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

(10) **DE 699 21 039 T2** 2006.02.16

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 0 977 396 B1**
(21) Deutsches Aktenzeichen: **699 21 039.9**
(96) Europäisches Aktenzeichen: **99 305 706.6**
(96) Europäischer Anmeldetag: **20.07.1999**
(97) Erstveröffentlichung durch das EPA: **02.02.2000**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **13.10.2004**
(47) Veröffentlichungstag im Patentblatt: **16.02.2006**

(51) Int Cl.[8]: ***H04L 9/08*** (2006.01)
H04L 9/32 (2006.01)

(30) Unionspriorität:
127769 **31.07.1998** **US**

(84) Benannte Vertragsstaaten:
DE, FR, GB

(73) Patentinhaber:
Lucent Technologies Inc., Murray Hill, N.J., US

(72) Erfinder:
Berenzweig, Adam L., New York 10003, US; Patel, Sarvar, Montville, US

(74) Vertreter:
derzeit kein Vertreter bestellt

(54) Bezeichnung: **Verfahren zur Erstellung eines Schlüssels unter Verwendung einer Funkkommunikation und eines Kennwortprotokolls**

Anmerkung: Innerhalb von neun Monaten nach der Bekanntmachung des Hinweises auf die Erteilung des europäischen Patents kann jedermann beim Europäischen Patentamt gegen das erteilte europäische Patent Einspruch einlegen. Der Einspruch ist schriftlich einzureichen und zu begründen. Er gilt erst als eingelegt, wenn die Einspruchsgebühr entrichtet worden ist (Art. 99 (1) Europäisches Patentübereinkommen).

Die Übersetzung ist gemäß Artikel II § 3 Abs. 1 IntPatÜG 1991 vom Patentinhaber eingereicht worden. Sie wurde vom Deutschen Patent- und Markenamt inhaltlich nicht geprüft.

Beschreibung

Erfindungsgebiet

[0001] Die vorliegende Erfindung betrifft ein Paßwort-Protokoll und ein Verfahren zur Erstellung eines Schlüssels unter Verwendung von drahtloser Kommunikation und in einer Ausführungsform das Paßwort-Protokoll.

Stand der Technik

[0002] In einem drahtlosen Kommunikationssystem werden die oft Mobilfunkgeräte genannten Handapparate, die von Mobilfunkgerätebenutzern gekauft werden, typischerweise zu einem in Netzdiensteanbieter genommen und in den Handapparat werden lange Schlüssel und Parameter eingegeben, um Dienst zu aktivieren. Vom Netz des Diensteanbieters wird auch eine Kopie der langen Schlüssel und Parameter für das Mobilfunkgerät unterhalten und dem Mobilfunkgerät zugeordnet. Wie wohl bekannt ist, können auf Grundlage dieser langen Schlüssel und Parameter Informationen sicher drahtlos zwischen dem Netz und dem Mobilfunkgerät übertragen werden.

[0003] Als Alternative empfängt der Benutzer lange Schlüssel von dem Diensteanbieter über einen sicheren Kommunikationskanal wie beispielsweise eine Fernsprech-/Festleitung und muß diese Codes von Hand in das Mobilfunkgerät eingeben.

[0004] Da die Übertragung der langen Schlüssel und Parameter über eine Fernsprech-/Festleitung oder beim Netzdiensteanbieter durchgeführt wird und nicht drahtlos, ist die Übertragung sicher gegen drahtlose Angriffe. Durch dieses Verfahren der sicheren Übertragung werden jedoch dem Mobilfunkgerätebenutzer gewisse Belastungen und Einschränkungen auferlegt. Vorzugsweise sollte der Mobilfunkgerätebenutzer in der Lage sein, seine Handapparate zu kaufen und dann den Dienst von jedem Diensteanbieter zu erhalten, ohne die Handapparate physisch zum Ort des Anbieters zu nehmen oder lange Schlüssel von Hand und fehlerfrei in das Mobilfunkgerät eingeben zu müssen. Die Fähigkeit zum Aktivieren und Ausstatten des Mobilfunkgeräts aus der Ferne ist Teil der nordamerikanischen drahtlosen Standards und wird als OTASP (Over The Air Service provisioning – drahtlose Dienstebeschaffung) bezeichnet.

[0005] Gegenwärtig ist im nordamerikanischen Zellularstandard IS41-C ein OTASP-Protokoll angegeben, das die wohlbekannte Diffie-Hellman-(DH-)Schlüsselvereinbarung zur Erstellung eines Geheimschlüssels zwischen zwei Teilnehmern benutzt. Fig. 1 zeigt die Anwendung der DH-Schlüsselvereinbarung zur Erstellung eines Geheimschlüssels zwischen einem Mobilfunkgerät **20** und einem Netz **10**, das in IS41-C benutzt wird. Die Fig. 1 zeigt in vereinfachter Form der Klarheit halber die Kommunikation zwischen einem Netz **10** und einem Mobilfunkgerät **20** gemäß der DH-Schlüsselvereinbarung. So wie er hier benutzt wird bezieht sich der Begriff Netz auf die Berechtigungszentren, Heimatregister, Besucherregister, Mobilvermittlungsstellen und Basisstationen, die von einem Netzdiensteanbieter betrieben werden.

[0006] Von Netz **10** wird eine Zufallszahl R_N erzeugt und ($g^{\wedge}R_N$ mod p) berechnet. Nach der Darsellung in Fig. 1 sendet das Netz **10** eine 512-Bit-Primzahl p, den Generator g der durch die Primzahl p erzeugten Gruppe und ($g^{\wedge}R_N$ mod p) zum Mobilfunkgerät **20**. Als nächstes erzeugt das Mobilfunkgerät **20** eine Zufallszahl R_M, berechnet ($g^{\wedge}R_M$ mod p) und sendet ($g^{\wedge}R_M$ mod p) zum Netz **10**.

[0007] Vom Mobilfunkgerät **20** wird das empfangene ($g^{\wedge}R_N$ mod p) vom Netz **10** zur Potenz R_M erhoben, um ($g^{\wedge}R_MR_N$ mod p) zu erhalten. Vom Netz **10** wird das empfangene ($g^{\wedge}R_M$ mod p) vom Mobilfunkgerät **20** zur Potenz R_N erhoben, um ebenfalls ($g^{\wedge}R_MR_N$ mod p) zu erhalten. Sowohl Mobilfunkgerät **20** als auch das Netz **10** erhalten dasselbe Ergebnis und erstellen die 64 niederwertigsten Bit als den A-Schlüssel genannten langlebigen Schlüssel. Der A-Schlüssel dient als Wurzelschlüssel zum Ableiten von anderen, bei der Sicherstellung der Kommunikation zwischen dem Mobilfunkgerät **20** und dem Netz **10** benutzten Schlüsseln.

[0008] Eines der Probleme bei dem DH-Schlüsselaustausch besteht darin, daß er unberechtigt ist und für einen Lauschangriff empfindlich ist. Beispielsweise kann in dem obigen Mobilfunkgerät-Netz-Beispiel mit zwei Teilnehmern ein Angreifer das Netz **10** vortäuschen und dann wiederum dem Netz **10** das Mobilfunkgerät **20** vortäuschen. Auf diese Weise kann der Angreifer den A-Schlüssel auswählen und kennen, da er Nachrichten zwischen dem Mobilfunkgerät **20** und dem Netz **10** weiterleitet, um die Berechtigungserfordernisse zu erfüllen. Der DH-Schlüsselaustausch ist ebenfalls für sogenannte Off-Line-Wörterbuchangriffe (Dictionary Attacks) empfänglich.

[0009] Ein weiteres wohlbekanntes Protokoll zum Schützen der drahtlosen Übertragung von Informationen wie beispielsweise dem A-Schlüssel ist der DH-EKE (Diffie-Hellman Encrypted Key Exchange – Verschlüsselter Diffie-Hellman-Schlüsselaustausch). DH-EKE ist ein auf Paßwort basierendes Protokoll zum Austausch von Informationen und nimmt an, daß sowohl der Mobilfunkgerätebenutzer als auch der Netzdiensteanbieter vor der drahtlosen Übertragung ein Paßwort erstellt haben. Ungleich dem in bezug auf Fig. 1 besprochenen DH-Schlüsselaustausch-

system schützt der DH-EKE gegen Lauschangriffe und Off-Line-Wörterbuchangriffe.

[0010] Der DH-EKE wird in bezug auf Fig. 2 beschrieben, die die Kommunikation zwischen dem Mobilfunkgerät **20** und dem Netz **10** gemäß dem DH-EKE-Protokoll darstellt. Nach der Darstellung sendet das Mobilfunkgerät **20** eine 512-Bit-Primzahl p und den Generator g zum Netz **10** zusammen mit (g^{R_M} mod p) verschlüsselt gemäß einem Verschlüsselungs/Entschlüsselungsalgorithmus ENC unter Verwendung des Paßworts P, das dem Mobilfunkgerätebenutzer und dem Netz **10** bekannt ist, als Verschlüsselungsschlüssel. Diese Berechnung wird als ENC_P (g^{R_M} mod p) dargestellt. Das Netz **10** entschlüsselt (g^{R_M} mod p) unter Verwendung des Paßworts P und berechnet (g^{R_M} mod p) ^{R_N}, was gleich ($g^{R_M R_N}$ mod p) ist. Vom Netz **10** wird ($g^{R_M R_N}$ mod p) ausgewählt, eine Mischsumme dieses Werts oder irgendeinen Teil derselben als ein Sitzungsschlüssel SK (Session Key).

[0011] Dann sendet das Netz **10** (g^{R_N} mod p) verschlüsselt nach ENC unter Verwendung des Paßworts P und eine Zufallszahl R_N' verschlüsselt nach ENC unter Verwendung der Sitzungsschlüssels SK zum Mobilfunkgerät **20**. Vom Mobilfunkgerät **20** wird (g^{R_N} mod p) unter Verwendung des Paßworts P entschlüsselt und dann auf (g^{R_N} mod p) ^{R_M} berechnet, was gleich ($g^{R_M R_N}$ mod p) ist. Dann wird vom Mobilfunkgerät **20** ($g^{R_M R_N}$ mod p), die Mischsumme davon oder ein Teil davon, so wie es das Netz **10** tat, als Sitzungsschlüssel SK ausgewählt. Unter Verwendung des Sitzungsschlüssels SK entschlüsselt das Mobilfunkgerät **20** dann R_N'.

[0012] Als nächstes erzeugt das Mobilfunkgerät **20** eine Zufallszahl R_M', verschlüsselt die Zufallszahlen R_M' und R_N' nach ENC unter Verwendung des Sitzungsschlüssels SK und sendet die verschlüsselten Zufallszahlen R_N' und R_M' zum Netz **10**. Vom Netz **10** werden die Zufallszahlen R_N' und R_M' unter Verwendung des Sitzungsschlüssels SK entschlüsselt und bestimmt, ob die entschlüsselte Version von R_N' der ursprünglich zum Mobilfunkgerät **20** gesendeten Version von R_N' gleich ist. Der Sitzungsschlüssel SK wird vom Netz **10** bestätigt, wenn die entschlüsselte Version von R_M' der ursprünglich zum Netz **10** gesendeten Version von R_M' gleich ist.

[0013] Das Netz **10** sendet dann die unter Verwendung des Sitzungsschlüssels SK verschlüsselte Zufallszahl R_M' zum Mobilfunkgerät **20**. Das Mobilfunkgerät **20** entschlüsselt die Zufallszahl R_M' unter Verwendung des Sitzungsschlüssels SK und bestimmt, ob die berechnete Version von R_M' der ursprünglich zum Netz **10** gesendeten Version von R_M' gleich ist. Der Sitzungsschlüssel SK wird vom Mobilfunkgerät **20** bestätigt, wenn die entschlüsselte Version von R_M' der ursprünglich zum Netz **10** gesendeten Version von R_M' gleich ist.

[0014] Sobald das Netz **10** und das Mobilfunkgerät **20** den Sitzungsschlüssel SK bestätigt haben, wird der Sitzungsschlüssel SK als der A-Schlüssel benutzt und Kommunikation zwischen dem Mobilfunkgerät **20** und dem Netz **10** wird unter Verwendung des A-Schlüssels umkonfiguriert.

[0015] Während das DH-EKE-Protokoll Lauschangriffe und Off-Line-Wörterbuchangriffe eliminiert, können Informationen immer noch aussickern und ein Angreifer kann das Paßwort P wiedergewinnen.

[0016] Jablon D.P.: „Strong Password-Only Authenticated Key Exchange" (Starker berechtigter Schlüsselaustausch nur mit Paßwort) Computer Communications Review, Association For Computing Machinery, New York, USA, Band 26, Nr. 5, 1. Oktober 1996 (1996-10-01), Seiten 5-26, XP000641968 ISSN:0146-4833 befaßt sich mit Schlüsselaustausch und insbesondere mit zwei Verfahren von starker Berechtigung nur mit Paßwort, die beide Formen eines berechtigten Schlüsselaustausch sind. Das erste Verfahren ist ein SPEKE-Austausch (Simple Password Exponential Key Exchange – Exponentieller Schlüsselaustausch mit einfachem Paßwort), der zwei Stufen aufweist. Die erste Stufe benutzt einen Diffie-Hellman (DH-)Austausch zur Erstellung eines gemeinsamen Schlüssels K, aber anstelle eines gemeinsam benutzten festen primitiven Oberfläche g, wandelt eine Funktion f ein Paßwort S in eine Basis zur Potenzierung um. Der Rest der ersten Stufe ist der Diffie-Hellman-Austausch. Die zweite Stufe ist eine Bestätigungsstufe zum Bestätigen der Kenntnis von K, ehe er als Sitzungsschlüssel benutzt wird.

[0017] Der DH-EKE-Austausch (Diffie-Hellman Encrypted Key Exchange) ist ein weiteres Berechtigungsverfahren mit zwei Stufen. Die erste Stufe benutzt einen DH-Austausch zum Erstellen eines gemeinsamen Schlüssels K, wo eine oder beide Teilnehmer die Potenz unter Verwendung eines Paßworts S verschlüsseln. Mit Kenntnis von S können sie beide die Nachricht des anderen in einer zweiten Stufe unter Verwendung E_S^{-1} entschlüsseln und denselben Schlüssel K berechnen.

Kurze Beschreibung der Erfindung

[0018] Verfahren gemäß der Erfindung entsprechend den unabhängigen Ansprüchen. Bevorzugte Ausführungsformen entsprechend den abhängigen Ansprüchen.

[0019] In Paßwort-Protokoll tauschen die kommunizierenden Teilnehmer Berechnungsergebnisse aus, die jeweils eine Potenz enthalten, um einen Schlüssel zu erzeugen. Beim Erzeugen der Berechnungsergebnisse addiert jeder Teilnehmer das Paßwort zu

seiner jeweiligen Potenz hinzu. Wenn die vorher von einem Teilnehmer gesendeten Berechtigungsinformationen für den anderen Teilnehmer annehmbar sind, dann benutzt dieser andere Teilnehmer den gemäß dem Paßwort-Protokoll erstellten Schlüssel. Die Berechtigungsinformationen werden über einen sicheren Kommunikationskanal gesendet. Durch Zufügen des Paßworts zu den jeweiligen Potenzen sickert weniger Information über das Paßwort aus und die Berechnung wird wirkungsvoller.

[0020] Der sichere Kommunikationskanal wird auch bei anderen Ausführungsformen zur Bestätigung einer Mischsumme an mindestens einem, zwischen den Teilnehmern gesendeten Berechnungsergebnis. Ungleich dem Paßwort-Protokoll enthalten jedoch die Berechnungsergebnisse nicht das Paßwort. Wenn die Haschsumme bestätigt wird, dann wird ein Schlüssel unter Verwendung der zwischen den Teilnehmern gesendeten Berechnungsergebnisse erstellt. Dieser Bestätigungsvorgang bietet ein Maß an Sicherheit vor Erstellung des Schlüssels.

[0021] Die vorliegende Erfindung weist verschiedene Anwendungen einschließlich der drahtlosen Industrie auf, wobei die Teilnehmer ein Mobilfunkgerät des Benutzers und ein Netz sind.

Kurze Beschreibung der Zeichnungen

[0022] Die vorliegende Erfindung wird aus der unten angeführten ausführlichen Beschreibung und den nur zu Erläuterungszwecken dargestellten begleitenden Zeichnungen besser verständlich, wobei gleiche Bezugsziffern in den Zeichnungen entsprechende Teile in den verschiedenen Zeichnungen bezeichnen. In den Zeichnungen zeigt:

[0023] Fig. 1 die Kommunikation zwischen einem Netz und einem Mobilfunkgerät entsprechend der Diffie-Hellman-Schlüsselvereinbarung;

[0024] Fig. 2 die Kommunikation zwischen einem Netz und einem Mobilfunkgerät entsprechend dem verschlüsselten Schlüsselaustauschprotokoll von Diffie-Hellman;

[0025] Fig. 3 die Kommunikation zwischen einem Netz und einem Mobilfunkgerätebenutzer über eine Fernsprech-/Festleitung und ein Mobilfunkgerät gemäß einer Ausführungsform der vorliegenden Erfindung;

[0026] Fig. 4 die Kommunikation zwischen einem Netz und einem Mobilfunkgerätebenutzer über eine Fernsprech-/Festleitung und ein Mobilfunkgerät gemäß einem zweiten Verfahren; und

[0027] Fig. 5 die Kommunikation zwischen einem Netz und einem Mobilfunkgerätebenutzer über eine Fernsprech-/Festleitung und ein Mobilfunkgerät gemäß einem dritten Verfahren.

Ausführliche Beschreibung der bevorzugten Ausführungsformen

[0028] Das System und Verfahren gemäß der vorliegenden Erfindung zur Erstellung eines Schlüssels unter Verwendung von drahtloser Kommunikation wird in seiner Anwendung auf ein drahtloses System beschrieben. Nämlich Erstellen eines Schlüssels zwischen einem Mobilfunkgerät **20** und einem Netz **10** unter Verwendung von sowohl einer Fernsprech-/Festleitung **30** und eines Paßwort-Protokolls wird beschrieben.

[0029] Fig. 3 zeigt die Kommunikation zwischen (1) dem Netzanbieter und dem Netz **10**, zusammen als das Netz **10** bezeichnet, und (2) einem Mobilfunkgerätebenutzer über eine Fernsprech-/Festleitung **30** und das Mobilfunkgerät **20** gemäß einer Ausführungsform der vorliegenden Erfindung. Nach der Darstellung steht ein Mobilfunkgerätebenutzer über die Fernsprech-/Festleitung **30** dem Netz **10** Berechtigungsinformationen (z.B. Kreditkarteninformationen für Gebührenzwecke) bereit. Wenn das Netz **10** die Berechtigungsinformationen annimmt, stellt das Netz **10** dem Mobilfunkgerätebenutzer ein vier-(4-)ziffriges Paßwort P über die Fernsprech-/Festleitung **30** bereit. Es könnte jedoch sein, daß das Paßwort P mehr oder weniger als vier Ziffern aufweist.

[0030] Der Mobilfunkgerätebenutzer gibt dann dieses kurze Paßwort P in das Teil eines Aktivierungsprogramms in das Mobilfunkgerät **20** ein. Unter Verwendung eines Zufallszahlgenerators erzeugt das Mobilfunkgerät **20** eine Zufallszahl R_M und berechnet $((g\hat{}R_M + P) \bmod p)$ unter Verwendung einer vorgespeicherten 512-Bit-Primzahl p und des Generators g der durch die Primzahl erzeugten Gruppe.

[0031] Das Mobilfunkgerät **20** sendet die Primzahl p und den Generator g zum Netz **10** zusammen mit $((g\hat{}R_M + P) \bmod p)$. Da $((g\hat{}R_M + P) \bmod p)$ gleich $(g\hat{}R_M \bmod P) + (P \bmod p)$ ist und das Netz **10** das Paßwort P kennt, berechnet das Netz **10** $(P \bmod p)$ und entnimmt $(g\hat{}R_M \bmod P)$ aus $((g\hat{}R_M + P) \bmod p)$. Nach Erzeugen einer Zufallszahl R_N berechnet das Netz **10** $(g\hat{}R_M \bmod p)\ \hat{}R_N$, was gleich $(g\hat{}R_MR_N \bmod p)$ ist. Vom Netz **10** wird $(g\hat{}R_MR_N \bmod p)$, dessen Mischsumme oder ein Teil davon als ein Sitzungsschlüssel SK ausgewählt. Beispielsweise würden die 64 niederwertigsten Bit von $(g\hat{}R_MR_N \bmod p)$ als Sitzungsschlüssel SK ausgewählt werden, wenn sie im IS41-Protokoll enthalten sind.

[0032] Dann wird vom Netz **10** $((g\hat{}R_N + P) \bmod p)$ berechnet und zum Mobilfunkgerät **20** gesendet. Nach Ableiten von $(g\hat{}R_N \bmod p)$ berechnet das Mobilfunkgerät **20** $(g\hat{}R_N \bmod p)\ \hat{}R_M$, was gleich

($g^{R_M R_N}$ mod p) ist. Vom Mobilfunkgerät **20** wird ($g^{R_M R_N}$ mod p), dessen Mischsumme oder ein Teil derselben auf dieselbe Weise wie beim Netz **10** als ein Sitzungsschlüssel SK ausgewählt. Beispielsweise würden die 64 niederwertigsten Bit von ($g^{R_M R_N}$ mod p) als Sitzungsschlüssel SK ausgewählt werden, wenn sie im IS41-Protokoll enthalten sind.

[0033] Sobald das Netz **10** und das Mobilfunkgerät **20** den Sitzungsschlüssel SK besitzen, wird der Sitzungsschlüssel SK als der A-Schlüssel benutzt und Kommunikation zwischen dem Mobilfunkgerät **20** und dem Netz **10** wird unter Verwendung des A-Schlüssels umkonfiguriert.

[0034] Der oben besprochene drahtlose Austausch gemäß der vorliegenden Erfindung benutzt ein Paßwort-Protokoll (d.h. die Übertragungen von ((g^{R_M} + P) mod p) und ((g^{R_N} + P) mod p) in der Fig. 3) das nicht so viel Information aussickern läßt, wie das DH-EKE-Protokoll. Weiterhin ist dieses Paßwort-Protokoll sicher, da durch Beseitigen der Wirkung des Paßworts nichts aufgedeckt wird. R_M und R_N sind gleichförmige Zufallszahlen. Erheben derselben zu g und dann Reduzieren um mod p ergibt ebenfalls gleichförmige Zufallszahlen aufgrund der durch die Potenzierung von mod p induzierten Permutation. So wird durch Hinzuaddieren eines P mod p zu dieser Zahl die Gleichförmigkeit und Zufallsmäßigkeit des Ergebnisses nicht geändert. Alle Zahlen sind gleichermaßen wahrscheinlich und Entfernen der Wirkungen anderer Paßworte erstellt ebenfalls gleichermaßen wahrscheinliche Zahlen sodaß keine Informationen aussickern. Der Fachmann wird auch erkennen, daß das oben besprochene Paßwort-Protokoll in seiner Anwendung nicht auf den drahtlosen Austausch von Informationen begrenzt ist. Beispielsweise könnte dieses Paßwort-Protokoll auf Instanzenauthentifizierung und Sitzungsschlüsselvereinbarung angewandt werden.

[0035] Fig. 4 zeigt die Kommunikation zwischen dem Netz **10** und einem Mobilfunkgerätebenutzer über die Fernsprech-/Festleitung **30** und das Mobilfunkgerät **20** gemäß einem zweiten Verfahren. Nach der Darstellung stellt ein Mobilfunkbenutzer Berechtigungsinformationen für das Netz **10** über die Fernsprech-/Festleitung **30** bereit. Wenn das Netz **10** die Berechtigungsinformationen annimmt, dann läuft der Initialisierungsvorgang weiter wenn das Mobilfunkgerät **20** eine Initialisierungsanforderung als Teil der Initialisierungsprozedur des Mobilfunkgeräts ausgibt.

[0036] Beispielsweise erzeugt das Mobilfunkgerät **20** eine Zufallszahl R_M, berechnet (g^{R_M} mod p) und sendet eine Initialisierungsanforderung zusammen mit (g^{R_M} mod p) zum Netz **10**.

[0037] Das Netz **10** erzeugt eine Zufallszahl R_N und sendet (g^{R_N} mod p) zum Mobilfunkgerät **20**.

[0038] Das Mobilfunkgerät **20** und das Netz **10** führen beide h((g^{R_N} mod p), (g^{R_M} mod p)) durch, was eine Sammel-Mischsumme mit (g^{R_N} mod p) und (g^{R_M} mod P) ist, unter Verwendung des wohlbekannten SHA-Algorithmus (Secure Hashing Algorithm – Sicherer Hash-Algorithmus). Es ist jedoch zu beachten, daß ein beliebiger Hash-Algorithmus benutzt werden kann. Das Mobilfunkgerät **20** zeigt die Ergebnisse der Mischsumme an und der Mobilfunkgerätebenutzer gibt die Ziffern der Mischsumme über die Fernsprech-/Festleitung **30** an das Netz **10** ab.

[0039] Wenn das Netz **10** eine Übereinstimmung zwischen den vom Mobilfunkgerätbenutzer bereitgestellten Ziffern und der durch das Netz **10** durchgeführten Mischsumme feststellt, wird Kommunikation bestätigt und der A-Schlüssel als ($g^{R_M R_N}$ mod p), dessen Mischsumme oder eines Teils derselben erstellt. Vom Mobilfunkgerät **20** wird der A-Schlüssel als solcher erstellt worden sein, aber das Netz **10** wird diesen A-Schlüssel nur dann dem Mobilfunkgerät **20** zuordnen, wenn die Mischsumme bestätigt ist.

[0040] Als alternatives oder drittes Verfahren liefert der Mobilfunkgerätebenutzer **20** zusammen mit den Berechtigungsinformationen genügend Informationen (z.B. die Kennummer des Mobilfunkgeräts usw.) an das Netz **10**, sodaß das Netz **10** mit dem Mobilfunkgerät **20** Kontakt aufnehmen und (g^{R_N} mod p) als Erstkommunikation senden kann.

[0041] Dieses dritte Verfahren ist für einen sogenannten Geburtstagsangriff (Birthday attack) empfindlich; das bedeutet daß zum Angreifen dieses Protokolls nur halb so viele Versuche von einem Lauscher unternommen werden müssen, als anfänglich angenommen werden würde. Gemäß einer Alternative des dritten Verfahrens wird jedoch der Angriff bedeutend verlangsamt wenn die Mischsumme auf h ((g^{R_M} mod p), (g^{R_N} mod p), ($g^{R_M R_N}$ mod p)) geändert wird, da der Angreifer zusammen mit den Mischsummen Potenzieren muß.

[0042] Als weitere Alternative für die dritte Ausführungsform enthält die zur Bestätigung der Kommunikation zwischen dem Mobilfunkgerät **20** und dem Netz **10** durchgeführte Mischsumme die Kennummer des Mobilfunkgeräts **20**.

[0043] Gemäß einer weiteren Abänderung des dritten Verfahrens (d.h. einem vierten Verfahren) sendet das Mobilfunkgerät **20** (g^{R_M} mod p) nur dann zum Netz **10** wie in **Fig.** 10 dargestellt, bis es (g^{R_N} mod p) vom Netz **10** empfangen hat. Bei der dritten Ausführungsform war der Lauschangreifer in der Lage, sowohl (g^{R_M} mod p) als auch (g^{R_N} mod p) zu sehen und daher den Geburtstagsangriff auszunutzen. Gemäß der vorliegenden vierten Ausführungsform muß der Angreifer sich auf ein (g^{R_N} mod p) festlegen, ehe das Mobilfunkgerät **20** mit einem (g^{R_M} mod p) ant-

wortet. Dadurch werden die Freiheitsgrade des Angreifers um einen verringert.

[0044] Fig. 5 zeigt die Kommunikation zwischen dem Netz **10** und einem Mobilfunkgerätebenutzer über die Fernsprech-/Festleitung **30** und das Mobilfunkgerät **20** gemäß einem fünften Verfahren. Nach der Darstellung liefert ein Mobilfunkbenutzer dem Netz **10** Berechtigungsinformationen über die Fernsprech-/Festleitung **30**. Wie oben besprochen kann das Mobilfunkgerät **20** zusammen mit den Berechtigungsinformationen dem Netz **10** genügend Informationen (z.B. die Mobilfunkgerätekennung usw.) liefern, damit das Netz **10** erst Kontakt mit dem Mobilfunkgerät **20** aufnehmen kann. Wenn das Netz **10** die Berechtigungsinformationen annimmt, dann läuft der Initialisierungsvorgang weiter.

[0045] Der Initialisierungsvorgang schreitet fort, wobei entweder das Mobilfunkgerät **20** oder das Netz **10** dem anderen Teilnehmer eine Initialisierungsanforderung sendet.

[0046] Wenn beispielsweise das Mobilfunkgerät **20** die Initialisierungsanforderung sendet, dann erzeugt das Netz **10** eine Zufallszahl R_N, berechnet ($g^{\wedge}R_N$ mod p) und die Mischsumme ($g^{\wedge}R_N$ mod p) und sendet h($g^{\wedge}R_N$ mod p) zum Mobilfunkgerät **20**. Das Mobilfunkgerät **20** erzeugt eine Zufallszahl R_M, berechnet ($g^{\wedge}R_M$ mod p) und sendet ($g^{\wedge}R_M$ mod p) zum Netz **10**. Das Netz **10** sendet wiederum ($g^{\wedge}R_N$ mod p) zum Mobilfunkgerät **20**.

[0047] Als nächstes berechnet das Mobilfunkgerät **20** die Mischsumme des empfangenen ($g^{\wedge}R_N$ mod p) und bestätigt, daß diese berechnete Version von h($g^{\wedge}R_N$ mod p) der anfänglich vom Netz **10** empfangenen Version gleich ist. Bei Bestätigung läuft das Initialisierungsverfahren weiter.

[0048] Sowohl das Mobilfunkgerät **20** als auch das Netz **10** führen h (($g^{\wedge}R_M$ mod p), h ($g^{\wedge}R_N$ mod p)) durch. Das Mobilfunkgerät **20** zeigt die Ergebnisse der Mischsumme an und der Mobilfunkgerätebenutzer gibt die Ziffern der Mischsumme über die Fernsprech-/Festleitung **30** an das Netz **10** ab.

[0049] Wenn das Netz **10** eine Übereinstimmung mit der durch das Netz **10** durchgeführten Mischsumme feststellt, dann wird Kommunikation bestätigt und der A-Schlüssel als ($g^{\wedge}R_MR_N$ mod p), dessen Mischsumme oder ein Teil desselben erstellt. Das Mobilfunkgerät **20** wird nämlich den A-Schlüssel als solchen erstellt haben, aber das Netz **10** wird diesen A-Schlüssel nur dann dem Mobilfunkgerät **20** zuordnen, wenn die Mischsumme bestätigt ist.

[0050] Wie oben besprochen wird die Initialisierungsanforderung vom Netz **10** anstatt vom Mobilfunkgerät **20** gesendet. Wenn das Netz **10** die Initialisierungsanforderung sendet, dann erzeugt das Mobilfunkgerät **20** eine Zufallszahl R_M, berechnet ($g^{\wedge}R_M$ mod p), berechnet die Mischsumme von ($g^{\wedge}R_M$ mod p) und sendet h($g^{\wedge}R_M$ mod p) zum Netz **10**. Das Netz **10** wiederum erzeugt eine Zufallszahl R_M, berechnet ($g^{\wedge}R_N$ mod p) und sendet ($g^{\wedge}R_N$ mod p) zum Mobilfunkgerät **20**.

[0051] Das Mobilfunkgerät **20** sendet ($g^{\wedge}R_M$ mod p) zum Netz **10** und das Netz **10** berechnet die Mischsumme ($g^{\wedge}R_M$ mod p). Dann bestätigt das Netz **10**, daß die berechnete Version von h($g^{\wedge}R_M$ mod p) gleich der anfänglich vom Mobilfunkgerät **20** empfangenen Version ist. Wenn sie gleich ist, läuft der Initialisierungsvorgang weiter.

[0052] Sowohl das Mobilfunkgerät **20** als auch das Netz **10** führen nämlich h(($g^{\wedge}R_N$ mod p), h($g^{\wedge}R_M$ mod p)) durch. Das Mobilfunkgerät **20** zeigt die Ergebnisse der Mischsumme an und der Mobilfunkgerätebenutzer gibt die Ziffern der Mischsumme über die Fernsprech-/Festleitung **30** an das Netz **10** ab.

[0053] Wenn das Netz **10** eine Übereinstimmung mit der durch das Netz **10** durchgeführten Mischsumme feststellt, dann wird Kommunikation bestätigt und der A-Schlüssel als ($g^{\wedge}R_MR_N$ mod p), dessen Mischsumme oder ein Teil desselben erstellt. Das Mobilfunkgerät **20** wird nämlich den A-Schlüssel als solchen erstellt haben, aber das Netz **10** wird diesen A-Schlüssel nur dann dem Mobilfunkgerät **20** zuordnen, wenn die Mischsumme bestätigt ist.

[0054] Als weitere Alternative enthält die zur Bestätigung von Kommunikation zwischen dem Mobilfunkgerät **20** und dem Netz **10** durchgeführte abschließende Mischsumme die Kennummer des Mobilfunkgeräts **20**.

[0055] Ein Lauschangreifer kann keinen Geburtstagsangriff anwenden, da, wenn er als Netz **10** handelt, er sich auf die von ihm (über die Mischsumme) benutzte Potenz festlegen muß, ehe er die Potenz des Mobilfunkgerätebenutzers sieht. Auf ähnliche Weise muß der Angreifer, wenn er als das Mobilfunkgerät **20** handelt, sich auf die Potenz festlegen, ehe der Wert der der Mischsumme zugeordneten Potenz des Netzes offenbart wird.

[0056] Bei einigen der vorherigen Verfahren wurde angenommen, daß die Primzahl p und der Generator g fest und im Mobilfunkgerät **20** vorgespeichert sind. Wenn dies jedoch nicht der Fall ist, dann kann der Angreifer g und p durch g' und p' ersetzen, wodurch der Angreifer den diskreten Logarithmus wirkungsvoll berechnen kann. Wenn g und p auch drahtlos gesendet werden, dann sollten sie auch als Teil der Mischsummenberechnung h(g,p, ($g^{\wedge}R_M$ mod p), ($g^{\wedge}R_N$ mod p) benutzt werden, um dem Austausch von g und p durch den Angreifer Halt zu bieten.

[0057] Weiterhin könnten, obwohl jedes Verfahren als eine Fernsprech-/Festleitung **30** benutzend beschrieben wurde, andere Formen sicherer Kommunikation die Fernsprech-/Festleitung **30** ersetzen. Beispielsweise könnte ein vorher aktiviertes Mobilfunkgerät die Fernsprech-/Festleitung ersetzen. Als Alternative, aber mit geringerer Sicherheit, könnten die Fernsprech-/Festleitungskommunikationen über einen Sprachkanal zwischen dem Mobilfunkgerät **20** und dem Netz **10** durchgeführt werden und die übrigen Kommunikationen könnten über einen Organisationskanal zwischen dem Mobilfunkgerät **20** und dem Netz **10** stattfinden.

[0058] Die so beschriebene Erfindung kann offensichtlich auf viele Weisen verändert werden. Diese Veränderungen sind nicht als eine Abweichung aus dem Rahmen der Erfindung zu betrachten und alle derartigen Abänderungen sollen dem Umfang der nachfolgenden Ansprüche enthalten sein.

Patentansprüche

1. Verfahren zur Erstellung eines Schlüssels bei einem ersten Teilnehmer unter Verwendung eines Passworts, mit folgenden Schritten:
(a) Erzeugen einer ersten Zufallszahl R_M beim ersten Teilnehmer;
(b) Erzeugen eines ersten Rechenergebnisses durch Berechnen von (((g^R_M) + P) mod p), wobei P ein Passwort, p eine Primzahl und g ein Generator einer durch die Primzahl p erzeugten Gruppe ist;
(c) Senden der Primzahl p, des Generators g und des ersten Rechenergebnisses zu einem zweiten Teilnehmer;
(d) Empfangen eines zweiten Rechenergebnisses gleich (((g^R_N) + P) mod p), von dem zweiten Teilnehmer, wobei R_N eine zweite Zufallszahl ist; und
(e) Erstellen eines Schlüssels auf Grundlage des zweiten Rechenergebnisses und der zweiten Zufallszahl.

2. Verfahren nach Anspruch 1, wobei Schritt (e) folgende Schritte umfaßt:
(e1) Berechnen von (P mod p);
(e2) Abziehen von (P mod p) von dem zweiten Rechenergebnis von (((g^R_N) + P) mod p), um ((g^R_N) mod p) zu erhalten, und
(e3) Erstellen des Schlüssels auf Grundlage von ((g^R_N) mod p) und der ersten Zufallszahl.

3. Verfahren nach Anspruch 1, wobei der erste Teilnehmer ein Mobilfunkgerät in einem drahtlosen System und der zweite Teilnehmer ein Netz ist.

4. Verfahren nach Anspruch 1, vor dem Schritt (b) weiterhin mit den folgenden Schritten:
(f) Senden von Berechtigungsinformationen über einen sicheren Kommunikationskanal zum zweiten Teilnehmer; und
(g) Empfangen des Passworts vom zweiten Teilnehmer über den sicheren Kommunikationskanal, wenn der zweite Teilnehmer die Berechtigungsinformationen annimmt.

5. Verfahren nach Anspruch 4, wobei der erste Teilnehmer ein Mobilfunkgerätbenutzer in einem drahtlosen System und der zweite Teilnehmer ein Netz ist; und der sichere Kommunikationskanal eine Festleitung ist.

6. Verfahren zum Erstellen eines Schlüssels bei einem ersten Teilnehmer unter Verwendung eines Passworts, mit folgenden Schritten:
(a) Empfangen bei einem ersten Teilnehmer einer Primzahl p, eines Generators g einer durch die Primzahl p erzeugten Gruppe und eines ersten Rechenergebnisses von einem zweiten Teilnehmer, wobei das erste Rechenergebnis ein Ergebnis des Berechnens von (((g^R_M) + P) mod p) ist, wobei P ein Passwort und R_M eine erste Zufallszahl ist;
(b) Erzeugen einer zweiten Zufallszahl R_N;
(c) Erzeugen eines zweiten Rechenergebnisses durch Berechnen von (((g^R_N) + P) mod p) ;
(d) Senden des zweiten Rechenergebnisses zum zweiten Teilnehmer; und
(e) Erstellen eines Schlüssels auf Grundlage des ersten Rechenergebnisses und der zweiten Zufallszahl.

7. Verfahren nach Anspruch 6, wobei der Schritt (e) folgende Schritte umfaßt:
(e1) Berechnen von (P mod p);
(e2) Abziehen von (P mod p) von dem ersten Rechenergebnis von (((g^R_M) + P) mod p), um ((g^R_M) mod p) zu erhalten, und
(e3) Erstellen des Schlüssels auf Grundlage von ((g^R_M) mod p) und der zweiten Zufallszahl.

8. Verfahren nach Anspruch 6, wobei der erste Teilnehmer ein Netz in einem drahtlosen System und der zweite Teilnehmer ein Mobilfunkgerät ist.

9. Verfahren nach Anspruch 6, vor dem Schritt (a), weiterhin mit folgenden Schritten:
(f) Empfangen von Berechtigungsinformationen über einen sicheren Kommunikationskanal von dem zweiten Teilnehmer; und
(g) Senden des Passworts zum zweiten Teilnehmer über den sicheren Kommunikationskanal, wenn die Berechtigungsinformationen annehmbar sind.

10. Verfahren nach Anspruch 9, wobei der erste Teilnehmer ein Netz in einem drahtlosen System und der zweite Teilnehmer ein Mobilfunkbenutzer ist; und der sichere Kommunikationskanal eine Festleitung ist.

Es folgen 3 Blatt Zeichnungen

Anhängende Zeichnungen

FIG. 1
(STAND DER TECHNIK)

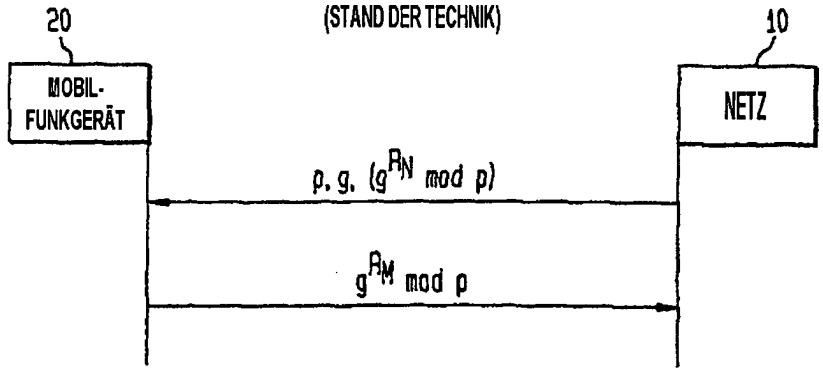


FIG. 2
(STAND DER TECHNIK)

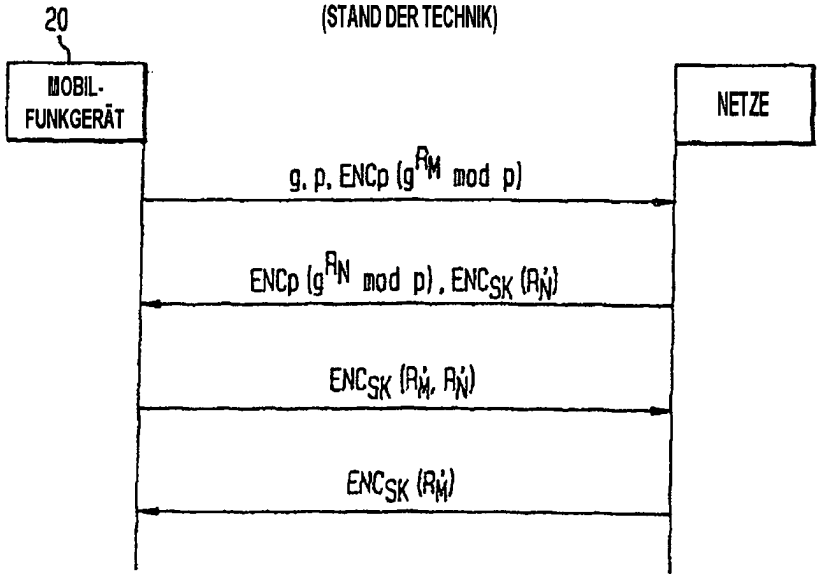


FIG. 3

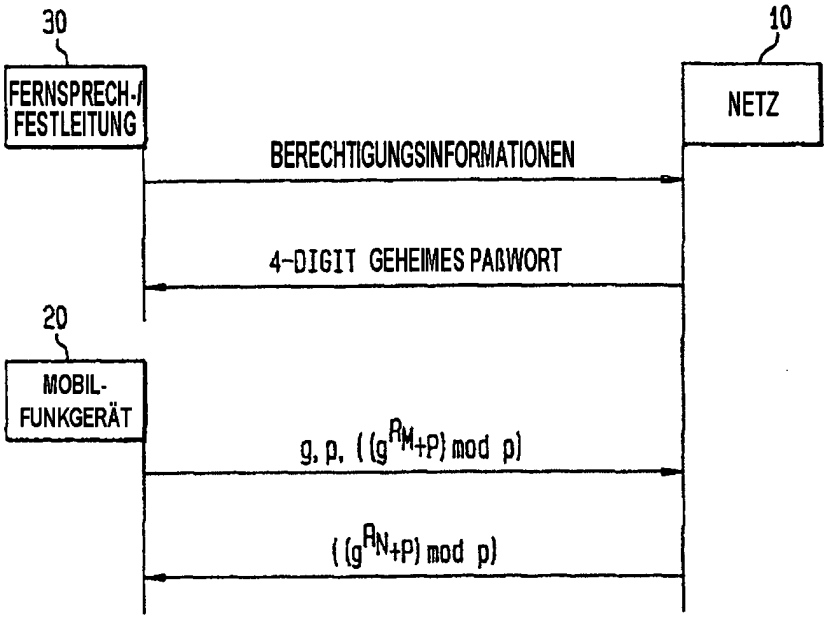

30
FERNSPRECH-/
FESTLEITUNG
10
NETZ
BERECHTIGUNGSINFORMATIONEN
4-DIGIT GEHEIMES PAßWORT
20
MOBIL-
FUNKGERÄT
g, p, ((g^AM+P) mod p)
((g^AN+P) mod p)

FIG. 4

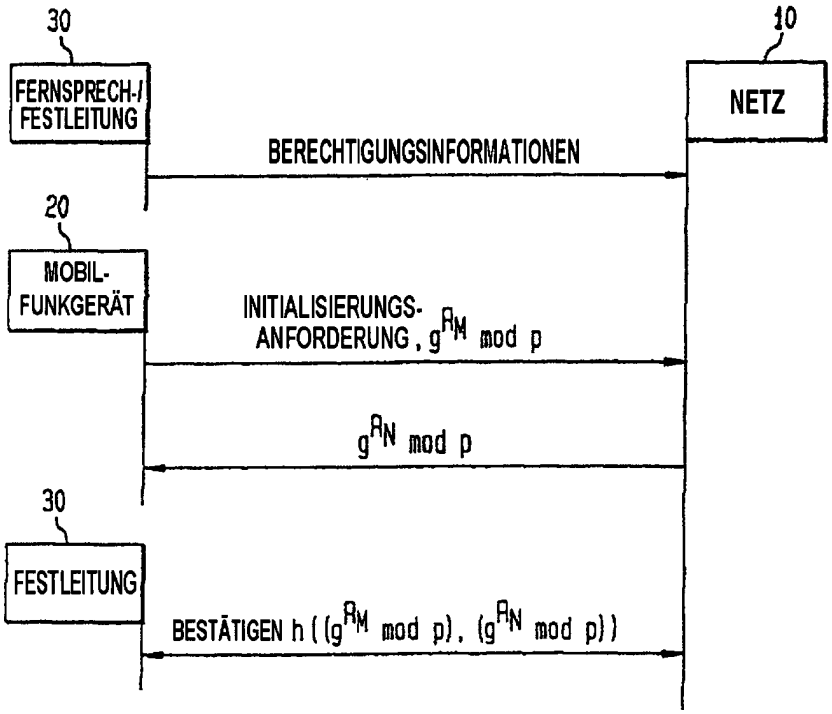
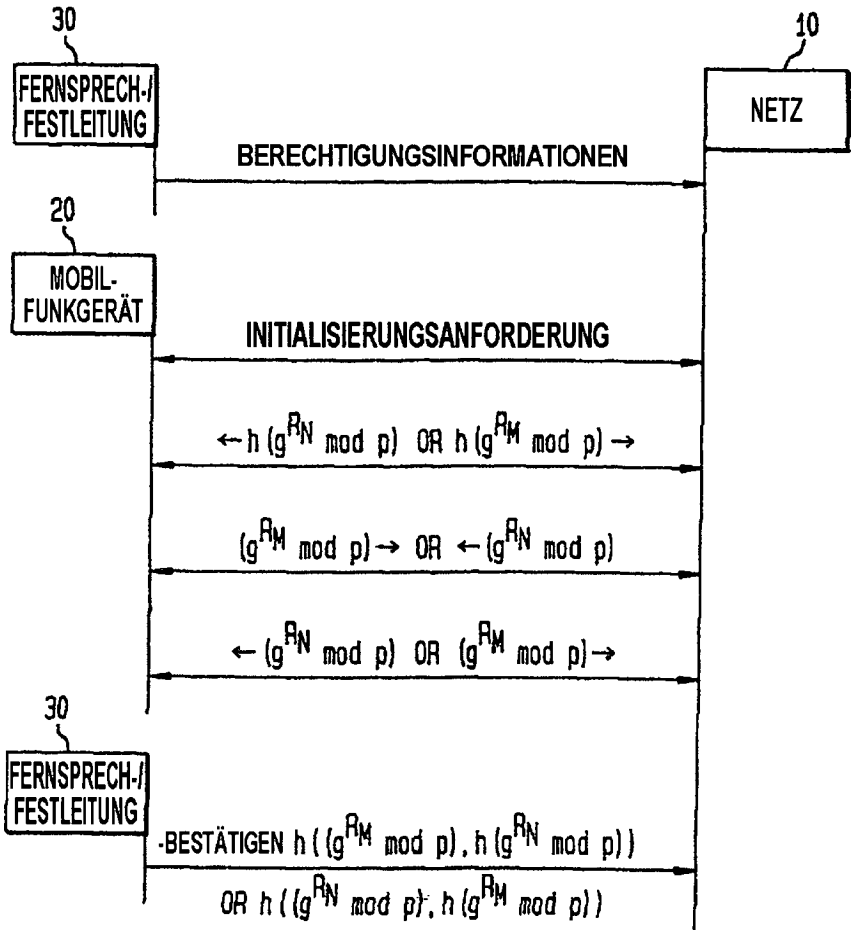

30
FERNSPRECH-/
FESTLEITUNG
10
NETZ
BERECHTIGUNGSINFORMATIONEN
20
MOBIL-
FUNKGERÄT
INITIALISIERUNGS-
ANFORDERUNG, g^AM mod p
g^AN mod p
30
FESTLEITUNG
BESTÄTIGEN h((g^AM mod p), (g^AN mod p))

FIG. 5


30
FERNSPRECH-/ FESTLEITUNG
10
NETZ
BERECHTIGUNGSINFORMATIONEN
20
MOBIL-FUNKGERÄT
INITIALISIERUNGSANFORDERUNG
← h (g^RN mod p) OR h (g^RM mod p) →
(g^RM mod p) → OR ← (g^RN mod p)
← (g^RN mod p) OR (g^RM mod p) →
30
FERNSPRECH-/ FESTLEITUNG
-BESTÄTIGEN h ((g^RM mod p), h (g^RN mod p))
OR h ((g^RN mod p), h (g^RM mod p))