



(11) **EP 1 193 665 B8**

(12) **CORRECTED EUROPEAN PATENT SPECIFICATION**

(15) Correction information:
Corrected version no 1 (W1 B1)
Corrections, see
Bibliography INID code(s) 72, 73

(51) Int Cl.:
H04L 9/06 (2006.01)

(86) International application number:
PCT/JP2001/001796

(48) Corrigendum issued on:
11.07.2012 Bulletin 2012/28

(87) International publication number:
WO 2001/067425 (13.09.2001 Gazette 2001/37)

(45) Date of publication and mention
of the grant of the patent:
15.02.2012 Bulletin 2012/07

(21) Application number: **01912172.2**

(22) Date of filing: **08.03.2001**

(54) **BLOCK ENCRYPTION DEVICE USING AUXILIARY CONVERSION**

BLOCKVERSCHLÜSSELUNGSEINRICHTUNG UNTER VERWENDUNG VON
HILFSUMWANDLUNGEN

SYSTEME DE CHIFFRAGE DE BLOCS UTILISANT LA CONVERSION AUXILIAIRE

(84) Designated Contracting States:
**AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE TR**

(30) Priority: **09.03.2000 JP 2000064614**

(43) Date of publication of application:
03.04.2002 Bulletin 2002/14

(60) Divisional application:
06010073.2 / 1 686 719
06010074.0 / 1 686 720
06010075.7 / 1 686 721
06010076.5 / 1 689 113
06010077.3 / 1 689 114
06010078.1 / 1 686 722

(73) Proprietors:
• **MITSUBISHI DENKI KABUSHIKI KAISHA**
Chiyoda-ku
Tokyo 100-8310 (JP)
• **Nippon Telegraph and Telephone Corporation**
Chiyoda-ku
Tokyo 100-0004 (JP)

(72) Inventors:
• **MATSUI, Mitsuru,**
c/o Mitsubishi Denki K.K.
Tokyo 100-8310 (JP)
• **TOKITA, Toshio,**
c/o Mitsubishi Denki K.K.
Tokyo 100-8310 (JP)
• **NAKAJIMA, Junko,**
c/o Mitsubishi Denki K.K.
Tokyo 100-8310 (JP)
• **KANDA, Masayuki,**
c/o Nippon Telegraph and Telephone Corporation
Tokyo 100-0004 (JP)
• **MORIAI, Shiho,**
c/o Nippon Telegraph and Telephone Corporation
Tokyo 100-0004 (JP)
• **AOKI, Kazumaro,**
c/o Nippon Telegraph and Telephone Corporation
Tokyo 100-0004 (JP)

(74) Representative: **Pfenning, Meinig & Partner GbR**
Patent- und Rechtsanwälte
Theresienhöhe 13
80339 München (DE)

(56) References cited:
WO-A1-97/09705 JP-A- 9 269 727
JP-A- 11 052 849

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

EP 1 193 665 B8

- | | |
|--|--|
| <ul style="list-style-type: none"> • MATSUI M: "New block encryption algorithm MISTY" FAST SOFTWARE ENCRYPTION. 4TH INTERNATIONAL WORKSHOP, FSE '97 PROCEEDINGS SPRINGER-VERLAG BERLIN, GERMANY, 1997, pages 54-68, XP002367857 ISBN: 3-540-63247-6 • KANDA M ET AL: "E2-a new 128-bit block cipher" IEICE TRANSACTIONS ON FUNDAMENTALS OF ELECTRONICS, COMMUNICATIONS AND COMPUTER SCIENCES INST. ELECTRON. INF. & COMMUN. ENG JAPAN, vol. E83-A, no. 1, January 2000 (2000-01), pages 48-59, XP002367858 ISSN: 0916-8508 • FUMIHIKO SANO ET AL.: 'Kakucho feistel gata angou kei ni okeru random kansuu ichi to shoumei kanou anzensei no kankei ni tsuite' 1997 NEN, ANGOU TO JOHO SECURITY SYMPOSIUM, SCIS97-24C 31 January 1997, pages 1 - 15, XP002942208 | <ul style="list-style-type: none"> • 'Applied cryptography', 1995, JOHN WILEY & SONS, INC. XP002942209 * page 336 - page 339 * • KAZUMARO AOKI ET AL.: '128 Bit block angou camellia' DENSHI JOHO TSUUSHIN GAKKAI GIJUTSU KENKYU HOKOKU (ISEC2000-73 vol. 100, no. 76, 18 May 2000, pages 47 - 75, XP002942210 • KAZUMARO AOKI ET AL.: '128 Bit block angou camellia no jissou hyouka' DENSHI JOHO TSUSSHIN GAKKAI GIJUTSU KENKYU HOKOKU (ISEC2000-73) vol. 100, no. 324, 22 September 2000, pages 131 - 138, XP002942211 |
|--|--|