PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
G06F 7/58

A3

(11) International Publication Number: **WO 96/24098**

(43) International Publication Date: 8 August 1996 (08.08.96)

(21) International Application Number: PCT/IB96/00077

(22) International Filing Date: 29 January 1996 (29.01.96)

(30) Priority Data:

95200242.6	1 February 1995 (01.02.95)	EP
(34) Countries for which the regional or international application was filed:		NL et al.
95200520.5	3 March 1995 (03.03.95)	EP
(34) Countries for which the regional or international application was filed:		NL et al.
95200580.9	9 March 1995 (09.03.95)	EP
(34) Countries for which the regional or international application was filed:		NL et al.
95200642.7	16 March 1995 (16.03.95)	EP
(34) Countries for which the regional or international application was filed:		NL et al.

(71) Applicant: PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(71) Applicant *(for SE only)*: PHILIPS NORDEN AB [SE/SE]; Kottygatan 5, Kista, S-164 85 Stockholm (SE).

(72) Inventors: HOLLMANN, Hendrik, Drik, Lodewijk; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL). BAGGEN, Constant, Paul, Marie, Jozef; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(74) Agent: DE HAAS, Laurens, J.; Internationaal Octrooibureau B.V., P.O. Box 220, NL-5600 AE Eindhoven (NL).

(81) Designated States: JP, KR, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

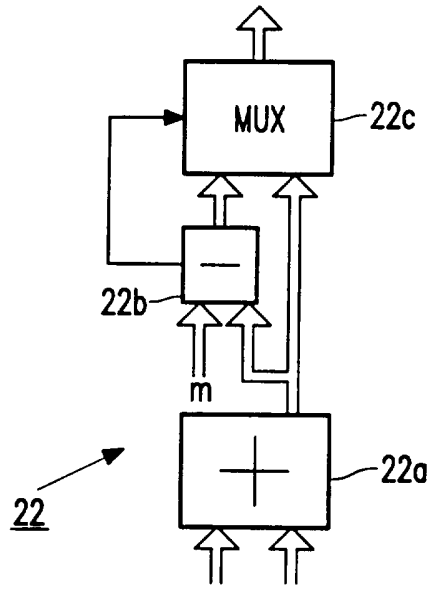
Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(88) Date of publication of the international search report:
26 September 1996 (26.09.96)

(54) Title: CIRCUIT ARRANGEMENT COMPRISING A PERMUTATION UNIT AND METHOD OF PROCESSING A BATCH OF ITEMS

(57) Abstract

The circuit arrangement calculates pseudo-random permutations of a set of numbers. It is required that the permutations that can be calculated by the circuit arrangement include compositions of some basic pseudo-random permutations and the inverse permutations of permutations that are calculated (a composition corresponds to cumulatively repeated reordering of the numbers, an inverse of a permutation is a permutation that undoes the permutation). The basic pseudo-random permutations, their compositions and inverses are all calculated by the same generator whose operation is commanded to calculate the appropriate permutation by specifying a set of integer coefficients f_i. The generator calculates the permutations $\sigma(n)$ of the numbers n=O..m-1 corresponding to I, whereα is an integer number which is divisible by all prime factors of m and by four if m is divisible by four, with a potency $s(\alpha)$ of two or higher. When the same α is used for all permutations it is assured that all compositions and inverses of the generated permutations can be calculated in the same way, by the same generator. By storing a batch of items in a storage medium in a first order and retrieving the items from the storage medium in a second order, the first and second order corresponding to different permutations which are both of this type, it is made possible to permute the batch pseudo-randomly and start storing the batch of items in the storage medium before a previous batch has been fully retrieved from it.



$$\sigma(n) = f_0 + \sum_{i=1}^{s} f_i \left[\frac{n}{i}\right] \alpha^{i-1} \bmod m$$

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia
AT	Austria
AU	Australia
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CS	Czechoslovakia
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgystan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakhstan
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB 96/00077

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: G06F 7/58
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)

IPC6: G06F, H04N

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 practicable, search terms used)

EPODOC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0406017 A1 (INDEPENDENT BROADCASTING AUTHORITY), 2 January 1991 (02.01.91), see whole document ---	7-16
Y	US 4547887 A (S.Y. MUI), 15 October 1985 (15.10.85), see whole document --- --------	7-16

☐ Further documents are listed in the continuation of Box C. ☒ See patent family 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" erlier 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 July 1996	25 -07- 1996
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Rune Bengtsson Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

Inter ɔnal application No.
PCT/IB 96/00077

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. [X] Claims Nos.: 1-6
because they relate to subject matter not required to be searched by this Authority, namely:

Rule 39.1

2. [ ] Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. [ ] Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. [ ] As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. [ ] As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. [ ] As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. [ ] No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

[ ] The additional search fees were accompanied by the applicant's protest.

[ ] No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

Information on patent family members

01/07/96

International application No.
PCT/IB 96/00077

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP-A1- 0406017	02/01/91	AU-A- 5942390	17/01/91
		WO-A,A- 9100672	10/01/91
US-A- 4547887	15/10/85	NONE	