Title (en)

METHOD FOR ENCODED DATA EXCHANGE, AND COMMUNICATION SYSTEM

Title (de)

VERFAHREN ZUM VERSCHLÜSSELTEN DATENAUSTAUSCH UND KOMMUNIKATIONSSYSTEM

Title (fr)

PROCÉDÉ D'ÉCHANGE CODÉ DE DONNÉES ET SYSTÈME DE COMMUNICATION

Publication

EP 2277279 A1 20110126 (DE)

Application

EP 09749677 A 20090324

Priority

- EP 2009053422 W 20090324
- EP 08009277 A 20080520
- EP 09749677 A 20090324

Abstract (en)

[origin: EP2124382A1] The method involves calculating a result of a scalar multiplication by the latter subscriber on a query of the former subscriber. A function value is determined from the result of the scalar multiplication with the help of non-injective reference, so that the function value does not allow clear conclusion on the result. The function value is transmitted back to the former subscriber as a response. The response comprises an x-coordinate of a point on the elliptical curve. An independent claim is included for a communication system for authentication of the subscribers of the communication system using cryptography with a data communicative connection.

IPC 8 full level

H04L 9/30 (2006.01); **H04L 9/32** (2006.01)

CPC (source: EP US)

G06F 7/725 (2013.01 - EP US); **H04L 9/3073** (2013.01 - EP US); **H04L 9/3252** (2013.01 - EP US); **H04L 9/3271** (2013.01 - EP US); H04L 2209/805 (2013.01 - EP US)

Citation (search report)

See references of WO 2009141187A1

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)

EP 2124382 A1 20091125; CN 102037675 A 20110427; EP 2277279 A1 20110126; US 2011107097 A1 20110505; WO 2009141187 A1 20091126

DOCDB simple family (application)

EP 08009277 A 20080520; CN 200980118112 A 20090324; EP 09749677 A 20090324; EP 2009053422 W 20090324; US 99384009 A 20090324