(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2015년05월06일
(11) 등록번호 10-1517361
(24) 등록일자 2015년04월28일

(51) 국제특허분류(Int. Cl.)
H03M 13/00 (2006.01)
(21) 출원번호 10-2014-0008850
(22) 출원일자 2014년01월24일
심사청구일자 2014년01월24일
(56) 선행기술조사문헌
KR101233860 B1
JP5227942 B2
KR100631242 B1

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

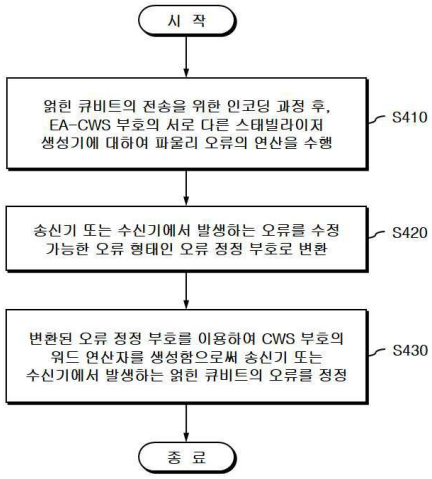
전체 청구항 수 : 총 5 항 심사관 : 조춘근

(54) 발명의 명칭 **수신기 측의 불완전한 얽힌 큐비트의 오류를 정정하는 방법**

(57) 요 약

불완전한 얽힌 큐비트의 오류를 정정하는 EA-CWS 양자 오류 정정 부호에 관한 것으로, 송신기 및 수신기가 공유하는 얽힌 큐비트를 이용하여 오류를 정정하는 방법은, 얽힌 큐비트의 전송을 위한 인코딩 과정 후, EA-CWS 부호의 서로 다른 스태빌라이저 생성기에 대하여 파울리(Pauli) 오류의 연산을 수행하고, 연산 결과 송신기 또는 수신기에서 발생하는 오류를 수정 가능한 오류 형태인 오류 정정 부호로 변환하며, 변환된 오류 정정 부호를 이용하여 CWS 부호의 워드 연산자를 생성함으로써 송신기 또는 수신기에서 발생하는 얽힌 큐비트의 오류를 정정한다.

대 표 도 - 도4



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

송신기 및 수신기가 공유하는 얽힌 큐비트(entangled qubit: ebit)를 이용하여 오류를 정정하는 방법에 있어서,

상기 송신기가 EA-CWS(entanglement assisted codeword stabilized quantum) 부호를 이용하여 채널 상에서 발생하는 오류를 정정하는 단계; 및

상기 수신기가 스태빌라이저(stabilizer) 부호를 이용하여 수신된 얽힌 큐비트(entangled qubit: ebit) 상에서 발생하는 오류를 정정하는 단계;를 포함하되,

상기 EA-CWS 부호 및 상기 스태빌라이저 부호의 2개의 오류 정정 부호를 결합하여 컴비네이션(combination) 부호를 형성하는 것을 특징으로 하는 방법.

청구항 2

제 1 항에 있어서,

상기 수신기는,

상기 컴비네이션 부호 내에 포함된 상기 스태빌라이저 부호를 통해, 송신 채널 상에서 발생하는 오류뿐만 아니라, 상기 송신 채널의 통과 후 상기 수신기에서 발생하는 오류를 정정하는 것을 특징으로 하는 방법.

청구항 3

송신기 및 수신기가 공유하는 얽힌 큐비트를 이용하여 오류를 정정하는 방법에 있어서,

얽힌 큐비트의 전송을 위한 인코딩 과정 후, EA-CWS 부호의 서로 다른 스태빌라이저 생성기(stabilizer generator)에 대하여 파울리(Pauli) 오류의 연산을 수행하는 단계;

상기 연산 결과, 상기 송신기 또는 상기 수신기에서 발생하는 오류를 수정 가능한 오류 형태인 오류 정정 부호로 변환하는 단계; 및

상기 변환된 오류 정정 부호를 이용하여 CWS 부호의 워드 연산자(word operator)를 생성함으로써 상기 송신기 또는 상기 수신기에서 발생하는 얽힌 큐비트의 오류를 정정하는 단계;를 포함하는 방법.

청구항 4

제 3 항에 있어서,

상기 서로 다른 스태빌라이저 생성기는 서로 다른 위치의 하나의 큐비트 상에 오류를 나타내는 X 연산자(X operator)를 포함함으로써, 파울리 오류의 연산을 통해 상기 송신기에서 발생하는 단일 오류를 Z 연산자 및 I 연산자만으로 구성되는 유효 오류를 생성하며, 상기 유효 오류를 수정 가능한 이진 오류로 변환하는 것을 특징으로 하는 방법.

청구항 5

제 3 항에 있어서,

상기 송신기 측의 오류와 상기 수신기 측의 오류는 등가 전환 관계를 형성함으로써, 상기 송신기가 다중 오류 정정을 이용하여 상기 수신기 측의 오류를 정정하는 것을 특징으로 하는 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 얽힌 큐비트의 오류를 정정할 수 있는 양자 오류 정정 부호 기술에 관한 것으로서, 특히 송신기와 수

신기가 불완전한 얽힌 큐비트를 공유하는 경우에 송신기뿐만 아니라 수신기 측에서 발생하는 불완전한 얽힌 큐비트의 오류를 정정하는 방법에 관한 것이다.

배 경 기 술

[0002] 양자정보통신(Quantum Information Communication Technology)은 20세기 말에 등장한 새로운 기술로 양자물리학의 원리에 입각하여 정보를 저장, 전송 그리고 처리하는 과정에 관한 테크놀로지로서, 양자물리학과 정보통신기술이 접목되어 형성되었다. 이와 관련하여 전자나 원자, 빛의 입자인 광자를 나노기술로 하나씩 제어할 수 있는 극미소 세계에서는 통상적인 거시 세계에서는 이해하기 어려운 신기한 현상이 일어난다. 입자로서 성질 외에 파동으로서 성질이 현저하게 나타나는 것인데, 이 세계는 양자역학으로만 설명할 수 있다. 양자역학에는 3가지 기본 성질인 중첩(superposition), 얽힘(entanglement) 및 관측을 이용하여 통신이나 정보처리에 이용하는 움직임이 활발하게 추진되고 있는데, 이를 위한 기술이 바로 양자정보기술이다.

[0003] 특히, 최근 들어 이런 특성을 활용해 양자암호통신, 양자프로세서, 양자시뮬레이션, 양자 컴퓨터 등 다양한 적용 대상이 제안되고 있다. 양자정보통신은 기존의 프로세서에서 사용하는 비트 대신에 큐비트(qubit)를 사용한다. 예를 들어, 고전 프로세서에서 10비트는 2의 10승, 즉 1024번의 연산을 차례차례 수행하지만 양자프로세서의 10큐비트는 1024번의 연산을 동시에 수행한다. 즉, 양자컴퓨터는 이런 특징을 이용해 연산 속도를 획기적으로 높일 수 있다.

[0004] 한편, 이러한 양자정보통신의 한 축으로서, 송수신에서의 오류를 정정하는 다양한 기술이 제안되고 있다. 비특허문헌 1에서는 양자 역학적 관점에서의 문제가 해결되어진 오류정정 부호가 가능함을 보이고 이것이 스태빌라이저(stabilizer) 부호라는 고전 오류 정정부호와 유사한 특징을 가진 양자 오류정정부호로 발전됨을 보인다. 또한, 비특허문헌 2에서는 송신자의 큐비트와 수신자의 공유된 큐비트 중 임의의 큐비트에서 발생하는 오류를 정정할 수 있는 얽힘 양자 오류정정부호 기법을 소개하였다.

선행기술문헌

비특허문헌

[0005] (비특허문헌 0001) Gottesman, D.: Ph.D. thesis, Caltech., 1997

(비특허문헌 0002) Shaw, Bilal., Wilde , Mark M., Oreshkov, Ognyan., Kremsky, Isaac., Lidar, Daniel A.:Encoding one logical qubit into six physical qubits., Phys. Rev. A. 78, 012337, 2008

발명의 내용

해결하려는 과제

[0006] 본 발명이 해결하고자 하는 기술적 과제는, 종래의 얽힌 보조 양자 오류 정정 부호에서 수신자 측의 얽힌 큐비트에서는 에러가 발생하지 않는다는 것을 가정함으로써 인하여 실제 상황에서 발생하는 송신자 측의 오류뿐만 아니라 수신자 측의 얽힌 큐비트 상에서 발생하는 오류를 정확히 처리할 수 없는 한계를 극복하고, 이로 인해 기존의 오류 정정 부호를 적용시킬 경우 오류 정정능력이 더욱 저하되는 문제점을 해결하고자 한다.

과제의 해결 수단

[0007] 상기 기술적 과제를 해결하기 위하여, 본 발명의 일 실시예에 따른 송신기 및 수신기가 공유하는 얽힌 큐비트(entangled qubit: ebit)를 이용하여 오류를 정정하는 방법은, 상기 송신기가 EA-CWS(entanglement assisted codeword stabilized quantum) 부호를 이용하여 채널 상에서 발생하는 오류를 정정하는 단계; 및 상기 수신기가 스태빌라이저(stabilizer) 부호를 이용하여 수신된 얽힌 큐비트(entangled qubit: ebit) 상에서 발생하는 오류를 정정하는 단계;를 포함하되, 상기 EA-CWS 부호 및 상기 스태빌라이저 부호의 2개의 오류 정정 부호를 결합하여 컴비네이션(combination) 부호를 형성한다.

[0008] 일 실시예에 따른 상기 오류를 정정하는 방법에서, 상기 수신기는, 상기 컴비네이션 부호 내에 포함된 상기 스태빌라이저 부호를 통해, 송신 채널 상에서 발생하는 오류뿐만 아니라, 상기 송신 채널의 통과 후 상기 수신기에서 발생하는 오류를 정정한다.

[0009] 상기 기술적 과제를 해결하기 위하여, 본 발명의 다른 실시예에 따른 송신기 및 수신기가 공유하는 얽힌 큐비트를 이용하여 오류를 정정하는 방법은, 얽힌 큐비트의 전송을 위한 인코딩 과정 후, EA-CWS 부호의 서로 다른 스태빌라이저 생성기(stabilizer generator)에 대하여 파울리(Pauli) 오류의 연산을 수행하는 단계; 상기 연산 결과, 상기 송신기 또는 상기 수신기에서 발생하는 오류를 수정 가능한 오류 형태인 오류 정정 부호로 변환하는 단계; 및 상기 변환된 오류 정정 부호를 이용하여 CWS 부호의 워드 연산자(word operator)를 생성함으로써 상기 송신기 또는 상기 수신기에서 발생하는 얽힌 큐비트의 오류를 정정하는 단계;를 포함한다.

[0010] 다른 실시예에 따른 상기 오류를 정정하는 방법에서, 상기 서로 다른 스태빌라이저 생성기는 서로 다른 위치의 하나의 큐비트 상에 오류를 나타내는 X 연산자(X operator)를 포함함으로써, 파울리 오류의 연산을 통해 상기 송신기에서 발생하는 단일 오류를 Z 연산자 및 I 연산자만으로 구성되는 유효 오류를 생성하며, 상기 유효 오류를 수정 가능한 이진 오류로 변환한다.

[0011] 다른 실시예에 따른 상기 오류를 정정하는 방법에서, 상기 송신기 측의 오류와 상기 수신기 측의 오류는 등가 전환 관계를 형성함으로써, 상기 송신기가 다중 오류 정정을 이용하여 상기 수신기 측의 오류를 정정한다.

[0012] 한편, 이하에서는 상기 기재된 송신기 및 수신기가 공유하는 얽힌 큐비트를 이용하여 오류를 정정하는 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공한다.

발명의 효과

[0013] 본 발명의 실시예들은, 두 개의 오류 정정 부호(EA-CWS 및 스태빌라이저 부호) 또는 EA-CWS의 고유한 특성을 이용한 하나의 오류 정정 부호를 이용하여 송수신자 양측의 오류를 정정함으로써, 수신자 측의 얽힌 큐비트에서 오류가 발생하는 경우에도 이러한 오류를 정정함으로써, 양자 오류 정정 부호의 성능을 향상시킬 수 있다.

도면의 간단한 설명

[0014] 도 1은 본 발명의 일 실시예에 따른 두 개의 양자 오류 정정 부호를 이용하여 오류를 정정할 수 있는 오류 정정 부호 모델을 도시한 도면이다.

도 2는 본 발명의 일 실시예에 따른 두 개의 양자 오류 정정 부호를 이용하여 송신기 및 수신기가 공유하는 얽힌 큐비트(entangled qubit: ebit)의 오류를 정정하는 방법을 도시한 흐름도이다.

도 3은 본 발명의 일 실시예에 따른 도 2의 오류 정정 방법에서의 인코딩 전후의 워드 스태빌라이저(word stabilizer)를 비교하여 예시한 도면이다.

도 4는 본 발명의 다른 실시예에 따른 하나의 양자 오류 정정 부호를 이용하여 송신기 및 수신기가 공유하는 얽힌 큐비트의 오류를 정정하는 방법을 도시한 흐름도이다.

도 5는 본 발명의 다른 실시예에 따른 도 4의 오류 정정 방법에서 정정할 수 있는 오류의 형태와 개수를 예시하고 있다.

도 6은 본 발명의 다른 실시예에 따른 도 4의 오류 정정 방법에서 찾을 수 있는 불완전한 얽힌 큐비트를 포함한 EA-CWS 부호의 테이블을 예시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0015] 본 발명의 실시예들을 설명하기에 앞서, 얽힘 보조 양자 오류 정정 기술에 관해 개괄적으로 소개하고, 이를 이용한 EA-CWS(Entanglement-assisted CWS)의 문제점들을 검토한 후, 이들 문제점을 해결하기 위해 본 발명의 실시예들이 채택하고 있는 기술적 수단을 순차적으로 소개하도록 한다.

[0016] 부호어 고정 양자 오류 정정 부호(codeword stabilized quantum code: CWS code)는 링 그래프와 고전 이진 부호로부터 가산(additive) 부호와 비가산(non-additive) 부호를 구성할 수 있는 통합된 형태의 양자 오류 정정 부호이다. 그러나 링 그래프를 바탕으로 기존 이진 부호를 이용하여 구성한 CWS 부호는 현재까지 최소 거리(minimum distance)가 4보다 큰 부호를 찾을 수 없다는 한계점을 가지고 있다.

[0017] 얽힘 보조(Entanglement-assisted) 양자 오류 정정 부호는 수신자와 송신자 사이에서 얽힌 큐비트를 공유함으로서 몇 가지 이점을 가질 수 있다. 특히 얽힌 큐비트(entangled qubit: ebit)는 양자 정보가 가지고 있는 독특한 특성으로 얽힌 큐비트를 이용할 경우 양자 정보 시스템의 많은 부분에서 용량을 증가시키는 효과를 가져 올 수 있는데 이런 얽힌 큐비트의 특성을 이용하면 최소 거리를 확장할 수 있다.

[0018] 이러한 특성을 기존 CWS에 적용하면 최소 거리를 4 이상으로 확장할 수 있다. Entanglement-assisted CWS(EA-CWS) 부호는 이러한 한계점을 극복할 수 있는 더욱 더 확장된 개념의 양자 오류 정정 부호이다. EA-CWS 부호는 송수신자 양쪽에서 최대로 얽힌(maximally entangled) 큐비트를 사용한다. 이를 이용하면 CWS 부호는 최소 거리가 4보다 더 큰 비가산 부호를 생성할 수 있고, 이와 더불어 얽힌 큐비트의 사용을 통해 듀얼 컨테이닝 제한(dual containing constraint) 문제를 극복할 수 있다.

[0019] 한편, 종래의 얽힘 보조 양자 오류 정정 부호는 수신자 측의 얽힌 큐비트에서는 에러가 발생하지 않는다는 것을 가정한다. 그러나 실제 상황에서는 송신자뿐만 아니라 수신자 측의 얽힌 큐비트 상에서도 오류가 발생할 수 있다. 불행히도 기존의 얽힘을 이용한 양자 오류 정정 부호에서는 수신자 측의 얽힌 큐비트는 송신 채널을 통과하지 않으므로 오류가 발생하지 않는다고 가정하므로 이 경우에 기존의 오류 정정부호를 적용시키면 오류 정정능력이 더욱 저하되는 결과가 초래된다. 따라서 이러한 경우에 얽힌 큐비트를 CWS 부호에 적용하여 양자 오류 정정 부호의 성능을 향상시킬 수 있는 설계 기법이 필요하다.

[0020] 이상과 같은 이유에서, 이하에서 기술되는 본 발명의 실시예들은 기존의 EA-CWS 양자 오류 정정 부호를 송신자 측뿐만 아니라 수신자 측의 오류까지 정정 가능한 형태의 부호 설계 기법을 제안하고자 한다. 특히, 본 발명의 실시예들은 기존의 EA-CWS 부호가 완전한 얽힘 큐비트를 공유하는 것과 달리 불완전한 얽힘 큐비트를 공유하였을 경우에도 적용 가능한 양자 오류 정정 부호의 설계 기법을 제시한다.

[0021] 앞서 소개한 바와 같이, 일반적으로 기존의 얽힘을 이용한 양자 오류 정정 부호에서는 대부분 수신자 측의 얽힌 큐비트는 송신 채널을 통과하지 않으므로 오류가 발생하지 않는다고 가정하였다. 하지만 실제 상황에서는 송신 채널뿐만 아니라 수신자의 얽힌 큐비트 상에서도 오류가 필연적으로 발생하게 되며, 이는 기존의 양자 오류 정정 부호의 오류 정정 능력을 떨어뜨리는 결과를 가져온다. 따라서 본 발명의 실시예들은 기존의 송신자 측에서 오류가 발생하는 경우의 오류 정정뿐만 아니라 수신자 측의 얽힌 큐비트에서 오류가 발생하는 경우와 송수신자 측에서 동시에 오류가 발생할 경우에 대해서도 오류를 정정할 수 있는 오류 정정 부호가 요구된다.

[0022] 본 발명의 실시예들은 기존의 양자 오류 정정 부호 중 CWS 부호와 얽힘 양자 오류 정정 부호(EA-QECCs)를 기반으로 한다. 그리고 이 두 가지 부호의 결합으로 EA-CWS 부호를 형성할 수 있다. 이 부호는 얽힌 큐비트의 사용으로 많은 이점을 가지게 된다. 특히 부호의 성능을 높이거나 제한을 완화시킬 목적으로 사용 가능하다. EA-QEC(Entanglement-assisted quantum error correction) 부호의 경우 송수신자 사이에 공유되는 얽힌 큐비트를 사용하여 고전 오류 정정 부호로부터 양자 오류 정정 부호를 설계하는데 있어서 걸림돌이 되는 듀얼 컨테이닝 제한을 극복할 수 있는 방법을 제시한다. 또한 얽힌 큐비트의 사용으로 인해 최소 거리 또는 부호율(code rate)를 증가시킬 수도 있다.

[0023] EA-CWS 부호는 이러한 장점을 이용하여 수신자 측의 얽힌 큐비트에는 오류가 발생하지 않는다는 것을 가정하고, 기존 CWS 부호에 얽힌 큐비트를 적용하여 부호의 성능을 향상 시키는 양자 오류 정정 부호이다. 기본 표기법(notation)은 $[[n,K,d;c]]$를 사용하며, 이는 n개(n은 양의 정수)의 물리적 큐비트와 c개(c는 양의 정수)의 얽힌 큐비트를 사용하여, K 차원(dimensional) 부호 공간과 최소 거리 d(d은 양의 정수)를 가지도록 인코딩하는 양자 부호를 의미한다. 이를 이용하면 CWS 부호는 최소 거리가 4보다 더 큰 비가산 부호를 체계적으로 구성할 수 있다.

[0024] 하지만 실제 상황에서는 송신 채널뿐만 아니라 수신자의 얽힌 큐비트 상에서도 오류가 필연적으로 발생하게 되며, 이는 오류 정정 부호의 오류 정정 능력을 떨어뜨리는 결과를 가져온다. 따라서 본 발명의 실시예들에서는 송수신자 양쪽에서 발생하는 오류를 모두 정정하기 위한 오류 정정 부호를 사용하는 기법을 설계하였다. 송수신부가 공유하는 c개의 얽힌 큐비트를 사용하여 최소 거리가 d인 양자 오류 정정 부호를 CWS기법을 이용하여 설계하는 2가지 방법을 살펴보면 다음과 같다.

[0025] 이하에서는 도면을 참조하여 본 발명의 실시예들을 구체적으로 설명하도록 한다. 다만, 하기의 설명 및 첨부된 도면에서 본 발명의 요지를 흐릴 수 있는 공지 기능 또는 구성에 대한 상세한 설명은 생략한다.

[0026] [첫 번째 실시예]

[0027] 첫 번째 기법은 수신자 측의 얽힌 큐비트 상에서도 오류가 발생하는 상황을 고려하여, 이로 인한 오류 정정 능력의 저하를 막기 위해 고안된 기법이다. 이를 위해 두 개의 오류 정정 부호를 사용하는데 송신자 측에는

$[[n,k,d_A;c]]$ EA-CWS 부호를, 수신자 측에는 $[[m,c,d_B]]$ 스태빌라이저(stabilizer) 부호를 사용한다. 그리고, 스태빌라이저 부호에서 사용된 파라미터는 m개(m은 양의 정수)의 물리적 큐비트를 사용하여 c개(c는 양의 정수) 차원의 부호 공간과 최소 거리 d_B(d_B는 양의 정수)를 가지도록 인코딩하는 것을 의미하며, 여기서 언급된 c는 얽힌 큐비트의 개수와 동일하다. 즉, 첫 번째 기법은 EA-CWS 부호와 스태빌라이저 부호를 결합한 형태인 컴비네이션(combination) 부호를 사용하게 된다.

[0028] 도 1은 본 발명의 일 실시예에 따른 두 개의 양자 오류 정정 부호를 이용하여 오류를 정정할 수 있는 오류 정정 부호 모델을 도시한 도면이다.

[0029] 도 1을 참조하면, 수신자(20) 측의 얽힌 큐비트 상에서도 오류가 발생하는 상황을 고려하여, 이로 인한 오류 정정 능력의 저하를 막기 위한 부호 구성을 제안하고 있다.

[0030] 이를 위해 기존의 EA-CWS 부호에 수신자(20) 측에 추가적으로 스태빌라이저 부호를 결합한 형태인 컴비네이션 부호를 사용한다. 부호의 기본 구성을 살펴보면, 도 1에 제시된 바와 같이 송신자(10) 측에는 채널상에서 발생하는 오류를 정정하기 위해 EA-CWS 부호를 사용하고, 수신자(20) 측에는 얽힌 큐비트 상에서 발생하는 오류를 정정하기 위해 스태빌라이저 부호를 사용한다.

[0031] 스태빌라이저 부호(Stabilizer codes)는 양자 오류 정정 부호에서 매우 중요한 부호이다. 스태빌라이저 부호는 기존 오류 정정 부호 중 선형 오류 정정 부호와 매우 유사한 특징을 가지고 있다. 스태빌라이저 부호를 살펴보기에 앞서 기존 선형 블록 부호를 간단하게 살펴보면, 기존 선형 블록 부호에서 각 코드워드(codeword)는 생성기 행렬(generator matrix)의 열 벡터(row vector)의 선형 결합으로 구성되며 코드워드 전체는 생성기 행렬이 스팬(span)하는 공간으로 간주할 수 있다. 선형 블록 부호의 복호는 패리티 검사 행렬(parity check matrix)을 이용하여 오류의 유무를 확인하고 오류 증상(error syndrome)을 이용하여 코드워드를 복원하는 과정을 수행하게 된다.

[0032] 스태빌라이저 부호는 파울리 그룹(Pauli group)의 부분 집합 중 아벨군을 형성하는 스태빌라이저 그룹을 사용하여 오류를 복원하는 오류 정정 부호이다. 스태빌라이저 코드워드는 스태빌라이저 그룹에 의해 고정된 공간으로 스태빌라이저 그룹에 속하는 어떤 연산자와 연산을 수행하더라도 코드워드 공간이 변하지 않는 특징을 가지고 있다. 매우 많은 수의 연산자를 포함하는 스태빌라이저 그룹을 보다 간단하게 표현하기 위해 스태빌라이저 생성기(stabilizer generator)를 생각할 수 있다. 스태빌라이저 생성기는 스태빌라이저 그룹을 형성하는 기저 원소로써 스태빌라이저 생성기의 선형 결합을 통해 스태빌라이저 그룹을 생성할 수 있다. 따라서, 코드워드가 스태빌라이저 그룹에 의해 고정되어 있다는 말은 스태빌라이저 생성기에 의해 고정되어 있다는 것과 동일하다.

[0033] 스태빌라이저 부호의 복호 기법은 기존 선형 블록 부호와 동일하게 증상(syndrome)을 바탕으로 하고 있다. 스태빌라이저 부호에서 오류 증상(error syndrome)은 스태빌라이저 생성기와 채널 오류 사이의 교환 법칙 성립 유무에 의해 결정된다. 일반적으로 파울리 그룹(Pauli group)에 속하는 모든 연산자들은 각 연산자 사이에 교환 법칙이 성립하거나 성립하지 않는 두 가지 관계에 놓여 있다.

[0034] 채널에서 발생하는 오류와 스태빌라이저 생성기는 모두 파울리 그룹의 원소이며, 채널에서 발생한 오류 E와 스태빌라이저 생성기 S_c 사이에 교환 법칙이 성립하는 경우 $[S_c,E]=0$ 으로 표시하고, 교환 법칙이 성립하지 않는 경우는 $[S_c,E]=1$ 이 된다. 오류 증상은 스태빌라이저 생성기의 개수와 동일한 크기의 벡터로 정의된다. 오류 증상의 각 원소는 '0' 혹은 '1'의 값을 갖고 각 값은 증상(syndrome) 원소에 해당하는 스태빌라이저 생성기와 채널 오류 사이의 교환 법칙 성립 관계를 나타낸다. 이는 기존 오류 정정 부호에서 수신된 부호가 패리티 검사(parity check) 방정식을 만족하는 경우 '0'을, 오류로 인해 패리티 검사 방정식을 만족하지 못하는 경우 '1'을 갖는 것과 동일한 결과를 나타내는 것과 동일하며, 스태빌라이저 부호에서는 스태빌라이저 생성기가 고전 오류 정정 부호의 패리티 검사 방정식과 같은 역할을 하게 된다.

[0035] 대표적인 스태빌라이저 부호의 범주로는 CSS 부호를 생각할 수 있다. CSS 부호의 이중 부호(dual-code) 특성은 스태빌라이저 부호에서 각 스태빌라이저 생성기 사이의 교환 법칙 성립을 위한 조건과 동일하다. 스태빌라이저 생성기에 해당하는 패리티 검사 방정식을 갖는 선형 블록 부호의 이중 부호 특성을 만족해야만 한다.

[0036] 현재 대부분은 스태빌라이저 부호는 기존 선형 블록 부호의 이중 부호를 이용하여 작성되고 있다. 하지만 이중 부호를 만족해야 하는 특성 때문에 기존 선형 블록 부호 중 성능이 좋은 부호(예를 들어, LDPC 부호가 될 수 있다.)의 적용이 제한을 받게 된다. 이러한 문제점을 해결하기 위한 방법으로 얽힌 상태(Entangled state)를 이용한 얽힌 보조(entanglement assisted) 양자 오류 정정 부호기 기법이 최근 연구되고 있다. 얽힌 상태를 사용할 경우 이중 부호 특성을 만족하지 않는 경우에도 기존 선형 블록 부호 기법을 스태빌라이저 부호에 적용할 수 있으며, 따라서 기존 성능이 좋은 다양한 오류 정정 부호를 양자 오류 정정 부호에 적용이 가능하다.

[0037] CSS 부호와 스태빌라이저 부호를 대표적으로 현재 연구되고 있는 양자 오류 정정 부호가 갖는 공통적인 특징은 양자 오류 정정 부호를 구성함에 있어서 양자 정보 시스템과 고전 정보 시스템의 많은 차이에도 불구하고 기존 오류 정정 부호의 기법을 양자 오류 정정 부호에 쉽게 적용할 수 있다는 것이다. 이와 더불어 최근에는 양자의 얽힘 현상을 이용하여 기존 선형 블록 부호의 이중 부호 특성이 없는 경우에도 기존 부호를 이용하여 양자 오류 정정 부호를 구성할 수 있는 방법이 연구되어 이론적으로는 거의 모든 기존 오류 정정 부호 기법을 양자 오류 정정 부호 기법에 적용할 수 있는 방법이 연구되고 있다.

[0038] 도 2는 본 발명의 일 실시예에 따른 두 개의 양자 오류 정정 부호를 이용하여 송신기 및 수신기가 공유하는 얽힌 큐비트(entangled qubit: ebit)의 오류를 정정하는 방법을 도시한 흐름도로서, 다음과 같은 단계들을 포함한다.

[0039] S210 단계에서, 송신기는 EA-CWS(entanglement assisted codeword stabilized quantum) 부호를 이용하여 채널 상에서 발생하는 오류를 정정한다. S220 단계에서, 수신기는 스태빌라이저(stabilizer) 부호를 이용하여 수신된 얽힌 큐비트(entangled qubit: ebit) 상에서 발생하는 오류를 정정한다. 여기서, 상기 EA-CWS 부호 및 상기 스태빌라이저 부호의 2개의 오류 정정 부호를 결합하여 컴비네이션(combination) 부호를 형성하게 된다. 특히, 상기 수신기는, 상기 컴비네이션 부호 내에 포함된 상기 스태빌라이저 부호를 통해, 송신 채널 상에서 발생하는 오류뿐만 아니라, 상기 송신 채널의 통과 후 상기 수신기에서 발생하는 오류를 정정할 수 있게 된다.

[0040] 불완전 얽힘 큐비트를 이용한 양자 오류 정정 부호에서는 기존의 완전한 오류가 없는 얽힘 큐비트를 이용한 양자 오류 정정 부호가 송수신과정에서 채널 오류만을 가정해서 EA-CWS 부호를 이용해서 채널 오류만을 정정할 수 있었던 것에 반해, 불완전 얽힘 큐비트를 가진 경우, 채널 오류는 기존의 EA-CWS 부호를 이용하여 정정하는 단계까지는 동일하나, 수신단인 Bob 측의 얽힘 큐비트에서 발생하는 스토리지(storage) 오류에 대해서 추가적인 고려가 필요하다.

[0041] 얽힘을 이용한 양자 오류 정정 부호인 EA-CWS 부호에서 수신단의 얽힘 큐비트에서 발생하는 스토리지 오류가 발생할 경우 이를 정정하기 위한 목적으로 스태빌라이저 부호를 사용하였다. 수신기 측인 Bob에서 발생하는 오류의 범위에 따라 적용하는 $[[m,c,d_B]]$ 의 파라미터 값은 바뀌게 되는데, 여기서 이용할 수 있는 스테빌라이져 부호의 파라미터 값은 다음 표 1과 같은 Markus의 코드 파라미터 테이블(M. Grassl, "Bounds on the minimum distance of linear codes and quantum codes,") 값을 활용할 수 있다.

표 1

[0042]

n/k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
1	1	1																													
2	2	1	1																												
3	2	1	1	1																											
4	2	2	2	1	1																										
5	3	3	2	1	1	1																									
6	4	3	2	2	2	1	1																								
7	3	3	2	2	2	1	1	1																							
8	4	3	3	3	2	2	2	1	1																						
9	4	3	3	3	2	2	2	1	1	1																					
10	4	4	4	3	3	2	2	2	2	1	1																				
11	5	5	4	3	3	3	2	2	2	1	1	1																			
12	6	5	4	4	4	3	3	2	2	2	2	1	1																		
13	5	5	4	4	4	3	3	3	2	2	2	1	1	1																	
14	6	5	5	4-5	4	4	4	3	3	2	2	2	2	1	1																
15	6	5	5	5	4	4	4	3	3	3	2	2	2	1	1	1															
16	6	6	6	5	5	4-5	4	4	3	3	3	2	2	2	2	1	1														
17	7	7	6	5-6	5	4-5	4-5	4	4	4	3	3	2	2	2	1	1	1													
18	8	7	6	5-6	5-6	5	5	4	4	4	3	3	2	2	2	2	2	1	1												
19	7	7	6	5-6	5-6	5-6	5	4-5	4	4	3-4	3	3	2	2	2	2	1	1	1											
20	8	7	6-7	6-7	6	5-6	5-6	4-5	4-5	4	4	3-4	3	3	2	2	2	2	2	1	1										
21	8	7	6-7	6-7	6-7	6	5-6	5-6	4-5	4-5	4	4	3-4	3	3	3	2	2	2	1	1	1									
22	8	7-8	6-8	6-7	6-7	6-7	5-6	5-6	5-6	4-5	4-5	4	4	3-4	3	3	2	2	2	2	2	1	1								

[0043] 앞서 정의한 코드 표기법에 따르면, 세로축은 m(표 1에서는 n으로 표기), 가로축은 c(표 1에서는 k로 표기)의 값을 의미한다. 그리고 가운데 부분에 기재된 숫자들은 m과 c 값에 따른 최소 거리 d의 값을 의미한다. 이 테이블 값은 현재까지 밝혀진 스테빌라이저 코드의 최적화 된 값을 정리해 놓은 테이블이며, 대부분의 스테빌라이져 논문은 이 코드값을 토대로 하게 된다.

[0044] 만약 본 발명에서 제안하는 실시예에 따른 코드에서 수신단 쪽에 2개의 오류가 발생했다면, 이를 정정하기 위해서 최소거리 d가 5 이상의 스테빌라이저 부호가 필요하므로, 표 1에서 d=5인 것 중 사용되는 큐비트 m이 가장 작은 11을 선택한다. 또한, 여기서 사용되는 c 값은 표 1에서 0과 1이 발견되는데, 이 값은 채널 오류 정정에 사용되는 $[[n,k,d_A;c]]$ EA-CWS 부호와 동일한 c 값을 이용하여 오류를 정정하게 된다.

[0045] 도 3은 본 발명의 일 실시예에 따른 도 2의 오류 정정 방법에서의 인코딩 전후의 워드 스테빌라이저(word stabilizer)를 비교하여 예시한 도면이다.

[0046] 예를 들어, $((7,4,5;4))$ 부호와 $[[11,4,3]]$ 스테빌라이저 부호(stabilizer code)를 결합한 컴비네이션 부호(combination code)를 사용하면, 기존의 CWS 양자 오류 정정 부호와 마찬가지로 채널 상에서 발생하는 2개의 오류를 정정할 수 있으며, 수신자 측에서 발생하는 1개의 오류 또한 정정할 수 있다. 이를 등가 오류 정정 부호인 $[[n+m,k,d]]=[[18,2,6]]$ 표준 스테빌라이저(standard stabilizer) 부호와 비교해 보면, 실제 채널에서 발생하는 오류에 대한 정정 능력은 2개로 동일하지만, 동일한 정보를 전송하기 위해 채널을 통해 전송된 물리적 큐비트는 EA-CWS 부호의 경우 7개의 큐비트로서 18개의 물리적 큐비트를 전송해야 하는 스테빌라이저 부호에 비해 더 좋은 채널 효율을 보여주는 것을 확인할 수 있다. 이를 통하여 송신자 측뿐만 아니라 수신자 측의 오류도 정정이 가능하게 되었고, 또한 기존의 양자 오류 정정 부호에 비해 더 향상된 오류 정정 능력을 가진 부호를 만들어 낼 수 있다.

[0047] [두 번째 실시예]

[0048] 두 번째 기법은 하나의 오류 정정 부호를 이용하여 송수신자 양측의 오류를 정정한다. 이를 위해 EA-CWS의 고유한 특성을 이용하는데 이는 인코딩 과정을 거친 후 각각의 서로 다른 스테빌라이저 생성기(stabilizer

generator)는 서로 다른 위치의 하나의 큐비트 상에 X 연산자(operator)를 갖는다는 것이다.

[0049] 이러한 특성을 이용하면 이 기법은 스태빌라이저와 파울리(Pauli) 오류의 연산을 통해 기존 EA-CWS 부호와 같이 송신자(이하에서 Alice로 예시된다.) 쪽에서 발생하는 단일 오류를 Z와 I 연산자(operator)만으로 구성되는 유효 오류(effective error)로 바꿀 수 있을 뿐만 아니라, 수신자 측(이하에서 Bob으로 예시된다.) 쪽에서 발생하는 오류 또한 유효 오류로 바꿀 수 있다. 여기서, Z 연산자는 페이즈 플립(Phase flip)을 의미하는 연산자이고, I는 아이덴티티 연산자(identity operator)를 의미한다. 양자 오류는 크게 크게 X, Y, Z와 이들의 조합으로 구성된 오류로 구성되며, 그 세부 내용은 다음의 수학식 1과 같다.

수학식 1

Quantum errors

- $i \in \{0,1\}$ and $\bar{i} = i \oplus 1$
- Bit flip 'X' : $|i\rangle \rightarrow |\bar{i}\rangle$
- Phase flip 'Z' : $|i\rangle \rightarrow (-1)^i |i\rangle$
- Bit-phase flip 'Y' : $|i\rangle \rightarrow (-1)^{\bar{i}} j|\bar{i}\rangle = jZX|i\rangle$
- In general, $E = e_1 I + e_2 X + e_3 Y + e_4 Z$,
  where I : identity operator
  e_k : complex number

[0050]

[0051] 'Z'와 'I'로 변경된 채널 오류는 각 각 '0'과 '1'로 대응되는 이진 오류로 대체하여 생각할 수 있으며, 워드 스태빌라이저(word stabilizer)에 의해 유도된 이진 오류를 수정할 수 있는 고전 오류 정정 부호를 이용하여 오류를 정정할 수 있다. 보다 구체적인 과정은 다음의 문헌(A. Cross, G. Smith, J. A. Smolin, and B. Zeng, "Codeword Stabilized Quantum codes" IEEE T. Inform. Theory 55, 433 ,2009.)에서 참조될 수 있으며, 특히 표준 형태(Standard form)의 CWS 부호에서 코드워드에 영향을 미치는 단일 파울리 오류 Z,X, Y=XZ는 스태빌라이저 생성기에 의해 Z로만 구성된 오류로 치환될 수 있음을 보이고 있다.

[0052] 도 4는 본 발명의 다른 실시예에 따른 하나의 양자 오류 정정 부호를 이용하여 송신기 및 수신기가 공유하는 얽힌 큐비트의 오류를 정정하는 방법을 도시한 흐름도로서, 다음의 단계들을 포함한다.

[0053] S410 단계에서, 오류 정정 장치는, 얽힌 큐비트의 전송을 위한 인코딩 과정 후, EA-CWS 부호의 서로 다른 스태빌라이저 생성기(stabilizer generator)에 대하여 파울리(Pauli) 오류의 연산을 수행한다.

[0054] S420 단계에서, 오류 정정 장치는, 상기 S410 단계의 연산 결과, 상기 송신기 또는 상기 수신기에서 발생하는 오류를 수정 가능한 오류 형태인 오류 정정 부호로 변환한다.

[0055] S430 단계에서, 오류 정정 장치는, 상기 S420 단계를 통해 변환된 오류 정정 부호를 이용하여 CWS 부호의 워드 연산자(word operator)를 생성함으로써 상기 송신기 또는 상기 수신기에서 발생하는 얽힌 큐비트의 오류를 정정한다.

[0056] 여기서, 상기 서로 다른 스태빌라이저 생성기는 서로 다른 위치의 하나의 큐비트 상에 오류를 나타내는 X 연산자(X operator)를 포함함으로써, 파울리 오류의 연산을 통해 상기 송신기에서 발생하는 단일 오류를 Z 연산자 및 I 연산자만으로 구성되는 유효 오류를 생성하며, 상기 유효 오류를 수정 가능한 이진 오류로 변환하게 된다.

[0057] 이상과 같이 두 번째 기법은 첫 번째 기법과는 달리 하나의 오류 정정 부호를 이용하여 송수신자 양측의 오류를 정정한다. 이를 위해 두 번째 기법에서는 EA-CWS의 고유한 특성을 이용하는데 이는 인코딩 과정을 거친 후 각각의 서로 다른 스태빌라이저 생성기는 아래의 수학식 2에서와 같이 서로 다른 위치의 하나의 큐비트 상에 X 연산자를 갖는다.

수학식 2

[0058]
$$\begin{cases} X_1 Z_2 I \ldots I Z_n | I^{\otimes c} \\ Z_1 X_2 Z_3 I \ldots I | I^{\otimes c} \\ I Z_2 X_3 Z_4 I \ldots I | I^{\otimes c} \\ \cdots \\ I \ldots I Z_{n-c-1} X_{n-c} Z_{n-c+1} I \ldots I | I \\ \cdots \\ I \ldots I Z_{n-2} I I | I \ldots I X_{c-2} I I \\ I \ldots I I Z_{n-1} I | I \ldots I I X_{c-1} I \\ I \ldots I I I I Z_n | I \ldots I I I X_c \end{cases}$$

[0059] 수학식 2에서, 각각의 스태빌라이저 생성기는 오류를 나타내는 X 연산자를 포함하고 있으며, 이들 X 연산자는 각각 서로 다른 위치에 하나씩 포함됨을 알 수 있다.

[0060] 이러한 특성을 이용하여 두 번째 기법은 스태빌라이저와 파울리(Pauli) 오류의 연산을 통해 기존 EA-CWS 부호와 같이 송신자인 Alice 쪽에서 발생하는 단일 오류를 Z와 I 연산자만으로 구성되는 유효 오류로 바꿀 수 있을 뿐만 아니라 수신자 측인 Bob 쪽에서 발생하는 오류 또한 유효 오류로 바꿀 수 있다.

[0061] 그러면,'Z'와 'I'로 변경된 채널 오류는 각각 '0'과 '1'로 대응되는 이진 오류로 대체하여 생각할 수 있으며, 워드 스태빌라이저(word stabilizer)에 의해 유도된 이진 오류를 수정할 수 있는 고전 오류 정정 부호를 이용하여 CWS 부호의 워드 연산자(word operator)를 구성할 수 있다.

[0062] 한편, 여기서 중요한 것은 송신자 측의 오류와 수신자 측의 오류 사이에 등가 전환 관계가 성립하게 된다는 것이다. 성립된 등가 관계를 이용하면 기존 EA-CWS 부호와 달리 송신자 측에서 다중 오류 정정 능력을 추가적으로 갖게 된다. 그리고 송신자 및 수신자 양측에서 발생하는 오류의 등가 전환 관계를 이용하면 송신자 측의 다중 오류 정정을 통해 수신자 측의 오류를 정정할 수 있는 능력을 얻게 됨을 알 수 있다.

[0063] 따라서, 상기된 본 발명의 다른 실시예는, 상기 송신기 측의 오류와 상기 수신기 측의 오류는 등가 전환 관계를 형성함으로써, 상기 송신기가 다중 오류 정정을 이용하여 상기 수신기 측의 오류를 정정할 수 있다.

[0064] 그리고 두 번째 기법에서 워드 연산자(word operator)는 기존 EA-CWS 부호의 경우와 동일하게 송신부와 수신부 모두에서 수행되는 연산자로 구성된다. 처음 가정에서 인코딩 연산은 송신부에서만 수행되어야하기 때문에 워드 연산자에 워드 스태빌라이저를 적용함으로써 워드 연산자에 존재하는 수신부 연산자를 소거하는 과정이 필요하다. 실제 워드 연산자는 'Z' 연산자로만 구성되어 있으며, 이는 수신부에 'Z' 연산자를 가지고 있는 워드 연산자에 동일하게 수신부에 'Z' 연산자를 가지고 있는 워드 스태빌라이저 연산자를 적용함으로써 워드 연산자의 연산이 송신부에서만 독립적으로 수행되게 할 수 있다.

[0065] 이제, 이 과정을 통해 고칠 수 있는 오류의 형태에 대해 살펴보면 도 5와 같은 결과를 얻게 됨을 알 수 있다.

[0066] 도 5는 본 발명의 다른 실시예에 따른 도 4의 오류 정정 방법에서 정정할 수 있는 오류의 형태와 개수를 예시하고 있다. 도 5에 예시된 표의 결과에서 알 수 있듯이, 최소 거리가 3일 때, 기존 ((n,K,d;c)) EA-CWS 부호의 경우에는 $3n$ 개의 Alice쪽의 단일 오류만 정정할 수 있었으나, 불완전 얽힘 큐비트를 가진 EA-CWS 부호를 이용한 두 번째 기법에서는 송수신자 양측에서 발생하는 오류를 모두 고려하고 있으므로 기존 부호에 비해 월등히 많은 $(3n+1)4^c$ 개의 오류를 고칠 수 있다.

[0067] 그리고 불완전한 얽힘 큐비트를 가진 경우에 있어서 EA-CWS 부호 설계 기법을 이용한 실제 부호의 설계 예로는 최소 거리가 3인 경우에 도 6의 EA-CWS 부호를 찾을 수 있다.

[0068] 도 6은 본 발명의 다른 실시예에 따른 도 4의 오류 정정 방법에서 찾을 수 있는 불완전한 얽힌 큐비트를 포함한 EA-CWS 부호의 테이블을 예시한 도면으로서, n, d 및 c에 따른 EA-CWS 부호를 도시하였다.

[0069] 이상에서 기술된 본 발명의 실시예들은, 기존의 EA-CWS 부호보다 일반적이고 다양한 실제 상황에 적용할 수 있는 불완전 얽힘 큐비트가 존재할 경우에 있어서의 EA-CWS 부호의 설계 방법을 제안하고 있다.

[0070] 기존의 부호에서는 부호어 양자 오류 정정부호 기법(codeword stabilized quantum codes: CWS codes)에 얽힌 큐비트(entanglement qubits)을 적용하여 양자 오류 정정 부호의 성능을 개선할 수 있었으나, 이는 수신자 측의 얽힌 큐비트가 송신 채널을 통과하지 않으므로 오류가 발생하지 않는다고 하는 가정 하에서만 유효하였다. 실제 상황에서는 수신자 측의 얽힌 큐비트에서도 오류가 발생할 수 있으므로 이 경우에 적용 가능한 양자 오류 정정 부호 개발을 통해 송수신자 양측에서 발생하는 오류를 정정할 수 있게 되었다.

[0071] 한편, 본 발명의 실시예들은 컴퓨터로 읽을 수 있는 기록 매체에 컴퓨터가 읽을 수 있는 부호로 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록 매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다.

[0072] 컴퓨터가 읽을 수 있는 기록 매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광 데이터 저장장치 등이 있으며, 또한 캐리어 웨이브(예를 들어 인터넷을 통한 전송)의 형태로 구현하는 것을 포함한다. 또한, 컴퓨터가 읽을 수 있는 기록 매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산 방식으로 컴퓨터가 읽을 수 있는 부호가 저장되고 실행될 수 있다. 그리고 본 발명을 구현하기 위한 기능적인(functional) 프로그램, 부호 및 부호 세그먼트들은 본 발명이 속하는 기술 분야의 프로그래머들에 의하여 용이하게 추론될 수 있다.

[0073] 이상에서 본 발명에 대하여 그 다양한 실시예들을 중심으로 살펴보았다. 본 발명에 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

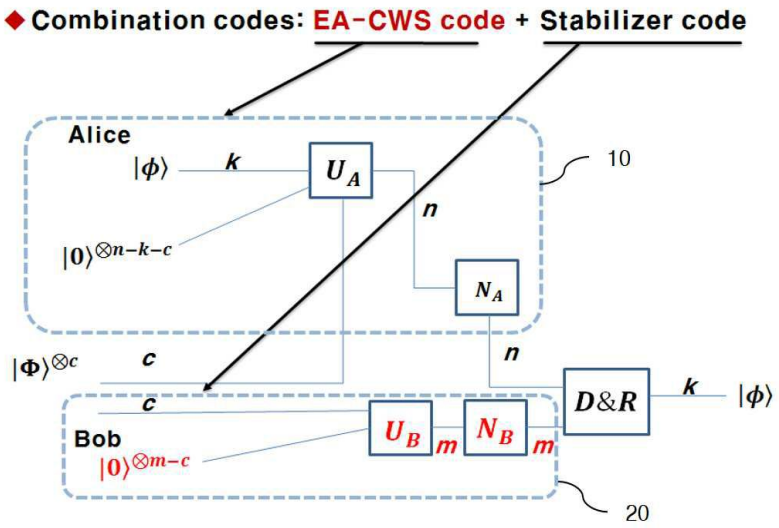
부호의 설명

[0074] 10 : 송신기

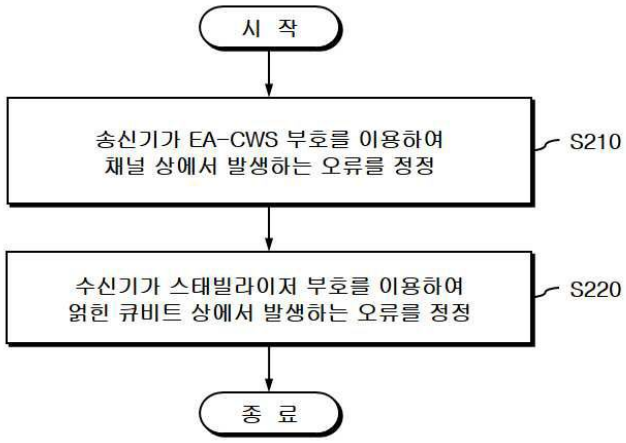
20 : 수신기

도면

도면1



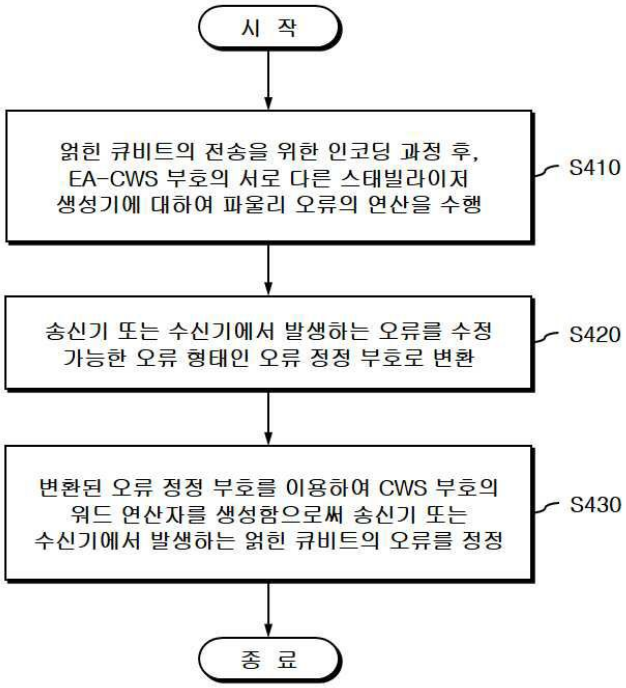
도면2



도면3

인코딩 전	범위
$g'_i = Z_i^A \vert I^B \otimes I^{\otimes m-c}$	$i = 1,\ldots,n-c$
$g'_i = Z_i^A \vert Z_j^B \otimes I^{\otimes m-c}$	$i = n-c+1,\ldots,b$ $j = i-(n-c)$
$g'_i = X_i^A \vert X_j^B \otimes I^{\otimes m-c}$	
$s_i = I^A \vert I^B \otimes Z_i$	$i = 1,\ldots,m-c$
인코딩 후	범위
$g'_i = Z_i^A \vert I^B \otimes I^{\otimes m-c}$	$i = 1,\ldots,n-c$
$g'_i = X_1 Z^r \vert Z_j^B \otimes I^{\otimes m-c}$	$i = n-c+1,\ldots,b$ $j = i-(n-c)$
$h_j = Z_i \vert X_j^B \otimes v_j$	
$s_i = I^A \vert I^B \otimes u_i$	$i = 1,\ldots,m-c$
$(\text{단}, u_i = U_B Z_i^B U_B^\dagger\ (i = 1,\ldots,m), v_j = U_B X_j^B U_B^\dagger\ (j = 1,\ldots,c))$	

도면4



도면5

오류 형태	오류의 갯수
Single error on Alice's side	$3n$
No error	1
Errors on Bob's side	4^c-1
Single error on Alice's side and errors on Bob's side take place at the same time	$3n(4^c-1)$
Total number of errors	$(3n+1)4^c$

도면6

EA-CWS code with Imperfect Ebit							
n=5, d=3	c						
	1	2	3	4			
	n	n	n	n			
n=6, d=3	c						
	1	2	3	4	5		
	n	n	n	n	n		
n=7, d=3	c						
	1	2	3	4	5	6	
	n	n	n	n	n	n	
n=8, d=3	c						
	1	2	3	4	5	6	7
	[[8,1,3;1]]	n	n	n	n	n	n
n=9, d=3	c						
	1	2	3	4	5	6	7
	[[9,3,3;1]]	[[9,1,3;2]]	n	n	n	n	n