(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 762 337 A2

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
12.03.1997 Patentblatt 1997/11

(51) Int. Cl.[6]: **G07B 17/04**

(21) Anmeldenummer: **96250191.2**

(22) Anmeldetag: **06.09.1996**

(84) Benannte Vertragsstaaten:
CH DE FR GB IT LI

(30) Priorität: **08.09.1995 DE 19534527**
08.09.1995 DE 19534529

(71) Anmelder: **Francotyp-Postalia Aktiengesellschaft & Co.**
16547 Birkenwerder (DE)

(72) Erfinder:
- **Kubatzki, Ralf**
  10405 Berlin (DE)
- **Thiel, Wolfgang, Dr.**
  13503 Berlin (DE)

(54) Verfahren und Anordnung zur Erhöhung der Manipulationssicherheit von kritischen Daten

(57) Ein Verfahren zur Erhöhung der Manipulationssicherheit von kritischen Registerdaten umfaßt die Schritte:

- Laden eines Codewortes, eines Zeigers oder MAC's, welcher einem Codewortes zugeordnet ist, in einen ersten nichtflüchtigen Speicher (20 bzw. 25), der gegen Herausnahme und Manipulation abgesichert ist,
- Laden eines Codewortes oder eines mittels des Codewortes gebildeten MAC's in zweite die Postregisterdaten enthaltende zu schützende nichtflüchtige Speicher (NVM 5a, 5b), wobei das Codewort dem letzten Betriebszustand der Frankiermaschine zugeordnet ist,
- Gültigkeitsprüfung des Codewortes oder des mittels des Codewortes gebildeten MAC's mindestens zum Zeitpunkt des Einschaltens der Frankiermaschine und nachfolgend mindestens aufgrund einer Pseudozufallsfolge in Abständen,
- Ersetzen des alten Codewortes durch ein vorbestimmtes neues Codewort, wenn der Prozessor, nach Gültigkeitsprüfung die Gültigkeit des alten Codewortes oder oder die Gültigkeit des mittels des Codewortes gebildeten MAC's anerkennt oder
- Blockierung der Frankiermaschine nach dem Zeitpunkt des Einschaltens der Frankiermaschine, wenn der Prozessor nach Gültigkeitsprüfung die Gültigkeit des alten Codewortes oder die Gültigkeit des mittels des Codewortes gebildeten MAC's aberkennt.

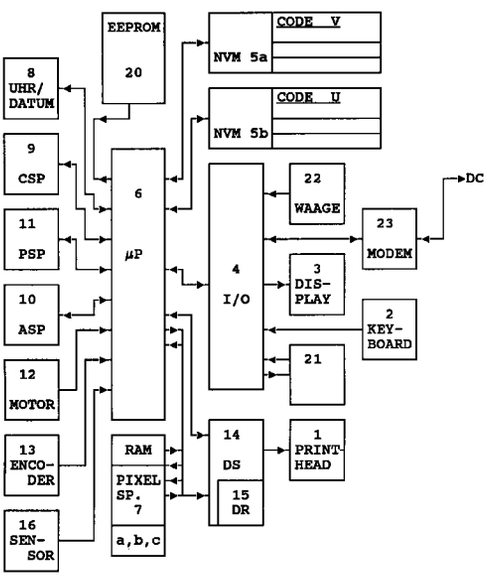

Fig. 1a

EP 0 762 337 A2

Beschreibung

Die Erfindung betrifft ein Verfahren und Anordnung zur Erhöhung der Manipulationssicherheit von kritischen Daten, welche in informationsverarbeitenden Einrichtungen vor einer Manipulation geschützt werden müssen, insbesondere von kritischen Registerdaten in elektronischen Frankiermaschinen oder in einer anderen elektronischen Einrichtung, in welcher sicherheitsrelevante Daten gehändelt werden bzw. in der eine Abrechnung von geldwerten Daten vorgenommen wird.

Frankiermaschinen sind, mit mindestens einem Eingabemittel, einem Steuermodul, einem Speichermittel und einem Druckermodul ausgerüstet. Im Speichermittel werden nichtflüchtig Daten gespeichert, welche zum Betrieb der Frankiermaschine erforderlich sind sowie Daten, welche Geldmitteln entsprechen.

Die Frankiermaschinentypen unterscheiden sich in Form und Ausstattung entsprechend des zu bearbeitenden Postaufkommens. Sollen aber verschiedene Typen an Frankiermaschinen produziert werden dann müssen eine Vielzahl an Schaltkreisen (ASIC's oder/ und andere Bauelemente) vorgesehen werden. Gerade die Vielzahl an Bauelementen und Schaltkreisen bietet dann Ansatzpunkte für eine Manipulation, wenn kein alternativer Aufwand getrieben oder ein Sicherheitsgehäuse eingesetzt wird.

Aus dem EP 465 236 A2 ist ein ASIC bekannt, welches eine Schaltung zur Drucksteuerung zur Motorsteuerung und zur Abrechnung umfaßt. Die Schaltung zur Drucksteuerung umfaßt einen Speicher für feste und einen anderen für variable Daten, welche mit den festen Daten überlagert werden. Ein Motorcontroller ist für ein Aktuieren eines Motorantriebes in Abhängigkeit von der Poststückzuführung vorgesehen. Ein Vorteil ist zweifellos die hohe Manipulationssicherheit aufgrund der Verwendung eines einzigen ASIC, d.h. resultierend allein bereits aus der eingeschränkten Anzahl an Ansatzpunkten für eine Manipulation. Ein Nachteil der Verwendung eines einzigen ASICs ist die schlechte Verwendbarkeit für unterschiedliche Frankiermaschinen, welche einen unterschiedlichen Drucker und Steuermodul je nach Art des realisierten Frankiermaschinensystems bzw. Poststraße aufweisen.

Aus der US 4 858 138 ist ein modulares System für eine Frankiermaschine mit Meter/Base-Trennung bekannt, wobei ein Sicherheitsmodul (Meter) mit einem Drucksteuermodul (Base) gekoppelt ist. Das Sicherheitsmodul kann Kreditkartenform aufweisen. Als elektrische Verbindungseinrichtung zum Drucksteuermodul dient hierbei ein als parallele CPU-Schnittstelle ausgebildeter Hochgeschwindigkeitskommunikationsbus. Der Drucksteuermodul weist einen Hochgeschwindigkeitsdrucker auf. Von der Tastatur des Drucksteuermoduls eingegebene Portobetrag wird zum Sicherheitsmodul übertragen. Der Sicherheitsmodul liefert eine digitale Darstellung des festen Teils des Postwertzeichens und eine verschlüsselte Gültigkeitsnummer. Die Gültigkeitsnummer umfaßt den Portobetrag und ggf. weitere Informationen, wie die Frankiermaschinenseriennummer und das Datum. Die verschlüsselte Gültigkeitsnummer ist geeignet, um ein illegales Drucken eines Geldbetrages, der nicht berechnet wurde, festzustellen. Die Fälschungsicherheit beruht auf einer in einer Sicherheitslogik vorgenommenen Verschlüsselung einer Gültigkeitsnummer, die über eine CPU-Schnittstelle übertragen wird. Diese Lösung bringt aber keinen Vorteil bei Manipulationen, welche im Sicherheitsmodul bzw. am Bus zwischen den Postwertspeichern und der Sicherheitslogik vorgenommen werden. Ein Nachteil ist hier, daß als einziger Schutz nur das Sicherheitsgehäuse des Sicherheitsmoduls vorgesehen ist. Nachteilig ist auch die hohe Anzahl der Leitungen der Meter/Base-Verbindung an der Schnittstelle zur Base und daß eine teure Hochgeschwindigkeitsschnittstelle erforderlich ist.

Eine weitere Manipulationsmöglichkeit besteht während der Dateneingabe beim Nachladen der Frankiermaschine mit einem Guthaben. In üblicher Weise wird von einer Datenzentrale bzw. von einem Speicher eines Übertragungsmittels, vorzugsweise einer Chipkarte, ein Guthaben geladen. Davon werden die durch die Frankiermaschine verbrauchten Portobeträge abgebucht.

Zur Sicherheit gegen betrügerische Manipulationen ist bereits weiterhin aus der DE 38 23 719 bekannt, ein repräsentatives Zeichenmuster ab einem bestimmten Datum auszudrucken. Bei der Prüfung der Post wird im Postamt das Druckdatum und das Zeichen mit dem Muster verglichen, das für dieses Datum berechtigt ist. Zum Drucken dient eine Berechtigungsvorrichtung, die eine Speichervorrichtung zur Speicherung einer Anzahl Zeichenmuster- und Datumsdaten aufweist. Die Daten, die das repräsentative Zeichenmuster einem definierten Datum zuordnen, werden über eine Fernwertvorgabe mittels einer externen Wahlvorrichtung dann aktualisiert, wenn die Anwender der Frankiermaschinen um eine Rekreditierung nachsuchen. Die Sicherheit der Daten beruht auf dem Prüfen der Daten in der Datenzentrale bevor ein Nachladen erfolgt und im Prüfen der Frankieraodrucke seitens der Postbehörde. Die Datenzentrale trägt somit zur Erhöhung der Manipulationssicherheit von kritischen Registerdaten bei. Dieses Sicherheitssystem ist jedoch auf Festnetze beschränkt und für tragbare Frankiermaschinen, die von einem Ort zu einem anderen Ort mitgeführt werden (mobiles Büro) nicht anwendbar. Eine Selbstprüfung seitens der Frankiermaschine auf Manipulation ist nicht vorgesehen.

Ein Portorechner, welcher aus dem Gewicht des Poststückes den gültigen Portobetrag bestimmt, ist gewöhnlich bereits in der an die Frankiermaschine angeschlossenen Waage integriert. Jedoch wurden auch schon Lösungen mit einem in die Frankiermaschine integrierten Portorechner vorgeschlagen. Einer Portogebührentabelle ist die für das Poststück erforderliche Portogebühr entnehmbar.

Beispielsweise weist eine aus der DE 42 13 278 A1

bekannte transportierbare Frankiermaschine Speichermittel und mit diesen in Verbindung stehende Empfangsmittel für über ein Übertragungsmittel übertragbare Daten auf. Das Speichermittel der Frankiermaschine weist aktualisierbare Abschnitte für an bestimmte Bedingungen geknüpfte Tabellen auf, beispielsweise für mindestens eine aktuelle Portogebührentabelle, anhand derer die jeweilige Portogebühr ermittelt wird. Die Frankiermaschine weist im Steuermodul erste Mittel auf, die bei Inbetriebnahme der Frankiermaschine mindestens eine Portogebührentabelle für die Frankiermaschine aus dem Speicher des Übertragungsmittels über die Empfangsmittel in einen vorbestimmten Speicherraum des Speichermittels laden. Sie enthält zweite Mittel im Steuermodul, die mittels der über dritte Mittel eingegebenen Bedingungen anhand des bereits eingegebenen Absendelandes bzw. - ortes und des Datums die aktuelle in Kraft befindliche Portogebührentabelle auswählen, um diese zu laden. Diese ersten und zweiten Mittel sind hardware- und/oder softwaremäßig als ein fest- oder freiprogrammierbarer Logikmodul bzw. Programm einer Mikroprozessorsteuerung ausgebildet und bewirken bei jedem Einschalten eine Verbindungsaufnahme zum externen Speicher.

Solche aktualisierbaren Abschnitte des Speichermittels sind ebenfalls für andere Informationen und/oder Zusatzinformationen vorgesehen. Insbesondere kann die Sicherheit vor betrügerischen Manipulationen dadurch erhöht werden, daß bei der Aktualisierung eine dem Aktualisierungsdatum zugeordnete Anzahl von Funktionen in die Frankiermaschine ladbar sind und die weiteren zu ladenden auslösbaren Funktionen vielfältig und nicht wählbar vorgegeben sind. Zur Sicherheit gegen betrügerische Manipulationen kann von der nationalen Postbehörde, zu der der jeweilige Absendeort gehört, ein nur von der jeweiligen nationalen Postbehörde maschinenlesbarer Ausdruck vorgegeben sein. Dieser Ausdruck kann beispielsweise die Transaktionsnummer für eine Berechtigungprüfung in Strichcodedarstellung sein oder ein anderes vereinbartes Zeichen, welches unter Verwendung des gleichen oder weiteren Druckers an einer definierten Stelle auf dem Postgut abgedruckt wird.

Solche Sicherheitsmaßnahmen sind geeignet den Einsatz eines Farbkopierers zur unerlaubten Vervielfälltigung eines Frankierabdruckes zu vereiteln. Sie können jedoch nicht die innere Manipulationssicherheit der Daten in der Frankiermaschine erhöhen.

Einige der Postbehörden fordern ein redundantes Abspeichern von Abrechnungsdaten in Speichern von unterschiedlicher Technologie. Jede Technologie ist mit spezifischen Vor- und Nachteilen behaftet. Einige Halbleiterspeicher benötigen keine Batterie, um eine Ladung über viele Jahre zu speichern. Sie haben aber zu wenig Speicherkapazität. Elektrisch programmierbare nichtflüchtige Speicher, welche keine Beschränkungen durch eine gegrenzte Batterielebensdauer haben, sind beispielsweise E^2PROM's. Der Nachteil der E^2PROM's besteht in der beschränkten Anzahl an zulässigen Schreib/Lesezyklen. Bei Überschreitung der zulässigen Anzahl an Schreib/Lesezyklen, können Fehler in einem benutzten Speicherbereich auftreten.

Im EP 457 114 B1 wurde eine Frankiermaschine mit nichtflüchtiger Speicherung von Abrechnungsdaten vorgeschlagen, wobei jeder Abrechnungsdatensatz einen Anfangsabschnitt mit Stückzahldaten enthält. Über die Anfangsabschnitte läßt sich der aktuelle Datensatz bestimmen. Bei einem Fehler in einem benutztem Speicherbereich wird auf einen anderen bisher ungenutzten Speicherbereich umgeschaltet, um den Datensatz abzuspeichern. Somit ist ein EPROM um so länger benutzbar, je mehr ungenutzte Speicherbereiche im Speicher noch vorrätig sind. Das beschränkt aber die Anzahl an zu speichernden Daten.

Gewöhnlich werden in Frankiermaschinen batteriegestützte CMOS-RAM's verwendet, um die Abrechnungsdaten in den Postregistern nichtflüchtig zu speichern. Nur begrenzt durch die Batterielebensdauer, können die Abrechnungsdaten beliebig oft gespeichert werden. Wenn eine Batterie für CMOS-RAM's gewechselt werden muß, müssen die Daten auf einen anderen Speicher, beispielsweise auf einem anderen batteriegestützten CMOS-RAM kopiert werden. Dieses Kopieren aller Daten von einem Speicher auf einen anderen Speicher wird auch als Klonen bezeichnet. Der neue batteriegestützte CMOS-RAM oder der alte batteriegestützte CMOS-RAM mit ausgewechselter bzw. erneuerter Batterie sind beide voll einsetzbar, wenn in ihren Speicherbereichen alle Daten identisch vorhanden sind. Durch Klonen könnten bei geöffneten Gehäuse auch unbefugte Personen beliebig viele Speicher mit identischen Dateninhalten versehen.

Damit nicht unbefugt die Speicherinhalte geklont wiederverwertet werden, müßte aber die Abrechnungseinheit wieder mit einem Sicherheitsgehäuse ausgerüstet werden. Andererseits ist dann aber dadurch weiterhin der Austausch defekter Bauelemente erschwert.

In der EP 560 714 A2 sind die Montageeinheiten durch ein Sicherheitsgehäuse gekapselt. Zur fälschungssicheren Übertragung von Abrechnungsdaten von einem Speicher in einer defekten Montageeinheit auf den Speicher einer in die Frankiermaschine neu eingesetzten Montageeinheit wird jede Montageeinheit mit zwei Steckereinheiten ausgerüstet. Zunächst wird der Datenfluß durch eine besondere Übertragungsleitung einer ersten Steckereinheit geschlauft, wobei aber an der gleichen ersten Steckereinheit der alten Montageeinheit die Schlaufung entfernt und der normale Datenfluß unterbrochen und umgeleitet ist. Vom Speicher der alten Montageeinheit wird über die letztgenannte Stekkereinheit und mittels einer zweiten Steckereinheit der neuen Montageeinheit der Datenfluß auf die neue Montageeinheit umgeleitet. Es sind mechanische Verriegelungsglieder vorgesehen, welche in Wirkverbindung mit einem eine elektronische Erkennungsmarke (Flag) setzenden Schalters stehen, welcher beim Herausnehmen der defekten Montageeinheit betätigt wird. Nach dem

Übertragen der Daten auf die neue Montageeinheit wird ein zweites unlöschbares Flag gesetzt, so daß eine zweite Datenübertragung unmöglich gemacht ist. Die Sicherheit beruht im wesentlichen auf der Kapselung von CPU und nichtflüchtigem Speicher auf der Montageeinheit und dem vorgenannten Schalter zum Setzen der Flags. Bei Kenntnis der Lage bzw. Anordnung des Schalters kann ein Eindringen und eine Manipulation in Fälschungsabsicht aber nicht verhindert werden.

Aus der DE 41 29 302 A1 ist die Verwendung eines Sensors bekannt, welcher beim Öffnen des Frankiermaschinengehäuses die Postregister löscht. Jedoch kann damit nicht verhindert werden, daß neue Daten in das Postregister von einem geschickten Manipulator eingeschrieben werden können, wenn das Gehäuse erst einmal geöffnet ist.

Aus der EP 231 452 A2 ist das periodische Abfragen von Sensoren entsprechend einer Softwareroutine einer CPU bekannt. Der Nachteil dieser Lösung besteht in einer hohen Rechenzeit bedingt durch das periodische Abtasten der Sensoren. Dieser Nachteil wird noch vergrößert, wenn es sich um eine besonders zeitkritische Abfrage handelt. Um möglichst schnell auf eine Zustandsänderung reagieren zu können, muß die Abfragefrequenz hoch gewählt werden. Somit verbringt der Mikroprozessor einen großen Anteil seiner Rechenzeit mit der Abfrage. Insbesondere kann nicht die Manipulation einer ausgeschalteten Maschine verhindert werden. Ebenfalls in der EP 231 452 A2 wird von einer redundanten Abspeicherung von Abrechnungsdaten ausgegangen. Da eine Kontrolle der abgespeicherten Registerwerte nicht alle Fehler festzustellen gestattet, wurden separate Adreß- und Datenleitungen jeweils für zwei redundante Speicher eingesetzt. Dadurch wird das Auftreten von bisher nicht entdeckbaren Fehlerbedingungen reduziert, die aufgrund von Fehlfunktionen der Maschine oder durch Spannungsausfall entstehen können. Fälschungen aufgrund einer unbefugten Manipulation, d.h. wenn beim Klonen der Postregister vom Orginal die Abrechnungsdaten insgesamt kopiert werden, sind aber durch vorgenannte Maßnahmen nicht feststellbar, denn die Kopie und Orginal sind voreinander ununterscheidbar.

Es wurde bereits in der DE 42 17 830 A1 ein Verfahren zum Betreiben einer Datenverarbeitungsanlage mit einem ersten nichtflüchtigen Speicher, einem Zustandsspeicher und einem zweiten nichtflüchtigen Speicher vorgeschlagen. Eine Modulkennung ermöglicht die Fortsetzung des Programms und eine Zustandskennung ermöglicht die Bearbeitung und Fortsetzung des Programmsabschnitts bei dem eine Programmunterbrechung eintrat, d.h. ggf. die Korrektur fehlerhaft eingeschreibener Daten in einem NVM aufgrund redundant vorliegender Daten in dem anderen NVM. Diese Lösung kann aber nicht den Dateninhalt, auf Vorliegen einer Manipulation überprüfen. Beim Klonen von Speicherinhalten werden korrekte Daten auf externe Speicher überspielt. Beim Rückübertragen dieser Speicherinhalte bzw. beim Einsatz dieser externen Speicher in die Frankiermaschine zu einem späteren Zeitpunkt wird ein von der Frankiermaschine selbst nicht als fehlerhaft erkennbarer Zustand wiederhergestellt, der zu einem früheren Zeitpunkt einmal korrekt war.

Es ist bereits ein Verfahren zur Verbesserung der Sicherheit von Frankiermaschinen vorgeschlagen worden (DE 43 44 476 A2) indem die Frankiermaschine zwischen autorisierten und unautorisierten Eingriff bzw. Öffnen ihres Gehäuses unterscheiden kann. Das Verfahren setzt aber voraus, daß die Frankiermaschine ständig mit Energie für die Selbstprüfung versorgt wird. In diesem Fall können keine sicherheitsrelevanten Daten aus der Frankiermaschine unerlaubt herausgeladen, abgenommen oder eingespeist werden, ohne daß dies im Rahmen der Selbstprüfung bemerkt würde. Dennoch sind zusätzliche Gehäuse, Siegel und/oder weitere Sicherheitsmaßnahmen erforderlich zum Schutz der ausgeschalteten Maschine.

Vielfach wird die Forderung erhoben, daß für Reparaturzwecke die Speicherbausteine leicht austauschbar sind, also weder gekapselt noch fest eingelötet sondern gesockelt werden. Nun wäre es damit aber nicht möglich, die tragbaren, d.h. die nicht fest über ein Telefonnetz installierten Frankiermaschinen im ausgeschalteten Zustand gegenüber betrügerischen Manipulationen abzusichern. Im Interesse der Manipulationssicherheit von kritischen Registerdaten muß bisher auf Verbesserungen beim Service für die Maschine verzichtet werden.

Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren zur Erhöhung der Manipulationssicherheit von kritischen Registerdaten zu entwickeln, welche die Nachteile des Standes der Technik vermeidet und für eine Vielzahl an Frankiermaschinenvarianten kostengünstig realisierbar ist, ohne dabei die Manipulationssicherheit zu vermindern.

Eine weitere Aufgabe ist es, bei einer Anordnung zum Frankieren von Postgut, vorzugsweise einer tragbaren ortsunabhängig betreibbaren Frankiermaschine der eingangs genannten Gattung eine Sicherheit gegen betrügerische Manipulationen jeder Art und ein Frankieren nach gültigen Posttarifen in Abhängigkeit von dem eingebbaren Gewicht und Format des Postgutes zu gewährleisten. Auch bei ausgeschalteter Frankiermaschine und ohne Stromversorgung soll die frankiermaschineninterne Sicherheitsschaltung für Postregisterdaten und andere sicherheitsrelevante Daten wirksam sein.

Die Aufgabe wird mit den Merkmalen der Ansprüche 1, 8, 22, 24 bzw. 25 gelöst.

Die Erfindung geht davon aus, daß ein Duplizieren bzw. Klonen des zu schützenden nichtflüchtigen Speichers NVM nicht verhindert werden braucht, sondern auch ein Duplikat des Speicherinhalts, welches gegen den Speicherinhalt des Orginals ausgetauscht wird, weiterverwendet werden kann. Im Reparaturfall wird oft ein Kopieren und Rücktausch der Speicherinhalte erforderlich, wobei allerdings vorausgesetzt wird, daß zwi-

schenzeitlich keine gültigen Frankierungen vorgenommen werden.

Erfindungsgemäß wird ein interner Prozessorspeicher verwendet, um ein Codewort nichtflüchtig zu speichern. Es ist vorgesehen, daß jedem zu schützenden nichtflüchtigen Speicher oder Speicherbereich ein separates Codewort zugeordnet wird, wobei mindestens eines der vorgenannten separaten Codeworte in einem weiteren internen Speicher eines Prozessorsystems, einer Chipkarte und/oder in einem ähnlichen System nichtflüchtig gespeichert worden ist und daß eine Bildung von neuen Codewörtern ab einem vorbestimmten Zeitpunkt und danach eine Einspeicherung der neuen Codewörtern in die vorgenannten nichtflüchtigen Speicher vorgenommen wird.

Die erfindungsgemäße Lösung verhindert also nicht, daß die Postregister einschließlich Inhalt entfernt werden, um beliebig viele Kopien anzufertigen, sondern sie verhindert, daß mit Hilfe dieser Kopien Postgüter frankiert werden können, ohne daß eine adäquate Abrechnung bei der Datenzentrale bzw. Bezahlung bei der Post vorgenommen wird. Eine Verkapselung der Bauelemente für die herausnehmbaren die Postregister speichernden NV-RAMs mit einem Sicherheitsgehäuse oder das Vorsehen anderer zusätzlicher Maßnahmen zum Schutz vor Entnahme, wie Aufkleben auf die Leiterplatte, Versiegeln oder Vergießen mit Epoxidharz sind nun nicht erforderlich.

Die frankiermaschineninterne Sicherheitsschaltung für Postregisterdaten und andere sicherheitsrelevante Daten beruht auf nichtflüchtigen Speicherbausteinen. Bei der ausgeschalteten Frankiermaschine bzw. bei ausgefallener Stromversorgung bleiben die Daten gespeichert. Solche beispielsweise mit einer Lithiumbatterie gestützten CMOS-SRAM's sind während ihrer Lebensdauer von ca. 10 Jahren beliebig oft beschreibbar. Die Batterie kann weder nachgeladen noch entladen werden, ohne den Speicherbaustein zu zerstören. Es wird davon ausgegangen, daß im Leben einer Frankiermaschine bis zu 150 000 Abdrucke möglich sind und daß die Lithiumbatterie während dieser Zeit nicht ausgewechselt werden muß.

Ebenfalls können Speichermittel von anderer Speichertechnologie durch die Sicherheitsschaltung entsprechend vor Mißbrauch geschützt werden, wenn zu vorbestimmten Ereignissen sicherheitsrelevante Daten in diese nichtflüchtigen Speicher gespeichert werden.

Vom Herstellerwerk der Frankiermaschine wird in die nichtflüchtigen Speicherbausteine (Bat-NV-CMOS-SRAM's und E^2PROM) ein Codewort eingespeichert, welches einer vorbestimmten Frankiermaschine zugeordnet ist. Das Codewort kann am Anfang beispielsweise die Seriennummer der Frankiermaschine umfassen oder kann ein Teil einer anderen Nummer sein. Außerdem werden die Registerspeicherplätze mit Anfangswerten vom Herstellerwerk vorbesetzt.

Die erfindungsgemäße Lösung vermeidet, daß die nichtflüchtigen Speicher (NV-RAMs, E^2PROMs) in Fälschungsabsicht verwendet werden könnten, welche ausgewechselt und geklont wurden, um später mit den geklonten oder ausgewechselten NV-RAMs bzw. E^2PROMs die Frankiermaschine FM zu betreiben. Die Erfindung geht von einem OTP-Prozessor mit einem internen OPT-ROM und internen OTP-RAM aus. Im internen OPT-ROM ist eine Liste von Codewörtern gespeichert, wobei jedes Codewort zeitweise und möglichst nur einmal aktiv ist. Das Codewort wird unabhängig vom Speicherinhalt der NV-RAMs aus der Tabelle - die im von außen nicht zugänglichen internen ROM-Bereich des OTP gespeichert vorliegt - ausgewählt.

Das neue Codewort wird mindestens beim Einschalten der Frankiermaschine der internen OTP-Tabelle entnommen und in den nichtflüchtigen Speichern (NV-RAMs, E^2PROMs) abgespeichert, wenn das alte in der Liste das jeweilige Vorgänger-Codewort war.

Beispielsweise ist ein E^2PROM der einzige nichtflüchtige Speicher der zusammen mit dem OTP-Prozessor unlösbar fest auf die Platine aufgeklebt ist. In einer bevorzugten Varianten wird während des Betriebes der Frankiermaschine vor jedem Abdruck und damit vor jeder neu zu registrierenden Stückzahl an Frankieraufdrucken auf Basis der vorhergehenden Stückzahl und gegebenenfalls der aktuellen vom Uhren/Datumsbaustein gelieferten Zeit eine Zufallszahl erzeugt. Hierzu kann ein Pseudo-zufallsgenerator hard- und/oder softwaremäßig realisiert werden. Im internen OPT-ROM des OTP-Prozessors liegt mindestens eines aus der Vielzahl von möglichen erzeugbaren Zufallswörtern gespeichert vor. Nach einem Vergleich innerhalb des OTP-Prozessors wird bei Übereinstimmung eine redundante Speicherung des neuen Codewortes einmal in die lösbaren nichtflüchtigen Speicher (NVRAMs) und erfindungsgemäß auch in den vorgenannten unlösbar fest auf die Platine aufgeklebten nichtflüchtigen Speicher (E^2PROM) vorgenommen. Die zulässige Anzahl an Schreib/Lese-Zyklen für den E^2PROM wird nicht überschritten, wenn beispielsweise durchschnittlich nur jede vierunzwanzigste Frankierung die nichtflüchtigen Speicher (E^2PROM und NVRAMs) redundant mit einem neuen Codewort beschrieben werden.

Zusätzlich werden die nichtflüchtigen Speicher (E^2PROM und NVRAMs) redundant mit einem neuen Codewort auch bei einem anderen letzten Betriebszustand der Frankiermaschine beschrieben, welcher vorbestimmten Zuständen zugeordnet ist, wie dem Ergebnis der Herstellung oder einer Nachladung der Frankiermaschine bzw. dem Ausschalten bzw. vor Spannungsausfall oder einer Stillstandszeit (Stand by) bzw. Programmunterbrechung und entsprechend anderen Ereignissen.

Das Weiterschalten der im internen OPT-ROM gelisteten Codewörter wird über Flags oder Zeiger, die in dem unlösbar fest eingebauten nichtflüchtigen Speicher gespeichert sind, realisiert. Der Zeiger wird außerhalb des jeweils zu überprüfenden lösbar eingebauten nichtflüchtigen Speichers (NV-RAMs) in dem ständig eingebauten und/oder während der Laufzeit der Frankiermaschine mit ihrem Prozessorsystem in Kom-

munikationsverbindung stehenden und gegen Herausnahme während der Laufzeit der Frankiermaschine abgesicherten ersten Sicherheitsspeicher nichtflüchtig gespeichert. Zur Verhinderung von Manipulationen in Fälschungsabsicht des vorgenannten ständig eingebauten und gegen Herausnahme abgesicherten Sicherheitsspeicher sollten diese Flag oder Zeiger MAC-gesichert gespeichert sein.

Das Verfahren zur Erhöhung der Manipulationssicherheit von kritischen Registerdaten umfaßt in einer bevorzugten Variante die folgenden Schritte:

- Laden einer Zahl oder eines Zeigers, welcher einem Codewortes zugeordnet ist, in einen ersten nichtflüchtigen Speicher, der gegen Herausnahme und Manipulation abgesichert ist,
- Laden eines Codewortes in zweite die Postregisterdaten enthaltenden nichtflüchtigen Speicher (NVM), wobei das Codewort dem letzten Betriebszustand der Frankiermaschine zugeordnet ist bzw. vom Prozessor entsprechend ausgewählt worden ist,
- Gültigkeitsprüfung des Codewortes mindestens zum Zeitpunkt des Einschaltens der Frankiermaschine und nachfolgend aufgrund eines Ereignisses,
- Ersetzen des alten Codewortes durch ein vorbestimmtes neues Codewort, wenn der Prozessor, nach Gültigkeitsprüfung mit Bezug auf das in seinem internen Prozessorspeicher aus einer Liste mit gespeicherten Codewörten entsprechend der Zahl bzw. der Zeigerstellung ausgewählte Codewort, die Gültigkeit des alten Codewortes anerkennt oder
- Blockierung der Frankiermaschine nach dem Zeitpunkt des Einschaltens der Frankiermaschine, wenn der Prozessor nach Gültigkeitsprüfung mit Bezug auf das ausgewählte in vorgenannter Liste gespeicherte Codewort die Gültigkeit des alten Codewortes aberkennt.

Das Programm für die Auswahl des jeweils neuen Codewortes ist im internen Programmspeicher (internen OTP-ROM bzw. OTP-EPROM) gespeichert. Die Auswahl des neuen Codewortes wird vom vorherigen und/oder vom Zustand der Frankiermaschine zu einem vorbestimmten Zeitpunkt bzw. bei einer vorbestimmten Stückzahl abhängig durchgeführt. Jedem nichtflüchtigem Speicher oder Speicherbereich, der geschützt werden muß, kann ein separates Codewort zugeordnet werden. Das kann in der Frankiermaschine ermöglichen, eine automatische Analyse vorzunehmen, welcher Speicherbaustein aus einer Vielzahl an Speicherbausteinen entnommen wurde.

Der vorgenannte dem Codewort entsprechende letzte Betriebszustand der Frankiermaschine entspricht insbesondere einem Zustand im Ergebnis der Herstellung oder einer Nachladung der Frankiermaschine oder im Ergebnis der Bildung einer Pseudozufallsfolge oder einem Zustand vor dem Ausschalten der Frankiermaschine oder einem Zustand vor einem Spannungsausfall oder vor einer Stillstandszeit (Stand by) bzw. vor Programmunterbrechung. Es ist vorgesehen, daß die Gültigkeitsprüfung des Codewortes mindestens zum Zeitpunkt des Einschaltens der Frankiermaschine und nachfolgend mindestens aufgrund einer Pseudozufallsfolge durchgeführt wird.

Für eine Anordnung zur Erhöhung der Manipulationssicherheit von kritischen Daten, insbesondere von Registerdaten in Frankiermaschinen mit Eingabe- und Anzeigemitteln, einer Steuereinrichtung und Speichern, ist vorgesehen, daß die Steuereinrichtung einen Mikroprozessor oder einen OTP-Prozessor (ONE TIME PROGRAMMABLE) aufweist. Im OTP sind neben einem Mikroprozessor CPU auch weitere Schaltungen und/oder Programme bzw. Daten im internen OTP-ROM bzw. im internen OTP-RAM in einem gemeinsamen Bauelementgehäuse untergebracht, welche ein erstes Sicherheitsmittel gegen unbefugte Manipulation bilden. Es ist vorgesehen, daß ein erster und ein zweiter nichtflüchtiger Speicher mit der Steuereinrichtung verbunden sind, wobei der erste nichtflüchtige Speicher NVM ein zweites Sicherheitsmittel gegen unbefugte Manipulation bildet und gegen Herausnahme gesichert ist.

In einer Variante ist vorgesehen, daß der erste nichtflüchtige Speicher als interner Prozessorspeicher zur nichtflüchtigen Speicherung im Prozessor realisiert und damit gegen eine Herausnahme und Manipulation gesichert ist.

In einer anderen Variante ist der erste nichtflüchtige Speicher als externer nichtflüchtiger Speicher NVM mit dem Prozessor elektrisch und mechanisch unlösbar über eine Leiterplatte verbunden.

In einer weiteren Variante ist der externe nichtflüchtiger Speicher NVM über einen Ein/AusgabeSteuermodul am Prozessor angeschlossen und während der Laufzeit der Frankiermaschine gegen eine Herausnahme gesichert. Es ist auch vorgesehen, daß der externe nichtflüchtiger Speicher NVM Bestandteil einer Chipkarte ist und über eine Chipkarten-Schreib/Leseeinheit am Ein/Ausgabe-Steuermodul angeschlossen ist.

Ein alternatives Verfahren geht von einer speziellen Bildung von Codewörtern in der OTP-CPU aus. Eine Auflistung von Codewörtern im internen OTP-ROM ist dann unnötig. Das Verfahren zur Erhöhung der Manipulationssicherheit von kritischen Registerdaten umfaßt die Schritte:

- Laden eines Codewortes in einen ersten internen Prozessorspeicher zur nichtflüchtigen Speicherung und in zweite die Postregisterdaten enthaltene nichtflüchtige Speicher (NVM), wobei das Codewort dem letzten Betriebszustand der Frankiermaschine entspricht,
- Gültigkeitsprüfung des Codewortes mindestens zum Zeitpunkt des Einschaltens der Frankiermaschine und nachfolgend aufgrund eines Ereignis-

ses,

- Ersetzen des alten Codewortes durch ein vorbestimmtes neues Codewort, wenn der Prozessor nach Gültigkeitsprüfung mit Bezug auf das in seinem ersten ersten nichtflüchtigen internen Prozessorspeicher (NVM) gespeicherte Codewort die Gültigkeit des alten Codewortes anerkennt oder
- Blockierung der Frankiermaschine nach dem Zeitpunkt des Einschaltens der Frankiermaschine, wenn der Prozessor nach Gültigkeitsprüfung mit Bezug auf das in seinem ersten nichtflüchtigen internen Prozessorspeicher (NVM) gespeicherte Codewort die Gültigkeit des alten Codewortes aberkennt.

Das Programm für die Bildung des jeweils neuen Codewortes ist im Programmspeicher (internen ROM bzw. EPROM) gespeichert. Die Bildung des neuen Codewort ist vom vorherigen abhängig. Jedem nichtflüchtigem Speicher oder Speicherbereich kann ein separates Codewort zugeordnet werden, wobei (vorher oder gleichzeitig) mindestens eines der vorgenannten Codeworte erfindungsgemäß im internen Prozessorspeicher nichtflüchtig gespeichert worden ist.

Es ist weiterhin alternativ zur vorgenannten Codewortauflistung vorgesehen, daß in einem Schritt zur Bildung eines neuen veränderbaren einzigartigen ersten Codewortes auch die Bildung des neuen zweiten Codewortes identisch zur Bildung des neuen ersten Codewortes erfolgt, um ein identisches neues zweites Codewort in die zu schützenden nichtflüchtigen Speicher zu laden.

Alternativ ist in einer weiteren Variante vorgesehen, daß in einem Schritt zur Bildung eines neuen veränderbares einzigartigen ersten Codewortes auch die Bildung des neuen zweiten Codewortes als komplementärer Schatten zum neuen ersten Codewortes erfolgt, um ein komplementäres neues zweites Codewort in die zu schützenden nichtflüchtigen Speicher zu laden.

Es ist in einer anderen Variante vorgesehen, daß in einem Schritt zur Bildung eines neuen veränderbares einzigartigen ersten Codewortes auch die Bildung des neuen zweiten Codewortes als zu dem neuen veränderbaren einzigartigen ersten Codewort identischen Codewort und als komplementärer Schatten zum neuen ersten Codewortes erfolgt, um mindestens ein neues zweites Codewort in die zu schützenden nichtflüchtigen Speicher zu laden oder daß beim Schutz eines entsprechenden Speichers in mindestens einem der Speicherbereiche auch mit dem komplementären Schatten gearbeitet wird.

In Weiterführung der Erfindung kann das vorgenannte in zeitlichen oder stückzahlmäßigen Abständen geänderte Codewort auch zur MAC-Absicherung der Postregisterdaten verwendet werden. In den zu schützenden nichtflüchtigen Speichern wird dann statt des Codewortes der MAC gespeichert. Ein solches Verfahren zur Erhöhung der Manipulationssicherheit von kritischen Registerdaten ist gekennzeichnet **durch** die Schritte:

- Laden eines mittels einem Codewort erzeugten Autentifikationscodes (MAC_n), welcher dem Codewort zugeordnet ist, welches Abrechnungsdaten verschlüsselt, in einen ersten nichtflüchtigen Speicher, der während der Laufdauer der Maschine gegen eine Herausnahme und Manipulation gesichert ist,
- Laden der Abrechnungsdaten und des vorgenannten Autentifikationscodes (MAC_n) in zweite die Postregisterdaten enthaltende zu schützende nichtflüchtige Speicher NVM, wobei das Codewort dem letzten Betriebszustand der Maschine zugeordnet ist,
- Gültigkeitsprüfung des Autentifikationscodes (MAC_n), welcher dem Codewort zugeordnet ist, mindestens zum Zeitpunkt des Einschaltens der Maschine und nachfolgend aufgrund eines Ereignisses,
- Ersetzen des alten Codewortes durch ein vorbestimmtes neues Codewort zur Bildung eines weiteren Autentifikationscodes (MAC_{n+1}), welcher dem neuen Codewort zugeordnet ist, welches Abrechnungsdaten verschlüsselt, wenn der Prozessor die Gültigkeit des alten Codewortes anerkennt oder
- Blockierung der Maschine nach dem Zeitpunkt ihres Einschaltens, wenn der Prozessor nach Gültigkeitsprüfung die Gültigkeit des anhand des alten Codewortes geprüften Autentifikationscodes (MAC_n) aberkennt.

Die Abstände für das Laden eines MESSAGE AUTHENTIFICATION CODE (MAC) nach dem Zeitpunkt des Einschaltens der Frankiermaschine sind zeitliche oder stückzahlmäßige Abstände und/oder solche mindestens aufgrund einer Pseudozufallsfolge bestimmten Abstände.

Vorteilhafte Weiterbildungen der Erfindung sind in den Unteransprüchen gekennzeichnet bzw. werden nachstehend zusammen mit der Beschreibung der bevorzugten Ausführung der Erfindung anhand der Figuren näher dargestellt. Es zeigen:

Figur 1a, Blockschaltbild einer Frankiermaschine mit erfindungsgemäß erhöhter Sicherheit nach einer ersten Variante mit E^2PROM,

Figur 1b, Blockschaltbild einer Frankiermaschine mit erfindungsgemäß erhöhter Sicherheit nach einer zweiten Variante mit OTP-internem E^2PROM,

Figur 2a, Variante mit OTP-Prozessor ohne internen E^2PROM nach der ersten Variante,

Figur 2b, Variante mit OTP-Prozessor mit internem E^2PROM nach der ersten Variante,

Figur 3, Gesamtablaufplan für die Frankiermaschine,

Figur 4, Details des Ablaufplans nach Figur 3,

Figur 5, Ablaufplan für den Frankiermodus,

Figur 6, Details des Ablaufplans nach Figur 4,

Figur 7, Flußplan für das erfindungsgemäße Verfahren zur Erhöhung der Manipulationssicherheit,

Figur 8a bis c, Zeigerstellungen nach dem erfindungsgemäßen Verfahren der ersten Variante.

Die Figur 1a zeigt ein Blockschaltbild der erfindungsgemäßen Frankiermaschine mit einem Druckermodul 1 für ein vollelektronisch erzeugtes Frankierbild, mit mindestens einem mehrere Betätigungselemente aufweisenden Eingabemittel 2, einer Anzeigeeinheit 3, einem die Kommunikation mit einer Datenzentrale herstellenden MODEM 23, welche über einen Ein/Ausgabe-Steuermodul 4 mit einer Steuereinrichtung 6 gekoppelt sind und mit mindestens einem nichtflüchtigen Speicher 5a bzw. 5b für die variablen und einen Speicher 10, 11 für die konstanten Teile des Frankierbildes.

Ein Charakterspeicher 9 liefert die nötigen Druckdaten für einen flüchtigen Arbeitsspeicher 7. Der flüchtige Arbeitsspeicher 7 umfaßt beispielsweise einen externen RAM in Verbindung mit einem im Prozessor angeordneten internen RAM 6b. Die Steuereinrichtung 6 weist einen entsprechend ausgebildeten Mikroprozessor µP auf und ist mit dem Ein/Ausgabe-Steuermodul 4, dem Charakterspeicher 9, dem flüchtigen Arbeitsspeicher 7, mit einem nichtflüchtigen Kostenstellenspeicher NVM 5a und mit einem nichtflüchtigen Arbeitsspeicher NVM 5b, mit einem anwendungsspezifischen Programmspeicher ASP 10 (Klischee-EPROM), einem Programmspeicher PSP 11 (Programm-EPROM), mit dem Motor einer Transport- bzw. Vorschubvorrichtung ggf. mit Streifenauslösung 12, einem Encoder (Codierscheibe) 13, einem Briefsensor 16 sowie mit einem Uhren/Datums-Baustein 8 verbunden. Ein entsprechendes Verfahren zum Steuern eines spaltenweisen Drucks eines Postwertzeichenbildes ist beispielsweise in der EP 578 042 A2 oder in der EP 576 133 A2 ausführlicher beschrieben.

Bei dem in der Figur 1a gezeigten Blockschaltbild einer Frankiermaschine wird die erfindungsgemäß erhöhte Sicherheit in Verbindung mit einem E^2PROM 20, welcher sich extern vom Mikroprozessorgehäuse befindet, erzielt. Beide sind unlösbar auf der Platine befestigt.

Die - in der Figur 2a näher dargestellte - Steuereinrichtung 6 weist einen Mikroprozessor oder einen OTP-Prozessor (ONE TIME PROGRAMMABLE) auf. Im OTP sind neben einem Mikroprozessor CPU 6a auch weitere Schaltungen in einem gemeinsamen Bauelementgehäuse untergebracht. Diese weiteren Schaltungen und/oder Programme bzw. Daten im internen OTP-ROM 6c bzw. im internen OTP-RAM 6b in dem gemeinsamen Prozessorgehäuse bilden eine Sicherheitsschaltung bzw. ein erstes Sicherheitsmittel gegen unbefugte Manipulation. Der erste nichtflüchtige Speicher NVM 20 ist beispielsweise ein E^2PROM und dient als zweites Sicherheitsmittel gegen unbefugte Manipulation.

Es ist außerdem vorgesehen, daß ein externer nichtflüchtiger Speicher NVM 25 ein zweites Sicherheitsmittel gegen unbefugte Manipulation bildet und über einen Ein/Ausgabe-Steuermodul 4 am Prozessor 6 angeschlossen ist und während der Laufzeit der Frankiermaschine gegen Herausnahme gesichert ist.

Die übrigen einzelnen Speicher können in mehreren physikalisch getrennten oder in gemäß der Figur 2a gezeigten Weise in wenigen Bausteinen zusammengefaßt verwirkicht sein. Vorzugsweise sind die Festwertspeicher CSP 9 und PSP 11 in einem EPROM und die zu schützenden nichtflüchtigen Speicher NVM 5a und 5b in einem Postregisterspeicher zusammengefaßt. Letzterer ist vorzugsweise doppelt vorhanden und wird in seinen Speicherbereichen redundant mit Daten beschrieben. Ein Verfahren zum Speichern Sicherheitsrelevanter Daten ist beispielsweise in der EP 615 211 A1 näher ausgeführt.

Das in der Figur 1b gezeigte Blockschaltbild einer Frankiermaschine erzielt erfindungsgemäß eine erhöhte Sicherheit mit einem OTP-internem nichtflüchtigen Speicher (NVM), vorzugsweise einem E^2PROM 6d.

Die - in der Figur 2b näher dargestellte - Steuereinrichtung 6 weist einen Mikroprozessor oder einen OTP-Prozessor (ONE TIME PROGRAMMABLE) auf. Im OTP sind neben einem Mikroprozessor CPU 6a auch interne nichtflüchtige Speicher NVM 6d und weitere Schaltungen in einem gemeinsamen Bauelementgehäuse untergebracht. Der vorgenannte interne nichtflüchtige Speicher NVM 6d und weitere Schaltungen und/oder Programme bzw. Daten im internen OTP-ROM 6c bzw. internen OTP-RAM 6b in dem gemeinsamen Prozessorgehäuse bilden wieder eine Sicherheitsschaltung bzw. ein Sicherheitsmittel gegen unbefugte Manipulation.

Ein interner nichtflüchtiger Speicher NVM 6d im Sicherheitsmittel des OTP-Prozessors (CPU) 6 arbeitet mit dem Programmspeicher 6c (internes EPROM oder ROM) und flüchtige Datenspeicher RAM 6b zusammen. Durch die Möglichkeit Sicherungsbits zu setzen (bei internen EPROM) bzw. während der Herstellung eine Maskenprogrammierung (bei internen ROM) vorzunehmen, kann das Auslesen des internen nichtflüchtigen

Speichers von außen verhindert werden.

Bei der Lösung nach der in der Figur 1a gezeigten - ersten Variante mit nichtflüchtigem Speicher NVM 20 extern vom OTP-Prozessor 6 bildet letzterer ein zweites Sicherheitsmittel gegen unbefugte Manipulation. Der externe nichtflüchtige Speicher NVM 20 ist in der bevorzugten Variante dabei - wie in der Figur 1a gezeigt - ein Bestandteil des Prozessorsystems der Frankiermaschine und arbeitet mit dem Programmspeicher 6c (internes EPROM oder ROM) und flüchtige Datenspeicher RAM 6b zusammen.

Im vorgenannten Blockschaltbild der erfindungsgemäßen Frankiermaschine 1 wird auch eine Chipkarten-Schreib-Lese-Einheit 21 dargestellt. Diese steht über einen BUS 11 mit einem Prozessor 6 direkt oder über Ein/Ausgangsmittel (I/O-Ports) 4 in Verbindung. Weiter ist ein - in der Figur 1a nicht näher dargestellter - Anschluß eines MODEMs 23 über den BUS 11 direkt oder über vorgenanntes Ein/Ausgangsmittel 4 vorgesehen. Die Chipkarte, welche in die Chipkarten-Schreib-Lese-Einheit 21 eingesteckt werden muß, schließt einen externen nichtflüchtigen Speicher 25 ein. Ein solcher nichtflüchtiger Speicher kann aber auch in einem ähnlichen System vorhanden sein.

Wie bereits erwähnt kann durch die Möglichkeit Sicherungsbits zu setzen (bei internen EPROM) bzw. während der Herstellung eine Maskenprogrammierung (bei internen ROM) vorzunehmen, das Auslesen des internen Programm-Speichers von außen verhindert werden. Die Sicherungsbits werden durch Programmierung des internen EPROM während der Herstellung der Frankiermaschine im OTP-Prozessor gesetzt. Das Observieren solcher sicherheitsrelevanter Routinen, wie beispielsweise Abrechnungsroutinen, mit einem Emulator/Debugger würde ebenfalls zu einem veränderten Zeitablauf führen, was durch den OTP feststellbar ist. Dieser umfaßt auch eine Taktgeber/Zähler-Schaltung für die Vorgabe von Zeitintervallen bzw. Taktzyklen beispielsweise für die Time-out-Generierung oder Druckersteuerung. Vorteilhaft wird die Taktgeber/Zähler-Schaltung für eine Programmlaufzeitüberwachung eingesetzt, welche in der Anmeldung EP 660 269 A2 genauer beschrieben ist. Wenn eine bestimmte Zeit abgelaufen und das erwartete Ereignis nicht eingetreten ist, wird vom der Taktgeber/Zähler-Schaltung ein Interrupt generiert, der dem Mikroprozessor den ergebnislosen Ablauf der Zeitspanne meldet, woraufhin der Mikroprozessor weitere Maßnahmen veranlaßt. Die Überwachungsfunktion wird in vorgenannter Weise durch das vorgenannte erste Sicherheitsmittel übernommen, das Bestandteil des Prozessors (OTP) ist und die in Verbindung mit einer entsprechenden Software während des Betriebes der Frankiermaschine wirksam wird. Bei einer vorteilhaften weiteren Variante der Zeitkontrolle wird ein Codewort im externen NVM 5a, 5b oder 25 gelöscht. Das kann durch Überschreiben mit einem vorbestimmten anderen Wort, beispielsweise 0000 erfolgen. Der Vorteil liegt insbesondere darin, daß die Sicherheitsschaltung während des Betriebes auf eine Manipulation durch unbefugten Eingriff in die Frankiermaschine reagiert.

Die Überwachungsfunktion wird auch bei der - in der Figur 1b und 2b gezeigten - zweiten Variante in vorgenannter Weise durch nun aber von der durch Mittel 6a und 6d gebildeten Sicherheitsschaltung übernommen, die Bestandteil des Prozessors (OTP) ist und die in Verbindung mit einer entsprechenden Software während des Betriebes der Frankiermaschine wirksam wird. Als Prozessor kann beispielsweise ein CMOS-Einchip-8-Bit-Microcontroller Philips 80C851 bzw. 83C851 mit einem nichtflüchtigen 256x8-bit E^2PROM als internen Prozessorspeicher eingesetzt werden. Das Codewort kann im o.g. internen Prozessorspeicher über 50 000 mal nichtflüchtig gespeichert werden. Der Datenerhalt wird ebenfalls für 10 Jahre garantiert. Ein anderer geeigneter Prozessor ist beispielsweise der TMS 370C010 von Texas Instruments, der ebenfalls einen internen 256 Byte E^2PROM aufweist.

Die frankiermaschineninterne Sicherheitsschaltung für Postregisterdaten und andere sicherheitsrelevante Daten schützt den Dateninhalt von nichtflüchtigen Speichern, beispielsweise von mit einer Lithiumbatterie gestützten CMOS-SRAM's, gegenüber einer Verwendung unerlaubt gekonter Kopien ohne Abrechnung.

Vorgenannte Lithiumbatterie gestützten CMOS-SRAM's haben eine Lebensdauer von mindestens 10 Jahren. Als nichtflüchtige Speicherbausteine sind beispielsweise von Dallas Semiconductor beim Typ DS1230Y/AB ein Speicherbereich von 256 K oder ein Speicherbereich von 1024 K für ein NV-SRAM beim Typ DS1245Y/AB verfügbar.

Ebenfalls kann der Uhren/Datums-Baustein 8 nach dem gleichen Verfahren geschützt werden. Dieser vorgenannte Baustein ist ein nichtflüchtiger Zeitgeber-RAM und enthält ebenfalls eine Lithiumbatterie für mindestens 10 Jahre. Der Baustein DS 1642 von Dallas Semiconductor weist einen 2K x 8 NV-SRAM auf.

Zusätzlich sind auch Speichermittel von anderer Speichertechnologie entsprechend ihrer Lebensdauer einsetzbar. Die Sicherheitsschaltung speichert in diese nichtflüchtigen Speicher beispielsweise nur Daten zum Zeitpunkt des Einschaltens bzw. Wiederinbetriebnahme der Frankiermaschine nach einem Stand by-Betrieb, also zu Zeitpunkten, wo kein Abrechnungserfordernis vorliegt und keine Frankierung erfolgt. Normale E^2PROM-Speicher, insbesondere vom Typ 28256 benötigen keine interne Batterie und lassen mindestens 10 000 bis 100 000 Schreib-/Lese-Zyklen zu. Die frankiermaschineninterne Sicherheitsschaltung für Postregisterdaten und andere sicherheitsrelevante Daten steuert entsprechend die vorgenannten nichtflüchtigen Speicherbausteine so an, daß die Lebensdauer erhöht bzw. ausreichend ist.

Wenn in den nichtflüchtigen Speichern 5a, 5b neben einem Codewort der Dateninhalt der Postregister als Checksumme verschlüsselt gespeichert wird, kann die Manipulation der Postregister wirksam von Anfang an verhindert werden. Beispielsweise wird ein OTP-Pro-

zessor (ONE TIME PROGRAMMABLE) eingesetzt, der im internen ROM einen gespeicherten Algorithmus für ein solches Prüfsummenverfahren aufweist. Gesetzte Flags verhindern ein Auslesen der sicherheitsrelevanten Daten aus dem Prozessor. Ein bekanntes Prüfsummenverfahren beruht auf einem MAC (MESSAGE AUTHENTIFICATION CODE) der an die zu sichernden Daten angehängt wird. Eine solche MAC-Absicherung wird vorteilhaft über die Postregisterdaten gelegt. In Weiterführung der Erfindung kann das vorgenannte in zeitlichen oder stückzahlmäßigen Abständen geänderte Codewort auch zur MAC-Absicherung der Postregisterdaten verwendet werden. Im Regelfall genügt bereits ein gespeichertes Codewort, welches in Zeitabständen geändert wird, um die Sicherheit zu garantieren.

Die Überwachungsfunktion wird auch bei der - in der Figur 1a und 2a gezeigten - ersten Variante im Prozessor realisiert. Dies kann beispielsweise ein 8051-Prozessor mit einem 16 kByte On-Chip-EPROM als internen Programmspeicher eingesetzt werden. Der interne OTP-RAM hat einen Speicherbereich von 256 Byte.

Erfindungsgemäß ist nun vorgesehen, daß die die Postregisterdaten enthaltenen nichtflüchtigen Speicher, insbesondere batteriegestützte CMOS-RAM's (Bat-NV-CMOS-RAM's) ein Codewort enthalten, welches dem letzten Betriebszustand der Frankiermaschine vor dem Ausschalten bzw. Spannungsausfall oder vor einer gewissen Stillstandszeit (Stand by) bzw. vor Programmunterbrechung entsprechend gewählt wurde und daß mindestens zum Zeitpunkt des Einschaltens der Frankiermaschine das alte Codewort durch ein vorbestimmtes neues Codewort ersetzt wird.

Erfindungsgemäß wird also das Codewort zu vorbestimmten Ereignissen durch die betriebsbereite Frankiermaschine automatisch in allen nichtflüchtigen Speichern, welche sicherheitsrelevante Daten händeln, geändert. Eine derartige Maßnahme verhindert, daR ein geklonter Speicherinhalt eines nichtflüchtigen Speichers (Bat-NV-CMOS-RAM's) öfter als einmal verwendet werden kann, weil das Codewort im nichtflüchtigen internen Prozessorspeicher und im Postregister (Bat-NV-CMOS-RAM's) geändert wird, sobald ein vorbestimmter Betriebszustand der Frankiermaschine nach dem Einschalten der Maschine bzw. nach Spannungswiederkehr nach einem Ausfall, nach Verlassen des Kommunikationsmodus bzw. dem Nachladen der Frankiermaschine mit einem Guthaben oder nach einer gewissen Stillstandszeit (Stand by) erreicht ist oder nach einer anderen Programmunterbrechung.

Dabei wird durch o.g. Maßnahme ein Duplizieren bzw. Klonen eines Bat-NV-CMOS-RAM's oder anderen NVRAM's nicht verhindert. Auch ein Duplikat des Speicherinhalts, welches gegen den Speicherinhalt des Orginals ausgetauscht wird, kann weiterverwendet werden. In diesem Fall wird das Codewort des Orginals später ungültig, d.h. ein Rücktausch der Speicherinhalte würde vom Prozessor aufgrund des inzwischen ebenfalls geänderten Codewortes im nichtflüchtigen internen Prozessorspeicher bemerkt werden.

Die Veränderung der Codeworte bei gleichgebliebenen Dateninhalt des Speichers kann ohne Kenntnis des Schlüssels und der Parameterdaten vom Manipulator auch nicht vorgenommen werden, wenn der Algorithmus zur Bildung des neuen Codewortes bekannt wäre. Deshalb kann ein bekanntes Verschlüsselungsverfahren, wie beispielsweise DES, eingesetzt werden.

Das Verfahren zur Erhöhung der Manipulationssicherheit von kritischen Registerdaten umfaßt weitere Sicherungsschritte, die in der Figur 7 dargestellt sind.

Im Schritt 106 werden nacheinander die in den zu schützenden nichtflüchtigen Speichern gespeicherten Codewörter gelesen und dann zum Prozessor übertragen. Der Prozessor führt einen Sicherungsschritt 107 zur Überprüfung des bisher gültigen Codewortes und einen Schritt 108 zur entsprechenden Veränderung des Codewortes aus, wenn die Überprüfung die Übereinstimmung bzw. Fehlerfreiheit ergeben hat. Anderenfalls wird vom Schritt 107 auf den Schritt 109 verzweigt, um einen eine den Kill-Mode kennzeichnende Zahl bzw. mindestens aber ein MAC-gesichertes Kill-Mode-Flag im ständig eingebauten nichtflüchtigen externen Sicherheits-Speicher zu setzen.

In den Figuren 8a bis c werden Zeigerstellungen nach dem erfindungsgemäßen Verfahren dargestellt. Die Figur 8a zeigt eine Anfangszustandsvoreinstellung. Eine solche wird im Schritt 107 (Fig.7) benötigt, um das richtige alte Codewort aus der gespeicherten Liste zu ermitteln. Der Zeiger steht beim ersten Initialisieren der Maschine im Herstellerwerk auf einer Zahl 1. Alternativ kann auch die Seriennummer der Frankiermaschine eine Anfangszahl bilden. Die Zeigerstellung (Zahl 1 bzw. Anfangszahl) wird gespeichert. Dann wird ein entsprechender erster Code, der in der Liste an einer ersten Stelle steht im zu schützenden NVM 5a bzw. 5b gespeichert. Die Frankiermaschine verläßt das Herstellerwerk auf eine Zahl 1 bzw. Anfangszahl gestellt. Beim Händler bzw. beim Kunden wird nun die Frankiermaschine eingeschaltet bzw. wiedereingeschaltet (Fig. 8b). Der erste Code wird entsprechend der Zeigerstellung aus der Liste gelesen und mit dem im zu schützenden NVM 5a bzw. 5b gespeichert vorliegenden ersten Code verglichen. Diese erste Phase entspricht dem Schritt 107 der Figur 7, in welcher festgestellt wird ob ein Speicher zwischenzeitlich ohne abzurechnen herausgenommen und durch einen anderen ersetzt worden war und nun erneut mit alten Datenbestand eingesetzt wurde. Sind die Code gleich, wird entsprechend der Figur 8c die Zeigerstellung auf ein zweites Codewort in der Liste weitergeschaltet, was dem Schritt 108 in der Figur 7 entnembar ist. Die Zeigerstellung wird in vorbestimmter Weise verändert. Im einfachsten Fall wird die Zeigerstellung inkrementiert oder dekrementiert. Der erste Code im zu schützenden NVM 5a bzw. 5b wird nun durch den zweiten Code ausgetauscht, d.h. überschrieben. Wird nun nach dem Ausschalten die Frankiermaschine eingeschaltet bzw. wiedereingeschaltet wird eine Überprüfung auf der Basis des aktu-

ellen Code analog zu der Fig. 8b und Fig. 7, Schritt 107 gezeigten Weise vorgenommen.

Im bevorzugten Ausführungsbeispiel wird für zwei nichtflüchtige Speicher NVM 6d und NVM 5a im Schritt 107 zur Überprüfung des bisher gültigen Codewortes V(-1), U(-1) ein für jeden physikalischen Speicherbaustein vorgesehenes separates Codewort W(-1), T(-1) verwendet.

Für zwei nichtflüchtige Speicher NVM 20 und NVM 5a wird nach Überprüfung des alten Codewortes im Schritt 107 und vor der entsprechenden Veränderung von Codewötern V und U zunächst im Schritt 108 ein neues Codewort W' und dannach ein Codewort T' gebildet, nach den Gleichungen:

$$W' := F\{P1\} \text{ und} \quad (1)$$

$$T' := F\{P2\}, \quad (2)$$

wobei P1 und P2 gelistete Codewörter sind.

In einer Variante werden mit den gelisteten Codewörtern und mit internen Daten nach einem internen Programm ein neues Codewort mittels einer solchen mathematischen Funktion F erzeugt, welche das externe Nachbilden von Codewörtern wesentlich erschwert, so daß eine Manipulation in Fälschungsabsicht praktisch unmöglich gemacht wird.

Im einfachsten Fall wird im internen NVM 20 ein Zählwert inkrementiert, bevor ein neues Codewort (W', T', U', V') gebildet wird. Als mathematische Funktion F kann beispielsweise eine kryptographische Funktion verwendet werden, welche im internen OTP-ROM als Algorithmus bzw. Programm gespeichert vorliegt. Zum Beispiel kann der DES-Algorithmus (Data-Encryption-Standard) oder eine Zufallsfunktion eingesetzt werden, beispeilsweise um den neuen Zeiger entsprechend F zu ermitteln.

Das vorgenannte Bilden von Codewörtern umfaßt das Berechnen und/oder das Auswählen aus einer Liste von Codewörtern, welche im internen OTP-ROM gespeichert vorliegt. Im Idealfall soll jedes Codewort nur ein einziges mal zur Absicherung der externen nichtflüchtigen Schreib/Lese-Speicher verwendet werden. Das erfordert aber eine Vielzahl von Codewörtern, welche im internen OTP-ROM gespeichert werden.

Lediglich die Zeigerstellung oder Zahl die auf die Stellung des jeweiligen Codewortes in der in OTP-ROM gespeicherten Liste hinweist muß extern vom OTP-Prozessor und extern von den zu schützenden nichtflüchtigen Schreib/Lese-Speichern NVM 5a und 5b besonders gesichert gespeichert werden. Dieses Sichern des zweiten Sicherheitsmittels 20 gegen Entnahme aus dem Prozessorsystem kann durch ein Aufkleben oder ein gesichertes Kapseln des vorgenannten Sicherheits-Speichers zusammen mit dem Prozessor gewährleistet werden.

Bei den erfindungsgemäßen Varianten mit Speicherung in der Chipkarte kann auf ein Aufkleben oder ein gesichertes Kapseln mindestens eines der externen nichtflüchtigen Schreib/Lese-Speicher verzichtet werden.

Diesen Varianten liegt die Voraussetzung zugrunde, daß der Speicher der Chipkarte nicht manipuliert oder geklont werden kann. Ein Manipulator darf das neu zu bildende Codewort vor dem Einschalten nicht abfragen können, um damit seine geklonten Speicher auszurüsten. Die Zeigerstellung bzw. Zahl kann mittels DES verschlüsselt werden, wenn diese zur Chipkarte transferiert wird. Alternativ wird das Codewort übermittelt, oder nur die Anweisung zu seiner Wiederherstellung oder wesentliche Teile der Anweisung. Die Übermittlung erfolgt wieder verschlüsselt bzw. als MAC-gesicherte Daten. Ein solches Verfahren hat den Vorteil, daß man ohne o.g. speziellen Prozessor auskommt und daß dennoch alle Postregister-NVRAMs weiterhin gesockelt und somit leicht austauschbar montiert sind.

Alternativ ist es auch möglich, daß ein in der Liste gespeichertes Codewort verschlüsselt ausgelesen werden kann, wenn ein spezieller Prozessor vorliegt. Die Codewörter aus dem zu schützenden Speicher und das Codewort aus der vorgenannten Liste, auf welches der Zeiger weist, werden verschlüsselt zur Chipkarte übertragen, die ebenfalls einen Prozessor aufweist, der auch einen Vergleich zwecks Sicherheitsüberprüfung vornemmen kann.

In einer weiteren Variante wird von der Frankiermaschine das Codewort zum Speicher eines entfernten ähnlichen Prozessorsystems übertragen. Bei jedem Einschalten der Frankiermaschine wird eine Verbindung zum Speicher des entfernten ähnlichen Prozessorsystems hergestellt. Die Fehlerfreiheit wird durch Vergleich des extern in dem entfernten ähnlichen Prozessorsystem gespeicherten Codewortes mit dem in den PostregisterNVRAM gespeicherten Codewort festgestellt, um dann ein neues Codewort zu bilden und im NVRAM des entfernten ähnlichen Prozessorsystems und im Postregister-NVRAM abzuspeichern. Der Vergleich der einzigartigen Codewörter wird in der Frankiermaschine durchgeführt.

Eine zweckmäßige Variante besteht im Abspeichern des nach einem Algorithmus gebildeten einzigartigen Codewortes in einem näherem speziellen Übertragungsmittel (z.B. Chipkarte). Eine Kommunikationsverbindung zum entfernten ähnlichen Prozessorsystem wäre dann keine Voraussetzung zur Inbetriebnahme der Frankiermaschine, wenn zu Beginn die Chipkarte gesteckt wurde, welche auch bei letzten Mal, d.h. bei vorherigen Frankieren eingesteckt war. Es ist selbstverständlich ein entsprechender Kommunikations-Modus 300 nach dem Einschalten während der Laufzeit der Frankiermaschine vorgesehen.

Bei der - in der Figur 1b und 2b gezeigten - zweiten Variante werden im Schritt 106 nacheinander in den zu schützenden nichtflüchtigen Speichern gespeicherten die Codewörter gelesen und dann zum Prozessor übertragen. Der Prozessor führt einen Sicherungsschritt 107 zur Überprüfung des bisher gültigen Codewortes und einen Schritt 108 zur entsprechenden Veränderung des

Codewortes aus, wenn die Überprüfung die Übereinstimmung bzw. Fehlerfreiheit ergeben hat. Anderenfalls wird vom Schritt 107 auf den Schritt 109 verzweigt, um ein Codewort Y zu löschen oder um mindestens ein Kill-Mode-Flag im prozessorinternen nichtflüchtigen Speicher 6d zu setzen.

Für zwei nichtflüchtige Speicher NVM 6d und NVM 5a wird nach Überprüfung des alten Codewortes im Schritt 107 und vor der entsprechenden Veränderung von Codewortern V und U zunächst im Schritt 108 ein neues Codewort W' und dannach ein Codewort T' für den zweiten prozessorinternen NVM 6d gebildet, nach den Gleichungen:

$$W' := F\{P1\} \text{ und} \quad (1)$$

$$T' := F\{P2\}, \quad (2)$$

wobei P1 und P2 verschiedene monoton stetig veränderbare Parameter sind, beispielsweise die aktuelle Zeit, Anzahl von Programmunterbrechungen bzw. andere Programm-, Zeit- oder pysikalische Parameter oder gelistete Code sind. In einer Variante werden wieder mit internen Daten und nach einem internen Programm ein neues Codewort mittels einer solchen mathematischen Funktion F erzeugt, welche das externe Nachbilden von Codewörtern wesentlich erschwert, so daß eine Manipulation in Fälschungsabsicht praktisch unmöglich gemacht wird.

Bei der erfindungsgemäßen zweiten Variante kann auf die Einbeziehung von Postregisterwerten als Prüfkennwert und auf ein Aufkleben oder ein gesichertes Kapseln mindestens eines der externen nichtflüchtigen Schreib/Lese-Speicher verzichtet werden. Erst später, beispielsweise im Frankiermodus 400 (Fig.5), wird bei der Abrechnung der Dateninhalt überprüft, ob die Registerwertsumme R3 gleich der Summe aus ascending Register R1 (Restwert) und descending Register R2 ist und/oder ob die Postregisterwerte gültig sind (z.B. durch Authentizitätsprüfungen, Plausibilitätsprüfungen und ähnliche Prüfungen).

Das erfindungsgemäße Verfahren ist in einem - in der Figur 3 dargestellten - Gesamtablaufplan der Frankiermaschine eingebunden. Nach dem Start 100 erfolgen in einem die Startroutine und Initialisierung umfassenden Schritt 101 Maßnahmen zur Sicherheitsüberprüfung und zur Wiederherstellung eines definierten Anfangszustandes.

Die weiteren Schritte 102 bis 105 erfolgen gegebenenfalls zur Wiederherstellung der Betriebbereitschaft beispielsweise nach einer Reparatur der Frankiermaschine und sind in der Figur 7 näher dargestellt.

In den Schritten 106 bis 109 werden die gelesenen alten Codewörter überprüft und gegen neue Codewörter ausgetauscht. Anschließend wird das neue Codewort auch in die NV-RAMs NVM 5a und NVM 5b übertragen und bildet dort ein entsprechendes Codewort (V', U'). Der Schritt 108 beinhaltet außerdem die Überprüfung des ordnungsgemäßen Einspeicherns der Codewörter (U',V' bzw. W', T'). Wird bei der Überprüfung des bisher gültigen Codewortes eine nicht plausible Abweichung festgestellt, wird zu einem Schritt 109 verzweigt, der Maßnahmen umfaßt, die letztlich weitere Frankierungen mit der Frankiermaschine verhindern. Beispielsweise kann ein drittes von einer Datenzentrale vorgegebenes Codewort Y gelöscht werden, dessen Fehlen die Manipulation belegt. Nachfolgend wird auf die Systemroutine (Punkt s) verzweigt.

Der in der Figur 3 dargestellte Gesamtablaufplan für die Frankiermaschine weist Schritte 201 bis 206 und 207 bis 208 für eine Überwachung weiterer Kriterien auf. Bei einer Verletzung beispielsweise eines im Schritt 207 überprüften Sicherheitskriteriums tritt die Frankiermaschine in einen entsprechenden Kill-Modus ein (Schritt 208), Die Frankiermaschine tritt aufgrund eines im Schritt 202 überprüften Sicherheitskriteriums in einen Sleeping-(Warn)-Modus (203-206) ein, wenn nach Verbrauch einer vorbestimmten Stückzahl noch keine Verbindung zur Datenzentrale aufgenommen wurde.

Die Frankiermaschine und die Datenzentrale verabreden jeweils eine vorbestimmte Stückzahl S, d.h. die Menge, die bis zur nächsten Verbindungsaufnahme frankiert werden kann. Falls eine Kommunikation nicht zustande kommt (Stückzahlkontrolle), verlangsamt die Frankiermaschine ihre Arbeitsweise (Sleeping Modus-Variante 1), damit bis zu einer nächsten Stückzahlgrenze ohne Anzeige einer Warnung weiter gearbeitet werden kann. Jedoch ist es möglich in immer kürzeren Abständen, d.h. nach einer vorbestimmten Anzahl an Frankierungen, eine erneute Warnung auszugeben, welche so immer dringlicher auf das Erfordernis einer Kommunikation mit der Datenzentrale aufmerksam macht (Sleeping Modus-Variante 2). Schließlich ist es möglich (Sleeping Modus-Variante 3), eine ständige Warnung für ein bevorstehendes Schlafenlegen der Frankierfunktion im Schritt 203 auszugeben, wenn dieser aufgrund des erfüllten Abfragekriteriums in Schritt 202 ständig durchlaufen werden muß, bevor Schritt 205 erreicht wird. Es ist weiterhin vorgesehen, daß der Schritt 203 einen Subschritt zur Fehlerstatistik entsprechend dem Statistik- und Fehlerauswertungsmodus 213 umfaßt. Diese Variante kommt ohne den vorgenannten Schritt 204 aus. Das Frankieren wird durch den Sleeping Modus nicht beeinträchtigt. Solange die Überprüfung im Schritt 205 ergibt, daß die Stückzahl S noch größer Null ist, wird der Schritt 207 erreicht. Lediglich die Warnung erscheint immer öfter in der Anzeige. Anderenfalls wird auf den Schritt 206 verzweigt, wobei beispielsweise ein FLAG gesetzt wird, welches später im Schritt 301 abgefragt und als Kommunikationsersuchen gewertet wird. Im Schritt 206 kann ebenfalls eine zusätzliche Anzeige erfolgen, daß nun automatisch die Kommunikation erfolgt und solange die Frankierfunktion ruht, bis die Kommunikation erfolgreich abgeschlossen ist. Natürlich kann jederzeit der Frankiermaschinenbenutzer schon vorher den Kommunikationsmodus 300 aufrufen. In einem dem Kommunikationsmodus 300

vorausgehenden Schritt 207 werden weitere für die Manipulationssicherheit relevante Kriterien überprüft. Bei einer festgestellten Manipulation der Maschine, die in Fälschungsabsicht vorgenommen wurde, wird zum Schritt 208 verzeigt, um ein Frankieren mit der manipulierten Maschine zu verhindern. Die Maschine würde in einem solchen Fall in den Kill-Mode eintreten. Befindet sich die Frankiermaschine nur im Sleeping-Mode wird ein Frankieren nicht verhindert.

Nach der Überprüfung der Kriterien für den Kill-Modus (Schritte 207 bis 208) und für den Sleeping-Modus (Schritte 202 bis 206) wird ein in der Figur 3 gezeigter Punkt t erreicht. Im Schritt 209 können Eingaben getätigt werden, bevor der Punkt e erreicht wird.

Mit dem Eintritt in den Kommunikationsmodus 300 besteht für den Nutzer die Möglichkeit eine Kommunikation mit der Datenzentrale herbeizuführen bzw. es wird gegebenenfalls eine Kommunikation mit der Datenzentrale automatisch - gemäß dem in der Figur 3 gezeigten Gesamtablaufplan - herbeigeführt.

Falls die Kommunikation erfolgreich war, wird im Schritt 211 abgefragt, ob Daten übermittelt wurden. Anschließend wird der Schritt 213 erreicht. Im Schritt 213 werden die aktuellen Daten ermittelt bzw. geladen, welche im Schritt 201 aufgerufen und anschließend wieder beim Vergleich im Schritt 202 benötigt werden. Das übermittelte Entscheidungskriterium ist vorzugsweise die neue Stückzahl S'.

Der Auswertemodus im Schritt 213 umfaßt erfindungsgemäß auch die Bildung neuer Codewörter U', V' für die zu schützenden nichtflüchtigen Speicher im Ergebnis eines Nachladevorganges, der in Kommunikationsverbindung mit einer Datenzentrale vorgenommen wurde. Hierbei laufen die in der Figur 7 für Codewort Y beispielhaft gezeigten Schritte 106 bis 109 in analoger Weise auch für die Codewörter U', V' ab.

Wurde zuvor bei der Datenzentrale eine Eingriffsbefugnis für die Frankiermaschine angefordert, wird ein von der Datenzentrale vorgegebenes neues drittes Codewort Y' geladen, welches das alte dritte Codewort Y ersetzen kann. Für Reparaturzwecke ist ein Öffnen der Frankiermaschine und ein Austausch defekter Bauelemente ggf. unvermeidlich. Deshalb sind vorausgehende Maßnahmen zur Erlangung einer Eingriffsbefugnis erforderlich, welche den Betrieb der Frankiermaschine nach deren Instandsetzung erlauben. Ein unbefugtes Öffnen der Frankiermaschine wird dabei ausgeschlossen. Wenn die Frankiermaschine nach dem Eingriff wieder in Betrieb genommen wird, kann aufgrund der Eingriffsbefugnis für die Frankiermaschine jenes von einer Datenzentrale vorgegebenes neues dritte Codewort Y' das alte dritte Codewort Y ersetzen, wie dies beispielsweise in der Anmeldung DE 43 44 476 A1 vorgeschlagen wurde.

Sollte also das von einer Datenzentrale vorgegebene alte dritte Codewort Y gelöscht werden, weil die Speicher vollständig ausgetauscht wurden und deren veränderbares Codewort (V, U) nicht vorhanden ist, bzw. nicht mit dem intern gespeicherten übereinstimmt, würde die Frankiermaschine weiterbetrieben werden können.

Der Weiterbetrieb der Frankiermaschine ist möglich, weil ein neues drittes Codewort Y'verwendet wird, wobei - wie in der Figur 7 dargestellt ist - auf den Schritt 108 verzweigt wird, um ein neues veränderbares Codewort (T', W') zu bilden und als Codewort (V', U') in die NV-RAMs zu laden.

In einer - gegenüber dem in der Figur 7 gezeigten Flußplan - modifizierten Flußplanvariante kann anstatt mit einem zu dem veränderbaren Codewort (W, T) identischen Codewort (V, U) auch mit dem komplementären Schatten (V", U") in mindestens einem der Speicherbereiche bzw. NVRAM's gearbeitet werden. Entsprechend verändern sich auch die Form der Überprüfung der bisher gültigen Codewörter und deren Ersatz durch neue Codewörter in einem der Speicherbereiche des nichtflüchtigen Speichers NVM 5a, 5b gemäß der - in den Figuren 3 und 5 gezeigten - Schritte 102 bis 105. Nach einem Verifizieren der gegebenenfalls in einem Speicherbereich E des NVM 5a, 5b gespeichert vorliegenden neuen Codewörter V', U' und/oder Y' werden die alten Codewörter gelöscht und die neuen Codewörter entsprechend abrufbar adressiert. Das kann vorteilhaft analog zum Ablauf - wie er in der Figur 7 in DE 43 44 476 A1 dargestellt ist - erfolgen, indem die neuen Codewörter V', U' und/oder Y'auf die Adresse der alten Codewörter V, U und/oder Y gesetzt werden.

Nach einem vorausgehenden Ereignis bzw. einer Programmunterbrechung (Stand by) wird ein Punkt p erreicht und gemäß den - in der Figur 4 dargestellten - Details des Ablaufplanes wird über Schritte 102 bis 105 ein erster Sicherungsschritt 106 des in der Figur 7 gezeigten Flußplanes des erfindungsgemäßen Verfahrens erreicht.

Nur bei einer Inbetriebnahme oder nach Spannungsausfall wird nach einem Initialisieren in einem dem vorgenannten Punkt p vorgelagerten Schritt 1050 zuerst das aktuelle Programmodul PM entsprechend der Modulkennung aufgerufen, dessen Abschnitte anschließend weiter bearbeitet werden sollen. Der in der Figur 3 gezeigte Schritt 101 umfaßt mehrere Subschritte, welche nachfolgend anhand der Figur 4 näher erläutert werden.

Zunächst laufen im Schritt 1010 übliche Hardware- und Anzeige-Initialisierungsroutinen ab, bevor ein Schritt 1011 zum Timer- und Interrupt-Start erreicht wird. Das interne Programm beginnt dann mit Startsicherheitsüberprüfungen. In vorteilhafter Weise kann hier im Schritt 1020 bereits geprüft werden, ob ein Codewort oder Speicherinhalt gültig ist. Anschließend wird bei Gültigkeit ein Schritt 1040 zur automatischen Eingabe gespeicherter Daten mit Druckdatenaufbereitung und Einbettung der Bilddaten erreicht.

Nach dem Aufruf des Merkers oder Zeigers im Schritt 1051 wird in einem weiteren Schritt 1052 getestet, ob der Programmodul weiterabgearbeitet werden muß. Ist das nicht der Fall wird im Schritt 1054 der nächste Programmodul PM(+1) aufgerufen. Anderenfalls

wird in einem Schritt 1053 überprüft, ob Programmabschnitte eines vorhergehenden Programmoduls PM(-1) zuende abgearbeitet werden müssen und zu einem Schritt 1056 verzweigt oder zu einem Schritt 1055 verzweigt, wenn ein Programmabschnitt des aktuellen Programmoduls PM weiter abgearbeitet werden muß. Nach Feststellung des aktuellen Programmoduls gemäß den Schritten 1054, 1055 oder 1056 wird auf den Punkt p verzweigt.

Für eine Abarbeitung kritischer und unkritischer Programmabschnitte innerhalb dieses Programmoduls werden Merker, beispielsweise eine Phasenkennung gesetzt, wie das aus DE 42 17 830 A1 bekannt ist, oder Zeiger gestellt, welche nach Spannungsausfall und Wiedereinschalten eine Rekonstruktion definierter Zustände für die weitere Programmabarbeitung ermöglicht.

Gemäß der Figur 3 wird nach Ausführung der Schritte 102 bis 105 und 106 bis 109 der Punkt s und damit die Systemroutine 200 erreicht. Außerdem wird der Punkt s nach Ausführung der Schritte für einen Testmodus 216, für einen Anzeigemodus 215 und für einen Frankiermodus 400 erreicht.

Die Erläuterung der Abläufe nach dem - in der Figur 5 gezeigten - Frankiermodus 400 erfolgt in Verbindung mit dem - in der Figur 1a dargestellten - Blockschaltbild und in dem - in der Figur 3 dargestellten - Gesamtablaufplan der elektronischen Frankiermaschine.

Die Erfindung geht davon aus, daß nach dem Einschalten automatisch der Postwert im Wertabdruck entsprechend der letzten Eingabe vor dem Ausschalten der Frankiermaschine und das Datum im Tagesstempel entsprechend dem aktuellem Datum vorgegeben werden, daß für den Abdruck die variablen Daten in die festen Daten für den Rahmen und für alle unverändert bleibenden zugehörigen Daten elektronisch eingebettet werden (Fig.4, Schritt 1040).

Außerdem läuft die Zeit im batteriegestützten Uhren/Datums-Baustein 8 ständig auch bei ausgeschalteter Frankiermaschine weiter und wird ständig aktuell mindestens als Datum gespeichert und im Schritt 1040 der Figur 4 in der Initialisierungsroutine 101 eingebettet.

Wird also nach dem Einschalten der Frankiermaschine, nach der durchgeführten Systemroutine 200 und während des Betriebsmodus der Schritt 401 im Frankiermodus 400 erreicht, kann auch ohne Eingabe auf bereits gespeicherte Daten zurückgegriffen werden. Diese Einstellung betrifft insbesondere die letzte Einstellung der Frankiermaschine hinsichtlich des Portowertes, welche im Schritt 209 angezeigt wird, bevor ggf. eine erneute Eingabe, Anzeige und Druckdatenaufbereitung erfolgt. Hierbei werden die aktuellen variablen Pixelbilddaten (Datum und Portowert) in die festen Rahmenpixelbilddaten eingebettet. Anschließend erfolgt im Schritt 401 eine Abfrage der Eingabemittel auf eventuelle weitere Eingaben. Liegen weitere Eingaben vor wird ein Schleifenzähler im Schritt 403 zurückgesetzt und zum Punkt t (Fig. 3) zurückverzweigt.

Die Eingabedaten, die mit einer Tastatur 2 oder aber über eine an die Ein/Ausgabeeinrichtung 4 angeschlossene, den Portowert errechnende, elektronische Waage 22 eingegeben werden, werden automatisch im Speicherbereich D des nichtflüchtigen Arbeitsspeichers NVM 5 gespeichert. Außerdem sind auch Datensätze der Subspeicherbereiche, zum Beispiel B_j, C usw., nichtflüchtig gespeichert. Damit ist gesichert, daß die letzten Eingabegrößen auch beim Ausschalten der Frankiermaschine erhalten bleiben, so daß nach dem Einschalten automatisch der Portowert im Wertabdruck entsprechend der letzten Eingabe vor dem Ausschalten der Frankiermaschine und das Datum im Tagesstempel entsprechend dem aktuellem Datum vorgegeben wird. Im Schritt 209 wird die eventuelle Eingabe neuer Werte abgefragt. Wenn beispielsweise kein neuer Portowert eingegeben wurde, dann wird auf den im Speicherbereich gespeichert vorliegenden bisherigen Portowert zurückgegriffen und der Punkt e (Fig.3) erreicht, um weitere Eingaben abzufragen, bevor der Frankiermodus 400 (Fig.5) erreicht wird.

Bei einer im Schritt 401 festgestellten erneuten Eingabeanforderung wird über den Schritt 403 wieder auf den Schritt 209 zurückverzweigt. Anderenfalls wird auf den Schritt 402 verzweigt, um den Schleifenzähler zu inkrementieren. Über den Schritt 404, in welchen die durchlaufenen Schleifenanzahl überprüft wird, wird der Schritt 405 erreicht, um die Druckausgabeanforderung abzuwarten. Durch einen Briefsensor wird ein Brief detektiert, welcher frankiert werden soll. Dadurch wird ein Signal für die Druckausgabeanforderung generiert.

Im Schritt 405 wird die Druckausgabeanforderung abgewartet, um dann über die Schritte 407, 409 und 410 zur Abrechnungs- und Druckroutine im Schritt 406 zu verzweigen. Liegt keine Druckausgabeanforderung (Schritt 405) vor, wird - nach dem in der Figur 3 gezeigten Gesamtablaufplan - zum Schritt 209 (Punkt t) und gegebenenfalls, wenn kein Kommunikationsersuchen vorliegt über die Schritte 211, 212 und 214 zum Schritt 401 des Frankiermodus 400 zurückverzweigt.

Wenn nach der - in der Figur 5 dargestellten - Weise nunmehr zum Punkt t zurückverzweigt und nach Schritt 209 der Schritt 301 erreicht wird, kann jederzeit durch manuelle Eingabe ein Kommunikationsersuchen gestellt oder eine andere Eingabe gemäß den Schritten Testanforderung 212 und Registercheck 214 getätigt werden. Wieder wird Schritt 401 erreicht. Wenn keine Eingabeanforderung erkannt wird, werden weitere Schritte 402 und 404 - wie in der Figur 5 gezeigt - durchlaufen. Ein weiteres Abfragekriterium kann in einem Schritt 404 abgefragt werden, um im Schritt 408 ein Standby-Flag zu setzen, wenn nach einer durchlaufenen Schleifenanzahl weder eine Eingabe getätigt wurde, noch keine Druck-ausgabeanforderung vorliegt.

Der Standby-Modus wird in einer anderen Variante auch erreicht, wenn ein ansich bekannter - in der Figur 1a dargestellter - Briefsensor 16 in vorbestimmter Zeit keinen nächsten Briefumschlag ermittelt, welcher frankiert werden soll. Der - in der Figur 4 gezeigte - Schritt

404 im Frankiermodus 400 umfaßt entweder eine Abfrage nach einem Zeitablauf oder nach der Anzahl an Durchläufen durch die Programmschleife, welche letztendlich wieder auf die Eingaberoutine gemäß Schritt 401 führt. Wird das Abfragekriterium erfüllt, wird im Schritt 408 ein Standby-Flag gesetzt und direkt auf den Punkt p oder alternativ dazu auf den Punkt s zur Systemroutine 200 zurückverzweigt, ohne daß die Abrechnungs- und Druckroutine im Schritt 406 durchlaufen wird. Bei einer Verzweigung auf den Punkt p kann ein zusätzlicher Wechsel der Codewörter während des Standby-Modus erzielt werden. Bei einer - in der Figur 5 nicht dargestellte - Variante mit einer Verzweigung auf den Punkt s kann dagegen nur ein Wechsel der Codewörter nur nach dem Einschalten erzielt werden.

Das Standby-Flag wird während der Systemroutine 200 im Schritt 211 abgefragt und gegebenenfalls nach der Checksummenprüfung im Schritt 213 zurückgesetzt, falls kein Manipulationsversuch erkannt wird.

Das Abfragekriterium im Schritt 211 wird dazu um die Frage erweitert, ob das Standby-Flag gesetzt ist, d.h. ob der Standby Modus erreicht ist. In diesem Fall wird einmal auf den Schritt 213 verzweigt. Eine bevorzugte Variante mit Manipulationsüberwachung während des Standby-Modus besteht darin, ein Codewort Y in der bereits beschriebenen Weise zu löschen, wenn ein Manipulationsversuch im Standby-Modus auf vorgenannte Weise im Schritt 213 festgestellt worden ist. Das Fehlen des Codewortes Y wird im Schritt 207 erkannt und dann auf den Schritt 208 verzweigt. Der Vorteil dieses Verfahrens in Verbindung mit dem ersten Modus besteht darin, daß der Manipulationsversuch statistisch im Schritt 213 erfaßt wird.

Somit kann das Standby-Flag im auf den Kommunikationsmodus 300 folgenden Schritt 211 abgefragt werden. Damit wird nicht auf den Frankiermodus 400 verzweigt, bevor nicht die Checksummenprüfung die Vollzähligkeit und Gültigkeit aller oder mindestens einiger ausgewählter sicherheitsrelevanter Programme ergeben hat.

Falls eine Druckausgabeanforderung im Schritt 405 erkannt wird, werden weitere Abfragen in den nachfolgenden Schritten 409 und 410 sowie im Schritt 406 getätigt. Beispielsweise kann im Schritt 407 eine Überprüfung der Registerwerte und zusätzlich des Codewortes Y vorgenommen werden und im Schritt 409 wird die Gültigkeit und zusätzlich das Vorhandensein eines im Schritt 208 (Fig.3) gesetzten Kill-Mode-Flag's festgestellt, um auf den Schritt 410 zu verzweigen. Anderenfalls wird auf den Schritt 413 zur Statistik- und/oder Fehlerauswertung und Schritt 415 zur Anzeige des Fehlers verzweigt, wenn die Registerwerte nicht authentisch waren.

Im Schritt 410 wird das Erreichen eines weiteren Stückzahlkriterium abgefragt. War die zum Frankieren vorbestimmte Stückzahl bei der vorhergehenden Frankierung verbraucht, d.h. Stückzahl gleich Null, wird automatisch zum Punkt e verzweigt, um in den Kommunikationsmodus 300 einzutreten, damit von der Datenzentrale eine neue vorbestimmte Stückzahl S wieder kreditiert wird. War jedoch die vorbestimmte Stückzahl noch nicht verbraucht, wird vom Schritt 410 über Schritte 4060, 4061 bzw. 4062 und 4063 auf die Abrechnungs- und Druckroutine im Schritt 406 verzweigt.

Im Schritt 4060 wird eine Pseudozufallsfolge während des Betriebes der Frankiermaschine vor jedem Abdruck und damit vor jeder neu zu registrierenden Stückzahl an Frankieraufdrucken auf Basis der vorhergehenden Stückzahl und gegebenenfalls der aktuellen vom Uhren/Datumsbaustein gelieferten Zeit eine Zufallszahl erzeugt. Dafür ist ein Pseudozufallsgenerator mit entsprechender - nicht dargestellter - Hardware oder mit einem im internen OPT-ROM des OTP-Prozessors gespeicherten Programm vorgesehen. Im internen OPT-ROM des OTP-Prozessors liegt mindestens eines aus der Vielzahl von möglichen erzeugbaren Zufallswörtern gespeichert vor. Nach einem Vergleich im Schritt 4061 und einer anschließenden Authentizitätsprüfung des MACs im Schritt 4062 innerhalb des OTP-Prozessors wird bei Übereinstimmung eine redundante Speicherung des neuen Codewortes einmal in die lösbaren nichtflüchtigen Speicher (NVRAMs) und erfindungsgemäß auch in den vorgenannten unlösbar fest auf die Platine aufgeklebten nichtflüchtigen Speicher (E^2PROM) 20 oder im internen OTP-NVM 6d bzw. im externen Speicher 25 vorgenommen. In - nicht näher dargestellten - Subschritten zum Schritt 4061 sind außerdem eine Vielzahl gespeicherter weiterer Bedingungen abfragbar, bei deren Eintreffen im Ergebnis die Abspeicherung eines neuen Codewortes in einem nichtflüchtigen Speicher 20, 25 bzw. im internen OTP-Speicher 6d zur Folge hat. Dabei ist ein E^2PROM einsetzbar. Die zulässige Anzahl an Schreib/Lese-Zyklen für einen E^2PROM wird nicht überschritten, wenn beispielsweise durchschnittlich nur jede vierunzwanzigste Frankierung die nichtflüchtigen Speicher (E^2PROM und NVRAMs) redundant mit einem neuen Codewort beschrieben werden.

Wird ein Codewort zur Verschlüsselung von Abrechnungsdaten eingesetzt, entsteht ein sogenannter MAC. Zur Speicherung von Abrechnungsdaten mit angehängten MAC in den zu schützenden nichtflüchtigen Speichern 5a und 5b bei jeder Abrechnung existiert parallel in unregelmäßigen Abständen eine Speicherung von Abrechnungsdaten mit angehängten MAC in dem jeweiligen als zweite Sicherungsmitteln gegen unbefugte Manipulation dienenden nichtflüchtigen Speicher, vorzugsweise einem E^2PROM 20 oder 25. Vor dem nächsten Abrechnen werden im Schritt 406 gewöhnlich die Abrechnungsdaten in den zu schützenden nichtflüchtigen Speichern 5a und 5b anhand des angehängten MAC's überprüft. Aber im Falle eines nächsten im Schritt 4061 eintreffenden Ereignis wird in - nicht näher dargestellten - Subschritten des Schrittes 4062 der Abrechnungsdatensatz in den OTP 6 übertragen, um ihn anhand desjenigen MAC's oder Codewor-

tes zu überprüfen, welches im - als zweites Sicherungsmittel gegen unbefugte Manipulation dienenden - nichtflüchtigen Speicher gespeichert vorliegt. Der Abrechnungsdatensatz wird mittels des Codewortes zu einem MAC verschlüsselt. Der so gebildete MAC wird mit dem an den Abrechnungsdatensatz angehängten MAC im zu schützenden nichtflüchtigen Speicher 5a und 5b verglichen. Der Vergleich kann auch im kreuzweisen Vergleich erfolgen. Bei authentischen MAC's wird auf den Schritt 4063 verzweigt.

Es ist vorgesehen, im Schritt 4063 sowohl die Bildung des neuen Codewortes als auch die Speicherung von Abrechnungsdaten zumindest vorzubereiten, bevor auf die Abrechnungs- und Druckroutine im Schritt 406 verzweigt wird. Vom Schritt 4062 wird bei einem festgestellen Fehler bzw. bei Nichtübereinstimmung der MACs auf den Schritt 413 zur Statistik- und Fehlerauswertung zurückverzweigt.

Anderenfalls, wenn im Schritt 4060 eine nicht passende Pseudozufallszahl Z_{ist} während des Betriebes der Frankiermaschine vor jedem Abdruck erzeugt wird, d.h. eine Pseudozufallszahl Z_{ist}, welche beim Vergleich im Schritt 4061 eine Nichtübereinstimmung mit der mindestens einen im internen OPT-ROM des OTP-Prozessors gespeichert vorliegenden Zufallszahl Z_{soll} ergibt, dann wird ohne ein neues Codewort zu bilden auf die Abrechnungs- und Druckroutine im Schritt 406 verzweigt. Die MAC-Bildung erfolgt dann mittels des bisher gültigen Codewortes.

Die Erfindung vermeidet, daß wenn die Postregister samt Inhalt unbefugt entfernt werden, um beliebig viele Kopien anzufertigen, daß dann ohne Abrechnung bei der Datenzentrale bzw. Bezahlung bei der Post Postgüter frankiert werden können, wenn geklonte Speicherinhalte eingesetzt werden. Eine Verkapselung der NVRAM-Bauelemente für die Postregister mit einem Sicherheitsgehäuse ist nicht erforderlich. Wenn ein potentieller Manipulator, beispielsweise von der 1. bis 23. Frankierung mit geklonten Speichern (batteriegestützten CMOS-RAMs) arbeitet, ist dies mittels einer Selbstüberprüfung durch die Frankiermaschine automatisch nachträglich feststellbar, wenn dazwischen ein Codewortwechsel stattfand.

Es ist vorgesehen, daß die in den Postregister - d.h. insbesondere in den batteriegestützten CMOS-NVRAM's - enthaltenen Daten nach einer Zufalls- bzw. Pseudozufallsfolge ermittelten Stückzahl an Frankierungen auch im E^2PROM 20, 25 bzw. im internen OTP-Speicher 6d nichtflüchtig gespeichert werden.

Ein potentieller Verletzer kann nicht voraussehen, wann dies geschieht. Dabei ergibt sich ein durchschnittliches Abspeichern von beispielsweise 24 Frankierungen, so daß die Lebensdauer der E^2PROMs nicht gegenüber der bisherigen Lösung verringert wird.

Es wird von einem Code ausgegangen, der vor jeder (im Ý ca. nach der 24.Frankierung erfolgenden) Abspeicherung im E^2PROM vom Prozessor überprüft wird (im Schritt 4062, Fig.5) und welcher für jede neue Abspeicherung im E^2PROM gewechselt wird (im Schritt 4063, Fig.5). Dieser Prüfcode wird in einem k-ten Register der NVRAMs gespeichert und kann zugleich eine Prüfsumme, beispielsweise eine MAC-Absicherung für die Registerwerte bilden. Die Prüfsumme bzw. MAC-Absicherung für die Registerwerte wird mittels wechselnder und für NVRAM und E^2PROM unterschiedlicher Algorithmen und Schlüssel gebildet, welche in einem OTP-ROM eines OTP-Prozessors gespeichert vorliegen. Damit ist ein Kopieren des E^2PROM-Speicherinhalt auf den NVRAM sinnlos, wenn verschiedenen Prüfcode verschiedene Speicher mit zusammengehörigen bzw. aufeinander bezogenen Speicherinhalten absichern.

In einer einfachen Variante, wird zur Überprüfung ein verschlüsselter Prüfcode aus den Registerwerten für jede Stückzahl $n = i_{-1}$ gebildet und mit dem im E^2PROM gespeicherten MAC verglichen. Bei Gleichheit, gibt es eine Stückzahl $n = m$, bei der im NVRAM und im E^2PROM Daten entsprechend gespeichert wurden. Die einzelnen Registerwerte bilden für eine Anzahl $n = z$ Frankierungen eine Tabelle, welche eine Zeile für die Stückzahl m einschließt, bei welcher der Prüfcode im E^2PROM als MAC gespeichert wurde. Somit ergibt sich eine historische Abfolge von Daten für eine begrenzte Anzahl z. Für eine redundante Abspeicherung der Registerwerte kann jeder einzelne Registerwert verschlüsselt im E^2PROM gespeichert werden. Ein Vorteil der Erfindung ist aber, daß dies nicht bei jeder Abrechnung erfolgen muß. Ebensowenig muß jeder einzelne Registerwert im E^2PROM redundant gespeichert werden. Ein potentieller Manipulator vermag die Zugehörigkeit der Daten zu einer Zeile der Tabelle selbst nicht wiederherzustellen. Welche Schlüssel und Algorithmen wo eingesetzt werden, ist im OTP-ROM gelistet.

Ein Zeiger, dessen Daten verschlüsselt oder MAC-gesichert im E^2PROM gespeichert werden, weist auf entsprechende Stellen in der Liste im OTP-ROM (siehe Fig.8). Hierzu kann ein Zähler de- oder inkrementiert werden, um den Zeiger zu bilden.

Wenn eine Pseudozufallszahl (im Schritt 4061, Fig.5) erreicht ist und die Überprüfung der MACs vom NVRAM und vom E^2PROM eine Authentizität der Daten ergab, wird in einer bevorzugten Variante, eine Abrechnung vorgenommen und eine CRC-Prüfsumme über alle Registerwerte zum Zeitpunkt unmittelbar vor einer Frankierung bzw. vor dem Schritt 406 für die übliche Abrechnungs-und Druckroutine gebildet und unterschiedlich verschlüsselt zum NVRAM im E^2PROM gespeichert (im Schritt 4063, Fig.5). Wird dann zum Schritt 406, (Fig.5) verzweigt, braucht nur noch die Druckroutine ausgeführt werden, wie sie beispielsweise im EP 576 113 A2, im Schritt 49 der Fig.6 ausgeführt wird. Anderenfalls wird vom Schritt 4061 auf die normale Abrechnungs- und Druckroutine (im Schritt 406, Fig.5) direkt verzweigt und die Abrechnung im Schritt 406 ausgeführt, bevor ein Drucken erfolgt.

Die erfindungsgemäße Lösung basiert auf einer Ausbausicherheit von Prozessor mit internen oder

externen E^2PROM mit einer unlösbaren E^2PROM-Befestigung auf der Prozessor-Leiterplatte. Vor jeder neu zu registrierenden Stückzahl an Frankieraufdrucken wird auf Basis der vorhergehenden Stückzahl und gegebenenfalls der aktuellen vom Uhren/Datumsbaustein gelieferten Zeit eine Zufallszahl erzeugt. Solche elektronischen Zähler können auch mittels des batteriegestützten Uhren/Datums-Bausteins 8 realisiert werden. Der Uhren/Datums-Baustein kann dabei nicht auf ein zurückliegendes Datum vor dem aktuellen Datum eingestellt werden. Die laufende Zeit wird gemessen und in einen Zufallsalgorithmus eingegeben, um eine Zahl zu bilden. Wird eine vorbestimmte Zahl erreicht, wird bei der nächstfolgenden Frankierung eine redundante Abspeicherung im E^2PROM und NVRAM in o.g. Weise entsprechend gesichert vorgenommen.

In einer anderen Variante wird ein Pseudozufalls-Algorithmus mittels eines Bitmustergenerators hardwaremäßig generiert. Hierbei handelt es sich um ein n-fach-Schieberegister mit spezieller Rückkopplung, welches vorzugsweise Bestandteil eines ASICs sein kann.

In dem vorgenannten ASIC können E^2PROM und Prozessor mindestens mit ihren sicherheitsrelevanten Teilen realisiert sein.

Durch den Pseudozufalls-Algorithmus ergibt sich ein durchschnittlicher Wert von ca. 24 Frankierungen, bei welchen redundant abgespeichert wird. Ein E^2PROM (ca.10.000 Zyklen) könnte somit 24 * 10.000 = 240.000 Frankierungen durchhalten.

Vorteilhaft wird von einem nichtflüchtigen Speicher im OTP bzw. (ausbau)sicher zum OTP angeordneten E^2PROM ausgegangen, um die Manipulationssicherheit gegenüber geklonten Speicherinhalten zu gewährleisten. Dabei wird nicht nur von bestimmten Zeitpunkten abhängig, wie beim Einschalten und/oder Übergang in den Standby-Betrieb, eine Speicherung vorgenommen, um die Manipulationssicherheit gegenüber geklonten Speicherinhalten zu gewährleisten (Verzweigung auf Punkt p, Fig.3), sondern der vorgenannte zeitpunkt ist nunmehr zufällig gewährt. Der Zeitpunkt des Abspeicherns kann somit von einem potentiellen Fälscher nicht mehr logisch abgeleitet bzw. vorausgesehen, sondern nur noch nachträglich in Bezug zur Stückzahl ermittelt werden.

Im Schritt 406 werden die in bekannter Weise zur Abrechnung eingezogenen Registerdaten ggf. inhaltlich überprüft und entsprechend geändert. Beispielsweise wird bei einem gültigen Frankieren mit einem Wert > 0 der Stückzähler R4 inkrementiert. Der Registerwert R1 wird verringert und der Registerwert R2 entsprechend erhöht, so daß der Registerwert R3 konstant bleibt. Danach wird eine Prüfsumme (beispielsweise CRC) über jeden der Registerwerte gebildet und im NVM 5a und/oder NVM 5b zusammen mit den zugehörigen Registerwerten gespeichert. Eine solche Absicherung, die über die einzelnen Registerdaten gelegt wurde, um eine Manipulation Verringern von R2 (Verbrauchssumme) und Erhöhung von R1 (Restwert) bei gleichbleibenden R3 während des laufenden Betriebes zu verhindern, wurde bereits in der Anmeldung DE 43 44 476 A1 vorgeschlagen. Der MAC (Message Authentification Code) ist eine verschlüsselte Checksumme, welche an den Registerwert bei Abrechnung im Schritt 406 (Fig.4) angehängt wird. Geeignet ist beispielsweise eine DES-Verschlüsselung. Im Frankiermodus 400 (Fig.4) kann bei der Abrechnung zusätzlich noch der Dateninhalt überprüft werden, ob die Registerwertsumme R3 gleich der Summe aus Ascending-Register R1 (Restwert) und Descending-Register R2 ist. Aufgrund der Absicherung mit den verschlüsselten Prüfsummen kann aber auf eine inhaltliche Überprüfung völlig verzichtet werden, zumal eine solche von der Datenzentrale bei jeder Kommunikation mit der Frankiermaschine durchgeführt wird. Sind alle Spalten eines Druckbildes gedruckt worden, wird wieder zur Systemroutine 200 zurückverzweigt.

Zusätzlich zur vorgenannten Bildung von neuen Codewörtern mittels Pseudozufallsfolge werden auch bei einem anderen letzten Betriebszustand der Frankiermaschine die nichtflüchtigen Speicher (E^2PROM und NVRAMs) redundant mit einem neuen Codewort beschrieben. Ein solche andere letzter Betriebszustand ist vorbestimmten Zuständen zugeordnet ist, wie vorstehen beschrieben wurde.

Die Anzahl von gedruckten Briefen, und die aktuellen Werte in den Postregistern werden entsprechend der eingegebenen Kostenstelle im nichtflüchtigen Speicher 5a der Frankiermaschine während der Abrechnungsroutine 406 registriert und stehen für eine spätere Auswertung zur Verfügung. Ein spezieller Sleeping-Mode-Zähler wird während der unmittelbar vor dem Druck erfolgenden Abrechnungsroutine veranlaßt, einen Zählschritt weiterzuzählen. Die Registerwerte können bei Bedarf im Anzeigemodus 215 (Fig.3) abgefragt werden. Von diesem wird anschließend zur Systemroutine 200 zurückverzweigt.

Für die frankiermaschineninterne Sicherheitsschaltung eignet sich der TMS370 C010 aus der Prozessor-Familie von Texas Instrument. Dieser weist ein internes E^2PROM von 256 Bytes als NVM auf.

In einer Variante enthalten der nichtflüchtige interne Prozessorspeicher und der zu schützende nichtflüchtige Postregisterspeicher (Bat-NV-CMOS-RAM's) nicht das identische, sondern einer von beiden das komplementäre Codewort. Das prozessorinterne Codewort ist nicht von außen abfragbar.

In einer anderen Variante sind verschiedene Codeworter einzelnen Speichern zugeordnet, wobei die verschiedenen Codewörter jedoch einen gemeinsamen Stamm haben, aus dem sie gebildet wurden und wobei der gemeinsame Stamm vom Prozessor rekonstruiert wird, um die Gültigkeit der einzelnen Codewörter zu überprüfen.

Die Routine zum Codewörter-Vergleich bzw. zur Gültigkeitsprüfung wird im Prozessor jeweils nach dem Einschalten bzw. bei Programmfortsetzung abgefragt. Wird beim Vergleich eine Unstimmigkeit festgestellt, wird die Frankiermaschine für den weiteren Betrieb

blockiert.

Es ist weiterhin vorgesehen, daß die Anzahl der Bildung von neuen Codewörtern ab einem vorbestimmten Zeitpunkt gezählt und nichtflüchtig prozessorintern gespeichert wird. Zum Zeitpunkt einer Kommunikation mit der Datenzentrale wird die vorgenannte Anzahl an in der Vergangenheit gebildeten Codewörtern und das aktuell gültige Codewort abgefragt. Das erlaubt bei einer unabsichtlichen Blockierung der Frankiermaschine aufgrund ungültiger Codewörter dann bei Bedarf die nachträgliche Wiederherstellung des alten Zustandes durch entsprechende Datenübermittlung seitens der Datenzentrale an die Frankiermaschine.

Es ist vorgesehen, daß ein dem Codewort entsprechender letzter Betriebszustand der Frankiermaschine einen Zustand im Ergebnis der Herstellung oder einer Nachladung der Frankiermaschine oder einen Zustand vor dem Ausschalten der Frankiermaschine oder einen Zustand vor einem Spannungsausfall oder vor einer Stillstandszeit (Stand by) bzw. vor Programmunterbrechung einschließt. Ebenfalls können bei der Überwachung weiterer Kriterien solche letzten Betriebszustände eintreten, indem die Frankiermaschine zu einem entsprechenden Modus übergeht. Solche Schritte 202 bzw. 207 für eine Überwachung weiterer Kriterien weist der in der Figur 3 dargestellte Gesamtablaufplan für die Frankiermaschine auf. Bei einer Verletzung eines der Sicherheitskriterien tritt die Frankiermaschine in einen entsprechenden Modus ein und führt zusätzlich in entsprechenden Subroutinen die - in der Figur 7 dargestellten - erfindungsgemäßen Schritte 106 bis 109 aus. Tritt die Frankiermaschine beispielsweise in einen Sleeping-Modus ein, wenn nach Verbrauch einer vorbestimmten Stückzahl noch keine Verbindung zur Datenzentrale aufgenommen wurde, und wird keine manuelle Auslösung einer Kommunikation durch den Nutzer vorgenommen, erfolgt bei Erschöpfung des Stückzahlkredites eine automatische Kommunikation mit der Datenzentrale und eine Durchführung des Verfahrens zur Erhöhung der Manipulationssicherheit von kritischen Registerdaten.

Die Erfindung ist nicht auf die vorliegenden Ausführungsform beschränkt, da offensichtlich weitere andere Anordnungen bzw. Ausführungen des Verfahrens für andere informationsverarbeitende Einrichtungen entwickelt bzw. eingesetzt werden können, die vom gleichen Grundgedanken der Erfindung ausgehend, von den anliegenden Ansprüchen umfaßt werden.

Patentansprüche

1. Verfahren zur Erhöhung der Manipulationssicherheit von kritischen Daten, insbesondere von Registerdaten in Frankiermaschinen, **gekennzeichnet**, durch die Schritte:

   - Laden einer Zahl oder eines Zeigers, welcher einem Codewortes zugeordnet ist, in einen ersten nichtflüchtigen Speicher (20 bzw 6d), der gegen Herausnahme und Manipulation abgesichert ist,
   - Laden eines Codewortes in zweite die Postregisterdaten enthaltenden nichtflüchtigen Speicher (NVM 5a, 5b), wobei das Codewort dem letzten Betriebszustand der Frankiermaschine zugeordnet ist bzw. vom Prozessor (6, 6a) entsprechend ausgewählt worden ist,
   - Gültigkeitsprüfung des Codewortes mindestens zum Zeitpunkt des Einschaltens der Frankiermaschine und nachfolgend aufgrund eines Ereignisses,
   - Ersetzen des alten Codewortes durch ein vorbestimmtes neues Codewort, wenn der Prozessor, nach Gültigkeitsprüfung mit Bezug auf das in seinem internen Prozessorspeicher (NVM 6c) aus einer Liste mit gespeicherten Codewörten entsprechend der Zahl bzw. der Zeigerstellung ausgewählte Codewort, die Gültigkeit des alten Codewortes anerkennt oder
   - Blockierung der Frankiermaschine nach dem Zeitpunkt des Einschaltens der Frankiermaschine, wenn der Prozessor nach Gültigkeitsprüfung mit Bezug auf das ausgewählte in vorgenannter Liste gespeicherte Codewort die Gültigkeit des alten Codewortes aberkennt.

2. Verfahren, nach Anspruch 1, **dadurch gekennzeichnet**, daß ein dem Codewort entsprechender letzter Betriebszustand der Frankiermaschine einen Zustand im Ergebnis der Herstellung oder einer Nachladung der Frankiermaschine oder im Ergebnis der Bildung einer Pseudozufallsfolge oder einen Zustand vor dem Ausschalten der Frankiermaschine oder einen Zustand vor einem Spannungsausfall oder vor einer Stillstandszeit (Stand by) bzw. vor Programmunterbrechung einschließt und daß die Gültigkeitsprüfung des Codewortes mindestens zum Zeitpunkt des Einschaltens der Frankiermaschine und nachfolgend mindestens aufgrund einer Pseudozufallsfolge in Abständen durchgeführt wird.

3. Verfahren, nach den Ansprüchen 1 bis 2, **dadurch gekennzeichnet**, daß ein Laden eines neuen Codewortes in zu schützende nichtflüchtige Speicher (NVM 5a, 5b), erfolgt, wobei das Programm für die Berechnung der Zeigerstellung bzw. Bildung des jeweils neuen Codewortes im Programmspeicher (PSP 11) gespeichert ist.

4. Verfahren, nach den Ansprüchen 1 bis 3, **dadurch gekennzeichnet**, daß der Zeiger außerhalb des jeweils zu überprüfenden lösbar eingebauten nichtflüchtigen Speichers (NVM 5a, 5b) in dem ständig eingebauten und/oder während der Laufzeit der Frankiermaschine mit ihrem Prozessorsystem in Kommunikationsverbindung stehenden und gegen Herausnahme und Manipulation während der Lauf-

zeit der Frankiermaschine abgesicherten ersten Sicherheitsspeicher nichtflüchtig gespeichert wird und daß die Auswahl des neuen Codewortes vom vorherigen abhängig ist.

5. Verfahren, nach den Ansprüchen 1 bis 4, **dadurch gekennzeichnet**, daß die Nachladung mit einem monetären Guthaben, Stückzahl S und/oder anderen Daten in einem Kommunikationsmodus (300) erfolgt, daß die Anzahl der Bildung von neuen Codewörtern ab einem vorbestimmten Zeitpunkt gezählt und nichtflüchtig prozessorintern gespeichert wird und zum Zeitpunkt einer Kommunikation mit der Datenzentrale die vorgenannte Anzahl an in der Vergangenheit gebildeten Codewörtern und das aktuell gültige Codewort abgefragt wird, zum Überwinden einer unabsichtlichen Blockierung der Frankiermaschine aufgrund ungültiger Codewörter bzw. bei Bedarf die nachträgliche Wiederherstellung des alten Zustandes durch entsprechende Datenübermittlung seitens der Datenzentrale an die Frankiermaschine.

6. Verfahren, nach den Ansprüchen 1 bis 5, **dadurch gekennzeichnet**, daß eine Überwachung weiterer Kriterien erfolgt und solche vorgenannten letzten Betriebszustände eintreten, indem die Frankiermaschine zu einem entsprechenden Modus bei einer Verletzung eines der Sicherheitskriterien übergeht, daß die in einen entsprechenden Modus eingetretene Frankiermaschine in zusätzlichen entsprechenden Subroutinen die Schritte (106 bis 109) zur Durchführung des Verfahrens zur Erhöhung der Manipulationssicherheit von kritischen Registerdaten ausführt.

7. Verfahren, nach den Ansprüchen 1 bis 6, **dadurch gekennzeichnet**, daß jedem nichtflüchtigem Speicher oder Speicherbereich ein separates Codewort zugeordnet wird, wobei mindestens eines der vorgenannten separaten Codeworte in einem weiteren internen Speicher eines Prozessorsystems, einer Chipkarte und/oder eines ähnlichen Systems nichtflüchtig gespeichert worden ist, welches während der Laufzeit der Frankiermaschine mit dem Prozessorsystem der Frankiermaschine in Kommunikationsverbindung steht und gegen Herausnahme und Manipulation während der Laufzeit der Frankiermaschine abgesichert ist und daß eine Bildung von neuen Codewörtern ab einem vorbestimmten Ereignis und danach eine Einspeicherung der neuen Codewörter in die zu schützenden nichtflüchtigen Speicher und in die weiteren nichtflüchtigen Speicher vorgenommen wird.

8. Verfahren zur Erhöhung der Manipulationssicherheit von kritischen Daten, insbesondere von Registerdaten in Frankiermaschinen, **gekennzeichnet**, durch die Schritte:

- Laden eines Codewortes in einen ersten internen Prozessorspeicher (NVM 6d) zur nichtflüchtigen Speicherung und in zweite die Postregisterdaten enthaltenen nichtflüchtigen Speicher (NVM 5a, 5b), wobei das Codewort dem letzten Betriebszustand der Frankiermaschine entspricht,
- Gültigkeitsprüfung des Codewortes mindestens zum Zeitpunkt des Einschaltens der Frankiermaschine und nachfolgend aufgrund eines Ereignisses,
- Ersetzen des alten Codewortes durch ein vorbestimmtes neues Codewort, wenn der Prozessor nach Gültigkeitsprüfung mit Bezug auf das in seinem ersten nichtflüchtigen internen Prozessorspeicher (NVM 6d) gespeicherte Codewort die Gültigkeit des alten Codewortes anerkennt oder
- Blockierung der Frankiermaschine nach dem Zeitpunkt des Einschaltens der Frankiermaschine, wenn der Prozessor nach Gültigkeitsprüfung mit Bezug auf das in seinem ersten nichtflüchtigen internen Prozessorspeicher (NVM 6d) gespeicherte Codewort die Gültigkeit des alten Codewortes aberkennt.

9. Verfahren, nach Anspruch 8, **dadurch gekennzeichnet**, daß ein dem Codewort entsprechender letzter Betriebszustand der Frankiermaschine einen Zustand im Ergebnis der Herstellung oder einer Nachladung der Frankiermaschine oder im Ergebnis der Bildung einer Pseudozufallsfolge oder einen Zustand vor dem Ausschalten der Frankiermaschine oder einen Zustand vor einem Spannungsausfall oder vor einer Stillstandszeit (Stand by) bzw. vor Programmunterbrechung einschließt und daß die Gültigkeitsprüfung des Codewortes mindestens zum Zeitpunkt des Einschaltens der Frankiermaschine und nachfolgend mindestens aufgrund einer Pseudozufallsfolge in Abständen durchgeführt wird.

10. Verfahren, nach Anspruch 9, **dadurch gekennzeichnet**, daß die Nachladung mit einem monetären Guthaben, Stückzahl S und/oder anderen Daten in einem Kommunikationsmodus (300) erfolgt, daß die Anzahl der Bildung von neuen Codewörtern ab einem vorbestimmten Zeitpunkt gezählt und nichtflüchtig prozessorintern gespeichert wird und zum Zeitpunkt einer Kommunikation mit der Datenzentrale die vorgenannte Anzahl an in der Vergangenheit gebildeten Codewörtern und das aktuell gültige Codewort abgefragt wird, zum Überwinden einer unabsichtlichen Blockierung der Frankiermaschine aufgrund ungültiger Codewörter bzw. bei Bedarf die nachträgliche Wiederherstellung des alten Zustandes durch entsprechende Datenübermittlung seitens der Datenzentrale an die Frankiermaschine.

11. Verfahren, nach Anspruch 9, **dadurch gekennzeichnet**, daß eine Überwachung weiterer Kriterien erfolgt und solche vorgenannten letzten Betriebszustände eintreten, indem die Frankiermaschine zu einem entsprechenden Modus bei einer Verletzung eines der Sicherheitskriterien übergeht, daß die in einen entsprechenden Modus eingetretene Frankiermaschine in zusätzlichen entsprechenden Subroutinen die Schritte (106 bis 109) zur Durchführung des Verfahrens zur Erhöhung der Manipulationssicherheit von kritischen Registerdaten ausführt.

12. Verfahren, nach Anspruch 8, **dadurch gekennzeichnet**, Laden eines Codewortes in den ersten internen Prozessorspeicher (NVM 6d) zur nichtflüchtigen Speicherung und in eine Vielzahl an zweiten die zusichernden Daten enthaltenen nichtflüchtigen Speichern (NVM 5a, 5b), wobei das alte Codewort dem vorletzten Betriebszustand der Frankiermaschine entsprechend für die Vielzahl nichtflüchtiger Speicher (NVM 6d, NVM 5a und NVM 5b) im Schritt 107 überprüft wird und vor der entsprechenden Veränderung von Codewörtern V und U zunächst im Schritt 108 ein neues Codewort W' und dannach ein Codewort T' für den zweiten prozessorinternen nichtflüchtigen Speicher (NVM 6d) gebildet wird, nach den Gleichungen:

$$W' := f\{P1\} \text{ und} \quad (1)$$

$$T' := f\{P2\} \quad (2)$$

wobei P1 und P2 verschiedene monoton stetig veränderbare Parameter sind, beispielsweise die aktuelle Zeit, Anzahl von Programmunterbrechungen bzw. andere Programm-, Zeit- oder pysikalische Parameter.

13. Verfahren, nach Anspruch 12, **dadurch gekennzeichnet**, daß vor dem Laden eines neuen Codewortes ein Zählwert inkrementiert und dann das neue Codewort (W', T', U', V') berechnet wird.

14. Verfahren, nach Anspruch 8, **dadurch gekennzeichnet**, daß die Bildung des neuen Codewort vom vorherigen abhängig ist, wobei für einen ersten und zweiten nichtflüchtige Speicher NVM (6d, 20, 25 und 5a, 5b) nach Uberprüfung des alten Codewortes im Schritt 107 und vor der entsprechenden Veränderung von Codewötern V und U zunächst im Schritt 108 ein neues Codewort W' und dannach ein Codewort T' gebildet wird, nach den Gleichungen:

$$W' := F\{P1\} \text{ und} \quad (1)$$

$$T' := F\{P2\}, \quad (2)$$

wobei P1 und P2 gelistete Codewörter sind.

15. Verfahren, nach Anspruch 8, **dadurch gekennzeichnet**, daß ein Laden eines neuen Codewortes erfolgt, wobei das Programm für die Berechnung des jeweils neuen Codewortes im Programmspeicher (PSP 11) gespeichert ist.

16. Verfahren, nach Anspruch 15, **dadurch gekennzeichnet**, daß als Programmspeicher ein ROM bzw. EPROM verwendet wird.

17. Verfahren zur Erhöhung der Manipulationssicherheit von kritischen Daten, **dadurch gekennzeichnet**, daß jedem nichtflüchtigem Speicher oder Speicherbereich ein separates Codewort zugeordnet wird, wobei (vorher oder gleichzeitig) mindestens eines der vorgenannten separaten Codeworte im internem Prozessorspeicher nichtflüchtig gespeichert worden ist, daß ein Wechsel des Codewortes ab einem vorbestimmten Ereignis und danach eine Einspeicherung der neuen Codewörter in die zu schützenden nichtflüchtigen Speicher vorgenommen wird, wobei der Wechsel vorgenommen wird, nach dem die Gültigkeit des Codewortes festgestellt worden ist, oder anderenfalls bei Ungültigkeit die Maschine gesperrt wird.

18. Verfahren, nach Anspruch 17, **dadurch gekennzeichnet**, daß das Codewort in zeitlichen oder stückzahlmäßigen Abständen gewechselt wird und daß die Bildung des neuen Codewortes vom vorherigen abhängig ist.

19. Verfahren, nach Anspruch 17, **dadurch gekennzeichnet**, daß in einem Schritt (108) zur Bildung eines neuen veränderbaren ersten Codewortes (T', W') auch die Bildung des neuen zweiten Codewortes (V', U') identisch zur Bildung des neuen ersten Codewortes (T', W') erfolgt, um ein identisches neues zweites Codewort (V', U') in die zu schützenden nichtflüchtigen Speicher (NVMs 5a, 5b) zu laden.

20. Verfahren, nach Anspruch 17, **dadurch gekennzeichnet**, daß in einem Schritt (108) zur Bildung eines neuen veränderbares ersten Codewortes (T', W') auch die Bildung des neuen zweiten Codewortes (V", U") als komplementärer Schatten (V", U") zum neuen ersten Codewortes (T', W') erfolgt, um ein komplementäres neues zweites Codewort (V', U') in die zu schützenden nichtflüchtigen Speicher (NVMs 5a, 5b) zu laden.

21. Verfahren, nach Anspruch 17, **dadurch gekennzeichnet**, daß in einem Schritt (108) zur Bildung eines neuen veränderbares ersten Codewortes (T', W') auch die Bildung des neuen zweiten Codewortes (V',U") als zu dem veränderbaren neuen ersten

Codewort (W') identischen Codewort (V') und als komplementärer Schatten (U") zum neuen ersten Codewortes (T') erfolgt, um mindestens ein neues zweites Codewort (V', U") in die zu schützenden nichtflüchtigen Speicher (NVMs 5a, 5b) zu laden oder daß beim Schutz eines entsprechenden Speichers (NVM's) in mindestens einem der Speicherbereiche auch mit dem komplementären Schatten (V" oder U") gearbeitet wird.

22. Verfahren zur Erhöhung der Manipulationssicherheit von kritischen Registerdaten gekennzeichnet **durch** die Schritte:

- Laden eines mittels einem Codewort erzeugten Autentifikationscodes (MAC_n), welcher dem Codewort zugeordnet ist, welches Abrechnungsdaten verschlüsselt, in einen ersten nichtflüchtigen Speicher (20 oder 25), der während der Laufdauer der Maschine gegen eine Herausnahme und Manipulation gesichert ist,
- Laden der Abrechnungsdaten und des vorgenannten Autentifikationscodes (MAC_n) in zweite die Postregisterdaten enthaltende zu schützende nichtflüchtige Speicher NVM (5a, 5b), wobei das Codewort dem letzten Betriebszustand der Maschine zugeordnet ist,
- Gültigkeitsprüfung des Autentifikationscodes (MAC_n), welcher dem Codewort zugeordnet ist, mindestens zum Zeitpunkt des Einschaltens der Maschine und nachfolgend aufgrund eines Ereignisses,
- Ersetzen des alten Codewortes durch ein vorbestimmtes neues Codewort zur Bildung eines weiteren Autentifikationscodes (MAC_{n+1}), welcher dem neuen Codewort zugeordnet ist, welches Abrechnungsdaten verschlüsselt, wenn der Prozessor die Gültigkeit des alten Codewortes anerkennt oder
- Blockierung der Maschine nach dem Zeitpunkt ihres Einschaltens, wenn der Prozessor nach Gültigkeitsprüfung die Gültigkeit des anhand des alten Codewortes geprüften Autentifikationscodes (MAC_n) aberkennt.

23. Verfahren, nach Anspruch 22, **dadurch gekennzeichnet**, daß die Abstände für das Laden eines Autentifikationscodes (MAC) nach dem Zeitpunkt des Einschaltens der Frankiermaschine zeitliche oder stückzahlmäßige Abstände und/oder solche mindestens aufgrund einer Pseudozufallsfolge bestimmten Abständen sind.

24. Verfahren zur Erhöhung der Manipulationssicherheit von kritischen Daten, **dadurch gekennzeichnet**, daß in jedem nichtflüchtigem Speicher oder Speicherbereich ein mittels einem separaten Codewort erzeugter Autentifikationscodes (MAC_n) gespeichert wird, wobei mindestens eines der vorgenannten Autentifikationscodes (MAC_n) und separaten Codeworte in einem ersten internen Speicher eines Prozessorsystems, einer Chipkarte und/oder eines ähnlichen Systems nichtflüchtig gespeichert worden ist, welches während der Laufzeit der Maschine mit ihrem Prozessorsystem in Kommunikationsverbindung steht und gegen Herausnahme und Manipulation während der Laufzeit der Maschine abgesichert ist und daß eine Bildung von neuen Codewörtern ab einem vorbestimmten Ereignis und danach eine Einspeicherung der mittels der neuen Codewörter erzeugten Autentifikationscodes (MAC_{n+1}) in die zu schützenden nichtflüchtigen Speicher und in die ersten nichtflüchtigen Speicher vorgenommen wird.

25. Anordnung zur Erhöhung der Manipulationssicherheit von kritischen Daten, insbesondere von Registerdaten in Frankiermaschinen mit Eingabe- und Ausgabemitteln, einer Steuereinrichtung und Speichern, **dadurch gekennzeichnet**, daß die Steuereinrichtung (6) einen Mikroprozessor oder einen OTP-Prozessor (ONE TIME PROGRAMMABLE) aufweist, in welchem neben einem Mikroprozessor CPU (6a) auch weitere Schaltungen und/oder Programme bzw. Daten im internen OTP-ROM (6c) bzw. im internen OTP-RAM (6b) in einem gemeinsamen Bauelementgehäuse untergebracht sind, welche ein erstes Sicherheitsmittel gegen unbefugte Manipulation bilden, daß ein erster und ein zweiter nichtflüchtiger Speicher mit der Steuereinrichtung (6) verbunden ist, wobei der erste nichtflüchtige Speicher NVM (6d, 20, 25) ein zweites Sicherheitsmittel gegen unbefugte Manipulation bildet und gegen Herausnahme gesichert ist.

26. Anordnung, nach Anspruch 25, **dadurch gekennzeichnet**, daß der erste nichtflüchtige Speicher als interner Prozessorspeicher (NVM 6d) zur nichtflüchtigen Speicherung im Prozessor (6) realisiert ist oder als externer nichtflüchtiger Speicher NVM (20, 25) am Prozessor (6) angeschlossen ist.

27. Anordnung, nach den Ansprüchen 25 bis 26, **dadurch gekennzeichnet**, daß der externe nichtflüchtiger Speicher NVM (25) über einen Ein/Ausgabe-Steuermodul (4) am Prozessor (6) angeschlossen ist und während der Laufzeit der Frankiermaschine gegen Herausnahme gesichert ist.

28. Anordnung, nach Anspruch 27, **dadurch gekennzeichnet**, daß der externe nichtflüchtiger Speicher NVM (25) Bestandteil einer Chipkarte ist und über eine Chipkarten-Schreib/Leseeinheit (21) am Ein/Ausgabe-Steuermodul (4) angeschlossen ist.

29. Anordnung, nach Anspruch 25, **dadurch gekennzeichnet**, daß der Programmspeicher ein EPROM

ist.

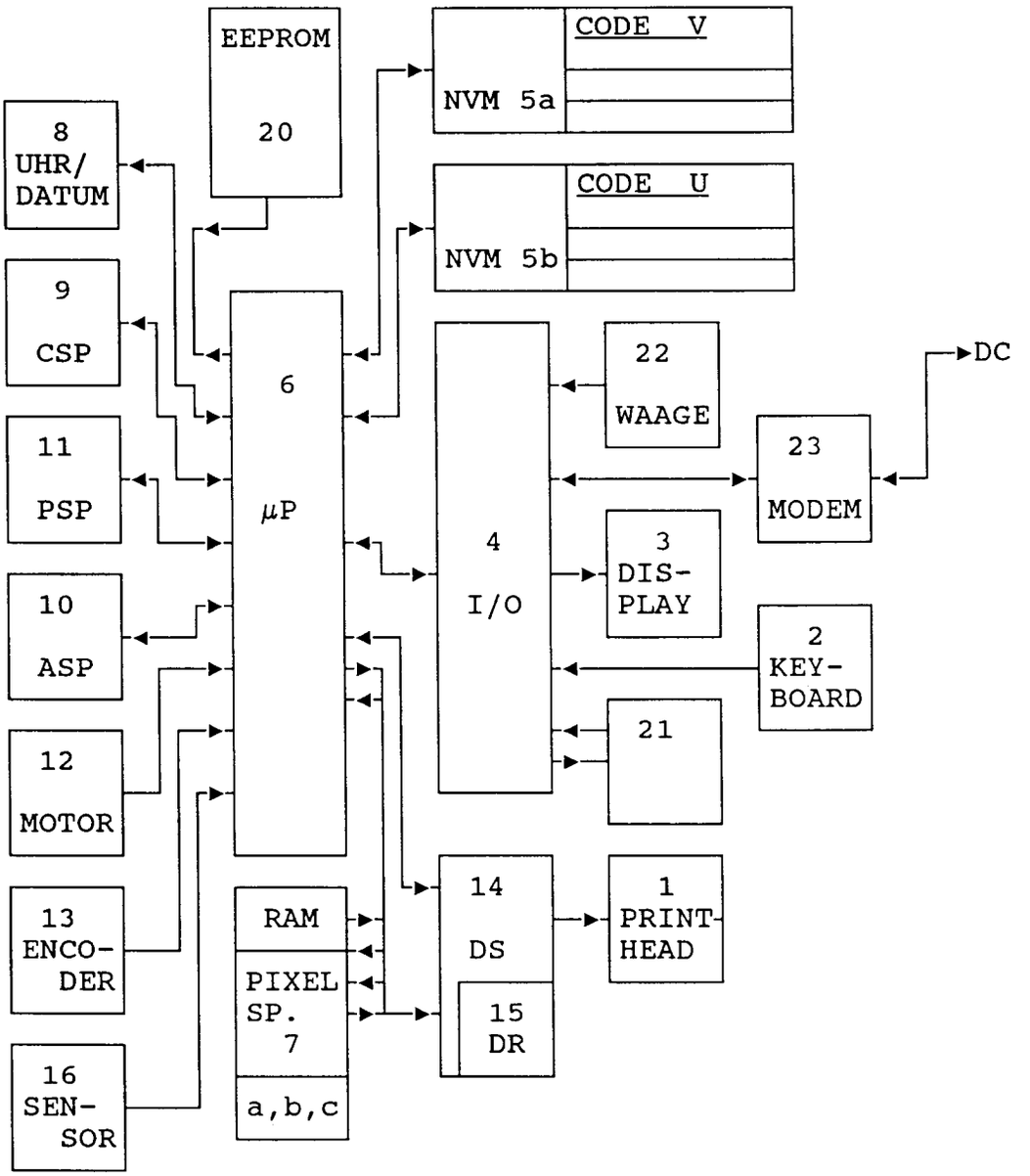
EEPROM
20
NVM 5a
CODE V
NVM 5b
CODE U
8
UHR/
DATUM
9
CSP
11
PSP
10
ASP
12
MOTOR
13
ENCO-
DER
16
SEN-
SOR
6
µP
RAM
PIXEL
SP.
7
a,b,c
4
I/O
22
WAAGE
23
MODEM
DC
3
DIS-
PLAY
2
KEY-
BOARD
21
14
DS
15
DR
1
PRINT-
HEAD

Fig. 1a

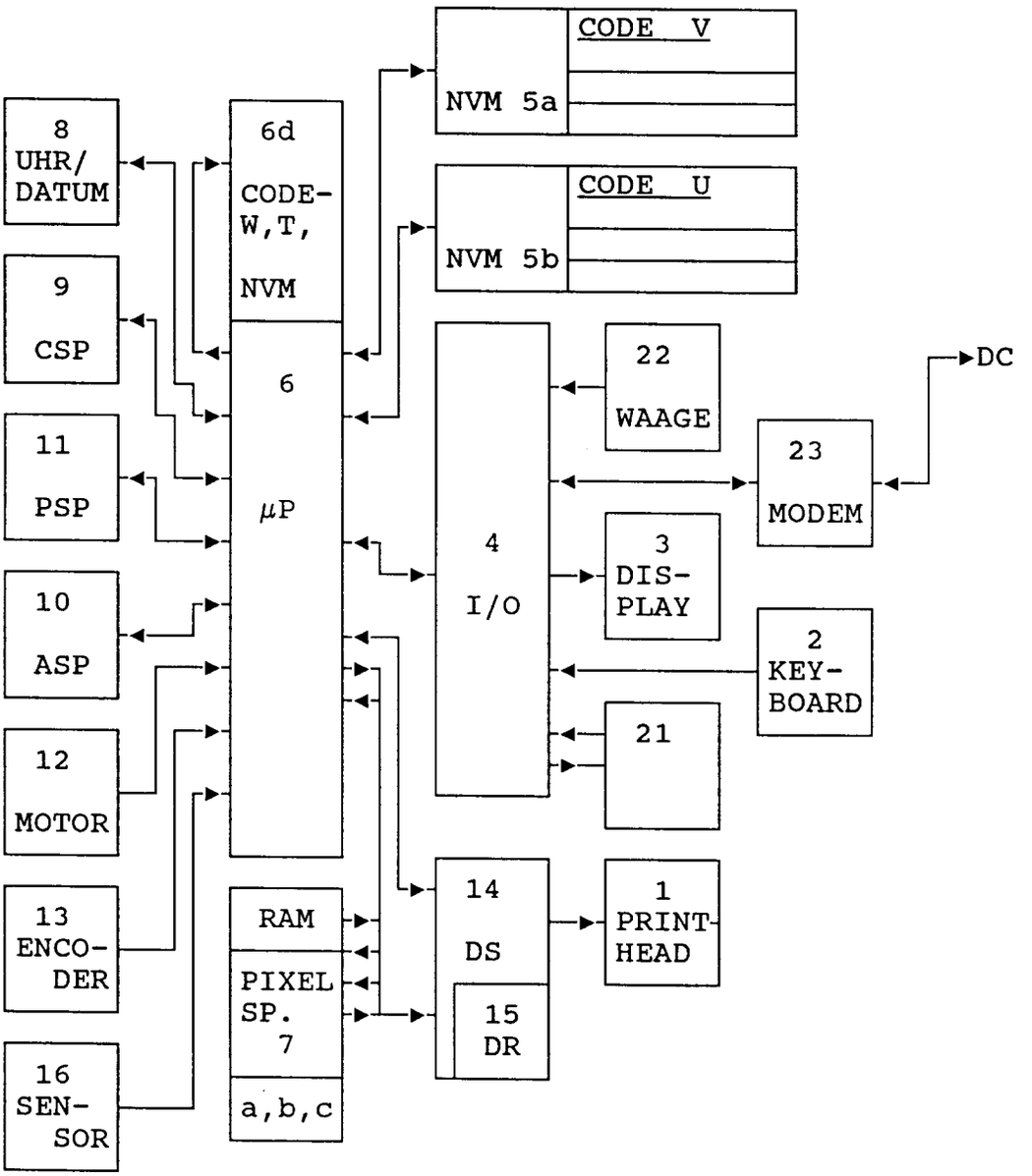
8
UHR/
DATUM
9
CSP
11
PSP
10
ASP
12
MOTOR
13
ENCO-
DER
16
SEN-
SOR
6d
CODE-
W,T,
NVM
6
µP
RAM
PIXEL
SP.
7
a,b,c
NVM 5a
CODE V
NVM 5b
CODE U
4
I/O
22
WAAGE
3
DIS-
PLAY
21
14
DS
15
DR
1
PRINT-
HEAD
23
MODEM
DC
2
KEY-
BOARD

Fig. 1b

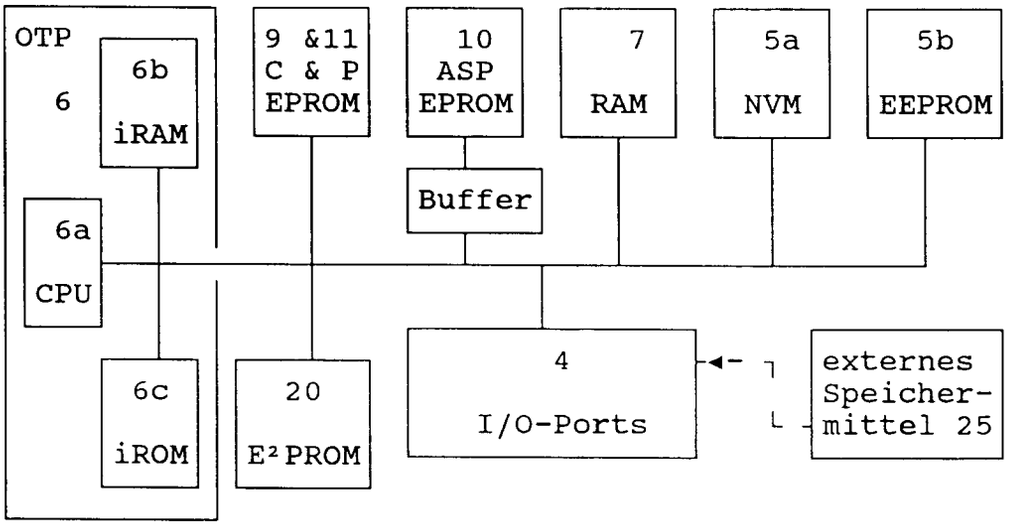
OTP
6
6b
iRAM
6a
CPU
6c
iROM
9 &11
C & P
EPROM
20
E²PROM
10
ASP
EPROM
Buffer
7
RAM
5a
NVM
5b
EEPROM
4
I/O-Ports
externes
Speicher-
mittel 25

Fig. 2a

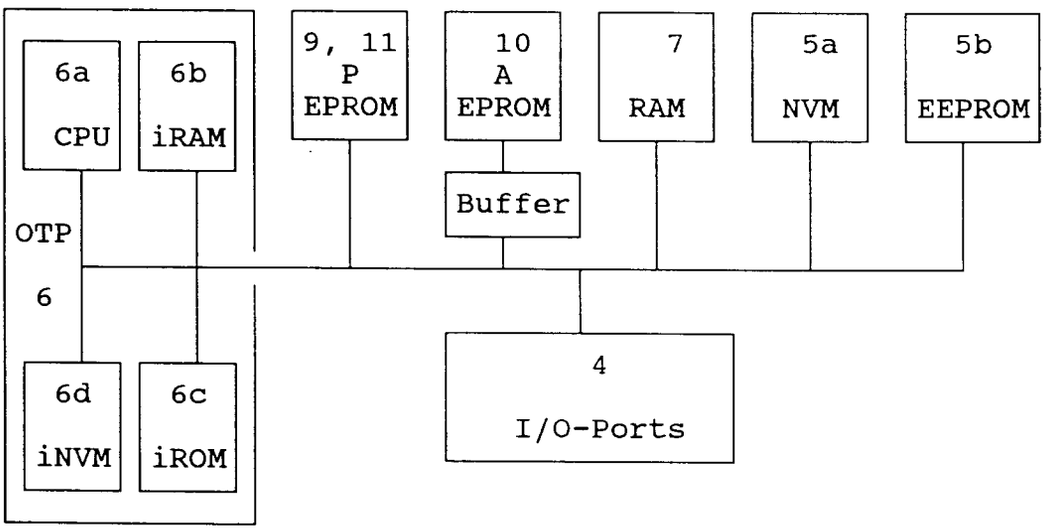
6a
CPU
6b
iRAM
OTP
6
6d
iNVM
6c
iROM
9, 11
P
EPROM
10
A
EPROM
Buffer
7
RAM
5a
NVM
5b
EEPROM
4
I/O-Ports

Fig. 2b

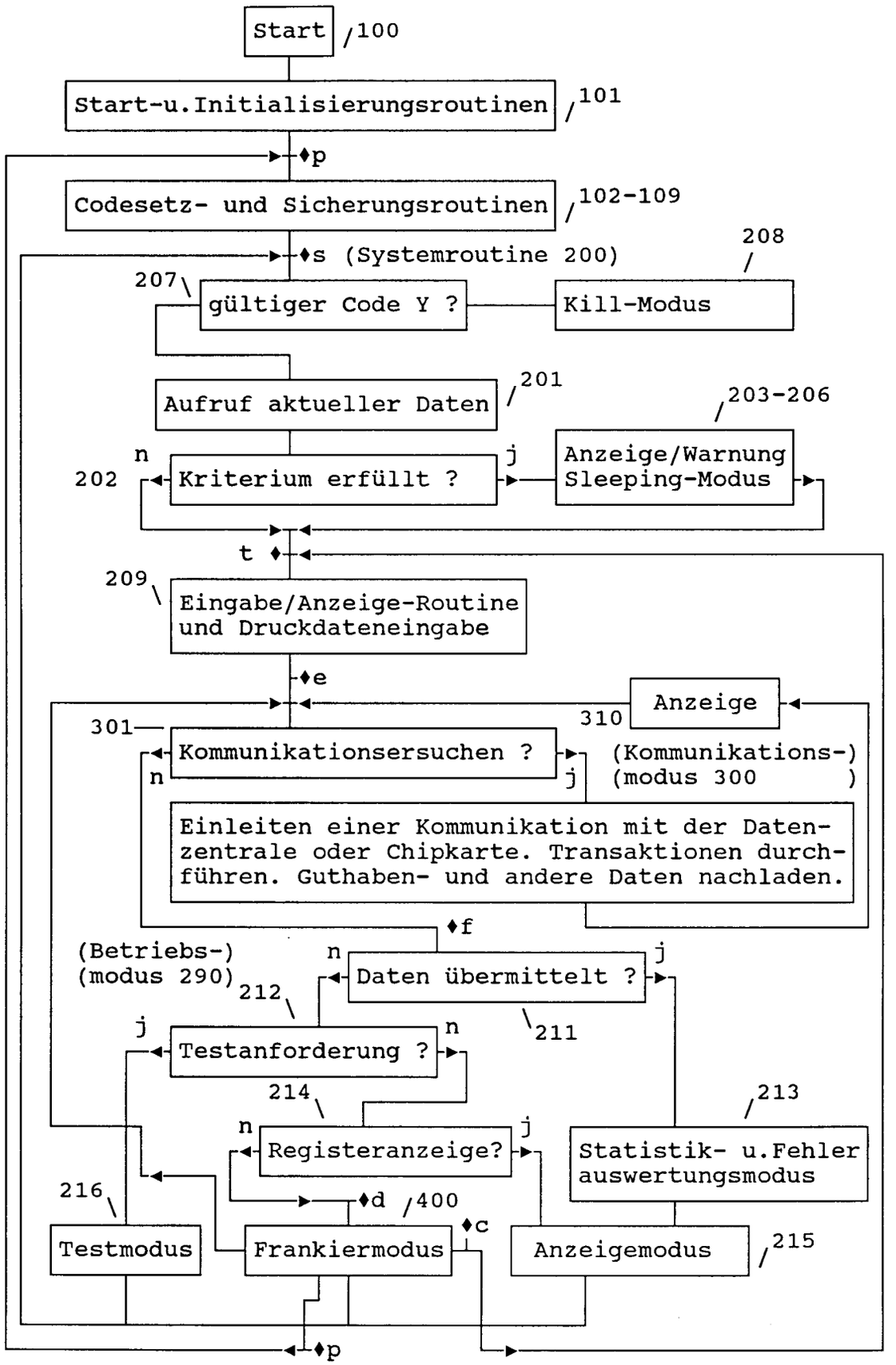
Start
100
Start-u.Initialisierungsroutinen
101
♦p
Codesetz- und Sicherungsroutinen
102-109
♦s (Systemroutine 200)
208
207
gültiger Code Y ?
Kill-Modus
Aufruf aktueller Daten
201
203-206
n
j
202
Kriterium erfüllt ?
Anzeige/Warnung
Sleeping-Modus
t ♦
209
Eingabe/Anzeige-Routine
und Druckdateneingabe
♦e
Anzeige
310
301
Kommunikationsersuchen ?
(Kommunikations-)
(modus 300)
Einleiten einer Kommunikation mit der Datenzentrale oder Chipkarte. Transaktionen durchführen. Guthaben- und andere Daten nachladen.
♦f
(Betriebs-)
(modus 290)
Daten übermittelt ?
212
211
Testanforderung ?
214
213
Registeranzeige?
Statistik- u.Fehler
auswertungsmodus
216
♦d
400
♦c
Testmodus
Frankiermodus
Anzeigemodus
215
♦p

Fig. 3

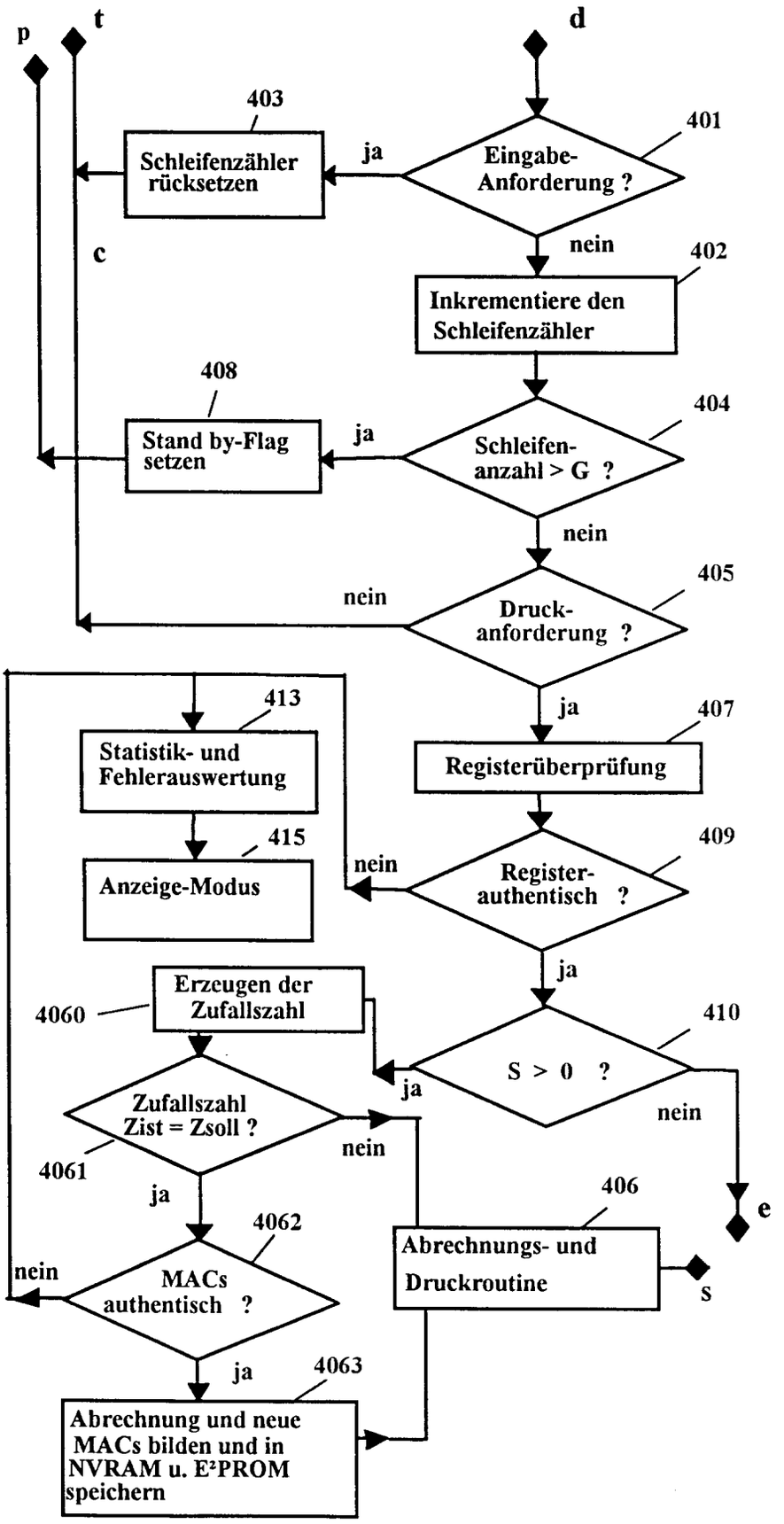
p
t
d
403
Schleifenzähler rücksetzen
ja
401
Eingabe-Anforderung ?
nein
c
402
Inkrementiere den Schleifenzähler
408
Stand by-Flag setzen
ja
404
Schleifen-anzahl > G ?
nein
nein
405
Druck-anforderung ?
ja
413
Statistik- und Fehlerauswertung
407
Registerüberprüfung
415
Anzeige-Modus
nein
409
Register-authentisch ?
ja
4060
Erzeugen der Zufallszahl
410
S > 0 ?
ja
nein
Zufallszahl Zist = Zsoll ?
nein
4061
ja
406
4062
Abrechnungs- und Druckroutine
e
s
nein
MACs authentisch ?
ja
4063
Abrechnung und neue MACs bilden und in NVRAM u. E²PROM speichern

Fig. 5

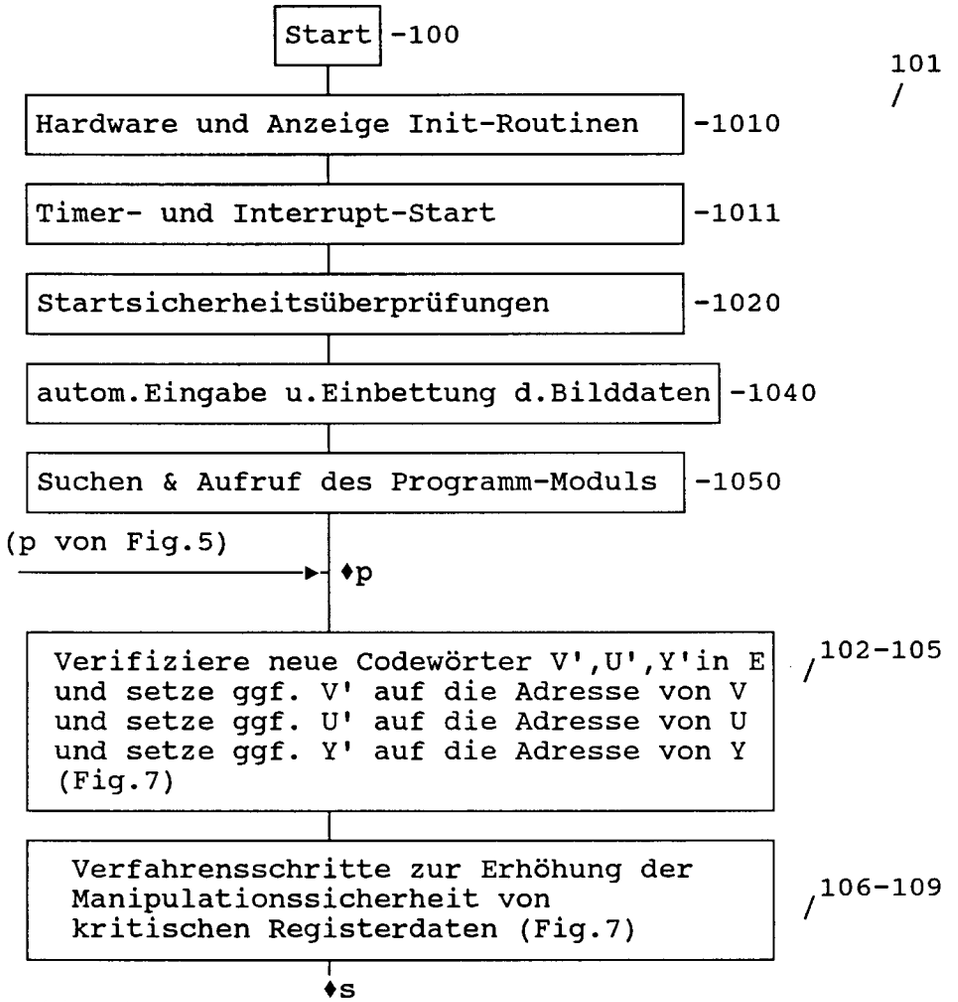
Start
-100
101
Hardware und Anzeige Init-Routinen
-1010
Timer- und Interrupt-Start
-1011
Startsicherheitsüberprüfungen
-1020
autom.Eingabe u.Einbettung d.Bilddaten
-1040
Suchen & Aufruf des Programm-Moduls
-1050
(p von Fig.5)
♦p
Verifiziere neue Codewörter V',U',Y'in E
und setze ggf. V' auf die Adresse von V
und setze ggf. U' auf die Adresse von U
und setze ggf. Y' auf die Adresse von Y
(Fig.7)
102-105
Verfahrensschritte zur Erhöhung der
Manipulationssicherheit von
kritischen Registerdaten (Fig.7)
106-109
♦s

Fig. 4

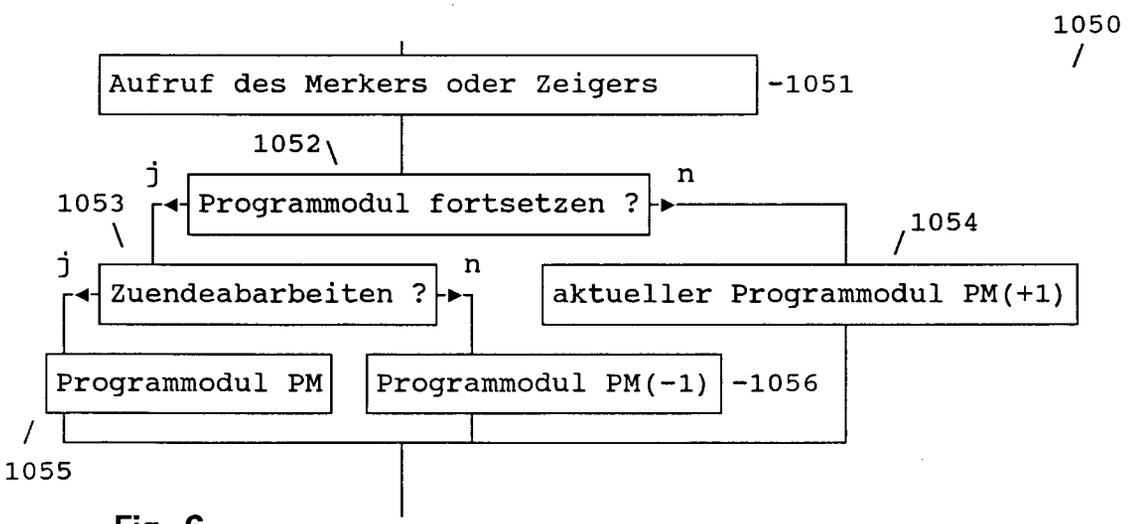
1050
Aufruf des Merkers oder Zeigers
-1051
1052
j
n
1053
Programmodul fortsetzen ?
1054
j
n
Zuendeabarbeiten ?
aktueller Programmodul PM(+1)
Programmodul PM
Programmodul PM(-1)
-1056
1055

Fig. 6

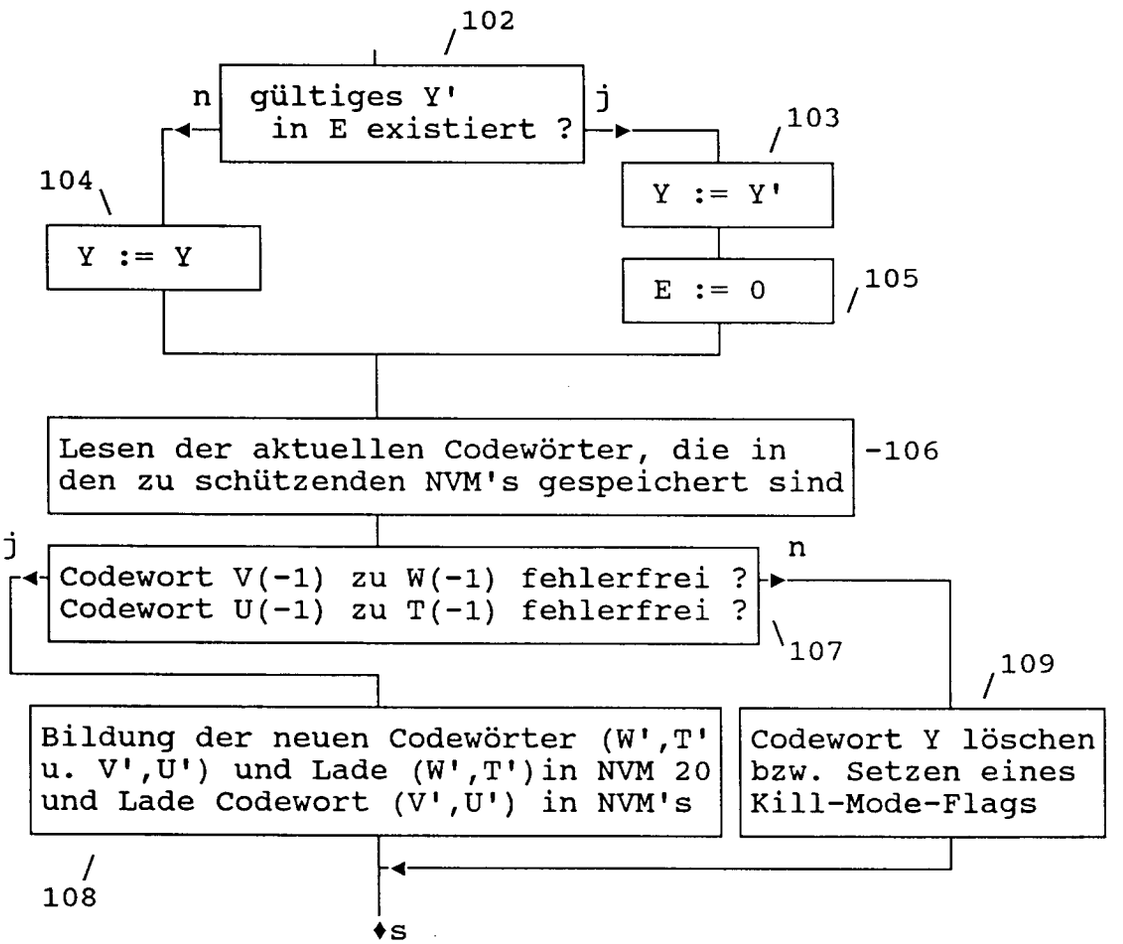
102
gültiges Y'
in E existiert ?
n
j
103
Y := Y'
104
Y := Y
E := 0
105
Lesen der aktuellen Codewörter, die in den zu schützenden NVM's gespeichert sind
-106
j
Codewort V(-1) zu W(-1) fehlerfrei ?
Codewort U(-1) zu T(-1) fehlerfrei ?
n
107
109
Bildung der neuen Codewörter (W',T' u. V',U') und Lade (W',T')in NVM 20 und Lade Codewort (V',U') in NVM's
Codewort Y löschen bzw. Setzen eines Kill-Mode-Flags
108
s

Fig. 7

Fig. 8a

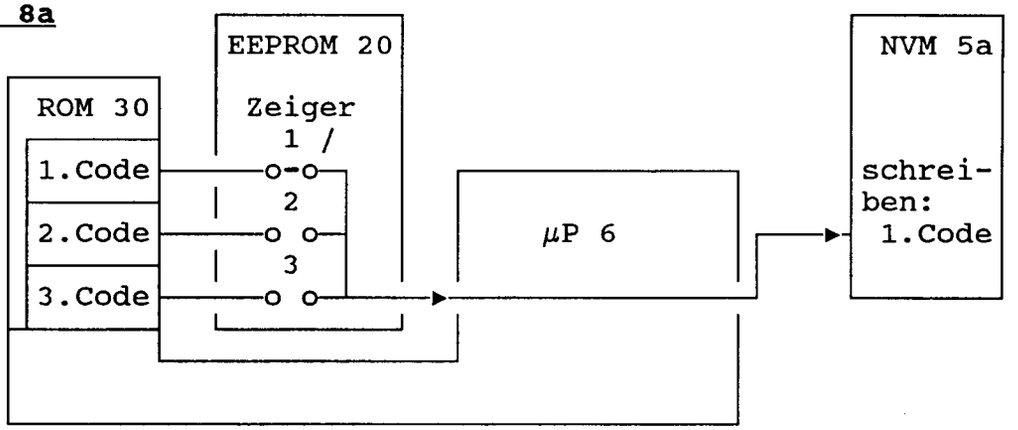

Fig. 8b

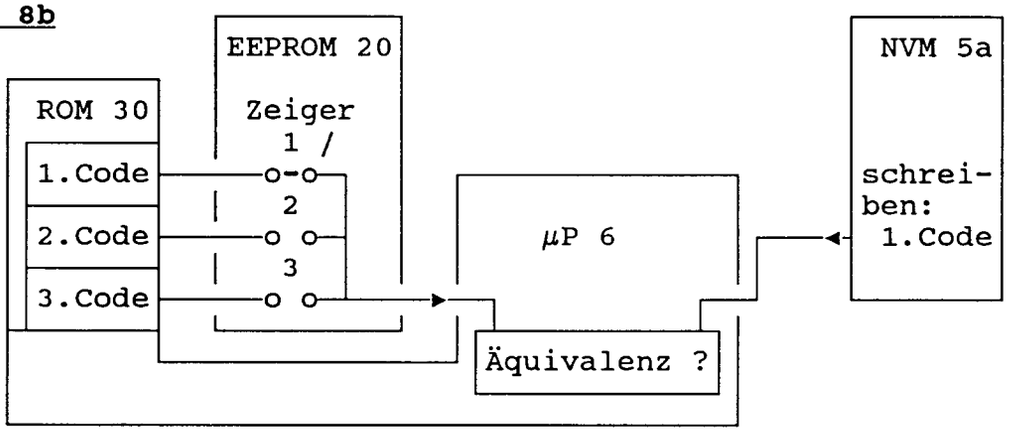

Fig. 8c