

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
23 December 2021 (23.12.2021)



(10) International Publication Number
WO 2021/254702 A1

(51) International Patent Classification:
H04L 9/08 (2006.01) *H04L 9/32* (2006.01)

(21) International Application Number:
PCT/EP2021/062941

(22) International Filing Date:
17 May 2021 (17.05.2021)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2009062.7 15 June 2020 (15.06.2020) 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).

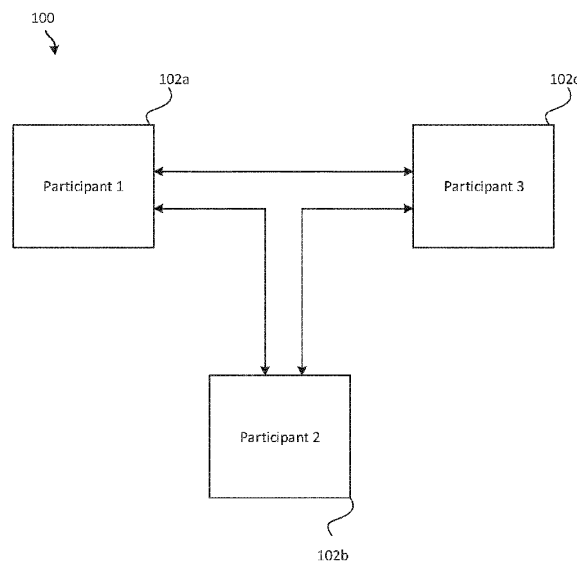
(74) Agent: TOWNSEND, Martyn, James; Page White & Farrer, Bedford House John Street, London WC1N 2BF (GB).

(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,

(54) Title: GENERATING SECRET SHARES

Figure 1



(57) Abstract: A computer-implemented method of generating shares of a shared secret, wherein each of a group of participants has a respective first secret share of the shared secret, wherein the method is performed by a first participant of the group and comprises: generating a respective blinding share of a shared blinding secret, obtaining at least a threshold number of respective intermediary shares from each of the first group of participants, wherein each respective intermediary share is generated based on a respective blinding share and a respective first secret share; generating an intermediary value based on each of the obtained intermediary shares; and generating a respective second secret share of the shared secret, wherein the respective second secret share is generated based on the intermediary value and the respective blinding share.

[Continued on next page]

WO 2021/254702 A1

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))