Title: IMPROVED CFM MODE SYSTEM

Abstract: A method for producing at least one ciphertext block from at least one plaintext block using a block cipher $E$ and a key $K$, the method including receiving $n$ plaintext blocks, wherein $n$ is an integer greater than 0, setting $Q_0$ equal to an initial value, and for each plaintext block of the $n$ plaintext blocks: computing $Q_i = E(K, Q_{i-1}) \ XOR \ P_i$; and computing $C_i = M(P_i, Q_i)$, thereby producing $n$ ciphertext blocks, wherein $0 < i \leq n$, and $P_i$ denotes an $i$-th plaintext block of the $n$ plaintext blocks, and $C_i$ denotes an $i$-th ciphertext block of the $n$ ciphertext blocks, and $M$ is a selector function which, for each bit $C_{i0}$ of block $C_i$, selects a first argument of $M$ if bit $P_{i0}$ is not to be encrypted, and selects a second argument of $M$ if bit $P_{i0}$ is to be encrypted. Related apparatus and methods are also provided.
INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL04/00144

A. CLASSIFICATION OF SUBJECT MATTER
IPCl(T) : H04L 1/100, 9/100; G06F 11/30
US CL : 380/28,29,37,265; 713/200
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. : 380/28,29,37,265; 713/200

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

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>A</td>
<td>US 6,578,150 B2 (LUYSTER) 10 June 2003 (10.06.2003)</td>
<td>1-30</td>
</tr>
<tr>
<td>A</td>
<td>US 6,249,582 B1 (GILLEY) 19 June 2001 (19.06.2001)</td>
<td>1-30</td>
</tr>
<tr>
<td>A</td>
<td>US 4,731,843 A (HOLMQUIST) 15 March 1988 (15.03.1988)</td>
<td>1-30</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

Name and mailing address of the ISA/US
Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
Facsimile No. (703) 305-3230

Date of mailing of the international search report
08 NOV 2004

Authorized officer
Ayaz Sheikh
Telephone No. 703-305-9648

Form PCT/ISA/210 (second sheet) (January 2004)