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

(11) EP 0 698 706 A1

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
28.02.1996 Patentblatt 1996/09

(51) Int. Cl.[6]: **E05B 49/00**

(21) Anmeldenummer: **95112137.5**

(22) Anmeldetag: **02.08.1995**

(84) Benannte Vertragsstaaten:
DE FR GB IT

(30) Priorität: **26.08.1994 DE 4430315**

(71) Anmelder: **TEMIC TELEFUNKEN microelectronic GmbH**
D-74072 Heilbronn (DE)

(72) Erfinder:
- **Hettich, Gerhard, Dr.**
  D-90499 Dietenhofen (DE)
- **Doerfler, Reiner, Dr.**
  D-90562 Heroldsberg (DE)

(74) Vertreter: **Maute, Hans-Jürgen, Dipl.-Ing.**
D-74025 Heilbronn (DE)

(54) Verfahren zum Betrieb eines Schliesssystems für verschliessbare Gegenstände

(57) Beschrieben wird ein Verfahren zum Betrieb eines Schließsystems für verschließbare Gegenstände. Das Schließsystem weist ein Schlüsselmodul (1) und ein Schloßmodul (2) auf, wobei bei einer Betätigung des Schlüsselmoduls vom Schlüsselmodul eine Schlüssel-Nachricht (SN) aus einem Schlüssel-Code (SC) und einer Schlüssel-Uhrzeit (SU) gebildet und zum Schloßmodul übertragen wird. Die Schlüssel-Nachricht wird vom Schloßmodul empfangen, entschlüsselt und durch Vergleich mit einem vom Schloßmodul gebildeten Schloß-Code und einer Schloß-Uhrzeit ausgewertet. Anhand dieser Auswertung wird ein Verifizierungsvorgang durchgeführt und bei erfolgreicher Verifizierung ein codierbares Ausgangssignal (AS) ausgegeben.

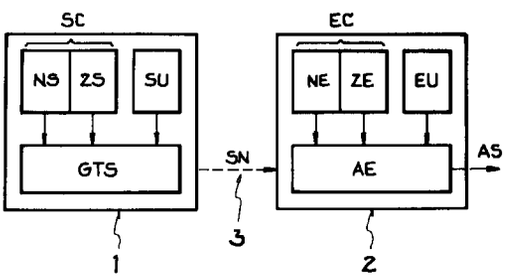

FIG.

EP 0 698 706 A1

Beschreibung

Zur Übermittlung verschlüsselter elektronischer Daten sind Datenübertragungssysteme aus einer batteriebetriebenen (IR-/HF-) Fernbedienung als Sendemodul und einem geeigneten Empfängermodul gebräuchlich. Derartige Datenübertragungssysteme werden oftmals in Schließsystemen zur Durchführung des Schließvorgangs bei verschließbaren Gegenständen eingesetzt und sind hierzu als Kombination aus elektronischem Schlüsselmodul und elektronischem Schloßmodul ausgebildet - solche elektronischen Schließsysteme kommen insbesondere im Kfz-Bereich zur Bedienung der Fahrzeugtüren und Diebstahlsicherungen von Kraftfahrzeugen in zunehmendem Maße auf den Markt.

Die Datenübertragung Zwischen dem Schlüsselmodul und dem Schloßmodul kann auf zweierlei Weise erfolgen: entweder mittels eines Festcodes, indem bei jeder Datenübertragung ein gleichbleibender Code zur Durchführung des Schließvorgangs übertragen wird oder mittels eines Wechselcodes, indem bei jeder Datenübertragung ein variabler, jeweils nur ein einziges Mal zur Durchführung des Schließvorgangs verwendbarer Code übertragen wird. Nachteilig bei diesen Datenübertragungsverfahren ist der Mangel an Mißbrauchsicherheit: bei der Festcode-Datenübertragung ist durch Abhören und Nachahmen des gleichbleibenden übertragenen Codes ein Mißbrauch durch Unbefugte leicht möglich (beispielsweise kann ein Kraftfahrzeug mit einem entsprechend nachprogrammierten Schlüsselmodul beliebig oft geöffnet und gestartet werden); bei der Wechselcode-Datenübertragung können mehrere aufeinanderfolgende Codes durch Unbefugte mittels einer selbstlernenden Fernbedienung ausgelesen werden, wodurch ein Mißbrauch in begrenztem Umfang möglich ist.

Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren gemäß dem Oberbegriff des Patentanspruchs 1 anzugeben, bei dem eine hohe Mißbrauchsicherheit gegeben ist. Diese Aufgabe wird erfindungsgemäß durch die Merkmale im Kennzeichen des Patentanspruchs 1 gelöst. Vorteilhafte Weiterbildungen und Ausgestaltungen des Verfahrens ergeben sich aus den Unteransprüchen.

Beim vorgestellten Verfahren wird bei jeder Datenübertragung zwischen Schlüsselmodul und Schloßmodul ein Verifizierungsvorgang unter Verwendung der von einer elektronischen Uhr des Schlüsselmoduls generierten Uhrzeit und der von einer elektronischen Uhr des Schloßmoduls generierten Uhrzeit durchgeführt. Wie in der Figur dargestellt, wird nach der Aktivierung des Schlüsselmoduls 1 (beispielsweise durch Betätigung eines Druckknopfes) vom Schlüsselmodul 1 eine Schlüssel-Nachricht SN bestehend aus einem verschlüsselten Schlüssel-Geheimtext GTS (generiert mit Hilfe einer Schlüssel-Nummer NS, einer Pseudo-Zufallszahl ZS und der Schlüssel-Uhrzeit SU) auf der Übertragungsstrecke 3 ausgesendet, die Schlüssel-Nachricht SN vom Schloßmodul 2 empfangen, von einer Auswerteeinheit AE entschlüsselt und mit einer Schloß-Nummer NE, einer Pseudo-Zufallszahl ZE und der Schloß-Uhrzeit EU verglichen; auf der Grundlage dieses Vergleichs - insbesondere wird die Schlüssel-Uhrzeit SU mit der Schloß-Uhrzeit EU verglichen und eine eventuell auftretende Zeitdifferenz ausgewertet - wird ein Verifizierungsvorgang durchgeführt.

Hierbei können folgende unterschiedliche Fälle auftreten:

- bei einer Übereinstimmung von Schlüssel-Code SC (dieser wird aus der Schlüssel-Nummer NS und der Pseudo-Zufallszahl ZS gebildet) und Schloß-Code EC (dieser wird aus der Schloß-Nummer NE und der Pseudo-Zufallszahl ZE gebildet) und wenn gleichzeitig die Zeitdifferenz zwischen Schlüssel-Uhrzeit SU und Schloß-Uhrzeit EU einen vorgegebenen Schwellwert nicht überschreitet, wird die Verifizierung als erfolgreich bewertet; daraufhin wird vom Schloßmodul 2 ein codierbares Ausgangssignal AS ausgegeben, durch das bestimmte Reaktionen initiiert werden (beispielsweise dient das Ausgangssignal AS als Steuersignal zum Öffnen der Türen oder zur Entriegelung der Wegfahrsperre eines Kraftfahrzeugs). Zusätzlich können die Uhren von Schlüsselmodul 1 und Schloßmodul 2 synchronisiert werden, indem die Schloß-Uhrzeit EU auf die Schlüssel-Uhrzeit SU nachgestellt wird.

- stimmen Schlüssel-Code SC und Schloß-Code EC überein, ist die Zeitdifferenz zwischen Schlüssel-Uhrzeit SU und Schloß-Uhrzeit EU jedoch größer als der vorgegebene Schwellwert (entweder infolge eines unterschiedlichen Gangs der beiden Uhren oder infolge unbefugten Auslesens), muß die Datenübertragung wiederholt werden; anhand dieser zweiten (Kontroll-) Datenübertragung wird überprüft, ob das korrekte Schlüsselmodul 1 verwendet wurde. Hierzu kann durch Vergleich des Zeitabstands zwischen der Uhrzeit der ersten Datenübertragung und der Uhrzeit der zweiten Datenübertragung sowohl beim Schlüsselmodul 1 als auch beim Schloßmodul 2 festgestellt werden, ob das Schlüsselmodul 1 eine fortlaufende Uhr enthält: Ist der Zeitabstand beim Schlüsselmodul 1 und beim Schloßmodul 2 gleich groß, war die Zeitdifferenz bei der ersten Datenübertragung durch den unterschiedlichen Gang der beiden Uhren bedingt; in diesem Fall wird eine Synchronisation der Schloß-Uhrzeit EU auf die Schlüssel-Uhrzeit SU vorgenommen und die Verifizierung als erfolgreich bewertet.
  Ist der Zeitabstand beim Schlüsselmodul 1 gleich Null bzw. weicht dieser signifikant vom Zeitabstand beim Schloßmodul 2 ab, kann auf ein einmaliges bzw. mehrmaliges unbefugtes Auslesen der Schlüssel-Nachricht SN geschlossen werden, da alle unbefugt ausgelesenen Schlüssel-Nachrichten SN die Schlüssel-Uhrzeit SU des Auslesevorgangs ent-

halten; diese feste(n) Schlüssel-Uhrzeit(en) SU differiert(en) von den im Schloßmodul 2 generierten variablen Schloß-Uhrzeiten EU, so daß sich bei der Bildung des Zeitabstands im Schlüsselmodul 1 der Wert Null (einmaliges unbefugtes Auslesen) oder ein falscher Wert (mehrmaliges unbefugtes Auslesen oder unbefugtes Auslesen mehrerer aufeinanderfolgender Codes) ergibt. Die Verifizierung wird somit als nicht-erfolgreich bewertet und eine Sperrung des Ausgangssignals AS vorgenommen.

- bei einer Abweichung von Schlüssel-Code SC und Schloß-Code EC - beispielsweise durch Betätigung eines nicht-zulässigen Schlüsselmoduls 1 - wird die Verifizierung als nicht-erfolgreich bewertet und das Ausgangssignal AS des Schloßmoduls 2 gesperrt.

Da bei jeder Datenübertragung zwischen Schlüsselmodul und Schloßmodul ein derartiger Verifizierungsvorgang der Schlüssel-Nachricht durchgeführt wird, ist ein Öffnen des verschließbaren Gegenstands durch Unbefugte auf keinen Fall - auch nicht in begrenztem Umfang - möglich; demnach ist eine hohe Sicherheit vor Mißbrauch (unbefugtes Auslesen) gegeben. Der Schwellwert für die zulässige Zeitdifferenz zwischen der Schlüssel-Uhrzeit und der Schloß-Uhrzeit bei der ersten Datenübertragung wird so vorgegeben, daß auch ein unmittelbar nach dem unbefugten Auslesen vorgenommener Mißbrauchsversuch erkannt wird; beispielsweise kann der Schwellwert im Bereich von einigen Sekunden (ca. 20 - 30 s) bis zu wenigen Minuten (beispielsweise max. 2 min) gewählt werden. Dagegen wird bei der zweiten Datenübertragung für die zulässige Differenz des Zeitabstands beim Schlüsselmodul und Schloßmodul ein minimaler Wert gewählt (beispielsweise 1 s), da die beiden Datenübertragungen relativ rasch aufeinanderfolgen und sich in dieser Zeitspanne noch keine Gangabweichung der beiden Uhren bemerkbar machen kann. Als zusätzliche Sicherheitsmaßnahme vor einem unbefugten Aus lesen mehrerer aufeinanderfolgender Codes kann der Zeitabstand zwischen der ersten und der zweiten Datenübertragung als Bedingung vorgeschrieben werden; dieser erforderliche Zeitabstand (beispielsweise 30 s) kann darüber hinaus variiert bzw. variabel vorgegeben werden und wird vorzugsweise mittels einer im Schloßmodul gespeicherten Zufallszahl erzeugt, so daß er beim Auslesevorgang nicht nachempfunden werden kann. Der Zeitpunkt der zweiten Datenübertragung kann auch vom Schloßmodul durch ein optisches oder akustisches Signal angezeigt oder angefordert werden.

Patentansprüche

1. Verfahren zum Betrieb eines Schließsystems für verschließbare Gegenstände, bestehend aus einem Schlüsselmodul (1) und einem Schloßmodul (2), dadurch gekennzeichnet:

   - bei einer Betätigung des Schlüsselmoduls (1) wird vom Schlüsselmodul (1) eine Schlüssel-Nachricht (SN) aus einem Schlüssel-Code (SC) und einer Schlüssel-Uhrzeit (SU) gebildet und zum Schloßmodul (2) übertragen,

   - die Schlüssel-Nachricht (SN) wird vom Schloßmodul (2) empfangen, entschlüsselt und durch Vergleich mit einem vom Schloßmodul (2) gebildeten Schloß-Code (EC) und einer Schloß-Uhrzeit (EU) ausgewertet,

   - anhand dieser Auswertung wird ein Verifizierungsvorgang durchgeführt und bei erfolgreicher Verifizierung ein codierbares Ausgangssignal (AS) ausgegeben.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der Schlüssel-Code (SC) aus einer Schlüssel-Nummer (NS) und einer Zufallszahl (ZS) und die Schlüssel-Uhrzeit (SU) von einer elektronischen Uhr im Schlüsselmodul (1) generiert wird, und daß der Schloß-Code (EC) aus einer Schloß-Nummer (NE) und einer Zufallszahl (ZE) und die Schloß-Uhrzeit (EU) von einer elektronischen Uhr im Schloßmodul (2) generiert wird.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß bei der Auswertung der Schlüssel-Nachricht (SN) ein Schwellwert für die zulässige Zeitdifferenz zwischen der Schlüssel-Uhrzeit (SU) und der Schloß-Uhrzeit (EU) vorgegeben wird.

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß bei einer Übereinstimmung von Schlüssel-Code (SC) und Schloß-Code (EC) und beim Unterschreiten des Schwellwerts für die zulässige Zeitdifferenz der Verifizierungsvorgang als erfolgreich bewertet wird.

5. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß bei einer Übereinstimmung von Schlüssel-Code (SC) und Schloß-Code (EC) und beim Überschreiten des Schwellwerts für die zulässige Zeitdifferenz eine zweite Datenübertragung vom Schlüsselmodul (1) vorgenommen werden muß, und daß anhand der Schlüssel-Nachricht (SN) der zweiten Datenübertragung überprüft wird, ob das korrekte Schlüsselmodul (1) verwendet wurde.

6. Verfahren nach Anspruch 5, dadurch gekennzeichnet, daß der Zeitabstand zwischen der ersten Datenübertragung und der zweiten Datenübertragung im Schlüsselmodul (1) und im Schloßmodul (2) bestimmt wird, daß die Zeitabstände des Schlüsselmoduls (1) und des Schloßmoduls (2) miteinander verglichen werden, und daß bei einer Übereinstim-

mung der Zeitabstände die Verifizierung als erfolgreich bewertet wird.

7. Verfahren nach Anspruch 5 oder 6, dadurch gekennzeichnet, daß die zweite Datenübertragung in einem bestimmten vorgebbaren Zeitabstand nach der ersten Datenübertragung vorgenommen werden muß.

8. Verfahren nach Anspruch 7, dadurch gekennzeichnet, daß der Zeitabstand variabel vorgegeben wird.

9. Verfahren nach Anspruch 7 oder 8, dadurch gekennzeichnet, daß der Zeitabstand vom Schloßmodul (2) vorgegeben wird.

10. Verfahren nach Anspruch 9, dadurch gekennzeichnet, daß der Zeitabstand mit Hilfe einer Zufallszahl (ZE) des Schloßmoduls (2) generiert wird.

11. Verfahren nach einem der Ansprüche 5 bis 10, dadurch gekennzeichnet, daß die zweite Datenübertragung vom Schloßmodul (2) durch ein akustisches oder optisches Signal angefordert wird.

12. Verfahren nach einem der Ansprüche 1 bis 11, dadurch gekennzeichnet, daß bei einer erfolgreichen Verifizierung die Schloß-Uhrzeit (EU) auf die Schlüssel-Uhrzeit (SU) synchronisiert wird.

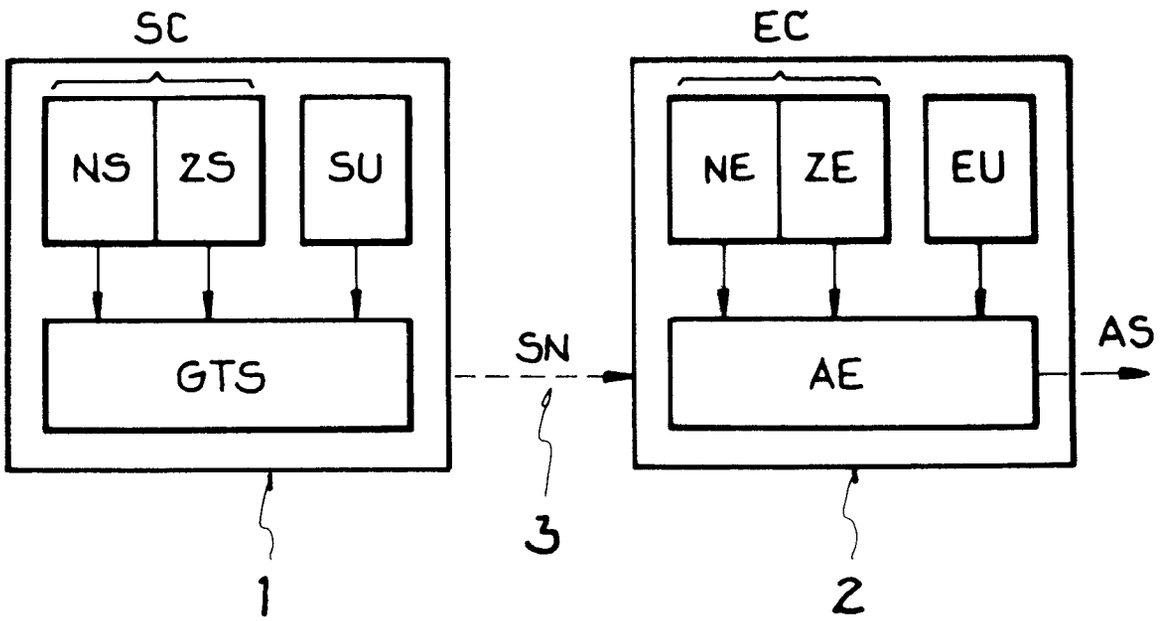

FIG.

Europäisches Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 95 11 2137

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (Int.Cl.6)
X A	EP-A-0 311 112 (MATSUSHIMA KOGYO KABUSHIKI KAISHA) * Spalte 3, Zeile 13 - Spalte 5, Zeile 43; Abbildungen 1,2 *	1,3,4 2,12	E05B49/00
X A	DE-C-42 27 887 (BARTEL) * Spalte 2, Zeile 48 - Spalte 7, Zeile 18; Abbildung 1 *	1,3,4 2,12	
X A	FR-A-2 607 544 (NEIMAN S.A.) * Seite 1, Zeile 31 - Seite 3, Zeile 31; Abbildung 4 *	1,3,4 2	

RECHERCHIERTE SACHGEBIETE (Int.Cl.6)

E05B

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
DEN HAAG	2.Oktober 1995	Herbelet, J.C.

KATEGORIE DER GENANNTEN DOKUMENTE

X : von besonderer Bedeutung allein betrachtet
Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie
A : technologischer Hintergrund
O : nichtschriftliche Offenbarung
P : Zwischenliteratur

T : der Erfindung zugrunde liegende Theorien oder Grundsätze
E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist
D : in der Anmeldung angeführtes Dokument
L : aus andern Gründen angeführtes Dokument

& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

EPO FORM 1503 03.82 (P04C03)