


Erfindungspatent für die Schweiz und Liechtenstein

Schweizerisch-liechtensteinischer Patentschutzvertrag vom 22. Dezember 1978

(12) PATENTSCHRIFT A5

(21) Gesuchsnummer: 2762/83

 (73) Inhaber:
Gretag Aktiengesellschaft, Regensdorf

(22) Anmeldungsdatum: 20.05.1983

 (72) Erfinder:
Klemenz, Hans-Jörg, Dielsdorf
Widmer, Walter Rudolf, Niederhasli

(24) Patent erteilt: 28.11.1986

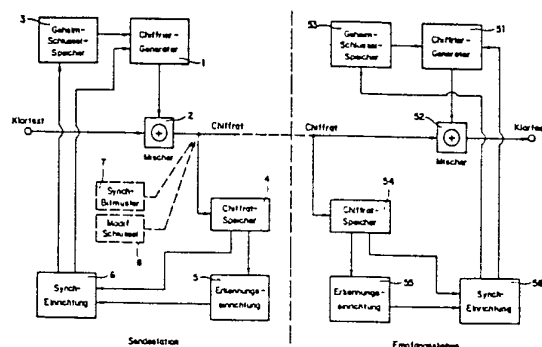
 (45) Patentschrift
veröffentlicht: 28.11.1986

 (74) Vertreter:
CIBA-GEIGY AG, Basel

(54) Verfahren und Vorrichtung zur chiffrierten Datenübermittlung.

(57) Sendeseitig wird das Chifftrat durch Mischen des Klar-texts mit einer von einem Chiffriergenerator (1) erzeugten Schlüsselimpulsfolge gebildet. Eine Erkennungseinrichtung (5) untersucht in Verbindung mit einem Chiffratspeicher (4) das Chifftrat laufend auf das Auftreten eines bestimmten Synchronisierbitmusters. Sobald dieses auftritt, wird eine Neuinitierung des Chiffriergenerators (1) ausgelöst, wobei als neuer Chiffrierschlüssel oder als Auswahladresse für in einem Schlüsselspeicher (3) vorrätig gehaltene Chiffrierschlüssel eine Anzahl von auf das Synchronisierbitmuster folgenden Chifftratbits verwendet werden. Empfangsseitig wird analog vorgegangen.

Auf diese Weise wird eine Übertragung von zusätzlicher Information bei der Neusynchronisation und damit eine Reduktion des Datendurchsatzes vermieden.


POOR QUALITY

PATENTANSPRÜCHE

1. Verfahren zur Übermittlung von Daten in chiffrierter Form durch sende- und empfangsseitiges Mischen des Klartexts bzw. des Chiffrats mit einer identischen Schlüsselimpulsfolge, die sende- und empfangsseitig in gleichen, durch wenigstens einen Chiffrierschlüssel determinierten Chiffriergeneratoren erzeugt wird, wobei die Chiffriergeneratoren von Zeit zu Zeit unter Wechsel des wenigstens einen Chiffrierschlüssels neu initiiert werden, dadurch gekennzeichnet, dass die Zeitpunkte der Neuinitialisierung durch das Auftreten eines vorgegebenen Synchronisationsbitmusters im Chifftrat bestimmt werden, und dass der wenigstens eine bei den Neuinitialisierungen neu zu ladende Chiffrierschlüssel aus einer vorgegebenen Anzahl von Chifftratbits bestimmt wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die vorgegebene Anzahl von Chifftratbits direkt als Chiffrierschlüssel verwendet wird.

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die vorgegebene Anzahl von Chifftratbits als Auswahladresse für einen Vorrat von sende- und empfangsseitig in gespeicherter Form vorliegenden Chiffrierschlüsseln verwendet wird.

4. Verfahren nach einem der Ansprüche 1 - 3, dadurch gekennzeichnet, dass bei gegebener Übertragungsrate das Synchronisationsbitmuster so gewählt wird, dass eine Neuinitialisierung im Mittel alle 0,5 bis 4 sek, vorzugsweise etwa alle Sekunden erfolgt.

5. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass das Synchronisationsbitmuster in geheimer, nicht zugänglicher Form gespeichert wird.

6. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass das Synchronisationsbitmuster beim Verbindungsaufbau aktiv übertragen wird.

7. Vorrichtung zur Durchführung des Verfahrens nach Patentanspruch 1 mit einer sendeseitigen Chiffrierstation und einer empfangsseitigen Dechiffrierstation, wobei beide Stationen mit einem autonomen Chiffriergenerator und einem Mischer zum Mischen von Klartext bzw. Chifftrat mit einer vom jeweiligen Chiffriergenerator erzeugten Schlüsselimpulsfolge ausgestattet sind und wobei beide Stationen ferner eine Synchronisationseinrichtung aufweisen, mit der wenigstens ein Chiffrierschlüssel in den Chiffriergenerator geladen und dieser dadurch initialisiert werden kann, dadurch gekennzeichnet, dass in Chiffrier- und Dechiffrierstation ein Chiffratspeicher sowie eine an diesen angeschlossene Erkennungseinrichtung vorgesehen sind, welche letztere beim Auftreten eines vorgegebenen Synchronisationsbitmusters im Chifftrat die Synchronisationseinrichtung zu einer Neuinitialisierung veranlasst, und dass die Synchronisationseinrichtung den neu zu ladenden Chiffrierschlüssel aus einer vorgegebenen Anzahl von Chifftratbits bestimmt.

8. Vorrichtung nach Anspruch 7, dadurch gekennzeichnet, dass die Synchronisationseinrichtung die vorgegebene Anzahl von Chifftratbits direkt als Chiffrierschlüssel in den jeweiligen Chiffriergenerator lädt.

9. Vorrichtung nach Anspruch 7, dadurch gekennzeichnet, dass in Chiffrier- und Dechiffrierstation ein Vorrat von Chiffrierschlüsseln gespeichert ist, und dass die Synchronisationseinrichtung den in den Chiffriergenerator neu zu ladenden Chiffrierschlüssel anhand der vorgegebenen Anzahl von Chifftratbits auswählt und lädt.

10. Vorrichtung nach einem der Ansprüche 7 - 9, dadurch gekennzeichnet, dass Schaltmittel vorgesehen sind, welche das Synchronisationsbitmuster beim Verbindungsaufbau aktiv übertragen.

Die Erfindung betrifft ein Verfahren und eine Vorrichtung zur chiffrierten Datenübermittlung gemäss Oberbegriff des Patentanspruchs 1 bzw. 7.

Chiffrier-/Dechiffriersysteme dieser Art sind heute allgemein bekannt und verbreitet. Einige typische Vertreter sind zum Beispiel in der US-PS 4 369 434 erwähnt und beschrieben.

Die Neuinitialisierung der Chiffriergeneratoren erfolgt bei diesen bekannten Systemen derart, dass entweder der neu zu ladende Chiffrierschlüssel selber (zufallsmässig erzeugter Zusatz- oder Modifizierschlüssel) und/oder — bei Systemen mit gespeichertem Schlüsselvorrat — eine Auswahladresse für den neu zu ladenden Schlüssel von der die Neuinitialisierung verlangenden Station zur Partnerstation übertragen wird. Durch diese Übertragung von zusätzlicher Information wird der (Nutz-)Datendurchsatz herabgesetzt, was insbesondere dann ins Gewicht fällt, wenn häufigere Nachsynchronisierungen (z.B. für Späteintritt oder nach Fehlern, häufiger Schlüsselwechsel) nötig oder erwünscht sind.

Durch die Erfindung soll nun dieses Problem überwunden und insbesondere das Verfahren und die Vorrichtung der zur Rede stehenden Art dahingehend verbessert werden, dass zur Neuinitialisierung der Chiffriergeneratoren keine Übertragung von zusätzlicher Information notwendig ist und damit der Nutzdendurchsatz dabei nicht reduziert wird.

Das erfindungsgemässe Verfahren und die entsprechende Vorrichtung, welche diesen Anforderungen genügen, sind in den Patentansprüchen 1 und 7 beschrieben. Bevorzugte Ausführungsformen und Weiterbildungen ergeben sich aus den abhängigen Ansprüchen.

Im folgenden wird die Erfindung anhand der Zeichnung beispielsweise näher erläutert. Die einzige Zeichnungsfigur zeigt ein auf das Wesentlichste reduziertes Blockschema eines Ausführungsbeispiels einer erfindungsgemässen Chiffrier-/Dechiffriervorrichtung.

Die dargestellte Chiffrier-/Dechiffriervorrichtung entspricht im wesentlichen den in der schon genannten US-PS 4 369 434 angeführten Vorrichtungen. In der Zeichnung sind daher nur die für das Verständnis der Erfindung unmittelbar notwendigen Funktionsblöcke gezeigt. Es sind dies auf Sendeseite und Empfangsseite je ein Chiffriergenerator 1 bzw. 51, ein Modulo-2-Mischer 2 bzw. 52, ein Schlüsselspeicher 3 bzw. 53, ein Chiffratspeicher 4 bzw. 54, eine Erkennungseinrichtung 5 bzw. 55 und eine Synchronisationseinrichtung 6 bzw. 56.

Mit Ausnahme des Chiffratspeichers 4 bzw. 54 und der Erkennungseinrichtung 5 bzw. 55 stimmt die gesamte Vorrichtung in Aufbau und Funktionsweise mit dem Stand der Technik, wie er z.B. durch die US-PS 4 369 434 repräsentiert ist, überein: Der Chiffriergenerator 1 bzw. 51, der bei jeder Neuinitialisierung via Synchronisationseinrichtung 6 bzw. 56 mit einem neuen Chiffrierschlüssel geladen wird, erzeugt eine Schlüsselimpulsfolge, die im Mischer 2 bzw. 52 zum Klartext bzw. Chifftrat hinzugegemischt wird, um das Chifftrat bzw. wieder den ursprünglichen Klartext zu ergeben.

Der Chiffrierschlüssel besteht in der Regel aus mehreren Teil-Schlüsseln, von denen einer ein sogenannter Grund- oder Geheimschlüssel und ein anderer ein sogenannter Zusatz- oder Modifizierschlüssel ist. Letzterer wird üblicherweise bei jeder Neuinitialisierung neu zufallsmässig erzeugt. Der Grund- oder Geheimschlüssel wird im Unterschied dazu nicht jedesmal neu erzeugt, sondern es ist im Schlüsselspeicher 3 bzw. 53 ein grösserer Vorrat an Geheimschlüsseln gespeichert vorhanden, aus denen beim Schlüsselwechsel mittels einer meist zufälligen Auswahladresse jeweils einer ausgewählt und in den Chiffriergenerator geladen wird.

Bei den in der US-PS 4 369 434 detaillierter erläuterten Chiffrier-/Dechiffriersystemen werden der zufallsmässige Modifizierschlüssel und die ebenfalls zufällige Auswahladresse für den Geheimschlüssel bei jeder Neuinitialisierung zur Partnersta-

tion übertragen, was zu der schon eingangs erwähnten Datendurchsatzreduktion führt. Beim System gemäss der Erfindung wird anders vorgegangen: Hier wird das Chiffprat sende- und empfangsseitig laufend über eine gewisse Anzahl von Bits auf das Auftreten eines vorgegebenen Bitmusters — des sogenannten Synchronisationsbitmusters — überwacht. Wenn dieses Bitmuster auftritt, wird eine Neuinitialisierung des Chiffriergenerators veranlasst, wobei eine bestimmte Anzahl von auf das Synchronisationsbitmuster folgenden Bits des Chiffrats entweder als neuer Modifizierungsschlüssel oder als Auswahladresse für den neu zu ladenden Geheimschlüssel verwendet werden. Gewünschtenfalls können beide Möglichkeiten auch kombiniert werden, wobei dann z.B. ein Teil dieser nachfolgenden Chiffpratbits den neuen Modifizierschlüssel und ein anderer Teil die Auswahladresse für den Geheimschlüssel bilden. Selbstverständlich können auch dem Synchronisationsbitmuster vorausgegangene Chiffpratbits als Schlüssel bzw. Auswahladressen benutzt werden.

Zur Realisierung dieses erfindungsgemässen Verfahrensprinzips sind nur wenige zusätzliche Funktionsstufen notwendig, und zwar der Chiffratspeicher 4 bzw. 54 und die Erkennungseinrichtung 5 bzw. 55. Der Chiffratspeicher kann z.B. ein Schieberegister sein, durch welches die Chiffpratbits im Takte der Übertragungsgeschwindigkeit durchgeschoben werden. Die Erkennungseinrichtung vergleicht die Inhalte einer gegebenen Anzahl von Speicherzellen des Chiffratspeichers mit einem vorprogrammierten Synchronisierbitmuster und löst bei Übereinstimmung die Neuinitialisierung via Synchronisierereinrichtung aus.

Das Synchronisierbitmuster ist vorzugsweise analog wie die Geheimschlüssel geheim, d.h. in nicht zugänglicher Form gespeichert. Es kann dadurch weniger leicht erkannt und gezielt gestört werden.

Bei den heutigen modernen Chiffrier/Dechiffriergeräten

sind die meisten Funktionen mittels eines Micro- oder Minicomputers und entsprechender Software implementiert. Dasselbe kann natürlich auch für die einzelnen Funktionsstufen der Vorrichtung gemäss der vorliegenden Erfindung gelten.

5 Durch das erfindungsgemässe Verfahrensprinzip wird also eine Übertragung von Chiffrierschlüsseln bzw. ihrer Auswahladressen überflüssig. Auf diese Weise kann — im Interesse der kryptologischen Sicherheit — ein sehr häufiger Schlüsselwechsel durchgeführt werden, ohne dass dadurch der Datendurchsatz 10 beeinträchtigt würde. Dasselbe gilt für Nachsynchronisation zum Zweck des Späteintritts oder Synchronisation nach Fehlern usw.

Die Länge des Synchronisierbitmusters ist an sich beliebig. Sie wird mit Vorzug so gewählt, dass bei gegebener Übertragungsrate im statischen Mittel eine gewünschte Anzahl — 15 beispielsweise etwa 0,2 bis 2, vorzugsweise rund 1, von Schlüsselwechseln pro Sekunde stattfindet. Bei einer Übertragungsrate von 19,2 KB/S findet z.B. bei einer Synchronisierbitmusterlänge von 14 Bit etwa alle Sekunden und bei einer Länge von 16 20 Bit etwa alle 3 Sekunden eine Neusynchronisierung statt.

Die Anzahl der als Chiffrierschlüssel bzw. Auswahladresse benutzten auf das Synchronisierbitmuster folgenden Chiffpratbits hängt von den verwendeten Chiffrierschlüsseln selbst bzw. der Anzahl der gespeicherten Schlüssel ab.

25 Zur Beschleunigung des Verbindungsaufbaus zwischen den Partnerstationen kann für die erste Synchronisation das Synchronisierbitmuster auch aktiv übertragen werden, anstatt zu warten, bis es zufällig erzeugt wird. In der Zeichnung ist dies durch die zwei dargestellten Funktionsblöcke 7 und 8 in der 30 Sendestation angedeutet. Block 7 legt bei der Verbindungsaufnahme das Synchronisierbitmuster auf die Chiffpratleitung, Block 8 lässt darauf eine als Modifizierschlüssel bestimmte Zufallsbitsequenz folgen. Chiffratspeicher und Erkennungseinrichtung funktionieren in gleicher Weise wie bisher beschrieben.

