(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 724 962 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
29.11.2006 Bulletin 2006/48

(43) Date of publication A2:
22.11.2006 Bulletin 2006/47

(21) Application number: **05023142.2**

(22) Date of filing: **24.10.2005**

(51) Int Cl.:
H04L 9/08 *(2006.01)*

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI SK TR
Designated Extension States:
AL BA HR MK YU

(30) Priority: **08.02.2005 JP 2005031914**

(71) Applicant: **KABUSHIKI KAISHA TOSHIBA**
Tokyo 105-8001 (JP)

(72) Inventor: **Ohno, Katsuya**
Minato-ku
Tokyo 105-8001 (JP)

(74) Representative: **HOFFMANN EITLE**
Patent- und Rechtsanwälte
Arabellastrasse 4
81925 München (DE)

(54) Data processing apparatus

(57) Upon encrypting and storing data C on a recording medium, data B corresponding to data C is embedded in a padding area together with parity data for data B and C as padding data, and data B and parity data are encrypted in correspondence with data C.

Encryption algorithm block length X n

B0	C0	parity 0	padding 0
B1	C1	parity 1	padding 1
B2	C2	parity 2	padding 2
B3	C3	parity 3	padding 3
...	...	...	...
Bn	Cn	parity n	padding n

FIG. 3

EP 1 724 962 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 05 02 3142

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
Y	PATENT ABSTRACTS OF JAPAN vol. 2002, no. 03, 3 April 2002 (2002-04-03) & JP 2001 318600 A (MITSUBISHI HEAVY IND LTD), 16 November 2001 (2001-11-16) * abstract * -----	1-7	INV. H04L9/08
Y	MENEZES, OORSCHOT, VANSTONE: "Handbook of Applied Cryptography, PASSAGE" CRC PRESS SERIES ON DISCRETE MATHEMATICS AND ITS APPLICATIONS, 1997, pages 362, 363, 551-553, XP002402027 , BOCA RATON, FL, US ISBN: 0-8493-8523-7 * page 362, paragraph 9.6.2 - page 363, line 11 * * page 551, paragraph 13.3.1 - page 552, line 16 * * page 553, line 11 - line 23 * -----	1-7	
A	SCHNEIER B: "Applied Cryptography, PASSAGE" APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS AND SOURCE CODE IN C, WILEY, NEW YORK, NY, US, January 1994 (1994-01), pages 190-191, XP002402028 * page 190, line 37 - page 191, line 12 * -----	1-7	TECHNICAL FIELDS SEARCHED (IPC) H04L G11B G06F

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Berlin	6 October 2006	CARNERERO ALVARO, F

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 05 02 3142

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

06-10-2006

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
JP 2001318600 A	16-11-2001	NONE	

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82