(19) Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 60 2004 007 116 T2** 2008.02.28

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 606 905 B1**
(21) Deutsches Aktenzeichen: **60 2004 007 116.1**
(86) PCT-Aktenzeichen: **PCT/IB2004/050242**
(96) Europäisches Aktenzeichen: **04 720 121.5**
(87) PCT-Veröffentlichungs-Nr.: **WO 2004/082201**
(86) PCT-Anmeldetag: **12.03.2004**
(87) Veröffentlichungstag der PCT-Anmeldung: **23.09.2004**
(97) Erstveröffentlichung durch das EPA: **21.12.2005**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **20.06.2007**
(47) Veröffentlichungstag im Patentblatt: **28.02.2008**

(51) Int Cl.[8]: ***H04L 9/08*** (2006.01)
G11B 20/00 (2006.01)

(30) Unionspriorität:
03100658 14.03.2003 EP

(73) Patentinhaber:
Koninklijke Philips Electronics N.V., Eindhoven, NL

(74) Vertreter:
Volmer, G., Dipl.-Ing., Pat.-Anw., 52066 Aachen

(84) Benannte Vertragsstaaten:
AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LI, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR

(72) Erfinder:
VAUCLAIR, Marc, NL-5656 AA Eindhoven, NL

(54) Bezeichnung: **GESCHÜTZTER RÜCKKANAL VOM DIGITALEN RECHTE VERWALTENDEN DONGLE**

Beschreibung

[0001] Die vorliegende Erfindung bezieht sich auf das Sichern der Übertragung von Daten und insbesondere auf ein Verfahren, eine Anordnung und ein System zum Sichern der Übertragung von Daten zwischen einer manipulationssicheren Anordnung und einer Senkenanordnung ("sink device").

[0002] Die Explosion in der Verwendung von Computer und Netzwerken, wie Internet, hat in Bezug auf den Schutz der Rechte des geistigen Eigentums auf Daten und Information, die übers Internet übertragen werden, zu Problemen geführt. Diese Probleme sind ein Ergebnis der Einfachheit, mit der digitale Information übertragen und kopiert werden kann. In digitaler Form kann Information, wie Video, Musik, Spiele, Software usw. mit einer derart hohen Qualität kopiert werden, dass sich die originalen und die kopierten Versionen der Information kaum unterscheiden lassen. Dadurch ist Information in digitaler Form ein verlockendes Ziel von Hackern.

[0003] Um das illegale Kopieren digitaler Information zu bekämpfen sind bereits mehrere Formen von Beschützung entwickelt worden. Wenn beispielsweise eine Quellenanordnung digitale Multimediainhalt zu einer Senkenanordnung sendet, kann der Inhalt in gewisser Weise verschlüsselt werden, bevor der Inhalt von der Quellenanordnung zu der Senkenanordnung übertragen wird, damit der digitale Inhalt vor Diebstahl oder unerlaubter Kopierung geschützt wird. Wie in Fig. 1 dargestellt, wird der Multimediainhalt **106** von der Quellenanordnung **102** zu der Senkenanordnung **104** zur Wiedergabe übertragen. Der Multimediainhalt **106** wird zunächst von einem Codierer **108** codiert. Der codierte Inhalt wird danach von einer Verschlüsselungsanordnung **110** unter Anwendung eines Verschlüsselungsschlüssels verschlüsselt. Die verschlüsselten Daten werden danach zu der Senkenanordnung übertragen. Die Senkenanordnung **104** benutzt den Verschlüsselungsschlüssel zum Entschlüsseln des verschlüsselten Inhalts unter Verwendung der Entschlüsselungsanordnung **114**. Der entschlüsselte Inhalt wird danach von einem Decoder **116** decodiert. Der decodierte Inhalt wird danach von einer Aufbereitungsanordnung **120** aufbereitet und an einer Wiedergabeanordnung **122** wiedergegeben. Ein Problem bei dieser Lösung ist, dass die Senkenanordnung den Verschlüsselungsschlüssel kennen muss, bevor der verschlüsselte Inhalt entschlüsselt werden kann. Auf diese Weise soll ein Lieferant von Inhalt sicher stellen, dass jeder rechtmäßiger Kunde einen Verschlüsselungsschlüssel hat. Dies könnte für große Lieferanten von Inhalt ein logistisches Problem sein. Weiterhin könnte ein Angreifer viele Quellen haben erfolgreich zu sein bei einem Versuch, den Verschlüsselungsschlüssel zu entdecken.

[0004] Ein System, das entwickelt worden ist, dieses Problem zu lösen ist die Verwendung asymmetrischer Schlüssel. Die Quellenanordnung **102** und die Senkenanordnung **104** können je einen asymmetrischen Schlüssel haben, der einen öffentlichen und einen privaten Schlüssel umfasst. Information, die mit einem öffentlichen Schlüssel verschlüsselt ist, kann nur mit Hilfe des privaten Schlüssels entschlüsselt werden und umgekehrt.

[0005] Die Verschlüsselung des Inhalts auf einer ungeschützten Verbindung zwischen der Quellenanordnung **102** und der Senkenanordnung **104** vermeidet ein unerwünschtes digitales Kopieren des Inhalts. Ein Angreifer kann aber dennoch versuchen, die Senkenanordnung **104** zu hacken um den Entschlüsselungsschlüssel zu erhalten und dadurch auf den Inhalt eingreifen zu können. Um derartige Angriffe zu bekämpfen kann die Entschlüsselung des Inhalts von einer manipulationssicheren Anordnung, wie einer Chipkarte oder einem Dongle durchgeführt werden, der entweder an die Senkenanordnung **104** angehängt ist oder einen Teil davon bildet, wie in Fig. 2 dargestellt. In diesem Szenario wird unter Verwendung eines Verschlüsselungsschlüssels der Inhalt verschlüsselt und der Verschlüsselungsschlüssel selber wird unter Verwendung des öffentlichen Schlüssels der manipulationssicheren Anordnung verschlüsselt. Wenn die manipulationssichere Anordnung den verschlüsselten Inhalt und den Schlüssel empfangt, wird unter Verwendung des privaten Schlüssels der manipulationssicheren Anordnung der verschlüsselte Verschlüsselungsschlüssel entschlüsselt. Der private Schlüssel ist auf sicher Weise innerhalb der manipulationssicheren Anordnung **201** gespeichert, so dass der Angreifer nicht auf den privaten Schlüssel zugreifen kann. Der empfangene verschlüsselte Inhalt wird unter Verwendung des gespeicherten entschlüsselten Verschlüsselungsschlüssels von der Entschlüsselungsanordnung **203** entschlüsselt. Der entschlüsselte Inhalt wird dem Decoder **116** zugeführt und wird verarbeitet, wie oben anhand der Fig. 1 beschrieben worden ist. Ein Nachteil dieses Systems ist, dass der Inhalt in einem ungeschützten Format von der manipulationssicheren Anordnung zu der Senkenanordnung **104** gesendet wird. Dadurch kann durch Einfügung einer Schnüffelanordnung zwischen die Senkenanordnung **104** und die manipulationssicheren Anordnung **201** dennoch eine unerlaubte Kopie des Inhalts gemacht werden. Dadurch gibt es ein Bedürfnis nach einem Verfahren und einem System zum Schützen der Verbindung zwischen der Senkenanordnung und der manipulationssicheren Anordnung.

[0006] Dem Dokument US2003/021420 liegt die Erkenntnis zugrunde, die Benutzerdaten, die aus dem Aufzeichnungsmedium innerhalb einer integrierten Einheit in der Treibereinheit und nicht innerhalb einer Applikationseinheit unter Verwendung einer PC Ap-

plikation ausgelesen werden, zu entschlüsseln und neu zu verschlüsseln.

[0007] Es ist nun u. a. eine Aufgabe der vorliegenden Erfindung, den oben genannten Nachteil dadurch zu überwinden, dass der Inhalt, der zwischen der manipulationssicheren Anordnung und der Senkenanordnung gesendet wird, verschlüsselt wird.

[0008] Nach einer Ausführungsform der vorliegenden Erfindung wird ein Verfahren, eine Anordnung und ein System zum Schaffen einer sicheren Kommunikation zwischen einer manipulationssicheren Anordnung und einer Senkenanordnung geschaffen. Verschlüsselter Inhalt wird von einer Quellenanordnung her bei der manipulationssicheren Anordnung empfangen, wobei der Inhalt unter Verwendung eines ersten Schlüsseln verschlüsselt worden ist. Der Inhalt wird unter Verwendung des entschlüsselten ersten Schlüssels entschlüsselt. Ein zweiter Schlüssel wird bei der manipulationssicheren Anordnung von der Senkenanordnung her empfangen, wobei der zweite Schlüssel unter Verwendung des öffentlichen Schlüssels der manipulationssicheren Anordnung verschlüsselt wird. Der zweite Schlüssel wird unter Verwendung des privaten Schlüssels der manipulationssicheren Anordnung entschlüsselt. Der Inhalt wird unter Verwendung des zweiten Schlüssels neu verschlüsselt. Der neu verschlüsselte Inhalt wird zu der Senkenanordnung übertragen.

[0009] Ausführungsbeispiele der vorliegenden Erfindung sind in der Zeichnung dargestellt und werden im Folgenden näher beschrieben. Es zeigen:

[0010] Fig. 1 ein Blockschaltbild eines bekannten Übertragungssystems zur Übertragung von Medieninhalt,

[0011] Fig. 2 ein Blockschaltbild eines bekannten Übertragungssystems zur Übertragung von Medieninhalt,

[0012] Fig. 3 eine Darstellung des Flusses der Daten und des verschlüsselten Schlüssels zwischen der Quellenanordnung, einer manipulationssicheren Anordnung und einer Senkenanordnung nach einer Ausführungsform der vorliegenden Erfindung, und

[0013] Fig. 4 ein Blockschaltbild eines Übertragungssystems zur Übertragung von Medieninhalt zu einer Ausführungsform der vorliegenden Erfindung.

[0014] Nach einer Ausführungsform der vorliegenden Erfindung sind einer Quellenanordnung, einer manipulationssichere Anordnung und einer Senkenanordnung je ein asymmetrischer öffentlich-privates Schlüsselpaar zugeordnet, das zum Authentisieren jeder Anordnung gegenüber anderen Anordnungen verwendet werden kann und die Schlüsselpaare werden auch zum Durchführen eines geschützten Informationsaustausches zwischen den jeweiligen Anordnungen verwendet. Anders als bei den bekannten oben beschriebenen Systemen benutzt die vorliegende Erfindung die öffentlichprivaten Schlüssel zum Verschlüsseln der Verschlüsselungsschlüssel, die zum Entschlüsseln des Inhalts bei der Verbindung zwischen der Quellenanordnung und der manipulationssicheren Anordnung und der Verbindung zwischen der manipulationssicheren Anordnung und der Senkenanordnung verwendet werden. Kurz gesagt wird der erste Verschlüsselungsschlüssel, der von der Quellenanordnung zum Verschlüsseln des Inhalts verwendet wird, von der Quellenanordnung der manipulationssicheren Anordnung zugesendet, die mit dem öffentlichen Schlüssel der manipulationssicheren Anordnung verschlüsselt ist (der verschlüsselte Schlüssel überträgt transparent über die Senkenanordnung). Dieser Schlüssel ist permanent und hängt an dem Inhalt. Die Senkenanordnung kennt den Schlüssel nicht. Außerdem wird ein zweiter Verschlüsselungsschlüssel, der von der manipulationssicheren Anordnung zum Verschlüsseln des Inhalts verwendet wird, der zwischen der manipulationssicheren Anordnung und der Senkenanordnung gesendet wird, selber unter Verwendung des öffentlichen Schlüssels der manipulationssicheren Anordnung verschlüsselt und wird von der Senkenanordnung der manipulationssicheren Anordnung zugeführt. In der alternativen Ausführungsform kann statt des zweiten Verschlüsselungsschlüssels der manipulationssicheren Anordnung ein Verwürfelungsschlüssel von der Senkenanordnung her gesendet werden, wie nachstehend noch näher beschrieben wird.

[0015] Der Daten- und Verschlüsselungsschlüsselstrom, der oben kurz beschrieben wurde, wird nun anhand der Fig. 3 näher beschrieben. Wie dargestellt, ist eine Quellenanordnung **301** über eine Übertragungsverbindung **302** mit einer manipulationssicheren Anordnung **303** verbunden und die manipulationssichere Anordnung **303** ist über eine Übertragungsverbindung **304** mit einer Senkenanordnung **304** verbunden. Es dürfte dem Fachmann einleuchten, dass die Übertragungsverbindungen jede Art von Übertragungsverbindung sein kann, und zwar drahtlos sowie verdrahtet, die imstande ist, digitale Information zu übertragen. Die Quellenanordnung **301** hat einen öffentlichen Schlüssel **1** und einen privaten Schlüssel 1. Die manipulationssichere Anordnung **302** hat einen öffentlichen Schlüssel 2 und einen privaten Schlüssel 2. Die Senkenanordnung **305** hat einen öffentlichen Schlüssel 3 und einen privaten Schlüssel 3. Die Anordnungen benutzen den öffentlichen und den privaten Schlüssel auf bekannte Art und Weise um sich anderen gegenüber zu authentisieren. Während die Anordnungen aus Fig. 3 je ein öffentliches/privates Schlüsselpaar haben, dürfte es dem Fachmann einleuchten, dass alle Anordnungen,

beispielsweise die Senkenanordnung, nicht ein öffentlichprivates Schlüsselpaar brauchen um die vorliegende Erfindung zu praktisieren.

[0016] Wie nachstehend noch näher erläutert wird, verschlüsselt die Quellenanordnung **301** den Multimedieninhalt unter Verwendung eines ersten Verschlüsselungsschlüssels **306** und überträgt den verschlüsselten Inhalt zu der manipulationssicheren Anordnung **303** über die Übertragungsverbindung **302**. Außerdem verschlüsselt der Verschlüsselungsschlüssel **306** den öffentlichen Schlüssel 2 der manipulationssicheren Anordnung **303** und überträgt den verschlüsselten Verschlüsselungsschlüssel zu der manipulationssicheren Anordnung **303** über die Übertragungsverbindung **302**. Kurz gesagt entschlüsselt danach die manipulationssichere Anordnung **303** den verschlüsselten Verschlüsselungsschlüssel **306** unter Verwendung des privaten Schlüssels. Die manipulationssichere Anordnung **303** entschlüsselt danach den verschlüsselten Inhalt unter Verwendung des entschlüsselten Verschlüsselungsschlüssels **306**. In der alternativen Ausführungsform können die Quellenanordnung **301** und die manipulationssichere Anordnung **303** während der Authentifizierungsphase des Protokolls Schlüsselmaterial austauschen. Das an beiden Seiten der Verbindung ausgetauschte Schlüsselmaterial wird danach gruppiert und in einem mathematischen Prozess zum Erzeugen eines Schlüsselgenerators verwendet, der an beiden Seiten der Verbindung denselben Schlüssel oder denselben Schlüsselstrom liefert, wenn der Verschlüsselungsschlüssel zu bestimmten Intervallen aktualisiert, modifiziert werden muss. In diesem Szenario würde die manipulationssichere Anordnung den Schlüssel erzeugen und den von der Quellenanordnung **301** empfangenen Inhalt decodieren.

[0017] Die Senkenanordnung **305** selektiert einen zweiten Verschlüsselungs- oder Verwürfelungsschlüssel **307**. Die Senkenanordnung verschlüsselt danach den zweiten Verschlüsselungs- oder Verwürfelungsschlüssel **307** unter Verwendung des öffentlichen Schlüssels 2 der manipulationssicheren Anordnung **303**. Der verschlüsselte zweite Verschlüsselungs- oder Verwürfelungsschlüssel **307** wird danach über die Übertragungsverbindung **304** der manipulationssicheren Anordnung **303** zugeführt. Die manipulationssichere Anordnung **303** entschlüsselt den zweiten Verschlüsselungs- oder Verwürfelungsschlüssel **307** unter Verwendung des privaten Schlüssels. Die manipulationssichere Anordnung **303** verschlüsselt danach den entschlüsselten Inhalt von der Quellenanordnung **301** unter Verwendung des zweiten Verschlüsselungs- oder Verwürfelungsschlüssels **307** und überträgt den neu verschlüsselten Inhalt zu der Senkenanordnung **305** über die Übertragungsverbindung **304**.

[0018] Die vorliegende Erfindung wird nun anhand der Fig. 4 detailliert beschrieben. Wie dargestellt, wird Multimedieninhalt von einer Quellenanordnung **402** zu einer Senkenanordnung **406** zur Wiedergabe übertragen. Die Quellenanordnung **402** umfasst u. a. Elemente, eine Speicheranordnung **408**, einen Bus **410**, einen Codierer **412**, eine Verschlüsselungsanordnung **414** und einen Prozessor **416** zur Steuerung des Betriebs der Quellenanordnung **402**. Es dürfte einleuchten, dass die Quellenanordnung andere Elemente enthalten kann und einige der genannten Elemente können zu einen einzigen Element kombiniert werden. Der gespeicherte Multimedieninhalt wird zunächst von dem Codierer **412** optisch codiert. Der (codierte) Inhalt wird danach von der Verschlüsselungsanordnung **414** unter Verwendung eines ersten Verschlüsselungsschlüssels verschlüsselt. Der erste Verschlüsselungsschlüssel wird danach unter Verwendung des Öffentlichen Schlüssels der manipulationssicheren Anordnung **404** von der Verschlüsselungsanordnung **414** verschlüsselt. Der verschlüsselte Inhalt und der verschlüsselte erste Verschlüsselungsschlüssel werden danach über die Übertragungsanordnung **418** zu der manipulationssicheren Anordnung **404** übertragen. Wie oben anhand der Fig. 3 beschrieben, können in der alternativen Ausführungsform die Quellenanordnung **301** und die manipulationssichere Anordnung **303** während der Authentifizierungsphase Schlüsselmaterial austauschen, um einander die Möglichkeit zu bieten, denselben ersten Verschlüsselungsschlüssel zu erzeugen. In diesem Szenario würde die Quellenanordnung **402** den ersten Verschlüsselungscode erzeugen und den Inhalt verschlüsseln, wobei der Inhalt der manipulationssicheren Anordnung **404** zugeführt wird.

[0019] Die manipulationssichere Anordnung **404** umfasst unter anderen Elementen eine Entschlüsselungsanordnung **420**, eine Verschlüsselungsanordnung **422**, eine Speicheranordnung **424**, einen Bus **428** und einen Prozessor **426** zur Steuerung des Betriebs der manipulationssicheren Anordnung. Die manipulationssichere Anordnung entschlüsselt zunächst unter Verwendung des privaten Schlüssels, der in dem Speicher **424** gespeichert ist, den ersten Verschlüsselungsschlüssel. Wenn der Verschlüsselungsschlüssel einmal von der Entschlüsselungsanordnung **420** einmal entschlüsselt worden ist, benutzt die Entschlüsselungsanordnung **420** den entschlüsselten Verschlüsselungsschlüssel um den verschlüsselten Inhalt zu entschlüsseln, der von der Quellenanordnung **402** her empfangen wurde. In der alternativen Ausführungsform könnte die manipulationssichere Anordnung **404** den ersten Verschlüsselungsschlüssel erzeugen und den verschlüsselten Inhalt entschlüsseln.

[0020] Die Senkenanordnung **406** umfasst unter anderen Elementen einen Bus **432**, eine Verschlüsse-

lungs-/Entschlüsselungsanordnung **434**, einen Decoder **436**, eine Aufbereitungsanordnung **438**, eine Ausgangsanordnung **440**, einen Speicher **442** und eine Verarbeitungsanordnung **444** zur Steuerung des Betriebs der Senkenanordnung **406**. Die Senkenanordnung **406** selektiert den zweiten Verschlüsselungsschlüssel, der verwendet wird zum Schützen des Inhaltes, der über die Übertragungsverbindung **430** zwischen der manipulationssicheren Anordnung **404** und der Senkenanordnung **406** übertragen wird. Die Verschlüsselungs-/Entschlüsselungsanordnung **434** verschlüsselt den zweiten Verschlüsselungsschlüssel unter Verwendung des öffentlichen Schlüssels der manipulationssicheren Anordnung **404** und überträgt den verschlüsselten Verschlüsselungsschlüssel zu der manipulationssicheren Anordnung über die Übertragungsverbindung **430**.

[0021] Die Entschlüsselungsanordnung **420** entschlüsselt den verschlüsselten zweiten Verschlüsselungsschlüssel unter Verwendung des privaten Schlüsseln der manipulationssicheren Anordnung **404**. Die Verschlüsselungsanordnung kann nun den entschlüsselten Inhalt von der Quellenanordnung **402** unter Verwendung des zweiten Verschlüsselungsschlüssels verschlüsseln. Der neu verschlüsselte Inhalt wird danach über die Übertragungsverbindung **430** der Senkenanordnung **46** zugeführt.

[0022] Die Senkenanordnung **406** benutzt den zweiten Verschlüsselungsschlüssel zum Entschlüsseln des verschlüsselten Inhalts, der von der manipulationssicheren Anordnung **404** her empfangen wird, und zwar unter Verwendung der Verschlüsselungs-/Entschlüsselungsanordnung **434**. Der entschlüsselte Inhalt wird danach ggf. von dem Decoder **436** decodiert. Der decodierte Inhalt wird danach weiter verarbeitet, so wird er beispielsweise von der Aufbereitungsanordnung **120** aufbereitet und an der Auslieferungsanordnung **440** wiedergegeben.

[0023] Der zweite Verschlüsselungsschlüssel kann viele Formen annehmen. So kann beispielsweise der zweite Verschlüsselungsschlüssel ein Verwürfelungsschlüssel sein, der benutzt wird um einen Pseudozufallsgenerator anzukurbeln, beispielsweise in der Verschlüsselungsanordnung **422**, wobei der Ausgang des Pseudozufallsgenerators öffentlich mit dem Inhalt in der manipulationssicheren Anordnung geXORt wird. Die Senkenanordnung **406** müsste dann die empfangenen Daten mit dem Ausgang des eigenen Pseudozufallsgenerators XORen, beispielsweise in der Verschlüsselungs-/Entschlüsselungsanordnung **434**, angekurbelt durch denselben zweiten Verschlüsselungsschlüssel. Es dürfte dem Fachmann einleuchten, dass jede beliebige sichere Stromverschlüsselungstechnik auch für diesen Vorgang geeignet ist und dass die vorliegende Erfindung sich nicht darauf beschränkt.

[0024] Der zweite Verschlüsselungsschlüssel ist vorübergehend und wird nur während der Inhaltsübertragung zwischen der manipulationssicheren Anordnung **404** und der Senkenanordnung **406** verwendet. Die Manipulationssichere Anordnung **404** erzwingt einen Applikationsschichtschutz, während die der Senkenanordnung **406** zugefügte kryptographische Fähigkeit einen Verbindungsschichtschutz erzwingt. Das Verfahren ist derart entworfen, dass die kryptographischen Fähigkeiten, die von der Senkenanordnung **406** erwartet werden, auf ein Minimum gehalten werden.

[0025] Es dürfte einleuchten, dass die verschiedenen Ausführungsformen der vorliegenden Erfindung sich nicht auf die genaue Reihenfolge der oben beschriebenen Schritte beschränken, da das Timing einiger Schritte ohne Beeinträchtigung des gesamten Betriebs der vorliegenden Erfindung getauscht werden kann. Weiterhin schließt der Ausdruck "enthalten" andere Elemente oder Schritte nicht aus und der Term "ein" schließt eine Anzahl nicht aus und ein einziger Prozessor oder eine andere Einheit kann die Funktionen verschiedener in den Patentansprüchen genannter Einheiten oder Schaltungsanordnungen erfüllen.

Patentansprüche

1. Verfahren zum Schaffen einer sicheren Kommunikation zwischen einer manipulationssicheren Anordnung und einer Senkenanordnung, wobei dieses Verfahren die nachfolgenden Verfahrensschritte umfasst:
– das Empfangen verschlüsselten Inhalts von einer Quellenanordnung an einer manipulationssicheren Anordnung, wobei der genannte Inhalt unter Anwendung eines ersten Schlüssels verschlüsselt worden ist;
– das Entschlüsseln des Inhalts unter Anwendung des ersten Schlüssels;
– das Empfangen eines zweiten Schlüssels an einer manipulationssicheren Anordnung aus der Senkenanordnung, wobei der zweite Schlüssel unter Anwendung des öffentlichen Schlüssels der manipulationssicheren Anordnung verschlüsselt ist;
– das Entschlüsseln des zweiten Schlüssels unter Anwendung des privaten Schlüssels der manipulationssicheren Anordnung;
– das Neuverschlüsseln des Inhalts unter Anwendung des genannten zweiten Schlüsselns; und
– das Übertragen des genannten neu verschlüsselten Inhalts zu der genannten Senkenanordnung.

2. Verfahren nach Anspruch 1, wobei der verschlüsselte Inhalt codiert wird.

3. Verfahren nach Anspruch 2, wobei das Verfahren weiterhin die nachfolgenden Verfahrensschritte umfasst:

– das Entschlüsseln des verschlüsselten Inhalts unter Anwendung des genannten zweiten Schlüsseln in der genannten Senkenanordnung;
– das Decodieren des verschlüsselten Inhalts;
– das Wiedergeben des genannten Inhalts.

4. Verfahren nach Anspruch 1, wobei die manipulationssichere Anordnung eine Chipkarte oder ein Dongle ist.

5. Verfahren nach Anspruch 1, wobei der zweite Schlüssel verwendet wird um einen ersten Zufallszahlgenerator anzukurbeln und wobei das Ausgangssignal des Generators mit den entschlüsselten Daten in der manipulationssicheren Anordnung "ge-XOR-t" wird.

6. Verfahren nach Anspruch 5, wobei die Senkenanordnung den empfangenen entschlüsselten Inhalt mit einem Ausgangssignal eines zweiten, von dem zweiten Schlüssel angekurbelten Zufallszahlgenerators "XOR-t".

7. Verfahren nach Anspruch 1, wobei der genannte Inhalt Multimedieninhalt ist.

8. Verfahren nach Anspruch 1, wobei die Quellenanordnung und die manipulationssichere Anordnung je denselben ersten Schlüssel erzeugen.

9. Verfahren nach Anspruch 1, wobei der erste Schlüssel der manipulationssicheren Anordnung zugeführt wird.

10. Verfahren nach Anspruch 9, wobei der erste Schlüssel unter Anwendung eines öffentlichen Schlüssels der manipulationssicheren Anordnung verschlüsselt wird.

11. Anordnung zum Schaffen einer sicheren Kommunikation zwischen einer manipulationssicheren Anordnung und einer Senkenanordnung, wobei diese Anordnung die nachfolgenden Elemente umfasst:
– Mittel zum Empfangen (**404**) verschlüsselten Inhalts von einer Quellenanordnung (**402**) an der manipulationssicheren Anordnung (**404**), wobei die genannten Daten unter Anwendung eines ersten Schlüssels verschlüsselt worden sind;
– Mittel zum Entschlüsseln (**420**) des Inhalts unter Anwendung des ersten Schlüssels;
– Mittel zum Empfangen (**404**) eines zweiten Schlüssels an der manipulationssicheren Anordnung aus der Senkenanordnung (**406**), wobei der zweite Schlüssel unter Anwendung des öffentlichen Schlüssels der manipulationssicheren Anordnung verschlüsselt ist;
– Mittel zum Entschlüsseln (**420**) des zweiten Schlüssels unter Anwendung des privaten Schlüssels der manipulationssicheren Anordnung;
– Mittel zum Neuverschlüsseln (**422**) des Inhalts unter Anwendung des genannten zweiten Schlüsselns; und
– Mittel zum Übertragen (**404**) des genannten neu verschlüsselten Inhalts zu der genannten Senkenanordnung.

Es folgen 3 Blatt Zeichnungen

Anhängende Zeichnungen

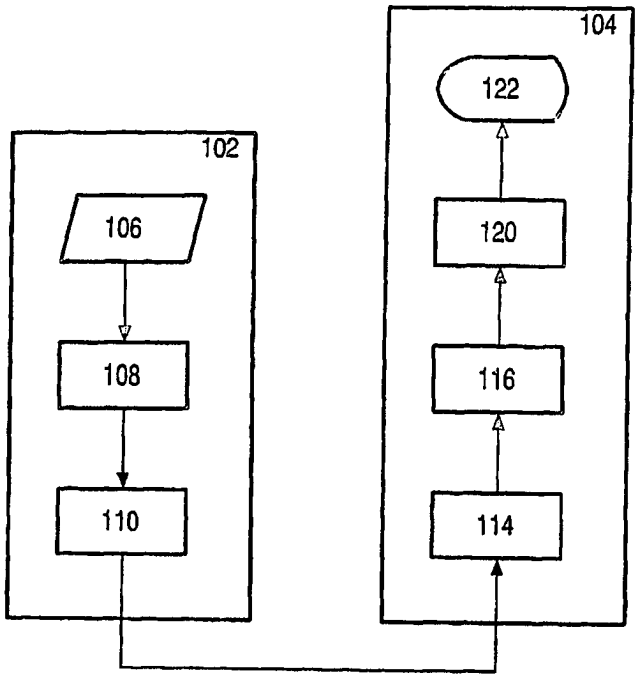

FIG. 1

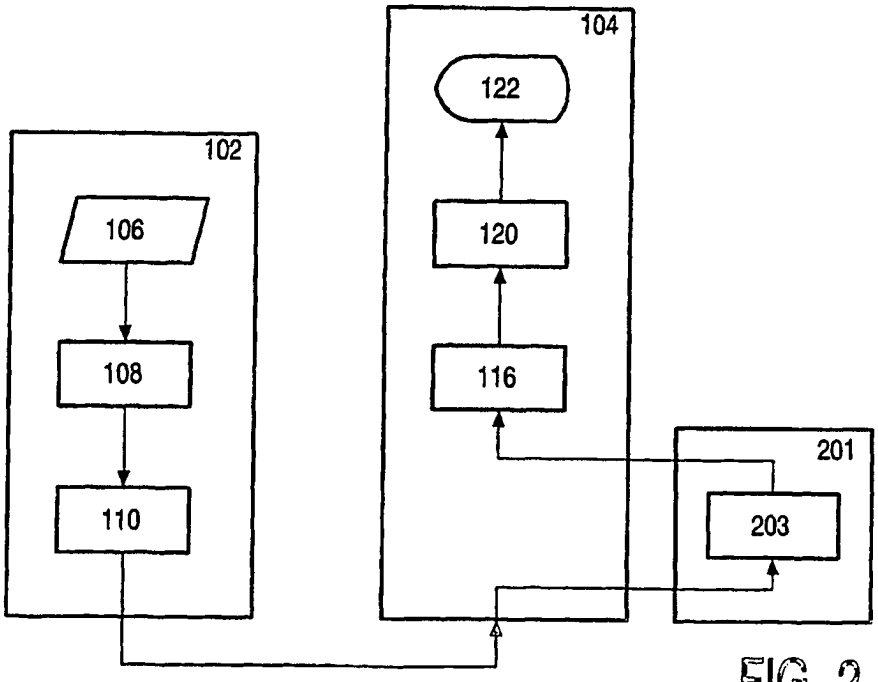

FIG. 2

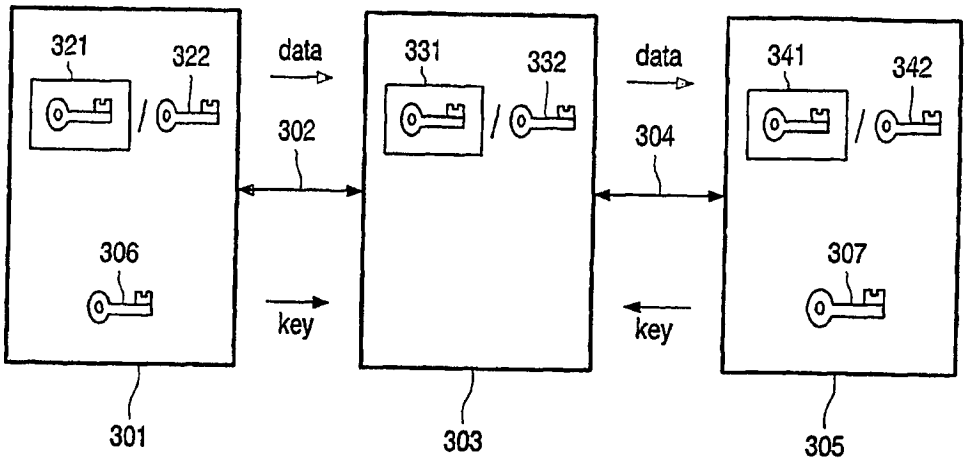
321
322
data
331
332
data
341
342
302
304
306
307
key
key
301
303
305

FIG. 3

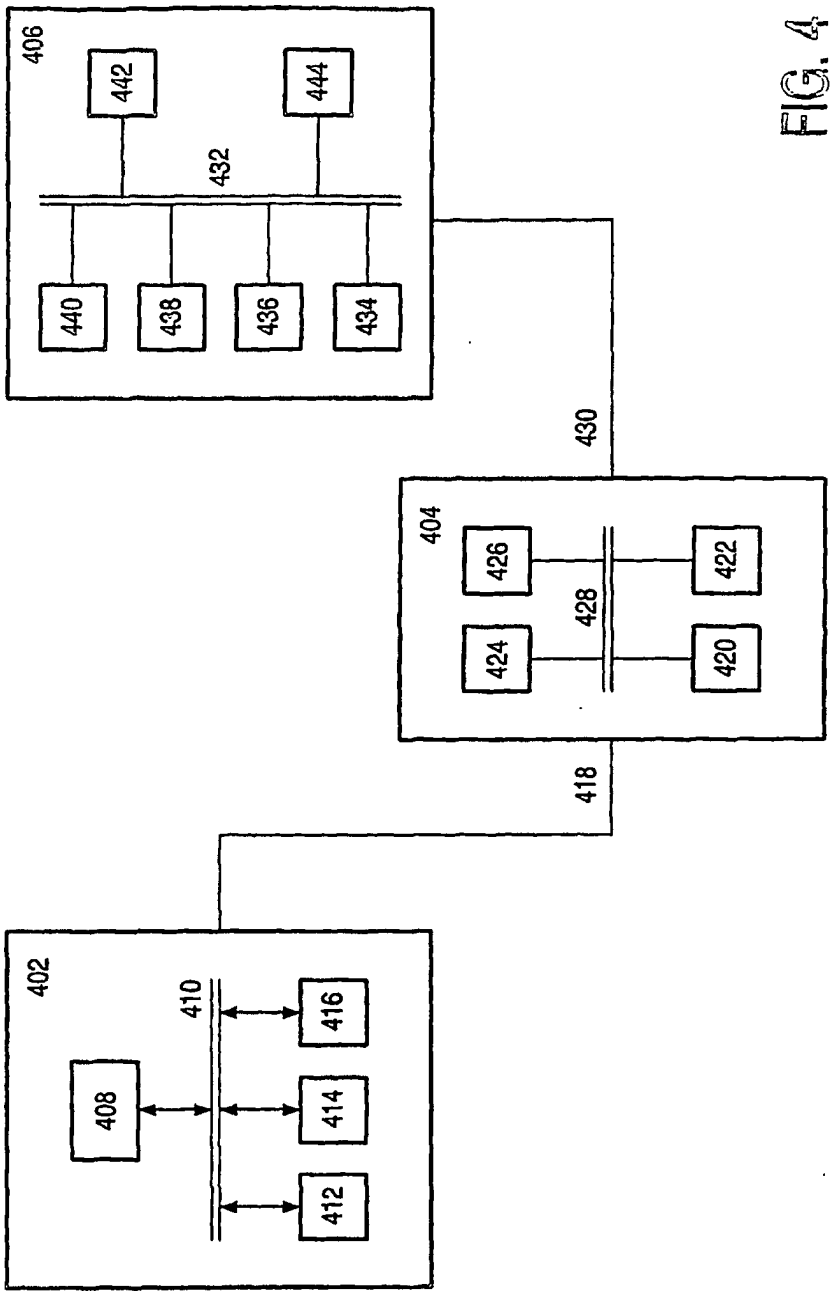
406
442
444
432
440
438
436
434
430
404
426
422
428
424
420
418
402
410
416
408
414
412

FIG. 4