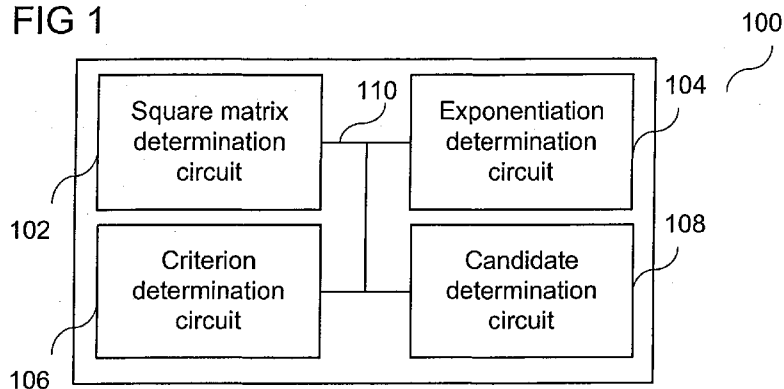




- (51) **International Patent Classification:**
G06F 17/16 (2006.01) *H04L 9/00* (2006.01)
G06F 21/00 (2006.01)
- (21) **International Application Number:**
PCT/SG2012/000165
- (22) **International Filing Date:**
10 May 2012 (10.05.2012)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
61/484,382 10 May 2011 (10.05.2011) US
- (71) **Applicant** (for all designated States except US): **NANYANG TECHNOLOGICAL UNIVERSITY** [SG/SG]; 50 Nanyang Avenue, Singapore 639798 (SG).
- (72) **Inventors; and**
- (75) **Inventors/Applicants** (for US only): **POSCHMANN, Axel** [DE/SG]; Nanyang Technological University, c/o Nanyang Innovation & Enterprise Office (NIEO), Blk 1, Unit 213, Innovation Centre, 16 Nanyang Drive, Singapore 637722 (SG). **PEYRIN, Thomas** [FR/SG]; Nanyang Technological University, c/o Nanyang Innovation & Enterprise Office (NIEO), Blk 1, Unit 213, Innovation Centre, 16 Nanyang Drive, Singapore 637722 (SG).
- (74) **Agent:** **VIERING, JENTSCHURA & PARTNER LLP**; P.O. Box 1088, Rochor Post Office, Rochor Road, Singapore 911833 (SG).
- (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, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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, 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, ML, MR, NE, SN, TD, TG).
- Published:**
— with international search report (Art. 21(3))

(54) **Title:** DEVICES FOR COMPUTER-BASED GENERATING OF A MIXING MATRIX FOR CRYPTOGRAPHIC PROCESSING OF DATA, ENCRYPTING DEVICES, METHODS FOR COMPUTER-BASED GENERATING OF A MIXING MATRIX FOR CRYPTOGRAPHIC PROCESSING OF DATA AND ENCRYPTING METHODS

FIG 1



(57) **Abstract:** In an embodiment, a device for computer-based generating of a mixing matrix for cryptographic processing of data may be provided. The device may include: a square matrix determination circuit configured to determine a square matrix with non-zero elements only in one diagonal or sub-diagonal and in one row or column; an exponentiation determination circuit configured to determine an exponentiation of the square matrix as a candidate for a mixing matrix; a criterion determination circuit configured to determine whether the candidate fulfils a pre-determined criterion; and a candidate determination circuit configured to determine the candidate as the mixing matrix if the candidate fulfils a pre-determined criterion.

