



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

(21) International Application Number:
PCT/US2019/045562

(22) International Filing Date:
07 August 2019 (07.08.2019)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/740,301 02 October 2018 (02.10.2018) US
62/851,565 22 May 2019 (22.05.2019) US

(71) Applicant: **VISA INTERNATIONAL SERVICE ASSOCIATION** [US/US]; P.O. BOX 8999, SAN FRANCISCO, 94128 (US).

(72) Inventors: **MUKHERJEE, Pratyay**; 3549 Monroe St., Apt. 524, Santa Clara, California 95051 (US). **CHEN, Binyi**; 6920 Whittier Drive, #130, Goleta, California 93117 (US). **CHEN, Yilei**; 2850 Middlefield Rd., E124, Palo Alto, California 94306 (US).

(74) Agent: **RACZKOWSKI, David B.** et al.; Kilpatrick, Townsend & Stockton LLP, 1100 Peachtree Street Suite 2800, Atlanta, Georgia 30309 (US).

(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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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: CONTINUOUS SPACE-BOUNDED NON-MALLEABLE CODES FROM STRONGER PROOFS-OF-SPACE

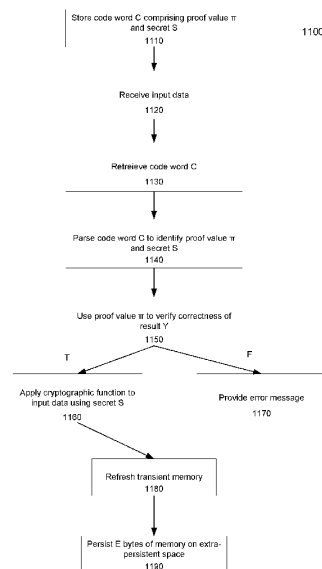


FIG. 11

(57) Abstract: Systems, methods, and apparatuses for protecting a secret on a device with limited memory, while still providing tamper resistance, are described. To achieve security, an encoding computer can apply a memory-hard function MHF to a secret S and determine a result Y, then determine a proof η for the result Y. Then, the encoding computer can send a codeword C comprising the secret S and the proof η to a decoding computer. The decoding computer can retrieve the codeword C from persistent memory and parse the secret S and the proof η . The decoding device can use transient memory to decode the codeword C by verifying the proof η was generated with the secret S and the result Y. When the correctness of the result Y is verified, the decoding device can apply a cryptographic function to input data using the secret S then reset the transient memory.

Declarations under Rule 4.17:

- *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

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