(19) **Bundesrepublik Deutschland**
Deutsches Patent- und Markenamt

(10) **DE 699 30 620 T2** 2006.08.24

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 076 951 B1**
(21) Deutsches Aktenzeichen: **699 30 620.5**
(86) PCT-Aktenzeichen: **PCT/US99/08913**
(96) Europäisches Aktenzeichen: **99 919 998.7**
(87) PCT-Veröffentlichungs-Nr.: **WO 1999/057843**
(86) PCT-Anmeldetag: **23.04.1999**
(87) Veröffentlichungstag der PCT-Anmeldung: **11.11.1999**
(97) Erstveröffentlichung durch das EPA: **21.02.2001**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **29.03.2006**
(47) Veröffentlichungstag im Patentblatt: **24.08.2006**

(51) Int Cl.[8]: ***H04L 9/00*** (2006.01)
H04Q 7/32 (2006.01)

(30) Unionspriorität:
74475 **07.05.1998** **US**

(84) Benannte Vertragsstaaten:
DE, FI, GB, NL, SE

(73) Patentinhaber:
Intel Corporation, Santa Clara, Calif., US

(74) Vertreter:
Patentanwälte Hauck, Graalfs, Wehnert, Döring, Siemons, Schildberg, 80339 München

(72) Erfinder:
LARSEN, E., Robert, Shingle Springs, CA 95682, US; HAZEN, K., Peter, Auburn, CA 95603, US; GULIANI, K., Sandeep, Folsom, CA 95630, US; HASBUN, N., Robert, Placerville, CA 95667, US; TALREJA, S., Sanjay, Folsom, CA 95630, US; ONG, Collin, Sacramento, CA 95831, US; BROWN, W., Charles, Folsom, CA 95630, US; KENDALL, L., Terry, Diamond Springs, CA 95619, US

(54) Bezeichnung: **VERFAHREN UND VORRICHTUNG ZUR VERMEIDUNG VON MI BRAUCH EINES ZELL-TELEFONS**

Beschreibung

GEBIET DER ERFINDUNG

[0001] Die vorliegende Erfindung betrifft allgemein das Verhindern der missbräuchlichen Verwendung eines Mobiltelefons, und im Besonderen betrifft sie ein eindeutiges Identifikationssystem zur Verhinderung von Missbrauch.

STAND DER TECHNIK

[0002] Die kabellose Kommunikation hat nachhaltige Auswirkungen auf die heutige Gesellschaft. In nur einigen wenigen Jahren haben Mobiltelefone Millionen von Teilnehmern in den USA, Europa und Asien angezogen. Diese besonders starke Entwicklung ist nur der Beginn der Telekommunikationsrevolution, gleichzeitig ist sie der Beginn einer Revolution auf dem Gebiet der Piraterie und der missbräuchlichen Verwendung von Mobiltelefonen.

[0003] Das kennzeichnende, dem Stand der Technik entsprechende Mobiltelefon verwendet einen nichtflüchtigen, beschreibbaren Speicher, um Daten oder Code oder beides zu speichern. Zu diesen nichtflüchtigen; beschreibbaren Speichern zählen elektrisch löschbare, programmierbare Nur-Lesespeicher (EEEPROMs als englische Abkürzung von Electrically Erasable Programmable Read-Only Memories) und Flash-EPROMs oder Flash-Speicher. Der Flash-Speicher des kennzeichnenden, dem Stand der Technik entsprechenden Mobiltelefons umfasst eine Geräteseriennummer (ESN) oder eine internationale Mobilgerätekennung (IMEI). Wenn das Mobiltelefon betrieben wird, wird die ESN oder die IMEI übertragen, um dem Mobilfunkbetreiber die Identifikation des Benutzers als befugter bzw. legitimer Teilnehmer zu ermöglichen, um dem Benutzer Zugang auf das Mobilfunknetz zu ermöglichen und um dem Benutzer den Zugang zu dem Netz in Rechnung stellen zu können. Ein missbräuchliches Clonen bzw. Klonen erfolgt, wenn die ESN oder die IMEI missbräuchlich erhalten und in ein anderes Mobiltelefon neu programmiert wird, wobei versucht wird, die Zahlung für den Mobiltelefondienst zu umgehen. Ferner weisen integrierte bzw. eingebettete Systeme ein ähnliches Problem auf, wobei ein Anwendungscode aus einem Flash-Speicher gelesen wird, wobei versucht wird, das Produkt zurückzuentwickeln.

[0004] Piraterie oder Missbrauch tritt in einem typischen dem Stand der Technik entsprechenden analogen Mobiltelefon auf, wenn das von dem Mobiltelefon übertragene analoge Signal abgefangen und decodiert wird, um dem Mobilfunkpiraten die ESN oder die IMEI des sendenden Benutzers bereitzustellen. Der Mobilfunkpirat verwendet die erhaltene ESN oder EMEI danach, indem diese in andere analoge Mobiltelefone programmiert wird. Wenn derartige missbräuchlich geclonte Mobiltelefone verwendet werden, werden die Mobilfunkminuten der missbräuchlich erlangten ESN oder IMEI in Rechnung gestellt.

[0005] Eine weitere Möglichkeit für die Mobilfunkpiraterie bietet sich, wenn die Mobilfunkgeräte von verschiedenen Service Providern im Ausland subventioniert werden. Zum Beispiel kann ein Service Provider in England einem Teilnehmer ein Mobiltelefon in Verbindung mit einem zweijährigen Dienstvertrag zu einem Preis von 200 US-Dollar überlassen. Im Gegensatz dazu überlässt ein Service Provider in Finnland ein Mobiltelefon in Verbindung mit einem über zwei Monate laufenden Dienstvertrag zu einem Preis von 1.000 US-Dollar. Abhängig von dem jeweiligen Land, in dem ein Mobiltelefon eingesetzt wird, kann das Telefon einen deutlich unterschiedlichen Wert aufweisen. Die sich ergebende Gelegenheit zum Missbrauch besteht darin, dass der Mobilfunkpirat Mobiltelefone in England für 200 US-Dollar kauft und diese nach Finnland einführt und dort zu einem Preis von weniger als 1.000 US-Dollar und gleichzeitig deutlich über einem Kaufpreis von 200 US-Dollar verkauft.

[0006] Da es keinen Sicherheitsstandard für den Hardwareschutz gibt, muss jeder OEM (OEM als englische Abkürzung von Original Equipment Manufacturer) ein eigenes System zum Schutz gegen Missbrauch implementieren. Einige OEMs von Mobiltelefonen unternehmen keine Anstrengungen, die Mobilfunkpiraterie zu unterbinden bzw. zu verhindern. Eine Technik zur Verhinderung von Missbrauch, die von einigen OEMs in einem typischen Mobiltelefon gemäß dem Stand der Technik eingesetzt wird, ist die Einbettung eines eindeutigen Codes in den Speicherraum der Systemsoftware des Mobiltelefons. Die Systemsoftware kennt die Adresse des Codes und verwendet diesen Code für den Zugriff auf die Systemsoftware. Das Problem bei dieser Technik ist es, dass sie leicht durch Löschen des ganzen Speichers und Installieren einer neuen Systemsoftware und der neuen Programmierung der gleichen Identifikation, wie sie ursprünglich vorhanden gewesen ist, überwunden werden kann.

[0007] Ein weiteres Problem in Bezug auf kennzeichnende dem Stand der Technik entsprechende GSM-Mobiltelefone (GSM als englische Abkürzung von Global System for Mobile Communications) stellt die missbräuchliche Verwendung der SIM-Karte (SIM als englische Abkürzung von Subscriber Identification Module bzw. Teilnehmeridentifikationskarte) oder der Smartcard dar. Die SIM-Karte, welche die Größe einer Kreditkarte aufweist, wird in Mobiltelefone eingeschoben, was es Benutzern ermöglicht, im Ausland Anrufe vorzunehmen oder entgegenzunehmen, wobei diese Anrufe in Rechnung gestellt werden, wenn sie wieder zu Hause sind. SIM-Karten wurden zwar zur Verwendung in Verbindung mit GSM-Mobil-

telefonen entwickelt, wobei aber auch in Erwägung gezogen wird, die SIM-Karten in Verbindung mit anderen Telefonen als GSM-Telefonen zu verwenden, wie zum Beispiel in Verbindung mit öffentlichen Fernsprechern, die mit Karten betrieben werden. Allerdings gelten hinsichtlich dieses Einsatzbereiches zunehmende Einschränkungen aufgrund der Sorgen darum, dass ein missbräuchlicher Einsatz der SIM-Karte sich kaum verhindern lässt.

[0008] Die GSM-Smartcard enthält Informationen, die Benutzer benötigen, um Anrufe über andere GSM-Netze zu tätigen, als über die Netze, deren Teilnehmer sie sind. Besonders nützlich ist dies bei Reisen ins Ausland, bei denen es Benutzern theoretisch möglich ist, ganz gleich wohin sie in Europa und zunehmend auch außerhalb Europas auch reisen, Anrufe vorzunehmen und entgegenzunehmen. Allerdings haben der Missbrauch und die offensichtliche Unfähigkeit von Netzbetreibern, mit diesem Problem fertig zu werden, dazu geführt, dass eine zunehmende Anzahl von Service Providern, die sich in der Mitte zwischen den Netzbetreibern und den Mobiltelefonbenutzern befinden, heute die Einsatzfähigkeit bzw. Nutzbarkeit der GSM-SIM-Karten absichtlich beschränken. Zu diesen Beschränkungen zählt es, dass die Funktionsfähigkeit der SIM-Karte nur auf das Telefon beschränkt wird, mit dem die Karte ausgeliefert worden ist, wobei diese Einschränkung jedoch praktisch den ursprünglichen Sinn und Zweck der Smartcard aufhebt. Als Folge der Mobilfunkpiraterie haben bestimmte Service Provider auch den gänzlichen Verzicht auf die SIM-Karten vorgeschlagen, wobei sie das Argument vorbringen, dass dies eine neue Stufe der Komplexität mit sich bringt, welche von Kriminellen genutzt werden kann.

[0009] Als Folge erheblicher Verlust, die ausländische Netzbetreiber erlitten haben, sperren eine Reihe von ausländischen Service Providern in einer Reihe von Ländern mittlerweile GSM-SIM-Karten, so dass diese im Ausland nicht mehr eingesetzt werden können. In Zukunft müssen Teilnehmer bzw. Vertragskunden von Netzen über diese Service Provider hohe Einlagen leisten, wenn sie ihre Telefone auf Auslandsreisen nutzen möchten. Ferner haben einige Service Provider aus dem Ausland mittlerweile das internationale Roaming eingestellt.

[0010] Das U.S. Patent US-A-5.337.345 offenbart ein Mobiltelefon mit einer Senderschaltkreisanordnung, die dazu dient, es zu verhindern, das unbefugte Anrufe übertragen werden. Die Schaltkreisanordnung stellt sicher, dass das Telefon nur Dienst- und Anrufanforderungen überträgt, die eine Geräteserienummer (ESN als englische Abkürzung von Equipment bzw. Electronic Serial Number) aufweist, die durch den Hersteller dauerhaft in einem nicht löschbaren ESN-Speicher in dem Telefon gespeichert wird. Die Schaltkreisanordnung weist auch eine ESN-Detektionsschaltkreisanordnung auf, die die Bitposition einer ESN in einer Dienst- oder Anrufanforderung bestimmt, und die ESN in der Anforderung entweder mit der in dem ESN-Speicher gespeicherten ESN vergleicht und nur Anforderungen überträgt, die übereinstimmende ESNs aufweisen, oder indem sie die ESN aus dem ESN-Speicher direkt in die Anforderungen einfügt, wenn diese übertragen werden. Somit ist jede ESN eindeutig, und wird durch den Hersteller einem Telefon zugeordnet.

[0011] WO 98/10611A offenbart ein Mobiltelefon mit einem elektronischen Speicher, der ein System aufweist, das einen Missbrauch des Speichers bzw. ungefugte Eingriffe an dem Speicher verhindern soll. Ein zugeordneter Prozessor weist eine Logik auf, die eingesetzt wird, um eine einseitig gerichtete Hash-Berechnung an dem Speicherinhalt vorzunehmen, wobei ein Hash-Prüfwert des Inhalts abgeleitet wird. Der Hash-Prüfwert wird mit einem authentifizierten gültigen Hash-Wert verglichen, der aus dem authentischen Speicherinhalt abgeleitet wird. Ein Unterschied zwischen dem Hash-Prüfwert und dem gültigen Hash-Wert kann einen Speichermissbrauch anzeigen. Aufgabe der vorliegenden Erfindung ist es, ein Verfahren und eine Vorrichtung zur Reduzierung von Missbrauch bereitzustellen, indem der Speicher sicherer gestaltet wird.

ZUSAMMENFASSUNG DER ERFINDUNG

[0012] Vorgesehen ist gemäß einem ersten Aspekt der vorliegenden Erfindung ein Verfahren gemäß dem gegenständlichen Anspruch 1.

[0013] Vorgesehen ist gemäß einem zweiten Aspekt der vorliegenden Erfindung eine Vorrichtung gemäß dem gegenständlichen Anspruch 5.

[0014] Vorgesehen ist gemäß einem dritten Aspekt der vorliegenden Erfindung ein Mobiltelefonsystem gemäß dem gegenständlichen Anspruch 8.

[0015] Weitere Merkmale und Vorteile der vorliegenden Erfindung werden aus den beigefügten Zeichnungen und aus der genauen Beschreibung sowie den anhängigen und folgenden Ansprüchen deutlich.

KURZE BESCHREIBUNG DER ZEICHNUNGEN

[0016] Die vorliegende Erfindung ist beispielhaft und ohne einzuschränken in den Abbildungen der beigefügten Zeichnungen veranschaulicht, wobei darin die gleichen Elemente mit den gleichen Bezugszeichen bezeichnet sind. In den Zeichnungen zeigen:

[0017] Fig. 1 ein elektronisches System mit einer Schaltkreisanordnung zur Missbrauchsverhinderung gemäß einem Ausführungsbeispiel;

[0018] Fig. 2 ein Blockdiagramm der Flash-Speichervorrichtung gemäß einem Ausführungsbeispiel;

[0019] Fig. 3 eine Speicherabbildung des OTP-Registers oder des Schutzregisters gemäß einem Ausführungsbeispiel;

[0020] Fig. 4 eine zulässige Wort-weite Adressiert für das Schutzregister gemäß einem Ausführungsbeispiel;

[0021] Fig. 5 eine zulässige Byte-weite Adressierung für das Schutzregister gemäß einem Ausführungsbeispiel;

[0022] Fig. 6 eine Lesekonfigurationstabelle der Flash-Speichervorrichtung eines Ausführungsbeispiels;

[0023] Fig. 7 ein Flussdiagramm des Steuerverfahrens des elektronischen Systems gemäß einem Ausführungsbeispiel; und

[0024] Fig. 8 ein Flussdiagramm des Verfahrens zur Missbrauchsverhinderung gemäß einem Ausführungsbeispiel.

GENAUE BESCHREIBUNG DER ERFINDUNG

[0025] Beschrieben werden ein Verfahren und eine Vorrichtung zum Steuern der Nutzung von und des Zugriffs auf ein elektronisches System. Im Besonderen werden ein Verfahren und eine Vorrichtung beschrieben, die eine missbräuchliche Nutzung eines Mobiltelefons verhindern sollen, wobei ein eindeutiges Identifikationssystem vor eine Speichervorrichtung bereitgestellt wird, das es ermöglicht, einen Identifikationscode in einer elektronischen Anwendung zu lesen, jedoch nicht zu modifizieren. In einem Ausführungsbeispiel ist ein Mobiltelefon-OEM mit einer Speichervorrichtung mit einem eindeutigen Identifikationscode versehen oder einer Nummer, festgelegt durch den Hersteller des Speicherbausteins bzw. der Speichervorrichtung in einem dauerhaft sperrbaren Speicher, oder in einem einmal programmierbaren (OTP) Speicherraum. In einem alternativen Ausführungsbeispiel legt der Mobiltelefon-OEM einen eindeutigen Identifikationscode (ID-Code) in einem einmal programmierbaren (OTP als englische Abkürzung von One-Time Programmable) Speicherraum des Flash-Speichers fest. Der Identifikationscode in dem OTP-Speicherraum ist in keinem der Ausführungsbeispiele modifizierbar.

[0026] Im Betrieb beider Ausführungsbeispiele prüft die Systemsoftware des Mobiltelefons, ob eine Übereinstimmung zwischen dem eindeutigen Identifikationscode des OTP-Speicherraums und eines anderen Komponentencodes gegeben ist, bevor mit dem Mobiltelefon Anruf vorgenommen werden dürfen. Zu den beabsichtigten Vorteilen der Schaltkreisanordnung zur Missbrauchsverhinderung können das Verhindern des missbräuchlichen Clonens von Mobiltelefonen zählen sowie das Verhindern des Diebstahls von Mobilfunksprechzeit und des Missbrauchs von Telefonsubventionen. Ferner umfassen die beabsichtigten Vorteile das Verhindern des Zugriffs auf elektronische Systeme, das Verhindern der Nutzung gestohlener Computer, das Verhindern der illegalen oder unbefugten Nutzung von Computern und das Erhöhen der Sicherheit elektronischer Systemkonstruktionen, indem es verhindert wird, dass ein Anwendungscode aus dem Speicher derartiger Systeme gelesen wird. Ferner kann der eindeutige Identifikationscode der Speichervorrichtung gemäß einem Ausführungsbeispiel als Freigabeeinrichtung eingesetzt werden, um dem Stand der Technik entsprechende Techniken zur Verhinderung des missbräuchlichen Clonens in Bezug auf Mobiltelefone zu verbessern.

[0027] Wie dies bereits vorstehend im Text beschrieben worden ist, handelt es sich um eine Art des missbräuchlichen Clonens von Mobiltelefonen, wenn die Mobiltelefone eines Mobilfunkanbieters so modifiziert werden, dass sie mit einem anderen Mobilfunkanbieter einsatzfähig sind. Für gewöhnlich erfolgt dies durch das Entfernen und den Austausch oder das Löschen und neuerliche Programmieren des Speichers des Mobiltelefons, da der Speicher die Mobiltelefonsoftware aufweist, die für einen bestimmten Mobilfunkanbieter spezifisch ist. Das missbräuchliche Klonen bzw. Clonen von Mobiltelefonen kann verhindert werden, indem der Mobiltelefonspeicher, die Mobiltelefon-Hardware und der Mobiltelefon-Mikrocontroller miteinander verbunden oder verknüpft werden. Diese Verbindung verhindert das missbräuchliche Clonen durch Sperren der Hardware eines bestimmten Mobiltelefons für einen bestimmten Service Provider. Das hierin beschriebene und beanspruchte Verfahren und die Vorrichtung stellen somit eine Lösung für die dem Stand der Technik entsprechende Piraterie bereit, indem der OEM und der Service Provider dabei unterstützt werden, das Telefon praktisch zu verfolgen, wobei dies verhindert, dass der Benutzer oder der missbräuchlich handelnde Händler die ESN oder IMEI oder einen anderen elektronischen Identifikationscode modifizieren.

[0028] Die Vorrichtung zur Verhinderung von Missbrauch gemäß einem Ausführungsbeispiel bietet zwei Möglichkeiten für einen eindeutigen Identifikationscode innerhalb des Flash-Speicherbausteins. Der Mobiltelefon-OEM kann einen oder beide Codes als Teil eines Verschlüsselungsmechanismus oder eines Quittungsaustauschmechanismus der Systemsoftware des Mobiltelefons beim Quittungsaustausch zwischen dem Flash-Speicher, dem Flash-Speichercode in dem Flash-Speicher und dem Mikrocontroller oder der Zentraleinheit des Mobiltelefons verwenden.

Wenn ein anderer Speicherbaustein in das Mobiltelefon eingesetzt worden ist, kann die Ausrichtung nicht verifiziert werden, und der Zugriff auf das Mobilfunknetz unter Verwendung des Mobiltelefons wird untersagt.

[0029] Die Abbildung aus Fig. 1 zeigt ein elektronisches System **100**, das eine Schaltkreisanordnung zur Verhinderung von Missbrauch gemäß einem Ausführungsbeispiel umfasst. Das elektronische System **100** umfasst eine Zentraleinheit (CPU) **102**, die mit einem Bus **104** gekoppelt ist. Eine Mehrzahl von anwendungsspezifischen Schaltungen (ASICs) **106**–**108** kann mit dem Bus **104** gekoppelt werden, um die Funktionen des jeweiligen elektronischen Systems **100** zu ermöglichen, wobei das Ausführungsbeispiel jedoch diesbezüglich nicht beschränkt ist. Ein Hauptspeicher **110** ist gemeinsam mit einem Zusatzspeicher **112** mit dem Bus **104** gekoppelt. Bei dem Zusatzspeicher **112** handelt es sich um eine kleine Speicheranordnung, die außerhalb des Hauptspeicheranordnungsraums **110** angeordnet ist. Der Zusatzspeicher **112** ist somit für das Speichern mindestens eines eindeutigen Identifikationscodes vorgesehen. In einem Ausführungsbeispiel handelt es sich bei dem Hauptspeicher **110** um einen Flash-Speicher, wobei das Ausführungsbeispiel darauf jedoch nicht beschränkt ist. Ferner kann es sich bei dem Zusatzspeicher **112** um einen Flash-Speicher handeln, wobei das Ausführungsbeispiel darauf jedoch nicht beschränkt ist. Die Sicherheit des elektronischen Systems **100** wird durch das Platzieren des Zusatzspeichers **112** auf dem gleichen Chip wie die Hauptspeicheranordnung **110** optimiert, wobei das Ausführungsbeispiel jedoch nicht darauf beschränkt ist. In einem Ausführungsbeispiel umfasst das elektronische System **100** ein Mobiltelefon. In einem alternativen Ausführungsbeispiel umfasst das elektronische System **100** ein elektronisches System auf Computerbasis. Die vorliegende Erfindung verwendet in der folgenden Beschreibung zwar ein Mobiltelefon als Beispiel für das elektronische System **100**, wobei das Ausführungsbeispiel jedoch nicht darauf beschränkt ist.

[0030] Die Abbildung aus Fig. 2 zeigt ein Blockdiagramm des Flash-Speicherbausteins **110** gemäß einem Ausführungsbeispiel. Eine Command User Interface (CUI) **202** dient als Schnittstelle zwischen dem Mikroprozessor oder Mikrocontroller des Mobiltelefons und des inneren Betriebs des Flash-Speicherbausteins **110**. Eine Write State Machine (WSM) bzw. Schreibzustandsmaschine **204** führt automatisch die für die Programmierungs- und Löschoperationen, einschließlich Verifizierung, erforderlichen Algorithmen und Zeitsteuerungen aus. Der Flash-Speicherbaustein **110** liest, programmiert und löscht somit in dem System über die CPU oder den Mikrocontroller des Mobiltelefons. An die CUI **202** bereitgestellte Befehle ermöglichen dem Benutzer den Zugriff auf die Haupt-Flash-Anordnung **206** und alternativ auf die einmal programmierbaren (OTP) Register **210**.

[0031] Der Speicherbaustein gemäß einem Ausführungsbeispiel umfasst ein Register **210** des Zusatzspeichers, das verwendet wird, um Missbrauch zu verhindern und um die Sicherheit eines Systemdesigns zu erhöhen. Das OTP-Register **210** oder Schutzregister umfasst eine 128-Bit-Nummer, die an einem internen Platz des Bausteins bzw. der Vorrichtung gespeichert ist. Das 128-Bit-Schutzregister ermöglicht eine Identifikation des eindeutigen Flash-Speicherbausteins, wobei die 128-Bit-Nummer zur Verhinderung von Missbrauch in elektronischen Vorrichtungen wie etwa Mobiltelefonen verwendet werden kann, wobei das Ausführungsbeispiel darauf jedoch nicht beschränkt ist. Zum Beispiel kann die in dem Schutzregister enthaltene Nummer verwendet werden, um die Flash-Komponente an andere Systemkomponenten anzupassen, welche die CPU, eine ASIC und einen Signalprozessor umfassen, wobei eine Gerätesubstitution verhindert wird, wobei das Ausführungsbeispiel jedoch nicht darauf beschränkt ist.

[0032] Die Abbildung aus Fig. 3 zeigt eine Speicherabbildung des OTP-Registers oder des Schutzregisters gemäß einem Ausführungsbeispiel. Das 128-Bit-Schutzregister **300** umfasst zwei Segmente **302**–**304**, wobei jedes Segment **64** Bits umfasst, wobei das Ausführungsbeispiel jedoch diesbezüglich nicht beschränkt ist. Das erste Segment **302** des Schutzregisters **300** umfasst eine eindeutige Teilnummer, die durch den Hersteller des Speicherbausteins zum Zeitpunkt der Fertigung vorab programmier wird. Die Nummer ist für jedes hergestellte Gerät eindeutig. In einem Ausführungsbeispiel wird diese vorab programmierte Nummer (64 Bits) unter Verwendung einer bestimmten Kombination abgeleitet, welche die Fab-Identifikation (ID)(8 Bit), die Chargen-ID (32 Bits), die Wafer-ID (8 Bits), die X-Position auf dem Halbleiterchip (8 Bits) und die Y-Position auf dem Halbleiterchip (8 Bits) umfasst, wobei das Ausführungsbeispiel diesbezüglich jedoch nicht beschränkt ist. Die eindeutige Identifikationsnummer kann verschlüsselt werden, wobei das Ausführungsbeispiel jedoch nicht darauf beschränkt ist. Nach der Programmierung kann der Inhalt des ersten Segments **302** des Schutzregisters **300** nicht verändert werden, da das erste Segment **302** des Schutzregisters **300** gesperrt ist.

[0033] Der OTP-Speicherraum **300** oder das Schutzregister können in zwei Abschnitten gesperrt werden. Nach der Programmierung des durch den Hersteller programmierbaren Segments des Schutzregisters **300**, des ersten Segments **302** oder der ersten 64 Bits (4 Wörter oder 8 Bytes) des Schutzregisters **300** wird das erste Segment **302** des OTP-Spei-

cherraums **300** gesperrt, indem zusätzlich ein Sperrbit **312** geschrieben wird. Das erste Segment **302** des OTP-Speicherraums **300** wird gesperrt, indem der OTP-Schutzprogrammbefehl zum Programmieren oder Schreibenn von „FFFE" (Wort-weit) oder von „FE" (Byte-weit) an die Adressposition **320** LOCK bzw. Sperren verwendet werden. Dieser Befehl programmiert oder legt das Bit 0 des Speicherplatzes PR-LOCK **312** auf 0 fest, wobei die ersten 64 Bits **302** ausgesperrt werden. Nach der Festlegung der Aussperrbits **312** bis **314** sind keine weiteren Veränderungen der in den entsprechenden Segmenten des Schutzregisters gespeicherten Werte zulässig. Versuche zum Programmieren eines gesperrten Schutzregistersegments führen zu einem Statusregister-Fehler. Der Sperrzustand des Schutzregisters ist nicht umkehrbar, wobei das Ausführungsbeispiel diesbezüglich jedoch nicht beschränkt ist.

[0034] Das zweite Segment des Schutzregisters **304** umfasst ein Segment, dass durch den Benutzer auf einen durch den Benutzer ausgewählten Wert programmierbar ist. Die Schutzregisterbits können durch den Benutzer unter Verwendung eines Schutzprogramm- oder OTP-Programmbefehls mit zwei Zyklen programmiert werden. Der 64-Bit-Registerwert wird mit jeweils 16 Bits für Wort-weite Teile und mit jeweils 8 Bits gleichzeitig für Byte-weite Teile programmiert. Bei der Programmierung des Schutzregisters **300** wird ein Befehl Schutzprogrammeinrichtung C0H während dem ersten Zyklus geschrieben. Der erste Zyklus bereit die CUI auf einen OTP-Programmbetrieb vor. Der zweite Zyklus speichert Adressen und Dateninformationen zwischen und startet die Schreibzustandsmaschine, so dass der OTP-Programmalgorithmus an das OTP-Register ausgeführt wird, wobei das folgende Schreiben an den Speicherbaustein den spezifizierten Platz des OTP-Registers programmiert. Die Abbildung aus **Fig. 4** zeigt die zulässige Wort-weite Adressierung für die Schutzregister eines Ausführungsbeispiels. Ein Befehl Anordnung Lesen wird zum Lesen der Anordnungsdaten nach der Programmierung verwendet. Versuche zur Adressierung von Schutzprogrammbefehlen außerhalb des definierten Schutzregister-Adressraums führen zu einem Statusregister-Fehler.

[0035] Nach der Programmierung des durch den Benutzer programmierbaren Segments des Schutzregisters wird das zweite Segment **304** oder die zweiten 64 Bits des Schutzregisters **300**, das zweite Segment **304** des OTP-Speicherraums **300** durch das Schreiben eines zusätzlichen Sperrbits **314** gesperrt. Das zweite Segment **304** des OTP-Speicherraums **300** wird gesperrt unter Verwendung des OTP-Schutzprogrammbefehls zum Programmieren oder Schreiben von „FFFD" (Wort-weit) oder von „FD" (Byte-weit) an die Adressposition „LOCK" (Sperren) **320**. Dieser Befehl programmiert oder setzt das Bit 1 der Position **314** PR-LOCK auf 0, wobei die zweiten 64 Bits **304** ausgesperrt werden. Nach dem Festlegen der Sperr- bzw. Ausperrbits **312** bis **314** sind an den in den entsprechenden Segmenten des Schutzregisters gespeicherten Werten keine weiteren Änderungen zulässig. Versuche zur Programmierung eines gesperrten Schutzregistersegments führen zu einem Statusregisterfehler. Der Schutzregister-Sperrzustand ist nicht umkehrbar, wobei das Ausführungsbeispiel diesbezüglich jedoch nicht beschränkt ist.

[0036] Der Flash-Speicherbaustein gemäß einem Ausführungsbeispiel weist zwei Schreibmodi und vier Lesemodi auf. Die beiden Schreibmodi umfassen Programmieren (Program) und Block Löschen (Block Erase). Die vier Lesemodi umfassen Anordnung Lesen (Read Array), Konfiguration Lesen (Read Configuration), Status Lesen (Read Status) und Anforderung Lesen (Read Query). Der entsprechende Lesemodusbefehl wird an die CUI erteilt, um in den entsprechenden Lesemodus einzutreten. Das Schutzregister wird in dem Modus Read Configuration gelesen und ist als solches in der Speicheranordnung nicht adressierbar.

[0037] Der Modus Read Configuration gibt den Hersteller-/Gerätebezeichner und den Inhalt des Schutzregisters, die einmal programmierbare (OTP) Missbrauchsverhinderungsnummer aus. Die Vorrichtung wechselt in den Modus Read Configuration, indem der Befehl Read Configuration (Konfiguration Lesen), 90 H, an die CUI gelesen wird. Die Abbildung aus **Fig. 6** zeigt eine Lesekonfigurationstabelle des Flash-Speicherbausteins gemäß einem Ausführungsbeispiel. Die Lesekonfigurationstabelle ist eine Tabelle mit spezifizierten Informationen, die in dem Lesekonfigurationsmodus während Lesezyklen aus Adressen des Flash-Speicherbausteins ausgelesen werden. In dem Lesekonfigurationsmodus rufen Lesezyklen von den Adressen aus den Abbildungen der **Fig. 4** und **Fig. 5** die Werte in dem Schutzregister ab.

[0038] Die Abbildung aus **Fig. 7** zeigt ein Flussdiagramm des Steuerverfahrens für das elektronische System gemäß einem Ausführungsbeispiel. Der Ablauf beginnt in dem Schritt **702**, wobei mindestens ein eindeutiger Code in einen Zusatzspeicher des elektronischen Systems programmiert wird. Der Zusatzspeicher ist ein dauerhaft sperrbarer Speicher, der außerhalb des Hauptspeicheranordnungsraums angeordnet ist. Der Zusatzspeicher kann in einem Konfigurationsspeicherraum angeordnet sein, wobei das Ausführungsbeispiel jedoch nicht darauf beschränkt ist. Der eindeutige Code wird in dem Schritt **704** mit mindestens einem Komponentencode verglichen. Der Einsatz des elektronischen Systems wird auf der Basis eines vordefinierten Verhältnisses zwischen dem eindeutigen Code und dem Komponentencode verglichen. In dem Schritt **706** wird bestimmt, ob das vorbestimmte Verhältnis erfüllt ist oder nicht. In einem

Ausführungsbeispiel handelt es sich bei dem vorbestimmten Verhältnis um eine Übereinstimmung zwischen dem eindeutigen Code und dem Komponentencode, wobei das Ausführungsbeispiel jedoch nicht darauf beschränkt ist. Wenn das vorbestimmte Verhältnis erfüllt ist, so wird die Nutzung des oder der Zugriff auf das elektronische System in dem Schritt **708** zugelassen. Wenn das vorbestimmte Verhältnis nicht erfüllt ist, so wird der Einsatz des elektronischen Systems in dem Schritt **710** nicht zugelassen.

[0039] Das elektronische System umfasst Mobiltelefone, eingebettete bzw. integrierte Systeme und Set-Top-Boxen, wobei das Ausführungsbeispiel jedoch nicht darauf beschränkt ist. Der Hauptspeicher eines Ausführungsbeispiels ist ein Flash-Speicher. Der Zusatzspeicher eines Ausführungsbeispiels ist ein Flash-Speicher. In einem Ausführungsbeispiel sind der Hauptspeicher und der Zusatzspeicher auf der gleichen integrierten Schaltung oder dem gleichen Chip angeordnet, wobei das Ausführungsbeispiel jedoch nicht darauf beschränkt ist. In einem alternativen Ausführungsbeispiel kann unter Verwendung eines seriellen Ports und eines Ein-Ausgabe-Ports (E/A-Ports) auf den Zusatzspeicher zugegriffen werden.

[0040] In einem Ausführungsbeispiel wird der eindeutige Code in einem Segment des Zusatzspeichers gespeichert, während der Komponentencode in einem einmal programmierbaren Speicher mindestens einer Komponente des elektronischen Systems festgelegt oder gespeichert wird. Die Komponente des elektronischen Systems kann einen Speicher, einen Mikrocontroller, eine anwendungsspezifische integrierte Schaltung, eine Zentraleinheit, einen Signalprozessor oder eine SIM-Karte umfassen, wobei das Ausführungsbeispiel diesbezüglich jedoch nicht beschränkt ist.

[0041] In einem alternativen Ausführungsbeispiel wird der eindeutige Code in einem ersten Segment des Zusatzspeichers gespeichert, und der Komponentencode wird in einem zweiten Segment des Zusatzspeichers gespeichert, wobei das Ausführungsbeispiel darauf jedoch nicht beschränkt ist. In diesem alternativen Ausführungsbeispiel wird der eindeutige Code zur Verschlüsselung eines Identifikationscodes verwendet. Der Identifikationscode kann mindestens ein Bit umfassen, das in dem Hauptspeicher des elektronischen Systems gespeichert ist. Ferner kann der Identifikationscode oder die Identifikationsnummer einen Identifikationscode umfassen, der sich in der Systemsoftware des elektronischen Systems befindet. Der verschlüsselte Identifikationscode wird mit dem in dem Zusatzspeicher gespeicherten Komponentencode verglichen. Der Einsatz des und der Zugriff auf das elektronische System wird gesperrt, wenn der verschlüsselte Identifikationscode nicht mit dem Komponentencode übereinstimmt.

[0042] In einem anderen Ausführungsbeispiel wird der Komponentencode zum Verschlüsseln des Identifikationscodes verwendet. Der verschlüsselte Identifikationscode wird mit dem in dem Zusatzspeicher gespeicherten eindeutigen Code verglichen. Der Einsatz des und der Zugriff auf das elektronische System wird gesperrt, wenn der verschlüsselte Identifikationscode nicht mit dem eindeutigen Code übereinstimmt.

[0043] In einem alternativen Ausführungsbeispiel wird der Komponentencode unter Verwendung des eindeutigen Codes verschlüsselt. Die Nutzung des und der Zugriff auf das elektronische System werden gesperrt, wenn der verschlüsselte Komponentencode nicht mit mindestens einem in dem Hauptspeicher oder in der Systemsoftware des elektronischen Systems gespeicherten Code übereinstimmt.

[0044] Die Abbildung aus Fig. 8 zeigt ein Flussdiagramm des Verfahrens zum Verhindern eines Missbrauchs gemäß einem Ausführungsbeispiel. Der Ablauf beginnt in dem Schritt **802**, in dem ein eindeutiger Code in ein Schutzregister eines Zusatzspeichers des Mobiltelefons programmiert wird. Wie dies bereits vorstehend im Text beschrieben worden ist, handelt es sich bei dem Zusatzspeicher um einen dauerhaft sperrbaren Speicher oder einen einmal programmierbaren Speicher. Wie dies bereits vorstehend im Text beschrieben worden ist, wird ein eindeutiger Code durch den Hersteller des Speicherbausteins in ein erstes 64-Bit-Segment des Schutzregisters programmiert und ein Sperrbit wird gesetzt, wobei die Modifikation des eindeutigen Codes untersagt ist. Nach dem Empfang des Speicherbausteins durch den Mobiltelefon-OEM kann der durch den Hersteller festgelegte eindeutige Code verwendet werden, um das Mobiltelefon vor missbräuchlichem Clonen zu schützen. Ferner ist ein zweites 64-Bit-Segment des Schutzregisters vorgesehen, wobei ein eindeutiger Code durch den Mobiltelefon-OEM programmiert werden kann. Nach der Programmierung des eindeutigen Codes durch den Mobiltelefon-OEM wird ein Sperrbit gesetzt, wobei eine Modifikation des eindeutigen Codes untersagt ist. Jeder programmierte Code oder beide programmierte Codes können in einem System zur Verhinderung von Missbrauch durch den Mobiltelefon-OEM verwendet werden.

[0045] Der eindeutige Code wird in dem Schritt **804** mit dem Komponentencode verglichen. Der Einsatz des Mobiltelefons wird auf der Basis eines vorher definierten Verhältnisses zwischen dem eindeutigen Code und dem Komponentencode geregelt bzw. gesteuert. In dem Schritt **806** wird bestimmt, ob das vorher definierte Verhältnis erfüllt ist oder nicht. In einem Ausführungsbeispiel handelt es sich bei dem vorher festgelegten Verhältnis um eine Übereinstimmung zwischen dem eindeutigen Code und dem Kompo-

nentencode, die durch eine Softwareabfrage verifiziert wird, wobei das Ausführungsbeispiel darauf jedoch nicht beschränkt ist. Wenn das vorher festgelegte Verhältnis erfüllt ist, so wird der Einsatz des Mobiltelefons in dem Schritt **808** zugelassen. Wenn das vorher festgelegte Verhältnis nicht erfüllt ist, wird der Einsatz des Mobiltelefons in dem Schritt **810** nicht zugelassen. Wenn in einem alternativen Ausführungsbeispiel das vorher festgelegte Verhältnis nicht erfüllt ist, kann eine eingeschränkte Aktivierung des Mobiltelefons zu Nachführungszwecken zugelassen werden, wobei das Ausführungsbeispiel darauf jedoch nicht beschränkt ist. Wenn das vorher festgelegte Verhältnis in einem alternativen Ausführungsbeispiel nicht erfüllt ist, kann eine Nachricht bzw. eine Meldung angezeigt werden, die den Benutzer auffordert, Kontakt mit dem Mobilfunkanbieter aufzunehmen.

[0046] Das vorher festgelegte Verhältnis zwischen dem eindeutigen Code und dem Komponentencode kann eine Übereinstimmung zwischen den Codes darstellen, wobei das Ausführungsbeispiel jedoch nicht darauf beschränkt ist. In alternativen Ausführungsbeispielen kann der Einsatz des Mobiltelefons durch den Einsatz des Komponentencodes zur Verschlüsselung oder Entschlüsselung des eindeutigen Codes geregelt werden. In anderen alternativen Ausführungsbeispielen kann der Einsatz des Mobiltelefons durch den Einsatz des eindeutigen Codes zum Verschlüsseln oder Entschlüsseln des Komponentencodes geregelt werden. In weiteren alternativen Ausführungsbeispielen kann der Einsatz des Mobiltelefons durch den Einsatz des eindeutigen Codes und des Komponentencodes als ein Verschlüsselungs-Validierungsschlüssel für die Systemsoftware des Mobiltelefons geregelt werden.

[0047] In einem Ausführungsbeispiel wird der eindeutige Code in einem Segment des Zusatzspeichers gespeichert, während der Komponentencode in einem dauerhaft sperrbaren oder einem einmal programmierbaren Speicher mindestens einer Komponente des Mobiltelefons festgelegt oder gespeichert wird. Der Komponentencode kann durch den Mobiltelefon-OEM oder durch den Mobilfunkanbieter programmiert werden. Alternativ kann der Mobiltelefon-OEM einen durch den Mobilfunkanbieter vorgesehenen Komponentencode programmieren. Auf diese Weise wird eine Reihe von Komponenten des Mobiltelefons miteinander verknüpft bzw. verbunden, wodurch der Einsatz des Mobiltelefons verhindert wird, wenn eine verbundene Komponente, wie zum Beispiel ein Flash-Speicher, entfernt und durch eine andere Komponente ersetzt wird. Die Komponente des Mobiltelefons kann einen Speicher, einen Mikrocontroller, eine anwendungsspezifische integrierte Schaltung, eine Zentraleinheit und einen Signalprozessor umfassen, wobei das Ausführungsbeispiel jedoch nicht darauf beschränkt ist. Ein GSM-Mobiltelefon verwendet eine portable SIM-Karte, welche die persönlichen Daten zu einem Benutzer aufweist, zu denen unter anderem, ohne darauf beschränkt zu sein, Abrechnungsdaten, ein Adressbuch und Vorzüge für die Handhabung von Anrufen zählen. In diesem GSM-System kann die SIM-Karte zwar auch in einem anderen Telefon eingesetzt werden, allerdings kann ein Komponentencode in einer Komponente der Infrastruktur des Mobiltelefons festgelegt werden, wobei die Infrastruktur ein Benutzerprofil umfasst, das sich in der SIM-Karte befindet.

[0048] In einem alternativen Ausführungsbeispiel wird der eindeutige Code in einem ersten Segment des Zusatzspeichers gespeichert, und der Komponentencode wird in einem zweiten Segment des Zusatzspeichers gespeichert, wobei das Ausführungsbeispiel jedoch nicht darauf beschränkt ist. In diesem alternativen Ausführungsbeispiel wird der eindeutige Code zum Verschlüsseln einer Identifikationsnummer verwendet. Diese Identifikationsnummer kann eine ESN, eine IMEI und eine Nummer umfassen, die von einem Mobilfunkanbieter in einem Signal bereitgestellt werden, das von dem Mobiltelefon von einer Mobilfunkbasisstation empfangen wird. Ferner kann die Identifikationsnummer eine Nummer aufweisen, die in dem Hauptspeicher des elektronischen Systems gespeichert ist. Darüber hinaus kann die Identifikationsnummer eine Bezeichnernummer umfassen, die sich in der Systemsoftware des elektronischen Systems befindet. Die verschlüsselte Identifikationsnummer wird mit dem Komponentencode verglichen, der in dem Zusatzspeicher gespeichert ist. Der Einsatz des Mobiltelefons wird zugelassen, wenn die verschlüsselte Identifikationsnummer mit dem Komponentencode übereinstimmt.

[0049] In einem weiteren alternativen Ausführungsbeispiel kann der Mobilfunkanbieter den eindeutigen Code aus dem Mobiltelefon lesen und den eindeutigen Code auf verschlüsselte Art und Weise in die GSM-SIM-Karte programmieren. Die Software des Mobiltelefons vergleicht den eindeutigen Code mit dem programmierten Code, wenn versucht wird, das Mobiltelefon zu aktivieren. Alternativ kann ein sich in einem Speicher der GSM-SIM-Karte befindender Code in den dauerhaft sperrbaren Speicher programmiert werden, wobei die Software des Mobiltelefons die beiden Codes vergleicht.

[0050] In einem Ausführungsbeispiel wird der Einsatz des Mobiltelefons verhindert, indem der Zugriff auf den Hauptspeicher des Mobiltelefons untersagt wird, wobei das Ausführungsbeispiel diesbezüglich nicht beschränkt ist. In einem alternativen Ausführungsbeispiel wird die Nutzung des Mobiltelefons zugelassen, indem der eindeutige Code und der Komponentencode zum Entschlüsseln der Systemsoftware des Mobiltelefons verwendet werden. In einem alternativen Ausführungsbeispiel wird der Einsatz des Mobiltelefons durch den Einsatz des eindeutigen

Codes in Verbindung mit einem Verschlüsselungsschlüssel zugelassen.

[0051] In der genauen Beschreibung wurden zwar Ausführungsbeispiele beschrieben, welche ein Flash-EPROM verwenden, wobei die vorliegende Erfindung jedoch auch in Verbindung mit jedem nichtflüchtigen beschreibbaren Speicher verwendet werden kann. Die vorliegende Erfindung wurde zwar in Bezug auf bestimmte Ausführungsbeispiele beschrieben, wobei jedoch ersichtlich ist, dass verschiedene Modifikationen und Abänderungen in Bezug auf diese Ausführungsbeispiele möglich sind, ohne dabei vom umfassenderen Umfang der Erfindung gemäß der Definition in den Ansprüchen abzuweichen. Somit dienen die Beschreibung und die Zeichnungen Zwecken der Veranschaulichung, ohne dass sie dabei einschränken.

Patentansprüche

1. Verfahren zum Steuern des Einsatzes eines elektronischen Systems (**100**), wobei das Verfahren folgendes umfasst:
das Abrufen eines eindeutigen Codes aus einem sperrbaren Zusatzspeicher (**112**) des elektronischen Systems, wobei der eindeutige Code zumindest teilweise auf einer vorprogrammierten eindeutigen Nummer basiert, die dem Zusatzspeicher zugeordnet ist; und
das Steuern (**706**) des elektronischen Systems auf der Basis eines vordefinierten Verhältnisses zwischen dem eindeutigen Code und einem Komponentencode, wobei der Komponentencode mindestens einer Komponente in dem elektronischen System zugeordnet ist.

2. Verfahren nach Anspruch 1, wobei das Steuern des Einsatzes des elektronischen Systems auf der Basis eines vordefinierten Verhältnisses zwischen dem eindeutigen Code und dem Komponentencode folgendes umfasst:
das Verschlüsseln einer Identifikationsnummer unter Verwendung des eindeutigen Codes als Verschlüsselungsschlüssel, so dass ein verschlüsselter Identifikationscode gebildet wird, wobei die Identifikationsnummer eine Nummer umfasst, die aus der Gruppe ausgewählt wird, welche eine Geräteseriennummer (ESN), eine internationale Mobilgerätekennung (IMEI), eine durch einen Mobilfunkanbieter in einem Signal bereitgestellte Nummer oder eine sich in dem Hauptspeicher befindende Nummer umfasst; und
das Deaktivieren des Einsatzes des elektronischen Systems, wenn der verschlüsselte Identifikationscode nicht mit dem Komponentencode übereinstimmt.

3. Verfahren nach Anspruch 1, wobei das Steuern des Einsatzes des elektronischen Systems auf der Basis eines vordefinierten Verhältnisses zwischen dem eindeutigen Code und dem Komponentencode folgendes umfasst:
das Verschlüsseln des Komponentencodes unter Verwendung des eindeutigen Codes, um einen verschlüsselten Komponentencode zu bilden; und
das Deaktivieren des Einsatzes des elektronischen Systems, wenn der verschlüsselte Komponentencode nicht mit mindestens einem Code übereinstimmt, der in einem Hauptspeicher des elektronischen Systems gespeichert ist.

4. Verfahren nach Anspruch 2, wobei der eindeutige Code in einem ersten Segment des Zusatzspeichers gespeichert ist, und wobei der Komponentencode in einem zweiten Segment des Zusatzspeichers gespeichert ist, und wobei die dem Zusatzspeicher zugeordnete vorprogrammierte eindeutige Nummer eine Teilnummer des Zusatzspeichers darstellt.

5. Vorrichtung zur Steuerung des Einsatzes eines Mobiltelefons, wobei die Vorrichtung folgendes umfasst:
einen sperrbaren Zusatzspeicher (**112**), der in einem Mobiltelefon angeordnet ist, das einen eindeutigen Code umfasst, wobei der eindeutige Code zumindest teilweise aus einer vorprogrammierten eindeutigen Nummer abgeleitet wird, welche dem Zusatzspeicher zugeordnet ist; und
eine Schaltkreisanordnung (**202**–**210**) zur Missbrauchsverhinderung, die mit dem Zusatzspeicher gekoppelt ist, wobei die Schaltkreisanordnung zur Missbrauchsverhinderung so konfiguriert ist, dass sie den eindeutigen Code mit einem Komponentencode vergleicht, der in einer Komponente gespeichert ist, welche innerhalb des Mobiltelefons angeordnet ist, wobei die Schaltkreisanordnung zur Missbrauchsverhinderung das Durchführen von Telefonanrufen ermöglicht, wenn der eindeutige Code ein vordefiniertes Verhältnis zu dem Komponentencode erfüllt.

6. Vorrichtung nach Anspruch 5, wobei eine Identifikationsnummer unter Verwendung des eindeutigen Codes verschlüsselt wird, um einen verschlüsselten Identifikationscode zu bilden, wobei Telefonanrufe durchgeführt werden können, wenn der verschlüsselte Identifikationscode mit dem Komponentencode übereinstimmt.

7. Vorrichtung nach Anspruch 4, wobei die Komponente aus einer Gruppe ausgewählt wird, die folgendes umfasst: einen Mikrocontroller, eine anwendungsspezifische integrierte Schaltung, eine Zentraleinheit, eine mobile Teilnehmeridentifikationskarte (SIM-Karte) oder einen Signalprozessor.

8. Mobiltelefonsystem, das folgendes umfasst:
eine Zentraleinheit (**102**) und mindestens eine anwendungsspezifische integrierte Schaltung (**106**, **108**), die mit einem Bus (**104**) gekoppelt ist;
gekennzeichnet durch einen Hauptspeicher (**110**)

und einen dauerhaft sperrbaren Zusatzspeicher (**112**), der mit dem Bus gekoppelt ist, wobei der dauerhaft sperrbare Zusatzspeicher einen eindeutigen Code umfasst, wobei der dauerhaft sperrbare Zusatzspeicher außerhalb eines Feldraums des Hauptspeichers angeordnet ist;
eine mit dem Zusatzspeicher gekoppelte Schaltkreisanordnung (**202**–**210**) zur Missbrauchsverhinderung, wobei die Schaltkreisanordnung zur Missbrauchsverhinderung so konfiguriert ist, dass sie den Einsatz des Mobiltelefons steuert, indem ein Komponentencode abgerufen und der eindeutige Code mit dem Komponentencode verglichen wird, wobei die Schaltkreisanordnung zur Missbrauchsverhinderung das Durchführen von Telefonanrufen zulässt, wenn der eindeutige Code ein vordefiniertes Verhältnis zu dem Komponentencode erfüllt.

9. Mobiltelefonsystem nach Anspruch 8, wobei eine Identifikationsnummer unter Verwendung des eindeutigen Codes verschlüsselt wird, so dass ein verschlüsselter Identifikationscode gebildet wird, und wobei Telefonanrufe durchgeführt werden können, wenn der verschlüsselte Identifikationscode mit dem Komponentencode übereinstimmt.

10. Mobiltelefonsystem nach Anspruch 9, wobei die Identifikationsnummer mindestens ein Bit umfasst, das in einem Hauptspeicher des Mobiltelefons gespeichert ist, mindestens ein durch den Mobilfunkanbieter in einem Signal, das von dem Mobiltelefon empfangen wird, bereitgestelltes Bit, und mindestens ein sich in der Systemsoftware des Mobiltelefons befindendes Bit.

Es folgen 8 Blatt Zeichnungen

Anhängende Zeichnungen

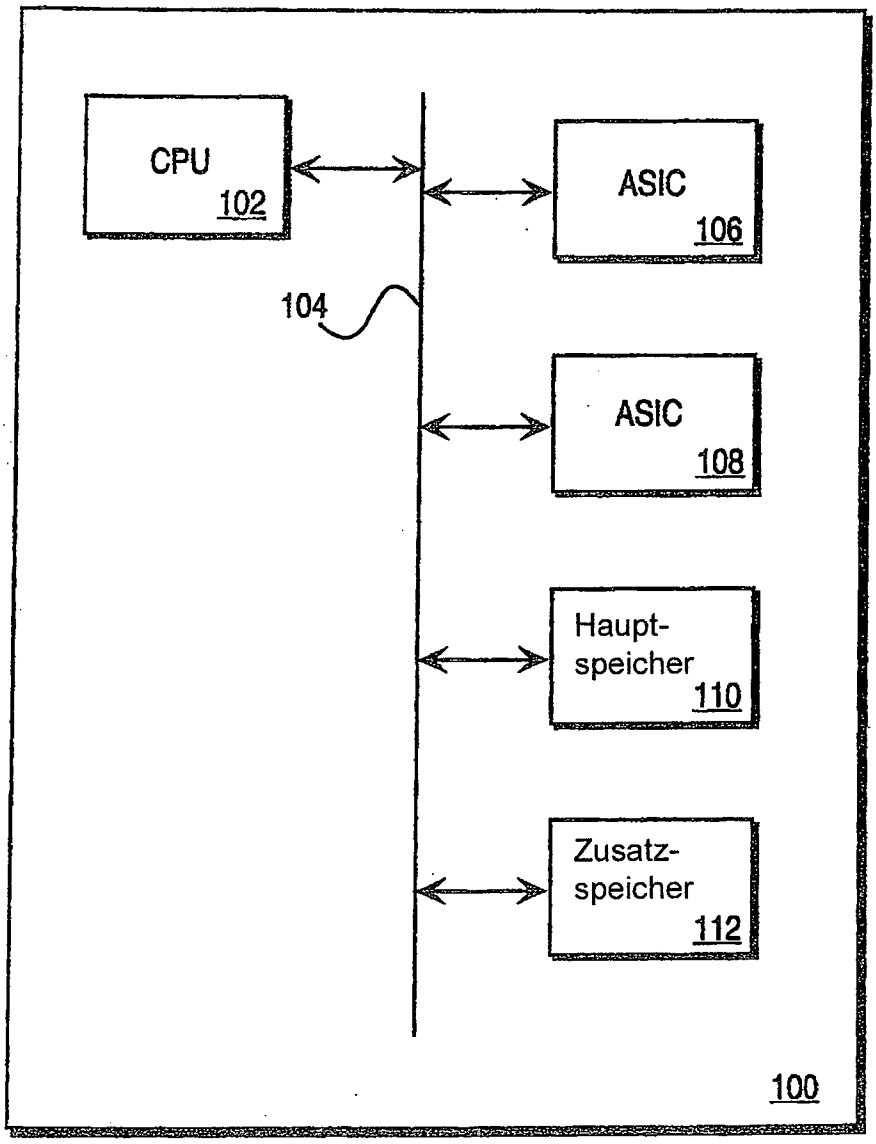

FIG. 1

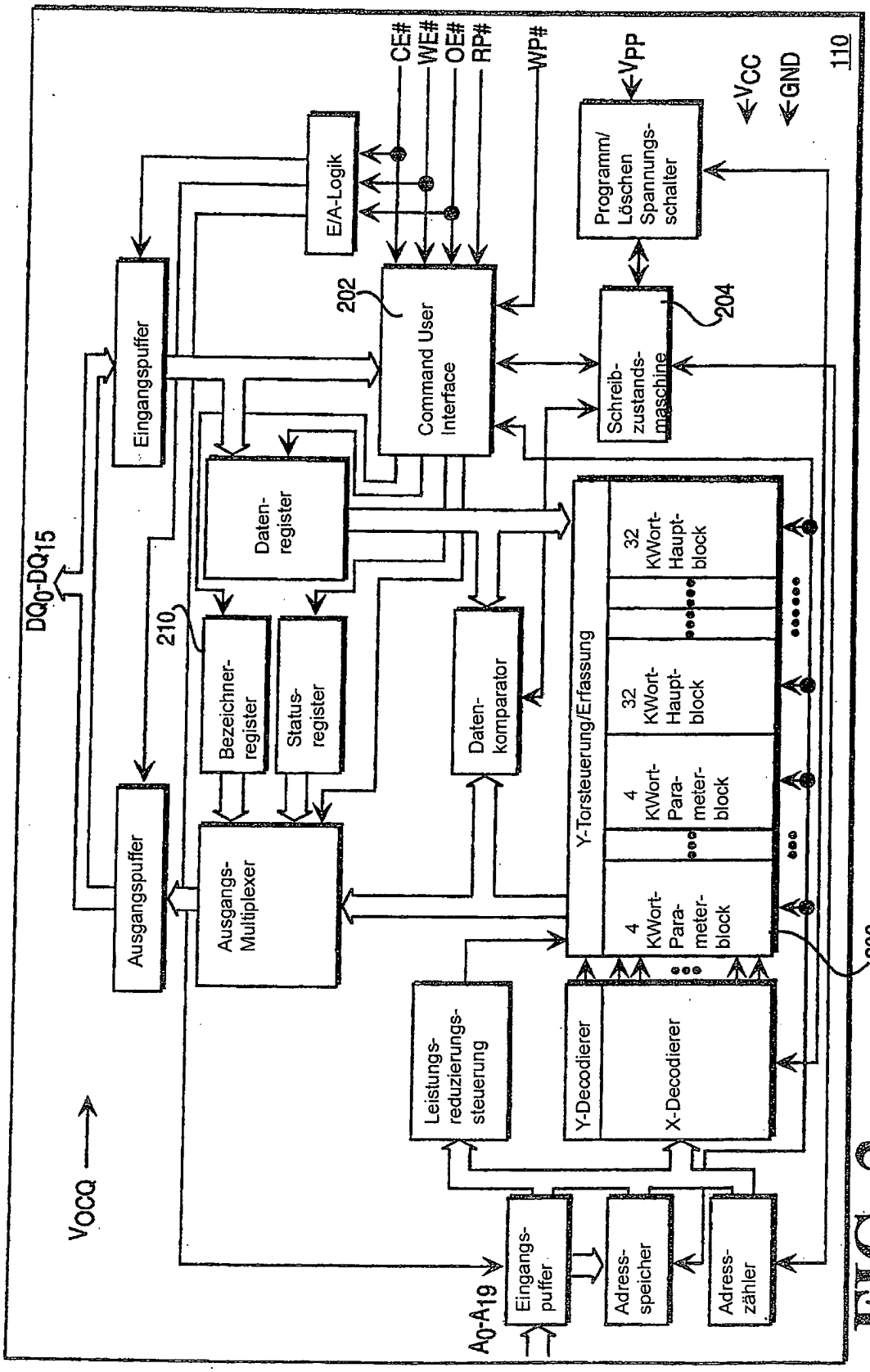
CE#
WE#
OE#
RP#
WP#
VPP
VCC
GND
110
E/A-Logik
Programm/ Löschen Spannungs- schalter
202
Command User Interface
204
Schreib- zustands- maschine
Eingangspuffer
Daten- register
DQ0-DQ15
210
Bezeichner- register
Status- register
Daten- komparator
Y-Torsteuerung/Erfassung
32 KWort- Haupt- block
32 KWort- Haupt- block
4 KWort- Para- meter- block
4 KWort- Para- meter- block
206
Ausgangspuffer
Ausgangs- Multiplexer
Leistungs- reduzierungs- steuerung
Y-Decodierer
X-Decodierer
VOCQ
A0-A19
Eingangs- puffer
Adress- speicher
Adress- zähler

FIG. 2

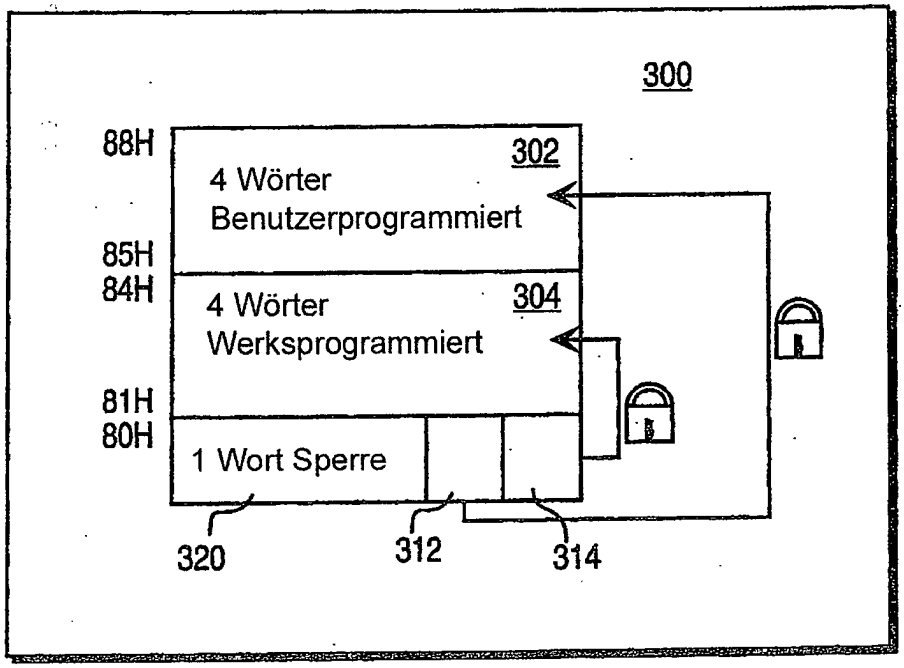
300
88H
302
4 Wörter
Benutzerprogrammiert
85H
84H
4 Wörter
Werksprogrammiert
304
81H
80H
1 Wort Sperre
320
312
314

FIG. 3

WORT-WEITE SCHUTZREGISTERADRESSIERUNG

WORT	EINSATZ	A7	A6	A5	A4	A3	A2	A1	A0
SPERRE	BEIDE	1	0	0	0	0	0	0	0
0	WERK	1	0	0	0	0	0	0	1
1	WERK	1	0	0	0	0	0	1	0
2	WERK	1	0	0	0	0	0	1	1
3	WERK	1	0	0	0	0	1	0	0
4	BENUTZER	1	0	0	0	0	1	0	1
5	BENUTZER	1	0	0	0	0	1	1	0
6	BENUTZER	1	0	0	0	0	1	1	1
7	BENUTZER	1	0	0	0	1	0	0	0

FIG. 4

BYTE-WEITE SCHUTZREGISTERADRESSIERUNG

BYTE	EINSATZ	A11	A7	A6	A5	A4	A3	A2	A1	A0
SPERRE	BEIDE	0	1	0	0	0	0	0	0	0
0	WERK	1	1	0	0	0	0	0	0	0
1	WERK	0	1	0	0	0	0	0	0	1
2	WERK	1	1	0	0	0	0	0	0	1
3	WERK	0	1	0	0	0	0	0	1	0
4	WERK	1	1	0	0	0	0	0	1	0
5	WERK	0	1	0	0	0	0	0	1	1
6	WERK	1	1	0	0	0	0	0	1	1
7	WERK	0	1	0	0	0	0	1	0	0
8	BENUTZER	1	1	0	0	0	0	1	0	0
9	BENUTZER	0	1	0	0	0	0	1	0	1
10	BENUTZER	1	1	0	0	0	0	1	0	1
11	BENUTZER	0	1	0	0	0	0	1	1	0
12	BENUTZER	1	1	0	0	0	0	1	1	0
13	BENUTZER	0	1	0	0	0	0	1	1	1
14	BENUTZER	1	1	0	0	0	0	1	1	1
15	BENUTZER	0	1	0	0	0	1	0	0	0

FIG. 5

OBJEKT	ADRESSE	DATEN
HERSTELLERCODE (x16)	00000	0089
HERSTELLERCODE (x8)	00000	89
GERÄTE-ID	00001	ID
BLOCKSPERRENKONFIGURATION	XX002	SPERRE
• BLOCK NICHT GESPERRT		DQ_0=0
• BLOCK GESPERRT		DQ_0=1
• BLOCK VERRIEGELT		DQ_1=1
SCHUTZREGISTERSPERRE	80	PR-LK
SCHUTZREGISTER (x16)	81-88	PR
SCHUTZREGISTER (x8)		PR

FIG. 6

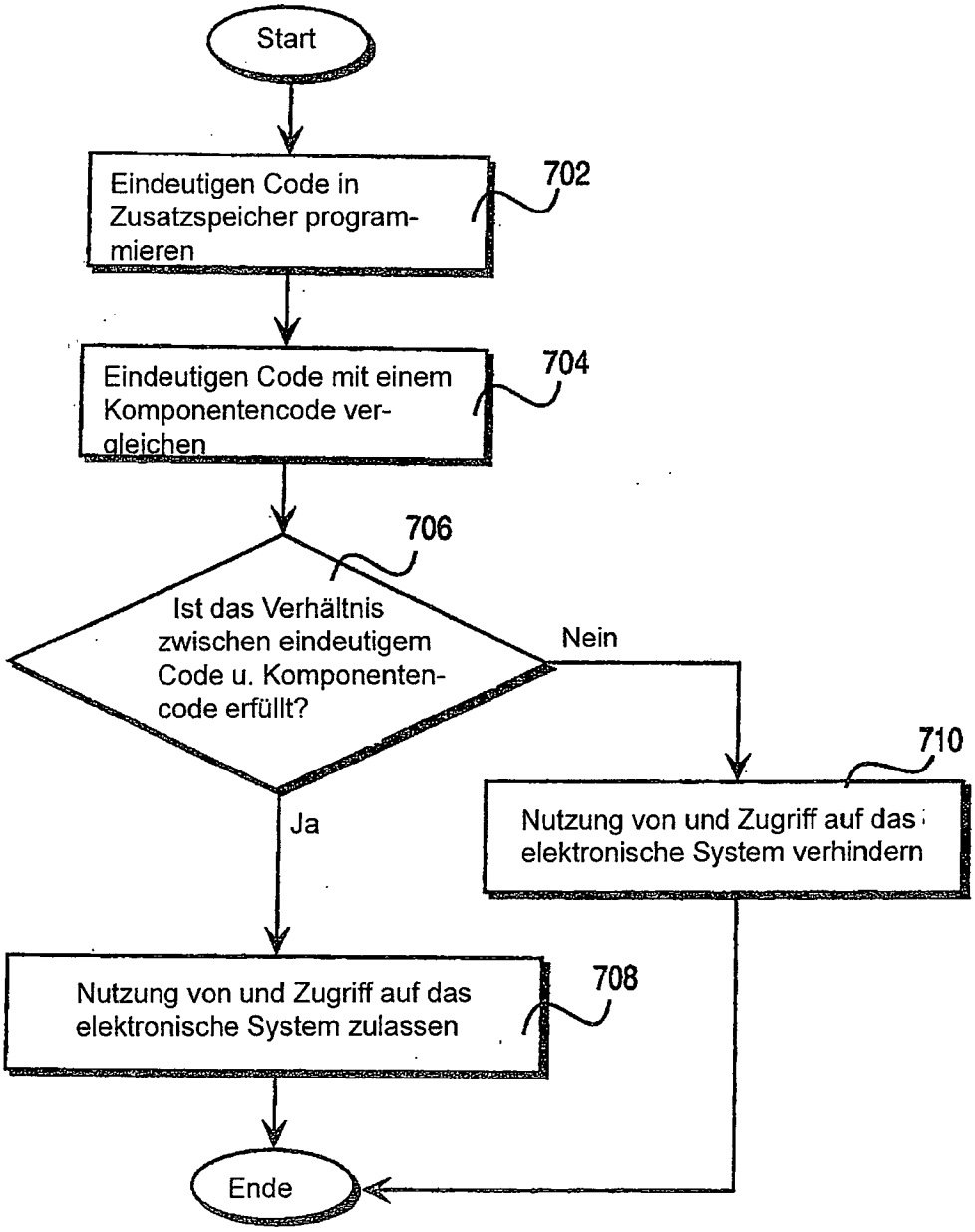
Start
Eindeutigen Code in Zusatzspeicher programmieren
702
Eindeutigen Code mit einem Komponentencode vergleichen
704
706
Ist das Verhältnis zwischen eindeutigem Code u. Komponentencode erfüllt?
Nein
Ja
710
Nutzung von und Zugriff auf das elektronische System verhindern
Nutzung von und Zugriff auf das elektronische System zulassen
708
Ende

FIG. 7

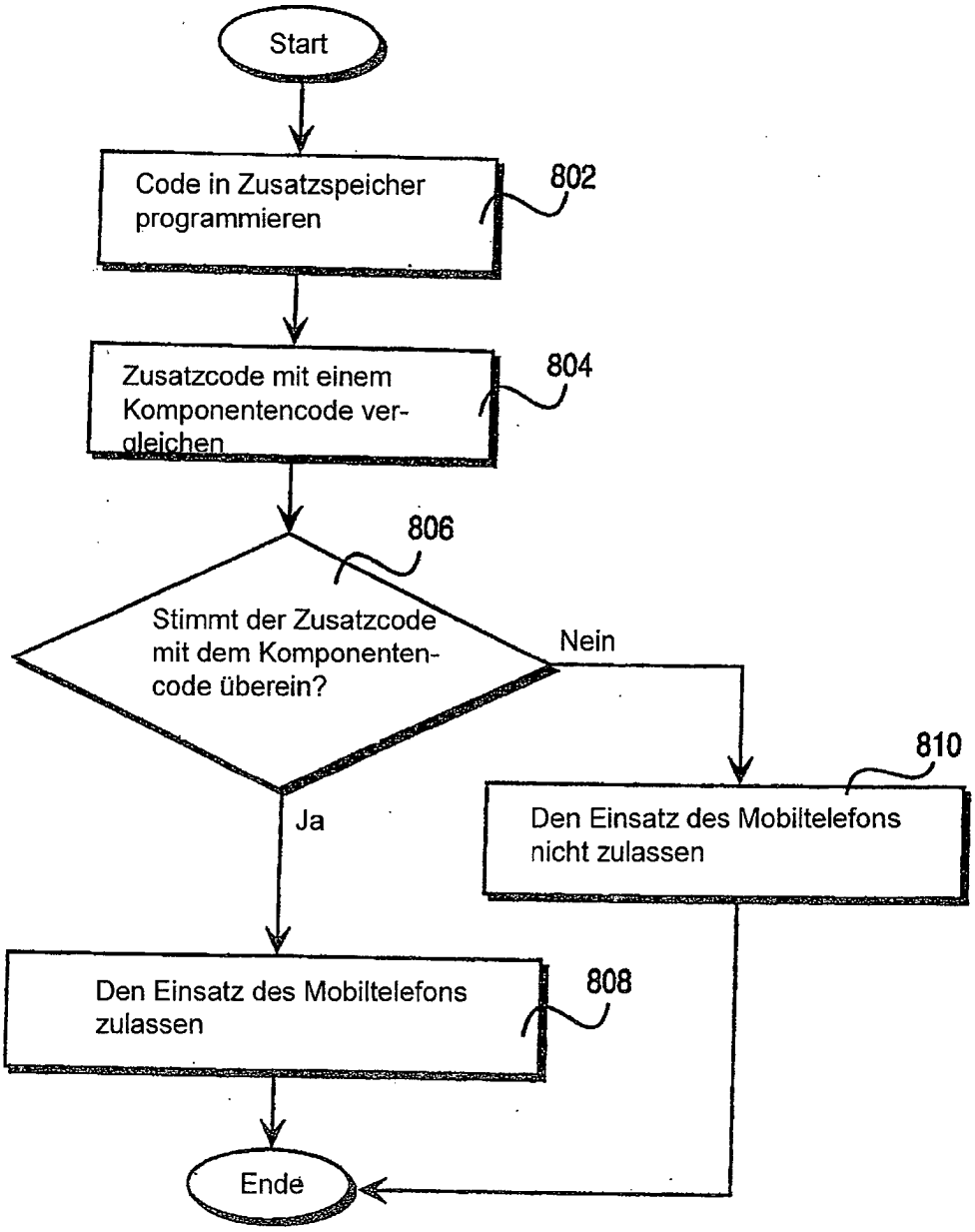
Start
Code in Zusatzspeicher programmieren
802
Zusatzcode mit einem Komponentencode vergleichen
804
806
Stimmt der Zusatzcode mit dem Komponentencode überein?
Nein
Ja
810
Den Einsatz des Mobiltelefons nicht zulassen
Den Einsatz des Mobiltelefons zulassen
808
Ende

FIG. 8