Title (en)

MODULAR REDUCTION FOR A CRYPTOGRAPHIC PROCESS AND COPROCESSOR FOR CARRYING OUT SAID REDUCTION

Title (de)

MODULARE REDUKTION FÜR EINEN KRYPTOGRAPHISCHEN PROZESS UND COPROZESSOR ZUR AUSFÜHRUNG DER REDUKTION

Title (fr)

REDUCTION MODULAIRE POUR UN PROCEDE CRYPTOGRAPHIQUE, ET COPROCESSEUR POUR LA REALISATION D'UNE TELLE REDUCTION MODULAIRE

Publication

EP 1660989 A2 20060531 (FR)

Application

EP 04786388 A 20040823

Priority

- FR 2004050390 W 20040823
- FR 0310445 A 20030904

Abstract (en)

[origin: WO2005024627A2] The invention relates to a cryptographic method wherein, in order to carry out a fully polynomial division of type Q (x) = [U (x) / N (x)], wherein Q (x), N (x) and U(x) are polynomials, respectively a result, dividend and a divider, multiplication of the two polynomial is carried out followed by displacement of the bits of the result of the multiplication. The following operation is performed on the body of the polynomials Fp[x]: formula (I). The invention also enables more complex operations to be carried out, including modular operations. The invention is an alternative to the Montgomery method and does not need any correction. It is useful, in particular, for cryptographic methods wherein polynomial operations are carried out on the body F2[x]. The invention also relates to an appropriate coprocessor for carrying out said method. Preferred application: chip cards.

IPC 1-7

G06F 7/72

IPC 8 full level

G06F 7/72 (2006.01)

CPC (source: EP US)

G06F 7/726 (2013.01 - EP US); **H04L 9/3066** (2013.01 - EP US); **H04L 9/3093** (2013.01 - EP US); **H04L 9/3252** (2013.01 - EP US)

Citation (search report)

See references of WO 2005024627A2

Designated contracting state (EPC)

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

DOCDB simple family (publication)

FR 2859585 A1 20050311; EP 1660989 A2 20060531; US 2007162530 A1 20070712; WO 2005024627 A2 20050317; WO 2005024627 A3 20050630

DOCDB simple family (application)

FR 0310445 A 20030904; EP 04786388 A 20040823; FR 2004050390 W 20040823; US 57050704 A 20040823