

Title (en)

KEY GENERATION AND PACE WITH PROTECTION AGAINST SIDE CHANNEL ATTACKS

Title (de)

SCHLÜSSELGENERIERUNG UND PACE MIT SICHERUNG GEGEN SEITENKANALANGRIFFE

Title (fr)

GÉNÉRATION DE CLÉ ET PROTOCOLE PACE AVEC PROTECTION CONTRE DES ATTAQUES PAR CANAL LATÉRAL

Publication

EP 4101118 A1 20221214 (DE)

Application

EP 21703830 A 20210203

Priority

- DE 102020000814 A 20200207
- EP 2021025040 W 20210203

Abstract (en)

[origin: WO2021156005A1] The invention provides a method for key generation, set up in a client processor device, by means of which a second public client key (Pc') of the client is generated, wherein the public key (Pc') is formed by a calculation, or sequence of calculations, that does not contain an operation whose result is exclusively dependent on the nonce (s) and at least one public value, or wherein the public key (Pc') is formed by a calculation, or sequence of calculations, in which in each operation in which the nonce (s) is used, at least one non-public value is used, in particular the first private client key (kc') or the second private client key (kc'), for example as the result of the calculation $Pc' = (kc' \cdot s) \cdot G + (kc' \cdot kc.) \cdot Pt$. The invention also specifies a method for authentication and key agreement between a client and a terminal using such a method for key generation, in particular for authentication and key agreement based on the PACE protocol in a form modified according to the invention.

IPC 8 full level

H04L 9/00 (2022.01); **H04L 9/08** (2006.01)

CPC (source: EP US)

H04L 9/003 (2013.01 - EP US); **H04L 9/0825** (2013.01 - US); **H04L 9/0841** (2013.01 - EP US); **H04L 9/0869** (2013.01 - US); **H04L 9/3066** (2013.01 - US); **H04L 9/3226** (2013.01 - US); **H04L 2209/046** (2013.01 - EP)

Citation (search report)

See references of WO 2021156005A1

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

Designated extension state (EPC)

BA ME

Designated validation state (EPC)

KH MA MD TN

DOCDB simple family (publication)

DE 102020000814 A1 20210812; EP 4101118 A1 20221214; US 2023041237 A1 20230209; WO 2021156005 A1 20210812

DOCDB simple family (application)

DE 102020000814 A 20200207; EP 2021025040 W 20210203; EP 21703830 A 20210203; US 202117760016 A 20210203