

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
15 June 2023 (15.06.2023)



(10) International Publication Number
WO 2023/107005 A3

- (51) **International Patent Classification:**
H04L 9/06 (2006.01) *G06F 7/58* (2006.01)
- (21) **International Application Number:**
PCT/SG2022/050885
- (22) **International Filing Date:**
05 December 2022 (05.12.2022)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
10202113695S 09 December 2021 (09.12.2021) SG
- (71) **Applicant:** AGENCY FOR SCIENCE, TECHNOLOGY AND RESEARCH [SG/SG]; 1 Fusionopolis Way, #20-10 Connexis North Tower, Singapore 138632 (SG).
- (72) **Inventors:** WONG, Ming Ming; c/o Institute of Microelectronics, 2 Fusionopolis Way, #08-02, Innovis, Singapore 138634 (SG). LIM, Jayce Lay Keng; c/o Institute of Microelectronics, 2 Fusionopolis Way, #08-02, Innovis, Singapore 138634 (SG). DO, Anh Tuan; c/o Institute of Microelectronics, 2 Fusionopolis Way, #08-02, Innovis, Singapore 138634 (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, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, 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, CV, 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, ME, 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).

Published:

- with international search report (Art. 21(3))
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))

(54) **Title:** AES CRYPTOGRAPHIC SYSTEM AND METHOD

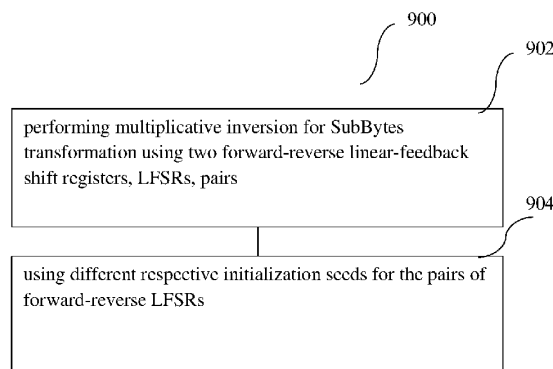


Figure 9

(57) **Abstract:** An Advanced Encryption Standard (AES) cryptographic system and a method of performing Advanced Encryption Standard (AES) cryptography. The method comprises the steps of performing multiplicative inversion for SubBytes transformation using two forward-reverse linear-feedback shift registers, LFSRs, pairs; and using different respective initialization seeds for the pairs of forward-reverse LFSRs.

[Continued on next page]

(88) Date of publication of the international search report:
10 August 2023 (10.08.2023)