PROJECT DOCUMENT

System Model (Sequence Diagram) Document

Project Name	기밀연산 인공위성 시스템 적용 (PQC 기반 보안 키 교환 및 OP-TEE 저장)

11 조

202002558 조민성
201902711 신희성
201802076 김주호

지도교수: 장진수 교수님 (서명)

Document Revision History

Rev#	Date	Affected Section	Author
1	2023/04/26	시퀀스다이어그램 초안 작성	조민성 신희성 김주호

Table of Contents

List of Figure

1. Introduction

1.1. Objective

이 문서는 기밀 연산 기반 인공위성 보안 시스템의 요구사항을 정의하고, 시스템이 제공해야 할 주요 기능을 명확히 설명하는 것을 목적으로 한다. 본 시스템은 Post-Quantum Cryptography(PQC) 기반의 키 교환 기술과 OP-TEE(Trusted Execution Environment) 기반의 보안 저장 기술을 결합하여, 보다 높은 수준의 위성 보안 체계를 구현한다. 또한, 각 기능에 대해 상세한 설명과 유스케이스 다이어그램 및 유스케이스 명세서를 포함하여 전체 시스템의 동작 흐름과 사용자 상호작용을 구조적으로 기술한다.

2.Use Case Diagram

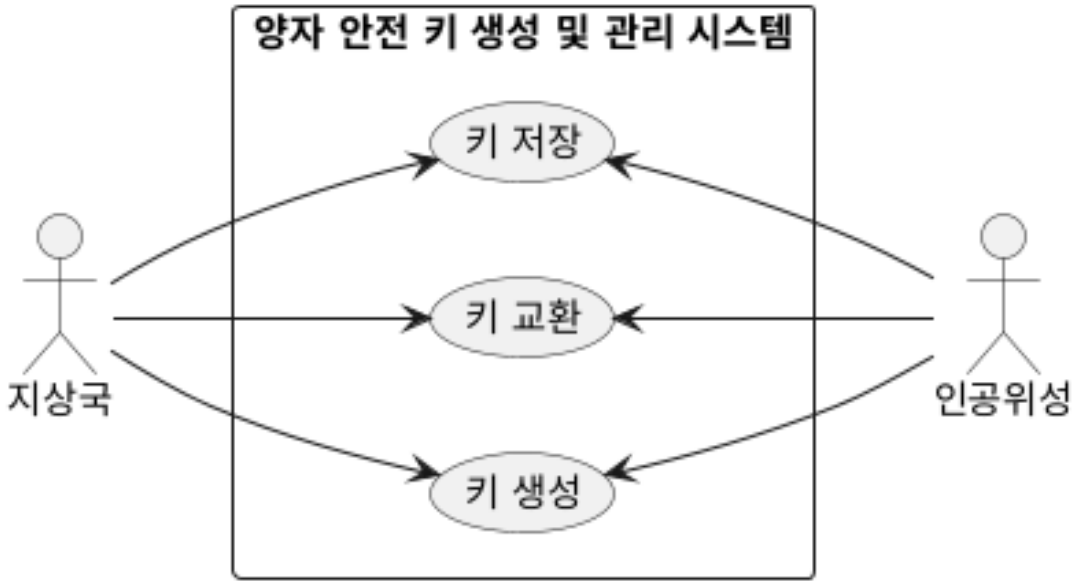


그림 1. 유스케이스 다이어그램

3.Sequence Diagram

3.1. 지상국-인공위성 PQC 키 생성 시퀀스 다이어그램

이름	지상국-인공위성 PQC 키 생성 시퀀스 다이어그램

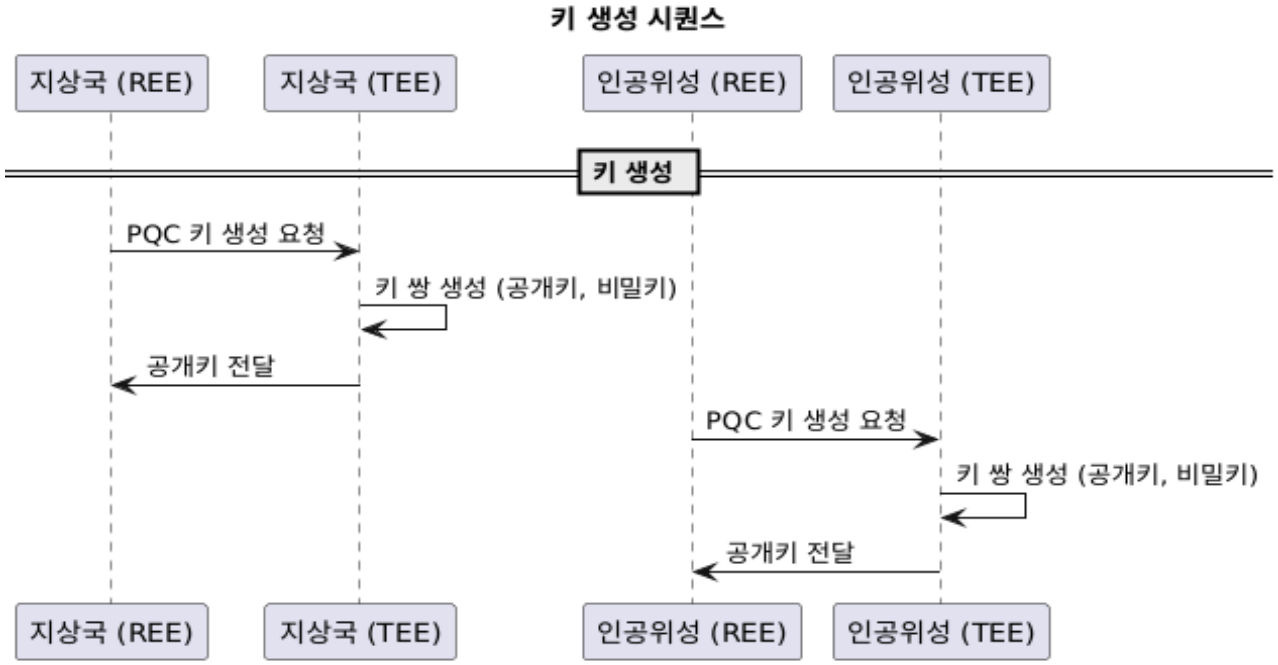


그림 2. 키 생성 시퀀스다이어그램

기능	지상국과 인공위성이 PQC 기반 키 쌍을 생성하는 과정을 나타낸다.
동작순서	1. 지상국에서 키 생성을 한다. 1.1. 지상국 REE에서 TEE로 키 생성 요청을 보낸다. 1.1.1. 지상국 TEE에서 PQC 알고리즘으로 키 쌍을 생성한다. 1.1.2. 지상국 TEE가 생성한 공개키를 REE로 전달한다. 1.2. 인공위성 REE에서도 TEE로 키 생성 요청을 보낸다. 1.2.1. 인공위성 TEE에서 키 쌍을 생성한다. 1.2.2. 인공위성 TEE가 공개키를 REE로 전달한다.

3.2. 지상국-인공위성 PQC 키 교환 시퀀스 다이어그램

이름	지상국-인공위성 PQC 키 교환 시퀀스 다이어그램

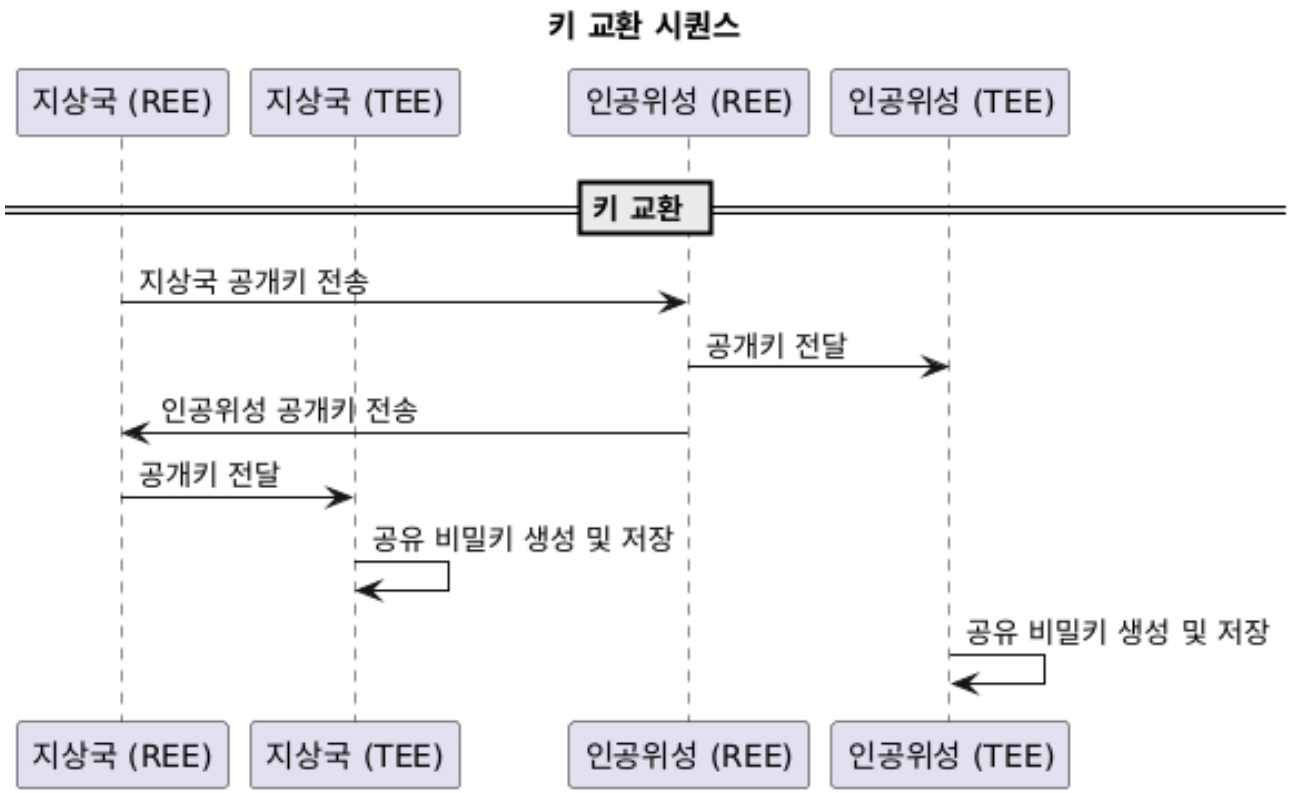


그림 3. 키 교환 시퀀스다이어그램

기능	지상국과 인공위성이 PQC 기반 키 쌍을 교환하는 과정을 나타낸다.
동작순서	2. 지상국에서 키 교환을 요청한다. 2.1. 지상국 REE가 자신의 공개키를 인공위성 REE로 전송한다. 2.1.1. 인공위성 REE가 수신한 공개키를 인공위성 TEE로 전달한다. 2.1.2. 인공위성 REE가 자신의 공개키를 지상국 REE로 전송한다. 2.2. 지상국 REE가 수신한 공개키로 비밀키를 생성한다. 2.2.1. 지상국 REE가 수신한 인공위성 공개키를 지상국 TEE로 전달한다. 2.2.2. 지상국 TEE가 상대방 공개키 + 자신의 비밀키로 공유 비밀키를 생성한다. 2.3. 인공위성 TEE도 동일하게 공유 비밀키를 생성하고 저장한다.

3.3. 지상국-인공위성 PQC 키 저장 시퀀스 다이어그램

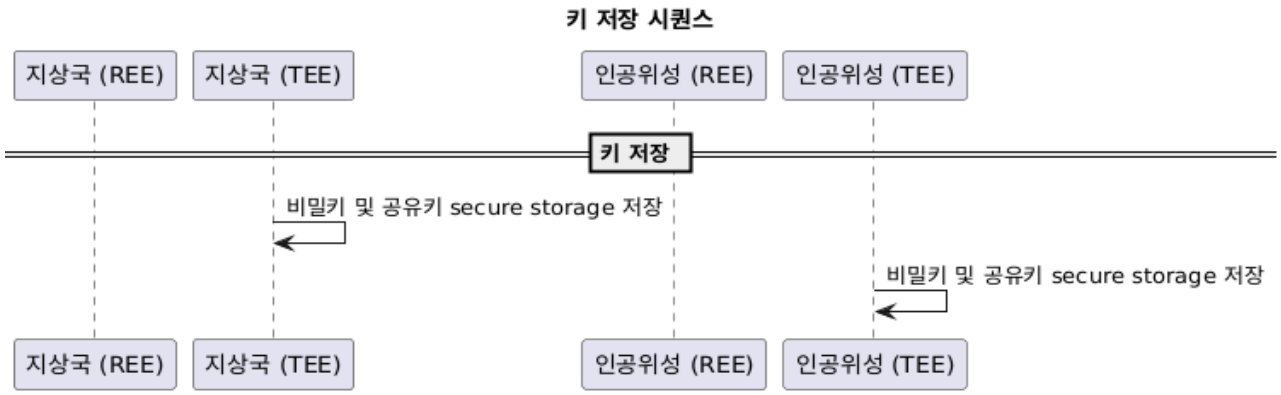
이름	지상국-인공위성 PQC 키 저장 시퀀스 다이어그램
	
기능	지상국과 인공위성이 PQC 기반 비밀키 및 공유키를 TEE 내부에 저장하는 과정을 나타낸다.
동작순서	3. 생성된 키 쌍을 저장한다. 3.1. 생성된 비밀키 및 공유키를 TEE 내부 Secure Storage에 저장한다. 3.2. 인공위성 TEE도 비밀키 및 공유키를 Secure Storage에 저장한다.

그림 4. 키 저장 시퀀스다이어그램

4.AI 도구 활용 정보

사용 도구	*GPT-o4*
사용 목적	*시퀀스 다이어그램 기능 및 동작 순서*
프롬프트	• *위 유스케이스와 같게 동작하는 시퀀스 다이어그램 기능 및 동작 순서 알려줘*
반영 위치	*1. 시퀀스 다이어그램 기능 및 순서 (p.7)*
수작업 수정	*있음(내용 보완 및 순서 정리)*