기밀연산 인공위성 시스템 적용

OPTEE와 PQC 알고리즘 포팅

11조 - 조민성, 신희성, 김주호
지도교수 - 장진수 교수님

Table of contents

프로젝트 개요

배경과 필요성

양자 컴퓨터의 등장
- 양자 컴퓨터란? 양자역학의 주된 현상인 중첩, 얽힘, 간섭을 정보 처리에 이용

기존 RSA 기반 비대칭키 시스템은 장기적으로 무력화될 가능성이 높음.
극한 환경(인공위성 등)에서 키 유출 없는 안전한 보안 연산이 필수
OP-TEE의 PQC 키 교환 및 보안 저장 구조 개발 필요
위성은 예시, 기존 통신 체계 보안성 향상을 위해서도 활용 가능

팀원소개 / 역할 분담 / 협업 방식 ?

조민성 : 팀장 / 주간 계획 설정 / 시스템 구축
신희성 : 발표 자료 수집 및 제작 / 시스템 구축
김주호 : 시스템 구축 / 사전 자료 조사

프로젝트 개요

OP-TEE + PQC?

현재 위성과 관련된 연구소에서는 QKD(양자키분배)방식을 연구 중
이론적으로 QKD가 보안적으로 뛰어남

OP-TEE + PQC 이점

1. 제약이 덜하다
   - QKD는 수억원에 달하는 장비가 필요한 데 반해 장비에 제약이 없고, 언제 어디서나 가능
2. 속도
   - OP-TEE + PQC는 0.15ms, QKD는 거리에 따라 급락
3. QKD는 통로의 도청 불가능성을 제공, 단말이 뚫리면 평문 유출 위험, TEE는 키 저장, 연산까지 하드웨어로 고립

사용자 분석

이해관계자 인터뷰

목표 사용자 : 고 신뢰 환경에서 기밀성을 요구하는 시스템 설계자

주요 요구사항

1. 양자 내성 암호 지원
2. 외부로부터 완전히 격리된 보안 연산 영역
3. 키 탈취 위험이 없는 안전한 저장 방식

핵심 아이디어

제안 방법

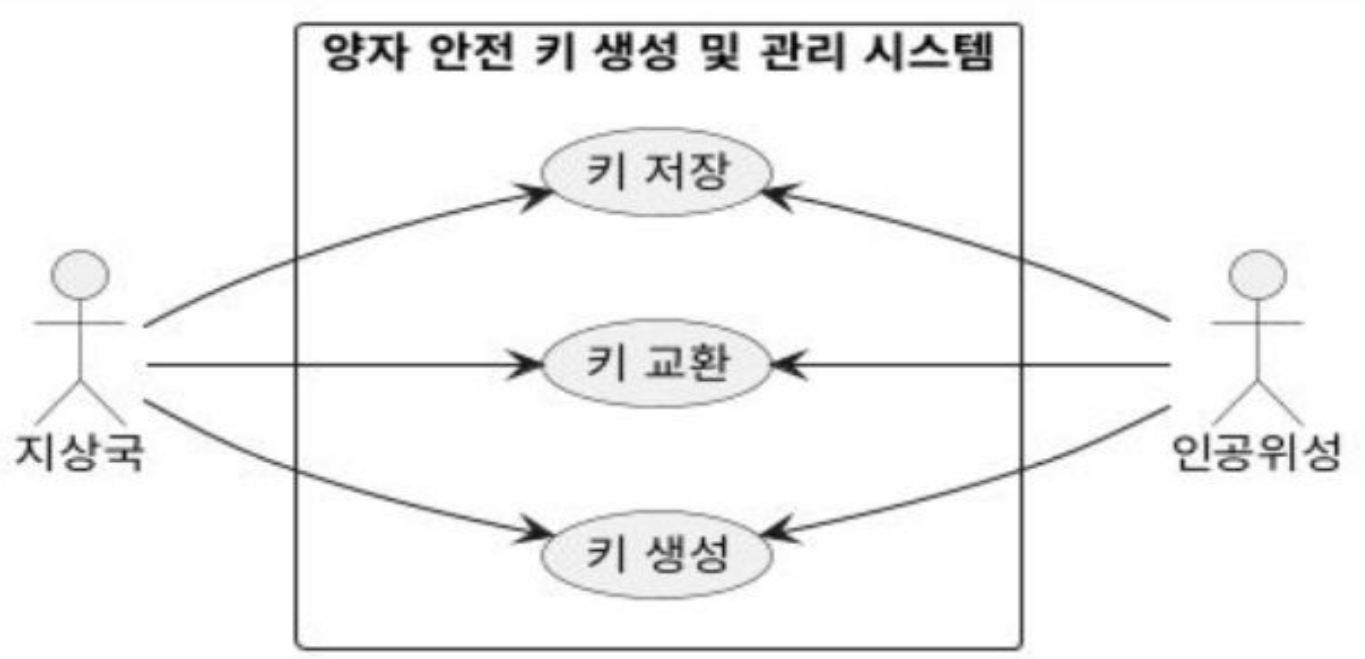
PQC(Kyber) 기반 키 생성 및 복호화를 OP-TEE Secure World 내에서 실행
키를 Secure Storage에 저장하여 키 탈취 방지

기존 해결 방법 개선점

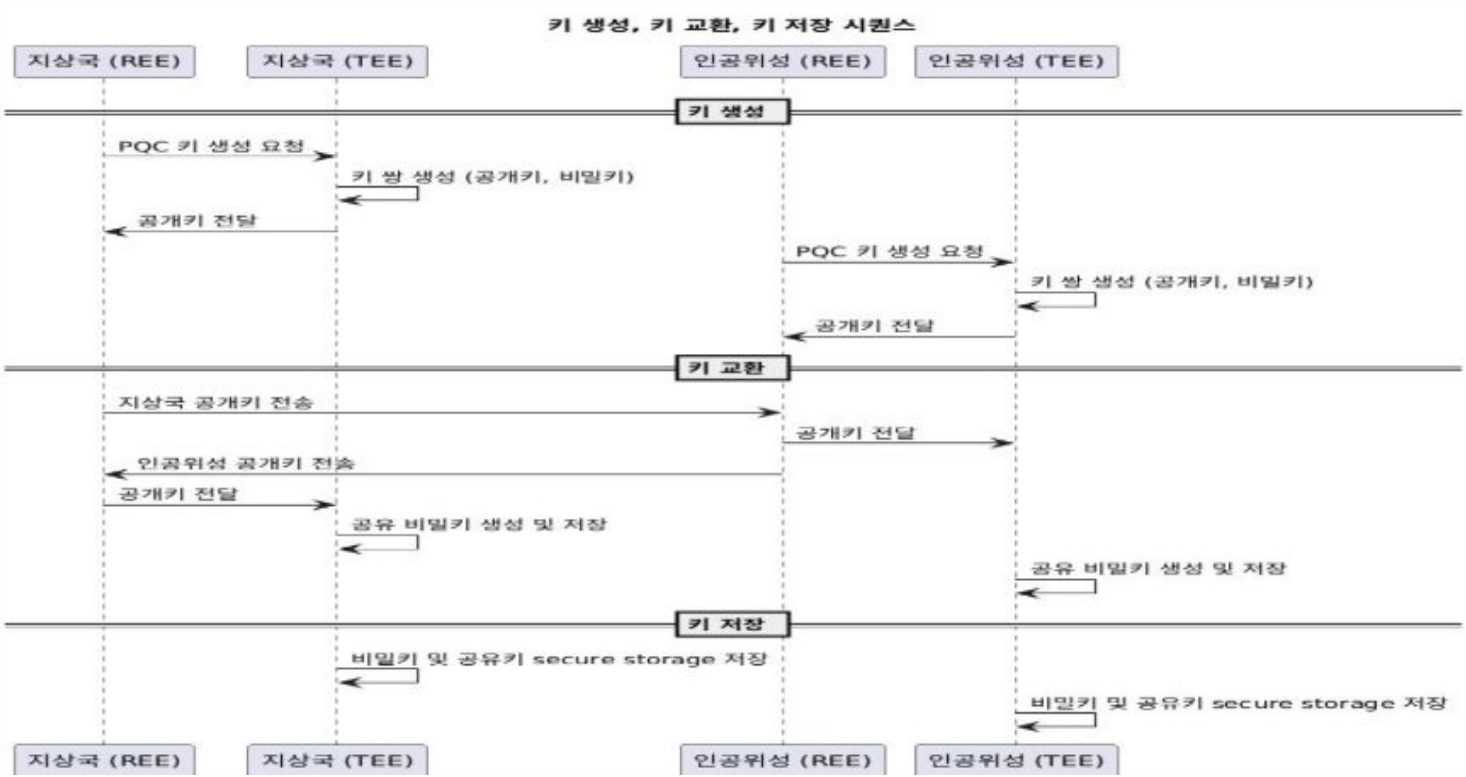
기존 방식	제안 방식
RSA/ECC 기반, 양자에 취약	PQC 기반으로 양자 환경 대비
일반 OS 영역에서 키 연산 수행	TEE 격리 영역에서 연산 수행
파일 기반 키 저장, 노출 가능성	OP-TEE Secure Storage에 저장

04. 데모

핵심 유스케이스



시퀀스 다이어그램


키 생성, 키 교환, 키 저장 시퀀스
지상국 (REE)
지상국 (TEE)
인공위성 (REE)
인공위성 (TEE)
키 생성
PQC 키 생성 요청
키 쌍 생성 (공개키, 비밀키)
공개키 전달
PQC 키 생성 요청
키 쌍 생성 (공개키, 비밀키)
공개키 전달
키 교환
지상국 공개키 전송
공개키 전달
인공위성 공개키 전송
공개키 전달
공유 비밀키 생성 및 저장
공유 비밀키 생성 및 저장
키 저장
비밀키 및 공유키 secure storage 저장
비밀키 및 공유키 secure storage 저장
지상국 (REE)
지상국 (TEE)
인공위성 (REE)
인공위성 (TEE)

테스트

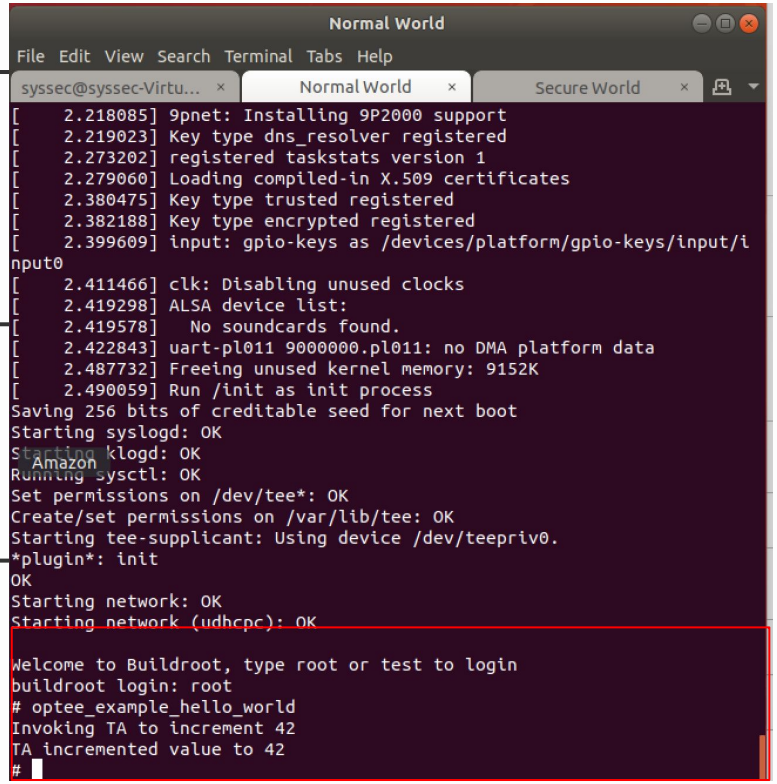
프로토타입 설계

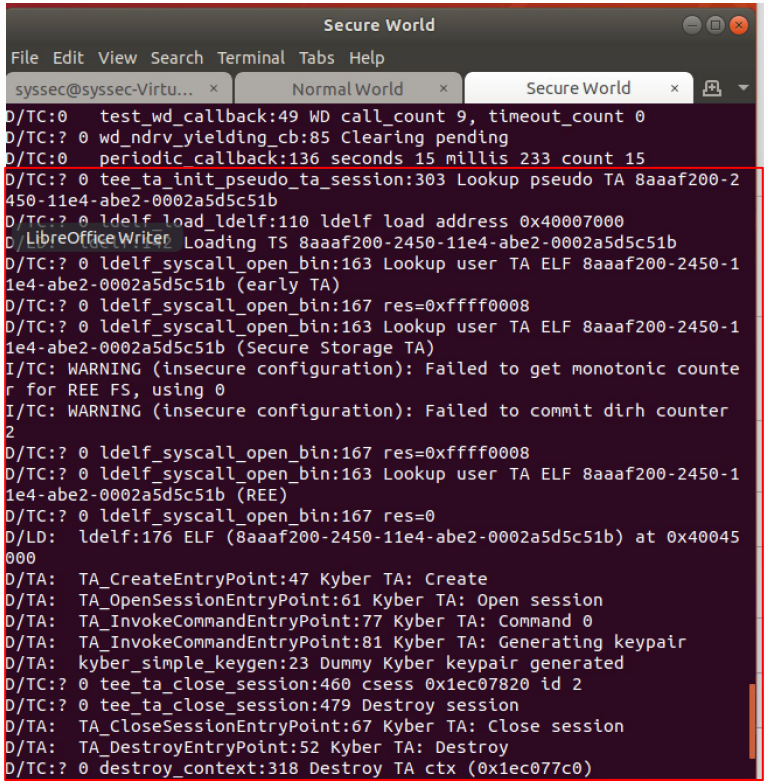
- QEMU 기반 ARM 환경에서 OP-TEE 실행
- TA 내부에 PQC 키 연산 구현

시제품 결과

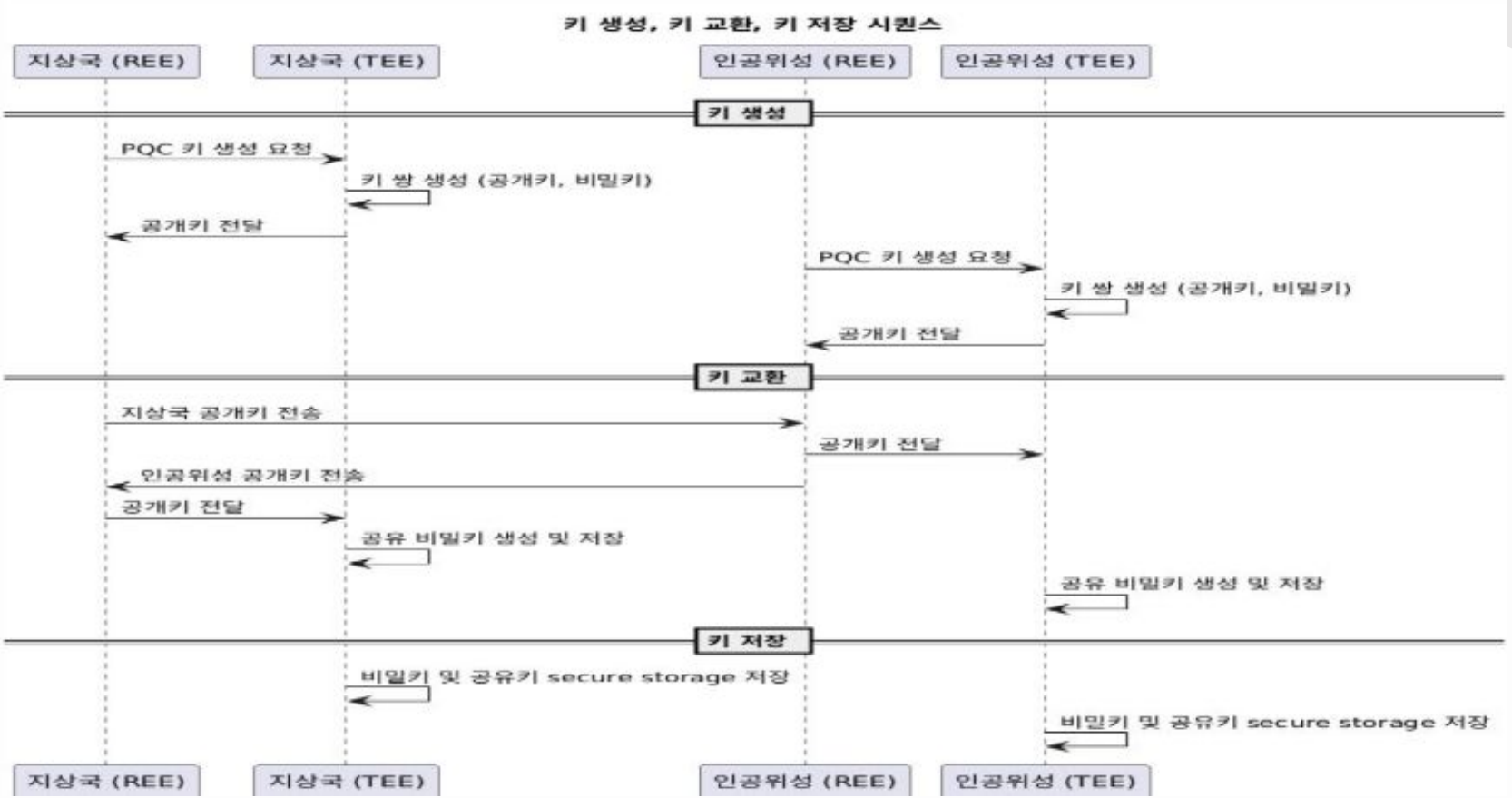
기능 테스트 방식을 사용 - 키 생성, 키 교환 요청, 키 저장, 통신 시나리오

시제품 결과


Normal World
File Edit View Search Terminal Tabs Help
syssec@syssec-Virtu...
Normal World
Secure World
[2.218085] 9pnet: Installing 9P2000 support
[2.219023] Key type dns_resolver registered
[2.273202] registered taskstats version 1
[2.279060] Loading compiled-in X.509 certificates
[2.380475] Key type trusted registered
[2.382188] Key type encrypted registered
[2.399609] input: gpio-keys as /devices/platform/gpio-keys/input/input0
[2.411466] clk: Disabling unused clocks
[2.419298] ALSA device list:
[2.419578] No soundcards found.
[2.422843] uart-pl011 9000000.pl011: no DMA platform data
[2.487732] Freeing unused kernel memory: 9152K
[2.490059] Run /init as init process
Saving 256 bits of creditable seed for next boot
Starting syslogd: OK
Starting klogd: OK
Running sysctl: OK
Set permissions on /dev/tee*: OK
Create/set permissions on /var/lib/tee: OK
Starting tee-supplicant: Using device /dev/teepriv0.
plugin: init
OK
Starting network: OK
Starting network (udhcpc): OK
Welcome to Buildroot, type root or test to login
buildroot login: root
optee_example_hello_world
Invoking TA to increment 42
TA incremented value to 42
#
Amazon


Secure World
File Edit View Search Terminal Tabs Help
syssec@syssec-Virtu...
Normal World
Secure World
D/TC:0 test_wd_callback:49 WD call_count 9, timeout_count 0
D/TC:? 0 wd_ndrv_yielding_cb:85 Clearing pending
D/TC:0 periodic_callback:136 seconds 15 millis 233 count 15
D/TC:? 0 tee_ta_init_pseudo_ta_session:303 Lookup pseudo TA 8aaaf200-2450-11e4-abe2-0002a5d5c51b
D/TC:? 0 ldelf load_ldelf:110 ldelf load address 0x40007000
D/TC:? 0 ldelf_syscall_open_bin:163 Loading TS 8aaaf200-2450-11e4-abe2-0002a5d5c51b
D/TC:? 0 ldelf_syscall_open_bin:163 Lookup user TA ELF 8aaaf200-2450-11e4-abe2-0002a5d5c51b (early TA)
D/TC:? 0 ldelf_syscall_open_bin:167 res=0xffff0008
D/TC:? 0 ldelf_syscall_open_bin:163 Lookup user TA ELF 8aaaf200-2450-11e4-abe2-0002a5d5c51b (Secure Storage TA)
I/TC: WARNING (insecure configuration): Failed to get monotonic counter for REE FS, using 0
I/TC: WARNING (insecure configuration): Failed to commit dirh counter 2
D/TC:? 0 ldelf_syscall_open_bin:167 res=0xffff0008
D/TC:? 0 ldelf_syscall_open_bin:163 Lookup user TA ELF 8aaaf200-2450-11e4-abe2-0002a5d5c51b (REE)
D/TC:? 0 ldelf_syscall_open_bin:167 res=0
D/LD: ldelf:176 ELF (8aaaf200-2450-11e4-abe2-0002a5d5c51b) at 0x40045000
D/TA: TA_CreateEntryPoint:47 Kyber TA: Create
D/TA: TA_OpenSessionEntryPoint:61 Kyber TA: Open session
D/TA: TA_InvokeCommandEntryPoint:77 Kyber TA: Command 0
D/TA: TA_InvokeCommandEntryPoint:81 Kyber TA: Generating keypair
D/TA: kyber_simple_keygen:23 Dummy Kyber keypair generated
D/TC:? 0 tee_ta_close_session:460 csess 0x1ec07820 id 2
D/TC:? 0 tee_ta_close_session:479 Destroy session
D/TA: TA_CloseSessionEntryPoint:67 Kyber TA: Close session
D/TA: TA_DestroyEntryPoint:52 Kyber TA: Destroy
D/TC:? 0 destroy_context:318 Destroy TA ctx (0x1ec077c0)
LibreOffice Writer

05. 테스트


키 생성, 키 교환, 키 저장 시퀀스
지상국 (REE)
지상국 (TEE)
인공위성 (REE)
인공위성 (TEE)
키 생성
PQC 키 생성 요청
키 쌍 생성 (공개키, 비밀키)
공개키 전달
PQC 키 생성 요청
키 쌍 생성 (공개키, 비밀키)
공개키 전달
키 교환
지상국 공개키 전송
공개키 전달
인공위성 공개키 전송
공개키 전달
공유 비밀키 생성 및 저장
공유 비밀키 생성 및 저장
키 저장
비밀키 및 공유키 secure storage 저장
비밀키 및 공유키 secure storage 저장
지상국 (REE)
지상국 (TEE)
인공위성 (REE)
인공위성 (TEE)

테스트

성능 평가

- 키 생성 Pass
- 키 교환 - 교환 요청은 가능하나 실제로 교환은 x Fail
- 키 저장 Pass
- 통신 시나리오 - 키 교환이 안되므로 Fail

사용자 테스트 **(A/B)**

A안 : 단순 RSA 기반 → 키 탈취 우려 발생

B안 : TEE 기반 PQC → 탈취 불가, 성능 안정적

추가 계획

추가 계획

- 실제 보드 (i.MX8MM) 이식 테스트
- 완전한 PQC 포팅 및 키 교환 구현
- 보안성 강화

기대 효과

인공위성과 같이 극한 환경에서도 적용 가능한 신뢰성 높은 보안 구조

PQC 내성 + 하드웨어 격리로 미래 보안 요구에 대응 가능

국방, 항공, 금융, 자율주행 등 다양한 분야로 확장 가능

출처

PQC 속도 : https://arxiv.org/pdf/2504.10730

Thanks!

CREDITS: This presentation template was created by **Slidesgo,** and includes icons, infographics & images by **Freepik**

https://github.com/isord/satellite_OPTEE/tree/week13