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 25. Juli 2012

Beschwerde-Aktenzeichen: T 0083/09 - 3.5.06

Anmeldenummer: 03735380.2

Veröffentlichungsnummer: 1506473

IPC: G06F 7/72

Verfahrenssprache: DE

Bezeichnung der Erfindung:
Ausspähungsgeschützte modulare Inversion

Anmelder:
Giesecke & Devrient GmbH

Stichwort:
Ausspähungsgeschützte modulare Inversion/GIESECKE & DEVRIENT

Relevante Rechtsnormen (EPÜ 1973):
EPÜ Art. 56, 82
EPÜ R. 30 (1,2)

Schlagwort:
"Erfinderische Tätigkeit - nach Änderung (ja)"
"Einheitlichkeit (ja)"

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

Aktenzeichen: T 0083/09 - 3.5.06

E N T S C H E I D U N G
der Technischen Beschwerdekammer 3.5.06
vom 25. Juli 2012

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

Vertreter:
Giesecke & Devrient GmbH
Patent- und Lizenzabteilung
Postfach 80 07 29
D-81607 München (DE)

Angefochtene Entscheidung:
Entscheidung der Prüfungsabteilung des Europäischen Patentamts, die am 14. Juli 2008 zur Post gegeben wurde und mit der die europäische Patentanmeldung Nr. 03735380.2 aufgrund des Artikels 97 (2) EPÜ 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 der Prüfungsabteilung, die Anmeldung 03 735 380.2 zurückzuweisen. In der Entscheidung werden u. a. die folgenden Dokumente zitiert:

D1: US 2001/0002486 A1
D4: WO 01/31436 A1
D5: Akkar M.-L. *et al.*, "An Implementation of DES and AES, Secure against Some Attacks", CHES 2001, LNCS 2162, 2001, Seiten 309-318,

und es wird argumentiert, dass der beanspruchte Gegenstand (gemäß einer Alternative) gegenüber D4 in Verbindung mit D5 nicht erfinderisch sei, Artikel 56 EPÜ 1973. In einem *obiter dictum* wird weiter argumentiert, dass die andere beanspruchte Alternative nicht erfinderisch sei gegenüber D4 in Kombination mit D1, dass beide Alternativen gemäß Anspruch 1 nicht einheitlich miteinander seien, Artikel 82 EPÜ 1973, und dass Ansprüche 7 und 8 gegen Artikel 83 EPÜ 1973 verstießen.

II. Beschwerde gegen diese Entscheidung ging am 25. Juli 2008 ein, und die Beschwerdegebühr wurde am selben Tag entrichtet. Eine Beschwerdebegründung wurde am 17. November 2008 eingereicht.

III. Mit einer Ladung zur mündlichen Verhandlung erhob die Kammer Einwände unter Artikel 83 und 84 EPÜ 1973, aber teilte der Beschwerdeführerin auch ihre vorläufige Meinung mit, nach der geeignet geänderte Ansprüche die erforderliche erfinderische Tätigkeit aufwiesen.

IV. In Erwiderung auf die Ladung legte die Beschwerdeführerin geänderte Ansprüche und Beschreibungsseiten vor und beantragte, die Entscheidung aufzuheben und ein Patent auf der Grundlage der folgenden Unterlagen zu erteilen.

Beschreibung, Seiten
1, 2, 8, 9 veröffentlichte Fassung
3-7, 10 eingereicht mit Schreiben vom 25. Juni 2012
Zeichnungen, Blatt
1 veröffentlichte Fassung
Ansprüche, Nr.
1-3 eingereicht mit Schreiben vom 25. Juni 2012

V. Die Kammer sagte daraufhin die anberaumte mündliche Verhandlung ab.

VI. Anspruch 1 lautet wie folgt:

"Verfahren zum ausspähungsgeschützten Bestimmen des modularen Inversen b eines Wertes a zum Modul n in einer kryptographischen Anwendung, bei der es sich um eine Schlüsselpaarbestimmung bei einem RSA-Codierverfahren oder einem RSA-Signaturverfahren handelt, wobei das Verfahren auf einem Prozessor ausgeführt wird und die folgenden Schritte umfasst:

a) Bestimmen (10) eines Hilfswerts β und eines dazu teilerfremden Hilfsmoduls δ zumindest in Abhängigkeit von dem Wert a, dem Modul n sowie mindestens einem Maskierungsparameter r und mindestens einem Hilfsparameter s derart, daß sich der Hilfswert β von dem Wert a und/oder der Hilfsmodul δ von dem Modul n unterscheiden/unterscheidet, wobei der mindestens

eine Maskierungsparameter r zufällig gewählt wird und/oder die Größenordnung des Moduls n aufweist und wobei der mindestens eine Hilfsparameter s zufällig gewählt wird und/oder die Größenordnung des Moduls n aufweist,

b) Bestimmen (20) eines Hilfsinversen β' als modulares Inverses des Hilfswertes β zum Hilfsmodul δ, und

c) Bestimmen (24) des modularen Inversen b zumindest in Abhängigkeit von den folgenden Werten:
- dem Hilfsinversen β',
- dem mindestens einen Maskierungsparameter r, und
- dem Hilfswert β und/oder dem Hilfsmodul δ, wobei der Hilfsparameter s nicht unmittelbar in die Bestimmung des modularen Inversen b einfließt,

wobei in Schritt a) der Hilfswert β und der Hilfsmodul δ gemäß den Gleichungen $ra=\alpha n+\beta$ und $sn=\gamma a+\delta$ mit $0\leq\beta<n$ und $0\leq\delta<a$ bestimmt werden und in Schritt c) das modulare Inverse b durch Auswerten der Gleichung $b=\beta' r+\delta'\gamma \bmod n$ mit $\delta'=(\beta\beta'-1)/\delta$ bestimmt wird oder
wobei in Schritt a) der Hilfswert β und der Hilfsmodul δ gemäß den Gleichungen $ra=\alpha n+\delta$ und $sn=\gamma a+\beta$ mit $0\leq\delta<n$ und $0\leq\beta<a$ bestimmt werden und in Schritt c) das modulare Inverse b durch Auswerten der Gleichung $b=-(\delta' r+\beta'\gamma) \bmod n$ mit $\delta'=(\beta\beta'-1)/\delta$ bestimmt wird."

Entscheidungsgründe

1. Die Erfindung bezieht sich auf das Gebiet der Kryptografie und betrifft die insbesondere bei der Schlüsselpaarberechnung im RSA-Verfahren benötigte Berechnung des modularen Inversen b eines Wertes a zum Modul n.

1.1. Um die Parameter dieses Verfahrens, wenn es auf einem Prozessor ausgeführt wird, gegen Ausspähung durch Messung "physischer Parameter" zu schützen, etwa durch Analyse der Laufzeit oder des Stromverbrauchs, schlägt die Erfindung eine "maskierte" Berechnung vor: Die Eingangswerte a und n werden dabei mit Hilfe sogenannter Maskierungsparameter in "Hilfswerte" transformiert, das modulare Inverse als "Hilfsinverses" für diese Hilfswerte bestimmt, und das Hilfsinverse in das gewünschte modulare Inverse der Eingangswerte rücktransformiert.

1.2. Spezifisch schlägt die Erfindung vor, einen Maskierungswert r und einen Hilfsparameter s zu wählen und den Hilfswert β bzw. den Hilfsmodul δ als die Reste der (ganzzahligen) Division von ra bzw. sn durch n bzw. a (oder umgekehrt) zu bestimmen. Die Gleichungen, die zur Bestimmung von β und δ sowie des ursprünglich gesuchten modularen Inversen b zu lösen sind, nämlich

$$ra = \alpha n + \beta \quad \text{mit } 0 \leq \beta < n,$$
$$sn = \gamma a + \delta \quad \text{mit } 0 \leq \delta < a, \quad \text{und}$$
$$b = (\beta' r + \delta' \gamma) \bmod n \quad \text{mit } \delta' = (\beta\beta' - 1)/\delta, \quad \text{bzw.}$$

$$ra = \alpha n + \delta \quad \text{mit } 0 \leq \delta < n$$
$$sn = \gamma a + \beta \quad \text{mit } 0 \leq \beta < a, \quad \text{und}$$
$$b = -(\delta' r + \beta' \gamma) \bmod n \quad \text{mit } \delta' = (\beta\beta' - 1)/\delta,$$

werden nun, als Alternativen, obligatorisch beansprucht.

1.3. Darüber hinaus spezifiziert die beanspruchte Erfindung (vgl. Anspruch 1, Schritt a) bevorzugte, aber optionale Kriterien, nach denen r und s zu wählen sind.

Artikel 123 (2) EPÜ, sowie Artikel 83 und 84 EPÜ 1973

2. Die Änderungen gehen nicht über den Inhalt der Anmeldung in der ursprünglichen Fassung hinaus und entsprechen somit den Erfordernissen von Artikel 123 (2) EPÜ: Die genannten Gleichungen sind in den Ansprüchen 6-10 und auf Seiten 6, 9 und 10 (jeweils 2. Abs.), und die Kriterien gemäß Schritt a) des Anspruchs 1 in den ursprünglichen Ansprüchen 2 und 4 sowie auf Seite 5 (ebenfalls 2. Abs.) der ursprünglichen Anmeldung offenbart. RSA ist im ursprünglichen Anspruch 11 sowie an verschiedenen Stellen der Beschreibung offenbart, darunter auf Seite 1, die Ausführung des Verfahrens auf einem Prozessor ist etwa im ursprünglichen Anspruch 12 offenbart. Die Änderungen an der Beschreibung beschränken sich auf solche, die notwendig sind, die Beschreibung in Einklang mit den geänderten Ansprüchen zu bringen (Artikel 84 EPÜ 1973).

3. Die im Ladungszusatz erhobenen Einwände unter Artikel 83 und 84 EPÜ 1973 hatte die Kammer mit ihrer Einschätzung begründet, dass die Anmeldung genau eine mathematische Lösung des genannten Problems offenbare und dem Fachmann auch keinen Hinweis gebe, wie er alternative Lösungen finden könne, ohne erfinderisch tätig zu werden. Durch die Beschränkung der Ansprüche auf diese eine, offenbarte Lösung haben sich diese Einwände erübrigt.

4. Die Entscheidung erhebt in einem ***obiter dictum*** den Einwand unter Artikel 83 EPÜ 1973, die Formeln gemäß (damals anhängigen) Ansprüchen 7 und 8 würden unter der Annahme $\alpha=\gamma=0$ "nicht ... zur korrekten Inversen des Wertes a führen". Die nun beanspruchten Gleichungen und Nebenbedingungen haben, wie sich der Fachmann leicht überzeugt, unter der Annahme $\alpha=\gamma=0$ keine Lösung. Die Kammer ist somit der Ansicht, dass der Fachmann diese nicht ausdrücklich beanspruchte Nebenbedingung ohne Weiteres ergänzen würde, so dass ihr Fehlen keinen Offenbarungsmangel im Sinne von Artikel 83 EPÜ darstellt.

Artikel 56 EPÜ 1973

5. Die Entscheidung der Prüfungsabteilung (Punkt B.1.1) geht in ihrer Analyse von Dokument D4 aus, das beispielhaft die "ungeschützte direkte Inversionsberechnung ... zur Berechnung eines geheimen RSA-Schlüssels" offenbart. Die Kammer folgt dieser Wahl.

6. Über die Unterschiede zwischen Anspruch 1 und D4 und deren technische Wirkung eines Ausspähungsschutzes besteht Einigkeit zwischen der Entscheidung und der Beschwerdeführerin (vgl. Entscheidung, Punkt B.1.1; Beschwerdebegründung, S. 1).

6.1. Die Entscheidung argumentiert weiter, dass D5 die beanspruchte Lösung nahelegen würde. D5 befasse sich mit dem Ausspähungsschutz kryptografischer Algorithmen und offenbare ein Verfahren, demgemäß insbesondere eine multiplikative Inversion durch Maskierung geschützt würde. Von diesem sei das beanspruchte Maskierungsverfahren nur geringfügig und nicht erfinderisch unterschieden (Punkt B.1.2). Die Tatsache, dass es sich in D5 mit AES um ein

symmetrisches und nicht, wie gemäß der Anmeldung mit RSA um ein asymmetrisches Verschlüsselungsverfahren handele, sei unerheblich angesichts der Tatsache, dass die multiplikative Inversion in beiden Fällen eine "modulare" sei (Punkt B.1.2.1).

6.2. Der Beschwerdeführer bringt demgegenüber vor, dass die modulare Inversion bei symmetrischen Algorithmen wie AES keine Rolle spiele und dass sich daher der Fachmann, der sich mit asymmetrischer Kryptografie beschäftige, nicht auf dem Gebiet der symmetrischen Kryptografie nach Problemlösungen umsehen würde. Der Fachmann würde somit D4 und D5 nicht kombinieren (vgl. Beschwerdebegründung, S. 2, insbes. Abs. 2 und 6). Darüber hinaus habe die multiplikative Inversion "an sich" nichts mit der in der asymmetrischen Kryptografie verwendeten modularen Inversion zu tun, und die Entscheidung würde nicht im Einzelnen darlegen, in welcher Weise D5 die fehlenden Merkmale nach Anspruch 1 offenbaren würde (Beschwerdebegründung, S. 3, Abs. 2 und 3) und wie die Entscheidung zur Auffassung gelangt sei, dass A_{ij}^{-1} ein modulares Inverses sei, obgleich dieser Begriff in D5 gar nicht erwähnt würde.

7. Die Kammer ist der Ansicht, dass dem mit Kryptografie befassten Fachmann symmetrische und asymmetrische Verfahren gleichermaßen geläufig sind, und dass er daher routinemäßig in Betracht ziehen würde, Verbesserungen bei den einen für die anderen verfügbar zu machen.

7.1. Die Kammer stimmt der Beschwerdeführerin aber darin zu, dass sich der Fachmann auch der Unterschiede beider Verfahren (z. B. mathematischer Art) bewusst wäre und somit erkennen würde, dass sich manche Lösungen in einem Ge-

biet nicht - oder nicht ohne Weiteres - auf das andere übertragen lassen.

7.2. Zwischen der multiplikativen Inversion aus D5 und der modularen Inversion nach Anspruch 1 bestehen Ähnlichkeiten und Unterschiede.

7.3. Gemäß D5 ist die multiplikative Inversion in $GF(2^8)$ zu bestimmen. $GF(2^8)$ ist der Raum der Polynome höchstens 7. Grades mit Addition (+) und Multiplikation (*) von Polynomen wie üblich bis auf Reduktion der Koeffizienten modulo 2 und, was die Multiplikation angeht, Reduktion modulo eines irreduziblen Polynoms f vom Grad 8. In AES ist dieses Polynom konkret festgelegt (vgl. D5, S. 314, vorletzte Zeile). Das multiplikative Inverse eines Polynoms a zum Modul f ist dann ein Polynom b, so dass a (*) b = 1 (mod f), also ein "modular Inverses" zum Modul f.

7.4. Andererseits ist die Kammer der Ansicht, dass die multiplikative Inversion aus D5 (über $GF(2^8)$) und die modulare Inversion (über einem Ring ganzer Zahlen modulo n), wie sie für RSA benötigt wird, wegen der zugrundeliegenden Addition und Multiplikation soweit verschieden sind, dass eine Maskierung der einen Operation sich nicht in offensichtlicher, geschweige denn unmittelbarer Weise auf eine Maskierung der anderen Operation übertragen lässt.

7.5. Die Kammer stimmt somit der Beschwerdeführerin darin zu, dass der Fachmann ausgehend von D4 und auf der Suche nach einer Maskierung der für RSA benötigten modularen Inversion nicht in D5 nach einer Lösung suchen würde. Aber selbst eine hypothetische Kombination von D4 mit D5 würde den Fachmann nicht zur beanspruchten Erfindung

führen, da in der D5 die nun spezifisch beanspruchten Gleichungen weder offenbart noch nahegelegt werden.

7.6. Was D1 angeht, so folgt die Kammer der Ansicht der Beschwerdeführerin, dass der Fachmann zur Bestimmung eines ausspähungssicheren Verfahrens zur Bestimmung des modular Inversen für RSA nicht auf D1 zurückgreifen würde (vgl. Eingabe vom 26. Mai 2008, S.3, letzter Abs.). Da die vorliegenden Ansprüche nun auf RSA beschränkt sind, erübrigt sich somit eine detaillierte Analyse von D1.

7.7. Insgesamt kommt die Kammer zu dem Ergebnis, dass die vorliegenden Ansprüche 1-3 den erforderlichen erfinderischen Schritt gegenüber D4, D5 und D1 aufweisen, Artikel 56 EPÜ 1973.

Artikel 82 EPÜ 1973

8. Die in Schritt c) von Anspruch 1 beanspruchten Alternativen sind durch analoge Gleichungssysteme definiert (vgl. Punkt 1.2), deren erfinderische Tätigkeit gegenüber D1, D4 und D5 sich in gleicher Weise aus den voranstehenden Betrachtungen ergibt. Diese Gleichungen müssen damit als besondere technische Merkmale im Sinne der Regel 30 (1) EPÜ 1973 gelten, und stellen somit Einheitlichkeit der Erfindung gemäß Artikel 82 EPÜ 1973 innerhalb des Anspruchs 1 her, vgl. Regel 30 (2) EPÜ 1973.

Entscheidungsformel

Aus diesen Gründen wird entschieden:

1. Die Entscheidung 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, 8, 9 veröffentlichte Fassung
3-7, 10 eingereicht mit Schreiben vom 25. Juni 2012
Zeichnungen, Blatt
1 veröffentlichte Fassung
Ansprüche, Nr.
1-3 eingereicht mit Schreiben vom 25. Juni 2012

Die Geschäftsstellenbeamtin: Der Vorsitzende:

B. Atienza Vivancos D. H. Rees