(19) Deutsches Patent- und Markenamt

(10) **DE 10 2013 105 248 A1** 2013.11.28

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2013 105 248.7**
(22) Anmeldetag: **23.05.2013**
(43) Offenlegungstag: **28.11.2013**

(51) Int Cl.: ***G06F 12/14*** (2013.01)

(30) Unionspriorität:
10-2012-0055527 24.05.2012 KR

(71) Anmelder:
Samsung Electronics Co., Ltd, Suwon-si, Gyeonggi-do, KR

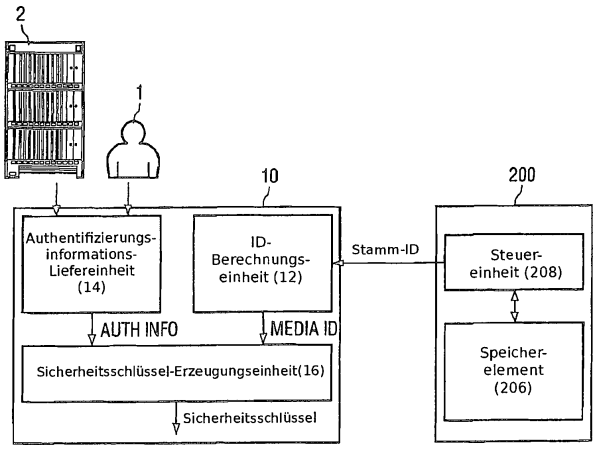
(74) Vertreter:
Kuhnen & Wacker Patent- und Rechtsanwaltsbüro, 85354, Freising, DE

(72) Erfinder:
Wang, Weixin, Gyeonggi-do, KR; Cho, Hee-Chang, Seoul, KR; Lee, Won-Seok, Gyeonggi-do, KR; Kim, Min-Wook, Seoul, KR; Jang, Hyoung-Suk, Suwon, Kyonggi, KR

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Vorrichtung zum Erzeugen eines Sicherheitsschlüssels unter Verwendung einer Vorrichtungs-ID und von Benutzer-Authentifizierungsinformation**

(57) Zusammenfassung: Eine Sicherheitsschlüssel-Erzeugungsvorrichtung (10) weist eine ID-Berechnungseinheit (12), die eine Stamm-ID von einer ersten Speichervorrichtung (200) empfängt und eine erste Medien-ID (eine eindeutige Kennung der ersten Speichervorrichtung) aus der ersten Stamm-ID berechnet; eine Benutzer-Authentifizierungsinformations-Bereitstellungsvorrichtung (14), die Benutzer-Authentifizierungsinformation zur Authentifizierung des aktuellen Benutzers (1) bereitstellt; und eine Sicherheitsschlüssel-Erzeugungseinheit (16) zum Erzeugen eines ersten Sicherheitsschlüssels unter Verwenden sowohl der ersten Medien-ID als auch der ersten Benutzer-Authentifizierungsinformation, auf. Der Sicherheitsschlüssel wird verwendet, um einen in der ersten Speichervorrichtung (200) gespeicherten Inhalt zu verschlüsseln/zu entschlüsseln. Die Sicherheitsschlüssel-Erzeugungseinheit (16) erzeugt einen ersten anderen Sicherheitsschlüssel unter Verwenden einer zweiten Medien-ID einer zweiten Speichervorrichtung und erzeugt einen zweiten anderen Sicherheitsschlüssel unter Verwenden zweiter Benutzer-Authentifizierungsinformation. Nur der erste Sicherheitsschlüssel kann verwendet werden, um in der ersten Speichervorrichtung (200) gespeicherten verschlüsselten Inhalt zu entschlüsseln, der unter Verwenden des ersten Sicherheitsschlüssels verschlüsselt worden ist.



Beschreibung

[0001] Diese Anmeldung beansprucht Priorität der koreanischen Patentanmeldung Nr. 10-2012-0055527, eingereicht am 24. Mai 2012 bei dem koreanischen Patentamt, die hier in ihrer Gesamtheit durch Bezugnahme mit aufgenommen wird.

HINTERGRUND

1. Technisches Gebiet

[0002] Die erfinderische Idee bezieht sich auf eine Sicherheitsschlüssel-Erzeugungsvorrichtung und insbesondere auf eine Vorrichtung zum Erzeugen eines Sicherheitsschlüssels, der sowohl zu einer speziellen Vorrichtung und einem speziellen Benutzer gehört, unter Verwenden sowohl einer Vorrichtungs-ID und einer Benutzer-Authentifizierungsinformation (wie z. B. ein Benutzerpasswort), eine den Sicherheitsschlüssel verwendende Speichervorrichtung und ein Sicherheitsschlüssel-Erzeugungsverfahren.

2. Verwandte Technik

[0003] In letzter Zeit sind unterschiedliche Typen von tragbaren Speichervorrichtungen auf dem Markt eingeführt worden. Diese tragbaren Speichervorrichtungen nehmen an Speicherkapazität zu und an Volumen ab und ihre Schnittstelle ist in/von gewöhnlich verfügbaren Host-Vorrichtungen einsetzbar/entfernbar (z. B. Computer, On-Demand-Druckern, Mobiltelefon, digitales Fernsehen, etc.). Mithin nimmt die Nachfrage nach tragbaren Speichervorrichtungen zu. Einige Beispiele der tragbaren Speichervorrichtungen weisen eine einen Flash-Speicher als Speichermedium verwendende Speicherkarte (z. B. SD-Karte), einen Universal-Serial-Bus-(USB)-Speicher („USB-Laufwerk"), der mit einem USB-Port verbunden werden kann, und ein Festkörperlaufwerk (SSD) auf. Zusätzlich sind tragbare Festplatten als günstige Speichervorrichtungen beurteilt worden und es ist ein externes Festplattenlaufwerk eingeführt worden. Das externe Festplattenlaufwerk bietet im Gegensatz zu einem herkömmlichen in einem PC eingebauten Festplattenlaufwerk Mobilität.

[0004] Dieser Trend ist nicht auf tragbare Speichervorrichtungen begrenzt. Host-Vorrichtungen, die mit den tragbaren Speichervorrichtungen verbunden werden können, werden ebenso kleiner. Dementsprechend ist eine Umgebung geschaffen worden, in der ein in einer tragbaren Speichervorrichtung gespeicherter digitaler Inhalt, immer und überall genutzt werden kann. Durch Bilden dieser Umgebung werden kommerziell hergestellte digitale Inhalte zunehmend verteilt und in Form von digitalen Daten verkauft. Dieses erhöht die Bedeutung von Technologien, die das illegale Kopieren von digitalem Inhalt verhindern.

[0005] Um das illegale Kopieren von digitalen Inhalten zu verhindern, kann der digitale Inhalt verschlüsselt werden und sodann in einer tragbaren Speichervorrichtung gespeichert werden. Hierbei werden die digitalen Inhalte unter Verwenden eines speziellen digitalen Sicherheitsschlüssels verschlüsselt. Verschlüsselungs- und Entschlüsselungstechnologien, die einen digitalen Verschlüsselungsschlüssel verwenden, der nur mit einer speziellen Vorrichtung in Verbindung gesetzt wird, beseitigen einen Datenschutz, wenn die spezifische Vorrichtung verwendet wird.

KURZFASSUNG

[0006] Aspekte der vorliegenden Erfindung sehen eine Vorrichtung zum Erzeugen eines Sicherheitsschlüssels vor, der sowohl zu einer speziellen Vorrichtung und einem speziellen Benutzer gehört, einen Speichervorrichtung-Verschlüsselungsinhalt, der den Sicherheitsschlüssel verwendet und den verschlüsselten Inhalt speichert, und ein Sicherheitsschlüssel-Erzeugungsverfahren vor. Während eine herkömmliche Verschlüsselungs- und Entschlüsselungstechnologie einen Schlüssel verwendet, der nur mit einer speziellen Vorrichtung in Verbindung gesetzt wird und einen Datenschutz entfernt, wenn die spezifische Vorrichtung verwendet wird, sehen Gesichtspunkte der vorliegenden Erfindung eine Vorrichtung zum Erzeugen eines Sicherheitsschlüssels vor, der sowohl zu einer speziellen Vorrichtung und einem speziellen Benutzer gehört, derart, dass nur eine spezifische Person den Inhalt ausspielen kann (z. B. auf der bestimmten Vorrichtung), um seine oder ihre Privatsphäre zu schützen. Gesichtspunkte der vorliegenden Erfindung sehen eine Technologie vor, die einen Sicherheitsschlüssel erzeugt und verwendet, der nicht ausschließlich zu einer speziellen Vorrichtung sondern auch zu einem spezifischen Benutzer gehört.

[0007] Aspekte der vorliegenden Erfindung sehen ebenso eine Vorrichtung zum Erzeugen eines Sicherheitsschlüssels unter Verwenden sowohl einer Kennung einer bestimmten Vorrichtung und Benutzer-Authentifizierungsinformation, die von einem Benutzer eingegeben wird, einen Speichervorrichtungs-Verschlüsselungsinhalt, der den Sicherheitsschlüssel verwendet, und ein Speichern des verschlüsselten Inhalts und ein Sicherheitsschlüssel-Erzeugungsverfahren, vor.

[0008] Aspekte der vorliegenden Erfindung sehen ebenso eine Vorrichtung zum sicheren Erzeugen eines Sicherheitsschlüssels in einer Host-Vorrichtung vor, die ein Trusted-Computing unterstützt.

[0009] Aspekte der vorliegenden Erfindung sehen ebenso eine Host-Schnittstelle vor, die einen Sicherheitsschlüssel in einer gesicherten Ausführungsum-

gebung erzeugt, um den Verlust einer Vorrichtung-ID zu hindern, eine Benutzer-Authentifizierungsinformation und den erzeugten Sicherheitsschlüssel vor.

[0010] Jedoch sind Aspekte der vorliegenden Erfindung nicht auf die hier zuvor dargelegten beschränkt. Die obigen und weitere Gesichtspunkte der vorliegenden Erfindung werden dem Durchschnittsfachmann, auf den sich die vorliegende Erfindung bezieht, durch Bezugnehmen auf eine detaillierte Beschreibung der weiter unten vorgestellten vorliegenden Erfindung klarer werden.

[0011] Gemäß einem Aspekt der vorliegenden Erfindung ist eine Sicherheitsschlüssel-Erzeugungseinheit, die eine ID-Berechnungseinheit aufweist, die eine Stamm-ID von einer Speichervorrichtung empfängt und eine Medien-ID, die eine eindeutige Kennung der Speichervorrichtung ist, von der Stamm-ID berechnet; eine Authentifizierungsinformations-Liefereinheit, die Authentifizierungsinformation zum Authentifizieren eines Benutzers an eine Sicherheitsschlüssel-Erzeugungseinheit liefert; und die Sicherheitsschlüssel-Erzeugungseinheit, die einen Sicherheitsschlüssel unter Verwenden sowohl der Medien-ID und der Authentifizierungsinformation erzeugt, vorgesehen.

[0012] Gemäß einem weiteren Aspekt der vorliegenden Erfindung sind eine Sicherheitsschlüssel-Erzeugungsvorrichtung mit einer Speicherschnittstelle, die eine Stamm-ID von einer Speichervorrichtung empfängt und die Stamm-ID einem Prozessor liefert, und der Prozessor, der eine Medien-ID, die eine eindeutige Kennung der Speichervorrichtung ist, von der Stamm-ID berechnet und einen Sicherheitsschlüssel unter Verwenden sowohl der Medien-ID und einer Authentifizierungsinformation zum Authentifizieren eines Benutzers erzeugt, vorgesehen.

[0013] Gemäß einem weiteren Aspekt der vorliegenden Erfindung sind eine Speichervorrichtung mit einem Speicherelement, das eine Speicher-ID, die eine eindeutige Kennung des Speicherelements ist, und eine verschlüsselte Speicher-ID speichert, die durch Verschlüsseln der Speicher-ID erhalten ist, eine Host-Schnittstelle, die Authentifizierungsinformation zum Authentifizieren eines Benutzers von einer Host-Vorrichtung empfängt und die Authentifizierungsinformation einer Sicherheitsschlüssel-Erzeugungseinheit liefert und einen Inhalt von der Host-Vorrichtung empfängt und den Inhalt einer Verschlüsselungseinheit liefert, eine speicherabgeleitete ID-Berechnungseinheit, die die verschlüsselte Speicher-ID von dem Speicherelement liest, die Speicher-ID durch Entschlüsseln der verschlüsselten Speicher-ID erhält und eine speicherabgeleitete ID, die eine weitere eindeutige Kennung des Speicherelements ist, unter Verwenden der Speicher-ID erzeugt, wobei die Sicherheitsschlüssel-Erzeugungseinheit einen Sicherheitsschlüssel unter Verwenden sowohl der Authentifizierungsinformation und der speicherabgeleiteten ID erzeugt, und, wobei die Verschlüsselungseinheit den Inhalt unter Verwenden des Sicherheitsschlüssels verschlüsselt und den verschlüsselten Inhalt in dem Speicherelement speichert, vorgesehen.

[0014] Ein Sicherheitsschlüssel-Erzeugungsverfahren weist ein elektrisches Verbinden einer Speichervorrichtung mit einer Sicherheitsschlüssel-Erzeugungsvorrichtung, ein Empfangen einer Stamm-ID von der Speichervorrichtung und ein Berechnen einer Medien-ID, die eine eindeutige Kennung der Speichervorrichtung ist, aus der Stamm-ID unter Verwenden der Sicherheitsschlüssel-Erzeugungseinheit, ein Empfangen von Authentifizierungsinformation zum Authentifizieren eines Benutzers direkt von dem Benutzer oder ein Empfangen der Authentifizierungsinformation von einer anderen Vorrichtung, die über ein Netzwerk unter Verwenden der Sicherheitsschlüssel-Erzeugungsvorrichtung verbunden ist und ein Erzeugen eines Sicherheitsschlüssels unter Verwenden sowohl der Medien-ID und der Authentifizierungsinformation unter Verwenden der Sicherheitsschlüssel-Erzeugungsvorrichtung, auf.

[0015] Die vorliegende Erfindung wird nun in Bezug auf die beigefügten Zeichnungen hiernach genauer beschrieben werden, in denen beispielhafte Ausführungsformen der Erfindung dargestellt sind. Jedoch kann diese Erfindung in unterschiedlichen Formen verkörpert sein und sollte nicht als auf die hier zuvor festgelegten beispielhaften Ausführungsformen beschränkend aufgefasst werden. Vielmehr sind diese beispielhaften Ausführungsformen vorgesehen, so dass diese Offenbarung gründlich und vollständig ist und den Schutzumfang der erfinderischen Idee den Fachleuten vollständig vermittelt. Die gleichen Bezugszeichen geben die gleichen Komponenten durchgängig durch die Spezifikation an. In den beigefügten Zeichnungen kann die Stärke von Schichten und Bereichen zur Klarheit übertrieben sein. Die Verwendung der Begriffe „einer/eine/eines" und ähnlicher Bezüge in diesem Zusammenhang zum Beschreiben der Erfindung (insbesondere in dem Zusammenhang der folgenden Ansprüche) sollen derart aufgefasst werden, dass sie sowohl die Singularform als auch die Pluralform mit einschließen, wenn hier nicht anders angegeben oder klar durch den Zusammenhang widersprochen wird. Die Begriffe „aufweisend", „enthaltend" und „beinhaltend" sind als nach oben hin offene Begriffe (z. B. mit der Bedeutung „aufweisend, aber nicht begrenzt darauf") aufzufassen, wenn es nicht anders angemerkt ist.

[0016] Wenn nicht anders definiert, haben alle technischen und wissenschaftlichen Begriffe, die hier verwendet werden, die gleiche Bedeutung wie gewöhnlich von einem Durchschnittsfachmann verstanden, an den sich diese Erfindung richtet. Es ist zu beach-

ten, dass die Verwendung von irgendwelchen und allen Beispielen, oder beispielhaften Begriffen, die hier vorgesehen sind, beabsichtigt ist, nur die Erfindung besser zu beleuchten und stellt keine Begrenzung des Umfangs der Erfindung dar, wenn es nicht anders angegeben ist. Darüber hinaus können alle Begriffe, die in allgemein verwendeten Wörterbüchern definiert sind, nicht als zu weit interpretiert werden.

KURZBESCHREIBUNG DER ZEICHNUNGEN

[0017] Die obigen und weitere Aspekte und Eigenschaften der vorliegenden Erfindung werden durch Beschreiben im Detail von beispielhaften Ausführungsformen davon in Bezug auf die beigefügten Zeichnungen klarer werden, wobei:

[0018] Fig. 1 ein Blockdiagramm einer Sicherheitsschlüssel-Erzeugungseinheit gemäß einer beispielhaften Ausführungsform der vorliegenden Erfindung ist;

[0019] Fig. 2 und Fig. 3 Blockdiagramme sind, die die Konfiguration in Verhältnis mit einer ID-Berechnungseinheit, die in der Sicherheitsschlüssel-Erzeugungsvorrichtung von der Fig. 1 enthalten ist, veranschaulicht;

[0020] Fig. 4 ein Referenzdiagramm ist, das den Betrieb der ID-Berechnungseinheit, die in der Sicherheitsschlüssel-Erzeugungsvorrichtung von der Fig. 1 enthalten ist, veranschaulicht;

[0021] Fig. 5 ein Blockdiagramm einer Sicherheitsschlüssel-Erzeugungsvorrichtung gemäß einer beispielhaften Ausführungsform der vorliegenden Erfindung ist;

[0022] Fig. 6 und Fig. 7 Blockdiagramme der Sicherheitsschlüssel-Erzeugungsvorrichtung von der Fig. 5 sind, wenn die Sicherheitsschlüssel-Erzeugungseinheit eine Vorrichtung ist, die ein Trusted-Computing unterstützt;

[0023] Fig. 8 ein Blockdiagramm einer Sicherheitsschlüssel-Erzeugungsvorrichtung gemäß einer beispielhaften Ausführungsform der vorliegenden Erfindung ist;

[0024] Fig. 9 ein Referenzdiagramm, das die Position einer Peripherielogik in der Sicherheitsschlüssel-Erzeugungsvorrichtung von der Fig. 8 veranschaulicht ist;

[0025] Fig. 10 und Fig. 11 Blockdiagramme der Sicherheitsschlüssel-Erzeugungsvorrichtung von der Fig. 8 sind, wenn die Sicherheitsschlüssel-Erzeugungsvorrichtung eine Verschlüsselung und eine Entschlüsselung durchführt;

[0026] Fig. 12 und Fig. 13 Blockdiagramme einer Speichervorrichtung gemäß einer beispielhaften Ausführungsform der vorliegenden Erfindung sind;

[0027] Fig. 14 ein Blockdiagramm eines Speichersystems gemäß einer beispielhaften Ausführungsform der vorliegenden Erfindung ist;

[0028] Fig. 15 ein Ablaufdiagramm ist, das ein Sicherheitsschlüssel-Erzeugungsverfahren gemäß einer beispielhaften Ausführungsform der vorliegenden Erfindung veranschaulicht;

[0029] Fig. 16 ein Ablaufdiagramm ist, das ein Verfahren zum Erzeugen eines Sicherheitsschlüssels und Verschlüsseln eines Inhalts unter Verwenden des Sicherheitsschlüssels gemäß einer beispielhaften Ausführungsform der vorliegenden Erfindung veranschaulicht;

[0030] Fig. 17 bis Fig. 20 Ablaufdiagramme sind, die ein Verfahren zum Erzeugen einer Medien-ID gemäß einer beispielhaften Ausführungsform der vorliegenden Erfindung veranschaulichen;

[0031] Fig. 21 ein Ablaufdiagramm ist, das ein Verfahren zum Erzeugen eines Sicherheitsschlüssels und ein Entschlüsseln eines Inhalts unter Verwenden des Sicherheitsschlüssels gemäß einer beispielhaften Ausführungsform der vorliegenden Erfindung veranschaulicht;

[0032] Fig. 22 ein Ablaufdiagramm ist, das ein Verfahren veranschaulicht, bei dem ein Entschlüsseln von illegal kopiertem Inhalt gemäß einer beispielhaften Ausführungsform der vorliegenden Erfindung fehlschlägt; und

[0033] Fig. 23 ein Ablaufdiagramm ist, das ein Verfahren veranschaulicht, bei dem ein Entschlüsseln von Inhalt fehlschlägt, wenn nicht korrekte Benutzer-Authentifizierungsinformation gemäß einer beispielhaften Ausführungsform der vorliegenden Erfindung eingegeben wurde.

DETAILLIERTE BESCHREIBUNG DER BEISPIELHAFTEN AUSFÜHRUNGSFORMEN

[0034] Die Konfiguration und der Betrieb der Sicherheitsschlüssel-Erzeugungsvorrichtung **10** gemäß einer beispielhaften Ausführungsform der vorliegenden Erfindung wird nun in Bezug auf die Fig. 1 beschrieben werden. Die Sicherheitsschlüssel-Erzeugungsvorrichtung **10** gemäß der vorliegenden beispielhaften Ausführungsform ist mit einer nicht flüchtigen Speichervorrichtung **200** verbunden und erzeugt einen Sicherheitsschlüssel unter Verwenden einer Medien-ID und Authentifizierungsinformation zum Authentifizieren eines Benutzers **1**. Die Medien-ID ist eine eindeutige Kennung der Speichervorrichtung **200**.

[0035] Die Sicherheitsschlüssel-Erzeugungseinheit **10** ist mit der Speichervorrichtung **200** verbunden und empfängt eine Stamm-ID von der Speichervorrichtung **200**. Die Stamm-ID entspricht einem oder mehrerer ID-Daten, die verwendet werden, um die Medien-ID zu berechnen. Die Stamm-ID unterscheidet sicht von der Medien-ID. Die Sicherheitsschlüssel-Erzeugungsvorrichtung **10** erzeugt die Medien-ID aus der pimitiven ID und nicht aus der Authentifizierungsinformation zum Authentifizieren eines Benutzers **1**. Folglich empfängt die Sicherheitsschlüssel-Erzeugungsvorrichtung **10** die Medien-ID nicht von der Speichervorrichtung **200**, sondern empfängt die Stamm-ID (Ursprungsdaten), die verwendet werden, um die Medien-ID zu erzeugen. Dies kann den Verlust oder Erfassung der Medien-ID verhindern. Die Sicherheitsschlüssel-Erzeugungseinheit **10** kann Daten speichern, die verwendet werden, um die Medien-ID aus der Stamm-ID zu erzeugen.

[0036] Die Sicherheitsschlüssel-Erzeugungsvorrichtung **10** gemäß der aktuellen beispielhaften Ausführungsform weist eine ID-Berechnungseinheit **12**, eine Authentifizierungsinformations-Liefereinheit **14** und eine Sicherheitsschlüssel-Erzeugungseinheit **16** auf. Die ID-Berechnungseinheit **12** empfängt eine Stamm-ID, die in der Speichervorrichtung gespeichert ist und berechnet eine Medien-ID (die eine eindeutige Kennung der Speichervorrichtung ist) von der Stamm-ID.

[0037] Die Authentifizierungsinformations-Liefereinheit **14** liefert der Sicherheitsschlüssel-Erzeugungseinheit **16** die Authentifizierungsinformation, die verwendet wird, um den Benutzer **1** zu authentifizieren. Die Authentifizierungsinformation kann der Sicherheitsschlüssel-Erzeugungsvorrichtung **10** direkt durch den Benutzer **1** eingegeben werden. Alternativ kann ein Benutzer-Authentifizierungsserver **2** die Benutzer-Authentifizierungsinformation der Sicherheitsschlüssel-Erzeugungsvorrichtung **10** liefern. Folglich kann die Authentifizierungsinformations-Liefereinheit **14** die Authentifizierungsinformation, die von dem Benutzer **1** oder von dem Benutzer-Authentifizierungsserver **2** empfangen wird, der Sicherheitsschlüssel-Erzeugungseinheit **16** liefern. Die Authentifizierungsinformation kann z. B. eine Benutzer-Authentifizierungsinformation sein, die in einem bestimmten Zugehörigkeitsservice, Benutzeridentifikationsinformation oder persönliche Information verwendet wird. Die persönliche Information stellt eine Information dar, die mit persönlichen Details eines Individuums in Verbindung steht. Beispiele persönlicher Information können eine Adresse, einen Geburtstag, eine Telefonnummer, eine E-Mailaddresse, eine Bewohner-Registrierungsnummer, biometrische Information des Benutzers und einen Code, der einer bestimmten Nummer auf einer durch den Benutzer **1** verwendeten Finanzsicherheitskarte entspricht, aufweisen.

[0038] Die Sicherheitsschlüssel-Erzeugungseinheit **16** erzeugt den Sicherheitsschlüssel unter Verwenden der Medien-ID und der Authentifizierungsinformation. Ein Verwenden der Medien-ID bei der Erzeugung des Speicherschlüssels bedeutet, dass die Medien-ID mindestens einmal eingegeben wird, um den Sicherheitsschlüssel zu erzeugen. Darüber hinaus bedeutet ein Verwenden der Authentifizierungsinformation bei der Erzeugung des Sicherheitsschlüssels, dass die Authentifizierungsinformation mindestens einmal eingegeben wird, um den Sicherheitsschlüssel zu erzeugen.

[0039] Die Sicherheitsschlüssel-Erzeugungseinheit **16** kann den Sicherheitsschlüssel durch Durchführen einer Binär-Operation von der Medien-ID und der Authentifizierungsinformation erzeugen. Beispiel der Binär-Operation können AND-, OR-, NOR-, XOR- und NAND-Operationen sein. Die Sicherheitsschlüssel-Erzeugungseinheit **16** kann den Sicherheitsschlüssel ebenso durch Durchführen eines String-Konkatenations-(STRCAT)-Vorgangs auf der Medien-ID und der Authentifizierungsinformation erzeugen. Bei dem STRCAT-Vorgang können Strings in einer festen Reihenfolge verkettet sein. Folglich können die Medien-ID und die Authentifizierungsinformation in dieser Reihenfolge oder der umgekehrten Reihenfolge verkettet sein.

[0040] Die Authentifizierungs-Schlüsselerzeugungseinheit **16** kann den Sicherheitsschlüssel ausschließlich unter Verwenden der Medien-ID und der Authentifizierungsinformation generieren oder unter Verwenden von einer oder mehrerer variablen oder nicht variablen Datenmengen zusätzlich zu der Medien-ID und die Authentifizierungsinformation erzeugen.

[0041] Der Sicherheitsschlüssel kann ausschließlich erzeugt werden, wenn alle der Benutzer-Authentifizierungsinformation der Medien-ID und eine Sicherheitsschlüssel-Berechnungsformel vorhanden sind. Folglich kann sogar, solange der Sicherheitsschlüssel selbst nicht entwichen ist, wenn die Sicherheitsschlüssel-Berechnungsformel veröffentlicht wird, der Sicherheitsschlüssel nicht erzeugt werden, sofern nicht sowohl die Benutzer-Authentifizierungsinformation und die Medien-ID authentifiziert sind. Die Medien-ID ist ein Wert, der nicht entweicht und kann nur durch einen Vorgang mit der Stamm-ID erhalten werden, die durch die Speichervorrichtung **200** geliefert wird. Darüber hinaus ist die Authentifizierungsinformation ein Wert, der nicht auf einfache Weise entweicht, da es durch den Benutzer **1** verwaltet werden würde, seinen Verlust zu verhindern. Folglich erzeugt die Sicherheitsschlüssel-Erzeugungsvorrichtung **10** gemäß der vorliegenden beispielhaften Ausführungsform den Sicherheitsschlüssel, der zu der Speichervorrichtung **200** wie auch zu dem Benutzer **1** gehört.

[0042] Der Betrieb der ID-Berechnungseinheit **12**, der eine Medien-ID von einer Stamm-ID berechnet, wird nun genauer in Bezug auf die Fig. 2 und Fig. 3 beschrieben werden.

[0043] Sowie oben beschrieben stellt die Stamm-ID unterschiedliche Daten von der Medien-ID dar und wird ebenso verwendet, um mindestens einen Teil der Speichervorrichtung **200** zu authentifizieren. Die Speichervorrichtung **200** kann z. B. einen ersten Teil und einen zweiten Teil aufweisen und eine erste Stamm-ID, die eine erste Kennung des ersten Teils ist, und eine zweite Stamm-ID, die eine Kennung des zweiten Teils ist, der ID-Berechnungseinheit **12** liefern. Die Stamm-ID weist hierbei die erste Stamm-ID und die zweite Stamm-ID auf.

[0044] In Bezug auf die Fig. 2 empfängt die ID-Berechnungseinheit **12** eine verschlüsselte Speicher-ID **264** von der Speichervorrichtung **200** als einen Teil der Stamm-ID. Die verschlüsselte Speicher-ID **264** stellt Daten dar, die durch Verschlüsseln einer Speicher-ID **262** erhalten werden, die eine eindeutige Kennung eines Speicherelements **206**, das in der Speichervorrichtung **200** enthalten ist. Die Speicher-ID **262** kann Daten darstellen, die von einem Anbieter des Speicherelements **206** programmiert worden sind, als das Speicherelement **206** hergestellt worden ist. Die Speicher-ID **262** kann in einem Systembereich gespeichert werden, auf den nicht auf dieselbe Weise zugegriffen werden kann, wie Daten, die in einem Benutzerbereich gespeichert werden. Die Speicher-ID **262** kann, wenn sie in dem Benutzerbereich gespeichert wird, gelöscht, verändert und ausgelesen werden. Die Speicher-ID **262** kann, wenn sie in einem Systembereich gespeichert wird, nicht zugreifbar, nicht gelöscht, verändert oder ausgelesen werden.

[0045] In Bezug auf die Fig. 3 empfängt die ID-Berechnungseinheit **12** eine Steuereinheit-Authentifizierungsinformation von der Speichervorrichtung **200** als einen weiteren Teil der Stamm-ID. Die Sicherheitsschlüssel-Erzeugungsvorrichtung **10** und eine Steuereinheit **208**, die in der Speichervorrichtung **200** enthalten ist, können sich gegenseitig authentifizieren. Die Steuereinheit-Authentifizierungsinformation stellt Daten dar, die die Steuereinheit **208** der Sicherheitsschlüssel-Erzeugungsvorrichtung **10** für diese gegenseitige Authentifizierung liefert.

[0046] Die Fig. 4 ist ein Referenzdiagramm, das ein Verfahren veranschaulicht, bei dem die ID-Berechnungseinheit **12** eine Medien-ID erzeugt.

[0047] Die ID-Berechnungseinheit **12** erhält die Speicher-ID **262** durch Entschlüsseln der verschlüsselten Speicher-ID **264** und erzeugt eine speicherabgeleitete ID aus der Speicher-ID **262**. Zusätzlich erhält die ID-Berechnungseinheit **12** eine Steuereinheit-ID, die eine eindeutige Kennung der Speicher-Steuereinheit **208** ist, von der Steuereinheit-Authentifizierungsinformation.

[0048] Ein erster Entschlüsselungs-Schlüssel, der verwendet wird, um die verschlüsselte Speicher-ID **264** zu entschlüsseln, kann von der Speichersteuereinheit **200** in einer verschlüsselten Form empfangen werden. Zusätzlich kann ein zweiter Entschlüsselungs-Schlüssel, der verwendet wird, um den verschlüsselten ersten Entschlüsselungs-Schlüssel zu entschlüsseln, in einer Speichervorrichtung (nicht dargestellt) gespeichert werden, die in der Sicherheitsschlüssel-Erzeugungsvorrichtung **10** gespeichert wird.

[0049] Folglich kann die ID-Berechnungseinheit **12** den verschlüsselten ersten Entschlüsselungs-Schlüssel von der Speichervorrichtung **200** empfangen und den ersten Entschlüsselungs-Schlüssel durch Entschlüsseln des verschlüsselten ersten Entschlüsselungs-Schlüssel unter Verwenden des zweiten Entschlüsselungs-Schlüssels erhalten. Sodann kann die ID-Berechnungseinheit **12** die verschlüsselte Speicher-ID **264** in die Speicher-ID **262** unter Verwenden des ersten Entschlüsselungs-Schlüssel entschlüsseln.

[0050] Die speicherabgeleitete ID ist eine weitere eindeutige Kennung des Speicherelements **206**. Folglich kann das Speicherelement **206** zwei eindeutige Kennungen aufweisen, z. B. die Speicher-ID **262**, die eine eindeutige Kennung darstellt, die durch den Anbieter des Speicherelements **206** programmiert wird, und die speicherabgeleitete ID, die unter Verwenden der Speicher-ID **262** erzeugt wird. Die Speicher-ID **262** wird in dem Speicherelement **206** gespeichert. Andererseits ist die speicherabgeleitete ID ein Wert, der nicht in dem Speicherelement **206** gespeichert wird, sondern durch die Sicherheitsschlüssel-Erzeugungsvorrichtung **10** erzeugt wird, die mit der Speichervorrichtung **200** verbunden ist.

[0051] Die ID-Berechnungseinheit **12** kann die Steuereinheit-ID unter Verwenden der Steuereinheit-Authentifizierungsinformation verwenden. Die Steuereinheit-Authentifizierungsinformation kann eine Steuereinheit-Authentifizierungs-Zertifikat-ID und einen eindeutigen Kennungs-Code der Steuereinheit **208** aufweisen. Die ID-Berechnungseinheit **12** kann die Steuereinheit-ID unter Verwenden der Steuereinheit-Authentifizierungs-Zertifikat-ID und den eindeutigen Kennungs-Code erzeugen. Die ID-Berechnungseinheit **12** kann z. B. die Steuereinheit-ID durch Durchführen eines String-Konkatenations-Verfahrens auf die Steuereinheit-Authentifizierungs-Zertifikat-ID und den eindeutigen Kennungs-Code erzeugen.

[0052] Die ID-Berechnungseinheit **12** erzeugt die Medien-ID durch Verwenden der speicherabgeleite-

ten ID und der Steuereinheit-ID. Die ID-Berechnungseinheit **12** kann z. B. die Medien-ID durch Eingeben der speicherabgeleiteten ID und der Steuereinheit-ID zu einer Binär-Operation oder einer String-Konkatenation-Operation erzeugen.

[0053] Die Konfiguration und der Betrieb der Sicherheitsschlüssel-Erzeugungsvorrichtung **20** gemäß einer beispielhaften Ausführungsform der vorliegenden Erfindung wird nun in Bezug auf die Fig. 5 bis Fig. 7 beschrieben werden.

[0054] In Bezug auf die Fig. 5 kann die Sicherheitsschlüssel-Erzeugungsvorrichtung **20** gemäß der aktuellen beispielhaften Ausführungsform einen Prozessor **102** und eine Speicherschnittstelle **104** aufweisen. Die Sicherheitsschlüssel-Erzeugungsvorrichtung **20** kann ferner einen Random-Access-Memory (RAM) **106**, der als Systemspeicher des Prozessors **102** verwendet wird und, der vorübergehend Befehle speichert, die durch den Prozessor **102** ausgeführt werden, und eine Eingabeeinheit **108**, die Benutzer-Authentifizierungsinformation empfängt, aufweisen. Der Prozessor **102**, die Speichervorrichtung **104**, der RAM **106** und die Eingabeeinheit **108** können mit einem internen Systembus **110** verbunden sein.

[0055] Sowie in der Fig. 5 dargestellt ist, kann die Speicherschnittstelle **104** Daten übertragen, die zwischen der Sicherheitsschlüssel-Erzeugungsvorrichtung **20** und einer Speichervorrichtung **200** ausgetauscht werden. Die Speicherschnittstelle **104** kann eine Stamm-ID von der Speichervorrichtung **200** empfangen und die empfangene Stamm-ID dem Prozessor **102** über den Systembus **110** liefern.

[0056] Der Prozessor **102** berechnet eine Medien-ID (eine eindeutige Kennung der Speichervorrichtung **200**) aus der empfangenen Stamm-ID. Der Prozessor **102** kann einen Sicherheitsschlüssel unter Verwenden sowohl der Medien-ID und der Authentifizierungsinformation zum Authentifizieren eines Benutzers erzeugen. Die Eingabeeinheit **108** kann die Authentifizierungsinformation von dem Benutzer empfangen und die empfangene Authentifizierungsinformation dem Prozessor **102** liefern. Der Prozessor **102** kann den Sicherheitsschlüssel für unterschiedliche Zwecke verwenden. Der Prozessor **102** kann z. B. den Sicherheitsschlüssel als die Authentifizierungsinformation des Benutzers bei einer Hochsicherheitsstufe oder als ein Entschlüsselungs-Schlüssel für Inhalte, die in der Speichervorrichtung **200** zu speichern sind, verwenden.

[0057] Die Sicherheitsschlüssel-Erzeugungsvorrichtung **20** gemäß der aktuellen beispielhaften Ausführungsform kann eine sichere Ausführungsumgebung unterstützen. Die sichere Ausführungsumgebung ist eine Umgebung, die eine sichere Ausführung von Programmen durch Komponenten wie z. B. einem Prozessor und einem Betriebssystem sicherstellt. Eine sichere Ausführung kann durch Integrität und Vertraulichkeit sichergestellt werden. Im Allgemeinen ist bekannt, dass ein hardwarebasiertes sicheres Ausführungsumgebungsverfahren sicherer ist als ein softwarebasiertes sicheres Ausführungsumgebungsverfahren. Es wird angenommen, dass die Sicherheitsschlüssel-Erzeugungsvorrichtung **20** gemäß der vorliegenden beispielhaften Ausführungsform eine hardwarebasierte sichere Ausführungsumgebung vorsieht.

[0058] In Bezug auf die Fig. 6 und Fig. 7 kann die Sicherheitsschlüssel-Erzeugungsvorrichtung **20** den Prozessor **102** mit zwei Kernen aufweisen, um eine Prozess-Ausführungsumgebung zu teilen. Der Prozessor **102** kann zwei oder mehrere physikalisch getrennte Kerne aufweisen und diese jeweils für einen sicheren Ausführmodus und einen nicht sicheren Ausführmodus verwenden. Alternativ kann der Prozessor **102** einen Kern virtuell in virtuelle Kerne aufteilen und diese jeweils für den sicheren Ausführmodus und den nicht sicheren Ausführmodus verwenden. In den Fig. 6 und Fig. 7 werden Beispiele beschrieben, bei denen der Prozessor **102** zwei virtuelle Kerne **120** und **124** aufweist.

[0059] Die Sicherheitsschlüssel-Erzeugungsvorrichtung **20** kann einem Vorgang, der in dem nicht sicheren Ausführmodus ausgeführt wird, der keine sichere Ausführumgebung von Zugangsdaten vorsieht, einen Zugriff auf Daten verweigern, die durch einen Vorgang erzeugt werden, der in dem sicheren Ausführmodus ausgeführt wird, der eine sichere Ausführungsumgebung vorsieht. Folglich kann ein Datenzugriff in dem sicheren Ausführmodus getrennt von einem Datenzugriff in dem nicht sicheren Modus sein. Der RAM **106** kann z. B. einen ersten Bereich, auf den durch einen Befehl zugegriffen werden kann, der in einem nicht sicheren virtuellen Kern **120** ausgeführt wird, und einen zweiten Bereich aufweisen, auf den nur durch einen Befehl zugegriffen werden kann, der auf dem sicheren virtuellen Kern **124** ausgeführt wird und, der nicht den ersten Bereich überlappt.

[0060] Wenn ein Kern des Prozessors **102** in den sicheren virtuellen Kern **124** zur Verfahrensausführung in den sicheren Ausführmodus und der nicht sichere virtuelle Kern **120** zur Verfahrensausführung in den nicht sicheren Ausführmodus logisch aufgespalten wird und entsprechend betrieben wird, kann jeder Wechsel zwischen dem sicheren Ausführmodus und dem nicht sicheren Ausführmodus durch einen Kontext-Wechselmechanismus durchgeführt werden.

[0061] Als eine ähnliche Technologie, die enthalten sein kann, um die oben beschriebene sichere Ausführungsumgebung zu liefern, kann der Prozessor **102** mindestens eines von TRUSTZONE von ARM, Wire-

less-TPM von INTEL, M-Shield von Texas Instrument und Sicherheitstechnologie von Freescale, SafeXcel TPM von SafeNet, SafeZone von SafeNet, eine Sicherheitsplattform von Discretix und SecureMSM von Qualcomm verwenden.

[0062] Ein Authentifizierungsverfahren kann erforderlich sein, um einen Verfahren in dem sicheren Ausführmodus des Prozessors **102** auszuführen. Das Authentifizierungsverfahren kann ein Verfahren mit einem Empfangen von Benutzer-Authentifizierungsinformation und einem Verifizieren sein, ob die empfangene Authentifizierungsinformation identisch mit der zuvor gespeicherten Authentifizierungsinformation ist. Wenn verifiziert ist, dass die empfangene Authentifizierungsinformation identisch mit der zuvor gespeicherten Authentifizierungsinformation, kann ein Interruptsignal zum Wechseln des Betriebsmodus des Prozessors **102** von dem nicht sicheren Ausführmodus zu dem sicheren Ausführmodus erzeugt werden. Sodann kann der Prozessor **102** als Antwort auf das Interruptsignal in den sicheren Ausführmodus wechseln. In Bezug auf die Fig. 6 führt der Prozessor **102**, der in dem nicht sicheren Modus arbeitet, eine Benutzer-Authentifizierung durch, um den sicheren Ausführmodus zu wechseln. Für die Benutzer-Authentifizierung empfängt der Prozessor **102** Benutzer-Authentifizierung von der Eingabeeinheit **108**. Wenn ein Benutzer erfolgreich unter Verwenden der Benutzer-Authentifizierungsinformation authentifiziert wird, wechselt der Prozessor **102** den virtuellen Kern (z. B. ein Umschalten von dem nicht sicheren virtuellen Kern **120** zu dem sicheren virtuellen Kern **124**) über ein Überwachungs-verfahren **122**.

[0063] Folglich empfängt, wenn er sich in dem nicht sicheren Ausführmodus befindet, der Prozessor **102** der Sicherheitsschlüssel-Erzeugungsvorrichtung **20** gemäß der aktuellen beispielhaften Ausführungsform Benutzer-Authentifizierungsinformation zum Wechseln seines Ausführungs-Modus. Folglich wechselt der Prozessor **102** seinen Ausführmodus zu dem sicheren Ausführmodus und erzeugt einen Sicherheitsschlüssel in dem sicheren Ausführmodus. Da die Sicherheitsschlüssel-Erzeugungsvorrichtung **20** gemäß der vorlegenden beispielhaften Ausführungsform einen Sicherheitsschlüssel in dem sicheren Ausführmodus erzeugt, kann der Verlust von Benutzer-Authentifizierungsinformation, einer Stamm-ID, einer Speicher-ID, einer Medien-ID etc. vermieden werden.

[0064] Der Prozessor **102** der Sicherheitsschlüssel-Erzeugungsvorrichtung **20** gemäß der vorliegenden beispielhaften Ausführungsform kann ebenso Benutzer-Authentifizierungsinformation und eine Stamm-ID nach dem Wechseln in den sicheren Ausführmodus empfangen und einen Sicherheitsschlüssel in dem sicheren Ausführmodus erzeugen. In Bezug auf die Fig. 7 empfängt die Sicherheitsschlüssel-Erzeugungsvorrichtung **20** gemäß der vorliegenden beispielhaften Ausführungsform Benutzer-Authentifizierungsinformation und eine Stamm-ID nach einem Wechseln in den sicheren Ausführmodus und erzeugt daraus einen Sicherheitsschlüssel. Der RAM **106**, der in der Sicherheitsschlüssel-Erzeugungsvorrichtung **20** gemäß der vorliegenden beispielhaften Ausführungsform enthalten ist, kann einen Sicherheitsbereich aufweisen, der nur zugreifbar ist, wenn der Prozessor **102** in dem sicheren Ausführmodus arbeitet, und der Prozessor **102** kann die Authentifizierungsinformation, die Stamm-ID, eine Medien-ID und den Sicherheitsschlüssel in dem sicheren Bereich speichern.

[0065] Gemäß der vorliegenden beispielhaften Ausführungsform arbeitet die Sicherheitsschlüssel-Erzeugungsvorrichtung **20** bereits in dem sicheren Ausführmodus zu einer Zeit, wenn sie Benutzer-Authentifizierungsinformation empfängt. Folglich kann der Verlust von Benutzer-Authentifizierungsinformation, einer Stamm-ID, einer Speicher-ID, einer Medien-ID, etc. verhindert werden.

[0066] Die Konfiguration und der Betrieb der Sicherheitsschlüssel-Erzeugungsvorrichtung **30** gemäß einer weiteren beispielhaften Ausführungsform der vorliegenden Erfindung wird nun in Bezug auf die Fig. 8 bis Fig. 11 beschrieben werden.

[0067] Die Fig. 8 veranschaulicht die Konfiguration der Sicherheitsschlüssel-Erzeugungsvorrichtung **30** gemäß einer beispielhaften Ausführungsform der vorliegenden Erfindung. In Bezug auf die Fig. 8 weist die Sicherheitsschlüssel-Erzeugungsvorrichtung **30** gemäß der vorliegenden beispielhaften Ausführungsform einen System-On-Chip (SoC) **302** und eine Speicherschnittstelle **104**, die mit dem SoC **302** verbunden ist, auf. Die Speicherschnittstelle **104** gemäß der vorliegenden beispielhaften Ausführungsform empfängt eine Stamm-ID von einer Speichervorrichtung **200**, wenn sie mit der Speichervorrichtung **200** verbunden ist, und liefert dem SoC **302** eine empfangene Stamm-ID.

[0068] Der SoC **302** entspricht der Umsetzung eines Systems mit unterschiedlichen Funktionen auf einem einzelnen Chip. Der SoC **302** gemäß der vorliegenden beispielhaften Ausführungsform weist eine Peripherielogik **320**, die eine Medien-ID (z. B. eine eindeutige Kennung der Speichervorrichtung **200**) aus der Stamm-ID berechnet, und erzeugt einen Sicherheitsschlüssel unter Verwenden sowohl der Medien-ID als auch der Authentifizierungsinformation zum Authentifizieren eines Benutzers.

[0069] Der SoC **302** kann ferner einen Kern **322** (Prozessor) aufweisen, der Befehle ausführt. Der Kern **322** kann Befehle lesen, die in einem RAM (nicht dargestellt) gespeichert sind, der in der Sicher-

heitsschlüssel-Erzeugungsvorrichtung **30** enthalten ist, und führt die Lesebefehle aus (z. B. Lesebefehle zum Lesen der Stamm-ID von der Speichervorrichtung **200**). Der RAM kann innerhalb oder außerhalb des SoC **302** vorgesehen sein. Der Kern **322** steuert Eingabe-/Ausgabe-bezogene Betriebsabläufe der Sicherheitsschlüssel-Erzeugungsvorrichtung **30**. Der Kern **322** empfängt z. B. Benutzer-Authentifizierungsinformation, die durch eine Eingabeeinheit **108** von dem Benutzer eingegeben wird. Der Kern **322** liefert die Benutzer-Authentifizierungsinformation zu der Peripherielogik **320**.

[0070] Die Peripherielogik **320** empfängt die Benutzer-Authentifizierungsinformation von dem Kern **322**, kann jedoch ebenso die Stamm-ID direkt von der Speicherschnittstelle **104** ohne Verwenden des Kerns **322** empfangen. Zu diesem Zweck kann in Bezug auf die Fig. 9 die Peripherielogik **320** auf einem Datenweg **325** zwischen der Speicherschnittstelle **104** und den Kern **322** verbunden sein. Die Peripherielogik **320** kann die Stamm-ID von der Speichervorrichtung **200** durch den Datenpfad **320** ohne ein Senden der Stamm-ID an den Kern **322** empfangen. Da der Kern **322** gegenüber Angriffsversuchen verletzlich ist und folglich keine Betriebsabläufe unter Verwenden der Stamm-ID durchführt, sendet die Peripherielogik **320** die Stamm-ID nicht dem Kern **322**.

[0071] Folglich arbeitet die Peripherielogik **320** unabhängig von dem Kern **322** bei der Erzeugung eines Sicherheitsschlüssels. Die Peripherielogik **320** ist für alle Betriebsabläufe verantwortlich, die mit der Erzeugung des Sicherheitsschlüssels in Verbindung stehen, außer für das Empfangen von Benutzer-Authentifizierungsinformation von dem Kern **322**. Zusätzlich fährt die Peripherielogik **320** keine Programme durch, die in dem RAM gespeichert sind. Die Peripherielogik **320** führt anstelle nur Sicherheitsschlüssel-Erzeugungsprogramme aus, die in einem nicht-flüchtigen Speicher (z. B. einem Read-Only-Speicher (ROM)) enthalten sind.

[0072] Die Peripherielogik **320** kann den erzeugten Sicherheitsschlüssel in einem Register **320**, das in dem SoC **302** enthalten ist, speichern.

[0073] Angriffsprogramme, die beabsichtigen einen Sicherheitsschlüssel, eine Medien-ID, eine Speicher-ID, etc. zu stehlen, werden im Allgemeinen auf dem Kern **322** ausgeführt werden. Deshalb kann, da die Peripherielogik **320** unabhängig von dem Kern **322** für alle Betriebsabläufe bezogen auf die Erzeugung des Sicherheitsschlüssels verantwortlich ist, die Sicherheitsschlüssel-Erzeugungsvorrichtung **30** gemäß der vorliegenden beispielhaften Ausführungsform effektiv den Verlust (z. B. Dieb) von Daten bezogen auf die Erzeugung des Sicherheitsschlüssel effektiv verhindern.

[0074] In Bezug auf die Fig. 10 kann die Sicherheitsschlüssel-Erzeugungsvorrichtung **30** gemäß der vorliegenden beispielhaften Ausführungsform Inhalte unter Verwenden des Sicherheitsschlüssels verschlüsseln und die verschlüsselten Inhalte in der Speichervorrichtung **200** speichern, die mit der Sicherheitsschlüssel-Erzeugungsvorrichtung **30** verbunden ist und mit der Stamm-ID geliefert wird, um eine Medien-ID zu erzeugen, die verwendet wird, um den Sicherheitsschlüssel zu erzeugen. Um die Sicherheit zu erhöhen, kann die Peripherielogik **320** ebenso für die Verschlüsselung der Inhalte, die in der Speichervorrichtung **200** zu speichern sind, verantwortlich sein. Die Peripherielogik **320** kann ebenso für das Entschlüsseln von verschlüsselten Inhalten, die von der Speichervorrichtung **200** wiederherzustellen sind, ebenso verantwortlich sein. Zu diesem Zweck kann die Peripherielogik **320** eine Verschlüsselungs-/Entschlüsselungs-Vorrichtung **321** aufweisen. Die Verschlüsselungs-/Entschlüsselungs-Vorrichtung **321** kann den Sicherheitsschlüssel, der in dem Register **324** gespeichert ist, als einen Verschlüsselungs-/Entschlüsselungs-Schlüssel verwenden.

[0075] In Bezug auf die Fig. 11 kann die Sicherheitsschlüssel-Erzeugungsvorrichtung **30**, die mit der Speichervorrichtung **200** verbunden ist, verschlüsselte Inhalte, die in der Speichervorrichtung **200** gespeichert sind, entschlüsseln. Um die verschlüsselten Inhalte zu entschlüsseln, sollte die Sicherheitsschlüssel-Erzeugungsvorrichtung **30** einen Entschlüsselungs-Schlüssel des verschlüsselten Inhalts der Speichervorrichtung **200** erzeugen. Insbesondere kann die Sicherheitsschlüssel-Erzeugungsvorrichtung **30** eine Stamm-ID von der Speichervorrichtung **200** empfangen, Authentifizierungsinformation von einem Benutzer der Sicherheitsschlüssel-Erzeugungsvorrichtung **30** empfangen, eine Medien-ID von der Speichervorrichtung **200** aus der Stamm-ID erzeugen und sodann den Entschlüsselungs-Schlüssel des verschlüsselten Inhalts unter Verwenden der Medien-ID und der Authentifizierungsinformation erzeugen.

[0076] Jede der oben beschriebenen Sicherheitsschlüssel-Erzeugungsvorrichtungen **10**, **20** und **30** kann auf einem Computer, Ultra-Mobile-PCs (UMPCs), Arbeitsstationen, Net-Books, Persönliche-Digitale-Assistenten (PDAs), einem tragbare Computer, Web-Tablets, einem Schnurlostelefon, Mobiltelefonen, Smart-Phones, e-Books, einem tragbare Multimediaspieler (PMPs), tragbaren Spielvorrichtungen, Navigationsvorrichtungen, Black-Boxes, Digitalkameras, dreidimensionalen Fernsehern, einem digitalen Audio-Aufnahmegeräte, einem digitalen Audio-Spieler, digitalen Bildaufnahmegeräte, einem digitalen Fotoabspieler, digitalen Videoaufnahmegeräte, digitalen Videoabspielgeräte, Vorrichtungen, die fähig sind, Information in Drahtlosumgebungen zu

übertragen/zu empfangen, eines oder mehrere elektronische Vorrichtungen, die in Heim-Netzwerken eingesetzt werden, eine von unterschiedlichen elektronischen Vorrichtungen, die ein Computernetzwerk bilden, eine von unterschiedlichen elektronischen Vorrichtungen, die ein Telematik-Netzwerk bilden, eine Radio-Frequenz-Identifikations-(RFID)-Vorrichtung, oder eine von unterschiedlichen Komponenten, die ein Computersystem ausmachen, sein.

[0077] Eine Speichervorrichtung **40** gemäß einer beispielhaften Ausführungsform der vorliegenden Erfindung wird nun in Bezug auf die Fig. 12 bis Fig. 14 beschrieben werden. Die Speichervorrichtung **40** gemäß der vorliegenden beispielhaften Ausführungsform weist eine Verschlüsselungsfunktion auf. Folglich, wenn die Speichervorrichtung **40** mit einer Host-Vorrichtung verbunden ist und von der Host-Vorrichtung zu speichernde Daten empfangt, speichert sie die empfangenen Daten, wenn sie empfangen werden, nicht, sondern verschlüsselt die empfangenen Daten und speichert dann die verschlüsselten Daten.

[0078] Die Speichervorrichtung **40** gemäß der vorliegenden beispielhaften Ausführungsform erzeugt einen Verschlüsselungs-Schlüssel, der verwendet wird, um die empfangenen Daten zu verschlüsseln, unter Verwenden von Benutzer-Authentifizierungsinformation von der Host-Vorrichtung und einer speicherabgeleiteten ID von einem Speicherelement **206**, das in der Speichervorrichtung **40** enthalten ist.

[0079] Die Konfiguration und der Betrieb der Speichervorrichtung **40** gemäß der vorliegenden beispielhaften Ausführungsform wird nun in Bezug auf die Fig. 12 beschrieben werden. In Bezug auf die Fig. 12 kann die Speichervorrichtung **40** gemäß der vorliegenden beispielhaften Ausführungsform das Speicherelement **206**, eine Host-Schnittstelle **210**, eine speicherabgeleitete ID-Berechnungseinheit **212**, eine Sicherheitsschlüssel-Erzeugungseinheit **214** und eine Verschlüsselungseinheit **216** aufweisen.

[0080] Die Host-Schnittstelle **210** empfängt von der Host-Vorrichtung die Authentifizierungsinformation zum Authentifizieren eines Benutzers und liefert die Authentifizierungsinformation der Sicherheitsschlüssel-Erzeugungsvorrichtung **210**. Zusätzlich empfängt die Host-Schnittstelle **210** Inhalte (z. B. Daten) von der Host-Vorrichtung und liefert die Inhalte der Verschlüsselungseinheit **216**.

[0081] Das Speicherelement **206** speichert eine Speicher-ID **262** und eine verschlüsselte Speicher-ID **264**, die durch Verschlüsseln der Speicher-ID **262** erhalten wird. Ein Speicherbereich des Speicherelements **206** kann in einen Benutzerbereich und einen Systembereich geteilt werden. Der Systembereich ist nicht in derselben Weise zugreifbar wie es der Benutzerbereich ist. Die Speicher-ID **262** und die verschlüsselte Speicher-ID **264** werden bevorzugt in dem Systembereich gespeichert.

[0082] Das Speicherelement **206** kann ein nichtflüchtiger Speicher sein und kann ein Chip oder ein Gehäuse sein, das einen NAND-FLASH-Speicher, einen NOR-FLASH-Speicher, einen Phase-Change-Random-Access-Memory (PRAM), einen Magnetic-Random-Access-Memory (MRAM), oder einen Resistive-Random-Access-Memory (RRAM) als ein Speichermedium verwendet. Das Speicherelement **206** kann in ein Gehäuse wie zum Beispiel ein Package-On-Package (PoP), Ball-Grid-Arrays (BGAs), Chip-Scale-Packages (CSPs), Plastic-Leaded-Chip-Carrier (PLCC), Plastic-Dual-In-Line-Package (PDIP), Die-In-Waffle-Pack, Die-In-Wafer-Form, Chip-On-Board (COB), Ceramic-Dual-In-Line-Package (CERDIP), Plastic-Metric-Quad-Flat-Pack (MQFP), Thin-Quad-Flat-Pack (TQFP), Small-Outline-Integrated-Circuit (SOIC), Shrink-Small-Outline-Package (SSOP), Thin-Small-Outline-Package (TSOP), Thin-Quad-Flat-Pack (TQFP), System-In-Package (SEP), Multi-Chip-Package (MCP), Wafer-Level-Fabricated-Package (WFP) und Wafer-Level-Processed-Stack-Package (WSP) montiert werden.

[0083] Die speicherabgeleitete ID-Berechnungseinheit **212** liest die verschlüsselte Speicher-ID **264** von dem Speicherelement **206**, erhält die Speicher-ID **262** durch Entschlüsseln der verschlüsselten Speicher-ID **264** und erzeugt eine speicherabgeleitete ID, die eine weitere eindeutige Kennung des Speicherelements **206** ist, unter Verwenden der Speicher-ID **262**.

[0084] Die Sicherheitsschlüssel-Erzeugungseinheit **214** erzeugt einen Sicherheitsschlüssel unter Verwenden sowohl der Authentifizierungsinformation und der speicherabgeleiteten ID. Die Sicherheitsschlüssel-Erzeugungseinheit **214** erzeugt den Sicherheitsschlüssel in der gleichen Weise, wie die Sicherheitsschlüssel-Erzeugungseinheit **16** der Sicherheitsschlüsselerzeugungsvorrichtung **10** von den Fig. 1 bis Fig. 4.

[0085] Die Verschlüsselungseinheit **216** verschlüsselt den Inhalt (Daten) unter Verwenden des Sicherheitsschlüssels und speichert den verschlüsselten Inhalt in dem Speicherelement **206**.

[0086] Wenn sie die Inhalte, die von der Host-Vorrichtung empfangen werden, verschlüsselt und die verschlüsselten Inhalte speichert, verwendet die Speichervorrichtung **40** gemäß der vorliegenden beispielhaften Ausführungsform einen Verschlüsselungs-Schlüssel, der durch Reflektieren einer eindeutigen Kennung des in der Speichervorrichtung **40** enthaltenen Speicherelements **206** erzeugt wird. Folglich wird vermieden, dass sie entschlüsselt werden, sogar wenn die verschlüsselten Inhalte in der Spei-

chervorrichtung **40** illegal kopiert werden. Dies beruht darauf, dass eine Speichervorrichtung, die die illegal kopierten verschlüsselten Inhalte speichert, nicht dieselbe Medien-ID wie eine Medien-ID in der Speichervorrichtung **40** aufweist, die die ursprünglich verschlüsselten Inhalte speichert.

[0087] Der Verschlüsselungs-Schlüssel, der in der Speichervorrichtung **40** gemäß der vorliegenden beispielhaften Ausführungsform erzeugt wird, wird ferner durch Reflektieren von Benutzer-Authentifizierungsinformation zum Authentifizieren eines Benutzers erzeugt. Folglich können Inhalte, die in der Speichervorrichtung **40** gespeichert werden, nicht entschlüsselt werden, wenn die Benutzer-Authentifizierungsinformation nicht vorhanden ist.

[0088] Die Speichervorrichtung **40** gemäß der vorliegenden beispielhaften Ausführungsform kann als eine Speichervorrichtung verwendet werden, die in einem Cloud-Server eines Cloud-Computing-Service enthalten ist. Folglich werden Inhalte oder Daten, die durch einen Benutzer des Cloud-Computing-Service hochgeladen werden, unter Verwendung sowohl von Authentifizierungsinformation des Benutzers und der Medien-ID der Speichervorrichtung **40** verschlüsselt und sodann entsprechend gespeichert. In diesem Fall, sogar, wenn die verschlüsselten Inhalte oder Daten gehackt oder entweichen (z. B. gestohlen) bei dem Server-Ende, können sie nicht entschlüsselt werden, ohne den entwichenen Inhalt oder die Daten in der Speichervorrichtung **40** (welche die Speichervorrichtung darstellt, die ursprünglich die entwichenen Inhalte oder Daten speichert) und wenn nicht die Authentifizierungsinformation des Benutzers verfügbar ist. Folglich, wenn die Speichervorrichtung **40** gemäß der vorliegenden beispielhaften Ausführungsform in dem Cloud-Server des Cloud-Computing-Service enthalten ist und als ein Speichermedium von hochgeladenen Inhalten oder Daten verwendet wird, kann die Wahrscheinlichkeit reduziert werden, dass Inhalte oder Daten, die durch einen Benutzer hochgeladen werden, entweichen werden.

[0089] Die Speichervorrichtung **40** gemäß der vorliegenden beispielhaften Ausführungsform kann einen Secure-Digital-(SD)-Card-Standard der SD-Vereinigung erfüllen. In diesem Fall kann die Host-Schnittstelle **210** die empfangene Authentifizierungsinformation der Sicherheitsschlüssel-Erzeugungseinheit **214** als einen Parameter eines Befehls gemäß dem SD-Kartenstandard liefern.

[0090] Die Speichervorrichtung **40** gemäß der vorliegenden beispielhaften Ausführungsform kann einen Solid-State-Drive-(SSD)- oder Hard-Disk-Drive(HDD)-Standard (die einen Flash-Speicher enthalten) entsprechen. In diesem Fall kann die Host-Schnittstelle **210** eine physikalische Schnittstelle sein, die Kommunikationsbefehle von Massenspeichervorrichtungen unterstützt, wie zum Beispiel Advanced-Technology-Attachment (ATA), Serial-ATA (SATA), Small-Computer-Small-Interface (SCSI), PCI-Express (PCI-E) oder Universal-Serial-Bus (USB).

[0091] In Bezug auf die Fig. 13 kann die Speichervorrichtung **40** gemäß der vorliegenden beispielhaften Ausführungsform den Sicherheitsschlüssel durch zusätzliches Verwenden einer Zufallszahl erzeugen. Die Sicherheitsschlüssel-Erzeugungseinheit **214** kann folglich den Sicherheitsschlüssel unter Verwenden aller der Zufallszahl, der Authentifizierungsinformation und der Medien-ID erzeugen. Die Speichervorrichtung **40** gemäß der vorliegenden beispielhaften Ausführungsform kann ferner einen Zufallszahlengenerator **214** aufweisen, der die Zufallszahl erzeugt und die erzeugte Zufallszahl der Sicherheitsschlüssel-Erzeugungseinheit **214** liefert. Die Speichereinheit **40** gemäß der vorliegenden beispielhaften Ausführungsform kann gemäß Opal-Security-Subsystem-Class-(OPAL SSC)-Spezifikationen der Trusted-Computing-Group arbeiten.

[0092] Ein Speichersystem **1000** gemäß einer beispielhaften Ausführungsform der vorliegenden Erfindung wird nun in Bezug auf die Fig. 14 beschrieben werden.

[0093] In Bezug auf die Fig. 14 weist das Speichersystem **1000** eine nichtflüchtige Speichervorrichtung **1100** und eine Steuereinheit **1200** auf. Die Speichervorrichtung **200**, die oben in Bezug zu den Fig. 1, Fig. 2 und Fig. 3 beschrieben wird, kann derart konfiguriert sein, dass sie ein Speichersystem **1000** (**1100** und **1200**) von der Fig. 14 realisiert.

[0094] Die nichtflüchtige Speichervorrichtung **1100** kann eines oder mehrere Speicherelemente **206** so wie oben beschrieben aufweisen.

[0095] Die Steuereinheit **1200** ist mit einer Host-Vorrichtung und der nichtflüchtigen Speichervorrichtung **1100** verbunden. Die Steuereinheit **1200** ist derart konfiguriert, dass sie auf die nichtflüchtige Speichervorrichtung **1100** als Antwort auf eine Anfrage der Host-Vorrichtung zugreift. Die Steuereinheit **1200** kann zum Beispiel derart konfiguriert sein, dass sie Lese-/Schreibe-/Lösch-/Hintergrund-Vorgänge der nichtflüchtigen Speichervorrichtung **1100** steuert. Die Steuereinheit **1200** kann derart konfiguriert sein, dass sie eine Schnittstelle zwischen der nichtflüchtigen Speichervorrichtung **1100** und der Host-Vorrichtung liefert. Die Steuereinheit **1200** kann derart konfiguriert sein, dass sie eine Firmware zum Steuern der nichtflüchtigen Speichervorrichtung **1100** antreibt.

[0096] Die Steuereinheit **1200** weist ferner wohlbekannte Komponenten, wie zum Beispiel einen

RRM, eine Verarbeitungseinheit, eine Host-Schnittstelle und eine Speicherschnittstelle auf. Der RAM wird mindestens verwendet als einer von einem Arbeitsspeicher der Verarbeitungseinheit, einem Cash-Speicher zwischen der nichtflüchtigen Speichervorrichtung **1100** und der Host-Vorrichtung und einem Pufferspeicher zwischen der nichtflüchtigen Speichervorrichtung **1100** und der Host-Vorrichtung. Die Verarbeitungseinheit steuert den Gesamtbetrieb der Steuereinheit **1200**.

[0097] Die Host-Schnittstelle weist ein Protokoll zum Datenaustausch zwischen der Host-Vorrichtung und der Steuereinheit **1200** auf. Die Steuereinheit **1200** kann zum Beispiel derart konfiguriert sein, dass sie mit einer externen Vorrichtung (zum Beispiel die Host-Vorrichtung) unter Verwenden mindestens eines von unterschiedlichen Schnittstellenprotokollen wie zum Beispiel USB-Protokoll, einem Multimediakarte-(MMC)-Protokoll, einem PCI-Protokoll, einem PCI-E-Protokoll, einem ATA-Protokoll, einem Seriell-ATA-Protokoll, einem Parallel-ATA-Protokoll, einem SCSI-Protokoll, einem Enhanced-Small-Disc-Interface-(ESDI)-Protokoll und einem Integrated-Drive-Electronics-(IDE)-Protokoll kommuniziert. Die Speicherschnittstelle verbindet sich mit der nichtflüchtigen Speichervorrichtung **1100**. Die Speicherschnittstelle weist zum Beispiel eine NAND-Flash-Schnittstelle oder eine NOR-Flash-Schnittstelle auf.

[0098] Das Speichersystem **1000** kann ferner einen Fehlerkorrekturblock (nicht dargestellt) aufweisen. Der Fehlerkorrekturblock kann derart konfiguriert sein, dass er einen Fehler in Daten, die von einer nichtflüchtigen Speichervorrichtung **1100** ausgelesen werden, durch Verwenden eines Fehlerkorrekturcodes (ECC) detektiert und korrigiert. Der Fehlerkorrekturblock kann als eine Komponente der Steuereinheit **1200** geliefert werden. Der Fehlerkorrekturblock kann alternativ als eine Komponente der nichtflüchtigen Speichervorrichtung **1100** geliefert werden.

[0099] Die Steuereinheit **1200** und die nichtflüchtige Steuervorrichtung **1100** können in einer Halbleitervorrichtung integriert sein. Die Steuereinheit **1200** und die nichtflüchtige Speichervorrichtung **1100** können zum Beispiel in eine Halbleitervorrichtung integriert sein, um eine Speicherkarte zu bilden. Die Steuereinheit **1200** und die nichtflüchtige Speichervorrichtung **1100** können zum Beispiel in eine Halbleitervorrichtung integriert werden, um eine PC-Karte (z. B. Personal-Computer-Memory-Card-International-Association (PCMCIA)), eine Compact-Flash-Karte (CF), eine Smart-Media-Karte (SM/SMC), einen Speicherstick, eine Multimediakarte (z. B. MMC, RS-MMC und MMCmicro), eine SD-Karte (zum Beispiel SD, miniSD, microSD und SDHC) oder einen Universal-Flashspeicher (UFS) zu bilden.

[0100] Die Steuereinheit **1200** und die nichtflüchtige Speichervorrichtung **1100** können bei einem weiteren Beispiel in einer Halbleitervorrichtung integriert sein, um eine SSD zu bilden. Die SSD weist ein Speicherelement auf, das Daten in einem Halbleiterspeicher speichert. Wenn das Speichersystem **1000** als ein SSD verwendet wird, kann die Betriebsgeschwindigkeit der Host-Vorrichtung, die mit dem Speichersystem **1000** verbunden ist, im Vergleich zu Festplattenlaufwerken (HDD) bedeutend erhöht werden.

[0101] Jede der Komponenten, die oben in Bezug auf die Fig. 1 bis Fig. 14 beschrieben werden, bezeichnet eine Software- oder Hardware-Komponente wie zum Beispiel einen Field-Programmable-Gate-Array (FPGA) oder Application-Specific-Integrated-Circuit (ASIC), ist jedoch nicht limitiert darauf. Eine Komponente kann vorteilhaft derart konfiguriert sein, dass sie auf dem adressierbaren Speichermedium gelegen ist und derart konfiguriert sein, dass sie einen oder mehrere Prozesse ausführt. Die Funktionalität, die in den Komponenten geliefert wird, kann folglich in weniger Komponenten oder ferner aufgeteilt in zusätzliche Komponenten kombiniert werden.

[0102] Ein Sicherheitsschlüssel-Erzeugungsverfahren gemäß einer beispielhaften Ausführungsform der vorliegenden Erfindung wird in Bezug auf die Fig. 15 beschrieben werden.

[0103] Das Sicherheitsschlüssel-Erzeugungsverfahren gemäß der vorliegenden beispielhaften Ausführungsform kann als ein Verfahren zusammengefasst werden, in dem eine Host-Vorrichtung eine Medien-ID von einer Speichervorrichtung erhält und einen Sicherheitsschlüssel unter Verwenden sowohl der Medien-ID und Benutzer-Authentifizierungsinformation erzeugt.

[0104] In Bezug auf die Fig. 15 speichert eine Speichervorrichtung eine Stamm-ID (Schritt S100). Die Stamm-ID kann in einem Speicherelement der Speichervorrichtung gespeichert werden.

[0105] Eine Host-Vorrichtung empfängt die Stamm-ID (Schritt S102) und berechnet eine Medien-ID, die eine eindeutige Kennung der Speichervorrichtung ist, von der Stamm-ID (Schritt S104). Die Stamm-ID weist eine erste Stamm-ID und eine zweite Stamm-ID auf. Eine zweite Kennung, in die die zweite Stamm-ID umgewandelt wird, kann mit der ersten Stamm-ID kombiniert werden, um die Medien-ID herzustellen. Die Stamm-ID kann alternativ ihrerseits die Medien-ID sein. Ein Verfahren zum Berechnen der Medien-ID wird später in Bezug auf die Fig. 19 bis Fig. 22 genauer beschrieben werden.

[0106] Die Host-Vorrichtung empfängt Benutzer-Authentifizierungsinformation. Die Benutzer-Authentifizierungsinformation kann durch einen Benutzer an ei-

ne Eingabeeinheit (nicht dargestellt), die in der Host-Vorrichtung enthalten ist, eingegeben werden oder kann durch den Benutzer an einem Eingabegerät (nicht dargestellt) anders als die Host-Vorrichtung eingegeben werden und der Host-Vorrichtung sodann geliefert werden.

[0107] Die Fig. 16 ist ein Ablaufdiagramm, das ein Verfahren zum Erzeugen eines Sicherheitsschlüssels und zum Verschlüsseln von Inhalten unter Verwenden des Sicherheitsschlüssels gemäß einer beispielhaften Ausführungsform der vorliegenden Erfindung veranschaulicht. In der Fig. 16 sind Schritte S100, S102, S104 und S106 zum Erzeugen eines Sicherheitsschlüssels identisch mit denen, die in der Fig. 15 dargestellt sind.

[0108] Eine Host-Vorrichtung gemäß der vorliegenden beispielhaften Ausführungsform erzeugt verschlüsselte Inhalte durch Verschlüsseln von Inhalt unter Verwendung des Sicherheitsschlüssels oder wandelt den Inhalt in den verschlüsselten Inhalt um (Schritt S108). Ein Verschlüsselungsalgorithmus und ein Verschlüsselungs-Schlüssel, der bei dem Verschlüsseln des Inhalts verwendet wird, sind nicht auf einen bestimmten Verschlüsselungsalgorithmus und einen bestimmten Verschlüsselungs-Schlüssel beschränkt. Ein symmetrischer Schlüssel-Verschlüsselungsalgorithmus kann jedoch verwendet werden, der denselben Schlüssel zum Verschlüsseln und Entschlüsseln verwendet, z. B. ein Advanced-Encryption-Standard-(AES)-Verschlüsselungsalgorithmus.

[0109] Die verschlüsselten Inhalte werden einer Speichervorrichtung (Schritt S110) geliefert und die Speichervorrichtung speichert die verschlüsselten Inhalte (Schritt S112). So wie in der Fig. 16 dargestellt kann die Host-Vorrichtung die verschlüsselten Inhalte in der Speichervorrichtung speichern, die eine Stamm-ID geliefert hat. Folglich braucht sich die Speichervorrichtung, die verschlüsselte Inhalte speichert, nicht von der Speichervorrichtung zu unterscheiden, die eine Stamm-ID geliefert hat.

[0110] In Bezug auf Fig. 16 liefert die Host-Vorrichtung weder einen Sicherheitsschlüssel der Speichervorrichtung noch weist sie den Sicherheitsschlüssel in dem verschlüsselten Inhalt auf. Folglich, um einen Entschlüsselungs-Schlüssel der verschlüsselten Inhalte zu erhalten, sollte eine Medien-ID der Speichervorrichtung, die die verschlüsselten Inhalte speichert, erhalten werden und der Entschlüsselungs-Schlüssel sollte von der Medien-ID erzeugt werden. Der Entschlüsselungs-Schlüssel des verschlüsselten Inhalts kann nicht direkt von der Speichervorrichtung erhalten werden. Folglich können sie nicht gemäß des Inhalt-Verschlüsselungsverfahrens von der Fig. 16 entschlüsselt werden, sogar wenn, die verschlüsselten Inhalte legal auf weitere Speichervorrichtung kopiert werden.

[0111] Ein Verfahren, bei dem die Host-Vorrichtung eine Medien-ID berechnet, wird detaillierter in Bezug auf die Fig. 17 bis Fig. 20 jetzt beschrieben werden.

[0112] Die Fig. 17 veranschaulicht ein Verfahren zum Berechnen einer Medien-ID in dem Fall, bei dem eine Speichervorrichtung einen ersten Teil und einen zweiten Teil aufweist und eine erste Stamm-ID zum Authentifizieren des ersten Teils und eine zweite Stamm-ID zum Authentifizieren des zweiten Teils aufweist. Jeder des ersten Teils und des zweiten Teils kennzeichnet ein Element oder Modul, das in der Speichervorrichtung enthalten ist und kann ebenso eine Elementgruppe oder Modulgruppe sein, die eine bestimmte Funktion durchführt. Der zweite Teil kann z. B. ein Element, ein Modul, eine Elementgruppe oder eine Modulgruppe sein, die eine Datenspeicherfunktion durchführt und der erste Teil kann ein Element, ein Modul, eine Elementgruppe oder eine Modulgruppe zum Durchführen einer Kontrollfunktion sein.

[0113] In Bezug auf Fig. 17 weist die Host-Vorrichtung die erste Stamm-ID und die zweite Stamm-ID auf (Schritt S114).

[0114] Die Host-Vorrichtung berechnet eine Medien-ID unter Verwenden mindestens einer von der ersten Stamm-ID und der zweiten Stamm-ID (Schritt S116). Wenn die Medien-ID unter Verwenden der ersten Stamm-ID nur berechnet wird, kann es spezifisch für den ersten Teil sein. Zusätzlich, wenn die Medien-ID nur unter Verwenden der zweiten Stamm-ID berechnet wird, kann es spezifisch für den zweiten Teil sein. Jedoch kann, wenn die Medien-ID unter Verwenden sowohl der ersten Stamm-ID und der zweiten Stamm-ID berechnet wird, es spezifisch für sowohl den ersten Teil als auch den zweiten Teil sein.

[0115] In Bezug auf Fig. 18 kann die zweite Stamm-ID in eine zweite Kennung (Schritt S118) umgewandelt werden und die Medien-ID kann unter Verwenden mindestens der ersten Stamm-ID und der zweiten Kennung berechnet werden (Schritt S120). Die Medien-ID kann z. B. berechnet werden unter Verwenden sowohl der ersten Stamm-ID und der zweiten Kennung.

[0116] Wenn eine eindeutige Kennung des zweiten Teils nicht entweichen sollte, können Daten, die durch Verschlüsseln der eindeutigen Kennung des zweiten Teils erhalten werden, der Host-Vorrichtung als die zweite Stamm-ID anstelle der eindeutigen Kennung des zweiten Teils geliefert werden. Die Host-Vorrichtung kann so dann die zweite Kennung erzeugen, die als weitere Kennung des zweiten Teils unter Verwenden der zweiten Stamm-ID verwendet werden.

[0117] Ein Verfahren zum Berechnen der Medien-ID wird nun in Bezug auf Fig. 19 bis Fig. 20 beschrieben werden.

[0118] In Bezug auf Fig. 19 kann der zweite Teil ein Speicherelement sein und der erste Teil kann eine Speicherelement-Steuereinheit sein. Das Speicherelement speichert seine eindeutige Kennung. Eine eindeutige Kennung der Speicherelement-Steuereinheit kann ebenso in dem Speicherelement gespeichert werden.

[0119] Als erstes wird ein Verfahren (Schritt S10) zum Erzeugen einer speicherabgeleiteten ID beschrieben, die als eine weitere Kennung des Speicherelements verwendet werden kann. Die speicherabgeleitete ID kann als identisch zu der zweiten Kennung verstanden werden, die oben in Bezug auf Fig. 18 beschrieben wurde.

[0120] Die Host-Vorrichtung empfängt von der Speichervorrichtung eine verschlüsselte Speicher-ID, die durch Verschlüsseln der gespeicherten eindeutigen Kennung des Speicherelements erhalten wird. Die verschlüsselte Speicher-ID kann ebenso in dem Speicherelement gespeichert werden. Die verschlüsselte Speicher-ID kann als identisch zu der zweiten Stamm-ID, die oben in Bezug auf Fig. 18 beschrieben wird, verstanden werden.

[0121] Die Host-Vorrichtung erzeugt eine Speicher-ID, die die eindeutige Kennung des Speicherelements durch Entschlüsseln der verschlüsselten Speicher-ID ist (Schritt S124).

[0122] Die Host-Vorrichtung erzeugt zweite Authentifizierungsinformation unter Verwenden der Speicher-ID (Schritt S126). Insbesondere kann die Host-Vorrichtung eine Zufallszahl erzeugen, einen Sitzungsschlüssel durch Verschlüsseln der Zufallszahl erzeugen und die zweite Authentifizierungsinformation durch Eingeben der eindeutigen Kennung (z. B. die Speicher-ID) des Speicherelements und des Sitzungsschlüssels für eine vorbestimmte Einwegfunktion erzeugen. Es ist rechnerisch unmöglich, einen entsprechenden Eingabewert der Einwegfunktion mit jedem Ausgabewert der Einwegfunktion zu finden. Die Einwegfunktion kann z. B. XOR unter bitweise Operationen sein, das zwei Operanden als Eingang erfordert.

[0123] Die Speichervorrichtung erzeugt erste Authentifizierungsinformation unter Verwenden der Speicher-ID (Schritt S128). Ein Ersatzschlüsselset, zusammengesetzt aus einer Mehrzahl von Ersatzschlüsseln, kann in dem Speicherelement zusätzlich zu der Speicher-ID gespeichert werden. Die Speichervorrichtung kann einen Sitzungsschlüssel durch Verschlüsseln eines der Ersatzschlüssel in dem Ersatzschlüsselset und Verschlüsseln des Ersatzschlüssels unter Verwenden einer Zufallszahl, die durch die Host-Vorrichtung als ein Verschlüsselungs-Schlüssel erzeugt wird, erzeugen. Die Speichervorrichtung kann dann die erste Authentifizierungsinformation durch Eingeben des Sitzungsschlüssels und der Speicher-ID zu einer vorbestimmten Einwegfunktion erzeugen.

[0124] Die Host-Vorrichtung empfängt die erste Authentifizierungsinformation von der Speichervorrichtung (Schritt S130) und verifiziert, ob die erste Authentifizierungsinformation mit der zweiten Authentifizierungsinformation zusammenpasst (Entscheidung Schritt S132). Wenn in Entscheidungsschritt S132 entschieden wird, dass die erste Authentifizierungsinformation nicht mit der zweiten Authentifizierungsinformation übereinstimmt (NEIN-Pfad von Entscheidungsschritt S132), kann eine Benachrichtigung eines Authentifizierungsfehlers geliefert werden (Schritt S134).

[0125] Wenn in Schritt S132 verifiziert wird, dass die erste Authentifizierungsinformation mit der zweiten Authentifizierungsinformation übereinstimmt (JA-Pfad des Entscheidungsschritts S132), wird eine speicherabgeleitete ID unter Verwenden der eindeutigen Kennung (z. B. der Speicher-ID) von dem Speicherelement erzeugt. Die speicherabgeleitete ID kann durch Eingeben der eindeutigen Kennung (z. B. die Speicher-ID) des Speicherelements und eines anwendungsspezifischen Sicherheitswerts (ASSV) zu einer vorbestimmten Einwegfunktion erzeugt werden.

[0126] Der ASSV kann jeder Anwendung, die auf der Host-Vorrichtung läuft, bereitgestellt werden. Unterschiedliche ASSVs können z. B. einer Musik-Aufnahmeanwendung, einer Video-Aufnahmeanwendung und einer Software-Aufnahmeanwendung bereitgestellt werden. Der ASSV kann einen eindeutigen Wert für jeden Typ von Inhalt aufweisen, der verschlüsselt wird oder für jede Anbieter-ID der Inhalte, die verschlüsselt werden. Bevorzugt kann der ASSV einen eindeutigen Wert für jede Art von Inhalten, die verschlüsselt werden, aufweisen. Der Typ von Inhalt kann z. B. Inhalt von Video, Musik, Dokument oder Software sein.

[0127] Als nächstes wird ein Verfahren zum Empfangen der eindeutigen Kennung (z. B. einer Steuereinheit-ID) der Speicherelement-Steuereinheit (Schritt S20) beschrieben werden.

[0128] Insbesondere wird nun ein Verfahren (Schritt S20) in Bezug auf die Fig. 20 beschrieben werden, bei dem die Host-Vorrichtung die eindeutige Kennung (z. B. die Steuereinheit-ID) von der Speicherelement-Steuereinheit von der Speichervorrichtung empfängt.

[0129] In Bezug auf Fig. 20 empfängt eine Host-Vorrichtung eine dritte Authentifizierungsinformation von

der Speichervorrichtung (Schritt S140). Sowie bereits oben erwähnt, kann die dritte Authentifizierungsinformation ein Authentifizierungszertifikat der Speichervorrichtung und die Steuereinheit-ID von der Steuereinheit, die in der Speichervorrichtung enthalten ist, aufweisen.

[0130] Die Host-Vorrichtung und die Speichervorrichtung können einander gegenseitig authentifizieren (Schritt S141). Diese gegenseitige Authentifizierung kann eine Authentifizierung basierend auf einem öffentlichen Schlüssel sein. Wenn die gegenseitige Authentifizierung fehlschlägt (NEIN-Pfad von Entscheidungsschritt S142), liefert die Host-Vorrichtung eine Nachricht eines Authentifizierungsfehlers (Schritt S144). Wenn die gegenseitige Authentifizierung erfolgreich ist (JA-Pfad der Entscheidung), kann die Host-Vorrichtung die Steuereinheit-ID von der dritten Authentifizierungsinformation (Schritt S148) erhalten.

[0131] Die Host-Vorrichtung berechnet eine Medien-ID unter Verwenden mindestens einer von der speicherabgeleiteten ID und der Steuereinheit-ID. Die Host-Vorrichtung berechnet bevorzugt die Medien-ID unter Verwenden sowohl der speicherabgeleiteten ID und der Steuereinheit-ID.

[0132] Die Medien-ID kann als Ergebnis der Durchführung eine Binär-Operation von der speicherabgeleiteten ID und der Steuereinheit-ID erhalten werden. Die Medien-ID kann Z. B. als ein Ergebnis von einem Durchführen einer Binär-Operation (z. B. AND, OR, XOR oder derselben), die zwei Operanden benötigt, auf der speicherabgeleiteten ID und der Steuereinheit-ID enthalten werden.

[0133] Die Medien-ID kann als ein Ergebnis von einem Durchführen einer STRCAT-Operation (z. B. durch Verketten der speicherabgeleiteten ID und der Steuereinheit-ID) in dieser Reihenfolge erhalten werden. Die Medien-ID kann alternativ als ein Ergebnis eines Durchführens einer STRCAT-Operation (z. B. Verketten der Steuereinheit-ID und der speicherabgeleiteten ID) in dieser Reihenfolge erhalten werden.

[0134] Ein Verfahren zum Erzeugen eines Sicherheitsschlüssels und Entschlüsseln von Inhalt oder Verwenden des Sicherheitsschlüssels gemäß einer beispielhaften Ausführungsform der vorliegenden Erfindung wird nun mit Bezug auf die Fig. 21 beschrieben werden.

[0135] In Bezug auf Fig. 21 werden eine Stamm-ID und verschlüsselte Inhalte in einer Speichervorrichtung gespeichert (Schritte S200 und S201). Es wird angenommen, dass die verschlüsselten Inhalte durch Verschlüsseln von Inhalt unter Verwenden eines Verschlüsselungs-Schlüssels, der unter Verwenden einer Medien-ID der Speichervorrichtung und Benutzer-Authentifizierungsinformation A (Passwort A) erzeugt werden.

[0136] Eine Host-Vorrichtung empfängt die Stamm-ID von der Speichervorrichtung (Schritt S202). Obwohl nicht in Fig. 21 dargestellt kann die Host-Vorrichtung die Speichervorrichtung anfordern, die Stamm-ID zu liefern und die Stamm-ID als Antwort auf die Anfrage zu empfangen. Die Host-Vorrichtung kann eine Anfrage an die Stamm-ID machen, wenn sie einen Befehl empfängt, um den verschlüsselten Inhalt von einem Benutzer auszuspielen.

[0137] Die Host-Vorrichtung berechnet die Medien-ID unter Verwenden der Stamm-ID (Schritt S203). Das Medien-ID-Berechnungsverfahren der Host-Vorrichtung kann identisch sein mit dem Medien-ID-Berechnungsverfahren der Host-Vorrichtung, die oben in Bezug auf Fig. 17 bis Fig. 20 beschrieben wird und folglich wird eine wiederholte Beschreibung davon weggelassen.

[0138] Die Host-Vorrichtung empfängt Authentifizierungsinformation (Passwort A) von dem Benutzer (Schritt S204). Die empfangene Authentifizierungsinformation kann identisch sein oder sich von der Authentifizierungsinformation unterscheiden, die verwendet wird, um den Verschlüsselungs-Schlüssel für den verschlüsselten Inhalt zu erzeugen, Zur Erleichterung der Beschreibung wird angenommen, dass die empfangene Authentifizierungsinformation identisch mit der Authentifizierungsinformation ist, die verwendet wird, um den Verschlüsselungs-Schlüssel für den verschlüsselten Inhalt zu erzeugen.

[0139] Die Host-Vorrichtung erzeugt einen Entschlüsselungs-Schlüssel unter Verwenden der Medien-ID und der Authentifizierungsinformation (Schritt S205).

[0140] Die Erzeugung des Entschlüsselungs-Schlüssels (Schritt S205) kann ausschließlich unter Verwenden der Medien-ID und der Authentifizierungsinformation oder unter Verwenden von einem oder mehreren variablen oder nicht variablen Daten zusätzlich zu der Medien-ID und der Authentifizierungsinformation durchgeführt werden.

[0141] Der Entschlüsselungs-Schlüssel kann z. B. Daten darstellen, die als ein Ergebnis von einem Durchführen einer Binär-Operation auf der Medien-ID und der Authentifizierungsinformation erzeugt werden. Insbesondere kann der Entschlüsselungs-Schlüssel Daten darstellen, die als ein Ergebnis eines Durchführens einer XOR-Operation erzeugt werden. Folglich kann der Entschlüsselungs-Schlüssel Daten darstellen, die als ein Ergebnis eines Durchführens einer XOR-Operation auf dem Medien-ID und der Authentifizierungsinformation erhalten werden.

[0142] Der Entschlüsselungs-Schlüssel kann ebenso Daten darstellen, die als ein Ergebnis von einem Durchführen einer STRCAT-Operation auf den Medien-ID und der Authentifizierungsinformation produziert werden. Bei der STRCAT-Operation können Strings in irgendeiner Reihenfolge verkettet werden. Die Medien-ID und die Authentifizierungsinformation können folglich in dieser Reihenfolge oder der entgegen gesetzten Reihenfolge verkettet werden.

[0143] Die Host-Vorrichtung liest den verschlüsselten Inhalt, der in der Speichervorrichtung gespeichert ist (Schritt S206), entschlüsselt den verschlüsselten Inhalt unter Verwenden des Entschlüsselungs-Schlüssel (Schritt S207) und gibt den entschlüsselten Inhalt (S208) aus.

[0144] Ein Verfahren, in dem eine Host-Vorrichtung daran scheitert, einen verschlüsselten Inhalt zu entschlüsseln, der illegal zu einer Inhaltspeichervorrichtung Y (**201**) von einer Inhaltspeichervorrichtung X (**200**) kopiert wird, wird nun in Bezug auf die Fig. 22 beschrieben.

[0145] In Bezug auf die Fig. 22 wird eine Stamm-ID Y, die sich von einer Stamm-ID unterscheidet, die in der Inhaltspeichervorrichtung X (**200**) gespeichert ist, in der Inhaltspeichervorrichtung Y (**201**) gespeichert (Schritt S210).

[0146] Darüber hinaus werden verschlüsselte Inhalte, die durch Verschlüsseln von Inhalten unter Verwenden der Inhalt-Verschlüsselungsverfahrens von der Fig. 16 vor dem Kopieren erhalten werden, in der Inhaltspeichervorrichtung X (**200**) gespeichert (Schritt S209). Es wird angenommen, dass Authentifizierungsinformation, die verwendet wird, um einen Entschlüsselungs-Schlüssel XA zu erzeugen, A (Passwort A) ist. Es wird ebenso angenommen, dass ein Benutzer den verschlüsselten Inhalt von der Inhaltspeichervorrichtung X (**200**) zu der Inhaltspeichervorrichtung Y (**201**) illegal kopiert hat (Schritt S211).

[0147] Wenn der Benutzer die Inhaltspeichervorrichtung Y (**201**) mit der Host-Vorrichtung verbindet und einen Befehl eingibt, den verschlüsselten Inhalt der Host-Vorrichtung auszuspielen, empfängt die Host-Vorrichtung die Stamm-ID Y, die in der Inhaltspeichervorrichtung Y (**201**) gespeichert wird (Schritt S213).

[0148] Die Host-Vorrichtung erzeugt eine Medien-ID der Inhaltspeichervorrichtung Y (**201**) unter Verwenden der Stamm-ID Y (Schritt S214).

[0149] Die Host-Vorrichtung empfängt Benutzer-Authentifizierungsinformation (Schritt S215). Es wird angenommen, dass die Benutzer-Authentifizierungsinformation A (Passwort A) ist, die identisch mit der Authentifizierungsinformation A ist, die verwendet wird, um den Verschlüsselungs-Schlüssel XA für den verschlüsselten Inhalt zu erzeugen.

[0150] Die Host-Vorrichtung erzeugt einen Entschlüsselungs-Schlüssel YA unter Verwenden der Medien-ID und der Benutzer-Authentifizierungsinformation A (Schritt S216).

[0151] Die Host-Vorrichtung versucht den verschlüsselten Inhalt, der von der Inhaltspeichervorrichtung Y (**201**) empfangen wird (Schritt S217), unter Verwenden des erzeugten Entschlüsselungs-Schlüssel YA (Schritt S218) zu entschlüsseln. Jedoch kann, da sich der Entschlüsselungs-Schlüssel YA, der in Schritt S216 erzeugt wird, von einem Entschlüsselungs-Schlüssel XA des verschlüsselten Inhalts unterscheidet, die Host-Vorrichtung nicht den verschlüsselten Inhalt entschlüsseln.

[0152] Folglich kann die Host-Vorrichtung den verschlüsselten Inhalt nicht ausspielen, der illegal kopiert auf und gespeichert in der Inhaltspeichervorrichtung Y ist (**201**) (Schritt S219).

[0153] In der Fig. 22 wird angenommen, dass der Benutzer korrekte Authentifizierungsinformation eingibt (z. B. Authentifizierungsinformation, die identisch mit der Benutzer-Authentifizierungsinformation A ist, die verwendet wird, um den Verschlüsselungs-Schlüssel XA zu erzeugen). Jedoch kann, sogar wenn der Benutzer nicht korrekte Authentifizierungsinformation eingibt z. B. Authentifizierungsinformation, die sich von der Benutzer-Authentifizierungsinformation A unterscheidet, die verwendet wird, um den verschlüsselten Schlüssel XA zu erzeugen, die Host-Vorrichtung den verschlüsselten Inhalt nicht ausspielen, der illegal kopiert auf und gespeichert in der Inhaltspeichervorrichtung Y (**201**) ist (Schritt S219).

[0154] Folglich kann der verschlüsselte Inhalt, der illegal kopiert auf und gespeichert in der Inhaltspeichervorrichtung Y (**201**) wird, nicht ausgespielt werden, ungeachtet, ob korrekte Benutzer-Authentifizierungsinformation eingegeben wurde.

[0155] Die Fig. 23 veranschaulicht eine beispielhafte Ausführungsform, in der eine Host-Vorrichtung versagt, einen verschlüsselten Inhalt auszuspielen, wenn Benutzer-Authentifizierungsinformation nicht korrekt ist, die verwendet wird, um einen Verschlüsselungs-Schlüssel für den verschlüsselten Inhalt zu erzeugen.

[0156] In Bezug auf die Fig. 23 speichert eine Inhaltspeichervorrichtung X (**200**) verschlüsselte Inhalte, die durch Verschlüsseln von Inhalt unter Verwenden eines Verschlüsselungs-Schlüssels XA, der unter Verwenden einer Medien-ID der Inhaltspeichervorrichtung X (**200**) und ersten Benutzer-Authenti-

fizierungsinformation A (Passwort A) erzeugt wird (Schritt S209). Die erste Authentifizierungsinformation A wird verwendet, um den Verschlüsselungs-Schlüssel XA für den verschlüsselten Inhalt zu erzeugen. Der Verschlüsselungs-Schlüssel XA kann ebenso als ein Entschlüsselungs-Schlüssel zum Entschlüsseln des verschlüsselten Inhalts verwendet werden.

[0157] Wenn ein zweiter Benutzer die Inhaltspeichervorrichtung X (**200**) mit der Host-Vorrichtung verbindet und einen Befehl eingibt, den verschlüsselten Inhalt zu der Host-Vorrichtung auszuspielen, empfängt die Host-Vorrichtung eine Stamm-ID X, die in der Inhaltspeichervorrichtung X (**200**) gespeichert wird.

[0158] Die Host-Vorrichtung erzeugt die Medien-ID der Inhaltspeichervorrichtung X (200) unter Verwenden der ersten ID X (Schritt S221).

[0159] Die Host-Vorrichtung empfängt zweite Benutzer-Authentifizierungsinformation B (Passwort B) von dem zweiten Benutzer (Schritt S222). Es wird angenommen, dass die zweite Benutzer-Authentifizierungsinformation B ist, die sich von der ersten Authentifizierungsinformation A unterscheidet, die verwendet wird, um den Verschlüsselungs-Schlüssel XA für den verschlüsselten Inhalt zu erzeugen.

[0160] Die Host-Vorrichtung erzeugt einen Entschlüsselungs-Schlüssel XB unter Verwenden der Medien-ID und der zweiten Benutzer-Authentifizierungsinformation B (Schritt S223).

[0161] Die Host-Vorrichtung versucht den verschlüsselten Inhalt zu entschlüsseln, der von der Inhaltspeichervorrichtung Y (**201**) (Schritt **224**) unter Verwenden des erzeugten Entschlüsselungs-Schlüssel XB (Schritt S225) empfangen wird. Jedoch kann, da sich der erzeugte Entschlüsselungs-Schlüssel XB von einem Entschlüsselungs-Schlüssel XA des verschlüsselten Inhalts unterscheidet, die Host-Vorrichtung den verschlüsselten Inhalt nicht entschlüsseln.

[0162] Folglich kann die Host-Vorrichtung den verschlüsselten Inhalt nicht ausspielen, der in der Inhaltspeichervorrichtung X (**200**) gespeichert ist (Schritt S219).

[0163] In der Fig. 23 wird angenommen, dass der Benutzer der Host-Vorrichtung ein zweiter Benutzer war, der sich von dem ersten Benutzer unterscheidet oder dergleiche erste Benutzer war, der nicht korrekte Authentifizierungsinformation eingegeben hat (z. B. Authentifizierungsinformation, die sich von der Benutzer-Authentifizierungsinformation A unterscheidet, die verwendet wird, um den Verschlüsselungs-Schlüssel XA zu erzeugen). Jedoch kann die Host-Vorrichtung den verschlüsselten Inhalt ausspielen, wenn der zweite Benutzer korrekte Authentifizierungsinformation eingibt, z. B. Authentifizierungsinformation, die identisch mit der ersten Benutzer-Authentifizierungsinformation A ist, die verwendet wird, um den Verschlüsselungs-Schlüssel XA zu erzeugen.

[0164] Die vorliegende Erfindung kann einen Sicherheitsschlüssel erzeugen, der sowohl zu einer spezifischen Vorrichtung als auch zu einem spezifischen Benutzer gehört. Inhalt, der z. B. unter Verwenden eines Sicherheitsschlüssels verschlüsselt wird, der durch eine Sicherheitsschlüssel-Erzeugungsvorrichtung gemäß der vorliegenden Erfindung erzeugt wird, kann nur entschlüsselt werden, wenn ein spezifischer Benutzer, der in Verbindung mit der Erzeugung des Sicherheitsschlüssels steht, eine spezifische Vorrichtung verwendet.

[0165] Darüber hinaus erzeugt sie, wenn die Sicherheitsschlüssel-Erzeugungsvorrichtung Trusted-Computing unterstützt, den Sicherheitsschlüssel in einem sicheren Modus, der eine Trusted-Computing-Umgebung unterstützt. Deshalb können der Informationsverlust (z. B. Datenklau) wie z. B. einer Benutzer-Authentifizierungsinformation, einer Vorrichtungs-ID und des erzeugten Sicherheitsschlüssels verhindert werden.

[0166] Fachleute werden verstehen, dass viele Abweichungen und Veränderungen von den beispielhaften Ausführungsformen vorgenommen werden können, ohne wesentlich von den Prinzipien der vorliegenden Erfindung abzuweichen. Daher werden die offenbarten beispielhaften Ausführungsformen der Erfindung nur in einem allgemeinen und beschreibenden Sinn und nicht beschränkend verwendet.

ZITATE ENTHALTEN IN DER BESCHREIBUNG

Diese Liste der vom Anmelder aufgeführten Dokumente wurde automatisiert erzeugt und ist ausschließlich zur besseren Information des Lesers aufgenommen. Die Liste ist nicht Bestandteil der deutschen Patent- bzw. Gebrauchsmusteranmeldung. Das DPMA übernimmt keinerlei Haftung für etwaige Fehler oder Auslassungen.

Zitierte Patentliteratur

- KR 10-2012-0055527 [**0001**]

Patentansprüche

1. Eine Sicherheitsschlüssel-Erzeugungsvorrichtung, die aufweist:
eine ID-Berechnungseinheit (**12**), die derart konfiguriert ist, dass sie eine erste Stamm-ID von einer ersten Speichervorrichtung (**200**) empfängt und eine erste Medien-ID aus der ersten Stamm-ID berechnet, wobei die erste Medien-ID eine digitale Kennung der ersten Speichervorrichtung (**200**) ist;
eine Authentifizierungsinformations-Liefereinheit (**14**), die derart konfiguriert ist, dass sie eine Sicherheitsschlüssel-Erzeugungseinheits-Benutzer-Authentifizierungsinformation zum Authentifizieren eines Benutzers (**1**) liefert; und
die Sicherheitsschlüssel-Erzeugungseinheit (**16**), die derart konfiguriert ist, dass sie einen entsprechenden Sicherheitsschlüssel unter Verwenden sowohl der ersten Medien-ID und der Benutzer-Authentifizierungsinformation erzeugt.

2. Vorrichtung nach Anspruch 1, wobei die erste Stamm-ID eine oder mehrere ID-Daten darstellt, die verwendet werden, um die erste Medien-ID zu berechnen und sich von der ersten Medien-ID unterscheidet.

3. Vorrichtung nach Anspruch 1, wobei die erste Stamm-ID eine erste verschlüsselte Speicher-ID (**264**) ist, die durch Verschlüsseln einer ersten Speicher-ID (**262**) erhalten wird, die eine Kennung eines ersten Speicherelements (**206**) ist, das in der ersten Speichervorrichtung (**200**) enthalten ist, und die D-Berechnungseinheit (**12**) die erste verschlüsselte Speicher-ID (**264**) in die erste Speicher-ID (**262**) entschlüsselt, eine erste speicherabgeleitete ID aus der ersten Speicher-ID berechnet und die erste speicherabgeleitete ID als die erste Medien-ID verwendet.

4. Vorrichtung nach Anspruch 1, wobei die erste Stamm-ID eine erste Steuereinheit-ID aufweist, die eine Kennung einer ersten Steuereinheit (**208**) ist, die in der ersten Speichervorrichtung (**200**) enthalten ist, und die ID-Berechnungseinheit (**12**) die erste Medien-ID unter Verwenden der ersten Steuereinheit-ID berechnet.

5. Vorrichtung nach Anspruch 4, wobei sich die ID-Berechnungseinheit (**12**) und die erste Steuereinheit (**208**) gegenseitig authentifizieren und die ID-Berechnungseinheit (**12**) die erste Steuereinheit-ID bei dem gegenseitigen Authentifizierungsverfahren empfängt.

6. Vorrichtung nach Anspruch 1, wobei die erste Stamm-ID eine erste verschlüsselte Speicher-ID (**264**) aufweist, die durch Verschlüsseln einer ersten Speicher-ID erhalten wird, die eine Kennung eines ersten Speicherelements (**206**) ist, das in der ersten Speichervorrichtung (**200**) enthalten ist, und durch Verschlüsseln einer ersten Steuereinheit-ID, die eine Kennung einer ersten Steuereinheit (**208**) ist, die in der ersten Speichervorrichtung (**200**) enthalten ist, und wobei die ID-Berechnungseinheit (**12**) die erste entschlüsselte Speicher-ID (**264**) in die erste Speicher-ID entschlüsselt, eine erste speicherabgeleitete ID von der ersten Speicher-ID berechnet und die erste Medien-ID unter Verwenden sowohl der ersten Steuereinheit-ID und der ersten speicherabgeleiteten ID berechnet.

7. Vorrichtung nach Anspruch 1, wobei die Authentifizierungsinformations-Liefereinheit (**14**) die Benutzer-Authentifizierungsinformation von dem aktuellen Benutzer (**1**) empfängt, wobei die Sicherheitsschlüssel-Erzeugungseinheit (**16**) derart konfiguriert ist, dass sie einen Sicherheitsschlüssel unter Verwendung sowohl der ersten Medien-ID und der aktuellen Benutzer-Authentifizierungsinformation erzeugt.

8. Vorrichtung nach Anspruch 2, wobei:
die ID-Berechnungseinheit (**12**) derart konfiguriert ist, dass sie eine zweite Stamm-ID von einer zweiten Speichervorrichtung (**200**) empfängt, und, dass sie eine zweite Medien-ID von der zweiten Stamm-ID berechnet, wobei die zweite Medien-ID eine digitale Kennung der zweiten Speichervorrichtung (**200**) ist;
wobei die Sicherheitsschlüssel-Erzeugungseinheit (**16**) derart konfiguriert ist, dass sie einen anderen Sicherheitsschlüssel entsprechend sowohl der zweiten Medien-ID und der Benutzer-Authentifizierungsinformation erzeugt, und
die zweite Stamm-ID eine oder mehrere ID-Datenmengen darstellt, die verwendet werden, um die zweite Medien-ID zu berechnen, und die Daten darstellt, die sich von der zweiten Stamm-ID unterscheiden.

9. Vorrichtung nach Anspruch 3, wobei:
die ID-Berechnungseinheit (**12**) derart konfiguriert ist, dass sie eine zweite Stamm-ID von einer zweiten Speichervorrichtung (**200**) empfängt und eine zweite Medien-ID von der zweiten Stamm-ID berechnet, wobei die zweite Medien-ID eine digitale Kennung der zweiten Speichervorrichtung (**200**) ist;
wobei die Sicherheitsschlüssel-Erzeugungseinheit (**16**) derart konfiguriert ist, dass sie einen anderen Sicherheitsschlüssel entsprechend sowohl der zweiten Medien-ID und der Benutzer-Authentifizierungsinformation erzeugt, und
die zweite Stamm-ID eine zweite verschlüsselte Speicher-ID ist, die durch Verschlüsseln einer zweiten Speicher-ID erhalten wird, die eine Kennung eines zweiten Speicherelements (**206**) ist, und die ID-Berechnungseinheit (**12**) die zweite verschlüsselte Speicher-ID in die zweite Speicher-ID entschlüsselt, eine zweite speicherabgeleitete ID aus der zweiten Speicher-ID berechnet und die zweite speicherabgeleitete ID als die zweite Medien-ID verwendet.

10. Sicherheitsschlüssel-Erzeugungsvorrichtung, die aufweist:
eine Speicherschnittstelle, die derart konfiguriert ist, dass sie eine erste Stamm-ID von einer ersten Speichervorrichtung (**200**) empfängt und die erste Stamm-ID einem Prozessor (**102**) liefert; und
den Prozessor (**102**), der derart konfiguriert ist, dass er eine erste Medien-ID, die eine Kennung der ersten Speichervorrichtung (**200**) ist, aus der ersten Stamm-ID berechnet und einen entsprechenden Sicherheitsschlüssel unter Verwenden sowohl der ersten Medien-ID und einer Authentifizierungsinformation zum Authentifizieren eines Benutzers (**1**) erzeugt.

11. Vorrichtung nach Anspruch 10, wobei der Prozessor (**102**) in einem von einem nicht sicheren Ausführmodus und einem sicheren Ausführmodus arbeitet, und die Authentifizierungsinformation bei einem Authentifizierungsverfahren verwendet wird, das verwendet wird, um einen Betriebsmodus des Prozessors (**102**) von dem nicht sicheren Ausführmodus in den sicheren Ausführmodus zu wechseln.

12. Vorrichtung nach Anspruch 11, wobei der Prozessor (**102**) einen nicht sicheren virtuellen Kern (**120**), der Befehle in dem nicht sicheren Ausführmodus ausführt, und einen sicheren virtuellen Kern (**124**), der Befehle in dem sicheren Ausführmodus ausführt, aufweist, wobei der nicht sichere virtuelle Kern (**102**) die Authentifizierungsinformation verifiziert und ein Unterbrechungssignal erzeugt, wenn die Authentifizierungsinformation erfolgreich verifiziert ist, wobei der Prozessor (**102**) den Betriebsmodus davon von dem nicht sicheren Ausführmodus zu dem sicheren Ausführmodus als Antwort auf das Unterbrechungssignal wechselt, und der sichere virtuelle Kern (**124**) den Sicherheitsschlüssel erzeugt.

13. Vorrichtung nach Anspruch 12, die ferner einen Random-Access-Speicher (RAM) (**106**) aufweist, wobei der RAM (**106**) einen ersten Bereich, auf den durch einen Befehl, der auf dem nicht sicheren virtuellen Kern (**120**) ausgeführt wird, zugegriffen werden kann und einen zweiten Bereich aufweist, auf den durch einen Befehl, der auf dem zweiten virtuellen Kern (**124**) ausgeführt wird, zugegriffen werden kann und sich nicht mit dem ersten Bereich überschneidet und der Befehl, der auf dem nicht sicheren virtuellen Kern (**120**) ausgeführt wird, nicht auf den zweiten Bereich zugreifen kann.

14. Vorrichtung nach Anspruch 10, die ferner eine Eingabeeinheit (**108**) zum Empfangen der Authentifizierungsinformation und Liefern der Authentifizierungsinformation an den Prozessor (**102**) aufweist, wobei der Prozessor (**102**) in einem von einem nicht sicheren Ausführmodus und einem sicheren Ausführmodus arbeitet und die Authentifizierungsinformation von der Eingabeeinheit (**108**) in dem sicheren Ausführmodus empfängt und den Sicherheitsschlüssel in dem sicheren Ausführmodus erzeugt.

15. Eine Host-Vorrichtung, die aufweist:
eine Speicherschnittstelle, die derart konfiguriert ist, dass sie eine Stamm-ID von einer ersten Speichervorrichtung (**200**) empfängt, wenn sie mit der ersten Speichervorrichtung (**200**) verbunden ist, und, dass sie die erste Stamm-ID einem System-On-Chip (SoC) (**302**) liefert; und
wobei der SoC (**302**) mit der Speicherschnittstelle (**104**) verbunden ist,
wobei der SoC (**302**) eine Peripherielogik (**320**) aufweist, die derart konfiguriert ist, dass sie eine erste Medien-ID, die eine eindeutige Kennung der ersten Speichervorrichtung (**200**) ist, von der ersten Stamm-ID berechnet und einen entsprechenden Sicherheitsschlüssel unter Verwenden sowohl der ersten Medien-ID und Benutzer-Authentifizierungsinformation zum Authentifizieren des aktuellen Benutzers (**1**) der Host-Vorrichtung erzeugt.

16. Host-Vorrichtung nach Anspruch 15, wobei der SoC (**302**) ferner einen Kern aufweist, der derart konfiguriert ist, dass er die Benutzer-Authentifizierungsinformation empfängt und die Benutzer-Authentifizierungsinformation der Peripherielogik (**320**) liefert.

17. Host-Vorrichtung nach Anspruch 15, die ferne eine Eingabeeinheit (**108**) aufweist, die durch den SoC (**302**) gesteuert wird, die derart konfiguriert ist, dass sie Authentifizierungsinformation von dem aktuellen Benutzer (**1**) empfängt und derart konfiguriert ist, dass sie die Authentifizierungsinformation dem SoC (**302**) liefert.

18. Host-Vorrichtung nach Anspruch 15, wobei der SoC (**302**) ferner ein Register (**324**) aufweist, das den Sicherheitsschlüssel speichert.

19. Host-Vorrichtung nach Anspruch 15, wobei die Peripherielogik (**320**) derart konfiguriert ist, dass sie einen Inhalt unter Verwenden des Sicherheitsschlüssels verschlüsselt und den verschlüsselten Inhalt der Speichervorrichtung (**200**) über die Speicherschnittstelle (**104**) liefert.

20. Host-Vorrichtung nach Anspruch 15, wobei die Speicherschnittstelle (**104**) derart konfiguriert ist, dass sie einen verschlüsselten Inhalt von der ersten Speichervorrichtung (**200**) empfängt und den verschlüsselten Inhalt dem SoC (**302**) liefert, und die Peripherielogik (**320**) derart konfiguriert ist, dass sie die erste Medien-ID, die eine eindeutige Kennung der ersten Speichervorrichtung (**200**) ist, von der ersten Stamm-ID berechnet und den entsprechenden Sicherheitsschlüssel zum Entschlüsseln des verschlüsselten Inhalts unter Verwenden sowohl der ersten Medien-ID und der Authentifizierungsinformation

zum Authentifizieren des aktuellen Benutzers (**1**) erzeugt.

21. Speichervorrichtung (**200**), die aufweist:
ein Speicherelement (**206**), das derart konfiguriert ist, dass es eine erste Speicher-ID, die eine eindeutige Kennung des ersten Speicherelements (**206**) ist, und eine erste verschlüsselte Speicher-ID, die durch Verschlüsseln der ersten Speicher-ID erhalten wird, speichert;
eine Host-Schnittstelle (**210**), die derart konfiguriert ist, dass sie Authentifizierungsinformation zum Authentifizieren eines Benutzers (**1**) von einer Host-Vorrichtung empfängt und die Authentifizierungsinformation einer Sicherheitsschlüssel-Erzeugungseinheit (**16**) liefert und einen Inhalt von der Host-Vorrichtung empfängt und den Inhalt einer Verschlüsselungseinheit (**216**) liefert;
eine speicherabgeleitete ID-Berechnungseinheit (**12**; **212**), die derart konfiguriert ist, dass sie die verschlüsselte Speicher-ID von dem Speicherelement (**206**) liest, die erste Speicher-ID durch Entschlüsseln der ersten verschlüsselten Speicher-ID erhält, und eine erste speicherabgeleitete ID, die eine weitere eindeutige Kennung des ersten Speicherelements (**206**) ist, unter Verwenden der ersten Speicher-ID erzeugt;
wobei die Sicherheitsschlüssel-Erzeugungseinheit (**16**) derart konfiguriert ist, dass sie einen Sicherheitsschlüssel unter Verwenden sowohl der Authentifizierungsinformation und der ersten speicherabgeleiteten ID erzeugt; und
wobei die Verschlüsselungseinheit (**216**) derart konfiguriert ist, dass sie den Inhalt unter Verwenden des Sicherheitsschlüssels verschlüsselt und den verschlüsselten Inhalt in dem Speicherelement (**206**) speichert.

22. Speichervorrichtung (**200**) nach Anspruch 21, wobei die Authentifizierungsinformation durch die Host-Vorrichtung als ein Parameter von einem Sicheren-Digitalen-(SD)-Karten-Standard-Befehl geliefert wird.

23. Speichervorrichtung (**200**) nach Anspruch 21, die ferner einen Zufallszahlengenerator aufweist, wobei die Sicherheitsschlüssel-Erzeugungseinheit (**16**) derart konfiguriert ist, dass sie den Sicherheitsschlüssel durch zusätzliches Verwenden einer Zufallszahl erzeugt, die durch den Zufallszahlengenerator (**214**) erzeugt wird.

24. Speichervorrichtung (**200**) nach Anspruch 23, wobei die Speichervorrichtung (**200**) gemäß Opal-Security-Subsystem-Class-(OPAL SSC)-Spezifikationen der Trusted-Computing-Group arbeitet.

25. Sicherheitsschlüssel-Erzeugungsverfahren, das aufweist:
elektrisches Verbinden einer ersten Speichervorrichtung (**200**) mit einer Sicherheitsschlüssel-Erzeugungsvorrichtung (**10**);
Empfangen einer ersten Stamm-ID von der ersten Speichervorrichtung (**200**) bei der Sicherheitsschlüssel-Erzeugungsvorrichtung (**10**) und Berechnen einer ersten Medien-ID, die eine eindeutige Kennung der ersten Speichervorrichtung (**200**) ist, aus der ersten Stamm-ID unter Verwenden der Sicherheitsschlüssel-Erzeugungsvorrichtung (**10**);
Empfangen von Benutzer-Authentifizierungsinformation direkt von dem aktuellen Benutzer (**1**) an der Sicherheitsschlüssel-Erzeugungsvorrichtung (**10**) zum Authentifizieren eines aktuellen Benutzers (**1**) oder Empfangen der Benutzer-Authentifizierungsinformation von einer weiteren Vorrichtung, die über ein Netzwerk verbunden ist; und
Erzeugen eines Sicherheitsschlüssel in der Sicherheitsschlüssel-Erzeugungsvorrichtung (**10**) unter Verwenden sowohl der ersten Medien-ID und der Benutzer-Authentifizierungsinformation.

Es folgen 20 Blatt Zeichnungen

Anhängende Zeichnungen

FIG. 1

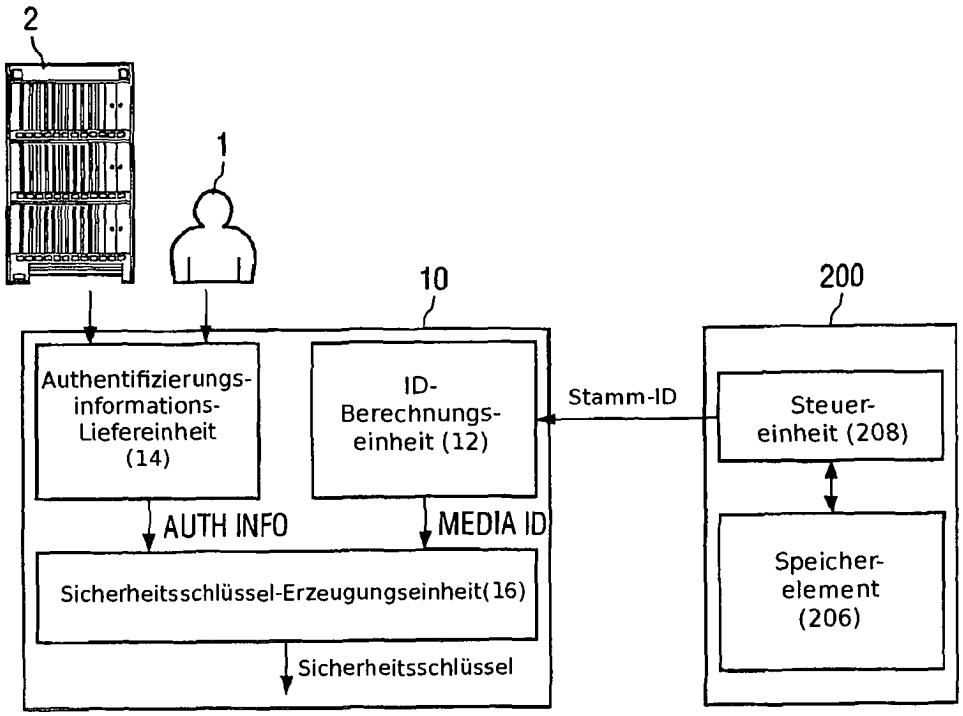


FIG. 2

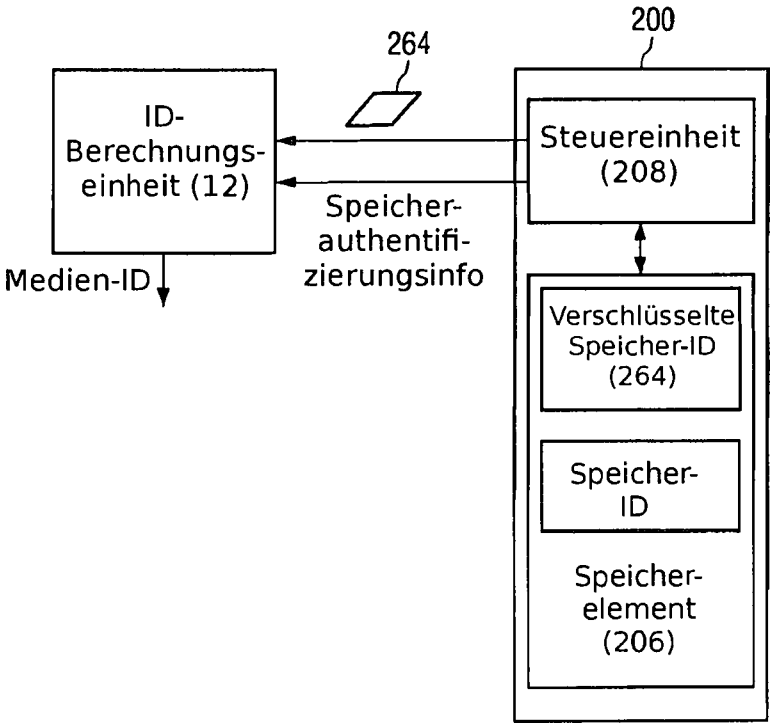

200
264
ID-Berechnungs-einheit (12)
Steuereinheit (208)
Speicher-authentifi-zierungsinfo
Medien-ID
Verschlüsselte Speicher-ID (264)
Speicher-ID
Speicher-element (206)

FIG. 3

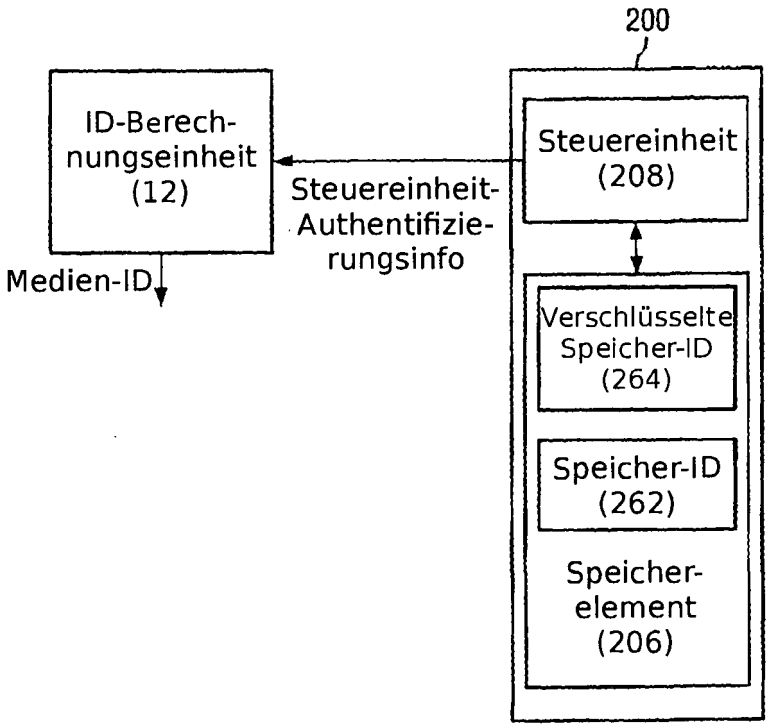

200
ID-Berech-
nungseinheit
(12)
Medien-ID
Steuereinheit-
Authentifizie-
rungsinfo
Steuereinheit
(208)
Verschlüsselte
Speicher-ID
(264)
Speicher-ID
(262)
Speicher-
element
(206)

FIG. 4

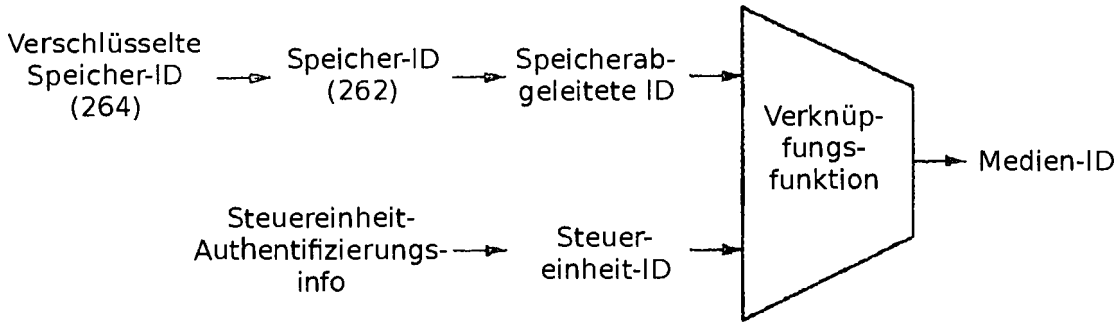

Verschlüsselte
Speicher-ID
(264)
Speicher-ID
(262)
Speicherab-
geleitete ID
Verknüp-
fungs-
funktion
Medien-ID
Steuereinheit-
Authentifizierungs-
info
Steuer-
einheit-ID

FIG. 5

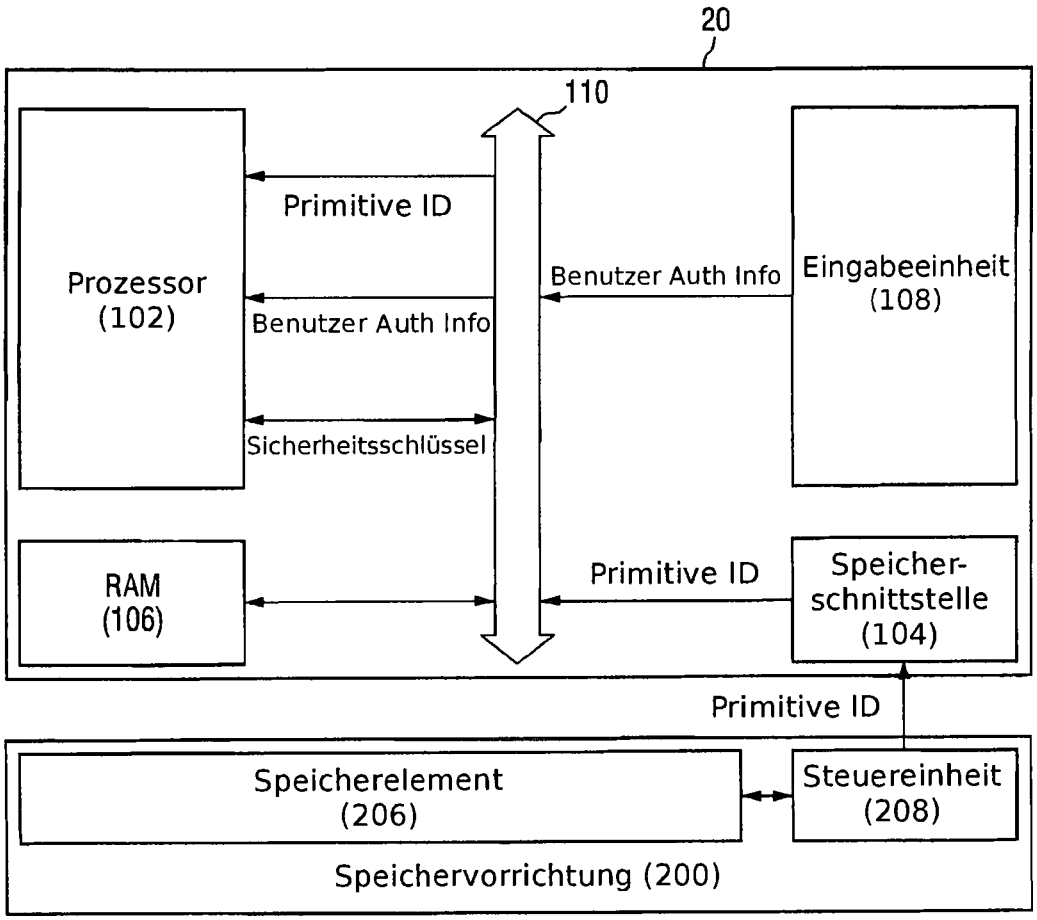

20
110
Primitive ID
Prozessor
(102)
Benutzer Auth Info
Eingabeeinheit
(108)
Benutzer Auth Info
Sicherheitsschlüssel
RAM
(106)
Primitive ID
Speicher-
schnittstelle
(104)
Primitive ID
Speicherelement
(206)
Steuereinheit
(208)
Speichervorrichtung (200)

FIG. 6

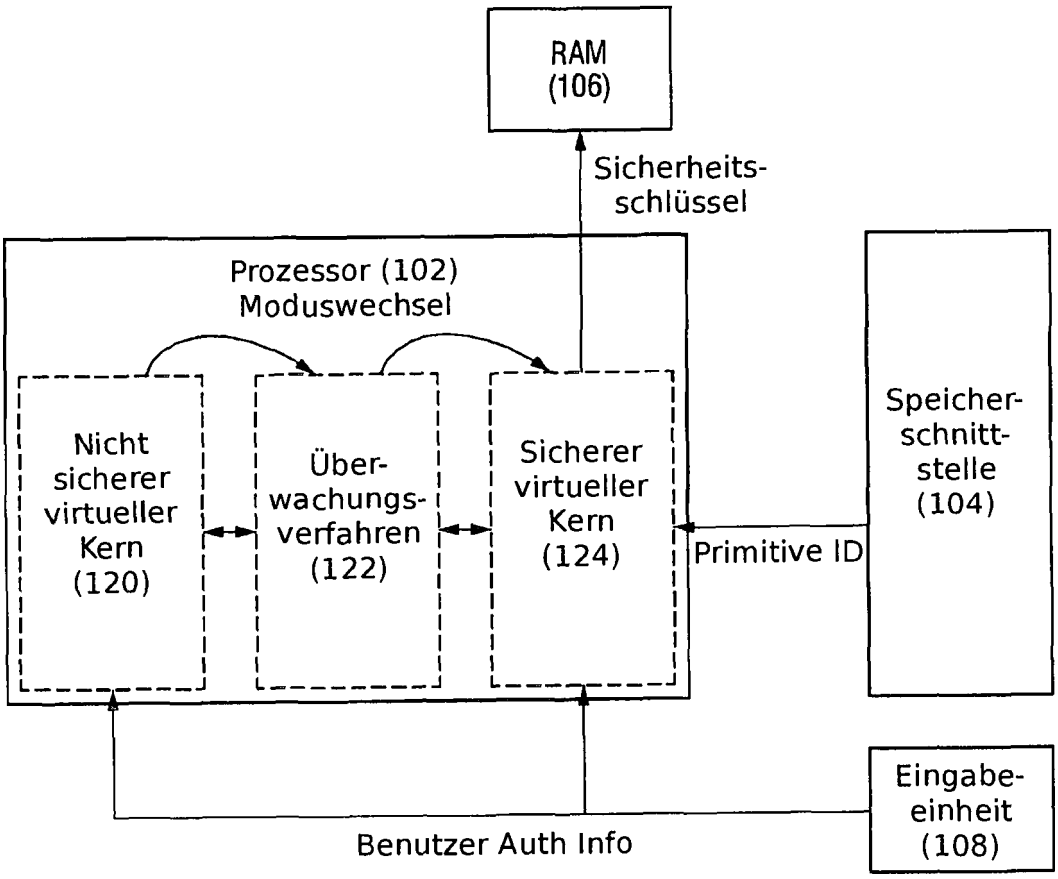

RAM
(106)
Sicherheits-
schlüssel
Prozessor (102)
Moduswechsel
Nicht
sicherer
virtueller
Kern
(120)
Über-
wachungs-
verfahren
(122)
Sicherer
virtueller
Kern
(124)
Primitive ID
Speicher-
schnitt-
stelle
(104)
Eingabe-
einheit
(108)
Benutzer Auth Info

FIG. 7

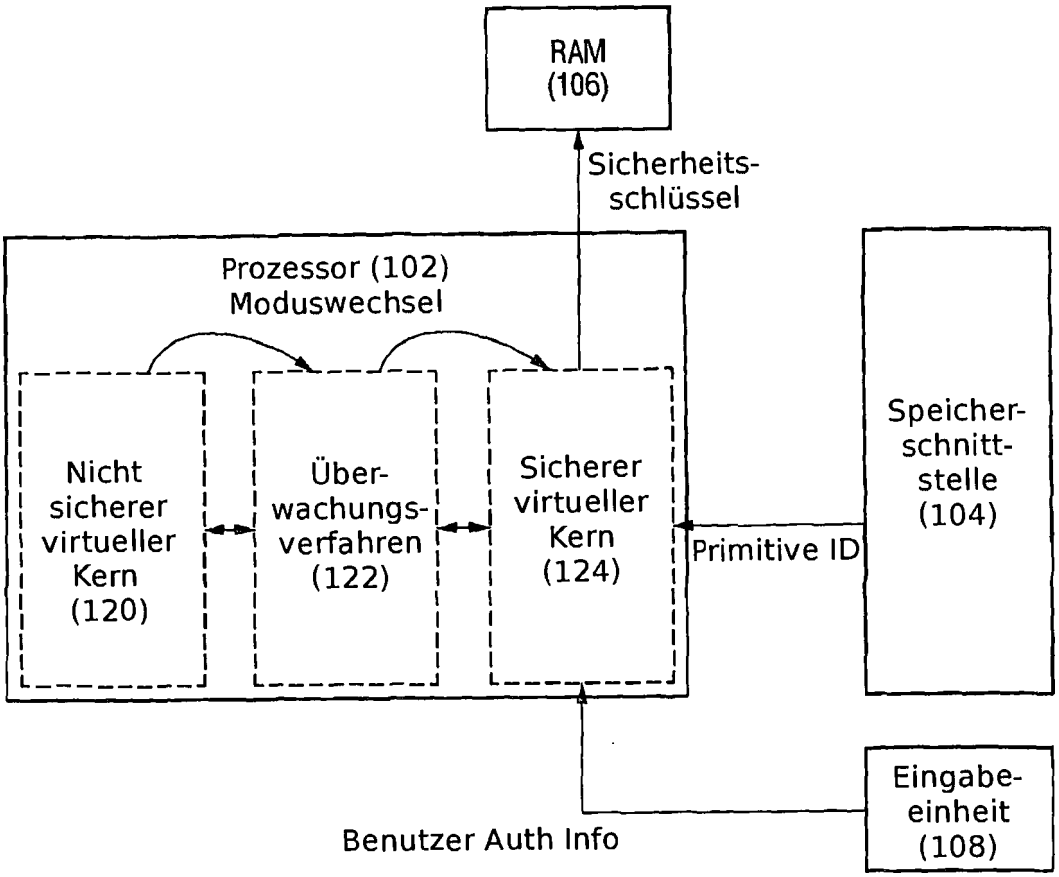

RAM
(106)
Sicherheits-
schlüssel
Prozessor (102)
Moduswechsel
Nicht
sicherer
virtueller
Kern
(120)
Über-
wachungs-
verfahren
(122)
Sicherer
virtueller
Kern
(124)
Primitive ID
Speicher-
schnitt-
stelle
(104)
Eingabe-
einheit
(108)
Benutzer Auth Info

FIG. 8

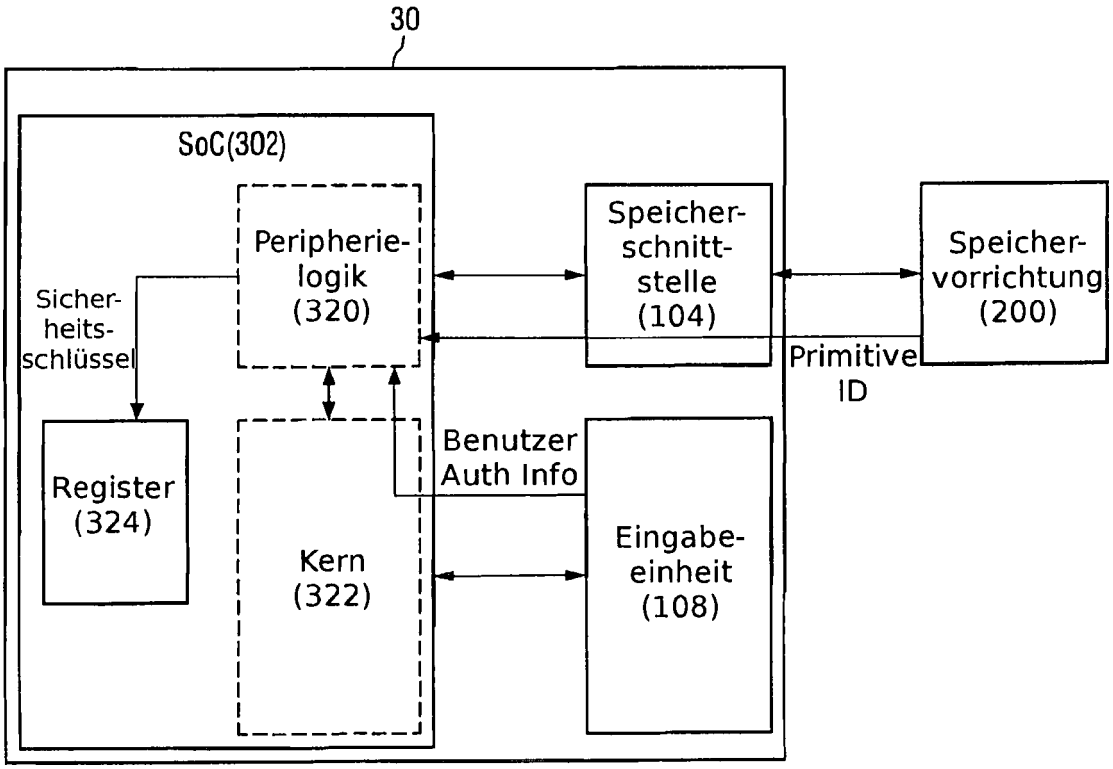

30
SoC(302)
Peripherie-logik (320)
Speicher-schnitt-stelle (104)
Speicher-vorrichtung (200)
Sicher-heits-schlüssel
Primitive ID
Register (324)
Benutzer Auth Info
Kern (322)
Eingabe-einheit (108)

FIG. 9

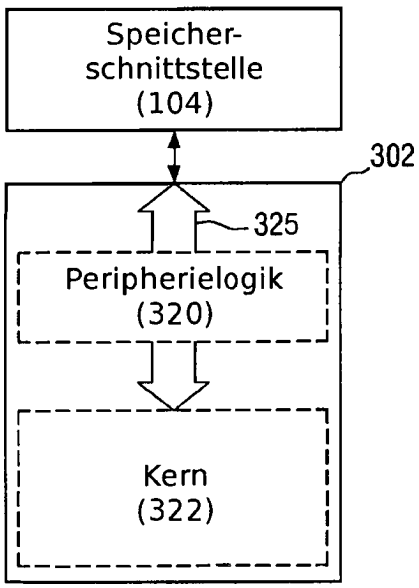

Speicher-
schnittstelle
(104)
302
325
Peripherielogik
(320)
Kern
(322)

FIG. 10

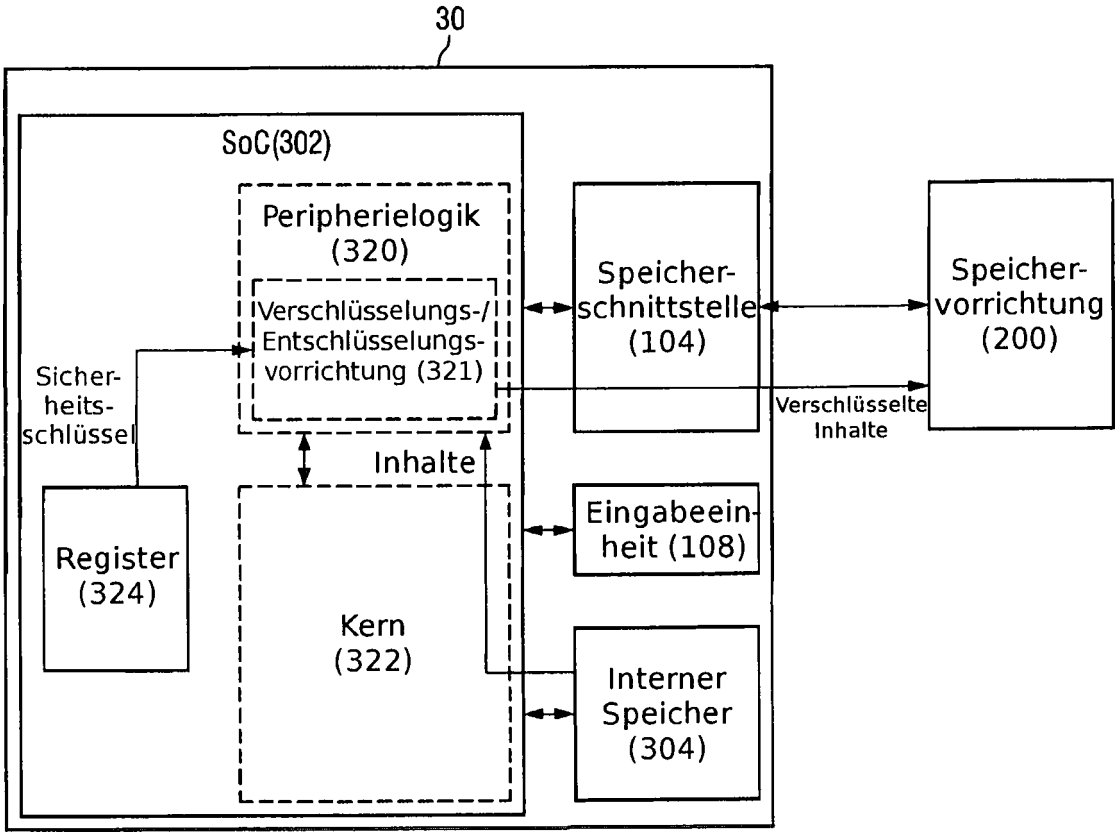

30
SoC(302)
Peripherielogik (320)
Verschlüsselungs-/ Entschlüsselungs-vorrichtung (321)
Sicher-heits-schlüssel
Register (324)
Inhalte
Kern (322)
Speicher-schnittstelle (104)
Speicher-vorrichtung (200)
Verschlüsselte Inhalte
Eingabeein-heit (108)
Interner Speicher (304)

FIG. 11

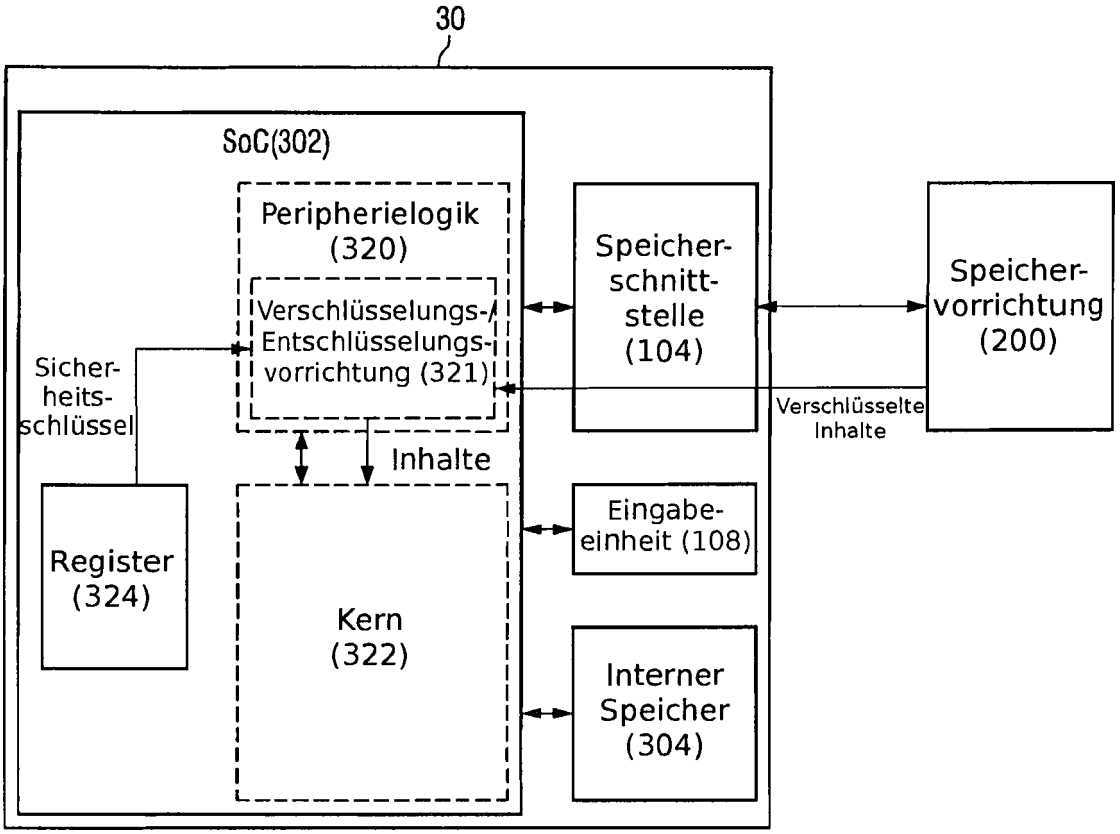

30
SoC(302)
Peripherielogik (320)
Verschlüsselungs-/ Entschlüsselungs-vorrichtung (321)
Sicher-heits-schlüssel
Inhalte
Register (324)
Kern (322)
Speicher-schnitt-stelle (104)
Speicher-vorrichtung (200)
Verschlüsselte Inhalte
Eingabe-einheit (108)
Interner Speicher (304)

FIG. 12

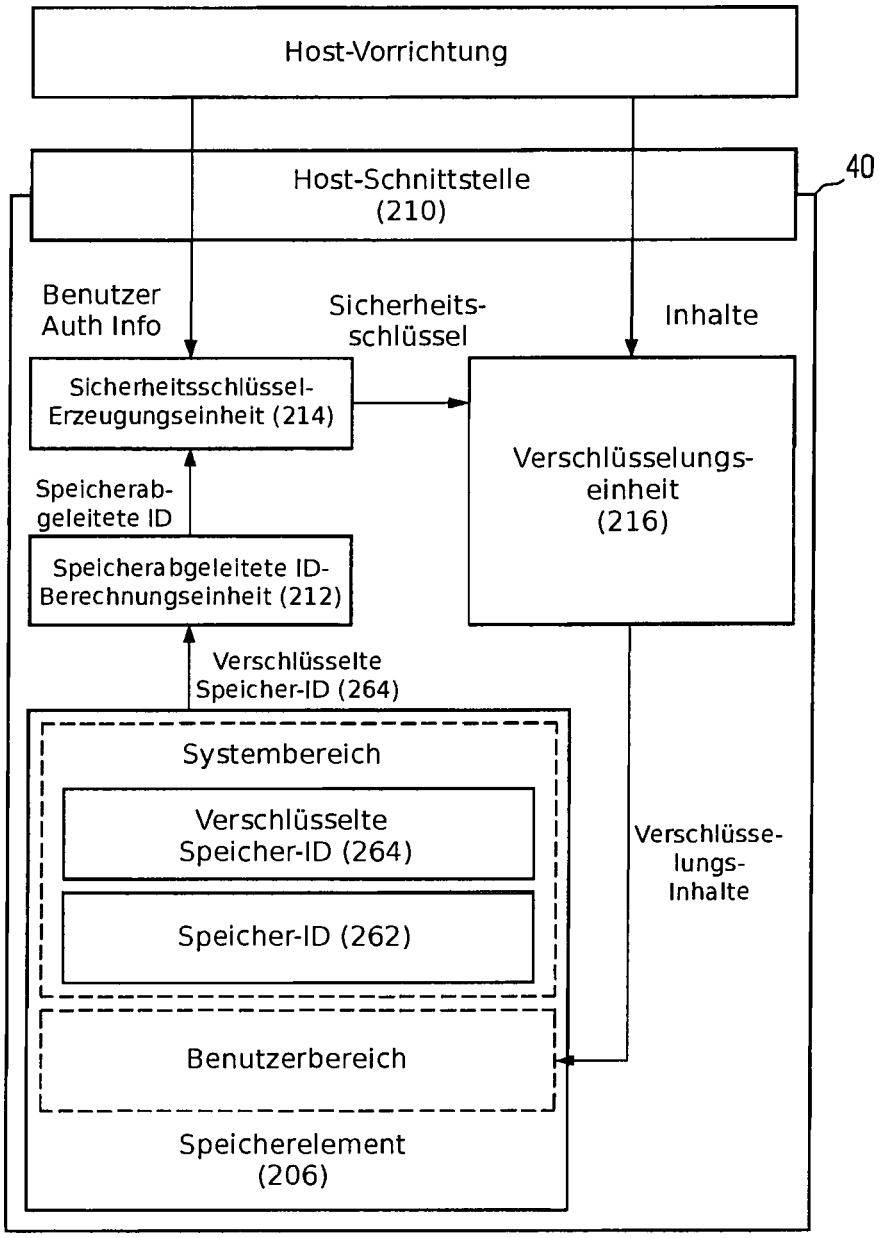

Host-Vorrichtung
Host-Schnittstelle (210)
40
Benutzer Auth Info
Sicherheits-schlüssel
Inhalte
Sicherheitsschlüssel-Erzeugungseinheit (214)
Verschlüsselungs-einheit (216)
Speicherab-geleitete ID
Speicherabgeleitete ID-Berechnungseinheit (212)
Verschlüsselte Speicher-ID (264)
Systembereich
Verschlüsselte Speicher-ID (264)
Speicher-ID (262)
Verschlüsse-lungs-Inhalte
Benutzerbereich
Speicherelement (206)

FIG. 13

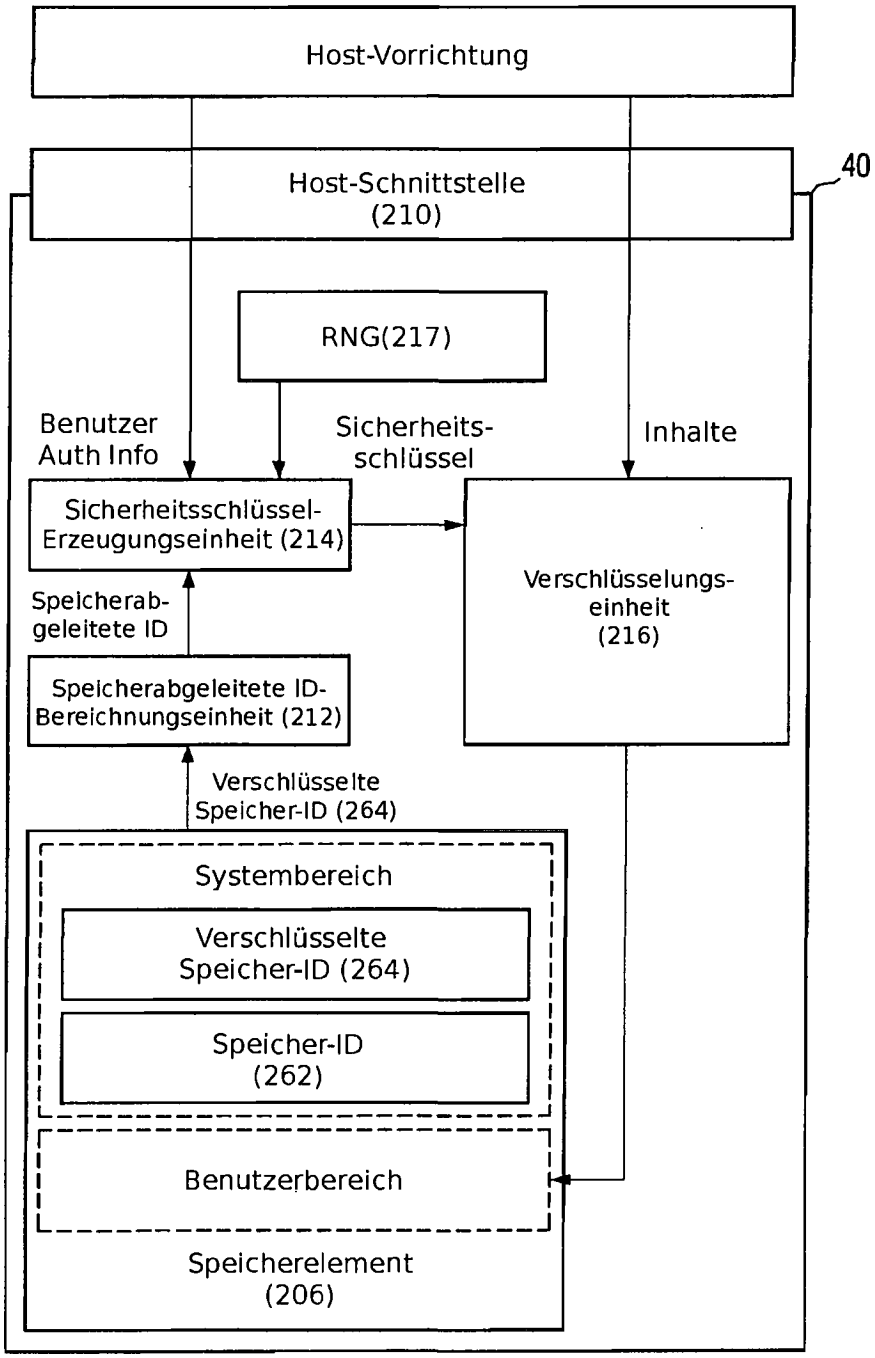

Host-Vorrichtung
Host-Schnittstelle (210)
40
RNG(217)
Benutzer Auth Info
Sicherheits-schlüssel
Inhalte
Sicherheitsschlüssel-Erzeugungseinheit (214)
Verschlüsselungs-einheit (216)
Speicherab-geleitete ID
Speicherabgeleitete ID-Bereichnungseinheit (212)
Verschlüsselte Speicher-ID (264)
Systembereich
Verschlüsselte Speicher-ID (264)
Speicher-ID (262)
Benutzerbereich
Speicherelement (206)

FIG. 14

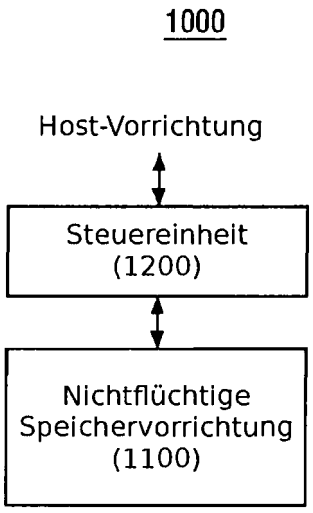

1000
Host-Vorrichtung
Steuereinheit
(1200)
Nichtflüchtige
Speichervorrichtung
(1100)

FIG. 15

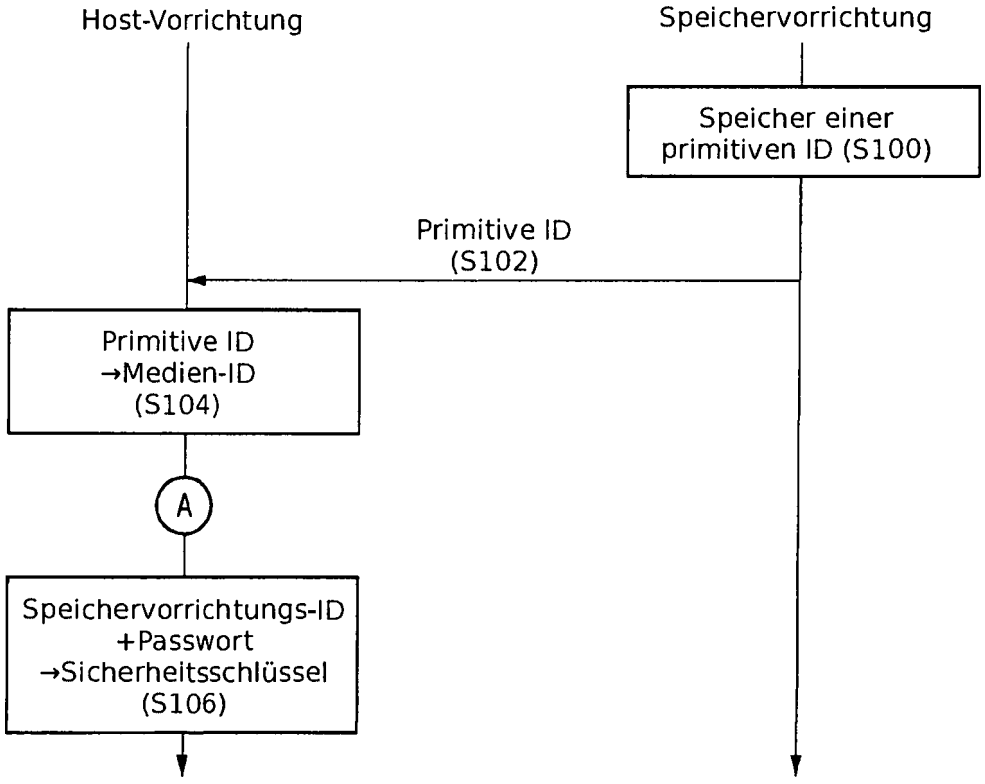

Host-Vorrichtung
Speichervorrichtung
Speicher einer
primitiven ID (S100)
Primitive ID
(S102)
Primitive ID
→Medien-ID
(S104)
A
Speichervorrichtungs-ID
+Passwort
→Sicherheitsschlüssel
(S106)

FIG. 16

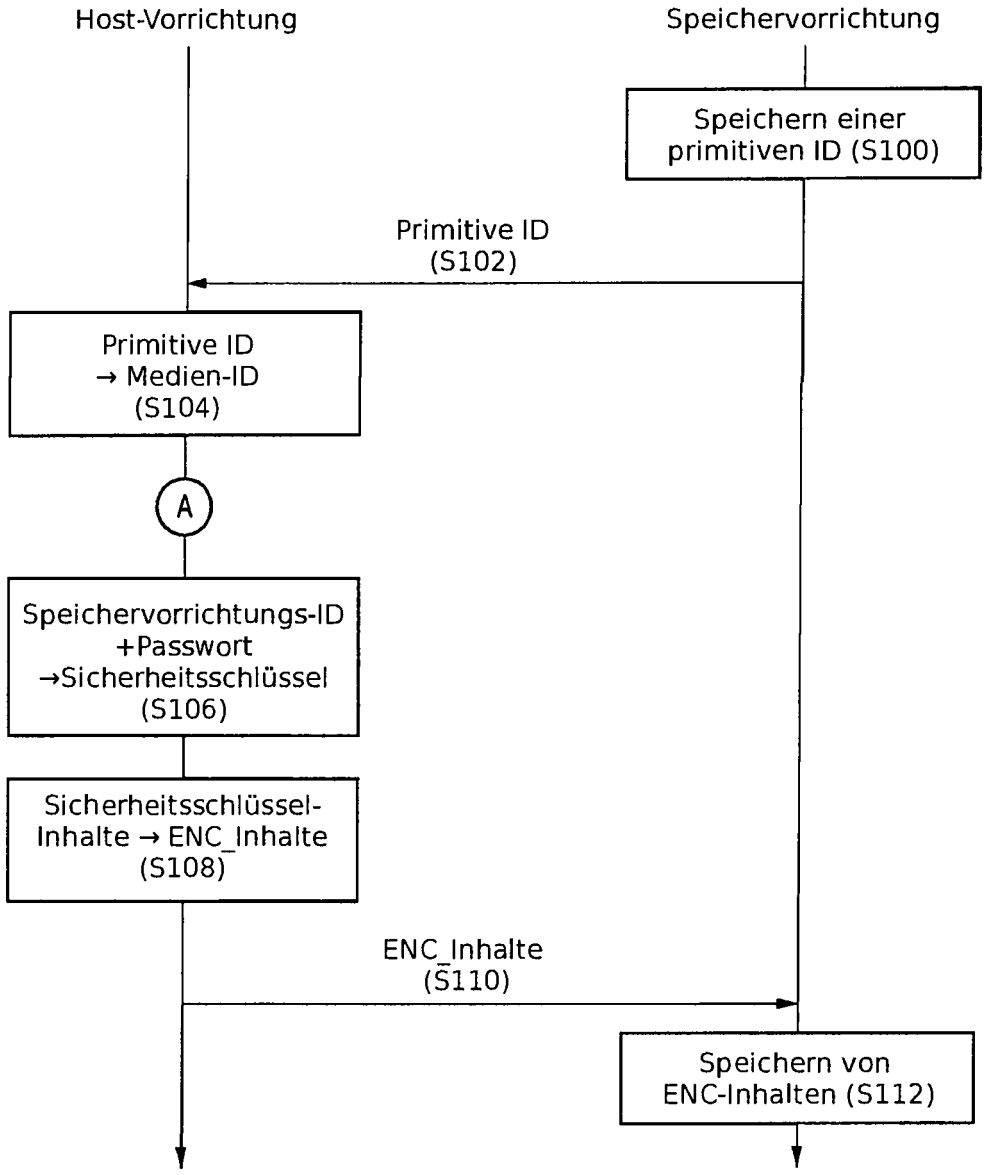

Host-Vorrichtung
Speichervorrichtung
Speichern einer primitiven ID (S100)
Primitive ID (S102)
Primitive ID → Medien-ID (S104)
A
Speichervorrichtungs-ID +Passwort →Sicherheitsschlüssel (S106)
Sicherheitsschlüssel-Inhalte → ENC_Inhalte (S108)
ENC_Inhalte (S110)
Speichern von ENC-Inhalten (S112)

FIG. 17

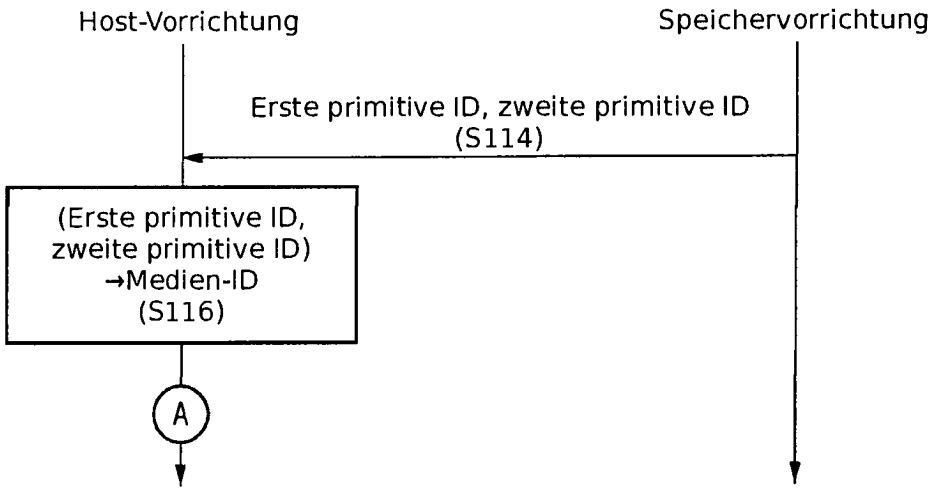

Host-Vorrichtung
Speichervorrichtung
Erste primitive ID, zweite primitive ID
(S114)
(Erste primitive ID,
zweite primitive ID)
→Medien-ID
(S116)
A

FIG. 18

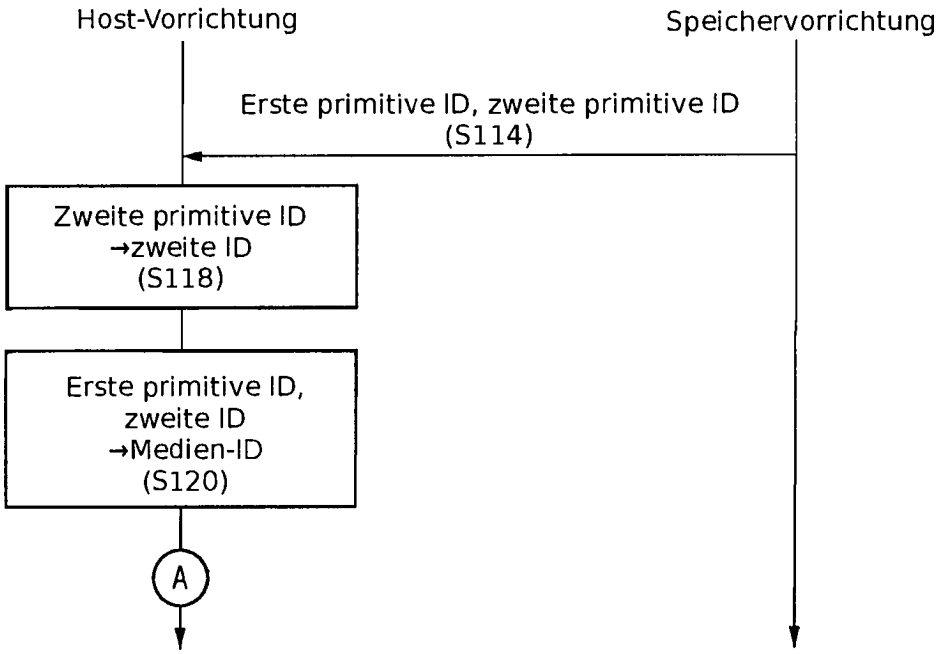

Host-Vorrichtung
Speichervorrichtung
Erste primitive ID, zweite primitive ID
(S114)
Zweite primitive ID
→zweite ID
(S118)
Erste primitive ID,
zweite ID
→Medien-ID
(S120)
A

FIG. 19

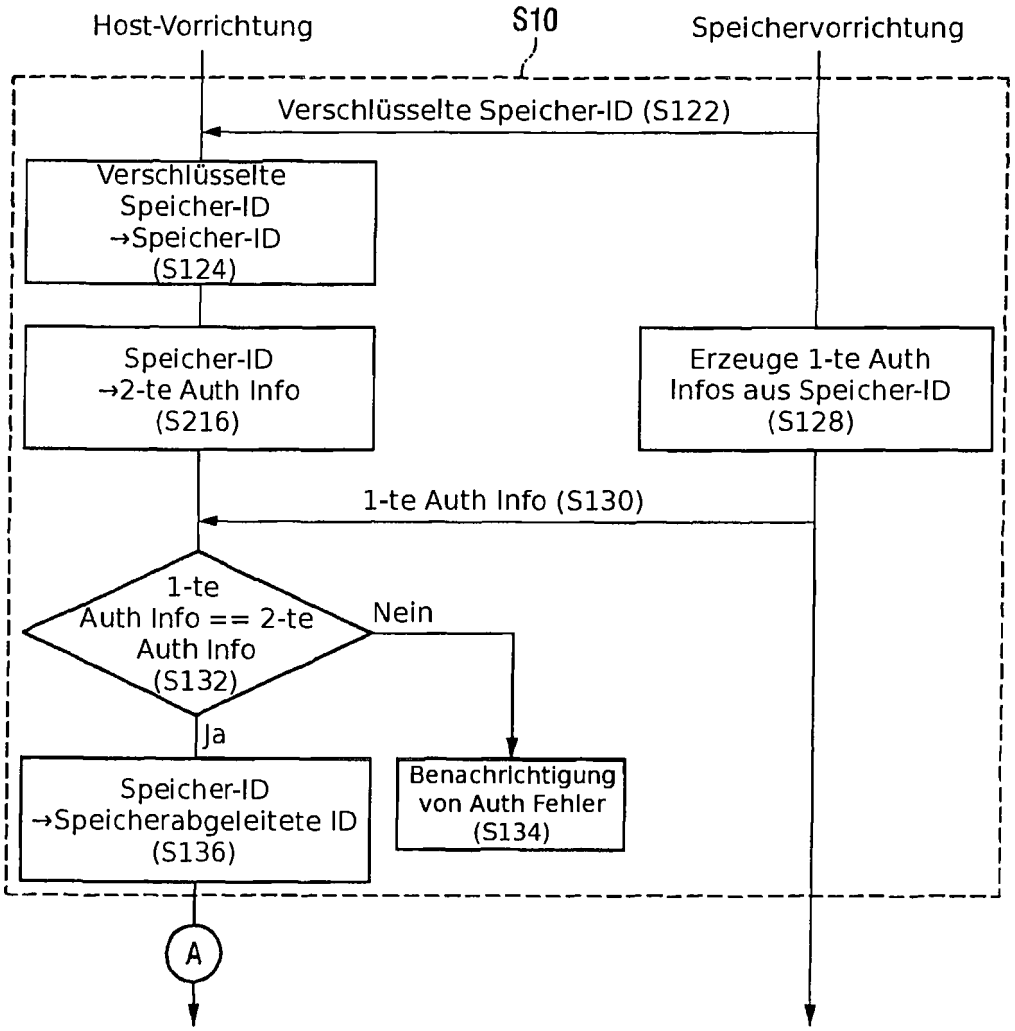

Host-Vorrichtung
S10
Speichervorrichtung
Verschlüsselte Speicher-ID (S122)
Verschlüsselte Speicher-ID →Speicher-ID (S124)
Speicher-ID →2-te Auth Info (S216)
Erzeuge 1-te Auth Infos aus Speicher-ID (S128)
1-te Auth Info (S130)
1-te Auth Info == 2-te Auth Info (S132)
Nein
Ja
Speicher-ID →Speicherabgeleitete ID (S136)
Benachrichtigung von Auth Fehler (S134)
A

FIG. 20

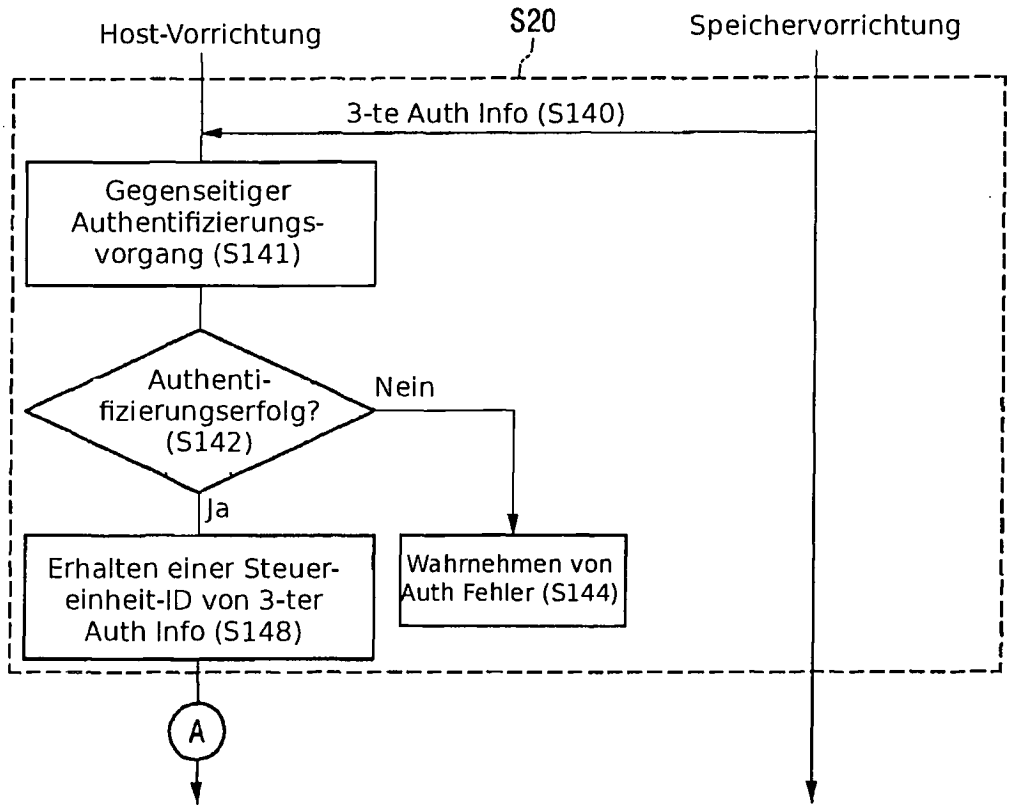

Host-Vorrichtung
S20
Speichervorrichtung
3-te Auth Info (S140)
Gegenseitiger Authentifizierungs-vorgang (S141)
Authenti-fizierungserfolg? (S142)
Nein
Ja
Erhalten einer Steuer-einheit-ID von 3-ter Auth Info (S148)
Wahrnehmen von Auth Fehler (S144)
A

FIG. 21

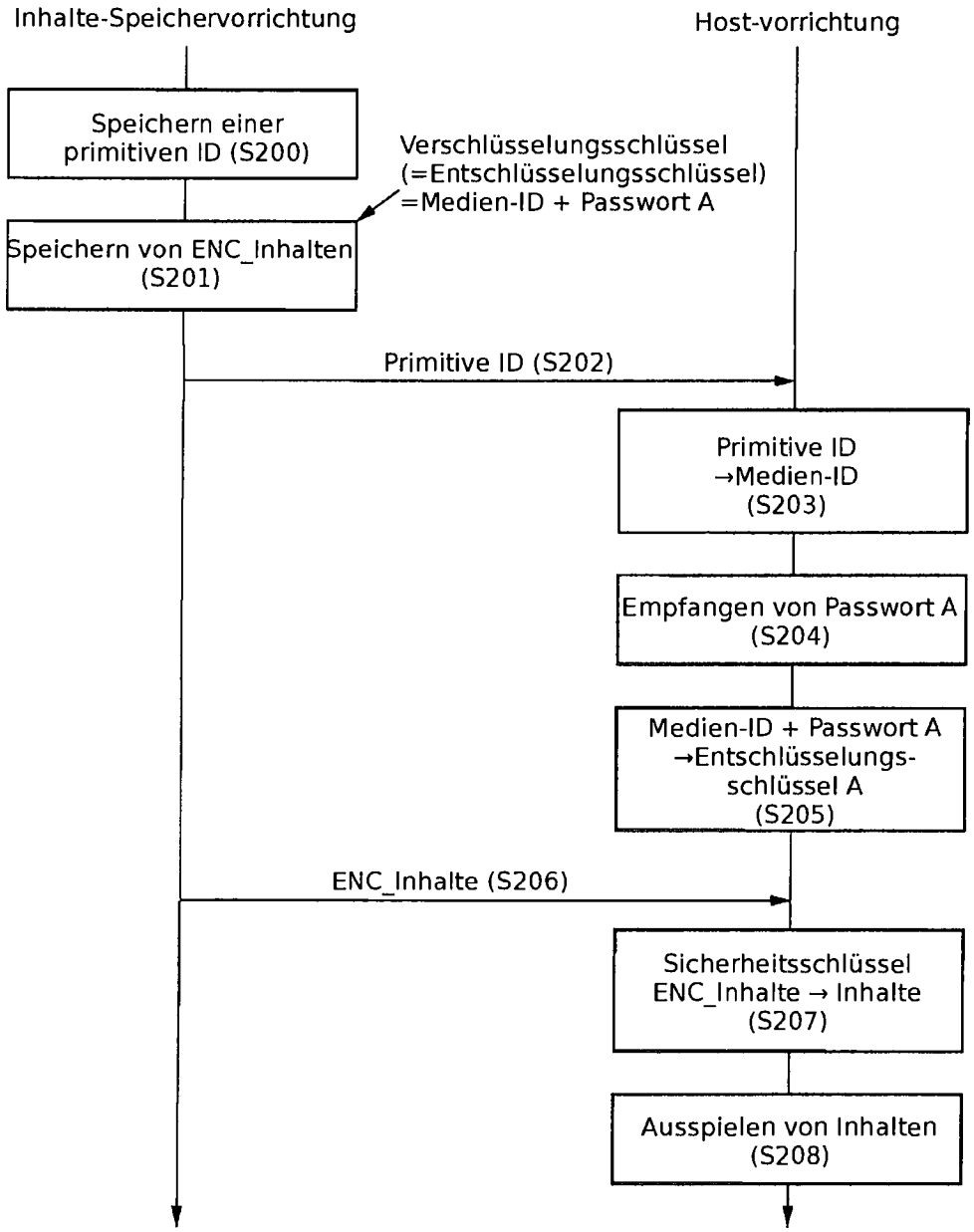

Inhalte-Speichervorrichtung
Host-vorrichtung
Speichern einer primitiven ID (S200)
Verschlüsselungsschlüssel (=Entschlüsselungsschlüssel) =Medien-ID + Passwort A
Speichern von ENC_Inhalten (S201)
Primitive ID (S202)
Primitive ID →Medien-ID (S203)
Empfangen von Passwort A (S204)
Medien-ID + Passwort A →Entschlüsselungs-schlüssel A (S205)
ENC_Inhalte (S206)
Sicherheitsschlüssel ENC_Inhalte → Inhalte (S207)
Ausspielen von Inhalten (S208)

FIG. 22

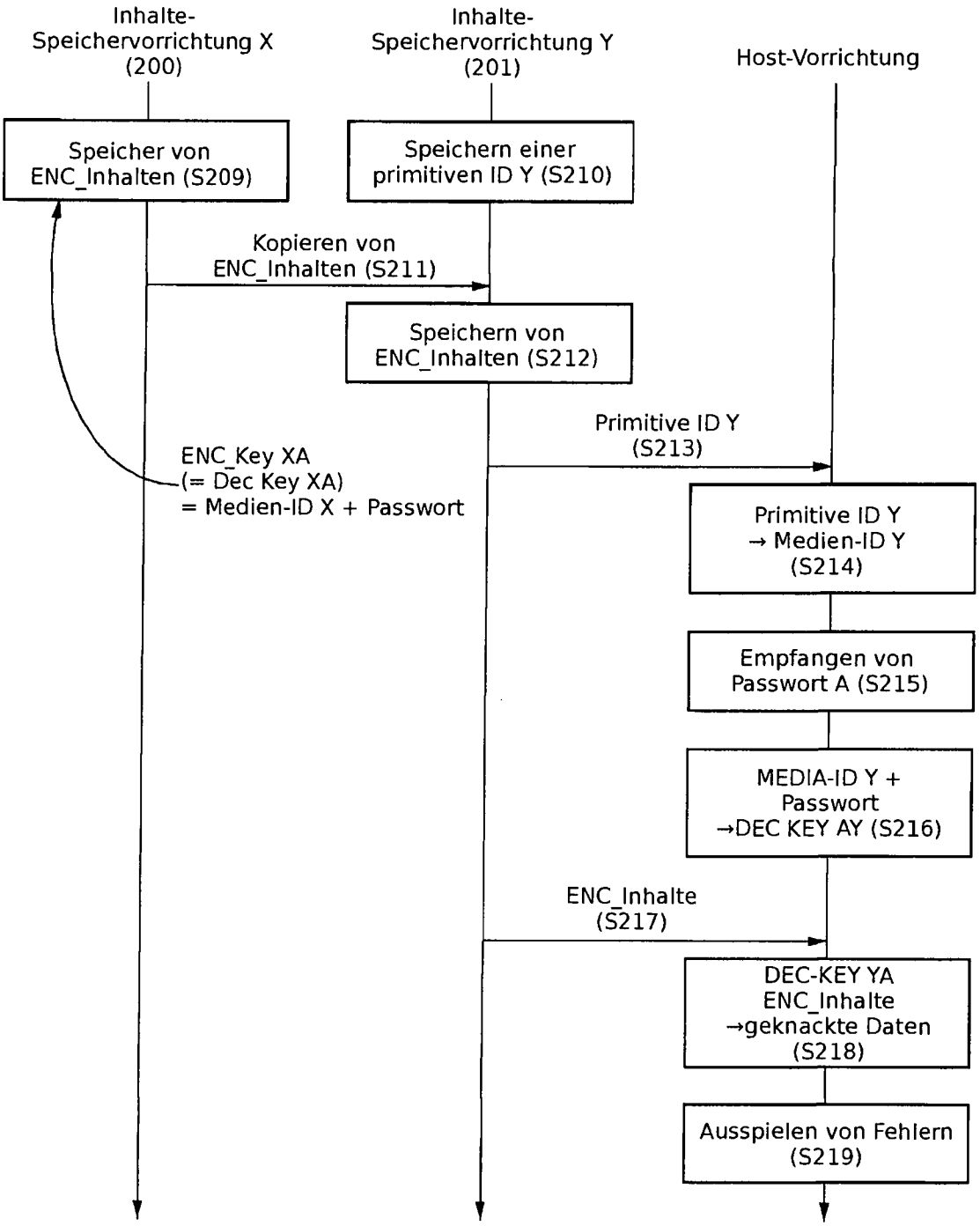
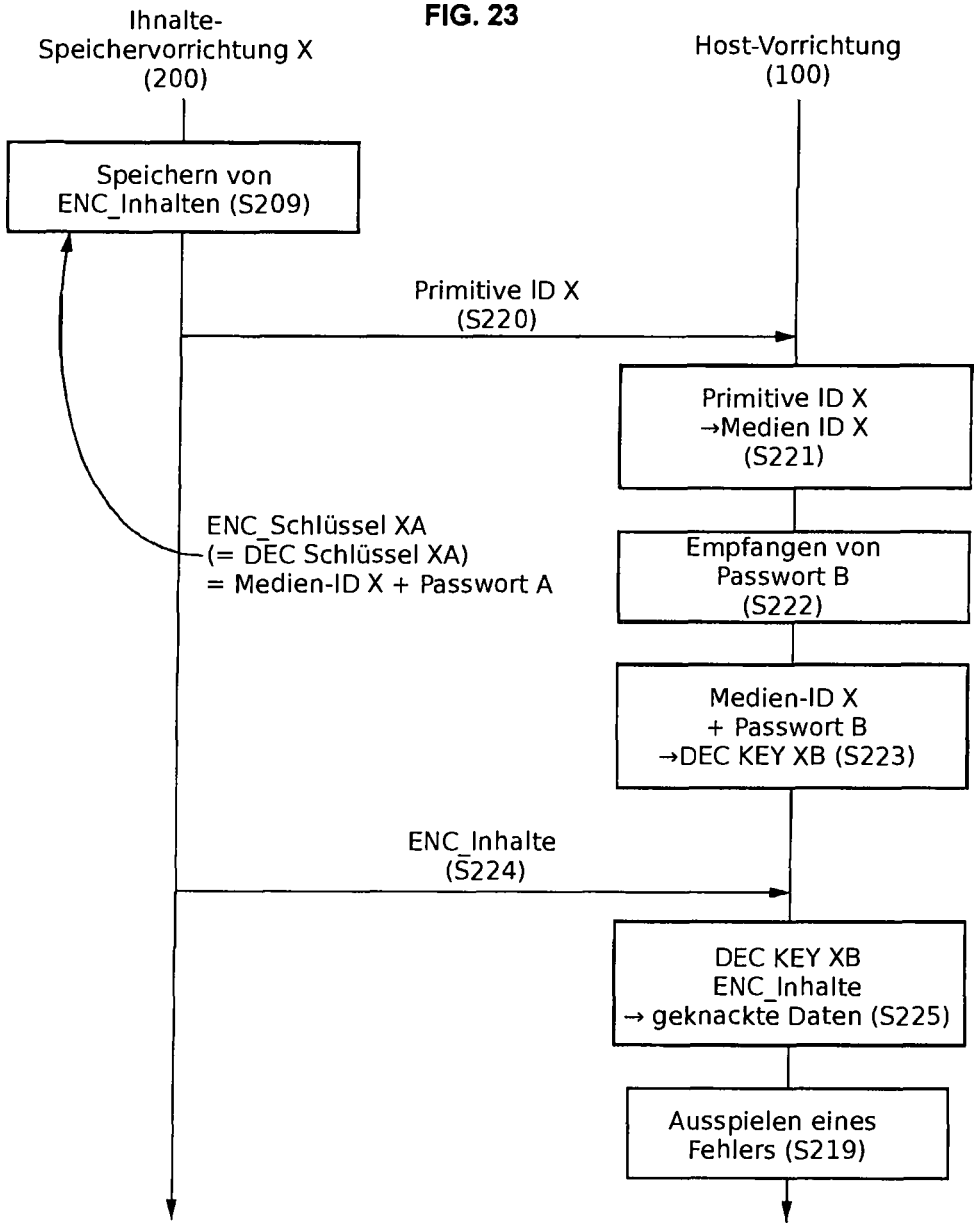

Inhalte-Speichervorrichtung X (200)
Inhalte-Speichervorrichtung Y (201)
Host-Vorrichtung
Speicher von ENC_Inhalten (S209)
Speichern einer primitiven ID Y (S210)
Kopieren von ENC_Inhalten (S211)
Speichern von ENC_Inhalten (S212)
Primitive ID Y (S213)
ENC_Key XA (= Dec Key XA) = Medien-ID X + Passwort
Primitive ID Y → Medien-ID Y (S214)
Empfangen von Passwort A (S215)
MEDIA-ID Y + Passwort →DEC KEY AY (S216)
ENC_Inhalte (S217)
DEC-KEY YA ENC_Inhalte →geknackte Daten (S218)
Ausspielen von Fehlern (S219)

FIG. 23


Ihnalte-
Speichervorrichtung X
(200)
Host-Vorrichtung
(100)
Speichern von
ENC_Inhalten (S209)
Primitive ID X
(S220)
Primitive ID X
→Medien ID X
(S221)
ENC_Schlüssel XA
(= DEC Schlüssel XA)
= Medien-ID X + Passwort A
Empfangen von
Passwort B
(S222)
Medien-ID X
+ Passwort B
→DEC KEY XB (S223)
ENC_Inhalte
(S224)
DEC KEY XB
ENC_Inhalte
→ geknackte Daten (S225)
Ausspielen eines
Fehlers (S219)