



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

(21) International Application Number:
PCT/US2018/052448

(22) International Filing Date:
24 September 2018 (24.09.2018)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **VISA INTERNATIONAL SERVICE ASSOCIATION** [US/US]; 900 Metro Center Boulevard, FOSTER CITY, California 94404 (US).

(72) Inventors: **GRYB, Oleg**; 3527 Kirkham Street, San Francisco, California 94122 (US). **NAGASUNDARAM, Sekhar**; 1445 Bayberry View Lane, San Ramon, California 94582 (US).

(74) Agent: **JEWIK, Patrick** et al.; KILPATRICK TOWNSEND & STOCKTON LLP, Mailstop: IP Docket-

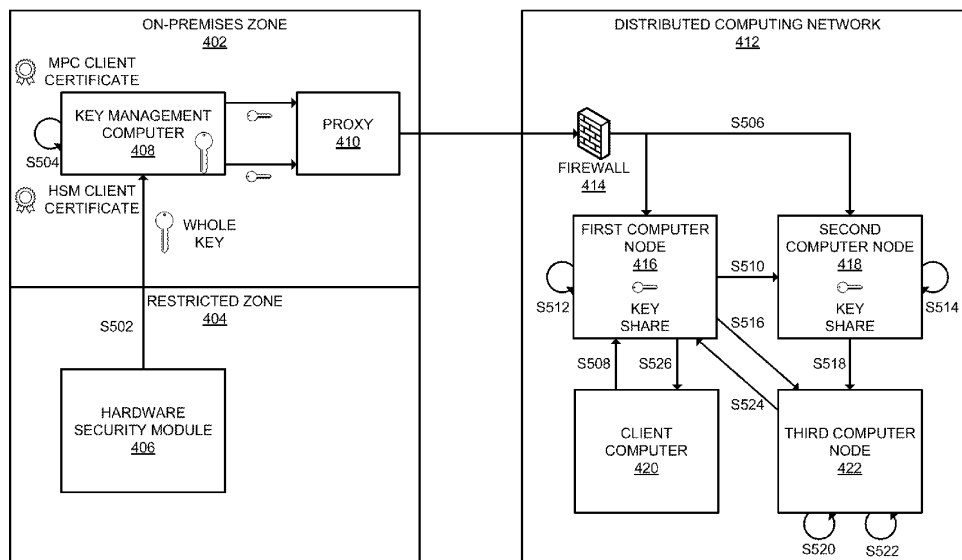
ing - 22, 1100 Peachtree Street, Suite 2800, Atlanta, Georgia 30309 (US).

(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,

(54) Title: KEY MANAGEMENT FOR MULTI-PARTY COMPUTATION

FIG. 4



(57) Abstract: Methods and systems for managing cryptographic keys in on-premises and cloud computing environments and performing multi-party cryptography are disclosed. A cryptographic key can be retrieved from a hardware security module by a key management computer. The key management computer can generate key shares from the cryptographic key, and securely distribute the key shares to computer nodes or key share databases. The computer nodes can use the key shares in order to perform secure multi-party cryptography.

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))*