



SCHWEIZERISCHE EIDGENOSSENSCHAFT
EIDGENÖSSISCHES INSTITUT FÜR GEISTIGES EIGENTUM

(11) **CH 698 585 B1**

(51) Int. Cl.: **G07F 7/02 (2006.01)**
G07C 9/00 (2006.01)

Erfindungspatent für die Schweiz und Liechtenstein

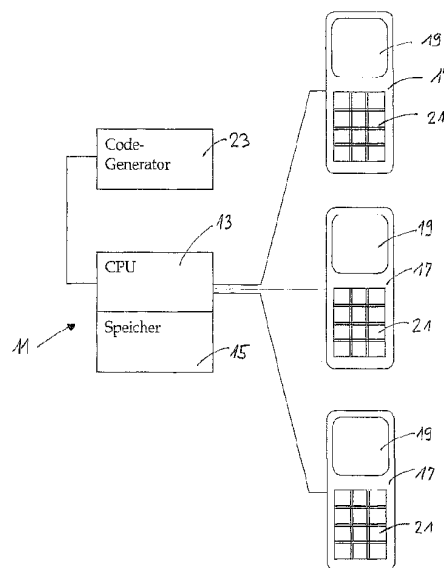
Schweizerisch-liechtensteinischer Patentschutzvertrag vom 22. Dezember 1978

(12) **PATENTSCHRIFT**

<p>(21) Anmeldenummer: 00179/06</p> <p>(22) Anmeldedatum: 06.02.2006</p> <p>(24) Patent erteilt: 15.09.2009</p> <p>(45) Patentschrift veröffentlicht: 15.09.2009</p>	<p>(73) Inhaber: Sven Sauter, Bächliweg 31 9495 Triesen (LI)</p> <p>(72) Erfinder: Sven Sauter, 9495 Triesen (LI)</p> <p>(74) Vertreter: Riederer Hasler & Partner Patentanwälte AG, Kappelstrasse 15 9492 Eschen (LI)</p>
--	--

(54) **Verfahren und Vorrichtung zur Gewährung eines Zutritts zu einem passwortgeschützten System.**

(57) Bei einer Vorrichtung und einem Verfahren zur Gewährung eines Zutritts zu einem passwortgeschützten System kann an einem mit einer Zentraleinheit (11) verbundenen Terminal (17), welcher mit einer Tastatur (21) und einer Anzeige (19) ausgestattet ist, ein Zutrittscode eingegeben werden. Der Zutrittscode wird mit einem in der Zentraleinheit (11) abgespeicherten Code verglichen und der Zutritt des Benutzers zum passwortgeschützten System nur dann gewährt, wenn der eingegebene Zutrittscode mit dem in der Zentraleinheit (11) gespeicherten Code übereinstimmt. Erfindungsgemäss bringt die Zentraleinheit (11) zwei Zeichensätze zur Anzeige, einen ersten geordneten Zeichensatz, welcher den Zutrittscode mindestens als Teilmenge enthält, und einen zweiten zufällig vermischten Zeichensatz. Dabei ist jedem Zeichen des ersten Zeichensatzes jeweils ein Zeichen des zweiten Zeichensatzes zugeordnet. Als Zutrittscode gelten jeweils jene Zeichen des zweiten Zeichensatzes, welche den Zeichen des im ersten Zeichensatz enthaltenen Zutrittscode zugeordnet sind.



Beschreibung

Gebiet der Erfindung

[0001] Die vorliegende Erfindung betrifft ein Verfahren und eine Vorrichtung zur Gewährung eines Zugangs zu einem passwortgeschützten System.

Stand der Technik

[0002] In der jüngeren Zeit sind Fälle bekannt geworden, wo Kreditkartenbetrüger mit Hilfe von bei Geldausgabeautomaten angebrachten Miniaturkameras festgehalten haben, welchen Eingabecode die Benutzer des Geldautomaten eingegeben haben. Durch den gleichzeitigen Einsatz von Lesegeräten am Schlitz der Kartenzuführung ist es Betrügern möglich, Duplikate von Bankkarten herzustellen. Somit sind sie in der Lage, mit Hilfe der gefälschten Karten und der Kenntnis des Kartencodes widerrechtlich Bargeld vom Konto des Karteninhabers abzuheben.

Aufgabe der Erfindung

[0003] Ausgehend von dieser unbefriedigenden Situation stellt sich die Erfindung zur Aufgabe, ein Verfahren und eine Vorrichtung zur Gewährung eines Zutritts zu einem passwortgeschützten System bereitzustellen. Insbesondere ist es ein Ziel zu verhindern, dass Dritte durch Beobachtung der Tasteneingabe auf den Zutrittscode schliessen können.

Beschreibung

[0004] Erfindungsgemäss wird die Aufgabe durch ein Verfahren gelöst, bei welchem die Zentraleinheit zwei Zeichensätze, nämlich einen ersten und einen zweiten Zeichensatz, auf der Anzeige darstellt, wobei der erste Zeichensatz den Zutrittscode mindestens als Teilmenge enthält, und jedem Zeichen des ersten Zeichensatzes jeweils ein Zeichen des zweiten Zeichensatzes zugeordnet wird und mindestens nach jeder erneuten Anmeldung eine neue, wechselnde Zuordnung des zweiten Zeichensatzes zum ersten Zeichensatz hergestellt wird, und als Zutrittscode jeweils jene Zeichen des zweiten Zeichensatzes gelten, welche dem im ersten Zeichensatz enthaltenen Zutrittscode zugeordnet sind. Beim erfindungsgemässen Verfahren wird also durch die Zuordnung eines zweiten Zeichensatzes ein quasi temporärer Zutrittscode gebildet, welcher an der Tastatur eingegeben werden muss, damit der Benutzer die Zutrittsberechtigung erhält. Das Verfahren hat den grossen Vorteil, dass auf Grund der Tasteneingabe nicht auf den wahren Zutrittscode geschlossen werden kann. Jedes Mal, wenn ein Nutzer sich erneut anmeldet, wird auf dem Display eine andere Zuordnung angezeigt, d.h. der temporäre (einzugebende) Zutrittscode ändert sich bei jeder Anmeldung.

[0005] Um einen bestmöglichen Schutz zu erreichen, kann die Anzeige des Display durch geeignete Massnahmen von der Einsehbarkeit durch Drittpersonen geschützt werden (z.B. Sichtschutz oder Folie mit begrenztem Durchblickwinkel).

[0006] Vorteilhaft wird der erste Zeichensatz in einer bestimmten Ordnung auf der Anzeige angezeigt, beispielsweise auf- oder absteigend oder in alphabetischer Reihenfolge. Dies hat den Vorteil, dass der zugeordnete temporäre Zutrittscode für den Nutzer besser auffindbar ist. Zweckmässigerweise ist die Zahl der im ersten Zeichensatz enthaltenen Zeichen umfangreicher als der eigentliche Zutrittscode. Dies hat den Vorteil, dass auf Grund des Umfangs des Zeichensatzes nicht auf die Länge des Zutrittscodes geschlossen werden kann. So können beispielsweise für einen vier- oder sechsstelligen Code die Ziffern 0,1, 2,... bis 9 (also insgesamt 10 Ziffern) in einer ersten Reihe oder ersten Spalte, und die zugeordneten, zufälligen Zahlen (ebenfalls 10 Ziffern) als zweite Reihe oder zweite Spalte auf dem Display angezeigt werden. Anhand des memorierten vier- oder sechsstelligen Zutrittscodes wird der temporäre Zutrittscode aus der zweiten Reihe oder Spalte abgelesen und eingegeben.

[0007] Es ist denkbar, dass der Zutrittscode und die Zeichensätze aus alphanumerischen Zeichen, Zahlen oder Buchstaben bestehen. Gemäss einer bevorzugten Variante umfassen der erste und der zweite Zeichensatz die Zahlen 0,1, 2, ... bis 9, wobei der zweite Zeichensatz jeweils zufällig bezüglich des ersten Zeichensatzes angeordnet wird.

[0008] Gegenstand der vorliegenden Erfindung ist auch eine passwortgeschützte Zutrittskontrolleinheit gemäss Oberbegriff von Anspruch 12, welche dadurch gekennzeichnet ist, dass die Zentraleinheit einem ersten Zeichensatz, welcher die Zeichen des Zutrittscode mindestens als Teilmenge enthält, nach einem bestimmten Algorithmus einen zweiten Zeichensatz zuordnet, wobei jedem Zeichen des ersten Zeichensatzes jeweils ein Zeichen des zweiten Zeichensatzes zugeordnet ist und jeweils bei jedem erneuten Erfassen des Identifikationscode eine neue, wechselnde Zuordnung des zweiten Zeichensatzes zum ersten Zeichensatz hergestellt wird, und den ersten und zweiten Zeichensatz auf der Anzeige anzeigt, und dass als Zutrittscode jeweils jene Zeichen des zweiten Zeichensatzes gelten, welche den Zeichen des im ersten Zeichensatz enthaltenen Zutrittscodes zugeordnet sind. Die Vorteile eines solchen Systems wurden bereits weiter oben diskutiert.

[0009] Vorteilhaft wird der Algorithmus, nach welchem der zweite Zeichensatz dem ersten Zeichensatz zugeordnet wird, als wesentlichen Bestandteil eine Tabelle mit einer Mehrzahl von zweiten Zeichensätzen enthält, wobei bei der Anmeldung eines Benutzers einer dieser zweiten Zeichensätze einem ersten Zeichensatz zugeordnet ist. Dabei kann die Auswahl des zweiten Zeichensatzes auf Zufallsprinzip beruhen, oder es kann jeweils der nächstfolgende Satz in der Tabelle ausgewählt werden. Gemäss einer anderen Variante enthält der Algorithmus, nach welchem der zweite Zeichensatz dem ersten Zeichensatz zugeordnet wird, als wesentlichen Bestandteil einen Zufallsgenerator, welcher bei der Anmeldung ein-

nes Benutzers jedem Zeichen des ersten Zeichensatzes ein Zeichen zuordnet, wobei einer dieser zweiten Zeichensätze einem ersten Zeichensatz zugeordnet wird. In der Praxis können also die Zeichen des ersten Zeichensatzes gemischt und als zweiter Zeichensatz dem ersten Zeichensatz zugeordnet werden. Es besteht also bezüglich Umfang und Art der verwendeten Zeichensätze eine grosse Freiheit. Allerdings müssen die Beziehungen eindeutig sein, d.h. jedes Zeichen darf nur einmal in einem Zeichensatz vorkommen.

[0010] Die erfindungsgemässe Einheit kann z.B. bei der Eingangskontrolle, bei Geldausgabeautomaten, zur Bedienung einer Einbruchmeldeanlage und ähnlichen Anwendungen Verwendung finden.

[0011] Die Erfindung wird nachfolgend unter Bezugnahme auf die Figuren anhand eines Anwendungsbeispiels näher im Detail beschrieben. Dabei sind in den Figuren für gleiche Teile jeweils gleiche Bezugsziffern verwendet. Es zeigt:

Fig. 1 schematisch eine Zentraleinheit mit Mikroprozessor und Speichereinheiten und daran angeschlossenen Terminals mit jeweils einer Anzeige und einer Tastatur;

Fig. 2 ein Ablaufschema.

[0012] In der Fig. 1 ist mit der Bezugsziffer 11 eine Zentraleinheit mit einem Mikroprozessor 13 und Datenspeicher 15 gezeigt. Die Zentraleinheit 11 ist mit einer Mehrzahl von Terminals 17 in Verbindung. Die Terminals 17 besitzen mindestens eine Anzeige 19 und eine Tastatur 21. Die Terminals 17 dienen der Anmeldung irgendeines Systembenutzers, welcher beispielsweise den physischen Zugang zu einer abgesperrten Zone oder eine Kommunikationsverbindung mit einem nicht näher beschriebenen Zentralsystem erlangen möchte.

[0013] Gemäss einer bevorzugten Ausführungsform der Erfindung steht die Zentraleinheit 11 zusätzlich in Verbindung mit einem Codegenerator 23. Der Codegenerator 23 kann beispielsweise ein Zufallsgenerator sein, welcher die Reihenfolge von Zahlen in zufälliger Weise festlegt. Denkbar ist jedoch auch, anstelle eines Zufallsgenerators einen Rechner zu verwenden, welcher die Reihenfolge der Zahlen nach einem bestimmten Schema ändert.

[0014] Die Zentraleinheit 11 sorgt nun dafür, dass auf der Anzeige 19 eines Terminals die Zeichen eines ersten Zeichensatzes in einer bestimmten Ordnung, beispielsweise auf- oder absteigend, und die Zeichen eines zweiten Zeichensatzes in einer zufälligen Reihenfolge, wie sie durch den Codegenerator erzeugt wurde, angezeigt wird. Dabei umfassen der erste und zweite Zeichensatz die gleichen Zeichen. Der erste und der zweite Zeichensatz sind vorzugsweise tabellenförmig angeordnet, sodass jeweils ein Zeichen des ersten Zeichensatzes einem Zeichen des zweiten Zeichensatzes eindeutig zugeordnet ist und umgekehrt. Die tabellenförmige Darstellung hat den Vorteil, dass die Zuordnung gut erkennbar ist.

Beispiel:

[0015]

0	1	2	3	4	5	6	7	8	9
5	3	0	7	6	1	2	8	4	9

[0016] Besitzt ein Zutrittsberechtigter beispielsweise den wahren Zutrittscode 1234, so muss er gemäss obigem Beispiel bei der Anmeldung die Zahlen 3076 (temporärer Zutrittscode) eingeben.

[0017] Denkbar ist nun, dass die Zentraleinheit, beispielsweise in Gestalt eines Computers, in bestimmten Abständen oder als Folge von bestimmten Ereignissen jeweils neue Zuordnungen von erster und zweiter Zahlenreihe macht, sodass bei jeder erneuten Anmeldung ein anderer Code eingegeben werden muss.

[0018] Es ist denkbar, dass zusätzlich zur Eingabe des richtigen Zutrittscodes auch zusätzliche Erfordernisse für die Gewährung des Zutritts zum abgesicherten System (Gelände, Kommunikationsnetzwerk etc.) erfüllt sein müssen. Bei einer Anwendung bei Geldausgabeautomaten würde der Benutzer vorgängig oder einfach zusätzlich mittels einer persönlichen Identifikationskarte identifiziert. Auf dieser Identifikationskarte können bestimmte zusätzliche Informationen gespeichert sein, welche auf ihre Plausibilität überprüft werden. Nur wenn die persönliche Identifikationskarte vorhanden ist, und der Zutrittscode richtig eingegeben wird, erhält die Person Zugang zum System.

Patentansprüche

1. Verfahren zur Gewährung eines Zutritts zu einem passwortgeschützten System, beispielsweise Zugang zu einem Gelände oder einem Computernetzwerk, bei welchem Verfahren an einem mit einer Zentraleinheit (11) verbundenen Terminal (17), welcher mit einer Tastatur (21) und einer Anzeige (19) ausgestattet ist, ein Zutrittscode eingegeben werden muss, welcher Zutrittscode mit einem in der Zentraleinheit (11) abgespeicherten Code verglichen wird und der Zutritt des Benutzers zum passwortgeschützten System nur dann gewährt wird, wenn der eingegebene Zutrittscode mit dem in der Zentraleinheit (11) gespeicherten Code übereinstimmt, dadurch gekennzeichnet, dass
– der Zutrittscode verschleiert wird, indem die Zentraleinheit (11) zwei Zeichensätze auf der Anzeige darstellt,

CH 698 585 B1

- wobei der erste Zeichensatz die Zeichen des gespeicherten Zutrittscodes mindestens als Teilmenge enthält,
 - jedem Zeichen des ersten Zeichensatzes jeweils ein Zeichen des zweiten Zeichensatzes zugeordnet ist und mindestens nach jeder erneuten Anmeldung eine neue, wechselnde Zuordnung des zweiten Zeichensatzes zum ersten Zeichensatz hergestellt wird; und
 - als Zutrittscode jeweils jene Zeichen des zweiten Zeichensatzes gelten, welche dem im ersten Zeichensatz enthaltenen Zutrittscode zugeordnet sind.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass der erste Zeichensatz in einer bestimmten Ordnung auf der Anzeige angezeigt wird.
 3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass die Zahl der im ersten Zeichensatz enthaltenen Zeichen umfangreicher ist als der eigentliche Zutrittscode.
 4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass der Zutrittscode und die Zeichensätze aus alphanumerischen Zeichen bestehen.
 5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass der Zutrittscode und die Zeichensätze aus Zahlen bestehen.
 6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass der erste Zeichensatz aus den Zahlen 0,1, 2,.. .bis 9 besteht.
 7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, dass der erste Zeichensatz in einer bestimmten Reihenfolge, beispielsweise auf- oder absteigend, in alphabetischer Reihenfolge, dargestellt ist.
 8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass die Zeichen des ersten Zeichensatzes zufällig gemischt und dann als zweiter Zeichensatz dem ersten Zeichensatz zugeordnet werden.
 9. Verfahren nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, dass die Reihenfolge des zweiten Zeichensatzes in bestimmten Zeitabständen oder als Reaktion auf ein Ereignis ändert.
 10. Verfahren nach einem der Ansprüche 1 bis 9, dadurch gekennzeichnet, dass zusätzlich weitere Daten auf ihr Vorhandensein resp. ihre Richtigkeit geprüft werden.
 11. Verfahren nach Anspruch 10, dadurch gekennzeichnet, dass das Vorhandensein resp. die Richtigkeit der weiteren Daten für die Zutrittsgewährung gegeben sein muss.
 12. Passwortgeschützte Zutrittskontrolleinheit mit
 - einer Zentraleinheit (11) mit einem Mikroprozessor (13) und einem Datenspeicher, in welchem u.a. die Zutrittscodes von zugriffsberechtigten Personen abgespeichert sind, und
 - mindestens einem mit der Zentraleinheit (11) verbundenen Terminal (17) mit einer Anzeige (19) und einer Tastatur (21),dadurch gekennzeichnet,
 - dass die Zentraleinheit (11) einem ersten Zeichensatz, welcher die Zeichen des Zutrittscodes mindestens als Teilmenge enthält, nach einem bestimmten Algorithmus einen zweiten Zeichensatz zuordnet, wobei jedem Zeichen des ersten Zeichensatzes jeweils ein Zeichen des zweiten Zeichensatzes zugeordnet ist und mindestens nach jeder erneuten Anmeldung einer Person eine neue, wechselnde Zuordnung des zweiten Zeichensatzes zum ersten Zeichensatz hergestellt wird, und den ersten und zweiten Zeichensatz auf der Anzeige (19) anzeigt, und
 - dass als temporärer Zutrittscode jeweils jene Zeichen des zweiten Zeichensatzes gelten, welche den im ersten Zeichensatz enthaltenen wahren Zutrittscode zugeordnet sind.
 13. Einheit nach Anspruch 12, dadurch gekennzeichnet, dass der Algorithmus, nach welchem der zweite Zeichensatz dem ersten Zeichensatz zugeordnet wird, als wesentlichen Bestandteil eine Tabelle mit einer Mehrzahl von zweiten Zeichensätzen enthält, wobei bei der Anmeldung eines Benutzers einer dieser zweiten Zeichensätze einem ersten Zeichensatz zugeordnet wird.
 14. Einheit nach Anspruch 12, dadurch gekennzeichnet, dass der Algorithmus, nach welchem der zweite Zeichensatz dem ersten Zeichensatz zugeordnet wird, als wesentlichen Bestandteil einen Zufallsgenerator enthält, welcher bei der Anmeldung eines Benutzers jedem Zeichen des ersten Zeichensatzes ein Zeichen zuordnet, wobei einer dieser zweiten Zeichensätze einem ersten Zeichensatz zugeordnet wird.
 15. Einheit nach einem der Ansprüche 12 bis 14, dadurch gekennzeichnet, dass eine Mehrzahl von Terminals (17) mit der Zentraleinheit (11) verbunden sind.
 16. Einheit nach einem der Ansprüche 12 bis 15, dadurch gekennzeichnet, dass am Terminal (17) ein Lesegerät vorhanden ist.

Fig. 1

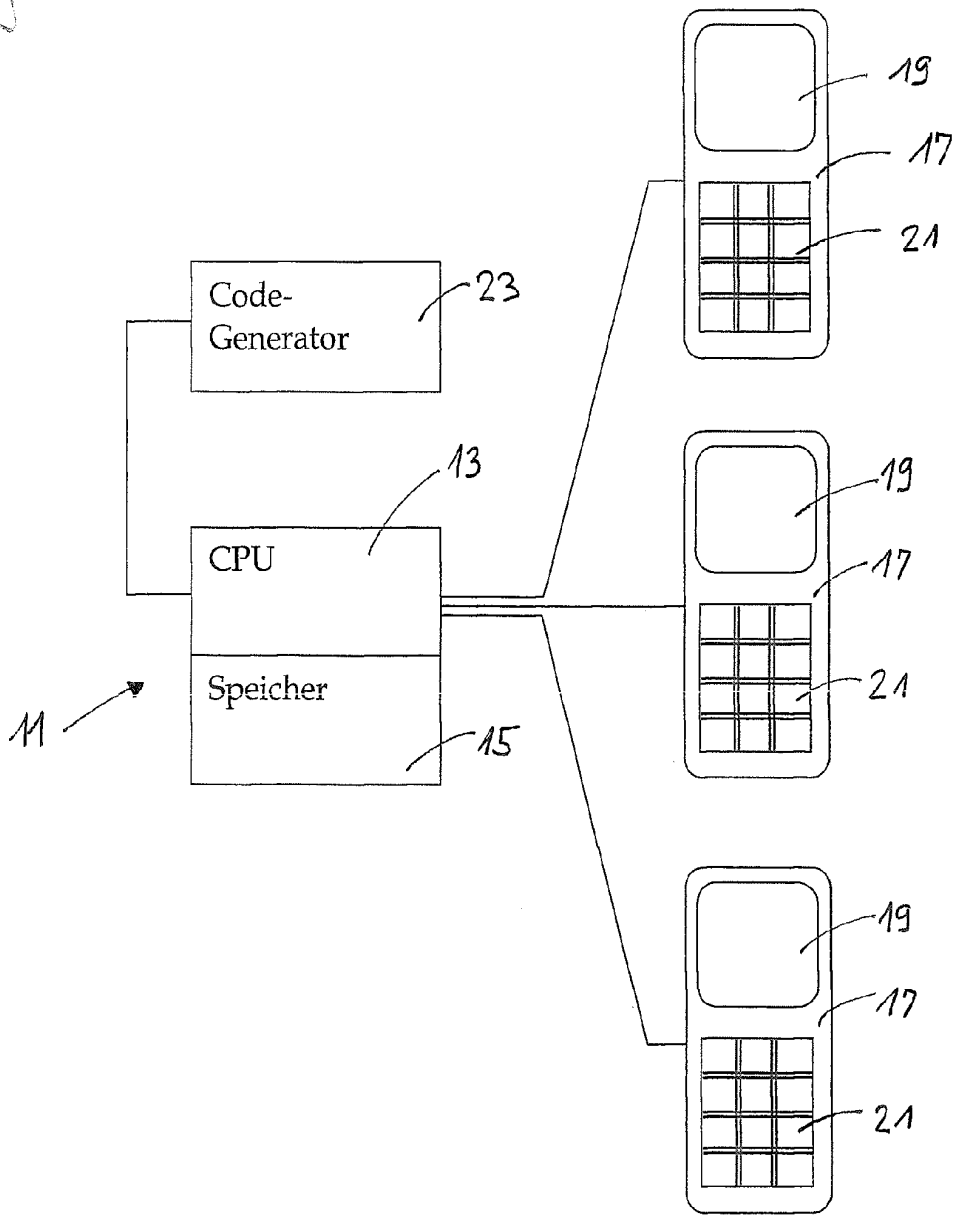


Fig 2

