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

(11) Veröffentlichungsnummer: **0 155 054**
**A2**

# (12) EUROPÄISCHE PATENTANMELDUNG

(21) Anmeldenummer: **85200324.3**

(22) Anmeldetag: **06.03.85**

(51) Int. Cl.⁴: **G 07 C 9/00**

(30) Priorität: **10.03.84 DE 3408904**

(43) Veröffentlichungstag der Anmeldung: **18.09.85**
**Patentblatt 85/38**

(84) Benannte Vertragsstaaten: **DE FR GB SE**

(71) Anmelder: **Philips Kommunikations Industrie AG,**
**Thurn-und-Taxis-Strasse 10, D-8500 Nürnberg 10 (DE)**
(84) Benannte Vertragsstaaten: **DE**

(71) Anmelder: **N.V. Philips' Gloeilampenfabrieken,**
**Groenewoudseweg 1, NL-5621 BA Eindhoven (NL)**
(84) Benannte Vertragsstaaten: **FR GB SE**

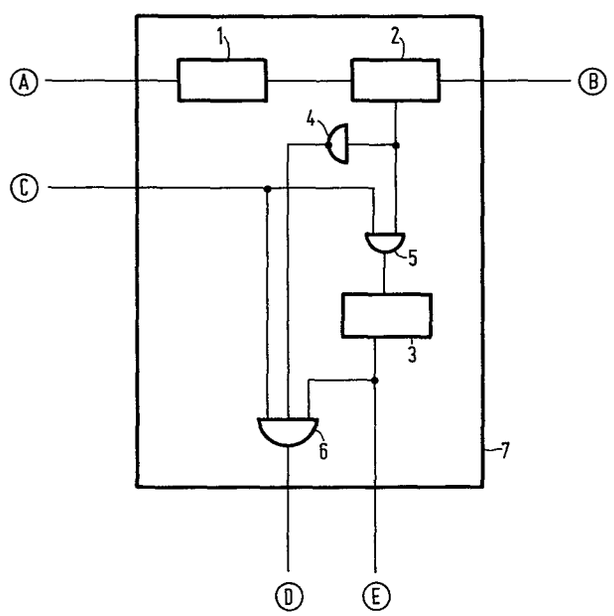
(72) Erfinder: **Logemann, Helmut, Kölner Strasse 12,**
**D-6100 Darmstadt (DE)**

(74) Vertreter: **Peuckert, Hermann et al, Philips**
**Patentverwaltung GmbH**
**Billstrasse 80 Postfach 10 51 49,**
**D-2000 Hamburg 28 (DE)**

## (54) Schaltungsanordnung zur Abwehr des unberechtigten Zugangs zu einem durch teilnehmerindividuelle Passworte gesicherten Kommunikationssystem.

(57) Bei einem durch teilnehmerindividuelle Passworte gesicherten Kommunikationssystem ist zur Abwehr des unberechtigten Zugangs häufig ein die möglichen Passworte enthaltender Speicher (1) und ein die jeweils empfangenen Passworte mit dem Speicherinhalt vergleichender Vergleicher (2) vorgesehen.

Zur Erhöhung der Sicherheit ist erfindungsgemäss zusätzlich eine am Ausgang des Vergleichers (2) über ein Eingangsgatter (5) angeschaltete monostabile Verzögerungsschaltung (3) mit nachgeschalteter Ausgangsverknüpfung (6) vorgesehen. Diese werden in Abhängigkeit vom Vorhandensein eines an einem besonderen Eingang (C) stehenden Aktivierungssignals derart vorbereitet, dass bei Nichtübereinstimmung des empfangenen mit dem gespeicherten Passwort die monostabile Verzögerungsschaltung (3) startet und während ihres Ablaufs die Ausgangsverknüpfung (6) sperrt, während bei Übereinstimmung die Ausgangsverknüpfung (6) öffnet.




EP 0 155 054 A2

0155054

Philips Kommunikations Industrie AG
N.V. Philips' Gloeilampenfabrieken

PHD 84381 EP
20.02.1985

# Schaltungsanordnung zur Abwehr des unberechtigten Zugangs zu einem durch teilnehmerindividuelle Paßworte gesicherten Kommunikationssystem

Die Erfindung betrifft eine Schaltungsanordnung zur Abwehr des unberechtigten Zugangs zu einem durch teilnehmerindividuelle Paßworte gesicherten Kommunikationssystem. Derartige Paßworte werden zur Legitimation eines Zugangsberechtigten zu einem gegen fremden Zugriff geschützten Kommunikationssystem den Zugangsberechtigten zusätzlich zu einer offenen Identifikation zugeordnet. Diese Paßworte dürfen nur dem jeweils Zugangsberechtigten und der über den Zugang zu befindenden Stelle bekannt sein. Vor der Freigabe eine Zuganges wird die Übereinstimmung dieser Zuordnung überprüft.

In der Regel sind die Zuordnungen der geheimen Paßworte aller Zugangsberechtigten in einer Datei der über den Zugang zu entscheidenden Stelle (n) gespeichert. Nach Erhalt einer Identifikation erwartet die entscheidende Stelle ein Paßwort, das mit dem aus ihrer Datei als zugeordnet abgefragten Paßwort übereinstimmt. Im Falle der Übereinstimmung der Paßworte gilt der Zugang Begehrende als zugangsberechtigt und identifiziert.

Die Sicherheit eines solchen Systems hängt wesentlich davon ab, wie sicher der Inhalt des Paßwortspeichers gegen unbefugtes Auslesen oder Verändern geschützt werden kann. Die Gefahr des unbefugten Auslesens ist mit der sprunghaft angestiegenen Anwendung von Heimcomputern und einer entsprechenden Verbreitung des entsprechenden Computerwissens in einem nicht mehr übersehbaren Teilnehmerkreis erheblich gewachsen. Erfolgreiche Versuche, durch rech-

nergeschütztes systematisches oder auch zufallsbedingtes Ausprobieren an geheime Paßworte zu gelangen, häufen sich.

Hier setzt die Erfindung ein. Es ist die Aufgabe der Erfindung, einem potentiellen Manipulanten, der sich mit einer Serie von mutmaßlichen Paßworten den Zugang zu einer gesicherten Information, z.B. einer Datenbank, einem Mobilfunknetz, einem Rechnerverbund zu erschleichen sucht, durch entsprechende Schaltungsmaßnahmen abzuwehren.

Diese Aufgabe wird durch die im Patentanspruch 1 angegebene Schaltungsanordnung gelöst.

Da die gesamte Schaltungsanordnung durch die Fortschritte der modernen Halbleiterspeichertechnik in ihrem Raumbedarf kaum ins Gewicht fällt, wird in weiterer Ausbildung der Erfindung ihre vielfache Anwendung vor jeder Freiwahlstufe eines Vermittlungssystems oder jedem belegbaren Kanal eine Mobilfunksystems vorgesehen. Damit sind einer beabsichtigten Blockierung eines Systems enge Grenzen gesetzt.

Zur Erhöhung der Sicherheit sind alle Elemente der Schaltungsanordnung zugriffsicher auf einem Träger aufgebracht und mit einer unlösbaren Umhüllung umgeben. Direkter gegenständlicher Zugriff zum Speicher setzt die Zerstörung der Speicheranordnung voraus. Elektrischer Zugriff verlängert im Falle der Nichtübereinstimmung einer Paßwortzuordnung die Zugriffszeit für die nächste Speicherabfrage um den Faktor $1 \times 10^8$. Ein 16-Bit-Paßwort kann theoretisch bis zu $2^{16}$ gleich 65 536 Zuordnungsversuche mit verlängerter Zugriffszeit erfordern, um eine einzige Zu-

ordnung zu ermitteln.

Die Sperrfrist nach einer Nichtübereinstimmung betrage im vorgegebenen Beispiel 1 x $10^8$ multipliziert mit einer Speicher-(regel-) zugriffszeit von 500 ns gleich 50s. Bei 65 536 möglichen Versuchen ergäbe dies eine Zeit von 65 536 mal 50 s gleich 910 Stunden oder 38 Tagen für die Ermittlung einer einzigen gültigen Zuordnung. Ein mittlerer Zeitbedarf von 10 bis 14 Tagen dürfte als realistisch für das Auffinden einer gültigen Zuordnung anzunehmen sein.

Die Figur zeigt die erfindungsgemäße Schaltungsanordnung. Im Speicher 1 sind die den offenen Identifikationen (Speicheradressen) am Eingang A zugeordneten geheimen Paßworte abgespeichert. Der Vergleicher 2 prüft die Übereinstimmung eines am Eingang B anstehenden äußeren Paßwortes mit dem aus dem Speicher 1 nach der offenen Identifikation am Eingang A zugeordneten geheimen Paßwort. Im Falle der Übereinstimmung liefert der Vergleicher 2 den Logikpegel low an das nachfolgende Gatter 5 und die Negation 4. Im Fehlerfalle liefert der Vergleicher 2 den Logikpegel high. Die Funktionen haben vorbereitenden Einfluß auf die monostabile Verzögerungsschaltung 3 und gemeinsam mit dieser auf die Ausgangsverknüpfung 6. Die monostabile Verzögerungsschaltung 3 liefert im Ruhezustand am Ausgang E und vorbereitend an der Ausgangsverknüpfung 6 den Logikpegel high. Der Ausgang D führt den Logikpegel low (Negativaussage). Mit dem Logikpegel high am Eingang C wird die Anordnung aktiviert.

Es sind folgende Fälle möglich:

Die Anordnung befindet sich im Ruhezustand und der Vergleicher 2 erkennt Übereinstimmung. Während des Logikpegels high am Eingang C führt der Ausgang D den Logikpegel high (Positivaussage). Die monostabile Verzögerungsschaltung 3 bleibt im Ruhezustand, damit führt deren Ausgang E den Logikpegel high (normaler Zugriff).

Die Anordnung befindet sich im Ruhezustand und der Vergleicher 2 erkennt Nichtübereinstimmung (Fehler). Mit dem Logikpegel high am Eingang C wird über das Gatter 5 die monostabile Verzögerungsschaltung 3 aktiviert. Der Ausgang E nimmt den Logikpegel low an und hält diesen bis zum Ablauf der Verzögerungsschaltung 3 (verzögerter Zugriff). Der Ausgang D bleibt während des Logikpegels high am Eingang C in Ruhelage, d.h. auf dem Logikpegel low (Negativaussage).

Die Anordnung befindet sich im Zustand "monostabile Verzögerungsschaltung läuft", der Vergleicher 2 erkennt Übereinstimmung. Ein Logikpegel high am Eingang C bleibt ohne Wirkung auf die Negativaussage low am Ausgang D. Der Ausgang E führt den Logikpegel low (verzögerter Zugriff).

Die Anordnung befindet sich im Zustand "monostabile Verzögerungsschaltung läuft", der Vergleicher 2 erkennt Nichtübereinstimmung. Ein Logikpegel high am Eingang C bleibt ohne Wirkung auf die Negativaussage low am Ausgang D und setzt ggf. die monostabile Verzögerungsschaltung 3 an den Anfang zurück (Nachtriggerung). Der Ausgang E führt den Logikpegel low (verzögerter Zugriff).

Die erfindungsgemäße Anordnung gewährt Schutz gegen das experimentelle Ermitteln geheimer Paßwortzuordnungen durch das Erschweren des elektrischen Zugriffs über die

Verlängerung der Zugriffszeit im Fehlerfalle.

Die gesamte Anordnung ist gegenständlich zugriffssicher auf einem Träger 7 aufgebracht und mit einer unlösbaren Umhüllung umgeben. Mechanische Manipulantionen setzen die Zerstörung der Anordnung voraus. Damit gewährt die Erfindung auch Schutz gegen direkten Zugriff zum Speicher 1.

Philips Kommunikations Industrie AG
N.V. Philips' Gloeilampenfabrieken



Patentansprüche

1. Schaltungsanordnung zur Abwehr des unberechtigten Zugangs zu einem durch teilnehmerindividuelle Paßworte gesicherten Kommunikationssystem, bestehend aus einem die möglichen Paßworte enthaltenden Speicher (1) und einem die jeweils empfangenen Paßworte mit dem Speicherinhalt vergleichenden Vergleicher (2), welcher im Falle der Übereinstimmung von empfangenen und gespeicherten Paßwort dem rufenden Teilnehmer den Zugang freigibt, gekennzeichnet durch eine am Ausgang des Vergleichers (2) über ein Eingangsgatter (5) angeschaltete monostabile Verzögerungsschaltung (3) mit nachgeschalteter Ausgangsverknüpfung (6), welche in Abhängigkeit vom Vorhandensein eines an einem besonderen Eingang (C) anstehenden Aktivierungssignals derart vorbereitet werden, daß bei Nichtübereinstimmung des empfangenen mit dem gespeicherten Paßwort die monostabile Verzögerungsschaltung (3) startet und während ihres Ablaufs die Ausgangsverknüpfung (6) sperrt, während bei Übereinstimmung die Ausgangsverknüpfung (6) öffnet.

2. Schaltungsanordnung nach Anspruch 1, dadurch gekennzeichnet, daß der Betriebszustand "monostabile Verzögerungsschaltung läuft" an einem besonderen Ausgang (E) erkennbar ist.

3. Schaltungsanordnung nach Anspruch 1 und 2, dadurch gekennzeichnet, daß alle Elemente der Schaltungsanordnung zugriffsicher auf einem Träger (7) aufgebracht und mit einer unlösbaren Umhüllung umgeben sind.

4. Schaltungsanordnung nach Anspruch 1, gekennzeichnet durch ihre vielfache Anwendung vor jeder Freiwahlstufe eines Vermittlungssystems oder jedem belegbaren Kanal eine Mobilfunksystems.

0155054