Interner Verteilerschlüssel:

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

Datenblatt zur Entscheidung vom 20. Juni 2018

Beschwerde-Aktenzeichen: T 1842/14 - 3.5.07

Anmeldenummer: 02774716.1

Veröffentlichungsnummer: 1442391

IPC: G06F17/10

Verfahrenssprache: DE

Bezeichnung der Erfindung:
Verfahren und Vorrichtung zum Absichern einer Berechnung in einem kryptographischen Algorithmus

Patentinhaberin:
Infineon Technologies AG

Einsprechende:
Giesecke+Devrient Mobile Security GmbH

Stichwort:
Absichern einer kryptographischen Berechnung/INFINEON TECHNOLOGIES

Relevante Rechtsnormen:
EPÜ Art. 56
EPÜ R. 22(3)

Schlagwort:

Übertragung der Einsprechendenstellung (ja)
Erfinderische Tätigkeit - Hauptantrag (ja)

Zitierte Entscheidungen:

G 0004/88, T 0261/03

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern

Boards of Appeal

Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

Beschwerde-Aktenzeichen: T 1842/14 - 3.5.07

E N T S C H E I D U N G
der Technischen Beschwerdekammer 3.5.07
vom 20. Juni 2018

Beschwerdeführerin: (Patentinhaberin)	Infineon Technologies AG Am Campeon 1-12 85579 Neubiberg (DE)
Vertreter:	Stöckeler, Ferdinand Schoppe, Zimmermann, Stöckeler Zinkler, Schenk & Partner mbB Patentanwälte Radlkoferstrasse 2 81373 München (DE)
Beschwerdegegnerin: (Einsprechende)	Giesecke+Devrient Mobile Security GmbH Prinzregentenstraße 159 81677 München (DE)
Angefochtene Entscheidung:	**Entscheidung der Einspruchsabteilung des Europäischen Patentamts, die am 18. Juni 2014 zur Post gegeben wurde und mit der das europäische Patent Nr. 1442391 aufgrund des Artikels 101 (2) und (3) b) EPÜ widerrufen worden ist**

Zusammensetzung der Kammer:

Vorsitzender R. Moufang
Mitglieder: R. de Man
K. Bengi-Akyuerek

Sachverhalt und Anträge

I. Die Beschwerde der Patentinhaberin (Beschwerdeführerin) richtet sich gegen die Entscheidung der Einspruchsabteilung, das europäische Patent Nr. 1 442 391 zu widerrufen.

II. Die Giesecke & Devrient GmbH hatte als Einsprechende das gesamte Patent gemäß Artikel 100 a) i.V.m. Artikel 56 EPÜ angegriffen.

III. In der Entscheidung wurden folgende Dokumente zitiert:

E1: DE 199 44 991 A1, veröffentlicht am 12. April 2001; und

E2: Rankl W. et al.: "Handbuch der Chipkarten", 3. Auflage, 1999, ISBN: 3-446-21115-2, Seiten 506-509.

Die Einspruchsabteilung entschied, dass der Gegenstand der erteilten unabhängigen Ansprüche sowie der unabhängigen Ansprüche gemäß dem ersten Hilfsantrag im Hinblick auf Dokument E1 in Verbindung mit dem durch Dokument E2 belegten Fachwissen nicht erfinderisch sei, dass die damaligen zweiten und dritten Hilfsanträge aufgrund von Verstößen gegen Regel 80 EPÜ nicht zugelassen werden könnten und dass der Gegenstand des Anspruchs 1 gemäß dem damaligen vierten Hilfsantrag nicht ausreichend offenbart im Sinne von Artikel 83 EPÜ sei.

IV. Mit der Beschwerdebegründung reichte die Beschwerdeführerin eine Kopie der Ansprüche gemäß dem ersten Hilfsantrag sowie geänderte Ansprüche gemäß einem zweiten und dritten Hilfsantrag ein. Die Beschwerdeführerin beantragte, die angefochtene Entscheidung

aufzuheben und, als Hauptantrag, das Patent in unveränderter Form aufrechtzuerhalten. Hilfsweise beantragte sie, das Patent auf der Grundlage der Ansprüche gemäß dem ersten, zweiten oder dritten Hilfsantrag aufrechtzuerhalten. Ferner beantragte sie eine mündliche Verhandlung.

V. Die Giesecke & Devrient GmbH reichte keine Erwiderung auf die Beschwerdebegründung ein.

VI. In einer ersten Mitteilung nach Regel 100 (2) EPÜ legte die Kammer ihre vorläufige Meinung dar, dass das Patent in unveränderter Form aufrechterhalten werden könne.

VII. Mit Schreiben vom 7. November 2017 reichte die Giesecke +Devrient Mobile Security GmbH eine Stellungnahme zur Mitteilung der Kammer ein.

VIII. Mit Schreiben vom 21. November 2017 teilte die Beschwerdeführerin mit, dass sie keine mündliche Verhandlung beantragte, sollte das Patent gemäß Hauptantrag aufrechterhalten werden.

IX. In einer zweiten Mitteilung nach Regel 100 (2) EPÜ lenkte die Kammer die Aufmerksamkeit der Beteiligten darauf, dass eine Übertragung der Einsprechenden-stellung bis dahin nicht beantragt worden sei, weshalb die Kammer davon ausgehe, dass der Schriftsatz vom 7. November 2017 als Einwendung eines Dritten gemäß Artikel 115 EPÜ zu betrachten sei.

X. Mit Schreiben vom 19. Januar 2018, das am selben Tag beim EPA einging, beantragte die Giesecke+Devrient Mobile Security GmbH, die Parteistellung als Einsprechende von der Giesecke & Devrient GmbH auf sie zu übertragen. Sie machte geltend, dass sich der

vorliegende Einspruch auf den Geschäftsbereich "Mobile Security" der ursprünglichen Einsprechenden bezog und dass dieser Geschäftsbereich mit Wirkung vom 30. Juni 2017 durch Ausgliederung auf sie übergegangen sei. Sie legte dazu folgende Dokumente vor:

Ü1: Auszug aus dem Handelsregister B des Amtsgerichts München betreffend die Giesecke & Devrient GmbH;

Ü2: Auszug aus dem Handelsregister B des Amtsgerichts München betreffend die Giesecke+Devrient Mobile Security GmbH; und

Ü3: Auszug aus dem Jahresbericht der Giesecke & Devrient GmbH: "Konzern-Lagebericht zum 31. Dezember 2016" (Seiten 28 und 29).

XI. Mit Schreiben vom 19. März 2018 bestritt die Beschwerdeführerin, dass die Einsprechendenstellung auf die Giesecke+Devrient Mobile Security GmbH übergegangen sei.

XII. Anspruch 1 des Patents wie erteilt (Hauptantrag) lautet:

"Rechnergestütztes Verfahren zum Absichern einer Berechnung in einem kryptographischen Algorithmus gegenüber einer Fehlerattacke auf einen Kryptoprozessor, der den kryptographischen Algorithmus ausführt, wobei die Berechnung Eingangsdaten erhält, um Ausgangsdaten zu erzeugen, mit folgenden Schritten:

Bereitstellen (10) der Eingangsdaten für die Berechnung an einer Eingangsdaten-Speicherstelle;

Durchführen (12) der Berechnung unter Verwendung der bereitgestellten Eingangsdaten durch den

Kryptoprozessor, um die Ausgangsdaten der Berechnung zu erhalten;

nach dem Durchführen der Berechnung in dem Kryptoprozessor, Zugreifen auf die Eingangsdaten-Speicherstelle, um einen Inhalt der Eingangsdaten-Speicherstelle zu erhalten, Überprüfen (14) unter Verwendung des Inhalts der Eingangsdaten-Speicherstelle, ob die Eingangsdaten während der Berechnung verändert wurden, unter Verwendung eines Überprüfungsalgorithmus, der sich von der Berechnung unterscheidet; und

falls das Überprüfen (14) ergibt, dass die Eingangsdaten an der Eingangsdaten-Speicherstelle während der Berechnung durch den Kryptoprozessor verändert wurden, Unterdrücken (16) einer Weitergabe der Ausgangsdaten der Berechnung."

Die Ansprüche 2 bis 13 sind abhängige Ansprüche.

Anspruch 14 des Patents lautet wie folgt:

"Rechnergestützte Vorrichtung zum Absichern einer Berechnung in einem kryptographischen Algorithmus gegenüber einer Fehlerattacke auf einen Kryptoprozessor, der den kryptographischen Algorithmus ausführt, wobei die Berechnung Eingangsdaten erhält, um Ausgangsdaten zu erzeugen, und wobei besagte Vorrichtung die folgenden Merkmale enthält;

eine Einrichtung zum Bereitstellen (10) der Eingangsdaten für die Berechnung an einer Eingangsdaten-Speicherstelle;

eine Einrichtung zum Durchführen (12) der Berechnung

unter Verwendung der bereitgestellten Eingangsdaten durch den Kryptoprozessor, um die Ausgangsdaten der Berechnung zu erhalten;

eine Einrichtung zum Überprüfen (14), ob die Eingangsdaten während der Berechnung verändert wurden, durch Zugreifen auf die Eingangsdaten-Speicherstelle, um einen Inhalt der Eingangsdaten-Speicherstelle zu erhalten, und unter Verwendung sowohl eines Überprüfungsalgorithmus, der sich von der Berechnung unterscheidet, als auch des Inhalts der Eingangsdaten-Speicherstelle, wobei besagte Einrichtung zum Überprüfen weiter Mittel zum Durchführen der [sic] besagten Überprüfungsalgorithmus, nachdem die Berechnung in dem Kryptoprozessor durchgeführt worden ist, enthält und

eine Einrichtung zum Unterdrücken (16) einer Weitergabe der Ausgangsdaten, falls die Einrichtung (14) zum überprüfen [sic] ermittelt, dass die Eingangsdaten an der Eingangsdaten-Speicherstelle während der Berechnung durch den Kryptoprozessor verändert wurden."

XIII. Der Wortlaut der Hilfsanträge ist für diese Entscheidung nicht von Bedeutung.

XIV. Entscheidungsrelevante Argumente der Parteien werden nachfolgend in den Entscheidungsgründen wiedergegeben.

Entscheidungsgründe

1. Die Beschwerde genügt den in Regel 101 EPÜ genannten Bestimmungen und ist somit zulässig.

2. *Übertragung der Einsprechendenstellung*

2.1 In ihrer Entscheidung G 4/88 (ABl. EPA 1989, 480) hat die Große Beschwerdekammer befunden, dass ein Einspruch als zum Geschäftsbetrieb des Einsprechenden gehörend zusammen mit jenem Bereich dieses Geschäftsbetriebs an einen Dritten übertragen werden kann, auf den sich der Einspruch bezieht. In einem solchen Fall ist die Übertragung der Einsprechendenstellung beim EPA zu beantragen und durch Belege nachzuweisen (siehe Rechtsprechung der Beschwerdekammern, 8. Auflage, 2016, IV.C.2.2.6).

2.2 Am 19. Januar 2018 hat die Giesecke+Devrient Mobile Security GmbH die Übertragung der Einsprechenden-stellung von der Giesecke & Devrient GmbH auf sich beantragt und unter Vorlage der Dokumente Ü1, Ü2 und Ü3 begründet. Die Handelsregisterauszüge Ü1 und Ü2 belegen, dass die Giesecke & Devrient GmbH im Wege einer Ausgliederung gemäß Ausgliederungsvertrag vom 7. Juni 2017 sowie der Beschlüsse der Gesellschafterversammlungen vom selben Tag Teile ihres Vermögens, insbesondere den sog. MS-Teilbetrieb, auf die Giesecke+Devrient Mobile Security GmbH übertragen hat. Im Einklang hiermit stellt der Jahresbericht (siehe Dokument Ü3) fest, dass den operativen Geschäftsbereichen ab 2017 mehr Selbständigkeit und Eigenverantwortlichkeit ermöglicht werden und deshalb u.a. das Mobile Security-Geschäft in der Giesecke +Devrient Mobile Security GmbH gebündelt werden soll. In der Giesecke & Devrient GmbH sollten nur noch "klassische Konzern-Steuerungsfunktionen" und "Verwaltungsfunktionen" verbleiben.

2.3 Die Beschwerdegegnerin hat vorgetragen, dass weder die Handelsregisterauszüge noch der Jahresbericht Ü3

belegen könnten, dass der Einspruch auf Veranlassung des Geschäftsbereichs "Mobile Security" eingelegt worden sei.

Da das angegriffene Patent Maßnahmen zum Absichern von kryptographischen Berechnungen betrifft, erachtet die Kammer es jedoch als glaubhaft, dass der von der Giesecke & Devrient GmbH eingelegte Einspruch sich ursprünglich auf ihren Geschäftsbereich "Mobile Security" bezogen hat. Die Übertragung der Einsprechendenstellung ist somit ausreichend nachgewiesen (vgl. hierzu auch die Zwischenentscheidung T 261/03 vom 24. November 2005, Gründe 3.5.5).

2.4 Mit der Einsprechendenstellung ist auch die Rechtsstellung als Beschwerdegegnerin auf die Giesecke +Devrient Mobile Security GmbH übergegangen.

3. *Schriftsatz im Namen der Giesecke+Devrient Mobile Security GmbH vom 7. November 2017*

Laut ständiger Rechtsprechung hat - in entsprechender Anwendung von Regel 22 (3) EPÜ - als wirksamer Zeitpunkt einer Übertragung der Einsprechendenstellung (sofern nicht durch Gesamtrechtsnachfolge bewirkt) der Tag zu gelten, an dem die Übertragung beim EPA beantragt wurde und entsprechende Beweismittel beigebracht wurden. Da im vorliegenden Fall die Übertragung erst am 19. Januar 2018 beantragt wurde und weder die ursprüngliche noch die jetzige Einsprechende den Inhalt des Schriftsatzes vom 7. November 2017 bekräftigt hat, ist der Schriftsatz als Einwendung eines Dritten gemäß Artikel 115 EPÜ zu betrachten.

4. *Die Erfindung*

4.1 Die vorliegende Erfindung betrifft ein Verfahren und eine Vorrichtung zum Absichern einer Berechnung in einem kryptographischen Algorithmus. Die Patentschrift erläutert, dass kryptographische Berechnungen gegenüber kryptographischen Angriffen, bei denen die den Algorithmus ausführende Hardware zu Fehlern gebracht wird, sehr anfällig sind. So kann beim RSA-CRT-Algorithmus der geheime Schlüssel schon ermittelt werden, wenn eine einzige fehlerhafte Berechnung des Algorithmus ausgewertet wird. Hardware-Fehler können zum Beispiel durch Aussetzen des Kryptoprozessors gegenüber einer elektrischen oder thermischen Belastung verursacht werden. Als Gegenmaßnahme gegen solche Angriffe kann das Ergebnis jeder Berechnung überprüft werden, bevor es ausgegeben wird.

4.2 Laut Absatz [0033] der Patentschrift liegt der Erfindung die Erkenntnis zugrunde, dass die Eingangsdaten für eine kryptographische Berechnung am ehesten "Opfer" einer kryptographischen Attacke werden. Sind die Eingangsdaten nach dem Ausführen einer Berechnung in einem kryptographischen Algorithmus im Vergleich zu ihrem Zustand vor der Ausführung des kryptographischen Algorithmus unverändert, so kann mit hoher Sicherheit davon ausgegangen werden, dass keine kryptographische Attacke stattgefunden hat.

4.3 Die Erfindung schlägt deshalb vor, nach dem Durchführen der Berechnung unter Verwendung eines Überprüfungsalgorithmus zu überprüfen, ob die Eingangsdaten an der Eingangsdaten-Speicherstelle während der Berechnung verändert wurden. Ergibt sich, dass Eingangsdaten verändert wurden, wird die Weitergabe der Ausgangsdaten der Berechnung unterdrückt.

5. *Hauptantrag – Patent wie erteilt*

5.1 Die Einspruchsabteilung hat Dokument E1 als nächstliegenden Stand der Technik angesehen.

Dokument E1 betrifft ein Verfahren zur Sicherung des Programmablaufs bei sicherheitsrelevanten Anwendungen, beispielsweise im Bereich von IC-Karten (Spalte 1, Zeilen 3 bis 11). Laut Spalte 1, Zeilen 12 bis 19, kann der Zugriff auf geheime verschlüsselte Daten dadurch erfolgen, dass der Programmablauf gezielt unterbrochen wird, so dass Fehler in den Verschlüsselungsroutinen entstehen, aus denen auf die geheimen Daten rückgeschlossen werden kann. Zur Vermeidung derartiger Angriffe ist es notwendig, Fehler oder Störungen des Programmablaufs sicher zu erkennen.

5.2 Dokument E1 schlägt vor, bei einem Programmaufruf die vom aufrufenden Programm an das aufgerufene Programm übergebenen Parameter zu überprüfen (Spalte 1, Zeilen 40 bis 58). Eine Ausführungsform sieht vor, dass zunächst vom aufrufenden Programm über die übergebenen Parameter eine Checksumme gebildet wird, welche in einem dafür vorgesehenen Speicherbereich abgelegt wird. Nach Übergabe der Parameter wird auch vom aufgerufenen Programm eine Checksumme gebildet. Sind die gebildeten Checksummen unterschiedlich, so wird das Programm abgebrochen.

Laut Dokument E1 wird auf diese Weise sichergestellt, dass ein Funktionsprogramm bereits zu Beginn auf Manipulationen untersucht wird, so dass der Start des aufgerufenen Programms mit fehlerhaften Parametern von vornherein verhindert werden kann und eine Auswertung

der fehlerbehafteten Daten nicht ermöglicht wird (Spalte 1, Zeilen 59 bis 65).

5.3 Die nähere Erläuterung dieser Erfindung anhand der Figur 1 bestätigt, dass ein aufgerufenes Unterprogramm zunächst die Checksumme – nunmehr Prüfsumme genannt – über die übergebenen Parameter bildet (Spalte 2, Zeilen 52 bis 59). Als nächstes erfolgt eine Überprüfung der vom aufrufenden und aufgerufenen Programm ermittelten Prüfsummen auf Gleichheit (Spalte 2, Zeilen 60 und 61). Wird festgestellt, dass die beiden Prüfsummen gleich sind, wird mit der eigentlichen Funktionsausführung begonnen (Spalte 3, Zeilen 2 bis 4). Sonst kann davon ausgegangen werden, dass bei der Übergabe der Programmparameter ein Fehler aufgetreten ist, welcher ein Hinweis auf eine beabsichtigte Störung sein kann, und es werden angemessene Maßnahmen getroffen (Spalte 2, Zeile 61, bis Spalte 3, Zeile 1).

5.4 Dokument E1 offenbart zwei weitere Sicherheitsmaßnahmen, nämlich die Überprüfung von Rücksprungadressen (Spalte 2, Zeilen 1 bis 10; Spalte 3, Zeilen 5 bis 21; Figur 2) und die Überprüfung der für den Programmablauf benötigten Taktzyklen (Spalte 2, Zeilen 11 bis 25; Spalte 3, Zeilen 22 bis 51; Figur 3). Weder die Argumentation der Einspruchsabteilung noch die der Beschwerdegegnerin stützt sich aber auf diese weiteren Ausführungsformen.

5.5 Es ist unbestritten, dass der Gegenstand des Anspruchs 1 sich von dem im Dokument E1 offenbarten Verfahren mindestens dadurch unterscheidet, dass nach dem Durchführen der kryptographischen Berechnung überprüft wird, ob die in der Eingangsdaten-Speicherstelle enthaltenen Eingangsdaten während der

Berechnung verändert wurden. Dokument E1 offenbart nur, dass vor dem Durchführen der eigentlichen Berechnung ("Funktionsausführung") überprüft wird, ob die Eingangsdaten in Form von Programmparametern bei der Übergabe an das Unterprogramm, das die kryptographische Berechnung ausführt, verändert wurden.

5.6 Dass die in der Eingangsdaten-Speicherstelle enthaltenen Eingangsdaten am ehesten Opfer einer kryptographischen Attacke werden, ist laut Absatz [0033] die der Erfindung zugrunde liegende Erkenntnis (vgl. oben, Punkt 4.2) und wurde von der Beschwerdegegnerin auch nicht bestritten. Das Kippen von Bits an der Eingangsdaten-Speicherstelle ist deshalb ein Indikator dafür, dass eine kryptographische Attacke stattgefunden hat.

Die beanspruchte Überprüfung der Eingangsdaten an der Eingangsdaten-Speicherstelle nach der Durchführung der kryptographischen Berechnung löst somit die objektive technische Aufgabe, bei der Durchführung der Verschlüsselungsroutine gemäß der Lehre von Dokument E1 Fehlerattacken zuverlässiger zu erkennen. Diese Aufgabe lässt sich auch der Patentschrift entnehmen (siehe z.B. Absatz [0037]).

5.7 Nach Auffassung der Einspruchsabteilung hatte der Fachmann Veranlassung, Veränderungen der Eingangs-schlüsseldaten während der Berechnung abzusichern, da ihm aus seinem Fachwissen bekannt sei, dass die Schlüsseldaten auch während der Berechnung verändert werden könnten. Dieses Fachwissen werde von Dokument E2 auf Seite 507, erster vollständiger Absatz, bestätigt.

5.8 Dokument E2 ist ein Auszug aus einem Handbuch im Chipkartenbereich. Es bespricht auf Seite 506, zweiter

vollständiger Absatz, bis Seite 508, zweiter Absatz, auf "differentieller Fehleranalyse" basierende Sicherheitsangriffe, die es ermöglichen, den in einer Chipkarte enthaltenen geheimen Schlüssel durch Einstreuung von Hardwarefehlern zu ermitteln.

Gemäß Seite 507, erstem vollständigen Absatz, wird bei solchen Angriffen zunächst ein beliebiger Klartext mit dem zu brechenden Schlüssel verschlüsselt und der erhaltene Geheimtext aufbewahrt. Anschließend wird die Chipkarte während der Abarbeitung des kryptographischen Algorithmus gestört, "so daß sich ein einzelnes Schlüsselbit an beliebiger Stelle bei der Berechnung verändert". Das Ergebnis davon ist ein Geheimtext, welcher aufgrund des gekippten Bits falsch verschlüsselt wurde. Dieses Verfahren wird mehrmals wiederholt, bis der Schlüssel mittels einer mathematischen Analyse aus den Ergebnissen ermittelt werden kann.

Der nächste Absatz fügt hinzu, dass es bei einem solchen Angriff "nicht einmal erforderlich ist zu wissen, an welcher Stelle des geheimen Schlüssels ein Bit gekippt wurde".

5.9 Obwohl diese Textstellen ausdrücklich Fehler in Form von gekippten Schlüsselbits erwähnen, belegen sie nach Auffassung der Kammer nicht, dass es zum Prioritätsdatum Teil des Fachwissens war, dass Fehlerangriffe insbesondere an gekippten Bits der Eingangsdaten-Speicherstelle zu erkennen sind. Vielmehr dürfte das Fachwissen nur darin bestanden haben, dass irgendein bei der kryptographischen Berechnung gekipptes Bit ein Sicherheitsrisiko aufweist (vgl. die Patentschrift, Absatz [0018], wonach bei dem RSA-CRT-Algorithmus eine einzige fehlerhafte RSA-Signatur

ausreicht). Dieses Fachwissen veranlasst den Fachmann zwar, nach einem Weg zu suchen, die Fehlerfreiheit der kryptographischen Berechnung zu überprüfen. Die beanspruchte Überprüfung der Eingangsdaten an der Eingangsdaten-Speicherstelle stellt im Grunde genommen aber keine Überprüfung dieser Fehlerfreiheit dar. Denn Bits an der Eingangsdaten-Speicherstelle, die erst kippen, nachdem sie zum Zwecke der Berechnung ausgelesen worden sind, können die Richtigkeit der Berechnung nicht mehr beeinträchtigen.

5.10 Dokument E2 offenbart zwei Schutzmaßnahmen:

- Zweimalige Durchführung der kryptographischen Berechnung und Vergleich der beiden Ergebnisse (Seite 507, letzter Absatz); und
- Vermeidung der wiederholten Verschlüsselung eines identischen Klartextes durch Voranstellen einer Zufallszahl (Seite 508, erster Absatz).

Keine von beiden Maßnahmen enthält den Hinweis, zu überprüfen, ob während der Berechnung die in der Eingangsdaten-Speicherstelle enthaltenen Daten verändert wurden.

Die weiteren von der Beschwerdeführerin genannten und in Dokument E2 auf Seiten 508 und 509 unter der Überschrift "Schutzkomponente: Chipkarten-Betriebssystem" offenbarten Schutzmaßnahmen sind nicht spezifisch als Maßnahmen gegen Fehlerangriffe vorgesehen.

5.11 Da Dokument E2 nach Auffassung der Kammer nicht belegt, dass das Fachwissen den Fachmann veranlasst, zum Schutz gegen Fehlerattacken Veränderungen der in der Eingangsdaten-Speicherstelle enthaltenen Eingangsdaten

während der Berechnung abzusichern, kann die Begründung der angefochtenen Entscheidung nicht überzeugen.

5.12 In ihrer mit Schreiben vom 25. März 2013 während des Einspruchsverfahrens eingereichten Stellungnahme hat die (damalige) Einsprechende argumentiert, dass schon das allgemeine Fachwissen, "dass auch ein Angriff auf die Durchführung einer Berechnung im Rahmen eines kryptographischen Algorithmus sicherheitskritische Auswirkungen haben kann", den Fachmann in naheliegender Weise von der im Dokument E1 offenbarten technischen Lehre zur beanspruchten Erfindung geführt hätte, indem er anstatt oder zusätzlich zu der Überprüfung der Eingangsparameter vor der Berechnung eine Überprüfung nach der Berechnung durchgeführt hätte.

Die Kammer bemerkt jedoch, dass in Dokument E1 die Überprüfung der Eingangsdaten vor der Berechnung primär das Ziel hat, den sicheren Übergang dieser Eingangsdaten vom aufrufenden zum aufgerufenen Programm festzustellen. Demgegenüber ist die beanspruchte Überprüfung der in der Eingangsdaten-Speicherstelle enthaltenen Eingangsdaten nach der Berechnung ein indirekter Indikator für eine Fehlerattacke (vgl. oben, Punkte 4.2 und 5.9). Im Hinblick auf diese zwei unterschiedlichen Ziele ist die Kammer nicht davon überzeugt, dass der Fachmann nur aufgrund seiner Kenntnisse von möglichen Fehlerangriffen dazu gekommen wäre, zum Schutz gegen kryptographische Attacken nach der Berechnung eine Überprüfung der Eingangsdaten an der Eingangsdaten-Speicherstelle vorzunehmen.

5.13 Im Schriftsatz vom 7. November 2017 hat die Beschwerdegegnerin, die zu diesem Zeitpunkt allerdings noch keine Partei, sondern Dritte im Sinne von Artikel 115 EPÜ war (vgl. Punkt 3 oben), vorgetragen,

dass bei dem im Dokument E1 offenbarten Verfahren nach der Übergabe der Eingangsdaten von einem aufrufenden Programm an ein aufgerufenes Programm überprüft werde, ob sich die Eingangsdaten während der Übergabe verändert habe. Aus Dokument E2 entnehme der Fachmann, dass Eingangsdaten daraufhin geprüft werden müssten, ob sie während der Maßnahme "Abarbeiten eines kryptographischen Algorithmus" verändert wurden. Es sei deshalb naheliegend, die Maßnahme "Übergabe von Parametern" durch die Maßnahme "Abarbeiten eines kryptographischen Algorithmus" zu ersetzen.

Die Kammer kann sich dieser Argumentation nicht anschließen. In dem aus Dokument E1 bekannten Verfahren werden die Parameter von einem aufrufenden Programm an ein aufgerufenes Programm übergeben, damit das aufgerufene Programm eine kryptographische Berechnung durchführen kann. Da die Parameterübergabe einen unabdingbaren Bestandteil der Lehre von E1 bildet (vgl. oben, Punkte 5.2 und 5.3), ergibt es in diesem Kontext keinen technischen Sinn, den Schritt "Übergabe von Parametern" ohne weitere - nicht im Schriftsatz vom 7. November 2017 dargelegte - Änderungen durch einen Schritt "Abarbeiten eines kryptographischen Algorithmus" zu ersetzen.

5.14 Aus den obigen Gründen beruht der Gegenstand des unabhängigen Anspruchs 1 auf einer erfinderischen Tätigkeit im Sinne der Artikel 52 (1) und 56 EPÜ. Dasselbe gilt in analoger Weise auch für den Gegenstand des korrespondierenden unabhängigen Vorrichtungsanspruchs 14.

6. *Schlussfolgerung*

Da der einzige geltend gemachte Einspruchsgrund der Aufrechterhaltung des Patents nicht entgegensteht, ist die angefochtene Entscheidung aufzuheben und dem Hauptantrag der Beschwerdeführerin stattzugeben.

Eine mündliche Verhandlung nach Artikel 116 (1) EPÜ war nicht erforderlich, da die Beschwerdegegnerin keinen entsprechenden Antrag gestellt hat und die Beschwerdeführerin in ihrem Schreiben vom 21. November 2017 deutlich gemacht hat, dass ihr Antrag auf mündliche Verhandlung nicht für den Fall gilt, dass das Patent wie erteilt aufrechterhalten wird.

Entscheidungsformel

Aus diesen Gründen wird entschieden:

1. Die angefochtene Entscheidung wird aufgehoben.

2. Das Patent wird in unveränderter Form aufrechterhalten.

Die Geschäftsstellenbeamtin: Der Vorsitzende:

I. Aperribay R. Moufang

Entscheidung elektronisch als authentisch bestätigt