



- (51) International Patent Classification:
H04L 9/08 (2006.01) *H04L 9/30* (2006.01)
- (21) International Application Number:
PCT/US2021/014006
- (22) International Filing Date:
19 January 2021 (19.01.2021)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
16/779,422 31 January 2020 (31.01.2020) US
- (71) Applicant: VISA INTERNATIONAL SERVICE ASSOCIATION [US/US]; P.O. Box 8999, San Francisco, California 94128 (US).
- (72) Inventors: MUKHERJEE, Pratyay; P.O. Box 8999, San Francisco, California 94128 (US). AGRAWAL, Shashank; P.O. Box 8999, San Francisco, California 94128 (US). RINDAL, Peter; P.O. Box 8999, San Francisco, California 94128 (US). LUYKX, Atul; P.O. Box 8999, San Francisco, California 94128 (US). DAI, Wei; P.O. 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, 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,

(54) Title: DISTRIBUTED SYMMETRIC ENCRYPTION

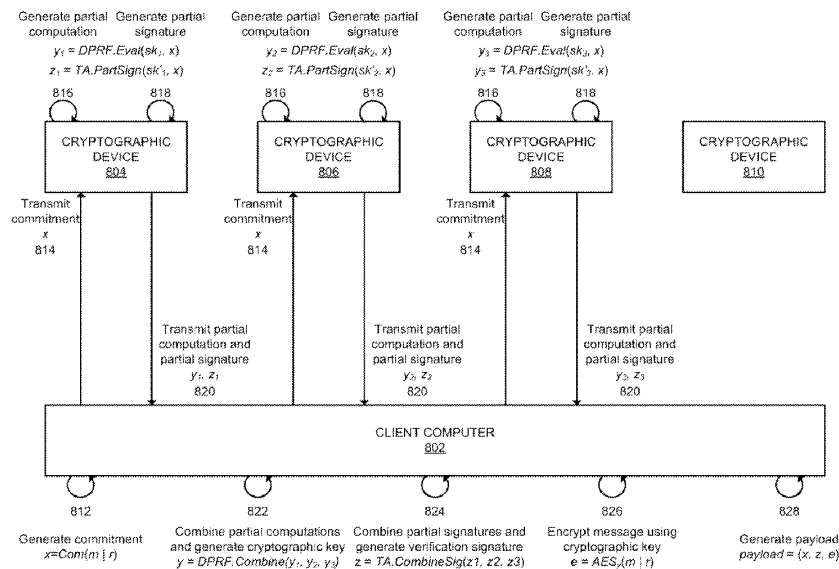


FIG. 8

(57) **Abstract:** Systems and methods for improved 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 a secret share and a verification share, which may be used in the process of encrypting or decrypting data. The client computer may generate a commitment and transmit the commitment to the cryptographic devices. Each cryptographic device may generate a partial computation based on the commitment and their respective secret share, and likewise generate a partial signature based on the commitment and their respective verification share. The partial computations and partial signatures may be transmitted to the client computer. The client computer may use the partial computations and partial signatures to generate a cryptographic key and verification signature respectively. The client computer may use the cryptographic key to encrypt or decrypt a message.

[Continued on next page]

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))*
