

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
05 May 2022 (05.05.2022)



(10) International Publication Number
WO 2022/089865 A1

(51) International Patent Classification:

H04L 9/32 (2006.01) H04L 9/30 (2006.01)
H04L 9/08 (2006.01)

(21) International Application Number:

PCT/EP2021/076686

(22) International Filing Date:

28 September 2021 (28.09.2021)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

2017103.9 28 October 2020 (28.10.2020) 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; 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.

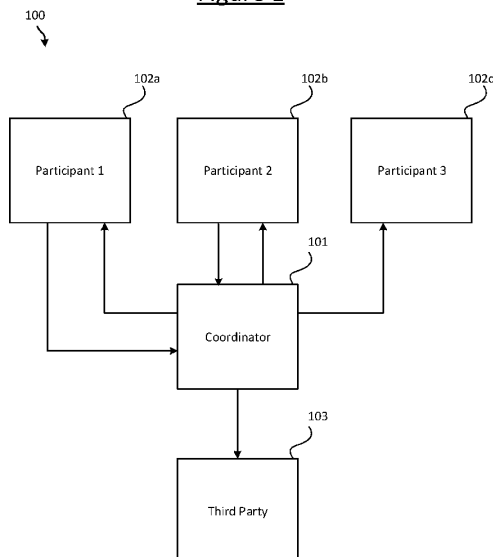
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, 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: IDENTIFYING DENIAL-OF-SERVICE ATTACKS

Figure 1



(57) Abstract: A computer-implemented method of identifying a denial-of-service attack during a threshold signature scheme, wherein each participant has respective shares of first and second shared secrets, wherein the method is performed by a first participant of the group and comprises: calculating a first target share; calculating a target value based on the first target share and a first predetermined amount of other target shares; calculating a target public key corresponding to the target value; calculating a first verification share based on the first share of the first shared secret and a public key corresponding to the second shared secret; calculating a verification public key based on at least the first verification share and a second predetermined amount of other verification shares; and determining whether at least one other participant is attempting a denial-of-service attack based on whether the verification public key matches the target public key.

WO 2022/089865 A1