Title (en)
SYMMETRIC CRYPTOGRAPHY METHOD AND DEVICE FOR VEHICLE PROCESSOR

Title (de)
VERFAHREN UND VORRICHTUNG FÜR SYMMETRISCHE KRYPTOGRAFIE FÜR EINEN FAHRZEUGPROZESSOR

Title (fr)
PROCÉDÉ ET DISPOSITIF DE CRYPTOGRAPHIE SYMÉTRIQUE POUR CALCULATEUR DE VÉHICULE

Publication
**EP 3932001 A1 20220105 (FR)**

Application
**EP 20707718 A 20200131**

Priority
• FR 1902095 A 20190228
• FR 2020050152 W 20200131

Abstract (en)
[origin: WO2020174137A1] The invention relates to a method and to a device for deciphering encrypted data using a secret key. To this end, a random duration is generated. A first final value of a first internal counter of the first device is determined depending on the random duration. One or more requests are transmitted to a second device. These requests allow the second device to determine a second final value of a second internal counter of the second device. The one or more requests are transmitted in such a way that the second final value is identical to the first final value. The secret key is generated by the first device using the first final value and the same secret key is also generated by the second device using the second final value. The data to be transmitted by the second device to the first device are encrypted with the secret key that the second device generated.

IPC 8 full level
**H04L 9/08** (2006.01); **G06F 21/57** (2013.01)

CPC (source: EP)
**G06F 21/572** (2013.01); **H04L 9/0825** (2013.01); **H04L 9/0869** (2013.01); H04L 2209/84 (2013.01)

Citation (search report)
See references of WO 2020174137A1

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

DOCDB simple family (publication)
**WO 2020174137 A1 20200903**; CN 113491084 A 20211008; EP 3932001 A1 20220105; FR 3093363 A1 20200904; FR 3093363 B1 20211203

DOCDB simple family (application)
**FR 2020050152 W 20200131**; CN 202080017209 A 20200131; EP 20707718 A 20200131; FR 1902095 A 20190228