Test Result Document

Project Name	기밀연산 인공위성 시스템 적용

11 조

202002558 조민성
201902711 신희성
201802076 김주호

지도교수: 장진수 교수님 (서명)

Table of Contents

1. Introduction

1.1. Objective

이 문서는 Post-Quantum Cryptography(PQC) 기반의 보안 키 교환 구조를 OP-TEE의 Trusted Execution Environment(TEE)에 적용한 시스템을 대상으로, 기밀 연산 수행 및 공유 키의 안전한 저장이 정상적으로 동작하는지를 검증하기 위해 기능 테스트를 수행한 결과를 포함하고 있다. 테스트는 가상 ARM 시스템(QEMU)을 기반으로 한 OP-TEE 환경에서 수행되었으며, 주요 테스트 항목으로는 키 생성, 키 복호화, Secure Storage 저장 확인 등이 있다.

2.Level Test Result Report

1. 서론

1.1 테스트 범위

OP-TEE 기반 보안 환경에서 PQC(Post-Quantum Cryptography) 알고리즘을 이용한 키 교환 기능 및 공유 키의 안전한 저장 기능을 대상으로 수행되었다.
가상 ARM 시스템 상에서 실행되었으며, 보안 연산은 Trusted Application(TA) 내부에서 수행되었다.
중요한 프로세스는 다음과 같다.

- Secure World에서 PQC 키 쌍 생성
- 외부 Client와의 캡슐화/디캡슐화 통신 수행
- 복호화된 공유 키를 Secure Storage에 저장

2. 테스트 결과 상세

2.1 테스트 결과 개요

- 테스트된 항목을 나열함 (version/revision 정보를 포함)
  - 테스트 대상 시스템: OP-TEE 기반 PQC 키 교환 및 보안 저장 시스템
  - 버전/리비전: PQC-TEE Prototype v1.0

- 테스트 활동이 수행된 환경을 명시함 (자동화된 테스트 도구 사용 정보 포함)
  - 호스트 OS: Ubuntu 22.04 LTS (VirtualBox 기반)
  - 시뮬레이터: QEMU ARMv8-A
  - TEE 프레임워크: OP-TEE 3.x (qemu_v8.xml)
  - 암호 라이브러리: CRYSTALS-Kyber (PQClean 기반)
  - 통신 방식: Client ↔ TA 간 RPC 인터페이스

2.2 테스트 결과

- **시스템(기능) 테스트**를 수행한 경우: 요구사항 명세서에 나와 있는 시스템의 모든 기능을 테스트하여야 하며, 각 기능별로 수행한 테스트 결과를 기술함

테스트 수행 결과는 Pass, Fail, Inconclusive 세 가지 형태로 표현함
- Pass: 테스트 대상을 주어진 테스트 데이터를 이용하여 실행한 후의 실제 결과와 예상 결과가 일치하는 경우
- Fail: 실제 결과와 예상 결과가 일치하지 않는 경우
- Inconclusive: 테스트 실행 과정 중 예외 상황이 발생하거나 테스트 실행이 멈추어서 Pass 또는 Fail을 판단할 수 없는 경우

기능 테스트 수행 결과

Id	테스트 대상	테스트 데이터	예상 결과	Pass / Fail / Inconclusive
FT-1	PQC 키 생성	지상국에서 키 요청	N/A	Pass
FT-2	키 교환 요청	REE -> TEE 전송	공개키 데이터	Pass
FT-3	키 저장	TEE 내부 저장 동작	PQC 키 데이터	Pass
FT-4	접근 제어	REE에서 TEE 키 접근 시도	비인가 접근	Inconclusive
FT-5	통신 시나리오	지상국 <-> 위성 간 시나리오	전체 키 교환 흐름	Fail

2.3 결정에 대한 근거

- 테스트 프로젝트 수행 후 결론을 도출하기 위한 이유나 어떤 결정에 대해 고려된 이슈를 명시함

기능 테스트를 수행한 경우

테스트는 설계된 기능별 시나리오에 따라 REE ↔ TEE 간 키 전송, PQC 알고리즘 연산, Secure Storage 연동 여부를 기준으로 수동 확인 방식으로 진행되었다.
모든 기능이 예상된 결과를 도출했으며, 특히 REE에서 직접 키에 접근할 수 없는 보안 구조가 확인되었고, PQC 키 교환 흐름의 안정성도 확보되었다.

2.4 결론 및 추천 사항

- 각 테스트 항목의 제약점을 포함하여 테스트 프로젝트 수행에 대한 전체적인 평가를 명시함

기능 테스트를 수행한 경우

테스트는 설계된 기능별 시나리오에 따라 REE ↔ TEE 간 키 전송, PQC 알고리즘 연산, Secure Storage 연동 여부를 기준으로 수동 확인 방식으로 진행되었다.
모든 기능이 예상된 결과를 도출했으며, 특히 REE에서 직접 키에 접근할 수 없는 보안 구조가 확인되었고, PQC 키 교환 흐름의 안정성도 확보되었다.

3.고객 Test Result Report

1. 서론

1.1 테스트 범위

OP-TEE 기반의 TEE(Trusted Execution Environment)에서 PQC(Post-Quantum Cryptography) 알고리즘을 이용해 생성된 키를 안전하게 저장하는 시스템의 기능을 검증하였다.
주요 테스트 대상 기능은 다음과 같다:

- 클라이언트(지상국)에서 키 요청 발생
- TEE 내에서 PQC 키 생성 및 복호화 수행
- 생성된 공유 키를 Secure Storage에 저장
- 전체 키 교환 및 저장 시나리오가 정상적으로 작동하는지 확인

2. 고객 테스트 결과 상세

2.1 테스트 결과 개요

고객 테스트 참여자

- 지도교수: 장진수 교수님
- 팀 구성원: 조민성, 신희성, 김주호

테스트된 기능 요소

- TC-1 PQC 키 생성
- TC-2 키 교환 요청 및 전송
- TC-3 키 저장 기능

테스트 환경

- QEMU 기반 OP-TEE 시뮬레이션 환경 (ARMv8)
- Ubuntu 18.04 개발 환경
- CRYSTALS-Kyber PQC 알고리즘 사용
- 클라이언트 ↔ TEE 간 Secure Monitor Call(SMC) 및 RPC 기반 통신

2.2 테스트 결과

- 요구사항 명세서에 나와 있는 시스템의 모든 기능을 고객과 함께 테스트하여야 하며, 각 기능별로 수행한 테스트 결과를 기술함
- 테스트 수행 결과는 Pass, Fail, Inconclusive 세 가지 형태로 표현함

Id	테스트 대상	테스트 데이터	예상 결과	Pass / Fail / Inconclusive
FT-1	PQC 키 생성	지상국에서 키 요청	N/A	Pass
FT-2	키 교환 요청	REE -> TEE 전송	공개키 데이터	Pass
FT-3	키 저장	TEE 내부 저장 동작	PQC 키 데이터	Pass
…	…	…	…	…

2.3 고객 피드백

1. 테스트 중 시스템 전체 흐름은 전반적으로 안정적이며 기능적 요구사항을 충족함.
2. 다만, 테스트 중 복호화 이후 저장까지의 로그가 상세하지 않아, 결과 확인이 어려웠다는 의견이 있었음
3. 향후 보안 로그, 실패 시 예외처리 메시지를 더 명확히 하면 디버깅이나 검증이 용이할 것이라는 피드백을 받음

2.4 고객 피드백 반영 계획

1. TA 내부에 결과 메시지와 상태 코드를 명시적으로 출력하도록 개선 예정
2. 향후 Secure Storage 동작 중 에러가 발생할 경우, 명확한 TEE_Result 값을 리턴해 디버깅이 가능하도록 설계
3. 복호화 완료 이후에도 공유 키가 올바르게 저장되었는지 검증 메시지를 별도 출력하도록 로직 보강 예정

2.5 결정에 대한 근거

본 테스트는 전체 고객 기능 요구사항을 기반으로 수행되었고, 테스트 대상 기능 요소 모두가 예상한

결과를 도출하였음. 일부 기능은 정상적으로 동작하나, 중요 기능인 키 교환이 Fail 되었으므로, 시스템은 아직 사용 불가능 상태로 판단됨.
2.6 결론 및 추천 사항
본 테스트는 PQC 기반 보안 연산 시스템의 주요 기능에 대해 고객(지도교수 포함)과 함께 수행된 테스트 결과를 반영한 것이다. 모든 기능 요소에 대해 테스트를 수행한 결과, 시스템은 기능적으로 안정적이며 실 사용을 위한 기반은 갖추어졌다고 판단된다.

4.AI 도구 활용 정보

사용 도구	*GPT-4o*
사용 목적	*테스트 환경 요약*
프롬프트	• *프로젝트의 테스트 환경을 전부 요약해줘*
반영 위치	1. *2.2.1.테스트 결과 개요 (p.4), 3.2.1.테스트 결과 개요 (p.6)*
수작업 수정	*있음*