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

(10) **DE 600 33 066 T2** 2007.06.21

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 453 060 B1**
(21) Deutsches Aktenzeichen: **600 33 066.4**
(96) Europäisches Aktenzeichen: **04 012 371.3**
(96) Europäischer Anmeldetag: **25.04.2000**
(97) Erstveröffentlichung durch das EPA: **01.09.2004**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **17.01.2007**
(47) Veröffentlichungstag im Patentblatt: **21.06.2007**

(51) Int Cl.[8]: ***G11C 16/22*** (2006.01)
G11C 27/00 (2006.01)
G06F 12/14 (2006.01)
G06F 1/00 (2006.01)

(30) Unionspriorität:

11944199	**27.04.1999**	**JP**
37478899	**28.12.1999**	**JP**

(84) Benannte Vertragsstaaten:
DE, FR, GB, IT, NL

(73) Patentinhaber:
Matsushita Electric Industrial Co., Ltd., Kadoma, Osaka, JP

(74) Vertreter:
Grünecker, Kinkeldey, Stockmair & Schwanhäusser, 80538 München

(72) Erfinder:
Hirota, Teruto, Moriguchi-shi, Osaka-fu 570-0015, JP; Tatebayashi, Makoto, Takarazuka-shi, Hyogo-ken 665-0852, JP; Yugawa, Taihei, Nara-shi, Nara-ken 631-0061, JP; Minami, Masataka, Mountain View California 94040, US; Kozuka, Masayuki, Arcadia, California 91008, US

(54) Bezeichnung: **Halbleiterspeicherkarte und Datenlesevorrichtung**

Beschreibung

HINTERGRUND DER ERFINDUNG

(1) Technisches Gebiet der Erfindung

[0001] Die vorliegende Erfindung bezieht sich auf eine Halbleiter-Speicherkarte zum Speichern digitaler Inhalte, und eine Datenlesevorrichtung zum Auslesen der digitalen Inhalte aus der Halbleiter-Speicherkarte. Insbesondere bezieht sich die vorliegende Erfindung auf eine Halbleiter-Speicherkarte und eine Datenlesevorrichtung, die zum Copyright-Schutz von digitalen Inhalten geeignet sind.

(2) Beschreibung des Standes der Technik

[0002] Die Multimedianetzwerktechnik hat sich dahingehend entwickelt, dass digitale Inhalte, wie Musikinhalte, über ein Kommunikationsnetzwerk, wie das Internet, verbreitet werden. Diese ermöglicht es, auf eine Varietät von Musik oder Ähnlichem, die von überall in der Welt bereit gestellt wird, von zu Hause aus zuzugreifen. Zum Beispiel kann ein Musikinhalt in einen Personalcomputer (im Folgenden als PC bezeichnet) heruntergeladen werden und dann in einer Halbleiter-Speicherkarte gespeichert werden, die in den PC geladen wird. Ebenso kann die Halbleiter-Speicherkarte von dem PC entfernt werden und in ein tragbares Musikwiedergabegerät geladen werden. Dies ermöglicht es einem, beim Gehen die Musik zu hören. Die Halbleiter-Speicherkarten sind kompakte und leichtgewichtige Karten, die einen Halbleiterspeicher (z. B. einen Flash-Speicher) enthalten, der nichtflüchtig ist und eine große Speicherkapazität aufweist.

[0003] In solch einer Musikverbreitung müssen die digitalen Inhalte, die in der Halbleiter-Speicherkarte gespeichert werden, zuvor verschlüsselt werden unter Verwendung eines Schlüssels oder Ähnlichem, um ein nicht autorisiertes Kopieren der digitalen Inhalte zu verhindern. Ebenso wird eine Anordnung benötigt, so dass Dateimanagement-Softwareprogramme, von denen viele zur Standardausrüstung von kommerziellen PCs gehören, nicht die digitalen Inhalte zu anderen Speichermedien kopieren können.

[0004] In einem möglichen Verfahren zum Verhindern von nicht autorisiertem Kopieren wird nur dedizierten Softwareprogrammen erlaubt, auf die Halbleiter-Speicherkarte zuzugreifen. Zum Beispiel, wenn ein Authentisierungsprozess zwischen einem PC und einer Halbleiter-Speicherkarte bejahend (zustimmend) beendet wurde, wird einem PC erlaubt, auf die Halbleiter-Speicherkarte zuzugreifen; und wenn der Authentisierungsprozess nicht bejahend beendet wurde aufgrund des Fehlens eines dedizierten Softwareprogramms, wird dem PC nicht erlaubt, auf die Halbleiter-Speicherkarte zuzugreifen.

[0005] Jedoch ist in dem obigen Verfahren, in dem PCs immer ein dediziertes Softwareprogramm aufweisen sollen, um auf die Halbleiter-Speicherkarte zuzugreifen, ein freier Datenaustausch mit Benutzern über die Halbleiter-Speicherkarte nicht verfügbar. Als ein Ergebnis verliert das obige Verfahren einen Vorzug gebräuchlicher Halbleiter-Speicherkarten, und zwar einen Verdienst, dass Dateimanagement-Softwareprogramme, die Standardausrüstungen auf kommerziellen PCs sind, verwendet werden können, um auf die Halbleiter-Speicherkarte zuzugreifen.

[0006] Halbleiter-Speicherkarten, auf die nur über dedizierte Softwareprogramme zugegriffen werden kann, sind besser als Speichermedien zum Speichern digitaler Inhalte, da diese Halbleiter-Speicherkarten funktionieren, um ein Copyright der digitalen Inhalte zu schützen. Jedoch weisen die Halbleiter-Speicherkarten das Problem auf, dass sie nicht als Externspeichervorrichtungen in Universalrechensystemen verwendet werden können.

ZUSAMMENFASSUNG DER ERFINDUNG

[0007] Es ist deshalb eine Aufgabe der vorliegenden Erfindung, eine Halbleiter-Speicherkarte, die als ein Speichermedium zum Speichern digitaler Inhalte und als ein Speichermedium zum Speichern von Universalrechnerdaten (die nicht Gegenstand eines Copyright-Schutzes sind) verwendet werden kann, bereit zu stellen, und eine Vorrichtung zum Auslesen von Daten aus dem Speichermedium bereit zu stellen.

[0008] Die oben stehende Aufgabe wird gelöst durch eine Halbleiter-Speicherkarte, die in einer elektronischen Vorrichtung verwendet werden kann und aus dieser entnommen werden kann, und die aufweist: einen wiederbeschreibbaren, nicht flüchtigen Speicher, und eine Steuerschaltung, die Zugriffe durch die elektronische Vorrichtung auf einen Authentisierungsbereich und einen Nicht-Authentisierungsbereich in dem wiederbeschreibbaren, nicht flüchtigen Speicher steuert; wobei der Steuerschaltkreis enthält: eine Nicht-Authentisierungsbereichs-Zugriffssteuereinheit, die Zugriffe durch die elektronische Vorrichtung auf den Nicht-Authentisierungsbereich steuert; eine Authentisierungseinheit, die einen Authentisierungsprozess durchführt, um zu prüfen, ob die elektronische Vorrichtung geeignet ist, und die elektronische Vorrichtung zustimmend authentisiert, wenn die elektronische Vorrichtung geeignet ist; und eine Authentisierungsbereichs-Zugriffssteuereinheit, die der elektronischen Vorrichtung nur dann erlaubt, auf den Authentisierungsbereich zuzugreifen, wenn die Authentisierungseinheit die elektronische Vorrichtung zustimmend authentisiert.

[0009] Mit der obigen Konstruktion können die Daten, die Gegenstand eines Copyright-Schutzes sind,

in dem Authentisierungsbereich gespeichert werden und andere Daten können in dem Nicht-Authentisierungsbereich gespeichert werden, was es möglich macht, eine derartige Halbleiter-Speicherkarte zu erzielen, die zusammen sowohl digitale Inhalte speichern kann, für die ein Copyright-Schutz durchzuführen ist, als auch andere Daten.

[0010] In der obigen Halbleiter-Speicherkarte kann die Authentisierungseinheit einen Schlüssel erzeugen, der ein Ergebnis des Authentisierungsvorgangs widerspiegelt, und die Zugriffssteuereinheit für den Authentisierungsbereich (Authentisierungsbereichszugriff-Steuereinheit) entschlüsselt einen verschlüsselten Befehl unter Verwendung des durch die Authentisierungseinheit erzeugten Schlüssels, und steuert Zugriffe der elektronischen Vorrichtung auf den Authentisierungsbereich in Übereinstimmung mit dem entschlüsselten Befehl, wobei der verschlüsselte Befehl von der elektronischen Vorrichtung gesendet wurde.

[0011] Mit der obigen Konstruktion wird, auch falls die Kommunikation zwischen der Halbleiter-Speicherkarte und einer elektronischen Vorrichtung angezapft wird, der Befehl, auf den Authentisierungsbereich zuzugreifen, verschlüsselt und spiegelt das Ergebnis der vorherigen Authentisierung wider. Dementsprechend weist eine solche Halbleiter-Speicherkarte eine zuverlässige Funktion zum Schutz des Authentisierungsbereichs vor ungesetzlichen Zugriffen auf.

[0012] In der obigen Halbleiter-Speicherkarte kann die Authentisierungseinheit eine gegenseitige Authentisierung mit der elektronischen Vorrichtung vom Typ mit Authentisierungsabfrage und -antwort ausführen und erzeugt den Schlüssel aus Abfragedaten und Antwortdaten, wobei die Abfragedaten zu der elektronischen Vorrichtung gesendet werden, um zu überprüfen, ob die elektronische Vorrichtung geeignet ist, und die Antwortdaten erzeugt werden, um zu zeigen, dass die Authentisierungseinheit geeignet ist.

[0013] Mit der obigen Konstruktion wird der Schlüssel von der Halbleiter-Speicherkarte und der elektronischen Vorrichtung nur dann geteilt, wenn beide Vorrichtungen einander bejahend authentisieren. Weiterhin ändert sich der Schlüssel für jede Authentisierung. Dies verbessert die Sicherheit des Authentisierungsbereichs, da auf den Authentisierungsbereich nicht ohne eine Verwendung des Schlüssels zugegriffen werden kann.

[0014] In der obigen Halbleiter-Speicherkarte kann der von der elektronischen Vorrichtung gesendete, verschlüsselte Befehl ein Etikettenfeld und ein Adressfeld umfassen, wobei das Etikettenfeld nicht verschlüsselt wurde und einen Typ eines Zugriffs auf den Authentisierungsbereich spezifiziert und das Adressfeld verschlüsselt wurde und eine Adresse eines Bereichs, auf den zugegriffen wird, spezifiziert, wobei die Zugriffssteuereinheit für den Authentisierungsbereich das Adressfeld unter Verwendung des Schlüssels entschlüsselt und Zugriffe von der elektronischen Vorrichtung auf den Authentisierungsbereich steuert, so dass ein Zugriff des in dem Etikettenfeld spezifizierten Typs auf den Bereich gemacht wird, der von der Adresse in dem entschlüsselten Adressfeld gekennzeichnet ist.

[0015] Mit der obigen Konstruktion wird nur das Adressfeld des Befehls verschlüsselt. Dies vereinfacht die Entschlüsselung und das Decodieren des Befehls durch die Halbleiter-Speicherkarte, die den Befehl empfängt.

[0016] Die obige Halbleiter-Speicherkarte kann weiterhin aufweisen: eine Speicherschaltung für Identifizierungsdaten, die im voraus Identifizierungsdaten speichern, die für die Halbleiter-Speicherkarte eindeutig sind und ermöglichen, die Halbleiter-Speicherkarte von anderen Halbleiter-Speicherkarten zu unterscheiden, wobei die Authentisierungseinheit eine gegenseitige Authentisierung mit der elektronischen Vorrichtung unter Verwendung der in der Speicherschaltung für Identifizierungsdaten gespeicherten Identifizierungsdaten ausführt, und den Schlüssel von den Identifizierungsdaten erzeugt.

[0017] Mit der obigen Konstruktion werden in dem gegenseitigen Authentisierungsvorgang Daten ausgetauscht, die für jede Halbleiter-Speicherkarte eindeutig sind. Dies behält ein höheres Sicherheitsniveau gegen ungesetzliches Decodieren der gegenseitigen Authentisierung bei.

[0018] Die obige Halbleiter-Speicherkarte kann weiterhin aufweisen: eine Bereichsgrößenänderungsschaltung, die die Größe des Authentisierungsbereichs und des Nicht-Authentisierungsbereichs ändert.

[0019] Mit der obigen Konstruktion kann die Halbleiter-Speicherkarte dynamisch verwendet werden. Das heißt, die Halbleiter-Speicherkarte kann hauptsächlich als ein Aufzeichnungsmedium für digitale Inhalte verwendet werden und kann als eine Externspeichervorrichtung in einem Computersystem verwendet werden.

[0020] In der obigen Halbleiter-Speicherkarte können der Authentisierungsbereich und der Nicht-Authentisierungsbereich durch ein Aufteilen eines ununterbrochenen Bereichs mit einer vorgegebenen Größe in dem wiederbeschreibbaren, nicht flüchtigen Speicher in zwei Teile hergestellt werden, und die Bereichsgrößenänderungsschaltung ändert die Größe des Authentisierungsbereichs und des Nicht-Authentisierungsbereichs durch Veränderung einer Adres-

se, die eine Grenze zwischen dem Authentisierungsbereich und dem Nicht-Authentisierungsbereich markiert.

[0021] Mit der obigen Konstruktion kann die Größe der Authentisierungs- und Nicht-Authentisierungsbereiche dadurch geändert werden, dass nur die Grenze bewegt wird. Dies reduziert die Größe des Schaltkreises.

[0022] In der obigen Halbleiter-Speicherkarte kann die Bereichsgrößenänderungsschaltung umfassen: eine Authentisierungsbereich-Umwandlungstabelle, die eine Übereinstimmung zwischen logischen Adressen und physikalischen Adressen in dem Authentisierungsbereich zeigt; eine Umwandlungstabelle für einen Nicht-Authentisierugsbereich (Nicht-Authentisierungsbereich-Umrechnungstabelle), die eine Übereinstimmung zwischen logischen Adressen und physikalischen Adressen in dem Nicht-Authentisierungsbereich zeigt; und eine Umwandlungstabellen-Änderungseinheit, die Inhalte der Authentisierungsbereich-Umwandlungstabelle und der Umwandlungstabelle für einen Nicht-Authentisierungsbereich in Übereinstimmung mit einem Befehl von der elektronischen Vorrichtung ändert, wobei die Zugriffssteuereinheit für einen Authentisierungsbereich Zugriffe von der elektronischen Vorrichtung auf den Authentisierungsbereich durch Verweisen auf die Authentisierungsbereich-Umwandlungstabelle steuert, und wobei die Zugriffssteuereinheit für einen Nicht-Authentisierungsbereich Zugriffe von der elektronischen Vorrichtung auf den Nicht-Authentisierungsbereich durch Verweisen auf die Umwandlungstabelle für einen Nicht-Authentisierungsbereich steuert.

[0023] Mit der obigen Konstruktion ist es möglich, den Authentisierungsbereich und den Nicht-Authentisierungsbereich hinsichtlich der Bereichsgröße und Beziehungen zwischen den logischen Adressen und physikalischen Adressen getrennt zu verwalten, da Umwandlungstabellen für diese Bereiche unabhängig voneinander betrieben werden.

[0024] In der obigen Halbleiter-Speicherkarte können ein mit höheren physikalischen Adressen adressierter Bereich und ein mit niedrigeren physikalischen Adressen adressierter Bereich, die beide den Bereich mit der vorgegebenen Größe bilden, jeweils dem Authentisierungsbereich und dem Nicht-Authentisierungsbereich zugeordnet werden, die Umwandlungstabelle für einen Nicht-Authentisierungsbereich zeigt eine Übereinstimmung zwischen logischen Adressen, die in einer aufsteigenden Reihenfolge angeordnet sind, und physikalischen Adressen, die in einer aufsteigenden Reihenfolge angeordnet sind, und die Authentisierungsbereich-Umwandlungstabelle zeigt eine Übereinstimmung zwischen logischen Adressen, die in einer aufsteigenden Reihenfolge angeordnet sind, und physikalischen Adressen, die in einer absteigenden Reihenfolge angeordnet sind.

[0025] Mit der obigen Konstruktion, die eine Verwendung der logischen Adressen in aufsteigender Reihenfolge ermöglicht, kann die Bereichsgröße einfach geändert werden, da die Wahrscheinlichkeit eines Verwendens eines Bereichs um die Begrenzung zwischen dem Authentisierungsbereich und dem Nicht-Authentisierungsbereich herum niedrig wird. Dies verkleinert ebenso die Wahrscheinlichkeit eines Auftretens eine Speicherns oder -Bewegens, von Daten, was notwendig ist, um die Begrenzung zu bewegen, resultierend in einer vereinfachten Bereichsgrößenänderung.

[0026] Die obige Halbleiter-Speicherkarte kann weiterhin aufweisen: eine Festwertspeicherschaltung, die Daten vorspeichert.

[0027] Mit der obigen Konstruktion wird die Funktion eines Copyright-Schutzes durch Speichern von Identifizierungsdaten der Halbleiter-Speicherkarte in dem dedizierten Speicher und Speichern der digitalen Inhalte in Abhängigkeit von den Ergebnissen einer Identifizierung beruhend auf den Identifizierungsdaten verbessert.

[0028] In der obigen Halbleiter-Speicherkarte kann sowohl der Authentisierungsbereich als auch der Nicht-Authentisierungsbereich aufweisen: einen Lese-/Schreib-Speicherbereich, von/zu dem die elektronische Vorrichtung Daten lesen/schreiben kann; und einen Festwertspeicherbereich, von dem die elektronische Vorrichtung Daten lesen kann, aber zu dem die elektronische Vorrichtung keine Daten schreiben kann, wobei der Steuerschaltkreis weiterhin umfasst: einen Zufallszahlengenerator, der eine Zufallszahl jedes Mal dann erzeugt, wenn die elektronische Vorrichtung Daten zu dem wiederbeschreibbaren, nicht flüchtigen Speicher schreibt, und wobei sowohl die Authentisierungsbereichs-Zugriffssteuereinheit als auch die Nicht-Authentisierungsbereichs-Zugriffssteuereinheit Daten unter Verwendung der Zufallszahl verschlüsseln, die verschlüsselten Daten zu dem Lese-/Schreib-Speicherbereich schreiben und die Zufallszahl zu dem Festwertspeicherbereich schreiben.

[0029] Mit der obigen Konstruktion können ungesetzliche Versuche, wie z. B. eine unsachgemäße Behandlung des Lese-/Schreib-Speicherbereichs, durch ein Prüfen der Kompatibilität mit der in dem Festwertspeicherbereich gespeicherten Zufallszahl geprüft werden. Dies verbessert die Sicherheit des Datenschreibens.

[0030] In der obigen Halbleiter-Speicherkarte kann die Steuerschaltung weiterhin umfassen: eine Um-

wandlungstabelle, die eine Übereinstimmung zwischen logischen Adressen und physikalischen Adressen in jedem des Authentisierungsbereichs und des Nicht-Authentisierungsbereichs zeigt; und eine Änderungsschaltung für eine Umwandlungstabelle, die Inhalte der Umwandlungstabelle in Übereinstimmung mit einem Befehl von der elektronischen Vorrichtung ändert, und die Zugriffssteuereinheit für einen Authentisierungsbereich und die Zugriffssteuereinheit für einen Nicht-Authentisierungsbereich steuern Zugriffe von der elektronischen Vorrichtung auf den Authentisierungsbereich und den Nicht-Authentisierungsbereich jeweils durch Verweisen auf die Umwandlungstabelle.

[0031] Mit der obigen Konstruktion können diese ebenso, falls die Mehrzahl von logischen Blöcken, die dieselbe Datei bilden, fragmentiert ist, einfach geändert werden, um logisch aufeinander folgend zu werden. Dies verbessert die Geschwindigkeit von Zugriffen auf dieselbe Datei.

[0032] In der obigen Halbleiter-Speicherkarte kann die Steuerschaltung weiterhin umfassen: eine Verschlüsselungs-/Entschlüsselungseinheit, die Daten verschlüsselt, die zu dem Authentisierungsbereich und dem Nicht-Authentisierungsbereich geschrieben werden, und Daten entschlüsselt, die aus dem Authentisierungsbereich und dem Nicht-Authentisierungsbereich ausgelesen werden.

[0033] Mit der obigen Konstruktion ist es möglich, den Authentisierungsbereich und den Nicht-Authentisierungsbereich gegen ungesetzliche Attacken zu verteidigen, wie ein Zerstören der Halbleiter-Speicherkarte und ein direktes Lesen der Inhalte aus diesen Bereichen.

[0034] In der obigen Halbleiter-Speicherkarte kann der nicht flüchtige Speicher ein Flash-Speicher sein, und der Steuerschaltkreis umfasst weiterhin: eine Nicht-Gelöscht-Listen-Aufnahmeeinheit, die in Übereinstimmung mit einer Anweisung von der elektronischen Vorrichtung nicht gelöschte Bereiche in dem Authentisierungsbereich und dem Nicht-Authentisierungsbereich identifiziert, und Informationen zu der elektronischen Vorrichtung sendet, die die nicht gelöschten Bereiche anzeigen.

[0035] Mit der obigen Konstruktion kann die elektronische Vorrichtung nicht gelöschte Bereiche identifizieren und die identifizierten nicht gelöschten Bereiche löschen bevor der Flash-Speicher wieder beschrieben wird. Dies vergrößert die Geschwindigkeit bei der Wiederbeschreibung.

[0036] In der obigen Halbleiter-Speicherkarte kann die Authentisierungseinheit einen Benutzer der elektronischen Vorrichtung auffordern, einen Anwenderschlüssel, der eine für den Benutzer eindeutige Information ist, während des Authentisierungsvorgangs einzugeben, und die Steuerschaltung umfasst weiterhin: eine Speichereinheit für Anwenderschlüssel (Benutzerschlüssel-Speichereinheit) die den Anwenderschlüssel speichert; eine Speichereinheit für Identifizierungsinformationen (Kennungsinformations-Speichereinheit) die einen Teil von Identifizierungsinformationen speichert, der eine elektronische Vorrichtung identifiziert, die bejahend von der Authentisierungseinheit authentisiert wurde; und eine Anwenderschlüsselanforderungsverhinderungseinheit (Benutzerschlüsselaufforderungs-Verbotseinheit) die einen Teil von Identifizierungsinformationen von einer elektronischen Zielvorrichtung erhält, nachdem die Authentisierungseinheit den Authentisierungsvorgang begonnen hat, überprüft, ob der Teil der von der elektronischen Zielvorrichtung erhaltene Identifizierungsinformation bereits in der Speichereinheit für Identifizierungsinformationen gespeichert ist, und verhindert, dass die Authentisierungseinheit einen Benutzer der elektronischen Vorrichtung auffordert, einen Anwenderschlüssel einzugeben, wenn der von der elektronischen Zielvorrichtung erhaltene Teil von Identifizierungsinformation bereits in der Speichereinheit für Identifizierungsinformation gespeichert wurde.

[0037] Mit der obigen Konstruktion muss der Anwender nicht bei jedem Zugreifen auf die Halbleiter-Speicherkarte ein Kennwort oder persönliche Daten eingeben. Dies verhindert das Auftreten eines ungesetzlichen Abgreifens und eine Verwendung der persönlichen Daten.

[0038] Die obige Aufgabe wird ebenso gelöst durch eine Datenlesevorrichtung zum Auslesen eines digitalen Inhalts aus der obigen Halbleiter-Speicherkarte, wobei der digitale Inhalt in dem Nicht-Authentisierungsbereich der Halbleiter-Speicherkarte gespeichert wurde, und Information, die die Häufigkeit kennzeichnet, mit der der in dem Authentisierungsbereich zuvor gespeicherte digitale Inhalt ausgelesen werden kann, wobei die Datenlesevorrichtung aufweist: eine Entscheidungseinrichtung zum Auslesen der Information, die die Häufigkeit anzeigt, mit der der digitale Inhalt aus dem Authentisierungsbereich ausgelesen werden kann, wenn der digitale Inhalt aus dem Nicht-Authentisierungsbereich ausgelesen werden soll, und zum Entscheiden, ob der digitale Inhalt beruhend auf der in der Information angezeigten Häufigkeit ausgelesen werden kann; und eine Wiedergabeeinrichtung zum Auslesen des digitalen Inhalts von dem Nicht-Authentisierungsbereich nur dann, wenn die Entscheidungseinrichtung beurteilt, dass der digitale Inhalt ausgelesen werden kann, und Reduzieren der Häufigkeit, mit der der digitale Inhalt ausgelesen werden kann, in der in dem Authentisierungsbereich gespeicherten Information.

[0039] Mit der obigen Konstruktion ist es möglich,

die Häufigkeit zu beschränken, mit der der digitale Inhalt aus der Halbleiter-Speicherkarte ausgelesen wird. Dies ermöglicht, die vorliegende Erfindung auf gebührenpflichtige Mietmusikinhalte anzuwenden.

[0040] Die obige Aufgabe wird ebenfalls gelöst durch eine Datenlesevorrichtung zum Auslesen eines digitalen Inhalts aus der obigen Halbleiter-Speicherkarte und zum Wiedergeben des ausgelesenen digitalen Inhalts als ein analoges Signal, wobei der digitale Inhalt, der als ein analoges Signal wiedergegeben werden kann, in dem Nicht-Authentisierungsbereich der Halbleiter-Speicherkarte gespeichert wurde, und Information, die die Häufigkeit kennzeichnet, mit der der digitale Inhalt digital von der elektronischen Vorrichtung ausgegeben werden kann, in dem Authentisierungsbereich gespeichert wurde, wobei die Datenlesevorrichtung aufweist: eine Wiedergabeeinrichtung zum Auslesen des digitalen Inhalts aus dem Nicht-Authentisierungsbereich und zum Wiedergeben des ausgelesenen digitalen Inhalts als ein analoges Signal; eine Entscheidungseinrichtung zum Auslesen der Information, die die Häufigkeit anzeigt, mit der der digitale Inhalt von der elektronischen Vorrichtung digital ausgegeben werden kann, und zum Entscheiden, ob der digitale Inhalt digital ausgegeben werden kann, beruhend auf der Häufigkeit, die in der Information angezeigt ist; und eine digitale Ausgabeeinrichtung bzw. Digitalaufgabe-Einrichtung zum digitalen Ausgeben des digitalen Inhalts nur dann, wenn die Entscheidungseinrichtung entscheidet, dass der digitale Inhalt digital ausgegeben werden kann, und zum Reduzieren der Häufigkeit, mit der der digitale Inhalt digital ausgegeben werden kann, in der in dem Authentisierungsbereich gespeicherten Information.

[0041] Mit der obigen Konstruktion ist es möglich, die Häufigkeit zu beschränken, mit der der digitale Inhalt digital von der Halbleiter-Speicherkarte kopiert wird. Dies stellt einen Copyright-Schutz bereit, der mit Vorsicht und Aufmerksamkeit, wie von dem Copyright-Inhaber beabsichtigt, detailliert ist.

[0042] Wie oben stehend beschrieben, ist die vorliegende Erfindung eine Halbleiter-Speicherkarte, die mit Flexibilität sowohl als ein Speichermedium zum Speichern digitaler Inhalte, als auch als eine Externspeichervorrichtung eines Computers funktioniert. Die vorliegende Erfindung gewährleistet insbesondere eine gesunde Verbreitung digitaler Inhalte für elektronische Musikverbreitung. Dies ist praktisch wertvoll.

KURZE BESCHREIBUNG DER ZEICHNUNGEN

[0043] Diese und andere Aufgaben, Vorteile und Merkmale der Erfindung werden sichtbar aus der folgenden Beschreibung hiervon in Verbindung mit den beiliegenden Zeichnungen, die eine spezifische Ausführungsform der Erfindung illustrieren. In den Zeichnungen:

[0044] Fig. 1 zeigt die Ansicht eines PCs, der eine Ausführungsform der vorliegenden Erfindung ist, und sich auf eine elektronische Musikverbreitung bezieht, und zeigt die Ansicht einer Halbleiter-Speicherkarte, die in den PC geladen und von diesem entfernt werden kann.

[0045] Fig. 2 zeigt die Ansicht eines tragbaren Wiedergabegeräts, für das die Halbleiter-Speicherkarte als ein Aufzeichnungsmedium verwendet wird;

[0046] Fig. 3 ist ein Blockdiagramm, das die Hardwarekonstruktion des PCs zeigt;

[0047] Fig. 4 ist ein Blockdiagramm, das die Hardwarekonstruktion des Wiedergabegeräts zeigt;

[0048] Fig. 5 zeigt die Ansicht und die Hardwarekonstruktion der Halbleiter-Speicherkarte;

[0049] Fig. 6 zeigt verschiedene Speicherbereiche in der Halbleiter-Speicherkarte, die von dem PC und dem Wiedergabegerät erkannt werden können;

[0050] Fig. 7A, Fig. 7B und Fig. 7C zeigen Beschränkungen und Befehlsformate, wenn der PC oder das Wiedergabegerät auf einen Bereich in der Halbleiter-Speicherkarte zugreifen, wobei Fig. 7A Regeln zeigt, die zum Zugreifen auf jeden Bereich befolgt werden müssen, Fig. 7B Regeln zeigt, die zum Ändern der Größe jedes Bereichs befolgt werden müssen, und Fig. 7C eine schematische Repräsentation von Bereichen in der Halbleiter-Speicherkarte zeigt;

[0051] Fig. 8 ist ein Flussdiagramm, das ein Verfahren zeigt, in dem der PC (oder das Wiedergabegerät) einen Musikinhalt oder Ähnliches in die Halbleiter-Speicherkarte schreibt;

[0052] Fig. 9 ist ein Flussdiagramm, das ein Verfahren zeigt, in dem ein Musikinhalt oder Ähnliches aus der Halbleiter-Speicherkarte ausgelesen und von dem Wiedergabegerät (oder dem PC) wiedergegeben wird;

[0053] Fig. 10 ist ein Flussdiagramm, das den Betrieb zeigt, in dem das Wiedergabegerät (oder der PC) die in dem Authentisierungsbereich in der Halbleiter-Speicherkarte gespeicherte Anzahl von Auslesevorgängen abwickelt;

[0054] Fig. 11 ist ein Flussdiagramm, das den Betrieb zeigt, in dem das Wiedergabegerät (oder der PC) die in dem Authentisierungsbereich in der Halbleiter-Speicherkarte gespeicherte Anzahl von erlaubten digitalen Ausgaben abwickelt;

[0055] Fig. 12 zeigt eine Datenstruktur, die die Authentisierungs- und Nicht-Authentisierungsbereiche der Halbleiter-Speicherkarte gemeinsam haben, und zeigt ebenso ein Flussdiagramm des Lese-/Schreibvorgangs entsprechend der Datenstruktur;

[0056] Fig. 13A bis Fig. 13D zeigen eine Änderung in der Beziehung zwischen den logischen Adressen und physikalischen Adressen, wobei Fig. 13A die Beziehung vor der Änderung zeigt, Fig. 13B die Beziehung nach der Änderung zeigt, Fig. 13C eine Umwandlungstabelle entsprechend Fig. A zeigt, und Fig. 13D eine Umwandlungstabelle entsprechend Fig. B zeigt;

[0057] Fig. 14A bis Fig. 14D zeigen Funktionen, die sich auf nicht-gelöschte Blöcke in der Halbleiter-Speicherkarte beziehen, wobei Fig. 14A den Benutzungszustand von logischen und physikalischen Blöcken und physikalischen Blöcken zeigt, Fig. 14B die Liste nicht-gelöschter Blöcke entsprechend dem Benutzungszustand der in Fig. 14A gezeigten Blöcke zeigt, Fig. 14C ein Flussdiagramm ist, das das Verfahren des PCs oder des Wiedergabegeräts zum Löschen von Blöcken im voraus unter Verwendung des Befehls für Listen Nicht-gelöschter Blöcke und des Löschbefehls, und Fig. 14D ist eine Tabelle, die den Benutzungszustand der logischen Blöcke zeigt;

[0058] Fig. 15 zeigt eine Kommunikationssequenz in einer Authentisierung zwischen dem Wiedergabegerät und der Halbleiter-Speicherkarte und zeigt ebenfalls Hauptkomponenten, die in der Authentisierung verwendet werden;

[0059] Fig. 16 zeigt eine Kommunikationssequenz in einer Variation der Authentisierung der vorliegenden Erfindung zwischen der Speicherkarte und einer externen Einrichtung;

[0060] Fig. 17 zeigt eine Kommunikationssequenz in einem detaillierten Verfahren der in Fig. 16 gezeigten gegenseitigen Authentisierung;

[0061] Fig. 18A bis Fig. 18C zeigen den Zustand, bevor die Begrenzung zwischen dem Authentisierungs- und Nicht-Authentisierungsbereich der Halbleiter-Speicherkarte geändert wird, wobei Fig. 18A ein Speicherabbild ist, das die Konstruktion der physikalischen Blöcke in dem Flash-Speicher zeigt, Fig. 18B eine Umwandlungstabelle zeigt, die für den Nicht-Authentisierungsbereich bestimmt ist, und Fig. 18C eine Umwandlungstabelle zeigt, die für den Authentisierungsbereich bestimmt ist; und

[0062] Fig. 19A bis Fig. 19C den Zustand zeigen, nachdem die Begrenzung zwischen dem Authentisierungs- und Nicht-Authentisierungsbereich der Halbleiter-Speicherkarte geändert wird, wobei Fig. 19A ein Speicherabbild ist, das die Konstruktion der physikalischen Blöcke in dem Flash-Speicher zeigt, Fig. 19B eine Umwandlungstabelle zeigt, die für den Nicht-Authentisierungsbereich bestimmt ist, und Fig. 19C eine Umwandlungstabelle zeigt, die für den Authentisierungsbereich bestimmt ist.

BESCHREIBUNG DER BEVORZUGTEN AUSFÜHRUNGSFORMEN

[0063] Eine Ausführungsform der vorliegenden Erfindung wird unter Bezugnahme auf die Zeichnungen beschrieben.

[0064] Fig. 1 ist eine schematische Repräsentation eines PCs, der digitale Inhalte, wie Musikinhalte, über ein Kommunikationsnetz herunterlädt, und einer Halbleiter-Speicherkarte (nachfolgend als Speicherkarte bezeichnet), die in den PC geladen und von diesem entfernt werden kann.

[0065] Ein PC **102** umfasst eine Anzeige **103**, eine Tastatur **104** und Lautsprecher **106**, und ist mit einer Kommunikationsleitung **101** über ein in den PC **102** eingefügtes Modem verbunden. Ein Speicherkartenschreibgerät **107** wurde in einen Karteneinschub (ein Einschubschlitz **105** für Speicherkartenschreibgeräte) des PCs **102** eingeführt. Der Einschubschlitz **105** für Speicherkartenschreibgeräte beruht auf PCMCIA (Personal Computer Memory Card International Association) Normen oder Ähnlichem. Das Speicherkarteschreibgerät **107** ist ein Adapter, der den PC **102** und eine Speicherkarte **109** elektrisch verbindet. Die Speicherkarte **109** ist in einen Einschubschlitz **108** für Speicherkarten des Speicherkartenschreibgeräts **107** eingefügt.

[0066] Der Benutzer erhält Musikdaten von einem Inhaltsanbieter im Internet unter Verwendung des obigen Systems und des folgenden Verfahrens.

[0067] Zuerst lädt der Benutzer einen gewünschten Musikinhalt in eine Festplatte in den PC **102** über die Kommunikationsleitung **101** herunter. Da der Musikinhalt verschlüsselt wurde, ist der Benutzer jedoch genötigt, ein gewisses Verfahren auszuführen, um den erhaltenen Musikinhalt auf dem PC **102** wieder zu geben.

[0068] Um den erhaltenen Musikinhalt wieder zu geben, muss der Benutzer dem Inhaltanbieter unter Verwendung einer Kreditkarte oder Ähnlichem im voraus die Gebühr bezahlen. Wenn der Benutzer die Gebühr bezahlt, empfängt der Benutzer ein Kennwort und Rechtsinformation von dem Inhaltsanbieter. Das Kennwort ist ein Schlüssel, der von dem Benutzer verwendet wird, um den verschlüsselten Musikinhalt zu entschlüsseln. Die Rechtsinformation zeigt verschiedene Bedingungen, unter denen dem Benutzer erlaubt wird, den Inhalt auf dem PC wieder zu geben, wie die Anzahl erlaubter Wiedergaben, die An-

zahl erlaubter Schreibvorgänge auf die Speicherkarte, und ein Ablaufdatum, das eine Periode kennzeichnet, in der dem Benutzer erlaubt wird, den Inhalt wieder zu geben.

[0069] Nach dem Erhalten des Kennworts und der Rechtsinformation gibt der Benutzer, beim Versuchen, die Musik über die Lautsprecher **106** des PCs **102** auszugeben, das Kennwort über die Tastatur **104** in den PC **102** ein, während ein dediziertes Anwendungsprogramm (im Folgenden bezeichnet als Anwendung) mit einer Copyright-Schutzfunktion auf dem PC **102** läuft. Die Anwendung überprüft dann die Rechtsinformation, entschlüsselt den verschlüsselten Musikinhalt und Verwendung des Kennworts und gibt den entschlüsselten Musikinhalt wieder, um die Töne über die Lautsprecher **106** auszugeben.

[0070] Wenn die Rechtsinformation anzeigt, dass es erlaubt ist, den Inhalt auf die Speicherkarte zu schreiben, kann die Anwendung die verschlüsselten Musikdaten, Kennwort und Rechtsinformation auf die Speicherkarte **109** schreiben.

[0071] Fig. 2 ist eine schematische Repräsentation einer tragbaren Kopier-/Wiedergabevorrichtung (im Folgenden bezeichnet als Abspielgerät) **201**, für die die Speicherkarte **109** als ein Aufzeichnungsmedium verwendet wird.

[0072] Auf der oberen Oberfläche des Abspielgeräts **201** sind eine Flüssigkristallanzeigeeinheit **202** und Bedienungstasten **203** gebildet. Auf der Vorderseite des Abspielgeräts **201** sind ein Einschubschlitz **206** für Speicherkarten und ein Kommunikationsanschluss **213** gebildet, wobei die Speicherkarte **109** in den Einschubschlitz **206** für Speicherkarten eingefügt ist, und der Kommunikationsanschluss **213** durch einen USB (Universal Serial Bus) oder ähnliches erreicht wird, und zu dem PC **102** verbunden ist. Auf einer Seite des Abspielgeräts **201** sind ein analoger Ausgabeanschluss **204**, ein digitaler Ausgabeanschluss **205** und ein analoger Eingabeanschluss **223** gebildet.

[0073] Das Abspielgerät **201** überprüft die Rechtsinformation, nachdem die Speicherkarte **109**, die die Musikdaten, ein Kennwort und Rechtsinformationen speichert, in das Abspielgerät **201** geladen wurde. Wenn es erlaubt ist, die Musik wiederzugeben, liest das Abspielgerät **201** die Musikdaten aus, entschlüsselt die ausgelesenen Musikdaten, wandelt den entschlüsselten Musikinhalt in ein Analogsignal um, und gibt die Töne des analogen Signals über Kopfhörer **208**, die mit dem analogen Ausgabeanschluss **204** verbunden sind, aus. Alternativ gibt das Abspielgerät **201** digitale Daten der Musikdaten zu dem digitalen Ausgabeanschluss **205** aus.

[0074] Das Abspielgerät **201** kann ebenfalls ein analoges Audiosignal, das über ein Mikrofon oder ähnliches über den analogen Eingabeanschluss **223** in das Abspielgerät **201** eingegeben werden, in digitale Daten umwandeln und speichert die digitalen Daten in der Speicherkarte **109**. Das Abspielgerät **201** kann ebenfalls Musikdaten, ein Kennwort und Rechtsinformation von dem PC **102** über den Kommunikationsport **213** herunterladen und die heruntergeladene Information auf der Speicherkarte **109** aufzeichnen. Anders ausgedrückt, das Abspielgerät **201** kann den PC **102** und das Speicherkartenschreibgerät **107**, die in Fig. 1 gezeigt sind, hinsichtlich des Aufzeichnens der Musikdaten auf der Speicherkarte **109** ersetzen und der Wiedergabe der auf der Speicherkarte **109** aufgezeichneten Musikdaten.

[0075] Fig. 3 ist ein Blockdiagramm, das die Hardwarekonstruktion vom PC **102** zeigt.

[0076] Der PC **102** umfasst eine CPU **110**, eine ROM **111**, die einen Einrichtungsschlüssel **111a** und ein Steuerprogramm **111b** vorspeichert, eine RAM **112**, die Anzeige **103**, einen Kommunikationsport **113**, der einen Modemport, der für die Verbindung zu der Kommunikationsleitung **101** verwendet wird, und einen USB, der für die Verbindung zu dem Abspielgerät **201** verwendet wird, umfasst, die Tastatur **104**, einen internen Bus **114**, das Speicherkartenschreibgerät **107**, das die Speicherkarte **109** und den internen Bus **214** verbindet, einen Descrambler **117** zum Entscrambeln der verschlüsselten Musikdaten, die aus der Speicherkarte **109** ausgelesen werden, einen AAC-Decodierer **118**, der konform zu der MPEG2-AAC (ISO13818-7)-Norm zum Decodieren der entscrambelten Musikdaten ist, einen D/A-Wandler **119** zum Umwandeln der decodierten digitalen Musikdaten in ein analoges Audiosignal, die Lautsprecher **106**, und eine Festplatte **120**, die ein Dateimanagementsoftwareprogramm und eine Anwendung speichert.

[0077] Der PC **102** kann das Folgende ausführen:

(1) Verwenden der Speicherkarte **109** als eine Externspeichervorrichtung mit einem unabhängigen Dateisystem (z. B. ISO9293), das Festplatten hat, durch Ausführen des in der Festplatte **120** gespeicherten Dateimanagementsoftwareprogramms,

(2) Herunterladen von Musikinhalten oder Ähnlichem von der Kommunikationsleitung **101** über den Modemport des Kommunikationsports **113** durch Ausführen der dedizierten, in der Festplatte **120** gespeicherten Anwendung,

(3) Speichern der Musikinhalte oder Ähnlichem in der Speicherkarte **109** nach einer gegenseitigen Authentisierung, und

(4) Auslesen der Musikinhalte oder Ähnlichem von der Speicherkarte **109** und Ausgeben der ausgelesenen Inhalte an die Lautsprecher **106** zur Wiedergabe.

[0078] Der in dem ROM **111** gespeicherte Einrichtungsschlüssel **111a** ist ein geheimer, für den PC **102** eindeutiger Schlüssel und wird, wie später beschrieben wird, für die gegenseitige Authentisierung oder Ähnliches verwendet.

[0079] Fig. 4 ist ein Blockdiagramm, das die Hardwarekonstruktion des Abspielgeräts **201** zeigt.

[0080] Das Abspielgerät **201** umfasst eine CPU **210**, ein ROM **211**, der einen Einrichtungsschlüssel **211a** und ein Steuerprogramm **211b** vorspeichert, ein RAM **212**, eine Flüssigkristallanzeigeeinheit **203**, einen Kommunikationsport **213**, der durch einen USB oder Ähnliches erzielt wird, der für die Verbindung zu dem PC **102** verwendet wird, Bedienungstasten **202**, einen internen Bus **214**, eine Kartenschnittstelleneinheit **215**, die die Speicherkarte **109** und den internen Bus **214** verbindet, eine Authentisierungsschaltung **216** zum Ausführen einer gegenseitigen Authentisierung mit der Speicherkarte **109**, einen Descrambler **217** zum Entscrambeln der verschlüsselten Musikdaten, die aus der Speicherkarte **109** ausgelesen werden, einen AAC-Decodierer **218**, der konform ist zu der MPEG2-AAC (ISO13818-7)-Norm zum Decodieren der entscrambelten Musikdaten, einen D/A-Wandler **219** zum Umwandeln der decodierten digitalen Musikdaten in ein analoges Audiosignal, Lautsprecher **224**, einen A/D-Wandler **221** zum Umwandeln eines von dem analogen Eingabeanschluss **223** eingegebenen analogen Audiosignal in digitale Musikdaten, einen AAC-Codierer **220**, der konform ist zu der MPEG2-AAC (ISO13818-7)-Norm zum Codieren der digitalen Musikdaten, einen Scrambler **222** zum Scrambeln der codierten Musikdaten, einen analogen Ausgabeanschluss **204**, einen digitalen Ausgabeanschluss **205** und einen analogen Eingabeanschluss **223**.

[0081] Das Abspielgerät **201** lädt das Steuerprogramm **211b** von dem ROM **211** in den RAM **212**, um der CPU **210** zu erlauben, das Steuerprogramm **211b** auszuführen. Durch ein Ausführen hiervon kann das Abspielgerät **201** Musikinhalte von der Speicherkarte **109** auslesen, wiedergeben und die ausgelesenen Musikinhalte an die Lautsprecher **224** ausgeben und kann ebenfalls über den analogen Eingabeanschluss **223** und Kommunikationsport **213** eingegebene Musikinhalte in der Speicherkarte **109** speichern. Anders ausgedrückt kann der Benutzer das Abspielgerät **201** nicht nur zum persönlichen Kopieren und Wiedergeben von Musik wie mit gewöhnlichen Wiedergabegeräten verwenden, sondern ebenfalls zum Kopieren und Wiedergeben solcher Musikinhalte (die durch Copyright geschützt sind), wie sie durch ein elektronisches Musikverbreitungssystem verbreitet werden und durch den PC **102** heruntergeladen werden.

[0082] Fig. 5 zeigt die Ansicht und Hardwarekonstruktion der Speicherkarte **109**.

[0083] Die Speicherkarte **109** enthält einen wiederbeschreibbaren nichtflüchtigen Speicher, zu dem Daten wiederholt geschrieben werden können. Der wiederbeschreibbare nichtflüchtige Speicher weist eine Kapazität von 64 MB auf und wird durch eine Spannungsversorgung von 3,3 V und ein Taktsignal, das von externen Quellen zugeführt wird, gesteuert. Die Speicherkarte **109** ist ein 2,1 mm dicker, 24 mm breiter und 32 mm tiefer rechteckiger Quader. Die Speicherkarte **109** wird mit einem Schreibschutzschalter auf ihrer Seite bereitgestellt und ist elektrisch mit einer externen Vorrichtung über einen Verbindungsanschluss mit neun Kontakten, der an einem Ende der Speicherkarte **109** ausgebildet ist, verbunden.

[0084] Die Speicherkarte **109** umfasst drei IC-Chips: einen Steuer-IC **302**, einen Flash-Speicher **303** und ein ROM **304**.

[0085] Der Flash-Speicher **303** ist ein Flash-löschbarer, wiederbeschreibbarer nichtflüchtiger Speicher vom Blocklöschungstyp und umfasst logische Speicherbereiche: einen Authentisierungsbereich **332** und einen Nicht-Authentisierungsbereich **331**. Auf den Authentisierungsbereich **332** kann nur von den Vorrichtungen zugegriffen werden, die als geeignete Vorrichtungen authentisiert wurden. Auf den Nicht-Authentisierungsbereich **331** kann von allen Vorrichtungen zugegriffen werden, gleich, ob diese authentisiert wurden oder nicht. In der vorliegenden Ausführungsform wird der Authentisierungsbereich **332** zum Speichern von wichtigen Daten, die sich auf Copyrightschutz beziehen, verwendet, und der Nicht-Authentisierungsbereich **331** wird als eine Externspeichervorrichtung in einem typischen Computersystem verwendet. Es ist festzuhalten, dass eine gewisse Adresse in dem Flash-Speicher **303** als eine Begrenzung zwischen diesen beiden Speicherbereichen verwendet wird.

[0086] Der ROM **304** umfasst einen Speicherbereich, der ein Festwertbereich ist und Spezialbereich genannt wird. Der Spezialbereich speichert Informationen vor, umfassend: eine Medium-ID **341**, die eine Identifizierung der Speicherkarte **109** ist; und einen Herstellernamen **342**, der den Namen des Herstellers der Speicherkarte **109** kennzeichnet. Es ist festzuhalten, dass die Medium-ID **341** für die Speicherkarte **109** eindeutig ist und die Speicherkarte **109** von den anderen Halbleiter-Speicherkarten unterscheidet, und dass die Medium-ID **341** für die gegenseitige Authentisierung zwischen Vorrichtungen verwendet wird und zum Verhindern eines nichtautorisierten Zugriffs auf den Authentisierungsbereich **332** verwendet wird.

[0087] Der Steuer-IC **302** ist eine Steuerschaltung bestehend aus aktiven Elementen (logischen Gattern

und Ähnlichem) und umfasst eine Authentisierungseinheit **321**, eine Befehlsentscheidungs-Steuereinheit **322**, eine Speichereinheit **323** für einen Master-Schlüssel, eine Spezialbereich-Zugriffssteuereinheit **324**, eine Authentisierungsbereichs-Zugriffssteuereinheit **325**, eine Nicht-Authentisierungsbereichs-Zugriffssteuereinheit **326** und eine Verschlüsselungs-/Entschlüsselungsschaltung **327**.

[0088] Die Authentisierungseinheit **321** ist eine Schaltung, die eine gegenseitige Authentisierung vom Herausforderungs-Antworttyp (Typ mit Authentisierungsabfrage und -antwort), ausführt, mit einer Fernvorrichtung, die versucht, auf die Speicherkarte **109** zuzugreifen. Die Authentisierungseinheit **321** umfasst einen Zufallsgenerator und eine Verschlüsselungseinheit und authentisiert die Fernvorrichtung als eine geeignete, wenn bestätigt wird, dass die Fernvorrichtung dieselbe Verschlüsselungseinheit aufweist wie die lokale Vorrichtung. Es ist festzuhalten, dass in der gegenseitigen Authentisierung vom Herausforderungs-Antworttyp beide der zwei sich in Kommunikation befindenden Vorrichtungen das Folgende ausführen: die lokale Vorrichtung sendet zuerst Herausforderungsdaten zu der Fernvorrichtung, die Fernvorrichtung wiederum erzeugt Antwortdaten durch Verarbeiten der empfangenen Herausforderungsdaten zum Zertifizieren der Eignung der Fernvorrichtung und sendet die erzeugten Antwortdaten zu der lokalen Vorrichtung, und die lokale Vorrichtung entscheidet, ob die Fernvorrichtung geeignet ist durch Vergleichen der Herausforderungsdaten mit den Antwortdaten.

[0089] Die Befehlsentscheidungs-Steuereinheit **322** ist eine Steuerung, die aus einer Decodierschaltung und einer Steuerschaltung aufgebaut ist. Die Decodierschaltung identifiziert einen Befehl (eine Anweisung an die Speicherkarte **109**), der über einen Befehlskontakt eingegeben wird, und führt den identifizierten Befehl aus. Die Befehlsentscheidungs-Steuereinheit **322** steuert die Komponenten **321** bis **327** in Übereinstimmung mit den empfangenen Befehlen.

[0090] Die von der Befehlsentscheidungs-Steuereinheit **322** empfangenen Befehle umfassen nicht nur Befehle zum Lesen, Schreiben und Löschen von Daten von/zu dem Flash-Speicher **303**, sondern auch Befehle zum Steuern des Flash-Speichers **303** (Befehle, die sich auf einen Adressraum, nicht-gelöschte Daten, etc. beziehen).

[0091] Zum Beispiel werden in Bezug auf ein Lesen/Schreiben von Daten der Befehl zum Zählen von SecureRead-Adressen (SecureRead address count command und der Befehl zum Zählen von SecureWrite-Adressen (SecureWrite address count command) als Befehle festgelegt, zum Zugreifen auf den Authentisierungsbereich **332**, und der Befehl zum Zählen von Leseadressen und der Befehl zum Zählen von Schreibadressen werden als Befehle zum Zugreifen auf den Nicht-Authentisierungsbereich **331** festgelegt. In den obigen Befehlen ist "Adresse" eine serielle Nummer des ersten Sektors einer Sequenz von Sektoren, von/zu denen Daten gelesen oder geschrieben werden durch den Befehl. "Zahl" (count) ist die totale Anzahl von Sektoren, von/zu denen Daten durch den Befehl gelesen oder geschrieben werden. "Sektor" ist eine Einheit, die die Menge von von/zu der Speicherkarte **109** gelesenen oder geschriebenen Daten repräsentiert. In der vorliegenden Ausführungsform ist ein Sektor 512 Bytes.

[0092] Die Speichereinheit **323** für einen Master-Schlüssel speichert einen Master-Schlüssel **323a** vor, der verwendet wird von der Fernvorrichtung während der gegenseitigen Authentisierung, und wird verwendet, um Daten in dem Flash-Speicher **303** zu schützen.

[0093] Die Spezialbereich-Zugriffssteuereinheit **324** ist eine Schaltung zum Auslesen von Information, wie der Medium-ID **341**, aus dem Spezialbereich (ROM) **304**.

[0094] Die Authentisierungsbereich-Zugriffsteuereinheit **325** und die Nicht-Authentisierungsbereich-Zugriffssteuereinheit **326** sind Schaltungen zum Lesen/Schreiben von Daten von/zu dem Authentisierungsbereich **332** und dem Nicht-Authentisierungsbereich **331**, jeweils. Jede der Einheiten **325** und **326** sendet/empfängt Daten zu/von externen Vorrichtungen (dem PC **102**, dem Abspielgerät **201**, etc.) über vier Datenkontakte.

[0095] Es wird hier festgehalten, dass die Zugriffssteuereinheiten **325** und **326** jeweils einen Pufferspeicher enthalten, der so groß ist wie ein Block (32 Sektoren, oder 16 Kbytes), und logisch Daten in Einheiten von Sektoren zu/von dem Bereich **332** oder **331** in Antwort auf einen von einer externen Vorrichtung ausgegebenen Befehl eingibt/ausgibt, obwohl diese Daten in Einheiten von Blöcken eingibt/ausgibt, wenn der Flash-Speicher **303** wiederbeschrieben wird. Spezifischer ausgedrückt, wenn ein Sektor in dem Flash-Speicher **303** wiederbeschrieben werden soll, liest die Zugriffssteuereinheit **325** oder **326** Daten von einem Block einschließlich des Sektors von dem Flash-Speicher **303** aus, löscht den Block in den Flash-Speicher **303** auf einmal, wiederbeschreibt den Sektor in dem Pufferspeicher und schreibt dann den Datenblock umfassend den wiederbeschriebenen Sektor zu dem Flash-Speicher **303**.

[0096] Die Verschlüsselungs-/Entschlüsselungsschaltung **327** ist eine Schaltung, die eine Verschlüsselung und Entschlüsselung unter Verwendung des in der Speichereinheit **323** für einen Masterschlüssel gespeicherten Masterschlüssels **323a** ausführt, unter der Steuerung durch die Authentisierungsbe-

reich-Zugriffssteuereinheit **325** und die Nicht-Authentisierungsbereich-Zugriffssteuereinheit **326**. Die Verschlüsselungs-/Entschlüsselungsschaltung **327** verschlüsselt Daten vor einem Schreiben der Daten zu dem Flash-Speicher **303** und entschlüsselt die Daten nach einem Auslesen der Daten aus dem Flash-Speicher **303**. Diese Verschlüsselung und Entschlüsselung werden ausgeführt, um ungesetzliche Vorgänge, wie einen Vorgang eines Zerlegens der Speicherkarte **109**, einem direkten Analysieren der Inhalte des Flash-Speichers **303** und einem Stehlen des Kennworts von dem Authentisierungsbereich **332** zu verhindern.

[0097] Es sollte an dieser Stelle festgehalten werden, dass der Steuerungs-IC **302** eine Synchronisierungsschaltung, einen flüchtigen Speicherbereich und einen nichtflüchtigen Speicherbereich sowie die Hauptkomponenten **321** bis **327** umfasst. Die Synchronisierungsschaltung erzeugt ein internes Taktsignal in Synchronisation mit einem von einem Taktsignalkontakt zugeführten Taktsignal, und führt das erzeugte, interne Taktsignal jeder Komponente zu.

[0098] Um die in dem Spezialbereich (ROM) **304** gespeicherte Information gegen ein Manipulieren durch nichtautorisierte Personen zu schützen, kann der Spezialbereich (ROM) **304** ebenfalls in den Steuer-IC eingebettet werden. Alternativ kann die Information in dem Flash-Speicher **303** gespeichert werden. In diesem Fall kann die Spezialbereich-Zugriffssteuereinheit **324** eine Beschränkung auf ein Schreiben von Daten zu der Information aufzwingen, oder die Verschlüsselungs-/Entschlüsselungsschaltung **327** kann die Information verschlüsseln, bevor die Information in dem Flash-Speicher **303** gespeichert wird.

[0099] Fig. 6 zeigt verschiedene Speicherbereiche in der Speicherkarte **109**, die von dem PC **102** und dem Abspielgerät **201** erkannt werden können. Die Speicherbereiche in der Speicherkarte **109** werden in drei Hauptbereiche klassifiziert: Spezialbereich **304**, Authentisierungsbereich **332** und Nicht-Authentisierungsbereich **331**.

[0100] Der Spezialbereich **304** ist ein Festwertbereich. Ein dedizierter Befehl wird verwendet, um Daten von dem Spezialbereich **304** zu lesen. Ein Lesen/Schreiben von Daten von/zu dem Authentisierungsbereich **332** ist nur dann möglich, wenn die Authentisierung zwischen dem PC **102** und dem Abspielgerät **201** und der Speicherkarte **109** bejahend war. Ein verschlüsselter Befehl wird verwendet, um auf den Authentisierungsbereich **332** zuzugreifen. Auf den Nicht-Authentisierungsbereich **331** kann durch Befehle zugegriffen werden, die öffentlich verfügbar sind, wie die Befehle, die zu der ATA (AT-Anhang) oder SCSI (Small Computer System Interface)-Norm konform sind. Anders ausgedrückt können Daten von/zu dem Nicht-Authentisierungsbereich **331** ohne einen Authentisierungsvorgang gelesen/geschrieben werden. Dementsprechend kann ein Dateimanagementsoftwareprogramm, das eine Standardausrüstung des PCs **102** ist, zum Lesen/Schreiben von Daten von/zu dem Nicht-Authentisierungsbereich **331** verwendet werden, wie mit einem Flash-ATA oder einem kompakten Flash.

[0101] Die drei Hauptbereiche speichern die Arten von Information, die unten stehend gezeigt werden, die den Bereichen eine Funktion als eine Externspeichervorrichtung für einen typischen PC, und eine Funktion, um die durch ein elektronisches Musikverbreitungssystem verbreiteten Musikdaten copyright zu schützen, bereitstellen.

[0102] Der Nicht-Authentisierungsbereich **331** speichert einen verschlüsselten Inhalt **426**, Anwenderdaten **427** etc. Der verschlüsselte Inhalt **426** ist Musikdaten, die Objekt eines Copyright-Schutzes sind und verschlüsselt wurden. Die Anwenderdaten **427** sind allgemeine Daten, die für einen Copyright-Schutz irrelevant sind. Der Authentisierungsbereich **332** speichert einen Verschlüsselungsschlüssel **425**, der ein geheimer Schlüssel ist, der für ein Entschlüsseln des verschlüsselten Inhalts **426**, der in dem Nicht-Authentisierungsbereich **331** gespeichert ist, verwendet wird. Der Spezialbereich **304** speichert die Medium-ID **341**, die für ein Zugreifen auf den Authentisierungsbereich **332** notwendig ist.

[0103] Der PC **102** oder das Abspielgerät **201** lesen zuerst die Medium-ID **341** aus dem Spezialbereich **304** in der Speicherkarte **109** aus, die darin geladen ist, und extrahieren dann den Verschlüsselungsschlüssel **425** und die Rechtsinformation aus dem Authentisierungsbereich **332** unter Verwendung der Medium-ID **341**. Wenn bestätigt wird von der Rechtsinformation, dass der in dem Nicht-Authentisierungsbereich **331** gespeicherte verschlüsselte Inhalt **426** wiedergegeben werden darf, kann der verschlüsselte Inhalt **426** ausgelesen und wiedergegeben werden, während dieser mit dem Verschlüsselungsschlüssel **425** entschlüsselt wird.

[0104] Hier sei angenommen, dass ein Anwender unter Verwendung des PCs **102** oder Ähnlichem nur die Musikdaten zu dem Nicht-Authentisierungsbereich **331** in der Speicherkarte **109** schreibt, die ungesetzlich erhalten wurden, dann versucht, die Musikdaten von der Speicherkarte **109**, die in das Abspielgerät **201** geladen wurde, wieder zu geben. In diesem Fall ist kein Verschlüsselungsschlüssel **425** oder Rechtsinforamation entsprechend den Musikdaten in dem Authentisierungsbereich **332** gespeichert, obwohl der Nicht-Authentisierungsbereich **331** in der Speicherkarte **109** die Musikdaten speichert. Somit gelingt es dem Abspielgerät **201** nicht, die Musikdaten wieder zu geben. Mit solch einer Konstruktion, in

der der Musikinhalt nicht wiedergegeben werden kann, wenn nur ein Musikinhalt zu der Speicherkarte **109** kopiert wird ohne autorisierten Verschlüsselungsschlüssel oder Rechtsinformation kann, ein nichtautorisiertes Kopieren von Digitalinhalten verhindert werden.

[0105] Die Fig. 7A, Fig. 7B und Fig. 7C zeigen Beschränkungen und Befehlsformate, wenn der PC **102** oder das Abspielgerät **201** auf einen Bereich in der Speicherkarte **109** zugreift. Fig. 7A zeigt Regeln, die befolgt werden müssen zum Zugreifen auf jeden Bereich. Fig. 7B zeigt Regeln, die befolgt werden müssen zum Ändern der Größe jedes Bereichs. Fig. 7C ist eine schematische Darstellung der Bereiche in der Speicherkarte **109**.

[0106] Der Spezialbereich **304** ist ein Festwertbereich, auf den durch einen dedizierten Befehl ohne einen Authentisierungsvorgang zugegriffen werden kann. Die in dem Spezialbereich **304** gespeicherte Medium-ID **341** wird verwendet, um den verschlüsselten Befehl, der verwendet wird, um auf den Authentisierungsbereich **332** zuzugreifen, zu erzeugen oder zu entschlüsseln. Spezifischer ausgedrückt liest der PC **102** oder das Abspielgerät **201** die Medium-ID **341** aus, verschlüsselt einen Befehl, der verwendet werden muss, um auf den Authentisierungsbereich **332** zuzugreifen, und sendet den verschlüsselten Befehl zu der Speicherkarte **109**. Beim Empfangen des verschlüsselten Befehls entschlüsselt die Speicherkarte **109** den verschlüsselten Befehl unter Verwendung der Medium-ID **341**, interpretiert und führt den Befehl aus.

[0107] Auf den Authentisierungsbereich **332** kann nur zugegriffen werden, wenn eine Authentisierung zwischen einer Vorrichtung, die versucht, auf die Speicherkarte **109** zuzugreifen, wie der PC **102** oder das Abspielgerät **201**, und der Speicherkarte **109** bejahend war. Die Größe des Authentisierungsbereichs **332** entspricht der Größe von (YYYY + 1) Sektoren. Das heißt, der Authentisierungsbereich **332** besteht logisch aus Sektor 0 bis Sektor YYYY (YYYYter Sektor), und besteht physikalisch aus Sektoren mit einer XXXXten Sektoradresse bis zu einer (XXXX + YYYY)ten Sektoradresse in dem Flash-Speicher **303**. Es ist festzuhalten, dass die Sektoradressen serielle Nummern sind, die eindeutig allen Sektoren zugewiesen sind, die den Flash-Speicher **303** bilden.

[0108] Auf den Nicht-Authentisierungsbereich **331** kann durch einen Standardbefehl, der zu der ATA oder SCSI-Norm konform ist, zugegriffen werden. Die Größe des Nicht-Authentisierungsbereichs **331** entspricht XXXX Sektoren, d. h., der Nicht-Authentisierungsbereich **331** besteht logisch und physikalisch aus Sektor 0 bis (XXXX – 1)ten Sektor.

[0109] Es sollte hier festgehalten werden, dass ein veränderbarer Blockbereich **501** zuvor in dem Flash-Speicher **303** zugewiesen werden kann. Der veränderbare Blockbereich **501** ist eine Gruppe von veränderbaren Blöcken, die verwendet werden, um fehlerhafte Blöcke (Blöcke, die einen fehlerhaften Speicherbereich aufweisen, von/zu dem Daten nicht normal gelesen/geschrieben werden können) in dem Authentisierungsbereich **332** oder dem Nicht-Authentisierungsbereich **331** zu ersetzen.

[0110] In der vorliegenden Ausführungsform kann auf den Spezialbereich **304** ohne Authentisierung zugegriffen werden. Jedoch kann der Spezialbereich **304** nur für solche Vorrichtungen zugänglich gemacht werden, die bejahend authentisiert werden, oder Befehle, die für ein Zugreifen auf den Spezialbereich **304** verwendet werden, können verschlüsselt werden, um eine ungesetzliche Analyse durch irgendwelche Personen zu verhindern.

[0111] Nun wird unter Bezugnahme auf die Fig. 7B und Fig. 7C ein Ändern der Größe des Authentisierungsbereichs **332** und des Nicht-Authentisierungsbereichs **331** beschrieben werden.

[0112] Die Gesamtspeicherkapazität des Authentisierungsbereichs **332** und des Nicht-Authentisierungsbereichs **331** in dem Flash-Speicher **303** entspricht der Kapazität von (XXXX + YYYY +1) Sektoren, was ein Festwert ist, der durch ein Subtrahieren des veränderbaren Blockbereichs **501** und anderen von allen Speicherbereichen in dem Flash-Speicher **303** erhalten wird. Die Größen der Bereiche **332** und **331** sind jeweils variabel und können durch Ändern des Begrenzungsadresswerts XXXX geändert werden.

[0113] Der erste Schritt in dem Vorgang zum Ändern der Größe eines Bereichs ist, Authentisierung ausführen. Diese Authentisierung wird ausgeführt, um alle Anwender davon abzuhalten, einfach die Größe des Bereichs unter Verwendung von Standardausrüstungsprogrammen, die unter PC-Anwendern weit verbreitet sind, oder eines für einen ungesetzlichen Zugriff gedachten Softwareprogramms, zu ändern. Nachdem die Authentisierung ausgeführt wurde, wird die Größe des Nicht-Authentisierungsbereichs **331** (die Anzahl neuer Sektoren, XXXX) zu der Speicherkarte **109** unter Verwendung eines dedizierten Befehls zum Ändern der Bereichsgröße gesendet.

[0114] Die Speicherkarte **109** speichert den Wert XXXX beim Erhalten des obigen dedizierten Befehls zum Ändern der Bereichsgröße in dem nichtflüchtigen Speicherbereich oder Ähnlichem in der Speicherkarte **109**, steuert dann die nachfolgenden Zugriffe auf den Authentisierungsbereich **332** und den Nicht-Authentisierungsbereich **331** unter Verwendung des Werts XXXX als eine neue Begrenzungsa-

dresse. Spezifischer ausgedrückt ordnet die Speicherkarte **109** den physikalischen Sektor 0 bis XXXXten Sektor in dem Flash-Speicher **303** dem Nicht-Authentisierungsbereich **331** zu, und den XXXXten bis (XXXX + YYYY)ten Sektor dem Authentisierungsbereich **332** zu. Die Zugriffssteuereinheiten **325** und **326** führen die Adressumwandlung zwischen einer logischen Adresse und einer physikalischen Adresse aus und überwachen eine Erzeugung eines ungeeigneten Zugriffs nach außerhalb eines zugewiesenen Speicherbereichs. Es soll hier festgehalten werden, dass logische Adressen von einer Externvorrichtung als Adressen in einem Datenraum der Speicherkarte **109** erkannt werden, entsprechend zu den Werten, die in den Befehlen verwendet werden, und dass die physikalischen Adressen Adressen in einem Datenraum des Flash-Speichers **303** sind, der in der Speicherkarte **109** enthalten ist.

[0115] Falls die Größe des Authentisierungsbereichs **332** vergrößert wird durch Reduzieren der Begrenzungsadresse, wird eine Anordnung benötigt, um die logische Kompatibilität zwischen vor und nach der Adressänderung aufrecht zu erhalten. Zu diesem Zweck werden alle in dem Authentisierungsbereich **332** gespeicherten Daten bewegt (kopiert) zu kleineren Adressen durch die Größe der Reduzierung der Begrenzungsadresse, zum Beispiel. Mit dieser Anordnung entsprechen physikalische Adressen den neuen logischen Adressen, beginnend mit der neuen Begrenzungsadresse. Mit dieser Anordnung wird der Datenraum des Authentisierungsbereichs **332** vergrößert, während die logischen Adressen für die in dem Authentisierungsbereich **332** gespeicherten Daten aufrecht erhalten werden.

[0116] Der dedizierte Befehl zum Ändern der Bereichsgröße kann vor einem Verwenden verschlüsselt werden, um ungesetzliche Zugriffe zu verhindern.

[0117] Fig. 8 ist ein Flussdiagramm, das einen Vorgang zeigt, in dem der PC **102** (oder das Abspielgerät **201**) einen Musikinhalt oder Ähnliches auf die Speicherkarte **109** schreibt. In der folgenden Beschreibung wird angenommen, dass der PC **102** Musikdaten zu der Speicherkarte **109** (S601) schreibt.

(1) Der PC **102** führt eine Authentisierung vom Herausforderungs-Antworttyp mit der Authentisierungseinheit **321** der Speicherkarte **109** aus, unter Verwendung des Einrichtungsschlüssels **111a** und Ähnlichem, und extrahiert den Master-Schlüssel **323a** von der Speicherkarte **109**, wenn die Authentisierung bejahend war (S602).

(2) Der PC **102** extrahiert dann die Medium-ID **341** von dem Spezialbereich **304** in der Speicherkarte **109** unter Verwendung eines dedizierten Befehls (S603).

(3) Der PC **102** erzeugt dann eine Zufallszahl und erzeugt ein Kennwort, das zum Verschlüsseln der Musikdaten verwendet wird, von dem extrahierten Master-Schlüssel **323a** und der Medium-ID **341** (S604). In dem obigen Schritt wird die Zufallszahl z. B. durch ein Verschlüsseln der Herausforderungsdaten (Zufallszahl), die während des Authentisierungsvorgangs zu der Speicherkarte **109** gesendet wird, erzeugt.

(4) Das erzeugte Kennwort wird unter Verwendung des Master-Schlüssels **323a** und der Medium-ID **341** verschlüsselt und dann zu dem Authentisierungsbereich **332** als der Verschlüsselungsschlüssel **425** (S605) geschrieben. Zu diesem Zeitpunkt wurde, bevor die Daten (Verschlüsselungsschlüssel **425**) übertragen werden, der Befehl, Daten zu dem Authentisierungsbereich **332** zu schreiben, verschlüsselt und zu der Speicherkarte **109** gesendet.

(5) Die Musikdaten werden unter Verwendung des Kennworts verschlüsselt und in dem Nicht-Authentisierungsbereich **331** als der verschlüsselte Inhalt **426** gespeichert (S606).

[0118] Fig. 9 ist ein Flussdiagramm, das einen Vorgang zeigt, in dem ein Musikinhalt oder Ähnliches aus der Speicherkarte **109** ausgelesen wird, und von dem Abspielgerät **201** (oder dem PC **102**) wiedergegeben wird. In der folgenden Beschreibung wird angenommen, dass in der Speicherkarte **109** gespeicherte Musikdaten von dem Abspielgerät **201** wiedergegeben werden (S701).

(1) Das Abspielgerät **201** führt eine Authentisierung vom Herausforderungs-Antworttyp mit der Authentisierungseinheit **321** der Speicherkarte **109** unter Verwendung eines Einrichtungsschlüssels **211a** und Ähnlichem aus, und extrahiert den Master-Schlüssel **323a** von der Speicherkarte **109**, wenn die Authentisierung bejahend war (S702).

(2) Das Abspielgerät **201** extrahiert dann die Medium-ID **341** von dem Spezialbereich **304** in der Speicherkarte **109** unter Verwendung eines dedizierten Befehls (S703).

(3) Das Abspielgerät **201** extrahiert dann den Verschlüsselungsschlüssel **425** der Musikdaten von dem Authentisierungsbereich **332** in der Speicherkarte **109** (S704). Zu diesem Zeitpunkt wurde, bevor die Daten (Verschlüsselungsschlüssel **425**) ausgelesen werden, der Befehl, die Daten aus dem Authentisierungsbereich **332** auszulesen, verschlüsselt und zu der Speicherkarte **109** gesendet.

(4) Der erhaltene Verschlüsselungsschlüssel **425** wird unter Verwendung des Master-Schlüssels **323a** und der Medium-ID **341** entschlüsselt, um ein Kennwort zu extrahieren (S705). Dieser Entschlüsselungsschritt ist ein Umkehrschritt des Verschlüsselungsschritts S605, der in Fig. 8 gezeigt ist.

(5) Der verschlüsselte Inhalt **426** wird aus dem Nicht-Authentisierungsbereich **331** ausgelesen

und unter Verwendung des in dem Schritt S705 extrahierten Kennworts entschlüsselt, während der entschlüsselte Inhalt als Musik wiedergegeben wird (S706).

[0119] Wie oben beschrieben können die in dem Nicht-Authentisierungsbereich **331** in der Speicherkarte **109** gespeicherten Musikdaten nicht ohne den in dem Authentisierungsbereich **332** gespeicherten Verschlüsselungsschlüssel **425** entschlüsselt werden. Dementsprechend können die kopierten Musikdaten nicht normal wiedergegeben werden, falls nur Musikdaten ungesetzlich zu einer anderen Speicherkarte kopiert werden. Mit dieser Konstruktion wird das Copyright der Musikdaten sicher geschützt.

[0120] Wie ebenfalls obenstehend beschrieben, wird nur Vorrichtungen, die bejahend authentisiert wurden, erlaubt, auf den Authentisierungsbereich in der Speicherkarte zuzugreifen. Diese Konstruktion stellt einen Copyright-Schutz bereit, in dem nur den Vorrichtungen, die gewisse Bedingungen erfüllen, erlaubt wird, auf den Authentisierungsbereich in der Speicherkarte zuzugreifen. Dies wird erzielt durch ein selektives Verwenden des Einrichtungsschlüssels, des Verschlüsselungsalgorithmuses oder Ähnlichem, die für eine Authentisierung verwendet werden.

[0121] In dem obigen Beispiel wird, wenn ein verschlüsselter Inhalt zu der Speicherkarte **109** geschrieben wird, zuerst das bei der Verschlüsselung verwendete Kennwort unter Verwendung des Master-Schlüssels und der Medium-ID verschlüsselt, dann wird das verschlüsselte Kennwort in dem Authentisierungsbereich **332** als der Verschlüsselungsschlüssel gespeichert (S605). Jedoch kann sowohl der Master-Schlüssel als auch die Medium-ID verwendet werden, um das Kennwort zu verschlüsseln. Diese Konstruktion vereinfacht die Verschlüsselung und hat den Vorzug, dass die Schaltungsgröße der Speicherkarte **109** oder des Abspielgeräts **102** reduziert wird, obwohl hier eine Möglichkeit besteht, dass die Intensität der Verschlüsselung abgeschwächt wird.

[0122] In dem obigen Beispiel können das Abspielgerät **201** und der PC **102** den Master-Schlüssel **323a** von der Speicherkarte **109** nur dann extrahieren, wenn die Authentisierung bejahend war. Jedoch kann der Master-Schlüssel **323a** in das Abspielgerät **201** oder den PC **102** zuvor eingebettet werden. Alternativ kann der Master-Schlüssel **323a** verschlüsselt und in dem Spezialbereich **304** als ein verschlüsselter Master-Schlüssel gespeichert werden.

[0123] Nun werden zwei Beispiele der Verwendung des Authentisierungsbereichs der Speicherkarte beschrieben. In den beiden Beispielen werden "die Anzahl der Auslesevorgänge" und "die Anzahl erlaubter digitaler Ausgaben" jeweils in dem Authentisierungsbereich gespeichert.

[0124] Fig. 10 ist ein Flussdiagramm, das den Betrieb zeigt, in dem das Abspielgerät **201** (oder der PC **102**) die Anzahl von in dem Authentisierungsbereich in der Speicherkarte **109** gespeicherten Auslesevorgängen **812** abwickelt. In dem vorliegenden Beispiel kann das Abspielgerät **201** die in dem Nicht-Authentisierungsbereich **331** in der Speicherkarte **109** gespeicherten Musikdaten als ein Audiosignal so häufig wiedergegeben, wie durch die Anzahl **812** von in der Speicherkarte **109** gespeicherten Auslesevorgängen angezeigt wird (S801).

(1) Das Abspielgerät **201** führt eine Authentisierung vom Herausforderungs-Antworttyp mit der Authentisierungseinheit **321** der Speicherkarte **109** unter Verwendung eines Einrichtungsschlüssels **211a** und Ähnlichem aus und extrahiert den Master-Schlüssel **323a** von der Speicherkarte **109**, wenn die Authentisierung bejahend war (S802).

(2) Das Abspielgerät **201** extrahiert dann die Medium-ID **341** von dem Spezialbereich **304** in der Speicherkarte **109** unter Verwendung eines dedizierten Befehls (S803).

(3) Das Abspielgerät **201** extrahiert dann den Verschlüsselungsschlüssel **425** der Musikdaten von dem Authentisierungsbereich **332** in der Speicherkarte **109** (S804). Zu diesem Zeitpunkt wurde, bevor die Daten (Verschlüsselungsschlüssel **425**) ausgelesen werden, der Befehl, Daten aus dem Authentisierungsbereich **332** auszulesen, verschlüsselt und zu der Speicherkarte **109** gesendet.

(4) Das Abspielgerät **201** extrahiert dann die Anzahl **812** von Auslesevorgängen von dem Authentisierungsbereich **332** in der Speicherkarte **109**, und überprüft die Anzahl **812** von Auslesevorgängen (S804). Wenn die Anzahl eine Erlaubnis von unbeschränkten Auslesevorgängen anzeigt, gibt das Abspielgerät **201** die Musik in Übereinstimmung mit dem Vorgang (S704 bis S706), der in Fig. 9 gezeigt ist, wieder (S806 bis S808).

(5) Wenn die Anzahl **812** von Auslesevorgängen 0 ist, wird entschieden, dass kein Auslesen erlaubt ist (S805) und der Wiedergabevorgang endet (S809). Wenn die Anzahl **812** von Auslesevorgängen ein anderer Wert als 0 ist, und keine Erlaubnis von unbeschränkten Auslesevorgängen anzeigt, reduziert das Abspielgerät **201** die Anzahl um 1, schreibt die resultierende Anzahl zu dem Authentisierungsbereich **332** (S805) und gibt dann die Musik in Übereinstimmung mit dem Vorgang (S704 bis S706), der in Fig. 9 gezeigt wird, wieder (S806 bis S808).

[0125] Wie obenstehend beschrieben, ist es dem Abspielgerät **201** möglich, die Häufigkeit zu steuern, mit der das Abspielgerät **201** die Musik wiedergibt, durch ein Vorabspeichern der Anzahl **812** von Ausle-

sevorgängen, die die Häufigkeit zeigt, mit der die Musik wiedergegeben werden kann. Dies ermöglicht der vorliegenden Technik bei einer analogen Reproduzierung von Musik angewendet zu werden, die zum Beispiel durch Miet-CDs oder Kiosk-Endgeräte (Online-Verkaufsmaschinen für Musikverteilung, die mit einem Kommunikationsnetz verbunden sind) erhalten wird.

[0126] Es sollte hier festgehalten werden, dass eine "Auslesezeit" anstelle der Anzahl **812** von Auslesevorgängen gespeichert werden kann, um eine Beschränkung auf die Gesamtzeit, in der der Musikinhalt wiedergegeben werden kann, aufzuzwingen. Alternativ kann stattdessen eine kombinierte Information der Häufigkeit und einer Zeit gespeichert werden. Als ein anderes Beispiel kann die Anzahl **812** von Auslesevorgängen reduziert werden, wenn ein Wiedergeben des Inhalts nach einer gewissen Periode (z. B. 10 Sekunden) beibehalten wird. Als ein anderes Beispiel kann die Anzahl **812** von Auslesevorgängen verschlüsselt und dann gespeichert werden, so dass die Information vor Manipulation geschützt wird.

[0127] Fig. 11 ist ein Flussdiagramm, das den Betrieb zeigt, in dem das Abspielgerät **201** (oder der PC **102**) die Anzahl erlaubter digitaler Ausgaben **913**, die in dem Authentisierungsbereich in der Speicherkarte **109** gespeichert ist, abwickelt. In dem vorliegenden Beispiel kann das Abspielgerät **201** die Musikdaten von dem Nicht-Authentisierungsbereich **331** in der Speicherkarte **109** auslesen und die gelesenen digitalen Musikdaten so oft ausgeben, wie durch die Anzahl von erlaubten digitalen Ausgaben **913**, die in der Speicherkarte **109** gespeichert ist, angezeigt wird (S901).

(1) Das Abspielgerät **201** führt, wie in den in Fig. 9 gezeigten Schritten S701 bis S705, eine Authentisierung mit der Speicherkarte **109** aus, um den Master-Schlüssel **323a** zu extrahieren (S902), extrahiert die Medium-ID **341** (S903), extrahiert den Verschlüsselungsschlüssel **425** (S904) und extrahiert ein Kennwort (S905).

(2) Das Abspielgerät **201** extrahiert dann die Anzahl erlaubter digitaler Ausgaben **913** von dem Authentisierungsbereich **332** in der Speicherkarte **109** und überprüft die Anzahl erlaubter digitaler Ausgaben **913** (S906). Wenn die Anzahl eine Erlaubnis unbeschränkter digitaler Ausgaben anzeigt, liest das Abspielgerät **201** den verschlüsselten Inhalt **426** aus dem Nicht-Authentisierungsbereich **331** aus und entschlüsselt den verschlüsselten Inhalt **426** zu digitalen Daten, unter Verwendung des in Schritt S905 extrahierten Kennworts, und gibt die entschlüsselten digitalen Daten aus dem digitalen Ausgabeanschluss **205** als digitale Musikdaten aus (S909).

(3) Wenn die Anzahl erlaubter digitaler Ausgaben **913** 0 ist, wird entschieden, dass keine digitale Ausgabe erlaubt ist (S908), und die Daten werden nur durch analoge Ausgabe wiedergegeben (S908). Spezifischer ausgedrückt wird der verschlüsselte Inhalt **426** aus dem Nicht-Authentisierungsbereich **331** ausgelesen und Musik wird wiedergegeben, während der Inhalt unter Verwendung des Kennworts entschlüsselt wird (S908).

(4) Wenn die Anzahl erlaubter digitaler Ausgaben **913** ein anderer Wert als 0 ist und nicht eine Erlaubnis unbeschränkter digitaler Ausgaben anzeigt, reduziert das Abspielgerät **201** die Anzahl um 1, schreibt die resultierende Anzahl in den Authentisierungsbereich **332** (S907), liest dann den verschlüsselten Inhalt **426** aus dem Nicht-Authentisierungsbereich **331** aus, entschlüsselt den verschlüsselten Inhalt **426** zu digitalen Daten unter Verwendung des in dem Schritt S905 extrahierten Kennworts, und gibt die entschlüsselten digitalen Daten über den digitalen Ausgabeanschluss **205** aus (S909).

[0128] Wie obenstehend beschrieben kann die Anzahl digitaler Ausgaben von dem Abspielgerät **201** durch ein Speichern der Anzahl erlaubter digitaler Ausgaben **913** in dem Authentisierungsbereich **332** in der Speicherkarte **109** gesteuert werden. Dies ermöglicht der vorliegenden Technik, für eine digitale Reproduzierung von Musik angewendet zu werden, die z. B. durch Miet-CDs oder Kiosk-Endgeräte erhalten wird, was bedeutet, dass ein digitales Überspielen von in einer Speicherkarte gespeicherten Musikdaten unter der Verwaltung des Copyright-Inhabers zu einer gewissen Häufigkeit erlaubt werden kann.

[0129] Hier sollte festgehalten werden, dass so wie mit "der Anzahl von Auslesevorgängen", eine "erlaubte digitale Ausgabezeit" anstelle der Anzahl erlaubter digitaler Ausgaben **913** gespeichert werden kann, um eine Beschränkung auf eine Gesamtzeit aufzuzwingen, in der digitale Daten des Musikinhalts ausgegeben werden können. Alternativ kann stattdessen kombinierte Information der Anzahl erlaubter digitaler Ausgaben und eine Zeit gespeichert werden. Als ein anderes Beispiel kann die Anzahl erlaubter digitaler Ausgaben **913** reduziert werden, wenn ein Ausgeben des Inhalts nach einer gewissen Periode (z. B. 10 Sekunden) beibehalten wird. Als ein anderes Beispiel kann die Anzahl erlaubter digitaler Ausgaben **913** verschlüsselt und dann gespeichert werden, so dass die Information vor Manipulation geschützt ist.

[0130] Eine Funktion kann hinzugefügt werden, so dass die Anzahl erlaubter digitaler Ausgaben durch eine Anzahl vergrößert werden kann, die von dem Copyright-Inhaber in Übereinstimmung mit einer Gebühr spezifiziert wird, die der Copyright-Inhaber empfängt.

[0131] Nun wird die physikalische Datenstruktur (Struktur des Sektors und des ECC-Blocks) der Spei-

cherkarte **109** beschrieben.

[0132] Die Speicherkarte **109** nimmt eine solche Datenstruktur an, die geeignet ist zum Verhindern ungesetzlicher Vorgänge in Bezug auf ein Sichern oder Wiederherstellen der in dem Flash-Speicher **303** gespeicherten Daten und zum Verhindern ungesetzlicher Vorgänge in Bezug auf eine Datenmanipulation. Solch eine Datenstruktur wird angenommen aufgrund der Notwendigkeit, sich mit ungesetzlichen Operationen zu befassen, die auf die oben beschriebenen Verfahren angewendet werden können, in denen "die Anzahl von Auslesevorgängen" oder "die Anzahl erlaubter digitaler Ausgaben" in dem Authentisierungsbereich **332** gespeichert wird und der Wert jedes Mal reduziert wird, wenn der Vorgang ausgeführt wird.

[0133] Spezifischer ausgedrückt kann die Musik wiederholt wiedergegeben werden nachdem die kompletten, in dem Flash-Speicher **303** aufgezeichneten Daten zu einer externen Externspeichervorrichtung oder Ähnlichem abgespeichert wird. Hierdurch kann, wenn die Anzahl erlaubter Wiedergabevorgänge 0 wird, die Musik wiederholt wiedergegeben werden durch ein Wiederherstellen der gesicherten Daten. Ebenso kann die Musik ungesetzlich wiederholt wiedergegeben werden durch ein Manipulieren der Anzahl von Auslesevorgängen. Als ein Ergebnis ist es notwendig, eine Anordnung vorzunehmen, um solch ungesetzliche Vorgänge zu verhindern.

[0134] Fig. 12 zeigt eine Datenstruktur, die der Authentisierungs- und Nicht-Authentisierungsbereich **332** und **331** der Speicherkarte **109** gemeinsam haben und zeigt ebenfalls ein Flussdiagramm des Lese-/Schreibvorgangs entsprechend der Datenstruktur.

[0135] In dem vorliegenden Beispiel wird der von dem Zufallsgenerator **103** der Authentisierungseinheit **321** in dem Steuer-IC **302** erzeugte Zählwert als ein zeitvarianter Schlüssel verwendet.

[0136] Ein 16-Byte Erweiterungsbereich **1005** wird jedem der 512-Byte-Sektoren **1004** in dem Flash-Speicher **303** zugewiesen. Jeder Sektor speichert Daten, die unter Verwendung des Zählwerts verschlüsselt wurden. Der Erweiterungsbereich **1005** besteht aus ECC-Daten **1006** und einem zeitvarianten Bereich **1007**. Die ECC (Fehlerkorrekturcode)-Daten **1006** sind 8-Byte Daten, die ein ECC für die in dem gegenwärtigen Sektor gespeicherten, verschlüsselten Daten sind. Der zeitvariante Bereich **1007** ist 8-Byte und speichert einen Zählwert, der zum Erzeugen der in dem gegenwärtigen Sektor gespeicherten Daten verwendet wird.

[0137] Es sollte hier festgehalten werden, dass nur auf die Sektoren **1004** logisch zugegriffen werden kann (d. h. unter Verwendung eines öffentlichen Befehls oder Ähnlichem) und dass nur auf den Erweiterungsbereich **1005** physikalisch zugegriffen werden kann (d. h. gesteuert durch eine Vorrichtung, die Daten von/zu der Speicherkarte liest/schreibt).

[0138] Mit der obigen Konstruktion kann eine ungesetzliche Datenmanipulation verhindert werden durch Vergleichen der Sektordaten mit den Inhalten des zeitvarianten Bereichs **1007**, wo die Inhalte des zeitvarianten Bereichs **1007** sich nicht ändern, ebenso falls die Sektordaten unter Verwendung eines Befehls oder Ähnlichem manipuliert wurden.

[0139] Spezifischer ausgedrückt schreibt/liest der PC **102** oder das Abspielgerät **201** Daten zu/von dem Authentisierungsbereich **332** oder dem Nicht-Authentisierungsbereich **331** in dem Flash-Speicher **109** gemäß dem unten stehenden, in Einheiten von Sektoren **1004** gezeigten Verfahren. Zuerst wird das Verfahren, in dem der PC **102** Daten zu der Speicherkarte **109** schreibt (S1001) beschrieben werden.

(1) Der PC **102** fordert die Speicherkarte **109** auf, einen Zählerwert auszugeben. In Antwort auf diese Aufforderung erzeugt der Steuer-IC **302** in der Speicherkarte **109** einen Zufallswert unter Verwendung eines Zufallsgenerators **1003**, der in dem Steuer-IC **302** enthalten ist (S1005) und sendet den erzeugten Zufallswert als den Zählerwert zu dem PC **102** (S1002).

(2) Ein Kennwort wird von dem empfangenen Zählerwert und dem Master-Schlüssel **323a** und der Medium-ID **341**, die bereits erhalten wurden, erzeugt (S1003).

(3) Ein Sektor von zu schreibenden Daten wird unter Verwendung eines Kennworts verschlüsselt und zu der Speicherkarte **109** gesendet (S1004). Zusammen mit den verschlüsselten Daten werden (i) Informationen, die den Ort eines Sektors spezifizieren, an den die verschlüsselten Daten zu schreiben sind, und (ii) der für die Verschlüsselung verwendete Zählerwert, zu der Speicherkarte **109** gesendet.

(4) Die Speicherkarte **109** schreibt die verschlüsselten Daten zu dem spezifizierten Sektor **1004** (S1006).

(5) Ein ECC wird durch Berechnung von den verschlüsselten Daten erhalten, und der erhaltene ECC wird zu dem Erweiterungsbereich **1005** als ECC-Daten **1006** geschrieben (S1007).

(6) Der zusammen mit den verschlüsselten Daten empfangene Zählerwert wird zu dem zeitvarianten Bereich **1007** geschrieben (S1008).

[0140] Als nächstes wird das Verfahren, in dem der PC **102** Daten aus der Speicherkarte **109** ausliest (S1011), beschrieben werden.

(1) Der PC **102** fordert die Speicherkarte **109** auf, Daten auszulesen, durch Spezifizieren des Ortes

eines Sektors, von dem die Daten ausgelesen werden sollen. Bei Erhalten der Aufforderung liest die Speicherkarte **109** zuerst verschlüsselte Daten aus dem spezifizierten Sektor **1004** aus und gibt die ausgelesenen Daten an den PC **102** aus (S1016). Der PC **102** empfängt die verschlüsselten Daten (S1012).

(2) Die Speicherkarte **109** liest dann einen Zählerwert aus dem zeitvarianten Bereich **1007** in dem Erweiterungsbereich **1005** aus, der dem spezifizierten Sektor **1004** entspricht, und sendet den ausgelesenen Zählerwert zu dem PC **102** (S1017). Der PC **102** empfängt den Zählerwert (S1013).

(3) Ein Kennwort wird von dem ausgelesenen Zählerwert und dem Master-Schlüssel **323a** und der Medium-ID **341**, die bereits erhalten wurden, erzeugt (S1014).

(4) Die verschlüsselten Daten werden unter Verwendung des Kennworts entschlüsselt (S1005).

[0141] Hier schlägt die Entschlüsselung fehl aufgrund einer Nichtübereinstimmung zwischen dem aus dem zeitvarianten Bereich **1007** ausgelesenen Zählwert, falls die Daten in dem Sektor **1004** durch Manipulation oder Ähnliches geändert wurden.

[0142] Wie obenstehend beschrieben enthält der Flash-Speicher **303** den zeitvarianten Bereich **1007**, einen versteckten Bereich, der nicht von Anwendern gesehen (zugegriffen) werden kann. Daten werden verschlüsselt und gespeichert unter Verwendung eines Kennworts, das unter Verwendung eines in dem zeitvarianten Bereich **1007** gespeicherten Zählwerts erzeugt wird. Mit dieser Konstruktion werden die Daten vor einem ungesetzlichen Manipulieren durch Anwender geschützt.

[0143] In dem obigen Beispiel wird der zeitvariante Bereich **1007** in dem Erweiterungsbereich **1005** zum Speichern der ECC bereit gestellt. Jedoch ist es möglich, den zeitvarianten Bereich **1007** innerhalb eines anderen Bereichs in dem Flash-Speicher **303** bereit zu stellen, unter der Bedingung, dass in dem Bereich gespeicherte Daten nicht von außerhalb der Speicherkarte geändert werden können.

[0144] In dem obigen Beispiel wird eine Zufallszahl als der Zählerwert verwendet. Jedoch kann der Zählerwert ein Taktwert sein, der eine Zeit angibt, die sich in jedem Moment ändert, oder kann die Häufigkeit sein, mit der Daten in den Flash-Speicher **303** geschrieben wurden.

[0145] Nun wird ein wünschenswertes Beispiel einer Beziehung zwischen den logischen Adressen und physikalischen Adressen in dem Flash-Speicher **303** beschrieben werden.

[0146] Die Fig. 13A bis Fig. 13D zeigen eine Änderung in der Beziehung zwischen den logischen Adressen und physikalischen Adressen. Fig. 13A zeigt die Beziehung vor der Änderung. Fig. 13B zeigt die Beziehung nach der Änderung. Fig. 13C zeigt eine Umwandlungstabelle **1101** entsprechend Fig. A. Fig. 13D zeigt die Umwandlungstabelle **1101** entsprechend Fig. B.

[0147] Die Umwandlungstabelle **1101** ist eine Tabelle, in der alle logischen Adressen (in Fig. 13A bis Fig. 13D Seriennummern der logischen Blöcke) mit entsprechenden physikalischen Adressen (in Fig. 13A bis Fig. 13D Seriennummern der physikalischen Blöcke, die den Flash-Speicher **303** bilden) gespeichert werden. Die Umwandlungstabelle **1101** ist in einem nichtflüchtigen Bereich in dem Steuer-IC **302** oder Ähnlichem gespeichert und auf sie wird verwiesen von der Authentisierungsbereich-Zugriffssteuereinheit **325** oder der Nicht-Authentisierungsbereich-Zugriffssteuereinheit **326**, wenn, z. B., eine logische Adresse in eine physikalische Adresse umgewandelt wird.

[0148] Einrichtungen, die auf die Speicherkarte **109** zugreifen, können nicht Daten zu allen Datenspeicherräumen schreiben, die physikalisch in der Speicherkarte **109** existieren (d. h. allen physikalischen Blöcken, die den Flash-Speicher **303** bilden), sondern können Daten lediglich zu logischen Datenräumen (logischen Blöcken) schreiben, die durch die logischen Adressen spezifiziert werden.

[0149] Die obige Anordnung wird aus einem Grund gemacht, und zwar um einen alternativen Bereich abzusichern, der einen Bereich ersetzen würde, von/zu dem Daten aufgrund eines partiellen Fehlers des Flash-Speichers **303** nicht gelesen/geschrieben werden können. Ebenso, falls solch ein Fehlerblock durch einen alternativen Block ersetzt wurde, ermöglicht ein Ändern der Umwandlungstabelle, um die Änderung in Übereinstimmung zwischen den logischen und physikalischen Blocknummern widerzuspiegeln, dem Flash-Speicher **303**, vorzugeben gegenüber externen Einrichtungen, dass keine Fehler bewirkt wurden. Dies ist möglich, da in jeder Datei die logische Kontinuität, die zu einer Mehrzahl von kontinuierlichen physikalischen Blöcken korrespondiert, beibehalten wird.

[0150] Jedoch steigt die Fragmentierung von logischen Blöcken, wenn z. B. eine aus einer Mehrzahl von Blöcken aufgebaute Datei wiederholt in/aus der Speicherkarte **109** gespeichert oder gelöscht wird. Ein spezifisches Beispiel hiervon wird in Fig. 13A gezeigt, in der die logischen Adressen (0 und 2) der logischen Blöcke, die die "Datei 1" bilden, diskontinuierlich sind.

[0151] Wenn eine solche Diskontinuität von logischen Blöcken auftritt, können Musikdaten z. B. nicht

zu kontinuierlichen logischen Bereichen in der Speicherkarte **109** geschrieben werden. Dies benötigt eine Ausgabe des Schreibbefehls "schreibe Adresszahl" für jeden Block, was in einer Reduzierung der Schreibgeschwindigkeit resultiert. Ähnlicherweise benötigt dies die Ausgabe des Lesebefehls "lese Adresszahl" für jeden Block, ebenso falls Musikdaten von einer Abstimmung (Tune) ausgelesen werden sollen, was die Echtzeitwiedergabe der Musikdaten schwierig macht.

[0152] Um das obige Problem zu lösen, hat der Steuer-IC **302** der Speicherkarte **109** eine Funktion, die Umwandlungstabelle **1101** beruhend auf einem von einer externen Einrichtung ausgegebenen Befehl wieder zu schreiben. Spezifischer ausgedrückt, wenn ein dedizierter Befehl zum Wiedereinschreiben der Umwandlungstabelle **1101** von einem Befehlskontakt eingegeben wird, interpretiert der Steuer-IC **302** der Speicherkarte **109** den dedizierten Befehl und schreibt die Umwandlungstabelle **1101** unter Verwendung eines Parameters, der nach dem dedizierten Befehl gesendet wird, wieder ein.

[0153] Die obige Operation wird unter Verwendung eines in den Fig. 13A bis Fig. 13D gezeigten Beispiels detailliert werden. Es wird angenommen, dass bevor der obige dedizierte Befehlt empfangen wird, der Flash-Speicher **303** Daten enthält, die die Datei "Datei 1" an Orten bilden, die durch physikalische Adressen 0 und 2 gekennzeichnet sind, und Daten, die die Datei "Datei 2" an einem Ort bilden, der durch die physikalische Adresse 1 gekennzeichnet ist, wie in Fig. 13A gezeigt, und dass die Umwandlungstabelle **1101** zeigt, dass die logischen Adressen mit den physikalischen Adressen übereinstimmen. Damit soll ausgedrückt werden, dass in den logischen Adressen sowie in den physikalischen Adressen, die Daten von "Datei 2" zwischen den Daten von "Datei 1" angeordnet sind (sandwiched).

[0154] In der Absicht, den obigen Zustand zu lösen, sendet eine externe Einrichtung den obigen dedizierten Befehl und einen Parameter zu dem Flash-Speicher **303**, wobei der dedizierte Befehl anweist, die Kontinuität von "Datei 1" sicherzustellen. Die Befehlsentscheidungs-Steuereinheit **322** der Speicherkarte **109** schreibt die Umwandlungstabelle **1101** wie in Fig. 13D gezeigt wieder ein, in Übereinstimmung mit dem empfangenen dedizierten Befehl und Parameter. Fig. 13B zeigt die Beziehung zwischen den logischen und physikalischen Adressen in dem Flash-Speicher **303**, nach der obigen Sequenz von Operationen.

[0155] Wie von Fig. 13B verstanden wird, wurden die logischen Blöcke, die "Datei 1" bilden, verschoben, um aufeinanderfolgend zu sein, obwohl die Anordnung der physikalischen Blöcke nicht geändert wurde. Mit dieser Anordnung kann die externe Einrichtung auf "Datei 1" mit einer höheren Geschwindigkeit als zuvor beim nächsten Zugriff und später zugreifen.

[0156] Die Umwandlungstabelle **1101** kann wie obenstehend wieder eingeschrieben werden, nicht nur, um die Fragmentierung von logischen Blöcken zu lösen, sondern ebenso, um die Größe sowohl des Authentisierungsbereichs **332** als auch des Nicht-Authentisierungsbereichs **331** in dem Flash-Speicher **303** zu ändern. In dem letzteren Falle ist eine Hochgeschwindigkeitsbereichsverschiebung möglich, da die Umwandlungstabelle **1101** derart wieder eingeschrieben wird, dass ein klein zu werdender physikalischer Block als ein groß zu werdender physikalischer Block angeordnet wird.

[0157] Nun wird eine Funktion der Speicherkarte **109** in Bezug auf nicht-gelöschte Blöcke beschrieben werden. Spezifischer ausgedrückt werden Operationen der Speicherkarte **109** beim Empfangen eines Befehls für eine Liste nicht-gelöschter Blöcke und eines Löschbefehls beschrieben werden. Hierin sind die nicht-gelöschten Blöcke physikalische Blöcke in dem Flash-Speicher **303**, die Daten enthalten, die nicht physikalisch gelöscht wurden. Das heißt, Daten in den nicht-gelöschten Blöcken müssen auf einmal gelöscht werden, bevor die Blöcke ein nächstes Mal benutzt werden (bevor andere Daten in die nicht-gelöschten Blöcke geschrieben werden).

[0158] Der Befehl für eine Liste nicht-gelöschter Blöcke ist einer der Befehle, den die Befehlsentscheidungs-Steuereinheit **322** interpretieren und ausführen kann, und wird verwendet, um eine Liste von allen nicht-gelöschten Blöcken in dem Flash-Speicher **303** zu erhalten.

[0159] Die existierenden, in dem Flash-Speicher **303** der Speicherkarte **109** gespeicherten Daten müssen in Einheiten von Blöcken gelöscht werden, bevor Daten erneut zu dem Flash-Speicher **303** geschrieben werden. Die Zeit für die Löschung ist annähernd die Hälfte der Gesamtzeit des Schreibens. Als ein Ergebnis wird die Gesamtzeit des Schreibens reduziert, falls die Löschung zuvor beendet wurde. Dementsprechend, um dies zu erreichen, stellt die Speicherkarte **109** der externen Einrichtung den Befehl für eine Liste nicht-gelöschter Blöcke und den Löschbefehl bereit.

[0160] Es sei angenommen, dass der gegenwärtige Benutzungszustand der logischen Blöcke und der physikalischen Blöcke des Flash-Speichers **303** in Fig. 14A gezeigt wird. Wie in Fig. 14A gezeigt wird, werden die logischen Blöcke 0 bis 2 gegenwärtig benutzt, und die physikalischen Blöcke 0 bis 2, 4 und 5 sind nicht-gelöschte Blöcke.

[0161] Eine Liste **1203** nicht-gelöschter Blöcke wird

in der Befehlsentscheidungs-Steuereinheit **322** in dem obigen Zustand gespeichert. Die Inhalte der Liste **1203** nicht-gelöschter Blöcke entsprechend dem Benutzungszustand der in Fig. 14A gezeigten Blöcke wird in Fig. 14B gezeigt. Hierin ist die Liste **1203** nicht-gelöschter Blöcke eine Speichertabelle bestehend aus Einträgen, die allen physikalischen Blöcken entsprechen, die den Flash-Speicher **303** bilden, und weist Werte auf, die die Datenlöschzustände (Blöcke, deren Daten gelöscht wurden, werden mit "0" gekennzeichnet, und Blöcke, deren Daten nicht gelöscht wurden, werden mit "1" gekennzeichnet) der entsprechenden physikalischen Blöcke unter der Steuerung der Befehlsentscheidungs-Steuereinheit **322** kennzeichnen.

[0162] Fig. 14C ist ein Flussdiagramm, das das Verfahren des PCs **102** oder des Abspielgeräts **201** zum Löschen von Blöcken im voraus unter Verwendung des Befehls für eine Liste nicht-gelöschter Blöcke und des Löschbefehls in den oben genannten Zuständen zeigt. Es wird hier vorausgesetzt, dass der Flash-Speicher **303** eine Tabelle, wie eine FAT (File Allocation Table) enthält, die die Benutzungszustände der logischen Blöcke zeigt, wie in Fig. 14D zeigt.

[0163] Eine externe Einrichtung, wie der PC **102** oder das Abspielgerät **201**, gibt den Befehl für eine Liste nicht-gelöschter Blöcke an die Speicherkarte **109** während einer Leerlaufzeit aus, in der nicht auf die Speicherkarte **109** zugegriffen wird (S1201). Beim Erhalten des Befehls verweist die Befehlsentscheidungs-Steuereinheit **322** der Speicherkarte **109** auf die Liste **1203** nicht-gelöschter Blöcke, die in der Befehlsentscheidungs-Steuereinheit **322** enthalten ist, erfasst, dass den physikalischen Blöcken 0 bis 2, 4 und 5 ein Zustandswert "1" zugewiesen ist, und sendet die physikalischen Blocknummern zu der externen Einrichtung.

[0164] Die externe Einrichtung verweist dann auf die in Fig. 14D gezeigte Tabelle, die den Benutzungszustand logischer Blöcke in dem Flash-Speicher **303** zeigt, um die Blöcke zu identifizieren, die nicht logisch verwendet werden (S1202).

[0165] Die externe Einrichtung identifiziert, beruhend auf der in den Schritten S1201 und S1202 erhaltenen Information, "löschbare" Blöcke, die nicht logisch verwendet werden und nicht physikalisch gelöscht wurden (physikalische Blöcke 4 und 5 in dem vorliegenden Beispiel) (S1203). Die externe Einrichtung gibt dann den Löschbefehl aus, unter Spezifizierung der physikalischen Blocknummern 4 und 5, zu der Speicherkarte **109** (S1204). Beim Erhalten des Befehls löscht die Befehlsentscheidungs-Steuereinheit **322** der Speicherkarte **109** die physikalischen Blöcke 4 und 5 durch Senden von Anweisungen zu der Authentisierungsbereichs-Zugriffssteuereinheit **325** und der Nicht-Authentisierungsbereichs-Zugriffssteuereinheit **326**.

[0166] Nachdem die obige Operation beendet ist, werden Daten mit einer hohen Geschwindigkeit zu den physikalischen Blöcken 4 und 5 geschrieben, da der Löschvorgang für das Schreiben nicht benötigt wird.

[0167] Nun wird eine Funktion der Speicherkarte **109** beschrieben, die sich auf einen Schutz persönlicher Daten bezieht. Spezifischer ausgedrückt wird die Funktion zum Schutz persönlicher Daten verwendet, wenn die Speicherkarte **109** eine externe Einrichtung auf Authentisierung überprüft und persönliche Daten des Benutzers der externen Einrichtung benötigt. Hier ist jeder Teil der persönlichen Daten für einen Anwender eindeutig und wird verwendet, um den Anwender zu identifizieren. Der Anwender mit geeigneten persönlichen Daten wird von der Speicherkarte **109** als ein autorisierter Benutzer erkannt, dem erlaubt ist, auf den Authentisierungsbereich **332** in der Speicherkarte **109** zuzugreifen.

[0168] Hier kann ein Problem auftreten, dass die persönlichen Daten von irgendjemandem abgezweigt werden oder von einem anderen Anwender, der eine Erlaubnis hat, auf den Authentisierungsbereich **332** zuzugreifen, gelesen werden, falls der Benutzer jedes Mal, wenn der Benutzer auf den Authentisierungsbereich **332** zugreift, aufgefordert wird, die persönlichen Daten einzugeben, oder falls die eingegebenen persönlichen Daten in dem Authentisierungsbereich **332** für jeden derartigen Zugriff gespeichert werden.

[0169] Eine mögliche Lösung dieses Problems wäre eine Verschlüsselung der persönlichen Daten unter Verwendung eines durch den Benutzer persönlich bereit gestellten Kennworts und Speichern der verschlüsselten persönlichen Daten auf dieselbe Art wie die Musikdaten.

[0170] Jedoch muss der Benutzer in dem obigen Fall das Kennwort jedes Mal eingeben, wenn die persönlichen Daten überprüft werden. Der Vorgang ist störanfällig, und die Verwaltung des Kennworts ist ebenso notwendig. Dementsprechend stellt die Speicherkarte **109** eine Funktion bereit, das Problem eines unnötigen und wiederholten Eingebens der persönlichen Daten zu umgehen.

[0171] Fig. 15 zeigt eine Kommunikationssequenz in einer Authentisierung zwischen dem Abspielgerät **201** und der Speicherkarte **109**, und zeigt ebenfalls Hauptkomponenten, die bei der Authentisierung verwendet werden. Es ist festzuhalten, dass die in Fig. 15 gezeigten Vorgänge hauptsächlich erzielt werden durch die Authentisierungsschaltung **216** des Abspielgeräts **201** und die Authentisierungseinheit **321** der Speicherkarte **109**.

[0172] Wie in Fig. 15 gezeigt ist, weist die Authentisierungsschaltung **216** des Abspielgeräts **201** die Verschlüsselungs- und Entschlüsselungsfunktionen auf und speichert einen Master-Schlüssel **1301** vor, der ein geheimer Schlüssel ist, der dem von der Speicherkarte **109** gehaltenen Master-Schlüssel **323a** entspricht, und eine Einrichtungs-ID **1302**, die eine für das Abspielgerät **201** eindeutige ID ist, wie eine Produktseriennummer (S/N).

[0173] Die Authentisierungseinheit **321** der Speicherkarte **109** weist die Verschlüsselungs-Entschlüsselungs- und Vergleichsfunktionen auf und umfasst ebenfalls zwei nichtflüchtige Speicherbereiche: einen Gruppenspeicherbereich **1310** für eine Einrichtungs-ID und einen Speicherbereich **1311** für Benutzerschlüssel. Der Gruppenspeicherbereich **1310** für Einrichtungs-IDs speichert Einrichtungs-IDs aller Einrichtungen, denen erlaubt ist, auf den Authentisierungsbereich **332** in der Speicherkarte **109** zuzugreifen. Der Speicherbereich **1311** für Benutzerschlüssel speichert einen von einer Einrichtung als persönliche Daten gesendeten Benutzerschlüssel.

[0174] Der Authentisierungsvorgang wird untenstehend im Detail erläutert werden. Es ist festzuhalten, dass bei den Übertragungen und Empfängen alle Daten vor Übertragung verschlüsselt werden und die verschlüsselten Daten auf der Empfängerseite entschlüsselt werden. Ein für die Verschlüsselung und Entschlüsselung zu verwendender Schlüssel wird während des folgenden Vorgangs erzeugt.

(1) Nachdem die Speicherkarte **109** mit dem Abspielgerät **201** verbunden ist, verschlüsselt das Abspielgerät **201** zuerst die Einrichtungs-ID **1302** unter Verwendung des Master-Schlüssels **1301** und sendet die verschlüsselte Einrichtungs-ID **1302** zu der Speicherkarte **109**.

(2) Die Speicherkarte **109** entschlüsselt die empfangene, verschlüsselte Einrichtungs-ID **1302** unter Verwendung des Master-Schlüssels **323a** und überprüft, ob die erhaltene Einrichtungs-ID **1302** bereits in dem Gruppenspeicherbereich **1310** für Einrichtungs-IDs gespeichert wurde.

(3) Wenn entschieden wird, dass die Einrichtungs-ID **1302** bereits gespeichert wurde, benachrichtigt die Speicherkarte **109** das Abspielgerät **201**, dass die Authentisierung bejahend war. Wenn entschieden wird, dass die Einrichtungs-ID **1302** nicht gespeichert ist, fordert die Speicherkarte **109** das Abspielgerät **201** auf, einen Benutzerschlüssel zu senden.

(4) Das Abspielgerät **201** verlangt von dem Benutzer, den Benutzerschlüssel einzugeben, erhält den Benutzerschlüssel als persönliche Daten des Benutzers und sendet den erhaltenen Benutzerschlüssel zu der Speicherkarte **109**.

(5) Die Speicherkarte **109** vergleicht den empfangenen Benutzerschlüssel mit dem Benutzerschlüssel, der in dem Speicherbereich **1311** für Benutzerschlüssel vorgespeichert wurde. Wenn entschieden wurde, dass die zwei Benutzerschlüssel übereinstimmen, oder wenn der Speicherbereich **1311** für Benutzerschlüssel leer ist, benachrichtigt die Speicherkarte **109** das Abspielgerät **201**, dass die Authentisierung bejahend war und speichert die Einrichtungs-ID **1302**, die in dem obigen Schritt (3) erhalten wurde, in dem Gruppenspeicherbereich **1310** für Einrichtungs-IDs.

[0175] Mit der obigen Anordnung muss der Benutzer persönliche Daten (einen Benutzerschlüssel) eingeben, wenn eine Einrichtung des Benutzers zum ersten Mal mit der Speicherkarte **109** verbunden wird. In der zweiten Verbindung und danach wird der Benutzer jedoch nicht mehr aufgefordert, die persönlichen Daten einzugeben, da die Authentisierung automatisch bejahend endet unter Verwendung der Einrichtungs-ID.

[0176] Nun wird unter Bezugnahme auf die Fig. 16 und Fig. 17 eine Variation des Authentisierungsprotokolls zwischen der Speicherkarte **109** und einer externen Einrichtung, wie dem PC **102** oder dem Abspielgerät **201**, beschrieben werden.

[0177] Fig. 16 zeigt eine Kommunikationssequenz in einer Variation der Authentisierung zwischen der Speicherkarte **109** und einer externen Einrichtung (in dem vorliegenden Beispielen das Abspielgerät **201**).

[0178] Es ist festzuhalten, dass die in Fig. 16 gezeigten Vorgänge hauptsächlich durch die Authentisierugsschaltung **216** des Abspielgeräts **201**, ein Steuerprogramm **111b** des PCs **102** und die Authentisierungseinheit **321** der Speicherkarte **109** erzielt werden. Es wird hier vorausgesetzt, dass die Master-Schlüssel-Speichereinheit **323** der Speicherkarte **109** einen verschlüsselten Master-Schlüssel (verschlüsselter Master-Schlüssel **323**) speichert, und dass der Spezialbereich **304** eine sichere Medium-ID **343** sowie die Medium-ID **341** speichert, wobei die sichere Medium-ID **343** durch Verschlüsseln der Medium-ID **341** erzeugt wird.

[0179] Zuerst gibt das Abspielgerät **201** einen Befehl zu der Speicherkarte **109** aus, um den Master-Schlüssel **323b** von der Speicherkarte **109** zu erhalten, und entschlüsselt den erhaltenen Master-Schlüssel **323b** unter Verwendung des Einrichtungsschlüssels **211a**. Der in dieser Entschlüsselung verwendete Entschlüsselungsalgorithmus entspricht dem in der Verschlüsselung des Master-Schlüssels **323b**, der nun aus der Speicherkarte **109** ausgelesen wurde, verwendeten Verschlüsselungsalgorithmus. Wenn der Einrichtungsschlüssel **211a**, den das Abspielgerät **201** aufweist, ein autorisierter ist, wird somit erwartet, dass die Entschlüsselung den Original-Master-Schlüssel wiederherstellt.

[0180] Das Abspielgerät **201** gibt dann einen Befehl an die Speicherkarte **109** aus, um die Medium-ID **341** von der Speicherkarte **109** zu erhalten, und verschlüsselt die erhaltene Medium-ID **341** und Verwendung des wiederhergestellten Master-Schlüssels. Der in dieser Verschlüsselung verwendete Verschlüsselungsalgorithmus ist derselbe, wie der in der Verschlüsselung der sicheren Medium-ID **343**, die in der Speicherkarte **109** gespeichert ist, verwendete Verschlüsselungsalgorithmus. Deshalb stellt die Verschlüsselung eine sichere Medium-ID bereit, die dieselbe ist wie die sichere Medium-ID **343**, die in der Speicherkarte **109** enthalten ist.

[0181] Das Abspielgerät **201** und die Speicherkarte **109** führen eine gegenseitige Authentisierung unter Verwendung der sicheren Medium-IDs, die sie jeweils haben, aus. Durch diese gegenseitige Authentisierung erzeugt jede der Einrichtungen (OK/NG) Information und einen sicheren Schlüssel, wobei die (OK/NG) Information anzeigt, ob die Ferneinrichtung authentisiert wurde, und wobei der sichere Schlüssel ein zeitvarianter Schlüssel ist, der von dem Authentisierungsergebnis abhängt. Die sicheren Schlüssel im Besitz der beiden Einrichtungen stimmen nur miteinander überein, wenn beide Einrichtungen **201** und **109** bejahend die anderen Einrichtungen authentisieren, und die sicheren Schlüssel ändern sich jedes Mal, wenn eine gegenseitige Authentisierung ausgeführt wird.

[0182] Nachdem eine gegenseitige Authentisierung bejahend beendet wurde, erzeugt das Abspielgerät **201** einen Befehl, der verwendet wird, um auf den Authentisierungsbereich **332** in der Speicherkarte **109** zuzugreifen. Spezifischer ausgedrückt werden, z. B. wenn Daten aus dem Authentisierungsbereich **332** ausgelesen werden, ein Parameter (eine 24-Bit Adresse "Adresse" und eine 8-Bit Zahl "Zählung") des Befehls "sichere Leseadresszählung" unter Verwendung des sicheren Schlüssels verschlüsselt, und ein verschlüsselter Befehl, der durch Kombinieren des verschlüsselten Parameters und eines Kennzeichners (ein 6-Bit Code, der einen Befehlstyp "sicheres Lesen" kennzeichnet) des Befehls erzeugt wird, wird zu der Speicherkarte **109** gesendet.

[0183] Beim Empfangen des verschlüsselten Befehls entscheidet die Speicherkarte **109** den Befehlstyp. In dem vorliegenden Beispiel wird entschieden, dass der Befehl ein "sicheres Lesen" zum Lesen von Daten aus dem Authentisierungsbereich **332** ist.

[0184] Wenn entschieden wird, dass der Befehl ein Befehl ist, um auf den Authentisierungsbereich **332** zuzugreifen, wird der in dem Befehl enthaltene Parameter unter Verwendung des durch die gegenseitige Authentisierung enthaltenen sicheren Schlüssels entschlüsselt. Der in dieser Entschlüsselung verwendete Entschlüsselungsalgorithmus entspricht dem in der Verschlüsselung des Befehls durch das Abspielgerät **201** verwendeten Verschlüsselungsalgorithmus. Wenn die gegenseitige Authentisierung bejahend endet, d. h., wenn die von beiden Einrichtungen verwendeten sicheren Schlüssel übereinstimmen, sollte der durch die Entschlüsselung erhaltene Parameter somit mit dem von dem Abspielgerät **201** verwendeten Originalparameter übereinstimmen.

[0185] Die Speicherkarte **109** liest dann den Verschlüsselungsschlüssel **425** aus einem Sektor in dem Authentisierungsbereich **332**, der durch den entschlüsselten Parameter gekennzeichnet wird, aus, verschlüsselt den ausgelesenen Verschlüsselungsschlüssel **425** unter Verwendung des sicheren Schlüssels und sendet den verschlüsselten Verschlüsselungsschlüssel zu dem Abspielgerät **201**.

[0186] Das Abspielgerät **201** entschlüsselt die empfangenen Daten unter Verwendung des durch die gegenseitige Authentisierung erhaltenen sicheren Schlüssels. Der bei dieser Entschlüsselung verwendete Entschlüsselungsalgorithmus entspricht dem bei der Verschlüsselung des Verschlüsselungsschlüssels **425** durch die Speicherkarte **109** verwendeten Verschlüsselungsalgorithmus. Wenn die gegenseitige Authentisierung bejahend endet, d. h., wenn die von beiden Einrichtungen verwendeten sichern Schlüssel übereinstimmen, sollten die bei der Entschlüsselung erhaltenen Daten somit mit dem Original-Verschlüsselungsschlüssel **425** übereinstimmen.

[0187] Jedes Mal, wenn ein Befehl zum Zugreifen auf den Authentisierungsbereich **332** ausgeführt wird, verwirft (löscht) die Speicherkarte **109** einen bei der Befehlsausführung verwendeten sicheren Schlüssel. Mit dieser Anordnung muss eine externe Einrichtung, die versucht auf den Authentisierungsbereich **332** in der Speicherkarte **109** zuzugreifen, jedes Mal eine gegenseitige Authentisierung ausführen, wenn die externe Einrichtung einen Befehl ausgibt, und in der Authentisierung zuvor bejahend sein.

[0188] Fig. 17 zeigt eine Kommunikationssequenz in einem detaillierten Verfahren der in Fig. 16 gezeigten gegenseitigen Authentisierung. In dem vorliegenden Beispiel führen die Speicherkarte **109** und das Abspielgerät **201** eine gegenseitige Authentisierung vom Herausforderungs-Antworttyp aus.

[0189] Die Speicherkarte **109** erzeugt eine Zufallszahl und sendet die Zufallszahl als Herausforderungsdaten zu dem Abspielgerät **201**, um die Eignung des Abspielgeräts **201** zu überprüfen. Das Abspielgerät **201** verschlüsselt die Herausforderungsdaten und sendet die verschlüsselten Herausforderungsdaten zu der Speicherkarte **109** als Antwortdaten zurück, um die Eignung des Abspielgeräts **201** zu zertifizieren. Die Speicherkarte **109** verschlüsselt die

als Herausforderungsdaten gesendete Zufallszahl und vergleicht die empfangenen Antwortdaten mit den verschlüsselten Herausforderungsdaten. Wenn die empfangenen Antwortdaten und die verschlüsselten Herausforderungsdaten übereinstimmen, entscheidet die Speicherkarte **109**, dass die Authentisierung des Abspielgeräts **201** bejahend war (OK) und empfängt einen Befehl des Abspielgeräts **201**, um auf den Authentisierungsbereich **332** zuzugreifen. Wenn die empfangenen Antwortdaten und die verschlüsselten Herausforderungsdaten nicht übereinstimmen, entscheidet die Speicherkarte **109**, dass die Authentisierung des Abspielgeräts **201** nicht bejahend war (NG), und falls das Abspielgerät **201** einen Befehl sendet, um nach der Entscheidung auf den Authentisierungsbereich **332** zuzugreifen, weist die Speicherkarte **109** den Befehl zurück.

[0190] Das Abspielgerät **201** führt einen ähnlichen Authentisierungsvorgang aus, um die Eignung der Speicherkarte **109** zu überprüfen. Das heißt, das Abspielgerät **201** erzeugt eine Zufallszahl und sendet die Zufallszahl zu der Speicherkarte **109** als Herausforderungsdaten, um die Eignung der Speicherkarte **109** zu überprüfen. Die Speicherkarte **109** verschlüsselt die Herausforderungsdaten und sendet die verschlüsselten Herausforderungsdaten zu dem Abspielgerät **201** als Antwortdaten zurück, um die Eignung der Speicherkarte **109** zu zertifizieren. Das Abspielgerät **201** verschlüsselt die als Herausforderungsdaten gesendete Zufallszahl und vergleicht die empfangenen Antwortdaten mit den verschlüsselten Herausforderungsdaten. Wenn die empfangenen Antwortdaten und die verschlüsselten Herausforderungsdaten übereinstimmen, entscheidet das Abspielgerät **201**, dass die Authentisierung der Speicherkarte **109** bejahend war (OK) und greift auf den Authentisierungsbereich **332** in der Speicherkarte **109** zu. Wenn die empfangenen Antwortdaten und die verschlüsselten Herausforderungsdaten nicht übereinstimmen, entscheidet das Abspielgerät **201**, dass die Authentisierung der Speicherkarte **109** nicht bejahend war (NG) und gibt ein Zugreifen auf den Authentisierungsbereich **332** auf.

[0191] Alle in der gegenseitigen Authentisierung verwendeten Verschlüsselungsalgorithmen sollten dieselben sein, solange die Speicherkarte **109** und das Abspielgerät **201** autorisiert sind. Die Speicherkarte **109** und das Abspielgerät **201** erhalten einen sicheren Schlüssel durch Ausführen einer Exklusiv-Oder Operation unter Verwendung der verschlüsselten Herausforderungsdaten und der Antwortdaten, die durch die Authentisierung und Zertifizierung der Eignung erhalten wurden. Der erhaltene sichere Schlüssel, oder das Ergebnis der obigen Exklusiv-Oder Operation wird zum Zugreifen auf den Authentisierungsbereich **332** in der Speicherkarte **109** verwendet. Mit dieser Anordnung ist es für beide Einrichtungen **109** und **201** möglich, einen zeitvarianten sicheren Schlüssel gemeinsam zu haben, den beide nur dann gemeinsam haben, wenn sie in der Authentisierung bejahend waren. Dies macht aus der bejahenden Authentisierung eine notwendige Bedingung zum Zugreifen auf den Authentisierungsbereich **332**.

[0192] Der sichere Schlüssel kann ein Ergebnis einer Exklusiv-Oder Operation unter Verwendung der verschlüsselten Herausforderungsdaten, der Antwortdaten und der sicheren Medium-ID sein.

[0193] Nun wird unter Bezugnahme auf die **Fig.** 18 und 19 eine Variation einer Funktion zum Ändern der Begrenzung zwischen dem Authentisierungsbereich **332** und Nicht-Authentisierungsbereich **331** in der Speicherkarte **109** beschrieben werden.

[0194] Die Fig. 18A bis Fig. 18C zeigen den Benutzungszustand des Flash-Speichers **303**, bevor die Begrenzung geändert wird. Fig. 18A ist ein Speicherabbild, das die Konstruktion der physikalischen Blöcke in dem Flash-Speicher **303** zeigt.

[0195] Fig. 18B zeigt eine Umwandlungstabelle **1103**, die für den Nicht-Authentisierungsbereich **331** bestimmt ist und in einem nichtflüchtigen Speicherbereich in der Nicht-Authentisierungsbereich-Zugriffssteuereinheit **326** gespeichert ist. Die Umwandlungstabelle **1103** zeigt Beziehungen zwischen den logischen Blöcken und physikalischen Blöcken in dem Nicht-Authentisierungsbereich **331**. Die Nicht-Authentisierungsbereich-Zugriffssteuereinheit **326** verweist auf die Umwandlungstabelle **1103**, um eine logische Adresse in eine physikalische Adresse umzuwandeln, oder um einen ungeeigneten Zugriff, der auf außerhalb eines zugewiesenen Speicherbereichs zugreift, zu erfassen.

[0196] Fig. 18C zeigt eine Umwandlungstabelle **1102**, die für den Authentisierungsbereich **332** bestimmt ist und in einem nichtflüchtigen Speicherbereich in der Authentisierungsbereich-Zugriffssteuereinheit **325** gespeichert ist. Die Umwandlungstabelle **1102** zeigt Beziehungen zwischen den logischen Blöcken und den physikalischen Blöcken in dem Authentisierungsbereich **332**. Die Authentisierungsbereich-Zugriffssteuereinheit **325** verweist auf die Umwandlungstabelle **1102**, um eine logische Adresse in eine physikalische Adresse umzuwandeln, oder um einen nicht geeigneten Zugriff eines Zugreifens auf außerhalb eines zugewiesenen Speicherbereichs zu erfassen.

[0197] Wie in Fig. 18A gezeigt ist, werden, bevor die Begrenzung geändert wird, aus dem aus den physikalischen Blöcken 0000 bis FFFF bestehenden Flash-Speicher **303** physikalische Blöcke F000 bis FFFF dem veränderbaren Blockbereich **501** zugewiesen, physikalische Blöcke 0000 bis DFFF, deren Adressen niedriger als die Begrenzung sind, werden

dem Nicht-Authentisierungsbereich **331** zugewiesen, und physikalische Blöcke E000 bis EFFF, deren Adressen größer als die Begrenzung sind, werden dem Authentisierungsbereich **332** zugewiesen.

[0198] Wie von der in Fig. 18B gezeigten Umwandlungstabelle **1103** verstanden wird, stimmen die logischen Blocknummern mit den physikalischen Blocknummern in dem Nicht-Authentisierungsbereich **331** überein. Andererseits, wie aus der in Fig. 18C gezeigten Umwandlungstabelle **1102** verstanden wird, gibt es eine inverse Beziehung zwischen den logischen Blocknummern und den physikalischen Blocknummern in dem Authentisierungsbereich **332**. Das heißt, logische Blöcke 0000 bis DFFF entsprechen jeweils physikalischen Blöcken EFFF bis E000. Diese Anordnung wurde gemacht unter Berücksichtigung, dass die logischen Blöcke in aufsteigender Reihenfolge verwendet werden, und dass, wenn die Begrenzung bewegt wird, Daten in den zu bewegenden physikalischen Blöcken gesichert oder bewegt werden müssen.

[0199] Die Fig. 19A bis Fig. 19C zeigen den Benutzungszustand des Flash-Speichers **303**, nachdem die Begrenzung geändert wurde. Die Fig. 19A bis Fig. 19C entsprechen jeweils den Fig. 18A bis Fig. 18C. Es ist festzuhalten, dass die Begrenzungsänderung durch das folgende Verfahren erzielt wird:

(1) Ein dedizierter Befehl, der eine Adresse der Begrenzung spezifiziert, wird über einen Befehlskontakt in die Befehlsentscheidungs-Steuereinheit **322** eingegeben; und

(2) die Befehlsentscheidungs-Steuereinheit **322** schreibt die Umwandlungstabelle **1102** wieder in die Authentisierungsbereich-Zugriffssteuereinheit **325** und die Umwandlungstabelle **1103** in den Nicht-Authentisierungsbereich **331** ein.

[0200] Wie in den Fig. 19A bis Fig. 19C gezeigt wird, wird die Begrenzung von zwischen den physikalischen Blöcken E000 und DFFF bis zwischen die physikalischen Blöcke D000 und CFFF bewegt. Das heißt, dass die Größe des Nicht-Authentisierungsbereichs **331** um 1000 (hex) Blöcke reduziert wird und die Größe des Authentisierungsbereich **332** um 1000 (hex) Blöcke vergrößert wird.

[0201] Wie in Fig. 19B gezeigt wird, wird mit der obigen Begrenzungsänderung die Größe der Umwandlungstabelle **1103** des Nicht-Authentisierungsbereichs **331** um 1000 (hex) Einträge reduziert und die Größe des Authentisierungsbereichs **332** wird um 1000 (hex) Einträge vergrößert, so dass die Umwandlungstabelle **1103** logische Blöcke 0000 bis CFFF mit entsprechenden physikalischen Blöcken 0000 bis CFFF zeigt. Im Gegensatz hierzu, wie in Fig. 19C gezeigt, wird die Größe der Umwandlungstabelle **1102** des Authentisierungsbereichs **332** um 1000 (hex) Einträge vergrößert und die Größe des Authentisierungsbereichs **332** wird um 1000 (hex) Einträge vergrößert, so dass die Umwandlungstabelle **1102** logische Blöcke 0000 bis 1FFF mit entsprechenden physikalischen Blöcken EFFF bis D000 zeigt.

[0202] Wie oben stehend beschrieben wird eine Begrenzung zwischen dem Authentisierungsbereich und dem Nicht-Authentisierungsbereich in dem Flash-Speicher **303** gesetzt, und die Größe beider Bereiche wird durch Bewegen der Begrenzung geändert. Dies ermöglicht der Speicherkarte **109**, für verschiedene Zwecke genutzt zu werden. Zum Beispiel kann die Speicherkarte **109** hauptsächlich genutzt werden zum Speichern digitaler Inhalte, deren Copyright geschützt werden muss, oder die Speicherkarte **109** kann hauptsächlich genutzt werden für anderes als speichern solch digitaler Inhalte.

[0203] Sowohl in dem Authentisierungsbereich als auch dem Nicht-Authentisierungsbereich kann die Verarbeitungsmenge beim Bewegen und Sichern beim Ändern der Begrenzung reduziert werden, dadurch, die logischen Blöcke mit den physikalischen Blöcken übereinstimmend zu machen, so dass physikalische Blöcke in der Reihenfolge der Entfernung beginnend mit dem am weitesten entfernten benutzt werden.

[0204] Die obige Übereinstimmung zwischen den logischen und physikalischen Blöcken wird einfach erricht, wenn die Umwandlungstabelle **1102**, die für den Authentisierungsbereich **332** bestimmt ist und die Umwandlungstabelle **1103**, die für den Nicht-Authentisierungsbereich **331** bestimmt ist, getrennt bereit gestellt werden.

[0205] In dem obigen Beispiel gibt es in dem Authentisierungsbereich **332** eine inverse Beziehung zwischen den logischen Adressen und den physikalischen Adressen in Blockeinheiten. Jedoch können andere Einheiten verwendet werden. Zum Beispiel kann es eine inverse Beziehung zwischen den logischen Adressen und den physikalischen Adressen in Einheiten von Sektoren oder Bytes geben.

[0206] Bis zu diesem Punkt wurde die Speicherkarte der vorliegenden Erfindung in ihrer Ausführungsform und Variationen beschrieben. Die vorliegende Erfindung ist jedoch nicht beschränkt auf die Ausführungsform und die Variationen.

[0207] In der obigen Ausführungsform müssen der PC **102** oder das Abspielgerät **201** eine gegenseitige Authentisierung mit der Speicherkarte **109** durchführen, unter Verwendung desselben Verfahrens jedes Mal, wenn dieser/dieses einen Befehl ausgibt, um auf den Authentisierungsbereich **332** in der Speicherkarte **109** zuzugreifen. Ein vereinfachtes Authentisierungsverfahren kann jedoch verwendet werden, um

auf den Authentisierungsbereich **332** zuzugreifen, in Abhängigkeit von dem Befehlstyp.

[0208] Wenn der Schreibbefehl "sicheres Schreiben" ausgegeben wird, können z. B. der verschlüsselte Master-Schlüssel **323b** und die Medium-ID **341** nicht von der Speicherkarte **109** erhalten werden, sondern die Speicherkarte **109** kann den Schreibbefehl "sicheres Schreiben" ausführen, auch wenn nur eine Einwegauthentisierung (eine Authentisierung einer Einrichtung durch die Speicherkarte **109**) bejahend beendet wird. Mit dieser Anordnung können Befehle, die sich nur wenig auf den Copyright-Schutz beziehen, mit einer hohen Geschwindigkeit ausgeführt werden.

[0209] Der Flash-Speicher **303** in der Speicherkarte **109** der vorliegenden Erfindung kann durch ein anderes Speichermedium (z. B. ein nichtflüchtiges Medium wie eine Festplatte, eine Bildplatte oder eine magneto-optische Platte) ersetzt werden. Eine tragbare Speicherkarte, die geeignet ist zum Sicherstellen eines Copyrights für die gespeicherten Daten, wie die vorliegende Erfindung, kann erzielt werden unter Verwendung irgendeines dieser Medien.

[0210] Die vorliegende Erfindung wurde vollständig beispielhaft beschrieben unter Bezugnahme auf die beiliegenden Zeichnungen. Es ist festzuhalten, dass verschiedene Änderungen und Modifizierungen von dem Fachmann erkannt werden. Solange solche Änderungen und Modifizierungen nicht den Schutzbereich der vorliegenden Erfindung verlassen, sollen diese somit als dann enthalten verstanden werden.

Patentansprüche

1. Halbleiterspeicherkarte (**109**), die in eine elektronische Vorrichtung eingesetzt und aus ihr entnommen werden kann und die umfasst:
einen wieder beschreibbaren, nicht-flüchtigen Speicher (**303**); und
eine Steuerschaltung (**302**), die Zugriffe durch die elektronische Vorrichtung auf einen Authentisierungsbereich (**332**) und einen Nicht-Authentisierungsbereich (**331**) in dem wieder beschreibbaren, nicht-flüchtigen Speicher steuert,
wobei die Steuerschaltung (**302**) enthält:
eine Nicht-Authentisierungsbereichs-Zugriffssteuereinheit (**326**), die Zugriffe von der elektronischen Vorrichtung auf den Nicht-Authentisierungsbereich (**331**) steuert;
eine Authentisierungseinheit (**321**), die einen Authentisierungsprozess durchführt, um zu prüfen, ob die elektronische Vorrichtung berechtigt ist, auf die Halbleiterspeicherkarte (**109**) zuzugreifen, und die elektronische Vorrichtung zustimmend authentisiert, wenn die elektronische Vorrichtung berechtigt ist, auf die Halbleiterspeicherkarte (**109**) zuzugreifen;
eine Authentisierungsbereichs-Zugriffssteuereinheit (**325**), die der elektronischen Vorrichtung Zugriff auf den Authentisierungsbereich (**332**) nur gestattet, wenn die Authentisierungseinheit (**321**) die elektronische Vorrichtung zustimmend authentisiert, wobei
der Authentisierungsbereich (**332**) und der Nicht-Authentisierungsbereich (**331**) durch Trennung eines kontinuierlichen Bereichs vorbestimmter Größe in dem wieder beschreibbaren, nicht-flüchtigen Speicher in zwei Teile erzeugt wird, und
die Halbleiter-Speicherkarte umfasst außerdem:
eine Einrichtung zur Speicherung von Information, die eine Grenze zwischen dem Authentisierungsbereich (**332**) und dem Nicht-Authentisierungsbereich (**331**) angibt; und
eine Bereichsgrößenänderungsschaltung (**322**, **325**, **326**), die die Größe des Authentisierungsbereichs (**332**) und des Nicht-Authentisierungsbereichs (**331**) ändert, wobei die Bereichsgrößenänderungsschaltung die Größe des Authentisierungsbereichs (**332**) und des Nicht-Authentisierungsbereichs (**331**) durch Änderung der Information, die die Grenze angibt ändert, nachdem der gesamte Inhalt des nicht-flüchtigen Speichers gelöscht wurde, und
die Authentisierungs-Bereichs-Zugriffssteuereinheit (**325**) und die Nicht-Authentisierungsbereichs-Zugriffssteuereinheit (**326**) Zugriffe von der elektronischen Vorrichtung auf den Authentisierungsbereich (**332**) und den Nicht-Authentisierungsbereich (**331**) unter Bezugnahme auf die Information, die die Grenze angibt, steuert.

2. Halbleiter-Speicherkarte nach Anspruch 1, wobei die Authentisierungseinheit (**321**) einen Schlüssel erzeugt, der ein Ergebnis des Authentisierungsprozesses reflektiert, und die Authentisierungsbereichszugriff-Steuereinheit (**325**) einen verschlüsselten Befehl unter Verwendung des Schlüssels entschlüsselt, der von der Authentisierungseinheit (**321**) erzeugt wird, und Zugriffe durch die elektronische Vorrichtung auf den Authentisierungsbereich (**332**) entsprechend dem entschlüsselten Befehl steuert, wobei der verschlüsselte Befehl von der elektronischen Vorrichtung gesendet wird.

3. Halbleiter-Speicherkarte nach Anspruch 2, wobei die Authentisierungseinheit (**321**) eine gegenseitige Authentisierung mit der elektronischen Vorrichtung vom Typ mit Authentisierungsabfrage und -antwort ausführt und den Schlüssel aus Abfrage- und Antwortdaten erzeugt, wobei die Abfragedaten zu der elektronischen Vorrichtung gesendet werden, um zu prüfen, ob die elektronische Vorrichtung berechtigt ist, auf die Halbleiter-Speicherkarte zuzugreifen, und die Antwortdaten erzeugt werden, um zu zeigen, dass die Authentisierungseinheit (**321**) berechtigt ist, auf die Halbleiter-Speicherkarte zuzugreifen.

4. Halbleiter-Speicherkarte nach Anspruch 3, wobei der verschlüsselte Befehl, der von der elektronischen Vorrichtung gesendet wird, ein Etikettenfeld

und ein Adressfeld enthält, wobei das Etikettenfeld nicht verschlüsselt worden ist und einen Typ eines Zugriffs auf den Authentisierungsbereich (**332**) angibt, wobei das Adressfeld verschlüsselt worden ist und eine Adresse eines Bereiches, auf den zuzugreifen ist, angibt, wobei die Authentisierungsbereichszugriff-Steuereinheit (**325**) das Adressfeld unter Verwendung des Schlüssels verschlüsselt und Zugriffe auf den Authentisierungsbereich (**332**) durch die elektronische Vorrichtung so steuert, dass ein Zugriff des Typs, der in dem Etikettenfeld angegeben ist, auf den Bereich erfolgt, der durch die Adresse in dem verschlüsselten Adressfeld angezeigt wird.

5. Halbleiter-Speicherkarte nach Anspruch 4, die des Weiteren umfasst:
eine Kennungsdaten-Speicherschaltung (**304**), die Kennungsdaten (**341**) vorspeichert, die der Halbleiter-Speicherkarte eindeutig zugeordnet sind, und es ermöglichen, die Halbleiter-Speicherkarte von anderen Halbleiter-Speicherkarten zu unterscheiden, wobei
die Authentisierungseinheit (**321**) eine gegenseitige Authentisierung mit der elektronischen Vorrichtung unter Verwendung der Kennungsdaten (**341**) ausführt, die in der Kennungsdaten-Speicherschaltung (**304**) gespeichert sind, und den Schlüssel aus den Kennungsdaten (**341**) erzeugt.

6. Halbleiter-Speicherkarte nach Anspruch 1, wobei die Bereichsgrößenänderungsschaltung (**322**, **325**, **326**) enthält:
eine Authentisierungsbereich-Umwandlungstabelle (**1102**), die Entsprechung zwischen logischen Adressen und physikalischen Adressen in dem Authentisierungsbereich (**332**) zeigt,
eine Nicht-Authentisierungsbereich-Umwandlungstabelle (**1103**), die Entsprechung zwischen logischen Adressen und physikalischen Adressen in dem Nicht-Authentisierungsbereich (**331**) zeigt, und
eine Umwandlungstabellen-Änderungseinheit (**322**), die Inhalte der Authentisierungsbereich-Umwandlungstabelle (**1102**) und der Nicht-Authentisierungsbereich-Umwandlungstabelle (**1103**) entsprechend einem Befehl von der elektronischen Vorrichtung ändert, wobei
die Authentisierungsbereichszugriff-Steuereinheit (**325**) Zugriffe durch die elektronische Vorrichtung auf den Authentisierungsbereich (**332**) steuert, indem sie auf die Authentisierungsbereich-Umwandlungstabelle (**1102**) Bezug nimmt, und
die Nicht-Authentisierungsbereichszugriff-Steuereinheit (**326**) Zugriffe durch die elektronische Vorrichtung auf den Nicht-Authentisierungsbereich (**331**) steuert, indem sie auf die Nicht-Authentisierungsbereich-Umwandlungstabelle (**1103**) Bezug nimmt.

7. Halbleiter-Speicherkarte nach Anspruch 6, wobei ein Bereich, der mit höheren physikalischen Adressen adressiert ist, und ein Bereich, der mit niedrigeren physikalischen Adressen adressiert ist, die beide den Bereich mit der vorgegebenen Größe bilden, dem Authentisierungsbereich (**332**) bzw. dem Nicht-Authentisierungsbereich (**331**) zugeordnet werden,
die Nicht-Authentisierungsbereich-Umwandlungstabelle (**1103**) Entsprechung zwischen logischen Adressen, die in aufsteigender Reihenfolge angeordnet sind, und
die Authentisierungsbereich-Umwandlungstabelle (**1102**) Entsprechung zwischen logischen Adressen, die in aufsteigender Reihenfolge angeordnet sind, und physikalischen Adressen, die in absteigender Reihenfolge angeordnet sind, zeigt.

8. Halbleiter-Speicherkarte nach Anspruch 1, die des Weiteren eine Festwertspeicherschaltung umfasst, die Daten vorspeichert.

9. Halbleiter-Speicherkarte nach Anspruch 1, wobei die Steuerschaltung (**302**) des Weiteren enthält:
eine Umwandlungstabelle (**1102**, **1103**), die Entsprechung zwischen logischen Adressen und physikalischen Adressen in dem Authentisierungsbereich (**332**) und dem Nicht-Authentisierungsbereich (**331**) zeigt, und
eine Umwandlungstabellen-Änderungseinheit (**322**), die Inhalte der Umwandlungstabelle entsprechend einem Befehl von der elektronischen Vorrichtung ändert, und
wobei die Authentisierungsbereichszugriff-Steuereinheit (**325**) und die Nicht-Authentisierungsbereichszugriff-Steuereinheit (**326**) Zugriffe durch die elektronische Vorrichtung auf den Authentisierungsbereich (**332**) bzw. den Nicht-Authentisierungsbereich (**331**) steuern, indem sie auf die Umwandlungstabelle Bezug nehmen.

10. Halbleiter-Speicherkarte nach Anspruch 1, wobei die Steuerschaltung (**302**) des Weiteren enthält:
eine Verschlüsselungs-/Entschlüsselungs-Einheit (**327**), die Daten verschlüsselt, die in den Authentisierungsbereich (**332**) und den Nicht-Authentisierungsbereich (**331**) zu schreiben sind, und Daten entschlüsselt, die aus dem Authentisierungsbereich (**332**) und dem Nicht-Authentisierungsbereich (**331**) ausgelesen werden.

11. Halbleiter-Speicherkarte nach Anspruch 1, wobei der nichtflüchtige Speicher (**303**) ein Flash-Speicher ist, und die Steuerschaltung (**302**) des Weiteren enthält:
eine Nicht-Gelöscht-Listen-Aufnahmeeinheit (**322**), die eine Nicht-Gelöscht-Liste aufnimmt, die eine Liste nicht gelöschter Bereiche in dem Authentisierungsbereich (**332**) und dem Nicht-Authentisierungsbereichsbereich (**331**) zeigt, und
eine Nicht-Gelöscht-Bereich-Sendeeinheit (**322**), die entsprechend einem Befehl von der elektronischen

Vorrichtung auf die Nicht-Gelöscht-Liste Bezug nimmt, um nicht gelöschte Bereiche in dem Authentisierungsbereich (**332**) und dem Nicht-Authentisierungsbereich (**331**) zu identifizieren, und Informationen, die die identifizierten, nicht gelöschten Bereiche anzeigen, zu der elektronischen Vorrichtung sendet.

12. Halbleiter-Speicherkarte nach Anspruch 1, wobei die Authentisierungseinheit (**321**) einen Benutzer der elektronischen Vorrichtung während des Authentisierungsprozesses auffordert, einen Benutzerschlüssel einzugeben, bei dem es sich um eine Information handelt, die dem Benutzer eindeutig zugeordnet ist, und die Steuerschaltung (**302**) des Weiteren enthält:
eine Benutzerschlüssel-Speichereinheit (**1311**), die den Benutzerschlüssel speichert,
eine Kennungsinformations-Speichereinheit (**1310**), die eine einzelne Kennungsinformation speichert, die eine elektronische Vorrichtung identifiziert, die von der Authentisierungseinheit (**321**) zustimmend authentisiert worden ist, und
eine Benutzerschlüsselaufforderungs-Verbotseinheit (**321**), die eine einzelne Kennungsinformation von einer elektronischen Zielvorrichtung bezieht, nachdem die Authentisierungseinheit (**321**) mit dem Authentisierungsprozess begonnen hat, prüft, ob die von der elektronischen Zielvorrichtung bezogene einzelne Kennungsinformation bereits in der Kennungsinformations-Speichereinheit gespeichert worden ist, und der Authentisierungseinheit (**321**) verbietet, einen Benutzer der elektronischen Vorrichtung zur Eingabe eines Benutzerschlüssels aufzufordern, wenn die von der elektronischen Zielvorrichtung bezogene einzelne Kennungsinformation bereits in der Kennungsinformations-Speichereinheit gespeichert worden ist.

13. Speichersystem, das eine Halbleiter-Speicherkarte nach Anspruch 1 so wie eine Datenlesevorrichtung (**201**) enthält, die einen digitalen Inhalt (**426**) aus der Halbleiter-Speicherkarte ausliest, wobei der digitale Inhalt in dem Nicht-Authentsierungsbereich (**331**) der Halbleiter-Speicherkarte gespeichert worden ist, und Information (**812**), die anzeigt, wie oft der digitale Inhalt ausgelesen werden kann, und die in dem Authentisierungsbereich (**332**) vorgespeichert ist, ausgelesen werden kann, wobei die Datenlesevorrichtung umfasst:
eine Entscheidungseinrichtung (S804), die, wenn der digitale Inhalt aus dem Nicht-Authentisierungsbereich (**331**) auszulesen ist, die Information, die anzeigt, wie oft der digitale Inhalt ausgelesen werden kann, aus dem Authentisierungsbereich (**332**) ausliest und auf der Grundlage der Häufigkeit, die in der Information angezeigt ist, entscheidet, ob der digitale Inhalt ausgelesen werden kann, und
eine Wiedergabeeinrichtung (S806–S808), die den digitalen Inhalt aus dem Nicht-Authentisierungsbereich (**331**) nur dann ausliest, wenn die Entscheidungseinrichtung entscheidet, dass der digitale Inhalt ausgelesen werden kann, und die Häufigkeit, mit der der digitale Inhalt ausgelesen werden kann, in der in dem Authentisierungsbereich (**332**) gespeicherten Information verringert.

14. Speichersystem, das eine Halbleiter-Speicherkarte nach Anspruch 1 und eine Lesevorrichtung (**201**) enthält, die einen digitalen Inhalt (**426**) der Halbleiter-Speicherkarte ausliest und den digitalen Inhalt als ein analoges Signal wiedergibt, wobei der digitale Inhalt in dem Nicht-Authentisierungsbereich (**331**) der Halbleiter-Speicherkarte (**109**) gespeichert worden ist, und Information (**913**), die anzeigt, wie oft der digitale Inhalt von der elektronischen Vorrichtung digital ausgegeben werden kann, in dem Authentisierungsbereich (**332**) gespeichert worden ist, wobei die Datenlesevorrichtung umfasst:
eine Wiedergabeeinrichtung (S908), die den digitalen Inhalt aus dem Nicht-Authentisierungsbereich (**331**) ausliest und den ausgelesenen digitalen Inhalt als ein analoges Signal wiedergibt,
eine Entscheidungseinrichtung (S906), die die Information, die anzeigt, wie oft der digitale Inhalt von der elektronischen Vorrichtung digital ausgegeben werden kann, ausliest und auf der Grundlage der Häufigkeit, die in der Information angezeigt ist, entscheidet, ob der digitale Inhalt digital ausgegeben werden kann, und
eine Digitalausgabeeinrichtung (S907, S909), die den digitalen Inhalt nur dann digital ausgibt, wenn die Entscheidungseinrichtung entscheidet, dass der digitale Inhalt digital ausgegeben werden kann, und die Häufigkeit, mit der der digitale Inhalt digital ausgegeben werden kann, in der in dem Authentisierungsbereich (**332**) gespeicherten Information verringert.

15. Steuerverfahren zur Verwendung in einer Halbleiter-Speicherkarte (**109**), die in eine elektronische Vorrichtung eingesetzt und aus ihr entnommen werden kann, wobei die Halbleiter-Speicherkarte (**109**) einen wieder beschreibbaren, nicht-flüchtigen Speicher (**303**) und eine Steuerschaltung enthält, wobei der nicht-flüchtige Speicher (**303**) einen Authentisierungsbereich (**332**) und einen Nicht-Authentisierungsbereich (**331**) enthält, wobei der Authentisierungsbereich (**332**) und der Nicht-Authentisierungsbereich (**331**) durch Unterteilung eines kontinuierlichen Bereichs vorbestimmter Größe in dem wieder beschreibbaren, nicht-flüchtigen Speicher in zwei Teile erzeugt wird und Information über eine Grenze zwischen dem Authentisierungsbereich (**332**) und dem Nicht-Authentisierungsbereich (**331**) in dem nicht-flüchtigen Speicher gespeichert ist, wobei das Steuerverfahren umfasst:
einen Nicht-Authentisierungsbereichs-Zugriffs-Steuerschritt, der Zugriffe von der elektronischen Vorrichtung auf den Nicht-Authentisierungsbereich (**331**) steuert,
einen Authentisierungsschritt, der einen Authentisierungsprozess ausführt, um zu prüfen, ob die elektro-

nische Vorrichtung berechtigt ist, auf die Halbleiter-Speicherkarte (**109**) zuzugreifen, und die elektronische Vorrichtung zustimmend authentisiert, wenn die elektronische Vorrichtung berechtigt ist, auf die Halbleiterspeicherkarte (**109**) zuzugreifen;

wobei der Nicht-Authentisierungsbereichs-Zugriffs-Steuerschritt auf die Information Bezug nimmt, die die Grenze angibt, und der Authentisierungsbereichs-Zugriffssteuerschritt auf die Information Bezug nimmt, die die Grenze angibt,

einen Authentisierungsbereichs-Zugriffssteuerschritt, der der elektronischen Vorrichtung Zugriff auf den Authentisierungsbereich (**332**) nur gestattet, wenn der Authentisierungsschritt die elektronische Vorrichtung zustimmend authentisiert, und

einen Bereichsgrößenänderungsschritt, der die Größe des Authentisierungsbereichs (**332**) und den Nicht-Authentisierungsbereichs (**331**) durch Änderung der Information, die die Grenze angibt, verändert, nachdem der gesamte Inhalt des nicht-flüchtigen Speichers gelöscht ist.

Es folgen 19 Blatt Zeichnungen

Anhängende Zeichnungen

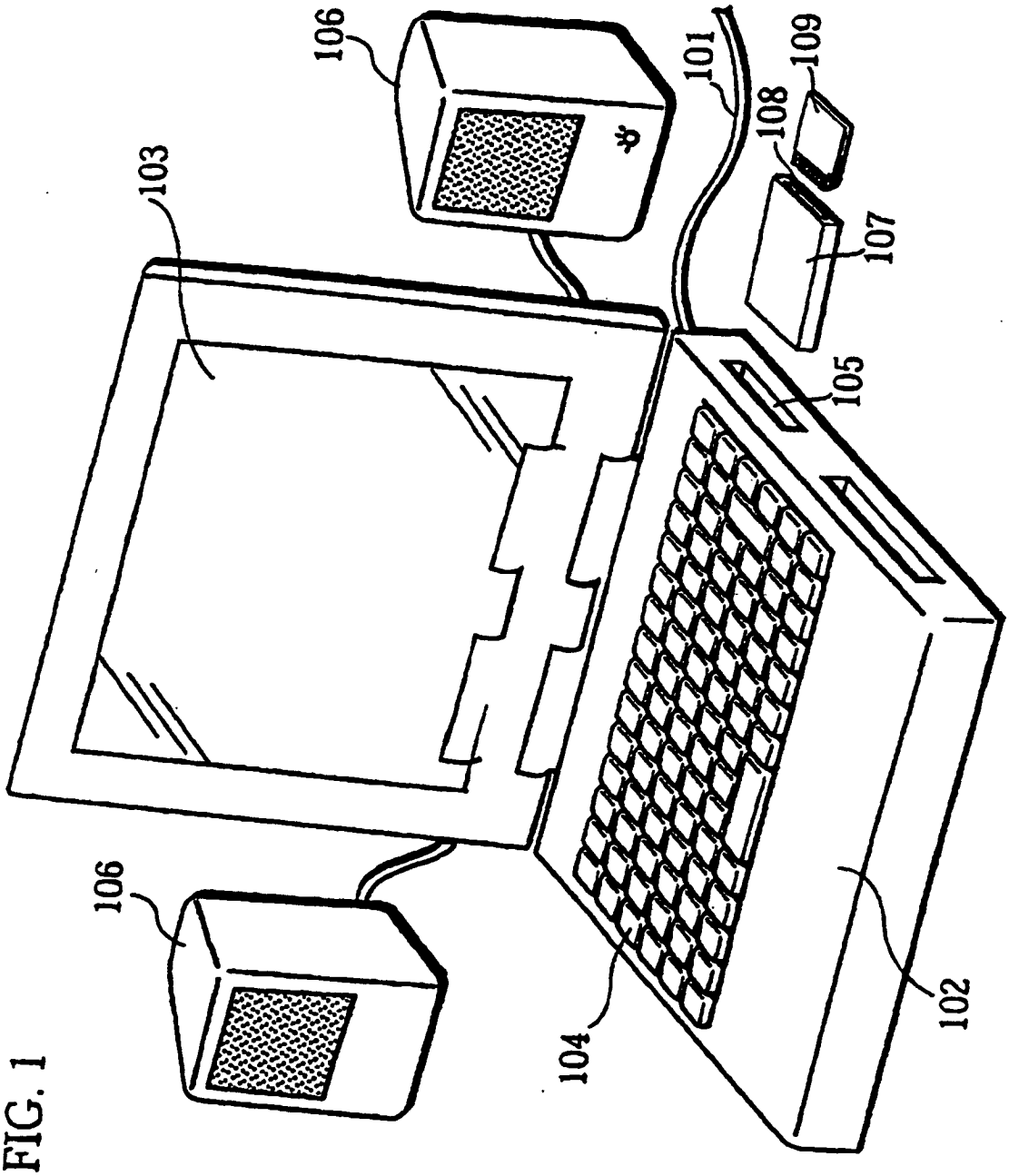


FIG. 1

FIG. 2

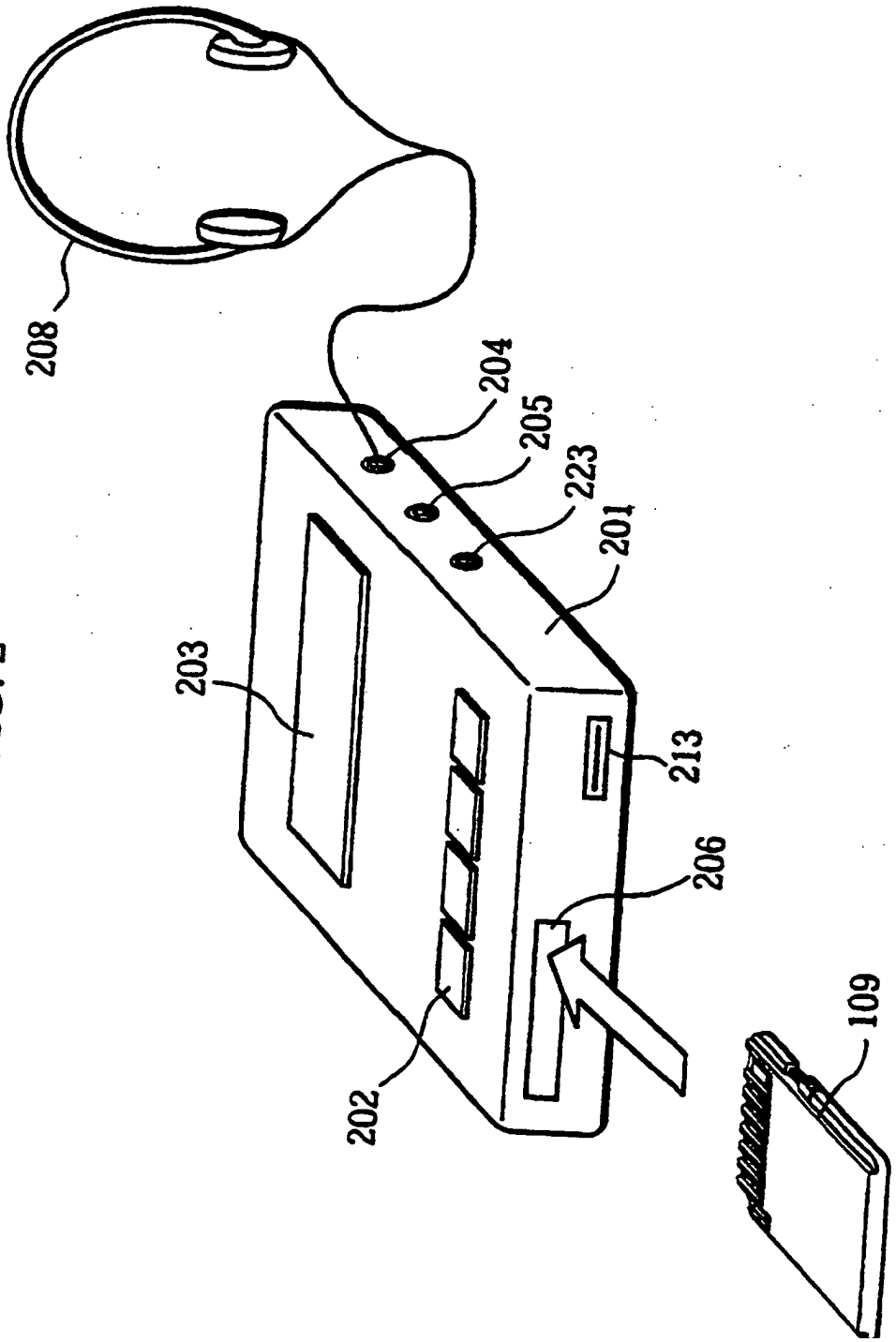


FIG. 3

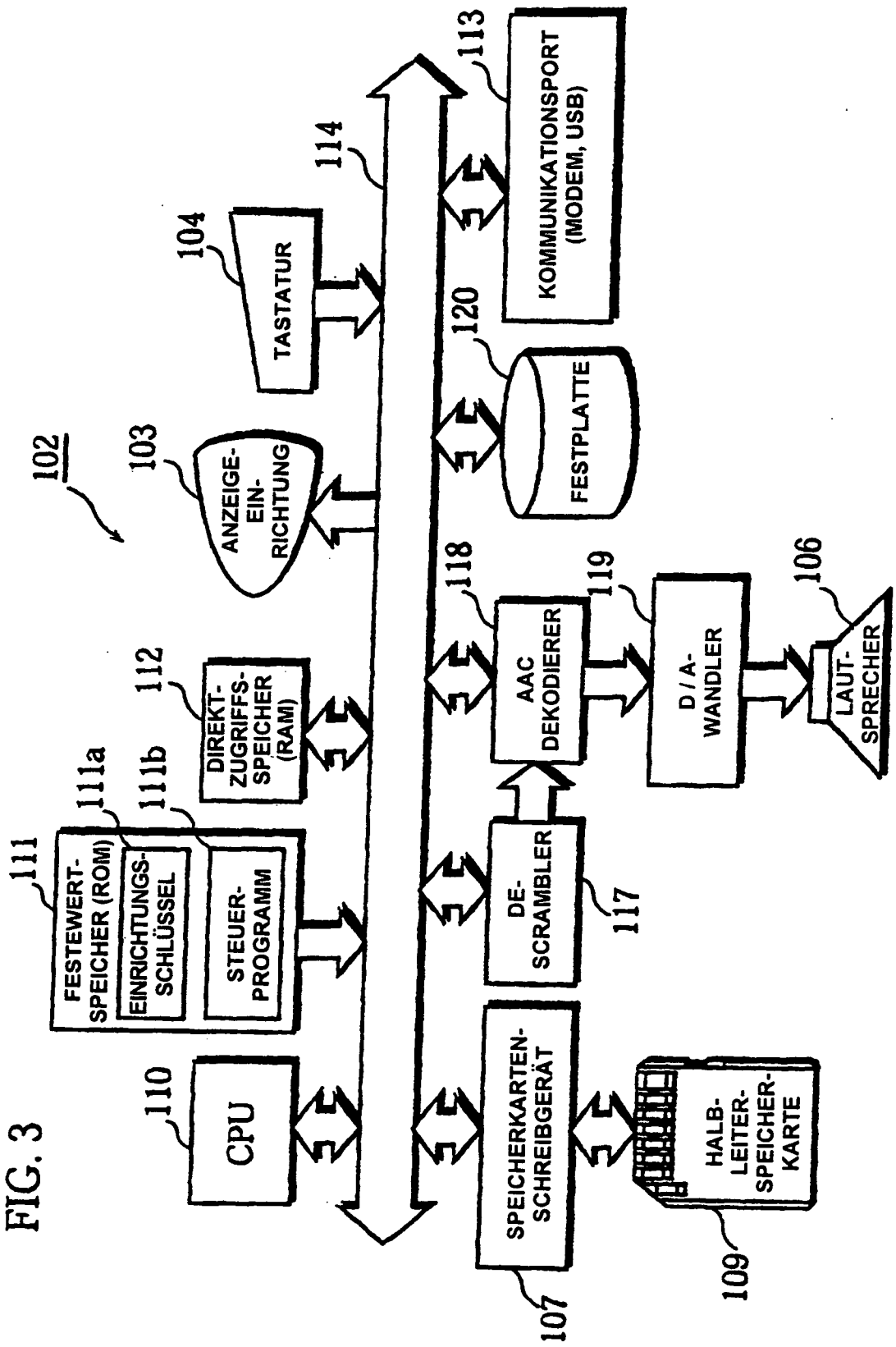

102
CPU
110
FESTEWERT-SPEICHER (ROM)
111
EINRICHTUNGS-SCHLÜSSEL
111a
STEUER-PROGRAMM
111b
DIREKT-ZUGRIFFS-SPEICHER (RAM)
112
ANZEIGE-EIN-RICHTUNG
103
TASTATUR
104
114
KOMMUNIKATIONSPORT (MODEM, USB)
113
FESTPLATTE
120
AAC DEKODIERER
118
D/A-WANDLER
119
LAUT-SPRECHER
106
DE-SCRAMBLER
117
SPEICHERKARTEN-SCHREIBGERÄT
107
HALB-LEITER-SPEICHER-KARTE
109

FIG. 4

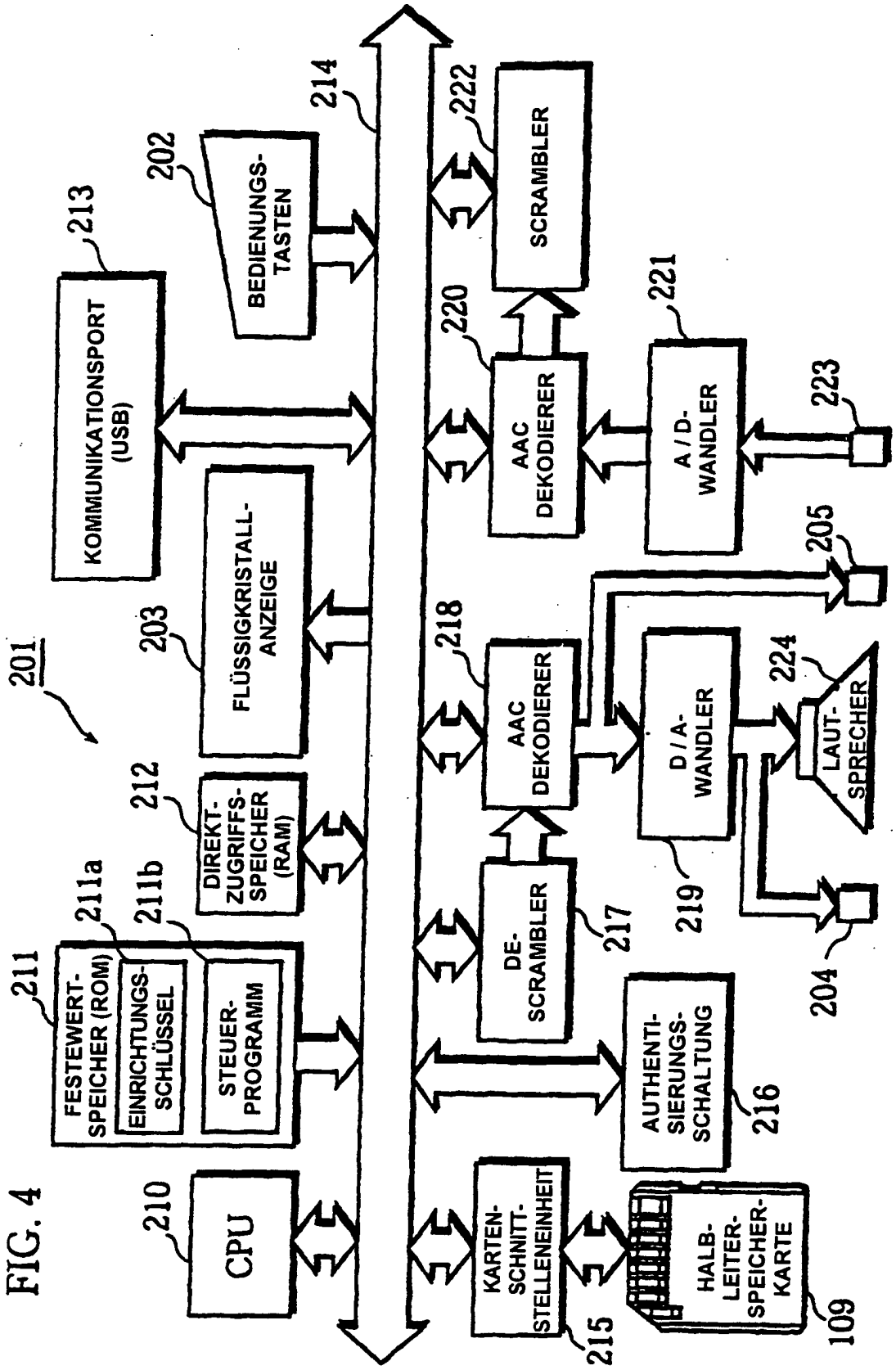

201
210
CPU
211
FESTEWERT-SPEICHER (ROM)
211a
EINRICHTUNGS-SCHLÜSSEL
211b
STEUER-PROGRAMM
212
DIREKT-ZUGRIFFS-SPEICHER (RAM)
213
KOMMUNIKATIONSPORT (USB)
202
BEDIENUNGS-TASTEN
203
FLÜSSIGKRISTALL-ANZEIGE
214
215
KARTEN-SCHNITT-STELLENEINHEIT
109
HALB-LEITER-SPEICHER-KARTE
216
AUTHENTI-SIERUNGS-SCHALTUNG
217
DE-SCRAMBLER
218
AAC DEKODIERER
219
D/A-WANDLER
204
205
220
AAC DEKODIERER
221
A/D-WANDLER
223
222
SCRAMBLER
224
LAUT-SPRECHER

FIG. 5

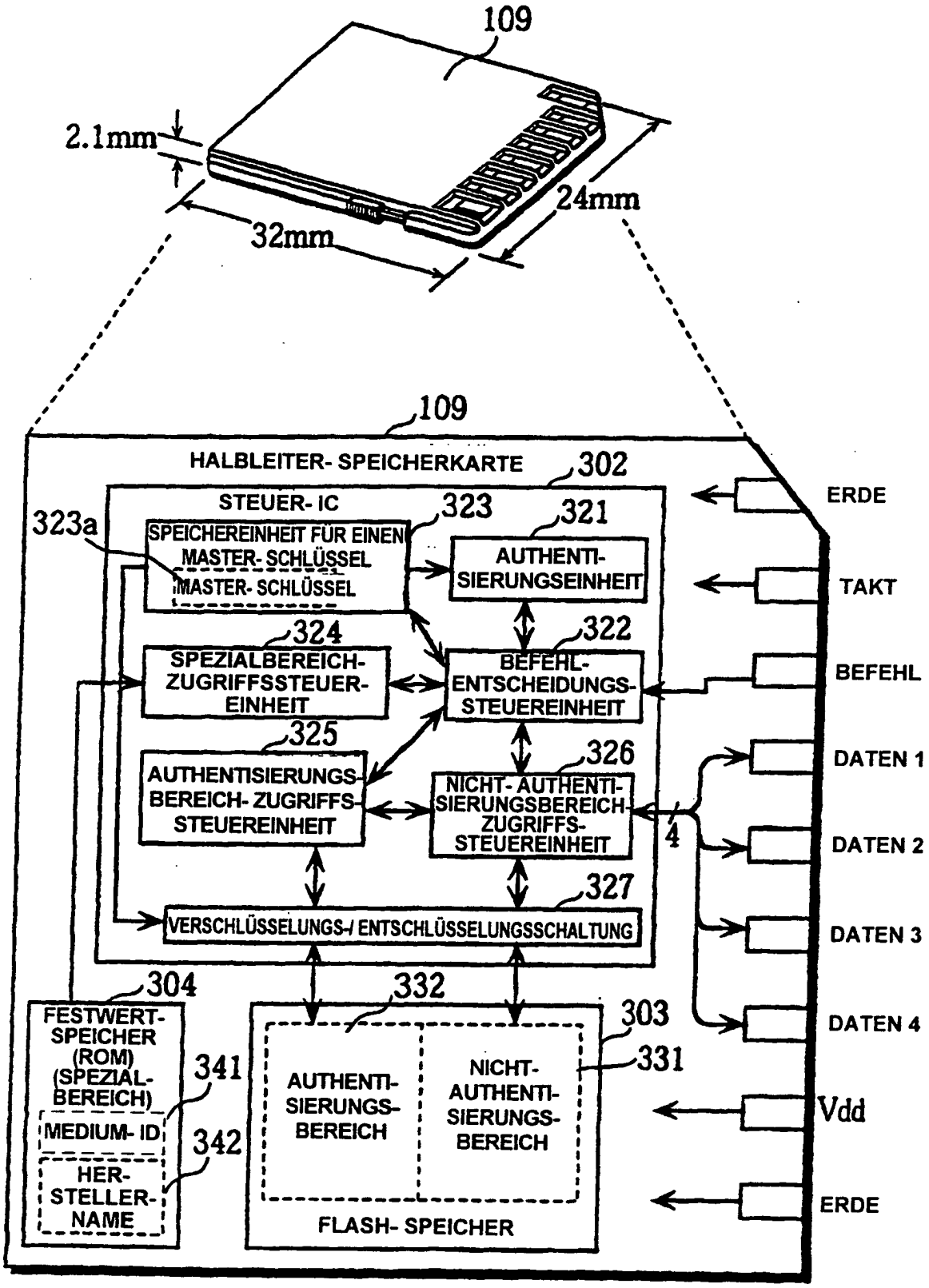
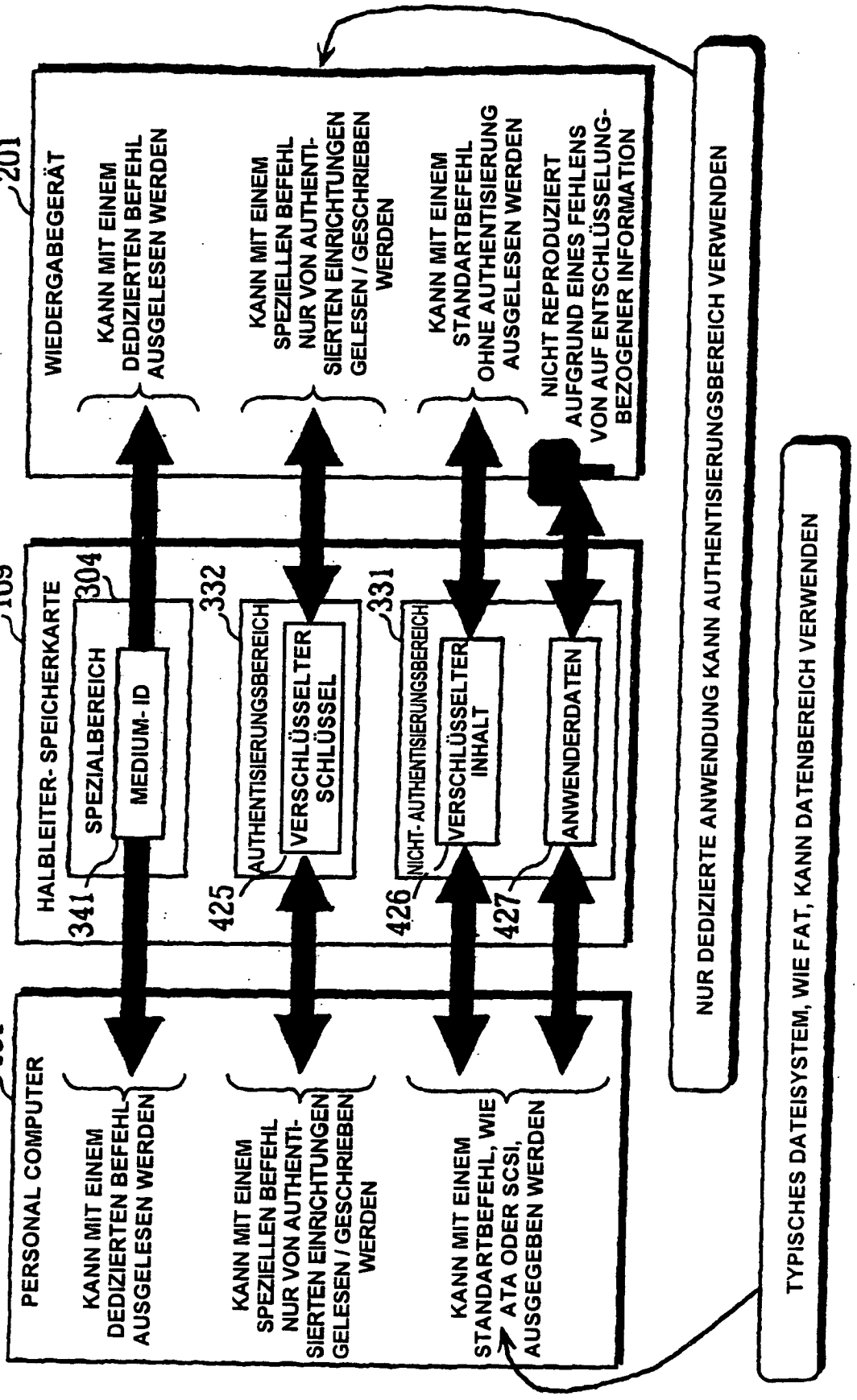

109
2.1mm
32mm
24mm
109
HALBLEITER- SPEICHERKARTE
302
STEUER- IC
323
321
323a
SPEICHEREINHEIT FÜR EINEN MASTER- SCHLÜSSEL
MASTER- SCHLÜSSEL
AUTHENTI- SIERUNGSEINHEIT
324
322
SPEZIALBEREICH- ZUGRIFFSSTEUER- EINHEIT
BEFEHL- ENTSCHEIDUNGS- STEUEREINHEIT
325
326
AUTHENTISIERUNGS- BEREICH- ZUGRIFFS- STEUEREINHEIT
NICHT- AUTHENTI- SIERUNGSBEREICH- ZUGRIFFS- STEUEREINHEIT
4
327
VERSCHLÜSSELUNGS-/ ENTSCHLÜSSELUNGSSCHALTUNG
304
332
303
FESTWERT- SPEICHER (ROM) (SPEZIAL- BEREICH)
341
MEDIUM- ID
342
HER- STELLER- NAME
AUTHENTI- SIERUNGS- BEREICH
NICHT- AUTHENTI- SIERUNGS- BEREICH
331
FLASH- SPEICHER
ERDE
TAKT
BEFEHL
DATEN 1
DATEN 2
DATEN 3
DATEN 4
Vdd
ERDE

FIG. 6


101
PERSONAL COMPUTER
KANN MIT EINEM DEDIZIERTEN BEFEHL AUSGELESEN WERDEN
KANN MIT EINEM SPEZIELLEN BEFEHL NUR VON AUTHENTI-SIERTEN EINRICHTUNGEN GELESEN / GESCHRIEBEN WERDEN
KANN MIT EINEM STANDARTBEFEHL, WIE ATA ODER SCSI, AUSGEGEBEN WERDEN
109
HALBLEITER- SPEICHERKARTE
304
SPEZIALBEREICH
MEDIUM- ID
341
332
AUTHENTISIERUNGSBEREICH
VERSCHLÜSSELTER SCHLÜSSEL
425
331
NICHT- AUTHENTISIERUNGSBEREICH
VERSCHLÜSSELTER INHALT
426
ANWENDERDATEN
427
201
WIEDERGABEGERÄT
KANN MIT EINEM DEDIZIERTEN BEFEHL AUSGELESEN WERDEN
KANN MIT EINEM SPEZIELLEN BEFEHL NUR VON AUTHENTI-SIERTEN EINRICHTUNGEN GELESEN / GESCHRIEBEN WERDEN
KANN MIT EINEM STANDARTBEFEHL OHNE AUTHENTISIERUNG AUSGELESEN WERDEN
NICHT REPRODUZIERT AUFGRUND EINES FEHLENS VON AUF ENTSCHLÜSSELUNG-BEZOGENER INFORMATION
NUR DEDIZIERTE ANWENDUNG KANN AUTHENTISIERUNGSBEREICH VERWENDEN
TYPISCHES DATEISYSTEM, WIE FAT, KANN DATENBEREICH VERWENDEN

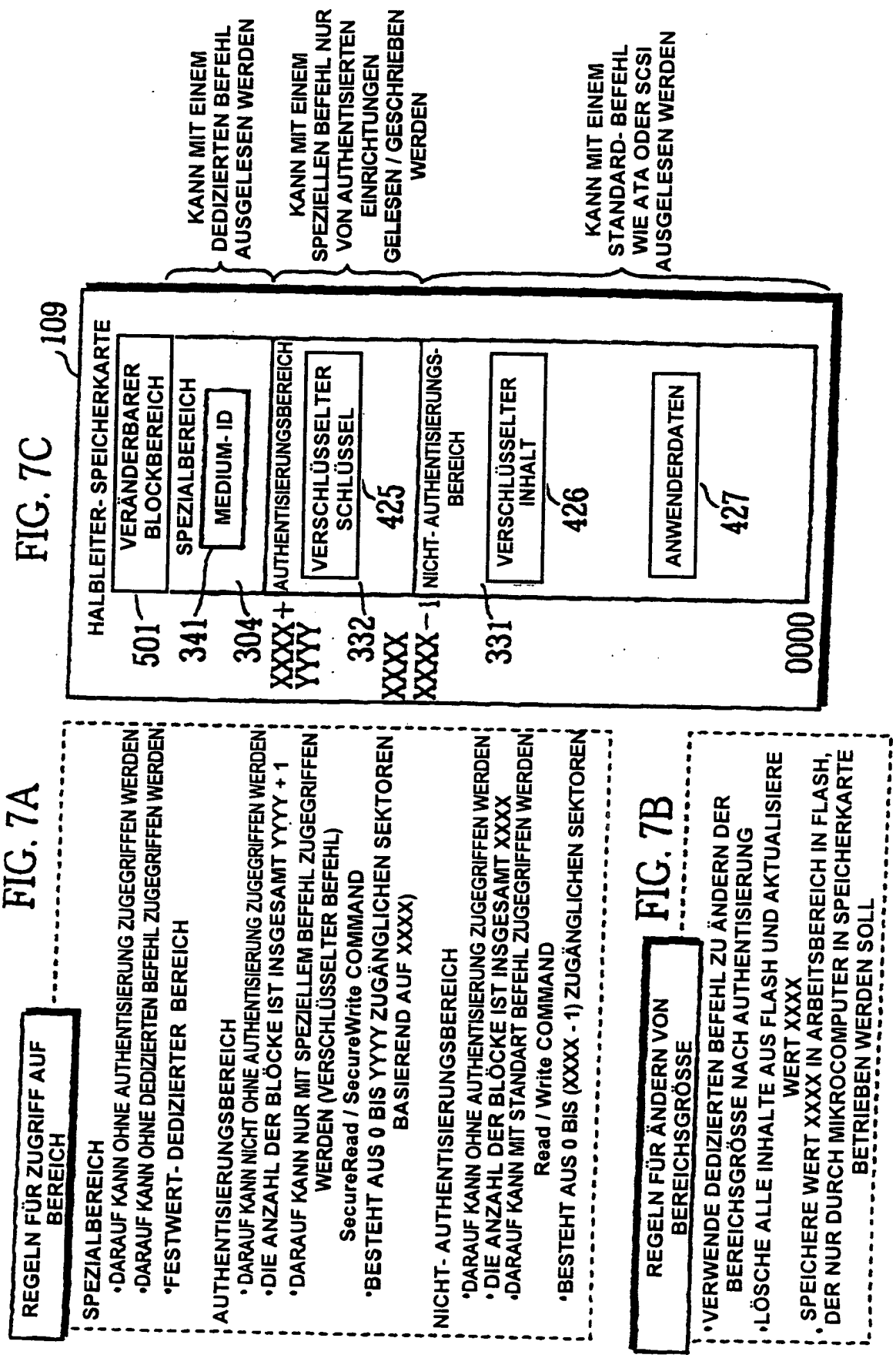


FIG. 7A
REGELN FÜR ZUGRIFF AUF BEREICH
SPEZIALBEREICH
•DARAUF KANN OHNE AUTHENTISIERUNG ZUGEGRIFFEN WERDEN
•DARAUF KANN OHNE DEDIZIERTEN BEFEHL ZUGEGRIFFEN WERDEN
•FESTWERT- DEDIZIERTER BEREICH
AUTHENTISIERUNGSBEREICH
•DARAUF KANN NICHT OHNE AUTHENTISIERUNG ZUGEGRIFFEN WERDEN
•DIE ANZAHL DER BLÖCKE IST INSGESAMT YYYY + 1
•DARAUF KANN NUR MIT SPEZIELLEM BEFEHL ZUGEGRIFFEN WERDEN (VERSCHLÜSSELTER BEFEHL)
SecureRead / SecureWrite COMMAND
•BESTEHT AUS 0 BIS YYYY ZUGÄNGLICHEN SEKTOREN BASIEREND AUF XXXX)
NICHT- AUTHENTISIERUNGSBEREICH
•DARAUF KANN OHNE AUTHENTISIERUNG ZUGEGRIFFEN WERDEN
•DIE ANZAHL DER BLÖCKE IST INSGESAMT XXXX
•DARAUF KANN MIT STANDART BEFEHL ZUGEGRIFFEN WERDEN
Read / Write COMMAND
•BESTEHT AUS 0 BIS (XXXX - 1) ZUGÄNGLICHEN SEKTOREN
FIG. 7B
REGELN FÜR ÄNDERN VON BEREICHSGRÖSSE
•VERWENDE DEDIZIERTEN BEFEHL ZU ÄNDERN DER BEREICHSGRÖSSE NACH AUTHENTISIERUNG
•LÖSCHE ALLE INHALTE AUS FLASH UND AKTUALISIERE WERT XXXX
•SPEICHERE WERT XXXX IN ARBEITSBEREICH IN FLASH, DER NUR DURCH MIKROCOMPUTER IN SPEICHERKARTE BETRIEBEN WERDEN SOLL
FIG. 7C
109
HALBLEITER- SPEICHERKARTE
VERÄNDERBARER BLOCKBEREICH
501
SPEZIALBEREICH
341
MEDIUM- ID
304
AUTHENTISIERUNGSBEREICH
XXXX+ YYYY
VERSCHLÜSSELTER SCHLÜSSEL
332
425
XXXX
NICHT- AUTHENTISIERUNGS- BEREICH
XXXX – 1
VERSCHLÜSSELTER INHALT
331
426
ANWENDERDATEN
427
0000
KANN MIT EINEM DEDIZIERTEN BEFEHL AUSGELESEN WERDEN
KANN MIT EINEM SPEZIELLEN BEFEHL NUR VON AUTHENTISIERTEN EINRICHTUNGEN GELESEN / GESCHRIEBEN WERDEN
KANN MIT EINEM STANDARD- BEFEHL WIE ATA ODER SCSI AUSGELESEN WERDEN

FIG. 8

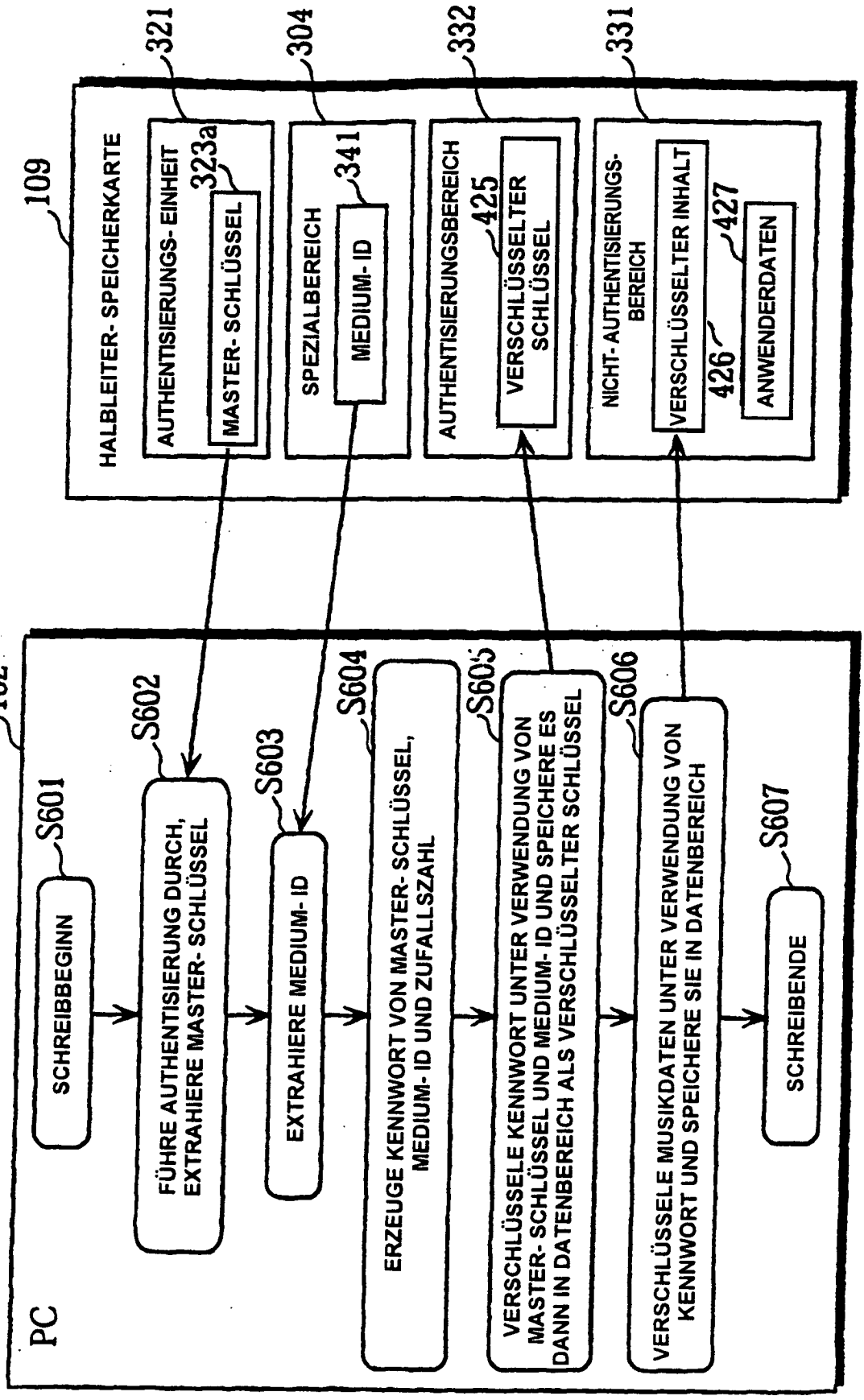

PC
102
SCHREIBBEGINN
S601
FÜHRE AUTHENTISIERUNG DURCH, EXTRAHIERE MASTER- SCHLÜSSEL
S602
EXTRAHIERE MEDIUM- ID
S603
ERZEUGE KENNWORT VON MASTER- SCHLÜSSEL, MEDIUM- ID UND ZUFALLSZAHL
S604
VERSCHLÜSSELE KENNWORT UNTER VERWENDUNG VON MASTER- SCHLÜSSEL UND MEDIUM- ID UND SPEICHERE ES DANN IN DATENBEREICH ALS VERSCHLÜSSELTER SCHLÜSSEL
S605
VERSCHLÜSSELE MUSIKDATEN UNTER VERWENDUNG VON KENNWORT UND SPEICHERE SIE IN DATENBEREICH
S606
SCHREIBENDE
S607
109
HALBLEITER- SPEICHERKARTE
321
AUTHENTISIERUNGS- EINHEIT
323a
MASTER- SCHLÜSSEL
304
SPEZIALBEREICH
341
MEDIUM- ID
332
AUTHENTISIERUNGSBEREICH
425
VERSCHLÜSSELTER SCHLÜSSEL
331
NICHT- AUTHENTISIERUNGS- BEREICH
426
VERSCHLÜSSELTER INHALT
427
ANWENDERDATEN

FIG. 9

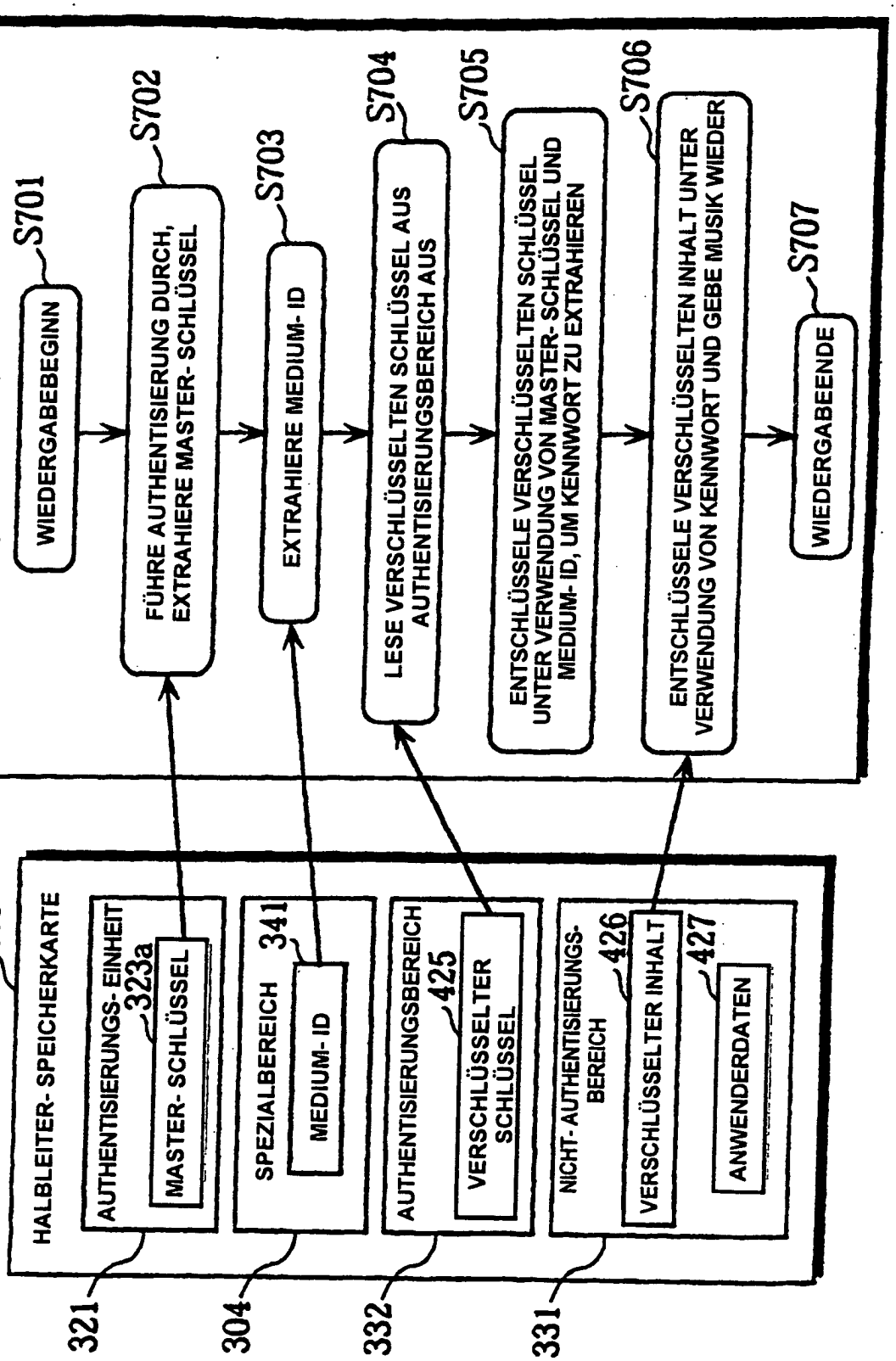

201
WIEDERGABEGERÄT
S701
WIEDERGABEBEGINN
S702
FÜHRE AUTHENTISIERUNG DURCH, EXTRAHIERE MASTER- SCHLÜSSEL
S703
EXTRAHIERE MEDIUM- ID
S704
LESE VERSCHLÜSSELTEN SCHLÜSSEL AUS AUTHENTISIERUNGSBEREICH AUS
S705
ENTSCHLÜSSELE VERSCHLÜSSELTEN SCHLÜSSEL UNTER VERWENDUNG VON MASTER- SCHLÜSSEL UND MEDIUM- ID, UM KENNWORT ZU EXTRAHIEREN
S706
ENTSCHLÜSSELE VERSCHLÜSSELTEN INHALT UNTER VERWENDUNG VON KENNWORT UND GEBE MUSIK WIEDER
S707
WIEDERGABEENDE
109
HALBLEITER- SPEICHERKARTE
AUTHENTISIERUNGS- EINHEIT
323a
MASTER- SCHLÜSSEL
SPEZIALBEREICH
341
MEDIUM- ID
AUTHENTISIERUNGSBEREICH
425
VERSCHLÜSSELTER SCHLÜSSEL
NICHT- AUTHENTISIERUNGS- BEREICH
426
VERSCHLÜSSELTER INHALT
427
ANWENDERDATEN
321
304
332
331

FIG. 10

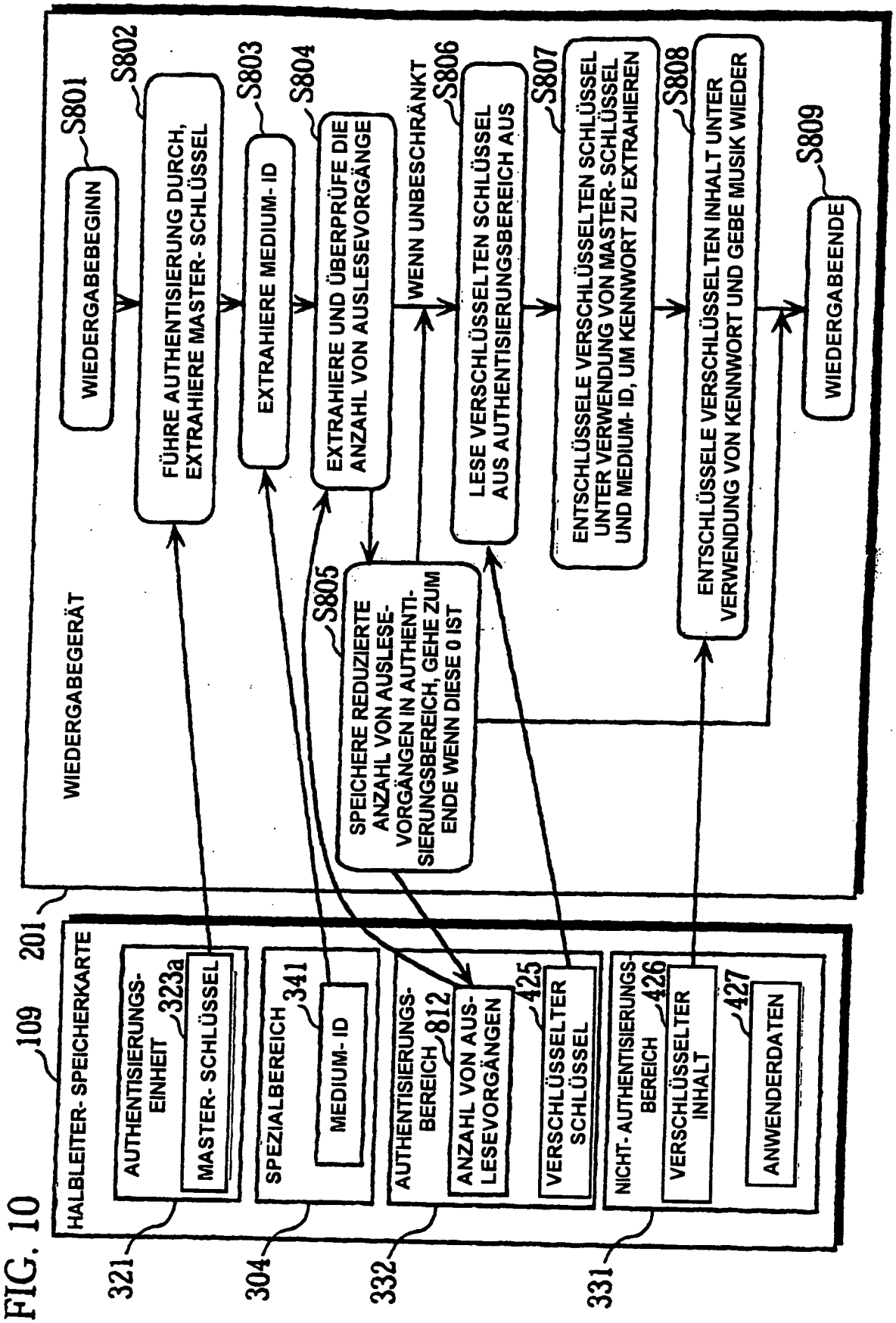

WIEDERGABEGERÄT
201
HALBLEITER- SPEICHERKARTE
109
AUTHENTISIERUNGS- EINHEIT
323a
MASTER- SCHLÜSSEL
SPEZIALBEREICH
341
MEDIUM- ID
AUTHENTISIERUNGS- BEREICH
812
ANZAHL VON AUS- LESEVORGÄNGEN
425
VERSCHLÜSSELTER SCHLÜSSEL
NICHT- AUTHENTISIERUNGS- BEREICH
426
VERSCHLÜSSELTER INHALT
427
ANWENDERDATEN
321
304
332
331
WIEDERGABEBEGINN
S801
FÜHRE AUTHENTISIERUNG DURCH, EXTRAHIERE MASTER- SCHLÜSSEL
S802
EXTRAHIERE MEDIUM- ID
S803
EXTRAHIERE UND ÜBERPRÜFE DIE ANZAHL VON AUSLESEVORGÄNGE
S804
SPEICHERE REDUZIERTE ANZAHL VON AUSLESE- VORGÄNGEN IN AUTHENTI- SIERUNGSBEREICH, GEHE ZUM ENDE WENN DIESE 0 IST
S805
WENN UNBESCHRÄNKT
S806
LESE VERSCHLÜSSELTEN SCHLÜSSEL AUS AUTHENTISIERUNGSBEREICH AUS
S807
ENTSCHLÜSSELE VERSCHLÜSSELTEN SCHLÜSSEL UNTER VERWENDUNG VON MASTER- SCHLÜSSEL UND MEDIUM- ID, UM KENNWORT ZU EXTRAHIEREN
S808
ENTSCHLÜSSELE VERSCHLÜSSELTEN INHALT UNTER VERWENDUNG VON KENNWORT UND GEBE MUSIK WIEDER
S809
WIEDERGABEENDE

FIG. 11

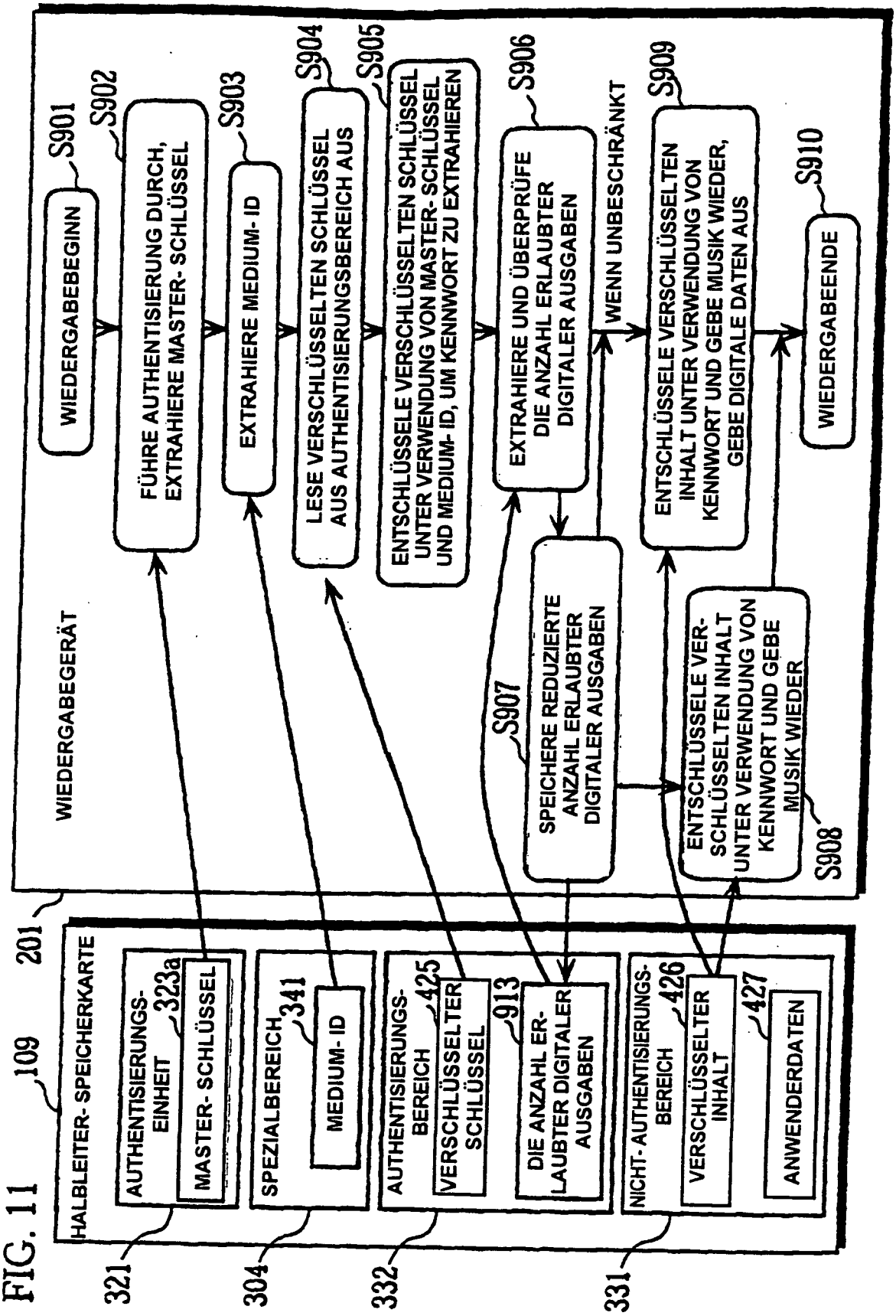
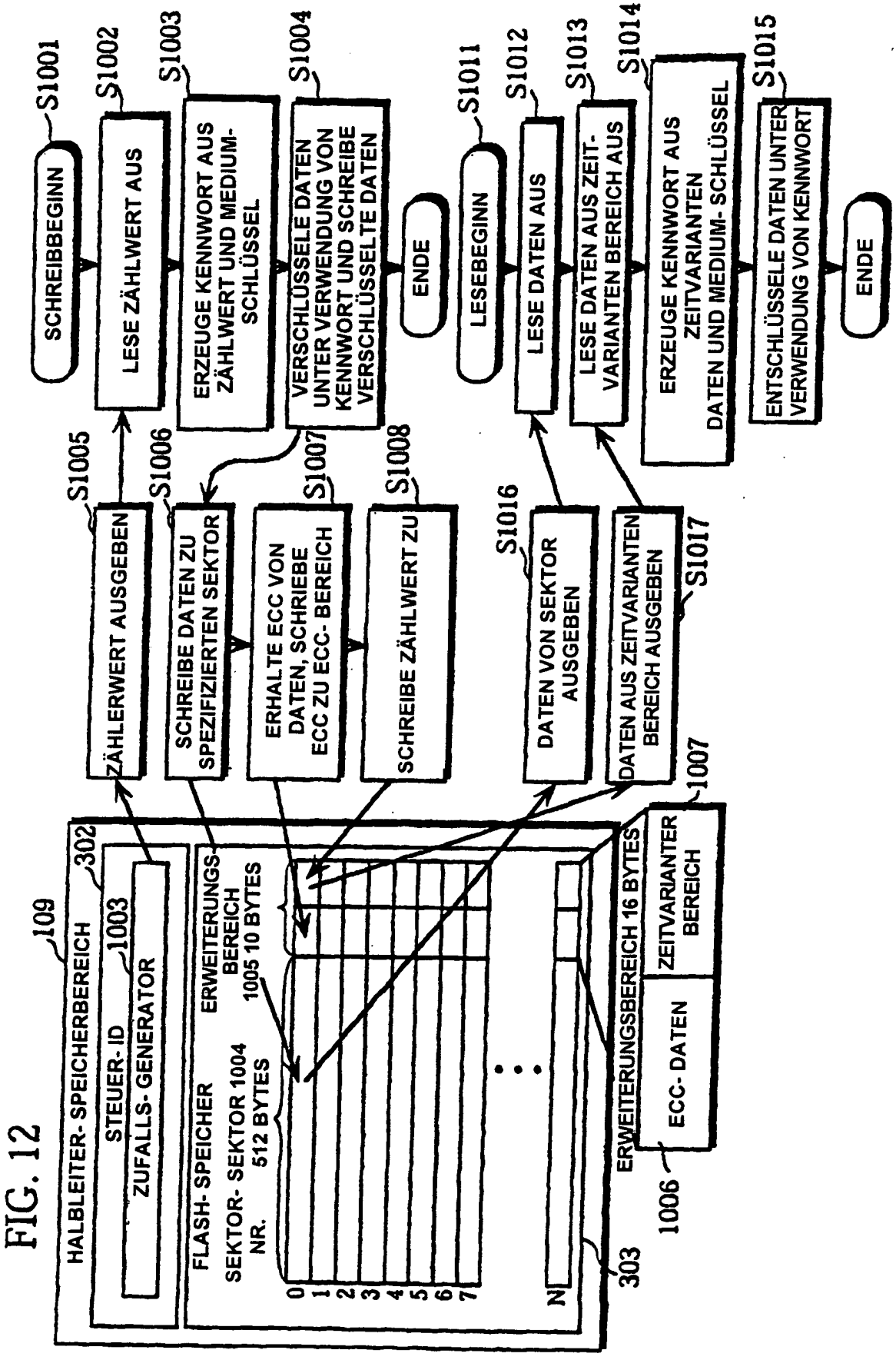

201
109
HALBLEITER- SPEICHERKARTE
AUTHENTISIERUNGS- EINHEIT
323a
MASTER- SCHLÜSSEL
SPEZIALBEREICH
341
MEDIUM- ID
AUTHENTISIERUNGS- BEREICH
425
VERSCHLÜSSELTER SCHLÜSSEL
913
DIE ANZAHL ER- LAUBTER DIGITALER AUSGABEN
NICHT- AUTHENTISIERUNGS- BEREICH
426
VERSCHLÜSSELTER INHALT
427
ANWENDERDATEN
321
304
332
331
WIEDERGABEGERÄT
S901
WIEDERGABEBEGINN
S902
FÜHRE AUTHENTISIERUNG DURCH, EXTRAHIERE MASTER- SCHLÜSSEL
S903
EXTRAHIERE MEDIUM- ID
S904
LESE VERSCHLÜSSELTEN SCHLÜSSEL AUS AUTHENTISIERUNGSBEREICH AUS
S905
ENTSCHLÜSSELE VERSCHLÜSSELTEN SCHLÜSSEL UNTER VERWENDUNG VON MASTER- SCHLÜSSEL UND MEDIUM- ID, UM KENNWORT ZU EXTRAHIEREN
S906
EXTRAHIERE UND ÜBERPRÜFE DIE ANZAHL ERLAUBTER DIGITALER AUSGABEN
S907
SPEICHERE REDUZIERTE ANZAHL ERLAUBTER DIGITALER AUSGABEN
WENN UNBESCHRÄNKT
S908
ENTSCHLÜSSELE VER- SCHLÜSSELTEN INHALT UNTER VERWENDUNG VON KENNWORT UND GEBE MUSIK WIEDER
S909
ENTSCHLÜSSELE VERSCHLÜSSELTEN INHALT UNTER VERWENDUNG VON KENNWORT UND GEBE MUSIK WIEDER, GEBE DIGITALE DATEN AUS
S910
WIEDERGABEENDE

FIG. 12


109
HALBLEITER- SPEICHERBEREICH
302
STEUER- ID
1003
ZUFALLS- GENERATOR
FLASH- SPEICHER
ERWEITERUNGS BEREICH
1005 10 BYTES
SEKTOR- SEKTOR 1004
NR.
512 BYTES
0
1
2
3
4
5
6
7
N
303
ERWEITERUNGSBEREICH 16 BYTES
ZEITVARIANTER BEREICH
ECC- DATEN
1006
1007
S1001
SCHREIBBEGINN
S1002
LESE ZÄHLWERT AUS
S1003
ERZEUGE KENNWORT AUS ZÄHLWERT UND MEDIUM- SCHLÜSSEL
S1004
VERSCHLÜSSELE DATEN UNTER VERWENDUNG VON KENNWORT UND SCHREIBE VERSCHLÜSSELTE DATEN
ENDE
S1005
ZÄHLERWERT AUSGEBEN
S1006
SCHREIBE DATEN ZU SPEZIFIZIERTEN SEKTOR
S1007
ERHALTE ECC VON DATEN, SCHRIEBE ECC ZU ECC- BEREICH
S1008
SCHREIBE ZÄHLWERT ZU
S1011
LESEBEGINN
S1012
LESE DATEN AUS
S1013
LESE DATEN AUS ZEIT- VARIANTEN BEREICH AUS
S1014
ERZEUGE KENNWORT AUS ZEITVARIANTEN DATEN UND MEDIUM- SCHLÜSSEL
S1015
ENTSCHLÜSSELE DATEN UNTER VERWENDUNG VON KENNWORT
ENDE
S1016
DATEN VON SEKTOR AUSGEBEN
S1017
DATEN AUS ZEITVARIANTEN BEREICH AUSGEBEN

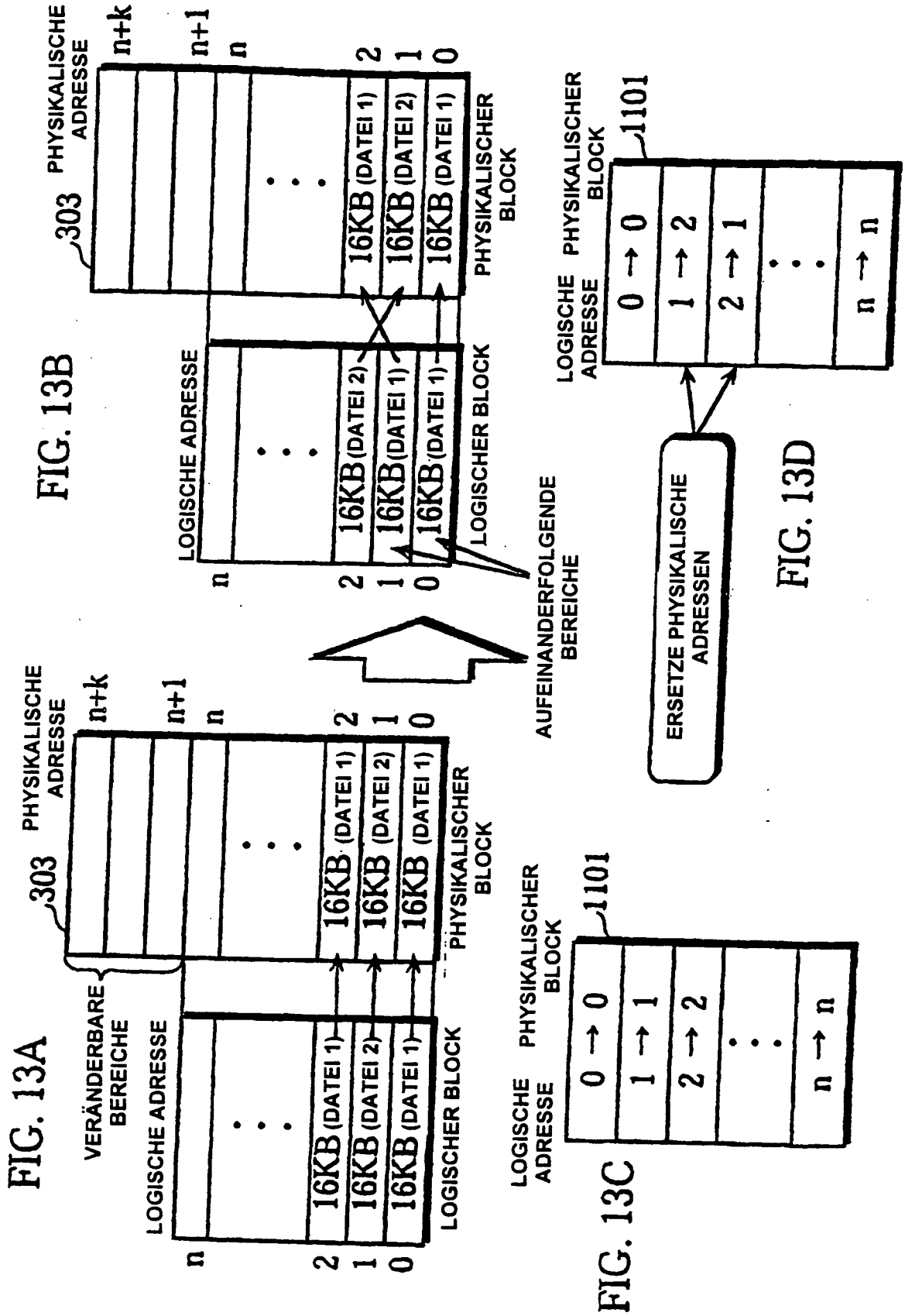


FIG. 13A
VERÄNDERBARE BEREICHE
LOGISCHE ADRESSE
PHYSIKALISCHE ADRESSE
303
n+k
n+1
n
2
1
0
16KB (DATEI 1)
16KB (DATEI 2)
16KB (DATEI 1)
LOGISCHER BLOCK
PHYSIKALISCHER BLOCK
FIG. 13B
AUFEINANDERFOLGENDE BEREICHE
FIG. 13C
LOGISCHE ADRESSE
PHYSIKALISCHER BLOCK
1101
0 → 0
1 → 1
2 → 2
n → n
ERSETZE PHYSIKALISCHE ADRESSEN
FIG. 13D
1 → 2
2 → 1

FIG. 14A

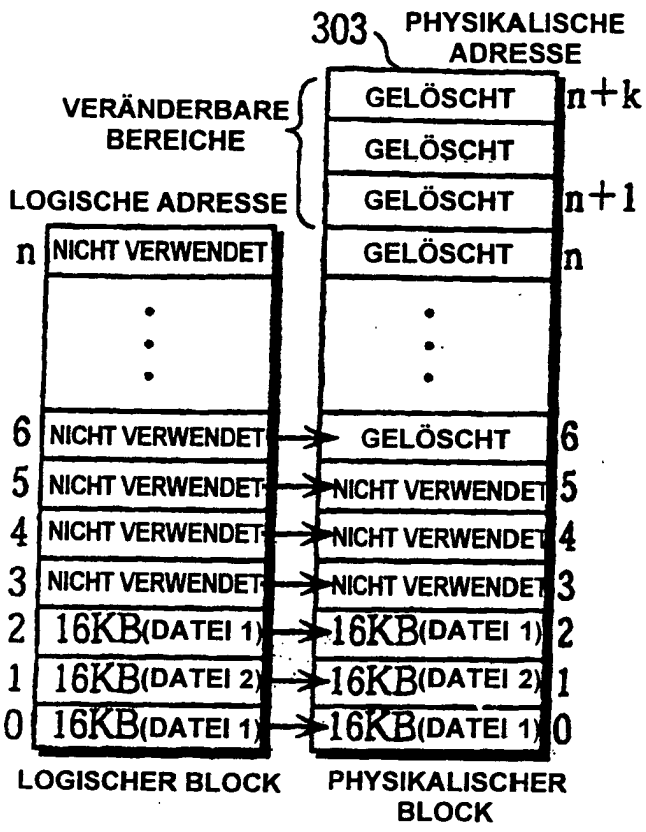


FIG. 14B

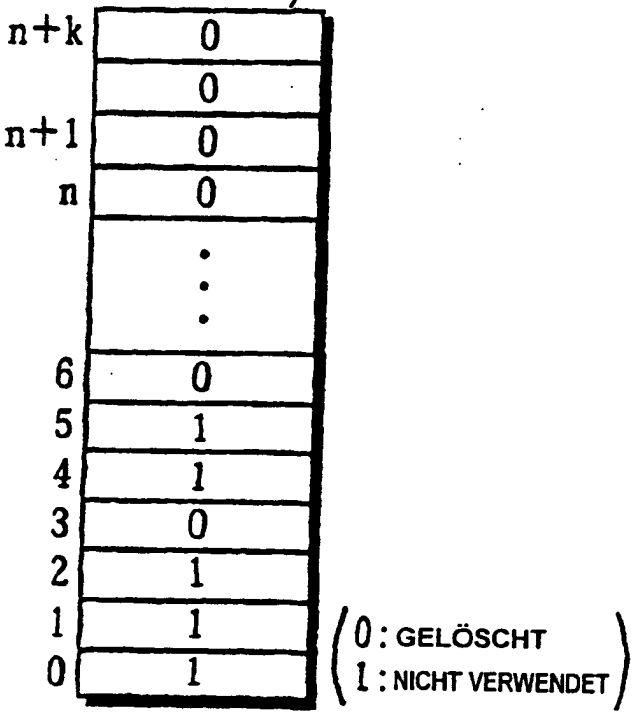


FIG. 14C

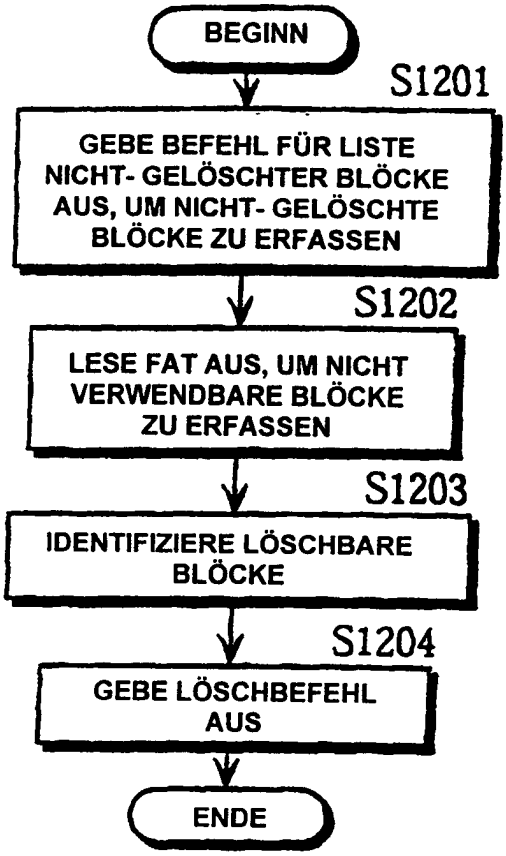


FIG. 14D

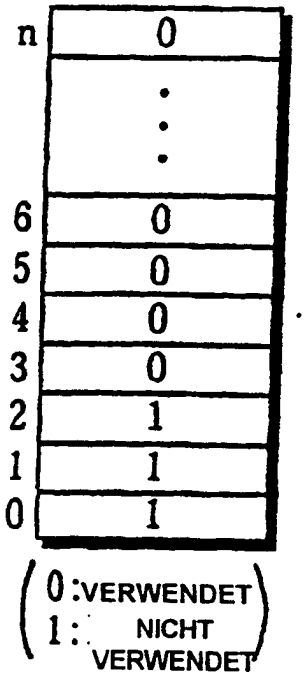


FIG. 15

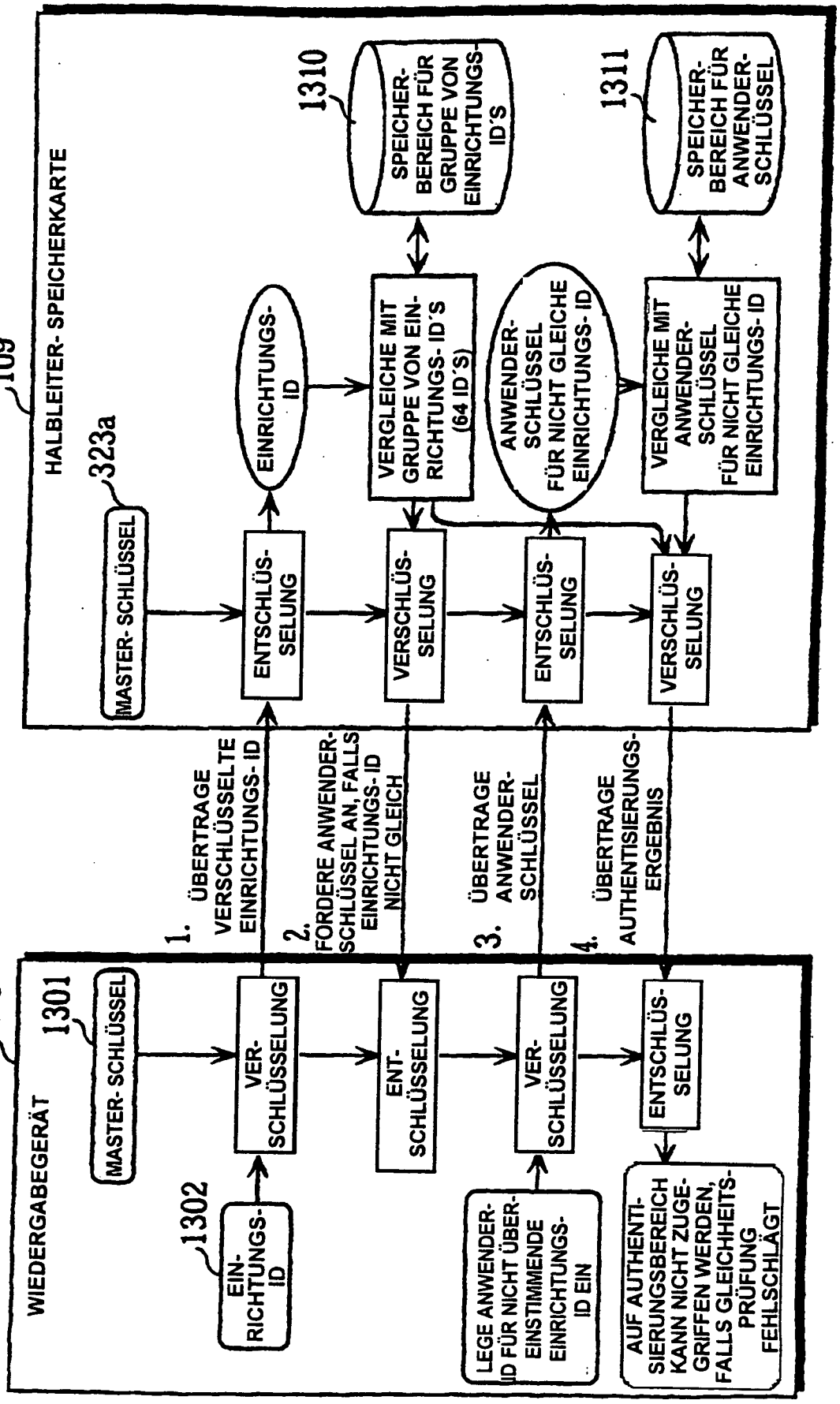

201
WIEDERGABEGERÄT
1301
MASTER-SCHLÜSSEL
1302
EIN-RICHTUNGS-ID
VER-SCHLÜSSELUNG
ENT-SCHLÜSSELUNG
VER-SCHLÜSSELUNG
ENTSCHLÜS-SELUNG
LEGE ANWENDER-ID FÜR NICHT ÜBER-EINSTIMMENDE EINRICHTUNGS-ID EIN
AUF AUTHENTI-SIERUNGSBEREICH KANN NICHT ZUGE-GRIFFEN WERDEN, FALLS GLEICHHEITS-PRÜFUNG FEHLSCHLÄGT
1. ÜBERTRAGE VERSCHLÜSSELTE EINRICHTUNGS-ID
2. FORDERE ANWENDER-SCHLÜSSEL AN, FALLS EINRICHTUNGS-ID NICHT GLEICH
3. ÜBERTRAGE ANWENDER-SCHLÜSSEL
4. ÜBERTRAGE AUTHENTISIERUNGS-ERGEBNIS
109
HALBLEITER-SPEICHERKARTE
323a
MASTER-SCHLÜSSEL
ENTSCHLÜS-SELUNG
VERSCHLÜS-SELUNG
ENTSCHLÜS-SELUNG
VERSCHLÜS-SELUNG
EINRICHTUNGS-ID
VERGLEICHE MIT GRUPPE VON EIN-RICHTUNGS-ID´S (64 ID´S)
ANWENDER-SCHLÜSSEL FÜR NICHT GLEICHE EINRICHTUNGS-ID
VERGLEICHE MIT ANWENDER-SCHLÜSSEL FÜR NICHT GLEICHE EINRICHTUNGS-ID
1310
SPEICHER-BEREICH FÜR GRUPPE VON EINRICHTUNGS-ID´S
1311
SPEICHER-BEREICH FÜR ANWENDER-SCHLÜSSEL

FIG. 16

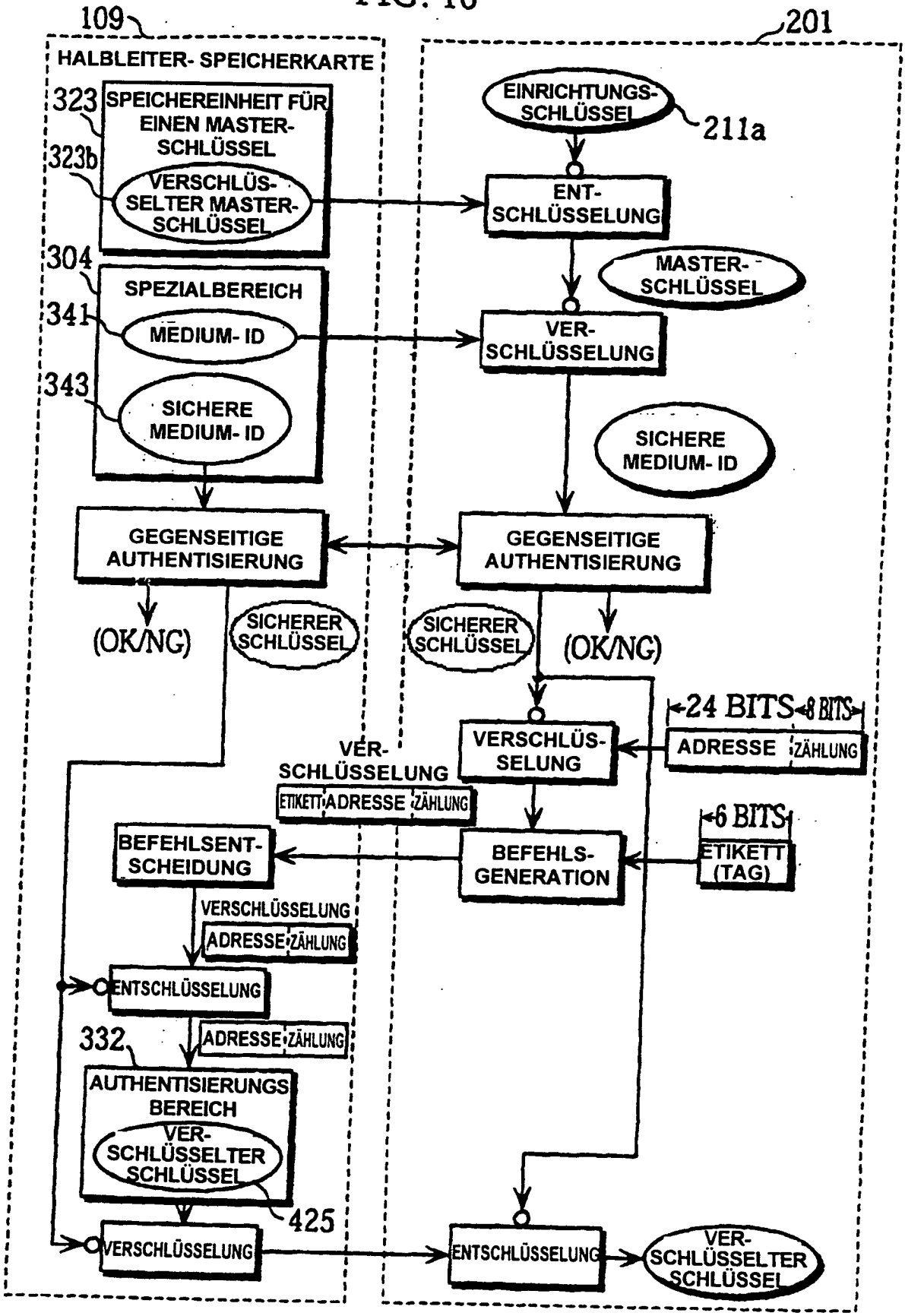

109
HALBLEITER- SPEICHERKARTE
323
SPEICHEREINHEIT FÜR EINEN MASTER-SCHLÜSSEL
323b
VERSCHLÜS-SELTER MASTER-SCHLÜSSEL
304
SPEZIALBEREICH
341
MEDIUM- ID
343
SICHERE MEDIUM- ID
GEGENSEITIGE AUTHENTISIERUNG
(OK/NG)
SICHERER SCHLÜSSEL
201
EINRICHTUNGS-SCHLÜSSEL
211a
ENT-SCHLÜSSELUNG
MASTER-SCHLÜSSEL
VER-SCHLÜSSELUNG
SICHERE MEDIUM- ID
GEGENSEITIGE AUTHENTISIERUNG
SICHERER SCHLÜSSEL
(OK/NG)
24 BITS
8 BITS
ADRESSE
ZÄHLUNG
VERSCHLÜS-SELUNG
VER-SCHLÜSSELUNG
ETIKETT
ADRESSE
ZÄHLUNG
6 BITS
ETIKETT (TAG)
BEFEHLS-GENERATION
BEFEHLSENT-SCHEIDUNG
VERSCHLÜSSELUNG
ADRESSE
ZÄHLUNG
ENTSCHLÜSSELUNG
ADRESSE
ZÄHLUNG
332
AUTHENTISIERUNGS BEREICH
VER-SCHLÜSSELTER SCHLÜSSEL
425
VERSCHLÜSSELUNG
ENTSCHLÜSSELUNG
VER-SCHLÜSSELTER SCHLÜSSEL

FIG. 17

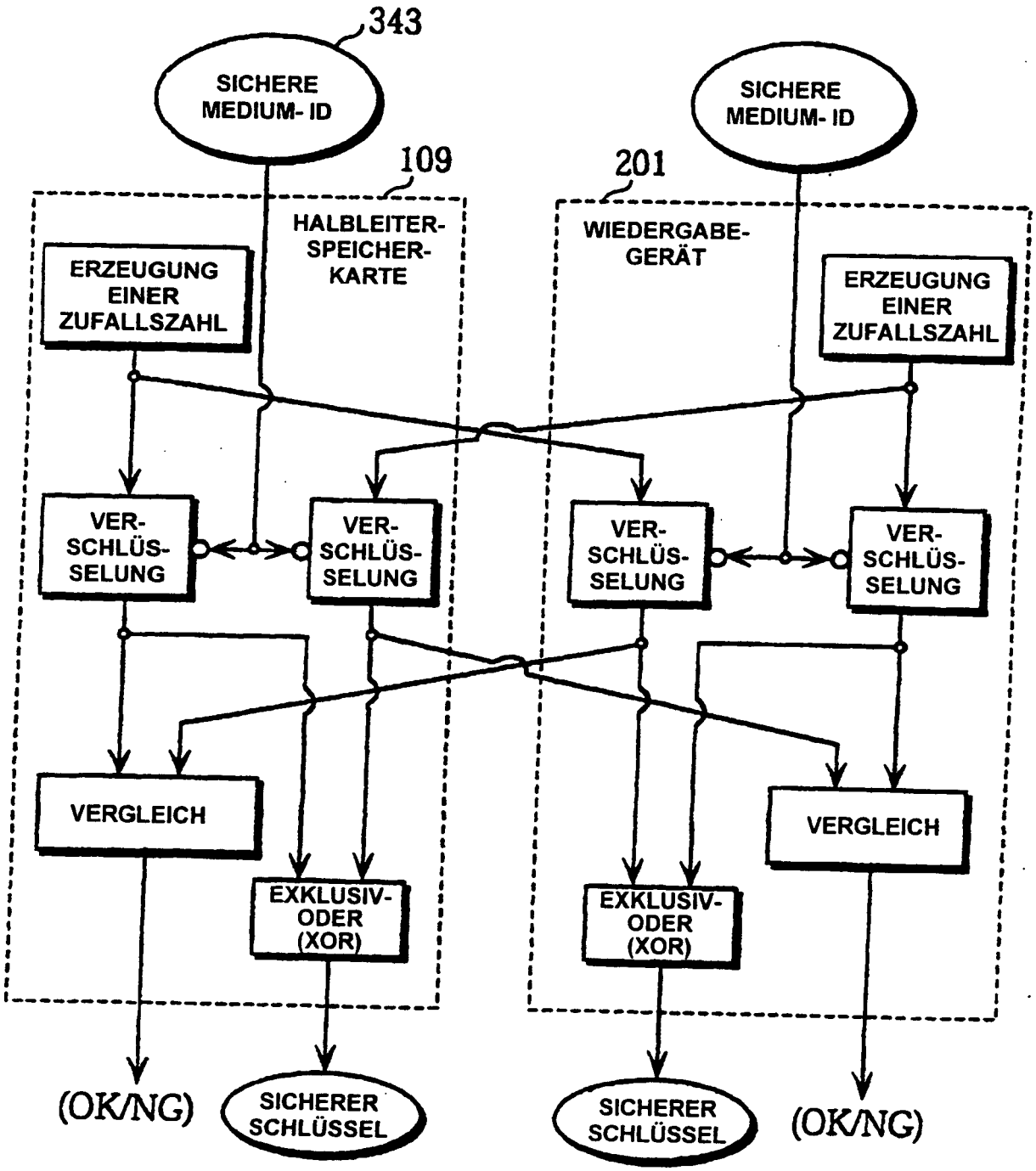

343
SICHERE MEDIUM- ID
109
HALBLEITER-SPEICHER-KARTE
ERZEUGUNG EINER ZUFALLSZAHL
VER-SCHLÜS-SELUNG
VER-SCHLÜS-SELUNG
VERGLEICH
EXKLUSIV-ODER (XOR)
(OK/NG)
SICHERER SCHLÜSSEL
SICHERE MEDIUM- ID
201
WIEDERGABE-GERÄT
ERZEUGUNG EINER ZUFALLSZAHL
VER-SCHLÜS-SELUNG
VER-SCHLÜS-SELUNG
VERGLEICH
EXKLUSIV-ODER (XOR)
SICHERER SCHLÜSSEL
(OK/NG)

FIG. 18A

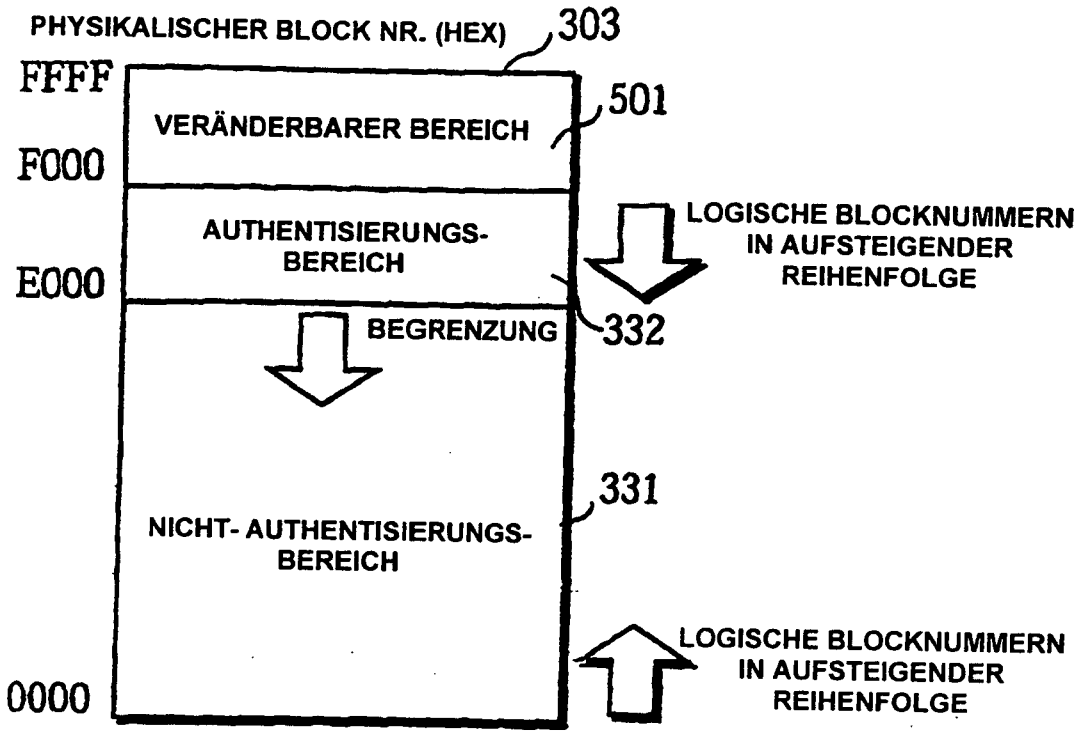


FIG. 18B

1103

LOGISCHE BLOCK- NR.	PHYSIKALISCHE BLOCK- NR.
0000	0000
0001	0001
0002	0002
•	•
•	•
•	•
•	•
•	•
•	•
DFFE	DFFE
DFFF	DFFF

FIG. 18C

1102

LOGISCHE BLOCK- NR.	PHYSIKALISCHE BLOCK- NR.
0000	EFFF
0001	EFFE
0FFE	E001
0FFF	E000

FIG. 19A

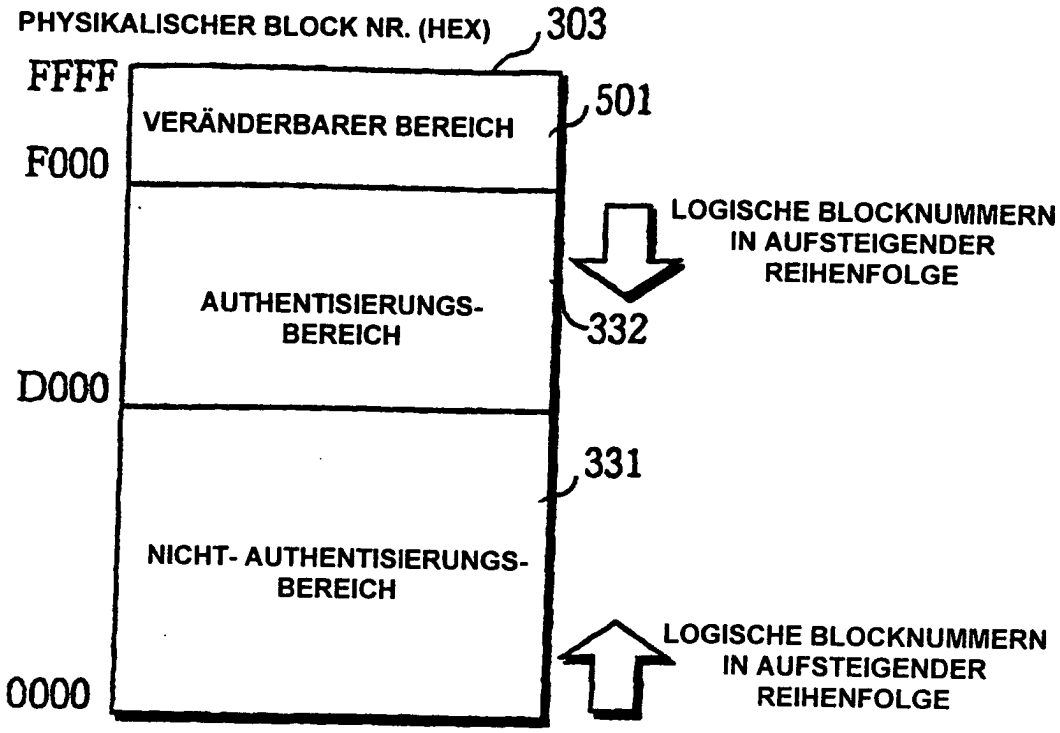


FIG. 19B

1103

LOGISCHE BLOCK- NR.	PHYSIKALISCHE BLOCK- NR.
0000	0000
0001	0001
0002	0002
•	•
•	•
•	•
•	•
•	•
•	•
CFFE	CFFE
CFFF	CFFF

FIG. 19C

1102

LOGISCHE BLOCK- NR.	PHYSIKALISCHE BLOCK- NR.
0000	EFFF
0001	EFFE
1FFE	D001
1FFF	D000