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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 June 2007 (14.06.2007)

PCT

(10) International Publication Number
WO 2007/067221 A3

(51) International Patent Classification:
H04L 9/00 (2006.01)

(21) International Application Number:
PCT/US2006/028746

(22) International Filing Date: 25 July 2006 (25.07.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/297,484 8 December 2005 (08.12.2005) US

(71) Applicant *(for all designated States except US)*: **AGERE SYSTEMS INC.** [US/US]; 1110 American Parkway NE, Allentown, PA 18109 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **CHAMBERS, Michael, Joseph** [GB/DE]; Am Europakanal 40, 91056 Erlangen (DE). **KIESSLING, Michael** [DE/DE]; Gartenstrasse 25, 85354 Freising (DE). **TUCHMAN, Kenneth, A.** [US/DE]; Kiesslingerstrasse 28a, 81829 Munich (DE). **WANG, Hai** [DE/DE]; Boehmerwaldstrasse 10, 85586 Poing (DE).

(74) Agent: **RYAN, Joseph, B.**; Ryan, Mason & Lewis, LLP, 90 Forest Avenue, Locust Valley, NY 11560 (US).

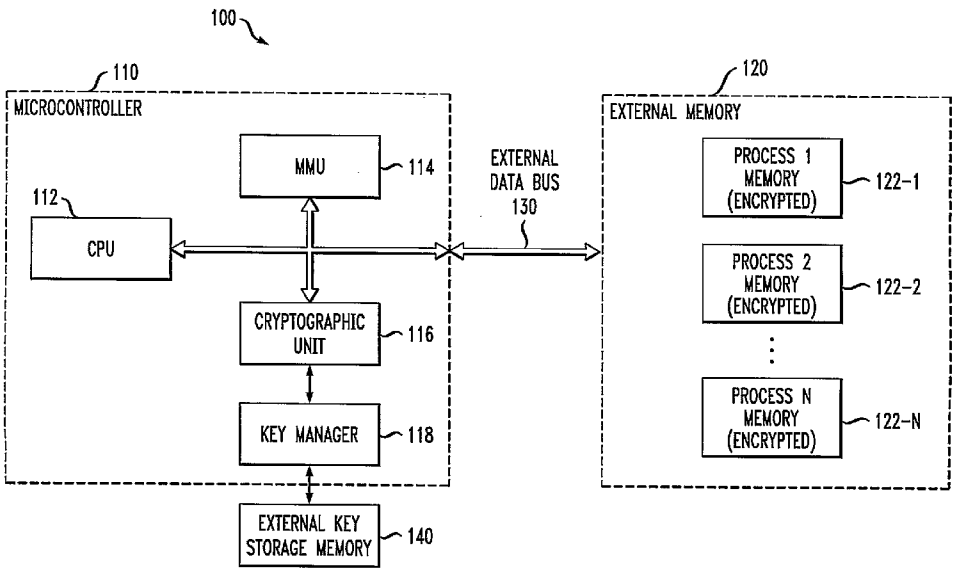
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ,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

(88) Date of publication of the international search report:
17 April 2008

(54) Title: METHODS AND APPARATUS FOR THE SECURE HANDLING OF DATA IN A MICROCONTROLLER



(57) Abstract: Apparatus and methods are presented for protecting data in microcontrollers from both malicious software processes running inside the device as well as from unauthorized attempts to read the data from an external data bus and/or external memory. An illustrative embodiment of the invention accomplishes these security improvements, in part, by utilizing an enhanced memory management unit (MMU). The enhanced MMU is configured to prevent one software process running on the microcontroller from accessing data associated with a different software process running on the same microcontroller. Moreover, data transmitted over an external data bus or stored in an external memory is encrypted, thereby reducing the chances that unauthorized users will gain exploitable information from this data.

WO 2007/067221 A3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 06/28746

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - H04L 9/00 (2007.01)
USPC - 713/171
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)
713/171

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC: 713/164; 380/181, 264, 277, 284

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

PubWEST - terms: central processing unit, CPU, memory unit, encrypted data, encryption data, data bus, random access memory, RAM, mobile device, flash memory, integrated circuit, microcontroller, electronic mail, email, cryptographic unit, encryption key, personal digital assistant, PDA, cellular phone, memory key storage ...

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 2003/0229789 A1 (MORAIS, et al.) 11 December 2003 (11.12.2003), abstract and para [0021]-[0104], [0113], [0115]-[0122], [0126], [0128]-[0130], [0134], [0141].	1-8, 10 and 18-19 --- 9, 11-17 and 20
Y	US 2002/0048369 A1 (GINTER, et al.) 25 April 2002 (25.04.2002), abstract and para [0466]-[0470], [0495], [0508]-[0509], [0525]-[0526], [0549]-[0562].	9, 11-13 and 20
Y	US 2003/0140245 A1 (DAHAN, et al.) 24 July 2003 (24.07.2003), abstract and para [0029], [0164]-[0173].	14-17
A	US 2005/0172121 A1 (RISAN, et al.) 4 August 2005 (04.08.2005), entire document, especially abstract and para [0043]-[0045], [0059]-[0069], [0098]-[0104], [0220], [0269]-[0271].	1-20

☐ Further documents are listed in the continuation of Box C. ☐

* 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 application or patent 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
30 July 2007 (30.07.2007)	01 FEB 2008
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. 571-273-3201	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774