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 7. Mai 2009

Beschwerde-Aktenzeichen: T 1348/04 - 3.5.01

Anmeldenummer: 00983200.7

Veröffentlichungsnummer: 1234239

IPC: G06F 12/14

Verfahrenssprache: DE

Bezeichnung der Erfindung:
Mikroprozessoranordnung mit Verschlüsselung

Anmelderin:
Infineon Technologies AG

Einsprechende:
-

Stichwort:
Mikroprozessoranordnung mit Verschlüsselung / INFINEON TECHNOLOGIES

Relevante Rechtsnormen:
EPÜ Art. 52(1), 123 (2)
VOBK Art. 13(1)

Relevante Rechtsnormen (EPÜ 1973):
EPÜ Art. 54(1)(2), 56

Schlagwort:
"Erfinderische Tätigkeit (bejaht - nach Änderung)"

Zitierte Entscheidungen:
-

Orientierungssatz:
-

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

Aktenzeichen: T 1348/04 - 3.5.01

E N T S C H E I D U N G
der Technischen Beschwerdekammer 3.5.01
vom 7. Mai 2009

Beschwerdeführerin: Infineon Technologies AG
St.-Martin-Straße 53
81669 München (DE)

Vertreter: -

Angefochtene Entscheidung: **Entscheidung der Prüfungsabteilung des Europäischen Patentamts, die am 15. Juli 2004 zur Post gegeben wurde und mit der die europäische Patentanmeldung Nr. 00983200.7 aufgrund des Artikels 97(1) EPÜ 1973 zurückgewiesen worden ist.**

Zusammensetzung der Kammer:

Vorsitzender: S. Steinbrener
Mitglieder: K. Bumes
G. Weiss

Sachverhalt und Anträge

I. Die Beschwerde richtet sich gegen die Entscheidung der Prüfungsabteilung, die europäische Patentanmeldung Nr. 00983200.7 mit der Bezeichnung "Mikroprozessoranordnung mit Verschlüsselung", veröffentlicht als

A2: WO-A2-01/40950,

zurückzuweisen.

II. Die Prüfungsabteilung hat die Anmeldung formal aufgrund Artikel 113 (2) EPÜ 1973 zurückgewiesen, nachdem die Anmelderin in der mündlichen Verhandlung vor der Prüfungsabteilung geänderte Ansprüche vorgelegt, die Prüfungsabteilung die späte Vorlage jedoch abgelehnt hatte (Regel 86 (3) EPÜ 1973).

Materielle Einwände (Artikel 56 EPÜ 1973) gibt die angegriffene Entscheidung als "Zusätzliche Bemerkungen" wieder, mit Gründen aus dem schriftlichen Verfahren. Die Prüfungsabteilung sieht den anmeldungsgemäßen Verschlüsselungsbetrieb als naheliegend an, ausgehend von D1: EP-A-0 887 723
in Verbindung mit dem Standardwerk

D3: Bruce Schneier, "Applied Cryptography, Second Edition", John Wiley & Sons Inc., New York 1996, insbesondere Seiten 3, 4, 173, 176, 197, 372 ff, 381 und 587.

III. Die Beschwerdeführerin beantragt die Aufhebung der angefochtenen Entscheidung und die Erteilung eines Patents auf der Grundlage geänderter Ansprüche 1 bis 3, die in der mündlichen Verhandlung vor der Kammer eingereicht wurden und wie folgt lauten:

"1. Datenverarbeitungsanordnung, die umfasst:
- eine zentrale Verarbeitungseinheit (1) und mindestens eine periphere Einheit (2, 3), die über einen Bus (4) miteinander verbunden sind,
- eine erste kryptographische Einheit (21, 31), die in der peripheren Einheit (2, 3) angeordnet ist und an den Bus (4) angeschlossen ist,
- eine zweite kryptographische Einheit (11), die in der zentralen Verarbeitungseinheit (1) angeordnet ist und an den Bus (4) angeschlossen ist, wobei
- Datenverkehr verschlüsselt über den Bus übertragen wird, indem der Datenverkehr von der sendenden Einheit verschlüsselt und von der empfangenden Einheit entschlüsselt wird,
- einen Zufallsgenerator (6) zur Erzeugung einer Folge von Zufallswerten, der mit der ersten und der zweiten kryptographischen Einheit (21, 31; 11) zur Einspeisung der Zufallswerte gekoppelt ist, wobei
- der kryptographische Betrieb der ersten und zweiten kryptographischen Einheiten (21, 31; 11) in Abhängigkeit von den vom Zufallsgenerator (6) erzeugten Zufallswerten steuerbar ist,

gekennzeichnet dadurch,

dass die Datenverarbeitungsanordnung eine monolithisch integrierte Mikroprozessoranordnung in einem mobilen Datenträger ist,

dass jede der kryptographischen Einheiten (11, 21, 31) umfasst:

- ein rückgekoppeltes Schieberegister (116), dem die vom Zufallsgenerator (6) erzeugten Zufallswerte zuführbar sind, und

- eine Anzahl von Datensignalpfaden mit je einem logischen Verknüpfungselement (112, 113, 114, 115),

welches eingangsseitig mit dem Signalpfad und einem Ausgang des rückgekoppelten Schieberegisters (116) verbunden ist und ausgangsseitig mit einem der Signalpfade,

und dass jede der kryptographischen Einheiten (11, 21, 31) durch einen Anschluss zur Einspeisung eines Taktsignals (CLK) taktsynchron steuerbar ist.

2. Datenverarbeitungsanordnung nach Anspruch 1, dadurch gekennzeichnet, dass das Schieberegister (116) linear rückgekoppelt ist.

3. Datenverarbeitungsanordnung nach einem der Ansprüche 1 oder 2, dadurch gekennzeichnet, dass die periphere Einheit (2) ein Speicherzellenfeld umfasst."

Mit den geänderten Ansprüchen hat die Beschwerdeführerin angepasste Beschreibungsseiten 1, 2, 2a, 3 bis 9 vorgelegt. Das Zeichnungsblatt 1/1 behält seine ursprüngliche Fassung.

IV. Mit der Ladung zur mündlichen Verhandlung teilte die Kammer ihre vorläufige Einschätzung des Anmeldungsgegenstands in Bezug auf den Stand der Technik nach D1 und D3 mit und führte eine weitere vorveröffentlichte Druckschrift ein,

D10: GB-A-2 099 195,

die eine verschlüsselte Datenübertragung mittels zweier kryptographischer Einheiten beschreibt, die von einem gemeinsamen Zufallsgenerator gesteuert werden.

V. Der in der Verhandlung vor der Kammer eingereichte Anspruch 1 ist gegenüber D10 abgegrenzt. Das Hauptargument der Beschwerdeführerin besteht darin, dass

es nicht naheliege, das aus D10 bekannte Verschlüsselungskonzept auf eine monolithisch integrierte Mikroprozessoranordnung anzuwenden, denn es sei nicht möglich, die räumlich getrennten kryptographischen Einheiten der D10 synchron mit dem hochfrequenten Takt einer Mikroprozessoranordnung zu steuern. Synchron getaktete Schieberegister seien vorteilhafterweise in der Lage, häufige Wechsel des steuernden Zufallswerts zu berücksichtigen, während D10 einen Wechsel des Zufallswerts nur einmal pro Transaktion vorsehe.

VI. Die Kammer verwies in der mündlichen Verhandlung auch auf die in der Beschreibungseinleitung der Anmeldung (A2, Seite 2, Absatz 2) genannte Druckschrift

D0: DE-A-196 42 560.

Sie verkündete ihre Entscheidung am Ende der mündlichen Verhandlung.

Entscheidungsgründe

1. Der geänderte Anspruchssatz ist zwar (auch) eine Reaktion auf die von der Kammer eingeführte Entgegenhaltung D10, wurde aber erst in einem sehr späten Stadium des Beschwerdeverfahrens, nämlich während der mündlichen Verhandlung, vorgelegt. Eine Zulassung des geänderten Vorbringens lag daher nach Artikel 13 (1) VOBK im Ermessen der Kammer.

Da der geänderte Antrag auf bereits auch in der angefochtenen Entscheidung ausführlich erörterten Merkmalen ursprünglicher abhängiger Ansprüche beruht und die Komplexität des Falls nicht erhöht, war der Kammer

eine Entscheidungsfindung ohne Verfahrensverlängerung möglich. Die Kammer ließ daher den Antrag zu.

2. Die Kammer hat keinen Zweifel an der ursprünglichen Offenbarung der beanspruchten Datenverarbeitungs-anordnung. Der geänderte Anspruch 1 fasst die Merkmale der ursprünglichen Ansprüche 1, 2, 4, 6 und 8 zusammen und fügt das Merkmal hinzu, dass der Datenverkehr verschlüsselt über den Bus übertragen wird. Dies gibt eine wesentliche Maßnahme der Anmeldung wieder (A2, Seite 3, Zeilen 16 bis 19; Seite 5, Zeile 27 bis Seite 6, Zeile 13).

Der jetzige Anspruch 2 entspricht dem ursprünglichen Anspruch 5, der jetzige Anspruch 3 dem ursprünglichen Anspruch 7. Auch die angepasste Beschreibung geht nicht über den Inhalt der ursprünglichen Anmeldung hinaus. Die präzisierte Aufgabenformulierung (Seite 2a unten) nennt geringen Schaltungsaufwand sowie die Fähigkeit zur Integration in Vorrichtungen mit kleinen Abmessungen, wie dies z. B. aus der ursprünglichen Seite 8 (letzter Absatz) bzw. Seite 1 (Absatz 2) hervorgeht.

Die geänderten Unterlagen erfüllen daher die Erfordernisse des Artikels 123 (2) EPÜ.

3. Ausgangspunkt der Anmeldung ist eine dank Verschlüsselung abhörsichere Datenübertragungsstrecke zwischen einer zentralen Verarbeitungseinheit (kurz: CPU) und einer peripheren Einheit (z. B. einer Ein-/Ausgabe-schaltung oder einem Speicher). Der kryptographische Betrieb der sendenden Einheit (und der komplementäre Betrieb der empfangenden Einheit) wird durch einen Zufallsgenerator variiert, so dass die verschlüsselten

Daten sich ändern, selbst wenn dieselben Klardaten wiederholt gesendet werden. Die beteiligten Einheiten brauchen nur den Zufallswert, aber keinen geheimhaltungsbedürftigen Schlüssel zu empfangen.

Gegenstand des vorliegenden Anspruchs 1 ist eine effektive Anwendung dieses Datenübertragungskonzepts auf eine monolithisch integrierte Mikroprozessoranordnung in einem mobilen Datenträger (z. B. einer Chipkarte).

4. Der Oberbegriff des geänderten Anspruchs 1 gibt die Merkmale wieder, die in Kombination aus der *Druckschrift D10* bekannt sind, nämlich eine Datenverarbeitungsanordnung *(Figur 1A)*, die umfasst:
- eine zentrale Verarbeitungseinheit *(processing station 55)* und mindestens eine periphere Einheit *(user station 53)*, die über einen Bus *(beschriftet mit ENCRYPTED DATA)* miteinander verbunden sind,
- eine erste kryptographische Einheit *(43, 45)*, die in der peripheren Einheit *(53)* angeordnet ist und an den Bus angeschlossen ist,
- eine zweite kryptographische Einheit *(49, 51)*, die in der zentralen Verarbeitungseinheit *(55)* angeordnet ist und an den Bus angeschlossen ist, wobei
- Datenverkehr verschlüsselt über den Bus übertragen wird, indem der Datenverkehr von der sendenden Einheit verschlüsselt wird *(encoding module 45)* und von der empfangenden Einheit entschlüsselt wird *(decoding module 51)*,
- einen Zufallsgenerator *(41)* zur Erzeugung einer Folge von Zufallswerten *(RN)*, der mit der ersten und der zweiten kryptographischen Einheit *(43, 45; 49, 51)* zur Einspeisung der Zufallswerte *(RN)* gekoppelt ist, wobei
- der kryptographische Betrieb der ersten und zweiten

kryptographischen Einheiten *(43, 45; 49, 51)* in Abhängigkeit von den vom Zufallsgenerator *(41)* erzeugten Zufallswerten *(RN)* steuerbar ist *(Seite 2, Zeilen 60 bis 104)*.

5. Aus der Entgegenhaltung D10 (die auf Anmeldungen der Jahre 1978/79 zurückgeht) geht weder explizit noch implizit hervor, ob die dort beschriebene Datenverarbeitungsanordnung einen Mikroprozessor umfasst. Nach dem Ausführungsbeispiel ist diese bekannte Anordnung zur Durchführung von Banktransaktionen vorgesehen, bei denen Daten von einer vom Benutzer bedienbaren Eingabestation an eine zentrale Verarbeitungsstation übermittelt werden (D10, Seite 1, Zeilen 6 bis 56). Somit unterscheidet sich die beanspruchte Datenverarbeitungsanordnung von der Lehre der D10 durch folgende Merkmale gemäß dem kennzeichnenden Teil des Anspruchs 1:

5.1 Die Datenverarbeitungsanordnung ist eine monolithisch integrierte Mikroprozessoranordnung in einem mobilen Datenträger.

5.2 Jede der kryptographischen Einheiten umfasst ein rückgekoppeltes Schieberegister (116), dem die vom Zufallsgenerator (6) erzeugten Zufallswerte zuführbar sind.

5.3 Jede der kryptographischen Einheiten umfasst eine Anzahl von Datensignalpfaden mit je einem logischen Verknüpfungselement (112, 113, 114, 115), welches eingangsseitig mit dem Signalpfad und einem Ausgang des rückgekoppelten Schieberegisters (116) verbunden ist und ausgangsseitig mit einem der Signalpfade.

5.4 Jede der kryptographischen Einheiten (11, 21, 31) ist durch einen Anschluss zur Einspeisung eines Taktsignals (CLK) taktsynchron steuerbar.

Die unterscheidenden Merkmale stellen die Neuheit der beanspruchten Datenverarbeitungsanordnung gegenüber der Lehre der D10 her. Auch keines der weiteren verfügbaren Dokumente zum Stand der Technik zeigt die Kombination der beanspruchten Merkmale. Der Gegenstand des Anspruchs 1 erfüllt daher das Erfordernis der Neuheit (Artikel 52 (1) EPÜ in Verbindung mit Artikel 54 (1) (2) EPÜ 1973).

6. Die unterscheidenden Merkmale erzielen folgende Wirkungen.

6.1 Indem das aus D10 bekannte Verschlüsselungsverfahren auf die Datenübertragung in einer monolithisch integrierten Mikroprozessoranordnung eines mobilen Datenträgers angewandt wird, werden sogar solche Daten gegen Abhören geschützt, die innerhalb eines Chips ausgetauscht werden. Dadurch sind mobile Datenträger, die für sicherheitskritische Anwendungen (Finanztransaktionen, Zugangskontrollen etc.) gedacht sind, vor Ausforschung und Fälschung geschützt.

6.2 Rückgekoppelte Schieberegister sind Schaltkreise niedriger Komplexität, die sich auf der begrenzten Fläche eines Chips platz- und kostensparend integrieren lassen. Sie lassen sich einfach auf einen Startwert setzen, und Datenbits des Klartexts und des Zufallswerts lassen sich einfach einspeisen. Die Weiterschaltung von einem Registerzustand zum nächsten lässt sich einfach

und schnell takten und erzeugt in Abhängigkeit von der Rückkopplung dennoch eine (pseudo-)zufällige Folge von Ausgangssignalen, die für einen Dritten, der die Rückkopplung des Schieberegisters nicht kennt, praktisch nicht vorhersehbar ist. Dennoch ist die Folge deterministisch, d.h. zwei gleich aufgebaute Schieberegister, die denselben Startwert und denselben Zufallswert empfangen, erzeugen dieselbe Folge von Ausgangssignalen. Zwei kryptographische Einheiten mit Schieberegistern gleichen Aufbaus können somit parallel den zusammengehörenden Ver- und Entschlüsselungs-Bitstrom erzeugen.

6.3 Logische Verknüpfungselemente, z. B. Exklusiv-Oder-Gatter (A2, Seite 5, Absatz 1; Seite 8, Zeilen 5 bis 10), sind ebenfalls Schaltkreise niedriger Komplexität, die sich platz- und kostensparend integrieren lassen. Sie ermöglichen eine einfache und schnelle Verknüpfung der von den Schieberegistern ausgegebenen Bits mit den Bits des Datensignalstroms, um diesen effizient (z. B. in Echtzeit) zu verschlüsseln bzw. zu entschlüsseln.

6.4 Dank monolithischer Integration und entsprechend kurzer Signalwege können die kryptographischen Einheiten der Datenübertragungsstrecke durch ein Taktsignal aus der die Strecke enthaltenden Mikroprozessoranordnung synchron gesteuert werden. Die taktsynchrone Steuerung stellt sicher, dass die Einheiten sich zu jedem Taktzeitpunkt im selben kryptographischen Modus befinden. Dadurch können die kryptographischen Einheiten wesentlich schneller als in der Anordnung nach D10 synchron getaktet werden. Ver- und Entschlüsselung auf dem Bus sind in einem schnellen (Echtzeit-)Betrieb möglich, der die Übertragungsrate des Busses (im

Vergleich zu einer unverschlüsselten Übertragung) wenig oder gar nicht einschränkt. Ferner können die kryptographischen Einheiten eine Änderung des Zufallswerts wesentlich öfter als einmal pro Transaktion berücksichtigen.

Die vorgenannten Wirkungen ergeben sich objektiv aus der Verwendung einer taktsynchronen Steuerung, auch wenn die ursprüngliche Anmeldung nur wenig zur Wirkung dieser Steuerung offenbart (A2, Seite 4, Zeilen 9 bis 11: "Zweckmäßigerweise ... taktsynchron"; Seite 6, Zeilen 18 bis 23; Seite 7, Zeile 31 bis Seite 8, Zeile 5).

7. Aus den objektiven Wirkungen leitet sich die Aufgabenstellung ab, die aus D10 für eine allgemeine Datenübertragungsstrecke bekannte und wünschenswerte Verschlüsselung in einer Weise umzusetzen, die eine effektive Anwendung auch unter den technisch und wirtschaftlich beschränkenden Rahmenbedingungen von Chipkarten (Platz- und Rechenzeitbeschränkung, billige Massenproduktion) gewährleistet.

8. Hinsichtlich des Erfordernisses erfinderischer Tätigkeit (Artikel 56 EPÜ 1973) beurteilt die Kammer die unterscheidenden Merkmale zunächst individuell wie folgt.

8.1 D1 betrifft zwar keine *monolithisch integrierte* Mikroprozessoranordnung, offenbart aber bereits die Idee und Notwendigkeit, den Datenverkehr auch innerhalb einer Mikroprozessoranordnung abhörsicher zu gestalten (Spalte 3, Zeilen 6 bis 37).

Aus D0 ist speziell bekannt, den internen Datenverkehr einer Chipkarte mit integriertem Mikrocontroller durch

Verschlüsselung gegen Abhören zu schützen (Spalte 1, Zeile 66 bis Spalte 2, Zeile 33).

8.2 Bekanntermaßen sollen geheime Schlüssel vorzugsweise Zufallszahlen sein (D3, Seite 173, Abschnitt "Random Keys"). Da jede Änderung der beiden in D10 verwendeten identischen Schlüssel (KEY, KEY') wieder zu einem identischen Schlüsselpaar führen muss (D10, Seite 2, Zeilen 79/80), setzt der Algorithmus der Schlüsselerzeugung eine pseudozufällige, reproduzierbare Folge von Zahlen voraus. Dies wird bekanntermaßen von rückgekoppelten Schieberegistern geleistet (D3, Kapitel 16, Abschnitte 16.2 bis 16.4, Seite 372 ff, z. B. Figur 16.2, Seite 374).

8.3 Eine einfache und schnelle Verschlüsselung ergibt sich durch logische Verknüpfung (z. B. durch Exklusiv-Oder-Gatter) der von Schieberegistern ausgegebenen (Schlüssel-)Bits mit den Bits des Datensignalstroms. Dies ist ein Standardverfahren der Kryptographie (siehe D3, Seite 13, Abschnitt 1.4 "Simple XOR", insbesondere Seite 14 Mitte: "The plaintext is being XORed with a keyword to generate the ciphertext"; D3, Abschnitt 9.4 "Stream Ciphers", Seiten 197/198; oder D0, Spalte 3, Zeilen 30 bis 45).

8.4 Die Vorgehensweise, die kryptographischen Einheiten der aus D10 bekannten Datenübertragungsstrecke synchron durch einen Takt einer sie enthaltenden Mikroprozessoranordnung zu steuern, wird wie folgt beurteilt.

8.4.1 In der Anordnung gemäß D10 wird nach jeder Transaktion (d.h. in Sekunden- oder Minutenintervallen) ein neuer

Zufallswert (RN) aus dem Zufallsgenerator (41) in die beiden Module (43, 49) eingespeist; mit anderen Worten wird der Betrieb der kryptographischen Einheiten nur in einem makroskopischen Sinn synchronisiert. Ferner beschreibt D10 nur eine verschlüsselnde Übertragungsstrecke (DATA ==> ENCRYPTED DATA ==> DECRYPTED DATA), nicht Herkunft oder Ziel der übertragenen Daten, und bietet auch von daher keinen Anlass, das Taktsignal der kryptographischen Einheiten aus einer Mikroprozessoranordnung zu beziehen, deren Daten übertragen werden sollen. Im Gegenteil, die räumliche Distanz zwischen Sendestation (53) und Empfangsstation (55) der D10 würde den Fachmann vom Versuch abhalten, die kryptographischen Einheiten z. B. mit der Arbeitsfrequenz eines Mikroprozessors (typischerweise im MHz-Bereich) zu takten, denn eine Synchronisierung der kryptographischen Einheiten könnte über die Entfernung nicht gewährleistet werden.

8.4.2 Die Entgegenhaltung D0 zielt jedoch bereits auf eine Echtzeitverschlüsselung des Datenverkehrs auf dem Datenbus einer integrierten Datenverarbeitungsschaltung mit CPU (Spalte 1, Zeile 66 bis Spalte 2, Zeile 7; Spalte 3, Zeilen 30 bis 45). Die Echtzeitfähigkeit wird durch eine Hardware-Verschlüsselung, z. B. durch eine Verschlüsselungsbaugruppe mit wenigstens einem EXOR-Glied, erreicht.

Da der verschlüsselnde Bus in Echtzeit Daten aus der CPU übertragen soll, müssen die kryptographischen Einheiten des Busses *de facto* im Takt der Mikroprozessoranordnung arbeiten. Auch wenn dies in D0 nicht ausgesprochen ist, dürfte der fachmännische Leser die Arbeitsweise der Schaltung aus technischen Gründen in dieser Weise

verstehen.

9. Obwohl somit im wesentlichen jedes einzelne Merkmal der beanspruchten Mikroprozessoranordnung für sich genommen aus dem nachgewiesenen Stand der Technik oder allgemeinem Fachwissen bekannt ist, anerkennt die Kammer in der Kombination der Merkmale aufgrund der vorteilhaften Gesamtwirkung, die über die Summe der Einzelwirkungen hinausgeht, eine erfinderische Tätigkeit.

Insbesondere ist nicht anzunehmen, dass der Fachmann ausgehend von der Entgegenhaltung D10 eine Anpassung der dort beschriebenen, diskret aufgebauten stationären Datenübertragungseinrichtung ohne rückschauende Betrachtungsweise für eine Chipkarte mit der beanspruchten Merkmalskombination vorgenommen hätte.

Der erzielte Synergieeffekt besteht darin, dass durch die taktsynchrone Steuerung der integrierten Einheiten nicht nur ein Echtzeitbetrieb der Ver- und Entschlüsselung auf dem Datenbus der D10 möglich wird, sondern darüber hinaus die wirksame kryptographische Komplikation der D10 - Einspeisung eines Zufallswerts in die kryptographischen Einheiten - weiter verstärkt wird, indem eine höhere Frequenz der Zufallswerteinspeisung als in D10 ermöglicht ist. Gleichzeitig erfüllen die hierzu verwendeten Mittel niedriger Komplexität - Schieberegister, logische Gatter - die Rahmenbedingungen mobiler Datenträger hinsichtlich Chipflächensparsamkeit, Funktionsschnelligkeit und billiger Massenherstellung.

Die Kammer sieht daher das Erfordernis erfinderischer Tätigkeit (Artikel 56 EPÜ 1973) für die Mikroprozessoranordnung nach Anspruch 1 als erfüllt an.

10. Der geänderte Anspruchssatz, die angepasste Beschreibung und das ursprüngliche Zeichnungsblatt 1/1 erfüllen nach dem Urteil der Kammer alle Erfordernisse des Übereinkommens.

Entscheidungsformel

Aus diesen Gründen wird entschieden:

1. Die angefochtene Entscheidung wird aufgehoben.

2. Die Angelegenheit wird an die erste Instanz zurückverwiesen mit der Anordnung, ein Patent mit folgenden Unterlagen zu erteilen:
   - Ansprüche 1 bis 3 eingereicht in der mündlichen Verhandlung am 7. Mai 2009;
   - Beschreibung Seiten 1, 2, 2a, 3 bis 9 eingereicht in der mündlichen Verhandlung am 7. Mai 2009;
   - Zeichnungsblatt 1/1 wie ursprünglich eingereicht.

Der Geschäftsstellenbeamte: Der Vorsitzende:

T. Buschek S. Steinbrener