TÉCNICO LISBOA

Design and Implementation of an Authenticated Post-Quantum Key Exchange Protocol

An Adaptation of the Encrypted Key Exchange Protocol using CRYSTALS-Kyber

Master's degree in Telecommunications and Informatics Engineering

Author:
Inês Martins Ribeiro

Professor
Prof. Ricardo Chaves

Indíce

1 Introduction 1

2 State of the Art 1

2.1 Encrypted Key Exchange (EKE) . . . 1

2.2 Post-Quantum cryptography (PQC) . . . 1

2.3 CRYSTALS-Kyber . . . 1

3 Proposed Design: PQ-EKE with Kyber 1

3.1 Architecture Overview . . . 1

3.2 Protocol Flow . . . 1

4 Implementation 1

4.1 Development Environment . . . 1

4.2 Core functionalities . . . 1

4.3 Simulation . . . 1

5 Security Analysis 1

6 Conclusion 1

1 Introduction

Write about the MOTIVATION: the current threat of quantum computers to classical cryptography, the need for post-quantum cryptography, etc.
Problem Statement: Why classical key exchange neeed to evolve
Objectives: Design and implement an authenticated post-quantum key exchange protocol based on EKE and CRYSTALS-Kyber

2 State of the Art

2.1 Encrypted Key Exchange (EKE)

2.2 Post-Quantum cryptography (PQC)

2.3 CRYSTALS-Kyber

3 Proposed Design: PQ-EKE with Kyber

3.1 Architecture Overview

3.2 Protocol Flow

4 Implementation

4.1 Development Environment

4.2 Core functionalities

4.3 Simulation

5 Security Analysis

6 Conclusion