(19) Deutsches Patent- und Markenamt

(10) **DE 11 2021 004 459 T5** 2023.06.15

(12) # Veröffentlichung

der internationalen Anmeldung mit der
(87) Veröffentlichungs-Nr.: **WO 2022/091544**
in der deutschen Übersetzung (Art. III § 8 Abs. 2 IntPatÜbkG)
(21) Deutsches Aktenzeichen: **11 2021 004 459.1**
(86) PCT-Aktenzeichen: **PCT/JP2021/031236**
(86) PCT-Anmeldetag: **25.08.2021**
(87) PCT-Veröffentlichungstag: **05.05.2022**
(43) Veröffentlichungstag der PCT Anmeldung in deutscher Übersetzung: **15.06.2023**

(51) Int Cl.: ***H04L 9/32*** (2006.01)

(30) Unionspriorität:
2020-180515 **28.10.2020** **JP**

(71) Anmelder:
Hitachi Astemo, Ltd., Hitachinaka-shi, Ibaraki, JP

(74) Vertreter:
MERH-IP Matias Erny Reichl Hoffmann Patentanwälte PartG mbB, 80336 München, DE

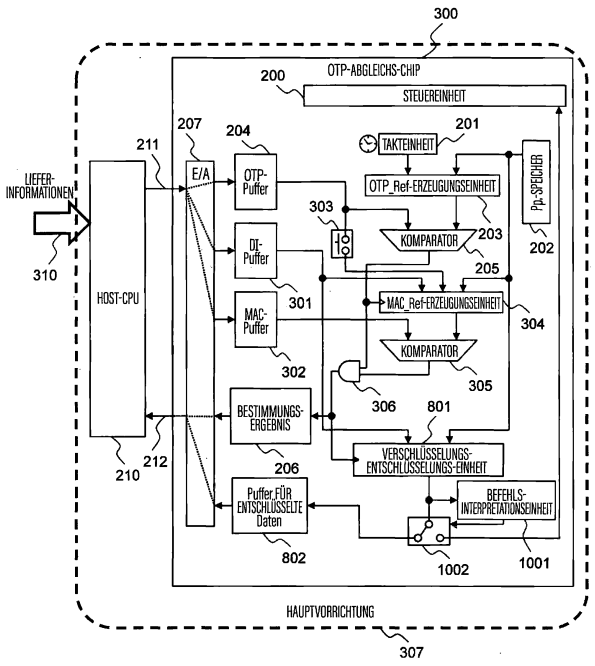
(72) Erfinder:
Miyake, Junji, Hitachinaka-shi, Ibaraki, JP

Prüfungsantrag gemäß § 44 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.

(54) Bezeichnung: **INFORMATIONSVERIFIZIERUNGSVORRICHTUNG, ELEKTRONISCHE STEUERVORRICHTUNG UND INFORMATIONSVERIFIZIERUNGSVERFAHREN**

(57) Zusammenfassung: In einer Informationsverifizierungsvorrichtung wird ein gemeinsamer Schlüssel, über den sich eine Informationsübertragungsquelle und die Informationsverifizierungsvorrichtung Kenntnis teilen, in einem Format gespeichert, das nicht einfach von außen gelesen werden kann. Wenn mindestens drei von einem Einmalpasswort, das aus der Informationsübertragungsquelle gesendet wird und durch eine synchronisierte Zeit und den gemeinsamen Schlüssel erzeugt wird, Lieferinformationen, die aus der Informationsübertragungsquelle gesendet werden und einen anderen Nutzungswert neben der Authentifizierung aufweisen, und einem Nachrichtenauthentifizierungscode, der aus der Informationsübermittlungsquelle gesendet wird und unter Verwendung des gemeinsamen Schlüssels aus diesen Informationselementen berechnet wird, eingegeben werden, wird zumindest ein Bestimmungsergebnis der Authentizität der Lieferinformationen ausgegeben.



Beschreibung

Einbeziehung durch Bezugnahme

[0001] Die vorliegende Anmeldung beansprucht die Priorität der Japanischen Patentanmeldung Nr. 2020-180515, die am 28. Oktober 2020 eingereicht wurde und deren Inhalt hier durch Bezugnahme vollständig mit aufgenommen ist.

Technisches Gebiet

[0002] Die vorliegende Erfindung bezieht sich auf eine Informationsverifizierungsvorrichtung und insbesondere auf eine Fälschungsdetektionstechnik für Informationen, die über einen Kommunikationsweg übertragen werden.

Stand der Technik

[0003] Um zu verifizieren, dass über ein Netz zu korrigierende Informationen nicht auf ihrem Weg verloren gehen oder nicht verfälscht wurden, wird im Allgemeinen eine digitale Signatur verwendet.

[0004] Als digitale Signatur wird jedoch die Verschlüsselung mit öffentlichem Schlüssel verwendet, um die Anfälligkeit gegenüber Abhören zum Zeitpunkt der Schlüssellieferung zu verringern, und ein Computer, der eine Zentraleinheit (CPU) mit relativ geringer Leistungsfähigkeit aufweist, wie beispielsweise eine eingebaute Vorrichtung, wird durch die Entschlüsselung der Signatureinheit schwer belastet.

[0005] Außerdem besteht in einem Fall, in dem die RSA-Verschlüsselung als Form der Verschlüsselung mit öffentlichem Schlüssel verwendet wird, bei der Realisierung eines Quantencomputers das Risiko, dass der geheime Schlüssel durch dessen Primfaktorzerlegungs-Rechenfähigkeit leicht gefunden werden kann und die Signatureinheit aufgrund dieses Kompromisses gefälscht werden kann.

[0006] Als Stand der Technik des vorliegenden technischen Gebiets sind JP 2002-259344 A (PTL 1) und JP 6078686 B (PTL 2) vorhanden.

[0007] JP 2002-259344 A (PTL 1) offenbart ein Einmalpasswort-Authentifizierungssystem, das einen Anwenderauthentifizierungsserver aufweist, der mit einem Anwenderendgerät und einem Mobiltelefon verbunden ist, wobei das Mobiltelefon umfasst: (1) eine mobiltelefonseitige Speichereinheit für geheime Informationen, die geheime Informationen speichert; (2) eine mobiltelefonseitige Hash-Erzeugungseinheit, die einen Hash-Wert unter Verwendung einer Anwender-ID, aktueller Zeitinformationen und der in der mobiltelefonseitigen Speichereinheit für geheime Informationen gespeicherten geheimen Informationen erhält und ein Einmalpasswort durch Umwandeln des erhaltenen Hash-Wertes in eine Zeichenkette erzeugt; und (3) eine Einmalpasswort-Arizeigeeinheit, die das erzeugte Einmalpasswort anzeigt, und der Anwenderauthentifizierungsserver umfasst: (4) eine Anwender-ID/Einmalpasswort-Empfangseinheit, die die Anwender-ID und das Einmalpasswort aus dem Anwenderendgerät empfängt; und (5) eine serverseitige Speichereinheit für geheime Informationen, die die gleichen geheimen Informationen wie die in der mobiltelefonseitigen Speichereinheit für geheime Informationen gespeicherten geheimen Informationen speichert, (6) eine serverseitige Hash-Erzeugungseinheit, die einen Hash-Wert unter Verwendung der empfangenen Anwender-ID, der aktuellen Zeitinformationen und der geheimen Informationen, die in der serverseitigen Speichereinheit für geheime Informationen gespeichert sind, erhält und ein Einmalpasswort durch Umwandeln des erhaltenen Hash-Werts in eine Zeichenkette erzeugt, (7) eine Einmalpasswort-Verifizierungseinheit, die das von der serverseitigen Hash-Erzeugungseinheit erzeugte Einmalpasswort mit dem von der Anwender-ID/Einmalpasswort-Empfangseinheit empfangenen Einmalpasswort vergleicht und in einem Fall, in dem sie übereinstimmen, bestimmt, dass ein Authentifizierungsergebnis erfolgreich ist und (8) eine Authentifizierungsergebnis-Sendeeinheit, die ein Authentifizierungsergebnis an das Anwenderendgerät sendet (siehe Anspruch 1).

[0008] JP 6078686 B2 (PTL 2) offenbart ein Authentifizierungssystem, das ein Bedienungsendgerät authentifiziert, das verwendet wird, um eine fahrzeuginterne Steuervorrichtung zu warten und zu verwalten, die einen Betrieb eines Fahrzeugs steuert. Das Authentifizierungssystem umfasst eine Authentifizierungsvorrichtung, die über eine Kommunikationsleitung mit dem Bedienungsendgerät verbunden ist und einen Bediener authentifiziert, der das Bedienungsendgerät bedient, und die fahrzeuginterne Steuervorrichtung ist dazu ausgelegt zu bestimmen, ob es dem Bedienungsendgerät erlaubt werden soll, einen Betrieb des Wartens und Verwaltens der fahrzeuginternen Steuervorrichtung durchzuführen. Die Authentifizierungsvorrichtung und die fahrzeuginterne Steuervorrichtung umfassen jeweils eine Quelle zur Erzeugung von variablem Code, die einen variablen Code erzeugt, der sich synchron zueinander ändert, eine Speichereinheit, die einen gemeinsamen Schlüssel speichert, der für das Fahrzeug einzigartig ist und der von der Authentifizierungsvorrichtung und der fahrzeuginternen Steuervorrichtung, und einen Authentifizierungscodegenerator, der einen Authentifizierungscode unter Verwendung des variablen Codes und des gemeinsamen Schlüssels erzeugt, wobei die Authentifizierungsvorrichtung die Bedienperson dann authentifiziert, wenn eine Authentifizie-

rungsanforderung von dem Bedienungsendgerät empfangen wird und wenn die Authentifizierung der Bedienperson erfolgreich ist, die Authentifizierungsvorrichtung Informationen zum Spezifizieren des gemeinsamen Schlüssels von dem Bedienungsendgerät erfasst und den Authentifizierungscode unter Verwendung des variablen Codes und des gemeinsamen Schlüssels erzeugt und den Authentifizierungscode an das Betriebsendgerät sendet, wobei das Bedienungsendgerät den von der Authentifizierungsvorrichtung empfangenen Authentifizierungscode an die fahrzeuginterne Steuervorrichtung sendet, die fahrzeuginterne Steuervorrichtung den Authentifizierungscode unter Verwendung des variablen Codes und des gemeinsamen Schlüssels erzeugt und dann, wenn der erzeugte Authentifizierungscode mit dem von dem Bedienungsendgerät empfangenen Authentifizierungscode übereinstimmt, dem Bedienungsendgerät erlaubt wird, einen Betrieb zum Warten und Verwalten der fahrzeuginternen Steuervorrichtung durchzuführen (siehe Anspruch 1).

[0009] Darüber hinaus beschreibt die Beschreibung der sicheren Modul-Bord-Kommunikation (NPL 1), dass eine Detektion der Fälschung von Informationen, die durch MAC-Authentifizierung ausgetauscht werden, durchgeführt wird und ein Wiederholungsangriff durch einen FV-Zähler detektiert wird, der in Lieferinformationen enthalten ist.

Entgegen haltungsliste

Patentdokument(e)

PTL 1: JP 2002-259344 A

PTL 2: JP 6078686 B1

Nichtpatentdokument (e)

[0010] NPL 1: „Specification of Module Secure Onboard Communication", [online], AUTOSAR, https://www.autosar.org/fileadmin/user_upload/standards/classic/4-2/AUTOSAR_SWS_SecureOnboardCommunication.pdf

Zusammenfassung der Erfindung

Technisches Problem

[0011] Die Verschlüsselung mit asymmetrischem Schlüssel, z. B. Verschlüsselung mit öffentlichem Schlüssel, zum Verarbeiten eines Signaturabschnitts einer digitalen Signatur bringt einen großen Rechenaufwand mit sich und erfordert eine große Verarbeitungskapazität, und daher ist es erforderlich, eine Verarbeitungslast durch Wechseln zu einem anderen Verfahren zu reduzieren.

[0012] Beispielsweise ist bei der Verschlüsselung mit öffentlichem Schlüssel wie etwa RSA die arithmetische Berechnung eines großen Potenzrests erforderlich. Andererseits kann die Berechnung einer Hash-Funktion, die für die MAC-Authentifizierung verwendet wird, durch eine logische Operation und eine Verschiebungsoperation implementiert werden und kann leicht von einer CPU mit niedriger Kapazität gehandhabt werden, die in einer fahrzeuginternen elektrischen Steuereinheit (ECU) für eingebettete Anwendungen oder einer Internet-der-Dinge-Vorrichtung (IoT-Vorrichtüng) verwendet wird.

[0013] In PTL 1 und PTL 2 wird das Einmalpasswort vom Zeitsynchronisationstyp unter Verwendung der MAC-Authentifizierung generiert, aber die als Authentifizierungsquelle dienenden Informationen umfassen keine anderen wertvollen Informationen als die Zeit und die Identifikationsinformationen der Vorrichtung. Das heißt, die Erfindung ist nur auf den Austausch von Authentifizierungsinformationen beschränkt und unterstützt keine andere MAC-Authentifizierungstechnologie als die Authentifizierung, wie z. B. Lieferinformationen.

[0014] Die vorliegende Erfindung löst zwei Probleme, nämlich dass eine MAC-Authentifizierung für Lieferinformationen, die einen anderen Nutzungswert neben einer Authentifizierung haben, verwendet wird und ein Verfahren vorgeschlagen wird, das gleichzeitig einen Wiedereinspielungsangriff detektieren kann. Hier ist der Wiedereinspielungsangriff ein Verfahren, bei dem ein Lauschender auf einem Kommunikationsweg frühere Informationen aufzeichnet, die den Kommunikationsweg durchlaufen haben, und dann die aufgezeichneten Informationen oder Sequenzen unverändert an ein Angriffsziel sendet, um das Angriffsziel zu täuschen. Da in der digitalen Signatur der Signaturabschnitt keine Zeitinformationen enthält, kann ein Wiedereinspielungsangriff nicht detektiert werden.

[0015] In NPL 1 (Beschreibung der sicheren Modul-Bord-Kommunikation) wird eine Fälschung von Informationen, die durch eine MAC-Authentifizierung ausgetauscht werden, detektiert und ein Wiedereinspielungsangriff wird unter Verwendung eines Frischewerts (FV) erkannt; der ein Zähler ist, der in Lieferinformationen enthalten ist.

[0016] Der FV ist ein Zähler, dessen Wert jedes Mal aktualisiert wird, wenn die Sendequelle Informationen sendet, und die Empfangsseite akzeptiert keine Informationen mit dem gleichen FV-Wert, wodurch der Wiedereinspielungsangriff eliminiert wird.

[0017] Da jedoch bei NPL 1 der gemeinsame Schlüssel für die MAC-Authentifizierung im Voraus durch das fahrzeuginterne LAN geliefert wird, besteht das Risiko, dass der gemeinsame Schlüssel

abgefangen wird. Daher ist dies zwar praktisch bei der Bord-Kommunikation, d. h. der Kommunikation in einem begrenzten Bereich wie einem fahrzeuginternen LAN, aber nicht sicher genug, um einen Schlüssel über das Internet zu liefern. Wenn der FV-Wert sowohl auf der Sendeseite als auch auf der Empfangsseite verwaltet wird, wird außerdem die Verwaltung des FV-Werts in einem Fall kompliziert, in dem die Anzahl von Lieferzielen zunimmt.

[0018] Eine Aufgabe der vorliegenden Erfindung besteht darin, das oben beschriebene Verlustproblem während der Schlüssellieferung zu lösen und eine Fälschung von über das Internet gesendeten Lieferinformationen zu detektieren. Ferner ist es eine Aufgabe der vorliegenden Erfindung, ein Verfahren zum Detektieren eines Wiedereinspielungsangriffs vorzuschlagen, das mit einer digitalen Signatur nicht möglich ist, und selbst in einem Fall, in dem die Anzahl von Lieferzielen steigt, zu verhindern, dass die Verwaltung kompliziert wird,.

Lösung des Problems

[0019] Ein repräsentatives Beispiel der in der Anmeldung offenbarten Erfindung lautet wie folgt. Das heißt, in einer Informationsverifizierungsvorrichtung wird ein gemeinsamer Schlüssel, über den sich eine Informationsübertragungsquelle und die Informationsverifizierungsvorrichtung Kenntnis teilen, in einem Format gespeichert, das nicht einfach von außen gelesen werden kann. Wenn mindestens drei von einem Einmalpasswort, das von der Informationsübertragungsquelle gesendet wird und durch eine synchronisierte Zeit und den gemeinsamen Schlüssel erzeugt wird, Lieferinformationen, die von der Informationsübertragungsquelle gesendet werden und einen anderen Nutzungswert neben der Authentifizierung aufweisen, und einem Nachrichtenauthentifizierungscode, der von der Informationsübermittlungsquelle gesendet wird und unter Verwendung des gemeinsamen Schlüssels aus diesen Informationselementen berechnet wird, eingegeben werden, wird zumindest ein Bestimmungsergebnis der Authentizität der Lieferinformationen ausgegeben.

Vorteilhafte Wirkungen der Erfindung

[0020] Gemäß einem Aspekt der vorliegenden Erfindung können Fälschungs- und Wiedereinspielungsangriffe auf Lieferinformationen detektiert werden. Aufgaben, Konfigurationen und Wirkungen zusätzlich zu der obigen Beschreibung werden durch die Erläuterung der folgenden Ausführungsformen ersichtlich.

Figurenliste

[**Fig. 1**] **Fig. 1** ist eine Darstellung, die einen Nutzungsfall eines OTP-Abgleichs-Chips als Prämisse zeigt.

[**Fig. 2**] **Fig. 2** ist ein Blockdiagramm, das den OTP-Abgleichs-Chip als eine Prämisse und eine Form, die in einer Sperrvorrichtung des OTP-Abgleichs-Chips untergebracht ist, zeigt.

[**Fig. 3**] **Fig. 3** ist ein Blockdiagramm, das Einzelheiten eines erweiterten OTP-Abgleichs-Chips gemäß einer ersten Ausführungsform zeigt.

[**Fig. 4**] **Fig. 4** ist eine Darstellung, die ein Verfahren der ersten Ausführungsform im Vergleich mit einer herkömmlichen digitalen Signatur zeigt.

[**Fig. 5**] **Fig. 5** ist ein Ablaufdiagramm, das die Lieferinformations-Verifizierungsverarbeitung der ersten Ausführungsform darstellt.

[**Fig. 6**] **Fig. 6** ist ein Zeitdiagramm, das eine Zeitreferenz eines OTP bei der Informationsübertragung gemäß der ersten Ausführungsform darstellt.

[**Fig. 7**] **Fig. 7** ist ein Zeitdiagramm, das einen Informationsübertragungsprozess und einen Person-in-der-Mitte-Angriff in einem Fall darstellt, in dem ein OTP nicht in einem Bereich eines MAC-Werts in der ersten Ausführungsform enthalten ist.

[**Fig. 8**] **Fig. 8** ist ein Blockdiagramm, das Einzelheiten eines erweiterten OTP-Abgleichs-Chips gemäß einer zweiten Ausführungsform darstellt.

[**Fig. 9**] **Fig. 9** ist ein Ablaufdiagramm, das die Lieferinformations-Verifizierungsverarbeitung der zweiten Ausführungsform darstellt.

[**Fig. 10**] **Fig. 10** ist ein Blockdiagramm, das Einzelheiten eines erweiterten OTP-Abgleichs-Chips gemäß einer dritten Ausführungsform darstellt.

[**Fig. 11**] **Fig. 11** ist ein Ablaufdiagramm, das die Lieferinformations-Verifizierungsverarbeitung der dritten Ausführungsform darstellt.

[**Fig. 12**] **Fig. 12** ist ein Ablaufdiagramm einer Festzeit-Unterbrechungsverarbeitung gemäß der dritten Ausführungsform.

[**Fig. 13**] **Fig. 13** ist eine Darstellung, die eine Empfangsvorrichtungsgruppe zeigt, die ein Empfangs-Cluster der dritten Ausführungsform dynamisch vergrößert oder verkleinert.

Beschreibung von Ausführungsformen

[0021] Nachfolgend werden Ausführungsformen der vorliegenden Erfindung unter Bezugnahme auf die

beigefügten Zeichnungen beschrieben. Ferner schränken die unten beschriebenen Ausführungsformen die Ansprüche der Erfindung nicht ein. Nicht alle Elemente und deren Kombinationen, die in den Ausführungsformen beschrieben sind, sind als Lösung der Erfindung wesentlich.

[0022] Es ist zu beachten, dass in den Zeichnungen zum Beschreiben der Ausführungsformen Abschnitte mit den gleichen Funktionen mit den gleichen Bezugszeichen bezeichnet sind und eine wiederholte Beschreibung davon weggelassen wird.

[0023] Außerdem können in der folgenden Beschreibung Ausdrücke, die sich auf einen Informationsspeicherbereich beziehen, wie „xxx-Register“ und „xxx-Speicher“, als Beispiel für Informationen verwendet werden, aber Attribute, die sich auf Eigenschaften des Speicherbereichs beziehen, d. h. Attribute z. B. ein Verfahren zum Spezifizieren eines Orts, Überlegenheit oder Unterlegenheit in Bezug auf eine Zugriffsgeschwindigkeit, Flüchtigkeit oder Nichtflüchtigkeit in Bezug auf einen Leistungsversorgungsbetrieb oder einen Auffrischungsbetrieb oder lesbar/beschreibbar oder nur lesbar werden nicht durch den Wortlaut klassifiziert. Außerdem kann eine beliebige Datenstruktur der Informationen verwendet werden. Das heißt, um anzugeben, dass die Informationen nicht von der Struktur des Speicherbereichs abhängen, kann „xxx-Registerinhalt“ als „xxx-Speicherinhalt“ bezeichnet werden. Ferner kann „xxx-Speicherinhalt“ einfach als „xxx-Inhalt“ bezeichnet werden. In der folgenden Beschreibung ist die Konfiguration jedes Informationselements ein Beispiel und Informationen können geteilt und gehalten oder kombiniert und gehalten werden.

<Prämissenkonfiguration>

[0024] Der Inhalt des OTP-Abgleichs-Chips (Einmalpasswort-Abgleichs-Chips) wird nachstehend vor der vorliegenden Anmeldung kurz beschrieben.

[0025] Fig. 1 ist eine Darstellung, die einen Nutzungsfall eines OTP-Abgleichs-Chips 110 als Prämisse darstellt.

[0026] Ein in einer Sperrvorrichtung 103 montierter OTP-Abgleichs-Chip 110 ist eine Vorrichtung mit einer arithmetischen Einheit, die eine vorbestimmte Verarbeitung ausführt, und einer Speichereinheit, auf die die arithmetische Einheit zugreifen kann, um einen Anwender 102 zu authentifizieren. Die arithmetische Einheit führt eine arithmetische Verarbeitung gemäß einer vorbestimmten Prozedur aus und der Prozessor kann ein vorbestimmtes Programm oder Hardware (FPGA, ASIC usw.) ausführen. Die Sperrvorrichtung 103 hat eine Funktion zum Verursachen eines Sperr-/Entsperrvorgangs der Sperrvorrichtung 103 gemäß dem Authentifizierungsergebnis des OTP-Abgleichs-Chips 110.

[0027] Der Anwender 102 meldet sich bei dem Server für Anwenderauthentifizierung & OTP-Ausgabe 100 durch strenge Anwenderauthentifizierung 107 an, und dann, wenn die Berechtigung erteilt wird, wird ein OTP 108 vom Zeitsynchronisationstyp aus dem Server für Anwenderauthentifizierung & OTP-Ausgabe 100 ausgegeben.

[0028] Der Anwender 102 offenbart der Sperrvorrichtung 103 das ausgegebene OTP 108 innerhalb einer vorbestimmten Zeit (das ausgegebene OTP 108 und ein in der Sperrvorrichtung 103 offenbartes OTP 109 sind gleich, außer dass die Bezugszeichen unterschiedlich sind). Die Sperrvorrichtung 103 fordert den internen OTP-Abgleichs-Chip 110 auf, die Authentizität des OTP 109 zu bestimmen, und führt einen vorbestimmten Betrieb durch, wenn die Authentifizierung durch die Bestimmung erfolgreich ist (wenn die Authentizität erkannt wird).

[0029] Der OTP-Abgleichs-Chip 110 teilt sich in der Herstellungsphase einen gemeinsamen Schlüssel einer Passphrase 106 mit dem Server für Anwenderauthentifizierung & OTP-Ausgabe100 und kann den gemeinsamen Schlüssel von der Herstellungsphase bis zur Betriebsphase des Produkts verbergen, ohne dass Informationen verloren gehen. Es kann gesagt werden, dass es sich bei den Schlüsselinformationen um eine stark physische Schlüssellieferung handelt, die nicht den Kommunikationsweg durchläuft.

[0030] Der OTP-Abgleichs-Chip 110 ist ausgezeichnet hinsichtlich der Manipulationssicherheit, der gemeinsame Schlüssel innen ist nicht physisch von außen zu finden und er hat eine Struktur, bei der nur Firmware innerhalb des OTP-Abgleichs-Chips auf Informationen zu dem gemeinsamen Schlüssel zugreifen kann. Daher kann der OTP-Abgleichs-Chip 110 als eine Art Hardware-Sicherheitsmodul (HSM) betrachtet werden.

[0031] Da der Takt 104 des Servers 100 und ein Takt 105 in dem OTP-Abgleichs-Chip 110 synchronisiert sind und der gemeinsame Schlüssel der Passphrase 106 von dem Server 100 und dem OTP-Abgleichs-Chip 110 geteilt wird, gelingt die Authentifizierung durch Abgleichen eines Werts (OTPs 108 und 109), der durch eine Hash-Funktion (später beschrieben) unter Verwendung der Zeit eines Takts 104 des Servers 100 und der Passphrase 106 berechnet wird, und eines Werts (nicht dargestellt) zum Vergleich, durch -die gleiche Hash-Funktion unter Verwendung des Takts 105 und der Passphrase 106 in dem OTP-Abgleichs-Chip 110 berechnet wird.

[0032] Hier wird für die vorliegende Ausführungsform der Server für Anwenderauthentifizierung &

OTP-Ausgabe 100 als zu einem Informationslieferungs-Server erweitert betrachtet (1300 in **Fig. 13**). Ferner wird ein Fall betrachtet, in dem die zwischenzeitliche Teilnahme des Anwenders 102 eliminiert wird und der Informationslieferungs-Server 1300 selbst das erweiterte OTP (422 in **Fig. 4**) direkt überträgt, indem er die Lieferinformationen auf Anfrage an die Sperrvorrichtung 103 und ferner zu dem OTP-Abgleichs-Chip 110 hinzufügt.

[0033] Dabei kann der als Passphrase 106 bezeichnete gemeinsame Schlüssel in dem OTP-Abgleichs-Chip 110 , der mit dem Informationslieferungs-Server1300 geteilt wird, zu der MAC-Authentifizierung umgeleitet werden und eine Fälschung der Lieferinformationen kann unter Verwendung der MAC-Authentifizierung detektiert werden.

[0034] Da dieser gemeinsame Schlüssel, wie es oben beschrieben ist, der physischen Verteilung von Schlüsselinformationen entspricht, die in dem OTP-Abgleichs-Chip 110 verborgen sind, besteht außerdem kein Abhörrisiko basierend auf der Schlüssellieferung auf einem Kommunikationsmedium wie in NPL 1 und es ist auch nicht erforderlich, wie digitale Signaturen die Verschlüsselung mit öffentlichen Schlüsseln zu verwenden.

[0035] Ferner ist es durch Hinzufügen eines Einmalpassworts vom Zeitsynchronisationstyp, das eine Originalfunktion ist, als Kopfstück zu dem Kopf der Lieferinformationen möglich zu verifizieren, dass die Informationen Informationen, die zu der entsprechenden Zeit in Verbindung mit der globalen Zeit übertragen werden, (keine Informationen, die nach der Aufzeichnung reproduziert werden) sind, und es ist möglich, einen Wiedereinspielungsangriff zu detektieren.

[0036] **Fig. 2** ist ein Blockdiagramm, das den OTP-Abgleichs-Chip 110 als eine Prämisse und eine in der Sperrvorrichtung 103 untergebrachte Form da rstel lt.

[0037] Die Sperrvorrichtung 103 umfasst eine Host-CPU 210 und einen OTP-Abgleichs-Chip 110. Die Host-CPU 210 und der OTP-Abgleichs-Chip 110 sind kommunikationstechnisch verbunden.

[0038] Herkömmlicherweise kann eine sicherheitsbezogene Berechnung in einem Hauptkörper-Chip (der oben beschriebenen Host-CPU 210) und einem separaten Sicherheits-Chip (dem oben beschriebenen OTP-Abgleichs-Chip 110) angesiedelt sein. Dies dient zum Verhindern von Informationslecks, so dass etwa ein geheimer Schlüssel Informationen, die als Verschlüsselungssystem mit öffentlichem Schlüssel bezeichnet werden) oder ein gemeinsamer Schlüssel (Informationen, die als Verschlüsselungssystem mit gemeinsamem Schlüssel bezeichnet werden), die geheim zu halten sind, in dem Sicherheits-Chip gespeichert werden. Wie es oben beschrieben ist, ist der Sicherheits-Chip von dem Hauptkörper-Chip getrennt und ein in der Hardware vollständig unabhängiges Modul wird als Hardware-Sicherheitsmodul (HSM) bezeichnet.

[0039] Durch Trennen des Sicherheits-Chips und des Hauptkörper-Chips kann der Speicherbereich des Sicherheits-Chips aus dem Hauptkörper-Chip vollständig uneinsehbar sein und ein Durchsickern vertraulicher Informationen kann verhindert werden. Außerdem kann unter dem Gesichtspunkt der Manipulationssicherheit ein Verbergungsverfahren, wie etwa ein Siliciumprozess (schwebende Kapazität), bei dem Informationen verschwinden, wenn die Versiegelung geöffnet wird, nur für den Sicherheits-Chip hergenommen werden.

[0040] Durch Trennen der Host-CPU 210 und des OTP-Abgleichs-Chips 110 voneinander kann die Manipulationssicherheit durch den OTP-Abgleichs-Chip 110 selbst sichergestellt werden, wie es oben beschrieben ist, und es ist möglich zu verhindern, dass Informationen über einen geheimen und geschützten gemeinsamen Schlüssel (z. B. die geteilte Kenntnis der Passphrase 106 mit dem Server für Anwenderauthentifizierung & OTP-Ausgabe 100 von **Fig. 1**) innerhalb des OTP-Abgleichs-Chips 110 durch die Host-CPU 210 gelesen werden.

[0041] Ein Einmalpasswort 109 wird über die Host-CPU 210 und den Kommunikationsweg 211 an den OTP-Abgleichs-Chip 110 gesendet. Das Verifizierungsergebnis wird von dem OTP-Abgleichs-Chip 110 über den Kommunikationsweg 212 an die Host-CPU 210 zurückgesendet. Aufgrund dieses Ergebnisses bestimmt die Host-CPU 210 die als Nächstes auszuführende Verarbeitung.

[0042] Auf dem Kommunikationsweg 211 von der Host-CPU 210 zu dem OTP-Abgleichs-Chip 110 werden ein von der Host-CPU 210 an den OTP-Abgleichs-Chip 110 gegebener Befehl, Taktzeitanpassungsdaten in dem OTP-Abgleichs-Chip 110 und extern authentifizierte OTP-Daten übertragen.

[0043] Auf dem Kommunikationsweg 212 von dem OTP-Abgleichs-Chip 110 zu der Host-CPU 210 werden das von dem OTP-Abgleichs-Chip 110 an die Host-CPU 210 zurückgegebene Authentifizierungsergebnis und verschiedene Zustandsberichtswerte übertragen.

[0044] Die Kommunikationswege 211 und 212 zwischen dem OTP-Abgleichs-Chip 110 und der Host-CPU 210 können eine serielle Übertragung oder eine parallele Übertragung wie etwa ein Bus sein. Ferner kann ein Netz verwendet werden, das durch ein anderes fortschrittliches Protokoll als seriell oder

parallel gesteuert wird. Die Kommunikationswege 211 und 212 werden von einer E/A-Einheit 207 innerhalb des OTP-Abgleichs-Chips 110 gesteuert.

[0045] Der OTP-Abgleichs-Chip 110 umfasst eine Steuereinheit 200, eine Takteinheit 201, einen Passphrasenspeicher 202, eine Vergleichs-OTP-Erzeugungseinheit 203, einen Empfangs-OTP-Puffer 204, der vorübergehend das Empfangs-OTP speichert, einen OTP-Komparator 205, ein Bestimmungsergebnisregister 206 für die Ausgabe und die oben beschriebene E/A-Einheit 207.

[0046] Die Steuereinheit 200 ist ein Teil, das den gesamten Betrieb des OTP-Abgleichs-Chips 110 steuert, und kann durch einen PLC (Controller mit programmierbarer Logik) implementiert werden oder kann durch Software oder Firmware durch eine allgemeine CPU implementiert werden.

[0047] Die Takteinheit 201 weist einen Takt auf, der autonom taktet, nachdem zu dem Zeitpunkt des anfänglichen Betriebs ein anfänglicher Zeitwert von der Host-CPU 210 über den Kommunikationsweg 211 eingestellt wurde. Auch wenn die gesamte Leistungsversorgung der Sperrvorrichtung 103 unterbrochen wird, wird eine Notleistung zugeführt, so dass nur die Takteinheit 201 weiter arbeitet.

[0048] In einem Fall, in dem die Notleistung unterbrochen und der Takt angehalten wird, oder in einem Fall, in dem der Takt durch die Rücksetzoperation des OTP-Abgleichs-Chips 110 initialisiert wird, wird der Zustand über den Kommunikationsweg 212 an die Host-CPU 210 gemeldet und das Zurücksetzen des Zeitwerts angefordert.

[0049] Der Passphrasenspeicher 202 ist ein Teil, der die Passphrase 106 speichert, wobei deren Kenntnis mit dem Server für Anwenderauthentifizierung & OTP-Ausgabe 100 geteilt wird, und weist eine hohe Manipulationssicherheit auf und schützt den gespeicherten Inhalt sogar gegen destruktives Lesen von außerhalb des Chips (Schutz gegen destruktive Lesevorgänge können die Erstellung von Emulations-Chips verhindern). Natürlich kann die Host-CPU 210 den in dem Passphrasenspeicher 202 gespeicherten Inhalt nicht lesen.

[0050] Um den Betrieb des OTP-Abgleichs-Chips 110 kurz zu beschreiben, wird das von außen gesendete OTP 109 in dem OTP-Empfangspuffer 204 des OTP-Abgleichs-Chips 110 über die Host-CPU 210 gespeichert. Eine OTP-Abgleichsanforderung wird von der Host-CPU 210 zusammen mit dem OTP 109 angewiesen.

[0051] Die Vergleichs-OTP-Erzeugungseinheit 203 des OTP-Abgleichs-Chips 110 berechnet einen Vergleichs-OTP-Wert aus der aktuellen Zeit, die aus der Takteinheit 201 gelesen wird, die mit dem Server für Anwenderauthentifizierung & OTP-Ausgabe 100 synchronisiert ist, und der Passphrase 106, die aus dem Passphrasenspeicher 202 gelesen wird.

[0052] Der OTP-Komparator 205 vergleicht den von der Vergleichs-OTP-Erzeugungseinheit 203 berechneten Wert mit dem in dem OTP-Empfangspuffer 204 gespeicherten Wert, bestimmt, dass die Authentifizierung erfolgreich war, wenn beide miteinander übereinstimmen, und bestimmt, dass die Authentifizierung fehlgeschlagen ist, wenn beide miteinander übereinstimmen. Das Bestimmungsergebnis wird an das Bestimmungsergebnisregister 206 gesendet und über den Kommunikationsweg 212 an die Host-CPU 210 gemeldet. Es wird angenommen, dass das aus dem OTP-Abgleichs-Chip 110 ausgegebene Bestimmungsergebnis nicht nur ein fester Wert wie z. B. ein Merker von 0 oder 1 ist, sondern in einem im Voraus mit der Host-CPU 210 bestimmten Format ausgegeben wird. Dies soll das Authentifizierungssystem (die Verknüpfungsoperation zwischen der Host-CPU 210 und dem OTP-Abgleichs-Chip 110) vor einer Ummodellierung, um einen gefälschten OTP-Abgleichs-Chip zu ersetzen, oder einem Angriff des Einspeisens falscher Informationen in den Kommunikationsweg 212 schützen.

<Erste Ausführungsform>

[0053] **Fig. 3** ist ein Blockdiagramm, das Einzelheiten des erweiterten OTP-Abgleichs-Chips 300 gemäß einer ersten Ausführungsform darstellt.

[0054] Im Übrigen unterscheidet sich die Hauptvorrichtung 307, die den OTP-Abgleichs-Chip 300 aufnimmt, von der Schließvorrichtung 103, die nur die OTP-Autheritifizierungsfunktion hat, und es wird beispielsweise im Fall einer Nutzung in dem Fahrzeug eine Vorrichtung, die den Kern eines fahrzeuginternen LAN bildet und als ein zentrales Gateway (CGW) arbeitet, das eine Weiterleitung (Datenweitergabe, Zyklusumsetzung, Protokollumsetzung, Datenrekombination usw.) zwischen ECUs durchführt, angenommen. Es ist zu beachten, dass in dem erweiterten OTP-Abgleichs-Chip 300 Komponenten mit den gleichen Funktionen wie jenen des oben beschriebenen OTP-Abgleichs-Chips 110 mit den gleichen Bezugszeichen bezeichnet sind und deren Beschreibung weggelassen wird.

[0055] Es wird angenommen, dass die in die Hauptvorrichtung 307 eingegebenen Lieferinformationen 310 Daten (Aktualisieren von Steuersoftware, Aktualisieren von Patch, Steuerparameter und Steuerregel) einer ECU (nicht dargestellt) sind, die unmittelbar unter dem CGW durch ein fahrzeuginternes LAN (nicht abgebildet) abgeschlossen ist und per OTA (über die Luft) aktualisiert wird.

[0056] Mehrere ECUs sind angeschlossen, während sie in systembasierte dedizierte Netze wie etwa ein Steuersystem, ein Sicherheitssystem, ein Körpersystem und ein Informationssystem unterteilt sind. Das CGW ist eine Vorrichtung, die als Hub eines Sternnetze, das diese dedizierten Netz umfasst, dient und auch als Schnittstelle fungiert, die mit der Außenseite des Fahrzeugs über Kommunikationsmittel wie drahtlos (Long Term Evolution (LTE), Wireless Fidelity (Wi -Fi) und Smartphone) oder drahtgebunden (Fehlerdiagnosetool, Ladestation).

[0057] Unter Verwendung der vorliegenden Erfindung authentifiziert das CGW strikt externe Aktivitäten als eine OTA-Übertragungsquelle, inspiziert strikt Fälschungen von übertragenen Lieferinformationen und verteilt Daten durch ein fahrzeuginternes LAN an jede ECU.

[0058] Bei der in **Fig. 3** werden Lieferinformationspuffer (DI-Puffer) 301, der die empfangenen Lieferinformationen vorübergehend speichert, ein Empfangs-MAC-Wert-Puffer 302 , der den empfangenen MAC-Wert (Nachrichtenauthentifizierungscode) vorübergehend speichert, ein Wechselschalter 303 (normalerweise „geschlossen“) zum Auswählen, ob das OTP in dem MAC-Wert enthalten ist, eine Vergleichs-MAC-Wert-Erzeugungseinheit 304, ein MAC-Wert-Komparator 305 und eine UND-Logik 306 , die den Inhalt des Bestimmungsergebnisregisters 206 nur dann als OK bestimmt, wenn die OTPs und der MAC-Wert übereinstimmen, zu dem in **Fig. 2** gezeigten Beispiel hinzugefügt.

[0059] Fig. 4 ist eine Darstellung, die eine Form eines Informationslieferungsprogramms der ersten Ausführungsform und ein Erzeugungsprinzip und ein Verifizierungsprinzip eines Prüfcodes (Signatur oder MAC-Wert) im Vergleich zu einer herkömmlichen digitalen Signatur zeigt.

[0060] In den Spalten der Tabelle sind von links der Reihe nach der Prozess 400 in dem Informationslieferungs-Server auf der Lieferseite, eine Informationsform auf dem Übertragungsweg (drahtgebunden, drahtlos) 401 und der Empfangsverifizierungsprozess 402 in einem Empfangsendgerät (Auto, IoT) dargestellt. Die Zeilen der Tabelle zeigen oben die herkömmliche digitale Signatur 410 und unten das Verfahren 420 der vorliegenden Ausführungsform.

[0061] Der Betrieb der herkömmlichen digitalen Signatur, der im oberen Abschnitt 410 dargestellt ist, wird beschrieben. Ein Feld 411 gibt eine Erzeugungsprozedur von zu sendenden Informationen mit einer digitalen Signatur von der Serverseite an. Die Lieferinformationen werden in eine unidirektionale Hash-Funktion eingegeben, um einen Hash-Wert (ein Nachrichtenextrakt) zu berechnen. Dabei ist die unidirektionale Hash-Funktion (im Folgenden wird Hash() kurz als Hash-Funktion oder als mathematische Funktion bezeichnet) eine kryptographische Funktion, die Daten beliebiger Länge in Daten fester Länge (etwa 128 bis 512 Bit) komprimiert und die folgenden Eigenschaften (1) bis (3) aufweist.

(1) Unidirektional: Es ist schwierig, den Eingabewert anhand des Ausgabewerts zu finden. Das heißt, wenn ein bestimmter Hash-Wert h gegeben ist, muss es schwierig sein, eine umgekehrte Operation durchzuführen, um ein beliebiges m zu erhalten, das h = Hash(m) erfüllt.

(2) Schwierigkeit bei der Berechnung von zweiten Primärbildern: Es ist schwierig, eine andere Eingabe zu bestimmen, die den gleichen Hash-Wert wie ein bestimmter Eingabewert ergibt. Das heißt, wenn m gegeben ist, muss es schwierig sein, m' (wobei $m \neq m'$) so zu erhalten, dass Hash(m) = Hash(m').

(3) Geringe Wahrscheinlichkeit von Kollisionen: Es ist schwierig, zwei Eingabewerte zu finden, die den gleichen Ausgabewert erzeugen. Das heißt, es muss schwierig sein, m und m' (wobei $m \neq m'$) zu erhalten, die Hash(m) = Hash(m') erfüllen.

[0062] Das heißt, die unidirektionale Hash-Funktion ist eine kryptografische Funktion, bei der eine Ausgabe leicht mit zuverlässiger Reproduzierbarkeit berechnet werden kann, wenn eine Eingabe gegeben ist, es jedoch schwierig ist, eine umgekehrte Operation von der Ausgabe zu der Eingabe durchzuführen (enormer Zeitaufwand ist erforderlich).

[0063] Da außerdem Daten beliebiger Größe zu einem Hash-Wert komprimiert und gesammelt werden können, um eine Ausgabe mit fester Länge zu erhalten, wird der Hash-Wert auch als Nachrichtenextrakt bezeichnet. Der Server erstellt eine Signatur, indem er eine Verschlüsselung mit öffentlichem Schlüssel unter Verwendung des geheimen Serverschlüssels an dem auf diese Weise berechneten Hash-Wert (Nachrichtenextrakt) durchführt.

[0064] Ein Feld 412 gibt Daten an, die über den Übertragungsweg der Lieferinformationen in der digitalen Signatur übertragen wurden. Das heißt, auf dem Übertragungsweg werden die Lieferinformationen und die Signatur in Paaren übertragen. Da die Signatur die Zeitkomponente nicht enthält, ist die Signatur gegen den Wiedereinspielungsangriff unwirksam. Das heißt, wenn das Paar aus den Lieferinformationen und der Signatur abgefangen wird, kann das Paar aus den Lieferinformationen und der Signatur, das durch das Abhören aufgezeichnet wird, beliebig oft an das Empfangsendgerät gesendet werden. Da die richtige Signatur angehängt ist, empfängt

das Empfangsendgerät die Lieferinformationen als gültig.

[0065] Ein Feld 413 gibt eine Verarbeitung auf der Seite des Empfangsendgeräts an. Das Empfangsendgerät führt eine Entschlüsselung mit öffentlichem Schlüssel an der gesendeten Signatur unter Verwendung des öffentlichen Schlüssels des Servers durch und erhält einen Hash-Wert der entschlüsselten Sendelieferinformationen. Außerdem erhält das Empfangsendgerät unabhängig einen Hash-Wert aus den empfangenen Lieferinformationen unter Verwendung der gleichen Hash-Funktion. Die beiden Hash-Werte werden verglichen und dann, wenn die Hash-Werte übereinstimmen, wird dies als OK bestimmt, da die Informationen zwischen der Sendeseite und der Empfangsseite korrekt übertragen wurden, und wenn die Hash-Werte nicht übereinstimmen, wird dies als NIO bestimmt, da ein Verlust oder eine Verfälschung der Informationen vorliegt.

[0066] Der untere Teil 420 zeigt den Betrieb des Servers und des Empfangsendgeräts der vorliegenden Ausführungsform. Ein Feld 421 gibt einen Betrieb auf der Seite des Informationslieferungs-Servers an. Ein OTP (Einmalpasswort) wird aus einer Passphrase, die ein gemeinsamer Schlüssel ist, der mit einer Empfangsseite geteilt wird, und Zeitinformationen erzeugt. Daher kann gesagt werden, dass das OTP der „MAC-Authentifizierungswert der Zeitinformationen“ ist. Anschließend wird der gesamte MAC-Wert aus dem OTP, den Lieferinformationen und der Passphrase mit Hilfe einer Hash-Funktion berechnet.

[0067] Ein Feld 422 gibt Daten an, die über den Übertragungsweg der Lieferinformationen in der vorliegenden Ausführungsform übertragen werden. Das heißt, auf dem Übertragungsweg werden drei Werte des OTP, der Lieferinformationen und des MAC-Werts als Satz übertragen. Anders als bei der herkömmlichen digitalen Signatur besteht, da das OTP die Zeitinformationen enthält, der Vorteil, dass der Wiedereinspielungsangriff detektiert werden kann.

[0068] Ein Feld 423 gibt eine Verarbeitung auf der Seite des Empfangsendgeräts an. Zuerst berechnet das Empfangsendgerät ein OTP aus einer Zeit und einer Passphrase, die aus einem mit einem Servertakt synchronisierten Takt erhalten werden. Wenn das berechnete OTP und das empfangene OTP unterschiedlich sind, sind der Server und die Passphrase unterschiedlich und die Lieferinformationen werden verworfen, ohne empfangen zu werden, da das Ziel der Lieferinformationen möglicherweise nicht dieses Empfangsendgerät ist oder sie möglicherweise einem Wiederholungsangriff ausgesetzt sind. Die obige Prozedur 424 ist eine Funktion des OTP-Abgleichs-Chips 110, der eine Grundkonfiguration der vorliegenden Ausführungsform ist.

[0069] Wenn andererseits das berechnete OTP mit dem empfangenen OTP übereinstimmt, wird der MAC-Wert aus dem OTP, den Lieferinformationen und der Passphrase unter Verwendung der Hash-Funktion berechnet. Wenn der berechnete MAC-Wert mit dem empfangenen MAC-Wert übereinstimmt, wird er als OK bestimmt, da die Informationen korrekt übertragen wurden, und wenn der berechnete MAC-Wert nicht mit dem empfangenen MAC-Wert übereinstimmt, wird er als NIO bestimmt, da ein Verlust oder eine Verfälschung der Informationen aufgetreten ist. Die in der Prozedur 424 enthaltene Hash-Funktion kann als die Hash-Funktion verwendet werden, die verwendet wird, um den MAC-Wert zu erzeugen. Auf diese Weise können die vorhandenen Rechenbetriebsmittel anderweitig genutzt werden und eine Kostensteigerung kann unterdrückt werden.

[0070] Wie es oben beschrieben ist, kann in dem Verfahren 420 der vorliegenden Ausführungsform als Grundfähigkeit der Wiedereinspielungsangriff immer detektiert werden. Wenn außerdem die Rechenaufwände auf der Seite des Empfangsendgeräts durch beide Verfahren verglichen werden und die Größe des Rechenaufwands durch ein Ungleichheitszeichen ausgedrückt wird, ist im Allgemeinen das Folgende erfüllt,

[0071] Entschlüsselungsverarbeitung der Verschlüsselung mit öffentlichem Schlüssel » Hash-Funktion-Verarbeitung.

Deshalb ist

[0072] Digitale Signatur (einmal Entschlüsselung der Verschlüsselung mit öffentlichem Schlüssel + Hash-Funktion) >> Vorliegendes Beispiel (Hash-Funktion zweimal)
erfüllt und somit ist das Verfahren 420 dieses Beispiels sehr viel geringer im Ausmaß.

[0073] Daher kann die Verarbeitung durch eine kostengünstige CPU mit einer geringen Rechenleistung ausgeführt werden und die Operation des MAC-Authentifizierungswerts und die Vergleichsverarbeitung können zusätzlich sogar wie in der vorliegenden Ausführungsform in dem OTP-Abgleichs-Chip 110 implementiert werden. Dies macht es auch möglich, eine Erhöhung der Herstellungskosten zum Erweitern des OTP-Abgleichs-Chips 110 zu unterdrücken.

[0074] Beim Empfangen der Menge von Werten 422 auf dem Übertragungsweg 401 in **Fig. 4**, das heißt, des OTP, der Lieferinformationen 310 und des MAC-Werts, speichert die Host-CPU 210 in **Fig. 3** die jeweiligen Werte in dem Empfangs-OTP-Puffer 204, dem Lieferinformations-Di-Puffer 301 und dem Empfangs-MAC-Wertpuffer 302 innerhalb des erweiterten OTP-Abgleichs-Chips 300 über den Kommunika-

tionsweg 211. Danach gibt die Host-CPU 210 ebenso eine Lieferinformation-Verifizierungsanforderung (nicht dargestellt) über den Kommunikationsweg 211 an den erweiterten OTP-Abgleichs-Chip 300 aus.

[0075] **Fig. 5** ist ein Ablaufdiagramm, das die Lieferinformations-Verifizierungsverarbeitung S500 der ersten Ausführungsform darstellt.

[0076] Bei der Bestimmung S501 bestimmt der OTP-Abgleichs-Chip 300, ob die Verifizierungsanforderung der Lieferinformationen von der Host-CPU 210 empfangen wurde. Wenn die Verifizierungsanforderung der Lieferinformationen empfangen wurde, geht der Prozess zu Schritt S502 über. Wenn die Verifizierungsanforderung der Lieferinformationen nicht empfangen wurde, geht der Prozess zu Schritt S509 über und die Lieferinformations-Verifizierungsverarbeitung endet.

[0077] In Schritt S502 bezieht sich der OTP-Abgleichs-Chip 300 auf eine eingebaute Taktvorrichtung. Die Zeit, zu der der Empfang des OTP beginnt, wird in einem spezifischen Register Reg(Zeit) der eingebauten Taktvorrichtung erfasst und die Zeit wird auf die variable Zeit gesetzt. Die Notwendigkeit der Zeiterfassungsfunktion wird später unter Bezugnahme auf **Fig. 6** beschrieben.

[0078] In Schritt S503 berechnet der OTP-Abgleichs-Chip 300 ein OTP zum Vergleich. Ein Symbol U in der Zeichnung stellt eine Datenkombination dar und bedeutet eine Kombination der Zeitinformationszeit und der Passphrase auf Daten*Strom-Weise. Das Format der Zeitinformationen und das Kombinationsverfahren (Ordnung oder dergleichen) mit der Passphrase werden mit der Seite des Informationslieferungs-Servers vereinheitlicht.

[0079] Bei dem Bestimmungsschritt S504 vergleicht der OTP-Abgleichs-Chip 300 das empfangene OTP mit dem intern berechneten OTP. Wenn die OTPs übereinstimmen, fährt der Prozess als Ergebnis des Vergleichs mit dem nächsten Schritt S505 fort, und wenn die OTPs nicht übereinstimmen, wird dies als das Bestimmungsergebnis NIO in Schritt S508 bestimmt, der Prozess fährt mit Schritt S509 fort und die Lieferinformations-Verifizierungsverarbeitung endet.

[0080] In Schritt S505 berechnet der OTP-Abgleichs-Chip 300 unabhängig den MAC-Wert der Empfangsinformationen. Wie in Schritt S503 stellt ein Symbol U in der Zeichnung eine Datenkombination dar. Genauso wie in Schritt S503 werden die drei Kombinationsverfahren auf Daten-Strom-Weise (Ordnung und dergleichen) des empfangenen OTP-Inhalts (OTP-Puffer), des empfangenen Lieferinformationsinhalts (DI-Puffer) und der Passphrase auf der Seite des Informationslieferungs-Servers vereinheitlicht (hier ist der Name des Speicherbereichs in Klammern () eingeschlossen, um den Inhalt des Speicherbereichs anzugeben. Das Gleiche gilt im Folgenden).

[0081] Bei dem Bestimmungsschritt S506 vergleicht der OTP-Abgleichs-Chip 300 den empfangenen MAC-Wert mit dem unabhängig berechneten MAC-Wert. Als Ergebnis des Vergleichs bestimmt dann, wenn die MAC-Werte miteinander übereinstimmen, der nächste Schritt S507, dass das Bestimmungsergebnis OK ist, und der Prozess fährt mit Schritt S509 fort, um die Lieferinformations-Verifizierungsverarbeitung zu beenden. Wenn andererseits die MAC-Werte nicht übereinstimmen, wird in Schritt S508 bestimmt, dass das Bestimmungsergebnis NIO ist und der Prozess fährt mit Schritt S509 fort, um die Lieferinformations-Verifizierungsverarbeitung zu beenden.

[0082] Die Informationen des Bestimmungsergebnisses OK in Schritt S507 und die Informationen des Bestimmungsergebnisses NG in Schritt S508 werden an das Bestimmungsergebnisregister 206 in **Fig. 3** gesendet und der Host-CPU 210 über den Kommunikationsweg 212 mitgeteilt.

[0083] Die von der Host-CPU 210 ausgegebene Lieferinformations-Verifizierungsanforderung (nicht dargestellt) wird vorzugsweise ausgegeben, nachdem die Übertragung der Menge aus dem Empfangs-OTP-Puffer 204, dem Lieferinformations-DI-Puffer 301 und dem Empfangs-MAC-Wert-Puffer 302 abgeschlossen ist. Um jedoch den Durchsatz zu verbessern, kann die Lieferinformations-Verifizierungsanforderung unmittelbar nach Ankunft des Datenkopfes des Empfangs-OTP an dem OTP-Abgleichs-Chip 300 ausgegeben werden. In diesem Fall kann die Bereitschaftsverarbeitung bis zum Abschluss der Übertragung des Empfangs-OTP-Puffers 204 unmittelbar vor dem Vergleich (S504) des OTP hinzugefügt werden, die Bereitschaftsverarbeitung bis zum Abschluss der Übertragung des Lieferinformations-Di-Puffers 301 unmittelbar vor der Vergleichs-MAC-Wert-Berechnung hinzugefügt werden (S505) und die Bereitschaftsverarbeitung bis zum Abschluss der Übertragung des Empfangs-MAC-Wert-Puffers 302 unmittelbar vor dem MAC-Wert-Vergleich hinzugefügt werden (S506).

[0084] **Fig. 6** ist ein Zeitdiagramm, das eine Referenz einer Zeit des OTP bei der Informationsübertragung von dem Server zu dem Empfangsendgerät darstellt.

[0085] Abschließend wird eine Reihe von Informationen mit dem OTP an der Spitze zu einem Kommunikationsweg 610 übertragen und die Kopfzeit, zu der die Übertragung des OTP beginnt, wird als Referenz-

zeit der OTP-Erzeugung festgelegt. Dadurch soll vermieden werden, dass die Wechselzeit des OTP-Werts überschritten wird, wenn die gesamte Übertragungszeit der Reihe von Informationen lang ist.

[0086] In **Fig. 6** sind eine Intra-Server-Verarbeitung 600, ein Kommunikationsweg 610 und eine Intra-OTP-Chip-Verarbeitung 620 in parallelen Zeitkoordinaten von oben dargestellt. In der Zeichnung vergeht die Zeit von links nach rechts.

[0087] Bei der Intra-Server-Verarbeitung 600 wird das OTP unter Bezugnahme auf eine geplante Zeit 630 berechnet, zu der die Übertragung der Reihe von Informationen an den Kommunikationsweg 610 beginnt (Prozess 601).

[0088] Wenn die geplante Zeit 630 erreicht wird, beginnt die Übertragung des OTP 611 an den Kommunikationsweg 610.

[0089] Anschließend werden bei der Intra-Server-Verarbeitung 600 Lieferinformationen konfiguriert (Prozess 602) und die konfigurierten Lieferinformationen 612 werden an den Kommunikationsweg 610 übertragen.

[0090] Anschließend wird bei der Intra-Server-Verarbeitung 600 ein MAC-Wert aus dem OTP und den Lieferinformationen berechnet (Prozess 603) und der berechnete MAC-Wert 613 wird an den Kommunikationsweg 610 übertragen.

[0091] Bei der Intra-OTP-Chip-Verarbeitung 620 werden das OTP 611, die Lieferinformationen 612 und der MAC-Wert 613, die über den Kommunikationsweg 610 übertragen werden, jeweils in dem OTP-Empfangspuffer 204 gespeichert (621), in dem Lieferinformations-DI-Puffer 301 gespeichert (622) und in dem Empfangs-MAC-Wertpuffer 302 gespeichert (623).

[0092] Bei der Intra-OTP-Chip-Verarbeitung 620 kann, wenn das OTP 611 ankommt, der Vergleichs-OTP-Berechnungsprozess 632 aktiviert werden. Bei dem Vergleichs-OTP-Berechnungsprozess 632 wird die Zeit erfasst, zu der der Empfang des OTP gestartet wird, und das Vergleichs-OTP wird berechnet, aber aufgrund der Verzögerung des Kommunikationswegs 610 und der Verzögerung der Informationsübertragung durch die Host-CPU 210 tritt eine geringfügige Zeitverzögerung Δt (631) auf. Da jedoch die Zeitverzögerung Δt (631) ausreichend kleiner als die Wechselzeit des OTP ist, kann der Einfluss davon ignoriert werden.

[0093] Wenn das Speichern (621) des OTP 611 in dem Empfangs-OTP-Puffer 204 abgeschlossen ist und der Vergleichs-OTP-Berechnungsprozess 632 beendet ist, kann der OTP-Verifizierungsprozess 633 ausgeführt werden.

[0094] Wenn das Speichern (622) der Lieferinformationen 612 in dem Di-Puffer für empfangene Lieferinformationen abgeschlossen ist, kann der Vergleichs-MAC-Wert-Berechnungsprozess 634 ausgeführt werden.

[0095] Wenn das Speichern (623) des MAC-Werts 613 in dem Empfangs-MAC-Wert-Puffer 302 abgeschlossen ist und der Vergleichs-MAC-Wert-Berechnungsprozess 634 abgeschlossen ist, kann eine Verifizierung der gesamten Lieferinformationen (Vergleich zwischen dem empfangenen MAC-Wert und dem unabhängig berechneten Vergleichs-MAC-Wert) durch den MAC-Wert-Verifizierungsprozess 635 ausgeführt werden.

[0096] Obwohl der Bereich der MAC-Authentifizierung als eine Kombination aus dem OTP und den Lieferinformationen beschrieben wurde, kann das OTP in einer bestimmten Anwendung aus dem Bereich der MAC-Authentifizierung ausgeschlossen und auf die Lieferinformationen beschränkt werden. Dies entspricht dem „Öffnen“ des Wechselschalters 303 im Blockdiagramm von **Fig. 3**. Ferner wird in dem Verarbeitungsablaufdiagramm von **Fig. 5** entspricht die Vergleichs-MAC-Wertberechnung in Schritt S505 Folgendem:

$$\mathrm{MAC\_Ref} = \mathrm{Hash}\left(\left(\mathrm{DI\text{-}Puffer}\right)\mathrm{U\ Passphrase}\right).$$

[0097] Im Ergebnis spiegelt sich die Verbindung zwischen dem OTP und den Lieferinformationen nicht in dem MAC-Wert wider und die OTP-Berechnung und die MAC-Wert-Berechnung können als unabhängige Prozesse behandelt werden. Ein Zeitdiagramm von **Fig. 7** zeigt Vor- und Nachteile, die mit dieser Änderung verbunden sind.

[0098] In **Fig. 7** sind von oben eine Intra-Server-Verarbeitung 700, eine Serverausgabe 710 , eine Ausgabe 720 eines Person-in-der-Mitte-Angriffs, bei dem ein Kommunikationsweg durch Unterbrechung zwischen dem Server und dem Empfangsendgerät verfälscht wird, und eine Erkennung 730 des OTP-Chips in parallelen Zeitkoordinaten dargestellt. In der Zeichnung läuft die Zeit von links nach rechts.

[0099] Es wird ein Fall betrachtet, in dem Lieferinformationen X beginnend zu dem Zeitpunkt t1 (740) und Lieferinformationen Y beginnend zu dem Zeitpunkt t2 (741) in der Intra-Server-Verarbeitung 700 übertragen werden.

[0100] Wie es dargestellt ist, können der Berechnungsprozess 701 des OTP (t1), die Konfiguration der Lieferinformationen X und die Berechnungsprozesse 702 und 703 von MAC (X) unabhängig parallel

ausgeführt werden. Ebenso können der Berechnungsprozess 704 des OTP (t2), die Konfiguration der Lieferinformationen Y und die Berechnungsprozesse 705 und 706 von MAC (Y) unabhängig parallel ausgeführt werden.

[0101] Daher ist die Verbesserung des Durchsatzes durch den parallelen Prozess vorteilhaft für den Informationslieferungs-Server, der unterschiedliche Lieferinformationen an verschiedene Endgeräte sendet.

[0102] Da das OTP, die Lieferinformationen und der MAC-Wert jedoch getrennt sind, besteht auch der Nachteil, dass die Gefahr besteht, einen Person-in-der-Mitte-Angriff zu empfangen. Nachfolgend wird dieser Nachteil beschrieben.

[0103] Die Serverausgaben 710 sind in der Reihenfolge OTP(t1) (711) - Lieferinformationen X (712) - MAC(X) (713) mit der Zeit t1 (740) als Startpunkt angeordnet. Ferner sind OTP(t2) (714) - die Lieferinformationen Y (715) - MAC(Y) (716) in dieser Reihenfolge beginnend mit der Zeit t2 (741) als Startpunkt angeordnet. In der Beschreibung von **Fig. 7** ist ein Symbol „-“ ein Verbindungssymbol, das eine Sequenz einer Datenanordnung darstellt.

[0104] Bei dem Person-in-der-Mitte-Angriff kann ein Angriff ausgeführt werden, bei dem ein Satz aus den Lieferinformationen X (712) und dem MAC(X) (713) als Ausgabe 720 gespeichert wird und nachfolgende Daten zu dem Zeitpunkt eines anderen OTP-Kopfstücks OTP(t2) (714) mit den Lieferinformationen X (712) anstelle der Lieferinformationen Y (715) umgeschrieben werden (721) und umzuschreibende Daten (722) mit dem MAC(X) (713) anstelle des MAC(Y) (716) gesendet werden. Die von dem Server gesendeten Informationslieferinformationen Y (715) und MAC(Y) (716) gehen in der Mitte des Kommunikationswegs verloren.

[0105] Bei der Erkennungsverarbeitung des OTP-Chips kommen Daten, die in der Reihenfolge OTP (t1) (711) - die Lieferinformationen X (712) - MAC (X) (713) angeordnet sind, und Daten, die in der Reihenfolge OTP (t2) (714) - die Lieferinformationen X (712) -MAC(X) (713) angeordnet sind. aus dem Server an und eine Kombination der Lieferinformationen und des MAC-Werts wird abgeglichen, so dass eine Fälschung nicht detektiert werden kann. Mit anderen Worten wird bei diesem Person-in-der-Mitte-Angriff der Wiedereinspielungsangriff der Lieferinformationen X (712) - MAC(X) (713) durchgeführt. Denn wenn unter dem zeitrichtigen OPT-Kopfstück das Paar aus Lieferinformationen und dem richtigen MAC-Wert angehängt ist, werden die Informationen widerspruchsfrei akzeptiert.

[0106] Wie es oben beschrieben ist, wurde ein weiteres Verfahren mit einem anderen MAC-Authentifizierungsbereich beispielhaft dargestellt, aber es ist wichtig unter Berücksichtigung der oben beschriebenen Vorteile und Risiken zu bestimmen, ob das Verfahren angewendet werden soll.

<Zweite Ausführungsform>

[0107] **Fig. 8** ist ein Blockdiagramm, das Einzelheiten des erweiterten OTP-Abgleichs-Chips 300 gemäß einer zweiten Ausführungsform der vorliegenden Erfindung darstellt. In der zweiten Ausführungsform wird der OTP-Abgleichs-Chip so erweitert, dass er der Verschlüsselung mit gemeinsamem Schlüssel der Lieferinformationen entspricht. Diese Erweiterung kann das Durchsickern von Lieferinformationen durch Abhören verhindern.

[0108] Ein Unterschied zwischen der Konfiguration in **Fig. 8** und der Konfiguration in **Fig. 3** besteht darin, dass ein Puffer für entschlüsselte Daten 802 zum Senden der entschlüsselten Lieferinformationen an die Host-CPU 210 hinzugefügt ist. Die Host-CPU 210 kann die entschlüsselten Lieferinformationen über den Kommunikationsweg 212 erfassen.

[0109] In einem Fall, in dem die Authentizität der Lieferinformationen bestätigt wird, das heißt in einem Fall, in dem die UND-Logik 306 mit der OTP-Koinzidenz und der MAC-Wert-Koinzidenz aktiv ist, wird eine Verschlüsselungs-Entschlüsselungs-Einheit 801 aktiv. Die Verschlüsselungs-Entschlüsselungs-Einheit 801 entschlüsselt den Inhalt des Lieferungsinformations-Di-Puffers 301 unter Verwendung der Passphrase, die in dem Passphrasenspeicher 202 als ein gemeinsamer Schlüssel gespeichert ist, und sendet den entschlüsselten Inhalt an den Puffer für entschlüsselte Daten 802.

[0110] In der obigen Beschreibung wurden alle gemeinsamen Schlüssel, deren Kenntnis mit dem Informationslieferungs-Server geteilt wird, als die Passphrasen beschrieben, aber die gemeinsamen Schlüssel sind nicht auf die gleichen Schlüssel beschränkt. Das heißt, der gemeinsame Schlüssel zum Erzeugen des OTP, der gemeinsame Schlüssel zum Erzeugen des MAC-Werts und der gemeinsame Schlüssel zum Verschlüsseln und Entschlüsseln der Lieferinformationen können jeweils als separate Schlüssel verwendet werden und können durch mehrere individuelle Schlüssel ausgebildet sein. Im Fall von mehreren individuellen Schlüsseln wird die Kenntnis jedes Schlüssels selbstverständlich mit dem Informationslieferungs-Server für jede Anwendung geteilt und der Schlüssel wird in dem erweiterten OTP-Abgleichs-Chip 300 in dem Passphrasenspeicher 202 mit ausgezeichneter Manipulationssicherheit gespeichert.

[0111] **Fig. 9** ist ein Ablaufdiagramm, das die Lieferinformations-Verifizierungsverarbeitung S500 der zweiten Ausführungsform darstellt.

[0112] Der Unterschied zwischen dem Verarbeitungsablauf der zweiten Ausführungsform und dem Verarbeitungsablauf der ersten Ausführungsform (**Fig. 5** , bei dem die Lieferinformationen nicht der Verschlüsselung mit gemeinsamem Schlüssel unterzogen werden, besteht darin, dass „Schritt S901: Lieferdaten entschlüsseln“ und „Schritt S902: entschlüsselte Daten im Puffer 802 für entschlüsselte Daten speichern“ in einem Fall, in dem das Bestimmungsergebnis in Schritt 507 OK ist, hinzugefügt werden.

[0113] Die zweite Ausführungsform gleicht der ersten Ausführungsform darin, dass das Bestimmungsergebnis in Schritt S507 OK ist, wenn der MAC-Wert verglichen wird und in der Bestimmung S506 bestimmt wird, dass keine Fälschung in den Lieferinformationen gefunden wird, aber die Lieferdaten werden in der zweiten Ausführungsform in Schritt S901 entschlüsselt, nachdem das Bestimmungsergebnis OK ist.

[0114] In dem Verarbeitungsablauf von **Fig. 9** wird die Passphrase in den folgenden drei Schritten verwendet. Es gibt die drei Schritte „Schritt S503: Vergleichs-OTP-Berechnung“, „Schritt S506: Vergleichs-MAC-Wert-Berechnung“ und „Schritt S901: Lieferdaten entschlüsseln". Wie es oben beschrieben ist, kann die gleiche Passphrase verwendet werden oder es kann für jede Verwendung eine andere Passphrase verwendet werden.

[0115] In dem nachfolgenden Schritt S902 werden die entschlüsselten Daten (Entschl_Daten) an den Puffer für entschlüsselte Daten 802 gesendet und der Prozess endet in Schritt S509.

[0116] Wie oben beschrieben ist, können in der zweiten Ausführungsform die Lieferinformationen durch das Verschlüsselungssystem mit gemeinsamem Schlüssel mit einem geringeren Rechenaufwand als bei der Verschlüsselung mit öffentlichem Schlüssel leicht verschlüsselt werden und ein Abhören kann verhindert werden.

<Dritte Ausführungsform>

[0117] **Fig. 10** ist ein Blockdiagramm, das Einzelheiten des erweiterten OTP-Abgleichs-Chips 300 gemäß der dritten Ausführungsform der vorliegenden Erfindung darstellt. In der dritten Ausführungsform wird der OTP-Abgleichs-Chip weiter erweitert, so dass er der Verschlüsselung mit gemeinsamem Schlüssel der Lieferinformationen entspricht. Mit dem erweiterten OTP-Abgleichs-Chip der dritten Ausführungsform sind die Lieferinformationen so konfiguriert, dass sie sowohl als Lieferinformationen für die Host-CPU 210 als auch als Lieferinformationen für den OTP-Abgleichs-Chip dienen, und Informationen für unterschiedliche Verwendungen können durch das gleiche Protokoll gänzlich geliefert werden.

[0118] Die Verschlüsselung mit gemeinsamem Schlüssel ist für Lieferinformationen für den OTP-Abgleichs-Chip wesentlich und der Lieferinhalt müssen vor Abhören geschützt werden. Außerdem besteht das Risiko eines Informationslecks, bei dem der Lieferinhalt für den entschlüsselten OTP-Abgleichs-Chip der Host-CPU 210 über den Puffer für entschlüsselte Daten 802 offengelegt wird, was vermieden werden sollte.

[0119] Ein Unterschied zwischen der Konfiguration der dritten Ausführungsform in **Fig. 10** und der Konfiguration der zweiten Ausführungsform in **Fig. 8** besteht darin, dass eine Befehlsinterpretationseinheit 1001 und ein bidirektionaler Daten-Wechselschalter 1002 hinzugefügt sind.

[0120] Ein Befehl, der angibt, ob die Lieferinformationen für die Host-CPU 210 oder den OTP-Abgleichs-Chip 300 sind, ist in den Lieferinformationen gespeichert. Die Befehlsinterpretationseinheit 1001 schaltet den Wechselschalter 1002 gemäß dem aus den entschlüsselten Lieferinformationen extrahierten Befehl um. Wenn die Lieferinformationen beispielsweise für die Host-CPU 210 sind, werden die entschlüsselten Daten wie in der zweiten Ausführungsform, die in **Fig. 8** dargestellt ist, an den Puffer für entschlüsselte Daten 802 gesendet. Wenn andererseits die Lieferinformationen für den OTP-Abgleichs-Chip 300 sind, wird der bidirektionale Daten-Wechselschalter 1002 umgeschaltet und die entschlüsselten Daten werden direkt an die Steuereinheit 200 und nicht an den Puffer für entschlüsselte Daten 802 gesendet. Beispiele der Daten für den OTP-Abgleichs-Chip umfassen Zeitabgleichsinformationen der Takteinheit 201 und Passphrasen-Aktualisierungsinformationen des Passphrasenspeichers 202.

[0121] Bei der Aktualisierung der Passphrase wird der gemeinsame Schlüssel, der von dem Informationslieferungs-Server geliefert wird, vorübergehend verwendet, ohne den Anfangsschlüssel, der zu dem Zeitpunkt der Herstellung des OTP-Abgleichs-Chips in einem gespeicherten Zustand festgelegt wird, zu verwenden. Der Grund, warum der Anfangsschlüssel gespeichert wird, ist, dass dann, wenn ein Fehler auftritt oder wenn der OTP-Abgleichs-Chip 300 auf den Ursprung zurückgesetzt wird, die Rückkehr zu dem Anfangsschlüssel als System robuster ist.

[0122] Die vorübergehend aktualisierte Passphrase wird in den Lieferinformationsdaten gespeichert und

an den OTP-Abgleichs-Chip 300 gesendet. Da jedoch, wie es oben beschrieben ist, der gemeinsame Schlüssel mit dem Anfangsschlüssel verschlüsselt ist, ist das Risiko eines Durchsickerns der aktualisierten Passphrase gering und er ist ausreichend sicher, auch wenn der Schlüssel über das Internet geliefert wird.

[0123] **Fig. 11** ist ein Ablaufdiagramm, das die Lieferinformations-Verifizierungsverarbeitung S500 der dritten Ausführungsform darstellt.

[0124] Der Unterschied zwischen dem Verarbeitungsablauf der dritten Ausführungsform und dem Verarbeitungsablauf der ersten Ausführungsform (**Fig. 5**) besteht darin, dass die Verarbeitungsschritte S901, S902und S1101 bis S1106 hinzugefügt sind, und der Unterschied zum Verarbeitungsablauf der zweiten Ausführungsform (**Fig. 9**) besteht darin, dass die Verarbeitungsschritte S1101 bis S1106 hinzugefügt sind.

[0125] Wenn der MAC-Wert verglichen wird und in Bestimmung S506 bestimmt wird, dass keine Fälschung in den Lieferinformationen vorliegt, ist ein Bestimmungsergebnis in Schritt S507 OK und die Lieferdaten werden in nachfolgendem Schritt S901, der der gleiche ist wie in der zweiten Ausführungsform, entschlüsselt. Danach wird bestimmt, ob die Lieferinformationen für die Host-CPU 210 oder den OTP-Abgleichs-Chip 300 bestimmt sind (S1101).

[0126] Die entschlüsselten Lieferinformationen enthalten einen Befehl für die Host-CPU 210 oder den OTP-Abgleichs-Chip 300 und die Verarbeitung wird basierend auf dem Befehl umgeschaltet. Dieser Mechanismus umfasst die Befehlsinterpretationseinheit 1001 und den Wechselschalter 1002 in dem Blockdiagramm (**Fig. 10**).

[0127] Wenn die Lieferinformationen für die Host-CPU 210 bestimmt sind, werden die in Schritt S902entschlüsselten Daten Entschl_Daten) an den Puffer für entschlüsselte Daten 802 gesendet und der Prozess endet in Schritt S509. Dieser Prozess ist der gleiche wie der der zweiten Ausführungsform.

[0128] Wenn hingegen die Lieferinformationen für den OTP-Abgleichs-Chip bestimmt sind, wird die Verarbeitung von S1102 bis S1106 ausgeführt.

[0129] Zuerst wird bestimmt, ob es sich bei den Lieferinformationen um einen Zeitaktualisierungsbefehl handelt (S1102). Wenn es sich bei den Lieferinformationen um den Zeitaktualisierungsbefehl handelt, wird eine Systemfunktion Zeiteinst() unter Verwendung eines Zeitaktualisierungswerts Zeit_ern in den Lieferinformationen als Argument aufgerufen, um die aktuelle Zeit der Taktvorrichtung zu ändern (Schritt 1103). Danach endet der Prozess in Schritt 509.

[0130] Wenn es sich bei den Lieferinformationen nicht um den Zeitaktualisierungsbefehl handelt, wird bestimmt, ob es sich bei den Lieferinformationen um einen Passphrasenaktualisierungsbefehl handelt (S1104) und ob eine Aktualisierungszielvorrichtungs-ID (IDentifizierung: Kennung) der Lieferinformationen übereinstimmt (S1105). Wenn es sich bei den Lieferinformationen nicht um den Passphrase-Aktualisierungsbefehl handelt oder die Aktualisierungszielvorrichtungs-ID nicht übereinstimmt, endet der Prozess in Schritt S509.

[0131] Wenn es sich bei den Übermittlungsinformationen um den Passphrasenaktualisierungsbefehl handelt und die Aktualisierungszielvorrichtungs-ID übereinstimmt, wird ein Passphrasenaktualisierungsmerker, der ein Ereignismerker ist, auf „1“ gesetzt, eine Aktualisierungseinstellungszeit wird aus den Lieferinformationen extrahiert und auf eine Systemvariable Zeit_änd gesetzt, die Aktualisierungs-Passphrase wird aus den Lieferinformationen extrahiert und auf eine Systemvariable Pp_neu gesetzt und der Prozess endet in Schritt S509.

[0132] Tatsächlich wird die Aktualisierung der Passphrase in der Festzeit-Unterbrechungsverarbeitung S1200 zur Zeitaktualisierung, die in **Fig. 12** dargestellt ist, ausgeführt. **Fig. 12** ist ein Ablaufdiagramm der Festzeit-Unterbrechungsverarbeitung, die durch den erweiterten OTP-Abgleichs-Chip 300 ausgeführt wird. Die Festzeit-Unterbrechungsverarbeitung ist eine Unterbrechungsverarbeitung der Steuereinheit 200, die jedes Mal zyklisch mit einer vorbestimmten Zeitauflösung aktiviert wird und eine Verwaltungsaufgabe durchführt.

[0133] Es wird bestimmt, ob der Merker zum Aktualisieren der Passphrase gesetzt wurde (ob der Wert 1 ist) (S1201). Wenn der Merker zum Aktualisieren der Passphrase nicht gesetzt wurde, ist kein Ereignis aufgetreten, und somit endet der Prozess in Schritt 1206, ohne dass irgendetwas ausgeführt wird.

[0134] Wenn der Merker zum Aktualisieren der Passphrase gesetzt ist (wenn der Wert 1 ist), tritt ein Passphrasenaktualisierungsereignis auf. Daher wird die aktuelle Zeit (der Inhalt von Regjetzt) unter Bezugnahme auf die Taktvorrichtung in die Variable Zeit eingegeben (S1202). Anschließend wird bestimmt, ob die aktuelle Zeit Zeit die Aktualisierungseinstellungszeit Zeit_änd überschritten hat (S1203). Wenn die aktuelle Zeit Zeit die Aktualisierungseinstellungszeit Zeit_änd überschritten hat, fährt der Prozess im Ergebnis mit Schritt 1204 fort. Wenn die aktuelle Zeit Zeit die Aktualisierungseinstellzeit Zeit_änd nicht überschritten hat, endet der Prozess in Schritt 1206, ohne dass irgendetwas ausgeführt wird.

[0135] In Schritt 1204 wird die aktualisierte Passphrase Pp_neu an den Passphrasenspeicher 202 gesendet und als Änderungswert der vergangenen Passphrase gesetzt. Anschließend wird in Schritt S1205 der Passphrasenaktualisierungsmerker gelöscht (auf „0“ gesetzt) und der Prozess endet in Schritt S1206.

[0136] Fig. 13 ist eine Darstellung, die eine Empfangsvorrichtungsgruppe zeigt, die einen Empfangs-Cluster unter Verwendung der oben beschriebenen Passphrasenänderungsfunktion dynamisch vergrößert oder verkleinert.

[0137] Wenn die Passphrase bestimmt wird, wird zu einem Zeitpunkt in der globalen Zeit nur ein OTP bestimmt. Daher wird dann, wenn der Informationslieferungs-Server 1300 ein OTP auswählt, nur ein Ziel bestimmt. Daher kann man sagen, dass die Passphrase eine Funktion der Zielauswahl (Adressierung) hat. Daher kann durch vorläufiges Zuweisen der gleichen Passphrase zu mehreren Empfangsendgeräten ein Empfangs-Cluster durch die mehreren Empfangsendgerätgruppen gebildet werden. Der Informationslieferungs-Server 1300 kann Lieferinformationen kollektiv gleichzeitig an dieses Empfangs-Cluster aussenden und kann die Informationen effizient liefern.

[0138] Der Zustand 1301 gibt eine Empfangsvorrichtungsgruppe an, die die Passphrase des Anfangsschlüssels aufweist, und die Zahl in dem Kreis gibt die individuelle ID des Empfängers an, das heißt die Identifikationsnummer der festgelegten Passphrase.

[0139] Der Zustand 1302 ist ein Zustand, in dem die Zeit t1 seit dem Zustand 1301 verstrichen ist. Unter Verwendung der oben beschriebenen Passphrasenaktualisierungsfunktion wird den Endgeräten 3, 5 und 6 eine vorläufige Passphrase 0 gegeben, um den Empfangs-Cluster 1310 zu bilden. Der Informationslieferungs-Server 1300 kann die Lieferinformationen gemeinsam an die Endgeräte des Empfangs-Clusters 1310 aussenden.

[0140] Der Zustand 1303 ist ein Zustand, in dem die Zeit t2 seit dem Zustand 1302 verstrichen ist. Unter erneuter Verwendung der oben beschriebenen Passphrasenaktualisierungsfunktion wird die vorläufige Passphrase des Endgeräts 0, das ursprünglich das Endgerät 6 war, in dem Empfangs-Cluster 1310 freigegeben und zu dem Anfangsschlüssel 6 zurückgeführt. Daher ist der Empfangs-Cluster 1311 kleiner als der Empfangs-Cluster 1310.

[0141] Wie es oben beschrieben ist, kann in der dritten Ausführungsform der Empfangs-Cluster unter Verwendung der Passphrasenaktualisierungsfunktion vergrößert oder verkleinert werden und Informationen können effizient geliefert werden.

[0142] Wie es oben in der ersten Ausführungsform, der zweiten Ausführungsform und der dritten Ausführungsform beschrieben ist, ist es gemäß den in der vorliegenden Beschreibung offenbarten Mitteln möglich, die Lieferinformationen zu verifizieren, ohne ein als digitale Signatur bezeichnetes Verfahren zu verwenden, das eine große Menge an Betriebsmitteln verbraucht, ist es möglich, die Verifizierung in einem kostengünstigen OTP-Abgleichs-Chip mit geringer Verarbeitungsfähigkeit auszuführen, und ist es möglich, einen hochzuverlässigen Informationsliefermechanismus zu realisieren.

[0143] Zusätzlich kann auch der Parameter des OTP-Abgleichs-Chips selbst von dem Server als Lieferinformationen geliefert und geändert werden. Basierend auf diesem Mechanismus können Empfangs-Cluster des gleichen Ziels dynamisch und einfach gebildet und eliminiert werden. Das heißt, die gleichen Informationen können gleichzeitig von dem Informationslieferungs-Server an die in demselben Empfangs-Cluster positionierten Vorrichtungen gesendet und geliefert werden und ein Mechanismus, der an Über-die-Luft (OTA) angepasst ist, wie z. B. fahrzeuginterne Vorrichtungen und IoT-Vorrichtungen, kann bereitgestellt sein.

[0144] Wie es oben beschrieben ist, werden dann, wenn mindestens drei von dem Einmalpasswort, das aus der Informationsübertragungsquelle (dem Informationslieferungs-Server 1300) gesendet wird und durch die synchronisierte Zeit und den gemeinsamen Schlüssel erzeugt wird, den Lieferinformationen, die aus der Informationsübertragungsquelle gesendet werden und ein anderer Nutzungswert neben der Authentifizierung haben, und dem Nachrichtenauthentifizierungscode (MAC-Wert), der aus der Informationsübertragungsquelle gesendet wird und unter Verwendung des gemeinsamen Schlüssels aus diesen Informationselementen berechnet wird, eingegeben werden, gibt die Informationsverifizierungsvorrichtung (OTP-Abgleichs-Chip 300) der vorliegenden Ausführungsform zumindest das Bestimmungsergebnis der Authentizität der Lieferinformationen aus. Daher kann die Fälschung der Lieferinformationen detektiert werden und der Wiedereinspielungsangriff kann detektiert werden. Darüber hinaus ist es möglich, eine Fälschungsdetektion und Wiedereinspielungsangriff-Detektion der Lieferinformationen durch Abwandeln des vorhandenen OTP-Abgleichs-Chips und gleichzeitiges Beibehalten der Grundkonfiguration zu realisieren. Außerdem kann eine Kostenerhöhung aufgrund des Hinzufügens einer Funktion minimiert werden und ein Mehrwert des OTP-Abgleichs-Chips selbst kann verbessert werden. Das heißt, eine Kostenerhöhung kann dadurch minimiert werden, dass eine neu hinzuge-

fügte MAC-Authentifizierungsfunktion durch Abzweigen eines bestehenden Rechenbetriebsmittels (beispielsweise einer Hash-Funktion) realisiert werden kann.

[0145] Da außerdem die Verarbeitungslast gering ist, kann die Verifizierungsverarbeitung in dem OTP-Abgleichs-Chip ausgeführt werden, die Belastung der Host-CPU 210 wird nicht erhöht und sogar auf der Host-CPU 210 mit geringer Leistungsfähigkeit für fahrzeuginterne Anwendungen und IoT-Anwendungen kann die Fähigkeit zur Sicherheitshandhabung verbessern, ohne die ursprüngliche Verarbeitung zu beeinträchtigen.

[0146] Da der gemeinsame Schlüssel physisch verteilt wird, ohne über den Kommunikationsweg übertragen zu werden, kann außerdem das Abhörrisiko verringert werden, und selbst dann, wenn der gemeinsame Schlüssel auf die Informationsübermittlung über das Internet angewendet wird, ist der gemeinsame Schlüssel ausreichend sicher.

[0147] In einem Fall, in dem das aus der Informationsübertragungsquelle gesendete Einmalpasswort mit einem in der Informationsverifizierungsvorrichtung berechneten Einmalpasswort übereinstimmt und der aus der Informationsübertragungsquelle gesendete Nachrichtenauthentifizierungscode mit einem in der Informationsverifizierungsvorrichtung berechneten Nachrichtenauthentifizierungscode übereinstimm, wird bestimmt, dass die Lieferinformationen authentisch sind, und die Lieferinformationen sind authentisch. Daher kann die Fälschung der Lieferinformationen detektiert werden und der Wiedereinspielungsangriff detektiert werden

[0148] Außerdem ist das aus der Informationsübertragungsquelle gesendete Einmalpasswort ein Einmalpasswort vom Zeitsynchronisationstyp, das basierend auf einer Übertragungsstartzeit aus einer Reihe von Informationen erzeugt wird, die von der Informationsübertragungsquelle an die Informationsverifizierungsvorrichtung übertragen werden. Daher besteht keine Notwendigkeit, die Zeitunterbrechung zum Erzeugen des Einmalpassworts zu berücksichtigen und der Freiheitsgrad beim Entwerfen der Vorrichtung wird verbessert.

[0149] Außerdem wird der aus der Informationsübertragungsquelle gesendete Nachrichtenauthentifizierungscode unter Verwendung des gemeinsamen Schlüssels basierend auf dem aus der Informationsübertragungsquelle gesendeten Einmalpasswort und den aus der Informationsübertragungsquelle gesendeten Lieferinformationen berechnet. Daher ist es möglich, eine hohe Sicherheit zu realisieren.

[0150] Da außerdem der von der Informationsübertragungsquelle übertragene Nachrichtenauthentifizierungscode unter Verwendung des gemeinsamen Schlüssels basierend auf den aus der Informationsübertragungsquelle gesendeten Lieferinformationen berechnet wird, können der Berechnungsprozess des Einmalpassworts, die Konfiguration der Lieferinformationen und der Berechnungsprozess des MAC-Werts unabhängig parallel ausgeführt werden und der Verarbeitungsdurchsatz kann verbessert werden.

[0151] Außerdem werden die Lieferinformationen durch den gemeinsamen Schlüssel verschlüsselt und aus der Informationsübertragungsquelle gesendet, und die arithmetische Vorrichtung ist zu Folgendem ausgelegt ist: Entschlüsseln der aus der Informationsübertragungsquelle gesendeten Lieferinformationen; und Ausgeben eines Authentizitätsbestimmungsergebnisses der Lieferinformationen und der entschlüsselten Lieferinformationen. Daher kann ein Durchsickern von Inhalt von Lieferinformationen aufgrund von Abhören verhindert werden.

[0152] Außerdem sind ein gemeinsamer Schlüssel zum Erzeugen des Einmalpassworts, ein gemeinsamer Schlüssel zum Erzeugen des Nachrichtenauthentifizierungscodes und ein gemeinsamer Schlüssel zum Verschlüsseln der Lieferinformationen ein gleicher Schlüssel oder mehrere separate Schlüssel. Daher kann der Anwendungsprozess bei einer Schlüsseländerung frei eingestellt werden. Außerdem können in einem Fall, in dem der gemeinsame Schlüssel der gleiche ist, die Lieferinformationen verschlüsselt werden, ohne einen anderen gemeinsamen Schlüssel festzulegen, und ein Durchsickern der Lieferinformationen kann verhindert werden.

[0153] Außerdem ist die Informationsübertragungsquelle so konfiguriert, dass sie an eine Hostvorrichtung adressierte Lieferinformationen liefern kann, deren Authentizität durch die Informationsverifizierungsvorrichtung verifiziert werden soll, und an die Informationsverifizierungsvorrichtung adressierte Aktualisierungsinformationen liefern kann, und dann, wenn die Lieferinformationen Aktualisierungsinformationen sind, die an die Informationsverifizierungsvorrichtung adressiert sind, gibt die Informationsverifizierungsvorrichtung die entschlüsselten Lieferinformationen nicht aus und ändert einen internen Wert der Informationsverifizierungsvorrichtung unter Verwendung der Aktualisierungsinformationen. Daher können die vom OTP-Abgleichs-Chip 300 benötigten Informationen (beispielsweise die Zeitabgleichsinformationen des internen Takts und die Aktualisierungsinformationen des gemeinsamen Schlüssels) zusätzlich zu den an die Host-CPU210 gelieferten Lieferinformationen gänzlich durch das gleiche Protokoll geliefert werden.

[0154] Außerdem umfassen die Aktualisierungsinformationen von der Informationsübertragungsquelle an die Informationsverifizierungsvorrichtung Zeitdaten zum Korrigieren eines Takts der Informationsverifizierungsvorrichtung und dann, wenn ein Authentizitätsbestimmungsergebnis der aus der Informationsübertragungsquelle gesendeten Lieferinformationen authentisch ist, korrigiert die arithmetische Vorrichtung einen Takt der Informationsverifizierungsvorrichtung unter Verwendung der Zeitdaten. Daher ist es möglich, die Zeit mit hoher Sicherheit zu aktualisieren.

[0155] Außerdem umfassen die Aktualisierungsinformationen von der Informationsübertragungsquelle an die Informationsverifizierungsvorrichtung mindestens drei von Daten zum Aktualisieren eines gemeinsamen Schlüssels, dessen Kenntnis zwischen der Informationsübertragungsquelle und der Informationsverifizierungsvorrichtung geteilt wird, einer Kennung der Informationsverifizierungsvorrichtung, für die der gemeinsame Schlüssel zu aktualisieren ist, und einer Aktualisierungszeit des gemeinsamen Schlüssels und die arithmetische Vorrichtung aktualisiert einen gemeinsamen Schlüssel, der in der Verifizierungsvorrichtung gespeichert ist, zu der Aktualisierungszeitvorgabe, wenn das Authentizitätsbestimmungsergebnis der aus der Informationsübertragungsquelle gesendeten Lieferinformationen authentisch ist und die Kennung mit der einer Informationsverifizierungsvorrichtung der Informationsverifizierungsvorrichtung übereinstimmt. Daher ist es möglich, den gemeinsamen Schlüssel mit hoher Sicherheit zu aktualisieren.

[0156] Außerdem wird ein Cluster durch mehrere Empfangsvorrichtungsgruppen gebildet, die die Informationsverifizierungsvorrichtung beherbergen, indem sie zu einem gleichen gemeinsamen Schlüssel wechseln, dessen Kenntnis sich die mehreren Informationsverifizierungsvorrichtungen mit der Informationsübertragungsquelle teilen, und mehrere Informationsverifizierungsvorrichtungen, die den Cluster bilden, empfangen gleichzeitig unter Verwendung des gleichen Einmalpassworts und des gleichen Nachrichtenauthentifizierungscodes die gleichen Lieferinformationen aus der Informationsübertragungsquelle. Daher können die Lieferinformationen kollektiv eins-zu-viele gleichzeitig an den Cluster gesendet werden und die Informationen können effizient geliefert werden.

[0157] Ferner ist die vorliegende Erfindung nicht auf die oben beschriebenen Ausführungsformen beschränkt. Verschiedene Abwandlungen und äquivalente Konfigurationen können im Umfang der Ansprüche enthalten sein. Beispielsweise sind die oben beschriebenen Ausführungsformen im Einzelnen angegeben, um ein einfaches Verständnis der vorliegenden Erfindung zu unterstützen. Die vorliegende Erfindung ist nicht darauf beschränkt, alle oben beschriebenen Konfigurationen bereitzustellen. Außerdem können einige der Konfigurationen einer bestimmten Ausführungsform durch die Konfiguration der anderen Ausführungsform ersetzt werden. Zudem können die Konfigurationen der anderen Ausführungsform zu den Konfigurationen einer bestimmten Ausführungsform hinzugefügt werden. Außerdem können einige der Konfigurationen jeder Ausführungsform in Bezug auf die Konfiguration der anderen Ausführungsform hinzugefügt, weggelassen oder ersetzt werden.

[0158] Zudem können die oben beschriebenen Konfigurationen, Funktionen, Verarbeitungseinheiten und Verarbeitungsmittel durch eine Hardware-Konfiguration realisiert werden, indem einige oder alle der Konfigurationen unter Verwendung einer integrierten Schaltung eingestellt werden, können durch eine Software-Konfiguration realisiert werden, indem ein Programm analysiert und ausgeführt wird, um die Funktionen durch den Prozessor zu realisieren, oder kann als Vorrichtungssteuerungssprache oder Firmware realisiert werden, die eng mit der integrierten Schaltung verwandt ist.

[0159] Die Informationen des Programms, das Funktionen, Tabellen und Dateien realisiert, können in einer Speichervorrichtung wie etwa einem Speicher, einer Festplatte, einem Festkörperlaufwerk (SSD) oder einem Aufzeichnungsmedium wie etwa einer IC-Karte, einer SD-Karte und einer DVD gespeichert werden.

[0160] Außerdem sind nur Steuerleitungen und Informationsleitungen dargestellt, die für die Erläuterung notwendig sind, aber nicht alle Steuerleitungen und Informationsleitungen, die für die Montage erforderlich sind. In der Praxis können fast alle Konfigurationen als miteinander verbunden betrachtet werden.

ZITATE ENTHALTEN IN DER BESCHREIBUNG

Diese Liste der vom Anmelder aufgeführten Dokumente wurde automatisiert erzeugt und ist ausschließlich zur besseren Information des Lesers aufgenommen. Die Liste ist nicht Bestandteil der deutschen Patent- bzw. Gebrauchsmusteranmeldung. Das DPMA übernimmt keinerlei Haftung für etwaige Fehler oder Auslassungen.

Zitierte Patentliteratur

- JP 2020180515 [0001]
- JP 2002259344 A [0006, 0007, 0009]
- JP 6078686 B [0006]
- JP 6078686 B2 [0008]
- JP 6078686 B1 [0009]

Patentansprüche

1. Informationsverifizierungsvorrichtung, wobei
ein gemeinsamer Schlüssel, über den sich eine Informationsübertragungsquelle und die Informationsverifizierungsvorrichtung Kenntnis teilen, in einem Format gespeichert ist, das nicht einfach von außen gelesen werden kann, und
dann, wenn mindestens drei von einem Einmalpasswort, das aus der Informationsübertragungsquelle gesendet wird und durch eine synchronisierte Zeit und den gemeinsamen Schlüssel erzeugt wird, Lieferinformationen, die aus der Informationsübertragungsquelle gesendet werden und einen anderen Nutzungswert neben der Authentifizierung aufweisen, und einem Nachrichtenauthentifizierungscode, der aus der Informationsübermittlungsquelle gesendet wird und unter Verwendung des gemeinsamen Schlüssels aus diesen Informationselementen berechnet wird, eingegeben werden, zumindest ein Bestimmungsergebnis der Authentizität der Lieferinformationen ausgegeben wird.

2. Informationsverifizierungsvorrichtung nach Anspruch 1, wobei in einem Fall, in dem das aus der Informationsübertragungsquelle gesendete Einmalpasswort mit einem in der Informationsverifizierungsvorrichtung berechneten Einmalpasswort übereinstimmt und der aus der Informationsübertragungsquelle gesendete Nachrichtenauthentifizierungscode mit einem in der Informationsverifizierungsvorrichtung berechneten Nachrichtenauthentifizierungscode übereinstimmt, bestimmt wird, dass die Lieferinformationen authentisch sind, und ausgegeben wird, dass die Lieferinformationen authentisch sind.

3. Informationsverifizierungsvorrichtung nach Anspruch 1, wobei das Einmalpasswort, das aus der Informationsübertragungsquelle gesendet wird, ein Einmalpasswort vom Zeitsynchronisationstyp ist, das basierend auf einer Übertragungsstartzeit aus einer Reihe von Informationen erzeugt wird, die aus der Informationsübertragungsquelle an die Informationsverifizierungsvorrichtung gesendet werden.

4. Informationsverifizierungsvorrichtung nach Anspruch 1, wobei der aus der Informationsübertragungsquelle gesendete Nachrichtenauthentifizierungscode unter Verwendung des gemeinsamen Schlüssels basierend auf dem aus der Informationsübertragungsquelle gesendeten Einmalpasswort und den aus der Informationsübertragungsquelle gesendeten Lieferinformationen berechnet wird.

5. Informationsverifizierungsvorrichtung nach Anspruch 1, wobei der aus der Informationsübertragungsquelle gesendete Nachrichtenauthentifizierungscode unter Verwendung des gemeinsamen Schlüssels basierend auf den aus der Informationsübertragungsquelle gesendeten Lieferinformationen berechnet wird.

6. Informationsverifizierungsvorrichtung nach Anspruch 1, wobei
die Lieferinformationen durch den gemeinsamen Schlüssel verschlüsselt werden und aus der Informationsübertragungsquelle gesendet werden, und
die Informationsverifizierungsvorrichtung zu Folgendem ausgelegt ist:
Entschlüsseln der aus der Informationsübertragungsquelle gesendeten Lieferinformationen; und
Ausgeben eines Authentizitätsbestimmungsergebnisses der Lieferinformationen und der entschlüsselten Lieferinformationen.

7. Informationsverifizierungsvorrichtung nach Anspruch 6, wobei ein gemeinsamer Schlüssel zum Erzeugen des Einmalpassworts, ein gemeinsamer Schlüssel zum Erzeugen des Nachrichtenauthentifizierungscodes und ein gemeinsamer Schlüssel zum Verschlüsseln der Lieferinformationen ein gleicher Schlüssel oder mehrere separate Schlüssel sind.

8. Informationsverifizierungsvorrichtung nach Anspruch 1, wobei
die Informationsübermittlungsquelle so ausgelegt ist, dass sie Lieferinformationen, die an eine Host-Vorrichtung adressiert sind, deren Authentizität von der Informationsverifizierungsvorrichtung verifiziert werden soll, und Aktualisierungsinformationen, die an die Informationsverifizierungsvorrichtung adressiert sind, liefern kann, und
dann, wenn die Lieferinformationen Aktualisierungsinformationen sind, die an die Informationsverifizierungsvorrichtung adressiert sind, gibt die Informationsverifizierungsvorrichtung die entschlüsselten Lieferinformationen nicht aus und ändert einen internen Wert der Informationsverifizierungsvorrichtung unter Verwendung der Aktualisierungsinformationen.

9. Informationsverifizierungsvorrichtung nach Anspruch 8, wobei
die Aktualisierungsinformationen aus der Informationsübertragungsquelle an die Informationsverifizierungsvorrichtung Zeitdaten zum Korrigieren eines Takts der Informationsverifizierungsvorrichtung umfassen, und
dann, wenn ein Authentizitätsbestimmungsergebnis der aus der Informationsübertragungsquelle gesendeten Lieferinformationen authentisch ist, die Informationsverifizierungsvorrichtung den Takt der Informationsverifizierungsvorrichtung unter Verwendung der Zeitdaten korrigiert.

10. Informationsverifizierungsvorrichtung nach Anspruch 8, wobei

die Aktualisierungsinformationen aus der Informationsübertragungsquelle an die Informationsverifizierungsvorrichtung mindestens drei von Daten zum Aktualisieren eines gemeinsamen Schlüssels, zu dem Kenntnis zwischen der Informationsübertragungsquelle und der Informationsverifizierungsvorrichtung geteilt wird, einer Kennung der Informationsverifizierungsvorrichtung, für die der gemeinsame Schlüssel aktualisiert werden soll, und einer Aktualisierungszeit des gemeinsamen Schlüssels umfassen, und
die Informationsverifizierungsvorrichtung einen gemeinsamen Schlüssel, der in der Verifizierungsvorrichtung gespeichert ist, zu der Aktualisierungszeitvorgabe aktualisiert, wenn das Authentizitätsbestimmungsergebnis der aus der Informationsübertragungsquelle gesendeten Lieferinformationen authentisch ist und die Kennung mit der der Informationsverifizierungsvorrichtung übereinstimmt.

11. Informationsverifizierungsvorrichtung nach Anspruch 10, wobei
ein Cluster durch mehrere Empfangsvorrichtungsgruppen, die die Informationsverifizierungsvorrichtung beherbergen, gebildet wird, indem sie zu einem gleichen gemeinsamen Schlüssel wechseln, über den sich die mehreren Informationsverifizierungsvorrichtungen Kenntnis mit der Informationsübertragungsquelle teilen, und
mehrere Informationsverifizierungsvorrichtungen, die den Cluster bilden, gleichzeitig unter Verwendung eines gleichen Einmalpassworts und eines gleichen Nachrichtenauthentifizierungscodes die gleichen Lieferinformationen aus der Informationsübertragungsquelle empfangen.

12. Elektronische Steuervorrichtung, die die Informationsverifizierungsvorrichtung nach einem der Ansprüche 1 bis 11 umfasst, wobei die elektronische Steuervorrichtung an einem Automobil montiert ist.

13. Informationsverifizierungsverfahren, das von einer Informationsverifizierungsvorrichtung ausgeführt wird, wobei
die Informationsverifizierungsvorrichtung durch eine arithmetische Vorrichtung ausgebildet wird, die eine vorbestimmte Verarbeitung ausführt, und einen gemeinsamen Schlüssel, über den Kenntnis zwischen einer Informationsübertragungsquelle und der Informationslieferungsvorrichtung geteilt wird, in einem Format speichert, das nicht einfach von außen gelesen werden kann, und
dann, wenn mindestens drei von einem Einmalpasswort, das aus der Informationsübertragungsquelle gesendet wird und durch eine synchronisierte Zeit und den gemeinsamen Schlüssel erzeugt wird, Lieferinformationen, die aus der Informationsübertragungsquelle gesendet werden und einem anderen Nutzungswert neben der Authentifizierung aufweisen, und einem Nachrichtenauthentifizierungscode, der aus der Informationsübermittlungsquelle gesendet wird und aus diesen Informationselementen unter Verwendung des gemeinsamen Schlüssels berechnet wird, eingegeben werden, die Informationsverifizierungsvorrichtung zumindest ein Bestimmungsergebnis der Authentizität der Lieferinformationen ausgibt.

Es folgen 11 Seiten Zeichnungen

Anhängende Zeichnungen

FIG. 1

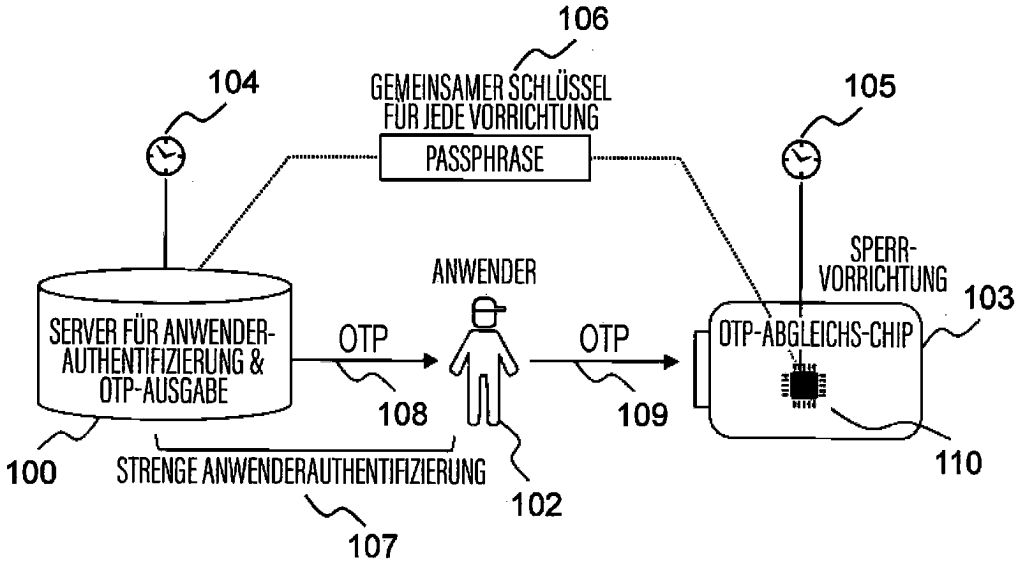


FIG. 2

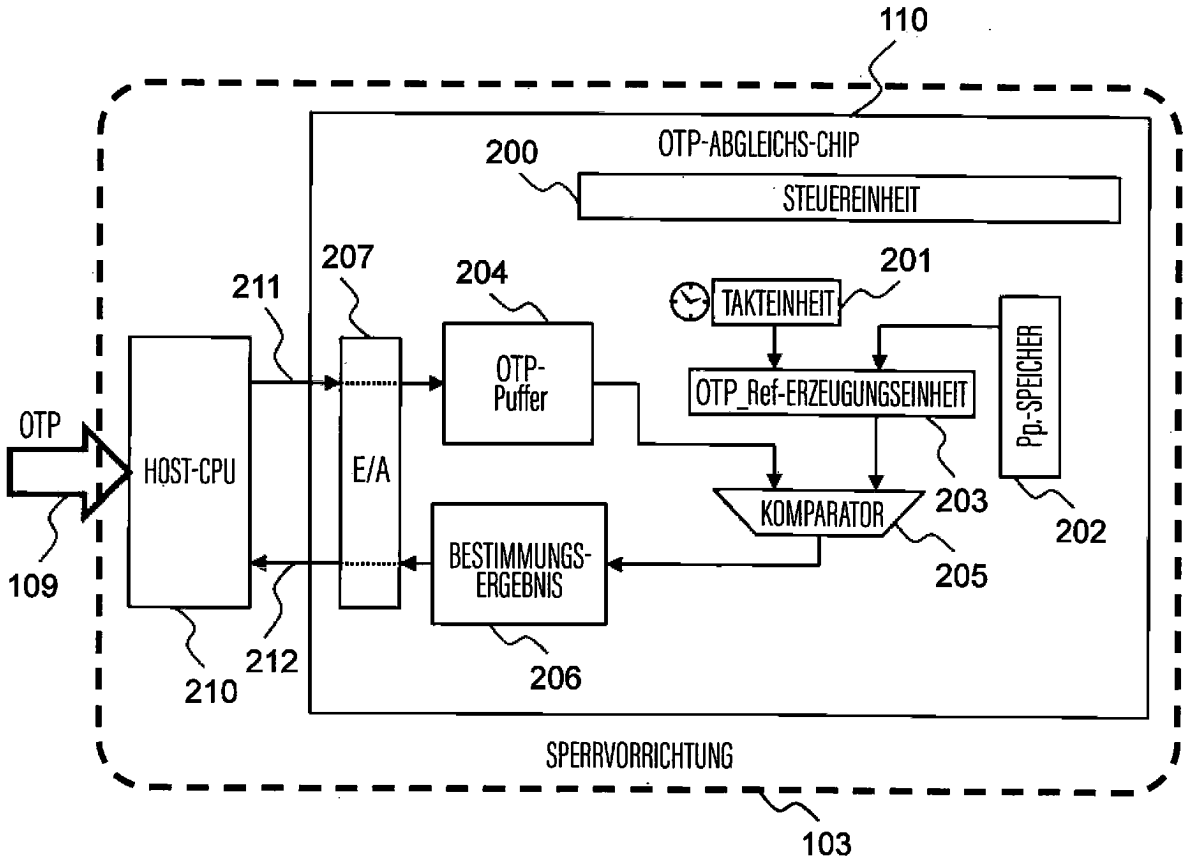


FIG. 3

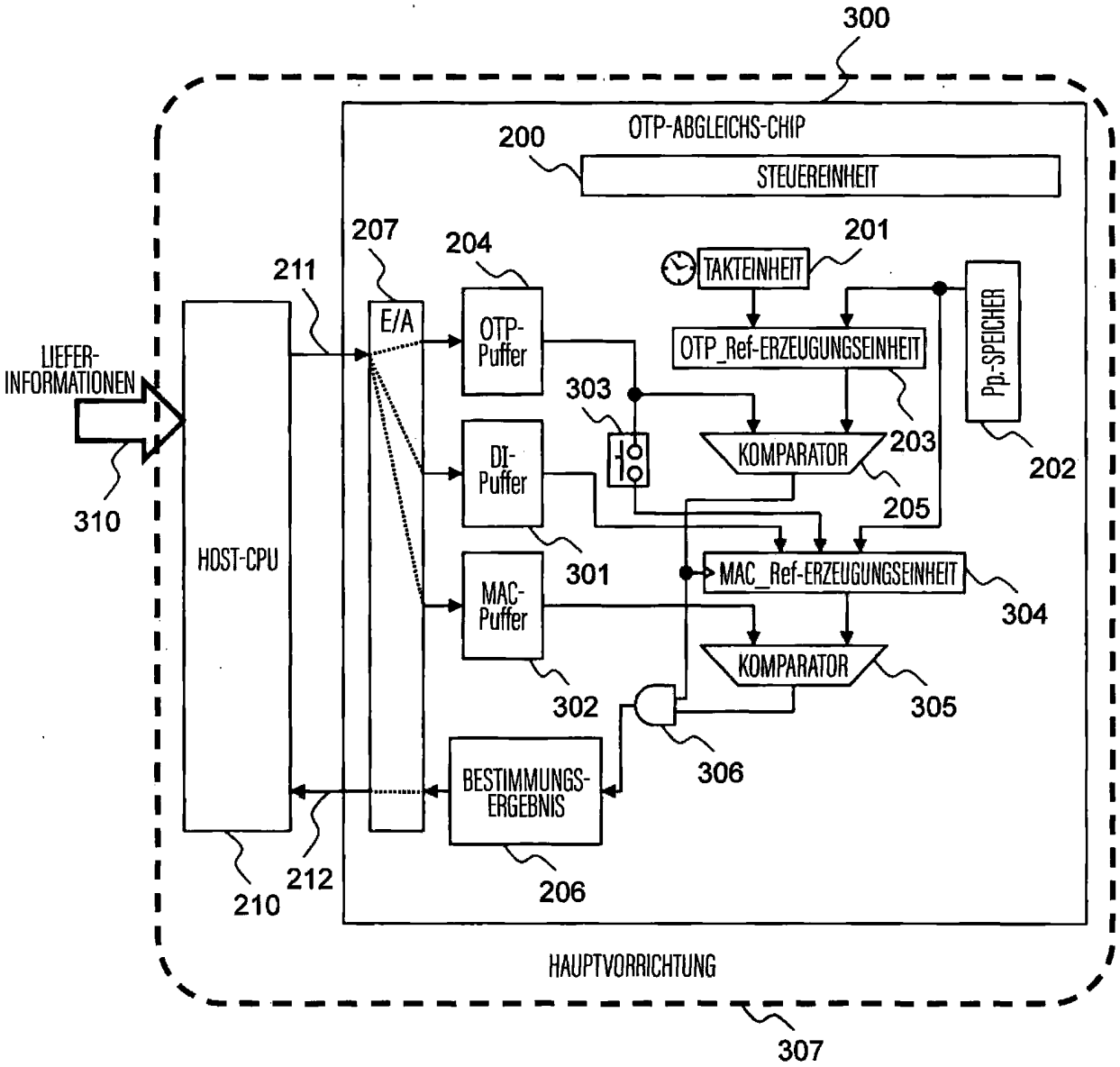

300
OTP-ABGLEICHS-CHIP
200
STEUEREINHEIT
207
204
201
211
TAKTEINHEIT
E/A
OTP-Puffer
OTP_Ref-ERZEUGUNGSEINHEIT
Pp.-SPEICHER
LIEFER-INFORMATIONEN
303
KOMPARATOR
203
202
DI-Puffer
205
310
HOST-CPU
301
MAC_Ref-ERZEUGUNGSEINHEIT
304
MAC-Puffer
KOMPARATOR
302
305
306
BESTIMMUNGS-ERGEBNIS
212
210
206
HAUPTVORRICHTUNG
307

FIG. 4

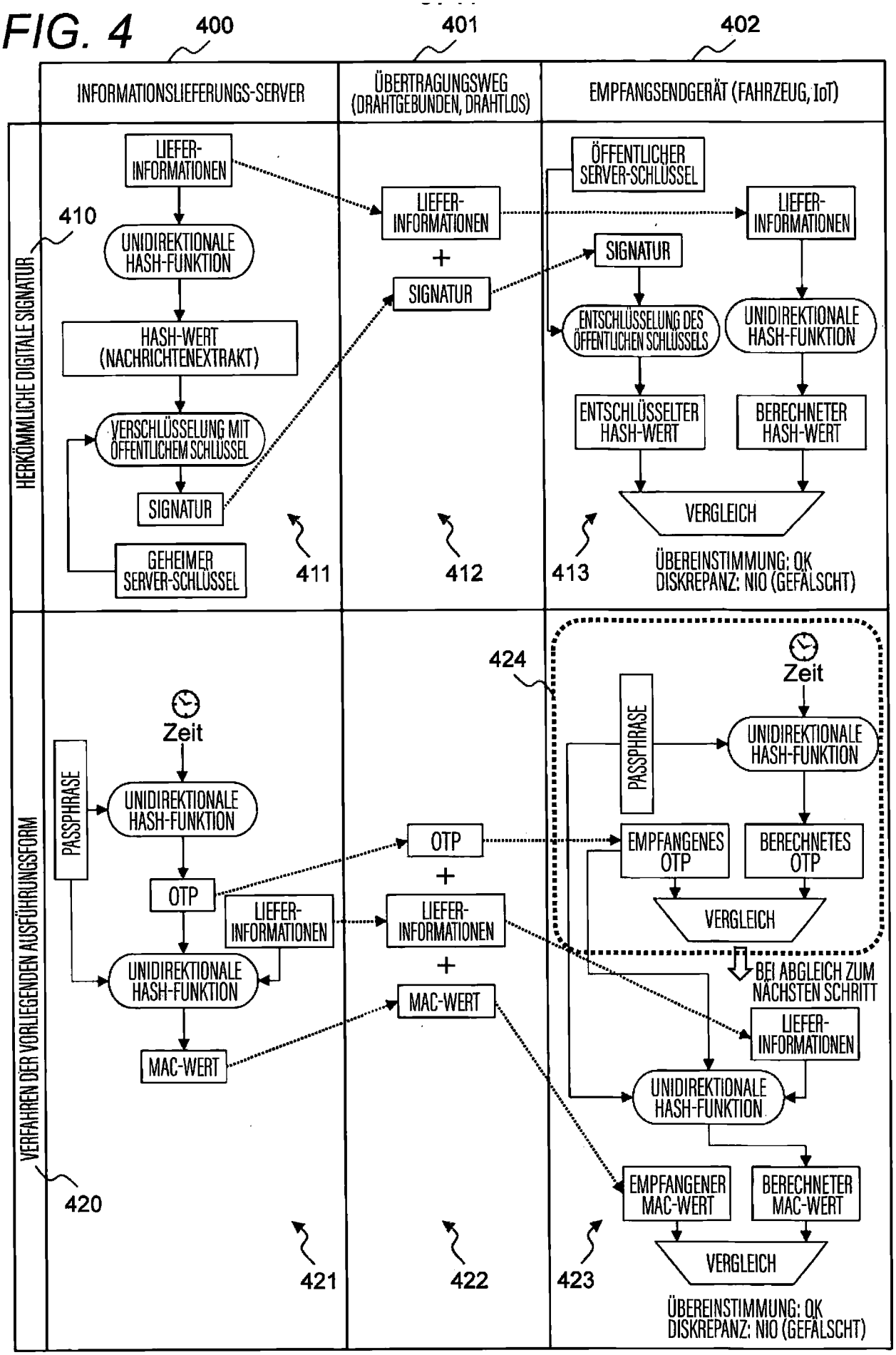

400
401
402
INFORMATIONSLIEFERUNGS-SERVER
ÜBERTRAGUNGSWEG (DRAHTGEBUNDEN, DRAHTLOS)
EMPFANGSENDGERÄT (FAHRZEUG, IoT)
HERKÖMMLICHE DIGITALE SIGNATUR
410
LIEFER-INFORMATIONEN
UNIDIREKTIONALE HASH-FUNKTION
HASH-WERT (NACHRICHTENEXTRAKT)
VERSCHLÜSSELUNG MIT ÖFFENTLICHEM SCHLÜSSEL
SIGNATUR
GEHEIMER SERVER-SCHLÜSSEL
LIEFER-INFORMATIONEN
+
SIGNATUR
ÖFFENTLICHER SERVER-SCHLÜSSEL
LIEFER-INFORMATIONEN
SIGNATUR
ENTSCHLÜSSELUNG DES ÖFFENTLICHEN SCHLÜSSELS
UNIDIREKTIONALE HASH-FUNKTION
ENTSCHLÜSSELTER HASH-WERT
BERECHNETER HASH-WERT
VERGLEICH
ÜBEREINSTIMMUNG: OK
DISKREPANZ: NIO (GEFÄLSCHT)
411
412
413
VERFAHREN DER VORLIEGENDEN AUSFÜHRUNGSFORM
420
Zeit
PASSPHRASE
UNIDIREKTIONALE HASH-FUNKTION
OTP
LIEFER-INFORMATIONEN
UNIDIREKTIONALE HASH-FUNKTION
MAC-WERT
OTP
+
LIEFER-INFORMATIONEN
+
MAC-WERT
424
Zeit
PASSPHRASE
UNIDIREKTIONALE HASH-FUNKTION
EMPFANGENES OTP
BERECHNETES OTP
VERGLEICH
BEI ABGLEICH ZUM NÄCHSTEN SCHRITT
LIEFER-INFORMATIONEN
UNIDIREKTIONALE HASH-FUNKTION
EMPFANGENER MAC-WERT
BERECHNETER MAC-WERT
VERGLEICH
ÜBEREINSTIMMUNG: OK
DISKREPANZ: NIO (GEFÄLSCHT)
421
422
423

FIG. 5

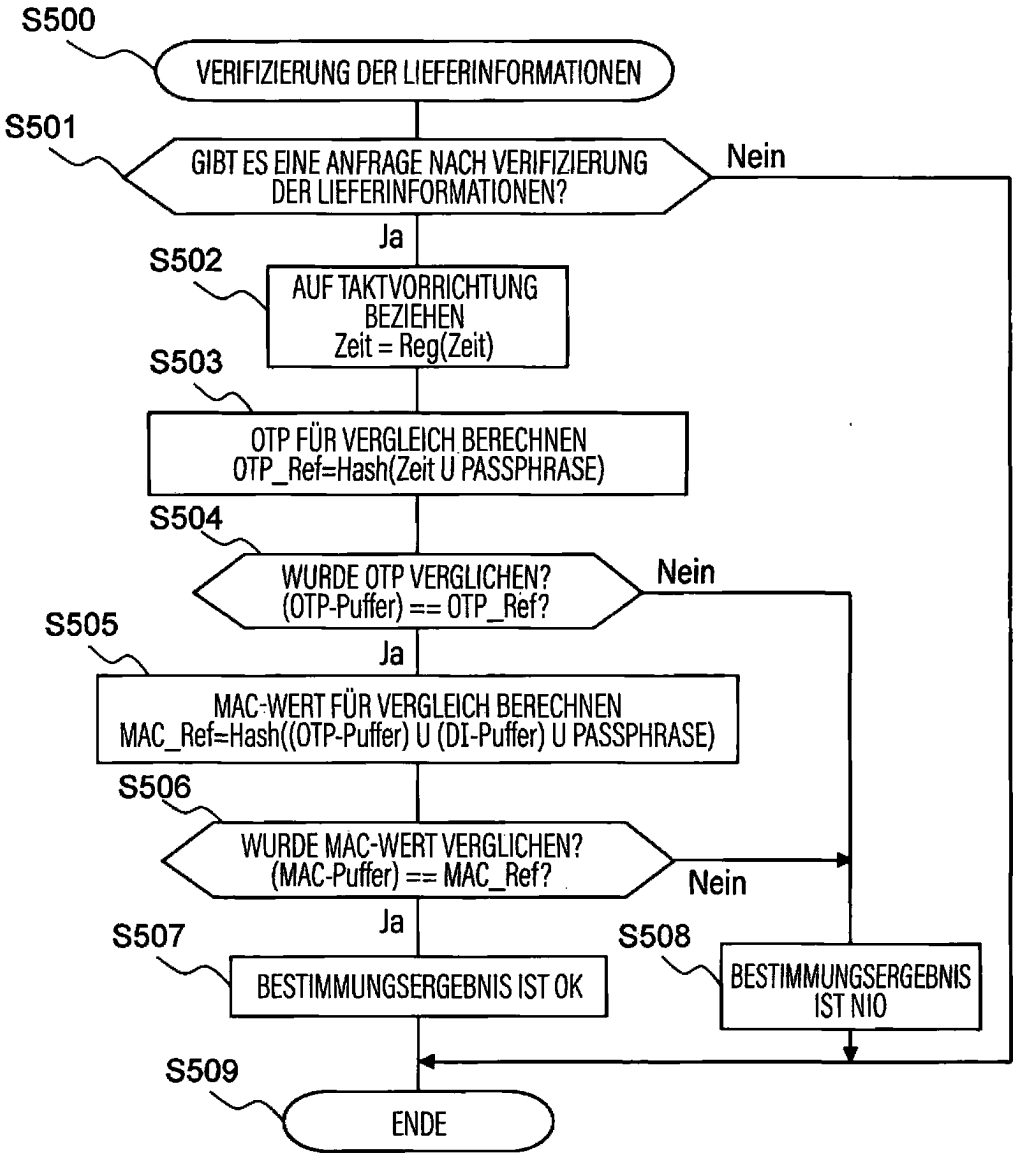

S500
VERIFIZIERUNG DER LIEFERINFORMATIONEN
S501
GIBT ES EINE ANFRAGE NACH VERIFIZIERUNG DER LIEFERINFORMATIONEN?
Nein
Ja
S502
AUF TAKTVORRICHTUNG BEZIEHEN
Zeit = Reg(Zeit)
S503
OTP FÜR VERGLEICH BERECHNEN
OTP_Ref=Hash(Zeit U PASSPHRASE)
S504
WURDE OTP VERGLICHEN?
(OTP-Puffer) == OTP_Ref?
Nein
Ja
S505
MAC-WERT FÜR VERGLEICH BERECHNEN
MAC_Ref=Hash((OTP-Puffer) U (DI-Puffer) U PASSPHRASE)
S506
WURDE MAC-WERT VERGLICHEN?
(MAC-Puffer) == MAC_Ref?
Nein
Ja
S507
BESTIMMUNGSERGEBNIS IST OK
S508
BESTIMMUNGSERGEBNIS IST NIO
S509
ENDE

FIG. 6

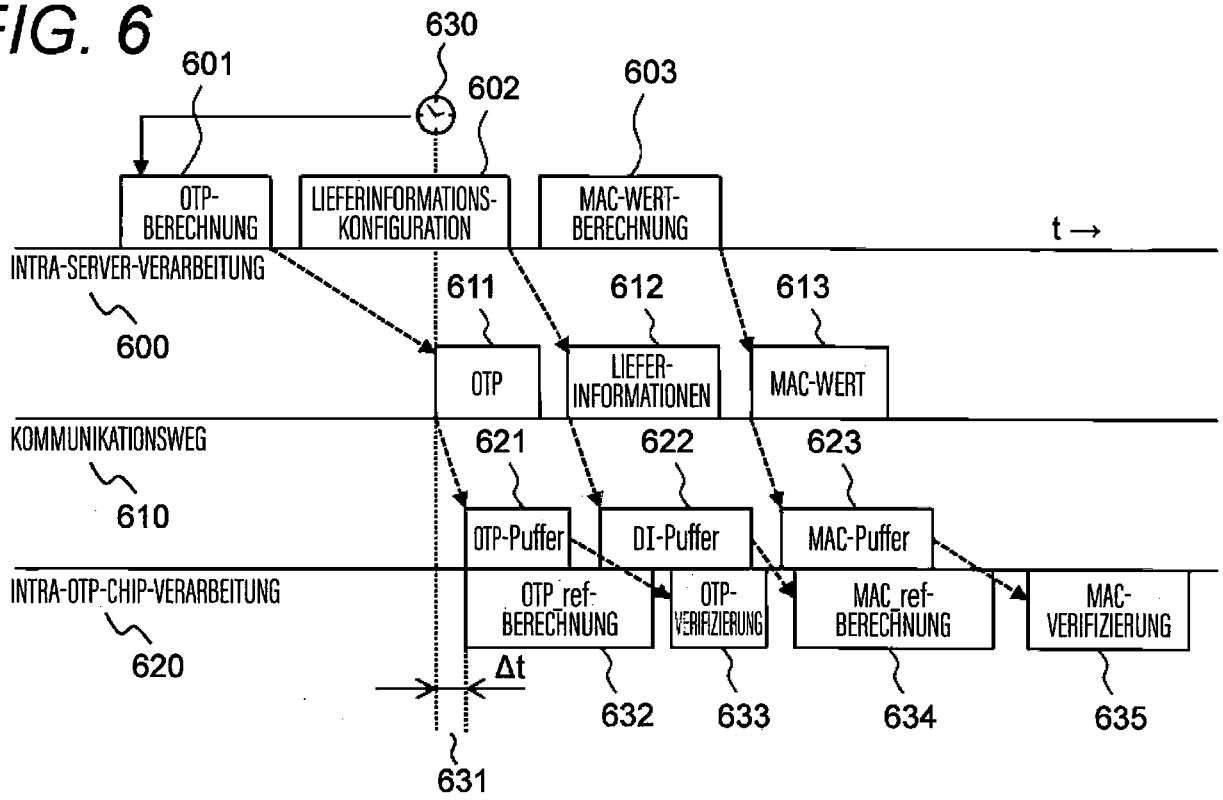

630
601
602
603
OTP-BERECHNUNG
LIEFERINFORMATIONS-KONFIGURATION
MAC-WERT-BERECHNUNG
t →
INTRA-SERVER-VERARBEITUNG
600
611
612
613
OTP
LIEFER-INFORMATIONEN
MAC-WERT
KOMMUNIKATIONSWEG
610
621
622
623
OTP-Puffer
DI-Puffer
MAC-Puffer
INTRA-OTP-CHIP-VERARBEITUNG
620
OTP_ref-BERECHNUNG
OTP-VERIFIZIERUNG
MAC_ref-BERECHNUNG
MAC-VERIFIZIERUNG
Δt
632
633
634
635
631

FIG. 7

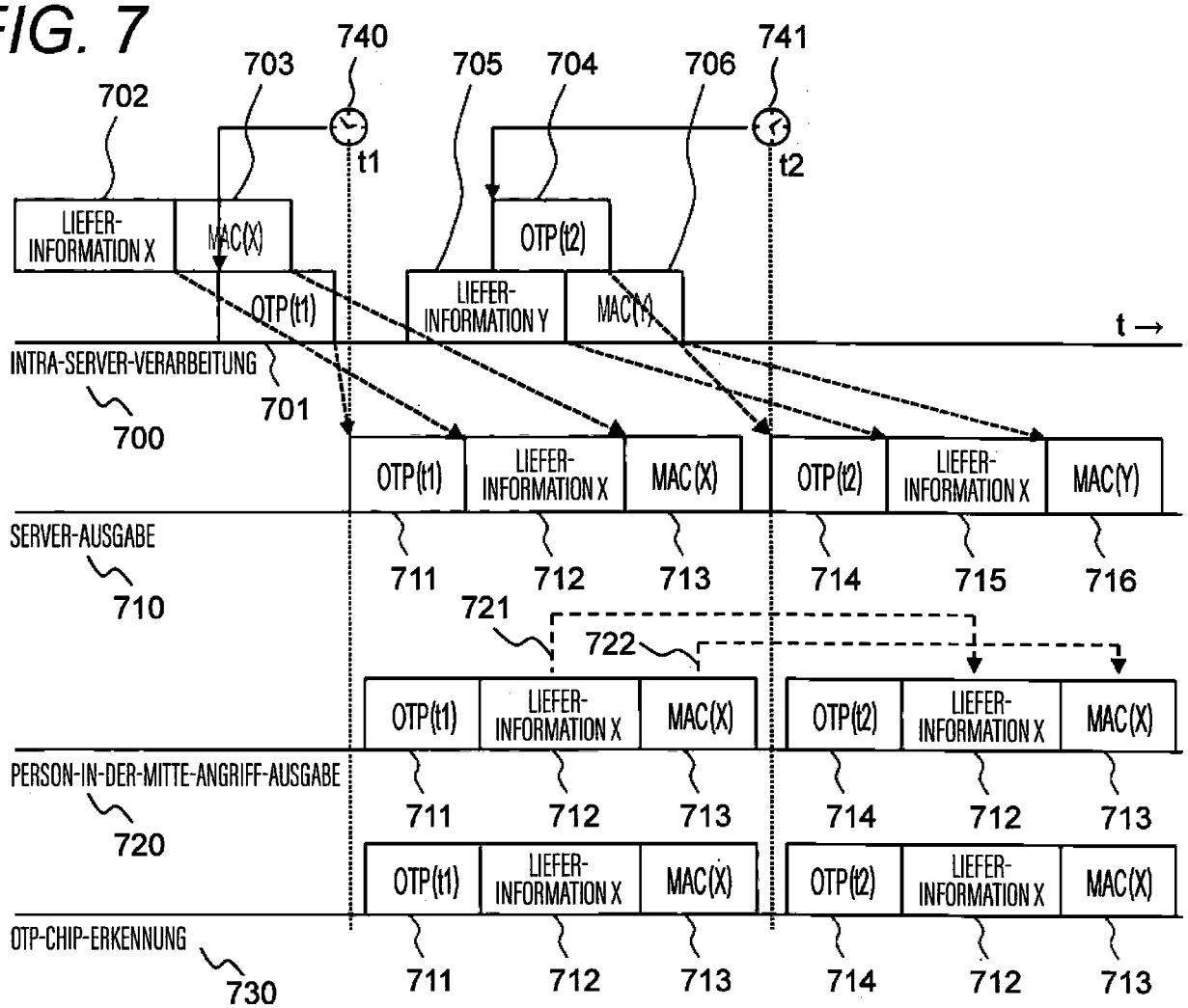

740
741
703
705
704
706
702
t1
t2
LIEFER-INFORMATION X
MAC(X)
OTP(t2)
OTP(t1)
LIEFER-INFORMATION Y
MAC(Y)
t →
INTRA-SERVER-VERARBEITUNG
701
700
OTP(t1)
LIEFER-INFORMATION X
MAC(X)
OTP(t2)
LIEFER-INFORMATION X
MAC(Y)
SERVER-AUSGABE
711
712
713
714
715
716
710
721
722
OTP(t1)
LIEFER-INFORMATION X
MAC(X)
OTP(t2)
LIEFER-INFORMATION X
MAC(X)
PERSON-IN-DER-MITTE-ANGRIFF-AUSGABE
711
712
713
714
712
713
720
OTP(t1)
LIEFER-INFORMATION X
MAC(X)
OTP(t2)
LIEFER-INFORMATION X
MAC(X)
OTP-CHIP-ERKENNUNG
711
712
713
714
712
713
730

FIG. 8

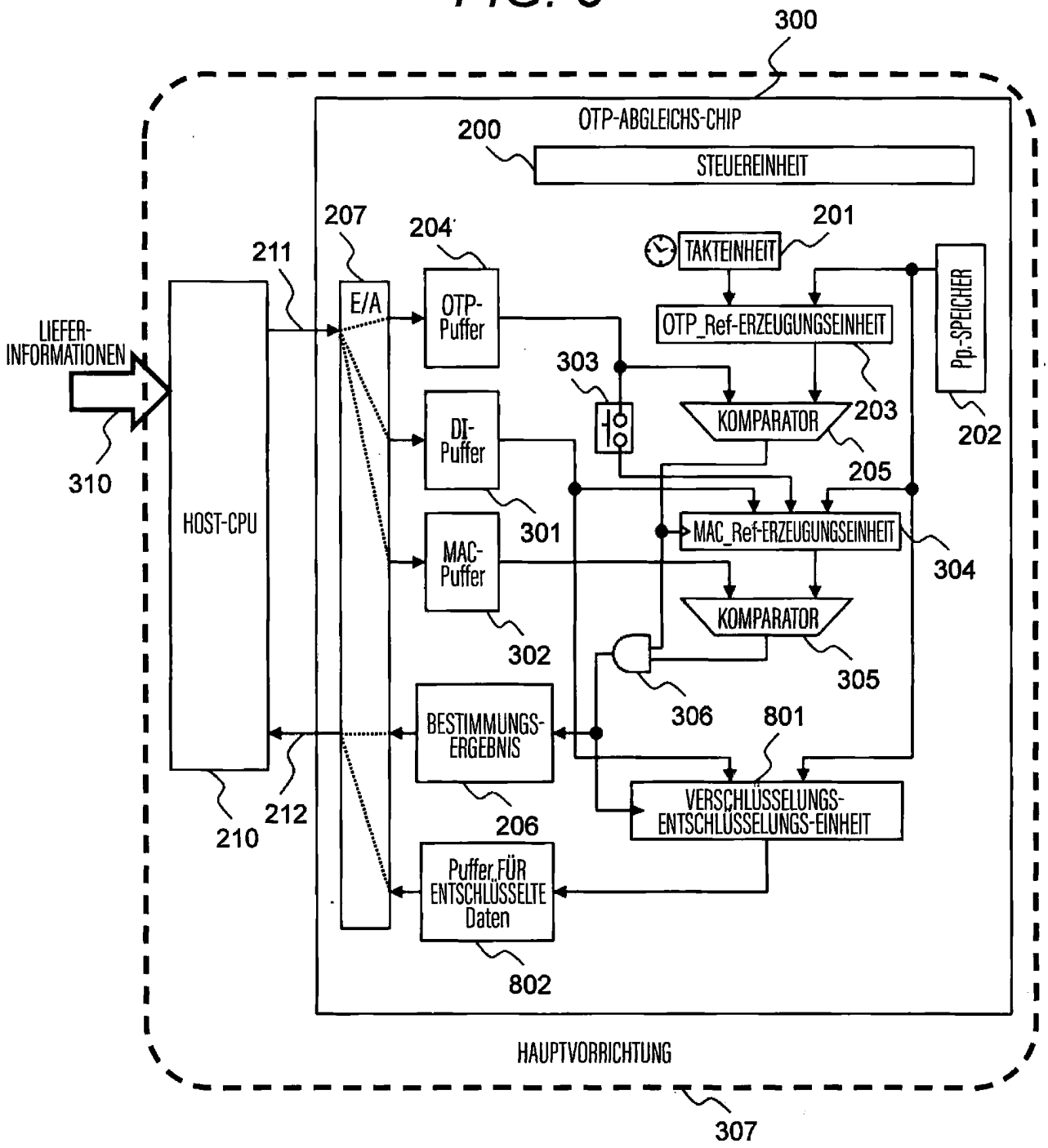

300
OTP-ABGLEICHS-CHIP
200
STEUEREINHEIT
207
204
201
TAKTEINHEIT
211
E/A
OTP-Puffer
OTP_Ref-ERZEUGUNGSEINHEIT
Pp.-SPEICHER
LIEFER-INFORMATIONEN
303
KOMPARATOR
203
202
DI-Puffer
205
HOST-CPU
MAC_Ref-ERZEUGUNGSEINHEIT
301
MAC-Puffer
304
KOMPARATOR
302
305
306
801
BESTIMMUNGS-ERGEBNIS
VERSCHLÜSSELUNGS-ENTSCHLÜSSELUNGS-EINHEIT
310
210
212
206
Puffer FÜR ENTSCHLÜSSELTE Daten
802
HAUPTVORRICHTUNG
307

FIG. 9

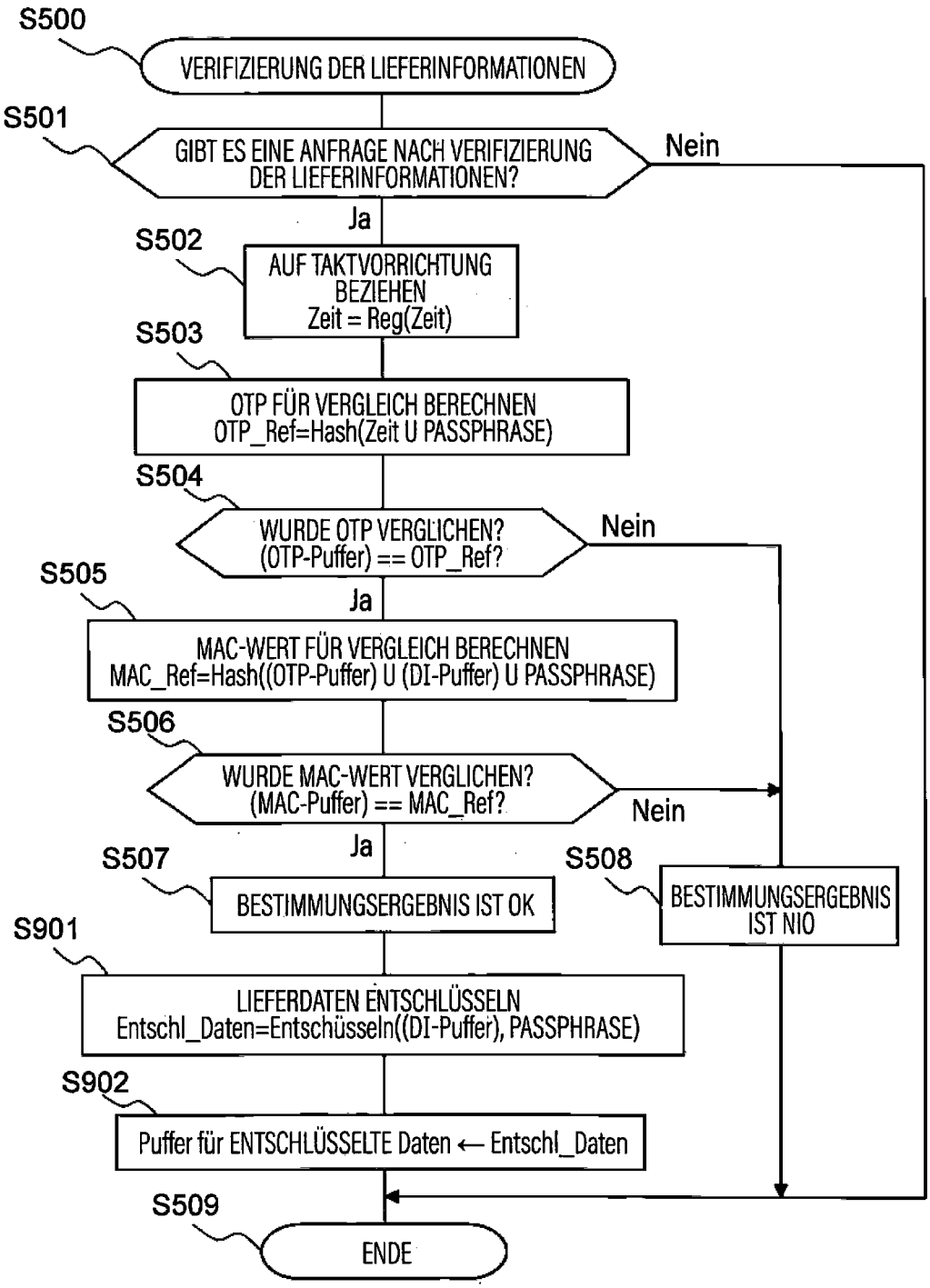

S500
VERIFIZIERUNG DER LIEFERINFORMATIONEN
S501
GIBT ES EINE ANFRAGE NACH VERIFIZIERUNG DER LIEFERINFORMATIONEN?
Nein
Ja
S502
AUF TAKTVORRICHTUNG BEZIEHEN
Zeit = Reg(Zeit)
S503
OTP FÜR VERGLEICH BERECHNEN
OTP_Ref=Hash(Zeit U PASSPHRASE)
S504
WURDE OTP VERGLICHEN?
(OTP-Puffer) == OTP_Ref?
Nein
Ja
S505
MAC-WERT FÜR VERGLEICH BERECHNEN
MAC_Ref=Hash((OTP-Puffer) U (DI-Puffer) U PASSPHRASE)
S506
WURDE MAC-WERT VERGLICHEN?
(MAC-Puffer) == MAC_Ref?
Nein
Ja
S507
BESTIMMUNGSERGEBNIS IST OK
S508
BESTIMMUNGSERGEBNIS IST NIO
S901
LIEFERDATEN ENTSCHLÜSSELN
Entschl_Daten=Entschüsseln((DI-Puffer), PASSPHRASE)
S902
Puffer für ENTSCHLÜSSELTE Daten ← Entschl_Daten
S509
ENDE

FIG. 10

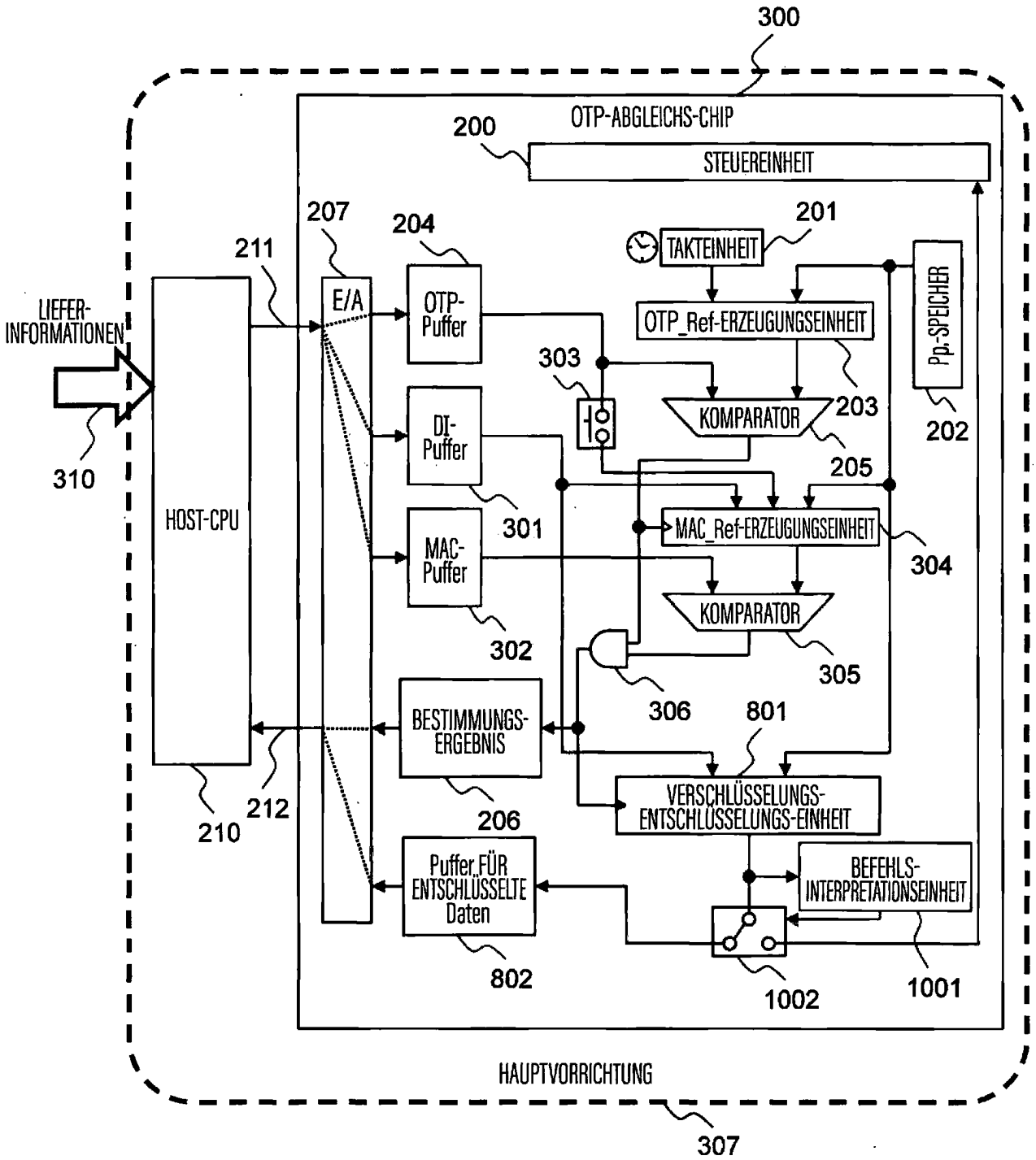

300
OTP-ABGLEICHS-CHIP
200
STEUEREINHEIT
207
204
201
TAKTEINHEIT
211
E/A
OTP-Puffer
OTP_Ref-ERZEUGUNGSEINHEIT
Pp.-SPEICHER
LIEFER-INFORMATIONEN
303
KOMPARATOR
203
202
DI-Puffer
205
HOST-CPU
MAC_Ref-ERZEUGUNGSEINHEIT
301
MAC-Puffer
304
KOMPARATOR
310
302
305
306
801
BESTIMMUNGS-ERGEBNIS
VERSCHLÜSSELUNGS-ENTSCHLÜSSELUNGS-EINHEIT
210
212
206
Puffer FÜR ENTSCHLÜSSELTE Daten
BEFEHLS-INTERPRETATIONSEINHEIT
802
1002
1001
HAUPTVORRICHTUNG
307

FIG. 11

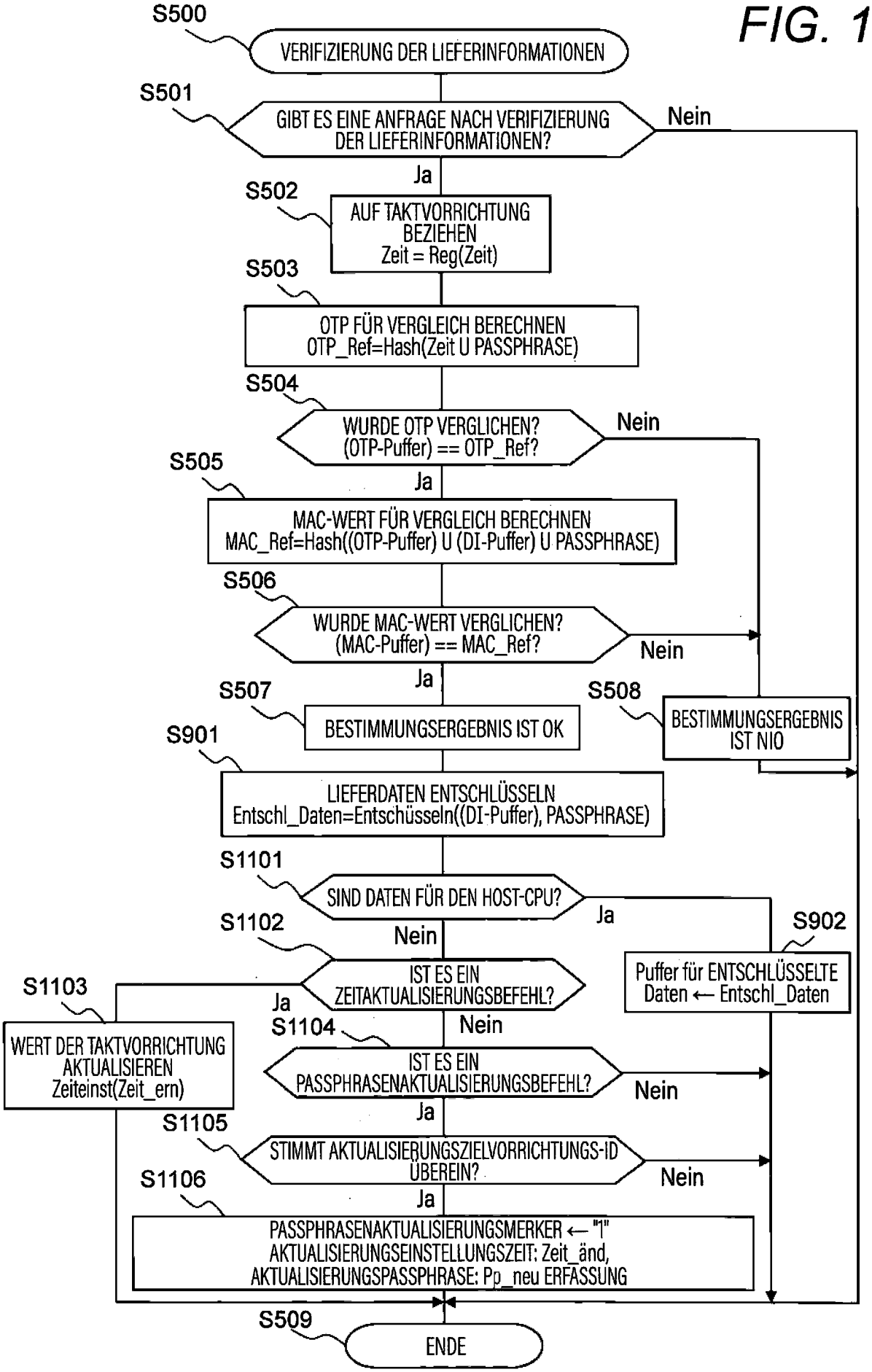

S500
VERIFIZIERUNG DER LIEFERINFORMATIONEN
S501
GIBT ES EINE ANFRAGE NACH VERIFIZIERUNG DER LIEFERINFORMATIONEN?
Nein
Ja
S502
AUF TAKTVORRICHTUNG BEZIEHEN
Zeit = Reg(Zeit)
S503
OTP FÜR VERGLEICH BERECHNEN
OTP_Ref=Hash(Zeit U PASSPHRASE)
S504
WURDE OTP VERGLICHEN?
(OTP-Puffer) == OTP_Ref?
Nein
S505
Ja
MAC-WERT FÜR VERGLEICH BERECHNEN
MAC_Ref=Hash((OTP-Puffer) U (DI-Puffer) U PASSPHRASE)
S506
WURDE MAC-WERT VERGLICHEN?
(MAC-Puffer) == MAC_Ref?
Nein
Ja
S507
BESTIMMUNGSERGEBNIS IST OK
S508
BESTIMMUNGSERGEBNIS IST NIO
S901
LIEFERDATEN ENTSCHLÜSSELN
Entschl_Daten=Entschüsseln((DI-Puffer), PASSPHRASE)
S1101
SIND DATEN FÜR DEN HOST-CPU?
Ja
S902
Puffer für ENTSCHLÜSSELTE Daten ← Entschl_Daten
Nein
S1102
IST ES EIN ZEITAKTUALISIERUNGSBEFEHL?
S1103
Ja
WERT DER TAKTVORRICHTUNG AKTUALISIEREN
Zeiteinst(Zeit_ern)
Nein
S1104
IST ES EIN PASSPHRASENAKTUALISIERUNGSBEFEHL?
Nein
Ja
S1105
STIMMT AKTUALISIERUNGSZIELVORRICHTUNGS-ID ÜBEREIN?
Nein
S1106
Ja
PASSPHRASENAKTUALISIERUNGSMERKER ← "1"
AKTUALISIERUNGSEINSTELLUNGSZEIT: Zeit_änd,
AKTUALISIERUNGSPASSPHRASE: Pp_neu ERFASSUNG
S509
ENDE

FIG. 12

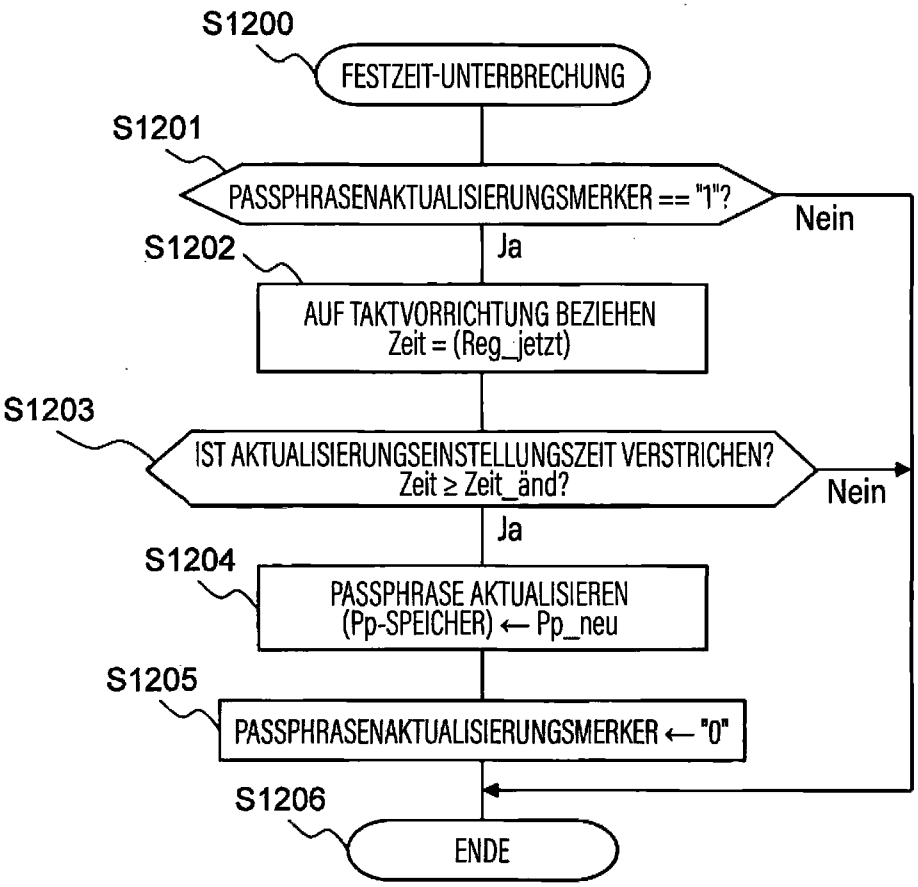

S1200
FESTZEIT-UNTERBRECHUNG
S1201
PASSPHRASENAKTUALISIERUNGSMERKER == "1"?
Nein
Ja
S1202
AUF TAKTVORRICHTUNG BEZIEHEN
Zeit = (Reg_jetzt)
S1203
IST AKTUALISIERUNGSEINSTELLUNGSZEIT VERSTRICHEN?
Zeit ≥ Zeit_änd?
Nein
Ja
S1204
PASSPHRASE AKTUALISIEREN
(Pp-SPEICHER) ← Pp_neu
S1205
PASSPHRASENAKTUALISIERUNGSMERKER ← "0"
S1206
ENDE

FIG. 13