



(11) **EP 1 293 891 B8**

(12) **CORRECTED EUROPEAN PATENT SPECIFICATION**

(15) Correction information:
Corrected version no 1 (W1 B1)
Corrections, see
Bibliography INID code(s) 72, 73

(51) Int Cl.:
G06F 7/72 (2006.01) **G06F 9/302 (2006.01)**

(48) Corrigendum issued on:
14.04.2010 Bulletin 2010/15

(45) Date of publication and mention
of the grant of the patent:
03.02.2010 Bulletin 2010/05

(21) Application number: **02027872.7**

(22) Date of filing: **20.04.1998**

(54) **Arithmetic processor accomodating different finite field size**

Arithmetischer Prozessor geeignet für verschiedenen endlichen Feldgrösse.

Processeur arithmétique accomodant différentes tailles de champ fini.

(84) Designated Contracting States:
CH DE FR GB LI

(30) Priority: **18.04.1997 GB 9707861**

(43) Date of publication of application:
19.03.2003 Bulletin 2003/12

(60) Divisional application:
03021261.7

(62) Document number(s) of the earlier application(s) in
accordance with Art. 76 EPC:
98920431.8 / 0 976 027

(73) Proprietor: **Certicom Corp.**
Mississauga, ON L4W 5L1 (CA)

(72) Inventors:
• **Vanstone, Scott A.**
Campbellville, ON N0P 1B0 (CA)
• **Lambert, Robert J.**
Cambridge, Ontario N3C 3N3 (CA)
• **Gallant, Robert P.**
Corner Brook, NL A2H 7J2 (CA)
• **Juriscic, Aleksandar**
100 Ljubljana (SI)
• **Vadekar, Ashok V.**
Rockwood, Ontario N0B 2K0 (CA)

(74) Representative: **Rickard, David John et al**
Ipulse
26 Mallinson Road
London
SW11 1BP (GB)

(56) References cited:
EP-A- 0 169 908 EP-A- 0 267 836
US-A- 5 268 854 US-A- 5 459 681

- **DE WINE ET AL: "A fast software implementation for arithmetic operations in GF(2)" LECTURE NOTES IN COMPUTER SCIENCE, SPRINGER VERLAG, NEW YORK, NY, US, 1996, pages 65-76, XP002081362 ISSN: 0302-9743**
- **HSU I S ET AL: "A COMPARISON OF VLSI ARCHITECTURE OF FINITE FIELD MULTIPLIERS USING DUAL, NORMAL, OR STANDARD BASES" IEEE TRANSACTIONS ON COMPUTERS, IEEE INC. NEW YORK, US, vol. 37, no. 6, 1 June 1988 (1988-06-01), pages 735-739, XP000576196 ISSN: 0018-9340**
- **FUCHS K C: "CRYPTOGRAPHIC SIGNAL PROCESSOR" MOTOROLA TECHNICAL DEVELOPMENTS, MOTOROLA INC. SCHAUMBURG, ILLINOIS, US, vol. 27, 1 May 1996 (1996-05-01), pages 81-82, XP000594566 ISSN: 0887-5286**

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

EP 1 293 891 B8