METHOD FOR DEFENCE AGAINST DIFFERENTIAL POWER ANALYSIS ATTACKS

\[ J(C)(K) \xrightarrow{\times n} J(C)(K) \xleftarrow{\phi^{-1}} \]

\[ \phi \downarrow \]

\[ J(\tilde{C})(K) \xrightarrow{\times n} J(\tilde{C})(K) \]

Abstract: In order to refine a method for defence against at least one attack made by means of differential power analysis on at least one hyperelliptic cryptosystem, in particular at least one hyperelliptic public key cryptosystem, which is given by at least one hyperelliptic curve (C) of any genus (g) over a finite field (K) in a first group, where the hyperelliptic curve (C) is given by at least one co-efficient, so that an essential contribution can be made towards an efficient and secure implementation of the hyperelliptic cryptosystem, it is proposed that the hyperelliptic curve (C) and/or at least one element of the first group, in particular at least one in particular reduced divisor and/or at least one intermediate result of a scalar multiplication, is randomised.
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 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, 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. X 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 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

"T" 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
23 November 2004

Date of mailing of the international search report
21/12/2004

Name and mailing address of the ISA
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epc 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>
<tbody>
<tr>
<td>X</td>
<td>CORON J-S: &quot;RESISTANCE AGAINST DIFFERENTIAL POWER ANALYSIS FOR ELLIPTIC CURVE CRYPTOSYSTEMS&quot; CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS. INTERNATIONAL WORKSHOP, XX, XX, August 1999 (1999-08), pages 292-302, XP000952243 page 301, line 1 - line 17</td>
<td>1,2,5-10</td>
</tr>
<tr>
<td>A</td>
<td>DE 100 57 203 C (CV CRYPTOVISION GMBH) 6 June 2002 (2002-06-06) paragraph '0023!</td>
<td>1-10</td>
</tr>
<tr>
<td>T</td>
<td>MENEZES A J ET AL: &quot;APPENDIX AN ELEMENTARY INTRODUCTION TO HYPERELLIPTIC CURVES&quot; ALGEBRAIC ASPECTS OF CRYPTOGRAPHY, XX, XX, 1998, pages 155-178, XP000987354</td>
<td>1-10</td>
</tr>
<tr>
<td>Patent document cited in search report</td>
<td>Publication date</td>
<td>Patent family member(s)</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-----------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>DE 10057203 C</td>
<td>06-06-2002</td>
<td>DE 10057203 C1</td>
</tr>
</tbody>
</table>