BUNDESPATENTGERICHT

20 W (pat) 327/04

(Aktenzeichen)

Verkündet am
2. Juli 2008
…

B E S C H L U S S

In der Einspruchssache

…

betreffend das Patent 101 62 496

…

hat der 20. Senat (Technischer Beschwerdesenat) des Bundespatentgerichts auf die mündliche Verhandlung vom 2. Juli 2008 durch den Vorsitzenden Richter Dipl.-Phys. Dr. Bastian, den Richter Dipl.-Phys. Dr. Hartung sowie die Richterin Martens und den Richter Dipl.-Ing. Kleinschmidt

beschlossen:

Das Patent wird mit neuen Patentansprüchen 1 und 14 sowie geänderter Patentschrift (Absatz [0035]), jeweils überreicht in der mündlichen Verhandlung, im Übrigen mit den erteilten Unterlagen, beschränkt aufrechterhalten.

G r ü n d e

I

Die Einsprechende macht mangelnde Patentfähigkeit geltend und stützt ihren Einspruch auf folgende Druckschriften

D6 F. Bao, R. H. Deng. Y. Han, A. Jeng, A. D. Narasimhalu, T. Ngair: "Breaking public key cryptosystems on tamper resistant devices in the presence of transient faults", in: Proceedings of the 5th Workshop on Secure Protocols, LNCS 1361, Springer-Verlag, Seiten 115-124, Paris, 7. bis 9. April 1997,

D7 D. Boneh, R. A. DeMillo, R. J. Lipton: "On the Importance of Checking Cryptographic Protocols for Faults", in: Advances in Cryptology, proceedings of EUROCRYPT '97, Seiten 37 bis 51, 1997;

D8 V. Klima und T. Rosa: "Attack on Private Signature Keys of the OpenPGP format", PGP™ program and other applications compatible with OpenPGP, 22. März 2001;

D9 EP 0 621 569 B1,

D10 Rankl/Effing, Handbuch der Chipkarten, 3. Auflage, Carl Hanser Verlag München Wien, 1999, insb. S. 138.

Kursorisch verweist die Einsprechende außerdem auf die im Prüfungsverfahren genannten Druckschriften

D1 DE 199 61 838 A1,

D2 DE 197 25 167 A1,

D3 DE 42 34 165 C1,

D4 EP 0 743 744 A2 und

D5 US 6 092 229.

Die Einsprechende stellt den Antrag,

das Patent zu widerrufen.

Die Patentinhaberin stellt den Antrag,

das Patent mit neuen Patentansprüchen 1 und 14 sowie geänderter Patentschrift (Absatz [0035]), jeweils überreicht in der mündlichen Verhandlung, im Übrigen mit den erteilten Unterlagen, beschränkt aufrechtzuerhalten.

Die in der mündlichen Verhandlung überreichten Patentansprüche 1 und 14 lauten (Gliederungszeichen a bis f in Patentanspruch 1 hinzugefügt):

"1. a) Verfahren zum Absichern einer Berechnung in einem kryptographischen Algorithmus, wobei die Berechnung Eingangsdaten erhält, um Ausgangsdaten zu erzeugen, mit folgenden Schritten:

b) Bereitstellen (10) der Eingangsdaten für die Berechnung;

c) Durchführen (12) der Berechnung, um die Ausgangsdaten der Berechnung zu erhalten;

d) nach dem Durchführen der Berechnung,

d1) Überprüfen (14), ob die Eingangsdaten während der Berechnung verändert wurden,

d2) unter Verwendung eines Überprüfungsalgorithmus, der sich von der Berechnung unterscheidet,

d3) ohne Verwendung der Ausgangsdaten; und

e) falls das Überprüfen (14) ergibt, dass die Eingangsdaten während der Berechnung verändert wurden,

f) Unterdrücken (16) einer Weitergabe der Ausgangsdaten der Berechnung."

"14. Vorrichtung ausgebildet zum Absichern einer Berechnung in einem kryptographischen Algorithmus, wobei die Berechnung Eingangsdaten erhält, um Ausgangsdaten zu erzeugen, mit folgenden Merkmalen:

einer Einrichtung ausgebildet zum Bereitstellen (10) der Eingangsdaten für die Berechnung;

einer Einrichtung ausgebildet zum Durchführen (12) der Berechnung, um die Ausgangsdaten der Berechnung zu erhalten;

einer Einrichtung ausgebildet zum Überprüfen (14), ob die Eingangsdaten während der Berechnung verändert wurden, unter Verwendung eines Überprüfungsalgorithmus, der sich von der Berechnung unterscheidet, ohne Verwendung der Ausgangsdaten; wobei die Einrichtung zum Überprüfen ausgebildet ist, um die Überprüfung durchzuführen, nachdem die Berechnung durchgeführt worden ist; und
einer Einrichtung ausgebildet zum Unterdrücken (16) einer Weitergabe der Ausgangsdaten, falls die Einrichtung zum Überprüfen (14) ermittelt, dass die Eingangsdaten während der Berechnung verändert wurden."

Zum Wortlaut der Patentansprüche 2 bis 13 wird auf die Akte verwiesen.

Die Patentinhaberin ist der Auffassung, die mit den neu vorgelegten Patentansprüchen 1 und 14 beanspruchten Gegenstände seien gegenüber dem mit den vorgenannten Druckschriften belegten Stand der Technik patentfähig. Sie macht außerdem geltend, dass die Druckschrift D8 nicht vorveröffentlicht sei, nachdem in einer Fußnote angegeben ist, dass die Referenzen am 17. Juni 2002, mithin nach dem Prioritätstag des Streitpatents (17. Oktober 2001) geringfügig geändert worden seien.

Nach Auffassung der Einsprechenden beruhen die Gegenstände der geltenden Patentansprüche 1 und 14 gegenüber dem vorliegenden Stand der Technik zumindest nicht auf einer erfinderischen Tätigkeit. Des Weiteren führt die Einsprechende aus, dass insbesondere das im geltenden Patentanspruch 1 unter dem Gliederungszeichen d3 hinzugefügte Merkmal "ohne Verwendung der Ausgangsdaten" den Unterlagen des Streitpatents nicht als zur Erfindung gehörend entnehmbar sei.

II

Der Einspruch führt zur beschränkten Aufrechterhaltung des Patents.

1. Die geltenden Patentansprüche 1 bis 14 sind zulässig. Die Merkmale der erteilten Ansprüche sind den ursprünglich eingereichten Unterlagen als zur Erfindung gehörend entnehmbar, vgl. die ursprünglich eingereichten Ansprüche 1 bis 14. Des Weiteren sind die Gegenstände der erteilten Patentansprüche 1 und 14 durch die in der mündlichen Verhandlung vorgelegten Ansprüche 1 und 14 zulässig beschränkt worden, indem das Überprüfen, ob die Eingangsdaten während der Berechnung verändert wurden, insbesondere "ohne Verwendung der Ausgangsdaten" erfolgt. Das beschränkende Merkmal ist vom zuständigen Fachmann, einem Informatiker mit Hochschulausbildung mit besonderer Erfahrung auf dem Gebiet der Kryptographie und den damit verbundenen mathematischen Berechnungsmethoden und deren verfahrens- und vorrichtungsmäßiger Umsetzung, als zu der beanspruchten Erfindung gehörend zu erkennen und der Streitpatentschrift und an entsprechender Stelle den ursprünglichen Unterlagen entnehmbar, vgl. die Patentschrift Seite 4, Absatz [0035], resp. die ursprünglich eingereichten Unterlagen gemäß Offenlegungsschrift Spalte 5 Zeilen 9 bis 12. Des Weiteren wurde die Vorrichtung und die dieser zugeordneten Einrichtungen gemäß Patentanspruch 14 dahingehend beschränkt, dass sie "ausgebildet" sind zur Durchführung der jeweiligen Verfahrensschritte entsprechend dem Verfahren des Patentanspruchs 1.

2. Stand der Technik

Aus der Entgegenhaltung D6, vgl. die Kapitel 3.2 und 3.5, ist ein Verfahren zum Absichern einer Berechnung in einem kryptographischen Algorithmus als bekannt entnehmbar, wobei die Berechnung Eingangsdaten p, q, x, g, k erhält, um Ausgangsdaten (die Signatur e, s) zu erzeugen (Merkmal a). Das in D6 am Beispiel einer Schnorr-Signatur beschriebene Verfahren weist die folgenden Schritte auf:

- Bereitstellen der Eingangsdaten für die Berechnung, vgl. Kapitel 3.2, 1. bis 2. Absatz – Merkmal b,
- Durchführen der Berechnung, um die Ausgangsdaten der Berechnung zu erhalten, vgl. Kapitel 3.2, 2. Absatz, wobei als Ausgangsdaten (Schnorr-Signatur) insbesondere $e = h(m \mid g^k \bmod p)$ und $s = ex + k \bmod q$ erhalten werden (Merkmal c),
- nach dem Durchführen der Berechnung, Überprüfen, ob die Eingangsdaten der Berechnung, bspw. das Eingangsdatum x nach x' verändert wurden, vgl. Kapitel 3.2, 5. Absatz, Kapitel 3.5, 2. bis 4. Absatz – Merkmale d und d1. Der zur Überprüfung verwendete Überprüfungsalgorithmus unterscheidet sich von der Berechnung (in dem kryptographischen Algorithmus, siehe vorangehenden Spiegelstrich), indem mit den vor der Berechnung abgespeicherten Eingangsdaten x, k und deren Inversen 1/x und 1/k nach der Berechnung von $s = ex + k$ der Wert von e gemäß dem Überprüfungsalgorithmus $e = k\ (s'\ (1/k) — 1)\ (1/x)$ verifiziert wird. Auch wird in D6 festgestellt, dass es sich bei der Überprüfung nicht um eine Zweit-Berechnung mit dem kryptographischen Algorithmus handelt, Kapitel 3.5, 4. Absatz i. V. m. 1. und 2. Absatz - Merkmal d2.
- falls das Überprüfen ergibt, dass die Eingangsdaten während der Berechnung verändert wurden (Kapitel 3.5, 3. Absatz und 4. Absatz, 2. und letzter Satz - Merkmal e), Unterdrücken einer Weitergabe der Ausgangsdaten der Berechnung (Kapitel 3.5, 2. Absatz, letzter Satz – Merkmal f).

Jedoch erfolgt gemäß dem aus der D6 als bekannt entnehmbaren Verfahren das Überprüfen, ob die Eingangsdaten während der Berechnung verändert wurden, entgegen dem Merkmal d3 des Patentanspruchs 1 nicht ohne Verwendung der Ausgangsdaten e und s (vgl. vorstehend dritten Spiegelstrich).

Die Abhandlung D7 beschreibt ebenfalls ein Verfahren zum Absichern einer Berechnung in einem kryptographischen Algorithmus, die Berechnung erhält Eingangsdaten r, s_i und N, um Ausgangsdaten y zu erzeugen, vgl. z. B. Seite 41, Abschnitt 4 – Merkmal a. Es werden Eingangsdaten für die Berechnung bereitgestellt und die Berechnung wird durchgeführt, um die Ausgangsdaten der Berechnung zu erhalten, vgl. Seite 41, Punkt 3: Alice berechnet aus bereitgestellten Eingangsdaten Ausgangsdaten y und sendet letztere an Bob - Merkmale b und c. Nach dem Durchführen der Berechnung werden die Eingangsdaten überprüft, ob sie während der Berechnung verändert wurden: nachdem Alice mit den Eingangsdaten r die Ausgangsdaten y gemäß $y = r \prod_{i \in S} s_i$ berechnet und an Bob gesendet hat, rekonstruiert Bob die Eingangsdaten r. Dabei nimmt Bob an, dass r verändert und durch r+E ersetzt ist, falls Bob E ungleich Null ermittelt, ist das Eingangsdatum r verändert, vgl. Seite 41, vierte Gleichung von unten (Merkmale d, d1). Jedoch erfolgt gemäß dem aus der D7 als bekannt entnehmbaren Verfahren das Überprüfen, ob die Eingangsdaten während der Berechnung verändert wurden, entgegen den Merkmalen d2 und d3 des Patentanspruchs 1 nicht unter Verwendung eines Überprüfungsalgorithmus, der sich von der Berechnung in einem kryptographischen Algorithmus ($y = r \prod_{i \in S} s_i$) unterscheidet, und nicht ohne Verwendung der Ausgangsdaten y. Für den Fall, dass das Überprüfen ergibt, dass die Eingangsdaten während der Berechnung verändert wurden (vgl. z. B. Seite 41, Absatz über der vierten Gleichung von unten - Merkmal e), zeigt die Entgegenhaltung D7 entgegen dem Merkmal f des Patentanspruchs 1 keine konkreten Folgemaßnahmen auf. Bzgl. Hardware- (Register-) Fehlern verweist die D7 auf zusätzliche Sicherungsmaßnahmen, z. B. das Vorsehen von CRCs (Seiten 38 und 49, jeweils vorletzter Absatz).

Die Entgegenhaltung D8, bei der es im Ergebnis dahinstehen kann, ob sie - wie von der Patentinhaberin geltend gemacht - nicht vorveröffentlicht ist, beschreibt u. a. ein Verfahren zum Absichern einer RSA-Signatur im Rahmen eines OpenPGP-Verschlüsselungsverfahrens und somit zum Absichern einer Berechnung in einem kryptographischen Algorithmus, vgl. D8, Seiten 7-11, Kapitel 5 bis

7, insbesondere sind in Kapitel 7 Gegenmaßnahmen gegen eine unzureichende Integrität von öffentlichem und privatem Schlüsseln, die in einer Datei abgespeichert sind, beschrieben. Die Berechnung der Signatur (mittels RSA-Signatur-Algorithmus entsprechend dem kryptographischen Algorithmus) erhält Eingangsdaten, um Ausgangsdaten (die Signatur) zu erzeugen, und erfolgt mit einem Schlüsselpaar von privatem Schlüssel (d, p, q, pInv) und öffentlichem Schlüssel (n, e) bzw. mit einem Exponentenpaar von privatem Exponenten d und öffentlichem Exponenten e, vgl. Seiten 7-10, Kapitel 5, insbes. Seiten 7-8, Kapitel 5.1 und 5.2, i. V. m. Seiten 1-2, Kapitel 1 – Merkmal a. Das Verfahren nach D8 weist die im Folgenden angegebenen Schritte auf. Es werden Eingangsdaten (Schlüssel, s. o.) für die Berechnung bereitgestellt und die Berechnung (der Signatur) durchgeführt, um die Ausgangsdaten (Signatur $s= m^d \bmod n$ der Nachricht m) zu erhalten (vgl. Seite 7, Kapitel 5.1 – Merkmale b und c). Die Integrität der in einer Datei abgespeicherten Schlüssel-Daten, d. h. auch der vorgenannten Eingangsdaten, kann verifiziert werden, indem insbesondere die unter den Punkten 1 bis 5 in Kapitel 7.3 auf Seite 11 angegebenen Beziehungen überprüft werden, vgl. dazu weiter die Seiten 10-11, Kapitel 7.1 bis 7.3. Diese Beziehungen sind erfüllt, wenn die Eingangsdaten unverändert sind; wurden die Eingangsdaten verändert, sind die Beziehungen i. d. R. nicht mehr erfüllt. Somit wird überprüft, ob die Eingangsdaten verändert wurden, wobei eine solche Veränderung der Daten während der Berechnung erfolgt sein kann. Gemäß D8, Seiten 18-20, Anhang 2, wird die Veränderung der Eingangsdaten durch einen Angriff ("attack") herbeigeführt, dadurch können Fehler während der Berechnung der Signatur erzeugt werden und auch durch direkte Angriffe auf abgespeicherte Schlüssel, Seite 19, Absatz unterhalb der ersten Berechnungsanleitung mit Schritten 1-5. Die Überprüfung gemäß Kapitel 7.3 der D8 erfolgt deshalb sinnvollerweise nach der Berechnung, da eine Veränderung während der Berechnung erfolgen kann (Merkmale d und d1), sie ist außerdem als ergänzende Überprüfung für den Fall des in Kapitel 5 der D8 beschriebenen Angriffs vorgesehen und kann eine gesonderte Überprüfung der Integrität des gespeicherten privaten Schlüssels (Eingangsdaten) nicht ersetzen, vgl. Seite 11, 2. Absatz, letzter Satz. Entgegen dem Merkmal d2 des Patentanspruchs 1 unterscheidet sich der

verwendete Überprüfungsalgorithmus nicht oder zumindest nur teilweise von der Berechnung in dem hier betrachteten RSA-Algorithmus, vgl. die Punkte 1 bis 4 gemäß Seite 11, Kapitel 7.3, mit den Definitionen zum RSA-Verfahren in Kapitel 5.1 auf Seite 7. Dementsprechend erfolgt auch das Überprüfen entgegen dem Merkmal d3 des Patentanspruchs 1 nicht ohne Verwendung der Ausgangsdaten, indem die Signatur $s= m^d \bmod n$ selbst oder Teile davon oder Zwischenergebnisse bei der Signaturberechnung, bspw. n = p*q und pInv, zum Überprüfen verwendet werden, vgl. auch hier Seite 19, Anhang 2, jeweils die Punkte 1 bis 5, oder die Punkte 3 und 4 gemäß Seite 11, Kapitel 7.3.

Aus der Druckschrift D9, vgl. insbesondere den Wortlaut des Patentanspruchs 14 i. V. m. der Fig. 2 und der dazugehörigen Beschreibung, ist ein Verfahren zum Absichern einer Berechnung in einem kryptographischen Algorithmus einer Chipkarte als bekannt entnehmbar, wobei ein verschlüsselter Benutzerschlüssel z. B. von einem Terminal aus in die Chipkarte geladen und dort als Eingangsdatum gespeichert und dadurch bereitgestellt wird (vgl. Spalte 3, Zeilen 15 - 38). Bei einer Sitzung mit der Chipkarte wird eine Berechnung mit einem kryptographischen Algorithmus (l'algorithme spécifique de chiffrement de clés: A.S.C.C.) durchgeführt, um mit Eingangsdaten Ausgangsdaten zu erzeugen, indem der verschlüsselte Benutzerschlüssel (Eingangsdaten) entschlüsselt wird, um einen entschlüsselten Benutzerschlüssel (Ausgangsdaten) zu erzeugen, letzterer wird dann in einer Sitzung mit der Chipkarte verwendet (Anspruch 14, insbesondere 4. und 5. Spiegelstrich, Spalte 4, Zeilen 33–57, Fig. 2, Schritt 23 - Merkmale a, b und c). Im Gegensatz zu den Merkmalen d und d1 des Patentanspruchs 1 erfolgt ein Überprüfen vor dem Durchführen der vorgenannten Berechnung, es wird somit überprüft, ob die Eingangsdaten vor der Berechnung verändert wurden (Anspruch 14, insbesondere 1. und 2. Spiegelstrich, Spalte 4, Zeilen 13–36, Fig. 2, Schritte 21, 22). Das Überprüfen erfolgt dergestalt, dass eine vorab abgespeicherte Schutzinformation, bspw. eine Prüfsumme oder eine zyklische Redundanzprüfung, mit einer Überprüfungsinformation verglichen wird, um die Integrität des Benutzerschlüssels zu überprüfen, der Überprüfungsalgorithmus unterscheidet sich demnach von der Berech-

nung mit einem kryptographischen Algorithmus und erfolgt ohne Verwendung der Ausgangsdaten (Anspruch 14, insbesondere 1. und 2. Spiegelstrich, Ansprüche 4 und 5, Spalte 3, Zeile 39 bis Spalte 4, Zeile 12 - Merkmale d2 und d3). Falls das Überprüfen ergibt, dass die Eingangsdaten (vor der Berechnung) verändert wurden, wird die Verwendung des verschlüsselten Benutzerschlüssels gesperrt (Anspruch 14, insbesondere 3. Spiegelstrich, Spalte 4, Zeilen 13–36, Fig. 2, Schritt 22 – Merkmale e und f teilweise).

Die Druckschriften D1 bis D5 und D10 haben in der mündlichen Verhandlung keine Rolle gespielt und bringen hinsichtlich der Beurteilung der Patentfähigkeit keine neuen Gesichtspunkte.

3. Neuheit

Der zweifelsfrei gewerblich anwendbare Gegenstand des Patentanspruches 1 ist neu, denn keine der Entgegenhaltungen zeigt alle seine Merkmale, wie sich aus den vorstehenden Ausführungen zum Stand der Technik ergibt.

4. Erfinderische Tätigkeit

Der Gegenstand des Patentanspruches 1 beruht auf einer erfinderischen Tätigkeit.

Es mag sein, dass der hier zuständige Fachmann, ausgehend von der sich ihm in der Praxis stellenden Aufgabe, ein sicheres und effizientes Konzept zum Absichern einer Berechnung in einem kryptographischen Algorithmus zu schaffen, in Betracht zieht, die aus den Entgegenhaltungen D6, D7 oder auch D8 als bekannt entnehmbaren Verfahren, die jeweils darauf abstellen, gemäß den Merkmalen a bis d1, teilweise auch d2 (Abhandlung D6) und e und f des Patentanspruchs 1, nach dem Durchführen der Berechnung in einem kryptographischen Algorithmus zu überprüfen, ob die Eingangsdaten für die Berechnung während der Berechnung verändert wurden, dahingehend zu verbessern, dass die Überprüfung mög-

lichst umfassend, aber auch mit geringem Rechenaufwand erfolgt, indem bspw. Doppelberechnungen mit ein und demselben kryptographischen Algorithmus vermieden werden, vgl. dazu die D6, Kapitel 3.5, 1. und 2. Absatz.

Keiner der vorgenannten Druckschriften D6 - D8 ist jedoch ein Hinweis darauf zu entnehmen, gemäß dem Merkmal d3 i. V. m. den Merkmalen d und d1 des Patentanspruchs 1 das Überprüfen, ob die Eingangsdaten während der Berechnung in dem kryptographischen Algorithmus verändert wurden, ohne Verwendung der Ausgangsdaten durchzuführen. Vielmehr erfolgt bei den in Betracht gezogenen Verfahren das Überprüfen stets mit Verwendung der Ausgangsdaten, vgl. Entgegenhaltung D6, Kapitel 3.5, 4. Absatz i. V. m. 1. und 2. Absatz, Ausgangsdaten e und s, weiter die Entgegenhaltung D7, Seite 41, vierte Gleichung von unten, Ausgangsdaten r und s_i, und D8, Seite 11, Kapitel 7.3 und Seite 19, Anhang 2, Ausgangsdatum Signatur $s= m^d \bmod n$.

Auch die Entgegenhaltung D9 hilft dem Fachmann nicht weiter. Das dort beschriebene Verfahren zur Überprüfung der Integrität eines Benutzerschlüssels (Eingangsdaten) benutzt zwar gemäß den Merkmalen d2 und d3 des Patentanspruchs 1 einen Überprüfungsalgorithmus, der sich von der Berechnung mit dem kryptographischen Algorithmus unterscheidet und ohne Verwendung der Ausgangsdaten erfolgt (vgl. D9, Anspruch 14, insbesondere 1. und 2. Spiegelstrich, Ansprüche 4 und 5, Spalte 3, Zeile 41 bis Spalte 4, Zeile 12), das Überprüfen erfolgt jedoch vor dem Durchführen der Berechnung mit dem kryptographischen Algorithmus, d. h. aber, dass die Eingangsdaten daraufhin überprüft werden, ob sie bereits vor der Berechnung verändert wurden (vgl. D9, Anspruch 14, insbesondere 1. und 2. Spiegelstrich, Spalte 4, Zeilen 13–36, Fig. 2, Schritte 21, 22). Mit dem Verfahren gemäß der D9 ist somit entgegen den Merkmalen d und d1 des Patentanspruchs 1 ein Überprüfen nach dem Durchführen der Berechnung, ob die Eingangsdaten während der Berechnung verändert wurden, nicht möglich. Nachdem der Fachmann gemäß Patentanspruch 1 aber gerade ein Verfahren zum Absichern einer Berechnung in einem kryptographischen Algorithmus anstrebt, das

darauf abstellt, dass nach dem Durchführen der Berechnung überprüft wird, ob die Eingangsdaten während der Berechnung verändert wurden, zieht er das Verfahren gemäß der D9 nicht in Betracht. Auch die aus den Entgegenhaltungen D6, D7 oder D8 als bekannt entnehmbaren Verfahren können den Fachmann, wie vorstehend dargelegt, nicht veranlassen, das in D9 beschriebene Vorgehen zum Einsatz zu bringen.

5. Der nebengeordnete Patentanspruch 14 ist auf eine Vorrichtung, ausgebildet zum Absichern einer Berechnung in einem kryptographischen Algorithmus, gerichtet, mit Einrichtungen, die korrespondierend zu den Verfahrenschritten des Anspruchs 1 ausgebildet sind. Insbesondere umfasst die Vorrichtung eine Einrichtung ausgebildet zum Überprüfen, ob die Eingangsdaten während der Berechnung verändert wurden, unter Verwendung eines Überprüfungsalgorithmus, der sich von der Berechnung unterscheidet, ohne Verwendung der Ausgangsdaten. Der Gegenstand des Patentanspruchs 14 ist daher sinngemäß aus den gleichen Gründen wie das Verfahren des Patentanspruchs 1 patentfähig.

6. Die auf den Patentanspruch 1 rückbezogenen Patentansprüche 2 bis 13 sind ebenfalls patentfähig. Sie betreffen über das Selbstverständliche hinausgehende Ausgestaltungen des Gegenstandes des Patentanspruches 1.

7. Die – geänderte - Beschreibung genügt den an sie nach § 34 PatG zu stellenden Anforderungen.

Dr. Bastian Dr. Hartung Martens Kleinschmidt

Pü