PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 : **G06F 12/14, H04L 9/08**	**A3**	**(11) Internationale Veröffentlichungsnummer: WO 99/28887** **(43) Internationales Veröffentlichungsdatum:** 10. Juni 1999 (10.06.99)

(21) Internationales Aktenzeichen: PCT/DE98/03470

(22) Internationales Anmeldedatum: 25. November 1998 (25.11.98)

(30) Prioritätsdaten:

197 53 274.8	1. Dezember 1997 (01.12.97)	DE
198 01 776.6	19. Januar 1998 (19.01.98)	DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: SIEMENS AKTIENGESELLSCHAFT [DE/DE]; Wittelsbacherplatz 2, D–80333 München (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: GEORGIADES, Jean [GR/DE]; Ungererstrasse 68 A, D–80805 München (DE).

(74) Gemeinsamer Vertreter: SIEMENS AKTIENGESELLSCHAFT; Postfach 22 16 34, D–80506 München (DE).

(81) Bestimmungsstaaten: CA, JP, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht
Mit internationalem Recherchenbericht.
Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist. Veröffentlichung wird wiederholt falls Änderungen eintreffen.

(88) Veröffentlichungsdatum des internationalen Recherchenberichts: 29. Juli 1999 (29.07.99)

(54) Title: METHOD FOR REDUCING STORAGE SPACE REQUIREMENTS FOR A FIRST ELECTRONIC KEY AND CODING/DECODING ARRANGEMENT

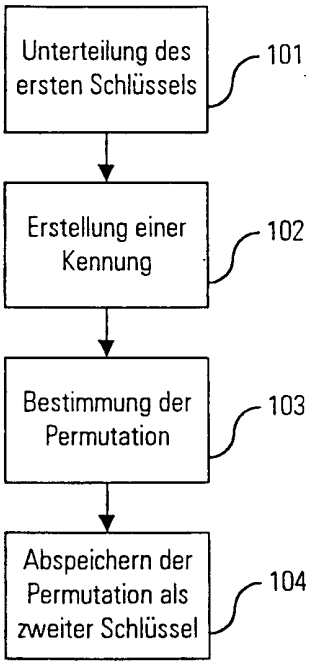
(54) Bezeichnung: VERFAHREN ZUR REDUZIERUNG VON SPEICHERPLATZBEDARF FÜR EINEN ELEKTRONISCHEN ERSTEN SCHLÜSSEL UND ANORDNUNG ZUR VER– UND ENTSCHLÜSSELUNG

(57) Abstract

In order to save the storage space required for a secret key, the latter is subdivided into blocks, the blocks are then permutated and a permutation-linked index is stored. The index is significantly shortened in relation to the secret key. On the other hand, the secret key can be recovered from the index by determining the permutation in the index. The secret key is determined by means of the non-secret permutated blocks and the permutation. The invention also relates to an arrangement, i.e. a chip card, for coding and decoding.

(57) Zusammenfassung

Um Speicherplatzbedarf für einen geheimen Schlüssel einzusparen wird dieser in Blöcke unterteilt, die Blöcke werden permutiert und ein mit der Permutation verknüpfter Index wird abgespeichert. Der Index ist gegenüber dem geheimen Schlüssel signifikant verkürzt. Umgekehrt wird aus dem Index der geheime Schlüssel wiedergewonnen, indem die Permutation aus dem Index ermittelt wird und mittels der nicht geheimzuhaltenden permutierten Blöcken und der Permutation der geheime Schlüssel ermittelt wird. Ferner wird eine Anordnung, z.B. eine Chipkarte, zur Durchführung der Ver- und Entschlüsselung angegeben.



101...SUBDIVISION OF FIRST KEY

102...CREATION OF ANSWER CODE

103...DETERMINATION OF PERMUTATION

104...STORAGE OF PERMUTATION AS SECOND KEY

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	**ES**	Spanien	**LS**	Lesotho	**SI**	Slowenien
AM	Armenien	**FI**	Finnland	**LT**	Litauen	**SK**	Slowakei
AT	Österreich	**FR**	Frankreich	**LU**	Luxemburg	**SN**	Senegal
AU	Australien	**GA**	Gabun	**LV**	Lettland	**SZ**	Swasiland
AZ	Aserbaidschan	**GB**	Vereinigtes Königreich	**MC**	Monaco	**TD**	Tschad
BA	Bosnien-Herzegowina	**GE**	Georgien	**MD**	Republik Moldau	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagaskar	**TJ**	Tadschikistan
BE	Belgien	**GN**	Guinea	**MK**	Die ehemalige jugoslawische Republik Mazedonien	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Griechenland			**TR**	Türkei
BG	Bulgarien	**HU**	Ungarn	**ML**	Mali	**TT**	Trinidad und Tobago
BJ	Benin	**IE**	Irland	**MN**	Mongolei	**UA**	Ukraine
BR	Brasilien	**IL**	Israel	**MR**	Mauretanien	**UG**	Uganda
BY	Belarus	**IS**	Island	**MW**	Malawi	**US**	Vereinigte Staaten von Amerika
CA	Kanada	**IT**	Italien	**MX**	Mexiko		
CF	Zentralafrikanische Republik	**JP**	Japan	**NE**	Niger	**UZ**	Usbekistan
CG	Kongo	**KE**	Kenia	**NL**	Niederlande	**VN**	Vietnam
CH	Schweiz	**KG**	Kirgisistan	**NO**	Norwegen	**YU**	Jugoslawien
CI	Côte d'Ivoire	**KP**	Demokratische Volksrepublik Korea	**NZ**	Neuseeland	**ZW**	Zimbabwe
CM	Kamerun			**PL**	Polen		
CN	China	**KR**	Republik Korea	**PT**	Portugal		
CU	Kuba	**KZ**	Kasachstan	**RO**	Rumänien		
CZ	Tschechische Republik	**LC**	St. Lucia	**RU**	Russische Föderation		
DE	Deutschland	**LI**	Liechtenstein	**SD**	Sudan		
DK	Dänemark	**LK**	Sri Lanka	**SE**	Schweden		
EE	Estland	**LR**	Liberia	**SG**	Singapur		

INTERNATIONAL SEARCH REPORT

Inte ɔnal Application No
PCT/DE 98/03470

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F12/14 H04L9/08

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	WO 97 05720 A (GEN INSTRUMENT CORP) 13 February 1997 see the whole document	1-12
A	US 5 003 596 A (WOOD MICHAEL C) 26 March 1991 see abstract; figures 3,12 see column 7, line 24 - column 8, line 2	1-12
A	US 5 097 504 A (CAMION PAUL ET AL) 17 March 1992	
A	EP 0 636 963 A (IBM) 1 February 1995	

☐ Further documents are listed in the continuation of box C.

☒ 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
28 May 1999	07/06/1999

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

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte onal Application No
PCT/DE 98/03470

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9705720 A	13-02-1997	AU 6681096 A	26-02-1997
		CA 2227375 A	13-02-1997
		CN 1195439 A	07-10-1998
		NO 980325 A	05-03-1998
US 5003596 A	26-03-1991	AT 160476 T	15-12-1997
		AU 635466 B	18-03-1993
		AU 6043190 A	03-04-1991
		CA 2064769 A	18-02-1991
		DE 69031736 D	02-01-1998
		DE 69031736 T	04-06-1998
		EP 0489742 A	17-06-1992
		JP 5501925 T	08-04-1993
		WO 9103113 A	07-03-1991
US 5097504 A	17-03-1992	FR 2596177 A	25-09-1987
		AT 72346 T	15-02-1992
		DE 3776472 A	12-03-1992
		EP 0261162 A	30-03-1988
		WO 8705726 A	24-09-1987
		JP 63503413 T	08-12-1988
EP 0636963 A	01-02-1995	JP 7107086 A	21-04-1995
		US 5661807 A	26-08-1997
		US 5592553 A	07-01-1997

INTERNATIONALER RECHERCHENBERICHT

Inter. ›nales Aktenzeichen
PCT/DE 98/03470

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 G06F12/14 H04L9/08

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 G06F H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	WO 97 05720 A (GEN INSTRUMENT CORP) 13. Februar 1997 siehe das ganze Dokument ---	1-12
A	US 5 003 596 A (WOOD MICHAEL C) 26. März 1991 siehe Zusammenfassung; Abbildungen 3,12 siehe Spalte 7, Zeile 24 - Spalte 8, Zeile 2 ---	1-12
A	US 5 097 504 A (CAMION PAUL ET AL) 17. März 1992 ---	
A	EP 0 636 963 A (IBM) 1. Februar 1995 -----	

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
28. Mai 1999	07/06/1999

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, 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

1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Inter. nales Aktenzeichen
PCT/DE 98/03470

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
WO 9705720 A	13-02-1997	AU 6681096 A	26-02-1997
		CA 2227375 A	13-02-1997
		CN 1195439 A	07-10-1998
		NO 980325 A	05-03-1998
US 5003596 A	26-03-1991	AT 160476 T	15-12-1997
		AU 635466 B	18-03-1993
		AU 6043190 A	03-04-1991
		CA 2064769 A	18-02-1991
		DE 69031736 D	02-01-1998
		DE 69031736 T	04-06-1998
		EP 0489742 A	17-06-1992
		JP 5501925 T	08-04-1993
		WO 9103113 A	07-03-1991
US 5097504 A	17-03-1992	FR 2596177 A	25-09-1987
		AT 72346 T	15-02-1992
		DE 3776472 A	12-03-1992
		EP 0261162 A	30-03-1988
		WO 8705726 A	24-09-1987
		JP 63503413 T	08-12-1988
EP 0636963 A	01-02-1995	JP 7107086 A	21-04-1995
		US 5661807 A	26-08-1997
		US 5592553 A	07-01-1997