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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
04 November 2021 (04.11.2021)

WIPO | PCT

(10) International Publication Number
WO 2021/222272 A1

(51) International Patent Classification:
H04L 9/08 (2006.01) *H04L 29/06* (2006.01)
H04L 9/06 (2006.01) *G06F 21/60* (2013.01)
H04L 9/32 (2006.01)

(21) International Application Number:
PCT/US2021/029429

(22) International Filing Date:
27 April 2021 (27.04.2021)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
16/861,138 28 April 2020 (28.04.2020) US
63/019,938 04 May 2020 (04.05.2020) US

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

(72) Inventors: **MUKHERJEE, Pratyay**; PO BOX 8999, SAN FRANCISCO, California 94128 (US). **SINHA, Rohit**; PO BOX 8999, SAN FRANCISCO, California 94128 (US). **GADDAM, Sivanarayana**; PO BOX 8999, SAN FRANCISCO, California 94128 (US). **CHRISTODORESCU, Mihai**; PO BOX 8999, SAN FRANCISCO, California 94128 (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,

(54) Title: ADAPTIVE ATTACK RESISTANT DISTRIBUTED SYMMETRIC ENCRYPTION

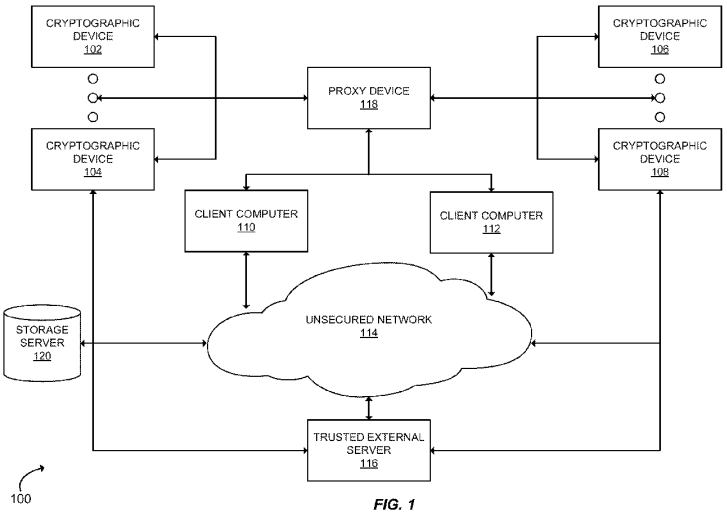


FIG. 1

(57) Abstract: Systems and methods for adaptive attack resistant and amortized distributed symmetric cryptography are disclosed. A client computer may communicate with a number of cryptographic devices in order to encrypt or decrypt data. Each cryptographic device may possess one or more secret shares corresponding to one or more distinct secret values, which may be used in the process of encrypting or decrypting data. The client computer may generate one or more commitments and transmit those commitments to the cryptographic devices. Each cryptographic device may generate a partial computation based on the commitments and their respective secret shares. The partial computations may be transmitted to the client computer. The client computer may use the partial computations to generate a cryptographic key or bulk key. The client computer may use the cryptographic key, or one or more message keys derived from the bulk key, to encrypt one or more messages or decrypt ciphertext.

WO 2021/222272 A1

[Continued on next page]

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, 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:

— *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))*