

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
15 September 2022 (15.09.2022)



(10) International Publication Number
WO 2022/188963 A1

- (51) **International Patent Classification:**
H04L 9/32 (2006.01) *H04L 29/06* (2006.01)
- (21) **International Application Number:**
PCT/EP2021/056003
- (22) **International Filing Date:**
10 March 2021 (10.03.2021)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (71) **Applicant:** **DFINITY STIFTUNG** [CH/CH]; Stocker-
strasse 47, 8002 Zürich (CH).
- (72) **Inventor:** **GROTH, Jens**; c/o Dfinity Stiftung Stocker-
strasse 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:** MULTI-PARTY COMPUTATIONS IN A DISTRIBUTED NETWORK

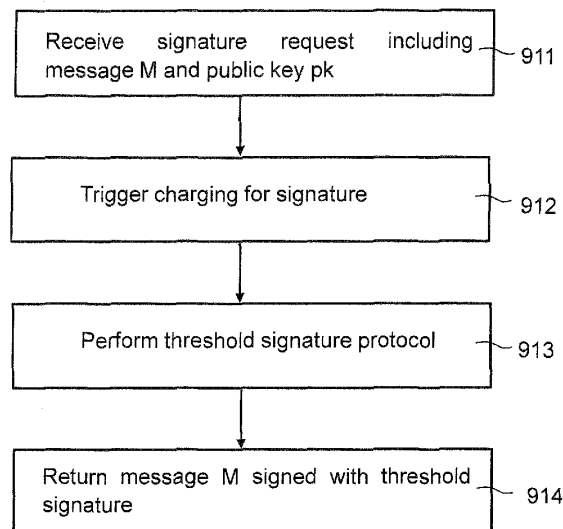


FIG. 9

(57) **Abstract:** Embodiments of the invention relate to a distributed network. The distributed network comprises a replicated system computing cluster comprising system computational units. The system computational units comprise deterministic subunits configured to perform a deterministic and replicated computation across the replicated system computing cluster and non-deterministic subunits for performing non-deterministic computations. The replicated system computing cluster is configured to perform a secure multi-party computation, in particular a computation of a threshold-signature.

WO 2022/188963 A1