



(51) International Patent Classification:

H04L 9/06 (2006.01) G06F 17/16 (2006.01)
H03K 19/00 (2006.01)

(21) International Application Number:

PCT/SG2021/050036

(22) International Filing Date:

26 January 2021 (26.01.2021)

(25) Filing Language:

English

(26) Publication Language:

English

(71) Applicant: **AGENCY FOR SCIENCE, TECHNOLOGY AND RESEARCH** [SG/SG]; 1 Fusionopolis Way, #20-10, Connexis North Tower, Singapore 138632 (SG).

(72) Inventors: **LAN, Jingjing**; c/o Industry Development, Institute of Microelectronics, 2 Fusionopolis Way, #08-02 Innovis Tower, Singapore 138634 (SG). **DO, Anh Tuan**; c/o Industry Development, Institute of Microelectronics, 2 Fusionopolis Way, #08-02 Innovis Tower, Singapore 138634 (SG). **PARAMASIVAM, Vishnu**; c/o Industry Development, Institute of Microelectronics, 2 Fusionopolis Way, #08-02 Innovis Tower, Singapore 138634 (SG).

(74) Agent: **DONALDSON & BURKINSHAW LLP**; 24 Raffles Place, #15-00 Clifford Centre, Singapore 048621 (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, 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, 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:

— of inventorship (Rule 4.17(iv))

(54) Title: AN ADVANCED ENCRYPTION STANDARD (AES) DEVICE

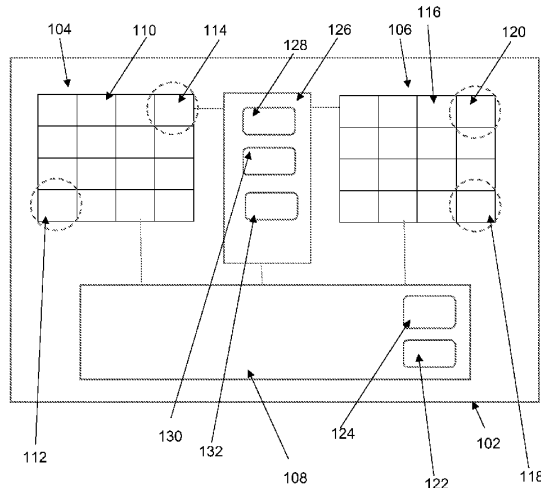


FIG. 1

(57) Abstract: An Advanced Encryption Standard (AES) device and a computer-implemented method of performing an AES operation may be provided, the AES device comprising a state array of components comprising a first plurality of controllable data processing components, the first plurality of controllable data processing components including two or more controllable data processing state members that each include an additional input control and an additional input port; a key array of components comprising a second plurality of controllable data processing components; a control block module coupled to the state array of components and the key array of components, the control block module arranged to transmit one or more control signals to the state array of components and the key array of components; wherein the two or more controllable data processing state members are disposed at predetermined positions within the state array of components; and further wherein the control block module is arranged to instruct performance of one or more AES operations via usage of the additional input port of at least one of the two or more controllable data processing state members based on a clock cycle count.

Published:

- with international search report (Art. 21(3))
- in black and white; the international application as filed contained color or greyscale and is available for download from PATENTSCOPE