CH 664 056 A5

(19) SCHWEIZERISCHE EIDGENOSSENSCHAFT
BUNDESAMT FÜR GEISTIGES EIGENTUM

(11) CH 664 056 A5

(51) Int. Cl.[4]: H 04 L 9/04
H 04 K 1/02

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

(12) PATENTSCHRIFT A5

(21) Gesuchsnummer: 5249/84

(22) Anmeldungsdatum: 02.11.1984

(24) Patent erteilt: 29.01.1988

(45) Patentschrift veröffentlicht: 29.01.1988

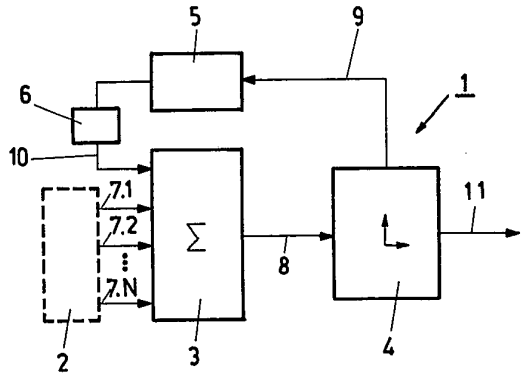
(73) Inhaber:
Borer Communications AG, Biberist

(72) Erfinder:
Massey, James L., Prof., Zürich
Rueppel, Rainer A., Wetzikon ZH

(74) Vertreter:
PPS Polyvalent Patent Service AG, Baden 2

(54) Verfahren und Vorrichtung für die Umwandlung einer digitalen Datensequenz in die verschlüsselte Form.

(57) Ein Wandler für die Herstellung von Pseudozufallssequenzen (11) unter der Kontrolle eines geheimen Schlüssel ist im wesentlichen durch ein Kombinationsmittel (1) mit Gedächtnis und Rückkopplung gebildet. Digitale periodische Sequenzen (7.1 bis 7.N) werden im Summierer (3) summiert, die digitale Summensequenz (8) wird im Aufteiler (4) getrennt und ein Teil dieser digitalen Summensequenz wird als eine digitale Rückführungssequenz (9) verwendet, die über ein digitales Speicherhilfsmittel (5) und eventuell über ein Logikhilfsmittel (6) als Rückkopplung an den Eingang des Summierers (3) geführt wird. Somit wird das gewünschte Gedächtnis und die Rückkopplung erreicht, die kompliziertere Pseudozufallssequenzen zur Folge hat.



PATENTANSPRÜCHE

1. Verfahren für die Umwandlung einer digitalen Datensequenz in eine verschlüsselte Form unter Kontrolle eines geheimen Schlüssels für die sichere Übertragung oder Speicherung durch die Kombination der digitalen Datensequenz mit einer von einem Wandler produzierten digitalen Pseudozufallssequenz, dadurch gekennzeichnet, dass im Wandler (1) wenigstens zwei periodische digitale Sequenzen (7.1 bis 7.N) aus einem periodischen Sequenzgenerator (2) in einen Summierer (3) geführt werden, dass die digitale Summensequenz (8) aus dem Summierer (3) in einem Aufteiler (4) in eine digitale Ausgangssequenz (11), welche die besagte Pseudozufallssequenz bildet, und in eine digitale Rückführungssequenz (9) aufgeteilt wird, dass die Symbole der digitalen Rückführungssequenz (9) in einem digitalen Speicherhilfsmittel (5) zwischengespeichert werden, dass die im digitalen Speicherhilfsmittel (5) zwischengespeicherten Symbole von einem Logikhilfsmittel (6) in die Symbole einer digitalen Hilfssequenz (10) transformiert werden und dass die digitale Hilfssequenz (10) zusätzlich zu den wenigstens zwei periodischen digitalen Sequenzen (7.1 bis 7.N) in den Summierer (3) geführt wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass der Aufteiler (4) das niederwertigste Bit des entsprechenden Symbols der digitalen Summensequenz (8) als entsprechendes Symbol der Ausgangssequenz (11) und den ganzzahligen Wert der verbleibenden Bits des entsprechenden Symbols der digitalen Summensequenz (8) als entsprechendes Symbol der digitalen Rückführungssequenz (9) ausgibt.

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass das Symbol im digitalen Speicherhilfsmittel (5) in seiner binären Darstellung abgespeichert wird und dass das Logikhilfsmittel (6) bewirkt, dass einzig der ganzzahlige Wert des im digitalen Speicherhilfsmittel (5) gespeicherten Symbols das entsprechende Symbol der digitalen Hilfssequenz (10) bildet.

4. Verfahren nach Anspruch 3, dadurch gekennzeichnet, dass das Logikhilfsmittel (6) bewirkt, dass das entsprechende Symbol der Hilfssequenz (10) der ganzzahligen Summe der Bits des im digitalen Speicherhilfsmittel (5) gespeicherten Symbols entspricht.

5. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die periodischen Sequenzen (7.1 bis 7.N) durch Ausgangssequenzen rückgekoppelter Schieberegister (12.1 bis 12.N) gebildet werden.

6. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die periodischen Sequenzen (7.1 bis 7.N) als das logische Bit-für-Bit Produkt je einer Ausgangssequenz der rückgekoppelten Schieberegister (12.1 bis 12.N) mit je einer Ausgangssequenz (14.1 bis 14.N) einer Stufe eines rückgekoppelten binären Wählschieberegisters (13) gebildet werden.

7. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die digitale Datensequenz und die Pseudozufallssequenz (11) durch binäre Sequenzen gebildet werden und die Kombination dieser beiden Sequenzen ihre Bit-für-Bit modulo 2 Summe ist.

8. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die verschlüsselte Form der digitalen Datensequenz und die Pseudozufallssequenz (11) durch binäre Sequenzen gebildet werden und die Kombination dieser zwei Sequenzen ihre Bit-für-Bit modulo 2 Summe ist.

9. Verfahren nach Anspruch 5 oder 6, dadurch gekennzeichnet, dass die Anfangszustände aller rückgekoppelten Schieberegister (12.1 bis 12.N, 13) und der Anfangszustand des digitalen Speicherhilfsmittels (5) durch einen geheimen Schlüssel bestimmt werden.

10. Verfahren für die Umwandlung einer nach Anspruch 1 verschlüsselten digitalen Datensequenz in die entschlüsselte Form, dadurch gekennzeichnet, dass die entschlüsselte Form der digitalen Datensequenz durch Kombination ihrer verschlüsselten Form mit der digitalen Pseudozufallssequenz (11) unter Kontrolle des geheimen Schlüssels wieder hergestellt wird.

11. Vorrichtung zur Durchführung des Verfahrens nach Anspruch 1, dadurch gekennzeichnet, dass ein periodischer Sequenzgenerator (2) mit wenigstens zwei Anschlüssen an einen Summierer (3) angeschlossen ist, dessen Ausgang mit dem Aufteiler (4) verbunden ist, wobei der Aufteiler (4) einerseits mit dem Ausgang für die pseudozufällige Ausgangssequenz (11) und andererseits mit dem digitalen Speicherhilfsmittel (5) verbunden ist, das über ein Logikhilfsmittel (6) wieder mit seinem Ausgang an den Eingang des Summierers (3) angeschlossen ist (Fig. 1).

BESCHREIBUNG

Die vorliegende Erfindung bezieht sich auf ein Verfahren für die Umwandlung einer digitalen Datensequenz in eine verschlüsselte Form unter Kontrolle eines geheimen Schlüssels für die sichere Übertragung oder Speicherung durch die Kombination der digitalen Datensequenz mit einer von einem Wandler produzierten digitalen Pseudozufallssequenz und auf eine Vorrichtung zur Durchführung des Verfahrens.

Verschiedene Verschlüsselungssysteme sind bereits bekannt. Einige dieser Systeme sind z.B. im Buch «CIPHER SYSTEMS The Protection of Communications» von Henry Beker und Fred Piper, Northwood Publications London, 1982, enthalten. So werden z.B. Nachrichten oder andere Daten im binären Code mit einer Pseudozufallssequenz in einem Wandler vermischt, gespeichert und/oder übertragen und wieder entschlüsselt. Für die Entschlüsselung ist selbstverständlich die Kenntnis des geheimen Schlüssels notwendig. Die Synchronisationsmethoden für die Übertragung der verschlüsselten Daten und für deren Entschlüsselung sind ebenfalls bekannt und auch im obengenannten Buch beschrieben. In diesem Buch ist auf S. 237, Fig. 6.8, ein Wandler zum Erreichen von Pseudozufallssequenzen beschrieben und dargestellt. Er arbeitet mit mehreren Schieberegistern, deren periodische digitale Sequenzen kombiniert werden. Die Kombination ist jedoch gedächtnisfrei und ohne Rückkopplung und somit auch die Wirksamkeit der Verschlüsselung beschränkt.

Die Aufgabe der Erfindung liegt darin, ein Verfahren und eine Vorrichtung der eingangs genannten Art zu schaffen, die die Sicherheit der Verschlüsselung und die Komplexität der Pseudozufallssequenz bei gegebenen Mitteln wesentlich erhöhen.

Die vorgenannte Aufgabe wird dadurch gelöst, dass im Wandler wenigstens zwei periodische digitale Sequenzen aus einem periodischen Sequenzgenerator in einen Summierer geführt werden, dass die digitale Summensequenz aus dem Summierer in einem Aufteiler in eine digitale Ausgangssequenz, welche die besagte Pseudozufallssequenz bildet, und in eine digitale Rückführungssequenz aufgeteilt wird, dass die Symbole der digitalen Rückführungssequenz in einem digitalen Speicherhilfsmittel zwischengespeichert werden, dass die im digitalen Speicherhilfsmittel zwischengespeicherten Symbole von einem Logikhilfsmittel in die Symbole einer digitalen Hilfssequenz transformiert werden und dass die digitale Hilfssequenz zusätzlich zu den wenigstens zwei periodischen digitalen Sequenzen in den Summierer geführt wird.

Der Vorteil der Erfindung ist darin zu sehen, dass die Kombination der Sequenzen erfindungsgemäss sowohl das Gedächtnis als auch die Rückkopplung besitzt, so dass die Verschlüsselung sicher ist und dass man mit denselben Mitteln eine komplexere Pseudozufallssequenz erreichen kann.

Die Weiterbildungen der Erfindung sind in den abhängigen Ansprüchen enthalten.

Es ist zweckmässig, dass der Aufteiler das niederwertigste Bit des entsprechenden Symbols der digitalen Summensequenz als entsprechendes Symbol der Ausgangssequenz und den ganzzahligen Wert der verbleibenden Bits des entsprechenden Symbols der digitalen Summensequenz als entsprechendes Symbol der digitalen Rückführungssequenz ausgibt.

Eine vorteilhafte Weiterbildung besteht darin, dass das Symbol im digitalen Speicherhilfsmittel in seiner binären Darstellung abgespeichert wird und dass das Logikhilfsmittel bewirkt, dass einzig der ganzzahlige Wert des im digitalen Speicherhilfsmittel gespeicherten Symbols das entsprechende Symbol der digitalen Hilfssequenz bildet.

Es ist zweckmässig, wenn das Logikhilfsmittel bewirkt, dass das entsprechende Symbol der Hilfssequenz der ganzzahligen Summe der Bits des im digitalen Speicherhilfsmittel gespeicherten Symbols entspricht.

Die periodischen Sequenzen werden vorteilhaft durch Ausgangssequenzen rückgekoppelter Schieberegister gebildet.

Nach einer anderen Variante werden die periodischen Sequenzen als das logische Bit-für-Bit Produkt je einer Ausgangssequenz der rückgekoppelten Schieberegister mit je einer Ausgangssequenz einer Stufe eines rückgekoppelten binären Wählschieberegisters gebildet.

Um eine zweckmässige Funktion zu sichern, werden die digitale Datensequenz und die digitale pseudozufällige Ausgangssequenz durch binäre Sequenzen gebildet, wobei die Kombination dieser beiden Sequenzen ihre Bit-für-Bit modulo 2 Summe ist.

Es ist ebenfalls zweckmässig, wenn die verschlüsselte Form der digitalen Datensequenz und die Pseudozufallssequenz durch binäre Sequenzen gebildet werden und die Kombination dieser zwei Sequenzen ihre Bit-für-Bit modulo 2 Summe ist.

Ein geheimer Schlüssel wird die Anfangszustände aller rückgekoppelten Schieberegister und den Anfangszustand des digitalen Speicherhilfsmittels vorteilhaft bestimmen.

Bei der Entschlüsselung wird die entschlüsselte Form der digitalen Datensequenz durch Kombination ihrer verschlüsselten Form mit der digitalen Pseudozufallssequenz unter Kontrolle des geheimen Schlüssels wieder hergestellt.

Eine einfache Vorrichtung zur Durchführung des Verfahrens besteht darin, dass ein periodischer Sequenzgenerator mit wenigstens zwei Anschlüssen an einen Summierer angeschlossen ist, dessen Ausgang mit dem Aufteiler verbunden ist, wobei der Aufteiler einerseits mit dem Ausgang für die pseudozufällige Ausgangssequenz und andererseits mit dem digitalen Speicherhilfsmittel verbunden ist, das über ein Logikhilfsmittel wieder mit seinem Ausgang an den Eingang des Summierers angeschlossen ist.

Der Erfindungsgegenstand wird anhand der Zeichnungen näher erläutert.

Es zeigt:

Fig. 1 eine beispielsweise erfindungsgemässe Ausbildung eines Kombinationsmittels, das Gedächtnis und Rückkopplung besitzt, mit einem gestrichelt gezeichneten periodischen Sequenzgenerator,

Fig. 2 eine einfache Ausbildung der erfindungsgemässen Vorrichtung und

Fig. 3 eine andere erfindungsgemässe Variante der Vorrichtung.

Gemäss Fig. 1 ist ein Kombinationsmittel 1 mit Gedächtnis und Rückkopplung als Blockschema dargestellt. Ein periodischer Sequenzgenerator 2 ist schematisch dargestellt und gestrichelt gezeichnet. Er ist mit mehreren Anschlüssen an einen Summierer 3 angeschlossen, dessen Ausgang mit dem Aufteiler 4 verbunden ist. Dieser Aufteiler 4 liefert einerseits die digitale pseudozufällige Ausgangssequenz 11, andererseits ist er mit dem digitalen Speichermittel 5 verbunden. Dieses digitale Speichermittel 5 ist über ein Logikhilfsmittel 6 mit seinem Ausgang an den Eingang des Summierers 3 angeschlossen.

Die Funktionsweise ist schon aus dem beschriebenen Schema ersichtlich. Der periodische Sequenzgenerator 2 liefert mehrere periodische digitale Sequenzen 7.1 bis 7.N, die im Summierer 3 summiert werden. Die digitale Summensequenz 8 wird in den Aufteiler 4 geleitet. Von der digitalen Rückführungssequenz 9 wird im digitalen Speicherhilfsmittel 5 das letzte Symbol abgespeichert. Wenn auch das Logikhilfsmittel 6 verwendet wird, produziert es eine digitale Hilfssequenz 11, die wieder an den Eingang des Summierers als eine Rückkopplung angeschlossen ist. Somit erreicht man, dass zusätzlich zu den periodischen digitalen Sequenzen 7.1 bis 7.N eine digitale Hilfssequenz 10 in den Summierer 3 geführt ist.

Gleiche Teile sind in allen Figuren mit denselben Bezugsziffern versehen.

Fig. 2 zeigt ein einfaches Schema der erfindungsgemässen Vorrichtung. Das Kombinationsmittel 1, das in der Fig. 1 enthalten ist, ist in der Fig. 2 wegen der Übersichtlichkeit nur als ein Block 1 gezeichnet. Mehrere Schieberegister 12.1 bis 12.N liefern periodische digitale Sequenzen 7.1 bis 7.N in das Kombinationmittel 1. Bei diesem Beispiel handelt es sich um rückgekoppelte Schieberegister 12.1 bis 12.N. Die Funktion entspricht derjenigen gemäss der Fig. 1.

Fig. 3 zeigt eine andere Variante der erfindungsgemässen Vorrichtung. Auch bei dieser Ausführungsform werden mehrere Schieberegister 12.1 bis 12.N verwendet, wie dies schon in der Lösung gemäss Fig. 2 der Fall ist. Zusätzlich wird ein rückgekoppeltes binäres Wählschieberegister 13 angesetzt, dessen einzelne Stufen an die Ausgänge der digitalen Schieberegister 12.1 bis 12.N angeschlossen sind. Diese Stufen des rückgekoppelten Wählschieberegisters 13 liefern dann entsprechende Sequenzen 14.1 bis 14.N. Bei dieser Ausgestaltung erhält man besonders komplizierte und komplexe digitale pseudozufällige Ausgangssequenzen 11.

Es ist selbstverständlich, dass bei Beibehaltung der Erfindungsidee die Wandler mit verschiedenen Quellen von periodischen digitalen Sequenzen ausgerüstet werden können. Bei der Verwendung von Schieberegistern 12.1 bis 12.N, 13, kann man verschiedene Kombinationen dieser Bestandteile ansetzen.

Bezeichnungsliste

1	=	Wandler / Kombinationsmittel mit Gedächtnis und Rückkopplung
2	=	periodischer Sequenzgenerator
3	=	Summierer
4	=	Aufteiler
5	=	digitales Speicherhilfsmittel
6	=	Logikhilfsmittel
7.1 bis 7.N	=	periodische digitale Sequenzen
8	=	digitale Summensequenz
9	=	digitale Rückführungssequenz
10	=	digitale Hilfssequenz
11	=	digitale Pseudozufallssequenz / digitale pseudozufällige Ausgangssequenz
12.1 bis 12.N	=	rückgekoppeltes Schieberegister
13	=	rückgekoppeltes Wählschieberegister
14.1 bis 14.N	=	Sequenzen des rückgekoppelten Wählschieberegisters

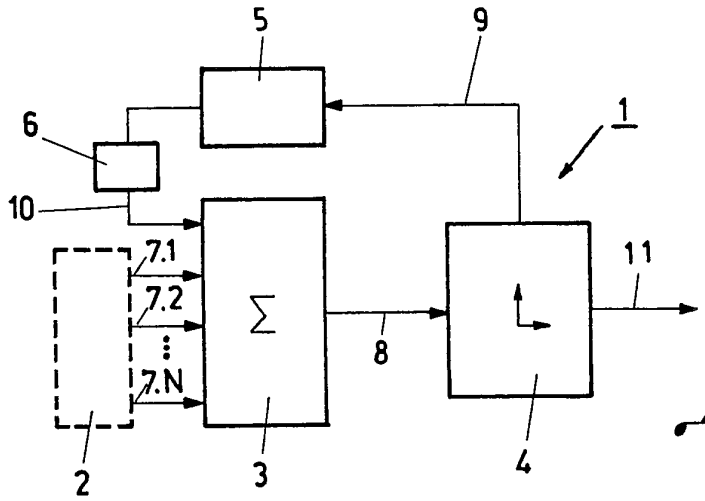


Fig. 1

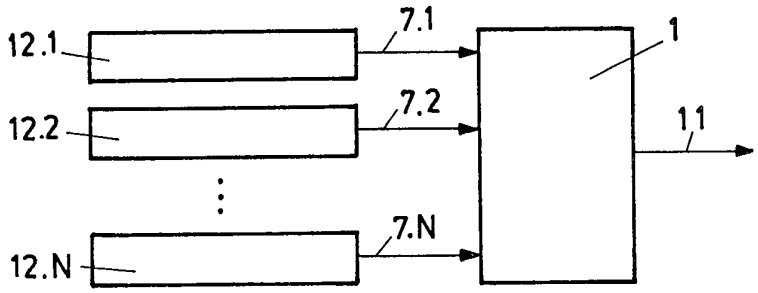


Fig. 2

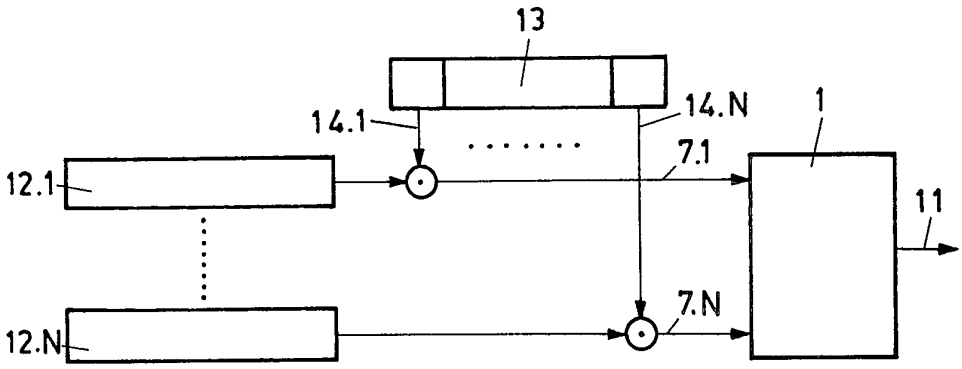


Fig. 3