(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 848 362 A2

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
17.06.1998 Patentblatt 1998/25

(51) Int. Cl.[6]: **G07F 7/10**, G07C 9/00

(21) Anmeldenummer: **97118867.7**

(22) Anmeldetag: **30.10.1997**

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

(30) Priorität: **14.12.1996 DE 19652161**

(71) Anmelder: **Deutsche Telekom AG**
53113 Bonn (DE)

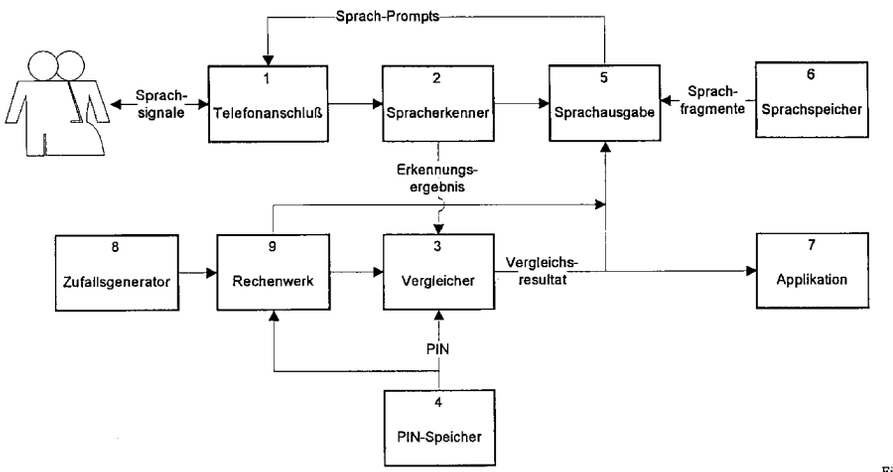
(72) Erfinder:
Naumburger, Volkmar, Dr.
15537 Erkner (DE)

(54) Verfahren und Anordnung zur abhörsicheren Eingabe von Pin-Codes im sprachlichen Dialog

(57) Die erfindungsgemäße Lösung ist auf eine sichere und schnelle Lösung zur abhörsicheren Eingabe von PIN-Codes per Sprache ausgerichtet.

Erfindungsgemäß wird nach Erkennung des Freigabewunsches des Nutzers für jede Ziffer der PIN eine nach dem Zufallsprinzip generierte Manipulationsziffer und eine aus der PIN-Ziffer und der Manipulationsziffer abgeleitete Manipulationsanweisung erzeugt. Die Manipulationsoperation wird im Rechenwerk (9) für jede PIN-Ziffer automatisch durchgeführt und als Pseudo-PIN gespeichert. Gleichzeitig werden nacheinander für jede PIN-Ziffer die Manipulationsziffer und die Manipulationsanweisung an den Nutzer ausgegeben. Der Nutzer gibt die Ergebnisse seiner Manipulationsoperationen über den öffentlichen Kommandoweg ein. Im Vergleicher (3) wird die gespeicherte Pseudo-PIN mit der durch den Nutzer eingegebenen Pseudo-PIN verglichen. Bei Übereinstimmung erfolgt die Freigabe.

Die erfindungsgemäße Lösung läßt sich vorteilhaft bei den Anwendungen einsetzen, bei denen eine mündliche Eingabe von PIN-Ziffern über einen öffentlichen Kommandoweg erfolgt.



Figur 1

EP 0 848 362 A2

Beschreibung

Die Erfindung betrifft ein Verfahren und eine Anordnung zur abhörsicheren Eingabe von PIN-Codes bei der Anwendung von spracherkennenden Eingabemedien.

Bekannte technische Lösungen basieren alle direkt (z. B. Geldautomaten) oder indirekt (z. B. Fernabfrage eines Anrufbeantworters) auf der Benutzung von numerischen Tastaturen. Dem Sicherheitsaspekt wird Rechnung getragen, indem während der Eingabe der PIN ein Sichtschutz um das Eingabemedium gewährleistet wird. Dieses Verfahren wird als ausreichend betrachtet, um die unbefugte Benutzung der PIN durch andere Personen zu verhindern.

Problematischer ist die Eingabe von PIN`s im direkten sprachlichen Dialog. Eine solche Situation ist gegeben, wenn telefonische Orders an einen Operator (z. B. Bankangestellte) oder Spracherkenner verfügt werden sollen. In solchen Fällen ist nicht immer eine geschützte Sphäre zu gewährleisten, so daß unbefugte Personen die Eingabe der PIN akustisch verfolgen können. Um die Geheimhaltung auch in diesen Fällen gewährleisten zu können, muß die PIN-Eingabe verschlüsselt erfolgen. Dabei kann davon ausgegangen werden, daß die Aufforderung (Kommandoweg) zur PIN-Eingabe durch die Benutzung nutzerbezogener Hörer, z. B. Telefonhörer oder Sprechgeschirr, nichtöffentlich stattfindet, während die Eingabe per Sprache durch den Nutzer (Eingabeweg) öffentlich bleibt.

Eine bekannte Lösung, mit der die Geheimhaltung der Sprach-Eingabe der PIN über einen öffentlichen Kommandoweg gewährleistet werden soll, beruht auf dem Verlesen der Ziffern von 0 bis 9 in aufsteigender Reihenfolge. Diese Ziffern werden dem Nutzer über den nichtöffentlichen Kommandoweg zur Auswahl angeboten. Tritt die entsprechende Ziffer der einzugebenden PIN auf, so spricht der Nutzer das unspezifische Wort "HALT", womit die geheime Ziffer gekennzeichnet wird. Auf diese Weise kann eine mehrstellige PIN durch wiederholte Anwendung dieses Verfahrens eingegeben werden. Nachteilig an diesem Verfahren ist, daß bei ungünstiger Wahl der PIN die Eingabeprozedur recht langwierig sein kann. Zum Beispiel würde die Eingabe der PIN "9999" länger als 2 Minuten in Anspruch nehmen, wenn das Vorlesen einer Ziffer inklusive Pause nur 3 Sekunden dauern würde. Ein weiterer Nachteil besteht in der eingeschränkten Sicherheit, denn mit einiger Übung kann aus dem Zeitpunkt, wenn das "HALT" gesprochen wird, auf die Ziffer rückgeschlossen werden.

Die Erfindung verfolgt das Ziel, eine abhörsicherere Lösung zur Eingabe von PIN-Codes per Sprache zu schaffen, die sicherer und schneller als die bekannten Lösungen ist.

Das erfindungsgemäße Verfahren beruht darauf, daß die Ziffern der einzugebenden PIN reihenfolgerichtig nacheinander in einzelnen in sich geschlossenen Frage-Antwort-Prozeduren abgefragt werden. Die Abfrageprozedur (Eingabeaufforderung an den Nutzer) erfolgt über den nichtöffentlichen Kommandoweg. Die Antwortprozedur (Antwort durch den Nutzer) erfolgt über den öffentlichen Kommandoweg. Durch die Eingabeaufforderung wird der Nutzer aufgefordert, zu der abgeforderten PIN-Ziffer eine über den nichtöffentlichen Kommandoweg vorgegebene Manipulationsziffer und eine mit der Manipulationsziffer logisch verknüpfte Manipulationsanweisung mit der PIN-Ziffer zu verrechnen. Die im Ergebnis dieser Operation entstehende Pseudo-PIN-Ziffer gibt der Nutzer über den öffentlichen Eingabeweg per Sprache ein. Die Sicherheit der PIN-Eingabe wird dadurch gewährleistet, daß ein Zufallsgenerator 8 auf der Kommandoseite sowohl die Manipulationsziffer als auch die Manipulationsanweisung ständig neu bestimmt. Damit die entsprechend der Manipulationsanweisung durchzuführende Rechenoperation, die vom Nutzer einzeln zu jeder PIN-Ziffer durchzuführen und einzugeben ist, nicht zu kompliziert wird, beschränkt sich die Manipulationsanweisung auf die Addition bzw. die Subtraktion. Die Festlegung der konkreten Manipulationsanweisung wird durch die Prämisse bestimmt, daß die nach der Manipulationsanweisung zu berechnende Pseudo-PIN-Ziffer die Zehnerposition nicht überschreitet, und daß bei der Subtraktion immer die größere Ziffer von der kleineren Ziffer abgezogen wird. Wird eine derart manipulierte PIN über den öffentlichen Kommandoweg eingegeben, so kann ein unbefugter Zuhörer in keiner Weise Rückschlüsse auf die wirkliche PIN ziehen. Das Verfahren wird über eine Anordnung realisiert, bei der die PIN-Abfrage über einen öffentlichen Telefonanschluß erfolgt. Dieser Telefonanschluß 1 ist im System mit einem Spracherkenner 2 verbunden, der über eine Sprachausgabe 5 an einem Sprachspeicher 6 anliegt. Die Sprachausgabe 5 ist gleichzeitig über eine Direktverbindung mit dem Telefonanschluß 1 verbunden. Der Spracherkenner 2 besitzt eine Verbindung zu einem Vergleicher 3. Desweiteren ist ein Zufallsgenerator 8 über ein Rechenwerk 9 mit dem Vergleicher 3 verbunden. Der Vergleicher 3 ist mit dem PIN-Speicher 4 und einer Baugruppe Applikation 7 verbunden. Der PIN-Speicher 4 besitzt eine Querverbindung zum Rechenwerk 9. Eine weitere Querverbindung besteht zwischen dem Rechenwerk 9, der Sprachausgabe 5 und der Applikation 7. Die Erfindung wird nachfolgend anhand eines Ausführungsbeispiels näher erläutert. In Figur 1 ist die dem Verfahren zugrunde liegend Anordnung in Form eines Blockschaltbildes dargestellt. Die PIN-Abfrage erfolgt über einen öffentlichen Telefonanschluß der in Fig.1 als Telefonanschluß 1 abgebildet ist. Im PIN-Speicher 4 ist die PIN in numerischer Form abgespeichert. Bei einer Nutzeridentifikation ist diese PIN durch einen berechtigten Nutzer zu reproduzieren. Die Prozedur wird gestartet, indem vom Sprachspeicher 6 über die Sprachausgabe 5 und den öffentlichen Kommandoweg die entsprechenden Sprach-Promts an den Nutzer ausgegeben wer-

den, die die Aufforderung zur PIN-Eingabe enthalten. Gleichzeitig wird der Stellenzähler im Rechenwerk 9 auf die erste Stelle rückgesetzt und inkrementiert. Damit zeigt der Stellenzähler 9 auf die erste Ziffer der gespeicherten PIN. Durch diesen Vorgang wird im Zufallsgenerator 8 die Erzeugung einer ersten Zufallszahl ausgelöst. Die Zufallszahl kann beispielsweise auf einen Wert zwischen 0 und 9 begrenzt sein. Im Rechenwerk 9 wird die erzeugte Zufallszahl mit der ersten Stelle der PIN verglichen. Ist die Summe beider Zahlen kleiner als 10, dann wird der Operand der Manipulationsoperation auf "plus" gesetzt, andernfalls auf "minus". Bei einer Subtraktion wird immer die kleinere Ziffer von der größeren Ziffer abgezogen. Das Rechenwerk 9 führt die vorgeschlagene Operation aus und speichert als Resultat die so erzeugte Pseudo-PIN-Ziffer für die erste Stelle der PIN. Mit der Stellenzahl n, der Zufallszahl x und der Verknüpfung plus oder minus erzeugt die Sprachausgabeeinrichtung 4 die Aussage:

"Bitte geben sie die *erste* Ziffer Ihrer PIN *plus/minus x* ein!"

Der Nutzer führt nun gedanklich dieses Kommando aus und spricht das Ergebnis in den Spracherkenner 2. Das Erkennungsergebnis wird ebenfalls gespeichert. Der Vergleicher 3 stellt fest, ob schon alle Ziffern der PIN abgearbeitet sind, wenn nicht, wird die Prozedur wiederholt, bis alle Stellen der PIN erfaßt worden sind. Im Beispiel hat die PIN vier Stellen, daher muß der Vergleicher 3 testen, ob die Schleife bereits viermal durchlaufen wurde. Wurde die Erfassung aller Stellen der PIN beendet, muß der Vergleich zwischen der durch den Nutzer eingegebenen Pseudo-PIN und der im PIN Speicher 4 gespeicherten PIN erfolgen. Für den Vergleich wird vorzugsweise die vom Nutzer eingegebene Pseudo-PIN mit der im Rechenwerk 9 generierten und gespeicherten Pseudo-PIN verglichen. Eine weitere Möglichkeit besteht darin, die vom Nutzer eingegebene Pseudo-PIN über das Rechenwerk 9 einer Umkehroperation zu unterziehen, in der die Pseudo-PIN wieder in die der Operation zugrunde liegende PIN umgewandelt wird. Anschließend wird die so gewonnene PIN mit der im PIN-Speicher gespeicherten PIN verglichen. Stimmen beide Ziffernfolgen überein, wurde die PIN-Eingabe erfolgreich durchgeführt. Andernfalls wird der Nutzer über die Sprachausgabe 5 zur erneuten PIN-Eingabe aufgefordert. Diese Möglichkeit sollte eingeräumt werden, um Irrtümer beim Rechnen oder eine mangelnde Erkennungssicherheit des Spracherkenners 2 zu berücksichtigen. Der Vergleicher 3 prüft aber, ob die Zahl der Fehlversuche größer als drei ist. Wenn das der Fall ist, dann ist anzunehmen, daß der Nutzer nicht im Besitz der richtigen PIN ist. Daher wird die PIN-Eingabe mit FEHLER abgebrochen. Dieser Sachverhalt wird dem Nutzer über eine entsprechende Ansage der Sprachausgabe 5 mitgeteilt.

Das erfindungsgemäße Verfahren läßt sich auch bei einem System verwenden, welches mehrere PIN' zuläßt, wie es beispielsweise bei einem Banking-System der Fall ist. Bei einem solchen System muß sich der Nutzer vor Abfrage der PIN mit einem öffentlichen Schlüssel ausweisen. Das kann beispielsweise die Kontonummer des Nutzers sein. Anhand des öffentlichen Schlüssels wird im System die PIN des Anrufers, die anhand der Kontonummer ermittelt wurde, bereitgestellt. Danach erfolgt, wie oben beschrieben, anhand der PIN und der zu den einzelnen PIN-Ziffern generierten Manipulationsziffern und Manipulationsanweisungen die Abfrage der Pseudo-PIN.

Bezugszeishenaufstellung

1	Telefonanschluß
2	Spracherkenner
3	Vergleicher
4	PIN-Speicher
5	Sprachausgabe
6	Sprachspeicher
7	Applikation
8	Zufallsgenerator
9	Rechenwerk

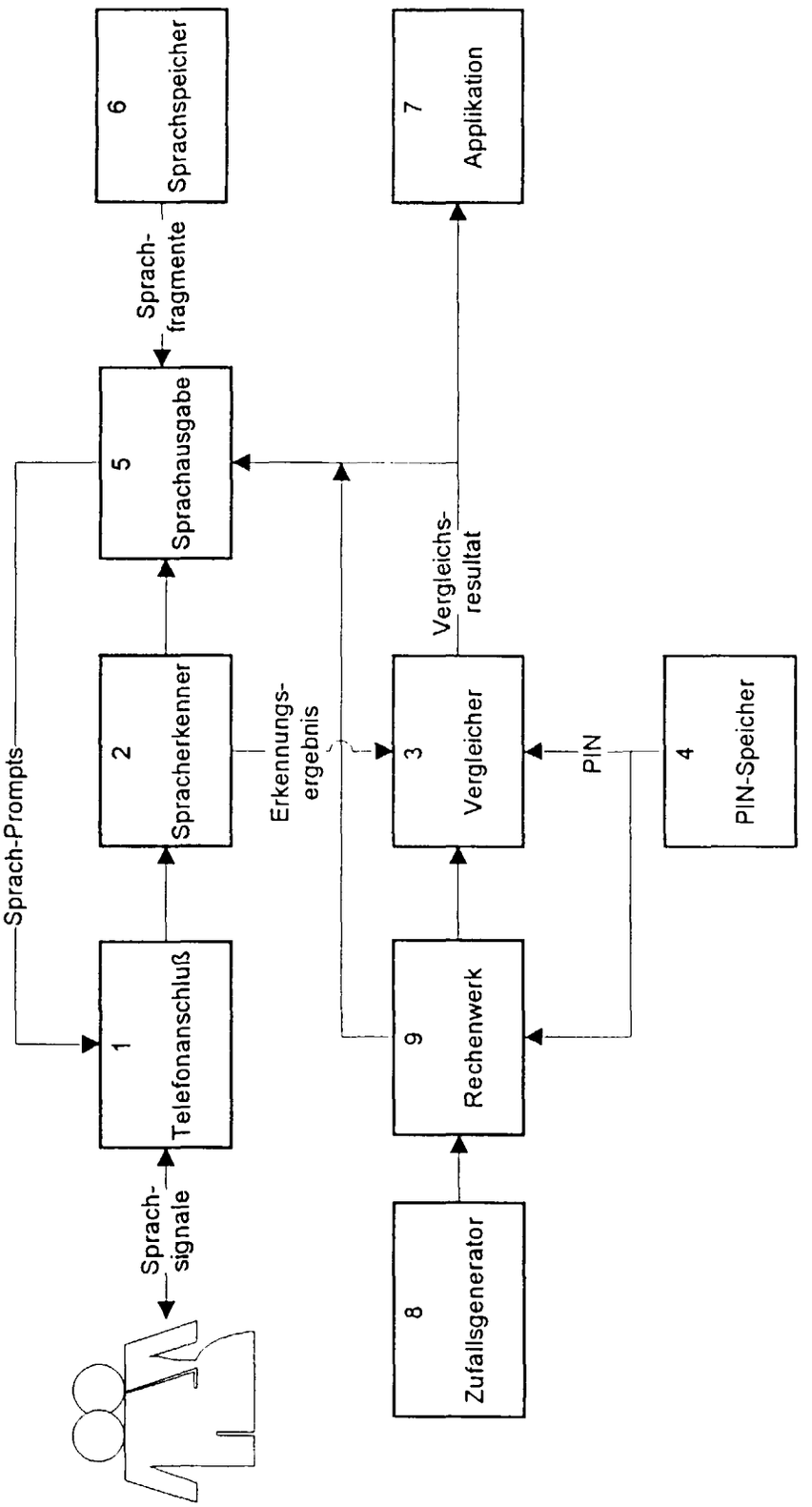
Patentansprüche

1. Verfahren zur abhörsicheren Sprach-Eingabe von PIN-Codes im sprachlichen Dialog, bei dem der Nutzer seine Berechtigung gegenüber dem System in einer Freigabeprozedur durch Eingabe einer dem System bekannten PIN nachweist, wobei die Aufforderung zur Eingabe der PIN an den Nutzer über einen nichtöffentlichen Kommandoweg und die Eingabe der PIN durch den Nutzer über einen öffentlichen Kommandoweg erfolgt, **dadurch gekennzeichnet**, daß nach Erkennung des Freigabewunsches des Nutzers für jede Ziffer der PIN eine nach dem Zufallsprinzip generierte Manipulationsziffer und eine aus der PIN-Ziffer und der Manipulationsziffer abgeleitete Manipulationsanweisung erzeugt werden, und daß alle aus PIN-Ziffer und Manipulationsziffer nach der jeweiligen Manipulationsanweisung berechneten Pseudo-PIN-Ziffern reihenfolgerichtig gespeichert werden, daß die Anfrage des Nutzers nach der PIN ziffernweise in einzelnen Schritten erfolgt, wobei dem Nutzer vor der Abfrage über den nichtöffentlichen Kommandoweg zu jeder PIN-Ziffer die nach dem Zufallsprinzip generierte Manipulationsziffer und die dazugehörige Manipulationsanweisung übermittelt werden, daß durch den Nutzer zu jeder PIN-Ziffer eine aus PIN-Ziffer und Manipulationsziffer nach Manipulationsanweisung erstellte Pseudo-PIN-Ziffer als Sprachinformation über den öffentlichen Kommandoweg eingegeben wird, daß nach Erfassung aller Pseudo-PIN-Ziffern die gespeicherte Pseudo-PIN mit der durch den Nutzer eingegebenen Pseudo-PIN verglichen wird, und daß bei Übereinstimmung die Freigabe erfolgt.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Manipulationsziffer nach dem Zufallsprinzip aus einem Wertevorrat von 1 bis 9 generiert wird, daß in dem Fall, daß die Summe aus PIN-Ziffer und Manipulationsziffer kleiner als 10 ist, der Operand der Manipulationsoperation auf plus gesetzt wird, und daß in dem Fall, daß die Summe aus PIN-Ziffer und Manipulationsziffer größer als 10 ist, der Operand der Manipulationsziffer auf Minus gesetzt wird und die größere Ziffer von der kleineren Ziffer abzuziehen ist, und daß die vorgeschlagene Operation über ein Rechenwerk (9) durchgeführt und als Pseudo-PIN gespeichert wird.

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der Nutzer sich bei einem System, das mehrere PIN zuläßt, vor der Abfrage der PIN mit einem öffentlichen Schlüssel ausweist, und daß im System anhand des öffentlichen Schlüssels die PIN des Anrufers bereitgestellt wird, so daß anhand der PIN und der zu den einzelnen PIN-Ziffern generierten Manipulationsziffern und Manipulationsanweisungen die Anfrage der Pseudo-PIN erfolgen kann.

4. Anordnung zur abhörsicheren Sprach-Eingabe von PIN-Codes im sprachlichen Dialog, **dadurch gekennzeichnet,** daß der Telefonanschluß (1) über seine Anschlußleitung mit einem Spracherkenner (2) verbunden ist, daß der Spracherkenner (2) mit einer Sprachausgabe (5) verbunden ist, an die ein Sprachspeicher (6) angeschaltet ist, daß an den Spracherkenner (2) ein Vergleicher (3) angeschaltet ist, daß ein Zufallsgenerator (8) über ein Rechenwerk (9) mit dem Vergleicher (3) verbunden ist, daß am Vergleicher (3) ein PIN-Speicher (4) angeschlossen ist, daß der Vergleicher (3) mit einer Baugruppe Applikation (7) verbunden ist, über die das Ergebnis der Abfrage weitergeleitet wird, daß der PIN-Speicher (4) eine Querverbindung zum Rechenwerk (9) besitzt, daß das Rechenwerk (9) über eine Querverbindung mit der Sprachausgabe (5) und der Applikation (7) verbunden ist, und daß die Sprachausgabe (5) eine Querverbindung zum Telefonanschluß (1) besitzt.


6
Sprachspeicher
7
Applikation
Sprach-
fragmente
5
Sprachausgabe
Vergleichs-
resultat
Sprach-Prompts
2
Spracherkenner
Erkennungs-
ergebnis
3
Vergleicher
PIN
4
PIN-Speicher
1
Telefonanschluß
9
Rechenwerk
Sprach-
signale
8
Zufallsgenerator

Figur 1