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

(11) EP 0 813 170 A2

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
17.12.1997 Patentblatt 1997/51

(51) Int. Cl.[6]: **G07C 9/00**

(21) Anmeldenummer: **97108942.0**

(22) Anmeldetag: **03.06.1997**

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

(30) Priorität: **03.06.1996 DE 19622255**

(71) Anmelder:
- **Eckel, Werner, Dipl.-Ing.**
  19348 Grenzheim (DE)
- **Kresimir, Neckov**
  22415 Hamburg (DE)

(72) Erfinder:
- **Eckel, Werner, Dipl.-Ing.**
  19348 Grenzheim (DE)
- **Kresimir, Neckov**
  22415 Hamburg (DE)

(74) Vertreter:
Grünecker, Kinkeldey,
Stockmair & Schwanhäusser
Anwaltssozietät
Maximilianstrasse 58
80538 München (DE)

(54) Elektronisches Zugangsberechtigungssystem und Verfahren zum Feststellen eines berechtigten Zugangs

(57) Es wird ein elektronisches Zugangsberechtigungssystem und ein Verfahren zum Feststellen eines berechtigten Zugangs zu einem System angegeben. Das Zugangsberechtigungssystem weist einen Schlüssel und ein Schloß auf und vergleicht einen vom Schlüssel zum Schloß übertragenden Code. Wenn die Codes übereinstimmen, wird der Zugang zum System freigegeben. Erfindungsgemäß sind im Speicher des Schlüssels eine Vielzahl von verschiedenen Codes und im Speicher des Schlosses eine entsprechende Vielzahl von dazu passenden Codes abgelegt. Eine Steuereinrichtung zur Steuerung des Systems ist so ausgebildet, daß im Betrieb jeder im Schloß gespeicherte Code nur einmal mit einem vom Schlüssel übertragenen Code verglichen wird.

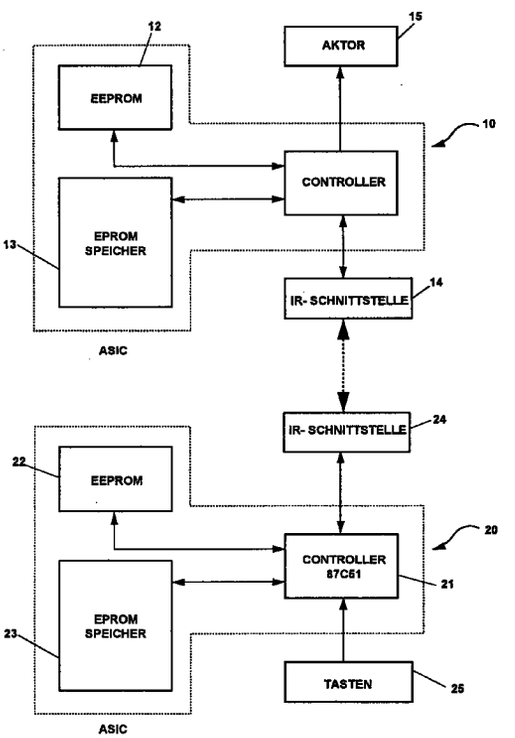

Fig. 1

EP 0 813 170 A2

Beschreibung

Die vorliegende Erfindung bezieht sich auf ein elektronisches Zugangsberechtigungssystem gemäß dem Oberbegriff des Patentanspruchs 1.

Weiterhin bezieht sich die vorliegende Erfindung auf ein Verfahren zum Feststellen eines berechtigten Zugangs zu einem System.

Elektronische Zugangsberechtigungssysteme sind heutzutage weit verbreitet. Unter einem Zugangsberechtigungssystem soll hier und im folgenden ein System verstanden werden, welches den Zugang nur bestimmter berechtigter Personen zum System ermöglicht. Typische Anwendungsfälle sind beispielsweise Computernetze, die einem zugangsberechtigten Benutzer Dienste oder Informationen anbieten. Ein weiterer Anwendungsfall ist ein elektronisches Schloß mit einem oder mehreren dazu gehörigen, in einem Handsender eingebauten elektronischen Schlüsseln. Das Schloß ist in einer Tür, beispielsweise eines Gebäudes oder eines Kfz eingebaut und öffnet sich nur im Ansprechen auf einen bestimmten vom Handsender übertragenen Code. Die Übertragung des Codes kann mit optischen, elektromagnetischen oder Schallsignalen erfolgen.

Die oben erwähnten Anwendungen sollen lediglich Beispiele für Zugangsberechtigungssysteme sein und es ist darauf hinzuweisen, daß die vorliegende Erfindung nicht auf die genannten Beispiele beschränkt ist.

Bei herkömmlichen Zugangsberechtigungssystemen erhält der Benutzer einer spezifischen persönlichen Code, der von dem System dazu verwendet wird, den Benutzer zu identifizieren.

Weiterhin ist es bekannt, Algorithmen zu benutzen, um aus dem spezifischen Code weitere Codes zu errechnen.

Die Problematik bei den bekannten Zugangsberechtigungssystemen liegt darin, daß sie keine ausreichende Sicherheit gegen Manipulationsversuche bieten. Sowohl der spezifische Code als auch die berechneten Codes können bei Beobachtung eines berechtigten Zugangs von einem Spezialisten, evtl. mit Computerhilfe geknackt werden. Es ist dann möglich, eine Kopie des Schlüssels anzufertigen und unberechtigen Zugang zum System zu erhalten.

Aufgabe der vorliegenden Erfindung ist es somit, bei einem elektronischen Zugangsberechtigungssystem und einem Verfahren zur Feststellung eines berechtigten Zugangs, die Sicherheit gegenüber Manipulationsversuche zu erhöhen.

Diese Aufgabe wird erfindungsgemäß von einem elektronischen Zugangsberechtigungssystem mit den Merkmalen des Patentanspruchs 1 sowie von einem Verfahren mit den Merkmalen des Patentanspruchs 10 gelöst.

Der entscheidende neue Gedanke beim erfindungsgemäßen elektronischen Zugangsberechtigungssystem besteht darin, daß nicht nur ein spezifischer Code, sondern eine Vielzahl von im Voraus abgespeicherten verschiedener Codes zur Feststellung der Zugangsberechtigung verwendet werden, wobei die Codes von Schlüssel und Schloß zueinander passen und jeder Code nur einmal verwendet wird. Dadurch wird bei jedem versuchten Zugang zum System ein anderer Code verwendet, wodurch selbst die Beobachtung eines erfolgreichen Zugangs zum System nicht auf den Code schließen läßt, der als nächstes verwendet wird. Ein derartiges Zugangsberechtigungssystem ist praktisch gegen jegliche Manipulation geschützt.

Bevorzugte Ausführungsbeispiele der Erfindung werden nunmehr unter Bezugnahme auf die begleitenden Figuren beschrieben. Es zeigen:

Fig. 1 den Aufbau der Hardware eines elektronischen Schlosses und eines dazu gehörigen elektronischen Schlüssels, und

Fig. 2 ein Ablaufdiagramm der Operationen im Schlüssel und Schloß zum Feststellen eines berechtigten Zugangs.

Bezugnehmend auf Fig. 1, bezeichnet das Bezugszeichen 10 allgemein ein elektronisches Schloß und das Bezugszeichen 20 einen dazugehörigen Schlüssel, wobei aus Gründen der Übersichtlichkeit der Darstellung nur ein Schlüssel gezeigt ist. Es ist für den Fachmann klar, daß bei einem Zugangsberechtigungssystem der in Rede stehenden Art ein Schloß und eine beliebige Anzahl von Schlüsseln vorgesehen sein können, wobei jeder Schlüssel alleine das Schloß öffnen kann. Alternativ dazu kann ein Schloß nur bei Anwesenheit mehrerer verschiedener Schlüssel zu öffnen sein. Weitere Kombinationen dieser Alternativen sind dem Fachmann bekannt.

Das elektronische Schloß 10 und jeder Schlüssel 20 weisen zur Steuerung ihrer Betriebsfunktionen einen 8-Bit-Controller 11, 21 auf, der beispielsweise vom Typ 87C51 ist. Das Steuerprogramm für den Controller ist in einem internen Speicher des Controllers abgelegt. In einem nicht-flüchtigen EEPROM-Speicher 12 des Schlosses ist eine Codeadresse abgelegt, was weiter unten ausführlich erläutert werden wird. Darüber hinaus ist in dem internen Speicher des Controllers eine Identifikationsadresse einer Länge von beispielsweise 32 Bit abgelegt, die eine eindeutige Identifikation von Schloß und Schlüssel erlauben.

Schloß und Schlüssel besitzen jeweils einen EPROM-Speicher 13, 23, in denen eine Vielzahl von verschiedenen Codes gespeichert sind, die eine Zufallsfolge darstellen. Das besondere an der Anordnung ist, daß der Inhalt der EPROM-Speicher, d.h. die Vielzahl der Codes bei zueinandergehörigem Schloß und Schlüssel zueinander passen, beispielsweise identisch sind. Die Speicherkapazität der EPROM-Speicher 13, 23 ist variabel in Abhängigkeit von der Anzahl der zu erwartenden Zugangsversuche. Eine typische Größenordnung für diesen Speicher liegt zwischen 1 MBit und 8 MBit.

Für Schloß und jeden Schlüssel sind der Controller

und die Speicher in einem ASIC, einer anwenderspezifischen Schaltung, integriert. Ein ASIC ist in der Massenproduktion wirtschaftlich fertigbar und bei Ergreifen geeigneter Maßnahmen gegen ein Auslesen der Speicherinhalte gesichert.

Schlüssel und Schloß besitzen eine Schnittstelle 14, 24 für eine geeignete Kommunikation, z.B. Infrarotlichtübertragung. Der Aufbau solcher Schnittstellen ist dem Fachmann geläufig und wird daher nicht detailliert beschrieben.

Weiter besitzt der Controller 21 des Schlüssels eine geeignete Schnittstelle für die händische Eingabe von Steuersignalen beispielsweise über eine Tastatur 25. Der Controller 11 des Schlosses 10 steuert einen Aktor 15, beispielsweise ein elektrisches Relais, welches den Zugang zu einem System ermöglicht.

Im folgenden wird der Aufbau eines beispielhaften EPROM-Speichers beschrieben.

In diesem Speicher sind abwechselnd Schloßcode und Schlüsselcode mit einer Länge von 24 Bit (3 Byte) gespeichert. Jeder Code ist eine Zufallsfolge, die beispielsweise durch Unterabtastung einer weißen thermischen Rauschquelle erzeugt worden ist. Der Speicher in dem hier beschriebenen Beispiel ist so aufgebaut, daß an jeder Adresse ein Datenbyte gespeichert ist. Daher stehen beispielsweise an den ersten drei Adressen des Speichers die 24 Bit des ersten Schloßcodes an den Adressen 4 bis 6 die 24 Bit des ersten Schlüsselcodes, an den Adressen 7 bis 9 die 24 Bit des zweiten Schloßcodes etc.. Für jeden Zugangsberechtigungsvorgang werden ein Schloßcode und ein Schlüsselcode zusammen also 48 Bit benötigt. Somit erlaubt ein EPROM mit einem Speichervermögen von 8 MBit das Durchführen von mehr als 150.000 Zugangsberechtigungsvorgängen.

Im folgenden werden ein Zugangsberechtigungsvorgang unter Bezugnahme auf die Fig. 1 und 2 detailliert beschrieben.

Das Schloß befindet sich zunächst im Wartezustand 100 und wartet auf eine Identifikation vom Schlüssel. Wenn der Bediener eine Betätigungstaste drückt (Schritt 200), sendet der Schlüssel seine gespeicherte Identifikation zum Schloß (Schritt 201). Wenn das Schloß eine Identifikation empfangen hat (Schritt 101), wird ein Vergleich zwischen der empfangenen und einer im Schloß gespeicherten Identifikation durchgeführt (Schritt 102). Bei Übereinstimmen der Identifikationen liest der Controller 11 die aktuelle Codeadresse aus dem EEPROM, aktualisiert die Codeadresse und schreibt sie in den EEPROM zurück.

Anschließend wird im Schritt 104 die gelesene Codeadresse und der dazugehörige 24-Bit-Schloßcode, welcher aus dem EPROM 13 ausgelesen wird, an den Schlüssel übertragen. Im Schlüssel findet ein Vergleich des empfangenen Codes mit demjenigen Code statt, der an der Codeadresse im EPROM-Speicher 23 des Schlüssels gespeichert ist (Schritt 202). Im Falle einer Übereinstimmung überträgt der Schlüssel den zum Schloßcode zugehörigen 24-Bit-Schlüsselcode im Schritt 203 an das Schloß. Das Schloß vergleicht den übertragenen Schlüsselcode mit seinem eigenen gespeicherten Schlüsselcode (Schritt 105) und gibt bei Übereinstimmung der Codes den Zugang zum System frei (Schritt 106). Dies kann beispielsweise die Erzeugung eines geeigneten Steuersignals für einen Aktor 15 auslösen.

Zusammenfassend ist festzustellen, daß nur bei Übereinstimmung der Identifikationen und der 24-Bit-Schloß- und Schlüsselcodes in den EPROM-Speichern von Schlüssel und Schloß eine Freigabe des Systems erfolgt. Da sich der ausgesandte Schloßcode und der vom Schlüssel als Antwortsignal erwartete Schlüsselcode nach jedem Vergleich ändern, ist das Zugangsberechtigungssystem immun gegenüber Manipulationen.

Für eine zusätzliche Erhöhung der Sicherheit kann eine Zähleinrichtung vorgesehen sein, die nach dem Empfang einer bestimmten Anzahl von falschen Codes eine temporäre oder dauerhafte Sperrung des Schlosses veranlaßt. Dann kann auch eine wiederholte Abfrage nach dem Zufallsprinzip bei diesem System nicht zum Erfolg führen.

Die Datenübertragung kann mit üblichen Kommunikationseinrichtungen erfolgen, beispielsweise mittels Infrarotsende- und Empfangsgeräten. Um eine zuverlässige Unterscheidung zwischen Manipulationsversuchen und einer fehlerhaften Datenübertragung zu erreichen, kann über eine Gruppe von jeweils 8 übertragenen Bits eine Checksumme gebildet werden, die mitübertragen wird. Nur wenn die Checksumme richtig ist, wird ein Datenempfang als ein Zugangsversuch gewertet. Anderenfalls wird ein beispielsweise unvollständig oder unrichtig übertragener Code als Empfang eines falschen Codes angesehen, was eine unnötige Sperrung des Schlosses zur Folge haben könnte. Es ist darauf hinzuweisen, daß bei der Erfindung das Übertragungsprotokoll und die Art der Datenübertragung vom Fachmann frei wählbar ist.

Wenn das erfindungsgemäße Zugangsberechtigungssystem bei einem Computernetz zum Einsatz kommt, sind im Zentralcomputer und beim Benutzer Chipsätze vorgesehen. Hier wird die persönliche Identifikationsnummer durch die im voraus gespeicherten Codes ersetzt.

Patentansprüche

1. Elektronisches Zugangsberechtigungssystem mit einem Schlüssel (20) und einem Schloß (10), die jeweils einen Speicher (13, 23) für einen Code aufweisen, umfassend:

   Einrichtungen (14, 24) zum Übertragen des Codes zwischen Schlüssel (20) und Schloß (10),

   eine Einrichtung (11) zum Vergleichen des vom Schlüssel übertragenen Codes mit dem im Schloß gespeicherten Code, und

Einrichtungen (11, 21) zum Steuern der Übertragungs- und Vergleichseinrichtungen und zum Freigeben des Zugangs, wenn die zu vergleichenden Codes übereinstimmen, **dadurch gekennzeichnet,** daß

im Speicher (23) des Schlüssels (20) eine Vielzahl von verschiedenen Codes und im Speicher (13) des Schlosses (10) eine entsprechende Vielzahl von dazu passenden Codes abgelegt sind, und

daß die Steuereinrichtungen (11, 21) so ausgebildet sind, daß im Betrieb des Systems jeder im Schloß gespeicherte Code nur einmal von der Vergleichseinrichtung verwendet wird.

2. Elektronisches Zugangsberechtigungssystem nach Anspruch 1, **dadurch gekennzeichnet,** daß das Schloß (10) eine Einrichtung (14) zum Übertragen eines Code-Anforderungssignals und der Schlüssel (20) eine für den Empfang dieses Signals geeignete Empfangseinrichtung (24) aufweist und der Schlüssel im Ansprechen auf das Code-Anforderungssignal den Code überträgt.

3. Elektronisches Zugangsberechnungssystem nach Anspruch 2, **dadurch gekennzeichnet,** daß das Code-Anforderungssignal ein Adressignal umfaßt zur Adressierung eines der Vielzahl der im Schlüssel (20) gespeicherten Codes.

4. Elektronisches Zugangsberechtigungssystem nach Anspruch 2 oder 3, **dadurch gekennzeichnet,** daß das Code-Anforderungssignal zumindest einen weiteren Zusatzcode umfaßt, welcher zusätzlich im Speicher von Schloß und Schlüssel abgelegt ist, und

daß der Schlüssel (20) eine Vergleichseinrichtung aufweist zum Vergleichen des vom Schloß empfangenen Zusatzcodes mit dem in seinem Speicher gespeicherten Zusatzcode und der Schlüssel seinen Code nur bei übereinstimmenden Zusatzcodes überträgt.

5. Elektronisches Zugangsberechtigungssystem nach einem der Ansprüche 1 bis 4, **dadurch gekennzeichnet,** daß der Schlüssel (20) eine Einrichtung zum Erzeugen und Übertragen einer Identifikation an das Schloß aufweist und das Schloß eine Einrichtung zur Überprüfung der Identifikation umfaßt.

6. Elektronisches Zugangsberechtigungssystem nach einem der Ansprüche 1 bis 5, **dadurch gekennzeichnet,** daß die Speicher für die Ablage der Codes EPROM's (13, 23) sind.

7. Elektronisches Zugangsberechtigungssystem nach wenigstens Anspruch 3, **dadurch gekennzeichnet,** daß die Steuereinrichtung des Schlosses einen nicht-flüchtigen Speicher (12) umfaßt zum Lesen und Schreiben des Adressignals.

8. Elektronisches Zugangsberechtigungssystem nach einem der Ansprüche 1 bis 7, **dadurch gekennzeichnet,** daß die dem Schlüssel (20) zugeordneten Vergleichs-, Steuer- und Speichereinrichtungen in einem ASIC integriert sind.

9. Elektronisches Zugangsberechtigungssystem nach einem der Ansprüche 1 bis 8, **dadurch gekennzeichnet,** daß die dem Schloß (10) zugeordneten Vergleichs-, Steuer- und Speichereinrichtungen in einem ASIC integriert sind.

10. Verfahren zum Feststellen eines berechtigten Zugangs zu einem System mit einem Schlüssel (20) und einem Schloß (10), die jeweils einen Speicher (13, 23) für einen Code aufweisen mit folgenden Schritten:

Übertragen (203) des Codes zwischen Schlüssel und Schloß,

Vergleichen (105) des vom Schlüssel übertragenen Codes mit dem im Schloß gespeicherten Code, und

Feststellen des berechtigten Zugangs, wenn die zu vergleichenden Codes übereinstimmen, **dadurch gekennzeichnet,** daß im Speicher (23) des Schlüssels eine Vielzahl von verschiedenen Codes und im Speicher (13) des Schlosses eine entsprechende Vielzahl von dazu passenden Codes abgelegt sind, und

daß jeder im Schloß gespeicherte Code nur einmal mit einem von dem Schlüssel übertragenen Code verglichen wird.

11. Verfahren nach Anspruch 10, **dadurch gekennzeichnet,** daß das Schloß ein Code-Anforderungssignal zum Schlüssel überträgt und dieser im Ansprechen darauf seinen Code an das Schloß sendet.

12. Verfahren nach Anspruch 11, **dadurch gekennzeichnet,** daß das Code-Anforderungssignal ein Adressignal umfaßt zur Adressierung eines der Vielzahl von im Schlüssel gespeicherten Codes.

13. Verfahren nach Anspruch 11 oder 12, **dadurch gekennzeichnet**, daß das Code-Anforderungssignal zumindest einen Zusatzcode umfaßt, welcher zusätzlich im Speicher von Schloß und Schlüssel abgelegt ist, und daß der Schlüssel den Zusatzcode mit dem in seinem Speicher (23) gespeicher-

ten Zusatzcode vergleicht und seinen Code nur bei übereinstimmenden Zusatzcodes überträgt.

14. Verfahren nach einem der Ansprüche 10 bis 13, **dadurch gekennzeichnet,** daß der Schlüssel eine Identifikation an das Schloß überträgt und das Schloß vor dem Aussenden des Code-Anforderungssignals die Identifikation überprüft.

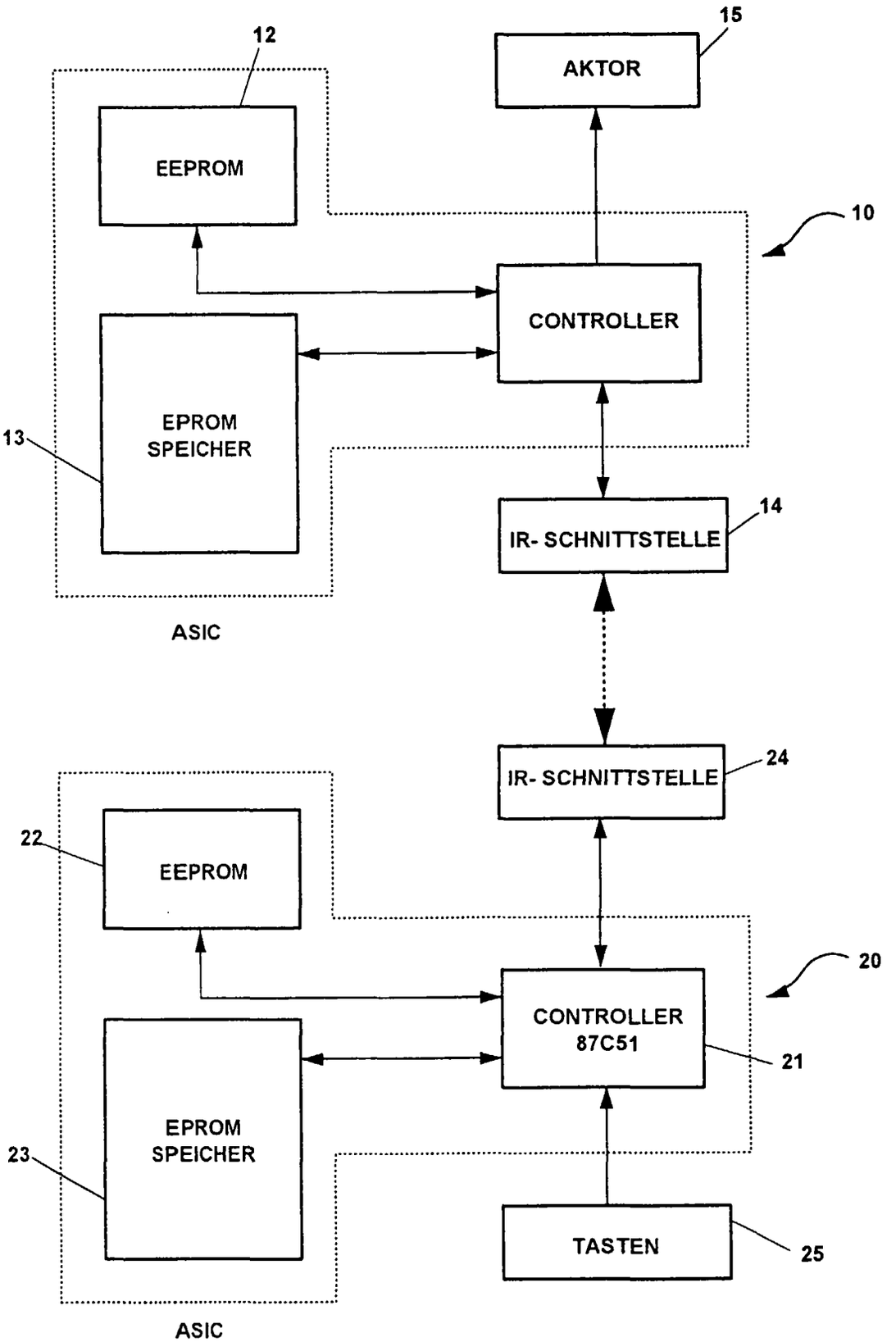
12
15
AKTOR
EEPROM
10
CONTROLLER
EPROM
SPEICHER
13
14
IR- SCHNITTSTELLE
ASIC
IR- SCHNITTSTELLE
24
22
EEPROM
20
CONTROLLER
87C51
21
EPROM
SPEICHER
23
TASTEN
25
ASIC

Fig. 1

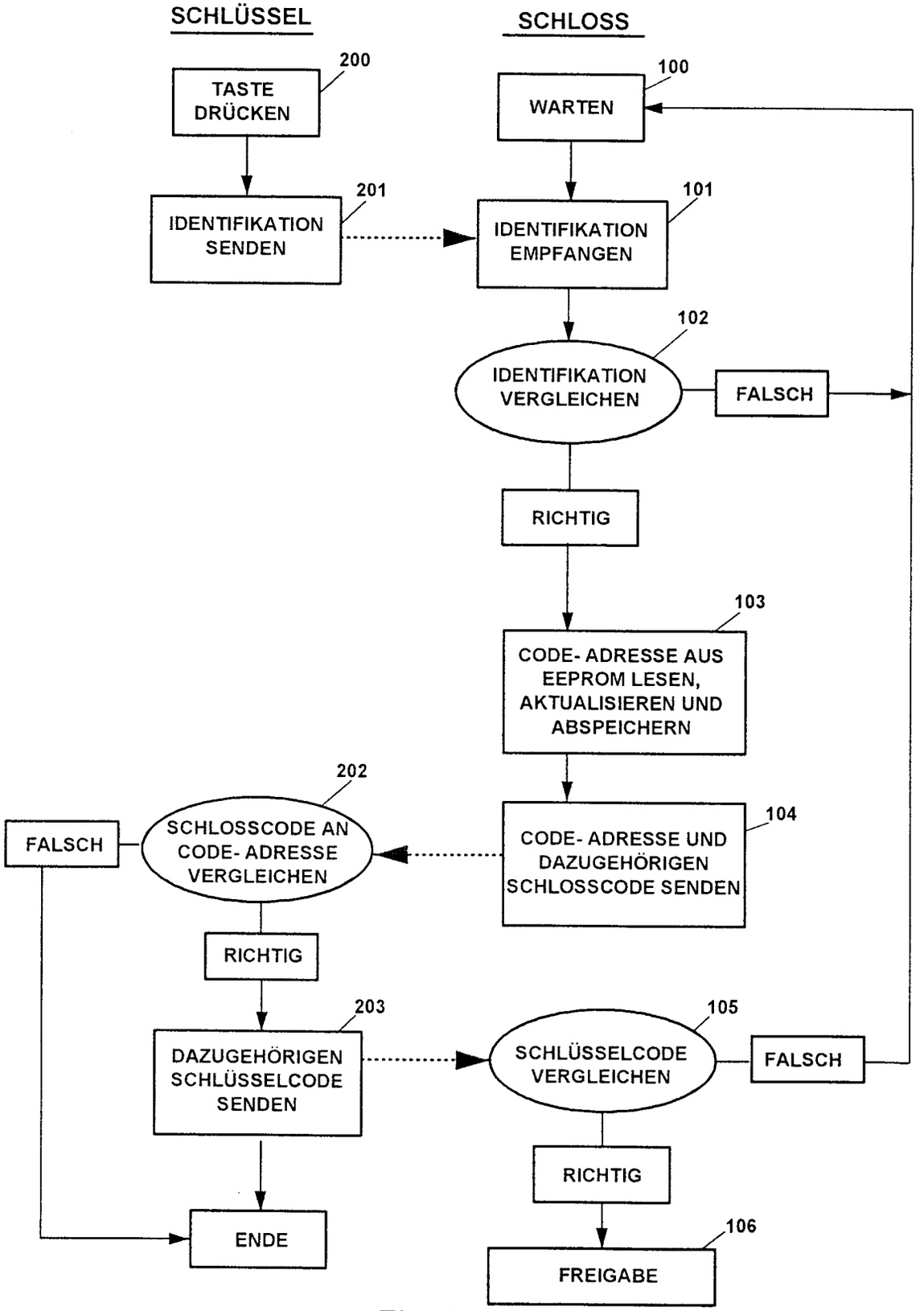
SCHLÜSSEL
SCHLOSS
TASTE DRÜCKEN
200
WARTEN
100
IDENTIFIKATION SENDEN
201
IDENTIFIKATION EMPFANGEN
101
IDENTIFIKATION VERGLEICHEN
102
FALSCH
RICHTIG
CODE- ADRESSE AUS EEPROM LESEN, AKTUALISIEREN UND ABSPEICHERN
103
CODE- ADRESSE UND DAZUGEHÖRIGEN SCHLOSSCODE SENDEN
104
SCHLOSSCODE AN CODE- ADRESSE VERGLEICHEN
202
FALSCH
RICHTIG
DAZUGEHÖRIGEN SCHLÜSSELCODE SENDEN
203
SCHLÜSSELCODE VERGLEICHEN
105
FALSCH
RICHTIG
ENDE
FREIGABE
106

Fig. 2