(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 March 2006 (16.03.2006)

PCT

(10) International Publication Number
WO 2006/027308 A3

(51) International Patent Classification:
G06F 1/00 (2006.01)

(21) International Application Number:
PCT/EP2005/053996

(22) International Filing Date: 15 August 2005 (15.08.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/938,773 10 September 2004 (10.09.2004) US

(71) Applicant *(for all designated States except US)*: **INTERNATIONAL BUSINESS MACHINES CORPORATION** [US/US]; New Orchard Road, Armonk, New York 10504 (US).

(71) Applicant *(for MG only)*: **IBM UNITED KINGDOM LIMITED** [GB/GB]; P.O. Box 41, North Harbour, Portsmouth, Hampshire PO6 3AU (GB).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **FAYAD, Camil** [US/US]; 106 Van Wagner Road, Apt # 2B, Poughkeepsie, New York 12603 (US). **LI, John** [US/US]; 26 Oriole Drive, Woodstock, New York 12498 (US). **SUTTER, Siegfried** [DE/DE]; Triberger Strasse 12, 71034 Boeblingen (DE).

(74) Agent: **WILLIAMS, Julian, David**; IBM United Kingdom Limited, Intellectual Property Law, Hursley Park, Winchester, Hampshire SO21 2JN (GB).

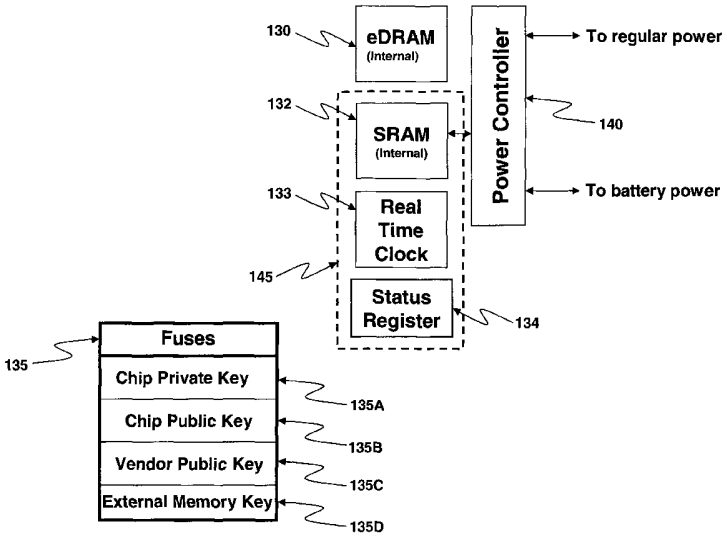
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) **Title:** AN INTEGRATED CIRCUIT CHIP FOR ENCRYPTION AND DECRYPTION HAVING A SECURE MECHANISM FOR PROGRAMMING ON-CHIP HARDWARE



(57) **Abstract:** An integrated circuit chip is provided which contains one or more processors and one or more cryptographic engines. A flow control circuit having a command processor accepts requests and data via a secure external interface through which only encrypted information is passed. The flow control circuit mediates decryption of this information using cryptographic keys that are present in hard coded form on the chip. In particular the flow control circuit includes a programmable hardware portion which is configurable in a secure manner to create a flexible internal chip architecture. The chip also includes a volatile memory disposed on a voltage island on which is maintained either through a battery backup or from a fixed power source (mains). The chip is thus enabled to securely perform cryptographic operations with the processors controlling the cryptographic engines through the flow control circuit.

WO 2006/027308 A3

(88) Date of publication of the international search report:
11 May 2006

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

International application No
PCT/EP2005/053996

A. CLASSIFICATION OF SUBJECT MATTER
G06F1/00

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)
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)

EPO-Internal, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 666 411 A (MCCARTY ET AL) 9 September 1997 (1997-09-09) column 4, line 53 - line 61 column 7, line 30 - line 37 column 11, line 5 - line 25 column 19 - column 20; figure 7	1-17
X	WO 01/45318 A (NOKIA NETWORKS OY; KIVIMAEKI, TOMMI) 21 June 2001 (2001-06-21) page 3, line 30 - line 32 page 4, line 20 - page 5, line 2 page 8, line 34 - page 9, line 9 page 13, line 18 - line 30 page 15, line 32 - page 16, line 10	1-17

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family 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.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
2 November 2005	24 02 2006

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Alecu, M

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2005/053996

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2003/163431 A1 (GINTER KARL L ET AL) 28 August 2003 (2003-08-28) paragraph [0005] paragraph [0073] paragraph [0167] - paragraph [0169] paragraph [0286] - paragraph [0615] paragraph [0994] paragraph [1064] - paragraph [1098] paragraph [1633] - paragraph [1708] figures 6-10,13,64,68,71	1-17
X	US 6 378 072 B1 (COLLINS THOMAS ET AL) 23 April 2002 (2002-04-23) column 4, line 8 - column 8, line 12	1-17
A	US 2002/166062 A1 (HELBIG WALTER A ET AL) 7 November 2002 (2002-11-07) the whole document	1-17
X	US 2002/199110 A1 (KEAN THOMAS A) 26 December 2002 (2002-12-26) paragraph [0008] paragraph [0012] paragraph [0014] paragraph [0133] - paragraph [0137] paragraph [0188]	1-17
A	SMITH S W ET AL: "Building a high-performance, programmable secure coprocessor" 23 April 1999 (1999-04-23), COMPUTER NETWORKS, ELSEVIER SCIENCE PUBLISHERS B.V., AMSTERDAM, NL, PAGE(S) 831-860 , XP004304521 ISSN: 1389-1286 the whole document	

INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP2005/053996

Box II Observations where certain claims were found unsearchable (Continuation of item 2 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 III Observations where unity of invention is lacking (Continuation of item 3 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.:

1-17

Remark on Protest

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

☐ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-17

Versatile flow control circuit

---

2. claims: 18-26

Method to improve encryption

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2005/053996

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5666411 A	09-09-1997	NONE	
WO 0145318 A	21-06-2001	AU 1981400 A	25-06-2001
		EP 1240743 A1	18-09-2002
US 2003163431 A1	28-08-2003	NONE	
US 6378072 B1	23-04-2002	TW 413988 B	01-12-2000
		WO 9939475 A1	05-08-1999
		US 2002073316 A1	13-06-2002
US 2002166062 A1	07-11-2002	NONE	
US 2002199110 A1	26-12-2002	NONE	