BUNDESPATENTGERICHT

17 W (pat) 96/08

_____

(Aktenzeichen)

Verkündet am
20. September 2012
…

B E S C H L U S S

In der Beschwerdesache

betreffend die Patentanmeldung 10 2006 001 872.9 - 53

…

hat der 17. Senat (Technischer Beschwerdesenat) des Bundespatentgerichts auf die mündliche Verhandlung vom 20. September 2012 unter Mitwirkung des Vorsitzenden Richters Dipl. Phys. Dr. Fritsch, der Richterin Eder, des Richters Dipl. Ing. Baumgardt und der Richterin Dipl. Phys. Dr. Thum Rung

beschlossen:

Auf die Beschwerde der Anmelderin wird der Beschluss der Prüfungsstelle für Klasse G 06 F des Deutschen Patent- und Markenamts vom 3. Juni 2008 aufgehoben und das Patent mit folgenden Unterlagen erteilt:

Patentansprüche 1 bis 11 und

Beschreibung Seiten 1, 4, 4a, 4b, 5, 15, 16, 23, 25, jeweils überreicht in der mündlichen Verhandlung,

Beschreibung Seiten 2, 3, 6 bis 14, 17 bis 22, 24 und 1 Blatt Bezugszeichenliste, jeweils vom Anmeldetag,

2 Blatt Zeichnungen mit 2 Figuren vom 6. Februar 2006.

G r ü n d e

I.

Die vorliegende Patentanmeldung wurde am 13. Januar 2006 beim Deutschen Patent- und Markenamt eingereicht. Sie trägt nunmehr die Bezeichnung:

"Vorrichtung und Verfahren zum Überprüfen einer Fehlererkennungsfunktionalität einer Datenverarbeitungseinrichtung auf Angriffe".

Die Anmeldung wurde durch Beschluss der Prüfungsstelle für Klasse G 06 F des Deutschen Patent- und Markenamts mit der Begründung zurückgewiesen, dass es, um zum Gegenstand des Patentanspruchs 1 nach Hauptantrag zu gelangen,

für den Durchschnittsfachmann keines erfinderischen Zutuns bedürfe; denjenigen der beanspruchten Merkmale, die im zitierten Stand der Technik nicht direkt beschrieben oder die für den Fachmann in diesem Zusammenhang offensichtlich seien, komme jedenfalls die Bedeutung einer technischen Neuerung nicht zu. Dasselbe gelte für die Patentansprüche 1 nach den drei Hilfsanträgen.

Gegen diesen Beschluss ist die Beschwerde der Anmelderin gerichtet. Sie erläutert den Unterschied der beanspruchten Gegenstände gegenüber dem von der Prüfungsstelle entgegengehaltenen Stand der Technik, und dass hierzu im Zurückweisungsbeschluss lediglich argumentativ behauptet werde, ihnen käme die Bedeutung einer technischen Neuerung oder gar eines erfinderischen Merkmals nicht zu. Dabei habe sich die Prüfungsstelle allein auf das technische Allgemeinwissen des Durchschnittsfachmanns berufen und sei somit für ein zentrales und wesentliches Merkmal jeglichen drucktechnischen Nachweis schuldig geblieben.

Auf den Ladungszusatz des Senats hin hat die Anmelderin ihr Patentbegehren weiter spezifiziert und klargestellt. Sie hält es zumindest in der nunmehr geltenden Fassung für durch den Stand der Technik nicht nahegelegt und patentfähig.

Die Anmelderin beantragt,

> den angegriffenen Beschluss aufzuheben und das nachgesuchte Patent mit folgenden Unterlagen zu erteilen:
>
> Patentansprüche 1 bis 11 und Beschreibung Seiten 1, 4, 4a, 4b, 5, 15, 16, 23, 25, jeweils überreicht in der mündlichen Verhandlung, Seiten 2, 3, 6 bis 14, 17 bis 22, 24 und 1 Blatt Bezugszeichenliste, jeweils vom Anmeldetag, 2 Blatt Zeichnungen mit 2 Figuren vom 6. Februar 2006.

Die geltenden Patentansprüche, hier bezüglich des Hauptanspruchs mit einer möglichen Gliederung versehen, lauten:

"**1**. Vorrichtung zur Überprüfung einer Fehlererkennungsfunktionalität auf Angriffe, mit folgenden Merkmalen:

(a) einer Datenverarbeitungseinrichtung (100; 300) mit einer Recheneinrichtung (110; 310-1), die ausgelegt ist, um basierend auf mindestens einem Eingangsdatum ein Ausgangsdatum bereitzustellen;

(b) einer Fehlererkennungseinrichtung (120; 320), die ausgebildet ist, um die Fehlererkennungsfunktionalität auszuführen

(b1) und bei einer korrekten Ausführung der Fehlererkennungsfunktionalität einen Fehler des Ausgangsdatums zu erkennen und, falls ein Fehler vorliegt, ein Fehlersignal zu erzeugen; und

(c) einer Kontrolleinrichtung (210; 410),

(c1) die ausgebildet ist, um in einem Normalbetriebsmodus das Fehlersignal an einen Fehlersignalausgang (170; 370) durchzulassen und in einem Überprüfungsmodus das Fehlersignal zu blockieren, um das Fehlersignal nicht an den Fehlersignalausgang (170; 370) durchzulassen,

(c2) und die ferner ausgebildet ist, um die Recheneinrichtung (110; 310-1) oder mindestens ein Eingangsdatum so zu beeinflussen, dass die Fehlererkennungseinrichtung (120; 320)

bei der korrekten Ausführung der Fehlererkennungsfunktionalität einen Fehler erkennt,

(c3) und, falls auf die Beeinflussung hin kein Fehlersignal empfangen wird, auf einen Angriff auf die Fehlererkennungseinrichtung (120; 320) zu schließen und ein Alarmsignal auszugeben.

2. Vorrichtung nach Anspruch 1, bei der die Fehlererkennungseinrichtung (120) ausgebildet ist, um abhängig von mindestens einem Eingangsdatum und dem Ausgangsdatum ein Vorliegen eines Fehlers zu erkennen.

3. Vorrichtung nach Anspruch 1, bei der die Datenverarbeitungseinrichtung (300) eine weitere Recheneinrichtung (310-2) aufweist, die ausgebildet ist, um basierend auf dem mindestens einen Eingangsdatum ein weiteres Ausgangsdatum bereitzustellen, und bei der die Fehlererkennungseinrichtung (320) ausgebildet ist, um abhängig von dem Ausgangsdatum und dem weiteren Ausgangsdatum ein Vorliegen eines Fehlers zu erkennen.

4. Vorrichtung nach Anspruch 3, bei der die Kontrolleinrichtung (410) weiterhin ausgebildet ist, um die weitere Recheneinrichtung (310-2) oder das mindestens eine Eingangsdatum beeinflussen zu können, um bei einer korrekten Ausführung der Fehlererkennungsfunktionalität durch die Fehlererkennungseinrichtung (320) zu einem Fehler zu führen.

5. Vorrichtung nach einem der Ansprüche 1 oder 2, bei der die Fehlererkennungseinrichtung (120; 320) ausgebildet ist, auf

einen Fehler zu schließen, wenn das Ausgangsdatum eine vorbestimmte Bedingung erfüllt.

6. Vorrichtung nach einem der vorhergehenden Ansprüche, bei der die Fehlererkennungseinrichtung (120; 320) ausgebildet ist, um auf einen Fehler zu schließen, wenn das Ausgangsdatum und das mindestens eine Eingangsdatum eine vorbestimmte Beziehung zueinander nicht aufweisen.

7. Vorrichtung nach einem der vorhergehenden Ansprüche, bei der die Kontrolleinrichtung (210; 410) ausgebildet ist, um in den Überprüfungsmodus zu wechseln, wenn eine vorbestimmte Auslösebedingung erfüllt ist, und in den Normalbetriebsmodus zu wechseln, wenn die vorbestimmte Auslösebedingung nicht erfüllt ist.

8. Vorrichtung nach Anspruch 7, bei der die vorbestimmte Auslösebedingung intermittierend erfüllt ist.

9. Vorrichtung nach einem der vorhergehenden Ansprüche, bei der die Kontrolleinrichtung (210; 410) weiterhin ausgebildet ist, um nach dem Empfang des Fehlersignals auf die Beeinflussung hin die Fehlererkennungseinrichtung (120; 320) ohne eine Beeinflussung zur Überprüfung des Ausgangsdatums auf einen Fehler hin zu veranlassen und, falls die Kontrolleinrichtung (210; 410) daraufhin weiterhin das Fehlersignal von der Fehlererkennungseinrichtung (120; 320) empfängt, das Alarmsignal auszugeben.

10. Vorrichtung nach einem der vorhergehenden Ansprüche, bei der die Vorrichtung in einer integrierten Schaltung umfasst ist.

11. Verfahren zum Überprüfen einer Fehlererkennungsfunktionalität einer Datenverarbeitungseinrichtung (100; 300) auf Angriffe,

wobei die Datenverarbeitungseinrichtung (100; 300) eine Recheneinrichtung (110; 310-1) aufweist, die ausgelegt ist, um basierend auf mindestens einem Eingangsdatum ein Ausgangsdatum bereitzustellen;

und eine Fehlererkennungseinrichtung (120; 320) aufweist, die ausgebildet ist, um die Fehlererkennungsfunktionalität auszuführen und bei einer korrekten Ausführung der Fehlererkennungsfunktionalität einen Fehler des Ausgangsdatums zu erkennen und, falls ein Fehler vorliegt, ein Fehlersignal zu erzeugen, mit folgenden Schritten:

in einem Normalbetriebsmodus:

- Ausführen der Fehlererkennungsfunktionalität durch die Fehlererkennungseinrichtung (120; 320);

- Erzeugen des Fehlersignals durch die Fehlererkennungseinrichtung (120; 320), wenn bei dem Ausführen der Fehlerer-kennungsfunktionalität ein Fehler des Ausgabedatums erkannt wurde;

- Durchlassen des Fehlersignals an einen Fehlersignalausgang (170; 370);

in einem Überprüfungsmodus:

- Blockieren des Fehlersignals, um dasselbe nicht an den Fehlersignalausgang (170; 370) durchzulassen;

- Beeinflussen der Recheneinrichtung (110; 310-1) oder mindestens eines Eingangsdatums, so dass die Fehlererkennungseinrichtung (120; 320) bei der korrekten Ausführung der Fehlererkennungsfunktionalität einen Fehler erkennt;

- Ausführen der Fehlererkennungsfunktionalität durch die Fehlererkennungseinrichtung (120; 320);

- Erzeugen des Fehlersignals durch die Fehlererkennungseinrichtung (120; 320), wenn bei dem Ausführen der Fehlerer-kennungsfunktionalität ein Fehler des Ausgabedatums erkannt wurde;

- Schließen auf einen Angriff auf die Fehlererkennungseinrichtung (120; 320) und Ausgeben eines Alarmsignals, falls die Fehlererkennungseinrichtung (120; 320) kein Fehlersignal ausgibt."

Dem Patentbegehren soll die Aufgabe zugrunde liegen, eine Vorrichtung und ein Verfahren zu schaffen, die eine erhöhte Sicherheit Angriffen auf eine Datenverarbeitungseinrichtung gegenüber ermöglichen (siehe geltende Beschreibung Seite 4b Absatz 2).

Von der Prüfungsstelle wurden folgende Druckschriften entgegengehalten:

D1 US 5 872 790 A
D2 US 5 515 383 A
D3 US 5 686 885 A

Der Senat hat nachträglich noch benannt:

D4 US 6 799 287 B1
D5 US 3 699 323

II.

Die rechtzeitig eingelegte Beschwerde ist auch sonst zulässig. Sie hat Erfolg, da das nunmehr geltende Patentbegehren durch den bekannt gewordenen Stand der Technik nicht vorweggenommen oder nahegelegt ist, und auch die übrigen Kriterien für eine Patenterteilung erfüllt sind (PatG §§ 1 bis 5, § 34).

1. Die vorliegende Patentanmeldung betrifft eine Schutzmaßnahme für in sensiblen Bereichen eingesetzte elektronische Datenverarbeitungseinrichtungen, wie insbesondere Chipkarten oder Smartcards.

Aufgrund des Wertes der durch sie geschützten Güter werden solche Datenverarbeitungseinrichtungen Angriffen ausgesetzt, denen man durch verschiedene Präventiv-Maßnahmen entgegenwirken kann. Die Anmeldung führt aus, dass Sensoren für mögliche Angriffe, z. B. Spannungs-, Temperatur-, Licht-, oder Frequenzsensoren bekannt seien, welche beim Überschreiten der erlaubten Messwert-Bereiche die Situation als Angriff erkennen könnten (siehe Absatz [0003] der Offenlegungsschrift). Als darüber hinausgehende Sicherungsmaßnahme seien sog. UmSLC-Module (UmSLC = user mode sensor life control) bekannt, welche

die Funktionalität der Überwachungsschaltungen überprüfen könnten: durch ein Verstellen der Sensoren oder Stimulieren der zugehörigen Komponenten könne gezielt ein "Fehlalarm" ausgelöst werden, welcher das ordnungsgemäße Funktionieren der Überwachungsschaltung bestätigte. Der so ausgelöste "Fehlalarm" werde jedoch nicht wirksam geschaltet, sondern es werde damit nur geprüft, ob er überhaupt erzeugt wurde. Falls bei einem solchen Test der Alarm ausbliebe, könne auf einen manipulativen Angriff auf die Überwachungsschaltung geschlossen und nunmehr durch das UmSLC-Modul ein Alarmsignal ausgelöst werden. Diese Schutzmaßnahme basierte jedoch grundsätzlich auf analogen Sensoren und deren Erkennung der Umwelt- oder Betriebsbedingungen.

Die Anmeldung hat zum Ziel, einen ähnlichen Schutz für die digitale Datenverarbeitung in den Überwachungsschaltungen zu erreichen. Sie geht aus von einer (vorhandenen) Fehlererkennungseinrichtung, welche eine Recheneinrichtung (Rechenwerk, ALU) überwacht, siehe Absatz [0005] Die Fehlererkennungsfunktionen können bei-spielsweise als Überprüfung von Paritätsbits (Parity-Check) oder anderer Fehlererkennungscodes (EDC = Error Detection Code, CRC = cyclic redundancy check, Hash-Werte - siehe Absatz [0028]) realisiert sein (erstes Ausführungsbeispiel, siehe Figur 1 und zugehörige Beschreibung). Alternativ oder auch zusätzlich kann ein zweites Rechenwerk parallel die gleichen oder veränderte, beispielsweise invertierte Daten verarbeiten, welche in einem weiteren Schritt mit den Ergebnissen des ersten Rechenwerks verglichen werden (zweites Ausführungsbeispiel, siehe Figur 2 und zugehörige Beschreibung).

Um die Fehlererkennungsfunktionalität der Fehlererkennungseinrichtung zu überwachen, ist nun erfindungsgemäß eine **Kontrolleinrichtung** vorgesehen, welche durch Beeinflussung der Recheneinrichtung oder mindestens eines Eingangsdatums einen Fehler provoziert, so dass die Fehlererkennungseinrichtung einen Fehler erkennen müsste. Durch eine von der Kontrolleinrichtung gesteuerte Signalweiche für das Fehlersignal wird sichergestellt, dass ein derart provoziertes Fehlersignal nicht wirksam nach außen abgegeben werden kann; stattdessen wird

intern überprüft, ob das Fehlersignal erzeugt wurde (siehe Absätze [0032], [0033]). Sollte kein Fehlersignal eintreffen, geht die Kontrolleinrichtung von einer Manipulation der Fehlererkennungseinrichtung aus und erzeugt ihrerseits ein Alarmsignal.

Als Fachmann, der mit der Aufgabe betraut wird, die Sicherheit einer Datenverarbeitungseinrichtung gegenüber manipulativen Angriffen zu erhöhen, ist ein Diplomingenieur der Elektrotechnik mit Hochschul- oder Fachhochschulabschluss und mehrjähriger Berufserfahrung im Bereich von Sicherheitsmaßnahmen insbesondere für Chipkarten, Smartcards u. ä. anzusehen.

2. Der Erteilungsantrag verlässt nicht den Rahmen der ursprünglichen Offenbarung.

Der neue Patentanspruch 1 basiert auf dem ursprünglichen Anspruch 1, klargestellt und ergänzt anhand der ursprünglichen Beschreibung, insbesondere Seite 8 Absatz 3 und Seite 24 Absatz 3. Der nebengeordnete Patentanspruch 11 basiert auf dem ursprünglichen Anspruch 11, ebenfalls klargestellt und ergänzt insbesondere gemäß Seite 8 Absatz 3 und Seite 24 Absatz 3, ferner bezüglich des Normalbetriebsmodus gemäß Seite 9 Absatz 3 und bezüglich des Überprüfungsmodus gemäß Seite 11 Absatz 2 / Seite 12 Absatz 1.

Der Unteranspruch 2 geht zurück auf den ursprünglichen Unteranspruch 2 und die Beschreibung Seite 9 Absatz 3. Die Unteransprüche 3 bis 9 basieren auf den ursprünglichen Ansprüchen 3 bis 6 und 8 bis 10, in einzelnen Details an die Formulierung des neuen Patentanspruchs 1 angepasst und ggf. klargestellt. Unteranspruch 10 gründet sich auf die ursprüngliche Beschreibung Seite 25 Zeile 30 bis 33.

Die Patentansprüche geben nunmehr klar und deutlich an, was durch sie unter Schutz gestellt werden soll.

Die Beschreibung wurde - unter Berücksichtigung des entgegengehaltenen Standes der Technik - in zulässiger Weise an das geltende Patentbegehren angepasst.

3. Der jeweilige Gegenstand des geltenden Patentanspruchs 1 und des ihm nebengeordneten Verfahrensanspruchs 11 ist durch den bekannt gewordenen Stand der Technik weder vorweggenommen noch nahegelegt.

3.1 Bei den in der Anmeldung als vorbekannt beschriebenen Schutzmaßnahmen durch ein UmSLC-Modul für analoge Angriffs-Sensoren (Offenlegungsschrift Absatz [0003]/[0004]) handelt es sich nach Auskunft der Anmelderin um firmeninterne Kenntnisse, die der Öffentlichkeit nicht zugänglich gemacht worden sind. Sie sind druckschriftlich nicht belegt. Daher können sie nicht zum Stand der Technik gerechnet werden.

3.2 Die entgegengehaltenen Druckschriften zeigen einzelne Aspekte der Vorrichtung nach Patentanspruch 1 oder des Überprüfungsverfahrens nach Patentanspruch 11 auf, ohne diese aber vollständig vorzubeschreiben. Die jeweiligen Gegenstände der beiden unabhängigen Patentansprüche sind daher neu.

Aus D1 ist ein Fehlergenerator entnehmbar, der zum Testen einer Fehlererkennungseinrichtung in einer Speichersteuerung eingesetzt wird (siehe Spalte 2 Zeile 6-24). Es sollen Einzel- oder Mehrfach-Bitfehler erzeugt werden, um die Funktionalität von Parity Checks und Error Correction Codes (ECC) zu überprüfen. Somit ist hier zwar eine "Vorrichtung zur Überprüfung einer Fehlererkennungsfunktionalität" beschrieben, jedoch ohne dass etwaige Angriffe auf die Fehlererkennungseinrichtung in die Lehre der **D1** eingeflossen wären. Das überprüfbare Ausgangs-datum wird aus einem Speicher abgerufen, hingegen nicht von einer Rechenein-richtung erzeugt. Der beschriebene Fehlergenerator im Sinne des Merkmals (**c**) soll ein Ausgangsdatum des Speichers so beeinflussen, dass ein Parity-Fehler oder falscher ECC vorliegt (Spalte 3 Zeile 28-36 - Teil von Merkmal (**c2)**). Aus der Aufgabenstellung Spalte 2 Zeile 9-11, Zeile 15-17 lässt sich ab-

leiten, dass die Speichersteuerung eine Fehlererkennungseinrichtung für Parity Fehler oder ECC aufweisen muss, die den provozierten Fehler erkennen sollte (implizit: Merkmale (**b**), (**b1)**). Der Fehler wird vom Benutzer durch Druck auf die Taste 36 ausgelöst. Offensichtlich steht hier die Erzeugung der Fehler und die Synchronisierung auf den Speicherzyklus im Mittelpunkt. Auf die Fehlerbehandlung in der Speichersteuerung können allenfalls vage Rückschlüsse gezogen werden, konkret ist weder eine Recheneinrichtung (Teil von Merkmal (**a**) und Merkmal (**c2)**) noch ein "Normalbetrieb" im Unterschied zu einem "Überprüfungsmodus" oder eine davon gesteuerte Weiche für das Fehlersignal beschrieben (Merkmal (**c1**) fehlt); was geschehen sollte, falls der Fehler nicht erkannt wird, bleibt völlig offen (Merkmal (**c3**) fehlt). Ein Verfahren zum Überprüfen einer Fehlererkennungsfunktionalität im Sinne von Anspruch 11 ist noch weniger beschrieben, gerade die beanspruchten Arbeitsschritte müsste der Fachmann aus der Idee des Fehlergenerators der **D1** erst ableiten.

D2 beschreibt Integrierte Schaltkreise mit einer eingebauten Selbsttest-Schaltung auf Basis von Parity-Signalen. Hier ist eine Umschaltung zwischen einem Normalbetriebsmodus und einem Selbsttest-Modus vorgesehen (Spalte 7 Zeile 48-58), in welchem u. a. Parity-Fehler provoziert werden können. Wenn im Selbsttest-Modus ein Fehler der Fehlererkennungs-Schaltung erkannt wird, wird ein Fehlersignal ausgegeben (Spalte 8 Zeile 1-18 u. a. - in etwa Merkmale (**b**), (**b1**), (**c**), (**c2)**). Eine Weiche für das Fehlersignal ist ebensowenig beschrieben wie eine konkrete Reaktion der Schaltung auf das Erkennen eines Fehlers (Merkmale (**c1**), (**c3**) fehlen). Es findet sich auch keine Anregung, die beschriebene Selbsttest-Schaltung für das Erkennen eines Angriffs auf die Fehlererkennungs-Schaltung einzusetzen.

D3 (in Zurückweisungsbeschluss als *Druckschrift 2)* bezeichnet) bezieht sich auf Feuerwarnanlagen und insbesondere auf Rauchsensoren; für diese wird u.a. ein durch Tastendruck ausgelöster Testmodus beschrieben. Das Dokument wurde von der Prüfungsstelle lediglich herangezogen, um aufzuzeigen, dass im

Testmodus ausgelöste Alarmsignale selbstverständlich keinen "echten" Alarm erzeugen dürfen (siehe **D3** Zusammenfassung - Grundprinzip von Merkmal **(c1)**).

D4 betrifft ein Verfahren und eine Vorrichtung zur Überprüfung einer Fehlerkorrektureinrichtung (siehe Zusammenfassung: "verifies the correctness of the error correcting code algorithm and -implementation"). Sie geht aus von einer Datenverarbeitungseinrichtung (100) mit einer Kodierungseinrichtung (110, 115), die basierend auf einem Eingangsdatum (Figur 2: 64 bit data in) ein Ausgangsdatum (Figur 2: 72 bit, aus 110) bereitstellt (teilweise Merkmal **(a)**). Ferner ist eine Fehlererkennungseinrichtung (130, 135) vorgesehen, welche bei einer korrekten Ausführung der Fehlererkennungsfunktionalität einen Fehler des Ausgangsdatums erkennen und, falls ein Fehler vorliegt, ein Fehlersignal erzeugen soll (Figur 2: no_error, single_error, multiple_error, siehe Spalte 4 Zeile 38 ff. - Merkmale **(b)**, **(b1)**). Eine zusätzliche Einrichtung (120, 140) beeinflusst das Ausgangsdatum der Kodiereinrichtung (110) so, dass die Fehlererkennungseinrichtung (130) bei der korrekten Ausführung der Fehlererkennungsfunktionalität einen Fehler erkennen müsste (Spalte 4 Zeile 23-37 - Merkmal **(c)**, teilweise **(c2)**). Falls auf die Beeinflussung hin kein Fehlersignal erzeugt wird, soll ein eine nicht korrekte Ausführung der Fehlererkennungsfunktionalität anzeigendes Alarmsignal ausgegeben werden (Figur 3B: Schritte 330, 350, 360, ggf. 370 - teilweise Merkmal **(c3)**).

Jedoch liefert **D4** keine Anregung, die Überprüfung der Fehlerkorrektureinrichtung zur Erkennung von Angriffen auf diese einzusetzen und, falls auf die Beeinflussung hin kein Fehlersignal empfangen wird, auf einen Angriff auf die Fehlererkennungseinrichtung zu schließen. Nach der Lehre der **D4** soll prinzipiell der Algorithmus und die Implementierung eines Fehlerkorrekturverfahrens verifiziert werden, daher ist eine Unterscheidung zwischen Normalbetriebsmodus und Überprüfungsmodus nicht vorgesehen, und es gibt auch keine Weiche für das Fehlersignal (Merkmal **(c1)** fehlt). Schließlich wird der provozierte Fehler direkt in ein Datenwort injiziert, eine mittelbare Überprüfung der Kodiereinrichtung durch Be-

einflussung des Eingangsdatums oder der Kodiereinrichtung im Sinne von Merkmal **(c2)** ist hingegen nicht beschrieben.

D5 beschreibt ein Fehlererkennungs- und -korrektursystem für eine Recheneinheit (ALU) eines Digitalrechners. Beispielsweise ist eine Parity-Berechnung vorgesehen (Spalte 3 Zeile 39 - 60, Spalte 4 Zeile 20 - 25). Ein Rechenbeispiel findet sich in Spalte 5 Zeile 1 bis 53. Hier wird deutlich, dass die Fehlererkennungseinrichtung (siehe Figur 1: Parity Predictor 1-30, Parity Calculator 1-26, Compare Unit 1-42) einen möglichen Fehler abhängig von Eingangsdaten (RegA, RegB, PA, PB) und dem Ausgangsdatum (RegC) bestimmt (zu Unteranspruch 2).

Es ist festzuhalten, dass keine dieser Druckschriften Anregungen für das Überprüfen einer Fehlererkennungsfunktionalität auf Angriffe liefert. Ferner ist eine Weiche für das Fehlersignal (Merkmal **(c1)**) nirgendwo konkret vorbeschrieben.

3.3 Die Vorrichtung nach dem geltenden Patentanspruch 1 und das Überprüfungsverfahren nach Patentanspruch 11 beruhen auch auf einer erfinderischen Tätigkeit.

Als nächstkommenden Stand der Technik betrachtet der Senat die Druckschrift **D4**, welche aber, wie beschrieben, keine Anregung liefert, auf einen Angriff auf die Fehlererkennungseinrichtung zu schließen, falls auf einen provozierten Fehler hin kein Fehlersignal erzeugt wird, und die auch keinen Unterschied zwischen Normalbetriebsmodus und Überprüfungsmodus und keine dadurch gesteuerte Weiche für das Fehlersignal (Merkmal **(c1)**) kennt.

Keine der übrigen Druckschriften kann dem Durchschnittsfachmann eine Veranlassung liefern, in dieser Richtung nachzudenken. Allenfalls würde der "gesunde Menschenverstand" den Fachmann im Sinne von Druckschrift **D3** dahin führen, dass ein im Überprüfungsmodus provoziertes Fehlersignal keinen "echten" Alarm erzeugen dürfte. Dies setzt aber bereits das Implementieren eines Normal-

betriebsmodus und eines separaten Überprüfungsmodus voraus. Selbst wenn der Fachmann diese Idee aus der **D2** aufgreifen würde, fehlte immer noch jeder Zusammenhang zum Erkennen von Angriffen auf eine Fehlererkennungseinrichtung, oder die mittelbare Überprüfung der Recheneinrichtung durch Beeinflussung des Eingangsdatums oder der Recheneinrichtung selbst, im Sinne von Merkmal **(c2)**. Dasselbe gilt analog für das beanspruchte Überprüfungsverfahren. D. h. es sind für den Fachmann in jedem Fall mehrere Schritte erforderlich, um zur beanspruchten Erfindung zu gelangen, ohne dass es grundsätzlich eine Anregung gab, in dieser Richtung vorzugehen, wobei auch nicht jeder (Teil-) Schritt im Stand der Technik eine konkrete Vorlage hat. Deshalb ist nicht festzustellen, dass die jeweils beanspruchte Erfindung für den Durchschnittsfachmann nahelag.

4. Die gewerbliche Anwendbarkeit der beanspruchten Vorrichtung wie auch des Überprüfungsverfahrens ist offensichtlich.

Folglich sind die unabhängigen Patentansprüche 1 und 11 gewährbar.

Die Unteransprüche 2 bis 10 betreffen nicht selbstverständliche Ausgestaltungen der beanspruchten Vorrichtung und sind in Verbindung mit Anspruch 1 ebenfalls gewährbar.

Dr. Fritsch Eder Baumgardt Dr. Thum-Rung

Me