Digital Innovations & Contemporary Research in SCIENCE, ENGINEERING & TECHNOLOGY
Vol. 14. No. 1, March 2026 Series

Article Citation Format
Ojeniyi, J.A., Fasola, O.O., Onyeabor, G.A., Agbu, E.A., Isah, S.B. & Muhammad, S.N. (2026): Finite-Length Analysis of Operational Perfect Secrecy and Key-Length Trade-Offs: A Systematic Review of Security Implications and Risk Analysis. Journal of Digital Innovations & Contemporary Research in Science, Engineering & Technology. Vol. 14, No. 1. Pp 81-96. www.isteams.net/digitaljournal. dx.doi.org/10.22624/AIMS/DIGITAL/V14N1P7

Article Progress Time Stamps
Article Type: Research Article
Manuscript Received: 12th January, 2026
Review Type: Blind Peer
Final Acceptance: 23rd March, 2026

Finite-Length Analysis of Operational Perfect Secrecy and Key-Length Trade-Offs: A Systematic Review of Security Implications and Risk Analysis

[1]Ojeniyi, J.A., [1]Fasola, O.O., [2]Onyeabor, G.A., [1]Agbu, E.A., [1]Isah, S.B. & [1]Muhammad, S.N.
[1]Department of Cyber Security Science, Federal University of Technology, Minna, Nigeria.
[2]Department of Data Science, Federal University of Technology, Minna, Nigeria.
E-mails: ojeniyija@futminna.edu.ng, Sanjo.fasola@futminna.edu.ng, grace.onyeabor@gmail.com, agbuenoch38@gmail.com, ibsbandi01@gmail.com, muhammedshuaibu03@gmail.com
Corresponding author: ojeniyija@futminna.edu.ng

ABSTRACT

Classical formulations of perfect secrecy rely on asymptotic assumptions that are incompatible with modern communication systems operating under strict resource constraints, such as quantum key distribution (QKD), ultra-reliable low-latency communication (URLLC), and emerging 6G networks. These limitations motivate finite-length security analysis, where secrecy must be evaluated under constrained key sizes, finite observations, and practical system conditions. This paper presents a systematic literature review of finite-length secrecy, focusing on operational perfect secrecy and key-length trade-offs across quantum and classical domains. The review synthesizes key frameworks, including entropy- based composable security, probabilistic leakage metrics, and finite blocklength information-theoretic models, and provides an integrated perspective on the inter- play between secrecy performance, reliability, and computational complexity. The findings show that finite-length constraints introduce unavoidable information leakage, probabilistic guarantees, and diminishing returns in key-length utilization. While metrics such as average information leakage and secrecy outage probability enable practical evaluation, their lack of standardization limits comparability. The paper identifies key research gaps and outlines directions toward unified, scalable, and practically deployable secrecy frameworks.

Keywords: Finite-Length Secrecy, Operational Perfect Secrecy, Key-Length Trade-Offs, Quantum Key Distribution (QKD), Physical-Layer Security, Information-Theoretic Security, Finite Blocklength Analysis, Secrecy Outage Probability (SOP), Average Information Leakage (AIL), Composable Security, Entropy Accumulation, Secure Communication Systems.

1. INTRODUCTION

The concept of perfect secrecy has traditionally been defined under asymptotic assumptions, where infinitely long keys and large blocklengths enable the complete elimination of information leakage. While such formulations provide elegant theoretical guarantees, they are increasingly misaligned with the requirements of modern communication systems.

Emerging applications—including quantum key distribution (QKD), ultra-reliable low-latency communication (URLLC), Internet of Things (IoT), and future 6G net- works—operate under stringent constraints on latency, bandwidth, computational re- sources, and transmission opportunities. In these environments, communication is inherently finite, and classical asymptotic security guarantees are no longer applicable (Gao et al., 2026; He et al., 2021). This shift has led to the development of finite-length secrecy analysis, where security must be evaluated under realistic constraints such as limited blocklengths, finite sample sizes, and imperfect system knowledge. Unlike asymptotic regimes, finite-length settings introduce statistical fluctuations, non-negligible information leakage, and probabilistic security guarantees. As a result, secrecy can no longer be treated as a binary property but must instead be quantified using operational metrics that capture leakage, reliability, and failure probability (Mamaghani et al., 2024a,b).

Recent research has explored finite-length secrecy from multiple perspectives. In quantum cryptography, composable security frameworks and entropy-based methods have been developed to provide rigorous finite-key guarantees (Tomamichel et al., 2012; Metger and Renner, 2023; George et al., 2025; Kanitschar and Huber, 2025). These developments build on earlier foundational finite-key analyses in QKD, including measurement-device- independent and imperfect-source models (Curty et al., 2014; Mizutani et al., 2015), as well as continuous-variable formulations (Leverrier et al., 1990). More recent works further extend these analyses to diverse protocol settings, including coherent one-way and discrete-phase randomized QKD (Li et al., 2024a; Wang et al., 2023a), as well as high-dimensional and multipartite systems (Grasselli et al., 2018; Yamano et al., 2024).

In classical physical-layer security, metrics such as secrecy outage probability and average information leakage have been introduced to characterize security under short- packet transmission (He et al., 2021; Mamaghani et al., 2024a,b). Meanwhile, advances in coding theory and optimization techniques—including polar coding, linear programming approaches, and finite-length secrecy code design—have enabled more efficient utilization of limited key resources (Shoushtari and Harrison, 2023; Mahdavifar and Abbasi, 2024; Nikkhah et al., 2024; Shakiba-Herfeh et al., 2021; Bunandar et al., 2020). Despite these developments, the literature remains fragmented, with differing models, metrics, and analytical approaches across domains. A central challenge emerging from this body of work is the trade-off between key length and secrecy performance. Increasing key length or blocklength can improve security, but only up to a point, beyond which diminishing returns and system constraints dominate. Finite-length effects introduce penalties due to statistical uncertainty, privacy amplification overhead, and computational limitations, making it necessary to carefully balance secrecy, efficiency, and system performance (Cheng et al., 2025; Mannalath et al., 2025).

Motivated by these challenges, this paper presents a systematic literature review of finite-length analysis in secure communication systems, with a focus on operational perfect secrecy and key-length trade-offs. The objectives of this review are threefold:

- To synthesize existing theoretical frameworks for finite-length secrecy across quantum and classical domains;
- To analyze the metrics and methodologies used to evaluate secrecy under finite constraints;
- To identify key trade-offs, limitations, and research gaps that shape current and future developments.

Through a comprehensive synthesis of recent studies, this review provides a unified perspective on the evolving role of finite-length analysis in modern security frameworks. The findings aim to bridge the gap between theoretical models and practical implementations, offering insights that can guide the design of next-generation secure communication systems. The remainder of this paper is organized as follows. Section 2 describes the methodology adopted for the systematic literature review. Section 3 presents a detailed synthesis of finite-length secrecy foundations, theoretical models, security metrics, and key-length trade-offs. Section 4 discusses open challenges and future research directions. Finally, Section 5 concludes the paper.

1.1 Methodology

This study adopts a systematic literature review (SLR) approach to identify, evaluate, and synthesize existing research on finite-length secrecy and key-length trade-offs. The methodology follows the principles of the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA), ensuring transparency, reproducibility, and methodological rigor.

1.2 Review Protocol and Research Scope

The review is designed to address the following core research objectives:

- To analyze the impact of finite-length constraints on operational perfect secrecy;
- To investigate key-length trade-offs in both classical and quantum communication systems;
- To evaluate emerging secrecy metrics and analytical frameworks;
- To identify research gaps and future directions in finite-length security modeling.

The scope of this review spans both classical information-theoretic security and quantum cryptographic systems, with a particular focus on studies that explicitly consider finite blocklength or finite-key effects.

1.3 Search Strategy

A comprehensive literature search was conducted across multiple academic databases, including IEEE Xplore, SpringerLink, ScienceDirect (Elsevier), and arXiv. The search was limited to publications between 2023 and 2025 to ensure relevance to current ad- vancements in finite-length security.

The following keywords and search strings were used:
“finite blocklength secrecy”
“finite-key quantum key distribution”
“information leakage finite length”
“physical layer security finite blocklength”
“key-length trade-off secrecy”

Boolean combinations of these terms were applied to refine search results and capture interdisciplinary contributions.

1.4 Study Selection Process

The study selection process followed a multi-stage filtering procedure inspired by PRISMA guidelines: Identification: An initial pool of studies was collected from selected databases based on keyword relevance.

- **Screening**: Titles and abstracts were reviewed to remove duplicates and clearly irrelevant studies.
- **Eligibility**: Full-text articles were assessed against inclusion and exclusion criteria.
- **Inclusion**: A final set of 39 papers was selected for detailed synthesis.

This process ensures that only high-quality and relevant studies are included in the review.

1.5 Inclusion and Exclusion Criteria

To maintain consistency and focus, the following criteria were applied:

Inclusion Criteria

- Studies addressing finite blocklength or finite-key security analysis;
- Research on quantum key distribution (QKD), wiretap channels, or physical-layer security;
- Papers proposing or evaluating secrecy metrics, entropy-based models, or optimization techniques;
- Peer-reviewed journal articles, conference papers, and high-quality preprints.

Exclusion Criteria

- Studies based solely on asymptotic or infinite-length assumptions;
- Papers not directly related to security or secrecy;
- Non-technical or purely conceptual discussions without analytical contribution.

1.6 Data Extraction and Synthesis Approach

For each selected study, key information was extracted, including:

- Research domain (e.g., QKD, wireless, coding theory);
- Methodological approach (analytical, numerical, optimization-based);
- Secrecy metrics used (e.g., leakage, outage probability);
- Key findings and limitations.

Rather than performing a paper-by-paper summary, this review adopts a thematic syn- thesis approach. Studies are grouped into conceptual categories, allowing for cross-paper comparison, identification of trends, and critical evaluation of methodological differences.

Quality Assessment

The quality of selected studies was evaluated based on:

- Theoretical rigour and clarity of assumptions;
- Relevance to finite-length secrecy;
- Methodological soundness (analytical or computational);
- Contribution to advancing secrecy metrics or system design.

This ensures that the synthesis is built upon credible and impactful research.

1.7 PRISMA Flow Representation

The study selection process can be visually summarized using a PRISMA flow diagram, illustrating the number of records identified, screened, excluded, and included at each stage. Although not

shown here, such a diagram can be incorporated to enhance transparency and reproducibility.

1.8 Thematic Synthesis

Finite-Length Secrecy Foundations

Recent advances in secure communication systems have emphasized the limitations of asymptotic secrecy models when applied to practical scenarios characterized by finite re- sources (Gao et al., 2026). In such settings, blocklength constraints, limited transmission opportunities, and computational overhead fundamentally alter the nature of achievable secrecy guarantees. As a result, secrecy must be redefined within an operational frame- work that explicitly accounts for finite-length effects. In finite blocklength regimes, secrecy can no longer be treated as an absolute property but must instead be quantified through probabilistic and information-theoretic measures. Studies such as He et al. (2021) and Mamaghani et al. (2024a) demonstrate that metrics like secrecy outage probability (SOP) and average information leakage (AIL) provide practical means of evaluating security under constrained transmission lengths. These approaches reflect a shift toward quantifying residual leakage rather than assuming its complete elimination.

In the context of quantum key distribution (QKD), finite-key analysis has further reinforced this transition. Metger and Renner (2023) and George et al. (2025) show that entropy accumulation techniques enable rigorous characterization of secrecy under finite sample sizes, while explicitly incorporating statistical fluctuations and adversarial uncertainty. Similarly, Mannalath et al. (2025) highlight that improved statistical tools can significantly reduce the minimum blocklength required to achieve a desired level of security, thereby bridging the gap between theoretical models and real-world implementations. A key implication across these studies is that information leakage becomes an inherent feature of finite-length systems (Mamaghani et al., 2024a; Metger and Renner, 2023). Unlike asymptotic regimes where leakage can be driven arbitrarily close to zero, finite- length constraints impose a non-negligible lower bound on adversarial knowledge. This observation necessitates the adoption of operational secrecy definitions, where security is evaluated based on acceptable thresholds of leakage and failure probability rather than absolute guarantees.

Furthermore, finite-length secrecy is intrinsically linked to system-level trade-offs. As shown in short-packet communication systems (He et al., 2021) and finite-key QKD implementations (George et al., 2025), reducing blocklength improves latency but increases statistical uncertainty and leakage. Conversely, increasing blocklength enhances secrecy performance at the cost of higher delay and computational complexity. This establishes secrecy as a multi-objective optimization problem, requiring careful balancing of competing system requirements. Despite these advancements, the literature remains fragmented in its treatment of finite-length secrecy. Physical-layer security studies often focus on outage-based metrics and channel models (He et al., 2021; Mamaghani et al., 2024a), while QKD research emphasizes entropy-based composable security frameworks (Metger and Renner, 2023; George et al., 2025). This divergence complicates direct comparison across domains and highlights the need for a unified theoretical framework capable of integrating these perspectives.

In summary, finite-length secrecy foundations represent a paradigm shift from idealized asymptotic models to practical, resource-constrained security formulations. The transition introduces unavoidable leakage, probabilistic guarantees, and complex system trade-offs, forming the basis for subsequent analysis of secrecy metrics and optimization strategies.

2. THEORETICAL MODELS AND ANALYTICAL FRAMEWORKS

Finite-length secrecy analysis relies on a diverse set of theoretical models that extend classical information-theoretic and cryptographic frameworks to non-asymptotic regimes. These models aim to capture the effects of limited blocklength, statistical uncertainty, and adversarial knowledge under realistic system constraints. In classical communication systems, finite blocklength information theory provides the foundational analytical framework. Building on the work of Polyanskiy et al., subsequent studies such as He et al. (2021) and Mamaghani et al. (2024a) incorporate secrecy constraints into short-packet communication models. These approaches extend traditional wiretap channel formulations by explicitly accounting for decoding error probability, channel dispersion, and finite-length penalties, enabling a more accurate characterisation of achievable secrecy rates in practical systems.

In parallel, quantum cryptography has developed rigorous finite-key security models based on composable security definitions. The framework introduced by Tomamichel et al. (2012) formalizes secrecy in terms of smooth entropy measures, allowing security guarantees to be expressed as explicit functions of key length, error rates, and failure probability. This approach has been further extended through entropy accumulation techniques, as demonstrated by Metger and Renner (2023) and George et al. (2025), which enable the analysis of sequential quantum processes and provide tight finite-key bounds for QKD protocols. Another important class of models focuses on coding-theoretic approaches to secrecy. Polar codes and related constructions have been widely studied for achieving secrecy capacity under finite-length constraints. For example, Mahdavifar and Abbasi (2024) and Shoushtari and Harrison (2023) explore the design of secure coding schemes that balance reliability and secrecy while maintaining computational efficiency. These works highlight the role of structured codes in bridging the gap between theoretical limits and implementable systems.

Optimization-based frameworks have also emerged as a key tool for analyzing finite- length secrecy. Studies such as Bunandar et al. (2020) formulate key distribution and resource allocation as optimization problems, where secrecy performance is maximized subject to constraints on key length, transmission rate, and system resources. Similarly, recent work by Popp et al. (2026) investigates adaptive strategies that dynamically adjust system parameters to maintain desired security levels under varying channel conditions. In addition to these frameworks, several recent studies have focused on improving the analytical and computational tooling available for finite-length secrecy analysis. For example, Mironowicz and Bourennane (2025) introduce a software-based framework for implementing entropy accumulation techniques, enabling more accessible evaluation of finite-key security bounds.

Similarly, Grosse et al. (2025) investigate generalized privacy amplification bounds using divergence-based methods, extending the theoretical foundations of secrecy analysis to broader classes of communication channels. These contributions highlight the growing importance of computational and software-assistedapproaches in bridging theory and practice. In addition, privacy amplification models play a critical role in both classical and quantum secrecy frameworks. The efficiency of privacy amplification directly affects the achievable secret key rate under finite-length constraints. Cheng et al. (2025) propose high-throughput privacy amplification schemes capable of handling extremely large input block sizes, demonstrating that algorithmic and architectural optimizations can significantly improve practical performance without compromising security guarantees.

Despite the diversity of these models, a common theme is the explicit incorporation of finite-length effects into secrecy analysis. Whether through entropy measures, coding theory, or optimization techniques, these frameworks converge on the need to quantify and manage the trade-offs introduced by finite resources. However, differences in assumptions, metrics, and analytical tools continue to limit interoperability across domains, underscoring the need for unified theoretical models.

2.1 Secrecy Metrics and Evaluation Criteria

A central challenge in finite-length secrecy analysis is the selection of appropriate metrics for quantifying security. Unlike asymptotic settings, where secrecy can be defined in ab- solute terms, finite-length regimes require metrics that capture probabilistic guarantees, residual leakage, and system-level trade-offs. In classical physical-layer security, secrecy outage probability (SOP) has emerged as a widely used metric. SOP measures the probability that the instantaneous secrecy capacity falls below a target threshold, reflecting the impact of channel variability and finite transmission opportunities. Studies such as He et al. (2021) demonstrate that SOP provides a practical means of evaluating security in short-packet communication systems, where reliability and latency constraints are tightly coupled with secrecy performance.

Another important metric is average information leakage (AIL), which quantifies the expected amount of information that an adversary can obtain about the transmitted message. Mamaghani et al. (2024a) and Mamaghani et al. (2024b) show that AIL offers a more granular measure of secrecy compared to outage-based metrics, as it captures the continuous nature of information leakage rather than binary success or failure events. This makes it particularly useful for analyzing trade-offs between secrecy and throughput. In quantum cryptography, secrecy is typically defined using composable security metrics based on trace distance or smooth entropy. The framework developed by Tomamichel et al. (2012) expresses secrecy as a bound on the distinguishability between the actual key and an ideal uniformly random key. This definition ensures that security guarantees remain valid even when the key is used in subsequent cryptographic applications.

Entropy accumulation techniques further refine these metrics by enabling the evaluation of secrecy over sequential processes. Metger and Renner (2023) and George et al. (2025) demonstrate that entropy accumulation provides tight finite-key bounds while ac- counting for statistical fluctuations and adversarial strategies. These methods allow for a more accurate characterization of security in realistic QKD implementations. In addition to these core metrics, recent studies have explored hybrid and application- specific evaluation criteria. For instance, Qian and Cheng (2025) consider joint reliability–security metrics that integrate error probability and information leakage into a unified framework.

Similarly, Gao et al. (2026) emphasize the importance of latency-aware secrecy metrics in next-generation communication systems, where delay constraints play a critical role. Overall, the choice of secrecy metric has a significant impact on system design and performance evaluation. While SOP and AIL are well-suited for classical communication scenarios, entropy-based metrics provide stronger guarantees in cryptographic contexts. However, the lack of standardization across these metrics complicates direct comparison between studies and highlights the need for unified evaluation frameworks.

2.2 Key-Length Trade-Offs and System Design Implications

Finite-length secrecy analysis reveals a fundamental trade-off between key length, secrecy performance, and system efficiency. Unlike asymptotic regimes, where increasing key length can arbitrarily improve security, finite systems exhibit diminishing returns due to statistical fluctuations, computational overhead, and resource constraints. Recent work has also examined finite blocklength secrecy in emerging wireless and networked systems. For instance, Li et al. (2024b) investigate blocklength allocation and power control in UAV-assisted URLLC systems using deep reinforcement learning, demonstrating the importance of adaptive resource management. Similarly, Abughalwa et al. (2025) analyze intelligent reflecting surface (IRS)-assisted systems under finite blocklength constraints, highlighting the impact of channel state information uncertainty on secrecy performance. In ultra-dense and multi-antenna networks, Wang et al. (2026) further show that finite blocklength considerations significantly influence system capacity and reliability trade-offs.

In classical communication systems, increasing blocklength generally improves secrecy by reducing the impact of channel dispersion and enabling more efficient coding schemes. However, as shown by He et al. (2021) and Mamaghani et al. (2024a), longer blocklengths also introduce higher latency and increased energy consumption, which may be unacceptable in applications such as URLLC and IoT networks. This creates a trade-off between secrecy and timeliness, requiring careful system-level optimization. In quantum key distribution, finite-key effects impose strict limits on the achievable secret key rate. Lim et al. (2021) and Liu et al. (2021) demonstrate that statistical fluctuations in parameter estimation can significantly reduce the effective key length, particularly in scenarios with limited data samples.

Similarly, Wang et al. (2023b) and Wang et al. (2023a) show that optimizing key length requires balancing error correction efficiency, privacy amplification overhead, and finite-size effects. Recent studies have also highlighted the role of advanced statistical methods in mitigating these trade-offs. Mannalath et al. (2025) and Kamin et al. (2025) propose improvedestimation techniques that reduce the penalty associated with finite sample sizes, thereby enabling shorter blocklengths without compromising security. These approaches demonstrate that algorithmic innovations can partially offset the limitations imposed by finite resources.

From a system design perspective, key-length trade-offs are closely linked to resource allocation and computational complexity. Bunandar et al. (2020) show that optimizing network parameters can significantly enhance key distribution efficiency, while Popp et al. (2026) explore adaptive strategies that dynamically adjust key length based on channel conditions and security requirements. Privacy amplification further complicates this trade-off by introducing additional processing overhead. As demonstrated by Cheng et al. (2025), achieving high throughput at large block sizes requires substantial computational resources, leading to a trade-off between performance and efficiency. This highlights the importance of hardware-aware and parallelized implementations in practical systems.
Overall, the literature indicates that key-length optimization is a multi-dimensional problem involving trade-offs between secrecy, latency, computational cost, and energy efficiency. Addressing these trade-offs requires integrated approaches that combine theoretical analysis with practical system design considerations.

3. PRACTICAL IMPLEMENTATIONS AND EMERGING APPLICATIONS

The transition from theoretical models to practical implementations of finite-length secrecy has been a major focus of recent research. Advances in hardware, algorithms, and system design have enabled the deployment of secure communication systems that operate under realistic constraints while maintaining strong security guarantees. Beyond these implementations, recent advances in QKD have explored a wide range of protocol variations and security proof techniques. For example, Staffieri et al. (2026a) analyze finite-size effects in continuous-variable QKD under Gaussian attacks, while Staffieri et al. (2026b) provide a comparative study of multiple proof techniques for finite-size security.

These works complement earlier advances in twin-field and satellite-based QKD (Yin and Chen, 2019; Sidhu et al., 2022), demonstrating the rapid evolution of finite-key methodologies across different physical platforms and protocol designs. In quantum key distribution, large-scale implementations have demonstrated the feasibility of finite-key secure communication over long distances. Yin and Chen (2019) and Sidhu et al. (2022) report significant progress in extending transmission distances and improving key generation rates, highlighting the practical viability of QKD in real-world networks. These systems incorporate finite-key analysis to ensure security under realistic operating conditions. Privacy amplification remains a critical component of practical implementations. Cheng et al. (2025) introduce a high-throughput privacy amplification scheme capable of processing input block sizes up to 1010 bits, achieving substantial improvements in secret key rate. This work demonstrates that optimized algorithms and parallel processing can overcome traditional bottlenecks in large-scale QKD systems.

Coding techniques also play a central role in practical secrecy systems. Mahdavifar and Abbasi (2024) and Shoushtari and Harrison (2023) develop efficient coding schemes that achieve strong secrecy guarantees while maintaining manageable computational complexity. These approaches are particularly relevant for resource-constrained environments such as IoT networks. Emerging applications of finite-length secrecy extend beyond traditional communication systems. In next-generation networks, including 5G and 6G, short-packet communication and low-latency requirements necessitate new security paradigms. Gao et al. (2026) and Qian and Cheng (2025) highlight the importance of integrating secrecy into system design from the outset, rather than treating it as an add-on feature.

Furthermore, satellite-based and global-scale quantum communication networks are increasingly being explored. Sidhu et al. (2022) discuss the challenges and opportunities associated with deploying QKD in space-based systems, where finite-length effects and resource constraints are particularly pronounced. Despite these advances, several challenges remain. Practical systems must balance security, scalability, and cost, while also addressing issues such as device imperfections, side-channel attacks, and integration with existing infrastructure. These challenges underscore the need for continued research into efficient, scalable, and robust finite-length secrecy solutions.

3.1 Open Challenges and Future Research Directions

Despite significant progress in finite-length secrecy analysis, the literature reveals several unresolved challenges that limit the practical deployment and theoretical unification of secure communication systems. As synthesized in Section 3, these challenges emerge from the interplay between theoretical modeling, metric selection, optimization complexity, and real-world implementation constraints. Addressing these issues is essential for advancing both classical and quantum secure communication paradigms.

3.2 Lack of Unified Theoretical Frameworks

One of the most prominent challenges is the absence of a unified framework for finite- length secrecy analysis. As discussed in Sections 3.2 and 3.3, quantum key distribution (QKD) research primarily relies on entropy-based composable security models, while clas-sical physical-layer security adopts probabilistic and information-theoretic formulations. For instance, entropy accumulation and composable security frameworks developed by Metger and Renner (2023) and George et al. (2025) provide rigorous guarantees in quan-tum settings, whereas classical approaches emphasize outage-based and leakage-based metrics as shown by He et al. (2021) and Mamaghani et al. (2024a). These fundamentally different perspectives make it difficult to directly compare results or transfer insights across domains.

Future research should therefore focus on developing integrated frameworks that unify entropy-based, probabilistic, and information-theoretic models. Such a unification would enable consistent evaluation of secrecy guarantees and facilitate cross-domain system design, particularly in emerging hybrid classical–quantum communication environments.

3.3 Inconsistency in Security Metrics

The diversity of secrecy metrics presents another major limitation. As shown in Section 3.3, metrics such as secrecy outage probability (SOP), average information leakage (AIL), entropy-based bounds, and secret key rate capture different aspects of security. For example, SOP reflects probabilistic failure events (He et al., 2021), while AIL quantifies expected leakage (Mamaghani et al., 2024a,b), and entropy-based measures provide composable worst-case guarantees (Tomamichel et al., 2012; Metger and Renner, 2023). This lack of standardization leads to inconsistent interpretations and complicates performance comparison across studies. Future work should focus on developing composite or hybrid metrics that integrate multiple dimensions of secrecy, including leakage magnitude, failure probability, and reliability. Establishing standardized benchmarking frameworks would further improve reproducibility and comparability.

3.4 Scalability of Optimization Techniques

Optimization techniques play a central role in finite-length secrecy analysis, particularly in resource allocation and key-rate maximization. However, as highlighted in Section 3.4, many existing approaches suffer from scalability limitations. For example, optimization- based frameworks proposed by Bunandar et al. (2020) and adaptive strategies explored by Popp et al. (2026) demonstrate strong performance but can become computationally expensive in large-scale or high-dimensional systems. This computational complexity poses a barrier to real-time deployment, especially in resource-constrained environments. Future research should explore scalable alternatives, including approximation methods, distributed optimization, and machine learning-driven approaches, to enable efficient exploration of the secrecy–performance trade-off space.

3.5 Limited Multi-Objective Optimization Frameworks

Another key limitation is the lack of comprehensive multi-objective optimization frame- works. As established in Sections 3.4 and 3.5, secrecy performance is inherently coupled with latency, reliability, and computational cost. Studies such as He et al. (2021) and Mamaghani et al. (2024a) demonstrate that improving secrecy often comes at the expense of delay or efficiency.

Despite this, many existing works optimize a single metric in isolation. Future research should prioritize the development of multi-objective optimization frameworks that jointly consider these competing requirements. Techniques such as Pareto optimization and cross-layer design could provide systematic approaches for identifying optimal trade-offs in practical systems.

A persistent challenge lies in bridging the gap between theoretical models and practical implementations. As highlighted in Section 3.5, many analyses assume idealized conditions, such as independent and identically distributed (i.i.d.) processes and perfectly characterized channels. In practice, these assumptions are often violated due to device imperfections, environmental variability, and system-level constraints. Experimental studies and large-scale implementations, such as those reported by Yin and Chen (2019) and Sidhu et al. (2022), demonstrate the feasibility of finite-length secure communication but also reveal practical limitations. Future work should incorporate realistic system models, including non-i.i.d. effects, hardware imperfections, and dynamic channel conditions, alongside experimental validation.

4. ADVANCED ADVERSARIAL MODELS AND RISK INTEGRATION

Current adversarial models in finite-length secrecy analysis are often simplified, focusing on passive or static attackers. However, as finite-length regimes inherently involve residual leakage and statistical uncertainty, more sophisticated adversarial strategies must be considered. Future research should investigate adaptive and multi-stage adversarial models capable of exploiting temporal correlations and accumulated leakage. Additionally, integrating secrecy analysis with formal risk assessment frameworks would enable a more comprehensive evaluation of system vulnerabilities, aligning security guarantees with practical threat models.

4.1 Emerging Applications and Cross-Domain Integration

The rise of emerging technologies—including 5G/6G networks, Internet of Things (IoT), and large-scale quantum communication systems—introduces new challenges for finite- length secrecy. As discussed in Sections 3.4 and 3.5, these systems operate under stringent latency, scalability, and energy constraints, requiring new security paradigms. Recent studies such as Gao et al. (2026) and Qian and Cheng (2025) highlight the importance of integrating secrecy into system design from the outset. Complementing these efforts, system-level frameworks such as Samuel propose adaptive and noise-aware privacy amplification strategies tailored for heterogeneous 6G environments, emphasizing the need for cross-layer and context-aware security design. These approaches illustrate a shift toward holistic security architectures that integrate physical-layer, cryptographic, and network-level considerations.

4.2 Summary of Research Directions

In summary, advancing finite-length secrecy analysis requires addressing several inter- connected challenges, including the unification of theoretical frameworks, standardization of security metrics, scalability of optimization techniques, and alignment with real- world conditions. Addressing these issues will enable the development of robust, efficient, and deployable secure communication systems capable of meeting the demands of next- generation technologies.

5. CONCLUSION

This systematic literature review has examined the evolving landscape of finite-length secrecy analysis, with a particular focus on operational perfect secrecy and key-length trade-offs across classical and quantum secure communication systems. Building on the synthesis presented in Sections 3 and 4, this study highlights a fundamental transition from asymptotic security models toward finite-resource frameworks that more accurately reflect real-world deployment conditions. The analysis demonstrates that finite-length regimes introduce unavoidable information leakage, probabilistic security guarantees, and complex interdependencies between key length, reliability, latency, and computational resources.

As shown through metrics such as secrecy outage probability (He et al., 2021), average information leakage (Mamaghani et al., 2024a), and entropy-based bounds (Tomamichel et al., 2012; Metger and Renner, 2023), secrecy in practical systems must be evaluated through measurable and context-dependent criteria rather than absolute guarantees. A key insight from this review is that key-length optimization is inherently constrained by finite-size effects, statistical uncertainty, and processing overhead. Studies on finite-key QKD (Lim et al., 2021; Liu et al., 2021; Wang et al., 2023b) and privacy amplification (Cheng et al., 2025) demonstrate that increasing key size does not yield linear improvements in secrecy performance. Instead, optimal system design requires balancing multiple competing objectives within realistic constraints.

Furthermore, this review emphasizes the importance of risk-aware security evaluation. Residual leakage, imperfect estimation, and system-level limitations introduce vulnerabilities that are often overlooked in asymptotic analyses. Incorporating probabilistic risk models and realistic adversarial assumptions is therefore essential for achieving robust security in practice. Despite significant progress, the literature remains fragmented, with diverse theoretical frameworks, metrics, and optimization strategies across domains.

As discussed in Section 4, addressing this fragmentation requires the development of unified models, standardized evaluation criteria, scalable optimization techniques, and closer integration between theory and implementation.In conclusion, finite-length secrecy analysis represents a critical step toward bridging the gap between theoretical security guarantees and practical deployment. By synthesizing current methodologies, trade-offs, and open challenges, this review provides a com- prehensive foundation for future research. Advancing this field will depend on the ability to develop unified, scalable, and multi-objective frameworks capable of supporting the security requirements of emerging technologies such as 6G networks, Internet of Things (IoT), and global quantum communication infrastructures.

REFERENCES

1. Monir Abughalwa, Diep N. Nguyen, Dinh Thai Hoang, Van-Dinh Nguyen, Ming Zeng, Quoc-Viet Pham, and Eryk Dutkiewicz. ”security for everyone” in finite blocklength irs-aided systems with perfect and imperfect csi. arXiv, 8 2025. URL http://arxiv. org/abs/2504.05067.
2. Darius Bunandar, Luke C.G. Govia, Hari Krovi, and Dirk Englund. Numerical finite-key analysis of quantum key distribution. npj Quantum Information, 6, 12 2020. ISSN 20566387. doi: 10.1038/s41534-020-00322-w.
3. Xi Cheng, Haokun Mao, Hongwei Xu, and Qiong Li. An efficient large-scale privacy amplification scheme exceeding 10g bits for quantum key distribution. EPJ Quantum Technology, 12, 12 2025. ISSN 21960763. doi: 10.1140/epjqt/s40507-025-00433-3.
4. Marcos Curty, Feihu Xu, Wei Cui, Charles Ci Wen Lim, Kiyoshi Tamaki, and Hoi Kwong Lo. Finite-key analysis for measurement-device-independent quantum key distribution. Nature Communications, 5, 4 2014. ISSN 20411723. doi: 10.1038/ncomms4732.
5. Junyuan Gao, Shuao Chen, Yongpeng Wu, Liang Liu, Giuseppe Caire, H. Vincent Poor, and Wenjun Zhang. Finite-blocklength information theory. Fundamental Research, 8:20–27, 2 2026. ISSN 26673258. doi: 10.1016/j.fmre.2025.12.032. URL https://
6. linkinghub.elsevier.com/retrieve/pii/S266732582600035X.
7. Ian George, Jie Lin, Thomas van Himbeeck, Kun Fang, and Norbert Lu¨tkenhaus. Finite- key analysis of quantum key distribution with characterized devices using entropy accumulation. Quantum, 9, 2025. ISSN 2521327X. doi: 10.22331/q-2025-12-12-1941.
8. Federico Grasselli, Hermann Kampermann, and Dagmar Bruß. Finite-key effects in multipartite quantum key distribution protocols. New Journal of Physics, 20, 11 2018. ISSN 13672630. doi: 10.1088/1367-2630/aaec34.
9. Leonhard Grosse, Sara Saeidian, Tobias J. Oechtering, and Mikael Skoglund. Bounds on the privacy amplification of arbitrary channels via the contraction of f-divergence. arXiv, 11 2025. URL http://arxiv.org/abs/2501.11473.
10. Jianhua He, Guangheng Zhao, Lu Wang, Xue Sun, and Lei Yang. Secrecy analysis of short-packet transmissions in ultra-reliable and low-latency communications. Eurasip Journal on Wireless Communications and Networking, 2021, 12 2021. ISSN 16871499. doi: 10.1186/s13638-020-01862-7.
11. Lars Kamin, Amir Arqand, Ian George, Norbert Lu¨tkenhaus, and Ernest Y.Z. Tan. Finite-size analysis of prepare-and-measure and decoy-state quantum key distribu- tion via entropy accumulation. PRX Quantum, 6, 4 2025. ISSN 26913399. doi: 10.1103/PRXQuantum.6.020342.
12. Florian Kanitschar and Marcus Huber. Composable finite-size security of high- dimensional quantum-key-distribution protocols. Physical Review Applied, 24, 11 2025. ISSN 23317019. doi: 10.1103/v51y-vkfr.
13. Anthony Leverrier, Fr´ed´eric Grosshans, and Philippe Grangier. Finite-size analysis of a continuous-variable quantum key distribution. Physical Review A, 81:62343, 1990. doi: 10.1103/PhysRevA.81.062343. URL https://iogs.hal.science/hal-00553554v1.

14. Ming Yang Li, Xiao Yu Cao, Yuan Mei Xie, Hua Lei Yin, and Zeng Bing Chen. Finite-key analysis for coherent one-way quantum key distribution. Physical Review Research, 6, 1 2024a. ISSN 26431564. doi: 10.1103/PhysRevResearch.6.013022.
15. Xinmin Li, Xuhao Zhang, Jiahui Li, Feiying Luo, Yi Huang, and Xiaoqiang Zhang. Block- length allocation and power control in uav-assisted urllc system via multi-agent deep reinforcement learning. International Journal of Computational Intelligence Systems, 17, 12 2024b. ISSN 18756883. doi: 10.1007/s44196-024-00530-8.
16. Charles Ci Wen Lim, Feihu Xu, Jian Wei Pan, and Artur Ekert. Security analysis of quantum key distribution with small block length and its application to quantum space communications. Physical Review Letters, 126, 3 2021. ISSN 10797114. doi: 10.1103/ PhysRevLett.126.100501.
17. Hang Liu, Zhen Qiang Yin, Rong Wang, Ze Hao Wang, Shuang Wang, Wei Chen, Guang Can Guo, and Zheng Fu Han. Tight finite-key analysis for quantum key distri- bution without monitoring signal disturbance. npj Quantum Information, 7, 12 2021. ISSN 20566387. doi: 10.1038/s41534-021-00428-9.
18. Hessam Mahdavifar and Fariba Abbasi. Finite-length analysis of polar secrecy codes for wiretap channels. In 2024 IEEE International Symposium on Information Theory (ISIT), pages 2951–2956. IEEE, 7 2024. ISBN 979-8-3503-8284-6. doi: 10.1109/ISIT57864.2024.10619177. URL https://www.emergentmind.com/papers/ 2407.01401.
19. Milad Tatar Mamaghani, Xiangyun Zhou, Nan Yang, A. Lee Swindlehurst, and H. Vin- cent Poor. On the information leakage performance of secure finite blocklength trans- missions over rayleigh fading channels. 2024 IEEE International Conference on Com- munications (ICC 2024), 1 2024a. URL http://arxiv.org/abs/2401.11219.
20. Milad Tatar Mamaghani, Xiangyun Zhou, Nan Yang, A. Lee Swindlehurst, and H. Vin- cent Poor. Performance analysis of finite blocklength transmissions over wiretap fading channels: An average information leakage perspective. IEEE Transactions on Wireless Communications, 23:13252–13266, 10 2024b. ISSN 1536-1276. doi: 10.1109/TWC.
21. 2024.3400601. URL https://ieeexplore.ieee.org/document/10536045/.
22. Vaisakh Mannalath, V´ıctor Zapatero, and Marcos Curty. Sharp finite statistics for quan- tum key distribution. Physical Review Letters, 135, 7 2025. ISSN 10797114. doi: 10.1103/l735-x48g.
23. Tony Metger and Renato Renner. Security of quantum key distribution from generalised entropy accumulation. Nature Communications, 14, 12 2023. ISSN 20411723. doi: 10.1038/s41467-023-40920-8.
24. Piotr Mironowicz and Mohamed Bourennane. Finite-size security analysis for quantum protocols: A python framework using the entropy accumulation theorem with graphical interface. arXiv, 6 2025. URL http://arxiv.org/abs/2506.18888.
25. Akihiro Mizutani, Marcos Curty, Charles Ci Wen Lim, Nobuyuki Imoto, and Kiyoshi Tamaki. Finite-key security analysis of quantum key distribution with imperfect light sources. New Journal of Physics, 17, 9 2015. ISSN 13672630. doi: 10.1088/1367-2630/ 17/9/093011.

26. Ali Nikkhah, Morteza Shoushtari, Bahareh Akhbari, and Willie K. Harrison. Secrecy coding for the binary symmetric wiretap channel via linear programming. arXiv, 1 2024. URL http://arxiv.org/abs/2401.07141.
27. Christopher Popp, Tobias C. Sutter, and Beatrix C. Hiesmayr. Computation of the smooth max-mutual information via semidefinite programming. Quantum Information Processing, 25, 3 2026. ISSN 15731332. doi: 10.1007/s11128-026-05101-8.
28. Shen Qian and Meng Cheng. Physical layer security in lossy untrusted relay networks with finite blocklength. Communications & Networks Connect, 1:1, 3 2025. doi: 10. 69709/coconnect.2024.003818.
29. Okai Tettey-Antie Samuel. Beyond static secrecy: A self-adaptive, noise-aware privacy amplification framework for heterogeneous 6g quantum-secured networks. Technical report.
30. Mahdi Shakiba-Herfeh, Laura Luzzi, and Arsenia Chorti. Finite blocklength secrecy analysis of polar and reed-muller codes in bec semi-deterministic wiretap channels. arXiv, 5 2021. URL http://arxiv.org/abs/2105.10747.
31. Morteza Shoushtari and Willie Harrison. Optimizing finite-blocklength nested linear secrecy codes: Using the worst code to find the best code. Entropy, 25, 10 2023. ISSN 10994300. doi: 10.3390/e25101456.
32. Jasminder S. Sidhu, Thomas Brougham, Duncan McArthur, Roberto G. Pousa, and Daniel K.L. Oi. Finite key effects in satellite quantum key distribution. npj Quantum Information, 8, 12 2022. ISSN 20566387. doi: 10.1038/s41534-022-00525-3.
33. Gabriele Staffieri, Giovanni Scala, and Cosmo Lupo. Finite-size secret-key rates of dis- crete modulation continuous-variable quantum key distribution under gaussian attacks. Physical Review A, 113:022445, 2 2026a. ISSN 2469-9926. doi: 10.1103/rwq3-p1m6. URL https://link.aps.org/doi/10.1103/rwq3-p1m6.
34. Gabriele Staffieri, Giovanni Scala, and Cosmo Lupo. Finite-size security of qkd: compar- ison of three proof techniques. arXiv, 1 2026b. URL http://arxiv.org/abs/2601. 03829.
35. Marco Tomamichel, Charles Ci Wen Lim, Nicolas Gisin, and Renato Renner. Tight finite-key analysis for quantum cryptography. Nature Communications, 3, 2012. ISSN 20411723. doi: 10.1038/ncomms1631.
36. Haoming Wang, Zhenzhen Zhang, Xinhao Wu, and Bing Li. Multiantenna noma with finite blocklength: A pragmatic paradigm for ultra-dense networking. Entropy, 28:
37. 281, 3 2026. ISSN 1099-4300. doi: 10.3390/e28030281. URL https://www.mdpi.com/
38. 1099-4300/28/3/281.
39. Rui Qiang Wang, Zhen Qiang Yin, Xiao Hang Jin, Rong Wang, Shuang Wang, Wei Chen, Guang Can Guo, and Zheng Fu Han. Finite-key analysis for quantum key distribution with discrete-phase randomization. Entropy, 25, 2 2023a. ISSN 10994300. doi: 10.3390/e25020258.
40. Ze Hao Wang, Rong Wang, Zhen Qiang Yin, Shuang Wang, Feng Yu Lu, Wei Chen, De Yong He, Guang Can Guo, and Zheng Fu Han. Tight finite-key analysis for mode-pairing quantum key distribution. Communications Physics, 6, 12 2023b. ISSN 23993650. doi: 10.1038/s42005-023-01382-y.

41. Shinichiro Yamano, Takaya Matsuura, Yui Kuramochi, Toshihiko Sasaki, and Masato Koashi. Finite-size security proof of binary-modulation continuous-variable quantum key distribution using only heterodyne measurement. Physica Scripta, 99, 2 2024. ISSN 14024896. doi: 10.1088/1402-4896/ad1022.
42. Hua Lei Yin and Zeng Bing Chen. Finite-key analysis for twin-field quantum key distri- bution with composable security. Scientific Reports, 9, 12 2019. ISSN 20452322. doi: 10.1038/s41598-019-53435-4.