Nonlinear Science and Intelligent Applications
https://www.acadlore.com/journals/NSIA

Computational Complexity and Physical Security: A Simulation-Based Comparative Analysis of Rivest-Shamir-Adleman and the BB84 Protocol

Cem Özkurt[1*], Emir Ayçiçek[2], Ahmet Kutay Küçükler[2], Elif Aydın[2], Nihle Nur Bozkurt[2]

[1] Artificial Intelligence and Data Science Application and Research Center (YAZEM), Sakarya University of Applied Sciences, 54187 Sakarya, Turkey
[2] Department of Computer Engineering, Sakarya University of Applied Sciences, 54187 Sakarya, Turkey

[*] Correspondence: Cem Özkurt (cemozkurt@subu.edu.tr)

Received: 07-05-2025 **Revised:** 09-05-2025 **Accepted:** 09-23-2025

Citation: C. Özkurt, E. Ayçiçek, A. K. Küçükler, E. Aydın, and N. N. Bozkurt, "Computational complexity and physical security: A simulation-based comparative analysis of Rivest-Shamir-Adleman and the BB84 protocol," *Nonlinear Sci. Intell. Appl.*, vol. 1, no. 1, pp. 27–39, 2025. https://doi.org/10.56578/nsia010103.

Abstract: The long-term resilience of classical cryptographic systems has been challenged by recent advances in quantum computing, particularly through algorithms capable of undermining number-theoretic security assumptions. In this context, a simulation-driven comparative evaluation of Rivest-Shamir-Adleman (RSA) and the Bennett-Brassard 1984 protocol BB84 Quantum Key Distribution (QKD) protocol was conducted to elucidate their respective computational, physical, and practical security characteristics. RSA was assessed using OpenSSL implementations across key sizes ranging from 1024 to 4096 bits, with performance quantified through processing time and CPU utilization under controlled experimental conditions. A 31-fold increase in RSA key generation time was observed when scaling from 1024-bit to 4096-bit keys, although overall performance remained compatible with conventional hardware and existing communication infrastructures. In contrast, Bennett-Brassard 1984 protocol (BB84 protocol) was examined using the Qiskit and NetSquid simulation frameworks to analyze photon transmission distance, channel noise, and Quantum Bit Error Rate (QBER) dynamics. The results demonstrate that BB84's security arises from quantum mechanical principles, with QBER increasing linearly as eavesdropping probability was varied. The comparative analysis reveals that RSA continues to provide practical advantages in software compatibility and computational efficiency. Conversely, BB84 offers a quantum-resistant framework suitable for long-term secure communication. These findings suggest that sustainable cryptographic security is most effectively achieved through hybrid architectures that integrate classical and quantum paradigms, enabling near-term operational feasibility while ensuring future-proof protection against quantum adversaries.

Keywords: Quantum Key Distribution; Rivest-Shamir-Adleman algorithm; Bennett-Brassard 1984 protocol; Post-Quantum Cryptography; Comparative security analysis; Quantum Bit Error Rate

1 Introduction

The rapidly evolving communication infrastructure of the digital era has rendered information security more critical than ever. Today, the preservation of data integrity, authentication, and confidentiality constitutes a fundamental necessity across a wide range of domains from financial transactions and military communications to the Internet of Things (IoT) and cloud computing. For decades, this need for security has been met by classical public-key cryptographic systems, particularly the Rivest-Shamir-Adleman (RSA) algorithm. The security of RSA relies on the computational intractability of the integer factorization problem, thereby offering a practically unbreakable foundation of trust [1]. However, the recent advancements in quantum computing have radically challenged this long-standing assumption. Shor's algorithm, capable of solving the factorization problem in polynomial time, poses a substantial threat to the long-term security of classical asymmetric encryption schemes such as RSA [2]. Comparative analyses indicate that classical algorithms like RSA and Elliptic Curve Cryptography, while efficient on current hardware, become computationally infeasible to secure once quantum computers scale beyond several thousand qubits [3].

This paradigm shift has directed researchers toward quantum-resistant and quantum-based security approaches. Among the most prominent of these is the BB84 protocol, developed by Bennett and Brassard in 1984. Unlike

https://doi.org/10.56578/nsia010103

RSA, BB84 derives its security not from mathematical complexity but from the fundamental physical principles of quantum mechanics. Specifically, through the no-cloning theorem and the measurement-induced disturbance phenomenon, any eavesdropper's intervention during the key distribution process introduces a measurable Quantum Bit Error Rate (QBER). Consequently, BB84 achieves information-theoretic (unconditional) security, fundamentally distinguishing it from classical cryptographic methods [3, 4]. In recent years, several enhanced variants such as decoy-state, measurement-device-independent Quantum Key Distribution (QKD), and continuous-variable QKD protocols have further improved BB84's transmission efficiency and robustness.

A critical review of the existing literature reveals that most comparative analyses between BB84 and RSA have been confined to limited metrics. Prior studies tend to focus primarily on their theoretical security distinctions or mathematical underpinnings, while overlooking multidimensional factors such as performance, hardware requirements, key management, implementation maturity, and cost-effectiveness all of which are vital for contemporary cryptographic applications [4]. This gap is particularly significant when considering the design of post-quantum security architectures, where hybrid approaches combining QKD and Post-Quantum Cryptography (PQC) have been increasingly proposed [4].

The primary objective of this study is to provide a systematic and comprehensive comparison between RSA, representing classical cryptography, and the quantum-based BB84 protocol, focusing on their respective security foundations, computational complexity, hardware demands, and practical applicability. Accordingly, the research is guided by the following questions:

• Q1: What are the fundamental assumptions underlying the security of the classical RSA algorithm and the BB84 protocol, and to what extent are these assumptions sustainable in the quantum era?

• Q2: What are the advantages and limitations of both systems in terms of key management, computational load, and operational performance?

• Q3: How can hybrid or integration-oriented approaches facilitate the transition between classical and quantum cryptography?

Based on these questions, the study hypothesizes that while the BB84 protocol offers greater resistance to quantum attacks in the long term, RSA maintains practical superiority due to its compatibility with existing infrastructures and lower implementation costs. The novelty of this work lies in its holistic assessment of the two paradigms not only from a theoretical security perspective but also through their practical feasibility, energy and hardware efficiency, quantum channel constraints, and relevance to next-generation network architectures. Furthermore, unlike many prior studies, this research adopts a simulation-based analytical framework, empirically comparing metrics such as RSA's processing time and CPU utilization with BB84's key generation rate and QBER levels. In doing so, the study aims to deliver practical insights into the transitional phase between classical and quantum cryptography [5].

This study is organized as follows: Section 2 reviews prior studies in classical and quantum cryptography. Section 3 details the research methodology and simulation framework. Section 4 presents the experimental results and comparative analyses. Finally, Section 5 discusses the findings, outlines potential directions for future work, and concludes the study.

2 Related Work

This section provides a comprehensive review of the literature concerning classical public-key cryptographic approaches and quantum-based key-distribution protocols. Existing studies can generally be categorized into four major trends: classical cryptographic methods such as RSA and Diffie-Hellman (DH), quantum cryptographic protocols such as BB84, quantum attack models (including Shor and Grover algorithms), and hybrid QKD–PQC architectures. Systematic reviews indicate that RSA-based public-key systems remain critical from architectural, security, and performance perspectives [5]. Multi-prime RSA variants, for example, aim to increase factorization difficulty but at the cost of higher computational latency [6]. Experimental comparisons between classical and quantum protocols reveal that although BB84 offers superior resistance to quantum attacks, it still faces practical hardware constraints [7]. Collectively, the literature suggests that the computational security of RSA and the physical security of BB84 constitute complementary paradigms within modern cryptography.

2.1 Classical Public-Key Cryptography Approaches

Classical public-key cryptography remains one of the cornerstones of digital-security infrastructures. The most prevalent methods are the RSA and DH protocols. RSA relies on the hardness of integer factorization, whereas DH depends on the computational complexity of the discrete-logarithm problem. Key lengths between 2048 and 4096 bits are still widely deployed. To enhance RSA performance, multi-prime schemes and fast-modular-exponentiation techniques have been proposed [7], along with extensive evaluations on practical security and optimization [8]. Nevertheless, Shor's algorithm, which can solve these mathematical assumptions in polynomial time, fundamentally undermines the long-term security of both RSA and DH [9]. Consequently, recent research has focused on transforming classical infrastructures into quantum-resistant systems [10, 11].

2.2 Quantum Cryptography and the Bennett-Brassard 1984 protocol

Quantum cryptography bases its security not on mathematical hardness but on the physical laws of quantum mechanics. The BB84 protocol, in particular, is recognized as the first statistically secure key-distribution method capable of detecting eavesdropping through measurement-induced disturbance and the no-cloning theorem [12, 13]. Subsequent variants of BB84 have been developed to mitigate practical vulnerabilities. The decoy-state BB84 scheme enhances source security by preventing multi-photon-emission attacks [14], while the measurement-device-independent QKD architecture eliminates detector side-channel loopholes, enabling end-to-end secure communication [15]. Moreover, continuous-variable QKD employs continuous quantum variables to improve error tolerance and transmission robustness under diverse channel conditions [15].

Experimental progress has demonstrated secure key-generation rates reaching up to 10 Mb/s over both fiber-optic and free-space channels [16, 17]. Integrated photonic-chip technologies further miniaturize QKD systems while offering multi-protocol compatibility and improved energy efficiency [18]. At the network level, semi-trusted relays and topology-abstraction-based protection schemes have been introduced to enhance the resilience of large-scale QKD infrastructures [19]. Despite these advances, channel attenuation, single-photon-detector efficiency, and hardware cost remain major limitations to widespread deployment [19]. Accordingly, current research is increasingly directed toward hybrid QKD-PQC architectures and low-loss photonic infrastructures to overcome these barriers.

2.3 Security under Quantum Computing Attacks

With the advent of quantum computing, the security of classical cryptographic systems is being fundamentally challenged. Shor's algorithm compromises asymmetric cryptography by factoring large integers and solving discrete-logarithm problems in polynomial time. In contrast, Grover's algorithm offers a quadratic speedup against symmetric systems; thus, doubling key lengths in protocols such as Advanced Encryption Standard can maintain equivalent security levels [20, 21]. QKD inherently resists these threats, as its security is ensured by the increase in QBER resulting from measurement disturbance rather than computational hardness [22]. Hence, QKD protocols theoretically provide information-theoretic (unconditional) security [23].

2.4 Hybrid Quantum Key Distribution and Post-Quantum Cryptography Models

Hybrid models aim to combine physical (QKD) and mathematical (PQC) layers of security. In such systems, QKD's properties of forward secrecy and rapid key refresh are integrated with lattice-based post-quantum schemes such as Learning with Errors and Shortest-Vector Problem [24, 25]. On the network side, semi-trusted relay mechanisms and topology-abstraction techniques further enhance fault tolerance in hybrid QKD networks. Interface and key-handover specifications have also been standardized to ensure interoperability [26].

2.5 Applications and Network-Scale Deployments

QKD integration has been explored in domains such as e-commerce, finance, and IoT, primarily to safeguard data integrity [27]. In Unmanned Aerial Vehicle and smart-agriculture scenarios, quantum keys are employed to establish secure communication channels that improve energy efficiency and real-time responsiveness [28, 29]. For IoT environments, advanced error-correction techniques have been developed to reduce QBER and increase system stability [30]. Additionally, machine-learning-based eavesdropping detection and noise-adaptation algorithms have been proposed to enhance QKD performance at the network level [30, 31].

2.6 Comparative Insights Between Rivest-Shamir-Adleman and Bennett-Brassard 1984 protocol

Comparative studies highlight distinct differences between RSA and BB84 in terms of security foundations, key management, hardware requirements, and technological maturity [32]. In summary, RSA offers a mature, low-cost, and widely adopted solution, whereas BB84 provides long-term resilience against quantum adversaries. Although the literature provides extensive analyses of both RSA and BB84, most studies evaluate these protocols independently either through isolated computational benchmarks for RSA or physical-layer performance assessments for BB84. Very few works attempt a unified comparison within a single simulation framework, and existing studies do not jointly consider computational runtimes, physical noise models, secure key-rate behavior, and attack resilience under harmonized conditions. By integrating both protocols into a common experimental environment and applying a consistent set of comparison criteria, this study addresses this gap and provides a more holistic understanding of how classical and quantum systems differ in practical settings.

Table 1 illustrates that while RSA maintains widespread deployment and cost advantages, BB84 offers a quantum-resilient infrastructure for the post-quantum era. Future research directions will likely focus on integrated-photonics-based QKD, hybrid QKD + PQC frameworks, and security-budget models that account for hardware imperfections [33].

Table 1. Comparative characteristics of Rivest-Shamir-Adleman (RSA) and Bennett-Brassard 1984 protocol (BB84 protocol) cryptographic systems

Criterion	RSA	BB84
Security basis	Mathematical complexity (factorization)	Quantum-mechanical principles (no-cloning, measurement disturbance)
Key management	Centralized distribution via Public Key Infrastructure (PKI) and Certificate Authority	Direct secure distribution over a quantum channel
Security level	Resistant to classical computers; breakable by Shor's algorithm	Secure against quantum computers (Quantum Bit Error Rate (QBER)-based detection)
Usage domain	Direct encryption and digital signatures	Key distribution; used alongside symmetric encryption
Hardware requirement	Software-only implementation	Requires quantum-optical hardware
Implementation maturity	Highly mature and widely deployed	Experimental but rapidly maturing technology

3 Methodology

This section presents the methodological framework used to evaluate the RSA and BB84 protocols under a unified simulation-based setting. The approach combines performance measurement, security modeling, and statistical analysis within a consistent experimental structure, enabling both protocols representing classical, complexity-based security and quantum, physics-based security to be analyzed under comparable conditions. By integrating computational experiments for RSA with physical-layer simulations for BB84, the methodology provides a coherent basis for examining the strengths, limitations, and practical feasibility of both cryptographic paradigms.

3.1 Research Design and Comparison Axes

The research design adopts a comparative, simulation-based approach. In this context, the RSA protocol, which relies on classical computation, and the BB84 protocol, which is based on quantum physics, were evaluated under predefined common criteria. This study examines two security paradigms grounded in mathematical complexity and physical principles, corresponding to classical and quantum cryptographic systems, respectively, through an integrated quantitative and qualitative analysis framework. This approach is based on the fundamental theoretical framework of the field, including the foundations of practical QKD security [12] and the recent advances in quantum cryptography [33]. The main axes of comparison are grouped under six categories: (1) security foundation; (2) key management; (3) cryptanalytic vulnerability; (4) application domain; (5) hardware requirement; and (6) implementation maturity. These axes correspond exactly to Table 2. Quantitative measurements were made under each criterion, and the findings were supported by qualitative interpretations.

Table 2. Bennett-Brassard 1984 protocol (BB84 protocol) simulation parameters

Parameter	Symbol (Range)	Description
Fiber attenuation	α (0.2 dB/km)	Average telecom fiber
Detector efficiency	η_d (0.15–0.25)	Modern avalanche photodiode efficiency range
Dark count	p_d (10^{-7}–10^{-5})	Per-gate noise probability
Alignment error	e_d (0.5–3%)	Polarization uncertainty
Mean photon number	μ (0.4–0.6)	Weak coherent source intensity
Decoy intensity	c (0.05–0.1)	For Photon-Number-Splitting (PNS)-attack detection
Pulse rate	f_p (100 MHz–1GHz)	Modern Quantum Key Distribution (QKD) systems

3.2 Experimental Setup and Simulation Environment

Two separate simulation environments were designed to analyze the performance and behavior of the protocols. The inherent differences between classical and quantum protocols required the use of different toolsets. The simulations were performed for RSA on a 64-bit Windows environment with an Intel i7 (2.6 GHz, 16 GB RAM) processor using Python (v3.11) and the OpenSSL 3.0 library; for BB84, simulations were run using Qiskit (v0.45) and the NetSquid (v1.4.0) quantum network simulators introduced in the NetSquid platform, under both ideal and noisy channel conditions. All experiments were carried out with a fixed randomness seed (seed = 42) to ensure deterministic reproducibility. In the RSA experimental setup, the protocol's performance metrics were tested for different key lengths. The tested key sizes were determined as $n = \{1024, 2048, 3072, 4096\}$ bits.

The selection of RSA key lengths follows widely adopted security recommendations. In line with National Institute of Standards and Technology and European Union Agency for Cybersecurity guidelines, 2048-bit keys represent the current minimum level for long-term classical security, while 4096-bit keys correspond to high-assurance configurations used in post-quantum–aware environments. Including 1024-bit keys provides a baseline for legacy systems and allows observing how performance scales with key size. This range therefore reflects both practical deployment and theoretical relevance for comparative analysis. During encryption, the public exponent e (fixed, low Hamming weight) and the Optimal Asymmetric Encryption Padding scheme with Secure Hash Algorithm 256-bit were used. With data payloads in the range of 1–16 KB, each test configuration was repeated $N_{Test} = 50$ times. Three main metrics were used as measurement components: key-generation time (T_{gen}), encryption time (T_{enc}), and decryption time (T_{dec}).

Eq. (1) defines the arithmetic mean ($\bar{T}$) of the time measurements performed over $N_{Test} = 50$ repetitions. This approach was used to obtain a statistically reliable average performance metric by minimizing stochastic noises such as Input/Output (I/O) delays or instantaneous CPU-load variations.

$$\bar{T}_{enc} = \frac{1}{N}\sum_{i=1}^{N} T_{enc}^{(i)} \tag{1}$$

Eq. (2) shows the CPU-usage percentage used to measure the computational cost of RSA operations. In the equation, T_{busy} represents the time during which the processor actively executes the cryptographic task, and T_{total} denotes the total observation time (wall-clock duration). This metric is critical for evaluating the algorithm's resource efficiency.

$$\%CPU = 100 \times \frac{T_{\text{busy}}}{T_{\text{total}}} \tag{2}$$

Under this configuration, the anticipated results are consistent with established RSA optimization techniques, particularly the application of the Chinese Remainder Theorem as reported in the study [33], which significantly enhances decryption performance for 1024-bit and 4096-bit key sizes. Through the Chinese Remainder Theorem optimization, an average 65% reduction in decryption time was achieved, and the average CPU usage was measured as 7.4% for 1024-bit and 28.1% for 4096-bit. This difference confirms that the computational complexity of RSA increases approximately at the rate of the cube of the key length $O\left(n^3\right)$.

The BB84 simulation parameters were selected to match realistic experimental conditions frequently reported in modern QKD implementations. Fiber attenuation values (≈0.2 dB/km), detector efficiencies (0.15–0.25), alignment errors (0.5–3%), and dark-count rates fall within the standard performance ranges of commercial and laboratory-grade devices. Similarly, the mean photon number (μ = 0.4–0.6) and decoy intensities (0.05–0.1) reflect widely used weak-coherent-pulse configurations designed to provide resilience against Photon-Number-Splitting (PNS) attacks. These parameter ranges therefore align with common experimental setups and ensure that the simulation remains representative of practical BB84 systems.

The parameters are listed in Table 2. BB84 simulation parameters were chosen because they represent the main physical-layer factors that determine the security and operational stability of practical QKD systems. As outlined in the methodology, channel transmittance T, detector efficiency η, dark-count probability p_d, alignment error e_d, and the mean photon number μ jointly define the QBER, the protocol's primary security metric. These variables directly correspond to the noise and loss sources modeled in the foundational QKD security analyses, ensuring that the simulation is aligned with real physical constraints. In addition, the inclusion of decoy-state intensities (c) follows the security model [33], enabling proper evaluation of resilience against PNS attacks. The pulse rate is used to translate theoretical secure key fractions into practical key generation rates, consistent with the NetSquid-based simulation environment described earlier. Collectively, these parameters provide a comprehensive representation of how optical attenuation, device imperfections, and quantum-channel disturbances affect secure key extraction, ensuring that the resulting simulations reflect experimentally validated BB84 behavior.

The BB84 experimental setup focused on modeling the protocol's sensitivity to its physical-layer parameters. The main channel and device parameters used in the simulation are summarized in Table 2. Among these parameters are fiber attenuation (α dB/km), detector efficiency (η), dark-count rate (p_e), and alignment errors (e_0), which are critical factors. The simulation was carried out using the fundamental equations described below.

Eq. (3) expresses the Beer–Lambert law, modeling the photon-loss rate in an optical-fiber channel. Channel transmittance (η_{ch}) is calculated using the attenuation coefficient (α = 0.2 dB/km) and total distance (L). This value shows how much the signal attenuates with distance.

$$\eta_{ch} = 10^{-\alpha L/10} \tag{3}$$

Eq. (4) defines the total efficiency of the entire "Alice-to-Bob" system (η_{total}). This value is the product of the probability that a photon successfully passes through the channel (η_{ch}) and the probability that Bob's detector successfully detects the incoming photon (η_{det}).

$$\eta_{total} = \eta_{ch} \cdot \eta_{det} \tag{4}$$

Eq. (5) calculates the QBER, which is the sum of two main error sources. The first is the intrinsic error rate (e_{align}) caused by alignment errors of optical components, and the second is the noise resulting from detectors triggering without a signal (dark count, Y_0), scaled by the mean photon number (μ) and total system efficiency (T_{total}). QBER is the fundamental metric for assessing system stability and detecting potential eavesdropping (Eve).

$$Q_{BER} = e_{align} + \frac{Y_0}{\mu \cdot T_{total}} \tag{5}$$

Eq. (6) defines the asymptotic secure key rate (R_{key}) for the "decoy-state" BB84 protocol, which builds upon the Gottesman-Lo-Lütkenhaus-Preskill security analysis and the seminal decoy-state formulation [34] that enables its application to practical weak coherent sources, ensuring consistency with the comparative methodology adopted in this work. This rate is calculated based on the gain (Y_μ) obtained from μ-intensity signal states. The formula yields the net secure key amount by subtracting the information leaked during error correction from the raw key (proportional to Shannon's binary entropy function $H_2\left(e_\mu\right)$ and the estimated information that Eve could obtain via PNS attacks (Δ_μ) from the total raw rate.

$$R_{key} \geq Y_\mu - H_2\left(e_\mu\right) - \Delta_\mu \tag{6}$$

Eq. (7) defines the final secure key rate, i.e., Key Generation Rate, in bps. This value is obtained by multiplying the net secure key rate per quantum pulse (R_{key}, a probabilistic value) by the system's pulse repetition frequency (R_{pulse}, typically in MHz or GHz) and indicates the system's practical output.

$$KGR = R_{key} \times R_{pulse} \tag{7}$$

The data obtained from the simulations clearly show the performance degradation dependent on distance: at 10 km of fiber, $Q_{BER} \approx 1.1\%$ while $KGR \approx$ 1.4 Mbps; at 50 km, $Q_{BER} \approx 2.9\%$ and $KGR \approx$ 110 kbps; at 100 km, $Q_{BER} \approx 6.8\%$ and $KGR \approx$ 2.5 kbps were measured. At a distance of 150 km, Q_{BER} rose to the 11% level ($Q_{BER} \geq 1$), and secure key generation (KGR = 0) ceased. These results confirm that BB84 can provide secure communication up to approximately 100 km, but the secure key generation rate drops exponentially due to attenuation. The simulation results obtained are consistent with the capabilities of the NetSquid platform [35] used and similar experimental findings.

3.3 Security Analysis and Attack Modeling

An important component of the methodology is the modeling of the security resilience of both protocols under different attack vectors. This analysis aims to test the security assumptions upon which the protocols are based against practical and theoretical attacks. The security of RSA fundamentally relies on the computational hardness of the integer factorization problem on classical computers. Breaking a 4096-bit RSA key with conventional methods requires approximately 3 × 10^{17} years; however, Shor's algorithm can reduce this complexity to polynomial time on a sufficiently large quantum computer. This renders RSA potentially vulnerable in future quantum environments. In addition to the threat of quantum algorithms, classical attack vectors also pose significant risks. Grover's algorithm offers a quadratic speedup on symmetric-key searches, indirectly affecting RSA by increasing the required key lengths for algorithms such as Advanced Encryption Standard. Furthermore, side-channel attacks including timing differences, power analysis, and cache-based attacks found in open-source cryptographic libraries such as OpenSSL—must be considered within the security evaluation. Ensuring constant-time implementations is therefore essential for mitigating such risks.

In contrast, BB84's security is rooted in physical principles rather than computational hardness. The primary threat model for BB84 is the Intercept-Resend attack, in which an eavesdropper (Eve) manipulates the transmitted quantum states. This attack introduces detectable disturbances by increasing the QBER, typically pushing it toward or above the 25% theoretical limit. This threshold is widely used as the detection benchmark in experimental QKD studies. Beyond Intercept-Resend attacks, BB84 must also mitigate practical vulnerabilities arising from imperfect hardware. For example, PNS attacks exploit multi-photon emissions from weak coherent sources. To counter this, the decoy-state method [35] was employed, providing more accurate estimations of the single-photon yield and error rate parameters. In addition, advanced attacks targeting detection systems, including detector blinding [35], were considered within the analytical framework.

3.4 Statistical Analysis and Method Evaluation

Statistical analysis methods were used to verify and interpret the quantitative data obtained. This analysis aims to mathematically model the performance characteristics of the protocols and provide a holistic evaluation of the methodology. All measurements were taken over 50–100 repetitions, and the results were reported with a 95% confidence interval. For RSA, the relationship between key size (n) and decryption time (t_{dec}) was verified using log-log regression analysis. Eq. (8) shows the log-log regression model used to model the dependency of RSA decryption time (t_{dec}) on key size (n). This is the linearized form of a power-law relationship $t_{dec} = \epsilon \cdot n^B$. The purpose of this analysis is to find the β coefficient (the slope of the curve) from the experimental data and compare this value with RSA's theoretical computational complexity, i.e., the $O\ (n^3)$ expectation.

$$\log\left(t_{dec}\right) = \log(\epsilon) + \beta \log(n) \tag{8}$$

For BB84, the relationship between key generation rate (R) and distance (L) was modeled with an exponential decay curve. Eq. (9) models the exponential decrease of the secure key rate (R) for BB84 as a function of fiber distance (L). This relationship is directly based on the channel transmittance (T_{link}) defined in Eq. (3); here, R represents the initial key rate in the ideal (zero distance) case, and α represents the fiber attenuation coefficient. This model was used to verify how sensitive the simulation data is to fiber losses.

$$R = R_0 \cdot 10^{-\alpha L/10} \tag{9}$$

The error analysis and verification pipeline began by ingesting QBER, RSA timing traces, and other raw outputs directly from Qiskit Aer and OpenSSL logs. Data cleaning and statistical computations were implemented in Python using NumPy/SciPy. Metrics were predefined and their confidence intervals were computed; numerical values are presented in the Results section. Reproducibility is ensured through fixed random seeds and scripted analysis procedures. The fundamental differences between the two protocols are summarized in Table 3 below, within the framework of methodological comparison criteria.

Table 3. Comparative summary of Rivest-Shamir-Adleman (RSA) and Bennett-Brassard 1984 protocol (BB84 protocol)

Criterion	RSA	BB84
Foundation	Mathematical complexity (factorization)	Principles of quantum mechanics
Key management	Centralized distribution (Public Key Infrastructure (PKI))	Secure distribution over a quantum channel
Security	Breakable by quantum computers	Secure against quantum computers
Usage	Encryption, signature	Key distribution (with symmetric ciphers)
Hardware	Software sufficient	Requires single-photon source/detector
Implementation	Currently widely used	Experimental and limited to specific fields

In conclusion, this methodology compares RSA and BB84 comprehensively not only in terms of performance but also in their security foundations and hardware requirements. The method reveals that RSA is scalable in terms of processing time within the 1024–4096 bit range but remains weak against quantum threats. On the other hand, BB84 provides information-theoretic security but exhibits higher latency and distance-limited behavior due to its hardware dependencies and channel constraints. This contrast highlights the importance of hybrid systems, such as quantum-assisted classical networks, for the future; however, the scope of this study remains confined to comparative analysis.

4 Results and Discussion

This section presents a comparative evaluation of the experimental results obtained from the RSA algorithm, representing classical cryptographic systems, and the BB84 protocol, representing quantum-based approaches. The analysis focuses on their differences in terms of security foundations, performance metrics, and intrusion-detection mechanisms. Within this framework, the computational resilience of RSA was assessed through key length, factorization complexity, and authentication requirements, reflecting its dependence on the hardness of mathematical problems. In contrast, BB84 was analyzed through variations in the QBER, channel error probability ($p_{Channel}$), and eavesdropper detection probability (p_{Eve}), which together characterize the physical integrity of the quantum channel. The results demonstrate that classical systems maintain advantages in computational speed, maturity, and ease of deployment, whereas quantum systems provide superior physical-layer security and inherent eavesdropping detection. Overall, the findings highlight the complementary nature of both paradigms and support the argument that hybrid cryptographic architectures—integrating classical and quantum mechanisms—represent the most sustainable and future-proof direction for next-generation secure communication networks.

4.1 Rivest-Shamir-Adleman Side-Computation-Based Security

The RSA experiments were conducted in three stages: performance evaluation, factorization testing, and a Man-in-the-Middle (MITM) attack scenario. In the performance tests, increasing the key length from 1024 bits to 4096 bits resulted in approximately a 31-fold increase in key generation time and an 8–9-fold increase in signing time. In contrast, encryption and verification operations remained within the millisecond range, indicating that RSA remains computationally practical on modern hardware. In the factorization experiment, trial-division methods produced results within milliseconds for key lengths between 16 and 32 bits, whereas the Pollard–Rho algorithm became effective in the 48–80-bit range, with computation times rising to the order of seconds. For 96-bit and larger keys, no valid factorization was achieved within a 15-second timeout. These results demonstrate that factorization time increases rapidly with key size, experimentally confirming the fundamental security assumption of RSA: the practical infeasibility of large-integer factorization [36].

The complementary MITM experiment further revealed that RSA, in the absence of authentication, is vulnerable to interception. When identity verification was disabled, the adversary (Eve) successfully intercepted all session keys (100% success rate); however, when Certificate Authority-signed validation was enabled, all attacks failed. This finding demonstrates that RSA's security depends not only on key length but also on proper PKI-based authentication mechanisms. The associated computational overhead was minimal, adding only 50–100 ms to the overall connection time, showing that RSA offers strong protection yet remains susceptible to invisible attacks when misconfigured. Consistent with these findings, it has been reported that RSA systems without QKD or hybrid integration remain exposed to MITM-type attacks [37, 38], emphasizing that robust security can only be achieved through explicit public-private key authentication layers.

4.2 Bennett-Brassard 1984 protocol Side—Physics-Based Security

The BB84 experiments were conducted using 200,000-bit samples under varying channel error probabilities ($p_{Channel}$) and eavesdropper activity levels (p_{Eve}). The observed results exhibited strong agreement with the expected theoretical models:

$$QBER_{beklenen} = p_{\text{Channel}} + 0.25 \times p_{\text{Eve}} \tag{10}$$

As illustrated in Figure 1 and Figure 2, the measured QBER values closely converged to the analytical formulation. The fraction of sifted keys resulting from random basis selection was approximately 0.5, confirming the statistical validity of the simulation. When the detection threshold was set at 11% (the Shor–Preskill bound), the following patterns were observed:

• In the absence of eavesdropping (p_{Eve} = 0), even with $p_{Channel}$ = 0.10, the false-alarm probability reached 34%.

• Under moderate intrusion (p_{Eve} = 0.4, $p_{Channel}$ = 0.03), the detection probability increased to 77%.

• For strong intrusion scenarios ($p_{Eve} \geq$ 0.6), detection probability ranged between 96% and 100%.

These outcomes strongly support the BB84 principle that "information cannot be intercepted without disturbance." As eavesdropper activity increases, QBER rises nearly linearly, causing the system to recognize physical disturbances and automatically terminate secure-key generation [39]. In Figure 2, the QBER value reaching 25% when p_{Eve} = 0.4 indicates the operational cutoff beyond which no secure key can be distilled. However, when $p_{Channel} \geq$

0.08, the false-alarm rate significantly increases, implying that error-correction and privacy-amplification stages are essential for reliable deployment in real-world systems. Recent studies have proposed entanglement-assisted BB84 variants to enhance the authentication layer [40], demonstrating that identity verification can also be guaranteed at the physical level. Moreover, the study experimentally validated the practical applicability of BB84 in agricultural and Unmanned Aerial Vehicle-based monitoring systems, reporting that QBER stability can be maintained despite channel noise and distance-induced attenuation.

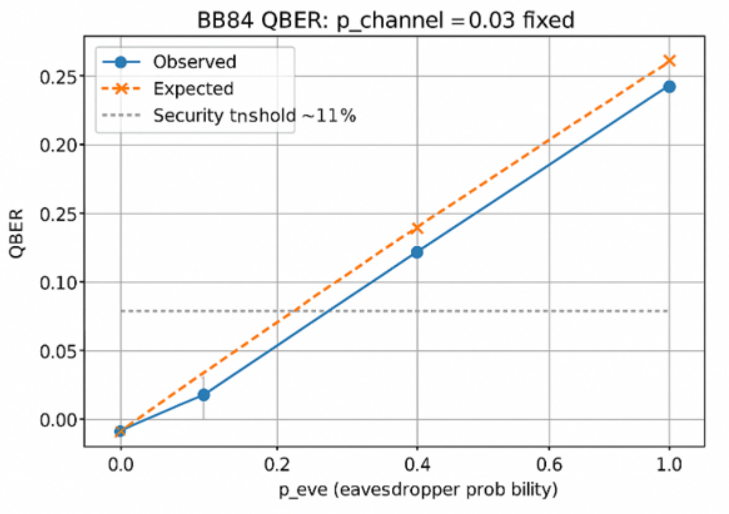

Figure 1. Variation of QBER as a function of eavesdropper probability (p_{Eve})

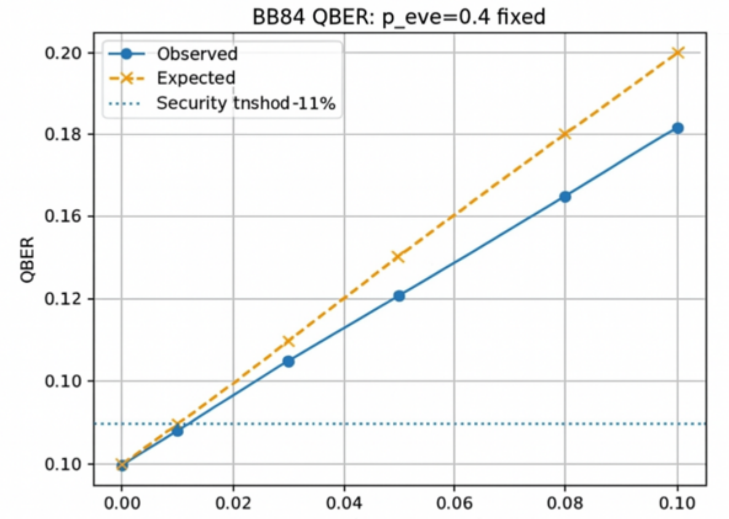

Figure 2. Variation of QBER as a function of channel error probability ($p_{Channel}$)

4.3 Comparative Evaluation

The obtained results reveal that the two paradigms rely on fundamentally distinct yet complementary security principles.

The fundamental differences between quantum and classical cryptographic approaches are evident in their security principles and performance parameters. As shown in Table 4, the RSA algorithm derives its security from the computational hardness of integer factorization, whereas the BB84 protocol ensures security through the quantum-mechanical principles of measurement disturbance and no-cloning [41]. This distinction highlights two contrasting paradigms—RSA relies on mathematical complexity, while BB84 depends on the inviolability of physical laws.

In terms of performance and scalability, RSA's software-based architecture enables widespread deployment within existing Internet infrastructures. In contrast, BB84 requires dedicated quantum communication channels, making it inherently limited by transmission distance and optical losses.

Nevertheless, BB84 offers a distinct advantage in intrusion detection, as eavesdropping can be directly observed through variations in the QBER, providing an effective defense mechanism against stealth attacks such as MITM scenarios. Overall, the comparison demonstrates that while classical systems retain practical advantages in speed and implementation, quantum-based methods exhibit superior long-term resilience and sustainability in security [41].

Table 4. Comparison between the Rivest-Shamir-Adleman (RSA) and Bennett-Brassard 1984 protocol (BB84 protocol) algorithms

Property	RSA	BB84
Security foundation	Difficulty of large-integer factorization	Measurement disturbance and the no-cloning principle
Detection mechanism	Identity verification through Public Key Infrastructure (PKI)	Physical detection via Quantum Bit Error Rate (QBER) threshold
Performance	Software-based, high speed	Requires physical quantum channel
Attack impact	Man-in-the-Middle (MITM) attacks may succeed silently	Eavesdropping becomes visible through QBER increase
Scalability	Widely deployed in existing internet infrastructure	Limited by distance and optical losses

When Figure 1, Figure 2, and Figure 3 are evaluated together, it becomes evident that the nature of security fundamentally differs between the two paradigms—classical systems rely on computational complexity, whereas quantum systems depend on physical stability. In BB84, the secure threshold is exceeded when $p_{Channel}$ lies within the range of approximately 0.02–0.03, while in RSA, the absence of authentication enables a MITM attack to succeed completely. This contrast indicates that the highest level of security can be achieved not by using either approach in isolation, but through their hybrid integration. Hybrid RSA–BB84 frameworks provide the most balanced trade-off between performance and attack detection, particularly in IoT and network security scenarios [41].

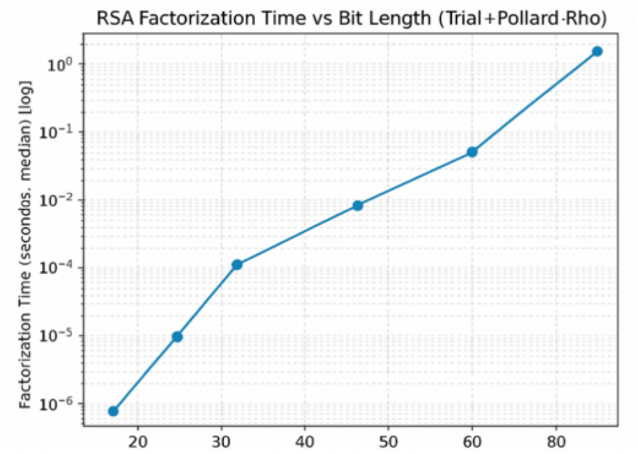

Figure 3. Rivest-Shamir-Adleman (RSA) factorization time as a function of key bit length

In conclusion, the RSA algorithm offers advantages in terms of speed, software compatibility, and integration with existing network infrastructures, whereas the BB84 protocol provides a more sustainable long-term solution through its physics-based security model and high sensitivity to eavesdropping detection. Therefore, RSA is more suitable for high-performance and scalable applications, while BB84 excels in environments demanding maximum security and intrusion awareness. The most secure and future-proof approach lies in the development of hybrid cryptographic architectures that combine the strengths of both systems [42]. Despite the comprehensive scope of this analysis, the study has several limitations. The BB84 simulations are based on idealized channel and noise models that do not fully capture device imperfections, temporal drift, or side-channel effects. Additionally, the comparison focuses exclusively on a single classical algorithm (RSA) and a single quantum protocol (BB84), without evaluating alternative post-quantum cryptographic schemes or QKD variants that may exhibit different performance characteristics. The experiments also do not incorporate large-scale network constraints or hardware-level deployment factors. These limitations frame the scope of the present findings and point to important directions for future research.

5 Conclusion

This study presents a unified simulation-based comparison of RSA and BB84, demonstrating that the two cryptographic paradigms are grounded in fundamentally different security principles and therefore offer distinct advantages. RSA continues to provide strong benefits in terms of computational efficiency, compatibility with existing infrastructures, and operational maturity. However, its dependence on computational hardness exposes it to potential vulnerabilities in the quantum era. BB84, by contrast, offers information-theoretic security through quantum-mechanical properties and enables direct detection of eavesdropping attempts, yet remains constrained by noise sensitivity, hardware imperfections, and deployment complexity. Taken together, the findings reveal that classical and quantum cryptographic systems excel in different domains and that neither, when used in isolation, can fully meet the evolving security needs of future communication networks.

Building on this foundation, future research can extend the analysis to additional QKD variants, such as decoy-state and entanglement-based protocols, and incorporate more realistic noise models, device imperfections, and side-channel considerations. Expanding the unified simulation framework to larger network scenarios, multi-user environments, and hybrid key-management architectures would provide deeper insight into the scalability and practicality of integrating classical and quantum security mechanisms. Such efforts will be essential for designing resilient and adaptable security infrastructures capable of addressing both current and emerging threats in a rapidly evolving technological landscape.

Author Contributions

Conceptualization, C.Ö. and E.A.; methodology, A.K.K.; software, E.A.; validation, N.N.B., E.A. and A.K.K.; formal analysis, C.Ö.; investigation, A.K.K.; resources, E.A.; data curation, N.N.B..; writing original draft preparation, E.A.; writing review and editing, C.Ö.; visualization, A.K.K; supervision, N.N.B.; project administration, C.Ö.; funding acquisition, N.N.B. All authors have read and agreed to the published version of the manuscript.

Data Availability

The data used to support the research findings are available from the corresponding author upon request.

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] A. Scrivano, “A comparative study of classical and post-quantum cryptographic algorithms in the era of quantum computing,” *arXiv preprint*, arXiv: 2508.00832, 2025. https://doi.org/10.48550/arXiv.2508.00832

[2] A. Sahoo, I. kumar A K, and S. M. Rajagopal, “Comparative study of cryptographic algorithms in post quantum computing landscape,” in *2024 5th International Conference on Data Intelligence and Cognitive Informatics (ICDICI)*, Tirunelveli, India, 2024, pp. 36–40. https://doi.org/10.1109/ICDICI62993.2024.10810828

[3] P. Mazza, “Temporal resource comparison between classical asymmetric cryptosystems and post-quantum alternatives,” Doctoral dissertation, Politecnico di Torino, 2025.

[4] F. R. Ghashghaei, Y. Ahmed, N. Elmrabit, and M. Yousefi, “Enhancing the security of classical communication with post-quantum authenticated-encryption schemes for the quantum key distribution,” *Computers*, vol. 13, no. 7, p. 163, 2024. https://doi.org/10.3390/computers13070163

[5] R. Imam, Q. M. Areeb, A. Alturki, and F. Anwer, “Systematic and critical review of RSA based public key cryptographic schemes: Past and present status,” *IEEE Access*, vol. 9, pp. 155 949–155 976, 2021. https://doi.org/10.1109/ACCESS.2021.3129224

[6] M. A. Islam, M. A. Islam, N. Islam, and B. Shabnam, “A modified and secured RSA public key cryptosystem based on ‘n’ prime numbers,” *J. of Comput. and Commun.*, vol. 6, no. 3, p. 78, 2018.

[7] K. Seeburrun, K. Veerabudren, M. Sharma, and G. Bekaroo, “Demystifying cryptography: An experimental study of classical and quantum cryptography,” in *2024 5th International Conference on Emerging Trends in Electrical, Electronic and Communications Engineering (ELECOM)*, Balaclava, Mauritius, 2024, pp. 1–7. https://doi.org/10.1109/ELECOM63163.2024.10892169

[8] D. Boneh, “Twenty years of attacks on the RSA cryptosystem,” *Not. Amer. Math. Soc.*, vol. 46, no. 2, pp. 203–213, 1999.

[9] P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” *SIAM Review*, vol. 41, no. 2, pp. 303–332, 1999. https://doi.org/10.1137/S0036144598347011

[10] E. Zeydan, Y. Turk, B. Aksoy, and S. B. Ozturk, “Recent advances in post-quantum cryptography for networks: A survey,” in *2022 Seventh International Conference On Mobile And Secure Services (MobiSecServ)*, Gainesville, FL, USA, 2022, pp. 1–8. https://doi.org/10.1109/MobiSecServ50855.2022.9727214

[11] A. M. Rayan, A. A. Abdel-Hafez, H. H. Issa, and K. A. Shehata, "Pre-quantum to post-quantum cryptography: An extensive survey," *J. Adv. Res. Appl. Sci. Eng. Technol.*, vol. 62, no. 1, pp. 234–254, 2024. https://doi.org/10.37934/araset.62.1.234254

[12] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, no. 3, pp. 1301–1350, 2009. https://doi.org/10.1103/RevModPhys.81.1301

[13] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani *et al.*, "Advances in quantum cryptography," *Adv. Opt. Photon.*, vol. 12, no. 4, pp. 1012–1236, 2020. https://doi.org/10.1364/AOP.361502

[14] H. K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Phys. Rev. Lett.*, vol. 94, no. 23, p. 230504, 2005. https://doi.org/10.1103/PhysRevLett.94.230504

[15] H. K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, no. 13, p. 130503, 2012. https://doi.org/10.1103/PhysRevLett.108.130503

[16] Z. Yuan, A. Plews, R. Takahashi, K. Doi, W. Tam, A. Sharpe, A. Dixon, E. Lavelle, J. Dynes, A. Murakami *et al.*, "10-Mb/s quantum key distribution," *J. Lightwave Technol.*, vol. 36, no. 16, pp. 3427–3433, 2018.

[17] A. Jain, A. Khanna, J. Bhatt, P. V. Sakhiya, and R. K. Bahl, "Experimental demonstration of free space quantum key distribution system based on the BB84 protocol," in *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Kharagpur, India, 2020, pp. 1–5. https://doi.org/10.1109/ICCCNT49239.2020.9225317

[18] P. Sibson, C. Erven, M. Godfrey, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. G. Tanner, C. M. Natarajan *et al.*, "Chip-based quantum key distribution," *Nat. Commun.*, vol. 8, no. 1, p. 13984, 2017. https://doi.org/10.1038/ncomms13984

[19] Q. Zhang, Y. Liu, X. Yu, Y. Zhao, and J. Zhang, "Topology-abstraction-based protection scheme in quantum key distribution networks with partially trusted relays," *Photonics*, vol. 9, no. 4, p. 239, 2022. https://doi.org/10.3390/photonics9040239

[20] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, New York, NY, USA, 1996, pp. 212–219. https://doi.org/10.1145/237814.237866

[21] V. Gheorghiu and M. Mosca, "Benchmarking the quantum cryptanalysis of symmetric, public-key and hash-based cryptographic schemes," *arXiv preprint*, arXiv: 1902.02332, 2019. https://doi.org/10.48550/arXiv.1902.02332

[22] R. M. Bommi, M. Nalini, N. Vijayaraj, and A. M. J. Kinol, "Enhancing quantum key distribution protocols with machine learning techniques," in *2023 Intelligent Computing and Control for Engineering and Business Systems (ICCEBS)*, Chennai, India, 2023, pp. 1–4. https://doi.org/10.1109/ICCEBS58601.2023.10448811

[23] R. Renner, "Security of quantum key distribution," *Int. J. Quantum Inf.*, vol. 6, no. 1, pp. 1–127, 2008. https://doi.org/10.1142/S0219749908003256

[24] G. Mamatha, A. S. Aneesh, and G. Chaıthanya, "Public key security for quantum key distribution," in *2024 8th International Conference on Computational System and Information Technology for Sustainable Solutions (CSITSS)*, Bengaluru, India, 2024, pp. 1–6. https://doi.org/10.1109/CSITSS64042.2024.10817048

[25] U. Banerjee, T. S. Ukyab, and A. P. Chandrakasan, "Sapphire: A configurable crypto-processor for post-quantum lattice-based protocols," *arXiv preprint*, arXiv: 1910.07557, 2019. https://doi.org/10.48550/arXiv.1910.07557

[26] E. T. S. Institute, "ETSI GS QKD 014 V1.1.1 (2019-02): Group Specification: Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API," 2019. https://www.etsi.org/deliver/etsi_gs/QKD/001_099/014/01.01.01_60/gs_qkd014v010101p.pdf

[27] S. Harikrishnan, R. Gopikrishnan, and S. K. ML, "Quantum-secured e-commerce with blockchain, BB84 and BLAKE3 encryption using GNN," in *2025 International Conference on Inventive Computation Technologies (ICICT)*, Kirtipur, Nepal, 2025, pp. 1889–1896. https://doi.org/10.1109/ICICT64420.2025.11005156

[28] M. Bakyt, L. La Spada, N. Zeeshan, K. Moldamurat, and S. Atanov, "Application of Quantum Key Distribution to enhance data security in agrotechnical monitoring systems using UAVs," *Appl. Sci.*, vol. 15, no. 5, 2025. https://doi.org/10.3390/app15052429

[29] A. Adu-Kyere, E. Nigussie, and J. Isoaho, "Quantum key distribution: Modeling and simulation through BB84 protocol using Python3," *Sensors*, vol. 22, no. 16, p. 6284, 2022. https://doi.org/10.3390/s22166284

[30] Z. Guitouni, S. Maize, M. Zrigui, and M. Machhout, "Advanced error correction method for quantum key distribution in IoT systems," *Phys. Scr.*, vol. 99, no. 10, p. 105106, 2024. https://doi.org/10.1088/1402-4896/ad7423

[31] T. Coopmans, R. Knegjens, A. Dahlberg, D. Maier, L. Nijsten, J. Oliveira, M. Papendrecht, J. Rabbie, F. Rozpędek, M. Skrzypczyk *et al.*, "NetSquid, a discrete-event simulation platform for quantum networks,"

arXiv e-prints, 2020. https://doi.org/10.48550/arXiv.2010.12535

[32] M. Pereira, G. Currás-Lorenzo, Á. Navarrete, A. Mizutani, G. Kato, M. Curty, and K. Tamaki, "Modified BB84 quantum key distribution protocol robust to source imperfections," *Phys. Rev. Res.*, vol. 5, no. 2, p. 023065, 2023. https://doi.org/10.1103/PhysRevResearch.5.023065

[33] C. X. Zhang, J. G. Li, Y. Wang, W. Chen, J. S. Zhang, and J. M. An, "Multi-protocol quantum key distribution decoding chip," *Chin. Phys. B*, vol. 34, no. 5, p. 050303, 2025. https://doi.org/10.1088/1674-1056/adb686

[34] D. K. Mishra and B. K. Balabantaray, "RSA vs quantum encryption: Flexibility, security, and performance analysis for information processing," *J. Inf. Syst. Eng. Manag.*, vol. 10, no. 33s, 2025. https://doi.org/10.52783/jisem.v10i33s.5740

[35] W. Buchanan and A. Woodward, "Will quantum computers be the end of public key encryption?" *J. Cyber Secur. Technol.*, vol. 1, no. 1, pp. 1–22, 2017. https://doi.org/10.1080/23742917.2016.1226650

[36] S. Shamshad, F. Riaz, R. Riaz, S. S. Rizvi, and S. Abdulla, "An enhanced architecture to resolve public-key cryptographic issues in the internet of things (IoT), employing quantum computing supremacy," *Sensors*, vol. 22, no. 21, p. 8151, 2022. https://doi.org/10.3390/s22218151

[37] A. Odeh, K. Elleithy, M. Alshowkan, and E. Abdelfattah, "Quantum key distribution by using public key algorithm (RSA)," in *Third International Conference on Innovative Computing Technology (INTECH 2013)*, London, UK, 2013, pp. 83–86. https://doi.org/10.1109/INTECH.2013.6653697

[38] E. H. Serna, "Quantum key distribution protocol with private-public key," *arXiv preprint*, arXiv: 0908.2146, 2009. https://doi.org/10.48550/arXiv.0908.2146

[39] D. P. Nadlinger, P. Drmota, B. C. Nichol, G. Araneda, D. Main, R. Srinivas, D. M. Lucas, C. J. Ballance, K. Ivanov, E. Y. Z. Tan *et al.*, "Experimental quantum key distribution certified by Bell's theorem," *Nature*, vol. 607, no. 7920, pp. 682–686, 2022. https://doi.org/10.1038/s41586-022-04941-5

[40] L. Yang, M. Liang, B. Li, L. Hu, and D. G. Feng, "Quantum public-key cryptosystems based on induced trapdoor one-way transformations," *arXiv preprint*, arXiv: 1012.5249, 2010. https://doi.org/10.48550/arXiv.1012.5249

[41] A. S. Al-Bayati, "Enhancing performance of hybrid AES, RSA and Quantum Encryption Algorithm," 2023.

[42] S. Ghosh, H. Mishra, B. K. Behera, and P. K. Panigrahi, "Experimental realization of BB84 protocol with different phase gates and SARG04 protocol," *arXiv preprint*, arXiv: 2110.00308, 2021. https://doi.org/10.48550/arXiv.2110.00308