Title (en)

CRYPTOGRAPHIC DEVICE AND METHOD FOR GENERATING PSEUDO-RANDOM NUMBERS

Title (de)

KRYPTOGRAFISCHE VORRICHTUNG UND VERFAHREN ZUR ERZEUGUNG VON PSEUDOZUFALLSZAHLEN

Title (fr)

DISPOSITIF ET PROCEDE DE CRYPTOGRAPHIE POUR GENERER DES NOMBRES PSEUDO-ALEATOIRES

Publication

EP 1984813 A2 20081029 (FR)

Application

EP 07731553 A 20070201

Priority

- FR 2007050725 W 20070201
- FR 0650506 A 20060213

Abstract (en)

[origin: WO2007093723A2] The invention concerns a cryptographic device and method for generating pseudo-random numbers (1), including the following steps: subdividing initial data (1) into a plurality of words (3) with definite b- bits in a finite body GF(2^b), assigning said words to cells (5) of a status board (7) to form an initial status block (13a); assembling the cells (5) of said status board (7) to assign a group (11) of cells to each set of d /b words, wherein d is a multiple of b strictly higher than b; and iteratively generating from said initial status block (13a), a succession of status blocks (13b) to form a final status block (13c), such that upon each iteration each set of d/b words of a current status block (13b) is replaced by at least another set of d/b words, using, to form a next status block, at least one reference table (9) comprising substitution elements with d-bits.

IPC 8 full level

G06F 7/58 (2006.01); **H04L 9/06** (2006.01); **H04L 9/22** (2006.01)

CPC (source: EP US)

G06F 7/582 (2013.01 - EP US); **H04L 9/0662** (2013.01 - EP US); H04L 2209/122 (2013.01 - EP US); H04L 2209/805 (2013.01 - EP US)

Citation (search report)

See references of WO 2007093723A2

Citation (examination)

K. FINKENZELLER: "RFID Handbook, Second Edition, pages 221-227, 278-284, 292-298", 2003, J. WILEY & SONS, Chichester, UK, ISBN: 978-0-470-84402-1, 348750

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 2897451 A1 20070817; EP 1984813 A2 20081029; US 2009022310 A1 20090122; WO 2007093723 A2 20070823; WO 2007093723 A3 20071025; WO 2007093723 B1 20071221

DOCDB simple family (application)

FR 0650506 A 20060213; EP 07731553 A 20070201; FR 2007050725 W 20070201; US 27858307 A 20070201