



(51) International Patent Classification:
H04L 9/32 (2006.01) H04L 9/00 (2022.01)
H04L 9/08 (2006.01)

(21) International Application Number:
PCT/IB2024/060864

(22) International Filing Date:
04 November 2024 (04.11.2024)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
63/547,714 08 November 2023 (08.11.2023) US
63/700,778 30 September 2024 (30.09.2024) US

(71) Applicant: DWALLET LABS LTD. [IL/IL]; 2 Har Sinai
Street, 6581602 Tel-Aviv (IL).

(72) Inventors: FRIEDMAN, Offir; 97 Rothschild Boulevard,
6523510 Tel Aviv (IL). MARMOR, Avichai; 14 Har Adir
Street, 4448322 Kfar-Saba (IL). MUTZARI, Dolev; 9 Ha-
Khelmonit Street, 7542009 Rishon-LeZion (IL). SADIKA,
Omer; 6 Mapu Street, 6357705 Tel-Aviv (IL). COHEN
SCALY, Yehonatan; 19 Levontin Street, 6511208 Tel-Aviv
(IL). YANAI, Avishay; 22 Tzahal Street, 4952115 Petach-
Tikva (IL).

(74) Agent: MEITAR PATENTS LTD.; 16 Abba Hillel Road,
5250608 Ramat-Gan (IL).

(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, MG, MK, MN, MU, MW, MX, MY, MZ, NA,

(54) Title: 2PC-MPC: ECDSA THRESHOLD SIGNATURE BASED ON A THRESHOLD ADDITIVELY HOMOMORPHIC EN-
CRYPTION

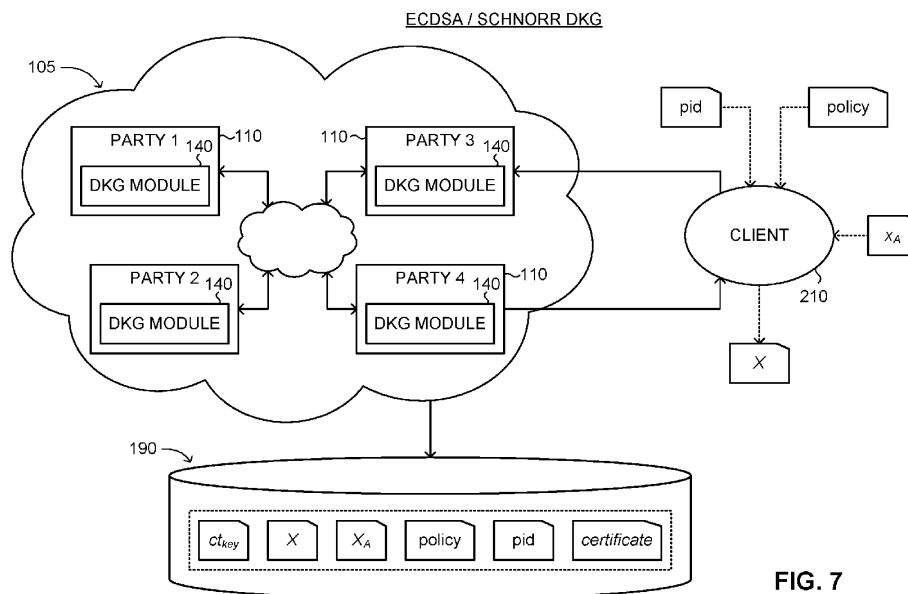


FIG. 7

(57) Abstract: Method and system for generating digital signature following one or more secure protocols based on a threshold additively homomorphic encryption (TAHE) over a broadcast channel, where a threshold of parties of a decentralized network produces digital signature by following a Universally Composable secure protocol configured to output Elliptic curve digital signature algorithm (ECDSA) signature or a Schnorr signature. At least one client may cooperate with the threshold of parties to generate digital signature, or threshold of parties may cooperate to generate digital signature without a client. Method may include additively homomorphic encryption (AHE) distributed key generation (DKG), ECDSA/Schnorr DKG, ECDSA/Schnorr presigning, providing ECDSA/Schnorr child keys, ECDSA/Schnorr signing, wallet transfer and/or network reconfiguration.

[Continued on next page]

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, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, 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))