



(11)

EP 4 170 964 B8

(12) **CORRECTED EUROPEAN PATENT SPECIFICATION**

(15) Correction information:
Corrected version no 1 (W1 B1)
Corrections, see
Bibliography INID code(s) 73

(51) International Patent Classification (IPC):
H04L 9/30 (2006.01) **H04L 9/08** (2006.01)
G06N 10/00 (2022.01) **G06F 21/60** (2013.01)
G06N 10/20 (2022.01) **H04L 9/00** (2022.01)

(48) Corrigendum issued on:
12.06.2024 Bulletin 2024/24

(52) Cooperative Patent Classification (CPC):
G06F 21/602; G06N 10/20; H04L 9/008;
H04L 9/3006; G06N 10/60

(45) Date of publication and mention
of the grant of the patent:
03.04.2024 Bulletin 2024/14

(21) Application number: **21214811.8**

(22) Date of filing: **15.12.2021**

(54) **A METHOD OF CONSTRUCTING A PUBLIC-KEY SYSTEM IN QAP-BASED HOMOMORPHIC ENCRYPTION**

VERFAHREN ZUR HERSTELLUNG EINES ÖFFENTLICHEN SCHLÜSSELSYSTEMS IN EINER QAP-BASIERTEN HOMOMORPHEN VERSCHLÜSSELUNG

PROCÉDÉ DE CONSTRUCTION D'UN SYSTÈME DE CLÉS PUBLIQUES DANS UN CHIFFREMENT HOMOMORPHE À BASE DE QAP

(84) Designated Contracting States:
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

(74) Representative: **Manitz Finsterwald**
Patent- und Rechtsanwaltspartnerschaft mbB
Martin-Greif-Strasse 1
80336 München (DE)

(30) Priority: **22.10.2021 US 202163270635 P**
11.11.2021 TW 110142063

(56) References cited:
• **GORJAN ALAGIC ET AL: "Quantum Fully Homomorphic Encryption With Verification", ARXIV.ORG, CORNELL UNIVERSITY LIBRARY, 201 OLIN LIBRARY CORNELL UNIVERSITY ITHACA, NY 14853, 30 August 2017 (2017-08-30), XP081291397, DOI: 10.1007/978-3-319-70694-8_16**
• **DULEK YFKE ET AL: "Quantum Homomorphic Encryption for Polynomial-Sized Circuits", 21 July 2016 (2016-07-21), ADVANCES IN BIOMETRICS : INTERNATIONAL CONFERENCE, ICB 2007, SEOUL, KOREA, AUGUST 27 - 29, 2007 ; PROCEEDINGS; [LECTURE NOTES IN COMPUTER SCIENCE; LECT.NOTES COMPUTER], SPRINGER, BERLIN, HEIDELBERG, PAGE(S) 3 - 32, XP047351656, ISBN: 978-3-540-74549-5 [retrieved on 2016-07-21] * Section 2.2. ** Section 3. ***

(43) Date of publication of application:
26.04.2023 Bulletin 2023/17

(73) Proprietor: **National Applied Research Laboratories**
Taipei City (TW)

(72) Inventors:
• **SU, Zheng-Yao**
Hsinchu (TW)
• **TSAI, Ming-Chung**
Hsinchu (TW)

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

EP 4 170 964 B8

- GUANGSHENG MA ET AL: "Quantum Fully Homomorphic Encryption without Preprocessing", ARXIV.ORG, CORNELL UNIVERSITY LIBRARY, 201 OLIN LIBRARY CORNELL UNIVERSITY ITHACA, NY 14853, 3 February 2021 (2021-02-03), XP081873964,