



(51) International Patent Classification:

H04L 9/08 (2006.01) H04L 9/00 (2006.01)
H04L 29/06 (2006.01) H04L 9/32 (2006.01)

(21) International Application Number:

PCT/EP2021/059896

(22) International Filing Date:

16 April 2021 (16.04.2021)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

20170889.8 22 April 2020 (22.04.2020) EP

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

(72) Inventors: JAKOBSEN, Thomas Pelle; Obstrupvej 12K, 8320 Mårslet (DK). TOFT, Tomas, Friis; Algade 24 Grundfor, 8382 Hinnerup (DK). ØSTERGAARD, Michael, Bækvang; Vestergårdsparken 20, 8361 Hasselager (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, 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,

(54) Title: RESTORATION OF A DISTRIBUTED KEY FROM A BACKUP STORAGE

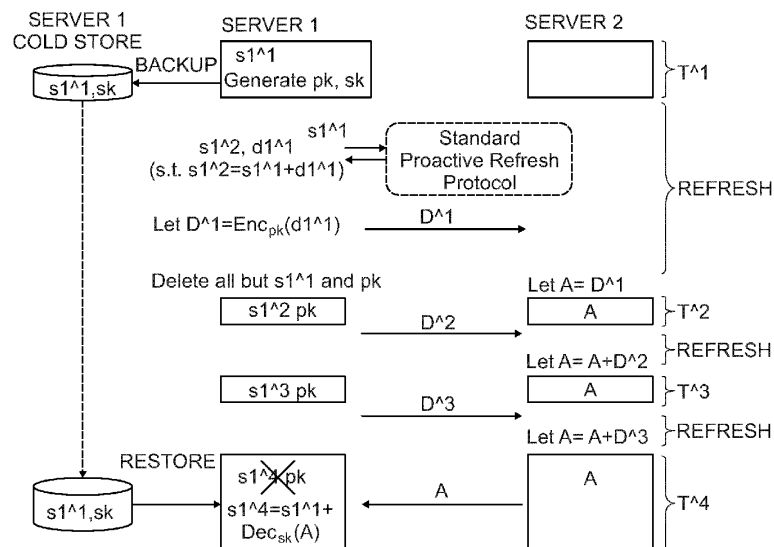


Fig. 2

(57) Abstract: A method for restoring a distributed secret key from a backup storage is disclosed. An original secret key is generated and distributed among two or more servers. A first server creates a backup containing at least the share of the original secret key which is held by the first server. The servers refresh the original secret key at least once. During each refresh the servers generate a refreshed distributed secret key and a distributed difference between the previous secret key and the refreshed secret key, each server generates a secret version of its share of the difference and shares the secret version with at least some of the other servers, and each server generates an accumulated secret version of the shares of the difference received from the other servers based on the received secret versions of the shares of the difference and previous accumulated secret versions. The first server restores its share of the original secret key from the backup and requests the accumulated secret version of its share of the difference from the other servers, and restores its share of the

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).

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

Published:

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