Title (en)

METHOD FOR DETERMINING A CHAIN OF KEYS, METHOD FOR TRANSMITTING A PARTIAL CHAIN OF THE KEYS, COMPUTER SYSTEM AND CHIP CARD

Title (de)

VERFAHREN ZUR BESTIMMUNG EINER KETTE VON SCHLÜSSELN, VERFAHREN ZUR ÜBERTRAGUNG EINER TEILKETTE DER SCHLÜSSEL, COMPUTERSYSTEM UND CHIPKARTE

Title (fr)

PROCÉDÉ DE DÉTERMINATION D'UNE CHAÎNE DE CLÉS, PROCÉDÉ DE TRANSMISSION D'UNE CHAÎNE PARTIELLE DE CLÉS, SYSTÈME INFORMATIQUE ET CARTE À PUCE

Publication

EP 2321927 A1 20110518 (DE)

Application

EP 09738250 A 20090504

Priority

- EP 2009055350 W 20090504
- DE 102008021933 A 20080502

Abstract (en)

[origin: WO2009133206A1] The invention relates to a method for determining a resultant chain (404) of keys, having the following steps: a first chain (400) of first keys is determined, wherein a predecessor key can be calculated from each successor key in the first chain by using a first function, wherein the first function is a one-way function or a one-way trapdoor function; a second chain (402) of second keys is determined by iteratively using a second function, wherein the second function is a one-way function or a one-way trapdoor function, wherein at least one first key in the first chain and one second key in the second chain are respectively used to calculate each key in the resultant chain.

IPC 8 full level

H04L 9/08 (2006.01); **H04L 9/12** (2006.01); **H04L 9/18** (2006.01)

CPC (source: EP US)

H04L 9/0861 (2013.01 - EP US); **H04L 9/12** (2013.01 - EP US); **H04L 9/50** (2022.05 - EP); H04L 9/50 (2022.05 - US); H04L 2209/127 (2013.01 - EP US); H04L 2209/805 (2013.01 - EP US)

Citation (search report)

See references of WO 2009133206A1

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 MK MT NL NO PL PT RO SE SI SK TR

Designated extension state (EPC)

AL BA RS

DOCDB simple family (publication)

DE 102008021933 A1 20091105; **DE 102008021933 B4 20110407**; EP 2321927 A1 20110518; US 2012027212 A1 20120202; WO 2009133206 A1 20091105

DOCDB simple family (application)

DE 102008021933 A 20080502; EP 09738250 A 20090504; EP 2009055350 W 20090504; US 200913124080 A 20090504