Title (en)

MULTI-LANE HIGH-SPEED ENCRYPTION AND DECRYPTION

Title (de)

MEHRSPURIGE HOCHGESCHWINDIGKEITSVERSCHLÜSSELUNG UND -ENTSCHLÜSSELUNG

Title (fr)

CHIFFREMENT ET DECHIFFREMENT MULTVOIE ULTRARAPIDE

Publication

EP 1955473 A1 20080813 (EN)

Application

EP 06821487 A 20061117

Priority

- IB 2006054319 W 20061117
- US 73921905 P 20051123

Abstract (en)

[origin: WO2007060587A1] An encryption system is configured to include a combination of block (130) and stream (150) cipher generators. The block cipher generator (130) provides a changing key (149) that is used to periodically re-key one or more stream cipher generators (150). Preferably an AES block encryptor (135) provides a set of 128-bit ciphers (139) that are used to provide a stream of 576-bit keys (149) that is used to periodically re-key one or more SNO W-2 stream cipher generators (150). The output (159) of the stream cipher generators (150) are used to encrypt multiple input data streams (263-264), or 'lanes' of data, using an optimized arrangement of the block (130) and stream (150) ciphers relative to these multiple lanes of data (263-264).

IPC 8 full level

H04L 9/18 (2006.01)

CPC (source: EP KR)

H04L 9/06 (2013.01 - KR); **H04L 9/0631** (2013.01 - EP); **H04L 9/065** (2013.01 - KR); **H04L 9/0662** (2013.01 - EP); H04L 2209/125 (2013.01 - EP)

Citation (search report)

See references of WO 2007060587A1

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 2007060587 A1 20070531; CN 101313509 A 20081126; EP 1955473 A1 20080813; JP 2009516976 A 20090423; KR 20080073348 A 20080808; RU 2008125109 A 20091227

DOCDB simple family (application)

IB 2006054319 W 20061117; CN 200680043844 A 20061117; EP 06821487 A 20061117; JP 2008541867 A 20061117; KR 20087015229 A 20080623; RU 2008125109 A 20061117