(51) Int. Cl. 2: H 04 L 9/02

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

DE 9 78 065 C1

(11) Patentschrift 9 78 065

(21) Aktenzeichen: P 9 78 065.8-31

(22) Anmeldetag: 21. 3. 60

(43) Offenlegungstag: —

(44) Bekanntmachungstag: —

(45) Ausgabetag: 15. 6. 78

(30) Unionspriorität:

(32) (33) (31) —

---

(54) Bezeichnung: Schaltungsanordnung zum Ver- bzw. Entschlüsseln von n unterscheidbaren, vorzugsweise binär codierten Schriftzeichen

(73) Patentiert für: Fa. Dr.-Ing. Rudolf Hell, 2300 Kiel

(72) Erfinder: Hell, Rudolf, Dr.-Ing., 2300 Kiel

---

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:

DE-PS 9 74 447
DE-PS 9 59 020
DE-AS 10 54 491

Erteilt auf Grund des Par. 30e PatG i.d. Fassung v. 09.05.61

DE 9 78 065 C1

Patentansprüche:

1. Schaltungsanordnung zum Ver- bzw. Entschlüsseln von *n* unterscheidbaren, vorzugsweise binär codierten Schriftzeichen durch Mischung der zu verschlüsselnden Klarzeichen bzw. der zu entschlüsselnden Geheimzeichen mit vorgegebenen Schlüsselzeichen nach einem beliebig wählbaren Mischgesetz, gekennzeichnet durch einen Klar- bzw. Geheimzeichengeber (7) mit *n* Ausgängen, durch *n* je *n* Ein- und Ausgänge aufweisende Permutationsschalter (8 bis 10), deren Eingänge gleicher Ordnungsnummer jeweils parallel mit dem entsprechenden Ausgang des Klar- bzw. Geheimzeichengebers (7) verbunden sind und deren jeder Ausgang mit dem ersten Eingang je einer Torschaltung (z. B. 13, 23 bis 25) verbunden ist, durch einen synchron mit dem Klar- bzw. Geheimzeichengeber (7) arbeitenden Schlüsselzeichengeber (21) mit *n* Ausgängen, deren jeder mit den zweiten Eingängen der jeweils einem Permutationsschalter (8 bis 10) zugeordneten Torschaltungen (z. B. 13, 23 bis 25) verbunden ist, und durch eine Ver- bzw. Entschlüsselungsausgabevorrichtung (27) mit *n* Eingängen, deren jeder mit den jeweils parallelgeschalteten Ausgängen entsprechender Torschaltungen (d. h. gleicher Ordnungsnummer) aller Permutationsschalter (8 bis 10) verbunden ist.

2. Schaltungsanordnung nach Anspruch 1, dadurch gekennzeichnet, daß die Permutationsschalter (8 bis 10) derart ausgebildet sind, daß die die Ein- und Ausgänge jedes Permutationsschalters miteinander verbindenden Schaltmittel wahlweise eine von zwei zueinander spiegelbildlichen Durchschaltungen ermöglichen.

3. Vorrichtung nach Anspruch 1 und 2, dadurch gekennzeichnet, daß die Permutationsschalter (8 bis 10) als Drehschalter mit zwei um 180° gegeneinander versetzten Schaltstellungen ausgebildet sind und daß die Eingangs- und gegenüberliegenden Ausgangskontakte ihrer Rotoren als Schleifkontakte oder Bürsten ausgebildet sind, die mit den in Form von zwei raumfest angeordneten, gegenüberliegenden Reihen von Schleifkontakten bzw. Bürsten ausgebildeten Ein- und Ausgängen bei Drehung der Rotoren der Permutationsschalter in den beiden ausgezeichneten Stellungen Kontakt geben.

4. Vorrichtung nach Anspruch 1 bis 3, dadurch gekennzeichnet, daß die Permutationsschalter (8 bis 10) als auswechselbare Steckeinheiten ausgebildet sind.

5. Schaltungsanordnung für sogenannten »On-Line«-Betrieb zur Fernübertragung verschlüsselter Nachrichten im Fernschreibcode nach Anspruch 1 bis 4 unter Verwendung von Umsetzern zum Umwandeln von Mehrschrittalphabetzeichen in Einschrittalphabetzeichen bzw. umgekehrt, gekennzeichnet durch eine Fernschreibmaschine (1), einen mit dieser verbundenen Impulsspeicher (5) zur Serien-Parallel-Umsetzung der Fernschreibzeichen in abgehender Richtung, einen dem Impulsspeicher (5) nachgeschalteten, als Klarzeichengeber ausgebildeten ersten Umsetzer (7), durch einen mit diesem synchronisierten Lochstreifenabtaster (15), dem ein als Schlüsselzeichengeber ausgebildeter zweiter Umsetzer (21) nachgeschaltet ist, einen dritten, als Ver- bzw. Entschlüsselungsausgabevorrichtung ausgebildeten Umsetzer (27) an der Ausgabeseite der Mischvorrichtung, durch einen dem Umsetzer (27) nachgeschalteten Impulsgeber (29) zur Parallel-Serien-Umsetzung der Fernschreibzeichen in abgehender und ankommender Richtung, einen mit den fünf Ausgängen des Impulsspeichers (5) für die abgehende Richtung verbundenen Impulsspeicher (33) zur Serien-Parallel-Umsetzung der Fernschreibzeichen in ankommender Richtung, durch jeweils ein Sperrtor (3, 41), über welches der Eingang des Impulsspeichers (5) für die abgehende Richtung und der Ausgang des Impulsgebers (29) an die Fernschreibmaschine (1) angeschlossen sind, und durch jeweils ein Sperrtor (31, 34), über welches der Ausgang des Impulsgebers (29) und der Eingang des Impulsspeichers (33) für die ankommende Richtung an die Fernleitung (32) angeschlossen sind.

Die Erfindung betrifft eine Schaltungsanordnung zum Ver- bzw. Entschlüsseln von *n* unterscheidbaren, vorzugsweise binär codierten Schriftzeichen durch Mischung der zu verschlüsselnden Klarzeichen bzw. der zu entschlüsselnden Geheimzeichen mit vorgegebenen Schlüsselzeichen nach einem beliebig wählbaren Mischgesetz.

Es ist seit langem ein Verschlüsselungsverfahren bekannt, das darin besteht, daß die Schriftzeichen (oder die diese darstellenden Codezeichen) des geheimzuhaltenden Klartextes mit den Schriftzeichen (oder den diese darstellenden Codezeichen) eines sinnlosen oder sinnvollen, nur den Chiffrierteilnehmern bekannten Schlüsseltextes paarweise gemischt werden, derart, daß sich als Ergebnis der Mischung ein Geheimtext ergibt, der eindeutig nur mit Hilfe des Schlüsseltextes und des Mischgesetzes durch Rückmischung entschlüsselt werden kann.

Hierbei ist jedem geordneten Paar aus einem Klarschriftzeichen K und einem Schlüsselzeichen S ein Geheimschriftzeichen G derselben Art eindeutig. Wegen der Notwendigkeit, den Geheimtext eindeutig mit Hilfe desselben Schlüsseltextes entschlüsseln zu können, ist an die Rückmischung die Forderung zu stellen, daß auch jedem geordneten Paar aus einem Geheimschriftzeichen G und einem Schlüsselzeichen S ein Klarschriftzeichen K eindeutig zugeordnet ist, d. h., daß die Zuordnung $G=f(K, S)$ bezüglich der Größe K umkehrbar eindeutig oder eineindeutig ist. Diese Zuordnung wird in Anlehnung an die Gruppentheorie als symbolische Multiplikation dargestellt:

$$G=K \cdot S$$

bzw.

$$K=G \cdot S$$

Die Zuordnung wird festgelegt, indem man eine quadratische Tabelle mit einem vertikalen Eingang, beispielsweise für die Klarzeichen, und einem horizontalen Eingang für die Schlüsselzeichen anlegt. In der Eingangsspalte und in der Eingangszeile werden die Schriftzeichen (oder diese darstellenden Codezeichen) in irgendeiner Reihenfolge, z. B. der alphabetischen, angeschrieben. In den Kreuzungspunkten der Spalten und Zeilen werden die zugeordneten Geheimschriftzeichen eingetragen. In der Eingangsspalte für die Klarzeichen sucht man die zu dem zu verschlüsselnden Klarzeichen gehörende Zeile auf. In der Eingangszeile

für die Schlüsselzeichen sucht man die zu dem gewählten Schlüsselzeichen gehörende Spalte auf. Im Kreuzungspunkt der betreffenden Zeile mit der betreffenden Spalte steht das Geheimzeichen. Die Zuordnung braucht nicht kommutativ zu sein, d. h., es braucht nicht notwendigerweise

$$G=K \cdot S=S \cdot K$$

zu sein. Bei kommutativer Zuordnung ist die Zuordnungsmatrix mit ihrer transponierten Matrix identisch. Dies bedeutet, daß die Spalten mit den Zeilen gleicher Ordnungsnummer übereinstimmen. Die Matrix erscheint in einem solchen Falle an der Hauptdiagonalen gespiegelt.

Damit die Entschlüsselung, d. h. die Rückmischung, eindeutig ist, ist hinreichend, aber nicht notwendig, daß in jeder Spalte jedes Geheimzeichen nur ein einziges Mal vorkommt und daß keine zwei gleichen Spalten vorhanden sind, d. h., daß alle Spalten verschiedene Permutationen aller beteiligten Schriftzeichen darstellen.

Zur Entschlüsselung geht man in diejenige Spalte hinein, die durch das betreffende Schlüsselzeichen am horizontalen Matrixeingang bestimmt ist und sucht das Geheimzeichen in dieser Spalte auf. Am vertikalen Eingang derjenigen Zeile, in der das zu entschlüsselnde Geheimzeichen angetroffen wird, steht das zugeordnete Klarzeichen.

Zweckmäßigerweise stellt man zum Entschlüsseln eine zweite Tabelle her, an deren vertikaler Eingangsspalte alle Geheimzeichen und an deren horizontaler Eingangszeile alle Schlüsselzeichen in möglichst derselben Reihenfolge wie bei der Verschlüsselungstabelle angeschrieben sind. In den Kreuzungspunkten der Zeilen und Spalten werden die zugeordneten Klarzeichen eingetragen.

Die Verschlüsselungstabelle wird im allgemeinen von der Entschlüsselungstabelle verschieden sein. Bei besonderer Wahl der Mischfunktion kann man es erreichen, daß die Entschlüsselungstabelle mit der Verschlüsselungstabelle identisch wird. Dann ist die Zuordnung involutorisch, d. h., die Umkehrungsfunktion oder die zu $G=f(K, S)$ inverse Funktion $K=g(G, S)$ ist bezüglich K mit der Mischfunktion $G=f(K, S)$ identisch, $f=g$, mit anderen Worten, die Mischfunktion ist zu sich selbst invers. Hierzu ist notwendig und hinreichend, daß die Spalten der Mischtabelle symmetrische Alphabetpermutationen darstellen. Eine symmetrische Permutation ist eine solche, die, mit sich selbst hintereinander ausgeführt, die identische Permutation ergibt. Man kann sogar Mischtabellen aufstellen, bei denen die Mischfunktion sowohl kommutativ als auch involutorisch ist.

Mischtabellen mit diesen Symmetrieeigenschaften werden beim Verschlüsseln bevorzugt, weil dabei der Verschlüsselungsschlüssel gleich dem Entschlüsselungsschlüssel ist und weil man den Klartext mit dem Schlüsseltext beim Mischen in der Reihenfolge vertauschen kann, was große gerätetechnische Vereinfachungen bedeutet, da alle Chiffrierteilnehmer die gleichen Geräte zum Ver- und Entschlüsseln verwenden können.

Besonders bevorzugt wird die folgende Mischzuordnung, die wegen ihrer sehr einfachen gerätetechnischen Durchführung vor allem bei sogenannten kommerziellen Fernschreibverbindungen sehr verbreitet ist, indem in vielen Fernschreibmaschinen eine solche Mischvorrichtung fest eingebaut ist, die unter der Bezeichnung »Zwillingskopf« bekannt ist.

Die Fernschreibzeichen werden bekanntlich als Variationen (permutierte Kombinationen) zweier verschiedener elektrischer Zustände zur fünften Klasse mit Wiederholung übertragen. Beim Fernschreib-Fünfercode gibt es dementsprechend $2^5=32$ verschieden mögliche Fernschreibzeichen. Die beiden elektrischen Zustände bestehen entweder aus zwei bipolaren Impulsen gleicher Amplitude oder aus zwei monopolaren Impulsen verschiedener Amplituden, deren eine meistens Null ist. Bezeichnet man diese beiden elektrischen Zustände mit den Zeichenelementen (+) und (−), so besteht die Mischung darin, daß die einzelnen einander entsprechenden Zeichenelemente gleicher Stellenzahl einer Klar- und einer Schlüsselzeichenkombination nach der Vorzeichenregel: Gleiche Vorzeichen ergeben das eine, ungleiche das andere Zeichenelement, paarweise miteinander gemischt werden. Hierfür gibt es zwei Möglichkeiten, nämlich

$$+ \cdot + = - \cdot - = +$$
$$+ \cdot - = - \cdot + = -$$

und

$$+ \cdot + = - \cdot - = -$$
$$+ \cdot - = - \cdot + = +,$$

die aber bekanntlich ineinander übergehen, wenn man die beiden Zeichenelemente (+) und (−) in den Gleichungen miteinander vertauscht, da ja die Zuordnung der beiden Zeichenelemente zu den beiden dualen Zuständen willkürlich ist.

Durch die paarweise erfolgende Mischung der Zeichenelemente ergibt sich zwangläufig eine Mischung der Zeichenelementekombinationen, deren Gesetz man in der folgenden Weise beschreiben kann: Identifiziert man das Zeichenelement (+) mit der Dualziffer 0 und das Zeichenelement (+) mit der Dualziffer 1, so stellen die 32 möglichen Zeichenelementekombinationen die Zahlen von 0 bis 31 in dualer Schreibweise dar. Die Mischung zweier Dualzahlen geschieht gemäß den Vorzeichenregeln dann in der Weise, daß die beiden Dualzahlen addiert werden, ohne die Zweier-Stellen-Übertragung vorzunehmen, d. h. modulo 2^1, 2^2, 2^3, 2^4; also etwa z. B.:

$$\begin{array}{r} 7 = 00111 \\ \underline{13 = 01101} \\ 10 = 01010 \end{array}$$

während die korrekte, arithmetisch richtige Addition mit Zweier-Stellen-Übertragung zu

$$\begin{array}{r} 7 = 00111 \\ \underline{13 = 01101} \\ 20 = 10100 \end{array}$$

führt.

Das angegebene Mischverfahren hat einige bemerkenswerte Symmetrieeigenschaften. Zunächst genießt die Zuordnung die Gruppeneigenschaften. So gibt es ein sogenanntes Einheitselement $E=00000$, welches, mit allen anderen Elementen A gemischt, diese ungeändert läßt:

$$A \cdot E=E \cdot A=A.$$

Ferner ergibt jedes Element A, mit sich selbst gemischt, das Einheitselement: $A^2=E$. Jedes Element A der Gruppe ist also zu sich selbst invers: $A^{-1}=A$. Weiter ist die Gruppe kommutativ: $A \cdot B=B \cdot A$. Schließlich ist die Zuordnung involutorisch, d. h., die

Entschlüsselungstabelle ist mit der Verschlüsselungstabelle identisch: Wenn

$$G=K \cdot S=S \cdot K,$$

so ist auch

$$K=G \cdot S=S \cdot G.$$

Die Mischung zweier komplementärer Dualzahlen, d. h. zweier Dualzahlen, die sich zu 31 ergänzen, ergibt stets 31. Es sind dies alle Dualzahlenpaare, deren Spalten- und Reihenkreuzungspunkte auf der Nebendiagonalen der Matrix liegen.

Auf Grund der weitgehenden Symmetrieeigenschaften und der daraus folgenden sehr einfachen gerätetechnischen Durchführung des erwähnten Mischverfahrens sowie seines Bekanntseins und seiner allgemeinen Verbreitung ist seine verschlüsselungstechnische Güte, d. h. die Sicherheit gegen unbefugte Entschlüsselung, nur gering. Es genügen verhältnismäßig wenige sogenannte phasengleiche Sprüche — das sind Sprüche, bei deren Verschlüsselung man fahrlässiger Weise in denselben Periodenabschnitt des Schlüsseltextes gelangt, den man schon einmal verwendet hat —, die durch Bedienungsfehler immer wieder vorkommen, um eine unbefugte Entschlüsselung zu ermöglichen.

Durch die deutsche Patentschrift 9 59 020 ist bereits eine elektronische Vorrichtung zur Mischung von Klarfernschreibzeichen mit Schlüsselfernschreibzeichen nach einer beliebig gewählten Mischtabelle bekannt; diese elektronische Vorrichtung ist aber verhältnismäßig kompliziert und aufwendig.

Nun kann man aber ein solches Mischverfahren auch als ein Tauschalphabetverfahren auffassen, d. h., für jedes zu verschlüsselnde Schriftzeichen wird nach einem bestimmten Programm ein Tauschalphabet aus einer gewissen Anzahl von verschiedenen Tauschalphabeten ausgewählt, die im vorliegenden Fall gleich der Anzahl der Schriftzeichen ist. Diese Tauschalphabete (im Falle des Schulalphabets 26 Stück, im Falle der Fernschreibzeichen 32 Stück) stellen die Spalten einer Mischtabelle dar. Das Auswahlprogramm besteht aus dem Schlüsseltext, dessen einzelne Schriftzeichen das zu wählende Tauschalphabet, d. h. also die Matrixspalte, bestimmen. Bei dieser Auffassung ergibt sich eine gegenüber der erwähnten Vorrichtung beträchtliche Vereinfachung der elektronischen Durchführung des Mischverfahrens mit beliebigen Mischtabellen.

Gemäß der Erfindung ist die Schaltungsanordnung gekennzeichnet durch einen Klar- bzw. Geheimzeichengeber mit n Ausgängen, durch n je n Ein- und Ausgänge aufweisende Permutationsschalter, deren Eingänge gleicher Ordnungsnummer jeweils parallel mit dem entsprechenden Ausgang des Klar- bzw. Geheimzeichengebers verbunden sind und deren jeder Ausgang mit dem ersten Eingang je einer Torschaltung verbunden ist, durch einen synchron mit dem Klar- bzw. Geheimzeichengeber arbeitenden Schlüsselzeichengeber mit n Ausgängen, deren jeder mit den zweiten Eingängen der jeweils einem Permutationsschalter zugeordneten Torschaltungen verbunden ist, und durch eine Ver- bzw. Entschlüsselungsausgabevorrichtung mit n Eingängen, deren jeder mit den jeweils parallelgeschalteten Ausgängen entsprechender Torschaltungen (d. h. gleicher Ordnungsnummer) aller Permutationsschalter verbunden ist.

Nach einer weiteren Ausbildung der Erfindung sind die Permutationsschalter derart ausgebildet, daß die die Ein- und Ausgänge jedes Permutationsschalters miteinander verbindenden Schaltmittel wahlweise eine von zwei zueinander spiegelbildlichen Durchschaltungen ermöglichen.

Nach einer weiteren Ausbildung der Erfindung sind die Permutationsschalter als Drehschalter mit zwei um 180° gegeneinander versetzten Schaltstellungen ausgebildet, und die Eingangs- und gegenüberliegenden Ausgangskontakte ihrer Rotoren sind als Schleifkontakte oder Bürsten ausgebildet, die mit den in Form von zwei raumfest angeordneten, gegenüberliegenden Reihen von Schleifkontakten bzw. Bürsten ausgebildeten Ein- und Ausgängen bei Drehung der Rotoren der Permutationsschalter in den beiden ausgezeichneten Stellungen Kontakt geben.

An Hand eines Blockschaltbildes wird die Erfindung an einem Ausführungsbeispiel näher erläutert.

Die Zeichnung zeigt eine Schaltungsanordnung für sogenannten »On-Line«-Betrieb zur Fernübertragung verschlüsselter Nachrichten im Fernschreibcode, bei der die Ver- und Entschlüsselung gemäß der Erfindung vor sich geht. Es sei angenommen, daß der Schlüsseltext im üblichen Fernschreibcode in einem Lochstreifen gespeichert vorliegt. Zur Ver- bzw. Entschlüsselung seien ferner bei den miteinander geheim verkehrenden Chiffrierteilnehmern gleiche Schlüssellochstreifen vorhanden. Es sei weiter vorausgesetzt, daß die Chiffrierteilnehmer an der gleichen Stelle der Schlüssellochstreifen, d. h. mit der gleichen Lochkombination, den Übertragungsbetrieb beginnen.

Die Beschreibung gliedert sich in zwei Teile, und zwar in die der Verschlüsselung und die der Entschlüsselung. Die Sende- und die Empfangsanlage sind einander völlig gleich. Die Anlage kann also sowohl zum Verschlüsseln und zum Senden als auch zum Empfangen und Entschlüsseln verwendet werden.

Verschlüsseln und Senden

Zunächst werde die Anlage als Sendestelle betrachtet. Von der Fernschreibmaschine **1** gelangt der Klartext durch unmittelbares Tasten oder durch Abtasten eines den Klartext in codierter Form enthaltenden Lochstreifens in Form von zeitlich aufeinanderfolgenden Impulsen der einzelnen Impulskombinationen über die Leitung **2**, das geöffnete Tor **3** und die Leitung **4** an den Impulsspeicher **5**, welcher jeweils die Impulse einer Kombination sammelt. An den fünf Ausgängen des Speichers **5** treten die Impulskombinationen als Potentialkonstellationen auf. Über die fünf Leitungen **6** ist der Impulsspeicher **5** mit dem Umsetzer **7** verbunden, der z. B. in bekannter Weise aus einer Diodenmatrix besteht. Der Umsetzer **7** hat entsprechend den $n=32$ verschiedenen möglichen Fernschreibzeichen $n=32$ Ausgänge **(1), (2),..., (32)**; jedoch tritt, wenn die entsprechende Fünfer-Potentialkonstellation am Eingang des Umsetzers **7** anliegt, jeweils an nur einem der Ausgänge eine Spannung bzw. eine Potentialänderung auf. Der Umsetzer **7** wirkt wie ein Geber für zu verschlüsselnde Klarzeichen im Code 1 aus n. An jede dieser Ausgangsklemmen ist eine Sammelleitung angeschlossen, die an jeweils alle diejenigen Eingangsklemmen, die die gleiche Ordnungsnummer wie die Ausgangsklemme haben, von $n=32$ verschiedenen Permutationsschaltern **8... 9... 10** geführt ist. Diese sind mechanische Drehschalter mit je $n=32$ Eingangs- und $n=32$ gegenüberliegenden Ausgangsklemmen und einem zylindrischen oder rechtkantförmigen Rotor, der ebenfalls $n=32$ Eingangs- und $n=32$ gegenüberliegende Ausgangskontakte enthält, die paarweise nach irgendeinem Vertauschungsschema durch entsprechen-

de Verdrahtungen oder Brücken miteinander verbunden sind und eine Vertauschung der Stromwege bewirken. Ein solcher Permutationsschalter kann mit seinen beiden gegenüberliegenden Reihen von Eingangs- und Ausgangskontakten in zwei ausgezeichnete, um 180° gegeneinander versetzte Lagen gebracht werden, wo er einrastet und wobei entweder seine Eingangskontakte mit den Eingangsklemmen, seine Ausgangskontakte mit den Ausgangsklemmen, oder seine Ausgangskontakte mit den Eingangsklemmen und seine Eingangskontakte mit den Ausgangsklemmen Kontakt geben. Die durch die Verdrahtung gegebene Zuordnung der Ausgangskontakte zu den Eingangskontakten kann von zweierlei Art sein, und zwar symmetrisch und unsymmetrisch. Ist die Permutation symmetrisch, die die Stromwege durch den Permutationsschalter erfahren, so geht das Verdrahtungsbild bei Spiegelung an der Mittelachse des Permutationsschalters in sich über. Ist die Permutation unsymmetrisch und spiegelt man das zugehörige Verdrahtungsbild an der Mittelachse des Permutationsschalters, so geht es in das dazu spiegelbildlich unsymmetrische Verdrahtungsbild über. Im ersten Fall ist es gleichgültig, ob man von links nach rechts oder von rechts nach links durch den Permutationsschalter hindurchgeht; in beiden Fällen gelangt man zu derselben Permutation der Stromwege. Im zweiten Fall gelangt man zu zwei verschiedenen Permutationen der Stromwege, je nach dem man von links nach rechts oder von rechts nach links durch den Permutationsschalter hindurchgeht. Dies ist von Bedeutung beim Entschlüsseln im Gegensatz zum Verschlüsseln. Beim Verschlüsseln geht man von links nach rechts durch die Permutationsschalter. Beim Entschlüsseln müßte man, um die Verschlüsselung rückgängig zu machen, in umgekehrter Richtung, also von rechts nach links, durch die Permutationsschalter gehen. Da das letztere schaltungstechnisch unbequem ist, dreht man lieber die Permutationsschalter beim Entschlüsseln um 180° und geht wieder von links nach rechts durch die Permutationsschalter. Dies ist notwendig, wenn die Permutationsschalter unsymmetrische Permutationen der Stromwege bewirken. Bewirken die Permutationsschalter hingegen symmetrische Permutationen der Stromwege, so ist das Verdrehen um 180° beim Entschlüsseln überflüssig. Die Verdrehbarkeit kann in diesem Falle also entfallen. Diese Tatsache entspricht der eingangs erwähnten Tatsache, daß, falls die Spalten der Mischtabelle symmetrische Permutationen darstellen, die Entschlüsselungstabelle mit der Verschlüsselungstabelle identisch wird entsprechend der Tatsache, daß die durch die Mischtabelle gegebene Zuordnung in diesem Falle involutorisch ist.

Um die Verdrehung der $n=32$ Permutationsschalter beim Entschlüsseln mit einem einzigen Handgriff vornehmen zu können, ist es zweckmäßig, die Enden der Schalterachsen mit Zahnrädern zu versehen und diese Zahnräder in eine gemeinschaftliche Zahnstange oder, bei kreisförmiger Anordnung der Permutationsschalter, in ein gemeinschaftliches Zahnrad eingreifen zu lassen, welche bzw. welches verstellt wird. Die Achsenzahnräder können auch als Kegelräder ausgebildet werden, in welche dazu senkrecht angeordnete Kegelräder eingreifen, die auf einer gemeinschaftlichen Welle befestigt sind, die verstellt wird.

Um die Mischtabelle gelegentlich ändern zu können, um z. B. einen Tages-, Wochen- oder Monatsschlüssel zur Verfügung zu haben, sind die Permutationsschalter als Steckeinheiten ausgebildet, die untereinander sowie gegen andere ausgetauscht werden können.

Angenommen, das zu verschlüsselnde Fernschreibzeichen sei die Kombination Nr. 17, dann liegt an der Ausgangsklemme **(17)** des Umsetzers **7** Spannung, die über die Sammelleitung **11** an alle Eingangsklemmen **(17)** der n Permutationsschalter **8 ... 9 ... 10** gelangt. Durch die Permutationsschalter hindurch gelangt die Spannung an jeweils die ersten Steuereingänge der den Ausgangsklemmen der Permutationsschalter zugeordneten UND-Tore **12 ... 13 ... 14,** deren Durchlaßbedingungen aber erst dann erfüllt sind, wenn an ihren beiden Steuereingängen gleichzeitig Spannung vorhanden ist. Sie bleiben also zunächst gesperrt.

Der Lochstreifenabtaster **15,** der über die Leitung **16,** das Differenzierglied **17** und die Leitung **18** durch den Umsetzer **7** synchronisiert ist, tastet im gleichen Takt wie die Fernschreibmaschine den Schlüssellochstreifen **19** ab. Die abgetasteten Lochkombinationen werden als Potentialkonstellationen über die fünf Verbindungsleitungen **20** zum Eingang des Umsetzers **21** geführt. Dieser arbeitet ebenso wie der Umsetzer **7.** Entsprechend der im Abtastzeitpunkt gerade anliegenden Schlüsselkombination entsteht an einem und nur einem der $n = 32$ Ausgänge **(1), (2) ..., (32)** des Umsetzers **21** Spannung. Diese Ausgänge stellen den Schlüsselzeichengeber dar. Jeder dieser Ausgänge ist jeweils mit allen $n = 32$ zweiten Steuereingängen aller n Und-Tore je eines der m Permutationsschalter verbunden, und zwar der Ausgang **(1)** mit allen 32 zweiten Steuereingängen der dem 1. Permutationsschalter **8** zugeordneten Und-Tore usw., und der letzte Ausgang **(32)** mit allen 32 zweiten Steuereingängen der dem 32. und letzten Permutationsschalter **10** zugeordneten Und-Tore. Der spannungsführende Ausgang des Umsetzers **21** liefert die zur Erfüllung der Durchlaßbedingungen für die Tore erforderliche zweite Spannung. Angenommen, das im betrachteten Zeitpunkt abgetastete Schlüsselfernschreibzeichen sei Nr. 16, dann entsteht am Ausgang **(16)** des Umsetzers **21** an der Leitung **22** Spannung. Diese Spannung wird den zweiten Steuereingängen aller Und-Tore **23 ... 13 ... 24 ... 25** des 16. Permutationsschalters **9** zugeführt. Das Und-Tor **13,** welches durch die Tastung bzw. Abtastung des Klarfernschreibzeichens Nr. 17 vorbereitet war, wird durchlässig. Alle übrigen Tore **23 ... 24 ... 25** des 16. Permutationsschalters **9** bleiben gesperrt. Es gelangt also Spannung an die Ausgangsleitung **26** des Und-Tores **13.** Der Permutationsschalter **9** hat durch seine innere Verdrahtung das Klarzeichen Nr. 17 in einem ersten Verschlüsselungsgang in ein anderes Zeichen, z. B. in das Geheimzeichen Nr. 7, verwandelt. Die Ausgangsleitung **26** des Tores **13** ist daher dem Fernschreibzeichen Nr. 7 zugeordnet und deshalb mit der siebten Eingangsklemme **(7)** des Umsetzers **27** verbunden. Die 32 Eingangsklemmen des Umsetzers **27** stellen die Verschlüsselungsausgabe dar. Über die fünf Ausgangsleitungen **28** wird die dem Zeichen Nr. 7 zugeordnete Fünfer-Kombination als Potentialkonstellation zu dem Impulsgeber **29** geleitet, der die Impulse der entsprechenden Impulskombination zeitlich nacheinander im Fernschreibtakt über die Leitung **30** und das geöffnete Tor **31** auf die Fernleitung **32** entläßt.

Empfangen und Entschlüsseln

Auf der Empfangsseite befindet sich die gleiche Anlage, wie sie auf der Sendeseite verwendet wird, erweitert um den Impulsspeicher **33.** Die Impulse der einzelnen Impulskombinationen der empfangenen Ge-

heimfernschreibzeichen gelangen zeitlich nacheinander im Fernschreibtakt von der Fernleitung **32** über das geöffnete Tor **34** und die Leitung **35** zum Impulsspeicher **33**, wo sie zunächst jeweils so lange gespeichert werden, bis ihrer je fünf beisammen sind. Als Fünfer-Potentialkonstellationen gelangen die Geheimzeichen über die fünf Leitungen **36**, die mit den entsprechenden fünf Leitungen **6** paarweise verbunden sind, an den Eingang des Umsetzers **7**. Dessen 32 Ausgänge stellen den Geber für die zu entschlüsselnden Geheimzeichen dar. Dem gewählten Beispiel entsprechend sei das empfangene Geheimzeichen das Fernschreibzeichen Nr. 7. Dann entsteht am Ausgang (7) des Umsetzers **7** Spannung, welche über die gestrichelt gezeichnete Sammelleitung **37** an alle Eingänge (7) aller Permutationsschalter **8 ... 9 ... 10** führt. Diese sind jetzt gegenüber der »Verschlüsselungs«-Stellung alle um 180° gedreht, d. h. auf »Entschlüsseln« gestellt. Dann liegt die gestrichelt gezeichnete Vertauschungsleitung (7) → (17) im Permutationsschalter **9** spiegelbildlich zu der beim Verschlüsseln verwendeten ausgezogenen Vertauchungsleitung (17) → (7) Permutationsschalters, so daß jetzt der Eingang (7) mit dem Ausgang (17) verbunden ist. Dieser Ausgang (17) ist über die gestrichelt gezeichnete Leitung **38** mit dem ersten Steuereingang des Und-Tores **24** verbunden, und die an der Leitung **38** liegende Spannung bereitet den Durchgang des Tores **24** vor.

Da auf der Empfangsseite der gleiche Schlüssellochstreifen wie auf der Sendeseite benutzt wird und auch die gleiche Lochkombination, nämlich Nr. 16, im Abtaster **15** gerade abgetastet wird, so entsteht an der Leitung **22**, die mit allen zweiten Steuereingängen der dem 16. Permutationsschalter **9** zugeordneten Und-Tore verbunden ist, Spannung. Für das Tor **24** ist damit die Durchlaßbedingung erfüllt, während sie für alle anderen Tore **23 ... 13 ... 25** nicht erfüllt ist. Über die gestrichelt gezeichnete Ausgangsleitung **39** des Tores **24** gelangt Spannung an den zugeordneten Eingang (17) des Umsetzers **27**, welcher die Entschlüsselungsausgabe darstellt, und in ihm wird das Klarzeichen Nr. 17 in die entsprechende Potentialkonstellation umgewandelt, die an den fünf Ausgangsleitungen **28** anliegt. Im Impulsgeber **29** wird die anliegende Potentialkonstellation in die im Fernschreibtakt zeitlich aufeinanderfolgenden Impulse der entsprechenden Impulskombination aufgelöst, und die Impulse gelangen über die Leitung **40**, im geöffneten Tor **41** und über die Leitung **2** zur Fernschreibmaschine **1**, durch die das Klarzeichen Nr. 17 geschrieben wird, wenn dieses ein Schriftzeichen und kein Funktionszeichen wie z. B. »*Bu*«, »*Zi*«, »*WR*«, »*Zl*« bedeutet.

Anstelle der mechanischen Permutationsschalter **8 ... 9 ... 10** kann auch eine quadratische Ringkernspeichermatrix mit $m = 32$ Ringkernspalten zu je $n = 32$ Ringkernen verwendet werden. Jedoch ist in diesem Falle die Entschlüsselung nicht so einfach wie bei den mechanischen Permutationsschaltern. Es müssen nämlich zu diesem Zweck die Fernschreibzeichen der Reihe nach versuchsweise so lange verschlüsselt werden, bis ein auf diese Weise erhaltenes Geheimzeichen mit dem zu entschlüsselnden Geheimzeichen übereinstimmt. Das in diesem Augenblick gerade verschlüsselte Fernschreibzeichen ist dann das gesuchte Klarzeichen.

Zur störungsfreien Arbeitsweise der Anlage sind noch einige selbsttätig wirkende Synchronisier- und Sperrmaßnahmen erforderlich. So ist zunächst der Steuerausgang des Umsetzers **7** über die Leitung **16**, das Differenzierglied **17** und die Leitung **18** mit dem Steuereingang des Schlüssellochstreifenabtasters **15** verbunden. Jedesmal, wenn der Umsetzer **7** in Tätigkeit tritt, sei es im Sendefalle durch ein von der Fernschreibmaschine **1** herrührendes Klarzeichen, sei es im Empfangsfalle durch ein von der Fernleitung **32** angeliefertes Geheimzeichen, wird durch ihn ein Synchronisierimpuls an den Lochstreifenabtaster **15** geliefert, wodurch dieser um einen Schritt weiterschaltet. Auf diese Weise wird auf der Sende- und Empfangsstelle ein gleicher Vorschub der beiden gleichen Schlüssellochstreifen erreicht, wodurch sichergestellt ist, daß zur Steuerung der Ver- und Entschlüsselung gleiche und einander entsprechende Lochkombinationen des Schlüssellochstreifens abgetastet werden.

Damit die zum fernen Chiffrierteilnehmer gesendeten Geheimzeichen nicht in die Empfangseinrichtungen der Sendeanlage zurückgelangen und dort Störungen hervorrufen, sind die Tore **34** und **41** vorgesehen, die in der Ruhestellung, d. h., wenn die Anlage nicht in Betrieb ist, geöffnet sind. Wenn beim Senden der Impulsspeicher **5** in Tätigkeit tritt, gibt er einen Sperrimpuls über die Leitung **42** auf die Tore **34** und **41**, die dadurch gesperrt werden und verhindern, daß Sendeimpulse über die Leitung **35** in die Empfangsrichtung und über die Leitung **40** an die Fernschreibmaschine **1** zurückgelangen.

Damit andererseits die zum fernen Chiffrierteilnehmer gesendeten Geheimzeichen nicht in die Sendeeinrichtungen der Empfangsanlage zurückgelangen und dort ihrerseits Störungen verursachen, sind die Tore **3** und **31** vorgesehen, die ebenfalls in der Ruhestellung geöffnet sind. Wenn beim Empfangen der Impulsspeicher **33** in Tätigkeit tritt, gibt er einen Sperrimpuls über die Leitung **43** auf die Tore **3** und **31**, die dadurch gesperrt werden und verhindern, daß Empfangsimpulse über die Leitung **4** in die Senderichtung und über die Leitung **30** auf die Fernleitung **32** zurückgelangen.

Der Vollständigkeit halber sei noch erwähnt, daß anstatt des beschriebenen »On-Line«-Betriebs, bei dem die Sende- und Empfangsanlagen völlig gleichartig aufgebaut und daher nicht voneinander zu unterscheiden sind, auch der »Off-Line«-Betrieb verwendet werden kann, der nicht die Symmetrie des »On-Line«-Betriebes aufweist. Der »Off-Line«-Betrieb wird vorzugsweise dann verwendet, wenn die eine Stelle nur zum Verschlüsseln und Senden und die andere Stelle nur zum Empfangen und Entschlüsseln benutzt wird. Es entfallen dann jeweils diejenigen Teile, die beim Sender zum Empfangen und beim Empfänger zum Senden vorgesehen sind. Die Erfindung bleibt jedoch von der Art des Fernübertragungsbetriebes unberührt.

Hierzu 1 Blatt Zeichnungen

Nummer: **9 78 065**
Int. Cl.²: **H 04 L 9/02**
Bekanntmachungstag: —