

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
6 December 2001 (06.12.2001)

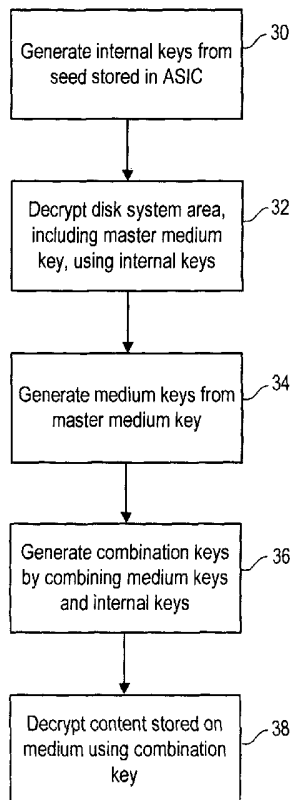
PCT

(10) International Publication Number  
WO 01/093002 A3

- (51) International Patent Classification<sup>7</sup>: G11B 20/00, (74) Agents: STEUBER, David, E. et al.; Skjerven Morrill G06F 12/14, H04L 9/06 LLP, 25 Metro Drive, Suite 700, San Jose, CA 95110 (US).
- (21) International Application Number: PCT/US01/17245 (81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.
- (22) International Filing Date: 25 May 2001 (25.05.2001)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data: 09/583,452 30 May 2000 (30.05.2000) US (84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).
- (71) Applicant: DATAPLAY, INCORPORATED [US/US]; 2560 55th Street, Boulder, CO 80301-5706 (US). Published: — with international search report
- (72) Inventors: ZAHARRIS, Daniel, R.; 7329 Mt. Meeker Road, Longmont, CO 80503 (US). LEE, Lane, W.; 894 Bermont Drive, Lafayette, CO 80026 (US).

[Continued on next page]

(54) Title: METHOD OF DECRYPTING DATA STORED ON A STORAGE DEVICE USING AN EMBEDDED ENCRYPTION/DECRYPTION MEANS



(57) Abstract: A method of decrypting data is provided for decrypting data stored on a storage medium using an encryption/decryption means embedded on data storage engine for reading the data from the medium. The data storage engine generates at least a set of internal keys. The internal keys (30) are used to decrypt a master media key stored on the storage medium (32). The master media key generates a set of medium keys. The medium keys are combined with the internal keys to generate a set of combined keys (36). The combined keys are used to decrypt portions of the data stored on the storage medium (38).



WO 01/093002 A3



---

**(88) Date of publication of the international search report:**  
7 August 2003

*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/US 01/17245

A. CLASSIFICATION OF SUBJECT MATTER  
IPC 7 G11B20/00 G06F12/14 H04L9/06

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 G11B 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, WPI Data, PAJ, INSPEC, COMPENDEX, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ° | Citation of document, with indication, where appropriate, of the relevant passages  | Relevant to claim No.            |
|------------|---|----------------------------------|
| X          | US 5 923 754 A (DRISCOLL DANIEL J ET AL)<br>13 July 1999 (1999-07-13)<br>abstract; figure 3<br>column 1, line 58 -column 2, line 14<br>column 3, line 13 - line 22<br>column 3, line 51 -column 5, line 3<br>---                          | 1-3,20                           |
| X          | EP 0 561 685 A (FUJITSU LTD)<br>22 September 1993 (1993-09-22)<br>abstract<br><br>column 1, line 39 -column 2, line 20<br>column 4, line 30 -column 5, line 40<br>column 6, line 13 -column 7, line 6<br>figures 1-3<br><br>-----<br>-/-- | 1,2,20,<br>21<br>3-5,7,<br>14,15 |

Further documents are listed in the continuation of box C.

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.

"&" document member of the same patent family

Date of the actual completion of the international search

25 November 2002

Date of mailing of the international search report

06.12.2002

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 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer

Schiwy-Rausch, G

## INTERNATIONAL SEARCH REPORT

 International Application No  
 PCT/US 01/17245

| C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT |  |                       |
|--|--|-----------------------|
| Category °   | Citation of document, with indication, where appropriate, of the relevant passages   | Relevant to claim No. |
| A  | MARIE: "ADSP-2141L Data Sheet"<br>INTERNET ARTICLE, 'Online!<br>20 January 2000 (2000-01-20), pages 1-39,<br>XP002174850<br>Retrieved from the Internet:<br><URL:http://www.analog.com/pdf/ADSP-2141L_0.pdf> 'retrieved on 2001-08-14!   | 1,20,21               |
| Y  | the whole document   | 3-5,7,<br>14,15       |
| X  | EP 0 679 977 A (IBM)<br>2 November 1995 (1995-11-02)<br>abstract<br>column 3, line 46 -column 4, line 32<br>column 11, line 32 - line 43<br>column 14, line 27 - line 49<br>column 18, line 47 -column 20, line 49<br>figure 20  | 1,20,21               |
| E  | WO 01 75562 A (DATAPLAY INC)<br>11 October 2001 (2001-10-11)<br>cited in the application<br>page 4, line 6 - line 18<br>page 6, line 14 -page 7, line 3<br>page 9, line 5 -page 11, line 26<br>page 18, line 24 -page 21, line 24  | 1-4,7,<br>20,21       |
| A  | EP 0 978 839 A (HEWLETT PACKARD CO)<br>9 February 2000 (2000-02-09)<br>abstract<br>page 2, line 28 - line 45<br>page 6, line 52 -page 7, line 6<br>page 13, line 25 - line 48<br>figures 2-4   | 1-3,6,20              |
| A  | ANONYMOUS: "ANALOG DEVICES AND IRE<br>ANNOUNCE FIRST DSP-BASED INTERNET SECURITY<br>SYSTEM-ON-A-CHIP"<br>INTERNET ARTICLE, 'Online!<br>19 January 1999 (1999-01-19), pages 1-3,<br>XP002184356<br>Norwood, MA, USA<br>Retrieved from the Internet:<br><URL:http://content.analog.com/pressreleas<br>e/prprintdisplay/0,1628,16,00.html><br>'retrieved on 2001-10-10!<br>the whole document | 1,7,14,<br>20-25      |
|  | -/--   |                       |

# INTERNATIONAL SEARCH REPORT

International application No.  
PCT/US 01/17245

## Box I Observations where certain claims were found unsearchable (Continuation of item 1 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 II Observations where unity of invention is lacking (Continuation of item 2 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.:

### 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: 1-21

Method of decrypting/encrypting data using different encryption/decryption keys from storage engine and storage medium in interaction.

2. Claims: 22-25

Method of decrypting data stored on a storage medium by a file system structure and a file pointer.