



(11) **EP 1 314 140 B1**

(12) **EUROPÄISCHE PATENTSCHRIFT**

(45) Veröffentlichungstag und Bekanntmachung des Hinweises auf die Patenterteilung:  
**05.10.2011 Patentblatt 2011/40**

(21) Anmeldenummer: **01953875.0**

(22) Anmeldetag: **07.07.2001**

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

(86) Internationale Anmeldenummer:  
**PCT/DE2001/002534**

(87) Internationale Veröffentlichungsnummer:  
**WO 2002/017238 (28.02.2002 Gazette 2002/09)**

(54) **EIN SICHERHEITSSYSTEM**

A SECURITY SYSTEM

SYSTEME DE SECURITE

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

(30) Priorität: **25.08.2000 AU PQ968200**

(43) Veröffentlichungstag der Anmeldung:  
**28.05.2003 Patentblatt 2003/22**

(73) Patentinhaber: **ROBERT BOSCH GMBH**  
**70442 Stuttgart (DE)**

(72) Erfinder:  
• **CROWHURST, Peter**  
**Melbourne, VIC 3178 (AU)**  
• **PAVATICH, Frank**  
**Melbourne, VIC 3038 (AU)**

(56) Entgegenhaltungen:  
**EP-A- 0 999 103 WO-A-00/05696**  
**WO-A-00/12848**

**EP 1 314 140 B1**

Anmerkung: Innerhalb von neun Monaten nach Bekanntmachung des Hinweises auf die Erteilung des europäischen Patents im Europäischen Patentblatt kann jedermann nach Maßgabe der Ausführungsordnung beim Europäischen Patentamt gegen dieses Patent Einspruch einlegen. Der Einspruch gilt erst als eingelegt, wenn die Einspruchsgebühr entrichtet worden ist. (Art. 99(1) Europäisches Patentübereinkommen).

## Beschreibung

**[0001]** Die vorliegende Erfindung bezieht sich auf ein Sicherheitssystem, insbesondere ein passives Sicherheitssystem für Fahrzeuge.

**[0002]** Derzeit existierende passive Fahrzeug-Sicherheitssysteme für den Zugang oder die Inbetriebsetzung von Fahrzeugen verwenden fernbetätigte elektronische Schlüssel, die einen Sender einschließen, der Authentifizierungsdaten an einen in dem Fahrzeug befindlichen Empfänger überträgt, wenn ein Transponder eines Schlüssels erregt wird, wenn der Schlüssel innerhalb eines vorbestimmten Bereichs des Empfängers ist. Das zwischen dem Sender und dem Empfänger aktivierte Kommunikationsprotokoll benutzt eine Radiofrequenz-Schnittstelle zum Führen der übertragenen Daten sowie aller Daten, die von dem Fahrzeug an den Schlüssel gesandt werden. Die Radiofrequenz (RF)-Schnittstelle hat einen begrenzten Bereich, um zu gewährleisten, daß die Kommunikationsverbindung unterbrochen wird, wenn sich eine im Besitz des Schlüssels befindliche Person aus der unmittelbaren Nähe des Fahrzeugs entfernt

**[0003]** Passive Sicherheitssysteme sind leicht Angriffen unbefugter Personen ausgesetzt, die Intercept-Einrichtungen benutzen, die in die Nähe des Fahrzeugs und des Schlüssels gebracht werden. Die Einrichtung wird benutzt, um den Schlüssel zu erregen, die von dem Schlüssel übermittelten Übertragungen zu empfangen und die Übertragungen an das Fahrzeug weiterzuübertragen. Die Intercept-Einrichtung, die vielfach als Relaisstelle bezeichnet wird, umfaßt normalerweise einen Empfänger und einen Verstärker innerhalb des Bereichs des Schlüssels, um das abgefangene Signal an einen Empfänger und einen Verstärker in der Nähe des Fahrzeugs zu übertragen, um Zugang zu dem Fahrzeug zu erhalten.

**[0004]** Aus der EP-A-0 999 103 ist eine Benutzeridentifikationseinrichtung bekannt, bei der zur Abwehr von Relaisangriffen die Kommunikation zwischen Fahrzeug und Benutzeridentifikationseinheit mit wechselnden Frequenzen stattfindet. Dazu werden die vom Benutzer zum Fahrzeug zu übermittelnden Daten in Datenblöcke unterteilt, und jedem Datenblock wird eine zufällig ermittelte Funkfrequenz innerhalb eines Frequenzbandes zugeordnet.

**[0005]** Weiterhin sind aus der WO-A-0012848 ein Verfahren zur Durchführung einer schlüssellosen Zugangsberechtigungskontrolle sowie eine schlüssellose Zugangsberechtigungskontrolleinrichtung bekannt, wobei zur Erkennung eines Angriffs durch eine Relaisstelle die Phasenlage eines ursprünglich gesendeten Fragesignals mit der eines von einem ID-Geber zurückgesendeten Antwortsignals verglichen wird. Eine Veränderung der Phasenlage des Antwortsignals über eine vorgegebene Toleranz hinaus läßt dann auf eine zwischengeschaltete Relaisstelle schließen.

**[0006]** Die Spezifikation der australischen Patentanmeldungen 33933/99 und 424 19/99 beschreiben Sicher-

heitssysteme, die benutzt werden können, um Angriffe seitens Relaisstellen zu verhindern oder zu erkennen, wenn die Relaisstelle einen Breitbandverstärker benutzt, um Signale abzufangen, die zwischen dem Schlüssel und dem Fahrzeug übertragen werden, wobei eine Anzahl von verschiedenen RF-Übertragungskanälen benutzt werden. Die Relaisstelle kann entdeckt werden, wenn ein sogenannter Zweitontest verwendet wird.

**[0007]** Gemäß diesem Zweitontest, um die Anwesenheit einer Relaisstelle aufgrund der Signalstörung, die diese hervorruft, zu entdecken, überträgt der Schlüssel zwei Grundfrequenzöne. In Beantwortung der Übermittlung der Grundöne wird der Empfänger im Fahrzeug die Ööne und zwei Intermodulationstöne dritter Ordnung empfangen. Die Grundöne sind in benachbarten Frequenzkanälen C2 und C3 untergebracht, während die durch Mischen der Grundöne erzeugten Intermodulationstöne eine reduzierte Amplitude haben und sich in einem niedrigeren Frequenzkanal C1 und einem höheren Frequenzkanal C4 befinden. Ein Eingangssignalstärkenanzeiger (RSSI) im Empfänger des Fahrzeugs kann eine Messung der in jedem der Kanäle C 1 bis C4 empfangenen Energiemenge bereitstellen. Die erzeugte RSSI-Ausgabe ist eine Spannung, die proportional zu der Im-Band-Energie des in jedem der gemessenen Kanäle C1 bis C4 empfangenen Signals ist. Die RSSI für jeden Kanal kann daher zur Bestimmung einer jeglichen Variation benutzt werden, die in den Modulationstönen dritter Ordnung und durch die Einführung einer Relaisstelle eingeführt wird, und zwar aufgrund der Nichtlinearität der Verstärker der Relaisstelle. Um diese Variation zu entdecken, wird zuerst eine normale Kommunikationsverbindung zwischen dem Schlüssel und dem Fahrzeug innerhalb des vorbestimmten Bereichs hergestellt, wobei das RSSI für jeden Kanal C1 bis C4 gemessen wird, und wobei dies als eine spektrale Signatur für den Sender des Schlüssels aufgezeichnet wird. Alle zukünftigen Übermittlungen können dann auf ähnliche Weise gemessen werden um festzustellen, ob irgendeine Relaisstelle in das System eingeführt wurde, um die Menge der empfangenen Intermodulationsenergie dritter Ordnung zu variieren.

**[0008]** Es ist jedoch möglich, dass eine Relaisstelle Einrichtungen verwendet, die keinen Breitbandverstärker einbeziehen, sondern sich stattdessen separater Empfänger, Filter und Verstärker für jeden Übertragungskanal bedienen. Die Relaisstelle kann separate Sender/Empfangsstationen haben, die jeweils mit einem Empfänger und Sender ausgerüstet sind, der auf jeden Radiofrequenzkanal in dem Frequenzband, in welchem das passive Sicherheitssystem betrieben wird, dediziert ist. Die Relaisstelle würde dann das Frequenzband des Sicherheitssystems nicht abzutasten brauchen, um die Kanäle zu lokalisieren, die beide für die spektrale Authentifizierung der Daten und Transponder verwendet werden. In diesem Szenario kann der Zweitontest nicht zur Erkennung angewendet werden, um die von dem abfangenden Breitbandverstärker beim Mischen der Über-

tragungskanäle erzeugte

**[0009]** Seitenbandintermodulation zu erkennen. Demgemäß ist es wünschenswert, ein Sicherheitssystem bereitzustellen, welches zur Verhinderung dieser Art Angriff oder zumindest als eine zweckmäßige Alternative zum Einsatz kommen kann.

**[0010]** Die vorliegende Erfindung stellt ein Sicherheitssystem vor, einschließlich einem elektronischen Schlüssel, der einen Sender aufweist, und einem gesicherten Objekt mit einer Basisstation, die einen Empfänger aufweist, wobei der Sender und der Empfänger so ausgelegt sind, dass sie miteinander kommunizieren, um Authentifizierungsdaten auszutauschen, indem der Schlüssel Daten in einer Nachricht übermittelt, wobei der Sender des Schlüssels einen ersten Oszillator zur Erzeugung eines ersten Grundtons und einen zweiten Oszillator zur Erzeugung eines zweiten Grundtons aufweist, wobei die erzeugten Frequenzsignale von einem Kombinator oder Summierverstärker zur Übertragung kombiniert werden, die Nachricht des Schlüssels einen ersten Teil mit einer ersten Periode aufweist, wobei die zwei kombinierten Grundtöne mit einer ersten Übertragungssignalleistung übermittelt werden, die Nachricht einen nachfolgenden zweiten Teil mit einer nachfolgenden zweiten Periode aufweist, wobei die zwei Grundtöne mit einer zweiten Übertragungssignalleistung übermittelt werden und wobei die zweite Übertragungssignalleistung verschieden von der ersten Übertragungssignalleistung ist, die Basisstation einen Mikrocontroller und einen Filterkreis umfasst, welche eine erste Bandbreiteneinstellung für die erste und zweite Periode benutzt und die erste Bandbreiteneinstellung jeweils erste Bandbreiten für die zwei Töne und die Intermodulationsprodukte der Töne aufweist, die Basisstation einen Analog(Digital-Umsetzer umfasst, um analoge Ausgangssignale des Empfängers in digitale Form für den Mikrocontroller umzusetzen, wobei diese Signale eine RSSI Ausgabe einschließen, welche eine Spektralsignatur für den Mikrocontroller bereitstellt, und die Spektralsignatur innerhalb der ersten Bandbreite für beide Übertragungssignalleistungen jeweils mit einer gespeicherten Spektralmaske verglichen wird, um eine Relaisstelle zu erkennen.

**[0011]** Die vorliegende Erfindung stellt auch eine Kommunikationsmethode vor, die von einem Sicherheitssystem durchgeführt wird, einschließlich einem elektronischen Schlüssel, der einen Sender aufweist, und einem gesicherten Objekt mit einer Basisstation, die einen Empfänger aufweist, wobei der Sender und der Empfänger so ausgelegt sind, dass sie miteinander kommunizieren, um Authentifizierungsdaten auszutauschen, indem der Schlüssel Daten in einer Nachricht übermittelt, wobei ein erster Oszillator des Senders des Schlüssels einen ersten Grundton erzeugt und ein zweiter Oszillator des Senders einen zweiten Grundton erzeugt, wobei die erzeugten Frequenzsignale von einem Kombinator oder Summierverstärker zur Übertragung kombiniert werden, die Nachricht des Schlüssels einen ersten Teil mit einer ersten Periode aufweist, wobei die zwei kombinierten

Grundtöne mit einer ersten Übertragungssignalleistung übermittelt werden, die Nachricht einen nachfolgenden zweiten Teil mit einer nachfolgenden zweiten Periode aufweist, wobei die zwei Grundtöne mit einer zweiten Übertragungssignalleistung übermittelt werden und wobei die zweite Übertragungssignalleistung verschieden von der ersten Übertragungssignalleistung ist, wobei mittels eines Mikrocontrollers und eines Filterkreises der Basisstation eine erste Bandbreiteneinstellung für die erste und zweite Periode erfolgt und die erste Bandbreiteneinstellung jeweils erste Bandbreiten für die zwei Töne und die Intermodulationsprodukte der Töne aufweist, wobei ein Analog/Digital-Umsetzer der Basisstation analoge Ausgangssignale des Empfängers in digitale Form für den Mikrocontroller umsetzt, wobei diese Signale eine RSSI Ausgabe einschließen, welche eine Spektralsignatur für den Mikrocontroller bereitstellt, und die Spektralsignatur innerhalb der ersten Bandbreite für beide Übertragungssignalleistungen jeweils mit einer gespeicherten Spektralmaske verglichen wird, um eine Relaisstelle zu erkennen.

**[0012]** Eine bevorzugte Realisierung der vorliegenden Erfindung ist nur beispielsweise nachfolgend mit Bezug auf die beiliegenden Zeichnungen beschrieben:

Figur 1 ist eine schematische Darstellung einer bevorzugten Realisierung eines Sicherheitssystems mit Relaisstelle;

Figur 2 ist ein Blockdiagramm eines Sicherheitssystems;

Figur 3 ist ein Zeigerdiagramm für von dem Sicherheitssystem übermittelte Signale;

Figur 4 ist ein Diagramm eines verfälschten Datensignals;

Figur 5 ist ein Diagramm eines Frequenzspektrums für Zweiton-Übertragung des Systems; und

Figur 6 ist ein Diagramm eines Frequenzspektrums für Datenübermittlung des Systems.

**[0013]** Ein passives Sicherheitssystem, wie in Figuren 1 und 2 gezeigt, umfasst einen elektronischen Schlüssel 4 mit einem Sender 6 und einer Sendeantenne 7, einer Basisstation 8 mit einem Empfänger 10 und Empfangsantenne 12. Die Basisstation 8 ist an einem gesicherten Ort untergebracht, wie z.B. einem Fahrzeug, und kontrolliert den Zugang zu dem gesicherten Ort und/oder zum Starten des Fahrzeugs. Wenn der Schlüssel 4 innerhalb eines bestimmten Bereichs der Antenne 12 des Empfängers 10 herangeführt wird, erregt der Empfänger 10 den Transponder des Schlüssels 4, und veranlaßt dadurch den Sender 6, die Übermittlung an den Empfänger 10 zu beginnen. Daten werden unter Verwendung von RF-Signalen übermittelt, welche eine Kommunikationsverbindung zwischen dem Schlüssel 4 und der Basisstation 8 herstellen. Die zwischen dem Schlüssel 4 und der Basisstation 8 übermittelten Daten werden durch ein Kommunikationsprotokoll bestimmt, welches der Schlüssel 4 und die Basisstation 8 befolgen, und welches

die Übermittlung von Authentifizierungsdaten von dem Schlüssel 4 an den Empfänger 10 beinhaltet. Zugang zu dem gesicherten Bereich und/oder zum Starten des Fahrzeugs wird von der Basisstation 8 nur dann zugelassen, wenn die übermittelten Authentifizierungsdaten mit den von der Basisstation 8 gespeicherten Authentifizierungsdaten übereinstimmen.

**[0014]** Der Schlüssel 4 schließt einen Mikrocontroller 35 ein, der Steuer-Software zur Steuerung der Schlüsselkomponenten als Teil des Kommunikationsprotokolls umfaßt. Der Mikrocontroller 35 steuert den Sender 6, welcher einen ersten Oszillator 30 zur Erzeugung des ersten Grundtons 60 und einen zweiten Oszillator 32 zur Erzeugung des zweiten Grundtons 62 einschließt. Die erzeugten Frequenzsignale werden von einem Kombinator (Antennenweiche) oder Summierverstärker 34 für Übertragung auf der UHF Sendeantenne 7 kombiniert. Der Mikrocontroller 35 ist auch zur Steuerung der Oszillatoren 30 und 32 angeschlossen, so daß er einen Frequenzversatz oder eine Frequenzabweichung, gestützt auf die zu übertragenden Daten, wie nachstehend beschrieben, bewirken kann. Der Mikrocontroller 35 ist auch befähigt, Steuerdaten von der Basisstation 8 über einen Niederfrequenz-Empfänger 9 und Antenne 31 zu empfangen. Der Schlüssel 4 schließt eine Transponderschaltungsanordnung (nicht dargestellt) ein, um den Schlüssel 4 zu erregen oder zu triggern, wenn er innerhalb eines vorbestimmten Bereichs der Basisstation 8 ist. Innerhalb dieses Bereichs kann ein Erregungssignal seitens des Fahrzeugs erzeugt werden, wenn ein bestimmtes Ereignis eintritt, wie z.B. das Anheben des Türgriffes oder ähnliches. Sobald der Schlüssel 4 erregt oder aktiviert ist, wird das Kommunikationsprotokoll 4 für die Zugriffsberechtigung des Fahrzeugs in Gang gesetzt.

**[0015]** Die Basisstation 8 umfaßt einen Mikrocontroller 40, der Steuer-Software aufweist und welcher den Betrieb der Komponenten der Basisstation 8 steuert. Diese Teile umfassen einen UHF-Empranger 36, der mit der Empfangsantenne 12 verbunden ist, um eine Ausgabe der für den Mikrocontroller 40 empfangenen Daten bereitzustellen. Ein Analog(Digital-Umsetzer 38 wird verwendet, um analoge Ausgangssignale des Empfängers 36 in digitale Form für den Mikrocontroller 40 umzusetzen. Diese Signale schließen eine RSSI (Eingangssignalstärkenanzeiger)- Ausgabe ein, welche spektrale Signaturdaten für den Mikrocontroller 40 bereitstellt. Zwischenfrequenzsignale, die von dem Empfänger 36 erzeugt werden, werden an Filter 43 zum Filtern weitergeleitet und dann an den Empfänger 36 zurückgeleitet, um die von den Signalen geführten Daten auszublenden. Die Filter 43 sind geschaltete ("switched") Zwischenfrequenzfilter mit Bandbreiten, die von dem Mikrocontroller 40 in Übereinstimmung mit dem Protokoll eingestellt werden. Die Basisstation 8 hat auch einen Niederfrequenzsender 37 und Antenne 39 zur Übertragung von Daten von dem Mikrocontroller 40 an den Schlüssel 4. Der Niederfrequenzsender 37, Antennen 31 und 39 und Empfänger 9 des Schlüssels 4 sind so ausgelegt, daß eine

Niederfrequenz-Kommunikationsverbindung nur dann hergestellt wird, wenn der Schlüssel 4 und die Basisstation 8 gemeinsam innerhalb des gesicherten Bereichs untergebracht sind, z.B. innerhalb des Fahrzeugs. Zum Beispiel kann die Sendeantenne 39 in Form einer Spule sein, die in dem Zündsystem (ignition barrel) 39 untergebracht ist, so daß

**[0016]** eine Verbindung nur dann mit der Antenne 31 hergestellt wird, wenn der Schlüssel 4 in den Zündschalter des Zündsystems eingeführt wird. Die Niederfrequenzkanal-Verbindung wird benutzt, um Synchronisationskontrolldaten von der Basisstation an den Schlüssel 4 zu senden zur Verwendung wenn der Schlüssel 4 das nächste Mal erregt wird. Die Synchronisationskontrolldaten werden dazu benutzt, die Zeiten T0, T1, T2, T3 und T4 für die verschiedenen Teile oder Komponenten der in dem Zugriffsberechtigungsprotokoll übersandten Nachrichten einzustellen.

**[0017]** Das in Figur 3 dargestellte Protokoll, beginnend bei Stufen (a) und (b) beinhaltet die zwei von dem Schlüssel 4 übermittelten Grundtöne mit 100 kHz Abstand, zuerst bei geringer Leistung und dann bei hoher Leistung, und Durchführung des Zweitontests. Ein Beispiel des Frequenzspektrums der von dem Empfänger 10 während zwei Tonübertragungen empfangenen Signale ist in Figur 5 dargestellt. Falls, zum Beispiel, die Grundton-Oszillatoren 30 und 32 dafür eingestellt sind, 433,9 MHz bzw. 434,1 MHz zu übertragen, dann werden alle Intermodulationsverzerrungsprodukte "dritter Ordnung" (third order) bei den Frequenzen 433,7 MHz und 434,3 MHz, 64 bzw. 66, erscheinen. Der Mikrocontroller 40 stellt die Filter 43 so ein, daß entsprechende Bandbreitenfilter von 100 kHz Breite für jede der Frequenzen 60, 62, 64 und 66 bereitgestellt werden. Die spektrale Information innerhalb dieser Bänder wird in eine Spektralsignatur für den Mikrocontroller 40 umgesetzt und mit gespeicherter Spektralmaske verglichen, um Störung einer jeden Relaisstelle 16 gemäß dem Zweitontest zu erkennen.

**[0018]** Die Fähigkeit, eine Relaisstelle mittels des Zweitontests zu erkennen, wird durch das synchronisierte Schalten der Niederleistungs- und der Hochleistungs-Übertragungsteile (a) und (b) der übermittelten Nachricht maximiert. Die von einer Relaisstation 16 in die Intermodulationsbänder eingeführten Verzerrungsprodukte vermehren sich dreifach für jede einzelne Leistungserhöhung. Während des Anfangsübertragungsteils (a) in geringer Leistung, müßte eine Relaisstelle 16 ihren Verstärker eine beträchtliche Leistungsverstärkung oder einen beträchtlichen Leistungsgewinn zuführen, um den Abstand zwischen dem Schlüssel 4 und der Basisstation 8 des Fahrzeugs zu überbrücken. Wenn der Schlüssel 4 beginnt, die Hochleistungs-komponente (b) durch Steigerung des Leistungsgewinns der Verstärker 34 bei einer Synchronisationszeit zu übertragen, die von der Basisstation 8 vorgeschrieben wird, ist die Relaisstelle 16 nicht in der Lage, den Leistungsgewinn Verstärker sofort auszugleichen, und wird ein übertrieben verstärktes Signal an den Empfänger 10 übertragen. Falls zum Beispiel der

Schlüssel 4 eine Leistungserhöhung von 30 dB am Ende der Periode TO einführt, dann werden sich die Verzerrungsprodukte in den Intermodulationsbändern um 90 dB erhöhen. Dadurch wird gewährleistet, daß in unvorteilhaften Umständen, wenn ansonsten die Intermodulationsprodukte innerhalb des Rauschpegels (noise floor) des Empfängers 10 wären, diese Produkte zu einem Leistungspegel angehoben würden um sicherzustellen, daß sie innerhalb der MeBfähigkeit des Empfängers 10 sind.

**[0019]** Bei Stufe (c) werden die zwischen der Basisstation und dem Schlüssel zu übertragenden Authentifizierungsdaten in einem ersten Teil gesandt. Sie werden jedoch gesandt unter Verwendung von Frequenzumschaltung (frequency shift keying) und Anlegen einer Frequenzabweichung, z.B. 200 kHz, von dem gewählten Übertragungskanal. In anderen Worten wird ein niedriges Signal 70 mit einer +200 kHz Abweichung gesandt, und ein höheres Signal 72 wird mit einer -200 kHz Abweichung gesandt. Das Frequenzspektrum der von dem Empfänger 10 während der fsk-Datenübertragung empfangenen Signale ist in Figur 6 dargestellt. Da die Filter 43 des Empfängers 10 vorher auf eine Bandbreite von 100 kHz eingestellt worden sind, müssen sie abgeglichen werden, um Datenverfälschung zu vermeiden. Dementsprechend wird während einer Anfangsübertragung, wie z.B. vor oder während des Zweitontests, der Schlüssel von der Basisstation angewiesen, eine bestimmte Anzahl von Bits bei einer gesetzten Frequenzabweichung nach den Stufen (a) und (b) zu übertragen. Dementsprechend wird der Filterkreis 43 in dem Empfänger 10 geändert, um die erforderliche neue Bandbreite von 400 kHz zur richtigen Zeit bedienen zu können. Die Anzahl der zu übertragenden Bits und Frequenzabweichungen können an den Schlüssel übersandt werden unter Verwendung einer Anfangsnachricht, die durch Erkennung und Gültigkeitsprüfung des Schlüssels seitens der Basisstation ausgelöst wird. Diese Anfangsnachricht wird verschlüsselt und unter Benutzung der Niederfrequenzverbindung gesandt. Der Zeitablauf der Kommunikation ist so ausgelegt, daß die Relaisstelle unfähig ist, Filter zur richtigen Zeit anzugleichen oder zu ändern. Wenn daher die Daten mit der breiteren Frequenzabweichung gesandt werden, kann das Abfangen durch eine Relaisstelle, die schmale Bandbreiten-Filter 100 kHz benutzt, um den Zweitontest zu umgehen, an der Basisstation 8 erkannt werden, da Benutzung der schmalen Bandbreitenfilter eine Datenverfälschung, wie in Figur 4 gezeigt, einführen würde. Die in Figur 4 dargestellte Verfälschung wird durch einen 150 kHz Bandbreitenfilter eingeführt, wenn eine Frequenzabweichung von +/- 150 kHz auf die übertragenen Daten angewendet wird.

**[0020]** Bei Stufe (d) werden die zwei Grundtöne wiederum mit 100 kHz Kanalabstand übertragen. Der Grund ist der, wiederum den Zweitontest durchzuführen, um zu erkennen, ob die Relaisstelle nun die Bandbreite irgendeines an der Relaisstelle benutzten Zwischenfrequenzfilters (IF) erweitert hat. Falls zum Beispiel die Bandbreite nun auf 400 kHz erhöht worden ist, wird der Zweitontest,

der an dieser Stufe benutzt wird, in der Lage sein, die Anwesenheit des breiteren Bandbreitenfilters zu erkennen, da sich dadurch ein Mischen der Töne und der erkennbaren Intermodulation ergeben wird. Die Dauer der während dieser Nachricht versandten Töne wird wiederum während der Anfangsnachricht an den Schlüssel 4 mitgeteilt. Dies wird wiederum verhindern, daß die Relaisstelle die Filter zur richtigen Zeit während des Kommunikationsprotokolls angleicht.

**[0021]** Bei Stufe (e) wird der zweite Teil der Authentifizierungsdaten bei einer Frequenzabweichung von +/- 200 kHz überwiesen. Dies wiederum wurde vorher von der Basisstation an den Schlüssel mitgeteilt, damit die Sicherheitssystemfilter entsprechend angeglichen oder geschaltet werden können.

**[0022]** Die Zeitabläufe für jeden der Teile der von dem Schlüssel 4 übertragenen Nachricht, T0, T1, T2, T3 und T4, und gegebenenfalls der zur Übertragung der Daten in den Datenteilen (c) und (e) benutzten Frequenzabweichungen werden von der Basisstation nach jeder gültigen Erkennung des Schlüssels 4 geändert. Diese Zeitablaufs- oder Synchronisationsdaten werden dem Schlüssel 4 mit der Anfangsnachricht zugeführt; Teile der Anfangsnachricht können, wie vorstehend beschrieben, während der Übertragung von Teilen der Nachricht durch den Schlüssel übertragen werden, werden aber bevorzugterweise übersandt, wenn der Schlüssel 4 und die Basisstation 8 gemeinsam innerhalb des gesicherten Bereichs untergebracht sind, z.B. nachdem das Fahrzeug gestartet worden ist. Die neuen Synchronisationszeiten und Abweichungen werden dann für die nächste Kommunikation über die RF Schnittstelle verwendet. Man bedient sich hierbei der Zufallsauswahl (random selection) um zu vermeiden, daß die Relaisstelle 16 die Zeitabläufe und Abweichungen lernt. Die Frequenzabweichungen zur Übertragung der hohen und niedrigen Bits der Daten kann gemäß den Fähigkeiten des eingesetzten Senders 6 und Empfängers 10 variiert werden. Zum Beispiel kann die Abweichung so gering wie z.B. +/- 25 kHz sein. Die Bandbreite des von dem Empfänger 10 benutzten Filters und die angewandte Abweichung braucht einfach nur während der Übertragung der Schlüsselnachricht geändert werden, um die Anwesenheit von Filtern zu erkennen, die von einer Relaisstelle 16 benutzt werden. Falls die Frequenzabweichung während der Übertragung der Datenteile über die Bandbreite des Filters einer Relaisstelle 16 hinausgeht, dann werden die Daten von der Relaisstelle 16 verfälscht und von der Basisstation 8 erkannt. Falls die Filter der Relaisstelle breit genug sind, daß die Daten nicht verfälscht werden, dann werden die zwei Töne von den Filtern durchgelassen und die erkennbaren Intermodulationsprodukte werden erzeugt. Auch wenn die Relaisstelle genügend durchgebildet ist, um Zwischenfrequenzfilter zu schalten, um die Änderung in der Bandbreite auszugleichen, ist die Relaisstelle 16 unfähig festzustellen, wann die Filterbandbreite geändert werden müßte. Um Erfolg zu haben, würde die Relaisstelle die Filterbandbreiten genau zum richtigen Zeit-

punkt ändern müssen, sonst wird der Zweitontest ihre Anwesenheit aufdecken oder aber die Daten werden verfälscht.

**[0023]** Das Protokoll kann abhängig von den Sicherheitserfordernissen für den gesicherten Bereich variiert werden. Zum Beispiel vielleicht die Entscheidung getroffen werden, daß die Unterteilung der Authentifizierungsdaten in zwei Teile nicht erforderlich ist, und daß alle Daten in der Periode anschließend an die ersten Zweitontests gesandt werden, wodurch sich die Notwendigkeit für Teil (d) erübrigt. Falls die Daten in einen Teil kombiniert werden, können sie mit den Niederleistungs- und Hochleistungs- Zweitontest-Teilen gesandt werden oder dem Zweitontest der einzelnen einheitlichen Leistung.

**[0024]** Synchronisierung erfolgt von dem Punkt an, wo der Schlüssel 4 erregt ist und gültige Kommunikation mit der Basisstation 8 einleitet. Diese gültige Kommunikation kann durch den Benutzer des Schlüssels, wie zuvor beschrieben, eingeleitet werden.

### Patentansprüche

1. Ein Sicherheitssystem (4,8), einschließlich einem elektronischen Schlüssel (4), der einen Sender (6) aufweist, und einem gesicherten Objekt mit einer Basisstation (8), die einen Empfänger (10) aufweist, wobei der Sender (6) und der Empfänger (10) so ausgelegt sind, dass sie miteinander kommunizieren, um Authentifizierungsdaten auszutauschen, indem der Schlüssel (4) Daten in einer Nachricht übermittelt die Teile mit jeweils vorherbestimmter Periode (T0, ..., T4) mit Übertragungssignalvariationen umfaßt, wobei

- der Sender (6) des Schlüssels (4) einen ersten Oszillator (30) zur Erzeugung eines ersten Grundtons (60) und einen zweiten Oszillator (32) zur Erzeugung eines zweiten Grundtons (62) aufweist, wobei die erzeugten Frequenzsignale von einem Kombinator oder Summierverstärker (34) zur Übertragung kombiniert werden,
- die Nachricht des Schlüssels (4) einen ersten Teil (a) mit einer ersten Periode (T0) aufweist, wobei die zwei kombinierten Grundtöne mit einer ersten Übertragungssignalleistung übermittelt werden,
- die Nachricht einen nachfolgenden zweiten Teil (b) mit einer nachfolgenden zweiten Periode (T1) aufweist, wobei die zwei Grundtöne (60, 62) mit einer zweiten Übertragungssignalleistung übermittelt werden und wobei die zweite Übertragungssignalleistung verschieden von der ersten Übertragungssignalleistung ist,
- die Basisstation (8) einen Mikrocontroller (40) und einen Filterkreis (43) umfaßt, welche eine erste Bandbreiteneinstellung für die erste und

zweite Periode (T0, T1) benutzt und die erste Bandbreiteneinstellung jeweils erste Bandbreiten für die zwei Töne und die Intermodulationsprodukte der Töne aufweist,

- die Basisstation (8) einen Analog/Digital-Umsetzer (38) umfaßt, um analoge Ausgangssignale des Empfängers (10) in digitale Form für den Mikrocontroller umzusetzen, wobei diese Signale eine RSSI Ausgabe einschließen, welche eine Spektralsignatur für den Mikrocontroller (40) bereitstellt,

- und die Spektralsignatur innerhalb der ersten Bandbreite für beide Übertragungssignalleistungen jeweils mit einer gespeicherten Spektralmaske verglichen wird, um eine Relaisstelle zu erkennen.

2. Ein Sicherheitssystem (4, 8) nach Anspruch 1, **dadurch gekennzeichnet, dass** die Nachricht einen nachfolgenden dritten Teil (c) mit einer nachfolgenden dritten Periode (T3) aufweist, wobei die Basisstation (8) eine zweite Bandbreiten ein stellung für die dritte Periode (T3) benutzt und wobei die erste Bandbreiteneinstellung eine Bandbreite hat, die schmäler ist als die Bandbreite der Frequenzabweichung der zweiten Bandbreiteneinstellung.

3. Ein Sicherheitssystem (4, 8) nach Anspruch 1, **dadurch gekennzeichnet, dass** die Perioden (T0, ..., T4) von der Basisstation (8) eingestellt werden und an den Schlüssel (4) kommuniziert werden.

4. Ein Sicherheitssystem (4, 8) nach Anspruch 3, **dadurch gekennzeichnet, dass** die Perioden (T0, ..., T4) mittels Zufallsauswahl bestimmt werden.

5. Ein Sicherheitssystem (4, 8) nach Anspruch 3, **dadurch gekennzeichnet, dass** die Perioden (T0, ..., T4) geändert und kommuniziert werden, wenn der Schlüssel (4) als gültig befunden worden ist.

6. Ein Sicherheitssystem (4, 8) nach einem der vorhergehenden Ansprüche 3 bis 5, **dadurch gekennzeichnet, dass** die Perioden (T0, ..., T4) kommuniziert werden, wenn der Schlüssel (4) sich in dem gesicherten Objekt befindet.

7. Eine Kommunikationsmethode, die von einem Sicherheitssystem (4, 8) durchgeführt wird, einschließlich einem elektronischen Schlüssel (4), der einen Sender (6) aufweist, und einem gesicherten Objekt mit einer Basisstation (8), die einen Empfänger (10) aufweist, wobei der Sender (6) und der Empfänger (10) so ausgelegt sind, dass sie miteinander kommunizieren, um Authentifizierungsdaten auszutauschen, indem der Schlüssel (4) Daten in einer Nachricht übermittelt, wobei

- ein erster Oszillator (30) des Senders (6) des Schlüssels (4) einen ersten Grundton (60) erzeugt und ein zweiter Oszillator (32) des Senders (6) einen zweiten Grundton (62) erzeugt, wobei die erzeugten Frequenzsignale von einem Kombinator oder Summierverstärker (34) zur Übertragung kombiniert werden,
- die Nachricht des Schlüssels (4) einen ersten Teil (a) mit einer ersten Periode (T0) aufweist, wobei die zwei kombinierten Grundtöne mit einer ersten Übertragungssignalleistung übermittelt werden,
- die Nachricht einen nachfolgenden zweiten Teil (b) mit einer nachfolgenden zweiten Periode (T1) aufweist, wobei die zwei Grundtöne (60, 62) mit einer zweiten Übertragungssignalleistung übermittelt werden und wobei die zweite Übertragungssignalleistung verschieden von der ersten Übertragungssignalleistung ist,
- wobei mittels eines Mikrocontrollers (40) und eines Filterkreises (43) der Basisstation (8) eine erste Bandbreiteneinstellung für die erste und zweite Periode (T0, T1) erfolgt und die erste Bandbreiteneinstellung jeweils erste Bandbreiten für die zwei Töne und die Intermodulationsprodukte der Töne aufweist,
- wobei ein Analog/Digital-Umsetzer (38) der Basisstation (8) analoge Ausgangssignale des Empfängers (10) in digitale Form für den Mikrocontroller umsetzt, wobei diese Signale eine RSSI Ausgabe einschließen, welche eine Spektralsignatur für den Mikrocontroller (40) bereitstellt,
- und die Spektralsignatur innerhalb der ersten Bandbreite für beide Übertragungssignalleistungen jeweils mit einer gespeicherten Spektralmaske verglichen wird, um eine Relaisstelle zu erkennen.
8. Eine Kommunikationsmethode nach Anspruch 7, **dadurch gekennzeichnet, dass** die Nachricht einen nachfolgenden dritten Teil (c) mit einer nachfolgenden dritten Periode (T3) aufweist, wobei für die Basisstation (8) eine zweite Bandbreiteneinstellung für die dritte Periode (T3) benutzt und wobei die erste und die zweite Bandbreiteneinstellung jeweils erste und zweite Bandbreiten für zwei Töne und Intermodulationsprodukte der Töne aufweisen.
9. Eine Kommunikationsmethode nach Anspruch 8, **dadurch gekennzeichnet, dass** die erste Bandbreiteneinstellung eine Bandbreite hat, die schmaler ist als die Bandbreite der Frequenzabweichung der zweiten Bandbreiteneinstellung.
10. Eine Kommunikationsmethode nach einem der vorhergehenden Ansprüche 7 bis 9, **dadurch gekennzeichnet, dass** die Perioden (T0, ..., T4) von der Basisstation (8) eingestellt werden und an den Schlüssel (4) kommuniziert werden.
11. Eine Kommunikationsmethode nach Anspruch 10, **dadurch gekennzeichnet, dass** die Perioden (T0, ..., T4) mittels Zufallsauswahl bestimmt werden.
12. Eine Kommunikationsmethode nach Anspruch 10, **dadurch gekennzeichnet, dass** die Perioden (T0, ..., T4) geändert und kommuniziert werden, wenn der Schlüssel (4) als gültig befunden worden ist.
13. Eine Kommunikationsmethode nach einem der vorhergehenden Ansprüche 10 bis 12, **dadurch gekennzeichnet, dass** die Perioden (T0, ..., T4) kommuniziert werden, wenn der Schlüssel (4) sich in dem gesicherten Objekt befindet.

### Claims

1. Security system (4, 8), including an electronic key (4), which has a transmitter (6), and a protected object having a base station (8) which has a receiver (10), wherein the transmitter (6) and the receiver (10) are designed such that they communicate with one another in order to interchange authentication data by virtue of the key (4) transmitting data in a message which comprises portions having respective predetermined periods (T0, ..., T4) with transfer signal variations, wherein
- the transmitter (6) in the key (4) has a first oscillator (30) for producing a first fundamental tone (60) and a second oscillator (32) for producing a second fundamental tone (62), wherein the frequency signals produced are combined by a combiner or summing amplifier (34) for the purpose of transfer,
  - the message from the key (4) has a first portion (a) with a first period (T0), wherein the two combined fundamental tones are transmitted at a first transfer signal power,
  - the message has a subsequent second portion (b) with a subsequent second period (T1), wherein the two fundamental tones (60, 62) are transmitted at a second transfer signal power and wherein the second transfer signal power is different from the first transfer signal power,
  - the base station (8) comprises a microcontroller (40) and a filter circuit (43) which uses a first bandwidth setting for the first and second periods (T0, T1), and the first bandwidth setting has respective first bandwidths for the two tones and the intermodulation products of the tones,
  - the base station (8) comprises an analogue/

- digital converter (38) in order to convert analogue output signals from the receiver (10) into digital form for the microcontroller, wherein these signals include an RSSI output which provides a spectral signature for the microcontroller (40),
- and the spectral signature is compared with the respective stored spectral mask within the first bandwidth for both transfer signal powers in order to identify a relay point.
2. Security system (4, 8) according to Claim 1, **characterized in that** the message has a subsequent third portion (c) with a subsequent third period (T3), wherein the base station (8) uses a second bandwidth setting for the third period (T3) and wherein the first bandwidth setting has a bandwidth which is narrower than the bandwidth of the frequency deviation in the second bandwidth setting.
  3. Security system (4, 8) according to Claim 1, **characterized in that** the periods (T0, ..., T4) are set by the base station (8) and are communicated to the key (4).
  4. Security system (4, 8) according to Claim 3, **characterized in that** the periods (T0, ..., T4) are determined by means of random selection.
  5. Security system (4, 8) according to Claim 3, **characterized in that** the periods (T0, ..., T4) are changed and communicated when the key (4) has been found to be valid.
  6. Security system (4, 8) according to one of the preceding claims (3, to 5, **characterized in that** the periods (T0, ..., T4) are communicated when the key (4) is in the protected object.
  7. Communication method which is carried out by a security system (4, 8), including an electronic key (4), which has a transmitter (6), and a protected object having a base station (8) which has a receiver (10), wherein the transmitter (6) and the receiver (10) are designed such that they communicate with one another in order to interchange authentication data by virtue of the key (4) transmitting data in a message which comprises portions having respective predetermined periods (T0, ..., T4) with transfer signal variations, wherein
    - a first oscillator (30) in the transmitter (6) in the key (4) produces the first fundamental tone (60) and a second oscillator (32) in the transmitter (6) produces a second fundamental tone (62), wherein the frequency signals produced are combined by a combiner or summing amplifier (34) for the purpose of transfer,
    - the message from the key (4) has a first portion (a) with a first period (T0), wherein the two combined fundamental tones are transmitted at a first transfer signal power,
    - the message has a subsequent second portion (b) with a subsequent second period (T1), wherein the two fundamental tones (60, 62) are transmitted at a second transfer signal power and wherein the second transfer signal power is different from the first transfer signal power,
    - wherein a microcontroller (40) and a filter circuit (43) in the base station (8) are used to make a first bandwidth setting for the first and second periods (T0, T1), and the first bandwidth setting has respective first bandwidths for the two tones and the intermodulation products of the tones,
    - wherein an analogue/digital converter (38) in the base station (8) converts analogue output signals from the receiver (10) into digital form for the microcontroller, wherein these signals include an RSSI output which provides a spectral signature for the microcontroller (40),
    - and the spectral signature is compared with the respective stored spectral mask within the first bandwidth for both transfer signal powers in order to identify a relay point.
  8. Communication method according to Claim 7, **characterized in that** the message has a subsequent third portion (c) with a subsequent third period (T3), wherein the base station (8) uses a second bandwidth setting for the third period (T3) and wherein the first and second bandwidth settings each have first and second bandwidths for two tones and intermodulation products of the tones.
  9. Communication method according to Claim 8, **characterized in that** the first bandwidth setting has a bandwidth which is narrower than the bandwidth of the frequency deviation in the second bandwidth setting.
  10. Communication method according to one of the preceding Claims 7 to 9, **characterized in that** the periods (T0, ..., T4) are set by the base station (8) and are communicated to the key (4).
  11. Communication method according to Claim 10, **characterized in that** the periods (T0, ..., T4) are determined by means of random selection.
  12. Communication method according to Claim 10, **characterized in that** the periods (T0, ..., T4) are changed and communicated when the key (4) has been found to be valid.
  13. Communication method according to one of the preceding Claims 10 to 12, **characterized in that** the

periods (T0, ..., T4) are communicated when the key (4) is in the protected object.

## Revendications

1. Système de sécurité (4, 8), incluant une clé électronique (4), laquelle présente un émetteur (6), et un objet sécurisé doté d'une station de base (8), laquelle présente un récepteur (10), l'émetteur (6) et le récepteur (10) étant conçus de telle sorte qu'ils communiquent entre eux pour échanger des données d'authentification en ce que la clé (4) communique des données dans un message, lequel inclut des parties avec des périodes (T0, ..., T4) à chaque fois prédéterminées avec des variations du signal de transmission,

- l'émetteur (6) de la clé (4) présentant un premier oscillateur (30) pour générer une première fréquence fondamentale (60) et un deuxième oscillateur (32) pour générer une deuxième fréquence fondamentale (62), les signaux de fréquence générés étant combinés par un combinateur ou un amplificateur additionneur (34) en vue de leur transmission,

- le message de la clé (4) présentant une première partie (a) avec une première période (T0), les deux fréquences fondamentales combinées étant communiquées avec une première puissance de signal de transmission,

- le message présentant une deuxième partie (b) suivante avec une deuxième période (T1) suivante, les deux fréquences fondamentales (60, 62) étant communiquées avec une deuxième puissance de signal de transmission et la deuxième puissance de signal de transmission étant différente de la première puissance de signal de transmission,

- la station de base (8) comprenant un microcontrôleur (40) et un circuit filtrant (43), laquelle utilise un premier réglage de largeur de bande pour la première et la deuxième période (T0, T1), et le premier réglage de largeur de bande présentant à chaque fois des premières largeurs de bande pour les deux tonalités et les produits d'intermodulation des tonalités,

- la station de base (8) comprenant un convertisseur analogique/numérique (38) pour convertir les signaux de sortie analogiques du récepteur (10) sous forme numérique pour le microcontrôleur, ces signaux incluant une édition RSSI qui fournit une signature spectrale pour le microcontrôleur (40),

- et la signature spectrale étant comparée à l'intérieur de la première largeur de bande pour les deux puissances de signal de transmission à chaque fois avec un masque spectral mémorisé

afin de détecter un point relais.

2. Système de sécurité (4, 8) selon la revendication 1, **caractérisé en ce que** le message présente une troisième partie (c) suivante avec une troisième période (T3) suivante, la station de base (8) utilisant un deuxième réglage de largeur de bande pour la troisième période (T3) et le premier réglage de largeur de bande ayant une largeur de bande qui est plus étroite que la largeur de bande de l'écart en fréquence du deuxième réglage de largeur de bande.
3. Système de sécurité (4, 8) selon la revendication 1, **caractérisé en ce que** les périodes (T0, ..., T4) sont réglées par la station de base (8) et sont communiquées à la clé (4).
4. Système de sécurité (4, 8) selon la revendication 3, **caractérisé en ce que** les périodes (T0, ..., T4) sont déterminées au moyen d'une sélection aléatoire.
5. Système de sécurité (4, 8) selon la revendication 3, **caractérisé en ce que** les périodes (T0, ..., T4) sont modifiées et sont communiquées lorsque la clé (4) a été constatée valide.
6. Système de sécurité (4, 8) selon l'une des revendications précédentes 3 à 5, **caractérisé en ce que** les périodes (T0, ..., T4) sont communiquées lorsque la clé (4) se trouve dans l'objet sécurisé.
7. Procédé de communication qui est mis en oeuvre par un système de sécurité (4, 8), incluant une clé électronique (4), laquelle présente un émetteur (6), et un objet sécurisé doté d'une station de base (8), laquelle présente un récepteur (10), l'émetteur (6) et le récepteur (10) étant conçus de telle sorte qu'ils communiquent entre eux pour échanger des données d'authentification en ce que la clé (4) communique des données dans un message, lequel inclut des parties avec des périodes (T0, ..., T4) à chaque fois prédéterminées avec des variations du signal de transmission,
  - un premier oscillateur (30) de l'émetteur (6) de la clé (4) générant une première fréquence fondamentale (60) et un deuxième oscillateur (32) de l'émetteur (6) générant une deuxième fréquence fondamentale (62), les signaux de fréquence générés étant combinés par un combinateur ou un amplificateur additionneur (34) en vue de leur transmission,
  - le message de la clé (4) présentant une première partie (a) avec une première période (T0), les deux fréquences fondamentales combinées étant communiquées avec une première puissance de signal de transmission,

- le message présentant une deuxième partie (b) suivante avec une deuxième période (T1) suivante, les deux fréquences fondamentales (60, 62) étant communiquées avec une deuxième puissance de signal de transmission et la deuxième puissance de signal de transmission étant différente de la première puissance de signal de transmission,
  - un premier réglage de largeur de bande pour la première et la deuxième période (T0, T1) étant effectué au moyen d'un microcontrôleur (40) et d'un circuit filtrant (43) de la station de base (8) et le premier réglage de largeur de bande présentant à chaque fois des premières largeurs de bande pour les deux tonalités et les produits d'intermodulation des tonalités,
  - un convertisseur analogique/numérique (38) de la station de base (8) convertissant les signaux de sortie analogiques du récepteur (10) sous forme numérique pour le microcontrôleur, ces signaux incluant une édition RSSI qui fournit une signature spectrale pour le microcontrôleur (40),
  - et la signature spectrale étant comparée à l'intérieur de la première largeur de bande pour les deux puissances de signal de transmission à chaque fois avec un masque spectral mémorisé afin de détecter un point relais.
8. Procédé de communication selon la revendication 7, **caractérisé en ce que** le message présente une troisième partie (c) suivante avec une troisième période (T3) suivante, la station de base (8) utilisant un deuxième réglage de largeur de bande pour la troisième période (T3) et le premier ainsi que le deuxième réglage de largeur de bande présentant respectivement une première et une deuxième largeur de bande pour deux fréquences et les produits d'intermodulation des fréquences.
9. Procédé de communication selon la revendication 8, **caractérisé en ce que** le premier réglage de largeur de bande possède une largeur de bande qui est plus étroite que la largeur de bande de l'écart en fréquence du deuxième réglage de largeur de bande.
10. Procédé de communication selon l'une des revendications précédentes 7 à 9, **caractérisé en ce que** les périodes (T0, ..., T4) sont réglées par la station de base (8) et sont communiquées à la clé (4).
11. Procédé de communication selon la revendication 10, **caractérisé en ce que** les périodes (T0, ..., T4) sont déterminées au moyen d'une sélection aléatoire.
12. Procédé de communication selon la revendication
- 10, **caractérisé en ce que** les périodes (T0, ..., T4) sont modifiées et sont communiquées lorsque la clé (4) a été constatée valide.
13. Procédé de communication selon l'une des revendications précédentes 10 à 12, **caractérisé en ce que** les périodes (T0, ..., T4) sont communiquées lorsque la clé (4) se trouve dans l'objet sécurisé.

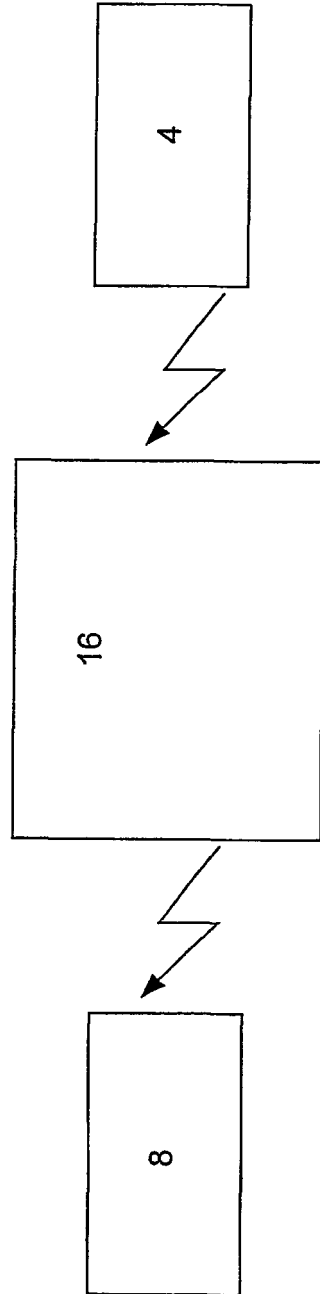


Figure 1

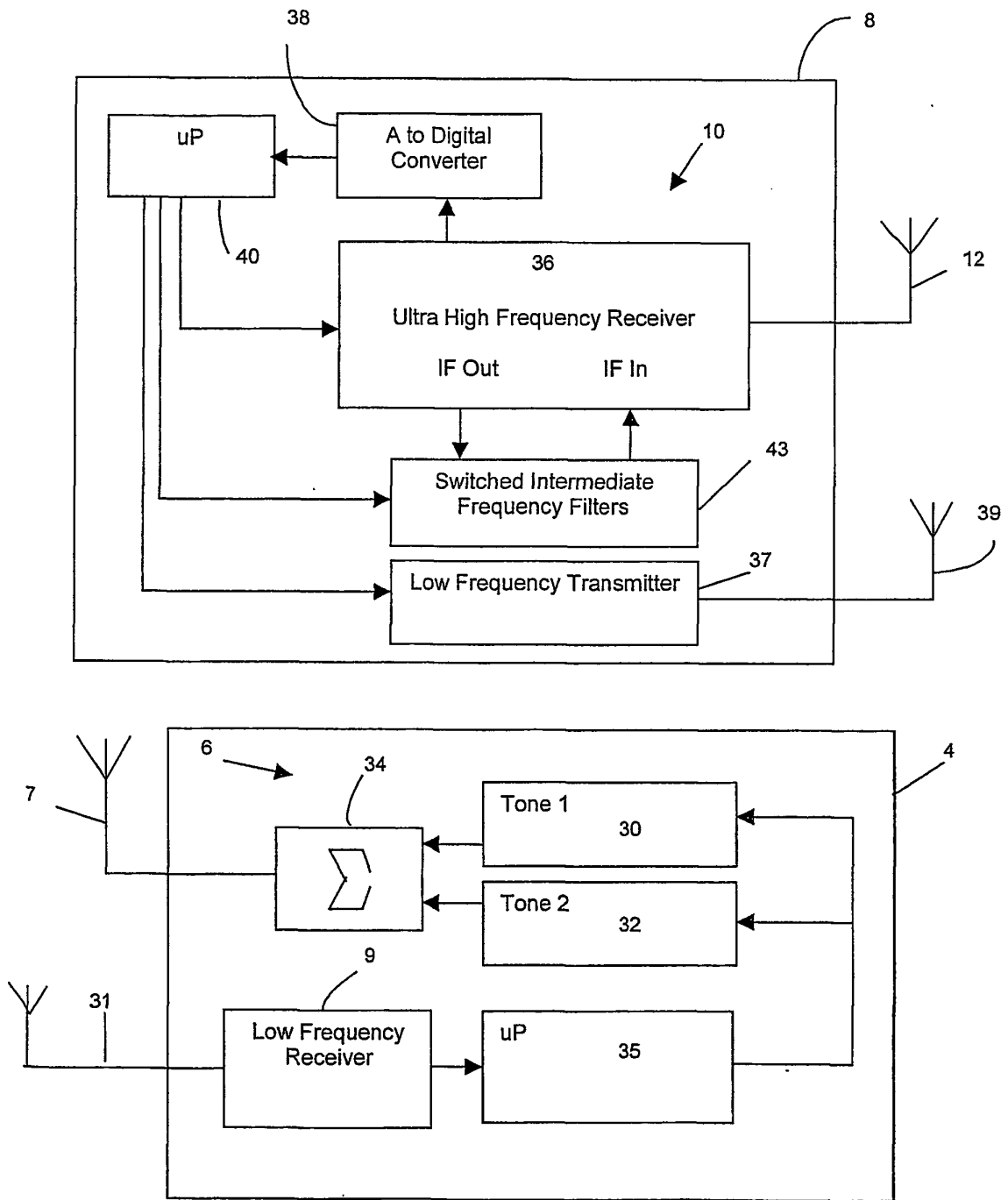


Figure 2

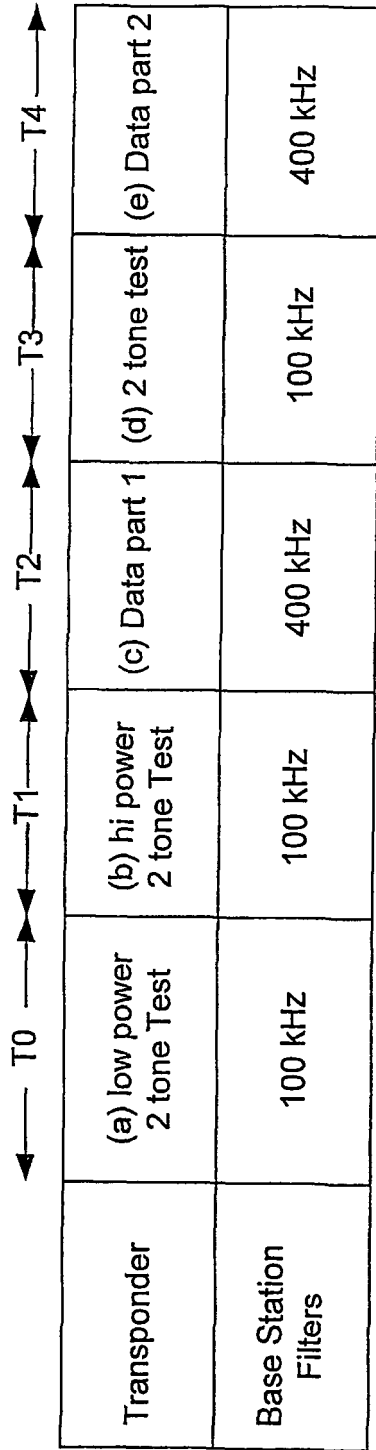


Figure 3

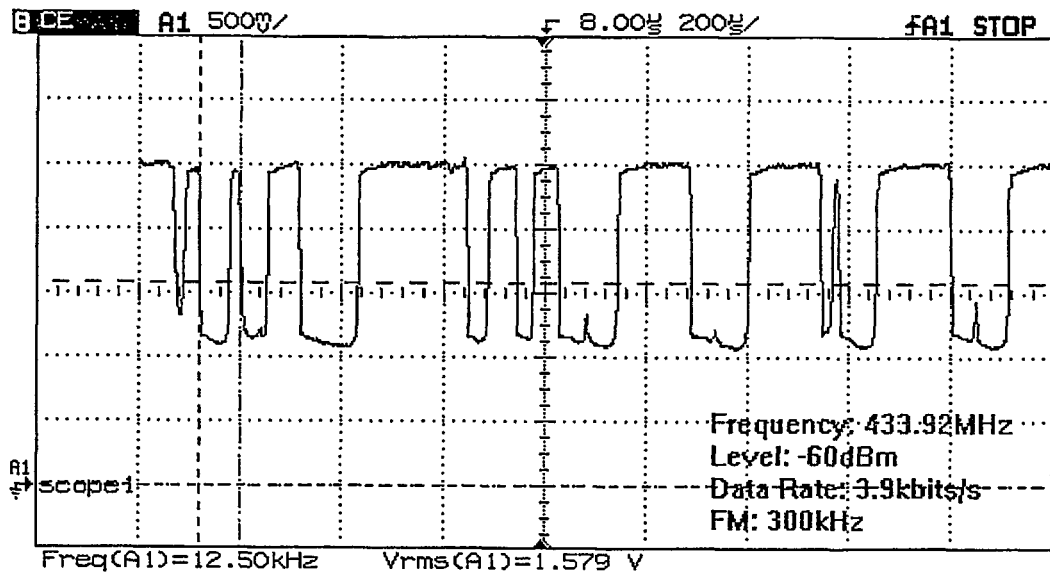


Figure 4

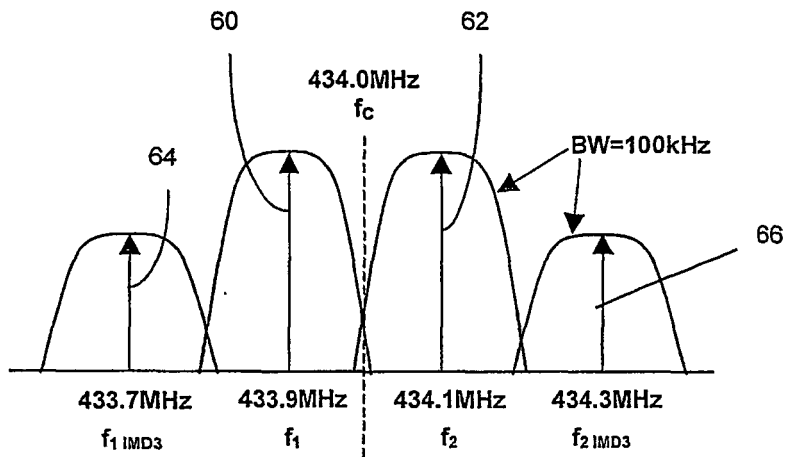


Figure 5

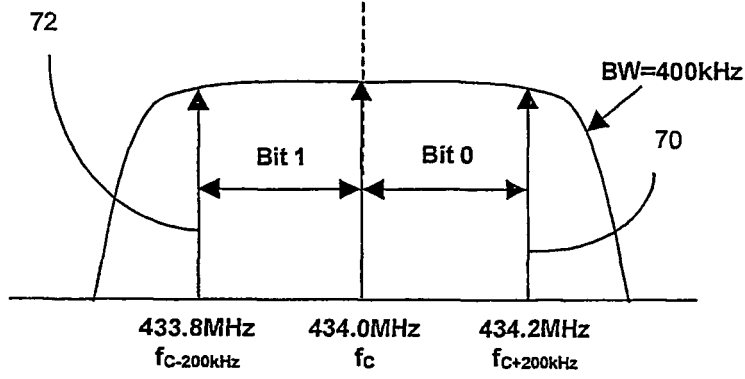


Figure 6

**IN DER BESCHREIBUNG AUFGEFÜHRTE DOKUMENTE**

*Diese Liste der vom Anmelder aufgeführten Dokumente wurde ausschließlich zur Information des Lesers aufgenommen und ist nicht Bestandteil des europäischen Patentdokumentes. Sie wurde mit größter Sorgfalt zusammengestellt; das EPA übernimmt jedoch keinerlei Haftung für etwaige Fehler oder Auslassungen.*

**In der Beschreibung aufgeführte Patentdokumente**

- EP 0999103 A [0004]
- WO 0012848 A [0005]
- AU 3393399 [0006]
- AU 4241999 [0006]