Title (en)

METHOD FOR PROBABILISTIC DIGITAL SIGNATURES

Title (de)

VERFAHREN ZUR ERZEUGUNG VON WAHRSCHEINLICHKEITSGESTÜTZTEN SIGNATUREN

Title (fr)

PROCEDE DE SIGNATURES NUMERIQUES PROBABILISTES

Publication

EP 1269683 A1 20030102 (FR)

Application

EP 01917165 A 20010316

Priority

- FR 0100795 W 20010316
- FR 0003918 A 20000328

Abstract (en)

[origin: WO0174009A1] The invention concerns a method for probabilistic signatures of a message, between a signatory and a verifier, from an algorithm based on the calculation of a discrete logarithm. The invention is characterised in that it consists: for the signatory, in generating at least two signatures for the same non-hash coded message, said signatures being calculated by the algorithm with common public and private parameters using respectively different random variables, and for the verifier, in verifying all the signatures of said message.

IPC 1-7

H04L 9/32

IPC 8 full level

H04L 9/32 (2006.01)

CPC (source: EP US)

H04L 9/3013 (2013.01 - EP US); **H04L 9/3252** (2013.01 - EP US)

Citation (search report)

See references of WO 0174009A1

Designated contracting state (EPC)

AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR

DOCDB simple family (publication)

WO 0174009 A1 20011004; AU 4425901 A 20011008; EP 1269683 A1 20030102; FR 2807248 A1 20011005; FR 2807248 B1 20020628; US 2001056537 A1 20011227

DOCDB simple family (application)

FR 0100795 W 20010316; AU 4425901 A 20010316; EP 01917165 A 20010316; FR 0003918 A 20000328; US 80296801 A 20010312