Title (en)

METHOD OF GENERATING A SIGNATURE WITH PROOF OF TIGHT SECURITY, ASSOCIATED VERIFICATION METHOD AND ASSOCIATED SIGNATURE SCHEME THAT ARE BASED ON THE DIFFIE-HELLMAN MODEL

Title (de)

VERFAHREN ZUR ERZEUGUNG EINER SIGNATUR MIT BEWEIS DER STRENGEN SICHERHEIT, ZUGEHÖRIGES VERIFIZIERUNGSVERFAHREN UND ZUGEHÖRIGES SIGNATURSCHEMA AUF BASIS DES DIFFIE-HELLMAN-MODELLS

Title (fr)

PROCÉDÉ DE GÉNÉRATION DE SIGNATURE AVEC PREUVE DE SÉCURITÉ "TIGHT", PROCÉDÉ DE VÉRIFICATION ET SCHÉMA DE SIGNATURE ASSOCIÉS BASÉS SUR LE MODÈLE DE DIFFIE-HELLMAN

Publication

EP 1820297 A1 20070822 (FR)

Application

EP 05858607 A 20051018

Priority

- EP 2005055347 W 20051018
- FR 0411789 A 20041105

Abstract (en)

[origin: FR2877788A1] Electronic signature generating method involves generating a random number from a set of integer modulo, and calculating and storing predetermined values using the hashing functions. An electronic signature of a message is produced based on the calculated predetermined values. Independent claims are also included for: (A) A method for verifying electronic signature; (B) An electronic signature scheme; and (C) A portable electronic component including a unit for implementing a method for generating and verifying an electronic signature.

IPC 8 full level

H04L 9/32 (2006.01)

CPC (source: EP US)

H04L 9/302 (2013.01 - EP US); **H04L 9/3249** (2013.01 - EP US); H04L 2209/68 (2013.01 - EP US)

Citation (search report)

See references of WO 2007065468A1

Designated contracting state (EPC)

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI SK TR

Designated extension state (EPC)

AL BA HR MK YU

DOCDB simple family (publication)

FR 2877788 A1 20060512; **FR 2877788 B1 20070105**; EP 1820297 A1 20070822; US 2009138718 A1 20090528; WO 2007065468 A1 20070614

DOCDB simple family (application)

FR 0411789 A 20041105; EP 05858607 A 20051018; EP 2005055347 W 20051018; US 66706205 A 20051018