

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
19 February 2004 (19.02.2004)

PCT

(10) International Publication Number  
WO 2004/015740 A3

(51) International Patent Classification<sup>7</sup>: H04L 9/32

CZ, DE, DK, DM, DZ, EC, 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, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(21) International Application Number:  
PCT/IL2003/000637

(22) International Filing Date: 4 August 2003 (04.08.2003)

(25) Filing Language: English

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

(26) Publication Language: English

(30) Priority Data:  
60/401,753 8 August 2002 (08.08.2002) US

(71) Applicant (for all designated States except US): M-SYSTEMS FLASH DISK PIONEERS LTD. [IL/IL]; Central Park 2000, 7 Atir Yeda St., 44425 Kfar Saba (IL).

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

(71) Applicant and  
(72) Inventor: DARIEL, Dani [IL/IL]; Mayshar 46, 76850 Ishuvey Gderot (IL).

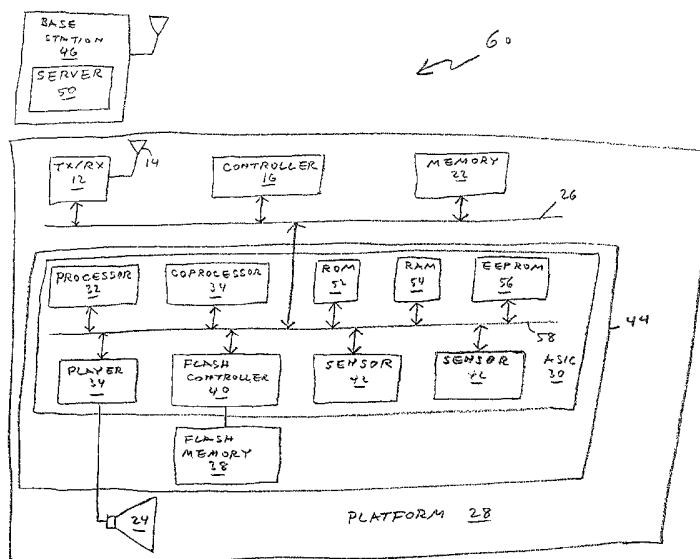
(88) Date of publication of the international search report:  
10 February 2005

(74) Agent: FRIEDMAN, Mark, M.; DR. MARK FRIEDMAN LTD., 7 Haomanim Street, 67897 Tel Aviv (IL).

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.

(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU,

(54) Title: INTEGRATED CIRCUIT FOR DIGITAL RIGHTS MANAGEMENT



(57) Abstract: An ASIC (30) for implementing digital rights management includes a processor for requesting encrypted digital data from a server (50) and decrypting the data, and a player (34) for transforming the decrypted data to analog signals. Preferably, the ASIC is tamper-resistant. Preferably, all the management code of the ASIC is stored on a ROM (36) in the ASIC. A device for receiving, decrypting and displaying encrypted digital data includes the ASIC, and also a transceiver for communicating with the server, a display mechanism for displaying the analog signals, and a nonvolatile memory for storing the encrypted data. A system for storing and displaying digital data includes both the server and the device. Preferably, the server is configured to send to the device only the encrypted digital data and associated decryption keys.

WO 2004/015740 A3

**INTERNATIONAL SEARCH REPORT**

International application No.

PCT/IL03/00637

<b>A. CLASSIFICATION OF SUBJECT MATTER</b>		
IPC(7) : H04L 9/32		
US CL : 713/189,193,194		
According to International Patent Classification (IPC) or to both national classification and IPC		
<b>B. FIELDS SEARCHED</b>		
Minimum documentation searched (classification system followed by classification symbols) U.S. : 713/189,193,194		
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 practicable, search terms used) <i>Please See Continuation Sheet</i>		
<b>C. DOCUMENTS CONSIDERED TO BE RELEVANT</b>		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,825,879 A(DAVIS) 20 October 1998 (20.10.1998), column 4, lines 325, li-67; column 5, lines 1-30.	1-42
X	US 4,914,697 A(DABBISH et al) 03 April 1990 (03.04.1990), column 3, lines 58-67; column 4, lines 3-18.	1,4,6,17,28,
A	US 5,267,312 A(THOMPSON et al) 30 November 1993 (30.11.1993), column 7, lines 1-44; column 18, lines 1-38.	1-42
A	US 6,185,737 B(NORTHCUTT et al) 06 February 2001(06.02.2001), column 3, lines 29-50; column 7, lines 45-67.	1-42
<input type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> 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	"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
"E"	earlier application or patent published on or after the international filing date	"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
"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)	"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
"O"	document referring to an oral disclosure, use, exhibition or other means	"&" document member of the same patent family
"P"	document published prior to the international filing date but later than the priority date claimed	
Date of the actual completion of the international search	Date of mailing of the international search report	
14 December 2004 (14.12.2004)	03 JAN 2005	
Name and mailing address of the ISA/US	Authorized officer	
Mail Stop PCT, Attn: ISA/US	Hosuk Song <i>Peggy Han</i>	
Commissioner for Patents	Telephone No. 703-305-3900	
P.O. Box 1450		
Alexandria, Virginia 22313-1450		
Facsimile No. (703) 305-3230		

**Continuation of B. FIELDS SEARCHED Item 3:**

EAST

search terms: IC, tamper-resistant, encrypt, decrypt, encipher, decipher, cipher, ROM, convert, transform, analog, audio, video, multimedia, digital, authenticate, validate, verify, non-volatile