전력 계통 양자 컴퓨팅 위협 대응을 위한 양자내성암호 적용 방안 연구

김수현, 김민용, 이준영*

한전KDN(주) 전력ICT기술원 전력보안기술부

{suhyeon2_12, kmyong_0902, ljy.953386}@kdn.com

A Study on the Application of Post Quantum Cryptography to Counter Quantum Computing Threats in Power Systems

SuHyeon Kim, MinYong Kim, JunYoung Lee*

KEPCO-KDN. Power ICT Technology Institute, Power Security R&D Team

요 약

양자컴퓨팅의 발전은 RSA, ECC 등 기존 공개키 암호체계의 안전성을 근본적으로 위협하고 있다. 전력 계통은 국가 핵심 기반 시설로, 보안 통신이 무력화될 경우 전력 공급 중단 등 심각한 사회적 피해가 발생할 수 있다. 이에 미국 NIST는 양자내성암호 표준화를 추진하여 FIPS 203, 204 등 표준을 발표하였다. 본 연구는 이러한 위협에 대응하기 위해 전력 계통에 적용 가능한 양자내성암호 활용 방안을 제안한다. 첫째, X.509 기반 인증서 체계를 PQC 알고리즘으로 확장하여 장기적 안전성을 확보한다. 둘째, 기존 KCMVP 검증 알고리즘과 PQC를 병행 지원하는 하이브리드 암호모듈을 설계하여 제도적 요구와 기술적 전환을 동시에 충족한다. 셋째, OpenSSL Provider 구조를 활용해 PQC 기반 TLS 보안 라이브러리를 구현함으로써 전력망 통신에서 효율적이고 안정적인 암호 서비스를 제공한다. 이를 통해 양자 시대에도 전력망의 안정적 운영 기반을 제공한다.

Ⅰ. 서 론

급속한 양자컴퓨터 기술의 발전으로 인해 현재 널리 사용되는 RSA, ECC 등의 공개키 암호체계는 근본적인 보안 위협에 직면하고 있다. 쇼어(Shor) 알고리즘과 그로버(Grover) 알고리즘은 주요 양자 알고리즘으로서, 공개키 및 대칭키 알고리즘을 쉽게 해독할 수 있다. 이러한 위기에 대응하기 위해 미국 NIST는 양자내성암호(PQC) 표준화를 적극 추진하고 있으며, 2024년 8월 FIPS 203, 204, 205 표준을 최종 발표하는 등 국제적으로 암호체계 전환에 대한 논의가 가속화되고 있다.[1]

항목	쇼어알고리즘	그로버알고리즘
적용 대상	공개키 암호(RSA, ECC 등)	대칭키 암호(ARIA, AES 등), 해시함수
특징	인수분해 문제 해결 속도 감소	정렬되지 않는 데이터베이스의 원소를 검색하는 속도 향상
영향	현재 암호로 해결할 수 없으므로 양자내성암호로 전환 필요	암호 알고리즘 키 길이 증가 필요

표 1. 기존 암호체계와 PQC 알고리즘 비교

특히 전력망은 국가 핵심 인프라로서 양자컴퓨터 공격에 취약한 기존 공개키 암호체계가 무력화될 경우, 악의적인 제어 명령 삽입이나 중요 데이터 유출을 통해 전력 공급 중단, 설비 손상 등이 발생하여 국가 차원에서 광범위한 사회·경제적 손실을 야기시킬 수 있다. 전력 계통의 SCADA, AMI, 분산 전원 관리 시스템 등은 실시간성과 안정성이 중요하므로, 암호체계 전환으로 인한 지연이나 장애는 국가 전력 공급에 치명적 영향을 미칠 수 있다. 이를 위해서는 기존 검증된 암호체계와 PQC를 하이브리드 방식으로 병행 운용하여 가용성을 확보하고, 시스템 전환에 따른 리스크를 완화할 수 있는 기술적 접근이 필요하다. 본 논문은 전력망 환경에 최적화된 PQC 기반 인증서 관리, 하이브리드 암호모듈 및 양자암호모듈 적용 TLS 기술 방안을 제시한다.

Ⅱ. 본론

2.1 PQC 기반 인증서 도입 및 관리

전력 계통은 안정적인 TLS 통신을 위해 PKI(Public Key Infrastructure, 공개키 기반 구조) 기반 인증서 체계를 필수적으로 사용한다. 이는 X.509 표준을 기반으로 하며, 루트 인증 기관(Certificate Authority)이 최종 사용자(End-Entity, EE)의 신원을 확인하기 위해 인증서를 발급한다[2]. 현재 발급되는 인증서는 주로 RSA 또는 ECDSA으로 서명되어 있으며, 이는 전력 계통 PKI 시스템 및 암호모듈에서도 동일하게 적용되고 있다.

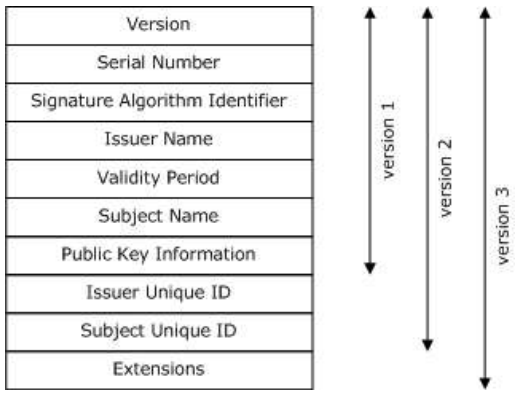

그림 1. X.509 아키텍처

그러나 RSA와 ECC는 양자컴퓨터의 쇼어 알고리즘에 의해 다항 시간 내에 해독될 수 있어, 장기간 운용되는 전력망 장비에서 심각한 보안 위협을 초래한다. 이는 인증서가 발급 시점에는 안전하더라도, 향후 양자 위협

이 현실화되면 전체 PKI 신뢰 체계가 붕괴될 수 있음을 의미한다. 따라서 전력 계통은 기존의 RSA 및 ECC 기반 인증서에서 벗어나 PQC 기반 인증서로의 전환이 필수적이다. NIST 표준화 과정에서 최종 선정된 ML-KEM, Falcon과 같은 알고리즘은 공개키 암호 및 전자서명 분야에서 양자환경에서도 안전성을 확보할 수 있는 대안으로 주목받고 있다. 이러한 PQC 알고리즘을 X.509 인증서 내부의 공개키 및 서명 필드에 반영하면, 기존 구조를 유지하면서도 양자 안전성을 보장할 수 있다. 구현 관점에서 PQC 기반 인증서 도입을 위해서는 PKI 시스템의 전면적 확장, 암호모듈의 PQC 알고리즘 지원, SCADA 및 AMI 등 환경에서의 운용 최적화가 종합적으로 고려되어야 한다. 이러한 전환은 단순히 새로운 알고리즘을 도입하는 수준이 아니라, 전력망 전체 보안 체계의 근본적 재구성을 의미한다. 궁극적으로, PQC 기반 인증서 체계는 양자 컴퓨팅 시대에도 전력 계통이 안정적이고 신뢰성 있게 운영될 수 있는 기반을 제공할 것이다.

2.2 PQC 적용 하이브리드 형태의 암호모듈 개발

전력 계통에서는「사이버 안보 업무 규정」제9조, 「전자정부 시행령」제 69조 등 관련 법령에 의거하여 암호모듈의 안전성과 구현 적합성을 검증하는 KCMVP(Korea Cryptographic Module Validation Program, 국내 암호모듈 검증 제도) 인증을 획득한 암호모듈 사용이 의무화되어 있다. 그러나 현재 NIST, K-PQC 표준에 따른 PQC 알고리즘은 아직 KCMVP 검증대상 알고리즘으로 지정되지 않아 즉시 적용하기에 제도적 한계를 가진다. 따라서 기존 검증 대상 알고리즘과 비검증대상 PQC 알고리즘을 선택적으로 병행 지원하는 하이브리드 암호모듈 개발이 필요하다.

제안하는 하이브리드 암호모듈은 KCMVP 검증 대상 알고리즘(ARIA, LEA, ECDSA 등)과 PQC 알고리즘(ML-KEM, ML-DSA 등)을 동시에 지원하는 구조를 갖는다. 현재 운영 단계에서는 KCMVP 검증 대상 알고리즘을 우선 적용하여 제도적 요구사항을 충족하고, 동시에 표준을 만족하는 PQC 알고리즘을 병행 지원하여 향후 PQC 알고리즘이 검증 대상 암호 알고리즘으로 등재되었을 경우 즉시 적용 가능하도록 구현되었다. 이를 통해 양자 위협에 대한 점진적인 보호를 제공한다.

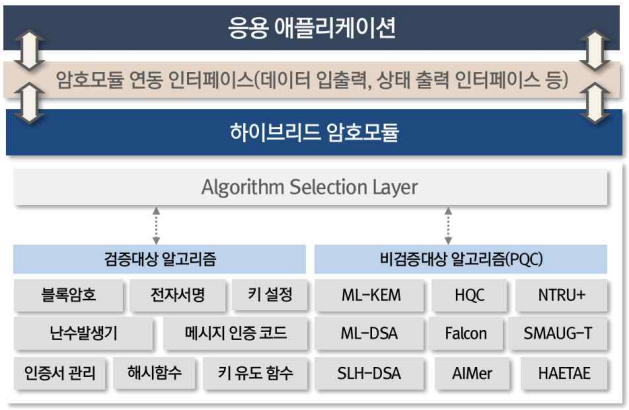

그림 2. 하이브리드 암호모듈 아키텍처

2.3 PQC 기반 TLS 보안 라이브러리 개발

양자내성암호의 산업계 활용에서 TLS 1.3 연계는 매우 중요한 요소이다. 기존 현대암호(RSA, ECC) 대비 PQC 알고리즘의 큰 키 크기와 서명 크기로 인해 높은 네트워크 부하를 발생시킬 가능성이 크기 때문이다. 이에 따라 TLS 1.3 Handshake 단계에서 발생하는 네트워크 부하를 고려한 최적화가 필수적이며, 특히 네트워크 패킷 교환 관점에서 중점적인 양자내성암호 최적화가 요구된다.

전력 계통에서 널리 사용되는 OpenSSL 프로토콜 환경에 PQC를 효율적으로 통합하기 위해 OpenSSL 3.0의 Provider 아키텍처를 활용한다. Provider는 OpenSSL 3.0부터 암호모듈의 유연한 확장을 위해 도입된 구조로, 신규 알고리즘 추가 및 기존 암호 변경이 간편하며, 플러그인 형태로 OpenSSL의 별도 재컴파일이 불필요하다는 장점을 가진다. 따라서 OpenSSL Provider를 통해 앞서 개발한 KCMVP 하이브리드 암호모듈을 연계하여 전력 계통 환경에 최적화된 PQC 지원 TLS 라이브러리를 구현한다.

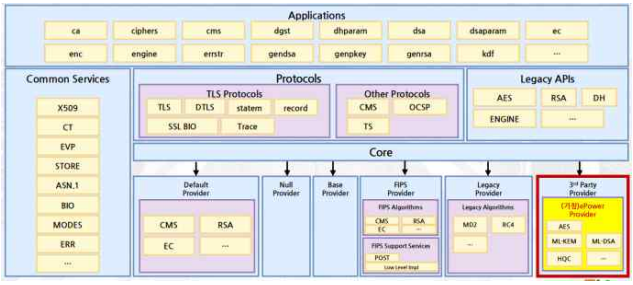

그림 3. OpenSSL Provider 구성도

Provider 설계 시에는 전력 계통의 다중 처리 환경을 고려하여 Multi-thread 안전성을 보장하도록 구현한다. 이를 통해 SCADA, AMI 등 동시다발적 통신이 발생하는 전력 계통 환경에서도 안정적인 암호화 서비스를 제공할 수 있다. 또한 양자내성암호 전환에 대비한 하이브리드 Ciphersuite 기능을 제공하여 기존 알고리즘과 PQC 알고리즘을 선택적으로 사용할 수 있도록 한다. 양자내성암호 KEM은 기존 ECDH 키 교환과 달리 키 캡슐화 메커니즘으로 동작하므로 PQC 인증서 기능 연계를 위해 TLS Handshake 단계에서 ML-KEM을 새롭게 구현한다.

Ⅲ. 결론

본 논문에서는 전력 계통의 양자 컴퓨팅 위협에 대응하기 위한 PQC 적용 방안을 제시하였다. PQC 기반 인증서 관리 체계 구축을 통해 전력 계통 전반의 신뢰성 있는 인증 기반을 마련하고, 하이브리드 암호모듈을 통해 기존 시스템과의 호환성을 보장하면서 점진적 전환이 가능한 구조를 제안하였다. 또한 양자암호모듈을 적용한 TLS 프로토콜 강화를 통해 전력 계통 통신의 종단간 보안을 확보하는 방안을 제시하였다.

제안된 기술들은 전력 계통의 제도적 요구사항과 기술적 특성을 모두 고려하여 설계되었으며, 실제 전력망 환경에서의 성능 검증과 상용화 가능성을 평가하기 위한 실증 계획을 수립하여 향후 연구를 진행할 예정이다. 이를 통해 국가 핵심 인프라인 전력 계통이 양자 컴퓨팅 시대에도 안전하고 안정적으로 운영될 수 있는 기술적 기반을 제공할 것으로 기대된다.

참 고 문 헌

[1] NIST, "Post-Quantum Cryptography Standardization," FIPS 203, 204, 205, August 2024.

[2] 심민주, 서화정, “양자내성암호와 X.509 설계 동향”, 정보보호학회지, 2024.12

[3] 심규석, 이원혁. “양자암호서비스를 위한 PQC-TLS 하이브리드 프로토콜 개발”. 한국통신학회 학술대회논문집, 2024.1.31.

[4] 김명준, 서유진, 김영식. “NIST PQC와 KpqC 알고리즘 비교 분석”. 한국통신학회 학술대회논문집. 2025.6.18.