(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
01 June 2023 (01.06.2023)

WIPO | PCT

(10) International Publication Number
WO 2023/096586 A3

(51) International Patent Classification:
H04L 9/08 (2006.01)

(21) International Application Number:
PCT/SG2022/050865

(22) International Filing Date:
28 November 2022 (28.11.2022)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10202113249R 29 November 2021 (29.11.2021) SG

(72) Inventors; and

(71) Applicants: **LIM, Han Chuen** [SG/SG]; 18 Sin Ming Lane, #08-36, Singapore 573960 (SG). **LIU, Maotong** [—/SG]; 18 Sin Ming Lane, #08-36, Singapore 573960 (SG).

(74) Agent: **OWEN, Samuel Man Hon**; Marks & Clerk Singapore LLP, Tanjong Pagar Post Office, P.O. Box 636, Singapore 910816 (SG).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ,

(54) Title: QUANTUM KEY GENERATION METHOD AND SYSTEM

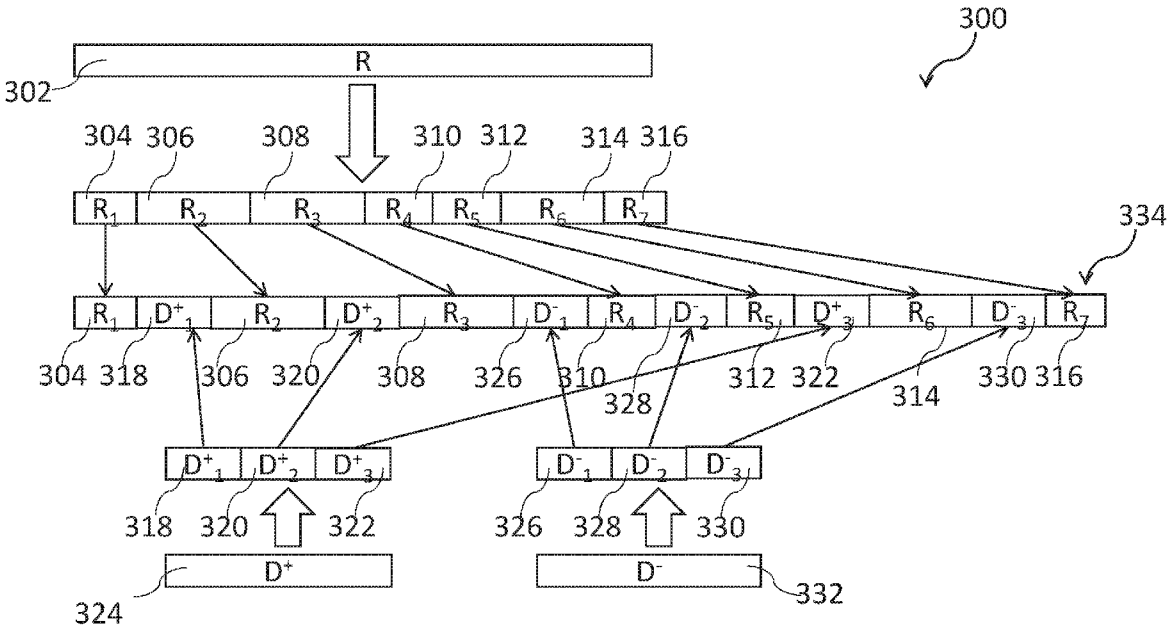

Fig. 5a

(57) Abstract: A quantum key generation method is disclosed herein. In a specific embodiment, the method comprises receiving a quantum transmission from a quantum transmission device 208, 508, 510, 520, the quantum transmission including quantum bits for obtaining a quantum key, detecting the quantum bits from the quantum transmission to obtain a detected bit-sequence; obtaining a derived value from the detected bit-sequence; and verifying that the derived value is consistent with an expected value of the derived value corresponding to a test value of a same statistical characteristic that is dependent on a statistical property of a key generation bit-sequence 334, 1334 used for encoding or decoding of quantum bits to detect tampering. A quantum key generation system 200 is also disclosed.

WO 2023/096586 A3

[Continued on next page]

TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, 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).

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

Published:

— *with international search report (Art. 21(3))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(88) Date of publication of the international search report:

22 June 2023 (22.06.2023)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SG2022/050865

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(2006.01); G06F 21/34(2013.01); G06N 10/00(2019.01); H04B 10/70(2013.01)

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
Japanese utility models and applications for utility models

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

eKOMPASS(KIPO internal) & Keywords: quantum key generation, key generation bit-sequence, quantum bit, test block, statistical characteristic, tampering

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	GUO-FANG SHI et al., `Quantum secure dialogue by using single photons', Optics Communications Volume 283, Issue 9, pages 1984-1986, 01 May 2010 section 2	1-42
A	LU YANG et al., `Quantum secure direct communication with entanglement source and single-photon measurement', Science China Physics, Mechanics & Astronomy, Vol. 63, Article number: 110311(2020), 25 August 2020 section 2	1-42
A	YU-BO SHENG et al., `One-step quantum secure direct communication', Science Bulletin, Volume 67, Issue 4, 04 November 2021 section 2	1-42
A	CN 111460421 A (NANJING UNIVERSITY) 28 July 2020 (2020-07-28) paragraphs [0029]-[0068]; and figures 1-6	1-42
A	US 2021-0152346 A1 (EAGLE TECHNOLOGY, LLC) 20 May 2021 (2021-05-20) paragraphs [0023]-[0063]; and figures 1-9B	1-42

☐ 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
"D" document cited by the applicant in the international application
"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	Date of mailing of the international search report
22 May 2023	**22 May 2023**

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office **189 Cheongsa-ro, Seo-gu, Daejeon** **35208, Republic of Korea**	**BYUN, SUNG CHEAL**
Facsimile No. **+82-42-481-8578**	Telephone No. **+82-42-481-8262**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/SG2022/050865

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 111460421 A	28 July 2020	US 2021-0374589 A1	02 December 2021
US 2021-0152346 A1	20 May 2021	US 11050559 B2	29 June 2021