



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2017-0109366
(43) 공개일자 2017년09월29일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) H04L 9/06 (2006.01)
(52) CPC특허분류
H04L 9/08 (2013.01)
H04L 9/0656 (2013.01)
(21) 출원번호 10-2016-0033388
(22) 출원일자 2016년03월21일
심사청구일자 2016년03월21일

(71) 출원인
경희대학교 산학협력단
경기도 용인시 기흥구 덕영대로 1732 (서천동, 경희대학교 국제캠퍼스내)
(72) 발명자
신현동
경기도 수원시 영통구 청명북로 81, 404동 901호 (영통동, 청명마을주공아파트)
정영민
경기도 수원시 영통구 매영로415번길 50, 305호(영통동, 스타빌)
주나이드
경기도 용인시 기흥구 덕영대로 1732 (서천동)
(74) 대리인
최영한, 지덕규

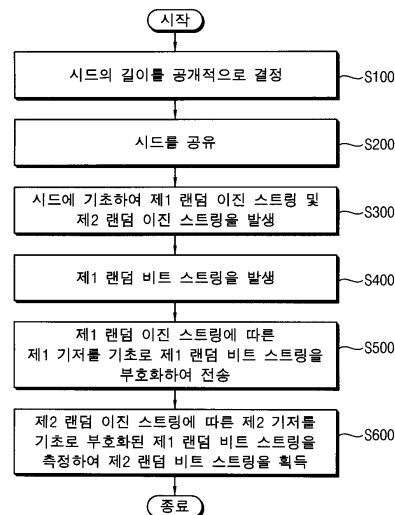
전체 청구항 수 : 총 15 항

(54) 발명의 명칭 양자 통신에서의 키 분배 방법, 이를 이용하는 양자 통신 방법 및 이를 수행하는 양자 통신 시스템

(57) 요약

양자 통신에서의 키 분배 방법에서, 송신기와 수신기가 시드의 길이를 공개적으로 결정한다. 송신기와 수신기가 미리 정해진 프로토콜을 실행하고 시드에 대한 제1 정보 조정 및 제1 비밀성 증폭을 수행하여, 시드를 공유한다. 송신기와 수신기가 시드에 기초하여 제1 랜덤 이진 스트링 및 제2 랜덤 이진 스트링을 각각 발생한다. 송신기가 제1 랜덤 비트 스트링을 발생한다. 송신기가 제1 랜덤 이진 스트링에 따른 제1 기저를 기초로 제1 랜덤 비트 스트링을 부호화하여 수신기에 전송한다. 수신기가 제2 랜덤 이진 스트링에 따른 제2 기저를 기초로 부호화된 제1 랜덤 비트 스트링을 측정하여 제2 랜덤 비트 스트링을 획득한다.

대표도 - 도2



(52) CPC특허분류

H04L 9/0852 (2013.01)

H04L 9/0869 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 R0190-15-2030

부처명 미래창조과학부

연구관리전문기관 한국연구재단

연구사업명 정보통신방송연구개발사업

연구과제명 양자암호통신망 구축을 통한 신뢰성 검증기술 및 QKD 고도화를 위한 핵심 요소기술 개발

기 여 율 1/1

주관기관 고려대학교 산학협력단

연구기간 2015.06.01 ~ 2016.05.31

명세서

청구범위

청구항 1

송신기와 수신기가 시드(seed)의 길이를 공개적으로(publicly) 결정하는 단계;

상기 송신기와 상기 수신기가 미리 정해진 프로토콜을 실행하고 상기 시드에 대한 제1 정보 조정(information reconciliation) 및 제1 비밀성 증폭(privacy amplification)을 수행하여, 상기 시드를 공유하는 단계;

상기 송신기와 상기 수신기가 상기 시드에 기초하여 제1 랜덤 이진 스트링 및 제2 랜덤 이진 스트링을 각각 발생하는 단계;

상기 송신기가 제1 랜덤 비트 스트링을 발생하는 단계;

상기 송신기가 상기 제1 랜덤 이진 스트링에 따른 제1 기저(basis)를 기초로 상기 제1 랜덤 비트 스트링을 부호화하여 상기 수신기에 전송하는 단계; 및

상기 수신기가 상기 제2 랜덤 이진 스트링에 따른 제2 기저를 기초로 상기 부호화된 제1 랜덤 비트 스트링을 측정하여 제2 랜덤 비트 스트링을 획득하는 단계를 포함하는 양자 통신에서의 키 분배 방법.

청구항 2

제 1 항에 있어서,

상기 미리 정해진 프로토콜은 BB84 프로토콜이며,

상기 시드를 공유하는 단계는,

상기 송신기가 랜덤 넘버인 상기 시드를 발생하는 단계;

상기 송신기가 상기 BB84 프로토콜에 기초하여 상기 시드를 상기 수신기에 전송하는 단계;

상기 송신기와 상기 수신기가 상기 시드의 동일성을 확보하기 위한 상기 제1 정보 조정을 수행하는 단계; 및

상기 송신기와 상기 수신기가 상기 시드에서 제3자에게 누설된 정보를 제거하기 위한 상기 제1 비밀성 증폭을 수행하는 단계를 포함하며,

상기 제1 정보 조정 및 상기 제1 비밀성 증폭에 의해, 상기 송신기와 상기 수신기가 상기 시드를 안전하게 공유하는 것을 특징으로 하는 양자 통신에서의 키 분배 방법.

청구항 3

제 2 항에 있어서,

상기 시드의 길이를 공개적으로 결정하는 단계는, 상기 송신기와 상기 수신기 사이의 공개 채널을 통해 수행되며,

상기 시드를 공유하는 단계는, 상기 공개 채널 및 상기 송신기와 상기 수신기 사이의 양자 채널을 통해 수행되는 것을 특징으로 하는 양자 통신에서의 키 분배 방법.

청구항 4

제 1 항에 있어서, 상기 송신기는 제1 랜덤 넘버 발생부를 포함하고, 상기 수신기는 상기 제1 랜덤 넘버 발생부와 동일한 타입의 상기 제2 랜덤 넘버 발생부를 포함하며,

상기 제1 랜덤 이진 스트링 및 상기 제2 랜덤 이진 스트링을 각각 발생하는 단계는,

상기 제1 랜덤 넘버 발생부가 상기 시드에 기초하여 상기 제1 랜덤 이진 스트링을 발생하는 단계; 및

상기 제2 랜덤 넘버 발생부가 상기 시드에 기초하여 상기 제2 랜덤 이진 스트링을 발생하는 단계를 포함하는 것

을 특징으로 하는 양자 통신에서의 키 분배 방법.

청구항 5

제 4 항에 있어서,

상기 제1 랜덤 이진 스트링의 비트 수 및 상기 제2 랜덤 이진 스트링의 비트 수는 상기 시드의 비트 수보다 큰 것을 특징으로 하는 양자 통신에서의 키 분배 방법.

청구항 6

제 5 항에 있어서,

상기 제1 랜덤 이진 스트링의 비트 수 및 상기 제2 랜덤 이진 스트링의 비트 수는 상기 제1 랜덤 비트 스트링의 비트 수 및 상기 제2 랜덤 비트 스트링의 비트 수와 동일한 것을 특징으로 하는 양자 통신 방법.

청구항 7

제 5 항에 있어서,

상기 제2 랜덤 이진 스트링은 상기 제1 랜덤 이진 스트링과 동일하며, 상기 제2 기저는 상기 제1 기저와 동일한 것을 특징으로 하는 양자 통신에서의 키 분배 방법.

청구항 8

제 7 항에 있어서,

상기 제2 랜덤 이진 스트링은 복수의 제1 비트들 및 복수의 제2 비트들을 포함하며,

상기 제1 비트는 수직 편광 신호 또는 수평 편광 신호를 측정하기 위한 십자 편광 필터에 상응하며, 상기 제2 비트는 대각 편광 신호를 측정하기 위한 대각 편광 필터에 상응하는 것을 특징으로 하는 양자 통신에서의 키 분배 방법.

청구항 9

제 1 항에 있어서,

상기 송신기와 상기 수신기가 상기 제1 및 제2 랜덤 비트 스트링들에 대한 제2 정보 조정 및 제2 비밀성 증폭을 수행하여, 보안 스트링을 공유하는 단계를 더 포함하는 것을 특징으로 하는 양자 통신에서의 키 분배 방법.

청구항 10

송신기와 수신기가 시드(seed)의 길이를 공개적으로(publicly) 결정하는 단계;

상기 송신기와 상기 수신기가 미리 정해진 프로토콜을 실행하고 상기 시드에 대한 제1 정보 조정(information reconciliation) 및 제1 비밀성 증폭(privacy amplification)을 수행하여, 상기 시드를 공유하는 단계;

상기 송신기와 상기 수신기가 상기 시드에 기초하여 제1 랜덤 이진 스트링 및 제2 랜덤 이진 스트링을 각각 발생하는 단계;

상기 송신기가 제1 랜덤 비트 스트링을 발생하는 단계;

상기 송신기가 상기 제1 랜덤 이진 스트링에 따른 제1 기저(basis)를 기초로 상기 제1 랜덤 비트 스트링을 부호화하여 상기 수신기에 전송하는 단계;

상기 수신기가 상기 제2 랜덤 이진 스트링에 따른 제2 기저를 기초로 상기 부호화된 제1 랜덤 비트 스트링을 측정하여 제2 랜덤 비트 스트링을 획득하는 단계;

상기 송신기와 상기 수신기가 상기 제1 및 제2 랜덤 비트 스트링들에 대한 제2 정보 조정 및 제2 비밀성 증폭을 수행하여, 보안 스트링을 공유하는 단계; 및

상기 송신기와 상기 수신기가 상기 보안 스트링을 기초로 데이터를 암호화하여 교환하는 단계를 포함하는 양자 통신 방법.

청구항 11

제 10 항에 있어서,

상기 보안 스트링의 비트 수는 상기 제1 랜덤 비트 스트링의 비트 수 및 상기 제2 랜덤 비트 스트링의 비트 수보다 작은 것을 특징으로 하는 양자 통신 방법.

청구항 12

제 10 항에 있어서,

상기 데이터는 상기 보안 스트링을 이용하는 원타임 패드(one-time pad) 방식에 의해 암호화되는 것을 특징으로 하는 양자 통신 방법.

청구항 13

시드(seed)에 기초하여 제1 랜덤 이진 스트링을 발생하고, 제1 랜덤 비트 스트링을 발생하며, 상기 제1 랜덤 이진 스트링에 따른 제1 기저(basis)를 기초로 상기 제1 랜덤 비트 스트링을 부호화하여 전송하는 송신기; 및

상기 시드에 기초하여 제2 랜덤 이진 스트링을 발생하고, 상기 제2 랜덤 이진 스트링에 따른 제2 기저를 기초로 상기 부호화된 제1 랜덤 비트 스트링을 측정하여 제2 랜덤 비트 스트링을 획득하는 수신기를 포함하고,

상기 송신기와 상기 수신기는, 상기 시드의 길이를 공개적으로(publicly) 결정하며, 미리 정해진 프로토콜을 실행하고 상기 시드에 대한 제1 정보 조정(information reconciliation) 및 제1 비밀성 증폭(privacy amplification)을 수행하여, 상기 시드를 공유하는 양자 통신 시스템.

청구항 14

제 13 항에 있어서,

상기 송신기와 상기 수신기 사이에 연결되는 공개 채널; 및

상기 송신기와 상기 수신기 사이에 연결되는 양자 채널을 더 포함하고,

상기 공개 채널을 통해 상기 시드의 길이가 공개적으로 결정되며,

상기 공개 채널 및 상기 양자 채널을 통해 상기 시드가 공유되는 것을 특징으로 하는 양자 통신 시스템.

청구항 15

제 13 항에 있어서,

상기 미리 정해진 프로토콜은 BB84 프로토콜이며,

상기 송신기가 랜덤 넘버인 상기 시드를 발생하고, 상기 송신기가 상기 BB84 프로토콜에 기초하여 상기 시드를 상기 수신기에 전송하고, 상기 송신기와 상기 수신기가 상기 시드의 동일성을 확보하기 위한 상기 제1 정보 조정을 수행하며, 상기 송신기와 상기 수신기가 제3자에게 누설된 정보를 제거하기 위한 상기 제1 비밀성 증폭을 수행하여, 상기 송신기와 상기 수신기가 상기 시드를 안전하게 공유하는 것을 특징으로 하는 양자 통신 시스템.

발명의 설명

기술 분야

[0001]

본 발명은 통신 시스템에 관한 것으로서, 더욱 상세하게는 양자 통신에서의 키 분배 방법, 상기 키 분배 방법을 이용하는 양자 통신 방법, 상기 키 분배 방법 및/또는 상기 양자 통신 방법을 수행하는 양자 통신 시스템에 관한 것이다.

배경 기술

[0002]

1984년 C. H. Bennett과 G. Brassard에 의해 고안된 양자 키 분배(quantum key distribution: QKD) 프로토콜은 BB84 프로토콜로 불릴 수 있다. 상기과 같은 BB84 프로토콜이 알려진 이후 양자 암호 분야에 엄청난 발전이 있어 왔다. 양자 키 분배 프로토콜의 핵심은 멀리 떨어져 있는 두 사용자가 공개된 통신 채널을 통해 암호 통신을

위한 비밀 키를 생성 및 공유하며, 동시에 공유된 비밀 키에 대한 무조건적 안전성(unconditional security)을 보장한다는 점이다.

- [0003] BB84 프로토콜은 안전한 방식이지만, 키 교환율(key exchange rate)이 상대적으로 낮을 수 있다. 따라서, 안전성이 보장되면서도 키 교환율을 향상시키기 위한 다양한 방식이 연구되고 있다.

발명의 내용

해결하려는 과제

- [0004] 본 발명의 일 목적은 키 교환율이 향상된 양자 통신에서의 키 분배 방법을 제공하는 것이다.
- [0005] 본 발명의 다른 목적은 상기 키 분배 방법을 이용하는 양자 통신 방법을 제공하는 것이다.
- [0006] 본 발명의 또 다른 목적은 상기 키 분배 방법 및/또는 상기 양자 통신 방법을 수행하는 양자 통신 시스템을 제공하는 것이다.

과제의 해결 수단

- [0007] 상기 일 목적을 달성하기 위해, 본 발명의 실시예들에 따른 양자 통신에서의 키 분배 방법에서, 송신기와 수신기가 시드(seed)의 길이를 공개적으로(publicly) 결정한다. 상기 송신기와 상기 수신기가 미리 정해진 프로토콜을 실행하고 상기 시드에 대한 제1 정보 조정(information reconciliation) 및 제1 비밀성 증폭(privacy amplification)을 수행하여, 상기 시드를 공유한다. 상기 송신기와 상기 수신기가 상기 시드에 기초하여 제1 랜덤 이진 스트링 및 제2 랜덤 이진 스트링을 각각 발생한다. 상기 송신기가 제1 랜덤 비트 스트링을 발생한다. 상기 송신기가 상기 제1 랜덤 이진 스트링에 따른 제1 기저(basis)를 기초로 상기 제1 랜덤 비트 스트링을 부호화하여 상기 수신기에 전송한다. 상기 수신기가 상기 제2 랜덤 이진 스트링에 따른 제2 기저를 기초로 상기 부호화된 제1 랜덤 비트 스트링을 측정하여 제2 랜덤 비트 스트링을 획득한다.
- [0008] 일 실시예에서, 상기 미리 정해진 프로토콜은 BB84 프로토콜일 수 있다. 상기 시드를 공유하는데 있어서, 상기 송신기가 랜덤 넘버인 상기 시드를 발생할 수 있다. 상기 송신기가 상기 BB84 프로토콜에 기초하여 상기 시드를 상기 수신기에 전송할 수 있다. 상기 송신기와 상기 수신기가 상기 시드의 동일성을 확보하기 위한 상기 제1 정보 조정을 수행할 수 있다. 상기 송신기와 상기 수신기가 상기 시드에서 제3자에게 누설된 정보를 제거하기 위한 상기 제1 비밀성 증폭을 수행할 수 있다. 상기 제1 정보 조정 및 상기 제1 비밀성 증폭에 의해, 상기 송신기와 상기 수신기가 상기 시드를 안전하게 공유할 수 있다.
- [0009] 일 실시예에서, 상기 시드의 길이를 공개적으로 결정하는 단계는, 상기 송신기와 상기 수신기 사이의 공개 채널을 통해 수행될 수 있다. 상기 시드를 공유하는 단계는, 상기 공개 채널 및 상기 송신기와 상기 수신기 사이의 양자 채널을 통해 수행될 수 있다.
- [0010] 일 실시예에서, 상기 송신기는 제1 랜덤 넘버 발생부를 포함하고, 상기 수신기는 상기 제1 랜덤 넘버 발생부와 동일한 타입의 상기 제2 랜덤 넘버 발생부를 포함할 수 있다. 상기 제1 랜덤 이진 스트링 및 상기 제2 랜덤 이진 스트링을 각각 발생하는데 있어서, 상기 제1 랜덤 넘버 발생부가 상기 시드에 기초하여 상기 제1 랜덤 이진 스트링을 발생할 수 있다. 상기 제2 랜덤 넘버 발생부가 상기 시드에 기초하여 상기 제2 랜덤 이진 스트링을 발생할 수 있다.
- [0011] 일 실시예에서, 상기 제1 랜덤 이진 스트링의 비트 수 및 상기 제2 랜덤 이진 스트링의 비트 수는 상기 시드의 비트 수보다 클 수 있다.
- [0012] 일 실시예에서, 상기 제1 랜덤 이진 스트링의 비트 수 및 상기 제2 랜덤 이진 스트링의 비트 수는 상기 제1 랜덤 비트 스트링의 비트 수 및 상기 제2 랜덤 비트 스트링의 비트 수와 동일할 수 있다.
- [0013] 일 실시예에서, 상기 제2 랜덤 이진 스트링은 상기 제1 랜덤 이진 스트링과 동일하며, 상기 제2 기저는 상기 제1 기저와 동일할 수 있다.
- [0014] 일 실시예에서, 상기 제2 랜덤 이진 스트링은 복수의 제1 비트들 및 복수의 제2 비트들을 포함할 수 있다. 상기 제1 비트는 수직 편광 신호 또는 수평 편광 신호를 측정하기 위한 십자 편광 필터에 상응하며, 상기 제2 비트는 대각 편광 신호를 측정하기 위한 대각 편광 필터에 상응할 수 있다.
- [0015] 일 실시예에서, 상기 송신기와 상기 수신기가 상기 제1 및 제2 랜덤 비트 스트링들에 대한 제2 정보 조정 및 제

2 비밀성 증폭을 수행하여, 보안 스트링을 더 공유할 수 있다.

[0016] 상기 다른 목적을 달성하기 위해, 본 발명의 실시예들에 따른 양자 통신 방법에서, 송신기와 수신기가 시드(seed)의 길이를 공개적으로(publicly) 결정한다. 상기 송신기와 상기 수신기가 미리 정해진 프로토콜을 실행하고 상기 시드에 대한 제1 정보 조정(information reconciliation) 및 제1 비밀성 증폭(privacy amplification)을 수행하여, 상기 시드를 공유한다. 상기 송신기와 상기 수신기가 상기 시드에 기초하여 제1 랜덤 이진 스트링 및 제2 랜덤 이진 스트링을 각각 발생한다. 상기 송신기가 제1 랜덤 비트 스트링을 발생한다. 상기 송신기가 상기 제1 랜덤 이진 스트링에 따른 제1 기저(basis)를 기초로 상기 제1 랜덤 비트 스트링을 부호화하여 상기 수신기에 전송한다. 상기 수신기가 상기 제2 랜덤 이진 스트링에 따른 제2 기저를 기초로 상기 부호화된 제1 랜덤 비트 스트링을 측정하여 제2 랜덤 비트 스트링을 획득한다. 상기 송신기와 상기 수신기가 상기 제1 및 제2 랜덤 비트 스트링들에 대한 제2 정보 조정 및 제2 비밀성 증폭을 수행하여, 보안 스트링을 공유한다. 상기 송신기와 상기 수신기가 상기 보안 스트링을 기초로 데이터를 암호화하여 교환한다.

[0017] 일 실시예에서, 상기 보안 스트링의 비트 수는 상기 제1 랜덤 비트 스트링의 비트 수 및 상기 제2 랜덤 비트 스트링의 비트 수보다 작을 수 있다.

[0018] 일 실시예에서, 상기 데이터는 상기 보안 스트링을 이용하는 원타임 패드(one-time pad) 방식에 의해 암호화될 수 있다.

[0019] 상기 또 다른 목적을 달성하기 위해, 본 발명의 실시예들에 따른 양자 통신 시스템은 송신기 및 수신기를 포함한다. 상기 송신기는 시드(seed)에 기초하여 제1 랜덤 이진 스트링을 발생하고, 제1 랜덤 비트 스트링을 발생하며, 상기 제1 랜덤 이진 스트링에 따른 제1 기저(basis)를 기초로 상기 제1 랜덤 비트 스트링을 부호화하여 전송한다. 상기 수신기는 상기 시드에 기초하여 제2 랜덤 이진 스트링을 발생하고, 상기 제2 랜덤 이진 스트링에 따른 제2 기저를 기초로 상기 부호화된 제1 랜덤 비트 스트링을 측정하여 제2 랜덤 비트 스트링을 획득한다. 상기 송신기와 상기 수신기는, 상기 시드의 길이를 공개적으로(publicly) 결정하며, 미리 정해진 프로토콜을 실행하고 상기 시드에 대한 제1 정보 조정(information reconciliation) 및 제1 비밀성 증폭(privacy amplification)을 수행하여, 상기 시드를 공유한다.

[0020] 일 실시예에서, 상기 양자 통신 시스템은 공개 채널 및 양자 채널을 더 포함할 수 있다. 상기 공개 채널은 상기 송신기와 상기 수신기 사이에 연결될 수 있다. 상기 양자 채널은 상기 송신기와 상기 수신기 사이에 연결될 수 있다. 상기 공개 채널을 통해 상기 시드의 길이가 공개적으로 결정될 수 있다. 상기 공개 채널 및 상기 양자 채널을 통해 상기 시드가 공유될 수 있다.

[0021] 일 실시예에서, 상기 미리 정해진 프로토콜은 BB84 프로토콜일 수 있다. 상기 송신기가 랜덤 넘버인 상기 시드를 발생하고, 상기 송신기가 상기 BB84 프로토콜에 기초하여 상기 시드를 상기 수신기에 전송하고, 상기 송신기와 상기 수신기가 상기 시드의 동일성을 확보하기 위한 상기 제1 정보 조정을 수행하며, 상기 송신기와 상기 수신기가 제3자에게 누설된 정보를 제거하기 위한 상기 제1 비밀성 증폭을 수행하여, 상기 송신기와 상기 수신기가 상기 시드를 안전하게 공유할 수 있다.

발명의 효과

[0022] 상기와 같은 본 발명의 실시예들에 따른 양자 통신에서의 키 교환 방법 및 양자 통신 방법에서는, 송신기와 수신기가 상대적으로 작은 비트 수의 시드만을 공유하고, 시드에 기초하여 양자 정보 측정 기저와 관련된 제1 및 제2 랜덤 이진 스트링들을 발생함으로써, 안전성이 보장되면서도 키 교환율이 향상될 수 있다. 따라서, 양자 통신에서의 키 교환 방법 및/또는 양자 통신 방법을 수행하는 양자 통신 시스템의 성능이 향상될 수 있다.

도면의 간단한 설명

[0023] 도 1은 본 발명의 실시예들에 따른 양자 통신 시스템을 나타내는 블록도이다.

도 2는 본 발명의 실시예들에 따른 양자 통신에서의 키 분배 방법을 나타내는 순서도이다.

도 3은 도 2의 시드를 공유하는 단계의 일 예를 나타내는 순서도이다.

도 4는 도 2의 제1 및 제2 랜덤 이진 스트링들을 발생하는 단계의 일 예를 나타내는 순서도이다.

도 5a, 5b 및 6은 본 발명의 실시예들에 따른 양자 통신에서의 키 분배 방법을 설명하기 위한 도면들이다.

도 7은 본 발명의 실시예들에 따른 양자 통신에서의 키 분배 방법의 성능을 설명하기 위한 도면이다.

도 8은 본 발명의 실시예들에 따른 양자 통신 방법을 나타내는 순서도이다.

발명을 실시하기 위한 구체적인 내용

- [0024] 본문에 개시되어 있는 본 발명의 실시예들에 대해서, 특정한 구조적 내지 기능적 설명들은 단지 본 발명의 실시예를 설명하기 위한 목적으로 예시된 것으로, 본 발명의 실시예들은 다양한 형태로 실시될 수 있으며 본문에 설명된 실시예들에 한정되는 것으로 해석되어서는 아니 된다.
- [0025] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 형태를 가질 수 있는바, 특정 실시예들을 도면에 예시하고 본문에 상세하게 설명하고자 한다. 그러나 이는 본 발명을 특정한 개시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다.
- [0026] 제1, 제2 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로 사용될 수 있다. 예를 들어, 본 발명의 권리 범위로부터 이탈되지 않은 채 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다.
- [0027] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다. 구성요소들 간의 관계를 설명하는 다른 표현들, 즉 "~사이에"와 "바로 ~사이에" 또는 "~에 이웃하는"과 "~에 직접 이웃하는" 등도 마찬가지로 해석되어야 한다.
- [0028] 본 출원에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 실시된 특징, 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.
- [0029] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미이다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미인 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.
- [0030] 한편, 어떤 실시예가 달리 구현 가능한 경우에 특정 블록 내에 명기된 기능 또는 동작이 순서도에 명기된 순서와 다르게 일어날 수도 있다. 예를 들어, 연속하는 두 블록이 실제로는 실질적으로 동시에 수행될 수도 있고, 관련된 기능 또는 동작에 따라서는 상기 블록들이 거꾸로 수행될 수도 있다.
- [0031] 이하, 첨부한 도면들을 참조하여, 본 발명의 바람직한 실시예를 보다 상세하게 설명하고자 한다. 도면상의 동일한 구성요소에 대해서는 동일한 참조부호를 사용하고 동일한 구성요소에 대해서 중복된 설명은 생략한다.
- [0032] 도 1은 본 발명의 실시예들에 따른 양자 통신 시스템을 나타내는 블록도이다.
- [0033] 도 1을 참조하면, 양자 통신 시스템(10)은 송신기(100), 수신기(200), 제1 채널(310) 및 제2 채널(320)을 포함한다.
- [0034] 양자 통신 시스템(10)은 양자역학(quantum mechanics)을 이용하여 구현되는 통신 방식이며, 광자(photon)의 편광 상태(polarization)에 기초하여 정보를 전달할 수 있다.
- [0035] 본 발명의 실시예들에 따른 양자 통신 시스템(10)에서, 송신기(100)와 수신기(200)는 상대적으로 작은 비트 수의 시드(seed) 키를 이용한 키 분배 방법에 기초하여 암호 키를 발생하고 상기 암호 키에 기초하여 보안 통신을 수행할 수 있다.
- [0036] 송신기(100)는 시드 발생부(110), 제1 랜덤 넘버 발생부(120), 데이터 제공부(130), 부호화부(140) 및 송신부(150)를 포함할 수 있다.

- [0037] 시드 발생부(110)는 랜덤 넘버인 시드(s)를 발생할 수 있다. 예를 들어, 시드 발생부(110)는 시드(s)를 발생하기 위한 임의의 랜덤 넘버 발생기를 포함할 수도 있고, 사용자 설정 신호에 기초하여 수동으로(manually) 시드(s)를 발생할 수도 있다.
- [0038] 제1 랜덤 넘버 발생부(120)는 시드(s)에 기초하여 제1 랜덤 이진 스트링(random binary string)(X)을 발생할 수 있다. 예를 들어, 제1 랜덤 넘버 발생부(120)는 제1 랜덤 이진 스트링(X)을 발생하기 위한 제1 의사(pseudo)랜덤 넘버 발생기를 포함할 수 있다. 시드(s)는 상기 제1 의사 랜덤 넘버 발생기의 초기 입력(initial input)으로 제공될 수 있다.
- [0039] 데이터 제공부(130)는 제1 랜덤 비트 스트링(random bit string)(Y)을 발생할 수 있다. 예를 들어, 시드 발생부(110)와 유사하게, 데이터 제공부(130)는 제1 랜덤 비트 스트링(Y)을 발생하기 위한 임의의 랜덤 넘버 발생기를 포함할 수도 있고, 사용자 설정 신호에 기초하여 수동으로 제1 랜덤 비트 스트링(Y)을 발생할 수도 있다. 도 8을 참조하여 후술하는 것처럼, 데이터 제공부(130)는 키 분배 이후에 양자 통신 시스템(10) 내에서 암호화하여 교환하고자 하는 데이터를 발생할 수도 있다.
- [0040] 부호화부(140)는 제1 랜덤 이진 스트링(X)에 따른 제1 기저(basis)를 기초로 제1 랜덤 비트 스트링(Y)을 부호화하여 부호화된 제1 랜덤 비트 스트링(EY)을 발생할 수 있다. 부호화부(140)의 부호화 방식에 대해서는 후술하도록 한다.
- [0041] 송신부(150)는 시드(s) 및 부호화된 제1 랜덤 비트 스트링(EY)을 수신기(200)에 전송할 수 있다. 송신부(150)는 시드(s) 및 부호화된 제1 랜덤 비트 스트링(EY)을 출력하도록 제1 및 제2 채널들(310, 320)과 연결될 수 있다.
- [0042] 수신기(200)는 수신부(210), 제2 랜덤 넘버 발생부(220) 및 복호화부(230)를 포함할 수 있다.
- [0043] 수신부(210)는 송신기(100)로부터 시드(s) 및 부호화된 제1 랜덤 비트 스트링(EY')을 수신할 수 있다. 수신부(210)는 시드(s) 및 부호화된 제1 랜덤 비트 스트링(EY')을 수신하도록 제1 및 제2 채널들(310, 320)과 연결될 수 있다.
- [0044] 제2 랜덤 넘버 발생부(220)는 시드(s)에 기초하여 제2 랜덤 이진 스트링(X')을 발생할 수 있다. 제2 랜덤 넘버 발생부(220)는 제1 랜덤 넘버 발생부(120)와 실질적으로 동일한 타입일 수 있다. 예를 들어, 제2 랜덤 넘버 발생부(220)는 제2 랜덤 이진 스트링(X')을 발생하기 위한 제2 의사 랜덤 넘버 발생기를 포함할 수 있다. 시드(s)는 상기 제1 의사 랜덤 넘버 발생기와 실질적으로 동일한 상기 제2 의사 랜덤 넘버 발생기의 초기 입력으로 제공될 수 있다.
- [0045] 복호화부(230)는 제2 랜덤 이진 스트링(X')에 따른 제2 기저를 기초로 부호화된 제1 랜덤 비트 스트링(EY')을 측정하여 제2 랜덤 비트 스트링(Y')을 획득할 수 있다. 복호화부(230)의 측정 방식에 대해서는 후술하도록 한다.
- [0046] 제1 및 제2 채널들(310, 320)은 송신기(100)와 수신기(200) 사이에 연결되어 정보 전달 경로를 제공할 수 있다. 예를 들어, 제1 채널(310)은 고전 채널(classical channel) 또는 공개 채널(public channel)로 불릴 수 있고, 제2 채널(320)은 양자 채널(quantum channel) 또는 보안 채널(secure channel)로 불릴 수 있다. 제1 채널(310)은 TCP/IP 프로토콜을 이용할 수 있다.
- [0047] 한편, 도시하지는 않았지만, 송신기(100) 및 수신기(200) 각각은 시드(s), 랜덤 이진 스트링들(X, X'), 랜덤 비트 스트링들(Y, Y') 등을 저장하는 저장부를 더 포함할 수 있다.
- [0048] 이하에서는 본 발명의 실시예들에 따른 양자 통신 시스템(10)의 동작(예를 들어, 키 분배 동작 및/또는 데이터 교환 동작)을 보다 상세하게 설명하도록 한다.
- [0049] 도 2는 본 발명의 실시예들에 따른 양자 통신에서의 키 분배 방법을 나타내는 순서도이다.
- [0050] 도 1 및 2를 참조하면, 본 발명의 실시예들에 따른 양자 통신에서의 키 분배 방법에서, 송신기(100)와 수신기(200)가 시드(s)의 길이를 공개적으로(publicly) 결정한다(단계 S100). 상기 시드(s)의 길이는 전송하고자 하는 데이터의 양(예를 들어, 제1 랜덤 비트 스트링(Y)의 비트 수 및 제2 랜덤 비트 스트링(Y')의 비트 수)에 상응할 수 있다. 예를 들어, 상기 시드(s)의 길이가 증가할수록 통신의 정확도가 향상될 수 있다.
- [0051] 송신기(100)와 수신기(200)가 시드(s)를 공유한다(단계 S200). 구체적으로, 상기 시드 공유 동작을 수행하기 위해, 송신기(100)와 수신기(200)는 미리 정해진 프로토콜을 실행하고 시드(s)에 대한 제1 정보 조정(information reconciliation) 및 제1 비밀성 증폭(privacy amplification)을 수행한다. 단계 S200에 대해서는 도 3을 참조

하여 후술하도록 한다.

- [0052] 일 실시예에서, 상기 시드의 길이(s)를 공개적으로 결정하는 단계(S100)는, 제1 채널(310)인 상기 공개 채널만을 통해 수행될 수 있다. 또한, 시드(s)를 공유하는 단계(S200)는, 제1 채널(310)인 상기 공개 채널 및 제2 채널(320)인 상기 양자 채널 모두를 통해 수행될 수 있다.
- [0053] 송신기(100)와 수신기(200)가 시드(s)에 기초하여 제1 랜덤 이진 스트링(X) 및 제2 랜덤 이진 스트링(X')을 각각 발생한다(단계 S300). 단계 S300에 대해서는 도 4를 참조하여 후술하도록 한다.
- [0054] 송신기(100)가 제1 랜덤 비트 스트링(Y)을 발생하며(단계 S400), 송신기(100)가 제1 랜덤 이진 스트링(X)에 따른 상기 제1 기저를 기초로 제1 랜덤 비트 스트링(Y)을 부호화하고 부호화된 제1 랜덤 비트 스트링(EY)을 수신기(200)에 전송한다(단계 S500).
- [0055] 수신기(200)가 제2 랜덤 이진 스트링(X')에 따른 상기 제2 기저를 기초로 상기 부호화된 제1 랜덤 비트 스트링(EY')을 측정하여 제2 랜덤 비트 스트링(Y')을 획득한다(단계 S600).
- [0056] 한편, 도 2에서 도시하지는 않았지만, 도 8을 참조하여 후술하는 것처럼 단계 S600 이후에, 송신기(100)와 수신기(200)가 제1 및 제2 랜덤 비트 스트링들(Y, Y')에 대한 제2 정보 조정 및 제2 비밀성 증폭을 수행하여, 보안 스트링을 공유할 수 있다. 키 분배 이후에, 양자 통신 시스템(10) 내에서 상기 보안 스트링에 기초하여 데이터를 암호화하여 교환할 수 있다.
- [0057] 본 발명의 실시예들에 따른 양자 통신에서의 키 분배 방법에서는, 송신기(100)와 수신기(200)가 상대적으로 작은 비트 수의 시드(s)만을 공유하고, 시드(s)에 기초하여 양자 정보 측정 기저(즉, 상기 제1 기저 및 상기 제2 기저)와 관련된 제1 및 제2 랜덤 이진 스트링들(X, X')을 발생함으로써, 안전성이 보장되면서도 키 교환율(key exchange rate)이 향상될 수 있다.
- [0058] 도 3은 도 2의 시드를 공유하는 단계의 일 예를 나타내는 순서도이다.
- [0059] 도 1, 2 및 3을 참조하면, 시드(s)를 공유(단계 S200)하는데 있어서, 송신기(100)가 단계 S100에서 결정된 상기 시드(s)의 길이에 기초하여 시드(s)를 발생할 수 있다(단계 S210). 단계 S210은 시드 발생부(110)에 의해 수행될 수 있다.
- [0060] 송신기(100)가 시드(s)를 수신기(200)에 전송할 수 있다(단계 S220). 예를 들어, 단계 S200에서 상기 미리 정해진 프로토콜은 BB84 프로토콜일 수 있으며, 송신기(100)는 상기 BB84 프로토콜에 기초하여(즉, 상기 BB84 프로토콜을 실행하여) 시드(s)를 수신기(200)에 전송할 수 있다. 단계 S220은 송신부(150)에 의해 수행될 수 있다.
- [0061] 송신기(100)와 수신기(200)가 시드(s)의 동일성을 확보하기 위한 상기 제1 정보 조정을 수행할 수 있고(단계 S230), 송신기(100)와 수신기(200)가 시드(s)에서 제3자(third party)에게 누설된 정보를 제거하기 위한 상기 제1 비밀성 증폭을 수행할 수 있다(단계 S240).
- [0062] 상기 제1 정보 조정은 노이즈 및/또는 간섭 등에 의해 송신기(100)에서 발생된 시드(s)와 수신기(200)에서 수신된 시드(s) 간에 발생하는 불일치(예를 들어, 채널 오류 또는 제3자의 도청에 의한 오류)를 제거하는 동작을 나타낸다. 예를 들어, 상기 불일치를 조정하기 위해 오류 정정 코드가 사용될 수 있으며, 따라서 상기 정보 조정을 오류 정정(error correction)이라 부를 수도 있다.
- [0063] 상기 제1 비밀성 증폭은 송신기(100)와 수신기(200)가 공통된 시드(s)를 획득하는 과정에서 제3자에게 누설된 정보를 제거하는 동작을 나타낸다. 상기 비밀성 증폭에 의해 상기 시드(s)의 길이가 단계 S100에서 결정된 길이보다 감소될 수 있지만, 시드(s)의 랜덤성, 보안성, 안전성 및/또는 기밀성이 확보될 수 있다.
- [0064] 상기와 같은 정보 조정 및 비밀성 증폭은 양자 후처리(post-process) 기술일 수 있으며, 단계 S230 및 S240은 송신기(100) 및 수신기(200) 내부의 별도의 후처리부(미도시)에 의해 수행될 수 있다. 상기 제1 정보 조정 및 상기 제1 비밀성 증폭에 의해, 송신기(100)와 수신기(200)가 실질적으로(예를 들어, 매우 높은 확률로) 동일한 시드(s)를 안전하게 공유할 수 있다.
- [0065] 도 4는 도 2의 제1 및 제2 랜덤 이진 스트링들을 발생하는 단계의 일 예를 나타내는 순서도이다.
- [0066] 도 1, 2 및 4를 참조하면, 제1 및 제2 랜덤 이진 스트링들(X, X')을 발생(S300)하는데 있어서, 송신기(100)에 포함되는 제1 랜덤 넘버 발생부(120)가 시드(s)에 기초하여 제1 랜덤 이진 스트링(X)을 발생할 수 있고(단계 S310), 수신기(200)에 포함되는 제2 랜덤 넘버 발생부(220)가 시드(s)에 기초하여 제2 랜덤 이진 스트링(X')을

발생할 수 있다(단계 S320).

- [0067] 도 3을 참조하여 상술한 것처럼, 상기 BB84 프로토콜의 실행, 상기 제1 정보 조정의 수행 및 상기 제1 비밀성 증폭의 수행에 의해 송신기(100)와 수신기(200)는 실질적으로 동일한 시드(s)를 안전하게 공유할 수 있다. 또한, 도 1을 참조하여 상술한 것처럼, 송신기(100)에 포함되는 제1 랜덤 넘버 발생부(120)와 수신기(200)에 포함되는 제2 랜덤 넘버 발생부(220)는 실질적으로 동일한 타입의 랜덤 넘버 발생기를 포함할 수 있다. 따라서, 동일한 타입의 제1 및 제2 랜덤 넘버 발생부들(120, 220)이 동일한 시드(s)를 기초로 발생하는 제1 및 제2 랜덤 이진 스트링들(X, X')은 실질적으로(예를 들어, 매우 높은 확률로) 동일할 수 있다.
- [0068] 일 실시예에서, 제1 랜덤 이진 스트링(X)의 비트 수 및 제2 랜덤 이진 스트링(X')의 비트 수는 시드(s)의 비트 수보다 클 수 있다. 다만, 상기 제1 및 제2 랜덤 이진 스트링들(X, X') 각각의 비트 수가 상기 시드(s)의 비트 수보다 크더라도, 시드(s)에 상응하는 제1 랜덤 넘버가 제1 및 제2 랜덤 이진 스트링들(X, X') 각각에 상응하는 제2 랜덤 넘버보다 작을 수 있다. 예를 들어, 시드(s)는 이진수로 "10"(즉, 상기 제1 랜덤 넘버가 십진수로 "2")일 수 있고, 제1 및 제2 랜덤 이진 스트링들(X, X') 각각은 "00001"(즉, 상기 제2 랜덤 넘버가 십진수로 "1")일 수 있다.
- [0069] 일 실시예에서, 상기 제1 랜덤 이진 스트링(X)의 비트 수 및 상기 제2 랜덤 이진 스트링(X')의 비트 수는 부호화하고자 하는 데이터의 비트 수와 실질적으로 동일할 수 있다. 예를 들어, 상기 제1 랜덤 이진 스트링(X)의 비트 수 및 상기 제2 랜덤 이진 스트링(X')의 비트 수는 상기 제1 랜덤 비트 스트링(Y)의 비트 수 및 상기 제2 랜덤 비트 스트링(Y')의 비트 수와 실질적으로 동일할 수 있다.
- [0070] 도 5a, 5b 및 6은 본 발명의 실시예들에 따른 양자 통신에서의 키 분배 방법을 설명하기 위한 도면들이다.
- [0071] 도 1, 2, 5a, 5b 및 6을 참조하면, 송신기(100)가 제1 랜덤 비트 스트링(Y)을 발생하고(단계 S400), 송신기(100)가 제1 랜덤 이진 스트링(X)에 따른 상기 제1 기저를 기초로 발생하는 부호화된 제1 랜덤 비트 스트링(EY)을 수신기(200)에 전송하며(단계 S500), 수신기(200)가 제2 랜덤 이진 스트링(X')에 따른 상기 제2 기저를 기초로 상기 부호화된 제1 랜덤 비트 스트링(EY')을 측정하여 제2 랜덤 비트 스트링(Y')을 획득한다(단계 S600). 단계 S400은 데이터 제공부(130)에 의해 수행될 수 있고, 단계 S500은 부호화부(140) 및 송신부(150)에 의해 수행될 수 있으며, 단계 S600은 수신부(210) 및 복호화부(230)에 의해 수행될 수 있다.
- [0072] 도 4를 참조하여 상술한 것처럼, 제1 랜덤 이진 스트링(X) 및 제1 랜덤 비트 스트링(Y)은 동일한 비트 수를 가질 수 있다. 예를 들어, 제1 랜덤 이진 스트링(X) 및 제1 랜덤 비트 스트링(Y) 각각은 복수의 제1 비트들(예를 들어, "0") 및 복수의 제2 비트들(예를 들어, "1")을 포함하여 구현될 수 있다. 이와 유사하게, 제2 랜덤 이진 스트링(X') 및 제2 랜덤 비트 스트링(Y')은 동일한 비트 수를 가질 수 있다.
- [0073] 또한, 도 4를 참조하여 상술한 것처럼, 제2 랜덤 이진 스트링(X')은 제1 랜덤 이진 스트링(X)과 실질적으로 동일할 수 있으며, 따라서 제2 랜덤 이진 스트링(X')에 따른 상기 제2 기저는 제1 랜덤 이진 스트링(X)에 따른 상기 제1 기저와 실질적으로 동일할 수 있다.
- [0074] 일 실시예에서, 제1 랜덤 비트 스트링(Y)에 포함되는 비트들 각각은 실제 데이터를 나타낼 수 있고, 제1 랜덤 이진 스트링(X)에 포함되는 비트들 각각은 상기 실제 데이터의 부호화 방식을 나타낼 수 있다.
- [0075] 구체적으로, 제1 랜덤 이진 스트링(X)에 포함되는 상기 제1 비트("0")는 상기 실제 데이터 내의 하나의 비트가 수직 편광(vertical polarization) 신호 또는 수평 편광(horizontal polarization) 신호로 부호화됨을 나타낼 수 있다. 이러한 부호화 방식을 computational basis 방식으로 부를 수 있으며, 상기 수직 편광 신호 또는 상기 수평 편광 신호를 측정하기 위해 도 5a에 도시된 십자 편광(rectilinear polarization 또는 horizontal-vertical polarization) 필터(filter 또는 beam splitter)가 사용될 수 있다.
- [0076] 또한, 제1 랜덤 이진 스트링(X)에 포함되는 상기 제2 비트("1")는 상기 실제 데이터 내의 하나의 비트가 대각 편광(diagonal polarization) 신호로 부호화됨을 나타낼 수 있다. 이러한 부호화 방식을 Hadamard basis 방식으로 부를 수 있으며, 상기 대각 편광 신호를 측정하기 위해 도 5b에 도시된 대각 편광 필터가 사용될 수 있다. 단계 S500에서 제1 랜덤 이진 스트링(X)에 따른 상기 제1 기저 및 단계 S600에서 제2 랜덤 이진 스트링(X')에 따른 상기 제2 기저는 각각 computational basis와 Hadamard basis의 조합으로 표현될 수 있다.
- [0077] 일 실시예에서, 도 6에 도시된 것처럼, computational basis에서 상기 제1 비트("0")는 상기 수직 편광 신호로 부호화될 수 있고, 상기 제2 비트("1")는 상기 수평 편광 신호로 부호화될 수 있다. Hadamard basis에서 상기 제1 비트("0")는 상기 수직 편광 신호가 오른쪽으로 약 45도 회전된 제1 대각 편광 신호로 부호화될 수 있고,

상기 제2 비트("1")는 상기 수직 편광 신호가 왼쪽으로 약 45도 회전된 제2 대각 편광 신호로 부호화될 수 있다. 다만, 이러한 부호화 방식은 실시예에 따라서 다양하게 변경될 수 있다. 상기 수직 편광 신호, 상기 수평 편광 신호, 및 상기 제1 및 제2 대각 편광 신호 각각을 큐비트(qubit)라고 부를 수 있다.

[0078] 도 5a, 5b 및 6에 도시된 실시예에 기초하여 도 1의 단계 S300, S400, S500 및 S600의 일 예를 구체적으로 설명하면, 먼저 제1 랜덤 넘버 발생부(120) 및 제2 랜덤 넘버 발생부(220)는 안전하게 공유된 시드(s)에 기초하여 "00101110"의 제1 및 제2 랜덤 이진 스트링들(X, X')을 발생할 수 있다. 상술한 것처럼, 공통의 동일한 시드(s)에 기초하여 발생하는 제1 및 제2 랜덤 이진 스트링들(X, X')은 실질적으로 동일할 수 있다. 데이터 제공부(130)는 제1 랜덤 이진 스트링(X)과 비트 수가 동일한 "01101001"의 제1 랜덤 비트 스트링(Y)을 발생할 수 있다. 부호화부(140)는 "00101110"의 제1 랜덤 이진 스트링(X)에 따른 "+ + × + × × + +"의 상기 제1 기저를 기초로 "01101001"의 제1 랜덤 비트 스트링(Y)을 부호화하여, " | - \ | \ / / - "의 부호화된 제1 랜덤 비트 스트링(EY)을 발생할 수 있다. 송신부(150)는 " | - \ | \ / / - "의 부호화된 제1 랜덤 비트 스트링(EY)(즉, 큐비트들)을 수신기(200)에 전송할 수 있다. 수신부(210)는 " | - \ | \ / / - "의 부호화된 제1 랜덤 비트 스트링(EY')을 수신할 수 있다. 복호화부(230)는 "00101110"의 제2 랜덤 이진 스트링(X')에 따른 "+ + × + × × + +"의 상기 제2 기저를 기초로 " | - \ | \ / / - "의 부호화된 제1 랜덤 비트 스트링(EY')을 측정하여, "01101001"의 제2 랜덤 비트 스트링(Y')을 획득할 수 있다. 제1 및 제2 랜덤 이진 스트링들(X, X')이 실질적으로 동일하므로, 제1 및 제2 랜덤 비트 스트링들(Y, Y') 또한 실질적으로 동일할 수 있다.

[0079] 일 실시예에서, 부호화부(140) 및/또는 송신부(150)는 상기와 같은 수직/수평 편광 신호들 및 제1/제2 대각 편광 신호들을 발생하기 위한 네 개의 서로 다른 편광판(polarizer)들을 포함할 수 있다. 수신부(210) 및/또는 복호화부(230)는 상기와 같은 수직/수평 편광 신호들 및 제1/제2 대각 편광 신호들을 수신 및 검출하기 위한 두 개의 서로 다른 편광 필터들을 포함할 수 있다.

[0080] 이상, 편광 상태를 이용하여 신호를 전송하는 양자 통신 방식에 기초하여 본 발명의 실시예들을 상세하게 설명하였으나, 본 발명의 실시예들은 위상차를 이용하여 신호를 전송하는 양자 통신 방식에 대해서도 적용될 수 있다.

[0081] 도 7은 본 발명의 실시예들에 따른 양자 통신에서의 키 분배 방법의 성능을 설명하기 위한 도면이다.

[0082] 도 7을 참조하면, 수평 축은 양자 통신 시스템 내에서 교환되는 큐비트들의 개수를 나타내며, 수직 축은 키 교환율을 나타낸다. CASE1은 본 발명의 실시예들에 따른 키 분배 방법의 성능을 나타내고, CASE2는 종래의 키 분배 방법의 성능을 나타낸다.

[0083] 도 7에 도시된 것처럼, 종래의 키 분배 방법은 교환되는 큐비트들의 개수와 무관하게 하나의 큐비트 교환 당 약 0.5 고전 비트(classical bit)의 키 교환율을 가지지만, 본 발명의 실시예들에 따른 키 분배 방법은 교환되는 큐비트들의 개수가 증가할수록 키 교환율이 향상되며, 특히 약 0.7KB 이상의 큐비트들을 교환하는 경우에 종래의 키 분배 방법보다 성능이 향상됨을 확인할 수 있다. 따라서, 본 발명의 실시예들에 따른 키 분배 방법은 대용량의 데이터를 교환하는 경우에 보다 유용하게 적용될 수 있다.

[0084] 구체적으로, 종래의 양자 통신 시스템에서 약 10MB의 데이터를 교환하고자 하는 경우에는, 교환하고자 하는 데이터와 동일한 양의 기저 정보가 함께 교환되어야 하며, 따라서 (10*1024*1024*8*2)개인 약 167772160개의 큐비트들이 교환되어야 한다. 본 발명의 실시예들에 따른 양자 통신 시스템에서 약 10MB의 데이터를 교환하고자 하는 경우에는, 교환하고자 하는 데이터보다 매우 적은 양의 시드 정보가 교환하고자 하는 데이터와 함께 교환되면 충분하며, 시드의 길이가 약 1KB인 경우에 (10*1024*1024*8)+(2*1024)개인 약 83888128개의 큐비트들이 교환되면 충분할 수 있다.

[0085] 도 8은 본 발명의 실시예들에 따른 양자 통신 방법을 나타내는 순서도이다.

[0086] 도 1 및 8을 참조하면, 본 발명의 실시예들에 따른 양자 통신 방법에서, 송신기(100)와 수신기(200)가 시드(s)의 길이를 공개적으로 결정하고(단계 S1100), 송신기(100)와 수신기(200)가 시드(s)를 공유하고(단계 S1200), 송신기(100)와 수신기(200)가 시드(s)에 기초하여 제1 랜덤 이진 스트링(X) 및 제2 랜덤 이진 스트링(X')을 각각 발생하고(단계 S1300), 송신기(100)가 제1 랜덤 비트 스트링(Y)을 발생하고(단계 S1400), 송신기(100)가 제1 랜덤 이진 스트링(X)에 따른 상기 제1 기저를 기초로 제1 랜덤 비트 스트링(Y)을 부호화하고 부호화된 제1 랜덤 비트 스트링(EY)을 수신기(200)에 전송하며(단계 S1500), 수신기(200)가 제2 랜덤 이진 스트링(X')에 따른 상기 제2 기저를 기초로 상기 부호화된 제1 랜덤 비트 스트링(EY')을 측정하여 제2 랜덤 비트 스트링(Y')을 획득한다(단계 S1600). 도 8의 단계 S1100 내지 S1600은 도 2의 단계 S100 내지 S600과 각각 실질적으로 동일할 수 있다.

다.

- [0087] 송신기(100)와 수신기(200)가 제1 및 제2 랜덤 비트 스트링들(Y, Y')에 대한 제2 정보 조정 및 제2 비밀성 증폭을 수행하여, 보안 스트링을 공유한다(단계 S1700). 송신기(100)와 수신기(200)가 상기 보안 스트링을 기초로 데이터를 암호화하여 교환한다(단계 S1800). 단계 S1700은 상기 별도의 후처리부에 의해 수행될 수 있고, 단계 S1800은 송신기(100) 및 수신기(200)의 전반적인 동작에 의해 수행될 수 있다.
- [0088] 일 실시예에서, 상기 제1 정보 조정 및 상기 제1 비밀성 증폭과 유사하게, 상기 제2 정보 조정은 상기 보안 스트링의 동일성을 확보하기 위한 동작일 수 있고, 상기 제2 비밀성 증폭은 상기 보안 스트링에서 제3자에게 누설된 정보를 제거하기 위한 동작일 수 있다. 상기 제2 정보 조정 및 상기 제2 비밀성 증폭에 의해, 송신기(100)와 수신기(200)가 실질적으로 동일한 상기 보안 스트링을 안전하게 공유할 수 있다.
- [0089] 제1 및 제2 랜덤 비트 스트링들(Y, Y')은 로우 키(raw key) 또는 선별 키(sifted key)라고 불릴 수 있고, 상기 보안 스트링은 최종 키(final key)로 불릴 수 있다. 키 분배 이후에 실제 데이터 교환 동작은 최종 키인 상기 보안 스트링에 기초하여 수행될 수 있다.
- [0090] 일 실시예에서, 상기 보안 스트링의 비트 수는 상기 제1 랜덤 비트 스트링(Y)의 비트 수 및 상기 제2 랜덤 비트 스트링(Y')의 비트 수보다 작을 수 있다. 예를 들어, 상기 제2 비밀성 증폭에 의해 상기 보안 스트링이 상대적으로 작은 비트 수를 가질 수 있다.
- [0091] 일 실시예에서, 단계 S1800에서 교환되는 상기 데이터는 상기 보안 스트링을 이용하는 원타임 패드(one-time pad) 방식에 의해 암호화될 수 있다. 다만, 상기 데이터의 암호화 방식은 실시예에 따라서 다양하게 변경될 수 있다.
- [0092] 본 발명의 실시예들에 따른 양자 통신 방법에서는, 송신기(100)와 수신기(200)가 상대적으로 작은 비트 수의 시드(s)만을 공유하고, 시드(s)에 기초하여 양자 정보 측정 기저(즉, 상기 제1 기저 및 상기 제2 기저)와 관련된 제1 및 제2 랜덤 이진 스트링들(X, X')을 발생하며, 최종 키인 상기 보안 스트링에 기초하여 실제 데이터 교환 동작이 수행됨으로써, 안전성이 보장되면서도 키 교환율이 향상될 수 있다.
- [0093] 본 발명의 실시예들에 따른 양자 통신 시스템, 양자 통신에서의 키 교환 방법 및/또는 양자 통신 방법은 컴퓨터로 판독 가능한 매체에 저장된 컴퓨터로 판독 가능한 프로그램 코드를 포함하는 제품 등의 형태로 구현될 수 있다. 상기 컴퓨터로 판독 가능한 프로그램 코드는 판독 장치를 통해 다양한 컴퓨터 또는 다른 데이터 처리 장치의 프로세서로 제공될 수 있다. 컴퓨터로 판독 가능한 매체는 컴퓨터로 판독 가능한 신호 매체 또는 컴퓨터로 판독 가능한 기록 매체일 수 있다. 컴퓨터로 판독 가능한 기록 매체는 명령어 실행 시스템, 장비 또는 장치 내에 또는 이들과 접속되어 프로그램을 저장하거나 포함할 수 있는 임의의 유형적인 매체일 수 있다.
- [0094] 본 발명의 실시예들에 따른 양자 통신 시스템, 양자 통신에서의 키 교환 방법 및/또는 양자 통신 방법은, 휴대폰(Mobile Phone), 스마트 폰(Smart Phone), 태블릿(Tablet) PC(Personal Computer), 노트북(Laptop Computer), 개인 정보 단말기(Personal Digital Assistant; PDA), 휴대형 멀티미디어 플레이어(Portable Multimedia Player; PMP), 디지털 카메라(Digital Camera), 음악 재생기(Music Player), 휴대용 게임 콘솔(Portable Game Console), 네비게이션(Navigation) 시스템 등과 같은 임의의 모바일 기기에 적용될 수도 있고, PC(Personal Computer), 서버 컴퓨터(Server Computer), 워크스테이션(Workstation), 디지털 TV(Digital Television), 셋-탑 박스(Set-Top Box) 등과 같은 임의의 컴퓨팅 시스템에 적용될 수도 있다. 상기 모바일 기기는 웨어러블(wearable) 기기, 사물 인터넷(Internet of Things: IoT) 기기, 만물 인터넷(Internet of Everything: IoE) 기기, e-북(e-book) 등을 더 포함할 수 있다.

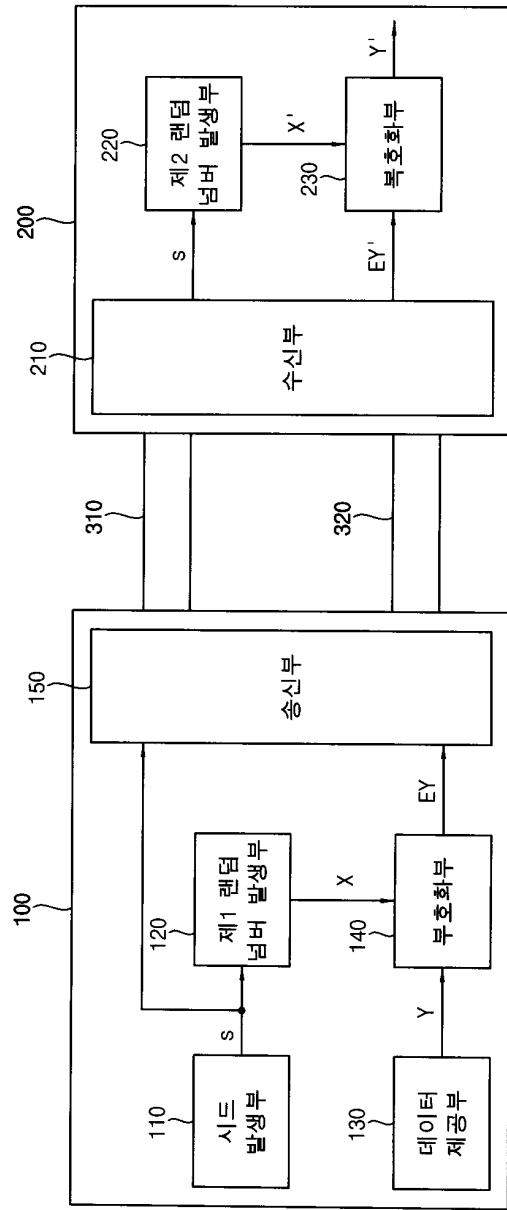
산업상 이용가능성

- [0095] 본 발명은 다양한 통신 장치 및 통신 시스템에 적용될 수 있다. 따라서 본 발명은 휴대폰, 스마트 폰, PDA, PMP, 디지털 카메라, 캠코더, PC, 서버 컴퓨터, 워크스테이션, 노트북, 디지털 TV, 셋-탑 박스, 음악 재생기, 휴대용 게임 콘솔, 네비게이션 시스템, 스마트 카드, 프린터 등과 같은 다양한 전자 기기에 유용하게 이용될 수 있다.
- [0096] 상기에서는 본 발명의 바람직한 실시예를 참조하여 설명하였지만, 해당 기술분야의 숙련된 당업자는 하기의 특허청구범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 것이다.

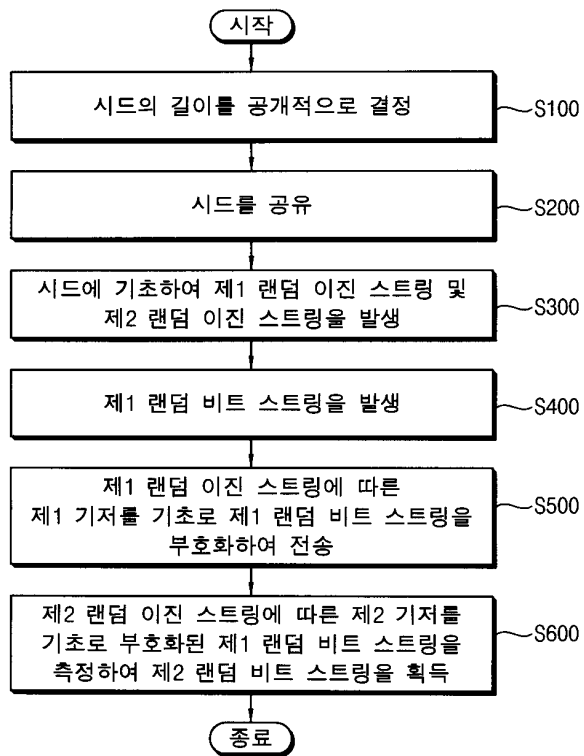
도면

도면1

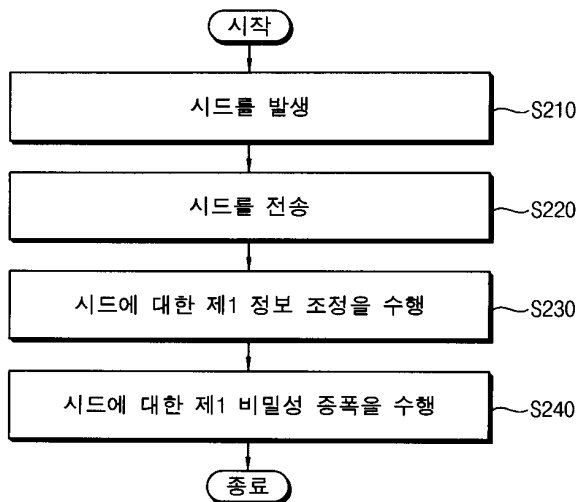
10



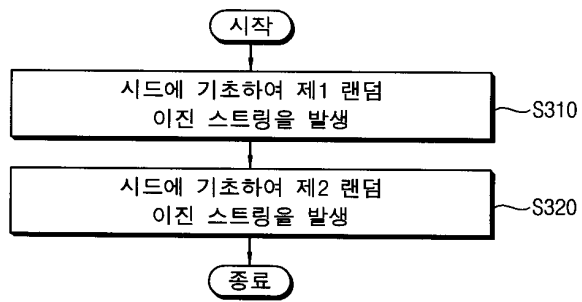
도면2



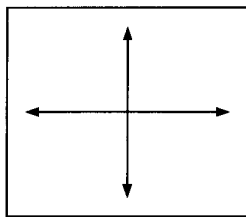
도면3



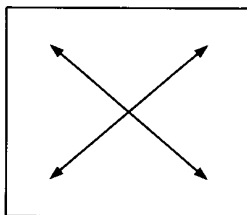
도면4



도면5a



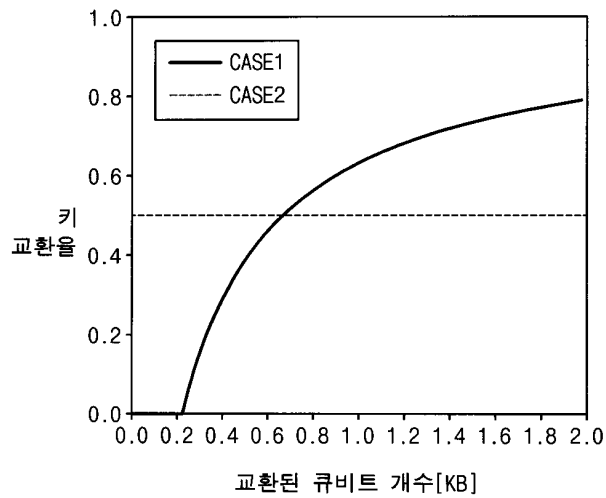
도면5b



도면6

	0	1

도면7



도면8

