Title (en)

METHOD OF ENCRYPTION PROTECTED AGAINST SIDE CHANNEL ATTACKS

Title (de)

VERFAHREN FÜR EINE GEGEN SEITENKANALANGRIFFE GESCHÜTZTE VERSCHLÜSSELUNG

Title (fr)

PROCEDE DE CHIFFREMENT PROTEGE CONTRE DES ATTAQUES PAR CANAUX AUXILIAIRES

Publication

EP 2803161 A1 20141119 (FR)

Application

EP 12821282 A 20121221

Priority

- FR 1250272 A 20120111
- FR 2012000546 W 20121221

Abstract (en)

[origin: WO2013104837A1] The invention relates to a method of symmetric block encryption (CP3) executed by a microcircuit, for transforming a message (M) into an encrypted message (C), on the basis of a secret key (K, Ko), comprising a first round (RD-i), intermediate rounds (RD2, RD|, RDNM) and a last round (RDNr). According to the invention, the method comprises several executions (N1, NuNu,) of the first and of the last round, and a number of executions (Ni) of at least one intermediate round (RDj) which is less than the number of executions (N1, NuNuGamma) of the first and last rounds. Application in particular to DES, triple DES, and AES methods.

IPC 8 full level

H04L 9/00 (2006.01)

CPC (source: EP US)

G06F 21/72 (2013.01 - US); **H04L 9/003** (2013.01 - EP US); **H04L 9/0625** (2013.01 - US); H04L 2209/08 (2013.01 - EP US)

Citation (search report)

See references of WO 2013104837A1

Citation (examination)

- FR 2873523 A1 20060127 - SAGEM [FR]
- DAG ARNE OSVIK ET AL: "Cache attacks and Countermeasures: the Case of AES", INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH,, vol. 20050817:193724, 17 August 2005 (2005-08-17), pages 1 - 25, XP061001655

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

Designated extension state (EPC)

BA ME

DOCDB simple family (publication)

FR 2985624 A1 20130712; **FR 2985624 B1 20141121**; CN 104094553 A 20141008; CN 104094553 B 20180831; EP 2803161 A1 20141119; US 2014351603 A1 20141127; WO 2013104837 A1 20130718; WO 2013104837 A8 20140807

DOCDB simple family (application)

FR 1250272 A 20120111; CN 201280066783 A 20121221; EP 12821282 A 20121221; FR 2012000546 W 20121221; US 201214371049 A 20121221