Title (en)

COUNTERMEASURE METHOD AND DEVICES FOR ASYMMETRICAL CRYPTOGRAPHY WITH SIGNATURE DIAGRAM

Title (de)

GEGENMASSNAHMENVERFAHREN UND VORRICHTUNGEN FÜR ASYMMETRISCHE KRYPTOGRAPHIE MIT EINEM UNTERSCHRIFTENDIAGRAMM

Title (fr)

PROCEDE ET DISPOSITIFS DE CONTRE-MESURE POUR CRYPTOGRAPHIE ASYMETRIQUE A SCHEMA DE SIGNATURE

Publication

EP 2248008 A2 20101110 (FR)

Application

EP 09718480 A 20090123

Priority

- FR 2009000072 W 20090123
- FR 0800345 A 20080123

Abstract (en)

[origin: WO2009109715A2] The invention relates to a method for countermeasures in an electronic component that uses a private-key asymmetrical cryptography algorithm, including the steps of generating (102) a first output data (s1) using a primitive, and (104) a protection parameter. The method further comprises the steps of converting (106), using said protection parameter, at least one of the elements of the set including the private key and an intermediate parameter obtained from the first output data (s1) in order to provide respectively first and second operands, and generating (108, 114) a second output data (s2) from an operation in which the first and second operands are involved.

IPC 8 full level

G06F 7/72 (2006.01); **G06K 19/073** (2006.01); **H04L 9/28** (2006.01)

CPC (source: EP US)

G06F 7/72 (2013.01 - EP US); **H04L 9/003** (2013.01 - EP US); **H04L 9/3013** (2013.01 - EP US); **H04L 9/3252** (2013.01 - EP US); G06F 7/722 (2013.01 - EP US); G06F 7/725 (2013.01 - EP US); G06F 2207/7219 (2013.01 - EP US); H04L 2209/046 (2013.01 - EP US)

Citation (search report)

See references of WO 2009109715A2

Designated contracting state (EPC)

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 SE SI SK TR

Designated extension state (EPC)

AL BA RS

DOCDB simple family (publication)

FR 2926652 A1 20090724; **FR 2926652 B1 20100618**; CA 2712180 A1 20090911; CN 101911009 A 20101208; CN 101911009 B 20121010; EP 2248008 A2 20101110; JP 2011510579 A 20110331; KR 20100117589 A 20101103; US 2011170685 A1 20110714; WO 2009109715 A2 20090911; WO 2009109715 A3 20100114

DOCDB simple family (application)

FR 0800345 A 20080123; CA 2712180 A 20090123; CN 200980102305 A 20090123; EP 09718480 A 20090123; FR 2009000072 W 20090123; JP 2010543544 A 20090123; KR 20107017062 A 20090123; US 84040710 A 20100721