



(19)
Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 601 04 420 T2 2005.07.21**

(12) **Übersetzung der europäischen Patentschrift**

(97) **EP 1 287 692 B1**

(21) Deutsches Aktenzeichen: **601 04 420.7**

(86) PCT-Aktenzeichen: **PCT/US01/18022**

(96) Europäisches Aktenzeichen: **01 946 074.0**

(87) PCT-Veröffentlichungs-Nr.: **WO 01/095623**

(86) PCT-Anmeldetag: **31.05.2001**

(87) Veröffentlichungstag
der PCT-Anmeldung: **13.12.2001**

(97) Erstveröffentlichung durch das EPA: **05.03.2003**

(97) Veröffentlichungstag
der Patenterteilung beim EPA: **21.07.2004**

(47) Veröffentlichungstag im Patentblatt: **21.07.2005**

(51) Int Cl.7: **H04N 7/16**
H04N 7/167, H04N 7/173

(30) Unionspriorität:
209898 P 07.06.2000 US

(73) Patentinhaber:
**General Instrument Corporation, Horsham, Pa.,
US**

(74) Vertreter:
Meissner, Bolte & Partner GbR, 80538 München

(84) Benannte Vertragsstaaten:
CH, DE, ES, FR, GB, LI, NL

(72) Erfinder:
**MORONEY, Paul, Encinitas, US; SPRUNK, J., Eric,
Carlsbad, US**

(54) Bezeichnung: **SCHAUZEITABHÄNGIGES BEZAHLSYSTEM FÜR INHALTSLIEFERUNG IN MEDIENABSPIELSYSTEMEN**

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

QUERVERWEISE AUF VERWANDTE ANMELDUNGEN

[0001] Diese Anmeldung beansprucht den Nutzen der vorläufigen US Patentanmeldung 60/209,898, eingereicht am 7. Juni 2000, mit dem Titel „Pay by Time System for Content Delivery to Media Playback Systems“.

HINTERGRUND DER ERFINDUNG

[0002] Die vorliegende Erfindung bezieht sich im Allgemeinen auf Zahlungsmodelle für Informationsverteilungssysteme und genauer auf ein System, das unterschiedliche Zahlungsmodelle ermöglicht, wenn ein Benutzer Inhalt wie etwa Videoprogramme in einem digitalen Format bezieht.

[0003] Es ist nützlich, flexible Zahlungsmodelle zu haben, um Benutzern die Möglichkeit einer breiten Auswahl beim Erwerb von digitalem Inhalt, wie etwa Video, Audio, Text oder anderen Informationen, zu ermöglichen. Beispielsweise können heutige Verbraucher „Per-Sendung-Bezahl“-Fernsehprogramme bestellen, die es dem Verbraucher ermöglichen, individuelle Programme zu erwerben. Jedoch sind die Kosten des Erwerbs eines Programms dieselben, unabhängig davon, ob der Verbraucher das ganze Programm erwirbt und betrachtet, oder nur einen Abschnitt des Programms. Wenn ein Verbraucher zum Beispiel ein Programm auf halbem Weg durch die Ausstrahlung des Programms auswählt, belaufen sich die Kosten für den Verbraucher immer noch auf den vollen Preis für das Programm. Daher wäre es nützlich, unterschiedliche Preismodelle zu ermöglichen, es so zum Beispiel einem Verbraucher zu ermöglichen, Abschnitte eines Programms zu einem reduzierten Preis zu erwerben.

[0004] Die Implementierung eines flexiblen Zahlungsmodells wäre vorzugsweise kompatibel mit bestehenden Liefermechanismen. Beispielsweise ist Sicherheit ein wichtiges Thema für die Lieferung digitalen Inhalts. Typischerweise sind die Informationen verschlüsselt oder auf andere Weise beschränkt, so dass Benutzer, die nicht bezahlt haben, die nicht autorisiert sind usw., davon abgehalten werden, von den Informationen Gebrauch zu machen. Ein Ansatz verwendet kryptographische „Schlüssel“, die verwendet werden, um digitale Informationen vor der Verwendung der Informationen, z. B. durch die Anzeige der Informationen auf einem Fernsehbildschirm, zu entschlüsseln. Derartige Schlüssel können in unterschiedlichen Intervallen, z. B. in der Größenordnung von Monaten bis zu jeder Zehntelsekunde oder dergleichen, erzeugt, wieder erzeugt oder abgeleitet werden. Jedes Zahlungsmodell muss innerhalb der Sicherheitsstruktur des Liefersystems für digitale In-

formationen funktionieren, um Zugriff auf die Informationen gemäß dem Zahlungsmodell bereitzustellen.

KURZE ZUSAMMENFASSUNG DER ERFINDUNG

[0005] Die Erfindung stellt ein Verfahren zum Messen des Empfangs von Programminhalt durch einen Benutzer bereit. Das Verfahren stellt Programminhalt für den Empfang durch den Benutzer bereit, es stellt mehrere Schlüssel zur Verwendung durch den Benutzer beim Entschlüsseln des Programminhalts bereit, so dass jeder der Schlüssel für einen vorbestimmten Abschnitt des Programminhalts funktionsfähig ist, und bestimmt eine Zeitdauer, über die der Benutzer den Programminhalt empfängt, basierend darauf, wie viele der Vielzahl von Schlüsseln dem Benutzer bereitgestellt sind. Dem Benutzer kann für die betrachtete Zeitdauer eine Rechnung erstellt werden, indem die Anzahl von betrachteten oder empfangenen Zeiträumen einem Gebührenabrechnungszentrum mitgeteilt wird.

[0006] Ein erfindungsgemäßes Verfahren ist in Anspruch 1 dargelegt.

KURZE BESCHREIBUNG DER ZEICHNUNGEN

[0007] [Fig. 1](#) stellt ein Flussdiagramm dar, das eine Ausführungsform der Erfindung zum Benutzen einer Vielzahl von kryptographischen Schlüsseln zum Bestimmen einer Zeitdauer, über die der Benutzer das Programm empfängt, beschreibt.

[0008] [Fig. 2a](#) und [Fig. 2b](#) stellen ein Flussdiagramm dar, das eine Ausführungsform der Erfindung zum Verfolgen einer Zeitdauer, über die sich ein Benutzer ein Programm anschaut, zum Bestimmen einer Aufzeichnung zur Rechnungserstellung für den Benutzer für das Programm beschreibt.

[0009] [Fig. 3](#) stellt ein Flussdiagramm dar, das eine Ausführungsform der Erfindung zum Verfolgen eines ersten Zeitraums, einer Gesamtzahl von bezogenen Schlüsseln, eines letzten empfangenen Zeitraums und einer Ereignisaufzeichnung für empfangenen Programminhalt beschreibt.

[0010] [Fig. 4](#) stellt eine Datenstruktur zum Aufzeichnen von beispielsweise einem Ereigniskennzeichner, einem Bezeichner des ersten Zeitraums, einer Gesamtzahl von Schlüsseln und einem Bezeichner des letzten Zeitraums dar.

[0011] [Fig. 5](#) stellt ein Flussdiagramm dar, das das Erstellen einer Aufzeichnung für einen Benutzer und die Rechnungserstellung für das Programm für den Benutzer beschreibt.

[0012] [Fig. 6](#) stellt ein Kommunikationssystem zum Implementieren einer Übertragung von Programmin-

halt an einen Inhaltsempfänger dar.

[0013] Fig. 7 stellt Programminhalt, der zum Empfang durch einen Benutzer erhältlich ist, und tatsächlich vom Benutzer empfangenen Inhalt sowie ein laufendes Konto, das die Gesamtmenge des von dem Benutzer empfangenen Programms beschreibt, dar.

[0014] Fig. 8 stellt eine Benutzeroberfläche dar, die es einem Zuschauer ermöglicht, ein Programm für ein Per-Zeit-Bezahl-Verfahren unter einer Ausführungsform der Erfindung auszuwählen.

[0015] Fig. 9 stellt ein Flussdiagramm zum Implementieren eines Per-Zeit-Bezahl-Verfahrens für eine Ausführungsform der Erfindung dar.

DETAILLIERTE BESCHREIBUNG DER ERFINDUNG

[0016] Die vorliegende Ausführungsform der Erfindung kann mit Bezug auf ein Programmliefersystem wie etwa die Art, die zum Liefern von Fernseh- oder Filmprogrammgestaltung an das Heim eines Benutzers verwendet wird, beschrieben werden. Per-Sendung-Bezahl-Systeme sind in der Vergangenheit verwendet worden, um es Benutzern zu ermöglichen, ein ganzes Programm zu erwerben, unabhängig von der Zeitdauer, über die sie sich das Programm tatsächlich anschauen. Auf diese Weise ist es beispielsweise möglich, einen Film als ein Per-Sendung-Bezahl in seinem Heim oder einem Hotel zu erwerben. Ferner ist es möglich, ein Sportereignis wie etwa einen Boxkampf zu erwerben, wann immer erwünscht. Dies sind jedoch Beispiele von Ereignissen, bei denen es einem Benutzer nichts ausmacht, für das ganze Ereignis zu zahlen, da sich der Benutzer typischerweise das ganze Ereignis anschaut. Beispielsweise will sich ein Benutzer üblicherweise einen Film vom Anfang bis zum Ende oder einen Boxkampf von Anfang an anschauen. Demzufolge macht es dem Benutzer nichts aus, für das ganze Ereignis zu zahlen.

[0017] Es gibt jedoch einige Arten von Programmgestaltung, für die ein Benutzer es vorziehen würde, nicht für die Zeit bezahlen zu müssen, in der das Programm nicht tatsächlich empfangen worden ist. So könnten zum Beispiel Abschnitte eines Lieds empfangen werden, ohne die Notwendigkeit, das ganze Lied anzuhören. Ähnlich könnten Abschnitte einer Nachrichtensendung, z. B. das Wetter, empfangen werden, ohne dass der Benutzer für den Empfang der restlichen Nachrichtenprogrammgestaltung zahlen wollte. Das normale Per-Sendung-Bezahl-System erfüllt diese Zuschaueranforderungen nicht. Somit erleichtert dies die kommerziellen Aspekte dieser Art der Programmgestaltung nicht, weder aus der Perspektive des Zuschauers, der die Programmgestaltung erwerben möchte, noch aus der des Dienst-

bieters, der die Programmgestaltung gern vermarkten möchte.

[0018] Eine Ausführungsform der Erfindung zielt auf diese Frage ab, um einige der Probleme zu lösen, die durch die Rechnungserstellung für ein ganzes Programm unter einem Per-Sendung-Bezahl-System entstehen. Und zwar stellt das in Fig. 1 gezeigte Verfahren ein gezähltes Zahlungssystem dar, bei dem der Empfang eines Programminhalts zur Rechnungserstellung für einen Kunden oder Teilnehmer gemessen wird.

[0019] In dem Verfahren 100 aus Fig. 1 wird in Kasten 104 Programminhalt zum Empfang durch einen Benutzer bereitgestellt. Zum Beispiel kann ein derartiger Programminhalt die Form eines Dienstes in einem Inhaltsstrom wie demjenigen, der privaten Teilnehmern von ihrem Kabelsystem bereitgestellt wird, annehmen. Typischerweise sind bei Kabelsystemen mehrere Dienste in einem Inhaltsstrom erhältlich, aus denen der Verbraucher einen gewünschten Dienst (z. B. HBO™, ESPN™, SHOWTIME™, einen Musikkanal, eine Internetseite usw.) auswählen kann. Typischerweise sind derartige Kabelübertragungen verschlüsselt, wobei an die Benutzer Schlüssel zum Entschlüsseln des verschlüsselten Programmstroms verteilt werden. Jedoch können die Intervalle, in denen diese Schlüssel an den Benutzer verteilt werden, variieren. Bei einigen Systemen kann ein einzelner Schlüssel für ein ganzes Programm oder für einen ganzen Monat verwendet werden, während bei anderen Systemen oder Arten von Programmgestaltung jedes Zehntel (1/10) einer Sekunde ein neuer Schlüssel gesendet werden kann. Im Allgemeinen werden Schlüssel für wertvollere Programmgestaltung häufiger gewechselt. Somit wird während eines Programms eine Vielzahl von Schlüsseln zur Verwendung beim Entschlüsseln des Programminhalts durch den Benutzer bereitgestellt, wie in Kasten 108 gezeigt. In Kasten 112 kann bestimmt werden, wie lange der Zuschauer das Programm empfangen hat, basierend auf den Schlüsseln, die von dem Benutzer für das Programm empfangen wurden.

[0020] Fig. 2a und Fig. 2b enthalten ein Flussdiagramm 200, das eine andere Ausführungsform der Erfindung darstellt. In Fig. 2a zeigt der Kasten 204, dass der Programminhalt verschlüsselt wird, zum Beispiel an der Kopfstelle eines Kabelsystems. In Kasten 208 werden Kryptoperioden bezeichnet, um Abschnitten des Programminhalts zu entsprechen. Zum Beispiel kann der Programminhalt in Intervalle von 133 Millisekunden unterteilt werden. Auf diese Weise wäre jedes 133-Millisekunden-Segment des Programms eine Kryptoperiode.

[0021] In Kasten 212 wird das verschlüsselte Programm von einem Sendegerät an einen Empfänger übertragen. Beispielsweise könnte das Programm

von der Kopfstelle eines Kabelsystems an einen Inhaltsempfänger, wie etwa eine Set-Top-Box, im Heim eines Verbrauchers übertragen werden.

[0022] So wird in Kasten **216** gezeigt, dass das verschlüsselte Programm am Empfänger empfangen wird.

[0023] In Kasten **220** wird bestimmt, ob der Benutzer den Programminhalt empfangen will. Zum Beispiel würde ein Benutzer, der Fernsehen schaut, normalerweise einen gewünschten Kanal auswählen, um den gewünschten Dienst zu empfangen. Wenn der Benutzer den Programminhalt für einen Dienst empfangen will, wählt der Benutzer den Kanal des Empfängers, von dem das Programm in Kasten **224** empfangen wird, aus.

[0024] Um es dem Benutzer zu ermöglichen, von dem Programminhalt Gebrauch zu machen, versieht der Dienstanbieter (z. B. das Kabelunternehmen) den Empfänger oder Benutzer mit einem Schlüssel, um das verschlüsselte Programmmaterial zu entschlüsseln, wie in Kasten **228** dargestellt. Der Schlüssel wird verwendet, um das verschlüsselte Programm in Kasten **232** zu entschlüsseln.

[0025] In [Fig. 7a](#) ist ein Musterprogramm oder -ereignis **700** gezeigt. Beispielsweise könnte das Ereignis ein Boxkampf sein. Das Ereignis ist in Zeiträume unterteilt, wie durch die unterteilten Abschnitte 1 bis 25 in [Fig. 7a](#) gezeigt. Ein beispielhafter Zeitraum **704** ist in Kasten 2 des Ereignisses **700** gezeigt. Jeder Zeitraum entspricht einer entsprechenden Kryptoperiode, in der das Programmmaterial für den Zeitraum durch einen kryptographischen Vorgang, wie etwa die Entschlüsselung durch die Verwendung eines Entschlüsselungsschlüssels, bezogen wird. Typischerweise würden neue Schlüssel für unterschiedliche Kryptoperioden verwendet. Jeder Zeitraum eines Programms kann durch einen Zeitraumbezeichner wie etwa einen binären Wert, der der Stelle des besonderen Zeitraums in dem Programm entspricht, bezeichnet werden. Somit könnte Kasten Nummer 2 in [Fig. 7a](#) als „00010“ bezeichnet werden, während Kasten **25** als „11001“ bezeichnet werden könnte.

[0026] In Kasten **236** aus [Fig. 2b](#) wird der Zeitraumbezeichner **236** gespeichert. Dies könnte an verschiedenen Stellen im System erfolgen. Jedoch wird es für den Zweck dieses Beispiels als am Empfänger erfolgreich beschrieben. Somit ist es möglich zu verfolgen oder aufzuzeichnen, wann ein Benutzer beginnt, ein ausgewähltes Programm zu empfangen, indem der Zeitraumbezeichner gespeichert wird. In Kasten **240** wird die laufende Summe für die Anzahl von Schlüsseln, die zum Entschlüsseln des Programms verwendet werden, eingestellt. Anfangs ist die laufende Summe null, bis der anfängliche Zeitraum empfangen wird. Somit kann bei der anfänglichen

Auswahl des Programms die Gesamtzahl von Schlüsseln auf 1 eingestellt werden. Mit dem Empfang zusätzlicher Schlüssel und entsprechender Zeiträume kann die Gesamtzahl von Schlüsseln demgemäß erhöht werden.

[0027] Zu irgendeinem Zeitpunkt wird sich der Benutzer entscheiden, den Kanal zu wechseln. Daher wird in Kasten **244** bestimmt, ob der Benutzer den Inhalt eines anderen Kanals beziehen will. Wenn der Benutzer keinen anderen Kanal beziehen will, wird der ursprüngliche Inhalt weiterhin entschlüsselt und die laufende Summe an Schlüsseln wird weiterhin erzeugt. Wenn der Benutzer jedoch den Inhalt eines anderen Kanals beziehen will, wird es dem Benutzer ermöglicht, den Kanal des Empfängers zu wechseln, wie in Kasten **248** gezeigt. Wenn sich der Benutzer entscheidet, den Kanal zu wechseln, wird der zuletzt empfangene Zeitraum bestimmt, so dass eine Aufzeichnung für den empfangenen Abschnitt des Programms erstellt werden kann, wie durch Kästen **252** und **256** gezeigt. Dies kann durch [Fig. 7b](#) dargestellt werden, die dem Intervall **708** in [Fig. 7a](#) entspricht.

[0028] In [Fig. 7b](#) ist eine Aufzeichnung eines Ereignisses, das einen Ereigniskennzeichner, einen Startzeitraum, eine Gesamtzahl von angeschauten Zeiträumen und einen Endzeitraum des Ereignisses aufweist, gezeigt. In [Fig. 7b](#) ist das Ereignis als „700“ bezeichnet. Auf ähnliche Weise ist der Startzeitraum des angeschauten Ereignisses als Zeitraum Nummer „4“ bezeichnet, und der Endzeitraum ist als Zeitraum Nummer 8 bezeichnet. Da insgesamt 5 Zeiträume für dieses Programm angeschaut wurden, ist das „Summe“-Feld der Aufzeichnung für diese erste Aufzeichnung als „5“ bezeichnet.

[0029] Wiederum unter Bezugnahme auf [Fig. 2b](#) kann die Aufzeichnung zur späteren Übertragung an ein Gebührenabrechnungszentrum an dem Empfänger gespeichert werden. Dies ermöglicht es, dem Benutzer eine Rechnung beispielsweise auf der Basis der Gesamtmenge des Programms, das empfangen wurde, zu erstellen. Nachdem der Benutzer einen neuen Kanal ausgewählt hat, kann der Prozess durch Rückkehr auf Kasten **220** in [Fig. 2a](#) wiederholt werden. Dies ermöglicht es dem Benutzer, eine neue Aufzeichnung für ein anderes Programm oder Ereignis, wie etwa einen Film anstelle des zuvor erwähnten Boxkampfes, zu erstellen.

[0030] Nachdem der Benutzer zu dem ursprünglichen Ereignis **700** zurückgekehrt ist, wird eine zweite Aufzeichnung erstellt. Die zweite Aufzeichnung kann durch den Start bei Kasten **220** in [Fig. 2a](#) und das Wiederholen der Kästen **224**, **228**, **232**, **236**, **240**, **244**, **248**, **252**, **256** und **260** angefangen werden. Das Format der zweiten Aufzeichnung kann unterschiedliche Formate annehmen, abhängig von der Konfiguration des Systems. [Fig. 7c](#) zeigt ein Format für eine

derartige zweite Aufzeichnung. In [Fig. 7c](#) umfasst die zweite Aufzeichnung, die den in [Fig. 7a](#) als 712 gezeigten Zeiträumen entspricht, einen Ereignisbezeichner „700“, einen Startzeitraum „4“, der dem ersten empfangenen Zeitraum in [Fig. 7a](#) entspricht, die Gesamtzahl von empfangenen Zeiträumen „11“ (die den empfangenen Zeiträumen 4, 5, 6, 7, 8 und 12, 13, 14, 15, 16, 17 entspricht) und einen Endzeitraum „17“, der dem letzten empfangenen Zeitraum entspricht. Dieser Datensatz könnte genauso gut alternative Formen annehmen, wie der durchschnittliche Fachmann verstehen würde.

[0031] Auf ähnliche Weise kann der Prozess mit der Erzeugung einer anderen Aufzeichnung **716** in [Fig. 7a](#), die dem Datensatz in [Fig. 7d](#) entspricht, noch einmal wiederholt werden. Die zweite Aufzeichnung **724** in [Fig. 7c](#) wird als die Daten aus der Aufzeichnung **720** in [Fig. 7b](#) benutzend gezeigt. Auf ähnliche Weise ist die Aufzeichnung **728** in [Fig. 7d](#) als Daten aus der Aufzeichnung **724** in [Fig. 7c](#) benutzend gezeigt. Wenn sich somit ein Benutzer entscheidet, den Empfang des Ereignisses zu beenden, kann auf die am Empfänger gespeicherte vorherige Aufzeichnung zugegriffen und diese modifiziert werden, um eine neue Aufzeichnung zu erstellen. Somit kann die Endaufzeichnung, die für ein Ereignis bereit wird, an das Gebührenabrechnungszentrum zur Rechnungserstellung übertragen werden, um das empfangene Ereignis, den Startzeitraum, die Gesamtzahl empfangener Zeiträume und den letzten empfangenen Zeitraum anzuzeigen.

[0032] Die Gebühr, die für einen Dienst oder ein spezifisches Programm in Rechnung gestellt wird, kann entweder auf einem vor der Auswahl eines Programms verabredeten Betrag oder einer von dem Dienstanbieter festgesetzten festen Gebühr basieren. So kann dem Benutzer zum Beispiel beim ersten Einschalten eines neuen Dienstes eine Benutzeroberfläche präsentiert werden, die folgendermaßen aussieht:

„Dieser Dienst wird auf einer Zählbasis von 0,01 \$/Minute berechnet. Bitte drücken Sie „KAUFEN“, wenn Sie mit dieser Gebühr einverstanden sind, und für den Rest des Monats wird Ihnen dann diese Gebühr berechnet, wann immer Sie diesen Dienst einschalten.“

[0033] In [Fig. 3](#) ist ein Verfahren **300** zum Erstellen einer Aufzeichnung dargestellt. In Kasten **304** ist ein erster Zeitraumbezeichner gespeichert, zum Beispiel in einem Speicher am Empfänger. In Kasten **308** wird die Gesamtzahl von Schlüsseln, die zum Entschlüsseln eines Programminhalts für ein Ereignis verwendet wird, im Speicher gespeichert. In Kasten **312** wird der Bezeichner für den letzten empfangenen Zeitraum im Speicher gespeichert. In Kasten **316** wird eine Aufzeichnung für das Ereignis erstellt, die den Ereigniskennzeichner, den Bezeichner des ersten

Zeitraums, die Gesamtzahl von Schlüsseln und den Bezeichner des letzten Zeitraums umfasst. Eine Datenstruktur für eine derartige Aufzeichnung ist in [Fig. 4](#) mit einem „Ereigniskennzeichner“-Feld **404**, einem „Bezeichner des ersten Zeitraums“-Feld **408**, einem „Gesamtzahl von Schlüsseln“-Feld **412** und einem „Bezeichner des letzten Zeitraums“-Feld **416** dargestellt.

[0034] In [Fig. 6](#) ist ein beispielhaftes System **600** zum Implementieren einer Ausführungsform der Erfindung gezeigt. [Fig. 6](#) zeigt eine Kopfstelle **604**, die auch als Gebührenabrechnungsprozessor für, zum Beispiel, ein Kabelsystem dienen kann. Die Kopfstelle ist mit einem Satellitenempfänger **608** gekoppelt, der seinerseits mit einem Satelliten **612** gekoppelt ist. Der Satellit kann dem Empfänger Inhalt zur Verwendung durch die Kopfstelle bereitstellen. Auf ähnliche Weise kann ein Server **624** der Kopfstelle über ein Netz, wie etwa das Internet **620**, Programminhalt bereitstellen. Weiterhin kann ein Sendegerät **616** an die Kopfstelle Inhalt zur Verteilung übertragen. Die Kopfstelle führt dann dem Benutzer am Inhaltsempfänger **630**, wie etwa einer Set-Top-Box für einen Fernseher **634**, Programminhalt zu, der mehrere Ereignisse umfasst.

[0035] Zu irgendeinem Zeitpunkt müssen die Informationen zu den betrachteten Programmen an das Gebührenabrechnungszentrum zur Rechnungserstellung für den Teilnehmer gemeldet werden. [Fig. 5](#) stellt ein Beispiel zum Implementieren eines derartigen Gebührenabrechnungssystems dar. In Kasten **504** aus [Fig. 5](#) wird für das empfangene Ereignis eine Aufzeichnung erstellt. Diese Aufzeichnung wird dann an den Gebührenabrechnungsprozessor übertragen, wie in Kasten **508** gezeigt. Am Gebührenabrechnungsprozessor kann die Anzahl von Schlüsseln, die zum Anschauen des Programms verwendet wurde, aus dem Datensatz bestimmt werden. Auf ähnliche Weise kann die Anzahl von empfangenen Zeiträumen bestimmt werden, da die Anzahl von Schlüsseln der Anzahl von empfangenen Zeiträumen entspricht. Danach kann die Gesamtzeit, über die ein Benutzer das Programm empfangen hat, berechnet werden, wie durch Kasten **516** gezeigt. Basierend auf der auf das Ereignis angewendeten Berechnungsgebühr kann dem Benutzer, wie durch Kasten **520** dargestellt, für das Ereignis eine Rechnung erstellt werden.

[0036] Zusätzlich zu einem gezahlten Per-Zeit-Bezahl ermöglicht eine Ausführungsform der Erfindung variable Per-Zeit-Bezahl-Preise. Diese Ausführungsform der Erfindung bietet einem Zuschauer, der eine Sendung einschaltet, nachdem die Sendung empfangen hat, unterschiedliche Zahlungsoptionen für das Betrachten der restlichen Sendung. Zum Beispiel stellt [Fig. 8](#) eine Benutzeroberfläche **800** dar, die verwendet werden könnte, um einem Benutzer unterschiedliche Optionen zum Betrachten einer Sendung

zu bieten. Die Benutzeroberfläche könnte einen Anzeigebereich **804** umfassen, der angibt, wie lange ein Programm dauert und wieviel Zeit des Programms verbleibt, die erworben werden kann. Dann könnten Alternativen zum Betrachten unterschiedlicher Abschnitte des verbleibenden Programms präsentiert werden. Im Anzeigebereich **808** gibt beispielsweise der Anzeiger an, dass die verbleibenden 120 Minuten des Programms für 5,00 \$ erworben werden können. Im Anzeigebereich **812** gibt der Anzeiger an, dass die letzten 90 Minuten des Programms für 4,00 \$ erworben werden können, während der Anzeigeabschnitt **816** angibt, dass die letzten 30 Minuten für 2,00 \$ erworben werden könnten. Anstatt die verbleibende Zeit, die zum Erwerb erhältlich ist, anzugeben, könnte als Alternative dazu ein Zeitblock, der zum Erwerb erhältlich ist, angegeben werden. Auf diese Weise gibt der Anzeiger **824** der Benutzeroberfläche **800** an, dass die nächsten 30 Minuten für 2,00 \$ erworben werden können, während der Kasten **828** angibt, dass die nächsten 60 Minuten für 3,00 \$ erworben werden können. Der Kasten **832** gibt dem Benutzer an, dass eine Wahl getroffen werden sollte, indem zum Beispiel auf ein Piktogramm geklickt wird. Dann kann ein „Erwerben“-Piktogramm **836** verwendet werden, um die Erwerbsswahl des Benutzers zu bestätigen.

[0037] [Fig. 9](#) stellt ein Verfahren **900** zum Implementieren des variablen Preismodells dar. In Kasten **910** bestimmt ein Programmanbieter einen Preis für die Lieferung eines Programms an einen Benutzer. Dann wird das Programm zur Verwendung durch Endverbraucher-Geräte, z. B. eine Set-Top-Box, Empfänger usw., wie in Kasten **920** gezeigt, zugeführt, und der Endverbraucher beginnt, den Programminhalt zu empfangen, wie in Kasten **930** gezeigt. An irgendeinem Punkt während der Programmlieferung wird ein Benutzer, der sich das Programm noch nicht anschaut, den Kanal, der den Programminhalt bereitstellt, einschalten. In diesem Stadium kann von dem Benutzer eine Vorschau auf den Programminhalt betrachtet werden, um den Benutzer dazu zu verleiten, das Programm zu betrachten, wie in Kasten **940** gezeigt. Dann wird bestimmt, ob der Benutzer einen Abschnitt des Programmmaterials empfangen will, wie in Kasten **950** gezeigt. Wenn sich der Benutzer das Programm nicht anschauen will, hört das Verfahren auf und die Vorschau kommt zu einem Ende oder wird beendet. Wenn der Benutzer jedoch den Programminhalt empfangen will, wird dem Benutzer anschließend eine Lieferung verbleibender Abschnitte des Programms zu einem Preis angeboten, der sich von dem Preis für das ganze Programm unterscheidet, wie in Kasten **960** gezeigt und ferner durch die Benutzeroberfläche in [Fig. 8](#) dargestellt. Wenn der Benutzer nur einen ersten Abschnitt des Programms erwirbt, könnte ein zweiter Abschnitt des Programms zum Erwerb angeboten werden, wie in Kasten **970** gezeigt.

[0038] In den meisten Fällen ist anzunehmen, dass der angebotene Preis für den verbleibenden Abschnitt eines Programms weniger betragen wird als für das ganze Programm. In einigen Fällen kann der Wert des Programms jedoch eine Funktion von Echtzeitereignissen sein. So könnte der Preis für das restliche Programm tatsächlich ansteigen, während sich die Ereignisse des Programms abspielen. Auf diese Weise könnte der Preis eines Basketballspiels, das anfänglich als einseitig empfunden worden war, für anfängliche Zuschauer niedriger liegen als für Zuschauer, die es später einschalten, wenn sich das Spiel als eng umkämpft oder möglicherweise strittig herausstellt.

[0039] Somit ermöglicht es das variable Preisberechnungsverfahren einem Dienstanbieter, weniger als das ganze Programm, mehr als das ganze Programm, eine Auswahl unterschiedlicher Mengen von Programmzeit, eine Auswahl unterschiedlicher Preise für unterschiedliche Mengen von Programmzeit, eine Auswahl von Zwischenabschnitten eines Programms sowie eine kostenlos verfügbare Vorschauperiode anzubieten.

[0040] Das oben beschriebene Verfolgungssystem kann verwendet werden, um die tatsächliche Anschauzeit des Benutzers zu verfolgen. Auf diese Weise kann eine tatsächliche Kryptoperiode, die einem Zeitraum des Programms entspricht, bestimmt werden. Ferner kann eine Aufzeichnung erstellt werden, um den zuerst angeschauten Zeitraum, den zuletzt angeschauten Zeitraum und die Anzahl von angeschauten Zeiträumen aufzuzeichnen. Somit können, obwohl dem Benutzer eine Rechnung gemäß den am Beginn der Sitzung vereinbarten Bedingungen erstellt wird, Daten über die Fernsehgewohnheiten des Zuschauers gesammelt werden. Wenn zum Beispiel in bekannten Zeiträumen eines Programms Werbeblöcke erscheinen, könnte die Aufzeichnung verwendet werden, um zu bestimmen, ob der Zuschauer während dieses Zeitraums umgeschaltet hat.

[0041] In einem Beispiel kann eine Set-Top-Box bereitgestellt werden, die einen Sicherheitsprozessor umfasst, in dem kryptographische Schlüssel zur Verwendung bei der Entschlüsselung eines ausgewählten Programminhalts verwendet werden. Wenn ein Benutzer ein gewünschtes verschlüsseltes Programm auswählt, kann der Sicherheitsprozessor so die oben beschriebene Aufzeichnung der Fernsehvorgeschichte weiterführen.

[0042] Nach dem Betrachten des allerersten Zeitschlüssel-Zeitraums könnte der sichere Chip zum Beispiel eine interne Zählung der betrachteten Zeiträume weiterführen, die sich während des Fortschreitens der Betrachtung erhöht. Würde der Benutzer das ganze Ereignis betrachten, würde das sichere Gerät nach dem Ende des Ereignisses eine einzige

Aufzeichnung melden, die den ersten betrachteten Zeitraum, eine Dauer, die allen Zeiträumen des Programms gleicht, und einen letzten betrachteten Zeitraum, der mit der Endzeit übereinstimmt, wie in der Zeitraumzählung gemessen, zeigt. Wenn der Benutzer jedoch nach einem Teil des Programms umschaltet, meldet das Sicherheitsgerät zu diesem Zeitpunkt eine Aufzeichnung, die eine kürzere Dauer und eine zuletzt betrachtete Zählung, die mit der Zeit des Umschaltens übereinstimmt, zeigt. Wenn der Benutzer anschließend zurückschaltet, kann die Zählung der Dauer wieder aufgenommen werden. Auf diese Weise kann ein Sicherheitsprozessor oder eine Vorrichtung interne Aufzeichnungen für Start/Dauer/Ende für mindestens so lange, wie das Ereignis läuft, weiterführen.

[0043] Um sicherzustellen, dass der nicht-sichere Teil der Set-Top-Box nicht ausfällt oder die Berichte ignoriert, kann ein Gebührenabrechnungsmechanismus benutzt werden. Beispielsweise können alle Aufzeichnungen, die von dem gesicherten Gerät erzeugt werden, untereinander verbunden werden. So kann ein Authentifikator, der eine Funktion der Verbindung aller vermutlich gemeldeten Ereignisse ist, erzeugt werden. Wenn ein Pirat auch nur ein Ereignis fallen lässt, werden die vom Gebührenabrechnungszentrum empfangenen Berichte nicht authentifiziert. Also erkennt das Gebührenabrechnungszentrum, dass ein Problem vorliegt. Das Gebührenabrechnungszentrum kann dann eine Wiederholung des Berichts anfordern, die jedwede Kommunikationsfehler aufklären oder verbleibende Störungen, die einen schlechten Teilnehmer oder einen Piratenteilnehmer anzeigen, angeben würde.

[0044] Wenn Per-Zeit-Bezahl-Ereignisaufzeichnungen zusammen mit Per-Sendung-Bezahl-Ereignissen betrachtet werden, können die Aufzeichnungen von jedem noch immer verbunden werden, um einen Authentifikator zu erzeugen. Beim Ein- und Ausschalten eines Per-Zeit-Bezahl-Ereignisses werden mehrere Aufzeichnungen erzeugt und mit vorhergehenden und nachfolgenden Aufzeichnungen verbunden. Es wird jedoch nur die letzte Aufzeichnung für Rechnungserstellungszwecke benötigt, da sich diese auf die Endstatistiken von Start/Dauer/Ende, die für die Rechnungserstellung wertvoll sind, bezieht. Jeder frühere Bericht kann verworfen werden, wenn eine Aktualisierung desselben Ereignisses erzeugt wird. Daher ist die oben beschriebene sichere Verbindung nur einmal pro Ereignis anstatt für jede einzelne, während des Verlaufs eines einzigen Ereignisses erzeugte Aufzeichnung notwendig.

[0045] Eine Weise, dies zu erreichen, liegt darin, ein eingeschlossenes Ereigniskennzeichen mit jeder Aufzeichnung einzuschließen und jede erzeugte Aufzeichnung für ein Per-Zeit-Bezahl-Ereignis mit der Endaufzeichnung für das vorhergehende Ereignis

rückzuverbinden. Auf diese Weise wird für jede Per-Zeit-Bezahl-Aufzeichnung, die für ein Ereignis erzeugt wird, die Aufzeichnung mit der Endaufzeichnung für das vorhergehende Ereignis rückverbunden. Dies beruht darauf, dass a priori nicht bekannt ist, welche Aufzeichnung die letzte für ein einzelnes Ereignis sein wird. So wird das Sicherheitsgerät den identischen Verkettungsalgorithmus für jede Aufzeichnung, die es für ein einzelnes Per-Zeit-Bezahl-Ereignis erzeugt, verwenden. Sobald die Endaufzeichnung tatsächlich berechnet ist, kann der Authentifikator errechnet werden, und individuelle Aufzeichnungen für jedes Ereignis (ob Per-Sendung-Bezahl oder Per-Zeit-Bezahl) können an das Gebührenabrechnungszentrum übertragen werden, wo sie mit dem Authentifikator authentifiziert werden.

[0046] Während verschiedene Ausführungsformen der Erfindung als Verfahren zum Implementieren der Erfindung beschrieben worden sind. Es sollte verstanden werden, dass die Erfindung durch einen Code, der mit einem Computer gekoppelt ist, z. B. einem auf einem Computer residenten oder für den Computer zugänglichen Code, implementiert werden kann. Zum Beispiel könnten Software und Datenbanken benutzt werden, um viele der oben diskutierten Verfahren umzusetzen. Zusätzlich zu Ausführungsformen, bei denen die Erfindung durch Hardware erreicht wird, wird somit auch angemerkt, dass diese Ausführungsformen durch den Gebrauch eines Manufakturerezeugnisses erreicht werden können, das ein maschinennutzbares Medium mit einem darin ausgeführten maschinenlesbaren Programmcode, der die Aktivierung der in dieser Beschreibung offenbarten Funktionen bewirkt, umfasst. Es ist daher wünschenswert, dass die oben geschilderten Ausführungsformen ebenfalls mit ihrem Programmcode-mittel als durch dieses Patent auch geschützt betrachtet werden.

[0047] Es ist auch vorgesehen, dass Ausführungsformen der Erfindung als in einer Trägerschwingung ausgeführte Computersignale erreicht werden könnten, sowie als Signale (z. B. elektrische und optische), die durch ein Übertragungsmedium verbreitet würden. Somit könnten die verschiedenen, oben diskutierten Informationen in einer Struktur, wie etwa einer Datenstruktur, formatiert und als ein elektrisches Signal über ein Übertragungsmedium übertragen oder auf einem maschinenlesbaren Medium gespeichert werden.

[0048] Es wird auch angemerkt, dass viele der hierin vorgetragenen Strukturen und Handlungen als Mittel zur Durchführung einer Funktion bzw. als Schritte zur Durchführung einer Funktion vorgetragen werden können. Daher versteht es sich, dass eine derartige Sprache berechtigt ist, alle derartigen Strukturen oder Handlungen, die innerhalb dieser Beschreibung offenbart werden, und ihre Entsprechungen abzude-

cken.

[0049] Es wird erwartet, dass die Verfahren der Ausführungsformen der vorliegenden Erfindung und viele der damit einhergehenden Vorteile aus dieser Beschreibung verstanden werden, und es ist offensichtlich, dass verschiedene Änderungen in der Form, Konstruktion und Anordnung ihrer Teile vorgenommen werden können, ohne den Bereich der Erfindung zu verlassen oder alle ihre materiellen Vorteile aufzugeben, wobei die hierin zuvor beschriebenen Form lediglich beispielhafte Ausführungsformen derselben sind.

Patentansprüche

1. Ein Verfahren zum Messen des Empfangs von Programminhalt durch einen Benutzer, wobei das Verfahren Folgendes umfasst:

Bereitstellen von Programminhalt für den Empfang durch den Benutzer;
Bestimmen eines Anfangszeitraums des vom Benutzer empfangenen Programminhalts;
Bereitstellen einer Vielzahl von Schlüsseln zur Verwendung durch den Benutzer beim Entschlüsseln des Programminhalts, wobei jeder der Vielzahl Schlüssel für einen vorbestimmten Abschnitt des Programminhalts funktionsfähig ist;
Bestimmen einer Gesamtzahl von Zeiträumen des vom Benutzer empfangenen Programminhalts aus dieser Vielzahl Schlüssel, wobei jeder der Zeiträume einem der Schlüssel, der für den vorbestimmten Abschnitt des Programminhalts funktionsfähig ist, entspricht, und wobei das Bestimmen der Gesamtzahl von Zeiträumen das Zählen der Schlüssel umfasst;
Bestimmen einer Zeitdauer, über die der Benutzer den Programminhalt empfängt, basierend auf dem Empfangen des Anfangszeitraums und dem Bestimmen der Gesamtzahl von Zeiträumen des vom Benutzer empfangenen Programminhalts.

2. Verfahren wie in Anspruch 1 beschrieben und das ferner Folgendes umfasst:
Aufzeichnen des letzten Zeitraums des vom Benutzer empfangenen Programms.

3. Verfahren wie in Anspruch 1 beschrieben und das ferner Folgendes umfasst:
Aktualisieren der Gesamtzahl von Zeiträumen des vom Benutzer empfangenen Programminhalts, während das Programm vom Benutzer empfangen wird; und
Aktualisieren der Aufzeichnung des letzten Zeitraums des vom Benutzer empfangenen Programms, während das Programm vom Benutzer empfangen wird.

4. Verfahren wie in Anspruch 2 beschrieben und das ferner Folgendes umfasst:
Aktualisieren der Aufzeichnung des letzten Zeit-

raums des vom Benutzer empfangenen Programms als Folge dessen, dass der Benutzer aufhört, den Programminhalt zu empfangen.

5. Verfahren wie in Anspruch 4 beschrieben und das ferner Folgendes umfasst:
Aktualisieren der Gesamtzahl von Zeiträumen des vom Benutzer empfangenen Programminhalts, während das Programm vom Benutzer empfangen wird, nachdem der Benutzer nach einem Beenden des Empfangens des Programminhalts zum Empfang des Programminhalts zurückgekehrt ist.

6. Verfahren wie in Anspruch 1 beschrieben und das ferner Folgendes umfasst:
Melden der Gesamtzahl von Zeiträumen an ein Gebührenabrechnungssystem.

7. Verfahren wie in Anspruch 6 beschrieben und das ferner Folgendes umfasst:
Rechnungserstellung für den Benutzer, basierend auf der Gesamtzahl der Zeiträume.

8. Verfahren wie in Anspruch 1 beschrieben und das ferner Folgendes umfasst:
Bestimmen variabler Kosten für den vom Benutzer empfangenen Programminhalt, wobei die variablen Kosten mindestens teilweise auf der Gesamtzahl der Zeiträume und dem anfänglich betrachteten Zeitraum basieren.

9. Verfahren wie in Anspruch 2 beschrieben und das ferner Folgendes umfasst:
Bestimmen variabler Kosten für den vom Benutzer empfangenen Programminhalt, wobei die variablen Kosten mindestens teilweise auf der Gesamtzahl der Zeiträume und dem zuletzt betrachteten Zeitraum basieren.

10. Verfahren wie in Anspruch 2 beschrieben und das ferner Folgendes umfasst:
Bestimmen variabler Kosten für den vom Benutzer empfangenen Programminhalt, wobei die variablen Kosten mindestens teilweise auf dem anfänglich betrachteten Zeitraum und dem zuletzt betrachteten Zeitraum basieren.

11. Verfahren wie in Anspruch 1 beschrieben und das ferner Folgendes umfasst:
Aufzeichnen der Gesamtzahl von Zeiträumen in einem sicheren Prozessor eines Kundengeräts; und
Aktualisieren der Gesamtzahl von Zeiträumen in dem sicheren Prozessor während des Empfangs des Programminhalts.

12. Verfahren wie in Anspruch 1 beschrieben und das ferner Folgendes umfasst:
Erstellen einer ersten Aufzeichnung für ein erstes Ereignis von Programminhaltmaterial, wobei die Aufzeichnung den anfänglich betrachteten Zeitraum und

die Gesamtzahl der Zeiträume umfasst;
Erstellen einer zweiten Aufzeichnung für ein zweites Ereignis von unterschiedlichem Programminhaltmaterial, wobei die zweite Aufzeichnung einen anfänglich betrachteten Zeitraum des zweiten Ereignisses und eine Gesamtzahl von Zeiträumen des zweiten Ereignisses umfasst;
Verbinden der ersten Aufzeichnung mit der zweiten Aufzeichnung zur Übertragung an ein Gebührenabrechnungszentrum; und
kryptographisches Übertragen der verbundenen ersten und zweiten Aufzeichnung an das Gebührenabrechnungszentrum.

13. Verfahren wie in Anspruch 1 beschrieben und das ferner Folgendes umfasst:
Erstellen einer Aufzeichnung in einem sicheren Prozessor an einem Kundengerät, wobei die Aufzeichnung den anfänglich betrachteten Zeitraum und die Gesamtzahl der Zeiträume umfasst;
Übertragen der Aufzeichnung an einen NC-Prozessor an dem Kundengerät;
Übertragen der Aufzeichnung an ein Gebührenabrechnungssystem.

14. Verfahren, wie in Anspruch 13 beschrieben, wobei die Übertragung der Aufzeichnung an das Gebührenabrechnungssystem das Übertragen eines Endberichts an das Gebührenabrechnungssystem umfasst, um die aktualisierten Berichte, die an das Gebührenabrechnungssystem geschickt werden, zu reduzieren.

15. Verfahren, wie in Anspruch 14 beschrieben, wobei der Endbericht der einzige Bericht ist, der an das Gebührenabrechnungssystem für den Programminhalt geschickt wird.

Es folgen 10 Blatt Zeichnungen

100

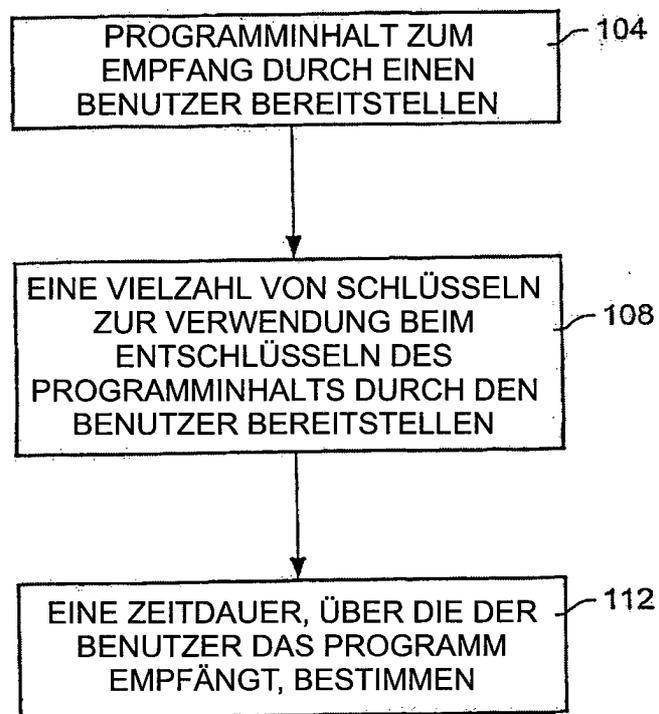


FIG. 1

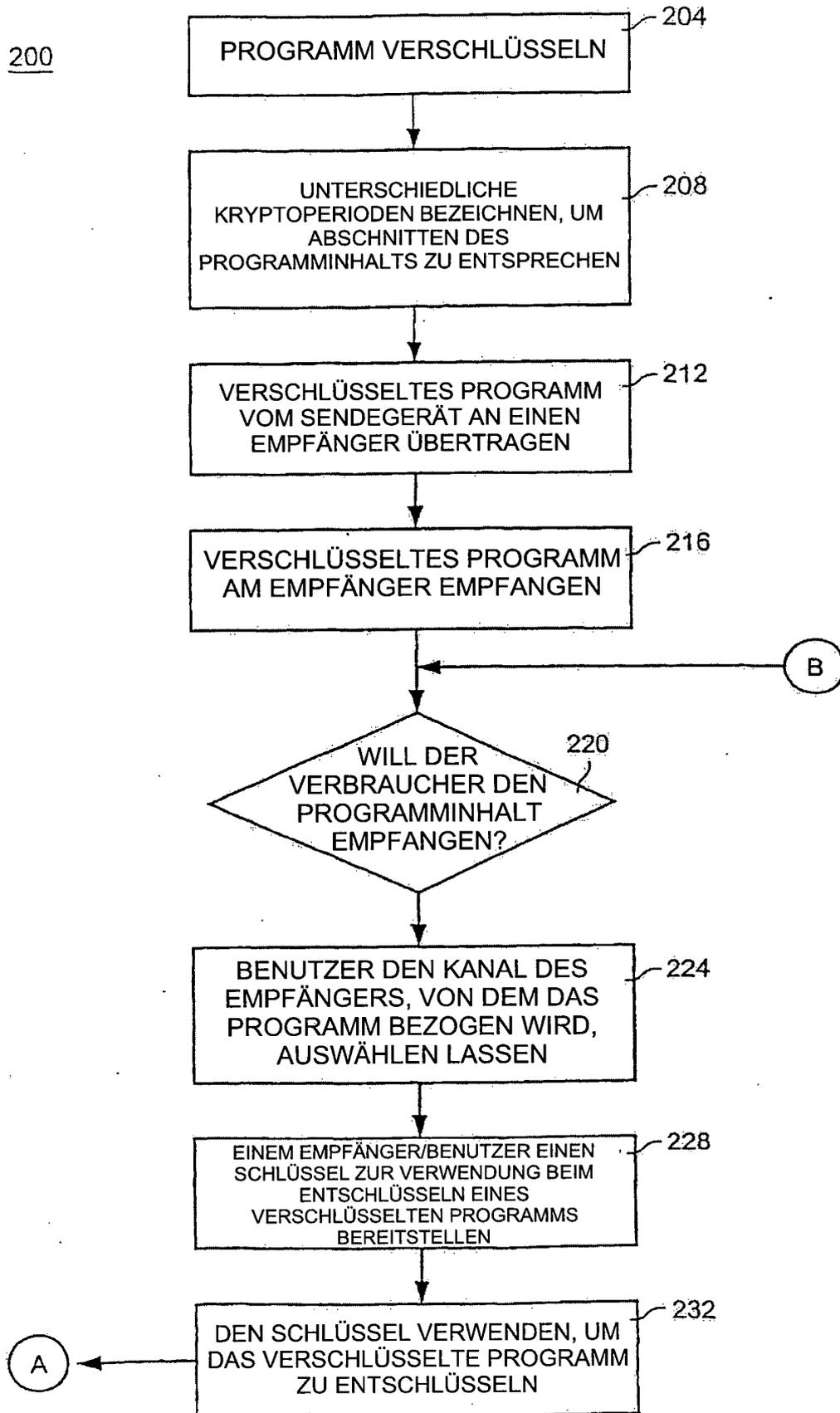


FIG. 2A

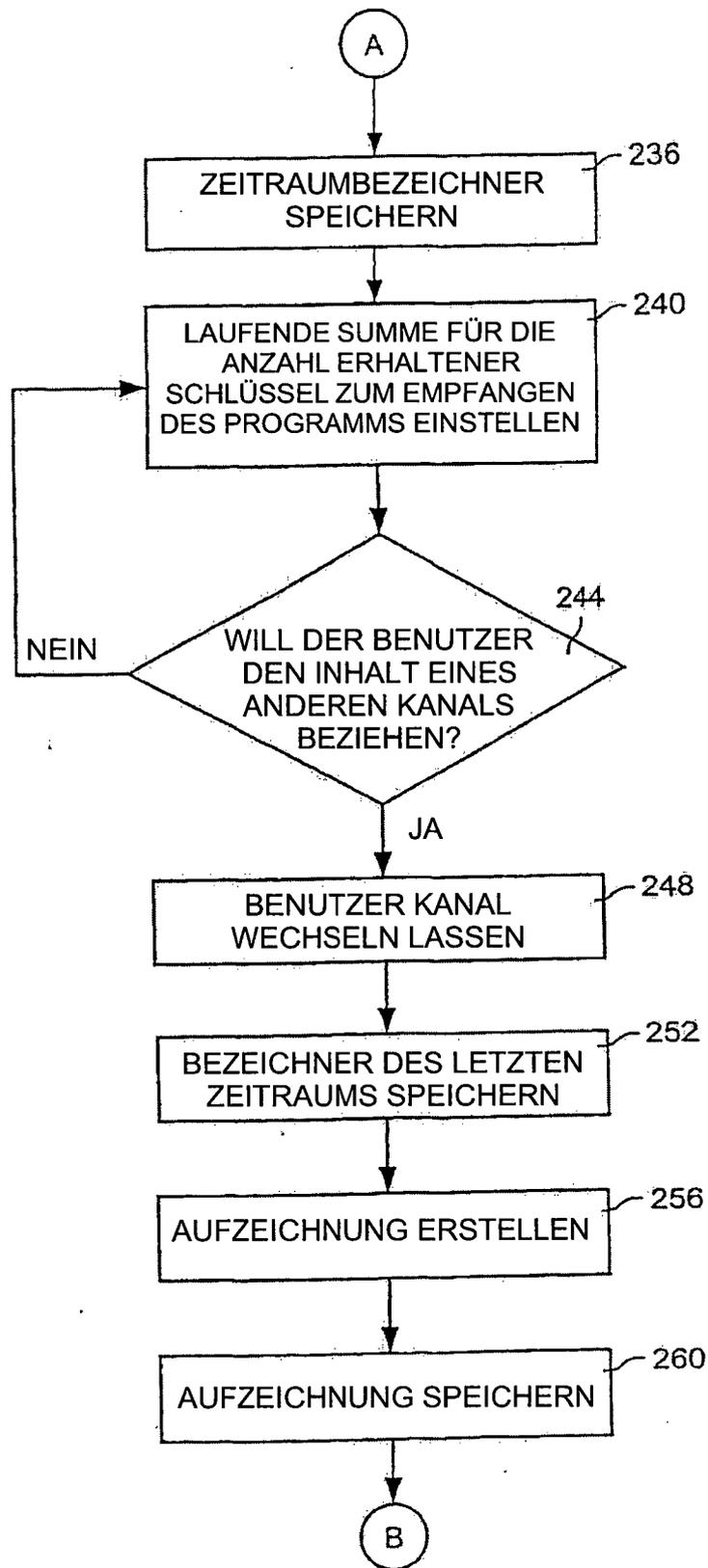


FIG. 2B

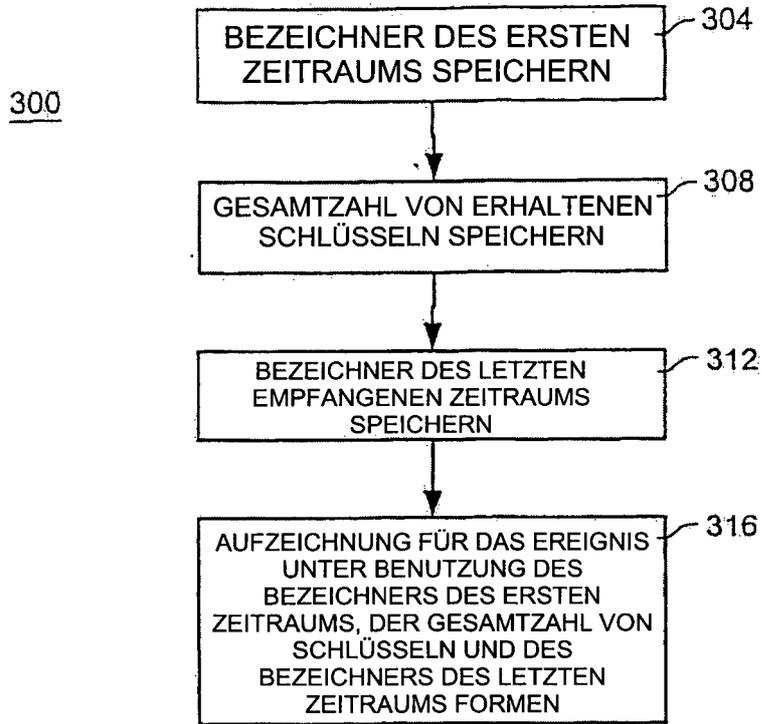


FIG. 3

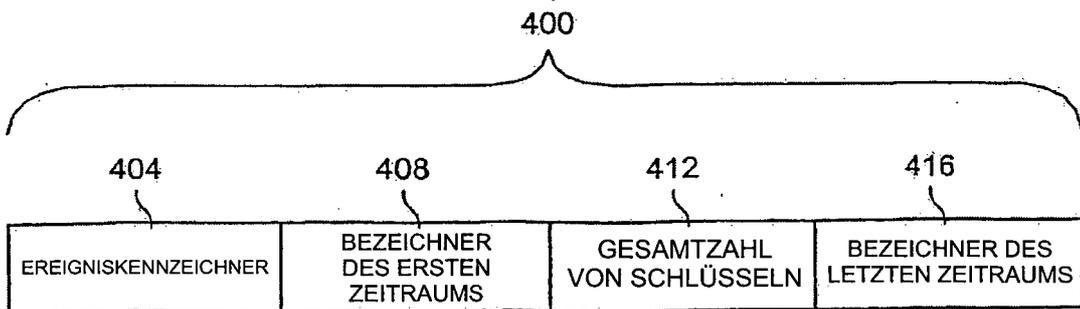


FIG. 4

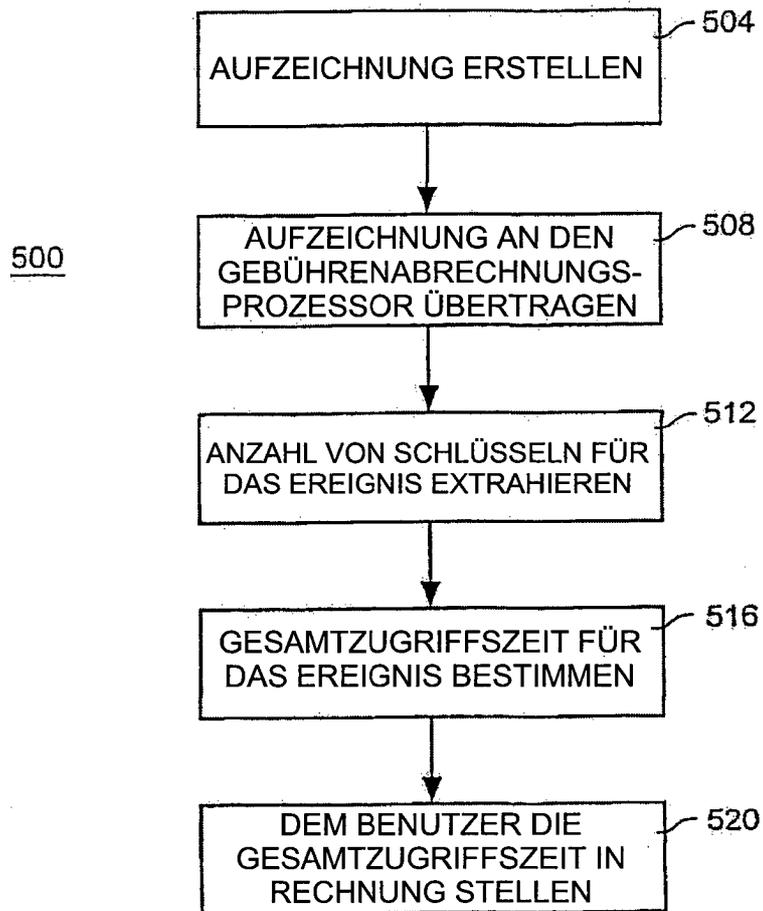


FIG. 5

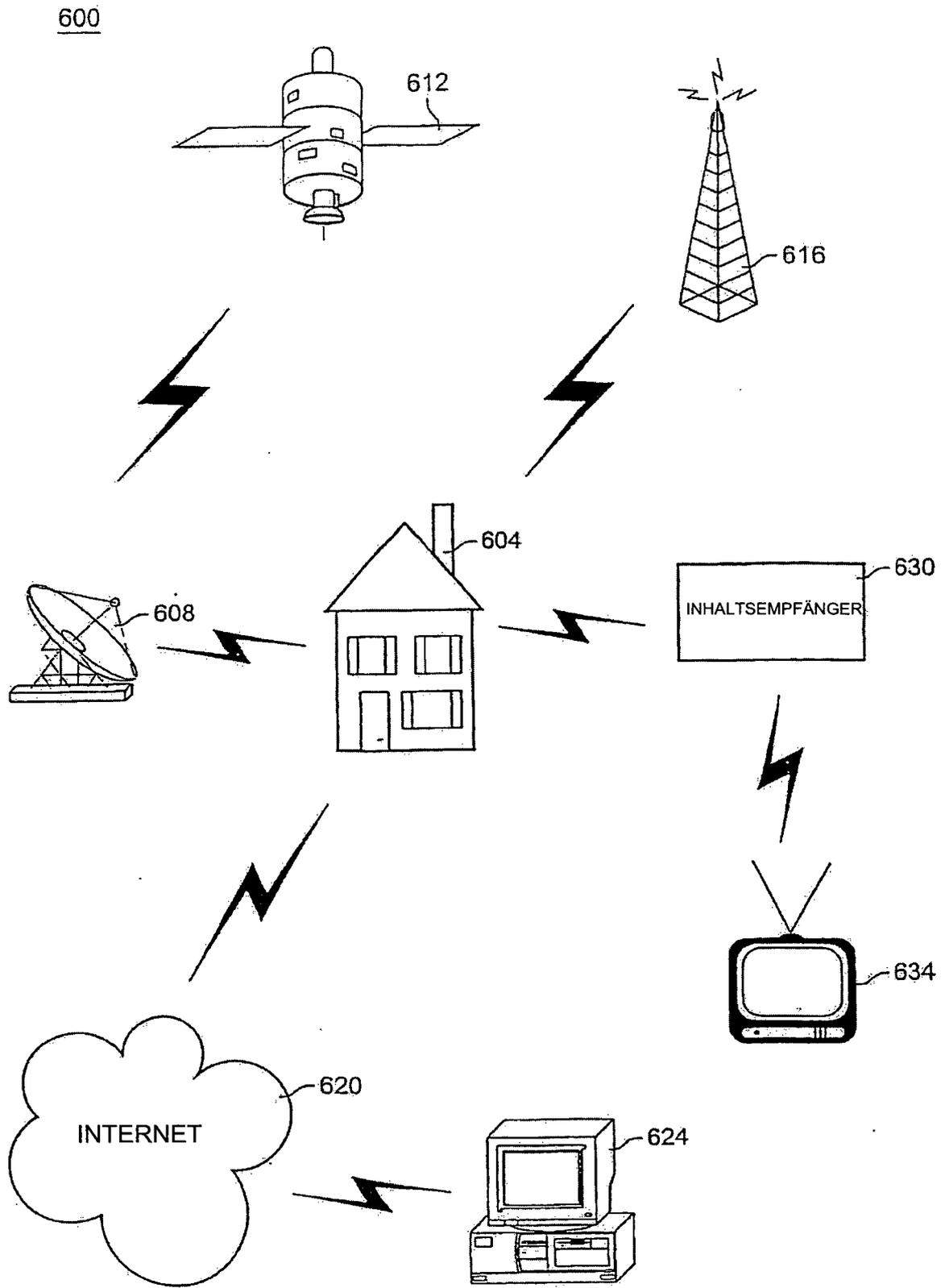


FIG. 6

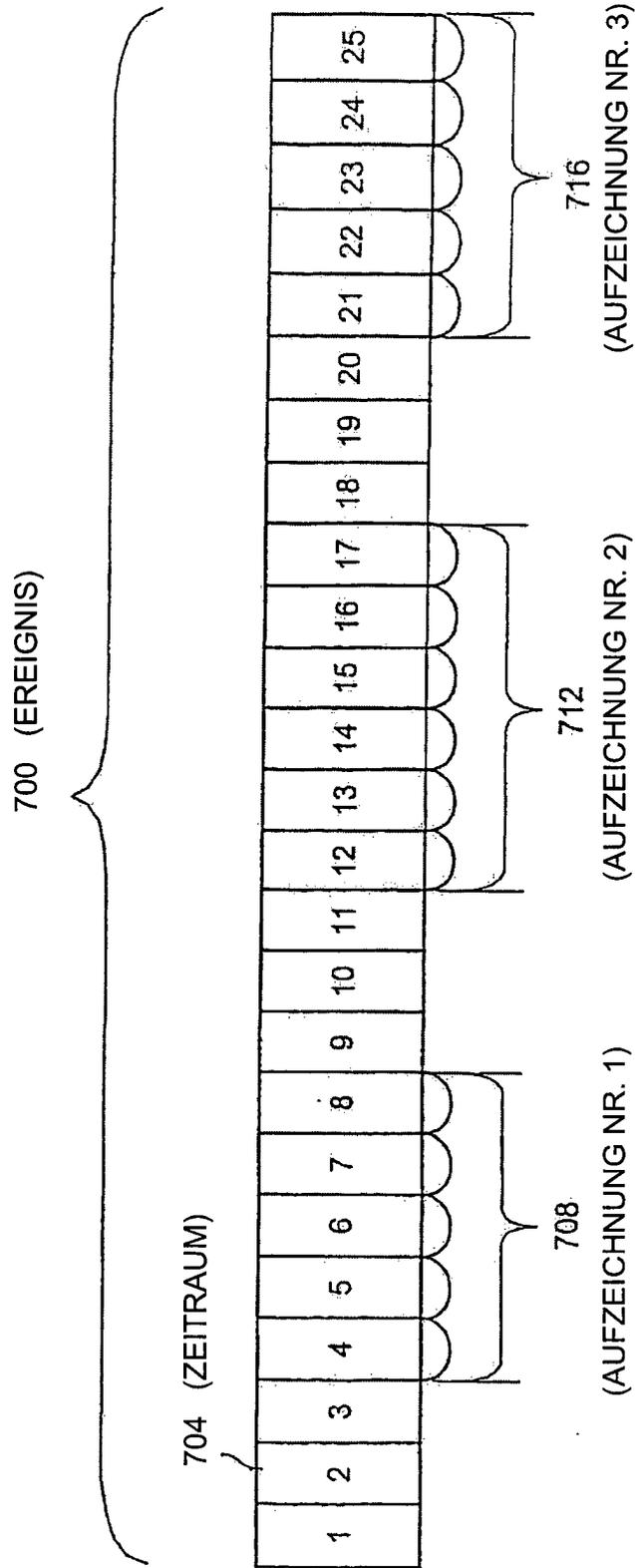


FIG. 7A

720

EREIGNIS	START	SUMME	ENDE
700	4	5	8

FIG. 7B

724

EREIGNIS	START	SUMME	ENDE
700	4	11	17

FIG. 7C

728

EREIGNIS	START	SUMME	ENDE
700	4	16	25

FIG. 7D

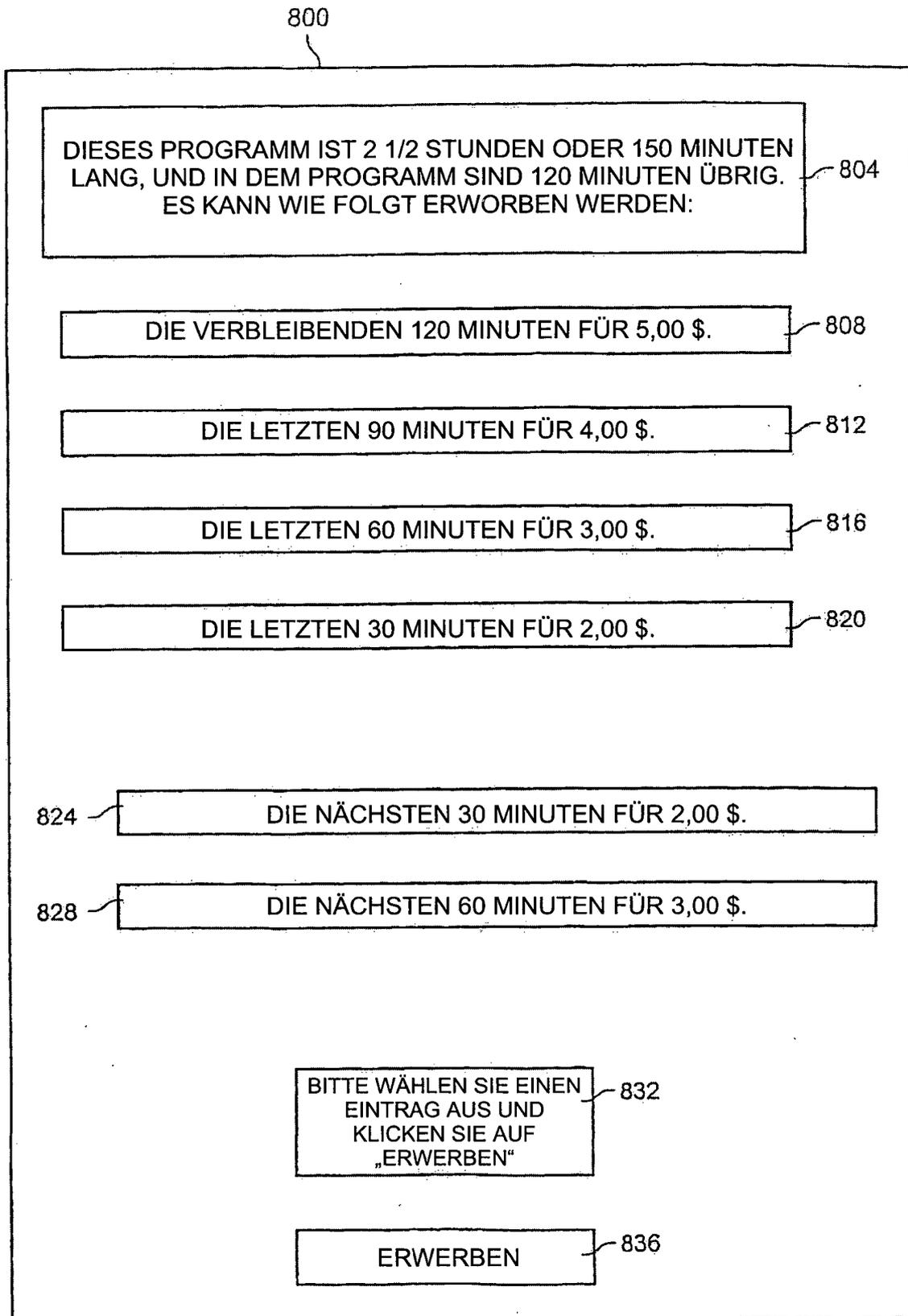


FIG. 8

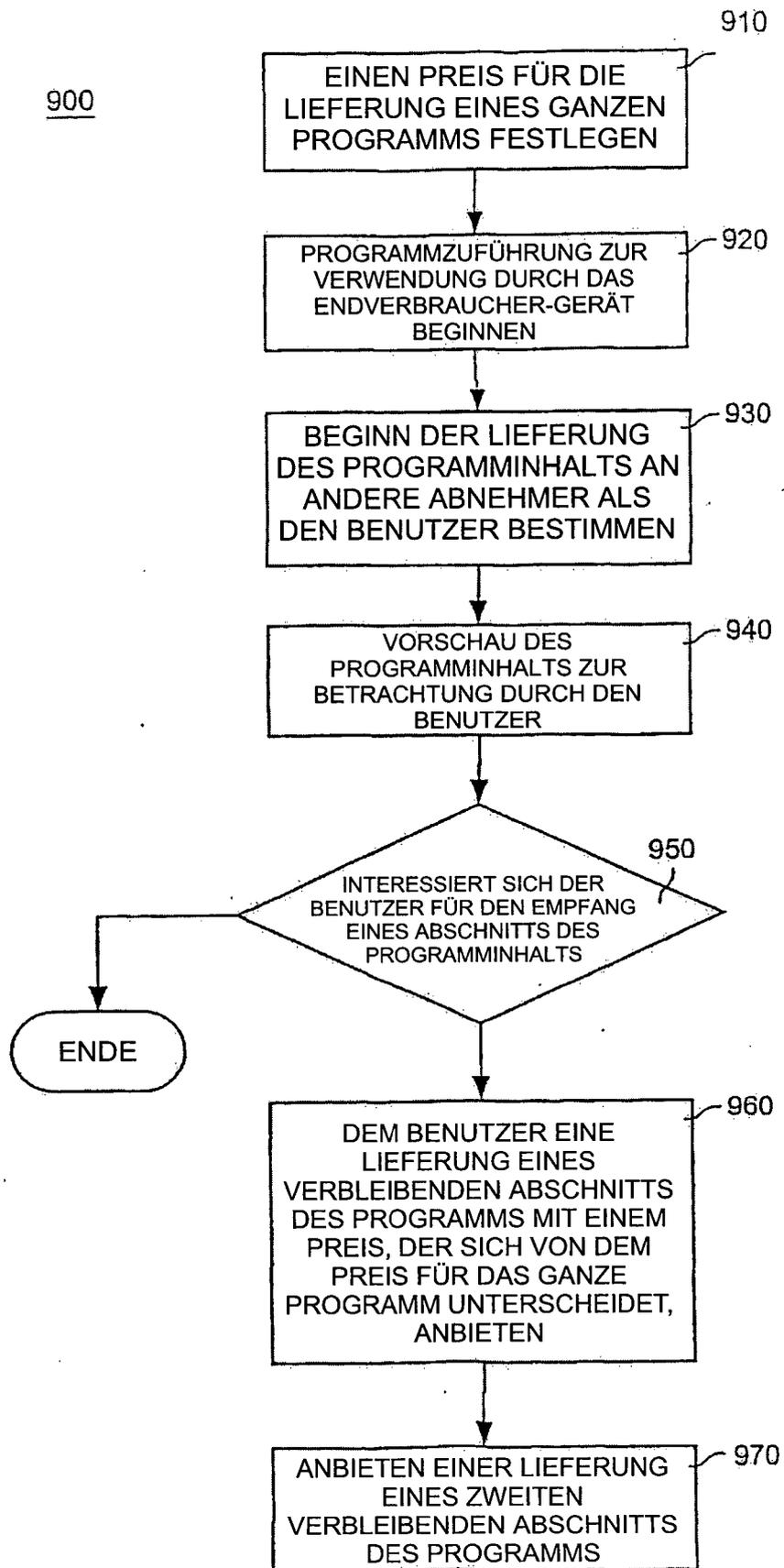


FIG. 9