People's Democratic Republic of Algeria
الجمهورية الجزائرية الديمقراطية الشعبية
Ministry of Higher Education and Scientific Research
وزارة التعليم العالي والبحث العلمي

Ferhat Abbas University
Setif 1
Faculty of Sciences
Department of Computer Science

جامعة فرحات عباس سطيف 1
كلية العلوم
قسم الإعلام الآلي

Master's thesis

FOR THE OBTAINMENT OF THE MASTER'S DEGREE IN COMPUTER SCIENCE

Speciality: Quantum Computing

Physics-Aware Performance Evaluation of Satellite-to-Ground Photonic Quantum Communication Links in Low Earth Orbit

Author:
Manar Boumendjel

Supervised by:
Dr. Hichem Talbi

Defended on June 23, 2026, before the jury composed of:

Dr. Safia Djemmam Zazoua (U. Setif 1 Ferhat Abbas)	: President
Pr. Karima Berkane(U. Setif 1 Ferhat Abbas)	: Examiner
Dr. Hichem Talbi (U. Constantine 2 Abdelhamid Mehri)	: Supervisor

Academic Year: 2025/2026

Abstract

Quantum Key Distribution (QKD) provides a fundamentally secure method for cryptographic key exchange by exploiting the principles of quantum mechanics. While terrestrial QKD systems have demonstrated secure communication over moderate distances, optical fiber attenuation limits their scalability. Satellite-based quantum communication has therefore emerged as a promising approach for extending secure quantum networks to regional and global scales. This thesis presents a physics-aware performance evaluation of satellite-to-ground photonic quantum communication links operating in Low Earth Orbit (LEO) environments. An integrated simulation framework was developed to establish a direct relationship between orbital geometry, free-space optical propagation, atmospheric channel effects, receiver characteristics, photon detection statistics, and BB84 QKD performance. The proposed framework incorporates key physical impairments affecting quantum signal transmission, including free-space diffraction losses, beam divergence, atmospheric attenuation, detector inefficiencies, dark counts, and background noise. Using these models, important performance metrics such as detection probability, Quantum Bit Error Rate (QBER), Secure Key Rate (SKR), and link availability were evaluated under realistic operating conditions. Simulation results indicate that system performance is strongly dependent on satellite elevation angle and channel transmittance. Free-space geometric losses were identified as the dominant impairment, while detector performance and background noise significantly influence secure key generation. Furthermore, secure key generation was found to be concentrated near the high-elevation portion of the satellite pass, where channel conditions are most favorable. The developed framework provides a useful tool for analyzing the interaction between physical propagation effects and quantum communication performance, contributing to the design and optimization of future satellite-based quantum communication systems.

Keywords: Quantum Communication; Quantum Key Distribution (QKD); BB84 Protocol; Satellite Quantum Communication; Low Earth Orbit (LEO); Free-Space Optical Communication; Quantum Bit Error Rate (QBER); Secure Key Rate (SKR).

Résumé

La Distribution Quantique de Clés (QKD) constitue une méthode fondamentalement sécurisée d'échange de clés cryptographiques fondée sur les principes de la mécanique quantique. Les limitations des réseaux terrestres, principalement dues à l'atténuation des fibres optiques, font des communications quantiques par satellite une solution prometteuse pour étendre les réseaux quantiques sécurisés à grande échelle. Cette thèse présente une évaluation des performances des liaisons de communication quantique photonique entre un satellite en orbite terrestre basse (LEO) et une station au sol, en tenant compte des principaux phénomènes physiques influençant la transmission des signaux quantiques. Un cadre de simulation intégré a été développé afin de relier la géométrie orbitale, la propagation optique en espace libre, les effets atmosphériques, les caractéristiques des détecteurs et les performances du protocole BB84. Les indicateurs de performance, notamment la probabilité de détection, le taux d'erreur binaire quantique (QBER), le taux de clé sécurisée (SKR) et la disponibilité de la liaison, ont été évalués dans des conditions réalistes. Les résultats montrent que les performances du système dépendent fortement de l'angle d'élévation du satellite et de la transmittance du canal. Les pertes géométriques en espace libre constituent le principal facteur limitant, tandis que les performances des détecteurs et le bruit de fond influencent significativement la génération de clés sécurisées, principalement lors des phases de forte élévation du satellite. Le cadre proposé constitue un outil pertinent pour analyser et optimiser les futurs systèmes de communication quantique par satellite.

Mots-clés : Communication quantique ; Distribution Quantique de Clés (QKD) ; Protocole BB84 ; Communication quantique par satellite ; Orbite terrestre basse (LEO) ; Communication optique en espace libre ; Taux d'erreur binaire quantique (QBER) ; Taux de clé sécurisée (SKR).

الملخص

يوفر توزيع المفاتيح الكمومية (QKD) وسيلةً آمنةً بشكلٍ جوهري لتبادل المفاتيح التشفيرية من خلال استغلال مبادئ ميكانيكا الكم. ورغم أن أنظمة توزيع المفاتيح الكمومية الأرضية أثبتت قدرتها على تحقيق اتصالات آمنة عبر مسافات متوسطة، فإن التوهين الذي تعاني منه الألياف الضوئية يحد من قابليتها للتوسع. ولذلك برز الاتصال الكمومي عبر الأقمار الصناعية كحل واعد لتوسيع شبكات الاتصال الكمومي الآمنة على المستويين الإقليمي والعالمي. تقدم هذه الأطروحة تقييماً للأداء يعتمد على الخصائص الفيزيائية لوصلات الاتصال الكمومي الفوتوني بين الأقمار الصناعية والمحطات الأرضية العاملة في بيئات المدار الأرضي المنخفض (LEO). وقد تم تطوير إطار محاكاة متكامل يربط بصورة مباشرة بين الهندسة المدارية، وانتشار الضوء في الفضاء الحر، وتأثيرات القناة الجوية، وخصائص المستقبل، وإحصائيات كشف الفوتونات، وأداء بروتوكول توزيع المفاتيح الكمومية BB84. ويتضمن الإطار المقترح أهم العوامل الفيزيائية المؤثرة في انتقال الإشارات الكمومية، بما في ذلك خسائر الحيود في الفضاء الحر، وتباعد الحزمة الضوئية، والتوهين الجوي، وعدم كفاءة الكواشف، والعدّات المظلمة، وضوضاء الخلفية. وباستخدام هذه النماذج, تم تقييم مجموعة من مؤشرات الأداء المهمة مثل احتمال الكشف، ومعدل خطأ البتات الكمومية (QBER)، ومعدل المفتاح الآمن (SKR)، وإتاحة الوصلة في ظل ظروف تشغيل واقعية. وتشير نتائج المحاكاة إلى أن أداء النظام يعتمد بدرجة كبيرة على زاوية ارتفاع القمر الصناعي ونفاذية القناة. كما تبين أن الخسائر الهندسية في الفضاء الحر تمثل العامل الأكثر تأثيراً، في حين تؤثر خصائص الكواشف وضوضاء الخلفية بصورة ملحوظة في توليد المفاتيح الآمنة. بالإضافة إلى ذلك، أظهرت النتائج أن توليد المفاتيح الآمنة يتركز بالقرب من الجزء ذي زاوية الارتفاع العالية من مسار القمر الصناعي، حيث تكون ظروف القناة أكثر ملاءمة. ويوفر إطار المحاكاة المطور أداةً فعالة لتحليل التفاعل بين تأثيرات الانتشار الفيزيائية وأداء أنظمة الاتصال الكمومي، مما يسهم في تصميم وتحسين أنظمة الاتصال الكمومي المستقبلية المعتمدة على الأقمار الصناعية.

الكلمات المفتاحية: الاتصال الكمومي؛ توزيع المفاتيح الكمومية (QKD)؛ بروتوكول BB84؛ الاتصال الكمومي عبر الأقمار الصناعية؛ المدار الأرضي المنخفض (LEO)؛ الاتصال البصري في الفضاء الحر؛ معدل خطأ البتات الكمومية (QBER)؛ معدل المفتاح الآمن (SKR).

Contents

Introduction **1**

1 Background and Motivation for Satellite-Based Quantum Communication **4**

1.1 Motivation 4

1.1.1 The Importance of Secure Communication 4

1.1.2 The Quantum Computing Threat to Classical Cryptography . . 5

1.1.3 Quantum Key Distribution as a Long-Term Solution 6

1.2 Quantum Communication Overview 6

1.2.1 Photons as Quantum Information Carriers 6

1.2.2 Fundamental Quantum Principles 8

1.2.3 Classical vs Quantum Communication Paradigms 8

1.3 Quantum Key Distribution (QKD) Overview 9

1.3.1 The Alice–Bob–Eve Security Model 9

1.3.2 Information-Theoretic Security in QKD 11

1.4 The BB84 Protocol — Conceptual Introduction 12

1.4.1 Basic Working Principle of BB84 12

1.4.2 Basis Selection and Measurement 13

1.4.3 Sifting and Key Agreement Process 14

1.5 Limitations of Fiber-Based QKD 15

1.5.1 Exponential Loss in Optical Fibers 15

1.5.2 Distance Limitations and the Repeater Problem 16

1.6 Satellite QKD as a Solution 17

1.6.1 Free-Space Optical Links as an Alternative 17

1.6.2 The Micius Experiment: First Demonstration of Space QKD . . 18

1.6.3 Low Earth Orbit (LEO) as the Optimal Platform 19

2 Satellite-to-Ground Quantum Communication System Model **21**

2.1 System Overview 21

2.1.1 Overall Architecture of the Satellite-to-Ground Link 22

2.1.2 Functional Components and Their Roles 23

2.2 Free-Space Optical Propagation 24

2.2.1 Gaussian Beam Propagation Model 24

2.2.2 Geometric (Diffraction) Loss 25

2.3 Beam Divergence and Pointing Loss 26

2.3.1 Beam Spreading Over Long Distances . . . 27
2.3.2 Pointing Error and Misalignment Loss . . . 27
2.4 Atmospheric Channel Model . . . 29
2.4.1 Molecular Absorption and Aerosol Scattering . . . 29
2.4.2 Atmospheric Turbulence Effects . . . 31
2.4.3 Background Noise and Sky Radiance . . . 32
2.5 LEO Satellite Geometry . . . 33
2.5.1 Orbital Altitude and Slant Range . . . 34
2.5.2 Elevation Angle and Temporal Variation . . . 35
2.5.3 Visibility Window of the Link . . . 36
2.6 Receiver Model . . . 38
2.6.1 Optical Telescope and Collection Efficiency . . . 38
2.6.2 Spectral and Spatial Filtering . . . 40
2.6.3 Single-Photon Detector Characteristics . . . 42
2.7 Total Link Transmittance Model . . . 43
2.7.1 Overall System Transmission Efficiency . . . 43
2.7.2 Summary of Loss Contributions . . . 44

3 QKD Protocol Modeling and Performance Metrics 48
3.1 BB84 Protocol Implementation Model . . . 49
3.1.1 Integration of the BB84 Protocol with the Physical Channel Model 49
3.1.2 End-to-End BB84 Communication Process . . . 50
3.1.3 Photon Encoding and Basis Selection . . . 52
3.1.4 Transmission and Measurement Procedure . . . 53
3.1.5 Raw Key Generation . . . 53
3.2 Photon Detection Statistics . . . 54
3.2.1 Photon Number Statistics . . . 54
3.2.2 Signal Detection Probability . . . 54
3.2.3 Dark Count Detection Probability . . . 55
3.2.4 Background Noise Detection Probability . . . 55
3.2.5 Total Detection Probability . . . 55
3.3 Quantum Bit Error Rate (QBER) Model . . . 56
3.3.1 Definition of Quantum Bit Error Rate . . . 56
3.3.2 Sources of QBER in Satellite QKD Systems . . . 56
3.3.3 Analytical QBER Model . . . 57
3.3.4 Impact of Channel Conditions on QBER . . . 58
3.4 Secure Key Rate Formulation . . . 58
3.4.1 Secret Key Generation in BB84 . . . 58
3.4.2 Asymptotic Secure Key Rate Model . . . 59

3.4.3 QBER Threshold for Positive Key Generation 60
3.4.4 Dependence on Channel Conditions 60
3.4.5 Classical Post-Processing in Secure Key Generation 61

4 Simulation Framework, Results, and Discussion 62
4.1 Simulation Framework 62
4.1.1 Overall Simulation Framework 62
4.1.2 System Parameters and Assumptions 63
4.1.3 Simulation Workflow 65
4.2 Simulation Scenarios 67
4.2.1 Elevation-Angle Scenarios 67
4.2.2 Atmospheric Condition Scenarios 68
4.2.3 Detector Performance Scenarios 71
4.2.4 Summary of Simulated Configurations 72
4.3 Results and Performance Evaluation 74
4.3.1 Link Transmittance During a Satellite Pass 74
4.3.2 Photon Detection Probability Analysis 75
4.3.3 QBER Performance Analysis 77
4.3.4 Secure Key Rate Performance 78
4.3.5 Link Availability Analysis 79
4.4 Sensitivity Analysis and Discussion 81
4.4.1 Sensitivity to System Parameters 81
4.4.2 Dominant Sources of Performance Degradation 82
4.4.3 Comparison with Published Results 83
4.5 Key Findings and Practical Implications 85
4.5.1 Concluding Remarks 85

Conclusion 87