

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES
PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro



(43) Internationales Veröffentlichungsdatum
23. September 2010 (23.09.2010)

(10) Internationale Veröffentlichungsnummer
WO 2010/105912 A1

- (51) Internationale Patentklassifikation:
G06F 21/00 (2006.01)
- (21) Internationales Aktenzeichen: PCT/EP2010/052733
- (22) Internationales Anmeldedatum:
4. März 2010 (04.03.2010)
- (25) Einreichungssprache: Deutsch
- (26) Veröffentlichungssprache: Deutsch
- (30) Angaben zur Priorität:
10 2009 001 719.4 20. März 2009 (20.03.2009) DE
- (71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme von US): **COMPUGROUP HOLDING AG** [DE/DE]; Maria Trost 21, 56070 Koblenz (DE).
- (72) Erfinder; und
- (75) Erfinder/Anmelder (nur für US): **SPALKA, Adrian** [DE/DE]; Moltkestr. 16, 56068 Koblenz (DE). **LENHARDT, Jan** [DE/DE]; Kurfürstenstr. 19a, 56068 Koblenz (DE).
- (74) Anwalt: **RICHARDT, Markus**; Wilhelmstraße 7, 65185 Wiesbaden (DE).

- (81) Bestimmungsstaaten (soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) Bestimmungsstaaten (soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— mit internationalem Recherchenbericht (Artikel 21 Absatz 3)

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD FOR CREATING ASYMMETRICAL CRYPTOGRAPHIC KEY PAIRS

(54) Bezeichnung : VERFAHREN ZUR ERZEUGUNG VON ASYMMETRISCHEN KRYPTOGRAFISCHEN SCHLÜSSEL-PAAREN

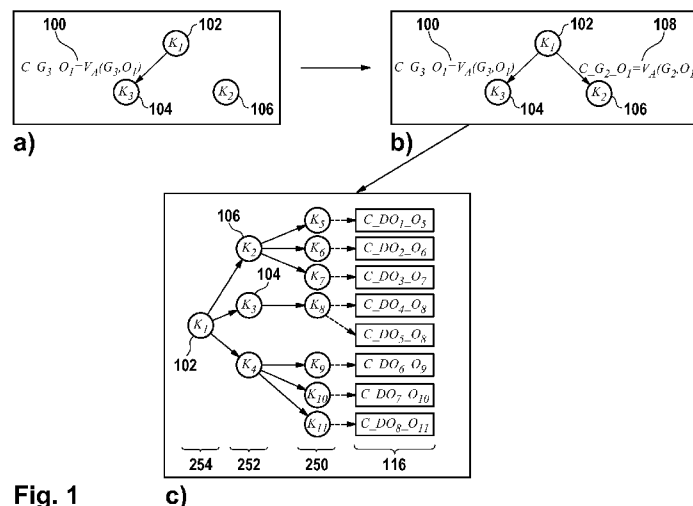


Fig. 1

(57) Abstract: The invention relates to a method for creating a set of asymmetrical cryptographic key pairs, wherein the set of key pairs has a first key pair (K1) and a second key pair (K2), wherein the first key pair is formed by a first private (G1) and a first public key (O1) and the second key pair is formed by a second private (G2) and a second public key (O2), wherein a first cipher (C_G2_O1) is allocated to the first and second key pair, wherein the first cipher is formed by an encryption of the second private key (G2) with the first public key (O1), having the following steps: adding a third asymmetrical cryptographic key pair (K3) to the set of key pairs, wherein the third key pair is formed by a third private (G3) and a third public key (O3); creating a second cipher (C_G3_O1) by encrypting the third private key (G3) with the first public key (O1); storing the second cipher (212; 186), wherein the set of key pairs has a directed graph structure.

(57) Zusammenfassung:

[Fortsetzung auf der nächsten Seite]



Die Erfindung betrifft ein Verfahren zur Erzeugung eines Satzes von asymmetrischen kryptografischen Schlüsselpaaren, wobei der Satz von Schlüsselpaaren ein erstes Schlüsselpaar (K1) und ein zweites Schlüsselpaar (K2) aufweist, wobei das erste Schlüsselpaar durch einen ersten privaten (G1) und einen ersten öffentlichen Schlüssel (O1) gebildet wird und das zweite Schlüsselpaar durch einen zweiten privaten (G2) und einen zweiten öffentlichen Schlüssel (O2) gebildet wird, wobei dem ersten und zweiten Schlüsselpaar ein erstes Chifftrat (C_G2_O1) zugeordnet ist, wobei das erste Chifftrat durch eine Verschlüsselung des zweiten privaten Schlüssels (G2) mit dem ersten öffentlichen Schlüssel (O1) gebildet wird, mit den folgenden Schritten: Hinzufügen eines dritten asymmetrischen kryptografischen Schlüsselpaars (K3) zu dem Satz von Schlüsselpaaren, wobei das dritte Schlüsselpaar durch einen dritten privaten (G3) und einen dritten öffentlichen Schlüssel (O3) gebildet wird, Erzeugung eines zweiten Chifftrats (C_G3_O1) durch Verschlüsselung des dritten privaten Schlüssels (G3) mit dem ersten öffentlichen Schlüssel (O1), Speicherung des zweiten Chifftrats (212; 186), wobei der Satz von Schlüsselpaaren eine gerichtete Graphstruktur aufweist.

Verfahren zur Erzeugung von asymmetrischen kryptografischen Schlüsselpaaren

5

B e s c h r e i b u n g

Die Erfindung betrifft ein Verfahren zur Erzeugung eines Satzes von asymmetrischen kryptografischen Schlüsselpaaren, ein Datenverarbeitungssystem zur Erzeugung eines Satzes von asymmetrischen kryptografischen Schlüsselpaaren, ein entsprechendes
10 Computerprogrammprodukt sowie ein Verfahren zur Bereitstellung von Chiffraten, ein Datenverarbeitungssystem zur Bereitstellung von Chiffraten und ein entsprechendes Computerprogrammprodukt.

Chipkarten werden heutzutage in vielfältiger Form zur Ver- und Entschlüsselung von
15 Daten eingesetzt. Ein Anwendungsgebiet für Chipkarten ist die sogenannte elektronische Gesundheitskarte, welche in Zukunft die Krankenversicherungskarte in Deutschland ersetzen soll. Ziel ist es dabei, eine Datenübermittlung zwischen medizinischen Leistungserbringern, Krankenkassen, Apotheken und Patienten in Zukunft kostengünstiger zu gestalten, zu vereinfachen und zu beschleunigen. Dazu
20 gehört auch u.a. die Ermöglichung eines Zugriffs auf einen elektronischen Arztbrief, eine elektronische Krankenakte sowie ein elektronisches Rezept mit Hilfe der elektronischen Gesundheitskarte.

Somit können medizinische Datenobjekte (MDOs) wie ein elektronischer Arztbrief, eine
25 elektronische Krankenakte oder ein elektronisches Rezept verschlüsselt und digital signiert auf einem zentralen Server gespeichert werden. Eine Verschlüsselung erfolgt dabei vorzugsweise über einen symmetrischen Schlüssel, der für jedes neue medizinische Datenobjekt einer elektronischen Krankenakte, wie z.B. einen elektronischen Arztbrief oder ein elektronisches Rezept, individuell zufällig erzeugt wird.
30 Der symmetrische Schlüssel selbst wird nach seiner Erstellung beispielsweise mit einem öffentlichen Schlüssel verschlüsselt und zusammen mit den verschlüsselten medizinischen Datenobjekten auf dem zentralen Server abgelegt. Dieser zur Verschlüsselung verwendete öffentliche Schlüssel bildet zusammen mit einem privaten Schlüssel, welcher auf der elektronischen Gesundheitskarte abgespeichert ist, ein
35 kryptografisches, asymmetrisches Schlüsselpaar. Damit ist gewährleistet, dass ausschließlich unter Verwendung des geheimen Gesundheitskartenschlüssels ein

Zugriff auf die verschlüsselten medizinischen Datenobjekte möglich ist. Bei einem solchen Zugriff erfolgt zunächst eine Entschlüsselung des verschlüsselten symmetrischen Schlüssels mittels des geheimen Gesundheitskartenschlüssels, woraufhin dann mit dem entschlüsselten symmetrischen Schlüssel eine weitere

5 Entschlüsselung der medizinischen Datenobjekte möglich ist. Wurde bei der Erstellung eines MDOs auch eine digitale Signatur mit dem geheimen Gesundheitskartenschlüssel erzeugt, so kann anschließend die Integrität des MDOs und die Authentizität des MDO-Erzeugers über die digitale Signatur verifiziert werden.

10 Aus dem Stand der Technik sind verschiedene Systeme zur Erzeugung und Verwaltung von kryptografischen Schlüsseln bekannt. Beispielsweise offenbart die WO 2008/026184 A2 ein hierarchisches Key-Management-System für den Zugriff auf verschlüsselte Daten. Die US 10/2008/0022361 beschreibt eine hierarchische Rechteverwaltung für ein Computer-Dateisystem. Die DE 101 34 489 B4 offenbart ein

15 asymmetrisches Kryptografieverfahren zur Wiedergewinnung eines geheimen Schlüssels.

US 20050238175 A1 beschreibt eine Methode zum schnellen Löschen von verschlüsselt abgelegten Daten durch das Löschen des Schlüssels, der zur

20 Verschlüsselung der Daten verwendet wurde. Der Schlüssel kann durch einen weiteren Schlüssel, welcher innerhalb einer Verschlüsselungshierarchie einen übergeordneten Platz einnimmt, verschlüsselt sein, welcher wiederum durch einen hierarchisch übergeordneten Schlüssel verschlüsselt sein kann. Anstatt wie in vorbekannten Verfahren die Verweise auf die Daten zu löschen oder sensible Daten durch

25 mehrfaches Überschreiben anderer Daten endgültig zu löschen (Nachteil: hoher Zeitaufwand), werden gemäß 20050238175 A1 alle Daten, die in der Verschlüsselungshierarchie von einem bestimmten Schlüssel hierarchisch untergeordnet sind durch das Löschen dieses Schlüssels schnell und unwiederbringlich gelöscht. „Hierarchisch untergeordnet“ bedeutet in diesem Kontext, dass die Daten

30 entweder von dem gelöschten Schlüssel direkt verschlüsselt wurden, oder von einem der Schlüssel, die von dem gelöschten Schlüssel verschlüsselt wurden, verschlüsselt worden sind.

Um einen Verlust von kryptografischen Schlüsselpaaren entgegenzutreten, schlägt die DE 101 34 489 B4 ein asymmetrisches Kryptografieverfahren vor, welches unter Verwendung von Recovery-Zertifikaten und sogenannten Recovery-Cards vorschlägt, den geheimen Schlüssel einer Rechneinrichtung mit Schlüsseln wenigstens zweier
5 unterschiedlicher Recovery-Rechneinrichtungen zu verschlüsseln und eine entsprechende Anzahl an den verschlüsselten Schlüssel aufweisenden Revocery-Zertifikaten zu erstellen. Dies ermöglicht eine Wiedergewinnung und Nutzung des geheimen Schlüssels, ohne dass dieser außerhalb einer Smartcard im Klartext vorliegt.

10 Demgegenüber liegt der Erfindung die Aufgabe zugrunde, ein verbessertes Verfahren zur Erzeugung eines Satzes von asymmetrischen kryptografischen Schlüsselpaaren, ein Verfahren zur Bereitstellung von Chiffreten sowie entsprechende Datenverarbeitungssysteme und Computerprogrammprodukte zu schaffen.

15 Die der Erfindung zugrundeliegenden Aufgaben werden jeweils mit den Merkmalen der unabhängigen Patentansprüche gelöst. Bevorzugte Ausführungsformen der Erfindung sind in den abhängigen Patentansprüchen angegeben.

Erfindungsgemäß wird ein Verfahren zur Erzeugung eines Satzes von asymmetrischen
20 kryptografischen Schlüsselpaaren geschaffen, wobei der Satz von Schlüsselpaaren ein erstes Schlüsselpaar und ein zweites Schlüsselpaar aufweist, wobei das erste Schlüsselpaar durch einen ersten privaten und einen ersten öffentlichen Schlüssel gebildet wird und das zweite Schlüsselpaar durch einen zweiten privaten und einen zweiten öffentlichen Schlüssel gebildet wird, wobei dem ersten und zweiten
25 Schlüsselpaar ein erstes Chiffret zugeordnet ist, wobei das erste Chiffret durch eine Verschlüsselung des zweiten privaten Schlüssels mit dem ersten öffentlichen Schlüssel gebildet wird, wobei das Verfahren die Schritte umfasst:

- Hinzufügen eines dritten asymmetrischen kryptografischen Schlüsselpaars zu dem
30 Satz von Schlüsselpaaren, wobei das dritte Schlüsselpaar durch einen dritten privaten und einen dritten öffentlichen Schlüssel gebildet wird,
- Erzeugung eines zweiten Chiffrets durch Verschlüsselung des dritten privaten Schlüssels mit dem ersten öffentlichen Schlüssel,

- Speicherung des zweiten Chiffrats.

Ohne Beschränkung der Allgemeinheit wird im Folgenden davon ausgegangen, dass
 5 alle betrachteten kryptografischen Schlüsselpaare nach einem auf elliptischen Kurven
 basierenden Kryptosystem aufgebaut sind. Allerdings lässt sich das Grundprinzip auch
 auf jegliche andere Arten von Verfahren zur Erzeugung von asymmetrischen
 Schlüsseln wie RSA-Verfahren, das Rabin-Verfahren, das Elgamal-Verfahren o.Ä.
 anwenden. Weiterhin gelten die folgenden Bezeichnungen:

- 10 • $K_i = (G_i, O_i)$ mit $i = 1, 2, 3, \dots$ bezeichne ein asymmetrisches kryptografisches
 Schlüsselpaar.
- G_i bezeichne die geheime Schlüsselpaarkomponente bzw. „den geheimen
 Schlüssel“ eines asymmetrischen kryptografischen Schlüsselpaars K_i .
- O_i bezeichne die öffentliche Schlüsselpaarkomponente bzw. „den öffentlichen
 15 Schlüssel“ eines asymmetrischen kryptografischen Schlüsselpaars K_i .
- $V_A(DO, O_i)$ bezeichne eine auf einem asymmetrischen Kryptosystem basierende
 Verschlüsselungsfunktion, die auf einem Datenobjekt DO unter Verwendung
 eines öffentlichen Schlüssels O_i ausgeführt wird.
- $C_DO_O_i = V_A(DO, O_i)$ bezeichne ein „Chifftrat“ bzw. das Ergebnis der
 20 Verschlüsselungs-funktion V_A , angewendet auf das Datenobjekt DO unter
 Verwendung des öffentlichen Schlüssels O_i .
- $E_A(C_DO_O_i, G_i) = DO$ bezeichne eine auf einem asymmetrischen Kryptosystem
 basierende Entschlüsselungsfunktion, die auf einem verschlüsselten Datenobjekt
 $C_DO_O_i$ unter Verwendung eines geheimen Schlüssels G_i ausgeführt wird.
 25 Dabei gilt, dass G_i zusammen mit dem für die Verschlüsselung von $C_DO_O_i$
 verwendeten öffentlichen Schlüssel O_i ein asymmetrisches kryptografisches
 Schlüsselpaar bildet.

Den Kern der Erfindung bildet die Verknüpfung zweier asymmetrischer kryptografischer
 Schlüsselpaare K_1 und K_2 , welche nach einem beliebigen asymmetrischen

- 30 Kryptosystem aufgebaut sind. Dabei wird die Verknüpfung der beiden Schlüsselpaare
 dadurch hergestellt, dass der geheime Schlüssel G_2 des zweiten Schlüsselpaars K_2 mit

dem öffentlichen Schlüssel O_1 des ersten Schlüsselpaars K_1 verschlüsselt und das Chiffre $C_{G_2, O_1} = V_A(G_2, O_1)$ gespeichert wird. Diese Speicherung von C_{G_2, O_1} kann im selben Speicher erfolgen, in dem auch alle öffentlichen Schlüssel O_i gespeichert werden. Dieser Speicher wird im Folgenden die „Public-Key-Infrastruktur“ oder „PKI“ genannt.

Durch die Speicherung und Abrufbarkeit des Chiffres C_{G_2, O_1} wird eine Abhängigkeit zwischen den Schlüsselpaaren K_1 und K_2 hergestellt: Ein Benutzer, der im Besitz des geheimen Schlüssels G_1 ist, kann damit nicht nur alle mit dem zugehörigen öffentlichen Schlüssel O_1 verschlüsselten Datenobjekte entschlüsseln, sondern auch das Chiffre C_{G_2, O_1} , also den verschlüsselten geheimen Schlüssel G_2 des Schlüsselpaars K_2 . Mit G_2 kann der Benutzer dann auch alle mit dem öffentlichen Schlüssel O_2 des Schlüsselpaars K_2 verschlüsselten Datenobjekte entschlüsseln.

Die durch die Speicherung von C_{G_2, O_1} entstandene Abhängigkeit zwischen den beiden Schlüsselpaaren K_1 und K_2 lässt sich als gerichteter Graph darstellen, bei dem die Schlüsselpaare K_1 und K_2 als Knoten des Graphen dargestellt werden und das öffentlich gespeicherte Chiffre $C_{G_2, O_1} = V_A(G_2, O_1)$ als die gerichtete Kante von K_1 nach K_2 zwischen den beiden Knoten. Die Verbindung von K_1 nach K_2 besagt also, dass das Chiffre $C_{G_2, O_1} = V_A(G_2, O_1)$ öffentlich gespeichert ist und damit bei Besitz des geheimen Schlüssels G_1 des Schlüsselpaars K_1 der geheime Schlüssel G_2 des Schlüsselpaars K_2 ebenfalls zugänglich ist.

Ausführungsformen der Erfindung haben den Vorteil, dass durch einen geheimen Schlüssel eines einzigen Schlüsselpaars Zugriff auf die geheimen Schlüssel mehrerer Schlüsselpaare erlangt werden kann. Sind beispielsweise Daten mit dem zweiten oder dritten öffentlichen Schlüssel verschlüsselt, so genügt die Kenntnis des ersten geheimen Schlüssels, um damit eine Datenentschlüsselung unter Verwendung der ersten und zweiten Chiffre durchzuführen.

Nach einer Ausführungsform der Erfindung umfasst das Verfahren ferner die Schritte des Hinzufügens eines asymmetrischen kryptografischen Nachfolger-Schlüsselpaars zu dem Satz von Schlüsselpaaren, wobei das Nachfolger-Schlüsselpaar durch einen privaten und einen öffentlichen Nachfolger-Schlüssel gebildet wird, wobei durch ein

Schlüsselpaar aus dem Satz von Schlüsselpaaren ein Vorgänger-Schlüsselpaar gebildet wird, wobei das Vorgänger-Schlüsselpaar einen privaten und einen öffentlichen Vorgänger-Schlüssel aufweist. Das Verfahren setzt sich fort mit der Erzeugung eines dritten Chiffrats durch Verschlüsselung des privaten Schlüssels des Nachfolger-Schlüsselpaars mit dem öffentlichen Schlüssel des Vorgänger-Schlüsselpaars und der Speicherung des dritten Chiffrats.

Bei einem Vorgänger-Schlüsselpaar handelt es sich um ein beliebiges Schlüsselpaar des Satzes von Schlüsselpaaren. Bei dem Nachfolgerschlüsselpaar handelt es sich um ein beliebiges weiteres zusätzliches Schlüsselpaar, welches dem Satz von Schlüsselpaaren hinzugefügt wird, wobei hierfür eine Abhängigkeit zwischen dem Vorgänger-Schlüsselpaar und dem Nachfolgerschlüsselpaar hergestellt wird, indem ein Chiffrat erzeugt wird. Das Chiffrat wird durch Verschlüsseln des privaten Schlüssels des Nachfolger-Schlüsselpaars mit dem öffentlichen Schlüssel des Vorgängerschlüsselpaars erzeugt.

Die Entwicklung des Graphen kann also so erfolgen, dass ein neuer Knoten mit ein oder mehreren Kanten oder eine neue Kante zu bestehenden Knoten eingefügt wird.

Nach einer weiteren Ausführungsform der Erfindung weist der Satz von Schlüsselpaaren eine gerichtete Graphstruktur auf, wobei die Knoten des Graphs die Schlüsselpaare repräsentieren, wobei eine Abhängigkeit zwischen einem Vorgänger-Schlüsselpaar und einem dem Vorgänger-Schlüsselpaar im Graph unmittelbar nachfolgenden Nachfolger-Schlüsselpaar durch ein Chiffrat gebildet wird, wobei das Chiffrat durch Verschlüsselung des privaten Schlüssels des Nachfolger-Schlüsselpaars mit dem öffentlichen Schlüssel des Vorgänger-Schlüsselpaars gebildet ist, wobei bis auf das den Wurzelknoten des Graphen bildende Schlüsselpaar jedes Schlüsselpaar im Graph durch mindestens ein Chiffrat von einem anderen Schlüsselpaar abhängig ist.

Damit lassen sich in einfacher Weise logische Strukturen aufbauen, beispielsweise indem als Graph eine Baumstruktur verwendet wird, welche es ermöglicht, in hierarchischer Weise auf voneinander durch die Chifftrate abhängige Schlüsselpaare zuzugreifen. Ein Benutzer, welcher über eines der Schlüsselpaare in der Graphstruktur

verfügt, ist damit in der Lage, alle nachfolgenden Schlüsselpaare für Ver- und Entschlüsselungsvorgänge zu verwenden. Schlüsselpaare hingegen, welche sich nicht im Pfad der Graphstruktur, nachfolgend dem Schlüsselpaar, über welches ein Benutzer verfügt, befinden, liegen damit außerhalb des Zugriffsbereichs des Benutzers, womit

5 sich in einfacher Weise hierarchische Strukturen implementieren lassen: So können verschiedene Hierarchieebenen des Graphs verschiedenen Benutzergruppen zugeordnet werden, sodass sich insgesamt beispielsweise die hierarchische Struktur einer Firmenorganisation in einfacher Weise abbilden lässt. Ein Schlüsselpaar eines Wurzelknotens wird beispielsweise einem Management zugeordnet, welches damit in

10 der Lage ist, Zugriff auf sämtliche nachfolgenden Schlüsselpaare für alle Ver- und Entschlüsselungsvorgänge zu haben. Eine Hierarchieebene darunter befinden sich Schlüsselpaare, welche einzelnen Abteilungsleitern zugeordnet sind. Diesen Schlüsselpaaren untergeordnet sind wiederum Schlüsselpaare einzelner Mitarbeiter, welche lediglich auf Ver- und Entschlüsselungsvorgänge in ihrem speziellen

15 Arbeitsbereich zugreifen können sollen.

Es sei jedoch angemerkt, dass die beschriebene Graphstruktur nicht nur auf einfache Baumstrukturen beschränkt ist, sondern allgemein eine beliebige Art von Graphen, wie azyklische oder zyklische Graphen, zulässt. Allgemein können damit beliebige Arten

20 von Netzwerken abgebildet werden, über welche in komplexer Weise Schlüsselpaare im Zusammenhang stehen. Ein Anwendungsgebiet hierfür kann beispielsweise ein sicherer Datenaustausch oder in spezieller Weise eine sichere Kommunikation in sogenannten Online-Communities (Community Plattform) sein, bei welchen eine Vielzahl von Nutzern in einem Netzwerk, wie dem Internet, miteinander in Kontakt

25 stehen, um sich dort auszutauschen.

Nach einer weiteren Ausführungsform der Erfindung ist bis auf das den Wurzelknoten des Graphen bildende Schlüsselpaar jedes Schlüsselpaar im Graph durch genau ein Chiffprat von einem anderen Schlüsselpaar abhängig.

30 Nach einer weiteren Ausführungsform der Erfindung weist der Satz von Schlüsselpaaren zwei beliebige Schlüsselpaare mit je einem privaten und einen öffentlichen Schlüssel auf, wobei das Verfahren ferner die Schritte umfasst des Erzeugens eines vierten Chiffrats durch Verschlüsselung des privaten Schlüssels des

ersten Schlüsselpaars der beliebigen Schlüsselpaare mit dem öffentlichen Schlüssel des zweiten Schlüsselpaars der beliebigen Schlüsselpaare und der Speicherung des vierten Chiffrats. Eine solche Erweiterung des Satzes von Schlüsselpaaren ist damit unabhängig von der Verwendung von Vorgänger- und Nachfolger-Schlüsselpaaren und erlaubt die Verknüpfung zweier beliebiger Schlüsselpaare in einem Graph von Schlüsselpaaren.

So kann beispielsweise temporär eine Abhängigkeit zwischen zwei Schlüsselpaaren hergestellt werden, welche einen Benutzer in die Lage versetzt, beide Schlüsselpaare und deren Nachfolger für Ver- und Entschlüsselungsvorgänge, beispielsweise über einen gewissen Zeitraum hinweg, zu verwenden. Soll zu einem späteren Zeitpunkt eine weitere Verknüpfung der beiden Schlüsselpaare aufgehoben werden, so genügt es, die die beiden Schlüsselpaare verknüpfende Chifftrate für diesen entsprechenden Benutzer nicht mehr zugänglich zu machen, z.B. zu löschen.

Nach einer weiteren Ausführungsform der Erfindung werden die Chifftrate in einer vertrauenswürdigen Stelle gespeichert. Vorzugsweise werden zusammen mit den Chiffraten auch Klassifizierungsmerkmale gespeichert, wobei die Klassifizierungsmerkmale eine Gültigkeit der Chifftrate festlegen, wobei die Gültigkeit angibt, dass nach Ablauf der Gültigkeit eine Verwendung der Chifftrate für weitere Datenverarbeitungsvorgänge verhindert werden soll; insbesondere kann das betreffende Chifftrat nach Ablauf der Gültigkeit gelöscht werden. Damit ist sichergestellt, dass ein Zugriff auf die Chifftrate kontrolliert werden kann.

Klassifizierungsmerkmale bezüglich der Gültigkeit von Schlüsselpaaren innerhalb von Informationssystemsitzungen können sein:

- Gültigkeit nach Zeitintervall: Es wird serverseitig im Informationssystem gespeichert, innerhalb welches Zeitintervalls ein Schlüsselpaar gültig ist. Wenn ein Benutzer versucht, ein „abgelaufenes“ Schlüsselpaar K_i zu benutzen (d.h., der Benutzer eröffnet eine Sitzung beim Informationssystem, bei der er sich mit dem Schlüsselpaar K_i authentisiert), verweigert das Informationssystem ihm dies.

- Gültigkeit nach Anzahl der Benutzungen: Es wird serverseitig im Informationssystem gespeichert, wie oft ein Schlüsselpaar maximal benutzt werden kann und wie oft es bereits benutzt wurde (d.h. wie oft eine Sitzung unter Verwendung des Schlüsselpaars bei der Authentisierung eröffnet wurde). Wenn
5 die Anzahl der bereits erfolgten Benutzungen eines Schlüsselpaars K_i dessen Maximalanzahl erreicht hat, verweigert das Informationssystem eine erneute Benutzung von K_i .
- Gültigkeit nach Art der Benutzung: Es wird serverseitig im Informationssystem für jedes Schlüsselpaar gespeichert, welche Operationen in einer Sitzung zulässig
10 sind, die unter Verwendung des Schlüsselpaars bei der Authentisierung eröffnet wurde. Wenn der Benutzer eine Operation durchzuführen versucht, die für die gerade bestehende Sitzung nicht zulässig ist, verweigert das Informationssystem dies.

- 15 Ausgehend davon lassen sich nun vielfältige weitere Nutzungsszenarien konstruieren, die ebenfalls lediglich diese Merkmale variieren.

Als Beispiel sei eine elektronische Patientenakte genannt, bei der ein Benutzer (ein Patient) einem anderen Benutzer (ein Arzt) ein Zugriffsrecht auf seine eigene Akte
20 erteilt, jedoch lediglich für maximal fünf Zugriffe auf die Akte und in einem Zeitfenster von nur einem Monat; darüber hinaus darf der Arzt auch ausschließlich lesend auf die Akte des Patienten zugreifen. Der Patient erzeugt also ein neues Schlüsselpaar K_P , bei dem der geheime Schlüssel G_θ des Schlüsselpaars des Patienten mit dem öffentlichen Schlüssel O_P des Arztes verschlüsselt und das Chiffre C_{G_θ, O_P} öffentlich im
25 Informationssystem gespeichert wird. Dieses Schlüsselpaar stellt der Patient dem Arzt zur Verfügung. Beispielsweise kann dieses Schlüsselpaar so attribuiert sein, dass es nur einmal für eine Entschlüsselungsoperation verwendet werden kann. Das Schlüsselpaar ist dann also als TAN ausgebildet.

- 30 Damit hat der Arzt nun innerhalb eines Monats fünf Mal die Möglichkeit, eine Sitzung beim Informationssystem zu eröffnen, innerhalb der er die Akte des Patienten lediglich lesen kann. Ein schreibender Zugriff auf die Akte des Patienten oder ein Versuch Rechte zu vergeben werden vom Informationssystem zurückgewiesen. Nach Ablauf des Zeitintervalls kann der Arzt genauso wie nach der fünften Benutzung keine Sitzung

unter Verwendung des Schlüsselpaars K_p bei der Authentisierung beim Informationssystem mehr eröffnen.

5 Dies erfordert vorzugsweise eine Authentisierung eines Benutzers gegenüber der vertrauenswürdigen Stelle, sodass in entsprechender Weise ein Zugriff auf die Chiffre gesteuert werden kann.

10 Nach einer weiteren Ausführungsform der Erfindung werden der zweite private Schlüssel und/oder der private Nachfolger-Schlüssel und/oder der private Schlüssel des ersten Schlüsselpaars der beliebigen Schlüsselpaare von einem tragbaren Datenträger empfangen. Beispielsweise handelt es sich bei dem tragbaren Datenträger um eine Chipkarte, welche gegebenenfalls auch einen Prozessor aufweisen kann, wobei das Verfahren zur Erzeugung der Schlüssel und/oder Ver- und Entschlüsselungsverfahren unter Verwendung der Schlüsselpaare von dem Prozessor des tragbaren Datenträgers
15 durchgeführt wird.

Beispielsweise kann es sich bei dem tragbaren Datenträger um eine Chipkarte, in einer konkreten Anwendung die elektronische Gesundheitskarte eines Patienten, handeln.

20 In einem weiteren Aspekt betrifft die Erfindung ein Computerprogrammprodukt mit von einem Prozessor ausführbaren Instruktionen zur Durchführung der Verfahrensschritte des erfindungsgemäßen Verfahrens.

25 In einem weiteren Aspekt betrifft die Erfindung ein Datenverarbeitungssystem zur Erzeugung eines Satzes von asymmetrischen kryptografischen Schlüsselpaaren.

30 In einem weiteren Aspekt betrifft die Erfindung ein Verfahren zur Bereitstellung von Chiffren, wobei die Chiffre einem Satz von asymmetrischen kryptografischen Schlüsselpaaren zugeordnet sind, wobei der Satz von Schlüsselpaaren eine gerichtete Graphstruktur aufweist, wobei die Knoten des Graphs die Schlüsselpaare repräsentieren, wobei eine Abhängigkeit zwischen einem Vorgänger-Schlüsselpaar und einem dem Vorgänger-Schlüsselpaar im Graph unmittelbar nachfolgenden Nachfolger-Schlüsselpaar durch ein Chiffre gebildet wird, wobei das Chiffre durch Verschlüsselung des privaten Schlüssels des Nachfolger-Schlüsselpaars mit dem

öffentlichen Schlüssel des Vorgänger-Schlüsselpaars gebildet ist, wobei das Verfahren die Chiffre-Bereitstellungsschritte umfasst:

- 5 - Empfang einer ersten und einer zweiten Kennung, wobei die erste Kennung einem ersten der Knoten zugeordnet ist und die zweite Kennung einem zweiten der Knoten zugeordnet ist,
 - 10 - Ermittlung aller Chiffre, welche sequentiell in der Graphstruktur eine Abhängigkeit zwischen dem ersten der Knoten und dem zweiten der Knoten beschreiben, falls ein solcher Pfad zwischen den ersten und zweiten Knoten existiert,
 - Bereitstellung der ermittelten Sequenz von Chiffren.
- 15 Durch das Verfahren zur Bereitstellung von Chiffren ist es möglich, ausgehend von einem Satz von Schlüsselpaaren und einem beliebigen asymmetrischen kryptografischen Schlüsselpaar dieses Satzes, einem Benutzer eine Sequenz von Chiffren bereitzustellen, welche vom Benutzer unter Verwendung seines zur Verfügung stehenden Schlüsselpaares sequentiell und aufeinander folgend
- 20 entschlüsselt werden können. Damit kann ausgehend von einem beliebigen Schlüsselpaar eines Benutzers unter Verwendung der Sequenz von Chiffren ein „Pfad“ von Schlüsseln bereitgestellt werden, sodass schließlich der Benutzer ausgehend von seinem persönlichen Schlüsselpaar Zugriff auf ein beliebiges anderes Schlüsselpaar erlangen kann, welches im Pfad der Schlüsselpaare, ausgehend von
- 25 seinem persönlichen Schlüsselpaar, liegt. Der Benutzer muss hierzu lediglich die erste Kennung angeben, welche sein persönliches Schlüsselpaar kennzeichnet, als auch die weitere Kennung angeben, welche jenes Schlüsselpaar kennzeichnet, auf welches der Benutzer gerne Zugriff erhalten möchte. Daraufhin ermittelt das erfindungsgemäße Verfahren automatisch einen Pfad zwischen diesen beiden Schlüsselpaaren, falls
- 30 existent, durch Bereitstellung einer entsprechenden Sequenz von Chiffren, deren sequentielle Entschlüsselung ausgehend vom Schlüsselpaar des Benutzers einen Zugriff auf das gewünschte Schlüsselpaar (des zweiten Knotens) ermöglicht.

Nach einer weiteren Ausführungsform der Erfindung ist bis auf das den Wurzelknoten des Graphen bildende Schlüsselpaar jedes Schlüsselpaar im Graph durch mindestens ein Chiffre von einem anderen Schlüsselpaar abhängig.

- 5 Nach einer weiteren Ausführungsform der Erfindung wird die Sequenz von Chiffren nach einer erfolgreichen Authentisierung ermittelt und/oder bereitgestellt. Damit ist, wie bereits oben erwähnt, sichergestellt, dass ein unbefugter Zugriff auf Chiffre verhindert wird. Damit können Chiffren auch entsprechende Klassifizierungsmerkmale bezüglich der Gültigkeit von Schlüsselpaaren innerhalb von Informationssystemsitzungen
- 10 zugeordnet werden. In diesem Fall sind die Chiffre mit Klassifizierungsmerkmalen verknüpft, wobei die Klassifizierungsmerkmale eine Gültigkeit der Chiffre festlegen, wobei die Gültigkeit angibt, dass nach Ablauf der Gültigkeit eine Bereitstellung der Chiffre verhindert werden soll, wobei eine Bereitstellung der Chiffre nur dann erfolgt, wenn die Gültigkeit der Chiffre erfolgreich validiert wurde. Vorzugsweise werden die
- 15 betreffenden Chiffre nach Ablauf der Gültigkeit gelöscht.

- Nach einer weiteren Ausführungsform der Erfindung ist die zweite Kennung einem Datenobjekt zugeordnet, wobei das Datenobjekt mit dem öffentlichen Schlüssel des Schlüsselpaars des zweiten der Knoten verschlüsselt ist. In anderen Worten sind dabei
- 20 vorzugsweise Datenobjekte von verschiedenen Benutzern mit unterschiedlichen Schlüsselpaaren der Benutzer verschlüsselt, wobei im Falle eines Graphen in Form eines Baumes die unterste Hierarchieebene des Abhängigkeitsbaumes, d.h. die „Blätter“ der baumförmigen Abhängigkeitshierarchie jene Schlüsselpaare repräsentieren, mit welchen eine Verschlüsselung der Datenobjekte vorgenommen
- 25 wird. Wenn ein Benutzer also eines seiner Datenobjekte abrufen und entschlüsseln möchte, muss er neben dem verschlüsselten Datenobjekt selbst auch alle verschlüsselten geheimen Schlüssel auf einem Pfad im Abhängigkeitsbaum entlang des Weges von seinem ihm zur Verfügung stehenden Schlüsselpaar, d.h. von dem entsprechenden Knoten des Baums bis zum verschlüsselten Datenobjekt,
- 30 entschlüsseln lassen.

Um dies durchzuführen, umfasst das Datenentschlüsselungsverfahren die Schritte der Ermittlung eines privaten Schlüssels durch Entschlüsselung des ersten Chiffres der Sequenz von Chiffren mit den privaten Schlüssel des Schlüsselpaars, welches dem

ersten der Knoten zugeordnet ist, der Ermittlung eines nächsten privaten Schlüssels für die Entschlüsselung des nächsten Chiffrats der Sequenz von Chiffraten mit dem zuvor ermittelten privaten Schlüssel und Wiederholung dieses Schrittes so lange, bis das letzte Chifftrat der Sequenz von Chiffraten entschlüsselt wurde. Das Verfahren zur Datenentschlüsselung endet schließlich mit der Entschlüsselung des verschlüsselten Datenobjekts.

Vorzugsweise werden der Schritt der Datenentschlüsselung und die Chiffratbereitstellungsschritte von unterschiedlichen Datenverarbeitungssystemen durchgeführt. Insbesondere wird der Schritt der Datenentschlüsselung durch eine vertrauenswürdige Stelle durchgeführt. Damit erhält das Datenverarbeitungssystem, welches die Chiffrate verwaltet und bereitstellt, zu keinem Zeitpunkt Informationen über etwaige Schlüssel im Klartext, welche zur Datenentschlüsselung verwendet werden.

Damit ist eine hohe Vertraulichkeit der Datenobjekte gewährleistet, da für jeden Benutzer, dessen Datenobjekte derartig verschlüsselt im Informationssystem abgelegt sind, sichergestellt ist, dass nur er selbst die Datenobjekte entschlüsseln kann. Der Betreiber des Informationssystems, welcher die Chiffrate verwaltet, hat keinen Zugriff auf die Datenobjekte des Benutzers. Ein technischer Beschlagnahmeschutz des Informationssystems besteht darin, dass die zur Entschlüsselung der Datenobjekte benötigten Geheimnisse der Benutzer zu keiner Zeit dem Betreiber des Informationssystems zugänglich sein dürfen, was zur Folge hat, dass der Betreiber des Informationssystems zu keiner Zeit die Möglichkeit hat, auf verschlüsselt gespeicherte Datenobjekte zuzugreifen. Beispielsweise ist es damit möglich, im Informationssystem die verschlüsselten Datenobjekte zusammen mit den Chiffraten abzuspeichern, ohne jedoch Gefahr zu laufen, dass auf Seite des Betreiberinformationssystems die Möglichkeit besteht, die Datenobjekte zu entschlüsseln.

Dies gilt insbesondere für den Fall, dass auf Seiten des Betreibers des Informationssystems der Versuch unternommen wird, eine rechtliche Verpflichtung zur Wahrung der Vertraulichkeit der Datenobjekte zu umgehen. Etwa könnte dies durch kriminelle Machenschaften korrupter Insider, zum Beispiel Administratoren, geschehen oder bei Diebstahl bzw. Beschlagnehmung des Rechnersystems, auf dem das

Informationssystem läuft, durch staatliche Organe bei gleichzeitiger Herausgabe des Informationssystem-Quellcodes.

Im Folgenden werden Ausführungsformen der Erfindung anhand der Zeichnungen
5 näher erläutert. Es zeigen:

- Figur 1 eine grafische Darstellung von verschiedenen Schritten, mittels welcher eine Graphstruktur in Form eines Baumes erzeugt werden kann,
- 10 Figur 2 ein Blockdiagramm eines Datenverarbeitungssystems,
- Figur 3 eine grafische Darstellung einer zyklischen Abhängigkeit zwischen zwei bzw. drei Schlüsselpaaren,
- 15 Figur 4 eine grafische Darstellung eines gerichteten azyklischen Graphen,
- Figur 5 zwei Abhängigkeitsbäume, vor und nach ihrer Verschmelzung zu einem gerichteten azyklischen Graphen,
- 20 Figur 6 ein Flussdiagramm eines Verfahrens zur Speicherung von Chiffraten,
- Figur 7 ein Flussdiagramm eines Verfahrens zur Bereitstellung einer ChiffratSequenz.
- 25 Die Figur 1 zeigt eine grafische Darstellung von verschiedenen Schritten, mittels welcher eine Graphstruktur in Form eines Baumes (Figur 1c) erzeugt werden kann, bei welcher Datenobjekte mit Blattknoten verschlüsselt werden. In der Figur 1a ist eine Abhängigkeit zwischen zwei asymmetrischen kryptografischen Schlüsselpaaren K_1 und K_3 gezeigt, wobei das Schlüsselpaar K_1 durch den Knoten 102 repräsentiert wird und
- 30 das Schlüsselpaar K_3 durch den Knoten 104 repräsentiert wird. Eine Verknüpfung der beiden Schlüsselpaare wird dadurch hergestellt, dass der geheime Schlüssel G_3 des zweiten Schlüsselpaars K_3 mit dem öffentlichen Schlüssel O_1 des ersten Schlüsselpaars K_1 verschlüsselt wird. Dies ergibt das Chifftrat 100.

Um nun zusätzlich ein Schlüsselpaar K_2 , repräsentiert durch den Knoten 106, zum Graphen hinzuzufügen, erfolgt in der Figur 1b ein weiterer Verschlüsselungsvorgang, bei welchem der geheime Schlüssel G_2 des Schlüsselpaars K_2 mit dem öffentlichen Schlüssel O_1 des ersten Schlüsselpaars K_1 verschlüsselt wird, woraus sich das
5 Chiffre 108 ergibt.

Diese Schritte können nun fortgeführt werden, indem eine beliebige Anzahl weiterer Schlüsselpaare dem Graphen der Figur 1b hinzugefügt werden, und entsprechende Chiffre berechnet und gespeichert werden. So wurde in der Figur 1c schließlich noch
10 ausgehend vom Schlüsselpaar K_1 ein weiteres Schlüsselpaar K_4 hinzugefügt und eine entsprechende Abhängigkeit hergestellt.

Während die Figur 1a eine „1:1-Abhängigkeit“ von K_1 nach K_3 zeigt, ist in der Figur 1b eine weitere 1:1-Abhängigkeit von K_1 nach K_2 gezeigt, die also besagt, dass ein
15 Benutzer, der im Besitz des geheimen Schlüssels G_1 von K_1 ist, nicht nur Zugriff auf den geheimen Schlüssel G_3 von K_3 hat, sondern auch den geheimen Schlüssel G_2 von K_2 .

Da bei diesem Szenario durch Zugriff auf den geheimen Schlüssel eines einzelnen
20 Schlüsselpaars Zugriff auf die geheimen Schlüssel mehrerer Schlüsselpaare erlangt wird, wird diese Abhängigkeit im Folgenden als „1:N-Abhängigkeit“ bezeichnet. Die einfachste Form einer solchen 1:N-Abhängigkeit ist in der Figur 1b gezeigt.

Eine weitere Variationsmöglichkeit bietet sich in der Hinzunahme eines weiteren
25 Schlüsselpaars in der Art und Weise, wie dies in der Figur 1c hinsichtlich der Schlüsselpaare K_3 und K_8 gezeigt ist. Hier wird der geheime Schlüssel G_8 von K_8 mit dem öffentlichen Schlüssel O_3 von K_3 verschlüsselt und das entsprechende Chiffre gespeichert. Damit kommt zu der bereits existierenden 1:1-Abhängigkeit von K_1 nach K_3 eine weitere 1:1-Abhängigkeit von K_3 nach K_8 hinzu. Das bedeutet, ein Benutzer, der in
30 Besitz des geheimen Schlüssels G_1 von K_1 ist, aufgrund der Speicherung des entsprechenden Chiffres $C_{G_3_O1}$ Zugriff auf den geheimen Schlüssel G_3 von K_3 bekommt und dadurch wiederum, aufgrund der Speicherung von $C_{G_8_O3}$ Zugriff auf den geheimen Schlüssel G_8 von K_8 . Die 1:1-Abhängigkeiten wirken also transitiv, d.h. falls eine 1:1-Abhängigkeit von K_1 nach K_3 und weiterhin eine 1:1-Abhängigkeit von K_3

nach K_8 besteht, dann besteht auch eine 1:1-Abhängigkeit von K_1 nach K_8 . Diese transitive Abhängigkeit wird auch 2-stufige Abhängigkeitshierarchie genannt.

Der oben beschriebenen 2-stufigen Abhängigkeitshierarchie, bestehend aus 3

- 5 Schlüsselpaaren, lassen sich nun beliebig viele weitere Schlüsselpaare hinzufügen, sowie eine entsprechende Menge von öffentlich gespeicherten Chiffraten, bei denen jeweils der geheime Schlüssel des Nachfolgerschlüsselpaars mit dem öffentlichen Schlüssel des Vorgängerschlüsselpaars verschlüsselt worden ist und so jeweils eine 1:1-Abhängigkeit von Vorgängerschlüsselpaar zu Nachfolgerschlüsselpaar besteht.

10

Nach dem oben beschriebenen Prinzip der Transitivität von verketteten 1:1-Abhängigkeiten gilt nun, dass ein Benutzer, der in Besitz des geheimen Schlüssels G_I von K_I ist, gleichsam Zugriff auf alle geheimen Schlüssel $G_3, G_8, \dots$, in der vorliegenden n -stufigen Abhängigkeitshierarchie hat oder genauer, dass ein Benutzer, der in Besitz

15 eines der geheimen Schlüssel $G_i \in \{G_I, G_8, \dots\}$ ist, gleichsam Zugriff auf alle in der Abhängigkeitshierarchie nachfolgenden geheimen Schlüssel dieser Menge hat.

Die sich in Figur 1c ergebenden Abhängigkeitshierarchien in Form eines Baumes kann definiert werden als eine Abhängigkeits-hierarchie $H = (K, C)$, für welche die folgenden

20 zwei Bedingungen erfüllt sind:

- Für alle Schlüsselpaare $K_i \in K$ gilt, bis auf ein einziges Schlüsselpaar $K_k \in K$, dass K_i immer nur von genau einem $K_j \in K$ mit $i \neq j$ abhängig ist.
- Es gibt genau ein Schlüsselpaar $K_k \in K$, welches von keinem $K_l \in K$ mit $k \neq l$ abhängig ist.

25

Es soll nun beschrieben werden, wie ein Graph, wie zum Beispiel der Graph in der Figur 1c, zur Rechteverwaltung in einem Informationssystem eingesetzt werden kann. Dabei wird ein Informationssystem betrachtet, in dem verschiedene Benutzer Datenobjekte verschlüsselt abspeichern und wieder abrufen können und das außerdem

30 einen technischen Beschlagnahmeschutz bietet.

Auch hier soll dem Informationssystem für jeden Benutzer B eine Hierarchie von voneinander abhängigen Schlüsselpaaren $H = (K, C) = (\{K_0, K_1, \dots, K_n\}, \{C_1, \dots, C_n\})$ hinzugefügt werden.

- 5 Darüber hinaus wird dem Szenario eine weitere Komponente hinzugefügt, die im Folgenden als „Vertrauenswürdige Stelle“ bezeichnet werden soll. Sie kann zwischen der Benutzerseite und der Seite des Informationssystems platziert werden und erfüllt dort die Funktion, dass alle Ver- und Entschlüsselungsvorgänge innerhalb ihres Bereichs durchgeführt werden und von der Seite des Informationssystems getrennt werden können. Alle Schlüssel, die innerhalb ihres Bereichs in nicht verschlüsselter Form vorliegen, gelangen zu keiner Zeit außerhalb ihres Bereichs. Sie bekommt als
- 10 Eingabe Schlüssel und Datenobjekte im Klartext von der Benutzerseite und in verschlüsselter Form von der Seite des Informationssystems und gibt als Ausgabe lediglich entschlüsselte Datenobjekte an die Benutzerseite sowie verschlüsselte
- 15 Schlüssel sowie verschlüsselte Datenobjekte ans Informationssystem aus.

Darüber hinaus sollen im Informationssystem die Datenobjekte der jeweiligen Benutzer mit unterschiedlichen Schlüsselpaaren, die jeweils aus der untersten Ebene des Abhängigkeitsbaumes stammen, sozusagen die „Blätter“ der baumförmigen

- 20 Abhängigkeitshierarchien verschlüsselt werden. Dabei kann auch mehr als ein Datenobjekt mit demselben Schlüsselpaar in der vertrauenswürdigen Stelle verschlüsselt worden sein. Abb. 1c) stellt den Baum inklusive der verschlüsselten Datenobjekte 116 beispielhaft dar.

- 25 Wenn ein Benutzer eines seiner Datenobjekte abrufen und entschlüsseln möchte, muss er neben dem verschlüsselten Datenobjekt selbst auch alle verschlüsselten geheimen Schlüsselpaare auf dem Pfad im Abhängigkeitsbaum entlang des Weges von der Wurzel des Baums bis zum verschlüsselten Datenobjekt in die vertrauenswürdige Stelle laden lassen. Dies sei durch das folgende Beispiel illustriert, das in Abb. 1c) grafisch
- 30 dargestellt wird: Wenn ein Benutzer das verschlüsselte Datenobjekt DO_4 abrufen und entschlüsseln lassen möchte, dann muss er dazu neben dem Datenobjekt selbst in seiner verschlüsselten Form $C_{DO_4}O_8$ auch die verschlüsselten geheimen Schlüssel $C_{G_8}O_3$ und $C_{G_3}O_1$ abrufen und in die vertrauenswürdige Stelle laden lassen, da er selbst nur über den geheimen Schlüssel G_1 des Schlüsselpaars K_1 verfügt, die

vertrauenswürdige Stelle zur Entschlüsselung von $C_{DO_4}O_8$ aber den geheimen Schlüssel G_8 des Schlüsselpaars K_8 benötigt. Mit G_1 entschlüsselt die vertrauenswürdige Stelle aus dem Chiffprat $C_{G_3}O_1$ den geheimen Schlüssel G_3 von K_3 und damit wiederum den geheimen Schlüssel G_8 von K_8 aus dem Chiffprat $C_{G_8}O_3$, mit dem sie
5 dann schließlich das verschlüsselte Datenobjekt $C_{DO_4}O_8$ entschlüsseln kann, welches sie dem Benutzer schließlich im Klartext ausgibt.

Die Figur 2 zeigt eine schematische Ansicht zweier Datenverarbeitungssysteme 200 und 224, welche zur Verwendung von Graphen für Ver- und Entschlüsselungsvorgänge
10 und zur Erzeugung entsprechender Graphen, d.h. der Herstellung von Verknüpfungen zwischen verschiedenen Sätzen von Schlüsselpaaren, vorgesehen sind. So dient beispielsweise das Datenverarbeitungssystem 200 einer Berechnung von Chiffraten sowie der Durchführung von Ver- und Entschlüsselungsvorgängen von Daten, wohingegen das Datenverarbeitungssystem 224 einer Datenspeicherung und der
15 Ermittlung von Chifftratsequenzen dient.

Das Datenverarbeitungssystem 200 weist Eingabemittel 202, wie beispielsweise eine Tastatur, eine Maus, sowie Eingabemittel auf, welche zum Empfang von biometrischen Merkmalen, wie Fingerabdrücken, geeignet sind. Ferner weist das
20 Datenverarbeitungssystem einen Bildschirm 204 auf sowie eine Schnittstelle 206, mittels welcher das Datenverarbeitungssystem mit externen Geräten, wie beispielsweise einer Chipkarte 216 und einem Netzwerk 226 und damit dem Datenverarbeitungssystem 224 kommunizieren kann.

Mittels eines Prozessors 208 ist das Datenverarbeitungssystem 200 dazu in der Lage, entsprechende Computerprogramminstruktionen 212 und 214 auszuführen, welche im Speicher 210 des Datenverarbeitungssystems enthalten sind. Bei den Instruktionen 212 und 214 handelt es sich beispielsweise um ein Modul 212 zur Berechnung von Chiffraten und ein Modul 214 zur Durchführung von Kryptografievorgängen, wie
30 beispielsweise Ver- und Entschlüsselungsvorgängen, von Daten.

Das Datenverarbeitungssystem 224 weist neben einer Schnittstelle 246, welche zur Kommunikation über das Netzwerk 226 mit dem Datenverarbeitungssystem 200 ausgebildet ist, einen Prozessor 244 auf, welcher ebenfalls in der Lage ist,

entsprechende Programminstruktionen durchzuführen, welche im Speicher 238 des Datenverarbeitungssystems 224 enthalten. Bei diesen Programminstruktionen kann es sich beispielsweise um Programmmodule handeln, wie zum Beispiel ein Programmmodul 240 zur Ermittlung einer Sequenz von Chiffraten, und ein
5 Programmmodul 242 zur Validierung der Gültigkeit eines entsprechenden Chiffrats.

Ferner weist das Datenverarbeitungssystem 224 eine Datenbank 228 auf, deren Zweck anhand eines Beispiels im Folgenden näher erläutert wird:

- 10 Zunächst sei davon ausgegangen, dass zur Durchführung von Ver- und Entschlüsselungsvorgängen eine Graphstruktur in der Datenbank 228 abgebildet ist, welche im Wesentlichen die Graphstruktur der Figur 1c widerspiegelt. In diesem Fall ist jedem Knoten der Figur 1c eine entsprechende Kennung 230 zugeordnet, mittels welcher eine Knotenidentifizierung möglich ist. Ein Benutzer hat ein Schlüsselpaar K_3 ,
15 welchem eine Kennung 230 „abc“ zugeordnet ist. Das Schlüsselpaar K_3 besteht aus einem privaten Schlüssel 218 und einem öffentlichen Schlüssel 220. Der private Schlüssel 218 ist auf einer Chipkarte 216 des Benutzers abgespeichert. Der öffentliche Schlüssel 220 ist ebenfalls auf der Chipkarte 216, als auch in der Datenbank 228, zusammen mit der Kennung 230 verknüpft abgespeichert. Die Abspeicherung des
20 öffentlichen Schlüssels 220 in der Datenbank 228 verletzt dabei kein Geheimnis, da ein beliebiger Benutzer unter Kenntnis des öffentlichen Schlüssels 220 lediglich einen weiteren Verschlüsselungsvorgang von Daten durchführen kann, eine Datenentschlüsselung hingegen mit dem öffentlichen Schlüssel 220 nicht möglich ist.
- 25 Außerdem ist die Speicherung des öffentlichen Schlüssels 220 in der Datenbank 228 insbesondere dann von Vorteil, wenn mittels dieses öffentlichen Schlüssels 220 beispielsweise eine Signaturverifizierung durchgeführt werden soll. Eine Signierung eines Datenobjekts wird durchgeführt, indem ein Benutzer beispielsweise den HASH-Wert des Datenobjekts mit seinem geheimen Schlüssel signiert. Daraufhin ist jeder
30 befugte Benutzer, welcher Zugriff auf die Datenbank 228 hat, in der Lage, mittels des öffentlichen Schlüssels 220 eine Verifikation dieses HASH-Wertes vorzunehmen, um somit zu überprüfen, ob das ihm vorliegende Datenobjekt jenes Datenobjekt ist, welches zuvor vom Benutzer signiert wurde.

Im Folgenden sei angenommen, dass ein Benutzer einen Entschlüsselungsvorgang des Datenobjektes 4 (DO_4) vornehmen will. Dieses Datenobjekt 4 kann dabei in der Datenbank 228 abgelegt sein, oder es ist möglich, das Datenobjekt 4 im Speicher 238 abzulegen oder in einer beliebigen externen Datenbank zu speichern. Um nun einen

5 Entschlüsselungsvorgang durchzuführen, benötigt der entsprechende Benutzer den geheimen Schlüssel G_8 , da das Datenobjekt 4 mit dem öffentlichen Schlüssel O_8 verschlüsselt gespeichert wurde. Zu diesem Zweck gibt der Benutzer in das Datenverarbeitungssystem 200 ein, dass er im Besitz des Schlüsselpaars K_3 ist und Zugriff auf den geheimen Schlüssel G_8 haben möchte. Daraufhin werden die

10 entsprechenden Kennungen 230 des Schlüsselpaars K_3 und K_8 an das Datenverarbeitungssystem 224 übermittelt. Das Datenverarbeitungssystem 224 überprüft daraufhin zunächst mittels des Validierungsmoduls 242, ob ein entsprechender Bereitstellungsvorgang des Chiffrats $C_G_8_O_3$ überhaupt zulässig ist. Zu diesem Zweck erfolgt ein Zugriff auf die Datenbank 228, in welcher neben

15 Kennungen 230 und öffentlichen Schlüsseln, wie dem öffentlichen Schlüssel 220 von K_8 , auch Chiffrate 234 und deren Klassifizierungsmerkmale 236 abgespeichert sind. Beispielsweise kann mit der Kennung bezüglich des Schlüsselpaares K_8 ein Merkmal 236 in Form eines Datums gespeichert sein, welches ein Verfallsdatum des Schlüsselpaars K_8 wiedergibt. In der Figur 2 ist hinsichtlich der Kennung „abc“ und

20 damit dem Schlüsselpaar K_8 ein Verfallsdatum 27. April 2011 angegeben. Ist als das Systemdatum des Datenverarbeitungssystems 224 älter als der 27. April 2011, so wird das Datenverarbeitungssystem 224 ein entsprechendes Chifftrat, welches eine Entschlüsselung von K_8 zulässt, nicht mehr an das Datenverarbeitungssystem 200 übermitteln.

25 Im Folgenden sei davon ausgegangen, dass das Schlüsselpaar K_8 und damit das entsprechende Chifftrat kein Klassifizierungsmerkmal aufweist, woraufhin das Datenverarbeitungssystem 224 mit der Ermittlung des bzw. der Chifftrate beginnt, welche die Schlüssel K_8 und K_3 miteinander verknüpfen. Dies erfolgt durch Ausführung

30 des Moduls 240. Im einfachen Fall der Schlüsselpaare K_3 und K_8 ergibt sich als Ergebnis lediglich ein Chifftrat, nämlich das Chifftrat $C_G_8_O_3$, welches daraufhin über das Netzwerk 226 an das Datenverarbeitungssystem 200 übermittelt wird. Das Datenverarbeitungssystem 200 ist dabei eine vertrauenswürdige Stelle, wie zum Beispiel eine Zertifizierungsstelle oder ein Trust-Centre. Handelt es sich bei den

- betrachteten Datenobjekten um medizinische Datenobjekte, so handelt es sich bei der vertrauenswürdigen Stelle beispielsweise um das Arztinformationssystem einer Arztpraxis oder eines Krankenhauses oder Apothekeninformationssystem. Auch kann es sich bei der vertrauenswürdigen Stelle allgemein um ein Datenverarbeitungssystem
- 5 eines Gesundheitsdienstleisters handeln, welcher in der Lage sein soll, auf seinem Bildschirm nach Einverständnis des Benutzers entsprechende medizinische Datenobjekte wie Krankenakten, medizinische Bilddaten, Rezepte oder Ähnliches, anzeigen zu lassen.
- 10 Auch kann es sich nach einer Ausführungsform der Erfindung bei dem Datenverarbeitungssystem 200 um ein Datenverarbeitungssystem, das auf einem separaten gesicherten Hardwaremodul abläuft, handeln. Hierbei kann zum Beispiel ein Trusted Platform Module (TPM) zum Einsatz kommen.
- 15 Nachdem nun also das entsprechende, die Schlüsselpaare K_8 und K_3 verknüpfende Chiffprat über das Netzwerk 226 eines Datenverarbeitungssystems 200 übermittelt wurde, kann daraufhin das Kryptografiemodul 214 zunächst eine Entschlüsselung des Chiffrats mittels des privaten Schlüssels 218 der Chipkarte 216 vornehmen. Ein solcher Entschlüsselungsvorgang kann entweder auf dem Datenverarbeitungssystem 200
- 20 selbst stattfinden, oder aber der Prozessor 222 der Chipkarte 216 kann den Entschlüsselungsvorgang des Chiffrats durchführen, was den Vorteil hat, dass der geheime Schlüssel 218 die Chipkarte 216 nicht verlässt.

- Nach Entschlüsselung des Chiffrats 234 und damit Erhalt des geheimen Schlüssels G_8
- 25 kann daraufhin eine Entschlüsselung des Datenobjektes 4 (DO_4) stattfinden.

- Im Folgenden sei nun eine Vorgehensweise zur Berechnung von Chiffraten vorgestellt. Hierbei wird davon ausgegangen, dass ein Graph, wie in der Figur 1a gezeigt, vorliegt. Dieser Graph der Figur 1a, bestehend aus den Schlüsselpaaren K_1 und K_3 , soll durch
- 30 Hinzufügen eines weiteren Schlüsselpaars K_2 vervollständigt werden. Zu diesem Zweck wird zunächst das Schlüsselpaar K_2 in das Datenverarbeitungssystem 200 geladen. Daraufhin wird im Datenverarbeitungssystem 200 mittels des Moduls 212 ein Chiffprat berechnet, indem der geheime Schlüssel G_2 des Schlüsselpaars K_2 mit dem öffentlichen Schlüssel O_1 des Schlüsselpaars K_1 verschlüsselt wird. Dieser

Verschlüsselungsvorgang findet vorzugsweise im Datenverarbeitungssystem 200 statt, kann jedoch mittels entsprechender Module auf einer Chipkarte stattfinden, auf welcher sich das Schlüsselpaar K_1 befindet. Nach Erzeugung des Chiffrats, d.h. des Chiffrats $C_G_2_O_1$ wird dieses Chifftrat zusammen mit einer entsprechenden Kennung an das Datenverarbeitungssystem 224 übermittelt, wo es gegebenenfalls zusammen mit einem Klassifizierungsmerkmal 236 gespeichert wird.

In der Figur 1c ist ein gerichteter azyklischer Graph in Form eines Baumes gezeigt, bei dem Datenobjekte nur mit Blattknoten verschlüsselt werden. Die Anwendung einer solchen hierarchischen Gruppierung und Verteilung von Schlüsselpaaren K_i lässt sich vorteilhaft anhand der hierarchisch aufgebauten Managementstruktur in einem Unternehmen und den daraus erwachsenden Kommunikationsanforderungen beispielhaft erläutern. Beispielsweise sind hierfür der Hierarchieebene 254 mit dem Schlüsselpaar K_1 die Kommunikationsteilnehmer „Management“ zugeordnet. Die Kommunikationsteilnehmer der Gruppe Management sollen in der Lage sein, auf alle verschlüsselten Daten 116 des Unternehmens zuzugreifen. Das Schlüsselpaar K_1 ermöglicht dies, da alle anderen Schlüssel K_2 bis K_{11} über entsprechende Chifftrate unter Verwendung des Schlüsselpaars K_1 erhalten werden können.

In der Hierarchieebene 252 mit den Schlüsselpaaren K_2 , K_3 und K_4 können nun verschiedene Bereiche des Unternehmens abgebildet sein. Beispielsweise sind die Schlüsselpaare K_2 , K_3 und K_4 verschiedenen Bereichsleitern zugeordnet. Jeder Bereich ist wiederum in verschiedene Abteilungen untergliedert, welche die Hierarchieebene 250 einnehmen. Die Abteilungen haben jeweils Schlüssel K_5 , K_6 , K_7 usw. bis K_{11} . Während jede Abteilung der Hierarchieebene 250 nur auf die direkt von ihr verschlüsselten Datenobjekte zugreifen kann, ist es den Bereichsleitern möglich, auf die Daten zuzugreifen, welche durch die untergeordneten Abteilungen erstellt und verschlüsselt worden sind. So kann beispielsweise mittels des Schlüsselpaars K_2 ein Zugriff auf alle Datenobjekte erfolgen, welche von Abteilungen mit den Schlüsselpaaren K_5 , K_6 und K_7 verschlüsselt wurden. Das Management, welches hingegen im Besitz des Schlüsselpaars K_1 ist, ist in der Lage, auf sämtliche verschlüsselten Datenobjekte 116 zuzugreifen.

Hinsichtlich der Figur 2 sei noch angemerkt, dass insbesondere dadurch sichergestellt werden kann, dass es sich bei dem Datenverarbeitungssystem 200 um eine vertrauenswürdige Stelle handelt, wenn ein entsprechender Authentisierungsvorgang des Datenverarbeitungssystems 200 gegenüber dem Datenverarbeitungssystem 224 stattfindet. Damit lässt das Datenverarbeitungssystem 224 einen Zugriff auf die Datenbank 228 nur zu, wenn zum einen eine entsprechende Authentisierung erfolgt ist und zum anderen die Merkmale 236 einen Zugriff auf die jeweiligen Chiffre zulassen.

Die Figuren 3a und 3b zeigen eine grafische Darstellung einer zyklischen Abhängigkeit zwischen zwei bzw. drei Schlüsselpaaren. In diesem Fall bilden Abhängigkeitshierarchien keine Kette, sondern einen Ring von 1:1-Abhängigkeiten.

Dies stellt sich so dar, dass zu einer Menge $K_1, \dots, K_n$ von Schlüsselpaaren für alle $i \in \{2, \dots, n\}$ jeweils $C_{G_i}O_{i-1}$, also der geheime Schlüssel G_i des Schlüsselpaars K_i , verschlüsselt mit dem öffentlichen Schlüssel O_{i-1} des Schlüsselpaars K_{i-1} gespeichert wird, zusätzlich dazu aber auch $C_{G_1}O_n$, der geheime Schlüssel G_1 von K_1 , verschlüsselt mit dem öffentlichen Schlüssel O_n von K_n .

Besitzt ein Benutzer nun den geheimen Schlüssel G_i des Schlüsselpaars K_i für ein beliebiges i aus $\{1, \dots, n\}$, so hat er wie bereits im Detail erwähnt Zugriff auf die geheimen Schlüssel $G_{i+1}, \dots, G_n$ der Schlüsselpaare $K_{i+1}, \dots, K_n$; darüber hinaus hat er aber aufgrund von $C_{G_1}O_n$ auch Zugriff auf den geheimen Schlüssel G_1 des Schlüsselpaars K_1 , und damit auch auf die geheimen Schlüssel $G_2, \dots, G_{i-1}$ der Schlüsselpaare $K_2, \dots, K_{i-1}$, also auf alle geheimen Schlüssel der gesamten betrachteten Abhängigkeitshierarchie.

Bei einer zyklischen Abhängigkeitshierarchie hat also jeder Benutzer, der im Besitz des geheimen Schlüssels eines der Schlüsselpaare aus der Abhängigkeitshierarchie ist, Zugriff auf alle anderen geheimen Schlüssel der Hierarchie, wobei egal ist, welchen geheimen Schlüssel der Benutzer besitzt. Die Figuren 3a und 3b zeigen grafischen Darstellungen zweier zyklischen Abhängigkeiten bei einer Menge von 2 bzw. 3 Schlüsselpaaren in der jeweiligen Abhängigkeitshierarchie.

Es sei angemerkt, dass unter einer streng theoretischen Betrachtungsweise ein Zyklus in einer Abhängigkeitshierarchie durch einen einzigen Knoten ersetzt werden kann, auf den die Benutzer einer Gruppe dann beispielsweise über eine N:1-Abhängigkeitshierarchie zugreifen können.

5

Die Figur 4 zeigt eine grafische Darstellung eines gerichteten azyklischen Graphen. Im Vergleich zu Bäumen entscheidend in der Figur ist nun, dass z.B. zwischen dem Schlüsselpaar K_3 und dem Schlüsselpaar K_5 eine zusätzliche Abhängigkeit durch ein entsprechendes Chiffre erzeugt wurde. Beispielsweise kann die Hinzufügung dieser

10 Abhängigkeit zwischen K_3 und K_5 die Ursache haben, dass dem Benutzer des Schlüsselpaars K_3 einmalig die Gelegenheit gegeben werden soll, auf Datenobjekte zuzugreifen, welche unter Verwendung der Schlüsselpaare K_9 und K_{10} verschlüsselt wurden. Somit handelt es sich bei dieser Verknüpfung zwischen den Schlüsselpaaren K_3 und K_5 um eine „Einmal-Verknüpfung“, sodass ein entsprechendes Chiffre nur

15 einmal verwendet werden kann, was etwa TAN-Systemen gleichkommt, die beim Online-Banking verwendet werden. Damit lässt sich erzwingen, dass ein entsprechendes Chiffre nur für eine Sitzung verwendet werden kann. Sobald eine einmalige Verwendung dieses Chiffres erfolgt ist, wird das entsprechende Chiffre als „benutzt“ in der Datenbank des Informationssystems gekennzeichnet und vorzugsweise

20 aus dem Informationssystem gelöscht, sodass der Benutzer von K_3 ein zweites Mal auf die Schlüsselpaare K_9 und K_{10} nicht mehr zugreifen kann.

Ferner ist in der Figur 4 gezeigt, dass das Schlüsselpaar K_{11} beispielsweise von zwei Schlüsselpaaren K_5 und K_6 abhängig ist. In anderen Worten ist mit dem

25 Schlüsselpaar K_{11} sowohl das Schlüsselpaar K_5 als auch das Schlüsselpaar K_6 über entsprechende Chiffre verknüpft. Sind Daten damit mit dem öffentlichen Schlüssel O_{11} des Schlüsselpaars K_{11} verschlüsselt, so ist ein Zugriff sowohl über K_5 als auch über K_6 möglich.

30 Ein konkreter Anwendungsfall einer solchen Abhängigkeit eines Schlüsselpaars über zwei verschiedene Chiffre ist im Näheren in den Figuren 5a und b erläutert. Die Figuren 5a und b zeigen zwei Abhängigkeitsbäume, vor und nach ihrer Verschmelzung zu einem gerichteten azyklischen Graphen. In der Figur 5a ist angenommen, dass verschiedene Benutzer eines Informationssystems jeweils einen eigenen Baum mit

- Schlüsselpaaren haben. Beispielsweise hat ein Benutzer B_1 den Baum der Figur 5a, welcher aus den Schlüsselpaaren K_1 , K_3 und K_4 besteht, wohingegen der Benutzer B_2 den Baum besitzt, welcher aus den Schlüsselpaaren K_2 und K_5 besteht. Anstelle einer Menge von überschneidungsfrei nebeneinander existierenden Schlüsselpaar-
- 5 Abhängigkeitsbäumen (jeder Benutzer des Informationssystems besitzt einen solchen Baum) soll nun zugelassen werden, dass sich die Abhängigkeitsbäume überschneiden, d.h. es wird zugelassen, dass zwei oder mehrere Abhängigkeitsbäume zu einem gerichteten azyklischen Graphen verschmelzen.
- 10 Dies hat zur Folge, dass sich mit Hilfe dieser gerichteten atypischen Graphen ein flexibles Rechtesystem etablieren lässt, bei dem ein Benutzer einem anderen Benutzer ausgewählte Teile seiner Datenobjekte freigeben und existierende Freigaben auch wieder entziehen kann. Dies ist im Detail in den Figuren 5a und 5b erläutert.
- 15 In diesem Beispiel werden zwei Schlüsselpaar-Abhängigkeitsbäume (Figur 5a) betrachtet: Der erste Baum, auf den der besitzende Benutzer B_1 über das Schlüsselpaar K_1 zugreift, weist auf der Blattebene zwei weitere Schlüsselpaare K_3 und K_4 auf, mit denen jeweils zwei Datenobjekte, DO_1 und DO_2 bzw. DO_3 und DO_4 verschlüsselt sind. Der zweite Baum, auf den der besitzende Benutzer B_2 über das Schlüsselpaar K_2
- 20 zugreift, hat auf der Blattebene lediglich ein weiteres Schlüsselpaar K_5 , mit dem die Datenobjekte DO_5 und DO_6 verschlüsselt sind.

Wenn Benutzer B_1 nun beschließen sollte, einen Teil seiner Datenobjekte für Benutzer B_2 zugänglich zu machen, beispielsweise die Datenobjekte DO_3 und DO_4 , dann kann er

25 dies dadurch tun, indem er der Schlüsselverwaltung im Informationssystem (die Menge C von verschlüsselten geheimen Schlüsseln), die zu diesem Zeitpunkt aus den Elementen $C_{G_3_O1}$, $C_{G_4_O1}$ und $C_{G_5_O2}$ besteht, ein weiteres Element $C_{G_4_O2} = V_A(G_4, O_2)$ hinzufügt, was im Graphen der Figur 5b einer zusätzlichen Verbindung vom Knoten K_2 zum Knoten K_4 entspricht.

30 Dadurch sind die zwei Abhängigkeitsbäume der Figur 5a zu einem gerichteten azyklischen Graphen, wie in Figur 5b gezeigt, verschmolzen, und Benutzer B_2 kann auf die Datenobjekte DO_3 und DO_4 von Benutzer B_1 zugreifen, indem er die verschlüsselten Datenobjekte $C_{DO_3_O4}$ und $C_{DO_4_O4}$ sowie $C_{G_4_O2}$ in die vertrauenswürdige Stelle

laden lässt, die dann erst $G_4 = E_A(C_{G_4}O_2, G_2)$ und dann $DO_3 = E_A(C_{DO_3}O_4, G_2)$ sowie $DO_4 = E_A(C_{DO_4}O_4, G_2)$ entschlüsselt.

Der Entzug einer bereits erteilten Freigabe auf Datenobjekte lässt sich in diesem
5 Szenario ebenfalls sehr einfach realisieren, nämlich dadurch, dass der entsprechende
verschlüsselte geheime Schlüssel aus der Abhängigkeitshierarchie des betreffenden
Benutzers gelöscht wird. Dadurch steht der besagte Schlüssel für den Benutzer, dem
die Freigabe ursprünglich erteilt worden ist, nicht mehr zur Verfügung, so dass er die
bisher freigegebenen Datenobjekte von der vertrauenswürdigen Stelle nicht mehr
10 entschlüsseln lassen kann.

An dieser Stelle wird die Funktion der zuvor eingeführten vertrauenswürdigen Stelle
deutlich: Sie erfüllt den Zweck, dass Benutzer Zugriff auf für sie freigegebene
Datenobjekte anderer Benutzer bekommen, ohne die zugehörigen geheimen Schlüssel
15 zu kennen, mit denen diese Datenobjekte entschlüsselt werden, da die geheimen
Schlüssel die vertrauenswürdige Stelle nicht verlassen. Wenn diese geheimen
Schlüssel zu irgendeinem Zeitpunkt in den Hoheitsbereich der Benutzer geraten
würden, könnte es nicht ausgeschlossen werden, dass korrupte Benutzer sich die
Schlüssel „merken“, d.h. sie mit Hilfe eines manipulierten Client-Programms o.ä.
20 abspeichern. In diesem Fall wäre es möglich, dass ein Benutzer auch nach Entzug
einer Freigabe Datenobjekte mit Hilfe eines irregulär „gemerkten“ geheimen Schlüssel
zu entschlüsseln kann, wodurch das Freigabekonzept unterlaufen werden könnte.
Durch die Einführung der vertrauenswürdigen Stelle jedoch behält das Konzept der
Nutzung von 1:N-Abhängigkeitshierarchien seine Nutzbarkeit.

25 Die Schlüssel werden daher nur in einer „vertrauenswürdigen Stelle“ zur Verfügung
gestellt. Unter einer „vertrauenswürdige Stelle“ wird hier jedes elektronische Gerät, wie
z.B. ein Computersystem, verstanden, in dem die schutzbedürftigen Datenobjekte im
Klartext vorliegen und/oder in dem Daten zur Überführung der Datenobjekte in Klartext
30 vorliegen und/oder welches Zugriff auf solche Daten hat.

Ein weiteres Konzept für eine Nutzung von Hierarchien ist dass sich mehrere Benutzer
 $B_1, \dots, B_n$ eines Informationssystems zu einer Gruppe B zusammenschließen, in der
vereinbart wird, dass jeder Benutzer B_i der Gruppe neben seinen eigenen auch die

- Datenobjekte aller anderen Benutzer $B_1, \dots, B_{i-1}, B_{i+1}, \dots, B_n$ aus der Gruppe entschlüsseln können soll. Dazu erteilt jeder Benutzer B_i aus B dem in der Reihenfolge nachfolgenden Benutzer B_{i+1} eine Freigabe auf seine eigenen Datenobjekte, indem er den geheimen Schlüssel G_i eines seiner Schlüsselpaare K_i mit dem öffentlichen Schlüssel O_{i+1} des Schlüsselpaars K_{i+1} des Benutzers B_{i+1} verschlüsselt und das Chifftrat $C_{G_i O_{i+1}}$ im Informationssystem abspeichert. Außerdem verschlüsselt Benutzer B_n seinen geheimen Schlüssel G_n mit dem öffentlichen Schlüssel O_1 des Schlüsselpaars K_1 von Benutzer B_1 und speichert das Chifftrat $C_{G_n O_1}$ ebenfalls im Informationssystem. In diesem Szenario ist es nun möglich, dass die vertrauenswürdige Stelle für einen Teilnehmer der Benutzergruppe B bei Eingabe dessen geheimen Schlüssels durch Entlanglaufen der kreisförmigen Hierarchie den geheimen Schlüssel von jedem anderen Teilnehmer nacheinander entschlüsselt und damit wiederum alle Datenobjekte, die mit jedem der zugehörigen öffentlichen Schlüssel verschlüsselt wurden, entschlüsseln kann. Jeder Teilnehmer von B kann also auf alle von allen anderen Teilnehmern von B verschlüsselten und ins Informationssystem eingestellten Datenobjekte zuzugreifen, jedoch ohne deren geheimen Schlüssel zu kennen.

- Einzelne Mitglieder können in diese Hierarchie aufgenommen sowie ausgeschlossen werden; es müssen nur die entsprechenden Verbindungen gelöscht bzw. neu hinzugefügt werden. Beim Hinzufügen eines neuen Mitglieds B_{n+1} wird die kreisförmige Hierarchie an einer Stelle aufgetrennt, d.h. es wird beispielsweise die Verbindung $C_{G_n O_1}$ gelöscht, und die Verbindungen $C_{G_n O_{n+1}}$ und $C_{G_{n+1} O_1}$ hinzugefügt.

- Analog dazu werden beim Löschen eines Mitglieds B_i aus der Hierarchie die Verbindungen $C_{G_{i-1} O_i}$ und $C_{G_i O_{i+1}}$ aus der Hierarchie gelöscht und eine neue Verbindung $C_{G_{i-1} O_{i+1}}$ zur Hierarchie hinzugefügt werden.

- Die Figur 6 zeigt ein Flussdiagramm eines Verfahrens zur Speicherung von Chiffraten. Das Verfahren beginnt in Schritt 600, in welchem Schlüsselpaare in Form eines Graphen bereitgestellt werden. Zu diesem existierenden Satz von Schlüsselpaaren soll nun ein weiteres Schlüsselpaar hinzugefügt werden, was in Schritt 602 erfolgt. Daraufhin erfolgt die Erzeugung einer Abhängigkeit zwischen diesem weiteren Schlüsselpaar und einem entsprechenden Vorgänger-Schlüsselpaar des bereitgestellten Satzes von Schlüsselpaaren, indem in Schritt 604 ein entsprechendes

Chiffirat erzeugt wird. Bei diesem Chiffirat wird dabei der geheime Schlüssel des weiteren Schlüsselpaars mit dem öffentlichen Schlüssel des Vorgänger-Schlüsselpaars verschlüsselt. Das so erzeugte Chiffirat wird in Schritt 606 in einer entsprechenden Datenbank gespeichert. Der Schritt 608 mit der Speicherung eines

5 Klassifizierungsmerkmals ist optional und kann dazu verwendet werden, um den Zugriff auf das Chiffirat zeitlich, nach der Benutzung oder nach Anzahl der Benutzungen einzuschränken.

Die Figur 7 zeigt ein Flussdiagramm eines Verfahrens zur Bereitstellung einer ChiffiratSequenz. Zunächst wird in Schritt 700 eine Authentisierung empfangen, mittels

10 welcher sichergestellt wird, dass ausschließlich ein befugter Benutzer Zugriff auf die Chiffirate hat. Ergibt der Überprüfungsschritt 702, dass ein Zugriff auf ein entsprechendes Chiffirat nicht erlaubt ist, so endet das Verfahren in Schritt 704. Ist hingegen das Ergebnis des Überprüfungsschrittes 702, dass ein Zugriff auf Chiffirate

15 erlaubt ist, so empfängt das System in Schritt 706 eine erste und zweite Kennung. Beispielsweise kennzeichnet die erste Kennung das Schlüsselpaar, welches das Schlüsselpaar ist, von welchem aus ein Entschlüsselungsvorgang von Daten stattfinden soll. Die zweite Kennung kennzeichnet entweder das zu entschlüsselnde Datenobjekt oder das letzte Schlüsselpaar in der Sequenz von Schlüsselpaaren, welches für einen

20 Entschlüsselungsvorgang verwendet werden soll.

Daraufhin werden in den Schritten 708, 710 und 712 die Chiffirate bestimmt, welche für die entsprechende Chiffirat-Entschlüsselungssequenz auf einem Pfad der Schlüsselpaare liegen, welcher durch die erste und zweite Kennung vorgegeben ist,

25 falls ein solcher Pfad existiert. Zur Suche eines solchen Pfads in dem Graphen können verschiedene an sich bekannte Verfahren verwendet werden, z.B. um einen kürzesten Pfad zu finden. So wird in Schritt 708 ein entsprechendes Chiffirat übermittelt und in Schritt 710 überprüft, ob das Chiffirat gültig ist. Hierbei kann es sich wie bereits oben erwähnt um eine Gültigkeit nach Zeitintervall, eine Gültigkeit nach Anzahl der

30 Benutzungen, um eine Gültigkeit nach Art der Benutzung handeln, etc.. Ist das ermittelte Chiffirat nicht gültig, so endet das Verfahren in Schritt 704. Ist das Chiffirat gültig, so erfolgt in Schritt 712 eine Überprüfung, ob ein weiteres Chiffirat notwendig ist, d.h. ob die Sequenz an Chiffiraten vollständig ist oder nicht. Ist die Sequenz noch nicht

vollständig, springt das Verfahren zu Schritt 708 zurück, wohingegen im Falle der Vollständigkeit der Sequenz die Chiffratsequenz in Schritt 714 bereitgestellt wird.

Bezugszeichenliste

5		
	100	Chiffprat
	102	Schlüsselpaar
	104	Schlüsselpaar
	106	Schlüsselpaar
10	108	Chiffprat
	116	verschlüsselte Datenobjekte
	200	Datenverarbeitungssystem
	202	Eingabemittel
	204	Bildschirm
15	206	Schnittstelle
	208	Prozessor
	210	Speicher
	212	Modul
	214	Modul
20	216	Chipkarte
	218	geheimer Schlüssel
	220	öffentlicher Schlüssel
	222	Prozessor
	224	Datenverarbeitungssystem
25	226	Netzwerk
	228	Datenbank
	230	Kennung
	234	Chiffprat
	236	Merkmal
30	238	Speicher
	240	Modul
	242	Modul
	244	Prozessor
	246	Schnittstelle

250	Hierarchieebene
252	Hierarchieebene
254	Hierarchieebene

Patentansprüche

1. Verfahren zur Erzeugung eines Satzes von asymmetrischen kryptografischen
5 Schlüsselpaaren, wobei der Satz von Schlüsselpaaren ein erstes Schlüsselpaar
(K1) und ein zweites Schlüsselpaar (K2) aufweist, wobei das erste Schlüsselpaar
durch einen ersten privaten (G1) und einen ersten öffentlichen Schlüssel (O1)
gebildet wird und das zweite Schlüsselpaar durch einen zweiten privaten (G2)
und einen zweiten öffentlichen Schlüssel (O2) gebildet wird, wobei dem ersten
10 und zweiten Schlüsselpaar ein erstes Chifftrat (C_G2_O1) zugeordnet ist, wobei
das erste Chifftrat durch eine Verschlüsselung des zweiten privaten Schlüssels
(G2) mit dem ersten öffentlichen Schlüssel (O1) gebildet wird, mit den folgenden
Schritten:
- Hinzufügen eines dritten asymmetrischen kryptografischen Schlüsselpaars
15 (K3) zu dem Satz von Schlüsselpaaren, wobei das dritte Schlüsselpaar durch
einen dritten privaten (G3) und einen dritten öffentlichen Schlüssel (O3)
gebildet wird,
 - Erzeugung eines zweiten Chifftrats (C_G3_O1) durch Verschlüsselung des
dritten privaten Schlüssels (G3) mit dem ersten öffentlichen Schlüssel (O1),
 - 20 – Speicherung des zweiten Chifftrats (212; 186),
wobei der Satz von Schlüsselpaaren eine gerichtete Graphstruktur aufweist,
wobei die Knoten des Graphs die Schlüsselpaare und die Kanten die Chifftrate
repräsentieren, wobei eine Abhängigkeit zwischen einem
Vorgängerschlüsselpaar und einem dem Vorgängerschlüsselpaar im Graph
25 unmittelbar nachfolgenden Nachfolgerschlüsselpaar durch ein Chifftrat gebildet
wird, wobei das Chifftrat durch Verschlüsselung des privaten Schlüssels des
Nachfolgerschlüsselpaars mit dem öffentlichen Schlüssel des
Vorgängerschlüsselpaars gebildet ist, wobei bis auf das den Wurzelknoten des
Graphs bildenden Schlüsselpaar jedes Schlüsselpaar im Graph durch
30 mindestens ein Chifftrat von einem anderen Schlüsselpaar abhängig ist.
2. Verfahren nach Anspruch 1, wobei bis auf das den Wurzelknoten des Graphs
bildenden Schlüsselpaar jedes Schlüsselpaar im Graph durch genau ein Chifftrat
von einem anderen Schlüsselpaar abhängig ist.

3. Verfahren nach einem der vorigen Ansprüche, wobei der Satz von Schlüsselpaaren zwei beliebige Schlüsselpaare mit je einem privaten und einem öffentlichen Schlüssel aufweist, ferner mit den Schritten:
 - 5 – Erzeugung eines vierten Chiffrats durch Verschlüsselung des privaten Schlüssels des ersten Schlüsselpaars der beliebigen Schlüsselpaare mit dem öffentlichen Schlüssel des zweiten Schlüsselpaars der beliebigen Schlüsselpaare,
 - Speicherung des vierten Chiffrats.
- 10 4. Verfahren nach einem der vorigen Ansprüche, wobei die Chifftrate in einer vertrauenswürdigen Stelle gespeichert werden.
5. Verfahren nach einem der vorigen Ansprüche, wobei der zweite private Schlüssel und/oder der private Nachfolgerschlüssel und/oder der private Schlüssel des ersten Schlüsselpaars der beliebigen Schlüsselpaare von einem tragbaren Datenträger empfangen wird.
- 15 6. Verfahren nach Anspruch 4, wobei der tragbare Datenträger einen Prozessor aufweist, wobei das Verfahren auf dem Prozessor des tragbaren Datenträgers durchgeführt wird.
- 20 7. Verfahren nach einem der vorigen Ansprüche, wobei zusammen mit den Chiffraten Klassifizierungsmerkmale gespeichert werden, wobei die Klassifizierungsmerkmale eine Gültigkeit der Chifftrate festlegen, wobei die Gültigkeit angibt, dass nach Ablauf der Gültigkeit eine Verwendung der Chifftrate für Datenverarbeitungsvorgänge verhindert werden soll.
- 25 8. Verfahren nach Anspruch 7, wobei es sich bei den Klassifizierungsmerkmalen um eine Gültigkeit nach Zeitintervall und/oder eine Gültigkeit nach Anzahl der Benutzungen und/oder eine Gültigkeit nach Art der Benutzung handelt.
- 30 9. Computerprogrammprodukt mit von einem Prozessor ausführbaren Instruktionen zur Durchführung der Verfahrensschritte des Verfahrens nach einem der vorigen Ansprüche.
- 35

10. Datenverarbeitungssystem zur Erzeugung eines Satzes von asymmetrischen kryptografischen Schlüsselpaaren, wobei der Satz von Schlüsselpaaren ein erstes Schlüsselpaar (K1) und ein zweites Schlüsselpaar (K2) aufweist, wobei das erste Schlüsselpaar durch einen ersten privaten (G1) und einen ersten öffentlichen Schlüssel (O1) gebildet wird und das zweite Schlüsselpaar durch einen zweiten privaten (G2) und einen zweiten öffentlichen Schlüssel (O2) gebildet wird, wobei dem ersten und zweiten Schlüsselpaar ein erstes Chifftrat (C_G2_O1) zugeordnet ist, wobei das Chifftrat durch eine Verschlüsselung des zweiten privaten Schlüssels (G2) mit dem ersten öffentlichen Schlüssel (O1) gebildet wird, wobei das Datenverarbeitungssystem umfasst:
- Mittel zum Hinzufügen eines dritten asymmetrischen kryptografischen Schlüsselpaars (K3) zu dem Satz von Schlüsselpaaren, wobei das dritte Schlüsselpaar durch einen dritten privaten (G3) und einen dritten öffentlichen Schlüssel (O3) gebildet wird,
 - Mittel zur Erzeugung eines zweiten Chifftrats (C_G3_O1) durch Verschlüsselung des dritten privaten Schlüssels (G3) mit dem ersten öffentlichen Schlüssel (O1),
 - Mittel zur Speicherung des zweiten Chifftrats (212; 186) ,
- wobei der Satz von Schlüsselpaaren eine gerichtete Graphstruktur aufweist, wobei die Knoten des Graphs die Schlüsselpaare und die Kanten die Chifftrate repräsentieren, wobei eine Abhängigkeit zwischen einem Vorgängerschlüsselpaar und einem dem Vorgängerschlüsselpaar im Graph unmittelbar nachfolgenden Nachfolgerschlüsselpaar durch ein Chifftrat gebildet wird, wobei das Chifftrat durch Verschlüsselung des privaten Schlüssels des Nachfolgerschlüsselpaars mit dem öffentlichen Schlüssel des Vorgängerschlüsselpaars gebildet ist, wobei bis auf das den Wurzelknoten des Graphs bildenden Schlüsselpaar jedes Schlüsselpaar im Graph durch mindestens ein Chifftrat von einem anderen Schlüsselpaar abhängig ist..
11. Verfahren zur Bereitstellung von Chiffraten, wobei die Chifftrate einem Satz von asymmetrischen kryptografischen Schlüsselpaaren zugeordnet sind, wobei der Satz von Schlüsselpaaren zusammen mit den Chiffraten eine gerichtete Graphstruktur aufweist, wobei die Knoten des Graphs die Schlüsselpaare repräsentieren und die Kanten die Chifftrate repräsentieren, wobei eine

Abhängigkeit zwischen einem Vorgängerschlüsselpaar und einem dem Vorgängerschlüsselpaar im Graph unmittelbar nachfolgenden

Nachfolgerschlüsselpaar durch ein Chifftrat gebildet wird, wobei das Chifftrat

durch Verschlüsselung des privaten Schlüssels des Nachfolgerschlüsselpaars

mit dem öffentlichen Schlüssel des Vorgängerschlüsselpaars gebildet ist, wobei das Verfahren die Chifftrat-Bereitstellungsschritte umfasst:

- Empfang einer ersten und einer zweiten Kennung, wobei die erste Kennung einem ersten der Knoten zugeordnet ist und die zweite Kennung einem zweiten der Knoten zugeordnet ist,

- Ermittlung aller Chifftrate, welche in der Graphstruktur eine Abhängigkeit zwischen dem ersten der Knoten und dem letzten der Knoten beschreiben,

- Bereitstellung der ermittelten Sequenz von Chiffraten.

12. Verfahren nach Anspruch 11, wobei bis auf das den Wurzelknoten des Graphs

bildenden Schlüsselpaar jedes Schlüsselpaar im Graph durch mindestens ein

Chifftrat von einem anderen Schlüsselpaar abhängig ist.

13. Verfahren nach einem der Ansprüche 11 oder 12, wobei die Sequenz von

Chiffraten nach einer erfolgreichen Authentisierung ermittelt und/oder

bereitgestellt wird.

14. Verfahren nach einem der vorigen Ansprüche 11 bis 13, wobei die Chifftrate mit

Klassifizierungsmerkmalen verknüpft sind, wobei die Klassifizierungsmerkmale

eine Gültigkeit der Chifftrate festlegen, wobei die Gültigkeit angibt, dass nach

Ablauf der Gültigkeit eine Bereitstellung der Chifftrate verhindert werden soll,

wobei eine Bereitstellung der Chifftrate nur dann erfolgt, wenn die Gültigkeit der Chifftrate erfolgreich validiert wurde.

15. Verfahren nach einem der Ansprüche 11 bis 14, wobei die zweite Kennung

einem Datenobjekt zugeordnet ist, wobei das Datenobjekt mit dem öffentlichen

Schlüssel desjenigen der Knoten verschlüsselt ist, dem das Datenobjekt

zugeordnet ist.

16. Verfahren nach Anspruch 15, ferner mit dem Schritt einer Datenentschlüsselung,

wobei die Datenentschlüsselung die Schritte umfasst:

- Ermittlung eines privaten Schlüssels durch Entschlüsselung des ersten Chiffrats der Sequenz von Chiffraten mit dem privaten Schlüssel des Schlüsselpaars, welches dem ersten der Knoten zugeordnet ist,
 - Ermittlung eines nächsten privaten Schlüssels durch Entschlüsselung des nächsten Chiffrats der Sequenz von Chiffraten mit dem zuvor ermittelten privaten Schlüssel und Wiederholung dieses Schrittes solange, bis das letzte Chifftrat der Sequenz von Chiffraten entschlüsselt wurde,
 - Entschlüsselung des verschlüsselten Datenobjekts.
- 10 17. Verfahren nach einem der vorigen Ansprüche 15 oder 16, wobei der Schritt der Datenentschlüsselung und die Chifftrat-Bereitstellungsschritte von unterschiedlichen Datenverarbeitungssystemen durchgeführt werden.
- 15 18. Verfahren nach Anspruch 17, wobei der Schritt der Datenentschlüsselung durch eine vertrauenswürdige Stelle durchgeführt wird.
- 20 19. Computerprogrammprodukt mit von einem Prozessor ausführbaren Instruktionen zur Durchführung der Verfahrensschritte des Verfahrens nach einem der vorigen Ansprüche 11 bis 18.
- 25 20. Datenverarbeitungssystem zur Bereitstellung von Chiffraten, wobei die Chifftrate einem Satz von asymmetrischen kryptografischen Schlüsselpaaren zugeordnet sind, wobei der Satz von Schlüsselpaaren eine gerichtete Graphstruktur aufweist, wobei die Knoten des Graphs die Schlüsselpaare repräsentieren und wobei die Kanten des Graphs die Chifftrate repräsentieren, wobei eine Abhängigkeit zwischen einem Vorgängerschlüsselpaar und einem dem Vorgängerschlüsselpaar im Graph unmittelbar nachfolgenden Nachfolgerschlüsselpaar durch ein Chifftrat gebildet wird, wobei das Chifftrat durch Verschlüsselung des privaten Schlüssels des Nachfolgerschlüsselpaars mit dem öffentlichen Schlüssel des Vorgängerschlüsselpaars gebildet ist, wobei das Datenverarbeitungssystem umfasst:
- 30
- Mittel zum Empfang einer ersten und einer zweiten Kennung, wobei die erste Kennung einem ersten der Knoten zugeordnet ist und die zweite Kennung einem zweiten der Knoten zugeordnet ist,

- Mittel zur Ermittlung aller Chiffrate, welche in der Graphstruktur eine Abhängigkeit zwischen dem ersten der Knoten und dem letzten der Knoten beschreiben,
- Mittel zur Bereitstellung der ermittelten Sequenz von Chiffraten.

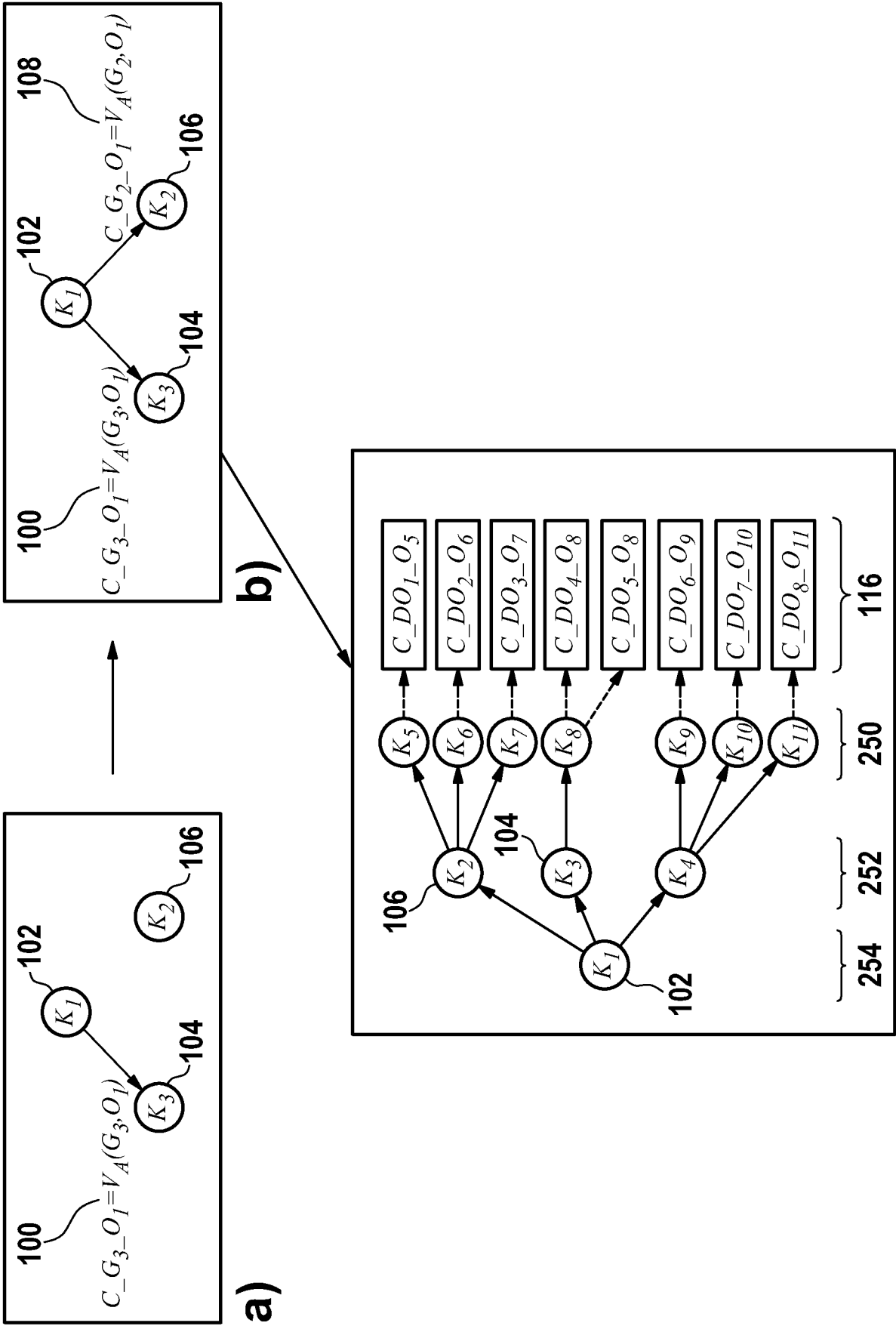


Fig. 1

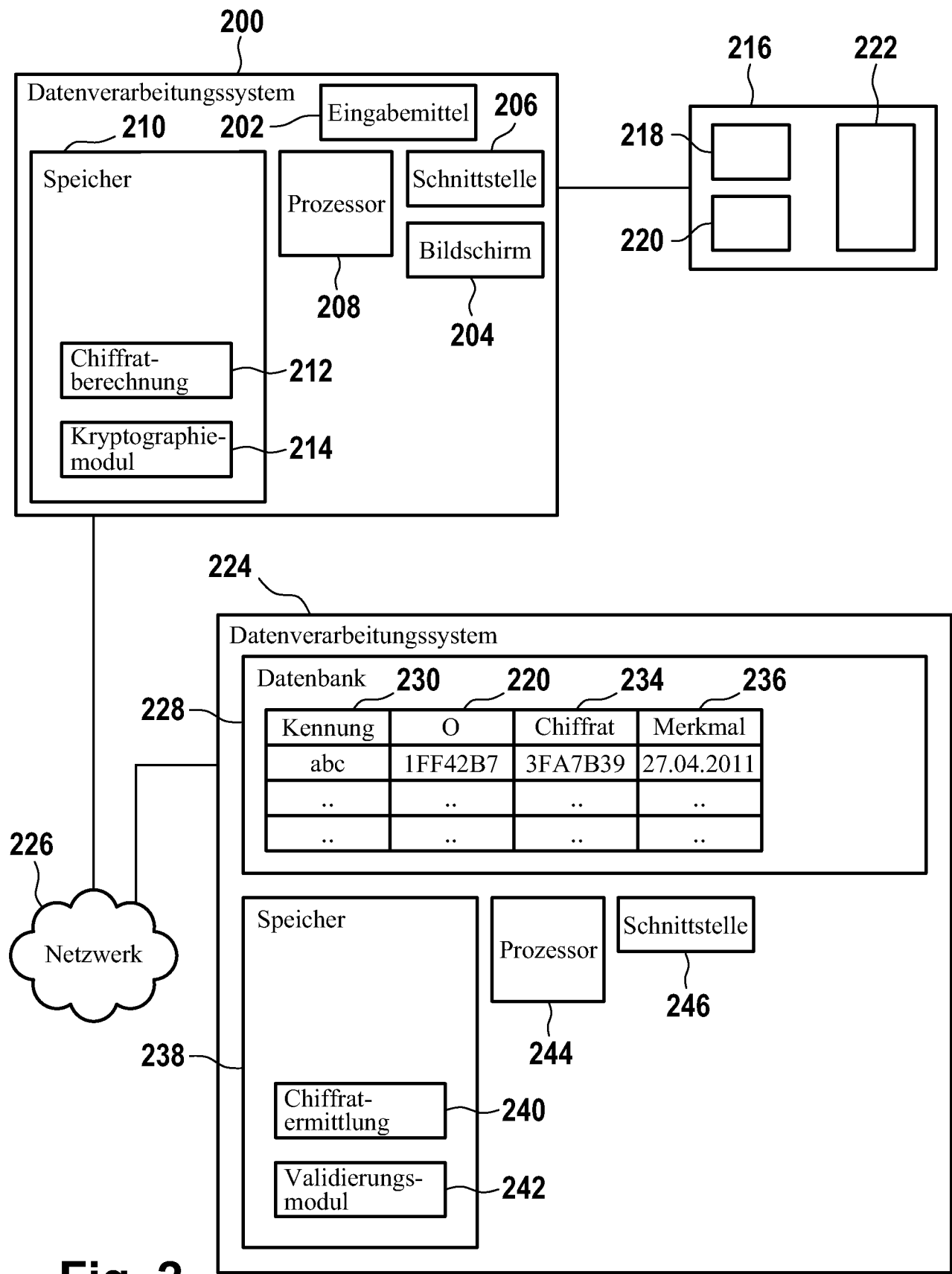


Fig. 2

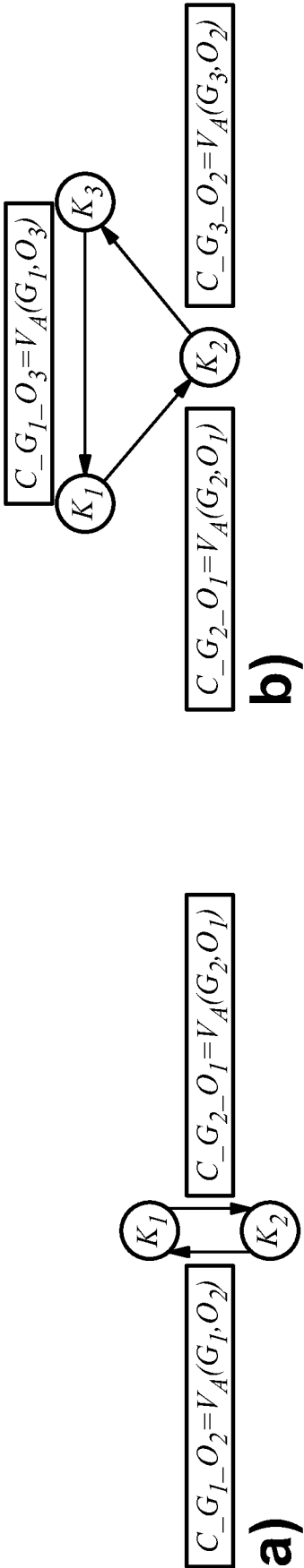


Fig. 3

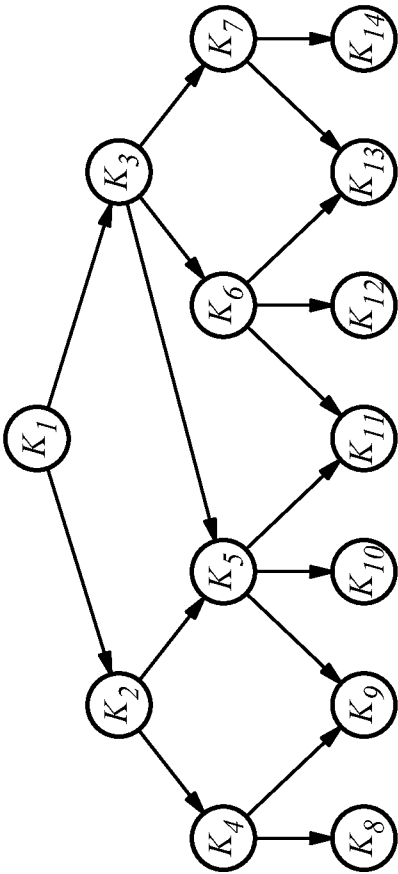


Fig. 4

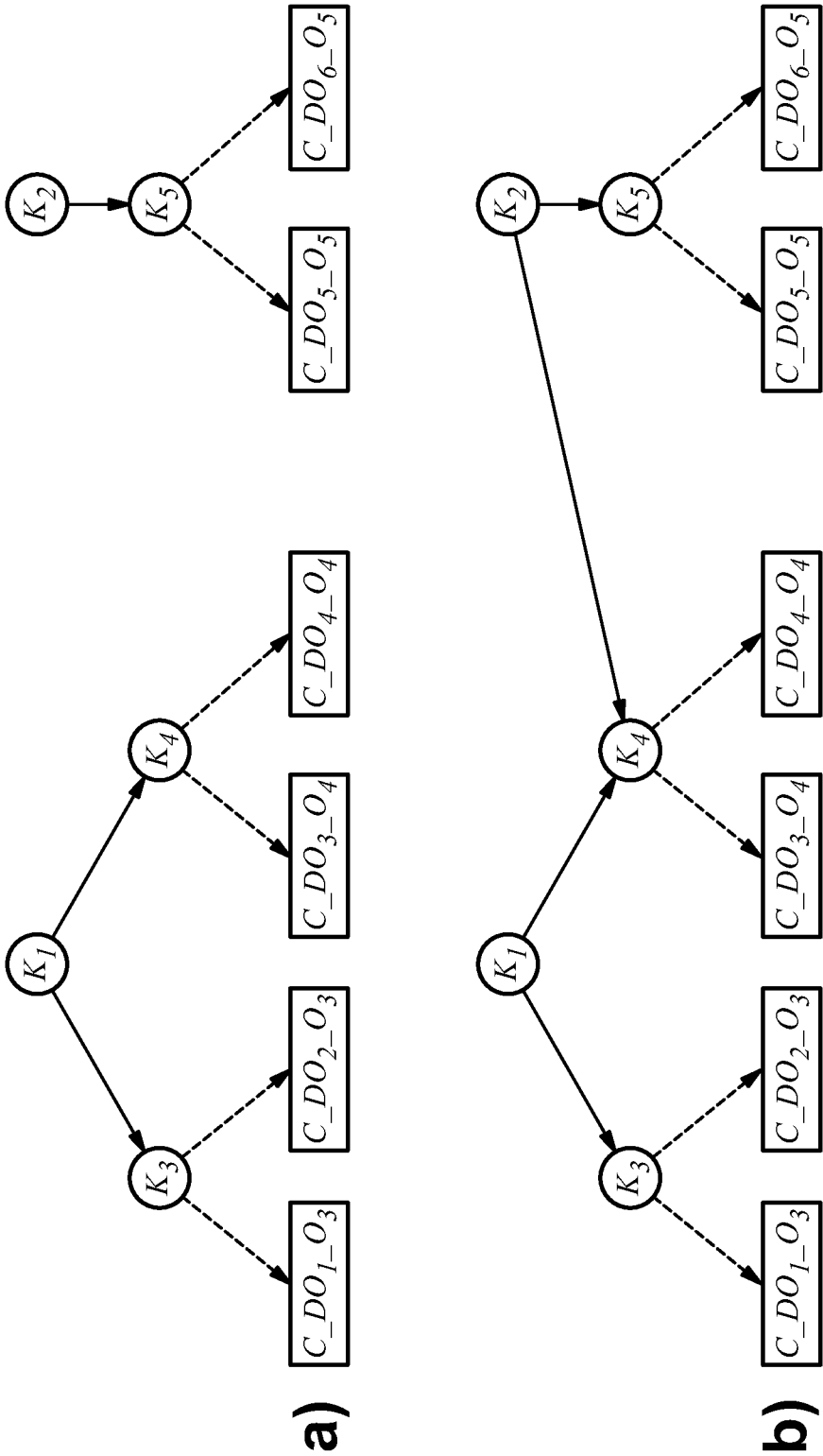
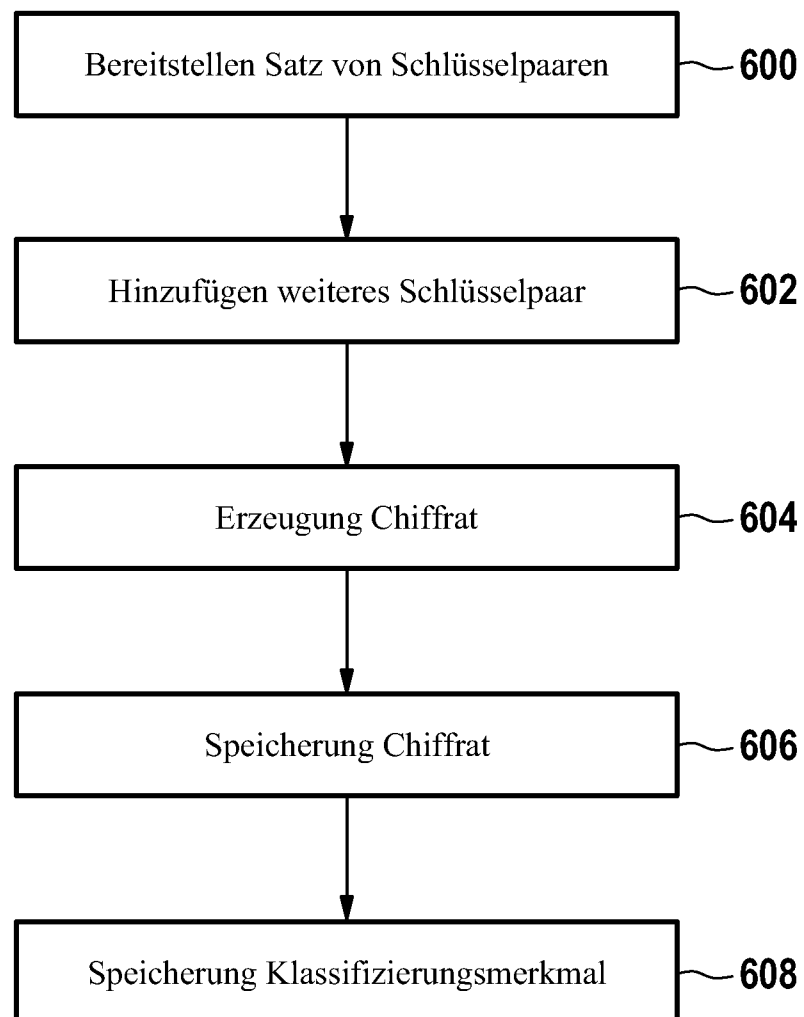
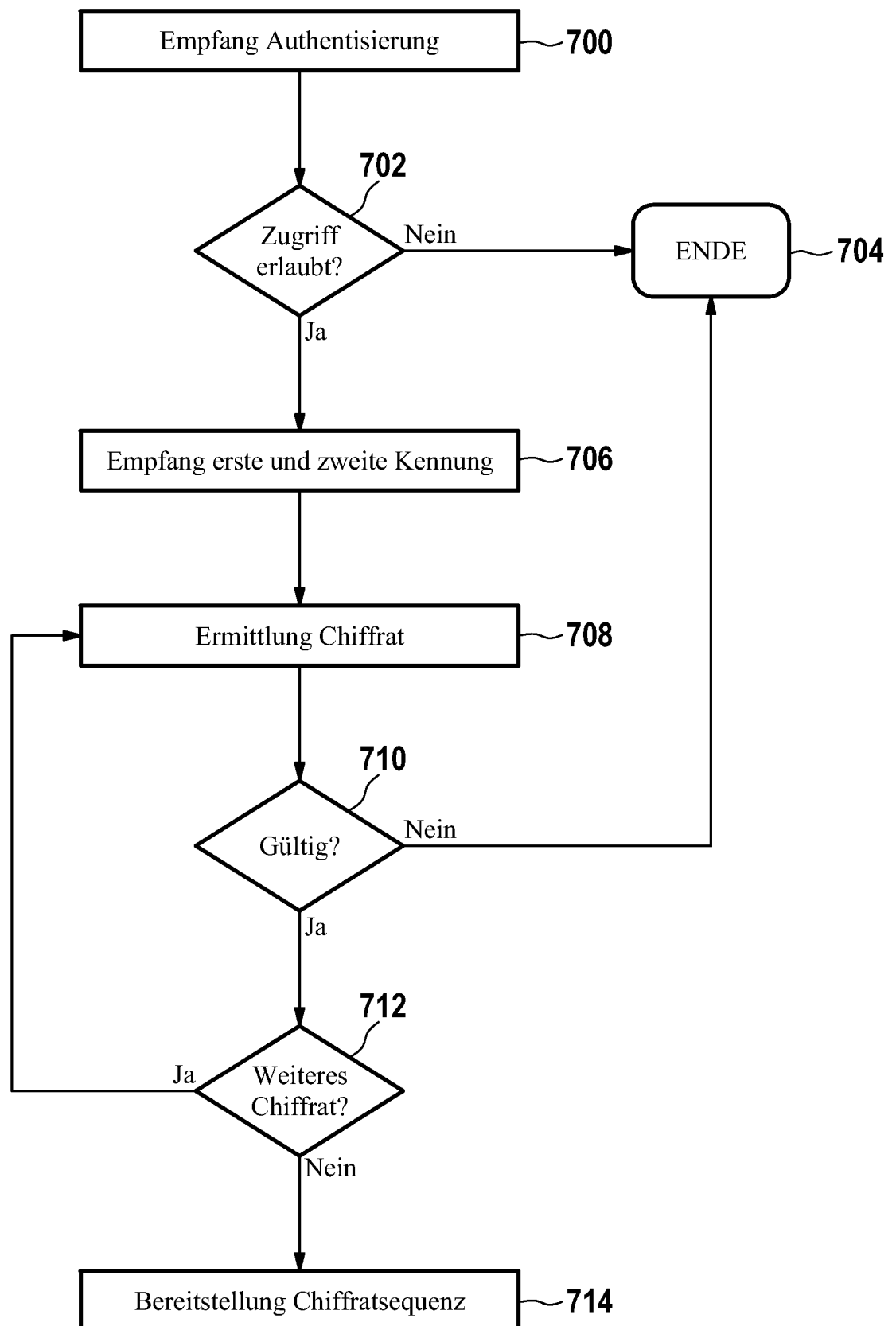


Fig. 5

**Fig. 6**

**Fig. 7**

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2010/052733

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	SANDHU R S: "On some cryptographic solutions for access control in a tree hierarchy" PROCEEDINGS 1987 FALL JOINT COMPUTER CONFERENCE - EXPLORING TECHNOLOGY: TODAY AND TOMORROW (CAT. NO.87CH2468-7) IEEE COMPUT. SOC. PRESS WASHINGTON, DC, USA, 1987, pages 405-410, XP007912584 ISBN: 0-8186-0811-0 Abschnitt 1 Abschnitt 3.2 ----- -/--	1-20

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

14 April 2010

Date of mailing of the international search report

20/04/2010

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Schäfer, Andreas

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2010/052733

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EHUD GUIDES: "The Design of a Cryptography Based Secure File System" IEEE TRANSACTIONS ON SOFTWARE ENGINEERING, vol. 6, no. 5, September 1980 (1980-09), pages 411-420, XP007912572 abstract Section IV. Hierarchical Protection Specification -----	1-20
X	KUO F H ET AL: "Cryptographic key assignment scheme for dynamic access control in a user hierarchy" IEE PROCEEDINGS: COMPUTERS AND DIGITAL TECHNIQUES, IEE, GB LNKD- DOI:10.1049/IP-CDT:19990311, vol. 146, no. 5, 22 September 1999 (1999-09-22), pages 235-240, XP006013180 ISSN: 1350-2387 abstract Abschnitt 3 -----	1-20
X	ATALLAH M J ET AL: "DYNAMIC AND EFFICIENT KEY MANAGEMENT FOR ACCESS HIERARCHIES" PROCEEDINGS OF THE 12TH. ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY. (CCS'05). ALEXANDRIA, VA, NOV. 7 - 11, 2005; [ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY], NEW YORK, NY : ACM, US LNKD- DOI:10.1145/1102120.1102147, vol. CONF. 12, 7 November 2005 (2005-11-07), pages 190-201, XP001241630 ISBN: 978-1-59593-226-6 Abschnitt 4 figure 1 -----	1-20
X	CHUNG ET AL: "Access control in user hierarchy based on elliptic curve cryptosystem" INFORMATION SCIENCES, AMSTERDAM, NL LNKD- DOI:10.1016/J.INS.2007.08.001, vol. 178, no. 1, 9 October 2007 (2007-10-09), pages 230-243, XP022289858 ISSN: 0020-0255 Abschnitt 3 -----	1-20

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES

INV. G06F21/00

ADD.

Nach der internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)

G06F

Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

EPO-Internal

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	SANDHU R S: "On some cryptographic solutions for access control in a tree hierarchy" PROCEEDINGS 1987 FALL JOINT COMPUTER CONFERENCE – EXPLORING TECHNOLOGY: TODAY AND TOMORROW (CAT. NO.87CH2468-7) IEEE COMPUT. SOC. PRESS WASHINGTON, DC, USA, 1987, Seiten 405-410, XP007912584 ISBN: 0-8186-0811-0 Abschnitt 1 Abschnitt 3.2 ----- -/--	1-20

☒ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen
 ☐ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

14. April 2010

Absendedatum des internationalen Recherchenberichts

20/04/2010

Name und Postanschrift der Internationalen Recherchenbehörde

Europäisches Patentamt, P.B. 5818 Patentlaan 2
 NL – 2280 HV Rijswijk
 Tel. (+31-70) 340-2040,
 Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Schäfer, Andreas

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	EHUD GUDES: "The Design of a Cryptography Based Secure File System" IEEE TRANSACTIONS ON SOFTWARE ENGINEERING, Bd. 6, Nr. 5, September 1980 (1980-09), Seiten 411-420, XP007912572 Zusammenfassung Section IV. Hierarchical Protection Specification -----	1-20
X	KUO F H ET AL: "Cryptographic key assignment scheme for dynamic access control in a user hierarchy" IEE PROCEEDINGS: COMPUTERS AND DIGITAL TECHNIQUES, IEE, GB LNKD- DOI:10.1049/IP-CDT:19990311, Bd. 146, Nr. 5, 22. September 1999 (1999-09-22), Seiten 235-240, XP006013180 ISSN: 1350-2387 Zusammenfassung Abschnitt 3 -----	1-20
X	ATALLAH M J ET AL: "DYNAMIC AND EFFICIENT KEY MANAGEMENT FOR ACCESS HIERARCHIES" PROCEEDINGS OF THE 12TH. ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY. (CCS'05). ALEXANDRIA, VA, NOV. 7 - 11, 2005; [ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY], NEW YORK, NY : ACM, US LNKD- DOI:10.1145/1102120.1102147, Bd. CONF. 12, 7. November 2005 (2005-11-07), Seiten 190-201, XP001241630 ISBN: 978-1-59593-226-6 Abschnitt 4 Abbildung 1 -----	1-20
X	CHUNG ET AL: "Access control in user hierarchy based on elliptic curve cryptosystem" INFORMATION SCIENCES, AMSTERDAM, NL LNKD- DOI:10.1016/J.INS.2007.08.001, Bd. 178, Nr. 1, 9. Oktober 2007 (2007-10-09), Seiten 230-243, XP022289858 ISSN: 0020-0255 Abschnitt 3 -----	1-20