BESCHWERDEKAMMERN DES EUROPÄISCHEN PATENTAMTS

BOARDS OF APPEAL OF THE EUROPEAN PATENT OFFICE

CHAMBRES DE RECOURS DE L'OFFICE EUROPEEN DES BREVETS

Interner Verteilerschlüssel:
(A) [ ] Veröffentlichung im ABl.
(B) [ ] An Vorsitzende und Mitglieder
(C) [X] An Vorsitzende
(D) [ ] Keine Verteilung

Datenblatt zur Entscheidung vom 30. November 2010

Beschwerde-Aktenzeichen: T 1326/06 - 3.5.06

Anmeldenummer: 03727434.7

Veröffentlichungsnummer: 1504337

IPC: G06F 7/72

Verfahrenssprache: DE

Bezeichnung der Erfindung:
Berechnung des modularen Inversen eines Wertes

Anmelder:
Giesecke & Devrient GmbH

Stichwort:
RSA Schlüsselpaarberechnung/GIESECKE & DEVRIENT

Relevante Rechtsnormen:
EPÜ Art. 52(1)(2)(3)

Relevante Rechtsnormen (EPÜ 1973):
EPÜ Art. 83

Schlagwort:
"Ausreichende Offenbarung (bejaht)"
"Patentfähige Erfindungen - technische Merkmale (bejaht)"
"Zurückverweisung zur Durchführung einer Recherche"

Zitierte Entscheidungen:
T 0027/97, T 0953/04, T 0641/00, T 0258/03, T 1242/04, G 0003/08

Orientierungssatz:
Verfahren zum Verschlüsseln/Entschlüsseln oder Signieren von elektronischen Nachrichten müssen als technische Verfahren gelten, selbst wenn sich diese wesentlich auf mathematische Verfahren stützen (Gründe 7).

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

Aktenzeichen: T 1326/06 - 3.5.06

E N T S C H E I D U N G
der Technischen Beschwerdekammer 3.5.06
vom 30. November 2010

Beschwerdeführer: Giesiecke & Devrient GmbH
Printregentenstraße 159
D-81677 München (DE)

Vertreter: -

Angefochtene Entscheidung: **Entscheidung der Prüfungsabteilung des Europäischen Patentamts, die am 28. März 2006 zur Post gegeben wurde und mit der die europäische Patentanmeldung Nr. 03727434.7 aufgrund des Artikels 97 (1) EPÜ 1973 zurückgewiesen worden ist.**

Zusammensetzung der Kammer:

Vorsitzender: D. H. Rees
Mitglieder: M. Müller
C. Heath

Sachverhalt und Anträge

I. Die Beschwerde richtet sich gegen die Entscheidung, die europäische Patentanmeldung 03727434.7 zurückzuweisen.

II. Die Anmeldung basiert auf einer internationalen Patentanmeldung, die als WO 03/093972 veröffentlicht wurde und für die das europäische Patentamt als internationale Recherchenbehörde zuständig war. In einer Erklärung über die Nichterstellung eines internationalen Recherchenberichts vom 23. August 2004 wurde festgestellt, dass sich die Ansprüche auf eine mathematische Theorie bezögen, für die gemäß Artikel 17 (2) und Regel 39.1 (i) PCT keine Recherche durchgeführt würde.

Es wurde weiter festgestellt, dass nach Eintritt in die regionale Phase vor dem EPA im Zuge der Prüfung eine weitere Recherche durchgeführt werden könne, sollten die Mängel behoben sein, die zu der Erklärung gemäß Artikel 17 (2) PCT geführt hätten.

III. In den Bescheiden der Prüfungsabteilung vom 12. Mai 2005 und 7. Oktober 2005 wurde dieser Einwand bekräftigt:

Die Ansprüche 1-8 seien als abstrakte mathematische Methode von der Patentierbarkeit gemäß Artikel 52 (2a) und (3) EPÜ ausgeschlossen, und behauptete technische Wirkungen würden nicht zwingend auftreten; das entsprechende Computerprogrammprodukt aus Anspruch 9 hätte ausschließlich Wirkungen auf von der Patentierbarkeit ausgeschlossenen Gebieten und wäre somit gemäß Artikel 52 (2c) und (3) EPÜ ebenfalls nicht patentierbar; und der bekannte Datenträger nach

Anspruch 10 würde in Verbindung mit einem "nicht-technischen" Verfahren kein technisches Problem lösen und demnach keine erfinderische Tätigkeit aufweisen.

Des Weiteren bestehe ein Mangel unter Artikel 83 EPÜ, da die Ansprüche auch Zerlegungen umfassen würden, die nicht das gewünschte Ergebnis hätten, den Modulus zu verkleinern und die Rechenzeit zu verkürzen.

IV. Die Entscheidung erging am 28. März 2006 unter Verweis auf diese beiden Bescheide.

V. Beschwerde gegen diese Entscheidung ging am 11. Mai 2006 ein. Die Beschwerdegebühr wurde am selben Tag entrichtet. Die Beschwerdebegründung ging am 2. August 2006 ein. Die Beschwerdeführerin beantragte die Aufhebung der Entscheidung und die Erteilung eines Patents "auf Grundlage der gültigen Unterlagen" (d. h. in der veröffentlichten Fassung).

VI. Mit einer Ladung zur mündlichen Verhandlung teilte die Kammer der Beschwerdeführerin ihre vorläufige Meinung mit, wonach die Entscheidung zu bestätigen sei, stellte aber für geeignet geänderte Ansprüche eine Zurückverweisung an die erste Instanz nach Artikel 111 (1) EPÜ in Aussicht.

VII. Die Beschwerdeführerin beantragt die Aufhebung der Entscheidung und die Weiterbehandlung auf Grundlage der Ansprüche 1-4, die mit Fax vom 24. September 2010 eingereicht wurden. Für den Fall einer Zurückverweisung an die erste Instanz wurde der Antrag auf mündliche Verhandlung zurückgezogen (siehe den am 11. August 2010 eingegangenen Schriftsatz).

Anspruch 1 gemäß diesem Antrag lautet:

"Computerimplementiertes Verfahren der Schlüsselpaarbestimmung bei einem RSA-Codier- oder Signaturverfahren durch Berechnung des modularen Inversen (R) eines Wertes (E) zu einem Modul (M) mittels der folgenden Schritte:

a) Bestimmen (10) einer Zerlegung des Moduls (M) in mindestens zwei Faktoren P-1 und Q-1, wobei P und Q die bei RSA vorgegebenen Primzahlen sind,

b) Berechnen (12,14) je eines Hilfswertes (R1,R2) zu jedem der in Schritt a) bestimmten Faktoren (P-1,Q-1), wobei jeder Hilfswert (R1,R2) das modulare Inverse des Wertes (E) zu dem jeweiligen Faktor (P-1,Q-1) als Modul ist, und

c) Berechnen (16) des modularen Inversen (R) des Wertes (E) zum Modul (M) zumindest unter Verwendung der in Schritt b) berechneten Hilfswerte (R1,R2)."

Ansprüche 2-4 entsprechen den ursprünglichen Ansprüchen 4-6.

VIII. Mit Schreiben vom 29. September 2010 wurde die anberaumte mündliche Verhandlung abgesagt.

Entscheidungsgründe

1. Die Beschwerde ist zulässig, da die Erfordernisse von Artikel 106-108 und Regel 64 EPÜ 1973 erfüllt sind, die nach J 10/07 (Gründe 1), anwendbar sind (vgl. Sachverhalt und Anträge, oben, Punkte IV und V).

Artikel 123 (2) EPÜ

2. Die obligatorische Verwendung der Faktoren P-1 und Q-1, wobei P und Q die bei RSA vorgegebenen Primzahlen sind, geht an verschiedenen Stellen aus der veröffentlichten Anmeldung hervor (z. B. S. 1, 2. Absatz in Verbindung mit S. 6, letzter Absatz). Es geht aus dem ursprünglichen Anspruch 8 hervor, dass die kryptografische Anwendung aus dem ursprünglichen Anspruch 1 die Schlüsselpaarbestimmung bei einem RSA-Codier- oder Signaturverfahren ist. Es ist explizit offenbart, dass die Berechnung des modularen Inversen computerimplementiert erfolgt (vgl. z. B. ursprüngliche Ansprüche 9 und 10, sowie S. 6, Zn. 17-21). Es ergibt sich aus dem RSA-Verfahren, dass mit dem Ergebnis der modularen Inversion das Schlüsselpaar zur Verfügung steht (vgl. S. 1, Zn. 10-18, sowie S. 6, Zn. 23-25); damit ist ein computerimplementiertes Verfahren der Schlüsselpaarbestimmung offenbart.

3. Die Kammer kommt somit zum Ergebnis, dass der vorliegende Anspruch 1 nicht über den Inhalt der Anmeldung in der ursprünglich eingereichten Fassung hinausgeht. Dasselbe gilt unmittelbar auch für die unveränderten Ansprüche 2-4.

Artikel 83 EPÜ 1973

4. Anspruch 1 verlangt obligatorisch die Zerlegung des Moduls M in wenigstens die zwei Faktoren P-1 und Q-1 (vgl. Anspruch 1, Schritt a). Diese Zerlegung ist konstruktionsbedingt immer möglich. Damit ist zum einen sichergestellt, dass der erfindungsgemäße Berechnungsvorteil (vgl. S. 8, Zn. 1-13) im gesamten Bereich des Anspruchs 1 tatsächlich eintritt, und zum anderen, dass die Suche nach einer geeigneten Faktorisierung keinen für den Fachmann unzumutbaren Aufwand darstellt. Demgemäß hat die Kammer keinen Zweifel daran, dass die Beschreibung den Gegenstand der Erfindung gemäß Anspruch 1 so deutlich und vollständig offenbart, dass ein Fachmann sie ausführen kann.

Artikel 52 (2) and (3) EPÜ

5. Der Gegenstand aller Ansprüche hat nach ständiger Rechtsprechung technischen Charakter und ist somit im Einklang mit Artikel 52 (2) und (3), da es sich um computerimplementierte Verfahren handelt (vgl. T 258/03, Hitachi; Leitsatz 1; Amtsblatt EPA, 2004, 575; sowie G 3/08; Gründe 10.7).

5.1 Das räumt den einzigen direkt gegen die ursprünglichen Verfahrensansprüche erhobenen Einwand aus. Ein Computerprogrammprodukt und ein tragbarer Datenträger werden nicht mehr beansprucht.

5.2 Allerdings war die Prüfungsabteilung der Meinung, dass das ursprünglich beanspruchte Computerprogrammprodukt nur Wirkungen auf von der Patentierbarkeit ausgeschlossenen Gebieten habe. Die Kammer nimmt an,

dass die Prüfungsabteilung diese Meinung auch für die ursprünglichen Verfahrensansprüche vertreten hätte, wenn diese als "computerimplementiert" beansprucht gewesen wären.

5.3 Eine direkte Zurückverweisung an die erste Instanz hätte daher aller Wahrscheinlichkeit nach zu einer neuen Zurückweisung mit Bezug auf Artikel 56 EPÜ 1973 anstelle von Artikel 52 (2) und (3) EPÜ aber mit im wesentlichen unveränderten Argumenten geführt.

5.4 Es erscheint der Kammer daher angemessen, im Rahmen ihrer Kompetenz unter Artikel 111 (1) EPÜ 1973 zu prüfen, ob die Verfahren nach Ansprüchen 1-4 über die Tatsache ihrer Computerimplementierung hinaus eine technische Wirkung entfalten.

Technizität

6. RSA ist ein asymmetrisches Kryptosystem, das sowohl zur Verschlüsselung als auch zur digitalen Signatur verwendet werden kann. Es verwendet ein Schlüsselpaar bestehend aus einem privaten Schlüssel, der zum Entschlüsseln oder Signieren von Daten verwendet wird, und einem öffentlichen Schlüssel, der zum Verschlüsseln oder Prüfen von Signaturen dient. Der private Schlüssel wird geheim gehalten und kann nicht oder nur mit extrem hohem Aufwand aus dem öffentlichen Schlüssel berechnet werden.

6.1 Schlüssel und Nachrichten werden als Zahlen dargestellt, und sowohl die Bestimmung des Schlüsselpaars, als auch das Ver-/Entschlüsseln oder Signieren von Nachrichten wird durch mathematische Operationen beschrieben: die

Wahl zweier großer Primzahlen P und Q und die Berechnung von N=P*Q und M=(P-1)*(Q-1), die Wahl einer zu M teilerfremden Zahl E und die Bestimmung des modularen Inversen von E zum Modulus M (bei der Schlüsselpaarbestimmung), sowie die Potenzierung modulo N (beim Ver-/Entschlüsseln bzw. Signieren). Zudem beruht die Geheimhaltung des privaten Schlüssels auf der begründeten mathematischen Annahme, dass die Primfaktorzerlegung ein prinzipiell schwieriges Problem, und insbesondere die Zerlegung von N in ihre Primfaktoren P und Q praktisch unmöglich ist. Somit erscheint RSA in großen Teilen als ein rein mathematisches Verfahren.

6.2 Andererseits befasst sich die asymmetrische Kryptografie mit der konkreten Aufgabe, einen sicheren Austausch von elektronischen Nachrichten zu gewährleisten und dabei gleichzeitig den Schlüsselaustausch und die Geheimhaltung zu erleichtern. Im Unterschied zur symmetrischen Krytografie, muss bei der asymmetrischen Krytografie jeder Nutzer des Systems nur seinen eigenen privaten Schlüssel geheim halten.

6.3 Nach Meinung der Kammer handelt es sich beim sicheren Austausch von elektronischen Nachrichten um eine technische Wirkung, die zu erzielen als eine technische Aufgabe angesehen werden muss.

6.4 RSA löst diese Aufgabe mit mathematischen Mitteln. Mit RSA gelang ein Durchbruch in der Entwicklung der Kryptografie: RSA wird als das erste praktikable, konkret implementierbare asymmetrische Kryptosystem angesehen und ist heute in zahlreichen kryptografischen Sicherheitssystemen eine zentrale Komponente. Die RSA

zugrundeliegende Mathematik dient somit unmittelbar der Lösung eines konkreten technischen Problems.

7. Die Kammer ist aus diesem Grund der Ansicht, das Verfahren zum Verschlüsseln/Entschlüsseln oder Signieren von elektronischen Nachrichten mittels RSA als technische Verfahren gelten müssen, selbst wenn sich diese wesentlich auf mathematische Verfahren stützen.

7.1 Mit dieser Einschätzung ist die Kammer im Einklang mit den Entscheidungen T 953/04, Software distribution/FUJITSU, und T 27/97, Cryptographie à clés publiques/FRANCE TELECOM (beide nicht im Amtsblatt veröffentlicht):

In T 953/04 wird festgestellt, dass die "Verwendung kryptografischer Verfahren im technischen Kontext von elektronischer Datenverarbeitung and Kommunikation ... sicherlich technischen Charakter" hat (Gründe 3.3; Übersetzung durch die Kammer), und T 27/97 kommt zu dem Ergebnis, dass ein "Verfahren zur Verschlüsselung oder Entschlüsselung einer in Form eines digitalen Wortes dargestellten Nachricht mit Hilfe von Algorithmen der asymmetrischen Kryptografie vom Typ RSA", das "zur Verwendung in elektronischen Systemen bestimmt" ist, nicht von der Patentierbarkeit gemäß Artikel 52 (2) und (3) EPÜ ausgeschlossen ist, "selbst wenn ein abstrakter Algorithmus oder ein mathematisches Verfahren der Erfindung zugrunde liegt" (Gründe 3, Übersetzung durch die Kammer).

7.2 Anspruch 1 richtet sich nach Oberbegriff auf ein computerimplementiertes Verfahren *der Schlüsselpaarbestimmung bei einem RSA-Codier- oder Signaturverfahren*.

Mit dieser Angabe geht nach Auffassung der Kammer Anspruch 1 darüber hinaus, nur die *Eignung* der Schlüsselpaarbestimmung für RSA zu fordern. Stattdessen wird so beschränkend festgelegt, dass die Schlüsselpaarbestimmung tatsächlich in ein RSA-Codier- oder Signaturverfahren eingebettet und mit diesem funktional verknüpft ist. Diese Beschränkung trägt somit zum technischen Charakter des Anspruchsgegenstands bei.

Wie das RSA-Codier- oder Signaturverfahren im einzelnen ausgestaltet ist und wie etwa die einschlägigen Verfahrensschritte auf unterschiedliche Programme, Datenträger oder Computer verteilt sind, bleibt in dieser Formulierung offen.

8. Die beanspruchten Berechnungsschritte beziehen sich ausschließlich auf die Schlüsselpaarbestimmung, wobei die so berechneten Schlüssel genau die bekannten, gemäß RSA definierten Schlüssel sind. Daher hat der beanspruchte Rechenweg keinerlei Wirkungen auf das RSA Codier- bzw. Signaturverfahren im engeren Sinne.

8.1 Allerdings stellt die Schlüsselpaarberechnung zweifellos eine wesentliche Komponente des RSA-Kryptosystems dar: Wie oben dargestellt ist die asymmetrische Kryptografie ohne Schlüssel mit den relevanten mathematischen Eigenschaften nicht denkbar.

8.2 Daher ist die Kammer der Meinung, dass auch die beanspruchte Berechnung des RSA-Schlüsselpaars mit all ihren Rechenschritten zum technischen Charakter der Erfindung nach Anspruch 1 beiträgt.

9. Nach gefestigter Rechtsprechung der Beschwerdekammern müssen bei der Beurteilung der erfinderischen Tätigkeit einer Erfindung diejenigen Merkmale berücksichtigt werden, die zum technischen Charakter der Erfindung beitragen (vgl. T 641/00, Comvik; Leitsatz 1; Amtsblatt EPA 2003, 352; und G 3/08; Gründe 12.2.1 and 12.2.2).

9.1 Die anspruchsgemäße Berechnung des modularen Inversen erfolgt nicht nach einem der in der Beschreibung genannten üblichen Berechnungsverfahren auf der Basis des euklidischen Algorithmus (vgl. S. 1, letzter Absatz - S. 2, 1. Absatz).

9.2 Die Kammer hat auch keinen Anhaltspunkt dafür anzunehmen, dass das beanspruchte Verfahren als notorisch bekannt gelten kann oder dem allgemeinen Fachwissen zugerechnet werden muss (vgl. T 1242/04, Bereitstellung produktspezifischer Daten/MAN; Gründe 9.2).

9.3 Damit kann über Neuheit und erfinderische Tätigkeit nicht ohne druckschriftlichen Stand der Technik entschieden werden, so dass die Akte zur Durchführung der angekündigten Zusatzrecherche und zur Fortsetzung des Prüfungsverfahrens zurückzuverweisen ist.

Entscheidungsformel

Aus diesen Gründen wird entschieden:

1. Die angefochtene Entscheidung wird aufgehoben.

2. Die Angelegenheit wird zur Weiterbehandlung an die erste Instanz zurückverwiesen.

Die Geschäftsstellenbeamtin: Der Vorsitzende:

B. Atienza Vivancos D. H. Rees