

(51) 국제특허분류:
H04L 9/08 (2006.01)

(21) 국제출원번호: PCT/KR2017/013755

(22) 국제출원일: 2017년 11월 29일 (29.11.2017)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2016-0174482 2016년 12월 20일 (20.12.2016) KR

(71) 출원인: 고려대학교 산학협력단 (KOREA UNIVERSITY RESEARCH AND BUSINESS FOUNDATION) [KR/KR]; 02841 서울시 성북구 안암로 145, Seoul (KR).

(72) 발명자: 허준 (HEO, Jun); 06359 서울시 강남구 광평로 10길 6, 206동 103호, Seoul (KR). 이성훈 (LEE, Sung Hoon); 02577 서울시 동대문구 무학로 184, 202호, Seoul (KR).

(74) 대리인: 심경식 등 (SHIM, Kyoung-Shik et al.); 06719 서울시 서초구 반포대로 10, 신원빌딩 4층 (서초동), Seoul (KR).

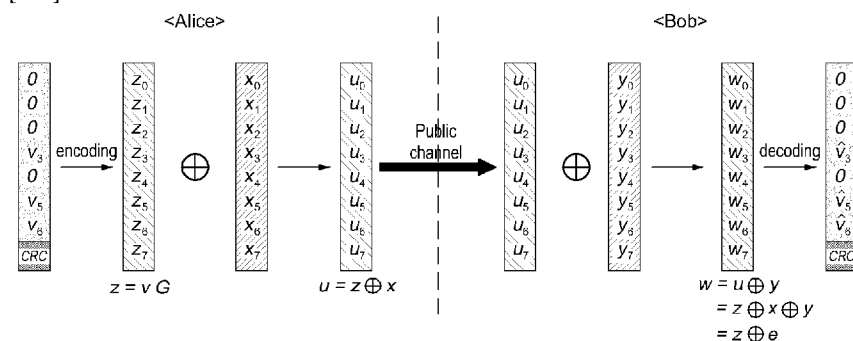
(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KW, KZ, LA, LC, LK, LR, LS, 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 국내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, 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,

(54) Title: SIGNAL TRANSMITTING APPARATUS AND SIGNAL RECEIVING APPARATUS FOR INFORMATION RECONCILIATION FOR QUANTUM KEY DISTRIBUTION

(54) 발명의 명칭: 양자 키 분배의 정보 조정을 위한 신호 송신 장치 및 수신 장치

[도5]



(57) Abstract: The present invention relates to a signal transmitting apparatus for information reconciliation for quantum key distribution and a signal receiving apparatus for information reconciliation for quantum key distribution for estimating a quantum key of a transmitting end by using a transmission/reception object character string, the signal transmitting apparatus comprising: an encoding unit for generating an encoding test character string that is a character string encoded by multiplying a test character string that is a character string including at least one arbitrary bit value, by a pre-stored generation matrix; a transmission/reception object character string generating unit for generating a transmission/reception object character string, on the basis of the encoding test character string and a quantum key of a signal transmitting end, which is an arbitrary character string generated through quantum key distribution; and a character string transmission unit for transmitting, via a public channel, the transmission/reception object character string to a signal receiving end.

(57) 요약서: 적어도 하나의 임의의 비트값을 포함하는 문자열인 시험 문자열에 미리 저장된 생성 행렬을 곱하여 시험 문자열을 부호화한 문자열인 부호화 시험 문자열을 생성하는 부호화부, 부호화 시험 문자열 및 양자 키 분배를 통해 생성된 임의의 문자열인 신호 송신단 측 양자 키에 기초하여 송수신 대상 문자열을 생성하는 송수신 대상 문자열 생성부 및 송수신 대상 문자열을 공개 채널을 통해 신호 수신단에 전송하는 문자열 송신부를 포함하는, 양자 키 분배의 정보 조정을 위한 신호 송신 장치 및 송수신 대상 문자열을 활용하여 송신단 측 양자 키를 추정하는 양자 키 분배의 정보 조정을 위한 신호 수신 장치에 관한 것이다.



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 제21조(3))

(88) 국제조사보고서 공개일:

2018 년 8 월 16 일 (16.08.2018)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2017/013755

A. CLASSIFICATION OF SUBJECT MATTER

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 9/08; H03M 13/00; G06N 99/00; H04L 9/32; G11B 20/18

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, key distribution, CRC, test, matrix

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	KR 10-2006-0059853 A (MITSUBISHI ELECTRIC CORPORATION) 02 June 2006 See claim 1; and figure 2.	1-10
Y	US 2016-0248586 A1 (LOS ALAMOS NATIONAL SECURITY, LLC.) 25 August 2016 See paragraphs [0018], [0095]; and figure 1.	1-10
Y	KR 10-2015-0002085 A (INDUSTRIAL COOPERATION FOUNDATION CHONBUK NATIONAL UNIVERSITY) 07 January 2015 See paragraph [0071]; and figure 1.	7
A	US 2015-0195087 A1 (KABUSHIKI KAISHA TOSHIBA) 09 July 2015 See paragraphs [0054]-[0057]; claims 1-10; and figure 8.	1-10
A	KR 10-2015-0097290 A (KOREA UNIVERSITY RESEARCH AND BUSINESS FOUNDATION) 26 August 2015. See paragraphs [0034]-[0039]; claims 1-6; and figure 1.	1-10



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

29 MAY 2018 (29.05.2018)

Date of mailing of the international search report

29 MAY 2018 (29.05.2018)

Name and mailing address of the ISA/KR

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

Facsimile No. +82-42-481-8578

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/KR2017/013755

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-2006-0059853 A	02/06/2006	AU 2003-262096 A1	08/04/2004
		CA 2499357 A1	01/04/2004
		CN 100706147 A	07/12/2005
		EP 1542390 A1	15/06/2005
		JP 2004-112278 A	08/04/2004
		JP 4290401 B2	08/07/2009
		NO 20042553 A	21/12/2004
		US 2006-0059403 A1	16/03/2006
		US 7609839 B2	27/10/2009
		WO 2004-028074 A1	01/04/2004
US 2016-0248586 A1	25/08/2016	WO 2015-102694 A2	09/07/2015
		WO 2015-102694 A3	20/08/2015
KR 10-2015-0002085 A	07/01/2015	KR 10-1502972 B1	17/03/2015
US 2015-0195087 A1	09/07/2015	JP 2015-130623 A	16/07/2015
		JP 6165637 B2	19/07/2017
		US 9569731 B2	14/02/2017
KR 10-2015-0097290 A	26/08/2015	KR 10-1559075 B1	19/10/2015

A. 발명이 속하는 기술분류(국제특허분류(IPC)) H04L 9/08(2006.01)i																				
B. 조사된 분야 조사된 최소문헌(국제특허분류를 기재) H04L 9/08; H03M 13/00; G06N 99/00; H04L 9/32; G11B 20/18 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: 양자, 키 분배, CRC, 시험, 행렬																				
C. 관련 문헌 <table border="1"> <thead> <tr> <th>카테고리*</th> <th>인용문헌명 및 관련 구절(해당하는 경우)의 기재</th> <th>관련 청구항</th> </tr> </thead> <tbody> <tr> <td>Y</td> <td>KR 10-2006-0059853 A (미쓰비시덴키 가부시키가이샤) 2006.06.02 청구항 1; 및 도면 2 참조.</td> <td>1-10</td> </tr> <tr> <td>Y</td> <td>US 2016-0248586 A1 (LOS ALAMOS NATIONAL SECURITY, LLC) 2016.08.25 단락 [0018], [0095]; 및 도면 1 참조.</td> <td>1-10</td> </tr> <tr> <td>Y</td> <td>KR 10-2015-0002085 A (전북대학교산학협력단) 2015.01.07 단락 [0071]; 및 도면 1 참조.</td> <td>7</td> </tr> <tr> <td>A</td> <td>US 2015-0195087 A1 (KABUSHIKI KAISHA TOSHIBA) 2015.07.09 단락 [0054]-[0057]; 청구항 1-10; 및 도면 8 참조.</td> <td>1-10</td> </tr> <tr> <td>A</td> <td>KR 10-2015-0097290 A (고려대학교 산학협력단) 2015.08.26. 단락 [0034]-[0039]; 청구항 1-6; 및 도면 1 참조.</td> <td>1-10</td> </tr> </tbody> </table>			카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항	Y	KR 10-2006-0059853 A (미쓰비시덴키 가부시키가이샤) 2006.06.02 청구항 1; 및 도면 2 참조.	1-10	Y	US 2016-0248586 A1 (LOS ALAMOS NATIONAL SECURITY, LLC) 2016.08.25 단락 [0018], [0095]; 및 도면 1 참조.	1-10	Y	KR 10-2015-0002085 A (전북대학교산학협력단) 2015.01.07 단락 [0071]; 및 도면 1 참조.	7	A	US 2015-0195087 A1 (KABUSHIKI KAISHA TOSHIBA) 2015.07.09 단락 [0054]-[0057]; 청구항 1-10; 및 도면 8 참조.	1-10	A	KR 10-2015-0097290 A (고려대학교 산학협력단) 2015.08.26. 단락 [0034]-[0039]; 청구항 1-6; 및 도면 1 참조.	1-10
카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항																		
Y	KR 10-2006-0059853 A (미쓰비시덴키 가부시키가이샤) 2006.06.02 청구항 1; 및 도면 2 참조.	1-10																		
Y	US 2016-0248586 A1 (LOS ALAMOS NATIONAL SECURITY, LLC) 2016.08.25 단락 [0018], [0095]; 및 도면 1 참조.	1-10																		
Y	KR 10-2015-0002085 A (전북대학교산학협력단) 2015.01.07 단락 [0071]; 및 도면 1 참조.	7																		
A	US 2015-0195087 A1 (KABUSHIKI KAISHA TOSHIBA) 2015.07.09 단락 [0054]-[0057]; 청구항 1-10; 및 도면 8 참조.	1-10																		
A	KR 10-2015-0097290 A (고려대학교 산학협력단) 2015.08.26. 단락 [0034]-[0039]; 청구항 1-6; 및 도면 1 참조.	1-10																		
☐ 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 “E” 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌 “L” 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌 “O” 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌 “P” 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌 “T” 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌 “X” 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신구성 또는 진보성이 없는 것으로 본다. “Y” 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다. “&” 동일한 대응특허문헌에 속하는 문헌																				
국제조사의 실제 완료일 2018년 05월 29일 (29.05.2018)		국제조사보고서 발송일 2018년 05월 29일 (29.05.2018)																		
ISA/KR의 명칭 및 우편주소  대한민국 특허청 (35208) 대전광역시 서구 청사로 189, 4동 (둔산동, 정부대전청사) 팩스 번호 +82-42-481-8578		심사관 노지명 전화번호 +82-42-481-8528 																		

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2006-0059853 A	2006/06/02	AU 2003-262096 A1 CA 2499357 A1 CN 100706147 A EP 1542390 A1 JP 2004-112278 A JP 4290401 B2 NO 20042553 A US 2006-0059403 A1 US 7609839 B2 WO 2004-028074 A1	2004/04/08 2004/04/01 2005/12/07 2005/06/15 2004/04/08 2009/07/08 2004/12/21 2006/03/16 2009/10/27 2004/04/01
US 2016-0248586 A1	2016/08/25	WO 2015-102694 A2 WO 2015-102694 A3	2015/07/09 2015/08/20
KR 10-2015-0002085 A	2015/01/07	KR 10-1502972 B1	2015/03/17
US 2015-0195087 A1	2015/07/09	JP 2015-130623 A JP 6165637 B2 US 9569731 B2	2015/07/16 2017/07/19 2017/02/14
KR 10-2015-0097290 A	2015/08/26	KR 10-1559075 B1	2015/10/19