(19) **Bundesrepublik Deutschland**
Deutsches Patent- und Markenamt

(10) **DE 697 38 636 T2** 2009.06.04

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 0 840 258 B1**
(21) Deutsches Aktenzeichen: **697 38 636.8**
(96) Europäisches Aktenzeichen: **97 119 056.6**
(96) Europäischer Anmeldetag: **31.10.1997**
(97) Erstveröffentlichung durch das EPA: **06.05.1998**
(97) Veröffentlichungstag
der Patenterteilung beim EPA: **16.04.2008**
(47) Veröffentlichungstag im Patentblatt: **04.06.2009**

(51) Int Cl.[8]: ***G07B 17/04*** (2006.01)
G07B 17/02 (2006.01)

(30) Unionspriorität:
742526 **01.11.1996** **US**

(84) Benannte Vertragsstaaten:
DE, FR, GB

(73) Patentinhaber:
Pitney Bowes, Inc., Stamford, Conn., US

(72) Erfinder:
Ryan, Frederick W. Jr., Oxford, CT 06478, US

(74) Vertreter:
HOFFMANN & EITLE, 81925 München

(54) Bezeichnung: **Verbessertes Verschlüsselungskontrollsystem für ein Postverarbeitungssystem mit Überprüfung durch das Datenzentrum**

Beschreibung

[0001] Die Erfindung betrifft ein Postsendungsverarbeitungssystem und Verfahren und genauer die Sicherheit von Postsendungs-Zählvorrichtungssystemen.

[0002] Neue Fortschritte in der digitalen Drucktechnologie haben es ermöglicht, ein digitales, d. h. Bitmap-adressierbares, Drucken für den Zweck eines Postsendungs-Zahlungsnachweises durch eine Postsendungs-Zählvorrichtungs-artige Vorrichtung zu implementieren. Wo es notwendig ist, solche Postsendungs-Zählvorrichtungsartigen Vorrichtungen von den typischen Postsendungs-Zählvorrichtungen zu unterscheiden, werden solche Vorrichtungen hier als Postsendungs-Nachweis-Vorrichtungen bzw. Postage Evidencing Devices oder PEDs bezeichnet. In solchen Vorrichtungen kann der Drucker ein typischer frei stehender Drucker sein. Der Computer-angesteuerte Drucker einer solchen PED kann den postamtlichen Freimachungsvermerk in einer gewünschten Position auf der Oberfläche der Postsendung drucken. Ferner wird der hier verwendete postamtliche Freimachungsvermerk als Postal Revenue Block bzw. Postamt-Einnahmeblock oder PRB definiert. Der PRB enthält typischerweise Daten wie zum Beispiel den Postsendungswert, eine eindeutige PED-Identifikationsnummer, das Datum und in einigen Anwendungen den Namen des Ortes, aus dem die Post kommt. Es muss jedoch erwähnt werden, dass der Ausdruck Postsendungs-Zählvorrichtung, wie er hier verwendet wird, verstanden wird, um alle verschiedenen Typen von Postsendungsabrechnungssystemen einschließlich solcher PEDs zu erfassen, und ist nicht auf den verwendeten Druckertyp beschränkt.

[0003] Aus der Sicht des Postamtes wird verstanden, dass ein ernsthaftes Problem in Verbindung mit PEDs darin besteht, dass das digitale Drucken es ziemlich leicht macht, das PRB zu fälschen, da jede r geeignete Computer und Drucker verwendet werden kann, um vielfache Bilder zu generieren. Tatsächlich können viele dieser neuen PED-Systeme Drucker verwenden, die in der Lage sind, legitime Freimachungsvermerke zu drucken, die von denen nicht unterscheidbar sind, die von anderen gedruckt sind, wobei diese gedruckt sind ohne jegliches Bestreben, eine Postsendung bzw. eine Postgebühr zu erwerben.

[0004] Um ein Poststück zu validieren bzw. zu überprüfen, das heißt sicherzustellen, dass eine Abrechnung für den auf dem Poststück gedruckten Postsendungsbetrag ordentlich durchgeführt wurde, ist es bekannt, dass man als ein Teil der Frankierung eine verschlüsselte Nummer berücksichtigen kann, wobei der Wert der Frankierung aus der Verschlüsselung bestimmt werden kann, um zu erfahren, ob der Wert korrekt ist, wie er auf dem Poststück gedruckt ist. Siehe zum Beispiel US-Patent mit den Nummern 4757537 und 4775246 an Edelmann u. a., wie auch US-Patent mit der Nummer 4649266 an Eckert. Es ist auch bekannt, ein Poststück durch ein Berücksichtigen der Adresse als einem weiteren Teil der Verschlüsselung zu authentifizieren, wie in US-Patent mit der Nummer 4725718 an Sansone u. a. und US-Patent mit der Nummer 4743747 an Fougere u. a. beschrieben.

[0005] Das US-Patent mit der Nummer 5170044 an Pastor beschreibt ein System mit einem binären Array und die tatsächlichen Pixelarrays werden gescannt, um den Poststück-Provider zu identifizieren und die verschlüsselte Klartextinformation wiederherzustellen. Das US-Patent mit der Nummer 5142577 an Pastor beschreibt verschiedene Alternativen zu der DES-Verschlüsselung zum Verschlüsseln einer Nachricht und zum Vergleichen der entschlüsselten postamtlichen Information mit der Klartextinformation auf dem Poststück.

[0006] UK 2251210 an Gilham beschreibt eine Zählvorrichtung, der einen elektronischen Kalender enthält, um einen Arbeitsvorgang der Frankiermaschine auf einer periodischen Grundlage zu verhindern, um zu gewährleisten, dass der Nutzer Abrechnungsinformationen an die Postamtbehörde weiterleitet. US-Patent mit der Nummer 5008827 an Sansone u. a. beschreibt ein System zum Aktualisieren von Raten und Regulierungsparametern bei jeder Zählvorrichtung über ein Kommunikationsnetzwerk zwischen der Zählvorrichtung und einem Datenzentrum. Während die Zählvorrichtung online ist, werden Statusregister in der Zählvorrichtung überprüft und ein Alarmzustand wird verursacht, wenn eine Anomalie erfasst wird.

[0007] US-Patent mit der Nummer 5390251 an Pastor u. a. beschreibt ein Postverarbeitungssystem, das die Gültigkeit von ausgedruckten Freimachungsvermerken auf Poststücken von einer potentiell großen Anzahl von Nutzern von Postsendungs-Zählvorrichtungen kontrolliert und eine Einrichtung beinhaltet, die in jeder Postsendungs-Zählvorrichtungen angeordnet ist, zum Generieren eines Codes und zum Drucken des Codes auf jedes Poststück. Der Code ist eine verschlüsselte Abbildung der Postsendungs-Zählvorrichtungs-Einrichtung, die das Freimachungsvermerk und andere Information druckt, um die Gültigkeit der Postsendung bzw. der Postgebühr auf dem Poststück eindeutig zu bestimmen. Die Schlüssel für die Code-Erzeugungseinrichtung werden zu vorbestimmten Zeitintervallen in jeder der Zählvorrichtung geändert. Ein Sicherheitszentrum enthält eine Einrichtung zum Unterhalten einer Sicherheitscode-Datenbank und Nachverfolgen der Schlüssel zum Generieren der Sicherheitscodes in Übereinstimmung mit den Veränderungen in jeder

generierenden Einrichtung und der Information, die auf dem Poststück durch die Postsendungs-Zählvorrichtungs-Einrichtung zum Vergleich mit dem auf dem Poststück gedruckten Code gedruckt wurde. Es können zwei gedruckte Codes vorhanden sein, einer, der durch den Postamtsservice für deren Sicherheitsüberprüfungen verwendet wird, und einer von dem Hersteller. Der Verschlüsselungsschlüssel kann zu vorbestimmten Intervallen oder täglich oder zum Drucken eines jeden Poststücks verändert werden.

[0008] Es wird verstanden werden, dass, um die Information in dem PRB unter Verwendung der verschlüsselten Nachricht zu verifizieren, der Prüfer erst in der Lage sein muss, den Schlüssel zu erhalten, der durch die bestimmte Zählvorrichtung verwendet wird. Bei dem Versuch Postsysteme zu behandeln, die solche Entschlüsselungssysteme aufnehmen können, muss zuerst verstanden werden, dass der Zählvorrichtungsabstand groß ist und konstanten Fluktuationen unterliegt, da Zählvorrichtungen dem Service zugefügt werden und entfernt werden. Wenn der gleiche Schlüssel für alle Zählvorrichtungen verwendet werden würde, ist die Schlüsselverteilung leicht aber das System ist nicht sicher. Sobald der Code durch irgendjemand entschlüsselt ist, kann der Schlüssel anderen, die das System verwenden, zur Verfügung gestellt werden und der gesamte Arbeitsablauf ist gefährdet. Wenn jedoch jeweils separate Schlüssel für jede Zählvorrichtung verwendet werden, wird die Schlüsselverwaltung dann möglicherweise extrem schwierig, wenn man die Fluktuationen in einem solchen großen Bestand berücksichtigt.

[0009] Die Europäische Patentveröffentlichung mit der Nummer 0647924, angemeldet am 7. Oktober 1994, die an den Rechtsnachfolger der vorliegenden Anmeldung übertragen wurde, beschreibt ein Schlüsselverwaltungssystem zur Postverarbeitung, das einen aus einem Satz von vorbestimmten Schlüsseln durch eine vorbestimmte Beziehung einer bestimmten Zählvorrichtung zuweist, wodurch mehreren Zählvorrichtungen effektiv erlaubt wird, einen einzigen Schlüssel gemeinsam zu nutzen. Das Schlüsselverwaltungssystem beinhaltet die Generation eines ersten Schlüsselsatzes, die dann für eine Vielzahl von jeweiligen Postsendungs-Zählvorrichtungen verwendet werden. Ein erster Schlüssel des ersten Schlüsselsatzes gehört dann zu einer bestimmten Zählvorrichtung, in Übereinstimmung mit einer Abbildung oder einem Algorithmus. Der erste Schlüssel kann durch das Eingeben eines zweiten Schlüssels über eine Verschlüsselung unter Verwendung des ersten Schlüssels verändert werden.

[0010] Es wurde gefunden, dass, obwohl das in der zuvor notierten Europäischen Patentveröffentlichung mit der Nummer 0647924, beschriebene System, und im Folgenden als "1000 Schlüssel-System" bezeichnet, ein verwaltbares Schlüsselverwaltungssystem bereitstellt, das System mehrere Zählvorrichtungen aufweist, die den gleichen Schlüssel gemeinsam nutzen.

[0011] Es ist daher eine Aufgabe der Erfindung ein Schlüsselverwaltungssystem bereitzustellen, das ein 1000-Schlüssel-System mit verbesserter Sicherheit bereitstellt und dennoch eine Erleichterung der Schlüsselverwaltung in einem sehr großen System erlaubt.

[0012] Es ist eine andere Aufgabe, ein Verfahren zum leichten Verändern der Schlüssel für jede Zählvorrichtung bereitzustellen, in einer Art und Weise, die eine verbesserte Sicherheit und eine systemweite Nachverfolgung der Schlüsselveränderungen bereitstellt.

[0013] Gemäß einem Aspekt der Erfindung wird ein Schlüssel-Management-Verfahren bzw. Schlüssel-Verwaltungs-Verfahren bereitgestellt zum Steuern der in einer Kodierungs-Information verwendeten, auf einer Postsendung zum Validieren bzw. Überprüfen der Postsendung zu druckenden Schlüssel, wobei das Verfahren die Schritte umfasst:
Generieren einer Vielzahl von Schlüsseln K, um einen festgelegten Schlüsselsatz $K_{pred(1-n)}$ zu erhalten; Zuweisen eines der Vielzahl von Schlüsseln K_{pred} auf eine spezielle Postsendungs-Zählvorrichtung M (**12**) mittels einer bestimmten mit der Postsendungs-Zählvorrichtung (**12**) verbundenen Beziehung, wobei die Beziehung als eine vorbestimmte Funktion F(M) abgeleitet wird, die der speziellen Postsendungs-Zählvorrichtung entspricht; Verschlüsseln des zugewiesenen Schlüssels K_{pred} mit einem Datum, um einen zugewiesenen datumsabhängigen Schlüssel K_{dd} zu erhalten; und Kombinieren des zugewiesenen datumsabhängigen Schlüssels K_{dd} mit Information, die eindeutig zu der speziellen Postsendungs-Zählvorrichtung M_{uni} sind, um einen endgültigen Schlüssel K_{final} für die spezielle Postsendungs-Zählvorrichtung M_{uni} zu erzeugen, so dass $K_{final} = f(K_{dd}, M_{uni})$.

[0014] Gemäß einem anderen Aspekt der Erfindung wird ein Schlüssel-Management-System bzw. Schlüssel-Verwaltungs-System zum Steuern der in einer Kodierungs-Information verwendeten, auf einer Postsendung zum Validieren bzw. Überprüfen der Postsendung zu druckenden Schlüssel, umfassend: ein Mittel zum Generieren einer Vielzahl von Schlüsseln K, um einen festgelegten Schlüssel-Satz $K_{pred(1-n)}$ zu erhalten; ein Mittel zum Zuweisen eines aus der Vielzahl von Schlüsseln K_{pred} an eine bestimmte Postsendungs-Zählvorrichtung M (**12**) mittels einer bestimmten, mit der Postsendungs-Zählvorrichtung (**12**) verbundenen Beziehung, wobei die Beziehung als eine vorbestimmte, der speziellen Postsendungs-Zählvorrichtung entsprechende Funktion F(M) abgeleitet wird; ein Mittel zum Verschlüsseln des zugewiesenen Schlüssels K_{pred} mit einem Datum, um ei-

nen zugewiesenen, datumsabhängigen Schlüssel K_{dd} zu erhalten; und ein Mittel zum Kombinieren des zugewiesenen datumsabhängigen Schlüssels K_{dd} mit Information, die eindeutig zu der speziellen Postsendungs-Zählvorrichtung M_{uni} ist, um einen endgültigen Schlüssel K_{final} für die spezielle Postsendungs-Zählvorrichtung M zu erzeugen, so dass $K_{final} = f(K_{dd}, M_{uni})$

[0015] Die obigen und andere Aufgaben und Vorteile der vorliegenden Erfindung werden nach der Berücksichtigung der folgenden detaillierten Beschreibung im Zusammenhang mit den begleitenden Zeichnungen ersichtlich, in denen gleiche Bezugszeichen sich durchweg auf gleiche Teile beziehen, und in denen:

[0016] Fig. 1 ist eine schematische Ansicht eines Systems, das in Übereinstimmung mit einer Ausführungsform der Erfindung verwendet werden kann;

[0017] Fig. 2a und Fig. 2b stellen die Information dar, die in einer ersten Ausführungsform eines PRB in Übereinstimmung mit einer Ausführungsform der Erfindung gedruckt werden kann;

[0018] Fig. 3a und Fig. 3b stellen eine Alternative zu der in den Fig. 2a und Fig. 2b gezeigten Information dar;

[0019] Fig. 4 ist ein Flussdiagramm des Betriebsablaufes zum Bereitstellen der Schlüssel in Übereinstimmung mit einer Ausführungsform der Erfindung;

[0020] Fig. 5 ist ein Flussdiagramm des Zählvorrichtungs-Betriebsablaufes in Übereinstimmung mit der bevorzugten Ausführungsform der Erfindung;

[0021] Fig. 6 ist ein Flussdiagramm des Zählvorrichtungs-Betriebsablaufes in Übereinstimmung mit einer alternativen Ausführungsform der Erfindung;

[0022] Fig. 7 ist ein Flussdiagramm des Datenzentrums-Betriebsablaufes in Übereinstimmung mit der bevorzugten Ausführungsform der Erfindung;

[0023] Fig. 8 ist ein Flussdiagramm des Überprüfungsprozesses;

[0024] Fig. 9 ist ein Blockdiagramm der bevorzugten Ausführungsform der vorliegenden Erfindung; und

[0025] Fig. 10 ist ein Blockdiagramm einer alternativen Ausführungsform der vorliegenden Erfindung;

[0026] Das Folgende beschreibt ein Schlüsselsteuerungssystem, das das Generieren eines ersten Satzes von vorbestimmten Schlüsseln K_{pred} umfasst, die dann als Hauptschlüssel für eine Vielzahl von jeweiligen Postsendungs-Zählvorrichtungen verwendet werden. Die Schlüssel beziehen sich dann auf jeweilige Zählvorrichtungen in Übereinstimmung mit einer Abbildung oder einem Algorithmus. Der vorbestimmte Hauptschlüssel K_{pred} wird mit dem Datum verschlüsselt, um einen Datums-abhängigen Schlüssel K_{dd} zu erhalten, der mit der jeweiligen Zählvorrichtung verbunden ist. Der Datums-abhängigen Schlüssel wird mit einem eindeutigen Identifikator der jeweiligen Zählvorrichtung verschlüsselt, um einen eindeutigen Schlüssel K_{final} zu erhalten, der durch die jeweilige Zählvorrichtung verwendet wird, um digitale Token zu generieren. Das Datenzentrum verschlüsselt das Datum mit jedem vorbestimmten Schlüssel K_{pred}, um eine Tabelle von abhängigen Schlüsseln K_{dd} zu erhalten. Die K_{dd}-Tabelle wird an Überprüfungsstellen verteilt. Die Überprüfungsstellen lesen eine Zählvorrichtungs-Identifikation von einem Poststück, das überprüft wird, um den abhängigen Schlüssel K_{dd} der Zählvorrichtung aus der verteilten Tabelle nachzuschlagen. Die Überprüfungsstellen verschlüsseln den abhängigen Schlüssel K_{dd} mit dem eindeutigen Identifikator, um den eindeutigen Zählvorrichtungsschlüssel zu erhalten, der verwendet wird, um von der Zählvorrichtung generierte Token zu überprüfen.

[0027] In einer bevorzugten Ausführungsform umfasst das Verfahren die Schritte zum Speichern des Hauptschlüssels K_{pred}, des Datums-abhängigen Schlüssels K_{dd} und des eindeutigen Schlüssels K_{final} in der Zählvorrichtung.

[0028] In einer alternativen Ausführungsform wird der Hauptschlüssel K_{pred} mit einem eindeutigen Zählvorrichtungs-Identifikator verschlüsselt, um den eindeutigen Schlüssel K_{final} zu erhalten, der in der Zählvorrichtung gespeichert wird. Die Zählvorrichtung generiert dann seinen Datumsabhängigen Schlüssel K_{dd}, der verwendet wird, um digitale Token zu erzeugen.

[0029] In Fig. 1 wird im Allgemeinen bei **10** ein gesamtes System in Übereinstimmung mit einer Ausführungsform der Erfindung gezeigt. In der dargestellten Ausführungsform umfasst das System eine Zählvorrichtung oder PED **12**, die mit einer Vielzahl von Zentral-Einrichtungen interagiert. Eine erste Zentraleinrichtung ist eine wohlbekannte Zählvorrichtungs-Geldmittel-Neueinstellungs-Zentraleinrichtung **14** eines Typs, die zum Beispiel in dem US-Patent mit der Nummer 4097923 beschrieben ist, und die geeignet ist zum entfernten Hinzufügen von Finanzmitteln zu der Zählvorrichtung, um sie in die Lage zu versetzten, den Ausgabebetrieb von Wert-tragenden Freimachungsvermerken fortzusetzen. In Übereinstimmung mit einer Ausführungsform der Erfindung wird auch eine Sicherheits- oder Forensic-Zentraleinrichtung **16** eingerichtet, die sich natürlich physikalisch in der Neueinstellungs-Zentraleinrichtung **14** befinden kann, aber hier zur Vereinfachung des Verständnisses separate gezeigt wird.

[0030] Alternativ kann eine solche Sicherheits- oder Forensic-Zentraleinrichtung eine gänzlich separate Einrichtung sein, die zum Beispiel durch die Postamtbehörden unterhalten wird, oder zwei separate Einrichtungen können unterhalten werden, um Sicherheitsstufen bereitzustellen, wenn es gewünscht wird. Die gestrichelten Linien in Fig. 1 bezeichnen eine Telekommunikation zwischen der Zählvorrichtung **12** und der Neueinstellungs-Zentraleinrichtung **14** (und/oder Forensic-Zentraleinrichtung **16**).

[0031] Typischerweise kann es eine zugehörige Zählvorrichtungs-Verteilungszentraleinrichtung **18** geben, die verwendet wird, um die Logistik zum Verteilen der Zählvorrichtungen mit jeweiligen Nutzern zu vereinfachen. Gleichermaßen wird eine Business-Verarbeitungszentraleinrichtung **20** verwendet für den Zweck des Verarbeitens von Bestellungen für Zählvorrichtungen und für die Administration der verschiedenen Aufgaben, die mit dem Zählvorrichtungsbestand als Ganzes verbunden sind.

[0032] Der bei **22** angezeigte Zählvorrichtungs-Hersteller stellt der Verteilungs-Zentraleinrichtung **18** kundenspezifische Zählvorrichtungen oder PEDs bereit, nach dem Einrichten der Durchführbarkeit mit Shop-Checks zwischen dem Hersteller und der Neueinstellungs-Zentraleinrichtung **14** und der Forensic-Zentraleinrichtung **16**. Die Zählvorrichtung oder PED wird in der Einrichtung des Nutzers durch einen Kundenservice-Repräsentanten frei geschaltet, der hier durch die Box **24** angezeigt ist.

[0033] In der Neueinstellungs-Zentraleinrichtung **14** wird eine Datenbank **26** unterhalten, die Zählvorrichtungen und Zählvorrichtungs-Transaktionen zuordnet. Die Neueinstellungs-Kombinationen werden durch eine gesicherte Einrichtung generiert, die hier als Black Box **28** bezeichnet wird. Die Details einer solchen Neueinstellungs-Anordnung werden in dem US-Patent mit der Nummer 4097923 gefunden, das hiermit speziell durch eine Referenz berücksichtigt wird, und wird hier nicht weiter beschrieben.

[0034] Die Datenbank **30** und die gesicherte Verschlüsselungs-Erzeugungseinrichtung, hier als Orange Box **32** designiert, werden in der Sicherheits- oder Forensic-Zentraleinrichtung unterhalten. Die Orange Box verwendet vorzugsweise die DES-Standard-Verschlüsselungstechnik, um eine codierte Ausgabe auf Grundlage der Schlüssel und anderer Information bereitzustellen, die in dem Nachrichtenstring zu ihr bereitgestellt. Es wird verstanden, dass andere Verschlüsselungsanordnungen bekannt sind und die Erfindung nicht auf die bestimmte Ausführungsform beschränkt ist, die die DES-Verschlüsselung verwendet. Die Sicherheits- oder Forensic-Zentraleinrichtung **16**, wo auch immer unterhalten, ist vorzugsweise durch eine Telekommunikation mit einer beliebigen Postoffice-Inspektionsstation verbunden, wobei eine davon hier bei **34** angezeigt ist.

[0035] Weitere Details können in der Europäischen Patentanmeldung mit der Nummer 0647924 gefunden werden, die vorher erwähnt wurde und hier speziell durch eine Referenz enthalten ist.

[0036] Die Zählvorrichtung **12** enthält, wie dargestellt, einen gesicherten Zeitgeber **40**, der verwendet wird, um eine Kalenderfunktion bereitzustellen, die durch den Hersteller programmiert wird. Der Zeitgeber und die Kalenderfunktion kann durch den Nutzer nicht modifiziert werden. Solche Zeitgeber sind wohlbekannt und können in Computerroutinen oder in dedizierten Chips implementiert werden, die programmierbare Kalenderausgaben bereitstellen können. In die Register der Zählvorrichtung **12** werden auch ein Geldmengen-Neueinstellungsschlüssel **42**, ein Sicherheitsschlüssel **44**, Verfallsdatum **47** und bevorzugt ein Eintragungsfreigabeflag **48** gespeichert. Um die Entschlüsselung der durch die Postsendungs-Zählvorrichtung zu druckenden verschlüsselten Nachricht zu verhindern, wird der Sicherheitsschlüssel **44** bevorzugt zu vorbestimmten Intervallen verändert, wie oben diskutiert.

[0037] Der Sicherheitsschlüssel **44** wird in Verbindung mit einer DES-Verschlüsselungseinrichtung in der Zählvorrichtung **12** verwendet, um eine Verschlüsselung von bestimmter Information in der PRB für jedes Drucken der PRB auf einem Poststück bereitzustellen. Bei jedem Druckbetrieb kann die gesamte verschlüsselte Nachricht auf dem Poststück gedruckt werden. Bevorzugt ist der Code, hier im Folgenden als ein ECODE bezeichnet (auch als ein digitaler Token bezeichnet), jedoch ein verkürzter Codetext, der durch eine DES-Verschlüsselung der Nachricht auf Grundlage von Postsendungsinformationen erzeugt wird, die der Zählvorrichtung zur Verfügung stehen. Die Überprüfung an der Sicherheitszentraleinrichtung besteht aus der Überprüfung, dass die verschlüsselte Information mit dem ECODE übereinstimmt.

[0038] Wenn ein automatisches Überprüfen des ECODE erwünscht ist, müssen sowohl der ECODE als auch der Klartext Maschinenlesbar sein. Eine typische Länge der Klartextinformation ist, nur als ein Beispiel und nicht als eine Beschränkung, die Summe aus der Zählvorrichtungs-ID (typischerweise 7-stellig), dem Datum (bevorzugt 2-stellig, geeignet die letzten 2 der Anzahl von Tagen von einem vorbestimmten Startdatum wie zum Beispiel der 1. Januar), dem Postsendungsumfang (4-stellig) und der Stückzahl für typischerweise insgesamt 16 Stellen. Lesevorrichtungen zum Herauslesen der Information, entweder aus einem Strichcode auf dem Poststück oder als OCR, sind wohlbekannt und werden nicht weiter diskutiert.

[0039] Ein DES-Block ist konventionell 64-Bits lang oder annähernd 20 Dezimalstellen. Ein Codeblock ist eine Verschlüsselung von 64 Datenbits. Es wird anerkannt werden, dass andere Information ausgewählt werden kann und dass weniger als die hier bereitgestellte Information in anderen Ausführungsformen der Erfindung verschlüsselt werden kann. Es ist jedoch wichtig zu erwähnen, dass die zu verschlüsselnde Information identisch zu der sein muss, die bei der Überprüfung verwendet wird. Zu diesem Zweck kann die Klartext-Nachricht Daten enthalten, die die bestimmte Information anzeigen, die verschlüsselt ist. Das kann die Form eines zusätzlichen Zeichens haben, eines zusätzlichen Strichcodes oder einer Markierung auf dem Poststück, wie es erwünscht wird.

[0040] Wenn es erwünscht ist, kann ein zweiter ECODE unter Verwendung eines DES-Schlüssels aus einem Satz von PS-DES-Schlüsseln gedruckt werden, die dem Postamtservice bekannt sind. Alternativ kann der Postamtservice wählen, seinen eigenen Schlüsselsatz zu verwalten, wie in Verbindung mit dem im Folgenden beschriebenen Schlüsselverwaltungssystem beschrieben.

[0041] In einer ersten Ausführungsform, wie in den Fig. 2a und Fig. 2b beschrieben, wird der Klartext unter Verwendung der PS-DES-Schlüssel verschlüsselt. Der Postamtservice verwendet den gleichen Schlüssel aus dem PS-DES-Satz, um die Nachricht zu überprüfen. Ein höheres Sicherheitsniveau wird durch den zweiten ECODE bereitgestellt.

[0042] In einer zweiten Ausführungsform werden zwei ECODEs generiert und auf das Poststück gedruckt, einer unter Verwendung eines PS-DES-Schlüssels, der durch den Postamtservice bereitgestellt wird, und der andere unter Verwendung eines Lieferanten-DES-Schlüssels, der zum Beispiel durch den Hersteller oder die Sicherheits-Zentraleinrichtung bereitgestellt wird. Der Postamtservice kann dann die Nachricht unter Verwendung seines eigenen Code-generierenden und Schlüsselverwaltungssystems überprüfen. Während der Lieferant separat die Gültigkeit der Nachricht unter Verwendung des generierten ECODE überprüfen kann, unter Verwendung seines separaten Schlüsselsystems. Die Fig. 3a und Fig. 3b zeigen das Format dieser zweiten Ausführungsform.

[0043] Fig. 4 zeigt eine Anordnung zum Verwalten der Zählvorrichtungs-Hauptschlüssel, wie in der vorher erwähnten Europäischen Patentveröffentlichung mit der Nummer 0647924 offenbart. Zuerst wird im Schritt **400** ein großer festgelegter Satz von vorbestimmten Schlüsseln K_{pred} generiert. Wie unten gezeigt, umfasst das System S in Übereinstimmung mit der Erfindung einen Satz von Zeigern {p}, einen Satz von Schlüsseln, die durch die Zeiger {keyp} indiziert sind, und eine **Abb.** F oder einen generierenden Algorithmus aus dem Satz von Zählvorrichtungen {M} zu dem Zeiger-Satz. Somit ist:

S = (F, {p}, keyp}) das System

F: {M} → {p}

und

F(M) = F(Zählvorrichtungs-ID) = p

findet den Zeiger für den Schlüssel einer bestimmten Zählvorrichtung M.

[0044] Zur Fig. 4 zurückkehrend, wird somit im Schritt **405**, als ein Beispiel, aus den Zählvorrichtungsparametern der Satz von Zeigern {p} generiert, was eine ganzzahlige Zahl von 1 bis 1000 sein kann. Die Funktion F kann dann im Schritt **410** ausgewählt werden, wiederum als Beispiel, als die DES-Verschlüsselung der Zählvorrichtungs-ID unter Verwendung eines DES-Schlüssels K, bevorzugt verkürzt auf drei Stellen, und beim Schritt **415** wird eine Nachschlagetabelle erzeugt. Es wird verstanden werden, dass andere funktionale Beziehungen ausgewählt werden können. Die Nachschlagetabelle umfasst einen Satz an Zählvorrichtungs-IDs und deren zugewiesene Zeiger. Für die größte Sicherheit wird es geschätzt werden, dass die Beziehung zwischen einem Zeiger p und dem dazugehörigen Schlüssel nicht leicht feststellbar sein sollte, noch sollte die Beziehung zwischen dem Zeiger und der Zählvorrichtungs-ID. Es wird auch verstanden, dass die Funktion F im Geheimen unterhalten werden sollte.

[0045] Nun auf die Fig. 5 und Fig. 9 Bezug nehmend, wird die bevorzugte Ausführungsform der Erfindung gezeigt. Im Schritt **420** wird unter Verwendung der Zählvorrichtungs-ID einer speziellen Zählvorrichtung in der Nachschlagetabelle der dazugehörige K_{pred} in der Zählvorrichtung gespeichert. Im Schritt **430** wird ein Datums-abhängiger Schlüssel K_{dd} aus dem vorbestimmten Schlüssel K_{pred} generiert, durch ein Verschlüsseln des Datums mit K_{pred}, um den K_{dd} für die Zählvorrichtung zu erhalten. Im Schritt **435** wird ein eindeutiger Zählvorrichtungs-Identifikator, wie zum Beispiel eine Zählvorrichtungs-Seriennummer, mit dem Datums-abhängigen Schlüssel K_{dd} verschlüsselt, um einen eindeutigen Schlüssel K_{final} für die Zählvorrichtung zu erzeugen. Die Zählvorrichtung erzeugt digitale Token unter Verwendung seines eindeutigen Schlüssels K_{final}.

[0046] Nun auf die Fig. 6 und Fig. 10 Bezug nehmend, wird eine alternative Ausführungsform des Zählvorrichtungsbetriebs gezeigt. Im schritt **470** wird ein eindeutiger Zählvorrichtungs-Identifikator, wie zum Beispiel eine Zählvorrichtungs-Seriennummer, mit dem vorbestimmten Hauptschlüssel K_{pred} ver-

schlüsselt, um einen eindeutigen Schlüssel K_{final} für die Zählvorrichtung zu erhalten. Der eindeutige Zählvorrichtungs-Schlüssel K_{final} wird im Schritt **475** in der Zählvorrichtung gespeichert. K_{final} wird verwendet, um einen Datums-abhängigen Schlüssel K_{dd} in der Zählvorrichtung zu generieren, wobei durch ein Verschlüsseln des Datums mit K_{final} der Datums-abhängige Schlüssel K_{dd} erzeugt wird.

[0047] Nun auf Fig. 7 Bezug nehmend, wird der Daten-Zentraleinrichtungsbetrieb für die bevorzugte Ausführungsform gezeigt. Im Schritt **450** wird das Datum mit jedem vorbestimmten Hauptschlüssel K_{pred} verschlüsselt, um eine Tabelle von Datums-abhängigen Schlüsseln K_{dd} zu erhalten. Im Schritt **455** verteilt die Daten-Zentraleinrichtung die K_{dd}-Tabelle auf jede der Überprüfungsstellen zum Verwenden bei der Überprüfung der durch die Zählvorrichtung erzeugten digitalen Token.

[0048] Nun auf Fig. 8 Bezug nehmend, wird ein Überprüfungsprozess gezeigt, der das Schlüsselverwaltungssystem in Übereinstimmung mit einer Ausführungsform der vorliegenden Erfindung verwendet. Um ein Poststück zu überprüfen, wird im Schritt **500** die auf dem Poststück gedruckte Zählvorrichtungs-ID-Nummer gelesen. Im Schritt **510** wird unter Verwendung der Zählvorrichtungs-ID-Nummer ein Datums-abhängiger Schlüssel K_{dd} in der K_{dd}-Tabelle gefunden, die durch die Daten-Zentraleinrichtung verteilt wird. Der Schlüssel wird gefunden unter Verwendung der Nachschlagetabelle oder des Algorithmus F aus der bestimmten Zählvorrichtungsnummer. Im Schritt **515** werden die identischen Zählvorrichtungsdaten, die durch die Zählvorrichtung verwendet wurden, um den eindeutigen Schlüssel K_{final} der Zählvorrichtung zu erhalten, mit dem Datums-abhängigen Schlüssel K_{dd} verschlüsselt. Im Schritt **520** wird die identische Klartextinformation, die verwendet wurde, um den ECODE zu erzeugen, nun in der Sicherheits-Zentraleinrichtung unter Verwendung von K_{final} verschlüsselt, und das Resultat wird im Schritt **530** mit dem Code verglichen, der auf das Poststück gedruckt ist. Wenn eine Übereinstimmung bei der Entscheidung im Schritt **540** vorliegt, ist das Poststück gültig. Wenn nicht, wird der NEIN-Zweig einen Alarm auslösen.

[0049] Für den Moment zu der Fig. 2a und der Fig. 3a zurückkehrend, ist der Postamtservice in diesen Ausführungsformen in der Lage, den PS-DES-Zeiger direkt von dem Freimachungsvermerk zu erhalten, ohne den in der Fig. 8 gezeigten Prozess zu verwenden. In den in den Fig. 2b und Fig. 3b gezeigten Fällen, wird der DES-Zeiger unter Verwendung eines vorbestimmten Algorithmus erhalten, der auf die Information angewendet wird, die in der PED-ID gedruckt ist, wie in Verbindung mit Fig. 8 beschrieben.

Patentansprüche

1. Schlüssel-Management-Verfahren zum Steuern der in einer Kodierungs-Information verwendeten, auf einer Postsendung zum Validieren der Postsendung zu druckenden Schlüssel, wobei das Verfahren die Schritte umfasst:
Generieren einer Vielzahl von Schlüsseln K, um einen festen Schlüsselsatz $K_{pred(1-n)}$ zu erhalten;
Zuweisen eines der Vielzahl von Schlüsseln K_{pred} auf eine spezielle Postsendungs-Zählvorrichtung M (**12**) mittels einer bestimmten mit der Postsendungs-Zählvorrichtung (**12**) verbundenen Beziehung, wobei die Beziehung als eine vorbestimmte Funktion F(M) abgeleitet wird, die der speziellen Postsendungs-Zählvorrichtung entspricht;
Verschlüsseln des zugewiesenen Schlüssels K_{pred} mit einem Datum, um einen zugewiesenen datumsabhängigen Schlüssel K_{dd} zu erhalten; und
Kombinieren des zugewiesenen datumsabhängigen Schlüssels K_{dd} mit Information, die eindeutig zu der speziellen Postsendungs-Zählvorrichtung M_{uni} sind, um einen endgültigen Schlüssel K_{final} für die spezielle Postsendungs-Zählvorrichtung M_{uni} zu erzeugen, so dass $K_{final} = f(K_{dd}, M_{uni})$

2. Verfahren nach Anspruch 1, wobei die bestimmte, mit der Postsendungs-Zählvorrichtung verbundene Beziehung ein mit der speziellen Postsendungs-Zählvorrichtung M verbundener Pointer p ist, wobei der Pointer p als eine Funktion F(M) abgeleitet wird, die vorbestimmten Parametern der speziellen Postsendungs-Zählvorrichtung M entspricht.

3. Verfahren nach Anspruch 1 oder 2, ferner die Schritte umfassend:
Verschlüsseln eines Datums mit jedem K_{pred} in dem festen Schlüsselsatz $K_{pred(1-n)}$, um eine Tabelle mit datumsabhängigen Schlüsseln $K_{dd(1-n)}$ zu erhalten; und
Verteilen der Tabelle mit datumsabhängigen Schlüsseln $K_{dd(1-n)}$ an Verifizierungsorte.

4. Verfahren nach Anspruch 1, ferner umfassend ein Installieren der zugehörigen Schlüssel K_{pred} in der speziellen Postsendungs-Zählvorrichtung.

5. Schlüssel-Management-System zum Steuern der in einer Kodierungs-Information verwendeten, auf einer Postsendung zum Validieren der Postsendung zu druckenden Schlüssel, umfassend:
ein Mittel zum Generieren einer Vielzahl von Schlüsseln K, um einen festen Schlüssel-Satz $K_{pred(1-n)}$ zu erhalten;
ein Mittel zum Zuweisen eines aus der Vielzahl von Schlüsseln K_{pred} an eine bestimmte Postsendungs-Zählvorrichtung M (**12**) mittels einer bestimmten, mit der Postsendungs-Zählvorrichtung (**12**) verbundenen Beziehung, wobei die Beziehung als eine vorbestimmte, der speziellen Postsendungs-Zählvorrichtung entsprechende Funktion F(M) abgeleitet

wird;
ein Mittel zum Verschlüsseln des zugewiesenen Schlüssels K_{pred} mit einem Datum, um einen zugewiesenen, datumsabhängigen Schlüssel K_{dd} zu erhalten; und
ein Mittel zum Kombinieren des zugewiesenen datumsabhängigen Schlüssels K_{dd} mit Information, die eindeutig zu der speziellen Postsendungs-Zählvorrichtung M_{uni} ist, um einen endgültigen Schlüssel K_{final} für die spezielle Postsendungs-Zählvorrichtung M zu erzeugen, so dass $K_{final} = f(K_{dd}, M_{uni})$.

Es folgen 6 Blatt Zeichnungen

Anhängende Zeichnungen

FIG. 1

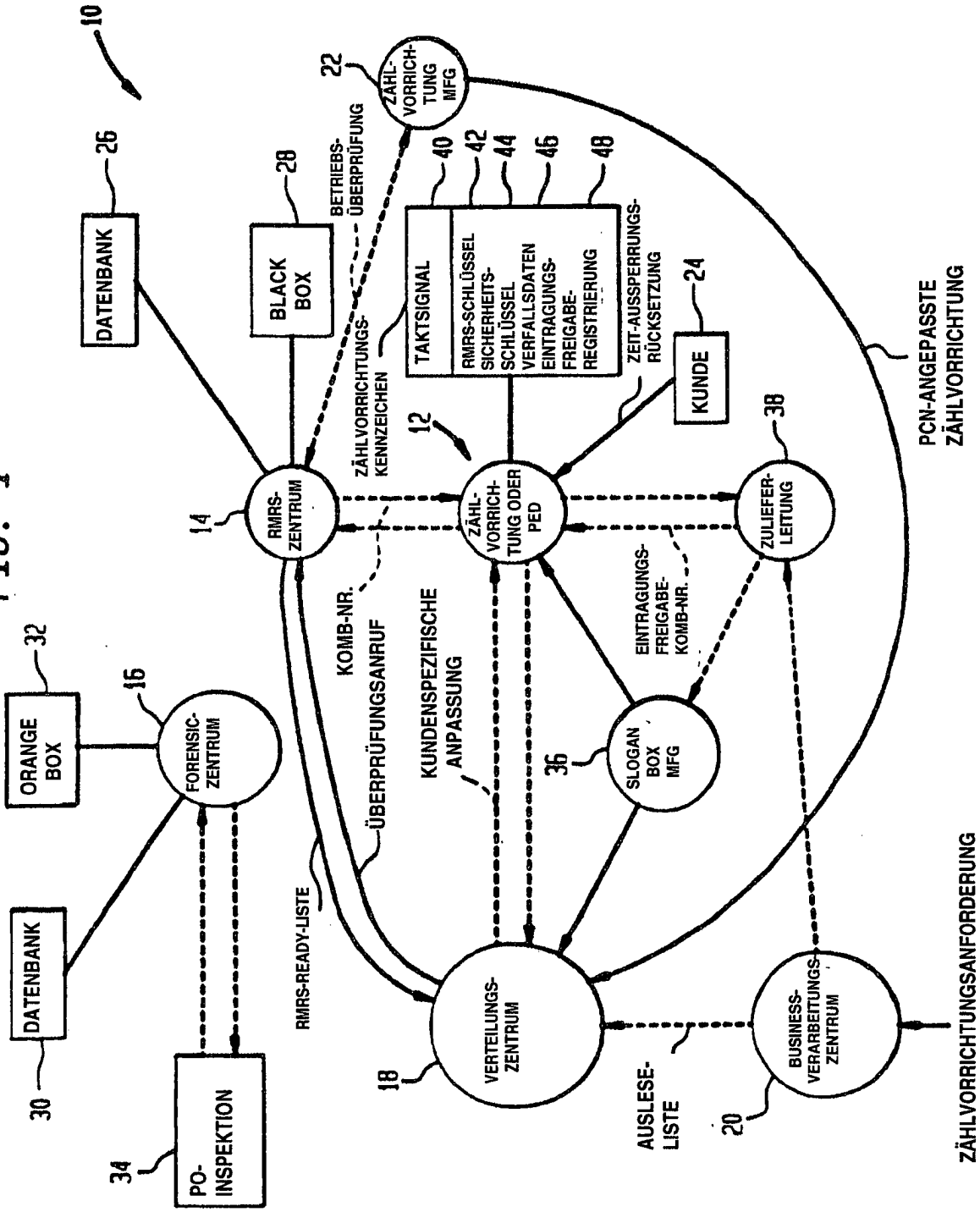

FIG. 2A

PED ID	PS-DES ZEIGER	PS-DES (JULIANISCHES DATUM,PORTO, SENDUNGSNUMMER, PED-ID)	VERKÄUFER ECODE	FEHLER-ERFASSUNG
1234567	89	0123456789012345789	012	2

FIG. 2B

PED ID	PS-DES (JULIANISCHES DATUM,PORTO, SENDUNGSNUMMER, PED-ID)	VERKÄUFER ECODE	FEHLER-ERFASSUNG
1234567	0123456789012345789	012	9

FIG. 3A

PED ID	PS-DES ZEIGER	JULIANISCHE DATUM	PORTO	SENDUNGS-NUMMER	PS-ECODE	VERKÄUFER ECODE	FEHLER-ERFASSUNG
1234567	89	01	.0290	678901	234	567	5

FIG. 3B

PED ID	JULIANISCHE DATUM	PORTO	SENDUNGS-NUMMER	PS-ECODE	VERKÄUFER ECODE	FEHLER-ERFASSUNG
1234567	01	.0290	678901	234	567	2

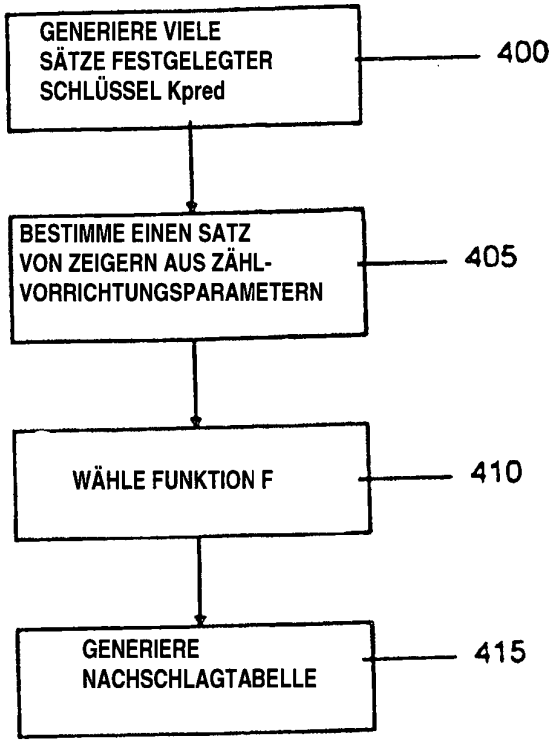

FIG. 4
SCHLÜSSEL-VERWALTUNG

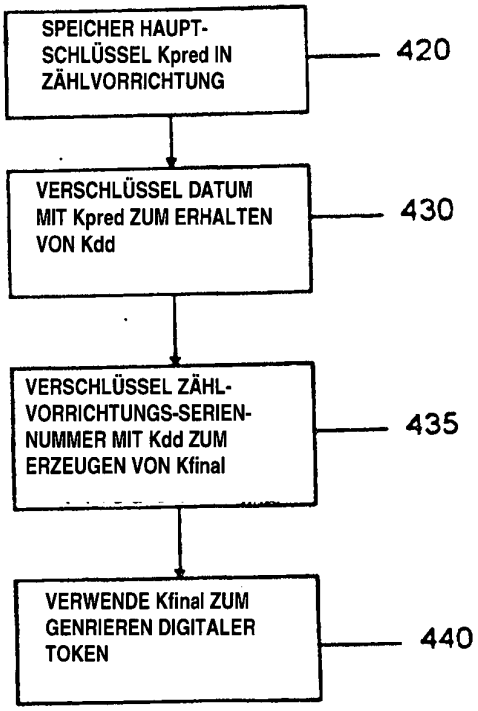

FIG. 5
ZÄHLVORRICHTUNGSBETRIEB

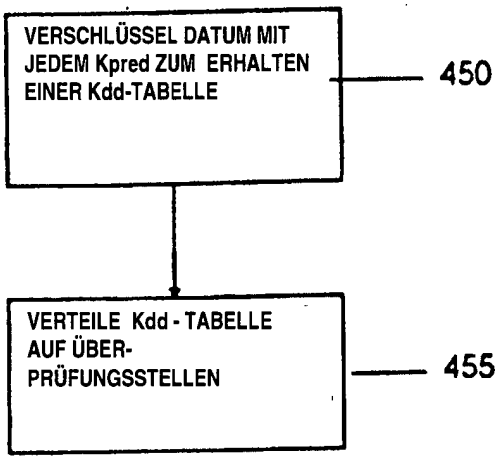

FIG. 7
DATENZENTRUMSBETRIEB

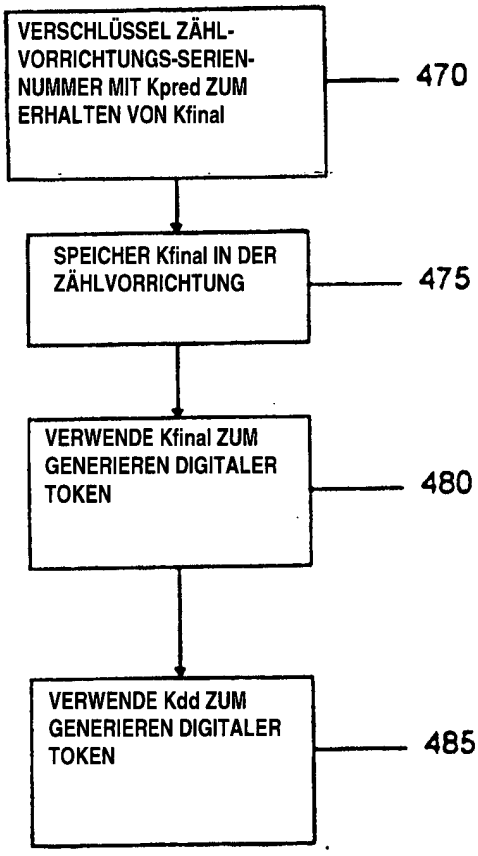

FIG. 6
ALTERNATIVER ZÄHLVORRICHTUNGSBETRIEB

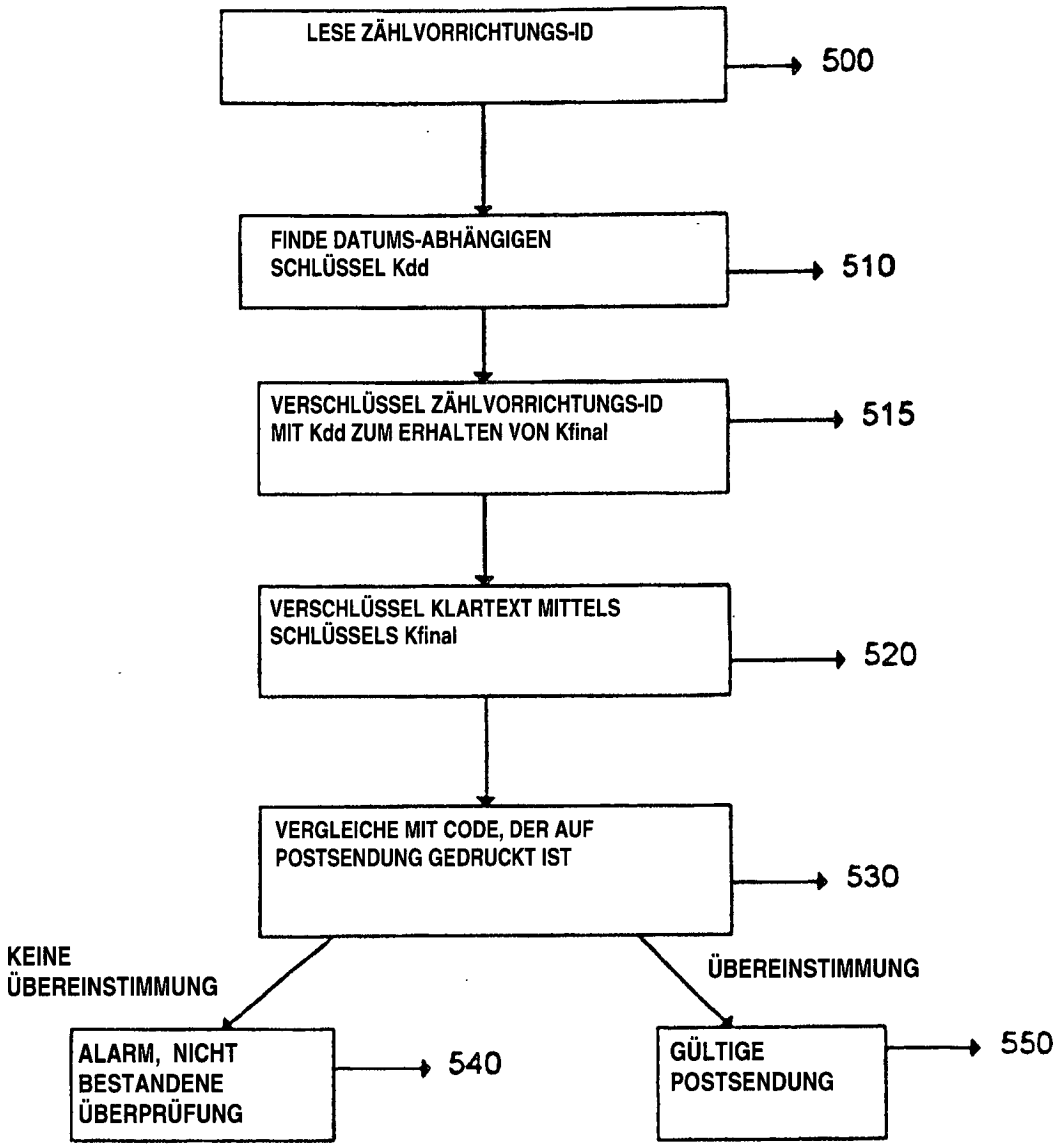

FIG. 8

ÜBERPRÜFUNG

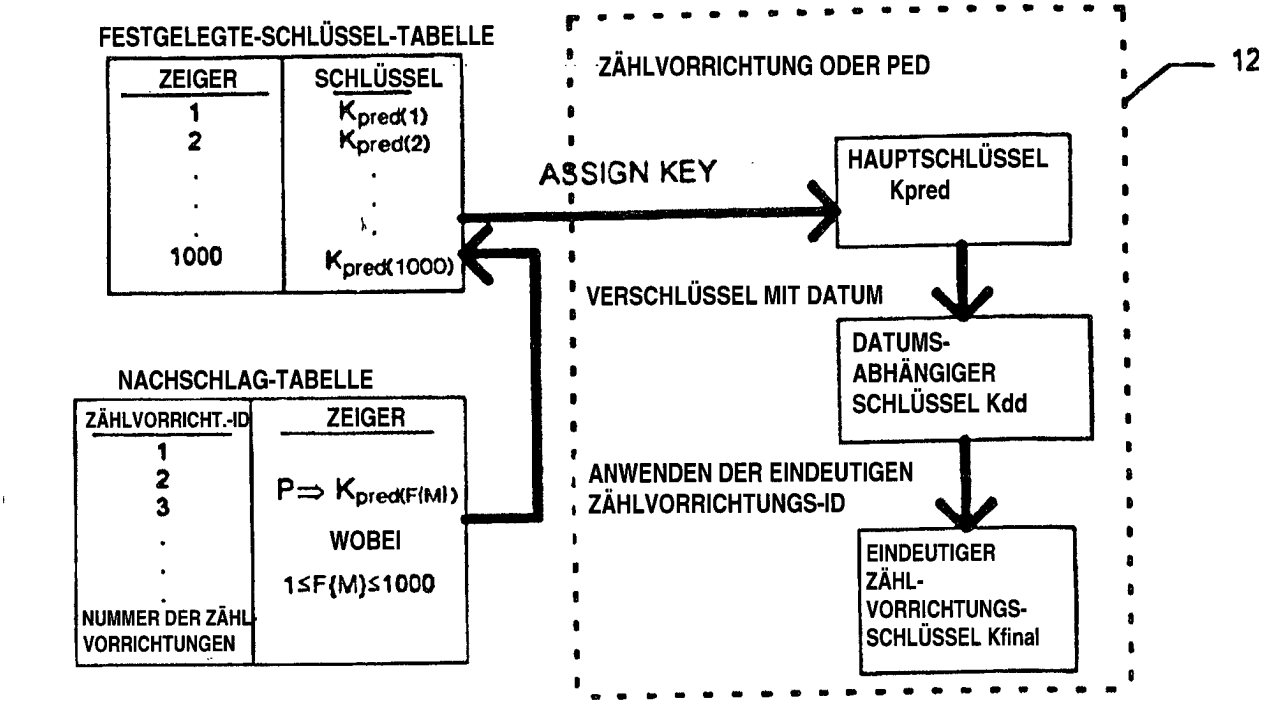
FESTGELEGTE-SCHLÜSSEL-TABELLE
ZEIGER
SCHLÜSSEL
1
2
1000
Kpred(1)
Kpred(2)
Kpred(1000)
ZÄHLVORRICHTUNG ODER PED
12
ASSIGN KEY
HAUPTSCHLÜSSEL
Kpred
VERSCHLÜSSEL MIT DATUM
DATUMS-
ABHÄNGIGER
SCHLÜSSEL Kdd
ANWENDEN DER EINDEUTIGEN
ZÄHLVORRICHTUNGS-ID
EINDEUTIGER
ZÄHL-
VORRICHTUNGS-
SCHLÜSSEL Kfinal
NACHSCHLAG-TABELLE
ZÄHLVORRICHT.-ID
ZEIGER
1
2
3
P⇒ Kpred(F(M))
WOBEI
1≤F(M)≤1000
NUMMER DER ZÄHL-
VORRICHTUNGEN

FIG. 9

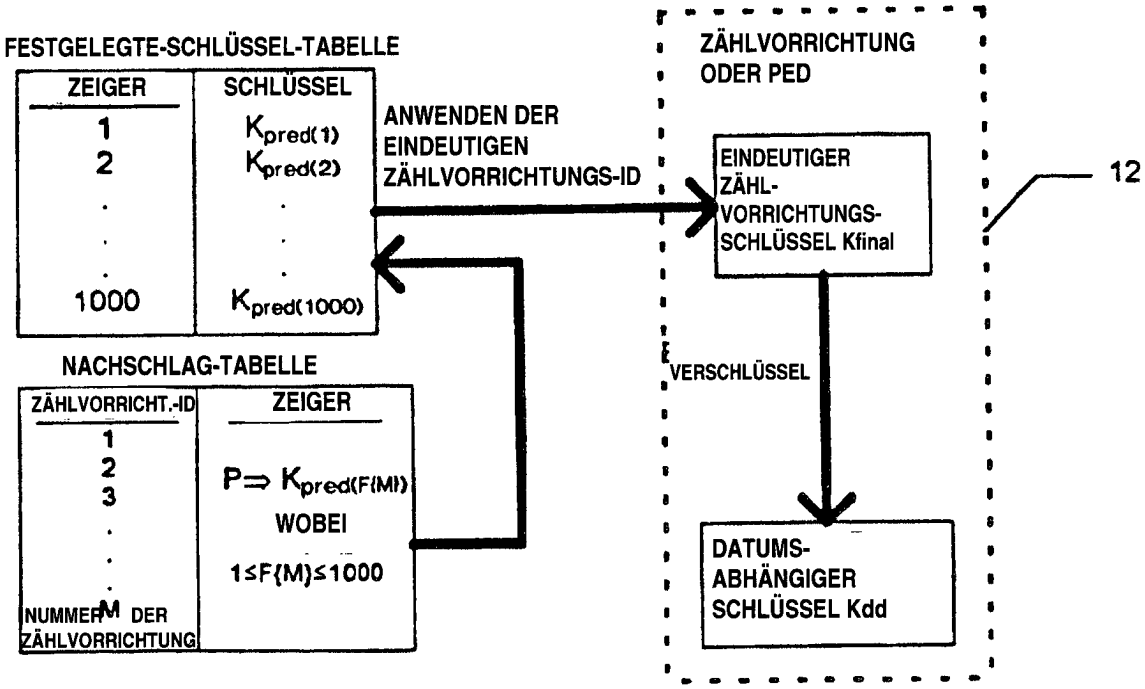
FESTGELEGTE-SCHLÜSSEL-TABELLE
ZEIGER
SCHLÜSSEL
1
2
1000
Kpred(1)
Kpred(2)
Kpred(1000)
ANWENDEN DER
EINDEUTIGEN
ZÄHLVORRICHTUNGS-ID
ZÄHLVORRICHTUNG
ODER PED
EINDEUTIGER
ZÄHL-
VORRICHTUNGS-
SCHLÜSSEL Kfinal
12
VERSCHLÜSSEL
DATUMS-
ABHÄNGIGER
SCHLÜSSEL Kdd
NACHSCHLAG-TABELLE
ZÄHLVORRICHT.-ID
ZEIGER
1
2
3
P⇒ Kpred(F(M))
WOBEI
1≤F(M)≤1000
NUMMER M DER
ZÄHLVORRICHTUNG

FIG. 10