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

(10) **DE 699 19 020 T2** 2004.12.09

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 133 338 B1**
(21) Deutsches Aktenzeichen: **699 19 020.7**
(86) PCT-Aktenzeichen: **PCT/FI99/00970**
(96) Europäisches Aktenzeichen: **99 958 207.5**
(87) PCT-Veröffentlichungs-Nr.: **WO 00/30725**
(86) PCT-Anmeldetag: **24.11.1999**
(87) Veröffentlichungstag der PCT-Anmeldung: **02.06.2000**
(97) Erstveröffentlichung durch das EPA: **19.09.2001**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **28.07.2004**
(47) Veröffentlichungstag im Patentblatt: **09.12.2004**

(51) Int Cl.[7]: **A63F 3/08**
A63F 13/00, G07F 17/32

(30) Unionspriorität:
982554 **25.11.1998** **FI**

(84) Benannte Vertragsstaaten:
AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LI, LU, MC, NL, PT, SE

(73) Patentinhaber:
Oy Veikkaus AB, Veikkaus, FI

(72) Erfinder:
RANTANEN, Anssi, FIN-00660 Helsinki, FI

(74) Vertreter:
Epping Hermann Fischer, Patentanwaltsgesellschaft mbH, 80339 München

(54) Bezeichnung: **METHODE UND SYSTEM ZUR DURCHFÜHRUNG VON SCHNELLEN ELEKTRONISCHEN LOTTERIEN**

Beschreibung

[0001] Die Erfindung betrifft allgemein die Übertragung vertraulicher Daten in einem Datennetzwerk. Die Erfindung betrifft insbesondere ein Verfahren und ein System zur Übertragung von Daten, die eine direkte Zuteilung eines nach dem Zufallsprinzip ermittelten Nutzens in einem Datennetzwerk in Reaktion auf eine geleistete Zahlung ermöglichen.

[0002] Herkömmliche Sofortgewinn-Lotterien basieren in der Regel auf Lotterielosen aus Papier oder Pappe, auf denen Informationen über einen möglichen Gewinn aufgedruckt sind, der mit dem Lotterielos angeboten wird. Die Informationen sind geschützt, beispielsweise mit einer Abreißlasche oder einer Abkratzoberfläche, die intakt sind, wenn das Los gekauft wird, und die vom Käufer erst abgelöst werden dürfen, wenn er das Los bezahlt hat.

[0003] Da Datenübertragungen und sogar Geldtransaktionen in zunehmendem Umfang elektronisch – in offenen Datennetzwerken wie beispielsweise dem Internet – abgewickelt werden, wäre es zweckmäßig, wenn man auch Dienstleistungsangebote wie Sofortgewinn-Lotterien auf elektronischem Weg in einem Datennetzwerk durchführen könnte. In diesem Zusammenhang meint "offenes Datennetzwerk" jede Art von Netzwerk oder Netzwerkkombination zur elektronischen Datenübertragung, wo die Datensicherheit kein inhärentes Element des Datennetzwerkes ist, sondern wo es nur mittels spezieller Verschlüsselungsroutinen möglich ist, auch vertrauliche Daten sicher zu übertragen. In dieser Patentanmeldung ist mit "elektronischen Sofortgewinn-Lotterien" ein Glücksspiel gemeint, bei dem der Kunde, d. h. der Mitspieler, einen Nutzen kauft, der gegen eine bestimmte Bezahlung sofort verfügbar ist, wobei der Wert des Nutzens nach dem Zufallsprinzip ermittelt wird. Bei Sofortgewinn-Lotterien mit elektronischen Benutzerschnittstellen können Lotterielose auf einer Anzeige bildlich nachgestellt werden, oder sie können in einer vollkommen anderen Art und Weise durchgeführt werden. Als ein Beispiel für verschiedene elektronische Sofortgewinn-Lotterien wäre ein interaktives Spiel denkbar, das über ein Datennetzwerk gespielt wird, wo ein Mitspieler durch Leistung einer Zahlung eine Klappe oder eine Tür öffnen kann, wodurch ein Objekt, ein Durchgang oder ein sonstiger Nutzen, der hinter der Tür zum Vorschein kommt, im wesentlichen nach dem Zufallsprinzip bestimmt wird.

[0004] Die Sicherheit ist beim Veranstalten elektronischer Sofortgewinn-Lotterien ein besonderes Problem. Spieler und Lotteriegesellschaft müssen in der Lage sein, einander als diejenigen zu authentifizieren, als die sie sich ausgeben. Der Inhalt von Daten, die ein Datennetzwerk durchlaufen, dürfen während der Übertragung nicht beschädigt werden, und dem Absender der Daten darf es nicht möglich sein, das Versenden seiner Daten hinterher nicht anzuerkennen. Außerdem darf es Dritten nicht möglich sein, den Schutz vertraulicher Daten zu durchbrechen. Allen Übertragungen von vertraulichen Daten über Datennetzwerke sind diese Merkmale gemein. Darüber hinaus umfasst im Fall elektronischer Sofortgewinn-Lotterien die Sicherheitsproblematik alle Vorbeugungsmaßnahmen gegen den Missbrauch des Systems. Beispielsweise könnte jemand in betrügerischer Absicht versuchen, die Gewinnlose und die damit verbundenen Gewinne herauszufinden, oder ein oder mehrere Mitspieler versuchen, elektronische Lotterielose zu erhalten, ohne die dafür fällige Gebühr bezahlt zu haben.

[0005] **Fig.** 1 zeigt ein herkömmliches System der Organisation von Sofortgewinn-Lotterien oder eines anderen Geldglücksspiels zumindest teilweise über ein Datennetzwerk. Der Computer **102** des Mitspielers und der Server der Lotteriegesellschaft sind mit dem Datennetzwerk **101** verbunden. Auf dem Server läuft ein Glücksspielprogramm **104**, in dem der Mitspieler Lose im generischen Sinn dieses Konzepts kaufen kann. Über den Spielzeitraum wird zwischen dem Computer **102** und dem Server **103** eine "geschützte" Sitzung aufgebaut, was in der Figur schematisch durch das Rohr **105** veranschaulicht ist. In dieser Sitzung werden alle oben genannten Merkmale, die für alle Übertragungen vertraulicher Daten gemeinsam gelten, realisiert.

[0006] Bei dem in **Fig.** 1 gezeigten System besteht das Problem, dass weder der Mitspieler noch die Glücksspielaufsichtsbehörde wissen, ob das Glücksspielprogramm **104** korrekt abläuft oder nicht. In der Praxis kann die Lotteriegesellschaft ihren Server beispielsweise so programmieren, dass ein Mitspieler nur sehr kleine Gewinne gewinnen kann. Da die Chancen auf Hauptgewinne in jedem Fall nur gering sind, kann der Mitspieler nicht wissen, ob er nicht gewinnt, weil er einfach kein Glück hat, oder ob er nicht gewinnt, weil die Lotteriegesellschaft ihn betrügt. Die Aufsichtsbehörde kann die Gewinnverteilung bestenfalls langfristig überprüfen und auf diese Weise versuchen herauszufinden, ob das Glücksspielprogramm in der Form funktioniert, wie die Lotteriegesellschaft es angegeben hat. Wenn die Lotteriegesellschaft ein Unternehmen mit mehreren Angestellten ist, so kann das Unternehmen an sich durchaus ehrliche Absichten hegen, doch es könnte passieren, dass ein oder mehrere Angestellte ihre Kenntnis der Struktur des Glücksspielprogramms dazu missbrauchen, sich unter Ausschluss des Zufallsprinzips Gewinne selbst zuzuweisen. Für die Lotteriegesellschaft, insbesondere bei Lotterien mit großen Einzelgewinnen, birgt das System von **Fig.** 1 das zusätzliche Problem, dass es nicht möglich ist, mit einem recht hohen Grad an Zuverlässigkeit eine Obergrenze für die Gesamtsumme der auszuzahlenden Gewinne festzusetzen.

[0007] Aus US-A-5,119,295, einer den Stand der Technik darstellenden Patentschrift der Telecredit, Inc. vom 2. Juni 1992, ist ein Verfahren und ein System für eine elektronische Sofortgewinn-Lotterie bekannt, bei der mehrere elektronische Sofortgewinnlose erzeugt werden. Jedes Los umfasst verschlüsselte Gewinndaten, die mit einem Los-bezogenen Schlüssel entschlüsselt werden können. Das System ermöglicht es Mitspielern, auf die gespeicherten elektronischen Sofortgewinnlose zuzugreifen und ein bestimmtes elektronisches Sofortgewinnlos zu erwerben. Bei diesem System nach dem Stand der Technik bleiben viele der oben angesprochenen Sicherheitsprobleme ungelöst.

[0008] Aufgabe der vorliegenden Erfindung ist es, ein Verfahren und ein System vorzuschlagen, die sicherer funktionieren als das oben beschriebene herkömmliche System. Eine weitere Aufgabe der Erfindung ist es, elektronische Sofortgewinn-Lotterien bereitzustellen, die für verschiedene Schnittstellen und Glücksspielsysteme Anwendung finden können.

[0009] Die Aufgaben der Erfindung werden durch die Verwendung verschlüsselter Lose und einer Schlüsseldatenbank, die von der Losdatenbank getrennt ist, gelöst.

[0010] Die Methode der Erfindung ist dadurch gekennzeichnet, dass sie folgende Schritte umfasst:

– Erzeugen und Speichern mehrerer Sofortgewinn-Lose, von denen ein jedes Gewinndaten umfasst, die verschlüsselt sind und mit einem Los-bezogenen Schlüssel entschlüsselt werden können;

– Speichern der Schlüssel, mit denen die verschlüsselten Gewinndaten gespeicherter elektronische Sofortgewinn-Lose entschlüsselt werden können, getrennt von den gespeicherten elektronischen Sofortgewinn-Losen;

– Bereitstellen eines Zugangs für einen bestimmten Mitspieler zu den gespeicherten elektronischen Sofortgewinn-Losen, dergestalt, dass der Mitspieler ein bestimmtes elektronisches Sofortgewinn-Los erwirbt; und

– Bereitstellen dieses Mitspielerzugangs zu den gespeicherten Schlüsseln, dergestalt, dass der Mitspieler einen Schlüssel erwirbt, der einem bestimmten elektronischen Sofortgewinn-Los zugeordnet ist.

[0011] Die Erfindung betrifft außerdem ein System, dass dadurch gekennzeichnet ist, dass es folgendes umfasst:

– ein erstes Datensystem zum Erzeugen wenigstens teilweise verschlüsselter elektronischer Sofortgewinn-Lose;

– ein zweites Datensystem zum Speichern der erzeugten wenigstens teilweise verschlüsselten elektronischen Sofortgewinn-Lose;

– ein drittes Datensystem zum Speichern der Los-bezogenen Schlüssel, mit denen die elektronischen Sofortgewinn-Lose entschlüsselt werden können, separat von den elektronischen Sofortgewinn-Losen;

– eine Datenübertragungsverbindung vom ersten Datensystem zum zweiten Datensystem und einem dritten Datensystem; und

– Mittel, mit denen einer Anzahl von Mitspielern eine Datenübertragungsverbindung zu dem zweiten Datensystem angeboten wird, um dem Mitspieler Zugang zu elektronischen Sofortgewinn-Losen zu gewähren, und mit denen dieser Anzahl von Mitspielern eine Datenübertragungsverbindung zu dem dritten Datensystem angeboten wird, um dem Mitspieler Zugang zu Schlüsseln, die den elektronischen Sofortgewinn-Losen zugeordnet sind, zu gewähren.

[0012] Die Verschlüsselung und Entschlüsselung von Nachrichten ist an sich bekannt. Gemäß der Erfindung wird jede Nachricht, die ein einzelnes elektronisches Los repräsentiert, separat verschlüsselt, und die verschlüsselten Lose werden in einer speziellen Losdatenbank gespeichert. Zusätzlich wird eine Schlüsseldatenbank eingerichtet, die einen Schlüssel enthält, der jedem einzelnen verschlüsselten Los zugeordnet ist, wobei der Schlüssel zum Entschlüsseln des Loses dient. Wenn ein Mitspieler ein bestimmtes Los erwirbt, so erhält er eine Nachricht, die das verschlüsselte Los repräsentiert, sowie eine Spielteilnahmequittung als Nachweis dafür, dass er das Los rechtmäßig erworben hat. Indem er seine Quittung der Schlüsseldatenbank vorlegt, erhält der Mitspieler einen Schlüssel, mit dem er das Los entschlüsseln kann. Wenn sich herausstellt, dass das Los einen Gewinn bedeutet, so kann der Mitspieler der Lotteriegesellschaft das Los und die Spielteilnahmequittungen als Nachweis über den rechtmäßigen Erhalt des Loses sowie den Schlüssel vorlegen, woraufhin die Lotteriegesellschaft dem Mitspieler den Gewinn übergibt. Die Reihenfolge, dass der Mitspieler zuerst Zugang zum Los und anschließend zum zugehörigen Schlüssel erhält, kann auch umgekehrt sein.

[0013] Eine Voraussetzung für das Gewährleisten der Sicherheit ist, dass die Lose durch eine spezielle Losdruckerei erzeugt und verschlüsselt werden, d. h. eine zuverlässige Partei, die nicht davon profitiert, ob die Gewinner-Lose verkauft werden oder nicht. Die Losdatenbank, die von der Losdruckerei erzeugt wurde und die die verschlüsselten Lose enthält, kann der Kontrolle der Lotteriegesellschaft unterstellt werden. Die Schlüsseldatenbank, die aus Schlüsseln besteht, die zum Entschlüsseln der Lose benötigt werden, kann der Kontrolle der Losdruckerei unterstellt werden oder kann einem bestimmten Schlüsselinhaber übergeben werden, bei dem es sich ebenfalls um eine zuverlässige Partei handelt, die nicht an dem

Glücksspiel beteiligt ist. Die Schlüsseldatenbank kann natürlich auch der Kontrolle der Lotteriegesellschaft unterstellt werden, was aber dazu führen kann, dass die Mitspieler weniger Vertrauen haben, dass alles mit rechten Dingen zugeht. Die Datenübertragungsverbindungen zwischen einem Mitspieler, einer Lotteriegesellschaft, einer Losdruckerei und einem Schlüsselinhaber über ein Datennetzwerk können mittels an sich bekannter Verfahren für die Übertragung vertraulicher Daten über ein Datennetzwerk geschützt werden.

[0014] Die Erfindung ist nachstehend näher erklärt, wobei auf beispielhafte bevorzugte Ausführungsformen und die begleitenden Zeichnungen bezug genommen wird. Es zeigen:

[0015] **Fig.** 1 zeigt ein herkömmliches elektronisches Glücksspielsystem.

[0016] **Fig.** 2 zeigt ein an sich bekanntes elektronisches Verschlüsselungssystem.

[0017] **Fig.** 3 zeigt ein elektronisches Zertifizierungssystem.

[0018] **Fig.** 4 zeigt das Prinzip der vorliegenden Erfindung.

[0019] **Fig.** 5a zeigt einen bevorzugten Aufbau eines elektronischen Loses.

[0020] **Fig.** 5b zeigt eine bevorzugte Datenbankorganisation.

[0021] **Fig.** 6 zeigt eine Methode gemäß der Erfindung.

[0022] **Fig.** 7 zeigt einen bevorzugten Aufbau einer Losanforderung.

[0023] **Fig.** 8 zeigt einen bevorzugten Aufbau einer Verkaufsquittung.

[0024] **Fig.** 9 zeigt einen bevorzugten Aufbau einer Antwortnachricht.

[0025] **Fig.** 10 zeigt einen bevorzugten Aufbau einer Schlüsselanforderungsnachricht.

[0026] **Fig.** 11 zeigt einen bevorzugten Aufbau einer Schlüsselquittung.

[0027] **Fig.** 12 zeigt einen bevorzugten Aufbau einer Schlüsselnachricht.

[0028] **Fig.** 13 zeigt einen bevorzugten Aufbau einer Gewinnbeanspruchungsnachricht.

[0029] **Fig.** 14 zeigt Bausteine des Systems gemäß der Erfindung.

[0030] **Fig.** 15 zeigt ein System gemäß der Erfindung.

[0031] **Fig.** 16 zeigt ein zweites System gemäß der Erfindung.

[0032] **Fig.** 17 zeigt ein drittes System gemäß der Erfindung.

[0033] Die oben besprochene Offenbarung nach dem Stand der Technik ist in **Fig.** 1 dargestellt, so dass sich die folgende Beschreibung der Erfindung und ihrer bevorzugten Ausführungsformen hauptsächlich auf die **Fig.** 2–17 bezieht. Für einander entsprechende Teile in den Figuren werden die gleichen Bezugszahlen verwendet.

[0034] In Verbindung mit der vorliegenden Erfindung werden vorzugsweise eine Reihe an sich bekannter Methoden zur Verschlüsselung und Entschlüsselung elektronischer Nachrichten verwendet. Um den Hintergrund der Erfindung darzulegen, werden diese Methoden als erstes erläutert.

[0035] Die Verschlüsselungsverfahren, die in Verbindung mit der elektronischen Datenverarbeitung Anwendung finden, lassen sich in symmetrische und asymmetrische Verfahren untergliedern. Die Erfindung als solche beschränkt nicht die Anwendung symmetrischer oder asymmetrischer Verfahren auf die Erfindung, auch wenn asymmetrische Verfahren für elektronische Lotterien aufgrund der solchen Lotterien innewohnenden Eigenheiten gewisse Vorteile mit sich bringen. In Verbindung mit der Erfindung sind auch Kombinationen aus symmetrischen und asymmetrischen Verfahren anwendbar.

[0036] Bei symmetrischen Verfahren wird zum Verschlüsseln und Entschlüsseln einer Nachricht derselbe Schlüssel verwendet. In diesem Fall muss sowohl die Person, welche die Nachricht verschlüsselt, als auch die Person, welche die Nachricht entschlüsselt, den Schlüssel kennen. Das bekannteste symmetrische Verfahren ist das Verfahren, das man das DES-Verfahren nennt (Data Encryption Standard). Bei asymmetrischen Verfahren bilden die Schlüssel einander entsprechende Paare, so dass eine Nachricht, die mit einem bestimmten ersten Schlüssel verschlüsselt wurde, mit einem zweiten Schlüssel entschlüsselt werden kann, welcher zum ersten Schlüssel passt. Die Person, welche die Verschlüsselung durchführt, braucht nicht den Entschlüsselungsschlüssel zu kennen, und umgekehrt braucht die Person, welche die Entschlüsselung durchführt, nicht den Verschlüsselungsschlüssel zu kennen. Das bekannteste asymmetrische Verfahren, das derzeit verwendet wird, ist das Verfahren, das man das RSA-Verfahren nennt (Rivest-Shamir-Adleman), wo-

bei der erste Schlüssel der "öffentliche Schlüssel" und der zweite Schlüssel der "private Schlüssel" heißt.

[0037] **Fig.** 2 zeigt ein System, das einen Absender (L) **201** und einen Empfänger (V) **202** umfasst. Der Absender kennt den öffentlichen Schlüssel AV_j des Empfängers, und der Empfänger kennt seinen eigenen privaten Schlüssel AV_y. Wenn der Absender **201** dem Empfänger **202** eine Nachricht S senden möchte, so verschlüsselt er sie vor dem Versenden mit dem öffentlichen Schlüssel des Empfängers, woraufhin die verschlüsselte Nachricht, die über die Datenübertragungsverbindung übertragen wird, als $AV_j(S)$ markiert werden kann. Nachdem der Empfänger **202** die verschlüsselte Nachricht erhalten hat, entschlüsselt er sie mit seinem privaten Schlüssel, was zu der ursprünglichen unverschlüsselten Nachricht führt. Dieser Schritt kann in folgender mathematischer Formel dargestellt werden:

$$AV_y[AV_j(S)] = S. \quad (1)$$

[0038] Die Schlüsseleigenschaften wurden so ausgewählt, dass es nahezu unmöglich ist, die verschlüsselte Nachricht mit etwas anderem zu öffnen als mit dem dafür vorgesehenen privaten Schlüssel des Empfängers.

[0039] Doch das oben beschriebene Verfahren überzeugt den Empfänger **202** nicht davon, dass die Nachricht von genau diesem Absender **201** stammt, da der öffentliche Schlüssel des Empfängers, der für die Verschlüsselung der Nachricht verwendet wurde, in der Regel öffentlich bekannt ist – wie schon der Name sagt. Die Authentizität des Absenders kann mit einer "digitalen Signatur" verifiziert werden, wobei man dem Prinzip folgt, dass der Absender **201** seinen eigenen privaten Schlüssel AL_y benutzt, um einen Teil der Nachricht zu verschlüsseln, und dass demzufolge der Empfänger den öffentlichen Schlüssel AL_j des Absenders benutzt, um diesen speziellen Teil der Nachricht zu entschlüsseln. Infolge der Schlüsseleigenschaften kann eine Nachricht, die mit einem bestimmten öffentlichen Schlüssel des Absenders entschlüsselt werden kann, nicht mit einem anderen Schlüssel verschlüsselt worden sein als mit dem speziellen privaten Schlüssel des Absenders.

[0040] Das Signaturverfahren kann im Grunde auch auf die gesamte Nachricht angewendet werden, woraufhin die Nachricht $AL_y[AV_j(S)]$ über die Datenübertragungsverbindung gesendet wird. Der vom Empfänger durchgeführte Entschlüsselungsschritt kann dann durch folgende Formel dargestellt werden.

$$AV_y[AL_j[AL_y[AV_j(S)]]] = AV_y[AV_j(S)] = S. \quad (2)$$

[0041] In der Praxis verwendet man gewöhnlich einen Hash, der mittels eines speziellen (fast) unzweideutigen Algorithmus' aus der Nachricht S gebildet wird und der in diesem Zusammenhang mit T(S) markiert werden kann. Der Hash dient als Prüfsumme, so dass, wenn der Inhalt der eigentlichen Nachricht beschädigt ist, derselbe Hash nicht mehr von ihm durch Berechnen gestört werden kann. Durch Vergleichen des ursprünglichen Hashs mit dem nachfolgend berechneten Hash kann man prüfen, ob die Nachricht nach ihrer Erzeugung modifiziert wurde. Ein Hash, der mittels des privaten Schlüssels des Absenders verschlüsselt wurde, wird mit T' markiert; d. h.

$$T' = AL_y[T(S)]. \quad (3)$$

[0042] Den verschlüsselten Hash T' nennt man die digitale Signatur des Absenders. Eine neue Nachricht S' wird gebildet, indem man der ursprünglichen Nachricht S den verschlüsselten Hash hinzufügt; d. h.

$$S' = S + T' \quad 4)$$

[0043] Diese neue Nachricht kann erforderlichenfalls mit dem öffentlichen Schlüssel des Empfängers weiter verschlüsselt werden, woraufhin die Nachricht $AV_j(S + T')$ über die Datenübertragungsverbindung gesendet wird. Der Empfänger **202** entschlüsselt zuerst die Nachricht mit seinem privaten Schlüssel und erhält so die Kombination S + T'. Wenn der davon getrennte verschlüsselte Hash T' mit dem öffentlichen Schlüssel des Absenders gemäß folgender Formel entschlüsselt wird:

$$AL_j[T'] = AL_j[AL_y[T(S)]] = T(S), \quad (5)$$

so weiß der Empfänger, dass der Hash nicht mit etwas anderem verschlüsselt worden sein kann als mit dem privaten Schlüssel des Absenders. Außerdem kann der Empfänger anhand des Hashs feststellen, dass der Inhalt der Nachricht seine Integrität behalten hat, seit sie vom Absender gebildet wurde.

[0044] Es wurde oben angenommen, dass öffentliche Schlüssel verlässlich einem bestimmten Inhaber zugeordnet werden können. Um dies zu gewährleisten, kann ein unabhängiger Dritter, in der Regel eine "Zertifizierungsinstitution" genannt, eingeschaltet werden. Das einfachste Verfahren besteht darin, dass die Zertifizierungsinstitution einen Index der öffentlichen Schlüssel aller Parteien herausgibt. Bei dieser Verfahrensweise muss aber dieser Index in jedem einzelnen Fall kontaktiert werden, um den Inhaber eines bestimmten öffentlichen Schlüssels zu überprüfen. Bei einem weiterentwickelten Verfahren erstellt die Zertifizierungsinstitution für jede Partei ein Zertifikat, wie in **Fig.** 3 veranschaulicht. Die Datenkommunikationspartei **301** legt der Zertifizierungsinstitution **302** ihren öffentlichen Benutzeridentifikator, ihren öffentlichen Schlüssel A_j und ihren Identitätsnachweis vor. Nachdem die Zertifizierungsinstitution anhand der oben genannten Elemente die Identität

der Datenkommunikationspartei **301** verifiziert hat, übergibt die Zertifizierungsinstitution der Partei ein Zertifikat gemäß der folgenden Formel und unter Nutzung der oben genannten Symbole:

$$\text{"Benutzer"} + A_j + AC_y(\text{"Benutzer"} + A_j), \quad (6)$$

wobei AC_y der private Schlüssel der Zertifizierungsinstitution ist. Wenn der zugehörige öffentliche Schlüssel AC_j öffentlich bekannt ist, so kann jeder das Zertifikat benutzen, um zu verifizieren, dass A_j der öffentliche Schlüssel ist, der von der Datenkommunikationspartei **301**, welche unter dem Benutzernamen "Benutzer" bekannt ist, verwendet wurde.

[0045] **Fig.** 4 ist eine schematische Darstellung einer bevorzugten Ausführungsform der Erfindung, die vier Parteien umfasst, die an dem Vorgang beteiligt sind: die Losdruckerei **401**, die Lotteriegesellschaft **402**, der Schlüsselinhaber **403** und der Mitspieler **404**. Die Datenübertragungsverbindungen zwischen den beteiligten Parteien verlaufen vorzugsweise über ein Datennetzwerk, obgleich sie in der Figur durch einzelne Linien dargestellt sind. Die Losdruckerei **401** hat die Aufgabe, elektronische Lose in Form von Datensätzen zu erstellen. Jeder Losdatensatz enthält einen unzweideutigen Identifikator und verschlüsselte Gewinndaten. Jeder Losdatensatz wurde mit einem separaten Los-bezogenen Schlüssel verschlüsselt. Die Losdruckerei erstellt eine Schlüsseldatenbank **405** aus Entschlüsselungsschlüsseln, die zu diesen Schlüsseln gehören, und diese Schlüsseldatenbank wird dem Schlüsselinhaber **403** übergeben. Die Losdatensätze werden in der Losdatenbank **406** gespeichert, die der Lotteriegesellschaft **402** übergeben werden. Die Lotteriegesellschaft führt auch eine Datenbank **407** der verkauften Lose und einen Gewinnauszahlungsdienst **408**, für den eine spezielle Gewinndatenbank **409** eingerichtet ist.

[0046] Wenn der Mitspieler **404** ein Los kaufen will, so kontaktiert er die Lotteriegesellschaft **402** und bezahlt das Los, d. h. er zahlt eine bestimmte Gebühr. Wie diese Zahlung erfolgt, wird weiter unten eingehender dargelegt. Nach Zahlung der Gebühr erhält der Mitspieler Zugang zu einem Los in der Losdatenbank und eine Quittung der rechtmäßig erfolgten Zahlung. Die Auswahl des Loses kann dem Mitspieler selbst überlassen bleiben, oder der Computer der Lotteriegesellschaft kann dies im Namen des Mitspielers übernehmen. Um bestimmte Sicherheitsrisiken auszuschalten, ist es bevorzugt, dass der Mitspieler sein Los nicht persönlich auswählen darf, sondern dass der Computer der Lotteriegesellschaft das Los nach dem Zufallsprinzip auswählt. Das ausgewählte Los wird aus der Losdatenbank **406** gelöscht oder wird als verkauft gekennzeichnet, damit dasselbe Los nicht zweimal verkauft wird. Gleichzeitig wird das Los in die Datenbank **407** der verkauften Lose eingegeben. Das die Losgewinndaten verschlüsselt sind, weiß der Mitspieler zu diesem Zeitpunkt noch nicht, ob er ein Gewinnlos erworben hat oder nicht.

[0047] Danach kontaktiert der Mitspieler den Schlüsselinhaber **403** und legt den Nachweis seines rechtmäßigen Kaufs eines bestimmten Loses vor, das er von der Lotteriegesellschaft erhalten hat. Zu dem Nachweis gehört ein unzweideutiger Losidentifikator, anhand dessen der Schlüsselinhaber **403** in der Schlüsseldatenbank **405** den Schlüssel sucht, der die Verschlüsselung dieses konkreten Loses entschlüsselt. Der Schlüsselinhaber übergibt den Schlüssel und den Nachweis über seinen Erhalt dem Mitspieler, der nunmehr Zugang sowohl zum Los als auch zu dem Schlüssel hat, mit dem er das Los entschlüsseln kann, um herauszufinden, ob es ein Gewinnlos ist oder nicht. Der Mitspieler besitzt auch Nachweise darüber, dass er Zugang zum Los und zum Schlüssel gemäß den Teilnahmebedingungen erhalten hat.

[0048] Der Mitspieler entschlüsselt das Los und den Schlüssel und prüft die Gewinndaten. Wenn das Los kein Gewinnlos war, so endet das Spiel an dieser Stelle. Wenn jedoch das Los Anspruch auf einen Gewinn verleiht, so kontaktiert der Mitspieler den Gewinnauszahlungsdienst **408** und legt das Los und die Nachweise, die er erhalten hat, vor. Der Gewinnauszahlungsdienst überprüft zuerst in seiner Datenbank **407** der verkauften Lose, ob dieses konkrete Los verkauft wurde. Anschließend verifiziert der Gewinnauszahlungsdienst die Nachweise, um zu bestätigen, dass der Spieler auf rechtmäßige Weise das Los erworben hat und in den Besitz des zugehörigen Entschlüsselungsschlüssels gelangt ist. Der Gewinnauszahlungsdienst überprüft des Weiteren, ob es sich bei dem Los tatsächlich um ein Gewinnlos handelt und dass der entsprechende Gewinn nicht schon abgeholt wurde. Wenn alle Verifizierungen erfolgreich vollzogen und keine Fehler festgestellt wurden, wird der Gewinn an den Mitspieler ausgezahlt.

[0049] **Fig.** 5a zeigt einen bevorzugten Aufbau eines Datensatzes, der zur Veranschaulichung eines elektronischen Loses verwendet werden kann. Der Datensatz **501** umfasst einen "primären" Losdatensatz **550** und ein Zusatzdatenfeld **560**. Der primäre Losdatensatz umfasst ein Klartext-Identifikatorfeld **502**, in dem ein unzweideutiger Losidentifikator steht. Außerdem umfasst der primäre Losdatensatz ein Gewinndatenfeld **503**, das Daten zur Höhe oder der Art des Gewinns **504** und außerdem eine Zufallszahl **505** enthält, die – aus einem weiter unten genannten Grund – zur "Maskierung" der Gewinndaten dient. Der Inhalt des Gewinndatenfeldes **503** ist mit der am weitesten innen liegenden digitalen Signatur **551** der Losdruckerei geschützt und mit einem bestimmten Los-bezogenen Schlüssel verschlüsselt. Die Verschlüsselung wird in der Figur durch die gerundeten Ecken des Gewinndatenfeldes **503** dargestellt. Bei

einer bevorzugten Ausführungsform der Erfindung ist das Gewinndatenfeld mit einem Schlüssel des symmetrischen Verschlüsselungsschlüssels, d. h. einem DES-Schlüssel, verschlüsselt. Es kann jedoch auch ein erster Los-bezogener Schlüssel in einem asymmetrischen Verschlüsselungssystem zur Verschlüsselung des Gewinndatenfeldes verwendet werden. Der primäre Losdatensatz, der durch das Identifikatorfeld **502** und das Gewinndatenfeld **503** gebildet wird, ist mit der zentralen digitalen Signatur **506** der Losdruckerei geschützt.

[0050] Das Zusatzdatenfeld **560** des Datensatzes **501** umfasst einen Hash **507**, der mittels einer unidirektionalen Funktion aus dem unverschlüsselten Gewinndatenfeld (Gewinndaten + eine Zufallszahl) erzeugt wurde, und einen Hash **508**, der mittels einer unidirektionalen Funktion aus dem Los-bezogenen Schlüssel, welcher die Gewinndaten entschlüsselt, erzeugt wurde. Außerdem kann der Hash, der aus dem Schlüssel erzeugt wurde, ebenfalls in den primären Losdatensatz aufgenommen werden, was jedoch nicht in **Fig.** 5 veranschaulicht ist. Die Los-bezogene Zufallszahl, die in dem Gewinndatenfeld neben den Gewinndaten enthalten ist, gewährleistet, dass die Gewinnlose nicht durch das Erzeugen von Hashs von allen potenziellen Gewinndaten erkannt werden können. Wenn zur Gewinndatenverschlüsselung das symmetrische Verfahren angewendet wurde, so wird in der Zukunft ein und derselbe Schlüssel als der Schlüssel angesehen. Wenn die Gewinndaten hingegen durch das asymmetrische Verfahren verschlüsselt wurden, so ist der Schlüssel, der zur Entschlüsselung benötigt wird, der zugehörige zweite Schlüssel des asymmetrischen Verfahrens. Unidirektionale Funktion bedeutet, dass die ursprünglichen Daten, aus denen der Hash berechnet wurde, oder der Modus der Hash-Berechnungsfunktion nicht aus dem durch sie erzeugten Hash hergeleitet werden kann. Außerdem wurde der gesamte Datensatz **501** mit der am weitesten außen gelegenen digitalen Signatur **509** der Losdruckerei signiert.

[0051] **Fig.** 5b zeigt die Datenbanken, die von der Losdruckerei erzeugt wurden, in einer bevorzugten Ausführungsform der Erfindung. Die Losdatenbank **510** ist einfach eine Datenbank, die eine Menge an Losdatensätzen **501** umfasst. Die Schlüsseldatenbank **511** umfasst einen Schlüsseldatensatz **512** für jeden Losdatensatz, der in der Losdatenbank **510** enthalten ist. Der Schlüsseldatensatz **512** umfasst einen Klartext-Losidentifikator **502** und den Schlüssel **513**, der für die Entschlüsselung des Loses benötigt wird. Der Schlüsseldatensatz ist mit der digitalen Signatur **514** der Losdruckerei signiert. Die Gewinndatenbank **515** ist eine Datenbank, die einen Gewinndatensatz **516** für jedes Los enthält. Der Datensatz umfasst einen Klartext-Losidentifikator **502** und einen Hash **507**, der aus dem Gewinndatenfeld des Loses berechnet wurde, und wurde mit der digitalen Signatur **517** der Losdruckerei geschützt.

[0052] **Fig.** 6 veranschaulicht im Detail ein bevorzugtes Verfahren für die Implementierung der Erfindung. Von den Parteien, die an dem Vorgang beteiligt sind, wurden die Losdruckerei **401**, die Lotteriegesellschaft **402**, der Schlüsselinhaber **403** und ein Mitspieler **404** separat veranschaulicht. Dem Fachmann leuchtet zwar ein, dass die elektronischen Sofortgewinn-Lotterien der Erfindung für eine sehr große Anzahl an Mitspielern gedacht sind, doch aus Gründen der Klarheit wird der Vorgang im Weiteren nur anhand eines einzigen Mitspielers beschrieben. Die Beschreibung kann ohne weiteres verallgemeinert und auf eine große Anzahl von Mitspielern angewendet werden. Verschiedene Passagen der folgenden Beschreibung beziehen sich auf öffentliche und private Schlüssel, weil davon ausgegangen wird, dass ein bestimmtes asymmetrisches Verschlüsselungssystem zum Verschlüsseln und Entschlüsseln bestimmter Nachrichten zur Verfügung steht.

[0053] In Schritt **605** erzeugt die Losdruckerei die Losdatenbank, die Schlüsseldatenbank und die Gewinndatenbank von **Fig.** 5b. Sie verschlüsselt die Losdatenbank und die Gewinndatenbank mit dem öffentlichen Transportschlüssel der Lotteriegesellschaft und sendet die verschlüsselten Datenbanken an die Lotteriegesellschaft. In ähnlicher Weise verschlüsselt die Losdruckerei die Schlüsseldatenbank mit dem öffentlichen Transportschlüssel des Schlüsselinhabers und sendet ihn an den Schlüsselinhaber. In Schritt **606** entschlüsselt die Lotteriegesellschaft die Transportverschlüsselung in der Losdatenbank und der Gewinndatenbank und installiert die Datenbanken auf einem bestimmten Lottoserver oder mehreren Lottoservern. In ähnlicher Weise entschlüsselt der Schlüsselinhaber in Schritt **607** die Transportverschlüsselung in der Schlüsseldatenbank und installiert sie auf einem bestimmten Schlüsselserver oder mehreren Schlüsselservern. Es werden Zugangsbeschränkungen, Firewalls, Kontrollen und sonstige Verfahren, die in der guten Datenschutzpraxis an sich bekannt sind, implementiert, um die Datenbanken, die auf den Spiel- und Schlüsselservern gespeichert sind, vor unbefugten Zugriffsversuchen zu schützen.

[0054] In Schritt **608** registriert sich der Mitspieler als Mitspieler in dem von der Lotteriegesellschaft betreuten Spielsystem. Zu Aufsichtszwecken kann vom Mitspieler verlangt werden, sich auch im System der Losdruckerei zu registrieren. Die Registrierung kann beispielsweise so organisiert werden, dass der Mitspieler von der Lotteriegesellschaft oder der Losdruckerei ein für das Spiel erforderliches Computerprogramm erhält. In Verbindung mit der Registrierung ist auch zweckmäßig, in dem von der Lotteriegesellschaft betreuten Datensystem ein Mitspielerkonto für den Mitspieler zu eröffnen, über das die Teilnahmegebühren und die Gewinnabholungen abgewickelt

werden. Elektronische Geldüberweisungen in einem Datennetzwerk oder in Verbindung mit einem Datennetzwerk sind an sich bekannt, und die Erfindung erlegt keinerlei Beschränkungen hinsichtlich der Durchführung solcher elektronischen Geldüberweisungen auf. Die Erfindung erfordert lediglich zwischen dem Mitspieler und der Lotteriegesellschaft ein Verfahrensarrangement, das es dem Mitspieler ermöglicht, die festgelegte Teilnahmegebühr zu bezahlen und Spielgewinne einzuziehen. In Schritt **608** erzeugt das für das Spiel erforderliche Computerprogramm außerdem die Anzahl an öffentlichen und privaten Schlüsseln, die der Mitspieler braucht. Um die Authentizität der öffentlichen Schlüssel zu gewährleisten, kann das oben beschriebene Zertifizierungsverfahren verwendet werden, wobei zum Beispiel die Losdruckerei als die Zertifizierungsinstitution fungiert.

[0055] In Schritt **609** entscheidet der Mitspieler, bei der Lotteriegesellschaft ein elektronisches Sofortgewinnlos zu kaufen. Das vom Mitspieler benutzte Computerprogramm erzeugt eine bestimmte Zufallszahl und errechnet anhand dieser Zahl einen Hash mit einer unidirektionalen Funktion. Der Mitspieler sendet über das Datennetzwerk eine Losanforderung an den Lottoserver der Lotteriegesellschaft. Die Anforderung erfolgt ganz besonders bevorzugt in der Form der Nachricht **701** von **Fig.** 7, die einen öffentlichen Schlüssel **702** für den Mitspieler, einen Hash **703** der oben erwähnten Zufallszahl und das Zertifikat **704** des Mitspielers umfasst. Die Nachricht ist mit der digitalen Signatur **705** des Mitspielers geschützt. Sie kann zusätzlich mit dem öffentlichen Schlüssel der Lotteriegesellschaft verschlüsselt werden. In Schritt **610** erhält die Lotteriegesellschaft die Nachricht, entschlüsselt eine Verschlüsselung mittels ihres privaten Schlüssels und identifiziert den Mitspieler anhand des in dem Zertifikat enthaltenen Benutzeridentifikators. Die Lotteriegesellschaft bucht den Los-Preis vom Mitspielerkonto ab und entnimmt der Losdatenbank nach dem Zufallsprinzip ein Los. Die Auswahl des Loses kann auch in der Weise getroffen werden, dass der Mitspieler zumindest den Eindruck bekommt, dass er das von ihm gewünschte Los persönlich auswählen darf. Beispielsweise kann auf dem Computerbildschirm des Mitspielers eine Lostrommel grafisch dargestellt werden, der der Mitspieler das von ihm gewünschte Los per Mausklick entnehmen kann. Im Interesse einheitlicher Bezugszahlen wird im Folgenden davon ausgegangen, dass das gewählte Los dasselbe ist, das oben in Verbindung mit den **Fig.** 5a und 5b erklärt wurde.

[0056] In Schritt **611** erzeugt die Lotteriegesellschaft eine Verkaufsquittung, die als Nachweis über den rechtmäßigen Erwerb eines bestimmten Loses durch einen bestimmten Mitspieler dienen soll. Bei der Verkaufsquittung handelt es sich ganz besonders bevorzugt um den Datensatz **801** von **Fig.** 8, der den Identifikator **502** des gewählten Loses, einen unzweideutigen Transaktionsidentifikator **802**, einen Schlüsselhash **508**, der in dem gewählten Los lesbar ist, und den Hash **703** der vom Mitspieler gesandten Zufallszahl umfasst. Die Lotteriegesellschaft schützt die oben erwähnten Verkaufsquittungsfelder mit ihrer digitalen Signatur **803**. Die Verkaufsquittung soll vom Schlüsselinhaber gelesen werden können, weshalb die Lotteriegesellschaft sie mittels des öffentlichen Schlüssels des Schlüsselinhabers verschlüsselt.

[0057] In Schritt **612** verschlüsselt die Lotteriegesellschaft den in dem gewählten Los enthaltenen primären Losdatensatz und die oben erzeugte Verkaufsquittung mittels des öffentlichen Schlüssels des Mitspielers und sendet beides an den Mitspieler. Für die Übertragung kann das Nachrichtenformular **901** von **Fig.** 9 verwendet werden. Es enthält den Transaktionsidentifikator **802**, den verschlüsselten primären Losdatensatz **550**, den verschlüsselten Verkaufsquittungsdatensatz **801** und das Zertifikat **902** der Lotteriegesellschaft. Die Nachricht ist mit der digitalen Signatur **903** der Lotteriegesellschaft geschützt. In der Regel ist es aber bevorzugt, ein Nachrichtenformular zu verwenden, in dem die gegenseitige Reihenfolge von Verschlüsselungen und Signaturen so gewählt wurde, dass die am weitesten außen liegende Operation immer eine Verschlüsselung ist. Das in **Fig.** 9 veranschaulichte Nachrichtenformular kann zum Beispiel zusätzlich mit dem öffentlichen Schlüssel des Mitspielers verschlüsselt werden. In **Fig.** 9 sind die Verschlüsselungen mit gerundeten Ecken, die mit Strichlinien gezeichnet sind, dargestellt.

[0058] In Schritt **613**, der vor oder nach dem Schritt **612** vollzogen werden kann, entfernt die Lotteriegesellschaft das verkaufte Los aus der Losdatenbank und erzeugt einen Datensatz in der Datenbank der verkauften Lose, der ganz besonders bevorzugt wenigstens den Transaktionsidentifikator, den verschlüsselten primären Losdatensatz, den verschlüsselten Verkaufsquittungsdatensatz und den Gewinndatenhash umfasst. Die Speicherung der Verkaufstransaktion in der Datenbank der verkauften Lose garantiert, dass, wenn ein Datenübertragungsfehler oder eine andere zeitweilige Störung verhindert, dass der Mitspieler die Antwortnachricht **901** erhält, die zu dem von ihm gekauften Los gehört, der Mitspieler die Lotteriegesellschaft bitten kann, sie ihm noch einmal zuzuschicken.

[0059] In Schritt **614** erhält der Mitspieler eine Nachricht **901**. Wenn die Nachricht in ihrer Gesamtheit mit dem öffentlichen Schlüssel des Mitspielers verschlüsselt ist, so entschlüsselt er sie mit seinem privaten Schlüssel. Mit seinem privaten Schlüssel entschlüsselt der Mitspieler den primären Losdatensatz und die am weitesten außen liegende Verschlüsselung des Verkaufsquittungsdatensatzes. Gleichzeitig vergewissert er sich anhand der in dem primären

Losdatensatz enthaltenen digitalen Signatur der Losdruckerei, dass die erhaltene Nachricht wirklich ein von der Losdruckerei erzeugtes Los enthielt, das nicht beschädigt war.

[0060] Als nächstes erwirbt der Mitspieler vom Schlüsselinhaber einen Schlüssel, der es ihm ermöglicht, das von ihm gekaufte Los zu entschlüsseln. Wenn der Mitspieler noch keinen Zugang zu dem öffentlichen Schlüssel des Schlüsselinhabers hat, so erwirbt er ihn auf eine an sich bekannte Weise. In Schritt **615** sendet der Mitspieler eine Schlüsselanforderungsnachricht an den Schlüsselinhaber, wobei es sich bei der Nachricht ganz besonders bevorzugt um eine Nachricht **1001** handelt, wie sie in **Fig.** 10 gezeigt ist. Sie enthält den Identifikator **502** des gekauften Loses, die Verkaufsquittung **801** (die noch immer mit dem öffentlichen Schlüssel des Schlüsselinhabers verschlüsselt ist), die zuvor vom Mitspieler erzeugte Zufallszahl **703'** (d. h. nicht der Hash dieser Zufallszahl), den öffentlichen Schlüssel **702** des Mitspielers und das Zertifikat **704** des Mitspielers. Wenn der Schlüsselhash nicht im primären Losdatensatz enthalten ist, so kann die Schlüsselanforderungsnachricht auch den Schlüsselhash in der Form enthalten, in der der Mitspieler ihn in dem von ihm erhaltenen primären Losdatensatz gelesen hat. Die Nachricht **1001** ist mit der digitalen Signatur **1002** des Mitspielers geschützt und kann mit dem öffentlichen Schlüssel des Schlüsselinhabers für die Übertragung verschlüsselt werden. Die Verschlüsselung ist in **Fig.** 10 mit abgerundeten Ecken, die in Strichlinien gezeichnet sind, veranschaulicht. Wie oben angesprochen, ist es in der Regel bevorzugt, als am weitesten außen liegende Operation eine Verschlüsselung anstelle einer digitalen Signatur zu wählen.

[0061] In Schritt **616** erhält der Schlüsselinhaber eine Nachricht **1001**, entschlüsselt die Verschlüsselung mittels seines privaten Schlüssels und entschlüsselt die in der Nachricht enthaltene Verkaufsquittungsverschlüsselung. Die Verkaufsquittung gibt dem Schlüsselinhaber die Bestätigung, dass die vom Mitspieler gesandte Schlüsselanforderung auf einem Los basiert, dass rechtmäßig bei der Lotteriegesellschaft erworben und ordnungsgemäß bezahlt wurde. Durch Vergleichen der vom Mitspieler gesandten Zufallsnummer mit ihrem in der Verkaufsquittung enthaltenen Hash vergewissert sich der Schlüsselinhaber, dass es sich bei dem Mitspieler, der die Schlüsselanforderung stellt, um genau den Mitspieler handelt, der dieses spezielle Los gekauft hat, weil nur dieser Mitspieler diese spezielle Zufallsnummer haben kann. Wenn die Überprüfung nichts Verdächtiges ergibt, ruft der Schlüsselinhaber diesen Schlüsseldatenbatz aus der Schlüsseldatenbank ab und überprüft zusätzlich mittels des Schlüsselhashs, der in der Verkaufsquittung – oder ansonsten in der Nachricht **1001** – enthalten ist, dass der Mitspieler tatsächlich ein Los gekauft hat, das zu diesem speziellen Schlüssel passt. Der Schlüsselinhaber protokolliert außerdem alle Daten im Zusammenhang mit der Schlüsselanforderung und der Schlüsselübergabe in einer speziellen Log-Datenbank.

[0062] In Schritt **617** erzeugt der Schlüsselinhaber eine Quittung der Schlüsselübergabe. Die Quittung gleicht ganz besonders bevorzugt derjenigen, die in **Fig.** 11 gezeigt ist, und sie umfasst den Transaktionsidentifikator **802** und das Zertifikat **1102** des Schlüsselinhabers in einer bestimmten Nachricht **1101**. Die Quittung ist zusätzlich mit der digitalen Signatur **1103** des Schlüsselinhabers geschützt, und da sie dafür bestimmt ist, von der Lotteriegesellschaft gelesen zu werden, ist sie mittels des öffentlichen Schlüssels der Lotteriegesellschaft verschlüsselt. Des Weiteren sendet der Schlüsselinhaber in Schritt **617** dem Mitspieler den Schlüssel, den er angefordert hat, in einer Nachricht, die ganz besonders bevorzugt derjenigen gleicht, die in **Fig.** 12 gezeigt ist. Die Nachricht **1201** umfasst einen Schlüsseldatensatz **512**, die oben erzeugte Schlüsselübergabequittung **1101** und die digitale Signatur **1202** des Schlüsselinhabers. Zur Übertragung wird die Schlüsselnachricht **1201** mit dem öffentlichen Schlüssel des Mitspielers verschlüsselt.

[0063] In Schritt **618** hat der Mitspieler die Schlüsselnachricht 1201 vom Schlüsselinhaber erhalten und kann beginnen zu überprüfen, ob das Los, das er gekauft hat, ein Gewinnlos ist. Der Mitspieler entschlüsselt die Schlüsselnachricht mit seinem privaten Schlüssel und überprüft mittels der in dem Schlüsseldatensatz enthaltenen digitalen Signatur, dass der Schlüsseldatensatz von der Losdruckerei stammt, dass er nicht während der Übertragung beschädigt wurde und dass er zu dem Los gehört, das sich im Besitz des Mitspielers befindet. Der Mitspieler entschlüsselt die Gewinndaten in dem Los mittels des in dem Schlüsseldatensatz enthaltenen Schlüssels und erfährt, ob das Los einen Gewinn beinhaltet oder nicht. Wenn das Los kein Gewinnlos war, so endet das Spiel damit.

[0064] Im Weiteren wollen wir aber davon ausgehen, dass das Los ein Gewinnlos ist. In diesem Fall stellen die Gewinndaten, die zwar entschlüsselt wurden, aber noch immer mit der am weitesten innen liegenden digitalen Signatur der Losdruckerei geschützt sind, eine Gewinnquittung dar. Anschließend geht der Mitspieler in Schritt **618** dazu über, eine an die Lotteriegesellschaft zu sendende Gewinnbeanspruchungsnachricht zu erzeugen, vorzugsweise eine Nachricht wie die in **Fig.** 13 gezeigte Nachricht **1301**. Sie umfasst den Transaktionsidentifikator **802**, die Gewinnquittung **1302**, die vom Schlüsselinhaber übergebene Schlüsselübergabequittung **1101** und das Zertifikat **704** des Mitspielers. Sie ist mit der digitalen Signatur **1303** des Mitspielers geschützt. Zur Übertragung verschlüsselt der Mitspieler die Gewinnbeanspruchungsnachricht **1301** ganz besonders be-

vorzugt mit dem öffentlichen Schlüssel der Lotteriegesellschaft, zu dem der Mitspieler in einem vorherigen Schritt mittels eines an sich bekannten Verfahrens Zugriff erhalten hat.

[0065] In Schritt **619** hat die Lotteriegesellschaft die Nachricht **1301** erhalten und hat eine Verschlüsselung dieser Nachricht mittels ihres privaten Schlüssels entschlüsselt. Die Lotteriegesellschaft überprüft die Authentizität der Gewinnquittung mittels der darin enthaltenen digitalen Signatur der Losdruckerei und mittels Vergleichen der Gewinnquittung mit den Daten in der Gewinndatenbank. Unter Verwendung desselben Losidentifikators sollte es möglich sein, in der Gewinndatenbank einen Datensatz zu finden, der denselben Hash umfasst wie der Hash, der anhand des Gewinndatenfeldes in der Gewinnquittung berechnet wurde. Außerdem erklärt die Lotteriegesellschaft mittels der vom Schlüsselinhaber übergebenen Quittung **1101**, dass der Mitspieler den Schlüssel auf rechtmäßige Weise erworben hat. Die Lotteriegesellschaft überprüft nun, ob dieses konkrete Los verkauft wurde, indem sie in der Datenbank der verkauften Lose nachsieht. Wenn diese Überprüfungen nichts Verdächtiges zu Tage fördern, so wird dem in der Gewinnbeanspruchungsnachricht genannten Mitspielerkonto der durch den Gewinn bezeichnete Betrag gutgeschrieben, das Los wird aus dem Datensatz der verkauften Lose gelöscht, und der Gewinn wird in der Gewinndatenbank als "abgeholt" gekennzeichnet.

[0066] Die oben beschriebene Verfahrensweise kann auf verschiedene Weise modifiziert werden, ohne dass der Geltungsbereich der vorliegenden Erfindung verlassen wird. Viele Varianten bestehen darin, dass sie die Sicherheit des Systems weiter erhöhen. Die Aufgabe einer Variante besteht darin, dass ein Mitspieler selbst dann, wenn er versehentlich die Daten gekaufter Lose vernichtet, für die mögliche Gewinne noch nicht abgeholt wurden, die Situation dadurch retten könnte, dass er die Lotteriegesellschaft bitte, die gekauften Lose noch einmal zuzusenden. Das kann beispielsweise dergestalt geschehen, dass der Mitspieler beim Kauf eines Loses die für diese Kauftransaktion erzeugte Zufallszahl mittels seines öffentlichen Schlüssels verschlüsselt und sie der Lotteriegesellschaft zusammen mit dem Transaktionsidentifikator zusendet. Die Lotteriegesellschaft speichert die Daten in der Datenbank, von wo sie bei Bedarf anhand der Transaktionsnummer abgerufen werden können. Der Mitspieler kann letztendlich darum bitten, dass ihm die Daten, die in der Datenbank der Lotteriegesellschaft gespeichert sind, erneut zugesandt werden, kann dann die Zufallszahl mit seinem privaten Schlüssel entschlüsseln und anschließend die Lotteriegesellschaft bitten, die Daten der vernichteten Lose erneut zuzusenden, die die Lotteriegesellschaft in der Datenbank der verkauften Lose liest.

[0067] Damit der Schlüsselinhaber dem Mitspieler den Schlüssel für dasselbe Los wiederholt übergeben kann, muss die Lotteriegesellschaft dem Mitspieler eine neue Verkaufsquittung in Verbindung mit der wiederholten Losanforderung geben, wobei die Verkaufsquittung ausweist, dass es sich um eine wiederholte Anforderung handelt. Sollte der Gewinn des Loses bereits abgeholt worden sein, so ist es natürlich unmöglich, die erneute Anforderung zu stellen, oder zumindest darf die Lotteriegesellschaft trotz der Anforderung keine Daten über die verkauften Lose übermitteln.

[0068] Es wurde oben angesprochen, dass der Schlüsselhash auch während des Schrittes des Erstellens der Losdatenbank in dem primären Losdatensatz aufgenommen werden kann, und dann erreicht er schließlich den Mitspieler, nachdem das Los gekauft wurde. Dies würde es dem Mitspieler, nachdem er den Schlüssel angefordert und erhalten hat, ermöglichen zu prüfen, ob der Hash, der aus dem Schlüssel berechnet wurde, den er erhalten hat, mit dem Schlüsselhash identisch ist, der zusammen mit dem Los übergeben wurde. Wenn die Hashs nicht identisch sind, so kann der Mitspieler feststellen, dass es auf irgend einer Stufe einen Fehler gegeben hat, der entweder den Inhalt eines Datensatzes beschädigt hat oder der zur Übermittlung des falschen Schlüsseldatensatzes vom Schlüsselinhaber zum Mitspieler geführt hat.

[0069] Es wurde oben wiederholt angemerkt, dass speziell die Lotteriegesellschaft und der Schlüsselinhaber eine Vielzahl von Überprüfungen durchführen, um sich zu vergewissern, ob eine bestimmte Nachricht mit einem rechtmäßigen Spielvorgang verknüpft ist oder nicht. Die Erfindung beschränkt nicht die Maßnahmen, die in einer Situation ergriffen werden, wo eine Überprüfung einen Fehler in einer Nachricht, in einem Datensatz oder in einem sonstigen Datenelement aufdeckt. Jedoch wird in einer solchen Situation das Spiel in der Regel unterbrochen, alle Arten von Gewinnauszahlungen in Verbindung mit dieser speziellen Spielrunde werden verhindert, und alle zu dieser Runde verfügbaren Daten werden in einer speziellen Fehlerdatenbank gespeichert, was es der Lotteriegesellschaft und/oder dem Schlüsselinhaber bzw. den Schlüsselinhabern ermöglicht, die Fehlerursache herauszufinden, die an der Spielrunde beteiligten Parteien zu ermitteln und festzustellen, ob hinter dem Fehler ein Betrugsversuch durch eine der Parteien steckt.

[0070] Eine Variante der oben beschriebenen Verfahrensweise ist es, die Losdatenbank periodisch um neue Lose zu ergänzen, bevor die Anzahl der verbleibenden unverkauften Lose unter einen bestimmten Schwellenwert sinkt. Diese Maßnahme verhindert insbesondere eine Situation, in der es eine außergewöhnlich große Zahl an Gewinnlosen unter den ver-

bliebenen unverkauften Losen gibt und die Gesamtgewinnsumme der Gewinnlose ihren Gesamtpreis übersteigt. Da Lose in einer im Wesentlichen zufälligen Reihenfolge verkauft werden, wäre eine solche Situation durchaus vorstellbar, wenn die Losdatenbank nicht wieder aufgefüllt werden würde. Wenn jemand herausfindet, dass eine solche Situation eingetreten ist, so würde es sich für denjenigen lohnen, alle restlichen Lose aufzukaufen.

[0071] Bei der Realisierung von Verschlüsselungsarrangements sollte beachtet werden, dass Computer mit immer höherer Rechenleistung ausgestattet werden. Alle auf Berechnungen beruhenden Verschlüsselungssysteme können geknackt werden, sofern ausreichende Ausgangsdaten, Rechenleistung und Zeit zur Verfügung stehen. Wenn die verfügbaren Schlüssel lang sind, d. h. wenn der verfügbare Schlüsselplatz groß ist, so wird immer noch sehr viel Zeit benötigt, auch wenn Rechenleistung zur Verfügung steht, die viel höher ist als die derzeit verfügbare. Die Größe des Schlüsselplatzes wird zweckmäßigerweise so gewählt, dass die absehbare Steigerung der Rechenleistung nicht ausreicht, um die Verschlüsselungssysteme während der prognostizierten Betriebsdauer des Systems knacken zu können.

[0072] Die Losdruckerei und der Schlüsselinhaber müssen nicht unbedingt zwei getrennte Parteien sein, sondern können stattdessen – weil sie in dem oben beschriebenen System beide als unabhängige "Dritte" angenommen wurden – auch ein und dieselbe Partei sein. Anderseits hindert die Lotteriegesellschaft nichts daran, gleichzeitig als Schlüsselinhaber zu fungieren, sofern die Losdatenbank und die Schlüsseldatenbank auf eine Art und Weise auseinander gehalten werden können, die von allen Parteien als verlässlich befunden wird, so dass nur ein Mitspieler, der rechtmäßig ein Los aus der Losdatenbank erworben hat, befähigt ist, einen Schlüssel, der zu dem Los gehört, aus der Schlüsseldatenbank zu erhalten.

[0073] Es wurde oben dargelegt, dass der Mitspieler immer zuerst ein elektronisches Sofortgewinn-Los erwirbt und erst danach den Schlüssel, mit dem die Gewinndaten in dem Los verschlüsselt sind. Die Erfindung schließt jedoch nicht die Möglichkeit aus, dass der Mitspieler zuerst den Schlüssel erwirbt und erst danach das zugehörige Los. Eine solche Reihenfolge des Ablaufs erfordert einige Änderungen bei den oben beschriebenen Nachrichtenmodi, wobei man aber davon ausgehen kann, dass die Vornahme solcher Änderungen – vor dem Hintergrund der obigen Beschreibung der "herkömmlichen" Reihenfolge der Übergaben und der damit verbundenen Nachrichten – für den Fachmann offensichtlich ist. Ebenso kann die Zahlung der Gebühr vom Erwerb des Schlüssels anstatt vom Erwerb des Loses abhängig gemacht werden.

[0074] Wenn die Parteien, die an dem Spiel beteiligt sind, großes Vertrauen zueinander und in die Sicherheit der Datenübertragung haben oder wenn der tatsächliche Wert des Nutzens, der aus dem Spiel gezogen werden kann, nur gering oder unbedeutend ist, so kann die oben beschriebene Verfahrensweise natürlich auch dahingehend geändert werden, dass die Sicherheit des Systems in der Praxis geschwächt wird. Bei einem sehr elementaren System der Erfindung fungiert ein und dieselbe Partei als Losdruckerei, Lotteriegesellschaft und Schlüsselinhaber (wobei aber auch hier die Losdatenbank und die Schlüsseldatenbank voneinander getrennt sind), und der Mitspieler braucht sich in keiner Weise zu registrieren. Der Losdatensatz kann einfach aus einem Identifikator und verschlüsselten Gewinndaten bestehen. Der Mitspieler fordert ein Los mit einer Klartextnachricht an und gibt gleichzeitig eine Kreditkartennummer oder sonstige Daten an, die das Abbuchen des Lospreises gestatten. Die Lotteriegesellschaft entnimmt der Losdatenbank das Los und übergibt es dem Mitspieler, der anhand des auf dem Los befindlichen Identifikators den richtigen Schlüssel aus der Schlüsseldatenbank anfordert und die verschlüsselten Gewinndaten auf dem Los mittels des Schlüssels entschlüsselt. Durch Vorlage der Klartext-Gewinndaten kann der Mitspieler die Auszahlung des Gewinnes in jeder an sich bekannten Weise beanspruchen. Dieses elementare System eignet sich beispielsweise für Kinderspiele, wo der Lospreis und der Gewinnbetrag in wertlosem Spielgeld bestimmt werden. Systeme mit verschiedenen Sicherheitsgraden werden dadurch geschaffen, dass man einem solchen sehr einfachen System verschiedene Grade an oben beschriebenen Verschlüsselungs-, Zertifizierungs-, Signatur- und Zufallszahlfunktionen hinzufügt, bis schließlich das System von **Fig.** 6 erreicht ist.

[0075] Abschließend wird eine Anzahl von Vorrichtungs-Ausführungsformen besprochen, die sich für die Implementierung des oben beschriebenen Verfahrens in der Praxis eignen. **Fig.** 14 zeigt eine Vorrichtungskomponente im allgemeinen, die von dem Typ ist, der in der Losdruckerei zum Erzeugen elektronischer Sofortgewinn-Lose und der zugehörigen Schlüssel, zum Veranstalten des eigentlichen Spiels unter der Kontrolle der Lotteriegesellschaft, zur Ausführung von Operationen im Zusammenhang mit der Schlüsseldatenbank unter der Kontrolle des Schlüsselinhabers oder als Computerterminal des Mitspielers, über den der Mitspieler sich an der elektronischen Sofortgewinn-Lotterie beteiligt, verwendet werden kann. Die Netzwerkverbindung **1401** verbindet die Vorrichtungskomponente im Duplex-Modus mit einem solchen Datenübertragungsnetz, das sich für die Datenübertragung zwischen der Losdruckerei, der Lotteriegesellschaft, dem Schlüsselinhaber und den Mitspielern eignet. Der Verschlüsselungs- und Entschlüsselungsblock **1402** ist verantwortlich für das Verschlüsseln, das Entschlüsseln, die digitalen

Signaturen und das Verifizieren der Signaturen aller Daten, die das Datenübertragungsnetz passieren, in einer an sich bekannten Weise. Bei diesen Funktionen wird der Block **1402** durch den Schlüsselverwaltungsblock **1403** unterstützt, in dem die öffentlichen und privaten Schlüssel, die für die oben genannten Funktionen benötigt werden, gespeichert werden.

[0076] Der Ablauf des eigentlichen Spielprogramms vollzieht sich im Spielprogrammablaufblock **1404**, der Befehle ausführt, die im Programmspeicher **1405** in einer bestimmten Reihenfolge gespeichert sind. Der nicht-flüchtige Speicher **1406** dient dem Speichern aller Daten, die auch nach einem Stromausfall oder einer ähnlichen Situation, welche zur Löschung der Ablaufdaten aus dem Arbeitsplatzspeicher **1407** führt, noch verfügbar sein müssen. Der Benutzer kann den Betrieb der Vorrichtung über die Schnittstelle **1408** steuern.

[0077] Die Verwendung der in **Fig.** 14 veranschaulichten Vorrichtungskomponente für unterschiedliche Funktionen in dem System erlegt seinen Bestandteilen geringfügig unterschiedliche Anforderungen auf. In der Losdruckerei werden mit der Lotteriegesellschaft und dem Schlüsselinhaber relativ große Datenbanken verwaltet, deren Operationen so verlässlich wie möglich sein müssen. Darum sollte der nicht-flüchtige Speicher **1406** dieser Anwendungen groß und vorzugsweise in einer an sich bekannten Weise gesichert sein. Die Vorrichtung der Lotteriegesellschaft muss möglicherweise eine sehr große Menge an verschlüsselter Datenkommunikation in Richtung des Mitspielers selbst über einen sehr kurzen Zeitraum bewältigen, was bedeutet, dass die Netzwerkverbindung **1401**, der Verschlüsselungs- und Entschlüsselungsblock **1402** und der Schlüsselverwaltungsblock **1403** in der Vorrichtung der Lotteriegesellschaft mit sehr hoher Kapazität ausgelegt werden müssen. Außerdem muss der Spielprogrammablaufblock **1404** in der Vorrichtung der Lotteriegesellschaft – verglichen mit dementsprechenden Block im Computerterminal des Mitspielers – mit einem Mehrfachen der Effizienz arbeiten. Dem Fachmann ist an sich klar, wie solche Anforderungen berücksichtigt werden, wenn das Blockschaubild von **Fig.** 14 auf die verschiedenen Bestandteile des Systems der Erfindung angewendet wird.

[0078] Den Schreibtransaktionen zwischen dem Spielablaufblock **1404** und dem nicht-flüchtigen Speicher **1406** wird vorzugsweise ein "Transaktionscharakter" auferlegt. Das hat den Grund, dass das Verfahren der vorliegenden Erfindung eine Anzahl von Schritten umfasst, die entweder allesamt erfolgreich sein oder allesamt fehlschlagen müssen. Beispielsweise sind bei dem Schritt, wo der Mitspieler ein elektronisches Sofortgewinn-Los in der Losdatenbank kauft, solche gegenseitig abhängigen Schritte die Abbuchung der Gebühr vom Mitspielerkonto des Mitspielers, das Gewähren des Zugangs zu einem bestimmten elektronischen Sofortgewinn-Los für den Mitspieler und das Markieren dieses elektronischen Sofortgewinn-Loses als "verkauft".

[0079] Auch wenn ein Stromausfall oder eine sonstige Fehlersituation den Systembetrieb in einem kritischen Moment unterbräche, darf dies nicht zu einer Situation führen, wo der Mitspieler zum Beispiel ein elektronisches Sofortgewinn-Los erhalten hat, aber die Gebühr nicht abgebucht oder dieses konkrete Los nicht als "verkauft" markiert wurde. Dem Fachmann ist an sich bekannt, wie gegenseitig abhängige Dateioperationen als Transaktionen ausgeführt werden, d. h. so ausgeführt werden, dass sie entweder allesamt erfolgreich sind oder allesamt fehlschlagen.

[0080] **Fig.** 15 zeigt ein System einer Ausführungsform der Erfindung, wobei das Internet **1501** als das zentrale Datenübertragungsmittel dient. Bei dieser Ausführungsform der Erfindung sind die Losdruckerei und der Schlüsselinhaber ein und dieselbe Partei, deren Datensystem um den Großrechner **1502** herum aufgebaut ist. Die Blöcke **1401**, **1402**, **1403**, **1404**, **1405** und **1407** in der Figur und die Datenübertragung zwischen diesen kann dadurch implementiert werden, dass man in einer an sich bekannten Weise den Prozessor, den Bus, den Speicher und weitere Bauteile des Computers **1502** (die in der Figur nicht eigens dargestellt sind) benutzt. Die Schnittstelle, d. h. Block **1408** von **Fig.** 14, besteht aus einem Anzeigegerät **1503** und einer Tastatur **1504**. Als nicht-flüchtigen Speicher enthält das System einen Speicherbaustein mit hoher Speicherkapazität, worin der Hauptmassenspeicher **1505** durch einen parallelen Massenspeicher **1506** abgesichert ist. Die Ausrüstung der Lotteriegesellschaft ist vom gleichen Typ, d. h. sie umfasst einen Großrechner **1507**, ein Anzeigegerät **1508**, eine Tastatur **1509** und die Massenspeicher **1510** und **1511**. Die Vorrichtung des Mitspielers ist ein Heimcomputer, der mit einem Internetanschluss ausgestattet ist und eine zentrale Recheneinheit 1512 zum Implementieren der Blöcke **1401**–**1407** von **Fig.** 14 sowie ein Anzeigegerät **1513** und eine Tastatur **1514** enthält.

[0081] **Fig.** 16 zeigt ein System einer zweiten Ausführungsform der Erfindung, wo die Bestandteile **1501**–**1511** mit denen in **Fig.** 15 identisch sind. Jedoch ist der Datenübertragungsbus in Richtung des Mitspielers ein digitales Fernsehnetzwerk **1601**, das ursprünglich für die Ausstrahlung digitaler Fernsehsendungen konzipiert war. Der Ausstrahlungspfad kann beispielsweise ein Kabelnetz oder ein zumindest teilweise kabellos ausgeführtes Netz sein, wobei die Links terrestrisch und/oder satellitengestützt sein können. Die Fernsehsendestation **1602** produziert Fernsehprogramme aus verschiedenen Programmquellen, was durch eine Echtzeit-Videokamera **1603** zum Produzieren von Fernsehoriginalübertragungen

beispielhaft veranschaulicht ist. Die Datenübertragungsverbindung zwischen der Lotteriegesellschaft und dem Mitspieler wird mit einer (vorzugsweise digitalen) Fernsehübertragung in einer Duplexer-Multiplexer-Einheit **1604** verschränkt, die ihrerseits gleichzeitig den Duplex-Modus der Datenübertragungsverbindung zwischen der Lotteriegesellschaft und dem Mitspieler besorgt. Wenn es im Sendenetzwerk lange Drahtloslink-Intervalle gibt, so kann es zweckmäßig sein, die Abwärts-Datenübertragung (in Richtung des Mitspielers) und die Aufwärts-Datenübertragung (vom Mitspieler in Richtung des Systems) wenigstens teilweise so voneinander zu trennen, dass die Aufwärts-Datenübertragung teilweise beispielsweise das Telefonnetz oder das Internet nutzt.

[0082] Die Vorrichtung des Mitspielers umfasst einen Empfänger für digitale Fernsehsendungen, d. h. eine Set Top Box **1605**, welche den Duplex-Modus von Verbindungen, die über das digitale Fernsehnetz übertragen werden, und möglicherweise auch das Routing von Aufwärts-Datenübertragungen über das Telefonnetz und/oder das Internet unterstützt. Darüber hinaus unterstützt der Empfänger **1605** eine Programmierschnittstelle, die an sich bekannt sein kann, wie beispielsweise DVB-J, und enthält die erforderlichen Sender-Empfänger-, Prozessor- und Speichermittel für die Implementierung der Blöcke **1401**–**1407** von **Fig.** 14. Die Benutzerschnittstelle besteht aus einem Fernsehbildschirm **1606** und einer Fernbedienung (oder beispielsweise einer drahtlosen Tastatur) **1607**. Einer der Vorteile der in **Fig.** 16 gezeigten Ausführungsform ist, dass die Programm-Updates und andere Abwärts-Datenübertragungen zur Vorrichtung des Mitspielers mühelos neben der digitalen Fernsehübertragung übertragen werden können, wodurch man den Vorteil der Kapazität der Abwärts-Datenübertragung, die von sich aus hoch ist, in dem digitalen Fernsehnetzwerk hat. Die Programm-Updates können die Übermittlung relativ großer Datenmengen erfordern, und im Rahmen der obigen weitgefassten Definition des elektronischen Sofortgewinn-Loses können selbst hochkomplexe "Lose", die viele Details beinhalten, erzeugt werden.

[0083] **Fig.** 17 veranschaulicht das System einer dritten Ausführungsform der Erfindung, wo die Bestandteile **1501**–**1511** immer noch mit denen von **Fig.** 15 identisch sind, nur dass anstelle des Internet ein fest-installiertes Telefonnetz **1704** als Datenübertragungsnetzwerk zwischen der Losdruckerei/dem Schlüsselinhaber und der Lotteriegesellschaft dient. Der Datenübertragungsbus in Richtung des Mitspielers besteht aus einem Paketradionetzwerk **1701**, bei dem es sich beispielsweise um ein an sich bekanntes GPRS (General Packet Radio Service)-Netzwerk oder ein beliebiges anderes Netzwerk handeln kann, das Datenverbindungen im Zusammenhang mit Portable-Terminal-Paketen anbieten kann. In das Paketradionetzwerk **1701** ist eine Basisstation **1702** integriert, die mit einem bestimmten Benutzerterminal **1703** in Funkverbindung steht. Alle in **Fig.** 14 gezeigten Blöcke sind in diesem Benutzerterminal **1703** integriert.

Patentansprüche

1. Verfahren zum Veranstalten elektronischer Sofortgewinn-Lotterien, das folgende Schritte umfasst:
– Erzeugen (**605**) und Speichern (**606**) mehrerer elektronischer Sofortgewinn-Lose (**510**), von denen ein jedes Gewinndaten umfasst, die verschlüsselt sind und mit einem Los-bezogenen Schlüssel entschlüsselt werden können; und
– Bereitstellen eines Zugangs für einen bestimmten Mitspieler zu den gespeicherten elektronischen Sofortgewinn-Losen, dergestalt, dass der Mitspieler ein bestimmtes elektronisches Sofortgewinn-Los erwirbt;
dadurch gekennzeichnet, dass das Verfahren folgende Schritte umfasst
– Speichern (**607**) der Schlüssel (**511**), mit denen die verschlüsselten Gewinndaten gespeicherter elektronischer Sofortgewinn-Lose entschlüsselt werden können, separat von den gespeicherten elektronischen Sofortgewinn-Losen; und
– Bereitstellen eines Zugangs für den Mitspieler zu den gespeicherten Schlüsseln, dergestalt, dass der Mitspieler einen Schlüssel erwirbt, der einem bestimmten elektronischen Sofortgewinn-Los zugeordnet ist.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass der Schritt des Bereitstellens eines Zugangs für einen bestimmten Mitspieler zu gespeicherten elektronischen Sofortgewinn-Losen dergestalt, dass der Mitspieler ein bestimmtes elektronisches Sofortgewinn-Los erwirbt, einen Unterschritt umfasst, bei dem der Mitspieler eine bestimmte Gebühr bezahlt.

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass der Schritt des Bereitstellens eines Zugangs für den Mitspieler zu den gespeicherten Schlüsseln dergestalt, dass der Mitspieler einen Schlüssel erwirbt, der zu einem bestimmten elektronischen Sofortgewinn-Los gehört, einen Unterschritt umfasst, bei dem der Mitspieler einen Nachweis seines Besitzes dieses speziellen elektronischen Sofortgewinn-Loses vorlegt.

4. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass der Schritt des Bereitstellens eines Zugangs für einen bestimmten Mitspieler zu den gespeicherten Schlüsseln dergestalt, dass der Mitspieler einen Schlüssel erwirbt, der zu einem bestimmten elektronischen Sofortgewinn-Los gehört, einen Unterschritt umfasst, bei dem der Mitspieler eine bestimmte Gebühr bezahlt.

5. Verfahren nach Anspruch 1, dadurch gekenn-

zeichnet, dass der Schritt des Bereitstellens eines Zugangs für den Mitspieler zu elektronischen Sofortgewinn-Losen dergestalt, dass der Mitspieler ein bestimmtes elektronisches Sofortgewinn-Los erwirbt, einen Unterschritt umfasst, bei dem der Mitspieler einen Nachweis seines Besitzes des Schlüssels, der zu diesem speziellen elektronischen Sofortgewinn-Los gehört, vorlegt.

6. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass der Schritt des Erzeugens (**605**) und Speicherns (**606**) mehrerer elektronischer Sofortgewinn-Lose für jedes elektronische Sofortgewinn-Los die folgenden Unterschritte umfasst:
– Erzeugen eines Datensatzes (**501**), der einen unzweideutigen Identifikator (**502**) des elektronischen Sofortgewinn-Loses und verschlüsselte Gewinndaten (**503**) umfasst;
– Schützen des Datensatzes mit einem elektronischen Identifikator (**551**, **506**, **509**), der angibt, wer der Originator der elektronischen Sofortgewinn-Lose ist und ob der Inhalt dieses speziellen elektronischen Sofortgewinn-Loses seit seiner Erzeugung verändert wurde.

7. Verfahren nach Anspruch 6, dadurch gekennzeichnet, dass zur Erzeugung des elektronischen Identifikators (**551**, **506**, **509**) ein bestimmtes asymmetrisches Verschlüsselungssystem und eine bestimmte unidirektionale Hash-Berechnungsfunktion verwendet werden, wobei der elektronische Identifikator die digitale Signatur des Originators der elektronischen Sofortgewinn-Lose ist und einen Hash umfasst, der mittels der Hash-Berechnungsfunktion auf einem bestimmten Teil des elektronischen Sofortgewinn-Loses berechnet ist, wobei der Hash mit einem bestimmten ersten Schlüssel des Originators elektronischer Sofortgewinn-Lose verschlüsselt ist, wobei ein zweiter Schlüssel, der zu diesem Schlüssel gehört, in dem asymmetrischen Verschlüsselungssystem bekannt ist.

8. Verfahren nach Anspruch 7, dadurch gekennzeichnet, dass der Schritt des Erzeugens (**605**) und Speicherns (**606**) mehrerer elektronischer Sofortgewinn-Lose für jedes elektronische Sofortgewinn-Los die folgenden Unterschritte umfasst:
– Erzeugen eines Gewinndatenfeldes (**503**), das aus einem Abschnitt (**504**), der einen zu dem elektronischen Sofortgewinn-Los gehörenden Gewinn anzeigt, und aus einer Zufallszahl (**505**) besteht und das mit der digitalen Signatur (**551**) des Originators des elektronischen Sofortgewinn-Loses geschützt ist und mit einem Los-bezogenen Schlüssel verschlüsselt und entschlüsselt werden kann;
– Erzeugen eines primären Losdatensatzes (**550**), der aus dem Gewinndatenfeld (**503**) und einem unzweideutigen Identifikator (**502**) des elektronischen Loses besteht und der mit der digitalen Signatur (**506**) des Originators der elektronischen Sofortgewinn-Lose geschützt ist;
– Erzeugen eines Zusatzdatenfeldes (**560**), das einen Hash (**507**), der aus dem Gewinndatenfeld berechnet wurde, und einen Hash (**508**), der aus dem Los-bezogenen Schlüssel berechnet wurde, umfasst;
– Schützen des elektronischen Sofortgewinn-Loses mit der digitalen Signatur (**509**) des Originators von Sofortgewinn-Losen.

9. Verfahren nach Anspruch 8, dadurch gekennzeichnet, dass zusätzlich ein Hash aus dem Los-bezogenen Schlüssel berechnet und dem primären Losdatensatz hinzugefügt wird.

10. Verfahren nach Anspruch 8, dadurch gekennzeichnet, dass – zum Speichern der Schlüssel; mit denen die verschlüsselten Gewinndaten der elektronischen Sofortgewinn-Lose entschlüsselt werden können – für jedes elektronische Sofortgewinn-Los ein Schlüsseldatensatz (**512**) gespeichert wird, der folgendes umfasst:
– den Identifikator (**502**) des zugehörigen elektronischen Sofortgewinn-Loses und
– den Schlüssel (**513**), mit dem die verschlüsselten Gewinndaten des zugehörigen elektronischen Sofortgewinn-Loses entschlüsselt werden können,
und der mit der digitalen Signatur (**514**) des Originators des Schlüsseldatensatzes geschützt ist.

11. Verfahren nach Anspruch 10, dadurch gekennzeichnet, dass für jedes elektronische Sofortgewinn-Los auch ein Gewinndatensatz (**516**) gespeichert wird, der folgendes umfasst:
– den Identifikator (**502**) des zugehörigen elektronischen Sofortgewinn-Loses und
– einen Hash (**507**), der aus einem bestimmten Gewinn-anzeigenden Abschnitt des elektronischen Sofortgewinn-Loses mit einer bestimmten unidirektionalen Hash-Berechnungsfunktion berechnet wurde,
und der mit der digitalen Signatur (**517**) des Originators des Gewinndatensatzes geschützt ist.

12. Verfahren nach Anspruch 11, dadurch gekennzeichnet, dass es Schritte umfasst, bei denen:
– eine bestimmte Losdruckerei eine Losdatenbank, die aus elektronischen Sofortgewinn-Losen besteht, eine Gewinndatenbank, die aus Gewinnaufzeichnungen besteht, die zu den erzeugten elektronischen Sofortgewinn-Losen gehören, und eine Schlüsseldatenbank (**605**), die aus Schlüsseldatensätzen besteht, die zu den erzeugten elektronischen Sofortgewinn-Losen gehören, erstellt,
– die Losdruckerei die Losdatenbank und die Gewinndatenbank einer bestimmten Lotteriegesellschaft (**510**, **515**) und die Schlüsseldatenbank einem bestimmten Schlüsselinhaber (**511**) übergibt,
– die Lotteriegesellschaft und der Schlüsselinhaber die übergebenen Datenbanken auf bestimmten Spiel- und Schlüsselservern (**606**, **607**) installieren,
– ein bestimmter Mitspieler sich in dem Spielsystem

der Lotteriegesellschaft registriert (**608**) und anschließend ein bestimmtes Mitspielerkonto für ihn in dem Spielsystem der Lotteriegesellschaft eröffnet wird,
– der Mitspieler der Lotteriegesellschaft eine Anforderung für ein elektronisches Sofortgewinn-Los und einen Auftrag zur Abbuchung der entsprechenden Gebühr von dem Mitspielerkonto (**701**) zusendet (**609**),
– die Lotteriegesellschaft eine dem elektronischen Sofortgewinn-Los entsprechende Gebühr von dem Mitspielerkonto abbucht und ein bestimmtes elektronisches Sofortgewinn-Los für den Mitspieler aussucht,
– die Lotteriegesellschaft eine bestimmte Verkaufsquittung (**801**) als Nachweis über den rechtmäßigen Erwerb des elektronischen Sofortgewinn-Loses durch den Mitspieler erzeugt (**611**),
– die Lotteriegesellschaft das elektronische Sofortgewinn-Los und die Verkaufsquittung (**901**) an den Mitspieler sendet (**612**),
– die Lotteriegesellschaft das übersandte elektronische Sofortgewinn-Los als verkauft markiert (**613**),
– der Mitspieler die Verkaufsquittung an den Schlüsselinhaber sendet (**615**), um den Schlüssel zu erhalten (**1001**), der zu dem elektronischen Sofortgewinn-Los gehört,
– der Schlüsselinhaber die Verkaufsquittung überprüft (**616**), um zu verifizieren, dass der Mitspieler den elektronischen Sofortgewinn-Schlüssel rechtmäßig erworben hat, und dem Mitspieler den Schlüssel, der zu dem elektronischen Sofortgewinn-Los gehört, und den Nachweis (**1101**), dass der Mitspieler den Schlüssel rechtmäßig erworben hat (**1201**), zusendet (**617**),
– der Mitspieler die Gewinndaten des in seinem Besitz befindlichen elektronischen Sofortgewinn-Loses entschlüsselt (**618**),
– der Mitspieler der Lotteriegesellschaft die entschlüsselten Gewinndaten und den erhaltenen Nachweis, dass er den Schlüssel rechtmäßig erworben hat (**1301**), zusendet,
– die Lotteriegesellschaft überprüft (**619**), ob das elektronische Sofortgewinn-Los verkauft wurde, ob der Mitspieler den Schlüssel rechtmäßig erworben hat und ob der Gewinndatensatz, der zu dem elektronischen Sofortgewinn-Los in der Gewinndatenbank gehört, dem Gewinndatensatz gleicht, den der Mitspieler zugesandt hat, und
– die Lotteriegesellschaft dem Mitspielerkonto des Mitspielers den Gewinn gutschreibt (**619**), der durch die Gewinndaten angegeben ist.

13. Verfahren nach Anspruch 12, dadurch gekennzeichnet, dass die Anforderung (**701**) für ein elektronisches Sofortgewinn-Los folgendes umfasst:
– den bestimmten öffentlichen Schlüssel (**702**) des Mitspielers in einem bestimmten asymmetrischen Verschlüsselungssystem,
– einen Hash (**703**), der aus einer bestimmten Zufallszahl mittels einer bestimmten unidirektionalen Hash-Berechnungsfunktion berechnet wurde, und
– ein Zertifikat (**704**), aus dem das Recht des Mitspielers auf den öffentlichen Schlüssel hervorgeht,
und mit der digitalen Signatur (**705**) des Mitspielers geschützt ist.

14. Verfahren nach Anspruch 12, dadurch gekennzeichnet, dass die Verkaufsquittung (**801**) folgendes umfasst:
– den Identifikator (**502**) eines elektronischen Sofortgewinn-Loses,
– den Verkaufstransaktionsidentifikator (**802**) eines elektronischen Sofortgewinn-Loses,
– einen Schlüsselhash (**508**), der in dem elektronischen Sofortgewinn-Los lesbar ist, und
– einen Hash (**703**), der aus der Zufallszahl, die von einem bestimmten Mitspieler übergeben wurde, mittels einer bestimmten unidirektionalen Hash-Berechnungsfunktion berechnet wurde,
und dass sie:
– mit der digitalen Signatur (**03**) der Lotteriegesellschaft geschützt ist und
– mit dem öffentlichen Schlüssel des Schlüsselinhabers in einem bestimmten asymmetrischen Verschlüsselungssystem verschlüsselt wurde.

15. Verfahren nach Anspruch 12, dadurch gekennzeichnet, dass – um dem Mitspieler ein elektronisches Sofortgewinn-Los und eine Verkaufsquittung zuzusenden – die Lotteriegesellschaft eine Nachricht (**901**) zusendet, die folgendes umfasst:
– den Verkaufstransaktionsidentifikator (**802**) des elektronischen Sofortgewinn-Loses,
– den primären Losdatensatz (**550**) des elektronischen Sofortgewinn-Loses,
– die Verkaufsquittung (**801**) und
– ein Zertifikat (**902**), welches das Recht der Lotteriegesellschaft auf einen bestimmten öffentlichen Schlüssel verbrieft,
und die mit der digitalen Signatur (**903**) der Lotteriegesellschaft geschützt ist.

16. Verfahren nach Anspruch 12, dadurch gekennzeichnet, dass – um dem Schlüsselinhaber die Verkaufsquittung zuzusenden – der Mitspieler eine Nachricht (**1001**) versendet, die folgendes umfasst:
– den Identifikator (**502**) des elektronischen Sofortgewinn-Loses,
– eine Verkaufsquittung (**801**),
– eine bestimmte Zufallszahl (**703'**)
– den bestimmten öffentlichen Schlüssel (**702**) des Mitspielers in einem bestimmten asymmetrischen Verschlüsselungssystem und
– ein Zertifikat (**704**), welches das Recht des Mitspielers auf den öffentlichen Schlüssel verbrieft,
und die mit der digitalen Signatur (**1002**) des Mitspielers geschützt ist.

17. Verfahren nach Anspruch 12, dadurch ge-

kennzeichnet, dass der Nachweis (**1101**) über den rechtmäßigen Erwerb des Schlüssels durch den Spieler folgendes umfasst:
– den Verkaufstransaktionsidentifikator (**802**) des elektronischen Sofortgewinn-Loses und
– ein Zertifikat (**1102**), welches das Recht des Schlüsselinhabers auf einen bestimmten öffentlichen Schlüssel verbrieft,
und er mit der digitalen Signatur (**1103**) des Schlüsselinhabers geschützt ist.

18. Verfahren nach Anspruch 12, dadurch gekennzeichnet, dass – um dem Mitspieler den Schlüssel zuzusenden – der Schlüsselinhaber eine Nachricht (**1201**) versendet, die folgendes umfasst:
– den Identifikator (**502**) des elektronischen Sofortgewinn-Loses,
– einen Schlüsseldatenbatz (**512**), der zu dem elektronischen Sofortgewinn-Los gehört und in der Schlüsseldatenbank lesbar ist, und
– einen Nachweis (**1101**) über den rechtmäßigen Erwerb des Schlüssels durch den Mitspieler,
und die mit der digitalen Signatur (**1202**) des Schlüsselinhabers geschützt ist.

19. Verfahren nach Anspruch 12, dadurch gekennzeichnet, dass – um der Lotteriegesellschaft die entschlüsselten Gewinndaten zuzusenden – der Mitspieler eine Nachricht (**1301**) versendet, die folgendes umfasst:
– den Verkaufstransaktionsidentifikator (**802**) des elektronischen Sofortgewinn-Loses,
– die entschlüsselten (**1302**) Gewinndaten,
– den Nachweis (**1101**) über den rechtmäßigen Erwerb des Schlüssels durch den Mitspieler und
– ein Zertifikat (**704**), welches das Recht des Mitspielers auf einen bestimmten öffentlichen Schlüssel verbrieft,
und die mit der digitalen Signatur (**1303**) des Mitspielers geschützt ist.

20. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Schritte
– des Erzeugens (**605**) und Speicherns (**606**) mehrerer elektronischer Sofortgewinn-Lose (**510**), von denen ein jedes Gewinndaten umfasst, die verschlüsselt sind und mit einem Los-bezogenen Schlüssel entschlüsselt werden können, und
– des Speicherns (**607**) der Schlüssel (**511**), mit denen die verschlüsselten Gewinndaten der gespeicherten elektronischen Sofortgewinn-Lose entschlüsselt werden können, separat von den elektronischen Sofortgewinn-Losen,
mehrere Male in bestimmten Abständen wiederholt werden, um eine Situation zu vermeiden, in der die verbleibende Anzahl zuvor erzeugter und gespeicherter elektronischer Sofortgewinn-Lose kleiner wäre als die Zahl, die durch einen bestimmten Schwellenwert bezeichnet ist.

21. System zum Veranstalten elektronischer Sofortgewinn-Lotterien, das folgendes umfasst:
– ein erstes Datensystem (**401**) zum Erzeugen wenigstens teilweise verschlüsselter elektronischer Sofortgewinn-Lose;
– ein zweites Datensystem (**402**, **406**) zum Speichernder erzeugten wenigstens teilweise verschlüsselten elektronischen Sofortgewinn-Lose; und
– Mittel zum Bereitstellen einer Datenübertragungsverbindung für mehrere Mitspieler (**404**) zu dem zweiten Datensystem, um dem Mitspieler Zugang zu elektronischen Sofortgewinn-Losen zu geben;
dadurch gekennzeichnet, dass das System folgendes umfasst:
– ein drittes Datensystem (**403**, **405**) zum Speichern der Los-bezogenen Schlüssel, mit denen die elektronischen Sofortgewinn-Lose entschlüsselt werden können, separat von den elektronischen Sofortgewinn-Losen;
– eine Datenübertragungsverbindung von dem ersten Datensystem zu dem zweiten Datensystem und zu dem dritten Datensystem sowie
– Mittel zum Bereitstellen einer Datenübertragungsverbindung für mehrere Mitspieler (**404**) zu dem dritten Datensystem, um dem Mitspieler Zugang zu Schlüsseln zu geben, die zu den elektronischen Sofortgewinn-Losen gehören.

22. System nach Anspruch 21, dadurch gekennzeichnet, dass das erste Datensystem (**410**) im Wesentlichen das gleiche ist wie das dritte Datensystem (**403**).

23. System nach Anspruch 21, dadurch gekennzeichnet, dass die Mittel zum Bereitstellen einer Datenübertragungsverbindung für mehrere Mitspieler Verbindungen von dem zweiten (**402**) und dem dritten (**403**) Datensystem zu einem offenen Datennetzwerk umfassen.

24. System nach Anspruch 21, dadurch gekennzeichnet, dass es – im Zusammenwirken mit dem zweiten Datensystem – Mittel (**407**) zum Absondern derjenigen elektronischen Sofortgewinn-Lose umfasst, zu denen ein bestimmter Mitspieler bereits Zugang erhalten hat.

25. System nach Anspruch 21, dadurch gekennzeichnet, dass es – im Zusammenwirken mit dem zweiten Datensystem – Mittel (**409**) zum Speichern von Gewinndaten, die zu jedem einzelnen elektronischen Sofortgewinn-Los gehören, separat von den elektronischen Sofortgewinn-Losen umfasst.

26. System nach Anspruch 21, dadurch gekennzeichnet, dass es – im Zusammenwirken mit dem dritten Datensystem – Mittel umfasst, mit denen der verifizierbare Besitz eines elektronischen Sofortgewinn-Los eines Mitspielers überprüft wird, bevor der Mitspieler Zugang zu dem Schlüssel erhält, der zu

diesem speziellen elektronischen Sofortgewinn-Los gehört.

27. System nach Anspruch 21, dadurch gekennzeichnet, dass es – im Zusammenwirken mit dem zweiten Datensystem – Mittel umfasst, mit denen der verifizierbare Besitz eines zu einem bestimmten elektronischen Sofortgewinn-Los gehörenden Schlüssels eines Mitspielers überprüft wird, bevor der Mitspieler Zugang zu dem elektronischen Sofortgewinn-Los erhält, das zu diesem speziellen Schlüssel gehört.

Es folgen 9 Blatt Zeichnungen

Anhängende Zeichnungen

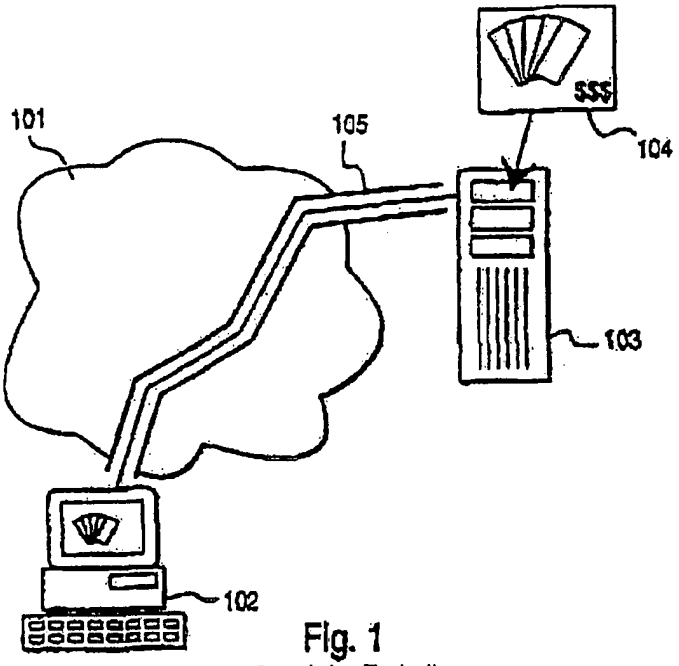


Fig. 1
Stand der Technik

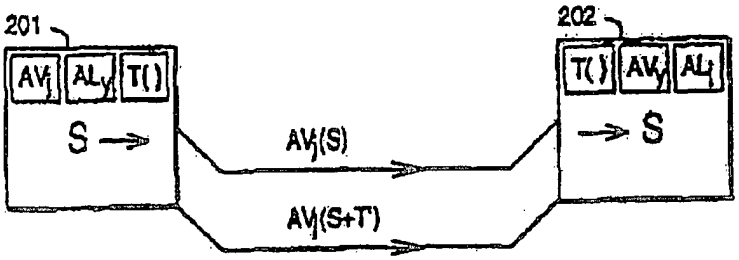


Fig. 2
Stand der Technik

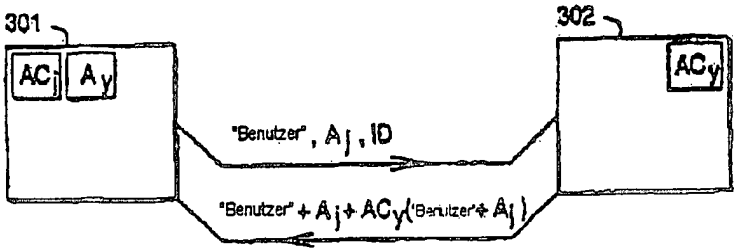


Fig. 3
Stand der Technik

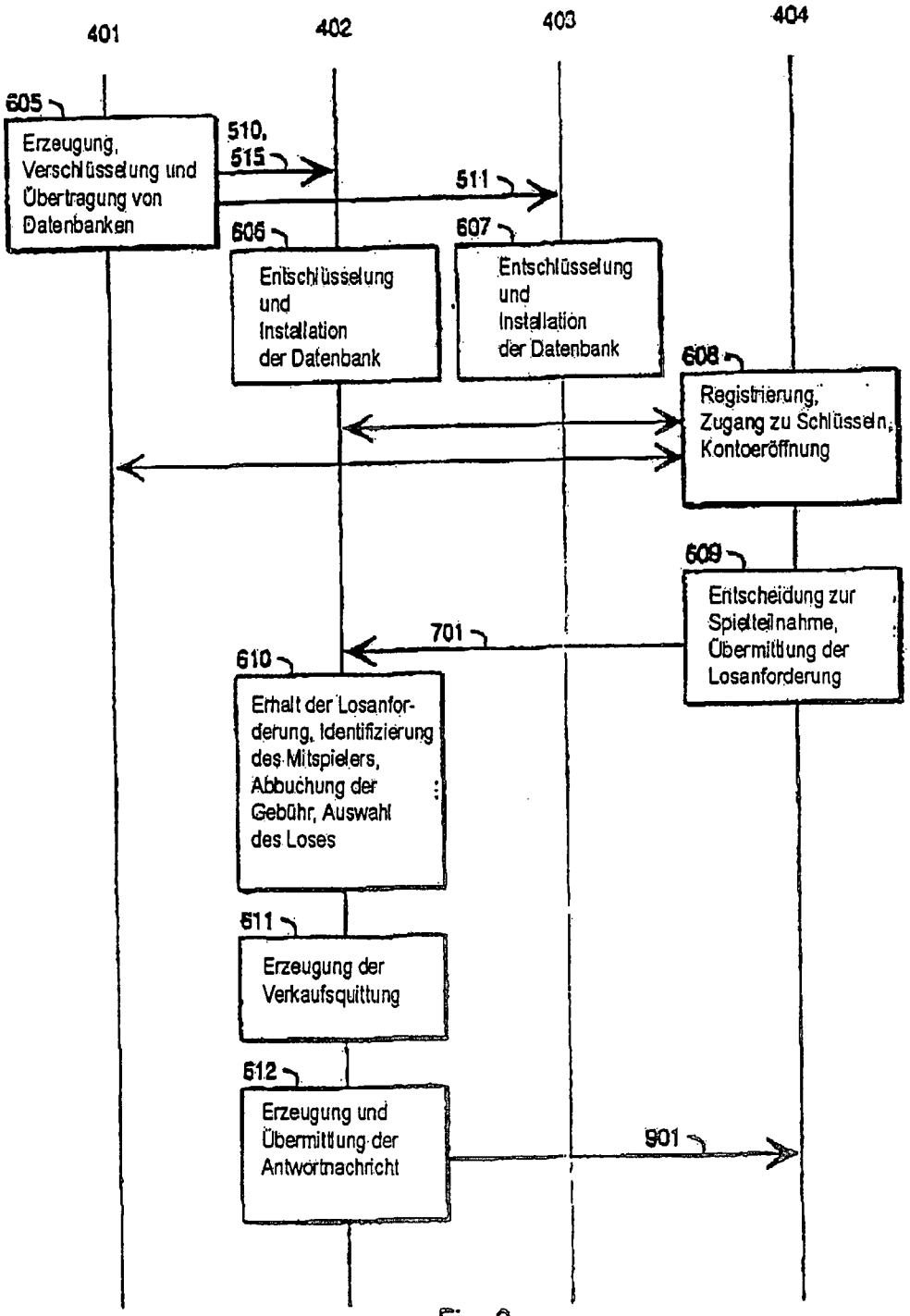
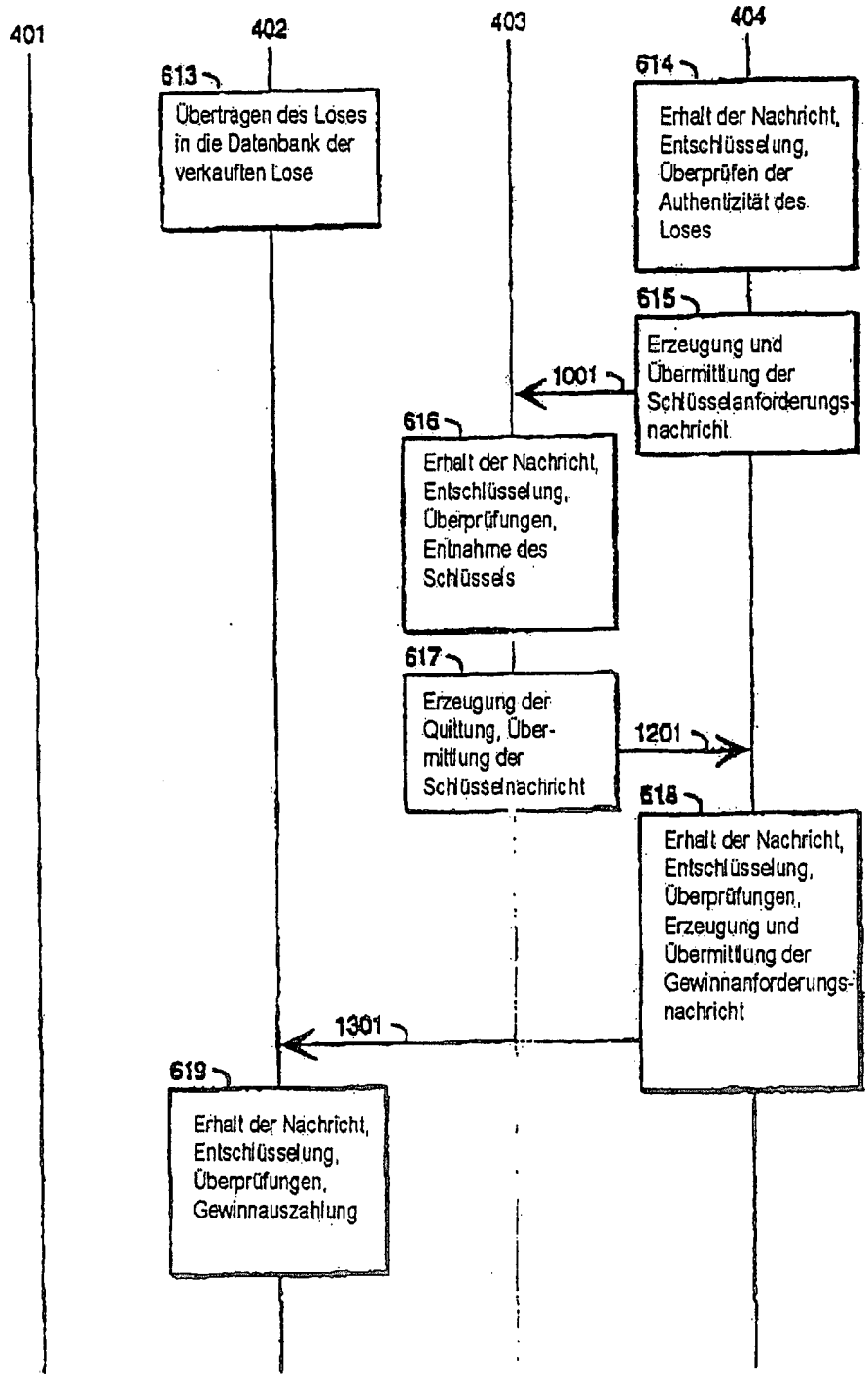

401
402
403
404
605
Erzeugung, Verschlüsselung und Übertragung von Datenbanken
510, 515
511
606
Entschlüsselung und Installation der Datenbank
607
Entschlüsselung und Installation der Datenbank
608
Registrierung, Zugang zu Schlüsseln, Kontoeröffnung
609
Entscheidung zur Spielteilnahme, Übermittlung der Losanforderung
701
610
Erhalt der Losanforderung, Identifizierung des Mitspielers, Abbuchung der Gebühr, Auswahl des Loses
611
Erzeugung der Verkaufsquittung
612
Erzeugung und Übermittlung der Antwortnachricht
901

Fig. 6...


401
402
403
404
613
Übertragen des Loses in die Datenbank der verkauften Lose
614
Erhalt der Nachricht, Entschlüsselung, Überprüfen der Authentizität des Loses
615
Erzeugung und Übermittlung der Schlüsselanforderungs-nachricht
1001
616
Erhalt der Nachricht, Entschlüsselung, Überprüfungen, Entnahme des Schlüssels
617
Erzeugung der Quittung, Übermittlung der Schlüsselnachricht
1201
618
Erhalt der Nachricht, Entschlüsselung, Überprüfungen, Erzeugung und Übermittlung der Gewinnanforderungs-nachricht
1301
619
Erhalt der Nachricht, Entschlüsselung, Überprüfungen, Gewinnauszahlung

...Fig. 6

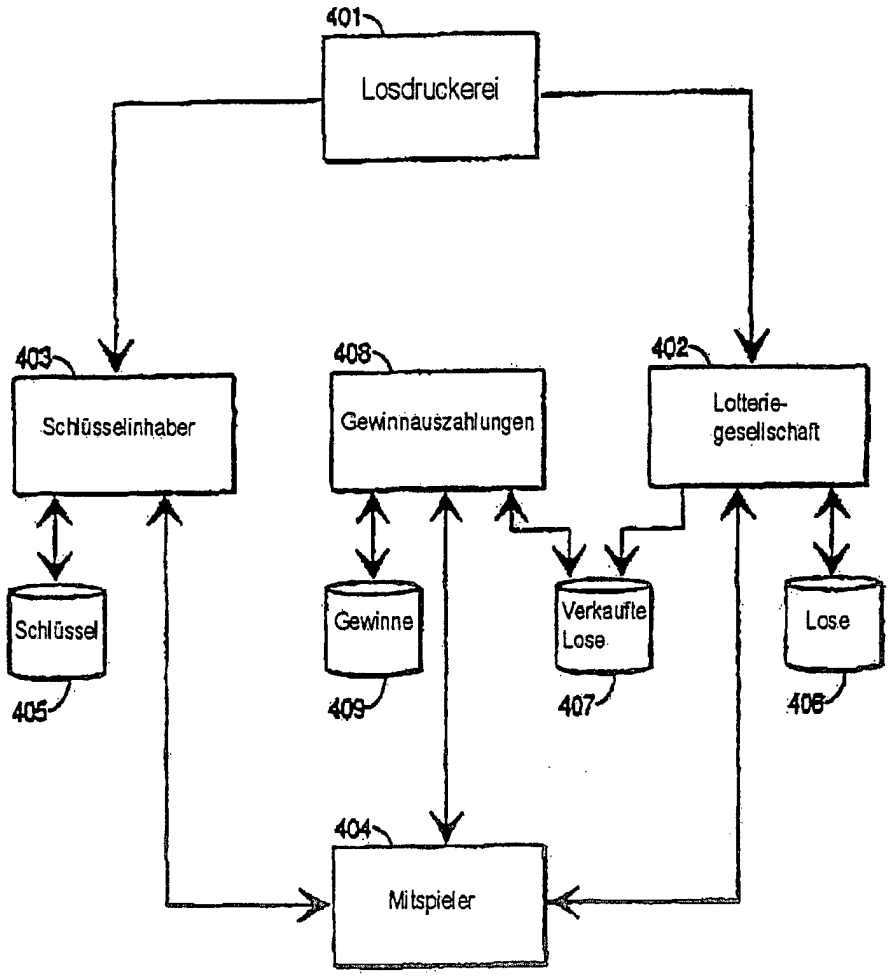

401
Losdruckerei
403
Schlüsselinhaber
408
Gewinnauszahlungen
402
Lotterie-
gesellschaft
Schlüssel
405
Gewinne
409
Verkaufte
Lose
407
Lose
406
404
Mitspieler

Fig. 4

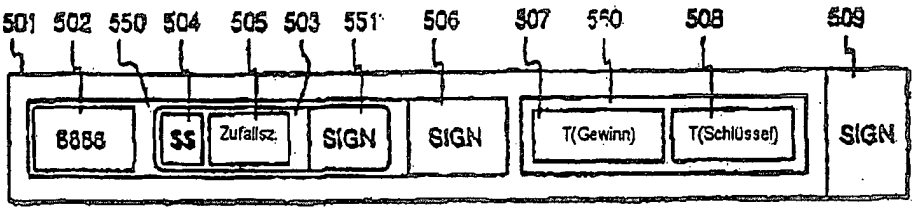

501
502
550
504
505
503
551
506
507
560
508
509
8888
SS
Zufallsz.
SIGN
SIGN
T(Gewinn)
T(Schlüssel)
SIGN

Fig. 5a

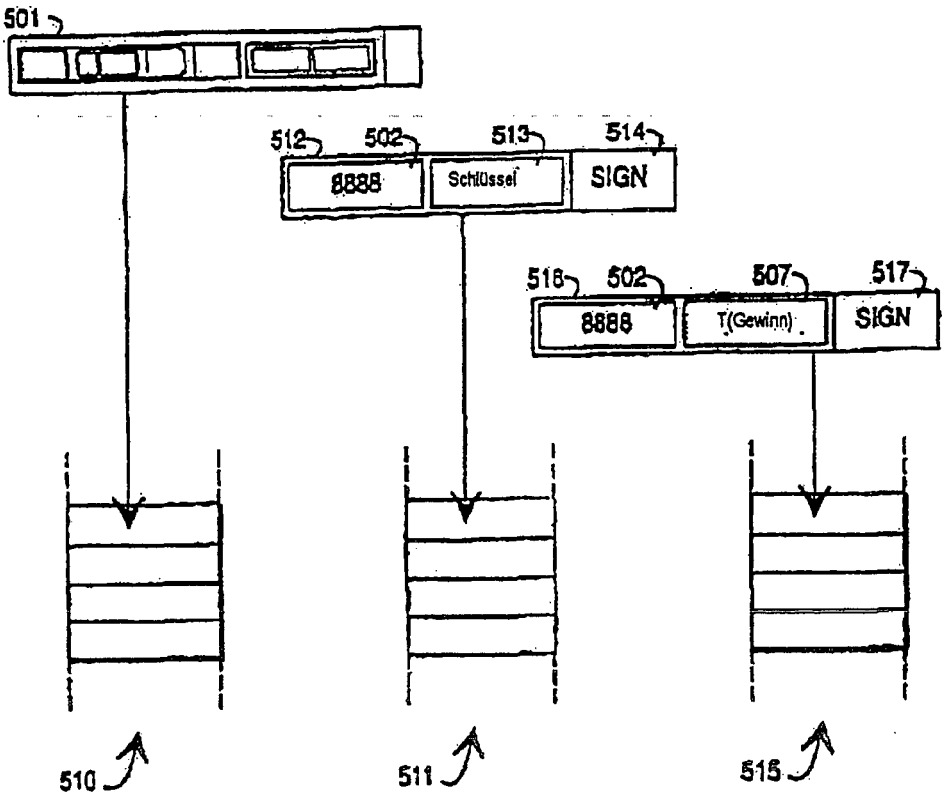


Fig. 5b

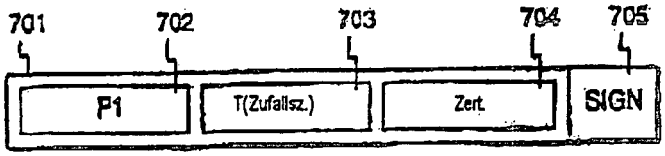


Fig. 7

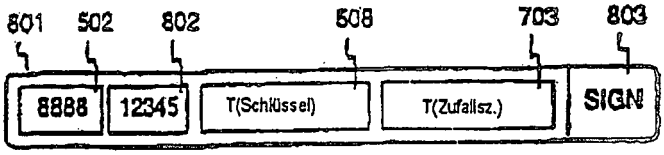


Fig. 8

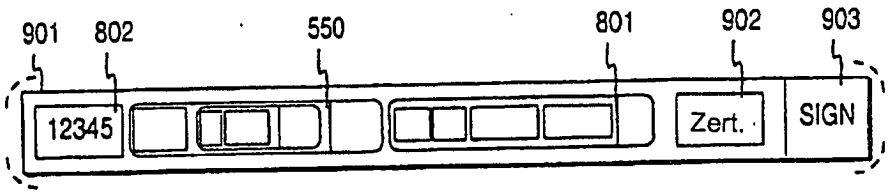


Fig. 9

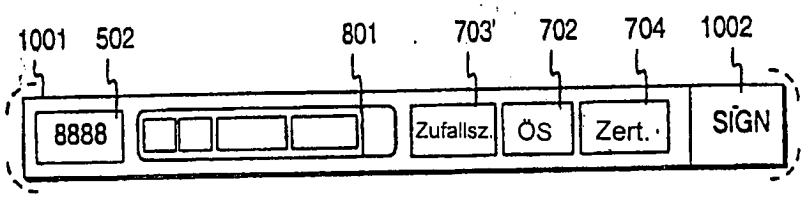


Fig. 10

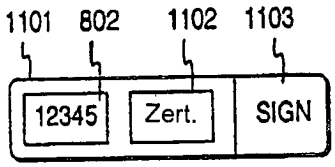


Fig. 11

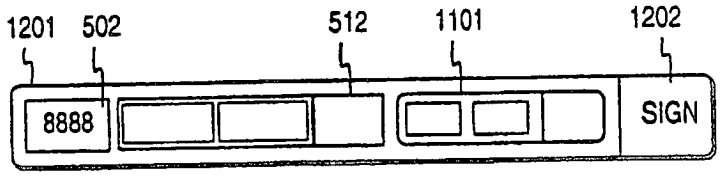


Fig. 12

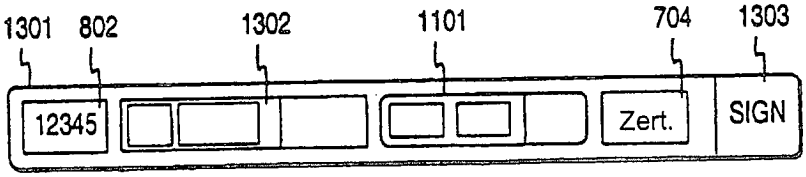


Fig. 13

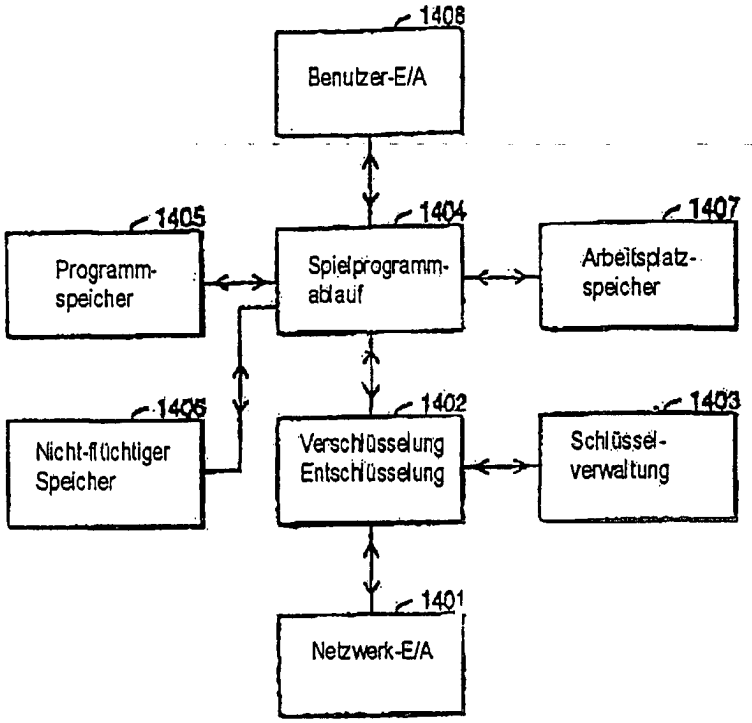

1408
Benutzer-E/A
1405
Programm-speicher
1404
Spielprogramm-ablauf
1407
Arbeitsplatz-speicher
1406
Nicht-flüchtiger Speicher
1402
Verschlüsselung Entschlüsselung
1403
Schlüssel-verwaltung
1401
Netzwerk-E/A

Fig. 14

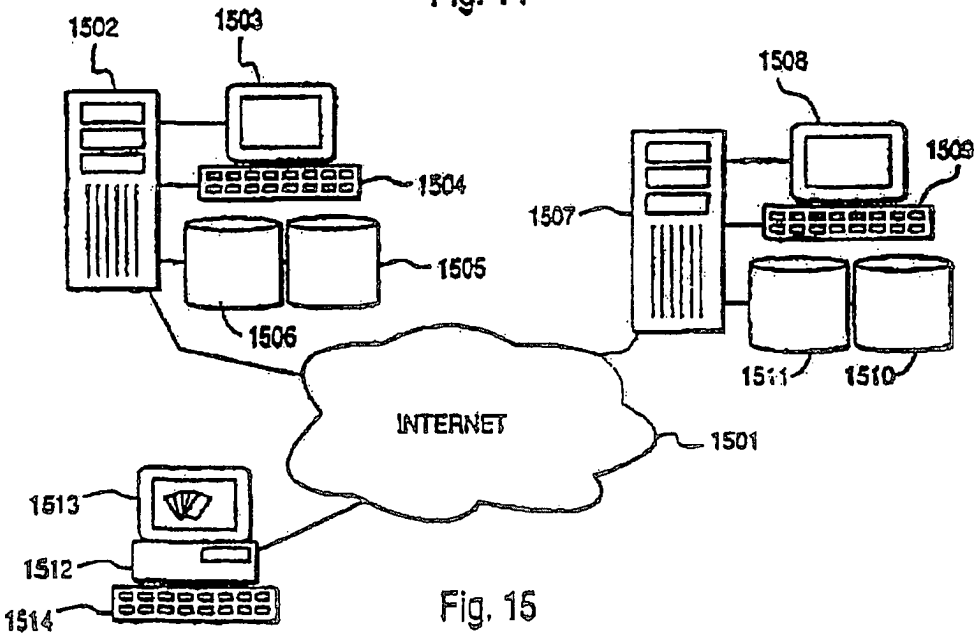

1502
1503
1504
1505
1506
1508
1509
1507
1511
1510
INTERNET
1501
1513
1512
1514

Fig. 15

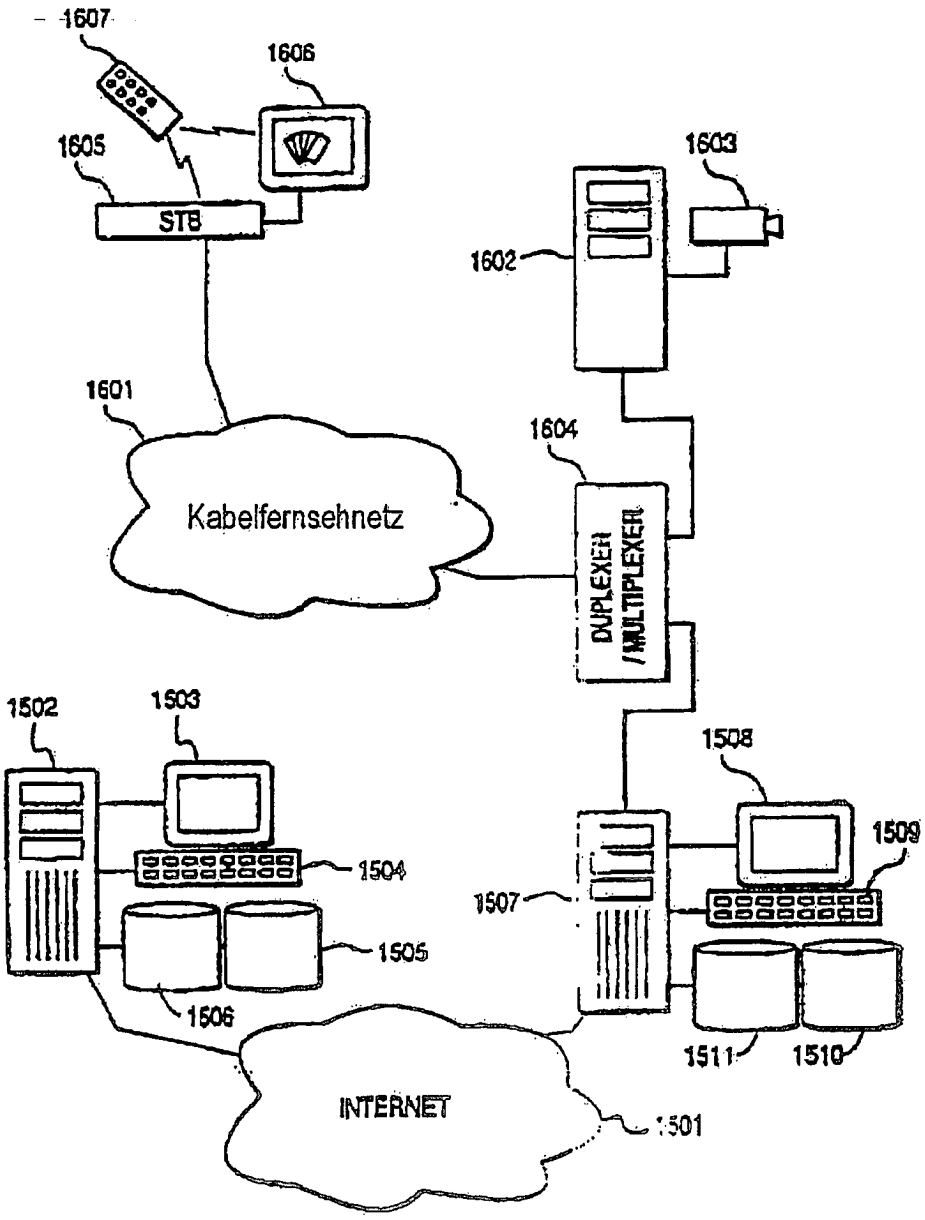

1607
1606
1605
STB
1603
1602
1601
1604
Kabelfernsehnetz
DUPLEXER /MULTIPLEXER
1502
1503
1508
1509
1504
1507
1505
1506
1511
1510
INTERNET
1501

Fig. 16

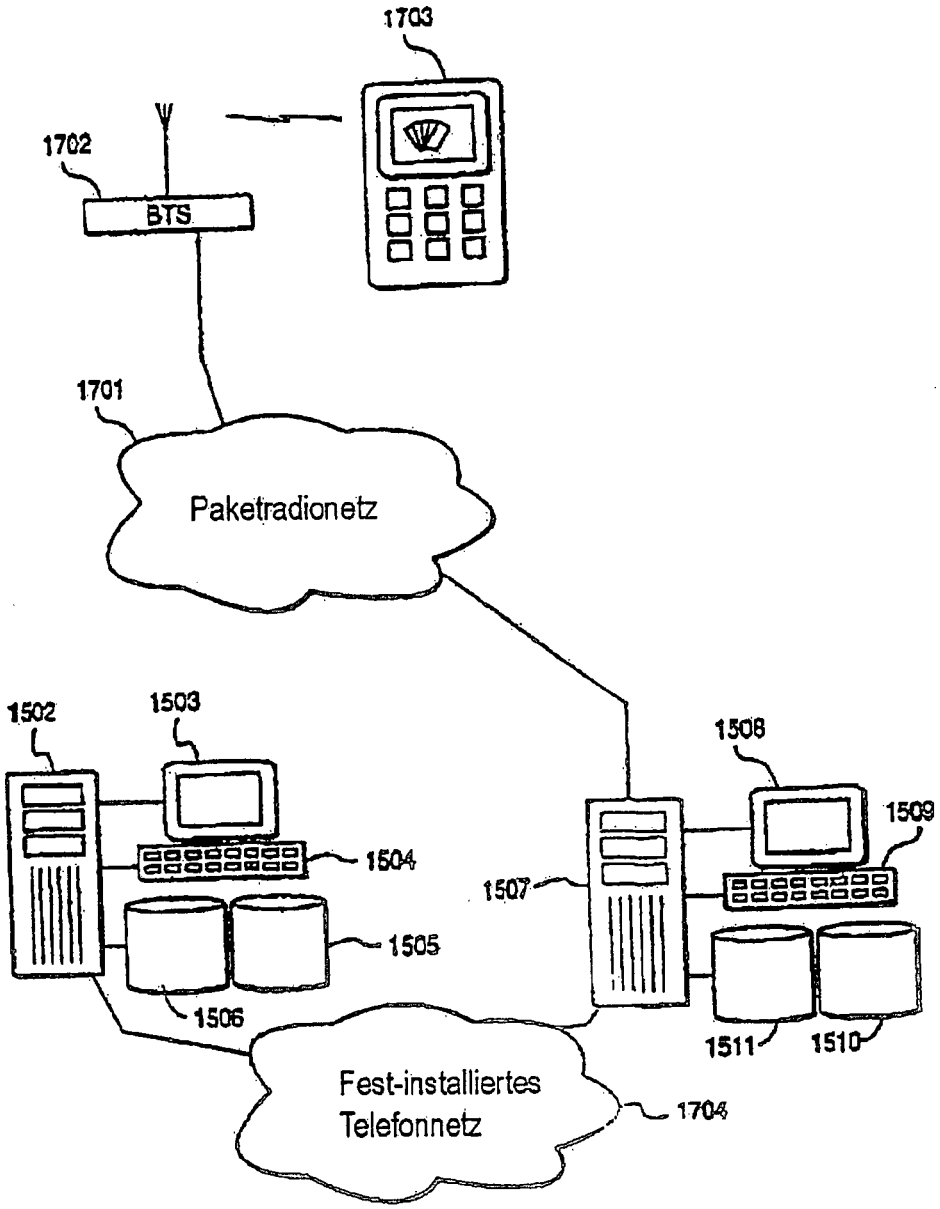

1703
1702
BTS
1701
Paketradionetz
1502
1503
1504
1505
1506
1507
1508
1509
1511
1510
Fest-installiertes
Telefonnetz
1704

Fig. 17