Title (en)

CONFIGURING A REDUCED INSTRUCTION SET COMPUTER PROCESSOR ARCHITECTURE TO EXECUTE A FULLY HOMOMORPHIC ENCRYPTION ALGORITHM

Title (de)

KONFIGURATION EINER RECHNERPROZESSORARCHITEKTUR MIT REDUZIERTEM BEFEHLSSATZ ZUR AUSFÜHRUNG EINES VOLLSTÄNDIG HOMOMORPHEN VERSCHLÜSSELUNGSALGORITHMUS

Title (fr)

CONFIGURATION D'UNE ARCHITECTURE DE PROCESSEUR INFORMATIQUE À ENSEMBLE D'INSTRUCTIONS RÉDUIT POUR EXÉCUTER UN ALGORITHME DE CHIFFREMENT ENTIÈREMENT HOMOMORPHIQUE

Publication

EP 4011030 A4 20231227 (EN)

Application

EP 20850899 A 20200805

Priority

- US 201962883967 P 20190807
- US 202016743257 A 20200115
- US 2020044944 W 20200805

Abstract (en)

[origin: WO2021026196A1] Systems and methods for configuring a reduced instruction set computer processor architecture to execute fully homomorphic encryption (FHE) logic gates as a streaming topology. The method includes parsing sequential FHE logic gate code, transforming the FHE logic gate code into a set of code modules that each have in input and an output that is a function of the input and which do not pass control to other functions, creating a node wrapper around each code module, configuring at least one of the primary processing cores to implement the logic element equivalents of each element in a manner which operates in a streaming mode wherein data streams out of corresponding arithmetic logic units into the main memory and other ones of the plurality arithmetic logic units.

IPC 8 full level

G06F 9/50 (2006.01); **G06F 15/173** (2006.01)

CPC (source: EP)

G06F 15/8007 (2013.01); **G06F 17/142** (2013.01); **G06F 21/602** (2013.01); **G06F 21/6227** (2013.01); **H04L 9/008** (2013.01); G06F 2221/2107 (2013.01); H04L 2209/122 (2013.01)

Citation (search report)

- [Y] US 2015012725 A1 20150108 - FURTEK FREDERICK [US], et al
- [Y] US 2005166033 A1 20050728 - JACOB ROJIT [US]
- [Y] US 2004236809 A1 20041125 - SAHA KAUSHIK [IN], et al
- [Y] US 2012036514 A1 20120209 - MASTER PAUL [US], et al
- [Y] RAHMAN MD. MASHIUR ET AL: "Dynamic Range Input FFT Algorithm for Signal Processing in Parallel Processor Architecture", PROCEEDINGS OF THE WORLD CONGRESS ON ENGINEERING AND COMPUTER SCIENCE 2011, 1 January 2011 (2011-01-01), pages 1 - 6, XP055790901, Retrieved from the Internet <URL:http://www.iaeng.org/publication/WCECS2011/WCECS2011_pp530-535.pdf> [retrieved on 20210329]
- [Y] DOROZ YARKIN ET AL: "Accelerating Fully Homomorphic Encryption in Hardware", IEEE TRANSACTIONS ON COMPUTERS, IEEE, USA, vol. 64, no. 6, 1 June 2015 (2015-06-01), pages 1509 - 1521, XP011580531, ISSN: 0018-9340, [retrieved on 20150508], DOI: 10.1109/TC.2014.2345388
- See references of WO 2021026196A1

Designated contracting state (EPC)

AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

DOCDB simple family (publication)

WO 2021026196 A1 20210211; CN 114631284 A 20220614; EP 4011030 A1 20220615; EP 4011030 A4 20231227

DOCDB simple family (application)

US 2020044944 W 20200805; CN 202080070677 A 20200805; EP 20850899 A 20200805