



(51) International Patent Classification:
H04L 9/08 (2006.01) **H04L 9/14** (2006.01)

(21) International Application Number:
PCT/GB2022/050164

(22) International Filing Date:
21 January 2022 (21.01.2022)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2100910.5 22 January 2021 (22.01.2021) GB

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

(72) Inventors: **CHILDE, Barry**; Reciprocity, 11 Albany Road, Seaford Sussex BN25 2QB (GB). **DAPRE, Jon**; 68 Pierrefondes Avenue, Farnborough Hampshire GU14 8PA (GB). **WEBB, David**; 39 Heathfield Road, Seaford Sussex BN25 1TJ (GB). **WILLIAMS, David**; Woldingfold House, Brighton Road, Lower Beeding, Horsham Surrey RH13 6TL (GB). **BROWN, James**; 27 Highfield Avenue,

Oxford Oxfordshire OX3 7LR (GB). **MARI, Michael**; 43 Westbourne Gardens, Hove Sussex BN3 5PL (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, 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,

(54) Title: A SYSTEM AND METHOD FOR TRUSTLESS KEY PROVISIONING

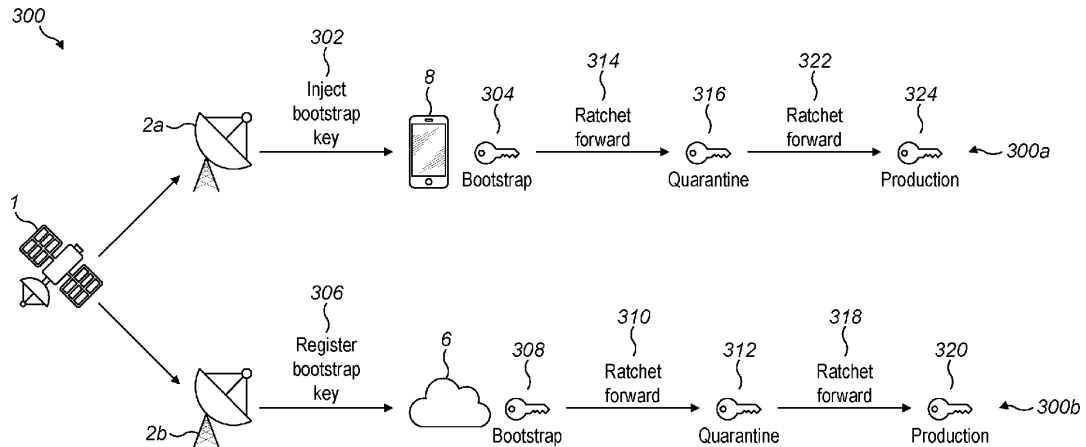


FIG. 3

(57) Abstract: A method of encryption key provisioning comprising: providing, by a quantum computing safe method, a shared secret data to a device and also to a security service; using the provided shared secret data to provide a root key; and using the root key as a basis for a sequence of stages, wherein each stage comprises an operation which converts a start key into a different generated key, and the same stages are carried out in parallel at the device and at the security service; wherein the root key is used as the start key for a first stage of the sequence, and a generated key produced by each stage of the sequence, except for the final stage of the sequence, is used as a start key for a next stage of the sequence; and wherein the generated keys produced by the last stage of the sequence at the device and at the security service are symmetric keys.

[Continued on next page]

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))