

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
27 January 2022 (27.01.2022)



(10) International Publication Number
WO 2022/018432 A1

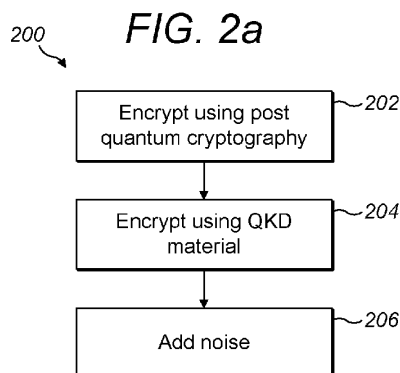
- (51) **International Patent Classification:**
H04L 9/00 (2006.01) *H04L 9/08* (2006.01)
- (21) **International Application Number:**
PCT/GB2021/051863
- (22) **International Filing Date:**
20 July 2021 (20.07.2021)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
2011219.9 20 July 2020 (20.07.2020) GB
- (71) **Applicant:** **ARQIT LIMITED** [GB/GB]; 1st Floor, 3 More London Riverside, More London Place, London Greater London SE1 2RE (GB).
- (72) **Inventors:** **BURNS, Daryl**; Rosetree Cottage, Sunnyfield Lane, Up Hatherley, Cheltenham Gloucestershire GL51 6JD (GB). **CHILDE, Barry**; Reciprocity, 11 Albany Road, Seaford Sussex BN25 2QB (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, 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))

(54) **Title:** KEY EXCHANGE PROTOCOL



(57) **Abstract:** Methods, apparatus, and systems are provided for performing a secure communication between a sender device and receiver device. This includes encapsulating or encrypting, by the sender device, a message using a post-quantum cryptographic algorithm and quantum key (QK) material derived from QK distribution with a receiver device. Noise is added, by the sender device, to the encapsulated or encrypted message. The sender device sends the noisy encapsulated/encrypted message to the receiver device. On receipt of the noisy encapsulated or encrypted message from the sender device, the receiver device decapsulates or decrypts the received message using corresponding QK used by the sender device. The receiver device decapsulates or decrypts the QK decapsulated/decrypted message using the corresponding post-quantum cryptographic algorithm used by the sender, and the receiver device outputs or uses the message sent by the sender.

WO 2022/018432 A1