(19) SCHWEIZERISCHE EIDGENOSSENSCHAFT
EIDGENÖSSISCHES INSTITUT FÜR GEISTIGES EIGENTUM

(11) CH 708 239 B1

(51) Int. Cl.: H04L 9/08 (2006.01)
G06F 21/44 (2013.01)

Erfindungspatent für die Schweiz und Liechtenstein
Schweizerisch-liechtensteinischer Patentschutzvertrag vom 22. Dezember 1978

# (12) PATENTSCHRIFT

(21) Anmeldenummer: 00973/14

(22) Anmeldedatum: 26.06.2014

(43) Anmeldung veröffentlicht: 31.12.2014

(30) Priorität: 27.06.2013 US 61/839,961

(24) Patent erteilt: 28.02.2019

(45) Patentschrift veröffentlicht: 28.02.2019

(73) Inhaber:
Infosec Global Inc., 2225 Sheppard Avenue West
Suite 1015
Toronto, Ontario M2J 5C2 (CA)

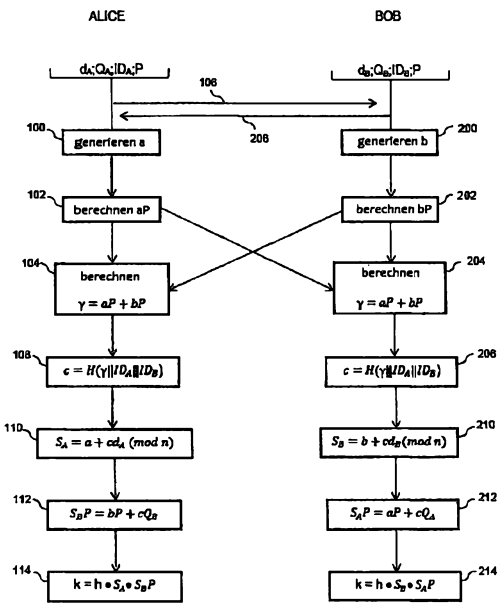
(72) Erfinder:
Scott A. Vanstone, Campbellville, Ontario L0P 1B0 (CA)
Adrian Antipa, Brampton, Ontario L6P 03E3 (CA)

(74) Vertreter:
Isler & Pedrazzini AG, Postfach 1772
8027 Zürich (CH)

## (54) Schlüsseleinigungsprotokoll.

(57) Die Erfindung betrifft ein Verfahren zur Ausführung eines Protokolls zur Einigung auf einen Schlüssel, das zwischen einem Paar Entitäten ausgeführt wird, die über ein Datenkommunikationssystem kommunizieren, ein Datenkommunikationssystem mit einem Paar kryptografischer Korrespondentengeräte, die konfiguriert sind, um das Verfahren umzusetzen, sowie ein kryptografisches Korrespondentengerät.

Beim erfindungsgemässen Verfahren wird von jeder Entität ein privater Sitzungsschlüssel (100, 200) und ein kryptografischer öffentlicher Sitzungsschlüssel (102, 202) generiert. Der öffentliche Sitzungsschlüssel (102, 202) wird von einer Entität an die jeweils andere Entität weitergegeben. Durch Kombinieren der öffentlichen Sitzungsschlüssel und der Identitäten der Entitäten wird ein gemeinsamer Wert generiert (104, 204). Dieser gemeinsame Wert wird mit dem privaten Sitzungsschlüssel und einem langfristigen privaten Sitzungsschlüssel der jeweiligen Entität kombiniert und so für jede Entität ein geheimer Wert generiert (108, 208). Das Berechnen eines ephemeren Wertes (112, 212) an jeder Entität umfasst das Kombinieren des öffentlichen Sitzungsschlüssels und eines langfristigen öffentlichen Schlüssels der anderen Entität sowie des gemeinsamen Wertes. Aus dem ephemeren Wert und dem geheimen Wert wird an jeder Entität eine geteilte geheime Information (114, 214) generiert, um einen geteilten Schlüssel zu erzielen.



## Beschreibung

### Technisches Gebiet

**[0001]** Die vorliegende Erfindung betrifft Datenkommunikationssysteme und Protokolle, die in derartigen Systemen verwendet werden.

### Allgemeiner Stand der Technik

**[0002]** Datenkommunikationssysteme werden verwendet, um Informationen zwischen Geräten auszutauschen. Die auszutauschenden Informationen umfassen Daten, die als Folgen von digitalen Bits organisiert sind, die formatiert sind, um für andere Geräte erkennbar zu sein und die Verarbeitung und/oder Wiederherstellung der Informationen zu erlauben.

**[0003]** Der Informationsaustausch kann über ein öffentlich zugängliches Netzwerk erfolgen, wie etwa über eine Kommunikationsverbindung zwischen zwei Geräten, über ein dediziertes Netzwerk innerhalb eines Betriebs oder kann zwischen zwei Geräten innerhalb der gleichen dedizierten Komponente erfolgen, wie etwa innerhalb eines Computers oder eines Verkaufsstellengeräts.

**[0004]** Die Geräte können von relativ grossen Computersystemen bis zu Telekommunikationsgeräten, Mobiltelefonen, Überwachungsgeräten, Sensoren, elektronischen Geldbörsen und Chipkarten und zahlreichen Geräten, die verbunden sind, um Daten zwischen zwei oder mehreren derartigen Geräten zu übertragen, reichen.

**[0005]** Es wurde eine grosse Anzahl von Kommunikationsprotokollen entwickelt, um den Austausch von Daten zwischen verschiedenen Geräten zu ermöglichen. Die Kommunikationsprotokolle ermöglichen den Austausch von Daten auf robuste Art und Weise, häufig mit einer Funktion der Fehlerkorrektur und Fehlerermittlung, und das die Daten dem beabsichtigten Empfänger zugeleitet und zur weiteren Verwendung wiederhergestellt werden.

**[0006]** Da die Daten für andere Geräte zugänglich sein können, sind sie für Abfangen und Beobachtung oder Manipulation anfällig. Die Empfindlichkeit der Informationen erfordert, dass Massnahmen getroffen werden, um die Informationen zu sichern und ihre Integrität sicherzustellen.

**[0007]** Eine gewisse Anzahl von Techniken, die insgesamt als Verschlüsselungsprotokolle und Authentifizierungsprotokolle bezeichnet werden, wurden entwickelt, um die notwendigen Attribute bereitzustellen und die Sicherheit und/oder Integrität beim Austausch von Informationen sicherzustellen. Diese Techniken verwenden einen Schlüssel, der mit den Daten kombiniert wird.

**[0008]** Es gibt zwei Hauptarten von Kryptosystemen, welche die Protokolle umsetzen, nämlich Kryptosysteme mit symmetrischem Schlüssel und Kryptosysteme mit asymmetrischem oder öffentlichem Schlüssel. Bei einem Kryptosystem mit symmetrischem Schlüssel teilen die Geräte, die Informationen austauschen, einen gemeinsamen Schlüssel, der nur den Geräten bekannt ist, die dazu gedacht sind, die Informationen zu teilen. Systeme mit symmetrischem Schlüssel bieten den Vorteil, dass sie relativ schnell sind und demnach in der Lage sind, auch mit begrenzter Rechenleistung grosse Datenmengen in relativ kurzer Zeit zu verarbeiten. Die Schlüssel müssen jedoch auf gesicherte Art und Weise an die verschiedenen Geräte ausgeteilt werden, was zu erhöhtem Aufwand und grösserer Anfälligkeit führt, wenn der Schlüssel fragwürdig ist.

**[0009]** Kryptosysteme mit asymmetrischem oder öffentlichem Schlüssel verwenden ein mit jedem Gerät verknüpftes Paar Schlüssel, von denen einer öffentlich und der andere privat ist. Der öffentliche Schlüssel und der private Schlüssel stehen durch ein «schwieriges» mathematisches Problem in Zusammenhang, sodass, selbst wenn der öffentliche Schlüssel und das zugrundeliegende Problem bekannt sind, der private Schlüssel nicht in einem machbaren Zeitraum wiederhergestellt werden kann. Ein derartiges Problem ist die Faktorisierung des Produkts zweier grosser Primzahlen, wie sie bei RSA-Kryptosystemen verwendet wird. Ein anderes ist das diskrete Logarithmusproblem in einer endlichen Gruppe. Ein Generator, $\alpha$, der zugrundeliegenden Gruppe wird als Systemparameter identifiziert, und eine zufällige Ganzzahl, k, wird zur Verwendung als privater Schlüssel generiert. Um einen öffentlichen Schlüssel, K, zu erzielen, wird eine k-fache Gruppenoperation ausgeführt, sodass $K = f(\alpha, k)$.

**[0010]** Es können verschiedene Gruppen in Kryptosystemen mit diskretem Logarithmus verwendet werden, wozu die multiplikative Gruppe eines endlichen Felds, die Gruppe von Ganzzahlen in einer endlichen zyklischen Gruppe p. Ordnung, die gewöhnlich mit $Zp^*$ bezeichnet wird und aus den Ganzzahlen 0 bis p–1 besteht, gehören. Die Gruppenoperation ist eine Multiplikation, sodass $K = f(\alpha^k)$.

**[0011]** Eine andere Gruppe, die zur besseren Sicherheit verwendet wird, ist eine elliptische Kurvengruppe. Die elliptische Kurvengruppe besteht aus Paaren von Elementen, von denen eines mit x und das andere mit y bezeichnet wird, in einem Feld, das die Gleichung der gewählten elliptischen Kurve erfüllt. Für eine elliptische Kurvengruppe p. Ordnung würde die elliptische Kurve im Allgemeinen durch die Beziehung $y^2 \bmod p = x^3 + ax + b \bmod p$ definiert. Andere Kurven werden für verschiedene Gruppen verwendet, wie es wohlbekannt ist. Jedes derartige Elementepaar ist ein Punkt auf der Kurve, und ein Generator der Gruppe wird als Punkt P bezeichnet. Die Gruppenoperation ist eine Addition, sodass ein privater Schlüssel k einen entsprechenden öffentlichen Schlüssel f(kP) aufweist.

**[0012]** Kryptosysteme mit öffentlichem Schlüssel reduzieren die Infrastruktur, die bei einem Kryptosystem mit symmetrischem Schlüssel notwendig ist. Ein Gerät kann eine Ganzzahl k generieren und kann den entsprechenden öffentlichen

Schlüssel kP generieren. Der öffentliche Schlüssel wird veröffentlicht, sodass er anderen Geräten zur Verfügung steht. Das Gerät kann dann ein geeignetes Signaturprotokoll verwenden, um eine Nachricht unter Verwendung des privaten Schlüssels k zu signieren, und andere Geräte können die Integrität der Nachricht unter Verwendung des öffentlichen Schlüssels kP bestätigen.

**[0013]** Ähnlich kann ein Gerät eine Nachricht, die an ein anderes Gerät gesendet werden soll, unter Verwendung des öffentlichen Schlüssels des anderen Gerätes verschlüsseln. Die Nachricht kann dann von dem anderen Gerät unter Verwendung des privaten Schlüssels wiederhergestellt werden. Diese Protokolle sind jedoch rechenintensiv und demnach im Vergleich mit den Protokollen von symmetrischen Kryptosystemen relativ langsam.

**[0014]** Kryptosysteme mit öffentlichem Schlüssel können ebenfalls verwendet werden, um einen Schlüssel zu erstellen, den sich zwei Geräte teilen. In seiner einfachsten Form, wie sie von Diffie-Hellman vorgeschlagen wird, sendet jedes Gerät einen öffentlichen Schlüssel an das andere Gerät. Die beiden Geräte kombinieren dann die empfangenen öffentlichen Schlüssel mit ihrem privaten Schlüssel, um einen geteilten Schlüssel zu erzielen.

**[0015]** Ein Gerät, das gewöhnlich als Entität (oder Korrespondent) bezeichnet wird, Alice, generiert einen privaten Schlüssel $k_a$ und sendet einem anderen Gerät bzw. einer anderen Entität, Bob, den öffentlichen Schlüssel $k_aP$.

**[0016]** Bob generiert einen privaten Schlüssel $k_b$ und sendet Alice den öffentlichen Schlüssel $k_bP$.

**[0017]** Alice berechnet $k_a \cdot k_bP$ und Bob berechnet $k_b \cdot k_aP$, sodass sie einen gemeinsamen Schlüssel $K = k_ak_bp = k_bk_aP$ teilen. Der geteilte Schlüssel kann dann in einem symmetrischen Schlüsselprotokoll verwendet werden. Weder Alice noch Bob kann den gegenseitigen privaten Schlüssel wiederherstellen, und Dritte können den geteilten Schlüssel nicht nachvollziehen.

**[0018]** Um die Integrität des geteilten Schlüssels sicherzustellen und um Angriffe abzuweisen, die entwickelt wurden, um den geteilten Schlüssel und/oder die privaten Schlüssel innerhalb des geteilten Schlüssels wiederherzustellen oder zu ersetzen, wurden Protokolle zum Erstellen von Schlüsseln entwickelt.

**[0019]** Die Erstellung von Schlüsseln ist der Prozess, durch den zwei (oder mehrere) Entitäten einen geteilten geheimen Schlüssel erstellen. Der Schlüssel wird anschliessend verwendet, um ein kryptografisches Ziel zu erreichen, wie etwa die Vertraulichkeit oder die Datenintegrität.

**[0020]** Im weitesten Sinne gibt es zwei Arten von Protokollen zum Erstellen von Schlüsseln: Schlüsseltransportprotokolle, bei denen ein Schlüssel von einer Entität angelegt wird und gesichert an die zweite Entität übertragen wird, und Schlüsseleinigungsprotokolle, bei denen beide Parteien Informationen beisteuern, die zusammen den geteilten geheimen Schlüssel erstellen. Die vorliegende Anmeldung betrifft Schlüsseleinigungsprotokolle für Kryptosysteme mit asymmetrischem (öffentlichem) Schlüssel.

**[0021]** Wenn Alice und Bob zwei rechtschaffene Entitäten, d.h. legitime Entitäten, sind, welche die Schritte eines Protokolls richtig ausführen, dann kann man informell von einem Schlüsseleinigungsprotokoll sagen, dass es eine implizite Schlüsselauthentifizierung (von Bob an Alice) bereitstellt, wenn sich die Entität Alice sicher ist, dass keine andere Entität ausser einer spezifisch identifizierten zweiten Identität Bob möglicherweise den Wert eines bestimmten geheimen Schlüssels erfahren kann. Der Besitz der impliziten Schlüsselauthentifizierung bedeutet nicht unbedingt, dass sich Alice sicher ist, dass Bob tatsächlich den Schlüssel besitzt, sondern dass sie sich sicher ist, dass niemand ausser Bob den Schlüssel besitzt. Ein Schlüsseleinigungsprotokoll, das eine implizite Schlüsselauthentifizierung für die beiden teilnehmenden Entitäten bereitstellt, wird als authentifiziertes Schlüsseleinigungs-(AK-)Protokoll bezeichnet.

**[0022]** Informell wird von einem Schlüsseleinigungsprotokoll gesagt, dass es eine Schlüsselbestätigung (von Bob an Alice) bereitstellt, falls sich die Entität Alice sicher ist, dass die zweite Entität Bob tatsächlich im Besitz eines bestimmten geheimen Schlüssels ist. Falls sowohl die implizite Schlüsselauthentifizierung als auch die Schlüsselbestätigung (von Bob an Alice) bereitgestellt werden, dann wird von dem Schlüsselerstellungsprotokoll gesagt, dass es eine explizite Schlüsselauthentifizierung (von Bob an Alice) bereitstellt. Ein Schlüsseleinigungsprotokoll, das eine explizite Schlüsselauthentifizierung für die beiden teilnehmenden Entitäten bereitstellt, wird als Protokoll mit authentifizierter Schlüsseleinigung mit Schlüsselbestätigung (AKC) bezeichnet. Eine ausführliche Abhandlung über die Erstellung von Schlüsseln wird in Kapitel 12 aus «Handbook of Applied Cryptography» von Menezes, van Oorshot und Vanstone, dessen Inhalt hiermit zur Bezugnahme übernommen wird, bereitgestellt.

**[0023]** Bei der Trennung der Schlüsselbestätigung von der impliziten Schlüsselauthentifizierung ist äusserste Vorsicht geboten. Falls ein AK-Protokoll, das keine Schlüsselbestätigung bietet, verwendet wird, dann ist es wünschenswert, wie es in dem Artikel von 1997 von S. Blake-Wilson, D. Johnson und A. Menezes unter dem Titel «Key agreement protocols and their security analysis» angeführt wird, dass der vereinbarte Schlüssel vor der kryptografischen Verwendung bestätigt wird. Das kann auf verschiedene Weisen erreicht werden. Falls der Schlüssel beispielsweise anschliessend verwendet werden soll, um Vertraulichkeit zu erreichen, dann kann die Verschlüsselung mit dem Schlüssel mit einigen (sorgfältig ausgewählten) bekannten Daten beginnen. Andere Systeme können eine Schlüsselbestätigung während eines «Echtzeit-»Telefongesprächs bereitstellen. Das Trennen der Schlüsselbestätigung von der impliziten Schlüsselauthentifizierung ist manchmal wünschenswert, weil es eine gewisse Flexibilität bei der bestimmten Umsetzung erlaubt, die gewählt wird, um die Schlüsselbestätigung zu erreichen, und somit die Arbeitslast der Schlüsselbestätigung von dem Erstellungsmechanismus auf die Anwendung überträgt.

**[0024]** Zahlreiche auf Diffie-Helman basierende AK- und AKC-Protokolle wurden in den letzten Jahren vorgeschlagen; bei vielen hat sich jedoch später herausgestellt, dass sie Sicherheitsfehler aufweisen. Die Hauptprobleme bestanden darin, dass entsprechende Bedrohungsmodelle und die Ziele von gesicherten AK- und AKC-Protokollen keine formelle Definition hatten. Blake-Wilson, Johnson und Menezes, die frühere Arbeiten von Bellare und Rogaway in der symmetrischen Umgebung anpassten, stellten ein formelles Modell für verteiltes Rechnen und rigorose Definitionen der Ziele der gesicherten AK- und AKC-Protokolle innerhalb dieses Modells bereit. Es wurden konkrete AK- und AKC-Protokolle vorgeschlagen und innerhalb dieses Rahmens in dem zufallsmässigen Vorhersagemodell als gesichert nachgewiesen.

**[0025]** Man geht davon aus, dass ein gesichertes Protokoll in der Lage sein sollte, sowohl passiven Angriffen (bei denen ein Gegner versucht zu verhindern, dass ein Protokoll seine Ziele erreicht, indem er einfach rechtschaffene Entitäten beobachtet, die das Protokoll ausführen) als auch aktiven Angriffen (bei denen ein Gegner zusätzlich die Kommunikationen durch Einschalten, Löschen, Ändern oder Wiederholen von Nachrichten untergräbt) zu widerstehen.

**[0026]** Zusätzlich zu der impliziten Schlüsselauthentifizierung und Schlüsselbestätigung wurde eine gewisse Anzahl von wünschenswerten Sicherheitsattributen von AK- und AKC-Protokollen identifiziert:

1. Sicherheit bekannter Schlüssel. Jeder Durchgang eines Schlüsseleinigungsprotokolls zwischen A und B muss einen einzigartigen geheimen Schlüssel erzeugen; solche Schlüssel werden Sitzungsschlüssel genannt. Ein Protokoll muss gegenüber einem Gegner, der einige andere Sitzungsschlüssel erfahren hat, weiterhin sein Ziel erreichen.

2. (Perfekte) Vorwärtsgeheimhaltung. Falls langfristige Schlüssel einer oder mehrerer Entitäten in Frage gestellt werden, ist die Geheimhaltung vorhergehender Sitzungsschlüssel, die von rechtschaffenen Entitäten erstellt wurden, nicht beeinträchtigt.

3. Schlüssel kompromittierende Nachahmung. Nehmen wir an, dass der langfristige Schlüssel von A aufgedeckt wurde. Offensichtlich kann ein Gegner, der diesen Wert kennt, nun A nachahmen, da genau dieser Wert A identifiziert. Es kann jedoch wünschenswert sein, dass es dieser Verlust einem Gegner nicht ermöglicht, andere Entitäten gegenüber A nachzuahmen.

4. Teilen unbekannter Schlüssel. Die Entität A kann nicht dazu gezwungen werden, ohne Wissen von A einen Schlüssel mit der Entität B zu teilen, d.h., wenn A glaubt, dass der Schlüssel mit einer Entität C ≠ B geteilt wird, und B (richtigerweise) glaubt, dass der Schlüssel mit A geteilt wird.

5. Schlüsselkontrolle. Keine der Entitäten darf in der Lage sein, den Sitzungsschlüssel zwangsweise auf einen vorgewählten Wert zu setzen.

**[0027]** Wünschenswerte Leistungsattribute von AK- und AKC-Protokollen umfassen eine Mindestanzahl von Durchgängen (die Anzahl von Nachrichten, die in einem Durchgang des Protokolls ausgetauscht werden), geringen Kommunikationsaufwand (gesamte Anzahl übertragener Bits) und geringen Rechenaufwand. Andere Attribute, die unter gewissen Umständen wünschenswert sein können, umfassen Rollensymmetrie (die Nachrichten, die zwischen den Entitäten übertragen werden, haben die gleiche Struktur), Nicht-Interaktivität (die Nachrichten, die zwischen den beiden Entitäten übertragen werden, sind unabhängig voneinander) und das Nicht-Beruhen auf Verschlüsselung, Hash-Funktionen (da diese bekanntlich schwer zu gestalten sind) und Zeitstempeln (da es schwierig ist, dies gesichert in die Praxis umzusetzen).

**[0028]** Es ist daher eine Aufgabe der vorliegenden Erfindung, ein Schlüsseleinigungsprotokoll bereitzustellen, bei dem die obigen Nachteile vermieden oder gemindert werden und bei dem das Erreichen der gewünschten Attribute erleichtert wird.

### Kurzdarstellung

**[0029]** Nach einem Aspekt wird ein Verfahren zur Ausführung eines Protokolls zur Einigung auf einen Schlüssel, das zwischen einem Paar Entitäten ausgeführt wird, die über ein Datenkommunikationssystem kommunizieren, bereitgestellt, wobei mit jeder der Entitäten ein langfristiger privater Schlüssel, ein zu diesem gehöriger kryptografischer langfristiger öffentlicher Schlüssel, der unter Verwendung des langfristigen privaten Schlüssels und eines zu einem diskreten logarithmischen Problem gehörenden Generatorpunkts generiert wird, und eine Identität verknüpft ist, wobei das Verfahren folgende Schritte umfasst: Generieren für jede Entität eines zu dieser Entität gehörenden privaten Sitzungsschlüssels und eines zu dieser Entität gehörenden kryptografischen öffentlichen Sitzungsschlüssels; Weitergeben an die andere Entität des öffentlichen Sitzungsschlüssels jeder Entität; Erzielen an jeder Entität einer Kennung für die beiden Entitäten; Generieren eines gemeinsamen Wertes, umfassend das Kombinieren an jeder Entität des öffentlichen Sitzungsschlüssels der Entität, des öffentlichen Sitzungsschlüssels der anderen Entität und der Identitäten jeder Entität; Generieren für jede Entität eines zu dieser Entität gehörenden geheimen Wertes, umfassend das Kombinieren des gemeinsamen Wertes mit dem privaten Sitzungsschlüssel und dem langfristigen privaten Schlüssel der Entität; Berechnen an jeder Entität eines ephemeren Wertes, umfassend das Kombinieren des öffentlichen Sitzungsschlüssels der anderen Entität, des gemeinsamen Wertes und des langfristigen öffentlichen Schlüssels der anderen Entität; und Generieren an jeder Entität einer geteilten geheimen Information aus dem geheimen Wert und dem ephemeren Wert der Entität, um einen geteilten Schlüssel zu erzielen.

**[0030]** Nach einem anderen Aspekt wird ein Datenkommunikationssystem bereitgestellt, wobei das Datenkommunikationssystem ein Paar kryptografische Korrespondentengeräte umfasst, die konfiguriert sind, um das Verfahren nach einem der Ansprüche 1 bis 10 umzusetzen.

**[0031]** Nach einem weiteren Aspekt wird ein kryptografisches Korrespondentengerät bereitgestellt, wobei das Korrespondentengerät einen Prozessor und einen Speicher umfasst, wobei in dem Speicher ein langfristiger privater Schlüssel gespeichert ist, wobei mit dem Gerät ferner ein kryptografischer entsprechender langfristiger öffentlicher Schlüssel, der unter Verwendung des langfristigen privaten Schlüssels und eines Generatorpunktes generiert wird, und eine Identität verknüpft sind, wobei in dem Speicher ferner Computeranweisungen gespeichert sind, die, wenn sie von dem Prozessor ausgeführt werden, bewirken, dass der Prozessor ein Verfahren umsetzt, das folgende Schritte umfasst: Generieren eines zu diesem kryptografischen Korrespondentengerät gehörenden privaten Sitzungsschlüssels und eines zu diesem kryptografischen Korrespondentengerät gehörenden kryptografisch entsprechenden öffentlichen Sitzungsschlüssels; Weitergeben des öffentlichen Sitzungsschlüssels über ein Datenkommunikationssystem an ein anderes kryptografisches Korrespondentengerät; Erzielen von dem anderen kryptografischen Korrespondentengerät eines öffentlichen Sitzungsschlüssels; Erzielen einer Kennung von beiden der kryptografischen Korrespondentengeräte; Generieren eines gemeinsamen Wertes, umfassend das Kombinieren des öffentlichen Sitzungsschlüssels des kryptografischen Korrespondentengerätes, des öffentlichen Sitzungsschlüssels des anderen kryptografischen Korrespondentengerätes und der Identitäten jedes der kryptografischen Korrespondentengeräte; Generieren eines zu diesem kryptografischen Korrespondentengerät gehörenden geheimen Wertes, umfassend das Kombinieren des gemeinsamen Wertes mit dem privaten Sitzungsschlüssel und dem langfristigen privaten Schlüssel des kryptografischen Korrespondentengerätes; Berechnen eines ephemeren Wertes, umfassend das Kombinieren des öffentlichen Sitzungsschlüssels des anderen kryptografischen Korrespondentengerätes, des gemeinsamen Wertes und des langfristigen öffentlichen Schlüssels des anderen kryptografischen Korrespondentengerätes; und Generieren einer geteilten geheimen Information aus dem geheimen Wert und dem ephemeren Wert des kryptografischen Korrespondentengerätes, um einen geteilten Schlüssel zu erzielen.

**[0032]** Im Allgemeinen kombiniert das Protokoll die öffentlichen Sitzungsschlüssel jeder Entität und die Identitäten jeder Entität, um einen gemeinsamen Wert zu erzielen, der die beiden Entitäten bindet. Dieser wird von jeder Entität verwendet, um einen jeweiligen geheimen Wert zu generieren, indem der gemeinsame Wert und sowohl der private Sitzungsschlüssel als auch der langfristige private Schlüssel der Entität kombiniert werden. Der geheime Wert wird als ephemerer privater Schlüssel verwendet. Die andere Entität berechnet einen ephemeren öffentlichen Schlüssel, der dem geheimen Wert der einen Entität unter Verwendung des gemeinsamen Wertes entspricht. Jede Entität kann dann eine geteilte geheime Information aus ihrem ephemeren privaten Schlüssel und dem ephemeren öffentlichen Schlüssel der anderen Entität generieren.

**[0033]** Bevorzugt wird die geteilte geheime Information als Eingabe in eine Schlüsselableitungsfunktion verwendet, um einen geteilten Schlüssel zu erzielen.

**[0034]** Bevorzugt wird auch das Protokoll in einem Kryptosystem mit elliptischen Kurven umgesetzt, und die Kombination der öffentlichen Schlüssel wird durch Punkteaddition ausgeführt.

**[0035]** Weiter bevorzugt wird die Identität der Entitäten aus einem kryptografischen Zertifikat erzielt, das von einem vertrauenswürdigen Dritten ausgestellt wird.

**[0036]** Dadurch, dass die Entitäten wie zuvor beschrieben gebunden sind, generiert jeder Durchgang einen neuen geheimen Wert, und mit der richtigen Auswahl der Parameter, die sich auf normale kryptografische Praktiken beziehen, werden die wünschenswerten Attribute erreicht.

### Beschreibung der Zeichnungen

**[0037]** Eine Ausführungsform der vorliegenden Erfindung wird nun rein beispielhaft mit Bezug auf die beiliegenden Zeichnungen beschrieben. Es zeigt:

| | |
|---|---|
| Fig. 1 | eine schematische Darstellung eines Datenkommunikationssystems; |
| Fig. 2 | eine Darstellung eines Gerätes, das in dem Datenkommunikationssystem aus Fig. 1 verwendet wird; und |
| Fig. 3 | ein Ablaufschema, welches das Protokoll zeigt, das zwischen einem Gerätepaar, das in Fig. 1 gezeigt ist, umgesetzt wird. |

### Ausführliche Beschreibung

**[0038]** Wie nachstehend beschrieben, wird ein effizientes AK-Protokoll mit zwei Durchgängen vorgeschlagen, das auf der Schlüsseleinigung nach Diffie-Hellman basiert und viele der wünschenswerten Sicherheits- und Leistungsattribute aufweist, die in dem Artikel von 1997 von S. Blake-Wilson, D. Johnson und A. Menezes unter dem Titel «Key agreement protocols and their security analysis» besprochen werden.

**[0039]** Das nachstehend beschriebene Protokoll wurde im Rahmen der Gruppe von Punkten auf einer elliptischen Kurve beschrieben, die über ein endliches Feld definiert ist. Es kann jedoch ohne weiteres geändert werden, um in einer beliebigen endlichen Gruppe zu funktionieren, in der das Problem des diskreten Logarithmus unlösbar erscheint. Geeignete Möglichkeiten umfassen die multiplikative Gruppe eines endlichen Feldes, Untergruppen von Z*n, wobei n eine zusammengesetzte Ganzzahl ist, und nicht triviale Untergruppen von Z*p der primen Ordnung q. Elliptische Kurvengruppen sind deshalb von Vorteil, weil sie eine gleichwertige Sicherheit bieten wie die anderen Gruppen, jedoch mit kleineren Schlüsselgrössen und schnelleren Rechenzeiten.

**[0040]** Daher umfasst mit Bezug auf Fig. 1 ein Datenkommunikationssystem eine Vielzahl von Geräten 12, die durch Kommunikationsverbindungen 14 zusammengeschaltet sind. Die Geräte 12 können von beliebiger bekannter Art sein, wozu ein Computer 12a, ein Server 12b, ein Mobiltelefon 12c, ein ATM 12d und eine Chipkarte 12e gehören. Die Kommunikationsverbindungen 14 können herkömmliche Festtelefonleitungen, drahtlose Verbindungen, die zwischen den Geräten 12 umgesetzt werden, Nahfeld-Kommunikationsverbindungen, wie etwa Bluetooth, oder eine andere herkömmliche Kommunikationsform sein.

**[0041]** Die Geräte 12 unterscheiden sich gemäss ihrem beabsichtigten Zweck, umfassen aber typischerweise ein Kommunikationsmodul 20 (Fig. 2) zur Kommunikation mit den Verbindungen 14. Ein Speicher 22 stellt ein Speichermedium für nicht vorübergehende Anweisungen bereit, um Protokolle umzusetzen und je nach Bedarf Daten zu speichern. Die Anweisungen werden von einem kryptografischen Prozessor ausgeführt. Ein gesichertes Speichermodul 24, das Teil des Speichers 22 oder ein getrenntes Modul sein kann, wird verwendet, um private Informationen zu speichern, wie etwa die privaten Schlüssel, die bei den Verschlüsselungsprotokollen verwendet werden, und um einer Manipulation an diesen Daten standzuhalten. Eine arithmetische Logikeinheit (ALU) 26 wird bereitgestellt, um die Anweisungen der arithmetischen Operationen durch den Speicher 22 unter Verwendung von Daten, die in den Speichern 22, 24 gespeichert sind, auszuführen. Ein Generator 28 von Zufalls- oder Pseudozufallszahlen ist ebenfalls enthalten, um Bitfolgen zu generieren, die Zufallszahlen auf kryptografisch gesicherte Art und Weise darstellen.

**[0042]** Es versteht sich, dass das in Fig. 2 abgebildete Gerät 12 sehr schematisch ist und ein herkömmliches Gerät darstellt, das in einem Datenkommunikationssystem verwendet wird.

**[0043]** Der Speicher 22 speichert umzusetzende Systemparameter für das Kryptosystem und einen Satz von computerlesbaren Anweisungen, um das benötigte Protokoll umzusetzen. Für den Fall eines Kryptosystems mit elliptischen Kurven bestehen die Domänenparameter der elliptischen Kurven aus sechs Grössen q, a, b, P, n und h, nämlich aus:

- der Feldgrösse q
- den elliptischen Kurvenkoeffizienten a und b
- dem Basispunktgenerator P
- der n. Ordnung des Basispunktgenerators
- dem Kofaktor h, der eine derartige Zahl ist, dass hn die Anzahl von Punkten auf der elliptischen Kurve ist.

**[0044]** Die Parameter werden als Bitfolgen dargestellt, und die Darstellung des Basispunktes G wird als Bitfolgenpaar dargestellt, die jeweils ein Element des zugrundeliegenden Feldes darstellen. Wie gewohnt kann eine dieser Folgen gekürzt werden, da man die vollständige Darstellung aus der anderen Koordinate und der gekürzten Darstellung wiederherstellen kann.

**[0045]** Das gesicherte Speichermodul 24 enthält eine Bitfolge, die einen langfristigen privaten Schlüssel d und den entsprechenden öffentlichen Schlüssel Q darstellt. Für ein Kryptosystem mit elliptischen Kurven ist der Schlüssel Q = dP.

**[0046]** Der gesicherte Speicher 24 umfasst auch eine Kennung ID des Geräts 12. Praktischerweise handelt es sich dabei um ein Zertifikat, das von einer vertrauenswürdigen Instanz ausgestellt wird, um eine Fremdüberprüfung der Identität zu ermöglichen. Eine praktische Zertifikatform ist ein ECQV-Zertifikat, wie es in der Norm SEC 4 dargelegt wird.

**[0047]** Ephemere Werte, die von der ALU berechnet werden, können ebenfalls in dem gesicherten Modul 24 gespeichert werden, falls ihr Wert geheim bleiben soll.

**[0048]** Das Schlüsseleinigungsprotokoll wird in Fig. 3 gezeigt, wie es zwischen einem Paar von Geräten ausgeführt wird, die als Entität Alice und Entität Bob bezeichnet werden. Die Werte, die mit Alice verknüpft sind, werden mit der Endung A bezeichnet und die von Bob mit der Endung B. Alice verfügt über einen langfristigen privaten Schlüssel $d_A$ und einen entsprechenden öffentlichen Schlüssel $Q_A$, die in dem gesicherten Speichermodul 24 gespeichert sind. Ähnlich verfügt Bob über einen privaten Schlüssel $d_B$ und einen entsprechenden öffentlichen Schlüssel $Q_B$, die in seinem gesicherten Speichermodul 24 gespeichert sind.

**[0049]** Die Entitäten Alice und Bob wollen einen gemeinsamen Schlüssel teilen und setzen daher über die Anweisungen, die in dem Speicher 22 gespeichert sind, das in Fig. 3 gezeigte Protokoll um.

**[0050]** In Block 100 generiert Alice eine zufällige Ganzzahl unter Verwendung des RNG 28 und speichert den ganzzahligen Wert als privaten Sitzungsschlüssel in dem gesicherten Modul 24. Die ALU 26 von Alice berechnet in Block 102 einen entsprechenden öffentlichen Sitzungsschlüssel aP, den sie über eine Kommunikationsverbindung 14 an Bob sendet. Der öffentliche Sitzungsschlüssel aP ist eine Darstellung eines Punktes auf der Kurve und verfügt über ein Paar Bitfolgen, die jeweils ein Element in dem zugrundeliegenden Feld darstellen. Bei einigen Umsetzungen der Berechnungen, die von der

ALU 26 ausgeführt werden, ist es nur notwendig, die X-Koordinate des Punktes zu verwenden, wobei die Y-Koordinate dann nicht notwendig ist. Die X-Koordinate ist in dieser Situation für den öffentlichen Schlüssel aP repräsentativ. Die Y-Koordinate kann bei Bedarf aus der X-Koordinate wiederhergestellt werden. Punktkompressionstechniken, bei denen eine Angabe des Wertes der Y-Koordinate mit der X-Koordinate gesendet wird, können gegebenenfalls ebenfalls verwendet werden, um die Bandbreite bei der Übertragung zu reduzieren.

**[0051]** Ähnlich generiert Bob in Block 200 mit seinem RNG 28 eine zufällige Ganzzahl, die er in seinem gesicherten Modul 24 als privaten Sitzungsschlüssel b speichert. Ein entsprechender öffentlicher Sitzungsschlüssel bP wird in Block 202 berechnet und über eine Kommunikationsverbindung 14 an Alice gesendet.

**[0052]** Sowohl Alice als auch Bob führen unter Verwendung der ALU 26 eine Punktaddition aus, um $\gamma = bP + aP$ zu berechnen, wie bei 104, 204 gezeigt. Dies wird wiederum zu einem weiteren Punkt, $\gamma$, auf der Kurve und ist somit als Elementepaar dargestellt. Bei einigen Ausführungsformen ist es möglich, nur die X-Koordinate der Summe der öffentlichen Schlüssel bei der Berechnung von $\gamma$ zu verwenden.

**[0053]** Bei weiteren Ausführungsformen, bei denen das Protokoll in einem Kryptosystem mit hyperelliptischen Kurven umgesetzt ist, wird die Kombination der öffentlichen Schlüssel durch Punktaddition in der Jacobi-Matrix der hyperelliptischen Kurve umgesetzt.

**[0054]** Sowohl Alice als auch Bob erzielen Kopien der gegenseitigen Identität ID (106, 206). Dies kann vor der Umsetzung des Protokolls erfolgen, oder das Zertifikat kann mit dem öffentlichen Sitzungsschlüssel gesendet werden. Das Zertifikat kann bei Bedarf vom Empfänger überprüft werden.

**[0055]** In Block 108, 208 berechnen Alice und Bob jeweils einen gemeinsamen Wert $c = H(\gamma//ID_A//ID_B)$, wobei H eine kryptografisch gesicherte Hash-Funktion ist, wie etwa eine SHA2-Hash-Funktion. Der Wert c wird in dem Speicher 22 gespeichert. Der gemeinsame Wert c bindet Alice und Bob. Durch das Verketten der Identitäten ID ist es notwendig, die Reihenfolge zu bestimmen, in der die Folge, die c darstellt, zusammengesetzt wird. Als Alternative können die Identitäten daher durch eine Operation XOR der ID kombiniert werden und dadurch ermöglichen, dass die Folge zusammengesetzt wird, ohne sich um ihre Reihenfolge zu kümmern. Soweit bevorzugt, kann $\gamma$ ähnlich eine XOR-Operation mit den ID erfahren.

**[0056]** Alice berechnet in Block 110 die Komponente $s_A = a + cd_A \pmod n$, welche die langfristigen und kurzfristigen privaten Schlüssel verwendet, die in dem gesicherten Modul 24 gespeichert sind.

**[0057]** Ähnlich berechnet Bob in Block 210 $s_B = b + cd_B \pmod n$.

**[0058]** Aus öffentlichen Informationen, zu denen der öffentliche Sitzungsschlüssel bP gehört, der von Bob empfangen wird, kann Alice $s_BP = bP + cQ_B$ berechnen, wie in 112 gezeigt.

**[0059]** Ähnlich kann Bob $s_AP = aP + cQ_A$ (212) berechnen.

**[0060]** Alice und Bob verfügen jeweils über eine Komponente, die aus privaten Informationen und dem gemeinsamen Wert berechnet wird, und eine Komponente, die aus öffentlichen Informationen berechnet wird. Diese können kombiniert werden, um eine geteilte geheime Information bereitzustellen.

**[0061]** Daher können in Block 114, 214 Alice und Bob beide den Wert $K = hs_As_BP$ als die geteilte geheime Information berechnen.

**[0062]** Alice hat $s_BP$ aus öffentlichen Informationen berechnet und hat den Wert $s_A$ gespeichert.

**[0063]** Ähnlich hat Bob $s_AP$ berechnet und hat den Wert $s_B$ gespeichert.

**[0064]** Eine andere Option, um die geteilte geheime Information zu berechnen, besteht darin, dass Alice $K = s_A \cdot s_BP$ berechnet und dass Bob $K = s_B \cdot s_AP$ berechnet, wobei der Kofaktor h ignoriert wird. Dies ist nützlich, wenn der Wert von h klein ist, z.B. 1, oder bei Widerstand gegen den kleinen Gruppenangriff.

**[0065]** Das zuvor beschriebene Protokoll erstellt somit eine geteilte geheime Information K zwischen zwei Entitäten. Eine Schlüsselableitungsfunktion muss dann verwendet werden, um einen geheimen Schlüssel aus der geteilten geheimen Information abzuleiten. Dies ist notwendig, weil die geteilte geheime Information K ein schwaches Bit aufweisen kann – Bits mit Informationen über K, die zu nicht unbeachtlichem Vorteil vorhergesagt werden können.

**[0066]** Eine Möglichkeit, einen Schlüssel aus der geteilten geheimen Information K abzuleiten, besteht darin, eine Einweg-Hash-Funktion, wie etwa SHA-1, auf K anzuwenden. Alternativ können andere Schlüsselableitungsfunktionen verwendet werden, wie es ausführlicher im Kapitel XX aus «Handbook of Applied Cryptography» beschrieben wird, dessen Inhalt hiermit zur Bezugnahme übernommen wird.

**[0067]** Zusammenfassend kann das Schlüsseleinigungsprotokoll unter Verwendung des folgenden Algorithmus umgesetzt werden:

1. Alice erzielt eine authentische Kopie des langfristigen öffentlichen Schlüssels $Q_B$ von Bob.
2. Alice generiert eine zufällige Ganzzahl, um einen privaten Sitzungsschlüssel a ($0 < a < n$) bereitzustellen.

3. Alice berechnet aP und sendet dies an Bob.
4. Bob erzielt eine authentische Kopie des öffentlichen Schlüssels $Q_A$ von Alice.
5. Bob generiert eine zufällige Ganzzahl b ($0 < b < n$).
6. Bob berechnet bP und sendet dies an Alice.
7. Alice berechnet $s_A = a + cd_A \pmod n$, wobei $c = H(\gamma//ID_A//ID_B)$. (Anmerkung: $ID_A$ und $ID_B$ können jeweils die öffentlichen Schlüssel von Alice und Bob enthalten).
8. Alice berechnet $s_BP = bP + cQ_B$. (Anmerkung: Bob hat Alice bP gesendet, und sie hat eine authentische Kopie von $Q_B$ erzielt).
9. Bob berechnet $s_B = b + cd_B \pmod n$.
10. Bob berechnet aus den öffentlichen Informationen $s_AP = aP + cQ_A$.
11. Sowohl Alice als auch Bob können nun $K = h \cdot s_A \cdot s_BP$ als geteilte geheime Information berechnen, wobei h der Kofaktor ist.
12. Die geteilte geheime Information kann bei Bedarf als Eingabe für eine Schlüsselableitungsfunktion verwendet werden.

**[0068]** Eine andere Option zum Berechnen der geteilten geheimen Information besteht darin, dass Alice $K = s_A \cdot s_BP$ berechnet und Bob $K = s_B \cdot s_AP$ berechnet, wobei der Kofaktor h ignoriert wird. Dies ist nützlich, wenn der Wert von h gering ist, z.B. 1, oder bei Widerstand gegen den kleinen Untergruppenangriff.

**Patentansprüche**

1. Verfahren zur Ausführung eines Protokolls zur Einigung auf einen Schlüssel, das zwischen einem Paar Entitäten ausgeführt wird, die über ein Datenkommunikationssystem kommunizieren,
wobei mit jeder der Entitäten ein langfristiger privater Schlüssel, ein zu diesem gehöriger kryptografischer langfristiger öffentlicher Schlüssel, der unter Verwendung des langfristigen privaten Schlüssels und eines zu einem diskreten logarithmischen Problem gehörenden Generatorpunkts generiert wird, und eine Identität verknüpft ist,
wobei das Verfahren folgende Schritte umfasst:
– Generieren für jede Entität eines zu dieser Entität gehörenden privaten Sitzungsschlüssels und eines zu dieser Entität gehörenden kryptografischen öffentlichen Sitzungsschlüssels;
– Weitergeben an die andere Entität des öffentlichen Sitzungsschlüssels jeder Entität;
– Erzielen an jeder Entität einer Kennung für die beiden Entitäten;
– Generieren eines gemeinsamen Wertes, umfassend das Kombinieren an jeder Entität des öffentlichen Sitzungsschlüssels der Entität, des öffentlichen Sitzungsschlüssels der anderen Entität und der Identitäten jeder Entität;
– Generieren für jede Entität eines zu dieser Entität gehörenden geheimen Wertes, umfassend das Kombinieren des gemeinsamen Wertes mit dem privaten Sitzungsschlüssel und dem langfristigen privaten Schlüssel der Entität;
– Berechnen an jeder Entität eines ephemeren Wertes, umfassend das Kombinieren des öffentlichen Sitzungsschlüssels der anderen Entität, des gemeinsamen Wertes und des langfristigen öffentlichen Schlüssels der anderen Entität; und
– Generieren an jeder Entität einer geteilten geheimen Information aus dem geheimen Wert und dem ephemeren Wert der Entität, um einen geteilten Schlüssel zu erzielen.
2. Verfahren nach Anspruch 1, wobei die geteilte geheime Information als Eingabe in eine Schlüsselableitungsfunktion verwendet wird, um den geteilten Schlüssel zu erzielen.
3. Verfahren nach Anspruch 1 oder 2, wobei das Generieren eines gemeinsamen Wertes das Anwenden einer XOR-Operation auf die Identitäten jeder Entität umfasst.
4. Verfahren nach einem der Ansprüche 1 bis 3, wobei das Verfahren in einem Kryptosystem mit elliptischen Kurven umgesetzt wird und die Kombination der öffentlichen Sitzungsschlüssel durch Punktaddition ausgeführt wird.
5. Verfahren nach einem der Ansprüche 1 bis 4, wobei das Verfahren in einem Kryptosystem mit elliptischen Kurven umgesetzt wird und das Generieren des gemeinsamen Wertes das Erzielen einer X-Koordinate der Summe der öffentlichen Schlüssel umfasst.
6. Verfahren nach einem der Ansprüche 1 bis 3, wobei das Verfahren in einem Kryptosystem mit hyperelliptischen Kurven umgesetzt wird und die Kombination der öffentlichen Schlüssel durch Punktaddition in der Jacobi-Matrix der hyperelliptischen Kurve ausgeführt wird.

7. Verfahren nach einem der Ansprüche 1 bis 6, wobei das Generieren des öffentlichen Sitzungsschlüssels eine skalare Multiplikation des privaten Sitzungsschlüssels und des Generatorpunktes umfasst.

8. Verfahren nach einem der Ansprüche 1 bis 7, wobei die Kombination des geheimen Wertes und des ephemeren Wertes die skalare Multiplikation des geheimen Wertes und des ephemeren Wertes ist.

9. Verfahren nach einem der Ansprüche 1 bis 7, wobei die Kombination des geheimen Wertes und des ephemeren Wertes die skalare Multiplikation eines Kofaktors, des geheimen Wertes und des ephemeren Wertes ist.

10. Verfahren nach einem der Ansprüche 1 bis 9, wobei die Identität der Entitäten aus einem kryptografischen Zertifikat erzielt wird, das von einem vertrauenswürdigen Dritten ausgestellt wird.

11. Datenkommunikationssystem, umfassend ein Paar kryptografische Korrespondentengeräte, die konfiguriert sind, um das Verfahren nach einem der Ansprüche 1 bis 10 umzusetzen.

12. Kryptografisches Korrespondentengerät, umfassend einen Prozessor und einen Speicher, wobei in dem Speicher ein langfristiger privater Schlüssel gespeichert ist, wobei mit dem Gerät ferner ein kryptografischer entsprechender langfristiger öffentlicher Schlüssel, der unter Verwendung des langfristigen privaten Schlüssels und eines Generatorpunktes generiert wird, und eine Identität verknüpft sind,
wobei in dem Speicher ferner Computeranweisungen gespeichert sind, die, wenn sie von dem Prozessor ausgeführt werden, bewirken, dass der Prozessor ein Verfahren umsetzt, das folgende Schritte umfasst:
– Generieren eines zu diesem kryptografischen Korrespondentengerät gehörenden privaten Sitzungsschlüssels und eines zu diesem kryptografischen Korrespondentengerät gehörenden kryptografisch entsprechenden öffentlichen Sitzungsschlüssels;
– Weitergeben des öffentlichen Sitzungsschlüssels über ein Datenkommunikationssystem an ein anderes kryptografisches Korrespondentengerät;
– Erzielen von dem anderen kryptografischen Korrespondentengerät einen öffentlichen Sitzungsschlüssel;
– Erzielen einer Kennung von beiden der kryptografischen Korrespondentengeräte;
– Generieren eines gemeinsamen Wertes, umfassend das Kombinieren des öffentlichen Sitzungsschlüssels des kryptografischen Korrespondentengerätes, des öffentlichen Sitzungsschlüssels des anderen kryptografischen Korrespondentengerätes und der Identitäten jedes der kryptografischen Korrespondentengeräte;
– Generieren eines zu diesem kryptografischen Korrespondentengerät gehörenden geheimen Wertes, umfassend das Kombinieren des gemeinsamen Wertes mit dem privaten Sitzungsschlüssel und dem langfristigen privaten Schlüssel des kryptografischen Korrespondentengerätes;
– Berechnen eines ephemeren Wertes, umfassend das Kombinieren des öffentlichen Sitzungsschlüssels des anderen kryptografischen Korrespondentengerätes, des gemeinsamen Wertes und des langfristigen öffentlichen Schlüssels des anderen kryptografischen Korrespondentengerätes; und
– Generieren einer geteilten geheimen Information aus dem geheimen Wert und dem ephemeren Wert des kryptografischen Korrespondentengerätes, um einen geteilten Schlüssel zu erzielen.

13. Kryptografisches Korrespondentengerät nach Anspruch 12, wobei die geteilte geheime Information als Eingabe in eine Schlüsselableitungsfunktion verwendet wird, um einen geteilten Schlüssel zu erzielen.

14. Kryptografisches Korrespondentengerät nach Anspruch 12 oder 13, wobei das Generieren eines gemeinsamen Wertes das Anwenden einer XOR-Operation auf die Identitäten jedes kryptografischen Korrespondentengerätes umfasst.

15. Kryptografisches Korrespondentengerät nach einem der Ansprüche 12 bis 14, wobei das Verfahren in einem Kryptosystem mit elliptischen Kurven umgesetzt wird und die Kombination der öffentlichen Sitzungsschlüssel durch Punktaddition ausgeführt wird.

16. Kryptografisches Korrespondentengerät nach einem der Ansprüche 12 bis 15, wobei das Verfahren in einem Kryptosystem mit elliptischen Kurven umgesetzt wird und das Generieren des gemeinsamen Wertes das Erzielen einer X-Koordinate der Summe des öffentlichen Schlüssels umfasst.

17. Kryptografisches Korrespondentengerät nach einem der Ansprüche 12 bis 14, wobei das Verfahren in einem Kryptosystem mit hyperelliptischen Kurven umgesetzt wird, und die Kombination des öffentlichen Schlüssels durch Punktaddition in der Jacobi-Matrix der hyperelliptischen Kurve ausgeführt wird.

18. Kryptografisches Korrespondentengerät nach einem der Ansprüche 12 bis 17, wobei das Generieren des öffentlichen Sitzungsschlüssels eine skalare Multiplikation des privaten Sitzungsschlüssels und des Generatorpunktes umfasst.

19. Kryptografisches Korrespondentengerät nach einem der Ansprüche 12 bis 18, wobei die Kombination des geheimen Wertes und des ephemeren Wertes die skalare Multiplikation des geheimen Wertes und des ephemeren Wertes ist.

20. Kryptografisches Korrespondentengerät nach einem der Ansprüche 12 bis 18, wobei die Kombination des geheimen Wertes und des ephemeren Wertes die skalare Multiplikation eines Kofaktors, des geheimen Wertes und des ephemeren Wertes ist.

21. Kryptografisches Korrespondentengerät nach einem der Ansprüche 12 bis 20, wobei die Identität des kryptografischen Korrespondentengerätes aus einem kryptografischen Zertifikat erzielt wird, das von einem vertrauenswürdigen Dritten ausgestellt wird.

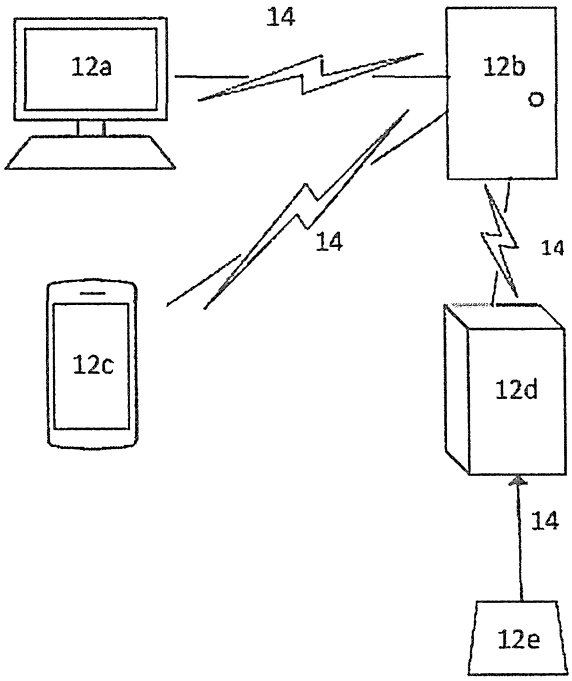



FIG. 1

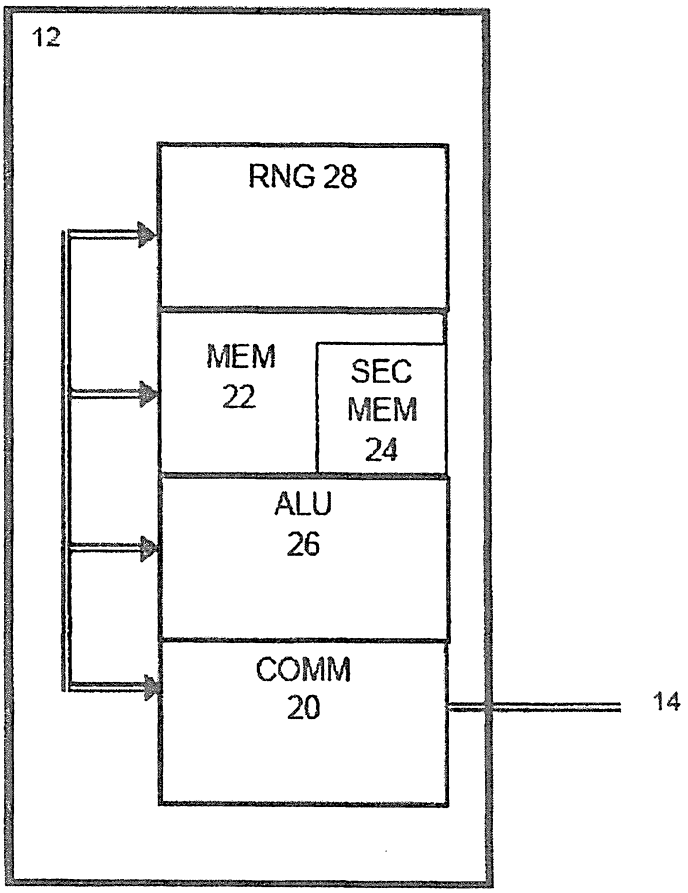



FIG. 2

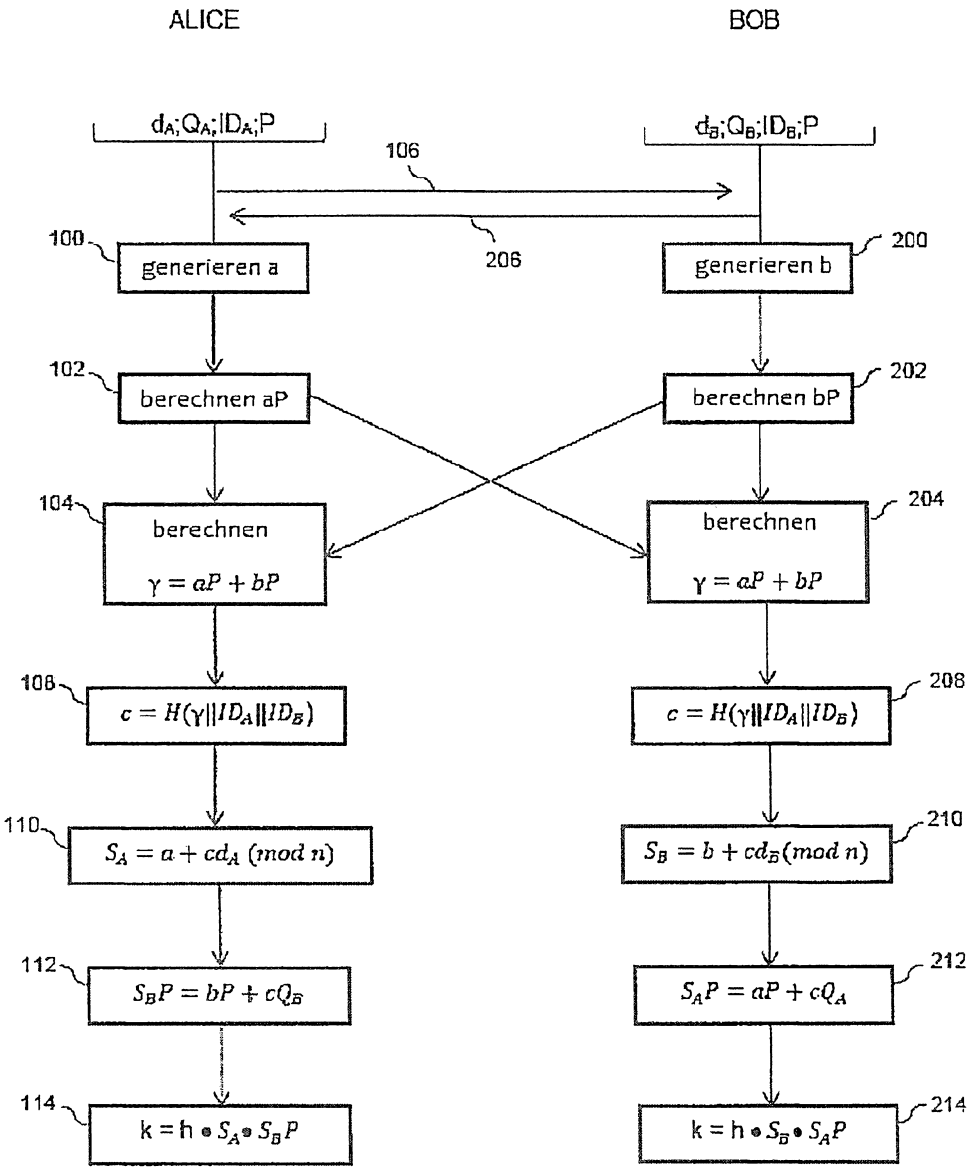

ALICE
BOB
$d_A;Q_A;ID_A;P$
$d_B;Q_B;ID_B;P$
106
206
100
generieren a
200
generieren b
102
berechnen aP
202
berechnen bP
104
berechnen
$\gamma = aP + bP$
204
berechnen
$\gamma = aP + bP$
108
$c = H(\gamma \| ID_A \| ID_B)$
208
$c = H(\gamma \| ID_A \| ID_B)$
110
$S_A = a + cd_A \ (mod\ n)$
210
$S_B = b + cd_B (mod\ n)$
112
$S_B P = bP + cQ_B$
212
$S_A P = aP + cQ_A$
114
$k = h \cdot S_A \cdot S_B P$
214
$k = h \cdot S_B \cdot S_A P$

FIG. 3