Title (en)

ELLIPTIC CURVE CRYPTOSYSTEMS FOR LOW MEMORY DEVICES

Title (de)

AUF ELLIPTISCHEN KURVEN BASIERENDES KRYPTOSYSTEM FÜR VORRICHTUNGEN MIT GERINGER SPEICHERKAPAZITÄT

Title (fr)

SYSTEMES DE CRYPTAGE A COURBE ELLIPTIQUE POUR DISPOSITIFS A MEMOIRE BASSE

Publication

EP 1112637 A1 20010704 (EN)

Application

EP 99949599 A 19990907

Priority

- US 9920411 W 19990907
- US 9942498 P 19980908

Abstract (en)

[origin: WO0014924A1] Each participant in a cryptographic system selects its own elliptic curve and verifies that the elliptic curve is sufficiently secure. A participant is represented by a handheld low memory device such as a smart card. A central facility is not required for key creation. The determination of whether an elliptic curve is sufficiently secure is made by counting the number of points on the curve and ensuring that this number is divisible by a prime number of at least a predetermined length.

IPC 1-7

H04L 9/30; G06F 7/72

IPC 8 full level

G09C 1/00 (2006.01); **G06F 7/72** (2006.01); **H04L 9/08** (2006.01); **H04L 9/30** (2006.01)

CPC (source: EP)

G06F 7/725 (2013.01); **H04L 9/3066** (2013.01); H04L 2209/80 (2013.01)

Citation (search report)

See references of WO 0014924A1

Designated contracting state (EPC)

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

DOCDB simple family (publication)

WO 0014924 A1 20000316; AU 6243899 A 20000327; EP 1112637 A1 20010704; JP 2002524778 A 20020806

DOCDB simple family (application)

US 9920411 W 19990907; AU 6243899 A 19990907; EP 99949599 A 19990907; JP 2000569548 A 19990907