

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

(19) World Intellectual Property
Organization
International Bureau

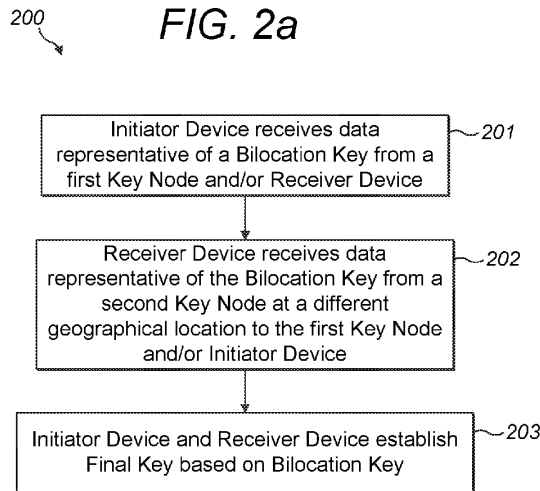
(43) International Publication Date
21 July 2022 (21.07.2022)



(10) International Publication Number
WO 2022/153051 A1

- (51) **International Patent Classification:**
H04L 9/08 (2006.01)
- (21) **International Application Number:**
PCT/GB2022/050069
- (22) **International Filing Date:**
13 January 2022 (13.01.2022)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
2100434.6 13 January 2021 (13.01.2021) GB
- (71) **Applicant:** **ARQIT LIMITED** [GB/GB]; 7th Floor, Nova North 11 Bressenden Place, London SW1E 5BY (GB).
- (72) **Inventors:** **WEBB, David**; 39 Heathfield Road, Seaford Sussex BN25 1TJ (GB). **BURNS, Daryl**; Rosetree Cottage, Sunnyfield Lane, Cheltenham Gloucestershire CR0 IEZ
- (GB), **WILLIAMS, David**; Woldringfold House, Brighton Road, Lower Beeding, Horsham Surrey RH13 6TL (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, 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,

(54) **Title:** SYSTEM AND METHOD FOR KEY ESTABLISHMENT



(57) **Abstract:** Methods, apparatus, and systems are provided for establishing a key between a first device and a second device using a quantum-secure network, the quantum-secure network comprising a first key node and a second key node, the first key node including a set of quantum distributed keys and the second key node including the same set of quantum distributed keys. The first device receives data representative of first key establishment data from at least the first key node and the second device for use in calculating a Bilocation Key. The Bilocation key is based on a selected quantum distributed key from the set of quantum distributed keys of the first key node and second key node. The second device receives data representative of second key establishment data from at least the first device for use in requesting the Bilocation Key from the second key node. The Bilocation Key is calculated by the second key node based on the selected quantum distributed key from the set of quantum distributed keys of the second key node. The first and second devices use their corresponding Bilocation Keys to generate the same key based on an agreed portion of the first key establishment data and second key establishment data.

WO 2022/153051 A1

[Continued on next page]

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))*