기밀연산 인공위성 시스템 적용

종합설계 7회차

11조 - 조민성, 신희성, 김주호
지도교수 - 장진수 교수님

Table of contents

PQC 알고리즘이란?

정의

Post-Quantum Cryptography, 양자 컴퓨터가 실용화 되어도 안전하게 사용할 수 있는 알고리즘

예시

1. 격자 문제 (Lattice Problems)
2. 다변수 다항식 문제 (Multivariate Polynomials)
3. 코드 기반 문제 (Code-Based Problems)
4. 해시 기반 서명 (Hash-Based Signatures)
5. 이산로그 기반 문제(SIDH, SIKE)

PQC 알고리즘의 장점

1. 양자 컴퓨터 공격에도 안전
   - 기존 RSA, ECC 기반 암호는 양자 컴퓨터 등장 시 깨질 위험 존재

2. 현실적인 적용 가능성
   - PQC 알고리즘은 현 시스템에 적용할 수 있도록 설계

3. 다양한 선택지
   - 시스템 요구사항에 알맞은 알고리즘 선택 가능

4. 긴 보안 수명
   - 장기적으로 데이터 안정성 보장

OP-TEE 와 **PQC** 인 이유

1. 해킹의 모든 루트를 차단
   - 하드웨어 보안(OP-TEE)과 네트워크 보안(PQC) 모두 만족

2. 장기적인 보안 수명 확보
   - 미래 공격까지 선제 대응

3. 보안 사고시 피해 최소화
   - 키 탈취 시 과거 데이터 보호

4. 국가기관/글로벌 표준에 부합
   - 미국 NIST 같은 기관이 요구하는 "포스트 양자 보안" 조건을 만족

02. OP-TEE & PQC

기존 암호화 방식과의 차이

구분	기존 보안 방식	OP-TEE + PQC 보안 방식
양자 컴퓨터 대응	대응 불가	대응 가능
키 보관 안정성	REE 메모리에 노출, 탈취 위험	TEE 내부 격리, 외부 접근 불가
시스템 해킹 대응	OS 커널 해킹, 루트 권한 탈취	OS가 뚫려도 키 보호 유지
보안 수명	향후 5~10년 내 무력화 예상	향후 20~30년 이상 안정성 확보
표준/ 규정 부합	점차 규정 미달 위험	최신 국제 표준 충족
성능/실용성	미래 대응 부족	장기적 실용성 확보

실제 적용 분야와 이유

적용 분야

인공위성 통신 분야

사용 이유

1. 우주에서는 한 번 키가 탈취되면 복구 불가
2. 통신 링크와 저장 영역 모두 고도의 보안 필요
3. 지구에서 양자 컴퓨터 공격이 가능할 경우를 대비

실제 적용 분야와 이유

적용 분야

금융 시스템

사용 이유

1. 양자 컴퓨터 사용시 암호화된 거래 정보 무력화 가능성
2. 고객 데이터, 전자 서명, 거래 기록을 장기간 안전하게 보호
3. 과거 기록 위조로 금전적 피해 우려

실제 적용 분야와 이유

적용 분야

국방/군사 통신 시스템

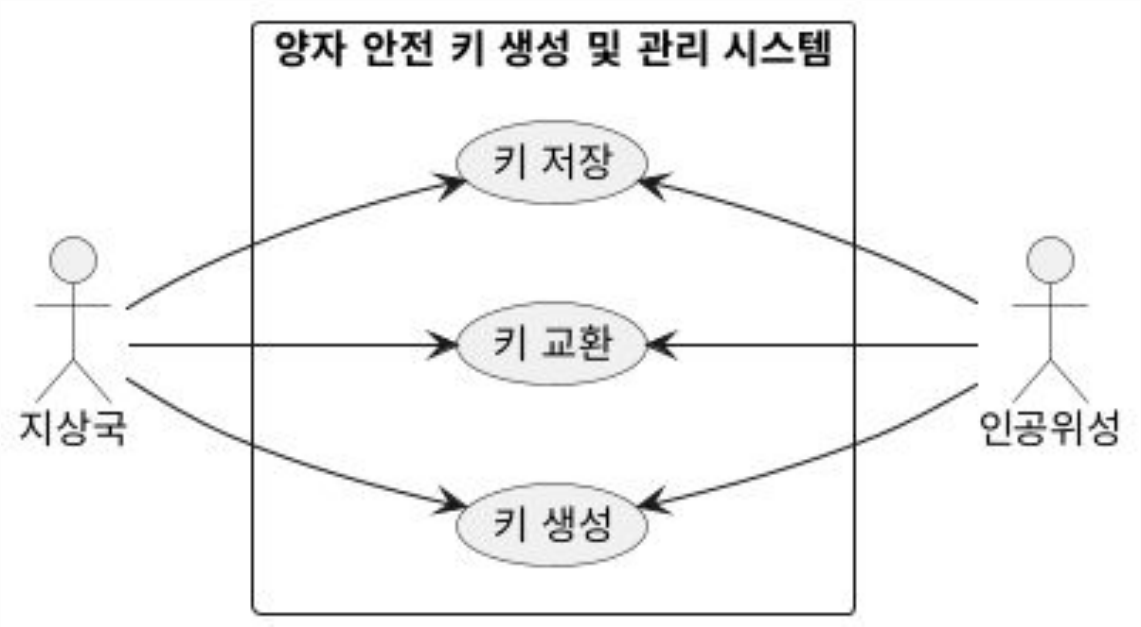
사용 이유

1. 기존 암호화 방식 무력화 가능성
2. 국방 데이터는 장기간 보안 유지될 필요성 존재
3. 단말기/장비 내부 보안 완성 가능

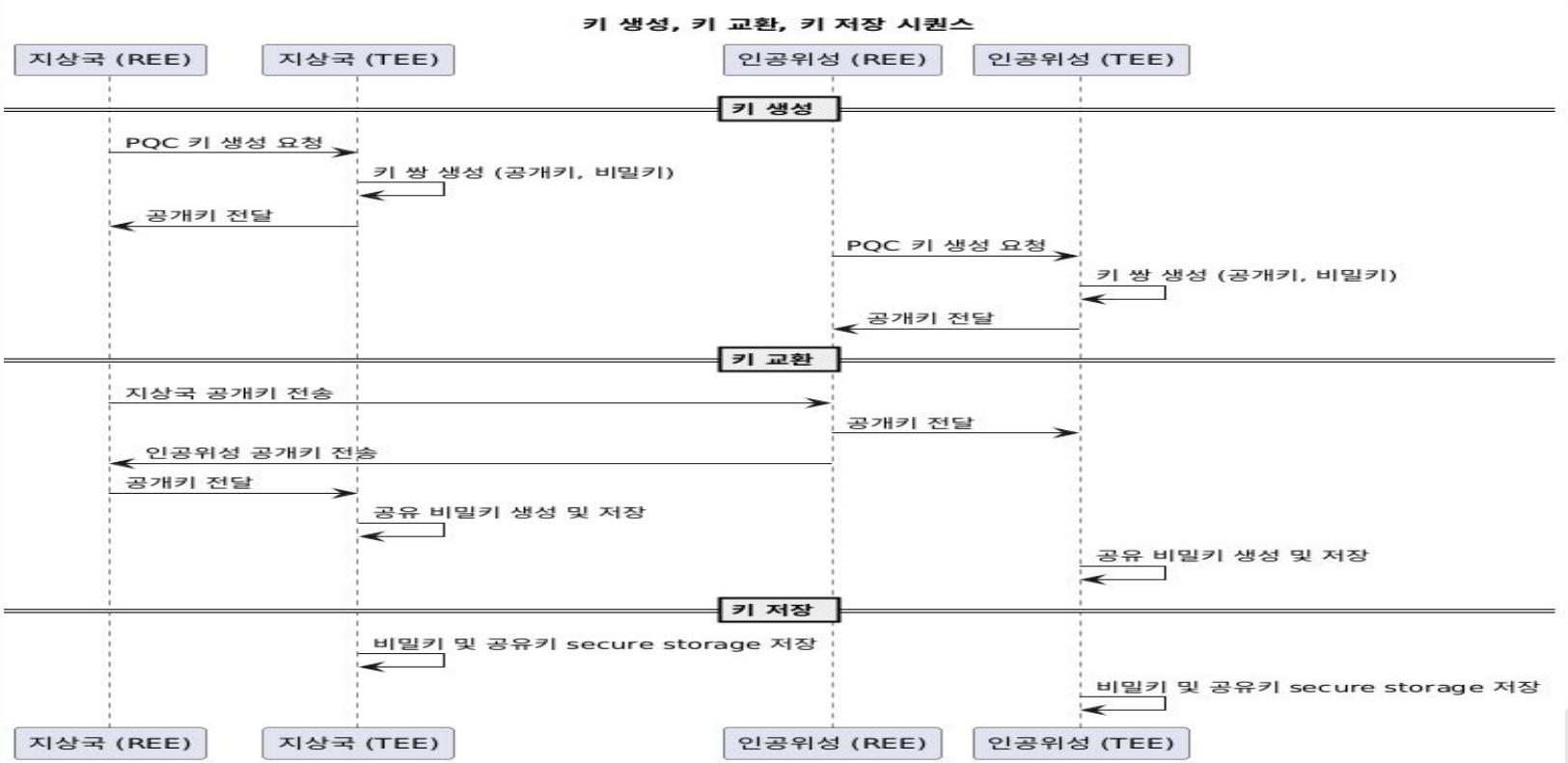
유스케이스

1. 키 생성
   - 대칭키 기반의 디지털 서명 방식을 통한 보안
2. 키 교환
   - PQC 알고리즘을 통한 암호화 데이터 통신
3. 키 저장
   - OP-TEE 환경을 사용해 보안 강화된 데이터 저장

유스케이스 다이어그램



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)

OP-TEE & PQC 기대 목표

실용 목표

OP-TEE와 PQC을 접목한 기술이 실현 가능하여야 하고 기존 보안과 차별화 되어 사용자의 수요를 만족시킨다.

보안 목표

1. 네트워크 및 하드웨어 등 모든 루트의 위협을 제거한다.
2. 키 탈취로 부터 과거 데이터를 보호한다.
3. 단 한 번의 세팅으로 장기간 보안을 유지한다.
4. 피해를 최소화하고 신속하게 복구할 수 있도록 한다.

출처

Thanks!

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

https://github.com/isord/satellite_OPTEE/tree/week3