(19) Deutsches Patent- und Markenamt

(10) **DE 10 2005 063 473 B4** 2016.05.19

(12) **Patentschrift**

(21) Aktenzeichen: **10 2005 063 473.7**
(22) Anmeldetag: **16.11.2005**
(43) Offenlegungstag: **01.06.2006**
(45) Veröffentlichungstag der Patenterteilung: **19.05.2016**

(51) Int Cl.: ***H04L 9/32*** (2006.01)
H02J 7/00 (2006.01)
G09F 3/00 (2006.01)

Innerhalb von neun Monaten nach Veröffentlichung der Patenterteilung kann nach § 59 Patentgesetz gegen das Patent Einspruch erhoben werden. Der Einspruch ist schriftlich zu erklären und zu begründen. Innerhalb der Einspruchsfrist ist eine Einspruchsgebühr in Höhe von 200 Euro zu entrichten (§ 6 Patentkostengesetz in Verbindung mit der Anlage zu § 2 Abs. 1 Patentkostengesetz).

(30) Unionspriorität:

2004-342945	**26.11.2004**	**JP**
2004-342946	**26.11.2004**	**JP**
2005-263010	**09.09.2005**	**JP**

(62) Teilung aus:
10 2005 054 646.3

(73) Patentinhaber:
Sony Corporation, Tokio/Tokyo, JP

(74) Vertreter:
Mitscherlich, Patent- und Rechtsanwälte PartmbB, 80331 München, DE

(72) Erfinder:
Sasaki, Dai, Tokyo, JP; Moriai, Shiho, Tokyo, JP

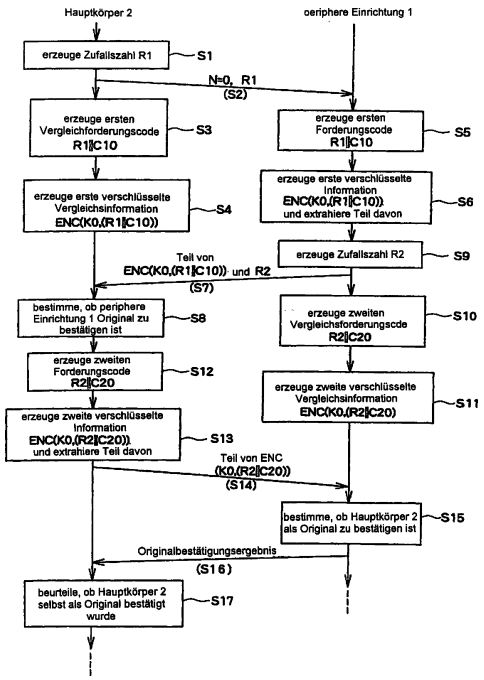
(56) Ermittelter Stand der Technik:

US	**6 795 913**	**B1**
EP	**0 984 542**	**A2**
JP	**H11- 163 853**	**A**

JP 2000-5 17 487-T2

(54) Bezeichnung: **Batterie und Originalbestätigungs-Anfrageeinrichtung**

(57) Hauptanspruch: Originalbestätigungssystem zum Originalbestätigen einer Batterie als periphere Einrichtung (1) durch einen Hauptkörper (2),
wobei die Batterie einen Steuerabschnitt (11) und der Hauptkörper (2) einen Steuerabschnitt (21) zur Durchführung einer Originalbestätigungsverarbeitung der Batterie aufweisen,
wobei der Steuerabschnitt (21) Mittel zur Prüfung aufweist, ob eine durchgeführte Originalbestätigungsverarbeitung der Batterie erfolgreich war oder nicht,
wobei der Hauptkörper (2) ferner einen Spannungssteuerabschnitt (27) aufweist,
wobei der Steuerabschnitt (21) Mittel zur Prüfung aufweist, ob der Spannungssteuerabschnitt (27) mit Spannung von einer externen Spannungsquelle beliefert wird oder nicht,
wobei der Steuerabschnitt (21) Mittel zum Setzen eines Wiederholungsintervalls für eine Durchführung der Originalbestätigungsverarbeitung der Batterie aufweist,
wobei der Steuerabschnitt (21), für den Fall dass der Spannungssteuerungsabschnitt (27) nicht mit Spannung von einer externen Spannungsquelle beliefert wird, das Wiederholungsintervall auf einen ersten Intervallwert setzt,
wobei der Steuerabschnitt (21) für den Fall dass der Spannungssteuerungsabschnitt (27) mit Spannung von einer externen Spannungsquelle versorgt wird, das Wiederholungsintervall auf einen zweiten Intervallwert setzt.



Beschreibung

[0001] Die Prioritätsanmeldungen mit den Nummern JP 2004-34 29 45, JP 2004-34 29 46 und JP 2005-26 30 10, auf denen diese Patentanmeldung basiert, werden hier durch Bezugnahme eingeführt.

[0002] Die vorliegende Erfindung bezieht sich auf eine Batterie als Gegenstand der Originalbestätigung und auf eine Originalanfrageeinrichtung, welche mit der Batterie verbunden ist und eine Batterie-Originalanfrage ausgibt.

[0003] In den vergangenen Jahren haben verschiedene elektronische Verbrauchergeräte einschließlich Heimspielmaschinen sich bezüglich der Funktionalität und der Arten vergrößert, deren Funktionen durch Verbinden von peripheren Einrichtungen mit dem Gerätehauptkörper erweitert werden können. Bei derartigen Geräten kann, um eine Schwierigkeit zu vermeiden, als Ergebnis, dass ein Benutzer versehentlich ein Produkt einer anderen Firma mit dem Gerätehauptkörper verbindet, ein Fall auftreten, dass gewünscht wird, zu beurteilen, ob eine periphere Einrichtung ein Original ist.

[0004] Ein Verfahren für diesen Zweck ist es, den Hauptgerätekörper und die periphere Einrichtung einer Originalbestätigungsverarbeitung zu unterwerfen, welche allgemein bei Computersystemen verwendet wird, um zu prüfen, ob eine periphere Einrichtung ein Original ist. Beispielsweise ist ein allgemeines Beispiel einer Abfrageantwort-Originalbestätigung in der JP-A 11-16 38 53 offenbart.

[0005] In den vergangenen Jahren sind übrigens sogar für Batterien Hersteller, welche Nachahmungsprodukte bereitstellen, erschienen, die in zunehmendem Maße Probleme verursachen, beispielsweise instabile Spannungsversorgung wegen der Unterschiede der elektrischen Kenndaten. Daher ist es sogar für Batterien nun im steigenden Maße notwendig, Originalbestätigungsverarbeitung durchzuführen, um zu prüfen, ob ein Produkt ein Original ist. Aus diesem Grund kann ein Batterie-Originalbestätigungsverfahren, welches in der JP-T-2000-517 487 offenbart ist (das Symbol ”JP-T”, wie es hier verwendet wird, bedeutet eine veröffentliche japanische Übersetzung einer PCT-Patentanmeldung), verwendet werden.

[0006] Im Gegensatz zu Informationsvorrichtungen können Geräten, welche Zuhause verwendet werden, beispielsweise elektronische Verbrauchergeräte, den Nachteil haben, eine große Menge von elektrischem Rauschen während des Betriebs zu erzeugen. Ein Weg, diesem entgegen zu wirken, besteht darin, die Originalbestätigungsverarbeitung wiederholt durchzuführen, um die Verlässlichkeit der Originalbestätigung zu steigern.

[0007] Wenn jedoch die Originalbestätigungsverarbeitung wiederholt durchgeführt wird, wird die Datenmenge, welche zwischen einer peripheren Einrichtung und dem Hauptkörper ausgetauscht wird, groß und die Kommunikationsbelastung steigt entsprechend an. Bei elektronischen Verbrauchergeräten und dgl. hat die Verarbeitung, welche sich auf die Funktionen des Geräts selbst bezieht, Priorität. Daher ist es nicht wünschenswert, die Kommunikationsbelastung zu erhöhen, welche zwischen dem Hauptkörper und einem peripheren Gerät durchgeführt wird und die sich nicht auf Funktionen des Geräts selbst bezieht.

[0008] Bei dem obigen herkömmlichen Originalbestätigungsverfahren wird der Ladestatus der Batterie nicht berücksichtigt.

[0009] Die EP 09 84 542 A2 offenbart ein Originalbestätigungssystem, bei dem eine Batterie und eine Originalbestätigungs-Anfrageeinrichtung zum Originalbestätigen der Batterie jeweils eine Berechnung mit einer gespeicherten Formel und der Zufallszahl ausführen und bei dem die Ergebnisse der Berechnungen in der Originalbestätigungs-Anfrageeinrichtung für eine Authentifizierung verglichen werden.

[0010] Ein Mobilfunkgerät mit einem Datenspeicher und einer Einrichtung zur Prüfung der Speicherintegrität nach einem erkannten kurzzeitigen Ausfall der Stromversorgung des Datenspeichers ist in der US 6 795 913 B1 beschrieben.

[0011] Es ist Aufgabe der vorliegenden Erfindung, ein Originalbestätigungssystem, ein Hauptkörper zum Originalbestätigen einer Batterie als periphere Einrichtung und ein Verfahren zum Originalbestätigen einer Batterie bereitzustellen, die eine verlässliche Originalbestätigung mit einer geringen Belastung der Originalbestätigungs-Anfrageeinrichtung erlauben.

[0012] Diese Aufgabe wird gemäß den Merkmalen der unabhängigen Patentansprüche gelöst. Weiterbildungen der Erfindung ergeben sich aus den abhängigen Ansprüchen.

Kurzbeschreibung der Zeichnungen

[0013] Fig. 1 ist ein Blockdiagramm, welches eine Übersicht über den Aufbau einer peripheren Einrichtung **1** zeigt;

[0014] Fig. 2 ist ein Blockdiagramm, welches eine Übersicht über den Aufbau eines Hauptkörpers **2** zeigt;

[0015] Fig. 3 ist ein Blockdiagramm, welches das Aufbaubeispiel eines Spannungssteuerabschnitts des Hauptkörpers **2** zeigt;

[0016] **Fig.** 4 ist ein Funktionsblockdiagramm eines Beispiels der peripheren Einrichtung **1**;

[0017] **Fig.** 5 ist ein Funktionsblockdiagramm eines Beispiels des Hauptkörpers **2**;

[0018] **Fig.** 6 ist ein Flussdiagramm, welches einen Kommunikationsfluss zwischen der peripheren Einrichtung **1** und dem Hauptkörper **2** zeigt; und

[0019] **Fig.** 7 ist ein Flussdiagramm, welches ein Verfahrensbeispiel zeigt, welches durch den Hauptkörper **2** ausgeführt wird. Beschreibung der bevorzugten Ausführungsform.

[0020] Eine Ausführungsform der vorliegenden Erfindung wird anschließend mit Hilfe der beiliegenden Zeichnungen beschrieben. Eine Batterie nach der Ausführungsform ist als eine periphere Einrichtung **1** realisiert. Wie in **Fig.** 1 gezeigt ist, besitzt die periphere Einrichtung **1** einen Steuerabschnitt **11**, einen Speicherabschnitt **12**, einen Kommunikationsabschnitt **13** und einen Funktionsabschnitt **14** und ist mit einem Hauptkörper **2** verbunden.

[0021] Der Steuerabschnitt **11** ist eine CPU oder dgl. und arbeitet gemäß Programmen, welche im Speicherabschnitt **12** gespeichert sind. Der Steuerabschnitt **11** führt eine Verarbeitung durch, um die Funktionen der peripheren Einrichtung **1** zu realisieren. Für eine Manipulationseinrichtung, beispielsweise einer Steuerung als periphere Einrichtung **1**, führt der Steuerabschnitt **11** eine Verarbeitung zum Übertragen von Information in Bezug auf eine Instruktionsmanipulation eines Benutzers zum Hauptkörper **2** durch. Für eine Speichereinrichtung, beispielsweise eine Speicherkarte als periphere Einrichtung **1**, führt der Steuerabschnitt **11** eine Verarbeitung zum Halten der Information, welche vom Hauptkörper **2** empfangen wird, und Verarbeiten zum Liefern der Information, die darin gehalten wird, zum Hauptkörper **2** als Antwort auf eine Anfrage vom Hauptkörper **2** durch. Obwohl in dieser Ausführungsform die Einrichtung, deren Original zu bestätigen ist, die Spannungsversorgung (d. h. die Batterie) ist, kann die periphere Einrichtung **1** als Einrichtung, deren Original zu bestätigen ist, irgendeine von anderen verschiedenen Einrichtungen sein, die eine Kommunikationseinrichtung aufweisen, eine Abbildeinrichtung, beispielsweise eine Kamera, und eine Toneinrichtung, beispielsweise einen Lautsprecher.

[0022] Um eine Originalbestätigungsfunktion zu realisieren, führt der Steuerabschnitt **11** außerdem eine Verarbeitung zum Empfangen erster code-bezogener Information durch, das Erlangen eines ersten Abfragecodes auf der Basis der empfangenen ersten code-bezogenen Information und das Erzeugen erster verschlüsselter Information durch Verschlüsseln des ersten Abfragecodes durch. Die Verarbeitung zum Realisieren der Originalbestätigungsfunktion der Steuerung **11** wird später ausführlich beschrieben.

[0023] Der Speicherabschnitt **12** weist ein Speicherelement auf, beispielsweise einen Flash-ROM und einen RAM, und speichert Programme, die durch den Steuerabschnitt **11** abzulaufen sind. Der Speicherabschnitt **12** arbeitet außerdem als Arbeitsspeicher zum Speichern verschiedener Daten, die während der Verarbeitung des Steuerabschnitts **11** notwendig sind.

[0024] Der Kommunikationsabschnitt **13** ist beispielsweise ein serieller Kommunikationsport, und er ist mit dem Hauptkörper **2** verbunden. Der Kommunikationsabschnitt **13** ist überträgt Information zum Hauptkörper **2** gemäß einer Instruktion, welche vom Steuerabschnitt **11** zugeführt wird. Außerdem gibt der Kommunikationsabschnitt **13** Information, welche vom Hauptkörper **2** empfangen wird, an den Steuerabschnitt **11** aus.

[0025] Der Funktionsabschnitt **14** liefert die Funktionen der peripheren Einrichtung **1**. Da bei dieser Ausführungsform die periphere Einrichtung die Batterie ist, umfasst der Funktionsabschnitt **14** eine Sekundärbatterie zum Liefern elektrischer Spannung.

[0026] Wie in **Fig.** 2 gezeigt ist, umfasst der Hauptkörper **2**, der beispielsweise eine Heimspielmaschine ist, einen Steuerabschnitt **21**, beispielsweise eine CPU, einen Speicherabschnitt **22**, einen Manipulationsabschnitt **23**, einen Anzeigesteuerabschnitt **24**, einen Kommunikationsabschnitt **25**, ein optisches Plattenlaufwerk **26** und einen Spannungssteuerabschnitt **27**.

[0027] Der Steuerabschnitt **21** arbeitet gemäß Programmen, welche im Speicherabschnitt **22** gespeichert sind. Beispielsweise führt der Steuerabschnitt **21** Verarbeitung, welche sich auf ein Spiel bezieht, durch. Bei dieser Ausführungsform filtert der Steuerabschnitt **21** außerdem Operationen einer Originalanfrageeinrichtung durch. Die ausführliche Verarbeitung, welche durch das Merkmal der Originalanfrageeinrichtung des Steuerabschnitts **21** durchgeführt wird, wird später beschrieben.

[0028] Der Speicherabschnitt **22**, der beispielsweise einen RAM aufweist, hält Spielprogramme, welche durch das optische Plattenlaufwerk **26** gelesen werden. Der Speicherabschnitt **22** umfasst außerdem ein nichtflüchtiges Speicherelement, wo Programme für die Originalanfrageeinrichtung gespeichert sind. Der Speicherabschnitt **22** arbeitet außerdem als Arbeitsspeicher für den Steuerabschnitt **21**.

[0029] Die Manipulationsabschnitt **23**, der eine Spielsteuerung ist, gibt den Inhalt einer Instruktions-

manipulation eines Spielers an den Steuerabschnitt **21** aus. Der Anzeigesteuerabschnitt **24**, der eine Grafikschaltung ist, zeigt ein Spielbild auf einer Anzeigeeinrichtung an, beispielsweise einem Heim-TV-Empfänger, gemäß einer Instruktion, die vom Steuerabschnitt **21** zugeführt wird. Der Kommunikationsabschnitt **25**, der beispielsweise ein serieller Kommunikationsport ist, ist mit dem Kommunikationsabschnitt **13** der peripheren Einrichtung **1** verbunden und tauscht Information mit dieser aus. Bei dieser Ausführungsform überträgt der Kommunikationsabschnitt **25** Information zur peripheren Einrichtung **1** gemäß einer Instruktion, welche von dem Steuerabschnitt **21** zugeführt wird, und gibt Information, welche von der peripheren Einrichtung **1** empfangen wird, an den Steuerabschnitt **21** aus.

[0030] Das optische Plattenlaufwerk **26**, welches beispielsweise ein DVD-ROM Laufwerk oder ein Blu-Ray-Disc-Laufwerk ist, liest Information, beispielsweise Programme von einem Aufzeichnungsträger, beispielsweise einer DVD, einer Blu-Ray-Disc oder dgl. und gibt diese an den Steuerabschnitt **21** aus.

[0031] Wie in **Fig.** 3 gezeigt ist, weist der Spannungssteuerabschnitt **27**, der mit der Batterie als periphere Einrichtung **1** verbunden ist, eine Spannungssteuerschaltung **31**, eine Ladeschaltung **32** und eine Spannungsversorgungsschaltung **33** auf. Die Spannungssteuerschaltung **31** steuert die Zufuhr von Spannung von der Batterie oder der Spannungsversorgungsschaltung **33** zu den individuellen Abschnitten, beispielsweise zum Steuerabschnitt **21**. Wenn beispielsweise ein Spieler die Spannung einschaltet, beginnt die Spannungssteuerschaltung **31**, Spannung zu den individuellen Abschnitten zu liefern. Wenn ein Spieler die Spannung abschaltet oder eine Instruktion, um die Spannung auszuschalten (Spannungsausschalteinstruktion), vom Steuerabschnitt **21** kommt, stoppt die Spannungssteuerschaltung **31** die Zufuhr von Spannung zu den individuellen Abschnitten.

[0032] Die Ladeschaltung **32** lädt die Batterie, wenn die Batterie mit dieser in einem Zustand verbunden ist, dass diese mit Spannung von der Spannungsversorgungsschaltung **33** beliefert wird. Die Spannungsversorgungsschaltung **33** ist beispielsweise ein Regler und ist mit einer externen Spannungsquelle verbunden (beispielsweise mit einer Wandsteckdose). Die Spannungsversorgungsschaltung **33** wird mit einer DC-Spannungsversorgungsspannung beliefert, welche auf der Basis der Spannung von der externen Spannungsquelle erzeugt wird, und gibt diese an die Spannungssteuerschaltung **31** und die Ladeschaltung **32** aus. Die Spannungsversorgungsschaltung **33** entspricht einem ”Spannungsempfangsabschnitt” der Erfindung.

[0033] Der Spannungssteuerabschnitt **27** beliefert die individuellen Abschnitte mit Spannung, welche von der Batterie geliefert wird, wenn die Batterie damit verbunden ist, in einem Zustand, dass die Spannungsversorgungsschaltung **33** nicht mit Spannung von einer externen Spannungsquelle beliefert wird. Wenn die Spannungsversorgungsschaltung **33** mit Spannung von einer externen Spannungsquelle beliefert wird, beliefert der Spannungssteuerabschnitt **27** die individuellen Abschnitte mit Spannung, welche von der externen Spannungsquelle geliefert wird. Weiter lädt der Spannungssteuerabschnitt **27** die Batterie, wenn die Batterie damit verbunden ist, in einem Zustand, dass die Spannungsversorgungsschaltung **33** mit Spannung von einer externen Spannungsquelle beliefert wird.

[0034] Es wird mm die Verarbeitung zum Realisieren der Originalbestätigungsfunktion beschrieben, welche durch den Steuerabschnitt **11** der peripheren Einrichtung **1** durchgeführt wird. Bei dieser Ausführungsform sind mehrere Verschlüsselungsschlüsselkandidaten k0, k1, ... vorher im Speicherabschnitt **12** der peripheren Einrichtung **1** gespeichert.

[0035] Funktionsmäßig ausgedrückt umfasst, wie in **Fig.** 4 gezeigt ist, der Steuerabschnitt **11** einen Originalanfrage-Verarbeitungsabschnitt **41** und einen Hauptkörper-Originalbestätigungsabschnitt **42**.

[0036] Der Originalanfrage-Verarbeitungsabschnitt **41** empfängt vom Hauptkörper **2** (Originalanfrageeinrichtung) über die Kommunikationsabschnitt **13** eine erste code-bezogene Information, von der ein erster Abfragecode zu erzeugen ist. Weiter empfängt der Originalanfrage-Verarbeitungsabschnitt **41** vom Hauptkörper **2** Verschlüsselungsschlüssel-Identifikationsinformation, welche zur Identifizierung eines Verschlüsselungsschlüssels zu verwenden ist, und liest vom Speicherabschnitt **12** einen Verschlüsselungsschlüssel kN, der durch die Verschlüsselungsschlüssel-Identifikationsinformation identifiziert wird (beispielsweise eine Schlüsselnummer N).

[0037] Es sei hier angenommen, dass die erste code-bezogene Information Teil eines ersten Abfragecodes ist. Wenn beispielsweise ein erster Abfragecode mit 128 Bits verwendet wird, sendet der Hauptkörper **2**, als erste code-bezogene Information, eine Information von 64 Bits, die der ersten Hälfte (oberen Hälfte) der Information von 128 Bits entspricht. Der Originalanfrage-Verarbeitungsabschnitt **41** erzeugt einen ersten Abfragecode auf der Basis der ersten code-bezogenen Information und erwirbt diese.

[0038] Bei dieser Ausführungsform sind mehrere erste Konstanten C10, C11 ... im Speicherabschnitt vorher gespeichert. Ein erster Abfragecode wird durch Lesen – vom Speicherabschnitt **12** – einer ers-

ten Konstanten C1N entsprechend einer Schlüsselnummer N erzeugt, welche als Verschlüsselungsschlüssel-Identifikationsinformation empfangen wird, und durch Platzieren der ersten gelesenen Konstante C1N nach der ersten empfangenen code-bezogenen Information. Wie oben beschrieben besteht die erste code-bezogene Information aus 64 Bits für den ersten Abfragecode aus 128 Bits, wobei jede der ersten Konstanten C10, C11, ... eine Konstante aus 64 Bits ist. Die erste Konstante ist "gemeinsamer Teil Information" der Erfindung.

[0039] Der Originalanfrage-Verarbeitungsabschnitt **41** erzeugt erste verschlüsselte Information durch Verschlüsseln des ersten Abfragecodes, der unter Verwendung des Verschlüsselungsschlüssels kN erzeugt wurde, der vom Speicherabschnitt **12** gelesen wurde.

[0040] Außerdem extrahiert der Originalanfrage-Verarbeitungsabschnitt **41** als erste verschlüsselungs-bezogene Information einen vorher festgelegten Teil (beispielsweise zweite Hälfte (untere Hälfte)) der ersten verschlüsselten Information und überträgt die extrahierte erste verschlüsselungs-bezogene Information zum Hauptkörper **2**. Wenn beispielsweise der erste Abfragecode aus 128 Bits besteht und der Algorithmus der obigen Verschlüsselung aus einem Codierverfahren besteht, welches die Codelänge der Verschlüsselungsobjektsinformation nicht ändert, hat die erste Verschlüsselungsinformation ebenfalls 128 Bits. Der Originalanfrage-Verarbeitungsabschnitt **41** überträgt den vorher festgelegten Teil (beispielsweise zweite Hälfte von 64 Bits) der ersten verschlüsselten Information aus 128 Bits zum Hauptkörper **2**.

[0041] Um den Hauptkörper **2** (Originalanfrageeinrichtung) zu bestätigen, erzeugt der Hauptkörper-Originalbestätigungsabschnitt **42** eine zweite code-bezogene Information, welche sich auf einen zweiten Vergleichsabfragecode bezieht (zweiter Abfragecode zum Vergleich), um für die Bestätigung des Hauptkörpers **2** verwendet zu werden. Beispielsweise erzeugt der Hauptkörper-Originalbestätigungsabschnitt **42** einen numerischen Wert, der eine vorgeschriebene Anzahl von Bits hat, durch eine Zufallszahlroutine und überträgt die erzeugte Zufallszahl als zweite code-bezogene Information über den Kommunikationsabschnitt **13** zum Hauptkörper **2**.

[0042] Der Hauptkörper-Originalbestätigungsabschnitt **42** erzeugt außerdem einen zweiten Vergleichsabfragecode auf der Basis der erzeugten zweiten code-bezogenen Information. Bei dieser Ausführungsform sind mehrere zweite Konstanten C20, C21, ... vorher im Speicherabschnitt **12** gespeichert. Eine zweite Konstante C2N entsprechend der Schlüsselnummer N, welche vorher als Verschlüsselungsschlüssel-Identifikationsinformation empfangen wurde, wird vom Speicherabschnitt **12** gelesen. Ein zweiter Vergleichsabfragecode wird durch Platzieren der zweiten Konstanten C2N nach der erzeugten zweiten code-bezogenen Information erzeugt. Die Datenmenge von Kommunikationen (Übertragung und Empfang) des zweiten Abfragecodes kann beispielsweise durch – wie oben beschrieben – zufallsmäßiges Bestimmen eines Teils des zweiten Abfragecodes und durch Ausbilden des verbleibenden Teils zu einer Konstanten reduziert werden.

[0043] Der Hauptkörper-Originalbestätigungsabschnitt **42** erzeugt zweite Verschlüsselungsvergleichsinformation durch Verschlüsseln des zweiten Vergleichsabfragecodes, der im Speicherabschnitt **12** gespeichert ist, unter Verwendung des Verschlüsselungsschlüssels kN, der unter Verwendung der Verschlüsselungsschlüssel-Identifikationsinformation identifiziert wird, welche beim Durchführen der Originalfunktionsverarbeitung empfangen wurde.

[0044] Weiter vergleicht der Hauptkörper-Originalbestätigungsabschnitt **42** einen vorher festgelegten Teil der zweiten Verschlüsselungsvergleichsinformation mit einem Teil der Information, welche durch Verschlüsseln des zweiten Abfragecodes im Hauptkörper **2** erlangt wird. Wenn die zweite Hälfte von 64 Bits als der vorherbestimmte Teil wie im oben beschriebenen Beispiel extrahiert wird, extrahiert der Hauptkörper-Originalbestätigungsabschnitt **42** die zweite Hälfte von 64 Bits von der zweiten Verschlüsselungsvergleichsinformation und vergleicht die extrahierte Information aus 64 Bits mit der zweiten verschlüsselungs-bezogenen Information (64 Bits), welche vom Hauptkörper **2** empfangen wird.

[0045] Wenn diese miteinander übereinstimmen, beurteilt der Hauptkörper-Originalbestätigungsabschnitt **42** (d. h., die periphere Einrichtung **1**), dass der Hauptkörper **2** ein Original ist und teilt das Beurteilungsergebnis dem Hauptkörper **2** mit. Wenn der Hauptkörper-Originalbestätigungsabschnitt **42** beurteilt, dass der vorher festgelegte Teil der zweiten Verschlüsselungsvergleichinformation nicht mit der zweiten verschlüsselungs-bezogenen Information, welche vom Hauptkörper **2** empfangen wird, übereinstimmt, d. h., dass der Hauptkörper **2** kein Original ist, teilt der Hauptkörper-Originalbestätigungsabschnitt **42** das Beuteilungsergebnis dem Hauptkörper **2** mit.

[0046] Anschließend wird die Arbeitsweise des Steuerabschnitts **21** des Hauptkörpers **2**, der als Originalanfrageeinrichtung arbeitet, beschrieben. Ein Verschlüsselungsschlüssel kN wird vorher im Speicherabschnitt **22** des Hauptkörpers **2** gespeichert. Der Verschlüsselungsschlüssel kN ist der gleiche wie die mehreren Verschlüsselungsschlüssel, welche in dem Speicherabschnitt **12** der peripheren Einrichtung **1** als die Einrichtung, deren Original zu prüfen

ist, gespeichert sind. Außerdem ist die Verschlüsselungsschlüssel-Identifikationsinformation (beispielsweise die Schlüsselnummer N), welche die Information ist, den Verschlüsselungsschlüssel in der peripheren Einrichtung **1** zu identifizieren, vorher im Speicherabschnitt **22** gespeichert.

[0047] Der Steuerabschnitt **21** des Hauptkörpers **2** realisiert Funktionen, die in **Fig.** 5 gezeigt sind. Funktionell ausgedruckt, wie in **Fig.** 5 gezeigt ist, weist der Steuerabschnitt **21** einen peripheren Einrichtungsoriginal-Bestätigungsabschnitt **45** und einen Originalanfrage-Verarbeitungsabschnitt **46** auf.

[0048] Der periphere Einrichtungsoriginal-Bestätigungsabschnitt **45** erzeugt erste code-bezogene Information, von welcher ein erster Vergleichsabfragecode zu erzeugen ist. Beispielsweise erzeugt der periphere Einrichtungsoriginal-Bestätigungsabschnitt **45** eine Zufallszahl durch eine Zufallszahlroutine und überträgt die erzeugte Zufallszahl als erste code-bezogene Information über den Kommunikationsabschnitt **25** zur peripheren Einrichtung **1**. Der periphere Einrichtungsoriginal-Bestätigungsabschnitt **45** überträgt außerdem die Verschlüsselungsschlüssel-Identifikationsinformation (beispielsweise die Schlüsselnummer N), die zum Identifizieren des Verschlüsselungsschlüssels kN zu verwenden ist.

[0049] Der periphere Einrichtungsoriginal-Bestätigungsabschnitt **45** erzeugt außerdem einen ersten Vergleichsabfragecode auf der Basis der ersten erzeugten code-bezogenen Information. Bei dieser Ausführungsform wird eine erste Konstante C11, welche in der peripheren Einrichtung **1** zu verwenden ist, vorher im Speicherabschnitt **22** gespeichert. Da in diesem Beispiel die erste Konstante C1N, welche unter Verwendung der Verschlüsselungsschlüssel-Identifikation identifiziert wird (Schlüsselnummer N), in der peripheren Einrichtung **1** verwendet wird, wird die erste Konstante C1N im Speicherabschnitt **22** gespeichert.

[0050] Der periphere Einrichtungsoriginal-Bestätigungsabschnitt **45** erzeugt einen ersten Vergleichsabfragecode durch Platzieren der ersten Konstante C1N, welche im Speicherabschnitt **22** gespeichert ist, nach der erzeugten code-bezogenen Information. Die Datenmenge von Kommunikationen (Übertragung und Empfang) eines Abfragecodes kann wie oben beschrieben durch zufallsmäßiges Bestimmen des Teils des Abfragecodes und durch Ausbilden des verbleibenden Teils zu einer Konstante reduziert werden.

[0051] Der periphere Einrichtungsoriginal-Bestätigungsabschnitt **45** erzeugt erste Verschlüsselungsvergleichsinformation, indem der erzeugte erste Vergleichssabfragecode durch den Verschlüsselungsschlüssel kN, der im Speicherabschnitt **22** gespeichert ist, erzeugt wird.

[0052] Außerdem empfängt der periphere Einrichtungsoriginal-Bestätigungsabschnitt **45** von der peripheren Einrichtung **1** als erste verschlüsselungsbezogene Information einen Teil eines Verschlüsselungsergebnisses des ersten Abfragecodes, was in der peripheren Einrichtung **1** ausgeführt wird, unter Verwendung des Verschlüsselungsschlüssels kN. Außerdem vergleicht der periphere Einrichtungsoriginal-Bestätigungsabschnitt **45** einen vorher festgelegten Teil der ersten Verschlüsselungsvergleichsinformation mit der ersten verschlüsselungsbezogenen Information, welche von der peripheren Einrichtung **1** empfangen wird. Wenn die zweite Hälfte von 64 Bits als der vorher festgelegte Teil wie im oben beschriebenen Beispiel extrahiert wird, extrahiert der periphere Einrichtungsoriginal-Bestätigungsabschnitt **45** die zweite Hälfte von 64 Bits von der ersten Verschlüsselungsvergleichsinformation und vergleicht die extrahierte Information aus 64 Bits mit der ersten verschlüsselungs-bezogenen Information (64 Bits), welche von der peripheren Einrichtung **1** empfangen wird.

[0053] Wenn sie miteinander übereinstimmen, beurteilt der periphere Einrichtungsoriginal-Bestätigungsabschnitt **45**, dass die periphere Einrichtung **1** ein Original ist.

[0054] Außerdem hält der Hauptkörper **2** vorher die zweite Konstante C2N, welche in der peripheren Einrichtung **1** verwendet wird. Der Originalanfrage-Verarbeitungsabschnitt **46** erzeugt einen zweiten Abfragecode durch Platzieren der zweiten Konstante C2N nach der zweiten code-bezogene Information, welche vom Hauptkörper-Originalbestätigungsabschnitt **42** der peripheren Einrichtung **1** empfangen wird.

[0055] Der Originalanfrage-Verarbeitungsabschnitt **46** erzeugt eine zweite verschlüsselte Information, wobei der Verschlüsselungscode kN vom Speicherabschnitt **22** gelesen wird und der erzeugte zweite Abfragecode unter Verwendung des Verschlüsselungscodes kN verschlüsselt wird. Außerdem extrahiert der Originalanfrage-Verarbeitungsabschnitt **46** als zweite verschlüsselungs-bezogene Information einen vorher festgelegten Teil (beispielsweise die zweite Hälfte) der zweiten Verschlüsselungsinformation und überträgt die zweite extrahierte verschlüsselungs-bezogene Information zur peripheren Einrichtung **1**.

[0056] Obwohl sich die obige Beschreibung auf den Fall richtet, dass sowohl die Originalbestätigungs-Verarbeitung der peripheren Einrichtung **1** als auch die Originalbestätigungs-Verarbeitung des Hauptkörpers **2** durch die periphere Einrichtung **1** durchgeführt werden, braucht lediglich die Verarbeitung, dass

der Hauptkörper **2** die periphere Einrichtung **1** als Original prüft, durchgeführt werden, wenn dies ausreichend ist. In diesem Fall sind der Hauptkörper-Originalbestätigungsabschnitt **42** der peripheren Einrichtung **1** und der Originalanfrage-Verarbeitungsabschnitt **46** des Hauptkörpers **2** nicht immer notwendig.

[0057] Ein wichtiges Merkmal dieser Ausführungsform ist, ab die Originalbestätigung erfolgreich war oder fehlgeschlagen hat, dass dies unter Verwendung von Daten berichtet wird, weiche einen vorher festgelegten Teil der zweiten Verschlüsselungsvergleichsinformation aufweisen. Bei dieser Ausführungsform wird ein Bericht mit der Wirkung, dass der Hauptkörper **2** als Original bestätigt wurde, durch eigenes Übertragen eines vorgeschriebenen Teils der zweiten Verschlüsselungsvergleichsinformation zum Hauptkörper **2** als Originalerfolgsdaten ausgeführt. Ein Bericht mit der Wirkung, dass der Hauptkörper **2** nicht als Original bestätigt wurde, wird durch Übertragen – zum Hauptkörper **2** – als Originalfehlerdaten von Daten gemacht, welche durch Negieren der individuellen Bits des vorgeschriebenen Teils der zweiten Verschlüsselungsvergleichsinformation erhalten werden. Die Negierung bedeutet einen Betrieb zum Ändern des Bits ”1” auf ”0” und des Bits ”0” auf ”1”. Ein logischer Betrieb zum Belassen jedes Datenbits so wie es ist, entspricht einer ”zweiten logischen Operation” der Erfindung, und ein logischer Betrieb zum Negieren jedes Datenbits entspricht einer ”ersten logischen Operation” der Erfindung. Entsprechend, wenn der Hauptkörper **2** berichtet, wenn die periphere Einrichtung **1** bestätigt wurde, überträgt der Hauptkörper **2** selbst ein vorgeschriebenes Teil der ersten Verschlüsselungsvergleichsinformation. Ein Bericht mit der Wirkung, dass die periphere Einrichtung nicht bestätigt wurde, wird durch Übertragen – zur peripheren Einrichtung **1** als Originalversagerdaten – von Daten durchgeführt, welche durch Negieren der individuellen Bits des vorgeschriebenen Teils der ersten Verschlüsselungsvergleichsinformation erlangt werden.

[0058] Der Hauptkörper **2** vergleicht die empfangenen Originalerfolgsdaten mit der zweiten verschlüsselungs-bezogenen Information, die vorher übertragen wurde. Wenn Übereinstimmung gefunden wird, beurteilt der Hauptkörper **2**, dass dieser beglaubigt wurde.

[0059] Die Originalerfolgsdaten und die Originalversagerdaten können eine vorher festgelegte Konstante sein, beispielsweise Daten, von denen alle Bits ”1” oder ”0” sind. Wenn jedoch beispielsweise eine Konstante für diesen Zweck verwendet wird, kann die Information für den Effekt, dass der Hauptkörper **2** beglaubigt wurde, durch Übertragen der Konstanten als Originalerfolgsdaten unter Verwendung eines illegal hergestellten MOD-Chips übertragen werden. Um diese Schwäche in der Sicherheit zu vermeiden, werden bei dieser Ausführungsform die Originalerfolgsdaten oder Originalversagerdaten unter Verwendung – anstelle einer Konstanten – eines vorher festgelegten Teils der Verschlüsselungsvergleichsinformation erzeugt, welche einen unterschiedlichen Wert annimmt, jedes Mal, wenn die Originalverarbeitung durchgeführt wird.

[0060] Bei dieser Ausführungsform werden ein erster oder zweiter Abfragecode (Codes) und eine erste und/oder zweite Verschlüsselungsinformation, die durch Verschlüsseln des ersten und/oder zweiten Abfragecodes (Codes) erlangt wird, insgesamt nicht übertragen und empfangen, und anstelle davon werden Teile von diesen übertragen und empfangen. Dies ermöglicht es, die Datenmenge zu reduzieren, welche für die Originalbestätigungsverarbeitung auszutauschen sind, um dadurch zu einer Verminderung der Kommunikationsbelastung beizutragen.

[0061] Anschließend werden die Operationen der peripheren Einrichtung **1** und des Hauptkörpers **2** als die Einrichtung, die zu bestätigen ist, bzw. die Einrichtung, welche die Originalbestätigung anfordert, mit Hilfe von **Fig.** 6 beschrieben. **Fig.** 6 ist ein Flussdiagramm, welches den Kommunikationsfluss zwischen der peripheren Einrichtung **1** und dem Hauptkörper **2** zeigt. Am Anfang werden ein Verschlüsselungsschlüssel k0, eine erste Konstante C10, und eine zweite Konstante C20, die der Verschlüsselungsschlüsselidentifikationsinformation N = 0 entsprechen, im Speicherabschnitt **22** des Hauptkörpers **2** gespeichert.

[0062] Wenn die periphere Einrichtung **1** mit dem Hauptkörper **2** verbunden ist, erzeugt der Hauptkörper **2** eine Zufallszahl R1 aus 64 Bits im Schritt S1 und überträgt die Verschlüsselungsschlüssel-Identifikationsinformation (in diesem Beispiel die Schlüsselnummer ”0”), die dazu verwendet wird, den Verschlüsselungsschlüssel k0 zu identifizieren, und eine Zufallszahl R1, die als erste code-bezogene Information dient, im Schritt S2 zur peripheren Einrichtung **1**.

[0063] Im Schritt S3 erzeugt der Hauptkörper **2** einen ersten Vergleichsabfragecode, wobei die erste Konstante C10 nach der Zufallszahl R1 platziert wird, welche die erste codebezogene Information ist, welche im Schritt S1 erzeugt wird. In der folgenden Beschreibung wird das Anordnen von zwei Abschnitten von Information benachbart zueinander durch das Symbol ”||” bezeichnet. Daher wird der erste Vergleichsabfragecode dargestellt durch ”R1||C10”.

[0064] Im Schritt S4 erzeugt der Hauptkörper erste Verschlüsselungsvergleichsinformation zum Verschlüsseln des ersten erzeugten Vergleichsabfragecodes R1||C10 unter Verwendung des Verschlüsselungsschlüssels k0. Es wird nun eine Regel festgelegt, dass Information, welche durch Verschlüsseln von Gegenstandsdaten d unter Verwendung eines

Verschlüsselungsschlüssels k erlangt werden, durch ENC (k, d) dargestellt werden sollte. Die erzeugte erste Verschlüsselungsvergleichsinformation wird durch ENC (k0, (R1||C10)) dargestellt.

[0065] Die periphere Einrichtung **1** empfängt die erste code-bezogene Information R1 und die Schlüsselnummer ”0” (Verschlüsselungsschlüssel-Identifikationsinformation) vom Hauptkörper **2** und liest einen Verschlüsselungsschlüssel k0 und eine erste Konstante C10, welche durch die Verschlüsselungsschlüssel-Identifikationsinformation ”0” identifiziert werden, vom Speicherabschnitt **12**. Im Schritt S5 erzeugt die periphere Einrichtung **1** einen ersten Abfragecode R1||C10, wobei die erste code-bezogene Information R1 und die erste Konstante C10 benachbart zueinander platziert werden.

[0066] Im Schritt S6 erzeugt die erste periphere Einrichtung **1** erste verschlüsselte Information ENC (k0, (R1||C10)) durch Verschlüsseln des ersten erzeugten Abfragecodes R1||C10 unter Verwendung des Verschlüsselungsschlüssels k4 und extrahiert einen vorgeschriebenen Teil (beispielsweise untere 64 Bits) der erzeugten ersten Verschlüsselungsinformation ENC (k0, (R1||C10)), um erste verschlüsselungs-bezogene Information zu erzeugen. Im Schritt S7 überträgt die periphere Einrichtung **1** die extrahierte erste verschlüsselungs-bezogene Information zum Hauptkörper **2**.

[0067] Der Hauptkörper **2** empfängt die erste verschlüsselungs-bezogene Information. Im Schritt S8 prüft der Hauptkörper **2**, ob der vorgeschriebene Teil (untere 64 Bits) der ersten Verschlüsselungsvergleichsinformation, welche im Schritt S4 erzeugt wurde, mit der ersten empfangenen verschlüsselungsbezogenen Information übereinstimmt und bestätigt dadurch die periphere Einrichtung **1**.

[0068] Allgemein kennt eine Partei, die beabsichtigt, eine periphere Einrichtung illegal herzustellen, nicht den Verschlüsselungsschlüssel k0 oder die erste Konstante C10, und kann daher nicht den ersten Abfragecode oder die erste Verschlüsselungsinformation erzeugen. Daher stimmen in diesem Fall allgemein im Schritt S8 der vorgeschriebene Teil (untere 64 Bits) der ersten Verschlüsselungsvergleichsinformation nicht mit der empfangenen ersten verschlüsselungs-bezogenen Information überein. Die periphere Einrichtung **1** kann somit als eine illegale Einrichtung beurteilt werden.

[0069] Die periphere Einrichtung **1** kann im Schritt S9 eine zweite code-bezogene Information erzeugen, die sich auf einen Abfragecode (zweiter Abfragecode) bezieht, der zur Originalbestätigung des Hauptkörpers **2** zu verwenden ist. Bei dieser Ausführungsform erzeugt die periphere Einrichtung **1** eine Zufallszahl R2 aus 64 Bits durch eine Zufallszahlroutine im Schritt S9 und überträgt die erzeugte Zufallszahl R2 als zweite code-bezogene Information zum Hauptkörper **2** zusammen mit der ersten verschlüsselungsbezogenen Information im Schritt S7.

[0070] Die periphere Einrichtung **1** erzeugt einen zweiten Vergleichsabfragecode auf der Basis der zweiten code-bezogenen Information R2. In diesem Fall liest die periphere Einrichtung **1** vom Speicherabschnitt **12** eine zweite Konstante C20 entsprechend der Schlüsselnummer ”0” als die Verschlüsselungsschlüssel-Identifikationsinformation, die im Schritt S2 empfangen wurde. Im Schritt S10 erzeugt die periphere Einrichtung **1** einen zweiten Vergleichsabfragecode R2||C20, wobei die zweite Konstante S20 nach der zweiten code-bezogenen Information R2 platziert wird.

[0071] Im Schritt S11 erzeugt die periphere Einrichtung **1** eine zweite Verschlüsselungsvergleichsinformation ENC (k0, (R2||C20)) durch Verschlüsseln des zweiten Vergleichsabfragecodes R2||C20 unter Verwendung des Verschlüsselungsschlüssels k0, der unter Verwendung der Verschlüsselungsnummer ”0” als die Verschlüsselungsschlüssel-Identifikationsinformation verwendet wird.

[0072] Im Schritt S12 erzeugt der Hauptkörper **2** einen zweiten Abfragecode R2||C20, wobei er die zweite Konstante C20 nach der zweiten code-bezogenen Information R2 platziert, welche im Schritt S7 empfangen wurde und den Abfragecode R2||C20 erlangt. Im Schritt S13 erzeugt der Hauptkörper **2** eine zweite verschlüsselte Information ENC (k0, (R2||C20)) durch Verschlüsseln des zweiten erzeugten Abfragecodes R2||C20 unter Verwendung des Verschlüsselungsschlüssels k0 und extrahiert einen vorgeschriebenen Teil (untere 64 Bits) der zweiten verschlüsselten Information ENC (k0, (R2||C20)), um zweite verschlüsselungs-bezogene Information zu erzeugen. Im Schritt S14 überträgt der Hauptkörper **2** die extrahierte zweite verschlüsselungs-bezogene Information zur peripheren Einrichtung **1**.

[0073] Wenn die zweite verschlüsselungs-bezogene Information vom Hauptkörper **2** empfangen wird, beurteilt im Schritt S15 die periphere Einrichtung **1**, ob der vorgeschriebene Teil (untere 64 Bits) der zweiten Verschlüsselungsvergleichsinformation, die im Schritt S11 erzeugt wurde, mit der zweiten verschlüsselungs-bezogenen Information übereinstimmt, welche vom Hauptkörper **2** empfangen wird. Im Schritt S16 überträgt die periphere Einrichtung **1** ein Ergebnis der Beurteilung zum Hauptkörper **2**.

[0074] Wie oben beschrieben überträgt, wenn der vorgeschriebene Teil (untere 64 Bits) der zweiten Verschlüsselungsvergleichsinformation, welche im Schritt S11 erzeugt wurde, mit der zweiten verschlüsselungs-bezogenen Information übereinstimmt, die

vom Hauptkörper **2** empfangen wurde, die periphere Einrichtung **1** selbst den vorgeschriebenen Teil der zweiten Verschlüsselungsvergleichsinformation, welche im Schritt S11 erzeugt wird, zum Hauptkörper **2** als Originalerfolgsdaten.

[0075] Wenn der vorgeschriebene Teil (untere 64 Bits) der zweiten Verschlüsselungsvergleichsinformation, welche im Schritt S11 erzeugt wurde, nicht mit der zweiten verschlüsselungs-bezogenen Information, welche vom Hauptkörper **2** empfangen wurde, übereinstimmt, erzeugt die periphere Einrichtung **1** Originalversagerdaten, indem jedes Bit des vorgeschriebenen Teils der zweiten Verschlüsselungsvergleichsinformation, welche im Schritt S11 erzeugt wurde, negiert wird, und überträgt die erzeugten Originalversagerdaten zum Hauptkörper **2**.

[0076] Im Schritt S17 beurteilt der Hauptkörper **2**, ob der Hauptkörper **2** selbst auf der Basis des Beurteilungsergebnisses, welches im Schritt S16 empfangen wurde, erfolgreich als Original bestätigt wurde. Bei dieser Ausführungsform vergleicht der Hauptkörper **2** den vorgeschriebenen Teil der zweiten verschlüsselten Information, welche im Schritt S13 übertragen wurde, mit der Information des Beurteilungsergebnisses, welches im Schritt S16 empfangen wurde. Wenn diese mit einander übereinstimmen, beurteilt der Hauptkörper **2**, dass er selbst erfolgreich als Original bestätigt wurde. Wenn beispielsweise der Verschlüsselungsschlüssel k0 entwichen ist, wird der Hauptkörper **2** wiederaufgefunden und der Verschlüsselungsschlüssel usw., die im Speicherabschnitt **22** gespeichert sind, werden ersetzt (überschrieben), beispielsweise durch einen Verschlüsselungsschlüssel k1, eine erste Konstante C11 und eine zweite Konstante C21 (von denen jede in der peripheren Einrichtung **1** vorher gespeichert wurde), welche identifiziert werden, unter Verwendung einer Schlüsselnummer ”1”. Die Verschlüsselungsschlüssel-Identifikationsinformation wird dann auf ”1” geändert. Dies ermöglicht es, den Verschlüsselungsschlüssel usw. ohne die Notwendigkeit zum Sammeln von peripheren Einrichtungen **1** zu aktualisieren (es sind viel mehr periphere Einrichtungen **1** auf dem Markt als Hauptkörper **2**).

[0077] Obwohl der Hauptkörper **2** und die periphere Einrichtung **1** miteinander verbunden sind, kann die Kommunikation, welche in **Fig.** 6 gezeigt ist, wiederholt durchgeführt werden, d. h., jedes Mal, wenn eine vorgeschriebene Zeit erreicht wird. Wenn die periphere Einrichtung **1** im Schritt S8 nicht als Original bestätigt wird, kann der Hauptkörper **2** zum Schritt S1 zurückkehren und den Prozess von **Fig.** 6 wieder durchführen. In gleicher Weise, wenn im Schritt S17 gefunden wird, dass der Hauptkörper **2** selbst nicht als Original bestätigt wurde, kann der Hauptkörper **2** zum Schritt **1** zurückkehren und den Prozess von **Fig.** 6 wieder durchführen.

[0078] Obwohl die obige Beschreibung so ist, dass Teile von sowohl dem ersten als auch dem zweiten Abfragecode als auch der ersten oder zweiten Verschlüsselungsinformation, die zur Originalbestätigungsverarbeitung verwendet werden, übertragen werden, kann eines von diesen in seiner Gesamtheit übertragen werden. Wenn eines von diesen in seiner Gesamtheit übertragen wird, steigt die Kommunikationsbelastung gemäß an, wobei jedoch der Sicherheitspegel vergrößert werden kann, wobei eine Übereinstimmungs-/Nichtübereinstimmungsbeurteilung beispielsweise durch Übertragen der ersten oder zweiten gesamten verschlüsselten Information beurteilt wird.

[0079] Wo ein Teil eines ersten oder zweiten Abfragecodes als erste oder zweite code-bezogene Information übertragen wird, ist die Reihenfolge der Verbindung der ersten oder zweiten code-bezogenen Information und der Konstanten C nicht auf die oben beschriebene Reihenfolge ”R2||C” beschränkt und kann ”C||R” sein. Außerdem kann die Verbindungsreihenfolge von diesen im Prozess zum Bestätigen der peripheren Einrichtung **1** durch den Hauptkörper **2** (Schritte S1–S8 in **Fig.** 6) und die im Prozess zum Bestätigen des Originals des Hauptkörpers **2** durch die periphere Einrichtung **1** (Schritte S9–S17 in **Fig.** 6) voneinander verschieden sind.

[0080] Der Steuerabschnitt **21** speichert ein Flag, welches ein Originalbestätigungsergebnis zeigt, im Speicherabschnitt **22**. Beispielsweise wird das Flag ”0” gesetzt, wenn die Originalbestätigungsverarbeitung erfolgreich war, und auf ”1”, wenn die Originalbestätigungsverarbeitung fehlgeschlagen hat.

[0081] Bei dieser Ausführungsform führt der Steuerabschnitt **21** des Hauptkörpers **2** und der Steuerabschnitt **11** der Batterie als periphere Einrichtung **1** Originalbestätigungsverarbeitung wiederum durch, wenn die Originalbestätigungsverarbeitung, die unmittelbar durchgeführt wurde, einen Versager zur Folge hatte. Sogar, wenn die Originalbestätigungsverarbeitung erfolgreich war, kann jeder der Steuerabschnitte **21** und **11** eine Originalbestätigungsverarbeitung wiederum nach einem Ablauf einer vorgeschriebenen Zeit durchführen.

[0082] Ein weiteres wichtiges Merkmal dieser Ausführungsform ist, dass der Originalbestätigungsprozess, der durch den Steuerabschnitt **21** ausgeführt wird, davon abhängt, ob der Spannungssteuerabschnitt **27** mit Spannung von einer externen Spannungsquelle beliefert wird. Wenn beispielsweise die Spannung eingeschaltet ist, prüft der Steuerabschnitt **21**, ob die Batterie als die periphere Einrichtung **1** mit dem Spannungssteuerabschnitt **27** verbunden ist oder nicht. Wenn die Batterie mit dem Spannungssteuerabschnitt **27** verbunden ist, beginnt der Steuerabschnitt **21** einen Prozess, der in **Fig.** 7 gezeigt

ist. Obwohl die folgende Beschreibung unter einer Annahme durchgeführt wird, dass ein Speicherbereich, der als Versagerzähler zum Halten der Häufigkeit von aufeinanderfolgenden Originalversagern dient, im Speicherabschnitt **22** gesichert ist, kann ein Versagerzähler in einem Register der CPU vorgesehen sein, welche als Steuerabschnitt **21** arbeitet.

[0083] Im Schritt S21 führt der Steuerabschnitt **21** die Batterieoriginalbestätigungsverarbeitung durch. Im Schritt S22 prüft der Steuerabschnitt **21**, ob die Batterieoriginalbestätigungsverarbeitung erfolgreich war oder nicht (d. h., ob die Batterie als bestätigt beurteilt wurde). Das heißt, der Steuerabschnitt **21** prüft, ob das originalbestätigungs-bezogene Flag auf ”1” gesetzt ist (d. h., den Wert, der zeigt, dass die Originalverarbeitung, die gerade durchgeführt wurde, einen Versager zum Ergebnis hat). Wenn beurteilt wird, dass die Originalbestätigungsverarbeitung fehlgeschlagen hat, wird im Schritt S23 der Versagerzähler um 1 erhöht. Im Schritt S24 beurteilt der Steuerabschnitt **21**, ob der Spannungssteuerabschnitt **27** mit Spannung von einer externen Spannungsquelle beliefert wird oder nicht.

[0084] Wenn der Spannungssteuerungsabschnitt **27** nicht mit Spannung von einer externen Spannungsquelle beliefert wird, setzt im Schritt S25 der Steuerabschnitt **21** das Originalbestätigungsverarbeitungs-Wiederholungsintervall auf einen ersten vorgeschriebenen Intervallwert (beispielsweise 100 ms), und setzt den Schwellenwert der Häufigkeit der Originalversager auf einen ersten Schwellenwert (beispielsweise 30). Im Schritt S26 prüft der Steuerabschnitt **21**, ob der Wert des Versagerzählers den Schwellenwert überschritten hat oder nicht. Wenn der Wert des Versagerzählers den Schwellenwert überschritten hat, führt im Schritt S27 der Steuerabschnitt **21** einen Versagerzeitprozess aus und das Verfahren endet. Das heißt, der Steuerabschnitt **21** führt den Versagerzeitprozess durch, wenn die Originalbestätigungsverarbeitung im Verlauf mehr als die Häufigkeit fehlgeschlagen hat, welche gleich dem festgelegten Schwellenwert ist, und schaltet dann die Spannung des Hauptkörpers **2** aus.

[0085] Wenn dagegen im Schritt S26 beurteilt wird, dass die Häufigkeit von Versagern den gesetzten Schwellenwert nicht überstiegen hat, setzt im Schritt S28 der Steuerabschnitt **21** den Prozess eine Zeitlang aus, d. h. gleich dem Originalbestätigungsverarbeitungs-Wiederholungsintervall. Nach Ablauf dieser Zeit kehrt der Prozess wiederum zurück zum Schritt S21 und wird neu begonnen.

[0086] Wenn im Schritt S24 beurteilt wird, dass der Steuerabschnitt **27** mit Spannung von einer externen Spannungsquelle versorgt wird, setzt im Schritt S29 der Steuerabschnitt **21** das Originalbestätigungsverarbeitungs-Wiederholungsintervall auf einen zweiten vorgeschriebenen Intervallwert (beispielsweise 500 ms) und setzt den Schwellenwert der Häufigkeit der Originalversager auf einen zweiten Schwellenwert (beispielsweise 600). Danach bewegt sich der Prozess zum Schritt S26 und wird fortgesetzt.

[0087] Wie oben beschrieben wird der vorgeschriebene Wiederholungsintervallwert und der Schwellenwert der Häufigkeit von Versagern geändert, und die Periode, während der die Originalbestätigungsverarbeitung wiederholt wird, wird dadurch in Abhängigkeit davon geändert, ob der Spannungsversorgungsabschnitt **27** mit Spannung von einer externen Spannungsquelle beliefert wird oder nicht. Diese Maßnahme betrachtet Fälle, wobei beispielsweise der Steuerabschnitt **11** nicht arbeitet, wenn die Sekundärbatterie des Funktionsabschnitts **14** fast keine Restenergie hat, obwohl die Batterie bestätigt ist. Wenn der Steuerabschnitt **11** nicht in Betrieb ist, sogar, wenn der Hauptkörper **2** (Originalanfrageeinrichtug) eine Zufallszahl zur Batterie überträgt, kann die Batterie die verschlüsselt-bezogene Information nicht übertragen und folglich beurteilt der Hauptkörper **2**, dass die Batterie nicht bestätigt wurde. Im Hinblick darauf wird bei dieser Ausführungsform, obwohl der Spannungssteuerabschnitt **27** mit Spannung von einer externen Spannungsquelle beliefert wird, und die Batterie geladen ist, das Originalverarbeitungsintervall länger eingestellt und die Häufigkeit von Wiederholungen der Originalbestätigungsverarbeitung größer eingestellt. Als Ergebnis wird, wenn die Batterie zu anfangs leer ist, die Originalbestätigungsverarbeitungs-Wiederholungsperiode herausgezogen, so dass die Batterie bis zu einem Ausmaß geladen wird, damit der Steuerabschnitt **11** arbeiten kann.

[0088] Wenn weiter im Schritt S22 beurteilt wird, dass die Batterie erfolgreich als Original bestätigt wurde, setzt im Schritt **30** der Steuerabschnitt **31** den Versagerzähler auf ”0” zurück. Danach setzt der Steuerabschnitt **21** das Originalbestätigungsverarbeitungs-Wiederholungsintervall auf einen dritten vorgeschriebenen Intervallwert (beispielsweise 30 s) im Schritt S31, und führt im Schritt S32 einen Erfolgzeitprozess aus. Das Verfahren bewegt sich zum Schritt S28 und wird weiter ausgeführt.

[0089] Beispielsweise kann der Versagerzeitprozess (Schritt S27) ein Prozess zum Instruieren des Spannungssteuerabschnitt **27** sein, die Spannung auszuschalten, um dadurch den Hauptkörper **2** auszuschalten, oder ein Prozess, um zu veranlassen, dass der Anzeigesteuerabschnitt **24** eine Anzeige tätigt ”nicht verwendbar” und die spiel-bezogene Verarbeitung stoppt.

[0090] Beispielsweise kann die Erfolgzeitverarbeitung (Schritt S32) ein Prozess zum Starten spiel-bezogener Verarbeitung sein. Wenn eine spiel-bezogene Verarbeitung schon begonnen wurde, ist es nicht

immer notwendig, dass eine aktuelle Verarbeitung im Erfolgzeitprozess durchgeführt wird.

[0091] Der Speicherbereich, beispielsweise der Versagerzähler, kann in einem nicht-flüchtigen Speicher des Speicherabschnitts **22** gesichert sein, so dass dessen Inhalt gehalten wird, sogar nach einer Spannungsausschaltung. Dies verhindert eine Handlung, ein Spiel intermittierend weiter zu spielen, indem beispielsweise der Versagerzähler auf halben Weg zurückgesetzt wird, indem eine externe Spannungsquelle mit dem Hauptkörper **2** verbunden oder unterbrochen wird, oder um regelmäßig ein Spiel zu unterbinden und die Spannung wiedereinzuschalten.

[0092] Wie oben beschrieben liefert die Ausführungsform einen Prozess, bei dem Betrachtung Problemen geschenkt wird, welche für die Bestätigung einer Batterie spezifisch sind, beispielsweise ein Problem, dass die Bestätigung einer Batterie als Haupteinheit zum Liefern von Spannung ausgeschaltet wird, da die Batterie noch nicht ausreichend geladen ist.

[0093] Obwohl sich die obige Beschreibung auf den Fall richtet, dass der Hauptkörper **2** eine Heimspielmaschine ist, ist die Erfindung nicht auf diesen Fall beschränkt. Beispielsweise ist es möglich, dass die periphere Einrichtung **1** eine Batterie ist und der Hauptkörper **2** dessen Ladegerät ist. In diesem Fall muss der Hauptkörper **2** nicht immer mit dem Manipulationsabschnitt **23** und dem Anzeigesteuerabschnitt **24** ausgestattet sein. Im Versagerzeitprozess und Erfolgszeitprozess, welche durch den Steuerabschnitt **21** ausgeführt werden, kann beispielsweise das Unterbinden des Ladens bzw. ein Start des Ladens sein.

[0094] Obwohl die vorliegende Erfindung hinsichtlich bevorzugter oder beispielhafter Ausführungsformen beschrieben wurde, ist sie nicht darauf beschränkt.

Patentansprüche

1. Originalbestätigungssystem zum Originalbestätigen einer Batterie als periphere Einrichtung (**1**) durch einen Hauptkörper (**2**),
wobei die Batterie einen Steuerabschnitt (**11**) und der Hauptkörper (**2**) einen Steuerabschnitt (**21**) zur Durchführung einer Originalbestätigungsverarbeitung der Batterie aufweisen,
wobei der Steuerabschnitt (**21**) Mittel zur Prüfung aufweist, ob eine durchgeführte Originalbestätigungsverarbeitung der Batterie erfolgreich war oder nicht,
wobei der Hauptkörper (**2**) ferner einen Spannungssteuerabschnitt (**27**) aufweist,
wobei der Steuerabschnitt (**21**) Mittel zur Prüfung aufweist, ob der Spannungssteuerabschnitt (**27**) mit Spannung von einer externen Spannungsquelle beliefert wird oder nicht,
wobei der Steuerabschnitt (**21**) Mittel zum Setzen eines Wiederholungsintervalls für eine Durchführung der Originalbestätigungsverarbeitung der Batterie aufweist,
wobei der Steuerabschnitt (**21**), für den Fall dass der Spannungssteuerungsabschnitt (**27**) nicht mit Spannung von einer externen Spannungsquelle beliefert wird, das Wiederholungsintervall auf einen ersten Intervallwert setzt,
wobei der Steuerabschnitt (**21**) für den Fall dass der Spannungssteuerungsabschnitt (**27**) mit Spannung von einer externen Spannungsquelle versorgt wird, das Wiederholungsintervall auf einen zweiten Intervallwert setzt.

2. Hauptkörper (**2**) zum Originalbestätigen einer Batterie als periphere Einrichtung (**1**) wobei der Hauptkörper (**2**) einen Steuerabschnitt (**21**) zur Durchführung einer Originalbestätigungsverarbeitung der Batterie aufweist,
wobei der Steuerabschnitt (**21**) Mittel zur Prüfung aufweist, ob eine durchgeführte Originalbestätigungsverarbeitung der Batterie erfolgreich war oder nicht,
wobei der Hauptkörper (**2**) ferner einen Spannungssteuerabschnitt (**27**) aufweist,
wobei der Steuerabschnitt (**21**) Mittel zur Prüfung aufweist, ob der Spannungssteuerabschnitt (**27**) mit Spannung von einer externen Spannungsquelle beliefert wird oder nicht,
wobei der Steuerabschnitt (**21**) Mittel zum Setzen eines Wiederholungsintervalls für eine Durchführung der Originalbestätigungsverarbeitung der Batterie aufweist,
wobei der Steuerabschnitt (**21**), für den Fall dass der Spannungssteuerungsabschnitt (**27**) nicht mit Spannung von einer externen Spannungsquelle beliefert wird, das Wiederholungsintervall auf einen ersten Intervallwert setzt,
wobei der Steuerabschnitt (**21**) für den Fall dass der Spannungssteuerungsabschnitt (**27**) mit Spannung von einer externen Spannungsquelle versorgt wird, das Wiederholungsintervall auf einen zweiten Intervallwert setzt.

3. Hauptkörper (**2**) nach Anspruch 2, **dadurch gekennzeichnet,** dass der Steuerabschnitt (**21**) Mittel zur wiederholten Durchführung der Originalbestätigungsverarbeitung aufweist,
wobei der Steuerabschnitt (**21**) Mittel zum Setzen eines Wiederholungsintervalls für eine Durchführung der Originalbestätigungsverarbeitung der Batterie aufweist,
wobei der Steuerabschnitt (**21**), für den Fall dass der Spannungssteuerungsabschnitt (**27**) nicht mit Spannung von einer externen Spannungsquelle beliefert wird, einen Schwellenwert eines Versagerzählers auf einen ersten Schwellenwert setzt,
wobei der Steuerabschnitt (**21**) für den Fall dass der Spannungssteuerungsabschnitt (**27**) mit Spannung von einer externen Spannungsquelle versorgt wird,

den Schwellenwert des Versagerzählers auf einen zweiten Schwellenwert setzt.

4. Hauptkörper (**2**) nach Anspruch 3, **dadurch gekennzeichnet,** dass der Steuerabschnitt (**21**) Mittel zur Durchführung eines Versagerzeitprozesses aufweist, wobei der Steuerabschnitt (**21**), für den Fall dass der zuvor gesetzte Schwellenwert des Versagerzählers den festgelegten Schwellenwert überstiegen hat den Spannungssteuerabschnitt (**27**) instruiert, die Spannung auszuschalten, um dadurch den Hauptkörper (**2**) auszuschalten.

5. Verfahren zum Originalbestätigen einer Batterie als periphere Einrichtung (**1**) durch einen Hauptkörper (**2**)
wobei das Verfahren zwischen einem Steuerabschnitt (**21**) des Hauptkörpers (**2**) und einem Steuerabschnitt (**11**) der Batterie durchgeführt wird,
wobei der Steuerabschnitt (**21**) prüft, ob eine durchgeführte Originalbestätigungsverarbeitung der Batterie erfolgreich war oder nicht,
wobei der Steuerabschnitt (**21**) bei einer fehlgeschlagenen Originalbestätigungsverarbeitung der Batterie anhand eines Spannungssteuerabschnittes (**27**) des Hauptkörpers (**2**) prüft, ob der Hauptkörper (**2**) mit Spannung von einer externen Spannungsquelle beliefert wird oder nicht,
wobei der Steuerabschnitt (**21**), für den Fall dass der Spannungssteuerungsabschnitt (**27**) nicht mit Spannung von einer externen Spannungsquelle beliefert wird, ein Wiederholungsintervall zur Durchführung einer erneuten Durchführung der Originalbestätigungsverarbeitung der Batterie auf einen ersten Intervallwert setzt,
wobei der Steuerabschnitt (**21**) für den Fall dass der Spannungssteuerungsabschnitt (**27**) mit Spannung von einer externen Spannungsquelle versorgt wird, das Wiederholungsintervall auf einen zweiten Intervallwert setzt.

Es folgen 5 Seiten Zeichnungen

Anhängende Zeichnungen

FIG. 1

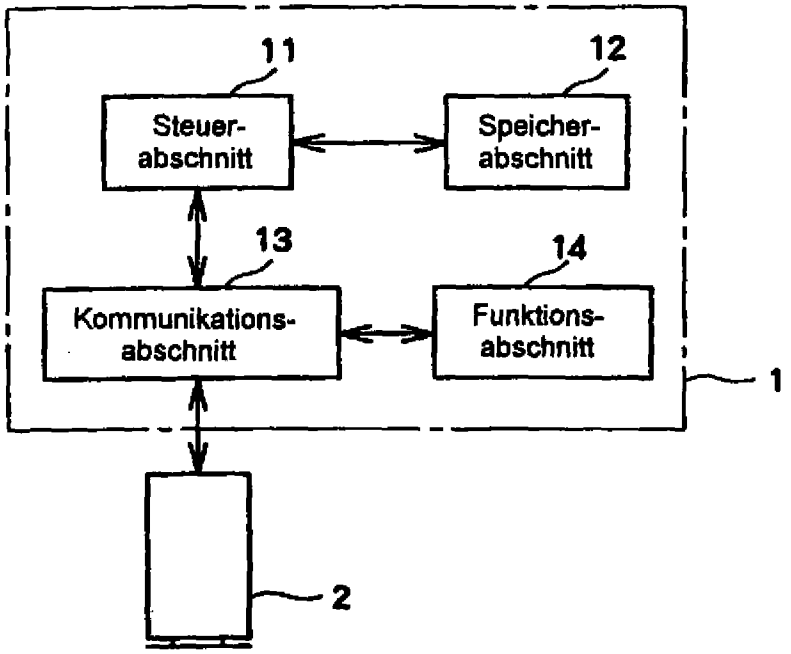


FIG. 2

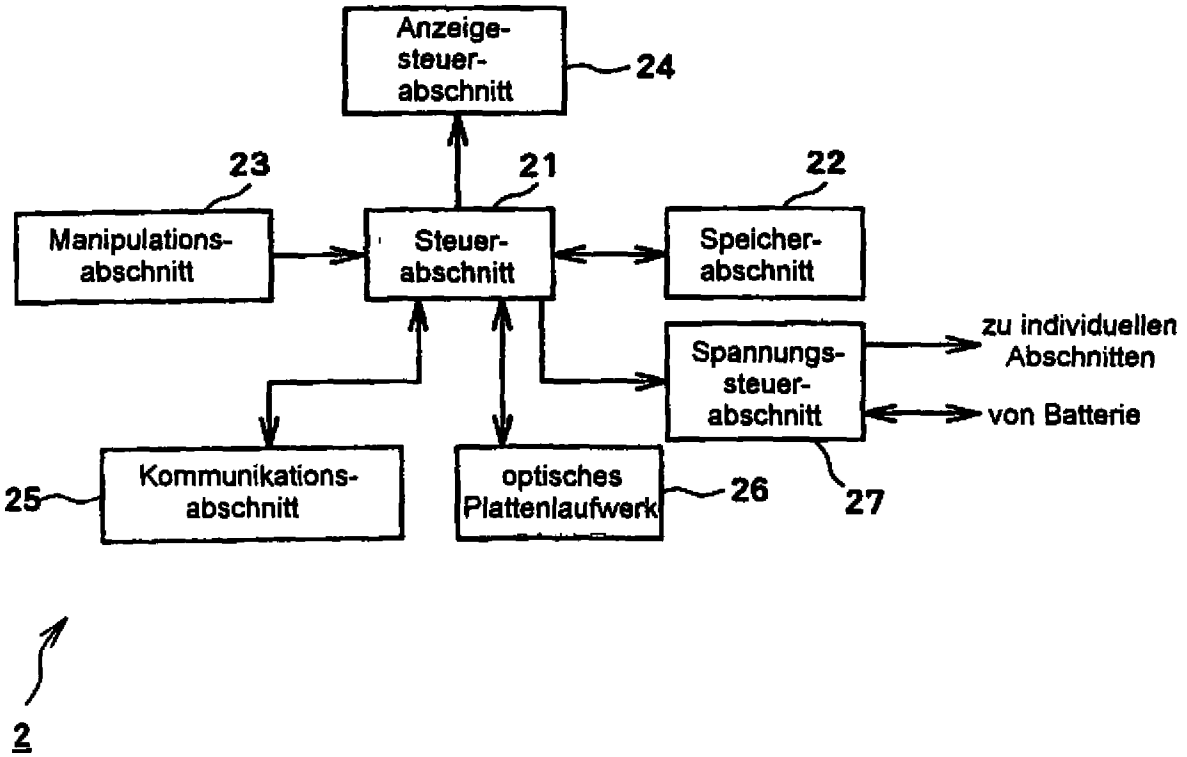


FIG. 3

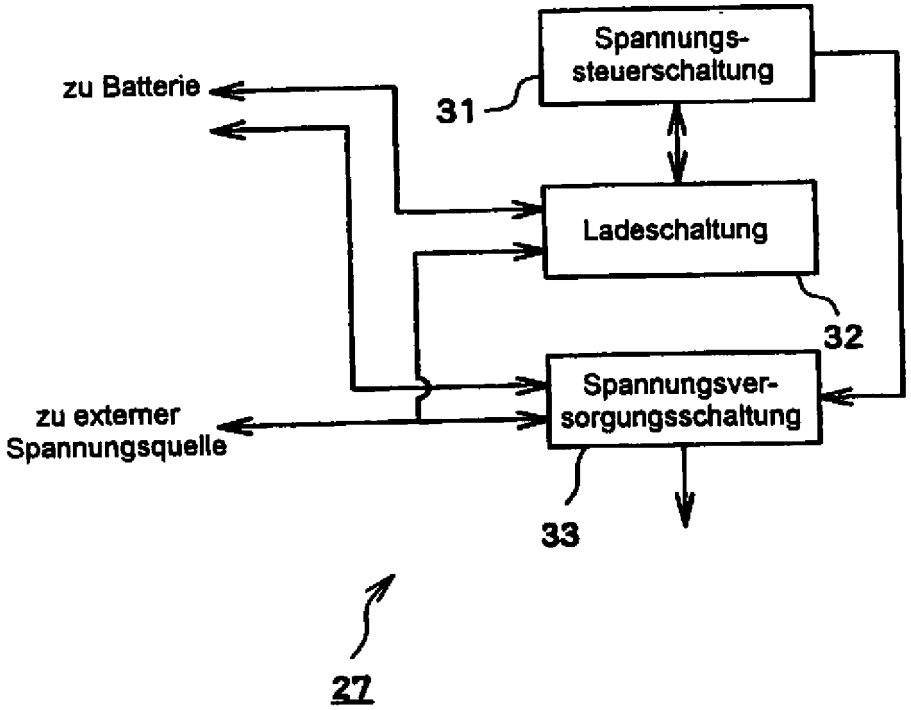

Spannungs-
steuerschaltung
zu Batterie
31
Ladeschaltung
32
Spannungsver-
sorgungsschaltung
zu externer
Spannungsquelle
33
27

FIG. 4

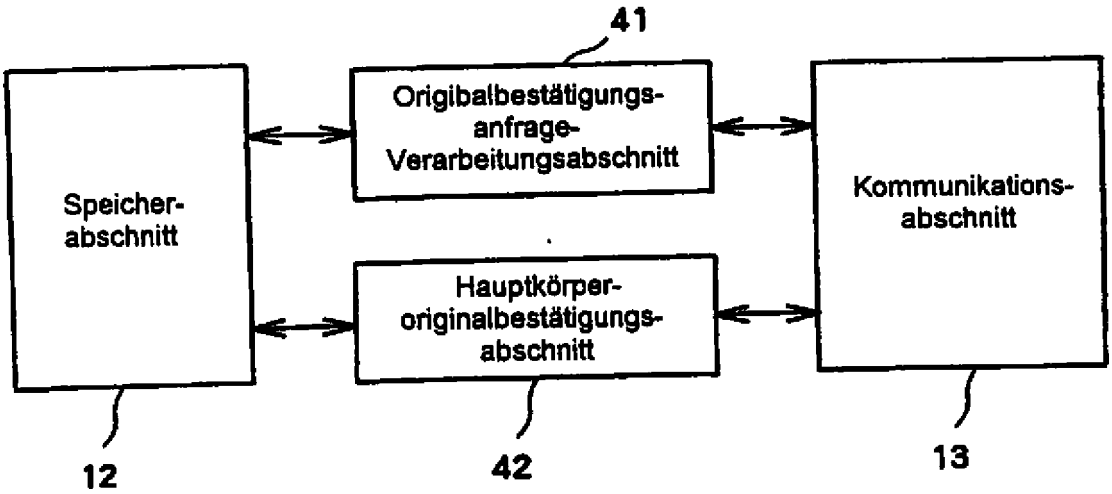

41
Origibalbestätigungs-
anfrage-
Verarbeitungsabschnitt
Speicher-
abschnitt
Kommunikations-
abschnitt
Hauptkörper-
originalbestätigungs-
abschnitt
12
42
13

FIG. 5

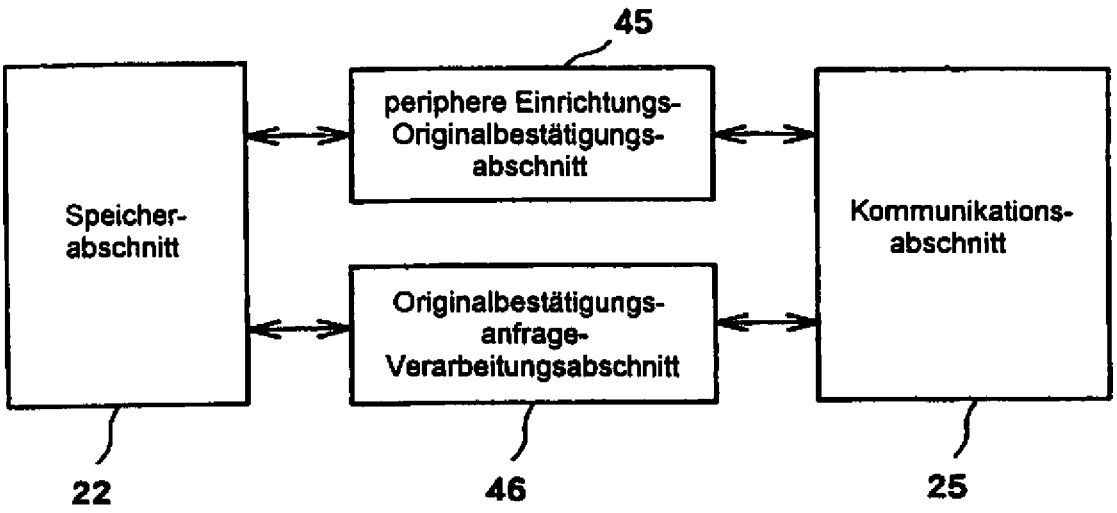

45
periphere Einrichtungs-Originalbestätigungs-abschnitt
Speicher-abschnitt
Originalbestätigungs-anfrage-Verarbeitungsabschnitt
Kommunikations-abschnitt
22
46
25

FIG. 6

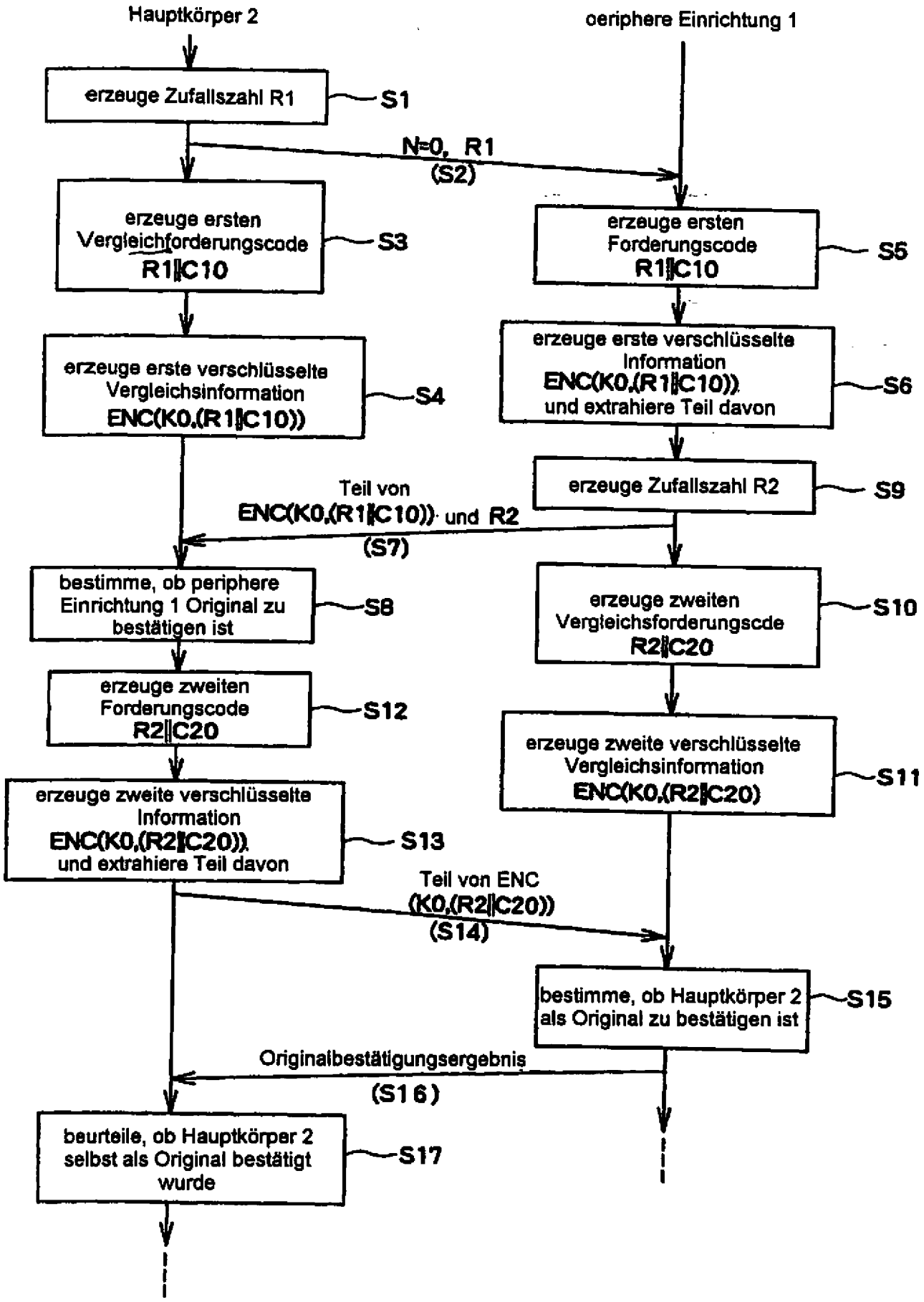
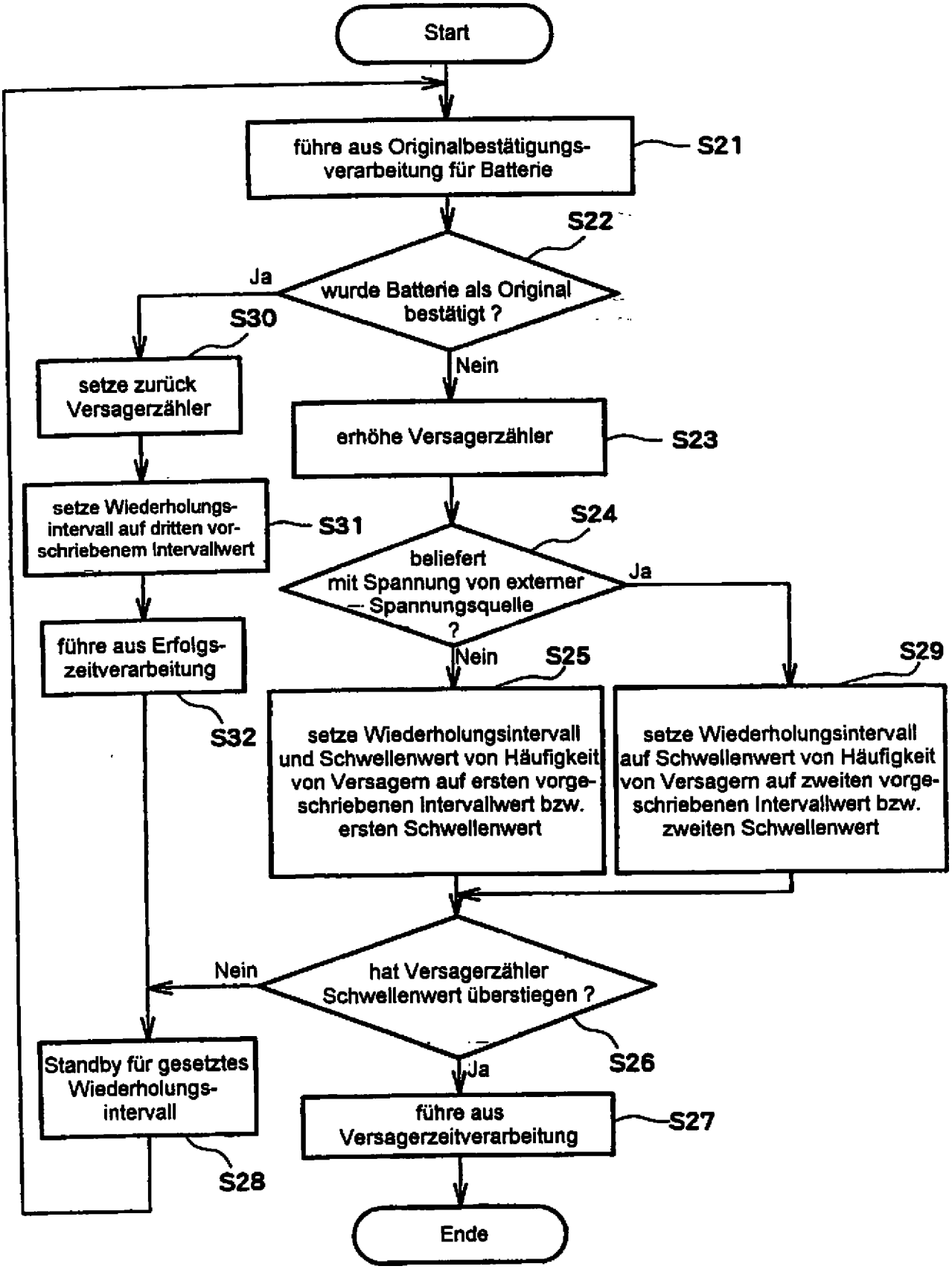

Hauptkörper 2
oeriphere Einrichtung 1
erzeuge Zufallszahl R1
S1
N=0, R1
(S2)
erzeuge ersten Vergleichforderungscode R1‖C10
S3
erzeuge ersten Forderungscode R1‖C10
S5
erzeuge erste verschlüsselte Vergleichsinformation ENC(K0,(R1‖C10))
S4
erzeuge erste verschlüsselte Information ENC(K0,(R1‖C10)) und extrahiere Teil davon
S6
erzeuge Zufallszahl R2
S9
Teil von ENC(K0,(R1‖C10)) und R2
(S7)
bestimme, ob periphere Einrichtung 1 Original zu bestätigen ist
S8
erzeuge zweiten Vergleichsforderungscde R2‖C20
S10
erzeuge zweiten Forderungscode R2‖C20
S12
erzeuge zweite verschlüsselte Vergleichsinformation ENC(K0,(R2‖C20)
S11
erzeuge zweite verschlüsselte Information ENC(K0,(R2‖C20)) und extrahiere Teil davon
S13
Teil von ENC (K0,(R2‖C20))
(S14)
bestimme, ob Hauptkörper 2 als Original zu bestätigen ist
S15
Originalbestätigungsergebnis
(S16)
beurteile, ob Hauptkörper 2 selbst als Original bestätigt wurde
S17

FIG. 7


Start
führe aus Originalbestätigungs-verarbeitung für Batterie
S21
S22
wurde Batterie als Original bestätigt ?
Ja
Nein
S30
setze zurück Versagerzähler
erhöhe Versagerzähler
S23
setze Wiederholungs-intervall auf dritten vor-schriebenem Intervallwert
S31
S24
beliefert mit Spannung von externer Spannungsquelle ?
Ja
Nein
S25
S29
führe aus Erfolgs-zeitverarbeitung
S32
setze Wiederholungsintervall und Schwellenwert von Häufigkeit von Versagern auf ersten vorge-schriebenen Intervallwert bzw. ersten Schwellenwert
setze Wiederholungsintervall auf Schwellenwert von Häufigkeit von Versagern auf zweiten vorge-schriebenen Intervallwert bzw. zweiten Schwellenwert
Nein
hat Versagerzähler Schwellenwert überstiegen ?
S26
Ja
Standby für gesetztes Wiederholungs-intervall
S28
führe aus Versagerzeitverarbeitung
S27
Ende