

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
11 August 2022 (11.08.2022)



(10) International Publication Number
WO 2022/167163 A1

- (51) **International Patent Classification:**
H04L 9/08 (2006.01) *H04L 9/32* (2006.01)
- (21) **International Application Number:**
PCT/EP2022/050116
- (22) **International Filing Date:**
05 January 2022 (05.01.2022)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
2101590.4 05 February 2021 (05.02.2021) GB
- (71) **Applicant:** NCHAIN LICENSING AG [CH/CH]; Grafenauweg 6, 6300 Zug (CH).
- (72) **Inventor:** PETTIT, Michaela; c/o nChain Licensing AG, 30 Market Place, London W1W 8AP (GB).
- (74) **Agent:** MARTYN JAMES TOWNSEND; PAGE WHITE & FARRER, Bedford House, John Street, London Greater London WC1N 2BF (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,

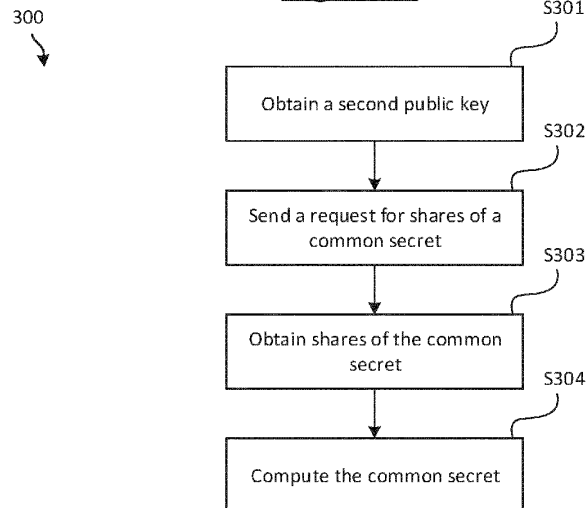
CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, 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:** THRESHOLD KEY EXCHANGE

Figure 3



(57) **Abstract:** A computer-implemented method of generating a shared cryptographic key based on at least one shared secret, wherein each participant belonging to a first group has a respective share of a first secret, the first secret having a first threshold and a corresponding first public key, wherein a second coordinator has a second public key corresponding to a second secret, wherein the second coordinator is configured to generate the same shared cryptographic key.

WO 2022/167163 A1