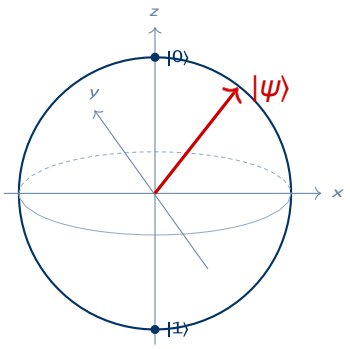
People's Democratic Republic of Algeria
Ferhat Abbas University — Sétif 1
Faculty of Sciences • Department of Computer Science

Master's Thesis

Domaine : Informatique | Specialisation : Quantum Computing

Intercept–Resend Attack in Single-Photon Protocol

Analysis, Simulation, and Security Evaluation of the BB84 Quantum Key Distribution Protocol



Bloch sphere



Presented by :

Arab Rahma

Beldjerou Youcef Achraf Eddine

Supervised by :

Berrah Smail

Professor, Departement of Computer Science

Jury Members

Prof. GHERBI Abdelhakim	Univ. Abderrahmane Mira –Bejaia	President
Prof. BERRAH Smail	Univ. Abderrahmane Mira –Bejaia	Supervisor
Dr. ADNANE Hamza	Univ. Akli Mohand Oulhadj –Bouira	Examiner

Academic Year : 2025–2026

Dedication

Praise be to Allah at the beginning and at the end. Praise be to Allah, by whose grace all good deeds are accomplished, and who enabled me to complete this work after much effort and perseverance. Peace and blessings be upon our Prophet Muhammad , the best of creation and the most honorable of messengers, and upon his family and companions.

To that version of myself who struggled greatly and never gave up, who spent long nights among codes, experiments, and books. To the days when the road was long but hope was even longer, and to every moment of doubt that I overcame by trying once again...

I dedicate this work to my family, who were the quiet support behind every step I took, and to everyone who offered me a kind word when I needed it most, without even realizing its impact.

To my supervisor, Prof. Smail Berrah, who guided this work with his valuable advice, sound scientific guidance, and continuous support. Whose knowledge and expertise had a significant impact on the completion of this thesis; to him, I express my sincere gratitude, appreciation, and respect.

To my esteemed teachers, who not only taught us knowledge, but also taught us how to search, how to think, and how to persevere despite difficulties.

And to every dream that started small and grew through patience and faith, I dedicate this humble work, praying to Allah for success in all that lies ahead. Praise be to Allah, first and last.

— Rahma

إلى من كلّله الله بالهيبة والوقار، إلى من أحمل اسمه بكل فخر، وساندني في كل خطوة... والدي العزيز. حفظك الله ورعاك وأطال في عمرك.

إلى الروح الطاهرة التي غادرتنا إلى دار البقاء، إلى من يسكن طيفها وجداني ودعائي، وأتمنى لو كانت هنا لتشهد قطاف ثمار غرسها... أمي الغالية (رحمها الله وغفر لها وأسكنها فسيح جناته).

إلى من بهم يشتدّ عضدي وتزدهر أيامّي، إخوتي وسندي في الحياة: أخي العزيز إياد، أختي الغالية ملاك. أتمنى لكم مستقبلا مَّشرقا مَّليئا بَّالنجاح والتوفيق.

إلى نبع البركة والدعاء المستجاب، إلى منبع الحنان والوقار... جدي العزيز وجدتي الغالية. أدام الله صحتكم وعافيتكم وحفظكم لنا ذخرًا.

إلى من تقاسمتُ معها كفاح هذا العمل، وكانت نعم الرفيقة والمثابرة في مشوار التحدي... رحمة. شكرا ً لكِ على طيب التعاون والجهد المشترك لشغلنا هذا.

إلى من شاركوني المسير، وقاسموني سهر الليالي، ومرارة التعب وحلاوة النجاح... أصدقائي الأوفياء. شكرا ً لأنكم كنتم نعم العون والرفقة في هذا الطريق الدراسي.

أهديكم جميعا ثَّمرة هذا الجهد والتخرج.

--- أشرف

Acknowledgements

We express our deepest gratitude to our thesis supervisor, Prof. Smail Berrah, for his continuous guidance, invaluable advice, and unwavering support throughout this research. Their expertise in quantum cryptography and information security provided the foundation upon which this work was built.

We extend our sincere thanks to the members of the jury for accepting to evaluate this thesis and for their constructive observations.

Our appreciation goes to all professors at the Department of Computer Science, Faculty of Sciences, University Ferhat Abbas – Sétif 1, whose dedicated teaching formed the scientific bedrock of this work.

Finally, we acknowledge the pioneering researchers in quantum cryptography – Bennett, Brassard, Shor, Preskill, and others – whose foundational contributions made this field possible.

Résumé

Ce mémoire présente une analyse approfondie de l'attaque *Intercept–Resend* appliquée au protocole BB84 de distribution quantique de clés (QKD) utilisant des photons uniques. En exploitant les principes fondamentaux de la mécanique quantique — la superposition, le principe de no-cloning et la perturbation par mesure — nous démontrons comment l'espion Eve introduit des erreurs détectables dans le canal quantique.

Nous dérivons analytiquement que l'attaque Intercept–Resend produit un Taux d'Erreur de Bit Quantique (QBER) théorique de 25% lorsque Eve intercepte tous les photons. Une simulation Python complète du protocole BB84, avec et sans attaque, valide ces résultats théoriques. De plus, une simulation optique sous OptiSystem modélise l'impact des paramètres physiques — distance de transmission, débit binaire et longueur d'onde — sur les performances du système.

Mots-clés: Cryptographie quantique, QKD, BB84, Photon unique, Attaque Intercept–Resend, QBER, Sécurité de l'information.

Abstract

This thesis presents a comprehensive analysis of the Intercept–Resend attack on the BB84 Quantum Key Distribution (QKD) protocol using single-photon sources. By leveraging the fundamental principles of quantum mechanics — superposition, the no-cloning theorem, and measurement-induced disturbance — we demonstrate how an eavesdropper (Eve) introduces statistically detectable errors into the quantum channel.

We analytically derive that the Intercept–Resend attack produces a theoretical Quantum Bit Error Rate (QBER) of 25% when Eve intercepts all transmitted photons. A comprehensive Python-based simulation of the BB84 protocol, with and without Eve's presence, validates these theoretical predictions. Additionally, an optical simulation in OptiSystem models the impact of physical channel parameters — transmission distance, bit rate, and wavelength — on system performance.

The results confirm that the BB84 protocol provides robust detection of eavesdropping when QBER thresholds are properly enforced, and that single-photon implementations face inherent trade-offs between transmission distance and key generation rate. Countermeasures including privacy amplification and quantum repeaters are discussed.

Keywords: Quantum cryptography, QKD, BB84, Single photon, Intercept–Resend attack, QBER, Information security.

الملخص

يقدم هذا البحث تحليلاً شاملاً لهجوم الاعتراض-وإعادة الإرسال (Intercept–Resend) على بروتوكول توزيع المفتاح الكمي BB84 باستخدام مصادر الفوتون الواحد. بالاعتماد على المبادئ الأساسية لميكانيكا الكم --- التراكب الكمي، ونظرية عدم الاستنساخ، والاضطراب الناتج عن القياس --- نوضح كيف يمكن للمتنصت (Eve) أن يُحدث أخطاء قابلة للكشف إحصائياً في القناة الكمية.

نشتق تحليلياً أن هجوم الاعتراض-وإعادة الإرسال ينتج نسبة خطأ كمية نظرية (QBER) مقدارها 25% عندما تعترض إيف جميع الفوتونات المرسلة. محاكاة شاملة باستخدام لغة بايثون لبروتوكول BB84، بحضور إيف وبدونها، تتحقق من صحة هذه التنبؤات النظرية. بالإضافة إلى ذلك، تقوم محاكاة بصرية في برنامج OptiSystem بنمذجة تأثير المعايير الفيزيائية للقناة --- مسافة الإرسال، ومعدل البت، والطول الموجي --- على أداء النظام.

تؤكد النتائج أن بروتوكول BB84 يوفر كشفاً قوياً لعملية التنصت عند تطبيق عتبات نسبة الخطأ الكمي بشكل صحيح، وأن تطبيقات الفوتون الواحد تواجه مقايضات متأصلة بين مسافة الإرسال ومعدل توليد المفتاح. يتم مناقشة الإجراءات المضادة بما في ذلك تضخيم الخصوصية والمكررات الكمية.

الكلمات المفتاحية: التشفير الكمي، توزيع المفتاح الكمي، BB84، الفوتون الواحد، هجوم الاعتراض-وإعادة الإرسال، نسبة الخطأ الكمي، أمن المعلومات.

Contents

List of Abbreviations xiii

General Introduction xiv

1 Foundations of Quantum Cryptography 1

1.1 Introduction . . . 1
1.2 Limitations of Classical Cryptography . . . 1
1.2.1 Symmetric Cryptography . . . 1
1.2.2 Public-Key Cryptography and Its Vulnerabilities . . . 2
1.3 Fundamentals of Quantum Mechanics for Cryptography . . . 2
1.3.1 Qubits . . . 2
1.3.2 Superposition . . . 3
1.3.3 Measurement Principle . . . 4
1.3.4 No-Cloning Theorem . . . 4
1.4 Quantum Key Distribution (QKD) . . . 5
1.4.1 General Concept . . . 5
1.4.2 Security Principles . . . 5
1.5 BB84 Protocol . . . 5
1.5.1 Protocol Description . . . 6
1.5.2 Polarization Bases . . . 6
1.5.3 Key Sifting Process . . . 7
1.5.4 Error Estimation . . . 7
1.6 Single Photon Implementation . . . 8
1.6.1 Photon Source . . . 8
1.6.2 Optical Fiber Transmission . . . 8
1.6.3 Detection System . . . 9
1.7 Conclusion . . . 9

2 Intercept–Resend Attack Analysis 10

2.1 Introduction . . . 10
2.2 Eavesdropping in QKD Systems . . . 10
2.3 Intercept–Resend Attack Principle . . . 11

2.3.1 Attack Scenario 11
2.3.2 Eve's Measurement Strategy 11
2.3.3 Resending Process 12
2.4 Mathematical Analysis of the Attack 12
2.4.1 Probability Calculations 12
2.4.2 Error Rate Derivation 12
2.5 Quantum Bit Error Rate (QBER) 13
2.5.1 Definition 13
2.5.2 QBER Without Attack 13
2.5.3 QBER Under Attack 13
2.6 Detection of the Attack 14
2.6.1 Threshold Values 14
2.6.2 Security Implications 14
2.7 Comparison with Other Attacks 15
2.7.1 Photon Number Splitting (PNS) Attack 15
2.7.2 Trojan Horse Attack 15
2.7.3 Time-Shift Attack 16
2.7.4 Collective and Coherent Attacks 16
2.8 Conclusion 16

3 Simulation and Implementation **17**
3.1 Introduction 17
3.2 Simulation Environment 18
3.2.1 Python Tools 18
3.2.2 OptiSystem Software 18
3.3 BB84 Simulation in Python 18
3.3.1 System Modeling 18
3.3.2 Key Generation Process 20
3.3.3 QBER Computation 20
3.4 Implementation of Intercept–Resend Attack 21
3.4.1 Modeling Eve 21
3.4.2 Impact on Key Rate 22
3.4.3 Error Analysis 23
3.5 Optical Fiber Simulation using OptiSystem 24
3.5.1 Transmission Distance Effect 24
3.5.2 Bit Rate Variation 25
3.5.3 Wavelength Influence 26
3.6 Results and Discussion 28

3.6.1 Graphical Analysis 28
3.6.2 Performance Comparison 30
3.7 Conclusion 31

4 Security Evaluation and Improvements **33**
4.1 Security Assessment 33
4.2 Limitations of Single Photon Protocol 35
4.3 Possible Countermeasures 35
4.4 Future Research Directions 36

General Conclusion **37**

A Complete Python Source Code **41**
A.1 Main Simulation File 41

B Simulation Parameters **44**

C Additional Graphs **45**

D Practical OptiSystem Simulation of BB84 (With and Without Attack) **46**
D.1 Introduction 46
D.2 Simulation Setup 47
D.2.1 Without Attack 47
D.2.2 With Attack (Eve Present) 47
D.3 Initial Results and Identified Inconsistency 48
D.4 Corrected Simulation 49
D.4.1 Parameter Correction 49
D.4.2 Corrected Results 49
D.5 Conclusion 50