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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 November 2022 (24.11.2022)

WIPO | PCT

(10) International Publication Number
WO 2022/243657 A1

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

(21) International Application Number:
PCT/GB2022/051193

(22) International Filing Date:
11 May 2022 (11.05.2022)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2107113.9 18 May 2021 (18.05.2021) GB

(71) Applicant: **ARQIT LIMITED** [GB/GB]; 7th Floor, Nova North, 11 Bressenden Place, London Greater London SW1E 5BY (GB).

(72) Inventors: **YEOMANS, Andrew**; 17 Hollyfield Close, Tring Hertfordshire HP23 5PL (GB). **IQBAL, Omar**; 16 Whittington Road, Petersfield Hampshire GU31 4FP (GB). **DAVID, Bestwick**; 26 Church Street, Great Baddow, Chelsford Essex CM2 7HY (GB).

(74) Agent: **HILL, Justin John** et al.; Dentons UK and Middle East LLP, One Fleet Place, London Greater London EC4M 7RA (GB).

(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, 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, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU,

(54) **Title:** RANDOM NUMBER GENERATION IN QUANTUM KEY DISTRIBUTION

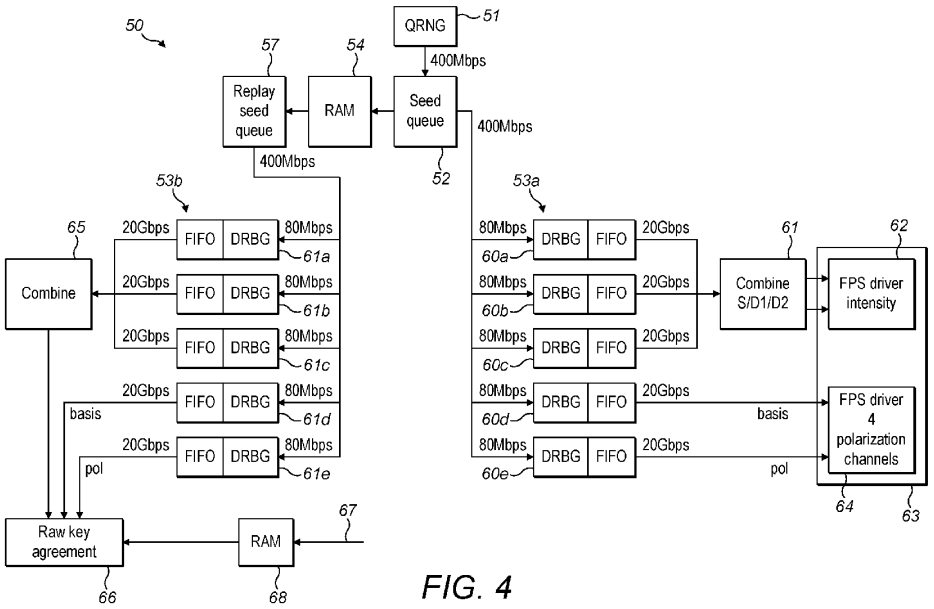



FIG. 4

(57) **Abstract:** A method of operating a quantum key distribution (QKD) system comprising: using at least one quantum random number generator (QRNG) to generate a random number string, and storing the random number string; providing the random number string to a first cryptographically secure pseudo-random number generator (CSPRNG) which uses random numbers of the random number string as seeds to generate respective first strings of pseudo-random numbers; using the first strings of pseudo-random numbers to encode photons or pulses transmitted by a transmitter of the QKD system; after a predetermined delay, providing the stored random number string to a second CSPRNG which uses random numbers of the random number string as seeds to generate respective second strings of pseudo-random numbers, the second CSPRNG being identically configured to the first CSPRNG; using the second strings of pseudo-random numbers, together with information regarding encoded photons or pulses received by a receiver of the QKD system, to

*[Continued on next page]*

WO 2022/243657 A1

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, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, 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, 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).

**Published:**

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

carry out raw key agreement and post processing to agree secure keys between the transmitter and the receiver.