Title (en)

METHOD FOR GENERATING PSEUDO RANDOM NUMBERS AND METHOD FOR ELECTRONIC SIGNATURES

Title (de)

VERFAHREN ZUM ERZEUGEN VON PSEUDOZUFALLSZAHLEN UND VERFAHREN FÜR ELEKTRONISCHE SIGNATUR

Title (fr)

PROCEDE DESTINE A GENERER DES NOMBRES PSEUDO-ALEATOIRES ET PROCEDE DE SIGNATURE ELECTRONIQUE

Publication

EP 1222527 A1 20020717 (DE)

Application

EP 00958257 A 20000816

Priority

- DE 0002776 W 20000816
- DE 19939059 A 19990818

Abstract (en)

[origin: WO0113218A1] The invention relates to a method for generating pseudo random numbers and a method for electronic signatures. According to the inventive method for generating pseudo random numbers, points are determined on at least two different elliptical curves. A pseudo random number is produced respectively by linking the points. The linking of points of different elliptical curves to generate a pseudo random number makes it impossible to deduce the individual elliptical curves on the basis of the pseudo random numbers. The cryptographic security of the inventive method is thus tremendously increased because the computation of discrete logarithms is made impossible.

IPC 1-7

G06F 7/58; H04L 9/32

IPC 8 full level

G06F 7/58 (2006.01); **G09C 1/00** (2006.01); **H04L 9/22** (2006.01); **H04L 9/30** (2006.01); **H04L 9/32** (2006.01); G06F 7/72 (2006.01)

CPC (source: EP)

G06F 7/584 (2013.01); **H04L 9/0656** (2013.01); **H04L 9/3066** (2013.01); **H04L 9/3247** (2013.01); G06F 7/725 (2013.01)

Citation (search report)

See references of WO 0113218A1

Designated contracting state (EPC)

CH DE FR GB LI

DOCDB simple family (publication)

WO 0113218 A1 20010222; CA 2381937 A1 20010222; EP 1222527 A1 20020717; JP 2003507761 A 20030225

DOCDB simple family (application)

DE 0002776 W 20000816; CA 2381937 A 20000816; EP 00958257 A 20000816; JP 2001517250 A 20000816