하이브리드 양자암호 연동형 유무선 통합 네트워크 아키텍처

김용환, 박종협, 김영재
트렌토 시스템즈
{yhkim, jhpark, yjkim}@trento.co.kr

Hybrid Quantum Cryptography Interworking Architecture for Converged Wired - Wireless Networks

Yong-hwan Kim, JongHyeop Park, Youngjae Kim
Trento Systems

요 약

본 논문은 유선 백본(QKD, Quantum Key Distribution)과 무선 구간(PQC, Post Quantum Cryptography), 그리고 개체 인증을 위한 양자서명을 상호보완적으로 결합하고, SDN 기반 네트워크 슬라이싱으로 서비스별 성능·보안 요구를 보장하는 하이브리드 양자암호 연동형 유무선 통합 아키텍처를 제안한다. 또한 하이브리드 키 유도(KDF, Key Derivation Function)로 QKD 키와 PQC 공유비밀을 결합해 종단간 세션키를 생성하는 방식을 제시하고, mONOS(mobility Open Network Operating System) 플랫폼과의 결합을 통해 CSMS/SUMS 규제 대응 및 모빌리티 서비스 적용 가능성을 논의한다. 본 아키텍처는 금융·의료·공공·자율주행 등에서의 상용 실증과 확산을 목표로 한다.

Ⅰ. 서 론

양자컴퓨터의 발전은 현행 공개키 암호의 안전성에 구조적 위협을 제기하며, 이에 대응하기 위한 양자암호통신 전환이 국제 표준 단위(ETSI, ITU T, ENISA)와 차세대 6G 연구(예: 6G SNS)에서 빠르게 논의되고 있다. 특히 5G·Wi Fi 기반의 이동·IoT 환경에서는 유선 구간만 보호하는 기존 체계로는 불충분하여 무선 구간까지 양자 보안 수준을 연동할 수 있는 체계가 요구된다[1].

유무선 통합 네트워크 아키텍처에서 절대적 안전성을 보장하는 QKD 중심 유선 백본망 구성, 무선 액세스 구간 데이터 암호화/인증을 위한 PQC, 개체 간 인증을 위한 양자 서명의 상호보완적 융합을 통한 응용 종단에 대한 양자 보안 체계를 구축함으로써 양자 암호 응용에 대한 하드웨어/소프트웨어 최적화와 실망 검증을 기반으로 양자 보안 인프라 전환에 대한 실효성을 입증할 필요가 있다. 또한 상용화된 유무선 통합 네트워크 솔루션과 연계하여 양자 암호 응용 기술 개발과 실제 양자암호통신 응용 유스케이스에서의 실증이 요구된다.

QKD 기반 양자암호통신은 사전에 QKD 과정을 통하여 통신을 수행하는 종단간 노드들만 알 수 있는 암호화키를 교환함으로써 암호화키를 획득하기 위하여 소요되는 암호화 알고리즘의 소요 시간을 단축할 수 있으며, 종단간 통신 과정에서 암호화에 따른 지연시간을 단축시킬 수 있다. 이에 따라, 초저지연을 요구하는 5G/6G 유스케이스에서 네트워크 성능과 보안성을 동시에 충족시키기 위한 좋은 대안으로 양자암호통신이 활용될 수 있으리라 기대된다.

한편, PQC는 고정된 전용 장비(QKD)에 의존하지 않고 소프트웨어 기반 구현이 가능하여, 향후 확장성 있는 보안 아키텍처 구축에 적합하다[2]. 이를 위해서는 SDN(Software Defined Network) 기반의 유무선 통합 제어가 필수적이며, 다양한 네트워크 슬라이스 환경에 따라 유연한 정책 기반 암호 연동 구조를 제공할 수 있어야 한다[3].

이에 따라, 본 논문에서는 5G/6G 유무선 통합 네트워크에서 초저지연과 보안성을 동시 달성하기 위하여 QKD 중심의 유선 백본, 무선 구간의 PQC, 개체 인증을 위한 양자서명을 상호보완적 융합으로 구성하고 SDN 슬라이싱으로 서비스 수준의 성능을 보장하는 하이브리드 양자암호 연동형 유무선 통합 네트워크 아키텍처를 제안하고자 한다.

Ⅱ. 본론

2.1 시스템 아키텍처

본 아키텍처는 유선(QKD) - 무선(PQC) - 양자서명을 상호보완적으로 결합하고, SDN 기반 네트워크 슬라이싱으로 서비스별 성능·보안 요구를 보장하도록 설계하였다. 무선 이동성과 운용 편의성을 위해 REST API/GUI, 토폴로지 가시화, 사용자·단말 등록/권한 관리를 포함한 통합 제어·관리 계층을 둔다.

- 유선 백본(QKD 중심): 고정 노드 간 물리계층 기반의 절대보안 키 분배로 키 생성·갱신을 담당. QKD를 통해 사전 공유 키를 확보하면 데이터 평면 암복호화 과정의 키 합의에 따른 지연을 줄일 수 있어 초저지연 유스케이스에 유리
- 무선 접속(PQC 중심): 5G/6G·Wi Fi·IoT 단말은 소프트웨어 구현이 가능한 PQC 기반 암호화·상호인증을 수행. 무선 이동성·자원 제약 특성상 경량화된 PQC 프로파일 채택이 타당하며, 국제 표준·정책의 조기 적용이 권고
- 개체 인증(양자서명): 고가치·고위험 트랜잭션(예: OTA SW 업데이트, 제어 명령)에는 양자서명을 적용하여 개체 신뢰를 강화. 이는 PQC 인증을 보완하는 고신뢰 레이어로 작동
- 통합 키·정책 관리(QKMS + SDN Controller): 제어면은 REST API 기반 슬라이싱 CRUD와 정책 기반 라우팅·암호 프로파일 배치를 수행하며, 토폴로지 가시화/사용자·단말 등록/접근권한 제어/모니터링 UI 제공

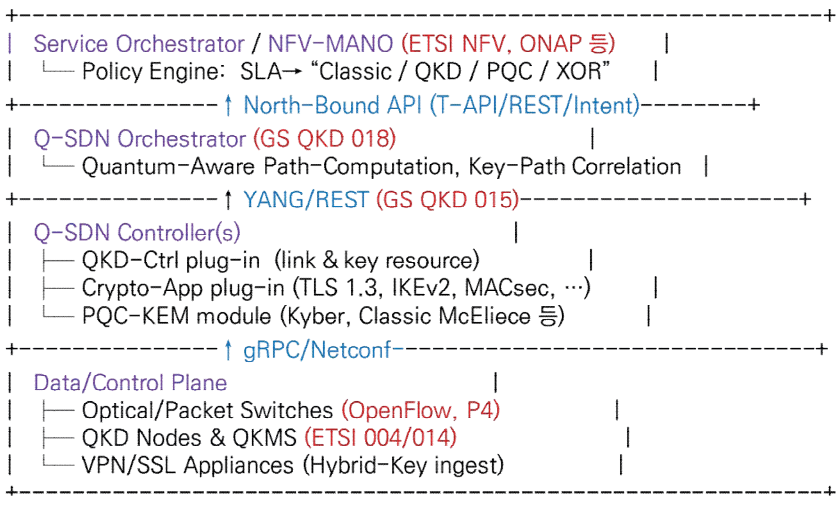

그림 1. 하이브리드 양자암호 연동형 유무선 통합 네트워크 구성도

- 하이브리드 키 유도(KDF): 세션키 K_{sess}는 $K_{sess} = KDF(K_{QKD} \| SS_{PQC} \| context)$로 구성. K_{QKD}는 백본에서 분배된 키, SS_{PQC}는 무선 구간의 PQC 키 합의로 얻은 공유비밀. 이 구조는 현재·미래 양자 위협에 대한 전이적 안전성을 확보함
- SDN 슬라이싱 제어평면: 서비스 수준 KPI를 충족하기 위해 슬라이스 유형을 정의하고, RESTful CRUD로 슬라이스를 관리하고, 슬라이스 생성, 네트워크 성능 충족, 슬라이스 간 격리를 KPI로 운용
- 가시화·운영 기능: 토폴로지 시각화·모니터링, 사용자/단말 인증·등록·권한 제어를 제공하며, 단말 이동 시 세션 유지/슬라이스 변경 제어를 지원
- 플랫폼 연계(mONOS): SDN/슬라이싱 기반 동적 보안 정책 구성과 다중계층보안(MLS, Multi-Level Security)로의 확장을 염두에 두고 mONOS와 결합해 구현 가능

2.2 SDN 기반 구조 및 네트워크 슬라이싱 연계

이기종 서비스가 공존하는 유무선 환경에서 성능(KPI)과 보안 수준을 동시에 보장하려면, 네트워크 자원을 논리적으로 분리해 운용하는 슬라이싱이 핵심 수단이다. 이를 실제로 관측·제어 가능한 운영 기능으로 구현하기 위해서는 SDN 기반의 유무선 통합 제어가 필수이며, 슬라이스별 용도와 위험도에 맞춰 유연한 정책 기반 암호 연동 구조를 제공해야 한다. 다시 말해, 각 슬라이스는 서비스 특성(초저지연, 고처리량, 안전제어 등)에 따라 QKD 키 활용 범위, PQC 프로파일, 양자서명 적용 범위가 정책으로 선언되고, SDN 제어면이 이를 일관되게 배치·갱신하는 형태가 요구된다.

암호 연동은 정책 중심으로 동작한다. 예를 들어, 초저지연 슬라이스는 백본 구간에서 QKD로 사전 분배된 키를 우선 활용해 핸드셰이크 부담을 최소화하고, 무선 구간은 경량화된 PQC 프로파일로 상호인증을 수행한 뒤 하이브리드 KDF로 세션키를 산출한다. 안전제어 슬라이스는 제어 명령·OTA 갱신에 양자서명을 추가 적용해 무결성과 보안성을 강화한다.

한편, 이동성 또한 슬라이싱 정책의 적용 대상이다. 단말 이동 시 세션을 유지하면서 슬라이스를 재선정하거나 정책을 동적으로 재배포해야 하므로, SDN 제어면은 무선 접속 이벤트와 연계된 세션 유지·슬라이스 변경 제어를 제공한다. 또한 SDN 기반 통합 운용은 토폴로지 시각화·사용자/단말 등록·접근권한 제어 UI와 함께 제공되어 현장 운영 복잡도를 낮춘다.

제안한 하이브리드 보안 아키텍처는 mONOS와 같은 SDN·네트워크 슬라이싱 기반 플랫폼 위에서 바로 구현할 수 있다. mONOS는 자체 네트워크 격리 도메인을 통해 슬라이스 간 트래픽을 분리하고, 응용 데이터의 암복호·인증 정책을 동적으로 구성할 수 있도록 설계되어 있어 동적 보안 정책 구성 가능하기 때문에 본 연구의 정책 기반 암호 연동을 슬라이스 단위로 배치·운영하는 데 적합하다. 또한 자동차 사이버보안 CSMS/SUMS 등 규제 대응을 목표로 한 적용 계획이 마련되어 있어, 실제 상용·규제 환경으로의 이전을 염두에 둔 실증에 유리하다.

해당 구조는 정책 템플릿을 슬라이스에 바인딩한 뒤, 텔레메트리 기반 KPI 모니터링으로 운용 편차를 감지하고, 편차가 발생하면 암호 프로파일(예: PQC 파라미터)이나 키 주기(QKD/PQC)를 자동 조정하는 폐루프(Closed Loop) 운용이 가능하다. mONOS의 동적 정책 구성 역량을 활용하면 이러한 자동 조정이 정책 수준에서 일관되게 적용되며, 규제 요건과 서비스 KPI를 동시에 만족하는 방향으로 수렴시킬 수 있다.

Ⅲ. 결론

본 논문은 하이브리드 양자암호 연동형 유무선 통합 네트워크 아키텍처를 제안한다. 본 네트워크 환경 구현은 단순한 보안 기술의 도입을 넘어서, 향후 양자 시대의 미래형 통신 인프라로 나아가기 위한 핵심 이행 단계로서의 의미가 있다. 특히, 정부기관, 금융, 의료, 자율주행 등 고신뢰 통신이 필요한 분야에 있어 본 환경은 실효적 보안성과 운용 효율성을 동시에 제공할 수 있는 기반 환경으로 작용할 것으로 기대된다.

ACKNOWLEDGMENT

본 연구는 2025년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구 결과 임 (RS-2024-00460803, SW 딥테크 기술 글로벌 경쟁력 강화 사업)

참 고 문 헌

[1] ETSI TS 103 744 V1.2.1, "Quantum Safe Hybrid Key Establishment", 2025 03..

[2] ITU T X.1714, "Key combination and confidential key supply for QKDN" 2020-10.

[3] Scalise, Paul, et al. "An Applied Analysis of Securing 5G/6G Core Networks with Post-Quantum Key Encapsulation Methods." Electronics 13.21 (2024): 4258.