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

(11) EP 0 889 445 A2

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
07.01.1999 Patentblatt 1999/01

(51) Int. Cl.[6]: **G07C 1/26**, G07C 1/24

(21) Anmeldenummer: **98108878.4**

(22) Anmeldetag: **15.05.1998**

(84) Benannte Vertragsstaaten:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Benannte Erstreckungsstaaten:
AL LT LV MK RO SI

(30) Priorität: **11.06.1997 DE 19724560**

(71) Anmelder: **Stobbe, Anatoli**
30890 Barsinghausen (DE)

(72) Erfinder: **Stobbe, Anatoli**
30890 Barsinghausen (DE)

(74) Vertreter:
Patentanwälte Thömen & Körner
Zeppelinstrasse 5
30175 Hannover (DE)

(54) Verfahren zur Identifizierung von an sportlichen Wettbewerben teilnehmenden Personen oder Tieren

(57) Es wird ein Verfahren zur Identifizierung von an sportlichen Wettbewerben teilnehmenden Personen oder Tieren, insbesondere Brieftauben beschrieben.

An den Personen oder Tieren wird ein Transponder angebracht, der einen Speicher enthält, in dem ein Datenwort speicherbar ist und mittels eines Schreib-Lesegerätes berührungslos gelesen, registriert und ausgewertet werden kann.

Beim Beschreiben wird zuerst ein in einem löschbaren Speicher des Transponders gespeichertes Datenwort gelesen, eine in dem Datenwort enthaltene Information ausgewertet und anschließend ein geändertes Datenwort erzeugt und im löschbaren Speicher des Transponders abgelegt. Beim Lesen wird dann das zuletzt gespeicherte Datenwort ausgelesen, ausgewertet und im Schreib-Lesegerät registriert.

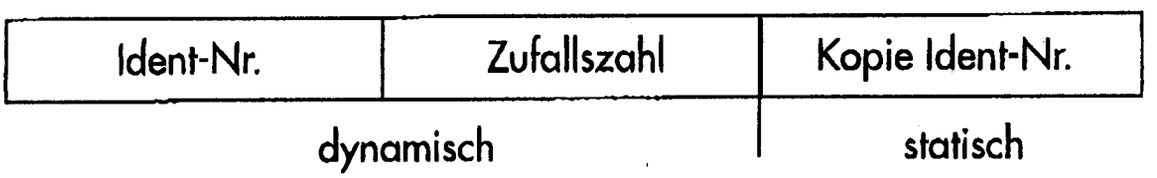

Fig. 1

EP 0 889 445 A2

Beschreibung

Die Erfindung betrifft ein Verfahren zur Identifizierung von an sportlichen Wettbewerben teilnehmenden Personen oder Tieren nach dem Oberbegriff des Anspruchs 1.

Aus der DE 36 32 958 A1 ist ein Verfahren zur Identifizierung von Brieftauben bekannt, bei welchem an einem Fuß der Taube ein Trägerring angebracht wird, der einen Mikrochip enthält. Dieser Mikrochip ist ein seriell lesbarer und schreibbarer Halbleiterspeicher, der einen den Tauben zugeordneten Identifikationscode speichert. Bei Ankunft der Brieftaube am Taubenschlag wird der Identifikationscode durch ein Lesegerät abgelesen, was kontaktlos über induktive Kopplung erfolgen kann. Da bei Wettflügen hohe Wetteinsätze gesetzt werden, wird ein hohes Maß an Sicherheit gegenüber Manipulationen gefordert. Dies ist bei dem bekannten Verfahren nicht gewährleistet, insbesondere ist es möglich, den Ring vom Fuße der Taube abzunehmen, indem der Ring aufgeschlitzt und anschließend dem Lesegerät zugeführt wird. Hierdurch kann dann eine frühere Ankunftszeit der Taube vorgetäuscht werden. Der gleiche oder ein anderer entsprechend kodierter Ring wird sodann am Fuß der Taube angebracht, wobei die Auftrennstellen geschickt kaschiert werden.

Zur Erhöhung der Sicherheit gegen Manipulationen wird in der DE 42 40 897 C2 vorgeschlagen, neben einem Identifikationscode, der in einem nicht löschbaren Speicher des Transponders gespeichert ist, einen Zufallscode in einem löschbaren Speicher zu speichern, der vom Schreib-Lesegerät generiert und zum Transponder übermittelt wird. Beim späteren Lesen wird der Identifikationscode und der Zufallscode ausgewertet. Manipulationsversuche mit einem zweiten Transponder, in dem eine Kopie des Identifikationscode gespeichert ist, können so entdeckt werden, da ja bei der Auswertung zusätzlich der Zufallscode mit ausgewertet wird und dieser mit hoher Wahrscheinlichkeit nicht im zweiten Transponder gespeichert sein kann.

Da bei der Datenkommunikation zwischen dem Schreib-Lesegerät und dem Transponder die vom Transponder benötigte Energie mit übertragen wird, erlaubt die verwendete Sendeleistung ein Abhören der Datenkommunikation mit empfindlichen Empfängern über eine Entfernung von mehreren Metern. Durch Abhören der Datenkommunikation kann der Zufallscode identifiziert und eine Speicherkopie in einem zweiten Transponder abgelegt werden. Der zugeordnete Identifikationscode wird ebenfalls übertragen, und zwar durch Lesen des nicht löschbaren Speichers, damit beim Schreib-Lesegerät eine Zuordnung zwischen Identifikationscode und Zufallscode möglich ist. Mit einer solchen Kopie kann dann ebenfalls eine frühere Ankunft der Taube vorgetäuscht werden.

Es besteht die Aufgabe, das Verfahren so auszubilden, daß die Manipulationssicherheit weiter verbessert wird.

Gelöst wird diese Aufgabe mit den kennzeichnenden Merkmalen des Anspruchs 1. Vorteilhafte Ausgestaltungen und weitere Maßnahmen zur Erhöhung der Sicherheit gegen Manipulationen sind den Unteransprüchen entnehmbar.

Bei der Erfindung wird davon ausgegangen, daß im löschbaren Speicher des Transponders von einer erstmaligen Programmierung her oder auch von vergangenen Einsatzfällen ein Datenwort gespeichert ist. Dieses Datenwort enthält eine Information, die eine dem Transponder zugeordnete Identnummer umfaßt. Zusätzlich kann die Informationen auch noch andere Angaben enthalten. Wenn nach Kenntnis dieses Datenwortes wiederum ein geändertes Datenwort generiert wird, so unterscheidet sich dieses von dem vorher ausgelesenen Datenwort. Daher ist es nicht möglich, ohne besondere Insiderkenntnisse durch einfaches Abhören der Datenkommunikation zwischen Schreib-Lesegerät und Transponder die Identnummer nach systematischen Gesichtspunkten zu selektieren.

Es besteht die Möglichkeit, im Schreib-Lesegerät eine Zuordnungsliste zwischen Datenworten und den Transpondern zugehörigen Identnummern zu speichern und die Zuordnungsliste bei Änderung von Datenworten zu aktualisieren. Ohne Zuordnungsliste lassen sich somit die Identnummern nicht entschlüsseln und für Manipulationszwecke verwenden.

Alternativ kann im Schreib-Lesegerät und/oder im Transponder ein Schlüssel gespeichert werden, mit dem die Information des Datenwortes entschlüsselbar ist und im Schreib-Lesegerät ferner Informationen für eine Anwendung des Schlüssels gespeichert werden. Dann lassen sich im Schreib-Lesegerät die Datenworte unter Anwendung des Schlüssels beim Lesen decodieren und beim Schreiben codieren.

Vorzugsweise wird das Datenwort aus einer verschlüsselten Identnummer und einer Zufallszahl erzeugt. In diesem Fall sind Identnummer und Zufallszahl nicht mehr getrennt, sondern bilden im seriellen Datenstrom einen untrennbaren Verbund.

Im einfachsten Fall kann der Schlüssel die Position der Bits im Datenwort verändern. Die Bits werden dann je nach dem verwendeten Schlüssel so verwürfelt, daß die Identnummer und die Zufallszahl ineinander verschachtelt sind und außerdem die einzelnen Stellen in anderer Reihenfolge erscheinen, als sie den Zahlen im Klartext entsprechen.

Eine Verbesserung gegen Brechen des Schlüssels besteht darin, daß der Schlüssel einen von mehreren gespeicherten Algorithmen zur Verschlüsselung des Datenwortes auswählt und aktiviert. In diesem Fall müßte also noch zusätzlich der Algorithmus bekannt sein, um die gesamte Verschlüsselung des Datenwortes aufheben zu können.

Darüber hinaus kann gemäß einer Weiterbildung der Schlüssel auch selbst Bestandteil der Algorithmen der Verschlüsselung des Datenwortes sein und zusammen mit dem Datenwort übertragen werden. Da in die-

sem Fall die Verschlüsselung noch komplizierter ist, erfordert die Entschlüsselung ebenfalls einen nochmals gesteigerten Aufwand.

Um eine Weitergabe des Schlüssels durch Spionage zu verhindern, kann der Schlüssel mittels eines Zufallsgenerators bei jedem Schreibvorgang erzeugt werden.

Zur Erhöhung der Betriebssicherheit wird nach jedem Schreibvorgang ein Kontrollesevorgang durchgeführt und bei fehlerhaften Daten ein Schreib- und anschließender Kontrollesevorgang mehrmals wiederholt. Dies stellt sicher, daß keine fehlerhaften Daten im Speicher des Transponders gespeichert werden, die eine Auswertung unmöglich machen oder erschweren. Im Hinblick auf Manipulationssicherheit dient dies dazu, solche Manipulationsversuche auszuschließen, die sich auf die Behauptung stützen, beim Schreibvorgang wären Daten zerstört worden.

Bei manueller Einbringung des Transponders in das Feld des Schreib-Lesegerätes wird nach einem erfolgreichen Schreib- und Kontrollesevorgang ein optisches und/oder akustisches Quittungssignal erzeugt. Hierdurch ist sichergestellt, daß die Datenkommunikation gerade so lange besteht, wie sie für ein korrektes Beschreiben des Speichers im Transponder erforderlich ist, aber andererseits nicht zu lange, um Manipulationen durch Abhören zu erleichtern.

Ferner kann vom Schreib-Lesegerät ein Fehlerprüfcode erzeugt und mit dem Datenwort übertragen werden und der Fehlerprüfcode im Speicher des Transponders abgelegt werden. Beim Lesen wird er zusammen mit dem Datenwort ausgelesen und die Gültigkeit des Datenwortes anhand des Fehlerprüfcodes im Schreib-Lesegerät ermittelt.

Die Verwendung eines Fehlerprüfcodes ermöglicht es ferner, nach dem Schreiben die Gültigkeit des Datenwortes anhand des Fehlerprüfcodes intern im Transponder zu ermitteln. Es kann dann beim Kontrollesevorgang ein Gültigkeitscode statt des Datenwortes übertragen werden. Auf diese Weise läßt sich verhindern, daß beim Kontrollesevorgang nochmals das verschlüsselte Datenwort übertragen wird.

Weiterhin kann beim Kontrollesevorgang und/oder beim Lesevorgang das geschriebene Datenwort in umcodierter Form rückübertragen werden. In diesem Fall reicht es nicht aus, das zum Transponder gesendete Datenwort zu speichern und bei Manipulationsversuchen identisch zu senden, da das beim Lesen abgefragte Datenwort ja ein anderes ist. Vielmehr müßte in diesem Fall das mit sehr viel geringerer Sendeleistung rückübertragene Datenwort abgehört und aufgezeichnet werden, was vom Aufwand her wesentlich schwieriger als das Abhören und Aufzeichnen des vom Schreib-Lesegerät zum Transponder gesendeten Datenwortes ist.

Eine weitere Verbesserung der Manipulationssicherheit wird erreicht, wenn beim Kontrollesevorgang und beim Lesevorgang das Datenwort zyklisch verändert wird. Es reicht dann nicht mehr aus, das beim Kontrollesevorgang übermittelte Datenwort aufzuzeichnen und wiederzugeben, da ja bei jedem weiteren Lesevorgang ein anderes Datenwort verlangt wird.

Weiterhin können bei jedem Identifikationsschritt mehrere Lesevorgänge ausgeführt werden. Wenn beim Kontrollesevorgang das nur einmal gesendete Datenwort abgehört und gespeichert wird, gelingt es nicht zwei gültige aber verschiedene Datenworte zu übertragen.

Schließlich kann das Zeitraster, in dem die Lesevorgänge stattfinden, vom Lesegerät veränderbar sein. Selbst wenn der beim Abhören eines Lesevorganges aufgezeichnete Datenstrom die richtigen Informationen enthielte, könnten Manipulationen erkannt werden, wenn bei Veränderung des Zeitrasters die Daten in einem anderen Zeitraster erwartet werden als sie gesendet werden.

Mit dem ersten und weiteren Identifikationsschritt können weitere physikalische Größen im Schreib-Lesegerät und/oder im Speicher des Transponders abgelegt oder gelesen werden. Hierbei kann es sich z.B. um Zeitangaben handeln.

Vorzugsweise ist in einem weiteren löschbaren Bereich des Speichers des Transponders eine Kopie der Identnummer abgelegt, die bedarfsweise auslesbar ist. Hierdurch läßt sich eine beim Schreiben beschädigte Identnummer wieder zurückgewinnen. Durch die Verwendung eines ebenfalls löschbaren Bereichs ist die Möglichkeit gegeben, den Transponder zur Wiederverwendung auch mit einer anderen Identnummer zu programmieren.

Ein Ausführungsbeispiel der Erfindung wird nachfolgend anhand der Zeichnung erläutert. Die Zeichnung zeigt in Fig. 1 bis 3 schematische Darstellungen eines löschbaren Speichers und die Zuordnung der Speicherstellen.

Verwendet wird ein Transponder mit einem löschbaren Speicher, der flexibel in mehrere Bereiche aufgeteilt sein kann, sowie einer Sendelogik, einer Stromversorgungselektronik und einer Antenne.

Die spätere Stromversorgung des Transponders erfolgt durch Gleichrichtung und Glättung des durch die Antenne empfangenen elektromagnetischen Feldes. Bei diesem Transponder wird in den löschbaren Speicher bei einer ersten Programmierung ein Datenwort eingegeben, das u. a. eine Identnummer des Transponders umfaßt. Diese Identnummer kann bei Verwendung als Taubentransponder das Geburtsjahr, das Geburtsland, die Taubenfarbe und das Geschlecht der Taube sowie eine fortlaufende Nummer enthalten. Damit gibt es eine eindeutige Zuordnung zwischen Tauben und Transpondern.

Fig. 1 zeigt den grundsätzlichen Aufbau eines Datenwortes, das aus einem Block mit der Bezeichnung "Identnummer" und einem Block mit der Bezeichnung "Zufallszahl" besteht. Die Eigenschaft "dynamisch" besagt, daß der Inhalt dieses Datenwortes und damit

des Speicherbereichs verändert wird. Ein weiterer Speicherbereich enthält eine Kopie der Identnummer. Die Eigenschaft "statisch" besagt, daß dieser Speicherbereich normalerweise nicht verändert wird, es sei denn, daß eine andere Identnummer gespeichert werden soll. Auf den statischen Speicherbereich kann auch beim normalen Lesen und Schreiben nicht zugegriffen werden. Dies ist nur durch eine besondere Freigabefunktion möglich, wenn eine beim Schreiben zerstörte Identnummer gelesen und repariert werden soll.

Fig. 2 zeigt ein erweitertes Datenwort, daß außer der Identnummer und der Zufallszahl auch einen Schlüssel und eine CRC-Prüfsumme enthält. Dem dargestellten Aufbau des Datenwortes ist die Speicherung im löschbaren Speicher anhand des Schlüssels gegenübergestellt. Außerdem ist durch Indizes die Wertigkeit der Bits darstellt. Der Schlüssel bestimmt, wie die einzelnen Bits der Identnummer I und der Zufallszahl Z miteinander verwürfelt gespeichert werden. Der Schlüssel selbst und die CRC Prüfsumme hingegen belegen in der Wertigkeit ihrer Bits unmittelbar aufeinanderfolgende Speicherplätze.

Fig. 3 zeigt eine Variante, bei der auch der Schlüssel S mit den Bits der Identnummer I und der Zufallszahl verwürfelt ist.

Das Datenwort kann durch ein Lesegerät berührungslos ausgelesen werden, wenn sich die Taube in der Nähe der Antenne des Schreib-Lesegerätes aufhält. Nimmt die Taube an einem Wettkampf teil, dann wird sie vor dem Einkorben in das Feld der Antenne eines Schreib-Lesegerätes gebracht. Das Schreib-Lesegerät liest und entschlüsselt eine nach einer Erstbeschreibung oder einer Beschreibung in vorangegangenen Einsatzfällen verschlüsselt gespeicherte Identnummer. Aus dieser Identnummer und einer erzeugten Zufallszahl wird anhand eines Schlüssels ein neues Datenwort erzeugt und dieses Datenwort seriell berührungslos zum Transponder übertragen. Dort wird es in einem löschbaren Speicher des Transponders abgelegt. Gleichzeitig werden die Daten auch im Schreib-Lesegerät gespeichert.

Gelangt die Taube zu ihrem Schlag, dann durchwandert sie das Feld eines Lesegerätes, welches das gespeicherte Datenwort ausliest, entschlüsselt und die zurückgewonnene Identnummer mit der Zufallszahl registriert. Dabei wird gleichzeitig die Ankunftszeit und das Datum registriert. Nach Koppelung mit dem Schreib-Lesegerät des Wettflugveranstalters erfolgt dann die Auswertung.

Patentansprüche

1. Verfahren zur Identifizierung von an sportlichen Wettbewerben teilnehmenden Personen oder Tieren, insbesondere Brieftauben, an denen ein Transponder angebracht wird, der einen Speicher enthält, in dem ein Datenwort speicherbar ist und mittels eines Schreib-Lesegerätes berührungslos gelesen, registriert und ausgewertet wird, dadurch gekennzeichnet, daß beim Beschreiben zuerst ein in einem löschbaren Speicher des Transponders gespeichertes Datenwort gelesen, eine in dem Datenwort enthaltene Information, die eine dem Transponder zugeordnete Identnummer umfaßt, ausgewertet wird und anschließend ein geändertes Datenwort erzeugt wird, das ebenfalls eine Information mit der dem Transponder zugeordneten Identnummer umfaßt, und dieses geänderte Datenwort im löschbaren Speicher des Transponders abgelegt wird und daß beim Lesen das zuletzt gespeicherte Datenwort ausgelesen, ausgewertet und im Schreib-Lesegerät registriert wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß im Schreib-Lesegerät eine Zuordnungsliste zwischen Datenworten und den Transpondern zugehörigen Identnummern gespeichert ist und die Zuordnungsliste bei Änderung von Datenworten aktualisiert wird.

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß im Schreib-Lesegerät und/oder im Transponder ein Schlüssel gespeichert ist oder wird, mit dem die Information des Datenwortes entschlüsselbar ist, daß im Schreib-Lesegerät ferner Informationen für eine Anwendung des Schlüssels gespeichert sind und daß im Schreib-Lesegerät die Datenworte unter Anwendung des Schlüssels beim Lesen decodiert und beim Schreiben codiert werden.

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß das Datenwort aus einer verschlüsselten Identnummer und einer Zufallszahl erzeugt wird.

5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß mittels des Schlüssels die Positionen der Bits im Datenwort verändert werden.

6. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß mittels des Schlüssels einer von mehreren gespeicherten Algorithmen zur Verschlüsselung des Datenwortes ausgewählt und aktiviert wird.

7. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß der Schlüssel selbst Bestandteil der Algorithmen zur Verschlüsselung des Datenwortes ist und zusammen mit dem Datenwort übertragen wird.

8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, daß der Schlüssel mittels eines Zufallsgenerators bei jedem Schreibvorgang

erzeugt wird.

9. Verfahren nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, daß nach jedem Schreibvorgang ein Kontrollesevorgang durchgeführt wird und bei fehlerhaften Daten ein Schreib- und anschließender Kontrollesevorgang mehrmals wiederholt wird.

10. Verfahren nach Anspruch 9, dadurch gekennzeichnet, daß bei manueller Einbringung des Transponders in das Feld des Schreib-Lesegerätes nach einem erfolgreichen Schreib- und Kontrollesevorgang ein optisches und/oder akustisches Quittungssignal erzeugt wird.

11. Verfahren nach einem der Ansprüche 1 bis 10, dadurch gekennzeichnet, das vom Schreib-Lesegerät ein Fehlerprüfcode erzeugt und mit dem Datenwort übertragen wird und daß der Fehlerprüfcode im Speicher des Transponders abgelegt wird und beim Lesen zusammen mit dem Datenwort ausgelesen wird und die Gültigkeit des Datenwortes anhand des Fehlerprüfcodes im Schreib-Lesegerät ermittelt wird.

12. Verfahren nach Anspruch 11, dadurch gekennzeichnet, daß nach dem Schreiben die Gültigkeit des Datenwortes anhand des Fehlerprüfcodes intern im Transponder ermittelt wird und daß beim Kontrollesevorgang nur ein Gültigkeitscode übertragen wird.

13. Verfahren nach einem der Ansprüche 1 bis 11, dadurch gekennzeichnet, daß beim Kontrollesevorgang und/oder beim Lesevorgang das geschriebene Datenwort in umkodierter Form rückübertragen wird.

14. Verfahren nach einem der Ansprüche 1 bis 13, dadurch gekennzeichnet, daß bei jedem Kontrollesevorgang und/oder bei jedem Lesevorgang das Datenwort zyklisch verändert wird.

15. Verfahren nach Anspruch 13, dadurch gekennzeichnet, daß bei jedem Identifikationsschritt der Lesevorgang mehrfach ausgeführt wird.

16. Verfahren nach Anspruch 15, dadurch gekennzeichnet, daß die Lesevorgänge in einem Zeitraster durchgeführt werden, das vom Lesegerät nach Zufallskriterien bestimmt wird.

17. Verfahren nach einem der Ansprüche 1 bis 16, dadurch gekennzeichnet, daß mit dem ersten und dem weiteren Identifikationsschritt weitere physikalische Größen im Schreib-Lesegerät und/oder im Speicher des Transponders abgelegt oder gelesen werden.

18. Verfahren nach einem der Ansprüche 1 bis 17, dadurch gekennzeichnet, das in einem weiteren löschbaren Bereich des Speichers des Transponders eine Kopie der Identnummer abgelegt wird, die bedarfsweise auslesbar ist.

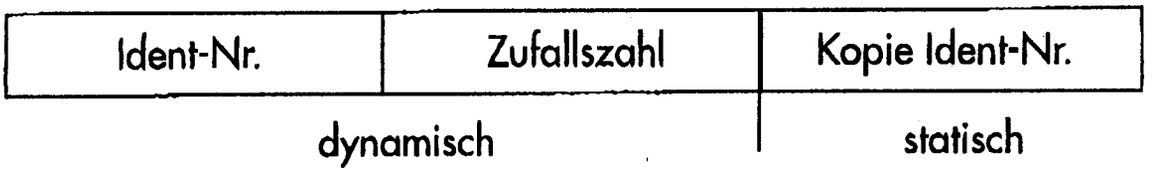

Fig. 1

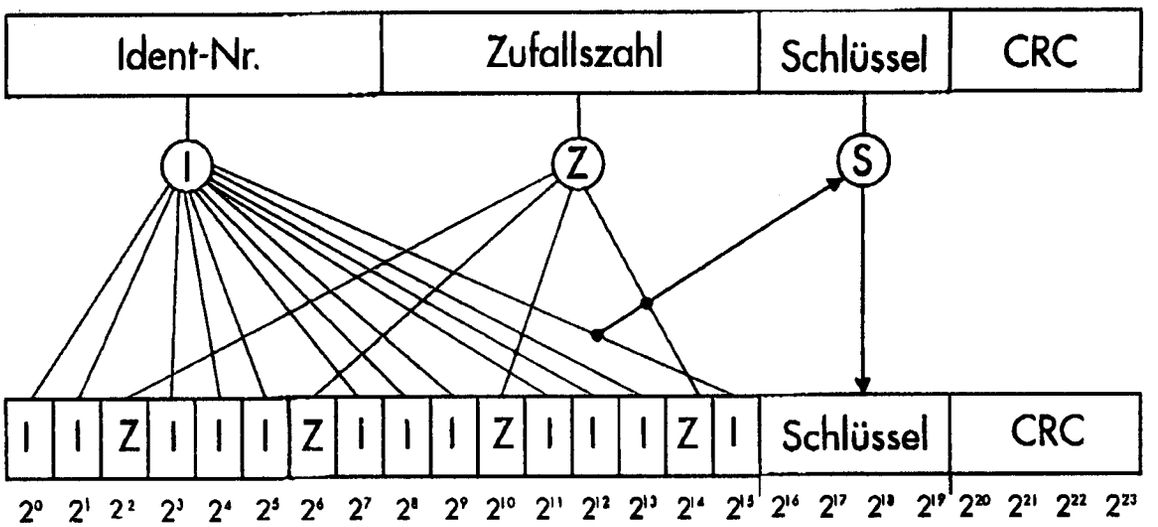

Fig. 2

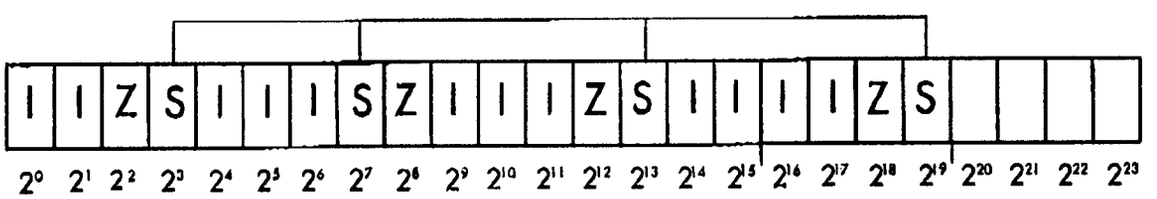

Fig. 3