Title (en)

CRYPTOGRAPHIC DATA VERIFICATION METHOD

Title (de)

VERFAHREN ZUR PRÜFUNG VON KRYPTOGRAFISCHEN DATEN

Title (fr)

MÉTHODE CRYPTOGRAPHIQUE DE VÉRIFICATION DES DONNÉES

Publication

EP 3928232 A1 20211229 (FR)

Application

EP 20704320 A 20200217

Priority

- FR 1901648 A 20190219
- EP 2020054126 W 20200217

Abstract (en)

[origin: CA3128869A1] The invention relates to a comparison method implemented by at least one apparatus (A; B), between a first and a second dataset, in particular with a view to determining whether these two datasets are identical, this method not requiring the presence of these two datasets on the apparatus, and comprising the following steps: a) mixing a number, referred to as the mixing number, with the first dataset, using a mixing function (105; 405), in order to obtain mixed data, b) hashing the mixed data using a hash function (106); 406), and c) comparing the hash thus obtained in step b) with a third dataset assumed to be the hash of the second dataset mixed with the same mixing number as that used in step a) and with the same mixing function (105; 405).

IPC 8 full level

G06F 21/44 (2013.01); **G06F 21/64** (2013.01); **H04L 9/06** (2006.01); **H04L 9/08** (2006.01); **H04L 9/32** (2006.01); **H04L 29/06** (2006.01)

CPC (source: EP KR US)

G06F 21/44 (2013.01 - EP KR); **G06F 21/602** (2013.01 - KR); **G06F 21/64** (2013.01 - EP KR US); **H04L 9/0643** (2013.01 - KR US); **H04L 9/0869** (2013.01 - EP KR); **H04L 9/3239** (2013.01 - EP KR US); **H04L 63/123** (2013.01 - EP KR)

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)

FR 3092923 A1 20200821; **FR 3092923 B1 20210521**; AU 2020225314 A1 20210902; CA 3128869 A1 20200827; CN 113811874 A 20211217; EP 3928232 A1 20211229; JP 2022521525 A 20220408; KR 20210153595 A 20211217; US 11914754 B2 20240227; US 2021165914 A1 20210603; US 2024160792 A1 20240516; WO 2020169542 A1 20200827

DOCDB simple family (application)

FR 1901648 A 20190219; AU 2020225314 A 20200217; CA 3128869 A 20200217; CN 202080015504 A 20200217; EP 2020054126 W 20200217; EP 20704320 A 20200217; JP 2021549168 A 20200217; KR 20217026080 A 20200217; US 202016793123 A 20200218; US 202418405094 A 20240105