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

(10) **DE 600 34 054 T2** 2007.12.06

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 224 827 B1**
(21) Deutsches Aktenzeichen: **600 34 054.6**
(86) PCT-Aktenzeichen: **PCT/FI00/00907**
(96) Europäisches Aktenzeichen: **00 969 608.9**
(87) PCT-Veröffentlichungs-Nr.: **WO 2001/030104**
(86) PCT-Anmeldetag: **18.10.2000**
(87) Veröffentlichungstag der PCT-Anmeldung: **26.04.2001**
(97) Erstveröffentlichung durch das EPA: **24.07.2002**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **21.03.2007**
(47) Veröffentlichungstag im Patentblatt: **06.12.2007**

(51) Int Cl.[8]: ***H04Q 7/38*** (2006.01)
H04L 9/32 (2006.01)

(30) Unionspriorität:

992258	**19.10.1999**	**FI**
992595	**02.12.1999**	**FI**

(84) Benannte Vertragsstaaten:
AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LI, LU, MC, NL, PT, SE

(73) Patentinhaber:
Setec Oy, Vantaa, FI

(72) Erfinder:
PAATERO, Lauri, FIN-00970 Helsinki, FI;
RANTALA, Janne, FIN-02260 Espoo, FI

(74) Vertreter:
Vossius & Partner, 81675 München

(54) Bezeichnung: **AUTHENTIFIZIERUNG EINER TEILNEHMERSTATION**

Beschreibung

[0001] Die Erfindung betrifft die Authentifizierung einer Teilnehmerstation, wobei die Identität der Teilnehmerstation auf der Basis eines teilnehmerstationsspezifischen, in der Teilnehmerstation gespeicherten geheimen Schlüssels verifiziert wird. Die Erfindung betrifft insbesondere eine Lösung zur Identifizierung einer Authentifikationsnachricht, die von einem externen Angreifer in einem Telekommunikationssystem generiert wird, und zur Gewährleistung, daß keine solche Information zur Verarbeitung dieser Authentifikationsnachricht den externen Angreifer erreicht, die den Angreifer in die Lage versetzen würde, den geheimen Schlüssel zu knacken.

[0002] Die Erfindung betrifft in erster Linie die Authentifizierung einer Teilnehmerstation in einem GSM-System (Globalen System für Mobilkommunikation). Zu beachten ist jedoch, daß die Erfindung auch in anderen Zusammenhängen angewandt werden kann, obwohl die Erfindung im folgenden hauptsächlich in Bezug auf das GSM-System beschrieben wird.

[0003] Im GSM-System basiert die Authentifizierung einer Teilnehmerstation auf einer Frage-Antwort-Prozedur. Für die Authentifizierung sind ein teilnehmerstationsspezifischer geheimer Schlüssel Ki und ein Authentifizierungsalgorithmus A3 auf der SIM-Karte (Teilnehmeridentitätsmodulkarte) der Teilnehmerstation gespeichert worden. Der teilnehmerstationsspezifische geheime Schlüssel Ki der Teilnehmerstation und der entsprechende Authentifizierungsalgorithmus A3 sind auch in einer Authentifizierungszentrale eines GSM-Netzes gespeichert worden. Um die Authentifizierung durchzuführen, erzeugt ein in der Authentifizierungszentrale angeordneter zunächst eine Zufallszahl und sendet sie als Eingangssignal zu einem Zähler. Als nächstes berechnet der Zähler eine Antwort SRES auf der Basis der Zufallszahl, des Authentifizierungsalgorithmus A3 und des geheimen Schlüssels Ki. Die Authentifizierungszentrale sendet dann die Zufallszahl und die Antwort SRES an ein Netzelement, das die eigentliche Authentifizierung durchführt und, im Hinblick auf das GSM-System, ein VLR (Besucherregister) ist.

[0004] Das Besucherregister leitet die empfangene Zufallszahl zu der zu authentifizierenden Teilnehmerstation weiter. Die Teilnehmerstation weist einen Zähler, der auf der Basis der empfangenen Zufallszahl eine Antwort SRES berechnet, einen geheimen Schlüssel Ki der Teilnehmerstation und einen Authentifizierungsalgorithmus A3 auf, und die Teilnehmerstation sendet die Antwort SRES an das VLR. Das VLR vergleicht dann die durch die Authentifizierungszentrale gesendete Antwort mit der durch die Teilnehmerstation gesendeten Antwort. Da der im Speicher der Teilnehmerstation gespeicherte geheime Schlüssel Ki teilnehmerstationsspezifisch ist, gibt es nur eine Teilnehmerstation, die eine richtige Antwort auf das an sie gesendete Eingangssignal generieren kann. Wenn die Antworten der Teilnehmerstation und der Authentifizierungszentrale identisch sind, ist die Teilnehmerstation folglich authentifiziert worden.

[0005] Ein Nachteil der oben beschriebenen bekannten Authentifizierungsprozedur ist, daß ein externer Angreifer, der den in der Teilnehmerstation gespeicherten geheimen Schlüssel knacken möchte, versuchen kann, den geheimen Schlüssel zu knacken, indem er der Teilnehmerstation (oder ihrer SIM-Karte) immer wieder verschiedene Eingangsignale übermittelt und die Antworten überwacht, die von der Teilnehmerstation gesendet werden. Wenn diese Prozedur häufig genug wiederholt wird und statistische Daten über die Eingangsignale und Antworten gesammelt werden, kann der geheime Schlüssel Ki auf der Basis der gesammelten Daten aufgedeckt werden. Wenn der externe Angreifer den Schlüssel knackt, ist er oder sie in der Lage, die Teilnehmerstation (oder die SIM-Karte) durch Erzeugen einer zweiten Teilnehmerstation mit einem identischen geheimen Schlüssel zu klonen, in welchem Fall die geklonte Teilnehmerstation für Anrufe benutzt werden kann, die dem Besitzer der ursprünglichen Teilnehmerstation in Rechnung gestellt werden.

[0006] Bisher ist aus WO 98/49855 A ein Authentifizierungsverfahren bekannt, wobei eine Zweiwegauthentifizierungsprozedur durchgeführt wird. Die Zweiwegprozedur ermöglicht sowohl der Teilnehmerstation als auch dem Netz, sicherzustellen, daß die andere Partei zuverlässig ist. Ein mit dieser Lösung verbundener wesentlicher Nachteil ist jedoch, daß die Lösung im Vergleich zu Lösungen nach dem Stand der Technik, die zum Beispiel im GSM-System genutzt werden, eine zusätzliche Signalübermittlung zwischen der Mobilstation und dem Netz erfordert. Im GSM-System existierende SIM-Karten können zum Beispiel keine Signalübermittlung verarbeiten, bei der die Mobilstation eine Zufallszahl zum Netz sendet, wie durch WO 98/49855 gelehrt. Die Einführung einer derartigen Lösung in bestehende Mobilkommunikationssysteme würde daher erfordern, daß alle existierenden Mobilstationen/SIM-Karten ausgetauscht werden, um die neue Signalübermittlung verarbeiten zu können.

[0007] Bisher ist außerdem aus WO 00/52949 A eine Lösung zur Verbesserung der Sicherheit von zweiseitigen Authentifizierungsverfahren bekannt. Dieses Dokument, das nach dem Prioritätsdatum der vorliegenden Patentanmeldung veröffentlicht wurde, offenbart für einen Fachmann eine zweiseitige Authentifizierungsprozedur, wobei eine erste Partei an eine zweite Partei eine Zufallszahl und einen ersten Teil einer verschlüsselten Zufallszahl sendet. Die

zweite Partei nutzt die empfangene Zufallszahl und einen geheimen Schlüssel, um zu ermitteln, ob die Zufallszahl von einer berechtigten Partei gesendet worden ist. Ein Nachteil bei einer derartigen Lösung ist, daß die zweite Partei im Vergleich zu Lösungen nach dem Stand der Technik imstande sein muß, eine Authentifikationsnachricht mit einem zusätzlichen Parameter zu verarbeiten, wobei es ausreicht, Authentifikationsnachrichten mit nur einem Eingangssignal zu verarbeiten. Die Einführung einer solchen Lösung in bestehende Mobilkommunikationssysteme würde daher erfordern, daß alle existierenden Mobilstationen/SIM-Karten ausgetauscht werden, um die neue Signalübermittlung verarbeiten zu können.

[0008] Bisher ist außerdem aus GB 2 319 150 A ein Sicherheitsverfahren zur Absicherung eines Authentifizierungsverfahrens bekannt, das einen geheimen Schlüsselalgorithmus nutzt.

[0009] Eine Aufgabe der vorliegenden Erfindung besteht darin, das oben erwähnte Problem zu mildern, indem eine Lösung bereitgestellt wird, welche die Probleme bei Lösungen nach dem Stand der Technik löst, indem sie für neue SIM-Karten und/oder Teilnehmerstationen ermöglicht, zu ermitteln, ob ein Eingangssignal in einer Authentifikationsnachricht aus einer zuverlässigen Quelle kommt oder nicht, während gleichzeitig alte SIM-Karten und/oder Teilnehmerstationen auch imstande sind, ein derartiges Eingangssignal zu verarbeiten, und es deshalb für einen externen Angreifer schwieriger ist, einen geheimen Schlüssel einer SIM-Karte und/oder Teilnehmerstation zu knacken. Die Aufgabe wird durch ein in dem unabhängigen Anspruch 1 definiertes Verfahren gelöst.

[0010] Die Erfindung betrifft ferner ein Telekommunikationssystem gemäß der Definition in dem unabhängigen Anspruch 6, in dem ein erfindungsgemäßes Verfahren angewandt werden kann.

[0011] Die Erfindung betrifft ferner eine Authentifizierungszentrale in einem Telekommunikationssystem, wie in dem unabhängigen Anspruch 11 definiert.

[0012] Die Erfindung betrifft ferner eine Teilnehmerstation eines Telekommunikationssystems, wie in dem unabhängigen Anspruch 12 definiert.

[0013] Die Erfindung betrifft ferner eine SIM-Karte, wie in dem unabhängigen Anspruch 16 definiert.

[0014] Der Erfindung liegt die folgende Idee zugrunde: wenn während der Authentifizierung einer Teilnehmerstation ein Eingangssignal, dessen Richtigkeit durch die Teilnehmerstation überprüft werden kann, anstelle einer Zufallszahl eingegeben wird, dann ist eine Lösung erreicht, um das Knacken eines teilnehmerstationsspezifischen geheimen Schlüssels noch schwieriger zu machen. Die Teilnehmerstation kann dann ein unrichtiges Eingangssignal erkennen, d. h. ein Eingangssignal, das in aller Wahrscheinlichkeit von einem externen Angreifer herrührt, der versucht, den geheimen Schlüssel der Teilnehmerstation zu knacken. Erfindungsgemäß kann die Teilnehmerstation programmiert werden, so zu arbeiten, daß das Knacken des geheimen Schlüssels wesentlich schwieriger wird, wenn die Teilnehmerstation ein Eingangssignal erkannt hat, das von einem externen Angreifer herrührt.

[0015] Die wichtigsten Vorteile der erfindungsgemäßen Lösung sind daher, daß es noch schwieriger für den externen Angreifer ist, den geheimen Schlüssel zu knacken, der bei der Authentifizierung einer bestimmten Teilnehmerstation benutzt wird, und daß die Erfindung mit äußerst geringfügigen Änderungen auf existierende Systeme angewandt werden kann. In dem GSM-System kann die Erfindung z. B. direkt in der Authentifizierungszentrale des Systems implementiert werden, was bedeutet, daß neue Telefone von Anfang an mit SIM-Karten ausgestattet werden können, die das erfindungsgemäße Eingangssignal überprüfen können. Es ist nicht notwendig, die SIM-Karten in alten Telefonen auszuwechseln, da die alten SIM-Karten das Eingangssignal verarbeiten können, das durch eine erfindungsgemäß arbeitende Authentifizierungszentrale erzeugt wird. Die alten Telefone nehmen einfach an, daß das Eingangssignal eine Zufallszahl ist, die wie zuvor in Verbindung mit der Authentifizierung zu verarbeiten ist.

[0016] In einer ersten Ausführungsform der Erfindung erzeugt und übermittelt die Teilnehmerstation ein Eingangssignal nur dann, wenn die Teilnehmerstation das Eingangssignal überprüft und für richtig befunden hat. Infolgedessen ist es schwieriger, den geheimen Schlüssel zu knacken, da ein externer Angreifer nicht weiß, wie das Eingangssignal so zu wählen ist, daß die durch die Teilnehmerstation durchgeführte Überprüfung die Richtigkeit des Eingangssignals anzeigt. Die Authentifizierungszentrale des Telekommunikationssystems weist zum Beispiel Informationen über die durch die Teilnehmerstation zu benutzenden Überprüfungsverfahren auf, was bedeutet, daß die Authentifizierungszentrale ein zur Teilnehmerstation zu übermittelndes Eingangssignal erzeugen kann, das auf der Basis der Überprüfung, die durch die Teilnehmerstation durchgeführt wird, richtig ist.

[0017] In einer zweiten bevorzugten Ausführungsform der Erfindung berechnet und übermittelt die Teilnehmerstation eine zufällige Antwort, wenn sie feststellt, daß das empfangene Eingangssignal unrichtig ist. Die zufällige Antwort kann nach einem anderen Algorithmus als dem Authentifizierungsalgorithmus berechnet werden. Alternativ kann die zufällige Ant-

wort nach dem Authentifizierungsalgorithmus berechnet werden, aber anstelle des geheimen Schlüssels der Teilnehmerstation nutzt die Berechnung einen anderen Schlüssel, der ein "Pseudoschlüssel" ist, oder alternativ kann die zufällige Antwort eine Zufallszahl enthalten, die durch einen Zufallszahlengenerator erzeugt wird. Das Entscheidende ist, daß die zufällige Antwort einer realen Antwort ähnelt, so daß ein externer Angreifer beispielsweise nicht anhand der Länge der Antwort erkennt, daß die zufällige Antwort keine reale Antwort ist, die mit einem Authentifizierungsalgorithmus und einem geheimen Schlüssel ausgestattet ist.

[0018] In einer dritten bevorzugten Ausführungsform der Erfindung unterhält die Teilnehmerstation eine Zählerfunktion, um die Anzahl von Eingangssignalen zu berechnen, die auf der Basis eines Nachrichtenauthentifizierungscodes falsch sind. Wenn in einem solchen Fall ein vorgegebener Grenzwert überschritten wird, blockiert die Teilnehmerstation, so daß sie keine richtige Antwort mehr auf das Eingangssignal liefert. In dieser Ausführungsform kann daher die Teilnehmerstation eine Antwort erzeugen und übermitteln, die entweder richtig oder falsch ist, ungeachtet dessen, ob das Eingangssignal richtig ist, bis die Zählerfunktion anzeigt, daß die maximale Anzahl falscher Eingangssignale überschritten ist, wodurch die Authentifizierungsfunktion der Teilnehmerstation blockiert. Die Blockierung kann entweder so erfolgen, daß die Teilnehmerstation überhaupt keine Antworten mehr liefert, oder alternativ kann die Teilnehmerstation zur Irreführung weiter ausschließlich falsche Antworten erzeugen, wie zum Beispiel zufällige Antworten. Dadurch wird verhindert, daß der externe Angreifer die Möglichkeit hat, den geheimen Schlüssel der Teilnehmerstation beispielsweise durch Anwendung von Statistik zu knacken.

[0019] Die Zählerfunktion der Teilnehmerstation kann z. B. so implementiert werden, daß die Zählerfunktion beim Einrichten auf einen bestimmten Anfangswert eingestellt worden ist, und daß außerdem sichergestellt worden ist, daß die Zählerfunktion nicht später manipuliert werden kann (beispielsweise um die Zählerfunktion auf den Anfangswert zurückzusetzen). Wenn die Zählerfunktion der Teilnehmerstation einen vorgegebenen Grenzwert erreicht, der in Abhängigkeit von der Anwendung im Bereich von 100 bis 10000 liegen kann, dann werden als nächstes ihre Authentifizierungsfunktionen permanent blockiert, so daß die Teilnehmerstation keine richtigen Antworten mehr liefert. Wenn es sich um eine Teilnehmerstation handelt, in der die Authentifizierungsfunktionen auf der SIM-Karte angeordnet sind, wie z. B. in einer GSM-Mobilstation, muß die Teilnehmerstation als nächstes mit einer neuen SIM-Karte ausgestattet werden, um die blockierte Karte auszutauschen.

[0020] Bevorzugte Ausführungsformen des Verfahrens, Systems, der Teilnehmerstation und der SIM-Karte gemäß der Erfindung werden in den beigefügten abhängigen Ansprüchen 2 bis 5, 7 bis 10, 13 bis 15, 17 und 18 offenbart.

[0021] Nachstehend wird die Erfindung unter Bezugnahme auf die beigefügten Zeichnungen näher erläutert. Dabei zeigen:

[0022] Fig. 1 ein Ablaufdiagramm, das eine erste bevorzugte Ausführungsform eines erfindungsgemäßen Verfahrens darstellt;

[0023] Fig. 2 ein Blockschaltbild, das eine erste bevorzugte Ausführungsform eines erfindungsgemäßen Systems darstellt;

[0024] Fig. 3 ein Eingangssignal, das bei der Authentifizierung einer Teilnehmerstation genutzt wird;

[0025] Fig. 4 ein Ablaufdiagramm, das die erste bevorzugte Ausführungsform des erfindungsgemäßen Verfahrens darstellt;

[0026] Fig. 5 ein Blockschaltbild, das eine dritte bevorzugte Ausführungsform des erfindungsgemäßen Systems darstellt; und

[0027] Fig. 6 ein Ablaufdiagramm, das eine zweite bevorzugte Ausführungsform des erfindungsgemäßen Verfahrens darstellt.

[0028] Fig. 1 zeigt ein Ablaufdiagramm, das eine erste bevorzugte Ausführungsform eines erfindungsgemäßen Verfahrens darstellt. Das Ablaufdiagramm von Fig. 1 kann z. B. bei der Verarbeitung einer Authentifikationsnachricht benutzt werden, die durch eine GSM-Teilnehmerstation/SIM-Karte empfangen wird.

[0029] Im Block A in Fig. 1 wird eine Authentifikationsnachricht empfangen, die ein Eingangssignal RAND enthält.

[0030] Im Block B wird entsprechend dem Eingangssignal RAND und einem vorgegebenen Prüfalgorithmus ein Nachrichtenauthentifizierungscode berechnet. Der verwendete Prüfalgorithmus sollte so gewählt werden, daß auf der Basis des Berechnungsergebnisses entschieden werden kann, ob das Eingangssignal richtig ist oder nicht. Eine solche Prüfung kann z. B. ausgeführt werden, indem vorher festgelegt wird, daß das Eingangssignal RAND immer aus zwei Teilen (wie durch Fig. 3 dargestellt) besteht und folglich eine Zufallszahl RND und einen Nachrichtenauthentifizierungscode MAC aufweist, der durch den vorgegebenen Prüfalgorithmus berechnet wird. Daher kann im Block B der Teil RND, der zur Berechnung des Nachrichtenauthentifizie-

rungscodes benutzt wird, aus dem Eingangssignal RAND abgerufen werden.

[0031] Nach der Berechnung des Nachrichtenauthentifizierungscodes wird im Block C geprüft, ob der übrige Teil MAC des Eingangssignals dem berechneten Nachrichtenauthentifizierungscode entspricht. Wenn das Eingangssignal auf der Basis des berechneten Nachrichtenauthentifizierungscodes falsch ist, kann die Schlußfolgerung gezogen werden, daß das Eingangssignal von einem externen Angreifer herrührt.

[0032] Das Ablaufdiagramm von Fig. 1 ermöglicht folglich die Erkennung eines Eingangssignals, das von einem externen Angreifer herrührt, was bedeutet, daß der Authentifizierungsvorgang von jetzt an so ablaufen kann, daß der externe Angreifer keine ausreichende Informationsmenge erhält, die es ihm oder ihr ermöglicht, den geheimen Schlüssel zu knacken.

[0033] Fig. 2 zeigt ein Blockschaltbild, das eine erste bevorzugte Ausführungsform eines erfindungsgemäßen Systems darstellt. Das System gemäß Fig. 2 kann z. B. ein GSM-System sein.

[0034] Im Fall von Fig. 2 ist der größte Teil der Authentifizierungsausrüstung des Systems in einer speziellen Authentifizierungszentrale AC angeordnet, die im Zusammenhang mit dem GSM-System, beispielsweise in Verbindung mit einem HLR (Heimstandortregister), aufgestellt werden kann. In dem GSM-System wird die Teilnehmerstation durch ein VLR (Besucherregister) authentifiziert, so daß das VLR von der Authentifizierungszentrale AC ein Eingangssignal RAND und eine Antwort SRES empfängt, die das VLR in die Lage versetzt, die Teilnehmerstation MS zu authentifizieren.

[0035] Die Authentifizierungszentrale AC von Fig. 2 weist einen Zufallszahlengenerator **1** zum Erzeugen einer Zufallszahl RND für einen Zähler **2** auf. Der Zähler **2** berechnet einen MAC (Nachrichtenauthentifizierungscode) auf der Basis der Zufallszahl RND und eines ersten vorgegebenen Algorithmus g. Als nächstes bildet der Zähler **2** ein Eingangssignal RAND aus der Zufallszahl RND und dem Nachrichtenauthentifizierungscode MAC. In dem beispielhaften Fall von Fig. 2 besteht folglich das Eingangssignal RAND aus zwei Teilen. Das Eingangssignal ist in Fig. 3 dargestellt.

[0036] Die Authentifizierungszentrale AC weist einen Speicher **4** auf, in dem die geheimen Schlüssel aller Teilnehmerstationen gespeichert sind, an deren Authentifizierung die Authentifizierungszentrale beteiligt ist. In der Praxis kann die Authentifizierungszentrale operatorspezifisch sein, in welchem Falle alle geheimen Schlüssel der Teilnehmerstationen des Operators in dem Speicher der Authentifizierungszentrale abgelegt sind. Im Fall von Fig. 2 ist der geheime Schlüssel Ki der Teilnehmerstation MS, die aus einer Mobilstation besteht, in dem Speicher abgelegt worden. Die Authentifizierungszentrale übermittelt den aus dem Speicher **4** abgerufenen geheimen Schlüssel Ki und das durch den Zähler **2** erzeugte Eingangssignal RAND zu einem Zähler **3**.

[0037] Der Zähler **3** berechnet eine Antwort SRES auf der Basis des geheimen Schlüssels Ki, des Eingangssignals RAND und des Authentifizierungsalgorithmus A3. Die Authentifizierungszentrale sendet das Eingangssignal RAND und die Antwort SRES zum VLR (Besucherregister).

[0038] Um die Teilnehmerstation MS zu authentifizieren, sendet das VLR das von der Authentifizierungszentrale empfangene Eingangssignal RAND zur Teilnehmerstation MS. Das VLR speichert die von der Authentifizierungszentrale empfangene Antwort im Speicher, so daß sie für ein Vergleichselement **10** verfügbar ist.

[0039] Das durch die Teilnehmerstation MS empfangene Eingangssignal RAND wird zu einem Zähler **5** übermittelt, der sich auf der SIM-Karte der Teilnehmerstation MS befindet. Der Zähler **5** berechnet dann einen Nachrichtenauthentifizierungscode unter Verwendung des vorgegebenen Teils des Eingangssignals und eines Prüfalgorithmus f. In der Ausführungsform gemäß Fig. 2 wird angenommen, daß die Struktur des durch die Authentifizierungszentrale AC erzeugten Eingangssignals RAND ähnlich derjenigen in Fig. 2 ist, d. h. das Eingangssignal besteht aus der Zufallszahl RND, die durch den Zufallszahlengenerator **1** erzeugt wird, und dem Nachrichtenauthentifizierungscode MAC, der durch den Algorithmus g (RND) berechnet wird. Der Prüfalgorithmus f der Teilnehmerstation ruft dann den ersten Teil RND des Eingangssignals RAND ab und berechnet als nächstes einen Nachrichtenauthentifizierungscode auf ähnliche Weise wie diejenige, die durch den Zähler **2** der Authentifizierungszentrale angewandt wird, d. h. durch den Algorithmus g (RND). Der Zähler **5** übermittelt den berechneten Nachrichtenauthentifizierungscode MAC zu einer Vergleichseinheit **6**. Als nächstes vergleicht die Vergleichseinheit den durch den Zähler **5** berechneten Nachrichtenauthentifizierungscode MAC mit dem Nachrichtenauthentifizierungscode MAC im Eingangssignal RAND. Wenn die Vergleichseinheit **6** feststellt, daß der durch den Zähler berechnete Nachrichtenauthentifizierungscode dem im Eingangssignal verbleibenden Teil MAC entspricht, dann zeigt die Vergleichseinheit **6** einer Steuereinheit **7** an, daß das Eingangssignal RAND richtig ist.

[0040] Wenn die Steuereinheit **7** feststellt, daß das Eingangssignal richtig ist, aktiviert sie einen Zähler **8**, um eine Antwort auf das Eingangssignal RAND zu

berechnen. Der Zähler **8** berechnet die Antwort SRES auf der Basis des Eingangssignals RAND, des in einem Speicher **9** abgelegten teilnehmerstationsspezifischen geheimen Schlüssels Ki und des Authentifizierungsalgorithmus A3. Der Algorithmus ist folglich der gleiche Algorithmus A3, und die Parameter sind daher die gleichen Parameter wie die durch den Zähler **3** der Authentifizierungszentrale benutzten. Die Teilnehmerstation erzeugt auf diese Weise die zum VLR übertragene Antwort SRES, die der durch die Authentifizierungszentrale gesendeten Antwort SRES entspricht. Wenn nach dem Vergleich die Vergleichseinheit **10** des VLR (Besucherregisters) feststellt, daß die Antworten identisch sind, zieht sie die Schlußfolgerung, daß die Teilnehmerstation MS authentifiziert worden ist.

[0041] Wenn andererseits die Vergleichseinheit **6** der Steuereinheit **7** anzeigt, daß das Eingangssignal RAND falsch ist, dann ist das Eingangssignal höchstwahrscheinlich durch einen externen Angreifer übermittelt worden. In einem solchen Fall unterbricht die Steuereinheit den Prozeß zur Authentifizierung der Teilnehmerstation, so daß durch die Teilnehmerstation keine Antwort gesendet wird. Alternativ kann die Steuereinheit **7** dann die Übermittlung einer zufälligen Antwort aktivieren. Die zufällige Antwort bezeichnet hierin irgendeine Antwort, die einer richtigen ähnelt. Eine solche zufällige Antwort kann z. B. eine Zufallszahl oder eine durch einen Algorithmus berechnete Antwort aufweisen. Entscheidend ist, daß die Antwort nicht durch den Authentifizierungsalgorithmus A3, den geheimen Schlüsse Ki und das Eingangssignal RAND berechnet wird. Wenn dies der Fall wäre, dann erhielte der externe Angreifer die reale Antwort auf das übermittelte Eingangssignal, die ihn beim Knacken des geheimen Schlüssels helfen könnte. Wenn andererseits der externe Angreifer eine zufällige Antwort erhält, die der realen Antwort ähnlich ist (d. h. die Länge der Antwort ist der Länge der realen Antwort ähnlich usw.), dann wird der externe Angreifer nie wissen, daß die Antwort falsch ist.

[0042] Das System gemäß Fig. 2 ist insofern vorzuziehen, als die darin dargestellte erfindungsgemäße Authentifizierungszentrale auch in Verbindung mit existierenden, mit anderen Worten alten, Teilnehmerstationen eingesetzt werden kann. Dies ist auch durchführbar, wenn das Eingangssignal RAND so gewählt wird, daß seine Länge dem zu den alten Teilnehmerstationen übermittelten Eingangssignal entspricht. Natürlich sind die alten Teilnehmerstationen nicht imstande, zu prüfen, ob die Antwort SRES richtig ist oder nicht, jedoch können sie die Antwort SRES aus dem Eingangssignal berechnen, das den Nachrichtenauthentifizierungscode enthält.

[0043] Die in dem Blockschaltbild von Fig. 2 dargestellten Blöcke können elektronische Schaltungen aufweisen, oder alternativ können ein oder mehrere Blöcke durch Software implementiert werden. Daher sind zum Beispiel keine zwei getrennten Zähler in der Teilnehmerstation oder der Authentifizierungszentrale notwendig, sondern die Zähler können beispielsweise durch einen Prozessor und ein Computerprogramm auf eine an sich bekannte Weise implementiert werden.

[0044] Obwohl im Zusammenhang mit Fig. 2 beschrieben worden ist, daß die SIM-Karte der Teilnehmerstation die notwendigen Teile zur Erzeugung einer Antwort in Verbindung mit der Authentifizierung aufweist, ist es natürlich möglich, daß diese Teile, statt auf der SIM-Karte, in der Teilnehmerstation angeordnet sind. Eine solche Lösung ist besonders in einem System von Bedeutung, das überhaupt keine SIM-Karten aufweist.

[0045] Fig. 3 veranschaulicht ein Eingangssignal, das bei der Authentifizierung einer Teilnehmerstation genutzt wird. In dem System von Fig. 2 kann zum Beispiel der Zähler **2** ein solches Eingangssignal unter Verwendung einer Zufallszahl RND und eines Algorithmus g erzeugen. Angewandt auf das GSM-System, beträgt die Gesamtlänge des Eingangssignals RAND 16 Bytes. Erfindungsgemäß kann die Länge der Zufallszahl RND dann zum Beispiel 8 bis 14 Bytes betragen. Die Länge des Nachrichtenauthentifizierungscodes MAC, der auf der Basis der Zufallszahl und des Algorithmus g berechnet wird, kann entsprechend 2 bis 8 Bytes betragen.

[0046] Wenn die erfindungsgemäße Teilnehmerstation das Eingangssignal gemäß Fig. 3 empfängt, berechnet sie unter Verwendung des Prüfalgorithmus und des vorgegebenen Teils des Eingangssignals, d. h. der Zufallszahl RND des Eingangssignals, einen Nachrichtenauthentifizierungscode. Wenn der durch die Teilnehmerstation berechnete Nachrichtenauthentifizierungscode dem übrigen Teil des Eingangssignals entspricht, d. h. dem Nachrichtenauthentifizierungscode MAC, dann zieht die Teilnehmerstation die Schlußfolgerung, daß das Eingangssignal richtig ist.

[0047] Fig. 4 zeigt ein Ablaufdiagramm, das eine zweite bevorzugte Ausführungsform des erfindungsgemäßen Verfahrens darstellt. Das Ablaufdiagramm von Fig. 4 kann z. B. bei der Verarbeitung einer Authentifikationsnachricht in der Teilnehmerstation gemäß Fig. 2 benutzt werden.

[0048] Die Blöcke A bis C in Fig. 4 sind ähnlich den Blöcken A bis C in Fig. 1, d. h. in diesen Blöcken wird auf der Basis des berechneten Nachrichtenauthentifizierungscodes geprüft, ob das empfangene Eingangssignal richtig ist oder nicht.

[0049] Wenn im Block C auf der Basis des berechneten Nachrichtenauthentifizierungscodes festge-

stellt wird, daß das Eingangssignal richtig ist, dann wird im Block D' eine Antwort SRES berechnet und übermittelt. Die Antwort wird auf der Basis des vorgegebenen Authentifizierungsalgorithmus A3, des geheimen Schlüssels Ki und des Eingangssignals RAND berechnet.

[0050] Wenn andererseits im Block C auf der Basis des Nachrichtenauthentifizierungscodes festgestellt wird, daß das Eingangssignal RAND falsch ist, dann rührt das Eingangssignal RAND höchstwahrscheinlich von einem externen Angreifer her, der versucht, den bei der Authentifizierung benutzten geheimen Schlüssel zu knacken. Erfindungsgemäß gibt es zwei alternative Vorgehensweisen.

[0051] Die erste Alternative wird durch den Pfeil E' bezeichnet, wobei die Verarbeitung der Authentifikationsnachricht unterbrochen wird. Dann wird keine Antwort auf die Authentifikationsnachricht gesendet. Folglich empfängt der externe Angreifer keine Antwort auf das Eingangssignal, was bedeutet, daß der Angreifer nicht imstande ist, eine Statistik über die Eingangssignale und Antworten zu erfassen oder eine derartige Statistik zum Knacken des geheimen Schlüssels zu verwenden.

[0052] Die zweite Alternative ist im Block F' dargestellt, wobei eine zufällige Antwort auf das Eingangssignal RAND erzeugt und übermittelt wird. Die zufällige Antwort kann irgendeine Antwort sein, die einer realen Antwort ähnelt und nicht auf ähnliche Weise wie die reale Antwort berechnet worden ist (vergleiche Block D'). Folglich kann die zufällige Antwort direkt durch den Zufallszahlengenerator erzeugt werden, oder sie kann unter Anwendung eines geeigneten Algorithmus und des Eingangssignals aus dem Eingangssignal berechnet werden. Der externe Angreifer empfängt daher eine falsche Antwort, wobei der Angreifer dies jedoch nicht weiß.

[0053] Fig. 5 zeigt ein Blockschaltbild, das eine zweite bevorzugte Ausführungsform des erfindungsgemäßen Systems darstellt. In der Ausführungsform gemäß Fig. 5 sind die Authentifizierungszentrale AC und das Besucherregister VLR ähnlich der Authentifizierungszentrale und dem Besucherregister VLR, die in der Ausführungsform von Fig. 2 dargestellt werden. Daher wird ein ähnliches Eingangssignal wie das in Verbindung mit der Ausführungsform von Fig. 2 beschriebene zu einer Teilnehmerstation MS' gesendet.

[0054] Eine in der Teilnehmerstation MS' von Fig. 5 untergebrachte SIM-Karte SIM' ist gleichfalls der SIM-Karte sehr ähnlich, die in Verbindung mit Fig. 2 beschrieben wurde. Die Ausführungsform gemäß Fig. 5 unterscheidet sich von dem Fall gemäß Fig. 2 darin, daß die SIM'-Karte der Teilnehmerstation eine Zählerfunktion für die Anzahl falscher Eingangssignale unterhält.

[0055] Das durch die Teilnehmerstation MS' empfangene Eingangssignal RAND wird zu dem Zähler **5** in ihrer SIM-Karte übermittelt. Der Zähler **5** berechnet dann unter Verwendung des vorgegebenen Teils des Eingangssignals und eines Prüfalgorithmus f einen Nachrichtenauthentifizierungscode. In der Ausführungsform gemäß Fig. 5 wird angenommen, daß die Struktur des durch die Authentifizierungszentrale AC erzeugten Eingangssignals RAND ähnlich derjenigen von Fig. 3 ist, d. h. das Eingangssignal besteht aus der durch den Zufallszahlengenerator **1** erzeugten Zufallszahl RND und dem durch den Algorithmus g (RND) berechneten Nachrichtenauthentifizierungscode MAC. Der Prüfalgorithmus f der Teilnehmerstation ruft dann den ersten Teil RND des Eingangssignals RAND ab und berechnet dann auf eine Weise ähnlich derjenigen, wie sie durch den Zähler **2** der Authentifizierungszentrale angewandt wird, d. h. durch den Algorithmus g (RND), einen Nachrichtenauthentifizierungscode MAC. Der Zähler **5** übermittelt den berechneten Nachrichtenauthentifizierungscode MAC zu der Vergleichseinheit **6**. Als nächstes vergleicht die Vergleichseinheit **6** den durch den Zähler **5** berechneten Nachrichtenauthentifizierungscode MAC mit dem Nachrichtenauthentifizierungscode MAC im Eingangssignal RAND. Wenn die Vergleichseinheit **6** feststellt, daß der durch den Zähler berechnete Nachrichtenauthentifizierungscode dem übrigen Teil MAC des Eingangssignals entspricht, zeigt die Vergleichseinrichtung **6** einer Steuereinheit **7'** an, daß das Eingangssignal RAND richtig ist.

[0056] Wenn die Steuereinheit **7'** feststellt, daß das Eingangssignal richtig ist, aktiviert sie einen Zähler **8'**, um eine Antwort auf das Eingangssignal RAND zu berechnen. Der Zähler **8'** berechnet die Antwort SRES auf der Basis des Eingangssignal RAND, des in einem Speicher **9'** abgelegten teilnehmerstationsspezifischen geheimen Schlüssels Ki und des Authentifizierungsalgorithmus A3. Der Algorithmus ist daher der gleiche Algorithmus A3, und die Parameter sind folglich die gleichen Parameter, wie sie durch den Zähler **3** der Authentifizierungszentrale benutzt werden. Folglich erzeugt die Teilnehmerstation MS die zum Besucherregister (VLR) gesendete Antwort SRES, die der durch die Authentifizierungszentrale gesendeten Antwort SRES entspricht. Wenn nach dem Vergleich die Vergleichseinheit **10** im VLR feststellt, daß die Antworten identisch sind, zieht sie die Schlußfolgerung, daß die Teilnehmerstation MS authentifiziert worden ist.

[0057] Wenn andererseits die Vergleichseinheit **6** der Steuereinheit **7'** anzeigt, daß das Eingangssignal RAND falsch ist, dann wird die Antwort höchstwahrscheinlich durch einen externen Angreifer übermittelt. Die Steuereinheit **7'** aktualisiert dann die Zähler-

funktion der Teilnehmerstation zur Protokollierung der Anzahl empfangener falscher Eingangssignale. In dem beispielhaften Fall von Fig. 5 kann dies mit Hilfe einer im Speicher **9'** abgelegten Variablen C und eines Grenzwerts Cmax ausgeführt werden. Bei der ersten Inbetriebnahme der SIM-Karte SIM' wurde die Variable C auf einen Anfangswert 0 gesetzt, der im Speicher **9'** gespeichert wurde. Entsprechend wurde die Variable Cmax auf einen Wert 1000 gesetzt, der im Speicher **9'** gespeichert wurde. Wenn die Vergleichseinheit **6** anzeigt, daß das empfangene Eingangssignal falsch ist, dann erhöht die Steuereinheit **7'** den Wert der Variablen C um eins und vergleicht weiter den neuen Wert der Variablen C mit dem Maximalwert Cmax. Wenn der Maximalwert erreicht worden ist, blockiert die Steuereinheit den Betrieb der SIM-Karte, so daß die SIM-Karte keine richtigen Antworten mehr auf die empfangenen Eingangssignale RAND erzeugt. In der Praxis kann dies so ausgeführt werden, daß die SIM-Karte überhaupt keine Antworten mehr erzeugt, oder die SIM-Karte erzeugt weiterhin ausschließlich zufällige Antworten, oder die SIM-Karte erzeugt nur eine Ansage, die anzeigt, daß sie blockiert ist.

[0058] Wenn die Steuereinheit **7'** durch die Vergleichseinheit über eine falsche Antwort informiert worden ist, und wenn die Variable C den Maximalwert Cmax in Verbindung mit der Aktualisierung der Zählerfunktion nicht erreicht hat, kann die Steuereinheit fallabhängig auf viele alternative Weisen weiter arbeiten. Eine Alternative ist, daß die Steuereinheit den Authentifizierungsprozeß der Teilnehmerstation unterbricht, so daß die Teilnehmerstation keine Antworten mehr sendet. Alternativ kann die Steuereinheit **7'** in einem ähnlichen Fall die Übermittlung einer zufälligen Antwort aktivieren. Die zufällige Antwort bezieht sich hierbei auf irgendeine Antwort, die einer realen Antwort ähnelt. Eine solche zufällige Antwort kann z. B. eine Zufallszahl und eine durch einen Algorithmus berechnete Antwort aufweisen. Entscheidend ist, daß die Antwort nicht durch den Authentifizierungsalgorithmus A3, den geheimen Schlüssel Ki und das Eingangssignal RAND berechnet wird. Wenn dies der Fall wäre, dann erhielte der externe Angreifer die reale Antwort auf das übermittelte Eingangssignal, die ihm beim Knacken des geheimen Schlüssels helfen könnte. Wenn andererseits der externe Angreifer eine zufällige Antwort erhält, die der realen Antwort ähnelt (d. h. die Länge der Antwort ist gleich der Länge der realen Antwort usw.), dann weiß der externe Angreifer nie, daß die Antwort falsch ist.

[0059] Die in dem Blockschaltbild von Fig. 5 dargestellten Blöcke können aus elektronischen Schaltungen bestehen, oder alternativ können ein oder mehrere Blöcke durch Software implementiert werden. Daher sind z. B. keine zwei getrennten Zähler in der Teilnehmerstation oder der Authentifizierungszentrale notwendig, sondern die Zähler können durch einen Prozessor und ein Computerprogramm auf eine an sich bekannte Weise implementiert werden.

[0060] Obwohl in Verbindung mit Fig. 5 beschrieben worden ist, daß die SIM-Karte der Teilnehmerstation die notwendigen Teile zur Erzeugung einer Antwort in Verbindung mit der Authentifizierung aufweist, ist es natürlich möglich, daß diese Teile, statt auf der SIM-Karte, in der Teilnehmerstation angeordnet sind. Eine solche Lösung ist besonders in einem System von Bedeutung, daß überhaupt keine SIM-Karten aufweist.

[0061] Fig. 6 zeigt ein Ablaufdiagramm, das eine dritte bevorzugte Ausführungsform des erfindungsgemäßen Verfahrens darstellt. Das Ablaufdiagramm gemäß Fig. 6 kann z. B. in der Teilnehmerstation gemäß Fig. 5 zur Verarbeitung einer Authentifikationsnachricht genutzt werden. In der Teilnehmerstation (oder ihrer SIM-Karte) ist dann bei ihrer Einrichtung eine vorgegebene Variable Cmax gespeichert worden, welche die höchste zulässige Anzahl falscher Eingangssignale anzeigt. Außerdem wird eine Variable C zur Protokollierung empfangener falscher Antworten auf einen vorgegebenen Anfangswert gesetzt.

[0062] Im Block A" von Fig. 6 wird eine Authentifikationsnachricht empfangen, die das Eingangssignal RAND aufweist.

[0063] Im Block B" wird geprüft, ob die durch die Zählerfunktion genutzte Variable C den Grenzwert Cmax erreicht hat oder nicht. Wenn ja, bedeutet dies, daß die höchste zulässige Anzahl empfangener falscher Eingangssignale Cmax bereits erreicht worden ist, was bedeutet, daß der Authentifizierungsprozeß unterbrochen wird. Andernfalls geht der Prozeß zum Block C" über.

[0064] Im Block C" wird entsprechend dem Eingangssignal RAND und einem vorgegebenen Prüfalgorithmus ein Nachrichtenauthentifizierungscode berechnet. Der verwendete Prüfalgorithmus ist so zu wählen, daß auf der Basis des Berechnungsergebnisses die Schlußfolgerung gezogen werden kann, ob das Eingangssignal richtig ist oder nicht. Eine derartige Prüfung kann z. B. ausgeführt werden, indem vorgegeben wird, daß ein Eingangssignal RAND stets aus zwei Teilen besteht (wie in Fig. 3 dargestellt) und daher eine Zufallszahl RND und einen durch den vorgegebenen Prüfalgorithmus berechneten Nachrichtenauthentifizierungscode MAC aufweist. Im Block C" kann der zum Berechnen des Nachrichtenauthentifizierungscodes benutzte Teil RND dann aus dem Eingangssignal RAND abgerufen werden. Nach Berechnung des Nachrichtenauthentifizierungscodes wird im Block D" geprüft, ob der übrige Teil MAC des Eingangssignals dem berechneten Nachrichtenauthentifizierungscode entspricht

oder nicht.

[0065] Wenn im Block D" auf der Basis des berechneten Nachrichtenauthentifizierungscodes entschieden wird, daß das Eingangssignal richtig ist, dann wird im Block E" eine Antwort SRES berechnet und übermittelt. Die Antwort wird auf der Basis des vorgegebenen Authentifizierungsalgorithmus A3, des geheimen Schlüssels Ki und des Eingangssignals RAND berechnet.

[0066] Wenn andererseits im Block D" auf der Basis des Nachrichtenauthentifizierungscodes festgestellt wird, daß das Eingangssignal RAND falsch ist, dann rührt das Eingangssignal RAND höchstwahrscheinlich von einem externen Angreifer her, der versucht, den bei der Authentifizierung verwendeten geheimen Schlüssel zu knacken. Der Prozeß geht dann zum Block F" über.

[0067] Im Block F" wird der Wert der in der Zählerfunktion verwendeten Variablen C aktualisiert, zum Beispiel durch Erhöhen oder Vermindern ihres Werts um eins (in Abhängigkeit davon, wie beim Einrichten der Zählerfunktion der Anfangswert von C und Cmax festgelegt wurden). Wenn der Wert der Variablen C verändert worden ist, gibt es vier alternative Möglichkeiten, wie erfindungsgemäß zu verfahren ist.

[0068] Die erste Alternative wird durch den Pfeil G1" bezeichnet, wobei die Antwort wie gewöhnlich berechnet und übermittelt wird. Ein externer Angreifer erhält dann die richtige Antwort auf das durch den Angreifer verwendete Eingangssignal. Die Möglichkeit, den geheimen Schlüssel unter Verwendung von Statistik zu knacken, ist jedoch eingeschränkt worden, da die Zählerfunktion benutzt werden kann, um festzulegen, daß das zu authentifizierende Gerät nur beispielsweise 1000 Antworten erzeugt, bevor es blockiert wird und die Erzeugung richtiger Antworten stoppt.

[0069] Die zweite Alternative wird durch den Pfeil G2" bezeichnet, wobei im Block H" eine zufällige Antwort erzeugt und gesendet wird. Die zufällige Antwort kann eine durch den Zufallszahlengenerator erzeugte Antwort oder alternativ eine Antwort sein, die nach einem anderen Schlüssel als dem für die Authentifizierung benutzten geheimen Schlüssel berechnet wird. Entscheidend ist, daß der externe Angreifer aus der Antwort nicht ableiten kann, ob die Antwort richtig ist oder nicht.

[0070] Die dritte Alternative wird durch den Pfeil G3" bezeichnet, d. h. im Block I" wird eine Anzeige erzeugt und übermittelt, um anzuzeigen, daß das Eingangssignal falsch ist.

[0071] Die vierte Alternative wird durch G4" bezeichnet, wobei die Verarbeitung der Authentifikationsnachricht unterbrochen wird. Dann wird keine Antwort auf die Authentifikationsnachricht gesendet. Der externe Angreifer wird daher keine Antwort auf das Eingangssignal empfangen, was bedeutet, daß der Angreifer keine Statistik über die Eingangssignale und Antworten erfassen oder eine derartige Statistik zum Knacken des geheimen Schlüssels benutzen kann.

[0072] Das Ablaufdiagramm in Fig. 6 zeigt, daß der Vergleich der Variablen C mit dem Grenzwert Cmax sofort nach Empfang des Eingangssignals im Block B" ausgeführt wird. Natürlich ist dies nur ein Beispiel dafür, wie der Vergleich implementiert werden kann. Es existieren folglich viele verschiedene Alternativen, wobei z. B. eine Alternative darin besteht, daß der Vergleich zwischen der Variablen C, die durch die Zählerfunktion genutzt wird, und dem Grenzwert Cmax erst ausgeführt wird, nachdem die empfangene Antwort als falsch ermittelt wurde und der Wert der Zählerfunktion aktualisiert worden ist.

[0073] Es versteht sich, daß die obige Beschreibung und die dazugehörigen Zeichnungen nur zur Erläuterung der vorliegenden Erfindung beabsichtigt sind. Für den Fachmann ist offensichtlich, daß die Erfindung auf verschiedene Arten modifiziert werden kann, ohne von dem in den beigefügten Ansprüchen offenbarten Umfang der Erfindung abzuweichen.

Patentansprüche

1. Verfahren zur Erkennung einer Authentifikationsnachricht, die von einem externen Angreifer in einem Telekommunikationssystem generiert wird, wobei das System aufweist:
mindestens eine Teilnehmerstation (MS, MS'), die einen Zähler (**8**, **8'**) und einen Speicher (**9**, **9'**) mit einem darin gespeicherten teilnehmerstationsspezifischen geschützten Schlüssel (Ki) aufweist, und
Authentifikationsmittel (**1**, **3**, **4**, VLR) zur Authentifikation bzw. Echtheitsprüfung der Teilnehmerstation, wobei die Authentifikationsmittel aufweisen: einen Zufallszahlengenerator (**1**), einen Zähler (**3**) und einen Speicher (**4**) mit dem darin gespeicherten teilnehmerstationsspezifischen geschützten Schlüssel (Ki) der mindestens einen Teilnehmerstation (MS, MS'), wobei die Authentifikationsmittel so eingerichtet sind, daß sie ein Eingangssignal (RAND), das eine unter Verwendung des Zufallszahlengenerators generierte Zufallszahl (RND) enthält, und einen Nachrichtenberechtigungscode (MAC), der mit der Zufallszahl und einem ersten Algorithmus (g) berechnet wird, zu der mindestens einen Teilnehmerstation senden und eine Antwort (SRES) auf der Basis des Eingangssignals (RAND), eines Authentifikationsalgorithmus (A3) und des teilnehmerstationsspezifischen geschützten Schlüssels (Ki) berechnen, und
wobei die Authentifikation einer Teilnehmerstation (MS, MS') durchgeführt wird, indem eine Antwort

(SRES), die von der Teilnehmerstation als Reaktion auf das Eingangssignal (RAND) empfangen wird, mit der durch die Authentifikationsmittel berechneten Antwort (SRES) verglichen wird, wobei das Verfahren aufweist:
Empfang einer das Eingangssignal (RAND) enthaltenden Authentifikationsnachricht mit der mindestens einen Teilnehmerstation (MS, MS'),
Prüfen der Richtigkeit des Eingangssignals durch Berechnen eines Nachrichtenberechtigungscodes in der mindestens einen Teilnehmerstation (MS, MS') unter Verwendung eines vorgegebenen, die Zufallszahl enthaltenden Teils (RND) des Eingangssignals (RAND) und eines Prüfalgorithmus (f), und
Erkennen des Eingangssignals als falsch und der Authentifikationsnachricht als durch den externern Angreifer generiert, wenn der berechnete Nachrichtenberechtigungscode nicht dem übrigen, den Nachrichtenberechtigungscode enthaltenden Teil (MAC) des Eingangssignals (RAND) entspricht, und
Berechnen einer Antwort (SRES) auf der Basis des Authentifikationsalgorithmus (A3), des Eingangssignals (RAND) und des geschützten Schlüssels (Ki), der im Speicher (**9**, **9'**) der Teilnehmerstation (MS, MS') abgelegt ist, und Übermitteln der Antwort (SRES) von der mindestens einen Teilnehmerstation (MS, MS'), wenn der berechnete Nachrichtenberechtigungscode dem übrigen, den Nachrichtenberechtigungscode enthaltenden Teil (MAC) des Eingangssignals (RAND) entspricht.

2. Verfahren nach Anspruch 1, das aufweist: Unterhalten einer Zählerfunktion, um ein Protokoll der Anzahl falscher Eingangsignale (RAND) zu führen, und Blockieren der Authentifikationsfunktion des zu authentifizierenden Geräts, so daß das zu authentifizierende Gerät in den Authentifikationsnachrichten keine richtigen Antworten (SRES) auf die Eingangsignale (RAND) mehr erzeugt, wenn die Zählerfunktion anzeigt, daß die Anzahl falscher Eingangsignale einen vorgegebenen Grenzwert erreicht hat.

3. Verfahren nach einem der Ansprüche 1 bis 2, das die Erzeugung und Übermittlung einer zufälligen Antwort aufweist, wenn das Eingangssignal (RAND) falsch ist.

4. Verfahren nach Anspruch 3, wobei die zufällige Antwort eine Zufallszahl ist.

5. Verfahren nach Anspruch 3, wobei die zufällige Antwort unter Verwendung des Eingangssignals (RAND) und eines vorgegebenen Algorithmus berechnet wird.

6. Telekommunikationssystem, das aufweist:
Authentifikationsmittel (**1**, **3**, **4**, VLR) zur Authentifikation einer Teilnehmerstation, wobei die Authentifikationsmittel einen Zufallszahlengenerator (**1**), einen Zähler (**3**) und einen Speicher (**4**) mit einem darin gespeicherten teilnehmerstationsspezifischen geschützten Schlüssel (Ki) der Teilnehmerstation (MS, MS') aufweisen, wobei die Authentifikationsmittel so eingerichtet sind, daß sie
– ein Eingangssignal (RAND) berechnen, indem ein Nachrichtenberechtigungscode mit einer Zufallszahl (RND) vom Zufallszahlengenerator (**1**) und einem ersten Algorithmus (g) berechnet wird und die Zufallszahl und der Nachrichtenberechtigungscode in das Eingangssignal (RAND) aufgenommen werden,
– eine Antwort (SRES) berechnen, die auf dem Eingangssignal (RAND), einem Authentifikationsalgorithmus (A3) und dem im Speicher (**4**) der Authentifikationsmittel abgelegten teilnehmerstationsspezifischen geschützten Schlüssel (Ki) basiert,
– das Eingangssignal (RAND) zur Teilnehmerstation (MS) senden und
– anzeigen, daß als Reaktion darauf, daß das Authentifikationsmittel (VLR) von der Teilnehmerstation (MS, MS') eine Antwort (SRES) empfängt, die einer durch die Authentifikationsmittel berechneten Antwort (SRES) entspricht, die Teilnehmerstation (MS, MS') authentifiziert worden ist, und
mindestens eine Teilnehmerstation (MS, MS'), die einen Zähler (**8**, **8'**) und einen Speicher (**9**, **9'**) mit einem darin abgelegten, für die Teilnehmerstation (MS, MS') spezifischen geschützten Schlüssel (Ki) aufweist, wobei die Teilnehmerstation (MS, MS') so eingerichtet ist, daß sie:
– einen vorgegebenen, die Zufallszahl enthaltenden Teil (RND) des Eingangssignals (RAND) und einen Prüfalgorithmus (f) nutzt, um einen Nachrichtenberechtigungscode (MAC) zu berechnen und die Richtigkeit eines empfangenen Eingangssignals (RAND) zu prüfen,
– als Reaktion auf einen berechneten Nachrichtenberechtigungscode (MAC), der einem den Nachrichtenberechtigungscode (MAC) enthaltenden restlichen Teil des Eingangssignals (RAND) nicht entspricht, das Eingangssignal (RAND) als falsch erkennt, und
– als Reaktion auf den berechneten Nachrichtenberechtigungscode (MAC), der dem restlichen Teil des Eingangssignals (RAND) entspricht, der den Nachrichtenberechtigungscode (MAC) enthält, auf der Basis des Authentifikationsalgorithmus (A3), des im Speicher (**9**, **9'**) der Teilnehmerstation (MS, MS') abgelegten geschützten Schlüssels (Ki) und des Eingangssignals (RAND) eine durch die Teilnehmerstation (MS, MS') zum Authentifikationsmittel (VLR) zu übermittelnde Antwort berechnet.

7. System nach Anspruch 6, wobei die Teilnehmerstation (MS') so eingerichtet ist, daß sie:
– eine Zählerfunktion (**7'**, **9'**) unterhält, um ein Protokoll der Anzahl (C) falscher Eingangssignale (RAND) zu führen, und
als Reaktion auf eine Anzeige durch die Zählerfunktion (**7'**, **9'**), daß die Anzahl (C) falscher Eingangsignale einem vorgegebenen Grenzwert (Cmax) entspricht, zu blockieren, so daß die Teilnehmerstation

nicht mehr für die Erzeugung richtiger Antworten auf die empfangenen Eingangssignale eingerichtet ist.

8. System nach Anspruch 6 oder 7, wobei die Teilnehmerstation (MS, MS') so eingerichtet ist, daß sie eine zufällige Antwort berechnet, die durch die Teilnehmerstation (MS, MS') als Reaktion auf ein falsches Eingangssignal zu dem Authentifikationsmittel (VLR) gesendet werden soll.

9. System nach Anspruch 6 oder 7, wobei die Teilnehmerstation (MS, MS') so eingerichtet ist, daß sie als Reaktion auf ein falsches Eingangssignal (RAND) keine Antwort zu dem Authentifikationsmittel sendet.

10. System nach einem der Ansprüche 6 bis 9, wobei das System ein mobiles Kommunikationssystem ist, vorzugsweise ein GSM-System.

11. Authentifikationszentrum (AC) eines Telekommunikationssystems, wobei das Telekommunikationssystem mindestens eine Teilnehmerstation (MS, MS') aufweist, die einen Zähler (**8**, **8'**) und einen Speicher (**9**, **9'**) mit einem darin gespeicherten teilnehmerstationsspezifischen geschützten Schlüssel (Ki) aufweist, und wobei die Authentifikation einer Teilnehmerstation (MS, MS') durchgeführt wird, indem ein Eingangssignal (RAND) zu der Teilnehmerstation gesendet wird und eine Antwort (SRES), die von der Teilnehmerstation als Reaktion auf das Eingangssignal (RAND) empfangen wird, mit einer durch das Authentifikationszentrum (AC) berechneten Antwort (SRES) verglichen wird, wobei das Authentifikationszentrum (AC) aufweist:
einen Zufallszahlengenerator (**1**),
einen Zähler (**3**), und
einen Speicher (**4**) mit darin abgelegten teilnehmerstationsspezifischen geschützten Schlüsseln von Teilnehmerstationen,
wobei das Authentifikationszentrum so eingerichtet ist, daß es:
– ein Eingangssignal (RAND) erzeugt, indem es mit einer Zufallszahl (RND) von dem Zufallszahlengenerator (**1**) und einem ersten Algorithmus (g) einen Nachrichtenberechtigungscode berechnet und die Zufallszahl und den Nachrichtenberechtigungscode in das Eingangssignal (RAND) aufnimmt, und
– auf der Basis eines aus dem Speicher (**4**) abgerufenen geschützten Schlüssels (Ki), des Eingangssignals (RAND) und eines Authentifikationsalgorithmus (A3) eine Antwort (SRES) berechnet, und
– das Eingangssignal (RAND) und die Antwort (SRES) zu einem Netzwerkelement sendet, das eine Authentifikation der Teilnehmerstation (MS, MS') durchführt.

12. Teilnehmerstation (MS, MS') eines Telekommunikationssystems, wobei das Telekommunikationssystem Authentifikationsmittel (**1**, **3**, **4**, VLR) zur Authentifikation der Teilnehmerstation aufweist, wobei die Authentifikationsmittel einen Zufallszahlengenerator (**1**), einen Zähler (**3**) und einen Speicher (**4**) mit einem darin gespeicherten teilnehmerstationsspezifischen geschützten Schlüssel (Ki) der mindestens einen Teilnehmerstation (MS, MS') aufweisen, wobei die Authentifikationsmittel so eingerichtet sind, daß sie ein Eingangssignal (RAND), das eine unter Verwendung des Zufallszahlengenerators generierte Zufallszahl (RND) enthält, und einen mit der Zufallszahl und einem ersten Algorithmus berechneten Nachrichtenberechtigungscode (MAC) zu der Teilnehmerstation senden und auf der Basis des Eingangssignals (RAND), eines Authentifikationsalgorithmus (A3) und des teilnehmerstationsspezifischen geschützten Schlüssels (Ki) eine Antwort (SRES) berechnen, und
wobei die Authentifikation einer Teilnehmerstation (MS, MS') durchgeführt wird, indem eine Antwort (SRES), die von der Teilnehmerstation als Reaktion auf das Eingangssignal (RAND) empfangen wird, mit der durch die Authentifikationsmittel berechneten Antwort (SRES) verglichen wird, wobei die Teilnehmerstation aufweist:
einen Speicher (**9**, **9'**) mit einem darin gespeicherten geschützten Schlüssel (Ki),
eine Einrichtung zum Empfang eines Eingangssignals (RAND) und
einen Zähler (**5**, **8**, **8'**), und
wobei die Teilnehmerstation so eingerichtet ist, daß sie einen vorgegebenen, die Zufallszahl enthaltenden Teil (RND) des Eingangssignals (RAND) und einen Prüfalgorithmus (f) nutzt, um einen Nachrichtenberechtigungscode (MAC) zu berechnen und die Richtigkeit eines Eingangssignals zu prüfen, und als Reaktion darauf, daß der berechnete Nachrichtenberechtigungscode (MAC) einem den Nachrichtenberechtigungscode (MAC) enthaltenden restlichen Teil des Eingangssignals (RAND) nicht entspricht, erkennt, daß das Eingangssignal (RAND) falsch ist, und
wobei der Zähler (**8**, **8'**) so eingerichtet ist, daß er als Reaktion darauf, daß der berechnete Nachrichtenberechtigungscode (MAC) einem den Nachrichtenberechtigungscode (MAC) enthaltenden restlichen Teil des Eingangssignals entspricht, auf der Basis des Authentifikationsalgorithmus (A3), des geschützten Schlüssels (Ki) und des Eingangssignals (RAND) eine Antwort (SRES) berechnet.

13. Teilnehmerstation nach Anspruch 12, wobei die Teilnehmerstation so eingerichtet ist, daß sie:
– eine Zählerfunktion (**7'**, **9'**) unterhält, um ein Protokoll der Anzahl (C) falscher Eingangsignale (RAND) zu führen, und
– als Reaktion auf eine Anzeige durch die Zählerfunktion (**7'**, **9'**), daß die Anzahl (C) falscher Eingangsignale einem vorgegebenen Grenzwert (Cmax) entspricht, blockiert, so daß die Teilnehmerstation nicht mehr für die Erzeugung richtiger Antworten auf emp-

fangene Eingangsignale eingerichtet ist.

14. Teilnehmerstation nach einem der Ansprüche 11 bis 13, wobei die Teilnehmerstation (MS, MS') eine Teilnehmerstation eines mobilen Kommunikationssystems, vorzugsweise eines GSM-Systems ist und der Speicher (**9**, **9'**) und/oder der Zähler (**5**, **8**, **8'**) auf einer SIM-Karte angeordnet sind, die abnehmbar an der Teilnehmerstation angebracht wird.

15. Teilnehmerstation nach einem der Ansprüche 11 bis 14, wobei der Zähler (**8**, **8'**) so eingerichtet ist, daß er eine zufällige Antwort berechnet, welche die Teilnehmerstation (MS, MS') als Reaktion auf ein falsches Eingangssignal (RAND) übermittelt.

16. SIM-Karte (SIM) für eine Teilnehmerstation eines Telekommunikationssystems, wobei das Telekommunikationssystem Authentifikationsmittel (**1**, **3**, **4**, VLR) zur Authentifikation einer Teilnehmerstation aufweist, wobei die Authentifikationsmittel einen Zufallszahlengenerator (**1**), einen Zähler (**3**) und einen Speicher (**4**) mit einem darin gespeicherten teilnehmerstationsspezifischen geschützten Schlüssel (Ki) der mindestens einen Teilnehmerstation (MS, MS') aufweisen, wobei die Authentifikationsmittel so eingerichtet sind, daß sie ein Eingangssignal (RAND), das eine unter Verwendung des Zufallszahlengenerators generierte Zufallszahl (RND) enthält, und einen mit der Zufallszahl und einem ersten Authentifikationsalgorithmus berechneten Nachrichtenberechtigungscode (MAC) zu der Teilnehmerstation senden und auf der Basis des Eingangssignals (RAND), eines Authentifikationsalgorithmus (A3) und des teilnehmerstationsspezifischen geschützten Schlüssels (Ki) eine Antwort (SRES) berechnen, und
wobei die Authentifikation einer Teilnehmerstation (MS, MS') durchgeführt wird, indem eine von der Teilnehmerstation als Reaktion auf das Eingangssignal (RAND) empfangene Antwort (SRES) mit der durch die Authentifikationsmittel berechneten Antwort (SRES) verglichen wird, wobei die SIM-Karte aufweist:
einen Zähler (**8**, **8'**) und
einen Speicher (**9**, **9'**) mit einem darin gespeicherten geschützten Schlüssel (Ki), und
einen Eingang zum Empfang eines Eingangssignals (RAND),
wobei die SIM-Karte so eingerichtet ist, daß sie
– einen vorgegebenen, die Zufallszahl enthaltenden Teil (RND) des Eingangssignals (RAND) und einen Prüfalgorithmus (f) nutzt, um einen Nachrichtenberechtigungscode (MAC) zu berechnen und die Richtigkeit des empfangenen Eingangssignals (RAND) zu prüfen,
– als Reaktion darauf, daß der berechnete Nachrichtenberechtigungscode (MAC) einem den Nachrichtenberechtigungscode (MAC) enthaltenden restlichen Teil des Eingangssignals (RAND) nicht entspricht, erkennt, daß das Eingangssignal (RAND) falsch ist, und
– als Reaktion darauf, daß der berechnete Nachrichtenberechtigungscode (MAC) einem den Nachrichtenberechtigungscode (MAC) enthaltenden restlichen Teil des Eingangssignals entspricht, eine Antwort (SRES) auf der Basis des Authentifikationsalgorithmus (A3), des geschützten Schlüssels (Ki) und des Eingangssignals (RAND) berechnet.

17. SIM-Karte nach Anspruch 16, wobei die SIM-Karte so eingerichtet ist, daß sie:
– eine Zählerfunktion (**7'**, **9'**) unterhält, um ein Protokoll der Anzahl (C) falscher Eingangsignale (RAND) zu führen, und
– als Reaktion auf eine Anzeige durch die Zählerfunktion (**7'**, **9'**), daß die Anzahl (C) falscher Eingangsignale (RAND) einem vorgegebenen Grenzwert (Cmax) entspricht, blockiert, so daß die SIM-Karte nicht mehr für die Erzeugung richtiger Antworten auf die empfangenen Eingangsignale eingerichtet ist.

18. SIM-Karte nach Anspruch 16 oder 17, wobei der Zähler (**8**, **8'**) so eingerichtet ist, daß er als Reaktion auf ein falsches Eingangssignal (RAND) eine zufällige Antwort berechnet.

Es folgen 5 Blatt Zeichnungen

Anhängende Zeichnungen

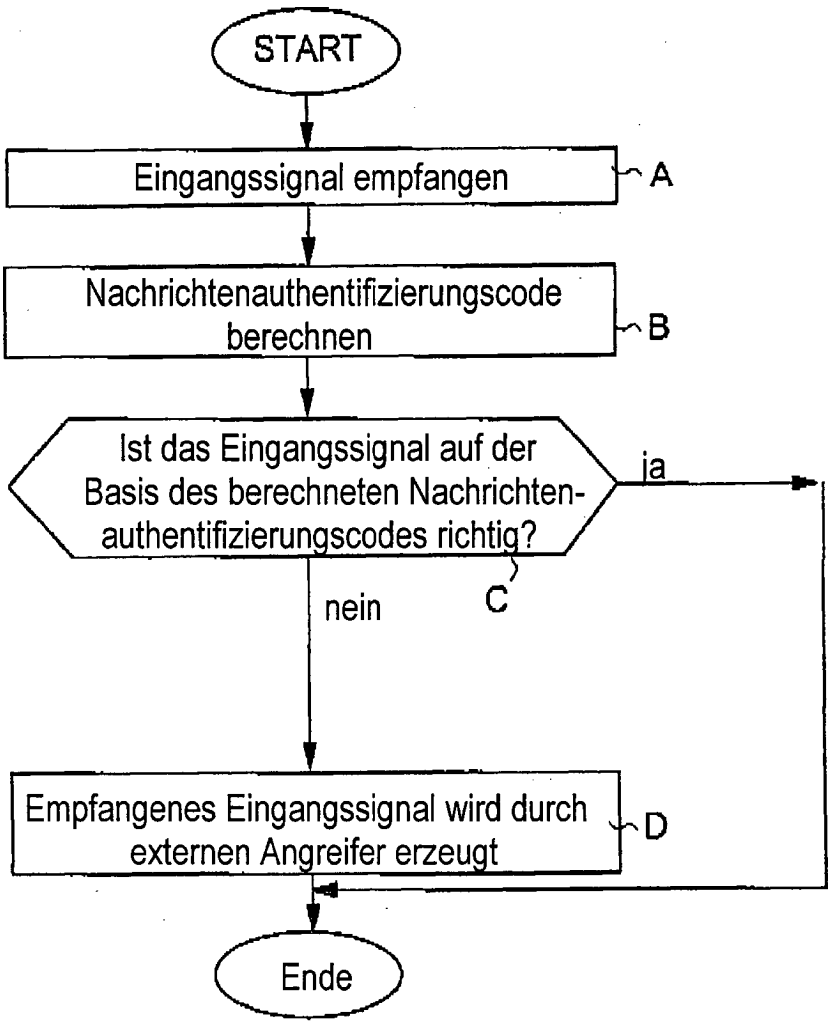

FIG. 1

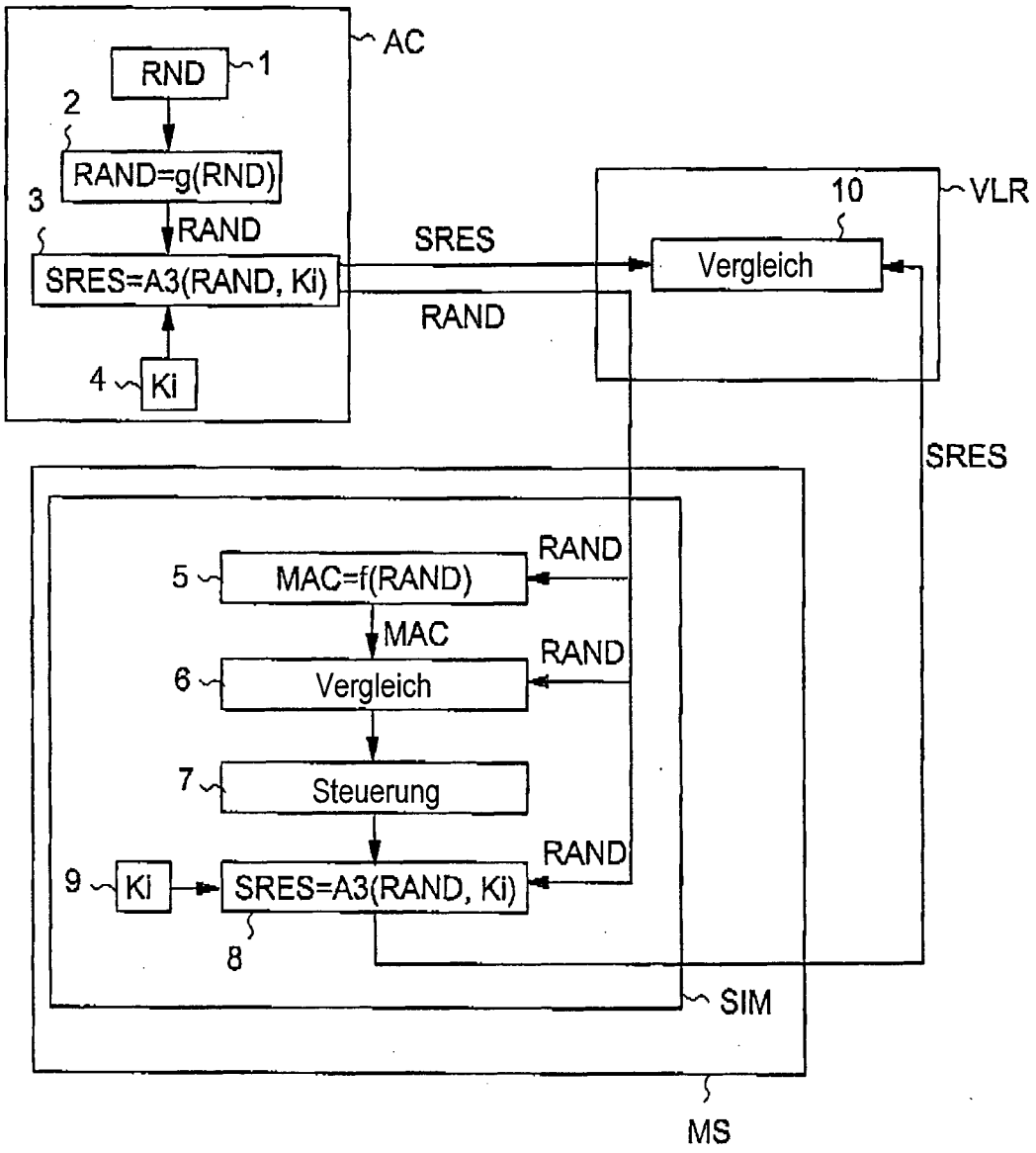
AC
RND
1
2
RAND=g(RND)
3
RAND
SRES=A3(RAND, Ki)
4
Ki
SRES
RAND
10
VLR
Vergleich
SRES
RAND
5
MAC=f(RAND)
MAC
RAND
6
Vergleich
7
Steuerung
RAND
9
Ki
SRES=A3(RAND, Ki)
8
SIM
MS

FIG. 2

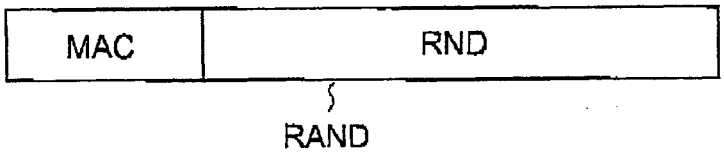
MAC
RND
RAND

FIG. 3

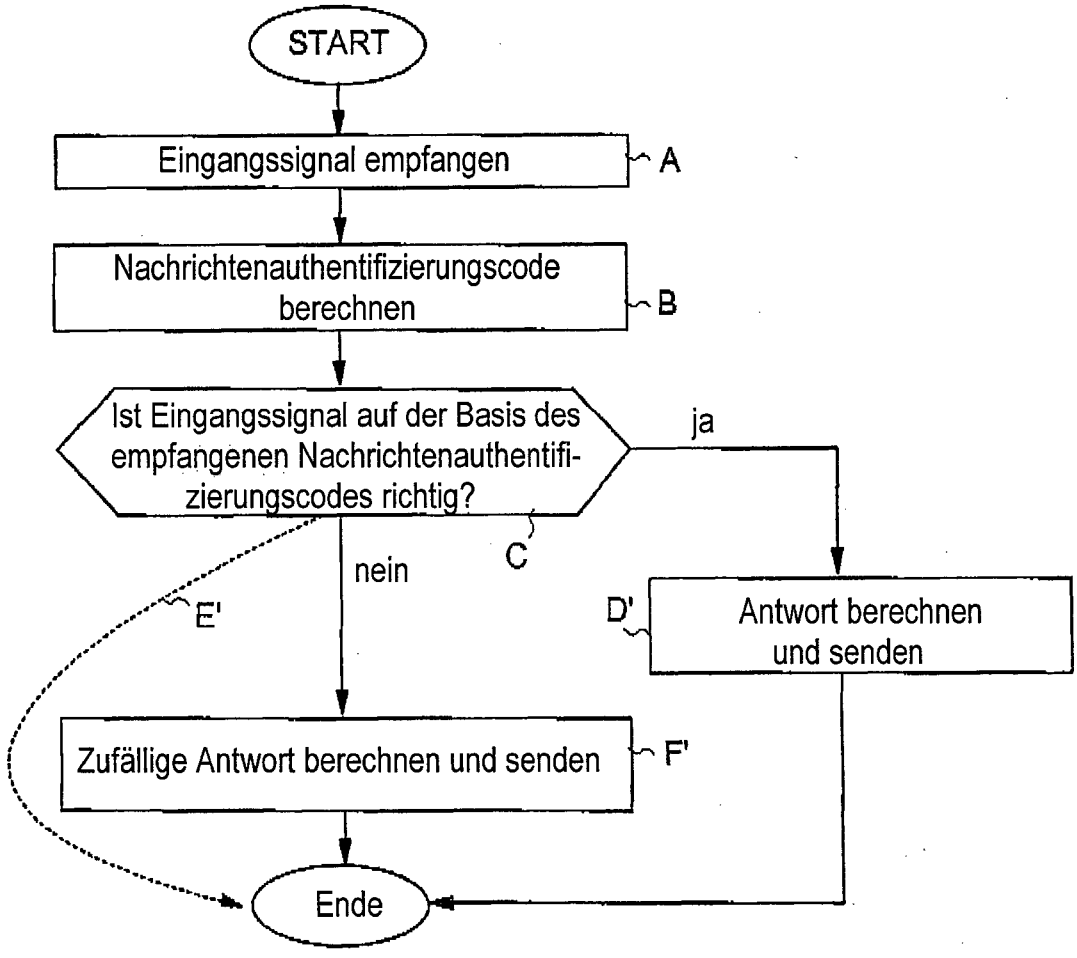
START
Eingangssignal empfangen
A
Nachrichtenauthentifizierungscode berechnen
B
Ist Eingangssignal auf der Basis des empfangenen Nachrichtenauthentifizierungscodes richtig?
C
ja
nein
E'
D'
Antwort berechnen und senden
Zufällige Antwort berechnen und senden
F'
Ende

FIG. 4

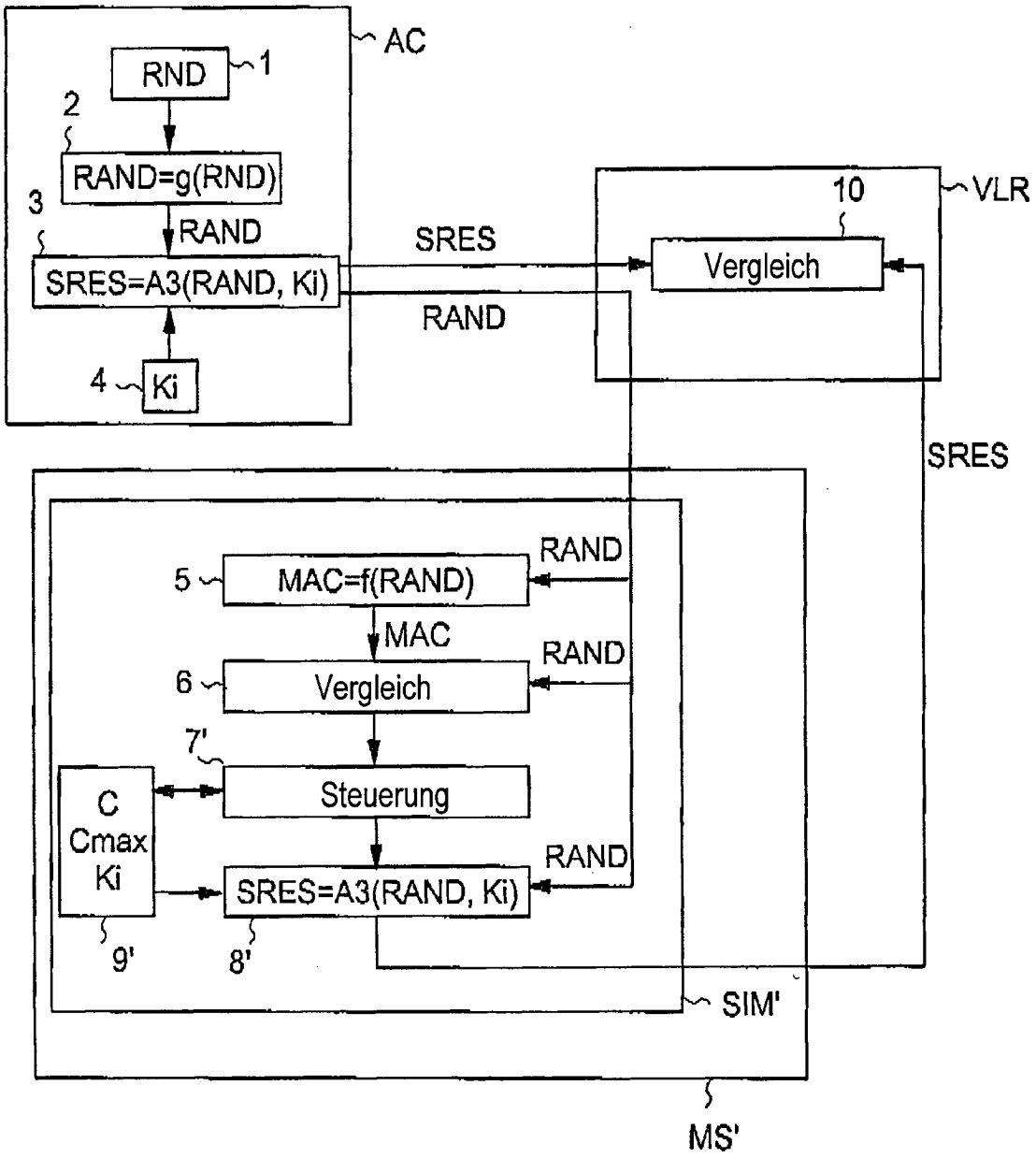
AC
RND
1
2
RAND=g(RND)
3
RAND
SRES=A3(RAND, Ki)
4
Ki
SRES
RAND
10
VLR
Vergleich
SRES
RAND
5
MAC=f(RAND)
MAC
RAND
6
Vergleich
RAND
7'
Steuerung
C
Cmax
Ki
RAND
SRES=A3(RAND, Ki)
9'
8'
SIM'
MS'

FIG. 5

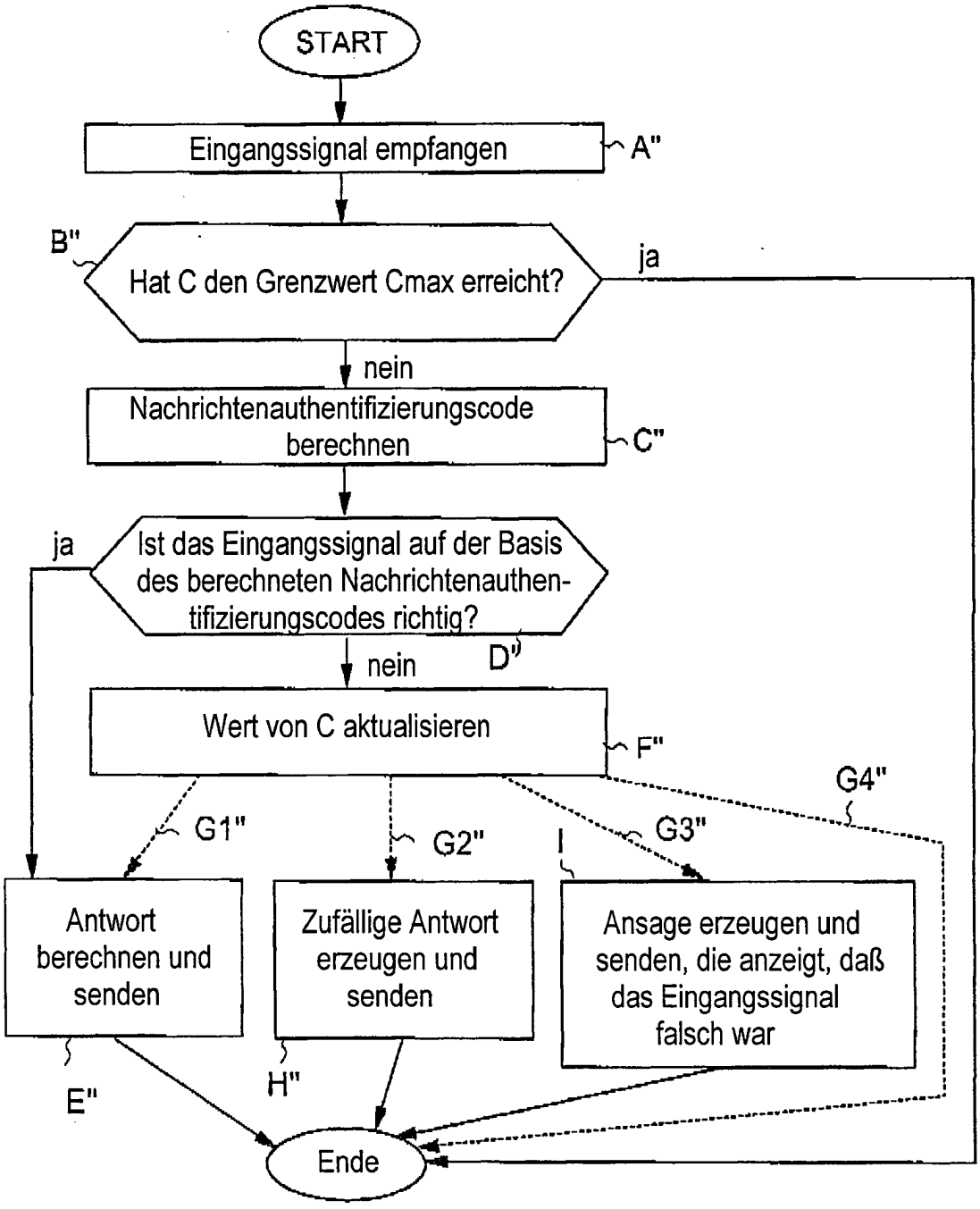
START
Eingangssignal empfangen
A"
B"
Hat C den Grenzwert Cmax erreicht?
ja
nein
Nachrichtenauthentifizierungscode berechnen
C"
ja
Ist das Eingangssignal auf der Basis des berechneten Nachrichtenauthentifizierungscodes richtig?
nein
D"
Wert von C aktualisieren
F"
G4"
G1"
G2"
G3"
I
Antwort berechnen und senden
Zufällige Antwort erzeugen und senden
Ansage erzeugen und senden, die anzeigt, daß das Eingangssignal falsch war
E"
H"
Ende

FIG. 6