Title (en)

COUNTERMEASURE METHOD AND DEVICES FOR ASYMMETRIC CRYPTOGRAPHY

Title (de)

GEGENMASSNAHMENVERFAHREN UND VORRICHTUNGEN FÜR ASYMMETRISCHE KRYPTOGRAPHIE

Title (fr)

PROCEDE ET DISPOSITIFS DE CONTRE-MESURE POUR CRYPTOGRAPHIE ASYMETRIQUE

Publication

EP 2248009 A2 20101110 (FR)

Application

EP 09719837 A 20090123

Priority

- FR 2009000071 W 20090123
- FR 0800344 A 20080123

Abstract (en)

[origin: WO2009112686A2] The invention relates to a countermeasure method in an electronic component that uses a private-key asymmetric cryptography algorithm, and comprises generating (100) a protection parameter and calculating (104), using a primitive, an intermediate data from said protection parameter. The method further comprises the steps of splitting (110) the binary representation of the private key into a plurality of binary units, converting (112) each binary unit using the protection parameter and, for each converted binary unit, carrying out (114) an intermediate calculation using the primitive, and calculating (106-122) an output datum by combining (116) the intermediate data with the intermediate calculations (114).

IPC 8 full level

G06F 7/72 (2006.01)

CPC (source: EP US)

G06F 7/723 (2013.01 - EP US); **G06F 7/725** (2013.01 - EP US); **H04L 9/002** (2013.01 - EP US); **H04L 9/302** (2013.01 - EP US); **H04L 9/3066** (2013.01 - EP US); G06F 2207/7219 (2013.01 - EP US)

Citation (search report)

See references of WO 2009112686A2

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 2926651 A1 20090724; **FR 2926651 B1 20100521**; CA 2712178 A1 20090917; CN 101925875 A 20101222; EP 2248009 A2 20101110; JP 2011510578 A 20110331; KR 20100113130 A 20101020; US 2011274271 A1 20111110; WO 2009112686 A2 20090917; WO 2009112686 A3 20100114

DOCDB simple family (application)

FR 0800344 A 20080123; CA 2712178 A 20090123; CN 200980102893 A 20090123; EP 09719837 A 20090123; FR 2009000071 W 20090123; JP 2010543543 A 20090123; KR 20107018452 A 20090123; US 84034710 A 20100721