양자 키 분배 광학 시스템 안전성 검증 동향

배광일, 이원혁*
*한국과학기술정보연구원
kibae@kisti.re.kr, *livezone@kisti.re.kr

Security test trends of QKD optical system

Kwangil Bae, Wonhyuk Lee*
*Korea Institute of Science and Technology Information

요 약

양자 키 분배 기술은 양자정보 분야 응용 기술 중 가장 기술성숙도가 높은 기술 중 하나이다. 현재까지 많은 양자 키 분배 프로토콜이 제안되어왔으며 다양한 수준의 도청 가정하에 프로토콜의 안전성을 증명하기 위한 연구도 활발히 이루어지고 있다. 양자 키 분배가 상용화 단계에까지 이른 기술인 바, 프로토콜의 이론적 안전성을 증명하는 것 외에 실제 구현 시 안전성을 검증하는 문제는 매우 중요하다고 할 수 있다. 본고를 통하여 QKD의 광학 장치를 중심으로 중요한 안전성 및 성능 점검 항목 제안 동향에 대하여 살펴본다.

Ⅰ. 서 론

양자 키 분배(QKD; Quantum Key Distribution) 프로토콜에서 통신자는 양자 기술을 활용하여 암호키를 나누어 갖는다. 이때 암호키 분배의 안전성은 정보이론적으로 보장됨이 증명된 바 있다. RSA 암호체계와 같이 그 안전성이 계산 복잡도에 기반하는 기존 암호시스템은 높은 계산능력을 가진 연산장치가 개발될 경우 보안위협이 생길 가능성이 있으나, 양자 키 분배는 이 같은 문제에서 자유롭다.

양자 키 분배 프로토콜의 안전성에 대한 논의는 꾸준히 발전해왔다. 2000년대 초반 D. Mayers와 P. Shor 등에 의해 초기 QKD 안전성 증명이 제안된 이후, 2005년 R. Renner는 좀더 세분화된 방식의 안전성 증명을 제안하였다. [1, 2] 이 같은 안전성 증명은 도청자 존재 하에 통신자가 얻을 수 있는 암호키 정보량을 엔트로피로 표현하여 그 하한값을 유도하는 방식으로 보일 수 있다. 이같은 안전성 증명에서 정보량의 하한값은 I. Devetak과 A. Winter에 의해 계산되었다. [3] 상기의 엔트로피를 활용한 방식 외에도 다양한 방식의 안전성 증명 방식이 존재한다. 특기할만한 결과 중 하나는 이른바 Gottesman-Lo-Lutkenhaus-Preskill (GLLP) 안전성 증명으로, 해당 증명에서는 이상적 장치가 아닌 WCP(Weack Coherent Pulse) 광원 등 실제적인 장치를 고려하여 안전성 증명 결과를 유도하였다. [4]

상기 안전성 증명은 QBER(Quantum Bit Error Rate) 등 안전성 증명 수식에서 고려하고 있는 다양한 측정변수를 측정하여 확인될 수 있다. 그러나 이 같은 이론적 안전성 증명 만족 여부를 확인하는 것 외에도, QKD 실제 구현 시 구성하는 광학 장치가 적절히 구현되었는지, 예상되는 양자 해킹에 대한 대응이 가능한지 확인하는 것은 시스템 안전성 증명에서 중요한 이슈라고 할 수 있다. [5] 2010년대 후반에는 QKD 구현과 그 구현의 안전성을 검증할 수 있는 방법을 표준화하여 정리하는 노력이 지속되고 있다. 이와 관련하여 QKD에 관한 유럽전기통신표준협회(ETSI)에서는 QKD 구성장치와 적절한 구현 방법 및 그 기준을 상세히 정리한 그룹 보고서를 발간한 바 있다. [5, 6] 최근 국내에서는 국정원 주도로 QKD를 위한 보안요구사항을 정리한 보고서가 발간된 바 있으며, 이러한 기조에 맞추어 국가보안기술연구소(NSR)도 QKD 안전성 검증 항목을 정리한 결과를 발표하였다. [7, 8]

본고에서는 QKD 시스템을 광원단, 측정단, 광학계로 구분하여, 최근 국내외 제안되고 있는 QKD 장비 검증 항목 제안 동향을 살펴보고 관련 시사점을 논하도록 한다.

Ⅱ. 본론

최근 국내외에서 제안되고 있는 QKD 광학계 안전성 및 성능 검증 항목을 살펴보도록 한다. 국가보안기술연구소에서 2022년 9월 발표한 QKD 광학파트 시험 항목은 총 11개로 항목으로 구성되어 있다. 시험 항목의 적용을 고려하고 있는 QKD 프로토콜은 decoy 상태 생성 방법론을 적용한 one-way, two-way BB84 프로토콜이다. 상기 항목을 광원단, 측정단, 전체 광학계에 대한 항목으로 구분하면 다음과 같다.

1) 광원단 검증 항목

양자 상태 생성 성능과 관련하여 확인이 필요한 항목으로는 평균 광자 수, 광자 수 분포, phase randomization, 펄스 구별불가능성(indistinguishibility)가 있다. 이때 광자 수 분포는 시간 지연이 0일 때의 이차 상관관계 함수($g^{(2)}(0)$) 측정을 통하여 검증된다. 상관관계 함수는 광원의 광자 수 통계에 대한 정보를 알려주며, 완벽한 단일 광자 광원의 경우 $g^{(2)}(0)=0$이며, 완벽한 결맞음 광원의 경우 $g^{(2)}(0)=1$이다. 실제 구현 시 $g^{(2)}(0)<1/2$인 경우, 좋은 단일광자광원이라 할 수 있다. 특기할 점은 펄스의 구별 불가능성을 signal/decoy 상태 간 구별 불가능성과 양자 상태 간 구별 불가능성으로 구별하여 검증항목을 구성하였다는 점이다. 상기 검증 항목 측정을 통한 양자 특성 측정 시 만족할 만한 값을 얻지 못하면 QKD 시스템 안전성을 보장하지 못할 수 있다. 예컨대, decoy 상태 생성 방법론에서는 안전성 증명에서 도청자가 광자 수 측정을 통해 signal/decoy 신호를 구별하지 못해야 한다는 사실을 활용한다. 따라서 signal/decoy 신호의 신호 세기 외 다른 물리적 특성이 동일함을 증명하는 것이 안전성 증명에 필수적임을 알 수 있다.

2) 측정단 검증 항목

양자 상태 측정단 성능 검증 항목으로는 단일광자 검출기 효율, dark count rate, after pulse 확률이 있다. InGaAs 단일광자 검출기의 경우 검출확률은 최대 50% 수준으로 알려져 있다. Dark count는 광자 캐리어가 도달하지 않았을 때, 열 효과 등에 의해서 SPAD에 원하지 않는 측정신호가 발생하는 현상을 말하며, after-pulse는 펄스로 인한 신호 생성 전에 다음의 gate 펄스가 입력되어 새로운 avalanche current가 발생하는 잡음 현상을 말한다. Dark count rate이나 afterpulsing 잡음이 높은 상황에서는 QKD가 높은 효율로 작동할 수 없다.

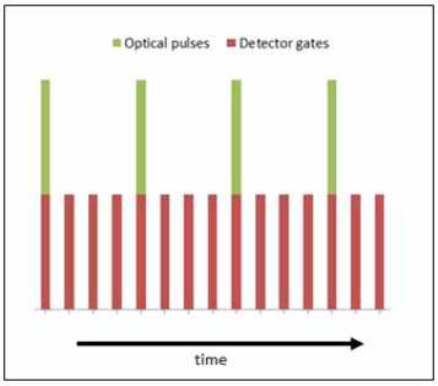

그림 1. 매 R번째 Gate에 대하여 광학 신호가 인가하는 방식의 측정방법. 위 그래프의 경우 R=4.

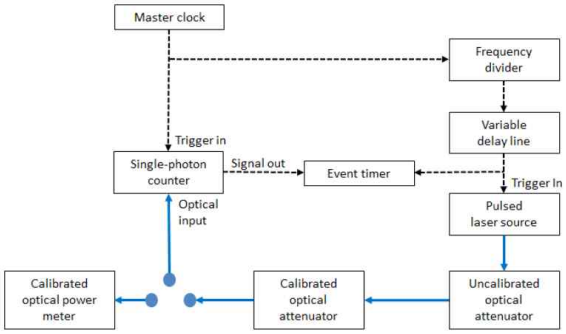

그림 2. 측정방법 3, 4 구현을 위한 측정 셋업

2016년 발간된 ETSI GS QKD 보고서에는 QKD 광학장치와 관련 측정 항목과 측정방법이 국내 발표 항목보다 상세히 정리되어 있다. [5] 해당 보고서 상에는 광원단, 측정단에 대한 측정항목을 각각 10개, 12개로 세분화하여 정리하였으며, 일반적으로 각 측정마다 측정방법이 다수 제안하고 있다. 예컨대 측정단 검증 항목 측정 방법으로는 4가지 방법과 그것의 변형 측정 방법을 제안하고 있으며, 내용은 다음과 같다.

측정 방법 1 : 빛이 조사되지 않은 측정기의 알려진 수의 게이트에 대하여 측정수 계산

측정 방법 2 : 측정기의 측정 간 시간 간격 계산

측정 방법 3 : 측정기의 매 R번째 게이트에 빛을 조사한 후 빛이 조사된 게이트에 대해서 'click'을 측정한다. 또한 빛이 조사된 게이트에 대한 'click'과 연속되는 빛이 조사되지 않은 게이트의 첫 'click' 사이의 시간간격에 대하여 측정한다.

측정방법 4 : 측정기의 매 R번째 게이트에 빛을 조사한 후 event timer를 활용하여 매 'click'을 기록한다.

상기 측정방법 중 측정방법 3, 4는 상대적으로 더 엄밀한 검증을 제공하며 그림 1, 2와 같은 측정방법과 측정 셋업을 활용한다.

3) 광학계 검증항목

광학계 검증 항목으로는 Bob 광학계의 투광율, 양자신호 광오류율, 광학계 허용 파장 특성이 있다. Bob 광학계의 투과율 측정은 Bob 광학계의 입사 신호세기와 투과후 신호세기를 비교하여 측정되며, 편광에 따른 투과율 변화도 측정해야 한다. 광 오류율은 양자 채널이 없을 때 encoding/decoding 신호 비교를 통해 오류 확률을 측정하게 된다. 마지막으로 광학계 허용 파장 특성은 파장 레이저를 사용하여 광학계에 대한 입출력 레이저 세기를 측정하여 유도한다.

Ⅲ. 결론

본고에서는 최근 국내 발표된 QKD 광학부 안전성 검증 항목을 각 부분별로 분류하여 정리하고, ETSI과 비교하여 살펴보았다. 결과적으로 ETSI 보고서 상에 QKD 내 광학 장치에 대한 검증 항목 및 방법이 더 상세히 정리되어 있는 것을 확인하였으며, 측정단 검증 항목을 예시로 이를 비교하였다. 특기할만한 점은 국내외 검증 항목은 one-way, two-way BB84 프로토콜 등 기초적인 QKD 프로토콜을 전제로 작성되었다는 점이다. 이는 최근 연구개발 중인 CV-QKD, MDI-QKD, DI-QKD, TF-QKD 등의 차세대 QKD 프로토콜에 대한 연구성과의 축적과 안전성 검증 항목의 표준화를 유도하기 위한 노력이 필요함을 시사한다.

ACKNOWLEDGMENT

본 연구는 2023년도 한국과학기술정보연구원(KISTI) 주요 사업 과제로 수행한 것입니다.

참 고 문 헌

[1] Mayers, Dominic "Unconditional security in quantum cryptography," J. ACM 48 (3), pp. 351-406, 2001

[2] Shor, Peter W, and Preskill, J. "Simple proof of security of the BB84 quantum key distribution protocol," Phys. Rev. Lett. 85, pp. 441-444, 2000

[3] Devetak, I., and Winter, A. "Distillation of secret key and entanglement from quantum states," Proc. R. Soc. London, Ser. A 461 (2053), pp. 207-235, 2005.

[4] Gottesman, D., Lo, H.-K., Lutkenhaus, N. and Preskill, J. Quantum Inf. Comput. 4, 325, 2004

[5] ETSI, "ETSI GS QKD 011 V1.1.1: Quantum Key Distribution (QKD); Component characterization: characterizing optical components for QKD systems", 2016.

[6] ETSI, "ETSI GR QKD 003 V2.1.1: Quantum Key Distribution (QKD); Quantum Key Distribution (QKD); Components and Internal Interfaces", 2018.

[7] NIA, "정보보호시스템 및 네트워크 장비 국가용 보안요구사항; 3편 제품 보안요구사항, 양자암호통신장비 제품군", 2022.

[8] NSR, "QKD 안전성(광학파트) 시험 항목 및 검증 수치", 2022.