Title: EXPONENTIATOR WITH POST-PROCESSING ADDER

Abstract: A cipher processor consists of an exponentiator and a modulo processor. The modulo processor comprises an adder, operable to perform modular reduction, A mod N, or addition, A+B. The modulo processor may be used independently of the exponentiator. It may be used as a carry resolving adder for adding intermediate results in carry-save format. A mod N is calculated in an iterative way, where A is an 2n-bit operand, whereas N is a n-bit operand.

(88) Date of publication of the international search report: 24 April 2003

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:
— with international search report
INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 G06F 7/72

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
WPI Data, PAJ, EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>US 5 479 365 A (OGURA NAOYUKI) 26 December 1995 (1995-12-26) column 14, line 48 -column 21, line 17; figures 1,2,15</td>
<td>1-3,6-9, 22, 24-26, 57,58, 60,61</td>
</tr>
</tbody>
</table>

Further documents are listed in the continuation of box C.

Patent family members are listed in annex.

* Special categories of cited documents:
  *A* document defining the general state of the art which is not considered to be of particular relevance
  *E* earlier document but published on or after the international filing date
  *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another document or to involve an inventive step when the document is taken alone
  *O* other, earlier document (as specified)
  *P* document published prior to the international filing date but later than the priority date claimed

Date of the actual completion of the international search
25 September 2002

Date of mailing of the international search report
22-01-03

Name and mailing address of the ISA
European Patent Office, P.B. 5819 Patentlaan 2
NL-2280 HV Rijswijk
Tel: (+31-70) 340-2040, Tx: 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer
VERHOOF, P
<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
</table>
**INTERNATIONAL SEARCH REPORT**

**Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)**

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.: because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.: because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. ☐ Claims Nos.: because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

**Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)**

This International Searching Authority found multiple inventions in this international application, as follows:

*see additional sheet*

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☑ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

   1, 9, 17-26, 57, 58, 60, 61

**Remark on Protest**

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.
This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. Claims: 1-9, 17-26, 57, 58, 60, 61

   1.1. Claims: 1, 2, 4-9, 22, 24-26, 57, 58, 60, 61
       Exponentiator with modulo post-processor capable of carry resolving addition and modulo reduction

   1.2. Claims: 3, 17-21, 23
       Exponentiator with modulo post-processor capable of addition and iterative modulo reduction

2. Claims: 10-16, 59, 62, 63

   Modulo reduction processor capable of calculating a Montgomery constant


   Iterative modulo reduction

4. Claims: 36-56, 80, 81

   Loading of operands in a modulo reduction processor

Please note that all inventions mentioned under item 1, although not necessarily linked by a common inventive concept, could be searched without effort justifying an additional fee.
<table>
<thead>
<tr>
<th>Patent document cited in search report</th>
<th>Publication date</th>
<th>Patent family member(s)</th>
<th>Publication date</th>
</tr>
</thead>
</table>