양자키분배 시스템 보안 요구 요구사항 도출 및 대응방안 연구

이원혁
한국과학기술정보연구원
livezone@kisti.re.kr

A Study on Derivation of quantum key distribution system security requirements and countermeasures

Wonhyuk Lee
Korea Institute of Science & Technology Information

요 약

QKMS를 포함한 QKD 장비 및 양자통신암호화장비(QENC)에 대한 보안요구 사항은 확정되지 않았지만, 여러 표준화 문서를 고려하여 연구개발의 진행과 함께 연구되어야 한다. 본 연구에서는 보안 적합성 제도와 양자키 분배 시스템의 관계에 대해서 알아본 후, 표준문서에 제시된 QKD 보안 요구 사항을 분석하고, QKMS에 보안 요구 사항에 대해 도출 연구하고자 한다.

1. 서론

양자컴퓨팅 시대의 도래에 따라 RSA 등 수학적 난제를 기반으로 설계된 기존 암호 시스템을 대체하기 위한 다양한 연구가 시도되고 있다. 국가연구망인 KREONET은 양자키분배장비(QKD)를 도입하여 네트워크를 구축하여 국가 QKD 연구는 물론 QKD를 통한 서비스를 수행하기 위해 연구 개발을 추진 중에 있다. 아직 QKMS를 포함한 QKD 장비 및 양자통신암호화장비(QENC)에 대한 보안 요구 사항은 확정되지 않았지만, 여러 표준화 문서를 고려하여 연구개발의 진행과 함께 연구되어야 한다. 본 연구에서는 보안 적합성 제도와 양자키 분배 시스템의 관계에 대해서 알아본 후, 표준문서에 제시된 QKD 보안 요구 사항을 분석하고, QKMS에 보안 요구 사항에 대해 도출 연구하고자 한다.

2. 보안 적합성 제도와 양자키 분배 시스템

정보보호제품의 보안기능을 검증하고 국가 정보보호 수준을 제고하기 위해 정부는 정보보호제품의 객관적이고 공정한 평가 시스템을 필요로 한다. 한국은 국가정보화 기본법 및 전자정부법 등의 기준에 따라 정보보호 관련 제품 및 시스템을 평가·인증하는 제도들을 체계화하고 있다. 국가·공공기관 대상으로 안전성과 신뢰성이 검증된 정보보호제품 공급 및 이용 촉진을 위해 시행중인 제도들은 다음과 같다.

- 보안적합성 검증제도
- 정보보호제품 평가·인증제도(CC 평가·인증)
- 암호모듈 검증제도

양자 키 분배 시스템이 국가·공공기관에 도입되기 위해서는 이 제도를 통해 안전성을 검증받아야 한다. 현재 ISO/IEC WD1 23837인 “Security requirements, test and evaluation methods for quantum key distribution”이 현재 Under Development 단계이고 이것이 표준화 되어야 이를 바탕으로 Protection profile이 생성될 수 있고 이를 통해 국제 CC가 통과될 수 있다. 국내도 마찬가지로 국내 CC제도 또는 국가용 PP에서 양자 키 분배 시스템에 대한 보안요구사항이 정의되어야 한다.

양자 키 분배 시스템의 보안요구사항이 정의될 경우, 이는 기존 양자 키 분배 시스템과 관련된 국내외 표준과 무관할 수 없다. 현재 국내 표준으로 등록된 문서 중 양자 키 분배 시스템과 관련이 있는 표준은 다음 두 가지이다. 본 연구에서는 이 두 가지 표준에 대한 분석을 통하여, 향후 필요한 보안 요구사항을 분석하여 적용하고자 한다.

- 양자키 분배 보안 요구사항 (Security Requirements for Quantum Key Distribution(QKD))
- 양자키 분배 (QKD): QKD 모듈 보안 규격 (Quantum Key Distribution (QKD): QKD Module Security Specification)

3. 양자 키 분배 보안 요구사항

이 문서의 번호는 TTAK.KO-12.0356 이며 2019년 12월 11일에 제정되었다. 이 표준의 목적은 양자 키 분배(QKD) 메커니즘의 안전성을 보장하기 위한 요구사항을 제시하는 것이다. 주요 내용은 BB84 프로토콜과 디코이 기법을 사용하며 단방향 기법으로 구현한 QKD 메커니즘의 보안 요구사항들을 명세한다.

또한 QKD 경계가 암호경계 내에 포함되어 키 생성 및 공유 서비스를 제공하는 경우 QKD 경계 내의 보안 요구사항을 정의한다.

3.1 적용 범위

이 표준은 BB84 프로토콜(TTAK.KO-12.0329-PART2)과 디코이 기법을 단방향 기법으로 구현한 양자 키 분배(QKD) 메커니즘의 보안 요구사항을 명세한다. QKD 메커니즘은 다른 안전성 평가 표준의 범위에 포함할 수 없는 물리적 장치와 절차로 구현되므로 새로운 평가 기준의 필요성이 대두됨에 따라 개발되었다. 따라서 어떤 암호장비가 QKD 메커니즘을 포함하는 경우 그 장비의 QKD 메커니즘만을 한정하여 안전성을 제시한 것으로 QKD 메커니즘 외의 안전성 관련 기능의 검증은 다른 표준을 적용하여야 한다.

3.2 양자키관리장비 보안요구 사항

QKMS의 보안요구사항을 정의하기 전에 QKMS가 QKD, QENC와 어떻게 운용되는지 먼저 정의할 필요가 있다. 아래 그림은 2022년 6월 10일 개최된 IT 보안제품 보안적합성 검증정책 설명회에 소개된 양자암호통신 장비 개념도이다. 국정원에 따르면 양자암호통신 장비들이 통신망에 구축되면 '양자키분배장비-양자키관리장비-양자통신암호화장비' 순으로 작동한다. 양자키분배장비가 양자키를 분배하면, 후처리 과정을 거친 '비밀키'가 양자키관리장비에 전달되고, 양자키관리장비는 내부적으로 (키를) 가공해 '공급키'라는 명칭으로 양자통신 암호화 장비로 보낸다. 이어 양자통신 암호화 장비에서는 기존 암호 기술로 공유한 '설정키'와 '공유키'의 조합인 '조합키'를 활용한다. 이 조합키를 이용해 데이터를 암호화해 활용하는 암호화 통신용 비밀키(데이터 통신 암호화 키)로 활용할 수 있게 된다.

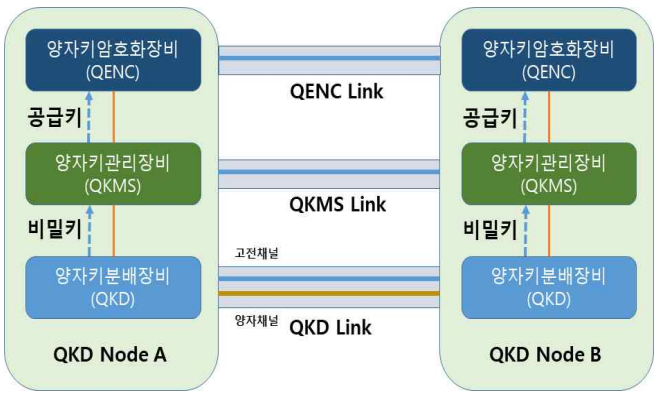

그림 1. 핵심 양자암호통신장비 개념도

상기 기능을 수행하기 위해 QKMS는 키 관리, 식별 및 인증, 보안관리, 전송데이터 보호, 저장데이터 보호, 자체시험, 감사기록, 접근통제 등의 기능이 필요할 것으로 예상된다. 다음 각 절에서는 해당 기능을 수행할 때의 보안요구사항에 대하여 정의하였으나, 본 논문에서는 지면상 상세 내용을 담지는 못하였다.

3.2.1 키관리

- 비밀키 수신/비밀키 가공 및 저장/가공키 동기화/공급키 송신

3.2.2 관리기능

- 관리자 인증 및 접속 / 관리자 암호 관리

3.2.3 암호기능

3.2.4 자체 시험

- 신뢰 부트 사용 및 자체 시험 바이너리/데이터 보호
- QKMS 소프트웨어 공급망 및 취약점 지속 점검

4. 결론 및 시사점

KREONET은 양자키분배장비(QKD)를 도입하여 네트워크를 구축하여 국가 QKD 연구는 물론 QKD를 통한 서비스를 수행하기 위해 연구 개발을 추진 중에 있다. QKD 장비는 거리의 제한 등으로 인해 신뢰된 노드에서 키를 전달하거나 양자통신암호화장비(QENC)에 QKD에서 교환한 비밀키를 전달해주는 계층인 양자키관리장비(QKMS)가 필요하다. QKMS에 가장 핵심적인 기능은 키관리 기능으로써 QKD에서 비밀키를 받아서 QENC에 공급키를 제공한다. 세부적으로 비밀키 수신, 비밀키 가공 및 저장, 가공키 동기화, 공급키 송신 등에서 공격이 발생할 수 있는 공격 표면을 고려하여 그에 대응하는 보안요구사항을 도출하였다. 두 번째 관리기능에서는 주로 관리자의 인증과 접속, 관리자 암호 관리에 대한 공격 표면과 대응을 위한 보안요구사항을 도출하였다. 셋째 암호기능에서는 일반 암호 관련 보안요구사항 보다는 실제적 문제가 되고 있는 검증필 암호모듈의 부적절 사용에 대한 방안을 제시하였다. 마지막으로 자체시험에서도 일반적인 내용은 제외하고 QKMS 자체의 신뢰성 문제와 공급망 보안/취약점 관리 문제를 다루고 이를 통해 보안요구사항을 도출하였다.

ACKNOWLEDGMENT

본 연구는 2023년도 한국과학기술정보연구원(KISTI) 주요사업 과제로 수행한 것 입니다.

참 고 문 헌

[1] 이원혁, 석우진, 손일권,"양자암호기반의 통신망 구축 및 성능시험 검증 연구", KNOM Review 22권 2호, pp39-47, 2019년10월

[2] 심동희, "양자키 분배 네트워크를 위한 보안 요구 사항과 난수 생성기 표준화 동향", Review of KIISC, 정보보호학회지, p.17-21, 2020

[3] 김용환, 심규석, 이원혁, "중장거리 양자 암호키 분배를 위한 키 관리 계층 기반 양자키 전달 구조 및 방안", 2021년도 한국통신학회 동계종합학술발표회, p74-75, 2021년 2월

[4] 심규석, 손일권, 김용환, 이은주, 배광일, 김현진, 이원혁, "국가과학기술연구망 기반 양자암호통신 구축을 위한 양자 키 관리 시스템 설계", 2021년도 한국통신학회 동계종합학술발표회, p70-71, 2021년 2월