



(10) **AT 515814 A1 2015-12-15**

(12) **Österreichische Patentanmeldung**

(21) Anmeldenummer: A 379/2014
 (22) Anmeldetag: 20.05.2014
 (43) Veröffentlicht am: 15.12.2015

(51) Int. Cl.: **H04L 9/06** (2006.01)
H04L 9/12 (2006.01)
G06F 7/58 (2006.01)
H04L 29/06 (2006.01)

(56) Entgegenhaltungen:
 AT 510730 B1
 EP 0615361 A1
 US 5859912 A
 WO 03075507 A1
 WO 2007059558 A1

(71) Patentanmelder:
 LogoDynamic Unit GmbH
 1040 Wien (AT)

(74) Vertreter:
 Haffner und Keschmann Patentanwälte GmbH
 Wien

(54) **Verfahren und Vorrichtung zur Durchführung einer symmetrischen Stromverschlüsselung von Daten**

(57) Bei einem Verfahren zur Durchführung einer symmetrischen Stromverschlüsselung von Daten unter Verwendung eines Schlüsselstroms und zur Übertragung der verschlüsselten Daten, wobei die Generierung des Schlüsselstroms unter Verwendung wenigstens eines rückgekoppelten Schieberegisters erfolgt, das zu seiner Initialisierung mit einer definierten Bitfolge gefüllt wird, werden die zu verschlüsselnden Daten in Datenpakete aufgeteilt, wobei jedes Datenpaket gesondert verschlüsselt wird. Das bzw. die rückgekoppelte(n) Schieberegister wird bzw. werden für die Verschlüsselung jedes Datenpakets neu initialisiert, wobei zur Initialisierung des bzw. der rückgekoppelten Schieberegisters jeweils wenigstens eine erste Bitfolge und eine zweite Bitfolge verwendet wird, wobei die erste Bitfolge dem jeweils verschlüsselten Datenpaket im Klartext oder in codierter Form hinzugefügt wird und die zweite Bitfolge einen geheimen Schlüssel darstellt, die den verschlüsselten Datenpaketen nicht hinzugefügt wird. Die verschlüsselten Datenpakete werden samt der jeweiligen hinzugefügten Bitfolge und ggf. Kopfdaten paketvermittelt übertragen. Die erste Bitfolge wird unter Verwendung eines nichtdeterministischen Zufallszahlengenerators generiert.

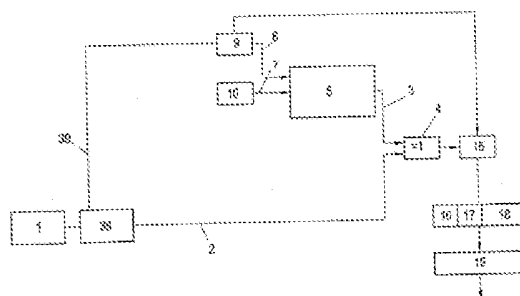


Fig. 1

Zusammenfassung:

Bei einem Verfahren zur Durchführung einer symmetrischen Stromverschlüsselung von Daten unter Verwendung eines Schlüsselstroms und zur Übertragung der verschlüsselten Daten, wobei die Generierung des Schlüsselstroms unter Verwendung wenigstens eines rückgekoppelten Schieberegisters erfolgt, das zu seiner Initialisierung mit einer definierten Bitfolge gefüllt wird, werden die zu verschlüsselnden Daten in Datenpakete aufgeteilt, wobei jedes Datenpaket gesondert verschlüsselt wird. Das bzw. die rückgekoppelte(n) Schieberegister wird bzw. werden für die Verschlüsselung jedes Datenpakets neu initialisiert, wobei zur Initialisierung des bzw. der rückgekoppelten Schieberegister jeweils wenigstens eine erste Bitfolge und eine zweite Bitfolge verwendet wird, wobei die erste Bitfolge dem jeweils verschlüsselten Datenpaket im Klartext oder in codierter Form hinzugefügt wird und die zweite Bitfolge einen geheimen Schlüssel darstellt, die den verschlüsselten Datenpaketen nicht hinzugefügt wird. Die verschlüsselten Datenpakete werden samt der jeweiligen hinzugefügten Bitfolge und ggf. Kopfdaten paketvermittelt übertragen. Die erste Bitfolge wird unter Verwendung eines nichtdeterministischen Zufallszahlengenerators generiert.

Fig. 1

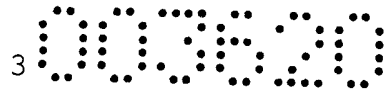
Die Erfindung betrifft Verfahren zur Durchführung einer symmetrischen Stromverschlüsselung von Daten unter Verwendung eines Schlüsselstroms und zur Übertragung der verschlüsselten Daten, wobei die Generierung des Schlüsselstroms unter Verwendung wenigstens eines rückgekoppelten Schieberegisters erfolgt, das zu seiner Initialisierung mit einer definierten Bitfolge gefüllt wird, wobei die zu verschlüsselnden Daten in Datenpakete aufgeteilt werden und jedes Datenpaket gesondert verschlüsselt wird, wobei das bzw. die rückgekoppelte(n) Schieberegister für die Verschlüsselung jedes Datenpakets neu initialisiert wird bzw. werden, wobei zur Initialisierung des bzw. der rückgekoppelten Schieberegister jeweils wenigstens eine erste Bitfolge und eine zweite Bitfolge verwendet wird, wobei die erste Bitfolge dem jeweils verschlüsselten Datenpaket im Klartext oder in codierter Form hinzugefügt wird und die zweite Bitfolge einen geheimen Schlüssel darstellt, die den verschlüsselten Datenpaketen nicht hinzugefügt wird, und wobei die verschlüsselten Datenpakete samt der jeweiligen hinzugefügten Bitfolge und ggf. Kopfdaten paketvermittelt übertragen werden.

Die Erfindung betrifft weiters eine Vorrichtung zum Verschlüsseln von Daten mit Hilfe einer symmetrischen Stromverschlüsselung unter Verwendung eines Schlüsselstroms, wobei zur Generierung des Schlüsselstroms wenigstens ein rückgekoppeltes Schieberegister vorgesehen ist, das zu seiner Initialisierung jeweils mit einer definierten Bitfolge gefüllt wird, wobei die Daten in Datenpakete aufgeteilt vorliegen, wobei Mittel zum Generieren und/oder Speichern wenigstens einer ersten Bitfolge und einer zweiten Bitfolge vorgesehen sind, die

mit dem bzw. den Schieberegister(n) derart zusammenwirken, dass wenigstens die erste Bitfolge und die zweite Bitfolge zur Initialisierung des bzw. der rückgekoppelten Schieberegister verwendet werden, wobei das bzw. die rückgekoppelte(n) Schieberegister für die Verschlüsselung jedes Datenpakets neu initialisiert wird bzw. werden, wobei Datenpaketverarbeitungsmittel vorgesehen sind, mit denen die Mittel zum Generieren bzw. Speichern der ersten und der zweiten Bitfolge derart zusammenwirken, dass die erste Bitfolge dem jeweils verschlüsselten Datenpaket im Klartext oder in codierter Form hinzugefügt wird und die zweite Bitfolge einen geheimen Schlüssel darstellt, die den verschlüsselten Datenpaketen nicht hinzugefügt wird, und wobei Datenübertragungsmittel zum paketvermittelten Versenden der verschlüsselten Datenpakete samt der jeweiligen hinzugefügten Bitfolge und ggf. Kopfdaten vorgesehen sind.

Ein solches Verfahren und eine solche Vorrichtung sind in der WO 2012/071597 A1 beschrieben.

Als Stromverschlüsselung bezeichnet man einen kryptographischen Algorithmus, bei dem Zeichen des Klartextes mit den Zeichen eines Schlüsselstroms einzeln verknüpft werden. Im Fall der Stromverschlüsselung von digitalen Daten - es kommen nur die Zeichen 0 und 1 zum Einsatz - erfolgt die Verknüpfung des Klartextstroms mit dem Schlüsselstrom mit Hilfe der XOR-Funktion. Der Schlüsselstrom ist eine pseudozufällige Zeichenfolge. Die meisten Stromchiffrierungen benutzen einen symmetrischen Schlüssel. Der Schlüssel bestimmt den Initialzustand des Systems.



Zur Erzeugung des Schlüsselstroms wird in der Regel wenigstens ein rückgekoppeltes Schieberegister verwendet. Linear rückgekoppelte Schieberegister können effizient sowohl direkt in Hardware, wie beispielsweise FPGAs, als auch in Software implementiert werden. Rückgekoppelte Schieberegister sind schnell und produzieren Pseudozufallsfolgen mit guten statistischen Eigenschaften. Ein rückgekoppeltes Schieberegister ist in der Digitaltechnik als ein Schieberegister mit n Speicherelementen realisiert. Die einzelnen Speicherelemente sind typischerweise D-Flipflops, welche je ein Bit speichern können. Im Gegensatz zu einem herkömmlichen Schieberegister bestehen zwischen bestimmten D-Flipflops Abzweigungen, welche die Rückkopplungen darstellen. Zur Rückkoppelung wird in der Regel jeweils eine XOR-Funktion verwendet. Statt der XOR-Verknüpfung kann aber auch eine XNOR-Verknüpfung eingesetzt werden.

Zur Initialisierung kann das Schieberegister mit XOR-Rückkopplung mit beliebigen Werten gefüllt werden, die den vom Schieberegister in der Folge generierten Schlüsselstrom bestimmen. Wie jedes andere Schieberegister verfügt auch das rückgekoppelte Schieberegister über einen Takteingang: Bei jedem Taktimpuls wird in den Folgezustand gewechselt, d.h. wenn ein Bit ausgegeben werden soll, werden alle Bits im Schieberegister um einen Speicherplatz verschoben; das neue Bit am Ende des Schieberegisters wird abhängig von den anderen Bits berechnet. Dieser Vorgang zählt als ein Takt. Für einen vollständigen Durchlauf aller Kombinationen sind 2^{n-1} Taktimpulse notwendig. Eine derartige Codesequenz hat somit eine Länge von 2^{n-1} bit (n = Anzahl der codegenerierenden in Reihe geschalteten Speicherelemente des Schieberegisters). Als Schlüsselstromgenerator werden

in der Regel mehrere lineare rückgekoppelte Schieberegister eingesetzt, die meist unterschiedlich lang sind und unterschiedliche Rückkopplungspolynome haben. Damit kombiniert man lineare rückgekoppelte Schieberegister zu nichtlinearen Generatoren.

Je größer die Länge der Codesequenz des Schlüsselstroms bzw. des Codes ist, desto schwerer ist dieser zu entschlüsseln. Beispielsweise bräuchte ein unendlicher Code gar nicht versteckt zu werden, da er ja nie ganz bekannt ist. Funktionell ist jeder Code als unendlich anzusehen, der sich nicht vor dem Ende der zu verschlüsselnden Information wiederholt. Ein funktionell unendlicher Code hat den Nachteil, dass er nicht übertragen werden kann; er muss generiert werden.

Nachteilig bei Codegeneratoren in der Form von herkömmlichen rückgekoppelten Schieberegistern ist die Tatsache, dass von der Codesequenz leicht auf die Struktur des Generators geschlossen werden kann, so dass sie mit einem gleichgebauten Generator nachgeneriert werden kann. Eine wesentliche Verbesserung wird in dieser Hinsicht durch den aus der WO 03/075507 A1 bekannten Codegenerator erzielt.

Ein weiterer Nachteil bei der herkömmlichen Stromverschlüsselung von Daten ist der Umstand, dass sie bei der paketvermittelten Datenübertragung (z.B. im Internet über das IP-Protokoll) nur unter Verringerung der Verschlüsselungssicherheit verwendet werden kann. Bei der paketvermittelten Datenübertragung muss jedes Datenpaket gesondert verschlüsselt werden und der für die Verschlüsselung jedes Datenpakets verwendete Schlüssel muss

beim Empfänger zum Zwecke der Entschlüsselung bekannt sein, um eine Entschlüsselung auch dann zu ermöglichen, wenn einzelne Datenpakete verloren gehen, Pakete doppelt beim Empfänger ankommen, Pakete verschiedene Wege nehmen oder Pakete fragmentiert beim Empfänger ankommen. Die einfachste Möglichkeit, auch unter den Bedingungen dieser Fehlfunktionen eine eindeutige Zuordnung von Daten mit dem Schlüssel bzw. Schlüsselstrom zu gewährleisten, ist es für jedes Datenpaket denselben Schlüsselstrom zu verwenden. Dies erleichtert es aber, die Verschlüsselung zu brechen.

In der WO 2012/071597 A1 wurde daher ein Verfahren vorgeschlagen, bei dem der Schlüsselstromgenerator für jedes Datenpaket neu initialisiert wird, wobei zur Initialisierung des bzw. der rückgekoppelten Schieberegister des Schlüsselstromgenerators jeweils wenigstens eine erste Bitfolge und eine zweite Bitfolge verwendet wird, wobei die erste Bitfolge dem jeweils verschlüsselten Datenpaket im Klartext oder in codierter Form hinzugefügt wird und die zweite Bitfolge einen geheimen Schlüssel darstellt, die den verschlüsselten Datenpaketen nicht hinzugefügt wird. Sämtliche für die Entschlüsselung jedes einzelnen Datenpakets erforderliche Information mit Ausnahme des geheimen Schlüssels wird im jeweiligen Paket mitgeführt, sodass die Kommunikationspartner lediglich den geheimen Schlüssel bzw. die für die Generierung des geheimen Schlüssels erforderlichen Informationen vor der Datenübermittlung austauschen müssen. Dadurch, dass jedes Datenpaket die erste Bitfolge im Klartext oder in codierter Form enthält, die zur Verschlüsselung des jeweiligen Datenpakets verwendet wurde, kann diese erste Bitfolge vom Empfänger aus dem jeweiligen Datenpaket ausgelesen und zum

Entschlüsseln herangezogen werden. Dies ermöglicht es, jedes Datenpaket mit einem anderen Schlüssel zu verschlüsseln, sodass ein Brechen der Verschlüsselung erschwert wird. Zu diesem Zweck wurde in der WO 2012/071597 A1 vorgeschlagen, als erste Bitfolge eine für das zu verschlüsselnde Paket eindeutige Paketnummer zu wählen.

Die vorliegende Erfindung zielt nun darauf, ab das Verfahren gemäß WO 2012/071597 A1 noch weiter zu verbessern, um das Brechen der Verschlüsselung zu verunmöglichen. Zur Lösung dieser Aufgabe sieht die Erfindung bei einem Verfahren der eingangs genannten Art vor, dass die erste Bitfolge unter Verwendung eines nichtdeterministischen Zufallszahlengenerators generiert wird. Als nichtdeterministischer Zufallszahlengenerator kann zum Beispiel ein hardwarebasierter, physikalischer Zufallsgenerator zum Einsatz kommen. Die zufällige Informationsquelle kann aber auch nicht vorhersehbare Zustände in bestimmten Prozessen des Systems sein. In besonders einfacher Weise kann der nichtdeterministische Zufallszahlengenerator einen Pseudozufallsgenerator umfassen, der eine pseudozufällige Zeichenfolge generiert, aus welcher zu zufälligen Zeitpunkten jeweils ein Teilabschnitt genommen und als erste Bitfolge verwendet wird.

Eine bevorzugte Ausbildung sieht in diesem Zusammenhang vor, dass die pseudozufällige Zeichenfolge in einen Ringpuffer geschrieben wird und die erste Bitfolge aus dem Ringpuffer ausgelesen wird. Hierbei sollte der Ringpuffer eine Speicherkapazität aufweisen, die einem Vielfachen der Länge der ersten Bitfolge entspricht.

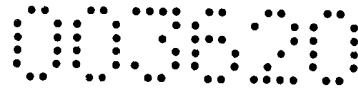
Besonders bevorzugt wird als zufälliger Zeitpunkt der Zeitpunkt des Eintreffens bzw. Detektierens eines zu verschlüsselnden Datenpakets gewählt.

Was die Codegenerierung selbst betrifft, können die folgenden bevorzugten Ausbildung zum Einsatz gelangen.

Wie erwähnt werden die erste und die zweite Bitfolge im Rahmen der Ver- bzw. Entschlüsselung dazu verwendet, das oder die rückgekoppelte(n) Schieberegister zu initialisieren. Für den Fall, dass wenigstens zwei miteinander verschaltete rückgekoppelte Schieberegister für die Generierung des Schlüsselstroms verwendet werden, wird dabei bevorzugt so vorgegangen, dass wenigstens ein erstes rückgekoppeltes Schieberegister zu seiner Initialisierung mit der ersten Bitfolge gefüllt wird und wenigstens ein zweites rückgekoppeltes Schieberegister zu seiner Initialisierung mit der zweiten Bitfolge gefüllt wird. Diese Vorgehensweise erschwert es, auf Grundlage der im Klartext mitübermittelten ersten Bitfolge die Struktur des Schlüsselstromgenerators und/oder den geheimen Schlüssel zu ermitteln.

Ein weiterer Vorteil des erfindungsgemäßen Verfahrens ist, dass die Generierung des Schlüsselstroms beginnen kann, sobald alle rückgekoppelten Schieberegister gleichzeitig mit der jeweiligen Bitfolge gefüllt werden.

Die Struktur des Schlüsselstromgenerators ist wie an sich bekannt bevorzugt so, dass zur Rückkoppelung des bzw. der Schieberegister wenigstens ein XOR-Gatter verwendet wird. Die Komplexität des Generators kann dabei in einfacher Weise dadurch erhöht werden, dass die rückgekoppelten

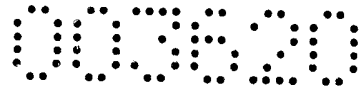


Schieberegister derart miteinander verschaltet sind, dass in Abhängigkeit vom Zustand des einen Schieberegisters das wenigstens eine XOR-Gatter des anderen Schieberegister an- oder abgeschaltet wird.

Eine überaus bevorzugte Weiterbildung ergibt sich, wenn ein Codegenerator zum Einsatz gelangt, wie er in der WO 03/075507 A1 beschrieben ist, wobei auf die Ansprüche 10 bis 12 sowie 22 bis 27 der vorliegenden Anmeldung verwiesen wird. Bei einem derartigen Codegenerator kann die Verschlüsselung nicht einmal dann gebrochen werden, wenn sowohl die Struktur des Codegenerators als auch der in ihm ablaufende Algorithmus bekannt sind. Die Struktur des Generators ist nämlich so geartet, dass sie eine derartig hohe Anzahl an unterschiedlichen Codes in einer derartig großen Länge zu generieren im Stande ist, dass die Entdeckung des gerade verwendeten Codes so wie die aktuell produzierte Stelle in der Codesequenz nur mit einer extrem geringen Wahrscheinlichkeit möglich ist. Der Code kann dann nicht nachgeneriert werden, wenn der Generator so viele verschiedene Codes erstellen kann, dass von einem Abschnitt des einzelnen Codes nicht auf dessen Fortsetzung geschlossen werden kann.

Gemäß einem weiteren Aspekt der vorliegenden Erfindung wird eine Verschlüsselungsvorrichtung vorgeschlagen.

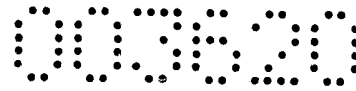
Die erfindungsgemäße Vorrichtung zum Verschlüsseln von Daten mit Hilfe einer symmetrischen Stromverschlüsselung unter Verwendung eines Schlüsselstroms, wobei zur Generierung des Schlüsselstroms wenigstens ein rückgekoppeltes Schieberegister vorgesehen ist, das zu seiner Initialisierung jeweils mit einer definierten



Bitfolge gefüllt wird, wobei die Daten in Datenpakete aufgeteilt vorliegen, wobei Mittel zum Generieren und/oder Speichern wenigstens einer ersten Bitfolge und einer zweiten Bitfolge vorgesehen sind, die mit dem bzw. den Schieberegister(n) derart zusammenwirken, dass wenigstens die erste Bitfolge und die zweite Bitfolge zur Initialisierung des bzw. der rückgekoppelten Schieberegister verwendet werden, wobei das bzw. die rückgekoppelte(n) Schieberegister für die Verschlüsselung jedes Datenpakets neu initialisiert wird bzw. werden, wobei Datenpaketverarbeitungsmittel vorgesehen sind, mit denen die Mittel zum Generieren bzw. Speichern der ersten und der zweiten Bitfolge derart zusammenwirken, dass die erste Bitfolge dem jeweils verschlüsselten Datenpaket im Klartext oder in codierter Form hinzugefügt wird und die zweite Bitfolge einen geheimen Schlüssel darstellt, die den verschlüsselten Datenpaketen nicht hinzugefügt wird, und wobei Datenübertragungsmittel zum paketvermittelten Versenden der verschlüsselten Datenpakete samt der jeweiligen hinzugefügten Bitfolge und ggf. Kopfdaten vorgesehen sind, ist dadurch gekennzeichnet, dass die Mittel zum Generieren der ersten Bitfolge einen nichtdeterministischen Zufallszahlengenerator umfassen.

Bevorzugte Weiterbildungen ergeben sich aus den Unteransprüchen.

Die Erfindung wird in der Folge anhand von in der Zeichnung schematisch dargestellten Ausführungsbeispielen näher erläutert. In dieser zeigen Fig.1 eine erfindungsgemäße Verschlüsselungsvorrichtung, Fig.2 eine zugehörige Entschlüsselungsvorrichtung, Fig.3, Fig.4 und Fig.5 verschiedene Ausbildungen eines in der Vorrichtung



verwendeten Schlüsselstromgenerators und Fig.6 einen in der Verschlüsselungsvorrichtung eingesetzten Zufallszahlengenerator.

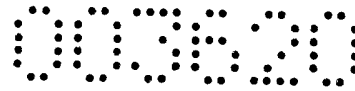
In Fig. 1 ist ein zu verschlüsselndes Datenpaket mit 1 bezeichnet, wobei das Datenpaket 1 eine Vielzahl von Bits im Klartext umfasst. Die Verschlüsselung erfolgt grundsätzlich derart, dass die Bits des Bitstroms 2 des Klartextes mit den Bits eines Schlüsselstroms 3 einzeln mit Hilfe eines XOR-Gatters 4 verknüpft werden. Der Erzeugung des Schlüsselstroms 3 dient ein Codegenerator 5, der an Hand der Fig. 3 bis 6 noch näher beschrieben werden wird. Der Codegenerator 5 erzeugt den Schlüsselstrom 3 auf Grundlage der Bitfolgen 6 und 7, die dem Codegenerator 5 als Initialwert und Schlüssel zugeführt werden. Eine erste Bitfolge 6 wird von einem Zufallszahlengenerator 9 für jedes Datenpaket 1 erzeugt. Zu diesem Zweck ist ein Paketdetektor 38 vorgesehen, der ein eintreffendes Datenpaket 1 detektiert und zum Zeitpunkt der Paketdetektion ein Triggersignal 39 erzeugt, das dem Zufallszahlengenerator 9 zugeführt wird. Der Zeitpunkt des Eintreffens eines Datenpakets 1 stellt hierbei ein zufälliges Ereignis dar, das sicherstellt, dass der Zufallszahlengenerator 9 tatsächlich nicht-deterministisch arbeitet. Die zweite Bitfolge 7 ist in einem Speicher 10 gespeichert. Auf Grund der Verwendung der zweiten Bitfolge 7 als Schlüssel für die Erzeugung des Schlüsselstroms 3 wird sichergestellt, dass nur der Empfänger, dem ebenfalls die Bitfolge 7 bekannt sein muss, die verschlüsselten Datenpakete entschlüsseln kann.

Die verschlüsselten Daten des Datenpakets werden nun Datenpaketverarbeitungsmitteln 15 zugeführt, mit denen der

Zufallszahlengenerator 9 derart zusammenwirkt, dass die erste Bitfolge 6 dem verschlüsselten Datenpaket im Klartext hinzugefügt wird. Die zweite Bitfolge 7 hingegen wird dem verschlüsselten Datenpaket nicht hinzugefügt, sondern stellt geheime Schlüssel dar, die nur dem Sender und dem Empfänger bekannt sind. Die Datenpaketverarbeitungsmittel 15 sorgen weiters dafür, dass das verschlüsselte Datenpaket mit den üblichen Kopfdaten versehen wird, die für die paketvermittelte Übertragung in einem Computernetzwerk erforderlich sind. Das für die Versendung vorbereitete Datenpaket besteht somit aus Kopfdaten 16, der ersten Bitfolge als Paketkennung 17 und den verschlüsselten Nutzdaten 18. Die Datenübertragungsmittel zum paketvermittelten Versenden des Datenpakets sind mit 19 bezeichnet.

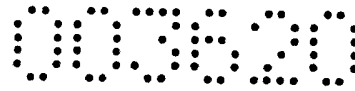
Die in Fig. 2 dargestellte Vorrichtung zum Entschlüsseln der verschlüsselten Datenpakete ist im Wesentlichen analog aufgebaut. Das die Kopfdaten 16, die erste Bitfolge als Paketkennung 17 und die verschlüsselten Nutzdaten 18 enthaltende Paket wird beim Eintreffen Auslesemitteln 20 zugeführt, in denen die erste Bitfolge 17 ausgelesen und einem Speicher 21 zugeführt wird. Die verschlüsselten Nutzdaten 18 werden in der Folge einem XOR-Gatter 22 zugeführt, in dem die Bits des verschlüsselten Bitstroms 23 und die Bits des Schlüsselstroms 3 miteinander verknüpft werden, um auf diese Weise das entschlüsselte Datenpaket 1 zu erhalten.

Der Schlüsselstrom 3, der für die Entschlüsselung eines bestimmten Datenpakets verwendet wird, muss der gleiche sein wie der Schlüsselstrom, der für die Verschlüsselung dieses Datenpakets verwendet wurde. Zu diesem Zweck werden



dieselben Bitfolgen 6 und 7 dem Generator 5 als Schlüssel zugeführt und der für die Entschlüsselung verwendete Generator 5 ist baugleich mit dem für die Verschlüsselung verwendeten Generator 5. Der Speicher für die zweite Bitfolge 7 ist mit 24 bezeichnet.

Fig. 3 zeigt eine Prinzipschaltung eines Schlüsselstromgenerators 5 mit einem Schieberegister 27, das aus einer Mehrzahl von zu einer codeproduzierenden Reihe zusammengeschalteten Speicherelementen, nämlich Flip-Flops FF1, FF2, ... FF9 besteht. Ein XOR-Gatter XORp1 ist so verschaltet, dass der eine Eingang des XOR-Gatters XORp1 mit dem Ausgang des in der codeproduzierenden Reihe befindlichen Speicherelements FF2 und der andere Eingang des XOR-Gatters XORp1 mit dem Ausgang des in der codeproduzierenden Reihe befindlichen Speicherelements FF5 und der Ausgang der XOR-Gatters XORp1 mit dem Eingang des in Flussrichtung dem mit dem einen Eingang des XOR-Gatters XORp1 verbundenen Speicherelements FF2 in der Reihe nachfolgenden Speicherelements FF3 - sohin rekursiv - verbunden ist. Weiters ist ersichtlich, dass das letzte Speicherelement FF9 über einen Inverter INV mit dem ersten Speicherelement FF1 verbunden ist. Sobald man das Schieberegister 27 mit einer Bitfolge befüllt, erhält man mit dieser Schaltung eine Codesequenz. Wenn, wie dies bei der Ausbildung gemäß Fig. 3 der Fall ist, nur ein einziges Schieberegister zum Einsatz gelangt, werden die Bitfolgen 6 und 7 dem Schieberegister 27 derart zugeführt, dass zunächst die Bitfolgen 6 und 7 mit Hilfe eines XOR-Gatters 28 miteinander verknüpft werden. Dabei ist es bevorzugt, dass die aus den Bitfolgen 6 und 7 generierte, dem Schieberegister 27 zugeführte Bitfolge nicht länger ist als dies der Anzahl der Speicherelemente im Schieberegister 27

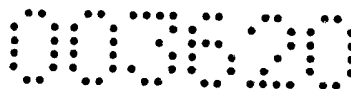


entspricht, da die Bitfolge andernfalls von der über den Inverter INV aus dem Speicherelemente FF9 kommenden Bitfolge überlagert würde.

Bei der abgewandelten Ausbildung gemäß Fig. 4 gelangen insgesamt zwei Schieberegister 30 und 31 zum Einsatz. Die Speicherelemente der einzelnen Schieberegister sind in diesem Beispiel jeweils auf gleiche Weise rekursiv verschaltet wie in Fig. 3. Die Schieberegister sind weiters derart miteinander verschaltet, dass in Abhängigkeit vom Zustand des zweiten Schieberegisters 31 die Funktion des XOR-Gatters XORp1 der rekursiven Verschaltung des ersten Schieberegisters 30 an- und abgeschaltet wird. Zu diesem Zweck ist der Ausgang des Flip-Flops FFp2 des Schieberegisters 31 mit dem Eingang eines UND-Gatters UNDp1 verbunden, das in die jeweilige rekursive Funktion XORp1 bzw. der Schieberegister 30 eingefügt ist.

Es entsteht somit ein Codegenerator 5 mit zwei Ebenen, wobei die Codegenerierung auf jeder Ebene durch Initialisieren des jeweiligen Schieberegisters 30, 31 mit der Bitfolge 6 und 7 beeinflusst wird. Die Initialisierung kann dabei bevorzugt so erfolgen, dass dem Schieberegister 30 der ersten Ebene die erste Bitfolge 6 und dem Schieberegister 31 der zweiten Ebene die zweite Bitfolge 7 zugeführt wird, wobei die Bitfolgen 6 und 7 bevorzugt so definiert sind wie in den Fig. 1 und 2 beschrieben.

Bei der Ausbildung gemäß Fig. 5 ist die in Fig. 4 gezeigte Struktur noch komplexer ausgestaltet und es sind insbesondere längere codeproduzierende Reihen und eine Mehrzahl von rekursiven Verschaltungen vorgesehen. Dabei ist eine Anzahl ununterbrochen in Reihe geschalteter



Speicherelemente in Form von Schieberegister SRG1, SRG2,... verwirklicht, die funktionell gesehen gemeinsam ein Schieberegister 33 im Sinne der Erfindung bilden. Es verdoppelt sich die Länge des Codes pro hinzugefügtem Speicherelement, so dass sich die Länge des Codes wie folgt berechnet

$$L_c = 2^n - 1$$

(L_c = Länge der Codesequenz; n = Anzahl der codegenerierenden in Reihe geschalteten Speicherelemente)

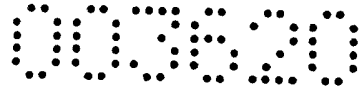
Wenn diese Einheit mit einem bestimmten Takt betrieben wird gilt für die Dauer des Codes:

$$T_c = \frac{2^n - 1}{f_c}$$

(T_c = Dauer bis sich der Code wiederholt; f_c = Codegenerierungstaktfrequenz)

Mit weniger als 50 Speicherelementen bei einer Codegenerierungstaktfrequenz von 384.000 Bit/s läuft der Code länger als ein Jahr ohne dass sich die Sequenz wiederholt, so dass ein zu verschlüsselndes Signal simultan über einen ebenso langen Zeitraum verschlüsselt über eine Standleitung übersendet und entschlüsselt werden kann, so dass Übertragungen live über einen ebenso langen Zeitraum möglich sind.

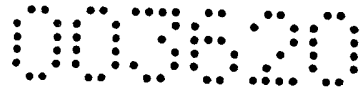
Wenn man nun bei entsprechender Länge des Schieberegisters 33 an mehreren Stellen dieses Schieberegisters 33 zwischen



einem Speicherelement $FF_{1,2,3,4}$ und dem nächsten in der Reihe befindlichen Speicherelement $FF_{2,3,4,5}$ ein XOR-Gatter $XOR_{p1,p2,p3,p4}$ einfügt und dieses dann mit dem Signal von einem dritten Speicherelement $FF_{8,15,20,23}$ speist, so verändert man jeweils den dadurch erzeugten Code (Fig. 5).

Bei einer Mehrzahl von codeverändernden XOR-Gattern $XOR_{p1,p2,p3,p4}$, siehe Fig. 5, soll sichergestellt sein, dass die verschiedenen codeverändernden XOR-Gatter $XOR_{p1,p2,p3,p4}$, deren erster Eingang von einem Ausgang eines Speicherelements $FF_{1,2,3,4}$ gespeist wird, ihren zweiten Eingang jeweils vom Ausgang eines Speicherelements $FF_{8,15,20,23}$ gespeist erhalten, welches eine Anzahl von Speicherelementen in Flussrichtung vom erstgenannten Speicherelement $FF_{1,2,3,4}$ entfernt ist, welche jeweils einer unterschiedlichen Primzahl entspricht, die größer als 1 aber kein Teilbetrag der Gesamtzahl der in Reihe R geschalteten Speicherelemente ist, sodass es bei der Beeinflussung der Codesequenz zu keinen codesequenzverkürzenden Resonanzeffekten kommt. Zwischen den entsprechenden Speicherelementpaaren $FF_{1,8}$; $FF_{2,15}$; $FF_{3,20}$; $FF_{4,23}$ liegt also jeweils eine Anzahl von 7, 13, 17 und 19 (Primzahlen) Speicherelementen.

Wenn man an einen der beiden Eingänge des jeweiligen XOR-Gatters XOR_{p1} bzw. $XOR_{p1,p2,p3,p4}$ den Ausgang eines UND-Gatters UND_{p1} bzw. $UND_{p1,p2,p3,p4}$ dessen einer Eingang am Ausgang des Speicherelements FF_3 bzw. $FF_{8,15,20,23}$ hängt, anschließt, dann kann man dieses XOR-Gatter XOR_{p1} bzw. $XOR_{p1,p2,p3,p4}$ in seiner codeverändernden Wirkung über den zweiten Eingang des UND-Gatters UND_{p1} bzw. $UND_{p1,p2,p3,p4}$ an- und abschalten und wenn man daran jeweils ein weiteres Speicherelement FF_{p1} bzw. $FF_{p1,p2,p3,p4}$ anschließt, das An-



und Abschalten der codebeeinflussenden Wirkung des XOR-Gatters XORp1 bzw. XORp1,p2,p3,p4 programmierbar machen. Die codeprogrammierenden Speicherelemente FFp1,p2,p3,p4 können dabei zu einem Schieberegister 34 zusammengeschaltet sein. In weiterer Folge können die codeprogrammierenden Speicherelemente FFp1,p2,p3,p4 des Schieberegisters 34 selbst wiederum mit Hilfe eines XOR-Gatters XORpp1 rekursiv verschaltet werden.

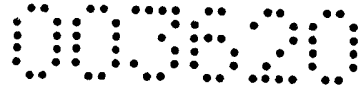
In Fig. 6 ist nun der nicht-deterministische Zufallszahlengenerator 9 dargestellt. Der Zufallszahlengenerator umfasst einen Codegenerator 40, der eine pseudozufällige Zeichenfolge 41 generiert. Der Codegenerator 40 kann grundsätzlich beliebig ausgestaltet sein. Bevorzugt handelt es sich um einen Codegenerator wie anhand von Fig. 3, 4 oder 5 bzw. in der WO 03/075507 A1 beschrieben. Die pseudozufällige Zeichenfolge 41 wird ununterbrochen in den Ringpuffer 42 geschrieben. Dem Ringpuffer 42 ist ein Controller 43 zugeordnet, der das Auslesen einer Zufallszeichenfolge 44 veranlasst. Zu diesem Zweck ist dem Controller ein von dem Paketdetektor 38 generiertes Triggersignal 39 zugeführt, das den Controller 43 veranlasst, einen Gateöffnungsbefehl 45 an den Ringpuffer 42 zu senden, worauf die Zufallszeichenfolge 44 ausgelesen wird. Die Zufallszeichenfolge 44 hat hierbei nicht-deterministischen Charakter, weil die Frequenz der Triggersignale 39 vom Zufall bestimmt ist. Aus dem Ringpuffer 42 wird somit diejenige Teilsequenz 44 ausgelesen, die sich zum Zeitpunkt des Triggersignals 39 bzw. des Gateöffnungsbefehls 45 zufällig im Ringpuffer 42 befindet, wobei die Speicherkapazität des Ringpuffers 42 wesentlich größer ist als die Länge der aus dem Ringpuffer 42 ausgelesenen Zufallszeichenfolge 44. Der Controller 43

gibt die Zufallszeichenfolge 44 als binäre Zufallszahl aus,
die als erste Bitfolge 6 dem Codegenerator 5 als Schlüssel
zugeführt wird, um diesen zu initialisieren.

Patentansprüche:

1. Verfahren zur Durchführung einer symmetrischen Stromverschlüsselung von Daten unter Verwendung eines Schlüsselstroms und zur Übertragung der verschlüsselten Daten, wobei die Generierung des Schlüsselstroms unter Verwendung wenigstens eines rückgekoppelten Schieberegisters erfolgt, das zu seiner Initialisierung mit einer definierten Bitfolge gefüllt wird, wobei die zu verschlüsselnden Daten in Datenpakete aufgeteilt werden und jedes Datenpaket gesondert verschlüsselt wird, wobei das bzw. die rückgekoppelte(n) Schieberegister für die Verschlüsselung jedes Datenpakets neu initialisiert wird bzw. werden, wobei zur Initialisierung des bzw. der rückgekoppelten Schieberegister jeweils wenigstens eine erste Bitfolge und eine zweite Bitfolge verwendet wird, wobei die erste Bitfolge dem jeweils verschlüsselten Datenpaket im Klartext oder in codierter Form hinzugefügt wird und die zweite Bitfolge einen geheimen Schlüssel darstellt, die den verschlüsselten Datenpaketen nicht hinzugefügt wird, und wobei die verschlüsselten Datenpakete samt der jeweiligen hinzugefügten Bitfolge und ggf. Kopfdaten paketvermittelt übertragen werden, dadurch gekennzeichnet, dass die erste Bitfolge unter Verwendung eines nichtdeterministischen Zufallszahlengenerators generiert wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass der nichtdeterministische Zufallszahlengenerator einen Pseudozufallsgenerator umfasst, der eine pseudozufällige Zeichenfolge generiert, aus welcher zu zufälligen Zeitpunkten jeweils ein Teilabschnitt genommen und als erste Bitfolge verwendet wird.



3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass die pseudozufällige Zeichenfolge in einen Ringpuffer geschrieben wird und die erste Bitfolge aus dem Ringpuffer ausgelesen wird.
4. Verfahren nach Anspruch 3, dadurch gekennzeichnet, dass der Ringpuffer eine Speicherkapazität aufweist, die einem Vielfachen der Länge der ersten Bitfolge entspricht.
5. Verfahren nach Anspruch 2, 3 oder 4, dadurch gekennzeichnet, dass als zufälliger Zeitpunkt der Zeitpunkt des Eintreffens bzw. Detektierens eines zu verschlüsselnden Datenpakets gewählt wird.
6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass wenigstens ein erstes rückgekoppeltes Schieberegister zu seiner Initialisierung mit der ersten Bitfolge gefüllt wird und wenigstens ein zweites rückgekoppeltes Schieberegister zu seiner Initialisierung mit der zweiten Bitfolge gefüllt wird.
7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, dass die Generierung des Schlüsselstroms beginnt, sobald alle rückgekoppelten Schieberegister mit jeweiligen Bitfolgen gefüllt sind.
8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass wenigstens zwei rückgekoppelte Schieberegister gleichzeitig mit der jeweiligen Bitfolge gefüllt werden.
9. Verfahren nach einem der Ansprüche 1 bis 8, dadurch

gekennzeichnet, dass zur Rückkoppelung des bzw. der Schieberegister wenigstens ein XOR-Gatter verwendet wird.

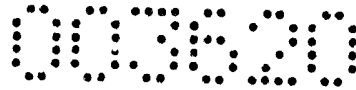
10. Verfahren nach einem der Ansprüche 1 bis 9, dadurch gekennzeichnet, dass die rückgekoppelten Schieberegister derart miteinander verschaltet sind, dass in Abhängigkeit vom Zustand des einen Schieberegisters das wenigstens eine XOR-Gatter des anderen Schieberegister an- oder abgeschaltet wird.

11. Verfahren nach einem der Ansprüche 1 bis 10, dadurch gekennzeichnet, dass das wenigstens eine rückgekoppelte Schieberegister eine Mehrzahl von zu einer codeproduzierenden Reihe geschalteten Speicherelementen aufweist, wobei der Ausgang des in der Reihe letzten Speicherelements mit dem Eingang des in der Reihe ersten Speicherelements zu einem Kreis zusammengeschlossen ist, wobei die Rückkoppelung mit Hilfe des wenigstens einen XOR-Gatters derart erfolgt, dass der erste Eingang des XOR-Gatters mit dem Ausgang eines in der codeproduzierenden Reihe befindlichen Speicherelements, der zweite Eingang mit dem Ausgang eines weiteren in der codeproduzierenden Reihe befindlichen Speicherelements und der Ausgang mit dem Eingang des in der codeproduzierenden Reihe dem mit dem ersten Eingang des XOR-Gatters verbundenen Speicherelement nachfolgenden Speicherelements verbunden ist.

12. Verfahren nach Anspruch 11, dadurch gekennzeichnet, dass in die den zweiten Eingang des wenigstens einen XOR-Gatters und den Ausgang des weiteren in der codeproduzierenden Reihe befindlichen Speicherelements verbindende Leitung ein UND-Gatter derart geschaltet ist, dass der Ausgang des UND-Gatters mit dem zweiten Eingang

des XOR-Gatters, der erste Eingang des UND-Gatters mit dem Ausgang des weiteren in der codeproduzierenden Reihe befindlichen Speicherelements und der zweite Eingang des UND-Gatters mit dem Ausgang eines codeprogrammierenden Speicherelements verbunden ist, wobei als codeprogrammierendes Speicherelement ein Speicherelement eines weiteren rückgekoppelten Schieberegisters verwendet wird, und dass bevorzugt der Ausgang eines in der codeproduzierenden Reihe befindlichen Speicherelements mit dem Eingang eines Inverters und der Ausgang des Inverters mit dem Eingang eines anderen in der codeproduzierenden Reihe angeordneten Speicherelements verbunden ist.

13. Vorrichtung zum Verschlüsseln von Daten mit Hilfe einer symmetrischen Stromverschlüsselung unter Verwendung eines Schlüsselstroms (3), insbesondere zur Durchführung des Verfahrens nach einem der Ansprüche 1 bis 12, wobei zur Generierung des Schlüsselstroms (3) wenigstens ein rückgekoppeltes Schieberegister (27; 30,31; 33,34) vorgesehen ist, das zu seiner Initialisierung jeweils mit einer definierten Bitfolge gefüllt wird, wobei die Daten in Datenpakete (1) aufgeteilt vorliegen, wobei Mittel (9,10) zum Speichern wenigstens einer ersten Bitfolge (6) und einer zweiten Bitfolge (7) vorgesehen sind, die mit dem bzw. den Schieberegister(n) (27; 30,31; 33,34) derart zusammenwirken, dass wenigstens die erste Bitfolge (6) und die zweite Bitfolge (7) zur Initialisierung des bzw. der rückgekoppelten Schieberegister (27; 30,31; 33,34) verwendet werden, wobei das bzw. die rückgekoppelte(n) Schieberegister (27; 30,31; 33,34) für die Verschlüsselung jedes Datenpakets (1) neu initialisiert wird bzw. werden, wobei Datenpaketverarbeitungsmittel (15) vorgesehen sind, mit denen die Mittel (9,10) zum Speichern der ersten (6)

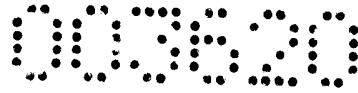


und der zweiten (7) Bitfolge derart zusammenwirken, dass die erste Bitfolge (6) dem jeweils verschlüsselten Datenpaket im Klartext (17) oder in codierter Form hinzugefügt wird und die zweite Bitfolge (7) einen geheimen Schlüssel darstellt, die den verschlüsselten Datenpaketen nicht hinzugefügt wird, und wobei Datenübertragungsmittel (19) zum paketvermittelten Versenden der verschlüsselten Datenpakete samt der jeweiligen hinzugefügten Bitfolge (17) und ggf. Kopfdaten (16) vorgesehen sind, dadurch gekennzeichnet, dass die Mittel zum Generieren der ersten Bitfolge einen nichtdeterministischen Zufallszahlengenerator (9) umfassen.

14. Vorrichtung nach Anspruch 13, dadurch gekennzeichnet, dass der nichtdeterministische Zufallszahlengenerator (9) einen Pseudozufallsgenerator (40) umfasst, der eine pseudozufällige Zeichenfolge (41) generiert, wobei Mittel zum Detektieren eines zufälligen Ereignisses vorgesehen sind, die mit der pseudozufälligen Zeichenfolge (41) derart zusammenwirken, dass bei Detektion des zufälligen Ereignisses jeweils ein Teilabschnitt (44) aus der pseudozufälligen Zeichenfolge genommen und als erste Bitfolge (6) verwendet wird.

15. Vorrichtung nach Anspruch 14, dadurch gekennzeichnet, dass ein mit dem Pseudozufallsgenerator (40) verbundener Ringpuffer (42) vorgesehen ist, um die pseudozufällige Zeichenfolge (41) in den Ringpuffer (42) zu schreiben und dass Mittel zum Auslesen der ersten Bitfolge aus dem Ringpuffer vorgesehen sind.

16. Vorrichtung nach Anspruch 15, dadurch gekennzeichnet, dass der Ringpuffer (42) eine Speicherkapazität aufweist,



die einem Vielfachen der Länge der ersten Bitfolge (6) entspricht.

17. Vorrichtung nach Anspruch 14, 15 oder 16, dadurch gekennzeichnet, dass die Mittel zum Detektieren eines zufälligen Ereignisses von einem Datenpaketdetektor (38) gebildet sind, der den Zeitpunkt des Eintreffens eines zu verschlüsselnden Datenpakets (1) detektiert.

18. Vorrichtung nach einem der Ansprüche 13 bis 17, dadurch gekennzeichnet, dass die Mittel (9,10; 20,21,24) zum Speichern bzw. Auslesen der ersten (6) und der zweiten (7) Bitfolge mit einem XOR-Gatter (28) derart zusammenwirken, dass die erste Bitfolge (6) und die zweite Bitfolge (7) mit Hilfe einer XOR-Funktion verknüpft werden, wobei die sich aus der Verknüpfung ergebende Bitfolge zur Initialisierung dem rückgekoppelten Schieberegister (27) zugeführt ist.

19. Vorrichtung nach einem der Ansprüche 13 bis 18, dadurch gekennzeichnet, dass die erste Bitfolge (6) wenigstens einem ersten rückgekoppelten Schieberegister (30;33) zu dessen Initialisierung zugeführt ist und die zweite Bitfolge (7) wenigstens einem zweiten rückgekoppelten Schieberegister (31;34) zu dessen Initialisierung zugeführt ist.

20. Vorrichtung nach einem der Ansprüche 13 bis 19, dadurch gekennzeichnet, dass die Generierung des Schlüsselstroms (3) beginnt, sobald alle rückgekoppelten Schieberegister (27; 30,31; 33,34) mit der jeweiligen Bitfolge gefüllt sind.

21. Vorrichtung nach einem der Ansprüche 13 bis 20, dadurch gekennzeichnet, dass wenigstens zwei rückgekoppelte Schieberegister (30,31; 33,34) gleichzeitig mit der jeweiligen Bitfolgen gefüllt werden.

22. Vorrichtung nach einem der Ansprüche 13 bis 21, dadurch gekennzeichnet, dass zur Rückkoppelung des bzw. der Schieberegister (27; 30,31; 33,34) wenigstens ein XOR-Gatter (XORp1, XORp2, XORp3, XORp4, XORpp1, XORppp1) eingesetzt ist.

23. Vorrichtung nach einem der Ansprüche 13 bis 22, dadurch gekennzeichnet, dass die rückgekoppelten Schieberegister (30,31; 33,34) derart miteinander verschaltet sind, dass in Abhängigkeit vom Zustand des einen Schieberegisters das wenigstens eine XOR-Gatter (XORp1, XORp2, XORp3, XORp4, XORpp1) des anderen Schieberegister an- oder abgeschaltet wird.

24. Vorrichtung nach einem der Ansprüche 12 bis 23, dadurch gekennzeichnet, dass das wenigstens eine rückgekoppelte Schieberegister (30,31; 33,34) eine Mehrzahl von zu einer codeproduzierenden Reihe geschalteten Speicherelementen (FF1, FF2,...; FFp1, FFp2,...) aufweist, wobei der Ausgang des in der Reihe letzten Speicherelements mit dem Eingang des in der Reihe ersten Speicherelements zu einem Kreis zusammengeschlossen ist, wobei die Rückkoppelung mit Hilfe des wenigstens einen XOR-Gatters (XORp1, XORp2, XORp3, XORp4, XORpp1) derart erfolgt, dass der erste Eingang des XOR-Gatters mit dem Ausgang eines in der codeproduzierenden Reihe befindlichen Speicherelements (FF2), der zweite Eingang mit dem Ausgang eines weiteren in der codeproduzierenden Reihe befindlichen Speicherelements

(FF5) und der Ausgang mit dem Eingang des in der codeproduzierenden Reihe dem mit dem ersten Eingang des XOR-Gatters verbundenen Speicherelement nachfolgenden Speicherelements (FF3) verbunden ist.

25. Vorrichtung nach Anspruch 24, dadurch gekennzeichnet, dass in die den zweiten Eingang des wenigstens einen XOR-Gatters (XORp1) und den Ausgang des weiteren in der codeproduzierenden Reihe (30;33) befindlichen Speicherelements (FF5) verbindende Leitung ein UND-Gatter (UNDp1) derart geschaltet ist, dass der Ausgang des UND-Gatters (UNDp1) mit dem zweiten Eingang des XOR-Gatters (XORp1), der erste Eingang des UND-Gatters (UNDp1) mit dem Ausgang des weiteren in der codeproduzierenden Reihe (30;33) befindlichen Speicherelements (FF5) und der zweite Eingang des UND-Gatters (UNDp1) mit dem Ausgang eines codeprogrammierenden Speicherelements (FFp2) verbunden ist und dass bevorzugt der Ausgang eines in der codeproduzierenden Reihe (30;33) befindlichen Speicherelements (FF9) mit dem Eingang eines Inverters (INV) und der Ausgang des Inverters (INV) mit dem Eingang eines anderen in der codeproduzierenden Reihe (30;33) angeordneten Speicherelements (FF1) verbunden ist, wobei als codeprogrammierendes Speicherelement ein Speicherelement eines weiteren rückgekoppelten Schieberegisters (31;34) verwendet wird.

26. Vorrichtung nach Anspruch 24 oder 25, dadurch gekennzeichnet, dass eine Mehrzahl von XOR-Gattern (XORp1,p2,p3,p4) vorgesehen ist, deren erster Eingang jeweils von einem Ausgang eines in der codeproduzierenden Reihe (30;33) befindlichen Speicherelements (FF1,2,3,4) gespeist wird und deren zweiter Eingang jeweils vom Ausgang

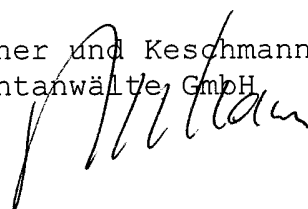
eines weiteren in der codeproduzierenden Reihe (30;33) befindlichen Speicherelements (FF8,15,20,23) gespeist wird, welches eine Anzahl von Speicherelementen in Flussrichtung der Reihe (30;33) von dem jeweils mit dem ersten Eingang verbundenen Speicherelement (FF1,2,3,4) entfernt ist, welche jeweils einer unterschiedlichen Primzahl entspricht, die größer als 1 und kein Teilbetrag der Gesamtzahl der in Reihe (30;33) geschalteten Speicherelemente (FF1,2,...n) ist.

27. Vorrichtung nach einem der Ansprüche 24 bis 26, dadurch gekennzeichnet, dass eine Mehrzahl von codeprogrammierenden, jeweils einem UND-Gatter (UNDp1,p2,p3,p4) und einem XOR-Gatter (XORp1,p2,p3,p4) zugeordneten Speicherelementen (FFp1,p2,p3,p4,...pn) vorgesehen und in einer zu einem Kreis geschlossenen Reihe (31;34) geschaltet ist und wenigstens ein XOR-Gatter (XORpp1) angeordnet ist, dessen erster Eingang mit dem Ausgang eines in der codeprogrammierenden Reihe (31;34) befindlichen Speicherelements (FFp6), dessen zweiter Eingang mit dem Ausgang eines weiteren in der codeprogrammierenden Reihe (31;34) befindlichen Speicherelements (FFp5) und dessen Ausgang mit dem Eingang des in der codeprogrammierenden Reihe (31;34) dem mit dem ersten Eingang des XOR-Gatters (XORpp1) verbundenen Speicherelement (FFp6) nachfolgenden Speicherelements (FFp1) verbunden ist.

Wien, am 20. Mai 2014

Anmelder
durch:

Haffner und Keschmann
Patentanwälte GmbH



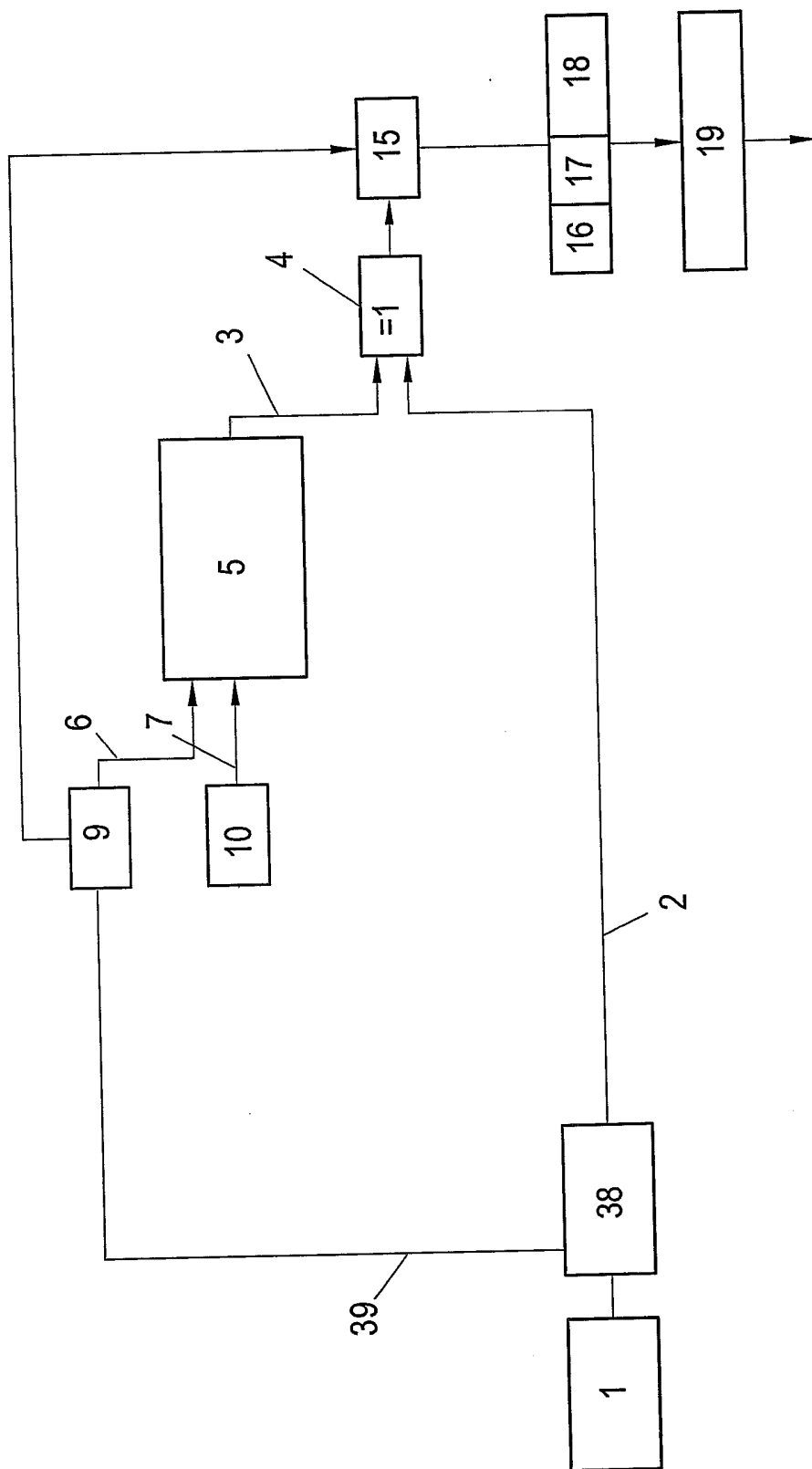


Fig. 1

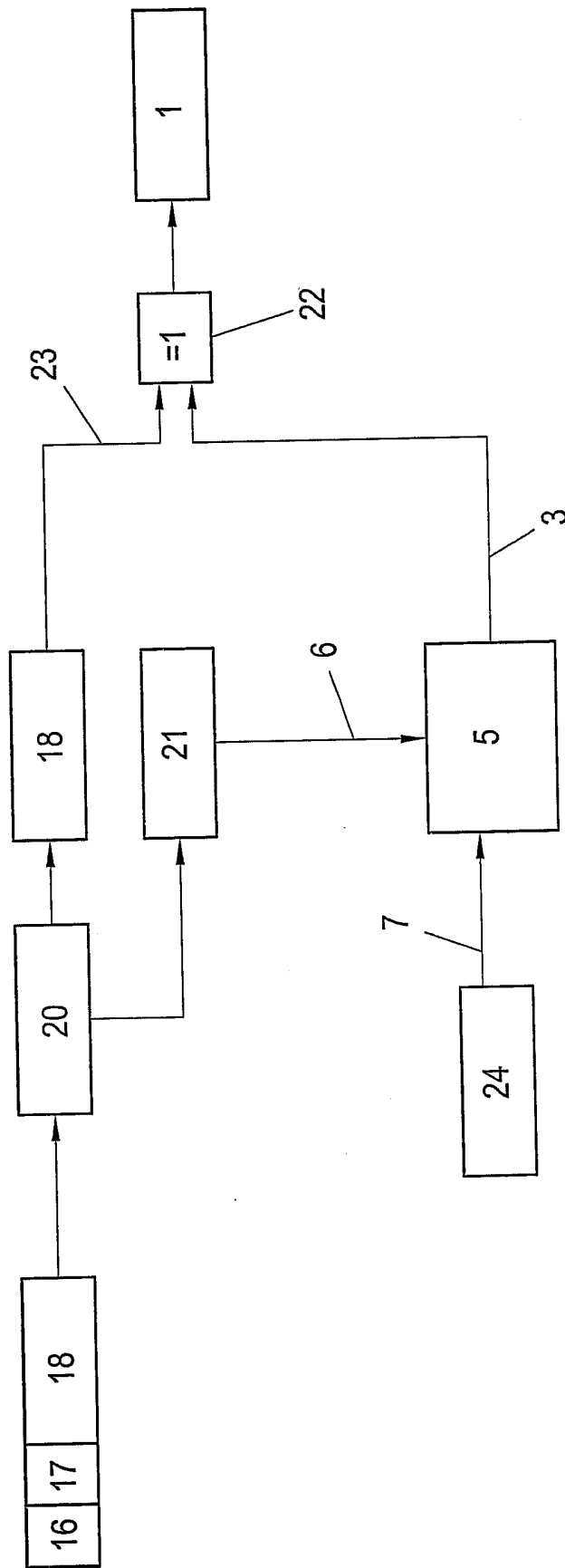


Fig. 2

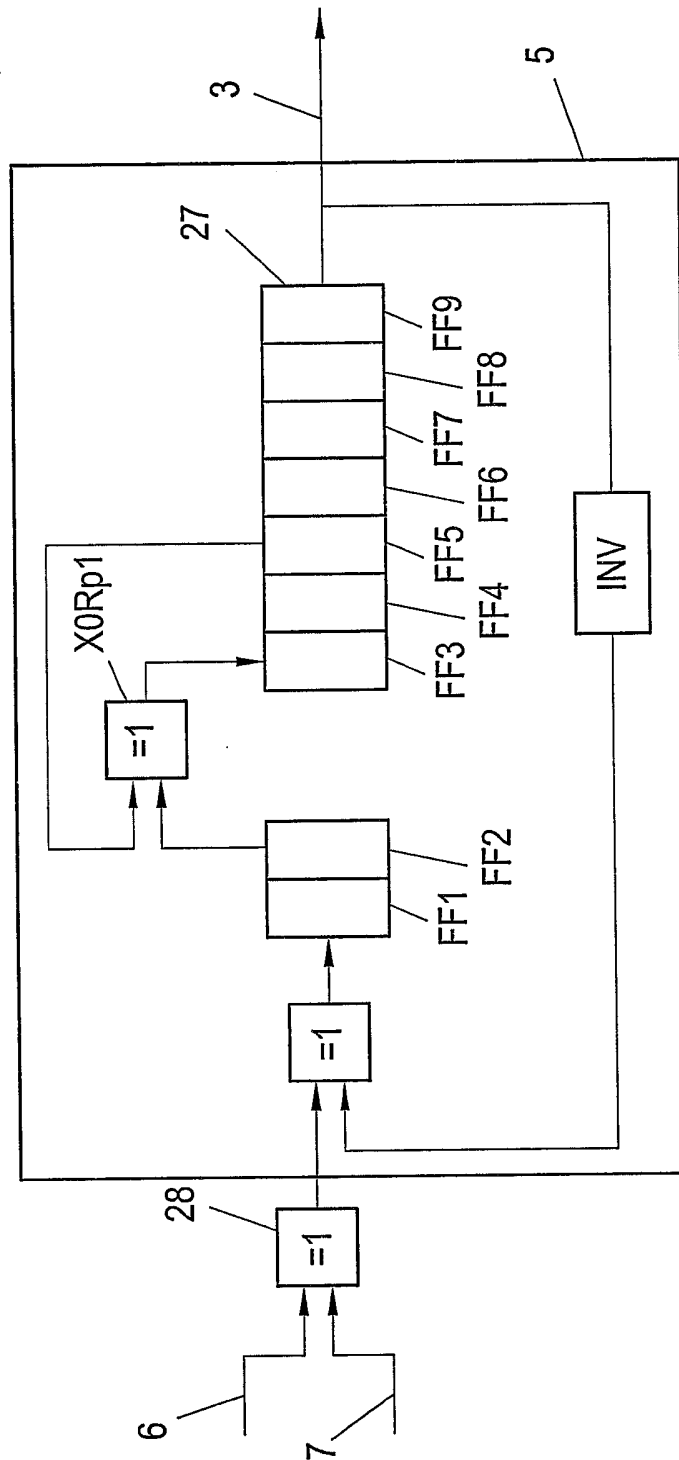


Fig. 3

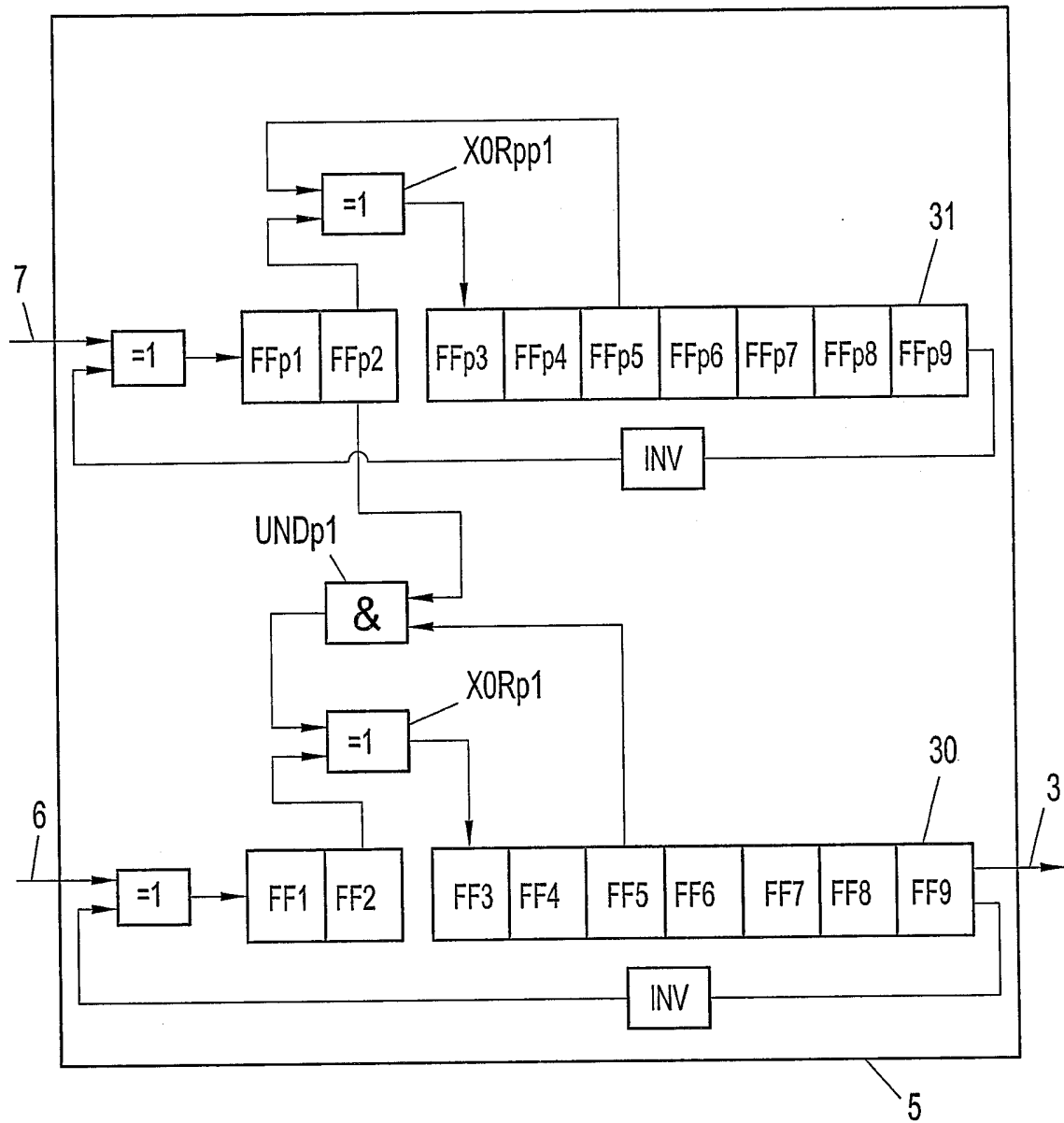


Fig. 4

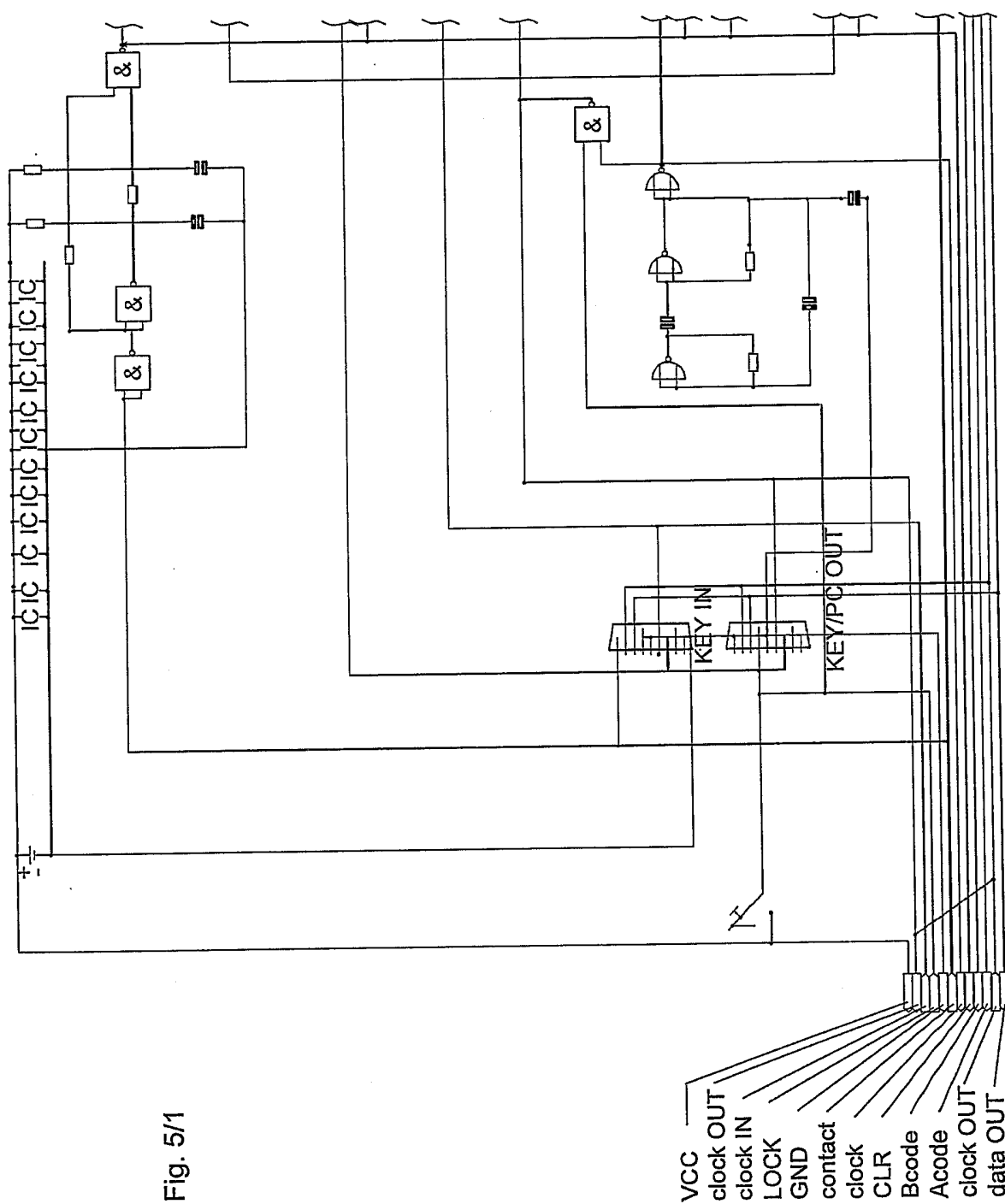
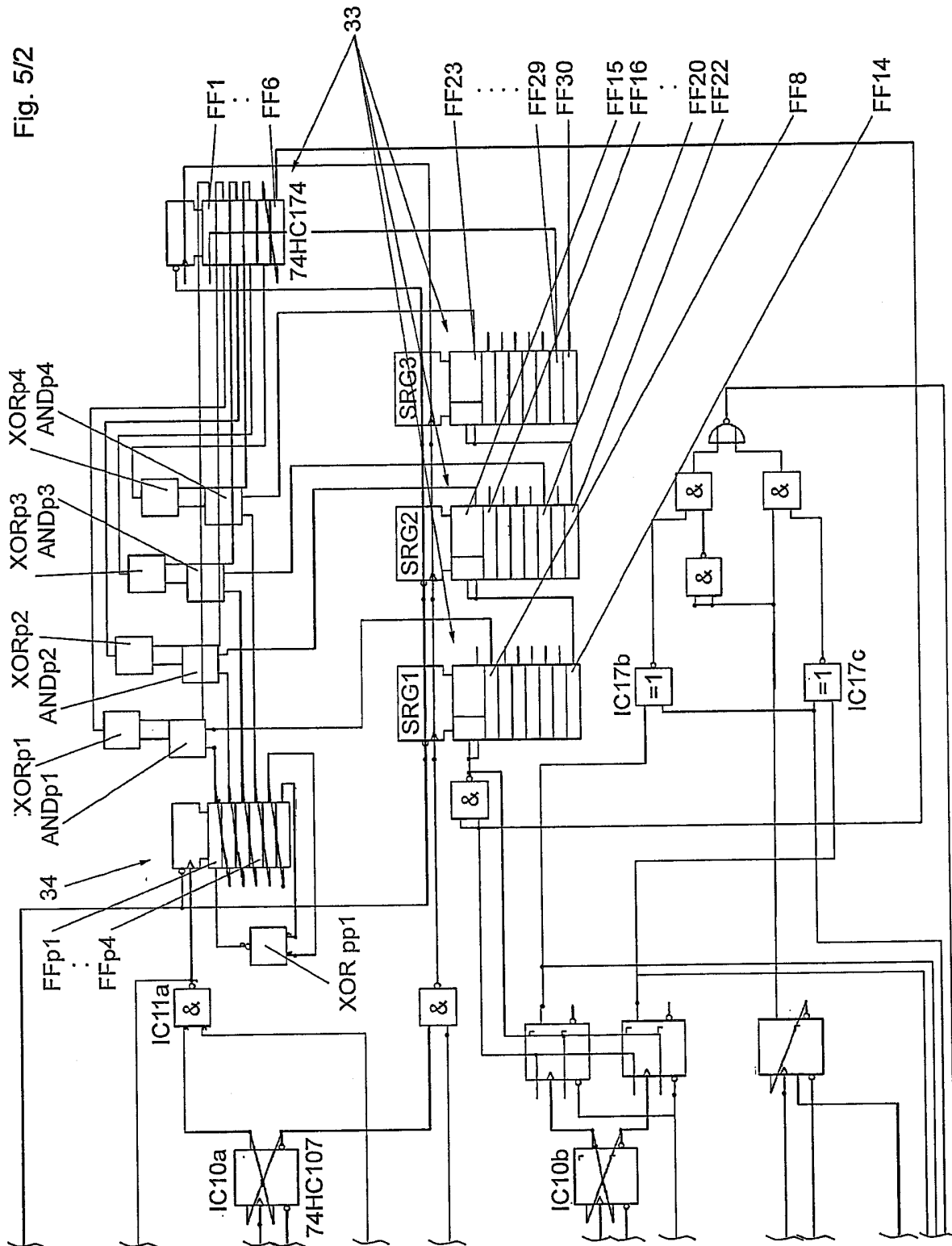


Fig. 5/2



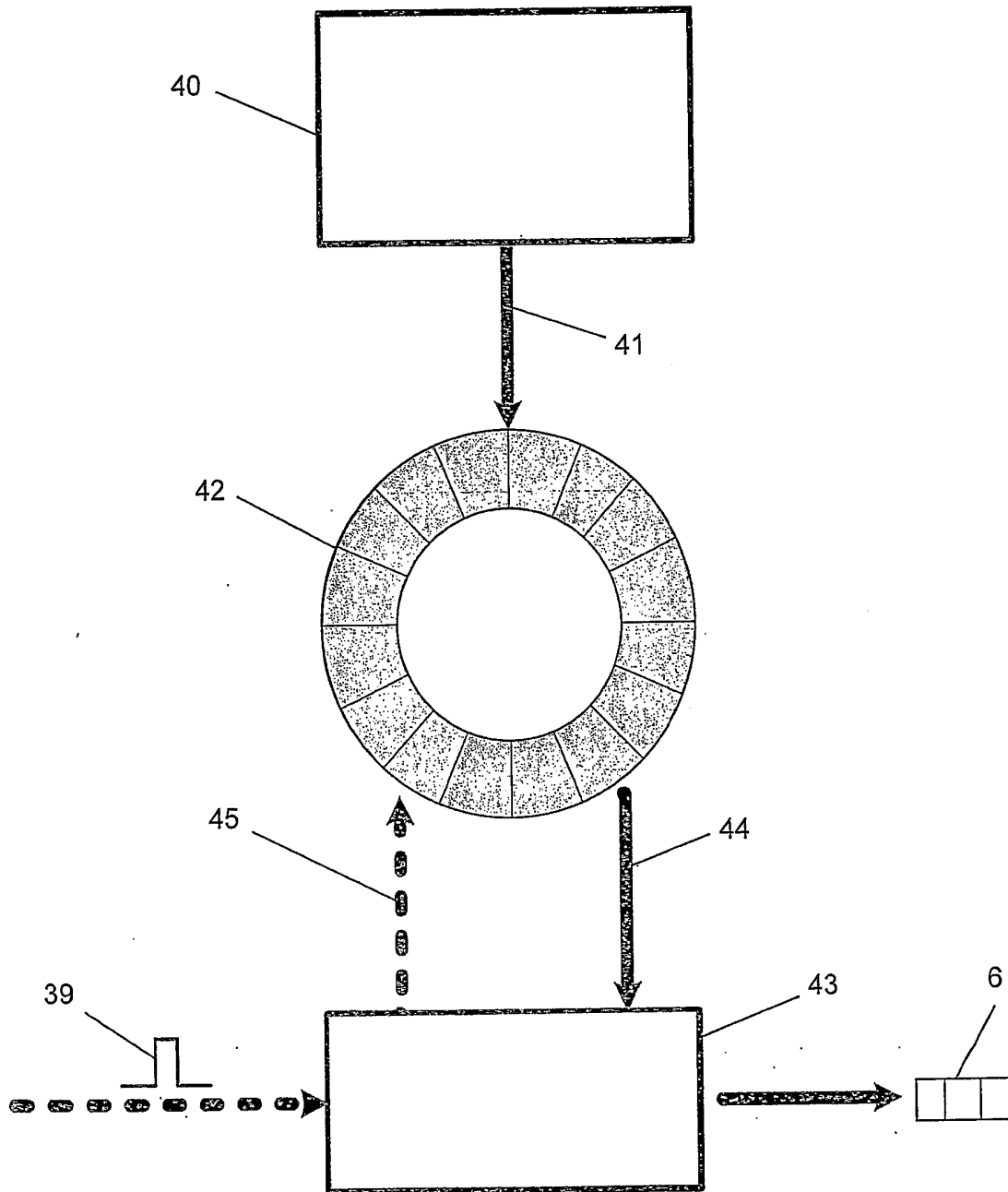


Fig. 6

Klassifikation des Anmeldungsgegenstands gemäß IPC:

H04L 9/06 (2006.01); **H04L 9/12** (2006.01); **G06F 7/58** (2006.01); **H04L 29/06** (2006.01)

Klassifikation des Anmeldungsgegenstands gemäß CPC:

H04L 9/0668 (2013.01); **H04L 9/12** (2013.01); **G06F 7/584** (2013.01); **G06F 7/588** (2013.01);
H04L 63/0457 (2013.01); **H04L 2209/12** (2013.01); **H04L 2463/121** (2013.01)

Recherchierter Prüfstoff (Klassifikation):

H04L, G06F

Konsultierte Online-Datenbank:

WPI, EPODOC, IEEEExplore

Dieser Recherchenbericht wurde zu den am **20.05.2014** eingereichten Ansprüchen **1-27** erstellt.

Kategorie ¹⁾	Bezeichnung der Veröffentlichung: Ländercode, Veröffentlichungsnummer, Dokumentart (Anmelder), Veröffentlichungsdatum, Textstelle oder Figur soweit erforderlich	Betreffend Anspruch
X	AT 510730 B1 (CORDES) 15. Juni 2013 (15.06.2013) Gesamtes Dokument.	1-27
A	EP 0615361 A1 (HUGHES AIRCRAFT) 14. September 1994 (14.09.1994) Figuren; Zusammenfassung.	1-27
A	US 5859912 A (HERSHEY et al.) 12. Jänner 1999 (12.01.1999) Figuren; Zusammenfassung.	1-27
A	WO 03075507 A1 (CORDES) 12. September 2003 (12.09.2003) Figuren; Zusammenfassung.	1-27
A	WO 2007059558 A1 (UNIVERSITY OF SYDNEY) 31. Mai 2007 (31.05.2007) Figuren; Zusammenfassung.	1-27

Datum der Beendigung der Recherche:
12.05.2015

Seite 1 von 1

Prüfer(in):

MESA PASCASIO Johannes

¹⁾ Kategorien der angeführten Dokumente:

- X** Veröffentlichung **von besonderer Bedeutung**: der Anmeldungsgegenstand kann allein aufgrund dieser Druckschrift nicht als neu bzw. auf erfinderischer Tätigkeit beruhend betrachtet werden.
- Y** Veröffentlichung **von Bedeutung**: der Anmeldungsgegenstand kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren weiteren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese **Verbindung für einen Fachmann naheliegend** ist.

- A** Veröffentlichung, die den allgemeinen **Stand der Technik** definiert.
- P** Dokument, das von **Bedeutung** ist (Kategorien **X** oder **Y**), jedoch **nach dem Prioritätstag** der Anmeldung veröffentlicht wurde.
- E** Dokument, das **von besonderer Bedeutung** ist (Kategorie **X**), aus dem ein „**älteres Recht**“ hervorgehen könnte (früheres Anmeldedatum, jedoch nachveröffentlicht, Schutz ist in Österreich möglich, würde Neuheit in Frage stellen).
- &** Veröffentlichung, die Mitglied der selben **Patentfamilie** ist.