

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
07 April 2022 (07.04.2022)



(10) International Publication Number
WO 2022/069035 A1

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

(21) International Application Number:
PCT/EP2020/077414

(22) International Filing Date:
30 September 2020 (30.09.2020)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **DFINITY STIFTUNG** [CH/CH]; Stockerstrasse 47, 8002 Zürich (CH).

(72) Inventors: **CAMENISCH, Jan**; c/o Dfinity Stiftung Stockerstrasse 47, 8002 Zürich (CH). **CERULLI, Andrea**; c/o Dfinity Stiftung Stockerstrasse 47, 8002 Zürich (CH). **DRIJVERS, Manu**; c/o Dfinity Stiftung Stockerstrasse 47, 8002 Zürich (CH). **GROTH, Jens**; c/o Dfinity Stiftung Stockerstrasse 47, 8002 Zürich (CH).

(74) Agent: **E. BLUM & CO. AG**; Vorderberg 11, 8044 Zürich (CH).

(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: REDISTRIBUTION OF SECRET SHARINGS

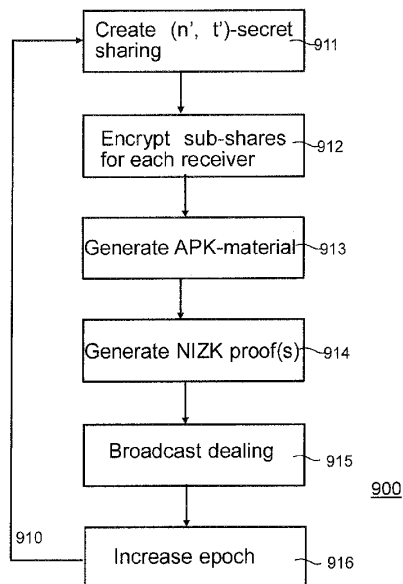


FIG. 9

(57) Abstract: Method for redistribution of a (n,t)-secret sharing of a secret s from a set of dealers to a set of receivers. The method comprises performing by each of at least the threshold number t of dealers, - creating a (n,t)-secret sharing of its respective secret share, - creating a set of ciphertexts comprising for each receiver one encrypted sub-share of the n-1 secret sub-shares of its respective secret share and being encrypted with respect to a public encryption key of the respective receiver. The public encryption key is a key of a public-key encryption scheme. - generating a non-interactive zero-knowledge proof that the set of ciphertexts jointly contain a redistribution of its secret share - broadcasting a dealing to the set of receivers, the dealing comprising the set of ciphertexts for the set of receivers and the corresponding non-interactive zero-knowledge proof.

WO 2022/069035 A1