Algerian Republic Democratic and Popular

Ministry of High Education and Scientific Research

Farhat Abbes Setif-1 University

Departement of Computer Science

Master Thesis

Field: Computer Science

Speciality: Quantum Computing

Title:

’’Quantum Key Distribution Inspired by DNA Encoding: A Novel Approach to Secure Communication’’

Presented by :

- RIDJALLINE Nabil
- MAYOUF Idriss

Directed by :

- **Dr. ACHIRI Leila**

Jury members :

- Dr. DJEMMAM Safia (MC. Univ. Ferhat Abbas. Sétif 1)
- Dr. KIDAR Halima Saadia (MC. Univ. Ferhat Abbas. Sétif 1)

Promotion 2024/2025

Abstract

This thesis explores the development of a hybrid cryptographic model that integrates **quantum cryptography** with **DNA-based encryption** to address the growing demand for secure communication in the face of emerging quantum threats. The study begins with a comprehensive review of classical, modern, and DNA-inspired cryptographic methods, highlighting their theoretical foundations and evaluating their resilience against contemporary security challenges.

Building upon this background, the thesis introduces the fundamental concepts of quantum computing—such as qubits, entanglement, and superposition—which are essential for understanding quantum key distribution (QKD) protocols. Special focus is given to the BB84 protocol, analyzing its operational mechanics, security guarantees, and vulnerability to eavesdropping.

The core contribution lies in the simulation of the BB84 protocol under two scenarios: with and without the presence of an eavesdropper. The generated quantum key is then utilized in a DNA-based encryption and decryption process, wherein classical data is encoded into synthetic DNA sequences using predefined biological mapping rules. This hybrid approach demonstrates enhanced security by combining the physical robustness of quantum mechanics with the structural complexity of DNA encoding.

The study concludes by summarizing key findings, acknowledging current limitations, and proposing future directions for optimizing and implementing the model in practical environments. The results highlight the potential of interdisciplinary cryptographic systems in building resilient security architectures for the post-quantum era.

Keywords: Quantum computing, Quantum cryptography, DNA encryption, Quantum key distribution (QKD), BB84 protocol, Secure communication

الملخص

يتناول هذا البحث تطوير نموذج تشفير هجين يجمع بين **التشفير الكمي والتشفير القائم على الحمض النووي(DNA)** ، بهدف الاستجابة للحاجة المتزايدة إلى وسائل اتصال آمنة في ظل التهديدات المتصاعدة الناتجة عن تطور الحوسبة الكمومية. يبدأ البحث بمراجعة شاملة لأساليب التشفير الكلاسيكية والحديثة، إضافةً إلى التشفير القائم على ال -DNA، مع تسليط الضوء على الأسس النظرية وآليات العمل ومواطن القوة والضعف لكل منها في سياق التحديات الأمنية المعاصرة.

يقدّم البحث بعد ذلك المبادئ الأساسية للحوسبة الكمومية مثل الكيوبتات، والتشابك الكمومي، والتراكب، والتي تُعد ضرورية لفهم بروتوكولات التشفير الكمي، مع التركيز بشكل خاص على **بروتوكول BB84** ، من خلال تحليل آليته التشغيلية، وضماناته الأمنية، وإمكانية تعرضه للتنصت.
أما المساهمة الأساسية للرسالة فتتمثل في محاكاة بروتوكول BB84 في حالتي وجود متنصت (المعروفة بشخصية "إيف") وغيابه، حيث يُستخدم المفتاح الناتج عن التوزيع الكمي في عملية تشفير وفك تشفير البيانات باستخدام ترميز قائم على الـ DNA ، يتم تحويل البيانات إلى تسلسلات DNA صناعية باستخدام قواعد ترميز بيولوجية محددة مسبقًا، مما يضيف طبقة أمنية إضافية من التعقيد البيولوجي.
يختتم البحث بتلخيص النتائج الرئيسية، ومناقشة التحديات والقيود الحالية، واقتراح اتجاهات بحث مستقبلية لتحسين وتطوير هذا النموذج الهجين. وتُظهر النتائج إمكانات الأنظمة التشفيرية متعددة التخصصات في بناء بنى أمنية قوية وموثوقة في عصر ما بعد الكم.

الكلمات المفتاحية: الحوسبة الكمومية، التشفير الكمومي، تشفير الحمض النووي(DNA) ، توزيع المفاتيح الكمومية(QKD) ، بروتوكولBB84 ، الاتصال الآمن.

Résumé
Ce mémoire porte sur le développement d'un modèle cryptographique hybride combinant la **cryptographie quantique** et le **chiffrement basé sur l'ADN**, afin de répondre aux besoins croissants en communication sécurisée face aux menaces émergentes de l'informatique quantique. L'étude commence par une revue complète des méthodes de cryptographie classique, moderne et inspirée de l'ADN, en mettant en lumière leurs fondements théoriques, mécanismes de fonctionnement, ainsi que leurs avantages et limites dans le contexte des défis actuels en cybersécurité.
Le mémoire introduit ensuite les principes fondamentaux de l'informatique quantique, tels que les qubits, l'intrication quantique et la superposition, indispensables à la compréhension des protocoles de distribution de clés quantiques (QKD). Une attention particulière est portée au protocole **BB84**, dont les mécanismes, garanties de sécurité et vulnérabilités face à l'espionnage sont analysés en profondeur.
La contribution principale du travail réside dans la simulation du protocole BB84 dans deux scénarios : en présence et en absence d'un espion (souvent nommé "Eve"). La clé générée est ensuite utilisée dans un processus de chiffrement et déchiffrement fondé sur l'ADN, où les données sont encodées sous forme de séquences d'ADN synthétique selon des règles de correspondance biologique prédéfinies. Cette approche hybride permet de renforcer la sécurité en combinant la solidité physique de la mécanique quantique avec la complexité structurelle du codage ADN.
L'étude se conclut par un résumé des résultats obtenus, une discussion des limitations du modèle proposé et des pistes futures pour son amélioration et sa mise en œuvre concrète. Les résultats mettent en évidence le potentiel des systèmes cryptographiques interdisciplinaires pour bâtir des architectures de sécurité robustes à l'ère post-quantique.

Mots-clés : Informatique quantique, Cryptographie quantique, Cryptage ADN, Distribution de clé quantique (QKD), Protocole BB84, Communication sécurisée.

Table of Contents