



BUNDESPATENTGERICHT

17 W (pat) 317/06

(AktENZEICHEN)

Verkündet am
28. Januar 2010

...

BESCHLUSS

In der Einspruchssache

betreffend das Patent 103 40 411

...

...

hat der 17. Senat (Technischer Beschwerdesenat) des Bundespatentgerichts auf die mündliche Verhandlung vom 28. Januar 2010 unter Mitwirkung des Vorsitzenden Richters Dipl.-Phys. Dr. Fritsch, der Richterin Eder sowie des Richters Dipl.-Ing. Baumgardt und der Richterin Dipl.-Ing. Wickborn

beschlossen:

Das deutsche Patent 103 40 411 wird widerrufen.

Gründe

I.

Auf die am 2. September 2003 beim Deutschen Patent- und Markenamt eingegangene Patentanmeldung 103 40 411.2 - 53 wurde durch Beschluss der Prüfungsstelle für Klasse G 06 F das Patent unter der Bezeichnung

" Vorrichtung und Verfahren zur sicheren Ausführung eines Programms "

erteilt. Veröffentlichungstag der Patenterteilung ist der 13. Oktober 2005.

Gegen das Patent ist Einspruch erhoben worden. Die Einsprechende stützt den Einspruch auf neue und die in der Patentschrift zitierten Druckschriften und macht geltend, der Gegenstand der erteilten unabhängigen Ansprüche sei durch den Stand der Technik vorweggenommen oder zumindest nahegelegt; dies treffe unter der Berücksichtigung des allgemein bekannten Fachwissens ebenfalls für die Un-

teransprüche zu. Ferner gehe der Gegenstand des Patents über den Inhalt der ursprünglichen Anmeldung hinaus.

Sie hält ihre Argumentation auch gegenüber dem nunmehr geltenden Hauptantrag und den fünf Hilfsanträgen aufrecht und beantragt,

das Patent in vollem Umfang zu widerrufen.

Die Patentinhaberin verteidigt das Patent in beschränkter Fassung. Sie stellt den Antrag,

das Patent in beschränktem Umfang mit folgenden Unterlagen aufrechtzuerhalten:

gemäß **Hauptantrag** mit Patentansprüchen 1-12, überreicht in der mündlichen Verhandlung, noch anzupassender Beschreibung und Zeichnungen mit Figuren gemäß Patentschrift,

gemäß **erstem Hilfsantrag** mit Patentansprüchen 1-12, überreicht in der mündlichen Verhandlung, im Übrigen wie Hauptantrag,

gemäß **zweitem Hilfsantrag** mit Patentansprüchen 1-11, überreicht in der mündlichen Verhandlung, im Übrigen wie Hauptantrag,

gemäß **drittem Hilfsantrag** mit Patentansprüchen 1-11, überreicht in der mündlichen Verhandlung, im Übrigen wie Hauptantrag,

gemäß **viertem Hilfsantrag** mit Patentansprüchen 1-9, überreicht in der mündlichen Verhandlung, im Übrigen wie Hauptantrag,

gemäß **fünftem Hilfsantrag** mit Patentansprüchen 1-9, überreicht in der mündlichen Verhandlung, im Übrigen wie Hauptantrag.

Im Laufe des Einspruchsverfahren wurden insgesamt folgende Druckschriften als Stand der Technik in Betracht gezogen:

- D1** Hölscher, Holger: Microcomputers in safety technique: An aid to orientation for developer and manufacturer. TÜV Study Group on Computer Safety - München: Verlag TÜV Bayern; Köln: Verlag TÜV Rheinland, 1986, Umschlagseite, bibl. Kurztitelaufnahme, Seiten 7-91, 7-92, 8-4, 8-6; **ferner** (*überreicht in der mündlichen Verhandlung*) Seiten 7-86 bis 7-90
- D2** Kollmann, Karl: Chipkarten und Verbraucher. In: "ASA NEWS" der Austrian Smart Card Association, Nr. 4, Juni 1996, S. 1-20
- D3** „Anforderungen zur informationstechnischen Sicherheit bei Chipkarten“ des Bayerischen Landesbeauftragten für Datenschutz, Stand 02.12.1996; als Internet-Auszug gemäß http://www.datenschutz-bayern.de/technik/orient/akt_chip.htm
- D4** US 2003 / 131 210 A1
- D5** US 5 018 146 A
- D6** EP 1 305 708 B1
- D7** US 6 006 328 A
- D8** Ramamoorthy, C.V. et al.: Reliability and integrity of large computer programs. In: GFK-GI-GMR Fachtagung Prozessrechner 1974, Springer Verlag, Berlin / Heidelberg, S. 86 – 161, hier insbesondere Seiten 147 – 151 (siehe <http://www.springerlink.com/content/y507239287640828/fulltext.pdf>)

D9 Keim, G.: Die Erhöhung der Sicherheit von Mikrocomputersystemen. In: Angewandte Informatik 2/80, S. 45 - 50

D10 EP 1 161 725 B1

In der Fassung gemäß **Hauptantrag** lauten die unabhängigen Patentansprüche 1, 11 und 12, hier mit der Gliederung der Einsprechenden und mit einer kursiven Kennzeichnung der Änderungen gegenüber der erteilten Fassung versehen:

- "1. Vorrichtung (202; 302; 402) zur sicheren Ausführung eines Programms, das eine Sequenz (100) von Programm-Befehlen umfasst,
- (a) wobei die Programm-Befehle Nutzbefehle (110, 112, 114, 116) und Überprüfungsbefehle (120, 122, 124) umfassen,
 - (b) wobei die Überprüfungsbefehle zwischen den Nutzbefehlen angeordnet sind,
 - (b1) so dass gemäß einem spezifizierten Ausführungspfad des Programms eine Reihenfolge der Ausführung der Überprüfungsbefehle festgelegt ist,

mit folgenden Merkmalen:

- (c) einer Einrichtung (203; 303; 403) zum Ausführen der Sequenz von Programm-Befehlen,
- (c1) wobei die Einrichtung zum Ausführen ausgebildet ist, um beim Ausführen eines Überprüfungsbefehls, gemäß einer Erstellungsvorschrift einen Überprüfungswert (130, 132, 134; 230; 330; 430) zu erzeugen;

- (d) einer Einrichtung (205; 512) zum separaten Bereitstellen eines Kontrollwertes (250; 550) ***nebenläufig zur Ausführung des Programms***,
 - (d1) wobei der Kontrollwert gemäß der Erstellungsvorschrift von einem vorangegangenen Kontrollwert abgeleitet ist;
 - (e) einer Einrichtung (206; 514) zum Vergleichen des Überprüfungswertes mit dem Kontrollwert ***nebenläufig zur Ausführung des Programms***; und
 - (f) einer Einrichtung (207; 514) zum Liefern eines Hinweises (262; 562) auf eine Störung der Ausführung des spezifizierten Ausführungspfades des Programms, bei Nichtübereinstimmung des Überprüfungswertes und des Kontrollwertes.
11. Verfahren zur sicheren Ausführung eines Programms, das eine Sequenz von Programm-Befehlen umfasst,
- (a) wobei die Programm-Befehle Nutzbefehle und Überprüfungsbefehle umfassen,
 - (b) wobei die Überprüfungsbefehle zwischen den Nutzbefehlen angeordnet sind,
 - (b1) so dass gemäß einem spezifizierten Ausführungspfades des Programms eine Reihenfolge der Ausführung der Überprüfungsbefehle festgelegt ist,

wobei das Verfahren folgende Schritte umfasst:

- (c) a) Ausführen der Sequenz von Programm-Befehlen,
 - (c1) wobei beim Ausführen eines Überprüfungsbefehls gemäß einer Erstellungsvorschrift ein Überprüfungswert erzeugt wird;
 - (d) b) Separates Bereitstellen eines Kontrollwertes ***nebenläufig zur Ausführung des Programms***,
 - (d1) wobei der Kontrollwert gemäß der Erstellungsvorschrift von einem vorangegangenen Kontrollwert abgeleitet ist;
 - (e) c) Vergleichen des Überprüfungswertes mit dem Kontrollwert ***nebenläufig zur Ausführung des Programms***; und
 - (f) d) Liefern eines Hinweises auf eine Störung der Ausführung des spezifizierten Ausführungspfad des Programms, bei Nichtübereinstimmung des Überprüfungswertes und des Kontrollwertes.
- 12. *Maschinen-lesbaren Träger, auf dem ein*** Computer-Programm mit einem Programmcode zur Durchführung des Verfahrens gemäß Anspruch 11 ***gespeichert ist.*** ”

Wegen der Unteransprüche wird auf die Akten verwiesen.

Die Fassung nach dem **ersten Hilfsantrag** unterscheidet sich davon durch folgendes geändertes Merkmal (identisch in den Patentansprüchen 1 und 11):

(d1*) wobei der Kontrollwert gemäß der Erstellungsvorschrift **unabhängig von Nutzbefehlen zwischen dem Überprüfungsbeehl und einem vorhergehenden Überprüfungsbeehl** von einem vorangegangenen Kontrollwert abgeleitet ist;

(im Übrigen wie Hauptantrag).

Der **zweite Hilfsantrag** beruht auf dem **Hauptantrag** (d. h. Merkmal **(d1)** ist unverändert), mit folgendem zusätzlichem Merkmal am Ende des Patentanspruchs 1:

(g) wobei die Einrichtung (205; 512) zum separaten Bereitstellen des Kontrollwertes (250; 550), die Einrichtung (206; 514) zum Vergleichen und die Einrichtung (207; 514) zum Liefern eines Hinweises (262; 562) in Hardware separat von der Einrichtung zum Ausführen der Sequenz von Programm-Befehlen ausgeführt sind.

und entsprechend am Ende des Patentanspruchs 11:

(g) wobei das separate Bereitstellen des Kontrollwertes (250; 550), das Vergleichen und das Liefern eines Hinweises (262; 562) in einer Hardware separat von der Einrichtung zum Ausführen der Sequenz von Programm-Befehlen ausgeführt werden.

Der nebengeordnete Patentanspruch 12 ist weggefallen.

Die Fassung nach dem **dritten Hilfsantrag** beruht auf dem zweiten Hilfsantrag, enthält jedoch in den Patentansprüchen 1 und 11 statt des Merkmals **(d1)** das

entsprechend dem ersten Hilfsantrag geänderte Merkmal **(d1*)**; der nebengeordnete Patentanspruch 12 fällt ebenfalls weg.

Der **vierte Hilfsantrag** beruht wieder auf dem **Hauptantrag** (d.h. Merkmal **(d1)** ist unverändert), mit folgenden zusätzlichen Merkmalen am Ende des Patentanspruchs 1:

- (g*)** wobei die Einrichtung zum separaten Bereitstellen eines Kontrollwertes ein Register (510) und einen Vorwärtszähler (512) aufweist, um ansprechend auf einen Überprüfungswert einen vorangegangenen Kontrollwert (550) zu erhöhen, um einen nachfolgenden Kontrollwert (551) zu erzeugen, oder
- (h)** wobei die Einrichtung zum Erzeugen eines Kontrollwertes einen Pseudo-Zufallszahlengenerator aufweist, der ansprechend auf einen Überprüfungswert einen nächsten Kontrollwert aus einem vorangegangenen Kontrollwert erzeugt.

Die Unteransprüche 7 und 8 (des Hauptantrages) sind gestrichen, der Nebenanspruch trägt daher die Nummer 9, und er ist entsprechend dem Hauptanspruch am Ende ergänzt:

- (g*)** wobei der Kontrollwert unter Verwendung eines Registers (510) und eines Vorwärtszähler (512) erzeugt wird, um ansprechend auf einen Überprüfungswert einen vorangegangenen Kontrollwert (550) zu erhöhen, um einen nachfolgenden Kontrollwert (551) zu erzeugen, oder
- (h)** wobei der Kontrollwert unter Verwendung einen Pseudo-Zufallszahlengenerators erzeugt wird, der ansprechend auf

einen Überprüfungswert einen nächsten Kontrollwert aus einem vorangegangenen Kontrollwert erzeugt.

Der nebengeordnete Patentanspruch 12 fällt ebenfalls weg.

Die Fassung nach dem **fünften Hilfsantrag** entspricht der des vierten Hilfsantrags, wobei jedoch das Merkmal (**g***) in den Patentansprüchen 1 und 9 ersatzlos gestrichen ist.

Im Übrigen wird auf die Akte verwiesen.

Als zugrundeliegende **Aufgabe** ist angegeben, eine Vorrichtung sowie ein Verfahren zur sicheren Ausführung eines Programms zu schaffen, die einen flexiblen, einfach und kostengünstig zu realisierenden sowie wirksamen Schutz der Ausführung des Programms ermöglichen (siehe Patentschrift Absatz [0011]).

II.

Der Einspruch wurde frist- und formgerecht erhoben, er ist mit nachprüfbaren Gründen versehen und auch sonst zulässig.

Er hat auch Erfolg, da sich der jeweilige Gegenstand der unabhängigen Patentansprüche nach Hauptantrag und nach allen fünf Hilfsanträgen als nicht patentfähig erweist.

1. Das Streitpatent betrifft Maßnahmen zur Erkennung einer Veränderung des vorgesehenen Programmlaufs eines Computerprogramms, beispielsweise verursacht durch einen Angreifer, der eine Schutzroutine des Programms durch gezielte Einflussnahme „überspringen“ möchte. In der Beschreibungseinleitung ist ausgeführt, dass insbesondere bei Chipkarten die Gefahr bekannt sei, durch elektri-

sche Störimpulse den Programm-Befehlszähler auf eine vom Entwickler nicht vorgesehene Weise zu verändern, so dass der Chipkarten-Controller danach die Programm-Ausführung an einer „falschen“ Stelle fortsetzt. Dadurch könnte es möglich sein, gezielt einzelne Programmabschnitte wie den Authentisierungsprozess, der die Chipkarte vor einem Zugriff Unbefugter schützt, zu umgehen (siehe Streitpatentschrift Absätze [0002], [0003]).

Das Streitpatent schlägt als Gegenmaßnahme vor, in den aus „Nutzbefehlen“ bestehenden Programmcode in beliebiger Häufigkeit besondere „Überprüfungsbefehle“ einzufügen, welche bei ihrer Ausführung gemäß einer vorgegebenen Erstellungsvorschrift (in der vorgesehenen Reihenfolge) Überprüfungswerte erzeugen. Parallel dazu werden separat nach derselben Erstellungsvorschrift Kontrollwerte bereitgestellt, die von dem jeweils vorangegangenen Kontrollwert abgeleitet sind, und mit dem aktuellen Überprüfungswert verglichen; bei fehlender Übereinstimmung wird ein Hinweis auf die damit entdeckte gestörte Ausführungs-Reihenfolge der Programmbefehle geliefert.

Als **Fachmann** für eine Verbesserung der Absicherung des Programmablaufs gegen Angriffe sieht der Senat einen Entwicklungsingenieur für mit Mikroprozessoren oder -controllern arbeitende Einrichtungen, insbesondere Chipkarten, mit Hochschul- oder Fachhochschulausbildung an.

2. Es kann dahinstehen, ob – wie die Einsprechende geltend macht – der Gegenstand des erteilten Patents oder der nunmehr geltenden Patentansprüche über den Inhalt der ursprünglich eingereichten Anmeldung hinausgeht; ebenfalls kann offenbleiben, inwieweit ein auf ein „Computer-Programm“ gerichteter Patentanspruch zulässig ist (und wie er nach Patenterteilung ohne Schutzbereichserweiterung noch geändert werden könnte). Denn hinsichtlich der gesetzlichen Patentierungsvoraussetzungen und Patentierungsausschlüsse muss keine bestimmte Prüfungsreihenfolge eingehalten werden (BGH BIPMZ 2004, 428 „Elektronischer Zahlungsverkehr“ II. 4.).

Im vorliegenden Fall ist das erteilte Patent schon deshalb zu widerrufen, weil der Gegenstand des Patentanspruchs 1 nach Hauptantrag ebenso wie nach dem ersten bis fünften Hilfsantrag zumindest nicht auf einer erfinderischen Tätigkeit beruht.

2.1 Zum Hauptantrag

2.1.1 Von den im Verfahren befindlichen Druckschriften ist von besonderem Interesse die in der von der Einsprechenden entgegengehaltenen **D1** als **/RCK/** zitierte, vom Senat nachträglich benannte Literaturstelle:

D8 Ramamoorthy, C.V. et al.: Reliability and integrity of large computer programs. In: GFK-GI-GMR Fachtagung Prozessrechner 1974, Springer Verlag, Berlin / Heidelberg, S. 86 – 161, hier insbesondere Seiten 147 – 151 (siehe <http://www.springerlink.com/content/y507239287640828/fulltext.pdf>)

Sie beschreibt im Kapitel 4.3.2.2 (Seiten 147 – 151) ein Verfahren (und, auf den das Verfahren nutzenden Rechner bezogen, implizit auch eine Vorrichtung) zur sicheren Ausführung einer Sequenz von Programm-Befehlen, welches eine Störung in der festgelegten Ausführungsreihenfolge erkennt [*Gattungsbegriff, Merkmal (c)*]. Gemäß Seite 148 / Figur 25 sind Überprüfungsbefehle (checkpoints) zwischen den Nutzbefehlen (normal program / CODES) angeordnet [*Merkmale (a), (b), (b1)*]. Jeder Überprüfungsbefehl vergleicht den Inhalt einer vorbestimmten, der jeweiligen Programm-Sequenz zugeordneten Speicherzelle (im Sinne eines „Kontrollwerts“ – *Merkmal (d)*) mit einem Überprüfungswert [*Merkmal (e)*], der fest in den Überprüfungsbefehl eingefügt ist (vgl. Streitpatent Absatz [0033] Zeile 1-9 – *Merkmal (c1)*). Bei Nicht-Übereinstimmung bricht das Programm ab („a trap routine is invoked“ – *Merkmal (f)*), bei Übereinstimmung wird der Inhalt geändert und die der nächsten Programm-Sequenz zugeordnete Speicherzelle mit einem neuen Kontrollwert beschrieben, welcher dann wiederum am Ende der

Sequenz verglichen und geändert wird.

Bei der praktisch implementierten Ausführungsform gemäß **Figur 27** ist eine Tabelle (KODE(IXn)) vorgesehen, die zahlreiche Einträge enthält, welche als Kontrollwerte verwendet werden können. Gemäß Flussdiagramm wird zuerst Eintrag Nummer 5 auf den Wert 123 („Kontrollwert“) gesetzt, der Index hingegen zeigt auf Eintrag Nummer 9. Im Laufe der Programm-Abarbeitung wird der Index verändert, so dass er bei ordnungsgemäßer Programmdurchführung am Ende auf den Eintrag Nummer 5 zeigt, und dann der Tabelleninhalt am angezeigten Eintrag mit dem Kontrollwert 123 verglichen (wenn hingegen ein Teil des Programms nicht ausgeführt wurde, würde der Index nicht auf Eintrag Nummer 5 zeigen und somit keine Übereinstimmung bestehen). Anschließend wird aus dem alten Kontrollwert (im Flussdiagramm: $KODE(5) = 123$) ein neuer Kontrollwert ($KODE(3) \leftarrow KODE(5)$ minus 26) berechnet, d. h. der nächste Kontrollwert wird gemäß einer Erstellungsverfahren von einem vorangegangenen Kontrollwert abgeleitet [*Merkmal (d1)*].

Damit ist der Gegenstand des erteilten Patentanspruchs 1 und des ihm nebengeordneten Anspruchs 11 durch **D8** vorweggenommen.

2.1.2 Demgegenüber wird das Patent nunmehr in beschränkter Fassung verteidigt: das separate Bereitstellen eines Kontrollwertes (Merkmal **(d)**) und das Vergleichen des Überprüfungswertes mit dem Kontrollwert (Merkmal **(e)**) sollen jeweils „**nebenläufig zur Ausführung des Programms**“ durchgeführt werden. (Gemäß Hauptantrag stellen diese beiden Zusätze die einzige Beschränkung dar.)

Eine entsprechende Offenbarung findet sich in den Absätzen [0029] und [0039] der Streitpatentschrift, die Formulierung ist daher insoweit zulässig.

Der Begriff „nebenläufig“ ist im Streitpatent allerdings nicht näher erläutert oder gar definiert. In der mündlichen Verhandlung hat die Patentinhaberin ausgeführt, dass hier „unabhängig von der Ausführung des Programms“ gemeint sei: das Be-

reitstellen eines Kontrollwertes und das Vergleichen mit dem Überprüfungswert solle neben der Ausführung der Nutzbefehle herlaufen, den Programmablauf nicht unterbrechen oder stören. Eine solche Maßnahme stelle einen deutlichen Unterschied zur Lehre der **D8** dar, denn dort werde beides mitten im Programm ausgeführt und unterbreche den normalen Programmablauf.

Dem ist entgegenzuhalten, dass der Begriff „nebenläufig“ wenig trennscharf, vielmehr sehr breit angelegt ist. Schon wenn, ausgehend von **D8**, die Kontrollwert-Bereitstellung und der Vergleich mit dem Überprüfungswert in ein Unterprogramm ausgelagert würden, wie es beim strukturierten Programmieren üblich ist, könnte dessen Ausführung als „nebenläufig“ zum Hauptprogramm verstanden werden. Somit wäre durch eine einfache, programmierer-typische Maßnahme, angewendet auf die Lehre der **D8**, der Gegenstand des Patentanspruchs 1 nach Hauptantrag bereits erreicht.

Unabhängig davon war es dem Fachmann zum Anmeldezeitpunkt des Streitpatents seit langem vertraut, die Sicherstellung eines ungestörten Programmablaufs nicht allein einer Software zu überlassen.

Beispielsweise wird auf Seite 7-88 der **D1** ein Zähler vorgeschlagen, dessen Zählerstand an bestimmten Stellen im Programmablauf hochgezählt und später mit einem Kontrollwert verglichen wird. Der Zähler kann in Software ausgeführt sein oder als Hardware-Zähler, außerhalb des Systems (siehe 7.34.1 Absatz 2). Auch in **D9** Seite 45, rechte Spalte Absatz 1 / Absatz 5, wird empfohlen, Hardware und Software zur gegenseitigen Überprüfung einzusetzen, um die Sicherheit eines Mikrocomputersystems zu erhöhen.

Schließlich beschreibt **D10** eine Vorrichtung und ein Verfahren zur sicheren Ausführung eines Programms, bei dem die Abfolge der Programmbefehle überwacht wird. In einem Vorbereitungsschritt wird für die Befehle eines bestimmten zu überwachenden Programmblocks (unter Berücksichtigung ihrer Reihenfolge) ein Hash-

Wert gebildet und im Programm abgespeichert. Bei Ausführung des Programms startet ein erster Überwachungsbefehl die Überprüfung des folgenden Befehlsblocks („Nutzbefehle“), wobei jeder einzelne Befehl **nebenläufig zum Programm in einer separaten Schaltung** (Figur 2: Unité Surveillance 22) mitgelesen und zur Hash-Wert-Bildung benutzt wird; ein zweiter Überwachungsbefehl beendet diese Phase und veranlasst, dass der aus den einzelnen Befehlen (unter Berücksichtigung ihrer Reihenfolge) gebildete Hash-Wert mit dem vorab gespeicherten Hash-Wert verglichen wird, und zwar in der separaten Unité Surveillance, getrennt vom eigentlichen Programmablauf, vgl. **D10** (EP 1 161 725 B1) Absatz [0053] / [0054].

Es lag für den Fachmann daher schon aufgrund seines allgemeinen Fachwissens (hier beispielhaft belegt durch Auszüge aus **D1**, **D9** und **D10**) nahe, zur Erhöhung der Sicherheit die Einrichtungen zur Bereitstellung der Kontrollwerte und zum Vergleich mit den Überprüfungswerten, die aus **D8** bekannt ist, separat in Hardware auszuführen; allein dadurch erfolgen dann die Bereitstellung und der Vergleich „nebenläufig zur Ausführung des Programms“, wie es in der geltenden Antragsfassung beansprucht wird.

Somit bedurfte es für eine Ausführung der Maßnahmen **(d)** und **(e)** „nebenläufig zur Ausführung des Programms“ keiner erfinderischen Tätigkeit. Der Hauptantrag kann daher keinen Bestand haben.

2.2 Zum ersten Hilfsantrag

Auch der erste Hilfsantrag kann keinen Erfolg haben. Er unterscheidet sich vom Hauptantrag lediglich durch folgende Formulierung des Merkmals **(d1)** in den Patentansprüchen 1 und 11 (Ergänzung kursiv dargestellt):

(d1*)wobei der Kontrollwert gemäß der Erstellungsvorschrift ***unabhängig von Nutzbefehlen zwischen dem Überprüfungs-***
befehl und einem vorhergehenden Überprüfungs-

befehl von einem vorangegangenen Kontrollwert abgeleitet ist.

Das Bestimmen des Kontrollwertes unterscheidet sich dadurch zwar, wie die Patentinhaberin vorträgt, von der Art der Kontrollwert-Bestimmung gemäß **D10**, wo jeder einzelne Nutzbefehl zur Bildung eines Hash-Wertes einbezogen wird; nicht jedoch von der Art der Kontrollwert-Bestimmung gemäß **D8**, bei welcher ein neuer Kontrollwert (s. o.: $KODE(3) \leftarrow KODE(5) \text{ minus } 26$) unabhängig von Nutzbefehlen allein durch eine arithmetische Operation aus einem vorangegangenen Kontrollwert abgeleitet wird.

Somit ergibt sich der Gegenstand der Patentansprüche 1 und 11 nach dem ersten Hilfsantrag für den Fachmann genauso aus **D8** und seinem allgemeinen Fachwissen, wie es bezüglich des Hauptantrags dargestellt wurde.

2.3 Zum zweiten Hilfsantrag

Der zweite Hilfsantrag führt ebenfalls nicht weiter. Er ist gekennzeichnet durch ein zusätzliches Merkmal in den unabhängigen Ansprüchen, das beim Anspruch 1 lautet:

- (g) wobei die Einrichtung (205; 512) zum separaten Bereitstellen des Kontrollwertes (250; 550), die Einrichtung (206; 514) zum Vergleichen und die Einrichtung (207; 514) zum Liefern eines Hinweises (262; 562) in Hardware separat von der Einrichtung zum Ausführen der Sequenz von Programmbefehlen ausgeführt sind.

Wie bereits beim Hauptantrag erläutert, lag eine Ausführung in Hardware für den Fachmann nahe. Beispielsweise **D10** zeigt explizit eine separate Schaltung (Figur 2: Unité Surveillance 22) zur Bereitstellung des Kontrollwertes (Hash-Wert),

zum Vergleichen mit dem Überprüfungswert (siehe Absatz [0074]) und zum Liefern eines Hinweises (siehe Absatz [0078]). Das genannte zusätzliche Merkmal **(g)** kann das Vorliegen einer erfinderische Tätigkeit daher nicht begründen.

2.4 Zum dritten Hilfsantrag

Der dritte Hilfsantrag enthält gegenüber dem zweiten Hilfsantrag in den Patentansprüchen 1 und 11 statt des Merkmals **(d1)** das Merkmal **(d1*)** entsprechend dem ersten Hilfsantrag. Dieses ist aber, wie dargelegt, aus **D8** bekannt und kann das Vorliegen einer erfinderische Tätigkeit nicht begründen, so dass auch der dritte Hilfsantrag erfolglos bleiben muss.

2.5 Zum vierten Hilfsantrag

Gemäß viertem Hilfsantrag ist der Patentanspruch 1 nach Hauptantrag am Ende um folgende Merkmale ergänzt:

- (g*)** wobei die Einrichtung zum separaten Bereitstellen eines Kontrollwertes ein Register (510) und einen Vorwärtszähler (512) aufweist, um ansprechend auf einen Überprüfungswert einen vorangegangenen Kontrollwert (550) zu erhöhen, um einen nachfolgenden Kontrollwert (551) zu erzeugen, **oder**
- (h)** wobei die Einrichtung zum Erzeugen eines Kontrollwertes einen Pseudo-Zufallszahlengenerator aufweist, der ansprechend auf einen Überprüfungswert einen nächsten Kontrollwert aus einem vorangegangenen Kontrollwert erzeugt.

Der nebengeordnete Patentanspruch 9 ist in analoger Weise eingeschränkt.

Die beiden zusätzlichen Merkmale sind (durch das „oder“ am Ende von Merkmal **(g*)**) als Alternativen beansprucht. Sie entsprechen den erteilten Unteransprüchen 7 und 8, die Anspruchsfassung ist daher insoweit zulässig.

Doch bereits die Untersuchung der ersten Alternative zeigt, dass der Antrag keinen Erfolg haben kann.

Denn aus der Seite 7-88 der **D1** ist es als Maßnahme zur Überwachung des Befehls-Ablaufes eines Computer-Programms bekannt, einen Zähler einzusetzen, der in Hardware ausgeführt sein kann und durch zwischengeschaltete Befehle des Programms weiterzählt („hardware counter external to the system, which e.g. is incremented as a result of an output command“). Am Ende muss der Zähler einen bestimmten, bei der Programmerstellung berechneten Wert haben („which must - at the end of the run through of the program - have some defined value, which is computed at the time when the program is set up“); dieser vorberechnete Wert („Überprüfungswert“) wird mit dem Zählerstand („Kontrollwert“) verglichen, und bei Nicht-Übereinstimmung wird eine Fehlermeldung erzeugt („if the value is incorrect ... a fault message is produced“). Offensichtlich sind hier somit sämtliche Merkmale des erteilten Patentanspruchs 1 vorbeschrieben.

Wie beim Hauptantrag bereits dargelegt, arbeitet dieser Zähler, zumindest wenn er in Hardware ausgeführt ist, „nebenläufig zur Ausführung des Programms“. Er erhöht bei jedem zwischengeschalteten Befehl des Programms den Zählerstand („Vorwärtszähler“), um so auch nachfolgende Kontrollwerte zu erzeugen. Dass zum Vergleichen ein „Register“ für den vom Programm gelieferten Überprüfungswert nötig ist, ist für den Fachmann ganz selbstverständlich. Damit sind die zusätzlichen Merkmale aus **D1** ebenfalls vorbekannt oder lassen sich daraus ableiten.

Sonach ergibt sich eine der nach viertem Hilfsantrag beanspruchten Alternativen (Merkmale **(a)** bis **(g*)**) für den Fachmann aufgrund seines Fachwissens allein aus Seite 7-88 der **D1**.

2.5 Zum fünften Hilfsantrag

Der fünfte Hilfsantrag beschränkt sich auf die zweite Alternative des vierten Hilfsantrags (Merkmal **(g*)** einschl. „oder“ ist gestrichen).

Doch auch das verbliebene Merkmal **(h)**, wonach zum Erzeugen eines Kontrollwertes ein Pseudo-Zufallszahlengenerator einzusetzen ist, überschreitet nicht den Rahmen des Wissens und Könnens des Durchschnittsfachmanns, so dass auch dieser Hilfsantrag keinen Erfolg hat:

Gemäß Absatz [0033] der Streitpatentschrift wird der Einsatz des Pseudo-Zufallszahlengenerators „bei erhöhten Sicherheitsanforderungen“ empfohlen, wobei „nachfolgende Überprüfungswerte als Pseudo-Zufallszahlensequenz erzeugt“ werden. „Die Nutzung eines Pseudo-Zufallszahlengenerators erhöht die Sicherheit, wenn eine sehr hohe Zahl von Überprüfungswerten benötigt wird“ (Absatz [0047]).

Es ist demnach klar, dass nicht nur die Kontrollwerte, sondern genauso die Überprüfungswerte durch den beanspruchten Pseudo-Zufallszahlengenerator erzeugt werden müssen (vgl. Anspruchsmerkmal **(c1)** mit Merkmal **(d1)** – als „Erstellungsvorschrift“ wird sozusagen die in den Pseudo-(!) Zufallszahlengenerator fest implementierte Erzeugungsregel benutzt).

Das zugrundeliegende objektive (Teil-) Problem bestand also darin, für eine große Zahl benötigter unterschiedlicher Überprüfungswerte eine möglichst zufällig erscheinende Folge von Zahlenwerten bereitzustellen, die aber dennoch reproduzierbar ist; d. h. die „Erstellungsvorschrift“ der Merkmale **(c1)** und **(d1)** sollte einerseits scheinbar zufällige Werte liefern, andererseits an zwei verschiedenen Stellen

(beim Ausführen eines Überprüfungsbefehls und separat davon beim Bereitstellen eines Kontrollwertes) unter gleichen Ausgangsbedingungen denselben Wert ausgeben.

Zum Zeitpunkt der Anmeldung des Streitpatents waren Pseudo-Zufallszahlengeneratoren allerdings, insbesondere im Umfeld des Schutzes von Chipkarten durch kryptographische Maßnahmen, allgemein bekannt und darum das „Mittel der Wahl“ für den Durchschnittsfachmann, wenn er viele unterschiedliche Werte in einer scheinbar zufälligen Zahlenfolge benötigte, die aber dennoch reproduzierbar sein sollten. Deshalb ist es als rein fachmännisches Handeln zu bewerten, zum parallelen Erzeugen der Kontroll- und Überprüfungswerte einen Pseudo-Zufallszahlengenerator auszuwählen; eine erfinderische Leistung kann der Senat darin nicht sehen.

III.

Nachdem keiner der gestellten Anträge einen Hauptanspruch umfasste, dessen Gegenstand auf erfinderischer Tätigkeit beruht, war das Streitpatent zu widerrufen.

Dr. Fritsch

Eder

Baumgardt

Wickborn

Me