Title (en)

CRYPTOGRAPHY METHOD ON ELLIPTIC CURVES

Title (de)

KRYPTOGRAPHISCHES VERFAHREN ÜBER ELLIPTISCHE KURVEN

Title (fr)

PROCEDE DE CRYPTOGRAPHIE SUR COURBES ELLIPTIQUES

Publication

EP 1277307 A1 20030122 (FR)

Application

EP 01927999 A 20010418

Priority

- FR 0101195 W 20010418
- FR 0005006 A 20000418

Abstract (en)

[origin: WO0180481A1] The invention concerns a cryptography method for generating probabilistic digital signatures and/or for a key-exchange a protocol and/or for an encryption algorithm, said method being based on the use of a public key algorithm on abnormal binary elliptic curve (E) (Koblitz curve) whereon a point P (x, y) is selected, pairs (k>i<, P>i<) being stored with P>i< the point corresponding to the scalar multiplication of the point P by k>i<, said method comprising steps which consist in generating a random variable (k) and in calculating a point C corresponding to the scalar multiplication of P by k (C = k.P). The invention is characterised in that the generation of said random variable (k) and the calculation of the point C are performed simultaneously.

IPC 1-7

H04L 9/30; G06F 7/72

IPC 8 full level

G09C 1/00 (2006.01); **H04L 9/30** (2006.01); G06F 7/72 (2006.01)

CPC (source: EP US)

H04L 9/0841 (2013.01 - EP US); **H04L 9/3066** (2013.01 - EP US); **H04L 9/3252** (2013.01 - EP US); G06F 7/725 (2013.01 - EP US); H04L 2209/08 (2013.01 - EP US)

Citation (search report)

See references of WO 0180481A1

Cited by

CN102546162A

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 0180481 A1 20011025; AU 5487801 A 20011030; CN 1425231 A 20030618; EP 1277307 A1 20030122; FR 2807898 A1 20011019; FR 2807898 B1 20020628; JP 2004501385 A 20040115; MX PA02010310 A 20030425; US 2003152218 A1 20030814; US 7218735 B2 20070515

DOCDB simple family (application)

FR 0101195 W 20010418; AU 5487801 A 20010418; CN 01808226 A 20010418; EP 01927999 A 20010418; FR 0005006 A 20000418; JP 2001576610 A 20010418; MX PA02010310 A 20010418; US 25712903 A 20030403