TTA Standard

정보통신단체표준(국문표준)

제정일: 20xx년 xx월 xx일

양자 키 분배 - 제2부: BB84 프로토콜

Quantum Key Distribution - Part2: BB84 Protocol

TTA 한국정보통신기술협회
Telecommunications Technology Association

표준초안 검토 위원회 정보보호기반 프로젝트그룹(PG501)

표준안 심의 위원회 정보보호 기술위원회(TC5)

	성명	소 속	직위	위원회 및 직위	표준번호
표준(과제) 제안	김나영	국가보안기술 연구소	연구원	정보보호기반 프로젝트그룹 위원	
표준 초안 작성자	김나영	국가보안기술 연구소	연구원	정보보호기반 프로젝트그룹 위원	
	홍창호	국가보안기술 연구소	선임연구원	-	
	권오성	국가보안기술 연구소	선임연구원	-	
	정연창	국가보안기술 연구소	선임연구원	-	
	지세완	국가보안기술 연구소	선임연구원	-	
	장진각	국가보안기술 연구소	책임연구원	-	
	권대성	국가보안기술 연구소	책임연구원	-	
사무국 담당	박수정	TTA	책임	-	

본 표준 발간 이전에 접수된 지식재산권 확약서 정보는 본 표준의 '부록(지식재산권 확약서 정보)'에 명시하고 있으며, 이후 접수된 지식재산권 확약서는 TTA 웹사이트에서 확인할 수 있습니다.
본 표준과 관련하여 접수된 확약서 외의 지식재산권이 존재할 수 있습니다.

발행인 : 한국정보통신기술협회 회장
발행처 : 한국정보통신기술협회
13591, 경기도 성남시 분당구 분당로 47
Tel : 031-724-0114, Fax : 031-724-0109
발행일 : 20xx.xx

서 문

1 표준의 목적

양자를 이용하여 비밀키를 공유하는 양자 키 분배(QKD, Quantum Key Distribution)를 실현하기 위한 다양한 프로토콜이 존재한다. 이 표준의 목적은 대표적인 QKD 프로토콜이며, 이론적으로 무조건부 안전성을 보장하는 BB84 프로토콜을 이용한 양자 키 분배 절차를 제시하는 것이다.

2 주요 내용 요약

QKD 표준은 제1부 일반, 제2부 BB84 프로토콜로 구성된다. 제1부 일반에서는 QKD의 개념을 바탕으로 일반적 모델을 정립하고, 다양한 QKD 프로토콜을 포괄할 수 있는 단계별 절차와 안전성 요구사항을 제시한다. 제2부인 이 표준은 QKD의 구현 안전성을 높이는 디코이 기법이 적용된 BB84 프로토콜의 단계별 세부 절차와 안전성 고려사항을 제시한다.

3 인용 표준과의 비교

3.1 인용 표준과의 관련성

해당사항 없음

3.2 인용 표준과 본 표준의 비교표

해당사항 없음

Preface

1 Purpose

There are various protocols for Quantum Key Distribution(QKD) to share random keys using quantum mechanics laws. The standard provides a QKD process using BB84 protocol which is a representative QKD protocol and guarantees unconditional security theoretically.

2 Summary

The QKD standards consist of Quantum Key Distribution – Part1: General and Part2: BB84 protocol. The part1 provides a general model which is based on the basic concept of QKD, stepwise process, and security requirements that would encompass the various QKD protocol. The part2 provides detailed process and security requirements for BB84 protocol with decoy method that enhance the implementation security of QKD.

3 Relationship to Reference Standards

- None

목 차

1 적용 범위 ····· 1

2 인용 표준 ····· 1

3 용어 정의 ····· 1

4 약어 및 기호 ····· 3

5 BB84 프로토콜을 이용한 QKD ····· 3
5.1 Raw키 생성 ····· 4
5.2 걸러진키 생성 ····· 7
5.3 비밀키 생성 ····· 8

6 BB84 프로토콜의 안전성 고려사항 ····· 10
6.1 Raw키 생성 ····· 10
6.2 걸러진키 생성 ····· 10
6.3 비밀키 생성 ····· 11

부록 Ⅰ-1 지식재산권 확약서 정보 ····· 12
Ⅰ-2 시험인증 관련 사항 ····· 13
Ⅰ-3 본 표준의 연계(family) 표준 ····· 14
Ⅰ-4 참고 문헌 ····· 15
Ⅰ-5 영문표준 해설서 ····· 17
Ⅰ-6 표준의 이력 ····· 18

양자 키 분배 - 제2부: BB84 프로토콜
(Quantum Key Distribution - Part2: BB84 Protocol)

1 적용 범위

양자 키 분배(Quantum Key Distribution, 이하 QKD)는 정당한 두 사용자가 양자(quantum)를 이용하여 안전하게 비밀키를 공유하는 것이다. 양자 키 분배는 조건부 안전성을 제공하는 기존 키 공유 기법과 달리 양자물리법칙에 기반하여 무조건부 안전성(unconditional security)이 보장된다. QKD를 실현하기 위한 프로토콜로 BB84[1)][1], B92[2], 6-state[3], Ekert91[4], BBM92[5] 등이 있으며, BB84 프로토콜을 비롯한 몇몇 기법들이 이론상 무조건부 안전성이 증명되었다.

다양한 QKD 프로토콜 중에서 BB84 프로토콜은 단일광자를 사용하는 구현 모델에서 이론적으로 안전성이 잘 증명되어 있고[6], 가장 많이 사용되고 있다. 그러나 물리적으로 단일광자 구현이 불가능한 현재, BB84 프로토콜은 디코이 기법[7]과 함께 사용되며 이에 대한 안전성 역시 잘 증명되어 있다[8,9]. 따라서 이 표준에서는 디코이 기법을 적용한 BB84 프로토콜을 대상으로 QKD의 각 단계에 필요한 세부 절차와 안전성 고려사항을 제시한다. 한편 BB84 프로토콜에서 양자상태를 전송하는 방법은 부호화 방식과 전송방향에 따라 다양한 선택이 가능하며, 사전 광학계 동기화 등 부수 작업이 필요하지만 이에 대한 상세한 설명은 BB84 프로토콜의 QKD 절차를 범위로 하는 본 표준에서는 다루지 않는다.

2 인용 표준

해당사항 없음

3 용어 정의

3.1 QKD 프로토콜(QKD protocol)
양자 키 분배를 하기 위한 통신 규약들

3.2 raw키(raw key)
양자채널을 통한 양자상태의 송·수신 결과인 키 수열

1) C.H. Bennett,와 G. Brassard,이 1984년에 제안한 프로토콜을 BB84 프로토콜이라 명명한다.

3.3 걸러진키(sifted key)
송·수신자 사이에 동일한 기저를 사용한 키 수열

3.4 광자(photon)
빛의 입자인 양자로 빛 에너지의 최소 단위

3.5 광자수 분리 공격(PNS, photon number splitting attack)
단일 광자 상태를 가정한 QKD 장비가 실제 구현에서 기술상의 한계로 인해 높은 확률로 다중 광자가 전송되므로 공격자가 다중 광자 중 일부 광자를 가로채어 키 정보를 알아내는 공격

3.6 공개채널(public channel)
도청자를 포함하여 외부에 완전히 공개된 채널로 非양자정보가 전송되는 채널. 공개채널로 전송되는 정보는 누구나 확인 가능하나 변조되지 않음을 가정하며 일반적으로 QKD에서 사용하는 공개채널은 고전채널(classical channel)이라 칭하기도 함

3.7 기저(basis)
양자상태를 구분 짓는 기준 좌표

3.8 디코이(decoy)
PNS 공격 감지를 위해 시그널과 다른 평균 광자 수를 가지도록 조작되어 섞인 양자상태

3.9 비밀증폭(privacy amplification)
오류정정 과정의 공개된 정보와 이로 인해 비밀키의 유추 가능한 정보를 제거하는 과정

3.10 비밀키(secret key)
QKD를 통해 생성된 최종 키. QKD의 최종 결과물

3.11 시그널(signal)
일반적으로 신호를 의미하는 용어이지만 QKD에서는 키 정보를 전달하는 데 직접적으로 관여하는 양자상태를 나타냄

3.12 양자비트오류율(QBER. quantum bit error rate)
걸러진키에서 오류의 정도

3.13 양자채널(quantum channel)
양자의 물리적 상태를 전송하는 채널

3.14 오류정정(reconciliation)
걸러진키의 오류를 수정하는 과정

3.15 위상 부호화(phase encoding)
광자의 위상차를 이용하여 부호화함

3.16 유니버셜 해시함수(universal hash function)
일방향 함수의 일종으로 충돌이 일어날 가능성이 최대 $1/2^M$이 되는 함수를 의미함. 여기서 M은 입력메시지의 전체 길이를 표현함

3.17 인증키(authentication key)
사용자 또는 장비 인증에 사용되는 키로 사전에 나누어 공유되거나 비밀키 중에서 일부를 인증키로 사용

3.18 편광 부호화(polarization encoding)
광자의 방향성을 이용하여 부호화함

3.19 후처리 과정(post process)
오류정정 단계와 비밀증폭 단계를 합쳐서 일컫는 과정

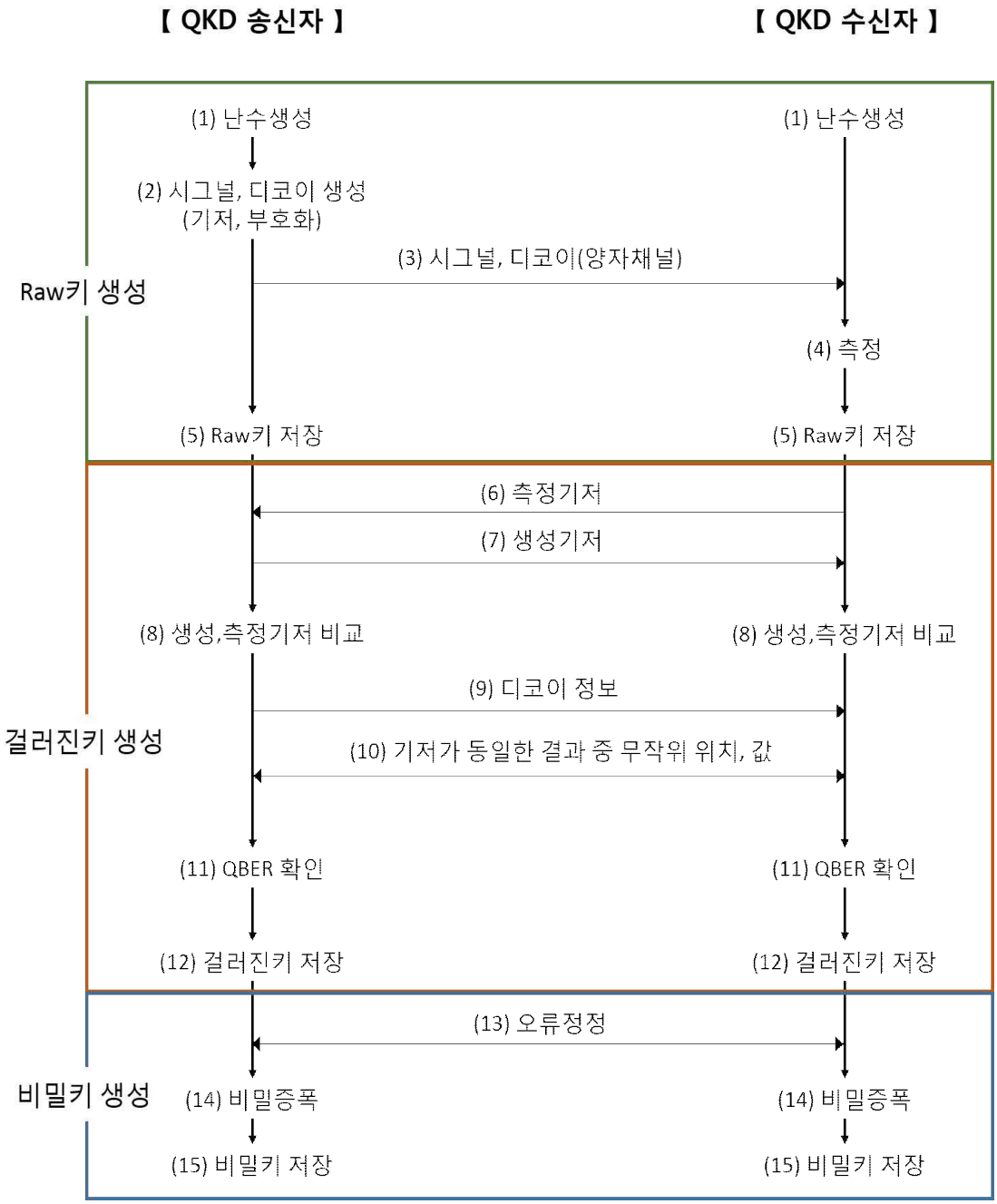
[출처(3.1~3.3, 3.6, 3.7, 3.9, 3.10, 3.13~3.16, 3.18, 3.19)]
TTAK.KO.-12.0xxx-Part1. 양자 키 분배 - 제1부: 일반

4 약어 및 기호

PNS	Photon Number Splitting
QBER	Quantum Bit Error Rate
QKD	Quantum Key distribution

5 BB84 프로토콜을 이용한 QKD

BB84 프로토콜을 이용한 QKD를 제1부 일반에서 제시한 QKD 일반 모델을 기준으로 제시한다. 여기에서 BB84 프로토콜은 디코이 기법[7]과 함께 사용한다. BB84 프로토콜은 QKD 절차 중 raw키 생성 단계 및 걸러진키 생성 단계와 직접 연관되어 있고, 비밀키 생성 단계와 함께 안전성 증명이 완성된다. 이 표준에서는 BB84 프로토콜의 세부절차를 제시하며 이는 (그림 5-1)과 같다.



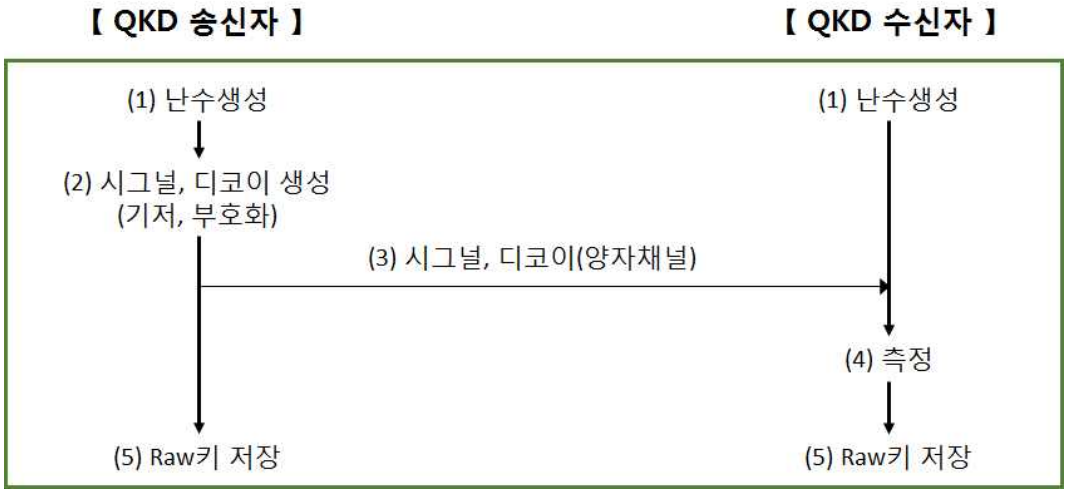
(그림 5-1) BB84 프로토콜을 이용한 QKD 절차

5.1 Raw키 생성

BB84 프로토콜의 raw키 생성 단계는 시그널과 디코이를 생성하여 각각에 대응되는 양자상태를 생성, 전송, 수신, 측정하는 단계이다. Raw키 생성에 필요한 핵심요소는 다음과 같다.

- **핵심요소** : 난수, 시그널, 디코이, 생성기저, 측정기저, 부호화 방식(편광, 위상), 구현 방향(단방향, 양방향)

BB84 프로토콜에서 raw키 생성 단계는 다음과 같이 진행되며 각 세부절차에 대한 상세한 내용을 하위 절에서 설명한다.



- Raw키 생성 단계

(1) 송·수신자는 시그널과 디코이 선택, 기저선택과 부호화(encoding) 등에 사용할 난수를 생성한다(5.1.1절).
(2) 송신자가 키 추출에 관여하는 시그널과 외부 공격에 대비하는 디코이를 무작위로 선택한다(5.1.2절).
(3) 선택한 시그널과 디코이에 대하여 생성기저와 부호화할 값을 각각 무작위로 선택하고 네 가지 양자상태 중 하나를 생성하여 양자채널을 통해서 수신자에게 전송한다(5.1.3절).
(4) 수신자는 두 측정 기저 중 하나를 무작위로 선택하여 신호를 측정한다(5.1.4절).
(5) 송신자는 생성한 양자상태를, 수신자는 측정한 양자상태의 결과를 각자 raw키로 저장한다(5.1.5절).

5.1.1 난수생성

송·수신자는 시그널과 디코이 선택, 기저와 전송 값 선택 등에 사용할 난수를 생성한다. 시그널과 디코이는 송신자를 제외하고 그 누구도 구별할 수 없어야 하므로 난수를 사용해 무작위로 선택한다. 마찬가지로 송신자의 생성기저와 전송 값, 수신자의 측정기저 모두 난수를 사용하여 무작위로 선택한다. QKD에서 난수발생기는 양자난수발생기의 사용을 권고한다. 그러나 양자난수발생기의 물리적 결함 등으로 완벽한 난수를 생성하기 어려울 경우 의사난수 발생기[10,11,12]를 사용할 수 있다.

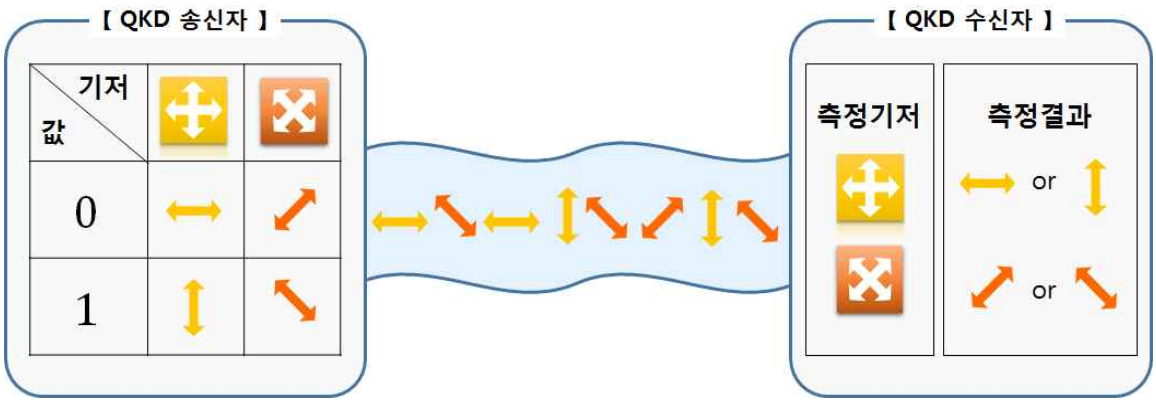
5.1.2 시그널과 디코이 선택

디코이 적용 BB84 프로토콜에서 raw키 생성은 우선 인증된 송신자가 키 추출에 관여하

는 시그널과 외부 공격에 대비하는 디코이를 무작위로 선택한다. 이때 시그널과 디코이는 송신자를 제외하고 그 누구도 구별할 수 없어야 한다. 만일 구별이 가능하다면, 다광자 환경에서 광자수 분리(PNS) 공격[13]이 가능하다.

5.1.3 양자상태 생성 및 전송

선택한 시그널이나 디코이에 대하여 두 기저 B_z와 B_x와 값 $0,1$ 중에 각각 하나씩 무작위로 선택한다. 무작위로 선택한 기저에 대하여 무작위로 선택한 값을 부호화하여 네 개의 양자상태 중 하나를 준비하고, 이를 양자채널을 통해서 수신자에게 전송한다. 네 개의 양자상태는 서로 비직교(nonorthogonal)한 관계인 두 기저 B_z와 B_x를 이용하여 나타낼 수 있으며, 각 기저내의 두 상태는 서로 직교한 관계에 있다. 예를 들어, 편광 부호화 방법을 이용하는 경우 네 양자상태는 두 기저, B_z와 B_x에 대해 각각 $\{|0\rangle,|1\rangle\}$와 $\{|+\rangle,|-\rangle\}$의 상태를 가진다. 여기서 $|+\rangle=\frac{1}{\sqrt{2}}\{|0\rangle+|1\rangle\}$이고 $|-\rangle=\frac{1}{\sqrt{2}}\{|0\rangle-|1\rangle\}$의 관계에 있다. 위상 부호화 방식을 사용하는 경우 네 가지 양자상태는 각 기저에 대해 $\{0,\pi\}$와 $\left\{\frac{1}{2}\pi,\frac{3}{2}\pi\right\}$로 표현될 수 있다. 양자상태를 전송하는 방법은 부호화 방식과 전송방향에 따라 다양한 선택이 가능하며, 사전 광학계 동기화 등 부수 작업이 필요하다. BB84 프로토콜의 편광 부호화 방식을 간단히 도시하면 (그림 5-2)와 같다.



(그림 5-3) BB84 프로토콜의 편광 부호화 방식 예시

5.1.4 양자상태 수신 및 측정

수신자는 송신자가 보내준 양자상태에 대해 두 측정 기저 $\{B_z, B_x\}$ 중 하나를 무작위로 선택하여 측정한다.

5.1.5 Raw키 저장

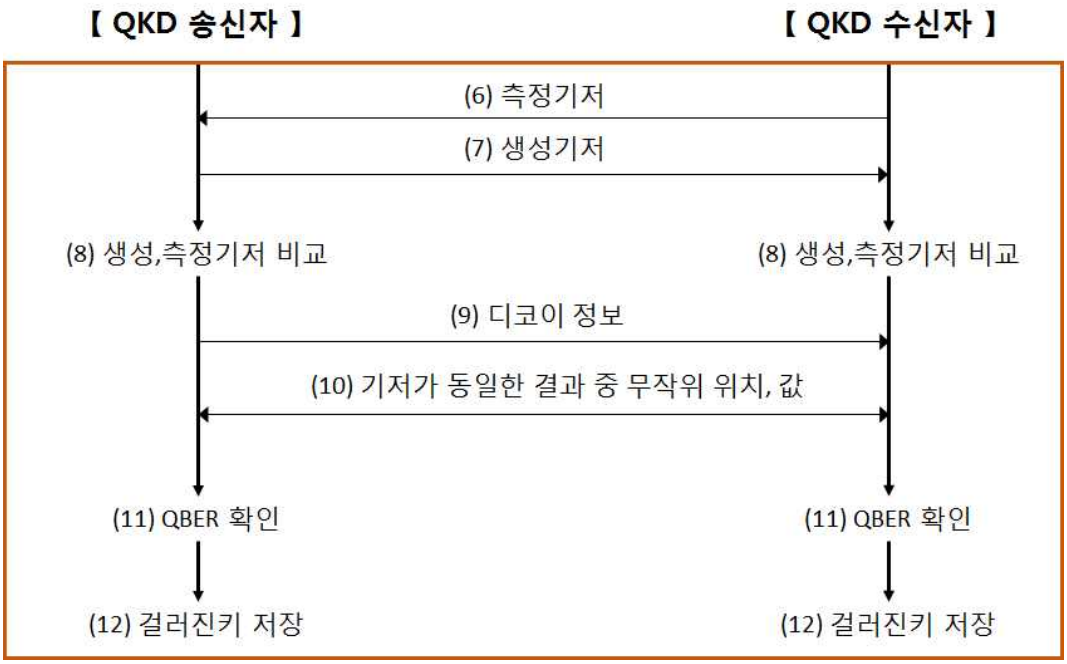
송신자는 생성한 양자상태를, 수신자는 측정한 양자상태의 결과를 각자 raw키로 저장한다.

5.2 걸러진키 생성

BB84 프로토콜의 걸러진키 생성 단계는 송·수신자가 각자 저장한 raw키에 대해 공개채널을 통해 가공하여 걸러진키로 만드는 단계이다. 걸러진키 생성에 필요한 핵심요소는 다음과 같다.

- **핵심요소 :** Raw키, 난수, 기저 정보, 디코이 정보

BB84 프로토콜에서 걸러진키 생성 단계는 다음과 같이 진행되며 각 세부절차에 대한 상세한 내용을 하위 절에서 설명한다.



- **걸러진키 생성 단계**

(6) 수신자는 공개채널을 이용하여 양자상태 측정에 사용한 기저를 공개한다(5.2.1절).
(7) 송신자는 공개채널을 이용하여 양자상태 생성에 사용한 기저를 공개한다(5.2.1절).
(8) 송·수신자는 교환한 기저정보를 비교한 후 기저가 동일한 결과만 저장한다(5.2.1절).
(9) 송신자는 사용한 디코이 정보를 수신자에게 전송한다(5.2.2절).
(10) 송·수신자는 기저가 동일한 결과들 중 일부를 무작위로 선택하고 그 위치와 값을 교환한다(5.2.3절).
(11) 도청 유무를 판단하기 위해 양자비트오류율(QBER)을 확인한다(5.2.3절).
(12) 송·수신자는 기저가 동일한 결과들 중 교환한 부분을 제외한 나머지를 각각 걸러진키로 저장한다. (5.2.4절)

5.2.1 기저 교환

송·수신자는 공개채널을 이용하여 각자 양자상태 생성과 측정에 사용한 기저를 공개하여 비교한 후 기저가 동일한 결과만 저장한다. 이 때 송신자가 생성한 양자상태와 수신자가 측정한 결과는 공개하지 않는다. 송신자와 수신자의 기저 선택이 완전히 무작위적이면 수신자가 측정한 양자상태들 중 확률적으로 절반 정도가 송신자가 사용한 기저와 같다.

5.2.2 디코이 정보 전송 및 수신

동일한 기저를 사용한 결과 중에서 송신자는 사용한 디코이 정보를 수신자에게 전송한다. 이 정보를 활용하여 수신자는 동일한 기저 중 시그널과 디코이를 구별한다.

5.2.3 양자비트오류율(QBER) 확인

양자채널의 안전성 확인을 위해 수신자는 기저가 동일한 결과들 중 일부를 무작위로 선택하여 그 위치를 송신자에게 알려주고, 송신자는 해당 부분들에 대해 준비한 양자상태들을 수신자에게 알려준다. 송신자와 수신자는 동일한 기저를 사용하였으므로 송신자가 공개한 양자상태는 수신자의 측정 결과와 동일해야 하지만, 실제 구현에서는 중간 공격자의 개입, 구성 장치들의 불완전함, 환경에 의한 오류 등에 의해 불일치한 결과들이 발생한다. 모든 불일치한 결과는 도청자의 공격으로 간주된다. 수신자는 이 단계에서 디코이를 활용하여 양자채널의 안전성을 판단하는 동시에 양자비트오류율(QBER, quantum bit error rate)을 추정한다. BB84 프로토콜을 이용한 QKD는 구현 환경 및 광학적 구현 모델에 따라 안전성이 보장 가능한 QBER의 상한이 정해지며, QBER이 정의된 상한 이하로 실측되어 양자채널이 안전하다고 판단되면 다음 단계로 진행하고, 그렇지 않으면 저장된 raw키를 모두 버리고 다시 raw키 생성 단계로 돌아간다.

5.2.4 걸러진키 저장

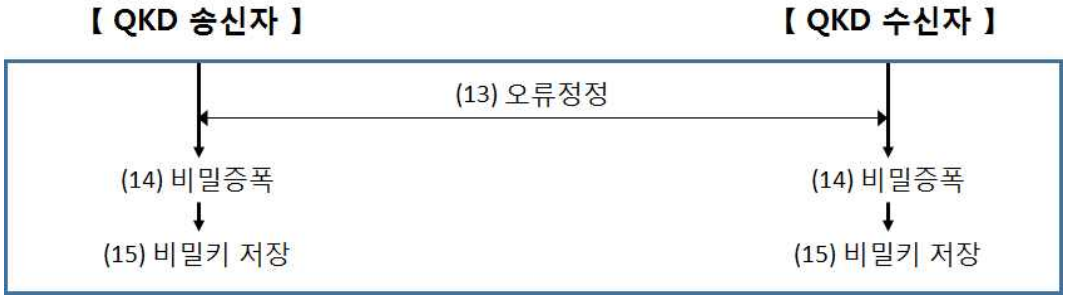
송신자와 수신자는 기저가 동일한 결과들 중 양자채널의 안전성을 검증하기 위해 쓰인 부분들을 제외하고 나머지 부분을 걸러진키로 저장한다.

5.3 비밀키 생성

BB84 프로토콜의 비밀키 생성 단계는 걸러진키에 후처리 과정인 오류정정(reconciliation)과 비밀증폭(privacy amplification) 절차를 적용하여 최종 비밀키를 생성하는 단계이다. 비밀키 생성에 필요한 핵심요소는 다음과 같다.

- **핵심요소 :** 걸러진키, 오류정정 기법, 비밀증폭 기법, 인증키

BB84 프로토콜에서 비밀키 생성 단계는 다음과 같이 진행되며 각 세부절차에 대한 상세한 내용을 하위 절에서 설명한다. 비밀키 생성 단계는 BB84프로토콜에 상관없이 진행되므로 제1부 일반에서 제시된 내용과 동일하다.



- 비밀키 생성 단계

(13) 송·수신자는 걸러진키를 일치시키기 위해 비트오류정정 기법을 이용하여 오류를 정정한다.(5.3.1절).

(14) 송·수신자는 오류정보 및 오류정정 과정에서 유출된 정보를 비밀증폭 과정으로 제거한다(5.3.2절)

(15) 송·수신자는 위의 모든 과정 수행 결과를 비밀키로 저장한다.(5.3.3절)

5.3.1 오류정정

송·수신자는 공개채널을 이용하여 공유된 걸러진키를 일치시키기 위해 다양한 비트오류정정 기법, 예를 들어 CASCADE[14], WINNOW[15], LDPC[16] 등을 사용하여 이전단계에서 확인된 QBER만큼의 오류정정을 수행한다. 이 때 수행되는 송·수신자 간의 통신에 의해 걸러진키에 대한 일부 정보가 유출된다.

5.3.2 비밀증폭

유출된 걸러진키의 정보와 이로 인해 유추 가능한 비밀키 정보를 제거하기 위해 비밀증폭 단계를 수행한다. 비밀증폭의 가장 일반적 방법은 일방향의 특성을 가진 유니버셜 해시 함수(universal hash function)를 이용하는 것이다. 이 때, 두 사용자가 사전에 공유한 인증키로 유니버셜 해시 함수를 구성하면 이 과정에서 서로의 신원을 확인하는 인증을 수행할 수 있다.

5.3.3 비밀키 저장

송·수신자는 오류정정과 비밀증폭 후 생성된 비밀키를 저장한다.

6. BB84 프로토콜의 안전성 고려사항

BB84 프로토콜이 제1부 일반에서 제시된 QKD의 안전성 요구사항을 충족하기 위해 고려해야 할 사항은 다음과 같다. QKD에서는 이론적 안정성뿐 아니라 물리적 구현의 안전성도 중요하다. 그러나 다양한 구현 환경과 광학적 구현 모델에 따라 물리적 구현의 고려사항이 달라진다. 이 표준에서는 QKD 프로토콜의 구현 환경 및 광학적 구현 모델에 의존하지 않고 BB84 프로토콜의 이론적 안전성을 보장하기 위해 필요한 고려사항을 제시한다.

6.1 Raw키 생성

Raw키 생성 단계에서 사용되는 정보의 무작위성이 보장되기 위하여 송신자는 시그널과 디코이의 구분, 양자상태의 기저와 부호화를 각각 무작위로 선택한다. 만일 위의 무작위성이 충족되지 않으면 도청자에게 키 정보가 유출될 수 있다.

무작위로 선택된 정보는 걸러진키 생성 단계 전까지 공개하지 않고 안전하게 보관한다. Raw키 생성 시 송신자의 양자상태 정보와 송·수신자의 기저 정보가 누출되면 이를 활용하여 도청자가 키 정보를 알 수 있다.

BB84 프로토콜에서는 디코이와 시그널의 평균 광자수는 서로 다르게 구성해야 한다. 그러나 송신자를 제외하고 시그널과 디코이는 그 누구도 구별할 수 없어야 한다. 만일 평균광자수를 다르게 구성하지 않으면 디코이 기법의 목적을 상실한다. 또한 raw키 생성 완료 전에 송신자를 제외한 누군가가 시그널과 디코이를 구별할 수 있으면 시그널 정보에 대한 PNS 공격이 가능하다.

6.2 걸러진키 생성

BB84 프로토콜 중 송·수신자는 '기저 교환(5.2.1절)' 과정에서 기저 정보만 공개한다. 예를 들어 부호화 정보와 같은 기저정보 이외 다른 정보가 '기저 교환' 과정에서 공개되면 도청자가 키 정보를 알 수 있다. 그러나 추후 '양자비트오류율(QBER) 확인(5.2.3절)'에서는 QBER을 실측하기 위해서 부호화 정보의 일부가 공개된다.

걸러진키 생성 단계에서 공개되는 정보는 변조가 불가능해야 하므로 다양한 무결성 보장 기법을 이용하여 정보의 변조 가능성을 확인한다. 공개채널로 송·수신되는 기저와 디코이 정보의 무결성을 보장하기 위해 전자 서명(digital signature), 암호 검사합(checksum), 오류 감지 코드(error detection code), 메시지 인증 코드(MAC) 기법 등이 사용될 수 있다.

걸러진키 생성과정을 통해 도청 여부가 확인되어야 하므로 '양자비트오류율(QBER) 확인(5.2.3절)' 에서 송·수신자는 동일한 기저를 가지는 결과 중 일부 부호화 정보를 무작위로

공개하여 QBER을 실측한다. 그리고 양자채널에서 실측된 QBER이 이론적 안전성이 보장되는 상한 이하인 경우에만 다음 절차를 진행한다. 그렇지 않은 경우는 도청자의 공격으로 간주하고 raw키 생성 단계로 돌아가서 양자채널을 다시 설정한다.

6.3 비밀키 생성

오류정정 기법에 필요한 정보들은 변조가 불가능해야 하므로 다양한 무결성 보장 기법을 적용하여 정보의 변조 가능성을 확인한다. 공개채널로 송·수신되는 오류정정 정보의 무결성을 보장하기 위해 전자 서명, 암호 검사합, 오류 감지 코드, 메시지 인증 코드 기법 등이 사용될 수 있다.

‘오류정정(5.3.1절)’ 에서 공개되는 정보는 반드시 제거해야 하며 공개된 내용을 통해 비밀키 정보가 유추될 수 있으므로 이를 보완하기 위해 ‘비밀증폭(5.3.2절)’을 수행해야 한다. 이때 QKD 안전성을 보장할 수 있는 비밀증폭 기법을 사용한다.

부 록 Ⅰ-1

지식재산권 확약서 정보

해당 사항 없음

부 록 Ⅰ-2

시험인증 관련 사항

해당 사항 없음

부 록 Ⅰ-3

본 표준의 연계(family) 표준

1-3.1 TTAK.KO.-12.0xxx - Part1.

QKD의 개념을 바탕으로 일반적 모델을 정립하고, 다양한 QKD 프로토콜을 포괄할 수 있는 단계별 절차와 안전성 요구사항을 제시함

부 록 Ⅰ-4

참고 문헌

[1] C.H. Bennett, G. Brassard, “Quantum cryptography: Public key distribution and coin tossing”, Proceedings of IEEE International Conference on Computer, Systems and Signal Processing, 175, 8, 1984.

[2] C.H. Bennett, “Quantum cryptography using any two nonorthogonal states”, Phys. Rev. Lett. 68, 3121, 1992.

[3] D. Bruss, “Optimal eavesdropping in quantum cryptography with six states”, Phys. Rev. Lett. 81, 3018, 1998.

[4] A.K. Ekert, “Quantum cryptography based on Bell’s theorem”, Phys. Rev. Lett. 67, 661, 1991

[5] C.H. Bennett, G. Brassard, N.D. Mermin, “Quantum cryptography without Bell’s theorem”, Phys. Rev. Lett. 68, 557, 1992.

[6] Peter W. Shor and John Preskill, “Simple Proof of Security of the BB84 Quantum Key Distribution Protocol”, Phys. Rev. Lett. 85, 441, 2000.

[7] Won-Young Hwang, “Quantum Key Distribution with High Loss: Toward Global Secure Communication”, Phys. Rev. Lett. 91, 057901, 2003.

[8] Xiang-Bin Wang, “Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography”, Phys. Rev. Lett. 94, 230503, 2005.

[9] Hoi-Kwong Lo, X. Ma, and K. Chen, “Decoy State Quantum Key Distribution”, Phys. Rev. Lett. 94, 230504, 2005.

[10] TTA TTAK.KO-12.0189/R1, “결정론적 난수발생기-제1부-블록암호 기반 난수발생기”, 2015.

[11] TTA TTAK.KO-12.0190, “결정론적 난수발생기-제2부-해시함수 기반 난수발생기”, 2012.

[12] TTA TTAK.KO-12.0191, “결정론적 난수발생기-제3부-HMAC 기반 난수발생기”, 2012.

[13] G. Brassard, N. Lutkenhaus, T. Mor, and B. C. Sanders, “Limitations on Practical Quantum Cryptography”, Phys. Rev. Lett. 85, 1330, 2000.

[14] F. Bessette, L. Salvail, “Secure key reconciliation by public discussion”, Advances in Cryptology-Proc. Eurocrypt '93, 410, 1994

[15] W.T. Buttler, S.K. Lamoreaux, J.R. Torgerson, G.H. Nickel, C.H. Donahue, C.G. Peterson, “Fast, efficient error reconciliation for quantum cryptography”, Phys. Rev. A 67, 52303, 2003

[16] D. Pearson, “High-speed QKD reconciliation using forward error correction”, Quantum Communication, Measurement and Computing, 04, 299, 2004

부 록 Ⅰ-5

영문표준 해설서

해당 사항 없음

부 록 Ⅰ-6

표준의 이력

판수	채택일	표준번호	내용	담당 위원회
제1판				