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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
04 August 2022 (04.08.2022)

WIPO | PCT

(10) International Publication Number
WO 2022/162390 A1

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

(21) International Application Number:
PCT/GB2022/050243

(22) International Filing Date:
28 January 2022 (28.01.2022)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

2101310.7	29 January 2021 (29.01.2021)	GB
2106980.2	14 May 2021 (14.05.2021)	GB

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

(72) Inventors: **YEOMANS, Andrew**; 17 Hollyfield Close, Tring, Hertfordshire HP23 5PL (GB). **MURPHY, Michael**; 26 River Mill One, Station Road, Lewisham, London, Greater London SE13 5FL (GB). **COHEN, Oliver**; 14 Nightingale Close, Winchester, Hampshire SO22 5QA (GB). **IQBAL, Omar**; 16 Whittington Road, Petersfield, Hampshire GU31 4FP (GB). **BROWN, James**; 27 Highfield Avenue, Oxford, Oxfordshire OX3 7LR (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, IR, IS, IT, JO, JP, KE, KG, KH, KN,

(54) Title: KEY EXCHANGE PROTOCOL FOR QUANTUM NETWORK

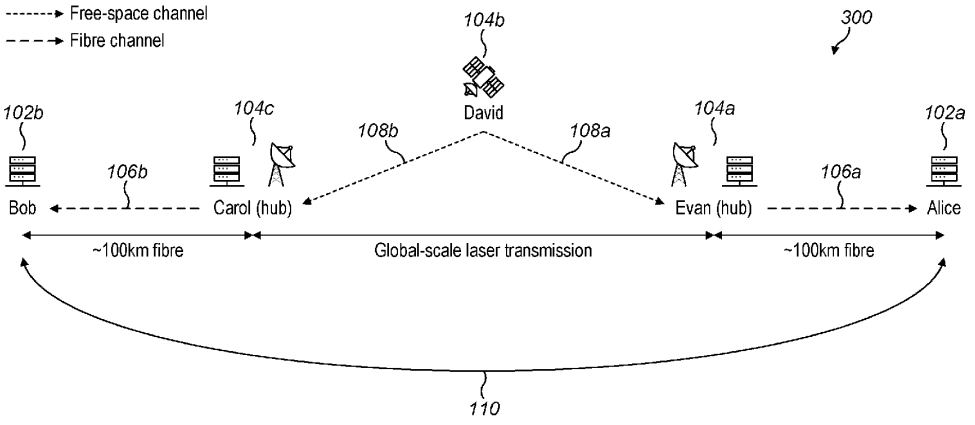

FIG. 3A

(57) Abstract: Methods, apparatus, and systems are provided for performing a key exchange between a first device, a second device, and an intermediary device. The intermediary device transmitting: a first secret symbol string over a first quantum channel to the first device; a first basis set over a first communication channel to the first device. The intermediary device; a second secret symbol string over a second quantum channel to the second device; a second basis set over a second communication channel to the second device. The intermediary device generating a third symbol string based on combining the first and second secret symbol strings and transmitting to the second device, via the second communication channel, data representative of the third symbol string. The first device and second device perform a quantum key exchange and sifting based on the corresponding received first and second secret symbol strings and first and second basis sets, and a fourth set of symbols generated by the second device generates a fourth set of symbols based on combining the second received secret symbols with the received third symbol string.

WO 2022/162390 A1

[Continued on next page]

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, 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))*