(19) SCHWEIZERISCHE EIDGENOSSENSCHAFT
EIDGENÖSSISCHES INSTITUT FÜR GEISTIGES EIGENTUM

(11) CH 711 134 A2

(51) Int. Cl.: H04L 9/30 (2006.01)

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

(12) PATENTANMELDUNG

(21) Anmeldenummer: 01276/15

(22) Anmeldedatum: 04.09.2015

(43) Anmeldung veröffentlicht: 30.11.2016

(30) Priorität: 26.05.2015 US 14/721,564

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

(72) Erfinder:
Adrian Antipa, L6POE3 Brampton, Ontario (CA)

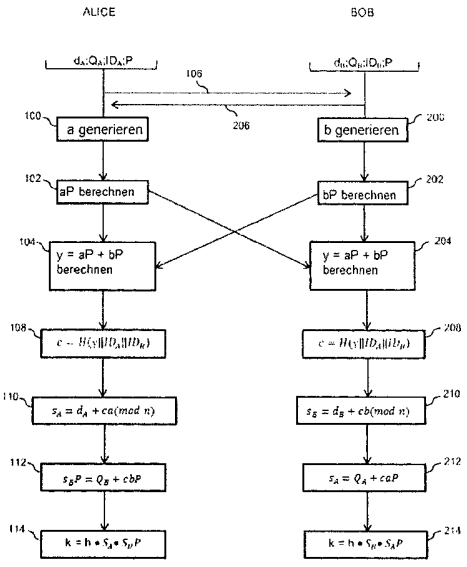
(74) Vertreter:
Braunpat Braun Eder AG, Reussstrasse 22
4054 Basel (CH)

(54) Schlüsselzustimmungsprotokoll.

(57) Die vorliegende Erfindung betrifft ein Schlüsselzustimmungsprotokoll, ein kryptographisches Kommunikationssystem und eine kryptographische Korrespondenzvorrichtung.

Das Protokoll wird zwischen zwei Instanzen ausgeführt und umfasst Folgendes:

- Generieren eines Private Keys und eines Public Keys
- Kommunizieren des Public Keys
- Generieren eines gemeinsamen Wertes (100, 200)
- Generieren von geheimen Werten (104, 204)
- Berechnen eines ephemeren Wertes
- Generieren eines gemeinsamen Geheimnisses



Beschreibung

TECHNISCHER BEREICH

[0001] Die vorliegende Erfindung betrifft Datenkommunikationssysteme und in solchen Systemen verwendete Protokolle.

HINTERGRUND

[0002] Datenkommunikationssysteme werden verwendet, um Informationen zwischen Vorrichtungen auszutauschen. Die auszutauschenden Informationen umfassen Daten, die als Folgen digitaler Bits angeordnet sind, die so formatiert sind, dass sie von anderen Vorrichtungen erkannt werden können und ermöglichen, dass die Informationen verarbeitet und/oder wiederhergestellt werden können.

[0003] Der Austausch von Informationen kann über ein öffentlich zugängliches Netzwerk wie einer Kommunikationsverbindung zwischen zwei Vorrichtungen, über ein zugehöriges Netzwerk innerhalb einer Organisation stattfinden oder kann zwischen zwei Vorrichtungen innerhalb derselben zugehörigen Komponente wie innerhalb einem Computer oder einer Verkaufspunktvorrichtung stattfinden.

[0004] Die Vorrichtungen reichen von relativ grossen Computersystemen bis hin zu Vorrichtungen für die Telekommunikation, Mobiltelefone, Überwachungsgeräte, Sensoren, elektronische Geldbörsen und Chipkarten und einer grossen Vielzahl von Vorrichtungen, die verbunden sind, um Daten zwischen zwei oder mehreren solchen Vorrichtungen zu übertragen.

[0005] Es wurde eine Vielzahl von Kommunikationsprotokollen entwickelt, um den Austausch von Daten zwischen unterschiedlichen Vorrichtungen zu ermöglichen. Die Kommunikationsprotokolle ermöglichen den Austausch von Daten auf robuste Art und Weise, oftmals mit Fehlerkorrektur und einer Funktionalität für die Fehlererkennung, und die Daten, an den beabsichtigten Empfänger zu leiten und für die Weiterverwendung wiederherzustellen.

[0006] Da die Daten für andere Vorrichtungen zugänglich sein können, sind sie für das Abfangen und die Überwachung oder Manipulation anfällig. Das sensible Wesen der Informationen macht es erforderlich, dass Schritte unternommen werden, um die Informationen zu sichern und ihre Integrität zu gewährleisten.

[0007] Es wurde eine Anzahl von Verfahren, die insgesamt als Verschlüsselungsprotokolle und Authentifizierungsprotokolle bezeichnet werden, entwickelt, um die geforderten Attribute bereitzustellen und beim Austausch von Informationen Sicherheit und/oder Integrität zu gewährleisten. Diese Verfahren verwenden einen Schlüssel, der mit den Daten kombiniert ist.

[0008] Es gibt zwei Hauptformen von Kryptosystemen, welche die Protokolle umsetzen: Kryptosysteme mit symmetrischen Schlüsseln und asymmetrische oder Public-Key-Kryptosysteme. In einem Kryptosystem mit symmetrischen Schlüsseln teilen die Vorrichtungen, welche Informationen austauschen, einen gemeinsamen Schlüssel, der nur den Vorrichtungen bekannt ist, welche die Informationen teilen sollen. Systeme mit symmetrischen Schlüsseln haben den Vorteil, dass sie relativ schnell sind und daher grosse Datenmengen in einer relativ kurzen Zeit verarbeiten können, sogar mit eingeschränkter Rechenleistung. Die Schlüssel müssen jedoch auf sichere Art und Weise an die verschiedenen Dienste verteilt werden, was zu erhöhten Betriebskosten und vermehrten Schwachstellen führt, wenn der Schlüssel gefährdet ist.

[0009] Asymmetrische Public-Key-Kryptosysteme verwenden ein Schlüsselpaar, wovon einer öffentlich und der andere privat ist und das jeder Vorrichtung zugeordnet wird. Der Public Key und der Private Key sind durch ein «schweres» mathematisches Problem verbunden, sodass der Private Key, selbst wenn der Public Key und das zugrunde liegende Problem bekannt sind, nicht in einer durchführbaren Zeit wiederhergestellt werden kann. Ein solches Problem ist die Faktorisierung des Produkts von zwei grossen Primzahlen, wie sie in RSA-Kryptosystemen verwendet werden. Ein anderes ist das diskrete Log-Problem in einer endlichen Gruppe. Ein Generator, α, der zugrunde liegenden Gruppe wird als ein Systemparameter identifiziert und eine zufällige ganze Zahl, k, wird zur Verwendung als ein Private Key generiert. Um einen Public Key, K, zu erhalten, wird eine k-fache Gruppenoperation ausgeführt, sodass $K = f(\alpha, k)$.

[0010] In diskreten Log-Kryptosystemen können verschiedene Gruppen verwendet werden, umfassend die multiplikative Gruppe eines endlichen Körpers, die Gruppe von ganzen Zahlen in einer endlichen zyklischen Gruppe der Ordnung p, üblicherweise angegeben als Zp^* und bestehend aus den ganzen Zahlen 0 bis p-1. Die Gruppenoperation ist eine Multiplikation, sodass $K = f(\alpha^k)$.

[0011] Eine andere Gruppe, die für eine verbesserte Sicherheit verwendet wird, ist eine Elliptische-Kurven-Gruppe. Die Elliptische-Kurven-Gruppe setzt sich aus Paaren von Elementen zusammen, von denen eines als x und das andere als y in einem Bereich, welcher der Gleichung der gewählten elliptischen Kurve genügt, angegeben wird. Für eine Elliptische-Kurven-Gruppe der Ordnung p wird die elliptische Kurve im Allgemeinen durch die Beziehung $y^2 \bmod p = x^3 + ax + b \bmod p$ festgelegt. Es ist wohlbekannt, dass für unterschiedliche Gruppen andere Kurven verwendet werden. Jedes derartige Paar von Elementen ist ein Punkt auf der Kurve und ein Generator der Gruppe wird als ein Punkt P angegeben. Die Gruppenoperation ist eine Addition, sodass ein Private Key k einen zugehörigen Public Key f(kP) aufweist.

[0012] Public-Key-Kryptosysteme reduzieren die Infrastruktur, die bei Kryptosystemen mit symmetrischen Schlüsseln erforderlich ist. Eine Vorrichtung kann eine ganze Zahl k und den zugehörigen Public Key kP generieren. Der Public Key wird veröffentlicht, sodass er für andere Vorrichtungen verfügbar ist. Die Vorrichtung kann dann ein geeignetes Signaturproto-

koll verwenden, um eine Nachricht unter Verwendung des Private Keys k zu signieren und andere Vorrichtungen können die Integrität der Nachricht unter Verwendung des Public Keys kP bestätigen.

[0013] Gleichermassen kann eine Vorrichtung eine Nachricht, die an eine andere Vorrichtung geschickt werden soll, unter Verwendung des Public Keys der anderen Vorrichtung verschlüsseln. Die Nachricht kann dann von der anderen Vorrichtung unter Verwendung des Private Keys wiederhergestellt werden. Diese Protokolle sind jedoch rechenintensiv und demzufolge im Vergleich zu symmetrischen Kryptosystem-Protokollen relativ langsam.

[0014] Public-Key-Kryptosysteme können ebenso verwendet werden, um einen Schlüssel zu erzeugen, der von zwei Vorrichtungen geteilt wird. In der einfachsten Form, wie sie von Diffie-Hellmann vorgeschlagen wird, schickt jede Vorrichtung einen Public Key an die andere Vorrichtung. Beide Vorrichtungen kombinieren dann den erhaltenen Public Key mit ihrem Private Key, um einen gemeinsamen Schlüssel zu erhalten.

[0015] Eine Vorrichtung, Alice, die üblicherweise als eine Instanz (oder Korrespondent) bezeichnet wird, generiert einen Private Key k_a und schickt den Public Key k_aP an eine andere Vorrichtung oder Instanz, Bob.

[0016] Bob generiert einen Private Key k_b und schickt den Public Key k_b an Alice.

[0017] Alice berechnet $k_a{}^{\bullet}k_bP$ und Bob berechnet $k_b{}^{\bullet}k_aP$, sodass sie einen gemeinsamen Schlüssel $K = k_ak_bP = k_bk_aP$ teilen. Der gemeinsame Schlüssel kann dann in einem symmetrischen Schlüsselprotokoll verwendet werden. Weder Alice noch Bob können den Private Key des anderen wiederherstellen und Dritte können den gemeinsamen Schlüssel nicht rekonstruieren.

[0018] Um die Integrität des gemeinsamen Schlüssels zu gewährleisten und um Angriffe abzuwehren, die entwickelt wurden, um den gemeinsamen Schlüssel und/oder die Private Keys innerhalb des gemeinsamen Schlüssels wiederherzustellen oder zu ersetzen, wurden Schlüsseletablierungsprotokolle entwickelt.

[0019] Die Schlüsseletablierung ist der Vorgang, bei dem zwei (oder mehrere) Instanzen einen gemeinsamen geheimen Schlüssel erzeugen. Der Schlüssel wird nachfolgend verwendet, um ein kryptographisches Ziel wie die Vertraulichkeit oder Datenintegrität zu erreichen.

[0020] Vereinfacht gesagt, gibt es zwei Arten von Schlüsseletablierungsprotokollen: Schlüsseltransportprotokolle, bei denen ein Schlüssel von einer Instanz erzeugt und sicher an die zweite Instanz übertragen wird und Schlüsselzustimmungsprotokolle, bei denen beide Parteien Informationen beisteuern, die zusammen den gemeinsamen geheimen Schlüssel erzeugen. Die vorliegende Anwendung ist auf Schlüsselzustimmungsprotokolle für die asymmetrischen (Public-Key-) Kryptosysteme ausgerichtet.

[0021] Wenn Alice und Bob zwei ehrliche Instanzen sind, d.h. legitime Instanzen, welche die Schritte eines Protokolls korrekt ausführen, dann soll ein Schlüsselzustimmungsprotokoll, pauschal gesagt, eine implizite Schlüsselauthentifizierung (von Bob an Alice) bereitstellen, wenn sich die Instanz Alice sicher ist, dass keine andere Instanz neben einer speziell identifizierten zweiten Instanz Bob möglicherweise den Wert eines bestimmten geheimen Schlüssels erfahren kann. Die Fähigkeit zur impliziten Schlüsselauthentifizierung bedeutet nicht zwangsläufig, dass sich Alice sicher ist, dass Bob tatsächlich den Schlüssel besitzt, sondern dass sich Alice sicher ist, dass niemand anderes als Bob den Schlüssel besitzt. Ein Schlüsselzustimmungsprotokoll, welches eine implizite Schlüsselauthentifizierung für beide beteiligten Parteien ermöglicht, wird als authentifiziertes Schlüsselzustimmungs- (AK-) Protokoll bezeichnet.

[0022] Pauschal gesagt, soll ein Schlüsselzustimmungsprotokoll eine Schlüsselbestätigung (von Bob an Alice) bereitstellen, wenn sich Instanz A sicher ist, dass die zweite Instanz Bob tatsächlich einen bestimmten geheimen Schlüssel besitzt. Wenn sowohl die implizite Schlüsselauthentifizierung als auch die Schlüsselbestätigung (von Bob an Alice) bereitgestellt werden, dann soll das Schlüsseletablierungsprotokoll eine explizite Schlüsselauthentifizierung (von Bob an Alice) bereitstellen. Ein Schlüsselzustimmungsprotokoll, welches eine explizite Schlüsselauthentifizierung für beide beteiligten Parteien ermöglicht, wird als authentifiziertes Schlüsselzustimmungsprotokoll mit Schlüsselbestätigung (AKC) bezeichnet. Eine umfangreiche Studie zur Schlüsseletablierung wird in Kapitel 12 des Handbook of Applied Cryptography von Menezes, van Oorshot und Vanstone bereitgestellt, dessen Inhalte durch Bezugnahme eingeführt werden.

[0023] Es muss mit äusserster Sorgfalt vorgegangen werden, wenn die Schlüsselbestätigung von der impliziten Schlüsselauthentifizierung getrennt wird. Wenn ein AK-Protokoll verwendet wird, das keine Schlüsselbestätigung anbietet, dann ist es, wie auch in der 1997 erschienen Abhandlung von S. Blake-Wilson, D. Johnson und A. Menezes mit dem Titel: «Key agreement protocols and their security analysis» aufgezeigt, wünschenswert, dass der vereinbarte Schlüssel vor einer kryptographischen Verwendung bestätigt wird. Dies kann auf unterschiedliche Art und Weise stattfinden. Wenn der Schlüssel zum Beispiel anschliessend verwendet werden soll, um Vertraulichkeit zu erreichen, dann kann die Verschlüsselung mit dem Schlüssel für einige (sorgfältig ausgewählte) bekannte Daten beginnen. Andere Systeme können die Schlüsselbestätigung während eines «Echtzeit-» Telefongesprächs bereitstellen. Das Trennen der Schlüsselbestätigung von der impliziten Schlüsselauthentifizierung ist gelegentlich wünschenswert, da es Flexibilität im Bezug auf die Auswahl zulässt, wie eine bestimmte Implementierung eine Schlüsselbestätigung erreichen möchte und somit die Last der Schlüsselbestätigung von dem Etablierungsmechanismus auf die Anwendung überträgt.

[0024] Über die Jahre hinweg wurden zahlreiche Diffie-Hellman-basierte AK- und AKC-Protokolle vorgeschlagen; für viele wurde jedoch anschliessend herausgefunden, dass sie Sicherheitslücken aufweisen. Die Hauptprobleme bestanden

darin, dass es für geeignete Gefahrenmodelle und die Ziele für sichere AK- und AKC-Protokolle an einer formalen Definition mangelte. Blake-Wilson, Johnson und Menezes stellten unter Anwendung einer früheren Arbeit von Bellare und Rogaway für die symmetrische Konfiguration ein formales Modell für die verteilte Berechnung und strikte Definitionen für die Ziele sicherer AK- und AKC-Protokolle innerhalb dieses Moduls bereit. Es wurden konkrete AK- und AKC-Protokolle vorgeschlagen und ihre Sicherheit in diesem Rahmen in dem Zufallsorakelmodell bewiesen.

[0025] Es wird erwartet, dass ein sicheres Protokoll sowohl passiven Angriffen (bei denen ein Gegenspieler versucht, ein Protokoll am Erreichen seiner Ziele zu hindern, indem es lediglich ehrliche Instanzen bei der Ausführung des Protokolls beobachtet) als auch aktiven Angriffen (bei denen ein Gegenspieler zusätzlich die Kommunikation durch das Einfügen, Löschen, Ändern oder erneute Abspielen von Nachrichten untergräbt) standhalten kann.

[0026] Zusätzlich zu der impliziten Schlüsselauthentifizierung und der Schlüsselbestätigung wurde eine Anzahl wünschenswerter Sicherheitsmerkmale von AK-und AKC-Protokollen identifiziert:

1) Sicherheit bekannter Schlüssel. Jeder Durchlaufeines Schlüsselzustimmungsprotokolls zwischen A und B sollte einen eindeutigen geheimen Schlüssel erzeugen; solche Schlüssel werden als Sitzungsschlüssel bezeichnet. Ein Protokoll sollte sein Ziel auch trotz eines Gegenspielers erreichen, der einige andere Sitzungsschlüssel erfahren hat.

2) (Perfect) Forward Secrecy. Wenn Langzeitschlüssel einer oder mehrerer Instanzen gefährdet sind, ist die Geheimhaltung vorheriger Sitzungsschlüssel, die von ehrlichen Instanzen erzeugt werden, nicht betroffen.

3) Nachahmung Schlüsselkompromiss. Es wird angenommen, dass der Langzeitschlüssel von A aufgedeckt wurde. Offensichtlich kann ein Gegenspieler, der diesen Wert kennt, nun A nachahmen, da es genau dieser Wert ist, der A identifiziert. Es kann jedoch wünschenswert sein, dass es dieser Verlust einem Gegenspieler nicht ermöglicht, andere Instanzen gegenüber A nachzuahmen.

4) Unknown-Key-Share. Instanz A kann nicht ohne das Wissen von A dazu gezwungen werden, einen Schlüssel mit Instanz B zu teilen, d.h. wenn A glaubt, dass der Schlüssel mit einer Instanz $C \neq B$ geteilt wird und B (korrekterweise) glaubt, das der Schlüssel mit A geteilt wird.

5) Schlüsselsteuerung. Keine der Instanzen sollte dazu in der Lage sein, den Sitzungsschlüssel auf einen vorher ausgewählten Wert zu drängen.

[0027] Wünschenswerte Leistungsmerkmale von AK- und AKC-Protokollen umfassen eine minimale Anzahl von Arbeitsgängen (die Anzahl der in einem Durchlauf des Protokolls ausgetauschten Nachrichten), einen geringen Kommunikationsaufwand (die Gesamtmenge der übertragenen Bits) und einen geringen rechnerischen Aufwand. Andere Merkmale, die wünschenswert sein können, umfassen die Rollensymmetrie (die zwischen den Instanzen übertragenen Nachrichten weisen die gleiche Struktur auf), die Nicht-Interaktivität (die zwischen den beiden Instanzen übertragenen Nachrichten sind voneinander unabhängig) und die Unabhängigkeit von der Verschlüsselung, Hashfunktionen (da diese bekanntermassen schwer zu entwickeln sind) und der Zeitmarkierung (da sie in der Praxis nur schwer sicher umzusetzen ist).

[0028] Daher ist es eine Aufgabe der vorliegenden Erfindung, ein Schlüsselzustimmungsprotokoll bereitzustellen, bei dem die zuvor genannten Nachteile vermieden oder abgeschwächt werden und das Erreichen der gewünschten Merkmale erleichtert wird.

ZUSAMMENFASSUNG

[0029] In einem Aspekt wird ein Schlüsselzustimmungsprotokoll bereitgestellt, das zwischen einem Paar von Instanzen ausgeführt wird, die über ein Datenkommunikationssystem kommunizieren, wobei mit jeder der Instanzen ein Langzeit-Private-Key, ein zugehöriger kryptographischer Langzeit-Public-Key, der unter Verwendung des Langzeit-Private-Keys generiert wird und eine Identität verknüpft sind, wobei das Protokoll Folgendes umfasst: für jede Instanz Generieren eines jeweiligen Private Keys für die Sitzung und eines zugehörigen kryptographischen Public Keys für die Sitzung; Kommunizieren des Public Keys für die Sitzung jeder Instanz an die andere Instanz; Erhalten der Identität der beiden Instanzen an jeder Instanz; Generieren eines gemeinsamen Werts, an jeder Instanz umfassend das Kombinieren des Public Keys für die Sitzung der Instanz, des Public Keys für die Sitzung der anderen Instanz und der Identitäten jeder Instanz; für jede Instanz Generieren eines jeweiligen geheimen Werts, umfassend das Multiplizieren des gemeinsamen Werts mit dem Private Key für die Sitzung der Instanz und Addieren des Ergebnisses mit dem Langzeit-Private-Key der Instanz; an jeder Instanz Berechnen eines ephemeren Werts, umfassend das Multiplizieren des Public Keys für die Sitzung der anderen Instanz mit dem gemeinsamen Wert und Addieren des Ergebnisses mit dem Langzeit-Public-Key der anderen Instanz; und an jeder Instanz Generieren eines gemeinsamen Geheimnisses durch Kombinieren des geheimen Werts der Instanz und des ephemeren Werts.

[0030] In einem anderen Aspekt wird ein kryptographisches Kommunikationssystem bereitgestellt, wobei das System ein Paar kryptographischer Korrespondenten umfasst, die konfiguriert sind, um die Ausführungsformen des Schlüsselzustimmungsprotokolls zu implementieren.

[0031] In einem weiteren Aspekt wird eine kryptographische Korrespondentvorrichtung, umfassend einen Prozessor und einen Speicher, bereitgestellt, wobei in dem Speicher ein Langzeit-Private-Key gespeichert ist, wobei mit der Vorrichtung ferner ein zugehöriger kryptographischer Langzeit-Public-Key, der unter Verwendung des Langzeit-Private-Keys generiert wird und eine Identität verknüpft sind, wobei in dem Speicher ferner Computerbefehle gespeichert sind, die, wenn sie von dem Prozessor ausgeführt werden, dazu führen, dass der Prozessor ein Schlüsselzustimmungsprotokoll umsetzt, das Folgendes umfasst: Generieren eines Private Keys für die Sitzung und eines zugehörigen kryptographischen Public Keys für die Sitzung; Kommunizieren des Public Keys für die Sitzung über ein Datenkommunikationssystem an eine andere kryptographische Korrespondentvorrichtung; von der anderen kryptographischen Korrespondentvorrichtung Erhalten ihres Public Keys für die Sitzung; Erhalten der Identität der beiden Korrespondenten; Generieren eines gemeinsamen Werts, umfassend das Kombinieren des Public Keys für die Sitzung des Korrespondenten, des Public Keys für die Sitzung des anderen Korrespondenten und der Identitäten jedes Korrespondenten; Generieren eines geheimen Werts, umfassend das Multiplizieren des gemeinsamen Werts mit dem Private Key für die Sitzung des Korrespondenten und Addieren des Ergebnisses mit dem Langzeit-Private-Key; Berechnen eines ephemeren Werts, umfassend das Multiplizieren des Public Keys für die Sitzung des anderen Korrespondenten und des gemeinsamen Werts und Addieren des Ergebnisses mit dem Langzeit-Public-Key des anderen Korrespondenten; und Generieren eines gemeinsamen Geheimnisses aus dem geheimen Wert des Korrespondenten und dem ephemeren Wert.

[0032] Allgemein gesagt, kombiniert das Protokoll die Public Keys für die Sitzung jeder Instanz und die Identitäten jeder Instanz, um einen gemeinsamen Wert zu erhalten, der die beiden Instanzen miteinander verbindet. Dies wird von jeder Instanz verwendet, um einen jeweiligen geheimen Wert durch das Kombinieren des gemeinsamen Werts und sowohl der Sitzungs- als auch der Langzeit-Private-Keys der Instanz zu generieren. Der geheime Wert wird als ein ephemerer Private Key verwendet. Die andere Instanz berechnet unter Verwendung des gemeinsamen Werts einen ephemeren Public Key, der dem geheimen Wert der einen Instanz entspricht. Jede Instanz kann dann aus ihrem ephemeren Private Key und dem ephemeren Public Key der anderen Instanz ein gemeinsames Geheimnis generieren.

[0033] Vorzugsweise wird das gemeinsame Geheimnis als eine Eingabe für eine Schlüsselableitungsfunktion verwendet, um einen gemeinsamen Schlüssel zu erhalten.

[0034] Vorzugsweise wird das Protokoll ebenso in einem Elliptische-Kurven-Kryptosystem implementiert und die Kombination der Public Keys für die Sitzungen wird durch Punktaddition ausgeführt.

[0035] Als eine weitere Präferenz wird die Identität der Instanzen durch ein kryptographisches Zertifikat erhalten, das von einer vertrauenswürdigen Partei erstellt wird.

[0036] Durch das Verbinden der Instanzen, wie oben beschrieben, generiert jeder Durchlauf einen neuen geheimen Wert und mit einer passenden Auswahl der Parameter unter Berücksichtigung der normalen kryptographischen Praxis werden die wünschenswerten Merkmale erreicht.

BESCHREIBUNG DER ZEICHNUNGEN

[0037] Eine Ausführungsform der vorliegenden Erfindung wird nun exemplarisch ausschliesslich in Bezug auf die beigefügten Zeichnungen beschrieben, in denen:

Fig. 1 eine schematische Darstellung eines Datenkommunikationssystems ist;

Fig. 2 eine Darstellung einer Vorrichtung ist, die in dem Datenkommunikationssystem aus Fig. 1 verwendet wird; und

Fig. 3 ein Ablaufplan ist, der das Protokoll zeigt, das zwischen einem Paar von Vorrichtungen, die in Fig. 1 gezeigt werden, implementiert wird.

DETAILLIERTE BESCHREIBUNG

[0038] Wie nachfolgend beschrieben, wird ein wirksames Zwei-Pass-AK-Protokoll vorgeschlagen, das auf einer Diffie-Hellmann-Schlüsselvereinbarung basiert und viele der wünschenswerten Sicherheits- und Leistungsmerkmale aufweist, die in der 1997 erschienen Abhandlung von S. Blake-Wilson, D. Johnson und A. Menezes mit dem Titel: «Key agreement protocols and their security analysis» erörtert werden.

[0039] Das nachfolgend beschriebene Protokoll wurde in dem Kontext der Gruppe von Punkten auf einer elliptischen Kurve beschrieben, die für einen endlichen Körper festgelegt sind. Es kann jedoch einfach verändert werden, um für eine beliebige endliche Gruppe zu funktionieren, in welcher das diskrete Logarithmus-Problem unlösbar erscheint. Geeignete Auswahlmöglichkeiten umfassen die multiplikative Gruppe eines endlichen Körpers, Untergruppen von Z^*_n, wobei n eine zusammengesetzte ganze Zahl ist und nicht triviale Untergruppen von Z^*_p der Primordnung q. Elliptische-Kurven-Gruppen sind vorteilhaft, da sie eine gleichwertige Sicherheit wie die anderen Gruppen anbieten, jedoch mit kleineren Schlüsselgrössen und schnelleren Rechenzeiten.

[0040] Daher umfasst ein Datenkommunikationssystem 10 in Bezug auf Fig. 1 eine Vielzahl von Vorrichtungen 12, die durch Kommunikationsverbindungen 14 miteinander verbunden sind. Die Vorrichtungen 12 können zu einer beliebigen bekannten Art gehören, umfassend einen Computer 12a, einen Server 12b, ein Mobiltelefon 12c, einen Geldautomaten 12d und eine Chipkarte 12e. Die Kommunikationsverbindungen 14 können herkömmliche Festnetztelefonanschlüsse, drahtlose Verbindungen, die zwischen den Vorrichtungen 12 implementiert sind, Verbindungen für die Nahfeldkommunikation wie Bluetooth oder andere herkömmliche Formen der Kommunikation sein.

[0041] Die Vorrichtungen 12 unterscheiden sich gemäss ihrem Verwendungszweck, umfassen aber üblicherweise ein Kommunikationsmodul 20 (Fig. 2) für die Kommunikation mit den Verbindungen 14. Ein Speicher 22 stellt ein Speichermedium für dauerhafte Befehle bereit, um Protokolle zu implementieren und Daten wie gewünscht zu speichern. Die Befehle werden von einem kryptographischen Prozessor (30) ausgeführt. Ein sicheres Speichermodul 24, welches Teil des Speichers 22 oder ein separates Modul sein kann, wird zum Speichern privater Informationen wie den in den Verschlüsselungsprotokollen verwendeten Private Keys verwendet und um einer Manipulation mit diesen Daten standzuhalten. Es wird eine arithmetische Logikeinheit (ALU) 26 bereitgestellt, um die arithmetischen Operationsbefehle von dem Speicher 22 unter Verwendung der in den Speichern 22, 24 gespeicherten Daten auszuführen. Es wird ebenso ein Zufalls- oder Pseudozufallszahlengenerator 28 integriert, um Bitfolgen zu generieren, die Zufallszahlen auf kryptographisch sichere Art und Weise darstellen.

[0042] Es wird gewürdigt, dass die in Fig. 2 veranschaulichte Vorrichtung 12 stark schematisiert und für eine in einem Datenkommunikationssystem verwendete herkömmliche Vorrichtung repräsentativ ist.

[0043] Der Speicher 22 speichert Systemparameter für das zu implementierende Kryptosystem und eine Reihe von computerlesbaren Befehlen zum Implementieren des geforderten Protokolls. Im Falle eines Elliptische-Kurven-Kryptosystems bestehen Elliptische-Kurven-Domänenparameter aus sechs Mengen q, a, b, P, n und h, die Folgendes sind:

- Die Feldgrösse q
- Die Koeffizienten der elliptischen Kurve a und b
- Der Basispunktgenerator P
- Die Ordnung n des Basispunktgenerators
- Der Kofaktor h, welcher die Anzahl ist, sodass hn die Anzahl von Punkten auf der elliptischen Kurve ist.

[0044] Die Parameter werden als Bitfolgen und die Darstellung des Basispunkts G wird als ein Paar von Bitfolgen dargestellt, die jeweils ein Element des zugrunde liegenden Felds darstellen. So wie es üblich ist, kann eine dieser Folgen gekürzt sein, da die vollständige Darstellung durch die andere Koordinate und die gekürzte Darstellung wiederhergestellt werden kann.

[0045] Das sichere Speichermodul 24 enthält eine Bitfolge, die einen Langzeit-Private-Key d und den zugehörigen Public Key Q darstellt. Für ein Elliptische-Kurven-Kryptosystem gilt: der Schlüssel Q = dP.

[0046] Der sichere Speicher 24 umfasst ebenso eine Identifizierung ID der Vorrichtung 12. Praktischerweise ist dies ein Zertifikat, das von einer vertrauenswürdigen Stelle erstellt wird, um die Überprüfung der Identität durch Dritte zu ermöglichen. Eine geeignete Form von Zertifikat ist ein ECQV-Zertifikat, wie in dem SEC 4-Standard dargelegt.

[0047] Ephemere Werte, die von der ALU berechnet werden, können ebenso in dem sicheren Modul 24 gespeichert werden, wenn ihr Wert geheim sein soll.

[0048] Das Schlüsselzustimmungsprotokoll wird in Fig. 3 gezeigt und zwischen einem Paar von Vorrichtungen ausgeführt, die als die Instanz Alice und die Instanz Bob bezeichnet werden. Mit Alice verknüpfte Werte werden mit dem Zusatz A und diejenigen von Bob mit dem Zusatz B gekennzeichnet. Alice weist einen Langzeit-Private-Key d_A und einen zugehörigen Public Key Q_A auf, die in dem sicheren Speichermodul 24 gespeichert sind. Gleichermassen weist Bob einen Private Key d_B und einen zugehörigen Public Key Q_B auf, die in seinem sicheren Speichermodul 24 gespeichert sind.

[0049] Die Instanzen Alice und Bob wollen einen gemeinsamen Schlüssel teilen und implementieren demzufolge durch die in dem Speicher 22 gespeicherten Befehle das in Fig. 3 gezeigte Protokoll.

[0050] Bei 100 generiert Alice unter Verwendung des RNG 28 eine zufällige ganze Zahl und speichert den ganzzahligen Wert a als den Private Key für die Sitzung in dem sicheren Modul 24. Die ALU 26 von Alice berechnet bei 102 einen zugehörigen Public Key für die Sitzung aP, welchen sie über eine Kommunikationsverbindung 16 an Bob sendet. Der Public Key für die Sitzung aP ist eine Darstellung eines Punktes auf der Kurve und weist ein Paar von Bitfolgen auf, die jeweils ein Element in dem zugrunde liegenden Feld darstellen. Bei einigen Implementierungen, der von der ALU 26 durchgeführten Berechnungen, ist es lediglich notwendig, die x-Koordinate des Punktes zu verwenden, wobei die y-Koordinate in diesem Fall nicht notwendig ist. Die x-Koordinate ist in dieser Situation für den Public Key aP repräsentativ. Die y-Koordinate kann bei Bedarf aus der x-Koordinate wiederhergestellt werden. Es können ebenso Verfahren für die Punktkompression verwendet werden, bei denen eine Angabe des Werts der y-Koordinate mit der x-Koordinate gesendet wird, falls sie bevorzugt sind, um die Bandbreite bei der Übertragung zu verringern.

[0051] Gleichermassen generiert Bob bei 200 mit seinem RNG 28 eine zufällige ganze Zahl, welche er in seinem sicheren Modul 24 als ein Private Key für die Sitzung b speichert. Ein zugehöriger Public Key für die Sitzung bP wird bei 202 berechnet und über eine Kommunikationsverbindung 16 an Alice gesendet.

[0052] Sowohl Alice als auch Bob führen unter Verwendung der ALU 26 eine Punktaddition aus, um $y = bP + aP$ zu berechnen, wie es bei 104, 204 gezeigt wird. Dies ist wiederum ein weiterer Punkt, y, auf der Kurve und wird demnach als ein Paar von Elementen dargestellt. In Ausführungsformen ist es möglich, lediglich die x-Koordinate der Summe der Public Keys bei der Berechnung von y zu verwenden.

[0053] In weiteren Ausführungsformen, wobei das Protokoll in einem Hyperelliptische-Kurven-Kryptosystem implementiert ist, wird die Kombination der Public Keys durch Punktaddition in der Jacobimatrix der hyperelliptischen Kurve ausgeführt.

[0054] Sowohl Alice als auch Bob erhalten Kopien der Identität des anderen (106, 206). Dies kann vor der Implementierung des Protokolls stattfinden oder das Zertifikat kann mit den Public Keys für die Sitzungen verschickt werden. Das Zertifikat kann bei Bedarf von dem Empfänger überprüft werden.

[0055] Bei 108, 208 berechnen Alice und Bob jeweils einen gemeinsamen Wert $c = H(y//ID_A//ID_B)$, wobei H eine kryptograpisch sichere Hashfunktion wie eine SHA2-Hash-Funktion ist. Der Wert c wird in dem Speicher 22 gespeichert. Der gemeinsame Wert c verbindet Alice und Bob. Durch die Konkatenation der Identitäten ID ist es notwendig, die Ordnung zu bestimmen, in welcher der String, der c darstellt, zusammengesetzt ist, wobei die Verwendung der lexikographischen Ordnung eine weit verbreitete Option darstellt. Als eine Alternative können die Identitäten demnach durch XOR-Verknüpfung der IDs kombiniert werden und dadurch wird es ermöglicht, dass der String ohne Rücksicht auf die Ordnung zusammengesetzt werden kann. Gleichermassen kann für y eine XOR-Verknüpfung mit den IDs hergestellt werden, falls bevorzugt.

[0056] Alice berechnet bei 110 eine Komponente $s_A = d_A + c \bullet a(\text{mod } n)$, welche die in dem sicheren Modul 24 gespeicherten Langzeit- und Kurzzeit- Private - Keys verwendet.

[0057] Gleichermassen berechnet Bob an 210 $s_B = d_B + c \bullet b(\text{mod } n)$.

[0058] Aus öffentlichen Informationen, umfassend den von Bob empfangenen Public Key für die Sitzung bP, kann Alice $s_BP = Q_B + c \bullet bP$ berechnen, wie bei 112 gezeigt.

[0059] Gleichermassen kann Bob $s_AP = Q_A + c \bullet aP(212)$ berechnen.

[0060] Alice und Bob weisen jeweils eine Komponente, die aus privaten Informationen und dem gemeinsamen Wert berechnet wurde und eine Komponente auf, die aus öffentlichen Informationen berechnet wurde. Diese können kombiniert werden, um ein gemeinsames Geheimnis bereitzustellen.

[0061] Daher können Alice und Bob bei 114, 214 beide den Wert $K = h^{\bullet}s_A{}^{\bullet}s_B{}^{\bullet}P$ als das gemeinsame Geheimnis berechnen.

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

[0063] Gleichermassen hat Bob s_AP berechnet und den Wert s_B gespeichert.

[0064] Eine andere Option zur Berechnung des gemeinsamen Geheimnisses ist für Alice die Berechnung von $K = s_A{}^{\bullet}s_BP$ und für Bob die Berechnung von $K = s_B{}^{\bullet}s_AP$, unter Nichtbeachtung des Kofaktors h. Dies ist nützlich, wenn der Wert von h klein, z.B. 1 ist oder wenn es Widerstand gegen den Kleingruppenangriff gibt.

[0065] Das zuvor beschriebene Protokoll erzeugt demnach ein gemeinsames Geheimnis K zwischen zwei Instanzen. Es sollte eine Schlüsselableitungsfunktion verwendet werden, um einen geheimen Schlüssel aus dem gemeinsamen Schlüssel abzuleiten. Dies ist notwendig, da das gemeinsame Geheimnis K ein schwaches Bit aufweisen kann – Bits von Informationen über K, die mit nicht unerheblichen Vorteilen korrekt vorhergesagt werden können.

[0066] Eine Möglichkeit zur Ableitung eines Schlüssels von dem gemeinsamen Geheimnis K ist die Anwendung einer Einweg-Hashfunktion wie SHA-1 für K. Alternativ können andere Schlüsselableitungsfunktionen verwendet werden, wie ausführlicher in Kapitel XX des Handbook of Applied Cryptography zu finden, dessen Inhalte durch Bezugnahme eingeführt werden.

[0067] Zusammenfassend kann das Schlüsselzustimmungsprotokoll unter Verwendung des folgenden Verfahrens implementiert werden:

1) Alice erhält eine authentische Kopie des Langzeit-Public-Keys von Bob Q_B.

2) Alice generiert eine zufällige ganze Zahl, um einen Private Key für die Sitzung $a(0 < a < n)$ bereitzustellen.

3) Alice berechnet aP und sendet dies an Bob.

4) Bob erhält eine authentische Kopie des Langzeit-Public-Keys von Alice Q_A.

5) Bob generiert eine zufällige ganze Zahl b, $(0 < b < n)$.

6) Bob berechnet bP und sendet dies an Alice.

7) Sowohl Alice als auch Bob berechnen $y = bP + aP$.

8) Sowohl Alice als auch Bob berechnen $c = H(y//ID_A//ID_B)$. (Hinweis: Die ID_A und ID_B können jeweils die Public Keys von Alice und Bob enthalten und sie sind lexikographisch geordnet).

9) Alice berechnet $s_A = d_A + c \bullet a(\text{mod } n)$.

10) Alice berechnet $s_BP = Q_B + c \bullet bP$. (Hinweis: Bob hat bP an Alice gesendet und sie hat eine authentische Kopie von QB erhalten).

11) Bob berechnet $s_B = d_B + c \bullet b(\text{mod } n)$.

12) Bob berechnet aus öffentlichen Informationen $sAP = QA + c \bullet aP$.

13) Alice kann nun $h^*s_A^*s_B^*P$ berechnen und Bob kann nun $h^*s_B^*s_AP$ berechnen. In beiden Fällen ist das Ergebnis das gleiche gemeinsame Geheimnis $K = h^*s_A^*s_B^*P$.

14) Das gemeinsame Geheimnis kann bei Bedarf als die Eingabe für eine Schlüsselableitungsfunktion verwendet werden.

[0068] Eine andere Option zur Berechnung des gemeinsamen Geheimnisses ist $K = s_A^*s_B^*P$, unter Nichtbeachtung des Kofaktors h. Dies ist nützlich, wenn der Wert von h klein, z.B. 1 ist oder wenn es Widerstand gegen den Kleinuntergruppenangriff gibt.

Patentansprüche

1. Schlüsselzustimmungsprotokoll, das zwischen einem Paar von Instanzen ausgeführt wird, die über ein Datenkommunikationssystem kommunizieren, wobei mit jeder der Instanzen ein Langzeit-Private-Key, ein zugehöriger kryptographischer Langzeit-Public-Key, der unter Verwendung des Langzeit-Private-Keys und eines Generatorpunkts generiert wird und eine Identität verknüpft sind, wobei das Protokoll Folgendes umfasst:
   für jede Instanz Generieren eines jeweiligen Private Keys für die Sitzung und eines zugehörigen kryptographischen Public Keys für die Sitzung;
   Kommunizieren des Public Keys für die Sitzung jeder Instanz an die andere Instanz; Erhalten der Identität der beiden Instanzen an jeder Instanz;
   Generieren eines gemeinsamen Werts, an jeder Instanz umfassend das Kombinieren des Public Keys für die Sitzung der Instanz, des Public Keys für die Sitzung der anderen Instanz und der Identitäten jeder Instanz;
   für jede Instanz Generieren eines jeweiligen geheimen Werts, umfassend das Multiplizieren des gemeinsamen Werts mit dem Private Key für die Sitzung der Instanz und Addieren des Ergebnisses mit dem Langzeit-Private-Key der Instanz;
   an jeder Instanz Berechnen eines ephemeren Werts, umfassend das Multiplizieren des Public Keys für die Sitzung der anderen Instanz mit dem gemeinsamen Wert und Addieren des Ergebnisses mit dem Langzeit-Public-Key der anderen Instanz; und
   an jeder Instanz Generieren eines gemeinsamen Geheimnisses durch Kombinieren des geheimen Werts der Instanz und des ephemeren Werts.
2. Protokoll nach Anspruch 1, wobei das gemeinsame Geheimnis als eine Eingabe für eine Schlüsselableitungsfunktion verwendet wird, um einen gemeinsamen Schlüssel zu erhalten.
3. Protokoll nach Anspruch 1, wobei das Generieren eines gemeinsamen Werts das Anwenden einer XOR-Operation für die Identitäten jeder Instanz umfasst.
4. Protokoll nach Anspruch 1, wobei das Protokoll in einem Elliptische-Kurven-Kryptosystem implementiert und die Kombination der Public Keys für die Sitzungen durch Punktaddition ausgeführt wird.
5. Protokoll nach Anspruch 1, wobei das Protokoll in einem Elliptische-Kurven-Kryptosystem implementiert wird und das Generieren des gemeinsamen Werts das Erhalten einer x-Koordinate aus der Summe der Public Keys umfasst.
6. Protokoll nach Anspruch 1, wobei das Protokoll in einem Hyperelliptische-Kurven-Kryptosystem implementiert und die Kombination der Public Keys durch Punktaddition in der Jacobimatrix der hyperelliptischen Kurve ausgeführt wird.
7. Protokoll nach Anspruch 1, wobei das Generieren des Public Keys für die Sitzung eine Skalarmultiplikation des Private Keys für die Sitzung und des Generatorpunkts umfasst.
8. Protokoll nach Anspruch 1, wobei die Kombination des geheimen Werts und des ephemeren Werts die Skalarmultiplikation des geheimen Werts und des ephemeren Werts ist.
9. Protokoll nach Anspruch 1, wobei die Kombination des geheimen Werts und des ephemeren Werts die Skalarmultiplikation des Kofaktors, des geheimen Werts und des ephemeren Werts ist.
10. Protokoll nach Anspruch 1, wobei die Identität der Instanzen durch ein kryptographisches Zertifikat erhalten wird, das von einer vertrauenswürdigen Partei erstellt wird.

11. Kryptographisches Kommunikationssystem, umfassend ein Paar kryptographischer Korrespondenten, die konfiguriert sind, um das Schlüsselzustimmungsprotokoll nach Anspruch 1 zu implementieren.

12. Kryptographische Korrespondentvorrichtung, umfassend einen Prozessor und einen Speicher, wobei in dem Speicher ein Langzeit-Private-Key gespeichert ist, wobei mit der Vorrichtung ferner ein zugehöriger kryptographischer Langzeit-Public-Key, der unter Verwendung des Langzeit-Private-Keys und eines kryptographischen Generatorpunkts generiert wird und eine Identität verknüpft sind, wobei in dem Speicher ferner Computerbefehle gespeichert sind, die, wenn sie von dem Prozessor ausgeführt werden, dazu führen, dass der Prozessor ein Schlüsselzustimmungsprotokoll umsetzt, das Folgendes umfasst:
Generieren eines Private Keys für die Sitzung und eines zugehörigen kryptographischen Public Keys für die Sitzung;
Kommunizieren des Public Keys für die Sitzung über ein Datenkommunikationssystem an eine andere kryptographische Korrespondentvorrichtung;
von der anderen kryptographischen Korrespondentvorrichtung Erhalten ihres Public Keys für die Sitzung;
Erhalten der Identität der beiden Korrespondenten;
Generieren eines gemeinsamen Werts, umfassend das Kombinieren des Public Keys für die Sitzung des Korrespondenten, des Public Keys für die Sitzung des anderen Korrespondenten und der Identitäten jedes Korrespondenten;
Generieren eines geheimen Werts, umfassend das Multiplizieren des gemeinsamen Werts mit dem Private Key für die Sitzung des Korrespondenten und Addieren des Ergebnisses mit dem Langzeit-Private-Key;
Berechnen eines ephemeren Werts, umfassend das Multiplizieren des Public Keys für die Sitzung des anderen Korrespondenten und des gemeinsamen Werts und Addieren des Ergebnisses mit dem Langzeit-Public-Key des anderen Korrespondenten; und
Generieren eines gemeinsamen Geheimnisses aus dem geheimen Wert des Korrespondenten und dem ephemeren Wert.

13. Vorrichtung nach Anspruch 12, wobei das gemeinsame Geheimnis als eine Eingabe für eine Schlüsselableitungsfunktion verwendet wird, um einen gemeinsamen Schlüssel zu erhalten.

14. Vorrichtung nach Anspruch 12, wobei das Generieren eines gemeinsamen Werts das Anwenden einer XOR-Operation für die Identitäten jedes Korrespondenten umfasst.

15. Vorrichtung nach Anspruch 12, wobei das Protokoll in einem Elliptische-Kurven-Kryptosystem implementiert und die Kombination der Public Keys für die Sitzungen durch Punktaddition ausgeführt wird.

16. Vorrichtung nach Anspruch 12, wobei das Protokoll in einem Elliptische-Kurven-Kryptosystem implementiert wird und das Generieren des gemeinsamen Werts das Erhalten einer x-Koordinate aus der Summe der Public Keys umfasst.

17. Vorrichtung nach Anspruch 12, wobei das Protokoll in einem Hyperelliptische-Kurven-Kryptosystem implementiert und die Kombination der Public Keys durch Punktaddition in der Jacobimatrix der hyperelliptischen Kurve ausgeführt wird.

18. Vorrichtung nach Anspruch 12, wobei das Generieren des Public Keys für die Sitzung eine Skalarmultiplikation des Private Keys für die Sitzung und des Generatorpunkts umfasst.

19. Vorrichtung nach Anspruch 12, wobei die Kombination des geheimen Werts und des ephemeren Werts die Skalarmultiplikation des geheimen Werts und des ephemeren Werts ist.

20. Vorrichtung nach Anspruch 12, wobei die Kombination des geheimen Werts und des ephemeren Werts die Skalarmultiplikation des Kofaktors, des geheimen Werts und des ephemeren Werts ist.

21. Vorrichtung nach Anspruch 12, wobei die Identität der Korrespondenten durch ein kryptographisches Zertifikat erhalten wird, das von einer vertrauenswürdigen Partei erstellt wird.

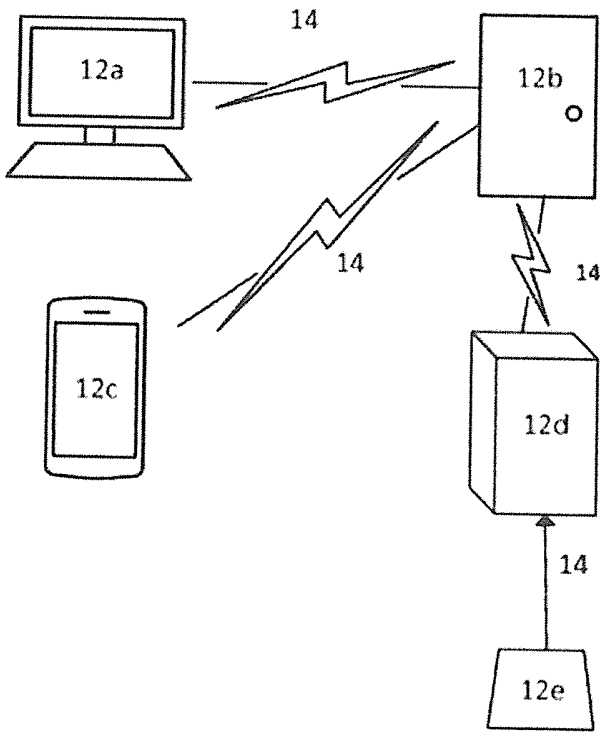


FIG. 1

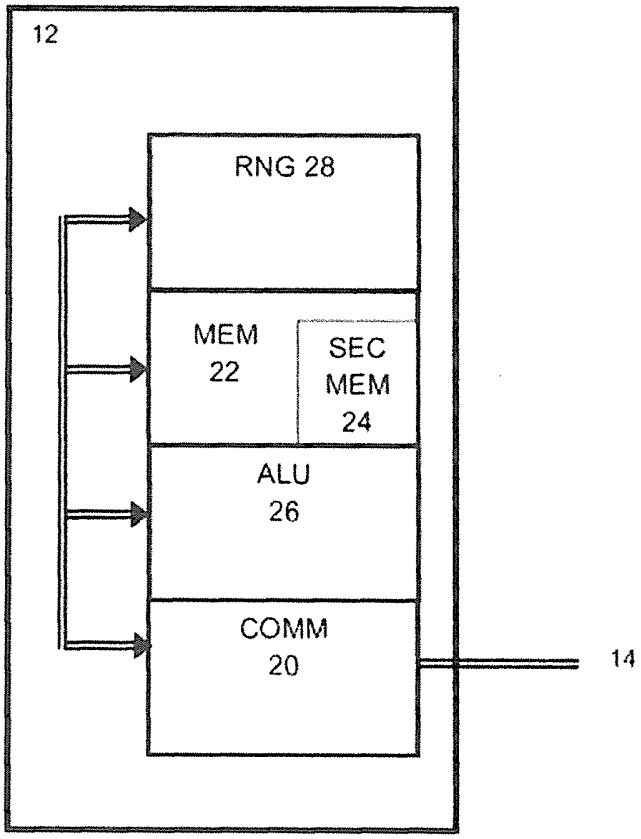


FIG. 2

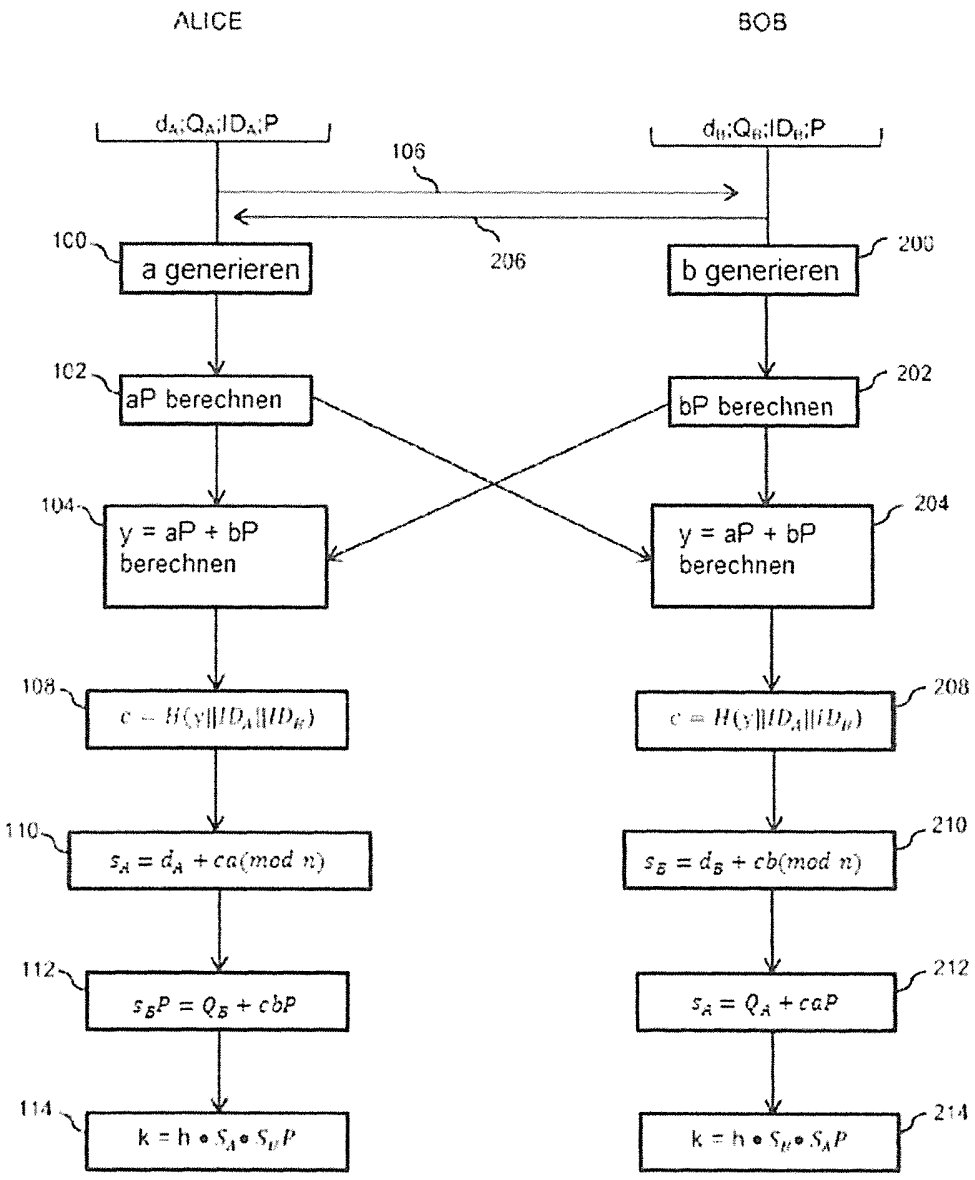

ALICE
BOB
$d_A;Q_A;ID_A;P$
$d_B;Q_B;ID_B;P$
106
206
100
a generieren
200
b generieren
102
aP berechnen
202
bP berechnen
104
y = aP + bP berechnen
204
y = aP + bP berechnen
108
$c = H(y\|ID_A\|ID_B)$
208
$c = H(y\|ID_A\|ID_B)$
110
$s_A = d_A + ca(mod\ n)$
210
$s_B = d_B + cb(mod\ n)$
112
$s_B P = Q_B + cbP$
212
$s_A = Q_A + caP$
114
$k = h \bullet S_A \bullet S_B P$
214
$k = h \bullet S_B \bullet S_A P$

FIG. 3