Title (en)

GENERATOR AND METHOD OF GENERATING A SECRET-KEY PSEUDO-RANDOM FUNCTION

Title (de)

GENERATOR UND VERFAHREN ZUM ERZEUGEN EINER GEHEIMSCHLÜSSEL-PSEUDOZUFALLSFUNKTION

Title (fr)

GENERATEUR ET PROCEDE DE GENERATION DE FONCTION PSEUDO-ALEATOIRE A CLE SECRETE

Publication

EP 2204007 A2 20100707 (FR)

Application

EP 08829862 A 20080826

Priority

- FR 2008051529 W 20080826
- FR 0757357 A 20070905

Abstract (en)

[origin: WO2009030857A2] The invention relates to a generator of a pseudo-random function with secret key K from an input block of m bits to an output block of n bits using a determined number a of cryptographic schemes F1(m1, n1),..., Fi(mi, ni),..., Fa(ma,na) nested in layers according to a recursive structure, each current cryptographic scheme Fi(mi, ni) associating ni output bits with mi input bits in a number of rounds ri, each round using an internal elementary function f(i) constructed on the basis of ti cryptographic schemes Fi+1(mi+1,ni+1) from ni+1 bits, to mi+1 bits, with ni+1 ni,mi+1 mi and ti = 1, each cryptographic scheme Fi(mi, ni) defining a minimum number of operations comp(mi, ni, ri), dependent on said number of rounds ri, required in order to distinguish it from a random function associating mi input bits ni output bits, the generator comprising calculation means (7) for calculating, for each cryptographic scheme Fi(mi, ni), said number of rounds ri so that said number of operations comp(mi, ni, ri) associated therewith is greater than or equal to a predetermined number 2c, c being an integer.

IPC 8 full level

H04L 9/06 (2006.01)

CPC (source: EP)

H04L 9/0625 (2013.01); **H04L 9/0662** (2013.01)

Citation (search report)

See references of WO 2009030857A2

Designated contracting state (EPC)

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MT NL NO PL PT RO SE SI SK TR

Designated extension state (EPC)

AL BA MK RS

DOCDB simple family (publication)

FR 2920617 A1 20090306; EP 2204007 A2 20100707; WO 2009030857 A2 20090312; WO 2009030857 A3 20090514

DOCDB simple family (application)

FR 0757357 A 20070905; EP 08829862 A 20080826; FR 2008051529 W 20080826