Title: HYBRID CRYPTOGRAPHIC ACCELERATOR AND METHOD OF OPERATION THEREOF

Abstract: The invention is directed toward a system-on-a-chip (SOC) having a secure execution environment (SEE) containing secure memory (120) and a cryptographic accelerator (140) which performs cryptographic functions. In one embodiment, the cryptographic accelerator includes a key register (142) located within the SEE and coupled to the secure memory (120) to receive a cryptographic key therefrom, and data input and output registers (144, 146) located outside of the SEE and coupled to the key register to allow the cryptographic key to be applied to input data arriving via the data input register to yield output data via the data output register.
Published:
— with international search report
— before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

(88) Date of publication of the international search report:
8 November 2007

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.
INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER
IPC: H04L 9/00 (2006.01)

USPC: 380/277
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)
U.S.: 380/277; 713/189

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EAST - USPG_PUB; USPAT; EPO; IPO; DERWENT; IBM_TDB

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>Y</td>
<td>2003/0185391 A1 (QI et al.) 2 October 2003 (02.10.2003), Figure 1, paragraphs 31, 34, 40-45.</td>
<td>1-20</td>
</tr>
<tr>
<td>Y</td>
<td>US 2002/0062444 (LAW et al) 23, May 2002 (23.05.2002), paragraph 37</td>
<td>3, 10, 17</td>
</tr>
<tr>
<td>Y</td>
<td>US 5,631,960 (LIKENS et al.) 20 May 1997 (20.05.1997), col. 7 lines 1-10.</td>
<td>4, 11, 18</td>
</tr>
</tbody>
</table>

Further documents are listed in the continuation of Box C. See patent family annex.

Date of the actual completion of the international search
26 July 2007 (26.07.2007)

Authorized officer
Kambiz Zand
Telephone No. (571) 272-3811

DEBORAH A. THOMAS
PARALEGAL SPECIALIST