



(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

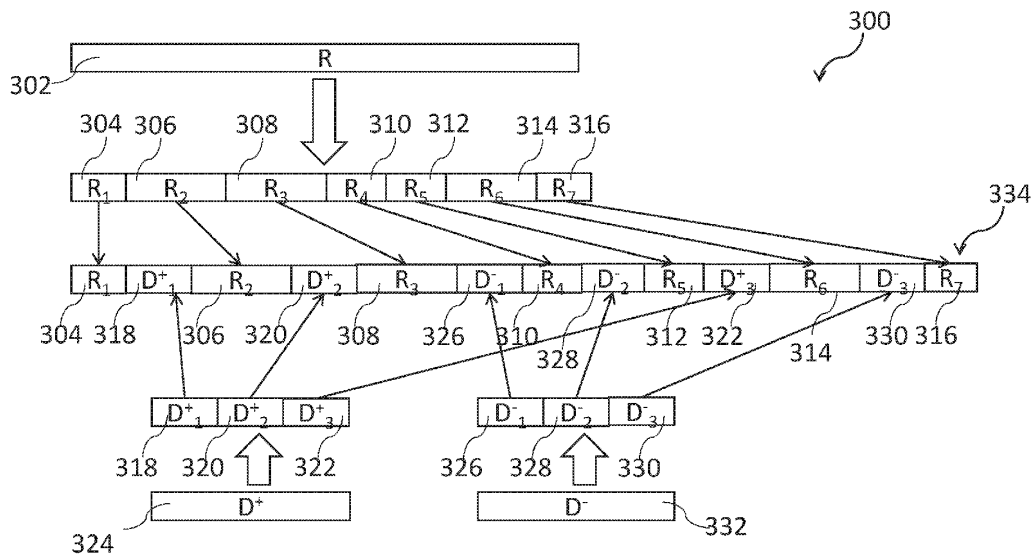


Fig. 5a

(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.

[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:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*