양자암호서비스 사용자 확장을 위한 적응형 암호화 양자키 공급 시스템

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

Adaptive Encryption Quantum Key Supply System for Expanding Quantum Cryptographic Service Users

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

요 약

QKD(Quantum Key Distribution) 기반의 양자암호통신 필요성이 증가하면서 양자암호통신망 활용성에 집중되고 있다. QKD 기반 양자암호통신은 양자컴퓨터에서 운용되는 Shor알고리즘으로부터 방어되는 암호체계로 기존 소인수분해 기반 RSA 암호체계를 대체할 수 있는 방법이다. QKD 기반 양자암호통신은 양자컴퓨터로부터 보안이 가능하다는 장점이 있지만, 네트워크 운용상으로 많은 단점을 가지고 있고, 이를 해결하기 위한 방법으로 QKMS(Quantum Key Management System)를 활용하여 QKD의 단점을 극복하는 방법을 사용한다. 본 논문에서는 양자암호서비스를 이용하려는 사용자의 확장을 위해 적응형 암호화를 통해 사용자 선택적 암호체계를 적용하여 양자키를 공급할 수 있는 시스템을 제안한다. 양자키관리 시스템은 QKD에서 생성된 키를 저장하고 있다가 사용자의 요청에 의해 사용자 보안요구사항에 맞는 양자키를 공급한다. 해당 구간에서 사용자는 양자키를 보호하기 위해 PQC(Post-Quantum Cryptography) 암호체계를 사용하여 키를 수신받거나, PQC 암호체계를 사용할 수 없는 환경이라면 TLS 암호체계를 사용한 양자키를 공급할 수 있는 시스템이다.

Ⅰ. 서 론

양자컴퓨터 개발로 인한 다양한 양자컴퓨터 기반 양자알고리즘들이 등장하면서 기존 체계들이 급변하고 있다. 그 중 대표적인 사례가 바로 Shor 알고리즘의 등장으로 인한 기존 암호체계 보안성이 낮아진 것이다. 기존 소인수분해 기반 RSA 암호체계는 Shor 알고리즘에 의해 비교적 짧은 시간안에 암호를 해독할 수 있고, 이에 따라 새로운 보안체계의 필요성이 증가되었다.

그 중 대표적인 보안체계는 QKD 기반의 양자암호통신이다. QKD는 양자컴퓨터로부터 안전하게 대칭키를 생성해내는 장치인데, 보안성은 높일 수 있지만 네트워크 운영 과정에서의 많은 한계들이 있다는 평가를 받는다. 네트워크 운영자 입장에서 이러한 한계를 해결하기 위한 방법들이 요구되고 있고, 양자키관리 시스템은 대표적인 방법이다. 양자키관리 시스템은 QKD에서 생성된 양자키를 안전하게 저장하고, 사용자의 요구에 따라 양자키를 공급한다. 그러나 사용자와 QKMS간의 연결에서 보안대책이 마련되지 않았으며, 사용자는 다양한 환경에서 존재한다. 예를 들면, 원격지의 사용자가 양자암호통신 서비스를 사용하기 위해서는 높은 보안성을 요구하며, 내부 사용자의 경우 기존 암호체계 정도의 보안성이 요구될 수 있다.

본 논문에서는 양자암호서비스 사용자의 다양한 환경을 고려하여 서비스 대상을 확장시키기 위해 유연한 보안 체계를 지원하는 시스템을 제안한다. 제안된 시스템은 QKD에서 생성된 키를 양자내성암호(PQC, Post-Quantum Cryptography) 기반 암호체계를 통해 안전하게 전달하거나 양자내성암호가 지원되지 않는 사용자의 경우 일반 TLS 암호체계를 활용하여 양자키를 공급하는 방식이다. 제안하는 시스템을 통해 다양한 사용자 환경에서 효과적으로 양자암호서비스를 제공할 수 있는 기반을 마련할 수 있다.

Ⅱ. 본론

본 논문에서는 양자암호서비스 사용자의 다양한 환경을 적용하기 위한 적응형 양자키 공급 시스템을 제안한다. 본 시스템은 양자키관리 시스템에서 사용자에게 키를 공급할 때 키를 암호화할 수 있는 방법을 사용자 환경에 맞게 적용한다. 따라서 본 장에서는 양자암호통신의 구조와 양자키관리 시스템에 대해 간략히 소개하고, 제안하는 시스템에 대한 내용을 소개한다.

양자암호통신 구조는 아래 그림과 같이 QKD, QKMS 그리고 사용자가 접근할 수 있는 QENC(Quantum Encryptor)로 구성된다. QKD는 양자키 분배장치로 양자역학적 원리를 이용하여 동일한 랜덤값을 두 장치간 나누어갖고, 그것을 키로 사용한다. QKMS는 QKD에서 생성한 양자키를 저장하고 관리하며, QKD에서 할 수 없는 다대다 통신, 중·장거리 통신을 가능하게 한다. 마지막으로 QENC는 QKMS에 키를 요구하며 해당 키를 받아서 실제 데이터를 해당 키로 암호화하고, 상대방 QENC와 인증을 통해 연결한 뒤 암호화된 데이터를 송신한다. 또한, 상대 QENC는 암호화된 데이터를 수신한 뒤 복호화 하여 사용자에게 전달한다.

그림 1 QKD 기반 양자암호통신 구조

양자키관리 시스템은 양자키분배 장치로부터 키를 수신하여 키의 생애 주기 관리 및 효율적인 양자암호통신망 운영을 위해 사용된다. QKD는 단대단으로 연결되어 대칭키를 공유하는 시스템으로 네트워크화하기에는 많은 한계가 존재한다. 대부분의 QKD 장비는 광원을 재료로 키를 생성하기 때문에 거리의 한계가 존재한다. 이 부분은 양자키관리 시스템의 키전달 기능으로 극복한다. 따라서 양자키관리 시스템은 양자암호통신 구조에서 매우 필수적인 구성요소이다.

현재 QKMS와 QENC 구간은 특별한 보안대책이 없다. 따라서 QKMS와 QENC를 물리적보안경계로 설정하여 물리적인 보안에 기대할 수 밖에 없다. 그러나 활용성 측면에서 많은 연구가 이루어지고 있고, 다양한 보안대책을 적용하고 있다. 그 중 가장 유력한 보안대책은 PQC 알고리즘을 사용하는 방법이다. 그러나 양자암호통신 사용자의 환경은 다양하고, 따라서 해당 구간 보안체계를 다양화할 수 있어야한다. 따라서 본 논문에서 제안하는 시스템은 QKMS에 내장되어 PQC 또는 기존 TLS 암호체계로 양자키를 보낼 수 있는 적응형 시스템을 제안한다.

제안하는 시스템 아래 그림과 같이 PQC를 지원하여 양자키를 암호화해서 양자키를 서비스노드에 전송할 수 있고, 또 다른 방식으로 기존 RSA 방식을 사용하여 서비스노드에 전송할 수 있다. A 서비스 노드는 PQC를 지원하는 노드로 PQC 암호화하여 키를 전송하였고, B 서비스 노드는 PQC를 지원하지 않기 때문에 RSA 방식으로 암호화하여 키를 전송하였다. 암호화하여 서비스노드에게 양자키를 보내 QKD 키를 이용한 양자암호통신을 완료하였다.

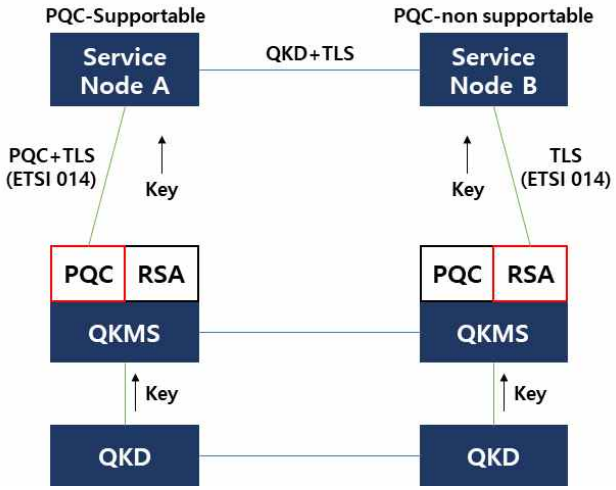

그림 2 적응형 양자키 공급 시스템

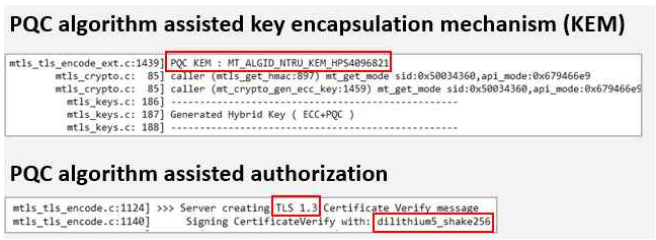

그림 3 인증 및 암복호화 PQC 알고리즘

본 시스템은 서비스 노드에서 QKMS로 키를 요청하고, QKMS는 서비스노드를 확인하는 과정에서 TLS 1.3 확장필드를 기반으로 서비스노드의 PQC 지원 가능성을 확인한다. TLS 1.3 필드에 QKMS가 지원할 수 있는 PQC 인증 및 암복호화 목록을 Client Hello 메시지에 포함시켜 보내고, 서비스노드는 Client Hello 메시지를 확인하여 서비스 노드에서 사용할 수 있는 PQC 인증 및 암복호화 알고리즘 목록을 Server Hello 메시지를 통해 전송한다. 만약 서비스 노드 B와 같이 PQC 알고리즘을 사용할 수 없는 노드라면 기존 TLS 암복호화를 수행한다. 그림 3은 해당 과정에서 PQC 알고리즘 사용 관련 로그메시지이다. 인증을 위한 알고리즘으로는 Dilithium5_shake256을 사용하였고, 암복호화 알고리즘으로 NTRU 알고리즘을 사용하였다.

최종적으로 두 서비스 노드간 양자키를 활용한 데이터 암호화를 통해 데이터 전송을 확인하였으며, 서비스 이용이 가능한 것을 확인하였다. 본 시스템을 통해 양자암호통신의 유연성을 크게 향상시킴으로써 다양한 환경에서 양자암호통신을 사용할 수 있는 것을 확인하였다.

Ⅲ. 결론

본 논문에서는 적응형 양자키 공급 시스템을 제안하여, 양자암호통신 환경에서 사용자의 다양한 요구와 환경에 대응할 수 있는 유연한 키 공급 방식을 구현하였다. 기존 QKD 기반 양자암호통신이 가진 거리적 제약과 단대단 통신의 한계를 보완하기 위해 QKMS의 기능을 확장하였으며, PQC와 기존 암호체계를 병행하여 보안성과 실용성을 동시에 확보하였다.

제안된 시스템은 TLS 1.3의 확장필드를 활용하여 서비스 노드의 PQC 지원 가능 여부를 확인하고, 적절한 키 암호화 방식을 선택적으로 적용하였다. 실제 실험에서 PQC를 지원하는 노드는 Dilithium5_shake256을 통해 인증을 하였고, NTRU 알고리즘을 사용한 암호화 방식을 적용하였다. 지원하지 않는 노드에는 기존 RSA 기반 암호화 방식을 활용하여 양자키를 안전하게 전달할 수 있도록 설계하였다.

향후 연구에서는 제안된 시스템의 성능을 실제 네트워크 환경에서 평가하고, 다양한 PQC 알고리즘과의 호환성을 검증함으로써 시스템의 안정성과 확장성을 더욱 강화해야 할 것이다. 이를 통해 적응형 양자키 공급 시스템은 차세대 양자암호통신망의 핵심 기술로 자리 잡을 수 있을 것으로 기대된다.

ACKNOWLEDGMENT

이 논문은 2025년도 한국과학기술정보연구원(KISTI)의 기본사업으로 수행된 연구입니다. (과제번호: K25L5M2C2)

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] 심규석, 김용환, 이찬균, 이원혁. “KREONET 양자암호통신 환경에서 양자키 관리 시스템을 위한 양자키 저장 관리 모듈 설계 및 검증”, 2022년 한국통신학회 동계학술대회

[3] Shim, Kyu-Seok, Yong-Hwan Kim, and Wonhyuk Lee. "A design of secure communication architecture applying quantum cryptography." Journal of Information Science Theory and Practice 10.spc (2022): 123-134.