(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 2 499 560 B8**

(12) **CORRECTED EUROPEAN PATENT SPECIFICATION**

(15) Correction information:
Corrected version no 1 (W1 B1)
Corrections, see
Bibliography INID code(s) 74

(48) Corrigendum issued on:
08.01.2014 Bulletin 2014/02

(45) Date of publication and mention of the grant of the patent:
16.10.2013 Bulletin 2013/42

(21) Application number: **10795047.9**

(22) Date of filing: **15.11.2010**

(51) Int Cl.:
G06F 7/00 *(2006.01)*

(86) International application number:
PCT/IB2010/055158

(87) International publication number:
WO 2011/141776 (17.11.2011 Gazette 2011/46)

(54) PROCESSOR WITH DIFFERENTIAL POWER ANALYSIS ATTACK PROTECTION

PROZESSOR MIT SCHUTZ VOR ANGRIFFEN DURCH DIFFERENZIELLE LEISTUNGSANALYSE

PROCESSEUR AVEC PROTECTION CONTRE LES ATTAQUES PAR ANALYSE DE CONSOMMATION DIFFÉRENTIELLE

(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

(30) Priority: **12.05.2010 GB 201007932**

(43) Date of publication of application:
19.09.2012 Bulletin 2012/38

(73) Proprietor: **NDS Limited**
Staines, Middlesex TW18 4EX (GB)

(72) Inventor: **KALUZHNY, Uri**
Ramat Beit Shemes 99621 (IL)

(74) Representative: **Fyfe, Fiona Allison Watson**
Murgitroyd & Company
Scotland House
165-169 Scotland Street
Glasgow G5 8PL (GB)

(56) References cited:
US-A1- 2007 076 864

- **ERIC BRIER ET AL: "Correlation Power Analysis with a Leakage Model", 8 July 2004 (2004-07-08), CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS - CHES 2004; [LECTURE NOTES IN COMPUTER SCIENCE;;LNCS], SPRINGER-VERLAG, BERLIN/HEIDELBERG, PAGE(S) 16 - 29, XP019009370, ISBN: 978-3-540-22666-6 section 2**

EP 2 499 560 B8