(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2015-0088490
(43) 공개일자 2015년08월03일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *H03M 13/00* (2006.01)
(21) 출원번호 10-2014-0008851
(22) 출원일자 2014년01월24일
심사청구일자 2014년01월24일

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
윤성식
서울특별시 성북구 안암로 145 (안암동5가) 고려대학교 전기전자전파공학과
허준
서울특별시 강남구 광평로10길 6 206-103(일원동, 한솔마을아파트)
(74) 대리인
특허법인충현

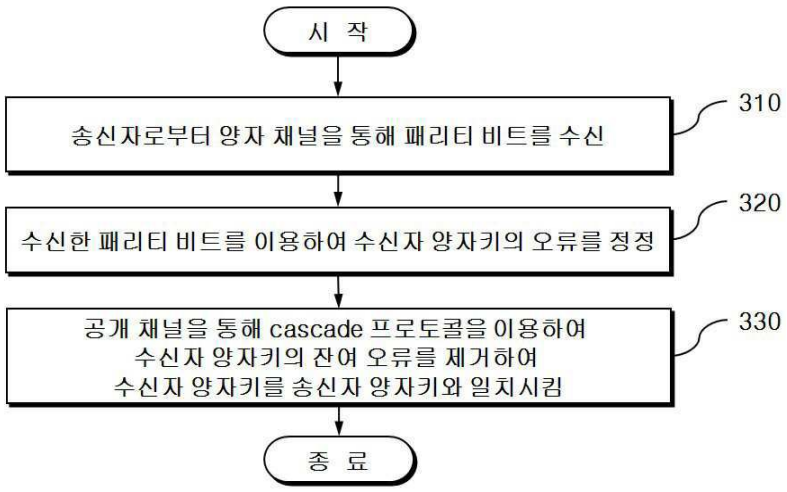
전체 청구항 수 : 총 7 항

(54) 발명의 명칭 **양자 채널을 통한 터보 코드 방식의 효율적인 정보 재건 기법**

(57) 요 약

본 발명은 정보 재건 방법에 관한 것으로서, 송신자와 수신자 간 양자키 분배 시스템에 있어서, 상기 송신자로부터 양자 채널을 통해 패리티 비트를 수신하는 단계, 상기 수신한 패리티 비트를 이용하여 수신자 양자키의 오류를 정정하는 단계, 및 공개 채널을 통해 cascade 프로토콜을 이용하여 상기 수신자 양자키의 잔여 오류를 제거하여 상기 수신자 양자키를 송신자 양자키와 일치시키는 단계를 포함하고, 상기 패리티 비트는 송신자에서 터보 코드를 이용하여 생성된 것을 특징으로 함으로써, 양자키 생성 효율을 높일 수 있다.

대 표 도 - 도3



이 발명을 지원한 국가연구개발사업
과제고유번호 1291104003130010100
부처명 미래창조과학부
연구관리전문기관 한국방송통신전파진흥원
연구사업명 방송통신기술개발사업
연구과제명 양자 통신 및 양자 정보 처리를 위한 기반 기술 개발
기 여 율 1/1
주관기관 고려대학교 산학협력단
연구기간 2013.03.01 ~ 2014.02.28

명 세 서

청구범위

청구항 1

송신자와 수신자 간 양자키 분배 시스템에 있어서,

터보 코드를 이용하여 송신자 양자키로부터 패리티 비트를 생성하는 단계; 및

상기 생성된 패리티 비트를 양자채널을 통해 상기 수신자에게 전송하는 단계를 포함하고,

상기 패리티 비트는 수신자가 수신자 양자키의 오류를 정정하는데 이용되는 것을 특징으로 하는 정보 재건(information reconciliation) 방법.

청구항 2

제 1 항에 있어서,

상기 패리티 비트는,

상기 수신자와 상기 송신자가 공유하는 랜덤 기저 열로부터 생성된 포톤(photon) 기저 열을 이용하여 포톤의 형태로 생성되는 것을 특징으로 하는 정보 재건 방법.

청구항 3

제 2 항에 있어서,

상기 랜덤 기저 열은,

보안이 보장된 이진 비트열로, 비트 값에 따라 포톤 기저 열로 대응되는 것을 특징으로 하는 정보 재건 방법.

청구항 4

제 1 항에 있어서,

상기 수신자 양자키는,

상기 패리티 비트에 의해 오류를 정정하고, 공개 채널을 통해 cascade 프로토콜을 이용하여 상기 수신자 양자키의 잔여 오류를 제거하여 상기 수신자 양자키를 상기 송신자 양자키와 일치시키는 것을 특징으로 하는 정보 재건 방법.

청구항 5

송신자와 수신자 간 양자키 분배 시스템에 있어서,

상기 송신자로부터 양자 채널을 통해 패리티 비트를 수신하는 단계;

상기 수신한 패리티 비트를 이용하여 수신자 양자키의 오류를 정정하는 단계; 및

공개 채널을 통해 cascade 프로토콜을 이용하여 상기 수신자 양자키의 잔여 오류를 제거하여 상기 수신자 양자키를 송신자 양자키와 일치시키는 단계를 포함하고,

상기 패리티 비트는 송신자에서 터보 코드를 이용하여 생성된 것을 특징으로 하는 정보 재건(information reconciliation) 방법.

청구항 6

제 5 항에 있어서,

상기 패리티 비트는,

상기 수신자와 상기 송신자가 공유하는 랜덤 기저 열로부터 생성된 포톤(photon) 기저 열을 이용하여 송신자에

의해 포톤의 형태로 생성되는 것을 특징으로 하는 정보 재건 방법.

청구항 7

제 6 항에 있어서,

상기 랜덤 기저 열은,

보안이 보장된 이진 비트열로, 비트 값에 따라 포톤 기저 열로 대응되는 것을 특징으로 하는 정보 재건 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 양자키 시스템에 있어서, 정보를 재건하는 방법에 관한 것으로서, 더욱 상세하게는 양자 채널을 통한 터보 코드 방식을 이용하여 정보를 재건하는 방법에 관한 것이다.

배 경 기 술

[0002] 양자키 분배 이론은 양자 채널과 공개 채널, 이렇게 두 가지 채널을 사용하여 보안키 분배하는 것으로 크게 네 가지 과정을 통해 이루어진다. 이는 양자 전송, 정보 재건, 비밀성 증폭, 그리고 입증 단계로 구성된다. 양자 전송 단계는 양자 채널을 통해 포톤 형태의 보안키를 전송한다. 이 과정에서 송수신자는 도청자의 도청 유무를 감지하여 그 영향력을 최소할 수 있고, 수신자는 양자 채널 오류율의 영향을 받은 양자키를 수신하게 된다. 그리고 정보 재건은 공개 채널을 통해 이루어지며 수신자의 양자키에 오류를 정정하여 송신자의 양자키와 동일한 이진 비트열을 갖도록 한다. 공개 채널은 오류가 발생하지 않는 무오류 채널(noiseless channel)이고 도청자가 악의적인 영향력을 행사할 수 없는 채널로 가정하지만, 모든 과정이 공개적으로 이루어지기 때문에 도청자 또한 양자키에 관한 정보를 얻을 수 있다. 비밀성 증폭은 이전 과정에서 도청자의 의해 누수 된 정보를 제거하여 양자키의 보안성을 강화하는 단계이다. 이 과정을 통해 도청자의 영향력에 비례하여 양자키의 길이는 줄어든다. 그리고 입증 단계는 이전 모든 단계에서 함께 수행되어야 하는 것으로, 양자키 생성 과정에서 도청자와 같은 제 3자가 아닌 약속된 송수신자를 통해 이루어지는지 여부를 확인하는 것을 의미한다.

[0003] 양자 전송 과정에서는 BB84와 같은 기법을 이용하여 양자 역학적 특성을 통해 도청자의 영향력을 확률적으로 최소화함과 동시에, 고전 보안통신 기법에 비하여 안전하게 키 정보 전송 과정을 수행할 수 있다. 그러나 공개 채널을 통한 정보 재건 과정에서는 사용된 프로토콜에 따라 누수 되는 정보양이 달라지며, 공개 채널 사용수 또한 양자키 생성율에 큰 영향을 끼친다. 지금까지 연구된 대표적인 정보 재건 기법으로는 우선 양방향 방식의 Cascade 프로토콜과 Winnow 프로토콜이 있다. Cascade 프로토콜은 이진 검색 기법을 사용하여 오류를 정정하며 복잡도가 낮은 장점이 있지만, 공개 채널이 과도하게 사용되어 지연문제가 크게 발생하는 문제점이 있다. 그리고 Winnow 프로토콜은 hamming codes를 이용하여 오류를 정정하며 Cascade 프로토콜의 지연 문제를 어느 정도 완화시켰지만, 오류정정 과정이 비효율적으로 이루어진다는 한계점이 있다. 다음으로 이러한 양방향 방식의 정보 재건 기법들의 단점을 보완하기 위하여 단방향 방식의 기법들이 연구되었으며, 대표적으로 LDPC codes를 이용한 정보 재건 프로토콜이 있다. 이것은 최소한의 공개 채널 사용을 통해 오류를 고칠 수 있으며, 높은 성능의 오류정정 능력을 가지고 있다. 그러나 오류 정정을 수행하는데 있어 양자 채널 오류율에 관계없이 고정된 정보의 누수가 발생하기 때문에 낮은 오류율의 양자 채널 상황에서 불필요한 정보의 누수가 생기며, 반대로 높은 오류율 상황에서 오류정정 능력이 충분하지 못해 오류정정을 실패한다는 단점도 있다.

[0004] 본 발명과 관련된 문헌은 다음과 같다.

[0005] [문헌 1] C. Berrou, A. Glavieux, P. Thitimajshima, “Near shannon limit error correction coding and decoding: Turbo codes. 1”, In proc. IEEE Int‘l Conf. on computers, pp.1064- 1070, May.1993.

[0006] 참고문헌에서는 터보 코드의 인코딩, 디코딩 과정의 구조를 제안하고 있다. 그리고 터보 코드는 LDPC 코드와 더불어 다른 오류정정 기법에 비해 우수한 오류정정 능력을 보임을 밝혔다.

[0007] [문헌 2] C. H. Bennett and G. Brasard, “Quantum cryptography: Public key distribution and coin tossing,” in Proc. IEEE Int’l Conf. on Computers, Systems and Signal, 1984, pp. 175?179.

[0008] 참고문헌에서는 양자키 분배 이론에 관한 기본적인 개념을 정립하고 과정 중 양자 포톤을 전송하는 BB84 기법에 관한 연구 결과를 보여준다.

[0009] [문헌 3] G. Brasard, L. Salail, “Secret key reconciliation by public discussion,” in Proc. Eurocypt, 1994, pp.410- 423.

[0010] 참고문헌에서는 공개 논의 과정에서 사용되는 Cascade 프로토콜을 제안하고 있다. 이 방식은 이진 검색 기법을 사용하여 양자 키의 오류를 정정하는 기법이다.

[0011] [문헌 4] W. T. Buttler, S. K. Lamoreaux, J. R. Torgerson, G. H. Nickel, C. H. Donahue, and C. G. Peterson, “Fast, efficient error reconciliation for quantum cryptography,” Phys. Rev. A, vol. 67, no. 052303, pp. 1?8, May.2003.

[0012] 참고문헌에서는 공개 논의 과정에서 사용되는 Winnow 프로토콜을 제안하고 있다. 이 기법은 Cascade와 마찬가지로 양방향 방식의 프로토콜로써 hamming codes를 이용하여 오류를 정정하며, Cascade 프로토콜의 문제점인 지연 문제를 완화시키는 성과를 보였다.

[0013] [문헌 5] A. D. Liveris, Z. Xiong, and C. N. Georghiades, “Compression of binary soueces with side information at the decoder using LDPC codes,” IEEE Commun. Lett., vol. 6, no. 10, pp. 440?442, Oct. 2002.

[0014] 참고문헌에서는 LDPC 코드를 이용한 정보재건 프로토콜을 제안하고 있다. 이 기법은 단방향 방식의 프로토콜로써 LDPC 코드의 syndrome 정보를 이용하여 오류 비트에 관한 정보를 얻고, 이를 바탕으로 오류정정 과정을 수행한다.

[0015] [문헌 6] W. Y. Hwang, I. G. Koh, and Y. D. Han, “Qunatum cryptography without announcement of bases,” Phys. Lett. A, vol. 224, pp. 489- 494, Aug. 2003.

[0016] 참고문헌에서는 양자키 확장 이론의 원리와 그 효과에 대한 분석이 되어있다. 송수신자는 이 방식을 이용하여 원하는 만큼 양자키의 크기를 확장함과 동시에 양자키 생성 효율을 높일 수 있음을 보였다.

발명의 내용

해결하려는 과제

[0017] 본 발명이 해결하고자 하는 과제는 양자 채널을 통한 터보 코드 방식을 이용하여 정보를 재건하는 방법을 제공하는 것이다.

과제의 해결 수단

[0018] 본 발명은 상기 과제를 달성하기 위하여, 송신자와 수신자 간 양자키 분배 시스템에 있어서, 터보 코드를 이용하여 송신자 양자키로부터 패리티 비트를 생성하는 단계; 및 상기 생성된 패리티 비트를 양자채널을 통해 상기 수신자에게 전송하는 단계를 포함하고, 상기 패리티 비트는 수신자가 수신자 양자키의 오류를 정정하는데 이용되는 것을 특징으로 하는 정보 재건(information reconciliation) 방법을 제공한다.

[0019] 본 발명의 실시예에 의하면, 상기 패리티 비트는, 상기 수신자와 상기 송신자가 공유하는 랜덤 기저 열로부터 생성된 포톤(photon) 기저 열을 이용하여 포톤의 형태로 생성되는 것을 특징으로 하는 정보 재건 방법일 수 있다.

[0020] 본 발명의 실시예에 의하면, 상기 랜덤 기저 열은, 보안이 보장된 이진 비트열로, 비트 값에 따라 포톤 기저 열로 대응되는 것을 특징으로 하는 정보 재건 방법일 수 있다.

[0021] 본 발명의 실시예에 의하면, 상기 수신자 양자키는, 상기 패리티 비트에 의해 오류를 정정하고, 공개 채널을 통해 cascade 프로토콜을 이용하여 상기 수신자 양자키의 잔여 오류를 제거하여 상기 수신자 양자키를 상기 송신자 양자키와 일치시키는 것을 특징으로 하는 정보 재건 방법일 수 있다.

[0022] 본 발명은 상기 과제를 달성하기 위하여, 송신자와 수신자 간 양자키 분배 시스템에 있어서, 상기 송신자로부터 양자 채널을 통해 패리티 비트를 수신하는 단계; 상기 수신한 패리티 비트를 이용하여 수신자 양자키의 오류를 정정하는 단계; 및 공개 채널을 통해 cascade 프로토콜을 이용하여 상기 수신자 양자키의 잔여 오류를 제거하여 상기 수신자 양자키를 송신자 양자키와 일치시키는 단계를 포함하고, 상기 패리티 비트는 송신자에서 터보 코드를 이용하여 생성된 것을 특징으로 하는 정보 재건 방법을 제공한다.

[0023] 본 발명의 실시예에 의하면, 상기 패리티 비트는, 상기 수신자와 상기 송신자가 공유하는 랜덤 기저 열로부터 생성된 포톤(photon) 기저 열을 이용하여 송신자에 의해 포톤의 형태로 생성되는 것을 특징으로 하는 정보 재건 방법일 수 있다.

발명의 효과

[0024] 본 발명에 따르면, 양자키 분배 과정에서 보다 진보된 방식의 정보 재건 기법을 적용하여 양자키 생성 효율을 높일 수 있다. 이는 기존의 정보 재건 기법에서 공개 채널만을 사용하는 것과는 다르게 도청자의 악의적인 영향력을 감지하고 예방할 수 있는 양자 채널 또한 오류 정정을 위한 채널로 사용함으로써 양자키의 정보 누수를 막을 수 있다. 누수 되는 양자키 정보의 양을 최소화 하고, 지연 문제를 또한 해결할 수 있다.

도면의 간단한 설명

[0025] 도 1은 본 발명의 실시예에 따른 정보 재건 방법이 적용된 양자키 분배 시스템의 블록도이다.

도 2는 본 발명의 일 실시예에 따른 정보 재건 방법의 송신자에서 흐름도이다.

도 3은 본 발명의 일 실시예에 따른 정보 재건 방법의 수신자에서 흐름도이다.

도 4는 본 발명의 실시예에 따른 정보 재건 방법이 적용된 시스템 모델이다.

도 5는 본 발명의 실시예에 따른 정보 재건 방법에서 고려하는 터보 인코더 구조이다.

도 6은 본 발명의 실시예에 따른 정보 재건 방법에서 고려하는 터보 디코더 구조이다.

도 7은 본 발명의 실시예에 따른 정보 재건 방법에서 사용된 랜덤 기저 열을 통한 포톤 생성 원리를 도시한 것이다.

도 8은 본 발명의 실시예에 따른 정보 재건 방법에서 적용된 터보 코드의 iteration 따른 오류정정 능력을 도시한 것이다.

도 9는 터보 코드를 이용한 오류정정 후, 수신자 양자키의 오류율 변화를 도시한 것이다.

도 10은 Cascade 프로토콜을 단독으로 사용할 경우와 제안된 기법을 사용할 경우 노출되는 양자키 비트의 비율을 도시한 것이다.

발명을 실시하기 위한 구체적인 내용

[0026] 본 발명에 관한 구체적인 내용의 설명에 앞서 이해의 편의를 위해 본 발명이 해결하고자 하는 과제의 해결 방안의 개요 혹은 기술적 사상의 핵심을 우선 제시한다.

[0027] 본 발명의 일 실시예에 따른 정보 재건 방법은 송신자와 수신자 간 양자키 분배 시스템에 있어서, 상기 송신자로부터 양자 채널을 통해 패리티 비트를 수신하는 단계, 상기 수신한 패리티 비트를 이용하여 수신자 양자키의 오류를 정정하는 단계, 및 공개 채널을 통해 cascade 프로토콜을 이용하여 상기 수신자 양자키의 잔여 오류를 제거하여 상기 수신자 양자키를 송신자 양자키와 일치시키는 단계를 포함하고, 상기 패리티 비트는 송신자에서 터보 코드를 이용하여 생성된 것을 특징으로 한다.

[0028] 이하 첨부된 도면을 참조하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 본 발명을 용이하게 실시할 수 있는 실시 예를 상세히 설명한다. 그러나 이들 실시예는 본 발명을 보다 구체적으로 설명하기 위한 것으로, 본 발명의 범위가 이에 의하여 제한되지 않는다는 것은 당업계의 통상의 지식을 가진 자에게 자명할 것이다.

[0029] 본 발명이 해결하고자 하는 과제의 해결 방안을 명확하게 하기 위한 발명의 구성을 본 발명의 바람직한 실시예에 근거하여 첨부 도면을 참조하여 상세히 설명하되, 도면의 구성요소들에 참조번호를 부여함에 있어서 동일 구성요소에 대해서는 비록 다른 도면상에 있더라도 동일 참조번호를 부여하였으며 당해 도면에 대한 설명시 필요한 경우 다른 도면의 구성요소를 인용할 수 있음을 미리 밝혀둔다. 아울러 본 발명의 바람직한 실시 예에 대한 동작 원리를 상세하게 설명함에 있어 본 발명과 관련된 공지 기능 혹은 구성에 대한 구체적인 설명 그리고 그 이외의 제반 사항이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우, 그 상세한 설명을 생략한다.

[0030] 도 1은 본 발명의 실시예에 따른 정보 재건 방법이 적용된 양자키 분배 시스템의 블록도이다.

[0031] 본 발명의 일 실시예에 따른 정보 재건 방법이 적용된 양자키 분배 시스템(100)은 송신자(110), 수신자(120), 양자채널(130), 및 공개채널(140)로 구성된다.

[0032] 효율적인 정보 재건을 위하여, 송신자(110)와 수신자(120)는 양자채널(130)을 통해 터보 코드를 이용하여 생성된 패리티 비트를 송수신하여 오류를 정정하고, 공개채널(140)을 통해 공개 논의(public discussion)을 통해 잔여 오류를 제거하여 정보를 재건(information reconciliation)한다. 즉, 공개채널(140)뿐만 아니라 양자채널(130) 또한 오류정정 과정을 수행하는데 사용하여 양자키 생성의 효율을 높인다. 본 발명에서 제안하는 정보 재건의 시스템 모델은 도 4와 같이, 크게 두 단계의 과정으로 구성되어 있다. 첫 번째 과정은 양자 채널을 사용한 오류정정 단계이고 두 번째 과정은 공개 채널을 이용한 공개 논의 과정에서의 정보 재건 과정이다.

[0033] 첫 번째 오류정정 과정에서는 터보 코드를 적용하였다. 기존의 터보 코드를 이용한 정보 재건 기법은 단방향 방식의 우수한 오류정정 능력을 가진 기법이지만, 패리티 정보를 전송하는 과정에서 막대한 양의 양자키 정보 누수로 인해 실용적인 관점에서 한계가 있었다. 그러나 본 발명 일 실시예에 따른 정보 재건에서는 양자 채널을 통하여 패리티 정보를 전송함으로써 누수 되는 양자키 정보의 양을 최소화하였다.

[0034] 도 5와 도 6은 터보코드를 이용한 오류정정 과정의 송수신단 구조를 보여준다.

[0035] 도 5는 터보코드 인코더 부분으로써 그 구조는 기존의 고전 통신 시스템에서 사용한 것과 동일한 구조로 구성되어 있다. 인코더 입력 값은 구별되는 두 개의 convolutional 인코더로 들어가게 되며, 이때 한쪽은 입력 값이 그대로 들어가고 다른 한쪽은 interleaving 과정을 거친 후 들어가게 된다. 그리고 출력 부분에서는 두 가지 출력이 나오게 되고 이것은 첫째, 입력 값과 동일한 systematic bit sequence 그리고 둘째, 두 convolutional 인코더 출력에 puncturing 과정을 거쳐서 만들어낸 parity bit sequence로 이루어져 있다. 이때 기존의 고전 통신 시스템에서 사용된 터보 인코더에서는 message bit sequence가 입력 값으로 들어가서 두 가지 출력을 만들게 되고, 이 두 가지 출력을 조합하여 무선채널을 통하여 수신자에게 전송하게 된다. 그러나 본 발명의 실시예에서는 입력 값이 송신자의 걸러진 키를 사용하게 된다. 그리고 출력단에서 생성하는 두 가지 bit sequence 중에서 오직 parity bit sequence만을 사용하여 양자 채널을 통해 수신자에게 전달하게 된다. 이때 이러한 parity bit sequence는 수신자 보안키의 오류를 정정하는 목적으로 사용된다.

[0036] 도 6은 터보 코드의 디코더 부분으로써 그 구조는 인코더와 마찬가지로 고전 통신 시스템에서 사용한 것과 동일한 구조로 구성되어 있다. 입력단에는 두 가지 정보가 입력으로 들어가게 되고 이것을 서로 다른 2-state decoder를 이용하여 확률적으로 오류를 정정하게 된다. 그리고 이 구조는 피드백 루프를 가지고 있으며 루프를 반복적으로 수행함으로써 더욱 큰 신뢰성을 가지고 오류를 고칠 수 있게 된다. 기존의 터보 디코더에서는 전송되어 온 인코딩 된 codeword를 두 부분으로 나누어서 디코더의 입력 부분에 각각 넣어주게 되고 송신자가 전송하고자 했던 message를 복원하게 된다. 그러나 본 발명의 실시예에서는 이전과는 다른 방식을 사용한다. 두 가지의 입력 정보로는 첫째, 수신자가 가지고 있는, 오류가 내재되어 있는, 걸러진 키를 사용하게 되고 둘째, 양자 채널을 통해 전송된 parity bit sequence를 입력으로 사용하게 된다. 디코딩 과정을 마친 후에는 수신자의 걸러진 키의 오류를 정정하게 된다.

[0037] 만일 오류정정 과정에서 송수신자가 서로 다른 양자 측정 기저를 가지고 있다면, BB84 프로토콜과 마찬가지로 전송 후 서로의 양자 측정 기저를 비교하는 과정을 반드시 수행해야만 한다. 송수신자는 두 가지 측정 기저를 랜덤하게 생성하여 이를 기반으로 양자키 정보를 인코딩하여 전송하게 되는데, 이때 확률적으로 약 50%의 양자 측정 기저는 동일한 기저를 사용하지만 나머지 50%는 서로 다른 기저를 사용할 가능성이 있다. 따라서 기저가 일치하지 않는 50%의 포톤은 양자 역학적 원리에 의하여 사용할 수 없게 된다. 이를 해결하기 위해 송수신자가 동일한 양자 측정 기저를 사용할 수 있도록 랜덤 기저 열을 공유한다. 랜덤 기저 열은 보안이 보장된 이진 비트 열을 의미하며, 비트 값에 따라 Z 또는 X 기저로 대응시킬 수 있다. 이렇게 생성된 양자 포톤 기저를 바탕으로 수신자에게 패리티 정보를 효율적으로 전송할 수 있으며, 포톤 생성 과정은 도 7과 같다. 이때 전송되는 패리티 정보는 양자 채널을 통해 전송이 되기 때문에 양자 채널 오류율의 영향을 받아 일부 오류 비트를 가지고 수신된다. 따라서 공개 채널을 사용하여 전송된 정보를 이용하여 오류정정을 수행할 경우와 비교하여 약간의 오류정정 능력의 성능 열화가 존재하지만 시뮬레이션 분석을 통해 목표치를 달성하는데 충분함을 확인하였다. 도 8은 iteration 횟수에 따른 터보 코드 방식의 오류정정 능력을 보여준다. 그리고 도 9는 첫 번째 오류정정을 마치고 난 후의 수신자 양자키의 오류율을 의미한다. 분석 결과, 양자 채널 오류율에 따라 약 2.5~100배까지 오류율이 감소하였음을 알 수 있다.

[0038] 첫 번째 오류정정 과정을 완료한 후, 두 번째 과정으로 공개 채널을 이용한 공개 논의 과정을 수행해야만 한다. 이는 첫 번째 과정에서 터보 코드의 우수한 오류정정 능력에도 불구하고, 수신자의 양자키에는 잔여 오류가 남아 있을 확률이 존재한다. 게다가 잔여 오류가 없도록 모든 오류를 정정했다 하더라도 그 확인을 위한 공개 논의 과정은 필수적이다. 본 발명에서는 양방향 방식의 cascade를 이용하여 잔여 오류를 제거한다. 다른 정보 재건 프로토콜을 이용할 수도 있다. Cascade 프로토콜은 지연 문제를 야기한다는 단점이 있지만 양자키 생성 효율이 우수한 기법으로, 양자키 비트열을 작은 크기의 블록 단위로 나누어 블록 단위 오류정정을 수행한다. 블록의 크기는 N=0.73/e으로 설정하고 이때 e는 양자 채널 오류율, 즉 수신자 양자키의 비트 오류율을 의미한다. 따라서 수신자 양자키의 오류율이 크게 감소하였기 때문에 보다 큰 크기의 블록을 통하여 오류를 정정할 수 있으며, 공개 채널 사용횟수 또한 크게 감소시킬 수 있다. 도 10은 기존의 방식대로 Cascade 프로토콜을 단독으로 사용했을 경우의 노출되는 양자키 비트의 비율과 제안된 프로토콜을 사용하였을 경우의 노출되는 양자키 비트의 비율을 비교한 결과이다.

[0039] 송신자는 상기 구성을 수행하기 위하여, 송신자 양자키로부터 패리티 비트를 생성하는 터보 인코더부, 송신자 양자키를 저장하는 저장부, 및 상기 생성된 패리티 비트를 수신자에 송신하는 통신부를 포함할 수 있고, 수신자는 송신자로부터 패리티 비트를 수신하는 통신부, 상기 패리티 비트를 이용하여 수신자 양자키의 오류를 정정하는 오류정정부, 및 공개채널의 cascade 프로토콜을 이용하여 공개논의를 통해 정보를 재건하는 정보재건부를 포함할 수 있다. 송신자(110)와 수신자(120)에서 정보를 재건하기 위하여 수행하는 구체적인 구성은 도 2 내지 도 3에서 자세히 다루도록 한다.

[0040] 도 2는 본 발명의 일 실시예에 따른 정보 재건 방법의 송신자에서 흐름도이다.

[0041] 210단계는 터보 코드를 이용하여 송신자 양자키로부터 패리티 비트를 생성하는 단계이다.

[0042] 보다 구체적으로, 터보 코드를 이용하여 송신자 양자키로부터 패리티 비트를 생성한다. 상기 송신자 양자키는 sifted key이다. 상기 패리티 비트는 상기 수신자와 상기 송신자가 공유하는 랜덤 기저 열로부터 생성된 포톤(photon) 기저 열을 이용하여 포톤의 형태로 생성된다. 상기 랜덤 기저 열은 보안이 보장된 이진 비트열로, 비트 값에 따라 포톤 기저 열로 대응된다. 도 5와 같이, 송신자의 양자키로부터 터보 코드를 이용하여 패리티 비트를 생성한다. 상기 생성된 패리티 비트는 도 7과 같이 포톤 형태로 생성된다. 즉, 랜덤 기저 열(Bases random sequence)을 인코딩하여 포톤 기저 열(photon bases)를 생성하고, 상기 생성된 포톤 기저 열을 이용하여 패리티 신호를 포톤의 형태로 생성한다.

[0043] 220 단계는 상기 생성된 패리티 비트를 양자채널을 통해 상기 수신자에게 전송하는 단계이다.

[0044] 보다 구체적으로, 210단계에서 생성된 패리티 비트를 수신자에게 전송한다. 상기 패리티 비트는 수신자가 수신자 양자키의 오류를 정정하는데 이용된다. 상기 수신자 양자키는 상기 패리티 비트에 의해 오류를 정정하고, 공개 채널을 통해 cascade 프로토콜을 이용하여 상기 수신자 양자키의 잔여 오류를 제거하여 상기 수신자 양자키를 상기 송신자 양자키와 일치시킨다.

[0045] 도 3은 본 발명의 일 실시예에 따른 정보 재건 방법의 수신자에서 흐름도이다.

[0046] 310단계는 상기 송신자로부터 양자 채널을 통해 패리티 비트를 수신하는 단계이다.

[0047] 보다 구체적으로, 송신자로부터 공개 채널이 아닌 양자 채널을 통해 패리티 비트를 수신한다. 상기 패리티 비트는 송신자에서 터보 코드를 이용하여 생성된다.

[0048] 상기 패리티 비트는 상기 수신자와 상기 송신자가 공유하는 랜덤 기저 열로부터 생성된 포톤(photon) 기저 열을 이용하여 송신자에 의해 포톤의 형태로 생성된다. 상기 랜덤 기저 열은, 보안이 보장된 이진 비트열로, 비트 값에 따라 포톤 기저 열로 대응된다.

[0049] 320단계는 상기 수신한 패리티 비트를 이용하여 수신자 양자키의 오류를 정정하는 단계이다.

[0050] 보다 구체적으로, 310단계에서 수신한 패리티 비트를 터보 코드를 이용하여 수신자 양자키의 오류를 정정한다. 송신자에서 터보 코드를 이용하여 인코딩된 패리티 비트를 수신자에서 터보 코드를 이용하여 디코딩함으로써 수신자 양자키의 오류를 정정한다. 상기 수신자 양자키는 sifted key이다.

[0051] 330단계는 공개 채널을 통해 cascade 프로토콜을 이용하여 상기 수신자 양자키의 잔여 오류를 제거하여 상기 수신자 양자키를 송신자 양자키와 일치시키는 단계이다.

[0052] 보다 구체적으로, 320단계에서 오류를 정정함에 있어서, 모든 오류가 제거되지 않는바, 공개 채널을 통해 cascade 프로토콜을 이용하여 상기 수신자 양자키의 잔여 오류를 제거하여 상기 수신자 양자키를 송신자 양자키와 일치시킴으로써 정보재건을 수행한다.

[0053] 본 발명의 실시예들은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 본 발명의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0054] 이상과 같이 본 발명에서는 구체적인 구성 요소 등과 같은 특정 사항들과 한정된 실시예 및 도면에 의해 설명되었으나 이는 본 발명의 보다 전반적인 이해를 돕기 위해서 제공된 것일 뿐, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상적인 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다.

[0055] 따라서, 본 발명의 사상은 설명된 실시예에 국한되어 정해져서는 아니되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등하거나 등가적 변형이 있는 모든 것들은 본 발명 사상의 범주에 속한다고 할 것이다.

부호의 설명

[0056] 100: 양자키 분배 시스템

110, 410: 송신자

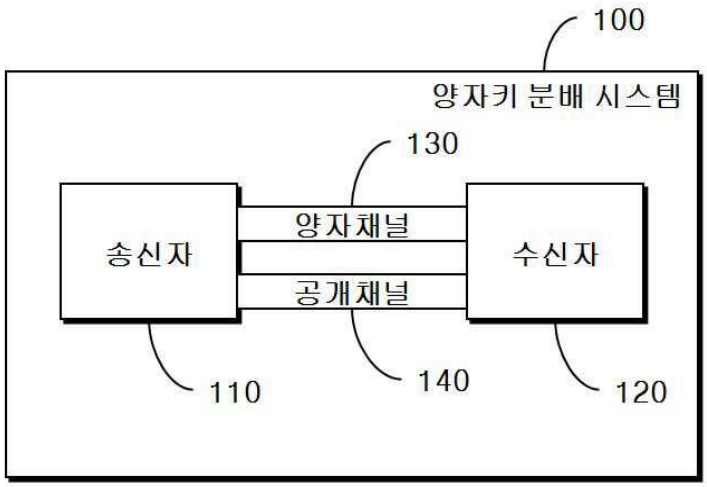
120, 420: 수신자

130, 430: 양자채널

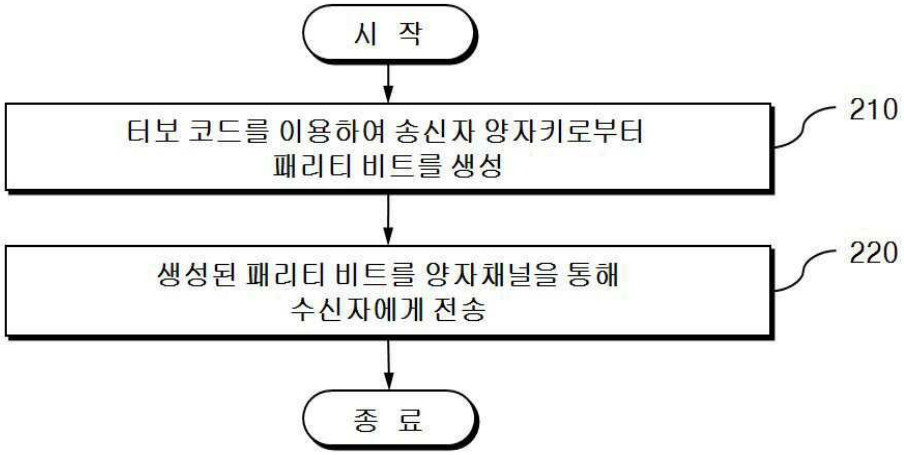
140, 440: 공개채널

도면

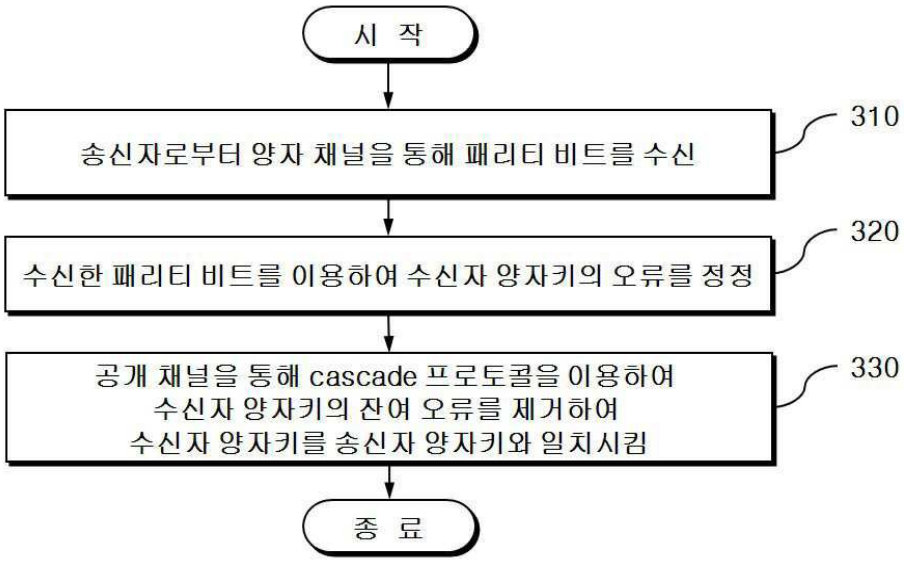
도면1


100
양자키 분배 시스템
130
송신자
양자채널
공개채널
수신자
110
140
120

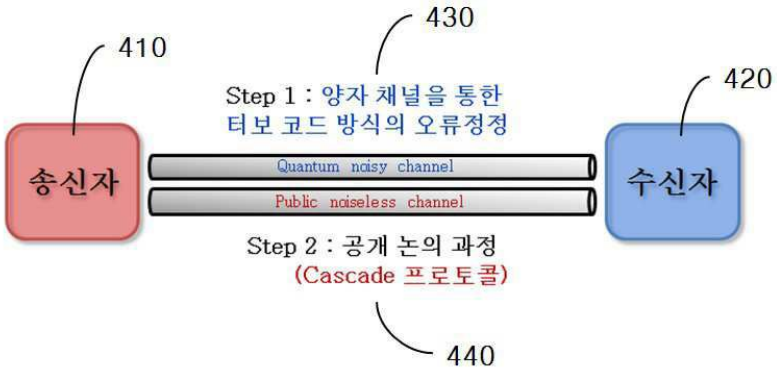
도면2


시 작
터보 코드를 이용하여 송신자 양자키로부터
패리티 비트를 생성
210
생성된 패리티 비트를 양자채널을 통해
수신자에게 전송
220
종 료

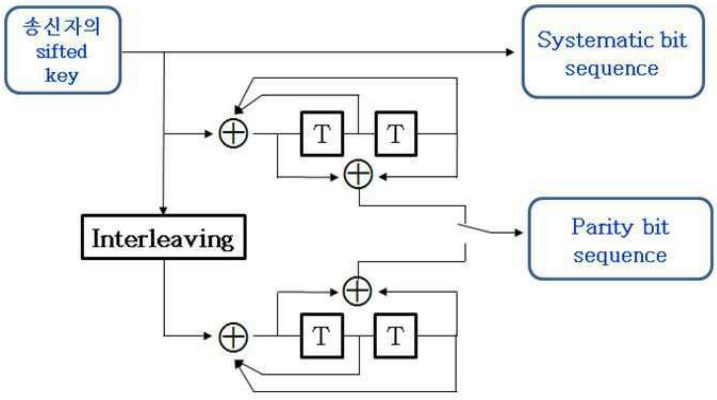
도면3


시 작
송신자로부터 양자 채널을 통해 패리티 비트를 수신
310
수신한 패리티 비트를 이용하여 수신자 양자키의 오류를 정정
320
공개 채널을 통해 cascade 프로토콜을 이용하여
수신자 양자키의 잔여 오류를 제거하여
수신자 양자키를 송신자 양자키와 일치시킴
330
종 료

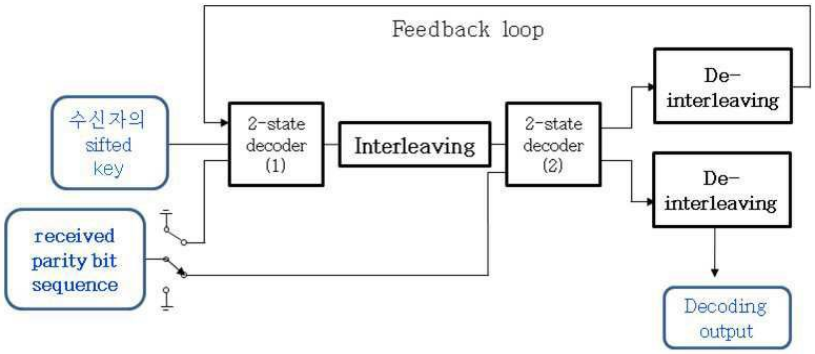
도면4


410
430
420
Step 1 : 양자 채널을 통한
터보 코드 방식의 오류정정
송신자
Quantum noisy channel
Public noiseless channel
수신자
Step 2 : 공개 논의 과정
(Cascade 프로토콜)
440

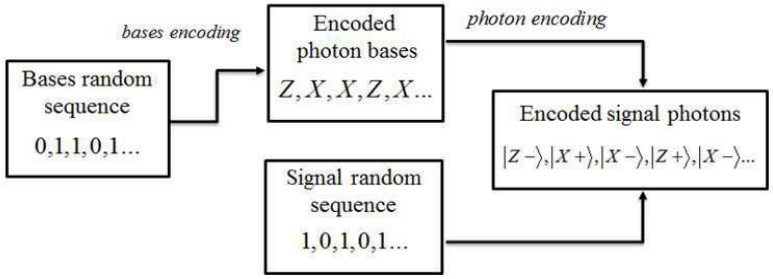
도면5


송신자의
sifted
key
Systematic bit
sequence
T
T
Interleaving
Parity bit
sequence
T
T

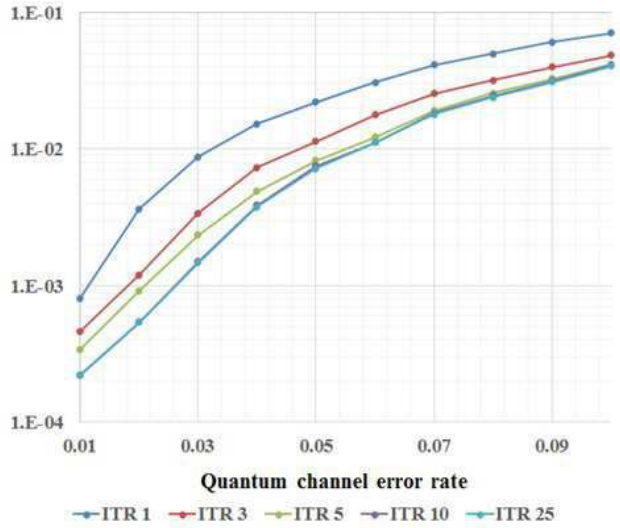
도면6


Feedback loop
수신자의 sifted key
2-state decoder (1)
Interleaving
2-state decoder (2)
De-interleaving
De-interleaving
received parity bit sequence
Decoding output

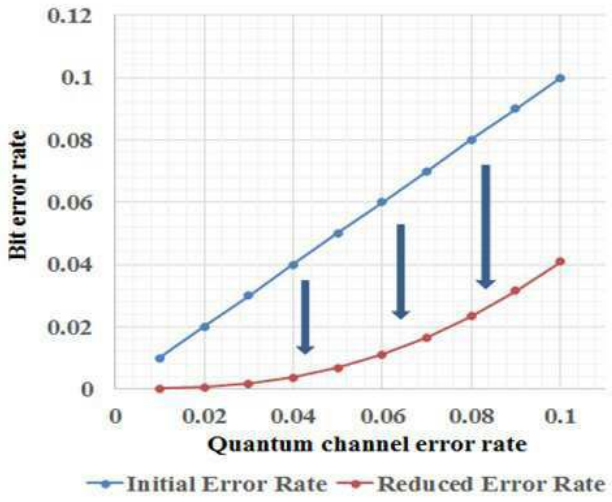
도면7


bases encoding
Encoded photon bases
$Z,X,X,Z,X...$
photon encoding
Bases random sequence
0,1,1,0,1...
Encoded signal photons
$|Z-\rangle,|X+\rangle,|X-\rangle,|Z+\rangle,|X-\rangle...$
Signal random sequence
1,0,1,0,1...

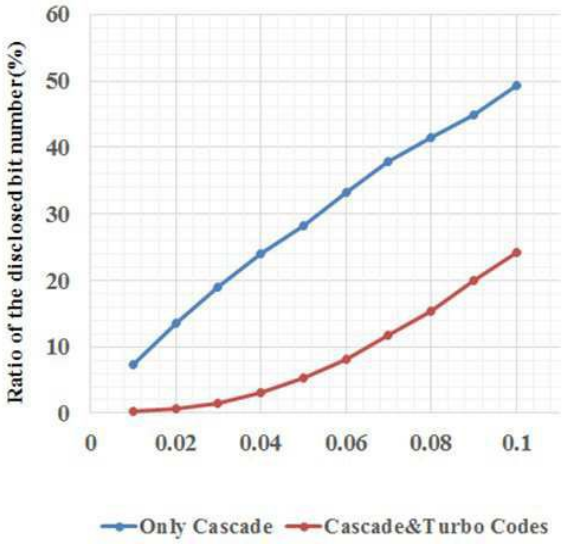
도면8


1.E-01
1.E-02
1.E-03
1.E-04
0.01
0.03
0.05
0.07
0.09
Quantum channel error rate
ITR 1
ITR 3
ITR 5
ITR 10
ITR 25

도면9


0.12
0.1
0.08
0.06
0.04
0.02
0
Bit error rate
0
0.02
0.04
0.06
0.08
0.1
Quantum channel error rate
Initial Error Rate
Reduced Error Rate

도면10


60
50
40
30
20
10
0
Ratio of the disclosed bit number(%)
0
0.02
0.04
0.06
0.08
0.1
Only Cascade
Cascade&Turbo Codes