Title (en)

METHOD AND DEVICE FOR ENCRYPTION/DECRYPTION OF AN INPUT DATA SEQUENCE

Title (de)

VERFAHREN UND EINRICHTUNG ZUR VERSCHLÜSSELUNG/ENTSCHLÜSSELUNG EINER EINGANGSDATENSEQUENZ

Title (fr)

PROCEDES ET DISPOSITIFS CRYPTOGRAPHIQUES DE GENERATION PSEUDO-ALEATOIRE DE CHIFFREMENT DE DONNEES ET DE HACHAGE CRYPTOGRAPHIQUE D'UN MESSAGE

Publication

EP 2165456 A2 20100324 (FR)

Application

EP 08760471 A 20080604

Priority

- EP 2008056889 W 20080604
- EP 07301086 A 20070605
- EP 08760471 A 20080604

Abstract (en)

[origin: EP2001154A1] The method involves successively applying a preset number of permutations on a provisional vector (Vprov) to generate a current value (Vn) of a state vector (V) during each iteration. The provisional vector has an intermediate vector (Vint1) formed from a section of a previous value (Vn-1) of the state vector generated at previous iteration. Each permutation is associated to a bit of a permutation key (C) issued from selection of certain bits among bits of the intermediate vector. The current value is obtained from a section of a resultant vector from application of permutations. Independent claims are also included for the following: (1) a method for encrypting an input data sequence (2) a device for encrypting an input data sequence, comprising a cryptographic generator (3) a cryptographic hashing device comprising a cryptographic generator (4) a computer program comprising instructions to perform a method for generating a pseudo-random data sequence (5) a computer program comprising instructions to perform a method for encrypting an input data sequence.

IPC 8 full level

H04L 9/18 (2006.01); **H04L 9/06** (2006.01)

CPC (source: EP KR US)

G09C 1/00 (2013.01 - EP US); **H04L 9/06** (2013.01 - KR); **H04L 9/0643** (2013.01 - EP US); **H04L 9/0656** (2013.01 - KR); **H04L 9/0662** (2013.01 - EP US); H04L 2209/125 (2013.01 - EP US)

Citation (search report)

See references of WO 2008148784A2

Citation (examination)

- JEAN-PIERRE TILLICH ET AL: "Hashing with SL 2", 21 August 1994, ADVANCES IN CRYPTOLOGY (CRYPTO). SANTA BARBARA, AUG. 21 - 25, 1994; [PROCEEDINGS OF THE ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE (CRYPTO)], BERLIN, SPRINGER, DE, PAGE(S) 40 - 49, ISBN: 978-3-540-58333-2, XP019194317
- JEAN-PIERRE TILLICH ET AL: "Group-theoretic hash functions", 19 July 1993, ALGEBRAIC CODING. FIRST FRENCH-ISRAELI WORKSHOP, SPRINGER, DE, PAGE(S) 90 - 110, ISBN: 978-3-540-57843-7, XP047000936

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)

EP 2001154 A1 20081210; AU 2008258582 A1 20081211; AU 2008258582 B2 20130530; CA 2687822 A1 20081211; CA 2687822 C 20160726; CN 101779412 A 20100714; CN 101779412 B 20141217; EP 2165456 A2 20100324; JP 2010529496 A 20100826; JP 2014139687 A 20140731; JP 5551065 B2 20140716; JP 5822970 B2 20151125; KR 101564601 B1 20151030; KR 20100031717 A 20100324; US 2010142705 A1 20100610; US 8837719 B2 20140916; WO 2008148784 A2 20081211; WO 2008148784 A3 20090820

DOCDB simple family (application)

EP 07301086 A 20070605; AU 2008258582 A 20080604; CA 2687822 A 20080604; CN 200880102186 A 20080604; EP 08760471 A 20080604; EP 2008056889 W 20080604; JP 2010510778 A 20080604; JP 2014064046 A 20140326; KR 20107000092 A 20080604; US 60262608 A 20080604