

Title (en)

METHOD FOR SECURING A COMPUTER INSTALLATION INVOLVING A CRYPTOGRAPHIC ALGORITHM USING BOOLEAN OPERATIONS AND ARITHMETIC OPERATIONS AND THE CORRESPONDING EMBEDDED SYSTEM

Title (de)

VERFAHREN ZUR SICHERUNG EINER ELEKTRONISCHEN EINHEIT ZUR AUSFÜHRUNG EINES KRYPTOGRAPHISCHEN ALGORITHMUS UNTER VERWENDUNG VON BOOLSCHEN UND ARITHMETISCHEN OPERATIONEN UND ZUGEHÖRIGES INTEGRIERTES SYSTEM

Title (fr)

PROCEDE DE SECURISATION D'UN ENSEMBLE ELECTRONIQUE METTANT EN OEUVRE UN ALGORITHME CRYPTOGRAPHIQUE UTILISANT DES OPERATIONS BOOLEENNES ET DES OPERATIONS ARITHMETIQUES, ET SYSTEME EMBARQUE CORRESPONDANT

Publication

**EP 1362451 A1 20031119 (FR)**

Application

**EP 02704839 A 20020214**

Priority

- FR 0200579 W 20020214
- FR 0102091 A 20010215

Abstract (en)

[origin: FR2820914A1] The invention relates to a method for securing a computer installation involving a cryptographic algorithm using boolean operations and arithmetic operations, in which at least one variable is separated into several parts by means of a boolean separation using a boolean operation and an arithmetic separation using an arithmetic operation. The inventive method is characterised in that in order to move from any of said separations to the other, a predetermined number of boolean and arithmetic operations are carried on said parts and at least one variate such that, for each of the values that appear during the calculation, there is no correlation with said variable. The invention also relates to an associated embedded system.

IPC 1-7

**H04L 9/06**

IPC 8 full level

**H04L 9/06** (2006.01)

CPC (source: EP US)

**H04L 9/003** (2013.01 - EP US); **G06F 2207/7219** (2013.01 - EP US)

Citation (search report)

See references of WO 02065692A1

Designated contracting state (EPC)

AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR

DOCDB simple family (publication)

**FR 2820914 A1 20020816**; EP 1362451 A1 20031119; US 2004139136 A1 20040715; US 7334133 B2 20080219; WO 02065692 A1 20020822

DOCDB simple family (application)

**FR 0102091 A 20010215**; EP 02704839 A 20020214; FR 0200579 W 20020214; US 46813004 A 20040105