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

(10) **DE 693 33 754 T2** 2005.08.04

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 0 561 685 B1**
(21) Deutsches Aktenzeichen: **693 33 754.0**
(96) Europäisches Aktenzeichen: **93 400 658.6**
(96) Europäischer Anmeldetag: **16.03.1993**
(97) Erstveröffentlichung durch das EPA: **22.09.1993**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **09.02.2005**
(47) Veröffentlichungstag im Patentblatt: **04.08.2005**

(51) Int Cl.[7]: **G06F 12/14**
G06F 1/00

(30) Unionspriorität:
5804892 16.03.1992 JP

(84) Benannte Vertragsstaaten:
DE, FR, GB

(73) Patentinhaber:
Fujitsu Ltd., Kawasaki, Kanagawa, JP

(74) Vertreter:
W. Seeger und Kollegen, 81369 München

(72) Erfinder:
Hasebe, Takayuki, Kawasaki-shi, Kanagawa 211, JP; Akiyama, Ryota, Kawasaki-shi, Kanagawa 211, JP; Yoshioka, Makoto, Kawasaki-shi, Kanagawa 211, JP

(54) Bezeichnung: **Schutzsystem für elektronische Daten**

Anmerkung: Innerhalb von neun Monaten nach der Bekanntmachung des Hinweises auf die Erteilung des europäischen Patents kann jedermann beim Europäischen Patentamt gegen das erteilte europäische Patent Einspruch einlegen. Der Einspruch ist schriftlich einzureichen und zu begründen. Er gilt erst als eingelegt, wenn die Einspruchsgebühr entrichtet worden ist (Art. 99 (1) Europäisches Patentübereinkommen).

Die Übersetzung ist gemäß Artikel II § 3 Abs. 1 IntPatÜG 1991 vom Patentinhaber eingereicht worden. Sie wurde vom Deutschen Patent- und Markenamt inhaltlich nicht geprüft.

Beschreibung

HINTERGRUND DER ERFINDUNG

1. Gebiet der Erfindung

[0001] Die vorliegende Erfindung betrifft ein Schutzsystem für elektronische Daten und betrifft im besonderen ein Schutzsystem für elektronische Daten zum Schützen von elektronischen Daten, wie zum Beispiel von Software, die für einen Computer verwendet wird, und von Daten, die elektronisch veröffentlicht werden, vor illegalem Kopieren durch einen Dritten.

2. Beschreibung der verwandten Technik

[0002] In letzter Zeit finden verschiedene Computer und dergleichen, die elektronische Daten nutzen, breite Verwendung auf verschiedenen Gebieten. Im allgemeinen sind Software und elektronische Daten durch das Urheberrecht in verschiedenen Ländern geschützt.

[0003] Für einen Dritten ist es jedoch relativ einfach, elektronische Daten illegal zu kopieren. Als Resultat des illegalen Kopierens erleidet ein Anbieter von elektronischen Daten einen beträchtlichen Schaden insofern, als er keine rechtmäßigen Gewinne erwirtschaften kann. Als Resultat dieses Schadens steigen die Kosten von elektronischen Daten, d. h., von Software und elektronisch veröffentlichten Daten so an, daß auch Nutzer auf Grund der erhöhten Preise darunter leiden.

[0004] Demzufolge ist es erforderlich, ein Schutzsystem für elektronische Daten, wie etwa Software und elektronisch veröffentlichte Daten, zusätzlich zu dem Schutz durch das Urheberrecht vorzusehen.

[0005] Ferner offenbart WO 88/02202 ein System zum Steuern und Berechnen des Heraussuchens von Daten aus einem CD-ROM-Speicher, der verschlüsselte Datendateien enthält, aus denen das Heraussuchen, wie in der Präambel von Anspruch 1, autorisiert sein muß. Dieses System enthält ein einzelnes Autorisierungs- und Schlüsselverteilungsterminal und eine Vielzahl von Kundenterminals zum Heraussuchen von Daten, in die solche Speicher geladen sind. Um dazu autorisiert zu werden, verschlüsselte Daten aus einer gegebenen Datei herauszusuchen, die in dem obigen Speicher gespeichert ist, bewirkt der Kunde ein Dateiverwendungsanforderungssignal, das zu dem Autorisierungs- und Schlüsselverteilungsterminal zu übertragen ist. Dieses Signal identifiziert die Datei, für die die Autorisierung zum Heraussuchen angefordert wird, und enthält auch eine ID-Nummer, die das Kundenterminal identifiziert, von dem das Signal gesendet wird. Wenn das Autorisierungs- und Schlüsselverteilungsterminal das Kundenterminal dazu autorisiert, Daten aus der Datei herauszusuchen, wird im besonderen für das Kundenterminal ein Dateiverschlüsselungsschlüssel bereitgestellt. Solch ein Dateischlüssel ist in einem Einheitsschlüssel verschlüsselt, der für das Kundenterminal einzigartig ist und in dem Autorisierungs- und Schlüsselverteilungsterminal gespeichert ist. Einheitsschlüssel für jedes der Kundenterminals werden gemäß der Kundenterminal-ID-Nummer individuell herausgesucht und auch in jedem Kundenterminal zum Heraussuchen von Daten gespeichert. Im Gegensatz zu der vorliegenden Erfindung ist es somit für den Nutzer nicht möglich, dieselben Daten von einer Vielzahl von Terminals herauszusuchen, da die gespeicherte ID-Nummer ein Terminal und dessen zugeordneten ROM (37) identifiziert, wodurch das Speichermedium nicht ohne weiteres auf ein anderes Kundenterminal übertragbar ist.

ZUSANMMENFASSUNG DER ERFINDUNG

[0006] Die Aufgabe der vorliegenden Erfindung ist das Vorsehen eines Schutzsystems für elektronische Daten, das einen gewissen Schutz von elektronischen Daten ermöglicht, wie etwa von Software, die für einen Computer verwendet wird, und von elektronisch veröffentlichten Daten, indem die Quelle von illegalen Kopien von Dritten detektiert wird.

[0007] Gemäß der vorliegenden Erfindung ist ein Schutzsystem für elektronische Daten nach Anspruch 1 vorgesehen, das elektronische Daten vor dem illegalen Kopieren durch einen Dritten schützt.

[0008] In einer bevorzugten Ausführungsform sind die elektronischen Daten Software, die in einem Computer verwendet wird.

[0009] In einer anderen bevorzugten Ausführungsform sind die elektronischen Daten elektronisch veröffentlichte Daten.

[0010] In noch einer anderen bevorzugten Ausführungsform speichert das Speichermedium eine Vielzahl von verschlüsselten elektronischen Daten und haben die verschlüsselten elektronischen Daten jeweilig einen verschiedenen Entschlüsselungsschlüssel der elektronischen Daten; verschlüsselt der Anbietercomputer nur einen elektronischen Entschlüsselungsschlüssel für die verschlüsselten elektronischen Daten, auf Erlaubnis durch einen Anbieter, unter Verwendung des Medienschlüssels, und speichert den verschlüsselten Schlüssel der elektronischen Daten auf dem Speichermedium als die verschlüsselten Erlaubnisinformationen; und entschlüsselt der Nutzercomputer die verschlüsselten elektronischen Daten entsprechend den verschlüsselten Erlaubnisinformationen.

[0011] In noch einer anderen bevorzugten Ausfüh-

rungsform schreibt der Nutzercomputer die Mediennummer in nichtüberschreibbarer Form auf das Speichermedium, die der Nutzercomputer nicht überschreiben kann.

KURZE BESCHREIBUNG DER ZEICHNUNGEN

[0012] Zu den Zeichnungen:

[0013] Fig. 1 ist ein schematisches Blockdiagramm eines herkömmlichen Schutzsystems für elektronische Daten;

[0014] Fig. 2 ist eine Hauptansicht der vorliegenden Erfindung;

[0015] Fig. 3 zeigt eine Ausführungsform der vorliegenden Erfindung;

[0016] Fig. 4 ist ein Flußdiagramm eines Speicherprozesses von Software gemäß der vorliegenden Erfindung;

[0017] Fig. 5A und Fig. 5B sind erläuternde Ansichten für ein Beispiel des Verschlüsselungsprozesses;

[0018] Fig. 6 zeigt eine Software-Verschlüsselungsschlüssel-Verwaltungstabelle gemäß einer Ausführungsform der vorliegenden Erfindung;

[0019] Fig. 7A und Fig. 7B sind Flußdiagramme zum Erzeugen von Erlaubnisinformationen;

[0020] Fig. 8 ist eine erläuternde Ansicht zur Erzeugung der Erlaubnisinformationen;

[0021] Fig. 9A und Fig. 9B sind Flußdiagramme für einen Entschlüsselungsprozeß von Software;

[0022] Fig. 10A, Fig. 10B und Fig. 10C sind erläuternde Ansichten eines Programms als elektronische Daten;

[0023] Fig. 11A, Fig. 11B und Fig. 11C sind erläuternde Ansichten von Daten als elektronische Daten;

[0024] Fig. 12 ist eine erläuternde Ansicht einer optischen Magnetplatte des ROM/RAM-Mischtyps;

[0025] Fig. 13 ist eine erläuternde Ansicht für Erlaubnisinformationen, die in einem anderen Speichermedium gespeichert sind; und

[0026] Fig. 14 ist eine erläuternde Ansicht von multipler Software, die auf ein Speichermedium geschrieben ist.

BESCHREIBUNG DER BEVORZUGTEN AUSFÜHRUNGSFORMEN

[0027] Bevor die bevorzugten Ausführungsformen beschrieben werden, werden unten die herkömmliche Technik und ihre Probleme erläutert.

[0028] Fig. 1 ist ein schematisches Blockdiagramm eines herkömmlichen Schutzsystems für elektronische Daten, und zwar im besonderen eines Softwareschutzsystems. Das Merkmal des herkömmlichen Softwareschutzsystems ist die Erzeugung von Erlaubnisinformationen **72** unter Verwendung einer persönlichen Nummer eines Nutzers **91**, wie es unten eingehend erläutert ist.

[0029] Ein Softwarespeichermedium **71**, wie zum Beispiel eine optische Magnetplatte, eine CD-ROM, eine Diskette und dergleichen, wird durch einen Anbieter einem Nutzer angeboten, wie in der Zeichnung gezeigt. Das heißt, der Anbieter bietet dem Nutzer das Softwarespeichermedium **71** an, das die Software speichert. Das Softwarespeichermedium **71** enthält die Erlaubnisinformationen **72** und verschlüsselte Software **73**. Der Anbietercomputer enthält eine Erzeugungseinheit eines persönlichen Schlüssels **81**, einen Softwareentschlüsselungsschlüssel **82** und eine Verschlüsselungsschaltung **83**. Ferner enthält der Nutzercomputer die persönliche Nummer des Nutzers **91**, eine Erzeugungseinheit eines persönlichen Schlüssels **92**, eine Entschlüsselungsschaltung **93**, einen Softwareentschlüsselungsschlüssel **94** und eine Entschlüsselungsschaltung **95**.

[0030] Die Software wird nach der Verschlüsselung in dem Softwarespeichermedium **71** gespeichert. Ein persönlicher Schlüssel eines Nutzers wird unter Verwendung der persönlichen Nummer des Nutzers **91** erzeugt, und der Softwareentschlüsselungsschlüssel **82** wird durch den persönlichen Schlüssel des Nutzers entschlüsselt, so daß die Verschlüsselungsschaltung **83** den Softwareentschlüsselungsschlüssel **82** verschlüsselt, um die Erlaubnisinformationen zu erzeugen. Die Erlaubnisinformationen werden auf dem Softwarespeichermedium **71** gespeichert.

[0031] Der Nutzer kauft das Softwarespeichermedium **71**, das die Erlaubnisinformationen **72** und die verschlüsselte Software **73** enthält, und der Nutzercomputer entschlüsselt die verschlüsselte Software **73**, so daß es möglich ist, das unverschlüsselte Programm auszuführen.

[0032] In dem Anbietercomputer erzeugt die Erzeugungseinheit des persönlichen Schlüssels **81** den persönlichen Schlüssel auf der Basis der persönlichen Nummer des Nutzers **91**, die zum Beispiel eine Apparatenummer eines Computers ist. Der Softwareentschlüsselungsschlüssel **82** entschlüsselt die verschlüsselte Software **73**. Die Verschlüsselungs-

schaltung **83** erzeugt die Erlaubnisinformationen **72** zur Speicherung auf dem Softwarespeichermedium **71**.

[0033] In dem Nutzercomputer empfängt die Erzeugungseinheit des persönlichen Schlüssels **92** die persönliche Nummer des Nutzers **91** und erzeugt sie den persönlichen Schlüssel des Nutzers. Die Entschlüsselungsschaltung **93** entschlüsselt die Erlaubnisinformationen **72** von dem Softwarespeichermedium **71** auf der Basis des persönlichen Schlüssels **81**. Der Softwareentschlüsselungsschlüssel **94** wird der Entschlüsselungsschaltung **95** eingegeben, die Entschlüsselungsschaltung **95** entschlüsselt die verschlüsselte Software **73**, um die Klartextsoftware zu erzeugen. Als Resultat wird die Klartextsoftware in einen Hauptspeicher des Nutzercomputers geladen.

[0034] Das herkömmliche Softwareschutzsystem nutzt, wie oben erläutert, eine persönliche Nummer eines Nutzers (oder eine Apparatenummer eines Computers) und einen persönlichen Schlüssel.

[0035] Bei Gebrauch der persönlichen Nummer für den Computer wird durch die Erlaubnisinformationen **72** die Ausführung für den Computer beantragt, so daß nur jener Computer die Klartextsoftware ausführen kann. Daher kann der Nutzer keinen anderen Computer nutzen, auch wenn er dazu autorisiert ist. Ferner ist es unmöglich, solche Klartextsoftware zu einem Dritten zu übertragen.

[0036] Bei Gebrauch der persönlichen Nummer für tragbare Hardware ist es erforderlich, eine Schnittstelle zwischen der Hardware und dem Computer vorzusehen, so daß die Gesamtkosten für den Schutz ansteigen.

[0037] Als Merkmal der vorliegenden Erfindung enthält ein Speichermedium zum Speichern von elektronischen Daten eine Mediennummer. Ein Anbieter genehmigt die Verwendung der Mediennummer. Gemäß der vorliegenden Erfindung ist es möglich, mit Autorisierung durch den Anbieter nur auf elektronische Daten zuzugreifen, die auf dem Medium gespeichert sind.

[0038] Fig. 2 ist eine Hauptansicht der vorliegenden Erfindung. In Fig. 2 enthält das Speichermedium **1** eine Mediennummer **12**, Erlaubnisinformationen **13** und verschlüsselte elektronische Daten **14**. Bei der vorliegenden Erfindung enthalten die elektronischen Daten Computersoftware und elektronisch veröffentlichte Daten, wie unten erläutert ist. Der Anbietercomputer enthält eine Erzeugungseinheit eines persönlichen Medienschlüssels **21**, einen Entschlüsselungsschlüssel der elektronischen Daten **22** und eine Entschlüsselungseinheit **23**. Der Nutzercomputer enthält eine Erzeugungseinheit eines persönlichen Medienschlüssels **31**, eine Entschlüsselungseinheit **32**, einen Entschlüsselungsschlüssel der elektronischen Daten **33** und eine Entschlüsselungseinheit **34**.

[0039] Die Erzeugungseinheiten des persönlichen Schlüssels **21** und **31** erzeugen einen Medienschlüssel auf der Basis der Mediennummer **12**. Die Verschlüsselungseinheit **23** verschlüsselt den Entschlüsselungsschlüssel der elektronischen Daten **22** auf der Basis des Medienschlüssels.

[0040] Die Entschlüsselungseinheit **32** entschlüsselt die Erlaubnisinformationen **13** auf der Basis des Medienschlüssels und erzeugt den Entschlüsselungsschlüssel der elektronischen Daten **33**. Ferner entschlüsselt die Entschlüsselungseinheit **34** die verschlüsselten elektronischen Daten **14** auf der Basis des Entschlüsselungsschlüssels der elektronischen Daten **33** und erzeugt sie die elektronischen Klartextdaten.

[0041] Kurz gesagt, bei der vorliegenden Erfindung werden zuvor nur die Mediennummer **12** und die verschlüsselten elektronischen Daten **14** in dem Speichermedium **1** gespeichert.

[0042] In dem Anbietercomputer erzeugt die Erzeugungseinheit des persönlichen Schlüssels **21** den Medienschlüssel auf der Basis der Mediennummer, verschlüsselt die Verschlüsselungseinheit **23** den Entschlüsselungsschlüssel der elektronischen Daten **22** auf der Basis des Medienschlüssels und schreibt die Verschlüsselungseinheit **23** die verschlüsselten Daten auf das Speichermedium **1** als Erlaubnisinformationen **13**.

[0043] In dem Nutzercomputer erzeugt die Erzeugungseinheit des persönlichen Schlüssels **31** den Medienschlüssel auf der Basis der Mediennummer **12** des Speichermediums **1**, entschlüsselt die Entschlüsselungseinheit **32** die Erlaubnisinformationen **13** auf der Basis des persönlichen Schlüssels und erzeugt sie einen Original-Entschlüsselungsschlüssel der elektronischen Daten **33** und entschlüsselt die Entschlüsselungseinheit **34** die verschlüsselten elektronischen Daten **14** auf der Basis des Original-Entschlüsselungsschlüssels der elektronischen Daten **33** und sieht sie die elektronischen Klartextdaten vor.

[0044] Ferner ist für alle verschlüsselten elektronischen Daten **14** ein verschiedener Entschlüsselungsschlüssel der elektronischen Daten **22** vorgesehen. Nur der Entschlüsselungsschlüssel der elektronischen Daten **22** der verschlüsselten elektronischen Daten **14**, bei dem die Verwendung in dem Anbietercomputer erlaubt ist, wird durch den Medienschlüssel verschlüsselt und auf dem Speichermedium **1** als Erlaubnisinformationen **13** gespeichert. Ferner werden nur die verschlüsselten elektronischen Daten, die diesen Erlaubnisinformationen **13** entsprechen, die auf dem Speichermedium **1** gespeichert sind, in dem

Nutzercomputer entschlüsselt, um die elektronischen Klartextdaten vorzusehen.

[0045] Des weiteren kann durch den Nutzercomputer nur die Mediennummer **12** auf das Speichermedium **1** in nichtüberschreibbarer Form geschrieben werden. Weiterhin können durch den Anbietercomputer nur die Erlaubnisinformationen **13** auf einem anderen Medium, wie zum Beispiel auf einer Diskette, gespeichert werden und zur Verwendung in dem Nutzercomputer vorgesehen werden. Darüber hinaus kann der Anbieter die Erlaubnisinformationen **13** über eine Übertragungsleitung zu dem Nutzercomputer übertragen, so daß der Nutzercomputer die verschlüsselten elektronischen Daten **14** auf der Basis der Erlaubnisinformationen **13** entschlüsseln kann, um die elektronischen Klartextdaten vorzusehen.

[0046] In diesem Fall sind die verschlüsselten elektronischen Daten **14** Software zum Betreiben verschiedener Computer oder verschiedene Typen von Daten (Zeichendaten, Bilddaten, Tondaten), und diese werden verschlüsselt, um deren Inhalt zu schützen. Da das Medium **1**, das die verschlüsselten elektronischen Daten **14** speichert, die Mediennummer in nichtüberschreibbarer Form enthält, erlaubt daher der Anbietercomputer die Verwendung der elektronischen Daten, die die Mediennummer haben. Somit ist es möglich, nur die verschlüsselten elektronischen Daten **14** zu verwenden, die auf dem korrekten Medium **1** gespeichert sind und wofür durch den Anbieter die Autorisierung erfolgt. Als Resultat ist es möglich, die gespeicherten elektronischen Daten zu einem anderen Nutzer zu übertragen, so daß dieses Medium **1** in einem anderen Computer verwendet werden kann.

[0047] Fig. 3 bis Fig. 14 sind erläuternde Ansichten für Ausführungsformen der vorliegenden Erfindung. Anhand eines Beispiels für elektronische Daten, das in Fig. 2 gezeigt ist, folgt als nächstes die Erläuterung für Software, die für einen Computer verwendet wird.

[0048] Fig. 3 zeigt eine Ausführungsform der vorliegenden Erfindung. In Fig. 3 ist das Softwarespeichermedium **11**, wie zum Beispiel eine optische Magnetplatte (besonders eine Platte mit einer Kapazität in dem Bereich von mehreren hundert MByte bis mehreren GByte), ein Medium zum Speichern von Software, wofür durch einen Anbieter die Autorisierung erfolgt, zur Verwendung durch einen Nutzer. Das Softwarespeichermedium **11** speichert die Mediennummer **12** in nichtüberschreibbarer Form, die Erlaubnisinformationen **13**, die dem Nutzer die Erlaubnis zur Verwendung der Software erteilen, und die verschlüsselte Software **15**.

[0049] Die Mediennummer **12** ist eine besondere Nummer für das Medium **11**, und diese Mediennummer kann durch den Nutzer nicht überschrieben werden (d. h., sie ist nicht überschreibbar). Das heißt, diese Mediennummer **12** wird in einen Bereich geschrieben, den der Nutzer nicht überschreiben kann. Dieser Bereich kann in verschiedenen Formen verwaltet werden. Zum Beispiel kann dieser Bereich durch ein Betriebssystem (OS) verwaltet werden. Ferner ist es möglich, ihn so anzuordnen, daß dieser Bereich durch das Betriebssystem nicht überschrieben werden kann.

[0050] Die Erlaubnisinformationen **13** werden von dem Anbieter für den Nutzer vorgesehen, um die Verwendung der Software zu erlauben. In diesem Fall inkorporieren diese Erlaubnisinformationen **13** Daten zum Entschlüsseln der verschlüsselten Software **15** (siehe Fig. 7 und Fig. 8). Die verschlüsselte Software **15** ist in Fig. 4 bis Fig. 6 gezeigt.

[0051] Der Anbietercomputer enthält die Erzeugungseinheit des persönlichen Schlüssels **21**, den Softwareentschlüsselungsschlüssel **24** und die Verschlüsselungseinheit **23**. Die Erzeugungseinheit des persönlichen Schlüssels **21** erzeugt den Medienschlüssel auf der Basis der Mediennummer **12**, die aus dem Softwarespeichermedium **11** gelesen wird (siehe Fig. 7). Die Verschlüsselungseinheit **23** verschlüsselt den Softwareentschlüsselungsschlüssel **24** auf der Basis des Medienschlüssels, der durch die Erzeugungseinheit des persönlichen Schlüssels **21** erzeugt wurde. Die durch die Verschlüsselungseinheit **23** verschlüsselten Daten werden in dem Softwarespeichermedium **11** als die Erlaubnisinformationen **13** gespeichert.

[0052] Der Nutzercomputer enthält die Erzeugungseinheit des persönlichen Schlüssels **31**, die Entschlüsselungseinheit **32**, den Softwareentschlüsselungsschlüssel **35** und die Entschlüsselungseinheit **34**. Die Erzeugungseinheit des persönlichen Schlüssels **31** erzeugt den Medienschlüssel auf der Basis der Mediennummer **12**, die von dem Softwarespeichermedium **11** gelesen wird (siehe Fig. 7). Die Entschlüsselungseinheit **32** entschlüsselt die Erlaubnisinformationen **13**, die von dem Softwarespeichermedium **11** gelesen werden, auf der Basis des Medienschlüssels, der durch die Erzeugungseinheit des persönlichen Schlüssels **31** erzeugt wurde, und erzeugt den Softwareentschlüsselungsschlüssel **35** (siehe Fig. 9). Die Entschlüsselungseinheit **34** entschlüsselt die verschlüsselte Software **15**, die von dem Softwarespeichermedium **11** gelesen wird, auf der Basis des Softwareentschlüsselungsschlüssels **35** und erzeugt die Klartextsoftware (siehe Fig. 9). Der Nutzercomputer führt dann die Klartextsoftware aus.

[0053] Fig. 4 ist ein Flußdiagramm eines Speicherprozesses der Software gemäß der vorliegenden Erfindung. Dieses Flußdiagramm zeigt den Speicherprozeß der verschlüsselten Software **15** und die verschlüsselten Erlaubnisinformationen **13**. Bei Schritt

S1 erzeugt der Anbieter die Software, zum Beispiel ein Auftragsprogramm, etc., und speichert die erzeugte Software auf dem Softwarespeichermedium. Bei Schritt S2 erzeugt der Anbieter den Softwareverschlüsselungsschlüssel. Bei Schritt S3 wird der Softwareverschlüsselungsschlüssel in einer Verschlüsselungsschlüssel-Verwaltungstabelle gespeichert (siehe Fig. 6), die jeder Software entspricht. Das heißt, der bei Schritt S2 erzeugte Verschlüsselungsschlüssel wird in der Verschlüsselungsschlüssel-Verwaltungstabelle in Entsprechung zu dem Namen der bei Schritt S1 erzeugten Software gespeichert.

[0054] Bei Schritt S4 wird der Softwareverschlüsselungsschlüssel, der der durch den Anbieter bezeichneten Software entspricht, der Verschlüsselungsschlüssel-Verwaltungstabelle entnommen. Bei Schritt S5 verschlüsselt der Anbieter die Klartextsoftware unter Verwendung des Softwäreverschlüsselungsschlüssels, der der Verschlüsselungsschlüssel-Verwaltungstabelle entnommen wurde, um die verschlüsselte Software zu erzeugen. Ein Hauptkörper der Software wird durch den Verschlüsselungsschlüssel so verschlüsselt, wie in Fig. 5 gezeigt, um den verschlüsselten Softwarekörper zum Beispiel unter Verwendung eines Datenverschlüsselungsstandards (Data Encryption Standard: DES) zu erzeugen, der in den Vereinigten Staaten weit verbreitet ist. Gemäß dem DES wird der Hauptkörper der Software mit einer 64-Bit-Folge, wie in Fig. 5B gezeigt, in dieselbe: 64-Bit-Folge, jedoch mit einer verschiedenen Bitreihenfolge verschlüsselt.

[0055] Bei Schritt S6 wird die verschlüsselte Software in dem Speichermedium des Anbieters (oder eines Herstellers des Mediums) gespeichert, so daß es möglich ist, die einmal verschlüsselte Software zu halten. Daher kann bei einer nachfolgenden Verwendung der Software der Verschlüsselungsprozeß durch den Anbieter weggelassen werden, da die auf dem Medium gehaltene Software wieder verwendet wird. Bei Schritt S7 wird die verschlüsselte Software auf dem Softwarespeichermedium **11** gespeichert. Bei Schritt S8 bestimmt der Anbieter, ob der Verschlüsselungsprozeß für die Software vollendet ist und die verschlüsselte Software auf dem Speichermedium gespeichert ist oder nicht. Wenn das Resultat "JA" lautet, ist der Verschlüsselungsprozeß durch den Anbieter vollendet.

[0056] Wenn das Resultat "NEIN" lautet, kehrt der Verschlüsselungsprozeß zu Schritt S7 zurück und speichert sequentiell die verschlüsselte Software, die den Namen der bezeichneten Software hat. Die verschlüsselte Software wird, wie oben erläutert, auf dem Softwarespeichermedium **11** gespeichert.

[0057] Fig. 5A und Fig. 5B sind erläuternde Ansichten von einem Beispiel für den Verschlüsselungsprozeß. Ein Header-Abschnitt H enthält einen Softwarenamen als Identifikator, und ein Hauptkörper der Software S enthält die Klartextsoftware. Der Header-Abschnitt H ist nicht verschlüsselt, und der Hauptkörper der Software S wird durch den Verschlüsselungsschlüssel K verschlüsselt. Die Verschlüsselung erfolgt zum Beispiel unter Verwendung des DES (Data Encryption Standard), wie in Fig. 5B gezeigt. Der DES ist in den Vereinigten Staaten bereits bekannt.

[0058] Gemäß dem Verschlüsselungsprozeß nach dem DES wird die 64-Bit-Bitfolge der Klartextsoftware in dieselbe 64-Bit-Folge wie oben konvertiert, wie in Fig. 5B gezeigt, wobei diese jedoch eine verschiedene Bitreihenfolge hat. Die Entschlüsselungseinheit entschlüsselt die verschlüsselte 64-Bit-Folge unter Verwendung des DES in die Klartextsoftware.

[0059] Fig. 6 zeigt eine Software-Verschlüsselungsschlüssel-Verwaltungstabelle gemäß einer Ausführungsform der vorliegenden Erfindung. Die Software-Verschlüsselungsschlüssel-Verwaltungstabelle **4** ist gebildet, wie in der Zeichnung gezeigt, aus dem Namen der Software und dem Verschlüsselungsschlüssel, der dem Namen der Software entspricht. Ein Codewechselzeichen "ENC" ist zu jedem Softwarenamen hinzugefügt, um anzugeben, daß die entsprechende Software bereits verschlüsselt ist. Ferner ist der verschlüsselte Schlüssel, wie oben erläutert, aus einer 64-Bit-Bitfolge gebildet.

(1) Was die Klartextsoftware betrifft, die auf dem Speichermedium zu speichern ist, wird der Softwareverschlüsselungsschlüssel der Software-Verschlüsselungsschlüssel-Verwaltungstabelle entnommen.

(2) Die Verschlüsselungsschaltung **41** verschlüsselt die Klartextsoftware auf der Basis des Softwareverschlüsselungsschlüssels, der oben bei (1) erhalten wurde.

(3) Die verschlüsselte Software wird auf dem Softwarespeichermedium **11** als verschlüsselte Software **15** gespeichert.

[0060] Die obigen Schritte werden für die gesamte Klartextsoftware wiederholt, die durch den Anbieter bezeichnet wurde. Da die einmal verschlüsselte Software durch den Anbieter gehalten wird, wie oben erläutert, wird diese verschlüsselte Software wieder auf dem Softwarespeichermedium gespeichert, wenn ein anderer Nutzer diese Klartextsoftware anfordert. Die Mediennummer **12** ist nur für das entsprechende Speichermedium vorgesehen, und sie wird in nichtüberschreibbarer Form auf das Medium **11** geschrieben (d. h., die persönliche Nummer kann nicht überschrieben werden).

[0061] Ferner koinzidiert der Verschlüsselungsschlüssel, der in der Software-Verschlüsselungsschlüssel-Verwaltungstabelle **4** gespeichert ist, mit dem Entschlüsselungsschlüssel, wenn eine Objektschlüsselnummer als Verschlüsselungsalgorithmus

verwendet wird. Der Softwareverschlüsselungsschlüssel, der der Klartextsoftware entspricht, wird, wie oben erläutert, der Software-Verschlüsselungsschlüssel-Verwaltungstabelle entnommen, die Klartextsoftware wird durch den Softwareverschlüsselungsschlüssel verschlüsselt, um die verschlüsselte Software zu erzeugen, und die verschlüsselte Software wird in dem Softwarespeichermedium **11** gespeichert.

[0062] Fig. 7A und Fig. 7B sind Flußdiagramme zum Erzeugen von Erlaubnisinformationen, und Fig. 8 ist eine erläuternde Ansicht zur Erzeugung der Erlaubnisinformationen. Das Flußdiagramm erläutert, daß die Erlaubnisinformationen **13** für die Software erzeugt werden, für die die Autorisierung erfolgen soll und die auf dem Softwarespeichermedium zu speichern ist.

[0063] Bei Schritt S11 wird der Name der Software, für die die Autorisierung erfolgen soll, für die Software-Entschlüsselungsschlüssel-Verwaltungstabelle **5** eingegeben. Bei Schritt S12 wird der Softwareentschlüsselungsschlüssel von der Software-Entschlüsselungsschlüssel-Verwaltungstabelle **5** geladen. Der Entschlüsselungsschlüssel, der dem Namen der Software entspricht, für die die Autorisierung erfolgen soll, wird, wie in Fig. 8 gezeigt, von der Software-Entschlüsselungsschlüssel-Verwaltungstabelle **5** zu der Verschlüsselungsschaltung **33** gesendet.

[0064] Bei Schritt S13 wird die Mediennummer **12** von dem Softwarespeichermedium **11** geladen. Bei Schritt S14 wird der Medienschlüssel in der Erzeugungsschaltung des persönlichen Schlüssels **211** erzeugt. Das heißt, wie in Fig. 7B gezeigt, die Mediennummer (Klartext, d. h. unverschlüsselt) wird durch einen Geheimschlüssel (oder einen Geheimalgorithmus) verschlüsselt, so daß der Medienschlüssel (verschlüsselt) erzeugt wird. Im allgemeinen wird bei Verwendung des DES ein Geheimschlüssel verwendet, und bei Verwendung eines Geheimalgorithmus wird der Geheimschlüssel nicht verwendet.

[0065] Bei Schritt S15 wird der Softwareentschlüsselungsschlüssel (Klartext, d. h. unverschlüsselt) durch den Medienschlüssel verschlüsselt, so daß die Erlaubnisinformationen (verschlüsselt) erzeugt werden. Der DES wird für den obigen Verschlüsselungsprozeß verwendet. Bei Schritt S16 werden die bei Schritt S15 verschlüsselten Erlaubnisinformationen in dem Softwarespeichermedium **11** gespeichert.

[0066] Kurz gesagt, die verschlüsselte Software wird, wie oben erläutert, auf dem Softwarespeichermedium **11** gespeichert, der Medienschlüssel **12** wird von ihm gelesen, der Softwareentschlüsselungsschlüssel wird durch den Medienschlüssel verschlüsselt, um die verschlüsselten Erlaubnisinformationen **13** zu erzeugen, und die verschlüsselten Erlaubnisinformationen **13** werden auf dem Softwarespeichermedium **11** gespeichert. Daher sind die verschlüsselte Software **15** und die verschlüsselten Erlaubnisinformationen **13** auf dem Softwarespeichermedium **11** gespeichert.

[0067] In Fig. 8 ist die Software-Entschlüsselungsschlüssel-Verwaltungstabelle **5** zum Verwalten des Softwareentschlüsselungsschlüssels vorgesehen, der verwendet wird, wenn die verschlüsselte Software **15** entschlüsselt wird, um die Klartextsoftware abzuleiten. Der Softwareentschlüsselungsschlüssel wird in Entsprechung zu dem Softwarenamen verwaltet. Die Software-Entschlüsselungsschlüssel-Verwaltungstabelle **5** speichert den Entschlüsselungsschlüssel und hat dieselbe Struktur wie die Software-Verschlüsselungsschlüssel-Verwaltungstabelle **4**.

(1) Wenn der Anbieter Erlaubnisinformationen an einen Nutzer verkauft, wird die Mediennummer **12** von dem Softwarespeichermedium **11** gelesen. Die Erzeugungsschaltung des persönlichen Schlüssels **211** empfängt diese Mediennummer und erzeugt den Medienschlüssel (siehe Schritt S14 von Fig. 7A).

(2) Als nächstes wird der Softwareentschlüsselungsschlüssel entsprechend der zu verkaufenden Software der Software-Entschlüsselungsschlüssel-Verwaltungstabelle **5** entnommen, und dieser Schlüssel wird der Verschlüsselungsschaltung **231** eingegeben. Dieser Softwareentschlüsselungsschlüssel wird durch den persönlichen Schlüssel in der Verschlüsselungsschaltung **231** verschlüsselt, so daß die Verschlüsselungsschaltung **231** die Erlaubnisinformationen **13** erzeugt. Die Erlaubnisinformationen **13** enthalten den Softwarenamen mit dem Codewechselzeichen ENC und die verschlüsselten Erlaubnisinformationen, und diese Erlaubnisinformationen **13** werden auf dem Softwarespeichermedium **11** gespeichert. In diesem Fall werden der Softwareentschlüsselungsschlüssel und der Algorithmus (oder der Geheimschlüssel) durch ein bekanntes Sicherheitsmittel (nicht gezeigt) geschützt.

[0068] Der Anbieter erzeugt, wie oben erläutert, den Medienschlüssel auf der Basis der Mediennummer **12**, die von dem Softwarespeichermedium **11** gelesen wird, verschlüsselt den Softwareentschlüsselungsschlüssel auf der Basis des Medienschlüssels und speichert diesen Softwareentschlüsselungsschlüssel in dem Softwarespeichermedium **11** als Erlaubnisinformationen **13**.

[0069] Fig. 9A und Fig. 9B sind Flußdiagramme eines Entschlüsselungsprozesses der Software. Der Nutzer kauft das Softwarespeichermedium **11** und montiert es in den Nutzercomputer. Die Software des Speichermediums **11** wird in einen Hauptspeicher geladen, um das Programm auszuführen.

[0070] Bei Schritt S21 empfängt der Nutzercomputer eine Instruktion zum Ausführen der Software. Bei Schritt S22 wird dem Softwarespeichermedium **11** die Mediennummer **12** entnommen. Bei Schritt S23 wird der Medienschlüssel (unverschlüsselt) durch den Geheimschlüssel (oder den Algorithmus) verschlüsselt, um den verschlüsselten Medienschlüssel zu erzeugen. Bei Schritt S24 werden die verschlüsselten Erlaubnisinformationen durch den Medienschlüssel entschlüsselt, so daß der Klartextsoftware-Entschlüsselungsschlüssel erzeugt wird.

[0071] Bei Schritt S25 wird die verschlüsselte Software **15** von dem Softwarespeichermedium **11** gelesen. Bei Schritt S26 wird die verschlüsselte Software durch den Softwäreentschlüsselungsschlüssel entschlüsselt, so daß die Klartextsoftware erzeugt wird. Bei Schritt S27 führt der Nutzercomputer die Klartextsoftware aus.

[0072] Kurz gesagt, der Medienschlüssel wird auf der Basis des Medienschlüssels **12** von dem Softwarespeichermedium **11** erzeugt, wie oben erläutert, die Erlaubnisinformationen **13** werden auf der Basis des Medienschlüssels entschlüsselt, um den Softwareentschlüsselungsschlüssel **35** zu erzeugen, und die verschlüsselte Software wird durch den Softwareentschlüsselungsschlüssel **35** entschlüsselt, um die Klartextsoftware zu erzeugen.

[0073] Fig. 10A, Fig. 10B und Fig. 10C sind erläuternde Ansichten eines Programms als elektronische Daten. Fig. 10A zeigt eine Gesamtstruktur, Fig. 10B zeigt ein Flußdiagramm, und Fig. 10C ist eine erläuternde Ansicht zur Ausführung der Software. In Fig. 10A entspricht die optische Magnetplatte **6** dem Softwarespeichermedium **11** von Fig. 2 und Fig. 3, und sie speichert die Mediennummer **12**, die Erlaubnisinformationen **13** und das verschlüsselte Programm **16**. Der Nutzer kauft die optische Magnetplatte **6** und montiert diese Platte in eine optische Magnetvorrichtung. Andere bekannte Beispiele für Speichermedien sind eine optische Platte, eine CD-ROM, eine Diskette, eine Festplatte, ein Magnetband, ein Kassettenband und dergleichen.

[0074] Ein Programmlader **61** hat die Funktion eines Schlüsselerzeugungsprozesses (Erzeugungsprozeß eines persönlichen Schlüssels **31**) und eines Entschlüsselungsprozesses (Entschlüsselungsprozeß **32** und **34**), und er lädt das entsprechende entschlüsselte Programm von der optischen Magnetplatte **6** in einen Hauptspeicher **63** in einem Ausführungsstadium der Programminstruktion, so daß der Ausführungszustand des Programms hergestellt wird. Der Hauptspeicher **63** ist aus einem RAM gebildet, um das Klartextprogramm zu expandieren, das der optischen Magnetplatte **6** entnommen wird.

[0075] In Fig. 10B empfängt der Programmlader **61** bei Schritt S31 die Ausführungsinstruktion für das Programm. Bei Schritt S32 lädt der Programmlader **61** ein Programm, das auszuführen ist, und entschlüsselt es. Bei Schritt S33 wird das Klartextprogramm in dem Hauptspeicher expandiert, um ein ausführbares Klartextprogramm zu erhalten. Bei Schritt S34 wird das Klartextprogramm in dem Hauptspeicher ausgeführt.

[0076] In Fig. 10C ist eine Beziehung zwischen dem Softwarespeichermedium und dem Nutzercomputer detailliert erläutert.

(1) Der Nutzercomputer entnimmt dem Softwarespeichermedium **11** die Mediennummer **12** und sendet sie zu der Erzeugungsschaltung des persönlichen Schlüssels **311**, um den verschlüsselten Medienschlüssel zu erzeugen (siehe Schritt S23 von Fig. 9).

(2) Die Entschlüsselungsschaltung **321** empfängt die Erlaubnisinformationen **13** von dem Softwarespeichermedium **13** und verschlüsselt sie auf der Basis des Medienschlüssels von der Erzeugungsschaltung **311**. Als Resultat wird der Softwareentschlüsselungsschlüssel **351** (der dem Softwareentschlüsselungsschlüssel **35** entspricht) durch die Entschlüsselungsschaltung **321** erhalten.

(3) Die Entschlüsselungsschaltung **341** empfängt die verschlüsselte Software **15** von dem Softwarespeichermedium **11** und entschlüsselt sie auf der Basis des Softwareentschlüsselungsschlüssels **351**, um das Klartextprogramm zu erzeugen, wonach das Klartextprogramm in dem Hauptspeicher **63** gespeichert wird.

[0077] Es ist unmöglich, wie oben erläutert, die verschlüsselte Software **15** zu entschlüsseln, ohne daß die Erlaubnisinformationen **13** gespeichert sind, so das es unmöglich ist, solch ein Programm auszuführen. Falls ferner das Softwarespeichermedium **11** durch einen Dritten illegal kopiert wird, ist es unmöglich, da die Mediennummer **12** nicht vorgesehen ist oder verschieden ist, den korrekten Softwareentschlüsselungsschlüssel **351** von den Erlaubnisinformationen **13** zu entschlüsseln. Als Resultat ist es unmöglich, das verschlüsselte Programm zu entschlüsseln, so daß es unmöglich ist, das Programm auszuführen. In dem Nutzercomputer werden, wie oben erläutert, ein Algorithmus und ein Geheimschlüssel in der Erzeugungsschaltung des persönlichen Schlüssels **311**, ein Softwaredecodierschlüssel und die Klartextsoftware durch ein bekanntes Sicherheitsmittel geschützt.

[0078] Fig. 11A, Fig. 11B und Fig. 11C sind erläuternde Ansichten für elektronische Daten, wie zum Beispiel Zeichendaten (Text), Symbole, Bilddaten und Tondaten. Fig. 11A zeigt eine Gesamtstruktur, Fig. 11B zeigt ein Flußdiagramm, und Fig. 11C ist eine erläuternde Ansicht, die die Ausführung der

Software zeigt.

[0079] In Fig. 11A entspricht eine optische Magnetplatte **6** dem Softwarespeichermedium **11** von Fig. 2 und Fig. 3, und sie speichert die Mediennummer **12**, die Erlaubnisinformationen **13** und die verschlüsselten Daten **17**. Der Nutzer kauft die optische Magnetplatte **6** und montiert diese Platte in eine optische Magnetvorrichtung. Andere bekannte Beispiele für Speichermedien sind eine optische Platte, eine CD-ROM, eine Diskette, eine Festplatte, ein Magnetband, ein Kassettenband und dergleichen.

[0080] Ein Lese/Schreib-(R/W)-Modul **64** hat eine Funktion eines Schlüsselerzeugungsprozesses (Erzeugungsprozeß eines persönlichen Schlüssels **31**) und eines Entschlüsselungsprozesses (Entschlüsselungsprozeß **32** und **34**) und speichert die entsprechenden entschlüsselten Daten von der optischen Magnetplatte **6** in einem Hauptspeicher **63** in einem Ausführungsstadium der Leseinstruktion. Der Hauptspeicher **63** ist aus einem RAM gebildet, um die unverschlüsselten Daten zu expandieren, die der optischen Magnetplatte **6** entnommen werden.

[0081] In Fig. 11B führt der R/W-Modul **64** bei Schritt S41 ein Anwendungsprogramm aus. Bei Schritt S42 liest der R/W-Modul **64** die Daten von der optischen Magnetplatte. Bei Schritt S43 nimmt der R/W-Modul die Daten und verschlüsselt sie. Bei Schritt S44 werden die unverschlüsselten Daten in dem Hauptspeicher **63** gespeichert. Bei Schritt S45 werden die Daten angezeigt und wiedergegeben.

[0082] In Fig. 11C wird eine Beziehung zwischen dem Datenspeichermedium und dem Nutzercomputer detailliert erläutert.

(1) Der Nutzercomputer entnimmt dem Datenspeichermedium **111** die Mediennummer **12** und sendet sie zu der Erzeugungsschaltung des persönlichen Schlüssels **311**, um den verschlüsselten Medienschlüssel zu erzeugen (siehe Schritt S23 von Fig. 9).

(2) Die Entschlüsselungsschaltung **321** empfängt die Erlaubnisinformationen **13** von dem Datenspeichermedium **111** und verschlüsselt sie auf der Basis des Medienschlüssels von der Erzeugungsschaltung **311**. Als Resultat wird der Datenentschlüsselungsschlüssel **352** (der dem Softwareentschlüsselungsschlüssel **35** entspricht) durch die Entschlüsselungsschaltung **321** erhalten.

(3) Die Entschlüsselungsschaltung **341** empfängt die verschlüsselten Daten **15** von dem Datenspeichermedium **111** und entschlüsselt sie auf der Basis des Datenentschlüsselungsschlüssels **351**, um die unverschlüsselten Daten zu erzeugen, wonach die unverschlüsselten Daten in dem Hauptspeicher **63** gespeichert werden.

[0083] Fig. 12 ist eine erläuternde Ansicht einer optischen Magnetplatte des ROM/RAM-Mischtyps. Die optische Magnetplatte des ROM/RAM-Mischtyps hat einen nichtüberschreibbaren Bereich zum Speichern der Mediennummer **12** und einen lesbaren/beschreibbaren Bereich für die Erlaubnisinformationen **13** und einen Nur-Lese-Bereich/Nur-Schreib-Bereich für die verschlüsselte Software **15**. Bei der vorliegenden Erfindung wird die Mediennummer der optischen Magnetplatte verliehen, um die Mediennummer in den nichtüberschreibbaren Bereich zu schreiben.

[0084] Fig. 13 ist eine erläuternde Ansicht der Erlaubnisinformationen, die in einem anderen Speichermedium gespeichert sind. In diesem Fall speichert das Softwarespeichermedium im voraus die Mediennummer und die verschlüsselte Software. Die Erlaubnisinformationen werden in einem anderen Speichermedium gespeichert. Dies bedeutet, daß die Mediennummer und die verschlüsselte Software (oder verschlüsselte Daten) im voraus zum Beispiel auf die CD-ROM geschrieben werden, die keinen Schreibbereich hat, und die Erlaubnisinformationen im voraus auf eine Diskette geschrieben werden.

[0085] Fig. 14 ist eine erläuternde Ansicht von multipler Software, die auf ein Speichermedium, wie zum Beispiel auf eine optische Platte und eine CD-ROM, geschrieben wird. Beim Anbieter verschlüsselt die Verschlüsselungsschaltung eine Vielzahl von Softwareentschlüsselungsschlüsseln 1 bis N auf der Basis des persönlichen Schlüssels, um eine Vielzahl von Erlaubnisinformationen 1 bis N zu erzeugen, die jeweils jedem Softwareentschlüsselungsschlüssel 1 bis N entsprechen.

[0086] Eine Vielzahl von Erlaubnisinformationen 1 bis N wird auf dem Softwarespeichermedium gespeichert.

[0087] Wenn der Nutzer einen gewünschten Softwarenamen von den verschlüsselten Arten der Software 1 bis N anfordert und diesen dem Anbieter mitteilt, verschlüsselt der Anbieter den Softwareentschlüsselungsschlüssel, der der gewünschten Software entspricht, durch den Medienschlüssel, der durch die Mediennummer erzeugt wurde, und speichert verschlüsselte Software auf dem Softwarespeichermedium **11**. Der Nutzer montiert dieses Softwarespeichermedium in den Computer, und der Nutzercomputer entschlüsselt die verschlüsselte Software, um die Klartextsoftware zu erzeugen.

[0088] Auch wenn ein Nutzer versucht, Software zu verwenden, für die er keine Erlaubnisnummer hat, kann er solche Software nicht verwenden, da die verschlüsselte Software nicht entschlüsselt werden kann. Selbst wenn der Nutzer ferner die Erlaubnisinformationen von einem anderen Softwarespeichermedium **11** kopiert, kann die Mediennummer in dem

Softwarespeichermedium nicht kopiert werden, so daß es unmöglich ist, die Software korrekt zu entschlüsseln. Daher ist es unmöglich, die Software individuell zu verkaufen.

[0089] Gemäß der vorliegenden Erfindung wird die Mediennummer **12**, wie oben erläutert, auf dem Speichermedium **1**, das die verschlüsselten elektronischen Daten speichert, in nichtüberschreibbarer Form gespeichert, und die Erlaubnis zum Verwenden der elektronischen Daten wird durch den Medienschlüssel **12** erteilt. Daher ist es möglich, nach Autorisierung durch den Anbieter nur die verschlüsselten elektronischen Daten, die in dem korrekten Medium **1** gespeichert sind, zu verwenden, so daß es möglich ist, das illegale Kopieren durch einen Dritten zu verhindern. Ferner ist es möglich, die elektronischen Daten, die in dem Speichermedium **1** gespeichert sind, zu übertragen. Des weiteren ist es möglich, dasselbe Speichermedium in einem anderen Computer zu verwenden. Außerdem ist es möglich, eine Vielzahl von elektronischen Daten in einem Medium zu speichern. Darüber hinaus ist es möglich, das Speichermedium individuell zu verkaufen.

Patentansprüche

1. Schutzsystem für elektronische Daten zum Identifizieren der Quelle des illegalen Kopierens von elektronischen Daten durch einen Dritten, welches System umfaßt:
ein Speichermedium (**1**, **11**) zum Speichern von verschlüsselten elektronischen Daten (**14**, **15**), einer Mediennummer (**12**) und von verschlüsselten Erlaubnisinformationen (**13**);
einen Anbietercomputer mit einem Erzeugungsmittel eines persönlichen Schlüssels (**21**) zum Erzeugen eines Medienschlüssels auf der Basis der Mediennummer (**12**), einem Entschlüsselungsschlüssel der elektronischen Daten (**22**, **24**) und einem Verschlüsselungsmittel (**23**) zum Verschlüsseln des Entschlüsselungsschlüssels der elektronischen Daten (**22**, **24**) auf der Basis des Medienschlüssels, um die verschlüsselten Erlaubnisinformationen (**13**) zu erzeugen; und
einen Nutzercomputer mit einem Erzeugungsmittel eines persönlichen Schlüssels (**31**) zum Erzeugen eines Medienschlüssels auf der Basis der Mediennummer (**12**), einem ersten Entschlüsselungsmittel (**32**) zum Entschlüsseln der verschlüsselten Erlaubnisinformationen (**13**) auf der Basis des Medienschlüssels, um einen Original-Entschlüsselungsschlüssel der elektronischen Daten (**33**, **35**) zu erzeugen, der derselbe wie der Entschlüsselungsschlüssel der elektronischen Daten (**22**, **24**) des Anbietercomputers ist, und einem zweiten Entschlüsselungsmittel (**34**) zum Entschlüsseln der verschlüsselten elektronischen Daten (**14**, **15**) auf der Basis des Original-Entschlüsselungsschlüssels der elektronischen Daten (**33**, **35**), um elektronische Klartextdaten zu erzeugen, bei dem die Mediennummer (**12**) nur für das entsprechende Speichermedium auf dem genannten Speichermedium in nichtüberschreibbarer Form vorgesehen wird und das **dadurch gekennzeichnet** ist, daß die Mediennummer durch den Nutzercomputer geschrieben wird und das Speichermedium eine optische Magnetplatte, eine optische Platte, eine CD-ROM, eine Diskette, ein Magnetband oder ein Kassettenband ist; wodurch die Verwendung desselben Speichermediums in einem anderen Computer zulässig ist.

2. Schutzsystem für elektronische Daten nach Anspruch 1, bei dem die elektronischen Daten Software sind, die für einen Computer verwendet wird.

3. Schutzsystem für elektronische Daten nach Anspruch 1, bei dem die elektronischen Daten elektronisch veröffentlichte Daten sind.

4. Schutzsystem für elektronische Daten nach Anspruch 1, bei dem das Speichermedium (**1**, **11**) eine Vielzahl der verschlüsselten elektronischen Daten (**14**, **15**) speichert und die verschlüsselten elektronischen Daten (**14**, **15**) jeweilig einen verschiedenen Entschlüsselungsschlüssel der elektronischen Daten haben; der Anbietercomputer nur den Entschlüsselungsschlüssel der elektronischen Daten von den verschlüsselten elektronischen Daten (**14**, **15**), autorisiert durch einen Anbieter, unter Verwendung des Medienschlüssels verschlüsselt, und den verschlüsselten Entschlüsselungsschlüssel der elektronischen Daten (**13**) auf dem Speichermedium (**1**, **11**) als die verschlüsselten Erlaubnisinformationen (**13**) speichert; und der Nutzercomputer die verschlüsselten elektronischen Daten (**14**, **15**) entsprechend den verschlüsselten Erlaubnisinformationen (**13**) entschlüsselt.

5. Schutzsystem für elektronische Daten nach Anspruch 1, bei dem der Anbietercomputer die verschlüsselten Erlaubnisinformationen (**13**) auf einem anderen, verschiedenen Speichermedium speichert und das verschiedene Speichermedium zur Verwendung in dem Nutzercomputer geliefert wird.

6. Schutzsystem für elektronische Daten nach Anspruch 1, bei dem die Anbietervorrichtung die verschlüsselten Erlaubnisinformationen (**13**) über eine Übertragungsleitung zu dem Nutzercomputer überträgt und die Nutzervorrichtung die verschlüsselten elektronischen Daten (**14**, **15**) von dem Speichermedium (**1**, **11**) auf der Basis der verschlüsselten Erlaubnisinformationen (**13**) entschlüsselt.

7. Schutzsystem für elektronische Daten nach Anspruch 1, bei dem der Anbietercomputer die verschlüsselten Erlaubnisinformationen (**13**) in einem Dokument zu dem Nutzer sendet und die Nutzervorrichtung die verschlüsselten elektronischen Daten

(**14**, **15**) von dem Speichermedium auf der Basis der verschlüsselten Erlaubnisinformationen (**13**) entschlüsselt, die in dem Dokument beschrieben sind.

8. Schutzsystem für elektronische Daten nach Anspruch 1, bei dem der Anbietercomputer ferner eine Software-Verschlüsselungsschlüssel-Verwaltungstabelle (**4**) umfaßt, die Softwarenamen und Verschlüsselungsschlüssel enthält, die jeweils jedem der Softwarenamen entsprechen.

9. Schutzsystem für elektronische Daten nach Anspruch 1, bei dem der Nutzercomputer ferner eine Software-Entschlüsselungsschlüssel-Verwaltungstabelle (**5**) umfaßt, die Softwarenamen und Entschlüsselungsschlüssel enthält, die jeweils jedem der Softwarenamen entsprechen.

Es folgen 21 Blatt Zeichnungen

Anhängende Zeichnungen

Fig. 1

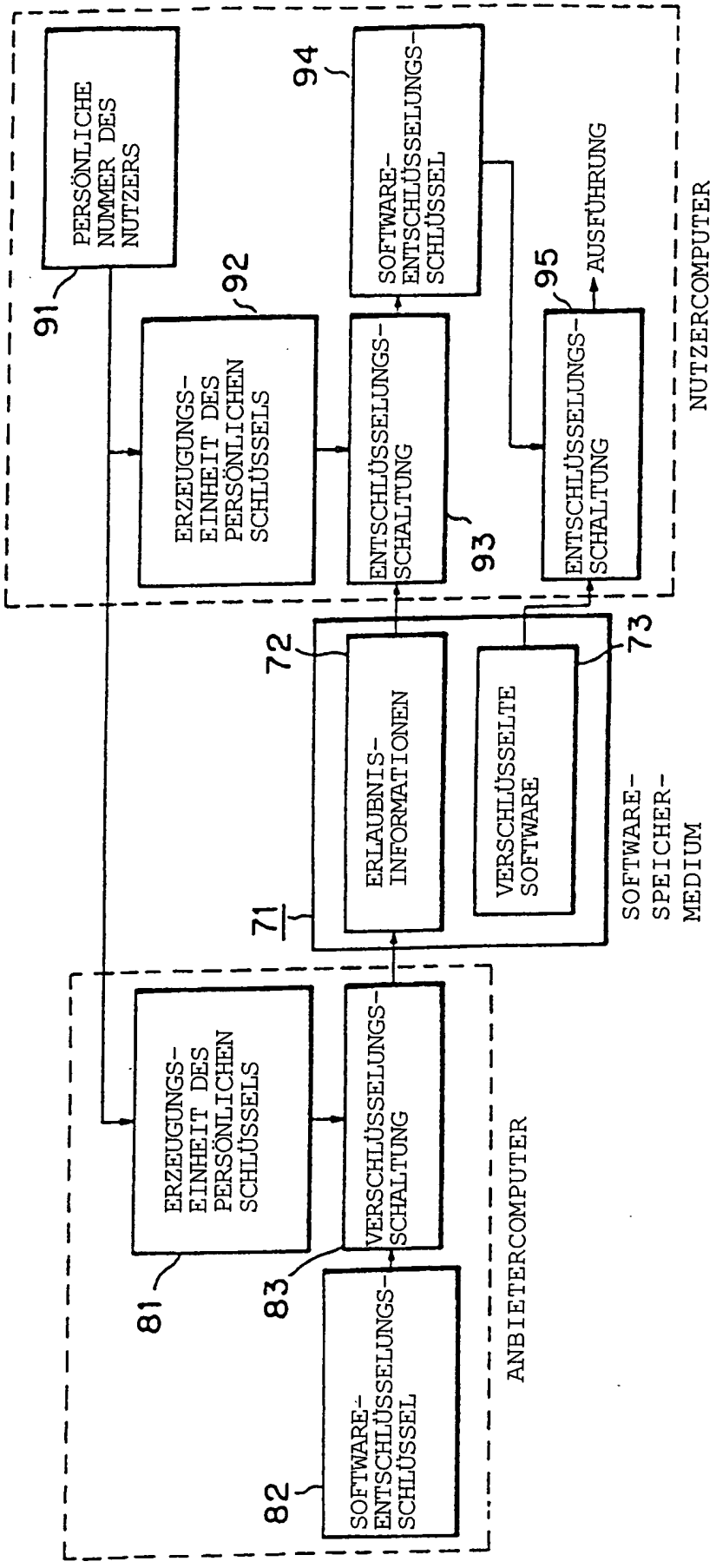


Fig. 2

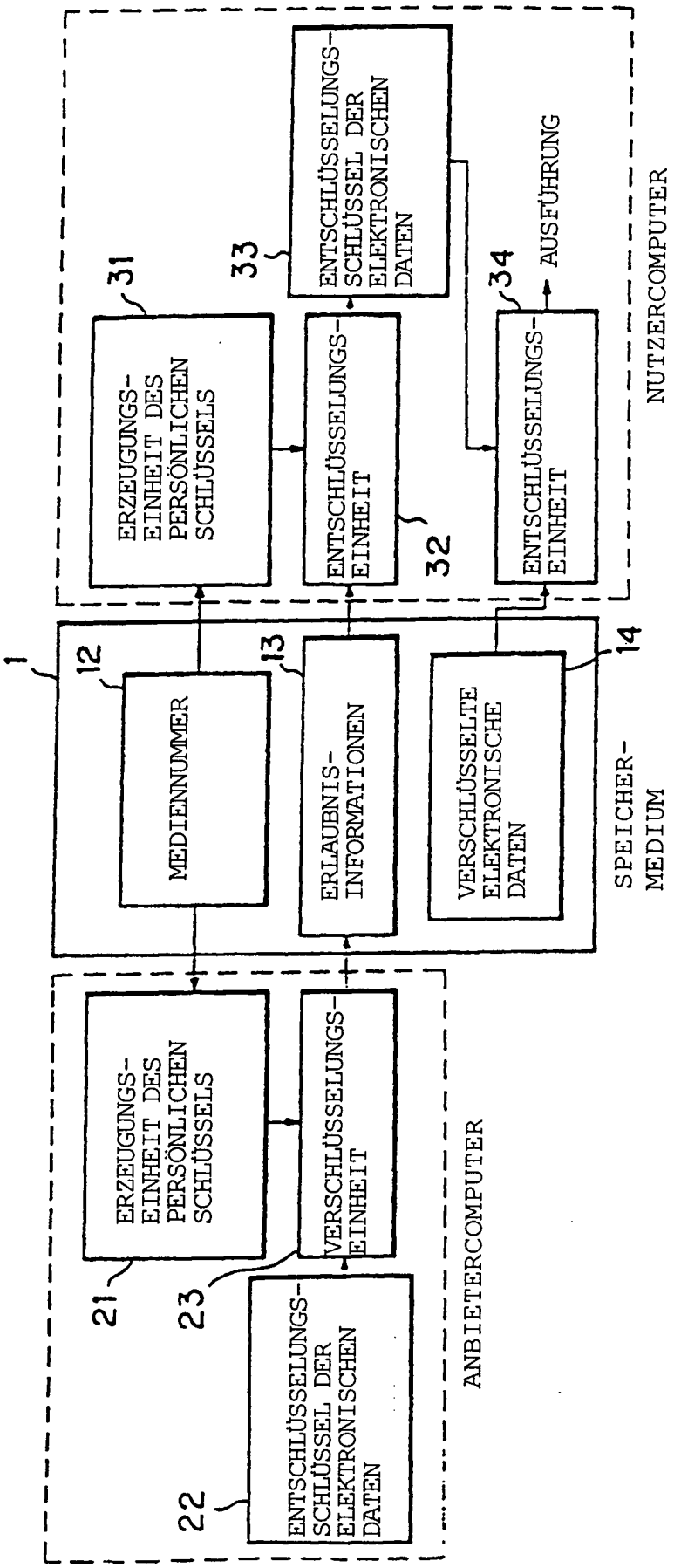

ANBIETERCOMPUTER
ERZEUGUNGS-EINHEIT DES PERSÖNLICHEN SCHLÜSSELS
21
VERSCHLÜSSELUNGS-EINHEIT
23
ENTSCHLÜSSELUNGS-SCHLÜSSEL DER ELEKTRONISCHEN DATEN
22
1
SPEICHER-MEDIUM
MEDIENNUMMER
12
ERLAUBNIS-INFORMATIONEN
13
VERSCHLÜSSELTE ELEKTRONISCHE DATEN
14
NUTZERCOMPUTER
ERZEUGUNGS-EINHEIT DES PERSÖNLICHEN SCHLÜSSELS
31
ENTSCHLÜSSELUNGS-EINHEIT
32
ENTSCHLÜSSELUNGS-SCHLÜSSEL DER ELEKTRONISCHEN DATEN
33
ENTSCHLÜSSELUNGS-EINHEIT
34
AUSFÜHRUNG

Fig. 3

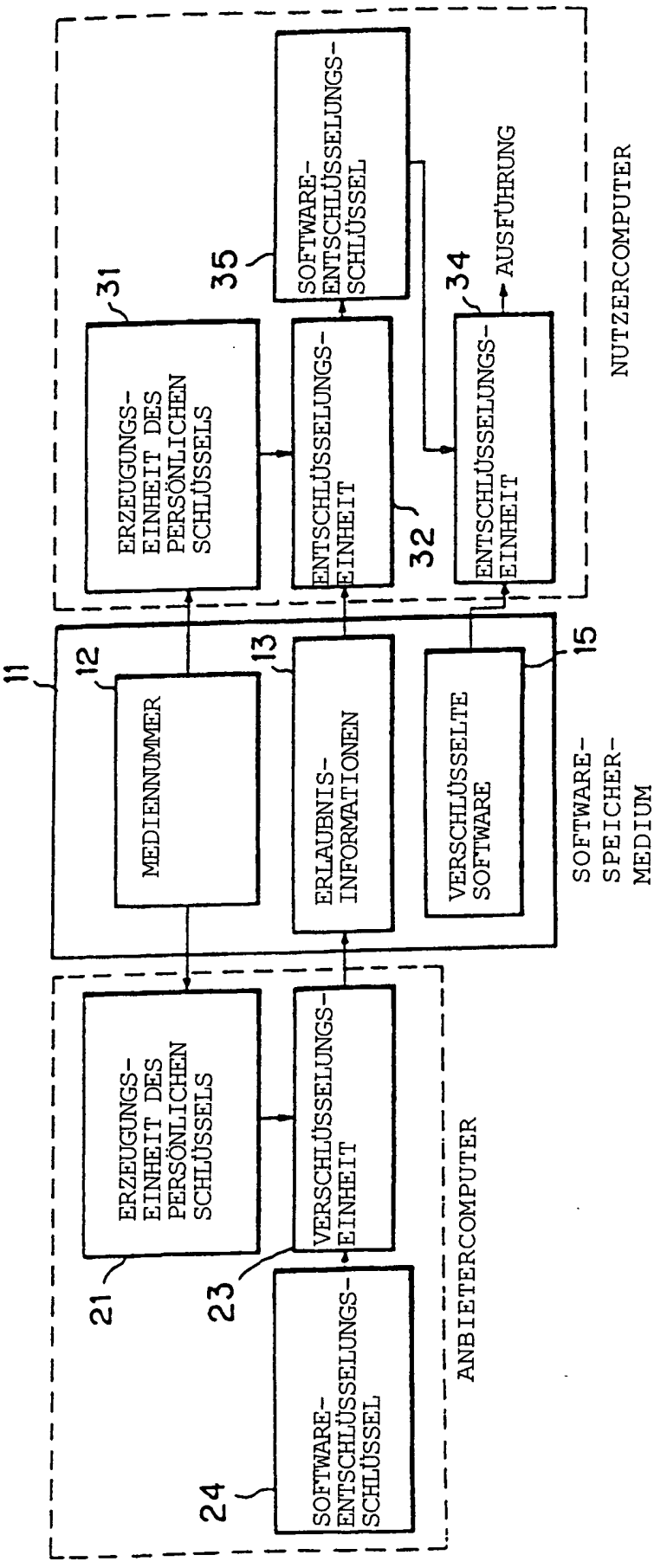

NUTZERCOMPUTER
ERZEUGUNGS-EINHEIT DES PERSÖNLICHEN SCHLÜSSELS
31
SOFTWARE-ENTSCHLÜSSELUNGS-SCHLÜSSEL
35
ENTSCHLÜSSELUNGS-EINHEIT
32
ENTSCHLÜSSELUNGS-EINHEIT
34
AUSFÜHRUNG
11
MEDIENNUMMER
12
ERLAUBNIS-INFORMATIONEN
13
VERSCHLÜSSELTE SOFTWARE
15
SOFTWARE-SPEICHER-MEDIUM
ERZEUGUNGS-EINHEIT DES PERSÖNLICHEN SCHLÜSSELS
21
VERSCHLÜSSELUNGS-EINHEIT
23
SOFTWARE-ENTSCHLÜSSELUNGS-SCHLÜSSEL
24
ANBIETERCOMPUTER

Fig. 4

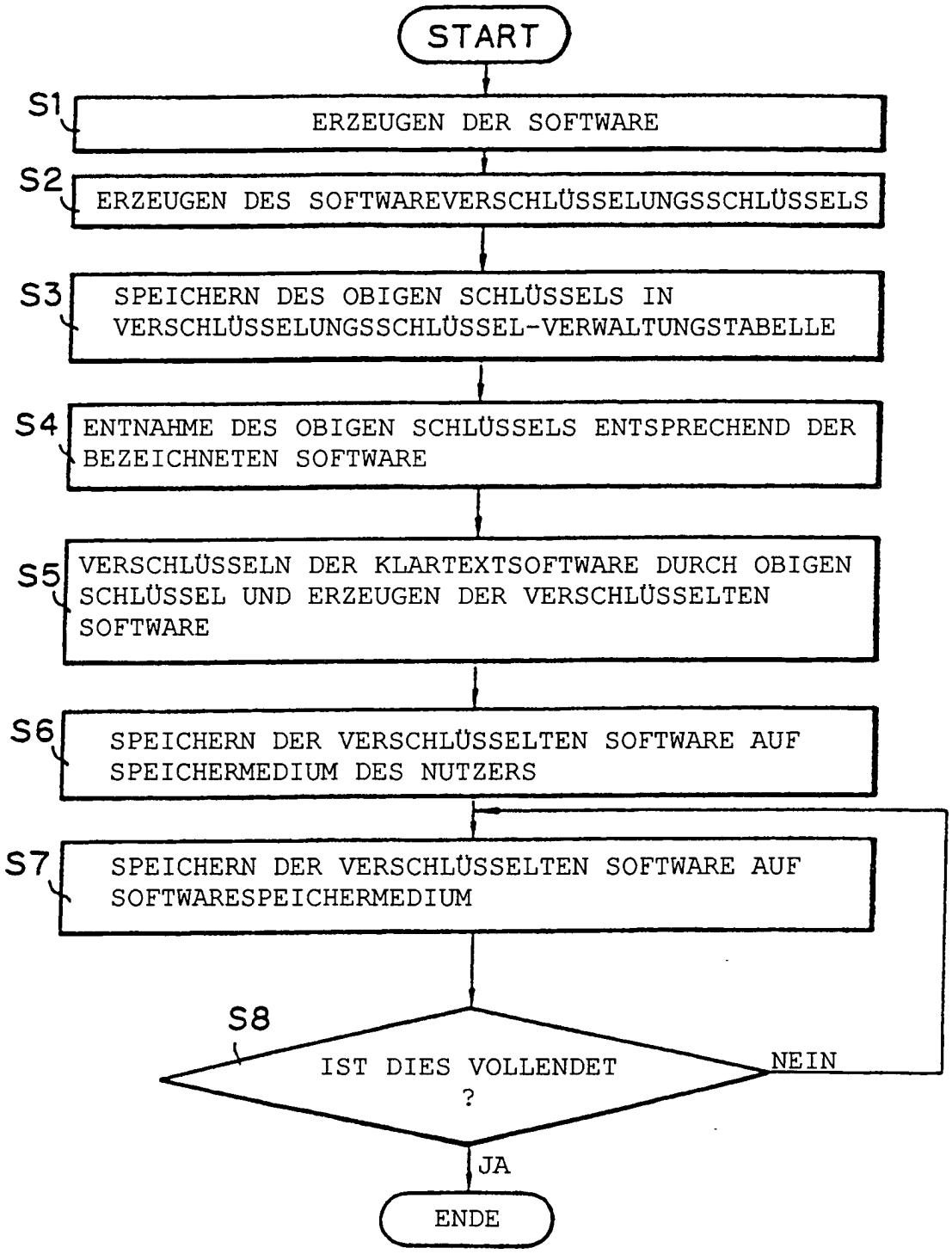

START
S1
ERZEUGEN DER SOFTWARE
S2
ERZEUGEN DES SOFTWAREVERSCHLÜSSELUNGSSCHLÜSSELS
S3
SPEICHERN DES OBIGEN SCHLÜSSELS IN VERSCHLÜSSELUNGSSCHLÜSSEL-VERWALTUNGSTABELLE
S4
ENTNAHME DES OBIGEN SCHLÜSSELS ENTSPRECHEND DER BEZEICHNETEN SOFTWARE
S5
VERSCHLÜSSELN DER KLARTEXTSOFTWARE DURCH OBIGEN SCHLÜSSEL UND ERZEUGEN DER VERSCHLÜSSELTEN SOFTWARE
S6
SPEICHERN DER VERSCHLÜSSELTEN SOFTWARE AUF SPEICHERMEDIUM DES NUTZERS
S7
SPEICHERN DER VERSCHLÜSSELTEN SOFTWARE AUF SOFTWARESPEICHERMEDIUM
S8
IST DIES VOLLENDET ?
NEIN
JA
ENDE

Fig. 5A

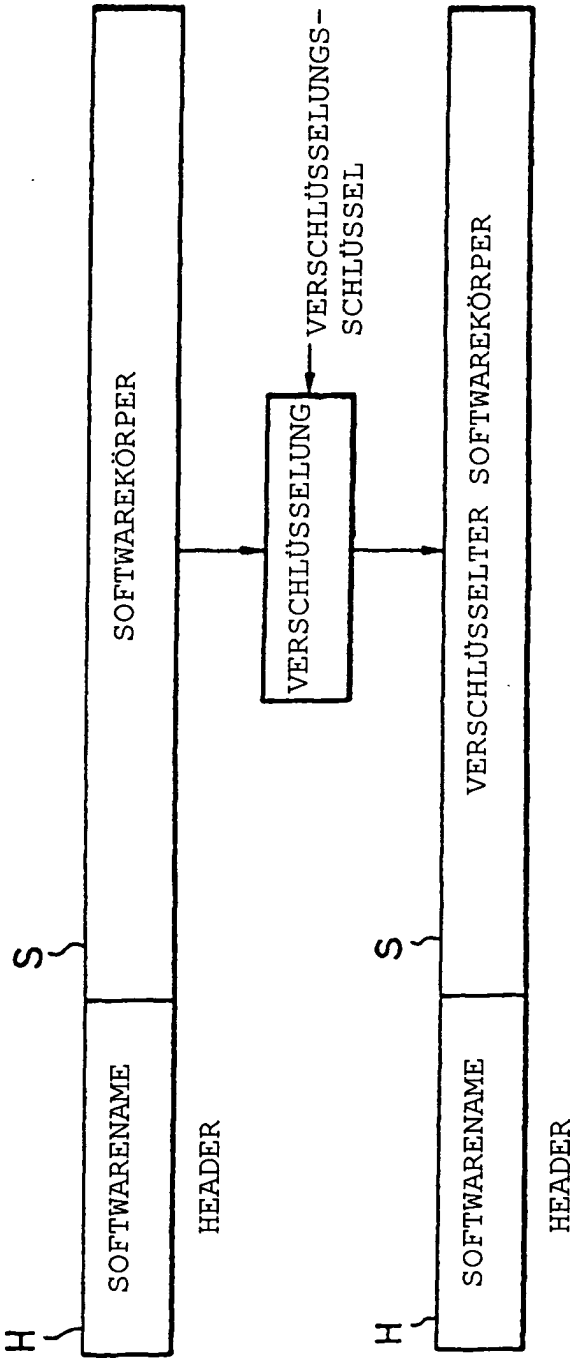

H
SOFTWARENAME
HEADER
S
SOFTWAREKÖRPER
VERSCHLÜSSELUNG
VERSCHLÜSSELUNGS-
SCHLÜSSEL
H
SOFTWARENAME
HEADER
S
VERSCHLÜSSELTER SOFTWAREKÖRPER

Fig. 5B

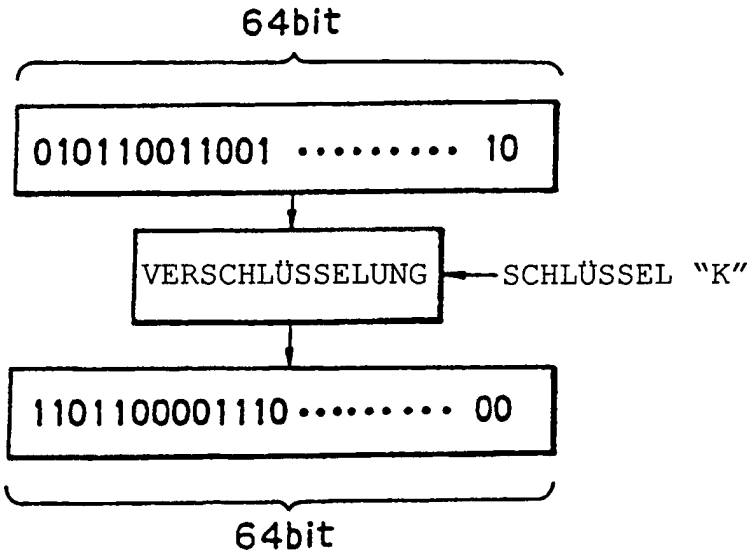

64bit
010110011001 10
VERSCHLÜSSELUNG
SCHLÜSSEL "K"
1101100001110 00
64bit

Fig. 6

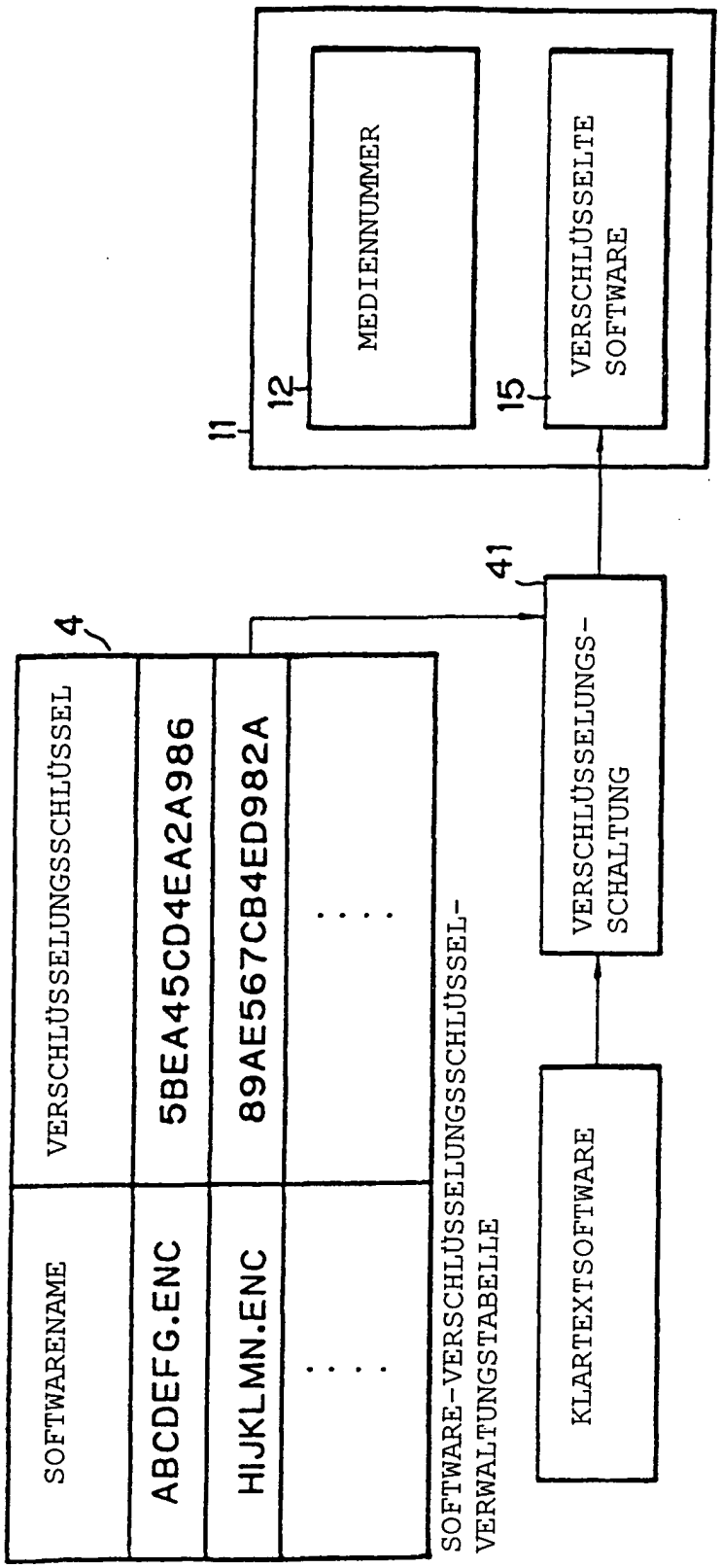

11
12
MEDIENNUMMER
15
VERSCHLÜSSELTE SOFTWARE
41
VERSCHLÜSSELUNGS-SCHALTUNG
KLARTEXTSOFTWARE
4
SOFTWARENAME
VERSCHLÜSSELUNGSSCHLÜSSEL
ABCDEFG.ENC
5BEA45CD4EA2A986
HIJKLMN.ENC
89AE567CB4ED982A
SOFTWARE-VERSCHLÜSSELUNGSSCHLÜSSEL-VERWALTUNGSTABELLE

Fig. 7A

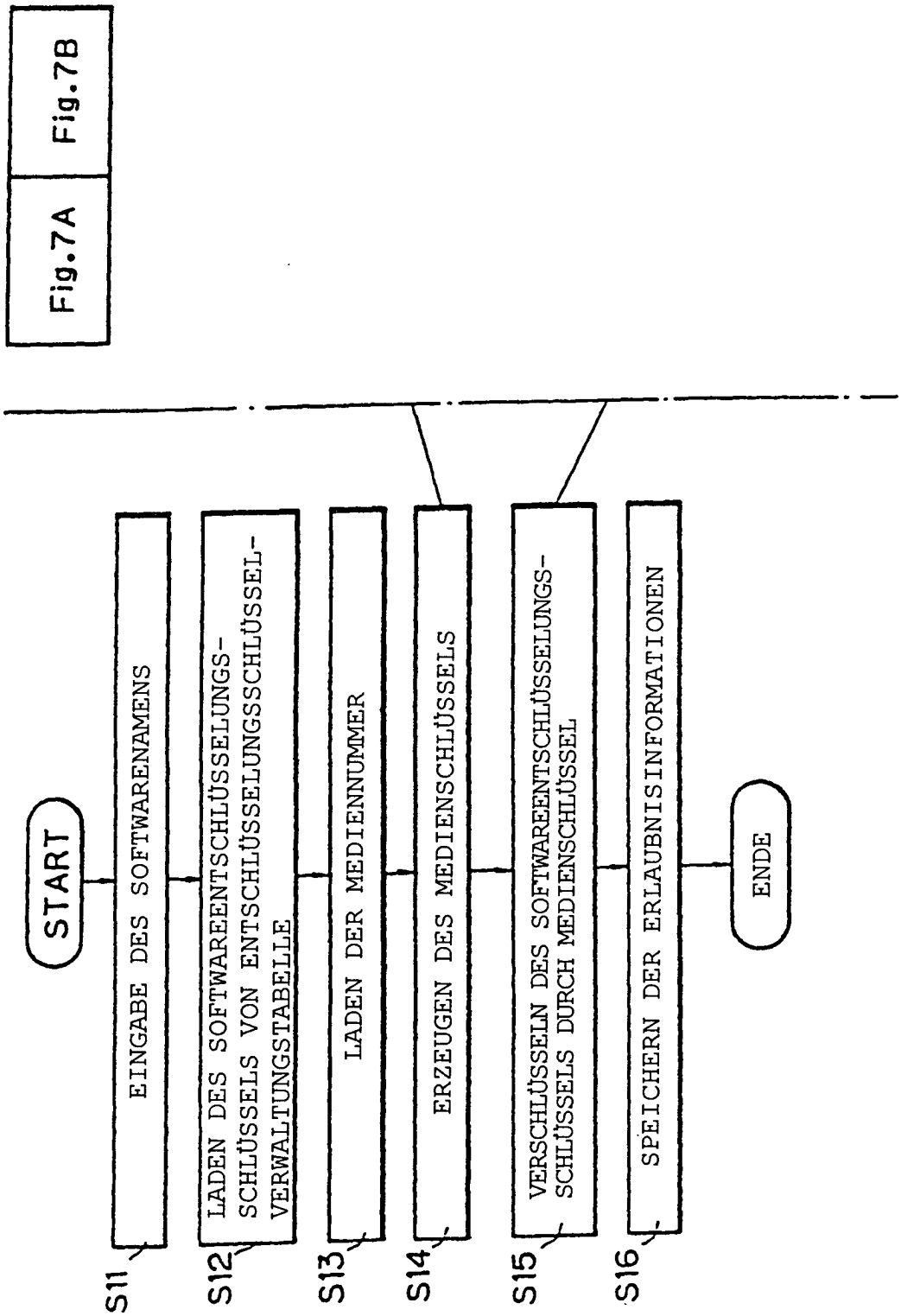

Fig.7
Fig.7A
Fig.7B
START
EINGABE DES SOFTWARENAMENS
LADEN DES SOFTWAREENTSCHLÜSSELUNGS-SCHLÜSSELS VON ENTSCHLÜSSELUNGSSCHLÜSSEL-VERWALTUNGSTABELLE
LADEN DER MEDIENNUMMER
ERZEUGEN DES MEDIENSCHLÜSSELS
VERSCHLÜSSELN DES SOFTWAREENTSCHLÜSSELUNGS-SCHLÜSSELS DURCH MEDIENSCHLÜSSEL
SPEICHERN DER ERLAUBNISINFORMATIONEN
ENDE
S11
S12
S13
S14
S15
S16

Fig. 7B

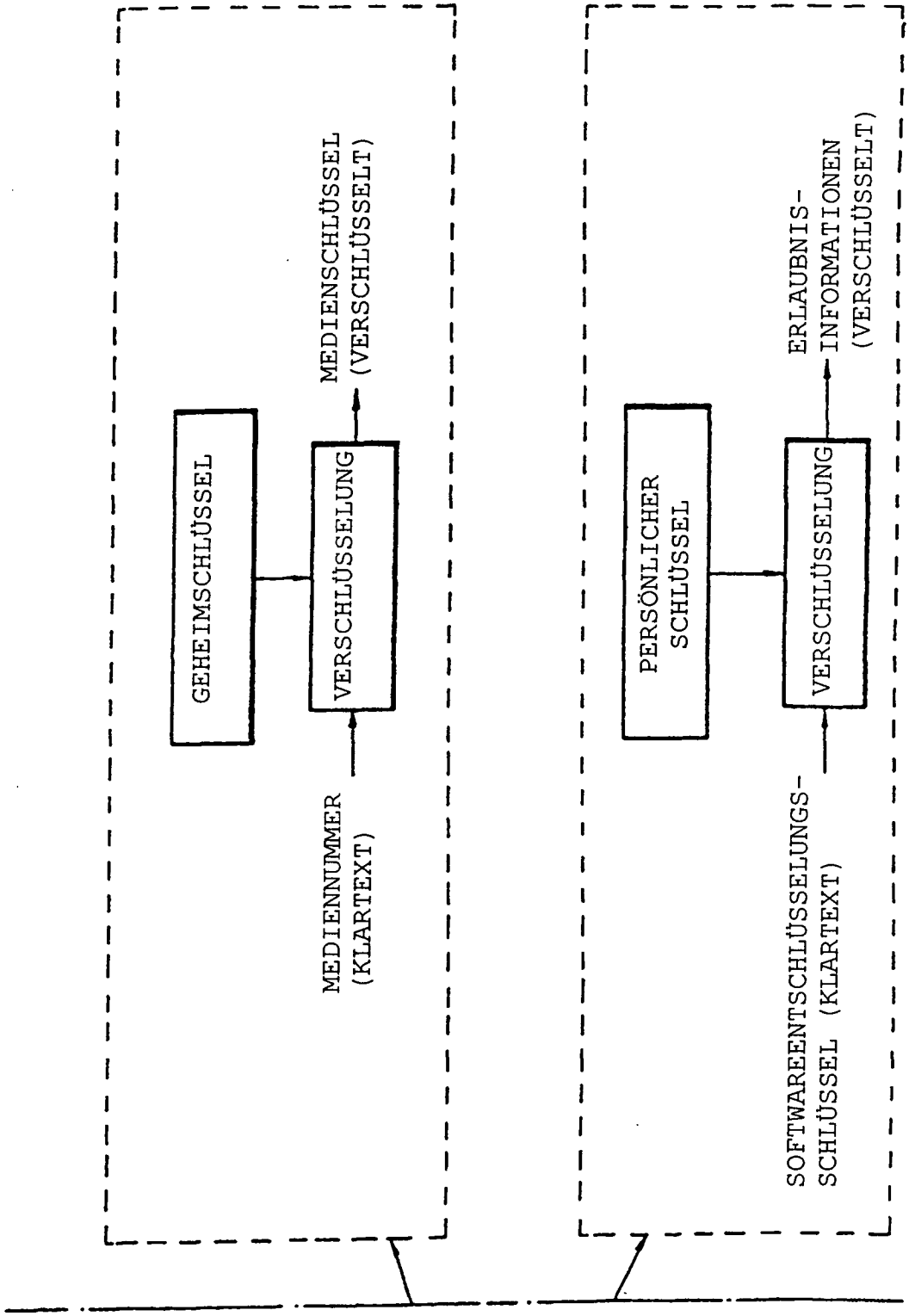

GEHEIMSCHLÜSSEL
VERSCHLÜSSELUNG
MEDIENSCHLÜSSEL (VERSCHLÜSSELT)
MEDIENNUMMER (KLARTEXT)
PERSÖNLICHER SCHLÜSSEL
VERSCHLÜSSELUNG
ERLAUBNIS-INFORMATIONEN (VERSCHLÜSSELT)
SOFTWAREENTSCHLÜSSELUNGS-SCHLÜSSEL (KLARTEXT)

Fig. 8

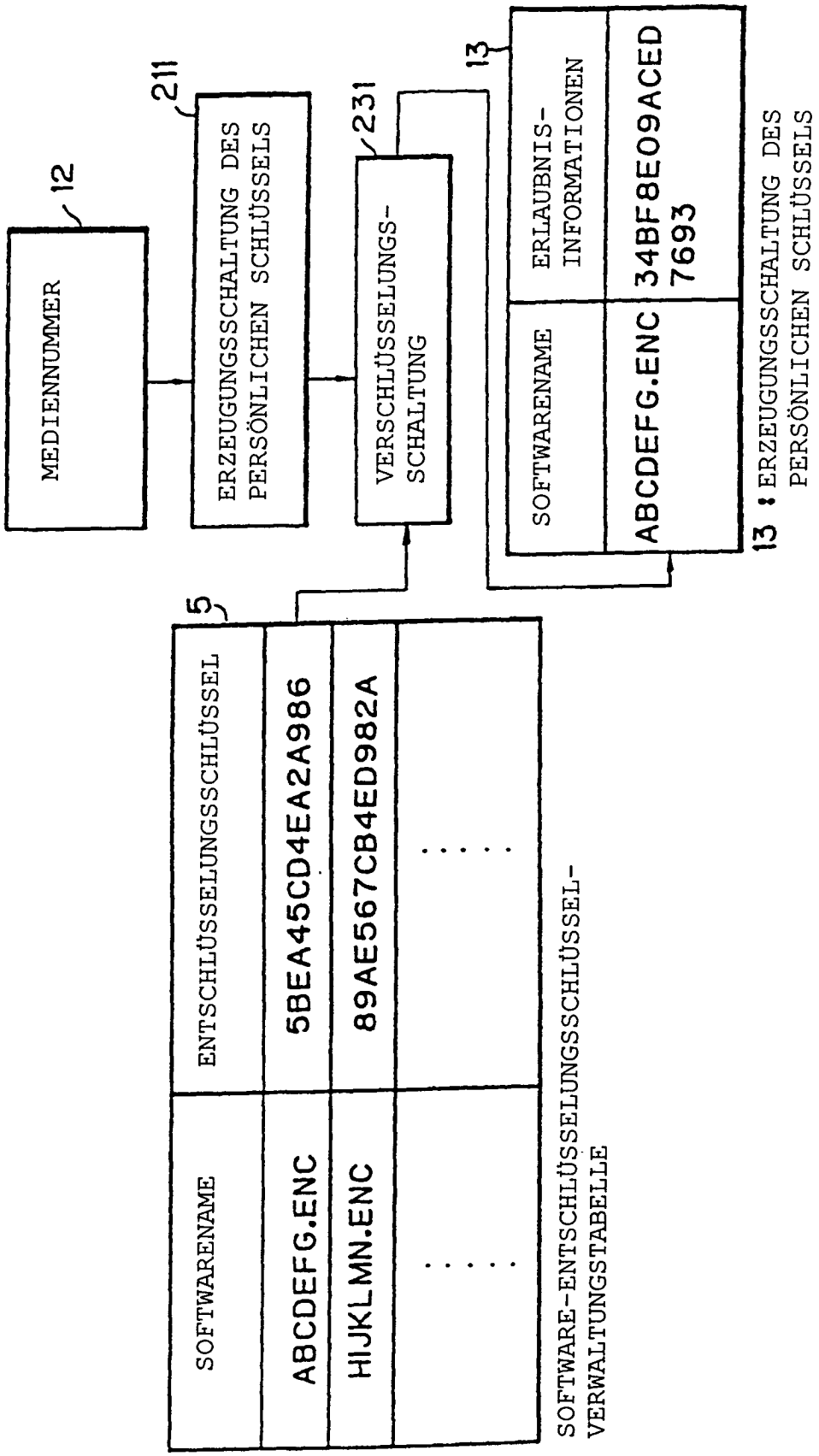

MEDIENNUMMER
12
ERZEUGUNGSSCHALTUNG DES PERSÖNLICHEN SCHLÜSSELS
211
VERSCHLÜSSELUNGS-SCHALTUNG
231
13
SOFTWARENAME
ERLAUBNIS-INFORMATIONEN
ABCDEFG.ENC
34BF8E09ACED7693
13 : ERZEUGUNGSSCHALTUNG DES PERSÖNLICHEN SCHLÜSSELS
5
SOFTWARENAME
ENTSCHLÜSSELUNGSSCHLÜSSEL
ABCDEFG.ENC
5BEA45CD4EA2A986
HIJKLMN.ENC
89AE567CB4ED982A
SOFTWARE-ENTSCHLÜSSELUNGSSCHLÜSSEL-VERWALTUNGSTABELLE

Fig.9

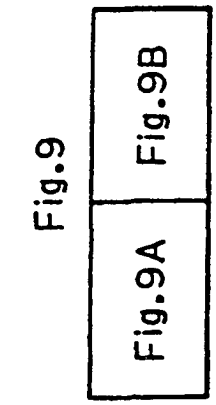

Fig.9A
Fig.9B

Fig. 9A

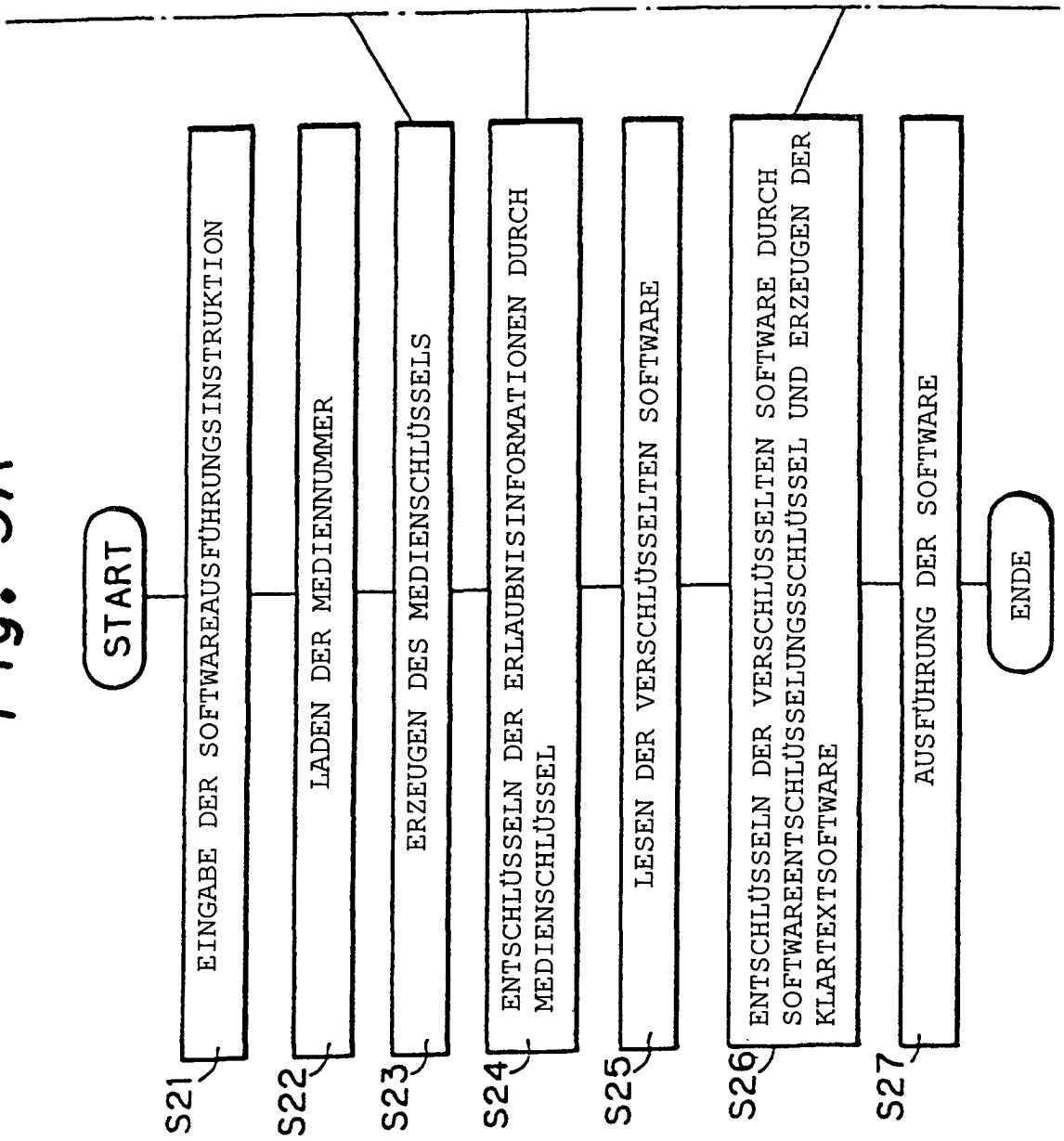

START
EINGABE DER SOFTWAREAUSFÜHRUNGSINSTRUKTION
LADEN DER MEDIENNUMMER
ERZEUGEN DES MEDIENSCHLÜSSELS
ENTSCHLÜSSELN DER ERLAUBNISINFORMATIONEN DURCH MEDIENSCHLÜSSEL
LESEN DER VERSCHLÜSSELTEN SOFTWARE
ENTSCHLÜSSELN DER VERSCHLÜSSELTEN SOFTWARE DURCH SOFTWAREENTSCHLÜSSELUNGSSCHLÜSSEL UND ERZEUGEN DER KLARTEXTSOFTWARE
AUSFÜHRUNG DER SOFTWARE
ENDE
S21
S22
S23
S24
S25
S26
S27

Fig. 9B

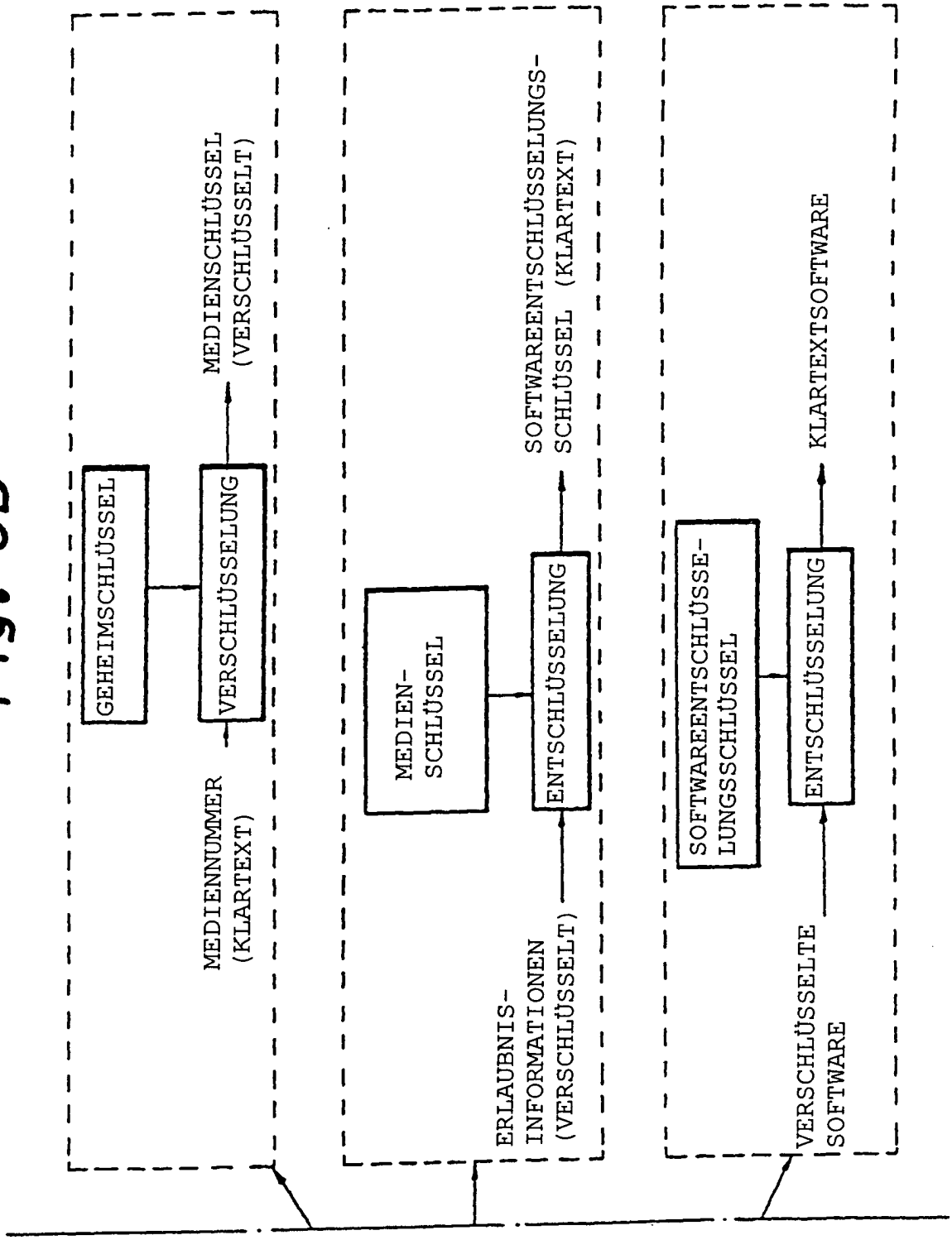

GEHEIMSCHLÜSSEL
VERSCHLÜSSELUNG
MEDIENSCHLÜSSEL (VERSCHLÜSSELT)
MEDIENNUMMER (KLARTEXT)
MEDIEN-SCHLÜSSEL
ENTSCHLÜSSELUNG
SOFTWAREENTSCHLÜSSELUNGS-SCHLÜSSEL (KLARTEXT)
ERLAUBNIS-INFORMATIONEN (VERSCHLÜSSELT)
SOFTWAREENTSCHLÜSSE-LUNGSSCHLÜSSEL
ENTSCHLÜSSELUNG
KLARTEXTSOFTWARE
VERSCHLÜSSELTE SOFTWARE

Fig. 10A

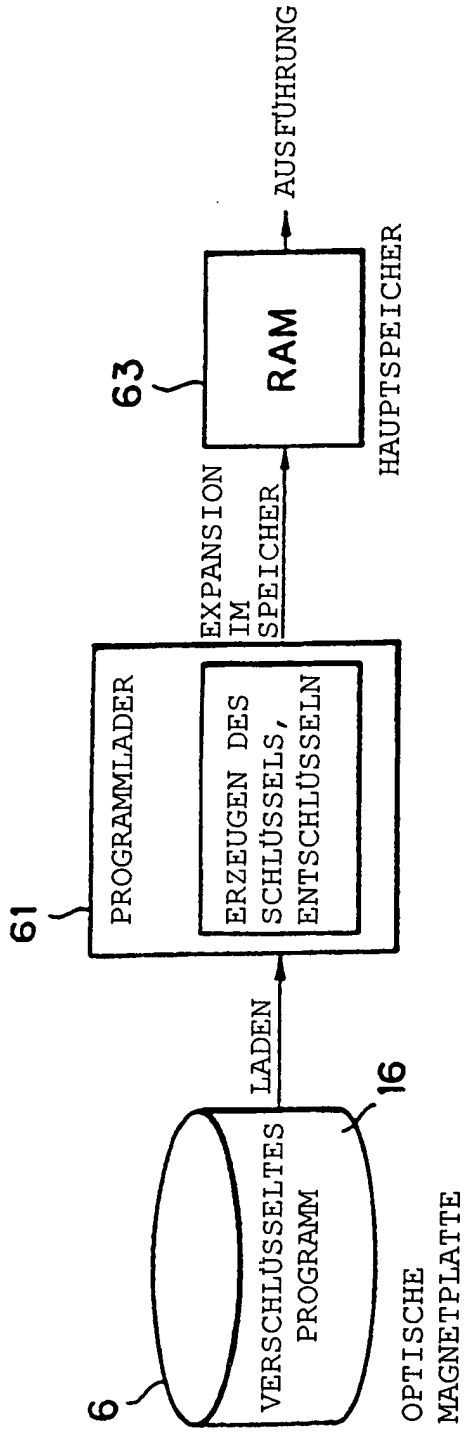

6
VERSCHLÜSSELTES PROGRAMM
OPTISCHE MAGNETPLATTE
16
LADEN
61
PROGRAMMLADER
ERZEUGEN DES SCHLÜSSELS, ENTSCHLÜSSELN
EXPANSION IM SPEICHER
63
RAM
HAUPTSPEICHER
AUSFÜHRUNG

Fig. 10B

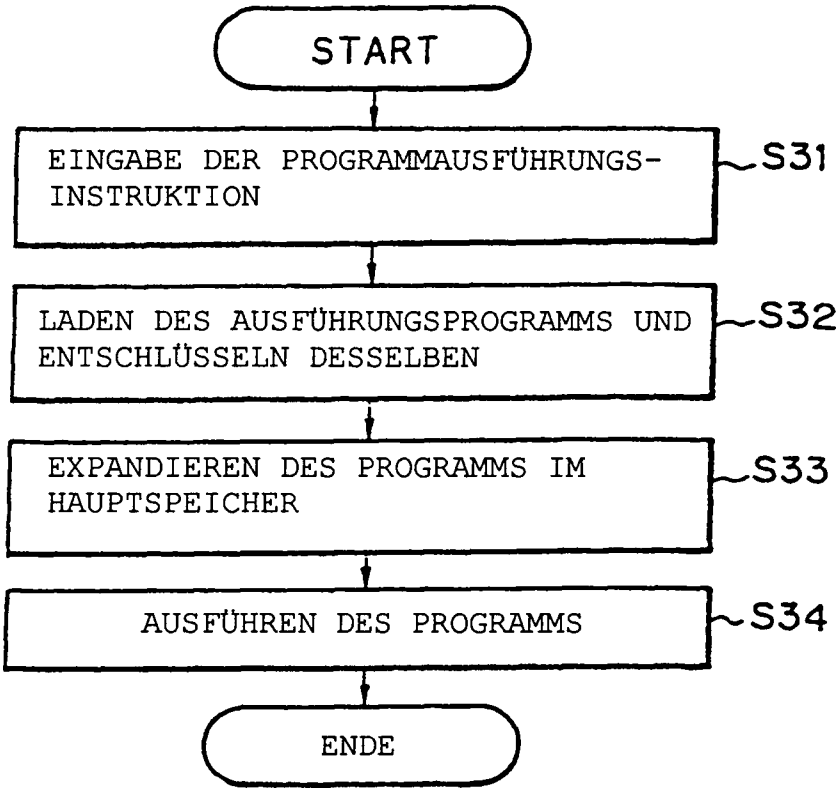

START
EINGABE DER PROGRAMMAUSFÜHRUNGS-INSTRUKTION
S31
LADEN DES AUSFÜHRUNGSPROGRAMMS UND ENTSCHLÜSSELN DESSELBEN
S32
EXPANDIEREN DES PROGRAMMS IM HAUPTSPEICHER
S33
AUSFÜHREN DES PROGRAMMS
S34
ENDE

Fig. 10C

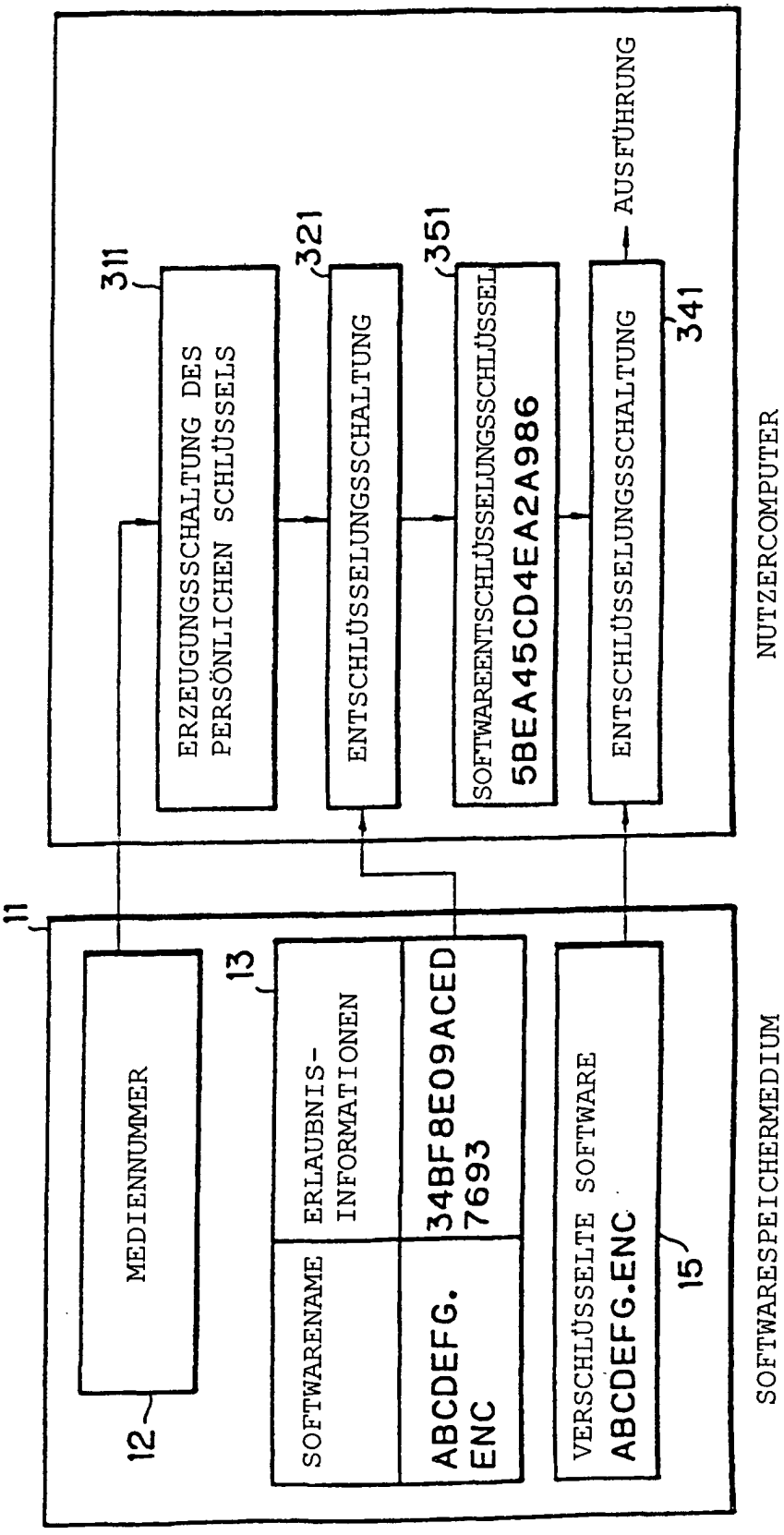

NUTZERCOMPUTER
311
ERZEUGUNGSSCHALTUNG DES PERSÖNLICHEN SCHLÜSSELS
321
ENTSCHLÜSSELUNGSSCHALTUNG
351
SOFTWAREENTSCHLÜSSELUNGSSCHLÜSSEL
5BEA45CD4EA2A986
AUSFÜHRUNG
341
ENTSCHLÜSSELUNGSSCHALTUNG
11
MEDIENNUMMER
12
13
SOFTWARENAME
ABCDEFG.ENC
ERLAUBNIS-INFORMATIONEN
34BF8E09ACED7693
VERSCHLÜSSELTE SOFTWARE
ABCDEFG.ENC
15
SOFTWARESPEICHERMEDIUM

Fig. 11A

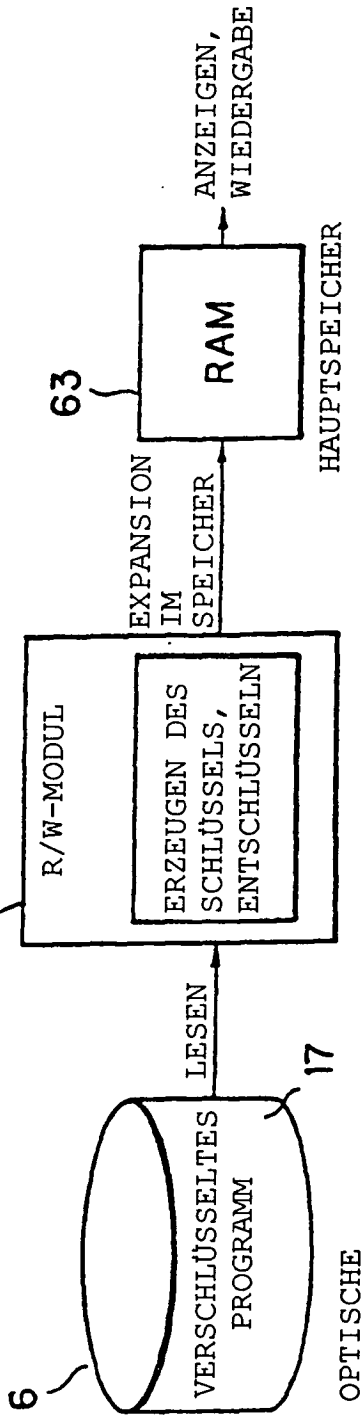

ANZEIGEN,
WIEDERGABE
63
RAM
HAUPTSPEICHER
EXPANSION
IM
SPEICHER
64
R/W-MODUL
ERZEUGEN DES
SCHLÜSSELS,
ENTSCHLÜSSELN
LESEN
17
VERSCHLÜSSELTES
PROGRAMM
6
OPTISCHE
MAGNETPLATTE

Fig. 11B

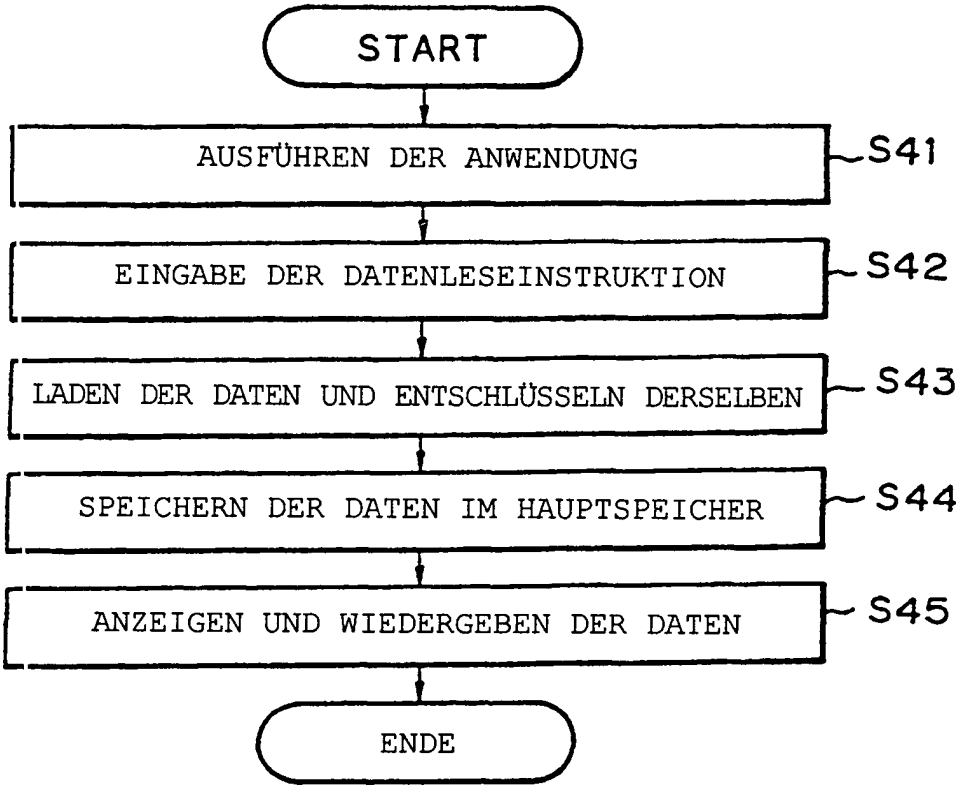

START
AUSFÜHREN DER ANWENDUNG
S41
EINGABE DER DATENLESEINSTRUKTION
S42
LADEN DER DATEN UND ENTSCHLÜSSELN DERSELBEN
S43
SPEICHERN DER DATEN IM HAUPTSPEICHER
S44
ANZEIGEN UND WIEDERGEBEN DER DATEN
S45
ENDE

Fig. 11C

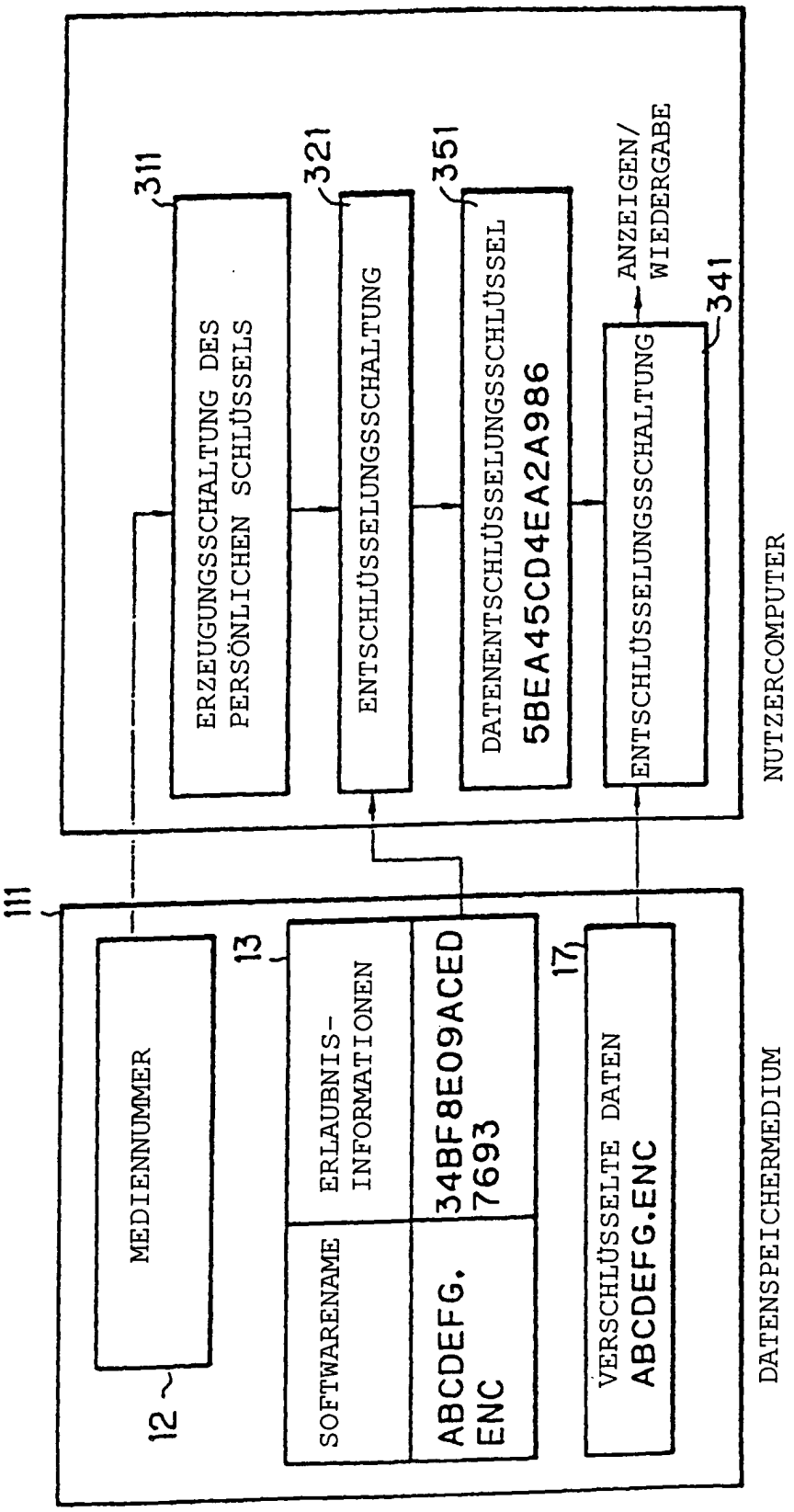

111
MEDIENNUMMER
12
13
SOFTWARENAME
ABCDEFG.
ENC
ERLAUBNIS-
INFORMATIONEN
34BF8E09ACED
7693
17
VERSCHLÜSSELTE DATEN
ABCDEFG.ENC
DATENSPEICHERMEDIUM
311
ERZEUGUNGSSCHALTUNG DES
PERSÖNLICHEN SCHLÜSSELS
321
ENTSCHLÜSSELUNGSSCHALTUNG
351
DATENENTSCHLÜSSELUNGSSCHLÜSSEL
5BEA45CD4EA2A986
ENTSCHLÜSSELUNGSSCHALTUNG
341
ANZEIGEN/
WIEDERGABE
NUTZERCOMPUTER

Fig. 12

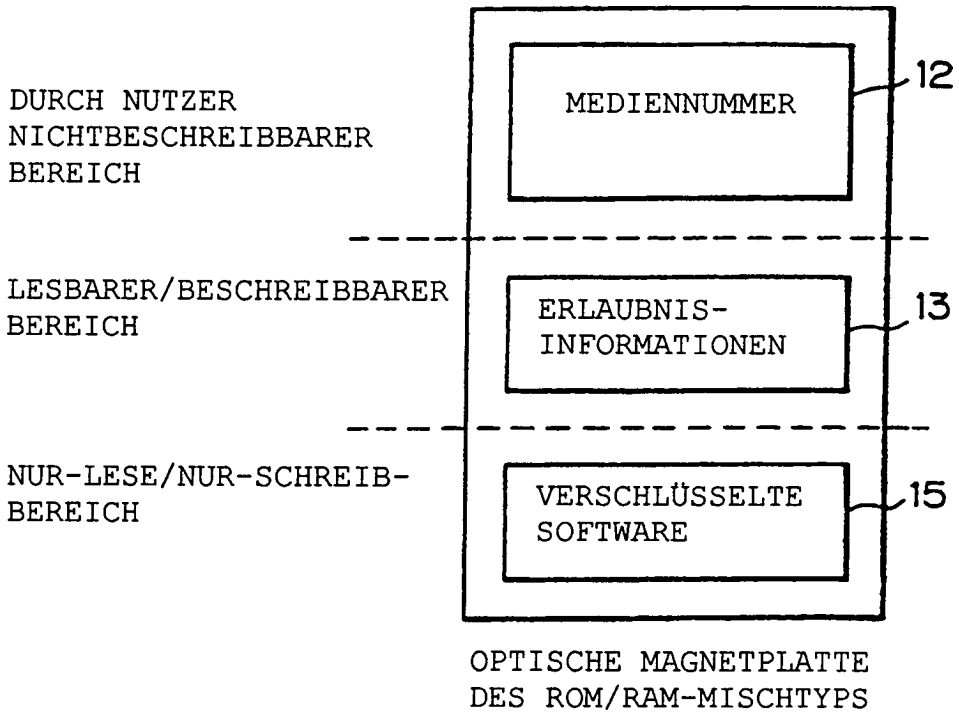

DURCH NUTZER NICHTBESCHREIBBARER BEREICH
MEDIENNUMMER
12
LESBARER/BESCHREIBBARER BEREICH
ERLAUBNIS-INFORMATIONEN
13
NUR-LESE/NUR-SCHREIB-BEREICH
VERSCHLÜSSELTE SOFTWARE
15
OPTISCHE MAGNETPLATTE DES ROM/RAM-MISCHTYPS

Fig. 13

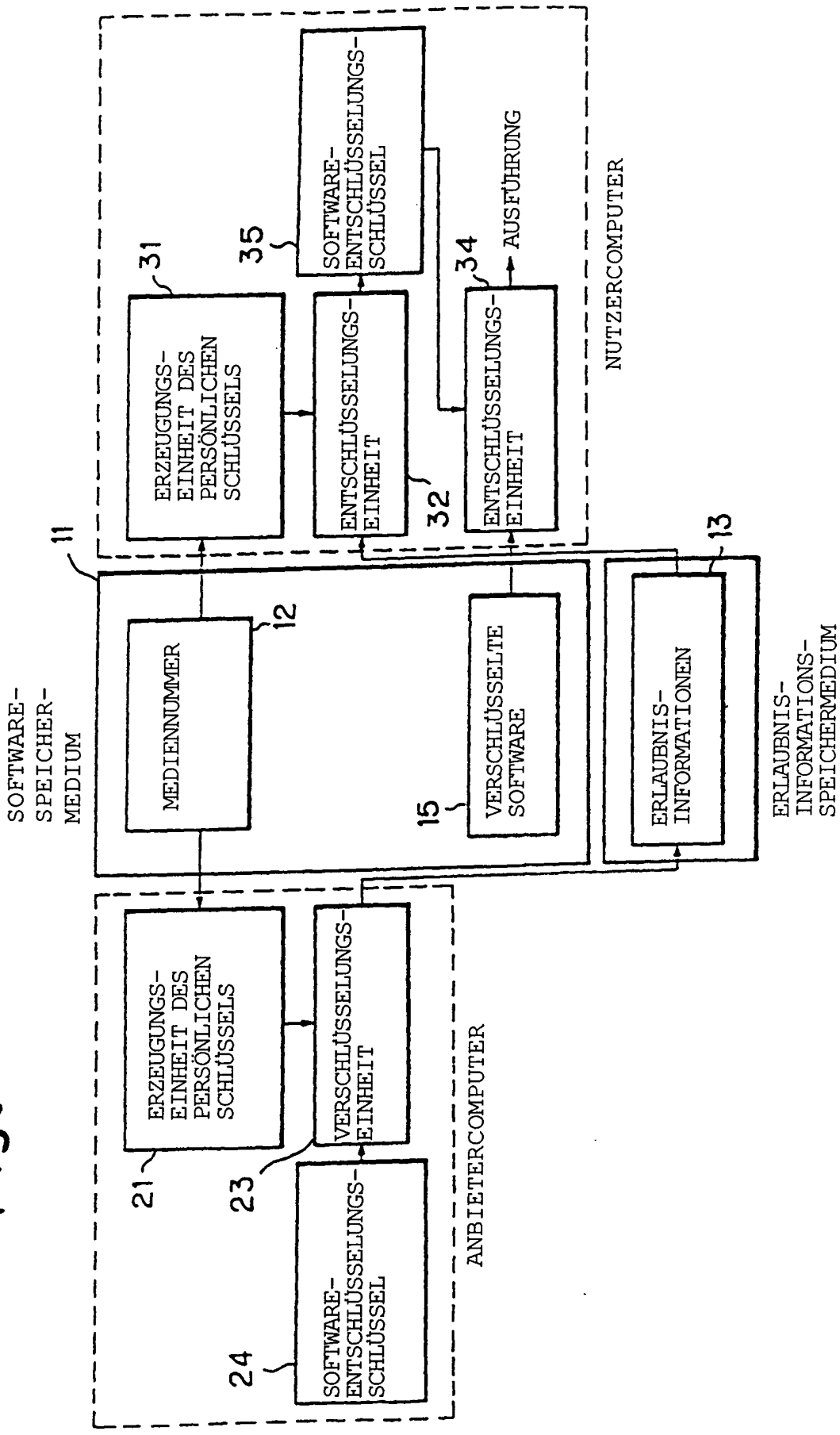
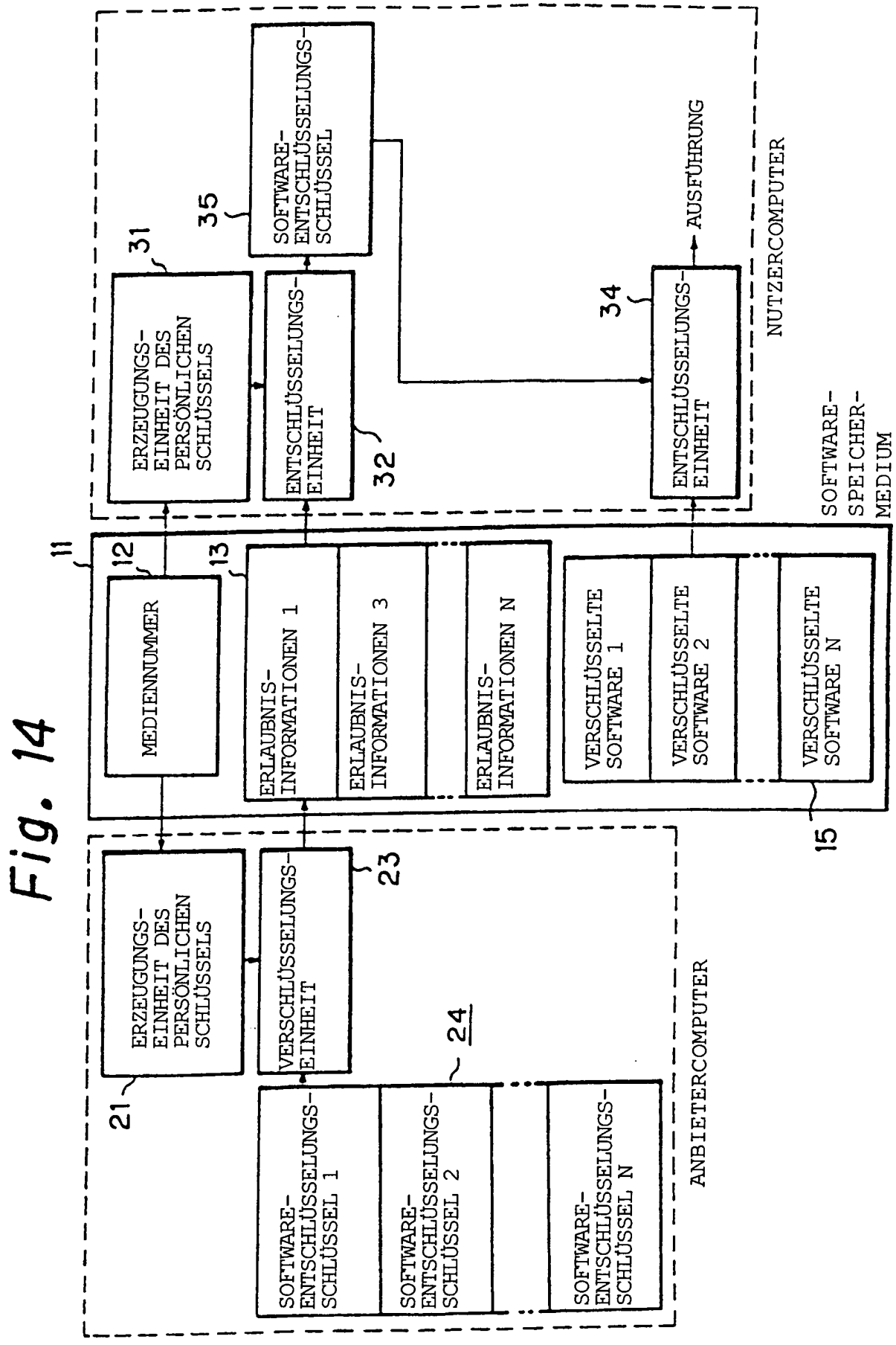

ANBIETERCOMPUTER
ERZEUGUNGS-EINHEIT DES PERSÖNLICHEN SCHLÜSSELS
21
VERSCHLÜSSELUNGS-EINHEIT
23
SOFTWARE-ENTSCHLÜSSELUNGS-SCHLÜSSEL
24
SOFTWARE-SPEICHER-MEDIUM
11
MEDIENNUMMER
12
VERSCHLÜSSELTE SOFTWARE
15
ERLAUBNIS-INFORMATIONEN
13
ERLAUBNIS-INFORMATIONS-SPEICHERMEDIUM
NUTZERCOMPUTER
ERZEUGUNGS-EINHEIT DES PERSÖNLICHEN SCHLÜSSELS
31
ENTSCHLÜSSELUNGS-EINHEIT
32
ENTSCHLÜSSELUNGS-EINHEIT
34
AUSFÜHRUNG
SOFTWARE-ENTSCHLÜSSELUNGS-SCHLÜSSEL
35

Fig. 14


ANBIETERCOMPUTER
NUTZERCOMPUTER
SOFTWARE-SPEICHER-MEDIUM
11
12
13
15
21
23
24
31
32
34
35
ERZEUGUNGS-EINHEIT DES PERSÖNLICHEN SCHLÜSSELS
VERSCHLÜSSELUNGS-EINHEIT
SOFTWARE-ENTSCHLÜSSELUNGS-SCHLÜSSEL 1
SOFTWARE-ENTSCHLÜSSELUNGS-SCHLÜSSEL 2
SOFTWARE-ENTSCHLÜSSELUNGS-SCHLÜSSEL N
MEDIENNUMMER
ERLAUBNIS-INFORMATIONEN 1
ERLAUBNIS-INFORMATIONEN 3
ERLAUBNIS-INFORMATIONEN N
VERSCHLÜSSELTE SOFTWARE 1
VERSCHLÜSSELTE SOFTWARE 2
VERSCHLÜSSELTE SOFTWARE N
ERZEUGUNGS-EINHEIT DES PERSÖNLICHEN SCHLÜSSELS
ENTSCHLÜSSELUNGS-EINHEIT
SOFTWARE-ENTSCHLÜSSELUNGS-SCHLÜSSEL
ENTSCHLÜSSELUNGS-EINHEIT
AUSFÜHRUNG