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

(10) **DE 603 16 861 T2** 2008.07.24

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 355 445 B1**
(21) Deutsches Aktenzeichen: **603 16 861.2**
(96) Europäisches Aktenzeichen: **03 251 967.0**
(96) Europäischer Anmeldetag: **28.03.2003**
(97) Erstveröffentlichung durch das EPA: **22.10.2003**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **17.10.2007**
(47) Veröffentlichungstag im Patentblatt: **24.07.2008**

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

(30) Unionspriorität:
0208858 18.04.2002 GB

(84) Benannte Vertragsstaaten:
DE, FR, GB

(73) Patentinhaber:
Hewlett-Packard Development Co., L.P., Houston, Tex., US

(74) Vertreter:
Schoppe, Zimmermann, Stöckeler & Zinkler, 82049 Pullach

(72) Erfinder:
Casassa Mont, Marco, Stoke Gifford, Bristol BS34 8BF, GB; Harrison, Keith Alexander, Chepstow, Monmouthshire NP16 7PX, GB; Sadler, Martin, Fishponds, Bristol BS16 3SQ, GB

(54) Bezeichnung: **Verfahren und Vorrichtung zur Verschlüsselung/Entschlüsselung von Daten**

Beschreibung

[0001] Die vorliegende Erfindung bezieht sich auf ein Verfahren und eine Vorrichtung zum Verschlüsseln/Entschlüsseln von Daten.

[0002] Beim Umgang mit geheimen (privaten) und vertraulichen Informationen besteht häufig ein Erfordernis, zu gewährleisten, dass die Informationen bis zu einem spezifischen Zeitpunkt geheim und vertraulich gehalten werden, beispielsweise muss bei unter Verschluss zu haltenden Angeboten der Urheber eines Angebots darauf vertrauen können, dass sein Angebot nicht vor einem spezifischen Datum offengelegt wird.

[0003] Eine Aufgabe der vorliegenden Erfindung besteht darin, die Freigabe vertraulicher Informationen zu (oder möglicherweise nach) einem spezifischen Zeitpunkt zu erleichtern.

[0004] Ein bekannter Lösungsansatz zum Aufrechterhalten der Vertraulichkeit von Daten ist die Verwendung von Verschlüsselung. Jedoch erfordern traditionelle Verschlüsselungstechniken, z. B. die Verwendung von symmetrischen Schlüsseln oder von PKI-Verschlüsselung, dass ein entsprechender Entschlüsselungsschlüssel zum Zeitpunkt der Verschlüsselung bekannt ist. Um die Vertraulichkeit zu gewährleisten, muss der Entschlüsselungsschlüssel somit sicher aufbewahrt werden, bis er benötigt wird. Sollte jedoch jemand unbefugten Zugriff auf den Entschlüsselungsschlüssel erlangen, könnte dies einen unbefugten Zugriff auf die vertraulichen Daten ermöglichen. Ferner kann die Installation und Verwendung von symmetrischen Schlüsseln und einer PKI-Verschlüsselung komplex sein.

[0005] Ein jüngeres kryptographisches Schema ist eine kennungsbasierte Verschlüsselung (IBE – identifier-based encryption). Bei diesem Schema verschlüsselt ein Datenanbieter Nutzdaten unter Verwendung einer Verschlüsselungsschlüssel-Zeichenfolge und von öffentlichen Daten, die durch eine vertrauenswürdige Autorität bereitgestellt werden; der Datenanbieter liefert anschließend die verschlüsselten Nutzdaten an einen Empfänger, der sie unter Verwendung eines Entschlüsselungsschlüssels, der durch die Vertrauensautorität bereitgestellt wird, zusammen mit den öffentlichen Daten der Letzteren entschlüsselt. Die öffentlichen Daten der vertrauenswürdigen Autorität werden durch die Autorität unter Verwendung von geheimen Daten unter Verwendung einer Ein-Weg-Funktion abgeleitet. Merkmale des IBE-Schemas sind, dass eine beliebige Art von Zeichenfolge (einschließlich eines Namens, einer Rolle usw.) als Verschlüsselungsschlüssel-Zeichenfolge verwendet werden kann und dass die Erzeugung des Entschlüsselungsschlüssels durch die Vertrauensautorität bewirkt wird, die die Verschlüsselungsschlüssel-Zeichenfolge und ihre geheimen Daten verwendet, wodurch ermöglicht wird, dass die Erzeugung des Entschlüsselungsschlüssels verschoben wird, bis sie zur Entschlüsselung benötigt wird.

[0006] Man kennt eine Anzahl von IBE-Algorithmen, einschließlich des „Quadratische Residuosität"-Verfahrens (QR-Verfahrens, QR = quadratic residuosity), das in dem folgenden Dokument beschrieben ist: „An Identity Based Encryption Scheme based an Quadratic Residues". C. Cocks Communications-Electronics Security Group (CESG), UK. http://www.cesg.gov.uk/technology/idpkc/media/ciren.pdf – 2001. Andere IBE-Algorithmen sind bekannt, beispielsweise die Verwendung von Weil- oder Tate-Paarungen – siehe beispielsweise: D. Boneh, M. Franklin – Identity-based Encryption from the Weil Pairing. Crypto 2001–2001.

[0007] Die japanische Patentanmeldung JP 11 027252 beschreibt eine Schlüsselverwaltungsausrüstung, die dahin gehend angeordnet ist, Öffentlicher-/Privater-Schlüssel-Paare (z. B. RSA-Schlüssel-Paare) zu erzeugen, Schlüsselpaare bestimmten Freigabezeiten zuzuweisen, eine anfordernde Partei zu liefern, wobei der öffentliche Schlüssel der durch die anfordernde Partei angegebenen Freigabezeit zugewiesen ist, und jeden privaten Schlüssel zu seiner zugeordneten Freigabezeit zu veröffentlichen.

Zusammenfassung der Erfindung

[0008] Gemäß einem ersten Aspekt der vorliegenden Erfindung ist ein Sicherheitsverfahren vorgesehen, das folgende Schritte aufweist:
erste Operationen, ausgeführt durch eine Offenbarungseinrichtung von Daten, die ein Verschlüsseln der Daten und ein Liefern der verschlüsselten Daten an einen Empfänger aufweisen, wobei der Verschlüsselungsprozess sowohl einen Verschlüsselungsschlüssel als auch öffentliche Daten, die durch eine vertrauenswürdige Partei geliefert und unter Verwendung von privaten Daten von derselben abgeleitet werden, verwendet; und
zweite Operationen, ausgeführt durch die vertrauenswürdige Partei, die ein Verwenden sowohl der privaten Daten als auch weiterer Daten, um einen Entschlüsselungsschlüssel, der anschließend ausgegeben wird, zu bestimmen, aufweisen;
gekennzeichnet dadurch, dass der durch die Datenoffenbarungseinrichtung verwendete Verschlüsselungsschlüssel einen Zeitwert aufweist, und dass der Entschlüsselungsschlüssel durch die vertrauenswürdige Partei periodisch mit den weiteren Daten, die, bei jeder Bestimmung, einen neuen aktuellen Zeitwert, der unabhängig von dem Verschlüsselungsschlüssel abgeleitet wird, aufweisen, bestimmt wird, wobei der Entschlüsselungsschlüssel so bestimmt wird, dass, für den aktuellen Zeitwert, der dem durch die Datenoffenbarungseinrichtung für ihren Ver-

schlüsselungsschlüssel verwendeten Zeitwert gleicht, der Entschlüsselungsschlüssel geeignet ist, die verschlüsselten Daten der Offenbarungseinrichtung zu entschlüsseln.

[0009] Dies liefert den Vorteil, zu gewährleisten, dass ein Entschlüsselungsschlüssel, der zum Entschlüsseln verschlüsselter Daten benötigt wird, nur erzeugt wird, wenn ein Zugriff auf vertrauliche Informationen autorisiert ist.

[0010] Gemäß einem zweiten Aspekt der vorliegenden Erfindung ist ein Computersystem vorgesehen, das eine erste Recheneinheit aufweist, die angeordnet ist, um, zur Ausgabe, erste Daten gemäß einem Verschlüsselungsprozess, in den sowohl ein Verschlüsselungsschlüssel als auch zweite, öffentliche Daten, bereitgestellt durch eine vertrauenswürdige Partei, eingebunden sind, zu verschlüsseln; eine zweite Recheneinheit, die der vertrauenswürdigen Partei zugeordnet ist und angeordnet ist, um, zur Ausgabe, unter Verwendung sowohl von dritten Daten als auch vierten, privaten, Daten, von denen die zweiten Daten abgeleitet wurden, einen Entschlüsselungsschlüssel zu bestimmen; und eine dritte Recheneinheit, die angeordnet ist, um sowohl die verschlüsselten ersten Daten als auch den Entschlüsselungsschlüssel zu empfangen und die empfangenen verschlüsselten ersten Daten unter Verwendung des empfangenen Entschlüsselungsschlüssels zu entschlüsseln; gekennzeichnet dadurch, dass die erste Recheneinheit angeordnet ist, um einen Zeitwert als den Verschlüsselungsschlüssel zu verwenden, und dass die zweite Recheneinheit angeordnet ist, um den Entschlüsselungsschlüssel periodisch zu bestimmen, wobei als die dritten Daten, bei jeder Bestimmung, ein neuer aktueller Zeitwert, der unabhängig von dem Verschlüsselungsschlüssel abgeleitet wird, verwendet wird, wobei der Entschlüsselungsschlüssel so durch die zweite Recheneinheit bestimmt wird, dass, für den aktuellen Zeitwert, der dem durch die erste Recheneinheit für ihren Verschlüsselungsschlüssel verwendeten Zeitwert gleicht, der Entschlüsselungsschlüssel geeignet ist, die verschlüsselten ersten Daten zu entschlüsseln.

[0011] Gemäß einem dritten Aspekt der vorliegenden Erfindung ist eine Vorrichtung zum Erzeugen eines Entschlüsselungsschlüssels vorgesehen, die einen Speicher zum Halten von privaten Daten, eine Quelle von Zeitsignalen, einen Prozessor zum Verwenden der privaten Daten, um, periodisch, Entschlüsselungsschlüssel zu erzeugen, die jeweils angepasst sind, um Daten, die mit einem jeweiligen entsprechenden Verschlüsselungsschlüssel verschlüsselt wurden, zu entschlüsseln, und eine Verteilungsanordnung zum Verteilen jedes Entschlüsselungsschlüssels zu einem jeweiligen Freigabezeitpunkt aufweist; gekennzeichnet dadurch, dass der Prozessor angeordnet ist, um jeden Entschlüsselungsschlüssel unter Verwendung sowohl der privaten Daten als auch eines aktuellen Zeitwerts, angezeigt durch die Quelle von Zeitsignalen, zu erzeugen, wobei jeder erzeugte Entschlüsselungsschlüssel geeignet ist, verschlüsselte Daten unter Verwendung sowohl von öffentlichen Daten, die unter Verwendung der privaten Daten abgeleitet wurden, als auch eines Verschlüsselungsschlüssels, der einen Zeitwert aufweist, der dem aktuellen Zeitwert, der bei dem Erzeugen des Entschlüsselungsschlüssels verwendet wurde, entspricht, zu entschlüsseln.

Kurze Beschreibung der Zeichnungen

[0012] Zum besseren Verständnis der vorliegenden Erfindung und zum Verständnis dessen, wie dieselbe verwirklicht werden kann, wird nun lediglich beispielhaft auf die beiliegenden Zeichnungen Bezug genommen, bei denen:

[0013] Fig. 1 ein Computersystem gemäß einem Ausführungsbeispiel der vorliegenden Erfindung veranschaulicht;

[0014] Fig. 2 eine Computervorrichtung gemäß einem Ausführungsbeispiel der vorliegenden Erfindung veranschaulicht.

Bester Modus zum Ausführen der Erfindung

[0015] Die vorliegende Erfindung wendet sich dem Problem des Steuerns eines Zugriffs auf Daten zu, wobei der Eigentümer/Urheber der relevanten Daten einen Zugriff auf die Daten bis zu einem spezifischen Zeitpunkt (der ein Jahr, Monat, einen Tag sowie Stunden und Minuten umfassen kann) beschränken möchte. Dies wird durch Verwendung eines Verschlüsselungsschlüssels erzielt, um die Daten zu verschlüsseln, wobei der Verschlüsselungsschlüssel unter Verwendung von Daten abgeleitet wird, die gleich der spezifischen Zeit sind, zu der der Eigentümer/Urheber der Daten einen Zugriff auf die Daten erlauben möchte, und wobei der entsprechende Entschlüsselungsschlüssel lediglich zu dieser spezifischen Zeit (d. h. zu der Zeit, da der Eigentümer/Urheber einen Zugriff auf die Daten ermöglichen möchte) erzeugt wird.

[0016] Fig. 1 veranschaulicht ein Computersystem **10** gemäß einem Ausführungsbeispiel der vorliegenden Erfindung. Das Computersystem **10** umfasst eine erste Computereinheit **11**, eine zweite Computereinheit **12**, eine dritte Computereinheit **13** und eine vierte Computereinheit **14**. Die drei Computereinheiten **11**, **12**, **13** sind über ein Netzwerk **15**, beispielsweise das Internet, gekoppelt, während die vierte Computereinheit **14** über eine sichere Verbindung direkt mit der dritten Computereinheit **13** gekoppelt ist.

[0017] Der ersten Computereinheit **11** ist eine

Dokumenterstellungssoftwareanwendung **16**, beispielsweise Acrobat writer, zugeordnet, der ein Software-Einfügeelement **161** zum Ermöglichen einer Verschlüsselung von durch die Anwendung erzeugten Dokumenten unter Verwendung eines kennungsbasierten Verschlüsselungs-IBE-Mechanismus umfasst, wie nachstehend beschrieben wird. Der zweiten Computereinheit **12** ist eine Dokumentenlesevorrichtungssoftwareanwendung **17**, beispielsweise Acrobat reader, zugeordnet, die ein Software-Einfügeelement **171** zum Ermöglichen einer Entschlüsselung von Dokumenten, die durch die Dokumenterstellungssoftwareanwendung **16** der ersten Computereinheit **11** unter Verwendung eines kennungsbasierten Verschlüsselungs-IBE-Mechanismus erzeugt wurden, umfasst, wie nachstehend beschrieben wird. Die dritte Computereinheit **13** fungiert als Verteilungsdienst **131** für die vierte Computereinheit **14**, wobei die vierte Computereinheit **14** als Vertrauensautorität **141** fungiert, die über den Verteilungsdienst **131** der dritten Computereinheit **13** Vertrauensautorität-Verschlüsselungsdaten **142** und -Entschlüsselungsschlüsseldaten **143** zur Verfügung stellt, wie nachstehend beschrieben wird. Wie Fachleuten einleuchten dürfte, kann der Verteilungsdienst **131** die Vertrauensautorität-Verschlüsselungsdaten **142** und die -Entschlüsselungsschlüsseldaten **143** auf vielerlei verschiedene Weise, beispielsweise über eine Website, zur Verfügung stellen.

[0018] Da die vierte Computereinheit **14** als Vertrauensautorität **141** fungiert, würde die vierte Computereinheit **14** im Idealfall in einer sicheren Umgebung arbeiten, beispielsweise in einem sicheren Gebäude oder einem sicheren Raum, und/oder sie wäre im Idealfall als verfälschungssicherer Kasten gebaut.

[0019] Wie in Fig. 2 gezeigt ist, sind in die vierte Computereinheit **14** eine Uhr **20**, ein Prozessor **21**, ein Speicher **22** zum Speichern der Verschlüsselungsdaten **142** der Vertrauensautorität und Algorithmen zur Erzeugung von Entschlüsselungsschlüsseln auf der Basis von IBE sowie eine Anwendungsprogrammschnittstelle **23** API integriert, um zu ermöglichen, dass die vierte Computereinheit **14** eine Schnittstelle mit der dritten Computereinheit **13** bildet. Bei diesem Ausführungsbeispiel umfassen die Verschlüsselungsdaten **142** der Vertrauensautorität unter Verwendung eines QR-IBE-Verschlüsselungs-/-Entschlüsselungsmechanismus:

– eine Hash-Funktions-Nr., die, wenn sie auf eine Zeichenfolge angewendet wird, einen Wert im Bereich 0 bis N – 1 zurückgibt, und

– einen Wert N, der ein Produkt zweier Zufallsprimzahlen p und q ist, wobei die Werte von p und q lediglich der Vertrauensautorität **141** bekannt sind; die Werte von p und q sollten im Idealfall im Bereich von 2^{511} und 2^{512} liegen und sollten beide die Gleichung p, q = 3mod4 erfüllen (jedoch müssen p und q nicht denselben Wert aufweisen).

[0020] Ein Prozess zum Ermöglichen einer Verschlüsselung von Daten unter Verwendung eines Verschlüsselungsschlüssels, der mit einem Datensatz, der eine Zeit darstellt, erzeugt wird, und einer Entschlüsselung der Daten unter Verwendung eines Entschlüsselungsschlüssels, der im Wesentlichen zur selben Zeit erzeugt wird wie zu der durch einen Datensatz dargestellten Zeit, wird nun beschrieben. In dem vorliegenden Kontext kann „Zeit" ein Tageszeitwert und/oder ein Kalenderdatum oder ein beliebiges anderes Zeitmaß sein.

[0021] Ein Benutzer der ersten Computereinheit **11** erstellt ein Dokument unter Verwendung der Dokumenterstellungssoftwareanwendung **16**. Wenn der Benutzer den Zugriff der beabsichtigten Empfänger auf das Dokument bis zu einer festgelegten Zeit (beispielsweise bis zu einer spezifischen Stunde eines gegebenen Tages, Monats und Jahres) beschränken möchte, gibt der Benutzer diese spezifische Zeit in die Dokumenterstellungssoftwareanwendung **16** ein, dies könnte beispielsweise dadurch erzielt werden, dass die Anwendung **16** dahin gehend angeordnet ist, sich bei dem Benutzer mit einer Anfrage bezüglich dessen zu melden, wann die Informationen dem Empfänger zur Verfügung gestellt werden sollten.

[0022] Unter Verwendung der seitens des Benutzers eingegebenen Zeitinformationen verschlüsselt das Software-Einfügeelement unter Verwendung des IBE-Mechanismus das Dokument unter Verwendung der Zeitinformationen oder üblicherweise einer digitalen Darstellung der Zeitinformationen als Verschlüsselungsschlüssel.

[0023] Beispielsweise unter Verwendung der QR-IBE-Verschlüsselungs-/-Entschlüsselungstechnik, um jedes Bit m des Dokuments des Benutzers zu verschlüsseln, erzeugt das Software-Einfügeelement **161** Zufallszahlen t_+ (wobei t_+ eine Ganzzahl im Bereich $[0, 2^N)$ ist), bis das Software-Einfügeelement **161** einen Wert von t_+ findet, der die Gleichung Jacobi $(t_+, N) = m$ erfüllt, wobei m einen Wert von –1 oder 1 aufweist, je nachdem, ob das entsprechende Bit des Dokuments des Benutzers 0 bzw. 1 ist. (Wie hinreichend bekannt ist, ist die Jacobi-Funktion derart, dass, wenn x^2 #modN, das Jacobi (#, N) = –1, falls x nicht vorhanden ist, und = 1, falls x vorhanden ist). Das Software-Einfügeelement **161** berechnet dann den Wert:

$$s_+ = (t_+ + \#(\text{encryptionkeystring})/t_+)\text{modN}$$

für jedes Bit m, wobei s_+ dem verschlüsselten Bit von m entspricht.

[0024] Da #(encryptionkeystring – Verschlüsselungsschlüssel-Zeichenfolge) nicht-quadratisch sein kann, erzeugt das Software-Einfügeelement **161** zu-

sätzlich weitere Zufallszahlen t_ (Ganzzahlen im Bereich [0, 2^N)), bis das Software-Einfügeelement **161** eine findet, die die Gleichung Jacobi(t_ , N) = m erfüllt. Das Software-Einfügeelement **161** berechnet dann den Wert:

$s_ \equiv (t_ - \#(encryptionkeystring)/t_) mod N$

für jedes Bit m.

[0025] Die Dokumenterstellungsanwendung **16** erhält die Vertrauensautoritäten-Verschlüsselungsdaten **142** anhand beliebiger geeigneter Mittel, beispielsweise könnten die Verschlüsselungsdaten in dem Software-Einfügeelement **161** vorabgeladen werden oder könnten über das Netzwerk **15** von dem Verteilungsdienst **131** heruntergeladen werden.

[0026] Das Zeitinformationsformat, das verwendet wird, um den Verschlüsselungsschlüssel zu erzeugen, wird üblicherweise durch die Vertrauensautorität **141** bestimmt, die den zugeordneten Entschlüsselungsschlüssel liefert, und wird üblicherweise standardisiert, beispielsweise westeuropäische Zeit (GMT – Greenwich Mean Time) oder UTC (Universal Time Co-ordinates, Standardweltzeit).

[0027] Nachdem sie verschlüsselt wurden, werden die verschlüsselten Daten (das heißt die Werte s_+ und s_ für jedes Bit m der Daten des Benutzers) dem beabsichtigten Empfänger über die zweite Computereinheit **17** anhand beliebiger geeigneter Mittel, beispielsweise über E-Mail oder durch ein Platzieren in einen elektronischen öffentlichen Bereich, zur Verfügung gestellt. Die Identität der Vertrauensautorität **141** und des Verschlüsselungsschlüssels (d. h. der benannte Zeitraum ab der Zeit, zu der der beabsichtigte Empfänger auf das Dokument zugreifen kann) können dem Empfänger ebenfalls bereitgestellt werden, falls der beabsichtigte Empfänger nicht bereits Zugriff auf diese Informationen hat.

[0028] Um die Daten zu entschlüsseln, muss das Dokumentenlesevorrichtungssoftwareanwendungs-Einfügeelement **171** von dem Verteilungsdienst **131** einen Entschlüsselungsschlüssel erhalten, der dem Verschlüsselungsschlüssel entspricht, wie nachstehend beschrieben wird, wobei der Entschlüsselungsschlüssel erst zu der entsprechenden Zeit erzeugt wird (d. h. im Wesentlichen zur selben Zeit wie die Zeit, die durch den Datensatz dargestellt wird, der zum Erzeugen des Verschlüsselungsschlüssels verwendet wird).

[0029] Die vierte Computereinheit **14** erzeugt unter Verwendung von Informationen bezüglich der Uhr **20** Entschlüsselungsschlüssel in bestimmten (vorzugsweise regelmäßigen) Zeitabständen. Es können beliebige Zeitabstände zur Erzeugung zugeordneter Entschlüsselungsschlüssel verwendet werden, je nach den Gegebenheiten könnten dies somit beispielsweise Sekunden, Minuten oder ein Tag sein. Demgemäß würde die Uhrzeit im Idealfall Jahre, Monate, Tage, Stunden und Minuten umfassen. Die erste Computereinheit **11** wählt den für ihren Verschlüsselungsschlüssel verwendeten Zeitwert so aus, dass er ein Wert ist, der einer Zeit entspricht, für die die Computereinheit einen Entschlüsselungsschlüssel erzeugt.

[0030] Wenn die Vertrauensautorität **141** beispielsweise dahin gehend angeordnet ist, jede Stunde zur vollen Stunde einen Entschlüsselungsschlüssel zu liefern, so berechnet der Prozessor **21** dann, wenn die Uhr **20** dem Prozessor **21** anzeigt, dass seit der Erzeugung des letzten Entschlüsselungsschlüssels eine Stunde verstrichen ist, unter Verwendung einer „encryptionkeystring" (Verschlüsselungsschlüssel-Zeichenfolge) einen Entschlüsselungsschlüssel, der der aktuellen Stundenzeit entspricht. Der resultierende Entschlüsselungsschlüssel eignet sich dafür, Daten, die unter Verwendung desselben „encryptionkeystring"-Wertes verschlüsselt wurden, zu entschlüsseln. Somit wird der Entschlüsselungsschlüssel, der dem durch die erste Computereinheit verwendeten Verschlüsselungsschlüssel entspricht, erst zu der bestimmten Zeit erzeugt, die durch die erste Computereinheit als Zeitpunkt einer Autorisierung eines Zugriffs auf die verschlüsselten Daten ausgewählt wurde. Falls Daten unter Verwendung eines Verschlüsselungsschlüssels verschlüsselt wurden, der beispielsweise 14.00 Uhr WEZ zu einem gegebenen Tag, Monat und Jahr entspricht, so berechnet der Prozessor **21** um 14.00 Uhr WEZ zu diesem spezifischen Tag, Monat und Jahr auf eine Angabe dessen seitens der Uhr **20** einen Entschlüsselungsschlüssel, der dem Verschlüsselungsschlüssel zugeordnet ist.

[0031] Der zugeordnete Entschlüsselungsschlüssel B wird durch die Vertrauensautorität **141** wie folgt bestimmt:

$B^2 \equiv \#(encryptionkeystring) mod N$ („positive" Lösung)

[0032] Falls ein Wert von B nicht existiert, dann gibt es einen Wert von B, der durch die Gleichung:

$B^2 \equiv -\#(encryptionkeystring) mod N$ („negative" Lösung)

erfüllt wird.

[0033] Da N ein Produkt von zwei Primzahlen p, q ist, wäre es äußerst schwierig, den Entschlüsselungsschlüssel B lediglich unter Kenntnis der Verschlüsselungsschlüssel-Zeichenfolge und von N zu berechnen. Da jedoch die Vertrauensautorität **141** von p und q (d. h. zwei Primzahlen) Kenntnis hat, ist es für die Vertrauensautorität **141** relativ unkompliziert, B zu berechnen.

[0034] Auf eine Berechnung des Entschlüsselungsschlüssels hin liefert die vierte Computereinheit **14** den Entschlüsselungsschlüssel an den Verteilungsdienst **131** (vorzugsweise zusammen mit einer Angabe, ob dies die „positive" oder „negative" Lösung für B ist), wodurch sie den Entschlüsselungsschlüssel dem Empfänger der verschlüsselten Daten zur Verfügung stellt und ermöglicht, dass der Empfänger die verschlüsselten Daten entschlüsselt.

[0035] Der Verteilungsdienst **131** kann den Entschlüsselungsschlüssel anhand beliebiger geeigneter Mittel, beispielsweise über eine Website oder in Verbindung mit Sendezeitinformationen über ein nationales oder globales Zeitverteilungssystem verteilt, zur Verfügung stellen. Der Verteilungsdienst **131** ist dahin gehend angeordnet, den Verschlüsselungsschlüssel zur Verwendung durch den Empfänger zur Verfügung zu stellen (d. h. zu veröffentlichen), wobei der Empfänger beispielsweise einer Gruppe von Menschen innerhalb eines Unternehmens oder global jedem Einzelnen entsprechen kann.

[0036] Falls der Verteilungsdienst **131** die Entschlüsselungsschlüssel über eine Website zur Verfügung stellt, könnte der Verteilungsdienst **131** (nicht gezeigte) Lastausgleichsmaschinen umfassen, um die Website-Zugriffslast zu verteilen.

[0037] Außerdem könnte der Verteilungsdienst **131** auch eine Datenbank von zuvor verfügbaren Entschlüsselungsschlüsseln unterhalten, wodurch es einem Empfänger von verschlüsselten Daten ermöglicht wird, einen entsprechenden Entschlüsselungsschlüssel für eine gewisse Zeit nach der dargestellten Zeit zu erhalten, die zum Erzeugen des Verschlüsselungsschlüssels verwendet wird.

[0038] Falls die Quadratwurzel des Verschlüsselungsschlüssels einen positiven Wert zurückgibt, können die Benutzerdaten M unter Verwendung von

$$m = \text{Jacobi}(s_+ + 2B, N)$$

wiederhergestellt werden.

[0039] Falls die Quadratwurzel des Verschlüsselungsschlüssels einen negativen Wert zurückgibt, können die Benutzerdaten M unter Verwendung von

$$m = \text{Jacobi}(s\_ + 2B, N)$$

wiederhergestellt werden.

[0040] Der Empfänger kann wählen, den Entschlüsselungsschlüssel in einem Cache zu speichern, um das Dokument zu einem späteren Zeitpunkt zu entschlüsseln.

[0041] Wie oben angegeben wurde, verwendet das obige Ausführungsbeispiel den QR-IBE-Verschlüsselungs-/-Entschlüsselungsmechanismus, jedoch könnten andere Formen von IBE verwendet werden, beispielsweise diejenigen, die auf Weil- oder Tate-Paarungen beruhen.

[0042] Obwohl das obige Ausführungsbeispiel die Steuerung eines Zugriffs auf ein Dokument beschreibt, könnte das obige Ausführungsbeispiel gleichermaßen auf andere Datenformen angewendet werden.

[0043] Außerdem könnte die vierte Computereinheit **14** dahin gehend konfiguriert sein, es einer autorisierten Einzelperson zu ermöglichen, die vierte Computereinheit **14** dahin gehend umzukonfigurieren, die Erzeugung von zuvor erstellten Entschlüsselungsschlüsseln zu ermöglichen, beispielsweise falls die Verteilungsdienst-Datenbank zerstört wurde.

[0044] Die seitens der Vertrauensautorität verwendete Zeitquelle muss nicht eine Uhr der Computereinheit **14** sein, sondern könnte Zeitsignale sein, die von einer anderen Quelle empfangen werden, obwohl in diesem Fall vorzugsweise entsprechende Maßnahmen getroffen werden, um zu gewährleisten, dass die Zeitsignale sicher sind.

Patentansprüche

1. Ein Sicherheitsverfahren, das folgende Schritte aufweist:
erste Operationen, ausgeführt durch eine Offenbarungseinrichtung (**11**) von Daten, die ein Verschlüsseln der Daten und ein Liefernder verschlüsselten Daten an einen Empfänger (**12**) aufweisen, wobei der Verschlüsselungsprozess sowohl einen Verschlüsselungsschlüssel als auch öffentliche Daten (**142**), die durch eine vertrauenswürdige Partei (**141**) geliefert und unter Verwendung von privaten Daten (**143**) von derselben abgeleitet werden, verwendet; und
zweite Operationen, ausgeführt durch die vertrauenswürdige Partei (**141**), die ein Verwenden sowohl der privaten Daten als auch weiterer Daten, um einen Entschlüsselungsschlüssel, der anschließend ausgegeben wird, zu bestimmen, aufweisen;
gekennzeichnet dadurch, dass der durch die Datenoffenbarungseinrichtung (**11**) verwendete Verschlüsselungsschlüssel einen Zeitwert aufweist, und dass der Entschlüsselungsschlüssel durch die vertrauenswürdige Partei (**141**) periodisch mit den weiteren Daten, die, bei jeder Bestimmung, einen neuen aktuellen Zeitwert, der unabhängig von dem Verschlüsselungsschlüssel abgeleitet wird, aufweisen, bestimmt wird, wobei der Entschlüsselungsschlüssel so bestimmt wird, dass, für den aktuellen Zeitwert, der dem durch die Datenoffenbarungseinrichtung für ihren Verschlüsselungsschlüssel verwendeten Zeitwert gleicht, der Entschlüsselungsschlüssel geeignet ist, die verschlüsselten Daten der Offenbarungseinrich-

tung zu entschlüsseln.

2. Ein Verfahren gemäß Anspruch 1, bei dem die vertrauenswürdige Partei (**141**) den aktuellen Zeitwert von einer der vertrauenswürdigen Partei zugeordneten Echtzeituhr (**20**) ableitet.

3. Ein Verfahren gemäß Anspruch 1 oder 2, bei dem der Entschlüsselungsschlüssel in regelmäßigen Zeitabständen bestimmt wird.

4. Ein Verfahren gemäß einem der vorhergehenden Ansprüche, bei dem der aktuelle Zeitwert einem Datum entspricht.

5. Ein Verfahren gemäß einem der vorhergehenden Ansprüche, bei dem der als der Verschlüsselungsschlüssel verwendete Zeitwert aus Zeitwerten, von denen bekannt ist, dass sie als aktuelle Zeitwerte bei einem Bestimmen des Entschlüsselungsschlüssels verwendet werden, ausgewählt wird.

6. Ein Verfahren gemäß einem der vorhergehenden Ansprüche, bei dem die ersten und zweiten Operationen kennungsbasierte kryptographische Prozesse sind, die quadratische Residuosität nutzen.

7. Ein Verfahren gemäß einem der Ansprüche 1 bis 5, bei dem die ersten und zweiten Operationen kennungsbasierte kryptographische Prozesse sind, die Weil- oder Tate-Paarungen nutzen.

8. Ein Computersystem, das eine erste Recheneinheit (**11**) aufweist, die angeordnet ist, um, zur Ausgabe, erste Daten gemäß einem Verschlüsselungsprozess, in den sowohl ein Verschlüsselungsschlüssel als auch zweite, öffentliche Daten (**142**), bereitgestellt durch eine vertrauenswürdige Partei (**141**), eingebunden sind, zu verschlüsseln; eine zweite Recheneinheit (**14**), die der vertrauenswürdigen Partei (**141**) zugeordnet ist und angeordnet ist, um, zur Ausgabe, unter Verwendung sowohl von dritten Daten als auch vierten, privaten, Daten, von denen die zweiten Daten abgeleitet wurden, einen Entschlüsselungsschlüssel zu bestimmen; und eine dritte Recheneinheit (**12**), die angeordnet ist, um sowohl die verschlüsselten ersten Daten als auch den Entschlüsselungsschlüssel zu empfangen und die empfangenen verschlüsselten ersten Daten unter Verwendung des empfangenen Entschlüsselungsschlüssels zu entschlüsseln; gekennzeichnet dadurch, dass die erste Recheneinheit (**11**) angeordnet ist, um einen Zeitwert als den Verschlüsselungsschlüssel zu verwenden, und dass die zweite Recheneinheit angeordnet ist, um den Entschlüsselungsschlüssel periodisch zu bestimmen, wobei als die dritten Daten, bei jeder Bestimmung, ein neuer aktueller Zeitwert, der unabhängig von dem Verschlüsselungsschlüssel abgeleitet wird, verwendet wird, wobei der Entschlüsselungsschlüssel so durch die zweite Recheneinheit (**14**) bestimmt wird, dass, für den aktuellen Zeitwert, der dem durch die erste Recheneinheit (**11**) für ihren Verschlüsselungsschlüssel verwendeten Zeitwert gleicht, der Entschlüsselungsschlüssel geeignet ist, die verschlüsselten ersten Daten zu entschlüsseln.

9. Ein Computersystem gemäß Anspruch 8, bei dem die zweite Recheneinheit (**14**) verfälschungssicher ist.

10. Ein Computersystem gemäß Anspruch 8 oder Anspruch 9, bei dem die zweite Recheneinheit (**14**) eine Echtzeituhr (**20**) umfasst, aus der die aktuellen Zeitwerte erzeugt werden.

11. Ein Computersystem gemäß einem der Ansprüche 8 bis 10, bei dem der aktuelle Zeitwert einem Datum entspricht.

12. Ein Computersystem gemäß einem der Ansprüche 8 bis 11, das ferner ein Verteilungsteilsystem zum Verteilen des Entschlüsselungsschlüssels aufweist.

13. Ein Computersystem gemäß einem der Ansprüche 8 bis 12, bei dem die zweite Recheneinheit (**14**) angeordnet ist, um den Entschlüsselungsschlüssel in regelmäßigen Zeitabständen zu bestimmen.

14. Ein Computersystem gemäß einem der Ansprüche 8 bis 13, bei dem die erste Recheneinheit (**11**) angeordnet ist, um, als die zweiten Daten, einen Zeitwert auszuwählen, von dem sie weiß, dass er einer ist, den die zweite Recheneinheit als den aktuellen Zeitwert zum Bestimmen des Entschlüsselungsschlüssels verwenden wird.

15. Ein Computersystem gemäß einem der Ansprüche 8 bis 14, bei dem der Verschlüsselungsprozess, der durch die erste Recheneinheit (**11**) ausgeführt wird, der Bestimmungsprozess für den Entschlüsselungsschlüssel, der durch die zweite Recheneinheit (**14**) ausgeführt wird, und der Prozess zum Entschlüsseln der verschlüsselten Daten, der durch die dritte Recheneinheit (**12**) ausgeführt wird, kennungsbasierte kryptographische Prozesse, die eine quadratische Residuosität nützen, sind.

16. Ein Computersystem gemäß einem der Ansprüche 8 bis 14, bei dem der Verschlüsselungsprozess, der durch die erste Recheneinheit (**11**) ausgeführt wird, der Bestimmungsprozess für den Entschlüsselungsschlüssel, der durch die zweite Recheneinheit (**14**) ausgeführt wird, und der Prozess zum Entschlüsseln der verschlüsselten Daten, der durch die dritte Recheneinheit (**12**) ausgeführt wird, kennungsbasierte kryptographische Prozesse, die Weil- oder Tate-Paarungen nutzen, sind.

17. Eine Vorrichtung (**13**, **14**) zum Erzeugen ei-

nes Entschlüsselungsschlüssels, die einen Speicher (**22**) zum Halten von privaten Daten (**143**), eine Quelle von Zeitsignalen (**20**), einen Prozessor (**21**) zum Verwenden der privaten Daten, um, periodisch, Entschlüsselungsschlüssel zu erzeugen, die jeweils angepasst sind, um Daten, die mit einem jeweiligen entsprechenden Verschlüsselungsschlüssel verschlüsselt wurden, zu entschlüsseln, und eine Verteilungsanordnung (**131**) zum Verteilen jedes Entschlüsselungsschlüssels zu einem jeweiligen Freigabezeitpunkt aufweist; gekennzeichnet dadurch, dass der Prozessor (**21**) angeordnet ist, um jeden Entschlüsselungsschlüssel unter Verwendung sowohl der privaten Daten als auch eines aktuellen Zeitwerts, angezeigt durch die Quelle von Zeitsignalen (**20**), zu erzeugen, wobei jeder erzeugte Entschlüsselungsschlüssel geeignet ist, verschlüsselte Daten unter Verwendung sowohl von öffentlichen Daten, die unter Verwendung der privaten Daten abgeleitet wurden, als auch eines Verschlüsselungsschlüssels, der einen Zeitwert aufweist, der dem aktuellen Zeitwert, der bei dem Erzeugen des Entschlüsselungsschlüssels verwendet wurde, entspricht, zu entschlüsseln.

18. Eine Vorrichtung gemäß Anspruch 17, bei der der aktuelle Zeitwert einem Datum entspricht.

19. Vorrichtung gemäß Anspruch 17 oder Anspruch 18, bei der der Entschlüsselungsschlüssel durch einen kennungsbasierten kryptographischen Prozess, der eine quadratische Residuosität nutzt, erzeugt wird.

20. Vorrichtung gemäß Anspruch 17 oder Anspruch 18, bei der der Entschlüsselungsschlüssel durch einen kennungsbasierten kryptographischen Prozess, der Weil- oder Tate-Paarungen nutzt, erzeugt wird.

Es folgen 2 Blatt Zeichnungen

Anhängende Zeichnungen

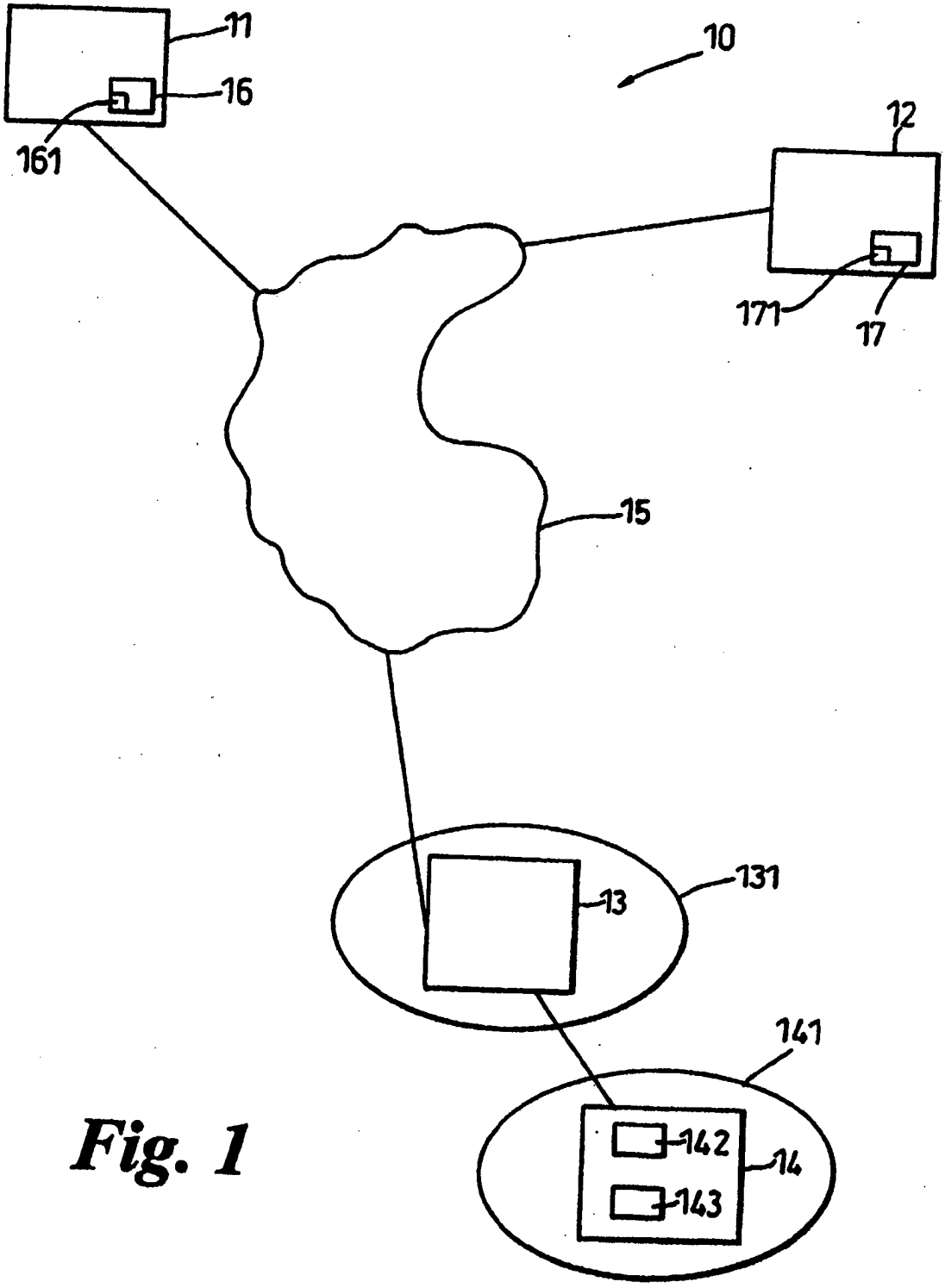

Fig. 1

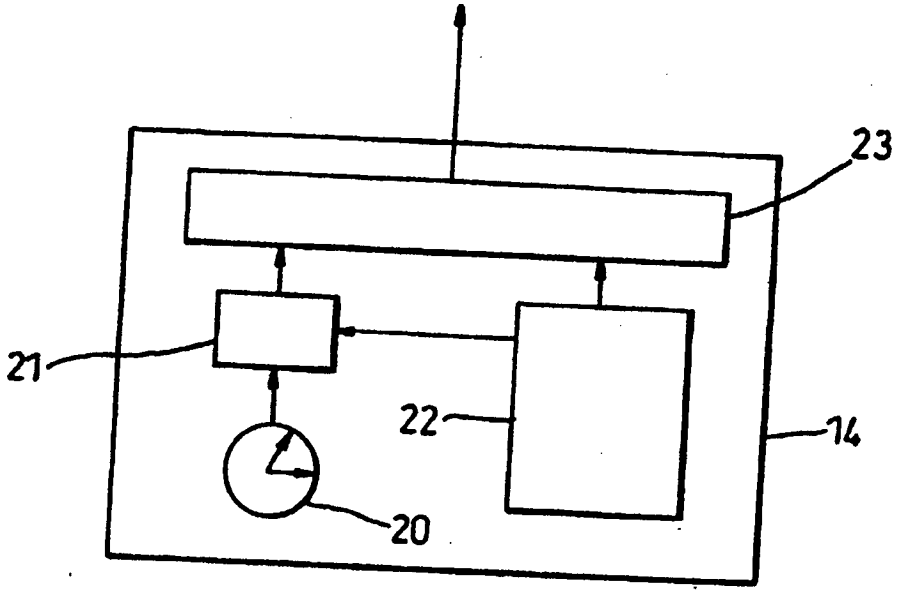

Fig. 2