Title (en)

METHOD AND SYSTEM FOR HIGH-SPEED ENCRYPTION

Title (de)

VERFAHREN UND SYSTEM FÜR HOCHGESCHWINDIGKEITSVERSCHLÜSSELUNG

Title (fr)

PROCEDE ET SYSTEME DE CHIFFREMENT A HAUT DEBIT

Publication

EP 1911190 A2 20080416 (FR)

Application

EP 06794528 A 20060803

Priority

- FR 2006050787 W 20060803
- FR 0552436 A 20050804

Abstract (en)

[origin: WO2007015034A2] The invention relates to a method and a system for encryption or decryption on the fly of a high-speed information stream. The information is in the form of blocks of bits (M<SUB>0</SUB>, M<SUB>1</SUB>,..., M<SUB>n-1 </SUB>), themselves grouped in sectors (S). The invention uses a block encryption method, for example, AES (Advanced Encryption Standard), carried out twice per sector and producing, for each sector, a secondary key (KS) used by a more rapid algorithm (for example XOR mask). The secondary keys are dependent on the sector content and the position thereof in the stream. The same information would be differently encrypted according to the context thereof. On decryption, the secondary key can be recalculated from the encrypted sector by means of the block encryption algorithm. The number of blocks per sector is adjusted to achieve the best compromise between speed of calculation and cryptographic security.

IPC 8 full level

H04L 9/06 (2006.01)

CPC (source: EP)

H04L 9/0631 (2013.01); H04L 2209/046 (2013.01); H04L 2209/30 (2013.01)

Citation (search report)

See references of WO 2007015034A2

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)

FR 2889637 A1 20070209; **FR 2889637 B1 20071019**; EP 1911190 A2 20080416; WO 2007015034 A2 20070208; WO 2007015034 A3 20070913

DOCDB simple family (application)

FR 0552436 A 20050804; EP 06794528 A 20060803; FR 2006050787 W 20060803