Quantum Cryptography: Principles, Protocols, and Applications

Aishez Singh
Roll No: 2101CS06

Abhijeet Kumar
Roll No: 2101CS02

April 2025

Abstract

The area of quantum cryptography is a new and emerging field in the domain of data security. Unlike traditional cryptographic techniques, quantum cryptography is faster and capable of handling large volumes of data, as it operates on qubits and relies on the principle of Heisenberg's uncertainty. Quantum cryptography is primarily used in security applications involving quantum computers. Furthermore, this paper includes a security evaluation showing that any attack would result in a minimum error rate of 46.875%. The paper presents various algorithms used in quantum cryptography and compares them with existing classical cryptographic algorithms. It also discusses the shortcomings of current approaches and explores the future prospects of quantum cryptography.

1 Introduction

The primary objective of quantum cryptography is to perform computations and achieve levels of security that are nearly impossible using classical cryptographic methods. Quantum cryptography leverages fundamental principles of quantum mechanics, such as the quantum no-cloning theorem and Heisenberg's uncertainty principle [?]. Unlike classical cryptography, whose security is often based on assumptions regarding computational hardness, quantum cryptography derives its security from the unalterable laws of physics.

Currently, proposed quantum cryptographic algorithms include Quantum Key Distribution (QKD), quantum bit commitment, and quantum coin tossing. These applications vary in their degree of implementation success, with QKD being the most prominent and widely studied. It has been shown to be provably secure [?], and experimental implementations have already demonstrated QKD over several kilometers using standard commercial telecommunication optical fibers as well as free-space channels.

Secret quantum key sharing is a fundamental mechanism for enabling secure data transfer among parties that may not fully trust each other. A quantum secret sharing (QSS) scheme is crucial in such scenarios, especially for distributing quantum keys used in QKD or other quantum cryptographic protocols [?]. Additionally, the concept of post-quantum cryptography has emerged, focusing on developing cryptographic systems—particularly public-key systems—that remain secure even against attacks by quantum computers.

2 Quantum Key Distribution

The origins of quantum cryptography can be traced back to the work of Stephen Wiesner, who proposed that quantum systems could be used to create unforgeable currency. His ideas, although formulated earlier, were formally published in 1983. Due to the difficulty in isolating quantum systems from environmental disturbances over long periods, his concepts were initially considered more theoretical than practical. However, Charles Bennett and Gilles Brassard realized that quantum systems could be used for secure information transmission rather than data storage. In 1984, they introduced the first practical quantum cryptography protocol, now known as BB84 [?].

A significant theoretical advancement occurred in 1991, when Artur Ekert proposed a quantum cryptography protocol based on Bell's inequalities, utilizing entangled particle pairs as described in the Einstein-Podolsky-Rosen (EPR) paradox. Around the same time, Bennett and his team demonstrated the feasibility of QKD by building a prototype of the BB84 protocol using photon polarization [?].

In a typical QKD scenario, two parties—commonly referred to as Alice and Bob—exchange quantum states and perform measurements on them. They compare certain portions of their measurement results to determine which data can contribute to a shared secret key. Some measurement results are discarded during a process called *sifting* [?], which eliminates incompatible outcomes due to differing measurement bases.

Following sifting, the parties engage in error correction to reconcile discrepancies, and then perform a security analysis to estimate the amount of information an eavesdropper (Eve) might have gained. If this estimate exceeds a certain threshold, the protocol is aborted to prevent key compromise. Otherwise, they apply a technique called *privacy amplification* [?], which reduces Eve's knowledge to a negligible level and finalizes a shared secret key. During these processes, classical communication must be authenticated to prevent man-in-the-middle attacks. It is also acknowledged that a small probability of failure is tolerable in some components of the protocol.

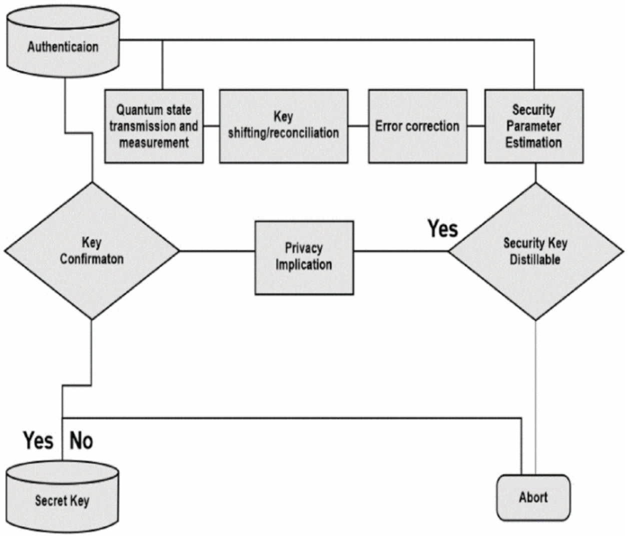

Figure 1: Flow chart of stages of qkd protocol

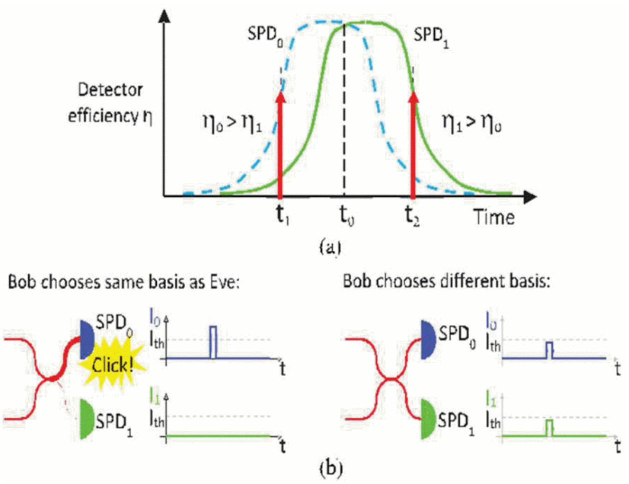

Figure 2: An illustration of detection efficiency mismatch within different spds

Table 1: Comparison between DiQKD and mdiQKD

Feature	**DiQKD**	**mdiQKD**
True random number generators	Yes	Yes
Trusted classical post-processing	Yes	Yes
Authenticated classical channel	Yes	Yes
No unwanted information leakage from the measurement unit	Yes	No
Characterized source	No	Yes

3 The Security of Quantum Key Distribution

Security checks are crucial because:

- They provide the foundation of security to a QKD protocol.
- They give a formula for the key generation rate of a QKD protocol.
- They even contribute to the classical post-processing protocols necessary for the generation of the final key.

While, in principle, QKD is secure, there is an important gap between the security checks made in QKD theory and the actual implementations. This gap exists because real-world devices suffer from inevitable imperfections that can cause them to behave differently from the idealized models used to prove security. Consequently, Eve (the eavesdropper) could exploit such imperfections to gain knowledge of the shared key without being detected.

One such attack is the time-shift attack, which was the first of its kind against a commercial QKD system [?]. Most QKD systems rely on at least two indicators to check two distinct bit values, but it is often challenging to ensure that the two indicators always have precisely the same location efficiency. In this scenario, Eve can simply shift the timing of each signal such that one indicator has a significantly higher location efficiency than the other. This way, she could gain partial knowledge of the final key without introducing any noticeable errors.

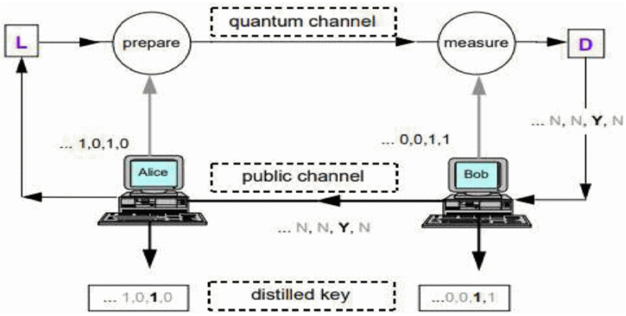

Figure 3: Schematic representation of the complete qkd system.

4 Quantum Cryptography Model

In the Quantum Key Distribution (QKD) model, Alice is considered the sender, Bob is the recipient, and Eve is the eavesdropper. Figure 3 illustrates the QKD model.

Table 2: Comparison of related work

Techniques	**Methodology**	**Advantage**
leftover hashing lemma	QKD	security of QKD
Blockchains	Post-Quantum	security of future blockchain
EDU	QKD	secure bit rate
Cloud computing	Cryptographic	secure cloud storage
Discrete Gaussian distribution	PQC	efficient, and high performance security

Table 3: Comparison of QKD Models

Year	Model Description	Technique	Objective
2017	High-Dimensional QKD based on Multicore Fiber	High-dimensional quantum key distribution protocol based on space division multiplexing in multicore fiber, silicon photonic integrated lightwave circuits are used	Reduce the bit error rate
2017	Continuous-variable QKD	Discrete quadrature-amplitude modulation and homodyne detection are used, utilizes a four-state and post-selection protocol and generates a secure key	Error correction and software-based post-processing
2018	High-dimensional QKD protocol on twisted photons	Experimentally evaluating and comparing the performance of different protocols	Implementing the different protocols over single apparatus
2019	Asymptotic Security of Continuous-Variable QKD	Lower bound on the asymptotic secret key rate of continuous-variable quantum key distribution, discrete modulation is considered	To achieve key distribution for 100 km
2019	Finite-key security for QKD	Quantum key distribution protocol based on weak coherent states, errorless unambiguous state	Constructing secure long-distance QKD links and multi-

5 Quantum vs. Public Key Cryptography

Quantum cryptography has transitioned from theory to practice. Quantum key distribution (QKD) has been successfully demonstrated over distances exceeding 100 km, achieving data transmission rates of approximately 2 kilobits per second. This makes QKD a viable solution not only in laboratory settings but also in real-world applications. In fact, some industrial firms are already marketing quantum key delivery systems based on these capabilities.

In a typical QKD setup, two parties—commonly referred to as Alice and Bob—exchange a cryptographic key through a secure quantum channel. This key is then used within a classical cryptographic integrity mechanism. However, for this process to be secure, Alice and Bob generally need some form of pre-established trust or shared information—much like the current practice when keys are exchanged using public key encryption methods.

Emerging research is exploring the concept of a *quantum router*—a device capable of recycling photons while preserving their polarization. This would potentially allow quantum cryptography to operate across broader networks. However, because photons cannot be stored for later use, a **real-time communication channel** is essential.

Additionally, both sender and receiver must coordinate during transmission to agree on the encoding basis and perform error detection before any key material is considered usable. This coordination is crucial to maintain the integrity and accuracy of the quantum key.

Despite its strengths, quantum cryptography currently lacks practical solutions for generating **digital signatures**—an essential component for ensuring authenticity and integrity in many cryptographic applications. While QKD is effective for securing communication between two static parties with large data volumes and high confidentiality requirements—such as connecting intelligence agency computers across different locations in a city—it is not yet suitable for broader use cases.

Although promising, **quantum encryption is unlikely to replace traditional cryptographic methods** for most everyday applications in the near future. Its current practicality is limited to specific, high-security scenarios.

5.1 Shor's Algorithm

Shor's efficient factorization algorithm indicates that classical cryptosystems are not secure against attacks by a sufficiently powerful quantum computer. The algorithm presents a method for integer factorization that can break widely-used encryption systems, such as RSA. Shor's approach reduces the problem of factoring large numbers to a special case of a mathematical problem known as the *Hidden Subgroup Problem (HSP)*. By providing an efficient quantum algorithm to solve this problem, Shor demonstrated the vulnerability of traditional public key cryptography in the quantum era.

Algorithm: Shor's Factorization Steps

1. Check if n is even, a prime number, or a perfect power. If so, terminate the algorithm.

2. Choose a random integer $x < n$ and compute $\gcd(x, n)$.
   If $\gcd(x, n) \neq 1$, then a non-trivial factor of n has been found.

3. **Quantum Computation:**
   Select q as the smallest power of 2 such that $n^2 \leq q < 2n^2$.
   Use a quantum algorithm to find the period r of the function $f(a) = x^a \mod n$.
   The algorithm returns a value c such that $\frac{c}{q} \approx \frac{d}{r}$, where $d \in \mathbb{N}$.

4. Use continued fraction expansion to determine the fraction $\frac{d}{r}$.
   Only proceed if $\gcd(d, r) = 1$ (i.e., the fraction is in lowest terms).

5. - If r is odd, return to Step 2.
   - If $x^{r/2} \equiv -1 \mod n$, return to Step 2.

- Otherwise, compute the non-trivial factors:

$$p = \gcd\left(x^{r/2} + 1, n\right), \quad q = \gcd\left(x^{r/2} - 1, n\right)$$

Table 4: Problems and complexities

Problem	**Group**	**Complexity**	**Cryptosystem**
Factorization	$\mathbb{Z}$	Polynomial	RSA
Discrete log	$\mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$	Polynomial	Diffie-Hellman, DSA
Elliptic curve discrete log	Elliptic curve	Polynomial	ECDH, ECDSA
Principal ideal	$\mathbb{R}$	Polynomial	Buchmann-Williams
Shortest lattice vector	Dihedral group	Sub-exponential	NTRU, Ajtai-Dwork
Graph isomorphism	Symmetric group	Exponential	–

Table 5: Proofs of different algorithms

Algorithm	**Technology**	**Problem solved**
Shor's algorithm	Integrated optics	Factorization of 21
Grover's algorithm [**?**]	NMR	Unstructured search, N = 8
Quantum annealing	D-Wave 2X	using model on a "Chimera" graph with 1097 vertices
HHL algorithm	Bulk optics, NMR	2×2 system of linear equations

5.2 COW Protocol

A new protocol was developed by Nicolas Gisin et al. in 2004 for practical quantum cryptography, known as the Coherent One-Way (COW) protocol. It is designed to operate using small constant-intensity pulses and aims to simplify implementation while maintaining security.

In the COW protocol, information is encoded in the time of arrival of the pulses on the data line, while coherence is monitored using an interferometer placed on a separate monitoring line. The monitoring line serves the sole purpose of detecting the presence of a potential eavesdropper—any attack would break the quantum coherence, making intrusion detectable.

The protocol is particularly robust against zero-error attacks, as such attacks do not increase the quantum bit error rate but only reduce the final key rate. The protocol relies on solid reference pulses and is designed to function even when quantum channel transmission is low.

In their paper, the authors propose several modifications to enhance the resilience and practicality of the protocol. Two notable types of attacks that affect the monitoring line are:

- **Persistent attack on two successive pulses:** A technique where the eavesdropper attempts to gather information by manipulating consecutive pulse sequences.

- **Intercept-resend attack:** In which the attacker intercepts the quantum signals, measures them, and then resends faked pulses to the receiver, thereby disrupting coherence.

These types of attacks introduce errors primarily on the monitoring line, thereby allowing the detection of an eavesdropper through observable disturbances.

5.3 SARG04 Protocol

The SARG04 protocol, introduced by V. Scarani et al. in 2004, was developed as an alternative to the BB84 protocol, specifically optimized for scenarios where thin laser pulses are used instead of ideal single-photon sources. Unlike BB84, which directly encodes the key bits in the quantum states, SARG04 uses the same four quantum states as BB84 but employs a different sifting process, allowing it to perform better under certain conditions.

SARG04 was presented in terms of preparation and measurement in Physical Review Letters. From a quantum processing perspective, it is functionally equivalent to BB84 in the ideal single-photon regime [?]. However, it demonstrates advantages in practical implementations that involve Poisson-distributed light sources and imperfect detectors, which are common in real-world quantum communication systems [?, ?].

Further studies by Tamaki and Lo have proven the protocol's security against attacks on one- and two-photon pulses, reinforcing its practical viability. Despite its theoretical equivalence to BB84 in the single-photon limit, experimental results have shown that SARG04 tends to have a lower performance under certain test conditions, especially in noisy environments or when detector inefficiencies are pronounced.

Overall, SARG04 represents a meaningful variation in quantum key distribution protocols, offering greater robustness in specific non-ideal settings.

Table 6: Comparison with some methodology and techniques

Techniques	**Features**	**Methodology**	**Advantages**
Spatial and temporal filtering	Free space quantum key	Quantum Cryptography	Secure key transmission
Time shift Attack [21]	Perfect-Eavesdropping	Quantum Position Cryptography	Position-Based Key Distribution
Classical cryptography	Quantum networks	Network-centric Quantum Communications	QKD in a secure manner
Stabilization	Polarization and phase drifts	One way optical scheme	Maintain QKD bit rate on relevant high level

6 Comparison of Latest Techniques

Floyd, D. (2006)

In this research, the author proposed and experimentally demonstrated a high-dimensional quantum key delivery protocol based on space-division multiplexing using a silicon photonic integrated lightwave circuit in multicore fiber. In a 4-D Hilbert space, the scientist constructed three mutually unbiased bases and achieved low and consistent quantum bit error rates within the limits of coherent and individual attacks. The utilization of multicore fiber significantly improves upon earlier demonstrations, enabling the creation of high-dimensional quantum states and surpassing the performance limits of conventional quantum key distribution (QKD) protocols.

Hughes, D. (2007)

This work marks a significant advancement towards full Continuous-Variable Quantum Key Distribution (CVQKD) security with discrete modulation. The author introduced a novel proof method to define a lower bound that remains valid in the asymptotic limit of infinite keys, even under collective attacks. This was specifically demonstrated using the QPSK protocol, with considerations for application to higher-order QAM protocols. The analysis reveals that the secret key rate under collective attacks mirrors that of arbitrary attacks in the asymptotic limit. This is verified through a semi-definite program involving Alice and Bob's covariance matrix in the entanglement-based version of the protocol. Although the bounds may not be optimal, they show secure key distribution is feasible over distances exceeding 100 km under practical excess noise conditions.

A. P. Bhatt, et al. (2018)

This study explores several classes of quantum distribution protocols such as BB84 and topological approaches by leveraging the orbital angular momentum (OAM) states of photons. Through experimental work in a laboratory setting, the author analyzed four classes of QKD protocols. The cross-talk among different OAM modes was found to degrade the performance of protocols in higher dimensions. For instance, the 8-dimensional BB84 offered no advantage over the 4-dimensional version when compared to the 2-dimensional BB84 protocol. Additionally, the sifting rate was observed to scale unfavorably with increased measurements, particularly in the case of the Chau15 protocol.

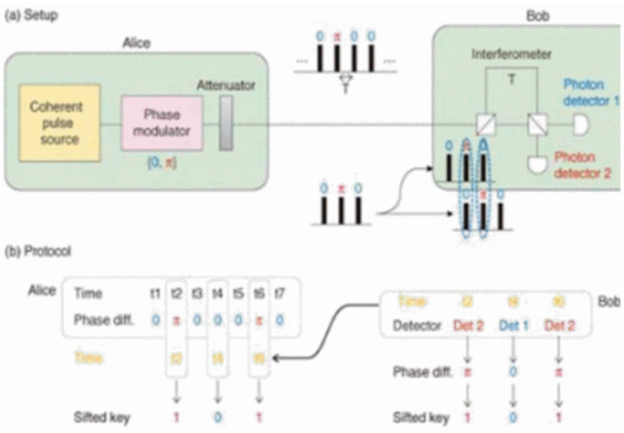

Figure 4: Schematic diagram of dps protocol.

7 Conclusion and Future Scope

The transition from classical cryptography to quantum cryptography is influenced by several factors, including performance gaps, cost, and ease of implementation. As a relatively nascent field, quantum cryptography presents numerous opportunities for advancement. Many challenges remain unresolved, and several applications are still under exploration.

Nevertheless, various techniques can be employed to achieve quantum secret key sharing, provided that the required security conditions are satisfied. For instance, classical coding methods may still be utilized by encoding classical information onto qubits entangled in a shared EPR (Einstein-Podolsky-Rosen) pair.

A critical area that demands further investigation is **Quantum Digital Signatures**, which could revolutionize authentication mechanisms in quantum networks. Another pressing concern is the issue of client impersonation. If an adversary with significant quantum computational power intercepts a qubit intended for a legitimate party and begins analyzing the signature, the adversary may be unable to extract meaningful information due to the no-cloning theorem and quantum measurement principles.

Quantum cryptography is gradually transitioning from theoretical exploration to practical deployment across various industries. With its ability to process large amounts of data securely and efficiently, it is poised to become the foundation of future security applications.

References

[1] T. Tsurumaru, ”Leftover hashing from quantum error correction: Unifying the two approaches to the security proof of quantum key distribution,” *IEEE Transactions on Information Theory*, 2020.

[2] A. K. Sharma and A. Ghunawat, ”A Review on Quantum Computers with Emphasize on Linear Optics Quantum Computing,” in *Proc. Int. Conf. on Issues and Challenges in Intelligent Computing Techniques (ICICT)*, 2019.

[3] A. Pljonkin and P. K. Singh, ”The Review of the Commercial Quantum Key Distribution System,” in *Proc. Int. Conf. on Parallel, Distributed and Grid Computing (PDGC)*, 2018.

[4] R. Asif, ”Future Quantum-to-the-Home (QTTH) All-Optical Networks (Invited Talk),” in *Proc. Int. Conf. on Advanced Infocomm Technology (ICAIT)*, 2018.

[5] Y. Cao, Q. Ou, Z. Liu, X. Liao, and J. Zhang, ”Soft-Reservation Based Resource Allocation in Optical Networks Secured by Quantum Key Distribution (QKD),” in *Asia Communications and Photonics Conference (ACP)*, 2017.

[6] L. Lydersen et al., ”Hacking commercial quantum cryptography systems by tailored bright illumination,” *Nature Photonics*, vol. 4, no. 10, pp. 686–689, 2010.

[7] Z. Yuan, J. Dynes, and A. Shields, ”Avoiding the blinding attacking QKD,” *Nature Photonics*, vol. 4, no. 12, pp. 800–801, 2010.

[8] L. Lydersen et al., ”Reply to ‘avoiding the blinding attack in QKD’,” *Nature Photonics*, vol. 4, no. 12, pp. 800–801, 2010.

[9] M.-S. Jiang et al., ”Intrinsic imperfection of self-differencing single-photon detectors harms the security of high-speed quantum cryptography systems,” *Phys. Rev. A*, vol. 88, no. 6, p. 062335, 2013.

[10] A. N. Bugge et al., ”Laser damage helps the eavesdropper in quantum cryptography,” *Phys. Rev. Lett.*, vol. 112, p. 070503, 2014.

[11] D. Y. Ding et al., ”High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits,” *npj Quantum Information*, vol. 3, no. 1, pp. 1–7, 2017.

[12] T. Hirano et al., ”Implementation of continuous-variable quantum key distribution with discrete modulation,” *Quantum Science and Technology*, vol. 2, no. 2, p. 024010, 2017.

[13] A. Kozubov, A. Gaidash, and G. Miroshnichenko, ”Finite-key security for quantum key distribution systems utilizing weak coherent states,” *arXiv preprint*, 2019.

[14] F. Bouchard et al., ”Experimental investigation of high-dimensional quantum key distribution protocols with twisted photons,” *Quantum*, vol. 2, p. 111, 2018.

[15] F. Xu et al., ”Experimental quantum key distribution with source flaws and tight finite-key analysis,” 2014.

[16] T. Ferreira da Silva, G. B. Xavier, G. P. Temporão, and J. P. von der Weid, ”Real-time monitoring of single-photon detectors against eavesdropping in quantum key distribution systems,” *Opt. Express*, vol. 20, no. 17, pp. 18911–18924, 2012.

[17] Z. Yuan, J. Dynes, and A. Shields, ”Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography,” *Appl. Phys. Lett.*, vol. 98, no. 23, pp. 231104, 2011.

[18] N. Gisin, S. Pironio, and N. Sangouard, ”Proposal for implementing device-independent quantum key distribution based on a heralded qubit amplifier,” *Phys. Rev. Lett.*, vol. 105, p. 070501, 2010.

[19] M. Curty and T. Moroder, ”Heralded-qubit amplifiers for practical device-independent quantum key distribution,” *Phys. Rev. A*, vol. 84, p. 010304, 2011.

[20] S. L. Braunstein and S. Pirandola, ”Side-channel-free quantum key distribution,” *Phys. Rev. Lett.*, vol. 108, no. 13, p. 130502, 2012.

[21] W. Hwang, ”Quantum key distribution with high loss: Toward global secure communication,” *Phys. Rev. Lett.*, vol. 91, p. 057901, 2003.

[22] H.-K. Lo, X. Ma, and K. Chen, ”Decoy state quantum key distribution,” *Phys. Rev. Lett.*, vol. 94, p. 230504, 2005.

[23] X. Wang, ”Beating the photon-number-splitting attack in practical quantum cryptography,” *Phys. Rev. Lett.*, vol. 94, p. 230503, 2005.

[24] C. Branciard et al., ”One-sided device-independent quantum key distribution: Security feasibility and the connection with steering,” *Phys. Rev. A*, vol. 85, no. 1, p. 010301, 2012.

[25] Z.-Q. Yin et al., ”Measurement-device-independent quantum key distribution with uncharacterized qubit sources,” *Phys. Rev. A*, vol. 88, no. 6, p. 062322, 2013.

[26] Z.-Q. Yin et al., ”Mismatched-basis statistics enable quantum key distribution with uncharacterized qubit sources,” *Phys. Rev. A*, vol. 90, no. 5, p. 052319, 2014.

[27] A. Rubenok et al., ”Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks,” *Phys. Rev. Lett.*, vol. 111, p. 130501, 2013.

[28] T. Ferreira da Silva et al., ”Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits,” *Phys. Rev. A*, vol. 88, p. 052303, 2013.

[29] G. Murali and R. S. Prasad, ”Comparison of cryptographic algorithms in cloud and local environment using quantum cryptography,” in *Proc. Int. Conf. on Energy Communication Data Analytics and Soft Computing (ICECDS)*, 2017.