CH 693 252 A5

(19) SCHWEIZERISCHE EIDGENOSSENSCHAFT
EIDGENÖSSISCHES INSTITUT FÜR GEISTIGES EIGENTUM

(11) CH 693 252 A5

(51) Int. Cl.[7]: H 04 L 009/30

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

(12) PATENTSCHRIFT A5

(21) Gesuchsnummer: 02372/97

(22) Anmeldungsdatum: 10.10.1997

(30) Priorität: 10.10.1996 US 08/729,012

(24) Patent erteilt: 30.04.2003

(45) Patentschrift veröffentlicht: 30.04.2003

(73) Inhaber:
Certicom Corp.,
200 Matheson Boulevard, West Suite 103,
Mississauga, Ontario L5R 3L7 (CA)

(72) Erfinder:
Donald B. Johnson, 7684 Knighthayes Drive,
20111 Manassa, Virginia (US)

(74) Vertreter:
A. Braun, Braun, Héritier,
Eschmann AG Patentanwälte, Holbeinstrasse 36–38,
4051 Basel (CH)

(54) Verfahren und Vorrichtung zur Erzeugung einer ganzen Zahl.

(57) Eine ganze Zahl für einen privaten Schlüssel wird unter Verwendung eines Paars von Bestandteilen erzeugt, die auf festgelegte vorhersagbare Weise miteinander verknüpft werden. Der erste Bestandteil wird von einem Sequenzer, beispielsweise einem Zähler, erzeugt, der einen sich nicht wiederholenden individuellen Wert erzeugt, und der zweite Bestandteil wird zufallsmässig erzeugt. Durch Verknüpfen der Bestandteile weist die ganze Zahl einen eindeutigen und unvorhersagbaren Wert auf.

Beschreibung

Die vorliegende Erfindung betrifft Verschlüsselungssysteme mit öffentlichem Schlüssel, insbesondere ein Verfahren und eine Vorrichtung zur Erzeugung einer ganzen Zahl zur Verwendung als privater Schlüssel in solchen Verschlüsselungssystemen.

Bei Verschlüsselungssystemen mit öffentlichem Schlüssel werden ein privater Schlüssel und ein öffentlicher Schlüssel eingesetzt, um einen sicheren Informationsaustausch herzustellen. Die Schlüssel stehen mathematisch zueinander in Beziehung, sodass mit dem einen eine Nachricht verschlüsselt und mit dem anderen die Nachricht wiederhergestellt werden kann. Bei einem typischen System kommen ein langfristiger privater Schlüssel und ein entsprechender öffentlicher Schlüssel, der in der Regel durch eine Zulassungsstelle authentifiziert wird, um den Besitzer des Schlüssels anzugeben, und ein kurzfristiger privater Schlüssel oder privater Sitzungsschlüssel mit dem entsprechenden öffentlichen Schlüssel zur Verschlüsselung einer bestimmten Nachricht zum Einsatz. Die Schlüssel können zum Verbergen des Inhalts einer Nachricht, wie bei einem Verschlüsselungsprotokoll, oder zum Authentifizieren einer Nachricht, wie bei einem digitalen Signaturprotokoll, verwendet werden.

Bei dem privaten Schlüssel handelt es sich in der Regel um eine ganze Zahl vorbestimmter Länge, und der öffentliche Schlüssel wird erhalten, indem mit einer bekannten Funktion die ganze Zahl verarbeitet wird. Bei einem fehlerfesteren der etablierten Verfahren wird ein Generator einer multiplikativen Gruppe mit der ganzen Zahl potenziert, und man verlässt sich auf die Unlösbarkeit des diskreten Logarithmusproblems, um die Vertraulichkeit der ganzen Zahl aufrechtzuerhalten. Bei einer besonders günstigen Realisierung eines derartigen Systems kann die ganze Zahl als Multiplikator eines Punktes auf einer elliptischen Kurve über einem endlichen Feld verwendet werden, wobei der resultierende Punkt als öffentlicher Schlüssel verwendet wird. Sofern das zu Grund liegende Feld eine ausreichende Grösse aufweist, wird durch diese Potenzierung sichergestellt, dass der private Schlüssel nicht aus dem öffentlichen Schlüssel hergeleitet werden kann.

Der private Schlüssel kann zwar möglicherweise nicht aus einer einzigen Untersuchung des öffentlichen Schlüssels hergeleitet werden, doch können durch die Untersuchung einer grossen Zahl von Nachrichten möglicherweise andere Angriffe eingeleitet werden. Die Wahl des privaten Schlüssels ist daher für die Sicherheit des Systems insgesamt wichtig und ist bei denjenigen Protokollen besonders wichtig, die den kurzfristigen privaten Schlüssel regelmässig aktualisieren. Jegliche Korrelation zwischen aufeinander folgenden öffentlichen Schlüsseln könnte den geheimen Schlüssel offenbaren und auf diese Weise die Übertragungen verletzbar machen.

Damit der private Schlüssel akzeptabel ist, muss er somit sowohl eindeutig als auch unvorhersagbar sein. Es wird üblicherweise angenommen, dass eine zufallsmässig erzeugte Zahl diesen Kriterien genügt, doch kann gezeigt werden, dass die gleiche ganze Zahl mit relativ hoher Wahrscheinlichkeit zufallsmässig gewählt wird, die so genannte «Geburtstagsüberraschung». Durch das Überwachen der Nachrichten kann somit ein gemeinsamer Schlüssel gewonnen werden, aus dem der private Schlüssel hergeleitet werden kann.

Eine Aufgabe der vorliegenden Erfindung besteht somit darin, ein Verfahren und eine Vorrichtung zum Wählen einer ganzen Zahl zu schaffen, die als privater Schlüssel verwendet werden kann.

Allgemein gesagt liefert die vorliegende Erfindung eine ganze Zahl, die aus zwei Bestandteilen gebildet wird. Der erst Bestandteil wird auf eindeutige Weise durch die Verwendung eines Sequenzers erzeugt, der sich bei jeder Erzeugung eines Schlüssels ändert. Der zweite Bestandteil wird zufallsmässig erzeugt, beispielsweise durch einen Zufallszahlengenerator, damit er unvorhersagbar ist. Die beiden Bestandteile werden miteinander verknüpft, um eine ganze Zahl zu ergeben, die sowohl unvorhersagbar als auch eindeutig ist.

Die beiden Bestandteile können durch Verkettung in beliebiger Reihenfolge miteinander verknüpft werden.

Es wird nunmehr eine Ausführungsform der Erfindung unter Bezugnahme auf die beiliegenden Zeichnungen nur beispielhaft beschrieben, bei denen

Fig. 1 eine schematische Darstellung eines Datenkommunikationssystems ist;

Fig. 2 eine Darstellung der ganzen Zahl ist;

Fig. 3 eine schematische Darstellung der Vorrichtung ist, die zum Erzeugen einer ganzen Zahl zur Verwendung als privater Schlüssel eingesetzt wird;

Fig. 4 eine schematische Darstellung einer zweiten Ausführungsform der Vorrichtung ist, und

Fig. 5 eine schematische Darstellung einer dritten Ausführungsform der Vorrichtung ist.

Bezug nehmend auf Fig. 1, enthält ein Datenkommunikationsnetz ein Paar Teilnehmer 12, 14, die über eine Kommunikationsverbindung 16 miteinander verbunden sind. Jeder der Teilnehmer 12, 14 hat einen privaten Schlüssel k_a bzw. k_b und einen entsprechenden, zu dem privaten Schlüssel mathematisch in Beziehung stehenden öffentlichen Schlüssel p_a bzw. p_b. In der Regel ist der private Schlüssel k ein Element in einer multiplikativen Gruppe über einem endlichen Feld und der öffentliche Schlüssel der Exponent α^k. Um eine Nachricht zu verschlüsseln, kann der Teilnehmer 12 den öffentlichen Schlüssel p_b des Teilnehmers 14 verwenden, um die Nachricht zu verschlüsseln und als Schlüsseltext über die Verbindung 16 zu übertragen. Der Teilnehmer 14 kann dann zur Wiederherstellung des Klartexts die Nachricht mit dem privaten Schlüssel k_b entschlüsseln.

Analog dazu kann eine Nachricht von dem Teilnehmer 12 unter Verwendung seines privaten Schlüssels k_a unterzeichnet und von dem Teilnehmer 14 unter Verwendung des öffentlichen Schlüssels p_a authentifiziert werden. Derartige Protokolle sind wohl bekannt und werden allgemein als öffentlicher Schlüsselaustausch nach Diffie-Hellman oder

als ElGamal-Signaturverfahren bezeichnet und brauchen hier nicht weiter beschrieben zu werden.

Um die Sicherheit der Verschlüsselung sicherzustellen und zu verhindern, dass der private Schlüssel durch eine Analyse des öffentlichen Schlüssels offen gelegt wird, sollte die ganze Zahl k eine gegebene Länge, d.h. 2n Bit, aufweisen und so gewählt sein, dass sie eindeutig und unvorhersagbar ist. Wie in den Fig. 2 und 3 gezeigt, wird die ganze Zahl k aus einem Paar von Bestandteilen G_1 bzw. G_2 gebildet, die jeweils eine Länge von n Bit haben und miteinander verknüpft werden, um eine ganze Zahl k mit den erforderlichen Eigenschaften zu liefern.

Der Bestandteil G_1 wird von einem Sequenzer erzeugt, der einen sich nicht wiederholenden, individuellen Wert über einen endlichen Bereich hinweg erzeugt. Bei der bevorzugten Ausführungsform ist dies ein n-Bit Zähler 20, der nach jeder Wahl eines neuen Schlüssels k durch ein Steuersignal 22 inkrementiert wird. Das Steuersignal 22 inkrementiert den Zähler 20 um einen festen Betrag, in der Regel einen einzelnen Zählwert, damit am Ausgang 23 eine sich nicht wiederholende, sich fortlaufend ändernde ganze Zahl bereitgestellt wird. Ausgang 23 ist mit einer Arithmetikeinheit 25 verbunden, die ein Schieberegister 24 enthält, Das Ausgangssignal des Zählers 20 wird auf die ersten n Zellen des Registers 24 übertragen.

Der Bestandteil G_2 wird von einem Zufallszahlengenerator 26 erzeugt, der an seinem Ausgang 28 eine n Bit lange zufallsmässige Bitkette erzeugt. Der Ausgang 28 ist mit den zweiten n Zellen des Schieberegisters 24 verbunden, um mit dem Ausgangssignal vom Zähler 20 verkettet zu werden und eine n Bit lange ganze Zahl zu erzeugen, die als der nachfolgende private Schlüssel k verwendet wird. Die Inhalte des Schieberegisters 24 werden dann abgerufen, und die resultierende ganze Zahl wird als privater Schlüssel k_a in einem sicheren Register 30 gespeichert.

Der Zähler 20 liefert durch seine fortschreitende Iteration einen eindeutigen Bestandteil, während der Zufallszahlengenerator 26 einen unvorhersagbaren Bestandteil liefert. Indem die beiden Bestandteile miteinander verknüpft werden, erhält man eine ganze Zahl mit den erforderlichen Eigenschaften.

Der Zähler 20 kann so ausgelegt sein, dass er um Beträge grösser als 1 inkrementiert, und kann, falls bevorzugt, unregelmässig inkrementieren, um bei dem Bestandteil G_1 ein Muster zu vermeiden. Unter der Voraussetzung, dass der Zähler 20 weiterhin inkrementiert, ist der Bestandteil G_1 eindeutig. Falls der Zähler 20 eine volle Anzahl erreicht, d.h. der endliche Bereich erschöpft ist, wird eine weitere Schlüsselwahl blockiert.

Der Darstellung zufolge steht der Bestandteil G_1 vor dem Bestandteil G_2, doch könnte die Reihenfolge auch vertauscht oder die Bestandteile könnten verschachtelt werden. Im Allgemeinen können die Bestandteile auf festgelegte vorhersagbare Weise miteinander verknüpft werden. Falls bevorzugt, könnte aber auch die Länge der Bestandteile unterschiedlich sein.

In Fig. 4 wird eine alternative Ausführungsform gezeigt, bei der gleiche Komponenten die gleichen Bezugszahlen aufweisen, wobei aus Gründen der Deutlichkeit ein «'» angefügt wird. Somit auf Fig. 4 Bezug nehmend, wird der Ausgang 28' des Zufallszahlengenerators 26' als anfänglicher Eingang 22' zum Zähler 20' verwendet. Der Zähler 20' inkrementiert den Zählwert, um einen eindeutigen Bestandteil G_1 zu liefern, doch kann der Anfangswert des Zählers nicht vorhergesagt werden.

Als weitere Ausführungsform, die in Fig. 5 mit dem Zusatz «zu gleichen Bezugszahlen gezeigt ist, wird der Ausgang des Zählers 20» als Eingang zu einer Permutationseinheit 32, beispielsweise einem DES-Verschlüsselungschip, verwendet. Die Permutationseinheit 32 wendet auf vorhersagbare Weise auf den Zählwert einen Verschlüsselungsalgorithmus an, da aber das Eingangssignal der Einheit 32 eindeutig ist, ist auch das Ausgangssignal eindeutig. Das Ausgangssignal der Einheit 32 wird dann im Register 24'' als Bestandteil G_1 verwendet.

Bei den obigen Ausführungsformen wurde der Bestandteil G_1 unter Einsatz eines Zählers 20 erzeugt. Unter der Voraussetzung, dass ein sich nicht wiederholender individueller Wert erhalten wird, können auch andere Sequenzer wie beispielsweise ein linear rückgekoppeltes Schieberegister oder eine deterministische Anordnung verwendet werden. Zur Lieferung des eindeutigen Bestandteils kann der Sequenzer entweder von einem Anfangswert aus inkrementieren oder von diesem Wert aus dekrementieren.

Patentansprüche

1. Verfahren zur Erzeugung einer ganzen Zahl zur Verwendung als privater Schlüssel in einem Verschlüsselungsschema mit öffentlichem Schlüssel, wobei das Verfahren folgende Schritte umfasst: Nutzen eines Ausgangssignals von einem Sequenzer als ersten Bestandteil, um für die ganze Zahl ein eindeutiges Element zu liefern, Nutzen einer zufallsmässig erzeugten ganzen Zahl als zweiten Bestandteil, Verknüpfen des ersten Bestandteils und des zweiten Bestandteils, um die genannte ganze Zahl zu liefern,

und Inkrementieren des Sequenzers vor der Erzeugung einer nachfolgenden ganzen Zahl, wodurch jede Erzeugung eine eindeutige und unvorhersagbare ganze Zahl zur Verwendung als den genannten privaten Schlüssel liefert.

2. Verfahren nach Anspruch 1, bei dem der erste und der zweite Bestandteil verkettet werden.

3. Verfahren nach Anspruch 2, bei dem der erste Bestandteil vor dem zweiten Bestandteil steht.

4. Verfahren nach Anspruch 1, bei dem mit dem zweiten Bestandteil der Sequenzer eingestellt wird.

5. Verfahren nach Anspruch 1, bei dem das Ausgangssignal des Sequenzers vor der Nutzung als erster Bestandteil permutiert wird.

6. Verfahren nach Anspruch 5, bei dem die Permutation durch einen Verschlüsselungsalgorithmus erfolgt.

7. Verfahren nach Anspruch 1, bei dem der Sequenzer ein Zähler ist, der inkrementiert.

8. Verfahren nach Anspruch 7, bei dem der Zähler gleichmässig inkrementiert.

9. Verfahren nach Anspruch 7, bei dem der Zähler ungleichmässig inkrementiert.

10. Vorrichtung zur Durchführung des Verfahrens nach Anspruch 1, zur Erzeugung einer ganzen Zahl zur Verwendung als privater Schlüssel in einem Verschlüsselungsschema mit öffentlichem Schlüssel, die Folgendes umfasst: eine Zähleinrichtung, die eine sich nicht wiederholende, sich fortlaufend ändernde ganze Zahl liefert und einen ersten Ausgang aufweist, einen Zahlengenerator, der auf unvorhersagbare Weise Zahlen erzeugt und einen zweiten Ausgang aufweist, eine Arithmetikeinheit, die die Ausgangssignale empfängt und die ganze Zahl und die unvorhersagbare Zahl miteinander verknüpft, um eine eindeutige und unvorhersagbare ganze Zahl zu liefern, eine Ausgabeeinrichtung, um die eindeutige und unvorhersagbare ganze Zahl aus der Arithmetikeinheit zwecks Verwendung als privaten Schlüssel abzurufen, und ein Steuersignal, um die Zähleinrichtung vor einer nachfolgenden Betätigung der Ausgabeeinrichtung zu inkrementieren.

11. Vorrichtung nach Anspruch 10, bei der die Arithmetikeinheit ein Schieberegister enthält, um die Ausgangssignale zu empfangen.

12. Vorrichtung nach Anspruch 11, bei der die Ausgangssignale verkettet werden.

13. Vorrichtung nach Anspruch 10, bei der die Arithmetikeinheit eine Permutierungseinrichtung enthält, an die der erste Ausgang angeschlossen ist.

14. Vorrichtung nach Anspruch 13, bei der die Permutierungseinrichtung an das Schieberegister angeschlossen ist.

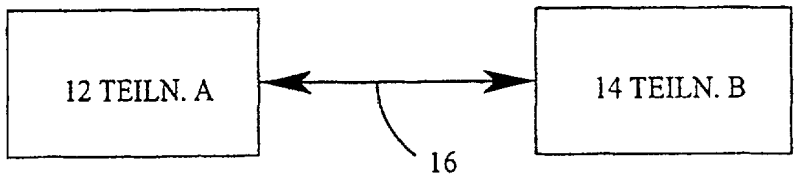

FIG. 1

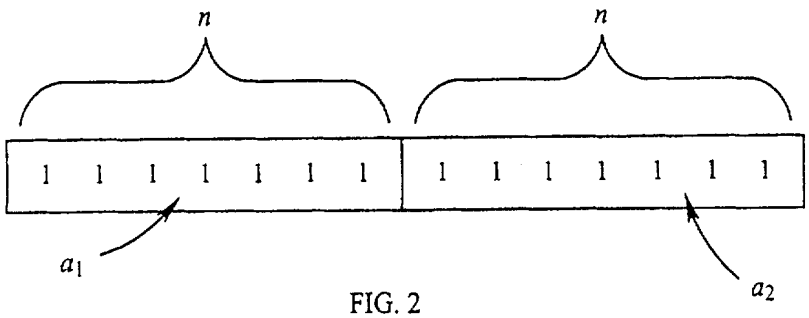

FIG. 2

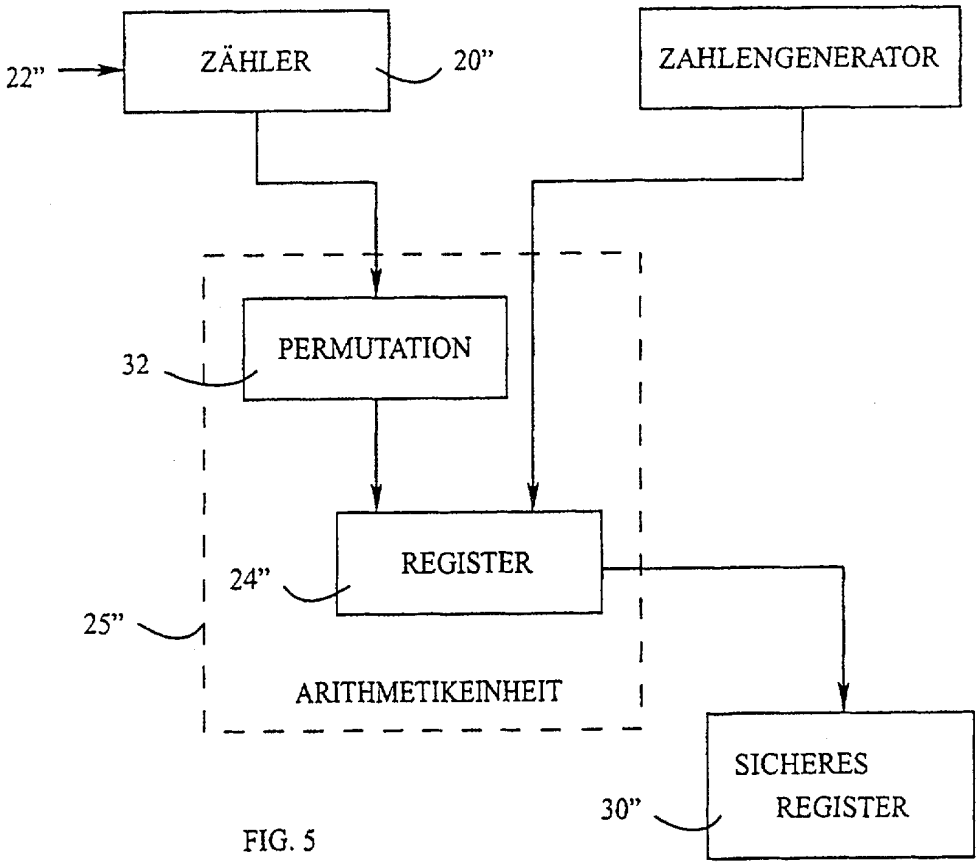

FIG. 5

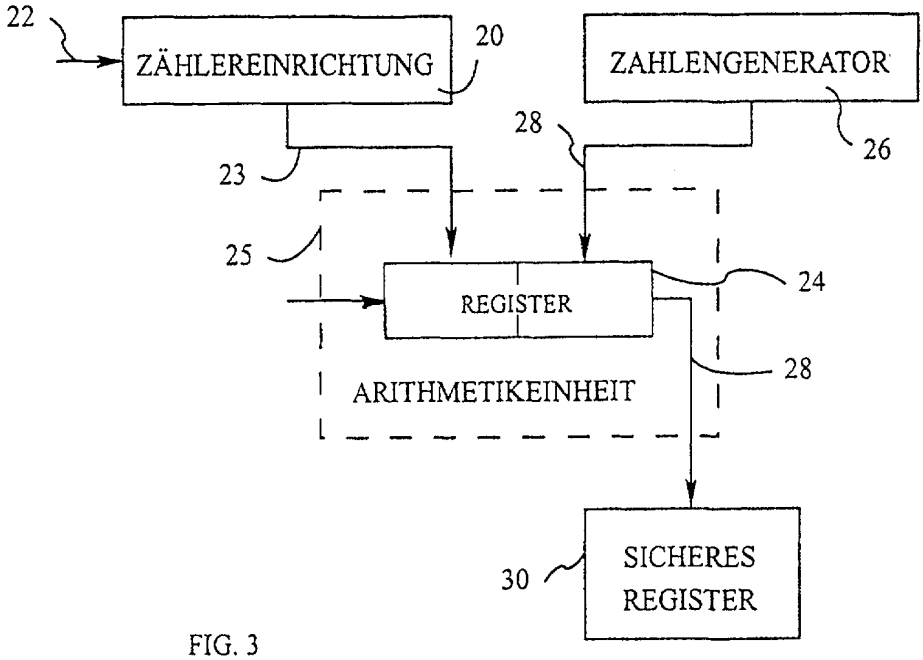
22
ZÄHLEREINRICHTUNG
20
ZAHLENGENERATOR
26
28
23
25
REGISTER
24
28
ARITHMETIKEINHEIT
30
SICHERES
REGISTER

FIG. 3

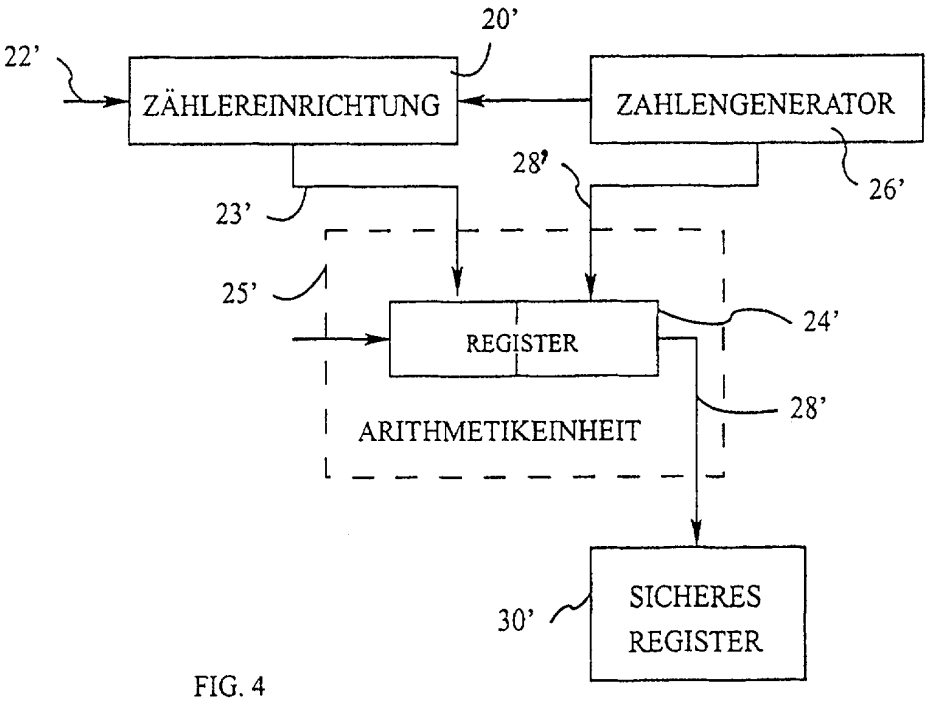
20'
22'
ZÄHLEREINRICHTUNG
ZAHLENGENERATOR
26'
28'
23'
25'
REGISTER
24'
28'
ARITHMETIKEINHEIT
30'
SICHERES
REGISTER

FIG. 4