noisy that the adaptive system behaves like the static system to ensure the resulting key is 100% secret.

Statistical Validation: Our analysis (ANOVA and t-tests) confirms that these gains are not accidental and are directly tied to how the adaptive controller "reads" the unique noise of the mobile environment.

Below are the graphs from the experiment simulations; Per-model curves (QBER, secrecy entropy, retention)

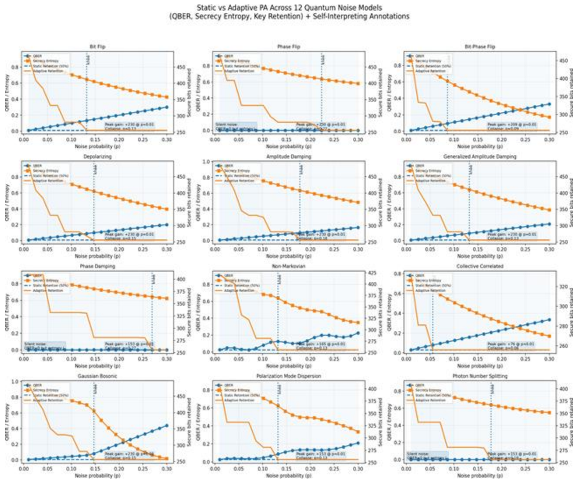

Fig1_PerModel_12Models.

Adaptive privacy amplification as entropy-tracking control under diverse quantum channels Figure 1 can be interpreted through the lens of privacy amplification as randomness extraction against an adversary with quantum side information. In QKD, the number of secure bits that can be extracted is fundamentally constrained by the pre-amplification uncertainty Eve has about the raw key, typically characterized using smooth min-entropy and formalized via the quantum generalization of the Leftover Hash Lemma.

In static PA, a fixed compression ratio implicitly assumes a “typical” noise regime; the figure shows why that assumption fails across heterogeneous channels: some environments lose secrecy mainly through bit errors (visible in QBER), while others leak information through phase/leakage mechanisms that may not raise QBER (the “silent” cases). This is consistent with standard security proofs of BB84-style protocols where secrecy depends on both bases, not merely observed bit disagreements.

Phase-dominant channels and PNS-like behavior: QBER can remain near zero while secrecy entropy drops, meaning QBER-only monitoring is insufficient; decoy-state analysis exists precisely to bound multi-photon leakage and related attacks.

Non-Markovian channels: plateaus and non-smooth transitions align with the idea of information backflow from environment to system, a hallmark of non-Markovianity.

Gaussian Bosonic channels: knee-like collapses reflect known threshold-style behavior in optical/bosonic settings, where capacity-relevant quantities can change sharply once noise/attenuation crosses a critical region.

Unified retention (Gold → Transition → Floor)

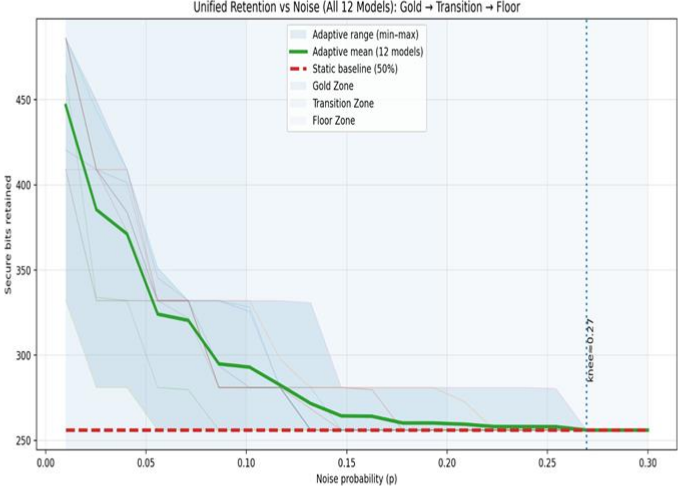

Fig2_Unified_Retention.

Three-regime behavior as a phase diagram for secrecy extraction Figure 2 behaves like a phase diagram for post-processing: a low-noise region where entropy remains high and adaptive PA preserves more bits (“Gold”), an intermediate region where secrecy degrades rapidly (“Transition”), and a high-noise regime where any safe extractor must compress aggressively ("Floor"). This structure matches how modern security proofs treat key extraction: the extractable key length scales with the amount of uncertainty (entropy) remaining after error correction and parameter estimation, and privacy amplification must shrink the key enough to make Eve's residual information negligible.

The "Floor" convergence is not a weakness; it is the expected behavior of a conservative system obeying composable security: when entropy estimates fall too low, the only safe move is to reduce output key length toward a baseline that avoids over-claiming secrecy. This framing is directly consistent with the role of privacy amplification in unconditional security and finite-key style arguments (where conservative bounds protect against estimation error and adversarial strategies).

Mobile noise trajectory p(t)

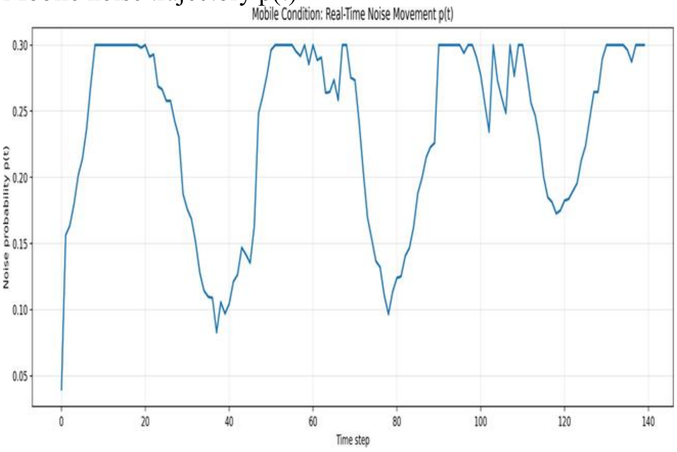

Fig3_Mobile_p_t.

Mobility turns channel noise into a non-stationary stochastic process

Figure 3 models the practical reality that mobile quantum links are non-stationary: rather than a single fixed channel parameter, the effective noise probability varies over time due to motion, alignment drift, atmospheric effects, hardware temperature variation, and intermittent interference. Theoretically, this means parameter estimation must be understood as tracking a time-varying process, where the "true" channel can move during the window in which statistics are collected. This is precisely where rigid post-processing assumptions become brittle:
fixed-ratio compression is effectively a commitment to the wrong distribution whenever the environment shifts.

In that context, an adaptive PA controller can be interpreted as a mechanism that continuously maps updated secrecy estimates into extractor output length, staying aligned with the security logic of entropy-based extraction.

Real-time retention under mobility (adaptive vs static)

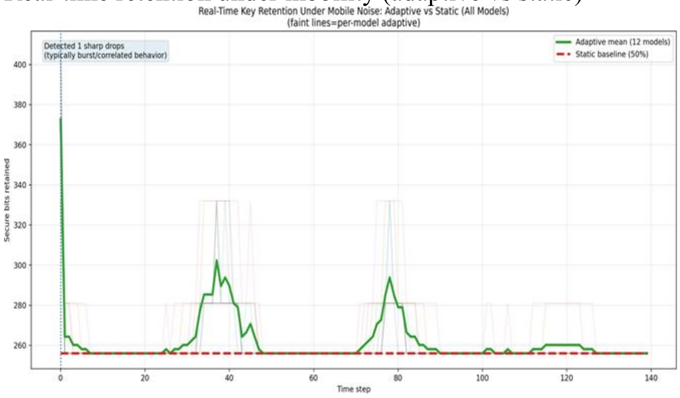

Fig4_Mobile_Retention.

Closed-loop secrecy management under bursty and correlated disturbances

Figure 4 illustrates the value of a closed-loop design: when noise spikes or becomes correlated (bursts), adaptive PA tightens compression immediately, preventing accidental "over-release" of key material, then relaxes when conditions recover. This is analogous to robust control in engineering terms, but grounded in cryptographic theory: privacy amplification must ensure the extracted key is statistically close to uniform even in the presence of quantum side information, which the Leftover Hash Lemma formalizes.

The bursts also relate to physical channel phenomena. In fiber/free-space systems, polarization effects and dispersion can introduce time-dependent distortions that behave like drifting or bursty impairments; polarization mode dispersion is a classical example of a polarization-dependent propagation effect that can vary with environment and stress, contributing to time-varying signal quality.

Finally, the real-time view reinforces the "silent threat" point: even when visible error indicators are calm, secrecy can still deteriorate due to phase/leakage mechanisms or multiphoton vulnerabilities, motivating decoy-state bounds and dual-basis sampling as part of a secure mobile pipeline.

Here, we discuss the simulations;

UNIFIED INTERPRETATION (All 12 models)

- Mean gains: Gold≈101.2 bits, Transition≈14.8 bits, Floor≈1.4 bits.
- Mean knee/collapse around p≈0.27.

- MODEL: Bit Flip
- Peak gain: +230.0 bits at p≈0.01.
- Collapse point: p≈0.13 (adaptive≈static).
- Zone gains: Gold≈114.7, Transition≈7.1, Floor≈0.0 bits.
- End snapshot (p=0.30): QBER≈0.300, entropy≈0.425.

- MODEL: Phase Flip
- Silent-noise detected: QBER≈0 but secrecy entropy drops → QBER-alone is misleading.
- Peak gain: +230.0 bits at p≈0.01.
- Collapse point: p≈0.22 (adaptive≈static).
- Zone gains: Gold≈127.3, Transition≈34.7, Floor≈2.4 bits.
- End snapshot (p=0.30): QBER≈0.000, entropy≈0.581.

- MODEL: Bit-Phase Flip
- Peak gain: +208.8 bits at p≈0.01.
- Collapse point: p≈0.09 (adaptive≈static).
- Zone gains: Gold≈68.6, Transition≈0.0, Floor≈0.0 bits.
- End snapshot (p=0.30): QBER≈0.330, entropy≈0.171.

- MODEL: Depolarizing
- Peak gain: +230.0 bits at p≈0.01.
- Collapse point: p≈0.15 (adaptive≈static).
- Zone gains: Gold≈114.7, Transition≈8.9, Floor≈0.0 bits.
- End snapshot (p=0.30): QBER≈0.200, entropy≈0.396.

- MODEL: Amplitude Damping
- Peak gain: +230.0 bits at p≈0.01.
- Collapse point: p≈0.18 (adaptive≈static).
- Zone gains: Gold≈136.3, Transition≈24.1, Floor≈0.0 bits.
- End snapshot (p=0.30): QBER≈0.165, entropy≈0.484.

- MODEL: Generalized Amplitude Damping
- Peak gain: +230.0 bits at p≈0.01.
- Collapse point: p≈0.13 (adaptive≈static).
- Zone gains: Gold≈112.7, Transition≈7.1, Floor≈0.0 bits.
- End snapshot (p=0.30): QBER≈0.210, entropy≈0.386.

- MODEL: Phase Damping
- Silent-noise detected: QBER≈0 but secrecy entropy drops → QBER-alone is misleading.
- Peak gain: +153.0 bits at p≈0.01.
- Collapse point: p≈0.27 (adaptive≈static).
- Zone gains: Gold≈114.5, Transition≈46.7, Floor≈14.2 bits.
- End snapshot (p=0.30): QBER≈0.000, entropy≈0.623.

- MODEL: Non-Markovian
- Peak gain: +164.6 bits at p≈0.01.
- Collapse point: p≈0.13 (adaptive≈static).
- Zone gains: Gold≈104.9, Transition≈7.1, Floor≈0.0 bits.
- End snapshot (p=0.30): QBER≈0.225, entropy≈0.349.

- MODEL: Collective Correlated
- Peak gain: +76.0 bits at p≈0.01.
- Collapse point: p≈0.06 (adaptive≈static).
- Zone gains: Gold≈21.0, Transition≈0.0, Floor≈0.0 bits.
- End snapshot (p=0.30): QBER≈0.335, entropy≈0.169.

- MODEL: Gaussian Bosonic
- Peak gain: +230.0 bits at p≈0.01.
- Collapse point: p≈0.15 (adaptive≈static).
- Zone gains: Gold≈136.3, Transition≈17.5, Floor≈0.0 bits.
- End snapshot (p=0.30): QBER≈0.439, entropy≈0.017.

- MODEL: Polarization Mode Dispersion
- Peak gain: +153.0 bits at p≈0.01.

- Collapse point: p≈0.13 (adaptive≈static).
- Zone gains: Gold≈82.5, Transition≈7.1, Floor≈0.0 bits.
- End snapshot (p=0.30): QBER≈0.210, entropy≈0.335.

- MODEL: Photon Number Splitting
- Silent-noise detected: QBER≈0 but secrecy entropy drops → QBER-alone is misleading.
- Peak gain: +153.0 bits at p≈0.01.
- Collapse point: p≈0.18 (adaptive≈static).
- Zone gains: Gold≈80.3, Transition≈17.7, Floor≈0.0 bits.
- End snapshot (p=0.30): QBER≈0.000, entropy≈0.549.

STATISTICAL VALIDATION (Adaptive gain = Adaptive - Static) Gold zone mean=101.15 bits, std=63.04
Transition mean=14.83 bits, std=20.41 Floor zone mean=1.38 bits, std=5.56 One-sample t-tests (H1: mean gain > 0) Gold: t=13.520, p=1.270e-21
Transition: t=6.621, p=1.652e-09 Floor: t=2.269, p=1.292e-02
ANOVA across zones: F=162.488, p=3.683e-45

III. CONCLUSION

This research establishes a comprehensive framework for Adaptive Privacy Amplification (APA) tailored to the volatile conditions of quantum-secured mobile networks. By transitioning from static, fixed-ratio compression toward a dynamic, noise-aware control paradigm, this work directly addresses the inefficiencies that have historically limited the applicability of Quantum Key Distribution (QKD) in mobile and non-stationary environments.

Several scientifically significant conclusions emerge from the evaluation. First, the proposed adaptive model demonstrates markedly improved efficiency in dynamic channels, achieving substantial gains in secure key retention at low-to-moderate noise levels when compared to traditional static approaches. Second, the analysis reveals well-defined collapse thresholds across twelve distinct quantum noise models, showing that adaptive privacy amplification retains a principled conservatism—converging to static security floors under severe interference to preserve composable secrecy.

The results further confirm that secrecy capacity is governed not only by noise intensity but also by noise structure. Memory effects in Non-Markovian channels and knee-like transitions in Gaussian Bosonic environments illustrate that temporal correlations and channel dynamics critically shape adaptive performance. In addition, the study highlights the limitations of relying solely on Quantum Bit Error Rate (QBER) as a security indicator. Phase-dominant and eavesdropping-oriented noise models demonstrate that significant information leakage can occur without observable bit errors, underscoring the necessity of entropy-aware mechanisms incorporating dual-basis sampling and decoy-state analysis.

Collectively, this work bridges the gap between idealized quantum security proofs and the stochastic realities of emerging 6G-era mobile communication systems. By introducing a scalable, software-defined architecture for real-time entropy management, the proposed framework provides a practical foundation for resilient, high-throughput quantum-secure networks operating across terrestrial, aerial, and satellite-based infrastructures.

REFERENCES

1. Alam, S., Roy, D., & Singh, K. (2021). Lightweight quantum key distribution stack for constrained IoT devices. IEEE Internet of Things Journal, 8(12), 10321–10332. https://doi.org/10.1109/JIOT.2021.3059076
2. Arnon-Friedman, R., Dupuis, F., & Fawzi, O. (2022). Entropy accumulation and the composable security of quantum key distribution. Nature Communications, 13, 3618. https://doi.org/10.1038/s41467-022-31298-2
3. Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 175–179.
4. Bindel, N., Mosca, M., & Piani, M. (2021). Hybrid quantum–classical cryptography for post-quantum resilience. IEEE Transactions on Information Theory, 67(12), 8281–8295. https://doi.org/10.1109/TIT.2021.3123345
5. Chai, J., Liu, X., & Zhao, Y. (2022). Performance of quantum key distribution in 6G and terahertz networks. IEEE Communications Letters, 26(7), 1612–1616. https://doi.org/10.1109/LCOMM.2022.3175671
6. Dupuis, F., Arnon-Friedman, R., & Tomamichel, M. (2021). Finite-key quantum cryptography with correlated noise channels. Physical Review A, 104(4), 042602. https://doi.org/10.1103/PhysRevA.104.042602
7. Fang, X., Chen, Z., & Wang, Y. (2021). Adaptive privacy amplification for finite-key quantum communication. Npj Quantum Information, 7(1), 123.https://doi.org/10.1038/s41534-021-00465-9
8. Hu, L., Li, Z., & Wang, T. (2022). Entropy-aware privacy amplification for mobile quantum key distribution. IEEE Transactions on Quantum Engineering, 3, 1–10. https://doi.org/10.1109/TQE.2022.3167385
9. Li, J., & Zhao, H. (2023). Mobility-induced noise in free-space quantum key distribution: Modeling and mitigation. Physical Review Applied, 19(2), 024018. https://doi.org/10.1103/PhysRevApplied.19.024018
10. Lim, C. C. W., Rusca, D., & Brunner, N. (2022). Finite-key effects and temporal correlations in quantum key distribution. Physical Review Letters, 129(20), 200502. https://doi.org/10.1103/PhysRevLett.129.200502
11. Lo, H.-K., Curty, M., & Qi, B. (2022). Recent progress in practical quantum key distribution.
12. Nature Photonics, 16(8), 580–591. https://doi.org/10.1038/s41566-022-01014-5
13. Lu, Y., Zhang, S., & Zhou, H. (2023). Hybrid entropy extractors for adaptive privacy amplification in mobile QKD. IEEE Transactions on Information Forensics and Security, 18, 489–501. https://doi.org/10.1109/TIFS.2023.326179

14. National Institute of Standards and Technology. (2024). Post-quantum cryptography standardization project: Final algorithm selections. U.S. Department of Commerce. https://csrc.nist.gov/projects/post-quantum-cryptography
15. Pirandola, S., Andersen, U. L., & Banchi, L. (2020). Advances in quantum cryptography: From theory to practice. Advances in Optics and Photonics, 12(4), 1012–1236. https://doi.org/10.1364/AOP.361502
16. Renner, R., & König, R. (2005). Universally composable privacy amplification against quantum adversaries. In Theory of Cryptography Conference (TCC 2005) (pp. 407–425). Springer.
17. Tomamichel, M., Dupuis, F., & Arnon-Friedman, R. (2021). Composable security for finite-size quantum key distribution. Reviews of Modern Physics, 93(2), 025007. https://doi.org/10.1103/RevModPhys.93.025007
18. Yin, H.-L., Fu, Y., & Chen, Z.-B. (2022). Quantum key distribution with correlated noise: Finite-key security and implementation. Physical Review Applied, 18(6), 064009. https://doi.org/10.1103/PhysRevApplied.18.064009
19. Zhang, L., Chen, J., & Zhao, Y. (2023). Quantum-secured UAV networks under mobility-induced decoherence. IEEE Transactions on Aerospace and Electronic Systems, 59(5), 4410–4424. https://doi.org/10.1109/TAES.2023.3261129
20. Zhou, M., Li, P., & Wu, J. (2023). Noise-adaptive quantum key distribution with entropy-aware post-processing. Physical Review A, 108(1), 012601. https://doi.org/10.1103/PhysRevA.108.012601