하드웨어 양자 보안모듈 기반 이동통신 단말 보안 관리 구조에 관한 연구

이효성*, 박근용
㈜MDS 테크
hyosoung.lee@mdstech.co.kr

A Study on Security Management Architecture for Mobile Communication Devices Based on Hardware Quantum Security Modules

Hyosoung Lee*, Keunyong Park
MDSTECH

요 약

본 논문에서는 5G 특화망 및 미션 크리티컬 통신(MCX) 환경에서 이동 단말의 보안 신뢰성을 강화하기 위한 하드웨어 양자 보안모듈(Hardware Quantum Security Module) 기반 통신망 보안 관리 구조를 제안한다. 기존 이동 단말은 소프트웨어 중심의 키 저장 및 인증 구조로 인해 단말 위·변조, 키 유출, 양자컴퓨팅 기반 공격에 취약한 한계를 가진다. 이를 해결하기 위해 본 연구에서는 이동 단말에 직접 연결되는 하드웨어 보안모듈을 통해 단말 식별, 초기 인증, 암호 연산, 양자난수 생성을 수행하는 구조를 설계하였다. 제안 방식은 일반 암호 알고리즘과 양자내성암호(PQC)를 병행 적용함으로써, 기존 통신 인프라와의 호환성을 유지하면서도 장기적인 보안성을 확보할 수 있다.

Ⅰ. 서 론

5G 이동통신 기술의 상용화와 함께 공공안전, 국방, 경호 분야에서는 고신뢰·저지연 통신을 요구하는 미션 크리티컬 통신 환경이 확대되고 있다. 이러한 환경에서는 네트워크 안정성뿐만 아니라, 단말 단위에서의 신뢰성 있는 인증과 보안 관리가 전체 시스템 안정성에 직접적인 영향을 미친다.

그러나 기존 이동 단말의 보안 구조는 운영체제 또는 애플리케이션 계층에 의존하는 방식이 대부분이며, 단말 탈취, 루팅, 악성 코드 삽입과 같은 공격에 취약하다. 또한 양자컴퓨터의 발전으로 인해 기존 공개키 암호 알고리즘의 안전성에 대한 우려가 제기되면서, 양자내성암호 및 하드웨어 기반 보안 기술의 필요성이 증가하고 있다.

본 논문에서는 이러한 문제를 해결하기 위해, 이동 단말에 하드웨어 양자 보안모듈을 연동한 통신망 보안 관리 구조를 제안하고, 그 동작 원리와 적용 가능성을 분석한다.

Ⅱ. 본론

제안하는 시스템은 이동 단말, 하드웨어 양자 보안모듈, 이동통신 네트워크(5G 특화망), 관리 서버로 구성된다.

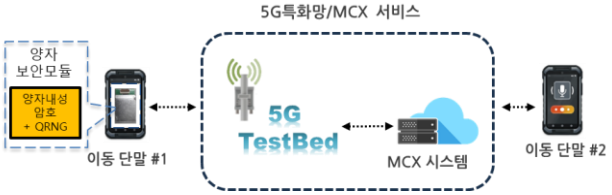

그림 1. 하드웨어 양자 보안 모듈 기반 이동통신 보안 관리 시스템 구성도

이동 단말은 5G 특화 망 네트워크를 통해 기지국 및 코어망과 연결되며, 보안 관련 핵심 연산은 단말과 분리된 하드웨어 보안 모듈에서 수행된다.

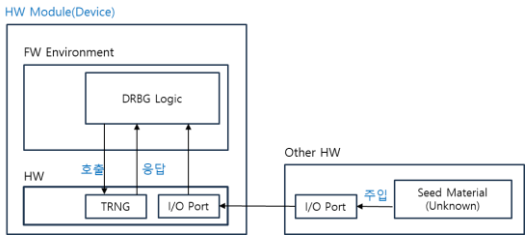

그림 2. 외부에서 전달받은 엔트로피를 입력할 수 있는 형태의 암호 모듈 형태

하드웨어 양자 보안 모듈은 초기 Seed key 를 내부 저장소에 안전하게 저장하고, 단말과 최초 연결 시 해당 Seed key 를 기반으로 인증 값을 생성한다. 이후 통신 과정에서는 생성된 인증 값을 이용하여 단말 식별 및 상호 인증을 수행함으로써, 단말 복제 및 인증 정보 재사용 공격을 방지한다.

암호 연산부는 일반 암호 연산부와 양자 암호 연산부로 구성된다. 일반 암호 연산부는 AES, ARIA 와 같은 기존 대칭 키 암호 알고리즘을 처리하며, 양자 암호 연산부는 ML-KEM 과 같은 양자내성암호(PQC) 알고리즘을 수행한다. 이를 통해 시스템은 기존 보안 체계와의 연속성을 유지하면서, 양자 보안 전환이 가능하다.

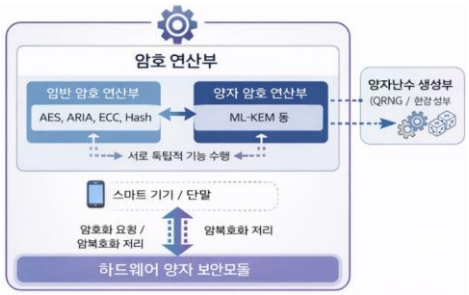

그림 3. 하드웨어 양자 보안모듈 내 이중 암호 연산부 구조

이중 암호 연산 구조를 통해 시스템은 다음과 같은 장점을 확보한다.

- 기존 통신 인프라 및 보안 체계와의 호환성 유지
- 서비스 중단 없이 양자내성암호(PQC) 기반 보안으로 단계적 전환 가능
- 단말, 네트워크, 서버 환경에 따라 암호 방식 유연 적용 가능

하드웨어 양자 보안 모듈은 일반 암호 연산부와 양자 암호 연산부로 구성된 이중 구조를 가지며, 기존 대칭·비대칭 암호(AES, ARIA, ECC, Hash)와 양자암호연산부(ML-KEM 등)를 병행 지원한다. 두 연산부는 상호 독립적으로 동작하며, 양자난수 생성부(QRNG/환경 잡음 기반)와 연계되어 높은 엔트로피를 확보함으로써 점진적인 양자 보안 전환을 가능하게 한다.

또한 양자 난수 생성부는 통신 요청 시점의 온도, 습도, 대기압과 같은 환경 정보를 입력 변수로 활용하여 난수를 생성함으로써, 예측 가능성을 최소화하고 암호키의 엔트로피를 향상시킨다.

그림 4. 하드웨어 양자 보안 모듈 형상과 이동단말 App 테스트 시험 환경 구성의 실시예

암호알고리즘 기능이 정확하게 개발되어 올바르게 기능을 제공하는지를 확인하기 위한 암호알고리즘 테스트 CAVP(Cryptographic Algorithm Validation Program) 검증 프로그램을 통해 시험을 수행한다.

제안 구조의 일반 암호 연산부는 AES·ARIA 등 국내 상용망에서 요구되는 검증 알고리즘을 처리하며, 키 관리·암호 경계·모듈 독립성 측면에서 KCMVP 요구사항과 정합 된다. 특히 암호 연산을 단말 OS 와 분리된 하드웨어 경계에서 수행함으로써 키 노출 및 무결성 훼손 위험을 최소화한다. 이는 소프트웨어 기반 암호 모듈 대비 보안성 및 검증 적합성을 향상시킨다.

MCX(MCPTT/MCVideo/MCData) 서비스는 SIP/미디어 평면에서의 종단 보안과 단말 인증 신뢰성이 핵심이다. 제안된 이중 암호 연산 구조는 MCX 단말 인증, 세션 키 보호, 미디어 암호화(SRTP 등) 단계에서 기존 암호 체계를 유지하면서도, 필요 시 양자내성암호를 적용할 수 있어 3GPP MCX 아키텍처와의 호환성을 보장한다. 또한 하드웨어 기반 인증 값 생성은 단말 복제 및 재사용 공격을 억제한다.

5G 보안은 접속(Access)·코어(Core)·서비스 계층 전반에서 키 관리와 암호화 연속성이 요구된다. 제안 구조는 5G 특화 망 환경에서 기존 5G 보안 절차(단말 인증·키 합의)와 충돌하지 않으며, 양자내성암호를 선택적으로 적용하는 하이브리드 방식으로 점진적 전환을 지원한다. 이는 현행 5G 인프라를 유지하면서 미래 양자 위협에 대비할 수 있는 현실적인 이행 전략을 제공한다.

Ⅲ. 결론

본 논문에서는 하드웨어 양자 보안모듈을 기반으로 한 이동통신 단말 보안 관리 구조를 제안하였다. 제안 방식은 단말 인증과 암호 연산을 하드웨어 수준에서 분리함으로써, 기존 소프트웨어 중심 보안 구조의 한계를 효과적으로 보완할 수 있다.

특히 5G 특화망 및 미션 크리티컬 통신 환경에 적용할 경우, 단말 신뢰성 향상과 함께 양자컴퓨팅 위협에 대비한 장기적인 보안성을 확보할 수 있을 것으로 기대된다. 향후 연구에서는 실제 MCX 단말 및 필드 환경에서의 실증 실험을 통해 성능과 운용 효율성을 정량적으로 분석할 예정이다.

ACKNOWLEDGMENT

본 연구는 대한민국 정부(산업통산자원부 및 방위사업청)

재원으로 민군협력진흥원에서 수행하는 민군기술협력사업의

연구비 지원으로 수행되었습니다. (과제번호 23-CM-TC-13).

참 고 문 헌

[1] 이효성 외, “하드웨어 양자 보안모듈에 기초한 통신망 보안 관리 시스템,” 특허출원, 2024.