CH 671 663 A5

(19) SCHWEIZERISCHE EIDGENOSSENSCHAFT
BUNDESAMT FÜR GEISTIGES EIGENTUM

(11) CH 671 663 A5

(51) Int. Cl.⁴: H 04 L 9/02

Erfindungspatent für die Schweiz und Liechtenstein
Schweizerisch-liechtensteinischer Patentschutzvertrag vom 22. Dezember 1978

(12) PATENTSCHRIFT A5

(21) Gesuchsnummer: 3977/82

(22) Anmeldungsdatum: 29.06.1982

(24) Patent erteilt: 15.09.1989

(45) Patentschrift veröffentlicht: 15.09.1989

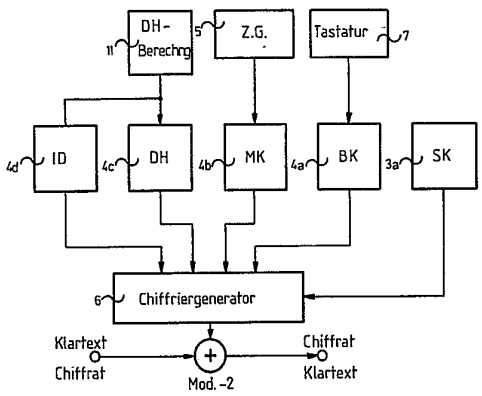
(73) Inhaber:
Gretag Aktiengesellschaft, Regensdorf

(72) Erfinder:
Mueller, Kurt Hugo, Dr., Wallisellen

(74) Vertreter:
CIBA-GEIGY AG, Basel

(54) Verfahren zur chiffrierten Uebermittlung von Nachrichten.

(57) Bei den bekannten Chiffriersystemen auf Basis von Einwegfunktions-Schlüsseln besteht keine Möglichkeit der Identifikation bzw. Authentizierung von Partnerstationen. Zur Behebung dieses Mangels wird nun bei der erstmaligen Verbindungsaufnahme zwischen zwei Stationen ein Kennungsschlüssel (ID) vereinbart und beidseitig gespeichert. Dieser Kennungsschlüssel (ID) wird nun in der Folge stets als zusätzlicher Chiffrierschlüssel für die Chiffrierung/Dechiffrierung mitverwendet. Der Kennungsschlüssel (ID) wird vorzugsweise vollautomatisch und zufallsmässig erzeugt und kryptologisch gesichert übertragen. Als zweckmässiger Sonderfall wird ein erster Einwegsfunktions-Schlüssel (DH) selbst als Kennungsschlüssel (ID) verwendet.



PATENTANSPRÜCHE

1. Verfahren zur chiffrierten Übermittlung von Nachrichten, dadurch gekennzeichnet, dass vor bzw. bei der erstmaligen Verbindungsaufnahme zwischen zwei Stationen wenigstens ein identischer Kennungsschlüssel vereinbart und beidseitig permanent gespeichert wird, und dass zumindest während eines bestimmten Zeitraums alle Nachrichten unter Mitverwendung dieses Kennungsschlüssels als Chiffrierschlüssel chiffriert bzw. dechiffriert werden.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass der Kennungsschlüssel in einer der Stationen zufallsmässig erzeugt und in kryptologisch gesicherter Form zur anderen Station übertragen wird.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass als Chiffrierschlüssel neben dem Kennungsschlüssel ein Einwegfunktions-Schlüssel verwendet wird.

4. Verfahren nach Anspruch 3, dadurch gekennzeichnet, dass als Kennungsschlüssel ebenfalls ein Einwegfunktions-Schlüssel verwendet wird.

5. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass der Kennungsschlüssel eine Funktion von zwei in je einer Station erzeugten und zur jeweils anderen Station in kryptologisch gesicherter Form übertragenen Zufallsgrössen ist.

6. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass bei Mehrpunkt-Kommunikationsnetzen für jede einzelne Zweipunktverbindung zumindest in einer Übertragungsrichtung ein eigener Kennungsschlüssel verwendet wird.

7. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass die beiden Stationen vor der Verbringung an ihre jeweiligen Einsatzorte aufeinander abgestimmt werden, indem sie per Kabel zusammengekoppelt werden und dabei der Kennungsschlüssel automatisch erzeugt und beidseits abgespeichert wird.

8. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass für jede Übertragungsrichtung ein eigener Kennungsschlüssel verwendet wird.

9. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass die Erzeugung zur Abspeicherung eines Kennungsschlüssels nur dann erfolgt, wenn beide beteiligten Stationen dies wünschen.

10. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass neben dem Kennungsschlüssel noch wenigstens zwei weitere Schlüssel als Chiffrierschlüssel verwendet werden.

BESCHREIBUNG

Die Erfindung betrifft ein Verfahren zur chiffrierten Übermittlung von Nachrichten gemäss dem Oberbegriff des Patentanspruches 1.

Einwegfunktionen, wie sie in den letzten Jahren für kryptologische Anwendungen propagiert wurden (siehe z.B. W. Diffie, M.E. Hellmann, «New Directions in Cryptography», IEEE Transactions on Information Theory, Vol. IT-22, Nov. 1976, pp. 644-654 oder US-PS 4 200 770 oder M.E. Hellmann, «An Overview of Public Key Cryptography», IEEE Communications Society Magazine, Nov. 1978, Vol. 16. No. 6, pp. 24-32), zeigen vor allem im Hinblick auf das Schlüsselmanagement neue Aspekte. Bei der klassischen Kryptographie kann zwar mit heutigen Methoden die Dechiffrierfestigkeit höchsten Ansprüchen genügen; dagegen sind aber potentielle Schwachstellen vorhanden im Bereich der Schlüsselerzeugung, -verteilung, -speicherung, -ladung, -vernichtung etc. Gerade hier eröffnen sich mittels mathematischer Einwegfunktionen gewisse Vorteile. Allerdings bringen die bekannten Verfahren inhärent auch gewisse Sicherheitsrisiken und Nachteile mit sich, welche die praktische Anwendung dann eben leider doch wieder etwas bedenklich erscheinen lassen. Der wohl augenscheinlichste Nachteil ist die fehlende Identifikation bzw. Authentizierung der Partnerstationen. Diesen Mangel bzw. Risikofaktor zu beseitigen bzw. weitestgehend zur reduzieren, ist Hauptaufgabe der vorliegenden Erfindung. Eine weitere Aufgabe besteht darin, unter Vermeidung des genannten Mangels ein möglichst vielseitiges, flexibles Chiffrier/Dechiffriersystem zu schaffen.

Das diesen Ansprüchen gerecht werdende erfindungsgemässe Verfahren ist im unabhängigen Patentanspruch beschrieben. Bevorzugte Ausführungsvarianten ergeben sich aus den abhängigen Ansprüchen.

Im folgenden wird die Erfindung anhand von Ausführungsbeispielen in Verbindung mit der Zeichnung näher erläutert. Es zeigen:

Fig. 1 ein Prinzip-Blockschaltbild einer Station einer zur Durchführung des erfindungsgemässen Verfahrens geeigneten Vorrichtung,

Fig. 2 ein Blockschema zur Erläuterung des engeren Chiffrier/Dechiffrierteils der Vorrichtung aus Fig. 1,

Fig. 3 eine bevorzugte Ausführungsform bzw. Variante der Einrichtung gemäss Fig. 2,

Fig. 4 ein Schema des Rechenablaufs bei Erzeugung und Austausch von Einwegfunktions-Chiffrierschlüsseln,

Fig. 5-7 Schemata zur Erläuterung verschiedener Varianten von Erzeugung und Austausch von Kennungsschlüsseln und

Fig. 8 und 9 Schemata zur Erläuterung der Einwirkung der Schlüssel auf einen Chiffriergenerator.

In Fig. 1 ist der grundsätzliche Aufbau einer Station einer Nachrichtenübermittlungsvorrichtung gezeigt, wobei die die eigentliche Übertragung der Nachrichten betreffenden Teile, also Sender, Empfänger etc. weggelassen und nur die unmittelbar mit der Chiffrierung bzw. Dechiffrierung bzw. mit den Schlüsseln zusammenhängenden Teile dargestellt sind.

Die Station ist, wie die meisten moderneren Geräte dieser Art, mittels eines Rechners implementiert und besteht dementsprechend aus einer Zentraleinheit 1, die über ein Busleitungssystem 2 mit einem Programmspeicher 3, einem Arbeitsspeicher 4, einem Zufallsgenerator 5 und einem Chiffriergenerator 6 sowie mit einer Tastatur 7, diversen Anzeigen 8, diversen Ein- und Ausgängen 9 und einem zum Übertragungskanal führenden Kanalein/ausgang 10 verbunden ist.

Die allgemeine Funktionsweise der Station ist gleich wie bei bekannten Stationen dieser Art und im wesentlichen etwa wie folgt:

In der Betriebsweise «Chiffrieren» wird der zu chiffrierende Klartext via Tastatur 7 oder via Eingang 9 eingegeben und mit einer vom Chiffriergenerator 6 erzeugten Chiffrierimpulssequenz modulo-2-gemischt. Das dabei entstehende Chiffrat geht dann in der Regel über den Kanalausgang 10 und den Übertragungskanal zur Partnerstation oder wird über die Anzeige 8 oder den Ausgang 9 ausgegeben. In der Betriebsart «Dechiffrieren» gelangt das Chiffrat in der Regel via den Kanaleingang 10 in die Station, es kann aber auch manuell oder über den Eingang 9 eingegeben werden. Es wird dann analog dem Chiffriervorgang wieder mit einer vom Chiffriergenerator 6 erzeugten Sequenz modulo-2-gemischt, und das den Klartext ergebende Mischprodukt wird dann gespeichert und/oder über den Ausgang 9 oder auch die Anzeige 8 ausgegeben. Der Chiffriergenerator 6 wird natürlich vor jeder Chiffrierung bzw. Dechiffrierung mit Hilfe eines oder mehrerer Chiffrierschlüssel in einen definierten Zustand gebracht. Die Art, Erzeugung, Auswahl und sonstige Handhabung der Chiffrierschlüssel wird weiter unten noch erläutert.

Wie schon erwähnt, entspricht die dargestellte Station bzw. Chiffrier/Dechiffriervorrichtung im grundsätzlichen Aufbau bis auf die noch zu erläuternden Unterschiede im Zusammenhang

mit den Chiffrierschlüsseln dem bekannten Stand der Technik, wie er beispielsweise in Kapitel 8 des Buchs «Fehlerkorrigierende Blockcodierung für die Datenübertragung» von F.J. Furrer beschrieben oder durch das Gerät Gretacoder 601 der Firma Gretag AG, Regensdorf, Schweiz, gegeben ist. Eine eingehendere Beschreibung des apparativen Teils der Station erübrigt sich daher.

In Fig. 2 ist das der Erfindung zugrundeliegende Arbeitsprinzip der Chiffrier/Dechiffriereinrichtung in seiner allgemeinsten Form schematisch dargestellt. Wie man sieht, arbeitet der Chiffriergenerator 6 mit fünf verschiedenen Chiffrierschlüsseln, und zwar einem im allgemeinen festen Strukturschlüssel SK, einem geheimen sog. Grundschlüssel BK, einem weiteren geheimen, sog. Einwegfunktions-Schlüssel DH und einem geheimen Kennungsschlüssel ID sowie einem in der Regel nicht geheimen Zusatzschlüssel MK, dessen Aufgabe es ist, entweder direkt Initialisierung und Ablauf des Chiffriergenerators zu beeinflussen oder aber mindestens einen der anderen Schlüssel — hier den Grundschlüssel — zu modifizieren. Der Strukturschlüssel SK ist in einem programmierten Festwertspeicher (PROM) 3a gespeichert, die übrigen Chiffrierschlüssel in Bereichen 4a-4d des Arbeitsspeichers 4. Der Grundschlüssel BK wird über die Tastatur 7 eingegeben, der Zusatzschlüssel MK wird normalerweise vom Zufallsgenerator 5 erzeugt. Der Einwegfunktions-Schlüssel DH wird nach einem weiter unten noch erläuterten Schema, das hier stellvertretend durch den Block 11 angedeutet ist, berechnet, ebenso der Kennungsschlüssel ID.

Strukturschlüssel SK, Grundschlüssel BK und Zusatzschlüssel MK sind die traditionellen Chiffrierschlüssel, die in zahlreichen Publikationen beschrieben und in vielen Chiffriergeräten praktisch angewendet werden und somit hier keiner näheren Erläuterung bedürfen. Der Einwegfunktions-Schlüssel DH ist ein nach den in den eingangs angeführten Publikationen beschriebenen Methoden erzeugter, zufälliger und geheimer Chiffrierschlüssel. Die Rolle des Kennungsschlüssels wird noch erläutert.

Alle fünf Schlüssel bilden in ihrer Gesamtheit eine Schlüsselinformation, die den Chiffriergenerator 6 eindeutig determiniert. Beim Ausführungsbeispiel nach Fig. 2 sind diese fünf Schlüssel unabhängig voneinander. In der Praxis wird man jedoch eher die Variante nach Fig. 3 wählen, bei der der Grundschlüssel BK, der Einwegfunktions-Schlüssel DH und der Kennungsschlüssel ID mittels eines Modulo-2-Mischers 12 miteinander verknüpft sind. Das Verknüpfungsprodukt kann dann als Geheim- oder Grundschlüssel der traditionellen Methoden angesehen werden, welcher dem Chiffriergenerator zusammen mit dem üblichen Strukturschlüssel SK und dem Zusatzschlüssel MK zugeführt wird. Die Variante nach Fig. 3 erlaubt es, als Geheimelement entweder nur mit dem traditionellen Grundschlüssel BK oder an dessen Stelle mit einem Einwegfunktions-Schlüssel DH oder aber auch mit diesen beiden Geheimschlüsseln zugleich zu arbeiten.

In Fig. 4 sind die Rechenabläufe bei der Erzeugung und beim Austausch eines Einwegfunktions-Schlüssels zwischen zwei Stationen am Beispiel des Diffie-Hellmann-Verfahrens (vgl. einleitende Literaturangaben) schematisch zusammengestellt. In beiden Partnerstationen sind zwei Zahlen Q und N gespeichert, die gewissen in der Literatur beschriebenen Einschränkungen genügen. Wenn nun ein Schlüssel erzeugt und ausgetauscht werden soll, bestimmt die aufrufende Station mittels Zufallsgenerator ZG eine Zufallszahl X, berechnet daraus die Zahl $U = Q^X \bmod N$ und überträgt dieses Resultat — fehlergesichert — zur Partnerstation. Analog bestimmt nun diese eine Zufallszahl Y, berechnet daraus die Zahl $V = Q^Y \bmod N$ und überträgt das Resultat zur ersten Station. Aus den übertragenen Zahlen U und V wird nun ein gemeinsamer Einwegfunktions-Schlüssel H gemäss $H = V^X \bmod N$ bzw. $H = U^Y \bmod N$ errechnet. Aus den übertragenen Informationen U und V lassen sich die Zufallszahlen X bzw. Y und damit H aufgrund des Einwegfunktionscharakters des Bildungsgesetzes für U und V nicht bestimmen.

Die Hauptvorteile eines so gebildeten Einwegfunktions-Schlüssel sind, dass das herkömmliche Schlüsselmanagement entfällt, dass ein häufigerer Schlüsselwechsel möglich ist, dass die Stationen keine Geheimelemente enthalten, und dass die Operateure die Schlüssel überhaupt nicht kennen und dadurch nicht erpressbar sind. Ein oftmals schwerwiegender Nachteil besteht darin, dass, wie schon erwähnt, die Stationen aufgrund fehlender Geheimelemente nicht ohne weiteres identifizierbar bzw. authentisierbar sind.

Dieser Nachteil wird nun gemäss dem Grundgedanken der Erfindung durch die Verwendung eines weiteren Chiffrierschlüssels, nämlich des Kennungsschlüssels ID behoben. Dieser Schlüssel wird vor bzw. bei der allerersten Verbindungsaufnahme zwischen zwei Stationen gegenseitig vereinbart und dann im Gerät abgespeichert, und zwar in einer nicht flüchtigen Art und Weise. Dieser Kennungsschlüssel ID bleibt dann für den gesamten Einsatz oder eventuell auch nur für eine gewisse längere Zeitspanne unverändert und wird als Chiffrierschlüssel mitverwendet, d.h., er bestimmt jeweils den Startzustand und Ablauf des Chiffriergenerators zusammen mit dem oder den anderen Chiffrierschlüsseln, die sich natürlich ständig ändern, mit.

Nach der ersten Verbindungsaufnahme von zwei Stationen sind diese somit aufeinander abgestimmt und die Identifizierung ist fortan gewährleistet. Nach diesem Zeitpunkt ist eine Verbindungsaufnahme durch Fremdstationen nicht mehr möglich (Freund-Feind-Erkennung) bzw. jeder solcher Versuch würde sofort bemerkt werden. Jeder Gerätewechsel, z.B. der Ersatz eines vernichteten Partners durch eine Feindstation oder Feindeinschaltung während einer Dislokation etc., ist sofort feststellbar.

Ein weiterer Vorteil besteht darin, dass die Abstimmung der Partner-Stationen vor ihrer Verbringung an den Einsatzort geschehen kann. Dazu können die beiden Stationen z.B. mittels eines kurzen Kabels verbunden werden und auf diese Weise eine Abspeicherung des (automatisch und zufällig erzeugten) Kennungsschlüssels auf beiden Seiten erfolgen.

Der Kennungsschlüssel ID selbst ist an sich beliebig. Er kann im Prinzip auf jede beliebige Weise zwischen den Partnerstationen vereinbart und dann abgespeichert werden. Auch ist es nicht nur zum Einsatz in Systemen mit Einwegfunktions-Schlüsseln geeignet, sondern selbstverständlich auch als (zusätzliche) Sicherung bei traditionellen Chiffriersystemen vorteilhaft.

Die Erzeugung und der Austausch der Kennungsschlüssel erfolgen gemäss einer vorteilhaften Ausgestaltung der Erfindung vollautomatisch, zufällig und in kryptologisch gesicherter Weise, so dass die Kennungsschlüssel für den Operateur (und einen allfälligen Abhorcher) unbekannt bleiben.

Die Fig. 5a und 5b zeigen beispielsweise, wie bei einer Punkt-Punkt-Verbindung ein gemeinsamer Kennungsschlüssel ID erzeugt und gespeichert werden kann. In der aufrufenden Station (in der Zeichnung links) wird via Zufallsgenerator ZG ein zufälliger Kennungsschlüssel ID erzeugt und abgespeichert. Dieser Schlüssel wird dann chiffriert, in chiffrierter Form T zur Partnerstation übertragen und dort dechiffriert und gespeichert. Für diesen (ersten) Chiffrier- bzw. Dechiffriervorgang werden die Chiffriergeneratoren lediglich mit dem oder den anderen Schlüsseln determiniert, der Kennungsschlüssel selbst wird erst bei der Verarbeitung der eigentlichen Nachrichten mitverwendet. Vorzugsweise wird als Chiffrierschlüssel für die Chiffrierung des Kennungsschlüssels ein Einwegfunktions-Schlüssel verwendet, was in den Fig. 5a und 5b durch den Buchstaben H (analog Fig. 4) angedeutet ist.

Als Alternative zu Fig. 5a kann die vom Zufallsgenerator ZG erzeugte Information von vornherein als chiffrierter Kennungsschlüssel aufgefasst werden. In diesem in Fig. 5b gezeigten Fall wird die Information T dann klar übertragen, aber auf

beiden Seiten dechiffriert und dann als Kennungsschlüssel ID gespeichert.

Die Fig. 6a und 6b zeigen zwei zu Fig. 5a und 5b analoge Varianten des Verfahrensablaufs, wenn bei einer Punkt-Punkt-Verbindung für jede Verbindungsrichtung ein eigener Kennungsschlüssel ID 1 bzw. ID 2 verwendet wird. Hierbei bestimmt jede Station mittels Zufallsgenerator ZG ihren eigenen Kennungsschlüssel ID 1, ID 2 und überträgt ihn in chiffrierter Form T1, T2 fehlergesichert zur jeweils anderen Station, wo er dechiffriert und neben dem eigenen gespeichert wird. Selbstverständlich ist es dabei völlig egal, für welche Richtung dann schlussendlich welcher Kennungsschlüssel verwendet wird, solange dies durch ein entsprechendes Protokoll geregelt ist.

Im übrigen ist es natürlich auch möglich, die beiden gemäss Fig. 6a oder 6b erzeugten Kennungsschlüssel ID 1 und ID 2 in beiden Stationen irgendwie, z.B. durch Modulo-2-Addition zu verknüpfen und daraus einen neuen, für beide Stationen gemeinsamen Kennungsschlüssel zu erzeugen.

Wenn mit einem Chiffriersystem auf Einwegfunktions-Basis, also unter (Mit-)Verwendung eines Einwegfunktions-Schlüssels gearbeitet wird, sind für den in Fig. 6a bzw. 6b gezeigten Verfahrensablauf vier fehlergesicherte Übertragungen nötig: zunächst U und V zwecks Berechnung von H, danach T1 und T2 für die Festlegung von ID 1 und ID 2. Man kann die Anzahl der Übertragungen auf die Hälfte reduzieren, wenn man T1 = U und T2 = V setzt. Verfährt man gemäss Fig. 6b, so entsprechen dann den vom Zufallsgenerator erzeugten und übertragenen Grössen T1 und T2 eben neu die Grössenn U und V gemäss Fig. 4.

U und V sind zwar nicht direkt vom Zufallsgenerator abgeleitete Grössen, wohl aber die ihrer Berechnung zugrundegelegten X und Y. Bei der verwendeten Art der Abbildung wird aber die Zufälligkeit nicht beeinflusst.

Dadurch, dass die Grössen U und V sowohl für die Bestimmung von H als auch für die Bestimmung von ID verwendet werden, tritt keine Beeinträchtigung der kryptologischen Sicherheit auf. Da ID 1 und ID 2 durch Dechiffrieroperationen mittels des ersten H erzeugt werden, ist die Sicherheit dieses ersten H (zumindest in Abwesenheit weiterer Geheimelemente) relevant für die Sicherheit von ID.

Im Falle von Streamcipher-Chiffrierung darf für die Übertragung von ID 1 und ID 2 niemals dieselbe Generatorsequenz verwendet werden, sonst wäre der Kennungsschlüssel dem abhorchenden Gegner sofort zugänglich. Diese könnte etwa durch zeitlich gestaffelte Benützung derselben Generatorsequenz vermieden werden, oder aber durch den Austausch von Zusatzschlüsseln (Modifiers), welche eine an beiden Stationen verschiedene Generatorsequenz erzwingen.

Um die Zahl der nötigen Übertragungen wirklich auf zwei zu beschränken, können die bei Streamcipher-Chiffrierung nötigen Zusatzschlüssel MK gemäss Fig. 7 definiert werden. Hier hat jede Dechiffrierbox DCH seitlich zwei Schlüsseleingänge für den Schlüssel H und den Zusatzschlüssel MK (Modifier), wobei T1 als Modifier bei der Dechiffrierung von T2 verwendet wird und umgekehrt. Praktisch werden die beiden Operationen natürlich zeitlich gestaffelt an einer einzigen Chiffriereinheit durchgeführt.

Wenn schliesslich als Kennungsschlüssel ID direkt der allererste Einwegfunktions-Schlüssel DH oder eine araus abgeleitete Grösse verwendet wird, fällt der Rechen- und Übertragungsaufwand für die Festlegung der Kennungsschlüssel praktisch komplett weg.

Würde beim System nach Fig. 3 der Einwegfunktions-Schlüssel DH (oder eventuell auch der Grundschlüssel BK) direkt als Kennungsschlüssel verwendet werden, so ergäben sich aufgrund der Modulo-2-Verknüpfung bei der ersten Betriebsaufnahme, wo die Schlüssel noch identisch sind, eine Auslöschung. Daher wird der Einwegfunktions-Schlüssel DH durch eine durch den Block 13 angedeutete Operation, z.B. eine Spiegelung um die Wortmitte o.ä., modifiziert und dann in dieser modifizierten Form als Kennungsschlüssel ID gespeichert bzw. verwendet. Der Schalter 14 soll andeuten, dass eine Verbindung zum Speicher 4d nur bei der erstmaligen Verbindungsaufnahme, also während des Abstimmungsprozesses besteht und später (in der Regel) keine Veränderung des Speicherinhalts mehr erfolgt.

Bei der in Fig. 3 gezeigten Variante der Chiffrier/Dechiffriervorrichtung wird der Chiffriergenerator durch drei Schlüsselgrössen determiniert, nämlich den Strukturschlüssel SK, den kombinierten Schlüssel aus ID, DH und BK und den Zusatz- oder Modifizierschlüssel MK. Dieses System nützt zwar nicht alle Freiheitsgrade aus, ist aber äusserst zweckmässig, um bestehende Chiffriereinheiten bis zu definierten Schnittstellen unverändert beizubehalten bei Erweiterungen zum 5-Schlüssel-System. Die Vorrichtung gemäss Fig. 3 kann mit geeigneter Intelligenz ausgestattet sein, welche z.B. ermöglicht, dass die Schlüssel selbst ausgewählt werden: Ist z.B. der Speicher 4a für den Grundschlüssel BK belegt, d.h. ein Schlüssel abgespeichert, so braucht kein DH-Schlüssel ausgetauscht zu werden. Sind bei einem geplanten Schlüsselwechsel die Speicher 4a und 4c für Grund- und Einwegfunktions-Schlüssel BK bzw. DH leer, so wird automatisch ein DH-Schlüssel ausgetauscht und abgespeichert. Der Kennungsschlüssel ID bleibt natürlich immer der gleiche. Selbstverständlich gibt es noch eine Reihe von weiteren Massnahmen, Bedienungserleichterungen und Automatismen, die je nach Anwendungsfall eingebaut werden können.

Bei Einsatz einer erfindungsgemässen Übermittlungsstation in einem Mehrpunktnetz kann die Handhabung des Kennungsschlüssels vielfältig organisiert sein. So ist es z.B. möglich, für alle Verbindungen innerhalb des Netzes denselben Kennungsschlüssel oder auch für jede einzelne Verbindung einen eigenen Kennungsschlüssel zu benutzen, wobei wiederum für die beiden Verbindungsrichtungen jeweils sowohl derselbe als auch unterschiedliche Kennungsschlüssel eingesetzt werden können.

Ein weiterer wesentlicher Punkt ist, dass der Austausch von Kennungsschlüsseln zwischen zwei Stationen, also deren gegenseitige Abstimmung, nicht akzidentiell oder ohne Zustimmung beider Partner erfolgen kann. Im wesentlichen genügt dazu, dass diejenigen Bedienungsorgane, mit welchen ein Kennungsschlüsselaustausch ausgelöst wird, einerseits mechanisch und andererseits mittels eines geeigneten Quittierungssystems geschützt sind. Derartige Schutzsysteme sind an sich bekannt und benötigen daher hier keine nähere Erläuterung.

Das in den Fig. 2 und 3 dargestellte Konzept arbeitet im Maximum mit fünf Schlüsseln und besitzt eine beträchtliche Flexibilität. Die einzelnen Schlüssel haben dabei unterschiedliche Aufgaben.

Für eine Neu-Initialisierung kann DH oder MK verwendet werden, da eine Erneuerung in jedem Fall sicherstellt, dass früherer Schlüsseltext bei Streamciphergeneratoren nicht wiederholt wird. Bei Verwendung des Modifiers MK entfällt natürlich der bei DH benötigte Rechenaufwand; der Übertragungsoverhead ist im allgemeinen kleiner (besonders bei marginalen Kanälen) und das Verfahren ist auch beim Simplex-Betrieb anwendbar. Die Erneuerung von DH dagegen bringt den Vorteil, dass mit der Löschung des früheren DH automatisch die früheren Übertragungen gegen Schlüsselkaperung geschützt sind. Welchem Verfahren man den Vorzug gibt, ist sicher vom Anwendungsprofil abhängig.

Bei den Schlüsseln BK und SK braucht etwa SK nicht unbedingt permanent gespeichert zu sein. Vielmehr lässt sich aus dem früheren Schlüssel und einem Modifier MK bei Bedarf ein neuer Schlüssel errechnen, der dann nach Löschung des früheren dessen Stelle einnimmt.

Beim 5-Schlüssel-Prinzip muss der Art der Einwirkung der einzelnen Schlüssel auf die Freiheitsgrade des Chiffriersystems

besondere Aufmerksamkeit geschenkt werden. Die Zahl dieser Freiheitsgrade, in Anzahl Bit gemessen — reicht von 56 beim normierten Digital Encryption Standard (DES) bis zu über 10 000 bei gewissen Streamciphergeneratoren. Es ist grundsätzlich vorzuziehen, wenn die zur Verfügung stehenden Freiheitsgrade durch die zur Verfügung stehenden Schlüssel möglichst optimal genutzt werden. Die beiden Extremfälle einfachster Verknüpfung und vollständiger «Nutzung» aller Schlüssel durch den Chiffriergenerator sind in den Fig. 8 und 9 dargestellt.

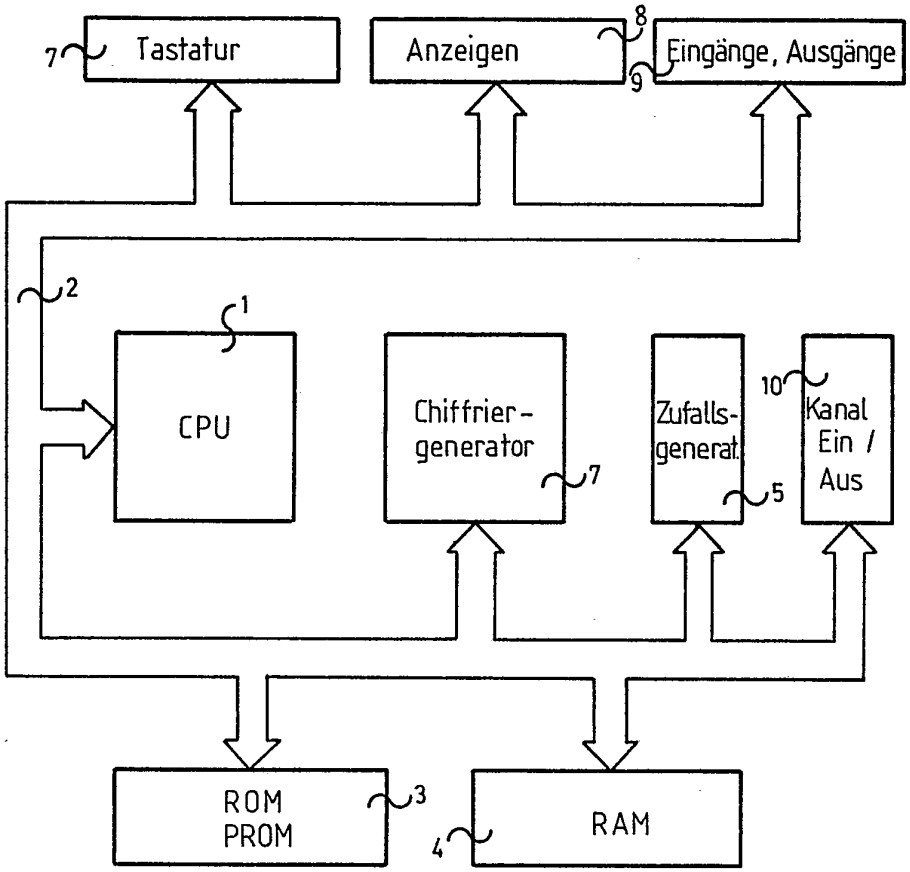

7
Tastatur
Anzeigen
8
9
Eingänge, Ausgänge
2
1
CPU
Chiffrier-
generator
7
Zufalls-
generat.
5
10
Kanal
Ein /
Aus
ROM
PROM
3
4
RAM

Fig. 1

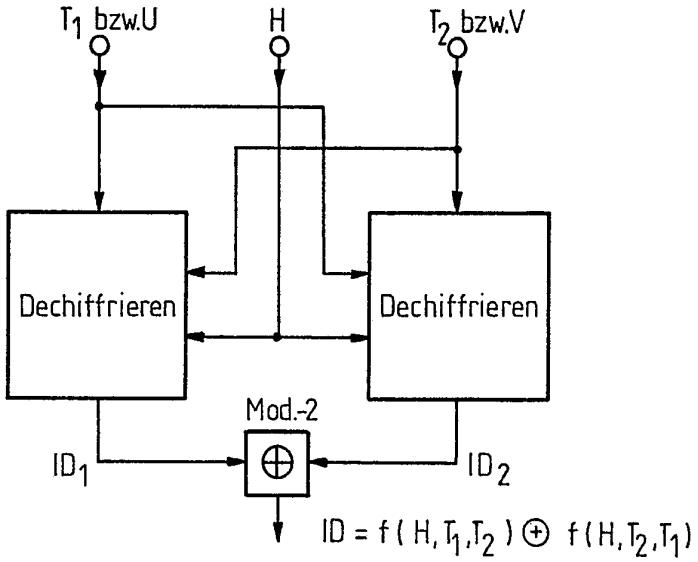

T1 bzw.U
H
T2 bzw.V
Dechiffrieren
Dechiffrieren
Mod.-2
ID1
ID2
ID = f (H, T1, T2) ⊕ f (H, T2, T1)

Fig. 7

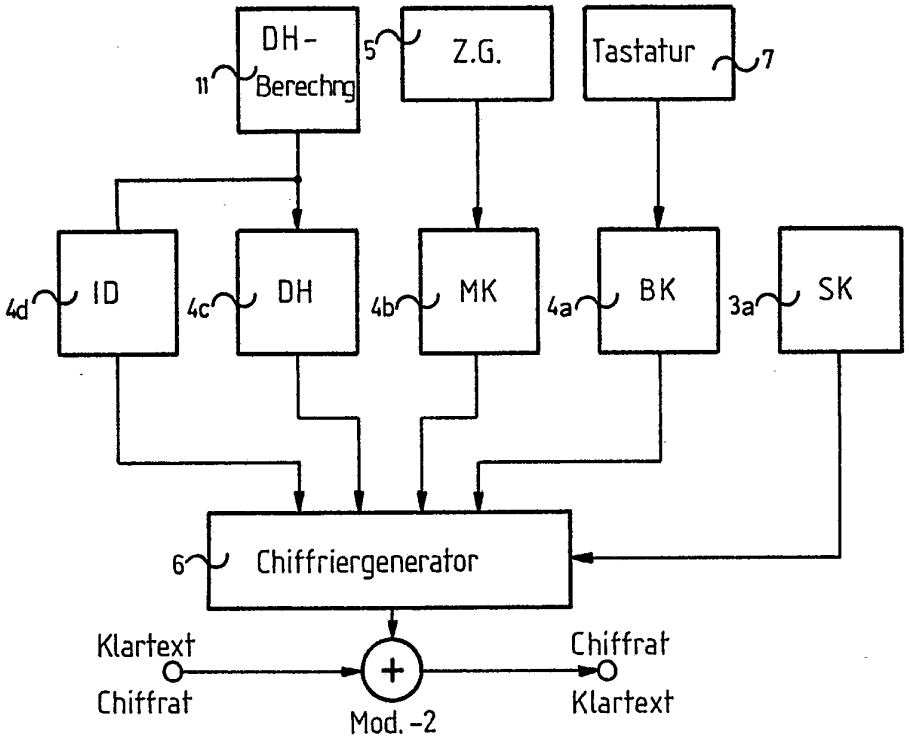

DH-
Berechng
11
5
Z.G.
Tastatur
7
ID
4d
DH
4c
MK
4b
BK
4a
SK
3a
6
Chiffriergenerator
Klartext
Chiffrat
Chiffrat
Klartext
Mod. -2

Fig. 2

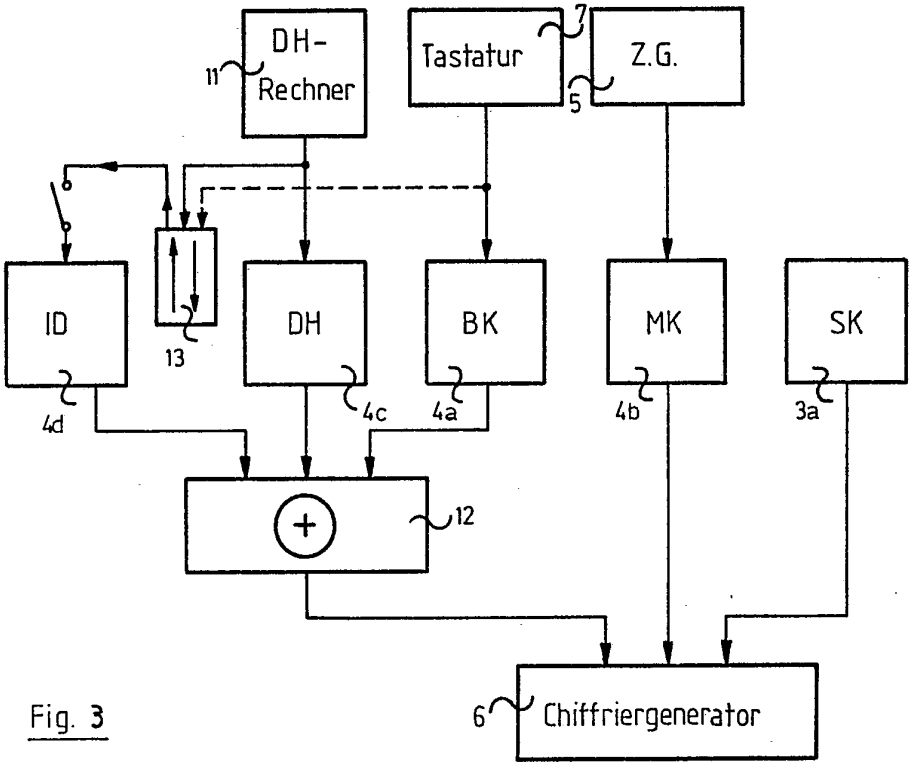

DH-
Rechner
11
Tastatur
7
Z.G.
5
ID
4d
13
DH
4c
BK
4a
MK
4b
SK
3a
12
6
Chiffriergenerator

Fig. 3

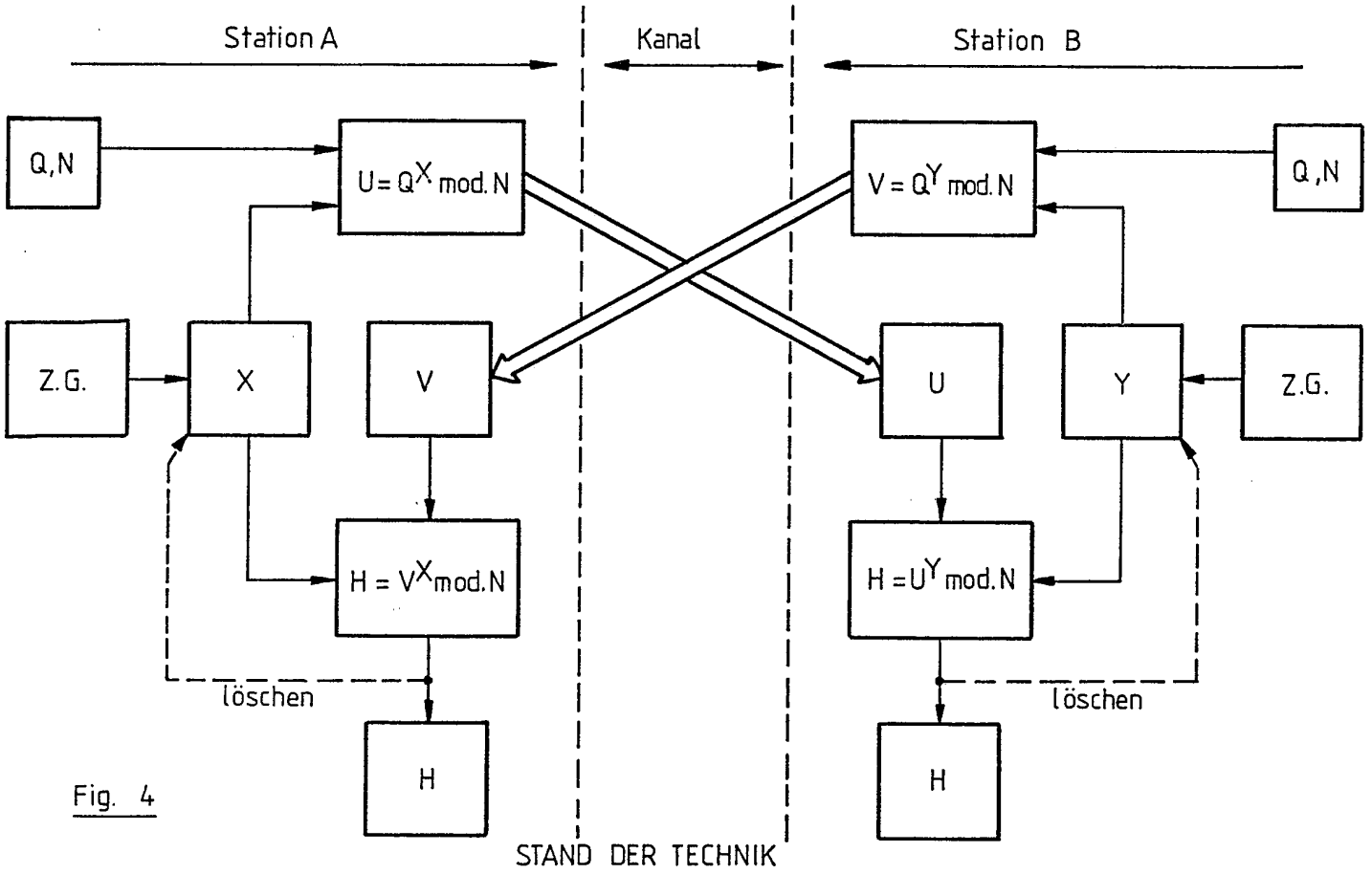

Station A
Kanal
Station B
Q,N
U = Q^X mod. N
V = Q^Y mod. N
Q,N
Z.G.
X
V
U
Y
Z.G.
H = V^X mod. N
H = U^Y mod. N
löschen
löschen
H
H
STAND DER TECHNIK

Fig. 4

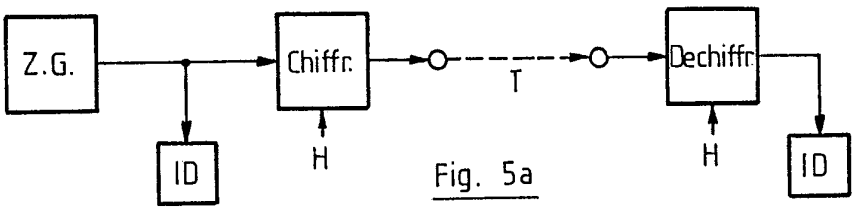


Fig. 5a

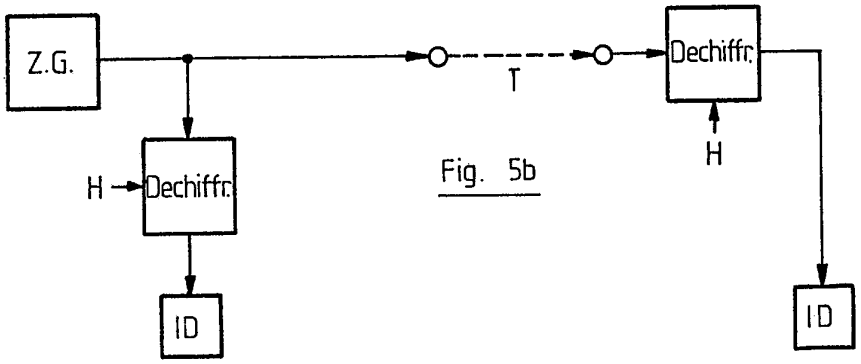


Fig. 5b

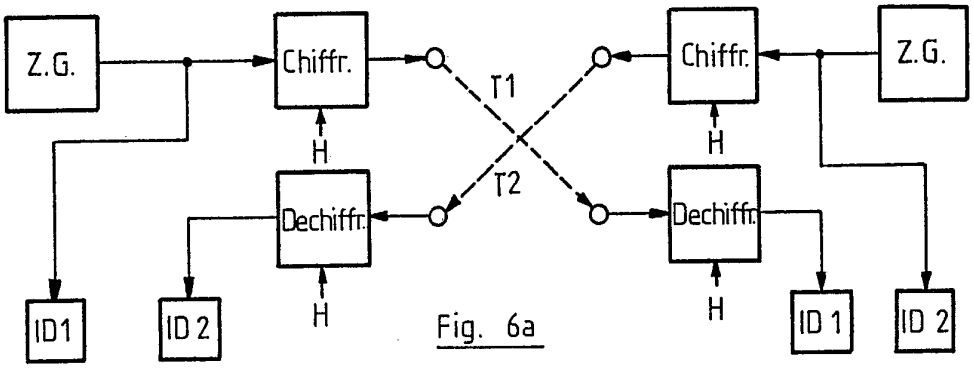


Fig. 6a

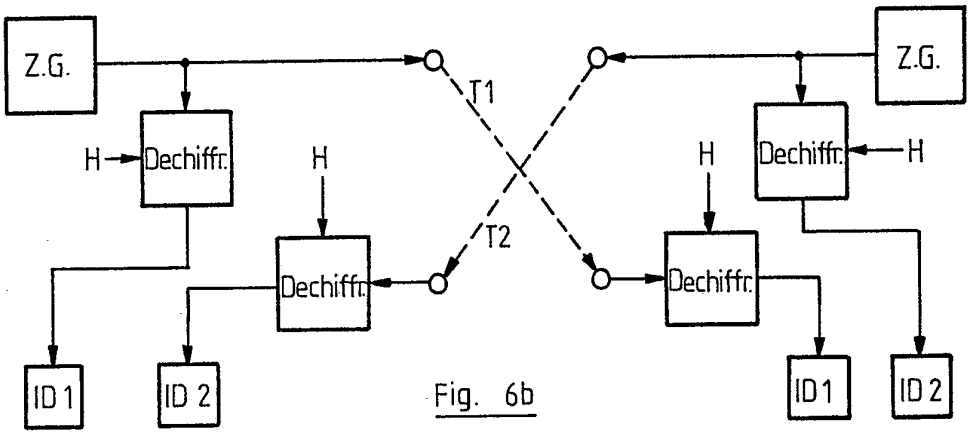


Fig. 6b

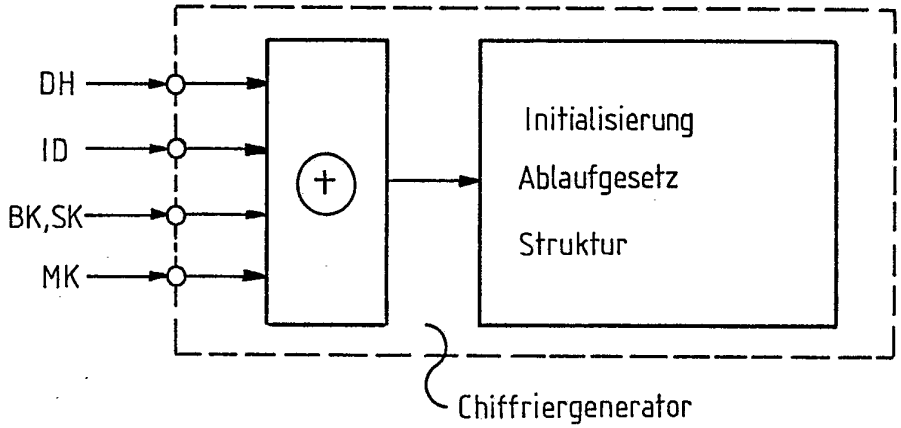

DH
ID
BK,SK
MK
+
Initialisierung
Ablaufgesetz
Struktur
Chiffriergenerator

Fig. 8

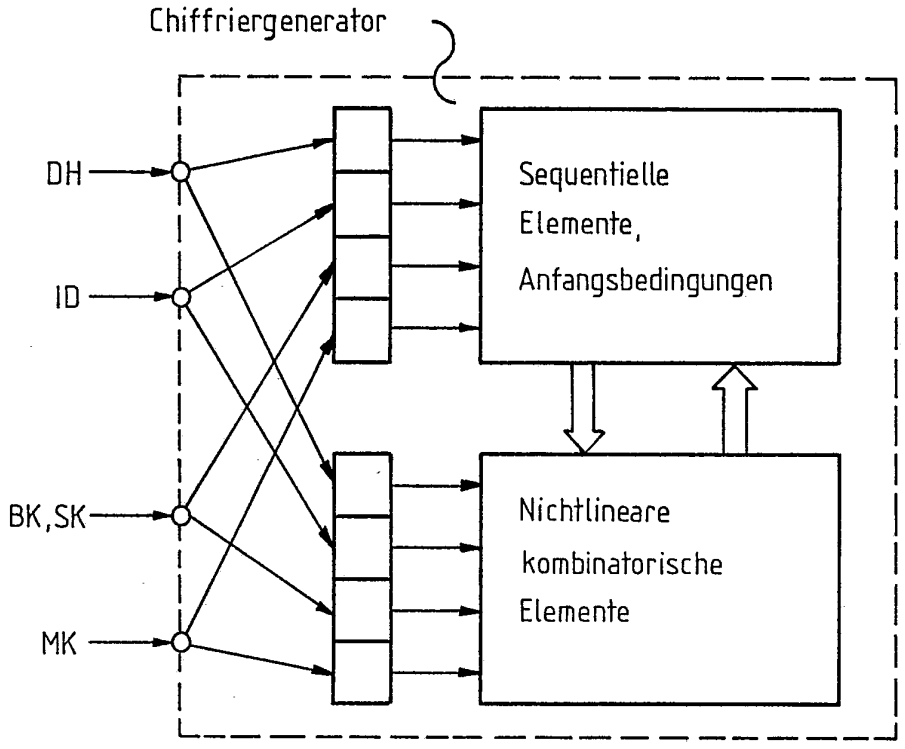

Chiffriergenerator
DH
ID
BK,SK
MK
Sequentielle
Elemente,
Anfangsbedingungen
Nichtlineare
kombinatorische
Elemente

Fig. 9