

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
06 April 2023 (06.04.2023)



(10) International Publication Number
WO 2023/052609 A1

(51) International Patent Classification:

H04L 9/08 (2006.01) H04L 9/00 (2006.01)
H04L 9/32 (2006.01)

(21) International Application Number:

PCT/EP2022/077329

(22) International Filing Date:

30 September 2022 (30.09.2022)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

63/250,696 30 September 2021 (30.09.2021) US

(71) Applicant: **DFINITY STIFTUNG** [CH/CH]; Genfer-
strasse 11, 8002 Zürich (CH).

(72) Inventors: **GROTH, Jens**; c/o Dfinity Stiftung, Genfer-
strasse 11, 8002 Zürich (CH). **SHOUP, Victor**; c/o Dfinity
Stiftung, Genferstrasse 11, 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, CV, CZ, DE, DJ, DK, DM,
DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,

HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, 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))
- in black and white; the international application as filed
contained color or greyscale and is available for download
from PATENTSCOPE

(54) Title: DIGITAL SIGNATURES WITH KEY-DERIVATION

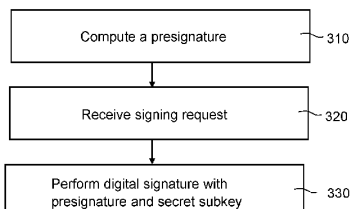


FIG. 3a

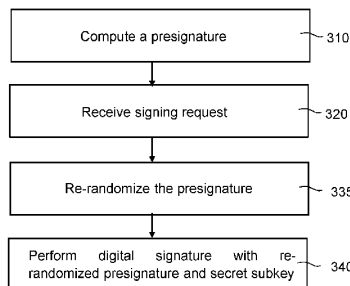


FIG. 3b

(57) Abstract: Embodiments of the invention relate to a computer-implemented method for performing a digital signature according to a public key signature scheme. The method comprises a step of computing a presignature. The method comprises further steps of providing a master secret key pair, the master secret key pair comprising a first master secret key and a second master secret key, and providing a master public key pair, the master public key pair comprising a first master public key and a second master public key. The method comprises further steps of deriving a secret subkey from the master secret key pair and deriving a public subkey from the master public key pair. The method further comprises performing the digital signature by means of the secret subkey and the computed presignature.

WO 2023/052609 A1