

(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 2022/018431 A1

(51) International Patent Classification:
H04L 9/08 (2006.01) *H04L 29/08* (2006.01)
H04L 29/06 (2006.01)

(21) International Application Number:
PCT/GB2021/051862

(22) International Filing Date:
20 July 2021 (20.07.2021)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2011220.7 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: **WILLIAMS, David**; Woldingfold House,
Brighton Road, Lower Beeding, Horsham Surrey RH13
6TL (GB). **CHILDE, Barry**; Reciprocity, 11 Albany Road,
Seaford Sussex BN25 2QB (GB).

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

(54) Title: QUANTUM STREAMING

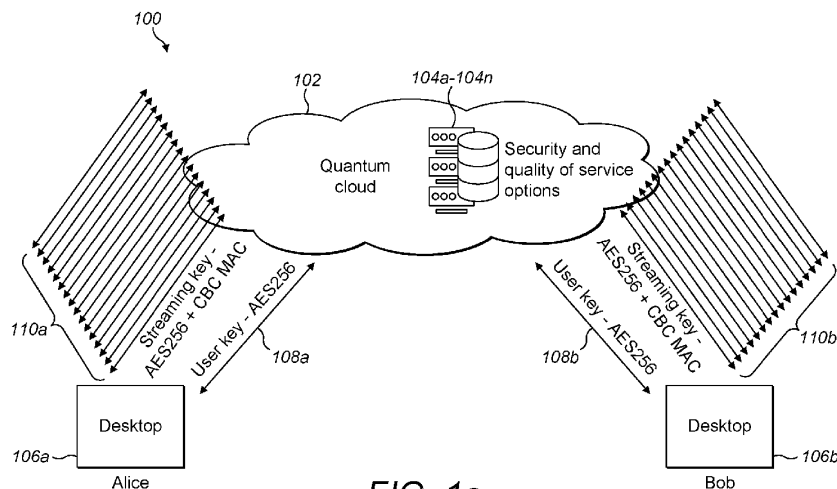


FIG. 1a

(57) Abstract: Method(s), system(s), apparatus are provided for quantum safe quantum streaming between a first endpoint device and second endpoint device via a server of a quantum cloud platform. Splitting, at the first endpoint device, a data item into a plurality of data shards that allow reconstruction of the data item. Encrypting, at the first endpoint device, each of the data shards separately using a first cryptographic key shared between the first endpoint device and the second endpoint device. Establishing, between the first endpoint device and the server, a first plurality of secure channels with the server of the quantum cloud platform using a second cryptographic key, the second cryptographic key shared between the endpoint and the server. Transmitting, from the first endpoint device to the server, the plurality of encrypted shards towards the second endpoint device via the server over the plurality of secure channels. Receiving, at the server, the plurality of encrypted data shards of the data item transmitted from the first endpoint device over

[Continued on next page]

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))

the first plurality of secure channels, each data shard encrypted using the first cryptographic key known only to the first endpoint device and the second endpoint device. Securely storing, by the server, the encrypted data shards of the data item in a secure storage of the quantum cloud platform. In response to the second endpoint logging onto the quantum cloud platform, establishing a second plurality of secure channels with the second endpoint using a third cryptographic key, the third cryptographic key shared between the second endpoint device and the server. Retrieving the encrypted data shards of the data item from secure storage. Transmitting the encrypted data shards over the second plurality of secure channels to the second endpoint device. Receiving, at the second endpoint, a plurality of encrypted data shards of the encrypted data item from the server over the second plurality. Decrypting the encrypted data shards using the first cryptographic key to reconstruct the data item transferred from the first endpoint device to the second endpoint device.