Title: METHOD AND APPARATUS FOR CRATING A MESSAGE DIGEST USING A PARALLEL, ONE-WAY HASH ALGORITHM

Abstract: A one-way hash algorithm is implemented in hardware and/or software. The hash algorithm creates a message digest from an input message. During one 16-operation round of the hash algorithm, a front computation process (202, Figure 2) computes a portion of a first operation. Then a systolic computation process (204, Figure 2) computes the remainder of the first operation and the next fifteen operations to complete the round. The systolic computation process pre-calculates (325, Figure 3) a portion of the next round in parallel with the completion of the current round. Because the systolic computation process has a shallower logic depth, and because certain calculations are done in parallel, an approximately four times reduction in the time to compute one round algorithm is identical to a message digest computed using a conventional MD5 implementation, when given the same input message.
Published: with international search report

(88) Date of publication of the international search report:
1 April 2004

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.
A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 H04L9/32

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 H04L

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)

EPO-Internal, PAJ, IBM-TDB, INSPEC

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>
</table>

X 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 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 citation or other special reason (as specified)
  *O* document referring to an oral disclosure, use, exhibition or other means
  *P* document published prior to the International filing date but later than the priority date claimed

**I** later document published after the International filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

**X** document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

**Y** document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

**Z** document member of the same patent family

Date of the actual completion of the international search

9 December 2003

Date of mailing of the International search report

02/01/2004

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL – 2280 HV Rijswijk
Tel. (+31-70) 340-2900, Tx. 31 651 epo-nl
Fax (+31-70) 340-3016

Authorized officer

Cretaine, 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>
<tbody>
<tr>
<td>A</td>
<td>the whole document</td>
<td>2-13, 15-25, 27-32, 34-36, 38-42</td>
</tr>
</tbody>
</table>

---

<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>A</td>
<td>the whole document</td>
<td>2-13, 15-25, 27-32, 34-36, 38-42</td>
</tr>
</tbody>
</table>