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

(10) **DE 102 33 122 A1** 2004.02.05

(12) # Offenlegungsschrift

(21) Aktenzeichen: **102 33 122.7**
(22) Anmeldetag: **20.07.2002**
(43) Offenlegungstag: **05.02.2004**

(51) Int Cl.[7]: **E05B 49/00**
E05B 65/12, E05B 65/36

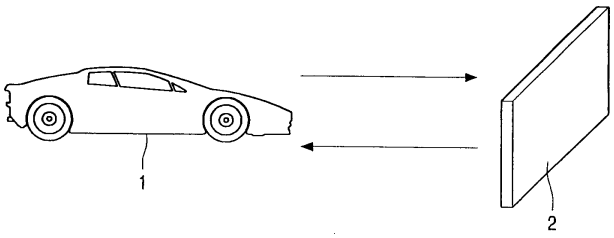
(71) Anmelder:
Philips Intellectual Property & Standards GmbH, 20099 Hamburg, DE

(72) Erfinder:
Zeeuw, Stephan, de, 22459 Hamburg, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Zugangssystem**

(57) Zusammenfassung: Die Erfindung betrifft ein Zugangssystem mit einer Basisstation (1) und wenigstens einer Nebenstation (2), wobei die Basisstation (1) für eine Erteilung einer Zugangsgenehmigung an die Nebenstation (2) eine einem HF-Träger aufmodulierte Anforderungs-Bitfolge, welche n Datenworte mit jeweils wenigstens einem Bit aufweist, an die Nebenstation (2) sendet, welche eine einem HF-Träger aufmodulierte Antwort-Bitfolge, welche m Datenworte mit jeweils wenigstens einem Bit aufweist, an die Basisstation (1) zurücksendet und wobei die Basisstation (1) die Reaktionszeit zwischen dem Absenden wenigstens einiger Datenworte der Anforderungs-Bitfolge und dem Empfang diesen jeweils zugeordneter Datenworte der Antwort-Bitfolge mit einer zulässigen Reaktionszeit vergleicht und der Nebenstation (2) nur dann eine Zugangsgenehmigung erteilt, wenn für die überprüften Datenworte einer Antwort die zulässige Reaktionszeit seltener als durch eine maximale Fehlerzahl vorgegeben überschritten wurde.



Beschreibung

[0001] Die Erfindung betrifft ein Zugangssystem mit einer Basisstation und wenigstens einer Nebenstation, wobei die Basisstation für eine Erteilung einer Zugangsgenehmigung an die Nebenstation eine einem HF-Träger aufmodulierte Anforderungs-Bitfolge, welchen Datenworte mit jeweils wenigstens einem Bit aufweist, an die Nebenstation sendet, welche eine einem HF-Träger aufmodulierte Antwort-Bitfolge, welchem Datenworte mit jeweils wenigstens einem Bit aufweist, an die Basisstation zurücksendet.

[0002] Bei einem solchen Zugangssystem handelt es sich um ein sogenanntes Passiv-Keyless-Entry-System, dass eine stark verbesserte Sicherheit gegenüber externen Angriffen gegenüber anderen Systemen besitzt. Derartige Systeme werden in zunehmendem Maße auch im Bereich der Kraftfahrzeugzugangssysteme eingesetzt. Sie eignen sich aber auch zur Realisierung von Zugangssystemen in Gebäuden oder Ähnlichem.

Stand der Technik

[0003] Ein potentielles Sicherheitsproblem bei derartigen Systemen ist, dass gegebenenfalls ein nicht autorisierter Angreifer eine sogenannten Relais-Attacke durchführt. Dabei wird auf dem Funkwege zwischen der Basisstation und der Nebenstation eine zusätzlich bidirektionale Verbindung mittels zweier sogenannter Relais-Stationen aufgebaut. Die tatsächlich zugangsberechtigte Nebenstation kann sich dann an einem weiter entfernten Ort befinden, beispielsweise bei dem tatsächlich autorisierten Benutzer der Nebenstation. Die Relais-Strecke wird von dem Angreifer dazu genutzt, mittels der tatsächlich berechtigten Nebenstation, die sich jedoch an einem anderen Ort befindet, eine Zugangsgenehmigung durch die Basisstation zu erhalten.

[0004] Zur Erkennung einer derartigen Relais-Attacke ist es aus der PCT-Anmeldung WO-0012848 bekannt, zur Ermittlung der Verzögerungszeit zwischen der Anforderungs-Bitfolge und der von der Nebenstation zurückgesendeten Antwort-Bitfolge eine Schwingungszählung der HF-Trägerwelle auf die, die Bit-Folgen aufmoduliert werden, in der Zeit zwischen Senden und Empfangen vorzunehmen. Ferner ist es aus dieser Veröffentlichung bekannt, einen Phasenvergleich und/oder ein Frequenzvergleich der gesendeten und empfangenen Trägerwelle vorzunehmen. Es wird also eine indirekte Laufzeitmessung mittels bestimmter Signalcharakteristika durchgeführt. Der wesentliche Nachteil dieser Anordnung besteht in dem relativ großen Aufwand, der beispielsweise insbesondere im Aufbau von Kraftfahrzeugen unerwünscht ist.

Aufgabenstellung

[0005] Es ist Aufgabe der Erfindung, ein Zugangssystem der eingangs genannten Art anzugeben, welches gegen eine sogenannte Relais-Attacke resistent ist und dennoch einen möglichst geringen Aufwand aufweist.

[0006] Diese Aufgabe ist erfindungsgemäß durch die Merkmale des Patentanspruchs 1 gelöst:

Zugangssystem mit einer Basisstation und wenigstens einer Nebenstation, wobei die Basisstation für eine Erteilung einer Zugangsgenehmigung an die Nebenstation eine einem HF-Träger aufmodulierte Anforderungs-Bitfolge, welche n Datenworte mit jeweils wenigstens einem Bit aufweist, an die Nebenstation sendet, welche eine einem HF-Träger aufmodulierte Antwort-Bitfolge, welche m Datenworte mit jeweils wenigstens einem Bit aufweist, an die Basisstation zurücksendet, und wobei die Basisstation die Reaktionszeit zwischen dem Absenden wenigstens einiger Datenworte der Anforderungs-Bitfolge und dem Empfang diesen jeweils zugeordneter Datenworte der Antwort-Bitfolge mit einer zulässigen Reaktionszeit vergleicht und der Nebenstation nur dann eine Zugangsgenehmigung erteilt, wenn für die überprüften Datenworte einer Antwort die zulässige Reaktionszeit seltener als durch eine maximale Fehlerzahl vorgegeben überschritten wurde.

[0007] Bei dem erfindungsgemäßen Zugangssystem weist die Anforderungs-Bitfolgen Datenworte auf, welche jeweils wenigstens 1 Bit aufweisen. Die durch die Nebenstation zurückgesendete Antwort-Bitfolge weist m Datenworte auf, welche ebenfalls jeweils wenigstens 1 Bit aufweisen. Dabei sind in der Anforderungs-Bitfolge wenigstens einige Datenworte vorgesehen, auf die eine Antwort durch die Basisstation mittels jeweils zugeordneter Datenworte der Antwort-Bitfolge vorgesehen ist. Mit anderen Worten: Es kann in der Anforderungs-Bitfolge Datenworte geben, auf die keine Datenworte durch die Nebenstationen zurückgesendet werden. Es gibt jedoch auch Datenworte, auf die eine Antwort mittels eines entsprechenden Datenwortes der Antwort-Bitfolge erwartet wird. Solchen Datenworten, auf die eine Reaktion erwartet wird, ist also jeweils ein entsprechendes, zugeordnetes Datenwort in der Antwort-Bitfolge vorgesehen.

[0008] Die Erfindung basiert nun darauf, die Reaktionszeit zwischen dem Absenden eines solchen Wortes der Anforderungs-Bitfolge, auf das ein zugeordnetes Antwort-Datenwort erwartet wird, und dem Eintreffen dieses Antwort-Datenwort mit einer maximal zulässigen Reaktionszeit zu vergleichen.

[0009] Da innerhalb einer Anforderungs-Bitfolge mehrere Datenworte existieren, auf die Antwort-Datenworte der Antwort-Bitfolge erwartet werden, wird dieser Vergleich mit der maximal vorgegebenen Reaktionszeit für jedes dieser zugeordneten Datenworte vorgenommen. Der Vergleich mit der maximalen Reaktionszeit erfolgt also innerhalb einer Anforderungs-Bitfolge für alle solche Datenworte, auf die zugeordnete Datenworte in der zurückgesendeten Antwort-Bitfolge existieren.

[0010] Gegenüber dem Stand der Technik weist die Erfindung mehrere Vorteile auf. Zum einen kann, wie bereits erwähnt, innerhalb einer Anforderungs-Bitfolge mehrfach eine Überprüfung der Reaktionszeit vorgenommen werden, nämlich genau so oft, wie zugeordnete Datenworte zwischen der Anforderungs-Bitfolge und Antwort-Bitfolge existieren. Damit wird nicht, wie beim Stand der Technik, nur eine einmalige Überprüfung der Reaktionszeit innerhalb einer Antwort-Bitfolge vorgenommen.

[0011] Ferner ist bei dem erfindungsgemäßen Zugangssystem keine Messung der Laufzeit durch Zählung von Trägerwellen oder ähnlichem erforderlich, sondern es genügt ein einfacher Laufzeitvergleich zwischen der Reaktionszeit und der maximal vorgegebenen Reaktionszeit, der durch Verzögerungsglieder relativ einfach realisiert werden kann. Es müssen keinerlei Zählvorgänge, Frequenzmessungen oder Phasenvergleiche vorgenommen werden.

[0012] Da innerhalb einer Anforderungs-Bitfolge, wie erläutert, eine mehrfache Überprüfung der Reaktionszeit vorgenommen wird, kann die erläuterte Entscheidung, ob die Reaktionszeit größer oder kleiner als die maximal zulässige Reaktionszeit ist, für jedes Paar der zugeordneten Datenworte vorgenommen werden. Innerhalb einer Anforderungs-Bitfolge findet also mehrfach eine Entscheidung statt. Daher wird darüber hinaus eine Entscheidung vorgenommen, wie oft während einer Anforderungs-Bitfolge die maximal zulässige Reaktionszeit überschritten wurde. Ist dies häufiger, als gemäß einer maximalen Fehlerzahl vorgegeben der Fall, wird ein Fehler bzw. eine Attacke erkannt und es wird keine Zugangsgenehmigung erteilt. Im anderen Fall wird eine solche erteilt.

[0013] Gemäß einer Ausgestaltung der Erfindung nach Anspruch 2 wird nach Absenden eines Datenwortes der Anforderungs-Bitfolge zunächst der Empfang des zugeordneten Datenwortes der Antwort-Bitfolge abgewartet und der oben erläuterte Vergleich mit der maximalen Reaktionszeit vorgenommen. Erst danach wird das nächste Datenwort der Anforderungs-Bitfolge gesendet. Mit dieser Vorgehensweise kann zum Beispiel eine Entscheidung über eine zulässige Anforderung bereits dann abgebrochen werden, wenn nach mehreren solcher Einzelvergleiche ein Überschreiten der maximalen Fehlerzahl festgestellt wird.

[0014] Bei der Anforderungs-Bitfolge kann es sich, wie gemäß einer weiteren Ausgestaltung der Erfindung nach Anspruch 3 vorgesehen, beispielsweise um einen Teil eines sogenannten Challenge-Response Zugangsverfahrens handeln. Derartige Verfahren sind nach dem Stande der Technik bekannt, können jedoch in dem erfindungsgemäßen Zugangssystem vorteilhaft eingesetzt werden, da während eines solchen Challenge-Response Verfahrens gleichzeitig bereits eine Überprüfung auf eine Relais-Attacke vorgenommen werden kann, dabei derartigen Zugangsverfahren ohnehin ein mehrfaches Senden und Antworten vorgesehen ist.

[0015] Die oben erläuterte maximale Reaktionszeit, mit der die gemessenen Zeiten verglichen werden, kann, wie gemäß einer weiteren Ausgestaltung der Erfindung nach Anspruch 5 vorgesehen ist, vorteilhaft variabel gestaltet sein. Sie kann beispielsweise an tatsächlich auftretende Reaktionszeiten anpassbar sein. Diese Anpassung darf natürlich nicht innerhalb eines Anforderungsvorganges erfolgen, da somit eine Anpassung an eine Relais-Attacke in unerwünschter Weise erfolgen würde. Sie kann jedoch langfristig über diverse Zugangsvorgänge vorgenommen werden, so dass beispielsweise eine Anpassung an schleichende Bauteilveränderungen vorgenommen werden kann.

[0016] Gemäß Anspruch 4 kann es innerhalb der Anforderungs-Bitfolge jeweils solche Datenworte geben, auf die kein zugeordnetes Datenwort der Antwort-Bitfolge existiert, auf die also kein unmittelbare Antwort mittels eines Datenwortes vorgesehen ist. Dabei kann, wie gemäß Anspruch 6 vorgesehen ist, eine Rücksendung eines Datenwortes in der Antwort-Bitfolge davon abhängig gemacht werden, welchen Inhalt ein Datenwort der Anforderungs-Bitfolge aufweist. Dabei kann eine inhaltliche Überprüfung vorgenommen werden, es kann aber auch, wie gemäß Anspruch 7 vorgesehen ist, ein Rücksenden eines solchen zugeordneten Datenwortes von einer bestimmten Bitfolge oder einem logischen Bitwert innerhalb des Datenwortes der Anforderungs-Bitfolge vorgenommen werden. Oder es kann, wie gemäß Anspruch 8 vorgesehen, eine Entscheidung anhand anderer, in der Basisstation vorliegender Daten vorgenommen werden.

Ausführungsbeispiel

[0017] Nachfolgend wird ein Ausführungsbeispiel der Erfindung anhand der Zeichnung der näher erläutert. Es zeigen:

[0018] **Fig.** 1 eine schematische Darstellung einer Basisstation in einem Fahrzeug und einer Nebenstation in einer Chipkarte,

[0019] **Fig.** 2 eine schematische Darstellung einer Anforderungs- und einer Antwort-Bitfolge und

[0020] **Fig.** 3 ein Blockschaltbild einer Basisstation.

[0021] In dem anhand der Zeichnung näher erläuterten Ausführungsbeispiel soll davon ausgegangen werden, dass das erfindungsgemäße Zugangssystem für ein Fahrzeug vorgesehen ist, dass also die Basisstation **1**, wie in **Fig.** 1 angedeutet ist, in einem Fahrzeug angeordnet ist. Es existiert wenigstens eine Nebenstation, über die gegebenenfalls ein Zugang zu dem Fahrzeug erfolgen soll. In der **Fig.** 1 ist eine Nebenstation **2** angedeutet, bei der es sich beispielsweise um eine Chip-Karte handeln kann. In der **Fig.** 1 ist ferner mittels zweier Pfeile schematisch angedeutet, dass zwischen der Basisstation **1** und der Nebenstation **2** ein Austausch von Daten über eine Hochfrequenzverbindung stattfindet.

[0022] Bei dem erfindungsgemäßen Zugangssys-

tem wird eine Anforderungs-Bitfolge, welchen Datenworte mit jeweils wenigstens einem Bit aufweist, einem Hochfrequenzträger aufmoduliert und an die Nebenstation **2** gesendet. Dies kann beispielsweise dann geschehen, wenn mittels Betätigung des Türgriffs des Fahrzeugs der Basisstation **1** signalisiert wird, dass eine Zugangsgenehmigung erfolgen soll. Die Basisstation **1** sendet dann diese Anforderungs-Bitfolge, die durch die Nebenstation **2** mit einer Antwort-Bitfolge beantwortet wird, welche an die Basisstation **1** gesendet wird und welchem Datenworte mit jeweils wenigstens einem Bit aufweist.

[0023] Hierbei kann beispielsweise ein sogenanntes Challenge-Response Verfahren eingesetzt werden, bei dem die Basisstation in der Anforderungs-Bitfolge die sogenannte Challenge sendet, die in der Basisstation **2** mittels eines kryptographischen Algorithmus und eines geheimen Schlüssels in eine Response umgewandelt wird. Diese Response wird dann an die Basisstation **1** in Form der Antwort-Bitfolge zurückgesendet und die Basisstation vergleicht die Response mittels eines gleichen Kryptoalgorithmus und des gleichen geheimen Schlüssels mit der Soll-Antwort. Bei Identität wird grundsätzlich eine Zugangsgenehmigung erteilt, wenn nicht die noch zu erläuternde, zulässige Reaktionszeit häufiger, als gemäß einer maximalen Fehlerzahl vorgegeben, überschritten wurde.

[0024] Bei der Erteilung einer Zugangsgenehmigung gemäß der Darstellung in **Fig.** 1 befindet sich die Nebenstation **2**, beispielsweise in der Chip-Karte, in der Nähe des Fahrzeugs. Der berechtigte Benutzer trägt diese Chip-Karte bei sich und kann, wie oben erläutert, durch Betätigung eines Tasters am Fahrzeug die Basisstation **1** aktivieren, so dass der oben beschriebene Zugangsgenehmigungsvorgang stattfindet. Es kann jedoch eine sogenannte Relais-Attacke vorgenommen werden, welche durch inhaltliches Auswerten der Datenworte nicht erkannt wird. Dabei findet zwischen der Basisstation **1** und der Nebenstation **2** nicht, wie in **Fig.** 1 angedeutet, eine unmittelbare Verbindung über einen Hochfrequenzträger statt, sondern es wird zwischen diese beiden Stationen eine sogenannte Relais-Strecke geschaltet. Dabei werden die Datenworte über eine solche Relais-Strecke gegebenenfalls über eine große Entfernung übertragen. In diesem Fall befindet sich die Nebenstation **2** weit entfernt vom Fahrzeug **1** und somit der Basisstation **1**, so dass eine unmittelbare Übertragung zwischen diesen nicht mehr stattfindet. Über die Relais-Strecke ist dieses dann jedoch dennoch möglich und es findet eine nicht erwünschte Zugangsgenehmigung statt. Es kann nämlich über diese Relais-Attacke jederzeit von unberechtigten Benutzern eine Anforderungs-Bitfolge ausgelöst werden, die über die Relais-Strecke zu einer weit entfernten Nebenstation **2** übertragen wird. Somit kann bei Einsatz einer solchen Relais-Strecke grundsätzlich jeder, der eine solche Strecke aufgebaut hat und am Fahrzeug **1** den Vorgang zur Durchführung einer Zugangsgenehmigung auslöst, einen Zugang zu dem Fahrzeug erhalten. Beim Hin- und Hersenden der Datenworte über eine solche Relais-Strecke treten jedoch größere Laufzeiten auf, als beim unmittelbaren Senden der Daten zwischen der Basisstation **1** und der Nebenstation **2**. Eine unmittelbare Messung der Laufzeiten würde eine Erkennung einer solchen Relais-Attacke gestatten, würde jedoch einen relativ hohen Bauaufwand, zumindest in der Basisstation **1**, erfordern.

[0025] In dem erfindungsgemäßen Zugangssystem ist daher in noch näher zu erläuternder Weise ein Vergleich der tatsächlich auftretenden Reaktionszeiten mit einer maximal zulässigen Reaktionszeit vorgesehen. Da ein solcher Vergleich mittels eines einfachen Verzögerungsgliedes und eines Komparators vorgenommen werden kann, ist hierbei der Bauaufwand wesentlich geringer. Ferner kann für mehrere Datenworte und entsprechend zugeordnete, zugesendete Datenworte jeweils ein Vergleich mit der maximalen Reaktionszeit vorgenommen werden, so dass also innerhalb einer Anforderungs-Bitfolge und einer zurückgesendeten Antwort-Bitfolge ein mehrfacher Vergleich mit der maximal zulässigen Reaktionszeit vorgenommen werden kann und nicht nur ein Vergleich für die gesamte Bitfolge.

[0026] **Fig.** 2 zeigt in schematischer Darstellung den oben beschriebenen Vorgang des Sendens der Datenworte einer Anforderungs-Bitfolge AF und des Rücksendens von Datenworten einer Antwort-Bitfolge AW.

[0027] Gemäß der schematischen Darstellung in **Fig.** 2 erfolgt dies in dem Ausführungsbeispiel in der zeitlichen Reihenfolge, dass die Basisstation **1** zunächst ein Datenwort **1** der Anforderungs-Bitfolge an die Nebenstation **2** sendet, welche daraufhin ein Datenwort **1** der Antwort-Bitfolge AW an die Basisstation **1** zurücksendet. Dieser Vorgang wiederholt sich mit weiteren Datenworten, bis schließlich die Basisstation **1** das letzte Datenwort n der Anforderungs-Bitfolge gesendet hat und die Nebenstation **2** mit dem Datenwort m der Antwort-Bitfolge geantwortet hat. Die Zahl der Datenworten der Anforderungs-Bitfolge und der Datenworte m der Antwort-Bitfolge muss nicht gleich sein. Es ist nämlich möglich, dass in der Anforderungs-Bitfolge Datenworte existieren, auf die innerhalb der Antwort-Bitfolge keine zugeordneten Datenworte existieren, auf die also mit anderen Worten keine Antwort durch ein Datenwort in der Antwort-Bitfolge erfolgt. Dies kann beispielsweise in in der Zeichnung nicht näher angedeuteten Weise vom Inhalt eines Datenwortes der Anforderungs-Bitfolge AF abhängig gemacht werden.

[0028] In der Darstellung gemäß **Fig.** 2 wird der Einfachheit halber jedoch davon ausgegangen, dass auf jedes Datenwort der Anforderungs-Bitfolge AF ein zugeordnetes Datenwort der Antwort-Bitfolge AW existiert.

[0029] Die Darstellung gemäß **Fig.** 2 zeigt, dass nach einem Absenden eines Datenwortes der Anforderungs-Bitfolge AF unmittelbar zunächst der Emp-

fang des zugeordneten Datenwortes der Antwort-Bitfolge AW abgewartet wird. Erst nach Empfang dieses zugeordneten Datenwortes der Antwort-Bitfolge sendet die Basisstation **1** das nächste Datenwort der Anforderungs-Bitfolge AF.

[0030] Diese Vorgehensweise ist bei einem Challenge-Response Verfahren sinnvoll, es kann jedoch bei anderen eingesetzten Verfahren auch eine andere Verschachtelung der Datenworte vorgesehen sein.

[0031] **Fig.** 3 zeigt in Form eines Blockschaltbildes ein Teil des Zugangssystems wie er in der Basisstation **1** vorgesehen ist.

[0032] Innerhalb der Basisstation **1** werden, wie oben erläutert, Datenworte innerhalb einer Anforderungs-Bitfolge erzeugt. Die Darstellung gemäß **Fig.** 3 zeigt, dass diese Datenworte AF_x mittels eines Ausgangsverstärkers L auf eine Sendeantenne **12** übertragen werden. Dabei sind die Datenworte AF_x in der **Fig.** 3 nicht näher angedeuteter Weise mittels eines Modulators auf einen Hochfrequenzträger aufmoduliert. In dieser aufmodulierten Form werden sie als Hochfrequenz-Impulse von der Sendeantenne **12** auf die Nebenstation **2** übertragen.

[0033] In der Basisstation ist gemäß **Fig.** 3 ein Verzögerungsglied **13** vorgesehen, das beispielsweise ein gesendetes Datenwort AF um eine vorgegebene Verzögerungszeit, bei der es sich um eine maximal zulässige Reaktionszeit handelt, verzögert. Das entsprechend verzögerte Ausgangssignal des Verzögerungsgliedes **13** gelangt an einen Entscheider **14**.

[0034] Dem Entscheider **14** wird ferner ein einem HF-Träger aufmoduliertes und mittels einer Empfangsantenne **15** empfangenes Datenwort der in der **Fig.** 3 nicht angedeuteten Nebenstation **2** zugeführt. Dieses Datenwort wird mittels eines Detektors **16** detektiert und ebenfalls dem Entscheider **14** zugeführt.

[0035] Dabei kann das Verzögerungsglied **13** beispielsweise in relativ einfacher Weise durch ein Surface-Acoustic-Wave-Element oder durch eine serielle Anordnung logischer Gatter realisiert sein.

[0036] Die Entscheiderschaltung **14** kann beispielsweise als einfache bistabile Kippschaltung realisiert sein, welche nach einer einmal getroffenen Entscheidung den Wert ihres Ausgangssignals nicht mehr verändert. Diese einfache Entscheidung wird anhand des Umstandes getroffen, welches der beiden Signale von dem Verzögerungsglied **13** bzw. dem Detektor **16** den Entscheider **14** zuerst erreicht. Abhängig von diesem Umstand liefert der Ausgang des Entscheiders **14** entweder dann eine logische 1, wenn der von dem Verzögerungsglied **13** gelieferte Impuls den Entscheider **14** zuerst erreicht. Dies ist beispielsweise dann der Fall, wenn durch die Nebenstation **2** kein Impuls zurückgesendet wurde oder dieser Impuls die maximal zulässige Verzögerungszeit überschreitet.

[0037] Umgekehrt liefert der Ausgang des Entscheiders dann eine logische 0, wenn der von der Nebenstation **2** zurückgesendete Impuls, also das zurückgesendete Datenwort der Antwort-Bitfolge, den Entscheider **14** vor dem von dem Verzögerungsglied **13** gelieferten Impuls erreicht.

[0038] Vor jedem neuen Entscheidungsprozeß wird der Entscheider **14** mittels eines Signals R zurückgesetzt.

[0039] Dieses Ausgangssignal des Entscheiders **14** wird mittels einer Logik **17** ausgewertet, welche beispielsweise berücksichtigen kann, ob auf ein gesendetes Datenwort überhaupt eine Reaktion eines zugeordneten Datenwortes der Antwort-Bitfolge erwartet wurde. Dazu wird ihr ein Signal D zugeführt, welches die Grundlage für diese Entscheidung ist.

[0040] In all denen Fällen, in denen eine tatsächliche Auswertung des Ausgangssignals des Entscheiders **14** vorgenommen werden soll, liefert die Logik **17** dieses Signal an einen Zähler **18**, welcher für mehrere innerhalb einer Anforderungs-Bitfolge gesendete Datenworte die entsprechenden von dem Entscheider **14** gelieferten Vergleichsergebnisse zählt.

[0041] In dem Ausführungsbeispiel liefert der Entscheider **14** immer dann eine 1, wenn die Reaktion eines zugeordneten Datenwortes zu spät oder gar nicht erfolgt. Dies wird durch die Logik **17** bewertet und an den Zähler **18** weitergegeben, der diese logischen 1'en für alle Datenworte innerhalb einer Anforderungs-Bitfolge zählt.

[0042] Mittels des Zählers **18** kann ferner ein Vergleich der tatsächlich auftretenden Fehler, die der Zähler **18** während des Empfangs/Sendens einer Anforderungs- und Antwort-Bitfolge gezählt hat, mit einer maximalen, zulässigen Fehlerzahl E_{max} vergleichen werden. Dies kann beispielsweise dadurch geschehen, dass der Zähler **18** vor dem Senden einer Anforderungs-Bitfolge auf diese maximale Fehlerzahl E_{max} gesetzt wird und mit jedem tatsächlich auftretenden Fehler **1**, der von dem Entscheider **14** der Logik **17** an den Zähler **18** gegeben wird, herunterzählt, bis der Wert 0 in dem Zähler **18** erreicht ist. Geschieht dies innerhalb einer Anforderungs-Bitfolge und einer zurückgesendeten Antwort-Bitfolge, so ist die maximale Fehlerzahl E_{max} erreicht und es wird für diese Anforderungs-Bitfolge keine Zugangsgenehmigung erteilt.

[0043] Ist jedoch am Ende des Hin- und Hersendens von Datenworten eine Anforderungs-Bitfolge und zugeordneten Datenworten einer Antwort-Bitfolge die maximale Fehlerzahl Emax nicht erreicht worden, so kann eine Zugangsgenehmigung an die jeweils betroffenen Nebenstationen gesendet werden.

[0044] In der Darstellung des Blockschaltbildes gemäß **Fig.** 3 kann diese Entscheidung in einfacher Weise anhand des Ausgangssignals E des Zählers **18** am Ende eines solchen Anforderungsvorganges vorgenommen werden.

[0045] Die Darstellung des Blockschaltbildes in **Fig.** 3 zeigt, dass bei dem erfindungsgemäßen Zugangssystem keine unmittelbare Messung von Reaktionszeiten vorgenommen wird. Auch ist es nicht erforderlich, Phasen oder Frequenzbeziehungen des gesendeten und empfangenen HF-Trägers zu detek-

tieren. Vielmehr wird anhand des Verzögerungsgliedes **13** und des Entscheiders **14** ein einfacher Vergleich der tatsächlichen Reaktionszeit mit einer maximal vorgegebenen Reaktionszeit für jedes Datenwort vorgenommen. Die maximal zulässige Reaktionszeit ist dabei durch die Verzögerungszeit, die das Verzögerungsglied **13** erzeugt, vorgegeben.

[0046] Gegebenenfalls kann diese Reaktionszeit, die das Verzögerungsglied **13** erzeugt, auch variabel gestaltet sein, um an verschiedenen Bedingungen anpassbar zu sein. Insgesamt gelingt mittels des erfindungsgemäßen Zugangssystems eine relativ sichere Erkennung einer Relais-Attacke, da für mehrere Datenworte der Anforderungs-Bitfolge und jeweils zugeordnete Datenworte der Antwort-Bitfolge ein Vergleich der tatsächlichen Reaktionszeit mit einer maximal zulässigen Reaktionszeit erfolgen kann. Es kann also innerhalb einer solchen Bitfolge ein mehrfacher Vergleich erfolgen.

Patentansprüche

1. Zugangssystem mit einer Basisstation (**1**) und wenigstens einer Nebenstation (**2**), wobei die Basisstation (**1**) für eine Erteilung einer Zugangsgenehmigung an die Nebenstation (**2**) eine einem HF-Träger aufmodulierte Anforderungs-Bitfolge, welche n Datenworte mit jeweils wenigstens einem Bit aufweist, an die Nebenstation (**2**) sendet, welche eine einem HF-Träger aufmodulierte Antwort-Bitfolge, welche m Datenworte mit jeweils wenigstens einem Bit aufweist, an die Basisstation (**1**) zurücksendet, und wobei die Basisstation (**1**) die Reaktionszeit zwischen dem Absenden wenigstens einiger Datenworte der Anforderungs-Bitfolge und dem Empfang diesen jeweils zugeordneter Datenworte der Antwort-Bitfolge mit einer zulässigen Reaktionszeit vergleicht und der Nebenstation (**2**) nur dann eine Zugangsgenehmigung erteilt, wenn für die überprüften Datenworte einer Antwort die zulässige Reaktionszeit seltener als durch eine maximale Fehlerzahl vorgegeben überschritten wurde.

2. Zugangssystem nach Anspruch 1, dadurch gekennzeichnet, daß die Basisstation (**1**) jeweils nach Absenden eines Datenwortes der Anforderungs-Bitfolge die Reaktionszeit des jeweils zugeordneten Datenwortes der Antwort-Bitfolge feststellt und mit der maximal zulässigen Reaktionszeit vergleicht und erst danach das nächste Datenwort der Anforderungs-Bitfolge sendet.

3. Zugangssystem nach Anspruch 1, dadurch gekennzeichnet, daß die Anforderungs-Bitfolge und die Antwort-Bitfolge Teil eines Challenge-Response Zugangsverfahrens sind.

4. Zugangssystem nach Anspruch 1, dadurch gekennzeichnet, daß die Basisstation (**1**) nur auf einige vorgegebene Datenworte der Anforderungs-Bitfolge ein jeweils zugeordnetes Datenwort der Antwort-Bitfolge erwartet.

5. Zugangssystem nach Anspruch 1, dadurch gekennzeichnet, daß die maximale Reaktionszeit variabel ist, insbesondere an tatsächlich auftretende Reaktionszeiten anpaßbar ist.

6. Zugangssystem nach Anspruch 1, dadurch gekennzeichnet, daß eine Rücksendung eines Datenwortes in der Antwort-Bitfolge abhängig vom Inhalt des zugeordneten Datenwortes der Anforderungs-Bitfolge ist.

7. Zugangssystem nach Anspruch 6, dadurch gekennzeichnet, daß eine Rücksendung eines Datenwortes der Antwort-Bitfolge auf ein zugeordnetes Datenwort der Anforderungs-Bitfolge nur dann erfolgt, wenn das Datenwort der Antwort-Bitfolge einen vorgegebenen logischen Bitwert aufweist.

8. Zugangssystem nach Anspruch 6, dadurch gekennzeichnet, daß eine Rücksendung eines Datenwortes der Antwort-Bitfolge auf ein zugeordnetes Datenwort der Anforderungs-Bitfolge in Abhängigkeit von in der Basisstation vorhandenen Daten erfolgt.

9. Anwendung des Zugangssystems nach einem der Ansprüche 1 bis 8 in einem Fahrzeug.

Es folgen 2 Blatt Zeichnungen

Anhängende Zeichnungen

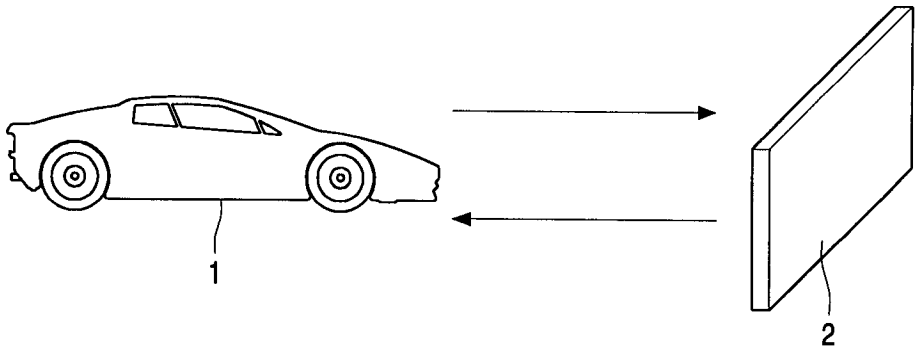


FIG. 1

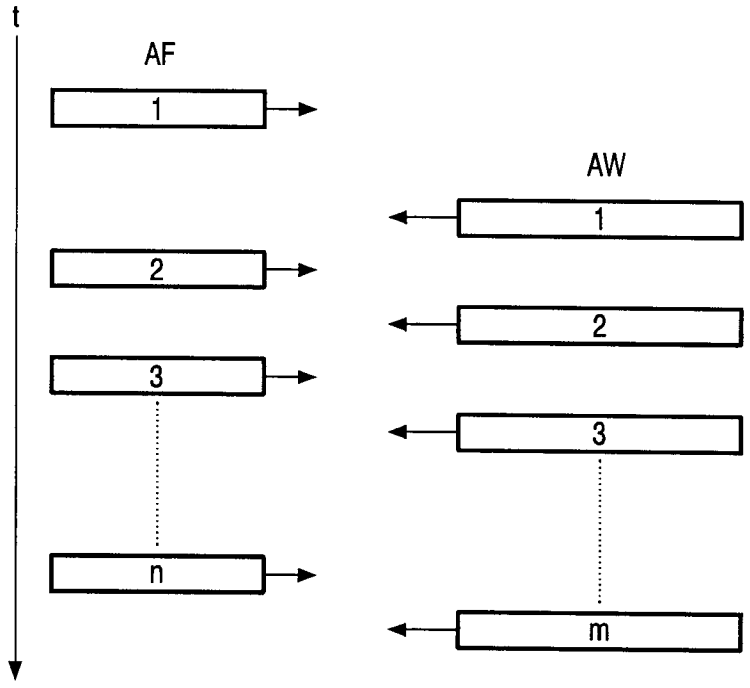


FIG. 2

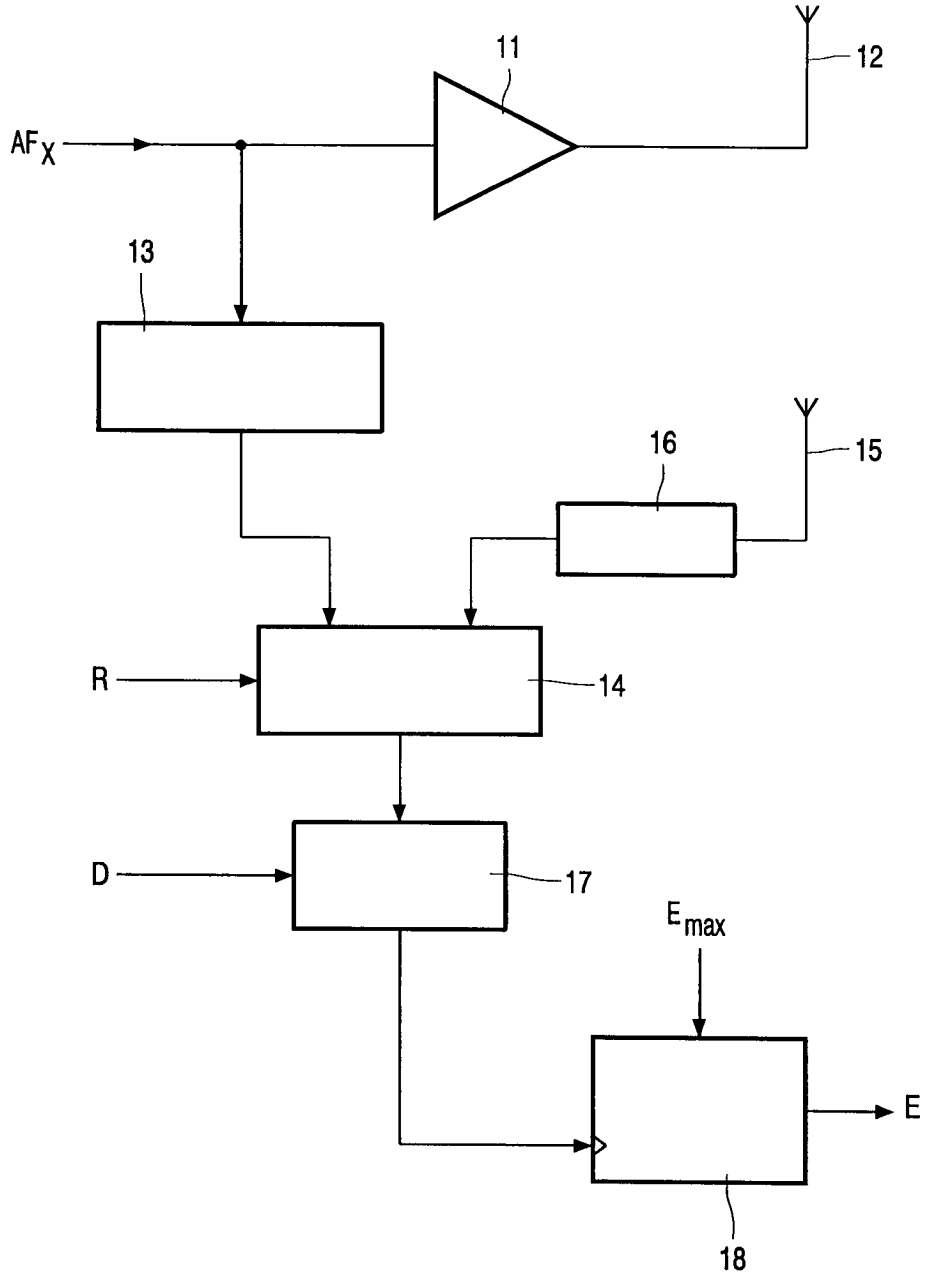


FIG. 3