

Interner Verteilerschlüssel:

- (A) [] Veröffentlichung im ABl.
(B) [] An Vorsitzende und Mitglieder
(C) [] An Vorsitzende
(D) [X] Keine Verteilung

E N T S C H E I D U N G
vom 14. Mai 2003

Beschwerde-Aktenzeichen: T 1104/00 - 3.5.2
Anmeldenummer: 94100237.0
Veröffentlichungsnummer: 0616429
IPC: H03K 3/84
Verfahrenssprache: DE

Bezeichnung der Erfindung:

Verfahren und Schaltungsanordnung zum Erzeugen einer Pseudozufallsfolge sowie deren Verwendung

Anmelder:

Infineon Technologies AG

Einsprechender:

-

Stichwort:

-

Relevante Rechtsnormen:

EPÜ Art. 123(2) und 56

Schlagwort:

"Verstoß gegen Artikel 123(2) - (nein)"
"Erfinderische Tätigkeit - (ja)"

Zitierte Entscheidungen:

-

Orientierungssatz:

-



Aktenzeichen: T 1104/00 - 3.5.2

E N T S C H E I D U N G
der Technischen Beschwerdekammer 3.5.2
vom 14. Mai 2003

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

Vertreter: Epping Hermann & Fischer
Ridlerstraße 55
D-80339 München (DE)

Angefochtene Entscheidung: Entscheidung der Prüfungsabteilung des Europäischen Patentamts, die am 11. Februar 2000 zur Post gegeben wurde und mit der die europäische Patentanmeldung Nr. 94 100 237.0 aufgrund des Artikels 97 (1) EPÜ zurückgewiesen worden ist.

Zusammensetzung der Kammer:

Vorsitzender: W. J. L. Wheeler
Mitglieder: J. -M. Cannard
B. J. Schachenmann

Sachverhalt und Anträge

I. Die Beschwerde richtet sich gegen die Zurückweisung der europäischen Patentanmeldung Nr. 94 100 237.0. Die Entscheidung der Prüfungsabteilung wurde damit begründet, daß der Gegenstand der seinerzeit geltenden Ansprüche 1 und 2 nicht auf einer erfinderischen Tätigkeit gegenüber folgendem Stand der Technik beruhe:

D2: Advances in Cryptology - AUSCRYPT '90,
International Conference on Cryptology,
Proceedings, Sydney, Australien, 8 bis 11
Januar 1990, Seiten 32 bis 36,

D3: US-A-5 060 265.

In der Zurückweisungsentscheidung wird auch ausgeführt, daß Anspruch 1 gegen Artikel 123 (2) EPÜ verstoße.

II. Die geltenden unabhängigen Ansprüche 1 und 2, die in der mündlichen Verhandlung vor der Kammer vom 14. Mai 2003 eingereicht worden sind, haben folgenden Wortlaut:

Anspruch 1:

"Verfahren zum Erzeugen einer Pseudozufallsfolge von Bitdaten (A) aus den Ausgangsdaten (P) einer rückgekoppelten Schieberegistereinrichtung (R, S) durch gesteuerte Ausblendung von Bits der Ausgangsdaten (P), wobei die Steuerung der Ausblendung ausschließlich durch den Schaltzustand von vorgegebenen Schieberegisterzellen (b, c, d, e) der Schieberegistereinrichtung (R, S) über eine nicht-lineare logische Funktion beeinflusst wird."

Anspruch 2:

"Schaltungsanordnung zur Durchführung des Verfahrens nach Anspruch 1, bei der eine ausgangsseitig eine Schalteinrichtung (T) aufweisende rückgekoppelte Schieberegistereinrichtung (S, R) eine Vielzahl hintereinander geschalteter Schieberegisterzellen (a...z) enthält, und bei der vorgegebene Schieberegisterzellen (b, c, d, e) ausgangsseitig mit einer nichtlinearen logischen Funktion (h) realisierenden Schaltung (F) verbunden sind, welche ausgangsseitig mit der Schalteinrichtung (T) zu deren Steuerung in Verbindung steht. dadurch gekennzeichnet, daß ausschließlich die vorgegebenen Schieberegisterzellen (b, c, d, e) der Schieberegistereinrichtung mit dem Eingang der nichtlinearen Funktion (h) verbunden sind."

Ansprüche 3 bis 5 sind vom Anspruch 2 abhängig. Die Verwendungsansprüche 6 und 7 sind von Ansprüchen 1 bis 5 abhängig.

III. Die Argumente des Beschwerdeführers lassen sich wie folgt zusammenfassen:

Wie es aus der einzigen Figur und dem entsprechenden Ausführungsbeispiel zu entnehmen sei, gehe das Verfahren gemäß Anspruch 1 nicht über den Inhalt der ursprünglich eingereichten Anmeldung hinaus.

Der Gegenstand der Patentansprüche 1 und 2 beruhe auf einer erfinderischen Tätigkeit. Im Unterschied zum aus dem Dokument D3 bekannten Verfahren werde erfindungsgemäß das Steuersignal durch Abgreifen vorbestimmter Zellen des rückgekoppelten Schieberegisters erzeugt. Im Unterschied zum Dokument D2 werde bei dem Verfahren

gemäß Anspruch 1, beziehungsweise der Anordnung gemäß Anspruch 2, ein am Ausgang des rückgekoppelten Schieberegisters angeordneter Schalter so gesteuert, daß der daraus resultierende Bitstrom eine Nichtlinearität aufweise. Da den Dokumenten D2 und D3 als solchen keinerlei Hinweis darauf zu entnehmen sei, daß die jeweilige Anordnung in Richtung auf die Gegenstände der Ansprüche 1 und 2 zu verändern sei, liege ausgehend von einem der beiden Dokumente keinerlei Grund für das Bestreiten erfinderischer Tätigkeit vor. Es gebe auch keine Anregung, den Stand der Technik gemäß D2 und D3 so zu kombinieren, daß man zum Gegenstand der Ansprüche 1 und 2 gelange. Insbesondere sei für den Fachmann nicht erkennbar, daß eine solche Kombination zu einer kostengünstigeren Herstellung oder zu einer besseren Lösung führen könnte.

- IV. Der Beschwerdeführer beantragt, die Zurückweisungsentscheidung aufzuheben und ein Patent mit folgenden Unterlagen zu erteilen:

Beschreibung, Ansprüche und Zeichnung in der Fassung wie in der Verhandlung vom 14. Mai 2003 eingereicht.

Entscheidungsgründe

1. Die Beschwerde ist zulässig.
2. *Änderungen*

Die Änderungen des Anspruchs 1 schränken seinen Gegenstand auf ein Verfahren ein, bei dem die Steuerung der Ausblendung von Bitdaten aus den Ausgangsdaten einer rückgekoppelten Schieberegistereinrichtung "ausschließ-

lich durch den Schaltzustand von vorgegebenen Schieberegisterzellen der Schieberegistereinrichtung über eine nicht-lineare logische Funktion beeinflusst wird". Der Anspruch 2 unterscheidet sich von dem ursprünglich eingereichten Anspruch 2 durch die Einfügung des Merkmals "ausschließlich die vorgegebenen Schieberegisterzellen... verbunden sind".

Der Beschwerdeführer hat in der mündlichen Verhandlung die Kammer davon überzeugt, daß der Fachmann das in den ursprünglich eingereichten Anmeldungsunterlagen beschriebene Ausführungsbeispiel (siehe die veröffentlichte Anmeldung: Figur; Spalte 5, Zeilen 12 bis 27) nur so hat verstehen können, daß **Bits** aus den Ausgangsdaten der Schieberegistereinrichtung (R, S) ausgeblendet würden, und die Steuerung der Ausblendung **ausschließlich** durch den Schaltzustand von vorgegebenen Zellen der Schieberegistereinrichtung über eine nicht-lineare logische Funktion beeinflusst werde. Unter diesen Verhältnissen kommt die Kammer zu dem Schluß, daß die geänderten Patentansprüche 1 und 2 nicht über den Inhalt der Anmeldung in der ursprünglich eingereichten Fassung hinausgehen (Artikel 123 (2) EPÜ).

Die Patentansprüche 3 bis 7 entsprechen den Ansprüchen 4 bis 8 in der ursprünglich eingereichten Fassung. Die an die geänderten Ansprüche angepaßten Seiten 1, 1a, 4 und 5 der Beschreibung verstoßen nicht gegen Artikel 123 (2) EPÜ.

3. *Erfinderische Tätigkeit*

- 3.1 Sowohl beim Verfahren gemäß Dokument D3 als beim Verfahren gemäß Anspruch 1 wird die Ausblendung von Bits aus dem Ausgang einer rückgekoppelten Schieberegister-

einrichtung gesteuert und die Steuerung durch den Schaltzustand einer Zelle dieser Einrichtung über eine Funktion so beeinflußt, daß der daraus resultierende Bitstrom eine Nichtlinearität aufweist, die eine hohe Sicherheit vor Fälschungen sicherstellt. Im Unterschied zu D3, wobei das Steuersignal dem Ausgangssignal einer eine nicht-lineare Funktion realisierenden Schaltung entspricht, die unter anderem aus einem XOR-Gatter, dessen zweiter Eingang mit den Ausgängen adressierbarer Register verbunden ist, und einem vorprogrammierten RAM Speicher (look-up table) besteht, wird die Steuerung beim Verfahren des Anspruchs 1 ausschließlich durch den Schaltzustand vorgegebener Zellen der Schieberegistereinrichtung selber über eine nicht-lineare logische Funktion beeinflußt. Ausgehend von D3 kann die Aufgabe demnach darin gesehen werden, ein Verfahren zu schaffen, das mit geringstmöglichem Aufwand eine höhere Sicherheit aufweist.

- 3.2 Beim Verfahren gemäß Dokument D2 werden die Inhalte der Zellen einer rückgekoppelten Schieberegistereinrichtung über eine nicht-lineare logische Funktion zu einem nicht-linearen Bitstrom umgewandelt. D2 gibt aber keinerlei Hinweise darauf, diesen Bitstrom zur Steuerung einer Ausblendung von Bits der Ausgangsdaten der Schieberegistereinrichtung zu verwenden.
- 3.3 Nach der Lehre der D3 wird die hohe Sicherheit durch die in die Pseudozufallsfolge eingefügte Nichtlinearität sichergestellt, die aus der Kombination der Inhalte von adressierbaren Registern mit dem Schaltzustand der letzten Zelle der rückgekoppelten Schieberegistereinrichtung resultiert. Es gibt aber für den Fachmann weder in D2 noch in D3 eine Anregung, die Inhalte dieser adressierbaren Register durch den Schaltzustand

vorgegebener Zellen der Schieberegistereinrichtung zu ersetzen. Durch Wegfall der in D3 beschriebenen adressierbaren Register fällt bei der Erfindung eine Eingreifsmöglichkeit aus, was die Sicherheit erhöht. Daß dieser Vorteil durch geschicktes Kombinieren von Merkmalen der D3 und D2 zu erreichen wäre, war für den Fachmann nicht ohne weiteres erkennbar. Der Fachmann hatte also keinen Grund, die Lehren von D3 und D2 so zu kombinieren, daß er zu dem Verfahren des Anspruchs 1 gelangte.

- 3.4 Das Verfahren gemäß Anspruch 1 wird also für den Fachmann durch den vorliegenden Stand der Technik nicht nahegelegt.
4. Dasselbe gilt für die Schaltungsanordnung gemäß Anspruch 2, deren Bestandteile alle in Verfahrensanspruch 1 genannten Schritte verwirklichen, und für die Verwendung des Verfahrens nach Anspruch 1 oder der Schaltungsanordnung nach einem der Ansprüche 2 bis 5 gemäß den Ansprüchen 6 und 7.
5. Der Gegenstand der Ansprüche 1, 2, 6 und 7 gilt daher als neu und auf einer erfinderischen Tätigkeit beruhend (Artikel 54 und 56 EPÜ).
6. Die Anmeldung gemäß dem geltenden Antrag genügt den Erfordernissen des EPÜ.

Entscheidungsformel

Aus diesen Gründen wird entschieden:

1. Die angefochtene Entscheidung wird aufgehoben.

2. Die Angelegenheit wird an die erste Instanz mit der Anordnung zurückverwiesen, ein Patent mit folgender Fassung zu erteilen:

Beschreibung: Seiten 1, 1a, 2 bis 10;

Ansprüche: Nr. 1 bis 7;

Zeichnungen: einzige Figur;

alles überreicht in der mündlichen Verhandlung vom 14. Mai 2003.

Die Geschäftsstellenbeamtin:

Der Vorsitzende:

D. Sauter

W. J. L. Wheeler