

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
24 February 2022 (24.02.2022)



(10) International Publication Number
WO 2022/039671 A1

(51) International Patent Classification:

G06F 7/58 (2006.01) G06F 1/08 (2006.01)
H04L 9/00 (2022.01) H04L 29/06 (2006.01)
G06F 21/00 (2013.01)

(21) International Application Number:

PCT/SG2021/050474

(22) International Filing Date:

13 August 2021 (13.08.2021)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

10202008065R 21 August 2020 (21.08.2020) SG

(71) Applicant: NATIONAL UNIVERSITY OF SINGAPORE [SG/SG]; 21 Lower Kent Ridge Road, Singapore 119077 (SG).

(72) Inventors: TANEJA, Sachin; c/o National University of Singapore, Faculty of Engineering, Department of Electrical and Computer Engineering, 21 Lower Kent Ridge Road, Singapore 119077 (SG). ALIOTO, Massimo; c/o Nation-

al University of Singapore, Faculty of Engineering, Department of Electrical and Computer Engineering, 21 Lower Kent Ridge Road, Singapore 119077 (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, 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,

(54) Title: METHOD AND APPARATUS FOR TRUE RANDOM NUMBER GENERATION WITHIN CRYPTOGRAPHIC HARDWARE

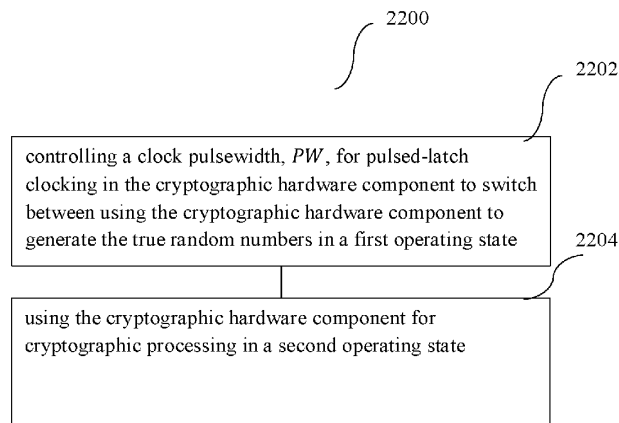


Figure 22

(57) Abstract: A method of generating true random numbers for use by a cryptographic hardware component for cryptographic algorithms or communication protocols, and a cryptographic hardware component for cryptographic algorithms or communication protocols. The method comprises the steps of controlling a clock pulsewidth, PW , for pulsed-latch clocking in the cryptographic hardware component to switch between using the cryptographic hardware component to generate the true random numbers in a first operating state; and using the cryptographic hardware component for cryptographic processing in a second operating state.

[Continued on next page]

WO 2022/039671 A1

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).

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*