

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

(19) World Intellectual Property  
Organization  
International Bureau

(43) International Publication Date  
13 August 2020 (13.08.2020)



(10) International Publication Number  
**WO 2020/162973 A1**

(51) International Patent Classification:  
*H04L 9/32* (2006.01) *H04L 9/08* (2006.01)  
*H04L 9/30* (2006.01)

(21) International Application Number:  
PCT/US2019/044753

(22) International Filing Date:  
01 August 2019 (01.08.2019)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
62/803,325 08 February 2019 (08.02.2019) US

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

(72) Inventors: **MUKHERJEE, Pratyay**; 3549 Monroe St., Apt. 524, Santa Clara, California 95051 (US). **CHEN, Yilei**; 2850 Middlefield Rd., E124, Palo Alto, California 94306 (US). **GENISE, Nicholas**; 900 Metro Center Boulevard, Foster City, California 94404 (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,

(54) Title: MORE EFFICIENT POST-QUANTUM SIGNATURES

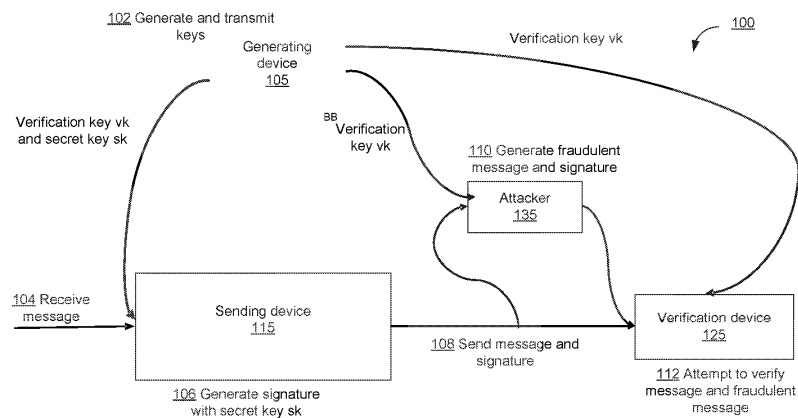


FIG. 1

(57) Abstract: Techniques of generating a lattice-based verification matrix and signature vector are disclosed. The method enables a generating device to sample a gadget matrix and then generate a reduced gadget matrix. The generating device may then sample a trapdoor matrix and use the trapdoor matrix and the reduced gadget matrix to generate a verification matrix. A sending device may receive the trapdoor matrix and the verification matrix from the generating device, in addition to receiving a message. The sending device may then use the trapdoor matrix and the verification matrix to generate a signature vector for the message. A verification device can receive the verification matrix, the message, and the signature vector. The verification device may use the verification matrix and the signature vector to verify the message.

[Continued on next page]

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).

**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))*