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

(11) **EP 2 190 143 A8**

(12) **CORRECTED EUROPEAN PATENT APPLICATION**

(15) Correction information:
Corrected version no 1 (W1 A1)
Corrections, see
Bibliography INID code(s) 71

(48) Corrigendum issued on:
06.10.2010 Bulletin 2010/40

(43) Date of publication:
26.05.2010 Bulletin 2010/21

(21) Application number: **09252412.3**

(22) Date of filing: **14.10.2009**

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

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO SE SI SK SM TR
Designated Extension States:
AL BA RS

(30) Priority: **20.11.2008 JP 2008296411**

(71) Applicant: **Sony Corporation**
Tokyo 108-0075 (JP)

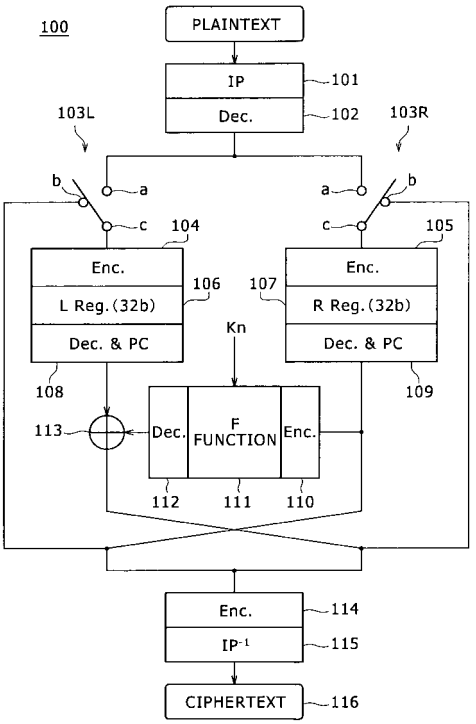
(72) Inventor: **Nobukata, Hiromi**
Tokyo 108-0075 (JP)

(74) Representative: **Turner, James Arthur et al**
D Young & Co LLP
120 Holborn
London EC1N 2DY (GB)

(54) **Cryptographic processing apparatus with improved resistance to power analysis**

(57) A cryptographic processing apparatus includes: at least one register configured to store data for operation; a first operation block configured to execute an operation in accordance with data stored in the register; a second operation block configured to execute a logic operation between one of a register-stored value and a key and an operation result of the first operation block; and a decode block configured to decode binary data in units of the predetermined number of bits to convert the binary data into decode data having the number of bits higher than the number of bits of the binary data.

FIG. 1



EP 2 190 143 A8