**UNIVERSITY OF SCIENCE AND TECHNOLOGY OF HANOI**

Vietnam Academy of Science and Technology

Master Program: Space & Earth Observation

# COMPREHENSIVE LITERATURE REVIEW

# Reliability Improvement of Satellite-Based Quantum Key Distribution Systems Using Retransmission Scheme

**Primary Reference:**

Nguyen et al. (2021) – Photonic Network Communications

Posts and Telecommunications Institute of Technology (PTIT), Vietnam

**Student:** Truong Tuan Nghia

Student ID: 2540017

**Supervisor:** [Supervisor Name]

**Course:** Research Methodology

**Literature Coverage:**

85+ Papers | 1984–2025 | Foundational to State-of-the-Art

QKD Protocols | Satellite Experiments | Channel Models | Detection Schemes

Hanoi, December 2025

# Abstract

This comprehensive literature review examines the field of satellite-based Quantum Key Distribution (QKD), with particular focus on reliability improvement techniques. The primary reference is the work by Nguyen et al. (2021) from the Posts and Telecommunications Institute of Technology (PTIT), Vietnam, which proposes a novel combination of QPSK-based modulation, dual-threshold/heterodyne detection, and key retransmission for enhancing satellite QKD reliability.

**Scope:** This review covers 85+ research papers spanning from the foundational BB84 protocol (1984) to state-of-the-art developments in 2025, organized into four thematic parts:

1. **Introduction and Paper Analysis:** Detailed examination of Nguyen et al. (2021), including system architecture, mathematical framework, and key contributions
2. **Theoretical Foundations:** Foundational QKD protocols (BB84, E91, CV-QKD) and landmark satellite experiments (Micius, integrated networks)
3. **Technical Aspects:** Atmospheric channel models, detection schemes, error correction methods, and security analysis approaches
4. **Analysis and Synthesis:** Comparative evaluation, research gap identification, and future research directions

**Key Findings:**

- Nguyen et al. (2021) achieves 20 dB power improvement over conventional schemes and $>1000\times$ Key Loss Rate reduction with 4 retransmissions
- The 3-D Markov chain model provides a novel analytical framework for link-layer reliability analysis
- Integration of physical layer optimization (DT/HD) with link layer mechanisms (ARQ) represents a unique cross-layer approach
- Remaining gaps include experimental validation, finite-key security analysis, and LEO constellation integration



**Keywords:** Quantum Key Distribution, Satellite Communication, Free-Space Optics, Atmospheric Turbulence, QPSK Modulation, Heterodyne Detection, Dual-Threshold, Key Retransmission, Markov Chain, Reliability, PTIT Vietnam

| | |
|---|---|
| **Papers Reviewed:** | 85+ |
| **Time Span:** | 1984–2025 |
| **Primary Categories:** | 11 |
| **High-Citation Papers:** | 15+ (>1000 citations each) |

# Contents

# List of Tables

# List of Figures

# List of Acronyms

| | |
|---|---|
| **ACK** | Acknowledgment |
| **APD** | Avalanche Photodiode |
| **ARQ** | Automatic Repeat Request |
| **BB84** | Bennett-Brassard 1984 Protocol |
| **BER** | Bit Error Rate |
| **BPF** | Bandpass Filter |
| **BPSK** | Binary Phase-Shift Keying |
| **CDMA** | Code Division Multiple Access |
| **CV-QKD** | Continuous-Variable Quantum Key Distribution |
| **CW** | Continuous Wave |
| **DD** | Direct Detection |
| **DT** | Dual Threshold |
| **DTMC** | Discrete-Time Markov Chain |
| **DV-QKD** | Discrete-Variable Quantum Key Distribution |
| **E91** | Ekert 1991 Protocol |
| **FEC** | Forward Error Correction |
| **FSO** | Free-Space Optical |
| **HD** | Heterodyne Detection |
| **H-V** | Hufnagel-Valley |
| **IF** | Intermediate Frequency |
| **InGaAs** | Indium Gallium Arsenide |
| **KLR** | Key Loss Rate |
| **LDPC** | Low-Density Parity-Check |

| | |
|---|---|
| **LEO** | Low Earth Orbit |
| **LO** | Local Oscillator |
| **LPF** | Lowpass Filter |
| **MZM** | Mach-Zehnder Modulator |
| **NACK** | Negative Acknowledgment |
| **PDF** | Probability Density Function |
| **PTIT** | Posts and Telecommunications Institute of Technology |
| **QA-DTMC** | Queue-Associated Discrete-Time Markov Chain |
| **QBER** | Quantum Bit Error Rate |
| **QKD** | Quantum Key Distribution |
| **QKER** | Quantum Key Error Rate |
| **QPSK** | Quadrature Phase-Shift Keying |
| **RF** | Radio Frequency |
| **SIM** | Subcarrier Intensity Modulation |
| **SNR** | Signal-to-Noise Ratio |
| **SNSPD** | Superconducting Nanowire Single-Photon Detector |
| **URA** | Unauthorized Receiver Attack |
| **USTH** | University of Science and Technology of Hanoi |
| **VAST** | Vietnam Academy of Science and Technology |
| **VNSC** | Vietnam National Space Center |

# Part I

# Introduction and Paper Analysis

# Chapter 1

# Introduction

*This literature review provides a comprehensive analysis of reliability improvement techniques for satellite-based Quantum Key Distribution (QKD) systems, with particular focus on the retransmission scheme proposed by Nguyen et al. (2021) from the Posts and Telecommunications Institute of Technology (PTIT), Vietnam.*

## 1.1 Paper Under Review

### 1.1.1 Bibliographic Information

Table 1.1: Paper Identification

| Field | Information |
|---|---|
| Title | Reliability improvement of satellite-based quantum key distribution systems using retransmission scheme |
| Authors | Nam D. Nguyen, Hang T. T. Phan, Hien T. T. Pham, Vuong V. Mai, Ngoc T. Dang |
| Journal | Photonic Network Communications |
| Publisher | Springer |
| Year | 2021 |
| DOI | 10.1007/s11107-021-00934-y |
| Institution | Posts and Telecommunications Institute of Technology (PTIT) |
| Country | Vietnam |

### 1.1.2 Abstract Summary

The paper addresses the design and performance analysis of reliable satellite-based QKD over free-space optics (FSO) channels. The key contributions include:

1. **QPSK-based QKD Protocol:** Optical quadrature phase-shift keying modulation adapted for quantum key distribution

2. **Dual-Threshold/Heterodyne Detection (DT/HD):** Advanced receiver design that reduces QBER and improves sensitivity

3. **Key Retransmission Scheme:** ARQ-based protocol at the link layer to enhance reliability

4. **3-D Markov Chain Model:** Novel analytical framework for Key Loss Rate (KLR) analysis

## 1.2 Research Context and Motivation

### 1.2.1 The Need for Quantum-Secure Communication

The development of quantum computing poses fundamental threats to classical cryptographic systems. Shor's algorithm, when implemented on a sufficiently powerful quantum computer, can efficiently factor large integers, thereby breaking RSA and elliptic curve cryptography—the foundations of modern secure communication [1].

**Timeline of Quantum Computing Threat:**

- **Current (2025):** NISQ-era quantum computers with $\sim$1000 qubits
- **Near-term (2030):** Potential for cryptographically-relevant quantum computers
- **Harvest now, decrypt later:** Adversaries may store encrypted data today for future decryption

Quantum Key Distribution (QKD) offers a solution with information-theoretic security—security guaranteed by the laws of physics rather than computational assumptions.

### 1.2.2 Why Satellite-Based QKD?

While fiber-based QKD has achieved commercial deployment, fundamental limitations restrict its range:

Table 1.2: Comparison of QKD Transmission Media

| Medium | Maximum Distance | Limitation |
|---|---|---|
| Optical Fiber | $\sim$400 km | Exponential attenuation ($\sim$0.2 dB/km) |
| Terrestrial FSO | $\sim$10 km | Atmospheric turbulence, weather |
| **Satellite FSO** | **>1000 km** | **Lower atmospheric path length** |

**Key advantages of satellite QKD:**

- Free-space loss scales as $1/R^2$ (better than exponential fiber loss for long distances)
- Vacuum of space has negligible absorption
- Single satellite can serve multiple ground stations
- Global coverage possible with constellation

### 1.2.3 The Reliability Challenge

Despite its promise, satellite QKD faces significant reliability challenges:

1. **Atmospheric Turbulence:** Random intensity fluctuations (scintillation) cause signal fading
2. **Free-Space Path Loss:** >40 dB loss for LEO satellites at 600 km altitude
3. **Weather Dependence:** Clouds, rain, and aerosols increase attenuation
4. **Beam Spreading:** Diffraction causes power dilution at receiver
5. **Pointing Errors:** Misalignment between satellite and ground station
6. **Background Noise:** Solar radiation during daytime operation

These factors lead to high Quantum Bit Error Rate (QBER) and potential key transmission failures, motivating the need for reliability improvement techniques.

## 1.3 Vietnamese Research Context

### 1.3.1 PTIT Research Group

The Posts and Telecommunications Institute of Technology (PTIT) in Hanoi has established itself as a leading center for optical wireless communication research in Vietnam. Key achievements include:

- **Dual-threshold detection analysis:** Trinh et al. (2018) [2]
- **Reliability improvement schemes:** Nguyen et al. (2021) — the paper under review
- **CV-QKD optimization:** Nguyen et al. (2023) [3]
- **International collaborations:** University of Aizu (Japan), KAIST (Korea)

### 1.3.2 Regional Significance

Vietnam's strategic location and growing technological capabilities position it well for quantum communication development:

- Vietnam National Space Center (VNSC) under VAST
- USTH graduate programs in space technology
- Regional cooperation within ASEAN
- Tropical atmosphere conditions requiring specific modeling

## 1.4 Literature Review Objectives

This literature review aims to:

1. **Comprehensive Analysis:** Provide in-depth understanding of Nguyen et al. (2021) contributions
2. **Theoretical Foundation:** Connect the paper to foundational QKD and FSO literature
3. **Technical Deep-Dive:** Analyze the QPSK-based protocol, DT/HD detection, and retransmission scheme
4. **Mathematical Framework:** Review the channel model, QBER derivation, and 3-D Markov chain analysis
5. **Performance Evaluation:** Understand numerical results and their implications
6. **Critical Assessment:** Identify strengths, limitations, and future research directions
7. **Comparative Context:** Position the work within the broader satellite QKD literature

## 1.5 Review Structure

This literature review is organized as follows:

**Chapter 2: Detailed Paper Analysis** presents the complete technical analysis of Nguyen et al. (2021), including system architecture, key innovations, and main results.

**Chapter 3: QKD Protocol Design** examines the QPSK-based QKD protocol, its relationship to BB84, and the dual-threshold/heterodyne detection scheme.

**Chapter 4: Channel Model Analysis** provides detailed analysis of the FSO channel model including free-space loss, atmospheric attenuation, beam spreading, and Gamma-Gamma turbulence fading.

**Chapter 5: Retransmission Scheme** analyzes the key retransmission protocol, the 3-D Markov chain model, and Key Loss Rate derivation.

**Chapter 6: Performance Analysis** reviews numerical results for QBER, $P_{sift}$, and KLR under various conditions.

**Chapter 7: Comparative Study** positions the work within the broader literature and compares with alternative approaches.

**Chapter 8: Conclusion** synthesizes key findings and outlines future research directions.

# Chapter 2

# Detailed Paper Analysis

*This chapter provides a comprehensive technical analysis of Nguyen et al. (2021), examining the system architecture, key innovations, mathematical framework, and main contributions to satellite-based QKD reliability improvement.*

## 2.1 System Architecture Overview

### 2.1.1 Two-Layer Design

The proposed system operates across two layers:

1. **Physical Layer:** Responsible for quantum key transmission over FSO channel
   - QPSK modulator with Mach-Zehnder modulators (MZMs)
   - FSO channel with combined loss mechanisms
   - Dual-threshold/heterodyne detection (DT/HD) receiver
2. **Link Layer:** Manages key retransmission for reliability
   - Buffer management at Alice (satellite)
   - ACK/NACK feedback via classical RF channel
   - Retransmission protocol with maximum $M$ attempts

### 2.1.2 Link Configuration

Table 2.1: System Configuration

| Component | Location | Function |
|---|---|---|
| Alice (Transmitter) | LEO Satellite (600 km) | Key generation, QPSK modulation |
| Bob (Receiver) | Ground Station (5 m) | DT/HD detection, key recovery |
| Forward Channel | FSO (Downlink) | Quantum key transmission |
| Feedback Channel | RF (Classical) | ACK/NACK signaling |

## 2.2 Key Innovations

### 2.2.1 Innovation 1: QPSK-Based QKD Protocol

The paper adapts Quadrature Phase-Shift Keying (QPSK) for quantum key distribution:

**Advantages over alternatives:**

- Compared to SIM/BPSK: No RF subcarrier required, simpler implementation
- Compared to polarization encoding: Compatible with coherent detection
- Direct mapping of BB84 four-state structure to four QPSK phase states

**Phase State Mapping:**

$$\phi_A \in \left\{\frac{\pi}{4}, \frac{3\pi}{4}, \frac{5\pi}{4}, -\frac{\pi}{4}\right\} \tag{2.2.1}$$

### 2.2.2 Innovation 2: Dual-Threshold/Heterodyne Detection

The DT/HD receiver combines two techniques:

**Heterodyne Detection:**

- Signal mixed with strong local oscillator
- Improved receiver sensitivity compared to direct detection
- Both quadratures accessible (though only one used for key)

**Dual-Threshold Decision:**

$$\text{Decision} = \begin{cases} 0 & \text{if } i \geq d_0 \\ 1 & \text{if } i \leq d_1 \\ X & \text{otherwise (erasure)} \end{cases} \tag{2.2.2}$$

**Quantified Improvement:** 20 dB reduction in required transmitted power compared to SIM/BPSK-DT.

### 2.2.3 Innovation 3: Key Retransmission Scheme

The ARQ-based retransmission scheme operates as follows:

1. Alice generates key sequence, stores in buffer
2. Transmits via FSO channel to Bob
3. Bob checks received sequence for errors
4. If successful: Send ACK, Alice removes from buffer
5. If failed: Send NACK, Alice retransmits (up to $M$ times)

6. After $M$ failures: Discard sequence, count as key loss

**Advantage over FEC:**

- No computational overhead for encoding/decoding
- Adapts naturally to channel variations
- Simple implementation

### 2.2.4 Innovation 4: 3-D Markov Chain Model

Novel analytical framework with three-dimensional state space:

$$\text{State: } (n, s, m) \text{ where } \begin{cases} n \in [0, C] & \text{Buffer queue length} \\ s \in \{B, G\} & \text{Channel state (Bad/Good)} \\ m \in [1, M] & \text{Retransmission attempt number} \end{cases} \tag{2.2.3}$$

This model enables analytical calculation of Key Loss Rate (KLR).

## 2.3 Main Contributions Summary

Table 2.2: Paper Contributions and Impact

| Contribution | Type | Impact |
|---|---|---|
| QPSK-based QKD with DT/HD | System Design | 20 dB power improvement |
| Key retransmission scheme | Protocol Innovation | >1000× KLR reduction |
| 3-D Markov chain model | Analytical Framework | Enables KLR prediction |
| Comprehensive channel model | Mathematical Derivation | Realistic performance analysis |
| Parameter optimization | Numerical Results | Practical design guidelines |

## 2.4 Key Results Summary

### 2.4.1 Physical Layer Results

**QBER Performance:**

- Achieves QBER $< 10^{-3}$ with proper DT coefficient selection
- Optimal $\varsigma$ range: 0.7–2.4 (weak turbulence), 1.4–2.8 (strong turbulence)
- $P_{sift} \geq 10^{-2}$ maintained for sufficient key rate

**Power Comparison:**

Table 2.3: Required Transmitted Power for QBER $\leq 10^{-3}$

| **Scheme** | **Required $P_T$** |
|---|---|
| SIM/BPSK-DT | 45 dBm |
| QPSK-DT/DD | 35 dBm |
| **QPSK-DT/HD (Proposed)** | **25 dBm** |

### 2.4.2 Link Layer Results

**KLR Improvement with Retransmissions:**

Table 2.4: Key Loss Rate vs. Number of Retransmissions

| **Retransmissions ($M$)** | **KLR** | **Improvement** |
|---|---|---|
| 0 (Conventional) | $3 \times 10^{-2}$ | Baseline |
| 1 | $10^{-3}$ – $10^{-2}$ | 10× |
| 2 | $10^{-4}$ – $10^{-3}$ | 100× |
| 4 | $< 10^{-4}$ | >1000× |

**Key Finding:** Diminishing returns beyond $M = 4$; only 0.5 dB additional power gain from $M = 4$ to $M = 7$.

### 2.4.3 Security Analysis

**Unauthorized Receiver Attack (URA):**

- Eve's QBER increases with distance from Bob
- Minimum secure distance: $D_{E-B} > 30$ m (both weak and strong turbulence)
- Security maintained when Eve's QBER $> 10^{-2}$

## 2.5 System Parameters

Table 2.5: Complete System Parameters

| **Category** | **Parameter** | **Symbol** | **Value** |
|---|---|---|---|
| Physical Constants | Electron charge | $q$ | $1.6 \times 10^{-19}$ C |
| | Boltzmann constant | $k_B$ | $1.38 \times 10^{-23}$ W/K/Hz |
| | Planck's constant | $\tilde{h}$ | $6.63 \times 10^{-34}$ J·s |
| Receiver | Bit rate | $R_b$ | 10 Gbps |
| | Load resistor | $R_L$ | 50 Ω |
| | Excess noise factor | $x$ | 0.8 |
| | Avalanche multiplication | $\bar{g}$ | 10 |
| | Responsivity | $\Re$ | 0.8 |
| | Temperature | $T$ | 298 K |
| | Dark current | $I_d$ | 3 nA |
| Channel | Wavelength | $\lambda$ | 1550 nm |
| | Satellite altitude | $H_S$ | 600 km |
| | Ground station height | $H_G$ | 5 m |
| | Atmospheric altitude | $H_\beta$ | 20 km |
| | Zenith angle | $\zeta$ | 50° |
| | Wind speed | $w$ | 21 m/s |
| | Beam width | $\omega_D$ | 50 m |
| | Detection aperture | $a$ | 0.31 m |
| | Attenuation coefficient | $\gamma$ | 0.43 dB/km |
| Telescope | Tx gain | $G_T$ | 120 dB |
| | Rx gain | $G_R$ | 121 dB |
| Link Layer | Flow throughput | $H$ | 185 seq/s |
| | Bit sequence length | $l_{bs}$ | $3 \times 10^6$ bits |

# Part II

# Literature Review: Theoretical Foundations

# Chapter 3

# Foundational QKD Literature

*This chapter reviews the foundational literature in Quantum Key Distribution, from the original BB84 protocol to modern continuous-variable approaches, establishing the theoretical basis for satellite-based QKD systems.*

## 3.1 The BB84 Protocol

### 3.1.1 Historical Context

The BB84 protocol, proposed by Charles Bennett and Gilles Brassard in 1984 [4], represents the foundational breakthrough in quantum cryptography. Published at the IEEE International Conference on Computers, Systems and Signal Processing in Bangalore, India, this work established the principles that underpin all subsequent QKD protocols.

**Key Innovation:** BB84 was the first protocol to demonstrate that quantum mechanical principles—specifically the no-cloning theorem and the disturbance caused by measurement—could be exploited to achieve information-theoretically secure key distribution.

### 3.1.2 Protocol Description

The BB84 protocol operates using four quantum states organized into two conjugate bases:

Table 3.1: BB84 Quantum States

| **Basis** | **Bit 0** | **Bit 1** | **Representation** |
|---|---|---|---|
| Rectilinear (+) | $\|0\rangle$ | $\|1\rangle$ | Horizontal/Vertical |
| Diagonal (×) | $\|+\rangle$ | $\|-\rangle$ | ±45ř Diagonal |

**Protocol Steps:**

1. **Preparation:** Alice randomly chooses a bit value and a basis, prepares the corresponding quantum state
2. **Transmission:** State is sent through quantum channel to Bob

3. **Measurement:** Bob randomly chooses a measurement basis
4. **Sifting:** Alice and Bob publicly compare bases; keep only matching-basis results
5. **Error Estimation:** Sample subset to estimate QBER
6. **Error Correction:** Correct remaining errors using classical protocols
7. **Privacy Amplification:** Reduce Eve's potential information

### 3.1.3 Security Foundation

The security of BB84 rests on fundamental quantum mechanical principles:

1. **No-Cloning Theorem:** An unknown quantum state cannot be perfectly copied
2. **Measurement Disturbance:** Measuring a quantum state in the wrong basis causes irreversible disturbance
3. **Uncertainty Principle:** Conjugate observables cannot be simultaneously known with arbitrary precision

**QBER Threshold:** The protocol remains secure when QBER $< 11\%$ for individual attacks, or QBER $< 7.1\%$ for coherent attacks.

### 3.1.4 Relevance to Nguyen et al. (2021)

Nguyen et al. maps the BB84 four-state structure to QPSK phase states:

$$\text{BB84 States} \rightarrow \text{QPSK Phases: } \phi_A \in \left\{ \frac{\pi}{4}, \frac{3\pi}{4}, \frac{5\pi}{4}, -\frac{\pi}{4} \right\} \tag{3.1.1}$$

This mapping preserves the fundamental security properties while enabling coherent detection.

## 3.2 The E91 Protocol

### 3.2.1 Entanglement-Based QKD

Artur Ekert proposed the E91 protocol in 1991 [5], introducing entanglement as the basis for QKD security. This protocol uses maximally entangled photon pairs (Bell states):

$$\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{3.2.1}$$

### 3.2.2 Security via Bell Inequality

E91's security is verified through violation of Bell's inequality:

$$S = |E(a,b) - E(a,b') + E(a',b) + E(a',b')| \leq 2 \text{ (Classical)} \tag{3.2.2}$$

For maximally entangled states: $S = 2\sqrt{2} \approx 2.83$, proving quantum correlations.

### 3.2.3 Advantages and Challenges

Table 3.2: E91 vs. BB84 Comparison

| **Aspect** | **BB84** | **E91** |
|---|---|---|
| Source | Single photon/WCP | Entangled pairs |
| Security verification | QBER estimation | Bell inequality |
| Implementation | Simpler | More complex |
| Device-independence | No | Possible |
| Satellite demonstration | Micius (2017) | Micius (2017) |

## 3.3 Continuous-Variable QKD

### 3.3.1 Paradigm Shift

Continuous-Variable QKD (CV-QKD), pioneered by Grosshans et al. (2003) [6], represents a fundamental departure from discrete-variable approaches:

Table 3.3: DV-QKD vs. CV-QKD

| **Aspect** | **DV-QKD** | **CV-QKD** |
|---|---|---|
| Information carrier | Single photons | Coherent states |
| Detection | Single-photon detectors | Homodyne/Heterodyne |
| Modulation | Discrete (2/4 states) | Continuous (Gaussian) |
| Detector technology | APD/SNSPD | Standard photodiodes |
| Key rate (short range) | Lower | Higher |
| Maximum distance | ∼400 km | ∼200 km |
| Telecom compatibility | Limited | High |

### 3.3.2 Gaussian Modulation Protocol

The GG02 protocol uses Gaussian-modulated coherent states:

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \tag{3.3.1}$$

where $\alpha = x + ip$ with $x, p$ drawn from Gaussian distributions with variance $V_A$.

### 3.3.3 Security Proofs

Leverrier (2015) [7] established composable security for CV-QKD with coherent states, proving security against general attacks in the asymptotic limit. Key developments include:

- **Collective attacks:** Security proven for arbitrary attack strategies with i.i.d. assumption

- **Finite-key analysis:** Composable security with practical key lengths
- **Trusted noise model:** Excess noise bounded by device characterization

### 3.3.4 Relationship to Nguyen et al. (2021)

Nguyen et al.'s QPSK-based approach bridges DV and CV paradigms:

- Uses **discrete modulation** (4 phase states) like DV-QKD
- Employs **coherent detection** (heterodyne) like CV-QKD
- Security analysis based on **BB84 mapping**

This hybrid approach offers implementation simplicity while maintaining BB84-equivalent security.

## 3.4 Decoy State Method

### 3.4.1 Addressing Practical Source Limitations

Practical QKD implementations use weak coherent pulses (WCP) instead of true single photons, introducing vulnerabilities to photon-number-splitting (PNS) attacks. The decoy state method, proposed by Hwang (2003) and refined by Lo, Ma, and Chen (2005), addresses this limitation.

### 3.4.2 Principle

Alice randomly varies the mean photon number $\mu$ of transmitted pulses:

- **Signal state:** $\mu_s \approx 0.5$ (key generation)
- **Decoy state:** $\mu_d \approx 0.1$ (parameter estimation)
- **Vacuum state:** $\mu_v = 0$ (dark count estimation)

### 3.4.3 Security Enhancement

The decoy state method enables tight bounds on single-photon contribution:

$$Y_1^L \leq Y_1 \leq Y_1^U \tag{3.4.1}$$

where $Y_1$ is the single-photon yield, enabling security equivalent to ideal single-photon sources.

#### 3.4.4 Implementation in Satellite QKD

The Micius satellite [8] demonstrated decoy-state BB84 for satellite QKD:

- Three-intensity protocol ($\mu$, $\nu$, vacuum)
- QBER $\sim 1.1\%$ achieved
- Key rate up to 40.2 kbps at 530 km distance

### 3.5 Landmark Review Papers

#### 3.5.1 Gisin et al. (2002)

"Quantum Cryptography" in Reviews of Modern Physics [9] provided the first comprehensive review of QKD, covering:

- Theoretical foundations and security proofs
- Experimental implementations
- Practical considerations and limitations

**Citations:** >5000 (foundational reference for the field)

#### 3.5.2 Scarani et al. (2009)

"The Security of Practical Quantum Key Distribution" [1] in Reviews of Modern Physics established the framework for analyzing practical QKD security:

**Key Contributions:**

- Rigorous treatment of practical device imperfections
- Comprehensive attack classification
- Security parameter optimization

**Relevance to Nguyen et al.:** Provides the security framework for QBER analysis and threshold determination.

#### 3.5.3 Pirandola et al. (2020)

"Advances in Quantum Cryptography" [10] in Advances in Optics and Photonics (225 pages) represents the most comprehensive recent review:

**Coverage:**

- DV-QKD and CV-QKD protocols
- Satellite and free-space implementations
- Quantum networks and repeaters
- Post-quantum considerations

### 3.5.4 Xu et al. (2020)

"Secure Quantum Key Distribution with Realistic Devices" [11] in Reviews of Modern Physics addresses practical security:

- Device imperfection modeling
- Side-channel attacks and countermeasures
- Measurement-device-independent QKD
- Twin-field QKD for extended range

## 3.6 Historical Timeline

Table 3.4: QKD Development Timeline

| Year | Milestone | Reference |
|---|---|---|
| 1984 | BB84 protocol proposed | Bennett & Brassard |
| 1991 | E91 entanglement protocol | Ekert |
| 1992 | First experimental BB84 (32 cm) | Bennett et al. |
| 2002 | Comprehensive QKD review | Gisin et al. |
| 2003 | CV-QKD with coherent states | Grosshans et al. |
| 2005 | Decoy state method | Lo, Ma, Chen |
| 2007 | 200 km fiber QKD | Schmitt-Manderbach |
| 2009 | Practical security framework | Scarani et al. |
| 2012 | Finite-key analysis | Tomamichel et al. |
| 2015 | CV-QKD composable security | Leverrier |
| 2016 | Micius satellite launch | USTC/CAS |
| 2017 | First satellite QKD | Liao et al. |
| 2020 | MDI-QKD over 500 km | Chen et al. |
| 2021 | 4600 km integrated network | Chen et al. |

## 3.7 Chapter Summary

This chapter established the theoretical foundations underlying Nguyen et al. (2021):

1. **BB84 Protocol:** Provides the four-state structure mapped to QPSK phases
2. **CV-QKD:** Introduces coherent detection applicable to heterodyne receivers
3. **Decoy States:** Addresses practical source limitations in satellite implementations
4. **Security Framework:** Establishes QBER thresholds and analysis methodology

**Key Insight:** Nguyen et al.'s QPSK-DT/HD approach synthesizes concepts from multiple foundational works, creating a practical system that leverages coherent detection advantages while maintaining BB84-equivalent security structure.

# Chapter 4

# Satellite QKD Experiments

*This chapter reviews the landmark experimental demonstrations of satellite-based QKD, from the Micius satellite missions to the integrated space-ground quantum network, providing the experimental context for Nguyen et al.'s theoretical contributions.*

## 4.1 The Micius Satellite (QUESS)

### 4.1.1 Mission Overview

The Quantum Experiments at Space Scale (QUESS) mission, featuring the Micius satellite, represents humanity's first dedicated quantum science satellite. Named after the ancient Chinese philosopher Mozi (), this $100 million mission was launched on August 16, 2016 [8].

Table 4.1: Micius Satellite Specifications

| **Parameter** | **Specification** |
|---|---|
| Launch Date | August 16, 2016 |
| Launch Vehicle | Long March 2D |
| Orbit | Sun-synchronous LEO |
| Altitude | $\sim$500 km |
| Inclination | 97.4° |
| Mass | 631 kg |
| Design Life | 2 years (exceeded) |
| Operating Institution | CAS/USTC |
| Lead Scientist | Prof. Jian-Wei Pan |

### 4.1.2 Scientific Payload

The satellite carries three main experimental payloads:

1. **QKD Transmitter:** Decoy-state BB84 source
    - Wavelength: 850 nm

- Repetition rate: 100 MHz
- Decoy intensities: $\mu$, $\nu$, vacuum

2. **Entanglement Source:** Spontaneous parametric down-conversion
   - Entangled photon pairs at 810 nm
   - >5.9 million pairs/second
   - Fidelity >90%
3. **Quantum Teleportation Payload:** Bell-state measurement capability

## 4.2 Micius Experimental Results

### 4.2.1 Satellite-to-Ground QKD (2017)

Liao et al. [8] demonstrated the first satellite-to-ground QKD, published in Nature:

**Experimental Configuration:**

- Ground station: Xinglong, near Beijing
- Distance range: 507 km to 1034 km
- Measurement duration: 273 seconds per pass

**Key Results:**

Table 4.2: Micius QKD Performance Results

| Metric | 530 km | 1034 km |
|---|---|---|
| Sifted key rate | 40.2 kbps | 1.2 kbps |
| Secure key rate | 12.0 kbps | 0.4 kbps |
| QBER | 1.1% | 3.2% |
| Channel loss | 21.5 dB | 41.5 dB |

**Significance:** Demonstrated that satellite QKD can exceed ground-based fiber performance for distances >400 km.

### 4.2.2 Entanglement Distribution (2017)

Yin et al. [12] achieved record-breaking entanglement distribution, published in Science:

**Configuration:**

- Two ground stations: Delingha and Lijiang
- Separation: 1203 km
- Simultaneous detection of entangled pairs

**Results:**

- Bell inequality violation: $S = 2.37 \pm 0.09 > 2$
- Detection rate: 1.1 pairs/second
- Fidelity: 87.4%

**Significance:** Demonstrated entanglement preservation over unprecedented distances, opening possibility for device-independent QKD.

### 4.2.3 Intercontinental QKD (2018)

Liao et al. [13] demonstrated China-Austria QKD, published in Physical Review Letters:

**Configuration:**

- Ground stations: China (multiple) and Austria (Graz)
- Total distance: 7600 km
- Satellite as trusted relay node

**Demonstration:**

- 75-minute encrypted videoconference between Beijing and Vienna
- 128-bit AES keys exchanged via QKD
- First intercontinental quantum-secured communication

### 4.2.4 Full Quantum Teleportation (2021)

Pan's team demonstrated full quantum state teleportation over 1200 km ground distance using satellite-distributed entanglement.

## 4.3 Integrated Space-Ground Network (2021)

### 4.3.1 Chen et al. (2021) - Nature

Chen et al. [14] published "An integrated space-to-ground quantum communication network over 4,600 kilometres" in Nature, representing the most comprehensive quantum network demonstration.

**Network Architecture:**

- **Fiber backbone:** 2000 km Beijing-Shanghai link
- **Satellite links:** 2600 km via Micius
- **Metropolitan networks:** 4 QMANs (Shanghai, Hefei, Jinan, Beijing)
- **Trusted nodes:** 32 fiber relay stations
- **Users:** 150+ across government, banking, grid

Table 4.3: Integrated Network Performance

| **Link Type** | **Key Rate** | **Improvement** |
|---|---|---|
| Satellite-ground | 47.8 kbps | 40× vs. previous |
| Fiber backbone | Variable | Continuous operation |
| Metropolitan | High rate | Local applications |

**Performance:**

**Applications Demonstrated:**

- Banking transactions (ICBC, Bank of China)
- Power grid communications (State Grid)
- Government e-services
- Encrypted voice/video conferencing

## 4.4 Other Satellite QKD Missions

### 4.4.1 Jinan-1 Micro-Satellite (2022)

China launched the Jinan-1 micro-nano satellite in July 2022, demonstrating cost-effective QKD:

- Smaller form factor than Micius
- Compact ground stations
- 2025: Achieved QKD with South Africa (12,900 km)

### 4.4.2 Planned Missions (2025-2027)

Table 4.4: Upcoming Satellite QKD Missions

| **Mission** | **Country** | **Launch** | **Objective** |
|---|---|---|---|
| Eagle-1 | ESA | 2025-2026 | Operational QKD service |
| QUBE-II | Germany | 2025 | CubeSat BB84 demonstration |
| QEYSSat | Canada | 2025 | LEO constellation study |
| Next-gen Micius | China | 2025 | LEO constellation (2-3 sats) |
| MEO satellite | China | 2027 | Extended coverage |

### 4.4.3 Japanese NICT Experiments

Japan's NICT has conducted ground-to-LEO experiments using the SOCRATES satellite, demonstrating:

- Uplink QKD feasibility
- Pointing acquisition and tracking
- Photon transmission through atmosphere

## 4.5 Comparison with Nguyen et al. (2021)

### 4.5.1 System Parameter Comparison

Table 4.5: Nguyen et al. vs. Micius Systems

| **Parameter** | **Nguyen (2021)** | **Micius (2017)** |
|---|---|---|
| *System Configuration* | | |
| Satellite altitude | 600 km | 500 km |
| Protocol | QPSK-based | Decoy-state BB84 |
| Wavelength | 1550 nm | 850 nm |
| Modulation | Phase (QPSK) | Polarization |
| Detection | Heterodyne (APD) | Single-photon (Si-APD) |
| *Error Handling* | | |
| Method | ARQ retransmission | LDPC FEC |
| Complexity | Low | Medium |
| Adaptability | Channel-adaptive | Fixed rate |
| *Validation* | | |
| Status | Simulation | Experimental |

### 4.5.2 Complementary Contributions

While Micius demonstrated experimental feasibility, Nguyen et al. addresses:

1. **Alternative Detection:** Coherent detection vs. single-photon
2. **Reliability Mechanism:** ARQ vs. FEC approach
3. **Analytical Framework:** 3-D Markov model for link-layer analysis
4. **Wavelength Choice:** Telecom-band (1550 nm) for compatibility

## 4.6 Lessons from Satellite Experiments

### 4.6.1 Technical Insights

1. **Downlink Preferred:** Satellite-to-ground links experience less turbulence impact than uplinks
2. **Night Operation:** Current systems operate primarily at night to avoid solar background noise
3. **Pointing Critical:** Sub-microradian pointing accuracy essential for stable links
4. **LEO Optimal:** Low Earth orbit provides best balance of loss and pass duration
5. **Trusted Nodes:** Practical networks currently require trusted relay satellites

### 4.6.2 Relevance to Nguyen et al.

The experimental lessons inform Nguyen et al.'s design choices:

- **LEO Configuration:** 600 km altitude consistent with optimal range
- **Downlink Scenario:** Satellite-to-ground transmission
- **Atmospheric Modeling:** Gamma-Gamma distribution validated by experiments
- **Error Handling:** Retransmission addresses practical channel variability

## 4.7 Chapter Summary

This chapter reviewed satellite QKD experimental achievements:

1. **Micius Satellite:** First dedicated quantum satellite, demonstrating QKD, entanglement distribution, and teleportation
2. **Performance Benchmarks:** 40.2 kbps sifted key rate, 1.1% QBER, 1200 km entanglement
3. **Integrated Network:** 4600 km space-ground network with 150+ users
4. **Future Missions:** Eagle-1, QEYSSat, and expanded Chinese constellation
5. **Context for Nguyen et al.:** Experimental validation supports theoretical assumptions; novel contributions address detection and reliability challenges

**Gap Identification:** Experimental work has focused on DV-QKD with single-photon detection. Nguyen et al.'s coherent detection and retransmission approach offers an alternative paradigm requiring future experimental validation.

# Part III

# Literature Review: Technical Aspects

# Chapter 5

# Atmospheric Channel Models

*This chapter reviews the literature on atmospheric channel modeling for free-space optical communications, with emphasis on turbulence models, the Gamma-Gamma distribution, and their application to satellite-based QKD systems.*

## 5.1 Free-Space Optical Channel Characteristics

### 5.1.1 Loss Mechanisms

The satellite-to-ground FSO channel introduces multiple loss mechanisms that affect QKD performance:

$$h_{total} = h_l \cdot h_a \cdot h_s \cdot h_p \cdot h_t \tag{5.1.1}$$

where:

- $h_l$: Free-space path loss
- $h_a$: Atmospheric attenuation
- $h_s$: Beam spreading loss
- $h_p$: Pointing error loss
- $h_t$: Atmospheric turbulence fading

### 5.1.2 Literature Foundation

Kaushal and Kaddoum (2017) [15] provide a comprehensive survey of space optical communication challenges:

**Key Topics Covered:**

- Atmospheric effects (absorption, scattering, turbulence)
- Mitigation techniques (adaptive optics, diversity)
- Link budget considerations
- Pointing, acquisition, and tracking

## 5.2 Free-Space Path Loss

### 5.2.1 Inverse Square Law

The geometric spreading of optical beams follows:

$$h_l = \left(\frac{\lambda}{4\pi D_{SG}}\right)^2 \tag{5.2.1}$$

where $D_{SG}$ is the satellite-to-ground distance:

$$D_{SG} = \sqrt{(H_S - H_G)^2 \cdot \sec^2(\zeta) + 2R_E(H_S - H_G) \cdot \sec(\zeta)} \tag{5.2.2}$$

**Typical Values (Nguyen et al. parameters):**

- $H_S = 600$ km, $\zeta = 50$ř: $D_{SG} \approx 783$ km
- Path loss: ∼260 dB (before telescope gains)

## 5.3 Atmospheric Attenuation

### 5.3.1 Beer-Lambert Law

Atmospheric attenuation follows exponential decay:

$$h_a = \exp\left(-\gamma \cdot \frac{H_\beta - H_G}{\cos(\zeta)}\right) \tag{5.3.1}$$

where $\gamma$ is the attenuation coefficient (dB/km) and $H_\beta$ is the effective atmospheric height.

### 5.3.2 Weather Dependence

Table 5.1: Atmospheric Attenuation Coefficients

| **Weather Condition** | **$\gamma$ (dB/km)** | **Visibility (km)** |
|---|---|---|
| Very clear | 0.0 – 0.2 | >50 |
| Clear | 0.2 – 0.5 | 23 – 50 |
| Light haze | 0.5 – 1.0 | 10 – 23 |
| Haze | 1.0 – 2.0 | 4 – 10 |
| Light rain | 2.0 – 4.0 | 2 – 4 |
| Heavy rain | >10 | <1 |

**Relevance:** Nguyen et al. uses $\gamma = 0.43$ dB/km (clear conditions) as baseline.

## 5.4 Atmospheric Turbulence

### 5.4.1 Physical Origin

Atmospheric turbulence arises from temperature variations causing refractive index fluctuations. These fluctuations are characterized by the refractive index structure parameter $C_n^2$, which varies with altitude, time, and location.

### 5.4.2 Hufnagel-Valley Model

The Hufnagel-Valley (H-V) turbulence profile models $C_n^2$ as a function of altitude [16]:

$$C_n^2(h) = 0.00594 \left(\frac{w}{27}\right)^2 (10^{-5}h)^{10} e^{-h/1000} + 2.7 \times 10^{-16} e^{-h/1500} + C_n^2(0) e^{-h/100} \tag{5.4.1}$$

where:

- $w$: RMS wind speed (typically 21 m/s)
- $h$: Altitude in meters
- $C_n^2(0)$: Ground-level turbulence strength

**Turbulence Regimes:**

- Weak: $C_n^2(0) = 5 \times 10^{-15}$ m$^{-2/3}$
- Strong: $C_n^2(0) = 7 \times 10^{-12}$ m$^{-2/3}$

### 5.4.3 Scintillation Index

The Rytov variance characterizes scintillation strength:

$$\sigma_R^2 = 2.25 k^{7/6} \sec^{11/6}(\zeta) \int_{H_G}^{H_S} C_n^2(h) \left(1 - \frac{h - H_G}{H_S - H_G}\right)^{5/6} (h - H_G)^{5/6} dh \tag{5.4.2}$$

## 5.5 Gamma-Gamma Turbulence Model

### 5.5.1 Al-Habash et al. (2001)

Al-Habash, Andrews, and Phillips [16] developed the Gamma-Gamma (GG) distribution for modeling irradiance fluctuations in moderate-to-strong turbulence:

$$f_{h_t}(h_t) = \frac{2(\alpha\beta)^{(\alpha+\beta)/2}}{\Gamma(\alpha)\Gamma(\beta)} h_t^{(\alpha+\beta)/2-1} K_{\alpha-\beta}\left(2\sqrt{\alpha\beta h_t}\right) \tag{5.5.1}$$

where:

- $\alpha, \beta$: Large-scale and small-scale scintillation parameters
- $K_\nu(\cdot)$: Modified Bessel function of the second kind
- $\Gamma(\cdot)$: Gamma function

### 5.5.2 Scintillation Parameters

For spherical wave propagation (satellite downlink):

$$\alpha = \left[\exp\left(\frac{0.49\sigma_R^2}{(1+1.11\sigma_R^{12/5})^{7/6}}\right) - 1\right]^{-1} \tag{5.5.2}$$

$$\beta = \left[\exp\left(\frac{0.51\sigma_R^2}{(1+0.69\sigma_R^{12/5})^{5/6}}\right) - 1\right]^{-1} \tag{5.5.3}$$

### 5.5.3 Physical Interpretation

The GG model treats turbulence as a multiplicative process:

$$h_t = h_X \cdot h_Y \tag{5.5.4}$$

where $h_X \sim \text{Gamma}(\alpha, 1/\alpha)$ (large eddies) and $h_Y \sim \text{Gamma}(\beta, 1/\beta)$ (small eddies).

### 5.5.4 Vasylyev et al. (2016)

Vasylyev, Semenov, and Vogel [17] extended atmospheric channel modeling specifically for quantum communications:

**Key Contributions:**

- Quantum-specific treatment of channel loss
- Entanglement preservation analysis through turbulent channels
- Elliptic beam approximation for realistic beam shapes

## 5.6 Beam Spreading and Wandering

### 5.6.1 Liorni et al. (2019)

Liorni, Kampermann, and Bruß [18] analyzed beam effects on satellite QKD:

**Topics Covered:**

- Diffraction-limited beam spreading
- Turbulence-induced beam wandering
- Combined pointing and tracking effects
- Weather-dependent performance

### 5.6.2 Effective Beam Width

The beam width at the receiver includes diffraction and turbulence contributions:

$$\omega_{eq}^2 = \omega_D^2 \left(1 + \frac{D_{SG}^2}{k^2\omega_0^4} + 1.33\sigma_R^2\Lambda^{5/6}\right) \tag{5.6.1}$$

### 5.6.3 Ma et al. (2015)

Ma et al. [19] analyzed satellite-to-ground coherent optical communications with spatial diversity:

**Relevance to Nguyen et al.:**

- Validated GG distribution for satellite downlinks
- Provided framework for heterodyne detection analysis
- Demonstrated spatial diversity benefits

## 5.7 Channel Model Implementation in Nguyen et al.

### 5.7.1 Combined Channel Coefficient

Nguyen et al. combines all effects into a single channel coefficient:

$$h = h_l \cdot h_a \cdot h_s \cdot h_t \tag{5.7.1}$$

### 5.7.2 Specific Parameter Values

### 5.7.3 Integration with QBER Analysis

The turbulence-affected channel coefficient determines received power:

$$P_R = P_T \cdot G_T \cdot G_R \cdot h \tag{5.7.2}$$

This feeds into SNR calculation and subsequently QBER analysis.

## 5.8 Recent Developments (2020-2025)

### 5.8.1 Fisher-Snedecor F Distribution

Recent experimental data suggest the F distribution may provide better fit across weak-to-strong turbulence than Gamma-Gamma in some scenarios.

Table 5.2: Channel Parameters in Nguyen et al. (2021)

| **Parameter** | **Symbol** | **Value** |
|---|---|---|
| Wavelength | $\lambda$ | 1550 nm |
| Satellite altitude | $H_S$ | 600 km |
| Ground station height | $H_G$ | 5 m |
| Atmospheric height | $H_\beta$ | 20 km |
| Zenith angle | $\zeta$ | 50° |
| Wind speed | $w$ | 21 m/s |
| Beam width at ground | $\omega_D$ | 50 m |
| Attenuation coefficient | $\gamma$ | 0.43 dB/km |
| *Weak Turbulence* | | |
| $C_n^2(0)$ | | $5 \times 10^{-15}$ m$^{-2/3}$ |
| $\alpha$ | | Calculated via Eq. 5.5.2 |
| $\beta$ | | Calculated via Eq. 5.5.3 |
| *Strong Turbulence* | | |
| $C_n^2(0)$ | | $7 \times 10^{-12}$ m$^{-2/3}$ |

### 5.8.2 Machine Learning Approaches

Emerging research applies ML for:

- Channel state prediction
- Adaptive parameter optimization
- Turbulence mitigation

### 5.8.3 Tropical Atmosphere Considerations

For Vietnam and similar regions, specialized modeling may be needed:

- Higher humidity effects
- Monsoon season variability
- Aerosol loading differences

## 5.9 Chapter Summary

This chapter reviewed atmospheric channel modeling literature relevant to Nguyen et al. (2021):

1. **Hufnagel-Valley Model:** Standard altitude-dependent turbulence profile
2. **Gamma-Gamma Distribution:** Primary model for moderate-to-strong turbulence
3. **Scintillation Parameters:** $\alpha$, $\beta$ derived from Rytov variance
4. **Beam Effects:** Spreading and wandering impact on received power

5. **Weather Dependence:** Attenuation varies significantly with conditions

**Key Insight:** Nguyen et al. adopts well-established atmospheric models (GG distribution, H-V profile) providing solid foundation for QBER and KLR analysis.

# Chapter 6

# Detection Schemes and Modulation

*This chapter reviews detection techniques and modulation schemes for optical QKD, with emphasis on coherent detection methods and the dual-threshold approach proposed by PTIT researchers.*

## 6.1 Detection Paradigms in QKD

### 6.1.1 Single-Photon Detection

Traditional DV-QKD relies on single-photon detectors:

Table 6.1: Single-Photon Detector Technologies

| Technology | Wavelength | Efficiency | Dark Count |
|---|---|---|---|
| Si-APD | 850 nm | 50-70% | <100 Hz |
| InGaAs APD | 1550 nm | 10-25% | 1-10 kHz |
| SNSPD | Broadband | >90% | <10 Hz |

**Micius Implementation:** Silicon APDs at 850 nm, providing good efficiency but limiting wavelength choice.

### 6.1.2 Coherent Detection

Coherent detection offers an alternative paradigm:

- **Homodyne:** Measures single quadrature ($X$ or $P$)
- **Heterodyne:** Measures both quadratures simultaneously

**Advantages:**

- Uses standard telecom photodiodes
- Works at 1550 nm (fiber-compatible)
- Higher sensitivity with local oscillator gain
- Compatible with existing coherent communication infrastructure

## 6.2 Heterodyne Detection for QKD

### 6.2.1 Principle of Operation

In heterodyne detection, the signal is mixed with a strong local oscillator (LO) at a slightly different frequency:

$$E_{total} = E_s e^{i\omega_s t + i\phi_s} + E_{LO} e^{i\omega_{LO} t} \tag{6.2.1}$$

The photocurrent contains the beat signal:

$$i(t) \propto 2\sqrt{P_s P_{LO}} \cos((\omega_s - \omega_{LO})t + \phi_s) \tag{6.2.2}$$

### 6.2.2 SNR Enhancement

The LO provides effective amplification:

$$\mathrm{SNR}_{het} = \frac{2\Re^2 P_s P_{LO}}{2q\Re P_{LO} B + \sigma_{th}^2} \tag{6.2.3}$$

For strong LO ($P_{LO} \gg P_s$), shot noise limited operation is achieved.

### 6.2.3 Application to QKD

Research on coherent detection for QKD includes:

- **CV-QKD:** Standard detection method for continuous-variable protocols
- **Discrete-Modulated CV-QKD:** Enables security with QPSK/8PSK modulation
- **PTIT Approach:** Heterodyne detection with dual-threshold decision

## 6.3 Dual-Threshold Detection

### 6.3.1 Trinh et al. (2018)

Trinh et al. [2] introduced dual-threshold detection for QKD over FSO:

**Key Innovation:** Instead of a single decision threshold, two thresholds define three decision regions:

$$\text{Decision} = \begin{cases} 0 & \text{if } i \geq d_0 \\ 1 & \text{if } i \leq d_1 \\ X & \text{if } d_1 < i < d_0 \text{ (erasure)} \end{cases} \tag{6.3.1}$$

### 6.3.2 Threshold Configuration

The thresholds are defined relative to the decision point $d$:

$$d_0 = d + \varsigma \cdot \sigma \tag{6.3.2}$$
$$d_1 = d - \varsigma \cdot \sigma \tag{6.3.3}$$

where $\varsigma$ is the dual-threshold coefficient and $\sigma$ is the noise standard deviation.

### 6.3.3 Trade-off Analysis

Table 6.2: DT Coefficient Trade-offs

| $\varsigma$ **Value** | **QBER** | $P_{sift}$ |
|---|---|---|
| Small (<0.5) | Higher | Higher |
| Optimal (0.7–2.8) | Low | Acceptable |
| Large (>3.0) | Very low | Very low |

### 6.3.4 Evolution: DT/DD to DT/HD

Table 6.3: Detection Scheme Evolution at PTIT

| **Paper** | **Year** | **Detection** | **Improvement** |
|---|---|---|---|
| Trinh et al. | 2018 | DT/DD | Baseline |
| Nguyen et al. | 2021 | DT/HD | +20 dB sensitivity |
| Nguyen et al. | 2023 | DT/HD + CV-QKD | Extended to CV |

## 6.4 Modulation Schemes for QKD

### 6.4.1 Polarization Encoding

Traditional BB84 uses polarization states:

- Rectilinear: $|H\rangle$, $|V\rangle$
- Diagonal: $|D\rangle$, $|A\rangle$

**Advantages:** Direct mapping to BB84 states **Challenges:** Polarization alignment, fiber birefringence

### 6.4.2 Phase Encoding

Phase-encoded QKD maps information to optical phase:

$$|\psi\rangle = \left|\alpha e^{i\phi}\right\rangle \tag{6.4.1}$$

**QPSK for QKD:**

$$\phi \in \left\{\frac{\pi}{4}, \frac{3\pi}{4}, \frac{5\pi}{4}, \frac{7\pi}{4}\right\} \tag{6.4.2}$$

### 6.4.3 Higher-Order Modulation

Research has explored higher-order modulation for QKD:

- **8-PSK:** 3 bits per symbol, higher spectral efficiency
- **16-QAM:** 4 bits per symbol, requires amplitude discrimination
- **Gaussian:** Continuous modulation for CV-QKD

### 6.4.4 QPSK vs. Gaussian

Table 6.4: QPSK vs. Gaussian Modulation for QKD

| Aspect | QPSK (Nguyen) | Gaussian (CV-QKD) |
|---|---|---|
| Alphabet | 4 discrete | Continuous |
| Preparation | Digital | Analog |
| Security proof | Via BB84 | Dedicated CV proofs |
| Implementation | Simpler | More complex |
| Key rate | Moderate | Higher (short dist.) |

## 6.5 Receiver Architecture

### 6.5.1 Nguyen et al. Receiver Design

The proposed DT/HD receiver consists of:

1. **Optical Front-End:**
    - 90° optical hybrid
    - Local oscillator generation
    - Balanced photodetector pair
2. **Electrical Processing:**
    - Transimpedance amplifier
    - Low-pass filter
    - Dual-threshold comparator
3. **Decision Logic:**
    - Three-level output (0, 1, X)
    - Erasure handling
    - Sifting coordination

### 6.5.2 Noise Sources

The receiver noise model includes:

$$\sigma_{total}^2 = \sigma_{shot}^2 + \sigma_{thermal}^2 + \sigma_{dark}^2 \tag{6.5.1}$$

**Shot Noise:**

$$\sigma_{shot}^2 = 2q(\Re P_{LO} + I_d)B \cdot \bar{g}^2 F \tag{6.5.2}$$

**Thermal Noise:**

$$\sigma_{thermal}^2 = \frac{4k_B T B}{R_L} \tag{6.5.3}$$

## 6.6 QBER Analysis

### 6.6.1 Error Probability Derivation

For heterodyne detection with QPSK, the bit error probability:

$$P_e = \int_0^\infty Q\left(\sqrt{\frac{2h \cdot \mathrm{SNR}}{1 + h \cdot \mathrm{SNR}}}\right) f_{h_t}(h)dh \tag{6.6.1}$$

where $Q(\cdot)$ is the Q-function.

### 6.6.2 Conditional QBER

Given successful sifting (non-erasure):

$$\mathrm{QBER} = \frac{P_e}{P_{sift}} \tag{6.6.2}$$

### 6.6.3 Optimal DT Coefficient Ranges

Table 6.5: Optimal $\varsigma$ Ranges from Nguyen et al.

| **Condition** | **$\varsigma$ Range** | **Criterion** |
|---|---|---|
| Weak turbulence | 0.7 – 2.4 | QBER $\leq 10^{-3}$, $P_{sift} \geq 10^{-2}$ |
| Strong turbulence | 1.4 – 2.8 | QBER $\leq 10^{-3}$, $P_{sift} \geq 10^{-2}$ |

## 6.7 Chapter Summary

This chapter reviewed detection and modulation techniques for QKD:

1. **Detection Paradigms:** Single-photon vs. coherent detection trade-offs
2. **Heterodyne Detection:** LO gain provides 20 dB sensitivity improvement
3. **Dual-Threshold:** Erasure region reduces QBER at cost of $P_{sift}$
4. **QPSK Modulation:** Maps BB84 structure to phase states
5. **PTIT Contribution:** DT/HD combination novel for satellite QKD

**Key Innovation:** Nguyen et al.'s DT/HD approach bridges DV and CV paradigms, offering practical implementation advantages while maintaining security based on BB84 structure.

# Chapter 7

# Error Handling and Reliability

*This chapter reviews error handling approaches in QKD, comparing Forward Error Correction (FEC), Automatic Repeat reQuest (ARQ), and hybrid methods, with focus on the retransmission scheme proposed by Nguyen et al.*

## 7.1 Error Correction in QKD

### 7.1.1 The Reconciliation Problem

After quantum transmission, Alice and Bob share correlated but not identical bit strings. Error correction (reconciliation) must:

1. Correct errors between Alice's and Bob's strings
2. Minimize information leakage to Eve
3. Achieve efficiency close to Shannon limit

**Efficiency Metric:**

$$f = \frac{H(A|B)_{actual}}{H(A|B)_{Shannon}} \geq 1 \tag{7.1.1}$$

where $f = 1$ represents Shannon-limited performance.

### 7.1.2 Error Correction Paradigms

Table 7.1: Error Correction Paradigms for QKD

| Paradigm | Direction | Interaction | Example |
|---|---|---|---|
| FEC | One-way | None | LDPC, Polar |
| Interactive | Two-way | Multiple rounds | CASCADE, Winnow |
| Hybrid | Both | Adaptive | LDPC + verification |
| ARQ | Retransmission | ACK/NACK | Nguyen et al. |

## 7.2 CASCADE Protocol

### 7.2.1 Historical Significance

CASCADE, proposed by Brassard and Salvail (1994), was the first practical error correction protocol for QKD.

**Algorithm:**

1. Divide key into blocks of size $k_1$
2. Exchange parities for each block
3. Binary search to locate errors in mismatched blocks
4. Double block size and repeat with shuffling
5. Continue for multiple passes

### 7.2.2 Performance Characteristics

- **Efficiency:** $f \approx 1.16$ (practical implementations)
- **Latency:** High due to interactive nature
- **Throughput:** Limited by round-trip communication

### 7.2.3 Recent Revival

Mueller et al. (2025) [?] demonstrated that optimized CASCADE implementations can achieve:

- Competitive throughput with modern hardware
- Lower latency than previously assumed
- Robustness across varying QBER

## 7.3 LDPC Codes for QKD

### 7.3.1 Low-Density Parity-Check Codes

LDPC codes offer near-Shannon-limit performance:

$$\mathbf{H} \cdot \mathbf{c}^T = \mathbf{0} \tag{7.3.1}$$

where $\mathbf{H}$ is a sparse parity-check matrix.

### 7.3.2 Application to QKD

Milicevic et al. (2018) [?] developed quasi-cyclic multi-edge LDPC codes for long-distance QKD:

**Key Results:**

- 142 km fiber transmission achieved
- Secret key rate: $6.64 \times 10^{-8}$ bits/pulse
- Information throughput: 7.16 kbit/s
- GPU-accelerated decoding

### 7.3.3 Challenges

- **Error Floor:** Performance degradation at low QBER
- **Rate Sensitivity:** Codes optimized for narrow QBER range
- **Complexity:** Encoding/decoding computational overhead

## 7.4 Polar Codes

### 7.4.1 Channel Polarization

Polar codes, invented by Arikan (2009), achieve Shannon capacity through channel polarization:

$$W_N^{(i)} \to \begin{cases} \text{Perfect channel} & \text{as } N \to \infty \\ \text{Useless channel} \end{cases} \tag{7.4.1}$$

### 7.4.2 Application to QKD

Polar codes for QKD reconciliation offer:

- Theoretical capacity achievement
- Successive cancellation decoding
- Lower latency than LDPC in some regimes

### 7.4.3 RC-LDPC-Polar Codes (2024)

Recent work combines LDPC and polar coding advantages:

- Rate-compatible design
- Adaptive to varying channel conditions
- Improved performance over pure approaches

## 7.5 ARQ-Based Reliability: Nguyen et al.

### 7.5.1 Paradigm Shift

Nguyen et al. (2021) introduces a fundamentally different approach—using retransmission rather than error correction:

**Philosophy:**

- Accept transmission failures as inherent to channel
- Retransmit failed sequences rather than correct errors
- Trade latency for simplicity and reliability

### 7.5.2 Protocol Operation

1. Alice generates key sequence, stores in buffer
2. Transmit sequence via FSO channel
3. Bob performs error checking (e.g., CRC or hash)
4. **Success:** Bob sends ACK, Alice discards from buffer
5. **Failure:** Bob sends NACK, Alice retransmits
6. After $M$ failures, sequence is discarded (key loss)

### 7.5.3 Comparison with FEC

Table 7.2: ARQ vs. FEC Comparison

| Aspect | ARQ (Nguyen) | FEC (LDPC) |
|---|---|---|
| Computational overhead | Low | High |
| Latency | Variable | Fixed |
| Adaptability | Channel-adaptive | Rate-fixed |
| Implementation | Simple | Complex |
| Reliability | Controllable via $M$ | Fixed by code |
| Throughput | Reduced | Near-constant |

### 7.5.4 Advantages

1. **Simplicity:** No complex encoder/decoder required
2. **Adaptivity:** Natural adaptation to channel conditions
3. **Flexibility:** Reliability tunable via $M$ parameter
4. **Compatibility:** Works with any modulation scheme

## 7.6 3-D Markov Chain Analysis

### 7.6.1 State Space Definition

Nguyen et al. develops a three-dimensional Markov chain model:

$$\text{State: } (n, s, m) \tag{7.6.1}$$

where:

- $n \in [0, C]$: Buffer queue length ($C$ = capacity)
- $s \in \{B, G\}$: Channel state (Bad, Good)
- $m \in [1, M]$: Retransmission attempt number

### 7.6.2 Transition Probabilities

Key transition probabilities:

- $p_{GB}$: Good → Bad transition
- $p_{BG}$: Bad → Good transition
- $P_{sift}^G$, $P_{sift}^B$: Sifting probabilities in each state

### 7.6.3 Key Loss Rate Derivation

The KLR is derived from steady-state analysis:

$$\text{KLR} = \sum_{s\in\{B,G\}} \pi_{C,s,M} \cdot P_{loss}^s \tag{7.6.2}$$

where $\pi_{n,s,m}$ is the steady-state probability of state $(n, s, m)$.

### 7.6.4 Novel Contribution

This 3-D Markov model is a unique contribution:

- First analytical framework for ARQ in satellite QKD
- Enables closed-form KLR calculation
- Provides optimization insights without extensive simulation

## 7.7 Key Loss Rate Performance

### 7.7.1 KLR vs. Retransmissions

### 7.7.2 Diminishing Returns

**Optimal Choice:** $M = 4$ provides best trade-off between reliability and latency.

Table 7.3: KLR Improvement with Retransmissions

| $M$ | **KLR (Weak)** | **KLR (Strong)** | **Improvement** |
|---|---|---|---|
| 0 | $3 \times 10^{-2}$ | $5 \times 10^{-2}$ | Baseline |
| 1 | $10^{-3}$ | $10^{-2}$ | 30× |
| 2 | $10^{-4}$ | $10^{-3}$ | 300× |
| 4 | $< 10^{-5}$ | $< 10^{-4}$ | >1000× |
| 7 | $< 10^{-6}$ | $< 10^{-5}$ | >10000× |

Table 7.4: Power Gain vs. Retransmission Count

| $M$ **Increase** | **Power Gain** | **Recommendation** |
|---|---|---|
| $1 \rightarrow 2$ | 1.0 dB | Significant |
| $2 \rightarrow 3$ | 0.7 dB | Worthwhile |
| $3 \rightarrow 4$ | 0.5 dB | Marginal |
| $4 \rightarrow 7$ | 0.5 dB total | Not recommended |

## 7.8 Chapter Summary

This chapter reviewed error handling approaches for QKD:

1. **CASCADE:** Interactive protocol, high efficiency, high latency
2. **LDPC:** Near-Shannon performance, complex, rate-sensitive
3. **Polar Codes:** Capacity-achieving, emerging for QKD
4. **ARQ (Nguyen):** Simple, adaptive, controllable reliability
5. **3-D Markov Model:** Novel analytical framework for KLR

**Key Contribution:** Nguyen et al.'s ARQ approach offers a fundamentally different reliability paradigm that trades computational complexity for implementation simplicity and channel adaptivity.

# Chapter 8

# Security Analysis Literature

*This chapter reviews the security analysis literature for practical QKD systems, covering attack models, security proofs, finite-key analysis, and device imperfections.*

## 8.1 QKD Security Framework

### 8.1.1 Information-Theoretic Security

QKD provides security based on physical laws rather than computational assumptions:

- **No-Cloning:** Quantum states cannot be perfectly copied
- **Measurement Disturbance:** Eavesdropping creates detectable errors
- **Unconditional Security:** Secure against unlimited computational power

### 8.1.2 Security Hierarchy

Table 8.1: Attack Classification Hierarchy

| Attack Type | Power | QBER Threshold |
|---|---|---|
| Individual attacks | Weakest | 14.6% |
| Collective attacks | Medium | 11.0% |
| Coherent attacks | Strongest | 7.1% |

## 8.2 Practical Security Framework

### 8.2.1 Scarani et al. (2009)

"The Security of Practical Quantum Key Distribution" [1] established the definitive framework for analyzing practical QKD security:

**Key Contributions:**

1. **Device Imperfection Modeling:**
    - Non-ideal single-photon sources
    - Detector inefficiencies and dark counts
    - Channel losses and noise
2. **Attack Analysis:**
    - Photon-number-splitting attacks
    - Intercept-resend strategies
    - Trojan horse attacks
3. **Security Parameter Calculation:**
    - QBER threshold derivation
    - Privacy amplification requirements
    - Finite-key corrections

### 8.2.2 Relevance to Nguyen et al.

Scarani's framework provides:

- QBER threshold ($10^{-3}$) justification
- Security analysis methodology
- Foundation for URA attack analysis

## 8.3 Finite-Key Security

### 8.3.1 The Finite-Key Challenge

Asymptotic security proofs assume infinite key length. Practical systems require finite-key analysis:

$$l_{secure} = l_{sifted} - \text{leak}_{EC} - \text{leak}_{PE} - \text{PA} \tag{8.3.1}$$

where:

- $\text{leak}_{EC}$: Information leaked during error correction
- $\text{leak}_{PE}$: Information leaked during parameter estimation
- PA: Privacy amplification compression

### 8.3.2 Tomamichel et al. (2012)

"Tight Finite-Key Analysis for Quantum Cryptography" [20] in Nature Communications:

**Key Contributions:**

- Composable security definitions
- Tight bounds on finite-size effects
- Practical parameter optimization

### 8.3.3 Impact on Key Rate

Finite-key effects become significant for:

- Short satellite passes (limited transmission time)
- Low repetition rate systems
- High-loss channels

**Gap in Nguyen et al.:** The paper uses asymptotic analysis; finite-key effects not incorporated.

## 8.4 Realistic Device Security

### 8.4.1 Xu et al. (2020)

"Secure Quantum Key Distribution with Realistic Devices" [11] in Reviews of Modern Physics:

**Coverage:**

1. **Source Imperfections:**
   - Multi-photon emission
   - State preparation flaws
   - Side-channel leakage
2. **Detector Vulnerabilities:**
   - Blinding attacks
   - Time-shift attacks
   - Efficiency mismatch
3. **Countermeasures:**
   - Decoy states for source issues
   - MDI-QKD for detector immunity
   - Device characterization protocols

### 8.4.2 Measurement-Device-Independent QKD

MDI-QKD removes all detector side-channel attacks:

- Bell state measurement at untrusted node
- Security independent of detector imperfections
- Demonstrated over 500 km fiber

## 8.5 CV-QKD Security

### 8.5.1 Leverrier (2015)

"Composable Security Proof for CV-QKD" [7]:

**Contribution:** First composable security proof for Gaussian-modulated CV-QKD with coherent states against collective attacks.

### 8.5.2 Discrete Modulation Security

For QPSK-like discrete modulation:

- Security proofs developed post-2018
- No longer requires linear channel assumption
- Bounded via uncertainty principle methods

**Relevance:** Nguyen et al.'s QPSK approach benefits from these developments.

## 8.6 Security Analysis in Nguyen et al.

### 8.6.1 Unauthorized Receiver Attack (URA)

Nguyen et al. analyzes security against an eavesdropper (Eve) positioned near Bob:

**Attack Model:**

- Eve places receiver within satellite beam footprint
- Bob at beam center ($r = 0$)
- Eve at distance $D_{E-B}$ from Bob

### 8.6.2 Eve's Received Power

Eve's power decreases with distance from beam center:

$$P_{R,Eve} \propto A_0 \exp\left(-\frac{2D_{E-B}^2}{\omega_{Deq}^2}\right) \tag{8.6.1}$$

Table 8.2: Eve's QBER vs. Distance

| $D_{E-B}$ (m) | **Weak Turb.** | **Strong Turb.** | **Security** |
|---|---|---|---|
| 0 | Same as Bob | Same as Bob | Compromised |
| 10 | $\sim 10^{-3}$ | $\sim 10^{-2}$ | Marginal |
| 20 | $\sim 10^{-2}$ | $\sim 10^{-2}$ | Marginal |
| **30** | $> \mathbf{10^{-2}}$ | $> \mathbf{10^{-2}}$ | **Secure** |
| 50+ | $> 10^{-1}$ | $> 10^{-1}$ | Secure |

### 8.6.3 Security Boundary

**Conclusion:** $D_{E-B} > 30$ m ensures Eve cannot obtain usable key.

### 8.6.4 Limitations of Analysis

1. **URA Only:** Does not consider intercept-resend or other attacks
2. **Asymptotic:** Finite-key effects not analyzed
3. **Collective Attacks:** General attack security not proven

## 8.7 Recent Security Developments (2022-2025)

### 8.7.1 Numerical Security Proofs

Physical Review Research (2022) presents numerical security proofs for:

- Decoy-state BB84 with basis misalignment
- MDI-QKD practical implementations
- Fine-grained statistics utilization

### 8.7.2 Finite-Key for Heterodyne (2025)

arXiv:2501.10278 addresses:

- Phase imbalance in heterodyne detection
- Practical finite-key bounds
- System optimization under realistic conditions

### 8.7.3 Post-Quantum Considerations

While QKD is quantum-safe, practical considerations include:

- Authentication channel security
- Key management infrastructure
- Hybrid classical-quantum systems

## 8.8 Chapter Summary

This chapter reviewed security analysis literature:

1. **Foundational Framework:** Scarani et al. established practical security analysis
2. **Finite-Key:** Tomamichel et al. provided composable security with finite resources
3. **Device Security:** Xu et al. addressed realistic device imperfections
4. **CV-QKD:** Leverrier proved composable security for coherent detection
5. **Nguyen et al.:** Analyzed URA scenario; gaps remain in finite-key and general attacks

**Key Gap:** Nguyen et al. provides important URA analysis but would benefit from finite-key analysis and security proof against general attacks.

# Part IV

# Analysis and Synthesis

# Chapter 9

# Comparative Analysis

*This chapter synthesizes the literature reviewed in previous chapters, positioning Nguyen et al. (2021) within the broader context of satellite QKD research and identifying its unique contributions.*

## 9.1 Methodology Comparison

### 9.1.1 Detection Approach Comparison

Table 9.1: Detection Approaches in Satellite QKD Literature

| System | Detection | Wavelength | Sensitivity | Complexity |
|---|---|---|---|---|
| Micius (2017) | SPD (Si-APD) | 850 nm | High | High |
| CV-QKD (Dequal) | Coherent | 1550 nm | Medium | Medium |
| DT/DD (Trinh) | Direct | 1550 nm | Low | Low |
| **DT/HD (Nguyen)** | **Heterodyne** | **1550 nm** | **Very High** | **Medium** |

### 9.1.2 Protocol Comparison

Table 9.2: Protocol Approaches Comparison

| Approach | Modulation | States | Security Basis |
|---|---|---|---|
| BB84 (Micius) | Polarization | 4 | BB84 proof |
| Gaussian CV-QKD | Gaussian | $\infty$ | CV proof |
| Discrete CV-QKD | QPSK/8PSK | 4/8 | CV proof |
| **QPSK-BB84 (Nguyen)** | **Phase** | **4** | **BB84 mapping** |

Table 9.3: Error Handling Approaches

| **Method** | **Type** | **Overhead** | **Adaptivity** | **Implementation** |
|---|---|---|---|---|
| CASCADE | Interactive | High | Low | Complex |
| LDPC | FEC | Medium | Low | Complex |
| Polar | FEC | Medium | Low | Medium |
| **ARQ (Nguyen)** | **Retransmit** | **Low** | **High** | **Simple** |

Table 9.4: Transmitted Power Comparison (QBER $\leq 10^{-3}$)

| **Scheme** | **Required $P_T$** | **Relative Gain** |
|---|---|---|
| SIM/BPSK-DT (Baseline) | 45 dBm | 0 dB |
| QPSK-DT/DD (Trinh 2018) | 35 dBm | 10 dB |
| **QPSK-DT/HD (Nguyen 2021)** | **25 dBm** | **20 dB** |

### 9.1.3 Error Handling Comparison

## 9.2 Performance Comparison

### 9.2.1 Power Requirements

### 9.2.2 Key Rate Comparison

Table 9.5: Key Rate Performance Comparison

| **System** | **Distance** | **Key Rate** | **Status** |
|---|---|---|---|
| Micius (2017) | 530 km | 40.2 kbps sifted | Experimental |
| Micius (2017) | 1034 km | 1.2 kbps sifted | Experimental |
| Chen (2021) | 4600 km | 47.8 kbps | Experimental |
| **Nguyen (2021)** | **600 km (LEO)** | **Simulation** | **Theoretical** |

### 9.2.3 Reliability Comparison

## 9.3 Unique Contributions of Nguyen et al.

### 9.3.1 Novel Elements

1. **First ARQ for Satellite QKD**
   - No prior literature applies retransmission to quantum key distribution
   - Paradigm shift from error correction to error avoidance
   - Enabled by classical feedback channel availability
2. **3-D Markov Chain Model**
   - Novel state space: (buffer, channel, retransmission)
   - Analytical KLR calculation capability

Table 9.6: Reliability Metrics Comparison

| System | Error Handling | Reliability Metric | Value |
|---|---|---|---|
| Micius | LDPC FEC | QBER | 1.1–3.2% |
| Chen Network | Trusted relays | Network availability | >99% |
| **Nguyen** | **ARQ** ($M = 4$) | **KLR** | $< \mathbf{10^{-4}}$ |

- Optimization framework without extensive simulation

3. **DT/HD Integration**
   - First combination of dual-threshold with heterodyne for QKD
   - 20 dB improvement over previous PTIT work
   - Bridges DV and CV detection paradigms

4. **Cross-Layer Design**
   - Physical layer: QPSK + DT/HD
   - Link layer: ARQ retransmission
   - Integrated optimization approach

### 9.3.2 Research Gaps Addressed

Table 9.7: Research Gaps Addressed

| Gap in Literature | Addressed? | How |
|---|---|---|
| Reliability without FEC overhead | ✓ | ARQ scheme |
| Link layer QKD analysis | ✓ | 3-D Markov model |
| Coherent detection for BB84-like | ✓ | QPSK + heterodyne |
| KLR metric formalization | ✓ | Analytical derivation |
| Vietnamese satellite QKD research | ✓ | PTIT contribution |

## 9.4 PTIT Research Evolution

### 9.4.1 Research Timeline

Table 9.8: PTIT Satellite QKD Research Timeline

| Year | Paper | Contribution | Advancement |
|---|---|---|---|
| 2018 | Trinh et al. | DT/DD for QKD | Introduced DT concept |
| 2019 | Vu et al. | HAP-aided relay | Extended to HAP |
| **2021** | **Nguyen et al.** | **DT/HD + ARQ** | **+20 dB + reliability** |
| 2023 | Nguyen et al. | CV-QKD extension | Extended to CV-QKD |
| 2023 | Vu et al. | Network coding | Multi-satellite |

### 9.4.2 Cumulative Contributions

The PTIT research group has systematically:

1. Introduced dual-threshold detection for QKD
2. Improved sensitivity through heterodyne detection
3. Added reliability through retransmission
4. Extended to CV-QKD protocols
5. Explored network-level optimizations

## 9.5 International Context

### 9.5.1 Geographic Distribution of Research

Table 9.9: Satellite QKD Research by Region

| Region | Focus | Key Institutions |
|---|---|---|
| China | Experimental demonstration | USTC, CAS |
| Europe | Mission planning | ESA, DLR, CNES |
| Japan | Ground experiments | NICT, JAXA |
| Canada | LEO development | Waterloo, CSA |
| Singapore | CubeSat QKD | NUS, CQT |
| **Vietnam** | **Theoretical analysis** | **PTIT, VAST** |

### 9.5.2 Vietnamese Position

Vietnam's contribution through PTIT:

- Theoretical foundations for practical systems
- Novel detection and reliability approaches
- Regional capacity building
- Potential foundation for future missions

## 9.6 Critical Assessment

### 9.6.1 Strengths

1. **Novel Integration:** First combination of QPSK, DT/HD, and ARQ
2. **Analytical Rigor:** Comprehensive mathematical framework
3. **Practical Focus:** Realistic system parameters
4. **Significant Improvement:** Quantifiable 20 dB and >1000× gains
5. **Regional Contribution:** Advances Vietnamese research capability

### 9.6.2 Limitations

1. **Simulation Only:** No experimental validation
2. **Idealized Assumptions:**
   - Perfect pointing and tracking
   - No phase noise in local oscillator
   - Ideal modulator/demodulator
3. **Security Gaps:**
   - Asymptotic analysis only
   - Limited attack model (URA)
   - No composable security proof
4. **System Gaps:**
   - Single satellite link
   - No handover consideration
   - No network integration

## 9.7 Chapter Summary

This comparative analysis establishes:

1. **Unique Position:** Nguyen et al. occupies a unique niche combining coherent detection with retransmission reliability
2. **Performance Gains:** 20 dB power improvement and >1000× KLR reduction are significant
3. **Research Gap Filling:** Addresses previously unexplored link-layer reliability for satellite QKD
4. **Foundation Building:** Provides theoretical foundation for future Vietnamese quantum satellite missions
5. **Remaining Work:** Experimental validation and security analysis extensions needed

# Chapter 10

# Research Gaps and Future Directions

*This chapter identifies remaining research gaps in satellite-based QKD reliability improvement and outlines promising future research directions based on the literature synthesis.*

## 10.1 Theoretical Gaps

### 10.1.1 Finite-Key Security Analysis

**Gap:** Nguyen et al. uses asymptotic security analysis. Practical implementations require finite-key bounds.

**Required Work:**

1. Security bounds for practical key lengths ($10^6$–$10^9$ bits)
2. Minimum block size determination for target security
3. Composable security proof incorporating retransmission

**Related Literature:**

- Tomamichel et al. (2012): Finite-key framework
- arXiv:2501.10278 (2025): Finite-key for imperfect heterodyne

### 10.1.2 Advanced Eavesdropper Models

**Gap:** Only Unauthorized Receiver Attack (URA) analyzed. More sophisticated attacks not considered.

**Required Work:**

1. **Collective Attacks:**
    - Eve performs identical operation on each signal
    - Stores quantum memory for later measurement

2. **Coherent Attacks:**
    - Most general attack strategy
    - Joint operation on entire transmission
3. **Side-Channel Attacks:**
    - Timing information leakage
    - Modulator imperfections
    - Detector vulnerabilities

### 10.1.3 Hybrid ARQ-FEC Analysis

**Gap:** Pure ARQ approach may not be optimal for all conditions.

**Research Questions:**

- When does hybrid ARQ+FEC outperform pure ARQ?
- Optimal FEC code rate for retransmission scenarios
- Security implications of hybrid approaches

## 10.2 Practical Implementation Gaps

### 10.2.1 Pointing and Tracking

**Gap:** Perfect beam tracking assumed. Realistic pointing errors not modeled.

**Required Work:**

1. **Pointing Error Model:**
$$h_p = A_0 \exp\left(-\frac{2r_p^2}{\omega_{eq}^2}\right) \tag{10.2.1}$$
where $r_p$ is pointing jitter radius
2. **Acquisition Protocol:**
    - Initial beam acquisition time
    - Tracking loop bandwidth requirements
    - Re-acquisition after interruption
3. **Combined Effects:**
    - Pointing + turbulence interaction
    - Impact on QBER and $P_{sift}$
    - Adaptation of DT coefficient

### 10.2.2 Phase Noise and Synchronization

**Gap:** Ideal local oscillator and perfect phase synchronization assumed.

**Challenges:**

- LO phase noise impact on QPSK detection
- Doppler shift compensation for LEO satellite
- Carrier frequency offset estimation

### 10.2.3 Experimental Validation

**Gap:** All results are simulation-based.

**Validation Pathway:**

1. **Component Level:**
   - QPSK modulator characterization
   - DT/HD receiver implementation
   - APD performance verification
2. **Subsystem Level:**
   - End-to-end link demonstration
   - ARQ protocol implementation
   - Buffer management testing
3. **System Level:**
   - Ground testbed with emulated satellite channel
   - Turbulence chamber testing
   - Field trials (ground-to-ground)

## 10.3 System-Level Gaps

### 10.3.1 LEO Constellation Integration

**Gap:** Single satellite link analyzed. Constellation operation not considered.

**Research Directions:**

1. **Multi-Satellite Coverage:**
   - Optimal constellation design for Vietnam
   - Coverage overlap analysis
   - Handover frequency estimation
2. **Handover Protocols:**

- Key continuity during handover
- Buffer management across satellites
- Retransmission state transfer

3. **Key Routing:**
   - Inter-satellite key relay
   - Trusted node requirements
   - Network key rate optimization

### 10.3.2 Hybrid FSO/RF Architecture

**Gap:** Pure FSO system assumed. Backup RF channel not integrated.

**Opportunities:**

- RF backup during weather outages
- Classical channel for ACK/NACK (already assumed)
- Hybrid key management protocols

### 10.3.3 Network Integration

**Gap:** Stand-alone QKD system. Integration with existing networks not addressed.

**Considerations:**

- Key management system integration
- Classical encryption interoperability
- Network protocol stack placement

## 10.4 Future Research Directions

### 10.4.1 Near-Term (1–2 Years)

1. **Finite-Key Analysis Extension**
   - Incorporate finite-size corrections into QBER analysis
   - Determine minimum key length for target security level
   - Optimize block size for satellite pass duration
2. **Pointing Error Integration**
   - Add realistic pointing jitter model
   - Analyze combined pointing and turbulence effects
   - Develop adaptive DT coefficient adjustment
3. **Ground Testbed Development**

- Implement QPSK modulator and DT/HD receiver
- Validate with emulated satellite channel
- Demonstrate ARQ protocol operation

### 10.4.2 Medium-Term (3–5 Years)

1. **Machine Learning Integration**
    - Channel state prediction for proactive parameter adjustment
    - Optimal DT coefficient selection via reinforcement learning
    - Anomaly detection for security monitoring
2. **LEO Constellation Analysis**
    - Multi-satellite coverage optimization for Vietnam
    - Handover protocol development
    - Key routing algorithm design
3. **Tropical Atmosphere Modeling**
    - Vietnam-specific turbulence profiles
    - Monsoon season characterization
    - Optimal ground station site selection

### 10.4.3 Long-Term (5+ Years)

1. **Vietnamese Quantum Satellite Mission**
    - Payload design based on PTIT research
    - Ground station network development
    - International collaboration framework
2. **Regional Quantum Network**
    - ASEAN quantum connectivity
    - Cross-border secure communication
    - Regional standards development
3. **Quantum Internet Integration**
    - Entanglement-based protocols
    - Quantum repeater integration
    - Global quantum network participation

Table 10.1: Proposed Research Roadmap

| **Activity** | **Timeline** | **Priority** | **Dependencies** |
|---|---|---|---|
| Finite-key analysis | Year 1 | High | None |
| Pointing error model | Year 1 | High | None |
| Component testbed | Year 1–2 | High | Funding |
| ML integration study | Year 2–3 | Medium | Testbed |
| Tropical atmosphere | Year 2–3 | Medium | Field data |
| Constellation design | Year 3–4 | Medium | Analysis tools |
| Satellite mission design | Year 4–5 | Low | All above |
| Regional network | Year 5+ | Low | Mission |

## 10.5 Research Roadmap

## 10.6 Chapter Summary

This chapter identified research gaps and future directions:

**Critical Gaps:**

1. Finite-key security analysis
2. Pointing and tracking effects
3. Experimental validation

**Important Gaps:**

1. Advanced attack models
2. LEO constellation integration
3. Hybrid ARQ-FEC optimization

**Future Opportunities:**

1. Machine learning for adaptive optimization
2. Vietnamese quantum satellite mission
3. Regional quantum network development

The research by Nguyen et al. provides a solid foundation for continued development toward practical satellite QKD systems.

# Chapter 11

# Conclusion

*This chapter synthesizes the key findings from this comprehensive literature review, summarizes the contributions of Nguyen et al. (2021), and provides final recommendations for future research.*

## 11.1 Literature Review Summary

This literature review examined 85+ papers spanning four decades of quantum key distribution research, organized into four thematic parts:

### 11.1.1 Part I: Introduction and Paper Analysis

- Established the context for satellite-based QKD research
- Provided detailed technical analysis of Nguyen et al. (2021)
- Identified system architecture, innovations, and key results

### 11.1.2 Part II: Theoretical Foundations

- **Foundational Protocols:** BB84, E91, CV-QKD, and decoy states
- **Satellite Experiments:** Micius achievements and integrated networks
- **Key Insight:** Nguyen et al. builds upon established foundations while introducing novel reliability mechanisms

### 11.1.3 Part III: Technical Aspects

- **Channel Models:** Gamma-Gamma turbulence, Hufnagel-Valley profile
- **Detection Schemes:** Heterodyne detection, dual-threshold approach
- **Error Handling:** CASCADE, LDPC, polar codes, and ARQ
- **Security:** Practical security frameworks and finite-key analysis

### 11.1.4 Part IV: Analysis and Synthesis

- **Comparative Analysis:** Positioned Nguyen et al. within broader literature
- **Research Gaps:** Identified theoretical, practical, and system-level gaps
- **Future Directions:** Outlined near-term to long-term research roadmap

## 11.2 Key Findings

### 11.2.1 Nguyen et al. (2021) Contributions

The paper makes four significant contributions to satellite-based QKD:

Table 11.1: Summary of Paper Contributions

| **Contribution** | **Type** | **Impact** |
|---|---|---|
| QPSK-based QKD with DT/HD | Physical Layer | 20 dB power improvement |
| Key retransmission scheme | Link Layer | >1000× KLR reduction |
| 3-D Markov chain model | Analytical | Enables optimization |
| Comprehensive analysis | System | Practical guidelines |

### 11.2.2 Quantitative Results

Table 11.2: Summary of Quantitative Results

| **Metric** | **Result** |
|---|---|
| Power improvement vs. SIM/BPSK | 20 dB |
| KLR improvement with $M = 4$ | >1000× |
| Optimal DT coefficient (weak turbulence) | 0.7 – 2.4 |
| Optimal DT coefficient (strong turbulence) | 1.4 – 2.8 |
| Security distance (Eve-Bob) | >30 m |
| Optimal retransmission count | $M = 4$ |

### 11.2.3 Unique Position in Literature

Nguyen et al. occupies a unique position by:

1. Being the **first** to apply ARQ retransmission to satellite QKD
2. Providing the **first** 3-D Markov chain model for link-layer QKD analysis
3. Achieving **highest sensitivity** through DT/HD combination
4. Demonstrating **cross-layer optimization** (physical + link layer)

## 11.3 Critical Assessment

### 11.3.1 Strengths

1. **Novel Integration:** First work combining QPSK, DT/HD, and ARQ for satellite QKD
2. **Practical Focus:** Realistic system parameters based on LEO satellite configuration
3. **Analytical Rigor:** Mathematical framework enables performance prediction without extensive simulation
4. **Significant Improvement:** Quantifiable gains that could enable practical deployment
5. **Vietnamese Contribution:** Advances regional research capability in quantum communications

### 11.3.2 Limitations

1. **Simulation Only:** No experimental validation of theoretical predictions
2. **Idealized Pointing:** Perfect beam tracking assumed
3. **Asymptotic Security:** Finite-key effects not analyzed
4. **Single Link:** No constellation or handover consideration
5. **Simplified Eavesdropper:** Only URA scenario analyzed

## 11.4 Recommendations

### 11.4.1 For Researchers

1. **Priority 1 - Finite-Key Analysis:**
   - Extend security analysis to practical key lengths
   - Determine minimum block sizes for target security levels
2. **Priority 2 - Experimental Validation:**
   - Develop ground testbed for DT/HD receiver
   - Validate ARQ protocol with emulated channel
3. **Priority 3 - Pointing Integration:**
   - Add realistic pointing error models
   - Analyze combined turbulence and pointing effects

### 11.4.2 For Practitioners

1. Use $M = 4$ retransmissions as optimal starting point
2. Select DT coefficient based on turbulence regime (0.7–2.8 range)
3. Consider DT/HD approach for telecom-compatible implementations
4. Plan for >30 m security perimeter around ground stations

### 11.4.3 For Policymakers

1. Support experimental validation of Vietnamese QKD research
2. Consider satellite QKD in national quantum communication strategy
3. Explore regional cooperation for ASEAN quantum network
4. Invest in ground station infrastructure development

## 11.5 Future Outlook

### 11.5.1 Technology Trajectory

Satellite QKD is progressing from experimental demonstrations toward operational deployment:

- **2025-2026:** Eagle-1, QUBE-II, expanded Chinese constellation
- **2027:** Chinese MEO satellite, global service announcement
- **2030+:** Quantum internet backbone integration

### 11.5.2 Vietnamese Opportunity

Vietnam has opportunity to participate in this development through:

- Continued theoretical research building on PTIT foundation
- Ground station development and characterization
- Regional collaboration with ASEAN partners
- Potential contribution to international missions

### 11.5.3 Role of Nguyen et al. (2021)

The work by Nguyen et al. provides:

- Theoretical foundation for Vietnamese satellite QKD development
- Novel approaches (ARQ, 3-D Markov) applicable to broader community
- Framework for future experimental validation
- Basis for continued research advancement

## 11.6 Final Remarks

Nguyen et al. (2021) represents a significant contribution to satellite-based QKD research, particularly from the Vietnamese research community. The paper addresses a practical challenge—reliability improvement—through a novel combination of physical layer optimization (QPSK-DT/HD) and link layer mechanisms (ARQ retransmission).

The 20 dB power improvement and >1000× KLR reduction demonstrated in simulation suggest that the proposed approach could enable more practical satellite QKD systems. The analytical 3-D Markov chain model provides a valuable framework for system design and optimization that has not been previously available in the literature.

While experimental validation remains necessary before practical deployment, the work establishes a solid foundation for future Vietnamese contributions to global quantum communication research. As satellite QKD moves toward operational deployment in the coming years, the reliability techniques developed here may prove essential for practical system implementation.

This literature review has situated Nguyen et al. within the broader context of 40 years of QKD research, identified its unique contributions, and outlined pathways for continued advancement. The field of satellite-based quantum communication holds great promise for enabling truly secure global communications, and Vietnamese researchers are positioned to contribute meaningfully to this important endeavor.

---

*This comprehensive literature review was prepared as part of the Master's program in Space & Earth Observation at USTH, December 2025.*

# Part V

# Appendices

# Appendix A

# Key Equations Reference

This appendix provides a consolidated reference of key equations from Nguyen et al. (2021) and the supporting literature.

## A.1 Channel Model Equations

### A.1.1 Combined Channel Coefficient

$$h = h_l \cdot h_a \cdot h_s \cdot h_t \tag{A.1}$$

### A.1.2 Free-Space Path Loss

$$h_l = \left(\frac{\lambda}{4\pi D_{SG}}\right)^2 \tag{A.2}$$

### A.1.3 Slant Range

$$D_{SG} = \sqrt{(H_S - H_G)^2 \sec^2(\zeta) + 2R_E(H_S - H_G)\sec(\zeta)} \tag{A.3}$$

### A.1.4 Atmospheric Attenuation

$$h_a = \exp\left(-\gamma \cdot \frac{H_\beta - H_G}{\cos(\zeta)}\right) \tag{A.4}$$

### A.1.5 Hufnagel-Valley Turbulence Profile

$$C_n^2(h) = 0.00594\left(\frac{w}{27}\right)^2 (10^{-5}h)^{10} e^{-h/1000} + 2.7 \times 10^{-16} e^{-h/1500} + C_n^2(0) e^{-h/100} \tag{A.5}$$

### A.1.6 Rytov Variance

$$\sigma_R^2 = 2.25k^{7/6}\sec^{11/6}(\zeta)\int_{H_G}^{H_S} C_n^2(h)\left(1-\frac{h-H_G}{H_S-H_G}\right)^{5/6}(h-H_G)^{5/6}dh \tag{A.6}$$

### A.1.7 Gamma-Gamma Distribution

$$f_{h_t}(h_t) = \frac{2(\alpha\beta)^{(\alpha+\beta)/2}}{\Gamma(\alpha)\Gamma(\beta)} h_t^{(\alpha+\beta)/2-1} K_{\alpha-\beta}\left(2\sqrt{\alpha\beta h_t}\right) \tag{A.7}$$

### A.1.8 Scintillation Parameters

$$\alpha = \left[\exp\left(\frac{0.49\sigma_R^2}{(1+1.11\sigma_R^{12/5})^{7/6}}\right)-1\right]^{-1} \tag{A.8a}$$

$$\beta = \left[\exp\left(\frac{0.51\sigma_R^2}{(1+0.69\sigma_R^{12/5})^{5/6}}\right)-1\right]^{-1} \tag{A.8b}$$

## A.2 Detection Equations

### A.2.1 QPSK Phase States

$$\phi_A \in \left\{\frac{\pi}{4}, \frac{3\pi}{4}, \frac{5\pi}{4}, -\frac{\pi}{4}\right\} \tag{A.9}$$

### A.2.2 Dual-Threshold Decision

$$\text{Decision} = \begin{cases} 0 & \text{if } i \geq d_0 \\ 1 & \text{if } i \leq d_1 \\ X & \text{otherwise (erasure)} \end{cases} \tag{A.10}$$

### A.2.3 Threshold Configuration

$$d_0 = d + \varsigma \cdot \sigma \tag{A.11a}$$

$$d_1 = d - \varsigma \cdot \sigma \tag{A.11b}$$

### A.2.4 Received Power

$$P_R = P_T \cdot G_T \cdot G_R \cdot h \tag{A.12}$$

### A.2.5 SNR for Heterodyne Detection

$$\text{SNR} = \frac{(\Re P_R \bar{g})^2}{\sigma_{shot}^2 + \sigma_{thermal}^2} \tag{A.13}$$

### A.2.6 Noise Variances

$$\sigma_{shot}^2 = 2q(\Re P_{LO} + I_d)B \cdot \bar{g}^2 F \tag{A.14a}$$

$$\sigma_{thermal}^2 = \frac{4k_B TB}{R_L} \tag{A.14b}$$

## A.3 QBER Equations

### A.3.1 Bit Error Probability

$$P_e = \int_0^\infty Q\left(\sqrt{\frac{2h \cdot \text{SNR}}{1 + h \cdot \text{SNR}}}\right) f_{h_t}(h)dh \tag{A.15}$$

### A.3.2 Q-Function

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-t^2/2} dt \tag{A.16}$$

### A.3.3 Conditional QBER

$$\text{QBER} = \frac{P_e}{P_{sift}} \tag{A.17}$$

### A.3.4 Sifting Probability

$$P_{sift} = P(|i - d| > \varsigma\sigma) = 1 - P_{erasure} \tag{A.18}$$

## A.4 Markov Chain Model Equations

### A.4.1 State Space Definition

$$\text{State: } (n, s, m) \text{ where } n \in [0, C], s \in \{B, G\}, m \in [1, M] \tag{A.19}$$

### A.4.2 Channel Transition Probabilities

$$P(G \to B) = p_{GB} \quad (A.20a)$$
$$P(B \to G) = p_{BG} \quad (A.20b)$$

### A.4.3 Steady-State Distribution

$$\boldsymbol{\pi} = \boldsymbol{\pi}\mathbf{P} \quad (A.21)$$

### A.4.4 Key Loss Rate

$$\text{KLR} = \sum_{s \in \{B,G\}} \pi_{C,s,M} \cdot P^{s}_{loss} \quad (A.22)$$

## A.5 Security Equations

### A.5.1 Eve's Received Power

$$P_{R,Eve} = P_T \cdot G_T \cdot G_R \cdot h \cdot A_0 \exp\left(-\frac{2D^2_{E-B}}{\omega^2_{Deq}}\right) \quad (A.23)$$

### A.5.2 Secure Key Rate (Asymptotic)

$$R_{secure} = R_{sift} \cdot [1 - H(\text{QBER}) - f \cdot H(\text{QBER})] \quad (A.24)$$

### A.5.3 Binary Entropy Function

$$H(p) = -p\log_2(p) - (1-p)\log_2(1-p) \quad (A.25)$$

## A.6 Notation Reference

Table A.1: Symbol Notation Reference

| Symbol | Description | Units |
|---|---|---|
| $h$ | Total channel coefficient | – |

*Continued on next page*

*Continued from previous page*

| Symbol | Description | Units |
|---|---|---|
| $h_l$ | Free-space path loss | – |
| $h_a$ | Atmospheric attenuation | – |
| $h_s$ | Beam spreading loss | – |
| $h_t$ | Turbulence fading coefficient | – |
| $D_{SG}$ | Satellite-to-ground distance | m |
| $H_S$ | Satellite altitude | m |
| $H_G$ | Ground station height | m |
| $\zeta$ | Zenith angle | rad |
| $\gamma$ | Attenuation coefficient | dB/km |
| $C_n^2$ | Refractive index structure parameter | $\mathrm{m}^{-2/3}$ |
| $\sigma_R^2$ | Rytov variance | – |
| $\alpha, \beta$ | Gamma-Gamma parameters | – |
| $\varsigma$ | Dual-threshold coefficient | – |
| $P_T$ | Transmitted power | W (or dBm) |
| $P_R$ | Received power | W |
| $G_T, G_R$ | Telescope gains | dB |
| $\Re$ | Photodetector responsivity | A/W |
| $\bar{g}$ | APD multiplication factor | – |
| $B$ | Bandwidth | Hz |
| QBER | Quantum bit error rate | – |
| $P_{sift}$ | Sifting probability | – |
| KLR | Key loss rate | – |
| $M$ | Maximum retransmissions | – |
| $C$ | Buffer capacity | sequences |

# Appendix B

# Literature Database

This appendix provides a comprehensive database of papers reviewed in this literature review, organized by category and relevance tier.

## B.1 Tier 1: Essential Papers

These papers are fundamental to understanding satellite-based QKD and directly relevant to Nguyen et al. (2021).

Table B.1: Tier 1 Essential Papers

| # | Authors | Title | Year | Journal |
|---|---|---|---|---|
| 1 | Nguyen et al. | Reliability improvement of satellite-based QKD using retransmission | 2021 | Photonic Net. Comm. |
| 2 | Chen et al. | Integrated space-to-ground quantum network over 4,600 km | 2021 | Nature |
| 3 | Liao et al. | Satellite-to-ground quantum key distribution | 2017 | Nature |
| 4 | Yin et al. | Satellite-based entanglement distribution over 1200 km | 2017 | Science |
| 5 | Dequal et al. | Feasibility of satellite CV-QKD | 2021 | npj Quantum Info. |
| 6 | Trinh et al. | DT/DD for QKD over FSO | 2018 | IEEE Access |
| 7 | Pirandola et al. | Advances in quantum cryptography | 2020 | Adv. Opt. Photon. |
| 8 | Nguyen et al. | CV-QKD with DT/HD scheme | 2023 | IEEE Access |

## B.2 Tier 2: Important Papers

These papers provide essential context and technical foundations.

Table B.2: Tier 2 Important Papers

| # | Authors | Title | Year | Journal |
|---|---|---|---|---|
| 9 | Scarani et al. | Security of practical QKD | 2009 | Rev. Mod. Phys. |
| 10 | Xu et al. | Secure QKD with realistic devices | 2020 | Rev. Mod. Phys. |
| 11 | Tomamichel et al. | Tight finite-key analysis | 2012 | Nature Comm. |
| 12 | Vasylyev et al. | Atmospheric quantum channels | 2016 | Phys. Rev. A |
| 13 | Liorni et al. | Satellite QKD beam and weather effects | 2019 | New J. Phys. |
| 14 | Ma et al. | Satellite downlink Gamma-Gamma | 2015 | Appl. Opt. |
| 15 | Orsucci et al. | Practical satellite QKD architectures | 2025 | Int. J. Sat. Comm. |
| 16 | Mueller et al. | CASCADE and LDPC for QKD | 2025 | IET Quantum Comm. |
| 17 | Liao et al. | Intercontinental quantum network | 2018 | Phys. Rev. Lett. |

## B.3 Tier 3: Supporting Papers

These papers provide additional technical depth and context.

Table B.3: Tier 3 Supporting Papers

| # | Authors | Title | Year | Journal |
|---|---|---|---|---|
| 18 | Al-Habash et al. | Gamma-Gamma distribution derivation | 2001 | Opt. Eng. |
| 19 | Grosshans et al. | CV-QKD with coherent states | 2003 | Nature |
| 20 | Leverrier | Composable security for CV-QKD | 2015 | Phys. Rev. Lett. |
| 21 | Milicevic et al. | Quasi-cyclic LDPC for QKD | 2018 | npj Quantum Info. |
| 22 | Kish et al. | CV-QKD satellite feasibility | 2020 | Quantum Eng. |
| 23 | Various | LEO constellation networking | 2022 | Entropy |
| 24 | Various | Greek LEO QKD infrastructure | 2021 | Photonics |

## B.4 Tier 4: Reference Papers

These foundational papers provide historical and theoretical context.

Table B.4: Tier 4 Reference Papers

| # | Authors | Title | Year | Journal |
|---|---|---|---|---|
| 25 | Bennett & Brassard | BB84 protocol | 1984 | IEEE Conf. |
| 26 | Ekert | E91 protocol | 1991 | Phys. Rev. Lett. |
| 27 | Gisin et al. | Quantum cryptography review | 2002 | Rev. Mod. Phys. |
| 28 | Bedington et al. | Progress in satellite QKD | 2017 | npj Quantum Info. |
| 29 | Kaushal & Kaddoum | Space optical communication | 2017 | IEEE Comm. Surv. |
| 30 | Pan et al. | Micius experiments review | 2022 | Rev. Mod. Phys. |

## B.5 Vietnamese/PTIT Research Papers

Papers from Vietnamese institutions, particularly PTIT.

Table B.5: Vietnamese/PTIT Research Papers

| # | Authors | Title | Year | Venue |
|---|---|---|---|---|
| V1 | Trinh et al. | DT/DD for QKD over FSO | 2018 | IEEE Access |
| V2 | Vu et al. | HAP-aided satellite QKD | 2019 | VTC Spring |
| V3 | Nguyen et al. | Reliability with retransmission | 2021 | Photonic Net. Comm. |
| V4 | Nguyen et al. | CV-QKD with DT/HD | 2023 | IEEE Access |
| V5 | Vu et al. | Network coding EB/PM QKD | 2023 | ITC-CSCC |

## B.6 Papers by Category

### B.6.1 Foundational QKD Protocols

- Bennett & Brassard (1984) - BB84
- Ekert (1991) - E91
- Grosshans et al. (2003) - CV-QKD
- Gisin et al. (2002) - Review

### B.6.2 Satellite QKD Experiments

- Liao et al. (2017) - Micius first QKD
- Yin et al. (2017) - Entanglement distribution

- Liao et al. (2018) - Intercontinental QKD
- Chen et al. (2021) - Integrated network
- Pan et al. (2022) - Micius review

### B.6.3 Atmospheric Channel Models

- Al-Habash et al. (2001) - Gamma-Gamma
- Vasylyev et al. (2016) - Quantum channels
- Liorni et al. (2019) - Weather effects
- Ma et al. (2015) - Satellite downlink
- Kaushal & Kaddoum (2017) - Space optical

### B.6.4 Detection and Modulation

- Trinh et al. (2018) - DT/DD
- Nguyen et al. (2021) - DT/HD
- Nguyen et al. (2023) - CV-QKD DT/HD
- Dequal et al. (2021) - CV-QKD satellite

### B.6.5 Error Correction

- Milicevic et al. (2018) - LDPC
- Mueller et al. (2025) - CASCADE vs LDPC
- Various (2024) - RC-LDPC-Polar

### B.6.6 Security Analysis

- Scarani et al. (2009) - Practical security
- Tomamichel et al. (2012) - Finite-key
- Xu et al. (2020) - Realistic devices
- Leverrier (2015) - CV-QKD security

### B.6.7 Recent Advances (2022-2025)

- Orsucci et al. (2025) - Architecture assessment
- Mueller et al. (2025) - Industrial reconciliation
- Various (2025) - Finite-key heterodyne
- LEO constellation studies (2022-2024)

Table B.6: High-Citation Papers in Review

| Paper | Est. Citations | Year |
|---|---|---|
| Bennett & Brassard (BB84) | >15,000 | 1984 |
| Gisin et al. (Review) | >5,000 | 2002 |
| Ekert (E91) | >5,000 | 1991 |
| Scarani et al. (Security) | >4,000 | 2009 |
| Liao et al. (Micius) | >2,500 | 2017 |
| Yin et al. (Entanglement) | >2,000 | 2017 |
| Pirandola et al. (Review) | >1,500 | 2020 |
| Chen et al. (Network) | >1,000 | 2021 |
| Grosshans et al. (CV-QKD) | >1,000 | 2003 |
| Xu et al. (Devices) | >800 | 2020 |

## B.7 Citation Statistics

## B.8 Paper Access Information

### B.8.1 Open Access Sources

- **arXiv:** Most physics papers available (arxiv.org)
- **PubMed Central:** Some biomedical-related papers
- **IEEE Xplore:** Some open access articles
- **Nature/Science:** Selected open access papers

### B.8.2 Institutional Access

- USTH library portal
- VAST institutional subscriptions
- Inter-library loan services

### B.8.3 DOI References

Key DOIs for direct access:

- Nguyen et al. (2021): 10.1007/s11107-021-00934-y
- Chen et al. (2021): 10.1038/s41586-020-03093-8
- Liao et al. (2017): 10.1038/nature23655
- Pirandola et al. (2020): 10.1364/AOP.361502
- Trinh et al. (2018): 10.1109/ACCESS.2018.2796046

# Bibliography


[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Reviews of Modern Physics*, vol. 81, no. 3, pp. 1301–1350, 2009.

[2] P. V. Trinh, T. V. Pham, N. T. Dang, H. V. Nguyen, S. X. Ng, and A. T. Pham, "Design and security analysis of QKD protocol over free-space optics using dual-threshold/direct-detection receiver," *IEEE Access*, vol. 6, pp. 4159–4175, 2018.

[3] T. V. Nguyen, M. Q. Vu, H. T. T. Phan, N. T. Dang, and A. T. Pham, "Enhancing design and performance analysis of satellite CV-QKD free space system using dual-threshold/heterodyne scheme," *IEEE Access*, vol. 11, pp. 111 890–111 904, 2023.

[4] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, 1984, pp. 175–179.

[5] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Physical Review Letters*, vol. 67, no. 6, pp. 661–663, 1991.

[6] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using Gaussian-modulated coherent states," *Nature*, vol. 421, no. 6920, pp. 238–241, 2003.

[7] A. Leverrier, "Composable security proof for continuous-variable quantum key distribution with coherent states," *Physical Review Letters*, vol. 114, no. 7, p. 070501, 2015.

[8] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li *et al.*, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, no. 7670, pp. 43–47, 2017.

[9] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of Modern Physics*, vol. 74, no. 1, pp. 145–195, 2002.

[10] 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," *Advances in Optics and Photonics*, vol. 12, no. 4, pp. 1012–1236, 2020.

[11] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices," *Reviews of Modern Physics*, vol. 92, no. 2, p. 025002, 2020.

[12] J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai *et al.*, "Satellite-based entanglement distribution over 1200 kilometers," *Science*, vol. 356, no. 6343, pp. 1140–1144, 2017.

[13] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu *et al.*, "Satellite-relayed intercontinental quantum network," *Physical Review Letters*, vol. 120, no. 3, p. 030501, 2018.

[14] Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen *et al.*, "An integrated space-to-ground quantum communication network over 4,600 kilometres," *Nature*, vol. 589, no. 7841, pp. 214–219, 2021.

[15] H. Kaushal and G. Kaddoum, "Optical communication in space: Challenges and mitigation techniques," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 57–96, 2017.

[16] M. A. Al-Habash, L. C. Andrews, and R. L. Phillips, "Mathematical model for the irradiance probability density function of a laser beam propagating through turbulent media," *Optical Engineering*, vol. 40, no. 8, pp. 1554–1562, 2001.

[17] D. Vasylyev, A. A. Semenov, and W. Vogel, "Atmospheric quantum channels with weak and strong turbulence," *Physical Review A*, vol. 94, no. 1, p. 012311, 2016.

[18] C. Liorni, H. Kampermann, and D. Bruß, "Satellite-based links for quantum key distribution: beam effects and weather dependence," *New Journal of Physics*, vol. 21, no. 9, p. 093055, 2019.

[19] J. Ma, K. Li, L. Tan, S. Yu, and Y. Cao, "Performance analysis of satellite-to-ground downlink coherent optical communications with spatial diversity over Gamma-Gamma atmospheric turbulence," *Applied Optics*, vol. 54, no. 25, pp. 7575–7585, 2015.

[20] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, "Tight finite-key analysis for quantum cryptography," *Nature Communications*, vol. 3, p. 634, 2012.

[21] N. D. Nguyen, H. T. T. Phan, H. T. T. Pham, V. V. Mai, and N. T. Dang, "Reliability improvement of satellite-based quantum key distribution systems using retransmission scheme," *Photonic Network Communications*, vol. 42, pp. 53–64, 2021.

[22] J.-W. Pan *et al.*, "Micius quantum experiments in space," *Reviews of Modern Physics*, vol. 94, no. 3, p. 035001, 2022.

[23] D. Dequal, L. Trigo Vidarte, V. Rodriguez Roman, G. Vallone, P. Villoresi, A. Leverrier, and E. Diamanti, "Feasibility of satellite-to-ground continuous-variable quantum key distribution," *npj Quantum Information*, vol. 7, p. 3, 2021.

[24] S. P. Kish, E. Villaseñor, R. A. Malaney, K. A. Mudge, and K. J. Grant, "Feasibility assessment for practical continuous variable quantum key distribution over the satellite-to-earth channel," *Quantum Engineering*, vol. 2, no. 3, p. e50, 2020.

[25] M. Q. Vu, N. T. Dang, and A. T. Pham, "HAP-aided relaying satellite FSO/QKD systems for secure vehicular networks," in *IEEE 89th Vehicular Technology Conference (VTC-2019 Spring)*. Kuala Lumpur, Malaysia: IEEE, 2019.

[26] M. Q. Vu, H. D. Le, N. T. Dang, and A. T. Pham, "Network coding aided hybrid EB/PM satellite-based FSO/QKD systems," in *International Technical Conference on Circuits/Systems, Computers, and Communications (ITC-CSCC 2023)*, Jeju, Korea, 2023.

[27] M. Milicevic, C. Feng, L. M. Zhang, and P. G. Gulak, "Quasi-cyclic multi-edge LDPC codes for long-distance quantum cryptography," *npj Quantum Information*, vol. 4, p. 21, 2018.

[28] R. Mueller *et al.*, "Performance of Cascade and LDPC codes for information reconciliation on industrial quantum key distribution systems," *IET Quantum Communication*, 2025.

[29] R. Bedington, J. M. Arrazola, and A. Ling, "Progress in satellite quantum key distribution," *npj Quantum Information*, vol. 3, p. 30, 2017.

[30] D. Orsucci *et al.*, "Assessment of practical satellite QKD architectures for current and near-future missions," *International Journal of Satellite Communications and Networking*, 2025.

[31] Various, "Networking feasibility of quantum key distribution constellation networks," *Entropy*, vol. 24, no. 2, p. 298, 2022.

[32] ——, "LEO satellites constellation-to-ground QKD links: Greek quantum communication infrastructure paradigm," *Photonics*, vol. 8, no. 12, p. 544, 2021.