양자 통신 시스템의 효율적 후처리 방식

이선의*, 정국현*, 김진영*

Efficient Post-Processing for Quantum Communication Systems

Sun Yui Lee*, Kuk Hyun Jung*, and Jin Young Kim*

요 약

양자 역학을 이용한 양자 암호 분야는 가장 구현가능성이 높은 분야중 하나이다. 그로인해 양자 암호는 꾸준히 연구되어 왔고 QKD 시스템의 대표적인 BB84 프로토콜 등 다양한 통신 방식이 개발되어 왔다. 본 논문에서는 양자 통신의 기본적인 개념을 설명하고 이를 이용한 양자 암호 교환 방식인 QKD 시스템을 설명한다. 또한 양자 암호의 개발이 필요한 이유와 보안성을 위협하는 QKD 공격방식을 소개한다. 양자 채널을 모델링하고 qubit의 위상을 추정하여 양자 암호 공격을 시뮬레이션 한다. 다양한 공격 방식이 QKD시스템에 보안성을 위협하는 원리를 설명하고 이를 극복하기 위한 양자 후처리 방식의 필요성을 논하고자 한다.

Key Words : Entanglement, No-cloning theorem, qubit, SPIR(Symmetrically privae information retrieval), QKD(Quantum Key Distribution), PNS(Photon number splitting), SSPDs(Superconducting Singlephoton Detectors), SPD(Single Photon Detector)

ABSTRACT

Quantum cryptography is one of the most feasible fields using quantum mechanics. Therefore, quantum cryptography has consistently been researched, and a variety of cryptographic exchange method has been developed, such as BB84, etc. This paper explains a basic concept of quantum communications and quantum key distribution systems using quantum mechanics. Also, it introduces a reason of the development of quantum cryptography and attack scenarios which threaten the security of QKD. Finally, the experiment of this paper simulates quantum key attack by estimating qubit phases through a modeled quantum channel, and discusses needs of post-processing methods for overcoming eavesdropping.

I. 서 론

고전양자 역학을 정리한 학자들의 이론들이 현대에 와서 양자 세계를 들여다볼 수 있는 기술들이 속속 나오게 되면서 연구가 활발히 진행 되고 있다. 양자 상태를 정의하고 그 상태를 고정 시켜서 양자를 이용한 메모리 기술부터 해킹이 불가능한 보안 솔루션이 될 수 있다 [1].

양자의 특성을 이용하여 정보를 전송하는 기술은 양자의 비연속성, 양자 상태의 중첩, 불확정성의 원리, 양자상태의 얽힘(entanglement) 및 복제 불가(No-cloning theorem) 등이 있다[2].

현재의 통신 방식은 정보를 0 과 1로 표현한 디지털 신호를 통하여 데이터를 표현하고 이진신호를 전자파 신호로 안테나를 통해 채널을 통과하여 전송된다. 양자를 이용한 정보전송은 양자 상태를 불연속인 전자의 준위를 통하여 0과 1로 표현한다. 이를 양자 계산에서 큐비트(qubit)라 하고 양자 상태의 중첩의 원리를 이용하여 고전 컴퓨터에서 할 수 없는 병렬연산을 동시에 수행하여 현재 공개 키 방식의 보안 솔루션을 연산의 속도를 통하여 암호를 알아내는 것이 가능하다 [3].

불확정성의 원리는 양자를 관찰하게 되면 관측한 것으로 인해서 양자의 상태가 변화하는 것을 말한다[4].

1994년에 Peter shor가 제시한 양자 정보 처리의 우수성은 이론적으로 우수하지만 구현이 불가능할 것으로 예상되었다. 하지만 다음 년도에 최초의 양자 오류 정정 부호를 발표함으로써 많은 발전이 이루어지게 되었고 양자 정보 처리 기술의 발전에 따라 양자 오류 정정 부호를 통하여 물리적으로 구현된 양자 통신 시스템에 신뢰성을 높이기 위한 연구가 활발히 진행되고 있다 [5].

본 연구는 광운대학교 2014년 교내연구비 지원에 의한 연구 결과임.
*광운대학교 전파공학과 소속 유비쿼터스 통신 연구실(sunyuil22@naver.com), (rnzpdl@nate.com), (jinyoung@kw.ac.kr)
접수일자 : 2014년 10월 1일, 수정완료일자 : 2014년 10월 22일, 최종게재확정일자 : 2014년 10월 30일

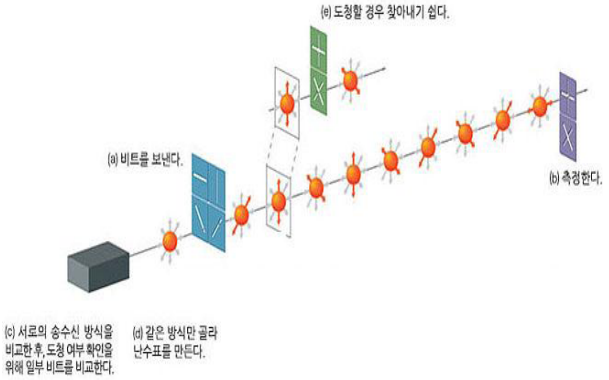

그림 1. BB84 프로토콜의 정보 교환 방식.

현재 양자의 상태를 알기 위해서는 양자를 아무 변화없이 관측할 수 는 없고 특정한 측정 슬릿을 통과 시켜야만 알 수 있기 때문에 이렇게 이해하기 쉽다. 하지만 불확정성의 원리는 측정의 부적합성에 있는 것이 아니고 관측을 하게 되는 상태가 결국 양자의 상태가 되기 때문에 중간에 누군가 관측을 하게 되면 다음에 관측하는 양자의 상태가 바뀐다는 것이다. 그림 1은 QKD시스템의 대표적인 예인 BB84 프로토콜의 정보 교환 방식을 설명한다.

양자 역학을 이용한 통신 방식이 최근에 구현이 활발히 진행되면서 많은 양자 비트를 처리하기 위한 방식들이 제안되어 지고 있다. 양자 역학을 이용한 양자 통신의 완전한 보안성은 국가의 중요한 정보 교환 방식을 보장하고 양자 컴퓨터는 기존의 암호 방식을 쉽게 해킹할 수 있어 기술 독점을 막기 위해 각국에서 활발히 개발하고 있다. 양자 통신은 양자 키 분배QKD(Quantum Key Distribution)라는 보안 프로토콜을 말하며 양자 정보이론을 통한 다양한 통신 방식이 개발되어 왔다.

양자 키 분배 QKD(Quantum Key Distribution)은 양자 물리법칙을 이용한 두 통신자간의 완전한 보안성을 제공하는 통신 방식이다. 하지만 양자 법칙을 이용한 양자 프로토콜이 보안성을 보장하더라도 양자 비트를 다루는 장치는 불완전하기 때문에 다양한 양자 암호 공격모델이 존재한다.

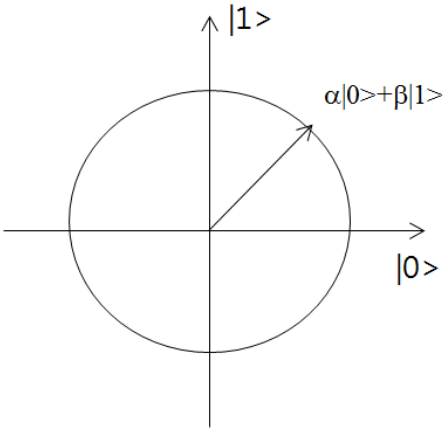

그림 2. Qubit의 벡터화.

암호 통신에서는 도청자가 전송된 메시지를 읽는 것을 차단하는 것뿐 아니라 메시지를 보내는 수신자의 프라이버시를 보호하는 것이 필수적이다. 예를 들어 상품을 판매하는 데이터베이스에서 누군가 가치 있는 데이터를 검색하고 구매하고 싶다면 데이터베이스의 주인이 내 구매 정보를 수집하고 있지 않을까 우려할 수가 있다 [6]. SPIR(Symmetrically privae information retrieval) protocol은 이러한 상황을 위해서 설계된 프로토콜이다 [7]. 검색자가 데이터베이스에서 정보를 구매와 동시에 주인은 데이터베이스에서 검색한 기록과 구매 기록을 모두 잃게 되어 서로의 프라이버시를 지키는 시스템이다. 또한 DPS-QKD는 수신자가 각각의 펄스를 랜덤하게 (0,π)의 위상 변조하여 상당히 감쇠된 동기 펄스 트레인을 전송한다. 전송되는 신호의 파워는 너무 작아서 평균적인 펄스분의 포톤의비가 하나보다 작게 된다. 그리고 포톤은 위상차에 따라서 간섭을 일이키는 인접 펄스에 따라 검출된다. 본 논문에서는 다양한 양자 암호 장치를 공격하는 암호 도청 시나리오와 대응 기술들을 소개하고 후처리의 필요성을 시뮬레이션을 통하여 설명한다.

Ⅱ. 양자 정보 시스템

qubit는 기존의 비트와 유사한 성질을 갖고 있고 기존의 정보 이론을 활용한 다양한 기술들을 적용하기 위한 시도를 하고 있다. 대표적으로 양자 전송, 양자 소인수 분해, 양자 암호 키 등 양자 역학을 이용한 기술들이 있다 [8]. 이 큐비트는 양자의 상태를 통하여 비트를 표현한 것이기 때문에 어떤 양자 상태를 이용할지는 많은 연구가 이루어지고 있다. 연구 초기부터 지금까지 활발하게 연구되는 양자는 광자를 이용한 편광 현상으로 베이시스를 서로 나누어 암호를 교환하는 방식이 있고 초전도체를 이용하여 양자 상태를 오래 유지시켜 양자 메모리를 구현하려는 연구가 있다 [9].

$$\alpha|0\rangle+\beta|1\rangle \xrightarrow{\ X\ } \alpha|1\rangle+\beta|0\rangle$$

$$\alpha|0\rangle+\beta|1\rangle \xrightarrow{\ Y\ } i\cdot(\alpha|1\rangle-\beta|0\rangle)$$

$$\alpha|0\rangle+\beta|1\rangle \xrightarrow{\ Z\ } \alpha|0\rangle-\beta|1\rangle$$

$$\alpha|0\rangle+\beta|1\rangle \xrightarrow{\ H\ } \alpha\frac{|0\rangle+|1\rangle}{\sqrt{2}}+\beta\frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

그림 3. 기본적인 quantum gate.

양자를 이용한 정보 교환 방식은 양자 역학의 기본적인 성질을 이용하기 때문에 높은 보안성을 보장하지만 실제 양

자 정보를 유지하고 처리하는데 문제가 많다. 또한 구현하기 위한 양자 검출기, 양자 생성기 등 현실적인 구현 디바이스는 도청의 위협으로부터 자유로울 수가 없다. 따라서 양자를 이용한 정보를 송수신하기 위한 후처리 방식이 필요하다. 현재의 통신 방식에 사용되는 정보이론에 기반을 둔 오류 정정 부호는 양자 정보이론에 그대로 적용할 수 없기 때문에 양자 고유의 오류를 정정하고 도청을 예방할 수 있는 후처리 방식이 연구되고 있다. 이번 장에서는 양자 정보 통시 시스템에서 사용되는 몇 가지 기본 개념들에 대해서 설명한다.

"Bit"는 기존 통신 시스템에서의 전송 및 정보 저장의 기본이 되는 단위이다. 하지만, 양자 정보 통신 시스템에서의 기본이 되는 단위는 더 이상 "bit"가 아니라 ""quantum bit (Qubit)" 이 라는 새로운 개념의 단위를 사용한다. 하나의 qubit은 '0'과 '1' 두 가지 상태를 표현 할 수 있으며, 각 각 |0>과 |1> 로 표현된다. 하지만, 기존의 bit 단위와는 다르게 qubit은, 그림 2에서와 같이 |0>과 |1> 두 상태를 동시에 표현 가능하며, 다음과 같이 나타낼 수 있다.

$$|\psi> = \alpha|0> + \beta|1>, \quad (1)$$

여기서, α, β는 복소수 이다. 식 (1)에서와 같이, 하나의 qubit으로 두 개의 상태를 표현할 수 있는 중첩이 가능하며, 두 개의 상태 중에서 하나의 상태를 선택하는 것은 α, β에 의해 확률적으로 결정된다. 다시 말해, 상태 |0>으로 결정될 확률은 $\| \alpha^2 \|$ 이며, 반대로 |1> 로 결정될 확률은 $\| \beta^2 \|$ 이다. 또한, 확률의 기본 법칙을 만족하기 위해선 각 확률의 합은 1이 되어야 하며, 따라서 다음과 같은 수식을 얻을 수 있다.

$$\| \alpha^2 \| + \| \beta^2 \| = 1, \quad (2)$$

그림 3은 주요한 4개의 quantum gate를 보여준다. 기존의 NOT gate 와 유사하게, quantum X gate 는 단일 qubit의 상태를 천이시킨다. 따라서, 그림 3에서와 같이, $\alpha|0> + \beta|1>$이 quantum X gate를 통과하게 되면, $\alpha|1> + \beta|0>$의 출력값을 갖는다. 다음으로 quantum Z gate는 상태 |1>의 위상을 천이시킨다. 즉, quantum Z gate는 $\alpha|0> + \beta|1>$의 단일 qubit을 $\alpha|0> - \beta|1>$으로 천이시킨다. 그림 3의 quantum Y gate는 quantum X gate와 Z gate의 혼합형으로, 각 단일 qubit의 상태를 천이시킴과 동시에, 상태 |1>의 위상을 천이시킨다. 마지막으로 quantum H gate는 가장 많이 쓰이고, 유용한 gate 중에 하나이다. Quantum H gate는 |0>을 $\frac{|0> + |1>}{\sqrt{2}}$로, |1>을 $\frac{|0> - |1>}{\sqrt{2}}$로 천이시킨다.

Ⅲ. 양자 암호 공격 시나리오

1. 빔 분할 공격

QKD에 대한 일반적이고 간단한 도청 방식이 간섭 빛을 이용하는 빔 분할 공격이다. 도청자는 트랜스미션 라인을 무손실로 교체하고 분할 후에 전송자의 신호를 원래 트랜스미션 라인의 손실만큼 저장한다. 그리고 수신자의 측정 시간이 종료된 후에 분산된 신호를 측정하는 방식이다. 이 공격 시나리오는 수신자가 받는 신호에 영향을 주지 않고 전혀 도청을 인식하지 못한다. 그러나 DPS 신호에서는 신호에 사용되는 포톤의 숫자가 작기 때문에 도청을 통한 정보의 양이 제한된다. 신호를 측정하는 분할과 저장과정에서 도청자는 두 인접한 펄스의 위상 차이를 수신자가 포톤을 식별하고 키 비트를 생성하는 것을 통해서 알아내려고 시도한다. 여기서 대응하는 펄스는 평균적으로 $2r\mu$ 포톤을 포함한다. μ는 송신자가 보낸 펄스분의 포톤의 숫자이고 r은 원래 트랜스미션 감쇄와 동일한 빔 분할 비율이다. 그러므로 도청자로부터 빔 분할 공격을 통한 정보 유출 rate는 $2r\mu$이고 이것은 평균 포톤 개수 μ 보다 작고 개인 증폭에 의한 키 비트를 통해서 제외될 수 있다.

2. 차단 재전송 공격

다른 방식의 도청인 차단 재전송 공격은 도청자가 송신자의 모든 펄스 신호를 측정하여 자신이 만든 복제 신호를 다시 수신자에게 보내는 방식이다. 그러나 도청자는 적은 포톤의 숫자 때문에 모든 펄스의 위상 차이를 측정할 수 없고 수신자에게 모든 복제 신호를 전송할 수 없다. 결과적으로 완벽하지 않은 복제 신호는 에러를 발생시키고 도청유무를 수신자가 알 수 있다. 도청자는 수신자와 동일한 장치를 사용하여 송신자의 신호를 측정한다. 송신자는 때로 광자를 검출하고 해당 펄스의 위상차를 알고 있다. 이때 송신자는 측정되지 않은 시간 슬롯에서 진공을 전송하는 동안 중첩된 포톤에 두 펄스의 측정된 위상차를 재전송한다. 그 후에 두 개의 분리된 펄스는 수신자에게 도달하고 수신자는 포톤을 가능한 3가지 시간의 포톤으로 검출한다. 첫 번째 슬롯은 펄스가 최단 거리를 통하여 검출기에 도달하였을 때, 다음 슬롯은 긴 거리를 통하여 최초의 펄스가 검출기에 도달하였을 때와 최단 거리를 통하여 두 번째 펄스가 검출기에 도달하였을 때, 세 번째 슬롯은 두 번째 펄스가 긴 거리를 통하여 검출기에 도달하였을 때이다. 포톤이 두 번째 타임 슬롯에 포톤이 검출 될 때, 두 개의 펄스는 서로 간섭을 일으키고 수신자에게 올바른 비트 정보를 제공한다. 수신자는 이 시나리오에서 도청자를 인식하지 못한다. 다른 상황에서는 첫 번째와 세 번째 타임 슬롯에서 상호 간섭이 일어나지 않고 포톤은 랜덤하게 검출기를 통과하게 된다. 이 검출 상황은 수신자의 데이터 에러가 발생하게 되고 도청자의 유무를 밝혀 낼 수 있

다. 첫 번째 또는 세 번째 타임 슬롯에서 광자의 검출 확률은 1/2이고 도청자에 의한 비트 에러 확률은 1/4이다.

3. 순차적 공격

순차적 공격은 인터셉트-재전송 공격의 종류이다. 순차적 공격의 예로 이전의 차단 재전송 공격에서 비트에러가 처음과 세 번째 타임 슬롯에서 포톤이 검출될 때 발생하였다. 즉 가장자리의 슬롯에서 간섭이 발생하지 않는다. 비트에러를 감소시키기 위하여 도청자는 연속적인 검출을 기다리고 두 개의 분리된 펄스를 위조된 신호로써 측정된 위상차의 펄스 시퀀스를 재전송한다. 이 위조된 신호는 가장자리 타음 슬롯에서의 광자 검출 확률이 차단 재전송 공격의 확률보다 작다.

게다가 도청자는 가장자리 펄스의 진폭이 중앙 펄스보다 작도록 펄스 시퀀스의 진폭을 변조한다. 가장자리 슬롯에서의 포톤 검출 확률이 재전송 전략으로 감소된다. 이어서 가장자리 슬롯에서 간섭 없는 검출로부터 발생된 수신자의 비트에러는 간단한 인터셉트-재전송 도청보다 작아진다.

4. 광자 번호 분할 공격

PNS(Photon number splitting) 공격은 많이 알려진 BB84 프로토콜에 가장 위협적인 약한 간섭광을 이용한 도청방식이다. 이 도청 방식을 방지하기 위하여 복잡한 키 생성 프로세스를 만드는 디코이 방식이 실제 BB84 시스템에 적용되고 있다.

이와 대조적으로, DPS프로토콜은 PNS 공격방식에 상당히 강하다. PNS 공격에서는 도청자는 송신신호에 포함된 광자 수를 탐지하고 두 개 이상의 광자를 포함하는 별도의 광자를 픽업과 측정한다. 이는 광자를 발생하는 장치가 단일 광자를 생성하기 어렵기 때문에 발생하는 문제이다. 광자를 전송할 때 의도하지 않은 많은 광자가 채널을 통과하는 중에 인터셉트되어 수신자가 모르게 정보가 유출될 수가 있다. 하지만 도청자에게는 불행히도 DPS신호의 위상 정보는 광자의 수가 탐지될 때 붕괴하고 수신자는 비트 에러가 발생을 감지하고 도청자의 존재를 알게 된다.

5. 일반적 개별 공격

일반적 개별 공격은 각 키 비트를 공격하는 개념의 도청 방식이다. 여기서 개별의 의미는 펄스 트레인의 각 단일 광자를 의미하는 것이 아니다. 도청자는 송신자의 펄스 시퀀스에 중첩시킨 하나의 포톤을 얻고, 송신자의 프로브 상태의 단일 상호작용을 만든다. 그리고 수신자의 포톤 측정 시간이 공개된 후 검침기의 상태를 측정한다.

이 도청 방식의 보안 키 생성 rate R은 다음과 같이 주어진다.

$$R = -p_{click}[-(1-2\mu)\log_2 P_{c0}(e) + f(e)h(e)], \quad (3)$$

여기서 p_{click}은 수신자의 포톤 검출 확률, μ은 펄스분에 평균 포톤의 수, e은 시스템의 error rate, $h(e) = -elog_2 e-(1-e)\log_2(1-e)$, $f(e)$는 Shannon limit redundancy factor, $P_{c0}(e) = 1-e^2-(1-6e)^2/2$ 이다. 현재까지 많은 DPS-QKD 실험이 위 방정식을 이용하여 성능을 평가한다.

6. 사이드 채널 공격

최근에 가장 QKD에서 이슈가 되고 있는 것이 사이드 채널 공격 방식이다. 사이드 채널 공격은 실제 QKD 구현에 사용되는 실제 소자들의 현실적인 결함을 활용하여 공격을 하는 방식이다. 또한 이 공격 방식은 초전도체를 사용하는 싱글 포톤 검출기 SSPDs(Superconducting Singlephoton Detectors) 로 구현된 DPS-QKD 시스템에 대하여 제안되었다. SSPD의 동작 특성을 활용하여 도청자는 밝은 빛을 주입하여 임의로 SSPD의 클릭을 조작한다. 도청자는 밝은 빛을 조작 신호로 인터셉트-재전송 공격을 통해서 완벽한 키 비트 정보를 얻을 수 있다.

7. 정교한 공격

일괄적 공격 또는 동기화 공격은 QKD시스템의 대한 가장 정교한 도청 방식이다. 도청자는 프로브 상태를 준비하고 송신자의 전체 신호상태와 상호 작용하게 한다. 그다음 수신자와 송신의 확인을 위한 상태 정보 교환 후에 프로브의 상태를 측정한다. DPS-QKD에 대한 도청 방식의 일반적인 분석은 송신자의 펄스의 지속이 길기 때문에 어렵다. 또한 수신자의 포톤 검출 후에 프로세싱을 통하여 하나의 시퀀스의 시간 위치를 임의로 선택할 수 있어 도청이 어렵다.

8. 검출 효율 불일치

단일 양자 검출기 SPD(Single Photon Detectior)에 발생하는 검출 효율의 불일치를 공격하는 도청 방식이다. 게이트 모드에서 동작하는 각각의 SPD는 자신의 시간 또는 파장에 의존 효율 곡선을 가지고 있다. 이것은 장치에 비대칭 또는 시간의 불일치에 의해서 발생한다. 도청자는 큐비트 간의 게이트 윈도우의 시간 인터벌을 조작하여 게이트 창에 대해 큐비트의 도달시간을 공격하여 효율 곡선의 불일치를 탐색할 수 있다. 또 다른 예로 타임 시프트 공격을 들 수 있다. 이는 도청자에 의한 인터셉트는 없지만 큐비트의 도달시간을 지연시켜 공격을 수행한다. 포톤이 도달하는 경로를 조작함으로써 도청자는 QBER의 증가 없이 보안키를 유출할 수 있도록 하지만 펄스의 위치를 게이트 윈도우에 위치시킬 수 있어 또 다른 검출기의 검출확률을 증가 시킬 수가 있다. 이 도청

방식의 단점은 도청자가 발생시키는 수신자의 검출 장치 효율의 감소 때문이다. 하지만 이는 도청자가 더 은밀하고 수신자의 수신부 도입부분에서 송신자의 상태를 이동시키거나 교체시킬 수 있다는 점을 가정해야한다.

Ⅳ. 양자 채널 실험

양자 통신을 실험하기 위하여 qubit이 에러를 발생하는 것을 3가지 모델로 가정하고 채널 모델을 시뮬레이션 하였다. 그림 4는 bit flip과 phase flip의 에러가 각각 생기는 경우와 동시에 발생하는 경우를 나타낸 그림이다. 양자를 이용한 통신 시스템을 구성하기 위해서는 양자의 상태를 추정하는 것이 무엇보다 중요하다. 3장에서 설명한 바와 같이 양자 통신의 공격 모델에서 양자 상태의 정확한 측정을 방해하는 공격 모델이 많은 것이 이 때문이다. 따라서 qubit의 phase estimation은 하나의 모듈처럼 동작하기 때문에 게이트를 통과한 qubit을 시뮬레이션을 통하여 측정한다.

실험은 qubit가 random state와 eigenstate인 두 가지 경우에 따라 qubit의 phase를 estimate한다. 그림 5,6은 5개의 qubit를 이용하여 유니터리 operator의 eigenstate phase를 추정한 확률 분포를 eigenstate와 randomstate에 따라서 나타낸다. 그림 5를 보면 eigenstate를 사용한 것은 측정 확률 분포가 고유한 eigenvector이기 때문에 처음 정한 위상에서 1에 가깝게 나온 것을 알 수 있고, 그림 6은 랜덤한 randomstate는 각각의 측정 확률 분포가 일정하지 않고 랜덤한 것을 알 수 있다.

실험을 통하여 가정한 양자 채널 모델은 송신자와 수신자는 qubit의 phase estimation은 굉장히 공격하기 쉽다는 것을 알 수 있다. 송신자는 고유한 단일 펄스를 이용하여 단일 광자를 보내겠지만 도청자는 이 펄스를 가로채 측정하거나 더 많은 광자 펄스를 주입하여 수신자의 phase estimation을 방해하여 도청 유무를 감추거나 이를 통하여 암호키를 추정할 수 있는 단서를 얻을 수 있다. 따라서 암호키가 유출될 수 있는 qubit의 detection을 보호할 있는 양자 후처리 알고리즘이 필요함을 알 수 있다.

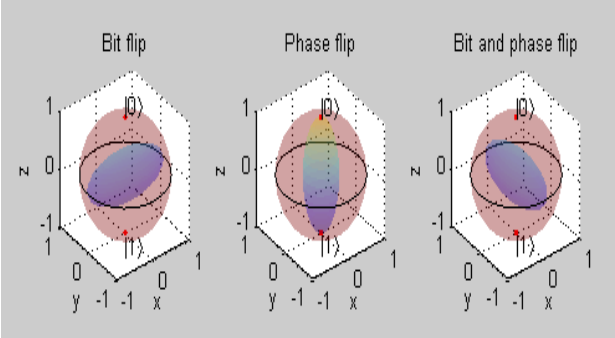

그림 4. Qubit의 채널 모델.

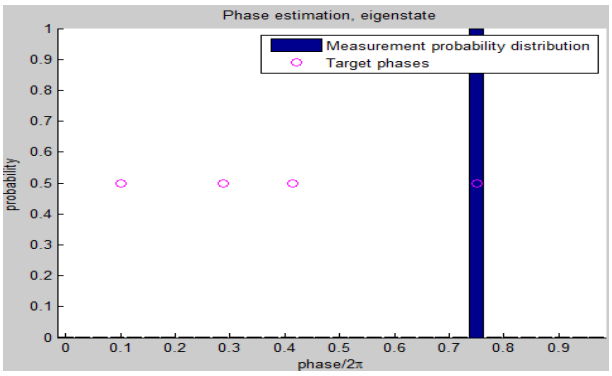

그림 5. Eigenstate phase estimation.

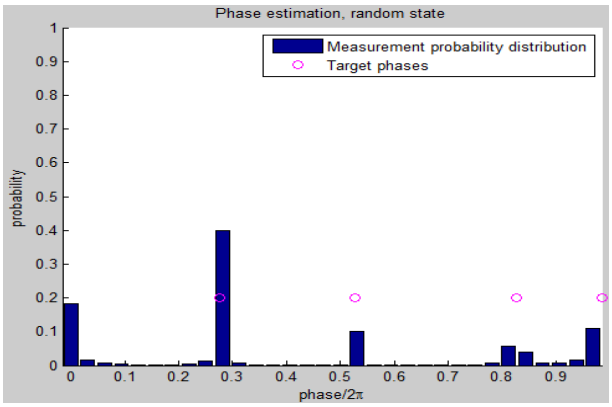

그림 6. Randomstate phase estimation.

Ⅴ. 결론

본 논문에서는 양자 역학을 이용한 정보 보안 기술의 변혁을 일으킬 양자 통신 시스템에 대해서 설명하였다. 양자 정보를 표현하는 기본적인 이론에 대해서 설명하고 양자 통신의 암호 교환 방식인 QKD 시스템의 기초적인 이론을 설명하였다. QKD 시스템을 분석하여 보안성을 부정할 수 있는 다양한 양자 통신 공격 방식을 설명하였다. 따라서 양자 통신을 구현하기 위한 디바이스들의 현실적인 한계가 보안성을 보장 할 수 없기 때문에 기존의 정보 이론을 이용한 후처리 방식을 연구하여 양자 정보를 도청자로부터 보호하고 전송 효율을 높이기 위한 연구가 필요하다.

참 고 문 헌

[1] N.Gisin,G. Ribordy,W. Tittel, andH. Zbinden, “Quantum cryptography,”*Rev. Mod. Phys.*, vol. 74, pp. 145 - 95, 2002.

[2] K. Inoue, E. Waks, and Y. Yamamoto, “Differential-phase-shift quantum key distribution,”*Phys. Rev. Lett.*, vol. 89, no. 3, pp. 037902-1 - 37902-3, Jul. 2002.

[3] K. Inoue, E. Waks, and Y. Yamamoto, “Differential-phase-shift quantum key distribution using coherent light,”*Phys. Rev.*

A, vol. 68, pp. 022317-1 - 022317-3, Aug. 2003.
[4] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, "Generalized privacy amplification,"*IEEE Trans. Inf. Theory,* vol. 41, no. 6, pp. 1915 - 1923, Nov. 1995.
[5] E. Waks, H. Takesue, and Y. Yamamoto, "Security of differential-phaseshift quantum key distribution against individual attacks,"*Phys. Rev. A, vol.* 73, no. 7, pp. 012344-1 - 12344-9, Jan. 2006.
[6] M. Curty, L. L. Zhang, H. -H. Lo, and N. L¨utkenhaus, "Sequential attacks against differential-phase-shift quantum key distribution with weak coherent states,"*Quant. Inf. Comput.,* vol. 7, no. 7, pp. 665 - 88,
[7] F. Gao, B. Liu, Q.-YWen, and H. Chen, "Flexible quantum private queries based on quantum key distribution,"*Opt. Exp., vol.* 20, pp. 17411 - 7420, 2012.
[8] J. Zhang, F.-Z Guo, F. Gao, B. Liu, and Q.-Y Wen, "Private database queries based on counterfactual quantum key distribution,"*Phys. Rev. A, vol.* 88, p. 022334, 2013.
[9] M. V. P. Rao and M. Jakobi, "Towards communication-efficient quantum oblivious key distribution," *Phys. Rev. A, vol.* 87, p. 012331, 2013.

저자

이 선 의(Sun Yui Lee)

・2013년 2월 : 광운대학교 전파공학과 졸업
・2013년 2월 ~ 현재 : 광운대학교 전파공학과 석박사통합과정

<관심분야> : 가시광 통신, 협력통신, 인 지무선통신, 양자통신

정 국 현(Kuk Hyun Jung)

・2013년 8월 : 광운대학교 전파공학과 졸업
・2013년 9월 ~ 현재 : 광운대학교 전파공학과 석사과정

<관심분야> : 가시광 통신, 협력통신, 인지무선통신

김 진 영(Jin Young Kim) **종신회원**

・1998년 2월 : 서울대학교 전자공학과 공학박사
・2001년 2월 : SK텔레콤 네트웍연구소 책임연구원
・2001년 3월 ~ 현재 : 광운대학교전자융합공학과 교수

<관심분야> : 다지털통신, 가시광통신, UWB, 부호화, 인지무선통신, 4G 이동통신