Title (en)

METHOD FOR SECURING CRYPTOGRAPHIC PROCESSING BY MEANS OF DECOYS

Title (de)

VERFAHREN ZUR SICHERUNG EINER KRYPTOGRAFISCHEN VERARBEITUNG MITTELS KÖDER

Title (fr)

PROCÉDÉ DE SÉCURISATION DE TRAITEMENTS CRYPTOGRAPHIQUES PAR LE BIAIS DE LEURRES

Publication

EP 1792435 A1 20070606 (FR)

Application

EP 05800594 A 20050901

Priority

- FR 2005002193 W 20050901
- FR 0410010 A 20040922

Abstract (en)

[origin: WO2006032746A1] The inventive method for securing a cryptographic processing against physical attacks consists in repeating entirely or partially said cryptographic processing several times, i.e. one or several times on correct data, other times on incorrect data in order to decoy an attacker, wherein the selection of iterations performed on correct or incorrect data is carried out randomly and the incorrect data is ignored in the final result of processing.

IPC 8 full level

H04L 9/06 (2006.01)

CPC (source: EP)

H04L 9/003 (2013.01); **H04L 9/0618** (2013.01); H04L 2209/125 (2013.01)

Citation (search report)

See references of WO 2006032746A1

Citation (examination)

- FR 2790347 A1 20000901 - ST MICROELECTRONICS SA [FR]
- WO 2004053684 A2 20040624 - ADVANCED RISC MACH LTD [GB], et al
- HOLLMANN H D L ET AL: "Protection of software algorithms executed on secure modules", FUTURE GENERATIONS COMPUTER SYSTEMS, ELSEVIER SCIENCE PUBLISHERS. AMSTERDAM, NL, vol. 13, no. 1, 1 July 1997 (1997-07-01), pages 55 - 63, XP004081709, ISSN: 0167-739X, DOI: 10.1016/S0167-739X(97)89111-X

Designated contracting state (EPC)

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI SK TR

DOCDB simple family (publication)

FR 2875657 A1 20060324; **FR 2875657 B1 20061215**; BR PI0515587 A 20080729; EP 1792435 A1 20070606; WO 2006032746 A1 20060330

DOCDB simple family (application)

FR 0410010 A 20040922; BR PI0515587 A 20050901; EP 05800594 A 20050901; FR 2005002193 W 20050901