CHAPTER 1
INTRODUCTION

The research background, the main problems found, and the research objectives of this master's thesis entitled Post-Quantum Cryptography Based on Kyber-Dilithium Signcryption for IoT Smart Home are explained in this chapter. The hypothesis of this research is also presented, and furthermore, an overview of the research methods used is conveyed in this chapter.

1.1 Background

The usefulness of the internet allows people to exchange information, where currently information exchange is not only carried out by people to people but also people to machines or vice versa and also machine to machine. The Internet of Things (IoT) is one of the products of the development of the internet that is currently used by society. IoT consists of sensors that are connected to process data and then present it to users through applications that can be accessed using the internet network. IoT can be implemented in many things based on the purpose of its use, one example is the smart home.

Smart homes are generally implemented with the aim of controlling and monitoring the home environment remotely. The increase in the use of smart homes has turned the home environment into a complex digital ecosystem, where every device in the smart home system sends data to users through the internet network, so that users can easily control and monitor the condition of the home environment. Smart homes are considered to have benefits for their users which are able to provide comfort, energy efficiency, and improved quality of life. However, this development also opens up the potential for cyber vulnerability, where the smart home itself is implemented quite close to people's lives so that the security of personal data and user privacy are a challenge in itself for smart homes.

Threats to data security in smart homes are not only limited to data theft of information, but also include the potential for illegal surveillance, disruption to home operations, and compromises on the physical security of residents. [1] said that there are reports of attacks on smart devices due to the lack of a robust security framework, information on smart homes is vulnerable to abuse, privacy violations, and even become a loophole for cybercrime. Therefore, risk mitigation strategies

and security implementation in smart homes are crucial to ensure that smart homes can be enjoyed by users without compromising users' privacy and fundamental security.

Using cryptography, data can be protected by disguising messages so that the information in the data cannot be read by unauthorized parties. On the other hand, implementing data security such as cryptography on smart homes is not easy because smart homes are part of IoT implementation, where IoT devices have small computing. Therefore, the form of cryptography needs to be adapted to the computing resources of IoT devices while still having good security to prevent cyberattacks. Furthermore, implementing data security in the smart home is a bit complicated because there is currently a massive research on quantum computers, which National Institute of Standards and Technology (NIST) considers this because quantum computers are assumed to be able to solve many of the public-key cryptographic systems that are currently commonly used [2].

[3] realizes that the current approach to cryptography faces several critical problems as a result of the widespread development of IoT in people's lives. Therefore, the [3] proposed Certificateless Elliptic Curve Aggregate Signcryption (CL-ECASC) as a form of security that can be used by IoT devices by combining signcryption and certificateless cryptography. As a result, on 1000 clients, CL-ECASC can be processed within 23,520 ms. Although CL-ECASC offers efficiencies, this study has not addressed Key Generation Center (KGC) vulnerabilities and has not considered post-quantum implications on actual IoT implementation. In addition, the [2] says that discrete log problems on elliptic curves are vulnerable to Shor's algorithm of quantum computers. Thus, to ensure the sustainability of data security and user privacy in the future, the use of cryptographic algorithms needs to be evaluated and changed with algorithms that are resistant to attacks from quantum computers.

Kyber and Dilithium are Post-Quantum Cryptography (PQC) algorithms that are standard candidates for securing data against attacks from quantum computers. Some research related to Kyber and Dilithium focuses on algorithm optimization, especially in the computationally intensive parts such as Number Theoretical Transform (NTT). For example, research on [4] and [5] developed operation-efficient hardware accelerators (NTTs) on FPGA and ASIC platforms, as well as Reduced Instruction Set Computing (RISC-V) based System-on-Chips (SoCs). The study [6] presents a benchmark of the performance of PQC network stacks on high-performance Data Processing Units (DPUs). However, the focus of the study [4],[5], and [6] tends to be on hardware optimization. Especially in the study [6],

the evaluation of the research was carried out on a server-grade platform that has abundant computing resources.

Therefore, this research is an update and a new step for evaluating the PQC. This thesis is a study that discusses the PQC based on Kyber-Dilithium signcryption in order to protect data in smart home environment. The research is carried out by implemented on Raspberry Pi as an IoT node gateway and a Virtual Machine (VM) as a web server to evaluate the use of Kyber-Dilithium signcryption in smart home environments.

Based on those issues, this research about Post-Quantum Cryptography based on Kyber-Dilithium Signcryption for IoT smart home is important to do. This research could provide new knowledge in PQC research and IoT security research to protect the smart home data from quantum computer attacks. Moreover, this research is also very useful for IoT engineers so that they could maximize the data security against cyber-attacks from quantum computer.

1.2 Problem Statement

With the threat of quantum computing to existing cryptographic systems today, the adoption of PQC algorithms such as Kyber and Dilithium is critical. Paper [7] has conducted a study on the performance of kyber where the results show that the resources owned by the raspberry pi can still support the use of the kyber algorithm. However, the use of kyber as a KEM can only secure data confidentiality which can prevent attackers from knowing the content of the message directly. Paper [6, 8] tested the performance of dilithium where the results showed that the resources owned by the raspberry pi could still support the use of the dilithium algorithm on the raspberry pi. However, the use of dilithium can only maintain data integrity which can provide a sense of security because when the data is changed, the digital signature will be invalid. Paper [3] conducted research related to signcrytion using classic cryptography where the use of this cryptographic method can maintain data integrity as well as data confidentiality.

1.3 Objective

This research aims to evaluate the performance of Post-Quantum Signcryption which is based on CRYSTALS Kyber and Dilithium. In this research, Kyber-Dilithium Signcryption is used to protect data integrity and confidentiality prepared in facing the quantum computer era. This study implements Kyber-Dilithium sign-

cryption on raspberry pi as an IoT node gateway that is connected to a Virtual machine as a web server. The analysis conducted in this research includes the overhead of computing resources including CPU and memory usage, as well as measuring operational latency, especially in keygen, signcrypt, and unsigncrypt operations. The results of this analysis are used to determine the feasibility and efficiency of using Kyber-Dilithium Signcryption in an effort to ensure data protection and privacy of smart home users against potential cyber threats in the post-quantum era.

1.4 Hypothesis

Based on the background analysis and research gaps regarding the adoption of PQC on limited embedded devices, this research proposes the main hypothesis that the implementation of Kyber-Dilithium Signcryption on the Raspberry Pi as an IoT node gateway in smart home scenarios involving large amounts of data, shows compute resource overhead as well as measurable and significant operational latency. However, it is predicted that the resulting overhead and latency could still allow the operational functionality of smart home systems. Furthermore, through a trade-off analysis between post-quantum security and device resource limitations, this research hypothesizes the determination of the feasibility limits of the implementation of Kyber-Dilithium Signcryption for data protection and user privacy against cyber threats in the post-quantum era.

1.5 Research Method

This Master's Thesis employs a multi-stage research methodology to accomplish its objectives. The research methods utilized are as follows:

1. Literature Study
   The basic theories related to CRYSTALS-Kyber and CRYSTALS-Dilithium as PQC need to be learned and understood as a support for Post-Quantum Cryptography Based on Kyber-Dilithium Signcryption For IOT Smart Home research. These related theories are sourced from research journals, conferences, and white papers.

2. Setup Smart Home Environment
   A smart home environment consisting of IoT devices, networks, and web applications needs to be built to simulate this research.

3. Configure Kyber-Dilithium Signcryption
   The configuration of Kyber with Dilithium as a signcryption method in a smart home environment is needed to be able to simulate and obtain the data required by this research.

4. Collect Simulation Data
   Data obtained from simulations conducted in smart home environments using Kyber-Dilithium Signcryption is required to be collected. The data needed is in the form of processing time and resource computation used by smart home devices when securing data using Kyber-Dilithium Signcryption.

5. Technical Analysis
   The data obtained from simulations conducted using Kyber-Dilithium Signcryption is being analyzed. This analysis is aimed at determining the performance of smart home devices against the use of PQC based on Kyber-Dilithium Signcryption.

6. Conclusion
   The results of the research, based on the data obtained and analyzed from the simulations conducted in this research, are concluded as an answer to the identification of future cryptographic problems. It is expected that the results presented by this research could be recommendations and suggestions for IoT engineers and cyber security enthusiasts, enabling them to create a safe and reliable smart home environment.