



(51) International Patent Classification:

H04L 9/08 (2006.01) **G06F 21/64** (2013.01)
G06F 21/62 (2013.01) **H04L 9/32** (2006.01)

(21) International Application Number:

PCT/EP2020/087410

(22) International Filing Date:

21 December 2020 (21.12.2020)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

63/046,371 30 June 2020 (30.06.2020) US

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

(72) Inventors: **CAMENISCH, Jan**; c/o Dfinity Stiftung Stockerstrasse 47, 8002 Zürich (CH). **DRIJVERS, Manu**; c/o Dfinity Stiftung Stockerstrasse 47, 8002 Zürich (CH). **GRANSTRÖM, Johan**; c/o Dfinity Stiftung Stockerstrasse 47, 8002 Zürich (CH). **KASHITSYN, Roman**; c/o Dfinity Stiftung Stockerstrasse 47, 8002 Zürich (CH). **NEVEN, Gregory**; c/o Dfinity Stiftung Stockerstrasse 47, 8002 Zürich (CH). **PIGNOLET, Yvonne-Anne**; c/o Dfinity Stiftung Stockerstrasse 47, 8002 Zürich (CH). **WIL-**

LIAMS, Dominic; 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).

(54) Title: VERIFICATION KEY GENERATION IN DISTRIBUTED NETWORKS

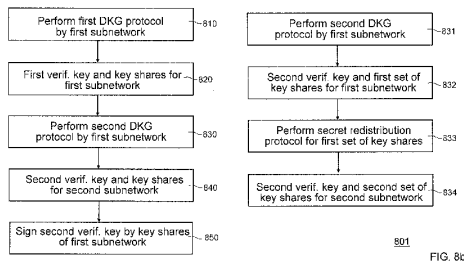


FIG. 8a

FIG. 8b

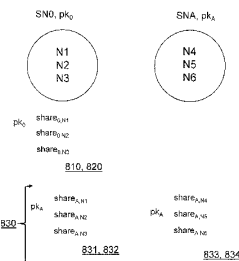


FIG. 8c

(57) Abstract: Embodiments of the invention relate to a computer-implemented method for generating verification keys of a public-key signature scheme in a distributed network. The method comprises performing, by a subset of the nodes of a first subnetwork of nodes, a first distributed key generation protocol, the first distributed key generation protocol being configured to generate jointly a verification key for the first subnetwork and a plurality of corresponding secret key shares for the nodes of the first subnetwork. The method further comprises a step of performing, for a second subnetwork, by a subset of the plurality of nodes of the first subnetwork, a second distributed key generation protocol, the second distributed key generation protocol being configured to generate jointly a verification key of the second subnetwork and a plurality of corresponding secret key shares for the nodes of the second subnetwork. A further step comprises signing, by a subset of the nodes of the first subnetwork, the verification key of the second subnetwork with a permissible subset of the secret key shares of the nodes of the first subnetwork, thereby generating a joint signature on the verification key of the second subnetwork. Further aspects relate to a distributed network, a node of a distributed network and corresponding computer program products.

Published:

— with international search report (Art. 21(3))