



(51) International Patent Classification:

H04L 9/08 (2006.01) H04L 9/32 (2006.01)
H04L 9/30 (2006.01) H04L 9/00 (2006.01)

(21) International Application Number:

PCT/EP2020/053101

(22) International Filing Date:

07 February 2020 (07.02.2020)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

19160731.6 05 March 2019 (05.03.2019) EP

(71) Applicant: **SEPIOR APS** [DK/DK]; Inge Lehmanns Gade 10, 6, 8000 Aarhus C (DK).

(72) Inventors: **JAKOBSEN, Thomas, Pelle**; Obstrupvej 12K, 8320 Måslet (DK). **DAMGÅRD, Ivan, Bjerre**; Johannes Ewalds Vej 9, 8230 Åbyhøj (DK). **ØSTERGAARD, Michael, Bækvang**; Vestergårdsparken 20, 8361 Hasselager (DK). **NIELSEN, Jesper, Buus**; Hjortensgade 26, 8000 Aarhus C (DK).

(74) Agent: **INSPICOS P/S**; Kogle Allé 2, 2970 Hørsholm (DK).

(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, 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: A METHOD FOR PROVIDING A DIGITAL SIGNATURE TO A MESSAGE

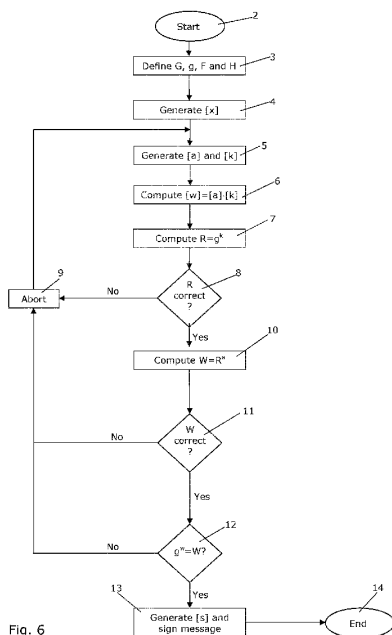


Fig. 6

(57) Abstract: A method for providing a digital signature to a message, M, in accordance with a digital signature algorithm (DSA) or an elliptic curve digital signature algorithm (ECDSA) is disclosed. A secret key, x, is generated as a random secret sharing [x] among at least two parties, such as among at least three parties. Random secret sharings, [a] and [k], are generated among the at least two parties and [w] = [a][k], $R = g^k$ and $W = R^a$ are computed and their correctness verified, [w] is verified by checking whether or not $g^w = W$. The message, M, is signed by generating a sharing, [s], among the at least two parties, using at least M, [w], R and [x].