Title (en)

METHOD AND APPARATUS FOR PERFORMING SYMMETRICAL STREAM ENCRYPTION OF DATA

Title (de)

VERFAHREN UND VORRICHTUNG ZUR DURCHFÜHRUNG EINER SYMMETRISCHEN STROMVERSCHLÜSSELUNG VON DATEN

Title (fr)

PROCÉDÉ ET DISPOSITIF PERMETTANT D'EFFECTUER UN CHIFFREMENT DE FLUX SYMÉTRIQUE DE DONNÉES

Publication

EP 2647157 A1 20131009 (DE)

Application

EP 11796910 A 20111201

Priority

- AT 20072010 A 20101202
- AT 2011000483 W 20111201

Abstract (en)

[origin: WO2012071597A1] In a method for performing symmetrical stream encryption of data using a key stream and for transmitting the encrypted data, wherein the key stream is generated using at least one feedback shift register which is filled with a defined bit sequence in order to initialize it, the data to be encrypted are split into data packets, with each data packet being encrypted separately. The feedback shift register(s) is/are reinitialised for the encryption of each data packet, with the feedback shift register(s) being initialized by using at least a first bit sequence and a second bit sequence in each case, wherein the first bit sequence is added to the respectively encrypted data packet in plain text or in encoded form and the second bit sequence represents a secret key, which is not added to the encrypted data packets. The encrypted data packets are transmitted in packet-switched fashion together with the respective added bit sequence and possibly header data.

IPC 8 full level

H04L 9/26 (2006.01); **G06F 7/58** (2006.01)

CPC (source: EP US)

H04L 9/0668 (2013.01 - EP US); **H04L 63/0435** (2013.01 - US); **H04L 63/0457** (2013.01 - EP US); G06F 7/584 (2013.01 - EP US); H04L 2209/12 (2013.01 - EP US); H04L 2463/121 (2013.01 - EP US)

Citation (search report)

See references of WO 2012071597A1

Designated contracting state (EPC)

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

DOCDB simple family (publication)

WO 2012071597 A1 20120607; AT 510730 A1 20120615; AT 510730 B1 20130615; EP 2647157 A1 20131009; US 2017264598 A1 20170914

DOCDB simple family (application)

AT 2011000483 W 20111201; AT 20072010 A 20101202; EP 11796910 A 20111201; US 201113991389 A 20111201