Title (en)

METHOD AND SYSTEM FOR DERIVING AN ENCRYPTION KEY USING JOINT RANDOMNESS NOT SHARED BY OTHERS

Title (de)

VERFAHREN UND SYSTEM ZUM ABLEITEN EINES VERSCHLÜSSELUNGSSCHLÜSSELS UNTER VERWENDUNG EINER NICHT MIT ANDEREN GETEILTEN VERBUNDZUFÄLLIGKEIT

Title (fr)

PROCEDE ET SYSTEME PERMETTANT DE DERIVER UNE CLE DE CHIFFREMENT AU MOYEN D'UN CARACTERE ALEATOIRE COMBINE NON PARTAGE PAR D'AUTRES

Publication

EP 1847060 A4 20110914 (EN)

Application

EP 06718847 A 20060119

Priority

- US 2006001839 W 20060119
- US 64748205 P 20050127
- US 71617705 P 20050912
- US 73433105 P 20051107
- US 31838105 A 20051223

Abstract (en)

[origin: WO2006081122A2] The present invention is related to a method and system for deriving an encryption key using joint randomness not shared by others (JRNSO). Communicating entities generate JRNSO bits from a channel impulse response (CIR) estimate and the JRNSO bits are used in generation of an encryption key. The authentication type may be IEEE 802.1x or a pre-shared key system. In an IEEE 802.1x system, a master key, a pairwise master key or a pairwise transient key may be generated using the JRNSO bits. The encryption key may be generated by using a Diffie-Hellman key derivation algorithm.

IPC 8 full level

H04L 9/00 (2006.01); **H04K 1/00** (2006.01); **H04L 9/08** (2006.01); **H04L 9/32** (2006.01)

CPC (source: EP KR)

H04L 9/06 (2013.01 - KR); **H04L 9/08** (2013.01 - KR); **H04L 9/0841** (2013.01 - EP); **H04L 9/0875** (2013.01 - EP); **H04L 9/32** (2013.01 - KR); **H04L 9/321** (2013.01 - EP); **H04L 63/06** (2013.01 - EP); **H04W 12/0431** (2021.01 - EP); H04L 63/065 (2013.01 - EP); H04L 63/0892 (2013.01 - EP); H04L 63/205 (2013.01 - EP); H04L 2209/34 (2013.01 - EP); H04L 2209/80 (2013.01 - EP); H04L 2463/061 (2013.01 - EP)

Citation (search report)

- [I] HERSHEY J E ET AL: "UNCONVENTIONAL CRYPTOGRAPHIC KEYING VARIABLE MANAGEMENT", IEEE TRANSACTIONS ON COMMUNICATIONS, IEEE SERVICE CENTER, PISCATAWAY, NJ. USA, vol. 43, no. 1, 1 January 1995 (1995-01-01), pages 3 - 06, XP000487370, ISSN: 0090-6778, DOI: 10.1109/26.385951
- [A] HAVISH KOORAPATY ET AL: "Secure Information Transmission for Mobile Radio", IEEE COMMUNICATIONS LETTERS, IEEE SERVICE CENTER, PISCATAWAY, NJ, US, vol. 4, no. 2, 1 February 2000 (2000-02-01), XP011010169, ISSN: 1089-7798
- See references of WO 2006081122A2

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)

WO 2006081122 A2 20060803; **WO 2006081122 A3 20071122**; CA 2596067 A1 20060803; CA 2596067 C 20130917; CN 101951383 A 20110119; CN 101951383 B 20130619; EP 1847060 A2 20071024; EP 1847060 A4 20110914; JP 2008529413 A 20080731; JP 4734344 B2 20110727; KR 101011470 B1 20110128; KR 101253370 B1 20130411; KR 20070088821 A 20070829; KR 20070096008 A 20071001; KR 20110076992 A 20110706; MX 2007009063 A 20071002; NO 20074210 L 20071024; TW 200633460 A 20060916; TW 200723818 A 20070616; TW I378701 B 20121201; TW I404393 B 20130801

DOCDB simple family (application)

US 2006001839 W 20060119; CA 2596067 A 20060119; CN 201010298170 A 20060119; EP 06718847 A 20060119; JP 2007553138 A 20060119; KR 20077018125 A 20060119; KR 20077018514 A 20060119; KR 20117010823 A 20060119; MX 2007009063 A 20060119; NO 20074210 A 20070816; TW 95102241 A 20060120; TW 95128389 A 20060120