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

(10) **DE 698 33 608 T2** 2007.02.15

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 0 874 300 B1**
(21) Deutsches Aktenzeichen: **698 33 608.9**
(96) Europäisches Aktenzeichen: **98 303 007.3**
(96) Europäischer Anmeldetag: **20.04.1998**
(97) Erstveröffentlichung durch das EPA: **28.10.1998**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **01.03.2006**
(47) Veröffentlichungstag im Patentblatt: **15.02.2007**

(51) Int Cl.[8]: ***G06F 21/00*** (2006.01)
G11B 19/04 (2006.01)
G11B 19/12 (2006.01)
G11B 20/00 (2006.01)

(30) Unionspriorität:

10610497	**23.04.1997**	**JP**
14369997	**02.06.1997**	**JP**
21089997	**05.08.1997**	**JP**

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

(73) Patentinhaber:
Sony Corp., Tokio/Tokyo, JP

(74) Vertreter:
Mitscherlich & Partner, Patent- und Rechtsanwälte, 80331 München

(72) Erfinder:
Ishiguro, Ryuji, Shinagawa-ku,Tokyo 141, JP;
Osawa, Yoshitomo, Shinagawa-ku,Tokyo 141, JP;
Osakabe, Yoshio, Shinagawa-ku,Tokyo 141, JP;
Sato, Makoto, Shinagawa-ku,Tokyo 141, JP

(54) Bezeichnung: **Informationsübertragung,-empfang und -aufzeichnung**

Beschreibung

[0001] Die vorliegende Erfindung bezieht sich auf eine Informationsübertragungsvorrichtung und -verfahren, auf eine Informationsempfangsvorrichtung und -verfahren, und auf einen Aufzeichnungsträger. Beispiele von Ausführungsformen der Erfindung beziehen sich auf ein Verfahren und auf einen Aufzeichnungsträger, wobei zugelassen wird, dass Daten mit einem höheren Sicherheitsgrad ausgetauscht werden können.

[0002] In den vergangenen Jahren wurde ein System vorgeschlagen, welches Teile elektronischer Geräte aufweist, beispielsweise AV-Vorrichtungen und Personalcomputer, die miteinander über übliche IEEE 1394-Seriell-Busse verbunden sind, wobei Daten unter den Geräteteilen ausgetauscht werden können.

[0003] Bei einem derartigen System kann der übliche Benutzer eine Bewegtbildinformation unter Verwendung eines DVD-Wiedergabegeräts wiedergeben und überträgt die Information zu einem Monitor über einen 1394-Seriell-Bus, um diese auf einem Monitor anzuzeigen. Die Handhabung, die durch den Benutzer ausgeführt wird, die Bewegtbildinformation anzuzeigen, wird durch den Urheber der Bewegtbildinformation normalerweise über eine Lizenz automatisch gestattet, die erhalten wurde, wenn der Benutzer die DVD der Bewegtbildinformation erworben hat. Um eine Handhabung durchzuführen, die Bewegtbildinformation, die vom DVD-Wiedergabegerät wiedergegeben wird, auf einen anderen Aufzeichnungsträger, beispielsweise eine optische Magnetplatte zu kopieren, ist es jedoch für den Benutzer erforderlich, eine spezielle Erlaubnis vom Urheber der Bewegtbildinformation zu erlangen. Im Fall einer Kopierlizenz wird üblicherweise die optische Magnetplattenvorrichtung auch dazu verwendet, einen Schlüssel zu speichern, um zu zeigen, ob das Aufzeichnen der Bewegtbildinformation auf eine optische Magnetplatte, die in der Vorrichtung befestigt ist, erlaubt ist oder nicht. Das heißt, dass der Schlüssel dazu verwendet wird, eine Beurteilung zu bilden, ob oder nicht die optische Magnetplattenvorrichtung eine berechtigte Vorrichtung ist, d.h., eine Vorrichtung, die durch den Urheber der Information lizenziert ist. Wenn die optische Magnetplattenvorrichtung als eine berechtigte Vorrichtung bestätigt wird, kann die Handlung, die Bewegtbildinformation auf der Vorrichtung aufzuzeichnen, so beurteilt werden, eine zugelassene Handhabung zu sein.

[0004] In einem solchen Fall ist es notwendig, zu verifizieren, ob die Bestimmungsvorrichtung eine berechtigte Vorrichtung bei einer Übertragung von Information von einer Vorrichtung ist, welche die Information zu einer Vorrichtung überträgt, welche die Information, d.h., die Bestimmungsvorrichtung empfängt. Es sei angemerkt, dass die Informationsübertragungsvorrichtung und die Informationsempfangsvorrichtung anschließend als Quelle bzw. als Senke bezeichnet werden.

[0005] Fig. 41 ist ein Diagramm, welches ein übliches Verfahren zur Bestätigung einer Bestimmungsvorrichtung zeigt. Wie in der Figur gezeigt ist, wird der Quelle und der Senke jeweils eine vorherbestimmte Funktion f vorher durch den Urheber gegeben. Wenn in einem Speicher die Quelle und die Senke gespeichert sind, ist es schwierig, die Funktion f von dessen Eingang und Ausgang zu identifizieren. Außerdem ist es schwierig für eine Person, welche die Funktion f nicht kennt, zwischen ein Ausgangssignal, welches durch die Funktion f erzeugt wird, und ein Eingangssignal in Bezug auf die Funktion f einzugreifen. Die Funktion f ist lediglich für eine Vorrichtung, die durch den Urheber lizenziert ist, vorgesehen und darin gespeichert.

[0006] Die Quelle erzeugt eine Zufallszahl r und überträgt die Zahl r zur Senke über einen 1394-Seriellbus. Die Quelle wendet außerdem die Funktion f auf die Zufallszahl r an, wobei eine Zahl x (= f (r)) erzeugt wird.

[0007] Wenn die Zufallszahl r von der Quelle empfangen wird, wendet die Senke die Funktion f auf die Zufallszahl r an, wobei eine Zahl y (= f(r)) erzeugt wird. Die Senke überträgt dann die Zahl y zur Quelle.

[0008] Die Quelle vergleicht dann die berechnete Zahl x mit der Zahl y, welche von der Senke empfangen wird, um eine Beurteilung zu bilden, ob die erstere gleich der letzteren (x = y) ist oder nicht. Wenn herausgefunden wird, dass die Zahl x gleich der Zahl y ist, beurteilt die Quelle, dass die Senke eine berechtigte Vorrichtung ist. In diesem Fall wird die Bewegtbildinformation unter Verwendung eines vorher festgelegten Schlüssels verschlüsselt, bevor diese zur Senke übertragen wird.

[0009] Als Schlüssel wird ein Wert k, der durch Anwenden der Funktion f auf die Zahl y erzeugt wird, welche durch die Quelle von der Senke f empfangen wird, verwendet (k = f(y)). Aus dem gleichen Grund wendet die Senke außerdem die Funktion f auf die Zahl y an, um den Wert k (= f (y)) zu erzeugen. Der Wert k wird dann im Gegensatz dazu als Schlüssel verwendet, um die verschlüsselte Bewegtbildinformation zu entschlüsseln.

[0010] Bei diesem Verfahren ist es jedoch für alle elektronischen Geräte notwendig, die als Quellen und Senken zum Übertragen und Empfangen von Information verwendet werden, entsprechend eine gleich bleibende Funktion f streng geheim zu halten.

[0011] Wenn als Ergebnis die Funktion f, die in ei-

nem elektronischen Gerät gehalten wird, beispielsweise durch einen nicht berechtigten Benutzer gestohlen wird, ist der nichtberechtigte Benutzer in der Lage, einen Schlüssel k zu erzeugen, wobei er Daten, welche über einen 1394-Seriell-Bus ausgetauscht werden, überwacht, und folglich ist er in der Lage, verschlüsselte Daten zu interpretieren oder zu entschlüsseln. Auf diese Weise ist der nichtberechtigte Benutzer in der Lage, illegal Information zu stehlen, indem er als berechtigter Benutzer unter Verwendung eines gewünschten elektronischen Geräts auftritt.

[0012] Die EP 0 686 973 A1 offenbart eine Datenwiedergabeeinrichtung und einen Datenaufzeichnungsträger, mit denen synchrone Reproduktion von Multiplexdaten von Videodaten, Audiodaten und Bildschirmdaten, die mit variablen Datenraten und mit verschiedenen Funktionsarten komprimiert sind, erzielt werden kann.

[0013] Merkmale der Erfindung sind in den Patentansprüchen angegeben, auf die aufmerksam gemacht wird.

[0014] Ausführungsformen der vorliegenden Erfindung suchen anschließend beispielsweise, die Sicherheit von übertragener Information weiter zu verbessern, indem ein nichtberechtigter Benutzer daran gehindert wird, als berechtigter Benutzer aufzutreten, wobei ein gewünschtes elektronisches Gerät verwendet wird, sogar, wenn Daten, die zum Verschlüsseln oder Entschlüsseln der Information erforderlich sind, durch einen nichtberechtigten Benutzer gestohlen werden.

[0015] Die vorliegende Erfindung wird deutlicher und wird daher schneller gewürdigt, da diese besser aus einem Studium der folgenden beispielhaften Beschreibung von einigen bevorzugten Ausführungsformen mit Hilfe der beiliegenden Zeichnungen verstanden wird, in denen:

[0016] Fig. 1 ein Blockdiagramm ist, welches einen typischen Aufbau eines Informationsverarbeitungssystems zeigt, für das eine Ausführungsform der vorliegenden Erfindung angewandt wird;

[0017] Fig. 2 ein Blockdiagramm ist, welches einen typischen Detailaufbau eines DVD-Wiedergabegeräts **1**, eines Personalcomputers **2** und eines optischen Magnetplattengeräts **3** bei dem Informationsverarbeitungssystem zeigt, welches in Fig. 1 gezeigt ist;

[0018] Fig. 3 ein erläuterndes Diagramm ist, welches zur Beschreibung von Bestätigungsverarbeitung verwendet wird;

[0019] Fig. 4 ein Diagramm ist, welches eine Ausführungsform zeigt, die eine Bestätigungsprozedur beinhaltet, um die Bestätigungsverarbeitung, welche in Fig. 3 gezeigt ist, auszuführen;

[0020] Fig. 5 ein Diagrammn ist, welches das Format einer spezifischen Knoten-ID zeigt;

[0021] Fig. 6 ist ein Diagramm, welches eine weitere Ausführungsform zeigt, welche die Bestätigungsprozedur erfüllt;

[0022] Fig. 7 ein Diagramm ist, welches eine weitere Ausführungsform zeigt, die die Bestätigungsprozedur erfüllt;

[0023] Fig. 8 ein Diagramm ist, welches eine noch weitere Ausführungsform zeigt, welches die Bestätigungsprozedur erfüllt;

[0024] Fig. 9 ein Diagramm ist, welches eine noch weitere Ausführungsform zeigt, welche die Bestätigungsprozedur erfüllt;

[0025] Fig. 10 ein Blockdiagramm ist, welches eine Ausführungsform zeigt, welche ein Informationsverarbeitungssystem erfüllt, für welches eine Ausführungsform der vorliegenden Erfindung angewandt wird, wo eine Quelle verschlüsselte Daten zu mehreren Senken überträgt;

[0026] Fig. 11 ein Blockdiagramm ist, welches einen typischen Aufbau einer 1394-Schnittstelleneinheit **26** zeigt, die bei einem DVD-Wiedergabegerät **1** verwendet wird, welches als Quelle in dem in Fig. 10 gezeigten System dient;

[0027] Fig. 12 ein Blockdiagramm ist, welches einen typischen ausführlichen Aufbau der in Fig. 11 gezeigten 1394-Schnittstelleneinheit **26** zeigt;

[0028] Fig. 13 eine Blockdiagramm ist, welches einen typischen ausführlichen Aufbau eines LFSR **92** zeigt, welches in der 1394-Schnittstelleneinheit **26**, die in Fig. 12 gezeigt ist, verwendet wird;

[0029] Fig. 14 ein Blockdiagramm ist, welches einen konkreteren Aufbau des LFSR **72**, das in Fig. 13 gezeigt ist, zeigt;

[0030] Fig. 15 ein Blockdiagramm ist, welches einen typischen Aufbau einer 1394-Schnittstelleneinheit **36** zeigt, die in einer optischen Magnetplattenvorrichtung **3** verwendet wird, die als Senke im in dem Fig. 10 gezeigten System dient;

[0031] Fig. 16 ein Blockdiagramm ist, welches einen typischen ausführlichen Aufbau der in Fig. 15 gezeigten 1394-Schnittstelleneinheit **36** zeigt;

[0032] Fig. 17 ein Blockdiagramm ist, welches ei-

nen typischen Aufbau einer 1394-Schnittstelleneinheit **49** zeigt, welche in einem Personalcomputer **2** verwendet wird, der als weitere Senke im in Fig. 10 gezeigten System dient;

[0033] Fig. 18 ein Blockdiagramm ist, welches einen typischen ausführlichen Aufbau der 1304-Schnittstelleneinheit zeigt, welche in Fig. 17 gezeigt ist;

[0034] Fig. 19 ein Blockdiagramm ist, welches einen typischen Aufbau eines Anwendungsmoduls **61** zeigt, welches im Personalcomputer **2** verwendet wird, der als weitere Senke in dem in Fig. 10 gezeigten System dient;

[0035] Fig. 20 ein Blockdiagramm ist, welches einen typischen ausführlichen Aufbau des in Fig. 19 gezeigten Anwendungsmoduls **61** zeigt;

[0036] Fig. 21 ein Blockdiagramm ist, welches einen weiteren typischen ausführlichen Aufbau der 1394-Schnittstelleneinheit **26** zeigt, die in dem DVD-Wiedergabegerät **1** verwendet wird, welches als Quelle bei dem in Fig. 10 gezeigten System dient;

[0037] Fig. 22 ein Blockdiagramm ist, welches einen weiteren typischen ausführlichen Aufbau der 1394-Schnittstelleneinheit **36** zeigt, welche bei der optischen Magnetplattenvorrichtung **3** verwendet wird, die als Senke in dem in Fig. 10 gezeigten System dient;

[0038] Fig. 23 ein Blockdiagramm ist, welches einen weiteren typischen ausführlichen Aufbau der 1394-Schnittstelleneinheit **49** zeigt, die im Personalcomputer **2** verwendet wird, der als weitere Senke in dem in Fig. 10 gezeigten System dient;

[0039] Fig. 24 ein Blockdiagramm ist, welches einen weiteren typischen Aufbau des Anwendungsmoduls **61** zeigt, welches bei dem Personalcomputer **2** verwendet wird, der als weitere Senke in dem in Fig. 10 gezeigten System dient;

[0040] Fig. 25 ein Diagramm ist, welches eine noch weitere Ausführungsform zeigt, welche die Bestätigungsprozedur erfüllt;

[0041] Fig. 26 ein Diagramm ist, welches eine Fortsetzungsprozedur zur in Fig. 25 gezeigten Bestätigungsprozedur zeigt;

[0042] Fig. 27 ein Diagramm ist, welches eine alternative Fortsetzungsprozedur zur in Fig. 25 gezeigten Bestätigungsprozedur zeigt;

[0043] Fig. 28 ein Blockdiagramm ist, welches dem Aufbau einer anderen Ausführungsform zeigt, die ein Informationsverarbeitungssystem erfüllt, bei dem eine Ausführungsform der vorliegenden Erfindung angewandt wird, wobei eine Quelle verschlüsselte Daten zu einer Senke überträgt;

[0044] Fig. 29 ein Blockdiagramm ist, welches einen Zufallszahlgenerator **903** oder **914** zeigt, welcher in der Quelle oder der Senke entsprechend in dem in Fig. 28 gezeigten System verwendet wird;

[0045] Fig. 30 ein Flussdiagramm zeigt, welches Arbeitsweisen darstellt, die durch eine Verarbeitungsschaltung **902** oder **913** ausgeführt werden, welche in der Quelle oder der Senke entsprechend in dem in Fig. 28 gezeigten System verwendet wird;

[0046] Fig. 31 ein Diagramm ist, welches eine noch weitere Ausführungsform zeigt, die die Bestätigungsprozedur erfüllt;

[0047] Fig. 32 ein Diagramm ist, welches das Format eines Pakets zeigt;

[0048] Fig. 33 ein Diagramm ist, welches eine noch weitere Ausführungsform zeigt, welche die Bestätigungsprozedur erfüllt;

[0049] Fig. 34 ein Blockdiagramm ist, welches einen typischen Aufbau eines CBC-Modus zeigt;

[0050] Fig. 35 ein Diagramm ist, welches eine noch weitere Ausführungsform zeigt, die die Bestätigungsprozedur erfüllt;

[0051] Fig. 36 ein Diagramm ist, welches eine noch weitere Ausführungsform zeigt, die die Bestätigungsprozedur erfüllt;

[0052] Fig. 37 ein Diagramm ist, welches eine noch weitere Ausführungsform zeigt, die die Bestätigungsprozedur erfüllt;

[0053] Fig. 38 ein Diagramm ist, welches eine noch weitere Ausführungsform zeigt, die die Bestätigungsprozedur erfüllt;

[0054] Fig. 39 ein Diagramm ist, welches eine noch weitere Ausführungsform zeigt, die die Bestätigungsprozedur erfüllt;

[0055] Fig. 40 ein Diagramm ist, welches eine noch weitere Ausführungsform zeigt, die die Bestätigungsprozedur erfüllt; und

[0056] Fig. 41 ein Diagramm ist, welches die übliche Bestätigungsprozedur zeigt.

[0057] Fig. 1 ist ein Blockdiagramm, welches einen typischen Aufbau eines Informationsverarbeitungssystems zeigt, für welches eine Ausführungsform der vorliegenden Erfindung angewandt wird. Wie in der

Figur gezeigt sind bei dem Aufbau ein DVD-Wiedergabegerät **1**, ein Personalcomputer **2**, eine optische Magnetplattenvorrichtung **3**, eine Daten-Sende-/Empfangsvorrichtung **4**, ein Monitor **5** und ein Fernsehempfänger **6** über einen IEEE 1394-Seriell-Bus **11** miteinander verbunden.

[0058] Fig. 2 ist ein Blockdiagramm, welches einen ausführlichen typischen Aufbau des DVD-Wiedergabegeräts **1**, des Personalcomputers **2** und der optischen Magnetplattenvorrichtung **3** bei dem in Fig. 1 gezeigten Informationsverarbeitungssystem zeigt. Das DVD-Wiedergabegerät **1** weist eine CPU **21**, eine ROM-Einheit **22**, eine RAM-Einheit **23**, eine Betätigungseinheit **24**, eine Ansteuerung **25**, eine 1394-Schnittstelleneinheit **26** und eine EEPROM-Einheit **27** auf, welche über einen internen Bus **28** miteinander verbunden sind. Wie in der Figur gezeigt, ist das DVD-Wiedergabegerät **1** über eine 1394-Schnittstelleneinheit **26** mit dem 1394-Seriell-Bus **11** verbunden. Die CPU **21** führt verschiedene Verarbeitungsarten aus, wobei ein Programm ausgeführt wird, welches in der ROM-Einheit **22** gespeichert ist. Die RAM-Einheit **23** wird zur genauen Speicherung von Information verwendet, beispielsweise Daten und das Programm, die durch CPU **21** beim Ausführen der Verarbeitung erforderlich sind. Die Betätigungseinheit **24** besitzt Komponenten, beispielsweise Tasten, Schalter und eine Fernsteuerung. Wenn der Benutzer die Betätigungseinheit **24** betätigt, wird ein Signal, welches die Betätigung zeigt, erzeugt. Die Ansteuerung **25** steuert eine DVD an, welche in der Figur nicht gezeigt ist, wobei Daten, welche auf der DVD aufgezeichnet sind, wiedergegeben werden. Die EEPROM-Einheit **27** wird dazu verwendet, Information zu speichern, welche zu speichern ist, sogar nachdem die Spannungsversorgung des DVD-Wiedergabegeräts **1** ausgeschaltet ist. Bei der vorliegenden Ausführungsform ist ein Beispiel einer solchen Information ein Verschlüsselungs-/Entschlüsselungsschlüssel. Der interne Bus **28** wird zum gegenseitigen Verbinden der CPU **21**, der ROM-Einheit **22**, der RAM-Einheit **23**, der Betätigungseinheit **24**, der Ansteuerung **25**, der 1394-Schnittstelleneinheit **26** und der EEPROM-Einheit **27** verwendet.

[0059] Ähnlich wie das DVD-Wiedergabegerät **1** besitzt die optische Magnetplattenvorrichtung **3** eine CPU **31**, eine ROM-Einheit **32**, eine RAM-Einheit **33**, eine Betätigungseinheit **34**, eine Ansteuerung **35**, eine 1394-Schnittstelleneinheit **36** und eine EEPROM-Einheit **37**, die miteinander über einen internen Bus **38** verbunden sind. Da die CPU **31** bis zum internen Bus **38** die gleichen Funktionen der CPU **21** zum internen Bus **28**, die bei dem DVD-Wiedergabegerät **1** verwendet werden, hat, wird eine Erläuterung dazu nicht wiederholt. Die einzige Ausnahme ist die, dass die Ansteuerung **35** eine optische Magnetplatte, welche in der Figur nicht gezeigt ist, anstelle einer DVD ansteuert. Die Ansteuerung **35** zeichnet Daten auf der optischen Magnetplatte auf und gibt diese davon wieder.

[0060] Zusätzlich zu einer CPU **41**, einer ROM-Einheit **42**, einer RAM-Einheit **43**, einer 1394-Schnittstelleneinheit **49** und einer EEPROM-Einheit **50**, welche miteinander über einen internen Bus **51** verbunden sind, weist der Personalcomputer **2** außerdem eine Eingangs/Ausgangs-Schnittstelleneinheit **44**, eine Tastatur **45**, eine Maus **46**, eine HDD (Festplatte) **47** und eine Erweiterungsschaltungsplatte **48** auf. Der Personalcomputer **2** ist über die 1394-Schnittstelleneinheit **49** mit dem 1394-Seriell-Bus **11** verbunden. Die CPU **41** führt verschiedene Verarbeitungsarten aus, wobei ein Programm ausgeführt wird, welches in der ROM-Einheit **42** gespeichert ist. Die RAM-Einheit **43** wird zur genauen Speicherung von Information verwendet, beispielsweise Daten und des Programms, welche durch die CPU **41** beim Ausführen der Verarbeitung erforderlich sind. Mit dem internen Bus **51** ist die Eingabe/Ausgabe-Schnittstelleneinheit **44** verbunden, die als Schnittstelle zwischen der CPU **41** und der Tastatur **45**, der Maus **46**, der HDD **47** und der Erweiterungsschaltung **48** dient. Die Eingabe-/Ausgabe-Schnittstelleneinheit **44** transportiert Signale, welche von der Tastatur **45** und der Maus **46** zugeführt werden, die mit der Schnittstelleneinheit **44** verbunden sind, weiter zur CPU **41** über den internen Bus **51**. Wenn die Eingabe-/Ausgabe-Schnittstelleneinheit **44** mit der HDD **47** verbunden ist, erlaubt sie es, dass Daten und ein Programm, welche vom internen Bus **51** kommen, auf der HDD **47** gespeichert werden, und dass im Gegensatz dazu Daten und ein Programm, welche der HDD **47** gespeichert sind, gelesen werden und zum internen Bus **41** weitergeleitet werden. Die Erweiterungsschaltung **48** ist mit der Eingangs-/Ausgangs-Schnittstelleneinheit **44** wenn notwendig verbunden, um notwendige Funktionen zuzulassen, die dem Personalcomputer **2** hinzuzufügen sind. Die EEPROM-Einheit **50** wird zum Speichern von Information verwendet, die zu speichern ist, sogar dann, wenn die Spannungsversorgung des Personalcomputers **2** abgeschaltet wird. Im Fall der vorliegenden Ausführungsform ist ein Beispiel einer solchen Information eine Vielzahl von Verschlüsselungs/Entschlüsselungs-Schlüssel. Der interne Bus **51** ist üblicherweise ein lokaler Bus, der durch einen PCI-Bus ausgeführt wird, um die CPU **41**, die ROM-Einheit **42**, die RAM-Einheit **43**, die 1394-Schnittstelleneinheit **49**, die EEPROM-Einheit **50** und die Eingangs/Ausgangsschnittstelleneinheit **44** miteinander zu verbinden.

[0061] Es sollte angemerkt sein, dass der interne Bus **51** in einer für den Benutzer offenen Architektur über die Eingangs-/Ausgangs-Schnittstelleneinheit **44** ausgebildet ist. Das heißt, dass es dem Benutzer erlaubt wird, eine zusätzliche Schaltungsplatte beispielsweise eine Erweiterungsplatte **48** mit der Eingangs-/Ausgangs-Schnittstelleneinheit **44** wenn er-

forderlich zu verbinden, und um ein Kundenprogramm für die zusätzliche Schaltung zu schreiben, welches im Personalcomputer **2** zu installieren ist. Die CPU **41** führt dann das Kundenprogramm aus, wobei die Daten mit der Erweiterungsplatte **48** über den internen Bus **51** passend ausgetauscht werden, um eine gewünschte Funktion auszuführen.

[0062] Bei einer elektronischen Konsumentenvorrichtung (CE), beispielsweise dem DVD-Wiedergabegerät **1** und der optischen Magnetplattenvorrichtung **3** sind deren interne Busse **28** und **38** nicht in einer für den Benutzer offenen Architektur ausgebildet. Somit ist der Benutzer nicht in der Lage, Daten, welche über den internen Bus **28** oder **38** übertragen werden, zu erwerben, wenn der interne Bus **28** oder **38** nicht speziell umgebildet wird.

[0063] Anschließend folgt eine Beschreibung der Verarbeitung der Bestätigung einer Senke, welche durch eine Quelle ausgeführt wird, unter Bezugnahme auf Fig. 3 und Fig. 4. Fig. 3 ist ein erläuterndes Diagramm, welches zum Beschreiben der Bestätigungsverarbeitung verwendet wird. Wie in der Figur gezeigt ist, wird die Verarbeitung üblicherweise durch Firmware **20** ausgeführt, die als Programm vorher in der ROM-Einheit **22** gespeichert ist, welche bei dem DVD-Wiedergabegerät **1** verwendet wird, welches als Quelle dient, um einen Lizenzmanager **62** zu bestätigen, welcher in der ROM-Einheit **42** gespeichert ist, welches als ein Programm durch die CPU **41** ausgeführt ist, welches im Personalcomputer **2** angewandt wird, der als Senke dient.

[0064] Fig. 4 ist ein Diagramm, welches eine Ausführungsform zeigt, bei der eine Prozedur ausgeführt wird, wodurch die Quelle, welche üblicherweise durch das DVD-Wiedergabegerät **1** erfüllt wird, die Senke bestätigt, welche üblicherweise durch den Personalcomputer **2** ausgeführt wird, wobei zugelassen wird, dass die Senke einen senkenseitigen-gemeinsamen Sitzungsschlüssel erzeugt, der den gleichen Wert hat wie der quellenseitige gemeinsame Sitzungsschlüssel, der durch Quelle erzeugt wird, lediglich dann, wenn die Senke eine berechtigte Senke ist. In der EEPROM-Einheit **27**, welche bei dem DVD-Wiedergabegerät **1** verwendet wird, werden ein Dienstschlüssel und eine Hash-Funktion vorher gespeichert. Der Dienstschlüssel und die Hash-Funktion werden durch einen Urheber einer Information für den Benutzer des DVD-Wiedergabegeräts **1** angegeben, der diese in der EEPROM-Einheit **27** streng geheim halten muss.

[0065] Der Urheber beliefert den Benutzer mit einem Dienstschlüssel für jeden Informationsabschnitt, welches durch den Urheber erzeugt wird. Der Dienstschlüssel wird wie ein Schlüssel verwendet, der für alle Vorrichtungen gemeinsam ist, die miteinander über den 1394-Seriell-Bus **11** verbunden sind, um ein System zusammenzusetzen. Es sollte angemerkt sein, dass bei der vorliegenden Ausführung der Ausdruck System verwendet wird, das gesamte System einzubeziehen, welches mehrere Vorrichtungen aufweist.

[0066] Die Hash-Funktion wird dazu verwendet, Eingangsdaten mit einer beliebigen Länge in Ausgangsdaten mit einer festen Länge, beispielsweise 64 Bits oder 128 Bits zu transformieren. Beispielsweise wird die Transformation durch y = hash (x) ausgedrückt, wo das Symbol x die Eingangsdaten in Bezug auf die Hash-Funktion sind, und das Symbol y die Daten sind, welche durch die Funktion ausgegeben werden. In diesem Fall ist Hash-Funktion eine komplexe Funktion, wo es schwierig ist, den Wert von x von einem gegebenen Wert y zu finden. Die Hash-Funktion ist eine solche komplizierte Funktion, dass es schwierig ist, ein Paar aus x1 und x2 herauszufinden, welches die Gleichung hash (x1) = hash (x2) zu erfüllen.

[0067] MD5 und SHA sind jeweils der Name einer Funktion, welche als eine repräsentative Einweg-Hash-Funktion bekannt ist. Für Details der Einweg-Hash-Funktion wird bezuggenommen auf einen Titel "Applied Cryptography" durch den Autor Bruce Schneider, wobei eine zweite Ausgabe durch Wiley veröffentlicht wurde.

[0068] Bei dem Personalcomputer **2**, der als typische Senke in dem in Fig. 4 gezeigten Beispiel verwendet wird, werden dagegen eine ID, welche für die elektronische Vorrichtung einmalig ist, d.h., den Personalcomputer **2** in diesem Fall, und ein Lizenzschlüssel, der vorher durch den Autor der Information bereitgestellt wird, streng geheim im EEPROM-Einheit **50** gespeichert. Diese einmalige Knoten-ID (Vorrichtungs-ID) wird normalerweise der elektronischen Vorrichtung durch den Hersteller des elektronischen Geräts wie später beschrieben wird zugeteilt. Der Lizenzschlüssel ist ein Wert, der von der Anwendung der Hash-Funktion auf (n + m)-Bit-Daten resultiert, welche durch Verkettung der n-Bit-ID mit dem m-Bit-Dienstschlüssel erlangt werden. Damit kann der Lizenzschlüssel durch die folgende Gleichung ausgedrückt werden:

Lizenzschlüssel = Hash (ID || Dienstschlüssel)

wobei die Bezeichnung "ID || Dienstschlüssel" eine Verkettung der ID mit dem Dienstschlüssel zeigt.

[0069] Eine einmalige Knoten-ID, welche durch Spezifikationen des 1394-Bus **11** bestimmt wird, kann üblicherweise als ID verwendet werden. Fig. 5 ist ein Diagramm, welches das Format der einmaligen Knoten-ID zeigt. Wie in der Figur gezeigt ist, weist die einmalige Knoten-ID 8 Bytes (oder 64 Bits) auf. Die ersten 3 Bytes werden durch die IEEE ge-

steuert und durch die IEEE einem Hersteller eines elektronischen Geräts als eine Zahl angegeben, die für den Hersteller einmalig ist. Dagegen können die niederwertigeren 5 Bytes durch den Hersteller des elektronischen Geräts selbst einem elektronischen Gerät, welches dem Benutzer verkauft wird, zugeteilt werden. Üblicherweise wird dieser Wert der gesamten niederwertigeren 5 Bytes durch den Hersteller des elektronischen Geräts einer elektronischen Vorrichtung als serielle Nummer der Vorrichtung zugeteilt. Da die höherwertigeren 3 Bytes einen Wert haben, der für den Hersteller des elektronischen Geräts einmalig ist, ist die einmalige Knoten-ID für alle elektronischen Vorrichtungen ohne Rücksicht darauf einmalig, ob die Vorrichtungen durch den gleichen Hersteller oder durch unterschiedliche Hersteller erzeugt wurden.

[0070] Wie in Fig. 4 gezeigt ist, beginnt die Prozedur mit einem Schritt S1, bei dem die Firmware **20** im DVD-Wiedergabegerät **1** die 1394-Schnittstelleneinheit **26** steuert, um eine Anforderung an den Personalcomputer **2** auf die ID zu führen, um diese über den 1394-Seriell-Bus **11** zu übertragen. Danach läuft die Prozedur weiter zu einem Schritt S2, bei dem ein Lizenzmanager **62** des Personalcomputers **2** die Anforderung nach der ID empfängt. Ausführlich ausgedrückt überträgt die 1394-Schnittstelleneinheit **49**, welche beim Personalcomputer **2** verwendet wird, die Anforderung nach der ID, welche durch das DVD-Wiedergabegerät über den 1394-Seriell-Bus **11** übertragen wird, zur CPU **41**. Die Prozedur läuft dann weiter zu einem Schritt S3, bei dem der Lizenzmanager **62**, der durch die CPU **41** ausgeführt wird, die ID aus der EEPROM-Einheit **50** gemäß der Anforderung liest, die zu diesem über die 1394-Schnittstelleneinheit **49** zugeführt wird, und überträgt die ID über die 1394-Schnittstelleneinheit **49** und den 1394-Seriell-Bus **11** zum DVD-Wiedergabegerät **1**.

[0071] Danach fährt die Prozedur zu einem Schritt S4 fort, bei dem die 1394-Schnittstelleneinheit **26**, welche bei dem DCD-Wiedergabegerät **1** verwendet wird, die ID empfängt und diese zur Firmware **20** weiterleitet, welche durch die CPU **21** ausgeführt wird.

[0072] Nachfolgend läuft die Prozedur weiter zu einem Schritt S5, bei dem die Firmware **20** die ID, welche vom Personalcomputer **2** empfangen wurde, mit einem Dienstschlüssel verkettet, der im EEPROM-Einheit **27** gespeichert ist, um Daten (ID || Dienstschlüssel) zu bilden. Danach wird ein Lizenzschlüssel lk durch Anwenden der Hash-Funktion auf die Daten (ID || Dienstschlüssel) berechnet, wie in der folgenden Gleichung gezeigt ist:

lk = hash (ID || Dienstschlüssel)

[0073] Die Prozedur läuft dann weiter zu einem Schritt S6, bei dem die Firmware **20** einen gemeinsamen quellenseitigen Sitzungsschlüssel sk erzeugt, wobei Details davon später beschrieben werden. Der quellenseitige gemeinsame Sitzungsschüssel sk wird als ein gemeinsamer Sitzungsschlüssel S sowohl durch das DVD-Wiedergabegerät **1**, um einen Klartext, der zu übertragen ist, als auch durch den Personalcomputer **2** verwendet, um einen verschlüsselten Text, der von dem DVD-Wiedergabegerät **1** empfangen wurde, zu entschlüsseln.

[0074] Danach läuft die Prozedur weiter zu einem Schritt S7, bei dem die Firmware **20** den quellenseitigen gemeinsamen Sitzungsschlüssel sk, der im Schritt S6 erzeugt wurde, unter Verwendung des Lizenzschlüssels lk verschlüsselt, der im Schritt S5 als ein Schlüssel berechnet wurde, um einen verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e gemäß der folgenden Gleichung zu erzeugen:

e = Enc (lk, sk)

[0075] Es sollte angemerkt sein, dass der Ausdruck Enc (A, B) auf der rechten Seite der obigen Gleichung ein gemeinsames Sitzungsverschlüsselungs-/Entschlüsselungsverfahren darstellt, wodurch Daten B unter Verwendung eines Schlüssels A verschlüsselt werden, um einen verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e auf der linken Seite der Gleichung zu erzeugen.

[0076] Anschließend läuft die Prozedur weiter zu einem Schritt S8, bei dem die Firmware **20** einen verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e, der im Schritt S7 erzeugt wurde, zum Personalcomputer **2** überträgt. Genauer ausgedrückt wird der verschlüsselte quellenseitige gemeinsame Sitzungsschlüssel e über die 1394-Schnittstelleneinheit **26**, die beim DVD-Wiedergabegerät **1** verwendet wird, über den 1394-Seriell-Bus **11** zum Personalcomputer **2** übertragen. Das Verfahren läuft dann weiter zu einem Schritt S9, bei dem die 1394-Schnittstelleneinheit **49**, die im Personalcomputer **2** verwendet wird, den verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e empfängt. Danach entschlüsselt der Lizenzmanager **62** den verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e, der diesem durch die 1394-Schnittstelleneinheit **49** zugeleitet wurde, unter Verwendung eines Lizenzschlüssels, der vorher durch den Urheber der Information bereitgestellt wurde und der im EEPROM **50** als Schlüssel gespeichert wurde, um einen senkseitigen gemeinsamen Sitzungsschlüssel sk' gemäß der folgenden Gleichung zu erzeugen:

sk' = Dec (Lizenzschlüssel, e)

[0077] Es sollte angemerkt sein, dass der Ausdruck Dec (A, B) auf der rechten Seite der obigen Gleichung das gemeinsame Sitzungsschlüssel-Verschlüsselungs-Entschlüsselungsverfahren zeigt, wo-

durch verschlüsselte Daten B in diesem Fall entschlüsselt werden, wobei ein Schlüssel A verschlüsselt wird, um einen senkseitigen gemeinsamen Sitzungsschlüssel sk' auf der linken Seite der Gleichung zu erzeugen.

[0078] Es sollte außerdem angemerkt sein, dass ein DES-Algorithmus als ein Datenverschlüsselungs-/Entschlüsselungsalgorithmus bekannt ist, der bei dem gemeinsamen Sitzungsschlüssel-Verschlüsselungs-/Entschlüsselungsverfahren angenommen wird, was ebenfalls ausführlich in der zweiten Ausgabe des Standes der Technik mit dem Titel "Applied Cryptographie", die oben aufgeführt wurde, beschrieben ist.

[0079] Der Lizenzschlüssel, der durch den Urheber der Information bereitgestellt wird und der in der EEPROM-Einheit **50** gespeichert ist, welche im Personalcomputer **2** vorher verwendet wurde, hat einen Wert, der durch den Urheber unter Verwendung der gleichen Hash-Funktion als Lizenz wie der Schlüssel lk durch das DVD-Wiedergabegerät 1 im Schritt S5 erzeugt wurde. Das heißt, dass die folgende Gleichung gilt:

lk = Lizenzschlüssel

[0080] Damit ist auf der Basis des gemeinsamen quellenseitigen Sitzungsschlüssel-Verschlüsselungs-/Entschlüsselungsverfahrens unter Verwendung des gleichen Schlüssels (Lizenz) die Verschlüsselung, welche durch den Personalcomputer **2** im Schritt S10 ausgeführt wird, unmittelbar ein Umkehrprozess der Verschlüsselung, welche durch das DVD-Wiedergabegerät im Schritt S7 ausgeführt wurde. Als Ergebnis ist, da e die verschlüsselten Daten des quellenseitigen gemeinsamen Sitzungsschlüssels sk sind, der durch das DVD-Wiedergabegerät 1 im Schritt S6 erzeugt wurde, der senkseitige gemeinsame Sitzungsschlüssel sk', der durch den Personalcomputer **2** berechnet wurde, d.h., ein Ergebnis der Entschlüsselung des verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssels e, gleich dem quellenseitigen gemeinsamen Sitzungsschlüssel sk. Das heißt, dass die folgende Gleichung gilt:

sk' = sk

[0081] Auf diese Weise können, da der quellenseitige und der senkseitige gemeinsame Sitzungsschlüssel sk und sk' die gleichen Werte haben, die Quelle, welche üblicherweise durch das DVD-Wiedergabegerät **1** ausgeführt wird, und die Senke, welche üblicherweise durch den Personalcomputer **2** ausgeführt wird, sich einen gemeinsamen Sitzungsschlüssel S anteilig aufteilen. Aus diesem Grund kann das DVD-Wiedergabegerät **1** den Schlüssel sk als einen Verschlüsselungsschlüssel unverändert verwenden, um einen Klartext zu verschlüsseln, der durch den Urheber erzeugt wurde, der zum Personalcomputer **2** zu übertragen ist. Aus dem gleichen Grund kann der Personalcomputer **2** den senkseitigen gemeinsamen Sitzungsschlüssel sk' als einen Entschlüsselungsschlüssel unverändert nutzen, um einen verschlüsselten Text, der durch das DVD-Wiedergabegerät **1** empfangen wurde, zu entschlüsseln. Als Alternative erzeugt das DVD-Wiedergabegerät **1** eine Pseudozufallzahl, die als Verschlüsselungsschlüssel zu verwenden ist, unter Verwendung des quellenseitigen gemeinsamen Sitzungsschlüssels sk als Basis, was später beschrieben wird. In gleicher Weise erzeugt der Personalcomputer **2** eine Zufallszahl, welche als Entschlüsselungsschlüssel zu verwenden ist, indem der senkseitige gemeinsame Sitzungsschlüssel sk' als Basis verwendet wird, wie später ebenfalls beschrieben wird.

[0082] Wie oben beschrieben wird der Lizenzschlüssel lk im Schritt S5 der in Fig. 4 gezeigten Prozedur erzeugt, wobei die Hash-Funktion auf eine Verkettung einer ID, welche für eine bestimmte elektronische Vorrichtung einmalig ist, und einen Dienstschlüssel, der für einen Text vorgesehen ist, der durch den Urheber gebildet ist, angewandt wird. Somit ist es bei einem Paar von zwei elektronischen Vorrichtungen, wo die Quelle nicht den Dienstschlüssel für den Text und/oder die Senke nicht die ID hat, die für den legalen Eigner einmalig ist, unmöglich, den korrekten Lizenzschlüssel lk zu erzeugen (siehe Schritt S5 der in Fig. 4 gezeigten Prozedur). Außerdem ist eine elektronische Vorrichtung, welche nicht durch den Autor bestätigt wird, nicht mit einem Lizenzschlüssel versehen, und somit nicht in der Lage, den Sitzungsschlüssel sk' zu erzeugen (siehe Schritt S10 der Prozedur, welche in Fig. 4 gezeigt ist). In einem Normalfall verschlüsselt, nachdem die in Fig. 4 gezeigte Prozedur abgeschlossen ist, das DVD-Wiedergabegerät **1** reproduzierte Daten oder einen Klartext unter Verwendung des quellenseitigen gemeinsamen Sitzungsschlüssels sk und überträgt die verschlüsselten Daten oder den verschlüsselten Text zum Personalcomputer **2**. Wenn der Personalcomputer mit einem korrekten Lizenzschlüssel versehen ist, ist dieser in der Lage, einen senkseitigen gemeinsamen Sitzungsschlüssel sk' zu erzeugen (siehe Schritt S10 der in Fig. 4 gezeigten Prozedur). Der Personalcomputer **2** ist somit in der Lage, die verschlüsselten Wiedergabedaten oder den verschlüsselten Text, der vom DVD-Wiedergabegerät **1** empfangen wird, mittels des senkseitigen gemeinsamen Sitzungsschlüssel sk' zu entschlüsseln. Wenn der Personalcomputer **2** keine lizenzierte elektronische Vorrichtung ist, wird es jedoch unmöglich, den senkseitigen gemeinsamen Sitzungsschlüssel sk' zu erzeugen, da der korrekte Lizenzschlüssel nicht verfügbar ist. Als Ergebnis ist in der nichtlizenzierte Personalcomputer **2** nicht in der Lage, die verschlüsselten Wiedergabedaten oder den verschlüsselten Text, der vom DVD-Wiedergabegerät **1** empfangen wird, zu ent-

schlüsseln. Anders ausgedrückt wird lediglich eine Senke, welche in der Lage ist, einen senkseitigen gemeinsamen Sitzungsschlüssel sk' zu erzeugen, der den gleichen Wert hat wie der quellenseitige gemeinsame Sitzungsschlüssel sk, der durch die Quelle erzeugt wird, schließlich bestätigt. Der Grund dafür liegt darin, dass lediglich eine bestimmte elektronische Vorrichtung, die als berechtigte Quelle dient, die einen Dienstschlüssel hat, der durch den Urheber für Information oder einen Text vorgesehen ist, der durch den Urheber erzeugt wird und eine korrekte ID von einer berechtigten Senke empfängt, in der Lage ist, den korrekten Lizenzschlüssel lk zu erzeugen. Aus dem gleichen Grund ist lediglich eine bestimmte elektronische Vorrichtung, welche als berechtigte Senke dient, die mit dem korrekten Lizenzschlüssel durch den Urheber versehen ist, in der Lage, den korrekten senkseitigen gemeinsamen Sitzungsschlüssel sk' zur Verwendung als Entschlüsselungsschlüssel zu verwenden, um verschlüsselte Daten oder einen verschlüsselten Text zu entschlüsseln.

[0083] Es sei angenommen, dass ein Lizenzschlüssel, der einem Personalcomputer **2** gewährt wurde, aufgrund irgendeiner Gelegenheit gestohlen ist. In diesem Fall kann trotzdem der gestohlene Lizenzschlüssel nicht bei einer anderen elektronischen Vorrichtung verwendet werden, um einen gültigen senkseitigen gemeinsamen Sitzungsschlüssel sk' zu erzeugen, da die andere Vorrichtung eine ID hat, die gegenüber der verschieden ist, welche dem Personalcomputer **2** zugeteilt ist. Da die ID von Vorrichtung zu Vorrichtung insoweit variiert, wird eine andere elektronische Vorrichtung nicht in der Lage sein, die verschlüsselten Wiedergabedaten oder den verschlüsselten Text, die vom DVD-Wiedergabegerät **1** empfangen werden, mittels des gestohlenen Lizenzschlüssels zu entschlüsseln. Als Folge davon kann die Sicherheit übertragener Information verbessert werden.

[0084] Nebenbei bemerkt kann ein nichtberechtigter Benutzer sowohl den verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e als auch den quellenseitigen gemeinsamen Sitzungsschlüssel sk aufgrund irgendeiner Gelegenheit kennen. Da in diesem Fall der verschlüsselte quellenseitige gemeinsame Sitzungsschlüssel e eine Art an Text ist, welcher aus der Verschlüsselung des quellenseitigen gemeinsamen Sitzungsschlüssels sk resultiert, wobei der Lizenzschlüssel lk verwendet wird, liegt es innerhalb der Grenzen der Möglichkeit, dass der nichtberechtigte Benutzer in der Lage ist, den korrekten Wert des Lizenzschlüssels lk zu erlangen, indem er alle Werte des Lizenzschlüssels lk bei der Verschlüsselung der quellenseitigen gemeinsamen Sitzungsschlüssels sk unter Verwendung des Lizenzschlüssels lk verwendet, um den verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e auf Versuch-Fehler-Basis zu berechnen, vorausgesetzt, dass der Algorithmus der Verschlüsselung offenbart ist.

[0085] Um zu verhindern, dass ein nichtberechtigter Benutzer irgendeine Art von Attacke startet, kann der Prozess, um einen Lizenzschlüssel von einem bekannten verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e und einem bekannten quellenseitigen gemeinsamen Sitzungsschlüssel sk umgekehrt herzuleiten, schwierig werden, um den Algorithmus der Verschlüsselung streng vertraulich zu halten, d.h., einen Teil oder den gesamten Verschlüsselungsalgorithmus nicht öffentlich zu offenbaren.

[0086] Aus dem gleichen Grund kann ein Prozess, um umgekehrt einen Dienstschlüssel von einem bekannten Lizenzschlüssel und einer ID herzuleiten, wobei alle Werte des Dienstschlüssels und der bekannten ID in einer Hash-Funktion verwendet werden, um den bekannten Lizenzschlüssel auf Versuch-Fehler-Basis zu erzeugen, kompliziert werden, indem die Hash-Funktion streng geheim gehalten wird, d.h., dass ein Teil oder die gesamte Hash-Funktion nicht öffentlich offenbart wird.

[0087] Fig. 6 ist ein Diagramm, welches eine weitere Ausführungsform zeigt, bei der eine Bestätigungsprozedur ausgeführt wird, wodurch eine Quelle, die üblicherweise durch das DVD-Wiedergabegerät **1** erfüllt wird, zwei Senken bestätigt, welche üblicherweise durch den Personalcomputer **2** bzw. die optische Magnetplattenvorrichtung **3** ausgeführt werden, indem jeder der Senken erlaubt wird, einen senkseitigen gemeinsamen Sitzungsschlüssel zu erzeugen, welcher den gleichen Wert hat wie der quellenseitige gemeinsame Sitzungsschlüssel, der durch die Quelle erzeugt wird, lediglich dann, wenn die Senken berechtigte Senken sind.

[0088] In der EEPROM-Einheit **50**, welche im Personalcomputer **2** verwendet wird, welche als erste Senke dient, sind eine ID1, eine Identifikation, welche vorher einmalig durch einen Hersteller des elektronischen Geräts den Personalcomputer **2** zugeteilt ist, und der Lizenzschlüssel **1**, ein Lizenzschlüssel, der vorher durch einen Urheber der Information dem Computer **2** mitgeteilt ist, gespeichert. Aus dem gleichen Grund sind in der EEPROM-Einheit **37**, welche in der optischen Magnetplattenvorrichtung **3** verwendet wird, die als zweite Senke dient, die ID2, eine ID, die vorher einmalig durch den Hersteller des elektronischen Geräts der Plattenvorrichtung **3** zugeteilt sind, und ein Lizenzschlüssel **2**, ein Lizenzschlüssel, der vorher durch den Urheber der Information der Plattenvorrichtung bereitgestellt wird, gespeichert.

[0089] Da Teile der Verarbeitung, welche in den Schritten S11 bis S20 durch das DVD-Wiedergabegerät ausgeführt werden, welches als Quelle dient, und durch den Personalcomputer **2**, der als erste

Senke dient, im Wesentlichen gleich denjenigen der Schritte S1 bis 10 der in Fig. 4 gezeigten Prozedur sind, wird eine Erläuterung dafür nicht wiederholt.

[0090] Kurz ausgedrückt erzeugt der Personalcomputer **2** einen berechtigten senkseitigen gemeinsamen Sitzungsschlüssel sk1' von einem verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e1, der von dem DVD-Wiedergabegerät empfangen wurde, im Schritt S20, wie oben beschrieben. Die Prozedur läuft dann weiter zu einem Schritt S21, bei dem die Firmware **20** im DVD-Wiedergabegerät **1** die 1394-Schnittstelleneinheit **26** steuert, um eine Anforderung an die optische Magnetplattenvorrichtung **3** nach deren ID zu tätigen, um diese mittels des 1394-Seriell-Busses **11** zu übertragen. Danach läuft die Prozedur weiter zu einem Schritt S22, bei dem Firmware **20** der optischen Magnetplattenvorrichtung **3**, welche in Fig. 10 gezeigt ist, die Anforderung nach der ID empfängt. Ausführlicher ausgedrückt leitet die 1394-Schnittstelleneinheit **36**, welche bei der optischen Magnetplattenvorrichtung **3** verwendet wird, die Anforderung auf die ID, welche durch das DVD-Wiedergabegerät **1** übertragen wird, über die 1394-Seriell-Bus **11** weiter zur CPU **31**. Die Prozedur läuft dann weiter zu einem Schritt S23, bei dem die Firmware, welche durch die CPU **31** ausgeführt wird, die Identifikations-ID2 von der EEPROM-Einheit **37** gemäß der Anforderung liest, die hier durch die 1394-Schnittstelleneinheit **36** zugeführt wird, und die Identifikations-ID2 zum DVD-Wiedergabegerät **1** über die 1394-Schnittstelleneinheit **36** und den 1394-Seriell-Bus **11** überträgt.

[0091] Danach läuft die Prozedur zu einem Schritt S24, bei dem die 1394-Schnittstelleneinheit **26**, welche bei dem DVD-Wiedergabegerät **1** verwendet wird, die Identifikations-ID2 empfängt und diese zur Firmware **20** weiterleitet, die durch die CPU **21** ausgeführt wird.

[0092] Nachfolgend läuft die Prozedur weiter zu einem Schritt S25, bei dem die Firmware **20** die Identifikations-ID2, welche von der optischen Magnetplattenvorrichtung **3** empfangen wird, mit einem Dienstschlüssel verkettet, der in der EEPROM-Einheit **27** gespeichert ist, um Daten (ID2 || Dienstschlüssel) zu bilden. Danach wird ein Lizenzschlüssel lk2 durch Anwenden der Hash-Funktion auf die Daten (ID2 || Dienstschlüssel) berechnet, wie in der folgenden Gleichung gezeigt ist:

lk2 = hash (ID2 || Dienstschlüssel)

[0093] Danach läuft die Prozedur weiter zu einem Schritt S26, bei dem die Firmware **20** den quellenseitigen gemeinsamen Sitzungsschlüssel sk, der im Schritt S16 erzeugt wurde, unter Verwendung des Lizenzschlüssels lk2 verschlüsselt, der im Schritt S25 berechnet wurde, als einen Schlüssel, um einen verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e2 gemäß der folgenden Gleichung zu erzeugen:

e2 = Enc (lk2, sk)

[0094] Anschließend läuft die Prozedur weiter zu einem Schritt S27, bei dem die Firmware **20** den verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e2, der im Schritt S26 erzeugt wurde, zur optischen Magnetplatte **3** überträgt. Ausführlich ausgedrückt wird der verschlüsselte quellenseitige gemeinsame Sitzungsschlüssel e2 durch die 1394-Schnittstelleneinheit **26**, welche im DVD-Wiedergabegerät **1** verwendet wird, über den 1394-Seriell-Bus **11** zur optischen Magnetplattenvorrichtung **3** übertragen.

[0095] Die Prozedur läuft dann weiter zu einem Schritt S28, bei dem die 1394-Schnittstelleneinheit **36**, die bei dem optischen Magnetplattengerät **3** verwendet wird, den verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e3 empfängt. Danach läuft die Prozedur weiter zu einem Schritt S29, bei dem die Firmware **30** den verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e2 entschlüsselt, der ihm durch die 1394-Schnittstelleneinheit **36** zugeführt wurde, wobei ein Lizenzschlüssel (Lizenzschlüssel **2**), der in der EEPROM-Einheit **37** gespeichert wurde, als ein Schlüssel zugeführt wird, um einen senkseitigen gemeinsamen Sitzungsschlüssel sk2' gemäß der folgenden Gleichung zu erzeugen:

sk2' = Dec (Lizenzschlüssel 2, e2)

[0096] Wie oben beschrieben erzeugen der Personalcomputer **2** und die optische Magnetplattenvorrichtung **3** die senkseitigen gemeinsamen Sitzungsschlüssel sk1' und sk2' in den Schritten S20 bzw. S29. Normalerweise haben die senkseitigen gemeinsamen Sitzungsschlüssel sk1' und sk2' den gleichen Wert wie der quellenseitige gemeinsame Sitzungsschlüssel sk, der durch das DVD-Wiedergabegerät **1** im Schritt S16 erzeugt wurde.

[0097] In der in Fig. 6 gezeigten Prozedur fragt das DVD-Wiedergabegerät **1** nach einer ID für den Personalcomputer **2** und das optische Magnetplattengerät **3** separat. Es sollte jedoch angemerkt sein, dass in dem Fall einer Sendekommunikation, wo Anforderungen im gleichen Zeitpunkt getätigt werden können, eine Verarbeitung gemäß einer Ausführungsform, welche eine Prozedur wie eine, die in Fig. 7 gezeigt ist, ausführen kann.

[0098] Wie in der Figur gezeigt ist, beginnt die Prozedur mit einem Schritt S41, bei dem das DVD-Wiedergabegerät **1** Anfragen an alle Senken tätigt, d.h., den Personalcomputer **2** und die optische Magnetplattenvorrichtung **3** nach deren IDs durch Sende-

kommunikation. Danach läuft die Prozedur weiter zu den Schritten S42 und S43, in denen der Personalcomputer **2** und die optische Magnetplattenvorrichtung **3** entsprechend die Anfragen nach den IDs empfangen. Die Prozedur läuft dann weiter zu den Schritten S44 und S45, in denen der Personalcomputer **2** und die optische Magnetplattenvorrichtung **3** die Identifikations-ID1 und ID2 entsprechend von den EEPROM-Einheit **50** und **37** liest und diese zum DVD-Wiedergabegerät **1** übertragen. Danach läuft die Prozedur weiter zu den Schritten S46 und S47, bei denen das DVD-Wiedergabegerät **1** die Identifikation-ID1 bzw. -ID2 empfängt.

[0099] Nachfolgend läuft die Prozedur weiter zu einem Schritt S48, bei dem das DVD-Wiedergabegerät **1** die Identifikations-ID1, welche vom Personalcomputer **2** empfangen wird, mit einen Dienstschlüssel verkettet, die in der EEPROM-Einheit **27** gespeichert ist, um Daten (ID1 || Dienstschlüssel) zu bilden. Danach wird ein Lizenzschlüssel lk1 durch Anwenden der Hash-Funktion auf die Daten (ID1 || Dienstschlüssel) berechnet, wie in der folgenden Gleichung gezeigt ist:

lk1 = hash (ID1 || Dienstsschlüssel)

[0100] Nachfolgend läuft die Prozedur weiter zu einem Schritt S49, bei dem das DVD-Wiedergabegerät **1** die Identifikations-ID2, welche von der optischen Magnetplattenvorrichtung **3** empfangen wird, mit dem Dienstschlüssel, der in der EEPROM-Einheit **27** gespeichert ist, verkettet, um Daten (ID2 || Dienstschlüssel) zu bilden. Danach wird ein Lizenzschlüssel lk2 durch Anwenden der Hash-Funktion auf die Daten (ID2 || Dienstschlüssel) berechnet, wie in der folgenden Gleichung gezeigt ist:

lk2 = hash (ID2 || Dienstschlüssel)

[0101] Die Prozedur läuft dann weiter zu einem Schritt S50, bei dem das DVD-Wiedergabegerät **1** einen quellenseitigen gemeinsamen Sitzungsschlüssel sk erzeugt. Danach fahren die Prozeduren weiter fort zu einem Schritt S51, bei dem das DVD-Wiedergabegerät **1** den quellenseitigen gemeinsamen Sitzungsschlüssel sk, der im Schritt S50 erzeugt wurde, unter Verwendung des Lizenzschlüssels lk1, der im Schritt S48 berechnet wurde, erzeugt, als Schlüssel, um einen verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e1 gemäß der folgenden Gleichung zu erzeugen:

e1 = Enc (lk1, sk)

[0102] Danach läuft die Prozedur weiter zu einem Schritt S52, bei dem das DVD-Wiedergabegerät **1** den quellenseitigen gemeinsamen Sitzungsschlüssel sk, der im Schritt S50 erzeugt wurde, unter Verwendung des Lizenzschlüssels lk2, der im Schritt S49 berechnet wurde, als Schlüssel verschlüsselt, um einen verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e2 gemäß der folgenden Gleichung zu erzeugen:

e2 = Enc (lk2, sk)

[0103] Die Prozedur läuft dann weiter zu einem Schritt S53, bei dem die Identifikations-ID1, der verschlüsselte quellenseitige gemeinsame Sitzungsschlüssel e1, die Identifikations-ID2 und der verschlüsselte quellenseitige gemeinsame Sitzungsschlüssel e2 gebündelt werden, um einen verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e wie folgt zu erzeugen:

e = ID1 || e1 || ID2 || e2

[0104] Anschließend läuft die Prozedur weiter zu einem Schritt S54, bei dem das DVD-Wiedergabegerät **1** einen verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e zum Personalcomputer **2** und zur optischen Magnetplattenvorrichtung **3** über Sendekommunikation überträgt. Die Prozedur läuft dann weiter zu den Schritten S55 und S56, in denen der Personalcomputer **2** und die optische Magnetplattenvorrichtung **3** den verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e empfangen. Die Prozedur läuft dann weiter zu den Schritten S57 und S58, in denen der Personalcomputer **2** und die optische Magnetplattenvorrichtung **3** die verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e1 und e2, welche von dem verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e extrahiert wurden, entschlüsselt, wobei die Lizenzschlüssel Lizenzschlüssel **1** und Lizenzschlüssel **2**, welche in den EEPROM-Einheiten **50** und **37** gespeichert sind, als Schlüssel verwendet werden, um senkseitige gemeinsame Sitzungsschlüssel sk1' und sk2' entsprechend gemäß den folgenden Gleichungen zu erzeugen:

sk1' = Dec (Lizenzschlüssel 1, e1)

sk2' = Dec (Lizenzschlüssel 2, e2)

[0105] Fig. 8 ist ein Diagramm, welches eine Ausführungsform zeigt, bei der eine Prozedur der Bestätigungsverarbeitung ausgeführt wird, wobei lediglich eine berechtigte Senke einen senkseitigen gemeinsamen Sitzungsschlüssel sk' erzeugen wird, der den gleichen Wert hat wie der quellenseitige gemeinsame Sitzungsschlüssel sk, der durch eine Quelle in einem System erzeugt wird, wo die Senke in der Lage ist, mehrere Dienste auszuführen, d.h., das Entschlüsseln mehrerer Informationsarten. Um die unterschiedlichen Informationsarten zu handhaben, ist der Personalcomputer **2**, der als Senke dient, mit mehreren Lizenztasten versehen, welche in der EEPROM-Einheit **50** gespeichert sind, beispielsweise

dem Lizenzschlüssel 1, dem Lizenzschlüssel **2**, dem Lizenzschlüssel **3** usw. für die unterschiedlichen Informationsarten. Aus dem gleichen Grund hat das DVD-Wiedergabegerät **1**, welches als Quelle dient, Information über mehrere Dienst-IDs, um zu identifizieren, welche Informationsarten zur Senke zu übertragen sind, und mehrere Dienstschlüssel, welche in der EEPROM-Einheit **27** gespeichert sind, beispielsweise den Dienstschlüssel **1**, den Dienstschlüssel **2**, den Dienstschlüssel **3**, usw., welche zum Erzeugen des Lizenzschlüssels **1**, des Lizenzschlüssels **2**, des Lizenzschlüssels **3** usw. entsprechend verwendet werden. Teile der Verarbeitung, welche in der in Fig. 8 gezeigten Prozedur ausgeführt werden, sind ähnlich denjenigen der in Fig. 4 gezeigten Prozedur, mit der Ausnahme der folgenden Schritte. Beginnend mit einem Schritt S81 überträgt das DVD-Wiedergabegerät **1** eine Anforderung nach einer ID gemeinsam mit einer Dienst-ID, um eine Informationsart zu identifizieren, die durch den Personalcomputer **2**, der als Senke verwendet wird, bedient wird, zum Personalcomputer **2**. Danach wird in einem Schritt S85 ein Lizenzschlüssel lk durch das DVD-Wiedergabegerät **1** durch Anwenden der Hash-Funktion auf eine ID, welche vom Personalcomputer **2** empfangen wird, und einen vom Dienstschlüssel **1**, Dienstschlüssel **2**, Dienstschlüssel **3**, usw. in der EEPROM-Einheit, die mit der Informationsart, die zur Senke übertragen werden soll, in Verbindung steht, d.h., mit der Dienst-ID in Verbindung steht, die zum Personalcomputer **2** im Schritt S81 übertragen wird, erzeugt. Schließlich erzeugt in einem Schritt S90 der Personalcomputer **2** einen senkseitigen gemeinsamen Sitzungsschlüssel sk' von einem verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e, der von dem DVD-Wiedergabegerät **1** in einem Schritt S89 empfangen wurde, und eine von dem Lizenzschlüssel **1**, Lizenzschlüssel **2**, Lizenzschlüssel **3**, usw. in der EEPROM-Einheit **50**, welche mit der Dienst-ID in Verbindung steht, die von dem DVD-Wiedergabegerät **1** im Schritt S82 empfangen wurde.

[0106] Fig. 9 ist ein Diagramm, welches eine weitere Ausführungsform zeigt, bei der eine Prozedur zum Bestätigen ausgeführt wird, wobei lediglich eine gültige Senke in der Lage ist, einen senkseitigen gemeinsamen Sitzungsschlüssel sk' zu erzeugen, der den gleichen Wert hat wie der quellenseitige gemeinsame Sitzungsschlüssel sk, der durch eine Quelle erzeugt wird. In diesem Fall hat das DVD-Wiedergabegerät **1**, welches als Quelle verwendet wird, einen Dienstschlüssel, eine Hash-Funktion und eine Pseudozufallszahl-Erzeugungsfunktion pRNG, die in der EEPROM-Einheit **27** gespeichert sind, die dadurch verwendet werden. Der Dienstschlüssel, die Hash-Funktion und die Pseudozufallszahl-Erzeugungsfunktion pRNG werden durch einen Urheber einer Information angegeben und streng geheim gehalten. Dagegen sind, welche in der EEPROM-Einheit **50** gespeichert sind, die durch den Personalcomputer **2** verwendet werden, der als Senke dient, eine ID, welche dem Personalcomputer **2** durch den Hersteller des elektronischen Geräts zugeteilt sind, wie Lizenzschlüssel LK und LK', eine Konfusionsfunktion G und eine Pseudozufallszahl-Erzeugungsfunktion pRNG, welche durch den Urheber der Information angegeben werden, gespeichert.

[0107] Der Lizenzschlüssel LK ist ein einzigartiger Zufallszahlenschlüssel, der durch den Urheber erzeugt wird, während der Lizenzschlüssel LK' ebenfalls durch den Urheber erzeugt wird, um die folgende Gleichung zu erfüllen:

LK' = G^ – 1 (R)

wobei R = pRNG (H) (+) pRNG (LK)
wobei H = hash ((ID || Dienstschlüssel)

[0108] Es sollte verstanden sein, obwohl das Symbol ^ die Leistungsschreibweise bezeichnet, die Bezeichnung "G ^ – 1" die inverse Funktion der Konfusionsfunktion G bedeutet. Der Wert der inversen Funktion G ^ – 1 kann leicht herausgefunden werden, vorausgesetzt, dass vorher festgelegte Regeln bekannt sind. Wenn die vorher festgelegten Regeln nicht bekannt sind, ist es jedoch schwierig, den Wert der inversen Funktion G ^ – 1 zu berechnen. Eine Funktion, welche zur Verschlüsselung auf der Basis eines offenbarten Schlüssels verwendet wird, kann als diese Funktion genutzt werden.

[0109] Außerdem kann die Funktion pRNG zum Erzeugen einer Zufallszahl durch Hardware ausgeführt werden.

[0110] Wie in Fig. 9 gezeigt ist, beginnt die Prozedur mit einem Schritt S101, bei dem die Firmware **20** im DVD-Wiedergabegerät **1** eine Anforderung an den Lizenzmanager **62** des Personalcomputers **2** nach dessen ID tätigt, um diese zu übertragen. Danach läuft die Prozedur weiter zu einem Schritt S102, bei dem der Lizenzmanager **62** des Personalcomputers **2** die Anforderung nach der ID empfängt. Die Prozedur läuft dann weiter zu einem Schritt S103, bei dem der Lizenzmanager **62** die ID von der EEPROM-Einheit **50** gemäß der Anforderung liest und die ID zum DVD-Wiedergabegerät **1** überträgt. Danach läuft die Prozedur weiter zu einem Schritt S104, in welchem das DVD-Wiedergabegerät **1** die ID empfängt.

[0111] Anschließend läuft die Prozedur weiter zu einem Schritt S105, in welchem die Firmware **20** die ID, welche vom Personalcomputer **2** empfangen wird, mit einem Dienstschlüssel, der in der EEPROM-Einheit **27** gespeichert ist, verkettet, um Daten (ID || Dienstschlüssel) zu bilden. Dann wird ein Wert H durch Anwenden der Hash-Funktion auf die Daten (ID || Dienstschlüssel) berechnet, wie in der folgen-

den Gleichung gezeigt ist:

H = hash (ID || Dienstschlüssel)

[0112] Die Prozedur läuft dann weiter zu einem Schritt S106, in welchem die Firmware **20** einen quellenseitigen gemeinsamen Sitzungsschlüssel sk erzeugt. Danach läuft die Prozedur weiter zu einem Schritt S107, in welchem die Firmware **20** einen verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e von dem Wert H, der im Schritt S105 erzeugt wurde, und dem quellenseitigen gemeinsamen Sitzungsschlüssel sk, der im Schritt S106 erzeugt wurde, gemäß der folgenden Gleichung erzeugt:

e = sk (+) pRNG (H)

wobei die Schreibweise (+), welche auf der rechten Seite der obigen Gleichung verwendet wird, der Operator der Operation ist, um eine exklusive logische Summe zu berechnen, und somit der Ausdruck A (+) B die exklusive logische Summe von A und B zeigt.

[0113] Das heißt, dass im Schritt S107 der quellenseitige gemeinsame Sitzungsschlüssel sk, der im Schritt S106 erzeugt wurde, verschlüsselt wird, um den verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e zu erzeugen, wobei die exklusive logische Summe jedes Bits des Schlüssels sk und des entsprechenden Bits von pRNG (H) gefunden wird, eine Zufallszahl, welche durch Anwenden der Pseudozufallszahl-Erzeugungsfunktion pRNG auf den Wert H erlangt wird, welche im Schritt S105 erzeugt wurde.

[0114] Anschließend läuft die Prozedur weiter zu einem Schritt S108, in welchem die Firmware **20** den verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e, der im Schritt S107 erzeugt wurde, zum Personalcomputer **2** überträgt.

[0115] Die Prozedur läuft dann weiter zu einem Schritt S109, in welchem der Personalcomputer **2** den verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e empfängt. Danach läuft die Prozedur weiter zu einem Schritt S110, in welchem der Lizenzmanager **62** den verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e unter Verwendung der Lizenzschlüssel LK und LK', welche in der EEPROM-Einheit **50** gespeichert sind, als Schlüssel entschlüsselt, um einen senkseitigen gemeinsamen Sitzungsschlüssel sk' gemäß der folgenden Gleichung zu erzeugen:

sk' = e (+) G (LK') (+) pRNG (LK)

[0116] Das heißt, dass im Schritt S110 der verschlüsselte quellenseitige gemeinsame Sitzungsschlüssel e, der von dem DVD-Wiedergabegerät **1** empfangen wird, entschlüsselt wird, um den senkseitigen gemeinsamen Sitzungsschlüssel sk' zu erzeugen, wobei die exklusive logische Summe des verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssels e gefunden wird, G (LK'), ein Wert, der durch Anwenden der Konfusionsfunktion G, welche in der EEPROM-Einheit **50** gespeichert ist, auf den Lizenzschlüssel LK' erlangt wird, der ebenfalls in der EEPROM-Einheit **50** gespeichert ist, und pRNG (LK), ein Wert, der durch Anwenden der Pseudozufallszahl-Erzeugungsfunktion pRNG erlangt wird, die ebenfalls in der EEPROM-Einheit **50** gespeichert ist, auf den Lizenzschlüssel LK, der ebenfalls in der EEPROM-Einheit **50** gespeichert ist.

[0117] Ähnlich wie die in Fig. 4 gezeigte Prozedur hat der senkseitige gemeinsame Sitzungsschlüssel sk', der durch den Personalcomputer 2 im Schritt S110 erzeugt wird, den gleichen Wert wie der quellenseitige gemeinsame Sitzungsschlüssel sk, der durch das DVD-Wiedergabegerät 1 im Schritt S6 erzeugt wird. Die Tatsache, dass sk = sk', wird durch folgendes erwiesen:

sk' = e (+) G (LK') (+) pRNG (LK)

[0118] Wenn e durch (sk (+) pRNG (H)) in der Gleichung auf der rechten Seite der obigen Gleichung ersetzt wird, ergibt sich die folgende Gleichung:

sk' = sk (+) pRNG (H) (+) G(LK') (+) pRNG (LK)

[0119] Da G (LK') = G (^ – 1 (R)) = R, wird die folgende Gleichung erlangt:

sk' = sk (+) pRNG (H) (+) R (+) pRNG (LK)

[0120] Wenn man R durch (pRNG (H) (+) (pRNG (LK)) in der Gleichung auf der rechten Seite der obigen Gleichung ersetzt, wird die folgende Gleichung erlangt:

sk' = sk (+) pRNG (H) (+) pRNG (H) (+) pRNG (LK) (+) pRNG (LK)

[0121] Wie oben beschrieben sind die quellenseitigen senkseitigen gemeinsamen Sitzungsschlüssel sk und sk' ein gemeinsamer Schlüssel S, der anteilig durch sowohl das DVD-Wiedergabegerät **1** als auch durch den Personalcomputer **2** genutzt wird, die als Quelle bzw. als Senke dienen. Außerdem ist es ungleich den oben beschriebenen Prozeduren lediglich ein Urheber der Information, der in der Lage ist, Lizenzschlüssel LK und LK' zu erzeugen. Damit wird ein Versuch, der durch eine Quelle getätigt wird, illegal die Lizenzschlüssel LK und LK' zu erzeugen, zu einem Fehler führen. Als Ergebnis kann die Sicherheit der übertragenen Information weiter verbessert werden.

[0122] Bei den oben beschriebenen Bestätigungs-

prozeduren bestätigt eine Quelle eine Senke, indem erlaubt wird, dass die Senke einen senkseitigen gemeinsamen Sitzungsschlüssel sk' erzeugt, der den gleichen Wert hat wie der quellenseitige gemeinsame Sitzungsschlüssel sk, der durch die Quelle erzeugt wird, lediglich dann, wenn die Senke eine berechtigte Senke ist. Die Prozedur kann auch beispielsweise dazu angewandt werden, die übliche Operation zu bestätigen, um ein Anwendungsprogramm in den Personalcomputer **2** zu laden, um zu verhindern, dass ein Anwendungsprogramm, welches illegal erlangt wird, ausgeführt wird. In diesem Fall ist es notwendig, eine Beurteilung zu machen, ob die Ausführung jedes Anwendungsprogramms durch den Urheber des Programms über die gleiche Prozedur wie die, die insoweit beschrieben wurden, erlaubt ist oder nicht, wodurch der Lizenzmanager **62** ein Anwendungsmodul **61**, wie in Fig. 3 gezeigt ist, bestätigt. Genauer ausgedrückt dient in der Bestätigungsprozedur, die in Fig. 3 gezeigt ist, der Lizenzmanager **62** als Quelle, wo das Anwendungsmodul **61** als Senke verwendet wird.

[0123] Wenn der Bestätigungsprozess, der oben beschrieben wurde, abgeschlossen ist, d.h., nachdem die Senke einen senkseitigen gemeinsamen Sitzungsschlüssel sk' erzeugt hat, der den gleichen Wert hat wie der quellenseitige gemeinsame Sitzungsschlüssel sk, der durch die Quelle erzeugt wurde, werden Daten oder ein Klartext, der durch die Quelle unter Verwendung eines Verschlüsselungsschlüssels verschlüsselt wurde, von der Quelle zur Senke übertragen. In der Senke werden die verschlüsselten Daten oder der verschlüsselte Text unter Verwendung eines Entschlüsselungsschlüssels zurück entschlüsselt. Wie oben beschrieben können die quellenseitigen senkseitigen gemeinsamen Sitzungsschlüssel sk und sk' als Entschlüsselungs- und Verschlüsselungsschlüssel entsprechend unverändert verwendet werden, oder als Alternative wird eine Zufallszahl, welche vom Sitzungsschlüssel sk oder sk' erzeugt wird, als Verschlüsselungs- oder Entschlüsselungsschlüssel anstelle davon verwendet. Der Betrieb, der durch die Quelle ausgeführt wird, Daten zu verschlüsseln, und der Betrieb, der durch die Senke ausgeführt wird, die verschlüsselten Daten zu entschlüsseln, werden wie folgt erläutert.

[0124] Bei einer elektronischen Vorrichtung, beispielsweise dem DVD-Wiedergabegerät **1** und der optischen Magnetplattenvorrichtung **3** werden die internen Funktionen, welche nicht in einer Architektur eingebaut sind, welche für den Benutzer offen ist, die Verarbeitung, um Daten, welche über den 1394-Seriell-Bus **11** übertragen werden, zu verschlüsseln und zu entschlüsseln, in einem System wie eines, welches in Fig. 10 gezeigt sind, einem Blockdiagramm, welches ein System zeigt, wo eine Quelle verschlüsselte Daten zu Senken überträgt, durch die 1394-Schnittstelleneinheiten **26** und **36** ausgeführt, welche im DVD-Wiedergabegerät **1** bzw. in der optischen Magnetplattenvorrichtung **3** verwendet werden. Daten werden verschlüsselt oder entschlüsselt unter Verwendung durch Verwendung eines Sitzungsschlüssels S, d.h., des quellenseitigen gemeinsamen Sitzungsschlüssels sk oder des senkseitigen gemeinsamen Sitzungsschlüssels sk', wie früher beschrieben, und eines zeitvariablen Schlüssels e, genauer ausgedrückt eines Schlüssel e', um den zeitvariablen Schlüssel i zu erzeugen. Der Sitzungsschlüssel S und der Schlüssel e' werden durch die Firmware **20** oder **30** zur 1394-Schnittstelleneinheit **26** bzw. zur Schnittstelleneinheit **36** geliefert. Der Sitzungsschlüssel S weist einen Anfangswertschlüssel Ss, der als Anfangswert verwendet wird, und einen Beeinflussungsschlüssel Si auf, um den zeitvariablen Schlüssel i umzuordnen. Der Anfangswertschlüssel Ss und der Beeinflussungsschlüssel Si können entsprechend aus einer vorher festgelegten Anzahl höherwertiger Bits und einer vorher festgelegten Anzahl niedrigwertiger Bist des senkseitigen gemeinsamen Sitzungsschlüssels sk oder des senkseitigen gemeinsamen Sitzungsschlüssels sk' gebildet werden, der den gleichen Wert hat wie sk, der im Prozess zum Bestätigen der Senke wie früher beschrieben verwendet wird. Der Sitzungsschlüssel S wird geeignet in jeder Sitzung aktualisiert, beispielsweise für jede Bewegtbildinformation oder für jede Wiedergabeoperation. Dagegen wird der zeitvariable Schlüssel i, der von dem Beeinflussungsschlüssel Si des Sitzungsschlüssel S erzeugt wird, und der Schlüssel i' häufig in einer Sitzung aktualisiert. Beispielsweise kann die Zeitinformation, welche mit einem vorher festgelegten zeitlichen Ablauf erlangt wird, üblicherweise als Schlüssel i' verwendet werden.

[0125] Es sei nun angenommen, dass Bewegtbilddaten, die wiedergegeben werden und durch die das DVD-Wiedergabegerät **1** ausgegeben werden, welches als Quelle dient, zur optischen Magnetplattenvorrichtung **3** und zum Personalcomputer **2**, welche als Senken verwendet werden, über den 1394-Seriell-Bus **11** übertragen werden und dann durch die Senken verschlüsselt werden. In diesem Fall werden die Daten durch die 1394-Schnittstelleneinheit **26** verschlüsselt, welche im DVF-Wiedergabegerät **1** verwendet wird, wobei der Sitzungsschlüssel S und der zeitvariable Schlüssel i verwendet werden, genauer ausgedrückt, der Schlüssel i' und die verschlüsselten Daten werden durch die 1394-Schnittstelleneinheit **36** wiederum entschlüsselt, die bei der optischen Magnetplattenvorrichtung **3** verwendet werden, wobei der Sitzungsschlüssel S und der zeitvariable Schlüssel verwendet werden, genauer ausgedrückt, der Schlüssel i'.

[0126] Im Personalcomputer **2** liefert dagegen der Lizenzmanager **62** den Anfangswertschlüssel Ss des Sitzungsschlüssels S zum Anwendungsmodul **61** und den Beeinflussungsschlüssel Si des Sitzungs-

schlüssels S und den zeitvariablen Schlüssel i, genauer ausgedrückt den Schlüssel i' zum Erzeugen des zeitvariablen Schlüssel i zur 1394-Schnittstelleneinheit **49**, die als Verknüpfungseinheit dient. In der 1394-Schnittstelleneinheit **49** wird der zeitvariable Schlüssel i vom Beeinflussungsschlüssel Si erzeugt und vom Schlüssel i' und zum Rückentschlüsseln der verschlüsselten Daten verwendet. Die entschlüsselten Daten werden weiter durch das Anwendungsmodul **61** unter Verwendung des Sitzungsschlüssels S entschlüsselt, genauer ausgedrückt unter Verwendung des Anfangswertschlüssels Ss des Sitzungsschlüssels S.

[0127] Wie oben beschrieben führt im Personalcomputer **2**, der eine Architektur hat, wo der interne Bus **51** in einer Architektur ausgebildet ist, welche für den Benutzer offen ist, die 1394-Schnittstelleneinheit **49** lediglich eine erste Stufe der Entschlüsselung der verschlüsselten Daten durch, wobei die Daten noch in einem verschlüsselten Zustand gelassen werden. Danach führt das Anwendungsmodul **61** weiter eine zweite Stufe der Entschlüsselung in Bezug auf die Daten durch, welche durch die 1394-Schnittstelleneinheit **49** entschlüsselt sind, um den Klartext zu erzeugen. Auf diese Weise wird verhindert, dass der Personalcomputer **2** Daten (d.h. einen Klartext), die über den internen Bus **51** übertragen werden, auf einen anderen Träger kopiert, beispielsweise eine Festplatte, die in der Festplattenansteuerung **47** befestigt ist, über die Verwendung einer passenden Funktion, welche dem internen Bus **51** hinzugefügt ist.

[0128] Wie oben beschrieben werden gemäß der Ausführungsform nach der vorliegenden Erfindung in einer CE-Vorrichtung mit einer Architektur, wo ein interner Bus nicht gegenüber dem Benutzer offen ist, verschlüsselte Daten lediglich einmal unter Verwendung eines Sitzungsschlüssels S und eines zeitvariablen Schlüssels i entschlüsselt, genauer ausgedrückt, eines Schlüssels i'. Bei einem CE-Gerät, beispielsweise dem Personalcomputer **2** mit einer Architektur, wo ein interner Bus gegenüber dem Benutzer offen ist, werden dagegen verschlüsselte Daten unter Verwendung eines zeitvariablen Schlüssel i entschlüsselt, der unter Verwendung des Beeinflussungsschlüssel Si eines Sitzungsschlüssels S und des Schlüssels i' erzeugt wird, in einer ersten Stufe der Entschlüsselung, und weiter unter Verwendung des Anfangswerts Ss des Sitzungsschlüssels S in einer zweiten Stufe der Entschlüsselung entschlüsselt. Die erste und die zweite Stufe der Entschlüsselungsverarbeitung werden durch die folgende Gleichung dargestellt:

Dec (Ss, Dec (i, Enc (algo (S + i'), Data)) = Data

wobei der Ausdruck algo (S + i'), der auf der linken Seite der obigen Gleichung ist, einen Wert zeigt, der aus der Anwendung eines vorher festgelegten Algorithmus in Bezug auf den Sitzungsschlüssel S und den zeitvariablen Schlüssels i resultiert, genauer ausgedrückt auf den Schlüssel i', wobei der Ausdruck Dec, der am linken Ende der Gleichung auftritt, die zweite Stufe der Entschlüsselung zeigt, die weitere Dec-Schreibweise die erste Stufe der Entschlüsselung zeigt und der Ausdruck Enc die Entschlüsselung zeigt, welche durch die Quelle ausgeführt wird.

[0129] Fig. 11 ist ein Blockdiagramm, welche einen typischen Aufbau der 1394-Schnittstelleneinheit **26** zeigt, die den Ausdruck Enc erfüllt, der in der Gleichung, die oben angegeben ist, erscheint, um die Verschlüsselung darzustellen, welche durch das DVD-Wiedergabegerät **1** ausgeführt wird, bei dem die 1394-Schnittstelleneinheit **26** verwendet wird. Wie in der Figur gezeigt ist, weist der Aufbau einen Zusatzgenerator **71** auf, ein LFSR (lineares Rückführschieberegister) **72** auf, einen Verkleinerungsgenerator **73** und einen Addierer **74**. m-Bit-Daten, welche durch den Zusatzgenerator **71** erzeugt werden, und 1-Bit-Daten, welche durch das LFDR zeugt werden, werden zum Verkleinerungsgenerator **73** geliefert. Der Verkleinerungsgenerator **73** wählt einige Abschnitte der m-Bit-Daten aus, welche vom Zusatzgenerator **71** empfangen werden, gemäß dem Wert der 1-Bit-Daten, welche durch das LFDR **72** geliefert werden, und gibt die ausgewählten m-Bit-Daten an den Addierer **74** als Verschlüsselungsschlüssel aus. Es sollte angemerkt sein, dass der m-Bit-Verschlüsselungsschlüssel, eine Zufallszahl, welche durch den Verkleinerungsgenerator **73** erzeugt wird, dem Schlüssel (S + i') in der oben angegebenen Gleichung entspricht. Der Addierer **74** fügt den m-Bit-Verschlüsselungsschlüssel, der vom Verkleinerungsgenerator **73** empfangen wird, einem zugeführten Klartext hinzu, d.h., m-Bit-Daten, die zum 1384-Seriell-Bus **11** zu übertragen sind, um einen verschlüsselten Text oder verschlüsselte Daten zu erzeugen.

[0130] Die Addition, welche durch den Addierer **74** ausgeführt wird, ist ein mod 2-^-m-Prozess, wobei das Symbol ^ die Leistungsdarstellung ist, was die Addition des Verschlüsselungsschlüssels, der durch den Verkleinerungsgenerator **73** erzeugt wird, zum Klartext bedeutet. Anders ausgedrückt ist der Prozess die Hinzufügung eines m-Bit-Schlüssels zu m-Bit-Daten, wobei ein Übertrag ignoriert wird.

[0131] Fig. 12 ist ein Blockdiagramm, welches einen ausführlichen Aufbau der 1394-Schnittstelleneinheit **26**, welche in Fig. 11 gezeigt ist, in einer einfachen und einer offenkundigen Weise zeigt. Wie in Fig. 12 gezeigt ist, wird der Anfangswertschlüssel Ss des Sitzungsschlüssels S, der von der Firmware **20** empfangen wird, zu einem Register **82** über den Addierer **81** geliefert und darin gehalten. Üblicherweise weist der Anfangswertschlüssel Ss 55 Wörter auf, die jeweils eine Länge im Bereich von 8 bis 32 Bits ha-

ben. Dagegen wird der Beeinflussungsschlüssel Si des Sitzungsschlüssels S in einem Register **85** gehalten. Üblicherweise ist der Beeinflussungsschlüssel Si die niedrigwertigeren 32 Bits des Sitzungsschlüssels S.

[0132] Der Schlüssel i' wird im 32-Bit-Register **84** gehalten. Der Schlüssel i' wird in einem Prozess zum Ansammeln von Bits erzeugt. Ausführlich ausgedrückt werden jedes Mal, wenn ein Paket über den 1394-Seriell-Bus **11** übertragen wird, üblicherweise 2 Bits, welche zum Bilden des Schlüssel i' verwendet werden, zum Register **84** geliefert. Die Bildung des 32-Bit-Schlüssels i' wird beendet, wenn **16** Pakete übertragen sind. In diesem Zeitpunkt wird der 32-Bit-Schlüssel i' dem Beeinflussungsschlüssel Si hinzugefügt, der im Register **85** gehalten wird, durch einen Addierer **86**, um schließlich einen zeitvariablen Schlüssel i zu erzeugen, welcher zum Addierer **81** geliefert wird. Der Addierer **81** addiert den zeitvariablen Schlüssel i, der durch den Addierer **86** ausgegeben wird, zum Anfangswertschlüssel Ss, der im Register **82** gehalten wird, wodurch das Ergebnis der Addition zurück in das Register **82** gespeichert wird.

[0133] Es sei angenommen, dass die Anzahl der Bits pro Wort im Register **82** gleich 8 beträgt. In diesem Fall, da der zeitvariable Schlüssel i, der durch den Addierer **86** ausgegeben wird, gleich 32 Bits bezüglich der Breite beträgt, wird der zeitvariable Schlüssel i in vier Bereiche unterteilt, die jeweils 8 Bit umfassen. Jeder der vier Bereiche wird dann zu einem Wort im Register **82** an einer vorher festgelegten Adresse addiert, d.h., bei einer der Adressen **0** bis **54**.

[0134] Wie oben beschrieben wird der Anfangswertschlüssel Ss anfänglich im Register **82** gehalten. Jedes Mal, wenn **16** Pakete eines verschlüsselten Texts danach übertragen werden, wird jedoch der Anfangswert Ss aktualisiert, wobei der zeitvariable Schlüssel i dazu addiert wird.

[0135] Ein Addierer **83** wählt zwei vorher festgelegte Wörter unter den **55** Wörtern des Registers **82** aus und addiert die ausgewählten beiden Wörter miteinander. Mit dem zeitlichen Ablauf, der in Fig. 12 gezeigt ist, werden Wörter bei Adressen **23** und **54** durch den Addierer **83** ausgewählt. Der Addierer **83** liefert das Ergebnis der Addition zum Verkleinerungsgenerator **73** und ein Wort in das Register **82**. Mit dem in Fig. 12 gezeigten zeitlichen Ablauf liefert der Addierer **83** das Ergebnis der Addition zum Wort des Registers **82** an einer Adresse **0**, um die Daten, die aktuell im Wort gespeichert sind, zu ersetzen.

[0136] Mit dem nächsten zeitlichen Ablauf werden die beiden Wörter, welche durch Addierer **83** ausgewählt wurden, von den Adressen **54** und **23** auf die Adressen **53** und **22** abgeändert, wobei eine Verschiebung in der Richtung, welche in der Figur gezeigt ist, durch ein Wort nach oben durchgeführt wird. Aus dem gleichen Grund wird der Bestimmungsort des Ergebnisses der Addition, der durch den Addierer **83** ausgegeben wird, ebenfalls nach oben verschoben. Da es kein Wort über der Adresse **0** gibt, wird jedoch der Bestimmungsort vom Wort bei der Adresse **0** zum Wort bei der Adresse **54** am Boden des Registers **82** abgeändert.

[0137] Es sollte angemerkt sein, dass in jedem der Addierer **81**, **83** und **86** Verarbeitung, um eine exklusive logische Summe zu berechnen, anstelle davon ausgeführt werden kann.

[0138] Fig. 13 ist ein Blockdiagramm, welches einen typischen Aufbau des LFDR **72** zeigt. Wie in der Figur gezeigt, besitzt das LFSR **72** ein m-Bit-Schieberegister **101** und einen Addierer **102** zum Aufsummieren der Werte einer vorher festgelegten Anzahl von Bits unter den n Bits. Ein Bit, welches aus der Addition durch den Addierer **102** resultiert, wird im äußerst linken Bit b_n des n-Bit-Schieberegisters **101** gespeichert, welches in der Figur gezeigt ist, und, im gleichen Zeitpunkt wird der vorherige Wert des Bits b_n zu einem Bit b_{n-1} auf die rechten Seite des Bits b_n verschoben. Aus dem gleichen Grund wird das Bitverschieben nach rechts auf die vorherigen Werte der Bits b_{n-1}, b_{n-2}, ..., usw. angewandt, wobei der vorherige Wert des äußerst rechten Bits b_1, der in Figur gezeigt ist, ausgegeben wird. Mit dem nächsten zeitlichen Ablauf wird ein Bit, welches von der Addition durch den Addierer **102** resultiert, wiederum im äußerst linken Bit b_n des n-Bit-Schieberegisters **101** gespeichert, und im gleichen Zeitpunkt wird wiederum der vorherige Wert des Bits b_n zu einem Bit b_{n-1} auf die rechte Seite des Bits b_n verschoben. Aus dem gleichen Grund wird das Bitverschieben nach rechts zu einem Gewinn, der auf die vorherigen Werte von Bits b_{n-1}, b_{n-2}, ... usw. angewandt wird, während der vorherige Wert des äußerst rechten Bits b wiederum ausgegeben wird. Diese Operationen werden wiederholt ausgeführt, wobei sequentiell Bits vom äußerst rechten Bit b_1 ein Bit nach dem anderen ausgegeben werden.

[0139] Fig. 13 ist ein Diagramm, welches einen typischen Aufbau des LFSR **72** allgemein zeigt. Dagegen ist Fig. 14 ein Diagramm, welches einen typischen Aufbau des LFSR **72** konkreter zeigt. In dem in Fig. 14 gezeigten Aufbau besitzt das Schieberegister **101** 31 Bits. Der Addierer **102** wird dazu verwendet, den Wert des äußerst linken Bits b_{31} zum Wert des äußerst rechten Bits b_1 zu addieren und das Ergebnis der Addition im äußerst linken Bit **31** des Schieberegisters **101** zu speichern.

[0140] Wie in Fig. 12 gezeigt ist, weist das Verkleinerungsgenerator **73** eine Bedingungsbeurteilungseinheit **91** und eine FIFO-Einheit **92** auf. Die Bedin-

gungsbeurteilungseinheit **91** leitet m-Bit-Daten, welche durch den Addierer **83** geliefert werden, der bei dem Zusatzgenerator **71** verwendet wird, weiter zur FIFO-Einheit **92**, um darin gehalten zu werden, sowie sie sind, wenn das LFDR **72** ein Bit ausgibt, welches den logischen Wert "1" hat. Wenn das LFSR **72** ein Bit ausgibt, welches den logischen Wert "0" hat, leitet dagegen die Bedingungsbeurteilungseinheit **91** die m-Bit-Daten, welche durch den Addierer **83** geliefert werden, der im Zusatzgenerator **71** verwendet wird, nicht zur FIFO-Einheit **92** weiter, wodurch der Verschlüsselungsprozess unterbunden wird. Auf diese Weise wählt die Bedingungsbeurteilungseinheit **91**, welche im Verkleinerungsgenerator **73** verwendet wird, lediglich Bereiche von m-Bit-Daten aus, die jeweils durch den Zusatzgenerator **71** erzeugt werden, während das LFSR **72** ein Bit mit dem logischen Wert "1" ausgibt und die m-Bit-Datenteile im FIFO-Einheit **92** des Generators **73** speichert.

[0141] Jedes Teil der m-Bit-Daten, welche in der FIFO-Einheit **92** gehalten werden, wird als Verschlüsselungsschlüssel zum Addierer **74** geliefert, um einen verschlüsselten Text zu erzeugen, wobei der Verschlüsselungsschlüssel den Daten hinzugefügt wird, welche einen Klartext darstellen, um zu einer Senke übertragen zu werden, d.h., Daten, welche von einer DVD in der Quelle wiedergegeben werden.

[0142] Die verschlüsselten Daten werden dann vom DVD-Wiedergabegerät **1** zur optischen Magnetplattenvorrichtung **3** und zum Personalcomputer **2** über den 1394-Seriell-Bus **11** übertragen.

[0143] Fig. 15 ist ein Diagramm, welches einen typischen Aufbau der 1394-Schnittstelleneinheit **36** zeigt, die bei der optischen Magnetplattenvorrichtung **3** verwendet wird, um die verschlüsselten Daten, welche vom DVD-Wiedergabegerät **1** empfangen werden, mittels des 1394-Seriell-Busses **11** zu entschlüsseln. Wie in der Figur gezeigt ist, weist ähnlich wie die 1394-Schnittstelleneinheit **26**, welche im DVD-Wiedergabegerät **1** verwendet wird, welches in Fig. 11 gezeigt ist, der Aufbau einen Zusatzgenerator **171**, ein LFSR **172**, einen Verkleinerungsgenerator **173** und einen Subtrahierteil **174** auf. m-Bit-Daten, welche durch den Zusatzgenerator **171** erzeugt werden, und 1-Bit-Daten, welche durch das LFSR **172** erzeugt werden, werden zum Verkleinerungsgenerator **173** geliefert. Der Verkleinerungsgenerator **173** wählt einige Teile der m-Bit-Daten aus, welche vom Zusatzgenerator **171** empfangen werden, gemäß dem Wert der 1-Bit-Daten, welche durch das LFSR **172** geliefert werden, und gibt die ausgewählten m-Bit-Daten an den Subtrahierer **174** als Verschlüsselungsschlüssel aus. Der Subtrahierer **174** subtrahiert den m-Bit-Entschlüsselungsschlüssel, der vom Verkleinerungsgenerator **173** empfangen wird, von einem verschlüsselten Text, d.h., m-Bit-Daten, welche vom DVD-Wiedergabegerät **1** empfangen werden, über den 1394-Seriell-Bus **11**, um den verschlüsselten Text zurück in Klartext zu entschlüsseln.

[0144] Es ist offensichtlich, dass der Aufbau der 1394-Schnittstelleneinheit **36**, welche im DVD-Wiedergabegerät **1** verwendet wird, welches in Fig. 15 gezeigt ist, grundsätzlich identisch mit dem der 1394-Schnittstelleneinheit **26** ist, welche bei der optischen Magnetplattenvorrichtung **3**, welche in Fig. 11 gezeigt ist, verwendet wird, mit der Ausnahme, dass der Subtrahierer **174**, der durch das frühere Gerät verwendet wird, als Ersatz für den Addierer **74** des letzteren verwendet wird.

[0145] Fig. 16 ist ein Diagramm, welches einen ausführlichen Aufbau der 1394-Schnittstelleneinheit **36** zeigt, welche in Fig. 15 gezeigt ist, in einer einfachen und einer offenkundigen Weise. Es ist außerdem offensichtlich, dass der Aufbau der 1394-Schnittstelleneinheit **36**, der bei dem DVD-Wiedergabegerät **1** verwendet wird, welches in Fig. 16 gezeigt ist, grundsätzlich identisch mit dem der 1394-Schnittstelleneinheit **26** ist, die bei der optischen Magnetplattenvorrichtung **3** verwendet wird, wie in Fig. 12 gezeigt ist, mit der Ausnahme, dass der Subtrahierer **174**, der früher verendet wurde, als Ersatz für den Addierer **74** des letzteren verwendet wird. Ein Zusatzgenerator **171**, ein LFSR **172**, ein Verkleinerungsgenerator **173**, ein Addierer **181**, ein Register **182**, ein Addierer **183**, ein Register **184**, ein Register **185**, ein Addierer **186**, eine Zustandsbeurteilungseinheit **191** und eine FIFO-Einheit **192**, welche bei der 1394-Schnittstelleneinheit **36** der optischen Magnetplattenvorrichtung **3**, welche in Fig. 16 gezeigt ist, verwendet werden, entsprechen dem Zusatzgenerator **71**, dem LFSR **72**, dem Verkleinerungsgenerator **73**, dem Addierer **81**, dem Register **82**, dem Addierer **83**, dem Register **84**, dem Register **85**, dem Addierer **86**, der Zustandsbeurteilungseinheit **91** und einer FIFO-Einheit **92**, welche bei der 1394-Schnittstelleneinheit **26** des DVD-Wiedergabegeräts **1**, welches in Fig. 12 gezeigt ist, verwendet werden.

[0146] Da somit der Betrieb der 1394-Schnittstelleneinheit **36**, die bei der optischen Magnetplattenvorrichtung **3** verwendet wird, die in Fig. 16 gezeigt ist, grundsätzlich der gleiche ist, wie der der 1394-Schnittstelleneinheit **26**, die im DVD-Wiedergabegerät **1** verwendet wird, welches in Fig. 12 gezeigt ist, wird eine Erläuterung dafür nicht wiederholt. Es sollte jedoch angemerkt sein, dass die frühere Vorrichtung gegenüber der späteren dahingehend verschieden ist, dass im Fall der früheren Vorrichtung der Subtrahierer **174** den m-Bit-Entschlüsselungsschlüssel, der von der FIFO-Einheit **192** empfangen wird, die bei dem Verkleinerungsgenerator **173** verwendet wird, von einem verschlüsselten Text, d.h., m-Bit-Daten, welche vom DVD-Wiedergabegerät **1** empfangen werden, mittels des 1394-Seriell-Busses **11** subtrahiert, um den verschlüsselten Text in den

Klartext zu entschlüsseln.

[0147] In der 1394-Schnittstelleneinheit **36**, welche bei der optischen Magnetplattenvorrichtung **3** verwendet wird, werden verschlüsselte Daten lediglich einmal unter Verwendung eines Sitzungsschlüssel S entschlüsselt, der einen Anfangswertschlüssel Ss und einen Beeinflussungsschlüssel Si aufweist, und einen zeitvariablen Schlüssel i, streng ausgedrückt den Schlüssel i', wie oben beschrieben.

[0148] Bei dem Personalcomputer **2** werden dagegen verschlüsselte Daten durch die 1394-Schnittstelleneinheit **49** unter Verwendung eines zeitvariablen Schlüssels **1** entschlüsselt, der durch den Beeinflussungsschlüssel Si des Sitzungsschlüssels S und eines Schlüssels i' in einer ersten Stufe einer Entschlüsselung erzeugt wird, und dann weiter durch die Anwendungseinheit **61** und Verwendung eines Anfangswertschlüssels Ss des Sitzungsschlüssels S in einer zweiten Stufe einer Verschlüsselung entschlüsselt.

[0149] Fig. 17 ist ein Diagramm, welches einen typischen Aufbau der 1394-Schnittstelleneinheit **49** zeigt, die beim Personalcomputer **2** verwendet wird, um die verschlüsselten Daten oder den verschlüsselten Text, der von dem DVD-Wiedergabegerät **1** empfangen wird, über den 1394-Seriell-Bus **11** mittels Hardware zu entschlüsseln. Wie in der Figur gezeigt ist, weist ähnlich wie die 1394-Schnittstelleneinheit **36**, welche in der optischen Magnetplattenvorrichtung **3** verwendet wird, die in Fig. 15 gezeigt ist, und die 1394-Schnittstelleneinheit **26**, welche im DVD-Wiedergabegerät **1** verwendet wird, welches in Fig. 11 gezeigt ist, der Aufbau einen Zusatzgenerator **271**, ein LFSR **272**, einen Verkleinerungsgenerator **273** und einen Subtrahierer **274** auf, die dem Zusatzgenerator **171**, dem LFSR **172**, dem Verkleinerungsgenerator **173** und dem Subtrahierer **174**, die in Fig. 15 entsprechend gezeigt sind, entsprechen. Der Schlüssel i' zum Erzeugen des zeitvariablen Schlüssels i und der Beeinflussungsschlüssel Si des Sitzungsschlüssels S zum Beeinflussen des zeitvariablen Schlüssels i, der der 1394-Einheit **49** zugeführt wird, die in Fig. 17 gezeigt ist, vom Lizenzmanager **62** sind gleich wie der Schlüssel i' und der Beeinflussungsschlüssel Si, welche der 1394-Schnittstelleneinheit **36**, welche in Fig. 15 gezeigt ist, von der Firmware **30** zugeführt wird. Jedoch werden alle Bits des Anfangswertschlüssels Ss des Sitzungsschlüssels S, die der 1394-Einheit **49** zugeführt werden, die in Fig. 17 gezeigt ist, auf 0 zurückgesetzt.

[0150] Fig. 18 ist ein Diagramm, welches einen ausführlichen Aufbau der 1394-Schnittstelleneinheit **49** zeigt, welche in Fig. 17 in einer einfachen und offenkundigen Weise gezeigt ist. Es ist ebenfalls offenkundig, dass der Aufbau der 1394-Schnittstelleneinheit **49**, der im Personalcomputer **2** verwendet wird, der in Fig. 18 gezeigt ist, grundsätzlich identisch mit dem der 1394-Schnittstelleneinheit **26** ist, die im DVD-Wiedergabegerät **1** verwendet wird, welches in Fig. 12 gezeigt ist, und der 1394-Schnittstelleneinheit **36**, welche in der optischen Magnetplattenvorrichtung **3** verwendet wird, die in Fig. 16 gezeigt ist, mit der Ausnahme, dass bei der in Fig. 18 gezeigten 1394-Schnittstelleneinheit **49**, da alle Bits des Anfangswertschlüssels Ss des Sitzungsschlüssels S, der der 1394-Einheit **49** zugeführt wird, die in Fig. 17 gezeigt ist, auf 0 zurückgesetzt sind, im Wesentlichen der Entschlüsselungsschlüssel lediglich von dem zeitvariablen Schlüssel i erzeugt wird, der von dem Schlüssel i' und dem Beeinflussungsschlüssel Si erzeugt wird, als ob der Anfangswertschlüssel Ss nicht verfügbar wäre. Als Ergebnis werden im Subtrahierer **274** die verschlüsselten Daten oder der verschlüsselte Text unter Verwendung lediglich des zeitvariablen Schlüssels i entschlüsselt. Da der Anfangswertschlüssel Ss nicht bei der Entschlüsselung verwendet wird, wird noch nicht ein vollständiger Klartext als Ergebnis der Entschlüsselung erlangt. Das heißt, dass das Ergebnis der Entschlüsselung noch ein Verschlüsselungszustand ist. Damit können Daten, welche aus der Entschlüsselung resultieren, nicht verwendet werden, so wie sie sind, sogar, wenn die Daten von dem internen Bus **51** zur Festplatte, die im Festplattenlaufwerk **47** befestigt ist, oder auf einen anderen Aufzeichnungsträger kopiert werden.

[0151] Dann werden die Daten oder der Text, der durch Hardware in der 1394-Schnittstelleneinheit **49** unter Verwendung des zeitvariablen Schlüssels i entschlüsselt wurden, weiter durch Software im Anwendungsmodul **61** entschlüsselt. Fig. 19 ist ein Diagramm, welches einen typischen Aufbau des Anwendungsmoduls **61** zeigt. Grundsätzlich ähnlich wie die 1394-Schnittstelleneinheit **26**, welche im DVD-Wiedergabegerät **1** verwendet wird, welches in Fig. 11 gezeigt ist, die 1394-Schnittstelleneinheit **36**, die in der optischen Magnetplattenvorrichtung **3** verwendet wird, die in Fig. 15 gezeigt ist, und die 1394-Schnittstelleneinheit **49**, welche im Personalcomputer **2** verwendet wird, die in Fig. 17 gezeigt ist, weist das Anwendungsmodul **61**, welches in Fig. 19 gezeigt ist, einen Zusatzgenerator **371**, ein LFSR **372**, einen Verkleinerungsgenerator **373** und einen Subtrahierer **374** auf, die einen Aufbau haben, der identisch mit dem Zusatzgenerator **171**, dem LFSR **172**, dem Verkleinerungsgenerator **173** und dem Subtrahierer **174** ist, der entsprechend in Fig. 15 gezeigt ist.

[0152] Es sollte jedoch angemerkt sein, dass, obwohl der Anfangswertschlüssel Ss des Sitzungsschlüssels S zum Anwendungsmodul **61** geliefert wird, so wie dies beim Fall bei der 1394-Schnittstelleneinheit **26** ist, welche im DVD-Wiedergabegerät **1** verwendet wird, welche in Fig. 11 gezeigt ist, und der 1394-Schnittstelleneinheit **36**, welche in der optischen Magnetplattenvorrichtung **3** verwendet wird,

die in Fig. 15 gezeigt ist, der Beeinflussungsschlüssel Si des Sitzungsschlüssels S zum Beeinflussen des zeitvariablen Schlüssels i und des Schlüssels i' jeweils ein Einheitselement sind, bei denen alle Bits auf 0 zurückgesetzt sind.

[0153] Fig. 20 ist ein Diagramm, welches einen ausführlichen Aufbau des Anwendungsmoduls **61**, welches in Fig. 19 gezeigt ist, in einer einfachen und offenkundigen Weise zeigt. Es ist ebenfalls offensichtlich, dass der Aufbau des Anwendungsmoduls **61** grundsätzlich gleich ist mit dem der 1394-Schnittstelleneinheit **26**, welche im DVD-Wiedergabegerät **1**, welches in Fig. 12 gezeigt ist, verwendet wird, der 1394-Schnittstelleneinheit **36**, welche bei der optischen Magnetplattenvorrichtung **3** verwendet wird, die in Fig. 16 gezeigt ist, und der 1394-Schnittstelleneinheit **49**, welche im Personalcomputer **1**, der in Fig. 18 gezeigt ist, verwendet wird. Komponenten, welche im Anwendungsmodul **61** verwendet werden, welches ausführlich in Fig. 20 gezeigt ist, vom Addierer **381**, der im Zusatzgenerator **371** verwendet wird, zur FIFO-Einheit **392**, welche im Verkleinerungsgenerator **373** verwendet wird, entsprechen den Komponenten, welche in der 1394-Schnittstelleneinheit **36** verwendet werden, welche in Fig. 16 gezeigt ist, vom Addierer **181**, der im Zusatzgenerator **171** verwendet wird, zur FIFO-Einheit **192**, die im Verkleinerungsgenerator **173** entsprechend verwendet wird. Da alle Bits des Schlüssels i', welche in einem Register **384** gehalten werden, und der Beeinflussungsschlüssel Si, der im Register **385** gehalten wird, 0 sind, sind jedoch alle Bits des zeitvariablen Schlüssels i, der durch den Addierer **386** erzeugt wird, 0. Als Folge davon arbeitet das Anwendungsmodul **61** im Wesentlichen, als ob der zeitvariable Schlüssel i nicht vorhanden wäre. Das heißt, dass die Erzeugung eines Entschlüsselungsschlüssels lediglich auf dem Anfangswertschlüssel Ss basiert. Dann entschlüsselt ein Subtrahierer **374** die verschlüsselten Daten oder unter Verwendung des Verschlüsselungsschlüssels, der auf diese Weise erzeugt wurde, um einen Klartext zu erzeugen. Wie oben beschrieben sind die verschlüsselten Daten ein Ergebnis der Entschlüsselung, welche durch die 1394-Schnittstelleneinheit **49** ausgeführt wurde, auf der Basis des zeitvariablen Schlüssels i, welcher vom Schlüssel i' und dem Beeinflussungsschlüssel Si erzeugt wird, in der sogenannten ersten Stufe der Entschlüsselung. Dagegen wird die Entschlüsselung, welche durch das Anwendungsmodul **61** auf der Basis des Anfangswertschlüssels Ss ausgeführt wird, als zweite Stufe der Verschlüsselung bezeichnet, um einen endgültigen vollständigen Klartext zu erzeugen.

[0154] Wenn die Entschlüsselung des verschlüsselten Texts, wie oben beschrieben, in der optischen Magnetplattenvorrichtung **3** beendet ist, liefert die CPU **31** die verschlüsselten Daten zum Laufwerk **35**, um die Daten auf einer magneto-optischen Platte aufzuzeichnen.

[0155] Im Personalcomputer **2** liefert dagegen die CPU **41** die entschlüsselten Daten, welche von der ersten Stufe der Entschlüsselung resultieren, die durch die 1394-Schnittstelleneinheit **49** ausgeführt wurde, üblicherweise zum Festplattenlaufwerk **47**, um die Daten über den internen Bus **51** aufzuzeichnen. Es sollte angemerkt sein, dass im Personalcomputer **2** eine vorher festgelegte Leiterplatte mit der Eingangs-/Ausgangsschnittstelleneinheit **44** als Erweiterungsplatte angeschaltet sein kann, um Daten, welche über den internen Bus **51** wie früher beschrieben zu überwachen. Trotzdem ist es lediglich das Anwendungsmodul **61**, welches in der Lage ist, endgültig Daten, welche über den internen Bus **51** übertragen werden, zu entschlüsseln. Somit sind, sogar, wenn die Erweiterungsplatte **48** in der Lage ist, verschlüsselte Daten zu überwachen, welche von der Entschlüsselung resultieren, die durch die 1394-Schnittstelleneinheit **49** ausgeführt wird, auf der Basis des zeitvariabeln Schlüssels i, die verschlüsselten Daten nicht vollständig Klartext, da die Daten durch das Anwendungsmodul **61** unter Verwendung des anfänglichen Wertschlüssels Ss des Sitzungsschlüssels S nicht entschlüsselt wurden. Als Ergebnis ist es möglich, zu verhindern, dass ein vollständiger Klartext illegal kopiert werden kann, vorausgesetzt, dass der vollständige Klartext, der von der endgültigen Verschlüsselung resultiert, welche durch das Anwendungsmodul **61** ausgeführt wird, niemals über den internen Bus **51** übertragen wird.

[0156] Üblicherweise erlaubt es die Anwendung des Diffie-Hellman-Verfahrens, dass der Sitzungsschlüssel S durch eine Quelle und Senken anteilig genutzt werden kann.

[0157] Es ist wert, anzumerken, dass es Fälle gibt, bei denen die 1394-Schnittstelleneinheit **49** oder das Anwendungsmodul **61**, welche im Personalcomputer **2** verwendet werden, eine relativ niedrige Verarbeitungsleistung hat, so dass dies nicht in der Lage ist, das Entschlüsseln von Daten auszuführen. Um mit einem derartigen Problem fertig zu werden, kann entweder der Anfangswertschlüssel Ss des Sitzungsschlüssels S und der zeitvariable Schlüssel i oder beide in der Quelle als Einheitselement erzeugt werden. Aus dem gleichen Grund können unter Verwendung einer oder beider Schlüssel als Einheitselement in der Senke Daten virtuell von der Quelle zur Senke übertragen werden, ohne den Anfangswertschlüssel Ss des Sitzungsschlüssels S und den zeitvariablen Schlüssel i zu verwenden. Mit diesem Verfahren ist es jedoch innerhalb des Bereichs des Möglichen wahrscheinlicher, dass die Daten illegal kopiert werden können.

[0158] Wenn das Anwendungsmodul **61** selbst eine illegale Kopie ist, muss man sehr befürchten, dass

der Klartext, der von der Entschlüsselung resultiert, welche durch das Anwendungsmodul **61** ausgeführt wird, ebenfalls illegal kopiert wird. Um dieses Problem zu lösen, kann der Lizenzmanager **62** das Anwendungsmodul **61** vor einer Entschlüsselung wie früher beschrieben bestätigen.

[0159] Als Verfahren zum Bestätigen des Anwendungsmoduls **61** kann eine digitale Signatur auf der Basis eines offenbarten Verschlüsselungsschlüssel-Verschlüsselungsverfahrens zusätzlich zu dem gemeinsamen Sitzungsschlüssel-Entschlüsselungs/Entschlüsselungsverfahren, welches früher beschrieben wurde, angenommen werden.

[0160] Die in Fig. 11, Fig. 12 und Fig. 15 bis Fig. 20 gezeigten Konfigurationen erfüllen einen Homomorphismus. Das heißt, wenn die Schlüssel K_1 und K_2 Elemente eines Galois-Felds G sind, ist ein Gruppenverarbeitungsergebnis K_1. K_2 der beiden Elemente ebenfalls ein Element des Galois-Felds G. Außerdem gilt mit Bezug auf die oben vorher festgelegte Funktion H die folgende Gleichung:

$$H(K_1 \cdot K_2) = H(K_1) \cdot H(K_2)$$

[0161] Fig. 21 ist ein Diagramm, welches einen weiteren typischen ausführlichen Aufbau der 1394-Schnittstelleneinheit **26** zeigt, welche im DVD-Wiedergabegerät **1** verwendet wird. Wie in der Figur gezeigt ist, wird der Anfangswertschlüssel Ss des Sitzungsschlüssels S zu LFSRs **501** bis **503** geliefert, um damit als Anfangswerte gesetzt zu werden. Die Breiten der LFSRs **501** bis **503** sind n_1 bis n_3 Bits entsprechend, welche in der Größenordnung von 20 Bits sind. Die LFSRs **501** bis **503** so bestimmt, dass ihre Breiten n_1 bis n_3 ein Element in Verbindung miteinander bilden. Das heißt, dass beispielsweise die höherwertigeren n1-Bits, die Bits n_2 einer Zwischenordnung und die niederwertigeren n_3 Bits des Anfangswertschlüssels Ss des Sitzungsschlüssels S in den LFSRs **501**, **502** bzw. **503** jeweils als Anfangswert eingestellt sind.

[0162] Wenn ein Freigabesignal mit dem logischen Wert 1 zu den LFSRs **501** bis **503** von einer Taktungsfunktionseinheit **506** geliefert wird, verschieben die LFSRs **501** bis **503** jeweils ihren Inhalt um m Bits, wobei m-Bit-Daten ausgegeben werden. Der Wert von m kann üblicherweise auf 8, 16, 32 oder 40 eingestellt werden.

[0163] Die Daten, welche durch das LFSR **501** ausgegeben werden, werden den Daten, welche durch das LFSR **502** ausgegeben werden, durch einen Addierer **504** hinzugefügt. Ein Übertrag des Ergebnisses der Addition, die durch den Addierer **504** ausgeführt wird, wird zur Taktungsfunktionseinheit **506** geliefert, und das Ergebnis der Addition selbst wird den Daten, welche durch das LFSR **503** ausgegeben werden, durch einen Addierer **505** hinzugefügt. Ein Übertrag des Ergebnisses der Addition, die durch den Addierer **504** ausgeführt wird, wird ebenfalls zur Taktungsfunktionseinheit **506** geliefert, und das Ergebnis der Addition selbst wird zu einer exklusiven logischen Summenberechnungsschaltung **508** geliefert.

[0164] Die Kombination der Überträge, welche durch die Addierer **504** und **505** zur Taktungsfunktionseinheit **506** geliefert werden, ist entweder 00, 01, 10 oder 11. Die Taktungsfunktionseinheit **506** gibt Daten, welche eine der Kombinationen **00** bis **11** zeigen, an die LFSRs **501** bis **503** gemäß der Kombination der Überträge, die von den Addierern **504** und **505** empfangen werden, aus. Wie oben beschrieben, wenn das Freigabesignal mit dem logischen Wert 1 zu den LFSRs **501** bis **503** von der Taktfunktionseinheit **506** geliefert wird, verschieben die LFSRs **501** bis **503** ihren Inhalt um m Bits, geben neue m-Bit-Daten aus. Wenn das Freigabesignal mit dem logischen Wert 0 zu den LFSRs **501** bis **503** von der Taktungsfunktionseinheit **506** geliefert wird, verschieben dagegen die LFSRs **501** bis **503** ihren Inhalt nicht, geben die gleichen m-Bit-Daten als die Daten aus, die unmittelbar vorher ausgegeben werden.

[0165] Die exklusive logische Summenberechnungsschaltung **508** empfängt das Additionsergebnis, welches durch den Addierer **505** ausgeführt wurde, und den zeitvariablen Schlüssel i, der im Register **507** gespeichert ist, und berechnet eine exklusive logische Summe der Eingangssignale. Eine exklusive logische Summenberechnungsschaltung **509** berechnet eine weitere exklusive logische Summe der exklusiven logischen Summe, die durch die exklusive logische Summenberechnungsschaltung **508** ausgegeben wird, und einen zugeführten Klartext, wobei die andere exklusive logische Summe als verschlüsselter Text ausgegeben wird.

[0166] Fig. 22 ist ein Diagramm, welches einen weiteren typischen ausführlichen Aufbau der 1394-Schnittstelleneinheit **36** zeigt, die in der optischen Magnetplattenvorrichtung **3** verwendet wird. Wie in der Figur gezeigt ist, haben alle Komponenten, welche in der 1394-Schnittstelleneinheit **36** verwendet werden, von einem LFSR **601** bis zu einer exklusiven logischen Summenberechnungsschaltung **609** den gleichen Aufbau wie die entsprechenden Elemente, welche in der 1394-Schnittstelleneinheit **26** verwendet werden, die in Fig. 21 gezeigt ist, vom LFSR **501** bis zur exklusiven logischen Summenberechnungsschaltung **509**. Da somit ihre Arbeitsweise grundsätzlich die gleiche ist, wird eine Erläuterung ihrer Arbeitsweise nicht wiederholt. Der einzige Unterschied zwischen der 1394-Schnittstelleneinheit, die in der optischen Magnetplattenvorrichtung **3** verwendet wird, die in Fig. 22 gezeigt ist, und der 1394-Schnittstelleneinheit **26**, welche im DVD-Wie-

dergabegerät **1** verwendet wird, welches in Fig. 21 gezeigt ist, ist der, dass die exklusive logische Summenberechnungsschaltung **609**, die früher verwendet wurde, einen verschlüsselten Text entschlüsselt, während die exklusive logische Summenberechnungsschaltung **509**, die später verwendet wird, einen Klartext verschlüsselt.

[0167] Fig. 23 ist ein Diagramm, welches einen weiteren typischen ausführlichen Aufbau der 1394-Schnittstelleneinheit **49** zeigt, welcher im Personalcomputer **2** verwendet wird. Wie in der Figur gezeigt ist, haben alle Komponenten, welche in der 1394-Schnittstelleneinheit **49** verwendet werden, von einem LFSR **701** bis zu einer exklusiven logischen Summenberechnungsschaltung **709** den gleichen Aufbau wie die entsprechenden Elemente, welche in der 1394-Schnittstelleneinheit **36** verwendet werden, die in Fig. 22 gezeigt ist, von dem LFSR **601** bis zur exklusiven logischen Summenberechnungsschaltung **609**. Der einzige Unterschied zwischen der 1394-Schnittstelleneinheit **36**, welche in der optischen Magnetplattenvorrichtung **3** verwendet wird, die in Fig. 22 gezeigt ist, und der 1394-Schnittstelleneinheit **49**, die im Personalcomputer **2** verwendet wird, der in Fig. 23 gezeigt ist, ist der, dass der Anfangswertschlüssel Ss des Sitzungsschlüssels S, der zu den LFSRs **701** bis **703** geliefert wird, der in der späteren Vorrichtung verwendet wird, ein Einheitselement ist, wobei alle Bits auf 0 zurückgesetzt sind. Damit basiert bei der 1394-Schnittstelleneinheit **49**, welche im Personalcomputer **2** verwendet wird, der in Fig. 23 gezeigt ist, die Entschlüsselung eines verschlüsselten Texts im Wesentlichen lediglich auf dem zeitvariablen Schlüssel i im Register **701**, der vom Schlüssel i' erzeugt wird, und dem Beeinflussungsschlüssel Si des Sitzungsschlüssels S.

[0168] Fig. 24 ist ein Diagramm, welches einen weiteren typischen ausführlichen Aufbau des Anwendungsmoduls **61** des Personalcomputers **2** zeigt. Wie in der Figur gezeigt ist, haben alle Komponenten, welche im Anwendungsmodul **61** verwendet werden, von einem LFSR **801** bis zu einer exklusiven logischen Summenberechnungsschaltung **809** den gleichen Aufbau wie die entsprechenden Komponenten, welche in der 1394-Schnittstelleneinheit **36** verwendet werden, die in Fig. 22 gezeigt ist, von dem LFSR **601** zur exklusiven logischen Summenberechnungsschaltung **609**. Der einzige Unterschied zwischen der 1394-Schnittstelleneinheit **36**, welche in der optischen Magnetplattenvorrichtung **3** verwendet wird, welche in Fig. 22 gezeigt ist, und dem Anwendungsmodul **61** des Personalcomputers **2**, der in Fig. 24 gezeigt ist, ist der, dass der zeitvariable Schlüssle i, der zum Register **807** geliefert wird, der im letzteren verwendet wird, ein Einheitselement ist, wobei alle Bits auf 0 zurückgesetzt sind. Somit basiert bei dem Anwendungsmodul **61**, welches im Personalcomputer **2** verwendet wird, der in Fig. 24 gezeigt ist, die Verschlüsselung von verschlüsselten Daten im Wesentlichen lediglich auf dem Anfangswertschlüssel Ss des Sitzungsschlüssels S.

[0169] Es sollte angemerkt sein, dass die Entschlüsselungsverarbeitung in jeder der Aufbauten, die in Fig. 19, Fig. 20 und Fig. 24 gezeigt sind, durch das Anwendungsmodul **61** ausgeführt wird, welche üblicherweise durch Software ausgeführt wird.

[0170] Der Lizenzschlüssel kann übrigens geändert oder aktualisiert werden, wenn dies notwendig ist, sollte der Lizenzschlüssel aus irgendeinem Grund durch irgendeine Gelegenheit gestohlen werden. Es erübrigt sich, auszuführen, dass ein Lizenzschlüssel auch einmal in einer vorher festgelegten Zeitperiode geändert werden kann, sogar wenn der Lizenzschlüssel nicht gestohlen ist, sollte dies ziemlich innerhalb des Bereichs des Möglichen sein, dass der Lizenzschlüssel gestohlen ist. In diesem Fall wird die Version eines Lizenzschlüssels, der die Gültigkeitsdauer zeigt, auf einer DVD aufgezeichnet sein. Bei der vorliegenden Ausführungsform wird die Gültigkeitsdauer eines Lizenzschlüssels durch die Häufigkeit dargestellt, mit der die Hash-Funktion angewandt wird, um den Lizenzschlüssel zu erzeugen. Wenn eine Informationsempfangsvorrichtung zum Empfangen von Information, die über einen Satelliten anstelle einer Information, die von einem DVD-Wiedergabegerät wiedergegeben wird, übertragen wird, ein Objekt ist, welches betrieben wird, wird lediglich Information einer berechtigten Version über den Satelliten zur Informationsempfangsvorrichtung übertragen.

[0171] Fig. 25 und Fig. 26 sind Diagramme, welche eine Ausführungsform zeigen, bei der eine Prozedur zum Erzeugen eines quellenseitigen gemeinsamen Sitzungsschlüssels sk im DVD-Wiedergabegerät **1** und eines senkseitigen gemeinsamen Sitzungsschlüssels sk' im Personalcomputer **2** unter Verwendung eines aktualisierten Lizenzschlüssels ausgeführt wird. Es sollte angemerkt sein, dass zusätzlich zu der Tatsache, dass verschiedene Informationsabschnitte in der EEPROM-Einheit **27** gespeichert sind, welche im DVD-Wiedergabegerät **1** verwendet wird, und in der EEPROM-Einheit **50**, welche im Personalcomputer **2** verwendet wird, der Ausführungsform, die in Fig. 4 gezeigt ist, die Hash-Funktion nicht nur in der EEPROM-Einheit **26**, sondern auch in der EEPROM-Einheit **50** bei der vorliegenden Ausführungsform gespeichert ist.

[0172] Wie in Fig. 25 gezeigt ist, beginnt die Prozedur mit einem Schritt S151, in welchem das DVD-Wiedergabegerät **1**, welches als Quelle dient, eine Anforderung an den Personalcomputer **2**, der als Senke dient, nach der ID macht. Danach läuft die Prozedur weiter zu einem Schritt S152, in welchem der Personalcomputer **2** die Anforderung nach der ID

empfängt. Die Prozedur läuft dann weiter zu einem Schritt 153, in welchem der Personalcomputer **2** die ID zum DVD-Wiedergabegerät **1** überträgt. Die Prozedur fährt dann fort zu einem Schritt S154, in welchem das DVD-Wiedergabegerät **1** die ID empfängt.

[0173] Nachfolgend läuft die Prozedur weiter zu einem Schritt S155, in welchem das DVD-Wiedergabegerät **1** die ID, welche vom Personalcomputer **2** empfangen wird, mit einem Dienstschlüssel verkettet, der in der EEPROM-Einheit **27** gespeichert ist, um Daten (ID || Dienstschlüssel) zu bilden. Dann wird ein Lizenzschlüssel lk berechnet, wobei die Hash-Funktion auf die Daten (ID || Dienstschlüssel) angewandt wird, wie in der folgenden Gleichung gezeigt ist:

lk = hash (ID || Dienstschlüssel)

[0174] Die Verarbeitungsabschnitte, die in den Schritten S151 bis S155 ausgeführt werden, sind wie oben beschrieben die gleichen wie die, welche in den Schritten S1 bis S5 der in Fig. 4 gezeigten Prozedur ausgeführt werden.

[0175] Die Prozedur läuft dann weiter zu einem Schritt S156, in welchem das DVD-Wiedergabegerät **1** eine Beurteilung tätigt, ob oder nicht der Lizenzschlüssel lk, der im Schritt S155 erzeugt wurde, eine berechtigte Version ist, d.h., ob der Lizenzschlüssel lk unter Anwendung der Hash-Funktion mit einer Häufigkeit gleich einem vorher festgelegten Wert, der auf der DVD aufgezeichnet ist, erzeugt wurde. Wie oben beschrieben ist die aktuell gültige Version eines Lizenzschlüssels lk als vorher festgelegter Wert aufgezeichnet, der die Häufigkeit zeigt, mit der die Hash-Funktion angewandt wird, um den Lizenzschlüssel lk zu erzeugen. Es sei angenommen, dass der vorher festgelegte Wert, der auf der DVD aufgezeichnet wurde, größer als eins ist. Da die Häufigkeit, mit der die Hash-Funktion angewandt wurde, um den Lizenzschlüssel lk im Schritt S155 zu erzeugen, gleich 1 ist, wird beurteilt, dass der Lizenzschlüssel lk ungültig ist. In diesem Fall läuft die Prozedur weiter zu einem Schritt S157, in welchem das DVD-Wiedergabegerät **1** eine Variable g initialisiert, welche die Häufigkeit zeigt, mit der die Hash-Funktion angewandt wurde, um den Lizenzschlüssel lk bei 1 zu erzeugen, und speichert den erzeugten Lizenzschlüssel lk in einer Variablen lk_g. Dann läuft die Prozedur weiter zu einem Schritt S158, in welchem die Hash-Funktion auf den Inhalt der Variablen lk_g angewandt wird, um einen neuen Lizenzschlüssel lk_{g+1} gemäß der folgenden Gleichung zu finden:

lk_{g+1} = hash (lk_g)

[0176] Nachfolgend läuft die Prozedur weiter zu einem Schritt S159, um eine Beurteilung zu bilden, ob der Lizenzschlüssel lk_{g+1}, der im Schritt S158 erzeugt wurde, eine gültige Version ist oder nicht. Wenn der Lizenzschlüssel lk_{g+1} keine gültige Version hat, d.h., wenn die Variable g nicht den vorher festgelegten Wert bei der vorliegenden Ausführungsform erreicht hat, läuft die Prozedur weiter zu einem Schritt S160, in welchem das DVD-Wiedergabegerät **1** den Wert der Variablen g um 1 inkrementiert und lk_{g+1} in der Variablen lk_g speichert. Die Prozedur kehrt dann zurück zum Schritt S158, in welchem die Hash-Funktion wiederum auf den Inhalt der Variablen lk_g angewandt wird.

[0177] Die Schritte S158 und S159 werden wiederholt ausgeführt, bis der Wert der Variablen g, d.h., die Häufigkeit, mit der die Hash-Funktion angewandt wurde, den Lizenzschlüssel zu erzeugen, den vorher festgelegten Wert erreicht, der auf der DVD als eine Version des Lizenzschlüssels aufgezeichnet wurde.

[0178] Es sollte angemerkt sein, dass der vorher festgelegte Wert, der als obere Grenze der Häufigkeit dient, mit der die Hash-Funktion angewandt werden kann, um den Lizenzschlüssel zu erzeugen, üblicherweise auf **100** festgelegt ist.

[0179] Wenn das Ergebnis der Beurteilung, welche im Schritt S159 gebildet wird, zeigt, dass die Häufigkeit, mit der die Hash-Funktion angelegt wurde, um den Lizenzschlüssel zu erzeugen, den vorher festgelegten Wert erreicht hat, der auf der DVD als eine Version des Lizenzschlüssels aufgezeichnet wurde, d.h., wenn das Ergebnis der Beurteilung zeigt, dass ein gültiger Lizenzschlüssel lk_{g+1} im Schritt S158 erlangt wurde, oder wenn das Ergebnis der Beurteilung, die im Schritt S156 gebildet wurde, zeigt, dass der Lizenzschlüssel lk, der im Schritt S155 erzeugt wurde, gültig ist, d.h., wenn die Häufigkeit, mit der die Hash-Information angewandt wird, um den Lizenzschlüssel zu erzeugen, gleich 1 ist, läuft dagegen die Prozedur zu einem Schritt S161, in welchem das DVD-Wiedergabegerät **1** einen quellenseitigen gemeinsamen Sitzungsschlüssel sk in der gleichen Weise wie die Prozedur von Fig. 4, die früher beschrieben wurde, erzeugt.

[0180] Dann läuft die Prozedur weiter zu einem Schritt S162, in welchem das DVD-Wiedergabegerät **1** den quellenseitigen gemeinsamen Sitzungsschlüssel sk, der im Schritt S161 erzeugt wurde, unter Verwendung des Lizenzschlüssels lk_g, der im Schritt S155 oder S158 als Schlüssel berechnet wurde, verschlüsselt, um einen verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e gemäß der folgenden Gleichung zu erzeugen:

e = Enc (lk_g, sk)

[0181] Anschließend läuft die Prozedur weiter zu einem Schritt S163, in welchem das DVD-Wiedergabegerät **1** den verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e, der im Schritt S162 er-

zeugt wurde, gemeinsam mit dem Wert der Variablen g, welche die Häufigkeit zeigt, mit der die Hash-Funktion angewandt wurde, um den Lizenzschlüssel lk_g zu erzeugen, zum Personalcomputer **2** überträgt. Die Prozedur läuft dann weiter zu einem Schritt S164, in welchem der Personalcomputer **2** den verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e und den Wert der Variablen g empfängt. Dann läuft die Prozedur weiter zu einem Schritt S165, in welchem der Personalcomputer **2** eine Variable w initialisiert, welche die Häufigkeit zeigt, mit der die Hash-Funktion angewandt wurde, um einen Lizenzschlüssel im Personalcomputer **2** bei **1** zu erzeugen. Die Prozedur läuft dann weiter zu einem Schritt S166, um eine Beurteilung zu bilden, ob der Wert der Variablen g, welche im Schritt S164 empfangen wurde, gleich dem Wert der Variabeln w, welche im Schritt S165 gesetzt wurde, ist oder nicht. Wenn diese nicht einander gleich sind, läuft die Prozedur weiter zu einem Schritt S167, bei dem die Hash-Funktion, welche in der EEPROM-Einheit gespeichert wurde, die im Personalcomputer **2** verwendet wurde, auf den Lizenzschlüssel w angewandt wird, der Lizenzschlüssel auch in der EEPROM-Einheit **50** gespeichert wird, um einen Lizenzschlüssel w + 1, einen neuen Lizenzschlüssel gemäß der folgenden Gleichung zu erzeugen:

$$Lizenzschlüssel_{w+1} = hash\ (Lizenzschlüssel_w)$$

[0182] Dann läuft die Prozedur weiter zu einem Schritt S168, in welchem der Personalcomputer **2** die Variable w um 1 inkrementiert und den $Lizenzschlüssel_{w+1}$ durch den $Lizenzschlüssel_w$ ersetzt. Die Prozedur kehrt dann zurück zum Schritt S166, um wiederum eine Beurteilung zu bilden, ob der Wert der Variablen w gleich dem Wert der Variablen w ist oder nicht. Diese Schritte S166 bis S168 werden wiederholt ausgeführt, bis der Wert der Variablen w, der die Häufigkeit zeigt, mit der die Hash-Funktion angewandt wurde, um den Lizenzschlüssel zu erzeugen, gleich dem Wert der Variablen g wird.

[0183] Wenn das Ergebnis der Beurteilung, die im Schritt S166 gebildet ist, zeigt, dass der Wert der Variablen w gleich dem Wert der Variablen g ist, d.h., wenn aktuell ein gültiger $Lizenzschlüssel_w$ erhalten wurde, läuft die Prozedur weiter zu einem Schritt S169, in welchem der Personalcomputer **2** den verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel entschlüsselt, um einen senkseitigen gemeinsamen Sitzungsschüssel sk' gemäß der folgenden Gleichung zu erzeugen:

$$sk' = Dec\ (Lizenzschlüssel_w, e)$$

[0184] Durch passendes Wiederholen der Anwendung der Hash-Funktion, um den Lizenzschlüssel wie oben beschrieben zu erzeugen, kann die Informationssicherheit weiter verbessert werden.

[0185] Gemäß der Prozedur, welche in Fig. 25 und Fig. 26 gezeigt ist, wird der Wert der Variablen g, welche die Version eines Lizenzschlüssels zeigt, durch die Quelle zur Senke übertragen. Es sollte angemerkt sein, dass die Anwendung der Hash-Funktion, um den Lizenzschlüssel zu erzeugen, so häufig wie erforderlich wiederholt werden kann, ohne die Notwendigkeit, die Version zu übertragen, wie dies der Fall bei einer Ausführungsform ist, bei der eine Prozedur, welche in Fig. 25 gezeigt ist, ausgeführt wird und die zur Fig. 27 anstelle zur Fig. 26 fortgesetzt wird.

[0186] Das heißt, dass bei dieser Ausführungsform lediglich der verschlüsselte quellenseitige gemeinsame Sitzungsschlüssel e durch das DVD-Wiedergabegerät **1** zum Personalcomputer **2** im Schritt S163 übertragen wird. In diesem Zeitpunkt wird der Wert der Variablen g, welcher die Version eines Lizenzschlüssels darstellt, nicht übertragen. Die Prozedur läuft dann weiter zu einem Schritt S164, in welchem der Personalcomputer **2** den verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e empfängt. Dann läuft die Prozedur weiter zu einem Schritt S165, in welchem der Personalcomputer **2** den verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e entschlüsselt, um einen senkseitigen gemeinsamen Sitzungsschüssel sk' unter Verwendung des Sitzungsschlüssels zu erzeugen, der in der EEPROM-Einheit **50** gespeichert ist, gemäß der folgenden Gleichung:

$$sk' = Dec\ (Lizenzschlüssel, e)$$

[0187] In der Zwischenzeit verschlüsselt in einem Schritt S166 das DVD-Wiedergabegerät **1** Daten, die zum Personalcomputer **2** zu übertragen sind, unter Verwendung unter anderen Schlüsseln des quellenseitigen gemeinsamen Sitzungsschlüssels sk, der im Schritt S161 erzeugt wurde, und überträgt die verschlüsselten Daten zum Computer **2**. Die Prozedur läuft dann weiter zu einem Schritt S167, in welchem der Personalcomputer **2** die verschlüsselten Daten empfängt, und dann zu einem Schritt S168, um die verschlüsselten Daten unter Verwendung unter anderen Schlüsseln des senkseitigen gemeinsamen Sitzungsschlüssels sk', der im Schritt S165 erzeugt wurde, zu entschlüsseln. Die Prozedur läuft dann weiter zu einem Schritt S169, in welchem der Personalcomputer **2** eine Beurteilung bildet, ob Daten, welche von der Entschlüsselung resultieren, die im Schritt S168 ausgeführt wurden, korrekt sind oder nicht. Beispielsweise haben die Daten, die als TS-Paket (Transportstrompaket) des MPEG-Systems empfangen werden, einen Code zur Synchronisation mit einem hexadezimalen Wert von **47** im Kopf des Pakets. In diesem Fall kann die Beurteilung, ob Daten korrekt sind oder nicht, durch Prüfen gebildet werden, ob der Synchronisationscode perfekt ist oder nicht.

[0188] Wenn die korrekt entschlüsselten Daten

nicht das Ergebnis im Schritt S168 waren, läuft die Prozedur weiter zu einem Schritt S170, in welchem der Personalcomputer **2** die Lizenzschlüssel gemäß der folgenden Gleichung aktualisiert:

Lizenzschlüssel = hash (Lizenzschlüssel)

[0189] Danach läuft die Prozedur weiter zu einem Schritt S171, in welchem der Personalcomputer **2** wiederum den verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e, der im Schritt S164 empfangen wurde, entschlüsselt, um einen neuen senkseitigen gemeinsamen Sitzungsschlüssel sk' unter Verwendung des aktualisierten Lizenzschlüssels, der im Schritt S170 erzeugt wurde, gemäß der folgenden Gleichung zu erzeugen:

sk' = Dec (Lizenzschlüssel, e)

[0190] Nachfolgend kehrt die Prozedur zurück zum Schritt S168, um wiederum die verschlüsselten Daten, welche im Schritt S167 empfangen werden, zu entschlüsseln, wobei unter anderen Schlüsseln der senkseitige gemeinsame Sitzungsschlüssel sk', der im Schritt S171 erzeugt wurde, verwendet wird. Dann läuft die Prozedur weiter zu einem Schritt S169, in welchem der Personalcomputer **2** eine Beurteilung bildet, ob Daten, welche von der Entschlüsselung resultieren, die im Schritt S168 ausgeführt wurde, korrekt sind oder nicht. Die Schritte S70, S171, S168 und S169 werden wiederholt, bis das Ergebnis der Beurteilung, welche im Schritt S169 gemacht wird, zeigt, dass korrekte entschlüsselte Daten im Schritt S168 erlangt wurden.

[0191] Auf diese Weise wird der Lizenzschlüssel aktualisiert, um korrekte verschlüsselte Daten zu erzeugen.

[0192] Wie durch die oben beschriebene Prozedur gezeigt ist, muss in der Quelle der quellenseitige gemeinsame Sitzungsschlüssel sk erzeugt werden, bevor Daten, welche zur Senke zu übertragen sind, unter Verwendung des quellenseitigen gemeinsamen Sitzungsschlüssels sk verschlüsselt werden. In der Senke dagegen muss die Entschlüsselung der verschlüsselten Daten, welche von der Quelle empfangen werden, mit der Entschlüsselung des verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssels e synchronisiert werden, der von der Quelle empfangen wird. Genauer ausgedrückt kann die Prozedur auf Seiten der Senke nicht vom Schritt S165, um den verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e zu entschlüsseln, zum Schritt S168 weitergehen, um die entschlüsselten Daten zu entschlüsseln, bis der Schritt S167, um die verschlüsselten Daten zu empfangen, abgeschlossen ist.

[0193] Zusätzlich muss die Entschlüsselung des verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssels e und eines verschlüsselten Texts, der durch die Senke ausgeführt wird, mit der Verschlüsselung eines quellenseitigen gemeinsamen Sitzungsschlüssels sk und eines Klartexts, der durch die Quelle durchgeführt wird, synchronisiert sein. Das heißt, ein Entschlüsselungsschlüssel, der durch die Komponenten erzeugt wird, welche die 1394-Schnittstelleneinheit **36** bilden, die in der optischen Magnetplattenvorrichtung **3** verwendet wird, welche in Fig. 22 gezeigt ist, vom LFSR **601** zur exklusiven logischen Summenberechnungsschaltung **608** einem Verschlüsselungsschlüssel entsprechen, der durch die Komponenten erzeugt wird, welche die 1394-Schnittstelleneinheit **26** bilden, die im DVD-Wiedergabegerät **1** verwendet wird, welches in Fig. 21 gezeigt ist, vom LFSR **501** zur exklusiven logischen Summenberechnungsschaltung **508**, und die verschlüsselten Daten, die unter Verwendung des Entschlüsselungsschlüssels entschlüsselt werden, müssen Daten sein, die von der Verschlüsselung eines Klartexts resultieren, wobei der Verschlüsselungsschlüssel verwendet wird. Wie oben beschrieben muss somit der Verschlüsselungsschlüssel durch die 1394-Schnittstelleneinheit **26**, die in Fig. 21 gezeigt ist, in Synchronisation mit (d.h. vor) der Verschlüsselung des zugeführten Klartexts erzeugt werden, und der Entschlüsselungsschlüssel muss daher durch die 1394-Schnittstelleneinheit **36**, die in Fig. 22 gezeigt ist, synchron mit (d.h. vorher) der Entschlüsselung des empfangenen Verschlüsselungstexts erzeugt werden, obwohl die Synchronisation in Fig. 21 und Fig. 22 nicht expliziert dargestellt ist.

[0194] Wenn folglich ein Bit aus irgendeinem Grund von einem Paket fehlt, welches eines verschlüsselten Text bildet, der von einer Quelle zu einer Senke über den 1394-Seriell-Bus **11** übertragen wird, kann eine Phase, die eine zeitliche Beziehung zwischen einem Klartext und einem Verschlüsselungsschlüssel in der Quelle zeigt, nicht als Phase aufrechterhalten werden, die eine zeitliche Beziehung zwischen einem verschlüsseltem Text und einem Entschlüsselungsschlüssel in der Senke darstellt. Dieses Problem kann jedoch durch Aktualisieren oder Neu-Initialisieren der Phase gelöst werden, welche eine zeitliche Beziehung zwischen einem verschlüsselten Text und einem Entschlüsselungsschlüssel in der Senke periodisch zeigt. Fig. 28 ist ein Diagramm, welches einen typischen Aufbau einer Ausführungsform zeigt, bei dem ein Quellen-/Senken-System zum Aktualisieren oder Neu-Initialisieren der Phase ausgeführt wird, welche eine zeitliche Beziehung zwischen einem verschlüsselten Text und einem Entschlüsselungsschlüssel in der Senke periodisch zeigt.

[0195] Wie in der Figur gezeigt ist, berechnet in der Quelle eine exklusive logische Summenberechnungsschaltung **901** eine exklusive logische Summe Ci einer Zufallszahl, welche durch einen Zufallszahl-

generator **903** erzeugt wird, und einen zugeführten Klartext und gibt die exklusive logische Summe Ci an eine exklusive logische Summenberechnungsschaltung **904** und eine Verarbeitungsschaltung **902** aus, die ebenfalls den Anfangswertschlüssel Ss eines Sitzungsschlüssels S empfängt. Die Verarbeitungsschaltung **902** führt eine vorher festgelegte Verarbeitung in Bezug auf den Anfangswertschlüssel Ss des Sitzungsschlüssels S und der exklusiven logischen Summe Ci durch, die durch die exklusive logische Summenberechnungsschaltung **901** ausgegeben wird, wobei ein Ergebnis Vi der Verarbeitung an den Zufallszahlgenerator **903** als Anfangswert ausgegeben wird.

[0196] Die exklusive logische Summenberechnungsschaltung **904** berechnet die exklusive logische Summe der exklusiven logischen Summe Ci, welche durch die exklusive logische Summenberechnungsschaltung **901** und einen zeitvariablen Schlüssel i erzeugt wird, um einen verschlüsselten Text zu erzeugen, der über den 1394-Seriell-Bus **11** zur Senke übertragen wird.

[0197] Die Senke führt den Betrieb in der umgekehrten Reihenfolge gegenüber dem, der durch die Quelle durchgeführt wird, aus. Genauer ausgedrückt berechnet eine exklusive logische Summenberechnungsschaltung **911** eine exklusive logische Summe Ci des verschlüsselten Texts, der über den 1394-Seriell-Bus **11** empfangen wurde, und den zeitvariablen Schlüssel i, wobei die exklusive logische Summe Ci an eine exklusive logische Summenberechnungsschaltung **912** und eine Verarbeitungsschaltung **913** ausgegeben wird, welche ebenfalls den Anfangswertschlüssel Ss des Sitzungsschlüssels S empfängt. Die Verarbeitungsschaltung **913** führt eine vorher festgelegte Verarbeitung in Bezug auf den Anfangswertschlüssel Ss des Sitzungsschlüssels S und die exklusive logische Summe Ci durch, welche durch die exklusive logische Summenberechnungsschaltung **911** ausgegeben wird, wobei ein Verarbeitungsergebnis Vi an einen Zufallszahlgenerator **914** ausgegeben wird. Der Zufallszahlgenerator **914** erzeugt eine Zufallszahl mit dem Verarbeitungsergebnis Vi von der Verarbeitungsschaltung **913**, der als Anfangswert verwendet wird. Die exklusive logische Summenberechnungsschaltung **912** berechnet eine endgültige exklusive logische Summe der Zufallszahl, welche durch den Zufallszahlgenerator **914** erzeugt wird, und die exklusive logische Summe Ci, welche durch die exklusive logische Summenberechnungsschaltung **911** erzeugt wird, wobei die endgültige exklusive logische Summe als Klartext ausgegeben wird.

[0198] Fig. 29 ist ein Diagramm, welches einen typischen Aufbau des Zufallszahlgenerators **903** zeigt. Wie in der Figur gezeigt ist, weist der Zufallszahlgenerator **903** Komponenten auf, von einem LFSR **931** zu einer Taktfunktionseinheit **936**. Jede der Komponenten, welche in der Figur gezeigt ist, hat eine Funktion, welche mit dem entsprechenden LFSR **501** usw., dem Addierer **504** usw. oder der Taktfunktionseinheit **506** usw. der in Fig. 21 bis Fig. 24 gezeigten Ausführungsformen identisch ist.

[0199] Es sollte angemerkt sein, dass der Zufallszahlgenerator **940** den gleichen Aufbau wie der in Fig. 29 gezeigte Zufallszahlgenerator **903** hat. Daher ist es nicht notwendig, den Aufbau des erstgenannten in einer separaten Figur zu zeigen.

[0200] Fig. 30 zeigt ein Flussdiagramm, welches Betriebsarten zeigt, welche durch jede der Verarbeitungsschaltungen **902** und **913** auf Seiten der Quelle bzw. der Senke ausgeführt werden.

[0201] Die Arbeitsweise wird unter Bezugnahme auf das in Fig. 30 gezeigte Flussdiagramm wie folgt erläutert.

[0202] Die Verarbeitungsschaltung **902** auf Seiten der Quelle hat eine Funktion f, welche durch eine Gleichung ausgedrückt wird, die unten angegeben wird, um einen Wert Vi von einem Eingangssignal Ci, das zu ihr über die exklusive logische Summeberechnungsschaltung **901** geliefert wird, und den Anfangswertschlüssel Ss eines Sitzungsschlüssels S zu berechnen.

$$Vi = f(Ss, Ci)$$

[0203] Wie in der Figur gezeigt ist, beginnt das Flussdiagramm mit einem Schritt S201, in welchem die Verarbeitungsschaltung **902** den Wert 0 als Anfangswert des Eingangssignals Ci verwendet, um einen Wert Vi = f (Ss, Ci) wie folgt zu berechnen:

$$V_0 = f(Ss, 0)$$

[0204] Der Arbeitsfluss läuft dann weiter zu einem Schritt S202, in welchem der Wert V_0, der im Schritt S201 berechnet wurde, zum Zufallszahlgenerator **903**, der in Fig. 29 gezeigt ist, geliefert wird. Im Zufallszahlgenerator **903** wird der Wert V_0, der durch die Verarbeitungsschaltung **902** ausgegeben wird, zum LFSR **931** bis **933** als Anfangswert geliefert. Unter Verwendung des gleichen Verfahrens wie die 1394-Schnittstelleneinheit **26**, welche in Fig. 21 gezeigt ist, und der anderen Ausführungsformen, welche in Fig. 22 bis Fig. 24 gezeigt sind, wird eine Zufallszahl erzeugt und durch den Addierer **935**, der im Zufallszahlgenerator **903** verwendet wird, an die exklusive logische Summenberechnungsschaltung **901** ausgegeben, welche in Fig. 28 gezeigt ist. Die exklusive logische Summenberechnungsschaltung **901** berechnet eine exklusive logische Summe Ci von der Zufallszahl, welche durch den Zufallszahlgenerator **903** erzeugt wurde, und einen zugeführten Klartext,

wobei die exklusive logische Summe Ci zurück zur Verarbeitungsschaltung **902** ausgegeben wird.

[0205] In der Zwischenzeit läuft der Betriebsfluss, der in Fig. 30 gezeigt ist, weiter zu einem Schritt S203, in welchem die Verarbeitungsschaltung **902** eine Variable i auf **1** setzt. Der Betriebsfluss läuft dann weiter zu einem Schritt S204, in welchem die exklusive logische Summe Ci, welche von der exklusiven logischen Summenberechnungsschaltung **901** empfangen wird, in einer Variablen C gespeichert wird.

[0206] Danach läuft der Betriebsfluss weiter zu einem Schritt S205, in welchem die Verarbeitungsschaltung **902** Verarbeitung gemäß der folgenden Gleichung ausführt:

$$Vi = f(Ss, Ci) + V_{i-1}$$

wobei Ci der Inhalt der Variablen C ist.

[0207] Da der Wert der Variablen i gleich 1 im aktuellen Zeitpunkt ist, kann die obige Gleichung wie folgt umgeschrieben werden:

$$V1 = f(SS, C_1) + V_0$$

wobei V_0 ein Wert ist, der im Schritt S201 berechnet wurde.

[0208] Anschließend läuft die Betriebsprozedur weiter zu einem Schritt S206, in welchem die Verarbeitungsschaltung **902** eine Beurteilung bildet, ob der Inhalt der Variablen C, d.h., in diesem Fall C_1, gleich einem vorher festgelegten Wert T ist, der vorher festgelegt ist, oder nicht. In der Zwischenzeit gibt die exklusive logische Summenberechnungsschaltung **901** eine andere exklusive logische Summe Ci an die Verarbeitungsschaltung **902** aus. Wenn herausgefunden wird, dass die exklusive logische Summe Ci ungleich dem Wert T im Schritt S206 wird, läuft der Verarbeitungsfluss weiter zu einem Schritt S207, in welchem der Inhalt der Variablen i um 1 inkrementiert wird, bevor zu einem Schritt S204 zurückgekehrt wird, in welchem die andere exklusive logische Summe Ci, welche von der exklusiven logischen Summenberechnungsschaltung **901** empfangen wird, d.h., C_2, da i = 2, in der Variablen C gespeichert wird.

[0209] Dann läuft der Betriebsfluss weiter zum Schritt S205, in welchem die Verarbeitungsschaltung **902** eine Verarbeitung gemäß der folgenden Gleichung ausführt:

$$V_2 = f(Ss, C_2) + V_1$$

wobei V1 ein Wert ist, der im Schritt S205 in der unmittelbar vorherigen Iteration berechnet wurde.

[0210] Nachfolgend läuft die Betriebsprozedur weiter zum Schritt S206, in dem die Verarbeitungsschaltung **902** eine Beurteilung bildet, ob die zugeführte exklusive logische Summe Ci, d.h., in diesem Fall C_2, gleich dem vorher festgelegten Wert T ist oder nicht. Wenn herausgefunden wird, dass die zugeführte exklusive logische Summe Ci ungleich dem Wert T ist, läuft der Betriebsfluss weiter zum Schritt S207, in welchem der Inhalt der Variablen i um 1 inkrementiert wird, bevor zum Schritt S204 zurückgekehrt wird. Auf diese Weise werden die Schritte S204 bis S207 wiederholt ausgeführt, bis die zugeführte exklusive logische Summe Ci gleich dem Wert T wird.

[0211] Wenn gefunden wird, dass die zugeführte exklusive logische Summe Ci gleich dem Wert T im Schritt S206 wird, läuft dagegen der Betriebsfluss weiter zum Schritt S208, bei dem der Wert Vi (d.h., in diesem Fall V_1), der im Schritt S205 berechnet wurde, an den Zufallszahlgenerator **903** als Wert V_0 ausgegeben wird, der im Schritt S201 berechnet wurde, der an den Zufallszahlgenerator **903** im Schritt S202 ausgegeben wurde. Im Zufallszahlgenerator **903** wird der Wert V1, der durch die Verarbeitungsschaltung **902** ausgegeben wird, zum LFSR **931** bis **933** als Anfangswert geliefert. Eine Zufallszahl für den Anfangswert wird erzeugt und durch den Addierer **935**, der im Zufallszahlgenerator **903** verwendet wird, an die exklusive logische Summenberechnungsschaltung **901**, welche in Fig. 28 gezeigt ist, ausgegeben. Die exklusive logische Summenberechnungsschaltung **901** berechnet eine exklusive logische Summe Ci von der Zufallszahl, welche durch den Zufallszahlgenerator **903** erzeugt wurde, und einen zugeführten Klartext, wobei die exklusive logische Summe Ci zurück an die Verarbeitungsschaltung **902** ausgegeben wird.

[0212] In der Zwischenzeit kehrt nach der Verarbeitungsschaltung, nachdem die Verarbeitungsschaltung **902** den Wert Vi im Schritt S208 an den Zufallszahlgenerator **903** ausgibt, der Betriebsfluss, der in Fig. 30 gezeigt ist, zurück zum Schritt S203, in welchem die Verarbeitungsschaltung **902** die Variable i auf **1** zurücksetzt. Danach werden die Schritte S203 bis S208 wiederholt ausgeführt.

[0213] Es sei angenommen, dass der Wert T eine Breite von 8 Bits hat und die Erzeugungswahrscheinlichkeit des Werts von Ci gleichbleibend ist. In diesem Fall beträgt die Wahrscheinlichkeit, dass der Ci-Wert gleich T ist, 1/256, wobei 256 die achte Potenz von 2 ist. Das heißt, dass die Erzeugung der exklusiven logischen Summe Ci, die einen Wert gleich T hat, mit einer Rate von einmal pro 256 sequentiellen Operationen auftritt, welche durch die exklusive logische Summenberechnungsschaltung **901** ausgeführt werden, um die exklusive logische Summe Ci zu erzeugen. Als Ergebnis wird der Anfangswert, der im Zufallszahlgenerator **903** verwendet wird, um eine Zufallszahl zu erzeugen, mit einer Rate von einmal pro

256 sequentiellen Operationen aktualisiert, welche durch die exklusive logische Summenberechnungsschaltung **901** ausgeführt werden, um die exklusive logische Summe Ci zu erzeugen.

[0214] Die exklusive logische Summe Ci, welche durch die exklusive logische Summenberechnungsschaltung **901** ausgegeben wird, wird außerdem zur exklusiven logischen Summenberechnungsschaltung **904** geliefert, um die exklusive logische Summe der exklusiven logischen Summe Ci und den zeitvariablen Schlüssel i zu berechnen. Die exklusive logische Summe, welche durch die exklusive logische Summenberechnungsschaltung **904** berechnet wird, wird an die 1394-Schnittstellenbus **11** als verschlüsselter Text ausgegeben.

[0215] In der Senke berechnet die exklusive logische Summenberechnungsschaltung **911** eine exklusive logische Summe Ci des verschlüsselten Texts, der über den 1394-Seriell-Bus **11** von der Quelle empfangen wird, und den zeitvariablen Schlüssel i, wobei die exklusive logische Summe Ci an die exklusive logische Summenberechnungsschaltung **912** und die Verarbeitungsschaltung **913** ausgegeben wird, die ebenfalls einen Anfangswertschlüssel Ss des Sitzungsschlüssels S empfängt. Wie die Verarbeitungsschaltung **902** auf der Seiten der Quelle führt die Verarbeitungsschaltung **913** die vorher festgelegte Verarbeitung in Bezug auf den Anfangswertschlüssel Ss des Sitzungsschlüssels S und der exklusiven logischen Summe Ci aus, die durch die exklusive logische Summenberechnungsschaltung **911** ausgegeben wird, wobei ein Verarbeitungsergebnis Vi an den Zufallszahlgenerator **914** mit einer Rate von einmal pro 256 sequentiellen Operationen ausgegeben wird, um die exklusive logische Summe Ci zu erzeugen. Der Zufallszahlgenerator **914** erzeugt eine Zufallszahl mit dem Verarbeitungsergebnis Vi, welches als Anfangswert verwendet wird. Die exklusive logische Summenberechnungsschaltung **912** berechnet eine endgültige exklusive logische Summe von der Zufallszahl, welche durch den Zufallszahlgenerator **914** erzeugt wird, und der exklusiven logischen Summe Ci, welche durch die exklusive logische Summenberechnungsschaltung **911** erzeugt wird, und gibt die endgültige exklusive logische Summe als Klartext aus.

[0216] Wie oben beschrieben gibt die Verarbeitungsschaltung **913** das Verarbeitungsergebnis Vi an den Zufallszahlgenerator **914** mit einer Rate von einmal pro 256 sequentiellen Operationen aus, die durch die exklusive logische Summenberechnungsschaltung **911** ausgeführt werden, um die exklusive logische Summe Ci zu erzeugen. Als Ergebnis kann eine Phase, welche eine zeitliche Beziehung zwischen einem verschlüsselten Text, der von einer Quelle zur einer Senke über den 1394-Seriell-Bus **11** übertragen wird, und einer Zufallszahl, die als Entschlüsselungsschlüssel in der Senke verwendet wird, in dem Fall wiederentwickelt werden, wenn ein Bit aus irgendwelchen Gründen von einem Paket fehlt, welches den verschlüsselten Text in dem Zeitpunkt bildet, wo die Verarbeitungsschaltung **913** das Verarbeitungsergebnis Vi an den Zufallszahlgenerator **914** mit einer Rate von einmal pro 256 sequentiellen Operationen ausgibt, um die exklusive logische Summe Ci zu erzeugen.

[0217] Es sollte angemerkt sein, dass, da die Verarbeitungsschaltung **902** oder **913** das Verarbeitungsergebnis Vi an den Zufallszahlgenerator **914** ausgibt, wenn die exklusive logische Summe Ci gleich dem Wert T wird (Ci = T), die Verarbeitungsschaltung **913** das Verarbeitungsergebnis Vi an den Zufallszahlgenerator **914** nicht periodisch ausgibt. Anstelle davon kann nichts weiter hinzugefügt werden, als die Tatsache, dass die Verarbeitungsschaltung **913** das Verarbeitungsergebnis Vi an den Zufallszahlgenerator **914** mit einer Wahrscheinlichkeit von einmal pro 256 sequentiellen Operationen ausgibt, um durchschnittlich die exklusive logische Summe Ci zu erzeugen.

[0218] Es ist erwähnenswert, dass die Rate, mit der die Verarbeitungsschaltungen **902** und **913** das Verarbeitungsergebnis Vi an die Zufallszahlgeneratoren **903** und **914** ausgeben, auch auf der Anzahl von Abschnitten verschlüsselter Daten basieren kann, welche durch die Quelle übertragen und durch die Senke empfangen werden. Wenn ein Datenabschnitt im Laufe der Übertragung über den 1394-Seriell-Bus **11** fehlt, wird jedoch dieses Verfahren die Schwierigkeit haben, dass der Datenabschnitt, der auf Seiten der Quelle gezählt wird, gegenüber dem Datenabschnitt verschieden ist, der auf Seiten der Senke gezählt wird, wodurch es nicht länger möglich ist, Synchronisation zwischen der Quelle und der Senke einzurichten. Es ist somit wünschenswert, das Synchronisationsverfahren anzunehmen, welches durch die oben beschriebene Ausführungsform ausgeführt wird.

[0219] Als Anfangswert, der im Zufallszahlgenerator **903** Oder **914** verwendet wird, kann die exklusive logische Summe Ci, welche durch die exklusive logische Summenberechnungsschaltung **901** oder **911** ausgegeben wird, zum Zufallszahlgenerator **903** oder **914** entsprechend geliefert werden, und zwar unverändert. In diesem Fall besteht jedoch, da über den 1394-Seriell-Bus **11** übertragen, die Gefahr, dass die exklusive logische Summe Ci gestohlen ist. Das heißt, warum die exklusive logische Summe Ci nicht unmittelbar als Anfangswert verwendet wird. Anstelle davon kann unter Verwendung eines Werts Vi, der von vorher festgelegter Verarbeitung resultiert, welche in Bezug auf die exklusive logische Summe Ci als Anfangswert ausgeführt wird, die Datensicherheit weiter verbessert werden.

[0220] Im übrigen gibt es zwei Verfahren zum Über-

tragen von Daten über den 1394-Seriell-Bus **11**. Eines von diesen ist ein asynchrones Übertragungsverfahren, während das andere ein isochrones Übertragungsverfahren ist. Bei dem asynchronen Übertragungsverfahren werden Daten zwischen zwei Vorrichtungen übertragen. Bei isochronen Übertragungsverfahren werden die Daten dagegen von einer Vorrichtung zu allen anderen, die mit dem 1394-Seriell-Bus verbunden sind, gesendet. Damit werden die Kommunikationen zur Bestätigung von Senken und Schlüsselaufteilungsprotokollen der in Fig. 4 gezeigten Ausübungsformen und den anderen Figuren normalerweise durch Annehmen des asynchronen Übertragungsverfahrens erreicht, da keine Notwendigkeit besteht, Information von der Quelle zu allen Senken zu senden.

[0221] Bei der Bestätigung und dem Schlüsselaufteilungsprotokoll der in Fig. 4 gezeigten Ausführungsform ist der Personalcomputer **2** in der Lage, einen verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e vom DVD-Wiedergabegerät zu erlangen, sogar, wenn der Personalcomputer **2** ein nicht bestätigtes Gerät ist, welches keinen korrekte Lizenzschlüssel hat. Wie oben beschrieben ist der quellenseitige verschlüsselte Sitzungsschlüssel e ein verschlüsselter Text, der von der Verschlüsselung eines quellenseitigen gemeinsamen Sitzungsschlüssels sk resultiert, wobei der Lizenzschlüssel lk verwendet wird. Da der Personalcomputer **2** eine nicht berechtigte Vorrichtung ist, die keinen korrekten Lizenzschlüssel hat, ist der Personalcomputer **2** nicht in der Lage, den korrekten senkseitigen gemeinsamen Sitzungsschlüssel sk' durch Entschlüsseln des verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssels e zu erlangen. Es besteht somit die große Gefahr trotzdem, dass der verschlüsselte quellenseitige gemeinsame Sitzungsschlüssel e unmittelbar bei der Entschlüsselung der verschlüsselten Information verwendet werden kann, und zwar unverändert.

[0222] Wenn der Personalcomputer **2** außerdem den quellenseitigen gemeinsamen Sitzungsschlüssel sk (einen Klartext) zusätzlich zum verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e empfängt (einen verschlüsselten Text, der aus Verschlüsselung des quellenseitigen gemeinsamen Sitzungsschlüssels sk unter Verwendung des Lizenzschlüssel lk resultiert), werden aus einigen Gründen sowohl der Klartext als auch die entsprechenden verschlüsselten Texte erlangt. In diesem Fall besteht die große Gefahr, dass der Klartext und der verschlüsselte Text zum Herausfinden des Lizenzschlüssels verwendet werden, den der Personalcomputer **2** nicht hat. Es sollte angemerkt sein, dass allgemein, um so mehr Paare von Klartexten und verschlüsselten Texten durch einen Angreifer bekannt sind, desto leichter das Umkehrverfahren, welches durch den Angreifer angenommen wird, um den Lizenzschlüssel zu kennen, der verwendet wird, die verschlüsselten Texte von den Klartexten zu erzeugen, angewandt werden kann.

[0223] Außerdem kann ein nicht berechtigter Personalcomputer **2** eine falsche ID zum DVD-Wiedergabegerät **1** übertragen, welches die falsche ID zum Berechnen des Lizenzschlüssels lk verwendet. Der Lizenzschlüssel lk wird wiederum zum Verschlüsseln des quellenseitigen gemeinsamen Sitzungsschlüssel sk verwendet, um den verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e zu erzeugen, der dann zum Personalcomputer **2** übertragen wird. Es sei angenommen, dass der Personalcomputer **2** eine Anforderung nach der Übertragung eines verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssels e während einer Sitzung durch Übertragen einer ID machen darf. Wenn eine derartige Anforderung mehrere Male getätigt wird, werden mehrere Lizenzschlüssel durch das DVD-Wiedergabegerät **1** von unterschiedlichen IDs erzeugt, welche vom Personalcomputer **2** empfangen werden. Als Ergebnis werden mehrere verschlüsselte quellenseitige gemeinsame Sitzungsschlüssel e, die von der Verschlüsselung des quellenseitigen gemeinsamen Sitzungsschlüssels sk für die Sitzung resultieren, durch den Personalcomputer **2** empfangen. Das heißt, wenn der Personalcomputer **2** den quellenseitigen gemeinsamen Sitzungsschlüssel sk erlangt, ist der Personalcomputer **2** in der Lage, mehrere Paare zu kennen, die jeweils den quellenseitigen gemeinsamen Sitzungsschlüssel sk und einen von den verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüsseln e aufweisen.

[0224] Eine Ausführungsform, bei der eine Bestätigungsprozedur ausgeführt wird, welche in Fig. 31 gezeigt ist, richtet sich auf das oben beschriebene Problem. Die Prozedur verhindert, dass eine nicht berechtigte Senke mehrere verschlüsselte quellenseitige gemeinsame Sitzungsschlüssel e empfängt, die von einer Verschlüsselung eines quellenseitigen gemeinsamen Sitzungsschlüssels sk resultieren, wobei unterschiedliche Lizenzschlüssel lk verwendet werden. Die in der Figur gezeigte Prozedur ist grundsätzlich die gleiche wie die, welche in Fig. 4 gezeigt ist, mit der Ausnahme, dass vor einer Anforderung nach einer ID, welche durch die Quelle an die Senke gemacht wird, einige Verarbeitungsabschnitte ausgeführt werden.

[0225] Ausführlicher ausgedrückt überträgt, wie in der Prozedur der Figur gezeigt ist, in einem Schritt S201 der Personalcomputer **2**, der als Senke dient, eine Anforderung nach Bestätigung, d.h., eine Anforderung für den Start eines Bestätigungsprotokolls, an das DVD-Wiedergabegerät **1**, welches als Quelle dient. Diese Anforderung nach Bestätigung wird unter Verwendung des asynchronen Übertragungsverfahrens wie dies der Fall bei den anderen Übertra-

gungen im Protokoll verwendet.

[0226] Vorrichtungen, welche mit dem IEEE-1394-Seriell-Bus **11** verbunden sind, haben jeweils eine spezielle Knotennummer, die in Bezug in einer Busrücksetzzeit zugeordnet sind. Die Knotennummer wird verwendet, eine Information, welche die Vorrichtung überträgt oder empfängt, anzugeben und zu identifizieren.

[0227] Fig. 32 ist ein Diagramm, welches das Format einer Schreibanforderung für ein Daten-Vierer-Paket zeigt, eines von asynchronen Paketen. Das Bestimmungs-ID-Feld des Formats ist die Knotennummer eines Informationsempfangsgeräts, und die Quellen-ID-Feld des Formats ist die Knotennummer einer Informationsübertragungsvorrichtung. Bei einem Paket, welches eine Anforderung nach Bestätigung liefert, sind Daten, welche zeigen, das das Paket eine Anforderung nach Bestätigung zeigt, im Vierer-Datenfeld enthalten.

[0228] Wenn das asynchrone Paket, welches eine Anforderung nach Bestätigung liefert, in einem Schritt S202 empfangen wird, holt das DVD-Wiedergabegerät **1** die Quellen-ID, d.h., die Knoten-ID einer Informationsübertragungsvorrichtung, welche das Paket überträgt. Die Prozedur läuft dann weiter zu einem Schritt S203, bei dem das DVD-Wiedergabegerät **1** eine Beurteilung bildet, ob ein verschlüsselter quellenseitiger gemeinsamer Sitzungsschlüssel e, der aus einer Verschlüsselung des quellenseitigen gemeinsamen Sitzungsschlüssels sk resultiert, für die vorliegende Sitzung zur Informationsempfangsvorrichtung, welche durch die Knotennummer identifiziert wird, übertragen wurde oder nicht. Wenn das Ergebnis der Beurteilung, die im Schritt S203 gebildet wird, zeigt, dass ein verschlüsselter quellenseitiger gemeinsamer Sitzungsschlüssel e, der von der Verschlüsselung des quellenseitigen gemeinsamen Sitzungsschlüssels sk für die vorliegende Sitzung resultieren, zur Informationsempfangsvorrichtung, welche durch die Knotennummer identifiziert wird, übertragen wurde, wird die Verarbeitung des Bestätigungsprotokolls für den Personalcomputer **2** beendet. Wenn das Ergebnis der Beurteilung, welche im Schritt S203 gebildet wird, zeigt, dass ein verschlüsselter quellenseitiger gemeinsamer Sitzungsschlüssel e, der aus einer Verschlüsselung des quellenseitigen gemeinsamen Sitzungsschlüssels sk für die vorliegende Sitzung resultiert, nicht zur Informationsempfangsvorrichtung, welche durch die Knotennummer identifiziert wird, übertragen wurde, läuft dagegen die Prozedur weiter zu einem Schritt S204, um die Ausführung des Bestätigungsprotokolls zu beginnen.

[0229] Abschnitte der Verarbeitung, welche in den Schritten S204 bis 213 der in Fig. 31 gezeigten Prozedur ausgeführt werden, sind die gleichen wie die der Schritte S1 bis S10 der in Fig. 4 gezeigten Prozedur.

[0230] Wenn die obigen Abschnitte der Verarbeitung ausgeführt sind, zeichnet in einem Schritt S214 das DVD-Wiedergabegerät **1** die Knotennummer des Personalcomputers **2**, die im Schritt S213 geholt wurde, in der EEPROM-Einheit **27** auf. Die Knotennummer wird hier solange gehalten, wie das DVD-Wiedergabegerät **1** den quellenseitigen gemeinsamen Sitzungsschlüssel sk der aktuellen Sitzung verwendet. Da ein weiterer Quellensitzungsschlüssel sk für eine nächste Sitzung erzeugt wird, wird die Knotennummer aus der EEPROM-Einheit **27** gelöscht.

[0231] Mit dem oben beschriebenen Protokoll wird lediglich ein verschlüsselter quellenseitiger gemeinsamer Sitzungsschlüssel e zu einer Senke übertragen. Als Ergebnis kann die Sicherheit der übertragenen Information verbessert werden.

[0232] Übrigens wird im Schritt S7 des in Fig. 4 gezeigten Bestätigungsprotokolls ein quellenseitiger gemeinsamer Sitzungsschlüssel sk durch eine Quelle unter Verwendung eines Lizenzschlüssels lk verschlüsselt, um einen verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e zu erzeugen, der dann zur Senke übertragen wird. Als Verschlüsselungsalgorithmus wird breit eine Blockverschlüsselung verwendet. In der Blockverschlüsselung wird ein Klartext zu festen Längenblockeinheiten verschlüsselt. Eine DES-Verschlüsselung ist eine allgemeine bekannte Blockverschlüsselung. Die DES-Verschlüsselung ist ein Verschlüsselungsalgorithmus, um jeden 64-Bit-Block eines Klartexts in einen 64-Bit-Verschlüsselungstext zu transformieren.

[0233] Es sei angenommen, dass eine n-Bit-Blockverschlüsselung ein Verschlüsselungsalgorithmus ist, welcher im Schritt S7 der in Fig. 4 gezeigten Prozedur verwendet wird, um einen n-Bit-Klartext in einen n-Bit-Verschlüsselungstext zu transformieren und die Anzahl von Bits im quellenseitigen gemeinsamen Sitzungsschlüssel sk n beträgt. Außerdem sei angenommen, dass ein n-Bit-Resultat, welches von der Anwendung des Verschlüsselungsalgorithmus auf den n-bit-quellenseitigen gemeinsamen Sitzungsschlüssel sk erlangt wird, und der Lizenzschlüssel lk unverändert als verschlüsselter quellenseitiger gemeinsamer Sitzungsschlüssel sk e verwendet wird.

[0234] Es sei angenommen, dass die Quelle versucht, einen anderen verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e zu einer Senke nach einem vorherigen verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e in der gleichen Sitzung zu übertragen. Außerdem sei angenommen, dass der vorherige verschlüsselte quellenseitige gemeinsame Sitzungsschlüssel e durch eine

nicht berechtigte Person gestohlen wurde. Da die Transaktion in der gleichen Sitzung ausgeführt wird, bleibt der quellenseitige gemeinsame Sitzungsschlüssel sk unverändert. Da außerdem der gleiche Verschlüsselungsalgorithmus angenommen wird, um den anderen verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e vom quellenseitigen gemeinsamen Sitzungsschlüssel sk zu erzeugen, und der gleiche Lizenzschlüssel lk im Algorithmus verwendet wird, ist der andere verschlüsselte quellenseitige gemeinsame Sitzungsschlüssel e der gleiche wie der obige verschlüsselte quellenseitige gemeinsame Sitzungsschlüssel e. Es liegt innerhalb der Grenzen der Möglichkeit, dass der andere verschlüsselte quellenseitige gemeinsame Sitzungsschlüssel e ebenfalls durch eine nicht berechtigte Person gestohlen ist. Wenn der andere verschlüsselte quellenseitige gemeinsame Sitzungsschlüssel e ebenfalls durch die nicht berechtigte Persona aufgrund irgendeiner Gelegenheit gestohlen ist, wird die Person erkennen, dass der gleiche quellenseitige gemeinsame Sitzungsschlüssel sk noch verwendet wird, was ein Problem verursacht.

[0235] Eine Ausführungsform, bei der die Bestätigungsprozedur, welche in Fig. 33 gezeigt ist, ausgeführt wird, richtet sich auf das oben beschriebene Problem. Da Abschnitte der Verarbeitung, welche in den Schritten S221 bis S226 der in der Figur gezeigten Prozedur die gleichen sind wie die der Schritte S1 bis S6 der in Fig. 4 gezeigten Prozedur, wird eine Erläuterung dazu nicht wiederholt.

[0236] In einem Schritt S227 erzeugt die Quelle eine n-Bit-Zufallszahl r. Die Prozedur läuft dann weiter zu einem Schritt S228, in welchem eine Verkettung der Zufallszahl r mit dem quellenseitigen gemeinsamen Sitzungsschlüssel sk unter Verwendung des Lizenzschlüssel lk wie folgt verschlüsselt wird:

e = Enc (lk, r || sk)

[0237] Die Verschlüsselung wird in einem Verschlüsselungsmodus, der als CBC-Modus bezeichnet wird, ausgeführt. Fig. 34 ist ein Diagramm, welches den Aufbau eines Systems zeigt, bei dem der CBC-Modus ausgeführt wird. Die linke Seitenhälfte und die rechte Seitenhälfte der Figur zeigen die Verschlüsselung bzw. die Entschlüsselung. Die gleichen Anfangswerte IV werden in Registern **1003** und **1012** gespeichert. Der Anfangswert IV ist durchwegs durch das Gesamtsystem fest.

[0238] Bei der Verschlüsselungsverarbeitung berechnet zunächst eine exklusive logische Summenverarbeitungsschaltung **1001** eine exklusive logische Summe eines ersten n-Bit-Blocks eines Klartexts und den Anfangswerts IV, der im Register **1003** gespeichert ist. Der exklusive logische Wert wird zu einem Verschlüsseler **1002** geliefert. Ein verschlüsselter n-Bit-Text, der durch den Verschlüsseler **1002** erzeugt wird, wird an eine Kommunikationsleitung als erster Block ausgegeben und zum Register **1003** zurückgeführt.

[0239] Wenn der zweite n-Bit-Block des Klartexts geliefert wird, berechnet die exklusive logische Summenverarbeitungsschaltung **1001** eine exklusive logische Summe des zweiten n-Bit-Blocks des Klartexts und des ersten Blocks des verschlüsselten Texts, der im Register **1003** gespeichert ist. Der exklusive logische Wert wird zum Verschlüsseler **1002** geliefert, wo er verschlüsselt wird. Ein verschlüsselter n-Bit-Text, der durch den Verschlüsseler **1002** erzeugt wird, wird an die Kommunikationsleitung als zweiter Block ausgegeben und zum Register **1003** zurückgeführt. Die oben beschriebenen Operationen werden wiederholt ausgeführt.

[0240] Auf der Entschlüsselungsseite dagegen wird der erste Block des verschlüsselten Texts, der über die Kommunikationsleitung übertragen wird, durch einen Entschlüsseler **1011** entschlüsselt. Eine exklusive logische Summenverarbeitungsschaltung **1013** berechnet eine exklusive logische Summe des Ausgangssignals des Entschlüsselers **1011** und den Anfangswert IV, der im Register **1012** gespeichert ist, um den ersten Block des Klartexts zu erzeugen.

[0241] Der erste Block des verschlüsselten Texts, der über die Kommunikationsleitung empfangen wird, wird ebenfalls im Register **1012** gespeichert. Danach wird der zweite Block des verschlüsselten Textes, der über die Kommunikationsleitung übertragen wird, empfangen und durch den Entschlüsseler **1011** entschlüsselt. Die exklusive logische Summenverarbeitungsschaltung **1013** berechnet eine exklusive logische Summe des zweiten Blocks des Entschlüsselungsergebnisses, welches durch den Entschlüsseler **1011** ausgegeben wird, und des ersten Blocks des verschlüsselten Texts, der im Register **1012** gespeichert ist, um den zweiten Block des Klartextes zu erzeugen.

[0242] Der zweite Block des verschlüsselten Textes, der über die Kommunikationsleitung empfangen wird, wird ebenfalls im Register **1012** gespeichert.

[0243] Die oben beschriebenen Operationen werden wiederholt ausgeführt, um Entschlüsselungsverarbeitung zu erreichen.

[0244] Es sollte angemerkt sein, dass der CBC-Modus ausführlich in der zweiten Ausgabe der Referenz mit dem Titel "Applied Cryptography" des Verfasser Bruce Schneider beschrieben ist.

[0245] Es wird nun wiederum die Prozedur, die in Fig. 33 gezeigt ist, betrachtet. Im Schritt S228 wird die n-Bit-Zufallszahl r und der quellenseitige gemein-

same Sitzungsschlüssel sk beim Verschlüsselungsalgorithmus als ersten und zweiten Blocks des Klartextes verwendet. Das heißt, dass die exklusive logische Summenverarbeitungsschaltung **1001** eine exklusive logische Summe der Zufallszahl r berechnet, d.h., den ersten n-Bit-Block des Klartextes, und den Anfangswert IV, der im Register **1003** gespeichert ist. Der exklusive logische Wert wird zum Verschlüsseler **1002** geliefert, wo er unter Verwendung des Lizenzschlüssels lk verschlüsselt wird. Damit erzeugt der Verschlüsseler **1002** Enc (lk, r (+) IV).

[0246] Das Ausgangssignal des Veschlüsselers **1002** wird im Register **1003** gespeichert. Wenn der quellenseitige gemeinsame Sitzungsschlüssel sk empfangen wird, d.h., der zweite Block des Klartexts eine exklusive logische Summe des zweiten Blocks des Klartextes empfangen wird, berechnet die exklusive logische Summenverarbeitungsschaltung **1001** eine exklusive logische Summe des zweiten Blocks des Klartexts und gibt das Ausgangssignal des Verschlüsselers, welches im Register **1003** gespeichert ist, aus. Als Ergebnis erzeugt der Verschlüsseler **1002** Enc (lk, sk (+) Enc (lk, r (+) IV)).

[0247] In einem Schritt S229 verkettet die Quelle die beiden Blöcke miteinander, um e zu erzeugen, welches zur Senke übertragen wird, gemäß der folgenden Gleichung:

E = Enc (lk, r (+) IV) || Enc (lk, sk (+) Enc (lk, r (+) IV))

[0248] Auf Seiten der Senke wird das Ausgangssignal e des Verschlüsselers **1002** in einem Schritt S230 empfangen. Die Prozedur läuft dann weiter zu einem Schritt S231, bei dem der verschlüsselte quellenseitige gemeinsame Sitzungsschlüssel e unter Verwendung des Lizenzschlüssels entschlüsselt wird, der in der EEPROM-Einheit **50** gespeichert ist. Ein Ergebnis der Entschlüsselung umfasst einen ersten Block r' und einen zweiten Block sk', den senkseitigen gemeinsamen Sitzungsschlüssel.

[0249] Bei der oben beschriebenen Verschlüsselung und Entschlüsselung werden lediglich die Verwendung des korrekten Lizenzschlüssels durch die Senke sich ergeben: sk = sk'. Als Ergebnis wird zugelassen, dass die Quelle und die Senke sich einen gemeinsamen einen gemeinsamen Sitzungsschlüssel anteilig teilen.

[0250] Die Gleichung des verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssels e, die oben angegeben ist, bedeutet, dass jedes Mal, wenn der quellenseitige gemeinsame Sitzungsschlüssel sk verschlüsselt wird, ein anderer verschlüsselter quellenseitiger gemeinsamer Sitzungsschlüssel e die Folge ist, sogar, wenn der Wert des Sitzungsschlüssels sk unverändert bleibt. Der Grund dafür liegt darin, dass die Zufallszahl r, die bei der Verschlüsselung beteiligt ist, sich ändert. Als Ergebnis ist es für eine Person schwierig, welche unterschiedliche Werte des verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssels sk stiehlt, zu bestimmen, ob die Werte in der gleichen Sitzung erzeugt sind oder nicht.

[0251] Es sollte angemerkt sein, dass zusätzlich zum oben beschriebenen CBC-Modus allgemein bekannte Verwendungsmoden der Blockverschlüsselung einen ECB-Modus, einen CFB-Modus und einen OFB-Modus aufweisen. Da die letzten beiden Moden jeweils eine Rückführschleife enthalten, können sie für die in Fig. 33 gezeigte Verarbeitung angewandt werden. Natürlich können irgendwelche Verschlüsselungsmoden auf die in Fig. 33 gezeigte Verarbeitung angewandt werden, solange sie eine Rückführschleife aufweisen. Verwendungsmoden der Blockverschlüsselung sind ebenfalls ausführlich in der zweiten Ausgabe der Literatur mit dem Titel "Applied Cryptography" des Autors Bruce Schneider beschrieben.

[0252] Übrigens verschlüsselt bei der Verarbeitung, welche durch die in Fig. 4 gezeigte Ausführungsform ausgeführt wird, die Quelle einen quellenseitigen gemeinsamen Sitzungsschlüssel sk und überträgt einen verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e zur Senke. Da lediglich eine bevollmächtigte Senke in der Lage ist, den verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e korrekt zu entschlüsseln, um einen senkseitigen gemeinsamen Sitzungsschlüssel sk' zu erzeugen, der den gleichen Wert wie der quellenseitige gemeinsame Sitzungsschlüssel sk hat, ist im Wesentlichen die Ausführungsform ein System, wo die Senke durch die Quelle bestätigt wird. Bei dieser Prozedur jedoch wird die Quelle selbst nicht bestätigt. Als Ergebnis, sogar, wenn eine nicht bestätigte Quelle willkürliche Daten als einen verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel zu einer Quelle überträgt, liegt es ziemlich im Bereich des Möglichen, dass die Senke ein Ergebnis der Entschlüsselung des verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssels e als einen senkseitigen gemeinsamen Sitzungsschlüssel sk' akzeptiert. Um dieses Problem zu lösen, ist eine Ausführungsform, bei der die Bestätigungsprozedur, die in Fig. 35 gezeigt ist, vorgesehen.

[0253] Wie in der Figur gezeigt ist, beginnt die Bestätigungsprozedur mit einem Schritt S241, bei dem der Personalcomputer **2**, der als Senke dient, eine Zufallszahl r erzeugt, welche eine vorher festgelegte Anzahl von Bits hat. Bei der Ausführungsform ist die Anzahl von Bits gleich 64, d.h., ein typischer Wert. Die Prozedur läuft dann weiter zu einem Schritt S242, bei dem die Zufallszahl zum DVD-Wiedergabegerät **1** übertragen wird, welches als Quelle dient. Dann läuft die Prozedur weiter zu einem Schritt S243, in welchem das DVD-Wiedergabegerät **1** die Zufallszahl r

empfängt. Anschließend läuft die Prozedur weiter zu einem Schritt S244, in welchem das DVD-Wiedergabegerät eine Anforderung nach einer ID an den Personalcomputer **2** macht. Die Prozedur läuft dann weiter zu einem Schritt S245, in welchem der Personalcomputer **2** die Anforderung empfängt. Danach läuft die Prozedur weiter zu einem Schritt S246, bei dem der Personalcomputer **2** die angeforderte ID von der EEPROM-Einheit **50** liest und die ID zum DVD-Wiedergabegerät **1** überträgt. Nachfolgend läuft die Prozedur weiter zu einem Schritt S247, in welchem das DVD-Wiedergabegerät **1** die ID empfängt.

[0254] Die Prozedur läuft dann weiter zu einem Schritt S248, in welchem das DVD-Wiedergabegerät **1** einen Lizenzschlüssel lk unter Verwendung der folgenden Gleichung erzeugt:

lk = hash (ID || Dienstschlüssel)

[0255] Danach läuft die Prozedur weiter zu einem Schritt S249, in welchem das DVD-Wiedergabegerät **1** einen quellenseitigen gemeinsamen Sitzungsschlüssel sk erzeugt.

[0256] Nachfolgend läuft die Prozedur weiter zu einem Schritt S250, bei dem das DVD-Wiedergabegerät **1** einen verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e unter Verwendung der folgenden Gleichung erzeugt:

e = Enc (lk, r || sk)

[0257] Die Prozedur läuft dann weiter zu einem Schritt S251, bei dem das DVD-Wiedergabegerät **1** den verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e zum Personalcomputer **2** überträgt.

[0258] Es sollte angemerkt sein, dass irgendein Verschlüsselungsmodus einschließlich einer Rückführschleife, beispielsweise der CBC-Modus bei der Verschlüsselung angenommen wird, welche im Schritt S20 ausgeführt wird.

[0259] Danach läuft die Prozedur weiter zu einem Schritt S252, in welchem der Personalcomputer **2** den verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e empfängt. Anschließend läuft die Prozedur weiter zu einem Schritt S253, in welchem der Personalcomputer **2** den verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e unter Verwendung des Lizenzschlüssels entschlüsselt, um r' || sk' zu erzeugen, eine Verkettung von r' mit sk'.

[0260] Die Anzahl von Bits, welche in r' enthalten sind, ist die gleiche wie die der Zufallszahl r, die im Schritt S241 erzeugt wird, die vorher bestimmt wird.

[0261] Die Prozedur läuft dann weiter zu einem Schritt S254, in welchem der Personalcomputer **2** prüft, ob gilt: r = r'. Wenn r = r', bestätigt der Personalcomputer **2** das DVD-Wiedergabegerät **1** als gültige (berechtigte) Quelle und akzeptiert den quellenseitigen gemeinsamen Sitzungsschlüssel sk' als korrekten Sitzungsschlüssel. Der Grund dafür liegt darin, dass lediglich eine Vorrichtung, die in der Lage ist, einen korrekten Lizenzschlüssel lk zu erzeugen, in der Lage ist, einen derartigen verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e zu erzeugen, wo ein Ergebnis r' der Entschlüsselung des verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssels e unter Verwendung des Lizenzschlüssels gleich der Zufallszahl r ist.

[0262] Wenn r = r' nicht gilt, bestätigt dagegen der Personalcomputer **2** das DVD-Wiedergabegerät **1** nicht als gültige Quelle, und rangiert folglich den quellenseitigen gemeinsamen Sitzungsschlüssel sk' aus.

[0263] Durch Bereitstellen einer Ausführungsform zum Ausführen einer Bestätigungsprozedur wie oben beschrieben ist die Senke in der Lage, die Quelle zu bestätigen. Zusätzlich hält außerdem die Bestätigungsprozedur das Merkmal, dass lediglich eine bestätigte Senke in der Lage ist, einen korrekten senkseitigen gemeinsamen Sitzungsschlüssel sk' zu erzeugen, wie dies der Fall bei der in Fig. 4 gezeigten Ausführungsform ist.

[0264] Fig. 36 ist ein Diagramm, welches eine weitere Ausführungsform zeigt, bei der eine Bestätigungsprozedur ausgeführt wird, wodurch die Senke in der Lage ist, die Quelle zu bestätigen. Da Abschnitte der Verarbeitung, welche in den Schritten S261 bis S266 der in der Figur gezeigten Prozedur die gleichen sind, wie die der Schritte S1 bis S6 der in Fig. 4 gezeigten Prozedur, wird eine Erläuterung dafür nicht wiederholt.

[0265] In einem Schritt S267 nimmt das DVD-Wiedergabegerät **1** Zeitinformation T auf. Ausführlicher ausgedrückt wird der Inhalt eines 32-Bit-Zykluszeitregisters, welches in den Spezifikationen durch IEEE 1394 vorgeschrieben ist, üblicherweise als Zeitinformation verwendet. Die Zykluszeitregister werden dazu verwendet, Zeitinformation von Vorrichtungen zu bilden, welche gleichbleibend mit dem IEEE 1394-Seriell-Bus **11** verbunden sind. Die Zykluszeitregister der Vorrichtungen werden gleichbleibend durch ein Paket aktualisiert, welches durch ein Zyklushauptgerät gesendet wird, eine Vorrichtung auf dem 1394-Seriell-Bus **11**. Der Inhalt jedes der Zykluszeitregister wird um 1 durch ein gemeinsames Taktsignal mit einer Frequenz von 24,576 MHz inkrementiert oder einmal für ungefähr alle **40** Nanosekunden über den 1394-Seriell-Bus **11**. Auf diese Weise werden die Zeiten der Vorrichtungen, welche mit dem 1394-Seriell-Bus **11** verbunden sind, eingestellt, da-

mit sie miteinander übereinstimmen.

[0266] Die Prozedur läuft dann weiter zu einen Schritt S268, bei dem das DVD-Wiedergabegerät **1** T || sk verschlüsselt, um einen verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e zu erzeugen. Danach läuft die Prozedur weiter zu einem Schritt S269, um den verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e zum Personalcomputer **2** zu übertragen. Es sei angemerkt, dass irgendein Verschlüsselungsmodus, der eine Rückführschleife aufweist, beispielsweise der CBC-Modus als ein Verschlüsselungsmodus angewandt wird.

[0267] Anschließend läuft die Prozedur weiter zu einem Schritt S270, in welchem der Personalcomputer **2** den verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e empfängt. Anschließend läuft die Prozedur weiter zu einem Schritt S271, bei dem der verschlüsselte quellenseitige gemeinsame Sitzungsschlüssel e unter Verwendung des Lizenzschlüssels entschlüsselt wird, um ein Ergebnis der Entschlüsselung T' || sk' zu erzeugen. Der T'-Bereich beim Ergebnis der Entschlüsselung besitzt eine Breite von 32 Bits.

[0268] Die Prozedur läuft dann weiter zu einem Schritt S272, um die Gültigkeit von T' zu prüfen, wobei T' mit dem Inhalt des Zykluszeitregisters des Personalcomputers **2** selbst verglichen wird. Wenn die Differenz kleiner ist als ein typischer vorher festgelegter Wert von beispielsweise 100 Millisekunden, wird beurteilt, dass T' gültig ist. Wenn die Differenz größer ist als der vorher festgelegte Wert, wird dagegen beurteilt, dass T' ungültig ist.

[0269] Wenn T' den Gültigkeitstest durchläuft, beurteilt der Personalcomputer **2**, dass das DVD-Wiedergabegerät **1** eine berechtigte Vorrichtung ist und akzeptiert folglich den senkseitigen gemeinsamen Sitzungsschlüssel sk'. Wenn T' nicht den Gültigkeitstest durchläuft, beurteilt dagegen der Personalcomputer **2**, dass das DVD-Wiedergabegerät **1** eine nichtberechtigte Vorrichtung ist. In diesem Fall wird der senkseitige gemeinsame Sitzungsschlüssel sk' ausrangiert. Der Grund dafür liegt darin, dass lediglich eine Vorrichtung, die in der Lage ist, einen korrekten Lizenzschlüssel lk zu erzeugen, in der Lage ist, einen derartigen verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e zu erzeugen, wo das Ergebnis T' der Entschlüsselung des verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssels e unter Verwendung des Lizenzschlüssel gleich dem Inhalt des Zykluszeitregisters ist.

[0270] Durch Bereitstellen einer Ausführungsform zum Ausführen einer Bestätigungsprozedur wie oben beschrieben ist die Senke in der Lage, die Quelle zu bestätigen. Außerdem hält die Bestätigungsprozedur ebenfalls das Merkmal, dass lediglich eine bestätigte Senke in der Lage ist, einen korrekten senkseitigen gemeinsamen Sitzungsschlüssel sk' wie in dem Fall zu erzeugen, wie bei der Ausführungsform welche in Fig. 4 gezeigt ist.

[0271] Bei der Verarbeitung, welche durch die in Fig. 4 gezeigte Ausführungsform ausgeführt wird, ist lediglich die bestätigte Senke, welche den Lizenzschlüssel hat, in der Lage, den verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e korrekt zu entschlüsseln, um einen senkseitigen gemeinsamen Sitzungsschlüssel sk' zu erzeugen, der gleich dem quellenseitigen gemeinsamen Sitzungsschlüssel sk ist. Damit ist im Wesentlichen die Ausführungsform ein System, wo die Quelle die Senke bestätigt. In diesem System jedoch ist sogar eine nicht bestätigte Senke in der Lage, einen verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e, der aus einer Verschlüsselung eines quellenseitigen gemeinsamen Sitzungsschlüssels sk resultiert, unter Verwendung eines Lizenzschlüssels lk zu erlangen. Es liegt somit im Bereich des Möglichen, dass eine nicht bestätigte Senke den verschlüsselten quellenseitigen gemeinsamen Sitzungsschlüssel e bei einem Versuch entschlüsselt, um einen senkseitigen gemeinsamen Sitzungsschlüssel sk' zu erlangen, der gleich dem quellenseitigen gemeinsamen Sitzungsschlüssel sk ist.

[0272] Fig. 37 ist ein Diagramm, welches eine Ausführungsform zeigt, bei der eine Bestätigungsprozedur ausgeführt wird, um das oben beschriebene Problem zu lösen, wodurch die Quelle einen verschlüsselten Text, der von einer Verschlüsselung des quellenseitigen gemeinsamen Sitzungsschlüssels sk resultiert, überträgt, lediglich nachdem die Quelle die Senke als gültige Vorrichtung bestätigt hat. Die Prozedur wird anschließend mit Hilfe von Fig. 37 erläutert. Bei dieser Ausführungsform kann ein Verschlüsselungsmodus, der eine Rückführschleife aufweist, beispielsweise der CBC-Modus als Verschlüsselungsmodus angenommen werden.

[0273] Da Abschnitte der Verarbeitung, welche in den Schritten S281 bis S285 der in der Figur gezeigten Prozedur die gleichen sind wie die der Schritte S1 bis S5 der in Fig. 4 gezeigten Prozedur, wird eine Erläuterung dafür nicht wiederholt. In einem Schritt S286 erzeugt das DVD-Wiedergabegerät **1** Zufallszahlen r1 und r2, die jeweils eine Anzahl von Bits haben, die vorher so bestimmt ist, dass diese typischerweise **64** sind, und verkettet diese, um M1 zu bilden. Die Prozedur läuft dann weiter zu einem Schritt S287, in welchem das DVD-Wiedergabegerät M1 verschlüsselt, wobei der Lizenzschlüssel lk verwendet wird, um X zu erzeugen, welches dann im Schritt S288 zum Personalcomputer **2** übertragen wird.

[0274] Der Personalcomputer **2**, der X in einem Schritt S289 empfängt, entschlüsselt X unter Ver-

wendung des Lizenzschlüssels in einem Schritt S290, um M' zu erzeugen, welches als r1' || r'' angesehen wird, eine Verkettung von r', die jeweils eine vorher festgelegte Anzahl von Bits aufweist, üblicherweise 64 Bits. Danach läuft die Prozedur weiter zu einem Schritt S291, um eine Zufallszahl r3 zu erzeugen, die eine vorher festgelegte Anzahl von Bits hat, üblicherweise 64. Anschließend läuft die Prozedur weiter zu einem Schritt S292, in welchem r3 mit r2' verkettet wird, um M2 zu bilden. Die Prozedur läuft dann weiter zu einem Schritt S293, bei dem M2 unter Verwendung des Lizenzschlüssels verschlüsselt wird, um Y zu erzeugen, welches dann im Schritt S294 zum DVD-Wiedergabegerät **1** übertragen wird.

[0275] Das DVD-Wiedergabegerät **1**, welches Y in einem Schritt S295 empfängt, entschlüsselt Y unter Verwendung des Lizenzschlüssels lk im Schritt S296, um M2' zu bilden, welches als r3' | r2'' betrachtet wird, eine Verkettung von r''' und r'', welche eine vorher festgelegte Anzahl von Bits aufweist, üblicherweise 64 Bits. Die Prozedur läuft dann weiter zu einem Schritt S297, in welchem r2'' mit r2 verglichen wird, welches im Schritt S286 erzeugt wird, um zu prüfen, ob sie einander gleich sind. Wenn herausgefunden wird, dass r2'' ungleich r2 ist, beurteilt das DVD-Wiedergabegerät **1**, dass der Personalcomputer **2** eine nicht bestätigte Vorrichtung ist und beendet daher das Bestätigungsprotokoll. Wenn herausgefunden wird, dass r2'' gleich r2 ist, läuft andererseits die Prozedur weiter zu einem Schritt S298, in welchem das DVD-Wiedergabegerät **1** einen quellenseitigen gemeinsamen Sitzungsschlüssel sk erzeugt. Die Prozedur läuft dann weiter zu einem Schritt S299, bei dem r3' mit sk verkettet wird, um M3 zu erzeugen. Danach läuft die Prozedur weiter zu einem Schritt S300, in welchem M3 unter Verwendung des Lizenzschlüssels lk verschlüsselt wird, um einen verschlüsselten Text Z erzeugen, der dann im Schritt S301 zum Personalcomputer **2** übertragen wird.

[0276] Der Personalcomputer **2**, der Z in einem Schritt S302 empfängt, entschlüsselt Z unter Verwendung des Lizenzschlüssels in einem Schritt S303, um M3' zu erzeugen, welches als r3'' || sk' angesehen wird, eine Verkettung von r3'' und sk', die jeweils eine vorher festgelegte Anzahl von Bits aufweisen, üblicherweise 64 Bits. Die Prozedur läuft dann weiter zu einem Schritt S304, um zu prüfen, ob r3'' gleich r3 ist, welches im Schritt S291 erzeugt wurde. Wenn herausgefunden wird, dass r3'' ungleich r3 ist, beurteilt der Personalcomputer **2**, dass das DVD-Wiedergabegerät eine nicht bestätigte Vorrichtung ist, und beendet folglich das Bestätigungsprotokoll. Wenn herausgefunden wird, dass r3'' gleich r3 ist, akzeptiert dagegen der Personalcomputer **2** den senkseitigen gemeinsamen Sitzungsschlüssel sk', der im Schritt S303 erzeugt wurde, als quellenseitigen gemeinsamen Sitzungsschlüssel sk.

[0277] Bei dem Bestätigungsprotokoll, welches durch die oben beschriebene Ausführungsform ausgeführt wird, überträgt, nachdem das DVD-Wiedergabegerät **1**, welches als Quelle dient, den Personalcomputer **2** als bestätigte Senke bestätigt hat, das DVD-Wiedergabegerät **1** den verschlüsselten Text Z, der von der Verschlüsselung des quellenseitigen gemeinsamen Sitzungsschlüssels sk resultiert, zur Senke. Auf dem Kopf davon, ähnlich wie bei der in Fig. 33 gezeigten Ausführungsform, variiert bei der vorliegenden Ausführungsform, sogar, wenn der quellenseitige gemeinsame Sitzungsschlüssel sk, von dem die Quelle einen verschlüsselten Text Z unter Verwendung des Lizenzschlüssel lk erzeugt, in einer Sitzung unverändert bleibt, Z von Verschlüsselung von Verschlüsselung während der Sitzung aufgrund der Tatsache, dass r3', eine variable Zahl bei jeder Verschlüsselung beteiligt ist. Als Ergebnis bietet bei der vorliegenden Ausführungsform diese ein Merkmal, welches es für eine nicht bestätigte Person schwierig macht, übertragene Information zu stehlen.

[0278] Die in Fig. 37 gezeigte Ausführungsform hat jedoch eine Schwierigkeit, wenn r1, r2, r3 und sk jeweils eine Breite von n Bits haben, aufgrund der Tatsache, dass ein n-Bit-Verschlüsselungsalgorithmus angenommen wird. Der Grund dafür liegt darin, wenn die ersten n Bits von Y, die im Schritt S295 empfangen werden, als erste n Bits von Z im Schritt S300 so wie sie sind verwendet werden, die Quelle den Gültigkeitstest, der durch die Senke im Schritt S303 ausgeführt wird, durchlaufen lässt, sogar, wenn die Quelle eine nicht bestätigte Vorrichtung ist.

[0279] Mit Richtung auf das oben beschriebene Problem liefert die vorliegende Erfindung weitere Ausführungsformen, welche in Fig. 38 bis Fig. 40 gezeigt ist, wobei Diagramme jeweils ein Bestätigungsprotokoll zeigen, bei dem die Quelle nicht nur einen verschlüsselten Text überträgt, der aus der Verschlüsselung eines quellenseitigen gemeinsamen Sitzungsschlüssels sk resultiert, nachdem die Gültigkeit der Senke verifiziert ist, sondern die Quelle auch in der Lage ist, die Quelle zu bestätigen. Die in Fig. 38 und Fig. 39 gezeigten Prozeduren ist jeweils eine typische Modifikation der in Fig. 37 gezeigten Ausführungsform.

[0280] Zunächst wird die Ausführungsform, bei der ein Bestätigungsprotokoll von Fig. 38 ausgeführt wird, erläutert. In dieser Ausführungsform kann irgendein Verschlüsselungsmodus, der eine Rückführungsschleife aufweist, beispielsweise der CBC-Modus als Verschlüsselungsmodus angenommen werden.

[0281] Da Abschnitte der Verarbeitung, welche in den Schritten S311 bis S327 der in der Figur gezeigten Prozedur die gleichen sind wie die der Schritte S281 bis S297 der in Fig. 37 gezeigten Prozedur,

wird eine Erläuterung dafür nicht wiederholt. In einem Schritt S328 erzeugt das DVD-Wiedergabegerät **1** eine Zufallszahl r4 und einen quellenseitigen gemeinsamen Sitzungsschlüssel sk, die jeweils eine Anzahl von Bits aufweisen, die vorher bei typisch 64 bestimmt ist. Die Prozedur läuft dann weiter zu einem Schritt S329, bei dem r4 mit r3' und sk verkettet wird, um M3 zu erzeugen. Die Prozedur läuft dann weiter zu einem Schritt S330, bei dem M3 unter Verwendung des Lizenzschlüssels lk verschlüsselt wird, um Z zu erzeugen, welches dann im Schritt S331 zum Personalcomputer **2** übertragen wird.

[0282] Der Personalcomputer **2**, der Z im Schritt S332 empfängt, entschlüsselt Z unter Verwendung des Lizenzschlüssels in einem Schritt S333, um M3' zu erzeugen, welches als r4' || r3" || sk' betrachtet wird, eine Verkettung von r4', r3" und sk', die jeweils eine vorher festgelegte Anzahl von Bits aufweisen, üblicherweise 64 Bits. Die Prozedur läuft dann weiter zu einem Schritt S334, um zu prüfen, ob r3" gleich r3 ist, welches im Schritt S321 erzeugt wird. Wenn herausgefunden wird, dass r3" ungleich r3 ist, beurteilt der Personalcomputer **2**, dass das DVD-Wiedergabegerät eine nicht bestätigte Vorrichtung ist, und folglich wird das Bestätigungsprotokoll beendet. Wenn herausgefunden wird, dass r3" gleich r3 ist, akzeptiert dagegen der Personalcomputer **2** den senkseitigen gemeinsamen Sitzungsschlüssel sk', der im Schritt S333 erzeugt wird, als quellenseitigen gemeinsamen Sitzungsschlüssel sk.

[0283] Bei der Ausführungsform, bei der das oben beschriebene Bestätigungsprotokoll ausgeführt wird, überträgt nicht nur die Quelle einen verschlüsselten Text, der von der Verschlüsselung eines quellenseitigen gemeinsamen Sitzungsschlüssels nach Verifizierung der Gültigkeit der Senke resultiert, sondern die Senke ist auch in der Lage, die Quelle zu bestätigen.

[0284] Ähnlich wie die oben beschriebene in Fig. 38 beschriebene Prozedur ist die in Fig. 39 gezeigte Prozedur auch eine typische Modifikation der in Fig. 37 gezeigten Ausführungsform. Bei dieser Ausführungsform kann ein Verschlüsselungsmodus, der eine Rückführungsschleife aufweist, beispielsweise der CBC-Modus als Verschlüsselungsmodus angenommen werden.

[0285] Da Abschnitte der Verarbeitung, welche in den Schritten S351 bis S361 der in Fig. 39 gezeigten Prozedur die gleichen sind wie diejenigen der Schritte S381 bis S291 der in Fig. 37 gezeigten Prozedur, wird eine Erläuterung dafür nicht wiederholt. Im Schritt S362 erzeugt der Personalcomputer **2** r2' || r3 als M2. Die Verarbeitung läuft dann weiter zu einem Schritt S363, in welchem der Personalcomputer **2** M3 unter Verwendung des Lizenzschlüssels verschlüsselt, um Y zu erzeugen, welches dann im Schritt S364 zum DVD-Wiedergabegerät **1** übertragen wird.

[0286] Das DVD-Wiedergabegerät **1**, welches Y in einem Schritt S365 empfängt, entschlüsselt Y unter Verwendung des Lizenzschlüssels lk im Schritt S366, um M2' zu erzeugen, welches als r2" || r3 angesehen wird, eine Verkettung von r2" und r3, die jeweils eine vorher festgelegte Anzahl von Bits aufweisen, üblicherweise 64 Bits. Die Prozedur läuft dann weiter zu einem Schritt S367, um zu prüfen, ob r2" gleich r2 ist, der im Schritt S356 erzeugt wird. Wenn herausgefunden wird, dass r2" ungleich r2 ist, beurteilt das DVD-Wiedergabegerät **1**, dass der Personalcomputer eine nicht bestätigte Vorrichtung ist, und beendet folglich das Bestätigungsprotokoll. Wenn herausgefunden wird, dass r2" gleich r2 ist, läuft dagegen die Prozedur weiter zu einem Schritt S368, in welchem das DVD-Wiedergabegerät einen quellenseitigen gemeinsamen Sitzungsschlüssel sk erzeugt. Die Prozedur läuft dann weiter zu einem Schritt S369, bei dem sk mit r3' verkettet wird, um M3 zu erzeugen. Danach läuft die Prozedur weiter zu einem Schritt S370, in welchem M3 unter Verwendung des Lizenzschlüssels lk verschlüsselt wird, um einen verschlüsselten Text Z zu erzeugen, der dann in einem Schritt S371 zum Personalcomputer **2** übertragen wird.

[0287] Der Personalcomputer **2**, der Z in einem Schritt S372 empfängt, entschlüsselt Z unter Verwendung des Lizenzschlüssels im Schritt S373, um M3' zu erzeugen, welches als r3" || sk' angesehen wird, eine Verkettung von r3" || sk', die jeweils eine vorher festgelegte Anzahl von Bits aufweisen, üblicherweise 64 Bits. Die Verarbeitung läuft dann weiter zu einem Schritt S374, um zu prüfen, ob r3" gleich r3 ist, welche im Schritt S361 erzeugt werden. Wenn herausgefunden wird, dass r3" ungleich r3 ist, beurteilt der Personalcomputer **2**, dass das DVD-Wiedergabegerät eine nicht bestätigte Vorrichtung ist, und beendet somit das Bestätigungsprotokoll. Wenn herausgefunden wird, dass r3" gleich r3 ist, akzeptiert dagegen der Personalcomputer **2** den senkseitigen gemeinsamen Sitzungsschlüssel sk', der im Schritt S373 erzeugt wurde, als quellenseitigen gemeinsamen Sitzungsschlüssel sk.

[0288] Bei der Ausführungsform, bei der das Bestätigungsprotokoll wie oben beschrieben ausgeführt wird, überträgt die Quelle einen verschlüsselten Text, der von der Verschlüsselung eines quellenseitigen gemeinsamen Sitzungsschlüssels sk resultiert, zu einer Senke, nachdem die Gültigkeit der Senke verifiziert ist, und zusätzlich ist auch die Senke in der Lage, die Quelle zu bestätigen. Außerdem variiert sehr ähnlich wie bei der in Fig. 33 gezeigten Ausführungsform in dem Fall bei der vorliegenden Ausführungsform, sogar wenn der quellenseitige gemeinsame Sitzungsschlüssel sk, von dem die Quelle einen verschlüsselten Text Z unter Verwendung des Lizenzschlüssels lk in einer Sitzung unverändert bleibt, Z von Verschlüsselung zu Verschlüsselung während der Sitzung aufgrund der Tatsache, dass r4, eine va-

riable Zahl, welche durch das DVD-Wiedergabegerät **1** erzeugt wird, bei jeder Verschlüsselung beteiligt ist. Als Ergebnis bietet die vorliegende Ausführungsform ein Merkmal, welches es für eine nicht bestätigte Person schwierig macht, übertragene Information zu stehlen.

[0289] In Fig. 40 ist ein Diagramm, welches eine Ausführungsform zeigt, bei der ein Bestätigungsprotokoll ausgeführt wird, welches die gleichen Funktionen hat, wie diejenigen, die in Fig. 38 und Fig. 39 gezeigt sind. Auch bei der vorliegenden Ausführungsform kann irgendein Verschlüsselungsmodus, der eine Rückführschleife aufweist, beispielsweise CBC-Modus als Verschlüsselungsmodus angenommen werden. Da Abschnitte der Verarbeitung, die in den Schritte S381 bis S384 der in der Figur gezeigten Prozedur die gleichen sind wie diejenigen der Schritte S1 bis S4 der in Fig. 4 gezeigten Prozedur, wird eine Erläuterung dafür nicht wiederholt. In einem Schritt S385 erzeugt das DVD-Wiedergabegerät **1** eine Zufallszahl Rsrx, welche eine vorher festgelegte Anzahl von Bits hat, üblicherweise 64 Bits. Die Prozedur geht dann weiter zu einem Schritt S386, bei dem die Zufallszahl Rscr zum Personalcomputer **2** übertragen wird.

[0290] Die Prozedur läuft dann weiter zu einem Schritt S387, in welchem der Personalcomputer **2** die Zufallszahl Rscr empfängt. Anschließend läuft die Prozedur weiter zu einem Schritt S388, in welchem der Personalcomputer **2** eine Zufallszahl Rsnk erzeugt, die eine vorher festgelegte Anzahl von Bits hat, üblicherweise 64 Bits. Die Prozedur läuft dann weiter zu einem Schritt S389, in welchem die Zufallszahl Rsrc mit der Zufallszahl Rsnk verkettet wird, um M1 zu erzeugen. Danach läuft die Prozedur weiter zu einem Schritt S390, in welchem M1 unter Verwendung des Lizenzschlüssels verschlüsselt wird, um X zu erzeugen, welches dann zum DVD-Wiedergabegerät in einem Schritt S391 übertragen wird.

[0291] In einem Schritt S392 empfängt das DVD-Wiedergabegerät **1** X. Die Prozedur läuft dann weiter zu einem Schritt S393, bei dem ein Lizenzschlüssel lk von einer ID, welche dem Personalcomputer **2** zugeteilt wird, und ein Dienstschlüssel berechnet wird. Im Schritt S394 wird der Lizenzschlüssel lk dazu verwendet, X zu entschlüsseln, um M2' zu erzeugen, welches als Rsnk' || Rsrc' angesehen wird, eine Verkettung von Rsnk' und Rsrc', die jeweils eine vorher festgelegte Anzahl von Bits aufweisen, üblicherweise 64 Bits. Danach läuft die Prozedur weiter zu einem Schritt S395, um zu prüfen, ob Rsrc' = Rsrc. Wenn herausgefunden wird, dass Rscr' ungleich Rsrc ist, wird beurteilt, dass der Personalcomputer **2** eine nicht bestätigte Vorrichtung ist, wobei in diesem Fall das Bestätigungsprotokoll beendet wird. Wenn herausgefunden wird, dass Rsrc' gle3ich Rsrc ist, läuft dagegen die Prozedur weiter zu einem Schritt S396, in welchem das DVD-Wiedergabegerät **1** einen quellenseitigen gemeinsamen Sitzungsschlüssel sk erzeugt. Nachfolgend läuft die Prozedur weiter zu einem Schritt S397, bei dem Rscr mit Rsnk' und sk verkettet wird, um M2 zu erzeugen. Die Prozedur läuft dann weiter zu einem Schritt S398, in welchem M2 verschlüsselt wird, unter Verwendung des Lizenzschlüssels lk, um Y zu erzeugen, welches dann in einem Schritt S399 zum Personalcomputer **2** übertragen wird.

[0292] Der Personalcomputer **2**, der Y in einem Schritt S400 empfängt, entschlüsselt Y unter Verwendung des Lizenzschlüssels in einem Schritt S401, um M3 zu erzeugen, welches als Rsrc" || Rsnk" || sk' angesehen wird, eine Verkettung von Rsrc", Rsnk" und Sk', die jeweils eine vorher festgelegte Anzahl von Bits aufweisen, üblicherweise 64 Bits. Die Prozedur läuft dann weiter zu einem Schritt S402, um zu prüfen, ob Rsnk" gleich Rsnk ist, welches im Schritt S388 erzeugt wird. Wenn herausgefunden wird, dass Rsnk" ungleich Rsnk ist, beurteilt der Personalcomputer **2**, dass das DVD-Wiedergabegerät ein nicht bestätigtes Gerät ist, wobei in diesem Fall der senkseitige gemeinsame Sitzungsschlüssel sk' ausrangiert wird. Wenn herausgefunden wird, dass Rsnk" gleich Rsnk ist, wird dagegen sk' als gemeinsamer Sitzungsschlüssel akzeptiert.

[0293] Bei der Ausführungsform, bei der das Bestätigungsprotokoll wie oben beschrieben ausgeführt wird, überträgt die Quelle einen verschlüsselten Text, der von der Verschlüsselung des quellenseitigen gemeinsamen Sitzungsschlüssels sk resultiert, zur Senke, nachdem die Gültigkeit der Senke verifiziert wurde, und zusätzlich ist auch die Senke in der Lage, die Quelle zu bestätigen. Außerdem variiert sehr ähnlich wie bei der in Fig. 33 gezeigten Ausführungsform im Fall der vorliegenden Ausführungsform, sogar wenn der quellenseitige gemeinsame Sitzungsschlüssel sk, von dem die Quelle einen verschlüsselten Text Y unter Verwendung des Lizenzschlüssel lk erzeugt, in einer Sitzung unverändert bleibt, Y von Verschlüsselung zu Verschlüsselung während der Sitzung aufgrund der Tatsache, dass Rscr, eine variable Zahl, welche durch DVD-Wiedergabegerät erzeugt wird, bei jeder Verschlüsselung beteiligt ist. Als Ergebnis bietet die vorliegende Ausführungsform ein Merkmal, welches es für eine nicht bestätigte Person schwierig macht, Übertragungsinformation zu stehlen.

[0294] Bei den oben beschriebenen Ausführungsformen dient das DVD-Wiedergabegerät **1** als Quelle, während der Personalcomputer **2** und die optische Magnetplattenvorrichtung **3** jeweils als Senke dienen. Es sei angemerkt, dass die Beschreibung nicht dazu dienen soll, in einem beschränkenden Sinn aufgebaut zu sein. Das soll heißen, dass jede beliebige elektronische Vorrichtung als Quelle oder als Senke

verwendet werden kann.

[0295] Während außerdem der 1394-Seriell-Bus **11** als externer Bus zum Verbinden der elektronischen Vorrichtungen, die aus einem Datenverarbeitungssystem bestehen, miteinander verwendet wird, ist der Rahmen der vorliegenden Erfindung nicht auf diese Ausführungsformen beschränkt. Das heißt, dass eine Vielzahl von Bussen als externer Bus verwendet werden können, und die elektronischen Vorrichtungen, die miteinander durch den externen Bus verbunden sind, nicht auf diejenigen beschränkt sind, die bei den oben beschriebenen Ausführungsformen verwendet werden. Alle beliebigen elektronischen Vorrichtungen können dazu verwendet werden, das Datenverarbeitungssystem zu bilden.

[0296] Es ist außerdem erwähnenswert, dass eine Vielzahl von Programmen, die aus Instruktionen bestehen, welche durch CPUs ausgeführt werden, dem Benutzer über das Bereitstellen von Medien, beispielsweise einer Magnetplatte, einer CD-ROM-Platte und einem Netzwerk gezeigt werden, und wenn notwendig, verwendet werden können, wobei die Programme in einer RAM-Einheit oder einer Festplatte gespeichert werden, die in der elektronischen Vorrichtung eingebaut ist.

[0297] Bei einem Beispiel einer Informationsverarbeitungsvorrichtung, bei einem Beispiel eines Informationsverarbeitungsverfahrens und einem Beispiel eines Aufzeichnungsträgers, die durch die vorliegende Erfindung bereitgestellt werden, wird ein erster Schlüssel LK auf der Basis von Identifikationsdaten erzeugt, die von einer anderen Informationsverarbeitungsvorrichtung empfangen werden, und ein zweiter Schlüssel SVK, der die vorher festgelegte Information zeigt, um vorher festgelegter Verarbeitung unterzogen zu werden. Als Ergebnis kann die Sicherheit übertragener Information mit einem hohen Verlässlichkeitsgrad sichergestellt werden.

[0298] Außerdem sind bei einer weiteren beispielhaften Informationsverarbeitungsvorrichtung, einem weiteren beispielhaften Informationsverarbeitungsverfahren und einem weiteren beispielhaften Aufzeichnungsträger, die durch die vorliegende Erfindung bereitgestellt werden, ein erster Schlüssel SVK, der vorher festgelegte Information zeigt, die vorher festgelegter Verarbeitung unterzogen wird, und eine vorher festgelegte Funktion vorher gespeichert. Ein zweiter Schlüssel LK wird durch Anwendung der vorher festgelegten Funktion auf die Identifikationsdaten erzeugt, welche vom anderen Informationsverarbeitungsgerät und dem ersten Schlüssel SVK empfangen werden. Ein dritter Schlüssel SK wird außerdem erzeugt, unter Verwendung des zweiten Schlüssels Lk verschlüsselt und zur anderen Informationsverarbeitungsvorrichtung übertragen. Als Ergebnis ist es möglich, lediglich es einem berechtigten Informationsverarbeitungsgerät zu erlauben, eine vorher festgelegte Verarbeitung in Bezug auf Information, die zu diesem übertragen wird, auszuführen, wodurch weiter die Sicherheit der Information sichergestellt wird.

[0299] Bei dem beispielhaften Informationsverarbeitungssystem, einem weiteren beispielhaften Informationsverarbeitungsverfahren und einem weiteren beispielhaften Aufzeichnungsträger, die durch die vorliegende Erfindung bereitgestellt werden, werden in der ersten Informationsverarbeitungsvorrichtung ein erster Schlüssel SVK in Verbindung mit Information, die zum zweiten Informationsverarbeitungsvorrichtung zu übertragen sind, und eine vorher festgelegte Funktion vorher gespeichert. Ein zweiter Schlüssel LK1 wird durch Anwendung der vorher festgelegten Funktion auf Identifikationsdaten erzeugt, welche der zweiten Informationsverarbeitungsvorrichtung zugeteilt werden und eines ersten Schlüssels SVK davon empfangen werden. Ein dritter Schlüssel SK1 wird außerdem dadurch erzeugt, unter Verwendung des zweiten Schlüssels LK2 verschlüsselt und zur zweiten Informationsverarbeitungsvorrichtung übertragen. In der zweiten Informationsverarbeitungsvorrichtung werden dagegen die Identifikationsdaten, welche der zweiten Informationsverarbeitungsvorrichtung zugeteilt sind, d.h., die Identifikationsdaten, welche der zweiten Informationsverarbeitungsvorrichtung gehören, welche der zweiten Informationsverarbeitungsvorrichtung spezifisch sind, und ein vierter Schlüssel LK2, der eine Erlaubnis zeigt, um vorher festgelegte Verarbeitung in Bezug auf vorher festgelegte Information auszuführen, welche von der ersten Informationsverarbeitungsvorrichtung empfangen wird, vorher gespeichert. Der verschlüsselte dritte Schlüssel, der von der ersten Informationsverarbeitungsvorrichtung empfangen wird, wird zurück in den dritten Schlüssel sk1 unter Verwendung des vierten Schlüssel LK2 entschlüsselt. Als Ergebnis kann ein Informationsverarbeitungssystem, welches eine hohe Sicherheit übertragener Information anbietet, ausgeführt werden.

[0300] Außerdem kann gemäß einem noch weiteren beispielhaften Informationsverarbeitungsgerät ein noch weiteres beispielhaftes Informationsverarbeitungsverfahren und ein noch weiteres beispielhafter Aufzeichnungsträger durch die vorliegende Erfindung bereitgestellt werden, wobei ein erster Schlüssel LK, ein zweiter Schlüssel LK' und eine vorher festgelegte Funktion G vorher gespeichert sind. Der zweite Schlüssel LK' wird vorher auf der Basis des ersten Schlüssels LK und der inversen Funktion G ^ – 1 der vorher festgelegten Funktion G erzeugt. Als Ergebnis kann die Sicherheit übertragener Information mit einem hohen Verlässlichkeitsgrad sichergestellt werden.

[0301] Gemäß einer noch weiteren beispielhaften Informationsverarbeitungsvorrichtung, einem noch

weiteren beispielhaften Informationsverarbeitungsverfahren und einem noch weiteren beispielhaften Aufzeichnungsträger, welche durch die vorliegende Erfindung bereitgestellt werden, werden Daten H unter Anwendung einer vorher festgelegten Funktion auf Identifikationsdaten, welche einer anderen Informationsverarbeitungsvorrichtung zugeteilt und davon empfangen werden, und eines ersten Schlüssels SVK erzeugt. Ein zweiter Schlüssel SK wird dann unter Verwendung einer Pseudozufallszahl PRNG (H) verschlüsselt, die von den Daten H erzeugt wird und zur anderen Informationsverarbeitungsvorrichtung übertragen wird. Als Ergebnis kann eine Informationsverarbeitungsvorrichtung, die eine hohe Sicherheit übertragener Information bietet, ausgeführt werden.

[0302] Außerdem werden bei einem noch weiteren beispielhaften Informationsverarbeitungssystem, einem noch weiteren beispielhaften Informationsverarbeitungsverfahren und bei einem noch weiteren beispielhaften Aufzeichnungsträger, die durch die vorliegende Erfindung bereitgestellt werden, werden Daten in der ersten Informationsverarbeitungsvorrichtung durch Anwendung der ersten Funktion H auf Identifikationsdaten erzeugt, die der zweiten Informationsverarbeitungsvorrichtung und dem ersten Schlüssel SVK zugeordnet sind und davon empfangen werden. Ein zweiter Schlüssel wird unter Verwendung einer Pseudozufallszahl pRNG (H) verschlüsselt, der von den Daten H erzeugt wird und zur zweiten Informationsverarbeitungsvorrichtung übertragen wird. In der zweiten Informationsverarbeitungsvorrichtung sind dagegen ein dritter Schlüssel LK, ein vierter Schlüssel LK' und eine vorher festgelegte Funktion G vorher gespeichert. Der vierte Schlüssel LK' wird auf der Basis des dritten Schlüssels LK und der inversen Funktion G^ 1 der vorher festgelegten Funktion G erzeugt. Als Ergebnis kann ein Informationsverarbeitungssystem, welches eine hohe Sicherheit übertragener Information bietet, ausgeführt werden.

Patentansprüche

1. Datenübertragungsvorrichtung (**1**) zum Übertragen von Daten, nachdem eine vorher festgelegte Verarbeitung durchgeführt wurde, auf der Basis des vorrichtungs-eigenen ID-Codes und eines ID-Codes, der von einer Partnervorrichtung empfangen wird, wobei die Datenübertragungsvorrichtung aufweist:
eine Signalempfangseinrichtung (**26**) zum Empfangen eines Signals von einer Partnervorrichtung (**2**), wobei die Signalbereitstellungsinformation die Partnervorrichtung zeigt;
eine Signalübertragungseinrichtung (**26**) zum Übertragen eines Signals zur Partnervorrichtung; und
eine Signalverschlüsselungseinrichtung zum Ausführen vorher festgelegter Verschlüsselung in Bezug auf ein Signal, welches zu übertragen ist,
wobei die Signalverschlüsselungseinrichtung die Information prüft, welche die Partnervorrichtung zeigt, welche von der Signalempfangseinrichtung empfangen wird, und, wenn ein Signal schon gefunden ist, welches zur Partnervorrichtung übertragen wurde, dieses Signal nicht wieder zur Partnervorrichtung übertragen wird.

2. Datenübertragungsvorrichtung nach Anspruch 1, wobei die Partnervorrichtung eine Signalübertragungsquelle aufweist.

3. Datenübertragungsvorrichtung nach Anspruch 2, wobei:
die Signalübertragungseinrichtung ein ID-Anforderungssignal und einen verschlüsselten Text überträgt;
die Signalempfangseinrichtung eine ID empfängt; und
die Signalverschlüsselungseinrichtung einen verschlüsselten Text von einem vorher festgelegten Schlüssel erzeugt.

4. Datenübertragungsverfahren zum Übertragen von Daten, nachdem eine vorher festgelegte Verarbeitung ausgeführt wurde, auf der Basis eines eigenen ID-Codes und eines ID-Codes, der von einer Partnervorrichtung empfangen wird, wobei das Verfahren aufweist:
Empfangen (S202) eines Signals von einer Partnervorrichtung (**2**), wobei die Signalbereitstellungsinformation diese Partnervorrichtung zeigt und;
Bestimmen (S203), wenn herausgefunden wird, dass ein Signal schon zur Partnervorrichtung übertragen wurde, und, wenn dies so ist, die Information nicht wiederum zur Partnervorrichtung übertragen wird, sondern, wenn, das Signal noch nicht zur Partnervorrichtung übertragen wurde, das Signal verschlüsselt wird und zur Partnervorrichtung übertragen wird (S204).

5. Datenübertragungsverfahren nach Anspruch 4, wobei das Signal unter Verwendung von Information, die vorher gespeichert wurde, und empfangener Information verschlüsselt wird.

6. Aufzeichnungsträger zum Speichern eines Programms, welches ein Datenübertragungsverfahren nach Anspruch 4 oder 5 vorschreibt.

7. Datenempfangsvorrichtung (**2**) zum Entschlüsseln von Daten, welche von einer Partnervorrichtung empfangen werden, unter Verwendung des vorrichtungs-eigenen Schlüssels, und Information, die auch von der Partnervorrichtung empfangen wird, wobei die Datenempfangsvorrichtung aufweist:
eine Signalempfangseinrichtung (**49**) zum Empfangen eines ID-Anforderungssignals von einer Partnervorrichtung (**1**);
eine Textentschlüsselungseinrichtung zum Ent-

schlüsseln eines verschlüsselten Texts, welcher durch die Signalempfangseinrichtung empfangen wird; und
eine Signalübertragungseinrichtung zum Übertragen eines Signals zu einer Partnervorrichtung,
wobei die Signalübertragungseinrichtung ein Beglaubigungsanforderungssignal und ein ID-Signal überträgt.

8. Datenempfangsverfahren zum Entschlüsseln von Daten, welche von einer Partnervorrichtung empfangen werden, unter Verwendung eines eigenen Schlüssels, und von Information, welche auch von der Partnervorrichtung empfangen wird, wobei das Verfahren folgende Schritte aufweist:
Übertragen (S201) eines Beglaubigungsanforderungssignals;
Empfangen (S205) eines ID-Anforderungssignals;
Übertragen (S206) einer ID;
Empfangen (S512) einer verschlüsselten Textes; und
Entschlüsselns (S213) eines empfangenen verschlüsselten Textes.

9. Aufzeichnungsträger zum Speichern eines Programms, welches ein Datenempfangsverfahren zum Entschüsseln von Daten nach Anspruch 8 vorschreibt.

Es folgen 39 Blatt Zeichnungen

Anhängende Zeichnungen

FIG. 1

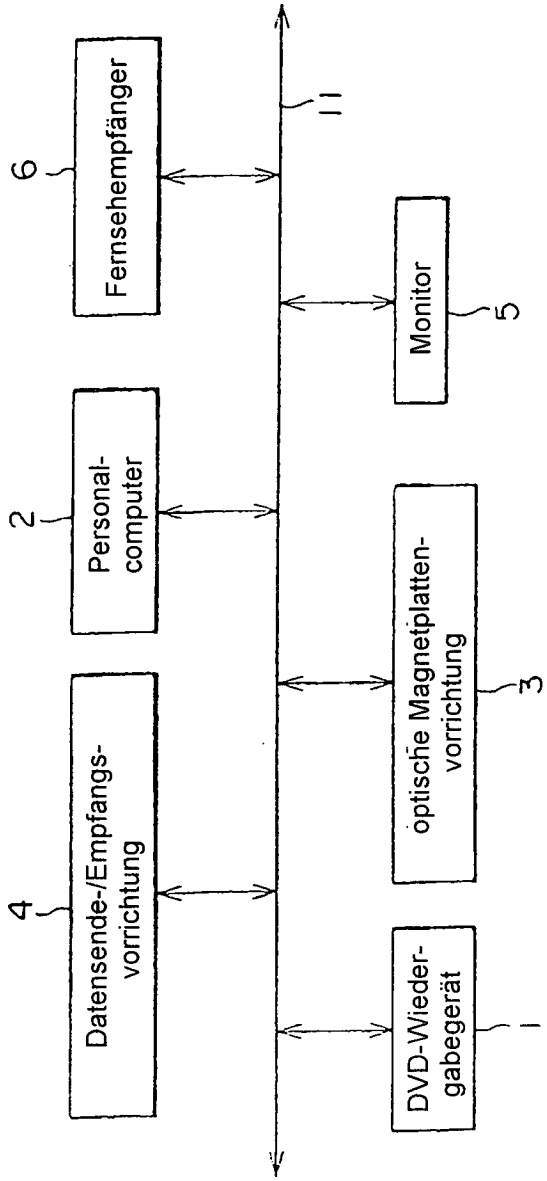


FIG. 2

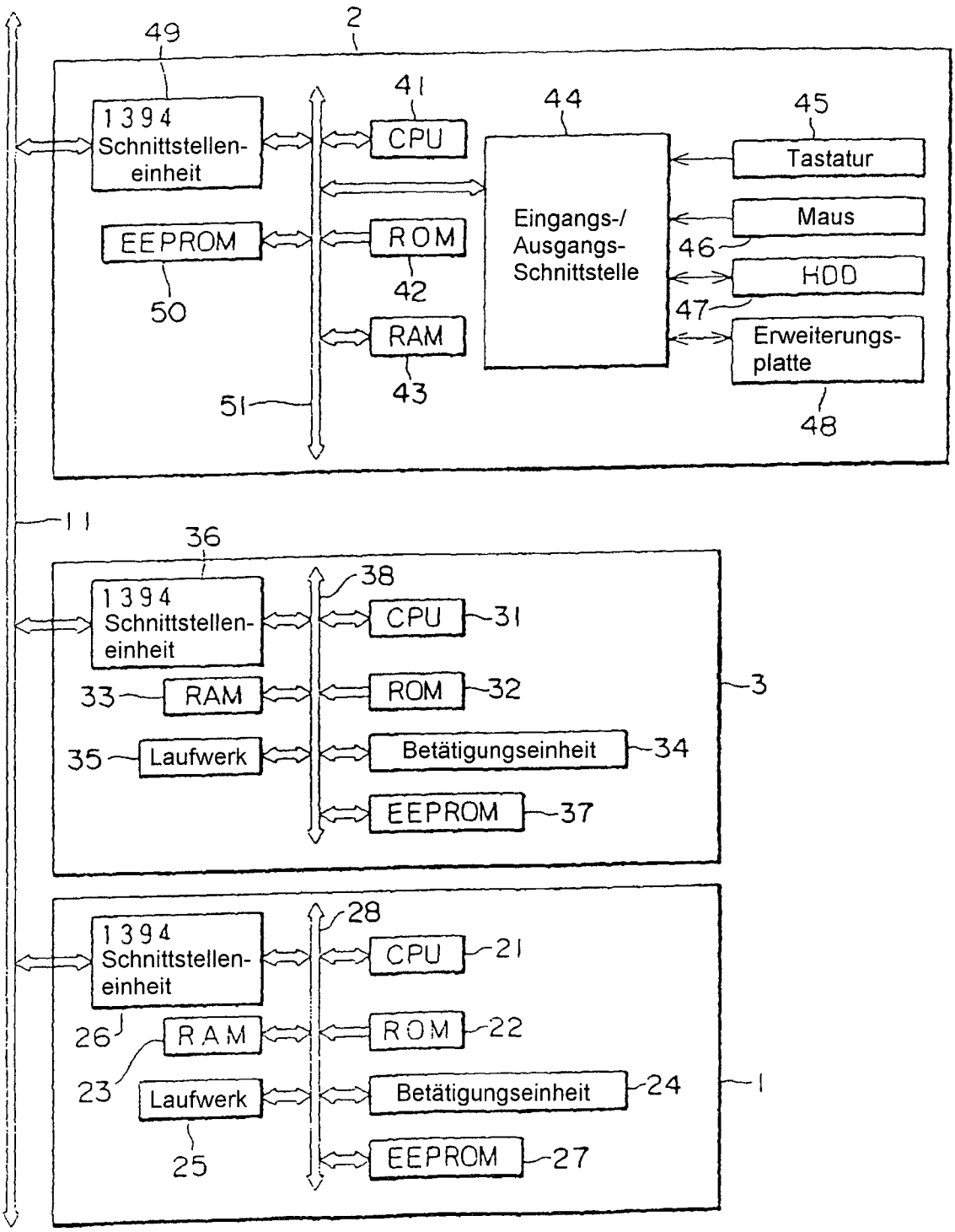

49
2
41
44
45
1394 Schnittstellen-einheit
CPU
Tastatur
Maus
EEPROM
ROM
Eingangs-/ Ausgangs-Schnittstelle
46
HDD
47
RAM
Erweiterungs-platte
50
42
43
51
48
11
36
38
1394 Schnittstellen-einheit
CPU
31
33
RAM
ROM
32
3
35
Laufwerk
Betätigungseinheit
34
EEPROM
37
28
1394 Schnittstellen-einheit
CPU
21
26
RAM
ROM
22
23
Laufwerk
Betätigungseinheit
24
1
25
EEPROM
27

FIG. 3

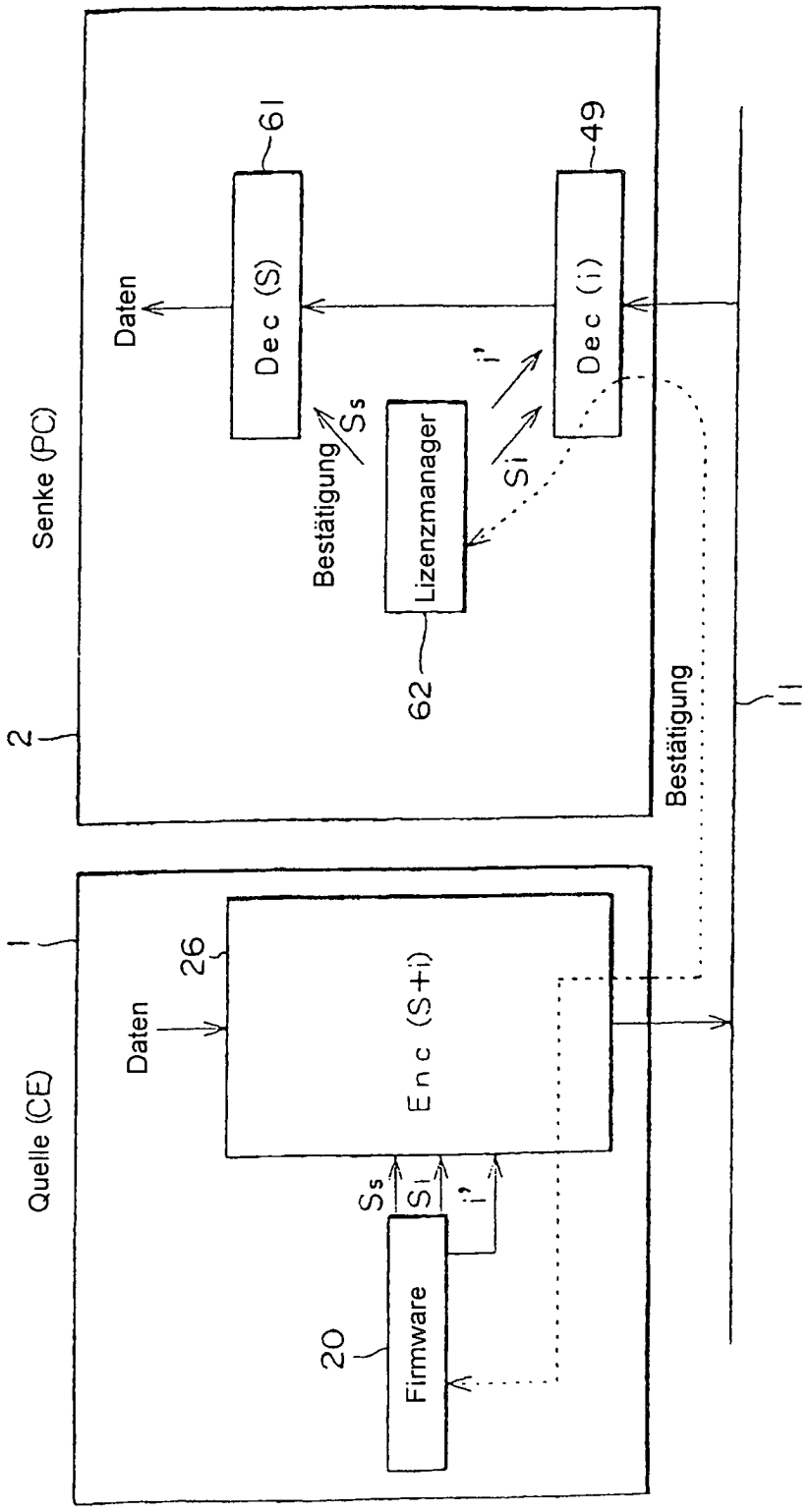

Senke (PC)
2
Daten
Dec (S)
61
Dec (i)
49
i'
Si
Ss
Bestätigung
Lizenzmanager
62
Bestätigung
11
Quelle (CE)
1
Daten
26
Enc (S+i)
Ss
Si
i'
Firmware
20

FIG. 4

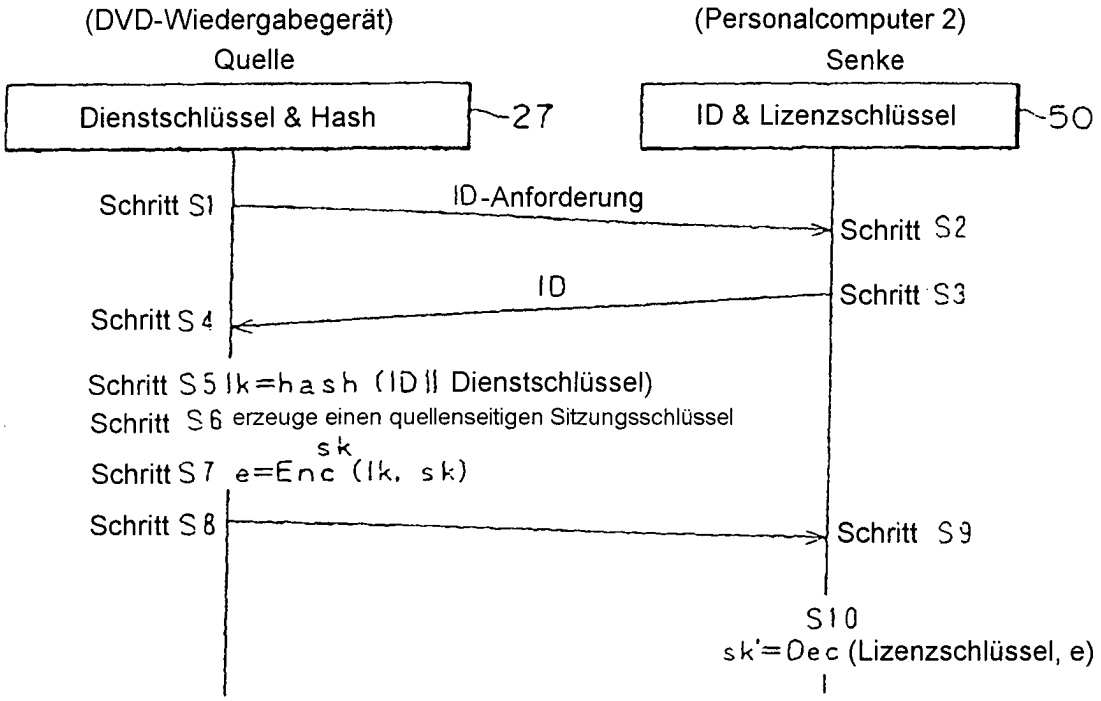

(DVD-Wiedergabegerät)
Quelle
(Personalcomputer 2)
Senke
Dienstschlüssel & Hash
27
ID & Lizenzschlüssel
50
Schritt S1
ID-Anforderung
Schritt S2
ID
Schritt S3
Schritt S4
Schritt S5 Ik=hash (ID|| Dienstschlüssel)
Schritt S6 erzeuge einen quellenseitigen Sitzungsschlüssel
Schritt S7 e=Enc sk (Ik, sk)
Schritt S8
Schritt S9
S10
sk'=Dec (Lizenzschlüssel, e)

FIG. 5

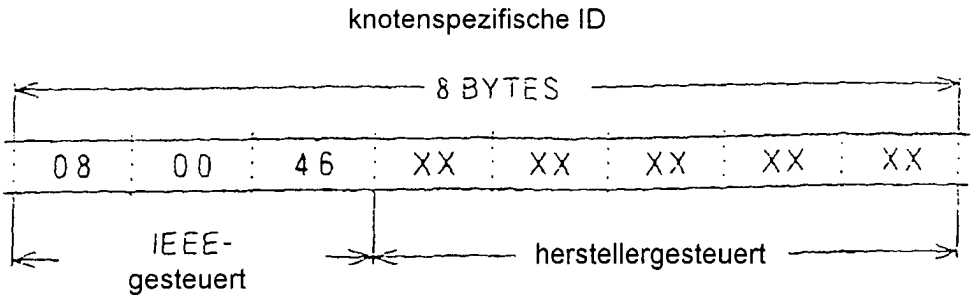

knotenspezifische ID
8 BYTES
08
00
46
XX
XX
XX
XX
XX
IEEE-
gesteuert
herstellergesteuert

FIG. 6

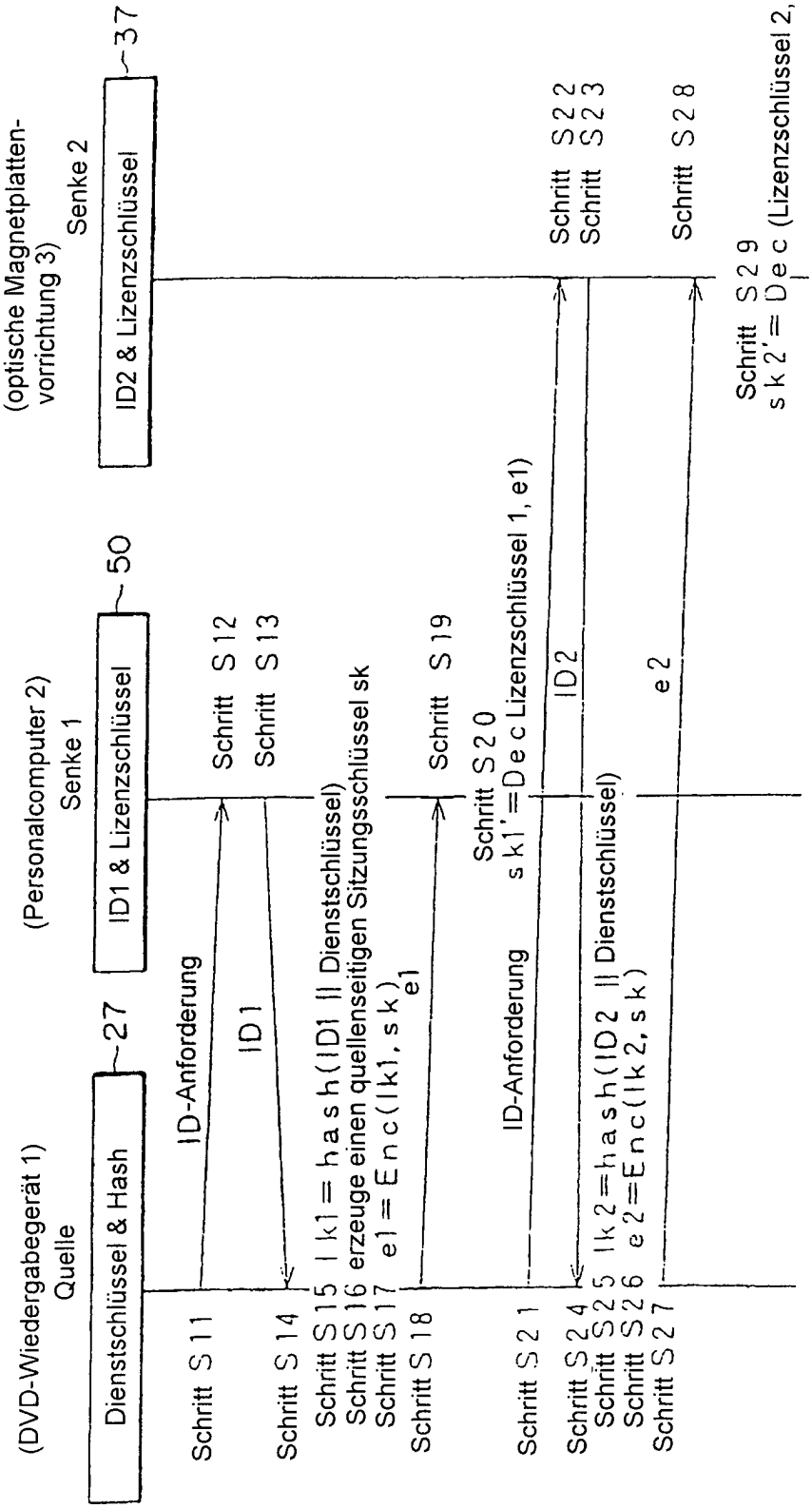

(DVD-Wiedergabegerät 1)
Quelle
Dienstschlüssel & Hash
27
(Personalcomputer 2)
Senke 1
ID1 & Lizenzschlüssel
50
(optische Magnetplatten-vorrichtung 3)
Senke 2
ID2 & Lizenzschlüssel
37
Schritt S11
ID-Anforderung
Schritt S12
Schritt S13
ID1
Schritt S14
Schritt S15 Ik1 = hash(ID1 || Dienstschlüssel)
Schritt S16 erzeuge einen quellenseitigen Sitzungsschlüssel sk
Schritt S17 e1 = Enc(Ik1, sk)
e1
Schritt S18
Schritt S19
Schritt S20
sk1' = Dec Lizenzschlüssel 1, e1)
Schritt S21
ID-Anforderung
Schritt S22
Schritt S23
ID2
Schritt S24
Schritt S25 Ik2 = hash(ID2 || Dienstschlüssel)
Schritt S26 e2 = Enc(Ik2, sk)
e2
Schritt S27
Schritt S28
Schritt S29
sk2' = Dec (Lizenzschlüssel 2, e2)

FIG. 7

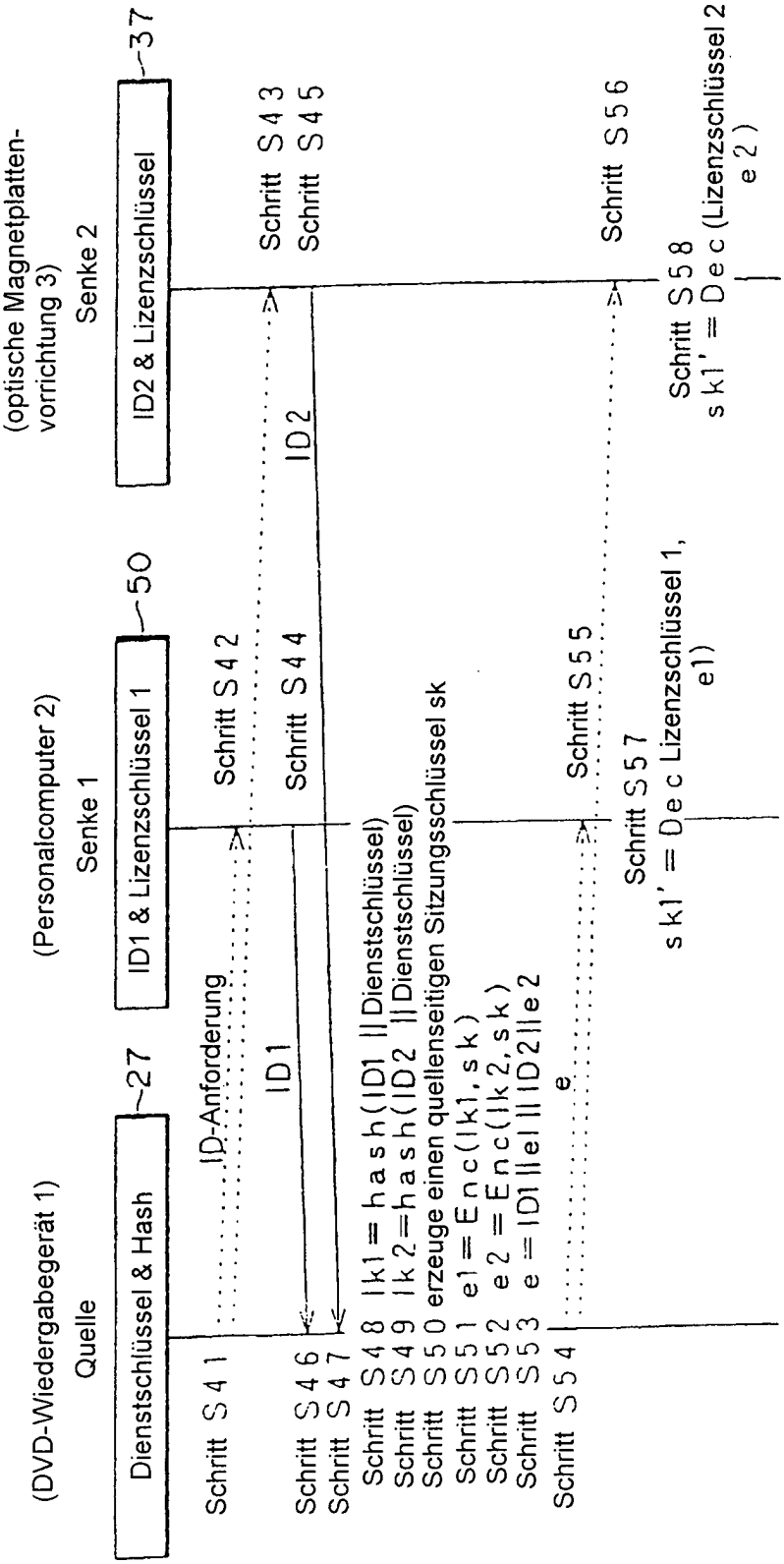

(DVD-Wiedergabegerät 1)
Quelle
Dienstschlüssel & Hash
27
(Personalcomputer 2)
Senke 1
ID1 & Lizenzschlüssel 1
50
(optische Magnetplatten-vorrichtung 3)
Senke 2
ID2 & Lizenzschlüssel
37
Schritt S41
ID-Anforderung
Schritt S42
Schritt S43
Schritt S44
ID1
ID2
Schritt S45
Schritt S46
Schritt S47
Schritt S48 lk1 = hash(ID1 || Dienstschlüssel)
Schritt S49 lk2 = hash(ID2 || Dienstschlüssel)
Schritt S50 erzeuge einen quellenseitigen Sitzungsschlüssel sk
Schritt S51 e1 = Enc(lk1, sk)
Schritt S52 e2 = Enc(lk2, sk)
Schritt S53 e = ID1 || e1 || ID2 || e2
Schritt S54
e
Schritt S55
Schritt S56
Schritt S57
sk1' = Dec Lizenzschlüssel 1, e1)
Schritt S58
sk1' = Dec (Lizenzschlüssel 2 e2)

FIG. 8

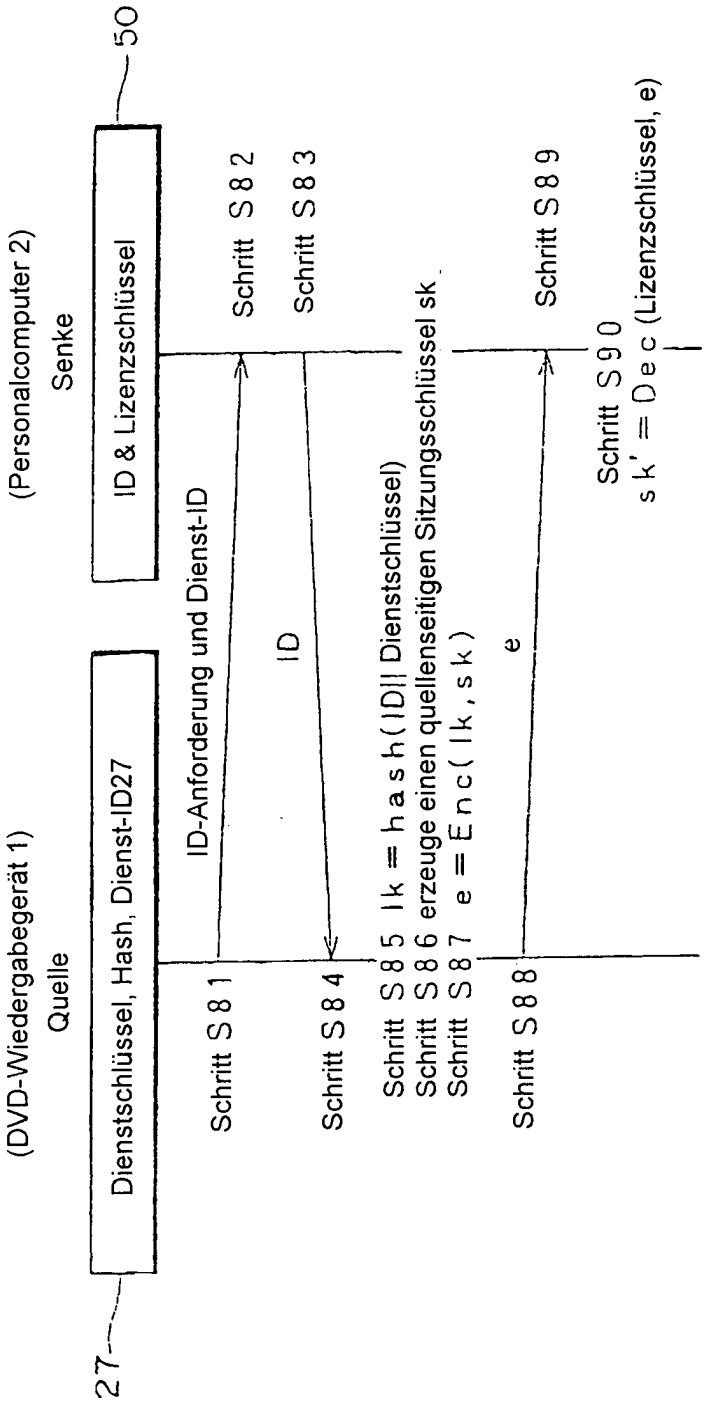

(DVD-Wiedergabegerät 1)
Quelle
Dienstschlüssel, Hash, Dienst-ID27
27
(Personalcomputer 2)
Senke
ID & Lizenzschlüssel
50
ID-Anforderung und Dienst-ID
Schritt S81
ID
Schritt S84
Schritt S82
Schritt S83
Schritt S85 Ik = hash(ID|| Dienstschlüssel)
Schritt S86 erzeuge einen quellenseitigen Sitzungsschlüssel sk
Schritt S87 e = Enc(Ik, sk)
e
Schritt S88
Schritt S89
Schritt S90
sk' = Dec (Lizenzschlüssel, e)

FIG. 9

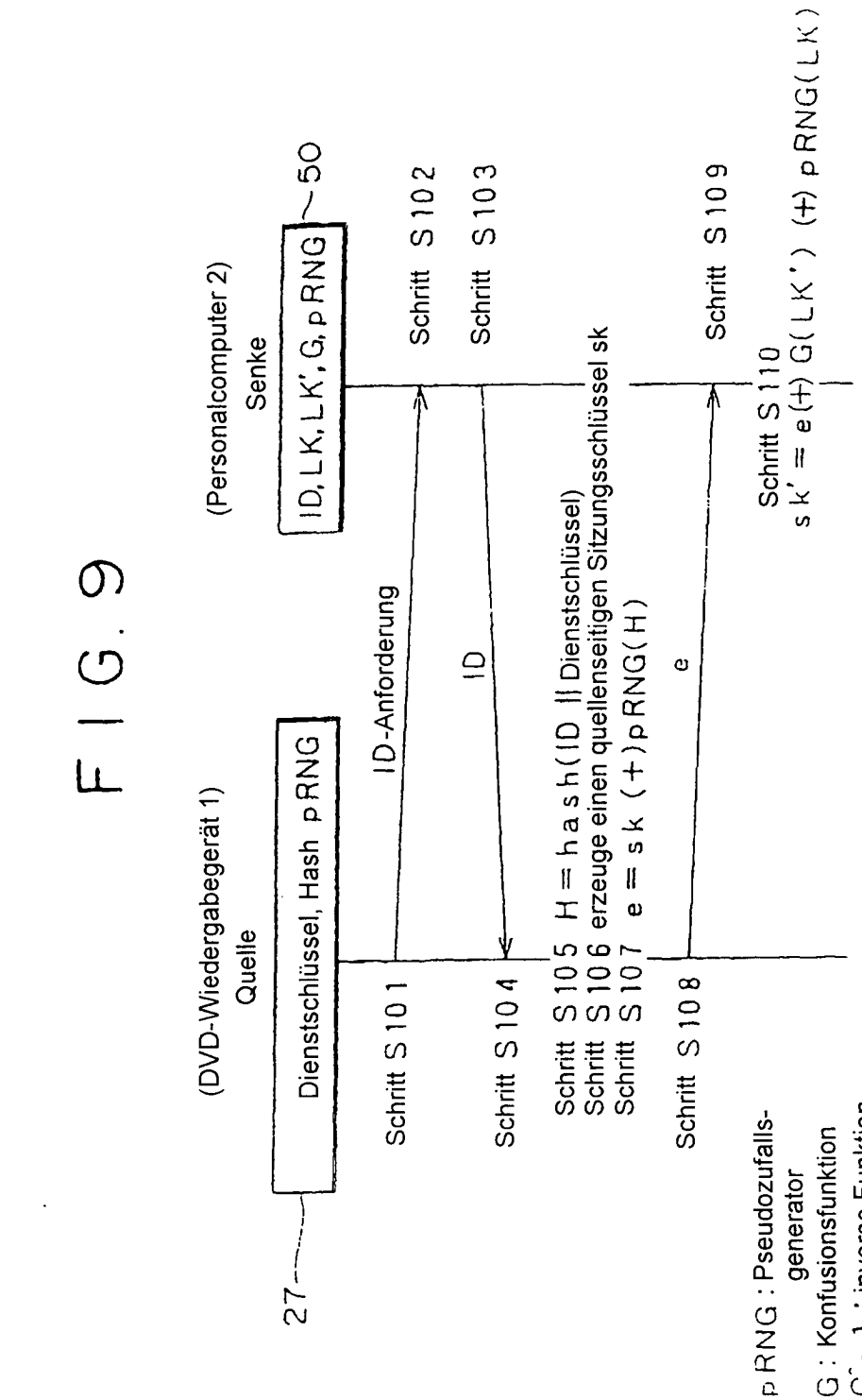

(DVD-Wiedergabegerät 1)
Quelle
Dienstschlüssel, Hash pRNG
27
(Personalcomputer 2)
Senke
ID, LK, LK', G, pRNG
50
Schritt S101
ID-Anforderung
Schritt S102
Schritt S103
ID
Schritt S104
Schritt S105 H = hash(ID || Dienstschlüssel)
Schritt S106 erzeuge einen quellenseitigen Sitzungsschlüssel sk
Schritt S107 e = sk (+) pRNG(H)
e
Schritt S108
Schritt S109
Schritt S110
sk' = e(+) G(LK') (+) pRNG(LK)
pRNG : Pseudozufalls-generator
G : Konfusionsfunktion
G^-1 : inverse Funktion von G
(+) : bitweise x or

FIG. 10

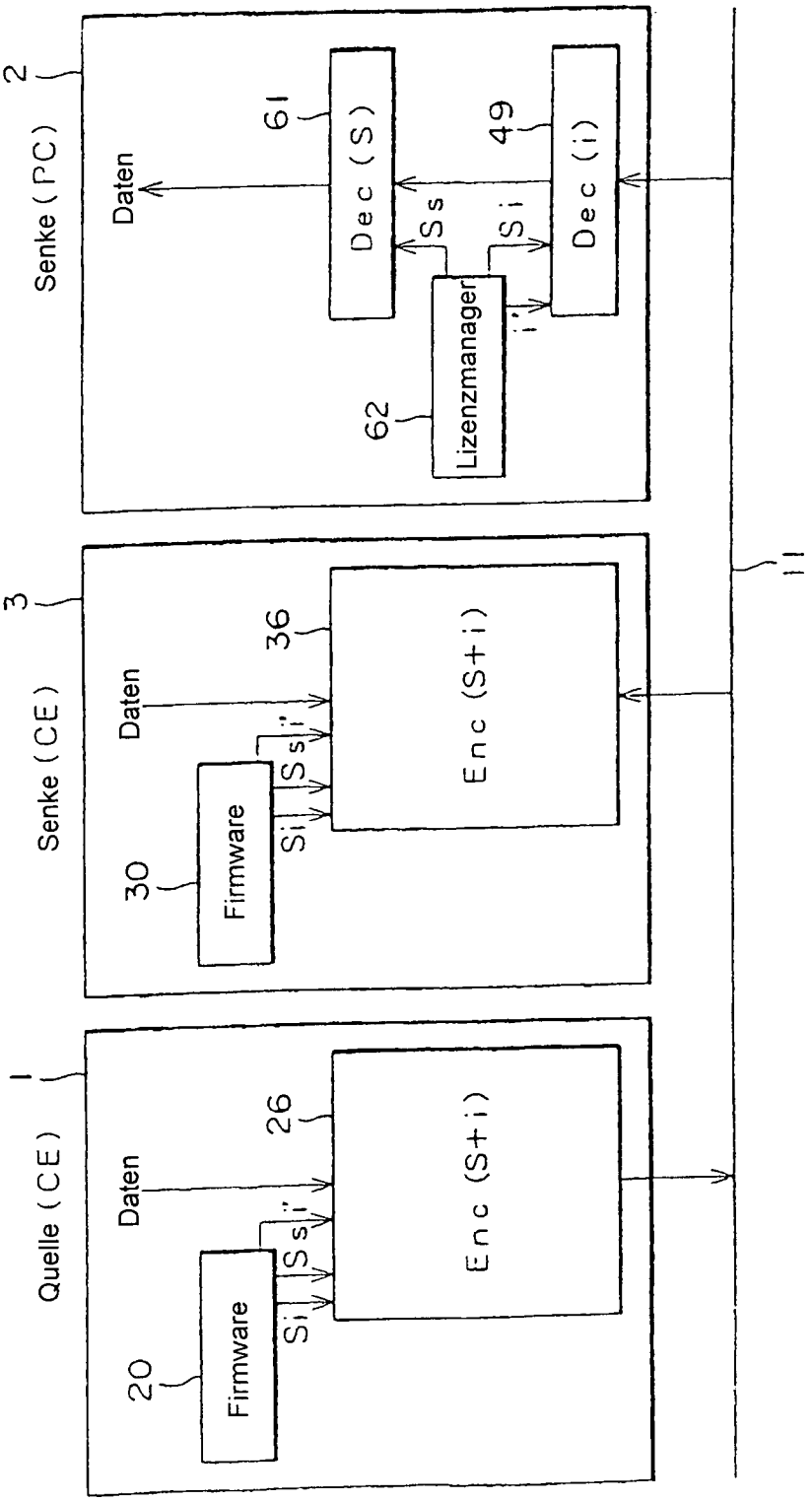

Quelle (CE)
1
Daten
26
Enc (S+i)
Ss
i'
Si
Firmware
20
Senke (CE)
3
Daten
36
Enc (S+i)
Ss
i'
Si
Firmware
30
Senke (PC)
2
Daten
61
Dec (S)
49
Dec (i)
Ss
Si
i'
Lizenzmanager
62
11

FIG. 11

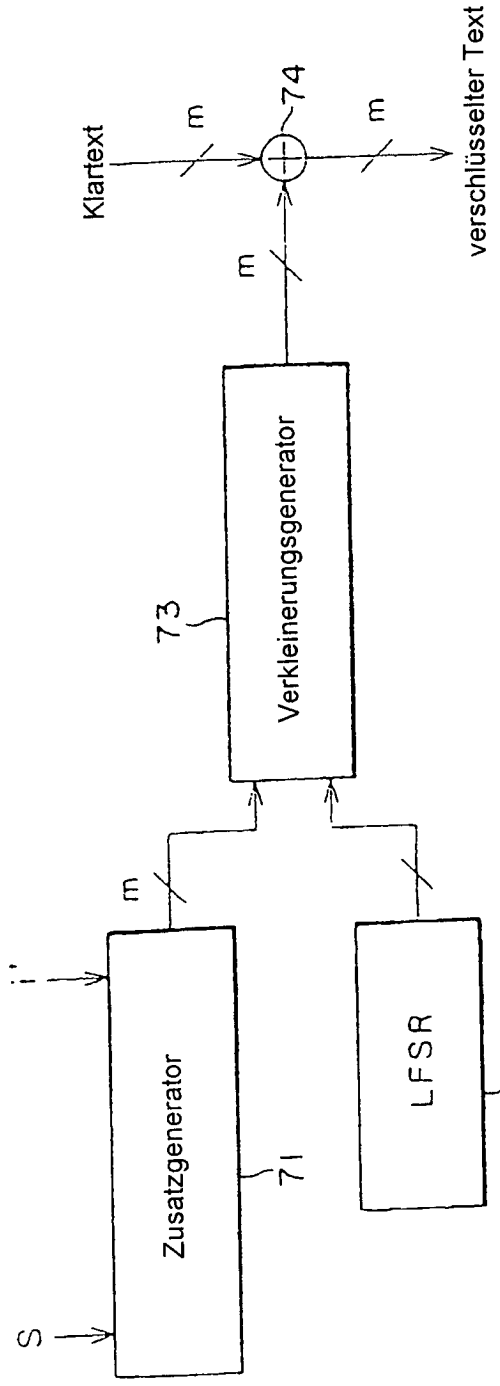

Klartext
m
74
m
verschlüsselter Text
m
Verkleinerungsgenerator
73
m
i
Zusatzgenerator
71
S
LFSR
72
26

FIG. 12

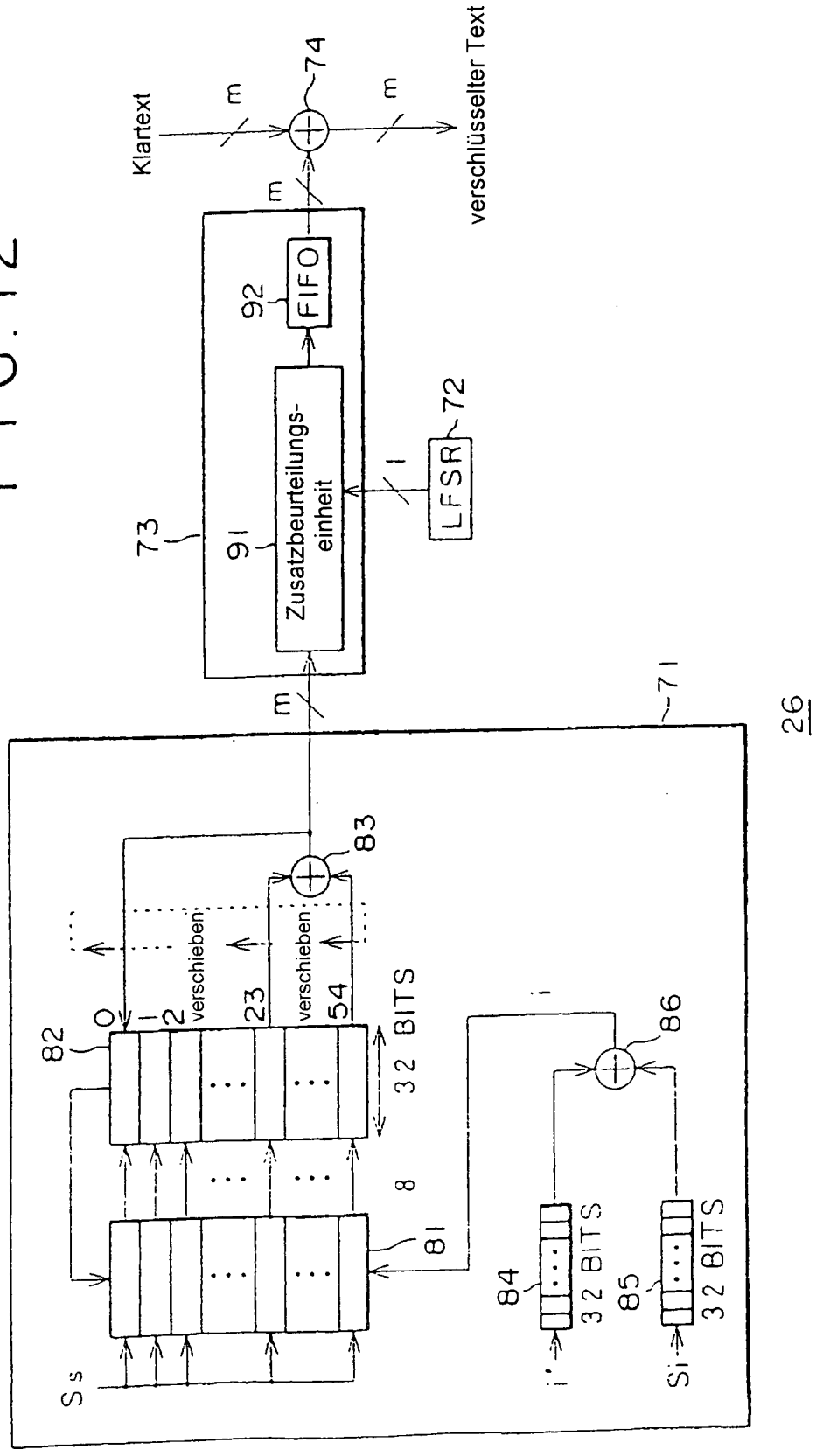
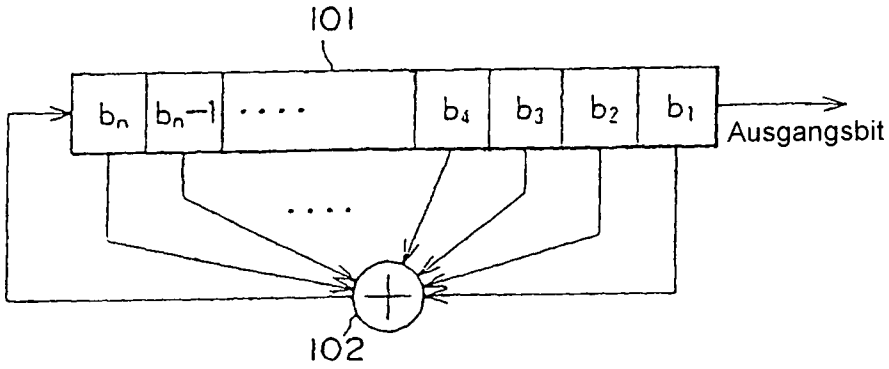
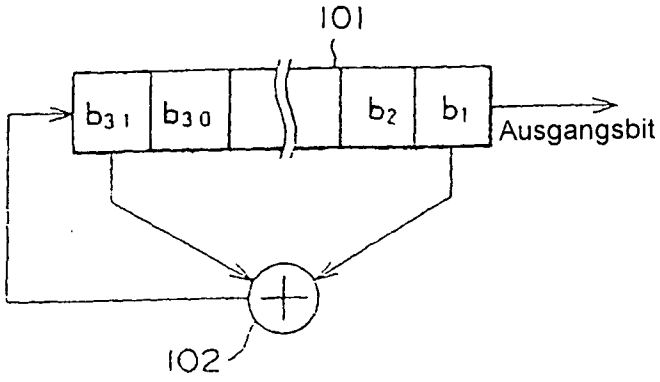

Klartext
m
74
m
verschlüsselter Text
m
92
FIFO
73
91
Zusatzbeurteilungs-
einheit
1
LFSR
72
m
71
26
83
verschieben
verschieben
0
1
2
23
54
82
32 BITS
8
81
i
86
84
32 BITS
85
32 BITS
Ss
i'
Si

FIG. 13



72

FIG. 14



72

FIG. 15

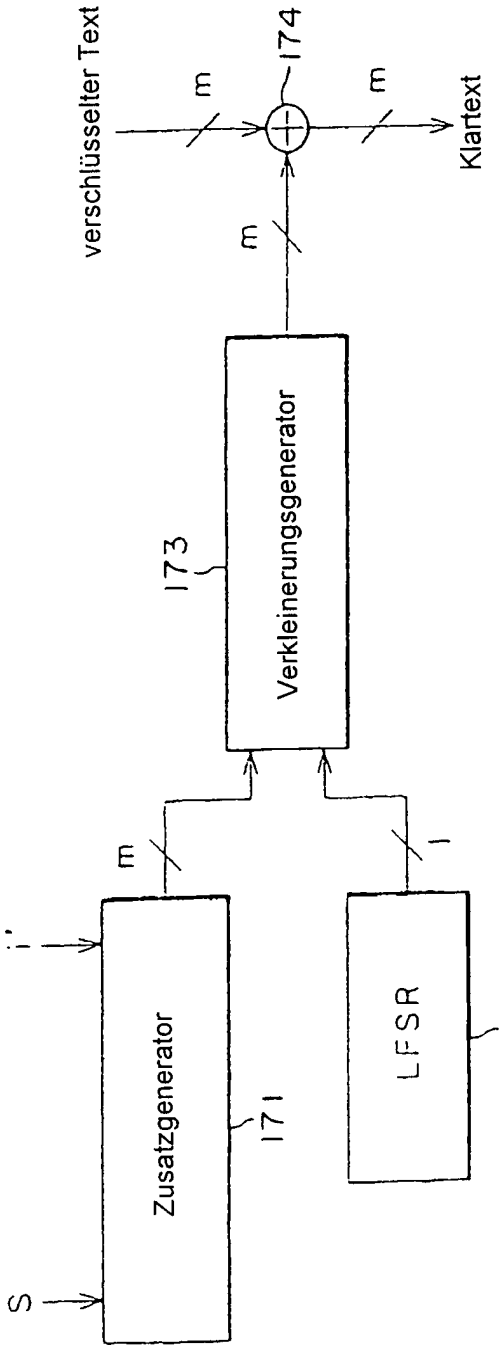

verschlüsselter Text
m
174
m
Klartext
m
Verkleinerungsgenerator
173
36
m
1
i
Zusatzgenerator
171
LFSR
172
s

FIG. 16

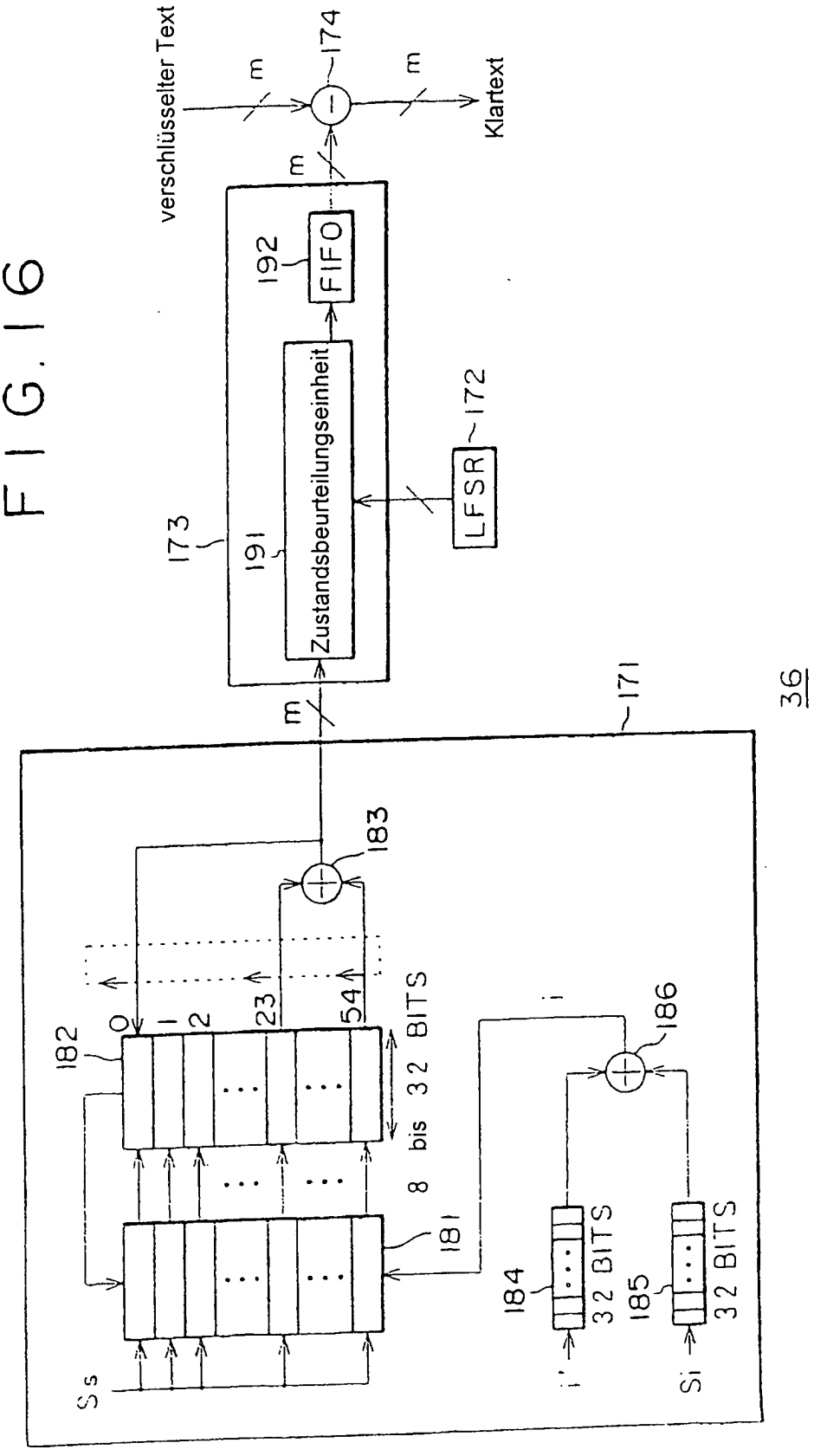
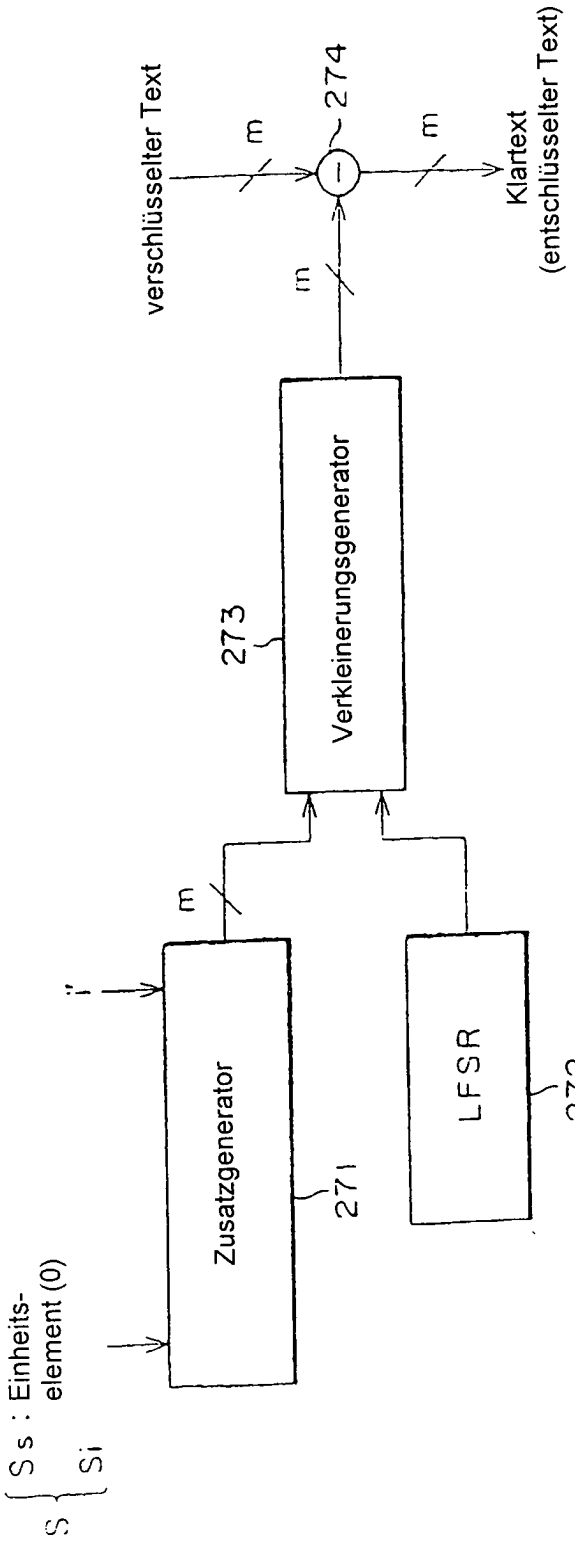

verschlüsselter Text
m
174
m
Klartext
m
192
FIFO
Zustandsbeurteilungseinheit
191
173
172
LFSR
m
171
36
183
0
1
2
23
54
182
8 bis 32 BITS
181
186
184
32 BITS
185
32 BITS
Ss
Si

FIG. 17


verschlüsselter Text
m
274
m
Klartext
(entschlüsselter Text)
m
273
Verkleinerungsgenerator
m
i
Zusatzgenerator
271
LFSR
272
Ss : Einheits-
element (0)
Si
S

49

FIG. 18

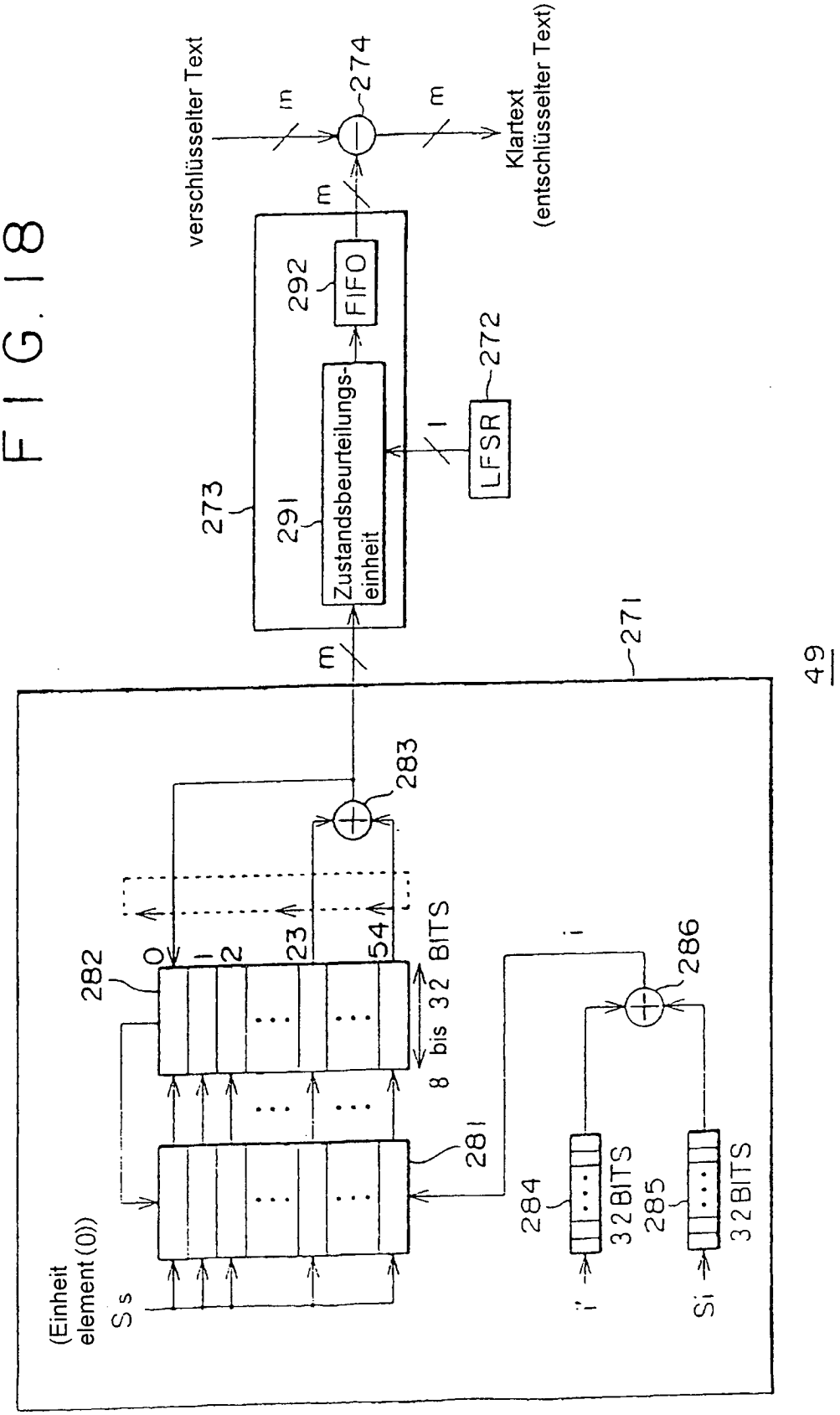

verschlüsselter Text
m
274
m
Klartext
(entschlüsselter Text)
m
292
FIFO
272
273
291
Zustandsbeurteilungs-
einheit
1
LFSR
m
271
49
283
282
0
1
2
23
54
8 bis 32 BITS
i
286
281
284
32BITS
285
32BITS
(Einheit
element (0))
Ss
i'
Si

FIG. 19

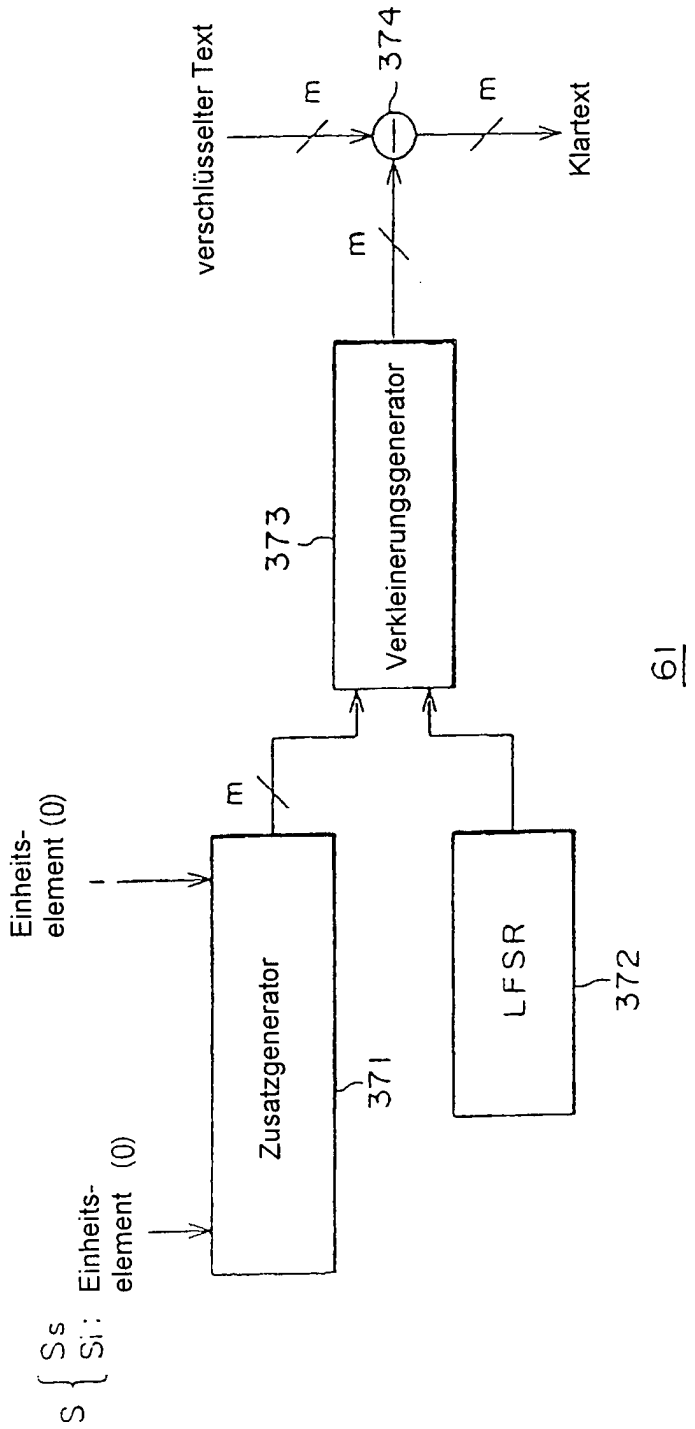

verschlüsselter Text
m
374
m
Klartext
m
373
Verkleinerungsgenerator
61
m
Einheits-
element (0)
1
Zusatzgenerator
371
LFSR
372
Einheits-
element (0)
S { Ss
Si :

FIG.20

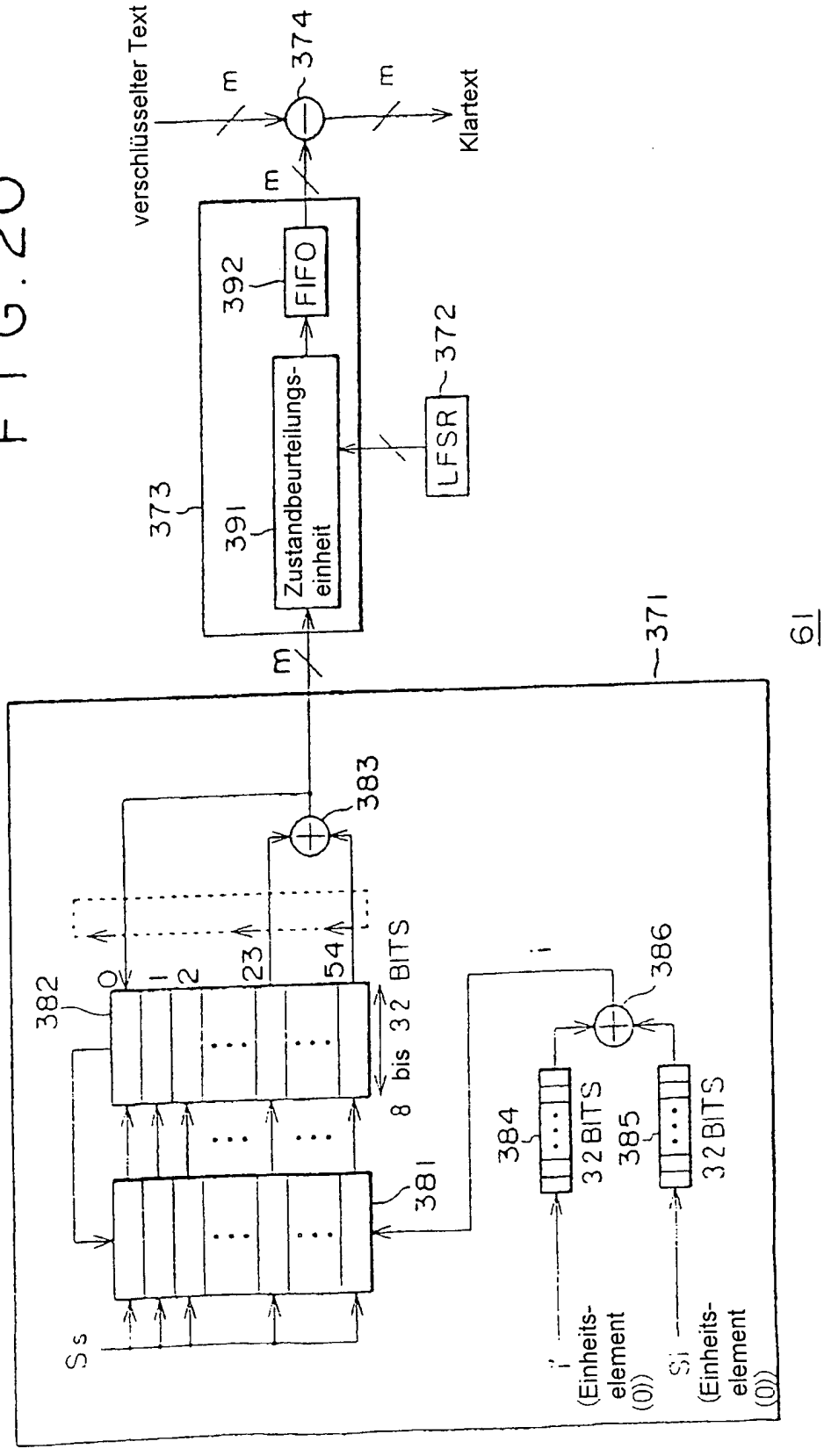

verschlüsselter Text
m
374
m
Klartext
m
392
FIFO
372
LFSR
373
391
Zustandbeurteilungs-einheit
m
371
61
383
382
0
1
2
23
54
8 bis 32 BITS
386
i
384
32 BITS
385
32 BITS
381
Ss
i'
(Einheits-element (0))
Si
(Einheits-element (0))

FIG. 21

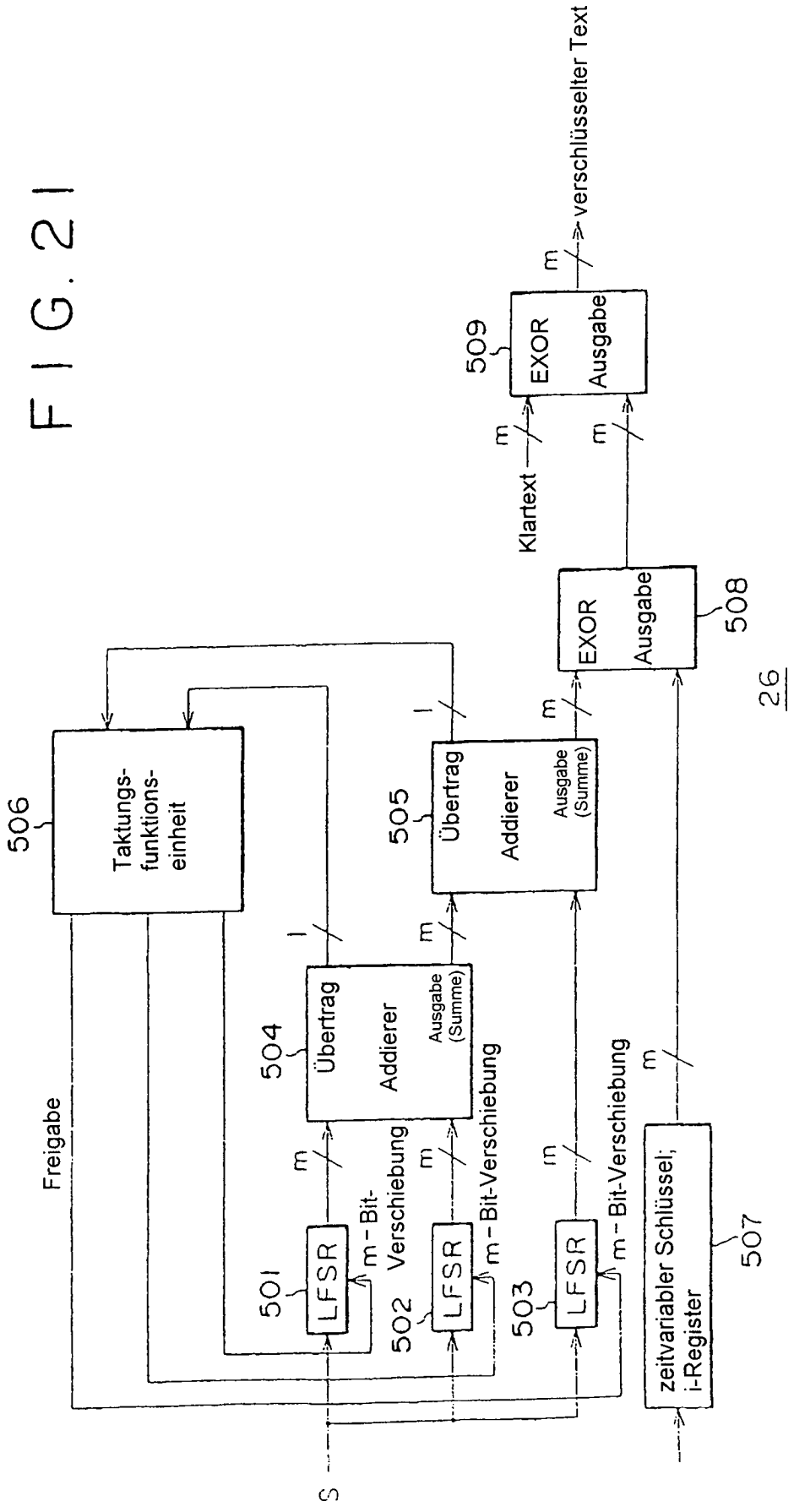

verschlüsselter Text
m
509
EXOR
Ausgabe
m
Klartext
m
m
EXOR
Ausgabe
508
26
506
Taktungs-funktions-einheit
505
Übertrag
Addierer
Ausgabe (Summe)
l
m
l
504
Übertrag
Addierer
Ausgabe (Summe)
Freigabe
m
m
m
501
LFSR
m-Bit-Verschiebung
502
LFSR
m-Bit-Verschiebung
503
LFSR
m-Bit-Verschiebung
m
zeitvariabler Schlüssel; i-Register
507
S

FIG. 22

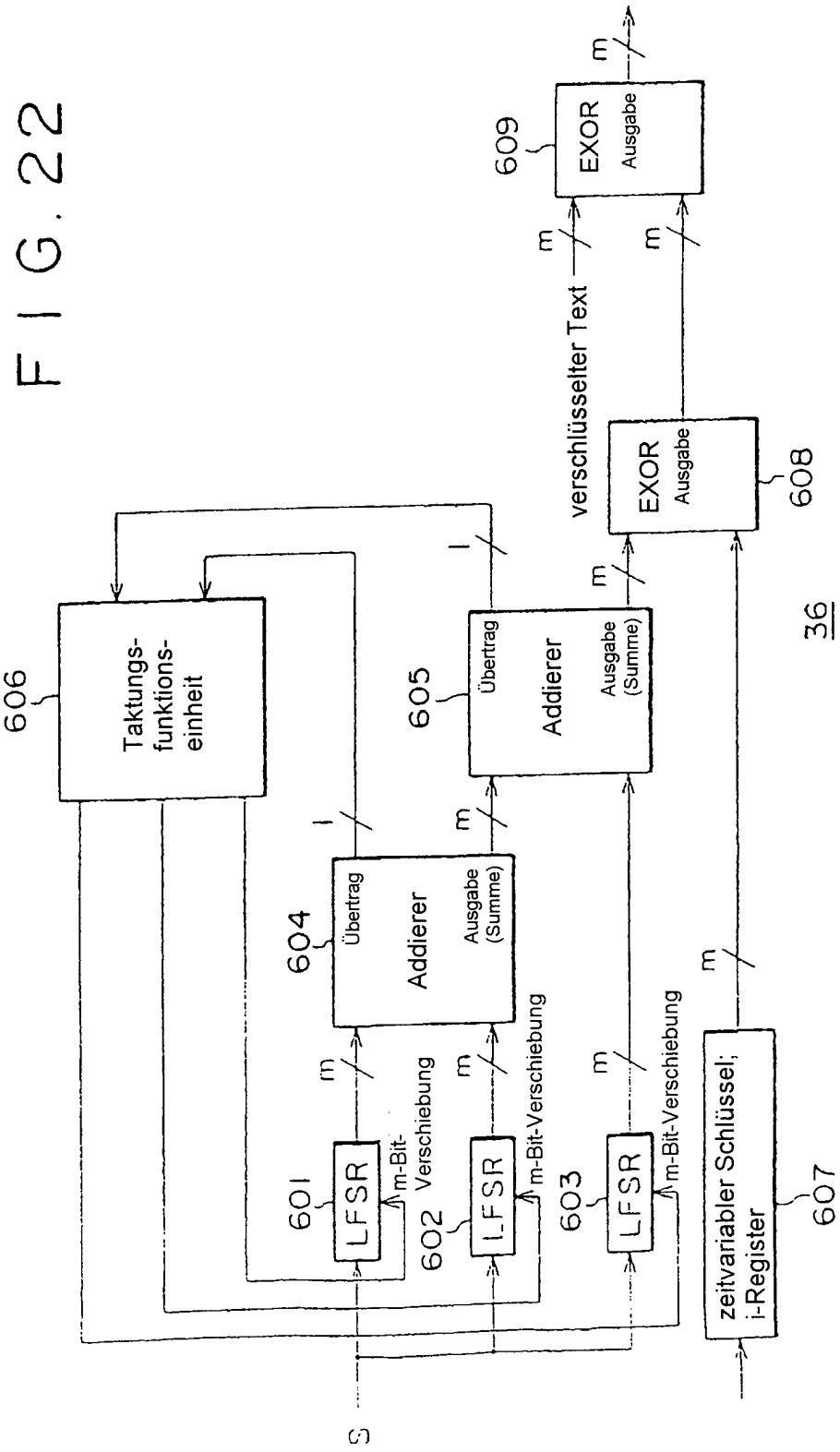

606
Taktungs-funktions-einheit
605
Addierer
Übertrag
Ausgabe (Summe)
604
Addierer
Übertrag
Ausgabe (Summe)
601
LFSR
602
LFSR
603
LFSR
m-Bit-Verschiebung
m-Bit-Verschiebung
m-Bit-Verschiebung
609
EXOR
Ausgabe
608
EXOR
Ausgabe
verschlüsselter Text
607
zeitvariabler Schlüssel; i-Register
36
S

FIG. 23

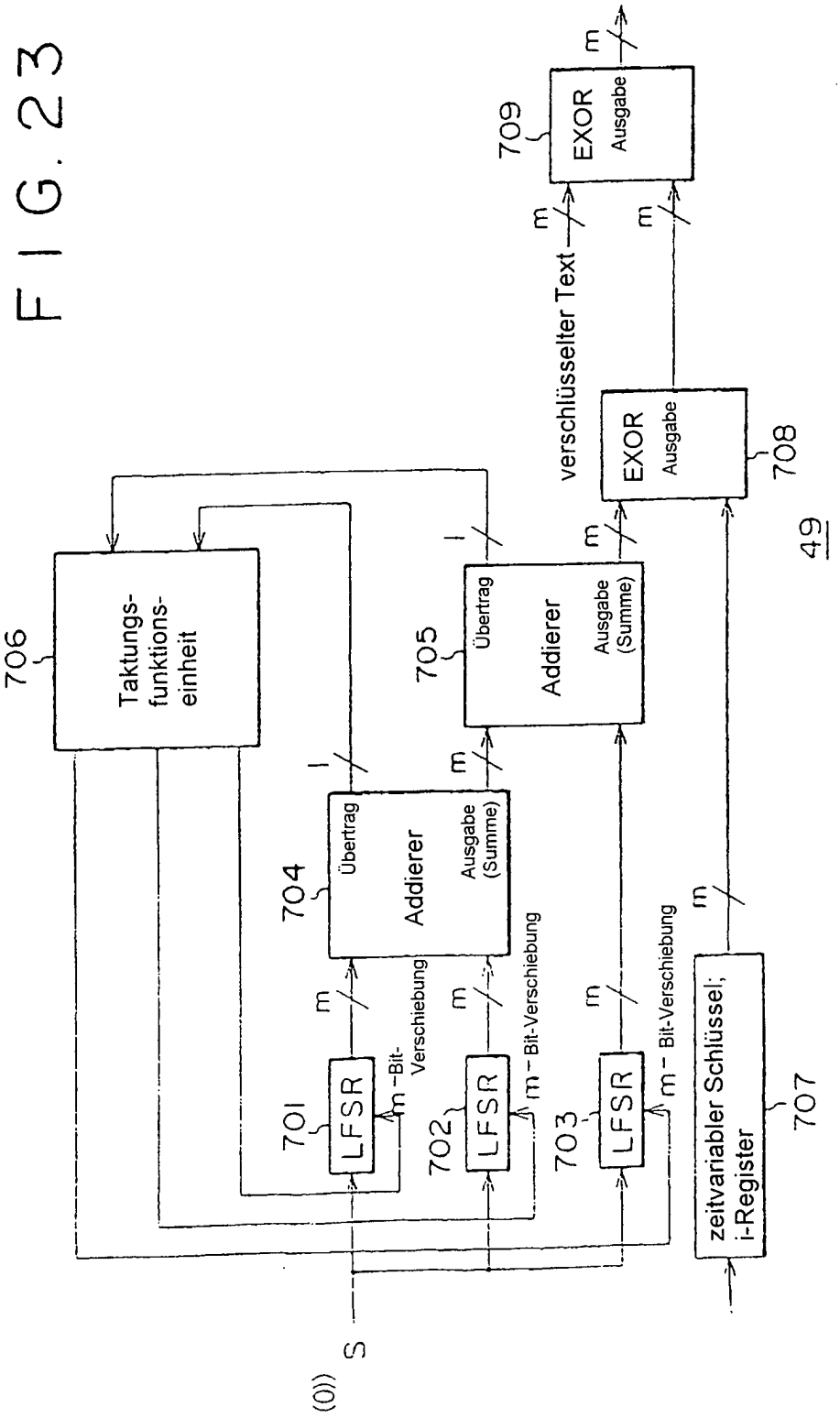

49
706
Taktungs-funktions-einheit
705
Addierer
Übertrag
Ausgabe (Summe)
704
Addierer
Übertrag
Ausgabe (Summe)
701
LFSR
702
LFSR
703
LFSR
m-Bit-Verschiebung
m-Bit-Verschiebung
m-Bit-Verschiebung
S
(0))
708
EXOR
Ausgabe
709
EXOR
Ausgabe
verschlüsselter Text
zeitvariabler Schlüssel; i-Register
707
m
l

FIG. 24

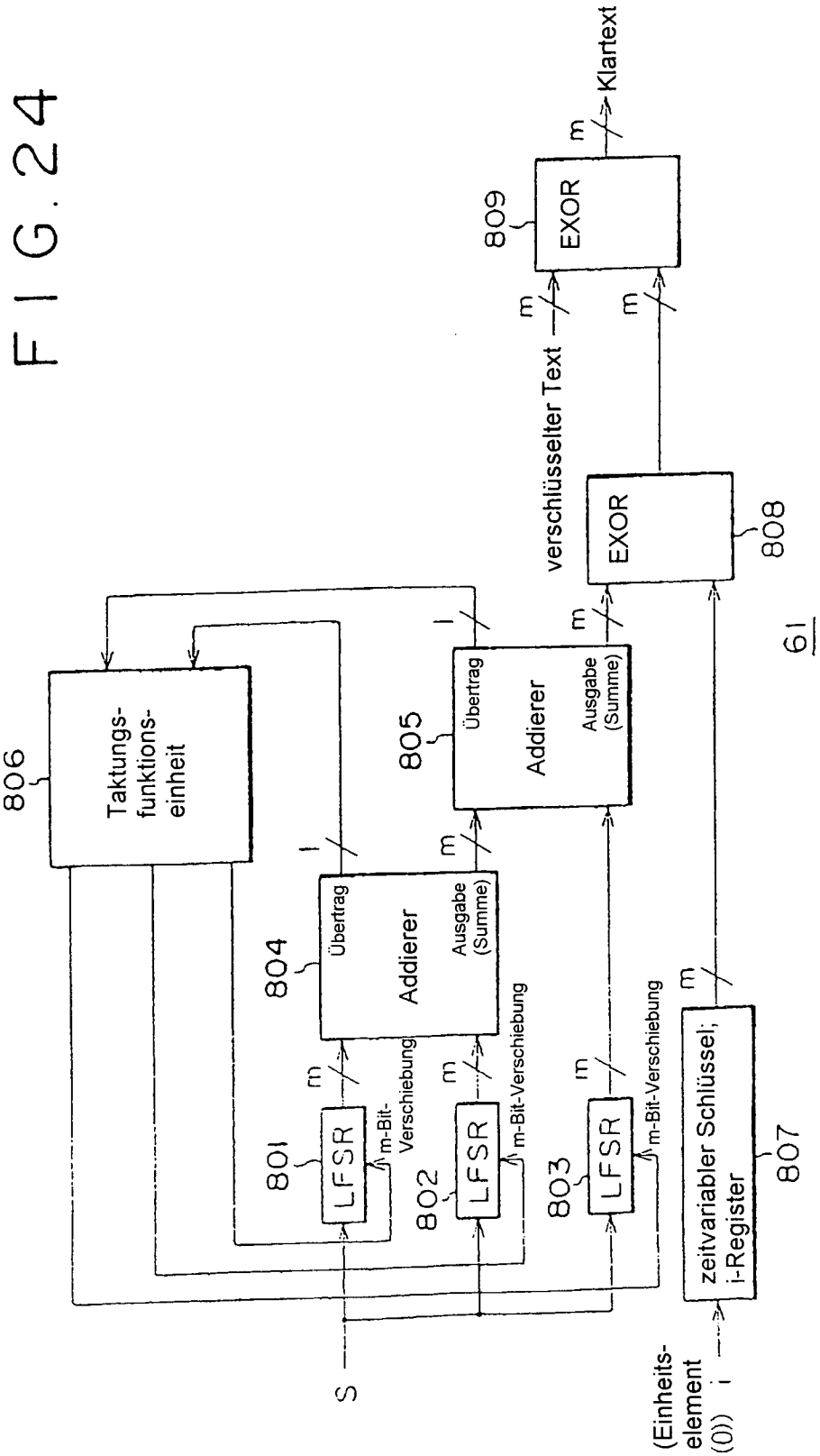

806
Taktungs-funktions-einheit
805
Addierer
Übertrag
Ausgabe (Summe)
804
Addierer
Übertrag
Ausgabe (Summe)
801
LFSR
802
LFSR
803
LFSR
m-Bit-Verschiebung
m-Bit-Verschiebung
m-Bit-Verschiebung
S
(Einheits-element (0)) i
zeitvariabler Schlüssel; i-Register
807
verschlüsselter Text
809
EXOR
Klartext
808
EXOR
61

FIG. 25

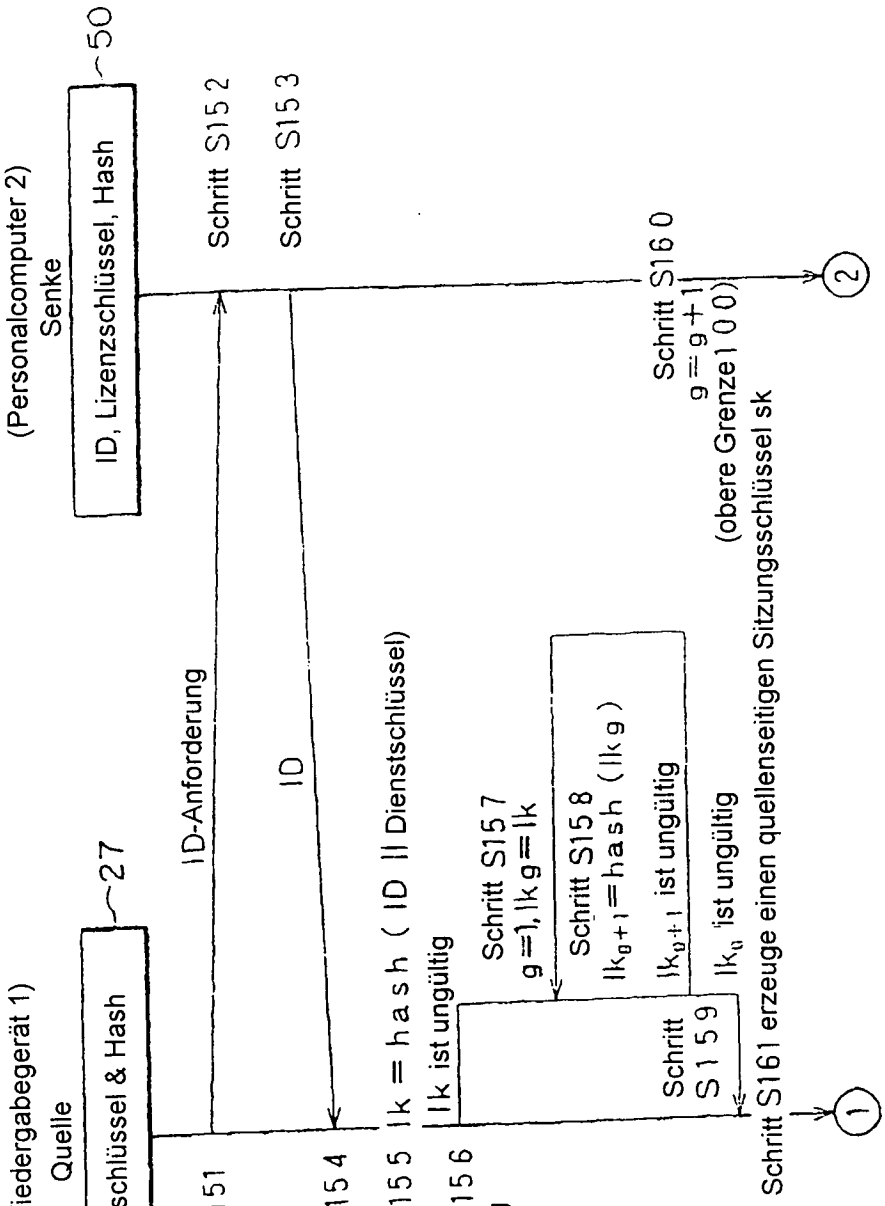

(DVD-Wiedergabegerät 1)
Quelle
Dienstschlüssel & Hash
27
(Personalcomputer 2)
Senke
ID, Lizenzschlüssel, Hash
50
SChritt S151
ID-Anforderung
Schritt S152
Schritt S153
ID
Schritt S154
Schritt S155
Ik = hash (ID || Dienstschlüssel)
Schritt S156
Ik ist gültig
Ik ist ungültig
Schritt S157
g=1, Ikg=Ik
Schritt S158
Ikg+1=hash (Ikg)
Ikg+1 ist ungültig
Schritt S159
Ik0 ist ungültig
Schritt S160
g=g+1
(obere Grenze 100)
Schritt S161 erzeuge einen quellenseitigen Sitzungsschlüssel sk
1
2

FIG. 26

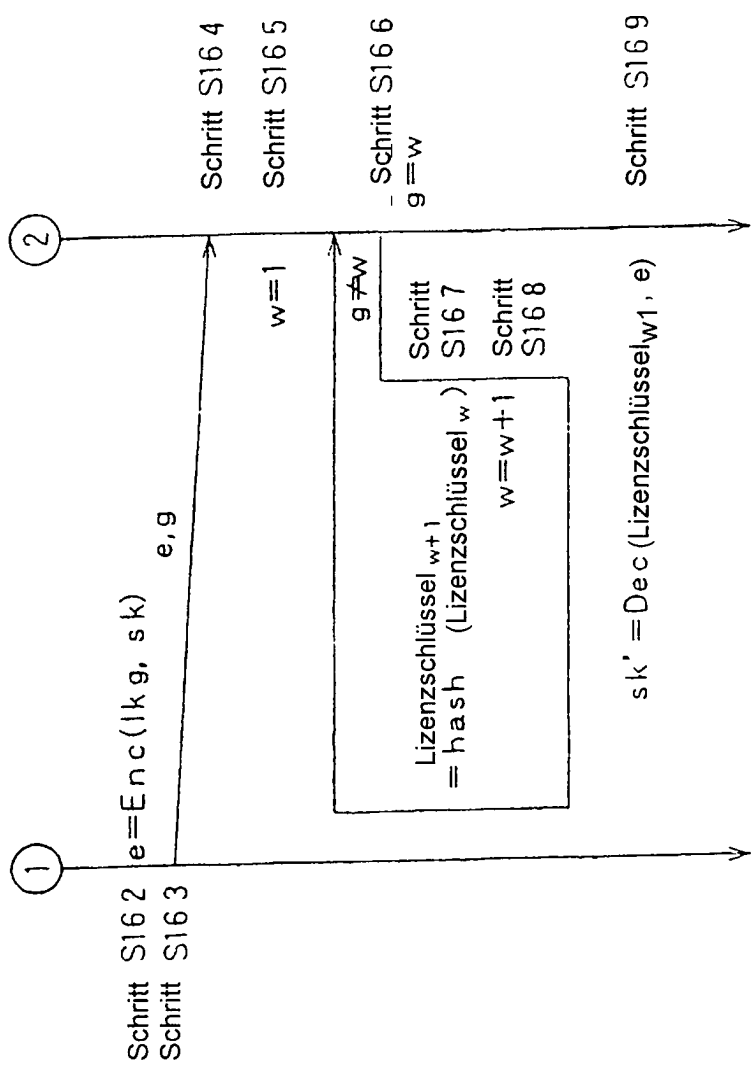

Schritt S162
Schritt S163
e=Enc(lkg, sk)
e, g
Schritt S164
Schritt S165
w=1
Schritt S166
g=w
g≠w
Schritt S167
Lizenzschlüssel w+1 = hash (Lizenzschlüssel w)
Schritt S168
w=w+1
Schritt S169
sk' = Dec (Lizenzschlüssel w1, e)
1
2

FIG. 27

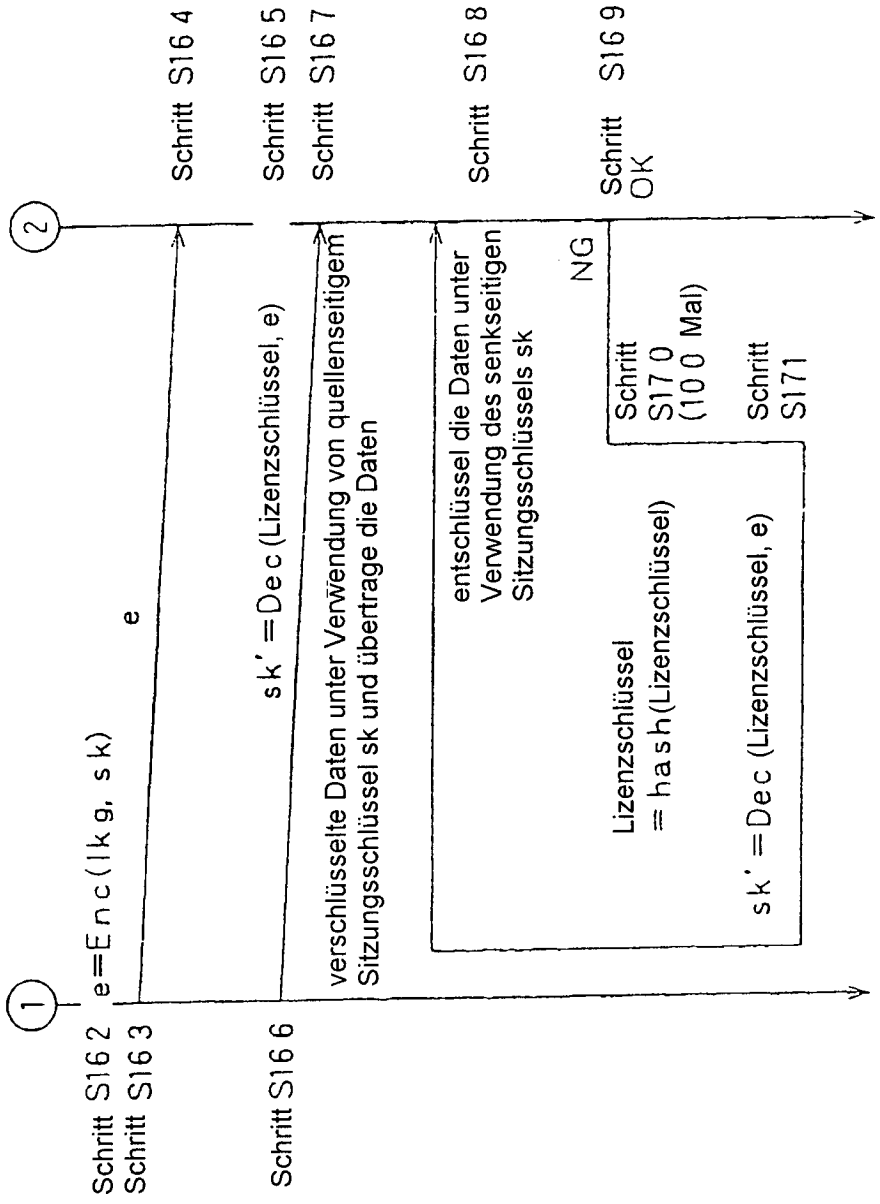

1
2
Schritt S162
Schritt S163
e=Enc(Ikg, sk)
e
Schritt S164
Schritt S165
sk'=Dec (Lizenzschlüssel, e)
Schritt S166
verschlüsselte Daten unter Verwendung von quellenseitigem Sitzungsschlüssel sk und übertrage die Daten
Schritt S167
entschlüssel die Daten unter Verwendung des senkseitigen Sitzungsschlüssels sk
Schritt S168
NG
Schritt S169
OK
Lizenzschlüssel = hash(Lizenzschlüssel)
Schritt S170 (100 Mal)
sk'=Dec (Lizenzschlüssel, e)
Schritt S171

FIG. 28

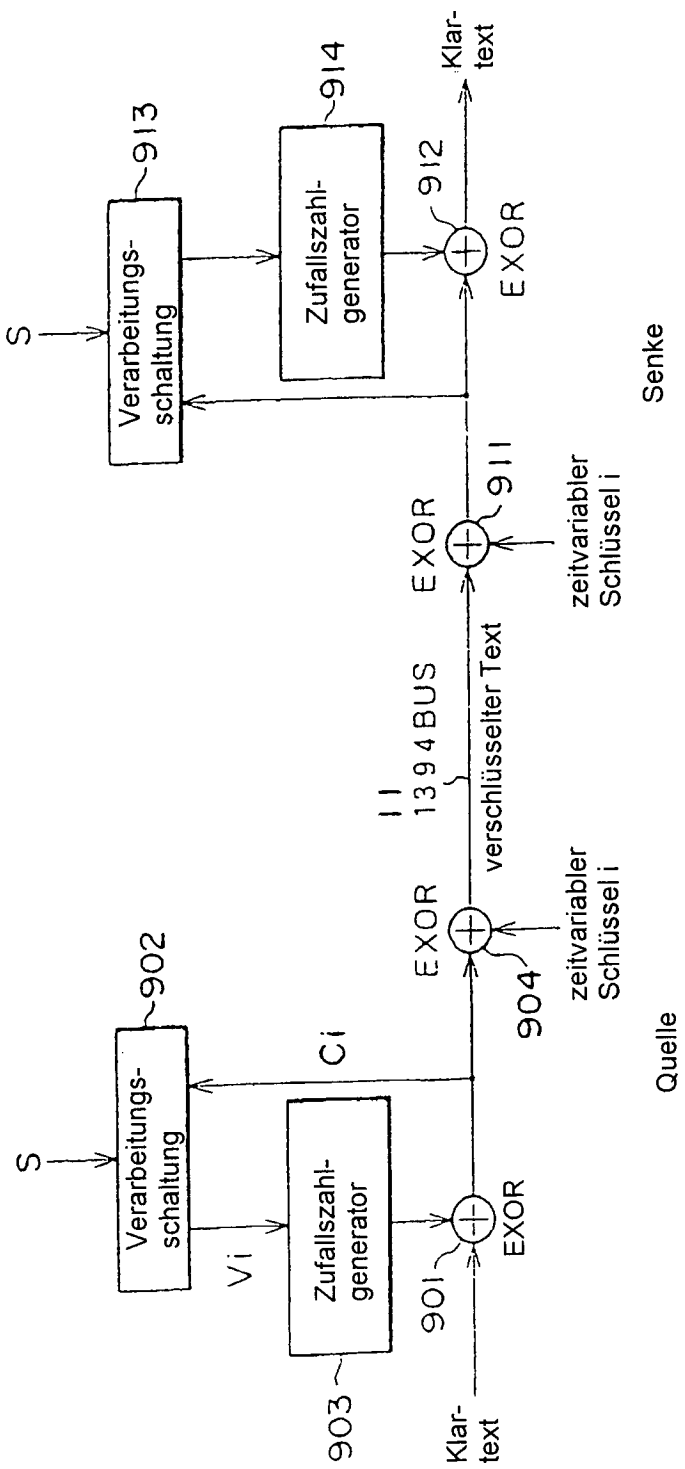

Quelle
Senke
S
Verarbeitungs-schaltung
902
Ci
Vi
Zufallszahl-generator
903
901
EXOR
Klar-text
904
zeitvariabler Schlüssel i
EXOR
11
1394 BUS
verschlüsselter Text
911
EXOR
zeitvariabler Schlüssel i
S
Verarbeitungs-schaltung
913
Zufallszahl-generator
914
912
EXOR
Klar-text

FIG. 29

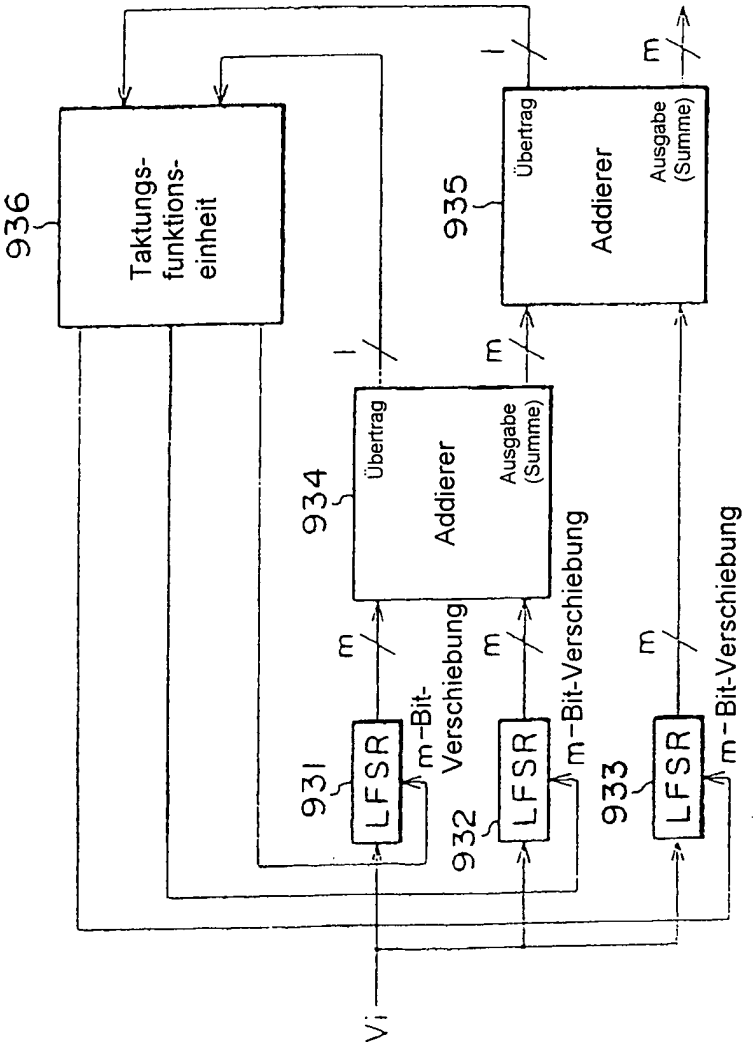

936
Taktungs-funktions-einheit
935
Addierer
Übertrag
Ausgabe (Summe)
934
Addierer
Übertrag
Ausgabe (Summe)
931
LFSR
m-Bit-Verschiebung
932
LFSR
m-Bit-Verschiebung
933
LFSR
m-Bit-Verschiebung
l
m
Vi

FIG. 30

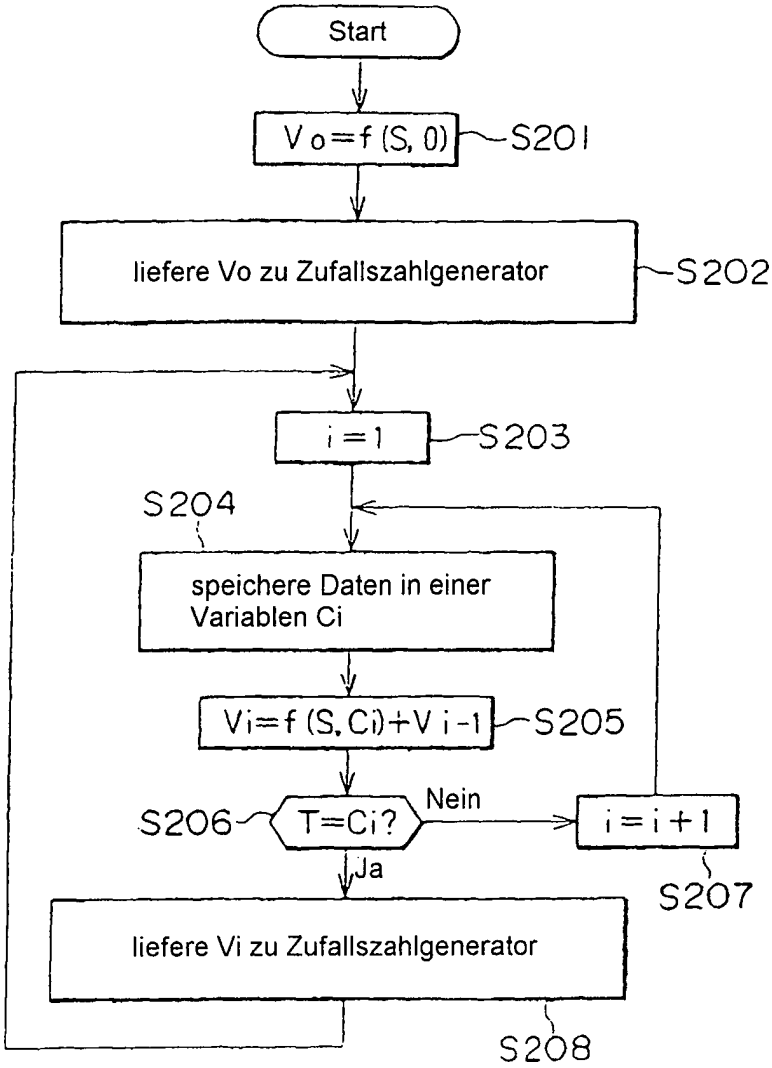

Start
Vo=f (S, 0)
S201
liefere Vo zu Zufallszahlgenerator
S202
i=1
S203
S204
speichere Daten in einer Variablen Ci
Vi=f (S, Ci)+V i-1
S205
S206
T=Ci?
Nein
i=i+1
S207
Ja
liefere Vi zu Zufallszahlgenerator
S208

FIG. 31

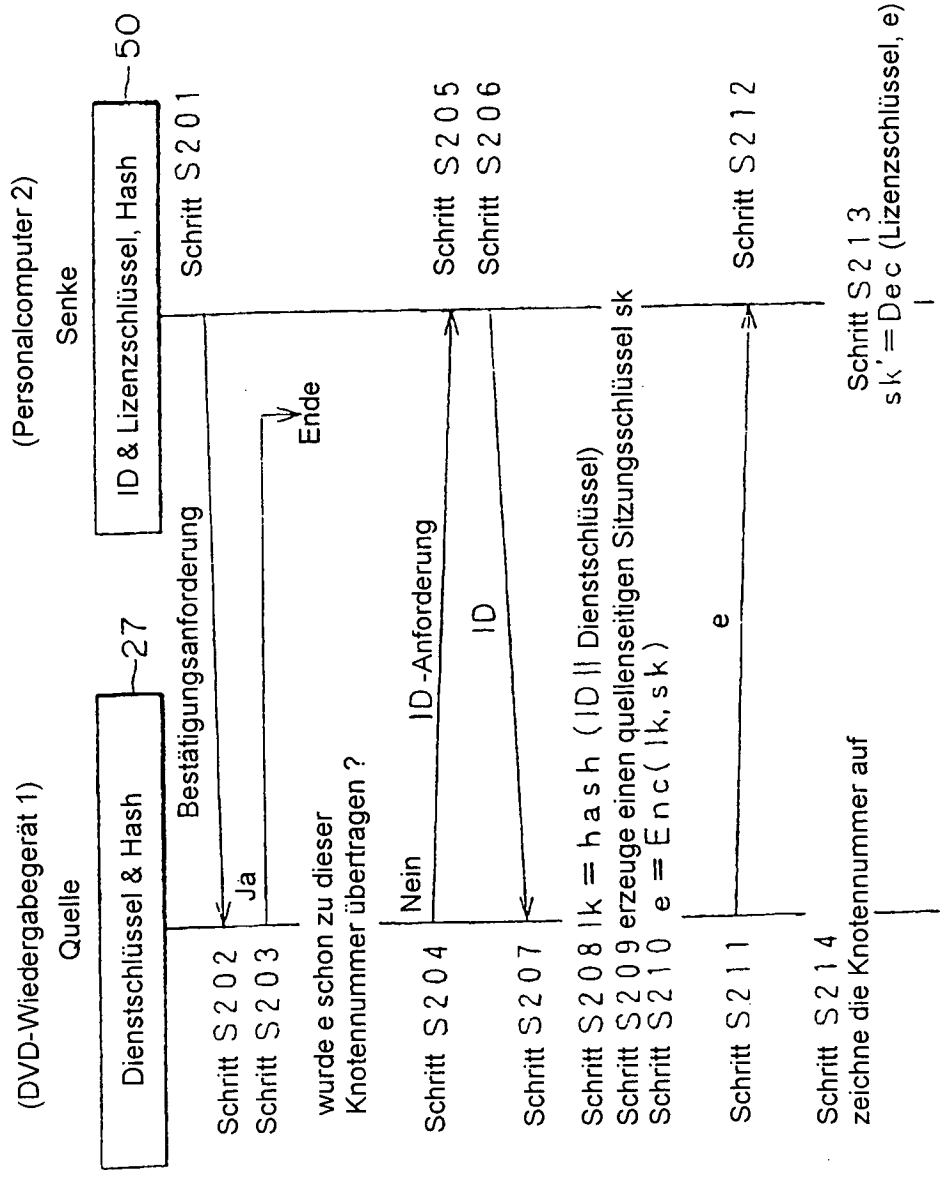

(DVD-Wiedergabegerät 1)
Quelle
Dienstschlüssel & Hash
27
(Personalcomputer 2)
Senke
ID & Lizenzschlüssel, Hash
50
Schritt S201
Bestätigungsanforderung
Schritt S202
Ja
Schritt S203
Ende
wurde e schon zu dieser Knotennummer übertragen ?
Schritt S204
Nein
ID-Anforderung
Schritt S205
Schritt S206
ID
Schritt S207
Schritt S208 Ik = hash (ID || Dienstschlüssel)
Schritt S209 erzeuge einen quellenseitigen Sitzungsschlüssel sk
Schritt S210 e = Enc(Ik, sk)
Schritt S211
e
Schritt S212
Schritt S213
sk' = Dec (Lizenzschlüssel, e)
Schritt S214
zeichne die Knotennummer auf

FIG. 32

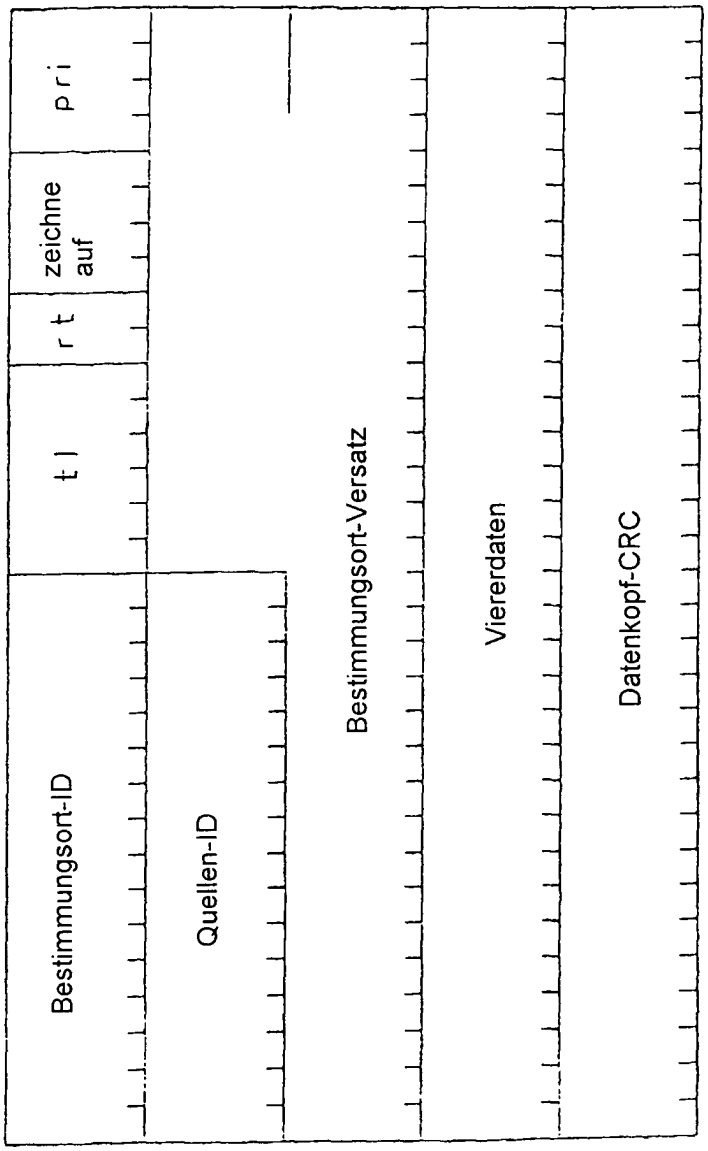

Bestimmungsort-ID
tl
rt
zeichne auf
pri
Quellen-ID
Bestimmungsort-Versatz
Viererdaten
Datenkopf-CRC

FIG. 33

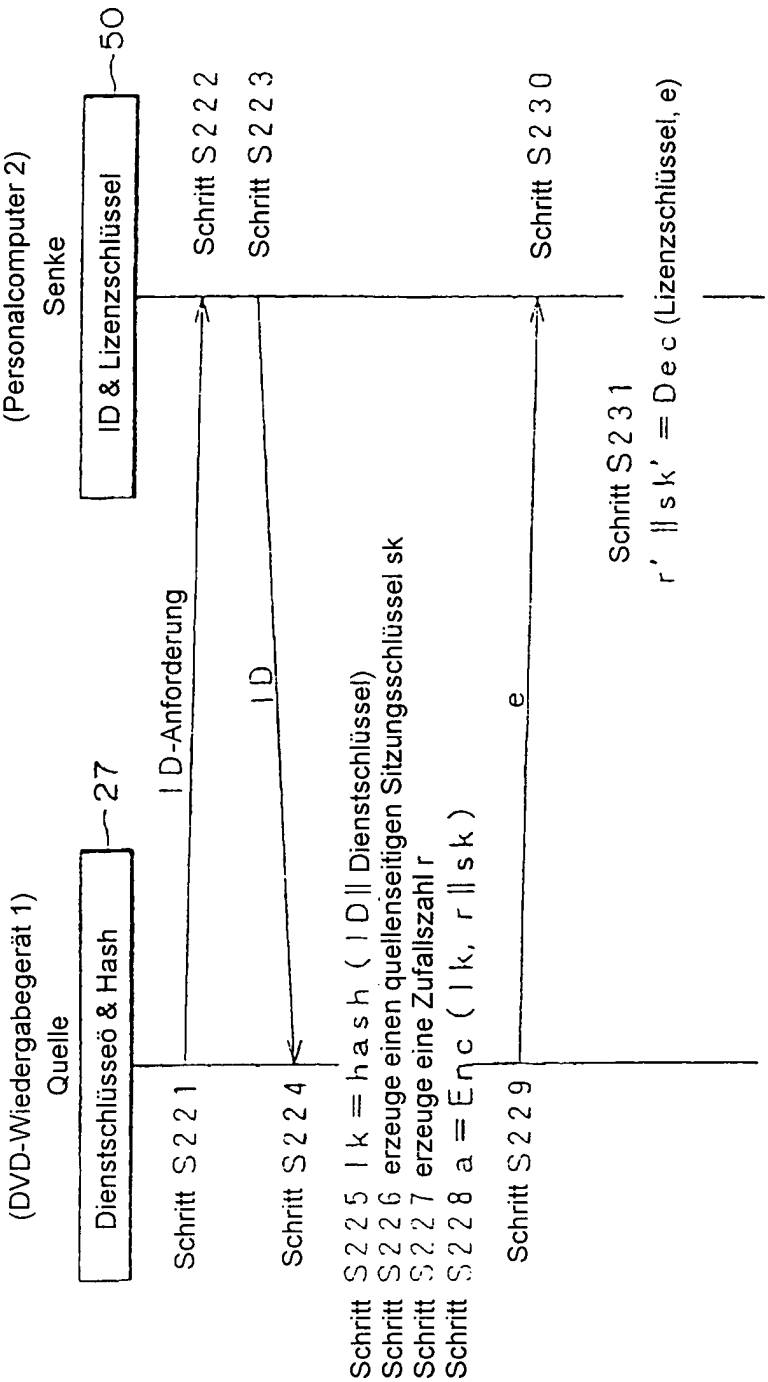

(DVD-Wiedergabegerät 1)
Quelle
Dienstschlüsseö & Hash
27
(Personalcomputer 2)
Senke
ID & Lizenzschlüssel
50
ID-Anforderung
Schritt S221
Schritt S222
ID
Schritt S223
Schritt S224
Schritt S225 Ik = hash (ID || Dienstschlüssel)
Schritt S226 erzeuge einen quellenseitigen Sitzungsschlüssel sk
Schritt S227 erzeuge eine Zufallszahl r
Schritt S228 a = Enc (Ik, r || sk)
e
Schritt S229
Schritt S230
Schritt S231
r' || sk' = Dec (Lizenzschlüssel, e)

FIG. 34

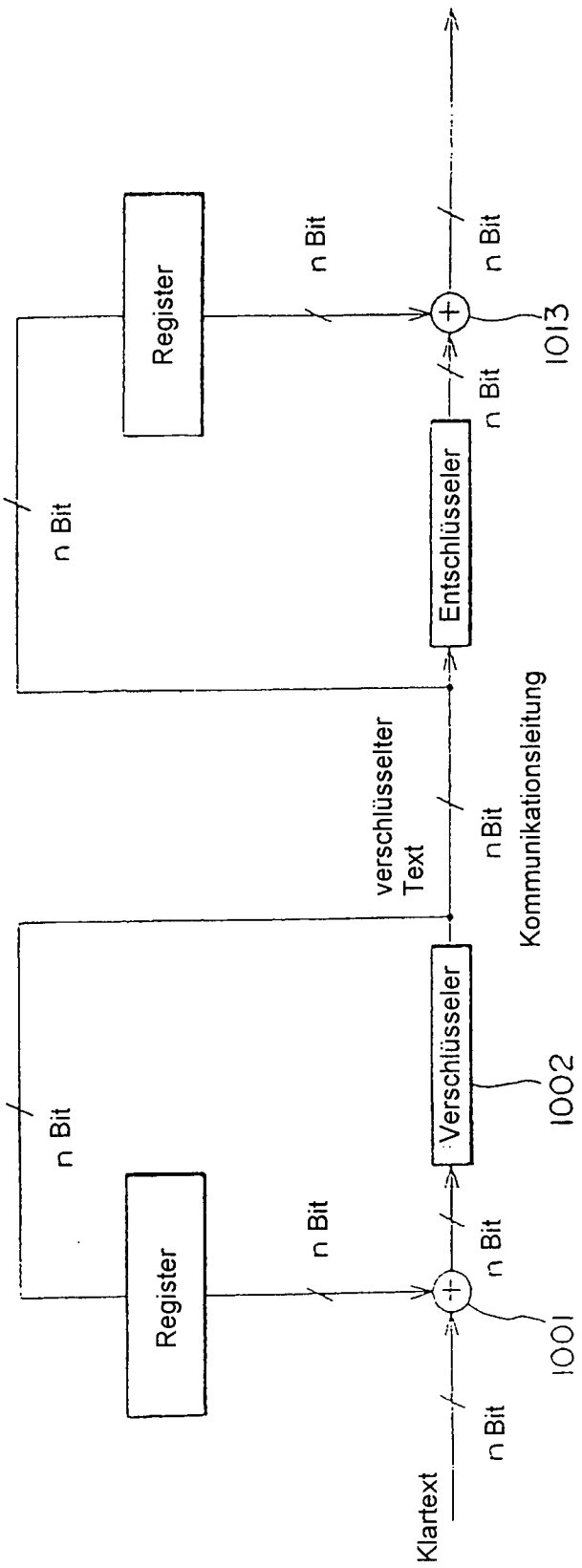

Register
n Bit
n Bit
1013
n Bit
Entschlüsseler
n Bit
n Bit
verschlüsselter Text
n Bit
Kommunikationsleitung
Verschlüsseler
1002
n Bit
Register
n Bit
n Bit
1001
n Bit
Klartext

FIG. 35

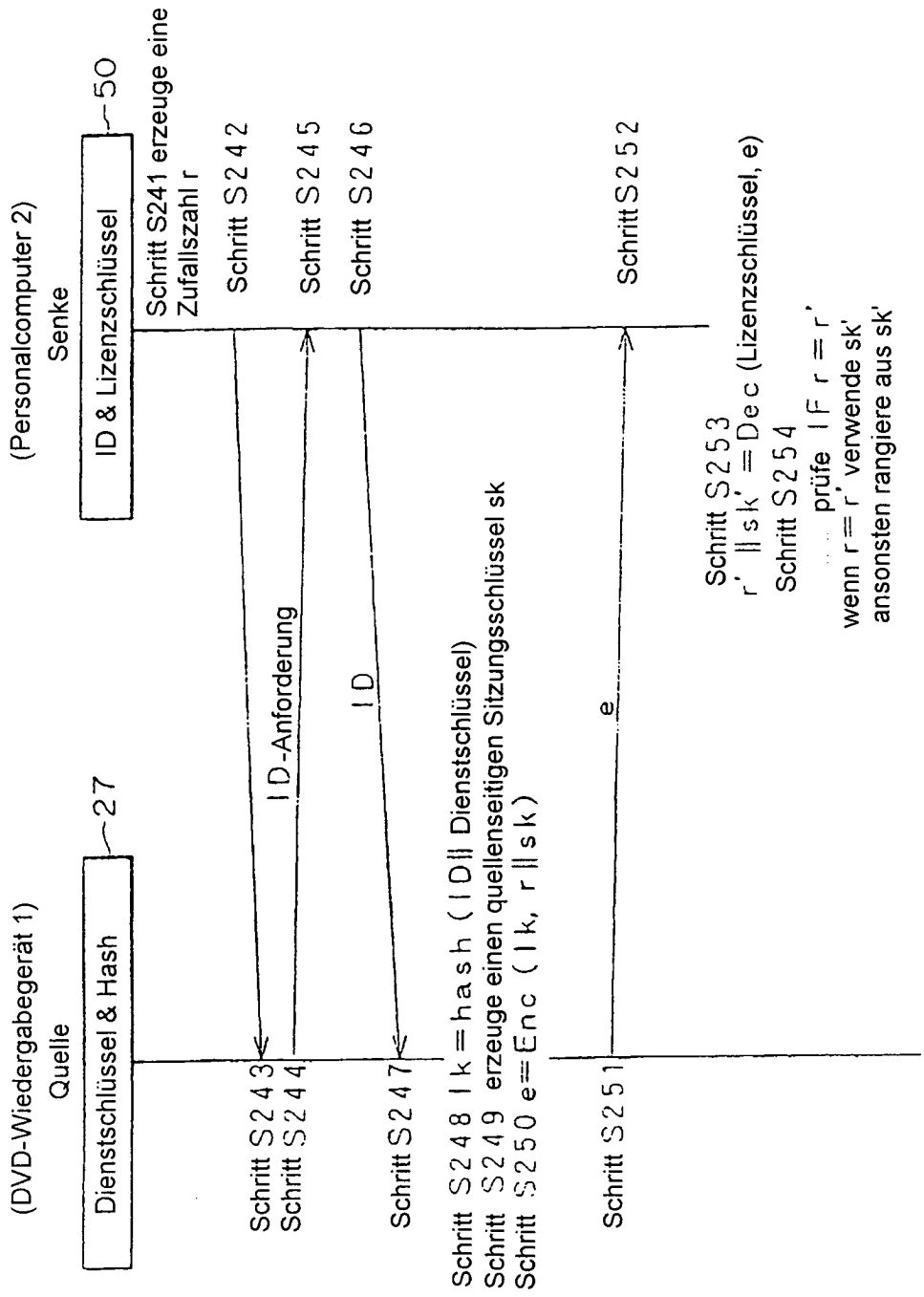

(DVD-Wiedergabegerät 1)
Quelle
Dienstschlüssel & Hash
27
(Personalcomputer 2)
Senke
ID & Lizenzschlüssel
50
Schritt S241 erzeuge eine Zufallszahl r
Schritt S242
Schritt S243
Schritt S244
ID-Anforderung
Schritt S245
Schritt S246
ID
Schritt S247
Schritt S248 Ik=hash (ID|| Dienstschlüssel)
Schritt S249 erzeuge einen quellenseitigen Sitzungsschlüssel sk
Schritt S250 e=Enc (Ik, r||sk)
Schritt S251
e
Schritt S252
Schritt S253
r'||sk'=Dec (Lizenzschlüssel, e)
Schritt S254
prüfe IF r=r'
wenn r=r' verwende sk'
ansonsten rangiere aus sk'

FIG. 36

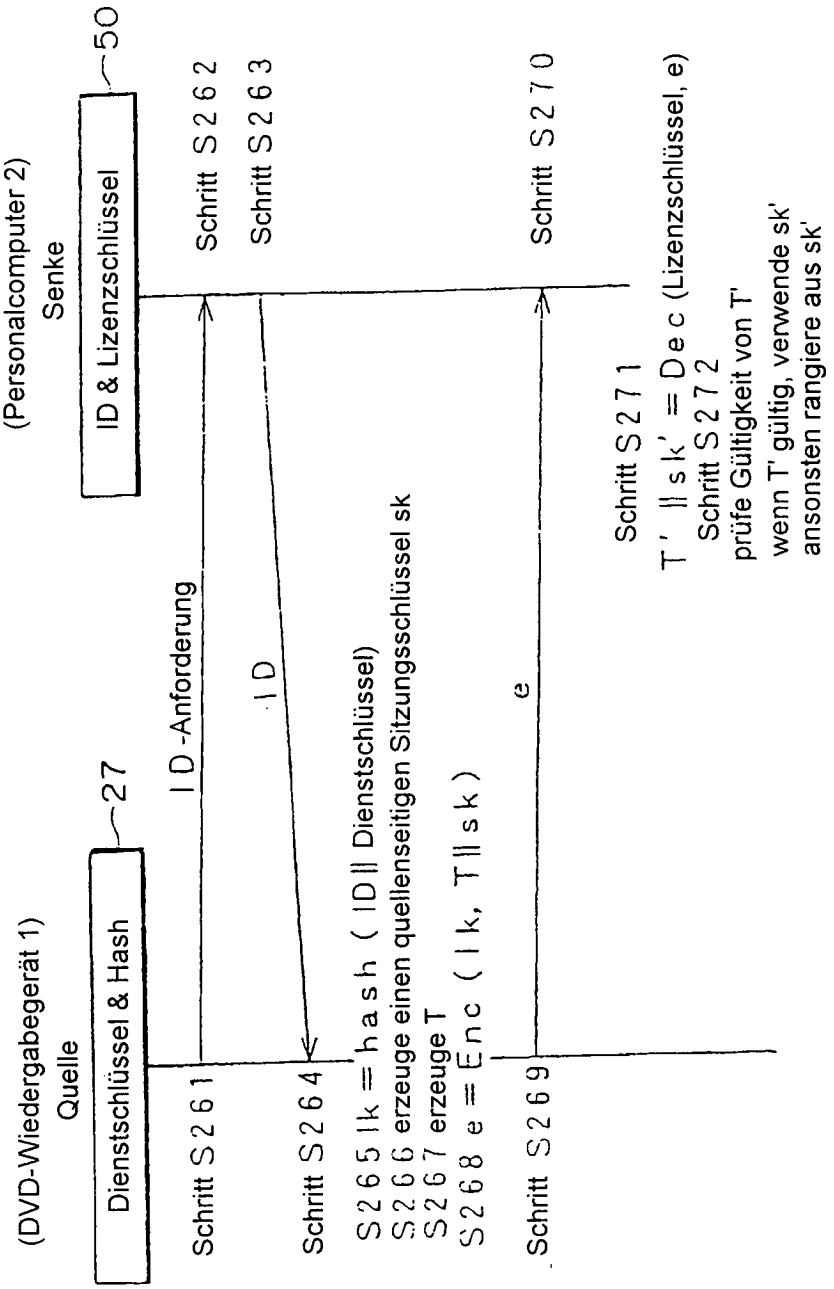

(DVD-Wiedergabegerät 1)
Quelle
Dienstschlüssel & Hash
27
(Personalcomputer 2)
Senke
ID & Lizenzschlüssel
50
ID-Anforderung
Schritt S261
Schritt S262
Schritt S263
ID
Schritt S264
S265 Ik = hash (ID|| Dienstschlüssel)
S266 erzeuge einen quellenseitigen Sitzungsschlüssel sk
S267 erzeuge T
S268 e = Enc (Ik, T|| sk)
e
Schritt S269
Schritt S270
Schritt S271
T' || sk' = Dec (Lizenzschlüssel, e)
Schritt S272
prüfe Gültigkeit von T'
wenn T' gültig, verwende sk'
ansonsten rangiere aus sk'

FIG. 37

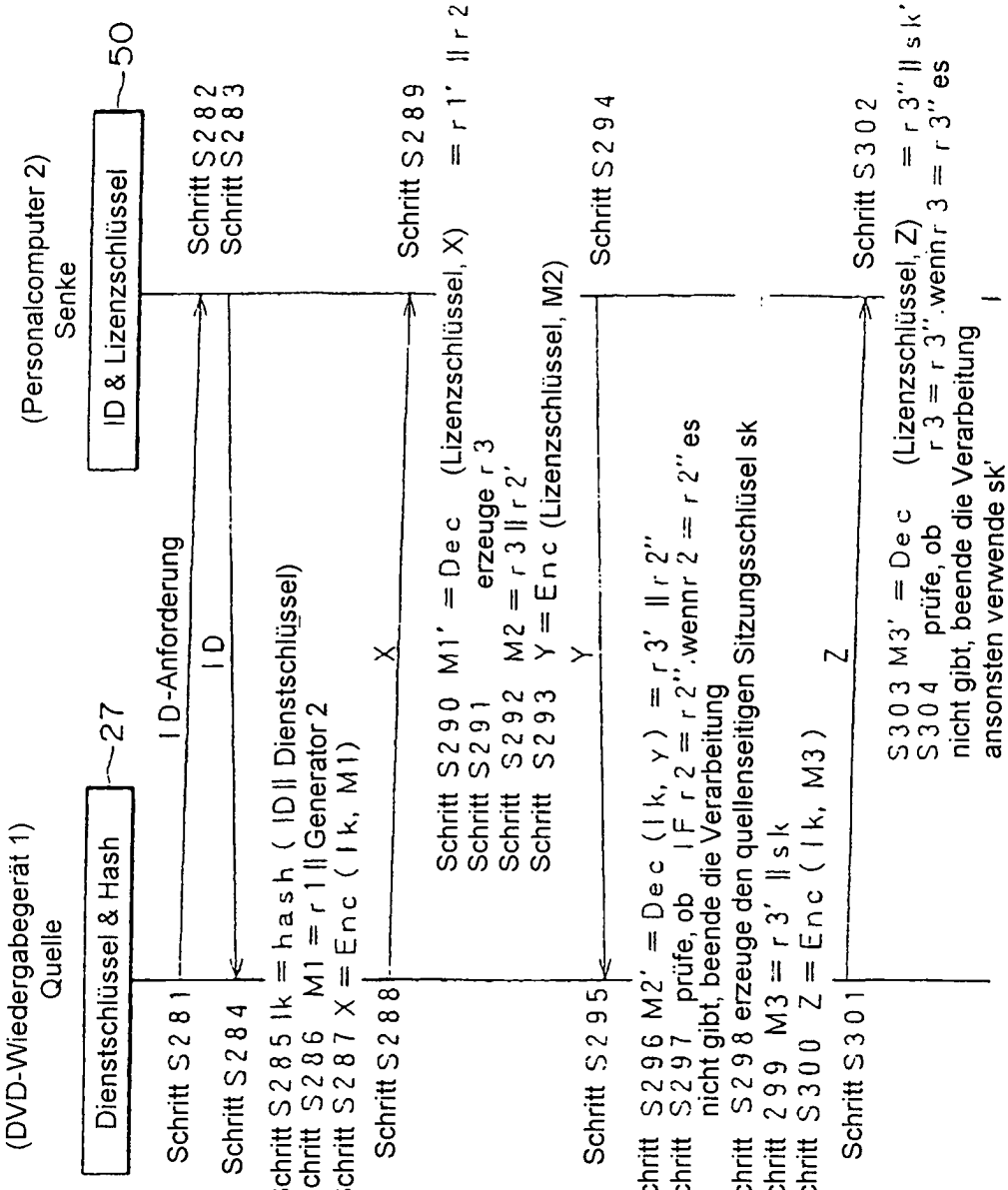

(DVD-Wiedergabegerät 1)
Quelle
Dienstschlüssel & Hash
~27
(Personalcomputer 2)
Senke
ID & Lizenzschlüssel
~50
Schritt S281
ID-Anforderung
Schritt S282
Schritt S283
ID
Schritt S284
Schritt S285 Ik = hash (IDII Dienstschlüssel)
Schritt S286 M1 = r1 II Generator2
Schritt S287 X = Enc (Ik, M1)
X
Schritt S288
Schritt S289
Schritt S290 M1' = Dec (Lizenzschlüssel, X) = r1' II r2'
Schritt S291 erzeuge r3
Schritt S292 M2 = r3 II r2'
Schritt S293 Y = Enc (Lizenzschlüssel, M2)
Y
Schritt S294
Schritt S295
Schritt S296 M2' = Dec (Ik, y) = r3' II r2''
Schritt S297 prüfe, ob IF r2 = r2''.wennr2 = r2'' es
nicht gibt, beende die Verarbeitung
Schritt S298 erzeuge den quellenseitigen Sitzungsschlüssel sk
Schritt 299 M3 = r3' II sk
Schritt S300 Z = Enc (Ik, M3)
Z
Schritt S301
Schritt S302
S303 M3' = Dec (Lizenzschlüssel, Z) = r3'' II sk'
S304 prüfe, ob r3 = r3''.wennr3 = r3'' es
nicht gibt, beende die Verarbeitung
ansonsten verwende sk'

FIG. 38

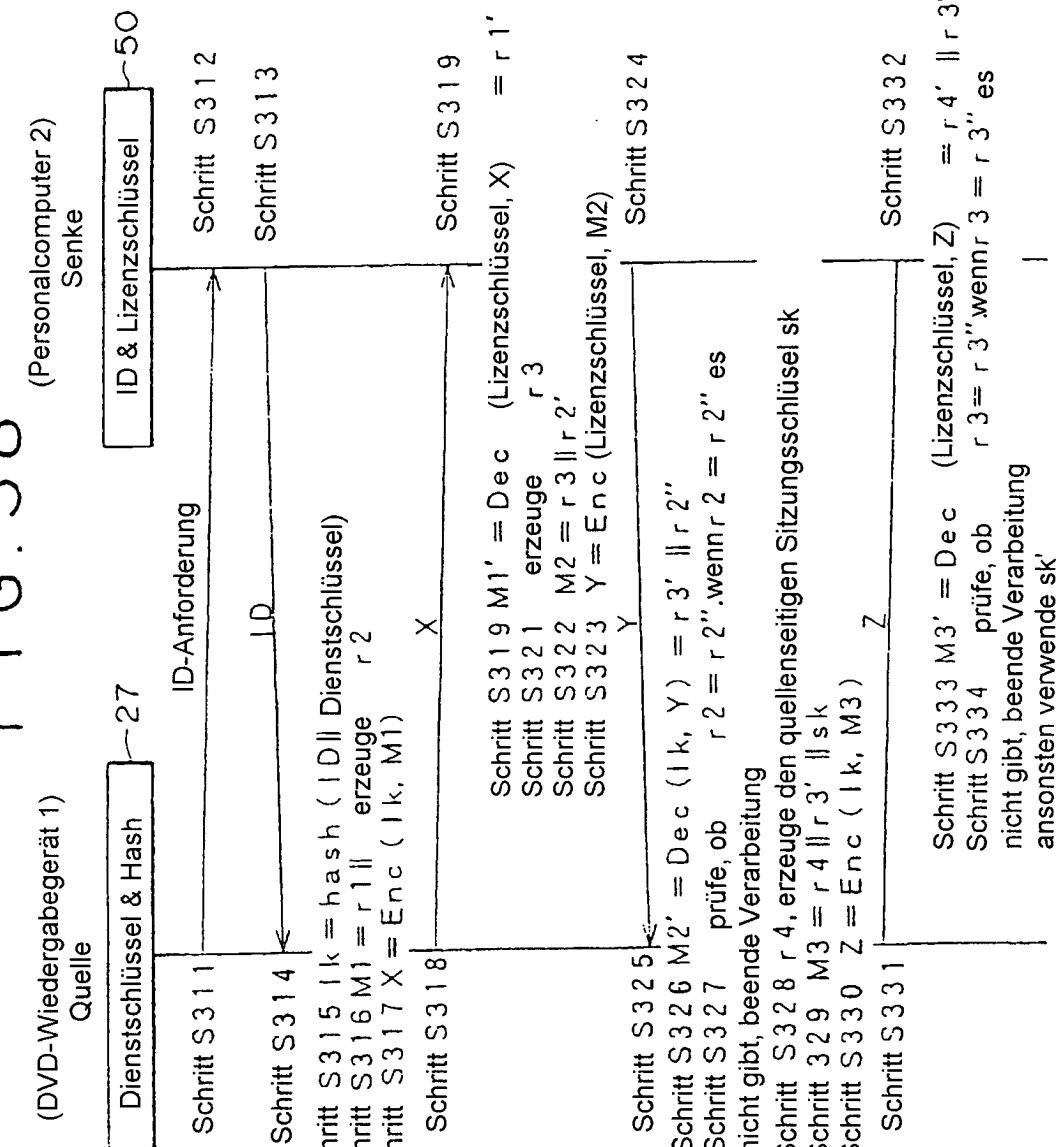

(DVD-Wiedergabegerät 1)
Quelle
Dienstschlüssel & Hash
27
(Personalcomputer 2)
Senke
ID & Lizenzschlüssel
50
Schritt S311
ID-Anforderung
Schritt S312
Schritt S313
ID
Schritt S314
Schritt S315 Ik = hash (ID|| Dienstschlüssel)
Schritt S316 M1 = r1|| erzeuge r2
Schritt S317 X = Enc (Ik, M1)
X
Schritt S318
Schritt S319
Schritt S319 M1' = Dec (Lizenzschlüssel, X) = r1' || r2'
Schritt S321 erzeuge r3
Schritt S322 M2 = r3 || r2'
Schritt S323 Y = Enc (Lizenzschlüssel, M2)
Y
Schritt S324
Schritt S325
Schritt S326 M2' = Dec (Ik, Y) = r3' || r2''
Schritt S327 prüfe, ob r2 = r2''.wenn r2 = r2'' es
nicht gibt, beende Verarbeitung
Schritt S328 r4, erzeuge den quellenseitigen Sitzungsschlüssel sk
Schritt 329 M3 = r4 || r3' || sk
Schritt S330 Z = Enc (Ik, M3)
Z
Schritt S331
Schritt S332
Schritt S333 M3' = Dec (Lizenzschlüssel, Z) = r4' || r3'' || sk'
Schritt S334 prüfe, ob r3 = r3''.wenn r3 = r3'' es
nicht gibt, beende Verarbeitung
ansonsten verwende sk'

FIG. 39

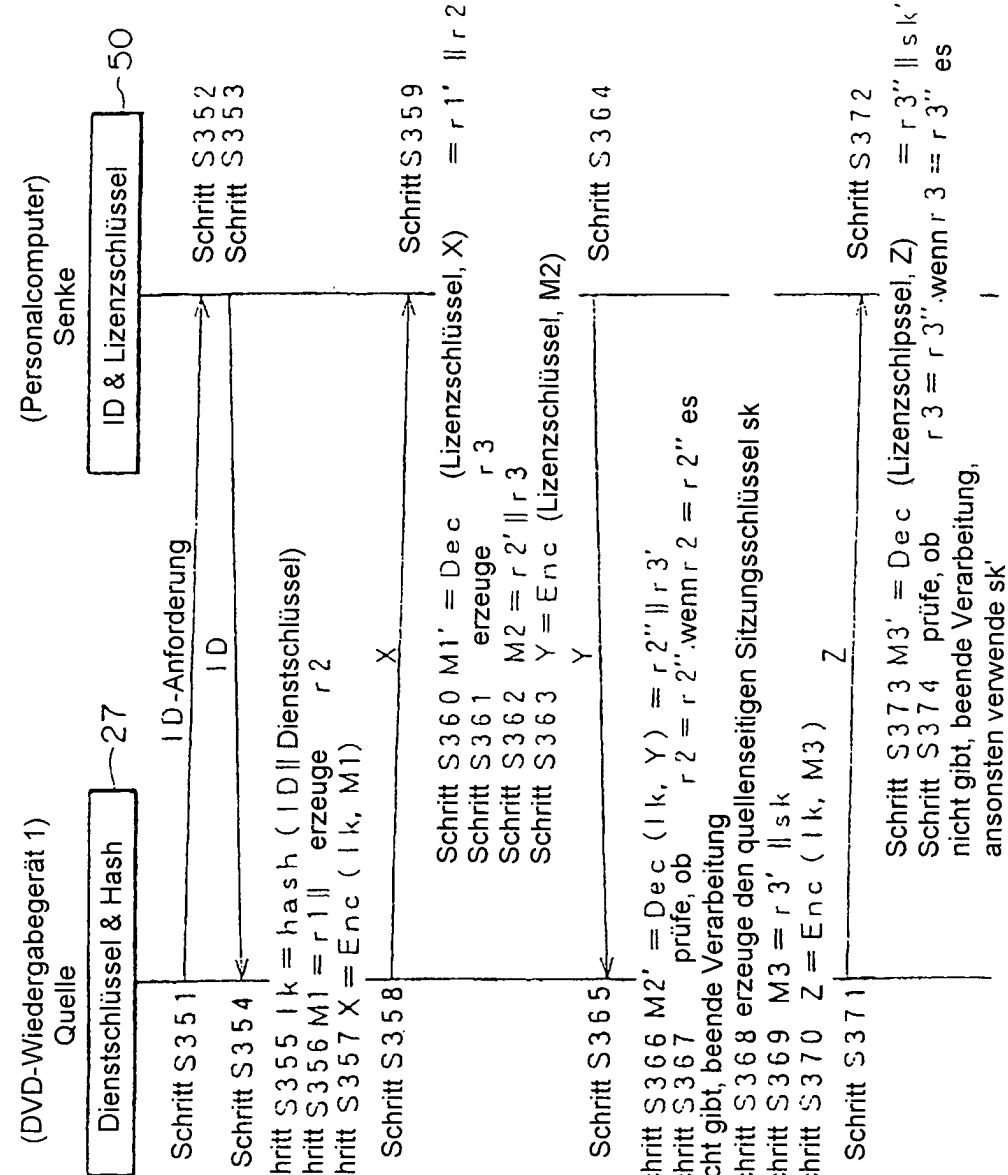

(DVD-Wiedergabegerät 1)
Quelle
Dienstschlüssel & Hash
27
(Personalcomputer)
Senke
ID & Lizenzschlüssel
50
Schritt S351
ID-Anforderung
Schritt S352
Schritt S353
ID
Schritt S354
Schritt S355 Ik = hash (ID|| Dienstschlüssel)
Schritt S356 M1 = r1 || erzeuge r2
Schritt S357 X = Enc (Ik, M1)
X
Schritt S358
Schritt S359
Schritt S360 M1' = Dec (Lizenzschlüssel, X) = r1' || r2'
Schritt S361 erzeuge r3
Schritt S362 M2 = r2' || r3
Schritt S363 Y = Enc (Lizenzschlüssel, M2)
Y
Schritt S365
Schritt S364
Schritt S366 M2' = Dec (Ik, Y) = r2'' || r3'
Schritt S367 prüfe, ob r2 = r2''.wenn r2 = r2'' es
nicht gibt, beende Verarbeitung
Schritt S368 erzeuge den quellenseitigen Sitzungsschlüssel sk
Schritt S369 M3 = r3' || sk
Schritt S370 Z = Enc (Ik, M3)
Z
Schritt S371
Schritt S372
Schritt S373 M3' = Dec (Lizenzschlpssel, Z) = r3'' || sk'
Schritt S374 prüfe, ob r3 = r3''.wenn r3 = r3'' es
nicht gibt, beende Verarbeitung,
ansonsten verwende sk'

FIG. 40

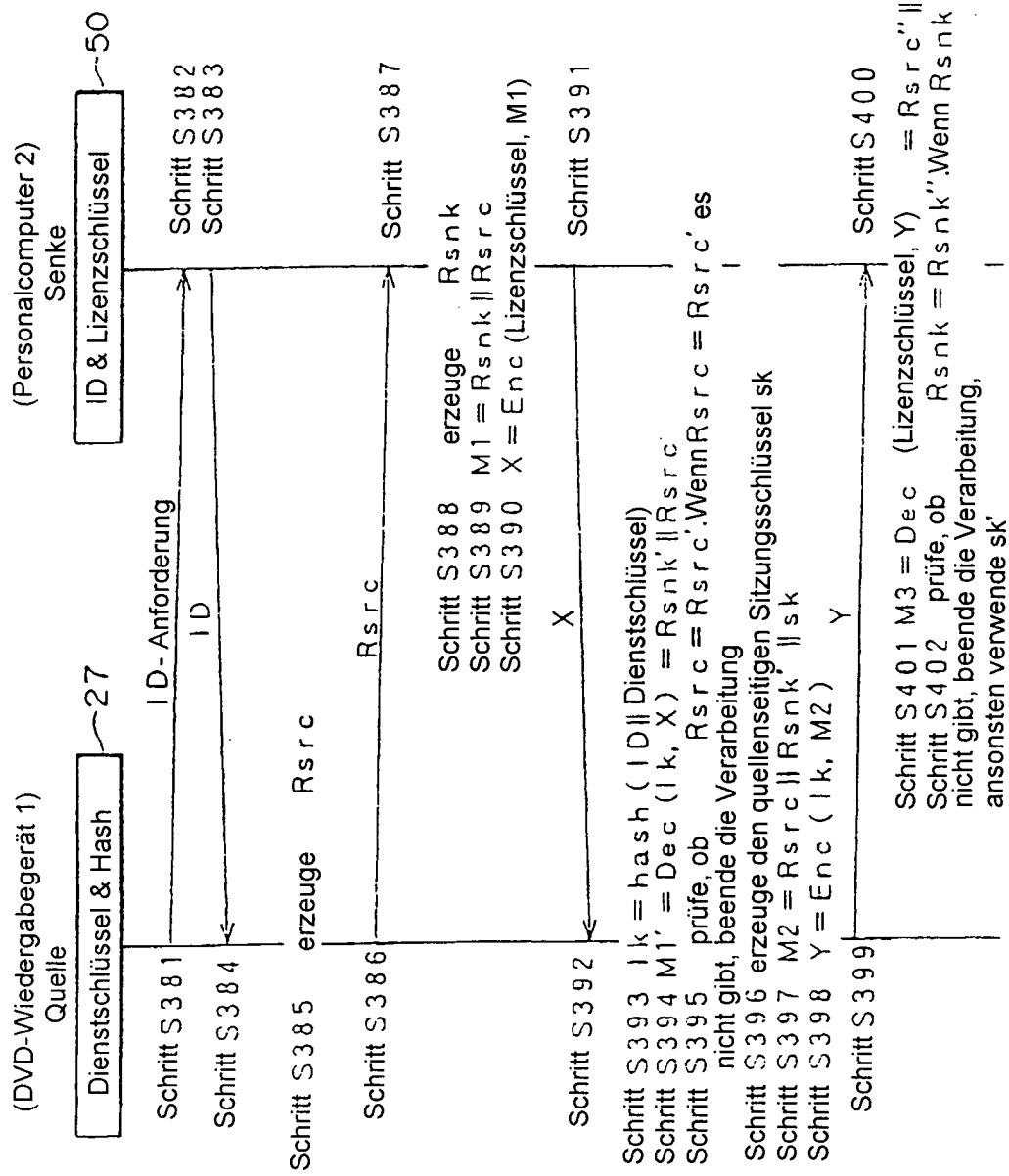

(DVD-Wiedergabegerät 1)
Quelle
Dienstschlüssel & Hash
27
(Personalcomputer 2)
Senke
ID & Lizenzschlüssel
50
ID-Anforderung
ID
Schritt S381
Schritt S382
Schritt S383
Schritt S384
Schritt S385 erzeuge Rsrc
Rsrc
Schritt S386
Schritt S387
Schritt S388 erzeuge Rsnk
Schritt S389 M1 = Rsnk || Rsrc
Schritt S390 X = Enc (Lizenzschlüssel, M1)
X
Schritt S391
Schritt S392
Schritt S393 Ik = hash (ID|| Dienstschlüssel)
Schritt S394 M1' = Dec (Ik, X) = Rsnk' || Rsrc'
Schritt S395 prüfe, ob Rsrc = Rsrc'.Wenn Rsrc = Rsrc' es nicht gibt, beende die Verarbeitung
Schritt S396 erzeuge den quellenseitigen Sitzungsschlüssel sk
Schritt S397 M2 = Rsrc || Rsnk' || sk
Schritt S398 Y = Enc (Ik, M2)
Y
Schritt S399
Schritt S400
Schritt S401 M3 = Dec (Lizenzschlüssel, Y) = Rsrc'' || Rsnk'' || sk'
Schritt S402 prüfe, ob Rsnk = Rsnk''.Wenn Rsnk = Rsnk'' es nicht gibt, beende die Verarbeitung, ansonsten verwende sk'

FIG. 41