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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 August 2023 (24.08.2023)

WIPO | PCT

(10) International Publication Number
WO 2023/158378 A3

(51) International Patent Classification:
G06F 21/57 (2013.01) *H04L 9/32* (2006.01)
G05F 1/565 (2006.01) *G06N 20/00* (2019.01)

(21) International Application Number:
PCT/SG2023/050088

(22) International Filing Date:
16 February 2023 (16.02.2023)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10202201503P 16 February 2022 (16.02.2022) SG

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

(72) Inventors: **FANG, Qiang**; c/o National University of Singapore , Faculty of Engineering, Department of Electrical and Computer Engineering, 21 Lower Kent Ridge Road, Singapore 119077 (SG). **LIN, Longyang**; 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 National University of Singapore, Faculty of Engineering, Department of Electrical and Computer Engineering, 21 Lower Kent Ridge Road, Singapore 119077 (SG).

(74) Agent: **SPRUSON & FERGUSON (ASIA) PTE LTD**; P.O. Box 1531, Robinson Road Post Office, Singapore 903031 (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.

(54) Title: DEVICE FOR COUNTERACTING SIDE-CHANNEL ATTACKS

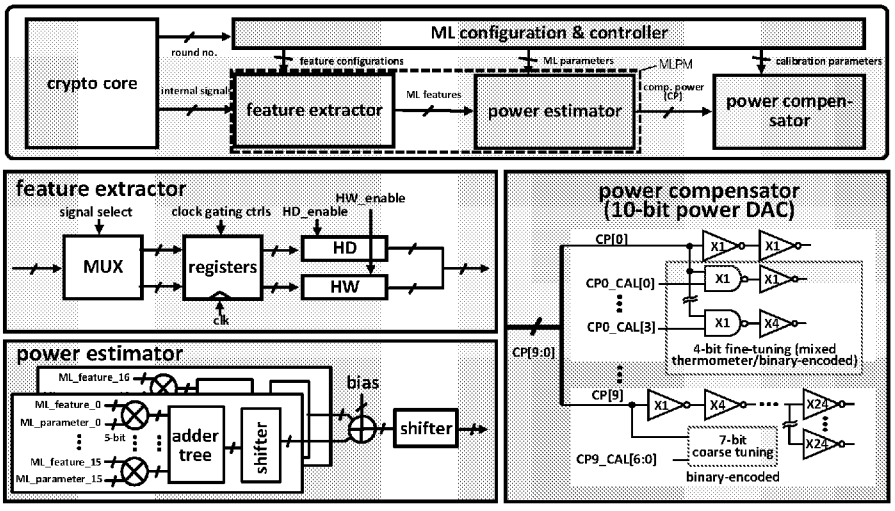

Fig. 2

(57) Abstract: A device for counteracting side-channel attacks (SCA), including a machine learning unit (MLU) that is connectable to a cryptographic core. The MLU includes: a feature extractor unit configured to extract selected information-sensitive signals from the cryptographic core and to generate machine learning features based on the selected information-sensitive signals; and a machine learning-based power estimator unit configured to output cumulative information-sensitive energy based on the generated machine learning features. The device further includes a power compensation unit that is configured to cancel out the cumulative information-sensitive energy so as to counteract side-channel attacks (SCA).

[Continued on next page]

WO 2023/158378 A3

(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, SC, 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).

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

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))*

(88) Date of publication of the international search report:
21 September 2023 (21.09.2023)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SG2023/050088

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/57 (2013.01) ***G05F 1/565 (2006.01)*** *H04L 9/32 (2006.01)* *G06N 20/00 (2019.01)*

According to International Patent Classification (IPC)

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F, H04L, G06N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

FAMPAT, Internet: side channel, 侧信道, linear regression, stochastic, 线性回归, 随机, machine learning, deep learning, 机器学习, 深度学习, LDO, 低压差, low dropout and other related terms

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Integrated and Distributed Digital Low-Drop-Out Regulators with Event-Driven Controls and Side-Channel Attack Resistance. 28 December 2020 [Retrieved on 2023-08-07 from https://academiccommons.columbia.edu/doi/10.7916/d8-mbs2-4z84] .2 Overall architecture, 5.3 Attack detector module, 5.4 EQZ-LDO core, 5.5 Prototype and measurements, Figs. 5.8-5.9	1-9
X	CN 113221118 A (ZHUOER ZHILIAN RESEARCH INSTITUTE) 6 August 2021 Paras. [0025]-[0029], [0041]-[0051] of the original non-English language document (a machine translation is enclosed **only** for your reference)	1, 3-5
A	Linear Regression Side Channel Attack Applied on Constant XOR. 19 December 2017 [Retrieved on 2023-08-07 from https://eprint.iacr.org/2017/1217] Whole document especially 4.1 Leakage under Constant XOR Mask	

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

*Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"D" document cited by the applicant in the international application

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
07/08/2023 *(day/month/year)*	16/08/2023 *(day/month/year)*

Name and mailing address of the ISA/SG

Intellectual Property Office of Singapore
1 Paya Lebar Link, #11-03
PLQ 1, Paya Lebar Quarter
Singapore 408533

Email: pct@ipos.gov.sg

Authorized officer

Yeo Eng Guan (Dr)

IPOS Customer Service Tel. No.: (+65) 6339 8616

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/SG2023/050088

Note: This Annex lists known patent family members relating to the patent documents cited in this International Search Report. This Authority is in no way liable for these particulars which are merely given for the purpose of information.

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
CN 113221118 A	06/08/2021	NONE	