Title (en)

A METHOD OF PERFORMING MATHEMATICAL OPERATIONS IN AN ELECTRONIC DEVICE, A METHOD OF GENERATING PSEUDO-RANDOM NUMBERS IN AN ELECTRONIC DEVICE, AND A METHOD OF ENCRYPTING AND DECRYPTING ELECTRONIC DATA

Title (de)

VERFAHREN ZUM AUSFÜHREN EINER MATHEMATISCHEN FUNKTION IN EINEM ELEKTRONISCHEN BAUSTEIN UND VERFAHREN ZUR VERSCHLÜSSELUNG UND ENTSCHLÜSSELUNG VON ELEKTRONISCHEN DATEN

Title (fr)

PROCEDE PERMETTANT D'EFFECTUER DES OPERATIONS MATHEMATIQUES DANS UN DISPOSITIF ELECTRONIQUE, PROCEDE PERMETTANT DE GENERER DES NOMBRES PSEUDO-ALEATOIRES DANS UN DISPOSITIF ELECTRONIQUE ET PROCEDE PERMETTANT DE CRYPTER ET DE DECRYPTER DES DONNEES ELECTRONIQUES

Publication

EP 1360767 A2 20031112 (EN)

Application

EP 01270019 A 20011207

Priority

- DK 0100814 W 20011207
- DK PA200001838 A 20001207

Abstract (en)

[origin: WO0247272A2] A method of performing numerical computations in a mathematical system comprises expressing the mathematical system in discrete terms, using fixed-point variables in the computations, and extracting a sub-set of digits of a number. The sub-set of digits may represent a random or pseudo-random number. The mathematical system may be a system of non-linear differential equations, such as a chaotic system, for example a system with a positive Lyapunov exponent, or a discrete mapping, such as a logistic map, an Anosov or a Hénon map. The method is applicable to encryption and decryption algorithms, including stream ciphers and block ciphers, systems for generating a digital signature, Hash functions, and MAC (Message Authentication Code) functions. A test for periodical behaviour of a solution to the mathematical system is provided.

IPC 1-7

H04L 9/00

IPC 8 full level

G06F 7/58 (2006.01); **G06F 17/10** (2006.01); **G09C 1/00** (2006.01); **H04L 9/00** (2006.01); **H04L 9/22** (2006.01)

CPC (source: EP)

G06F 7/586 (2013.01); **G06F 17/10** (2013.01); **H04L 9/001** (2013.01); **H04L 9/0662** (2013.01); H04L 2209/26 (2013.01)

Citation (search report)

See references of WO 0247272A2

Citation (examination)

- SALIBRICI B.: "Fixed-point DSP chip can generate real-time random noise", EDN ELECTRICAL DESIGN NEWS, vol. 38, no. 9, 29 April 1993 (1993-04-29), ROGERS PUB. CO., ENGLEWOOD, COLO, USA, pages 119 - 122, XP000362820, ISSN: 0012-7515
- HAK FUI G. TAM: "STUDIES OF DISCRETE LOGISTIC MAP", 21 February 2003 (2003-02-21), Retrieved from the Internet <URL:http://www.phy.cuhk.edu.hk/sure/comments_2000/tam_paper.html> [retrieved on 20050818]

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)

WO 0247272 A2 20020613; **WO 0247272 A3 20030828**; AU 2053402 A 20020618; CA 2430858 A1 20020613; EP 1360767 A2 20031112; JP 2004530919 A 20041007

DOCDB simple family (application)

DK 0100814 W 20011207; AU 2053402 A 20011207; CA 2430858 A 20011207; EP 01270019 A 20011207; JP 2002548877 A 20011207