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

(11) Veröffentlichungsnummer: **0 265 728**
A2

(12) EUROPÄISCHE PATENTANMELDUNG

(21) Anmeldenummer: **87114656.9**

(51) Int. Cl.4: **E05B 49/00**

(22) Anmeldetag: **07.10.87**

(30) Priorität: **29.10.86 DE 3636822**

(43) Veröffentlichungstag der Anmeldung: **04.05.88 Patentblatt 88/18**

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

(71) Anmelder: **Wilhelm Ruf KG**
Schwanthaler Strasse 18
D-8000 München 2(DE)

(72) Erfinder: **Keller, Herbert**
Mühlenstrasse 17
D-8212 Übersee(DE)

(74) Vertreter: **von Bülow, Tam, Dipl.-Ing., Dipl.-Wirtsch.-Ing. et al**
SAMSON & BÜLOW Widenmayerstrasse 5
D-8000 München 22(DE)

(54) Elektronische Fernbetätigungseinrichtung, insbesondere für Zentralverriegelungsanlagen von Kraftfahrzeugen.

(57) Die elektronische Fernbetätigungseinrichtung arbeitet nach dem bekannten Prinzip der Code-Fortschaltung, bei dem nach jedem Sende-/Empfangsvorgang ein anderes Code-Wort verwendet wird. Bei der Erfindung wird das jeweils neue Code-Wort aus einem gespeicherten Ur-Code-Wort (1, 19) und dem bisherigen Code-Wort (3; 17, 21) durch logische Verknüpfung (2, 20) nach einer vorgegebenen Funktion neu erzeugt. Im Empfänger werden bei Nichtübereinstimmung zwischen empfangenen und empfangsseitig neu ermitteltem Code-Wort vorwärts fortschaltend weitere Code-Worte (CDW x + 1 ..., CDW x + n) erzeugt. Wird dabei keine Übereinstimmung festgestellt, so schaltet der Empfänger auf erhöhte Sicherheit um, bei der zwei unmittelbar aufeinanderfolgende Code-Worte übereinstimmen müssen.

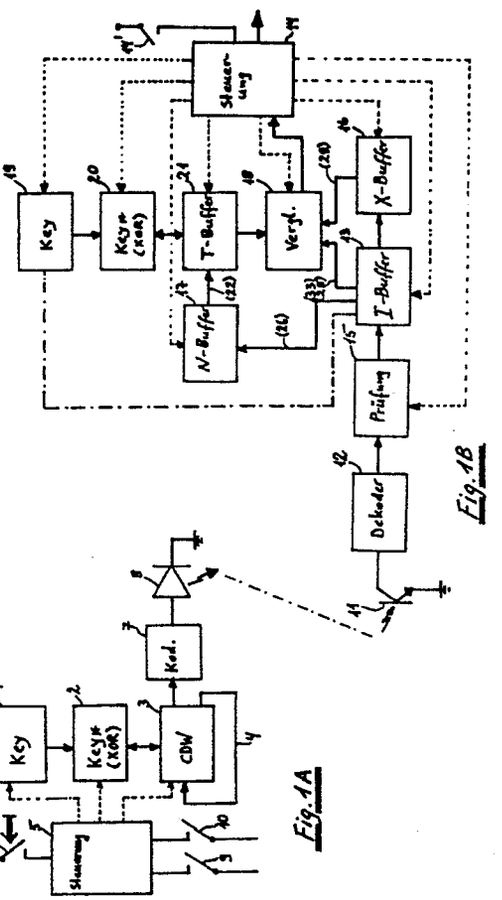

Fig.1B

Fig.1A

EP 0 265 728 A2

Elektronische Fernbetätigungseinrichtung, insbesondere für Zentralverriegelungsanlagen von Kraftfahrzeugen

Die Erfindung bezieht sich auf eine elektronische Fernbetätigungseinrichtung gemäß dem Oberbegriff des Patentanspruches 1. Aus der DE-PS 32 44 049 ist eine fernbetätigbare Zentralveriegelungsanlage für Kraftfahrzeuge der oben genannten Art bekannt, bei der im Sender und Empfänger jeweils die gleiche Reihe von Code-Bits gespeichert ist, die eine Anzahl geordneter Code-Wörter, die jeweis mehrere Bits haben, darstellt. Pro Betätigung des Senders werden im Sender und Empfänger die Code-Bits um eine konstante Anzahl von Bit-Stellen, die der Länge eines Code-Wortes entspricht, weitergeschaltet. Beim letzten Wort wird auf das erste Wort zurückgeschaltet. Bei jeder Betätigung wird überprüft, ob das ausgesandte Code-Wort und das im Empfänger anstehende, aktuelle Code-Wort übereinstimmen. Bei Übereinstimmung wird die Tür geöffnet. Bei dieser Anlage ist eine Synchronisation zwischen Sender und Empfänger unbedingt nötig. Falls diese Synchronisation verlorengegangen ist, beispielsweise durch Betätigung des Senders außerhalb der Reichweite des Empfängers (sog. Leerbetätigung), kann eine Übereinstimmung nicht mehr gefunden werden. Hierfür sieht die bekannte Anlage vor, daß durch Drücken einer Sondertaste Sender und Empfänger wieder auf ein festgelegtes Wort synchronisiert werden.

Diese Anlage hat den Nachteil, daß der Speicherplatzbedarf im Sender und Empfänger direkt von der Anzahl der Kombinationsmöglichkeiten abhängt. Aus Sicherheitsgründen ist es sinnvoll, eine möglichst große Anzahl von Code-Wörtern vorzusehen, um damit den Zyklus, in dem sich die Code-Wörter wiederholen, sehr lang zu machen. Andernfalls könnte durch unbefugtes "Abhören" des Codes dieser zu leicht "geknackt" werden. Besonders kritisch für die "Abhörsicherheit" ist jedoch der Synchronisationsbefehl. Ermittelt jemand unbefugt den Code des Synchronisationsbefehles, so muß er nur noch das sich bei Synchronisation einstellende Code-Wort kennen und braucht nicht mehr die gesamte Bitfolge zu ermitteln.

Der Sicherheitsvorteil eines sich ständig ändernden Codes (sog. Code-Fortschaltung) wird also durch den Zwang zur Synchronisation wieder wesentlich abgeschwächt, da die Synchronisation im Ergebnis die Code-Fortschaltung hinfällig macht. Besonders deutlich wird dies bei einer Grenzwertbetrachtung. Synchronisiert man bei jeder Über tragung, so erkennt man, daß sich veränderbarer Code und Synchronisation widersprechen.

Das Prinzip der Code-Fortschaltung ist auch aus der DE-OS 33 20 721 bekannt. Dort wird mit jedem ausgesendeten Wort eine Zusatzinformation übertragen, die eine Information darüber enthält, welche Code-Nummer aus dem im Empfänger gespeicherten Vorrat auszuwählen ist. Auch hier ist eine Synchronisation zwischen Sender und Empfänger erforderlich. Zur Erhöhung der Sicherheit ist dort vorgeschlagen, daß eine Nachsynchronisation nur in Richtung zu höheren Code-Nummern möglich ist, was unbefugt aufgezeichnete Codes entwertet. Weiterhin soll der Empfänger eine Nachsynchronisation nur in einem engen Intervall von Code-Nummern annehmen. Auch hier wird aber eine Synchronisations-Information über die Sendestrecke geschickt und kann daher aufgezeichnet werden.

Die Probleme der Synchronisation bei Code-Fortschaltung sind auch in den DE-OSen 32 34 538, 34 07 436 und 34 07 469 beschrieben.

Aufgabe der Erfindung ist es, die gattungsbildende elektronische Fernbetätigungseinrichtung dahingehend zu verbessern, daß sie bei geringem Speicherplatzbedarf für die geordnete Menge von Code-Wörtern höhere Sicherheit bietet.

Diese Aufgabe wird bei der gattungsbildenden Einrichtung durch die im Kennzeichenteil des Patentanspruches 1 angegebenen Merkmale gelöst. Vorteilhafte Ausgestaltung und Weiterbildungen der Erfindung sind den Unteransprüchen zu entnehmen.

Kurz zusammengefaßt arbeitet die Erfindung ebenfalls nach dem Prinzip der Code-Fortschaltung. Es wird jedoch nur sehr geringer Speicherplatz benötigt, da die einzelnen Code-Wörter laufend neu aus einem einzigen Ur-Wort ermittelt werden, womit sich eine enorme Vielzahl von Kombinationsmöglichkeiten ergibt. Weiterhin müssen Sender und Empfänger bei der Erfindung nicht starr synchronisiert sein. Vielmehr synchronisiert sich der Empfänger automatisch auf den Sender, ohne daß es externer Maßnahmen durch den Benutzer bedarf. Als vorgegebene Funktion für die logische Verknüpfung kann im Prinzip jeder "Pseudo-Zufallsgenerator" benutzt werden, sofern die "Zufallsfolge" eindeutig determiniert ist, so daß zwei unabhängige Pseudo-Zufallsgeneratoren in einem Sender-/Empfängerpaar dieselbe Zufallsfolge erzeugen.

Mit den Merkmalen des Anspruches 2 wird die Sicherheit weiter erhöht. Versucht jemand unbefugt mit einem falschen Code das Schloß zu öffnen, so wird auf erhöhte Sicherheit umgeschaltet. Ist die Wahrscheinlichkeit, durch Zufall das richtige Code-

wort zu finden $1/2^n$, so wird sie bei der erhöhten Sicherheit zu $1/2^{2n}$. Es sei darauf hingewiesen, daß bei einer Unterkombination der Ansprüche 1 und 2 die Anzahl n (von Anspruch 1) gleich Null sein kann, womit dann ständig mit der erhöhten Sicherheit der Doppelwortübereinstimmung gearbeitet wird.

Mit den Merkmalen der Ansprüche 3 bis 5 erhält man die für die Codefortschaltung benötigten neuen Code-Wörter, ohne daß sie alle gespeichert sein müssen, wobei die Merkmale des Anspruches 5 eine zusätzliche Sicherheit dahingehend bieten, daß der Code nicht "geknackt" werden kann.

Mit Anspruch 6 erreicht man, daß Sender und Empfänger nicht durch Fremdsender derart beeinflußt werden können, daß sie in ihrer Codefortschaltung so weit auseinanderliegen, daß sie nicht mehr zusammenfinden.

Mit Anspruch 7 erreicht man, daß Fremdsysteme beispielsweise Schlüssel anderer Automarken, die nach demselben Prinzip arbeiten, keine Code-Fortschaltung im Empfänger auslösen sowie auch die Möglichkeiten, mehrere voneinander unabhängige Funktionen vorzusehen wie z.B. Öffnen und Schließen der Tür, Ein-und Ausschalten zusätzlicher Alarmeinrichtungen etc. Schließlich können für ein Sender-/Empfängerpaar auch unterschiedliche Schlüsseltypen vorgesehen werden, wie es bei mechanischen Autotürschlüsseln bereits üblich ist. Beispielsweise schließt ein Schlüssel nur die Türen, nicht jedoch den Kofferraum, ein zweiter Schlüssel nur den Kofferraum jedoch nicht die Türen und ein dritter Schlüssel sämtliche Schlösser.

Mit Anspruch 10 erreicht man eine automatische Nachsynchronisation im vollständigen Codevorrat auch dann, wenn Sender und Empfänger um mehr als m + n (Anspruch 2) Schritte auseinanderliegen. Mit den Merkmalen der Ansprüche 1 und 2 bricht die Einrichtung die Codefortschaltung ja nach m + n Fortschaltungen ab. Der Benutzer muß dann die Tür mit einem mechanischen Schlüssel öffnen. Um auch in solchen Fällen, die z.B. durch Ausfall der Stromversorgung im Sender oder Empfänger auftreten, noch eine Synchronisation erreichen zu können, wird bei Erfüllung zweier Kriterien (z.B. geöffnetes Schloß und eingeschaltete Zündung) der volle Code-vorrat durchlaufen, womit dann mit Sicherheit, wenn auch in längerer Zeit, der synchrone Lauf zwischen Sender und Empfänger wieder hergestellt wird.

Im folgenden wird ein Ausführungsbeispiel der Erfindung im Zusammenhang mit der Zeichnung ausführlicher erläutert. Es zeigt:

Fig. 1A ein Blockschaltbild des Senders;

Fig. 1B ein Blockschaltbild des Empfängers;

Fig. 2 ein Kreisdiagramm der Codefortschaltung zur Erläuterung der Arbeitsweise der Erfindung.

Fig. 3 ein Flußdiagramm zur Erläuterung der Funktionsweise des Empfängers;

Fig. 3A einen Ausschnitt des Flußdiagramms der Fig. 3 mit einer zusätzlichen Variante zur automatischen Nachsynchronisation; und

Fig. 4 ein Diagramm zur Erläuterung des Übertragungsformates der Code-Wörter.

Der in Fig. 1A dargestellte Sender enthält einen ersten Speicher 1, in welchem ein Ur-Code-Wort gespeichert ist, welches im folgenden als "Key-Code-Wort" bezeichnet wird. Dieser Speicher 1 kann in Form einer festen Verdrahtung vorliegen, bevorzugt wird allerdings ein programmierbarer Speicher, insbesondere ein EEPROM. Die Länge dieses Key-Code-Wortes ist im Prinzip beliebig. Zur Erläuterung eines konkreten Ausführungsbeispieles sei angenommen, daß dieses Key-Code Wort 32 Bit lang ist. Es ist so organisiert, daß 24 Bit davon das eigentliche, jedem Sender-/Empfängerpaar individuell zugeordnete Key-Code-Wort sind, während die übrigen 8 Bits sog. Systembits sind, die für verschiedene Unterscheidungen herangezogen werden können wie z.B.:

a) Kennzeichnung von Schlüsseltypen, die unterschiedliche Schließfunktionen haben, w.z.B. Türschlösser, Türschlösser und Kofferraum

b) Systemkennzeichnungen w.z.B. Automarke, Schlüsselsystem

c) Auszulösende Funktionen w.z.B. Öffnen/Schließen etc.

d) Steuerbits

e) Parity-Check-Bit, etc.

Der Speicher 1 ist mit einem Schaltkreis 2 verbunden, der aus dem Key-Code-Wort nach einer vorgegebenen logischen Funktion ein aktuelles Code-Wort (im folgenden CDW genannt) erzeugt, das in einem weiteren Speicher 3 abgespeichert wird. Bei einem bevorzugten Ausführungsbeispiel der Erfindung ist der Schaltkreis 2 durch eine Kette von Exklusiv-ODER-Gattern realisiert, die nach dem Verfahren des Generator-Polynoms bzw. Polynomringes aus dem Key-Code-Wort allein oder dem Key-Code-Wort und dem bisherigen CDW ein neues Code-Wort erzeugt. Zur Erläuterung des Verfahrens des Polynomringes sei zunächst ein vereinfachtes Beispiel gewählt,bei dem das CDW nur aus dem Key-Codewort ermittelt wird.

In einem rückgekoppelten Schieberegister mit 4 Bit-Stellen sei ein Anfangswort (Key-Code-Wort) "0110" gespeichert. Zwischen der ersten und der zweiten Bit-Stelle (von rechts gesehen) sei ein Exklusiv-ODER-Gatter geschaltet, das die aktuellen Bit-Stelle des ersten und zweiten Bits miteinander

verknüpft und das Verknüpfungsergebnis in die erste Bit-Stelle einschreibt, worauf dann alle Bit-Stellen um eine Stelle nach rechts versetzt werden und die erste Bitstelle an die vierte Bitstelle rückt. Hierbei ergibt sich dann folgende Ablauffolge:

Bitstelle:4321

CDW 0	0110
CDW 1	0011
CDW 2	1000
CDW 3	0100
CDW 4	0010
CDW 5	0001
CDW 6	1001
CDW 7	1101
CDW 8	1111
CDW 9	1110
CDW10	0111
CDW11	1010
CDW12	0101
CDW13	1011
CDW14	1100
CDW15(0)	0110
CDW16(1)	0011 usw.

Der Polynomring hat also 15 verschieden Zustände. Bei diesem Beispiel verändert sich das ursprünglich gespeicherte Key-Codewort laufend.Kennt man die logische Verknüpfung bzw. das Bildungsgesetz der "Folge", so kann man von einem beliebigen CDW ausgehend das nächste CDW bestimmen.Dieser Code kann also noch leicht entschlüsselt werden. Aus obiger Tabelle ist weiterhin zu erkennen, daß von CDW 2 bis CDW 5 jeweils nur die eine 1 von links nach rechts durchwandert. Nimmt nun jemand unbefugt CDW 2 und CDW 3 auf, so kann er relativ leicht daraus auf CDW 4 und CDW 5 schließen. An bestimmten Ablaufstellen dieser Codefortschaltung ist der Code also besonders leicht zu "knacken". Deswegen sieht die Erfindung weiterhin vor, daß die logische Verknüpfung nur dann durchgeführt wird, wenn ein bestimmtes Bit, das als Steuerbit wirkt, eine logische 1 führt. Beispielsweise wählt man hierfür das höchstrangige Bit (Bitstelle 4 in obiger Tabelle). Dadurch wird zwar der Polynomring verkürzt, es ist jedoch schwieriger das Bildungsgesetz herauszufinden, mit dem man von einem Code-Wort CDW x auf das folgende Code-Wort CDW x+1 schließen kann.

Eine weitaus bessere Variante des Prinzips des Generatorpolynoms wird bei dem Ausführungsbeispiel der Fig. 1 angewandt: Bei unveränderbarem Key-Code-Wort erfolgt Bit-Stellenweise eine Exklusiv-ODER-Verknüpfung zwischen den Bits des Key-Code-Wortes und denen des bisherigen CDW's. Selbst wenn man das Bildungsgesetz der Folge und das bisherige CDW kennt, kann man ohne Kenntnis des Key-Codewortes das neue CDW nicht ermitteln.

Nach einer Ausgestaltung der Erfindung wird dies so durchgeführt, daß nur an den Stellen, an denen das Key-Code-Wort eine logische 1 führt, die Exklusiv-ODER-Verknüpfung mit der entsprechenden Bit-Stelle des CDW durchgeführt wird. Ein Beispiel eines 16 Bit langen Wortes soll dies verdeutlichen:

Key-Codewort: 1010100011100110
Letztes CDW (x-1): 0110010101001011
XOR wo Key = 1: x x x xxx xx
Key (XOR) CDW: 1100110110101101
Verschieben um eine Stelle nach rechts = Neues CDW (x): 1110011011010110

Es läßt sich zeigen, daß sich das CDW hierdurch laufend ändert. Bei dieser Art von Verknüpfung werden ausgehend von bestimmten Key-Codewörtern auch alle Kombinationsmöglichkeiten durchlaufen, bevor eine der Kombinationsmöglichkeiten zum zweiten Mal wiederholt wird. Bei einer Länge von Key-Code-Wort und CDW von 32 Bit ergeben sich damit $2^{32} = 4{,}29 \times 10^9$ Möglichkeiten. Bei einigen Key-Codewörtern (z.B.:000000....00) bzw. Arten der logischen Verknüpfung durchläuft der "Polynomring" zwar nicht alle Kombinationsmöglichkeiten, der Polynomring ist also verkürzt, was jedoch für das Grundprinzip der Erfindung ohne Bedeutung ist. Nach erfolgter logischer Verknüpfung wird dann das CDW im Speicher 3 um eine Bit-Stelle verschoben, wobei das letzte Bit dann an die erste Stelle geschoben wird. Dies ist durch die Leitung 4 dargestellt. Diese Vorgänge erfolgen unter Steuerung durch eine Steuereinheit 5, die die benötigten Taktfrequenzen und die einzelnen Steuersignale erzeugt. Drückt der Benutzer eine Taste 6, so wird ein Sendezyklus ausgelöst, bei dem in der beschriebenen Weise ein neues CDW erzeugt wird, welches dann unter Steuerung durch die Steuereinheit 5 aus dem Speicher 3 seriell ausgelesen und über einen Kodierer 7 mit Modulator und Verstärker zu einer Sendeeinheit 8 gelangt, die hier eine im Infrarotbereich strahlende Leuchtdiode ist.

Bei einer Variante der Erfindung erfolgt die Bildung des CDW nur durch Verknüpfung mit dem eigentlichen Key-Code-Wort, während die übrigen Systembits jeweils unverändert ausgesandt werden, wofür mehrere Varianten möglich sind:

1) Die Systembits werden zeitlich vor dem CDW gesandt.

2) Die Systembits werden zeitlich nach dem CDW gesandt.

3) Die Systembits werden teilweise vor und teilweise nach dem CDW gesandt.

4) Die Systembits werden im CDW verschachtelt gesandt.

Im Ausführungsbeispiel der Fig.1 A sind an die Steuereinheit noch weitere Schalter 9 und 10 angeschlossen, über die andere Funktionen w.z.B. Öffnen oder Schließen einer Tür etc. ausgewählt werden können. Wird einer dieser Schalter betätigt, so werden lediglich ein oder mehrere Systembits geändert, während die übrige Ablauffolge unverändert durchgeführt wird.

Das von Leuchtdiode 8 ausgesandte Licht wird in Form codierter Lichtimpulse übertragen. Beispielsweise kann eine Impuls-Abstand-Modulation gewählt werden, bei der die Abstände zwischen zwei benachbarten Licht-Impulsen bei einer logischen 1 und einer logischen 0 unterschiedlich lang sind (vgl. Fig. 4). Natürlich kommen auch andere bekannte Modulations-Verfahren in Betracht. Diese Licht-Impulse werden im Empfänger (Fig.1B) von einem Fotosensor 11 erfaßt, in einer Pulsaufbereitungseinheit 12 decodiert und verstärkt und dann unter Steuerung durch eine Steuereinheit 14 zunächst darauf überprüft, ob die Impulsfolge von ihrem Format her überhaupt ein gültiges CDW sein kann. Hierbei werden beispielsweise überprüft: Anzahl der Bits, Mindestlänge einer Pause nach dem letzten empfangenen Bit, Übereinstimmung bestimmter Systembits etc.. Diese Prüfung wird in einer Einheit 15 durchgeführt. Ist das Prüfungsergebnis positiv, so wird das empfangene CDW in einen Empfangsbuffer-Speicher 13 (I-Buffer) geschrieben. Unter Steuerung durch die Steuereinheit 14 wird dann in gleicher Weise wie beim Sender das nächstfolgende CDW ermittelt und in einen temporären Speicher 21 (T-Buffer) eingeschrieben. Sodann werden der Inhalt des T-Buffers 21, also das im Empfänger erzeugte aktuelle Code-Wort und das im I-Buffer 13 gespeicherte empfangene Wort, das also vom Sender erzeugt wurde, in einem Vergleicher 18 miteinander verglichen. Stimmen diese beiden Worte überein, so wird dies der Steuereinheit 14 gemeldet, die ein Betätigungssignal abgibt, beispielsweise ein Türöffnungssignal.

Zur Erzeugung des aktuellen CDW im Empfänger ist dort ebenfalls ein Speicher 19 für das Key-Code-Wort vorgesehen sowie eine logische Verknüpfung 20 (hier: Exclusiv-ODER-Verknüpfung) . Die prinzipielle Arbeitsweise zur Erzeugung des aktuellen CDW im Empfänger entspricht der des Senders.

Bei normalem Betrieb schalten Sender und Empfänger bei jeder Betätigung jeweils um ein Code-Wort weiter. Man kann auch sagen, sie laufen synchron.

Nun können aber Sender und Empfänger auch "außer Tritt" geraten, beispielsweise durch folgende Ursachen:

a) Betätigung des Senders und damit Code-Fortschaltung außerhalb der Reichweite des Empfängers (sog. Leerbetätigung)

b) Fortschalten des Empfängers durch einen systemgleichen Fremdschlüssel (z.B. auf einem Parkplatz)

c) Fortschalten des Empfängers durch unbefugte Öffnungsversuche

d) Stromausfall im Sender oder Empfänger und damit Rücksetzen flüchtiger Speicher.

Der in der Praxis häufigste Fall ist die Leerbetätigung des Senders, dem hier besonderes Augenmerk geschenkt werden soll. Unter Bezugnahme auf Fig.2 sollen die diesbezüglichen Merkmale der Erfindung verdeutlicht werden. Es sei angenommen, daß Sender und Empfänger von ihrem Ur-Zustand (CDW 0) im Gleichtakt bis zu einem beliebigen CDW x gelaufen sind. Durch eine Leerbetätigung des Senders sei dieser dann auf CDW x+1, während der Empfänger noch auf CDW x steht. Der Sender ist also dem Empfänger um einen (oder auch mehrere) Schritte voraus. Empfängt nun der Empfänger, der noch auf CDW x steht, das CDW x+1, so stellt der Vergleicher 18 eine Nichtübereinstimmung fest. Das Schloß wird also nicht geöffnet. Daraufhin löst jedoch die Steuereinheit 14 im Empfänger eine Codefortschaltung aus, so daß fortschreitend dort die nächsten aufeinanderfolgenden Code-Wörter bestimmt werden, maximal jedoch eine vorgegebene Anzahl n, also die Code-Wörter CDW x bis CDW x+n. In einem praktischen Ausführungsbeispiel wird man n in der Größenordnung von zehn Schritten wählen. Wird innerhalb dieser n Fortschaltungen (Code-Wörter CDW x bis CDW x+n) mit dem empfangenen Code-Wort (hier:CDW x+1) Übereinstimmung festgestellt, so wird das Betätigungssignal erzeugt und im Empfänger wird das CDW, bei dem Übereinstimmung erzielt wurde (hier also CDW x+1) als gültiges Code-Wort für die nächsten Betätigungen in einem Speicher 17 (N-Buffer) gespeichert. Solange keine Übereinstimmung festgestellt wird, wird das jeweils aktuell im Sender ermittelte CDW nur in dem T-Buffer 21 gespeichert. Erst bei Übereinstimmung wird der Inhalt des T-Buffers 21 in den N-Buffer 17 übernommen. Es kann aber auch das empfangene CDW aus dem I-Buffer 13 dann in den N-Buffer 17 übernommen werden.

Es ist ersichtlich, daß hierbei der Empfänger sog. verlorene Code-Wörter nachrechnet, so daß sich Sender und Empfänger selbsttätig synchronisieren, ohne daß Synchronisationsimpulse, die ja unbefugt aufgenommen werden können, über die Sendestrecke laufen müssen. Der Benutzer merkt von dieser Synchronisation nichts.

Nun kann es vorkommen, daß der Sender mehr als n Leerbetätigungen erlebt hat. Innerhalb der n vom Empfänger nachgerechneten CDW's (CDW x bis CDW x+n) wird keine Übereinstimmung festgestellt. Der Empfänger - schaltet dann nach einem weiteren Merkmal der Erfindung auf erhöhte Sicherheit um, bei der zwei unmittelbar aufeinanderfolgende CDW's übereinstimmen müssen.

Es werden eine Anzahl m weitere Code-Worte (also CDW x + n bis CDW x + n + m) ermittelt, wobei m größer n ist (z. B. m = 256). Ist der Empfänger in diesem Betriebszustand, so muß der Benutzer also am Sender zweimal seine Taste drücken. Die Kombinationsmöglichkeiten entsprechen dann denen eines $2 \times 32 = 64$ Bit langen Wortes, d.h. ca. $1{,}8 \times 10^{19}$ Möglichkeiten. Wird innerhalb der Folge CDW x+n bis CDW x+n+m die Doppelübereinstimmung festgestellt, so wird wieder das Betätigungssignal erzeugt und das zuletzt empfangene CDW wird in den N-Buffer 17 übernommen. Wird dagegen auch hier keine Übereinstimmung festgestellt, so ist der Öffnungsversuch gescheitert, das Schloß muß dann beispielsweise mit einem mechanischen Schlüssel geöffnet werden und das zuletzt empfangene CDW wird vom I-Buffer 13 in einen weiteren Empfangsspeicher 16 (X-Buffer) übertragen.

Eine automatische Nachsynchronisation kann nach den bisher beschriebenen Merkmalen der Erfindung also nur in den Sektoren n und m der Fig. 2 erfolgen. Durch Ausfall der Stromversorgung im Sender oder Empfänger können diese - je nach Vorgeschichte, d. h. Anzahl von früheren Betätigungen - auch so weit auseinanderliegen, daß sie nicht mehr in den erwähnten Sektoren liegen. Nach einer Ausgestaltung der Erfindung, die im Zusammenhang mit Fig. 3A noch näher erläutert wird, kann auch dann noch eine Nachsynchronisation erfolgen. Aus Sicherheitsgründen gegen unbefugtes Öffnen soll im Normalfall die Nachsynchronisation ja nur in einem engen Bereich (n + m) durchgeführt werden, damit nicht ein Unbefugter mit einem Funktionsgenerator einfach alle Möglichkeiten durchspielt. Auch sind die Zahlen n und m nicht zu groß zu wählen, um den Empfänger bei unbefugten Öffnungsversuchen nicht zu lange zu sperren. Um nun aber auch bei dem geschilderten Fall noch eine Nachsynchronisation erreichen zu können, ist nach der Erfindung vorgesehen, daß die Anzahl m dann unbegrenzt ist, wenn zwei Kriterien erfüllt sind. Vorzugsweise sind diese Kriterien:

1. Türschloß (mit mechanischem Schlüssel geöffnet) und

2. weiteres Kriterium wie z.B. Zündung des Autos eingeschaltet.

Läßt sich das Türschloß elektronisch trotz zweimaliger Betätigung der Sendertaste nicht öffnen, so muß der Benutzer also das Türschloß mechanisch aufschließen, die Zündung einschalten und dann noch einmal die Sendertaste drücken. Der Empfänger rechnet dann alle Codemöglichkeiten nach, bis eine Übereinstimmung gefunden wurde, also im Extremfall den vollen Kreis der Fig. 2. Rechnet man mit durchschnittlich zehn Betätigungen eines Autoschlosses pro Tag, so werden im Laufe von zehn Jahren lediglich 36500 Codefortschaltungen durchgeführt. Verglichen mit den $4{,}2 \times 10^9$ theoretischen Codefortschaltungen bei einem 32 Bit langen CDW, ist dies eine relativ kleine Zahl. Empfänger und Sender werden also selbst nach zehnjähriger Betriebsdauer noch relativ nahe am CDW Null sein. Damit nun nicht der volle Kreis der Fig. 2 durchgerechnet werden muß, ist es empfehlenswert, den Sender durch kurzes Herausnehmen der Batterie in seinen Urzustand zu versetzen, also den Zustand CDW Null. Da der Empfänger insgesamt ja nur die relativ kleine Anzahl von 36500 Codefortschaltungen gemacht hat, wird dann die Synchronisation schneller gefunden, als wenn der volle Kreis der Fig. 2 durchgerechnet wird.

Es kann nun auch vorkommen, daß durch einen Fremdsender die beschriebenen n und bei dessen zweimaliger Betätigung sogar die Schritte n+m im Empfänger abgelaufen sind. Da durch diesen Fremdsender jedoch kein Öffnen ausgelöst wurde, steht im N-Buffer 17 noch das letzte Übereinstimmungswort, also das Wort CDW x. Allerdings hat der Empfänger auf die Betriebsweise der Übereinstimmung zwei aufeinanderfolgender Worte umgeschaltet. Sendet nun der richtige Sender das CDW x so öffnet die Tür noch nicht. Der Benutzer muß dann den Sender noch ein zweites Mal betätigen. Sodann werden CDW x und CDW x+1 als Paar übereinstimmen, die Tür öffnet und das CDW x+1 wird in den N-Buffer 17 übernommen.

Nach einer weiteren Variante der Erfindung kann die Anzahl n auch zu "Null" gesetzt werden. In diesem Fall wird stets mit der erhöhten Sicherheit gearbeitet. Es kann dann auch vorgesehen sein, daß bei einmaligere Betätigung der Taste 6 (Fig. 1A) stets zwei aufeinanderfolgende CDW's ermittelt und ausgesandt werden.

Nach einem weiteren Merkmal der Erfindung sind beide Speicher 1 und 19 für das Key-Code-Wort als EEPROM's (elektrisch löschbare, programmierbare Speicher) ausgebildet. Dies hat zum einen fertigungstechnische Vorteile, da alle Sender und Empfänger hardwaremäßig jeweils identisch aufgebaut sein können und erst nach hardwaremäßiger Fertigstellung der Key in ein Sender/Empfänger-Paar einprogrammiert wird.

Zum anderen ist dies auch bei Verlust eines Senders (Schlüssels) von Vorteil. Es muß dann nicht das gesamte System ausgewechselt werden. Vielmehr genügt es, einen neuen Sender (Schlüssel) zu kaufen und den Empfänger neu zu programmieren. Selbstverständlich ist dies nur bei geöffneter Tür möglich. Durch einen Schalter 14' wird der Empfänger auf "Lernphase" umgeschaltet. Der neue Sender sendet dann einmal das Key-Code-Wort, das in dieser Lernphase dann in den Key-Speicher 19 des Empfängers eingeschrieben wird.

Das Flußdiagramm der Fig. 3 verdeutlicht noch einmal die Ablaufschritte, wobei die entsprechenden Bezugszeichen der Schritte auch in Fig. 1B eingetragen sind. Auf den Empfang eines formal gültigen empfangenen Code-Wortes wird im Schritt 22 das aktuelle CDW (N-Buffer 17) in den T-Buffer 21 geschoben. Sodann wird im Schritt 23 geprüft, ob das System auf einfacherer Sicherheit oder höherer Sicherheit steht. Steht es auf einfacher Sicherheit, so wird im Schritt 24 der Inhalt des T-Buffers 21 mit dem Inhalt des Key-Speichers 19 logisch verknüpft, wobei das Ergebnis das neue CDW ist , das im T-Buffer 21 gespeichert wird. Sodann wird im Schritt 25 überprüft, ob dieses neue CDW mit dem Inhalt des I-Buffers 13 übereinstimmt. Ist dies der Fall, so wird über Schritt 26 die gewünschte Funktion ausgelöst und der Inhalt des I-Buffers 13 in den N-Buffer 17 übernommen. Ergibt die Prüfung des Schritts 25 dagegen ein negatives Ergebnis, so wird im Schritt 27 abgefragt, ob bereits die Anzahl von n-Versuchen durchgeführt wurde. Bei negativem Ergebnis geht die Schleife zurück zum Schritt 24, bei positivem Ergebnis wird im Schritt 28 auf erhöhte Sicherheit umgeschaltet.

Ist bei Empfang eines gültigen Code-Wortes das System auf erhöhter Sicherheit, so verzweigt Schritt 23 auf Schritt 29, wo geprüft wird, ob der Inhalt des T-Buffers 21 mit dem Inhalt des I-Buffers 13 übereinstimmt. Ist dies nicht der Fall, so wird im Schritt 30 ein neues CDW ermittelt, wobei dieser Vorgang gemäß Schritt 31 bis zu m-mal wiederholt wird. Ergibt sich bei diesen m Versuchen keine Übereinstimmung gemäß Schritt 29, so wird der Inhalt des I-Buffers 13 in den X-Buffer 16 übernommen. Ergibt dagegen die Prüfung im Schritt 29 eine Übereinstimmung, so wird im Schritt 32 das nächstfolgende CDW errechnet und im Schritt 33 überprüft, ob auch dieses neue (zweite) CDW mit dem beim zweiten Sendeschritt übermittelten Inhalt des I-Buffers 13 übereinstimmt. Ist dies der Fall, so wird wieder die gewünschte Funktion ausgelöst und im Schritt 26 wird wieder auf einfache Sicherheit zurückgeschaltet und - schließlich auch der Inhalt des I-Buffers 13 in den N-Buffer 17 eingeschrieben.

Fig. 3A zeigt einen Ausschnitt der Fig. 3 mit der zusätzlichen Variante des Nachsynchronisierens im vollständigen Codevorrat. Wird bei der höheren Sicherheit im Schritt 31 festgestellt, daß die Anzahl von m-Versuchen abgelaufen ist, so würde nach der Variante der Fig. 3 die Codefortschaltung abgebrochen. Ein Öffnen der Türe wäre nicht mehr möglich. Nach der Variante der Fig. 3A wird in diesem Fall im Schritt 35 geprüft, ob die Tür offen ist. Ist dies nicht der Fall, so wird die Codefortschaltung wieder abgebrochen (Schritt 34). Ist dies dagegen der Fall, so wird im Schritt 36 geprüft, ob das weitere Kriterium erfüllt ist, also beispielsweise die Zündung eingeschaltet ist. Ist dies nicht der Fall, so wird wiederum abgebrochen (Schritt 34). Ist dies dagegen der Fall, so wird zu Schritt 29 zurückgeschaltet. Die Schleife der Schritte 29, 30, 31, 35, 36 wird dann solange durchlaufen, bis eine Übereinstimmung erzielt wurde. Bei einem zusammengehörigen, einwandfrei funktionierenden Sender-/Empfängerpaar wird dann also mit Sicherheit wieder ein synchroner Lauf erreicht.

Fig. 4 verdeutlicht noch das Übertragungsformat. Auf die Betätigung der Taste 6 des Senders wird zunächst ein Vorimpuls als sog. Weckimpuls ausgesandt, der den Empfänger in Empfangsbereitschaft setzt. Sodann werden die eigentlichen Daten in Form des Code-Wortes ausgesandt (Fig. 4a). Die Daten sind so organisiert, daß zunächst acht Systembits gesandt werden und dann das eigentliche CDW (Fig.4b). Die logischen Zustände "1" und "0" werden hier durch eine sog. Pulsabstandsmodulation dargestellt. Pro Bit werden mehrere Einzelimpulse, in denen die lichtemittierende Diode 8 eingeschaltet ist, ausgesandt und zwar wie aus den Fig. 4c und 4d hervorgeht, am Anfang und am Ende eines Bits je eine konstante Anzahl von Impulsen, beispielsweise 6. Der zeitliche Abstand zwischen den Impulsgruppen am Anfang und am Ende eines Bits bestimmt dann, ob das Bit eine logische "1" oder eine logische "0" ist.

Abschließend sei noch darauf hingewiesen, daß die beiden oben beschriebenen Varianten des "Generatorpolynoms" keine abschließende Aufzählung darstellen. Es können natürlich auch andere Verknüpfungsmöglichkeiten verwendet werden. So können beispielsweise auch alle Bits des Key-Code-Wortes und des aktuellen CDWs miteinander verknüpft werden und nicht nur diejenigen Bits, bei denen das Key-Code-Wort eine "1" führt. Um die Anzahl der verschiedenen Codierungsmöglichkeiten jedoch möglichst groß zu halten, ist darauf zu achten, daß eine solche Verschlüsselung gewählt wird, daß keine verkürzten Polynomringe auftreten oder nur geringfügig verkürzte Polynomringe.

Das beschriebene Verfahren des Generatorpolynoms kann allgemeiner als Erzeugung einer "Pseudo-Zufallsfolge" angesehen werden. Es ist klar, daß bei der Erfindung auch alle anderen bekannten Verfahren zur Erzeugung von "Pseudo-Zufallsfolgen" verwendet werden können, sofern sichergestellt ist, daß im Sender und Empfänger - ausgehend von ein und demselben Key-Code-Wort dieselbe "Pseudo-Zufallsfolge" erzeugt wird.
Weiterhin ist darauf zu achten, daß die Zyklen für die n-und m-Schritte nicht zu lang sind, damit der Empfänger durch Fremdsender nicht zu lange blockiert wird und damit die Wahrscheinlichkeit, daß ein Unbefugter mit einem Funktionsgenerator, der alle Bitkombinationen durchspielt, die Tür nicht öffnet, nicht zu gering wird. Zu diesem Zwecke kann man auch zusätzlich vorsehen, daß der Empfänger nach jedem empfangenen CDW eine vorgegebene Zeitdauer von einigen Sekunden gesperrt ist, womit die Zeitdauer für das Durchspielen aller Kombinationen auf mehrere Jahre vergrößert wird. Im Falle der Nachsynchronisation durch den gesamten Codevorrat (Fig. 3A) sollte allerdings keine künstliche Zeitverzögerung vorgesehen sein.

Als besondere Vorteile der Erfindung sind hervorzuheben: Man kann nahezu beliebig lange Code-Wörter vorsehen, wobei der Speicherplatzbedarf trotzdem in engen Grenzen bleibt. Es müssen - im Gegenstand zum Stand der Technik - eben nicht alle Code-Wörter fest eingespeichert sein;
selbst wenn jemand den Algorithmus für die Ermittlung eines neuen Code-Wortes kennt und unbefugt frühere Code-Wörter aufgezeichnet hat, so kann er das nächst folgende Code-Wort doch nicht bestimmen, da er das Key-Code-Wort nicht kennt. Dieses kann er aber auch nicht unbefugt aufzeichnen, da es nicht über die "Sendestrecke" ausgesandt wird;
der Empfänger synchronisiert sich automatisch auf den Sender, ohne daß es hierzu über die Sendestrecke ausgesandter und damit aufzeichenbarer Befehle bedarf. Damit werden die bei der bekannten Code-Fortschaltung in Kauf genommenen Nachteile der Synchronisation beseitigt;
die Sicherheit gegen Entschlüsselung des Codes ist extrem hoch;
Leerbetätigung des Senders und Betätigungen des Empfängers durch Fremdsender zeigen keine für den Benutzer spürbare Folgen;
bei Verlust eines Senders (Schlüssels) kann der Empfänger in einfacher Weise auf einen neuen Sender angepaßt werden, ohne daß hierdurch die Sicherheit herabgesetzt wird.

Sämtliche in den Patentansprüchen, der Beschreibung und der Zeichnung dargestellten technischen Einzelheiten können sowohl für sich als auch in beliebiger Kombination miteinander erfindungswesentlich sein.

Ansprüche

1. Elektronische Fernbetätigungseinrichtung, insbesondere für Zentralverriegelungsanlagen von Kraftfahrzeugen, mit
-einem als Schlüssel arbeitenden Sender und
-einem als Schloß arbeitenden Empfänger,
-wobei der Sender bei Betätigung ein Code-Wort in Form codierter Signale (Bit-Folge) aussendet und zwar pro Betätigung fortschaltend ein ande res Code-Wort aus einer geordneten Menge von Code-Wörtern,
-wobei der Empfänger auf den Empfang eines formal gültigen Wortes in gleicher Weise ein Vergleichscodewort aus der geordneten Menge von Code-Wörtern zum Vergleich mit dem vom Sender ausgesandten Code-Wort bereitstellt und bei Übereinstimmung dieser Wörter ein Betätigungssignal erzeugt,
dadurch **gekennzeichnet,**
-daß im Sender und im Empfänger in gleicher Weise ausgehend von einem gemeinsamen Ur-Code-Wort bei jeder Fortschaltung ein neues Code-Wort (CDW x) durch logische Verknüpfung (2, 20) nach einer vorgegebenen Funktion erzeugt wird und
-daß der Empfänger bei Nichtübereinstimmung zwischen dem empfangenen Code-Wort und dem Vergleichscode-Wort vorwärts fortschaltend weitere Code-Worte (CDW x + 1 ..., CDW x + n) erzeugt und diese mit dem empfangenen Code-Wort vergleicht, jedoch dabei höchstens eine vorgegebene Anzahl n von Fortschaltungen und Vergleichen durchführt.

2. Fernbetätigungseinrichtung nach Anspruch 1, dadurch gekennzeichnet, daß der Empfänger bei Nichtübereinstimmung während der Anzahl n Fortschaltungen und Vergleiche auf den Empfang eines zweiten Code-Wortes vorwärts fortschaltend eine weitere Anzahl m aufeinanderfolgender Vergleichscode-Wörter (CDW x + n + 1 ..., CDW x + n + m) erzeugt und dabei vergleicht, ob die beiden unmittelbar aufeinanderfolgend empfangenen Code-Wörter mit zwei unmittelbar aufeinanderfolgenden Vergleichswörtern übereinstimmen, wobei die Anzahl m größer ist als die Anzahl n.

3. Fernbetätigungseinrichtung nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die Erzeugung der aufeinanderfolgenden Code-Wörter im Sender und im Empfänger jeweils durch eine Pseudo-Zufallsfolge und insbesondere durch eine Exklusiv-ODER-Verknüpfung (2, 20) einzelner Bitstellen des Ur-Code-Wortes erfolgt.

4. Fernbetätigungseinrichtung nach Anspruch 3, dadurch gekennzeichnet, daß im Sender und im Empfänger das fest vorgegebene Ur-Code-Wort (Key-Code-Wort; Speicher 1, 19) und das aktuelle Code-Wort (CDW x; 3, 21) gespeichert sind, wobei das nächst folgende Code-Wort (CDW x + 1)

dadurch ermittelt wird, daß diejenigen Bitstellen des aktuellen Code-Wortes (CDW x), die eine logische "1" führen, mit der entsprechenden Bitstelle des fest vorgegebenen Code-Wortes (Key-Code-Wort) exklusiv-ODER-verknüpft werden (2, 20) und anschliessend alle Bits des aktuellen Code-Wortes um eine Bitstelle verschoben werden, wobei die letzte Bitstelle zur ersten Bitstelle verschoben wird.

5. Fernbetätigungseinrichtung nach Anspruch 4, dadurch gekennzeichnet, daß die Exklusiv-ODER-Verknüpfung (2, 20) nur dann durchgeführt wird, wenn eine vorbestimmte Bitstelle (Steuerbit) eine logische "1" führt, während bei einer logischen "0" dieses Steuerbits nur die Verschiebung durchgeführt wird, und zwar so oft, bis das Steuerbit eine logische "1" führt oder bis eine vorgegebene Anzahl von Verschiebungen durchgeführt wurde.

6. Fernbetätigungseinrichtung nach Anspruch 5, dadurch gekennzeichnet, daß die höchstrangige Bitstelle das Steuerbit ist.

7. Fernbetätigungseinrichtung nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß das aktuelle Vergleichswort bei den n und den m Fortschaltungen und Vergleichen in einem temporären Speicher (21) gespeichert ist und nur bei Übereinstimmung mit dem bzw. den empfangenen Code-Wörtern als neues Code-Wort in einen weiteren Speicher (17) übernommen wird.

8. Fernbetätigungseinrichtung nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, daß die Code-Wörter eine oder mehrere Bitstellen aufweisen, die unveränderbar sind und unter Umgehung der Exklusiv-ODER-Verknüpfung (2, 20) direkt einer Sendeeinrichtung (7, 8) und dem Vergleicher (18) zugeführt werden.

9. Fernbetätigungseinrichtung nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, daß der Speicher (1, 19) für das Ur-Code-Wort zumindest im Empfänger ein elektrisch löschbarer, programmierbarer Speicher (EEPROM) ist.

10. Fernbetätigungseinrichtung nach einem der Ansprüche 2 bis 9, dadurch gekennzeichnet, daß bei geöffnetem Schloß und Erfüllung einer zusätzlichen Bedingung (z.B. wenn die Zündung eines Kfz eingeschaltet ist) die Anzahl m unbegrenzt ist.

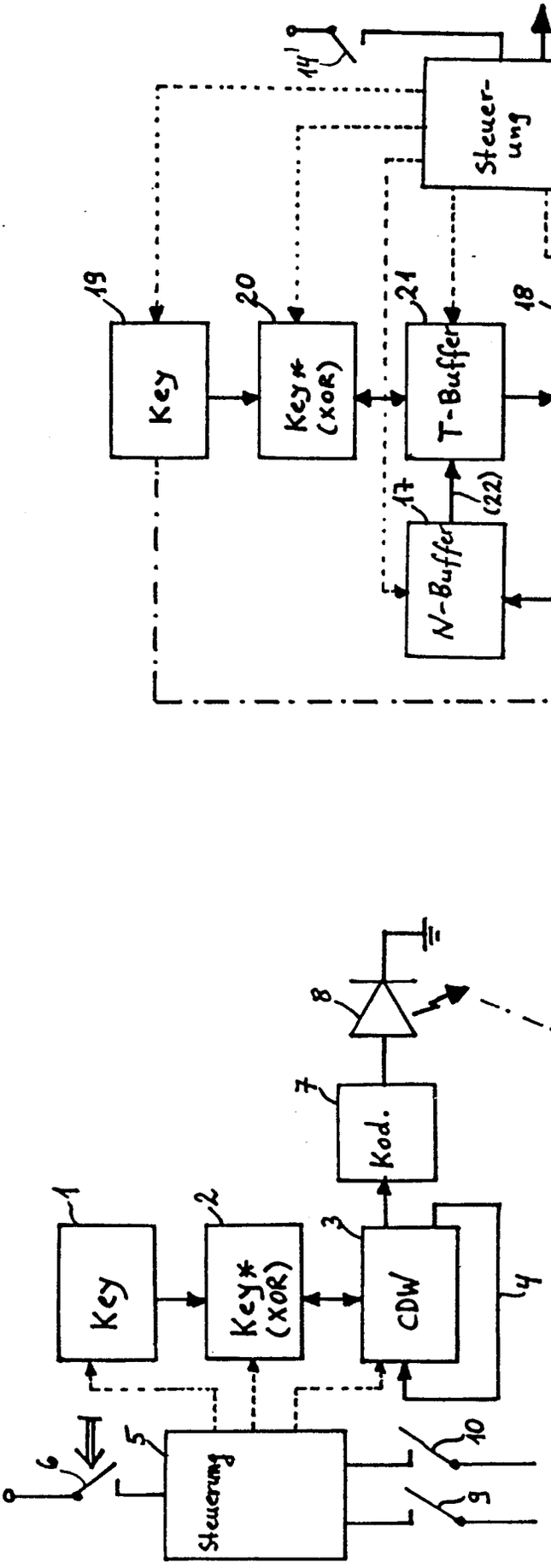
Steuerung
Key
Key* (XOR)
CDW
Kod.
Steuerung
Key
Key* (XOR)
T-Buffer
Vergl.
X-Buffer
N-Buffer
I-Buffer
Prüfung
Dekoder

Fig. 1A

Fig. 1B

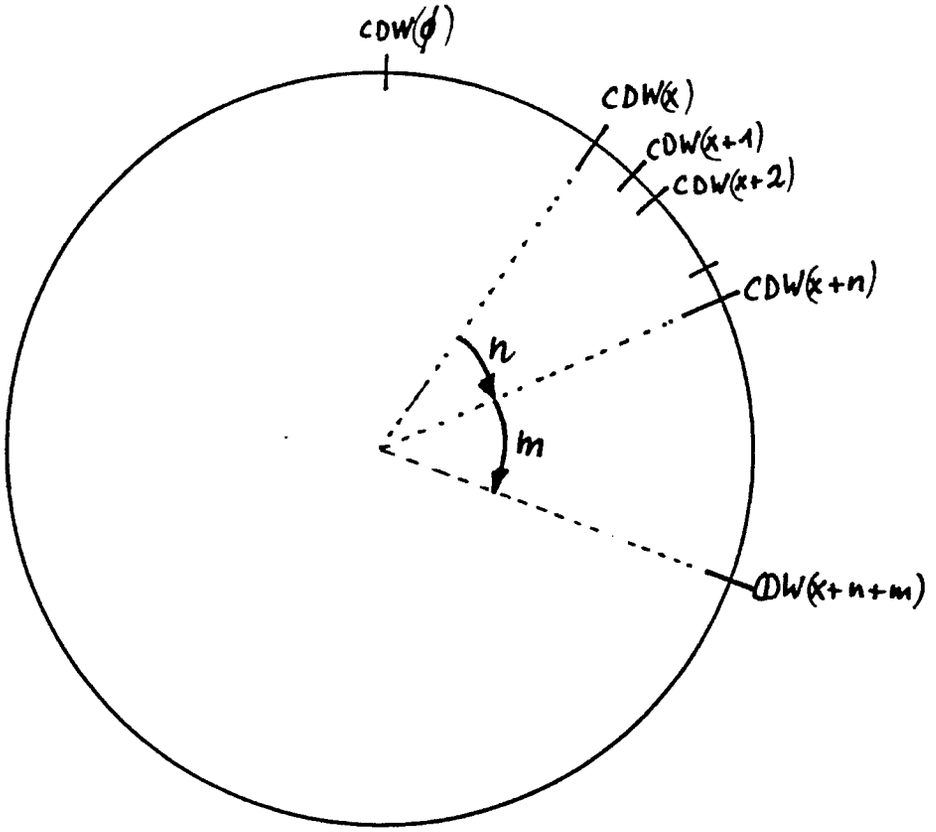

Fig. 2

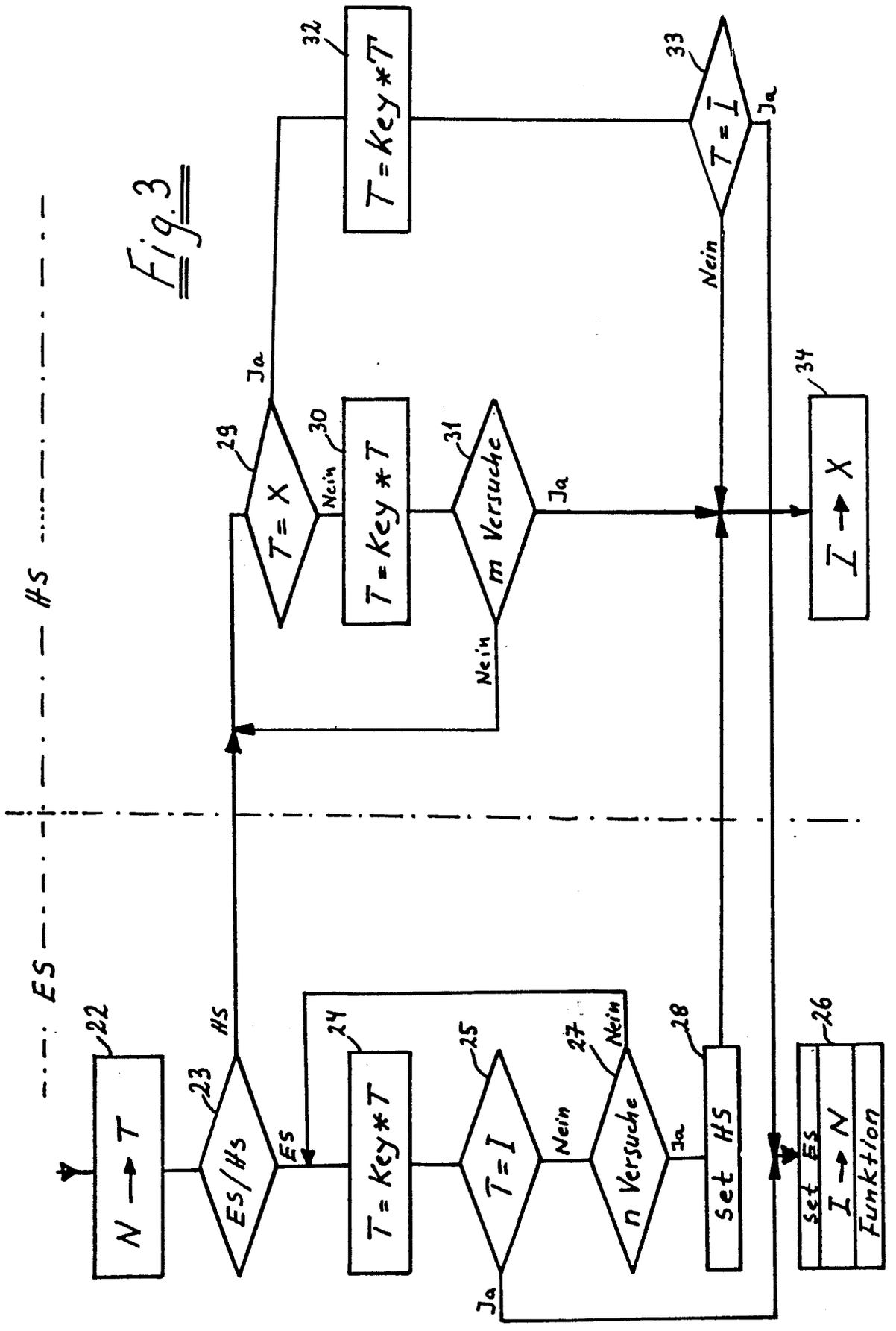
ES
HS
N → T
ES/HS
HS
ES
T = Key * T
T = I
Nein
n Versuche
Ja
Set HS
Set ES
I → N
Funktion
T = X
Nein
T = Key * T
m Versuche
Ja
T = Key * T
T = Ī
Ja
Nein
Ī → X
22
23
24
25
27
28
26
29
30
31
32
33
34

Fig. 3

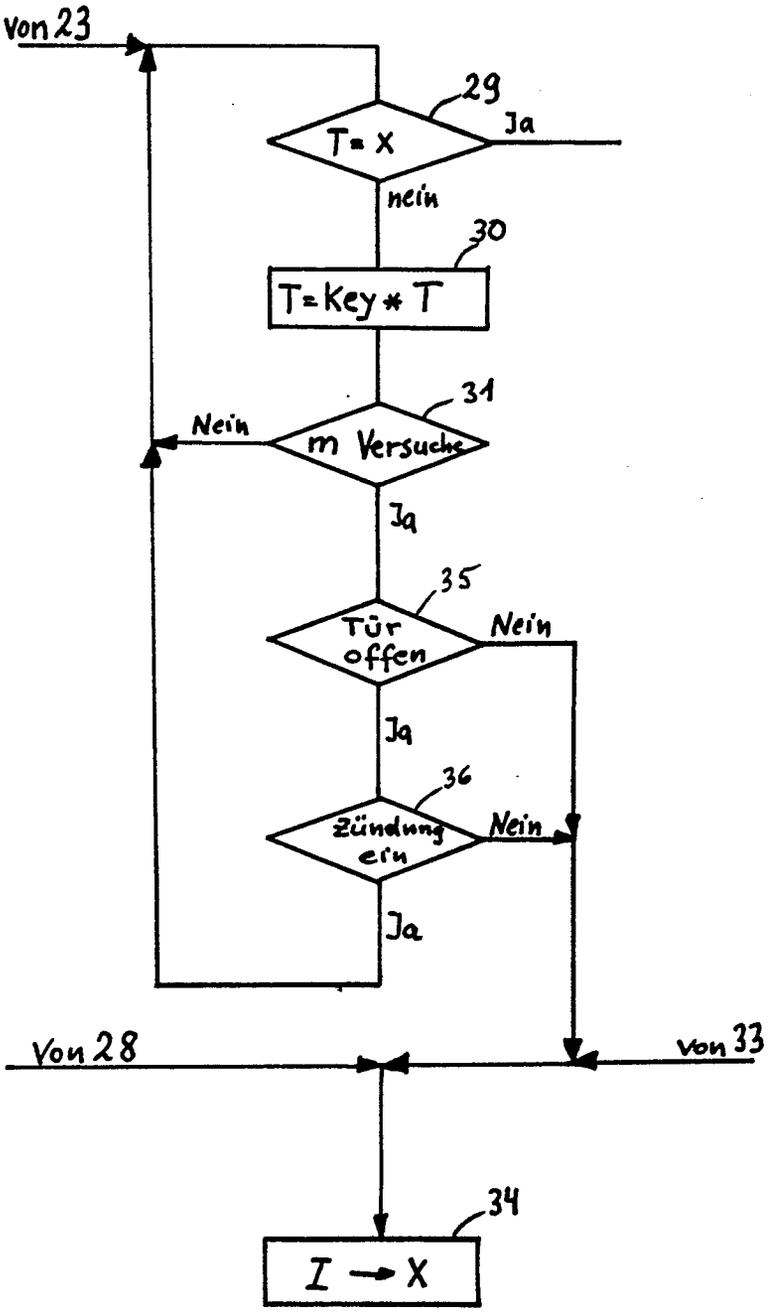
Von 23
29
T = X
Ja
nein
30
T = Key * T
31
Nein
m Versuche
Ja
35
Tür offen
Nein
Ja
36
Zündung ein
Nein
Ja
Von 28
von 33
34
I → X

Fig. 3A

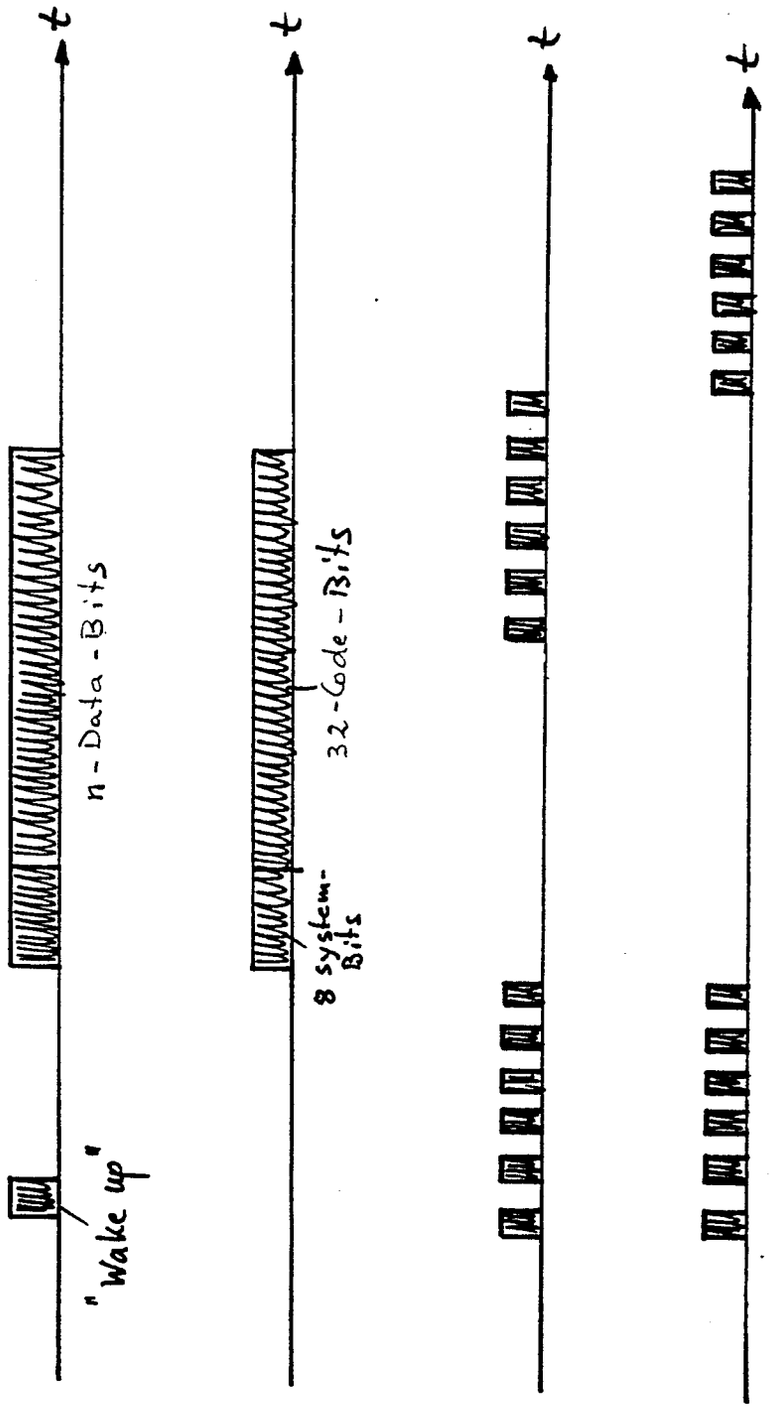

Fig. 4