



(11) **EP 1 441 465 B8**

(12) **CORRECTED EUROPEAN PATENT SPECIFICATION**

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

(51) Int Cl.:
H04L 9/14 (2006.01) H04L 9/10 (2006.01)

(86) International application number:
PCT/JP2002/011050

(48) Corrigendum issued on:
13.04.2011 Bulletin 2011/15

(87) International publication number:
WO 2003/039066 (08.05.2003 Gazette 2003/19)

(45) Date of publication and mention
of the grant of the patent:
26.01.2011 Bulletin 2011/04

(21) Application number: **02770255.4**

(22) Date of filing: **24.10.2002**

(54) **ENCRYPTED COMMUNICATION APPARATUS**

VORRICHTUNG ZUR VERSCHLÜSSELTEN KOMMUNIKATION

APPAREIL DE COMMUNICATION CHIFFREE

(84) Designated Contracting States:
DE FR GB

(56) References cited:
JP-A- 3 139 717 JP-A- 10 154 976
JP-A- 11 145 950 JP-A- 61 017 175
US-A- 5 524 116 US-A- 6 118 873

(30) Priority: **29.10.2001 JP 2001330190**

(43) Date of publication of application:
28.07.2004 Bulletin 2004/31

(73) Proprietor: **Mitsubishi Electric Corporation**
Tokyo 100-8310 (JP)

(72) Inventors:
• **YAMADA, Keiki**
Tokyo 100-8310 (JP)
• **SATO, Tsuneo**
Tokyo 100-8310 (JP)

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

- **LIH-YANG WANG ET AL: "On the hardware design for DES cipher in tamper resistant devices against differential fault analysis" ISCAS 2000. PROCEEDINGS OF THE 2000 IEEE INTERNATIONAL SYMPOSIUM ON CIRCUITS AND SYSTEMS. GENEVA, SWITZERLAND, MAY 28-31, 2000, IEEE INTERNATIONAL SYMPOSIUM ON CIRCUITS AND SYSTEMS, NEW YORK, NY, US, vol. 1 of 5, 28 May 2000 (2000-05-28), pages 697-700, XP002202154 ISBN: 0-7803-5483-4**
- **KARRI R ET AL: "Concurrent error detection of fault-based side-channel cryptanalysis of 128-bit symmetric block ciphers" PROCEEDINGS OF THE 38TH. ANNUAL DESIGN AUTOMATION CONFERENCE. (DAC). LAS VEGAS, NV, JUNE 18 - 22, 2001, PROCEEDINGS OF THE DESIGN AUTOMATION CONFERENCE, NEW YORK, NY : ACM, US, vol. CONF. 38, 18 June 2001 (2001-06-18), pages 579-584, XP010552454 ISBN: 1-58113-297-2**

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 1 441 465 B8