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

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
22. Januar 2009 (22.01.2009)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2009/010200 A3

(51) Internationale Patentklassifikation:
H04L 9/08 (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2008/005488

(22) Internationales Anmeldedatum:
4. Juli 2008 (04.07.2008)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2007 033 845.9 18. Juli 2007 (18.07.2007) DE
10 2007 033 846.7 18. Juli 2007 (18.07.2007) DE
10 2007 033 847.5 18. Juli 2007 (18.07.2007) DE
10 2007 033 848.3 18. Juli 2007 (18.07.2007) DE

(71) Anmelder und
(72) Erfinder: **FREISLEBEN, Bernd** [DE/DE]; Philipps-Universität Marburg, Hans-Meerwein- Strasse, 35032 Marburg (DE). **SCHRIDDE, Christian** [DE/DE]; Pasternakstrasse 3, 35039 Marburg (DE). **SMITH, Matthew David** [DE/DE]; Ernst-Lemmerstrasse 70, 35041 Marburg (DE). **KEWITZ, Ansgar** [DE/DE]; Schwanheimer Strasse 65, 60528 Frankfurt (DE).

(74) Anwalt: **2K PATENTANWÄLTE KEWITZ & KOLLEGEN**; Corneliusstrasse 18, 60325 Frankfurt am Main (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE,

[Fortsetzung auf der nächsten Seite]

(54) **Title**: METHOD AND APPARATUS FOR PRODUCING CRYPTOGRAPHIC KEYS FOR PERFORMING KEY AGREEMENT FOR SECURE DIGITAL COMMUNICATION

(54) **Bezeichnung**: VERFAHREN UND VORRICHTUNG ZUR ERZEUGUNG VON KRYPTOGRAPHISCHEN SCHLÜSSELN ZUR DURCHFÜHRUNG EINER SCHLÜSSELEINIGUNG FÜR EINE SICHERE DIGITALE KOMMUNIKATION

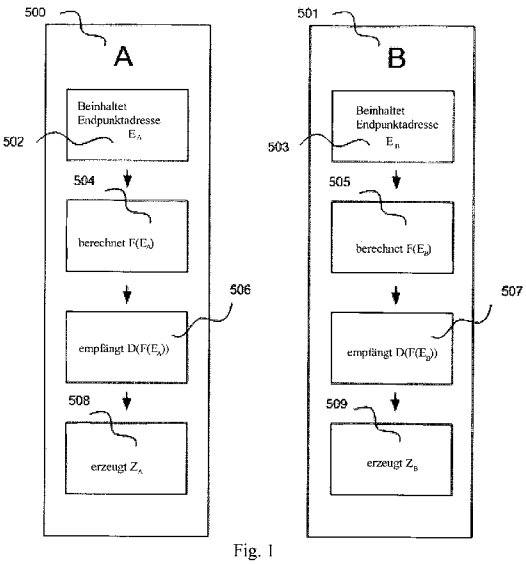


Fig. 1

502 Contains endpoint address E_A
503 Contains endpoint address E_B
504 calculates $F(E_A)$
505 calculates $F(E_B)$
506 receives $D(F(E_A))$
507 receives $D(F(E_B))$
508 produces Z_A
509 produces Z_B

(57) **Abstract**: A method for producing a cryptographic key for performing a method for key agreement for encrypted digital communication, wherein an endpoint address E_A for a communication appliance A is converted directly or indirectly into a portion of the cryptographic key by applying the inverse function L of a trap door one-way function L and is used for the key agreement.

(57) **Zusammenfassung**: Ein Verfahren zur Erzeugung eines kryptographischen Schlüssels zur Durchführung eines Verfahrens zur Schlüsseleinigung für eine verschlüsselte digitale Kommunikation, wobei eine Endpunktadresse E_A eines Kommunikationsgerätes A direkt oder indirekt durch Anwendung der inversen Funktion L einer Einweg-Funktion L mit Falltür in einen Teil des kryptographischen Schlüssels umgewandelt und für die Schlüsseleinigung verwendet wird.

WO 2009/010200 A3

DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Erklärungen gemäß Regel 4.17:

— *hinsichtlich der Berechtigung des Anmelders, ein Patent zu beantragen und zu erhalten (Regel 4.17 Ziffer ii)*

Veröffentlicht:

— *mit internationalem Recherchenbericht (Artikel 21 Absatz 3)*

— *vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eingehen (Regel 48 Absatz 2 Buchstabe h)*

(88) Veröffentlichungsdatum des internationalen Recherchenberichts:

13. August 2009

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2008/005488

A. CLASSIFICATION OF SUBJECT MATTER
INV. 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)
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)
EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 150 411 A (MAURER UELI [CH]) 22 September 1992 (1992-09-22) abstract column 4, line 47 - column 9, line 35 figure 1	1-4,7, 10,11, 17-20, 22,23, 26,27
X	US 2004/240669 A1 (KEMPF JAMES [US] ET AL) 2 December 2004 (2004-12-02) abstract paragraph [0010] - paragraph [0040] paragraph [0072] - paragraph [0076]	1-4,7, 10-13, 15-20, 22,23, 26-29, 31,32

-/--

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

[X] 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" 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
3 Juni 2009	16/06/2009

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, Fax: (+31-70) 340-3016	Dujardin, Corinne

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2008/005488

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	MENEZES A J ET AL: HANDBOOK OF APPLIED CRYPTOGRAPHY; [CRC PRESS SERIES ON DISCRETE MATHEMATICES AND ITS APPLICATIONS], CRC PRESS, BOCA RATON, FL, US, 1 January 1997 (1997-01-01), pages 493,561-562, XP002518153 ISBN: 978-0-8493-8523-0 page 561, line 18 - page 562, line 25	1-4,7, 10,11, 17-20, 22,23, 26,27

INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP2008/005488

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 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. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☒ Claims Nos.: 33
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:

see extra sheet PCT/ISA/210

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 No. III Observations where unity of invention is lacking (Continuation of item 3 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 additional fees, this Authority did not invite payment of additional fees.

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 and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

PCT/EP2008/005488
PCT/ISA/210

Continuation of Box II.2

Claim 33

Claim 33 does not meet the requirements of PCT Article 6. The reasons are the following:

1) Claim 33 is not clear (PCT Article 6):
- Claim 33 refers to a key according to claim 1. However, claim 1 does not define a key but a method in which a part of a cryptographic key is produced.
- Claim 33 attempts to define a data carrier by the method used for producing the content thereof. However, this method is not a feature of the data carrier because it is impossible to determine on the basis of only the data carrier and its content how the content was produced.

The search with respect to claim 33 was therefore restricted to a digital data carrier which comprises a key.

2) Any digital data carrier can therefore be regarded as a data carrier according to claim 33, because any digital content can be regarded as a key.
A very large number of documents is essential for the assessment of novelty. The search yielded such a large number of documents that it became impossible to identify which parts of claim 33 define the subject matter for which protection might justifiably be sought (PCT Article 6). For these reasons, the failure to meet the relevant requirements was taken into consideration in determining the scope of protection of claim 33.

The applicant is advised that claims relating to inventions in respect of which no international search report has been established cannot normally be the subject of an international preliminary examination (PCT Rule 66.1(e)). In its capacity as International Preliminary Examining Authority the EPO generally will not carry out a preliminary examination for subject matter that has not been searched. This also applies in cases where the claims were amended after receipt of the international search report (PCT Article 19) or where the applicant submits new claims in the course of the procedure under PCT Chapter II. However, after entry into the regional phase before the EPO an additional search may be carried out in the course of the examination (cf. EPO Guidelines, C-VI, 8.5) if the deficiencies that led to the declaration under PCT Article 17(2) have been corrected.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2008/005488

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5150411 A	22-09-1992	AT 119726 T	15-03-1995
		CA 2054037 A1	25-04-1992
		DE 69017686 D1	13-04-1995
		EP 0482233 A1	29-04-1992
US 2004240669 A1	02-12-2004	JP 2004040762 A	05-02-2004

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2008/005488

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. H04L9/08

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
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)
EPO-Internal, WPI Data, INSPEC

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 5 150 411 A (MAURER UELI [CH]) 22. September 1992 (1992-09-22) Zusammenfassung Spalte 4, Zeile 47 - Spalte 9, Zeile 35 Abbildung 1 -----	1-4,7, 10,11, 17-20, 22,23, 26,27
X	US 2004/240669 A1 (KEMPF JAMES [US] ET AL) 2. Dezember 2004 (2004-12-02) Zusammenfassung Absatz [0010] - Absatz [0040] Absatz [0072] - Absatz [0076] -----	1-4,7, 10-13, 15-20, 22,23, 26-29, 31,32

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen [X] 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
3. Juni 2009	16/06/2009

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Fax: (+31–70) 340–3016	Dujardin, Corinne

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2008/005488

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	MENEZES A J ET AL: HANDBOOK OF APPLIED CRYPTOGRAPHY; [CRC PRESS SERIES ON DISCRETE MATHEMATICES AND ITS APPLICATIONS], CRC PRESS, BOCA RATON, FL, US, 1. Januar 1997 (1997-01-01), Seiten 493,561-562, XP002518153 ISBN: 978-0-8493-8523-0 Seite 561, Zeile 18 - Seite 562, Zeile 25	1-4,7, 10,11, 17-20, 22,23, 26,27

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2008/005488

Feld Nr. II Bemerkungen zu den Ansprüchen, die sich als nicht recherchierbar erwiesen haben (Fortsetzung von Punkt 2 auf Blatt 1)

Gemäß Artikel 17(2)a) wurde aus folgenden Gründen für bestimmte Ansprüche kein internationaler Recherchenbericht erstellt:

1. ☐ Ansprüche Nr.
weil sie sich auf Gegenstände beziehen, zu deren Recherche diese Behörde nicht verpflichtet ist, nämlich

2. ☒ Ansprüche Nr. 33
weil sie sich auf Teile der internationalen Anmeldung beziehen, die den vorgeschriebenen Anforderungen so wenig entsprechen, dass eine sinnvolle internationale Recherche nicht durchgeführt werden kann, nämlich

siehe BEIBLATT PCT/ISA/210

3. ☐ Ansprüche Nr.
weil es sich dabei um abhängige Ansprüche handelt, die nicht entsprechend Satz 2 und 3 der Regel 6.4 a) abgefasst sind.

Feld Nr. III Bemerkungen bei mangelnder Einheitlichkeit der Erfindung (Fortsetzung von Punkt 3 auf Blatt 1)

Diese Internationale Recherchenbehörde hat festgestellt, dass diese internationale Anmeldung mehrere Erfindungen enthält:

1. ☐ Da der Anmelder alle erforderlichen zusätzlichen Recherchengebühren rechtzeitig entrichtet hat, erstreckt sich dieser internationale Recherchenbericht auf alle recherchierbaren Ansprüche.

2. ☐ Da für alle recherchierbaren Ansprüche die Recherche ohne einen Arbeitsaufwand durchgeführt werden konnte, der zusätzliche Recherchengebühr gerechtfertigt hätte, hat die Behörde nicht zur Zahlung solcher Gebühren aufgefordert.

3. ☐ Da der Anmelder nur einige der erforderlichen zusätzlichen Recherchengebühren rechtzeitig entrichtet hat, erstreckt sich dieser internationale Recherchenbericht nur auf die Ansprüche, für die Gebühren entrichtet worden sind, nämlich auf die Ansprüche Nr.

4. ☐ Der Anmelder hat die erforderlichen zusätzlichen Recherchengebühren nicht rechtzeitig entrichtet. Dieser internationale Recherchenbericht beschränkt sich daher auf die in den Ansprüchen zuerst erwähnte Erfindung; diese ist in folgenden Ansprüchen erfasst:

Bemerkungen hinsichtlich eines Widerspruchs

☐ Der Anmelder hat die zusätzlichen Recherchengebühren unter Widerspruch entrichtet und die gegebenenfalls erforderliche Widerspruchsgebühr gezahlt.

☐ Die zusätzlichen Recherchengebühren wurden vom Anmelder unter Widerspruch gezahlt, jedoch wurde die entsprechende Widerspruchsgebühr nicht innerhalb der in der Aufforderung angegebenen Frist entrichtet.

☐ Die Zahlung der zusätzlichen Recherchengebühren erfolgte ohne Widerspruch.

WEITERE ANGABEN **PCT/ISA/** 210

Fortsetzung von Feld II.2

Ansprüche Nr.: 33

Anspruch 33 erfüllt nicht die Erfordernisse des Artikels 6 PCT.
Die Gründe dafür sind die folgenden:

1) Anspruch 33 ist nicht klar (Artikel 6 PCT):
-- Anspruch 33 verweist auf einen Schlüssel gemäß Anspruch 1. Anspruch 1 definiert aber keinen Schüssel sondern ein Verfahren wobei ein Teil eines kryptographischen Schlüssels erzeugt wird.
-- In Anspruch 33 wird versucht einen Datenträger durch das zur Erzeugung seines Inhalts benutzte Verfahren zu definieren. Dieses Verfahren ist aber kein Merkmal des Datenträgers, da nur aus dem Datenträger und seinem Inhalt unmöglich ist zu bestimmen wie der Inhalt erzeugt wurde.

Die Recherche des Anspruchs 33 wurde folglich auf einen digitalen Datenträger der einen Schlüssel umfasst begrenzt.

2) Jeder beliebige digitale Datenträger kann dann aber als ein Datenträger gemäß Anspruch 33 betrachtet werden, da jeder beliebige digitale Inhalt als Schlüssel betrachtet werden kann.
Eine sehr große Anzahl von Dokumenten ist für die Beurteilung der Neuheit von Bedeutung. Es wurden so viele Dokumente gefunden, dass es unmöglich ist zu bestimmen, welche Teile des Anspruchs 33 den Gegenstand definieren, für den ein Schutzanspruch gerechtfertigt wäre (Artikel 6 PCT). Aus diesen Gründen wurde die Verletzung der einschlägigen Erfordernisse bei der Bestimmung des Recherchenumfangs für den Anspruch 33 berücksichtigt.

Der Anmelder wird darauf hingewiesen, dass Patentansprüche auf Erfindungen, für die kein internationaler Recherchenbericht erstellt wurde, normalerweise nicht Gegenstand einer internationalen vorläufigen Prüfung sein können (Regel 66.1(e) PCT).In seiner Eigenschaft als mit der internationalen vorläufigen Prüfung beauftragte Behörde wird das EPA also in der Regel keine vorläufige Prüfung für Gegenstände durchführen, zu denen keine Recherche vorliegt.Dies gilt auch für den Fall, dass die Patentansprüche nach Erhalt des internationalen Recherchenberichtes geändert wurden (Art. 19 PCT), oder für den Fall, dass der Anmelder im Zuge des Verfahrens gemäss Kapitel II PCT neue Patentansprüche vorlegt.Nach Eintritt in die regionale Phase vor dem EPA kann jedoch im Zuge der Prüfung eine weitere Recherche durchgeführt werden (Vgl. EPA-Richtlinien C-VI, 8.2), sollten die Mängel behoben sein, die zu der Erklärung gemäss Art. 17 (2) PCT geführt haben.

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2008/005488

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 5150411 A	22-09-1992	AT 119726 T	15-03-1995
		CA 2054037 A1	25-04-1992
		DE 69017686 D1	13-04-1995
		EP 0482233 A1	29-04-1992
US 2004240669 A1	02-12-2004	JP 2004040762 A	05-02-2004