양자암호서비스를 위한 PQC-TLS 하이브리드 프로토콜 개발

심규석, 이원혁
한국과학기술정보연구원
{kusuk007, livezone}@kisti.re..kr

Developing a PQC-TLS Hybrid Protocol for Quantum Cryptography Services

Kyu-Seok Shim, Wonhyuk Lee
Korea Institute of Science and Technology Information

요 약

국가연구망은 스타형 네트워크 토폴로지 형태를 가지고 있으며 이에 맞는 양자암호통신망을 구축하기 위한 양자키 관리망을 구축하고 있다. 양자암호통신망을 구축하기 위해 양자키분배 장치(Quantum Key Distribution, QKD), 양자키관리 시스템(Quantum Key Management System, QKMS), 양자암호모듈(Quantum Encryptor, QENC)를 구성해야하며, 모든 구성요소가 연결되어 하나의 양자암호통신망을 구축할 수 있다. 현재 각 구성요소간 연결을 위해 지속적인 표준문서가 발표되고 있지만, 상세한 부분에 대한 내용은 포함하고 있지 않다. 따라서 본 논문에서는 양자키관리 시스템에서 양자암호모듈로 양자키를 공급할 때 해당 구간의 양자내성을 가지기 위한 현재의 암호 기술과 양자내성암호(Post-Quantum Cryptography, PQC) 기술을 결합한 하이브리드 형태의 TLS 암호 기술을 개발한 내용을 제안한다. 제안하는 기술은 양자키를 담고 있는 메시지를 전달하기 위해 PQC 인증 및 암호화알고리즘 뿐만아니라 현재 암호기술인 KCMVP 검증 대상 알고리즘을 하이브리드 형태로 사용하여 해당 구간 양자내성을 확인하였다.

Ⅰ. 서 론

국가 과학기술연구망은 양자컴퓨터 시대를 대비한 차세대 보안으로 양자암호통신망 구축을 진행하고 있다[1]. 이제 양자키분배장치, 양자키관리 시스템 등 양자암호통신망을 구성하는 구성요소들을 개발하고 운영하기 위한 기술을 개발하고 있다[2]. 또한 각 구성요소들을 개발하고 각 구성요소들간의 양자키 및 설정정보, 상태정보를 전송하기 위한 인터페이스 개발을 진행하고 있다. 인터페이스 개발을 위해 국외 및 국내 표준을 준용하여 향후 호환성 측면을 고려하여 개발해야한다[3]. 하지만 안전한 양자암호통신망을 구축하기 위해서는 표준을 준용하면서 보안성도 매우 고려해야한다.

현재 양자키관리 시스템과 양자암호모듈간의 인터페이스에서는 양자암호모듈이 양자키로 데이터를 암·복호화 하기 위해서는 양자키관리 시스템에서 양자키를 공급해야한다. 이 과정에서 양자키가 직접 전달되며 매우 보안성을 고려해야하는 구간이다. 기존 해당 구간 보안성을 고려하기 위해 물리적 보안경계 구간으로 설정하여 인가된 사용자만의 물리적 보안경계로 들어와서 사용할 수 있다는 설정을 하였다. 하지만 사용성이 감소되고, 인가된 사용자에 대한 오류가 발생할 수 있기에 불완전한 방법이다. 따라서 본 논문에서는 용이한 양자암호서비스를 위해 해당 구간을 양자내성암호와 기존 암호기술을 하이브리드 형태로 사용하여 양자내성을 가질 수 있는 PQC-TLS 하이브리드 프로토콜 개발한 내용을 제안한다. 제안하는 방법은 양자키를 담고 있는 메시지를 전달하기 위해 양자키관리 시스템과 양자암호모듈간의 PQC 대상 인증 알고리즘인 Dilithium 알고리즘을 사용하여 인증을 수행하고, PQC 대상 암복호화 알고리즘인 NTRU 알고리즘 및 KCMVP 대상 알고리즘인 ARIA 알고리즘을 하이브리드 형태로 사용하여 암복호화한다. 해당 개발 기술을 검증한 결과 PQC 알고리즘을 활용한 인증 및 암복호화를 모두 수행하고, 암복호화 속도 또한 기존 ARIA 알고리즘 기준인 24mbps 이상의 암복호화 속도를 검증하였다.

Ⅱ. 본론

본 논문에서는 양자키관리 시스템과 양자암호모듈간의 양자내성 보안성을 보장하기 위한 현재의 암호 기술과 양자내성암호 기술을 결합한 하이브리드 형태의 TLS 암호기술을 제안한다. 제안하는 방법은 양자키관리 시스템에 설치되며 응용서비스의 하이브리드 TLS 요청에 대하여 연결설정과 양자키를 제공하는 프록시 데몬과 응용서비스에게 하이브리드 TLS 인터페이스를 제공하는 클라이언트 API로 구성된다. PQC-TLS 하이브리드 프록시는 양자키고나리 시스템 장비 내부에 설치되는 소프트웨어로 아래 그림1과 같은 블록 구성을 가진다.

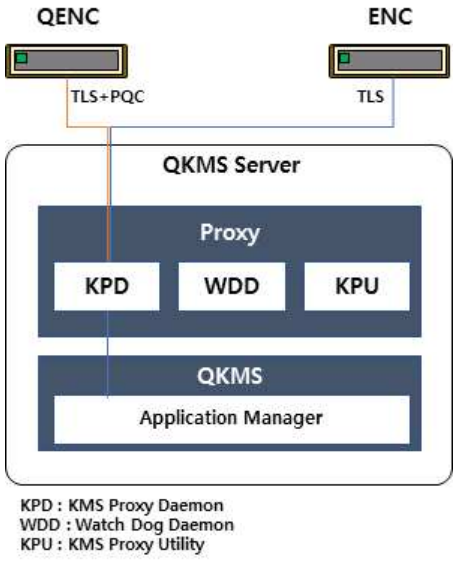

그림 1 PQC-TLS 하이브리드 프록시 블록 구성

그림1의 블록에서 KPD는 TLS+PQC 프로토콜 서비스 처리 데몬을 의

미하고, WDD는 프로세스 감시 데몬, 그리고 KPU는 운용 관리 유틸리티로 구성한다. 시스템의 외부연동은 양자 암호 응용서비스와 연동 및 양자키관리 시스템과 연동을 수행하고 응용서비스와는 하이브리드 TLS 인터페이스에 따라 TLS+PQC 또는 TLS 프로토콜을 선택적으로 기동하여 연동하고 양자키관리 시스템과는 TLS v1.3 프로토콜로 연동한다.

TLS 프로토콜 내의 KCMVP 암호모듈과 PQC 암호모듈을 구성하기 위해 아래 그림2와 같이 알고리즘을 정의하였다. PQC Key Share 알고리즘으로 NTRU KEM 알고리즘, PQC Signature 알고리즘으로는 dilithium_shake256 알고리즘을 선정하였다.

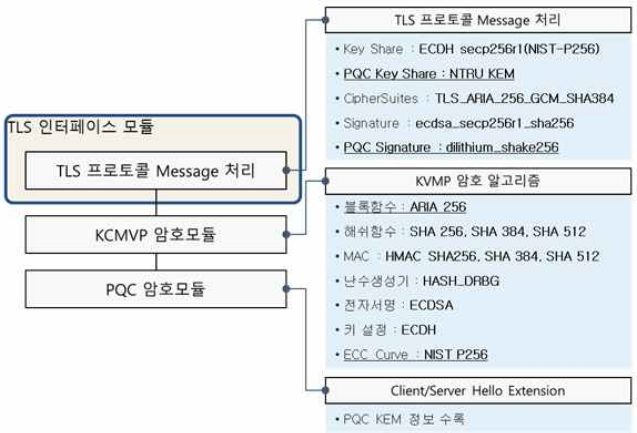

그림 2 KCMVP 및 PQC 알고리즘 정의

TLS 프로토콜 메시지의 Key Share, CipherSuites, Signature는 KCMVP 검증 대상 암호 알고리즘에 대응하여 정의하고, PQC 알고리즘을 사용한 TLS 프로토콜의 Client Hello Extrension과 Server Hello Extension 메시지를 확정 정의하였다.

위와 같이 구성된 PQC-TLS 하이브리드 프로토콜을 사용하여 패킷을 캡처하고, 캡처한 패킷에서 Client Hello 메시지를 확인한 결과 아래 그림3과 같은 결과를 얻을 수 있었다. Client Hello 메시지 내에 Extenstion Signature Algorithm 부분을 확인하면 0xff01, 0xff02, 0xff03, 0xff04와 같은 결과가 도출되는데 이는 Wireshark에서 dilithium 알고리즘을 파싱하지 못하여 정의한 내용을 보여주는 결과이다. 정의된 내용은 다음 표1와 같다.

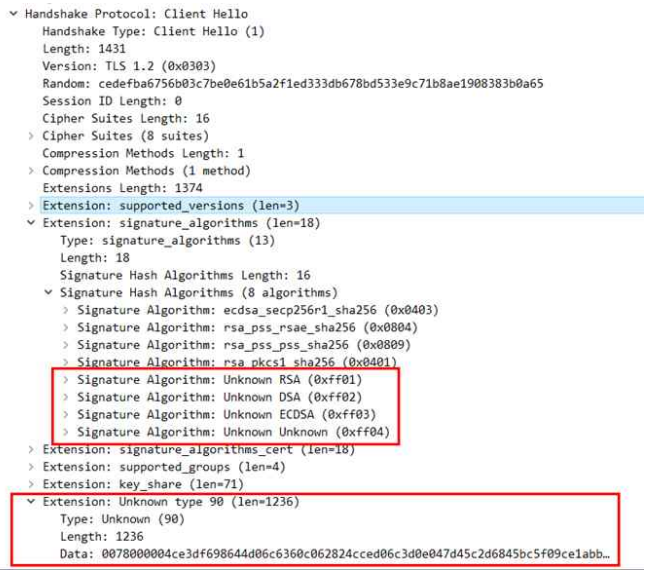

그림 3 Client Hello 메시지

표 1 Extension Signature Algorithm 정의

코드	정의
0xff01	mt_sigalg_dilithium3_shake256
0xff02	mt_sigalg_dilithium3_aes_shake256
0xff03	mt_sigalg_dilithium5_shake256
0xff04	mt_sigalg_dilithium5_aes_shake256

또한, 그림3에서 Extension: Unknown Type 90으로 정의한 부분은 PQC Key share를 위해 정의한 부분으로 90번으로 정의하여 해당 부분에 PQC Key를 삽입하였다. 마지막으로 평문을 활용하여 암복호화 속도를 측정하였을 때 초당 3Mbyte 이상 암복호화 송수신하는 결과를 확인하였다.

Ⅲ. 결론

본 논문에서는 양자키관리 시스템과 양자암호모듈간의 인터페이스에서 보안성을 강화하기 위해 해당 구간을 양자내성화하였다. 양자내성화를 위해 PQC 알고리즘을 TLS 프로토콜에 확장시켜 사용하였으며 기존 컴퓨팅 체계로도 취약해지지 않도록 기존 암호기술과 함께 하이브리드 형태로 개발하였다. 해당 구간을 양자내성화 함으로써 호환성 및 양자암호 서비스 활용도가 높아질 것으로 기대하며, 향후 국가 과학기술연구망에서 사용될 때 다수의 사용자에게 양자암호서비스를 공급할 수 있으며, 안전한 양자암호통신 서비스를 제공할 수 있을 것으로 기대한다.

ACKNOWLEDGMENT

본 연구는 2024년도 한국과학기술정보연구원(KISTI) 주요 사업 과제로 수행한 것입니다.

참 고 문 헌

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum Cryptography,” Rev. Mod. Phys., Vol.74, No.1, 2002, p.145

[2] 이원혁, 석우진, 박찬진, 권우창, 손일권, 김승해, 박병연, “양자암호기반의 통신망 구축 및 성능시험 검증연구”. KNOM Review, 2019, vol.22, No.02, pp39-47

[3] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus,“Field test of quantum key distribution in the Tokyo QKD Network”, Optics Express, Vol 19, Issue 11, 2011