**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) [ ] An Vorsitzende
(D) [X] Keine Verteilung

# Datenblatt zur Entscheidung vom 23. Mai 2012

**Beschwerde-Aktenzeichen:** T 2318/08 - 3.5.06

**Anmeldenummer:** 06013333.7

**Veröffentlichungsnummer:** 1746495

**IPC:** G06F 7/72

**Verfahrenssprache**: DE

**Bezeichnung der Erfindung:**
Verwendung eines Koprozessors zur modularen Inversion

**Anmelder:**
Giesecke & Devrient GmbH

**Stichwort:**
Koprozessor zur modularen Inversion/GIESECKE & DEVRIENT

**Relevante Rechtsnormen (EPÜ 1973):**
EPÜ Art. 56

**Schlagwort:**
"Technische Aufgabe gelöst - nach Änderung (ja)"
"Erfinderische Tätigkeit - nach Änderung (ja)"

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

**Aktenzeichen:** T 2318/08 - 3.5.06

# E N T S C H E I D U N G
**der Technischen Beschwerdekammer 3.5.06**
**vom 23. Mai 2012**

**Beschwerdeführer**: (Anmelder)
Giesecke & Devrient GmbH
Prinzregentenstraße 159
D-81677 München (DE)

**Vertreter**:
Giesecke & Devrient GmbH
Patent- und Lizenzabteilung
Prinzregentenstraße 159
D-81677 München (DE)

**Angefochtene Entscheidung:**
**Entscheidung der Prüfungsabteilung des Europäischen Patentamts, die am 26. Juni 2008 zur Post gegeben wurde und mit der die europäische Patentanmeldung Nr. 06013333.7 aufgrund des Artikels 97 (2) EPÜ zurückgewiesen worden ist.**

**Zusammensetzung der Kammer:**

**Vorsitzender:** D. H. Rees
**Mitglieder:** M. Müller
M-B. Tardo-Dino

## Sachverhalt und Anträge

I. Die Beschwerde richtet sich gegen die Entscheidung der Prüfungsabteilung vom 26. Juni 2008, die europäische Patentanmeldung 06013333.7 zurückzuweisen mangels erfinderischer Tätigkeit, Artikel 56 EPC 1973, im Lichte der folgenden Dokumente:

D1: A. K. Lenstra, "Computational Methods in Public Key Cryptology", 13. August 2001
D2: US 5 961 578.

II. Beschwerde gegen diese Entscheidung ging am 19. August 2008 ein, und die Beschwerdegebühr wurde am selben Tag entrichtet. Eine Beschwerdebegründung ging am 28. Oktober 2008 ein. Es wurde beantragt, die angefochtene Entscheidung aufzuheben und das Patent auf Basis eines neuen, mit der Beschwerdebegründung vorgelegten Anspruchssatzes zu erteilen.

III. Mit einer Ladung zur mündlichen Verhandlung teilte die Kammer der Beschwerdeführerin ihre vorläufige Meinung mit, nach der die Ansprüche mangels ersichtlichen technischen Effekts nicht erfinderisch seien, Artikel 56 EPÜ 1973. Darüber hinaus erhob die Kammer Einwände unter Artikel 84 und Regel 29 (4) EPÜ 1973.

IV. In Erwiderung darauf legte die Beschwerdeführerin vier neue Anspruchssätze gemäß einem Hauptantrag und drei Hilfsanträgen vor. Die Kammer teilte der Beschwerdeführerin mit, dass sie zwar den 1. Hilfsantrag, nicht aber den Hauptantrag für erteilbar hielte, und wies darauf hin, dass die Beschreibung noch anzupassen sei.

V. Die Beschwerdeführerin zog daraufhin den Hauptantrag zurück und beantragte die Erteilung eines Patents auf Grundlage der folgenden Unterlagen:

Beschreibung, Seiten
1, 2, 7-11 wie ursprünglich eingereicht
3 eingereicht am 23. April 2012
4-6, 12 eingereicht am 9. Mai 2012
Zeichnungen, Blatt
1/1 wie ursprünglich eingereicht
Ansprüche, Nr.
1-7 gemäß 1. Hilfsantrag vom 23. April 2012.

VI. Aufgrund dieser Änderungen wurde die anberaumte mündliche Verhandlung abgesagt.

VII. Anspruch 1 des einzigen Antrags lautet wie folgt:

"Verfahren zur Verwendung eines Koprozessors (16) zur Bestimmung des modularen Inversen x eines Eingangswertes u bezüglich eines Moduls v, wobei:
- aus dem Eingangswert u derart ein erster erweiterter Wert U mit einer gegenüber dem Eingangswert u vergrößerten Bitlänge bestimmt wird, dass sich in einem Bitabschnitt des ersten erweiterten Werts U die Informationen des Eingangswerts u befinden, wobei das Bestimmen des ersten erweiterten Werts U die Multiplikation des Eingangswertes u mit einem Erweiterungsfaktor f umfasst und wobei f>2v gilt,
- aus dem Modul v derart ein zweiter erweiterter Wert V mit einer gegenüber dem Eingangswert v vergrößerten Bitlänge bestimmt wird, dass sich in einem Bitabschnitt des zweiten erweiterten Werts V die Informationen des Moduls v befinden, wobei das Bestimmen des zweiten

erweiterten Werts V die Multiplikation des Moduls v mit dem Erweiterungsfaktor f umfasst,

- der Koprozessor (16) für Ganzzahl-Berechnungen mit zumindest der vergrößerten Bitlänge vorgesehen ist,
- mindestens einer der erweiterten Werte U, V eine Störung an einer Bitposition enthält, die von denjenigen Bitpositionen, an denen sich die Informationen des Eingangswerts u bzw. des Moduls v befinden, beabstandet ist,
- ausgehend von den beiden erweiterten Werten U und V unter Verwendung des Koprozessors (16) Verarbeitungsschritte (34) eines euklidischen Verfahrens ausgeführt werden, solange eine vorgegebene Ausführungsbedingung erfüllt ist, und
- das modulare Inverse x in Abhängigkeit von dem Ergebnis der ausgeführten Verarbeitungsschritte (34) bestimmt wird."

## Entscheidungsgründe

1. Die Kammer hat keinen Zweifel daran, dass die vorliegenden Ansprüche den Erfordernissen des Artikel 84 EPÜ 1973 entsprechend deutlich und knapp gefasst und durch die geänderte Beschreibung gestützt sind, sowie dass der Gegenstand der geänderten Anmeldung nicht über den Inhalt der Anmeldung in ihrer ursprünglich eingereichten Fassung hinausgeht, Artikel 123 (2) EPÜ. Der derzeitige Anspruch 1 insbesondere stützt sich auf die ursprünglichen Ansprüche 1, 6, 7 und 12 in Verbindung mit der ursprünglichen Beschreibung auf Seite 6, Zeile 24 - Seite 7, Zeile 16.

2. Die Erfindung betrifft ein Verfahren zur Berechnung des in kryptografischen Verfahren relevanten modularen Inversen eines Wertes u zu einem Modul v. Die Erfindung geht von einem zur Berechnung des modularen Inversen bekannten erweiterten euklidischen Verfahren aus (vgl. ursprüngliche Beschreibung, Seiten 2 und 3, je 4. Absatz).

2.1 Die Kernidee des Verfahrens besteht darin, die Ausgangswerte u und v nicht wie gewöhnlich "rechtsbündig" in den niederwertigen Bitpositionen darzustellen, sondern sie so weit in höherwertige Positionen zu verschieben, dass in den niederwertigen Positionen Raum für die übrigen Parameter des Verfahrens entsteht, in Verbindung mit der Erkenntnis, dass auf der so geänderten Darstellung (im wesentlichen) nur die Rechenschritte des gewöhnlichen euklidischen Verfahrens durchgeführt werden müssen, um die Ergebnisse des erweiterten Verfahrens zu erhalten. Somit benötigt das neue Verfahren weniger Rechenschritte als das erweiterte euklidische Verfahren, allerdings um den Preis einer größeren Bitlänge der Eingangswerte (vgl. ursprüngliche Beschreibung, Seite 3, 4. Absatz - Seite 4, 1. Absatz).

2.2 Die praktische Relevanz des Verfahrens ergibt sich aus den folgenden Beobachtungen: In der kryptografischen Praxis wird die modulare Inversion typischerweise mit einem Koprozessor durchgeführt, der für Operationen auf ganzen Zahlen ausgelegt sind, deren Bitlänge sich wiederum nach der in RSA üblichen Schlüssellänge richtet. Die zu RSA alternativen sogenannten EC-Verfahren verwenden wesentliche kürzere Schlüssel, so dass die modulare Inversion nur für kleinere Zahlen durchgeführt werden muss. Wenn demnach ein für RSA optimierter Koprozessor für EC eingesetzt wird, bleibt ein Teil seiner Bits

systematisch ungenutzt. Das erfindungsgemäße Verfahren nutzt diese ohnehin vorhandenen überzähligen Bits zur Beschleunigung des gewünschten Verfahrens.

3. Aus dem vorliegenden Stand der Technik geht als bekannt hervor, dass es für die in der Kryptografie notwendigen modularen Ganzzahl-Berechnungen dedizierte Koprozessoren gibt (vgl. D2, Spalte 8, Zeilen 50-59), und dass Varianten des Euklidischen Verfahren zur Berechnung des modularen Inversen verwendet werden (vgl. D1, Abschnitt 3.3, Seiten 14-19). Beides wurde schon in der ursprünglichen Anmeldung als bekannt anerkannt (Seite 1, 3. Absatz, sowie Seite 2, Zeile 18 - Seite 3, Zeile 7) und von der Beschwerdeführerin nicht bestritten. Auch unbestritten ist, dass das beanspruchte Verfahren gegenüber den bekannten euklidischen Verfahren neu ist. Neuheit der beanspruchten Erfindung steht somit nicht in Frage.

4. Ebenso wenig steht in Frage, dass die geschickte Verwendung eines bekannten Koprozessors zur beschleunigten Implementierung eines ebenfalls bekannten Verfahrens eine technische Aufgabe löst und somit grundsätzlich die Erfordernisse des Artikels 56 EPÜ 1973 erfüllen kann.

4.1 Die Prüfungsabteilung begründete ihre Entscheidung damit, dass dem Gegenstand des unabhängigen Anspruchs 1 seinem damaligen Wortlaut nach eine Lösung dieser technischen Aufgabe nicht zugeschrieben werden könne. Dazu fehle es ihm zum einen an der Beschränkung auf einen Koprozessor, der "für Ganzzahl-Berechnungen mit zumindest der vergrößerten Bitlänge vorgesehen ist", zum anderen an der Angabe, dass die Hilfsvariablen in den niederwertigen Bits der vergrößerten Bitlänge mitgeführt würden (vgl. Entscheidung, Punkte 7.2 und 11).

4.2 Der vorliegende Anspruch 1 ist nun in der geforderten Weise beschränkt: Der beanspruchte Koprozessor ist für eine Bitlänge "vorgesehen", die größer ist als diejenige, die für die Eingangswerte u und v nötig sind. Anspruchsgemäß werden die überzähligen Bits genutzt, indem u und v durch Multiplikation mit einem Erweiterungsfaktor in höhere "Bitabschnitte" verschoben werden, und in die damit freiwerdenden, niederwertigen Bitabschnitte "Störungen" eingebracht werden, die als Ausgangswerte für Hilfsvariablen der anschließenden Berechnung dienen.

5. Dass der beanspruchte Gegenstand - soweit er die behauptete technische Aufgabe löst - gegenüber dem zitierten Stand der Technik naheliegend sei, wird in der strittigen Entscheidung nicht behauptet. Im Gegenteil beurteilt die Entscheidung in einem *obiter dictum* einen geeignet beschränkten Anspruch als erfinderisch (vgl. Punkt 11).

5.1 Die Kammer stimmt der Prüfungsabteilung in dieser Bewertung zu. Daraus, dass zum einen kryptografische Koprozessoren und zum anderen das Euklidische Verfahren und seine Varianten bekannt sind, ergibt sich nur, dass die Implementierung Euklidischer Verfahren auf kryptografischen Koprozessoren für den Fachmann naheliegen würde.

5.2 Es ergibt sich daraus jedoch kein Hinweis darauf, freibleibende Bitabschnitte in einem solchen Koprozessor in der beanspruchten Weise zur Beschleunigung des Verfahrens zu verwenden.

5.3 Daher ist der beanspruchte Gegenstand erfinderisch gegenüber dem aus D1 und D2 bekannten Stand der Technik, Artikel 56 EPÜ 1973.

## Entscheidungsformel

## Aus diesen Gründen wird entschieden:

1. Die Beschwerde wird aufgehoben.

2. Die Sache wird an die Prüfungsabteilung zurückverwiesen mit der Anordnung ein Patent auf Grundlage der folgenden Unterlagen zu erteilen:

Beschreibung, Seiten
1, 2, 7-11 wie ursprünglich eingereicht
3 eingereicht am 23. April 2012
4-6, 12 eingereicht am 9. Mai 2012
Zeichnungen, Blatt
1/1 wie ursprünglich eingereicht
Ansprüche, Nr.
1-7 gemäß 1. Hilfsantrag vom 23. April 2012.

Die Geschäftsstellenbeamtin: Der Vorsitzende:

B. Atienza Vivancos D. H. Rees