(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 May 1998 (28.05.1998)

PCT

(10) International Publication Number
WO 98/022878 A3

(51) International Patent Classification[6]: G06F 12/14

(21) International Application Number: PCT/EP97/05916

(22) International Filing Date: 20 October 1997 (20.10.1997)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
9624187.2 21 November 1996 (21.11.1996) GB

(71) Applicant *(for all designated States except US)*: **MOTOROLA LIMITED** [GB/GB]; Jays Close, Viables Industrial Estate, Basingstoke, Hampshire RG22 4PD (GB).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **STOUT, Graham, Henry** [GB/GB]; 42 Carrick Crescent, Giffnock, Glasgow G46 6PP (GB).

(74) Agents: **IBBOTSON, Harry** et al.; Motorola, European Intellectual Property Operations, Midpoint, Alencon Link, Basingstoke, Hampshire RG21 7PL (GB).

(81) Designated States *(national)*: CN, JP, US.

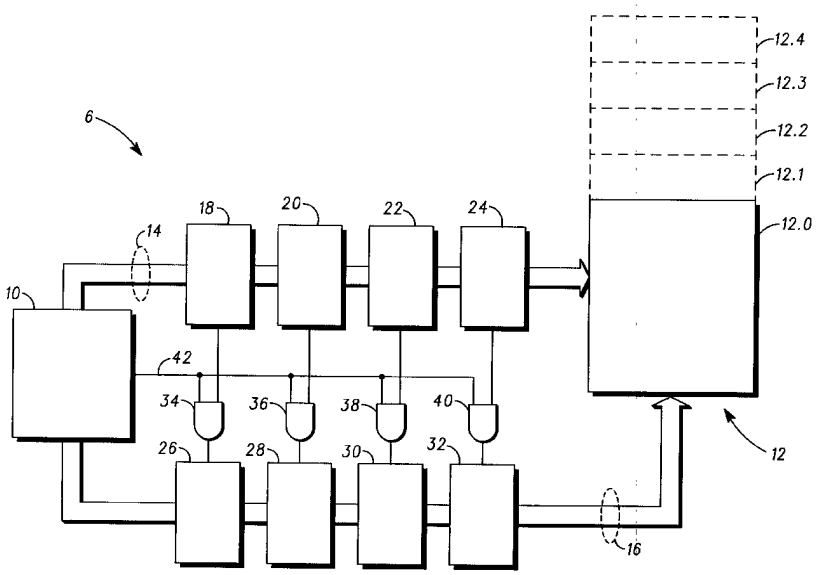
(84) Designated States *(regional)*: European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published:
— *with international search report*

(88) Date of publication of the international search report:
3 October 2002

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.

(54) Title: ARRANGEMENT FOR ENCRYPTION/DECRYPTION OF DATA AND DATA CARRIER INCORPORATING SAME



(57) Abstract: An arrangement (6) for encrypting/decrypting data comprising: random access memory (12) for holding the data; a processor (10) for processing the data, the processor having a memory map including a first portion (12.0) mapped onto the random access memory and a second portion (12.1); and control means (18, 34, 26) coupled to receive an instruction to write data to an address in the second portion of the memory map and in response thereto to write the data in a perdetermined permuted form to an associated address in the random access memory, whereby data read from said associated address in the random access memory is an encrypted/decrypted version of the data written to said address in the second portion of the memory map.

WO 98/022878 A3

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 97/05916

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F12/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F H04L

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 practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 001 753 A (DAVIO MARC ET AL) 19 March 1991 see the whole document ---	1-6
A	KROPF T ET AL: "A HARDWARE IMPLEMENTATION OF A MODIFIED DES-ALGORITHM" MICROPROCESSING AND MICROPROGRAMMING, vol. 30, no. 1 / 05, 1 August 1990, pages 59-65, XP000141633 see page 60, left-hand column, paragraph 2 - page 63, right-hand column, paragraph 1 ---	1-6
A	ANONYMOUS: "Software Data Encryption Standard" IBM TECHNICAL DISCLOSURE BULLETIN, vol. 29, no. 12, May 1987, NEW YORK, US, pages 5594-5595, XP002057001 see the whole document --- -/--	1-6

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"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)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"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

"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

"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.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 February 1998	10/03/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Powell, D

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	PFITZMANN A ET AL: "MORE EFFICIENT SOFTWARE IMPLEMENTATIONS OF (GENERALIZED) DES" COMPUTERS & SECURITY INTERNATIONAL JOURNAL DEVOTED TO THE STUDY OF TECHNICAL AND FINANCIAL ASPECTS OF COMPUTER SECURITY, vol. 12, no. 5, 1 August 1993, pages 477-500, XP000398172 see the whole document	1-6
A	GB 2 250 617 A (MITSUBISHI ELECTRIC CORP) 10 June 1992	
A	US 4 573 119 A (WESTHEIMER THOMAS O ET AL) 25 February 1986	

INTERNATIONAL SEARCH REPORT

nformation on patent family members

International Application No
PCT/EP 97/05916

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5001753 A	19-03-91	FR 2611962 A	09-09-88
		DE 3885123 D	02-12-93
		DE 3885123 T	05-05-94
		EP 0282123 A	14-09-88
		JP 63236074 A	30-09-88
		KR 9610767 B	08-08-96
GB 2250617 A	10-06-92	JP 4205043 A	27-07-92
		DE 4139197 A	11-06-92
		US 5319765 A	07-06-94
US 4573119 A	25-02-86	NONE	