

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2014년 5월 8일 (08.05.2014)



(10) 국제공개번호
WO 2014/069773 A1

- (51) 국제특허분류:
H04L 9/12 (2006.01) H04L 9/08 (2006.01)
- (21) 국제출원번호: PCT/KR2013/007511
- (22) 국제출원일: 2013년 8월 21일 (21.08.2013)
- (25) 출원언어: 한국어
- (26) 공개언어: 한국어
- (30) 우선권정보:
10-2012-0121540 2012년 10월 30일 (30.10.2012) KR
- (71) 출원인: 에스케이텔레콤 주식회사 (SK TELECOM CO., LTD.) [KR/KR]; 100-999 서울시 중구 을지로 2가 11번지, Seoul (KR).
- (72) 발명자: 조정식 (CHO, Jeong-sik); 305-333 대전시 유성구 어은동 한빛아파트 108동 1004호, Daejeon (KR).
최정운 (CHOI, Jeong-woon); 448-160 경기도 용인시 수지구 죽전동 832번지 벽산 1단지아파트 103동 903호, Gyeonggi-do (KR).
- (74) 대리인: 이철희 (LEE, Chulhee); 135-911 서울시 강남구 역삼동 647-13 동궁빌딩 5층, Seoul (KR).

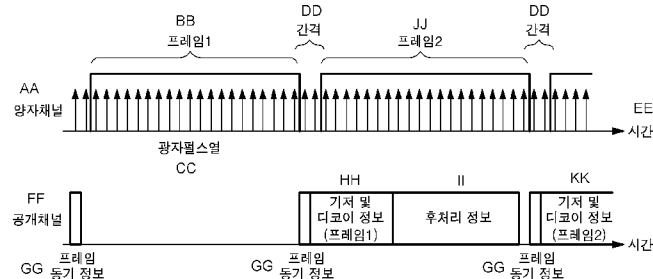
- (81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

공개:

— 국제조사보고서와 함께 (조약 제 21 조(3))

(54) Title: METHOD AND APPARATUS FOR GENERATING AND PROCESSING QUANTUM SIGNAL IN REGULAR FRAME UNIT FOR QUANTUM ENCRYPTION KEY DISTRIBUTION

(54) 발명의 명칭 : 양자 암호키 분배를 위해 정기적인 프레임 단위의 양자 신호를 생성하고 처리하는 방법 및 장치



AA ... Quantum channel
BB ... Frame 1
CC ... Photon pulse sequence
DD ... Interval
EE ... Time
FF ... Open channel

GG ... Frame synchronization information
HH ... Base and decoy information (frame 1)
II ... Post-processing information
JJ ... Frame 2
KK ... Base and decoy information (frame 2)

(57) Abstract: Disclosed are a method and apparatus for generating and processing a quantum signal in a regular frame unit for quantum encryption key distribution. According to one aspect of the present embodiments, a transmission device of a quantum encryption key distribution system includes: a photon pulse sequence generating unit that generates quantum information in a numbered frame unit and periodically transmits the quantum information through a quantum channel; an open channel transceiving unit that communicates with a reception device of the quantum encryption key distribution system through an open channel; a frame synchronization information generating unit that generates frame synchronization information for operating frame synchronization of the reception device and transmits the frame synchronization information to the reception device through the open channel transceiving unit for each frame or several frames; and a signal processing unit that transceives open information for each frame through the open channel transceiving unit and signal processes the quantum information as a frame unit, wherein the quantum signal is generated and processed as a regular frame unit.

(57) 요약서:

[다음 쪽 계속]

WO 2014/069773 A1



양자 암호키 분배를 위해 정기적인 프레임 단위의 양자 신호를 생성하고 처리하는 방법 및 장치를 개시한다. 본 실시예의 일 측면에 의하면, 양자 암호키 분배 시스템의 송신장치에 있어서, 양자정보를 번호가 부여된 프레임 단위로 생성하여 양자채널을 통해 주기적으로 전송하기 위한 광자펄스열 생성부, 공개채널을 통해 상기 양자 암호키 분배 시스템의 수신장치와 통신하기 위한 공개채널 송수신부, 매 프레임마다 또는 수 개의 프레임마다, 상기 수신장치의 프레임 동기화 작업을 위한 프레임동기정보를 생성하여 상기 공개채널 송수신부를 통해 상기 수신장치에 전송하기 위한 프레임 동기정보 발생부 및 상기 공개채널 송수신부를 통해 상기 프레임별 공개정보를 송수신하여, 상기 양자정보를 프레임 단위로 신호처리하기 위한 신호처리부를 포함하는 정기적인 프레임 단위로 양자 신호를 생성 및 처리하는 송신장치를 제공한다.

명세서

발명의 명칭: 양자 암호키 분배를 위해 정기적인 프레임 단위의 양자 신호를 생성하고 처리하는 방법 및 장치

기술분야

- [1] 본 실시예는 양자 암호키 분배를 위해 정기적인 프레임(Frame) 단위의 양자 신호를 생성하고 처리하는 방법 및 장치에 관한 것이다. 보다 상세하게는, 송신부에서는 번호를 부여한 프레임 단위의 양자신호를 주기적으로 생성하여 전송하고 수신부에서는 해당 번호에 맞게 처리하여 시스템의 성능을 향상하는, 양자 암호키 분배를 위해 정기적인 프레임 단위의 양자 신호를 생성하고 처리하는 방법 및 장치에 관한 것이다.

배경기술

- [2] 이 부분에 기술된 내용은 단순히 본 실시예에 대한 배경 정보를 제공할 뿐 종래기술을 구성하는 것은 아니다.
- [3] 양자 암호키 분배 시스템(Quantum Key Distribution System: QKD System)이 고속화되면서 양자신호 생성 및 검출 속도가 빨라지고 있다. 최종 키 생성 속도를 높이기 위해서는 신호처리 회로의 고속화뿐만 아니라 효율적인 신호처리가 필요하다. 그러나 공개채널을 통한 정보전송 및 수신이 완료되기를 기다리는 시간 및 그 이후에 전후처리를 진행해야 하는 순서 등은 신호처리 회로의 고속화와 무관한 요소이며, 이 때문에 양자정보를 처리하는 전체 시간이 양자정보전송 및 검출 시간에 비해 지연되는 경우가 발생한다.
- [4] 양자정보 전송 시에는 시스템 클럭 대비 수신부에서 광자 신호를 검출하는 횟수가 매우 작으므로 신호처리 시 수신 정보의 배열 순서를 맞추기 힘들고, 기저 비교 및 디코이 신호 처리를 위해서는 송수신 양자가 생성한 정보를 신호처리 완료 전까지 모두 저장하고 있어야 한다는 점을 고려하면, 양자정보를 프레임(Frame) 단위로 묶어 전송하고 신호처리를 수행하는 것이 유리하다. 프레임은 비트/기저 정보에 따른 위상 또는 편광 변조와 디코이 정보에 따른 진폭 변조를 수행하고 이후의 신호처리를 위해 각 정보를 저장할 때 한 단위로 취급되는 정보의 덩어리를 말한다.
- [5] 이와 같이 프레임 단위로 양자정보를 전송할 경우에는 프레임 한 주기 내에 신호처리가 완료되어야 하는데, 통신 및 신호처리에 소요되는 시간을 고려하면 현실적으로 한 주기 내에 처리하기가 어려우며, 결국 시스템의 키 생성 속도가 저하되고 양자채널 및 공개채널의 대역폭이 효율적으로 활용되지 못하게 된다.
- [6] 예컨대, 미국등록특허 제7,539,314호에서는, 송신부에서 프레임 단위로 신호를 생성하여 전송하면, 수신부에서는 이에 대한 처리를 완료한 이후 송신부에 준비신호를 전송하고, 송신부에서는 준비신호를 확인한 후에 비로소 다음 프레임을 전송하는 QKD 시스템을 개시하고 있다.

- [7] 이에 따르면, 송신부에서는 수신부로부터 준비신호를 받기 전까지 프레임단위의 양자 신호를 전송하지 않기 때문에, 수신부의 신호처리에 오버플로우(Overflow)가 발생하는 것을 방지할 수 있다. 그러나 송수신부 전체 시스템의 동작 측면에서는 동작 속도 대비 실제 정보교환의 비율이 낮아지게 되어 키생성률이 저하되는 문제점이 있다.

발명의 상세한 설명

기술적 과제

- [8] 본 실시예는, 송신부에서는 번호를 부여한 프레임 단위의 양자신호를 주기적으로 생성하여 전송하고 수신부에서는 해당 번호에 맞게 처리하여 시스템의 성능을 향상시킬 수 있는 정기적인 프레임 단위의 양자 신호를 생성하고 처리하는 방법 및 장치를 제공하는 데 주된 목적이 있다.

과제 해결 수단

- [9] 본 실시예의 일 측면에 의하면, 양자 암호키 분배 시스템의 송신장치에 있어서, 양자정보를 번호가 부여된 프레임 단위로 생성하여 양자채널을 통해 주기적으로 전송하기 위한 광자펄스열 생성부, 공개채널을 통해 상기 양자 암호키 분배 시스템의 수신장치와 통신하기 위한 공개채널 송수신부, 매 프레임마다 또는 수 개의 프레임마다, 상기 수신장치의 프레임 동기화 작업을 위한 프레임동기정보를 생성하여 상기 공개채널 송수신부를 통해 상기 수신장치에 전송하기 위한 프레임동기정보 발생부 및 상기 공개채널 송수신부를 통해 상기 프레임별 공개정보를 송수신하여, 상기 양자정보를 프레임단위로 신호처리하기 위한 신호처리부를 포함하는, 정기적인 프레임 단위로 양자 신호를 생성 및 처리하는 송신장치를 제공한다.
- [10] 상기 공개정보신호 및 상기 프레임동기정보는 관련된 프레임의 번호 정보를 포함하는 것이 바람직하다.
- [11] 또한, 상기 양자정보를 프레임 단위로 전송하기에 앞서서, 상기 광자펄스열 생성기는 동기화용 프레임을 상기 양자채널을 통해 전송하고, 상기 공개채널 송수신부는 상기 동기화용 프레임에 관한 공개정보인 동기화 정보를 공개채널을 통해 전송하는 것이 바람직하다.
- [12] 또한, 상기 공개채널 송수신부는 상기 프레임에 관한 공개정보신호를 전송함에 있어서, 상기 수신장치의 전처리 작업을 위한 공개정보신호를 상기 수신장치의 후처리 작업을 위한 공개정보신호에 우선하여 전송하는 것이 바람직하다.
- [13] 본 실시예의 또다른 측면에 의하면, 양자 암호키 분배 시스템의 수신장치에 있어서, 공개채널을 통해 상기 양자 암호키 분배 시스템의 송신장치와 통신하기 위한 공개채널 송수신부, 상기 공개채널 송수신부를 통해 상기 송신장치로부터 프레임동기정보를 수신하여 프레임 동기화 작업을 수행하기 위한 프레임동기 정보 처리부, 양자채널을 통해 상기 송신장치로부터 전송되는 광자펄스신호를 검출하기 위한 단일광자검출부 및 상기 프레임동기정보에 포함된 프레임의

번호 정보 및 상기 공개채널 송수신부를 통해 상기 송신장치와 송수신한 프레임 단위의 신호처리 정보를 기초로, 상기 단일광자검출부의 출력으로부터 검출된 양자정보를 프레임 단위로 신호처리하기 위한 신호처리부를 포함하는, 정기적인 프레임 단위로 양자 신호를 생성 및 처리하는 수신장치를 제공한다.

- [14] 본 실시예의 또다른 측면에 의하면, 양자 암호키 분배 시스템의 송신장치가 양자신호를 정기적인 프레임 단위로 생성 및 처리하는 방법에 있어서, 상기 수신장치의 프레임 동기화 작업을 위한 프레임동기정보를 공개채널을 통해 전송하는 제1과정, 양자정보를 번호가 부여된 프레임 단위로 생성하여 양자채널을 통해 상기 수신장치에 주기적으로 전송하는 제2과정 및 상기 프레임에 관한 공개정보신호를 상기 공개채널을 통해 전송하는 제3과정을 포함하는 양자신호를 정기적인 프레임 단위로 생성 및 처리하는 방법을 제공한다.
- [15] 상기 제1과정은 상기 프레임동기정보를 매 프레임마다 또는 수 개의 프레임마다 전송하는 것이 바람직하다.
- [16] 또한, 상기 프레임동기정보는 관련된 프레임의 번호 정보를 포함하는 것이 바람직하다.
- [17] 또한, 상기 제2과정은 상기 양자정보를 프레임 단위로 전송하기에 앞서서, 상기 수신장치의 동기화 작업을 위한 동기화용 프레임을 상기 양자채널을 통해 전송하고 상기 동기화용 프레임에 관한 동기화 정보를 상기 공개채널을 통해 전송하는 것이 바람직하다.
- [18] 또한, 상기 제3과정은 상기 프레임에 관한 공개정보신호 중 상기 수신장치의 전처리 작업을 위한 공개정보신호를, 상기 수신장치의 후처리 작업을 위한 공개정보신호에 우선하여 전송하는 것이 바람직하다.
- [19] 더불어, 상기 방법은 각 프레임에서 생성된 키 정보를 양자 암호키로 사용할지 여부를, 상기 수신장치로부터 프레임처리완료 신호를 소정의 기준에 부합하게 수신하였는지 여부에 따라 결정하는 제4과정을 더 포함할 수 있다.
- [20] 본 실시예의 또다른 측면에 의하면, 양자 암호키 분배 시스템의 수신장치가 양자신호를 정기적인 프레임 단위로 수신 및 처리하는 방법에 있어서, 상기 양자 암호키 분배 시스템의 송신장치로부터 공개채널을 통해 프레임동기정보를 수신하여 프레임 동기화 작업을 수행하는 제1과정, 양자채널을 통해 전송된 프레임 단위의 양자정보가 실린 광자펄스열로부터 초기양자정보를 생성하는 제2과정, 상기 송신장치로부터 상기 공개채널을 통해 프레임 단위의 공개정보신호를 수신하는 제3과정 및 상기 프레임동기정보에 포함된 프레임의 번호 정보 또는 신호처리 정보를 기초로 상기 초기양자정보를 프레임 단위로 신호처리하는 제4과정을 포함하는 양자신호를 정기적인 프레임 단위로 수신 및 처리하는 방법을 제공한다.
- [21] 상기 방법은 상기 송신장치로부터 상기 공개채널을 통해 동기화용 프레임을 수신하고 상기 동기화용 프레임에 관한 동기화 정보를 상기 공개채널을 통해

수신하여, 상기 송신장치와의 동기화 작업을 수행하는 과정을 더 포함할 수 있다.

- [22] 또한, 상기 방법은 상기 송신장치 및 수신장치가 상대방에게 신호처리가 완료된 프레임에 관한 프레임처리완료 신호를 상기 공개채널을 통해 송신하는 과정을 더 포함할 수 있다.

발명의 효과

- [23] 본 실시예에 따르면, 수신부의 프레임수신 및 신호처리 완료 정보를 기다리지 않고 주기적으로 프레임을 계속 생성해서 보내므로 양자암호키분배 시스템의 운영 효율을 향상시키고 키생성률을 높일 수 있다.
- [24] 또한, 동기식 공개채널을 기반으로 하는 경우에는 보다 정확한 프레임동기신호를 전송할 수 있다.
- [25] 또한, 프레임마다 번호를 부여하여 신호처리에 활용하게 하므로 혼란을 방지하며 여러 프레임의 후처리 정보를 모아서 전송할 수 있으므로 공개채널의 활용효율을 높일 수 있다.
- [26] 더불어, 신호처리 완료신호를 확인하므로 최종 생성 키의 무결성을 보장할 수 있다.

도면의 간단한 설명

- [27] 도 1, 도 2 및 도 3은 본 발명의 일 실시예에 따른 양자 암호키 분배 시스템에 있어서, 프레임 단위의 양자정보신호 및 신호처리정보의 전송 방식을 예시한 도면이다.
- [28] 도 4는 본 발명의 일 실시예에 따른 정기적인 프레임 단위로 양자 신호를 생성 및 처리하는 양자 암호키 분배 시스템의 구성을 개략적으로 도시한 도면이다.

발명의 실시를 위한 형태

- [29] 이하, 본 발명의 일부 실시예들을 예시적인 도면을 통해 상세하게 설명한다. 각 도면의 구성요소들에 참조부호를 부가함에 있어서, 동일한 구성요소들에 대해서는 비록 다른 도면상에 표시되더라도 가능한 한 동일한 부호를 가지도록 하고 있음에 유의해야 한다. 또한, 본 발명을 설명함에 있어, 관련된 공지 구성 또는 기능에 대한 구체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명은 생략한다.
- [30] 또한, 본 발명의 구성 요소를 설명하는 데 있어서, 제 1, 제 2, A, B, (a), (b) 등의 용어를 사용할 수 있다. 이러한 용어는 그 구성 요소를 다른 구성 요소와 구별하기 위한 것일 뿐, 그 용어에 의해 해당 구성 요소의 본질이나 차례 또는 순서 등이 한정되지 않는다. 명세서 전체에서, 어떤 부분이 어떤 구성요소를 '포함', '구비'한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다. 또한, 명세서에 기재된 '...부', '모듈' 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어나 소프트웨어 또는

하드웨어 및 소프트웨어의 결합으로 구현될 수 있다.

- [31] 본 발명의 일 실시예에 따른 양자 암호키 분배 시스템에서, 송신부는 번호를 부여한 프레임단위의 양자신호를 주기적으로 전송하고 양자신호 전송 이전에 프레임동기를 위한 정보를 전송하며, 수신부는 프레임 동기정보를 해석하여 해당 양자신호를 수신 및 저장하고 프레임 번호 정보에 맞게 신호처리를 수행하여 양자암호키를 생성한다.
- [32] 도 1, 도 2 및 도 3은 본 발명의 일 실시예에 따른 양자 암호키 분배 시스템에 있어서, 프레임 단위의 양자정보신호 및 신호처리정보의 전송 방식을 예시한 도면이다.
- [33] 본 실시예에서 송신장치는 도 1과 같이 양자채널을 통해 양자정보신호를 프레임 단위로 전송하며, 각 프레임에 1~N의 번호를 부여한다. 또한 송신장치는 공개채널을 통해 프레임 동기정보를 보내거나 신호처리를 위한 정보를 보낼 때 해당 프레임번호 정보를 포함하여 전송한다. 수신장치는 양자정보신호를 수신할 때 프레임번호 정보와 함께 저장하여 신호처리시 활용하며, 공개채널을 통해 신호처리 정보를 전송할 때 해당 프레임번호를 함께 전송한다. 이를 통해 송수신장치 양자가 각 프레임에 해당하는 신호처리를 올바르게 수행할 수 있다.
- [34] 시스템의 운용효율을 높이기 위해서는 각 프레임간의 간격을 최소화하는 것이 바람직하다. 이상적인 경우는 각 프레임 사이에 단일광자 펄스가 없도록 만들어야 하지만, 수신부에서 프레임 동기신호를 수신하고 수신을 준비하는 시간 및 공개채널의 정보 송수신량 및 신호처리 시간 등을 고려하여 신호처리에 오버플로우(Overflow)가 발생하지 않도록 최소한의 간격을 설정하여야 할 것이다.
- [35] 한편, 각 프레임의 간격 동안에 송신장치는 단일광자 펄스를 전송하지 않을 수도 있으나, 계속하여 단일광자 펄스를 전송하는 것이 바람직하다. 각 프레임의 간격 동안에 전송되는 단일광자 펄스는 인코딩될 수도 있고, 그 반대일 수도 있다. 송신장치가 각 프레임 사이에 인코딩된 단일광자 펄스를 전송하더라도, 수신장치는 이러한 단일광자 펄스 또는 이에 실린 정보를 무시한다.
- [36] 공개채널 운영 시 프레임 동기신호는 가장 우선 순위가 높은 정보이므로 주기를 정확히 지켜서 전송해야 한다.
- [37] 신호처리 중 전처리에 해당하는 기저(Basis) 교환 및 디코이(Decoy) 정보 처리를 위한 정보는 해당 프레임 전송 직후에 바로 보내어 유효 비트 선택 과정을 수행하도록 하여 송수신부의 메모리 활용 부담을 줄이는 것이 바람직하다. 송수신부의 신호처리 장치와 연동되는 메모리에는 생성한 비트, 기저, 디코이 정보를 저장하며 전처리 이후에는 유효 비트만 선정하여 저장하고 나머지 정보는 버린다.
- [38] 프레임 동기정보는 도 1과 같이 매 프레임 전송 전에 주기적으로 보내거나 도 2와 같이 모든 프레임이 아닌 M (N 이하의 값) 개의 프레임마다 한 번씩 보낼 수 있다. 프레임 생성 및 전송과 신호처리에는 주기성이 있으므로 동기화 시간을

적절히 관리하면 프레임 단위의 양자정보를 송신하는 매 순간마다 프레임동기정보를 보낼 필요가 없다. 다만, 프레임 카운트 수 N (M 이 아님)이 1로 초기화되는 순간에는 프레임동기정보를 다시 보낼 필요가 있다.

[39] 프레임의 길이와 N 및 간격의 설정은 시스템 설치시에 시스템 운영자에 의해 임의의 값으로 설정되며, 송수신부는 그 설정 값을 미리 알고 있으므로 신호 생성, 전송, 수신, 저장 등을 해당 설정 값에 따라 주기적으로 진행할 수 있다.

[40] 도 4는 본 발명의 일 실시예에 따른 정기적인 프레임 단위로 양자 신호를 생성 및 처리하는 양자 암호키 분배 시스템의 구성을 개략적으로 도시한 도면이다.

[41] 프레임동기신호는 공개채널을 통해 전송되며 신호 취득, 전처리 등에 활용된다. 전처리 된 정보는 후처리 부로 전달되어 각 프레임에 맞는 후처리를 위한 정보를 송수신하는 과정과 연동되어 처리된다.

[42] 본 발명의 일 실시예에 따른 양자 암호키 분배 시스템(400)에서, 송신장치(410)는 자체 기준 클럭 신호에 타이밍(Timing)되어 광자펄스신호 생성 및 공개채널을 이용한 통신을 수행하고, 수신장치(450)는 동기식 공개채널 또는 별도의 클럭 전송 채널(도 4에 미도시)에서 클럭 정보를 추출하여 수신장치(450)의 기준 클럭 신호로 이용함으로써 송신장치(410)와 동기화한다.

[43] 또한, 송신장치(410)는 번호를 부여한 프레임단위의 양자신호를 주기적으로 전송하고, 양자신호 전송 이전에 프레임동기를 위한 정보가 포함된 프레임동기정보를 전송한다. 수신장치(450)는 프레임동기정보를 해석하여 해당 양자신호를 수신 및 저장하고 프레임 번호 정보에 맞게 신호처리를 수행하여 양자암호키를 생성한다.

[44] 도 4에 도시된 바와 같이, 송신장치(410)는 기준 클럭 신호를 생성하는 기준클럭 생성부(411), 기준 클럭 신호에 따라 양자채널을 통해 프레임 단위의 양자정보가 실린 광자 펄스열을 생성하는 광자펄스열 생성부(412), 기준 클럭 신호에 따라 프레임동기신호를 생성하여 공개채널 송수신부(414)에 전달하는 프레임동기신호 생성부(413), 공개채널을 통해 수신장치(450)와 공개정보가 실린 데이터를 교환하는 공개채널 송수신부(414), 프레임 단위로 베이스스 비교 및 디코딩 신호 처리 등의 전처리 작업을 수행하는 전처리부(415) 및 비트 오류 정정 등의 후처리 작업을 수행하는 후처리부(416)를 포함할 수 있다.

[45] 기준클럭 생성부(411)는 송신장치(410)와 수신장치(450)가 동기화되는 기준 클럭 신호를 생성하여, 동기화가 필요한 송신장치의 각 구성요소에 타이밍 신호를 공급한다.

[46] 광자펄스열 생성부(412)는 기준 클럭 신호에 따라 광자펄스를 생성하고, 이를 변조하여 프레임 단위로 양자정보를 광자펄스열을 양자채널을 통해 수신장치(450)에 전송한다. 광자펄스열 생성부(412)는 프레임 단위로 양자정보를 전송하기에 앞서, 수신장치(450)의 동기화 작업을 위한 동기화용 프레임을 전송할 수 있다. 광자펄스열 생성부(412)에는 동기화가 필요한 구성요소로서 광자펄스를 생성하는 레이저 다이오드, 광자펄스의 위상 또는

편광을 변조하는 변조기 등이 포함될 수 있다.

- [47] 공개채널 송수신부(414)는 기준 클럭 신호에 따라 동기화되어 공개채널을 통해 수신장치(450)와 프레임 단위로 구분된 공개정보를 포함하는 패킷을 송수신한다. 공개채널 송수신부(414)가 동기식으로 구현될 경우에는 수신장치(450)가 공개채널로부터 클럭 정보를 적절하게 추출할 수 있도록, 스크램블링 기법(Scrambling Scheme)을 사용하여 패킷에 0, 1이 적당히 섞이도록 하는 것이 바람직하다. 또한, 공개채널 송수신부(414)는 광자펄스열 생성부(412)가 동기화용 프레임을 전송하는 것에 맞춰 동기화 정보가 포함된 공개정보를 수신장치에 전송할 수 있다.
- [48] 전처리부(415)는 프레임 단위로 베이스 비교 및 디코딩 신호 처리 등의 전처리 작업을 수행하는 과정에서 공개채널 송수신부(414)를 통해 수신장치(450)와 프레임 단위의 전처리 정보를 주고받는다.
- [49] 후처리부(416)는 전처리부(415)로부터 전처리 작업 결과 생성된 걸러진 키(Sifted Key)를 전달받아 비트 오류 정정 등의 후처리 작업을 수행하는 과정에서 공개채널 송수신부(414)를 통해 수신장치(450)와 프레임 단위의 후처리 정보를 주고 받는다.
- [50] 도 4에 도시된 바와 같이, 수신장치(450)는 상기 공개채널 송수신부(456)의 출력 데이터로부터 클럭 신호를 추출하거나 별도의 클럭 채널을 통해 전송된 신호로부터 클럭 신호를 추출하는 동기클럭신호 추출부(451), 상기 추출된 클럭 신호에 동기화된 기준 클럭 신호를 생성하는 기준클럭 생성부(452), 송신장치(410)로부터 양자정보가 실린 광자펄스열을 수신하는 광자 검출부(453), 광자 검출부(453)의 출력 신호를 기반으로 유효 검출 정보를 판별하는 신호판별부(454), 공개채널을 통해 송신장치(410)와 공개정보가 실린 데이터를 교환하는 공개채널 송수신부(456), 공개채널 송수신부(456)가 수신한 프레임동기정보를 포함한 패킷으로부터 프레임 시작을 알리는 트리거 신호(Trigger)를 신호판별부(454) 및 전처리부(457)에 제공하는 프레임동기신호 처리부(455), 상기 생성된 기준 클럭 신호에 동기화되어 상기 신호판별부(454)가 취득한 양자정보를 프레임 단위로 베이스 비교 및 디코딩 신호 처리 등의 전처리 작업을 수행하는 전처리부(457) 및 상기 전처리부(457)로부터 걸러진 키를 전달받아 상기 생성된 기준 클럭 신호에 동기화되어, 프레임 단위로 비트 오류 정정 등의 후처리 작업을 수행하는 후처리부(458)를 포함할 수 있다.
- [51] 동기클럭신호 추출부(451)는 공개채널 또는 별도의 동기 채널로부터 송신장치(410)에서 사용된 기준 클럭 신호를 추출한다. 즉, 동기클럭신호 추출부(451)는 공개채널 송수신부(456)가 수신한 패킷의 상승 및 하강 시점을 검출하여 데이터 변화를 나타내는 전이 펄스를 생성하고, 이를 기초로 패킷에 포함된 클럭 신호를 추출하거나 별도의 동기 채널을 통해 전송된 클럭 신호로부터 클럭 신호를 추출할 수 있다. 특히 동기클럭신호 추출부(451)는 시스템의 부팅, 초기화 단계 등에서 프레임동기정보에 앞서

- 송신장치(410)로부터 전송된 동기화 정보를 포함한 패킷을 이용할 수 있다.
- [52] 기준클럭 생성부(452)는 동기클럭신호 추출부(451)가 추출한 클럭 신호에 동기화된 기준 클럭 신호를 생성한다.
- [53] 광자 검출부(453)는 기준 클럭 신호를 바탕으로, 송신장치(410)에서 전송된 광자펄스의 도착 타이밍에 동기화되어 광자펄스열을 검출한다.
- [54] 신호판별부(454)는 광자 검출기의 출력신호를 이용하여 유효 검출 정보를 판별하여 신호처리를 위한 정보를 생성하여 전처리부(457)에 전달하고, 전처리부(457)는 해당 정보를 프레임 단위로 저장한 후 처리한다.
- [55] 공개채널 송수신부(456)는 기준 클럭 신호에 따라 동기화되어 공개채널을 통해 송신장치(410)와 프레임 단위로 구분된 공개정보를 포함하는 패킷을 송수신한다.
- [56] 프레임동기신호 처리부(455)은 공개채널 송수신부(456)가 수신한 프레임동기정보를 포함한 패킷으로부터 프레임 시작을 알리는 트리거 신호(Trigger)를 신호판별부(454) 및 전처리부(457)에 제공한다.
- [57] 전처리부(457)는 프레임 단위로 베이스 비교 및 디코딩 신호 처리 등의 전처리 작업을 수행하는 과정에서 공개채널 송수신부(456)를 통해 송신장치(410)와 프레임 단위의 전처리 정보를 주고받는다.
- [58] 후처리부(458)는 전처리부(457)로부터 전처리 작업 결과 생성된 걸러진 키(Sifted Key)를 전달받아 비트 오류 정정 등의 후처리 작업을 수행하는 과정에서 공개채널 송수신부(456)를 통해 송신장치(410)와 프레임 단위의 후처리 정보를 주고 받는다.
- [59] 한편, 송신장치(410)에서 공개채널을 통한 프레임동기 패킷 송신, 광자펄스열 생성 및 변조 과정에서 발생할 수 있는 시간 지터(Jitter)의 양이나, 수신장치(450)에서 프레임동기 패킷 수신, 광자펄스열 수신 및 양자정보 획득 및 획득된 양자정보를 신호처리하여 양자 암호키를 생성하는 과정에서 발생할 수 있는 시간 지터의 양은 시스템(400) 동작 속도의 한 주기를 고려하여 관리되어야 한다. 예컨대, 100 MHz 동작속도를 가진 시스템은 10 ns 이내의 지터를 갖도록 패킷을 처리하는 것이 바람직하며, 이를 초과할 경우 생성된 양자 암호키의 오류율이 높아질 수 있다. 이를 위해 FPGA(Field Programmable Gate Array)와 같은 병렬 처리 및 실시간 신호처리 기능을 구현할 수 있는 소자를 사용할 수 있다.
- [60] 이상의 설명은 본 실시예의 기술 사상을 예시적으로 설명한 것에 불과한 것으로서, 본 실시예가 속하는 기술 분야에서 통상의 지식을 가진 자라면 본 실시예의 본질적인 특성에서 벗어나지 않는 범위에서 다양한 수정 및 변형이 가능할 것이다. 따라서, 본 실시예들은 본 실시예의 기술 사상을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시예에 의하여 본 실시예의 기술 사상의 범위가 한정되는 것은 아니다. 본 실시예의 보호 범위는 아래의 청구범위에 의하여 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술

사상은 본 실시예의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

[61] (부호의 설명)

[62] 400: 양자 암호키 분배 시스템 410: 송신장치

[63] 411: 기준클럭 생성부 412: 광자펄스열 생성부

[64] 413: 프레임동기정보 발생부 414: 공개채널 송수신부

[65] 415: 전처리부 416: 후처리부

[66] 450: 수신장치 451: 동기클럭신호 추출부

[67] 452: 기준클럭 생성부 453: 광자 검출부

[68] 454: 신호판별부 455: 프레임동기정보 처리부

[69] 456: 공개채널 송수신부 457: 전처리부

[70] 458: 후처리부

[71]

[72] CROSS-REFERENCE TO RELATED APPLICATION

[73] 본 특허출원은 2012년 10월 30일 한국에 출원한 특허출원번호 제 10-2012-0121540 호에 대해 미국 특허법 119(a)조(35 U.S.C § 119(a))에 따라 우선권을 주장하면, 그 모든 내용은 참고문헌으로 본 특허출원에 병합된다. 아울러, 본 특허출원은 미국 이외에 국가에 대해서도 위와 동일한 이유로 우선권을 주장하면 그 모든 내용은 참고문헌으로 본 특허출원에 병합된다.

청구범위

- [청구항 1] 양자 암호키 분배 시스템의 송신장치에 있어서,
양자정보를 번호가 부여된 프레임 단위로 생성하여 양자채널을
통해 주기적으로 전송하기 위한 광자펄스열 생성부;
공개채널을 통해 상기 양자 암호키 분배 시스템의 수신장치와
통신하기 위한 공개채널 송수신부;
매 프레임마다 또는 수 개의 프레임마다, 상기 수신장치의 프레임
동기화 작업을 위한 프레임동기정보를 생성하여 상기 공개채널
송수신부를 통해 상기 수신장치에 전송하기 위한 프레임동기정보
발생부; 및
상기 공개채널 송수신부를 통해 상기 프레임별 공개정보를
송수신하여, 상기 양자정보를 프레임단위로 신호처리하기 위한
신호처리부
를 포함하는, 정기적인 프레임 단위로 양자 신호를 생성 및
처리하는 송신장치.
- [청구항 2] 제1항에 있어서,
상기 공개정보신호 및 상기 프레임동기정보는,
관련된 프레임의 번호 정보를 포함하는 것을 특징으로 하는,
정기적인 프레임 단위로 양자 신호를 생성 및 처리하는 송신장치.
- [청구항 3] 제1항에 있어서,
상기 양자정보를 프레임 단위로 전송하기에 앞서서,
상기 광자펄스열 생성기는 동기화용 프레임을 상기 양자채널을
통해 전송하고, 상기 공개채널 송수신부는 상기 동기화용
프레임에 관한 공개정보인 동기화 정보를 공개채널을 통해
전송하는 것을 특징으로 하는, 정기적인 프레임 단위로 양자
신호를 생성 및 처리하는 송신장치.
- [청구항 4] 제1항에 있어서,
상기 공개채널 송수신부는,
상기 프레임에 관한 공개정보신호를 전송함에 있어서,
상기 수신장치의 전처리 작업을 위한 공개정보신호를 상기
수신장치의 후처리 작업을 위한 공개정보신호에 우선하여
전송하는 것을 특징으로 하는, 정기적인 프레임 단위로 양자
신호를 생성 및 처리하는 송신장치.
- [청구항 5] 양자 암호키 분배 시스템의 수신장치에 있어서,
공개채널을 통해 상기 양자 암호키 분배 시스템의 송신장치와
통신하기 위한 공개채널 송수신부;
상기 공개채널 송수신부를 통해 상기 송신장치로부터

프레임동기정보를 수신하여 프레임 동기화 작업을 수행하기 위한 프레임동기 정보 처리부;

양자채널을 통해 상기 송신장치로부터 전송되는 광자펄스신호를 검출하기 위한 단일광자검출부; 및

상기 프레임동기정보에 포함된 프레임의 번호 정보 및 상기 공개채널 송수신부를 통해 상기 송신장치와 송수신한 프레임 단위의 신호처리 정보를 기초로, 상기 단일광자검출부의 출력으로부터 검출된 양자정보를 프레임 단위로 신호처리하기 위한 신호처리부

를 포함하는, 정기적인 프레임 단위로 양자 신호를 생성 및 처리하는 수신장치.

[청구항 6]

양자 암호키 분배 시스템의 송신장치가 양자신호를 정기적인 프레임 단위로 생성 및 처리하는 방법에 있어서,

상기 양자 암호키 분배 시스템의 수신장치의 프레임 동기화 작업을 위한 프레임동기정보를 공개채널을 통해 전송하는 제1과정;

양자정보를 번호가 부여된 프레임 단위로 생성하여 양자채널을 통해 상기 수신장치에 주기적으로 전송하는 제2과정; 및

상기 양자정보의 프레임별 공개정보신호를 상기 공개채널을 통해 전송하는 제3과정

을 포함하는, 양자신호를 정기적인 프레임 단위로 생성 및 처리하는 방법.

[청구항 7]

제6항에 있어서,

상기 제1과정은,

상기 프레임동기정보를 매 프레임마다 또는 수 개의 프레임마다 전송하는 것을 특징으로 하는, 양자신호를 정기적인 프레임 단위로 생성 및 처리하는 방법.

[청구항 8]

제7항에 있어서,

상기 프레임동기정보는,

관련된 프레임의 번호 정보를 포함하는 것을 특징으로 하는, 양자신호를 정기적인 프레임 단위로 생성 및 처리하는 방법.

[청구항 9]

제6항에 있어서,

상기 제2과정은,

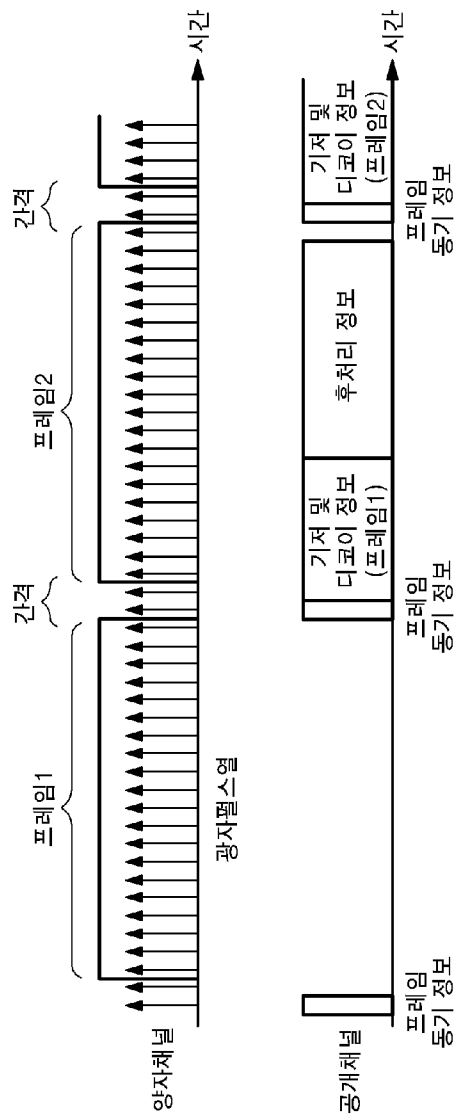
상기 양자정보를 프레임 단위로 전송하기에 앞서서, 상기 수신장치의 동기화 작업을 위한 동기화용 프레임을 상기

양자채널을 통해 전송하고 상기 동기화용 프레임에 관한 동기화 정보를 상기 공개채널을 통해 전송하는 것을 특징으로 하는,

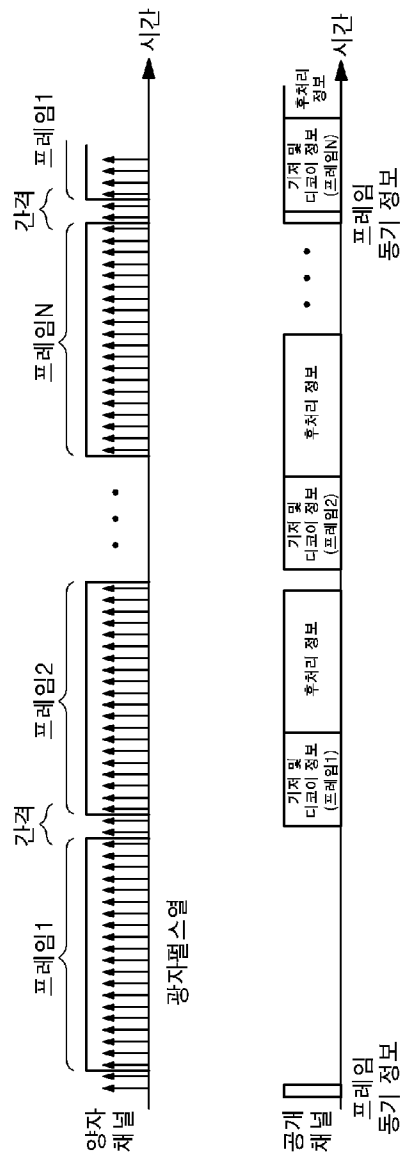
양자신호를 정기적인 프레임 단위로 생성 및 처리하는 방법.

- [청구항 10] 제6항에 있어서,
상기 제3과정은,
상기 프레임에 관한 공개정보신호 중 상기 수신장치의 전처리 작업을 위한 공개정보신호를, 상기 수신장치의 후처리 작업을 위한 공개정보신호에 우선하여 전송하는 것을 특징으로 하는, 양자신호를 정기적인 프레임 단위로 생성 및 처리하는 방법.
- [청구항 11] 제6항에 있어서,
각 프레임에서 생성된 키 정보를 양자 암호키로 사용할지 여부를, 상기 수신장치로부터 프레임처리완료 신호를 소정의 기준에 부합하게 수신하였는지 여부에 따라 결정하는 제4과정을 더 포함하는 것을 특징으로 하는, 양자신호를 정기적인 프레임 단위로 생성 및 처리하는 방법.
- [청구항 12] 양자 암호키 분배 시스템의 수신장치가 양자신호를 정기적인 프레임 단위로 수신 및 처리하는 방법에 있어서,
상기 양자 암호키 분배 시스템의 송신장치로부터 공개채널을 통해 프레임동기정보를 수신하여 프레임 동기화 작업을 수행하는 제1과정;
양자채널을 통해 전송된 프레임 단위의 양자정보가 실린 광자펄스열로부터 초기양자정보를 생성하는 제2과정;
상기 송신장치로부터 상기 공개채널을 통해 프레임 단위의 공개정보신호를 수신하는 제3과정; 및
상기 프레임동기정보에 포함된 프레임의 번호 정보 또는 신호처리 정보를 기초로 상기 초기양자정보를 프레임 단위로 신호처리하는 제4과정을 포함하는, 양자신호를 정기적인 프레임 단위로 수신 및 처리하는 방법.
- [청구항 13] 제12항에 있어서,
상기 송신장치로부터 상기 공개채널을 통해 동기화용 프레임을 수신하고 상기 동기화용 프레임에 관한 동기화 정보를 상기 공개채널을 통해 수신하여, 상기 송신장치와의 동기화 작업을 수행하는 과정을 더 포함하는 것을 특징으로 하는, 양자신호를 정기적인 프레임 단위로 수신 및 처리하는 방법.
- [청구항 14] 제12항에 있어서,
상기 송신장치 및 수신장치가 상대방에게 신호처리가 완료된 프레임에 관한 프레임처리완료 신호를 상기 공개채널을 통해 송신하는 과정을 더 포함하는 것을 특징으로 하는, 양자신호를 정기적인 프레임 단위로 수신 및 처리하는 방법.

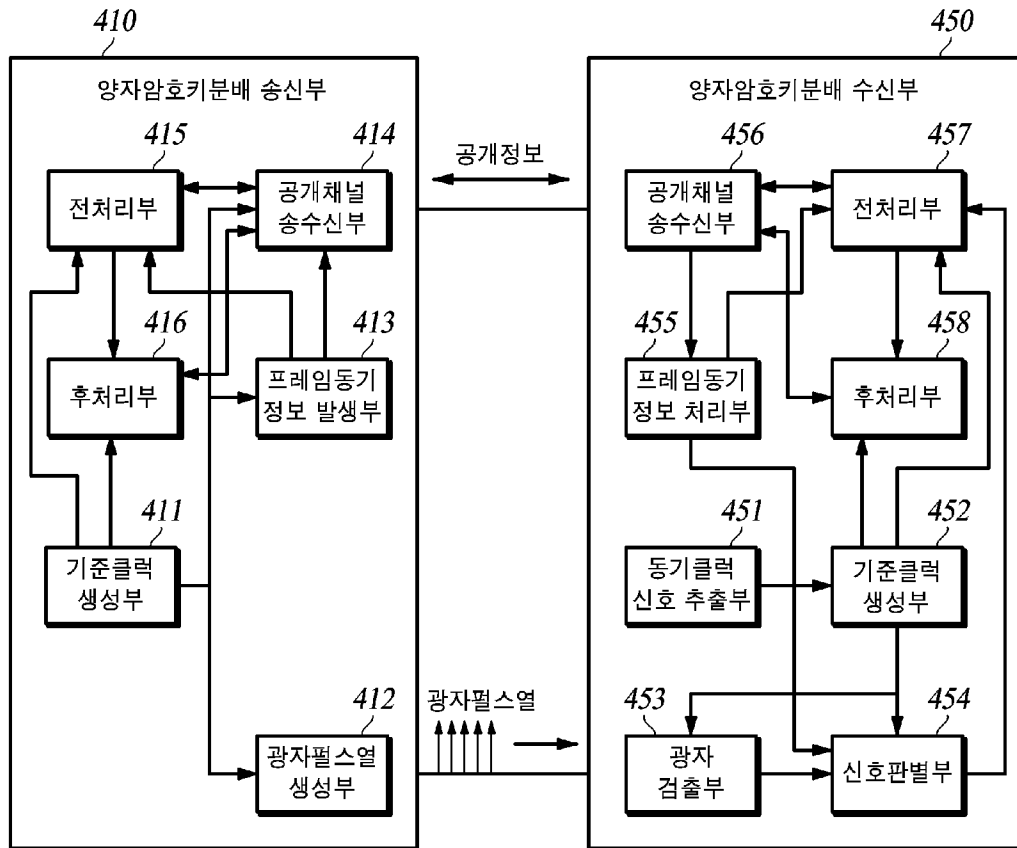
[Fig. 1]



[Fig. 2]



[Fig. 4]

400

INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2013/007511**A. CLASSIFICATION OF SUBJECT MATTER****H04L 9/12(2006.01)i, H04L 9/08(2006.01)i**

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L 9/12; H04K 1/00; H04L 27/28; H04L ; H04L 9/00; H04L 12/28; H04L 12/56; H04L 9/08

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean Utility models and applications for Utility models: IPC as above

Japanese Utility models and applications for Utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & Keywords: quantum information, transmit, reception, frame, signal processing

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2004-073235 A2 (MAGIQ TECHNOLOGIES INC.) 26 August 2004 See pages 4-23; and figures 1A-8.	1-14
A	US 2007-0025551 A1 (HARRISON, Keith Alexander et al.) 01 February 2007 See paragraphs [0019]-[0038]; and figures 1-5.	1-14
A	JP 2010-273267 A (NEC CORP.) 02 December 2010 See paragraphs [0019]-[0022]; and figures 1, 2.	1-14
A	US 2005-0190921 A1 (SCHLAFER, John D. et al.) 01 September 2005 See paragraphs [0030]-[0065]; and figures 4-15.	1-14
A	US 2012-0045003 A1 (LI, Qinghua et al.) 23 February 2012 See paragraphs [0007]-[0024]; and figures 1, 2.	1-14

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

23 DECEMBER 2013 (23.12.2013)

Date of mailing of the international search report

24 DECEMBER 2013 (24.12.2013)

Name and mailing address of the ISA/KR



Korean Intellectual Property Office
Government Complex-Daejeon, 189 Seonsa-ro, Daejeon 302-701,
Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/KR2013/007511

Patent document cited in search report	Publication date	Patent family member	Publication date
WO 2004-073235 A2	26/08/2004	EP 1522166 A2	13/04/2005
		EP 1522166 B1	27/02/2008
		EP 1537698 A2	08/06/2005
		EP 1590918 A2	02/11/2005
		JP 04353946 B2	28/10/2009
		JP 04358829 B2	04/11/2009
		JP 2006-512879 A	13/04/2006
		JP 2006-513678 A	20/04/2006
		JP 2006-514512 A	27/04/2006
		US 2004-0161109 A1	19/08/2004
		US 2005-0066721 A1	31/03/2005
		US 2006-0018475 A1	26/01/2006
		US 2006-0059343 A1	16/03/2006
		US 7036364 B2	02/05/2006
		US 7227955 B2	05/06/2007
		WO 2004-073228 A2	26/08/2004
		WO 2004-073228 A3	18/11/2004
		WO 2004-073234 A2	26/08/2004
		WO 2004-073234 A3	18/11/2004
		WO 2004-073235 A3	14/04/2005
US 2007-0025551 A1	01/02/2007	GB 0611936 D0	26/07/2006
		GB 2427317 A	20/12/2006
		GB 2427317 B	19/05/2010
		GB 2427336 A	20/12/2006
		GB 2427336 B	20/01/2010
		GB 2430775 A	04/04/2007
		GB 2430845 A	04/04/2007
		GB 2430846 A	04/04/2007
		GB 2430847 A	04/04/2007
		GB 2430848 A	04/04/2007
		GB 2430850 A	04/04/2007
		US 07721955 B2	25/05/2010
		US 07864958 B2	04/01/2011
		US 08050411 B2	01/11/2011
		US 08054976 B2	08/11/2011
		US 08250363 B2	21/08/2012
		US 2007-0014415 A1	18/01/2007
		US 2007-0016534 A1	18/01/2007
		US 2007-0016794 A1	18/01/2007
		US 2007-0074276 A1	29/03/2007
		US 2007-0074277 A1	29/03/2007
		US 2007-0101410 A1	03/05/2007
		US 2007-0172054 A1	26/07/2007
		US 2007-0177424 A1	02/08/2007
JP 2010-273267 A	02/12/2010	NONE	
US 2005-0190921 A1	01/09/2005	US 2006-0222180 A1	05/10/2006

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/KR2013/007511

Patent document cited in search report	Publication date	Patent family member	Publication date
US 2012-0045003 A1	23/02/2012	US 7627126 B1	01/12/2009
		CN 103168431 A	19/06/2013
		EP 2609689 A2	03/07/2013
		KR 10-2013-0047761 A	08/05/2013
		US 8446971 B2	21/05/2013
		WO 2012-027060 A2	01/03/2012
		WO 2012-027060 A3	26/04/2012

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H04L 9/12(2006.01)i, H04L 9/08(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

H04L 9/12; H04K 1/00; H04L 27/28; H04L ; H04L 9/00; H04L 12/28; H04L 12/56; H04L 9/08

조사된 기술분야에 속하는 최소문헌 이외의 문헌

한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))

eKOMPASS(특허청 내부 검색시스템) & 키워드: 양자정보, 송신, 수신, 프레임, 신호처리

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
X	WO 2004-073235 A2 (MAGIQ TECHNOLOGIES INC.) 2004.08.26 페이지 4-23; 및 도면 1A-8 참조.	1-14
A	US 2007-0025551 A1 (KEITH ALEXANDER HARRISON et al.) 2007.02.01 단락 [0019]-[0038]; 및 도면 1-5 참조.	1-14
A	JP 2010-273267 A (NEC CORP.) 2010.12.02 단락 [0019]-[0022]; 및 도면 1, 2 참조.	1-14
A	US 2005-0190921 A1 (JOHN D. SCHLAFFER et al.) 2005.09.01 단락 [0030]-[0065]; 및 도면 4-15 참조.	1-14
A	US 2012-0045003 A1 (QINGHUA LI et al.) 2012.02.23 단락 [0007]-[0024]; 및 도면 1, 2 참조.	1-14

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

“A” 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

“T” 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

“E” 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

“X” 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

“L” 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

“Y” 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

“O” 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

“&” 동일한 대응특허문헌에 속하는 문헌

“P” 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

국제조사의 실제 완료일

2013년 12월 23일 (23.12.2013)

국제조사보고서 발송일

2013년 12월 24일 (24.12.2013)

ISA/KR의 명칭 및 우편주소

 대한민국 특허청
(302-701) 대전광역시 서구 청사로 189,
4동 (둔산동, 정부대전청사)

팩스 번호 +82-42-472-7140

심사관

김도원

전화번호 +82-42-481-5560



국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
WO 2004-073235 A2	2004/08/26	EP 1522166 A2 EP 1522166 B1 EP 1537698 A2 EP 1590918 A2 JP 04353946 B2 JP 04358829 B2 JP 2006-512879 A JP 2006-513678 A JP 2006-514512 A US 2004-0161109 A1 US 2005-0066721 A1 US 2006-0018475 A1 US 2006-0059343 A1 US 7036364 B2 US 7227955 B2 WO 2004-073228 A2 WO 2004-073228 A3 WO 2004-073234 A2 WO 2004-073234 A3 WO 2004-073235 A3	2005/04/13 2008/02/27 2005/06/08 2005/11/02 2009/10/28 2009/11/04 2006/04/13 2006/04/20 2006/04/27 2004/08/19 2005/03/31 2006/01/26 2006/03/16 2006/05/02 2007/06/05 2004/08/26 2004/11/18 2004/08/26 2004/11/18 2005/04/14
US 2007-0025551 A1	2007/02/01	GB 0611936 D0 GB 2427317 A GB 2427317 B GB 2427336 A GB 2427336 B GB 2430775 A GB 2430845 A GB 2430846 A GB 2430847 A GB 2430848 A GB 2430850 A US 07721955 B2 US 07864958 B2 US 08050411 B2 US 08054976 B2 US 08250363 B2 US 2007-0014415 A1 US 2007-0016534 A1 US 2007-0016794 A1 US 2007-0074276 A1 US 2007-0074277 A1 US 2007-0101410 A1 US 2007-0172054 A1 US 2007-0177424 A1	2006/07/26 2006/12/20 2010/05/19 2006/12/20 2010/01/20 2007/04/04 2007/04/04 2007/04/04 2007/04/04 2007/04/04 2007/04/04 2010/05/25 2011/01/04 2011/11/01 2011/11/08 2012/08/21 2007/01/18 2007/01/18 2007/01/18 2007/03/29 2007/03/29 2007/05/03 2007/07/26 2007/08/02
JP 2010-273267 A	2010/12/02	없음	
US 2005-0190921 A1	2005/09/01	US 2006-0222180 A1	2006/10/05

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
		US 7627126 B1	2009/12/01
US 2012-0045003 A1	2012/02/23	CN 103168431 A	2013/06/19
		EP 2609689 A2	2013/07/03
		KR 10-2013-0047761 A	2013/05/08
		US 8446971 B2	2013/05/21
		WO 2012-027060 A2	2012/03/01
		WO 2012-027060 A3	2012/04/26