Title (en)

PSEUDO-RANDOM GENERATOR BASED ON A HASH CODING FUNCTION FOR CRYPTOGRAPHIC SYSTEMS REQUIRING RANDOM DRAWING

Title (de)

AUF EINER HASH-FUNKTION BASIERENDER PSEUDOZUFALLSGENERATOR FÜR GEHEIMÜBERTRAGUNSSYSTEME WELCHE EINE ZUFALLSZAHL BENÖTIGEN

Title (fr)

GENERATEUR PSEUDO-ALEATOIRE BASE SUR UNE FONCTION DE HACHAGE POUR SYSTEMES CRYPTOGRAPHIQUES NECESSITANT LE TIRAGE D'ALEAS

Publication

EP 0980607 A1 20000223 (FR)

Application

EP 98924379 A 19980505

Priority

- FR 9800901 W 19980505
- FR 9706198 A 19970507

Abstract (en)

[origin: FR2763194A1] The invention concerns a cryptographic system, normally requiring the drawing of a random number k, which is a whole number. The system is characterised in that it is operated by replacing said random number k by the value h (m/secret) in which h is a hash coding function, m is the message intervening in said system and "secret" is a secret unknown to the world outside the cryptographic system. The invention is particularly applicable to communicating media such as smart cards, PCMCIA cards, badges, contactless cards or any other portable medium.

IPC 1-7

H04L 9/32

IPC 8 full level

G07F 7/10 (2006.01); **G09C 1/00** (2006.01); **H04L 9/32** (2006.01)

CPC (source: EP)

G06Q 20/341 (2013.01); **G06Q 20/40975** (2013.01); **G07F 7/1008** (2013.01); **H04L 9/0841** (2013.01); **H04L 9/3252** (2013.01); H04L 2209/20 (2013.01); H04L 2209/80 (2013.01)

Citation (search report)

See references of WO 9851038A1

Designated contracting state (EPC)

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

DOCDB simple family (publication)

FR 2763194 A1 19981113; **FR 2763194 B1 20000728**; AU 7659598 A 19981127; CA 2288767 A1 19981112; CN 1262830 A 20000809; EP 0980607 A1 20000223; JP 2001507479 A 20010605; WO 9851038 A1 19981112

DOCDB simple family (application)

FR 9706198 A 19970507; AU 7659598 A 19980505; CA 2288767 A 19980505; CN 98806980 A 19980505; EP 98924379 A 19980505; FR 9800901 W 19980505; JP 54778798 A 19980505