



(10) **DE 11 2022 004 670 T5** 2024.08.01

(12) **Veröffentlichung**

der internationalen Anmeldung mit der
(87) Veröffentlichungs-Nr.: **WO 2023/053621**
in der deutschen Übersetzung (Art. III § 8 Abs. 2
IntPatÜbkG)
(21) Deutsches Aktenzeichen: **11 2022 004 670.8**
(86) PCT-Aktenzeichen: **PCT/JP2022/024875**
(86) PCT-Anmeldetag: **22.06.2022**
(87) PCT-Veröffentlichungstag: **06.04.2023**
(43) Veröffentlichungstag der PCT Anmeldung
in deutscher Übersetzung: **01.08.2024**

(51) Int Cl.: **H04L 9/00 (2022.01)**

(30) Unionspriorität:
2021-161212 30.09.2021 JP
(71) Anmelder:
DENSO CORPORATION, Kariya-city, Aichi, JP
(74) Vertreter:
**Winter, Brandl - Partnerschaft mbB,
Patentanwälte, 85354 Freising, DE**

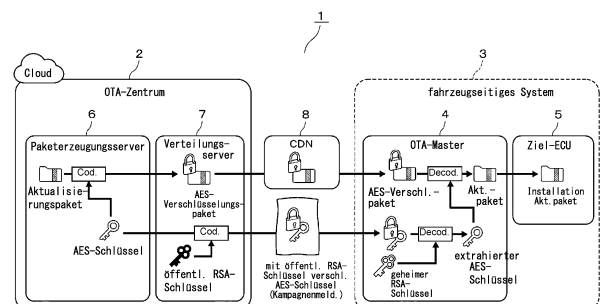
(72) Erfinder:
**Yoshimi, Hideo, Kariya-city, Aichi-pref., JP; Abe,
Masaaki, Kariya-city, Aichi-pref., JP; Tomatsu,
Koto, Kariya-city, Aichi-pref., JP**

Prüfungsantrag gemäß § 44 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.

(54) Bezeichnung: **DATENKOMMUNIKATIONSSYSTEM, ZENTRUMSVORRICHTUNG, MASTERVORRICHTUNG,
VERSCHLÜSSELUNGSPROGRAMM UND ENTSCHLÜSSELUNGSPROGRAMM**

(57) Zusammenfassung: Ein Datenkommunikationssystem (1) weist auf: eine Zentrumsvorrichtung (2), die Aktualisierungsdaten an eine Mastervorrichtung verteilt; und eine Mastervorrichtung (4), die die Aktualisierungsdaten, die von der Zentrumsvorrichtung heruntergeladen wurden, in einer neu zu programmierenden elektronischen Steuerungsvorrichtung installiert. Es wird ein Zählermodus (CTR) als ein Verschlüsselungsverfahren und ein Entschlüsselungsverfahren für die Aktualisierungsdaten verwendet.



Beschreibung**Zusammenfassung der Erfindung**

Querverweis auf betreffende Anmeldungen

[0001] Die vorliegende Anmeldung beansprucht die Priorität der am 30. September 2021 eingereichten japanischen Patentanmeldung Nr. 2021-161212. Der gesamte Inhalt der obigen Anmeldung ist hiermit durch Bezugnahme darauf enthalten.

Technisches Gebiet

[0002] Die vorliegende Erfindung betrifft ein Datenkommunikationssystem, eine Zentrumsvorrichtung, eine Mastervorrichtung, ein Verschlüsselungsprogramm und ein Entschlüsselungsprogramm.

Stand der Technik

[0003] In den vergangenen Jahren hat sich mit einer Diversifizierung von Fahrzeugsteuerungen wie beispielsweise einer Fahrunterstützungsfunktion und einer automatisierten Fahrfunktion der Umfang von Anwendungsprogrammen für eine Fahrzeugsteuerung, eine Fahrzeugdiagnose und Ähnliches, die in einer elektronischen Steuerungseinheit (im Folgenden als ECU abgekürzt) installiert sind, erhöht. Außerdem gibt es mit einem Versions-Upgrade durch eine Funktionsverbesserung oder Ähnliches mehr Möglichkeiten zur Neuprogrammierung des Anwendungsprogramms der ECU. Die Neuprogrammierung kann auch als Programmaktualisierung bezeichnet werden. Mit der Entwicklung von Kommunikationsnetzwerken und Ähnlichem hat sich andererseits eine Connected-Car-Technologie bzw. eine Technologie eines vernetzten Fahrzeugs verbreitet. Diesbezüglich offenbart die Patenliteratur 1 beispielsweise eine Technik zum Verteilen eines Aktualisierungspakets, in dem Aktualisierungsdaten gepackt sind, von einer Zentrumsvorrichtung an eine fahrzeugseitige Mastervorrichtung durch eine Over-The-Air-Technik (OTA). Die Mastervorrichtung ist eine Vorrichtung, die eine Neuprogrammierung des Anwendungsprogramms der ECU steuert. Die Aktualisierungsdaten, die von der Zentrumsvorrichtung an die Mastervorrichtung verteilt bzw. geliefert bzw. zugeführt werden, enthalten beispielsweise Anwendungsprogramme und Daten einer automatisierten Fahrt von fortgeschrittenen Fahrunterstützungssystemen (ADAS), Multimediadaten und Ähnliches.

Literatur des Standes der Technik**Patentliteratur**

[0004] Patentliteratur 1: JP 2020- 276 424 A

[0005] In den vergangenen Jahren hat sich zur Verbesserung einer Nutzererfahrung (im Folgenden als UX abgekürzt) eines Fahrzeugs die Datengröße eines Aktualisierungspakets, das von einer Zentrumsvorrichtung an eine Mastervorrichtung verteilt wird, auf eine Größenordnung von mehreren GB oder mehr erhöht. Außerdem wurde überlegt, die Aktualisierungsfrequenz bzw. Aktualisierungshäufigkeit durch häufigeres Aktualisieren des Anwendungsprogramms zu erhöhen.

[0006] Unter Berücksichtigung einer Hardwarebeschränkung des Mikrocomputers, der in der Mastervorrichtung montiert ist, stellt jedoch der Entschlüsselungsprozess des fortgeschrittenen Verschlüsselungsstandards (Advanced Encryption Standard, im Folgenden als AES abgekürzt) ein Flaschenhals dar. Wenn ein Chiffrierungsblockkettenmodus (Cipher Block Chaining, im Folgenden als CBC-Modus abgekürzt) einer allgemeinen Blockverschlüsselung für das Verschlüsselungsverfahren und das Entschlüsselungsverfahren verwendet wird, wird erwartet, dass der Durchsatz etwa 10 Mbps beträgt. In der Mastervorrichtung dauert es in einem Fall, in dem ein Aktualisierungspaket mit einer Datengröße von mehreren GB oder mehr von der Zentrumsvorrichtung mit einem Durchsatz von etwa 10 Mbps heruntergeladen wird, beispielsweise näherungsweise 30 Minuten, um das Aktualisierungspaket herunterzuladen, wenn die Datengröße gleich 2 GB ist, und es dauert näherungsweise 5 Stunden, um das Aktualisierungspaket in einem Fall herunterzuladen, in dem die Datengröße gleich 20 GB ist. Wenn wie oben beschrieben die Zeit, die zum Herunterladen des Aktualisierungspaketes benötigt wird, lang ist, muss der Fahrer mehr als notwendig während des Herunterladens des Aktualisierungspaketes je nach Nutzungsszene warten, und die UX des Fahrers kann negativ sein.

[0007] Es ist eine Aufgabe der vorliegenden Erfindung, einen Durchsatz geeignet zu erhöhen, wenn eine Mastervorrichtung Aktualisierungsdaten von einer Zentrumsvorrichtung herunterlädt.

[0008] Gemäß einem Aspekt der vorliegenden Erfindung werden eine Zentrumsvorrichtung, die Aktualisierungsdaten an eine Mastervorrichtung verteilt bzw. liefert bzw. zuführt, und eine Mastervorrichtung, die die Aktualisierungsdaten, die von der Zentrumsvorrichtung heruntergeladen wurden, in einer neu zu programmierenden elektronischen Steuerungseinheit installiert, bereitgestellt. Die Zentrumsvorrichtung und die Mastervorrichtung verwenden einen Zählermodus (CTR) als ein Verschlüsselungsverfahren und ein Entschlüsselungsverfahren der Aktualisierungsdaten.

[0009] In der Konfiguration, bei der CBC-Modus als das Verschlüsselungsverfahren und das Entschlüsselungsverfahren verwendet wird, gibt es Nachteile dahingehend, dass es nicht möglich ist, eine Vorbereitung zur Verschlüsselung und Entschlüsselung durchzuführen, es nicht möglich ist, den parallelen Prozess der Verschlüsselung durchzuführen, und Ähnliches. Andererseits gibt es in der Konfiguration, in der der CTR-Modus als das Verschlüsselungsverfahren und das Entschlüsselungsverfahren verwendet wird, den Vorteil einer Verbesserung des Durchsatzes derart, dass es möglich ist, eine Vorbereitung zur Verschlüsselung und Entschlüsselung durchzuführen, und es möglich ist, den parallelen Prozess der Verschlüsselung und Entschlüsselung durchzuführen. Der CTR-Modus, der zu der Verbesserung des Durchsatzes beiträgt, wird im Vergleich zu dem herkömmlichen Verfahren, das den CBC-Modus verwendet, verwendet. Es ist möglich, den Durchsatz geeignet zu erhöhen, wenn die Mastervorrichtung die Aktualisierungsdaten von der Zentrumsvorrichtung herunterlädt.

[0010] Gemäß einem Aspekt der vorliegenden Erfindung werden eine Zentrumsvorrichtung, die Aktualisierungsdaten an eine Mastervorrichtung verteilt, und eine Mastervorrichtung, die die Aktualisierungsdaten, die von der Zentrumsvorrichtung heruntergeladen werden, in einer neu zu programmierenden elektronischen Steuerungseinheit installiert, bereitgestellt. Die Zentrumsvorrichtung und die Mastervorrichtung verwenden einen Ausgangsrückführungsmodus (OFB-Modus) als ein Verschlüsselungsverfahren und ein Entschlüsselungsverfahren der Aktualisierungsdaten.

[0011] In der Konfiguration, in der der CBC-Modus als das Verschlüsselungsverfahren und das Entschlüsselungsverfahren verwendet wird, gibt es Nachteile dahingehend, dass es nicht möglich ist, eine Vorbereitung zur Verschlüsselung und Entschlüsselung durchzuführen, es nicht möglich ist, den parallelen Prozess der Verschlüsselung durchzuführen, und Ähnliches. Andererseits gibt es in der Konfiguration, in der der OFB-Modus als das Verschlüsselungsverfahren und das Entschlüsselungsverfahren verwendet wird, den Vorteil der Verbesserung des Durchsatzes derart, dass es möglich ist, eine Vorbereitung zur Verschlüsselung und Entschlüsselung durchzuführen. Der OFB-Modus, der zu der Verbesserung des Durchsatzes beiträgt, wird im Vergleich zu dem herkömmlichen Verfahren verwendet, das den CBC-Modus verwendet. Es ist möglich, den Durchsatz geeignet zu erhöhen, wenn die Mastervorrichtung die Aktualisierungsdaten von der Zentrumsvorrichtung herunterlädt.

Kurze Beschreibung der Zeichnungen

[0012] Die obige Aufgabe und weitere Aufgaben, Merkmale und Vorteile der vorliegenden Erfindung werden anhand der folgenden detaillierten Beschreibung mit Bezug auf die zugehörigen Zeichnungen deutlich. Es zeigen:

Fig. 1 ein Diagramm, das einen Fluss eines Prozesses in einem gesamten System gemäß der ersten Ausführungsform darstellt;

Fig. 2 ein Funktionsblockdiagramm eines OTA-Zentrums und eines OTA-Masters;

Fig. 3 ein Diagramm zum Beschreiben eines Verschlüsselungsprozesses in einem CTR-Modus;

Fig. 4 ein Diagramm zum Beschreiben eines Entschlüsselungsprozesses in einem CTR-Modus;

Fig. 5 ein Diagramm, das einen Vergleich zwischen Vorteilen und Nachteilen eines CBC-Modus und eines CTR-Modus darstellt;

Fig. 6 ein Diagramm, das einen Vergleich eines Durchsatzes zwischen einem CBC-Modus und einem CTR-Modus darstellt;

Fig. 7 ein Diagramm zum Beschreiben eines Entschlüsselungsprozesses in einem CBC-Modus;

Fig. 8 ein Diagramm zum Beschreiben eines Entschlüsselungsprozesses in einem CTR-Modus;

Fig. 9 ein Diagramm, das einen Prozess eines OTA-Zentrums darstellt;

Fig. 10 ein Diagramm, das einen Prozess des Zentrums darstellt;

Fig. 11 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 12 ein Diagramm, das einen Prozess eines OTA-Masters darstellt;

Fig. 13 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 14 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 15 ein Diagramm zum Beschreiben eines Verschlüsselungsprozesses in einem OFB-Modus gemäß der zweiten Ausführungsform;

Fig. 16 ein Diagramm zum Beschreiben eines Entschlüsselungsprozesses in einem OFB-Modus;

Fig. 17 ein Diagramm, das einen Vergleich von Vorteilen und Nachteilen zwischen dem CBC-Modus und dem OFB-Modus darstellt;

Fig. 18 ein Diagramm, das einen Vergleich eines Durchsatzes zwischen einem CBC-Modus und einem OFB-Modus darstellt;

Fig. 19 ein Diagramm zum Beschreiben eines Entschlüsselungsprozesses in einem CTR-Modus;

Fig. 20 ein Diagramm zum Beschreiben eines Entschlüsselungsprozesses in einem OFB-Modus;

Fig. 21 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 22 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 23 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 24 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 25 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 26 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 27 ein Diagramm, das einen Fluss eines Prozesses in dem gesamten System gemäß der dritten Ausführungsform darstellt;

Fig. 28 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 29 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 30 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 31 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 32 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 33 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 34 ein Diagramm, das einen Fluss eines Prozesses in dem gesamten System gemäß der vierten Ausführungsform darstellt;

Fig. 35 ein Funktionsblockdiagramm des OTA-Zentrums und des OTA-Masters;

Fig. 36 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 37 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 38 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 39 ein Diagramm, das einen Prozess des OTA-Masters gemäß der fünften Ausführungsform darstellt;

Fig. 40 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 41 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 42 ein Diagramm, das eine Beziehung zwischen einer Speicherkapazität und einer Zugriffsgeschwindigkeit darstellt;

Fig. 43 ein Diagramm, das einen Fluss eines Prozesses in dem gesamten System gemäß der sechsten Ausführungsform darstellt;

Fig. 44 ein Funktionsblockdiagramm des OTA-Zentrums und des OTA-Masters;

Fig. 45 ein Diagramm, das einen Modus darstellt, bei dem RP-Metadaten übertragen werden;

Fig. 46 ein Diagramm, das eine Konfiguration der RP-Metadaten darstellt;

Fig. 47 ein Diagramm, das eine Konfiguration der RP-Metadaten darstellt;

Fig. 48 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 49 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 50 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 51 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 52 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 53 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 54 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 55 ein Diagramm, das einen Fluss eines Prozesses in dem gesamten System gemäß der siebten Ausführungsform darstellt;

Fig. 56 eine Funktion in einem CCMP-Modus;

Fig. 57 ein Diagramm zum Beschreiben einer Schätzung eines Durchsatzes in dem CCMP-Modus;

Fig. 58 ein Funktionsblockdiagramm eines herkömmlichen Verfahrens;

Fig. 59 ein Diagramm zum Beschreiben einer Schätzung eines Durchsatzes durch ein herkömmliches Verfahren;

Fig. 60 ein Diagramm, das einen Vergleich des Durchsatzes zwischen dem CCMP-Modus und dem herkömmlichen Verfahren darstellt;

Fig. 61 ein Funktionsblockdiagramm des OTA-Zentrums und des OTA-Masters;

Fig. 62 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 63 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 64 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 65 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 66 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 67 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 68 ein Diagramm, das einen Fluss eines Prozesses in dem gesamten System gemäß der achten Ausführungsform darstellt;

Fig. 69 ein Funktionsblockdiagramm in einem GCMP-Modus;

Fig. 70 ein Diagramm zum Beschreiben einer Schätzung eines Durchsatzes in dem GCMP-Modus;

Fig. 71 ein Diagramm, das einen Vergleich eines Durchsatzes zwischen dem GCMP-Modus und dem herkömmlichen Verfahren darstellt;

Fig. 72 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 73 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 74 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 75 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 76 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 77 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 78 ein Diagramm, das einen Fluss eines Prozesses in dem gesamten System gemäß der neunten Ausführungsform darstellt;

Fig. 79 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 80 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 81 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 82 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 83 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 84 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 85 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 86 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 87 ein Diagramm, das einen Fluss eines Prozesses in dem gesamten System gemäß der zehnten Ausführungsform darstellt;

Fig. 88 ein Diagramm, das einen Kostenvergleich eines CDN darstellt;

Fig. 89 ein Diagramm, das einen Kostenvergleich eines CDN darstellt;

Fig. 90 ein Diagramm, das eine CDN-Preistabelle jeweiliger Cloud-Dienste darstellt;

Fig. 91 ein Diagramm, das eine Preistabelle eines Speicherverfahrens jeweiliger Cloud-Dienst-Geschäftsbetreiber darstellt;

Fig. 92 ein Diagramm, das eine Preistabelle für jeweilige Streaming-Größen in einem Streaming-Verfahren jeweiliger Cloud-Dienst-Geschäftsbetreiber darstellt;

Fig. 93 ein Diagramm, das eine Preistabelle für jeweilige Streaming-Größen in dem Streaming-Verfahren jeweiliger Cloud-Dienst-Geschäftsbetreiber darstellt;

Fig. 94 ein Funktionsblockdiagramm des OTA-Zentrums und des OTA-Masters;

Fig. 95 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 96 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 97 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 98 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 99 ein Diagramm, das einen Fluss eines Prozesses in dem gesamten System gemäß der elften Ausführungsform darstellt;

Fig. 100 ein Diagramm, das einen gemeinsamen Schlüssel für einen Schlüsselaustausch durch DHE oder ECDHE;

Fig. 101 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 102 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 103 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 104 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 105 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 106 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 107 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 108 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 109 ein Diagramm, das einen Fluss eines Prozesses in dem gesamten System gemäß der zwölften Ausführungsform darstellt;

Fig. 110 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 111 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 112 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 113 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 114 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 115 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 116 ein Diagramm, das einen Fluss eines Prozesses in dem gesamten System gemäß der dreizehnten Ausführungsform darstellt;

Fig. 117 ein Diagramm zum Beschreiben eines Verschlüsselungsprozesses in dem CTR-Modus;

Fig. 118 ein Diagramm zum Beschreiben eines Entschlüsselungsprozesses in dem CTR-Modus;

Fig. 119 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 120 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 121 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 122 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 123 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 124 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 125 ein Diagramm, das einen Fluss eines Prozesses in dem gesamten System gemäß der vierzehnten Ausführungsform darstellt;

Fig. 126 ein Diagramm zum Beschreiben von individuellen AES-Schlüsseln;

Fig. 127 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 128 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 129 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 130 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 131 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 132 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 133 ein Diagramm, das einen Fluss eines Prozesses in dem gesamten System gemäß der fünfzehnten Ausführungsform darstellt;

Fig. 134 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 135 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 136 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 137 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 138 ein Diagramm, das einen Fluss eines Prozesses in dem gesamten System gemäß der sechzehnten Ausführungsform darstellt;

Fig. 139 ein Diagramm, das einen Angriff von einem Zwischenangreifer darstellt;

Fig. 140 ein Diagramm, das einen Modus darstellt, bei dem eine digitale Signatur zugewiesen wird;

Fig. 141 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 142 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 143 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 144 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 145 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 146 ein Diagramm, das einen Fluss eines Prozesses in dem gesamten System gemäß der siebzehnten Ausführungsform darstellt;

Fig. 147 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 148 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 149 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 150 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 151 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 152 ein Diagramm, das einen Fluss eines Prozesses in dem gesamten System gemäß der achtzehnten Ausführungsform darstellt;

Fig. 153 ein Diagramm, das eine CDN-Preistabelle jeweiliger Cloud-Dienste darstellt,

Fig. 154 ein Diagramm, das eine CDN-Preistabelle jeweiliger Cloud-Dienste darstellt;

Fig. 155 ein Diagramm, das eine Preistabelle eines Speicherverfahrens jeweiliger Cloud-Dienst-Geschäftsbetreiber darstellt;

Fig. 156 ein Diagramm, das eine Preistabelle eines Speicherverfahrens jeweiliger Cloud-Dienst-Geschäftsbetreiber darstellt;

Fig. 157 ein Diagramm, das eine Preistabelle jeweilige Streaming-Größen in dem Streaming-Verfahren jeweiliger Cloud-Dienst-Geschäftsbetreiber darstellt;

Fig. 158 ein Diagramm, das eine Preistabelle für jeweilige Streaming-Größen in dem Streaming-Verfahren jeweiliger Cloud-Dienst-Geschäftsbetreiber darstellt;

Fig. 159 ein Diagramm, das eine Preistabelle für jeweilige Streaming-Größen in dem Streaming-Verfahren jeweiliger Cloud-Dienst-Geschäftsbetreiber darstellt;

Fig. 160 ein Diagramm, das eine Preistabelle für jeweilige Streaming-Größen in dem Streaming-Verfahren jeweiliger Cloud-Dienst-Geschäftsbetreiber darstellt;

Fig. 161 ein Diagramm, das Qualitätsinformationen jeweiliger Cloud-Dienst-Geschäftsbetreiber darstellt;

Fig. 162 ein Diagramm zum Beschreiben einer Auswahl eines CDN-Verkäufers;

Fig. 163 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 164 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 165 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 166 ein Diagramm, das eine Modifikation der elften Ausführungsform zeigt und das einen Teil eines Flusses eines Prozesses in dem gesamten System zeigt;

Fig. 167 ein Diagramm, das einen Teil eines Flusses eines Prozesses in dem gesamten System darstellt;

Fig. 168 ein Diagramm, das einen Teil eines Flusses eines Prozesses in dem gesamten System darstellt;

Fig. 169 ein Diagramm, das einen Teil eines Flusses eines Prozesses in dem gesamten System darstellt;

Fig. 170 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 171 ein Diagramm, das einen Prozess des PC darstellt;

Fig. 172 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 173 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 174 ein Diagramm, das eine Modifikation der zwölften Ausführungsform zeigt und einen Teil eines Flusses eines Prozesses in dem gesamten System darstellt;

Fig. 175 ein Diagramm, das einen Teil eines Flusses eines Prozesses in dem gesamten System darstellt;

Fig. 176 ein Diagramm, das einen Teil eines Flusses eines Prozesses in dem gesamten System darstellt;

Fig. 177 ein Diagramm, das einen Teil eines Flusses eines Prozesses in dem gesamten System darstellt;

Fig. 178 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 179 ein Diagramm, das einen Prozess des PC darstellt;

Fig. 180 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 181 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 182 ein Diagramm, das eine Modifikation der sechzehnten Ausführungsform zeigt und einen Teil eines Flusses eines Prozesses in dem gesamten System darstellt;

Fig. 183 ein Diagramm, das einen Teil eines Flusses eines Prozesses in dem gesamten System darstellt;

Fig. 184 ein Diagramm, das einen Teil eines Flusses eines Prozesses in dem gesamten System darstellt;

Fig. 185 ein Diagramm, das einen Teil eines Flusses eines Prozesses in dem gesamten System darstellt;

Fig. 186 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 187 ein Diagramm, das einen Prozess des PC darstellt;

Fig. 188 ein Diagramm, das einen Prozess des OTA-Zentrums darstellt;

Fig. 189 ein Diagramm, das einen Prozess des OTA-Masters darstellt;

Fig. 190 ein Diagramm, das einen Fluss eines Prozesses in dem gesamten System gemäß der neunzehnten Ausführungsform darstellt;

Fig. 191 ein Diagramm, das einen Prozess des Kampagnenmeldungserzeugungsabschnittes zeigt;

Fig. 192 ein Diagramm, das einen Prozess des CDN-Verkäuferauswahlabschnittes darstellt;

Fig. 193 ein Diagramm, das einen Prozess des CDN-Verkäuferauswahlabschnittes darstellt;

Fig. 194 ein Diagramm, das einen Fluss eines Prozesses in dem gesamten System gemäß der ersten Modifikation der neunzehnten Ausführungsform darstellt;

Fig. 195 ein Diagramm, das einen Prozess des CDN-Verkäuferauswahlabschnittes darstellt;

Fig. 196 ein Diagramm, das einen Fluss eines Prozesses in dem gesamten System gemäß der zweiten Modifikation der neunzehnten Ausführungsform darstellt;

Fig. 197 eine Ansicht, die eine Auswahltable darstellt;

Fig. 198 ein Diagramm, das einen Prozess des CDN-Verkäuferauswahlabschnittes darstellt;

Fig. 199 ein Diagramm, das einen Prozess des CDN-Verkäuferauswahlabschnittes darstellt;

Fig. 200 ein Diagramm, das einen Prozess des Leistungsmessabschnittes darstellt;

Fig. 201 ein Diagramm, das einen Prozess des CDN-Serververifizierungsabschnittes darstellt;

Fig. 202 ein Diagramm, das einen Fluss eines Prozesses in dem gesamten System gemäß der dritten Modifikation der neunzehnten Ausführungsform darstellt;

Fig. 203 ein Diagramm, das einen Prozess des Protokollübertragungsabschnittes 3a darstellt;

Fig. 204 ein Diagramm, das einen Prozess des Leistungsmessabschnittes darstellt;

Fig. 205 ein Diagramm, das einen Prozess des Leistungsmessabschnittes darstellt;

Fig. 206 ein Diagramm, das die vierte Modifikation der neunzehnten Ausführungsform zeigt und einen Prozess des CDN-Verkäuferauswahlabschnittes 7a darstellt;

Fig. 207 ein Diagramm, das einen Prozess des Kampagnenmeldungserzeugungsabschnittes darstellt;

Fig. 208 ein Diagramm, das einen Fluss eines Prozesses in dem gesamten System gemäß der fünften Modifikation der neunzehnten Ausführungsform darstellt;

Fig. 209 ein Diagramm, das eine Round-Robin-Aufzeichnung darstellt;

Fig. 210 ein Diagramm, das einen Prozess des CDN-Verkäuferauswahlabschnittes 7a darstellt;

Fig. 211 ein Diagramm, das einen Prozess des Wechselabschnittes darstellt;

Fig. 212 ein Diagramm, das einen Fluss eines Prozesses in dem gesamten System gemäß der zwanzigsten Ausführungsform darstellt;

Fig. 213 ein Diagramm, das ein Berechnungsverfahren darstellt;

Fig. 214 ein Diagramm, das einen Prozess des Kampagnenmeldungserzeugungsabschnittes zeigt;

Fig. 215 ein Diagramm, das einen Prozess des CDN-Verkäuferauswahlabschnittes darstellt;

Fig. 216 ein Diagramm, das einen Prozess des CDN-Verkäuferauswahlabschnittes darstellt;

Fig. 217 ein Diagramm, das einen Prozess des CDN-Verkäuferauswahlabschnittes darstellt;

Fig. 218 ein Diagramm, das einen Prozess des CDN-Verkäuferauswahlabschnittes darstellt;

Fig. 219 ein Diagramm, das einen Prozess des CDN-Verkäuferauswahlabschnittes darstellt;

Fig. 220 ein Diagramm, das einen Prozess des CDN-Verkäuferauswahlabschnittes darstellt;

Fig. 221 ein Diagramm, das einen Prozess des CDN-Verkäuferauswahlabschnittes darstellt;

Fig. 222 ein Diagramm, das einen Prozess des Fortschrittsinformationsverwaltungsabschnittes darstellt;

Fig. 223 ein Diagramm, das einen Prozess des CDN-Verkäuferauswahlabschnittes darstellt; und

Fig. 224 ein Diagramm, das einen Prozess des Kampagnenmeldungserzeugungsabschnittes darstellt.

Beschreibung der Ausführungsformen

[0013] Im Folgenden werden mehrere Ausführungsformen mit Bezug auf die Zeichnungen beschrieben. In den folgenden Ausführungsformen wird nach Bedarf die Beschreibung eines Inhaltes, der bereits in einer vorhergehenden Ausführungsform beschrieben wurde, weggelassen.

Erste Ausführungsform

[0014] Die erste Ausführungsform wird mit Bezug auf die **Fig. 1** bis **14** beschrieben. Wie es in **Fig. 1** dargestellt ist, enthält ein Datenkommunikationssystem 1 ein OTA-Zentrum 2 und ein fahrzeugseitiges System 3, das an einem Fahrzeug montiert ist, und das OTA-Zentrum 2 und das fahrzeugseitige System 3 sind in der Lage, eine Datenkommunikation durchzuführen. Das OTA-Zentrum 2 entspricht einer Zentrumsvorrichtung. Das OTA-Zentrum 2 und das fahrzeugseitige System 3 weisen eine Einzahl-zu-Mehrzahl-Beziehung auf, und das OTA-Zentrum 2 kann eine Datenkommunikation mit einer unspezifizierten Anzahl von fahrzeugseitigen Systemen 3 durchführen.

[0015] Das fahrzeugseitige System 3 enthält einen OTA-Master 4 und eine Ziel-ECU 5. Der OTA-Master 4 entspricht einer Mastervorrichtung. Der OTA-Master 4 und die Ziel-ECU 5 sind mit einem fahrzeugeigenen Netzwerk wie beispielsweise einem Steuerbereichsnetzwerk (CAN) (eingetragene Marke) verbunden und können Daten über das fahrzeugeigene Netzwerk austauschen. Das fahrzeugeigene Netzwerk kann ein lokales Verbindungsnetzwerk (LIN), FlexRay (eingetragene Marke), CAN mit flexibler Datenrate (CAN FD) (eingetragene Marke), Ethernet (eingetragene Marke) oder Ähnliches sein. Die Ziel-ECU 5 ist eine ECU, die ein Neuprogrammierungsziel des Anwendungsprogramms ist, und kann beispielsweise eine ECU, die ein automatisiertes Fahrsystem steuert, eine ECU, die ein ADAS-System steuert, eine ECU, die ein Multimediasystem steuert, oder Ähnliches sein. Das Anwendungsprogramm ist ein Programm betreffend die Ausführung einer Anwendung und beinhaltet beispielsweise ein Anwendungsprogramm, ein Firmware-Programm und/oder ein Betriebssystem-Programm.

[0016] Das OTA-Zentrum 2 enthält einen Paketerzeugungsserver 6 und einen Verteilungsserver 7. Der Paketerzeugungsserver 6 ist ein Server, der eine Funktion zum Packen von Aktualisierungsdaten aufweist, um ein Aktualisierungspaket zu erzeugen. Das Aktualisierungspaket ist beispielsweise eine Zip-Datei, in der mehrere Dateien, in der Aktualisierungs-

daten gespeichert sind, komprimiert und gespeichert sind. Der Verteilungsserver 7 ist ein Server, der eine Funktion zum Verteilen bzw. Liefern bzw. Zuführen des Aktualisierungspaketes, das durch den Paketerzeugungsserver 6 erzeugt wurde, an das fahrzeugseitige System 3 aufweist.

[0017] Das OTA-Zentrum 2 verteilt eine Kampagnenmeldung an das fahrzeugseitige System 3 oder ein mobiles Informationsendgerät wie beispielsweise ein Smartphone eines Nutzers, wenn beispielsweise eine Neuprogrammierungsanfrage für ein Anwendungsprogramm der ECU entsprechend einem Versions-Upgrade zur Funktionsverbesserung oder Ähnlichem erzeugt wird. Das OTA-Zentrum 2 platziert ein Aktualisierungspaket in einem Inhaltsliefernetzwerk (im Folgenden als CDN abgekürzt) 8 und verteilt das Aktualisierungspaket an den OTA-Master 4 über das CDN 8 unter der Bedingung, dass eine Herunterladeerlaubnis bzw. -bewilligung bzw. Download-Bewilligung von dem Nutzer erhalten wurde. In einem Fall, in dem das Aktualisierungspaket bereits in dem CDN 8 platziert wurde, verteilt alternativ das OTA-Zentrum 2 das Aktualisierungspaket von dem CDN 8 an den OTA-Master 4 unter der Bedingung, dass die Download-Bewilligung von dem Nutzer erhalten wurde.

[0018] Wenn der OTA-Master 4 das Aktualisierungspaket von dem OTA-Zentrum 2 herunterlädt oder heruntergeladen hat, überträgt der OTA-Master 4 das Aktualisierungspaket an die Ziel-ECU 5 und installiert das Aktualisierungspaket in der Ziel-ECU 5 unter der Bedingung, dass die Installationsbewilligung von dem Nutzer erhalten wird bzw. wurde. Ein Geschäftsbetreiber, der das CDN 8 als einen Dienst bereitstellt, wird als CDN-Verkäufer bezeichnet. Außerdem beschafft der OTA-Master 4 das Aktualisierungspaket durch Zugreifen auf den CDN-Server des CDN 8. Der Begriff „beschaffen“ bedeutet im Folgenden auch „erlangen“ oder „empfangen“ oder „erhalten“.

[0019] Um den Entschlüsselungsprozess des fortgeschrittenen Verschlüsselungsstandards (Advanced Encryption Standard, im Folgenden als AES abgekürzt) in dem fahrzeugseitigen System 3 zu beschleunigen, wird in der vorliegenden Ausführungsform nicht der Chiffrierungsblockkettenmodus (Cipher Block Chaining, im Folgenden als CBC-Modus abgekürzt) einer allgemeinen Blockverschlüsselung, sondern der Zählermodus (Counter, im Folgenden als CTR-Modus abgekürzt), der für eine Streaming-Verschlüsselung repräsentativ ist, als der Verschlüsselungsmodus verwendet. In der vorliegenden Ausführungsform verschlüsselt das OTA-Zentrum 2 das Aktualisierungspaket mit dem AES-Schlüssel in dem CTR-Modus. Außerdem verschlüsselt das fahrzeugseitige System 3 das Aktualisierungspaket mit dem AES-Schlüssel in dem CTR-

Modus. Das OTA-Zentrum 2 enthält einen öffentlichen RSA-Schlüssel (RSA: Rivest-Shamir-Adleman Cryptosystem) für jedes Fahrzeug. Ein geheimer RSA-Schlüssel wird in der Fahrzeugherstellungsstufe in den OTA-Master 4 geschrieben.

[0020] Wie es in **Fig. 2** dargestellt ist, enthält das OTA-Zentrum 2 als Funktionsblöcke betreffend die Verschlüsselung einen Gemeinsamer-Schlüssel-Erzeugungsabschnitt 2a, einen Aktualisierungspaketverschlüsselungsabschnitt 2b, einen Gemeinsamer-Schlüssel-Verschlüsselungsabschnitt 2c, einen Gemeinsamer-Schlüssel-Speicherabschnitt 2d, einen Verschlüsselungspaketplatzierungsabschnitt 2e und einen Kampagnenmeldungsübertragungsabschnitt 2f. Der Aktualisierungspaketverschlüsselungsabschnitt 2b entspricht einem Aktualisierungsdatenverschlüsselungsabschnitt. Der Verschlüsselungspaketplatzierungsabschnitt 2e entspricht einem Verschlüsselungsdatenplatzierungsabschnitt. Jeder der Abschnitte 2a bis 2f wird durch Kooperation von Hardware und Software eines Mikrocomputers realisiert, der eine zentrale Verarbeitungseinheit (CPU), einen Speicher mit wahlfreiem Zugriff (RAM), einen Nur-Lese-Speicher (ROM), eine Eingabe/Ausgabe-Schnittstelle (IO) und Ähnliches enthält. Die CPU realisiert die Funktion des OTA-Zentrums 2 durch Ausführen von verschiedenen Programmen einschließlich einem Verschlüsselungsprogramm, einem Aktualisierungsdatenplatzierungsprogramm, einem Geheiminformationsaustauschprogramm und Ähnlichem, die in dem ROM gespeichert sind.

[0021] Der Gemeinsamer-Schlüssel-Erzeugungsabschnitt 2a erzeugt einen AES-Schlüssel als einen gemeinsamen Schlüssel zur Verschlüsselung des Aktualisierungspaketes. Der Paketverschlüsselungsabschnitt 2b verschlüsselt das Aktualisierungspaket mit dem erzeugten AES-Schlüssel in dem CTR-Modus. Der Paketverschlüsselungsabschnitt 2b führt einen AES-Blockverschlüsselungsprozess hinsichtlich des Zählerwertes mit dem AES-Schlüssel durch, um den Zählerwert zu verschlüsseln. Der Paketverschlüsselungsabschnitt 2b führt einen Ausschließlich-Oder-Betrieb bzw. eine XOR-Operation (XOR) hinsichtlich des verschlüsselten Zählerwertes und des Aktualisierungspaketes durch, kombiniert die verschlüsselten Fragmente und erzeugt ein Aktualisierungspaket, das mit dem AES-Schlüssel verschlüsselt ist. Der Zählerwert ist beispielsweise eine achtstellige Zahl und erhöht sich jeden AES-Block um „1“.

[0022] Der Gemeinsamer-Schlüssel-Verschlüsselungsabschnitt 2c verschlüsselt den AES-Schlüssel mit dem öffentlichen RSA-Schlüssel. Der Gemeinsamer-Schlüssel-Speicherabschnitt 2d speichert den AES-Schlüssel, der mit dem öffentlichen RSA-Schlüssel verschlüsselt ist, in der Kampagnenmel-

dung. Der Verschlüsselungspaketplatzierungsabschnitt 2e platziert das Aktualisierungspaket, das mit dem AES-Schlüssel verschlüsselt ist, in dem CDN 8. Der Kampagnenmeldungsübertragungsabschnitt 2f überträgt eine Kampagnenmeldung, in der der verschlüsselte AES-Schlüssel gespeichert ist, an das neu zu programmierende fahrzeugseitige System 3. Der Kampagnenmeldungsübertragungsabschnitt 2f kann die Kampagnenmeldung an ein mobiles Informationsendgerät wie beispielsweise ein Smartphone des Nutzers verteilen.

[0023] Der OTA-Master 4 enthält einen Gemeinsamer-Schlüssel-Beschaffungsabschnitt 4a, einen Gemeinsamer-Schlüssel-Entschlüsselungsabschnitt 4b, einen Verschlüsselungspaketbeschaffungsabschnitt 4c, einen Blockverschlüsselungsverarbeitungsabschnitt 4d, einen Verschlüsselungspaketentschlüsselungsabschnitt 4e und einen Installationsverarbeitungsabschnitt 4f als Funktionsblöcke betreffend eine Entschlüsselung. Der Verschlüsselungspaketbeschaffungsabschnitt 4c entspricht einem Verschlüsselungsdatenbeschaffungsabschnitt. Der Verschlüsselungspaketentschlüsselungsabschnitt 4a entspricht einem Verschlüsselungsdatenentschlüsselungsabschnitt. Jeder der Abschnitte 4a bis 4f wird durch Kooperation von Hardware und Software eines Mikrocomputers realisiert, der eine CPU, einen RAM, einen ROM, eine I/O-Schnittstelle und Ähnliches enthält. Die CPU realisiert die Funktion des OTA-Masters 4 durch Ausführen von verschiedenen Programmen einschließlich eines Entschlüsselungsprogramms, eines Aktualisierungsdatenbeschaffungsprogramms, eines Geheiminformationsaustauschprogramms und Ähnlichem, die in dem ROM gespeichert sind.

[0024] Wenn der Gemeinsamer-Schlüssel-Beschaffungsabschnitt 4a die Kampagnenmeldung beschafft, da die Kampagnenmeldung, die von dem OTA-Zentrum 2 übertragen wird, von dem OTA-Master 4 empfangen wird, beschafft der Gemeinsamer-Schlüssel-Beschaffungsabschnitt 4a einen verschlüsselten AES-Schlüssel aus der beschafften Kampagnenmeldung. Der Gemeinsamer-Schlüssel-Entschlüsselungsabschnitt 4b entschlüsselt den verschlüsselten AES-Schlüssel mit dem geheimen RSA-Schlüssel, um den AES-Schlüssel zu extrahieren. Der Verschlüsselungspaketbeschaffungsabschnitt 4c lädt und beschafft das verschlüsselte Aktualisierungspaket von dem CDN 8. Gleichzeitig führt der Blockverschlüsselungsverarbeitungsabschnitt 4d parallel zu dem Verschlüsselungspaketbeschaffungsabschnitt 4c, der das verschlüsselte Aktualisierungspaket von dem CDN 8 herunterlädt und beschafft, einen AES-Blockverschlüsselungsprozess des Zählerwertes mit dem AES-Schlüssel aus, um den Zählerwert zu verschlüsseln. Der Verschlüsselungspaketentschlüsselungsabschnitt 4e

führt einen Ausschließlich-Oder-Betrieb (XOR-Betrieb) des verschlüsselten Zählerwertes und des verschlüsselten Aktualisierungspaketes, das von dem CDN 8 heruntergeladen wurde, durch, um den Zählerwert und das verschlüsselte Aktualisierungspaket zu entschlüsseln. Der Installationsverarbeitungsabschnitt 4f überträgt das entschlüsselte Aktualisierungspaket an die Ziel-ECU 5 und installiert das Aktualisierungspaket in der Ziel-ECU 5.

[0025] Der Verschlüsselungsprozess in dem CTR-Modus ist in **Fig. 3** dargestellt, und der Entschlüsselungsprozess in dem CTR-Modus ist in **Fig. 4** dargestellt. Wie es in **Fig. 5** dargestellt ist, besteht der Vorteil des CTR-Modus darin, dass es möglich ist, eine Vorbereitung zur Verschlüsselung und Entschlüsselung durchzuführen, so dass eine hohe Geschwindigkeit möglich ist, und „es möglich ist, den parallelen Prozess zur Verschlüsselung und Entschlüsselung durchzuführen, wohingegen der Nachteil des CBC-Modus darin besteht, dass es nicht möglich ist, eine Vorbereitung zur Verschlüsselung und Entschlüsselung durchzuführen, und es nicht möglich ist, einen parallelen Prozess zur Verschlüsselung durchzuführen. D.h., als ein Vorteil des Beitrags zu der Verbesserung des Durchsatzes durch Verwendung des CTR-Modus als den Verschlüsselungsmodus kann der Durchsatz um etwa 40% im Vergleich zu dem Fall verbessert werden, in dem der CBC-Modus einer allgemeinen Blockverschlüsselung durchgeführt wird, wie es in **Fig. 6** dargestellt ist.

[0026] Wie es in **Fig. 7** dargestellt ist, kann, da in dem Entschlüsselungsprozess in dem CBC-Modus der Chiffrierungstext den Eingang bildet bzw. eingegeben wird, der Entschlüsselungsprozess nicht gestartet werden, bis das Aktualisierungspaket, das der Chiffrierungstext ist, empfangen wird. Wie es in **Fig. 8** dargestellt ist, kann andererseits in dem Entschlüsselungsprozess in dem CTR-Modus, da dort der Zählerwert eingegeben wird bzw. den Eingang bildet, der Entschlüsselungsprozess gestartet werden, bevor das Aktualisierungspaket, das der Chiffrierungstext ist, empfangen wird. Da es keine Abhängigkeitsbeziehung untereinander gibt, können außerdem mehrere kryptographische Betriebe gleichzeitig parallel ausgeführt werden.

[0027] Im Folgenden wird der Betrieb der oben beschriebenen Konfiguration mit Bezug auf die **Fig. 9** bis **14** beschrieben.

(1-1) Prozess des OTA-Zentrums 2 (siehe Figuren 9 bis 11)

[0028] Das OTA-Zentrum 2 erzeugt einen AES-Schlüssel zum Verschlüsseln des Aktualisierungspaketes (A011, entspricht einem Gemeinsamer-Schlüssel-Erzeugungsschritt). Das OTA-Zentrum 2 verschlüsselt das Aktualisierungspaket mit dem

erzeugten AES-Schlüssel in dem CTR-Modus (A012, entspricht einem Aktualisierungsdatenverschlüsselungsschritt). Das OTA-Zentrum 2 verschlüsselt den AES-Schlüssel mit dem öffentlichen RSA-Schlüssel (A013, entspricht einem Gemeinsamer-Schlüssel-Verschlüsselungsschritt). Das OTA-Zentrum 2 speichert den AES-Schlüssel, der mit dem öffentlichen RSA-Schlüssel verschlüsselt ist, in der Kampagnenmeldung (A014, entspricht einem Gemeinsamer-Schlüssel-Speicherschritt). Das OTA-Zentrum 2 platziert das aktualisierte Paket, das mit dem AES-Schlüssel verschlüsselt ist, in dem CDN 8 (A015, entspricht einem Verschlüsselungsdatenplatzierungsschritt). Eine Platzierung des Aktualisierungspaketes in dem CDN 8 gibt eine Platzierung des Aktualisierungspaketes in dem Ursprungs-Server des CDN 8 an. Das OTA-Zentrum 2 überträgt eine Kampagnenmeldung, in der der verschlüsselte AES-Schlüssel gespeichert ist, an das neu zu programmierende fahrzeugseitige System 3 (A016, entspricht einem Kampagnenmeldungsübertragungsschritt).

(1-2) Prozess des OTA-Masters 4 (siehe Figuren 12 bis 14)

[0029] Wenn der OTA-Master 4 eine Kampagnenmeldung beschafft, da die Kampagnenmeldung, die von dem OTA 2 übertragen wird, empfangen wird, beschafft der OTA-Master 4 einen AES-Schlüssel aus der beschafften Kampagnenmeldung (B011, entspricht einem Gemeinsamer-Schlüssel-Beschaffungsschritt). Der OTA-Master 4 entschlüsselt den verschlüsselten AES-Schlüssel mit dem geheimen RSA-Schlüssel, um den AES-Schlüssel zu extrahieren (B012, entspricht einem Gemeinsamer-Schlüssel-Entschlüsselungsschritt). Der OTA-Master 4 lädt und beschafft das verschlüsselte Aktualisierungspaket von dem CDN 8 (B013, entspricht dem Verschlüsselungsdatenbeschaffungsschritt).

[0030] Hier führt der OTA-Master 4 parallel zu einem Herunterladen und Beschaffen des verschlüsselten Aktualisierungspaketes von dem CDN 8 einen AES-Blockverschlüsselungsprozess des Zählerwertes mit dem AES-Schlüssel aus, um den Zählerwert zu verschlüsseln (B014, entspricht einem Blockverschlüsselungsverarbeitungsschritt). Der OTA-Master 4 führt einen XOR-Betrieb durch und entschlüsselt den verschlüsselten Zählerwert und das verschlüsselte Aktualisierungspaket, das von dem CDN 8 heruntergeladen wurde (B015, entspricht einem Verschlüsselungsdatenentschlüsselungsschritt). Der OTA-Master 4 überträgt das entschlüsselte Aktualisierungspaket an die Ziel-ECU 5 und installiert das Aktualisierungspaket in der Ziel-ECU 5 (B016, entspricht einem Installationsverarbeitungsschritt). Durch Verschlüsseln und Entschlüsseln des Differenzprogramms in dem Aktualisierungspaket in dem CTR-Modus anstelle des Verschlüsseln und Ent-

schlüsselns des Differenzprogramms in dem CBC-Modus kann der Durchsatz des Entschlüsselungsprozesses in der Ziel-ECU 5 um etwa 40% erhöht werden.

[0031] Wie es oben beschrieben ist, können gemäß der ersten Ausführungsform die folgenden vorteilhaften Wirkungen erzielt werden.

[0032] Der CTR-Modus wird als das Verschlüsselungsverfahren und das Entschlüsselungsverfahren des Aktualisierungspaketes verwendet. Unter Verwendung des CTR-Modus ist es möglich, eine Vorbereitung zum Verschlüsseln und Entschlüsseln durchzuführen, und es ist möglich, einen parallelen Prozess zum Verschlüsseln und Entschlüsseln im Vergleich zu dem herkömmlichen Fall durchzuführen, in dem der CBC-Modus verwendet wird. Als Ergebnis ist es möglich, die Vorteile des CTR-Modus zu genießen und geeignet den Durchsatz zu erhöhen, wenn der OTA-Master 4 das Aktualisierungspaket von dem OTA-Zentrum 2 herunterlädt.

Zweite Ausführungsform

[0033] Die zweite Ausführungsform wird mit Bezug auf die Fig. 15 bis 26 beschrieben. Während die erste Ausführungsform den CTR-Modus als den Verschlüsselungsmodus verwendet, verwendet die zweite Ausführungsform einen Ausgangsrückführungsmodus (im Folgenden als OFB-Modus bezeichnet) als den Verschlüsselungsmodus.

[0034] In diesem Fall verschlüsselt der Paketverschlüsselungsabschnitt 2b das Aktualisierungspaket mit dem erzeugten AES-Schlüssel in dem OFB-Modus. Parallel zu dem Herunterladen und Beschaffen des verschlüsselten Aktualisierungspaketes von dem CDN 8 durch den Verschlüsselungspaketbeschaffungsabschnitt 4c führt der Blockverschlüsselungsverarbeitungsabschnitt 4d einen Initialisierungsvektor-Wert-basierten (IV-basierten) AES-Stromverschlüsselungsprozess bzw. AES-Stream-Verschlüsselungsprozess mit einem AES-Schlüssel durch, um den IV-Wert zu verschlüsseln. Der IV-Wert ist ein Initialisierungsvektorkwert und gibt beispielsweise eine zufällig erzeugte Bitkette an. Der Verschlüsselungspaketentschlüsselungsabschnitt 4e führt einen XOR-Betrieb durch und entschlüsselt den verschlüsselten IV-Wert und das verschlüsselte Aktualisierungspaket, das von dem CDN 8 heruntergeladen wurde.

[0035] Der OFB-Modusverschlüsselungsprozess ist in Fig. 15 dargestellt, und der OFB-Modusentschlüsselungsprozess ist in Fig. 16 dargestellt. Wie es in Fig. 17 dargestellt ist, besteht der Vorteil des OFB-Modus darin, dass es möglich ist, eine Vorbereitung zum Verschlüsseln und Entschlüsseln durchzuführen, so dass eine hohe Geschwindigkeit möglich ist,

wohingegen der Nachteil des CBC-Modus darin besteht, dass es nicht möglich ist, eine Vorbereitung zum Verschlüsseln und Entschlüsseln durchzuführen, und es nicht möglich ist, einen parallelen Prozess zur Verschlüsselung durchzuführen. D.h., der Vorteil des Beitrags zu der Verbesserung des Durchsatzes durch den OFB-Modus als dem Verschlüsselungsmodus kann der Durchsatz um etwa 25% im Vergleich zu einem Fall verbessert werden, in dem der CBC-Modus einer allgemeinen Blockverschlüsselung verwendet wird, wie es in Fig. 18 dargestellt ist.

[0036] Wie es in Fig. 19 dargestellt ist, kann, da in dem Entschlüsselungsprozess in dem CTR-Modus der Zählerwert den Eingang bildet, der Entschlüsselungsprozess gestartet werden, bevor das Aktualisierungspaket, das der Chiffrierungstext ist, empfangen wird. Da es außerdem keine Abhängigkeitsbeziehung untereinander gibt, können mehrere kryptographische Betriebe gleichzeitig parallel ausgeführt werden. Wie es in Fig. 20 dargestellt ist, können andererseits in dem Entschlüsselungsprozess in dem OFB-Modus, in dem eine Abhängigkeitsbeziehung untereinander besteht, nicht mehrere kryptographische Betriebe gleichzeitig parallel ausgeführt werden. Es können jedoch ein Prozess zum Durchführen eines XOR-Betriebes, d.h. eine Entschlüsselung des verschlüsselten IV-Wertes und des verschlüsselten Aktualisierungspaketes, parallel ausgeführt werden. Daher kann in dem Entschlüsselungsprozess in dem OFB-Modus der Durchsatz nicht so viel wie in dem Entschlüsselungsprozess in dem in der ersten Ausführungsform beschriebenen CTR-Modus verbessert werden, aber der Durchsatz kann im Vergleich zum dem Fall verbessert werden, in dem der CBC-Modus verwendet wird.

[0037] Im Folgenden wird der Betrieb der oben beschriebenen Konfiguration mit Bezug auf die Fig. 21 bis 26 beschrieben.

(2-1) Prozess der OTA-Zentrums 2 (siehe Figuren 21 bis 23)

[0038] Das OTA-Zentrum 2 erzeugt einen AES-Schlüssel zum Verschlüsseln des Aktualisierungspaketes (A021, entspricht einem Gemeinsamer-Schlüssel-Erzeugungsschritt). Das OTA-Zentrum 2 verschlüsselt das Aktualisierungspaket mit dem erzeugten AES-Schlüssel in dem OFB-Modus (A022, entspricht einem Aktualisierungsdatenverschlüsselungsschritt). Das OTA-Zentrum 2 verschlüsselt den AES-Schlüssel mit dem öffentlichen RSA-Schlüssel (A023, entspricht einem Gemeinsamer-Schlüssel-Verschlüsselungsschritt). Das OTA-Zentrum 2 speichert den AES-Schlüssel, der mit dem öffentlichen RSA-Schlüssel verschlüsselt ist, in der Kampagnenmeldung (A024, entspricht einem

Gemeinsamer-Schlüssel-Speicherschritt). Das OTA-Zentrum 2 platziert das Aktualisierungspaket, das mit dem AES-Schlüssel verschlüsselt ist, in dem CDN 8 (A025, entspricht einem Verschlüsselungsdatenplatzierungsschritt). Das OTA-Zentrum 2 überträgt eine Kampagnenmeldung, in der der verschlüsselte AES-Schlüssel gespeichert ist, an das neu zu programmierende fahrzeugseitige System 3 (A026, entspricht einem Kampagnenmeldungsübertragungsschritt).

(2-2) Prozess des OTA-Masters 4 (siehe Figuren 24 bis 26)

[0039] Wenn der OTA-Master 4 eine Kampagnenmeldung beschafft, die Kampagnenmeldung, die von dem OTA-Zentrum 2 übertragen wird, von dem OTA-Master 4 empfangen wird, beschafft der OTA-Master 4 den AES-Schlüssel aus der beschafften Kampagnenmeldung (B021, entspricht einem Gemeinsamer-Schlüssel-Beschaffungsschritt). Der OTA-Master 4 entschlüsselt den verschlüsselten AES-Schlüssel mit dem geheimen RSA-Schlüssel, um den AES-Schlüssel zu extrahieren (B022, entspricht einem Gemeinsamer-Schlüssel-Entschlüsselungsschritt). Der OTA-Master 4 lädt und beschafft das verschlüsselte Aktualisierungspaket von dem CDN 8 (B023, entspricht einem Verschlüsselungsdatenbeschaffungsschritt).

[0040] Zu dieser Zeit führt der OTA-Master 4 parallel zu einem Herunterladen und Beschaffen des verschlüsselten Aktualisierungspaketes von dem CDN 8 den IV-Wert-basierten AES-Stromverschlüsselungsprozess mit dem AES-Schlüssel durch, um den IV-Wert zu verschlüsseln (B024, entspricht dem Blockverschlüsselungsverarbeitungsschritt). Der OTA-Master führt einen XOR-Betrieb durch und entschlüsselt den verschlüsselten IV-Wert und das verschlüsselte Aktualisierungspaket, das von dem CDN 8 heruntergeladen wurde (B025, entspricht einem Verschlüsselungsdatenentschlüsselungsschritt). Der OTA-Master 4 überträgt das entschlüsselte Aktualisierungspaket an die Ziel-ECU 5 und installiert das Aktualisierungspaket in der Ziel-ECU 5 (B026, entspricht einem Installationsverarbeitungsschritt). Mittels Durchführung des Verschlüsseln und Entschlüsseln in dem OFB-Modus anstelle der Durchführung des Verschlüsseln und Entschlüsseln des Differenzprogramms in dem Aktualisierungspaket in dem CBC-Modus kann der Durchsatz des Entschlüsselungsprozesses in der Ziel-ECU 5 auch um etwa 25% erhöht werden.

[0041] Wie es oben beschrieben ist, können gemäß der zweiten Ausführungsform die folgenden vorteilhaften Wirkungen erzielt werden.

[0042] Der OFB-Modus wird als das Verschlüsselungsverfahren und das Entschlüsselungsverfahren

des Aktualisierungspaketes verwendet. Unter Verwendung des OFB-Modus ist es im Vergleich zu dem herkömmlichen CBC-Modus möglich, eine Vorbereitung zum Verschlüsseln und Entschlüsseln durchzuführen. Als Ergebnis ist es, wenn der OTA-Master 4 das Aktualisierungspaket von dem OTA-Zentrum 2 herunterlädt, möglich, die Vorteile des OFB-Modus zu genießen und geeignet den Durchsatz zu erhöhen.

Dritte Ausführungsform

[0043] Die dritte Ausführungsform wird mit Bezug auf die Fig. 27 bis 33 beschrieben. In der dritten Ausführungsform wird das Hypertext-Transfer-Protokoll (im Folgenden als HTTP abgekürzt) als ein Kommunikationsprotokoll zwischen dem CDN 8 und dem OTA-Master 4 verwendet, es wird eine Bereichsanfrage an das CDN 8 übertragen, und es wird ein Aktualisierungspaket in einem Streaming-Verfahren heruntergeladen, wodurch die Verteilungskosten im Vergleich zu einem Fall verringert werden, in dem das Hypertext-Transfer-Protokoll-Secure (im Folgenden als HTTPS abgekürzt) verwendet wird. In Abhängigkeit von dem CDN-Verkäufer kann die Verteilungsgebühr des CDN 8 zwischen einem Fall, in dem HTTP verwendet wird, und einem Fall, in dem HTTPS als ein Kommunikationsprotokoll für das CDN 8 verwendet wird, unterschiedlich sein. Wenn HTTPS verwendet wird, muss das CDN 8 einen Handshake-Prozess, einen Verschlüsselungsschlüsselaustauschprozess oder einen kryptographischen Betriebsprozess, der in einer Transportschichtssicherheit (im Folgenden als TLS abgekürzt) definiert ist, durchführen, und es erhöht sich die Verarbeitungslast der CPU des CDN 8. Daher ist eine Verteilungsgebühr bei HTTPS in der Gebührentabelle etwa 30% höher als bei HTTP. Daher werden die Verteilungskosten unter Verwendung von HTTP zum Herunterladen des Aktualisierungspaketes verringert. In der dritten Ausführungsform wird HTTPS nicht verwendet, wenn das Aktualisierungspaket von dem CDN 8 an das fahrzeugseitige System 3 verteilt wird.

[0044] In diesem Fall überträgt der Kampagnenmeldungsübertragungsabschnitt 2f nach der Errichtung einer TLS-Kommunikation zwischen dem OTA-Zentrum 2 und dem OTA-Master 4 eine Kampagnenmeldung, in der ein verschlüsselter AES-Schlüssel gespeichert ist, an das neu zu programmierende fahrzeugseitige System 3. Wenn der Gemeinsamer-Schlüssel-Beschaffungsabschnitt 4a eine Kampagnenmeldung beschafft, da die Kampagnenmeldung, die von dem OTA-Zentrum 2 übertragen wird, von dem OTA-Master 4 empfangen wird, nachdem die TLS-Kommunikation errichtet ist, beschafft der Gemeinsamer-Schlüssel-Beschaffungsabschnitt 4a den AES-Schlüssel aus der beschafften Kampagnenmeldung. Der Verschlüsselungspaketbeschaffungsabschnitt 4c überträgt eine Bereichsanfrage

an das CDN 8, um einen Datenbereich für das Herunterladen zu bezeichnen bzw. bestimmen, und lädt und beschafft das verschlüsselte Aktualisierungspaket von dem CDN 8 unter Verwendung eines Streaming-Verfahrens. Der Installationsverarbeitungsabschnitt 4f überträgt das entschlüsselte Aktualisierungspaket an die Ziel-ECU 5 durch ein Streaming-Verfahren und installiert das Aktualisierungspaket in der Ziel-ECU 5.

[0045] In der vorliegenden Ausführungsform ist beschrieben, dass der OTA-Master 4 das verschlüsselte Aktualisierungspaket von dem CDN 8 unter Verwendung des Streaming-Verfahrens beschafft, aber das verschlüsselte Aktualisierungspaket kann von dem CDN 8 unter Verwendung des Speicherverfahrens beschafft werden. Da in dem Streaming-Verfahren die Kopfinformationen bzw. Header-Informationen zu der Zeit der Kommunikation enthalten sind, ist es möglich, die Verteilungskosten unter Verwendung von HTTP weiter zu verringern.

[0046] Im Folgenden wird der Betrieb der oben beschriebenen Konfiguration mit Bezug auf die **Fig. 28** bis **33** beschrieben.

(3-1) Prozess des OTA-Zentrums 2 (siehe Figuren 28 bis 30)

[0047] Das OTA-Zentrum 2 erzeugt einen AES-Schlüssel zur Verschlüsselung des Aktualisierungspaketes (A031). Das OTA-Zentrum 2 verschlüsselt das Aktualisierungspaket mit dem erzeugten AES-Schlüssel in dem CTR-Modus (A032). Das OTA-Zentrum 2 verschlüsselt den AES-Schlüssel mit dem öffentlichen RSA-Schlüssel (A033). Das OTA-Zentrum 2 speichert den AES-Schlüssel, der mit dem öffentlichen RSA-Schlüssel verschlüsselt ist, in der Kampagnenmeldung (A034). Das OTA-Zentrum 2 platziert das Aktualisierungspaket, das mit dem AES-Schlüssel verschlüsselt ist, in dem CDN 8 (A035). Nach einer Errichtung einer TLS-Kommunikation zwischen dem OTA-Zentrum 2 und dem OTA-Master 4 überträgt das OTA-Zentrum 2 eine Kampagnenmeldung, in der ein verschlüsselter AES-Schlüssel gespeichert ist, an das neu zu programmierende fahrzeugseitige System 3 (A036).

(3-2) Prozess des OTA-Masters 4 (siehe Figuren 31 bis 33)

[0048] Wenn der OTA-Master 4 die Kampagnenmeldung beschafft, da die Kampagnenmeldung, die von dem OTA-Zentrum 2 übertragen wird, von dem OTA-Master 4 empfangen wird, nachdem die TLS-Kommunikation errichtet ist, beschafft der OTA-Master 4 den AES-Schlüssel aus der beschafften Kampagnenmeldung (B031). Der OTA-Master 4 entschlüsselt den verschlüsselten AES-Schlüssel mit dem geheimen RSA-Schlüssel, um den AES-Schlüssel

zu extrahieren (B032). Der OTA-Master 4 überträgt eine Bereichsanfrage an das CDN 8, um einen Datenbereich für das Herunterladen zu bezeichnen bzw. bestimmen, und lädt und beschafft das verschlüsselte Aktualisierungspaket von dem CDN 8 durch ein Streaming-Verfahren (BOSS). D.h., der OTA-Master 4 bestimmt den Datenbereich für das Herunterladen, wodurch das Aktualisierungspaket von dem CDN 8 durch das Teilungs-Streaming-Verfahren heruntergeladen und beschafft wird.

[0049] Gleichzeitig führt der OTA-Master 4 parallel zu dem Herunterladen und Beschaffen des verschlüsselten Aktualisierungspaketes von dem CDN 8 durch den Verschlüsselungspaketbeschaffungsabschnitt 4c einen AES-Blockverschlüsselungsprozess des Zählerwertes mit dem AES-Schlüssel durch, um den Zählerwert zu verschlüsseln (B034). Der OTA-Master 4 führt eine XOR-Betrieb durch und entschlüsselt den verschlüsselten Zählerwert und das verschlüsselte Aktualisierungspaket, das von dem CDN 8 heruntergeladen wurde (BOSS). Der OTA-Master 4 überträgt das entschlüsselte Aktualisierungspaket an die Ziel-ECU 5 durch ein Streaming-Verfahren und installiert das Aktualisierungspaket in der Ziel-ECU 5 (B036).

[0050] Wie es oben beschrieben ist, können gemäß der dritten Ausführungsform die folgenden Wirkungen erzielt werden.

[0051] HTTP wird als ein Kommunikationsprotokoll zwischen dem CDN 8 und dem OTA-Master 4 verwendet, und der OTA-Master 4 überträgt eine Bereichsanfrage an das CDN 8, um ein Aktualisierungspaket von dem CDN 8 durch ein Streaming-Verfahren herunterzuladen. Demzufolge ist es möglich, im Vergleich zu dem herkömmlichen Fall, in dem HTTPS als das Kommunikationsprotokoll verwendet wird, die Verteilungskosten geeignet zu verringern, wenn der OTA-Master 4 das Aktualisierungspaket von dem OTA-Zentrum 2 herunterlädt.

Vierte Ausführungsform

[0052] Die vierte Ausführungsform wird mit Bezug auf die **Fig. 34** bis **38** beschrieben. In der vierten Ausführungsform wird die Berechnung sämtlicher Schlüssel-Streams bzw. Schlüsselströme im Voraus im Hintergrund ausgeführt, bevor die Download-Bewilligung von dem Nutzer erlangt wird, wodurch der Entschlüsselungsprozess zu der Zeit des Herunterladens des Aktualisierungspaketes beschleunigt wird.

[0053] Wie es in **Fig. 35** dargestellt ist, enthält in diesem Fall der OTA-Master 4 einen Schlüsselstromberechnungsabschnitt 4g zusätzlich zu dem Gemeinsamer-Schlüssel-Beschaffungsabschnitt 4a, dem Gemeinsamer-Schlüssel-Entschlüsselungsabschnitt

4b, dem Verschlüsselungspaketbeschaffungsabschnitt 4c, dem Blockverschlüsselungsverarbeitungsabschnitt 4d, dem Verschlüsselungspaketentschlüsselungsabschnitt 4e und dem Installationsverarbeitungsabschnitt 4f. Der Schlüsselstromberechnungsabschnitt 4g führt im Voraus eine Berechnung sämtlicher Schlüsselströme im Hintergrund aus, bevor die Download-Bewilligung von dem Nutzer erhalten wird. Der Verschlüsselungspaketbeschaffungsabschnitt 4c lädt und beschafft das verschlüsselte Aktualisierungspaket von dem CDN 8 unter der Bedingung, dass die Download-Bewilligung von dem Nutzer erhalten wird bzw. wurde. Der Verschlüsselungspaketentschlüsselungsabschnitt 4e führt einen XOR-Betrieb durch und entschlüsselt den berechneten Schlüsselstrom und das verschlüsselte Aktualisierungspaket, das von dem CDN 8 heruntergeladen wurde.

[0054] Im Folgenden wird der Betrieb der oben beschriebenen Konfiguration mit Bezug auf die Fig. 36 bis 38 beschrieben.

(4-1) Prozess des OTA-Zentrums 2

[0055] Der Prozess des OTA-Zentrums 2 ist ähnlich wie der Prozess (Fig. 9 bis 11) des OTA-Zentrums 2, der in der ersten Ausführungsform beschrieben wurde.

(4-2) Prozess des OTA-Masters 4 (siehe Figuren 36 bis 38)

[0056] Wenn der OTA-Master 4 eine Kampagnenmeldung beschafft, da die Kampagnenmeldung, die von dem OTA-Zentrum 2 übertragen wird, von dem OTA-Master 4 empfangen wird, beschafft der OTA-Master 4 einen AES-Schlüssel aus der beschafften Kampagnenmeldung (B041). Der OTA-Master 4 entschlüsselt den verschlüsselten AES-Schlüssel mit dem geheimen RSA-Schlüssel, um den AES-Schlüssel zu extrahieren (B042). Der OTA-Master 4 führt eine Berechnung sämtlicher Schlüsselströme im Hintergrund im Voraus aus, bevor eine Download-Bewilligung von dem Nutzer erhalten wird (B043). Es werden jedem Schlüsselstrom Identifikations- bzw. Identifizierungsinformationen zugewiesen, und die Reihenfolge der Anwendung auf das verschlüsselte Aktualisierungspaket ist angegeben.

[0057] Der OTA-Master 4 verteilt die Kampagnenmeldung an das fahrzeugseitige System 3 oder ein mobiles Informationsendgerät wie beispielsweise ein Smartphone des Nutzers, um einen Download-Bewilligungsbildschirm auf einer Mensch-Maschine-Schnittstelle (HMI) anzuzeigen (B044). Der OTA-Master 4 lädt und beschafft das verschlüsselte Aktualisierungspaket von dem CDN 8 unter der Bedingung, dass die Download-Bewilligung von dem Nutzer erhalten wird bzw. wurde (B045). Der

OTA-Master 4 führt einen XOR-Betrieb durch und entschlüsselt den im Voraus berechneten Schlüsselstrom und das verschlüsselte Aktualisierungspaket, das von dem CDN 8 heruntergeladen wurde (B046). Der OTA-Master 4 überträgt das entschlüsselte Aktualisierungspaket an die Ziel-ECU 5 und installiert das Aktualisierungspaket in der Ziel-ECU 5 (B047).

[0058] Wie es oben beschrieben ist, können gemäß der vierten Ausführungsform die folgenden vorteilhaften Wirkungen erhalten werden.

[0059] Sämtliche Schlüsselströme werden im Hintergrund im Voraus berechnet, bevor die Download-Bewilligung von dem Nutzer erhalten wird. Als Ergebnis kann der Entschlüsselungsprozess des Aktualisierungspaketes in dem OTA-Master 4 beschleunigt werden, und es kann der Durchsatz, wenn der OTA-Master 4 das Aktualisierungspaket von dem OTA-Zentrum 2 herunterlädt, erhöht werden.

Fünfte Ausführungsform

[0060] Die fünfte Ausführungsform wird Bezug auf die Fig. 39 bis 42 beschrieben. In der vierten Ausführungsform werden sämtliche Schlüsselströme im Hintergrund im Voraus berechnet, bevor die Download-Bewilligung von dem Nutzer erhalten wird, aber in der fünften Ausführungsform werden nur einige Schlüsselströme im Hintergrund im Voraus berechnet, bevor die Download-Bewilligung von dem Nutzer erhalten wird. Diese zu berechnenden Schlüsselströme werden unter Berücksichtigung der Speicherkapazität des Cache-Speichers der CPU und des Durchsatzes des AES-Kryptographiebetriebs bestimmt und weisen eine Größe auf, die in dem Cache-Speicher gespeichert werden kann.

[0061] In diesem Fall führt der Schlüsselstromberechnungsabschnitt 4g eine Berechnung einiger der Schlüsselströme im Hintergrund im Voraus aus, bevor die Download-Bewilligung von dem Nutzer erhalten wird. Der Schlüsselstromberechnungsabschnitt 4g erzeugt einen Schlüsselstrom und fügt den Schlüsselstrom zu dem Cache-Speicher parallel zu dem Herunterladen und Beschaffen des verschlüsselten Aktualisierungspaketes von dem CDN 8 durch den Verschlüsselungspaketbeschaffungsabschnitt 4c hinzu.

[0062] Im Folgenden wird der Betrieb der oben beschriebenen Konfiguration mit Bezug auf die Fig. 39 bis 42 beschrieben.

(5-1) Prozess des OTA-Zentrums 2

[0063] Der Prozess des OTA-Zentrums 2 ist ähnlich wie der Prozess (Fig. 9 bis 11) des OTA-Zentrums 2,

der in der ersten Ausführungsform beschrieben wurde.

(5-2) Prozess des OTA-Masters 4 (siehe Figuren 39 bis 41)

[0064] Wenn der OTA-Master 4 eine Kampagnenmeldung beschafft, da die Kampagnenmeldung, die von dem OTA-Zentrum 2 übertragen wird, durch den OTA-Master 4 empfangen wird, beschafft der OTA-Master 4 einen AES-Schlüssel aus der beschafften Kampagnenmeldung (B051). Der OTA-Master 4 entschlüsselt den verschlüsselten AES-Schlüssel mit dem geheimen RSA-Schlüssel, um den AES-Schlüssel zu extrahieren (B052). Der OTA-Master 4 führt die Berechnung einiger Schlüsselströme im Hintergrund im Voraus aus, bevor eine Download-Bewilligung von dem Nutzer erhalten wird (BOSS).

[0065] Der OTA-Master 4 verteilt die Kampagnenmeldung an das fahrzeugseitige System 3 oder ein mobiles Informationsendgerät wie beispielsweise ein Smartphone des Nutzers, um einen Download-Bewilligungsbildschirm auf der HMI anzuzeigen (B054). Der OTA-Master 4 lädt und beschafft das verschlüsselte Aktualisierungspaket von dem CDN 8 unter der Bedingung, dass die Download-Bewilligung von dem Nutzer erhalten wird bzw. wurde (B055). Der OTA-Master 4 führt einen XOR-Betrieb durch und entschlüsselt den im Voraus berechneten Schlüsselstrom und das verschlüsselte Aktualisierungspaket, das von dem CDN 8 heruntergeladen wurde (B056).

[0066] Zu dieser Zeit erzeugt der OTA-Master 4 parallel zu dem Herunterladen und Beschaffen des verschlüsselten Aktualisierungspaketes von dem CDN 8 einen Schlüsselstrom, fügt den Schlüsselstrom zu dem Cache-Speicher hinzu (B057) und berechnet einen verbleibenden Schlüsselstrom. Der OTA-Master 4 überträgt das entschlüsselte Aktualisierungspaket an die Ziel-ECU 5 und installiert das Aktualisierungspaket in der Ziel-ECU 5 (B058). Die Beziehung zwischen der Speicherkapazität und der Zugriffsgeschwindigkeit ist in **Fig. 42** dargestellt, und die Größe des Cache-Speichers kann entsprechend der benötigten Zugriffsgeschwindigkeit bestimmt werden.

[0067] Wie es oben beschrieben ist, können gemäß der fünften Ausführungsform die folgenden vorteilhaften Wirkungen erzielt werden.

[0068] Einige Schlüsselströme werden im Hintergrund im Voraus berechnet, bevor die Download-Bewilligung von dem Nutzer erhalten wird. Als Ergebnis kann der Entschlüsselungsprozess des Aktualisierungspaketes in dem OTA-Master 4 beschleunigt werden, während der Speicherplatz des OTA-Masters 4 eingespart bzw. beschränkt werden kann,

und es kann der Durchsatz, wenn der OTA-Master 4 das Aktualisierungspaket von dem OTA-Zentrum herunterlädt, erhöht werden.

Sechste Ausführungsform

[0069] Die sechste Ausführungsform wird mit Bezug auf die **Fig. 43** bis **54** beschrieben. In der sechsten Ausführungsform ist ein Verschlüsselungsverfahren in Neuprogrammierungs-Konzept-Metadaten (im Folgenden als RP-Metadaten bezeichnet) oder Ähnlichem enthalten und wird von dem OTA-Zentrum 2 an den OTA-Master 4 übertragen, so dass der OTA-Master 4 das Verschlüsselungsverfahren identifiziert. Das Verschlüsselungsverfahren, das von dem OTA-Zentrum 2 an den OTA-Master 4 übertragen wird, enthält einen Verschlüsselungsalgorithmus, eine Verschlüsselungsschlüssellänge, einen Verschlüsselungsmodus, einen Algorithmus eines Nachrichtenauthentifizierungscodes (im Folgenden als MAC bezeichnet) und Ähnliches.

[0070] Die RP-Metadaten sind Daten, die Konfigurationsinformationen über das Aktualisierungspaket, d.h. Informationen enthalten, die einen Konfigurationstyp des Aktualisierungspaketes angeben, und Daten zum Verhindern eines Fehlers bei der Verteilung des Aktualisierungspaketes durch Überprüfen des Dateninhaltes durch den OTA-Master 4. Durch Konfigurieren der RP-Metadaten derart, dass sie eine dreischichtige Struktur bzw. 3-Ebenen-Struktur einer Verteilung, eines Masters und eines Ziels aufweisen, ist es sogar in dem Fall, in dem ein Übertragungsverfahren, ein Typ einer Plattform, ein Typ eines Aktualisierungspaketes und Ähnliches größer sind, möglich, diese flexibel zu definieren und zu handhaben und eine Neuprogrammierung der Ziel-ECU 5 durchzuführen. Der OTA-Master 4 kann das Verschlüsselungsverfahren dadurch identifizieren, dass das Verschlüsselungsverfahren in Download-Metadaten bzw. Herunterlade-Metadaten (im Folgenden als DL-Metadaten bezeichnet) oder Ähnlichem enthalten ist und das Verschlüsselungsverfahren von dem OTA-Zentrum 2 an den OTA-Master 4 übertragen wird. Die DL-Metadaten sind Daten, die Informationen zum Herunterladen eines Aktualisierungspaketes für jede der Ziel-ECUs 5 enthalten und einen durch den OTA-Master 4 zu erfassenden Inhalt definieren.

[0071] Wie es in **Fig. 44** dargestellt ist, enthält das OTA-Zentrum 2 einen RP-Metadatenerzeugungsabschnitt 2f und einen RP-Metadatenverschlüsselungsabschnitt 2h zusätzlich zu dem Gemeinsamer-Schlüssel-Erzeugungsabschnitt 2a, dem Aktualisierungspaketverschlüsselungsabschnitt 2b, dem Gemeinsamer-Schlüssel-Verschlüsselungsabschnitt 2c, dem Gemeinsamer-Schlüssel-Speicherabschnitt 2d, dem Verschlüsselungspaketplatzierungsabschnitt 2e und dem Kampagnenmeldungsübertra-

gungsabschnitt 2f. Der RP-Metadatenerzeugungsabschnitt 2g erzeugt RP-Metadaten, die ein Gemeinsamer-Schlüssel-Verschlüsselungsverfahren enthalten. Der RP-Metadatenverschlüsselungsabschnitt 2h verschlüsselt die RP-Metadaten mit dem öffentlichen RSA-Schlüssel.

[0072] Der OTA-Master 4 enthält einen RP-Metadatenbeschaffungsabschnitt 4h, einen RP-Metadatenentschlüsselungsabschnitt 4i und einen Gemeinsamer-Schlüssel-Verschlüsselungsverfahrensidentifizierungsabschnitt 4j zusätzlich zu dem Gemeinsamer-Schlüssel-Beschaffungsabschnitt 4a, dem Gemeinsamer-Schlüssel-Entschlüsselungsabschnitt 4b, dem Verschlüsselungspaketbeschaffungsabschnitt 4c, dem Blockverschlüsselungsverarbeitungsabschnitt 4d, dem Verschlüsselungspaketentschlüsselungsabschnitt 4e und dem Installationsverarbeitungsabschnitt 4f. Der RP-Metadatenbeschaffungsabschnitt 4h lädt und beschafft die verschlüsselten RP-Metadaten von dem CDN 8. Der RP-Metadatenentschlüsselungsabschnitt 4i entschlüsselt die verschlüsselten RP-Metadaten mit dem geheimen RSA-Schlüssel, um die RP-Metadaten zu extrahieren. Der Gemeinsamer-Schlüssel-Verschlüsselungsverfahrensidentifizierungsabschnitt 4j interpretiert den Inhalt der RP-Metadaten, um das Gemeinsamer-Schlüssel-Verschlüsselungsverfahren zu identifizieren.

[0073] Der Fluss von dem OTA-Zentrum 2 über das CDN 8 zur Verteilung des Aktualisierungspaketes ist der Folgende. Eine Kampagnenmeldung wird von dem OTA-Zentrum 2 an den OTA-Master 4 oder ein mobiles Informationsendgerät des Nutzers übertragen. Wenn der OTA-Master 4 danach auf das CDN 8 zugreift, werden die RP-Metadaten und die DL-Metadaten von dem CDN 8 an den OTA-Master 4 übertragen, und das Aktualisierungspaket wird von dem CDN 8 an das OTA-Zentrum 2 verteilt.

[0074] Wie es in **Fig. 45** dargestellt ist, werden die RP-Metadaten und die DL-Metadaten von dem OTA-Zentrum 2 an den OTA-Master 4 vor dem Herunterladen des Aktualisierungspaketes übertragen. Wie es in den **Fig. 46** und **47** dargestellt ist, enthalten die RP-Metadaten Informationen über eine RP-Metadatenversion, eine Verteilungsschicht, eine Master-Schicht und eine Zielschicht. Ein jeweiliger Informationsteil ist wie folgt ausgebildet.

(a) RP-Metadatenversion

[0075] Diese ist eine Version der RP-Metadaten und ist beispielsweise eine Versionsinformation wie beispielsweise „1.00“ oder „2.00“.

(b) Verteilungsschicht

(b-1) Kommunikationsprotokoll

[0076] Dieses ist ein Protokoll, das zur Kommunikation mit dem OTA-Zentrum 2 verwendet wird, und ist eine Information, die beispielsweise Uptane (eingetragene Marke), Open Mobile Alliance-Device Management (OMA-DM), oder Ähnliches angibt.

(b-2) Kommunikationseinrichtung

[0077] Diese ist eine Verteilungsrouten des Aktualisierungspaketes und bildet Informationen, die ein Mobiltelefon, ein Smartphone, einen USB-Speicher oder Ähnliches als OTA-Master 4 angeben.

(c) Master-Schicht

[0078] Diese bildet eine Information über den OTA-Master 4.

(c-1) PF

[0079] Diese bildet eine Information, die angibt, dass die Plattform (PF) des OTA-Masters 4 beispielsweise eine adaptive Plattform (AP) von AUTOSAR, eine klassische Plattform (CP) von AUTOSAR, Automotive Grade Linux (AGL) oder Android (eingetragene Marke) ist. Für eine Paketstruktur zum Verteilen eines Aktualisierungspaketes entsprechend einer Plattform einer ECU wird eine Datenanforderung, die für eine klassische Plattform (CP) anwendbar ist, die in einem statischen OS der Standardisierungsorganisation AUTOSAR betrieben wird, in einer Spezifikation der Associations und General Incorporated Foundations, JASPAR, definiert. Außerdem sind in AUTOSAR Datenanforderungen, die für einen neuen Typ von adaptiver Plattform (AP) verwendbar sind, die in einem dynamischen OS betrieben wird, spezifiziert. AGL ist ein fahrzeugeigenes Linux (eingetragene Marke) und Android ist ein Android-Automotive-OS. AP und CP geben Softwareplattformen an. Die Softwareplattform wird auch Softwarearchitektur bezeichnet. AP und CP verwenden unterschiedliche Betriebssysteme und unterschiedliche Entwicklungssprachen. Die Struktur des empfangbaren Aktualisierungspaketes unterscheidet sich zwischen einer ECU, die entsprechend der CP-Spezifikation betrieben wird, und einer ECU, die entsprechend der AP-Spezifikation betrieben wird. Der Unterschied in der Struktur zwischen diesen Aktualisierungspaketen wird hauptsächlich durch einen Unterschied in der Verarbeitungsleistungsfähigkeit der ECU bewirkt. Da im Allgemeinen die Verarbeitungsleistungsfähigkeit einer ECU, die entsprechend der CP-Spezifikation betrieben wird, relativ niedrig ist, werden Spezifikationsdaten und Ähnliches, die in dem Aktualisierungspaket enthalten sind, auch als binäre Daten beschrieben, und die

Datenstruktur ist sogar für eine ECU mit niedrigem Verarbeitungsleistungsvermögen zur Interpretation und Verarbeitung einfach. Da andererseits das Verarbeitungsleistungsvermögen einer ECU, die entsprechend der AP-Spezifikation betrieben wird, relativ hoch ist, ist es möglich, eine Parser-Funktion zu installieren, die strukturelle Zeichendaten, die in irgendeiner Sprache beschrieben sind, analysiert und die strukturellen Zeichendaten in eine Datenstruktur umwandelt, die durch ein Programm gehandhabt werden kann, und da ein objektorientiertes Datenformat wie beispielsweise JavaScript Object Notation (JSON) anstelle von einfachen binären Daten in der Datenstruktur verwendet werden kann, wird eine flexible Datenstruktur erhalten.

(c-2) Steuerungsverfahren

[0080] Dieses ist eine Information wie beispielsweise ein Parameter, der entsprechend einem Parameter zu verarbeiten ist, der entsprechend einem speziellen Format, einem Skript, das in einem freieren Beschreibungsformat ohne spezielles Format zu verarbeiten ist, oder Ähnlichem festgelegt wird.

(c-3) Verschlüsselungsverfahren

[0081] Dieses bildet eine Information einschließlich einem Verschlüsselungsalgorithmus, einer Verschlüsselungsschlüssellänge, einem Verschlüsselungsmodus, einem Padding-Verfahren, einem Verschlüsselungsschlüssel-ID, einem Signaturalgorithmus, einem Signaturschlüssel-ID, einem Signaturmodus, einem Hash-Algorithmus, einem Vorhandensein oder einer Abwesenheit einer Bereichsbezeichnung, einer Offset-Größe und einer Schutzdatengröße.

(d) Zielschicht

[0082] Dieses ist eine Information über die Ziel-ECU 5.

(d-1) PF

[0083] Diese ist ähnlich wie die Master-Schicht.

(d-2) Übertragungsverfahren

[0084] Dieses ist irgendein Speicherverfahren oder Streaming-Verfahren.

(d-3) Steuerungsverfahren

[0085] Dieses ist ähnlich wie die Master-Schicht.

(d-4) Ziel-ID

[0086] Dieser ist optional.

(d-5) Verschlüsselungsverfahren

[0087] Dieses ist ähnlich wie die Master-Schicht.

[0088] Im Folgenden wird der Betrieb der oben beschriebenen Konfiguration mit Bezug auf die Fig. 48 bis 54 beschrieben.

(6-1) Prozess des OTA-Zentrums 2 (siehe Figuren 48 bis 51)

[0089] Das OTA-Zentrum 2 erzeugt einen gemeinsamen Schlüssel zur Verschlüsselung des Aktualisierungspaketes (A061). Das OTA-Zentrum 2 verschlüsselt das Aktualisierungspaket in einem speziellen Verschlüsselungsmodus unter Verwendung des erzeugten gemeinsamen Schlüssels (A062). Das OTA-Zentrum 2 verschlüsselt den gemeinsamen Schlüssel mit dem öffentlichen RSA-Schlüssel (A063). Das OTA-Zentrum 2 speichert den gemeinsamen Schlüssel, der mit dem öffentlichen RSA-Schlüssel verschlüsselt ist, in der Kampagnenmeldung (A064). Das OTA-Zentrum 2 erzeugt RP-Metadaten einschließlich eines Gemeinsamer-Schlüssel-Verschlüsselungsverfahrens (A065). Das OTA-Zentrum 2 verschlüsselt die RP-Metadaten mit dem öffentlichen RSA-Schlüssel (A066). Das OTA-Zentrum 2 platziert das Aktualisierungspaket, das mit dem gemeinsamen Schlüssel verschlüsselt ist, und die RP-Metadaten, die mit dem öffentlichen RSA-Schlüssel verschlüsselt sind, in dem CDN 8 (A067). Das OTA-Zentrum 2 überträgt eine Kampagnenmeldung, in der der verschlüsselte gemeinsame Schlüssel gespeichert ist, an das neu zu programmierende fahrzeugseitige System 3 (A068).

(6-2) Prozess des OTA-Masters 4 (siehe Figuren 52 bis 54)

[0090] Wenn der OTA-Master 4 eine Kampagnenmeldung beschafft, da die Kampagnenmeldung, die von dem OTA-Zentrum 2 übertragen wird, von dem OTA-Master 4 empfangen wird, beschafft der OTA-Master 4 einen gemeinsamen Schlüssel aus der beschafften Kampagnenmeldung (B061). Der OTA-Master 4 entschlüsselt den verschlüsselten gemeinsamen Schlüssel mit dem geheimen RSA-Schlüssel, um den gemeinsamen Schlüssel zu extrahieren (B062). Der OTA-Master 4 lädt und beschafft die verschlüsselten RP-Metadaten von dem CDN 8 (B063). Der OTA-Master 4 entschlüsselt die verschlüsselten RP-Metadaten mit dem geheimen RSA-Schlüssel, um die RP-Metadaten zu extrahieren (B064). Der OTA-Master 4 interpretiert den Inhalt der RP-Metadaten und identifiziert ein Gemeinsamer-Schlüssel-Verschlüsselungsverfahren (B065). Der OTA-Master 4 lädt und beschafft das verschlüsselte Aktualisierungspaket von dem CDN 8 (B066). Danach führt der OTA-Master 4 den Prozess in und nach Schritt B014, der in der ersten Ausführungsform beschrie-

ben wurde, durch, wenn der CTR-Modus als der spezielle Verschlüsselungsmodus verwendet wird, oder führt den Prozess in und nach Schritt B024, der in der zweiten Ausführungsform beschrieben wurde, durch, wenn der OFB-Modus als der spezielle Verschlüsselungsmodus verwendet wird. In den anderen Verschlüsselungsmodi wird auf ähnliche Weise das Aktualisierungspaket entschlüsselt, und es werden Daten an die Ziel-ECU entsprechend einer dem Verschlüsselungsmodus entsprechenden Prozedur übertragen.

[0091] Wie es oben beschrieben ist, können gemäß der sechsten Ausführungsform die folgenden vorteilhaften Wirkungen erzielt werden.

[0092] Das Verschlüsselungsverfahren ist in den RP-Metadaten oder den DL-Metadaten enthalten und wird von dem OTA-Zentrum 2 an den OTA-Master 4 übertragen. Als Ergebnis kann der OTA-Master 4 das Verschlüsselungsverfahren identifizieren.

Siebte Ausführungsform

[0093] Die siebte Ausführungsform wird mit Bezug auf die **Fig. 55 bis 67** beschrieben. In der siebten Ausführungsform wird ein Zählermodus mit einem Chiffrierungsblock-Ketten-Nachrichtenauthentifizierungscodeprotokoll (Cipher Block Chaining Message Authentication Code Protokoll, als CCMP-Modus abgekürzt) für eine Kommunikationspfadverschlüsselung und eine Maßnahme gegen eine Datenverfälschung verwendet.

[0094] Wie es in den **Fig. 56 bis 60** dargestellt ist, ist in diesem Fall, wenn die Konfiguration, die den CCMP-Modus verwendet, mit der Konfiguration verglichen wird, die die Entschlüsselungs- und Signaturverifizierung eines Hashed-Message-Authentication-Mode-Code-Secure-Hash-Algorithmus (AES CBC-HMAC SHA) 2 als herkömmliches Verfahren verwendet, die Verarbeitungszeit des Hardwarebeschleunigers in beiden Fällen dominant gegenüber der Verarbeitungszeit des Hauptkernes, aber der Durchsatz kann unter Verwendung des CCMP-Modus verbessert werden.

[0095] Wie es in **Fig. 61** dargestellt ist, enthält das OTA-Zentrum 2 einen MAC-Schlüsselerzeugungsabschnitt 2i zusätzlich zu dem Gemeinsamer-Schlüssel-Erzeugungsabschnitt 2a, dem Aktualisierungspaketverschlüsselungsabschnitt 2b, dem Gemeinsamer-Schlüssel-Verschlüsselungsabschnitt 2c, dem Gemeinsamer-Schlüssel-Speicherabschnitt 2d, dem Verschlüsselungspaketplatzierungsabschnitt 2e und dem Kampagnenmeldungsübertragungsabschnitt 2f. Der MAC-Schlüsselerzeugungsabschnitt 2i erzeugt einen MAC-Schlüssel zur Verhinderung einer Verfälschung des Aktualisierungspaketes.

[0096] Der OTA-Master 4 enthält einen MAC-Schlüsselbeschaffungsabschnitt 4k zusätzlich zu dem Gemeinsamer-Schlüssel-Beschaffungsabschnitt 4a, dem Gemeinsamer-Schlüssel-Entschlüsselungsabschnitt 4b, dem Verschlüsselungspaketbeschaffungsabschnitt 4c, dem Blockverschlüsselungsverarbeitungsabschnitt 4d, dem Verschlüsselungspaketentschlüsselungsabschnitt 4a und dem Installationsverarbeitungsabschnitt 4f. Wenn der MAC-Schlüsselbeschaffungsabschnitt 4k die Kampagnenmeldung beschafft, da die Kampagnenmeldung, die von dem OTA-Zentrum 2 übertragen wird, durch den OTA-Master 4 empfangen wird, beschafft der MAC-Schlüsselbeschaffungsabschnitt 4k einen MAC-Schlüssel aus der beschafften Kampagnenmeldung.

[0097] Im Folgenden wird der Betrieb der oben beschriebenen Konfiguration mit Bezug auf die **Fig. 62 bis 67** beschrieben.

(7-1) Prozess des OTA-Zentrums 2 (siehe Figuren 62 bis 64)

[0098] Das OTA-Zentrum 2 erzeugt einen AES-Schlüssel zum Verschlüsseln des Aktualisierungspaketes und einen MAC-Schlüssel zum Verhindern einer Verfälschung des Aktualisierungspaketes (A071). Das OTA-Zentrum 2 verschlüsselt das Aktualisierungspaket mit dem erzeugten AES-Schlüssel und dem erzeugten MAC-Schlüssel in dem CCMP-Modus und weist einen MAC zu (A072). Das OTA-Zentrum 2 verschlüsselt den AES-Schlüssel und den MAC-Schlüssel mit dem öffentlichen RSA-Schlüssel (A073). Das OTA-Zentrum 2 speichert den AES-Schlüssel und den MAC-Schlüssel, die mit dem öffentlichen RSA-Schlüssel verschlüsselt sind, in der Kampagnenmeldung (A074). Das OTA-Zentrum 2 platziert ein Aktualisierungspaket, das mit dem AES-Schlüssel und dem MAC-Schlüssel verschlüsselt ist, in dem CDN 8 (A075). Das OTA-Zentrum 2 überträgt eine Kampagnenmeldung, in der der verschlüsselte AES-Schlüssel und der verschlüsselte MAC-Schlüssel gespeichert sind, an das neu zu programmierende fahrzeugseitige System 3 (A076).

(7-2) Prozess des OTA-Masters 4 (siehe Figuren 65 bis 67)

[0099] Wenn der OTA-Master 4 die Kampagnenmeldung beschafft, da die Kampagnenmeldung, die von dem OTA-Zentrum 2 übertragen wird, durch den OTA-Master 4 empfangen wird, beschafft der OTA-Master 4 einen AES-Schlüssel und einen MAC-Schlüssel aus der beschafften Kampagnenmeldung (B071). Der OTA-Master 4 entschlüsselt den verschlüsselten AES-Schlüssel und den verschlüsselten MAC-Schlüssel mit dem geheimen RSA-Schlüssel, um den AES-Schlüssel und den MAC-Schlüssel

zu extrahieren (B071). Der OTA-Master 4 lädt und beschafft das verschlüsselte Aktualisierungspaket von dem CDN 8 (B073).

[0100] Zu dieser Zeit führt der OTA-Master 4 parallel zu einem Herunterladen und Beschaffen des verschlüsselten Aktualisierungspaketes von dem CDN 8 einen AES-Blockverschlüsselungsprozess des Zählerwertes mit dem AES-Schlüssel aus, um den Zählerwert zu verschlüsseln (B074). Der OTA-Master 4 führt einen XOR-Betrieb durch und entschlüsselt den verschlüsselten Zählerwert und das verschlüsselte Aktualisierungspaket, das von dem CDN 8 heruntergeladen wurde (B075). Der OTA-Master 4 erzeugt und verifiziert einen MAC in dem AES-CBC-Modus aus dem Klartext des entschlüsselten Aktualisierungspaketes unter Verwendung des MAC-Schlüssels (B076). Wenn die MACs übereinstimmen, überträgt der OTA-Master 4 das entschlüsselte Aktualisierungspaket an die Ziel-ECU 5 und installiert das Aktualisierungspaket in der Ziel-ECU 5 (B077). Wenn die MACs nicht übereinstimmen, beendet der OTA-Master 4 den Prozess. Wenn der Prozess aufgrund einer fehlenden Übereinstimmung der MACs beendet wird, kann der OTA-Master 4 ein Protokoll aufzeichnen, das angibt, dass der Prozess aufgrund der fehlenden Übereinstimmung der MACs beendet wurde, und einen Fehler in einer HMI (nicht dargestellt) anzeigen. Alternativ kann der OTA-Master 4 einen XOR-Betrieb durchführen und das verschlüsselte Aktualisierungspaket entschlüsseln, und kann das entschlüsselte Aktualisierungspaket an die Ziel-ECU 5 übertragen. In diesem Fall kann der OTA-Master 4 ausgelegt sein, den MAC in dem AES-CBC-Modus aus dem Klartext des entschlüsselten Aktualisierungspaketes unter Verwendung des MAC-Schlüssels zu erzeugen und verifizieren und der Ziel-ECU 5 die Löschung der Installation mitteilen, wenn bestimmt wird, dass die MACs nicht übereinstimmen.

[0101] Wie es oben beschrieben ist, können gemäß der siebten Ausführungsform die folgenden vorteilhaften Wirkungen erzielt werden.

[0102] Der CCMP-Modus wird als eine Kommunikationsverschlüsselung und eine Maßnahme gegen eine Verfälschung von Daten zwischen dem OTA-Zentrum 2 und dem OTA-Master 4 verwendet. Unter Verwendung des CCMP-Modus ist es möglich, eine Datenverfälschungsgegenmaßnahme zusätzlich zu der Kommunikationspfadverschlüsselung bereitzustellen, wenn der OTA-Master 4 das Aktualisierungspaket von dem OTA-Zentrum 2 herunterlädt. Als Ergebnis kann die Sicherheit gewährleistet werden, und es kann eine noch sicherere OTA-Verteilung realisiert werden.

Achte Ausführungsform

[0103] Die achte Ausführungsform wird mit Bezug auf die **Fig. 68 bis 77** beschrieben. In der achten Ausführungsform wird ein Galois/Zähler-Modusprotokoll (GCMP-Modus) als eine Kommunikationspfadverschlüsselung und eine Maßnahme gegen eine Datenverfälschung verwendet.

[0104] Wie es in den **Fig. 69 bis 71** dargestellt ist, ist in diesem Fall, wenn die Konfiguration, die den GCMP-Modus verwendet, mit der Konfiguration, die den CCMP-Modus verwendet, oder der Konfiguration, die die Entschlüsselung und Signaturverifizierung von AES CBC-HMAC SHA2 als das herkömmliche Verfahren verwendet, verglichen wird, in beiden Fällen die Verarbeitungszeit des Hardwarebeschleunigers gegenüber der Verarbeitungszeit des Hauptkerns dominant, aber es kann der Durchsatz unter Verwendung des GCMP-Modus weiter verbessert werden.

[0105] Im Folgenden wird der Betrieb der oben beschriebenen Konfiguration mit Bezug auf die **Fig. 72 bis 77** beschrieben.

(8-1) Prozess des OTA-Zentrums 2 (siehe Figuren 72 bis 74)

[0106] Das OTA-Zentrum 2 erzeugt einen AES-Schlüssel zur Verschlüsselung des Aktualisierungspaketes und einen MAC-Schlüssel zur Verhinderung einer Verfälschung des Aktualisierungspaketes (A081). Das OTA-Zentrum 2 verschlüsselt das Aktualisierungspaket mit dem erzeugten AES-Schlüssel und dem erzeugten MAC-Schlüssel in dem GCMP-Modus und weist einen MAC zu (A082). Das OTA-Zentrum 2 verschlüsselt den AES-Schlüssel und den MAC-Schlüssel mit dem öffentlichen RSA-Schlüssel (A083). Das OTA-Zentrum 2 speichert den AES-Schlüssel und den MAC-Schlüssel, die mit dem öffentlichen RSA-Schlüssel verschlüsselt sind, in der Kampagnenmeldung (A084). Das OTA-Zentrum 2 platziert ein Aktualisierungspaket, das mit dem AES-Schlüssel und dem MAC-Schlüssel verschlüsselt ist, in dem CDN 8 (A085). Das OTA-Zentrum 2 überträgt eine Kampagnenmeldung, in der der verschlüsselte AES-Schlüssel und der verschlüsselte MAC-Schlüssel gespeichert sind, an das neu zu programmierende fahrzeugseitige System 3 (A086).

(8-2) Prozess des OTA-Masters 4 (siehe Figuren 75 bis 77)

[0107] Wenn die Kampagnenmeldung beschafft wird, da die Kampagnenmeldung, die von dem OTA-Zentrum 2 übertragen wird, durch den OTA-Master 4 empfangen wird, beschafft der OTA-Master 4 einen AES-Schlüssel und einen MAC-Schlüssel

aus der beschafften Kampagnenmeldung (B081). Der OTA-Master 4 entschlüsselt den verschlüsselten AES-Schlüssel und verschlüsselten MAC-Schlüssel mit dem geheimen RSA-Schlüssel, um den AES-Schlüssel und den MAC-Schlüssel zu extrahieren (B082). Der OTA-Master 4 lädt und beschafft das verschlüsselte Aktualisierungspaket von dem CDN 8 (B083).

[0108] Zu dieser Zeit führt der OTA-Master 4 parallel zu einem Herunterladen und Beschaffen des verschlüsselten Aktualisierungspaketes von dem CDN 8 einen AES-Blockverschlüsselungsprozess des Zählerwertes mit dem AES-Schlüssel aus, um den Zählerwert zu verschlüsseln (B084). Der OTA-Master 4 führt einen XOR-Betrieb aus und entschlüsselt den verschlüsselten Zählerwert und das verschlüsselte Aktualisierungspaket, das von dem CDN 8 heruntergeladen wurde (B085). Der OTA-Master 4 erzeugt und verifiziert einen MAC in dem GMAC-Modus aus dem Klartext des entschlüsselten Aktualisierungspaketes unter Verwendung des MAC-Schlüssels (B086). Wenn die MACs übereinstimmen, überträgt der OTA-Master das entschlüsselte Aktualisierungspaket an die Ziel-ECU 5 und installiert das Aktualisierungspaket in der Ziel-ECU 5 (B087).

[0109] Wie es oben beschrieben ist, können gemäß der achten Ausführungsform die folgenden Wirkungen erzielt werden.

[0110] Der GCMP-Modus wird als eine Kommunikationspfadverschlüsselung und eine Maßnahme gegen eine Datenverfälschung zwischen dem OTA-Zentrum 2 und dem OTA-Master 4 verwendet. Wenn der OTA-Master 4 das Aktualisierungspaket von dem OTA-Zentrum 2 herunterlädt, ist es unter Verwendung des GCMP-Modus möglich, eine Datenverfälschungsgegenmaßnahme zusätzlich zu der Kommunikationspfadverschlüsselung bereitzustellen. Als Ergebnis kann die Sicherheit verbessert werden, und es kann eine noch sicherere OTA-Verteilung realisiert werden.

Neunte Ausführungsform

[0111] Die neunte Ausführungsform wird mit Bezug auf die **Fig. 78 bis 86** beschrieben. In der neunten Ausführungsform wird nicht nur das CDN 8, sondern auch ein Smartphone, ein USB-Speicher oder Ähnliches für die Verteilungsrouten der Aktualisierungsdaten verwendet, um der Vielzahl von Verteilungsrouten gerecht zu werden, so dass der Freiheitsgrad des OTA-Aktualisierungssystems des Nutzers erhöht wird. Das Smartphone oder der USB-Speicher entsprechen einem Aufzeichnungsmedium. Im Folgenden wird das Smartphone oder der USB-Speicher als ein Beispiel des Speichermediums beschrieben, aber es kann eine SD-Karte, eine Mikro-SD-Karte,

ein Kompakt-Flash-Speicher oder Ähnliches als Speichermedium verwendet werden.

[0112] Im Folgenden wird der Betrieb der oben beschriebenen Konfiguration mit Bezug auf die **Fig. 79 bis 86** beschrieben.

(9-1) Prozess des OTA-Zentrums 2 (siehe Figuren 79 bis 82)

[0113] Das OTA-Zentrum 2 erzeugt einen gemeinsamen Schlüssel zur Verschlüsselung des Aktualisierungspaketes (A091). Das OTA-Zentrum 2 verschlüsselt das Aktualisierungspaket in einem speziellen Verschlüsselungsmodus unter Verwendung des erzeugten gemeinsamen Schlüssels (A092). Das OTA-Zentrum 2 verschlüsselt den gemeinsamen Schlüssel mit dem öffentlichen RSA-Schlüssel (A093). Das OTA-Zentrum 2 speichert den gemeinsamen Schlüssel, der mit dem öffentlichen RSA-Schlüssel verschlüsselt ist, in der Kampagnenmeldung (A094). Das OTA-Zentrum 2 erzeugt RP-Metadaten, die das Gemeinsamer-Schlüssel-Verschlüsselungsverfahren und die Verteilungsrouten enthalten (A095). Das OTA-Zentrum verschlüsselt die RP-Metadaten mit dem öffentlichen RSA-Schlüssel (A096). Das OTA-Zentrum 2 platziert das Aktualisierungspaket, das mit dem gemeinsamen Schlüssel verschlüsselt ist, und die RP-Metadaten, die mit dem öffentlichen RSA-Schlüssel verschlüsselt sind, in dem CDN 8 (A097). Das OTA-Zentrum 2 überträgt eine Kampagnenmeldung, in der der verschlüsselte gemeinsame Schlüssel gespeichert ist, an das neu zu programmierende fahrzeugseitige System 3 (A098).

(9-2) Prozess des OTA-Masters 4 (siehe Figuren 83 bis 86)

[0114] Wenn die Kampagnenmeldung beschafft wird, da die Kampagnenmeldung, die von dem OTA-Zentrum 2 übertragen wird, durch den OTA-Master 4 empfangen wird, beschafft der OTA-Master 4 den verschlüsselten gemeinsamen Schlüssel aus der beschafften Kampagnenmeldung (B091). Der OTA-Master 4 entschlüsselt den verschlüsselten gemeinsamen Schlüssel mit dem geheimen RSA-Schlüssel, um den gemeinsamen Schlüssel zu extrahieren (B092). Der OTA-Master 4 lädt und beschafft die verschlüsselten RP-Metadaten von dem CDN 8 (B093). Der OTA-Master 4 entschlüsselt die verschlüsselten RP-Metadaten mit dem geheimen RSA-Schlüssel, um die RP-Metadaten zu extrahieren (B094). Der OTA-Master 4 interpretiert den Inhalt der RP-Metadaten und identifiziert das Gemeinsamer-Schlüssel-Verschlüsselungsverfahren und die Verteilungsrouten (B095). Der OTA-Master 4 beschafft das verschlüsselte Aktualisierungspaket über die identifizierte Verteilungsrouten (B096). D.h., in einem Fall, in dem das Smartphone als Verteilungsrouten

identifiziert wird, lädt der OTA-Master 4 das verschlüsselte Aktualisierungspaket von dem CDN 8 über das Smartphone durch das Batch-Verfahren herunter. In einem Fall, in der USB-Speicher als Verteilungsrouten identifiziert wird, lädt der OTA-Master 4 das verschlüsselte Aktualisierungspaket von dem CDN 8 über den USB-Speicher durch das Batch-Speicherverfahren herunter. Danach führt der OTA-Master 4 den Prozess in und nach Schritt B014, der in der ersten Ausführungsform beschrieben ist, durch, wenn der CTR-Modus als der spezielle Verschlüsselungsmodus verwendet wird, oder führt den Prozess in und nach Schritt B024, der in der zweiten Ausführungsform beschrieben ist, durch, wenn der OFB-Modus als der spezielle Verschlüsselungsmodus verwendet wird.

[0115] Wie es oben beschrieben ist, können gemäß der neunten Ausführungsform die folgenden vorteilhaften Wirkungen erzielt werden.

[0116] Das Aktualisierungspaket wird von dem CDN 8 über ein Aufzeichnungsmedium wie beispielsweise ein Smartphone oder einen USB-Speicher beschafft. Die Verteilungsrouten des Aktualisierungspaketes weist somit eine Diversität auf, und es kann diejenige Verteilungsrouten, die bessere Verteilungskosten und eine bessere Verfügbarkeit aufweist, ausgewählt werden. Als Ergebnis können die Verteilungskosten geeignet verringert werden, wenn der OTA-Master 4 das Aktualisierungspaket von dem OTA-Zentrum 2 herunterlädt, und es kann der Nutzererfahrungswert verbessert werden. In der oben beschriebenen Ausführungsform interpretiert der OTA-Master 4 den Inhalt der RP-Metadaten in Schritt B095, um das Gemeinsamer-Schlüssel-Verschlüsselungsverfahren und die Verteilungsrouten zu identifizieren. Wenn mehrere Verteilungsrouten in den RP-Metadaten beschrieben sind, kann der OTA-Master 4 irgendeine der Verteilungsrouten auswählen.

Zehnte Ausführungsform

[0117] Die zehnte Ausführungsform wird mit Bezug auf die Fig. 87 bis 98 beschrieben. In der zehnten Ausführungsform werden mehrere CDN-Verkäufer dynamisch als Platzierungsziele des Aktualisierungspaketes für das CDN 8 entsprechend einem Verteilungsverfahren, einem OTA-Zielbereich, der ein Verteilungsbereich ist, und einer Verteilungsdatengröße ausgewählt, und es werden die Verteilungskosten verringert. Der Kostenvergleich des CDN ist in Fig. 88 und Fig. 89 gezeigt. Die Preistabelle ist in den Fig. 90 bis 93 dargestellt. Jeder CDN-Verkäufer weist eine andere Überlegenheit und Unterlegenheit hinsichtlich des Preises je nach Verteilungsbereich, Verteilungsdatengröße und Ähnliches in Japan, Nordamerika und Ähnlichem auf. Wenn beispielsweise wie in Fig. 90 gezeigt eine Datengröße von 100 TB je Monat verteilt bzw. gelie-

fert wird, ist in Japan das CDN 2 das kostengünstigste, aber das CDN 1 ist das kostengünstigste in Nordamerika und in der EU. Auf der Grundlage dieser Feststellung wird ein CDN-Verkäufer mit den niedrigsten Verteilungskosten entsprechend dem Verteilungsverfahren, dem OTA-Zielbereich und der Verteilungsdatengröße ausgewählt.

[0118] Wie es in Fig. 94 dargestellt ist, enthält das OTA-Zentrum 2 einen CDN-Verkäuferauswahlabschnitt 2j zusätzlich zu dem Gemeinsamer-Schlüssel-Erzeugungsabschnitt 2a, dem Aktualisierungspaketverschlüsselungsabschnitt 2b, dem Gemeinsamer-Schlüssel-Verschlüsselungsabschnitt 2c, dem Gemeinsamer-Schlüssel-Speicherabschnitt 2d, dem Verschlüsselungspaketplatzierungsabschnitt 2e und dem Kampagnenmeldungsübertragungsabschnitt 2f. Der CDN-Verkäuferauswahlabschnitt 2j wählt einen CDN-Verkäufer durch Bezugnahme auf die CDN-Verkäuferverwaltungsdatenbank (Datenbank wird hier auch als DB abgekürzt) aus.

[0119] Im Folgenden wird der Betrieb der oben beschriebenen Konfiguration mit Bezug auf die Fig. 95 bis 98 beschrieben.

(10-1) Prozess des OTA-Zentrums 2 (siehe Figuren 95 bis 98)

[0120] Das OTA-Zentrum 2 erzeugt einen AES-Schlüssel zur Verschlüsselung des Aktualisierungspaketes (A101). Das OTA-Zentrum 2 verschlüsselt das Aktualisierungspaket mit dem erzeugten AES-Schlüssel in dem CTR-Modus (A102). Das OTA-Zentrum 2 verschlüsselt den AES-Schlüssel mit dem öffentlichen RSA-Schlüssel (A103). Das OTA-Zentrum 2 speichert den AES-Schlüssel, der mit dem öffentlichen RSA-Schlüssel verschlüsselt ist, in der Kampagnenmeldung (A104). Das OTA-Zentrum 2 identifiziert das Verteilungsverfahren (A105), identifiziert den OTA-Zielbereich (A106), identifiziert die Verteilungsdatengröße (A107) und nimmt Bezug auf die Preistabelle in der CDN-Verkäuferverwaltungsdatenbank unter Verwendung des Verteilungsverfahrens, des OTA-Zielbereiches und der Verteilungsdatengröße als Schlüssel (A108). In diesem Fall kann das OTA-Zentrum 2 Bezug auf die Preistabelle unter Verwendung mindestens eines aus den Folgenden als Schlüssel Bezug nehmen: ein Verteilungsverfahren wie beispielsweise ein Speicherverfahren oder ein Streaming-Verfahren, ein OTA-Zielbereich wie beispielsweise Japan, Nordamerika oder die Europäische Union (EU), und eine Verteilungsdatengröße wie beispielsweise GB, TB oder PB. Das OTA-Zentrum 2 wählt einen CDN-Verkäufer mit dem niedrigsten Verteilungskosten für einen jeweiligen Bereich aus und platziert ein Aktualisierungspaket, das mit einem AES-Schlüssel verschlüsselt ist, in dem ausgewählten CDN 8 (A109, entspricht einem CDN-Ver-

käuferauswahlschritt). Alternativ kann das OTA-Zentrum 2 ein Aktualisierungspaket, das mit einem AES-Schlüssel verschlüsselt ist, in jedem CDN 8 platzieren. Das OTA-Zentrum 2 überträgt den verschlüsselten AES-Schlüssel und eine Kampagnenmeldung, in der das Datenspeicherziel des Aktualisierungspaketes und URI-Informationen gespeichert sind, so dass auf den ausgewählten CDN-Verkäufer zugegriffen werden kann, an das neu zu programmierende fahrzeugseitige System 3 (A110).

(10-2) Prozess des OTA-Masters 4

[0121] Der Prozess des OTA-Masters 4 ist ähnlich wie der Prozess (**Fig. 12 bis 14**) des OTA-Masters 4, der in der ersten Ausführungsform beschrieben wurde.

[0122] Wie es oben beschrieben ist, können gemäß der zehnten Ausführungsform die folgenden vorteilhaften Wirkungen erzielt werden.

[0123] Durch Bezugnahme auf die CDN-Verkäuferverwaltungsdatenbank wird das CDN 8 mit den besten Verteilungskosten aus mehreren CDNs 8, die unterschiedliche Verteilungskosten aufweisen, entsprechend dem Verteilungsverfahren, dem OTA-Zielbereich und der Verteilungsdatengröße ausgewählt, und das Aktualisierungspaket wird in dem ausgewählten CDN 8 platziert. Es ist möglich, die Verteilungskosten geeignet zu verringern, wenn der OTA-Master 4 das Aktualisierungspaket von dem OTA-Zentrum 2 herunterlädt. Außerdem gibt es durch Verschlüsseln des Aktualisierungspaketes in dem OTA-Zentrum 2 im Prinzip kein Sicherheitsproblem, und zwar auch dann nicht, wenn es keine Vertrauenswürdigkeit aufweist (Zero Trust). Daher besteht keine Notwendigkeit, die Aktualisierungsdaten auf der Endseite des CDN 8 zu verschlüsseln, und es können die Verarbeitungslast und die Sicherheitsfunktionen des CDN 8 verringert werden. Bevor das Aktualisierungspaket den OTA-Master 4 von dem OTA-Zentrum 2 aus erreicht, wird sogar dann, wenn es eine Datenverfälschung gibt oder das CDN 8 einem DDoS-Angriff auf einem Zwischenpfad ausgesetzt wird, das OTA-System nicht beeinflusst, und es ist möglich, auf intelligente Sicherheitsmaßnahmen, beispielsweise Sicherheitshilfsmaßnahmen einer Mehrschichtverteidigung wie beispielsweise einer Web-Anwendungs-Firewall, einer TLS-Kommunikation und einer signierten URL, die den OTA-Master 4 für die Verteilung beschränkt, zu verzichten. Als Ergebnis können die laufenden Kosten des OTA-Systems auf einer Kostengrundlage verringert werden, und es können die Verteilungskosten in einer beliebigen Systemkonfiguration verringert werden.

Elfte Ausführungsform

[0124] Die elfte Ausführungsform wird mit Bezug auf die **Fig. 99 bis 108** beschrieben. In der elften Ausführungsform wird ein Diffie-Hellman-Schlüsselaustausch (im Folgenden als DHE abgekürzt) oder ein Elliptic-Curve-Diffie-Hellmann-Schlüsselaustausch (im Folgenden als ECDHE abgekürzt) zur Schlüsselverteilung zwischen dem OTA-Zentrum 2 und dem OTA-Master 4 verwendet, und das OTA-Zentrum 2 verschlüsselt den AES-Schlüssel auf der Grundlage von ausgetauschten geheimen Informationen, die für jedes Fahrzeug unterschiedlich sind, und verteilt den verschlüsselten AES-Schlüssel an den OTA-Master 4, so dass ein Fahrzeugmodell, das für das CDN 8 verwendbar ist, oder ein Aktualisierungspaket, das für eine jeweilige spezielle Fahrzeuggruppe verwendbar ist, verteilt wird, wodurch der Vorteil genutzt werden kann, dass eine Vorwärts-Geheimhaltung des ECDHE gewährleistet werden kann.

[0125] Wie es in **Fig. 100** dargestellt ist, erzeugen und tauschen beide Seiten jeweilige öffentliche Schlüssel (A, B) aus zufälligen Zahlen bzw. Zufallszahlen (= geheime Schlüssel a, b) aus und führen eine Berechnung in Kombination mit ihren eigenen geheimen Schlüsseln durch, wodurch die geheimen Informationen (S) geheim ausgetauscht werden. Paare aus dem geheimen Schlüssel und dem öffentlichen Schlüssel (a/A, b/B) können nach dem Austausch der geheimen Informationen (S) verworfen werden, und sowohl das OTA-Zentrum 2 als auch der OTA-Master 4 müssen die Paare aus dem geheimen Schlüssel und dem öffentlichen Schlüssel nicht in einem HSM (Hardware-Sicherheitsmodul) speichern, so dass die geheimen Informationen (S) sehr sicher ausgetauscht werden können. Die ausgetauschten geheimen Informationen (S) können für einen Schlüssel einer Gemeinsamer-Schlüssel-Verschlüsselung oder Ähnliches verwendet werden, aber da die Originaldaten eine Zufallszahl (a, b) sind, sind die ausgetauschten geheimen Informationen (S) für jeden OTA-Master 4 ein anderer Schlüssel.

[0126] Im Folgenden wird der Betrieb der oben beschriebenen Konfiguration mit Bezug auf die **Fig. 101 bis 108** beschrieben.

(11-1) Prozess des OTA-Zentrums 2 (siehe Figuren 101 bis 104)

[0127] Das OTA-Zentrum 2 erzeugt einen AES-Schlüssel zur Verschlüsselung des Aktualisierungspaketes (A111). Das OTA-Zentrum 2 verschlüsselt das Aktualisierungspaket mit dem erzeugten AES-Schlüssel in dem CTR-Modus (A112). Das OTA-Zentrum 2 erzeugt ein Schlüsselpaar des ECDHE aus der Zufallszahl (A113). Das OTA-Zentrum 2 tauscht einen geheimen Schlüssel mit dem OTA-

Master 4 in dem ECDHE-Algorithmus aus (A114, entspricht einem Geheiminformaustauschschritt). Das OTA-Zentrum 2 verschlüsselt den AES-Schlüssel mit dem geheimen Schlüssel (A115). Das OTA-Zentrum 2 speichert den AES-Schlüssel, der mit dem geheimen Schlüssel verschlüsselt ist, in der Kampagnenmeldung (A116). Das OTA-Zentrum 2 platziert das Aktualisierungspaket, das mit dem AES-Schlüssel verschlüsselt ist, in dem CDN 8 (A117). Das OTA-Zentrum 2 überträgt eine Kampagnenmeldung, in der der verschlüsselte AES-Schlüssel gespeichert ist, an das neu zu programmierende fahrzeugseitige System 3 (A118, entspricht einem Verschlüsselungsschlüsselverteilungsschritt).

[0128] Hier wird Schritt A114 beschrieben. Wenn die Zündung des Fahrzeugs eingeschaltet wird und eine vorbestimmte Zeitdauer seit der Synchronisation der vorherigen Fahrzeugkonfigurationsinformationen verstrichen ist, fragt der OTA-Master 4 die ECU, die in dem Fahrzeug montiert ist, nach der Programmversion und sammelt die Fahrzeugkonfigurationsinformationen. Alternativ fragt der OTA-Master 4 auf ein Empfangen der Push-Meldung betreffend die Kampagne von dem OTA-Zentrum 2 hin die ECU nach der Programmversion und sammelt die Fahrzeugkonfigurationsinformationen. Auf ein Sammeln der Fahrzeugkonfigurationsinformationen hin errichtet der OTA-Master 4 eine TLS-Kommunikation mit dem OTA-Zentrum 2, um die Fahrzeugkonfigurationsinformationen an das OTA-Zentrum 2 zu übertragen. Zu dieser Zeit sammelt der OTA-Master 4 die Fahrzeugkonfigurationsinformationen und erzeugt ein Schlüsselpaar des ECDHE. Wenn die TLS-Kommunikation mit dem OTA-Zentrum 2 errichtet wird, überträgt der OTA-Master 4 einen öffentlichen Schlüssel des OTA-Masters 4 des Schlüsselpaares an das OTA-Zentrum 2. Der Prozess, in dem der OTA-Master 4 die Fahrzeugkonfigurationsinformationen sammelt, wird auch für andere Ausführungsformen verwendet. Das OTA-Zentrum 2 beschafft einen geheimen Schlüssel in dem ECDHE-Algorithmus auf der Grundlage des öffentlichen Schlüssels des OTA-Masters 4, der von dem OTA-Master 4 beschafft wird, und des geheimen Schlüssels des OTA-Zentrums 2.

(11-2) Prozess des OTA-Masters 4 (siehe Figuren 105 bis 108)

[0129] Der OTA-Master 4 erzeugt ein Schlüsselpaar des ECDHE aus der Zufallszahl (B111). Der OTA-Master 4 tauscht einen geheimen Schlüssel mit dem OTA-Zentrum 2 in dem ECDHE-Algorithmus aus (B112, entspricht einem Geheiminformaustauschschritt). Wenn der OTA-Master 4 eine Kampagnenmeldung beschafft, da die Kampagnenmeldung, die von dem OTA-Zentrum 2 übertragen wird, durch den OTA-Master 4 empfangen wird, beschafft der OTA-Master 4 einen AES-Schlüssel

aus der beschafften Kampagnenmeldung (B113). Der OTA-Master 4 entschlüsselt den verschlüsselten AES-Schlüssel mit dem geheimen Schlüssel, um einen AES-Schlüssel zu extrahieren (B114). Der OTA-Master 4 lädt und beschafft das verschlüsselte Aktualisierungspaket von dem CDN 8 (B115).

[0130] Zu dieser Zeit führt der OTA-Master 4 parallel zu einem Herunterladen und Beschaffen des verschlüsselten Aktualisierungspaketes von dem CDN 8 einen AES-Blockverschlüsselungsprozess des Zählerwertes mit dem AES-Schlüssel aus, um den Zählerwert zu verschlüsseln (B116). Der OTA-Master 4 führt einen XOR-Betrieb durch und entschlüsselt den verschlüsselten Zählerwert und das verschlüsselte Aktualisierungspaket, das von CDN 8 heruntergeladen wurde (B117). Der OTA-Master 4 überträgt das entschlüsselte Aktualisierungspaket an die Ziel-ECU 5 und installiert das Aktualisierungspaket in der Ziel-ECU 5 (B118).

[0131] Wie es oben beschrieben ist, können gemäß der elften Ausführungsform die folgenden vorteilhaften Wirkungen erzielt werden.

[0132] Es wird DHE oder ECDHE zur Schlüsselverteilung zwischen dem OTA-Zentrum 2 und dem OTA-Master 4 verwendet, und das OTA-Zentrum 2 verschlüsselt den AES-Schlüssel auf der Grundlage der geheimen Informationen, die für jedes für den Austausch vorgesehene Fahrzeug unterschiedlich sind, und verteilt den AES-Schlüssel an den OTA-Master 4. Als Ergebnis kann eine effiziente Verteilung der Aktualisierungsdaten durch das CDN 8 realisiert werden, während die Vorwärts-Geheimhaltung des ECDHE gewährleistet wird.

Modifikation der elften Ausführungsform

[0133] Eine Modifikation der elften Ausführungsform wird mit Bezug auf die **Fig.** 166 bis 173 beschrieben. Die elfte Ausführungsform basiert auf der Annahme, dass eine Drahtloskommunikationseinheit an dem Fahrzeug montiert ist und der OTA-Master 4 Daten mit dem OTA-Zentrum 2 oder dem CDN 8 über eine Drahtloskommunikationsleitung bzw. -verbindung austauschen kann. Es jedoch einen Fall geben, in dem die Drahtloskommunikationseinheit nicht an dem Fahrzeug montiert ist, oder einen Fall, in dem der Nutzer nicht wünscht, die Drahtloskommunikationsleitung zu verwenden. In der Modifikation der elften Ausführungsform wird eine Situation beschrieben, in der der OTA-Master 4 keine Daten über eine Drahtloskommunikationsleitung mit dem OTA-Zentrum austauscht, sondern stattdessen eine Programaktualisierung unter Verwendung eines Speichermediums wie beispielsweise einer SD-Karte ausführt.

[0134] Der OTA-Master 4 und das OTA-Zentrum 2 verwenden ein Speichermedium zur Datenübertragung mit der Außenseite. Eine Datenübertragung zwischen dem OTA-Master 4 und dem Speichermedium verwendet einen Port für das Speichermedium, der in dem Fahrzeug installiert ist. Der Port, der in dem Fahrzeug installiert ist, ist ein Port, der beispielsweise in einer Fahrzeugnavigationseinheit, einer zentralen Anzeigeeinheit oder einer anderen Fahrzeugsteuerungseinheit installiert ist.

[0135] Eine Datenübertragung zwischen dem OTA-Zentrum 2 und dem Speichermedium wird durch Verbinden des Speichermediums mit einem Personalcomputer (im Folgenden als PC abgekürzt) durchgeführt. Das Speichermedium wird beispielsweise mit einem PC verbunden, es wird auf eine Webseite des OTA-Zentrums 2 oder des CDN 8 zugegriffen, und es werden Daten, die in dem Speichermedium gespeichert sind, durch Betreiben des PC zu dem OTA-Zentrum 2 hochgeladen, oder es werden Daten, die in dem OTA-Zentrum 2 gespeichert sind, durch Betreiben des PC auf das Speichermedium heruntergeladen. Ein Smartphone, ein Tablet oder Ähnliches, das mit dem Speichermedium kompatibel ist, kann anstelle des PC verwendet werden. Ein PC, ein Smartphone, ein Tablet oder Ähnliches, das mit dem Speichermedium kompatibel ist, wird auch als Betriebsendgerät bezeichnet.

[0136] Es wird mit Bezug auf die **Fig.** 166 bis 169 ein Fall beschrieben, in dem eine SD-Karte als ein Speichermedium verwendet wird. In diesem Fall wird der Prozess in der Reihenfolge einer Übertragung von Daten von dem OTA-Master 4 an eine SD-Karte 11, eines Hochladens von Daten von der SD-Karte 11 zu dem OTA-Zentrum 2, eines Herunterladens von Daten von dem OTA-Zentrum 2 auf die SD-Karte 11 und eines Übertragens von Daten von der SD-Karte 11 an den OTA-Master 4 durchgeführt.

[0137] Die Übertragung von Daten von dem OTA-Master 4 an die SD-Karte 11 wird mit Bezug auf **Fig.** 166 beschrieben. Der OTA-Master 4 beschafft Softwareversionsinformationen und Ähnliches von der Ziel-ECU 5, überträgt die beschafften Softwareversionsinformationen und Ähnliches an die SD-Karte 11 als Fahrzeugkonfigurationsinformationen und speichert die Fahrzeugkonfigurationsinformationen in der SD-Karte. Der OTA-Master 4 erzeugt ein Schlüsselpaar des ECDHE aus einer Zufallszahl und überträgt den öffentlichen ECDHE-Schlüssel an die SD-Karte 11 und speichert den öffentlichen ECDHE-Schlüssel dort. Die SD-Karte 11 speichert die Fahrzeugkonfigurationsinformationen, die von dem OTA-Master 4 übertragen werden, und den öffentlichen ECDHE-Schlüssel des OTA-Masters 4.

[0138] Mit Bezug auf **Fig.** 167 wird ein Hochladen von Daten von dem PC, mit dem die SD-Karte 11 ver-

bunden ist, zu dem OTA-Zentrum 2 beschrieben. Wenn die SD-Karte 11 verbunden ist, liest der PC die Fahrzeugkonfigurationsinformationen und den öffentlichen ECDHE-Schlüssel des OTA-Masters 4, die in der SD-Karte 11 gespeichert sind, aus und lädt die Fahrzeugkonfigurationsinformationen und den öffentlichen ECDHE-Schlüssel des OTA-Masters 4, die ausgelesen wurden, zu dem OTA-Zentrum 2 hoch. Die Fahrzeugkonfigurationsinformationen, die zu dem OTA-Zentrum 2 hochgeladen werden, werden durch einen Paketerzeugungsserver 6 verwendet, um das Vorhandensein oder die Abwesenheit einer Kampagne zu bestimmen. Der öffentliche ECDHE-Schlüssel des OTA-Masters 4, der zu dem OTA-Zentrum 2 hochgeladen wird, tauscht einen geheimen Schlüssel auf der Grundlage eines ECDHE-Algorithmus in dem Verteilungsserver 7 aus. Der geheime Schlüssel ist in diesem Fall ein für jedes Fahrzeug anderer geheimer Schlüssel.

[0139] Ein Herunterladen von Daten von dem OTA-Zentrum 2 auf die SD-Karte 11 wird mit Bezug auf **Fig.** 168 beschrieben. Hier ist ein Fall dargestellt, in dem es eine Kampagne gibt. Das OTA-Zentrum 2 lädt das Aktualisierungspaket, das mit dem AES-Schlüssel verschlüsselt ist, auf die SD-Karte 11 herunter und speichert das Aktualisierungspaket in dieser. Das OTA-Zentrum 2 erzeugt ein Schlüsselpaar des ECDHE aus einer Zufallszahl und lädt einen mit dem OTA-Master 4 auszutauschenden Schlüssel (der öffentliche ECDHE-Schlüssel des OTA-Zentrums 2), auf die SD-Karte 11 herunter, um den Schlüssel zu speichern. Das OTA-Zentrum 2 lädt die Kampagnenmeldung, in der der verschlüsselte AES-Schlüssel gespeichert ist, auf die SD-Karte 11 herunter und speichert die Kampagnenmeldung darin. Die SD-Karte 11 speichert das Aktualisierungspaket, das von dem OTA-Zentrum 2 heruntergeladen wurde, den öffentlichen ECDHE-Schlüssel des OTA-Zentrums 2 und den verschlüsselten AES-Schlüssel.

[0140] Die Übertragung von Daten von der SD-Karte 11 an den OTA-Master 4 wird mit Bezug auf **Fig.** 169 beschrieben. Der OTA-Master 4 liest und beschafft das verschlüsselte Aktualisierungspaket, den öffentlichen ECDHE-Schlüssel des OTA-Zentrums 2 und den verschlüsselten AES-Schlüssel, die in der SD-Karte 11 gespeichert sind, von der SD-Karte 11.

[0141] Im Folgenden wird der Betrieb der oben beschriebenen Konfiguration mit Bezug auf die **Fig.** 170 bis 174 beschrieben.

(11-3) Prozess des OTA-Masters 4 (siehe Figur 170)

[0142] Wenn die SD-Karte 11 mit dem fahrzeugseitigen System 3 verbunden und eine vorbestimmte Bedingung erfüllt ist, fordert der OTA-Master 4 die

Ziel-ECU 5 auf, Konfigurationsinformationen wie beispielsweise Softwareversionsinformationen zu übertragen und beschafft die Konfigurationsinformationen wie beispielsweise die Softwareversionsinformationen, die von der Ziel-ECU 5 übertragen werden, als Fahrzeugkonfigurationsinformationen (B1111). Auf ein Beschaffen der Fahrzeugkonfigurationsinformationen hin überträgt der OTA-Master 4 die beschafften Fahrzeugkonfigurationsinformationen an die SD-Karte 11 und speichert die Fahrzeugkonfigurationsinformationen darin (B1112). Der OTA-Master 4 erzeugt ein Schlüsselpaar des ECDHE aus einer Zufallszahl (B1113). In diesem Fall enthält das Schlüsselpaar den öffentlichen ECDHE-Schlüssel und den geheimen ECDHE-Schlüssel des OTA-Masters 4. Der OTA-Master 4 überträgt den öffentlichen ECDHE-Schlüssel des OTA-Masters 4 an die SD-Karte 11 und speichert den öffentlichen ECDHE-Schlüssel dort (B1114). Wenn die Fahrzeugkonfigurationsinformationen und der öffentliche ECDHE-Schlüssel des OTA-Masters 4 auf diese Weise gespeichert sind, wird die SD-Karte 11 von dem fahrzeugseitigen System 3 getrennt und mit dem PC verbunden.

(11-4) Prozess des PC (siehe Figur 171)

[0143] Wenn die SD-Karte 11 verbunden ist, liest der PC die Fahrzeugkonfigurationsinformationen und den öffentlichen ECDHE-Schlüssel des OTA-Masters 4, die in der SD-Karte 11 gespeichert sind, aus und lädt die Fahrzeugkonfigurationsinformationen und den öffentlichen ECDHE des OTA-Masters 4, die ausgelesen wurden, zu dem OTA-Zentrum 2 hoch (C1111). Der PC wartet auf einen Empfang der Kampagnenmeldung, in der der öffentliche ECDHE-Schlüssel und der AES-Schlüssel des OTA-Masters 4 gespeichert sind, und des verschlüsselten Aktualisierungspaketes von dem OTA-Zentrum 2 und wartet außerdem auf einen Empfang einer Meldung ohne Kampagne (C1112, C1113). Wenn bestimmt wird, dass die Kampagnenmeldung, in der der öffentliche ECDHE-Schlüssel und der AES-Schlüssel des OTA-Masters 4 gespeichert sind, und das verschlüsselte Aktualisierungspaket von dem OTA-Zentrum 2 empfangen wurden (C1112: ja), oder wenn bestimmt wird, dass eine Meldung ohne Kampagne empfangen wurde (C1113: ja), beendet der PC den Prozess.

(11-5) Prozess des OTA-Zentrums 2 (siehe Figur 172)

[0144] Das OTA-Zentrum 2 erzeugt einen AES-Schlüssel zur Verschlüsselung des Aktualisierungspaketes und verschlüsselt das Aktualisierungspaket mit dem AES-Schlüssel in dem CTR-Modus. Das OTA-Zentrum 2 beschafft die Fahrzeugkonfigurationsinformationen und den öffentlichen ECDHE-Schlüssel des OTA-Masters 4, die von dem PC heraufgeladen wurden, mit dem die SD-Karte 11 ver-

bunden wurde (A1111). Das OTA-Zentrum 2 bestimmt auf der Grundlage der Fahrzeugkonfigurationsinformationen, ob es eine Kampagne gibt (A1112). Wenn bestimmt wird, dass es keine Kampagne gibt (A1112: nein), überträgt das OTA-Zentrum 2 eine Meldung ohne Kampagne an den PC (A1113) und beendet den Prozess.

[0145] Wenn bestimmt wird, dass es eine Kampagne gibt (A1112: ja), erzeugt das OTA-Zentrum 2 ein Schlüsselpaar des ECDHE aus einer Zufallszahl (A1114). In diesem Fall ist das Schlüsselpaar der öffentliche ECDHE-Schlüssel und der geheime ECDHE-Schlüssel des OTA-Zentrums 2. Das OTA-Zentrum 2 lädt den öffentlichen ECDHE-Schlüssel des OTA-Zentrum 2 auf die SD-Karte 11 herunter und speichert den öffentlichen ECDHE-Schlüssel darin (A1115). Das OTA-Zentrum 2 erzeugt einen gemeinsamen ECDHE-Schlüssel (geheimer Schlüssel) aus dem geheimen ECDHE-Schlüssel des OTA-Zentrums 2 und dem öffentlichen ECDHE-Schlüssel des OTA-Masters 4 (A1116) und verschlüsselt den AES-Schlüssel mit dem erzeugten gemeinsamen ECDHE-Schlüssel (geheimer Schlüssel) (A1117). Das OTA-Zentrum 2 speichert den verschlüsselten AES-Schlüssel in der Kampagnenmeldung und lädt die Kampagnenmeldung, in der der verschlüsselte AES-Schlüssel gespeichert ist, auf die SD-Karte 11 herunter und speichert die Kampagnenmeldung darin (A1118). Das OTA-Zentrum 2 lädt das verschlüsselte Aktualisierungspaket auf die SD-Karte 11 herunter und speichert das verschlüsselte Aktualisierungspaket darin (A1119).

(11-6) Prozess des OTA-Masters 4 (siehe Figur 173)

[0146] Wenn die SD-Karte 11 mit dem fahrzeugseitigen System 3 verbunden ist, beschafft der OTA-Master 4 den öffentlichen ECDHE-Schlüssel, die Kampagnenmeldung und das Aktualisierungspaket des OTA-Zentrums 2 von der SD-Karte 11 (B1121). Der OTA-Master 4 erzeugt einen gemeinsamen ECDHE-Schlüssel (gemeinsamer Schlüssel) aus dem geheimen ECDHE-Schlüssel des OTA-Masters 4 und dem öffentlichen ECDHE-Schlüssel des OTA-Zentrums 2 (B1122). Der OTA-Master 4 extrahiert den verschlüsselten AES-Schlüssel aus der Kampagnenmeldung und entschlüsselt den verschlüsselten AES-Schlüssel mit dem gemeinsamen ECDHE-Schlüssel (geheimer Schlüssel) (B1123). Der OTA-Master 4 führt einen AES-Blockverschlüsselungsprozess des Zählerwertes mit dem AES-Schlüssel durch, um den Zählerwert zu verschlüsseln (B1124). Der OTA-Master 4 führt einen XOR-Betrieb durch und entschlüsselt den verschlüsselten Zählerwert und das verschlüsselte Aktualisierungspaket (B1125). Der OTA-Master 4 überträgt das entschlüsselte Aktualisierungspaket an die Ziel-ECU 5 und installiert das Aktualisierungspaket in der Ziel-ECU 5 (B1126).

[0147] Gemäß einer derartigen Konfiguration kann eine effiziente Verteilung der Aktualisierungsdaten durch das CDN 8 geeignet realisiert werden, während die Vorwärts-Geheimhaltung des ECDHE geeignet gewährleistet wird, ohne von einer Drahtloskommunikationsfunktion des fahrzeugseitigen Systems 3 abhängig zu sein. Durch Verringern der Häufigkeit der Datenübertragung zwischen dem OTA-Master 4 und der SD-Karte 11 und des Herauf- und Herunterladens zwischen dem OTA-Zentrum 2 und der SD-Karte 11 kann außerdem der Komfort für den Nutzer verbessert werden.

Zwölfte Ausführungsform

[0148] Die zwölfte Ausführungsform wird mit Bezug auf die **Fig. 109 bis 115** beschrieben. In der zwölften Ausführungsform ist in dem Schlüsselaustausch durch ECDHE die Zufallszahl *a*, die in dem OTA-Zentrum 2 erzeugt wird, eine Zufallszahl (Zufallszahl entsprechend einer speziellen Regel) für jedes Fahrzeugmodell, und die Zufallszahl *b*, die in dem OTA-Master 4 erzeugt wird, ein fester Wert, ein Zählwert oder ein Hash-Wert einer Softwareversion des OTA-Masters 4 oder irgendeine Kombination aus diesen für jedes Fahrzeugmodell, so dass ein geheimer Schlüssel, der durch ECDHE ausgetauscht wird, für die Fahrzeugmodelle gemeinsam ist, es wird ein Prozess zum Verteilen des Schlüssels weggelassen, und es wird der Vorteil der Gewährleistung der Vorwärts-Geheimhaltung von ECDHE gewährt und ein Verschlüsselungspaket, das für ein jeweiliges Fahrzeugmodell oder eine spezielle Fahrzeuggruppe anwendbar ist, durch das CDN verteilt.

[0149] Im Folgenden wird der Betrieb der oben beschriebenen Konfiguration mit Bezug auf die **Fig. 110 bis 115** beschrieben.

(12-1) Prozess des OTA-Zentrums 2 (siehe Figuren 110 bis 112)

[0150] Das OTA-Zentrum 2 erzeugt ein Schlüsselpaar von ECDHE aus einer Zufallszahl, die jedem Fahrzeugmodell oder jeder Fahrzeuggruppe gemeinsam ist (A121). Das OTA-Zentrum 2 tauscht einen geheimen Schlüssel mit dem OTA-Master 4 in dem ECDHE-Algorithmus aus (A122, entspricht einem Geheiminformationsaustauschschritt). In der vorliegenden Ausführungsform wird ein geheimer Schlüssel, der mit dem OTA-Master 4 in dem ECDHE-Algorithmus ausgetauscht wird, als ein AES-Schlüssel zum Verschlüsseln des Aktualisierungspaketes verwendet. Außerdem verwendet der OTA-Master 4 einen geheimen Schlüssel, der mit dem OTA-Zentrum 2 ausgetauscht wird, als einen AES-Schlüssel zum Entschlüsseln des verschlüsselten Aktualisierungspaketes. Das OTA-Zentrum 2 erzeugt einen AES-Schlüssel zum Verschlüsseln des Aktualisierungspaketes (A123). Das OTA-Zent-

rum 2 verschlüsselt das Aktualisierungspaket mit dem erzeugten AES-Schlüssel in dem CTR-Modus (A124). Das OTA-Zentrum 2 platziert das Aktualisierungspaket, das mit dem AES-Schlüssel verschlüsselt ist, in dem CDN 8 (A125). Das OTA-Zentrum 2 überträgt eine Kampagnenmeldung, in der der verschlüsselte AES-Schlüssel gespeichert ist, an das neu zu programmierende fahrzeugseitige System 3 (A126, entspricht einem Verschlüsselungsschlüsselverteilungsschritt).

(12-2) Prozess des OTA-Masters 4 (siehe Figuren 113 bis 115)

[0151] Der OTA-Master 4 erzeugt ein Schlüsselpaar des ECDHE aus der Zufallszahl, die entsprechend der oben genannten speziellen Regel erzeugt wird (B121). Das OTA-Zentrum 2 tauscht einen geheimen Schlüssel mit dem OTA-Master 4 in dem ECDE-Algorithmus aus (B122, entspricht einem Geheiminformationsaustauschschritt). Der OTA-Master 4 lädt und beschafft das verschlüsselte Aktualisierungspaket von dem CDN 8 (B123).

[0152] Zu dieser Zeit führt der OTA-Master 4 parallel zu einem Herunterladen und Beschaffen des verschlüsselten Aktualisierungspaketes von dem CDN 8 einen AES-Blockverschlüsselungsprozess des Zählerwertes mit dem AES-Schlüssel durch, um den Zählerwert zu verschlüsseln (B124). Der OTA-Master 4 führt einen XOR-Betrieb durch und entschlüsselt den verschlüsselten Zählerwert und das verschlüsselte Aktualisierungspaket, das von dem CDN 8 heruntergeladen wurde (B125). Der OTA-Master 4 überträgt das entschlüsselte Aktualisierungspaket an die Ziel-ECU 5 und installiert das Aktualisierungspaket in der Ziel-ECU 5 (B126).

[0153] Wie es oben beschrieben ist, können gemäß der zwölften Ausführungsform die folgenden vorteilhaften Wirkungen erzielt werden.

[0154] Es wird DHE oder ECDHE zur Schlüsselverteilung zwischen dem OTA-Zentrum 2 und dem OTA-Master 4 verwendet, und ein geheimer Schlüssel, der durch ECDHE ausgetauscht wird, ist für jedes Fahrzeugmodell gemeinsam. Als Ergebnis kann eine effiziente Verteilung der Aktualisierungsdaten durch das CDN 8 geeignet realisiert werden, während die Vorwärts-Geheimhaltung von ECDHE geeignet gewährleistet wird und die Zeit und Mühe der Schlüsselverteilung im Vergleich zu der elften Ausführungsform verringert werden.

Modifikation der zwölften Ausführungsform

[0155] Eine Modifikation der zwölften Ausführungsform wird mit Bezug auf die **Fig. 174 bis 181** beschrieben. Auch in der Modifikation der zwölften Ausführungsform wird wie in der Modifikation der elf-

ten Ausführungsform eine Situation beschrieben, bei der der OTA-Master 4 keine Daten mit dem OTA-Zentrum 2 oder dem CDN 8 über die Drahtloskommunikationsleitung austauscht und stattdessen eine Programmaktualisierung unter Verwendung eines Speichermediums wie beispielsweise einer SD-Karte ausführt.

[0156] Die Übertragung von Daten von dem OTA-Master 4 an die SD-Karte 11 wird mit Bezug auf **Fig. 174** beschrieben. Der OTA-Master 4 beschafft Softwareversionsinformationen und Ähnliches von der Ziel-ECU 5, überträgt die beschafften Softwareversionsinformationen und Ähnliches an die SD-Karte 11 als Fahrzeugkonfigurationsinformationen und speichert die Fahrzeugkonfigurationsinformationen darin. Der OTA-Master 4 erzeugt ein Schlüsselpaar von ECDHE, das für jedes Fahrzeugmodell gemeinsam ist, unter Verwendung eines festen Werts, eines Zählwerts oder eines Hash-Werts einer Softwareversion des OTA-Masters 4 oder irgendeiner Kombination aus diesen für jedes Fahrzeugmodell und überträgt einen Schlüssel, der mit dem OTA-Zentrum 2 auszutauschen ist (öffentlicher ECDHE-Schlüssel des OTA-Masters 4), an die SD-Karte 11 und speichert den Schlüssel darin. Irgendein Wert aus einem festen Wert, einem Zählwert und einem Hash-Wert einer Softwareversion des OTA-Masters 4 oder irgendeine Kombination aus diesen für jedes Fahrzeugmodell entspricht einer speziellen Regel. Die SD-Karte 11 speichert die Fahrzeugkonfigurationsinformationen, die von dem OTA-Master 4 übertragen werden, und den öffentlichen ECDHE-Schlüssel des OTA-Masters 4.

[0157] Mit Bezug auf **Fig. 175** wird ein Heraufladen von Daten von dem PC, mit dem die SD-Karte verbunden ist, an das OTA-Zentrum 2 beschrieben. Wenn die SD-Karte 11 verbunden ist, liest der PC die Fahrzeugkonfigurationsinformationen und den öffentlichen ECDHE-Schlüssel des OTA-Masters 4, die in der SD-Karte 11 gespeichert sind, aus und lädt die Fahrzeugkonfigurationsinformationen und den öffentlichen ECDHE-Schlüssel des OTA-Masters 4, die ausgelesen wurden, zu dem OTA-Zentrum 2 hoch. Die Fahrzeugkonfigurationsinformationen, die zu dem OTA-Zentrum 2 hochgeladen wurden, werden durch einen Paketerzeugungsserver 6 verwendet, um das Vorhandensein oder die Abwesenheit einer Kampagne zu bestimmen. Außerdem wird der öffentliche ECDHE-Schlüssel des OTA-Masters 4, der zu dem OTA-Zentrum 2 hochgeladen wurde, als ein geheimer Schlüssel auf der Grundlage eines ECDHE-Algorithmus in dem Verteilungsserver 7 geteilt bzw. getauscht. Der geheime Schlüssel ist in diesem Fall ein für jedes Fahrzeugmodell gemeinsamer geheimer Schlüssel.

[0158] Ein Herunterladen von Daten von dem OTA-Zentrum 2 an die SD-Karte 11 wird mit Bezug auf

Fig. 176 beschrieben. Das OTA-Zentrum 2 erzeugt ein Schlüsselpaar von ECDHE aus einer jedem Fahrzeugmodell oder jeder Fahrzeuggruppe gemeinsamen Zufallszahl, lädt einem mit dem OTA-Master 4 auszutauschenden Schlüssel (den öffentlichen ECDHE-Schlüssel des OTA-Zentrums 2), auf die SD-Karte 11 herunter, um den Schlüssel dort zu speichern. Das OTA-Zentrum 2 verschlüsselt das Aktualisierungspaket unter Verwendung des geheimen Schlüssels, der durch ECDHE ausgetauscht werden kann, als AES-Schlüssel und lädt das verschlüsselte Aktualisierungspaket zu der SD-Karte 11 herunter und speichert das Aktualisierungspaket dort. Die SD-Karte 11 speichert den öffentlichen ECDHE-Schlüssel und das Aktualisierungspaket des OTA-Zentrums 2, das von dem OTA-Zentrum 2 heruntergeladen wurde.

[0159] Die Übertragung von Daten von der SD-Karte 11 an den OTA-Master 4 wird mit Bezug auf **Fig. 177** beschrieben. Der OTA-Master 4 liest und beschafft das verschlüsselte Aktualisierungspaket und den öffentlichen ECDHE-Schlüssel des OTA-Zentrums 2, die in der SD-Karte 11 gespeichert sind. Der OTA-Master 4 tauscht einen geheimen Schlüssel auf der Grundlage des ECDHE-Algorithmus aus. Der OTA-Master 4 entschlüsselt das verschlüsselte Aktualisierungspaket unter Verwendung des geheimen Schlüssels, der durch ECDHE ausgetauscht bzw. geteilt wird, als AES-Schlüssel.

[0160] Im Folgenden wird der Betrieb der oben beschriebenen Konfiguration mit Bezug auf die **Fig. 178 bis 181** beschrieben.

(12-3) Prozess des OTA-Masters 4 (siehe Figur 178)

[0161] Wenn die SD-Karte 11 mit dem fahrzeugseitigen System 3 verbunden und eine vorbestimmte Bedingung erfüllt ist, fordert der OTA-Master 4 die Ziel-ECU 5 auf, Konfigurationsinformationen wie beispielsweise Softwareversionsinformationen zu übertragen und beschafft die Konfigurationsinformationen wie beispielsweise die Softwareversionsinformationen, die von der Ziel-ECU 5 übertragen werden, als Fahrzeugkonfigurationsinformationen (B1211). Auf ein Beschaffen der Fahrzeugkonfigurationsinformationen hin überträgt der OTA-Master 4 die beschafften Fahrzeugkonfigurationsinformationen an die SD-Karte 11 und speichert die Fahrzeugkonfigurationsinformationen darin (B1212). Der OTA-Master 4 erzeugt ein Schlüsselpaar von ECDHE aus einer Zufallszahl, die entsprechend einer speziellen Regel erzeugt wird (B1213). In diesem Fall enthält das Schlüsselpaar den öffentlichen ECDHE-Schlüssel und den geheimen ECDHE-Schlüssel des OTA-Masters 4. Der OTA-Master 4 überträgt den öffentlichen ECDHE-Schlüssel des OTA-Masters 4 an die SD-Karte 11 und speichert den öffentlichen ECDHE-Schlüssel

(B1214). Das Schlüsselpaar von ECDHE ist eine Zufallszahl, die entsprechend einer speziellen Regel wie in der zwölften Ausführungsform erzeugt wird, und ist jedem Fahrzeugmodell gemeinsam. Wenn die Fahrzeugkonfigurationsinformationen und der öffentliche ECDHE-Schlüssel des OTA-Masters 4 auf diese Weise gespeichert sind, wird die SD-Karte 11 von dem fahrzeugseitigen System 3 getrennt und mit dem PC verbunden.

(12-4) Prozess des PC (siehe Figur 179)

[0162] Wenn die SD-Karte 11 verbunden ist, liest der PC die Fahrzeugkonfigurationsinformationen und den öffentlichen ECDHE-Schlüssel des OTA-Masters 4, die in der SD-Karte 11 gespeichert sind, aus und lädt die Fahrzeugkonfigurationsinformationen und den öffentlichen ECDHE-Schlüssel des OTA-Masters 4, die ausgelesen wurden, zu dem OTA-Zentrum 2 hoch (C1211). Der PC wartet auf einen Empfang der Kampagnenmeldung, in der der öffentliche ECDHE-Schlüssel des OTA-Masters 4 gespeichert ist, und des verschlüsselten Aktualisierungspaketes von dem OTA-Zentrum 2 oder wartet auf einen Empfang einer Meldung ohne Kampagne (C1212, C1213). Wenn bestimmt wird, dass eine Kampagnenmeldung, in der der öffentliche ECDHE-Schlüssel des OTA-Masters 4 gespeichert ist, und ein verschlüsseltes Aktualisierungspaket von dem OTA-Zentrum 2 empfangen wurde (C1212: ja), oder wenn bestimmt wird, dass die Meldung ohne Kampagne empfangen wurde (C1213: ja), beendet der PC den Prozess.

(12-5) Prozess des OTA-Zentrums 2 (siehe Figur 180)

[0163] Das OTA-Zentrum 2 beschafft die Fahrzeugkonfigurationsinformationen und den öffentlichen ECDHE-Schlüssel des OTA-Masters 4, die von dem PC heraufgeladen wurden, mit dem die SD-Karte 11 verbunden ist (A1211). Das OTA-Zentrum 2 bestimmt der Grundlage der Fahrzeugkonfigurationsinformationen, ob es eine Kampagne gibt (A1212). Wenn bestimmt wird, dass es keine Kampagne gibt (A1212: nein), überträgt das OTA-Zentrum 2 die Meldung ohne Kampagne an den PC (A1213) und beendet den Prozess.

[0164] Wenn bestimmt wird, dass es eine Kampagne gibt (A1212: ja), erzeugt das OTA-Zentrum 2 ein Schlüsselpaar des ECDHE aus einer jedem Fahrzeugmodell oder jeder Fahrzeuggruppe gemeinsamen Zufallszahl (A1214). In diesem Fall ist das Schlüsselpaar der öffentliche ECDHE-Schlüssel und der geheime ECDHE-Schlüssel des OTA-Zentrums 2. Das OTA-Zentrum 2 lädt den öffentlichen ECDHE-Schlüssel des OTA-Zentrums 2 zu der SD-Karte 11 herunter und speichert den öffentlichen ECDHE-Schlüssel darin (A1215). Das OTA-Zentrum

2 erzeugt einen gemeinsamen ECDHE-Schlüssel (geheimer Schlüssel) aus dem geheimen ECDHE-Schlüssel des OTA-Zentrums 2 und dem öffentlichen ECDHE-Schlüssel des OTA-Masters 4 (A1216) und verschlüsselt das Aktualisierungspaket mit dem erzeugten gemeinsamen ECDHE-Schlüssel (geheimer Schlüssel) (A1217). Das OTA-Zentrum 2 lädt das verschlüsselte Aktualisierungspaket zu der SD-Karte 11 herunter und speichert das verschlüsselte Aktualisierungspaket darin (A1218).

(12-6) Prozess des OTA-Masters 4 (siehe Figur 181)

[0165] Wenn die SD-Karte 11 mit dem fahrzeugseitigen System 3 verbunden ist, beschafft der OTA-Master 4 den öffentlichen ECDHE-Schlüssel und das Aktualisierungspaket des OTA-Zentrums 2 von der SD-Karte 11 (B1221). Der OTA-Master 4 erzeugt einen gemeinsamen ECDHE-Schlüssel (geheimer Schlüssel) aus dem geheimen ECDHE-Schlüssel des OTA-Masters 4 und dem öffentlichen ECDHE-Schlüssel des OTA-Zentrums 2 (B1222). Der OTA-Master 4 führt einen AES-Blockverschlüsselungsprozess des Zählerwertes mit dem AES-Schlüssel aus, um den Zählerwert zu verschlüsseln (B1223). Der OTA-Master 4 führt einen XOR-Betrieb durch und entschlüsselt den verschlüsselten Zählerwert und das verschlüsselte Aktualisierungspaket (B1224). Der OTA-Master 4 überträgt das entschlüsselte Aktualisierungspaket an die Ziel-ECU 5 und installiert das Aktualisierungspaket in der Ziel-ECU 5 (B1225).

[0166] Gemäß einer derartigen Konfiguration kann eine effiziente Verteilung der Aktualisierungsdaten durch das CDN 8 geeignet realisiert werden, während die Vorwärts-Geheimhaltung von ECDHE geeignet gewährleistet wird, ohne von einer Drahtloskommunikationsfunktion des fahrzeugseitigen Systems 3 abhängig zu sein, und die Zeit und der Aufwand der Schlüsselverteilung können im Vergleich zu der elften Ausführungsform verringert werden. Außerdem kann durch Verringern der Häufigkeit der Datenübertragung zwischen dem OTA-Master 4 und der SD-Karte 11 und des Heraufladens und Herunterladens zwischen dem OTA-Zentrum 2 und der SD-Karte 11 der Komfort für den Nutzer verbessert werden.

Dreizehnte Ausführungsform

[0167] Die dreizehnte Ausführungsform wird mit Bezug auf die Fig. 116 bis 124 beschrieben. In der dreizehnten Ausführungsform wird nicht einfach der CTR-Modus angewendet, sondern es wird der Zählerwert sicherer ausgelegt. Insbesondere wird der CTR-Modus durch Einfügen einer Nonce in die Kampagnenmeldung, die als erstes zwischen dem OTA-Zentrum 2 und dem OTA-Master 4 zu kommunizieren ist, und Einfügen der Nonce in den Zählerwert siche-

rer gemacht. Der Verschlüsselungsprozess, in dem die Nonce in dem CTR-Modus eingefügt wird, ist in **Fig. 117** dargestellt, und der Entschlüsselungsprozess, in dem die Nonce in dem CTR-Modus eingefügt wird, ist in **Fig. 118** dargestellt.

[0168] Im Folgenden wird der Betrieb der oben beschriebenen Konfiguration mit Bezug auf die **Fig. 119** bis 124 beschrieben.

(13-1) Prozess des OTA-Zentrums 2 (siehe Figuren 119 bis 121)

[0169] Das OTA-Zentrum 2 erzeugt einen AES-Schlüssel zum Verschlüsseln des Aktualisierungspaketes (A131). Das OTA-Zentrum 2 erzeugt eine Nonce auf der Grundlage einer Zufallszahl (A132). Das OTA-Zentrum 2 verschlüsselt das Aktualisierungspaket mit dem erzeugten AES-Schlüssel und der Nonce in dem CTR-Modus (A133). Das OTA-Zentrum 2 verschlüsselt den AES-Schlüssel mit dem öffentlichen RSA-Schlüssel (A134). Das OTA-Zentrum 2 kann die Nonce mit dem öffentlichen RSA-Schlüssel gleichzeitig mit der Verschlüsselung des AES-Schlüssels mit dem öffentlichen RSA-Schlüssel verschlüsseln. Das OTA-Zentrum 2 speichert den AES-Schlüssel und die Nonce, die mit dem öffentlichen RSA-Schlüssel verschlüsselt sind, in der Kampagnenmeldung (A135). Das OTA-Zentrum 2 platziert das Aktualisierungspaket, das mit dem AES-Schlüssel verschlüsselt ist, in dem CDN 8 (A136). Das OTA-Zentrum 2 überträgt eine Kampagnenmeldung, in der der verschlüsselte AES-Schlüssel und die ggf. verschlüsselte Nonce gespeichert sind, an das neu zu programmierende fahrzeugseitige System 3 (A137).

(13-2) Prozess des OTA-Masters 4 (siehe Figuren 122 bis 124)

[0170] Wenn der OTA-Master 4 eine Kampagnenmeldung beschafft, da die Kampagnenmeldung, die von dem OTA-Zentrum 2 übertragen wird, durch den OTA-Master 4 empfangen wird, beschafft der OTA-Master 4 den AES-Schlüssel und die Nonce aus der beschafften Kampagnenmeldung (B131). Der OTA-Master 4 entschlüsselt den verschlüsselten AES-Schlüssel mit dem geheimen RSA-Schlüssel, um einen AES-Schlüssel zu extrahieren (B132). Der OTA-Master 4 lädt und beschafft das verschlüsselte Aktualisierungspaket von dem CDN 8 (B133). Der OTA-Master 4 entschlüsselt das verschlüsselte Aktualisierungspaket, das von dem CDN 8 heruntergeladen wurde, mit dem AES-Schlüssel und der Nonce (B134). Der OTA-Master 4 überträgt das entschlüsselte Aktualisierungspaket an die Ziel-ECU 5 und installiert das Aktualisierungspaket in der Ziel-ECU 5 (B135).

[0171] Wie es oben beschrieben ist, können gemäß der dreizehnten Ausführungsform die folgenden vorteilhaften Wirkungen erzielt werden.

[0172] Die Nonce ist in einer Kampagnenmeldung, die als erstes zwischen dem OTA-Zentrum 2 und dem OTA-Master 4 zu kommunizieren ist, enthalten, und die Nonce ist in einem Zählerwert enthalten. Als Ergebnis ist es möglich, den CTR-Modus durch Einschließen der Nonce in dem Zählerwert sicherer zu machen.

Vierzehnte Ausführungsform

[0173] Die vierzehnte Ausführungsform wird mit Bezug auf die **Fig. 125** bis 132 beschrieben. In der vierzehnten Ausführungsform wird anstelle eines gemeinsamen Schlüssels für alle Fahrzeuge als einen Schlüssel, der zur Verschlüsselung verwendet wird, um einen Einflussbereich zu der Zeit einer Schlüsselgefährdung einzugrenzen, ein hergeleiteter Schlüssel, der für jede Einheit einer speziellen Fahrzeuggruppe individualisiert ist, verwendet, wodurch ein Verlust zu der Zeit eines Leckens eines Schlüssels lokalisiert wird, während eine Verteilungs-Cache-Effizienz des CDN 8 aufrechterhalten wird, und es wird eine OTA-Verteilung sicherer durchgeführt. Wie es in **Fig. 126** dargestellt ist, wird die VIN-Nummer in mehrere Abschnitte für dasselbe Fahrzeugmodell und das Herstellungsjahr unterteilt, und es werden unterschiedliche individuelle AES-Schlüssel für die jeweiligen Abschnitte verwendet. Die Nummer wird beispielsweise in VIN-Nummern AAA bis CCC, VIN-Nummern DDD bis KKK und VIN-Nummern SSS bis ZZZ unterteilt, und es werden unterschiedliche individuelle AES-Schlüssel verwendet. Die Individualschlüsseldatenbank enthält beispielsweise einen OEM-Code, ein Fahrzeugmodell, ein Herstellungsjahr, einen AES-Masterschlüssel, einen Keimwert und einen individuellen AES-Schlüssel, separiert durch VIN-Nummern.

[0174] Im Folgenden wird der Betrieb der oben beschriebenen Konfiguration mit Bezug auf die **Fig. 127** bis 132 beschrieben.

(14-1) Prozess des OTA-Zentrums 2 (siehe Figuren 127 bis 129)

[0175] Das OTA-Zentrum 2 erzeugt einen individuellen AES-Schlüssel zum Verschlüsseln des Aktualisierungspaketes aus einem AES-Masterschlüssel und einem Keimwert (A141). Der Keimwert ist beispielsweise eine Zufallszahl, ein Zählerwert, ein Zeitstempel oder Ähnliches. Das OTA-Zentrum 2 verschlüsselt das Aktualisierungspaket mit einem der erzeugten individuellen AES-Schlüssel und der Nonce in dem CTR-Modus (A142). Das OTA-Zentrum 2 verschlüsselt den individuellen AES-Schlüssel mit dem öffentlichen RSA-Schlüssel (A142). Das

OTA-Zentrum 2 speichert den individuellen AES-Schlüssel und die Nonce, die mit dem öffentlichen RSA-Schlüssel verschlüsselt sind, in der Kampagnenmeldung (A144). Das OTA-Zentrum 2 platziert ein Aktualisierungspaket, das mit einem der individuellen AES-Schlüssel und der Nonce verschlüsselt ist, in dem CDN 8 (A145). Das OTA-Zentrum 2 überträgt eine Kampagnenmeldung, in der der verschlüsselte individuelle AES-Schlüssel und die Nonce gespeichert sind, an das neu zu programmierende fahrzeugseitige System 3 (A146).

(14-2) Prozess des OTA-Masters 4 (siehe Figuren 130 bis 132)

[0176] Wenn die Kampagnenmeldung beschafft wird, da die Kampagnenmeldung, die von dem OTA-Zentrum 2 übertragen wird, durch den OTA-Master 4 empfangen wird, beschafft der OTA-Master 4 den individuellen AES-Schlüssel und die Nonce aus der beschafften Kampagnenmeldung (B 141). Der OTA-Master 4 entschlüsselt den verschlüsselten individuellen AES-Schlüssel mit dem geheimen RSA-Schlüssel, um einen individuellen AES-Schlüssel zu extrahieren (B142). Der OTA-Master 4 lädt und beschafft das verschlüsselte Aktualisierungspaket von dem CDN 8 (B143). Der OTA-Master 4 entschlüsselt das verschlüsselte Aktualisierungspaket, das von dem CDN 8 heruntergeladen wurde, mit dem individuellen AES-Schlüssel und der Nonce (B144). Der OTA-Master 4 überträgt das entschlüsselte Aktualisierungspaket an die Ziel-ECU 5 und installiert das Aktualisierungspaket in der Ziel-ECU 5 (B145).

[0177] Wie es oben beschrieben ist, können gemäß der vierzehnten Ausführungsform die folgenden vorteilhaften Wirkungen erzielt werden.

[0178] Anstelle der Verwendung eines Schlüssels, der sämtlichen Fahrzeugen gemeinsam ist, für einen Schlüssel, der zur Verschlüsselung verwendet wird, wird ein hergeleiteter Schlüssel, der für jede Einheit einer speziellen Fahrzeuggruppe individualisiert ist, verwendet. Es ist möglich, einen Verlust zu der Zeit eines Leckens bzw. Durchsickerns eines Schlüssels zu lokalisieren, während eine Verteilungs-Cache-Effizienz des CDN 8 aufrechterhalten wird. Als Ergebnis kann die Sicherheit, wenn der OTA-Master 4 das Aktualisierungspaket von dem OTA-Zentrum 2 herunterlädt, verbessert werden, und es kann eine sicherere OTA-Verteilung realisiert werden.

Fünfzehnte Ausführungsform

[0179] Die fünfzehnte Ausführungsform wird mit Bezug auf die **Fig.** 133 bis 137 beschrieben. In der fünfzehnten Ausführungsform wird in Vorbereitung für einen Fall eines Leckens bzw. Durchsickerns

eines geheimen Schlüssels, der der schlechteste Fall ist, eine Schlüsselversion derart zugewiesen, dass der Schlüssel durch OTA aktualisiert und von dem OTA-Zentrum 2 verwaltet werden kann, und es wird ein Schlüsselaktualisierungsschlüssel in dem HSM-Bereich des OTA-Masters gespeichert. Das OTA-Zentrum 2 verwaltet Versionsinformationen über einen öffentlichen RSA-Schlüssel, der zur Verschlüsselung eines AES-Schlüssels verwendet wird, und eines geheimen RSA-Schlüssels, der zu der Entschlüsselung verwendet wird. Die Versionsinformationen werden derart verwaltet, dass sie nicht downgradet werden, wenn der geheime RSA-Schlüssel und der öffentliche RSA-Schlüssel aktualisiert werden. Das OTA-Zentrum 2 und der OTA-Master 4 enthalten jeweils einen Schlüsselaktualisierungsschlüssel, der zum Aktualisieren des geheimen Schlüssels verwendet wird. In dem OTA-Zentrum 2 wird ein neues geheimes Schlüsselpaar zu der Zeit eines Leckens bzw. Durchsickerns eines geheimen Schlüssels oder in regelmäßigen Intervallen erzeugt, es wird ein Schlüsselaktualisierungspaket unter Verwendung des Schlüsselaktualisierungsschlüssels erzeugt, und das Schlüsselaktualisierungspaket wird an den OTA-Master 4 übertragen, wodurch eine Schlüsselaktualisierung des geheimen Schlüssels implementiert wird.

[0180] Im Folgenden wird der Betrieb der oben beschriebenen Konfiguration mit Bezug auf die **Fig.** 134 bis 137 beschrieben.

(15-1) Prozess des OTA-Zentrums 2 (siehe Figuren 134 bis 135)

[0181] Das OTA-Zentrum 2 erzeugt ein neues Schlüsselpaar aus einem neuen geheimen RSA-Schlüssel und einem neuen öffentlichen RSA-Schlüssel (A151). Das OTA-Zentrum 2 verschlüsselt den erzeugten neuen geheimen RSA-Schlüssel und führt einen MAC-Betrieb desselben mit dem Schlüsselaktualisierungsschlüssel in dem CTR-Modus durch und erzeugt ein Schlüsselaktualisierungspaket (A152). Das OTA-Zentrum 2 wechselt von dem alten öffentlichen RSA-Schlüssel zu dem neuen öffentlichen RSA-Schlüssel (A153). Das OTA-Zentrum 2 überträgt das Schlüsselaktualisierungspaket an das neu zu programmierende fahrzeugseitige System 3 (A154).

(15-2) Prozess des OTA-Masters 4 (siehe Figuren 136 bis 137)

[0182] Der OTA-Master 4 beschafft das Schlüsselaktualisierungspaket und entschlüsselt und MAC-verifiziert den neuen geheimen RSA-Schlüssel mit dem Schlüsselaktualisierungsschlüssel in dem CTR-Modus (B151). Der OTA-Master 4 wechselt den alten geheimen RSA-Schlüssel in den ent-

schlüsselten neuen geheimen RSA-Schlüssel (B152).

[0183] Wie es oben beschrieben ist, können gemäß der fünfzehnten Ausführungsform die folgenden vorteilhaften Wirkungen erzielt werden.

[0184] Es wird ein neues geheimes Schlüsselpaar zu der Zeit eines Leckens eines geheimen Schlüssels oder in regelmäßigen Intervallen erzeugt, das Schlüsselaktualisierungspaket wird unter Verwendung des Schlüsselaktualisierungsschlüssels erzeugt, und das Schlüsselaktualisierungspaket wird an den OTA-Master 4 übertragen. Als Ergebnis kann durch Schlüsselaktualisierung des geheimen Schlüssels die Sicherheit, wenn der OTA-Master 4 das Aktualisierungspaket von dem OTA-Zentrum 2 herunterlädt, erhöht werden, und es kann eine sichere OTA-Verteilung realisiert werden.

Sechzehnte Ausführungsform

[0185] Die sechzehnte Ausführungsform wird mit Bezug auf die **Fig. 138 bis 145** beschrieben. In der sechzehnten Ausführungsform wird in einem Schlüsselaustausch durch ECDHE ein Schlüsselaustausch zwischen dem OTA-Zentrum 2 und dem OTA-Master 4 auf sichere Weise für einen Schlüssel realisiert, dem eine digitale Signatur zugewiesen ist und der für ein Verschlüsselungspaket verwendbar ist, um dem Angriff von einem Zwischenangreifer zu widerstehen. Wie es in den **Fig. 139 bis 140** dargestellt ist, ist der DHE in Bezug auf einen Angriff von einem Zwischenangreifer verletzbar, widersteht aber dem Angriff von einem Zwischenangreifer durch Zuweisen einer digitalen Signatur. Als digitale Signatur wird eine digitale Signatur verwendet, die einen Verschlüsselungsalgorithmus von RSA verwendet, oder es wird ein DSA mit elliptischer Kurve verwendet.

[0186] Im Folgenden wird der Betrieb der oben beschriebenen Konfiguration mit Bezug auf die **Fig. 141 bis 145** beschrieben.

(16-1) Prozess des OTA-Zentrums 2 (siehe Figuren 141 bis 143)

[0187] Das OTA-Zentrum 2 erzeugt ein Schlüsselpaar des ECDHE aus einer Zufallszahl, die für jedes Fahrzeugmodell oder jede Fahrzeuggruppe erzeugt wird (A161). Das OTA-Zentrum 2 weist dem ECDHE-Schlüssel unter Verwendung des geheimen RSA-Schlüssels eine digitale Signatur zu (A162). Hier wird der geheime RSA-Schlüssel verwendet, aber die vorliegende Erfindung ist nicht auf den geheimen RSA-Schlüssel beschränkt, und es ist anderes möglich, solange wie es sich um ein Öffentlicher-Schlüssel-Verschlüsselungsverfahren handelt, und es kann beispielsweise ein digitaler Signaturalgorithmus mit elliptischer Kurve (ECDSA) für

einen geheimen Schlüssel verwendet werden. Das OTA-Zentrum 2 überträgt den öffentlichen ECDHE-Schlüssel, dem die digitale Signatur zugewiesen ist, an das neu zu programmierende fahrzeugseitige System 3 (A163). Das OTA-Zentrum 2 tauscht einen geheimen Schlüssel mit dem OTA-Master 4 in dem ECDHE-Algorithmus aus (A164). Das OTA-Zentrum 2 erzeugt einen AES-Schlüssel zur Verschlüsselung des Aktualisierungspaketes (A165). Das OTA-Zentrum 2 verschlüsselt das Aktualisierungspaket mit dem erzeugten AES-Schlüssel in dem CTR-Modus (A166). Das OTA-Zentrum 2 platziert das Aktualisierungspaket, das mit dem AES-Schlüssel verschlüsselt ist, in dem CDN 8 (A167). Das OTA-Zentrum 2 überträgt eine Kampagnenmeldung, in der der verschlüsselte AES-Schlüssel gespeichert ist, an das neu zu programmierende fahrzeugseitige System 3 (A168).

(16-2) Prozess des OTA-Masters 4 (siehe Figuren 144 bis 145)

[0188] Der OTA-Master 4 erzeugt ein Schlüsselpaar des ECDHE aus einer Zufallszahl, die entsprechend einer speziellen Regel erzeugt wird (B161). Der OTA-Master 4 signiert den öffentlichen ECDHE-Schlüssel, der von dem OTA-Zentrum 2 empfangen wird, digital mit dem öffentlichen RSA-Schlüssel und verifiziert diesen (B162). Hier besteht wie in dem OTA-Zentrum 2 keine Beschränkung auf den öffentlichen RSA-Schlüssel, und es ist anderes möglich, solange es sich um ein Öffentlicher-Schlüssel-Verschlüsselungsverfahren handelt, und es kann beispielsweise ein öffentlicher ECDSA-Schlüssel verwendet werden. Wenn das Verifizierungsergebnis positiv ist, tauscht der OTA-Master 4 den geheimen Schlüssel mit dem OTA-Zentrum 2 in dem ECDHE-Algorithmus aus (B163). Danach führt der OTA-Master 4 den Prozess in und nach Schritt B113, der in der elften Ausführungsform beschrieben wurde, durch.

[0189] Wie es oben beschrieben wurde, können gemäß der sechzehnten Ausführungsform die folgenden vorteilhaften Wirkungen erzielt werden.

[0190] Es wird eine digitale Signatur in dem Schlüsselaustausch durch ECDHE zugewiesen. Als Ergebnis ist es durch Zuweisen einer digitalen Signatur möglich, einem Angriff von einem Zwischenangreifer zu widerstehen, und es ist möglich, eine sichere OTA-Verteilung zu gewährleisten.

Modifikation der sechzehnten Ausführungsform

[0191] Eine Modifikation der sechzehnten Ausführungsform wird mit Bezug auf die **Fig. 182 bis 189** beschrieben. Auch in der Modifikation der sechzehnten Ausführungsform wird wie in den Modifikationen der elften Ausführungsform und der zwölften Ausführungsform eine Situation beschrieben, in der der

OTA-Master 4 Daten mit dem OTA-Zentrum 2 oder dem CDN 8 nicht über eine Drahtloskommunikationsleitung austauscht, sondern stattdessen eine Programmaktualisierung unter Verwendung eines Speichermediums wie beispielsweise einer SD-Karte ausführt. Der Hauptunterschied zwischen der Modifikation der sechzehnten Ausführungsform und der Modifikation der zwölften Ausführungsform besteht darin, dass ein Angriff von einem Zwischenangreifer durch Anwenden einer digitalen Signatur für einen öffentlichen ECDHE-Schlüssel eines OTA-Zentrums 2 mit einem Schlüssel eines Öffentlicher-Schlüssel-Verschlüsselungsverfahrens widerstanden wird.

[0192] Die Fig. 182 bis 185 stellen eine Übertragung von Daten von dem OTA-Master 4 an die SD-Karte 11, ein Heraufladen von Daten von dem PC, mit dem die SD-Karte 11 verbunden ist, an das OTA-Zentrum 2, ein Herunterladen von Daten von dem OTA-Zentrum 2 auf die SD-Karte 11 und eine Übertragung von Daten von der SD-Karte 11 an den OTA-Master 4 dar. Der Hauptunterschied zu der Modifikation der zwölften Ausführungsform besteht darin, dass, wie es in Fig. 184 dargestellt ist, das OTA-Zentrum 2 eine digitale Signatur einem Schlüssel, der mit dem OTA-Master 4 auszutauschen ist (der öffentliche ECDHE-Schlüssel des OTA-Zentrums 2), mit einem Schlüssel eines Öffentlicher-Schlüssel-Verschlüsselungsverfahrens, beispielsweise einem geheimen RSA-Schlüssel oder einem geheimen ECDSA-Schlüssel, zuweist. Das OTA-Zentrum 2 überträgt den signierten öffentlichen ECDHE-Schlüssel an die SD-Karte 11 und speichert den signierten öffentlichen ECDHE-Schlüssel darin. Wie es in Fig. 185 dargestellt ist, liest der OTA-Master 4 den signierten öffentlichen ECDHE-Schlüssel aus der SD-Karte 11 aus und verifiziert den öffentlichen ECDHE-Schlüssel unter Verwendung des öffentlichen RSA-Schlüssels, der in dem fahrzeugseitigen System 3 gespeichert ist.

[0193] Im Folgenden wird der Betrieb der oben beschriebenen Konfiguration mit Bezug auf die Fig. 186 bis 189 beschrieben.

(16-3) Prozess des OTA-Masters 4 (siehe Figur 186)

[0194] Wenn die SD-Karte 11 mit dem fahrzeugseitigen System 3 verbunden und eine vorbestimmte Bedingung erfüllt ist, fordert der OTA-Master 4 die Ziel-ECU 5 auf, Konfigurationsinformationen wie beispielsweise Softwareversionsinformationen zu übertragen, und beschafft die Konfigurationsinformationen wie beispielsweise die Softwareversionsinformationen, die von der Ziel-ECU 5 übertragen werden, als Konfigurationsinformationen (B1611). Auf ein Beschaffen der Konfigurationsinformationen hin überträgt der OTA-Master 4 die beschafften Fahrzeugkonfigurationsinformatio-

nen an die SD-Karte 11 und speichert die Konfigurationsinformationen darin (B 1612). Der OTA-Master 4 erzeugt ein Schlüsselpaar des ECDHE aus einer Zufallszahl, die entsprechend einer speziellen Regel erzeugt wird (B1613). In diesem Fall enthält das Schlüsselpaar den öffentlichen ECDHE-Schlüssel und den geheimen ECDHE-Schlüssel des OTA-Masters 4. Der OTA-Master 4 überträgt den öffentlichen ECDHE-Schlüssel des OTA-Masters 4 an die SD-Karte 11 und speichert den öffentlichen ECDHE-Schlüssel (B1614). Das Schlüsselpaar des ECDHE ist eine Zufallszahl, die entsprechend einer speziellen Regel wie in der zwölften Ausführungsform erzeugt wird, und ist jedem Fahrzeugmodell gemeinsam. Wenn die Fahrzeugkonfigurationsinformationen und der öffentliche ECDHE-Schlüssel des OTA-Masters 4 auf diese Weise gespeichert sind, wird die SD-Karte 11 von dem fahrzeugseitigen System 3 getrennt und mit dem PC verbunden.

(16-4) Prozess des PC (siehe Figur 187)

[0195] Wenn die SD-Karte 11 verbunden ist, liest der PC die Fahrzeugkonfigurationsinformationen und den öffentlichen ECDHE-Schlüssel des OTA-Masters 4, die in der SD-Karte 11 gespeichert sind, aus und lädt die Fahrzeugkonfigurationsinformationen und den öffentlichen ECDHE-Schlüssel des OTA-Masters 4, die ausgelesen wurden, zu dem OTA-Zentrum 2 hoch (C1611). Der PC wartet auf einen Empfang einer Kampagnenmeldung, in der der öffentliche ECDHE-Schlüssel des OTA-Masters 4 gespeichert ist, und des verschlüsselten Aktualisierungspaketes von dem OTA-Zentrum 2, oder wartet auf einen Empfang einer Meldung ohne Kampagne (C1612, C1613). Wenn bestimmt wird, dass eine Kampagnenmeldung, in der der öffentliche ECDHE-Schlüssel des OTA-Masters 4 gespeichert ist, und ein verschlüsseltes Aktualisierungspaket von dem OTA-Zentrum 2 empfangen wurden (C1612: ja), oder wenn bestimmt wird, dass eine Meldung ohne Kampagne empfangen wurde (C1613: ja), beendet der PC den Prozess.

(16-5) Prozess des OTA-Zentrums 2 (siehe Figur 188)

[0196] Das OTA-Zentrum 2 beschafft die Fahrzeugkonfigurationsinformationen und den öffentlichen ECDHE-Schlüssel des OTA-Masters 4, die von dem PC heraufgeladen wurden, mit dem die SD-Karte 11 verbunden ist (A1611). Das OTA-Zentrum 2 bestimmt auf der Grundlage der Fahrzeugkonfigurationsinformationen, ob es eine Kampagne gibt (A1612). Wenn bestimmt wird, dass es keine Kampagne gibt (A1612: nein), überträgt das OTA-Zentrum 2 eine Meldung ohne Kampagne an den PC (A1613) und beendet den Prozess.

[0197] Wenn bestimmt wird, dass es eine Kampagne gibt (A1612: ja), erzeugt das OTA-Zentrum 2 ein Schlüsselpaar des ECDHE aus einer Zufallszahl, die jedem Fahrzeugmodell oder jeder Fahrzeuggruppe gemeinsam ist (A1614). In diesem Fall ist das Schlüsselpaar der öffentliche ECDHE-Schlüssel und der geheime ECDHA-Schlüssel des OTA-Zentrums 2. Das OTA-Zentrum 2 signiert den öffentlichen ECDHA-Schlüssel des OTA-Zentrums 2 mit dem geheimen RSA-Schlüssel (A1615) und lädt den signierten öffentlichen ECDHE-Schlüssel des OTA-Zentrums 2 auf die SD-Karte 11 herunter und speichert den signierten öffentlichen ECDHE-Schlüssel dort (A1616). Das OTA-Zentrum 2 erzeugt einen gemeinsamen ECDHA-Schlüssel (geheimer Schlüssel) aus dem geheimen ECDHE-Schlüssel des OTA-Zentrums 2 und dem öffentlichen ECDHA-Schlüssel des OTA-Masters 4 (A1617) und verschlüsselt das Aktualisierungspaket mit dem erzeugten gemeinsamen ECDHE-Schlüssel (geheimer Schlüssel) (A1618). Das OTA-Zentrum 2 lädt das verschlüsselte Aktualisierungspaket auf die SD-Karte 11 herunter und speichert das verschlüsselte Aktualisierungspaket darin (A1619).

(16-6) Prozess des OTA-Masters 4 (siehe Figur 189)

[0198] Wenn die SD-Karte 11 mit dem fahrzeugseitigen System 3 verbunden ist, beschafft der OTA-Master 4 den signierten öffentlichen ECDHE-Schlüssel des OTA-Zentrums 2 und das Aktualisierungspaket von der SD-Karte 11 (B1621). Der OTA-Master 4 verifiziert den signierten öffentlichen ECDHE-Schlüssel des OTA-Zentrums 2 mit dem öffentlichen RSA-Schlüssel (B1622). Der OTA-Master 4 bestimmt, ob das Verifizierungsergebnis normal ist (B1623), und wenn bestimmt wird, dass das Verifizierungsergebnis nicht normal ist, d.h., wenn es abnorm ist (B1623: nein), gibt der OTA-Master 4 eine Fehlermeldung aus (B1624).

[0199] Wenn bestimmt wird, dass das Verifizierungsergebnis normal ist (B1623: ja), erzeugt der OTA-Master 4 einen gemeinsamen ECDHE-Schlüssel (geheimer Schlüssel) aus dem geheimen ECDHE-Schlüssel des OTA-Masters 4 und dem öffentlichen ECDHA-Schlüssel des OTA-Zentrum 2 (B1625). Der OTA-Master 4 führt einen AES-Blockverschlüsselungsprozess des Zählerwertes mit dem AES-Schlüssel aus, um den Zählerwert zu verschlüsseln (B1626). Der OTA-Master 4 führt einen XOR-Betrieb durch und entschlüsselt den verschlüsselten Zählerwert und das verschlüsselte Aktualisierungspaket (B1627). Der OTA-Master 4 überträgt das entschlüsselte Aktualisierungspaket an die Ziel-ECU 5 und installiert das Aktualisierungspaket in der Ziel-ECU 5 (B1628).

[0200] Gemäß einer derartigen Konfiguration ist es möglich, einem Angriff von einem Zwischenangreifer

zu widerstehen, ohne von einer Drahtloskommunikationsfunktion des fahrzeugseitigen Systems 3 abzuhängen, und es ist möglich, eine sichere OTA-Verteilung zu realisieren. Durch Verringern der Anzahl von Datenübertragungen zwischen dem OTA-Master 4 und der SD-Karte 11 und des Heraufladens und Herunterladens zwischen dem OTA-Zentrum 2 und der SD-Karte 11 kann der Nutzerkomfort verbessert werden.

Siebzehnte Ausführungsform

[0201] Die siebzehnte Ausführungsform wird mit Bezug auf die **Fig. 146** bis 151 beschrieben. Während die zehnte Ausführungsform ausgelegt ist, einen CDN-Verkäufer mit den niedrigsten Verteilungskosten aus mehreren CDN-Verkäufern für jeden Bereich auszuwählen, ist die siebzehnte Ausführungsform ausgelegt, einen CDN-Verkäufer, der die Verteilungskosten verringern kann, statistisch aus mehreren CDN-Verkäufern auszuwählen. Während in der zehnten Ausführungsform das Aktualisierungspaket in dem OTA-Zentrum 2 verschlüsselt wird, und dann die Verteilungskosten entsprechend dem Verteilungsverfahren, dem OTA-Zielbereich und der Verteilungsdatengröße minimiert werden, wird in der siebzehnten Ausführungsform das Aktualisierungspaket nicht in dem OTA-Zentrum 2 verschlüsselt, und es wird eine Kommunikation zwischen dem CDN 8 und dem OTA-Master 4 durch eine TLS-Kommunikation geschützt, und dann werden die Verteilungskosten entsprechend dem Verteilungsverfahren, dem OTA-Zielbereich und der Verteilungsdatengröße minimiert.

[0202] Im Folgenden wird der Betrieb der oben beschriebenen Konfiguration mit Bezug auf die **Fig. 147** bis 151 beschrieben.

(17-1) Prozess des OTA-Zentrums 2 (siehe Figuren 147 bis 148)

[0203] Das OTA-Zentrum 2 identifiziert ein Verteilungsverfahren (A171), identifiziert einen OTA-Zielbereich (A172), identifiziert, ob TLS in einem Kommunikationsprotokoll für das Fahrzeug verwendet wird (A173), identifiziert eine Verteilungsdatengröße (A174) und nimmt Bezug auf die Preistabelle in der CDN-Verkäuferverwaltungsdatenbank mit dem Verteilungsverfahren, dem OTA-Zielbereich, dem Kommunikationsprotokoll und der Verteilungsdatengröße als Schlüssel (A175). In diesem Fall kann das OTA-Zentrum 2 Bezug auf die Preistabelle unter Verwendung mindestens eines der folgenden als Schlüssel nehmen: Verteilungsverfahren, OTA-Zielbereich, Kommunikationsprotokoll und Verteilungsdatengröße. Das OTA-Zentrum 2 wählt einen CDN-Verkäufer mit den geringsten Verteilungskosten für jeden Bereich aus und platziert ein Aktualisierungspaket in dem ausgewählten CDN 8 (A176). Das OTA-

Zentrum 2 überträgt eine Kampagnenmeldung an das neu zu programmierende fahrzeugseitige System 3 (A177).

(17-2) Prozess des OTA-Masters 4 (siehe Figuren 149 bis 151)

[0204] Der OTA-Master 4 beschafft die Kampagnenmeldung, wenn die Kampagnenmeldung, die von dem OTA-Zentrum 2 übertragen wird, durch den OTA-Master empfangen wird (B171). Der OTA-Master 4 errichtet eine TLS-Kommunikation mit dem CDN-Verkäufer, der in der Kampagnenmeldung gelistet ist, um das Aktualisierungspaket zu beschaffen (B172). Solange wie die URI-Informationen in der Kampagnenmeldung beschrieben sind, müssen die CDN-Verkäuferinformationen nicht beschrieben sein. Nach Errichtung der TLS-Kommunikation tauscht der OTA-Master 4 einen gemeinsamen Schlüssel von AES in dem TLS-Kommunikationsprotokoll aus. Es wird eine Verhandlung durchgeführt, um den AES-CTR-Modus als den Verschlüsselungsmodus auszuwählen. Der OTA-Master 4 lädt und beschafft das Aktualisierungspaket, das mit dem gemeinsamen AES-Schlüssel von TLS verschlüsselt ist, von dem CDN 8 auf der Grundlage der URI-Informationen (B173, entspricht einem Aktualisierungsdatenbeschaffungsschritt).

[0205] Zu dieser Zeit führt der OTA-Master 4 parallel zu einem Herunterladen und Beschaffen des verschlüsselten Aktualisierungspaketes von dem CDN 8 einen AES-Blockverschlüsselungsprozess des Zählerwertes mit dem AES-Schlüssel aus, um den Zählerwert zu verschlüsseln (B 174). Der OTA-Master 4 führt einen XOR-Betrieb durch und entschlüsselt den verschlüsselten Zählerwert und das verschlüsselte Aktualisierungspaket, das von dem CDN 8 heruntergeladen wurde (B175). Der OTA-Master 4 überträgt das entschlüsselte Aktualisierungspaket an die Ziel-ECU 5 und installiert das Aktualisierungspaket in der Ziel-ECU 5 (B176).

[0206] Wie es oben beschrieben ist, können gemäß der siebzehnten Ausführungsform die folgenden vorteilhaften Wirkungen erzielt werden.

[0207] Das Aktualisierungspaket wird nicht durch das OTA-Zentrum 2 verschlüsselt, eine Kommunikation zwischen dem CDN 8 und dem OTA-Master 4 wird durch eine TLS-Kommunikation geschützt, und es werden die Verteilungskosten entsprechend dem Verteilungsverfahren, dem OTA-Zielbereich, dem Kommunikationsprotokoll und der Verteilungsdaten-größe minimiert. Als Ergebnis ist es möglich, die Verteilungskosten geeignet zu verringern, wenn der OTA-Master 4 das Aktualisierungspaket von dem OTA-Zentrum 2 herunterlädt.

Achtzehnte Ausführungsform

[0208] Die achtzehnte Ausführungsform wird mit Bezug auf die **Fig. 152** bis **165** beschrieben. In der achtzehnten Ausführungsform wird der optimale CDN-Verkäufer unter Berücksichtigung nicht nur der Verteilungskosten, sondern auch des Durchsatzes und der Antwortverzögerungszeit des CDN-Verkäufers ausgewählt, die Preistabelle und die Qualitätseigenschaft des CDN-Verkäufers werden periodisch überprüft, die CDN-Verkäuferverwaltungsdatenbank wird konstant auf dem letzten bzw. jüngsten Zustand gehalten, und der CDN-Verkäufer mit dem konstant besten Wettbewerbsvorteil auf dem Markt wird ausgewählt. Die Preistabelle ist in den **Fig. 153** bis **160** dargestellt, und die Qualitätsinformationen über jeden Cloud-Dienst-Geschäftsbetreiber sind in **Fig. 161** dargestellt. Wie es in **Fig. 162** dargestellt ist, ist, wenn ein CDN-Verkäufer A mit einem CDN-Verkäufer B verglichen wird, der CDN-Verkäufer B dem CDN-Verkäufer A hinsichtlich der Verteilungskosten überlegen, aber der CDN-Verkäufer A ist dem CDN-Verkäufer B hinsichtlich einer Gewichtung des Durchsatzes und einer Gewichtung der Antwortverzögerungszeit überlegen. Unter Berücksichtigung nicht nur der Verteilungskosten, sondern auch des Durchsatzes, der Antwortverzögerungszeit und Ähnlichem des CDN-Verkäufers ist es möglich, den Schluss zu ziehen, dass unter Berücksichtigung des Durchsatzes, der Antwortverzögerungszeit und Ähnlichem des CDN-Verkäufers der CDN-Verkäufer A eher als der CDN-Verkäufer B, der nur hinsichtlich der Verteilungskosten überlegen ist, ausgewählt werden sollte.

[0209] Im Folgenden wird der Betrieb der oben beschriebenen Konfiguration mit Bezug auf die **Fig. 163** bis **165** beschrieben.

(18-1) Prozess des OTA-Zentrums 2 (siehe Figuren 163 bis 165)

[0210] Das OTA-Zentrum 2 identifiziert das Verteilungsverfahren (A1 81), identifiziert den OTA-Zielbereich (A182) und nimmt Bezug auf die Preistabelle in der CDN-Verkäuferverwaltungsdatenbank unter Verwendung des Verteilungsverfahrens und des OTA-Zielbereichs als Schlüssel (A183). In diesem Fall kann das OTA-Zentrum 2 Bezug auf die Preistabelle unter Verwendung des Verteilungsverfahrens und/oder des OTA-Zielbereichs als Schlüssel nehmen. Das OTA-Zentrum 2 identifiziert eine Qualitätseigenschaft jedes CDN-Verkäufers aus der CDN-Verkäuferverwaltungsdatenbank (A184). Das OTA-Zentrum 2 wählt einen optimalen CDN-Verkäufer für jeden Bereich aus der CDN-Verkäuferauswahllogik, die in der CDN-Verkäuferauswahllogikdatenbank registriert ist, auf der Grundlage der Verteilungskosten und der Qualitätseigenschaft des CDN-Verkäufers für jeden Bereich aus und platziert das Aktualisie-

rungspaket, das mit dem AES-Schlüssel verschlüsselt ist, in dem ausgewählten CDN 8 (A185). Das OTA-Zentrum 2 überträgt eine Kampagnenmeldung, in der der verschlüsselte AES-Schlüssel gespeichert ist, an das neu zu programmierende fahrzeugseitige System 3 (A186).

[0211] Das OTA-Zentrum 2 beschafft automatisch die Preistabelle der jeweiligen CDN-Verkäufer von den jeweiligen Webseiten und aktualisiert die CDN-Verkäuferverwaltungsdatenbank (A187). Das OTA-Zentrum 2 misst den Durchsatz und die Antwortverzögerungszeit jedes CDN-Verkäufers und aktualisiert die CDN-Verkäuferverwaltungsdatenbank (A188). Der Verteilungsserver 7 besucht beispielsweise regelmäßig die Webseite jedes CDN-Verkäufers und lädt die letzte bzw. jüngste Preistabelle herunter. Wenn der CDN-Verkäufer die Aktualisierungsinformationen über die Webseite liefert, lädt der Verteilungsserver 7 alternativ die letzte bzw. jüngste Preistabelle durch Registrierung der Aktualisierungsinformationen in dem Verteilungsdienst herunter.

(18-2) Prozess des OTA-Masters 4

[0212] Der Prozess des OTA-Masters 4 ist ähnlich wie der Prozess (Fig. 12 bis 14) des OTA-Masters 4, der in der ersten Ausführungsform beschrieben wurde.

[0213] Wie es oben beschrieben wurde, können gemäß der achtzehnten Ausführungsform die folgenden vorteilhaften Wirkungen erzielt werden.

[0214] Der optimale CDN-Verkäufer wird unter Berücksichtigung nicht nur der Verteilungskosten, sondern auch des Durchsatzes und der Antwortverzögerungszeit des CDN-Verkäufers ausgewählt, die Preistabelle und die Qualitätseigenschaft des CDN-Verkäufers werden periodisch überprüft, die CDN-Verkäuferverwaltungsdatenbank wird konstant auf dem jüngsten bzw. neuesten Zustand gehalten, und der CDN-Verkäufer mit dem konstant besten Wettbewerbsvorteil auf dem Markt wird ausgewählt. Als Ergebnis ist es möglich, die Verteilungskosten geeignet zu verringern, wenn der OTA-Master 4 das Aktualisierungspaket von dem OTA-Zentrum 2 herunterlädt.

[0215] Die Qualitätseigenschaft des CDN ist nicht auf den Durchsatz und die Antwortverzögerungszeit beschränkt, sondern es können eine Inhalt-Cache-Trefferrate, Problemaufzeichnungen der Vergangenheit und Ähnliches berücksichtigt werden, und diese können in der CDN-Verkäuferverwaltungsdatenbank enthalten sein. Außerdem ist es möglich, ein Hinzufügen oder Löschen eines CDN-Verkäufers, mit dem das OTA-Zentrum 2 verbunden ist, zu überprüfen

und mit einem CDN-Verkäufer, der auf dem Markt wettbewerbsfähig ist, eine Verbindung zu erstellen.

Neunzehnte Ausführungsform

[0216] Die neunzehnte Ausführungsform wird mit Bezug auf die Fig. 90 und 190 bis 193 beschrieben. Die oben beschriebene zehnte Ausführungsform weist eine Konfiguration auf, bei der ein CDN-Verkäufer mit den niedrigsten Verteilungskosten für einen jeweiligen Bereich aus mehreren CDN-Verkäufern ausgewählt wird. Anhand der neunzehnten Ausführungsform wird die Auswahl eines CDN-Verkäufers speziell beschrieben. In der neunzehnten Ausführungsform wird als ein Platzierungsziel des Aktualisierungspaketes in dem CDN 8 ein CDN-Verkäufer mit den niedrigsten Verteilungskosten dynamisch entsprechend einer Verteilungsdatengröße, einem OTA-Zielbereich (in einigen Fällen auch als Region bezeichnet) als einem Verteilungsbereich und einem Verteilungsverfahren unter mehreren CDN-Verkäufern ausgewählt. Die neunzehnte Ausführungsform wird Bezug auf die in Fig. 90 dargestellte Preistabelle beschrieben. Die Preistabelle kann eine andere Form als diejenige in Fig. 90 aufweisen.

[0217] Wie es in Fig. 190 dargestellt ist, enthält der Verteilungsserver 7 in dem OTA-Zentrum 2 einen CDN-Verkäuferauswahlabschnitt 7a, einen Datenspeicherabschnitt 7b, einen Kampagnenmeldungs-erzeugungsabschnitt 7c und einen CDN-Verteilungsabschnitt 7d zusätzlich zu einer CDN-Verkäuferverwaltungs-DB. Der CDN-Verkäuferauswahlabschnitt 7a wählt einen CDN-Verkäufer auf der Grundlage von Auswahlinformationen und Aktualisierungspaketinformationen, die Informationen sind, die zur Auswahl des CDN-Verkäufers benötigt werden, aus. Die Auswahlinformationen enthalten Informationen über eine Datengröße der Ziel-Kampagne, die Anzahl der Verteilungszielfahrzeuge der Ziel-Kampagne, eine Region, ein Verteilungsverfahren und Ähnliches. Zusätzliches zu einem Speichern der Kampagneninformationen speichert der Datenspeicherabschnitt 7b Identifizierungsinformationen, die den CDN-Verkäufer identifizieren können, der durch den CDN-Verkäuferauswahlabschnitt 7a ausgewählt wird. Die Identifizierungsinformationen enthalten beispielsweise einen Namen eines CDN-Verkäufers, eine Identifizierungsnummer zum Identifizieren des CDN-Verkäufers, eine URL, die den CDN-Verkäufer angibt, und Ähnliches. Der Kampagnenmeldungs-erzeugungsabschnitt 7c beschafft Informationen von dem Datenspeicherabschnitt 7b und erzeugt eine Kampagnenmeldung, die an das Fahrzeug oder Ähnliches zu verteilen ist.

[0218] Der CDN-Verteilungsabschnitt 7d enthält einen Speicherbereich, der einem jeweiligen CDN-Verkäufer entspricht. Der Speicherbereich enthält

beispielsweise einen Speicherbereich A, einen Speicherbereich B und einen Speicherbereich C. Jeder Speicherbereich des CDN-Verteilungsabschnittes 7d ist mit dem CDN-Server synchronisiert. D.h., wenn beispielsweise Daten von dem CDN-Server A an das fahrzeugseitige System 3 verteilt werden, platziert der CDN-Verteilungsabschnitt 7d die Daten in dem Speicherbereich A und überträgt die Daten an den CDN-Server A. Wenn die Daten von dem CDN-Verteilungsabschnitt 7d übertragen werden, verteilt der CDN-Server A die übertragenen Daten an das fahrzeugseitige System 3. Jeder Speicherbereich des CDN-Verteilungsabschnittes 7d kann auch als Ursprungsserver eines jeweiligen CDN-Servers bezeichnet werden.

[0219] Im Folgenden wird der Betrieb der oben beschriebenen Konfiguration mit Bezug auf die **Fig. 191 bis 193** beschrieben. Der Prozess zum Verschlüsseln und Ähnliches des Aktualisierungspaketes durch das OTA-Zentrum 2 ist ähnlich wie derjenige in der zehnten Ausführungsform oder anderen Ausführungsformen. Außerdem ist der Prozess des OTA-Masters 4 ähnlich wie derjenige der ersten Ausführungsform oder einer anderen Ausführungsform. In der neunzehnten Ausführungsform wird hauptsächlich die Auswahl eines CDN-Verkäufers beschrieben.

(19-1) Verarbeitung des
Kampagnenmeldungserzeugungsabschnittes 7c
(siehe Figur 191)

[0220] Wenn eine Kampagne auftritt, beschafft der Kampagnenmeldungserzeugungsabschnitt 7c Informationen von der Außenseite wie beispielsweise einem OEM-Server (A191). Die Kampagneninformationen enthalten Informationen über die Datengröße der Ziel-Kampagne, die Anzahl der Verteilungsziel-fahrzeuge der Ziel-Kampagne, die Region und das Verteilungsverfahren. Der Kampagnenmeldungserzeugungsabschnitt 7c speichert die beschafften Kampagneninformationen in dem Datenspeicherabschnitt 7b (A192). Das Speichern der Kampagneninformationen kann auch als Platzieren der Kampagneninformationen bezeichnet werden.

[0221] Der Kampagnenmeldungserzeugungsabschnitt 7c benachrichtigt den CDN-Verkäuferauswahlabschnitt 7a hinsichtlich einer Anfrage zum Auswählen des CDN-Verkäufers (A193) und wartet auf eine Beschaffung der Auswahlmeldung von dem CDN-Verkäuferauswahlabschnitt 7a. Wenn die Auswahlmeldung von dem CDN-Verkäuferauswahlabschnitt 7a beschafft wird (A194), greift der Kampagnenmeldungserzeugungsabschnitt 7c auf den Datenspeicherabschnitt 7b zu und beschafft die Identifizierungsinformationen hinsichtlich des CDN-Verkäufers, der durch den CDN-Verkäuferauswahlabschnitt 7a ausgewählt wird (A195).

[0222] Auf der Grundlage der Identifizierungsinformationen hinsichtlich des CDN-Verkäufers erzeugt der Kampagnenmeldungserzeugungsabschnitt 7c eine Parameterdatei, die die URL des ausgewählten CDN enthält, als eine Kampagnenmeldung (A196). Der Kampagnenmeldungserzeugungsabschnitt 7c verteilt die erzeugte Kampagnenmeldung an das fahrzeugseitige System 3 (A197).

(19-2) Prozess des CDN-
Verkäuferauswahlabschnittes 7a (siehe Figuren 192
bis 193)

[0223] Wenn der CDN-Verkäuferauswahlabschnitt 7a eine Anfrage zum Auswählen des CDN-Verkäufers, die von dem Kampagnenmeldungserzeugungsabschnitt 7 gemeldet wird, beschafft hat (A191 1), greift der CDN-Verkäuferauswahlabschnitt 7a auf den Datenspeicherabschnitt 7b zu und beschafft die Auswahlinformationen (A1912), und dann schreitet der Prozess zu einem ersten CDN-Auswahlprozess (A1913).

[0224] Wenn der erste CDN-Auswahlprozess gestartet wird, berechnet der CDN-Verkäuferauswahlabschnitt 7a eine Verteilungsdatengröße, die eine Datengröße angibt, die von dem CDN-Server an das zu aktualisierende Fahrzeug zu verteilen ist (A1921). Insbesondere multipliziert der CDN-Auswahlabschnitt 7a die Datengröße der Ziel-Kampagne mit der Anzahl der Verteilungszielfahrzeuge der Ziel-Kampagne und berechnet die Größe der Verteilungsdaten, deren Verteilung von dem CDN-Server geplant wird.

[0225] Der CDN-Verkäuferauswahlabschnitt 7a wiederholt den anschließenden Prozess für jeden CDN-Verkäufer (A1922 bis 1929). Der CDN-Verkäuferauswahlabschnitt 7a beschafft Gebühreninformationen aus der CDN-Verkäuferverwaltungs-DB auf der Grundlage der Verteilungsdatengröße, die oben berechnet wurde, und der Bereichsinformationen bzw. Regioneninformationen betreffend die Region (A1923). In dem Fall einer Kampagne von 30 TB für Nordamerika beschafft der CDN-Verkäuferauswahlabschnitt 7a beispielsweise Gebühreninformationen etwa für „bis 10 TB“ und „bis 40 TB“ in der Region „Nordamerika“. Die Gebühreninformationen können für sämtliche Datengrößen beschafft werden.

[0226] Der CDN-Verkäuferauswahlabschnitt 7a nimmt Bezug auf die Gebühreninformationen auf der Grundlage der Verteilungsdatengröße und berechnet einen Verteilungsabrechnungsbetrag (A1924). Die Berechnung des Verteilungsabrechnungsbetrags kann für jeden CDN-Verkäufer unterschiedlich sein und wird durch ein Verfahren zum Berechnen des Verteilungsabrechnungsbetrags für den CDN-Verkäufer bestimmt. Wenn beispielsweise der Verteilungsabrechnungsbetrag für das CDN 1 in

der Preistabelle der **Fig. 90** berechnet wird, wird, wenn die Region „Nordamerika“ ist und die Verteilungsdatengröße gleich 30 TB ist, Bezug auf die Preistabellen von „bis 10 TB“ und „bis 40 TB“ genommen.

[0227] Der CDN-Verkäuferauswahlabschnitt 7a bestimmt, ob der CDN-Verkäufer, der zu untersuchen ist, ein CDN-Verkäufer ist, der entsprechend der Anzahl der Anfragen abrechnet (A1925). Wenn bestimmt wird, dass der CDN-Verkäufer ein CDN-Verkäufer ist, der nicht entsprechend der Anzahl der Anfragen abrechnet (A1925: nein), bestimmt der CDN-Verkäuferauswahlabschnitt 7a den Verteilungsabrechnungsbetrag als Abrechnungsbetrag des CDN-Verkäufers (A1928), beendet die Berechnung des Abrechnungsbetrags für den CDN-Verkäufer und berechnet den Abrechnungsbetrag des nächsten CDN-Verkäufers.

[0228] Wenn bestimmt wird, dass der CDN-Verkäufer ein CDN-Verkäufer ist, der entsprechend der Anzahl der Anfragen abrechnet (A1925: ja), berechnet der CDN-Verkäuferauswahlabschnitt 7a die Anzahl der Anfragen (A1926). Die Anzahl der Anfragen variiert in Abhängigkeit von dem Verteilungsverfahren. Wenn das Verteilungsverfahren das Speicherverfahren ist, wird die Anzahl der Verteilungszielfahrzeuge der Kampagne als die Anzahl der Anfragen festgelegt. Wenn das Verteilungsverfahren das Streaming-Verfahren ist, wird die Anzahl der Anfragen durch Teilen der Datengröße der Ziel-Kampagne durch die Stückgröße zu der Zeit des Streamens und Multiplizieren mit der Anzahl der Verteilungszielfahrzeuge der Kampagne berechnet.

[0229] Nach der Berechnung der Anzahl der Anfragen berechnet der CDN-Verkäuferauswahlabschnitt 7a einen Abrechnungsbetrag (der auch als Anfrageabrechnungsbetrag bezeichnet werden kann) auf der Grundlage der berechneten Anzahl von Anfragen (A1927). Der Anfrageabrechnungsbetrag ist eine Multiplikation aus dem Abrechnungsbetrag je Anfrage und der Anzahl der Anfragen. Der CDN-Verkäuferauswahlabschnitt 7a bestimmt die Gesamtsumme des Verteilungsabrechnungsbetrags und des Anfrageabrechnungsbetrags als den Abrechnungsbetrag des CDN-Verkäufers (A1928), beendet die Berechnung des Abrechnungsbetrags des CDN-Verkäufers, der zu untersuchen ist, und berechnet den Abrechnungsbetrag des nächsten CDN-Verkäufers.

[0230] Nach der Berechnung des Abrechnungsbetrags für sämtliche CDN-Verkäufer wählt der CDN-Verkäuferauswahlabschnitt 7a einen CDN-Verkäufer mit den niedrigsten Verteilungskosten, d.h. einen CDN-Verkäufer mit dem niedrigsten Abrechnungsbetrag aus (A1930) und beendet den ersten CDN-Aus-

wahlprozess. Bei Beendigung des ersten CDN-Auswahlprozesses speichert der CDN-Verkäuferauswahlabschnitt 7a das Auswahlergebnis, d.h. die Identifizierungsinformationen hinsichtlich des ausgewählten CDN-Verkäufers, in dem Datenspeicherabschnitt 7b (A1914) und meldet dem Kampagnenmeldungserzeugungsabschnitt 7c das Auswahlergebnis (A1915).

[0231] Wie es oben beschrieben wurde, können gemäß der neunzehnten Ausführungsform die folgenden vorteilhaften Wirkungen erzielt werden.

[0232] Der Verteilungsserver 7 nimmt Bezug auf die CDN-Verkäuferverwaltungs-DB, wählt ein CDN 8 mit überlegenen Verteilungskosten entsprechend dem Verteilungsverfahren, dem OTA-Zielbereich und der Verteilungsdatengröße aus den CDNs 8 aus, die unterschiedliche Verteilungskosten aufweisen, und platziert das Aktualisierungspaket in dem ausgewählten CDN 8. Als Ergebnis ist es möglich, die Verteilungskosten geeignet zu verringern, wenn der OTA-Master 4 das Aktualisierungspaket von dem OTA-Zentrum 2 herunterlädt.

Modifikationen der neunzehnten Ausführungsform

[0233] Modifikationen der neunzehnten Ausführungsform werden mit Bezug auf die **Fig. 194** bis 211 beschrieben. Hier wird die erste Modifikation bis fünfte Modifikation beschrieben.

Erste Modifikation der neunzehnten Ausführungsform

[0234] Die erste Modifikation der neunzehnten Ausführungsform wird mit Bezug auf die **Fig. 194** bis 195 beschrieben. In der ersten Modifikation wird die URL des CDN-Servers, die in der Kampagnenmeldung enthalten ist, die an das fahrzeugseitige System 3 verteilt wird, nicht unter Verwendung eines Servers eines Domännennamensystems (DNS) geändert. In der neunzehnten Ausführungsform wird ein CDN-Verkäufer mit den niedrigsten Verteilungskosten für jede Kampagne ausgewählt. Die Kampagnenmeldung enthält die URL des CDN-Servers. Wenn der CDN-Server mit den niedrigsten Verteilungskosten geändert wird, wird daher die URL, die in der Kampagnenmeldung beschrieben ist, geändert. Jedes Mal, wenn eine Kampagnenmeldung erzeugt wird, muss der Kampagnenmeldungserzeugungsabschnitt 7c auf den Datenspeicherabschnitt 7b zugreifen, um CDN-Verkäuferinformationen zu beschaffen.

[0235] Andererseits kann in der ersten Modifikation dadurch, dass der DNS-Einstellabschnitt 7e die Umwandlungsinformationen hinsichtlich der URL und der IP-Adresse, die in dem DNS registriert ist, aktualisiert, der Kampagnenmeldungserzeugungsabschnitt 7c konstant dieselbe URL in die Kampag-

nenmeldung schreiben. Wenn der CDN-Verkäufer mit den niedrigsten Verteilungskosten geändert wird, kann das fahrzeugseitige System 3 auf den ausgewählten CDN-Server durch Ändern der Informationen über einen DNS-Server 12 zugreifen. Mit anderen Worten, in der neunzehnten Ausführungsform weist jeder CDN-Server eine einzigartige IP-Adresse und eine einzigartige URL auf. Andererseits weist in der ersten Modifikation jeder CDN-Server eine einzigartige IP-Adresse auf, weist aber eine den CDN-Servern gemeinsame URL auf.

[0236] Wie es in **Fig. 194** dargestellt ist, enthält der Verteilungsserver 7 in dem OTA-Zentrum 2 einen DNS-Einstellabschnitt 7e zusätzlich zu der CDN-Verkäuferverwaltungs-DB, dem CDN-Verkäuferauswahlabschnitt 7a, dem Datenspeicherabschnitt 7b, dem Kampagnenmeldungserzeugungsabschnitt 7c und dem CDN-Verteilungsabschnitt 7d. Die Unterschiede zu der neunzehnten Ausführungsform werden im Folgenden hauptsächlich beschrieben.

[0237] Der DNS-Server 12 ist ein Server, der einen Mechanismus zum Umwandeln eines Domännennamens und einer IP-Adresse bereitstellt. Die Kampagnenmeldung, die durch das fahrzeugseitige System 3 empfangen wird, enthält die URL des CDN-Servers, auf den zum Herunterladen von Daten zugegriffen wird. Auf ein Empfangen der Kampagnenmeldung hin fragt das fahrzeugseitige System 3 den DNS-Server 12 hinsichtlich der URL, die in der empfangenen Kampagnenmeldung enthalten ist. Der DNS-Server 12 überträgt die IP-Adresse für die URL, von der die Anfrage beschafft wird, an das fahrzeugseitige System 3 oder überträgt das Verbindungsziel an eine Adresse, die durch die IP-Adresse bestimmt wird.

[0238] Der DNS-Einstellabschnitt 7e speichert die Identifizierungsinformationen und die IP-Adresse des CDN-Verkäufers. Wenn der CDN-Verkäufer durch den CDN-Verkäuferauswahlabschnitt 7a ausgewählt ist, überträgt der DNS-Einstellabschnitt 7e eine IP-Adresseinstellanfrage an den DNS-Server 12 und stellt Registrierungsinformationen in dem DNS ein.

[0239] Im Folgenden wird der Betrieb der oben beschriebenen Konfiguration mit Bezug auf **Fig. 195** beschrieben.

(19-3) Prozess des CDN-Verkäuferauswahlabschnittes 7a (siehe Figur 195)

[0240] Wenn der CDN-Verkäuferauswahlabschnitt 7a den ersten CDN-Auswahlprozess beendet und das Auswahlergebnis in dem Datenspeicherabschnitt 7b gespeichert hat (A1914), bewirkt der CDN-Verkäuferauswahlabschnitt 7a, dass der DNS-Einstellabschnitt 7e eine IP-Adresseinstellanfrage an

den DNS-Server 12 überträgt, und stellt Registrierungsinformationen in dem DNS durch den DNS-Einstellabschnitt 7e ein (A1931). Als Ergebnis wird die URL, die in der Kampagnenmeldung enthalten ist, die an das fahrzeugseitige System 3 verteilt wird, sogar dann nicht geändert, wenn sich der CDN-Verkäufer ändert. Wenn das fahrzeugseitige System 3 auf den CDN-Server, der durch die URL angegeben wird, zugreift, beschafft der DNS-Server 12 eine Anfrage der IP-Adresse, um die IP-Adresse des ausgewählten CDN-Servers an das fahrzeugseitige System 3 zu übertragen.

[0241] Der DNS-Einstellabschnitt 7e kann Informationen über den DNS-Server 12 beschaffen oder Einstellinformationen in dem vorherigen DNS-Server 12 speichern und eine Aktualisierungsanfrage der IP-Adresse an den DNS-Server 12 übertragen, wenn der CDN-Server, der in dem DNS-Server 12 registriert ist, sich von dem CDN-Server unterscheidet, der durch den CDN-Verkäuferauswahlabschnitt 7a ausgewählt wird. Wenn die Auswahlmeldung von dem CDN-Verkäuferauswahlabschnitt 7a beschafft wird, erzeugt der Kampagnenmeldungserzeugungsabschnitt 7c eine Kampagnenmeldung, die eine feste URL enthält.

[0242] Gemäß einer derartigen Konfiguration können zusätzlich zu dem Erzielen derselben vorteilhaften Wirkungen wie in der neunzehnten Ausführungsform die URL-Informationen über das CDN, das in der Kampagnenmeldung enthalten ist, konstant dieselben sein, und es kann die Sicherheit verbessert werden.

Zweite Modifikation der neunzehnten Ausführungsform

[0243] Die zweite Modifikation der neunzehnten Ausführungsform wird mit Bezug auf die **Fig. 196** bis 201 beschrieben. Sogar wenn der CDN-Verkäufer, der die Verteilungskosten des Aktualisierungspaketes minimiert, ausgewählt wird, gibt es die Möglichkeit, dass sich die Kommunikationsgeschwindigkeit aufgrund von Wartungsarbeiten, Problemen, einer Zugriffskonzentration und Ähnlichem des CDN-Servers verringert. Die Erfinder der vorliegenden Anmeldung haben sich auf die Auswahl eines CDN-Verkäufers auf der Grundlage der Verteilungskosten und des Verteilungsleistungsvermögens fokussiert.

[0244] Wenn gemäß der zweiten Ausführungsform das fahrzeugseitige System 3 den DNS-Server 12 anfragt, die IP-Adresse, die der URL entspricht, die in der Kampagnenmeldung angegeben ist, zu beschaffen, überprüft der DNS-Server 12 den Verteilungsstatus des CDN-Servers und informiert das fahrzeugseitige System 3 hinsichtlich der IP-Adresse des CDN-Servers mit den zweitniedrigsten Vertei-

lungskosten, wenn bestimmt wird, dass die Verteilung unmöglich ist.

[0245] Wie es in **Fig. 196** dargestellt ist, enthält der Verteilungsserver 7 in dem OTA-Zentrum 2 einen Leistungsmessabschnitt 7f zusätzlich zu der CDN-Verkäuferverwaltungs-DB, dem CDN-Verkäuferauswahlabschnitt 7a, dem Datenspeicherabschnitt 7b, dem Kampagnenmeldungserzeugungsabschnitt 7c, dem CDN-Verteilungsabschnitt 7d und dem DNS-Einstellabschnitt 7e. Der DNS-Server 12 enthält einen CDN-Serververifizierungsabschnitt 12a. In dem Speicherbereich des CDN-Verteilungsabschnittes 7d wird eine Testdatei zum Messen des Leistungsvermögens des CDN-Servers platziert. Der Leistungsmessabschnitt 7f überträgt eine Verteilungsanfrage der Testdatei an den CDN-Server, verteilt die Testdatei von dem CDN-Server und misst eine Zeit, die zum Verteilen der Testdatei benötigt wird, als eine Verteilungszeit. Die Verteilungszeit ist beispielsweise eine Zeit von dem Zeitpunkt, zu dem die Verteilung der Testdatei gestartet wird, bis zu dem Zeitpunkt, zu dem eine Beendigung des Empfangs der Testdatei identifiziert wird.

[0246] Wie es in **Fig. 197** dargestellt ist, enthält die CDN-Verkäuferverwaltungs-DB eine CDN-Serverauswahltablette. Die Auswahltablette enthält den Kostenrang, der durch den CDN-Verkäuferauswahlabschnitt 7a bestimmt wird, und das Verteilungs-Flag, das durch den Leistungsmessabschnitt 7f bestimmt wird.

[0247] Der Leistungsmessabschnitt 7f berechnet eine Antwortgeschwindigkeit aus der Zeit, die benötigt wird, um die Testdatei zu verteilen, für jeden CDN-Server und gibt ein Bestimmungsergebnis auf der Grundlage der berechneten Antwortgeschwindigkeit in die Auswahltablette ein. Wenn die Antwortgeschwindigkeit gleich oder größer als ein spezifizierter bzw. vorbestimmter Wert ist, stellt der Leistungsmessabschnitt 7f das Verteilungs-Flag des CDN-Servers auf ein (wahr) bzw. setzt dieses, und wenn die Antwortgeschwindigkeit kleiner als der spezifizierte Wert ist, setzt der Leistungsmessabschnitt 7f das Verteilungs-Flag des CDN-Servers auf aus (falsch) bzw. setzt dieses zurück.

[0248] Wenn die Anfrage hinsichtlich der IP-Adresse entsprechend der URL von dem fahrzeugseitigen System 3 beschafft wird, bestimmt der CDN-Serververifizierungsabschnitt 12a, ob der CDN-Server, der durch die URL bezeichnet wird, sich in einem verteilungsfähigen Zustand befindet, und wenn bestimmt wird, dass sich der CDN-Server nicht in einem verteilungsfähigen Zustand befindet, informiert er hinsichtlich der IP-Adresse eines anderen CDN-Servers.

[0249] Im Folgenden wird der Betrieb der oben beschriebenen Konfiguration mit Bezug auf die **Fig. 198 bis 201** beschrieben.

(19-4) Prozess des CDN-Verkäuferauswahlabschnittes 7a (siehe Figuren 198 bis 199)

[0250] Wenn in dem ersten CDN-Auswahlprozess der Abrechnungsbetrag für jeden CDN-Verkäufer berechnet ist (A1921 bis A1929), bestimmt der CDN-Verkäuferauswahlabschnitt 7a den Kostenrang des CDN-Verkäufers (A1951). D.h., der CDN-Verkäuferauswahlabschnitt 7a bestimmt den Rang des CDN-Verkäufers mit den niedrigsten Verteilungskosten als den ersten Rang und bestimmt den Rang des CDN-Verkäufers mit den zweitniedrigsten Verteilungskosten als den zweiten Rang. Wenn das Auswahlergebnis in dem Datenspeicherabschnitt 7b gespeichert ist (A1914), speichert der CDN-Verkäuferauswahlabschnitt 7a den Kostenrang in der Auswahltablette der CDN-Verkäuferverwaltungs-DB (A1941).

(19-5) Prozess des Leistungsmessabschnittes 7f (siehe Figur 200)

[0251] Der Leistungsmessabschnitt 7f wiederholt den anschließenden Prozess für jeden CDN-Verkäufer (A1961 bis A1966). Der Leistungsmessabschnitt 7f führt den anschließenden Prozess in regelmäßigen Intervallen oder zu einem beliebigen Zeitpunkt, der von dem Administrator des Verteilungsservers 7 vorgegeben wird, aus, während der Verteilungsserver 7 aktiviert ist.

[0252] Der Leistungsmessabschnitt 7f greift auf den CDN-Server zu (A1962), um eine Testdateiverteilungsanfrage an den CDN-Server zu übertragen. Der Leistungsmessabschnitt 7f berechnet eine Antwortgeschwindigkeit auf der Grundlage der Zeit, die benötigt wird, um die Testdatei zu verteilen, und bestimmt, ob die berechnete Antwortgeschwindigkeit gleich oder größer als ein spezifizierter bzw. vorbestimmter Wert ist (A1963). Die Zeit, die zur Verteilung benötigt wird, kann mit dem spezifizierten Wert verglichen werden, ohne die Antwortgeschwindigkeit zu berechnen, oder es kann die Verteilungsdatengröße je Zeiteinheit mit dem spezifizierten Wert verglichen werden.

[0253] Wenn bestimmt wird, dass die Antwortgeschwindigkeit gleich oder größer als der spezifizierte Wert ist (A1963: ja), bestimmt der Leistungsmessabschnitt 7f, dass der CDN-Server ein Server ist, der zur Verteilung verfügbar ist, und setzt das Verteilungs-Flag auf ein (A1964). Wenn bestimmt wird, dass die berechnete Antwortgeschwindigkeit kleiner als der spezifizierte Wert ist (A1963: nein), bestimmt der Leistungsmessabschnitt 7f, dass der CDN-Server

ver ein Server ist, der nicht zur Verteilung verfügbar ist, und setzt das Verteilungs-Flag auf aus bzw. zurück (A1965).

(19-6) Prozess des CDN-
Serververifizierungsabschnittes 12a (siehe Figur
201)

[0254] Die Kampagnenmeldung gibt die URL zum Zugriff für das Herunterladen der Aktualisierungsdaten an. Das fahrzeugseitige System 3 fragt den DNS-Server 12 hinsichtlich der IP-Adresse, auf die zum Herunterladen des Aktualisierungspaketes zuzugreifen ist.

[0255] Der CDN-Serververifizierungsabschnitt 12a beschafft eine IP-Adressanfrage hinsichtlich der URL, die in der Kampagnenmeldung angegeben ist, von dem fahrzeugseitigen System 3 (A1971). Der CDN-Serververifizierungsabschnitt 12a fragt die CDN-Verkäuferverwaltungs-DB des Verteilungsservers 7 hinsichtlich des Verteilungsstatus des CDN-Servers, der durch die Kampagnenmeldung angegeben wird, an (A1972). In diesem Fall entspricht der CDN-Server dem CDN-Verkäufer, dessen Daten zu beschaffen sind, und der Verteilungsstatus entspricht dem Verteilungs-Flag. Wenn das Verteilungs-Flag des CDN-Verkäufers, dessen Daten zu beschaffen sind, von dem Verteilungsserver beschafft wurde, bestimmt der CDN-Serververifizierungsabschnitt 12a, ob der CDN-Verkäufer, dessen Daten zu beschaffen sind, verfügbar ist (A1973). D.h., der CDN-Serververifizierungsabschnitt 12 bestimmt, ob das beschaffte Verteilungs-Flag auf ein (gesetzt) oder aus (zurückgesetzt) gesetzt ist.

[0256] Wenn bestimmt wird, dass das Verteilungs-Flag auf ein gesetzt ist (A1973: ja), informiert der CDN-Serververifizierungsabschnitt 12a das fahrzeugseitige System 3 hinsichtlich der IP-Adresse, die dem CDN-Verkäufer entspricht, oder überträgt die Verbindung mit dem fahrzeugseitigen System 3 an die IP-Adresse und wechselt zu dem CDN-Verkäufer entsprechend der URL der Kampagnenmeldung (A1974). Wenn bestimmt wird, dass das Verteilungs-Flag auf aus gesetzt ist (A1973: nein), stellt der CDN-Serververifizierungsabschnitt 12a den CDN-Verkäufer mit dem nächsthöchsten Kostenrang als den CDN-Verkäufer mit der zweiten Priorität ein und stellt den CDN-Verkäufer mit der zweiten Priorität als den CDN-Verkäufer ein, dessen Daten zu beschaffen sind (A1975), und dann kehrt der Prozess zu Schritt A1973 zurück.

[0257] Gemäß einer derartigen Konfiguration ist es möglich, einen normal betriebenen CDN-Server auszuwählen, während die Verteilungskosten so weit wie möglich verringert werden. Der CDN-Serververifizierungsabschnitt 12a kann eine Übertragung der Auswahltablelle durch Zugreifen auf die CDN-Ver-

käuferverwaltungs-DB jedes Mal, wenn eine bestimmte Periode verstrichen ist, anfordern. Wenn in diesem Fall die Anfrage hinsichtlich der IP-Adresse von dem fahrzeugseitigen System 3 beschafft wird, kann durch Bezugnahme auf die Auswahltablelle, die durch den CDN-Serververifizierungsabschnitt 12a gehalten bzw. gespeichert wird, bestimmt werden, ob der CDN-Verkäufer, dessen Daten zu beschaffen sind, verfügbar ist, anstelle auf die CDN-Verkäuferverwaltungs-DB zuzugreifen. Außerdem ist es möglich, eine Kommunikation zwischen dem DNS-Server 12 und dem Verteilungsserver 7 zu verringern und einen normal betriebenen CDN-Server auszuwählen, während die Verteilungskosten so weit wie möglich verringert werden.

Dritte Modifikation der neunzehnten
Ausführungsform

[0258] Die dritte Modifikation der neunzehnten Ausführungsform wird mit Bezug auf die **Fig.** 202 bis 205 beschrieben. In der dritten Modifikation misst der Leistungsmessabschnitt 7f in dem Verteilungsserver 7 die Leistungsfähigkeit des CDN-Servers auf der Grundlage der Log-Informationen bzw. Protokollinformationen von dem fahrzeugseitigen System 3 und wertet diese aus. Der Betrieb, wenn der DNS-Server 12 eine Anfrage hinsichtlich einer IP-Adresse für eine URL von dem fahrzeugseitigen System 3 beschafft, ist ähnlich wie derjenige der zweiten Modifikation. Auch in der dritten Modifikation enthält die CDN-Verkäuferverwaltungs-DB wie in der zweiten Modifikation eine Auswahltablelle.

[0259] Das fahrzeugseitige System 3 enthält einen Protokollübertragungsabschnitt 3a. Wenn das Herunterladen der Aktualisierungsdaten von dem CDN-Server beendet ist, überträgt der Protokollübertragungsabschnitt 3a Protokollinformationen betreffend das Herunterladen, die eine Herunterladezeit enthalten, die eine Zeit angibt, die für das Herunterladen benötigt wird, an den Leistungsmessabschnitt 7f des Verteilungsservers 7. Die Protokollinformationen betreffend das Herunterladen können zusätzlich zu der Herunterladezeit Informationen wie beispielsweise Identifizierungsinformationen hinsichtlich eines heruntergeladenen Paketes, einer Datengröße und eines maximalen Durchsatzes während des Herunterladens enthalten.

[0260] Auf ein Empfangen der Protokollinformationen betreffend das Herunterladen von dem Protokollübertragungsabschnitt 3a hin berechnet der Leistungsmessabschnitt 7f einen Durchsatz aus der Herunterladezeit und gibt ein Bestimmungsergebnis auf der Grundlage des berechneten Durchsatzes in die Auswahltablelle ein. Der Leistungsmessabschnitt 7f setzt das Verteilungs-Flag des CDN-Servers auf ein (wahr), wenn der Durchsatz gleich oder größer als ein spezifizierter bzw. bestimmter Wert ist, und

setzt das Verteilungs-Flag des CDN-Servers auf aus (falsch), wenn der Durchsatz kleiner als der spezifizierte Wert ist.

[0261] Im Folgenden wird der Betrieb der oben beschriebenen Konfiguration mit Bezug auf die Fig. 203 bis 205 beschrieben.

(19-8) Prozess des
Protokollübertragungsabschnittes 3a (siehe Figur 203)

[0262] Wenn das Herunterladen des Aktualisierungspaketes von dem CDN-Server beendet ist (A1981), überträgt der Protokollübertragungsabschnitt 3a Protokollinformationen betreffend das Herunterladen einschließlich einer Herunterladezeit, die eine Zeit angibt, die für das Herunterladen benötigt wird, an den Verteilungsserver 7 (A1982).

(19-9) Prozess des
Leistungsbestimmungsabschnittes 7f (siehe Figur 204)

[0263] Wenn die Protokollinformationen betreffend das Herunterladen von dem Protokollübertragungsabschnitt 3a empfangen wurden (A1991), berechnet der Leistungsbestimmungsabschnitt 7f einen Durchsatz aus der Herunterladezeit (A1992) und bestimmt, ob der berechnete Durchsatz gleich oder größer als ein spezifizierter bzw. vorbestimmter Wert ist (A1993).

[0264] Wenn bestimmt wird, dass der berechnete Durchsatz gleich oder größer als der spezifizierte Wert ist (A1993: ja), bestimmt der Leistungsmessabschnitt 7f, dass der CDN-Server ein Server ist, der zur Verteilung verfügbar ist, und setzt das Verteilungs-Flag auf ein (A1994). Wenn bestimmt wird, dass der berechnete Durchsatz kleiner als der spezifizierte Wert ist (A1993: nein), bestimmt der Leistungsmessabschnitt 7f, dass der CDN-Server ein Server ist, der zur Verteilung nicht verfügbar ist, und setzt das Verteilungs-Flag auf aus (A1995).

(19-10) Prozess des
Leistungsbestimmungsabschnittes 7f (siehe Figur 205)

[0265] Der Leistungsbestimmungsabschnitt 7f führt periodisch einen Zurück-Prozess des CDN-Servers durch, bei dem das Verteilungs-Flag auf aus gesetzt wird. Der Leistungsmessabschnitt 7f benachrichtigt die CDN-Verkäuferverwaltungs-DB hinsichtlich der Informationsanfrage des CDN-Servers, in dem das Verteilungs-Flag auf aus gesetzt ist, identifiziert den CDN-Server, in dem das Verteilungs-Flag auf aus gesetzt ist (A19101), und wiederholt den anschließenden Prozess für jeden CDN-Verkäufer (A19102 bis 19107). Der Leistungsmessabschnitt 7f führt den

anschließenden Prozess in regelmäßigen Intervallen oder zu einem beliebigen Zeitpunkt, der durch den Administrator des Verteilungsservers 7 festgelegt wird, aus, während der Verteilungsserver 7 aktiviert ist.

[0266] Der Leistungsmessabschnitt 7f benachrichtigt den CDN-Server hinsichtlich der Testdateiverteilungsanfrage, berechnet den Durchsatz aus der Herunterladezeit der Datei, die von dem CDN-Server verteilt wird (A19103), und bestimmt, ob der berechnete Durchsatz gleich oder größer als ein spezifizierter bzw. vorbestimmter Wert ist (A19104).

[0267] Wenn bestimmt wird, dass der berechnete Durchsatz gleich oder größer als der spezifizierte Wert ist (A19104: ja), ändert der Leistungsmessabschnitt 7f das Verteilungs-Flag von aus nach ein (A19105). Wenn bestimmt wird, dass der berechnete Durchsatz kleiner als der spezifizierte Wert ist (A19104: nein), hält der Leistungsmessabschnitt 7f das Verteilungs-Flag auf aus (A19106). Der Leistungsmessabschnitt 7f kann dann, wenn der Verteilungsserver aktiviert wird, oder jede vorbestimmte Periode das Verteilungs-Flag, das auf aus gesetzt ist, in der CDN-Verkäuferverwaltungs-DB auf ein setzen.

[0268] Gemäß einer derartigen Konfiguration ist es im Vergleich zu der zweiten Modifikation, bei der die Verteilungsanfrage der Testdatei an den CDN-Server übertragen wird, um die Antwort des CDN-Servers zu identifizieren, nicht notwendig, die Verteilungsanfrage der Testdatei an den CDN-Server zu übertragen, und es ist möglich, die Last und die Kosten auf dem Kommunikationsnetzwerk zu verringern. Wenn durch Bereitstellen der Funktion des Messens der Herunterladegeschwindigkeit des Aktualisierungspaketes in dem fahrzeugseitigen System 3 bestimmt wird, dass der Durchsatz kleiner als der spezifizierte Wert ist, kann die Verbindung in eine Verbindung mit einem anderen CDN-Server geändert werden.

[0269] Die Kampagnenmeldung, die von dem Verteilungsserver 7 verteilt wird, kann zusätzlich zu der URL des CDN-Servers, mit dem zuerst zu verbinden ist, die URL eines freien CDN-Servers, mit dem zu verbinden ist, wenn der Durchsatz des CDN-Servers niedrig ist, enthalten. Der freie CDN-Server ist beispielsweise ein CDN-Server mit den zweitniedrigsten Verteilungskosten oder ein freier CDN-Server, der im Voraus bestimmt wird. Wenn mehrere CDN-Server als freie CDN-Server bestimmt werden, können Informationen, die eine Verbindungsreihenfolge angeben, hinzugefügt werden.

[0270] Wenn das Herunterladen des Aktualisierungspaketes gestartet wird, misst das fahrzeugseitige System 3 den Durchsatz und überprüft, ob der Durchsatz gleich oder größer als der spezifizierte

Wert ist. Wenn bestimmt wird, dass der Durchsatz nicht gleich oder größer als der spezifizierte Wert ist, fragen das Fahrzeug und das beidseitige System 3 den DNS-Server 12 hinsichtlich der IP-Adresse der URL des freien CDN-Servers, der in der Kampagnenmeldung angegeben ist, und ändern die Verbindung mit dem ursprünglichen CDN-Server in diejenige mit dem neuen CDN-Server. Da die Identifizierungsinformationen zu den verteilten Daten für jedes Paket hinzugefügt werden, kann das Aktualisierungspaket sogar dann, wenn der CDN-Server in der Mitte des Herunterladens des Aktualisierungspaketes geändert wird, kontinuierlich heruntergeladen werden.

Vierte Modifikation der neunzehnten Ausführungsform

[0271] Die vierte Modifikation der neunzehnten Ausführungsform wird mit Bezug auf die **Fig.** 206 bis 207 beschrieben. In der vierten Modifikation wählt der CDN-Verkäuferabschnitt 7a mehrere CDN-Verkäufer aus, und der Kampagnenmeldungserzeugungsabschnitt 7c erzeugt mehrere Kampagnenmeldungen für die jeweiligen CDN-Verkäufer. Wenn die Kampagnenmeldung an das fahrzeugseitige System 3 verteilt wird, wird ein jeweils anderer CDN-Server unter Verwendung eines Round-Robin-Verfahrens (Ringverfahren) bestimmt.

(19-11) Prozess des Kampagnenmeldungserzeugungsabschnittes 7c (siehe Figur 206)

[0272] Wenn CDN-Verkäuferinformationen (A195) beschafft wurden, erzeugt der Kampagnenmeldungserzeugungsabschnitt 7c eine Kampagnenmeldung für jeden CDN-Verkäufer (A1911). D.h., der Kampagnenmeldungserzeugungsabschnitt 7c erzeugt zwei oder mehr Kampagnenmeldungen für eine Kampagne. Der Kampagnenmeldungserzeugungsabschnitt 7c verteilt die Kampagnenmeldungen derart, dass der Server auf eine Round-Robin-Weise wechselt (A1912). In einem Fall beispielsweise, in dem zwei CDN-Server, d.h. ein CDN 11 und ein CDN 12, ausgewählt werden, verteilt der Kampagnenmeldungserzeugungsabschnitt 7c eine Kampagnenmeldung, die die URL des CDN 11 enthält, an das erste Fahrzeug, verteilt eine Kampagnenmeldung, die die URL des CDN 12 enthält, an das nächste Fahrzeug und verteilt eine Kampagnenmeldung, die die URL des CDN 11 enthält, an das weiter folgende Fahrzeug, wenn die Kampagnenmeldungen verteilt werden.

(19-12) Prozess des CDN-Verkäuferauswahlabschnittes 7a (siehe Figur 207)

[0273] In der neunzehnten Ausführungsform wählt der CDN-Verkäuferabschnitt 7a den CDN-

Verkäufer mit den niedrigsten Verteilungskosten aus, aber in der vierten Modifikation werden mehrere CDN-Verkäufer in aufsteigender Reihenfolge der Verteilungskosten ausgewählt (A19121).

[0274] Gemäß einer derartigen Konfiguration ist es möglich, zu verhindern, dass sich ein Zugriff auf einen speziellen CDN-Server konzentriert, wenn die Verteilungskosten der CDN-Server verringert werden, und es ist möglich, eine Verringerung des Durchsatzes durch Verhindern einer Zugriffskonzentration zu verhindern.

Fünfte Modifikation der neunzehnten Ausführungsform

[0275] Die fünfte Modifikation der neunzehnten Ausführungsform wird mit Bezug auf die **Fig.** 208 bis 211 beschrieben. In der vierten Modifikation werden mehrere CDN-Verkäufer, deren Verteilungskosten geringer sind, ausgewählt, es werden mehrere Kampagnenmeldungen mit unterschiedlichen CDN-Serverinformationen erzeugt, und die Kampagnenmeldung wird an das fahrzeugseitige System 3 derart verteilt, dass der CDN-Server in einer Round-Robin-Weise geändert wird. Andererseits werden in der fünften Modifikation mehrere CDN-Verkäufer, deren Verteilungskosten geringer sind, ausgewählt, es wird eine Kampagnenmeldung erzeugt, und die erzeugte Kampagnenmeldung wird an das fahrzeugseitige System 3 verteilt. Wenn der DNS-Server 12 die Anfrage hinsichtlich der IP-Adresse entsprechend der URL, die in der Kampagnenmeldung angegeben ist, von dem fahrzeugseitigen System 3 beschafft, wird der CDN-Server, der auf das fahrzeugseitige System 3 antwortet, für jedes fahrzeugseitige System 3 geändert. Mit anderen Worten, in dem DNS-Server 12 wird der CDN-Server auf Round-Robin-Weise ausgewählt.

[0276] Wie es in **Fig.** 208 dargestellt ist, enthält der DNS-Server 12 einen Wechselabschnitt 12b. Wenn eine Anfrage hinsichtlich der IP-Adresse von dem fahrzeugseitigen System 3 beschafft wird, ändert der Wechselabschnitt 12b aufeinanderfolgend die IP-Adresse, auf die von dem fahrzeugseitigen System 3 zu antworten ist, gemäß dem Round-Robin-Verfahren. Der Verteilungsserver enthält den DNS-Einstellabschnitt 7e. Der DNS-Einstellabschnitt 7e der fünften Modifikation überträgt die Round-Robin-Aufzeichnung, die in **Fig.** 209 dargestellt ist, an den DNS-Server 12.

(19-13) Prozess des CDN-Verkäuferauswahlabschnittes 7a (siehe Figur 210)

[0277] Wie in der vierten Modifikation wählt der CDN-Verkäuferabschnitt 7a mehrere CDN-Verkäufer in aufsteigender Reihenfolge der Vertei-

lungskosten aus (A19121) und stellt eine Round-Robin-Aufzeichnung ein (A19131).

(19-14) Prozess des Wechselabschnittes 12b (siehe Figur 211)

[0278] Wenn die Anfrage hinsichtlich der IP-Adresse von dem fahrzeugseitigen System 3 beschafft wird (A19141), nimmt der DNS-Server 12 Bezug auf die Round-Robin-Aufzeichnung (A19142), um die IP-Adresse, die dem beschriebenen CDN-Server entspricht, an das fahrzeugseitige System 3 zu übertragen (A19143). Der DNS-Server 12 wiederholt den oben beschriebenen Prozess jedes Mal, wenn die Anfrage hinsichtlich der IP-Adresse von dem fahrzeugseitigen System 3 beschafft wird, und wenn die Anfrage hinsichtlich der IP-Adresse von einem anderen fahrzeugseitigen System 3 beschafft wird, nimmt der DNS-Server Bezug auf die Round-Robin-Aufzeichnung, um eine IP-Adresse entsprechend einem CDN-Server, der nicht derjenige zu der vorherigen Zeit ist, an das fahrzeugseitige System 3 zu übertragen. D.h., der DNS-Server 12 überträgt aufeinanderfolgend die IP-Adressen der CDN-Server an die fahrzeugseitigen Systeme 3 entsprechend dem Round-Robin-Verfahren.

[0279] Gemäß einer derartigen Konfiguration ist es möglich, zu verhindern, dass sich ein Zugriff auf einen speziellen CDN-Server konzentriert, während die Verteilungskosten der CDN-Server verringert werden, und es ist möglich, eine Verringerung des Durchsatzes durch Verhindern einer Zugriffskonzentration zu verhindern.

Zwanzigste Ausführungsform

[0280] Die zwanzigste Ausführungsform wird mit Bezug auf die **Fig. 212** bis 224 beschrieben.

[0281] In der zwanzigsten Ausführungsform werden in einem Fall, in dem Informationen über mehrere Kampagnen in einer vorbestimmten Periode beschafft werden können, mehrere CDN-Verkäufer dynamisch als Platzierungsziele eines Aktualisierungspaketes in dem CDN 8 entsprechend einem Verteilungsverfahren, einem OTA-Zielbereich, der ein Verteilungsbereich ist, und einer Verteilungsdatengröße ausgewählt, um die Verteilungskosten zu verringern. Die vorbestimmte Periode ist beispielsweise der anschließende Monat.

[0282] In der oben beschriebenen neunzehnten Ausführungsform wird der CDN-Verkäufer mit den niedrigsten Verteilungskosten für eine Kampagne ausgewählt. Es ist jedoch auch denkbar, dass eine Kampagne von dem OEM-Server für mehrere Kampagnen, deren Verteilung geplant ist, für eine vorbestimmte Zeitdauer, beispielsweise den folgenden

Monat, zu registrieren. In einem Fall, in dem Informationen über die Datengröße jeder Kampagne, die Anzahl der Verteilungszielfahrzeuge, den OTA-Zielbereich und das Verteilungsverfahren im Voraus für mehrere Kampagnen beschafft werden, besteht die Möglichkeit, dass ein anderer CDN-Verkäufer als derjenige in dem Fall, in dem ein CDN-Verkäufer für eine jeweilige Kampagne wie in der neunzehnten Ausführungsform ausgewählt wird, der CDN-Verkäufer mit den niedrigsten Verteilungskosten ist.

[0283] Wie es in **Fig. 212** dargestellt ist, enthält das OTA-Zentrum 2 die CDN-Verkäuferverwaltungs-DB, den CDN-Verkäuferauswahlabschnitt 7a, den Datenspeicherabschnitt 7b, den Kampagnenmeldungserzeugungsabschnitt 7c, den CDN-Verteilungsabschnitt 7d und einen Fortschrittsinformationsverwaltungsabschnitt 7g. Der Fortschrittsinformationsverwaltungsabschnitt 7g hält einen Vorhersagewert, der angibt, wieviel der Kampagne an das fahrzeugseitige System 3 innerhalb einer vorbestimmten Periode verteilt wird. Sogar wenn die Kampagne in dem OTA-Zentrum 2 registriert wird und die Kampagnenmeldung an das fahrzeugseitige System 3 verteilt wird, wenden nicht alle Fahrzeuge unmittelbar die Kampagne an und laden das Aktualisierungspaket von dem CDN-Server herunter. Der Fortschrittsinformationsverwaltungsabschnitt 7g speichert den Vorhersagewert, um genauer die Verteilungsdatengröße des Aktualisierungspaketes von dem CDN-Server an das fahrzeugseitige System 3 vorherzusagen. In der vorliegenden Ausführungsform wird die vorbestimmte Periode als ein Monat beschrieben, aber es können andere Perioden bzw. Zeitspannen verwendet werden.

[0284] Ein Berechnungsverfahren der zwanzigsten Ausführungsform wird mit Bezug auf **Fig. 213** beschrieben. In der zwanzigsten Ausführungsform wird der Abrechnungsbetrag des CDN-Verkäufers durch drei später beschriebene Berechnungsverfahren berechnet. In dem ersten Berechnungsverfahren wird ein CDN-Verkäufer mit den niedrigsten Verteilungskosten in jeder Kampagne ausgewählt. In diesem Fall können unterschiedliche CDN-Verkäufer für die jeweiligen Kampagnen ausgewählt werden. **Fig. 213** stellt einen Fall dar, in dem ein CDN 1 für eine Kampagne 1 ausgewählt wird, ein CDN 2 für eine Kampagne 2 ausgewählt wird und ein CDN 3 für eine Kampagne 3 ausgewählt wird.

[0285] In dem zweiten Berechnungsverfahren wird die Gesamtverteilungsdatengröße aller Kampagnen berechnet, und der CDN-Verkäufer mit den niedrigsten Verteilungskosten wird auf der Grundlage der berechneten Gesamtverteilungsdatengröße aller Kampagnen ausgewählt. In diesem Fall wird derselbe CDN-Verkäufer für alle Kampagnen ausgewählt. **Fig. 213** stellt einen Fall dar, in dem der

CDN 1 für die Kampagnen 1 bis 3 ausgewählt wird. In dem dritten Berechnungsverfahren wird die Gesamtverteilungsdatengröße der Kampagne für jedes Verteilungsverfahren berechnet, und der CDN-Verkäufer mit den niedrigsten Verteilungskosten wird auf der Grundlage der berechneten Gesamtverteilungsdatengröße der Kampagne für jedes Verteilungsverfahren ausgewählt. Für jedes Verteilungsverfahren, d.h. Streaming-Verfahren und Speicherverfahren, wird ein CDN-Verkäufer ausgewählt. **Fig. 213** stellt einen Fall dar, in dem das Verteilungsverfahren für die Kampagne 1 zu dem für die die Kampagnen 2 und 3 unterschiedlich ist, das CDN 1 für die Kampagne 1 ausgewählt wird und das CDN 2 für die Kampagnen 2 und 3 ausgewählt wird.

[0286] Im Folgenden wird der Betrieb der oben beschriebenen Konfiguration mit Bezug auf die **Fig. 214** bis 224 beschrieben.

(20-1) Prozess des
Kampagnenmeldungserzeugungsabschnittes 7c
(siehe Figur 214)

[0287] Der Kampagnenmeldungserzeugungsabschnitt 7c beschafft Kampagneninformationen, deren Verteilung von der Außenseite wie beispielsweise einem OEM-Server geplant ist, von dem OEM-Server (A201). Die Kampagneninformationen, deren Verteilung geplant ist, enthalten Informationen über ein Verteilungsstartdatum, eine Datengröße einer Zielkampagne, die Anzahl der Verteilungszielfahrzeuge der Zielkampagne, eine Region und ein Verteilungsverfahren. Der Kampagnenmeldungserzeugungsabschnitt 7c speichert die beschafften Kampagneninformationen in dem Datenspeicherabschnitt 7b (A202).

[0288] Der Kampagnenmeldungserzeugungsabschnitt 7c benachrichtigt den CDN-Verkäuferauswahlabschnitt 7a hinsichtlich der CDN-Verkäuferauswahlfrage (A203) und wartet auf die Beschaffung der Auswahlmeldung von dem CDN-Verkäuferauswahlabschnitt 7a. Wenn die Auswahlmeldung von dem CDN-Verkäuferauswahlabschnitt 7a beschafft ist (A204), greift der Kampagnenmeldungserzeugungsabschnitt 7c auf den Datenspeicherabschnitt 7b zu und beschafft die Identifizierungsinformationen hinsichtlich des CDN-Verkäufers, der durch den CDN-Verkäuferauswahlabschnitt 7a ausgewählt wird (A205).

[0289] Auf der Grundlage der Identifizierungsinformationen über den CDN-Verkäufer erzeugt der Kampagnenmeldungserzeugungsabschnitt 7c eine Parameterdatei, die die URL des ausgewählten CDN enthält, als eine Kampagnenmeldung, deren Verteilung geplant ist (A206). Der Kampagnenmeldungserzeugungsabschnitt 7c verteilt die erzeugte Kampagne-

nenmeldung, deren Verteilung geplant ist, an das fahrzeugseitige System 3 (A207).

(20-2) Prozess des CDN-
Verkäuferauswahlabschnittes 7a (siehe Figuren 215
bis 221)

[0290] Wenn der CDN-Verkäuferauswahlabschnitt 7a die CDN-Verkäuferauswahlfrage, die von dem Kampagnenmeldungserzeugungsabschnitt 7 gemeldet wird, beschafft hat (A2011), greift der CDN-Verkäuferauswahlabschnitt 7a auf den Datenspeicherabschnitt 7b zu, um Auswahlinformationen zu beschaffen (A2012). In diesem Fall enthalten die Auswahlinformationen Informationen über die Datengrößen aller Zielkampagnen, deren Verteilung geplant ist, die Anzahl der Verteilungszielfahrzeuge, die Region, das Verteilungsverfahren und das Verteilungsstartdatum jeder Kampagne.

[0291] Der CDN-Verkäuferauswahlabschnitt 7a beschafft den Verteilungsvorhersagewert von dem Fortschrittsinformationsverwaltungsabschnitt 7g (A2013). Der CDN-Verkäuferauswahlabschnitt 7a berechnet die Verteilungsdatengröße für jede Kampagne (A2014). Insbesondere multipliziert der CDN-Verkäuferauswahlabschnitt 7a die Datengröße der Kampagne, die Anzahl der Verteilungszielfahrzeuge der Kampagne und den Verteilungsvorhersagewert miteinander und multipliziert außerdem einen Korrekturwert entsprechend der Verteilungsperiode. Je nach Kampagne gibt es einen Fall, in dem die Verteilungsperiode kurz ist, beispielsweise in einem Fall, in dem das Verteilungsstartdatum auf das Ende eines nächsten Monats festgelegt ist, und somit wird eine Einstellung mit einem Korrekturwert entsprechend der Verteilungsperiode durchgeführt. In einem Fall beispielsweise, in dem als Ergebnis einer Verzögerung des Verteilungsstartdatums die Verteilungsperiode nur 10 Tage aus 30 Tagen beträgt, wird 0,3 oder Ähnliches als Korrekturwert festgelegt.

[0292] Der CDN-Verkäuferauswahlabschnitt 7a schreitet mit dem Prozess zum zweiten CDN-Auswahlprozess (A2015). Wenn der zweite CDN-Auswahlprozess gestartet wird, geht der CDN-Verkäuferauswahlabschnitt 7a aufeinanderfolgend zu einem Abrechnungsbetragsberechnungsprozess durch das erste Berechnungsverfahren, einem Abrechnungsbetragsberechnungsprozess durch das zweite Berechnungsverfahren und einem Abrechnungsbetragsberechnungsprozess durch das dritte Berechnungsverfahren über (A2021 bis A2023).

[0293] In dem Abrechnungsbetragsberechnungsprozess durch das erste Berechnungsverfahren wählt der CDN-Verkäuferauswahlabschnitt 7a einen CDN-Verkäufer mit den niedrigsten Verteilungskosten für jede Kampagne aus. Wenn der Abrechnungs-

betragsberechnungsprozess durch das erste Berechnungsverfahren gestartet wird, wiederholt der CDN-Verkäuferauswahlabschnitt 7a den anschließenden Prozess für jede Kampagne (A2031 bis A2041) und wiederholt den Prozess für jeden CDN-Verkäufer (A2032 bis A2039). Der CDN-Verkäuferauswahlabschnitt 7a beschafft die Gebühreninformationen aus der CDN-Verkäuferverwaltungs-DB auf der Grundlage der Verteilungsdatengröße und der Regioneninformationen (A2033). Der CDN-Verkäuferauswahlabschnitt 7a nimmt Bezug auf die Gebühreninformationen auf der Grundlage der Verteilungsdatengröße und berechnet einen Verteilungsabrechnungsbetrag (A2034).

[0294] Wie in der neunzehnten Ausführungsform bestimmt der CDN-Verkäuferauswahlabschnitt 7a, ob der betreffende CDN-Verkäufer ein CDN-Verkäufer ist, der entsprechend der Anzahl der Anfragen abrechnet, und bestimmt den Abrechnungsbetrag des CDN-Verkäufers (A2035 bis A2038). Der CDN-Verkäuferauswahlabschnitt 7a wiederholt die Berechnung des Verteilungsabrechnungsbetrags für jeden CDN-Verkäufer und jede Kampagne. Wenn die Abrechnungsbeträge aller CDN-Verkäufer für eine Kampagne berechnet sind, wählt der CDN-Verkäuferauswahlabschnitt 7a denjenigen CDN-Verkäufer mit den niedrigsten Verteilungskosten für die jeweilige Kampagne aus (A2040).

[0295] Bei Beendigung der Berechnung des Verteilungsabrechnungsbetrags und der Auswahl des CDN-Verkäufers für alle Kampagnen summiert der CDN-Verkäuferauswahlabschnitt 7a die Verteilungsabrechnungsbeträge aller Kampagnen und berechnet den Gesamtbetrag (A2042) und beendet den Prozess zum Berechnen des Abrechnungsbetrags durch das erste Berechnungsverfahren und schreitet zum Prozess der Berechnung des Abrechnungsbetrags durch das zweite Berechnungsverfahren.

[0296] In dem Abrechnungsbetragsberechnungsprozess durch das zweite Berechnungsverfahren wählt der CDN-Verkäuferauswahlabschnitt 7a einen CDN-Verkäufer auf der Grundlage der Gesamtverteilungsdatengröße aller Kampagnen, deren Verteilung geplant ist, aus. Wenn der Abrechnungsbetragsberechnungsprozess durch das zweite Berechnungsverfahren gestartet wird, summiert der CDN-Verkäuferauswahlabschnitt 7a die Verteilungsdatengrößen der jeweiligen Kampagnen, berechnet dadurch die Gesamtverteilungsdatengröße (A2051) und wiederholt dann den anschließenden Prozess für jeden CDN-Verkäufer (A2052 bis A2059). Der CDN-Verkäuferauswahlabschnitt 7a beschafft die Gebühreninformationen aus der CDN-Verkäuferverwaltungs-DB auf der Grundlage der Gesamtverteilungsdatengröße und der Regioneninformationen (A2053). Der CDN-Verkäuferauswahlabschnitt 7a nimmt Bezug auf die Gebühreninformationen auf der Grundlage

der Gesamtverteilungsdatengröße und berechnet einen Verteilungsabrechnungsbetrag (A2054).

[0297] Wie in der neunzehnten Ausführungsform bestimmt der CDN-Verkäuferauswahlabschnitt 7a, ob der betreffende CDN-Verkäufer ein CDN-Verkäufer ist, der entsprechend der Anzahl der Anfragen abrechnet, und bestimmt den Abrechnungsbetrag des CDN-Verkäufers (A2055 bis A2058). Der CDN-Verkäuferauswahlabschnitt 7a wiederholt die Berechnung des Verteilungsabrechnungsbetrags für jeden CDN-Verkäufer. Der CDN-Verkäuferauswahlabschnitt 7a wählt einen CDN-Verkäufer mit den niedrigsten Verteilungskosten aus (A2060). Die Verteilungsabrechnungsbeträge aller Kampagnen, deren Verteilung geplant ist, werden aufsummiert, um den Gesamtbetrag zu berechnen (A2061), der Abrechnungsbetragsberechnungsprozess durch das zweite Berechnungsverfahren wird beendet, und der Prozess schreitet zu dem Abrechnungsbetragsberechnungsprozess durch das dritte Berechnungsverfahren.

[0298] In dem Abrechnungsbetragsberechnungsprozess durch das dritte Berechnungsverfahren wählt der CDN-Verkäuferauswahlabschnitt 7a einen CDN-Verkäufer nach einem Sammeln von Kampagnen für jedes Verteilungsverfahren aus. Wenn der Abrechnungsbetragsberechnungsprozess durch das dritte Berechnungsverfahren gestartet wird, bestimmt der CDN-Verkäuferauswahlabschnitt 7a, ob alle Verteilungsverfahren der Kampagne, deren Verteilung geplant ist, dieselben sind (A2071). Wenn bestimmt wird, dass alle Verteilungsverfahren der Kampagnen, deren Verteilung geplant ist, dieselben sind, d.h., wenn alle Kampagnen, deren Verteilung geplant ist, das Streaming-Verfahren verwenden, oder wenn alle Kampagnen das Speicherverfahren verwenden (A2071: ja), beendet der CDN-Verkäuferauswahlabschnitt 7a den Abrechnungsbetragsberechnungsprozess durch das dritte Berechnungsverfahren, da der Abrechnungsbetragsberechnungsprozess derselbe wie der Abrechnungsbetragsberechnungsprozess durch das oben beschriebene zweite Berechnungsverfahren ist.

[0299] Wenn bestimmt wird, dass nicht alle Verteilungsverfahren der Kampagnen, deren Verteilung geplant ist, dieselben sind, d.h., wenn das Streaming-Verfahren und das Speicherverfahren der Kampagnen, deren Verteilung geplant ist, gemischt sind (A2071: nein), gruppiert der CDN-Verkäuferauswahlabschnitt 7a die Kampagnen entsprechend den Verteilungsverfahren (A2072) und geht zum Prozess für den Abrechnungsbetragsberechnungsprozess für das Streaming-Verfahren für die Gruppen (A2073) und zu dem Abrechnungsbetragsberechnungsprozess für das Speicherverfahren für die Gruppen über (A2074).

[0300] Wenn der Abrechnungsbetragsberechnungsprozess für das Streaming-Verfahren gestartet wird, berechnet der CDN-Verkäuferauswahlabschnitt 7a die Summe der Verteilungsdatengrößen der jeweiligen Kampagnen, die durch das Streaming-Verfahren verteilt werden (A2081), und wiederholt den anschließenden Prozess für jeden CDN-Verkäufer (A2082 bis A2089). Der CDN-Verkäuferauswahlabschnitt 7a beschafft die Gebühreninformationen aus der CDN-Verkäuferverwaltungs-DB auf der Grundlage der Summe der Verteilungsdatengrößen und der Regioneninformationen (A2083). Der CDN-Verkäuferauswahlabschnitt 7a nimmt Bezug auf die Gebühreninformationen auf der Grundlage der Summe der Verteilungsdatengrößen und berechnet den Verteilungsabrechnungsbetrag (A2084).

[0301] Wie in der neunzehnten Ausführungsform bestimmt der CDN-Verkäuferauswahlabschnitt 7a, ob der betreffende CDN-Verkäufer ein CDN-Verkäufer ist, der entsprechend der Anzahl der Anfragen abrechnet, und bestimmt den Abrechnungsbetrag des CDN-Verkäufers (A2085 bis A2088). Der CDN-Verkäuferauswahlabschnitt 7a wiederholt die Berechnung des Verteilungsabrechnungsbetrags für jeden CDN-Verkäufer. Der CDN-Verkäuferauswahlabschnitt 7a wählt den CDN-Verkäufer mit den niedrigsten Verteilungskosten in dem Streaming-Verfahren aus (A2090) und beendet den Abrechnungsbetragsberechnungsprozess des Streaming-Verfahrens.

[0302] Wenn andererseits der Abrechnungsbetragsberechnungsprozess für das Speicherverfahren gestartet wird, berechnet der CDN-Verkäuferauswahlabschnitt 7a die Summe der Verteilungsdatengrößen der jeweiligen Kampagnen, die durch das Speicherverfahren verteilt werden (A2091), und wiederholt den anschließenden Prozess für jeden CDN-Verkäufer (A2092 bis A2099). Der CDN-Verkäuferauswahlabschnitt 7a beschafft die Gebühreninformationen aus der CDN-Verkäuferverwaltungs-DB auf der Grundlage der Summe der Verteilungsdatengrößen und der Regioneninformationen (A2093). Der CDN-Verkäuferauswahlabschnitt 7a nimmt Bezug auf die Gebühreninformationen auf der Grundlage der Summe der Verteilungsdatengrößen und berechnet den Verteilungsabrechnungsbetrag (A2094).

[0303] Wie in der neunzehnten Ausführungsform bestimmt der CDN-Verkäuferauswahlabschnitt 7a, ob der betreffende CDN-Verkäufer ein CDN-Verkäufer ist, der entsprechend der Anzahl von Anfragen abrechnet, und bestimmt den Abrechnungsbetrag des CDN-Verkäufers (A2095 bis A2098). Der CDN-Verkäuferauswahlabschnitt 7a wiederholt die Berechnung des Verteilungsabrechnungsbetrags für jeden CDN-Verkäufer. Der CDN-Verkäuferauswahlabschnitt 7a wählt den CDN-Verkäufer mit den niedrigsten Verteilungskosten in dem Speicherverfahren

aus (A20100) und beendet den Abrechnungsbetragsberechnungsprozess des Speicherverfahrens.

[0304] Nach Beendigung des Abrechnungsbetragsberechnungsprozesses durch das erste Berechnungsverfahren, des Abrechnungsbetragsberechnungsprozesses durch das zweite Berechnungsverfahren und des Abrechnungsbetragsberechnungsprozesses durch das dritte Berechnungsverfahren bestimmt der CDN-Verkäuferauswahlabschnitt 7a ein Berechnungsverfahren, das die Verteilungskosten minimiert (A2024), wählt einen CDN-Verkäufer jeder Kampagne aus (A2025) und beendet den zweiten CDN-Auswahlprozess. Bei Beendigung des zweiten CDN-Auswahlprozesses speichert der CDN-Verkäuferauswahlabschnitt 7a das Auswahlresultat, d.h. die Identifizierungsinformationen zum Identifizieren des ausgewählten CDN-Verkäufers, in dem Datenspeicherabschnitt 7b (A2016). Hier speichert der CDN-Verkäuferauswahlabschnitt 7a Identifizierungsinformationen zum Identifizieren des CDN-Verkäufers der Kampagne, deren Verteilung geplant ist, in dem Datenspeicherabschnitt 7b. Der CDN-Verkäuferauswahlabschnitt 7a meldet dem Kampagnenmeldungserzeugungsabschnitt 7c die Auswahlmeldung (A2017).

(20-3) Prozess des
Fortschrittsinformationsverwaltungsabschnittes 7g
(siehe Figur 222)

[0305] Der Fortschrittsinformationsverwaltungsabschnitt 7g speichert einen Vorhersagewert, der angibt, wie viele Kampagnen an das fahrzeugseitige System 3 in einer vorbestimmten Periode verteilt werden. Es wird angenommen, dass dieser Vorhersagewert entsprechend dem tatsächlichen Verteilungsstatus, der von dem OEM-Server übertragen wird, aktualisiert wird.

[0306] Der Fortschrittsinformationsverwaltungsabschnitt 7g beschafft den Verteilungsstatus von dem OEM-Server (A20111). Der Fortschrittsinformationsverwaltungsabschnitt 7g bestimmt, ob die Differenz zwischen dem Verteilungsstatus und dem gespeicherten Vorhersagewert gleich oder größer als ein vorbestimmter Wert ist (A20112). Wenn bestimmt wird, dass die Differenz zwischen dem Verteilungsstatus und dem gespeicherten Vorhersagewert kleiner als der vorbestimmte Wert ist (A20112: nein), beendet der Fortschrittsinformationsverwaltungsabschnitt 7g den Prozess.

[0307] Wenn bestimmt wird, dass die Differenz zwischen dem Verteilungsstatus und dem gespeicherten Vorhersagewert gleich oder größer als der vorbestimmte Wert ist (A20112: ja), aktualisiert der Fortschrittsinformationsverwaltungsabschnitt 7g den gespeicherten Vorhersagewert (A20113) und meldet dem CDN-Verkäuferauswahlabschnitt 7a die Aktuali-

sierung des Vorhersagewertes (A20114). Der Fortschrittsinformationsverwaltungsabschnittes 7g kann einen einzigen Vorhersagewert aufweisen, der allen Kampagnen gemeinsam ist, oder kann unterschiedliche Vorhersagewerte für die jeweiligen Kampagnen, die jeweiligen zu aktualisierenden Fahrzeuge und die jeweiligen Typen von Kampagnen aufweisen.

(20-4) Prozess des CDN-Verkäuferauswahlabschnittes 7a (siehe Figur 223)

[0308] Wenn die Aktualisierung des Vorhersagewertes, die von dem Fortschrittsinformationsverwaltungsabschnitt 7g gemeldet wird, beschafft wurde (A20121), beschafft der CDN-Verkäuferauswahlabschnitt 7a die Auswahlinformationen (A20122), beschafft den Verteilungsvorhersagewert von dem Fortschrittsinformationsverwaltungsabschnitt 7g (A20123) und berechnet die Verteilungsdatengröße für jede Kampagne (A20124). Wenn in diesem Fall die Verteilungsdatengröße berechnet wird, stellt der CDN-Verkäuferauswahlabschnitt 7a den Korrekturwert unter Berücksichtigung der Anzahl der Verteilungstage ein.

[0309] Der CDN-Verkäuferauswahlabschnitt 7a schreitet zu dem zweiten CDN-Auswahlprozess (A20125), und wenn der zweite CDN-Auswahlprozess beendet ist, bestimmt der CDN-Verkäuferauswahlabschnitt 7a, ob es eine Änderung des CDN-Verkäufers gibt (A20126). Wenn bestimmt wird, dass es keine Änderung des CDN-Verkäufers gibt (A20126: nein), beendet der CDN-Verkäuferauswahlabschnitt 7a den Prozess. Wenn es eine Änderung des CDN-Verkäufers gibt, wird das Auswahlergebnis in dem Datenspeicherabschnitt 7b aktualisiert. Wenn bestimmt wird, dass es keine Änderung des CDN-Verkäufers gibt (A20126: ja), aktualisiert der CDN-Verkäuferauswahlabschnitt 7a das Auswahlergebnis (A20127), um eine CDN-Änderungsmeldung an den Kampagnenmeldungserzeugungsabschnitt 7c zu übertragen (A20128). Der CDN-Verkäuferauswahlabschnitt 7a kann in vorbestimmten Intervallen überprüfen, ob der Vorhersagewert, der in dem Fortschrittsinformationsverwaltungsabschnitt 7g gespeichert ist, sich geändert hat.

(20-5) Prozess des Kampagnenmeldungserzeugungsabschnittes 7c (siehe Figur 224)

[0310] Wenn die CDN-Änderungsmeldung, die von dem CDN-Verkäuferauswahlabschnitt 7a gemeldet wird, beschafft wurde (A20131), greift der Kampagnenmeldungserzeugungsabschnitt 7c auf den Datenspeicherabschnitt 7b zu, beschafft aktualisierte CDN-Verkäuferinformationen (A20132) und erzeugt die Kampagnenmeldung, deren Verteilung geplant

ist, neu auf der Grundlage der beschafften aktualisierten CDN-Verkäuferinformationen (A20133).

[0311] Wie es oben beschrieben ist, können gemäß der zwölften Ausführungsform die folgenden vorteilhaften Wirkungen erzielt werden.

[0312] Durch Bezugnahme auf die CDN-Verkäuferverwaltungsdatenbank wird das CDN 8, das überlegene Verteilungskosten aufweist, aus mehreren CDN 8, die unterschiedliche Verteilungskosten aufweisen, entsprechend dem Verteilungsverfahren, dem OTA-Zielbereich und der Verteilungsdatengröße ausgewählt, und das Aktualisierungspaket wird in dem ausgewählten CDN 8 platziert. Es ist möglich, die Verteilungskosten geeignet zu verringern, wenn der OTA-Master 4 das Aktualisierungspaket von dem OTA-Zentrum 2 herunterlädt.

Weitere Ausführungsformen

[0313] In der obigen Ausführungsform kann eine Ausführungsform, die nicht für das Streaming-Verfahren oder das Speicherverfahren spezifiziert ist, sowohl für das Streaming-Verfahren als auch für das Speicherverfahren verwendet werden.

[0314] In einigen der oben beschriebenen Ausführungsformen ist beschrieben, dass die Kampagnenmeldung von dem OTA-Zentrum 2 an den OTA-Master 4 übertragen wird, nachdem die TLS-Kommunikation errichtet ist. In allen Ausführungsformen kann jedoch die Kampagnenmeldung von dem OTA-Zentrum 2 an den OTA-Master 4 übertragen werden, nachdem die TLS-Kommunikation errichtet wurde. Durch Errichten der TLS-Kommunikation kann die Sicherheit weiter erhöht werden. Alternativ kann die Kampagnenmeldung von dem OTA-Zentrum 2 an den OTA-Master 4 ohne Errichtung einer TLS-Kommunikation übertragen werden.

[0315] Das fahrzeugseitige System 3 der vorliegenden Ausführungsform kann die folgende Konfiguration aufweisen. Das fahrzeugseitige System 3 kann ein Datenkommunikationsmodul (DCM) und ein zentrales Gateway (CGW) aufweisen, und das DCM und das CGW können zum Datenaustausch kommunizierbar über einen Bus verbunden sein. Das CGW wird auch als zentrale ECU bezeichnet. Der Bus kann beispielsweise ein Ethernet, ein CAN (eingetragene Marke) oder Ähnliches sein.

[0316] Einige oder alle Funktionen des OTA-Masters 4 können in dem CGW implementiert sein. Gemäß einem Beispiel kann das DCM eine Datenkommunikation mit der Außenseite wie beispielsweise dem CDN 8 und dem OTA-Zentrum 2 durchführen, und alle Funktionen des OTA-Masters 4 können in dem CGW implementiert sein. In diesem Fall überträgt das DCM alle Daten, die durch draht-

lose Kommunikation mit der Außenseite empfangen werden, an das CGW. Alternativ kann das DCM zusätzlich zu der Durchführung der Datenkommunikation mit der Außenseite als eine Herunterladeeinrichtung des OTA-Masters 4 dienen. Die Funktionen der Herunterladeeinrichtung sind beispielsweise die Erzeugung von Fahrzeugkonfigurationsinformationen, eine Verifizierung von Metadaten, eine Verifizierung eines Paketes und eine Verifizierung von Kampagneninformationen. Alternativ kann die Funktion des OTA-Masters 4 in dem DCM implementiert sein. In diesem Fall werden Funktionen, die nicht in dem OTA-Master 4 implementiert werden, in dem CGW implementiert. Alternativ können das DCM und das CGW integriert sein.

[0317] Das CGW kann einige oder alle Funktionen des DCM aufweisen, oder das DCM kann einige oder alle Funktionen des CGW aufweisen. D.h., in dem OTA-Master 4 kann die Funktion, die von dem DCM und dem CGW gemeinsam verwendet wird, auf beliebige Weise ausgebildet sein. Der OTA-Master 4 kann die ECUs des DCM und des CGW enthalten oder kann eine integrierte ECU enthalten, die eine Funktion des DCM als auch eine Funktion des CGW aufweist.

[0318] Auch wenn die vorliegende Erfindung anhand ihrer Ausführungsformen beschrieben wurde, ist es selbstverständlich, dass die vorliegende Erfindung nicht auf die obigen Ausführungsformen und Strukturen beschränkt ist. Die vorliegende Erfindung kann verschiedene Modifikationsbeispiele und Modifikationen innerhalb des Äquivalenzbereiches enthalten. Zusätzlich zu den obigen sind weitere Kombinationen und Modi einschließlich nur einem Element, mehr Elementen oder weniger Elementen innerhalb des Bereiches der vorliegenden Erfindung möglich.

[0319] Die Einrichtungen und Funktionen, die durch eine jeweilige Vorrichtung bereitgestellt werden, können durch Software, die im Wesentlichen in einer Speichervorrichtung aufgezeichnet ist, und einen Computer, der die Software ausführt, nur durch Software, nur durch Hardware oder eine Kombination aus diesen bereitgestellt werden. Wenn beispielsweise der Steuerungsabschnitt durch eine elektronische Schaltung, die eine Hardware ist, bereitgestellt wird, kann der Steuerungsabschnitt durch eine digitale Schaltung bereitgestellt werden, die eine große Anzahl von Logikschaltkreisen enthält, oder durch einen analogen Schaltkreis.

[0320] Der Steuerungsabschnitt und dessen Verfahren, die hier beschrieben sind, können durch einen zugehörigen Computer realisiert werden, der durch Konfigurieren eines Prozessors, der programmiert ist, eine oder mehrere Funktionen auszuführen, die durch ein Computerprogramm ausgeführt werden,

und eines Speichers gebildet wird. Alternativ können der Steuerungsabschnitt und dessen Verfahren, die hier beschrieben sind, durch einen zugehörigen Computer realisiert werden, der durch Konfigurieren eines Prozessors durch eine oder mehrere zugehörige Hardwarelogikschaltkreise konfiguriert wird. Alternativ können der Steuerungsabschnitt und dessen Verfahren, die hier beschrieben sind, durch einen oder mehrere zugehörige Computer realisiert werden, die durch eine Kombination aus einem Prozessor, der programmiert ist, eine oder mehrere Funktionen auszuführen, und einem Speicher sowie einem Prozessor, der durch eine oder mehrere Hardwarelogikschaltungen konfiguriert wird, gebildet werden. Außerdem kann das Computerprogramm in einem computerlesbaren nichtflüchtigen dinglichen Aufzeichnungsmedium als von einem Computer auszuführende Anweisungen gespeichert sein.

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 2021161212 [0001]
- JP 2020276424 A [0004]

Patentansprüche

1. Datenkommunikationssystem, das aufweist: eine Zentrumsvorrichtung (2), die Aktualisierungsdaten an eine Mastervorrichtung verteilt; und eine Mastervorrichtung (4), die die Aktualisierungsdaten, die von der Zentrumsvorrichtung heruntergeladen wurden, in einer neu zu programmierenden elektronischen Steuerungseinheit installiert, wobei die Zentrumsvorrichtung und die Mastervorrichtung einen Zählermodus (CTR) als ein Verschlüsselungsverfahren und ein Entschlüsselungsverfahren der Aktualisierungsdaten verwenden.

2. Datenkommunikationssystem nach Anspruch 1, wobei die Mastervorrichtung einen Entschlüsselungsprozess der Aktualisierungsdaten parallel ausführt.

3. Datenkommunikationssystem nach Anspruch 1 oder 2, wobei die Zentrumsvorrichtung und die Mastervorrichtung eine Nonce in einen Zähler einfügen.

4. Datenkommunikationssystem, das aufweist: eine Zentrumsvorrichtung (2), die Aktualisierungsdaten an eine Mastervorrichtung verteilt; und eine Mastervorrichtung (4), die die Aktualisierungsdaten, die von der Zentrumsvorrichtung heruntergeladen wurden, in einer neu zu programmierenden elektronischen Steuerungseinheit installiert, wobei die Zentrumsvorrichtung und die Mastervorrichtung einen Ausgangsrückführungsmodus (OFB) als ein Verschlüsselungsverfahren und ein Entschlüsselungsverfahren der Aktualisierungsdaten verwenden.

5. Datenkommunikationssystem nach einem der Ansprüche 1 bis 4, wobei die Mastervorrichtung eine Vorbereitung für einen Entschlüsselungsprozess der Aktualisierungsdaten im Hintergrund separat von einem Herunterladen der Aktualisierungsdaten von der Zentrumsvorrichtung startet.

6. Datenkommunikationssystem nach Anspruch 5, wobei die Mastervorrichtung die Vorbereitung für den Entschlüsselungsprozess der Aktualisierungsdaten im Hintergrund zu einem Zeitpunkt startet, zu dem eine Kampagnenmeldung, die von der Zentrumsvorrichtung übertragen wird, empfangen wird.

7. Datenkommunikationssystem nach Anspruch 5 oder 6, wobei die Mastervorrichtung die Vorbereitung für den Entschlüsselungsprozess der Aktualisierungsdaten im Hintergrund startet, bevor eine Herunterladebewilligung von einem Nutzer erhalten wird.

8. Datenkommunikationssystem nach einem der Ansprüche 5 bis 7, wobei die Mastervorrichtung alle

Schlüsselströme als Vorbereitung für den Entschlüsselungsprozess der Aktualisierungsdaten berechnet.

9. Datenkommunikationssystem nach einem der Ansprüche 5 bis 7, wobei die Mastervorrichtung einige Schlüsselströme als Vorbereitung für den Entschlüsselungsprozess der Aktualisierungsdaten berechnet.

10. Datenkommunikationssystem nach einem der Ansprüche 1 bis 9, wobei die Zentrumsvorrichtung einen Schlüssel, der für eine spezielle Fahrzeuggruppe individualisiert ist, als einen Verschlüsselungsschlüssel verwendet.

11. Datenkommunikationssystem nach einem der Ansprüche 1 bis 10, wobei die Zentrumsvorrichtung und die Mastervorrichtung einen Schlüsselaktualisierungsschlüssel zur Aktualisierung eines geheimen Schlüssels halten, und die Zentrumsvorrichtung ein Geheimer-Schlüssel-Aktualisierungspaket unter Verwendung des Schlüsselaktualisierungsschlüssels erzeugt, um das erzeugte Geheimer-Schlüssel-Aktualisierungspaket an die Mastervorrichtung zu übertragen.

12. Datenkommunikationssystem nach einem der Ansprüche 1 bis 11, wobei die Zentrumsvorrichtung und die Mastervorrichtung einen Chiffrierungsblockkettenmodus (CBC) als einen Nachrichtenauthentifizierungscode (MAC) verwenden.

13. Datenkommunikationssystem nach einem der Ansprüche 1 bis 11, wobei die Zentrumsvorrichtung und die Mastervorrichtung einen Modus eines Galois-Nachrichtenauthentifizierungscodes (GMAC) als einen Nachrichtenauthentifizierungscode (MAC) verwenden.

14. Datenkommunikationssystem nach Anspruch 12 oder 13, wobei die Zentrumsvorrichtung und die Mastervorrichtung eine Datengrößeneinheit, der der Nachrichtenauthentifizierungscode zugewiesen ist, gegenseitig erkennen.

15. Datenkommunikationssystem nach einem der Ansprüche 1 bis 14, wobei die Zentrumsvorrichtung ein Verschlüsselungsverfahren in Neuprogrammierungs-Konzept-Metadaten und/oder Herunterlade-Metadaten einfügt, um das Verschlüsselungsverfahren an die Mastervorrichtung zu übertragen.

16. Zentrumsvorrichtung (2), die Aktualisierungsdaten an eine Mastervorrichtung verteilt, wobei die Zentrumsvorrichtung aufweist: einen Gemeinsamer-Schlüssel-Erzeugungsabschnitt (2a), der einen gemeinsamen Schlüssel zur Verschlüsselung von Aktualisierungsdaten erzeugt;

einen Aktualisierungsdatenverschlüsselungsabschnitt (2b), der die Aktualisierungsdaten mit dem gemeinsamen Schlüssel in einem Zählermodus (CTR) verschlüsselt;
 einen Gemeinsamer-Schlüssel-Verschlüsselungsabschnitt (2c), der den gemeinsamen Schlüssel mit einem öffentlichen RSA-Schlüssel verschlüsselt;
 einen Gemeinsamer-Schlüssel-Speicherabschnitt (2d), der den gemeinsamen Schlüssel, der mit dem öffentlichen RSA-Schlüssel verschlüsselt ist, in einer Kampagnenmeldung speichert;
 einen Verschlüsselungsdatenplatzierungsabschnitt (2e), der die Aktualisierungsdaten, die mit dem gemeinsamen Schlüssel verschlüsselt sind, in einem Inhaltsliefernetzwerk (CDN) platziert; und
 einen Kampagnenmeldungsübertragungsabschnitt (2f), der eine Kampagnenmeldung, in der der verschlüsselte gemeinsame Schlüssel gespeichert ist, an ein neu zu programmierendes fahrzeugseitiges System überträgt.

17. Zentrumsvorrichtung (2), die Aktualisierungsdaten an eine Mastervorrichtung verteilt, wobei die Zentrumsvorrichtung aufweist:

einen Gemeinsamer-Schlüssel-Erzeugungsabschnitt (2a), der einen gemeinsamen Schlüssel zur Verschlüsselung von Aktualisierungsdaten erzeugt;
 einen Aktualisierungsdatenverschlüsselungsabschnitt (2b), der die Aktualisierungsdaten mit dem gemeinsamen Schlüssel in einem Ausgangsrückführungsmodus (OFB) verschlüsselt;
 einen Gemeinsamer-Schlüssel-Verschlüsselungsabschnitt (2c), der den gemeinsamen Schlüssel mit einem öffentlichen RSA-Schlüssel verschlüsselt;
 einen Gemeinsamer-Schlüssel-Speicherabschnitt (2d), der den gemeinsamen Schlüssel, der mit dem öffentlichen RSA-Schlüssel verschlüsselt ist, in einer Kampagnenmeldung speichert;
 einen Verschlüsselungsdatenplatzierungsabschnitt (2e), der die Aktualisierungsdaten, die mit dem gemeinsamen Schlüssel verschlüsselt sind, in einem Inhaltsliefernetzwerk (CDN) platziert; und
 einen Kampagnenmeldungsübertragungsabschnitt (2f), der eine Kampagnenmeldung, in der der verschlüsselte gemeinsame Schlüssel gespeichert ist, an ein neu zu programmierendes fahrzeugseitiges System überträgt.

18. Mastervorrichtung (4), die Aktualisierungsdaten, die von einer Zentrumsvorrichtung heruntergeladen werden, in einer neu zu programmierenden elektronischen Steuerungseinheit installiert, wobei die Mastervorrichtung (4) aufweist:

einen Gemeinsamer-Schlüssel-Beschaffungsabschnitt (4a), der einen gemeinsamen Schlüssel aus Kampagnenmeldungen, die von einer Zentrumsvorrichtung beschafft werden, beschafft;
 einen Gemeinsamer-Schlüssel-Entschlüsselungsabschnitt (4b), der den verschlüsselten gemeinsamen Schlüssel mit einem geheimen RSA-Schlüssel

entschlüsselt, um den gemeinsamen Schlüssel zu extrahieren;
 einen Verschlüsselungsdatenbeschaffungsabschnitt (4c), der verschlüsselte Aktualisierungsdaten von einem Inhaltsliefernetzwerk (CDN) herunterlädt und beschafft;
 einen Blockverschlüsselungsverarbeitungsabschnitt (4d), der einen Zählerwert durch Ausführen eines AES-Blockverschlüsselungsprozesses des Zählerwertes mit einem AES-Schlüssel parallel zu dem Herunterladen und Beschaffen der verschlüsselten Aktualisierungsdaten von dem CDN durch den Verschlüsselungsdatenbeschaffungsabschnitt verschlüsselt;
 einen Verschlüsselungsdatenentschlüsselungsabschnitt (4e), der eine Ausschließlich-Oder-Operation des verschlüsselten Zählerwertes und der verschlüsselten Aktualisierungsdaten, die von dem CDN heruntergeladen wurden, durchführt, um den verschlüsselten Zählerwert und die verschlüsselten Aktualisierungsdaten zu entschlüsseln; und
 einen Installationsverarbeitungsabschnitt (4f), der die entschlüsselten Aktualisierungsdaten an die neu zu programmierende elektronische Steuerungseinheit überträgt und die Aktualisierungsdaten in der elektronischen Steuerungseinheit installiert.

19. Mastervorrichtung (4), die Aktualisierungsdaten, die von einer Zentrumsvorrichtung heruntergeladen werden, in einer neu zu programmierenden elektronischen Steuerungseinheit installiert, wobei die Mastervorrichtung (4) aufweist:

einen Gemeinsamer-Schlüssel-Beschaffungsabschnitt (4), der einen gemeinsamen Schlüssel aus Kampagnenmeldungen, die von einer Zentrumsvorrichtung beschafft werden, beschafft;
 einen Gemeinsamer-Schlüssel-Entschlüsselungsabschnitt (4b), der den verschlüsselten gemeinsamen Schlüssel mit einem geheimen RSA-Schlüssel entschlüsselt, um den gemeinsamen Schlüssel zu extrahieren;
 einen Verschlüsselungsdatenbeschaffungsabschnitt (4c), der verschlüsselte Aktualisierungsdaten von einem Inhaltsliefernetzwerk (CDN) herunterlädt und beschafft;
 einen Blockverschlüsselungsverarbeitungsabschnitt (4d), der einen IV-Wert durch Ausführen eines IV-Wert-basierten gemeinsamen Stromverschlüsselungsprozesses mit einem AES-Schlüssel parallel zu dem Herunterladen und Beschaffen der verschlüsselten Aktualisierungsdaten von dem CDN durch den Verschlüsselungsdatenbeschaffungsabschnitt verschlüsselt;
 einen Verschlüsselungsdatenentschlüsselungsabschnitt (4e) der eine Ausschließlich-Oder-Operation des verschlüsselten IV-Wertes und der verschlüsselten Aktualisierungsdaten, die von dem CDN heruntergeladen wurden, durchführt, um den verschlüsselten IV-Wert und die verschlüsselten Aktualisierungsdaten zu entschlüsseln; und

einen Installationsverarbeitungsabschnitt (4f), der die entschlüsselten Aktualisierungsdaten an die neu zu programmierende elektronische Steuerungseinheit überträgt und die Aktualisierungsdaten in der elektronischen Steuerungseinheit installiert.

20. Verschlüsselungsprogramm zum Bewirken, dass eine Zentrumsvorrichtung (2), die Aktualisierungsdaten an eine Mastervorrichtung verteilt, ausführt:

- einen Gemeinsamer-Schlüssel-Erzeugungsschritt zum Erzeugen eines gemeinsamen Schlüssels zum Verschlüsseln von Aktualisierungsdaten;
- einen Aktualisierungsdatenverschlüsselungsschritt zum Verschlüsseln der Aktualisierungsdaten mit dem gemeinsamen Schlüssel in einem Zählermodus (CTR);
- einen Gemeinsamer-Schlüssel-Verschlüsselungsschritt zum Verschlüsseln des gemeinsamen Schlüssels mit einem öffentlichen RSA-Schlüssel;
- einen Gemeinsamer-Schlüssel-Speicherschritt zum Speichern des gemeinsamen Schlüssels, der mit dem öffentlichen RSA-Schlüssel verschlüsselt ist, in einer Kampagnenmeldung;
- einen Verschlüsselungsdatenplatzierungsschritt zum Platzieren der Aktualisierungsdaten, die mit dem gemeinsamen Schlüssel verschlüsselt sind, in einem Inhaltsliefernetzwerk (CDN); und
- einen Kampagnenmeldungsübertragungsschritt zum Übertragen einer Kampagnenmeldung, in der der verschlüsselte gemeinsame Schlüssel gespeichert ist, an ein neu zu programmierendes fahrzeugseitiges System.

21. Verschlüsselungsprogramm zum Bewirken, dass eine Zentrumsvorrichtung (2), die Aktualisierungsdaten an eine Mastervorrichtung verteilt, ausführt:

- einen Gemeinsamer-Schlüssel-Erzeugungsschritt zum Erzeugen eines gemeinsamen Schlüssels zum Verschlüsseln von Aktualisierungsdaten;
- einen Aktualisierungsdatenverschlüsselungsschritt zum Verschlüsseln der Aktualisierungsdaten mit dem gemeinsamen Schlüssel in einem Ausgangsrückführungsmodus (OFB);
- einen Gemeinsamer-Schlüssel-Verschlüsselungsschritt zum Verschlüsseln des gemeinsamen Schlüssels mit einem öffentlichen RSA-Schlüssel;
- einen Gemeinsamer-Schlüssel-Speicherschritt zum Speichern des gemeinsamen Schlüssels, der mit dem öffentlichen RSA-Schlüssel verschlüsselt ist, in einer Kampagnenmeldung;
- einen Verschlüsselungsdatenplatzierungsschritt zum Platzieren der Aktualisierungsdaten, die mit dem gemeinsamen Schlüssel verschlüsselt sind, in einem Inhaltsliefernetzwerk (CDN); und
- einen Kampagnenmeldungsübertragungsschritt zum Übertragen einer Kampagnenmeldung, in der der verschlüsselte gemeinsame Schlüssel gespeichert

ist, an ein neu zu programmierendes fahrzeugseitiges System.

22. Entschlüsselungsprogramm zum Bewirken, dass eine Mastervorrichtung (4), die Aktualisierungsdaten, die von einer Zentrumsvorrichtung heruntergeladen werden, in einer neu zu programmierenden elektronischen Steuerungseinheit installiert, ausführt:

- einen Gemeinsamer-Schlüssel-Beschaffungsschritt zum Beschaffen eines gemeinsamen Schlüssels aus Kampagnenmeldungen, die von einer Zentrumsvorrichtung beschafft werden;
- einen Gemeinsamer-Schlüssel-Entschlüsselungsschritt zum Entschlüsseln des verschlüsselten gemeinsamen Schlüssels mit einem geheimen RSA-Schlüssel, um den gemeinsamen Schlüssel zu extrahieren;
- einen Verschlüsselungsdatenbeschaffungsschritt zum Herunterladen und Beschaffen von verschlüsselten Aktualisierungsdaten von einem Inhaltsliefernetzwerk (CDN);
- einen Blockverschlüsselungsverarbeitungsschritt zum Verschlüsseln eines Zählerwertes durch Ausführen eines AES-Blockverschlüsselungsprozesses des Zählerwertes mit einem AES-Schlüssel parallel zu dem Herunterladen und Beschaffen der verschlüsselten Aktualisierungsdaten von dem CDN durch den Verschlüsselungsdatenbeschaffungsschritt;
- einen Verschlüsselungsdatenentschlüsselungsschritt zum Durchführen einer Ausschließlich-Oder-Operation des verschlüsselten Zählerwertes und der verschlüsselten Aktualisierungsdaten, die von dem CDN heruntergeladen wurden, um den verschlüsselten Zählerwert und die verschlüsselten Aktualisierungsdaten zu entschlüsseln; und
- einen Installationsverarbeitungsschritt zum Übertragen der entschlüsselten Aktualisierungsdaten an die neu zu programmierende elektronische Steuerungseinheit und zum Installieren der Aktualisierungsdaten in der elektronischen Steuerungseinheit.

23. Entschlüsselungsprogramm zum Bewirken, dass eine Mastervorrichtung (4), die Aktualisierungsdaten, die von einer Zentrumsvorrichtung heruntergeladen werden, in einer neu zu programmierenden elektronischen Steuerungseinheit installiert, ausführt:

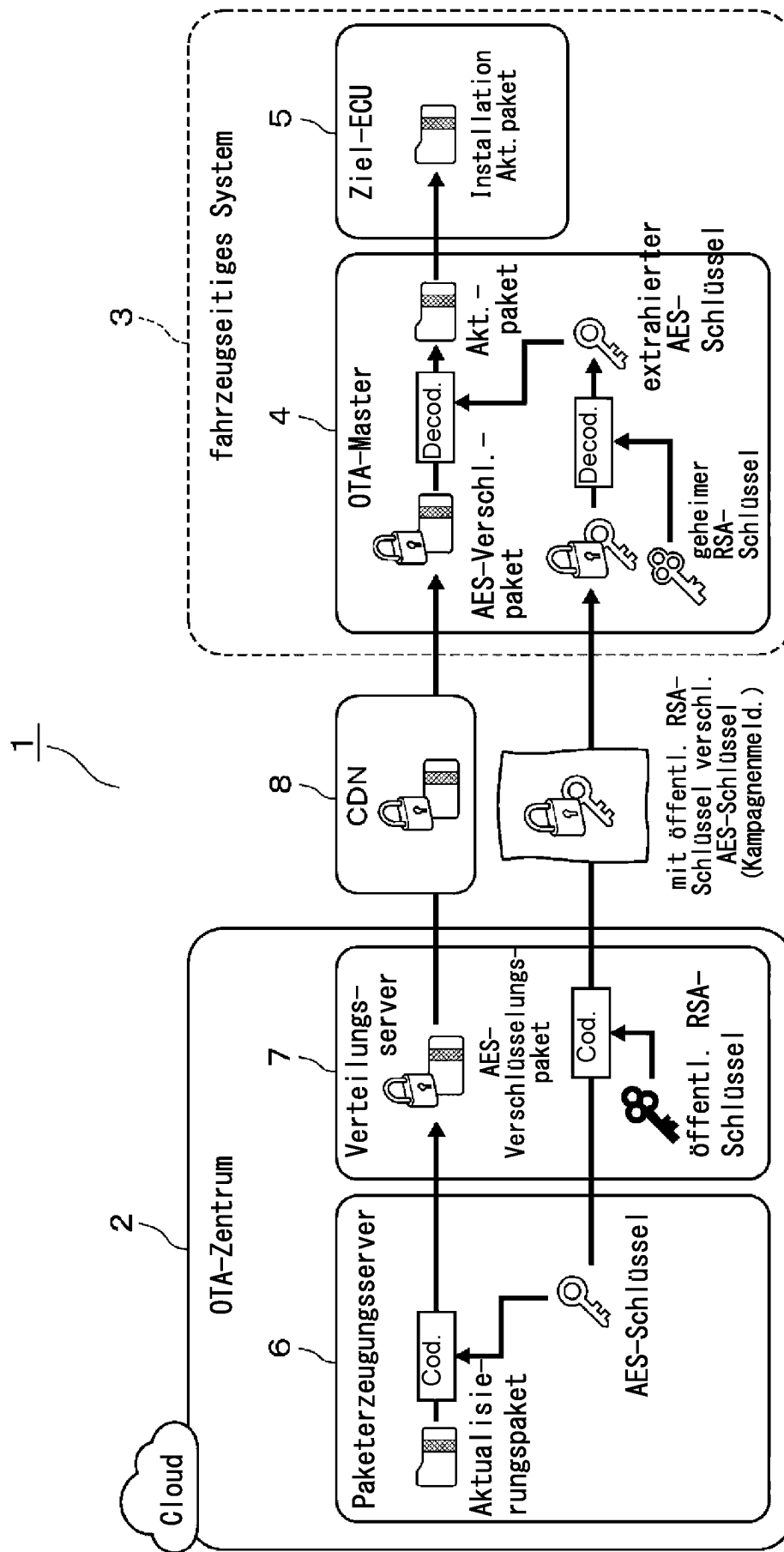
- einen Gemeinsamer-Schlüssel-Beschaffungsschritt zum Beschaffen eines gemeinsamen Schlüssels aus Kampagnenmeldungen, die von einer Zentrumsvorrichtung beschafft werden;
- einen Gemeinsamer-Schlüssel-Entschlüsselungsschritt zum Entschlüsseln des verschlüsselten gemeinsamen Schlüssels mit einem öffentlichen RSA-Schlüssel, um den gemeinsamen Schlüssel zu extrahieren;
- einen Verschlüsselungsdatenbeschaffungsschritt zum Herunterladen und Beschaffen von verschlüsselten

selten Aktualisierungsdaten von einem Inhaltsliefer-
netzwerk (CDN);
einen Blockverschlüsselungsverarbeitungsschritt
zum Verschlüsseln eines IV-Wertes durch Ausfüh-
ren eines IV-Wert-basierten gemeinsamen Strom-
verschlüsselungsprozesses mit einem AES-Schlüs-
sel parallel zu dem Herunterladen und Beschaffen
der verschlüsselten Aktualisierungsdaten von dem
CDN durch den Verschlüsselungsdatenbeschaf-
fungsschritt;
einen Verschlüsselungsdatenentschlüsselungs-
schritt zum Durchführen einer Ausschließlich-Oder-
Operation des verschlüsselten IV-Wertes und der
verschlüsselten Aktualisierungsdaten, die von dem
CDN heruntergeladen wurden, um den verschlüs-
selten IV-Wert und die verschlüsselten Aktualisie-
rungsdaten zu entschlüsseln; und
einen Installationsverarbeitungsschritt zum Übertra-
gen der entschlüsselten Aktualisierungsdaten an die
neu zu programmierende elektronische Steuerungs-
einheit und zum Installieren der Aktualisierungsda-
ten in der elektronischen Steuerungseinheit.

Es folgen 224 Seiten Zeichnungen

Anhängende Zeichnungen

FIG. 1



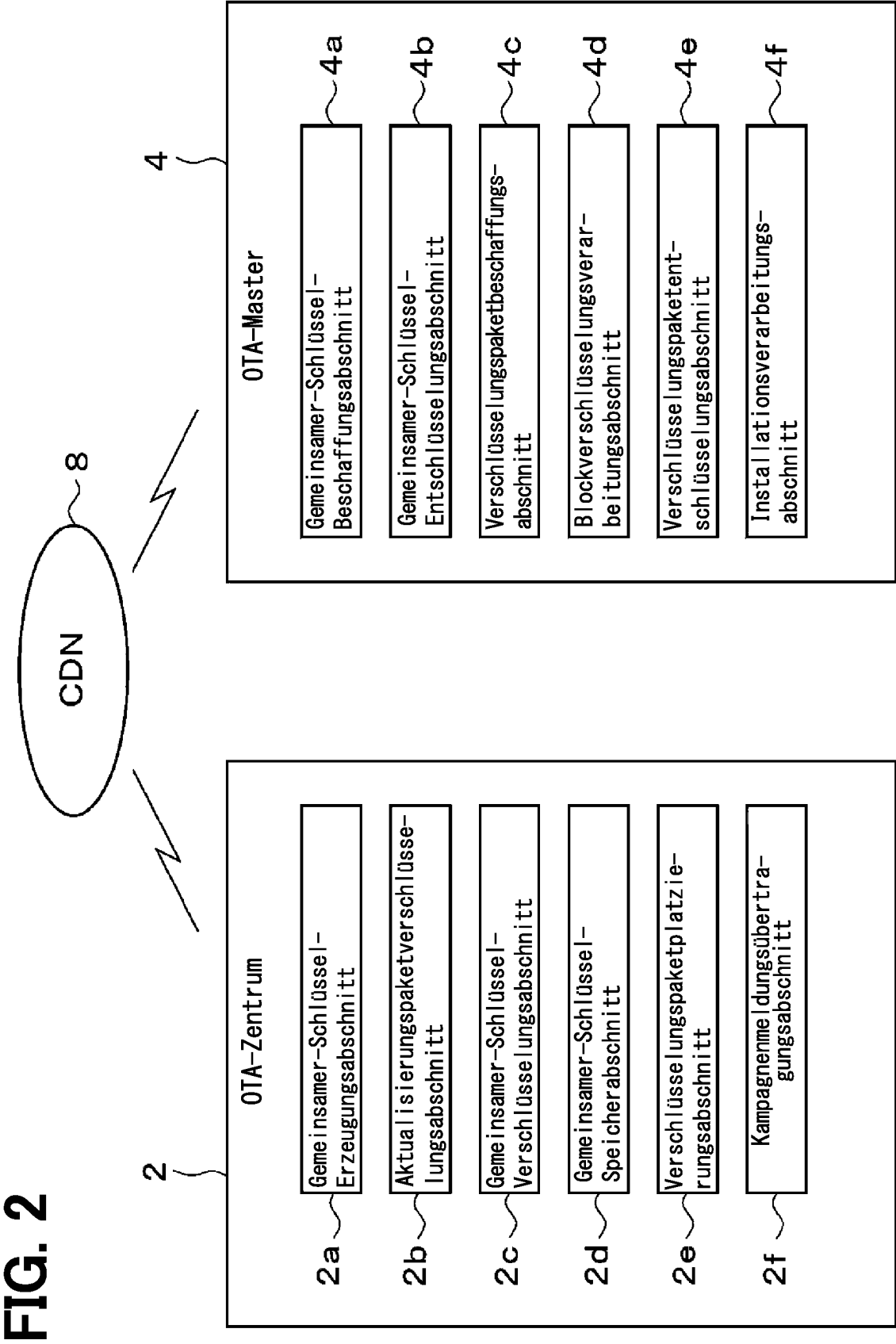


FIG. 3

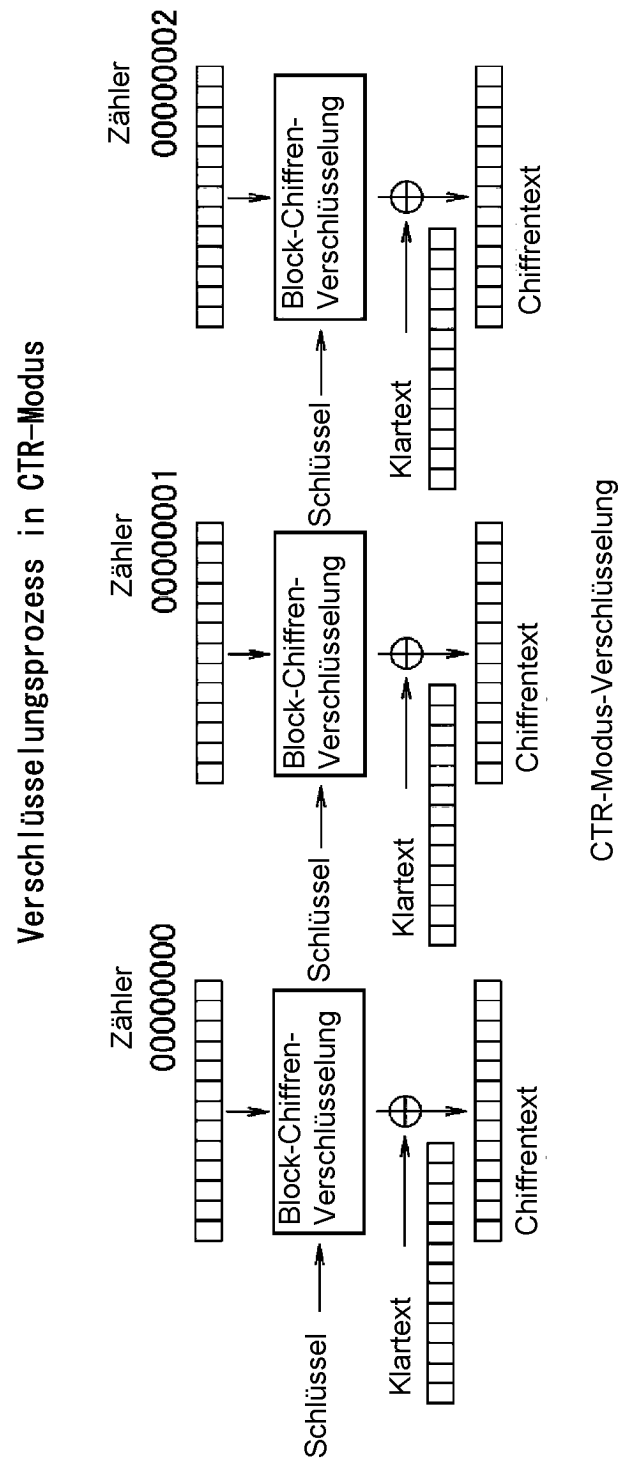


FIG. 4

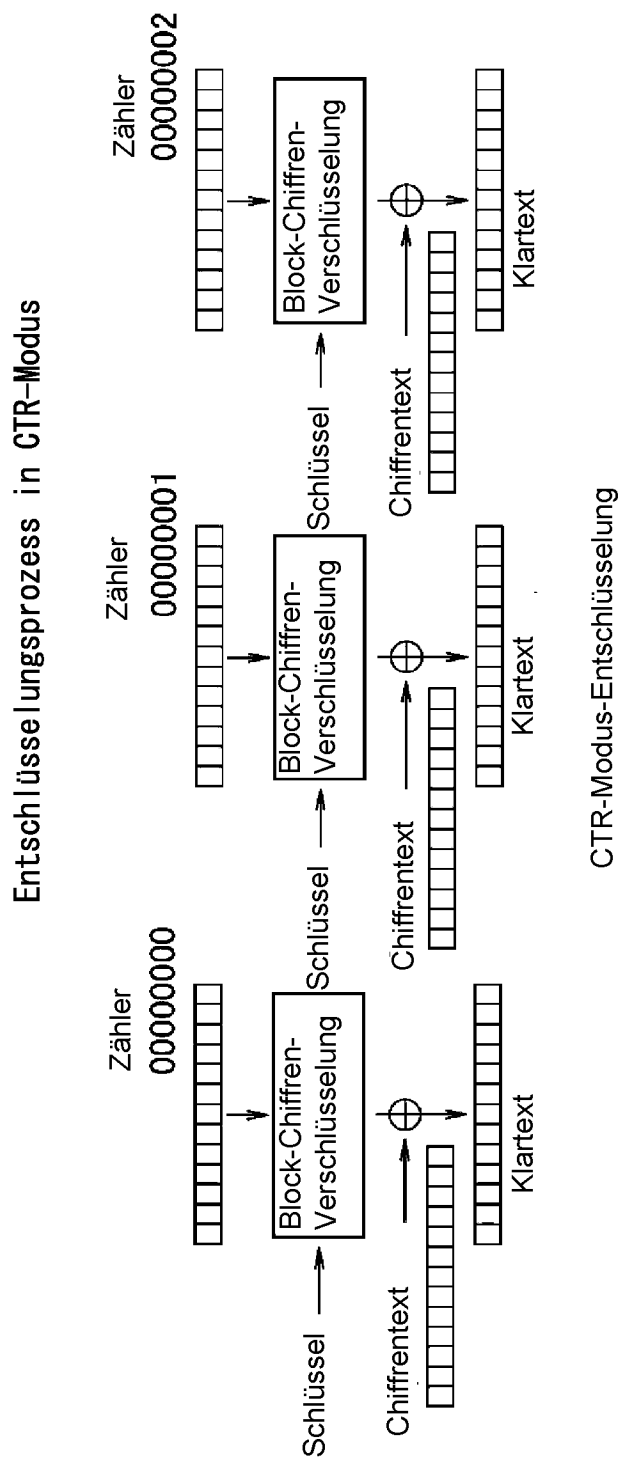


FIG. 5

	Name	Vorteile	Nachteile	Empfehlung
CBC-Modus	Chiffren-Block-Kettenbildung Chiffren-Block-Kettenmodus	• wiederholter Klartext wird nicht in Chiffrentext reflektiert, hohe Sicherheit	• Wenn Chiffrentext mit Fehler in Einheiten von Bits entschlüsselt wird, sind gesamter Block und nächstes entspr. Bit fehlerhaft (Fehlerstreuung). • Vorbereitung für Verschl. und Entschl. möglich • Paraller Prozess von Verschlüsselung nicht möglich	CRYPTOREC empfohlene Verschlüsselung
CTR-Modus	Zähler Zählermodus	• Vorbereitung für Verschl. und Entschl. möglich, so dass hohe Geschwindigkeit möglich • Paraller Prozess von Verschlüsselung und Entschlüsselung möglich • Entschlüsseln von Chiffrentext mit bitweisem Fehler liegt innerhalb von Fehler von nur entspr. Bit von Klartext	• Wenn aktiver Angreifer Bits von Chiffren-Block invertiert, werden Bits von entsprechendem Klartext-Block invertiert	CRYPTOREC empfohlene Verschlüsselung

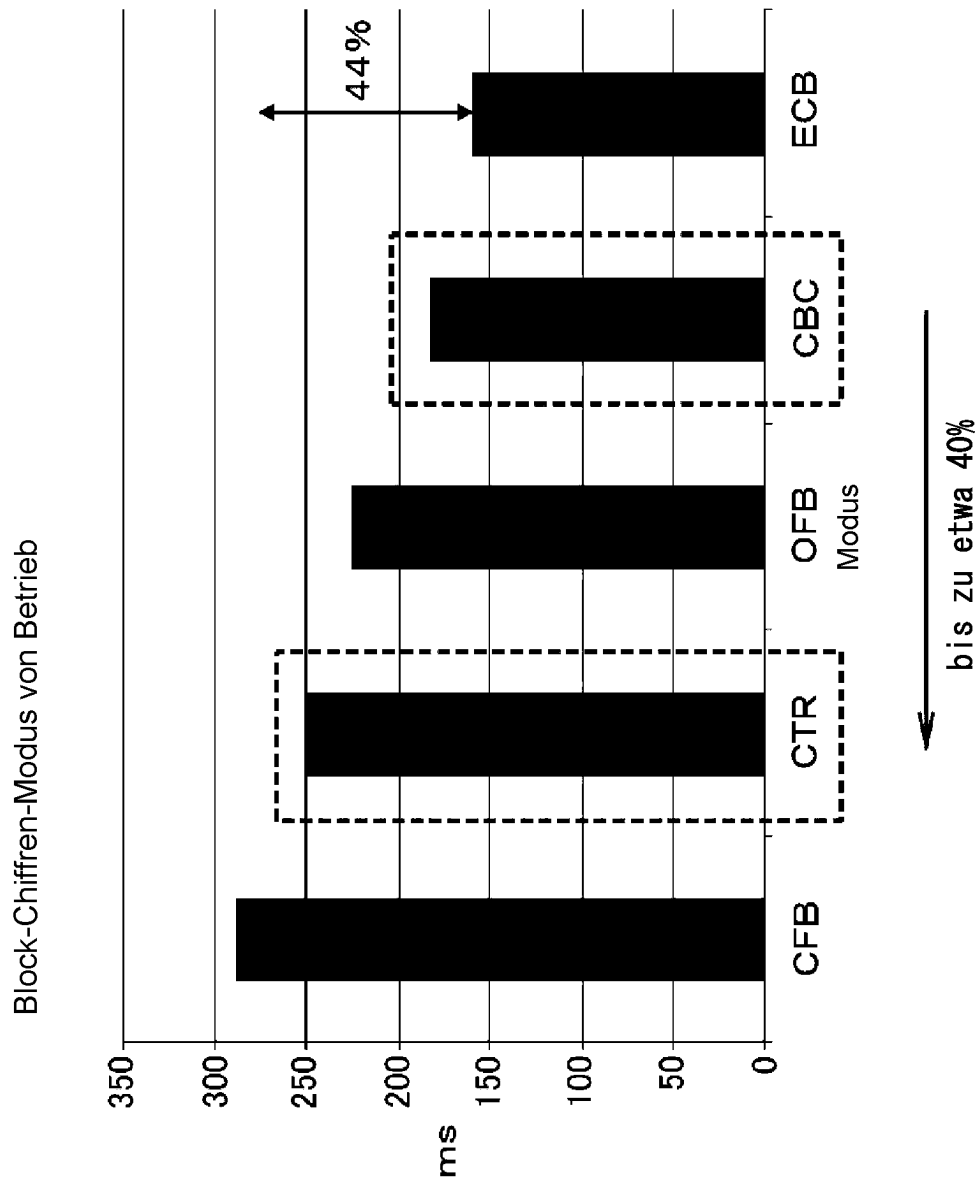
FIG. 6

FIG. 7

Da Chiffrentext eingegeben wird, kann Entschlüsselungsprozess nicht gestartet werden, bis Aktualisierungspaket als Chiffrentext empfangen wird

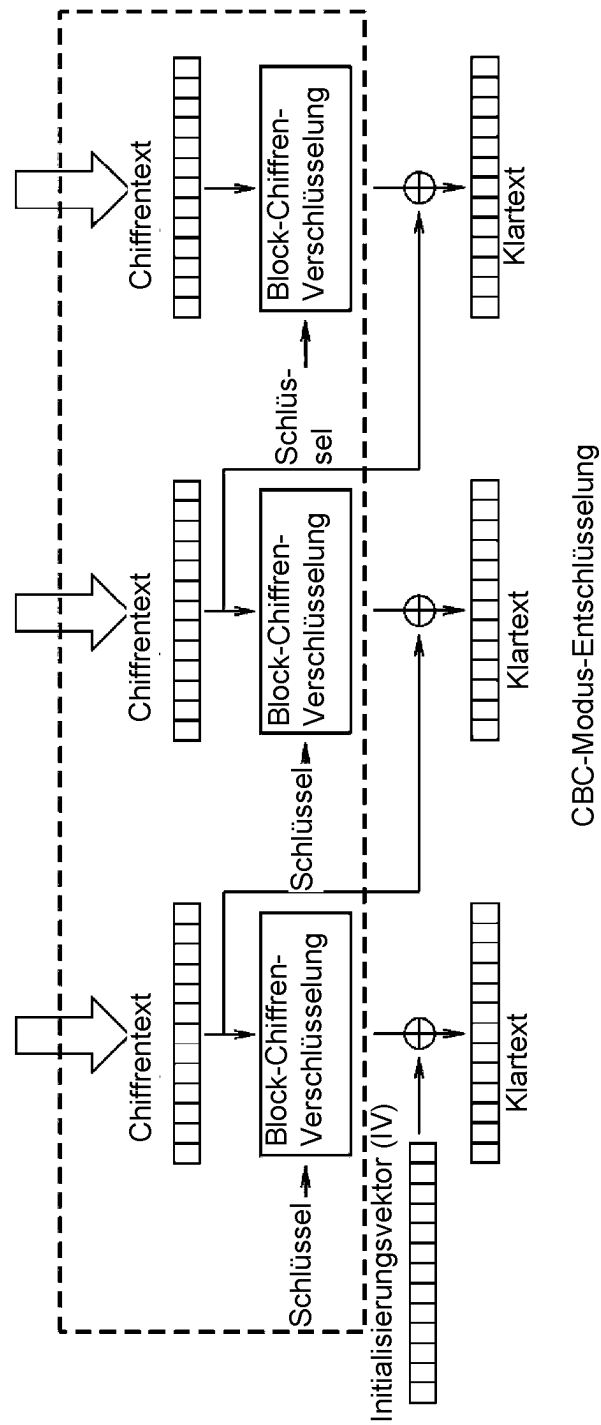
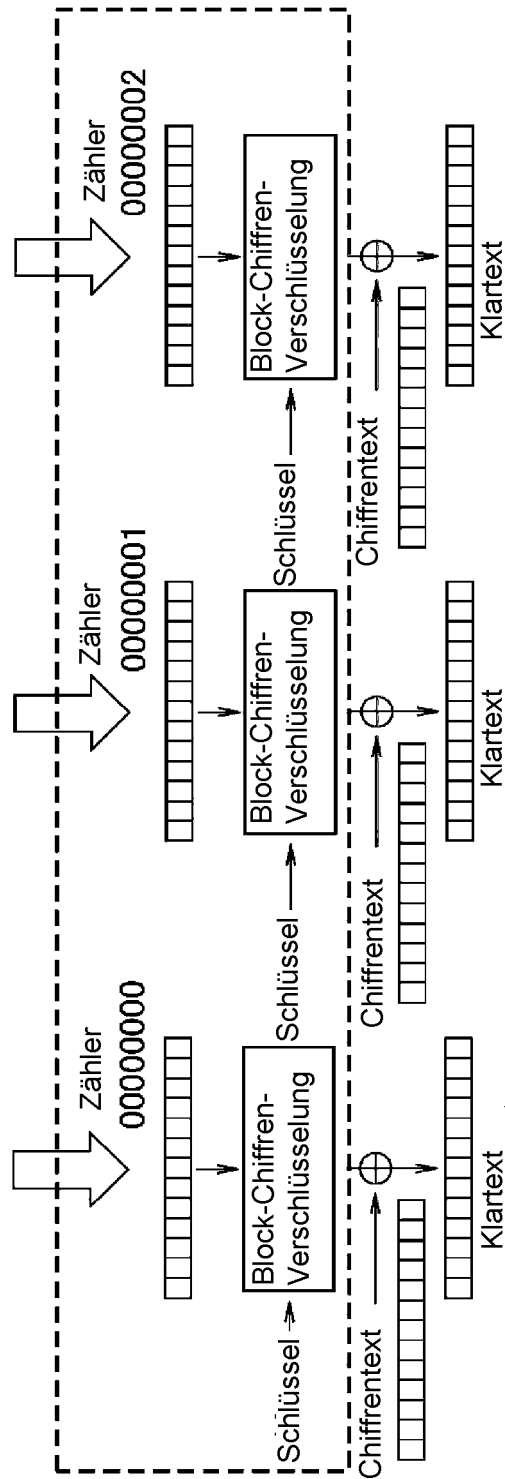


FIG. 8

Da Zählerwert eingegeben wird, kann Entschlüsselungsprozess vor Empfang von Aktualisierungspaket als Chiffrentext gestartet werden.
Da keine gegenseitige Abhängigkeit besteht, können mehrere kryptographische Betriebe gleichzeitig parallel ausgeführt werden



CTR-Modus-Entschlüsselung

FIG. 9

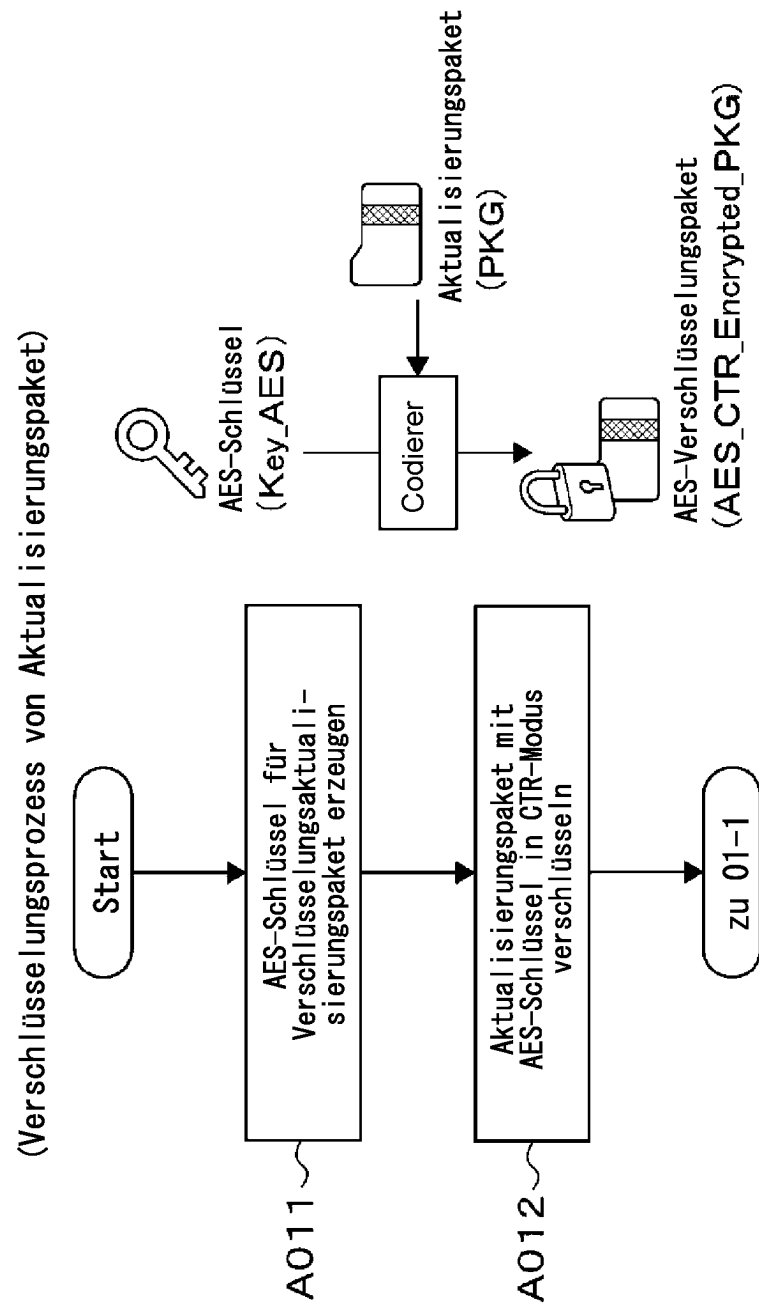


FIG. 10

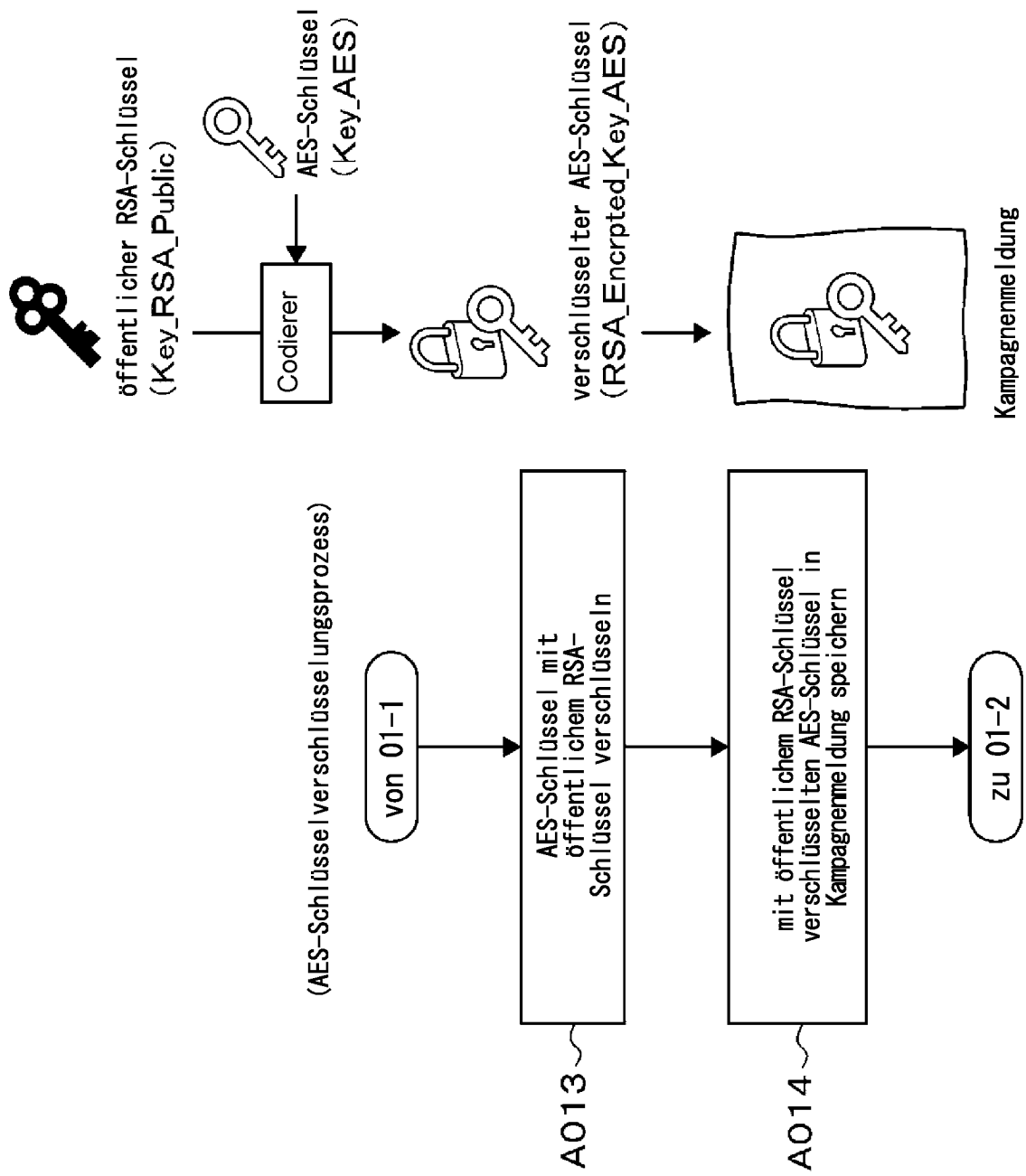


FIG. 11

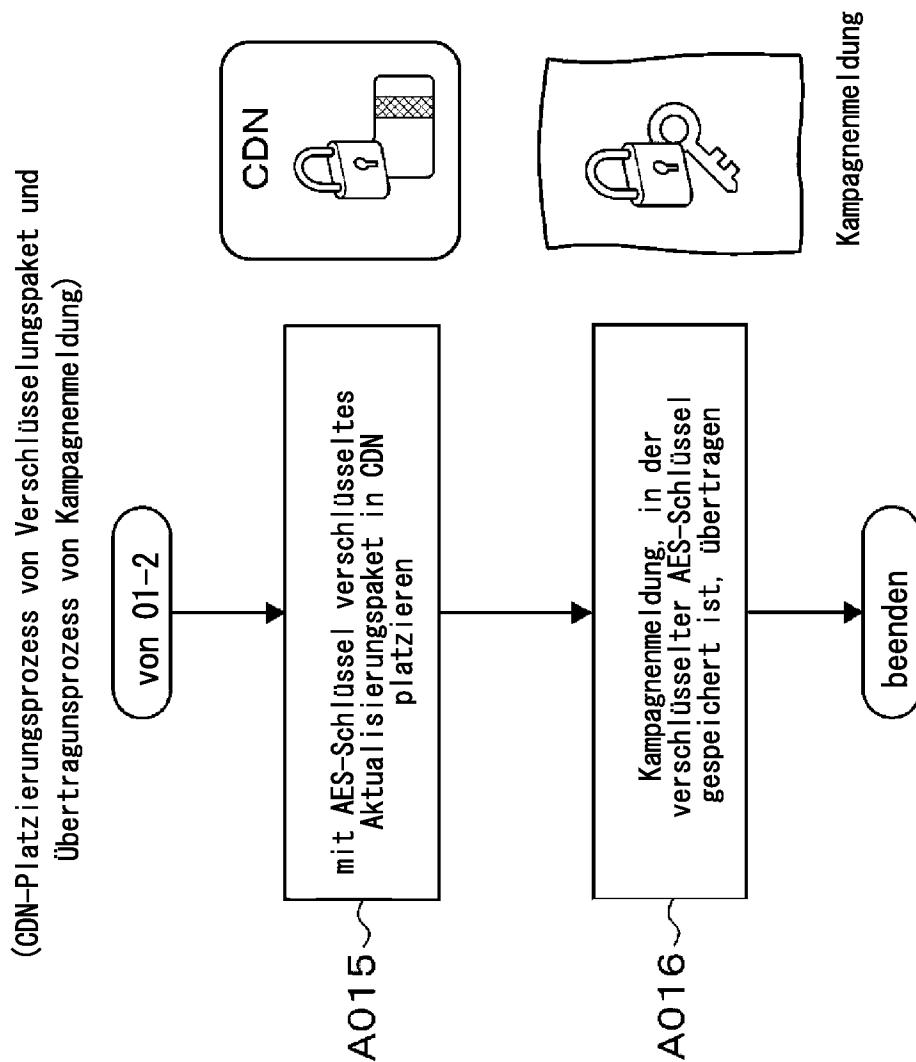


FIG. 12

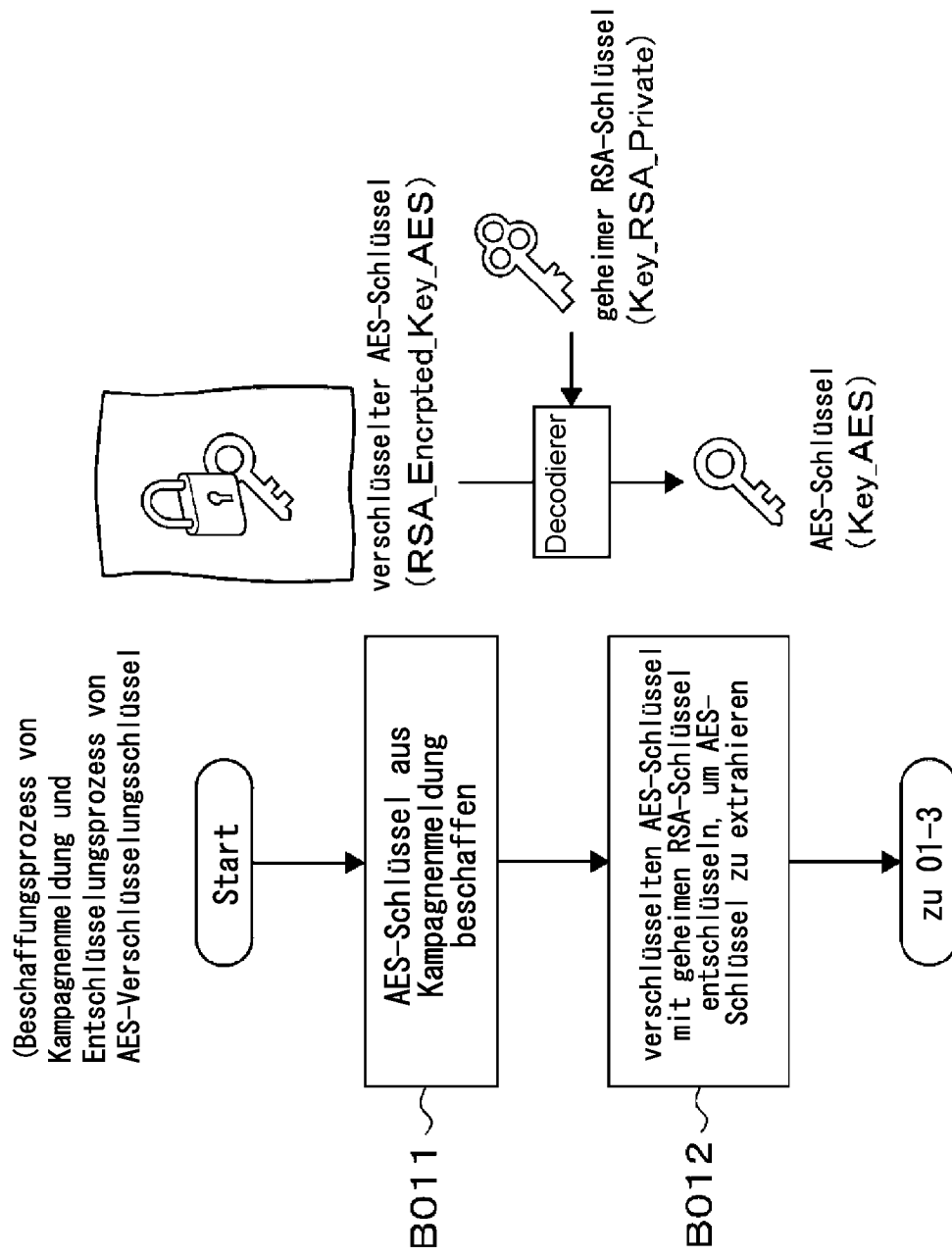


FIG. 13

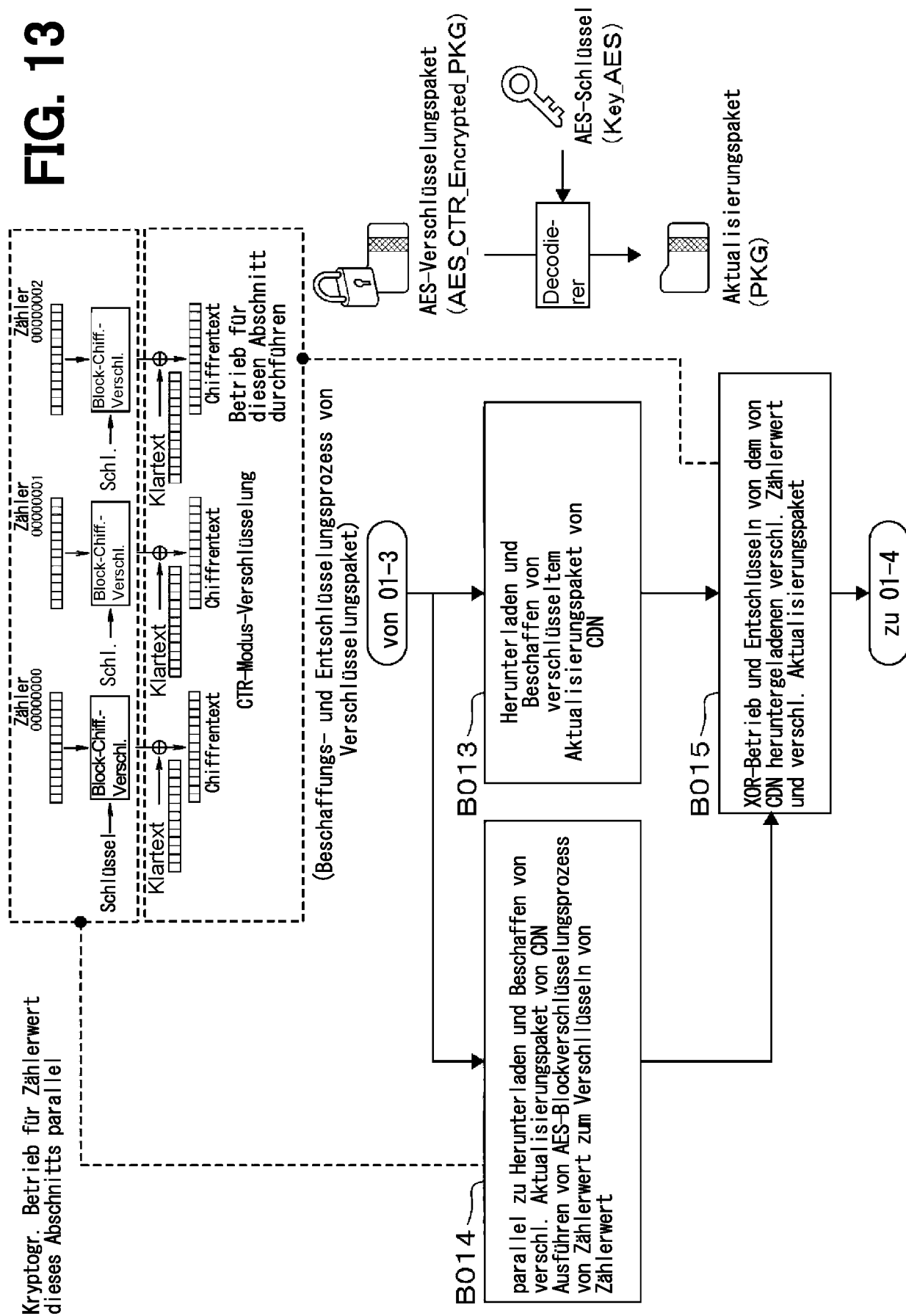


FIG. 14

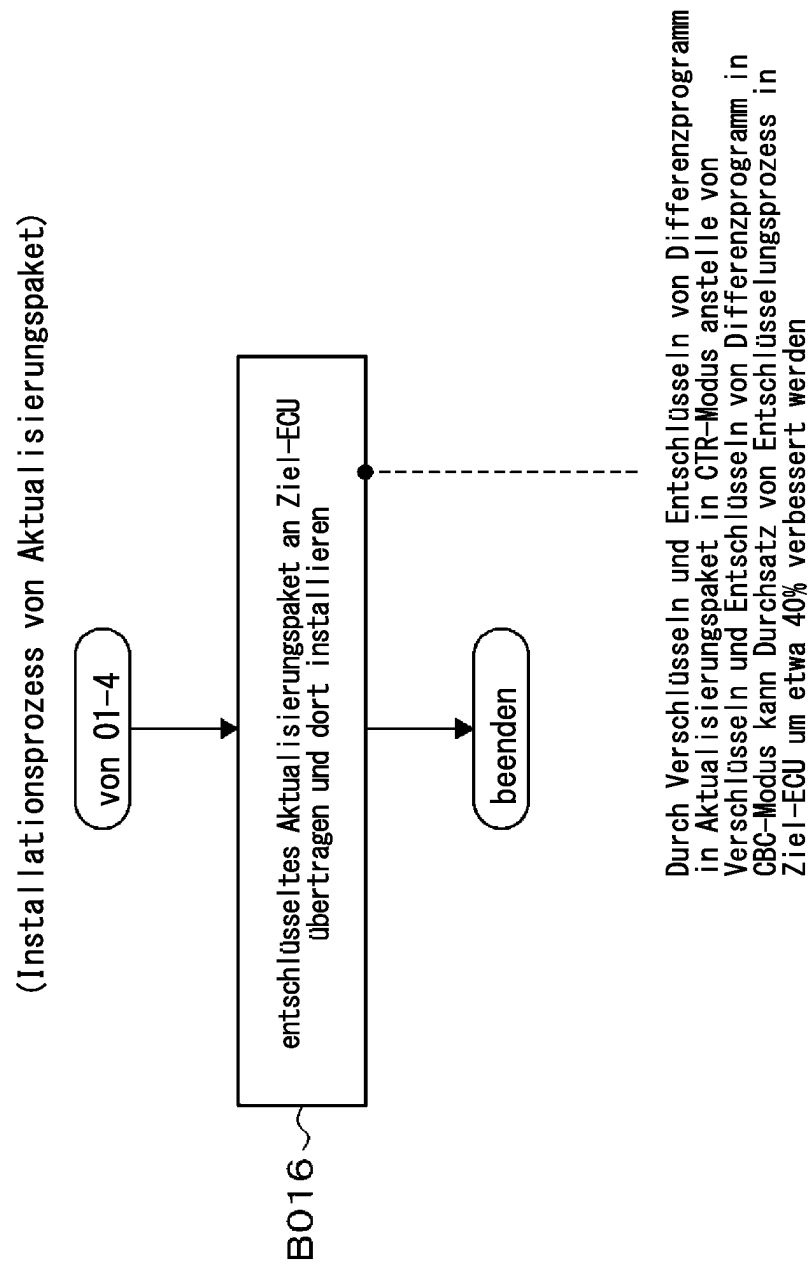


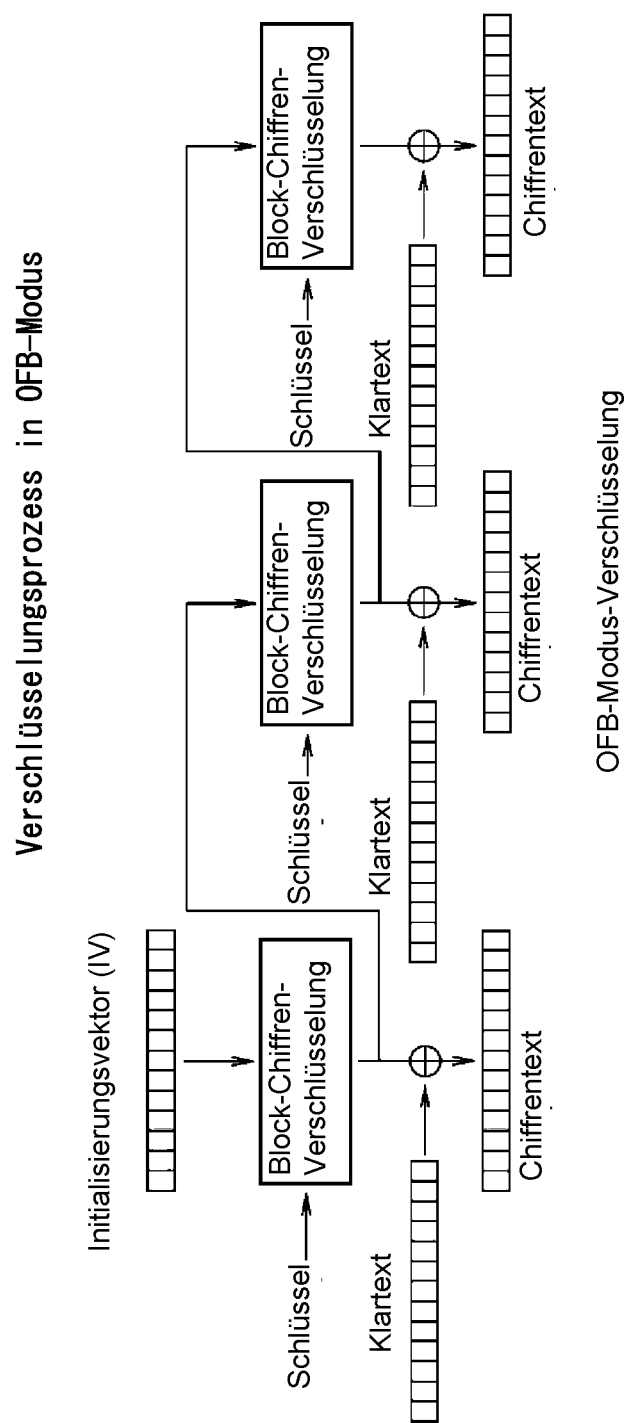
FIG. 15

FIG. 16

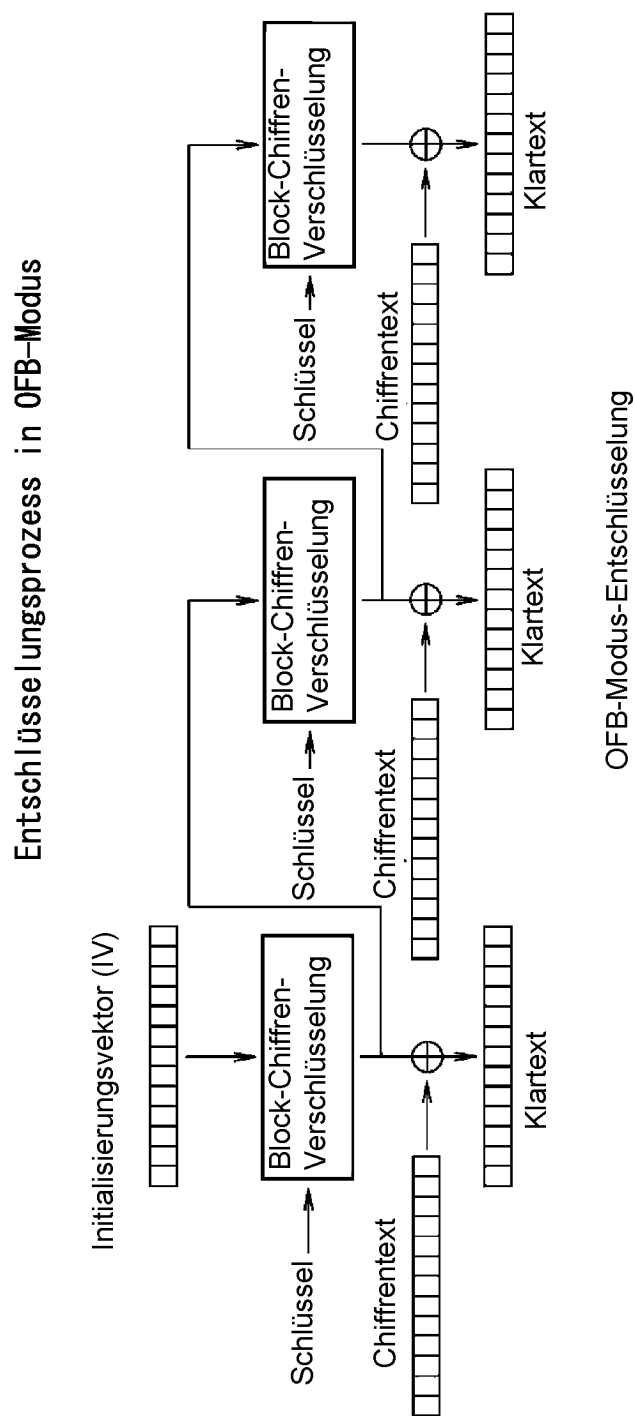


FIG. 17

	Name	Vorteile	Nachteile	Empfehlung
CBC-Modus	Chiffren-Block-Kettenbildung Chiffren-Block-Kettenmodus	· wiederholter Klartext wird nicht in Chiffrentext reflektiert, hohe Sicherheit	· Wenn Chiffrentext mit Fehler in Einheiten von Bits entschlüsselt wird, sind gesamter Block und nächstes entspr. Bit fehlerhaft (Fehlerstreuung). · Vorbereitung für Verschl. und Entschl. möglich. · Paralleler Prozess von Verschlüsselung nicht möglich.	CRYPTOREC empfohlene Verschlüsselung
OFB-Modus	Ausgangsrückführung Ausgangsrückführungsmodus	· Vorbereitung für Verschl. und Entschl. möglich, so dass hohe Geschwindigkeit möglich · Entschlüsseln von Chiffrentext mit bitweisem Fehler liegt innerhalb von Fehler von nur entspr. Bit von Klartext	· Wenn aktiver Angreifer Bits von Chiffren-Block invertiert, werden Bits von entsprechendem Klartext-Block invertiert. · Paralleler Prozess (Verschlüsselung und Entschlüsselung) nicht möglich	CRYPTOREC empfohlene Verschlüsselung

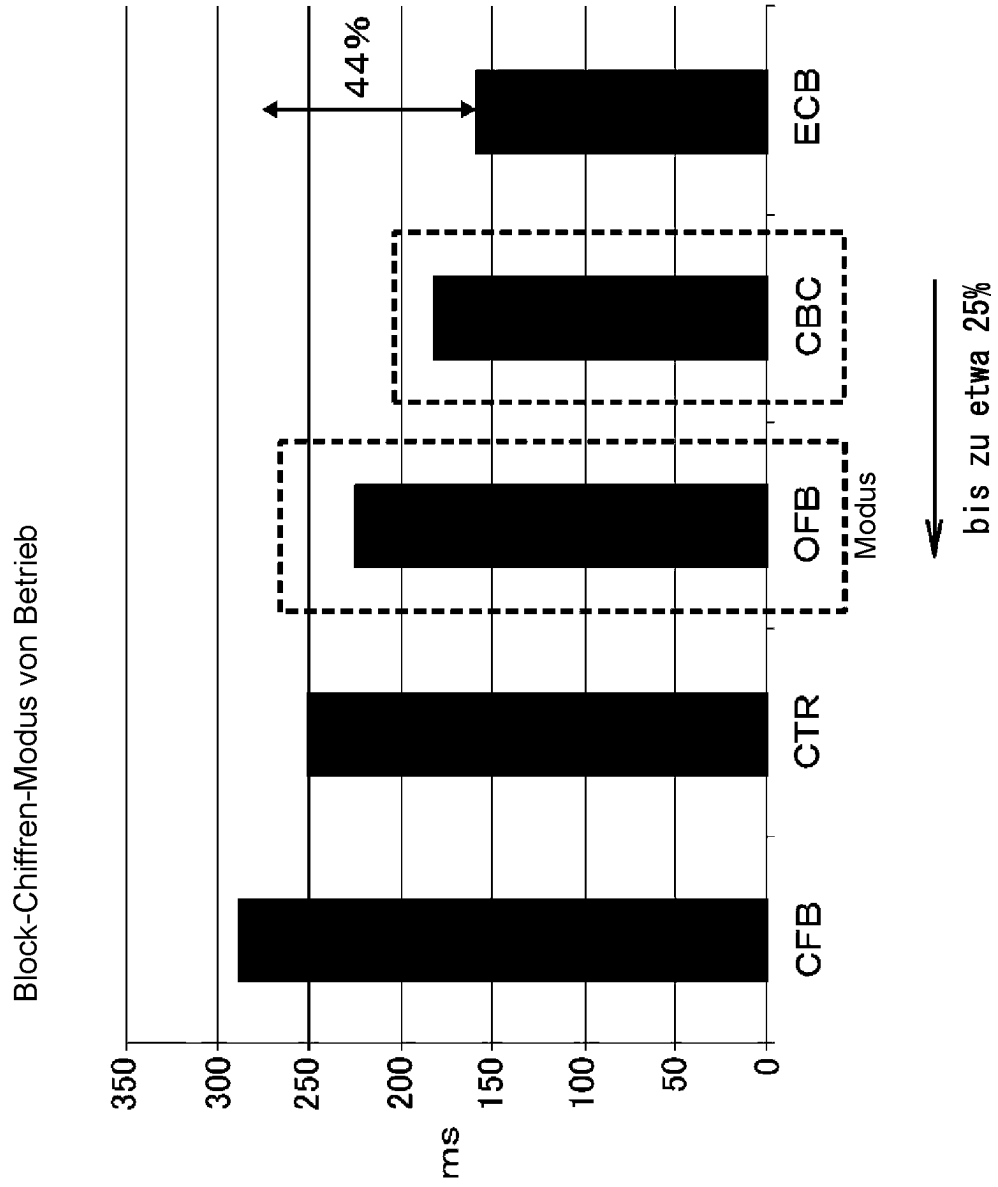
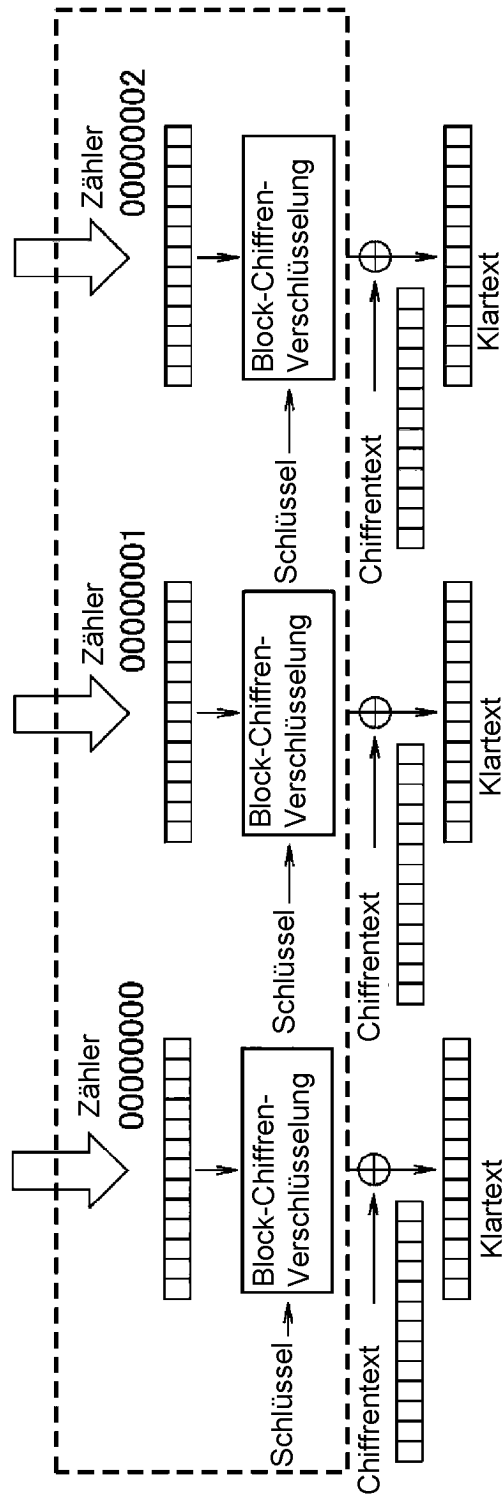
FIG. 18

FIG. 19

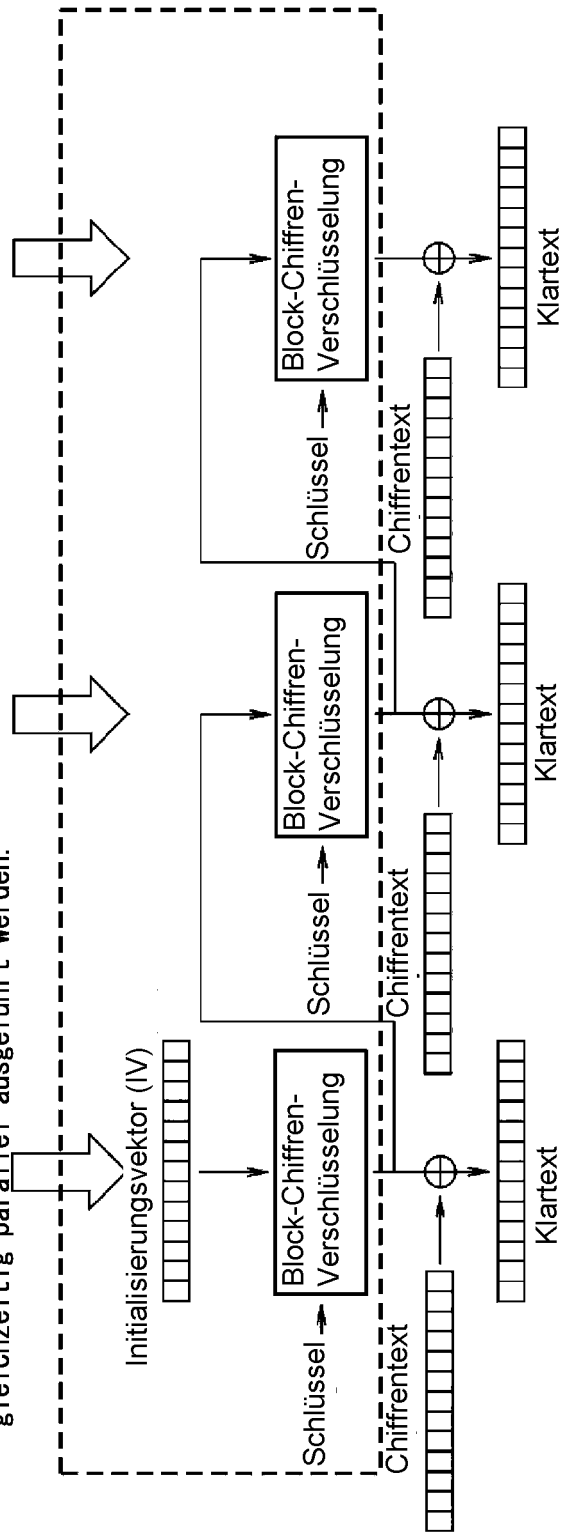
Da Zählerwert eingegeben wird, kann Entschlüsselungsprozess gestartet werden, bevor Aktualisierungspaket als Chiffrentext empfangen wird.
Da es keine gegenseitige Abhängigkeit gibt, können mehrere kryptographische Betriebe gleichzeitig parallel ausgeführt werden.



CTR-Modus-Entschlüsselung

FIG. 20

Aufgrund von gegenseitiger Abhängigkeit kann Entschlüsselungsprozess vor Empfang von Aktualisierungspaket als Chiffrentext gestartet werden.
Da keine gegenseitige Abhängigkeit besteht, können mehrere kryptographische Betriebe gleichzeitig parallel ausgeführt werden.



OFB-Modus-Entschlüsselung

FIG. 21

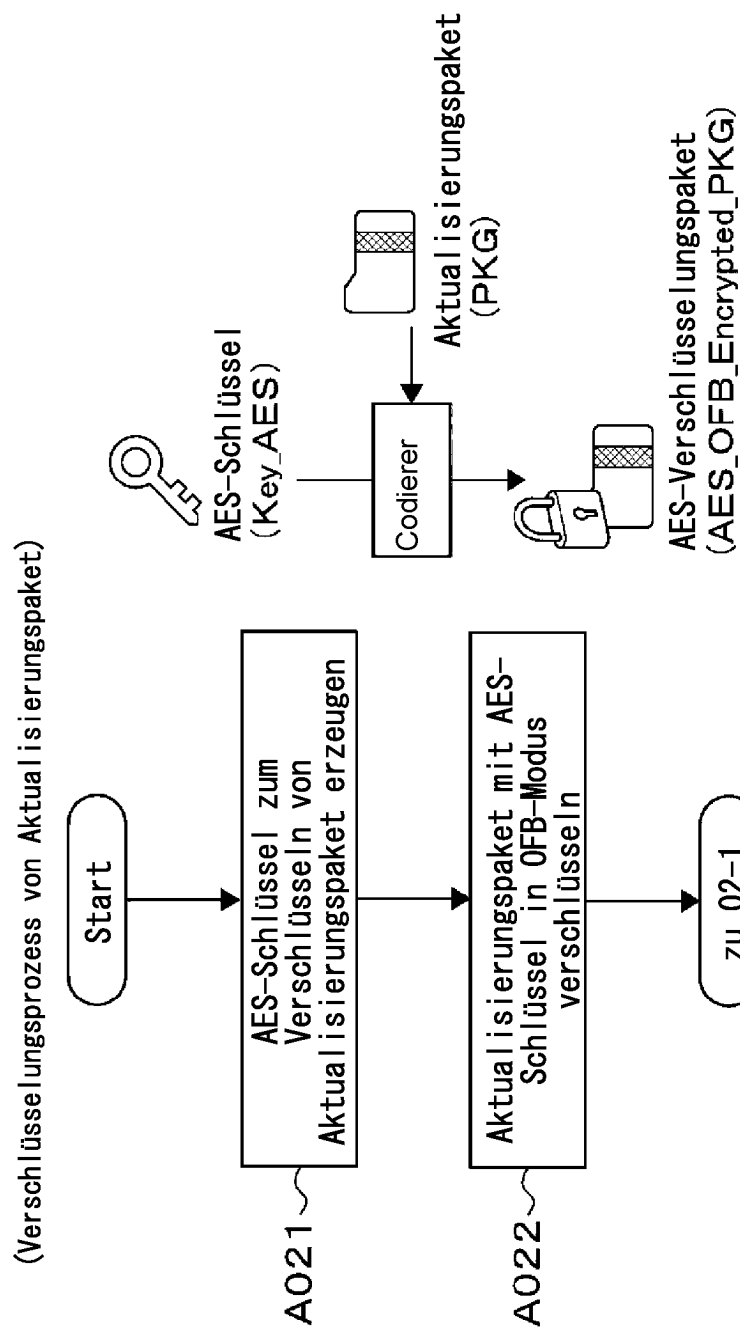


FIG. 22

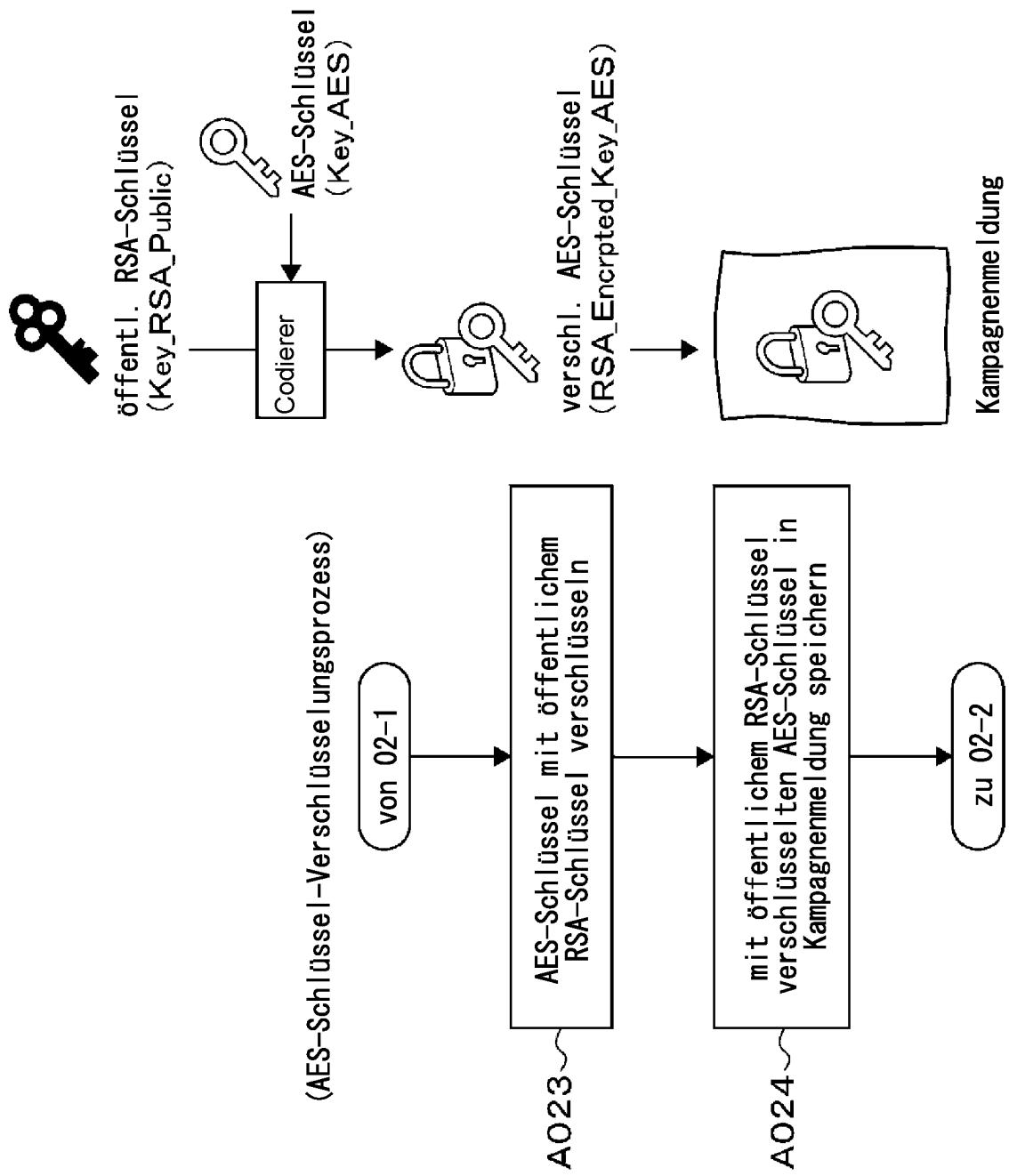


FIG. 23

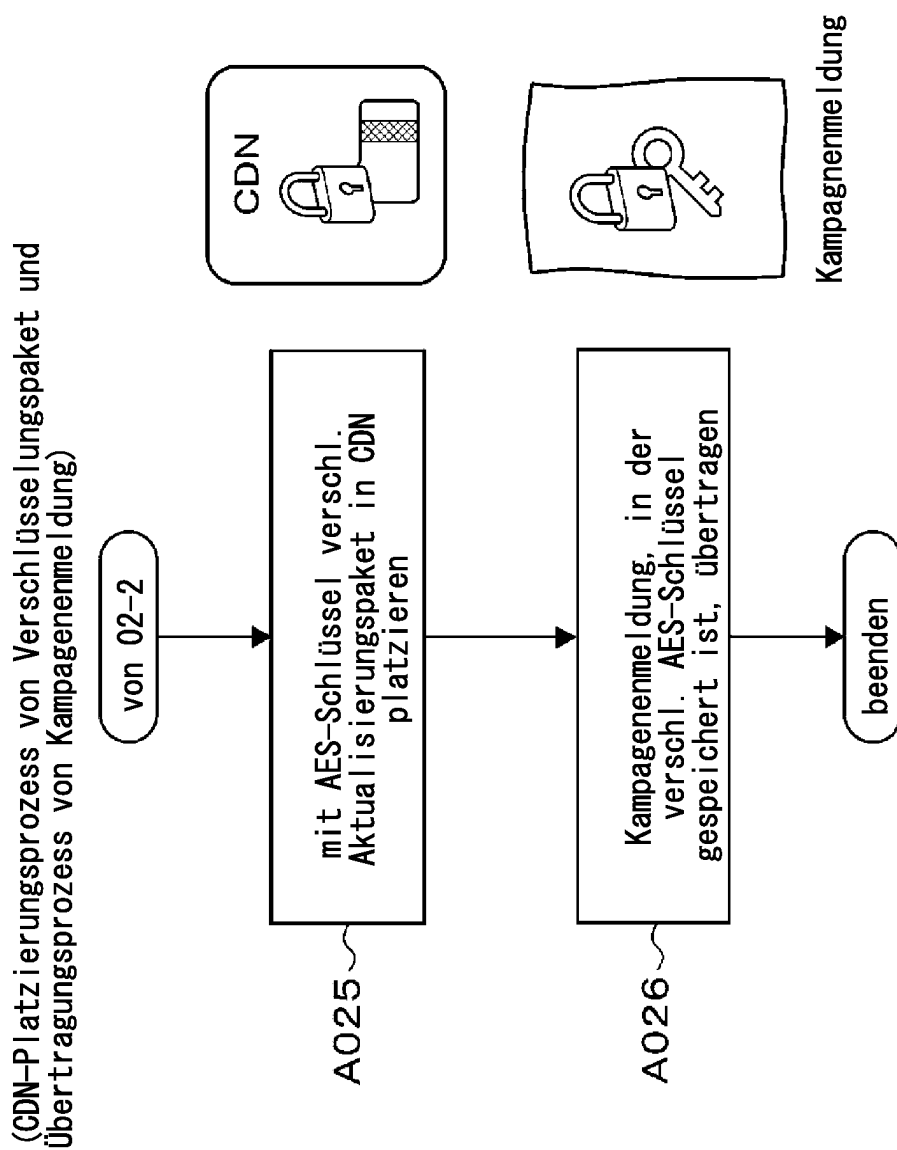


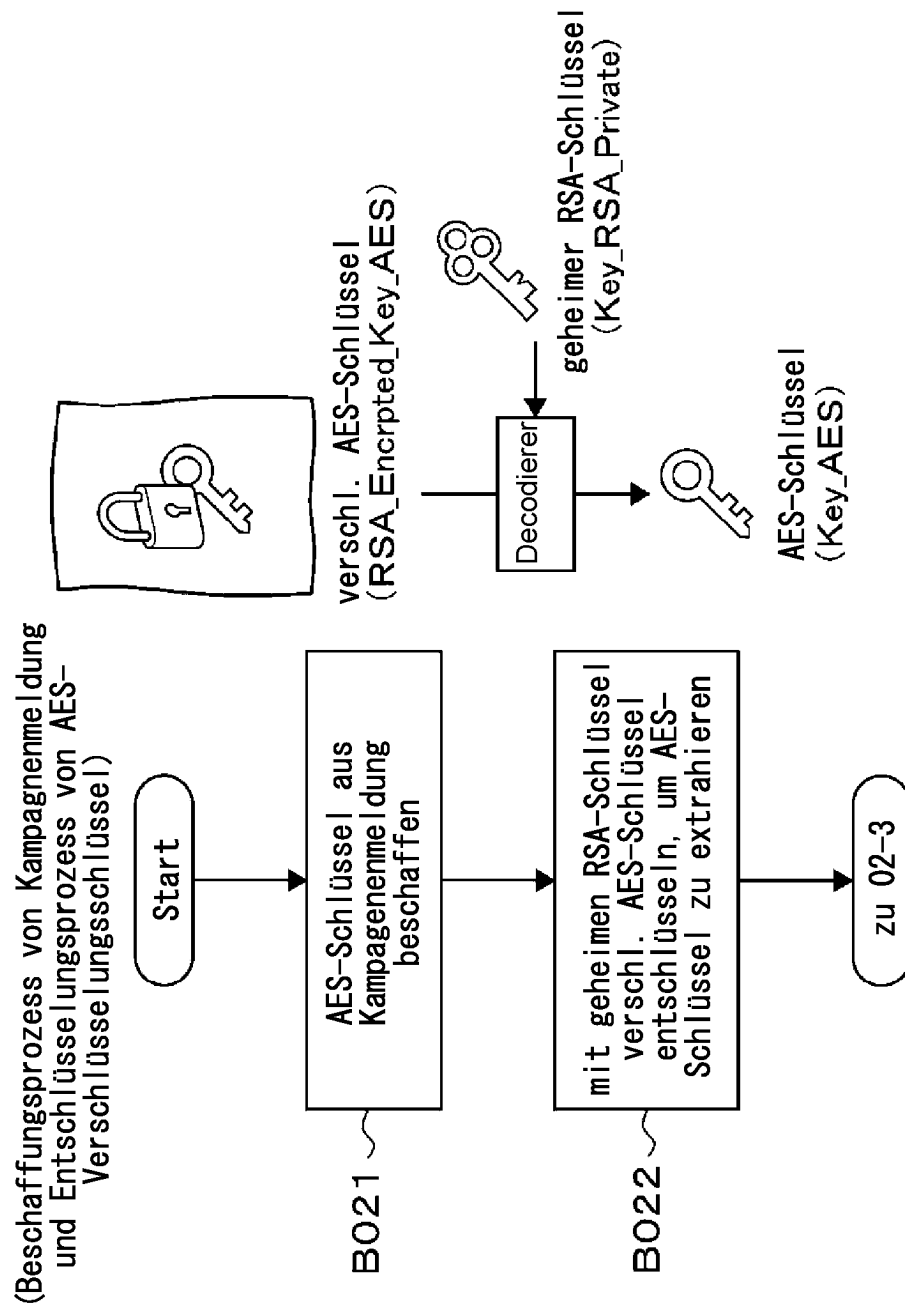
FIG. 24

FIG. 25

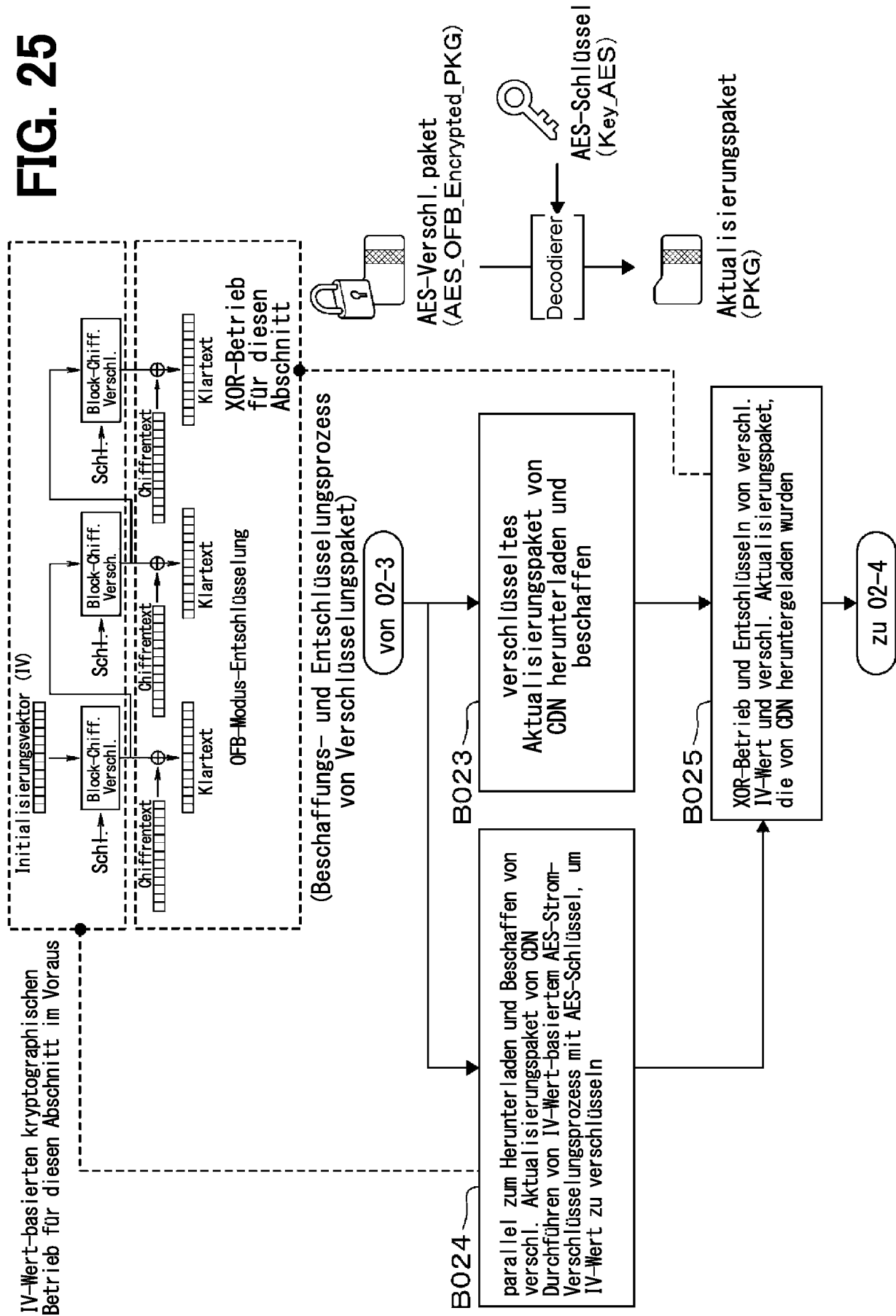


FIG. 26

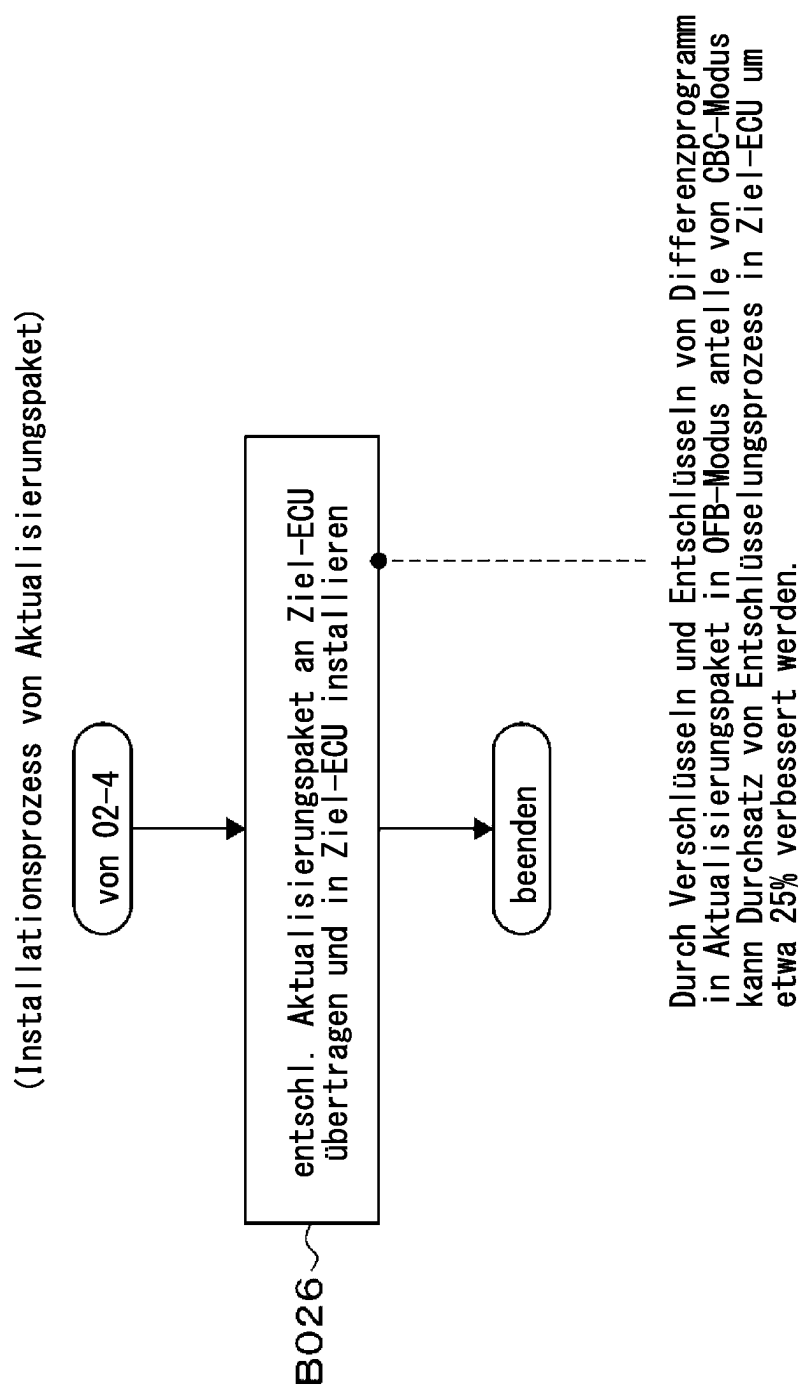


FIG. 27

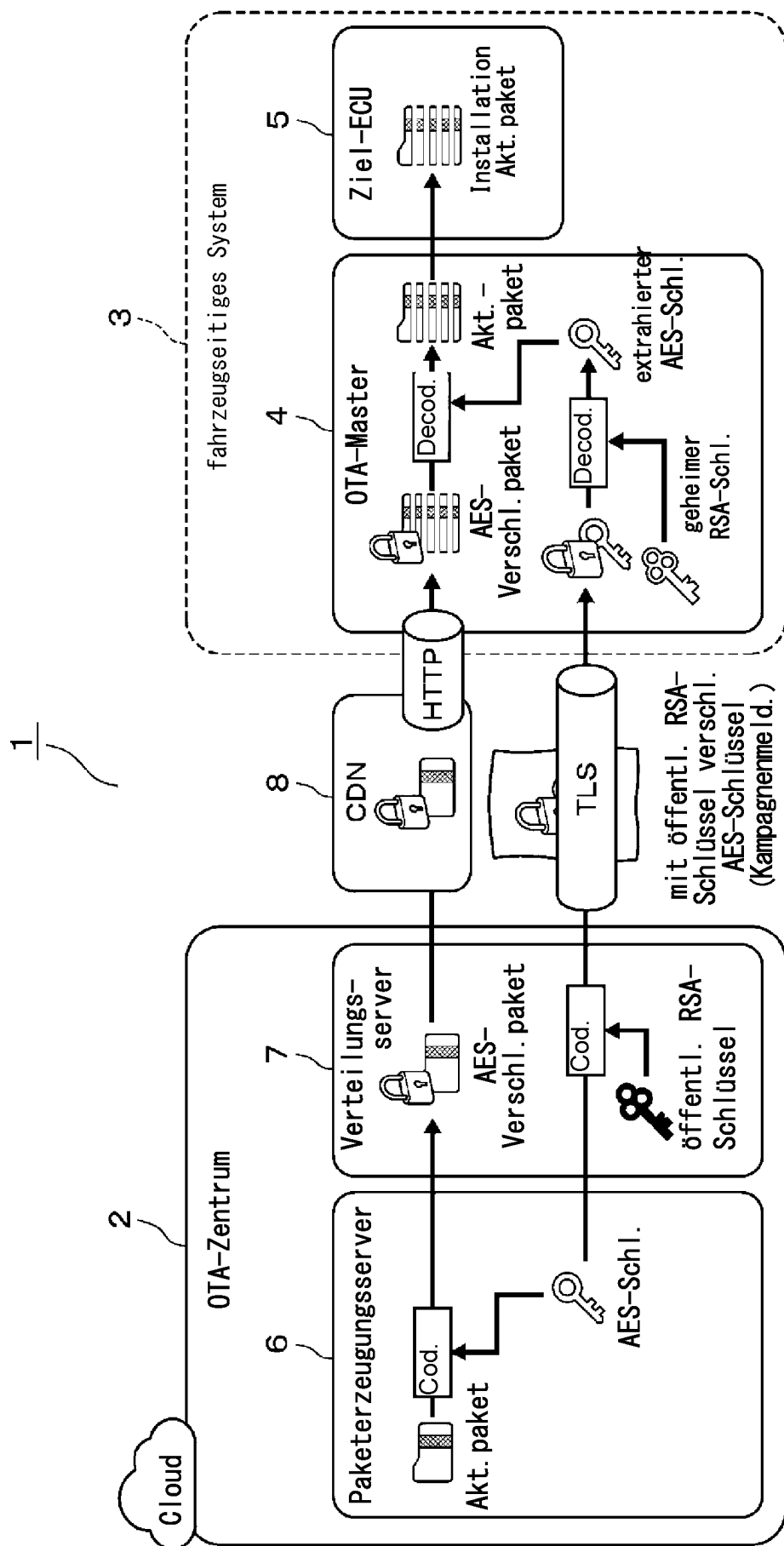


FIG. 28

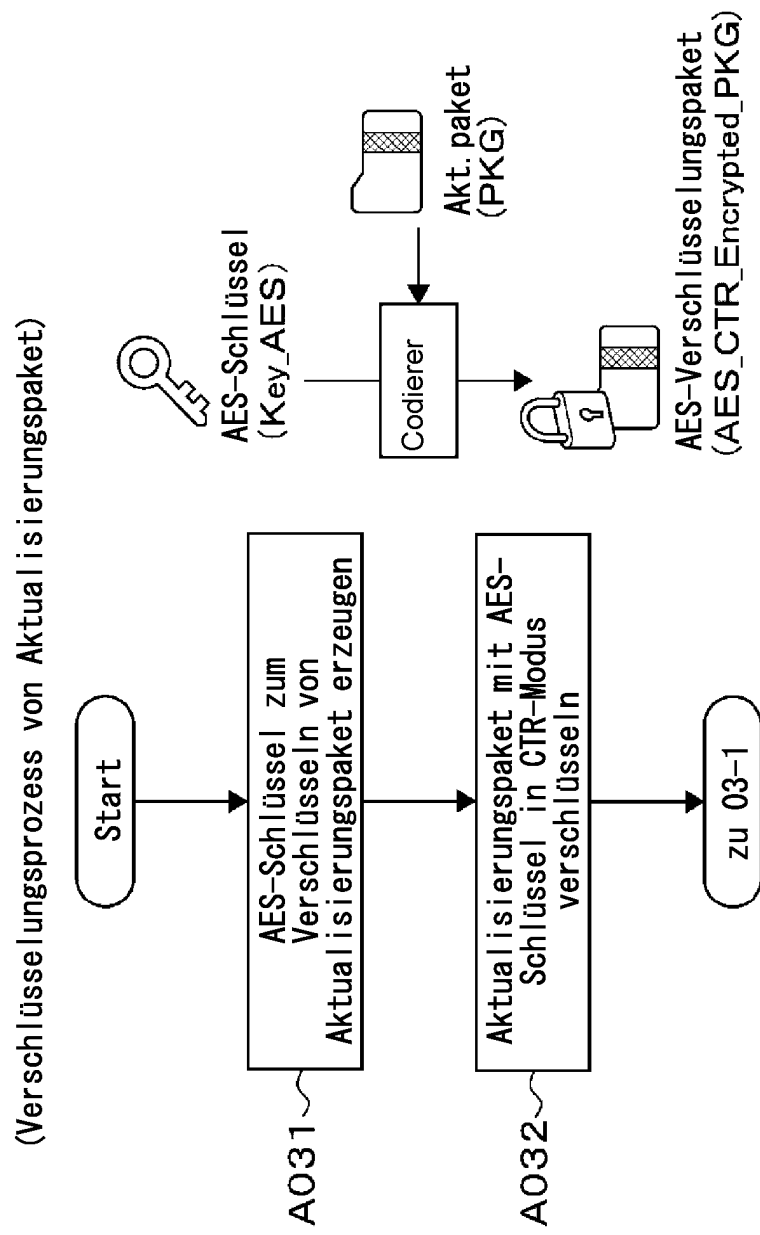


FIG. 29

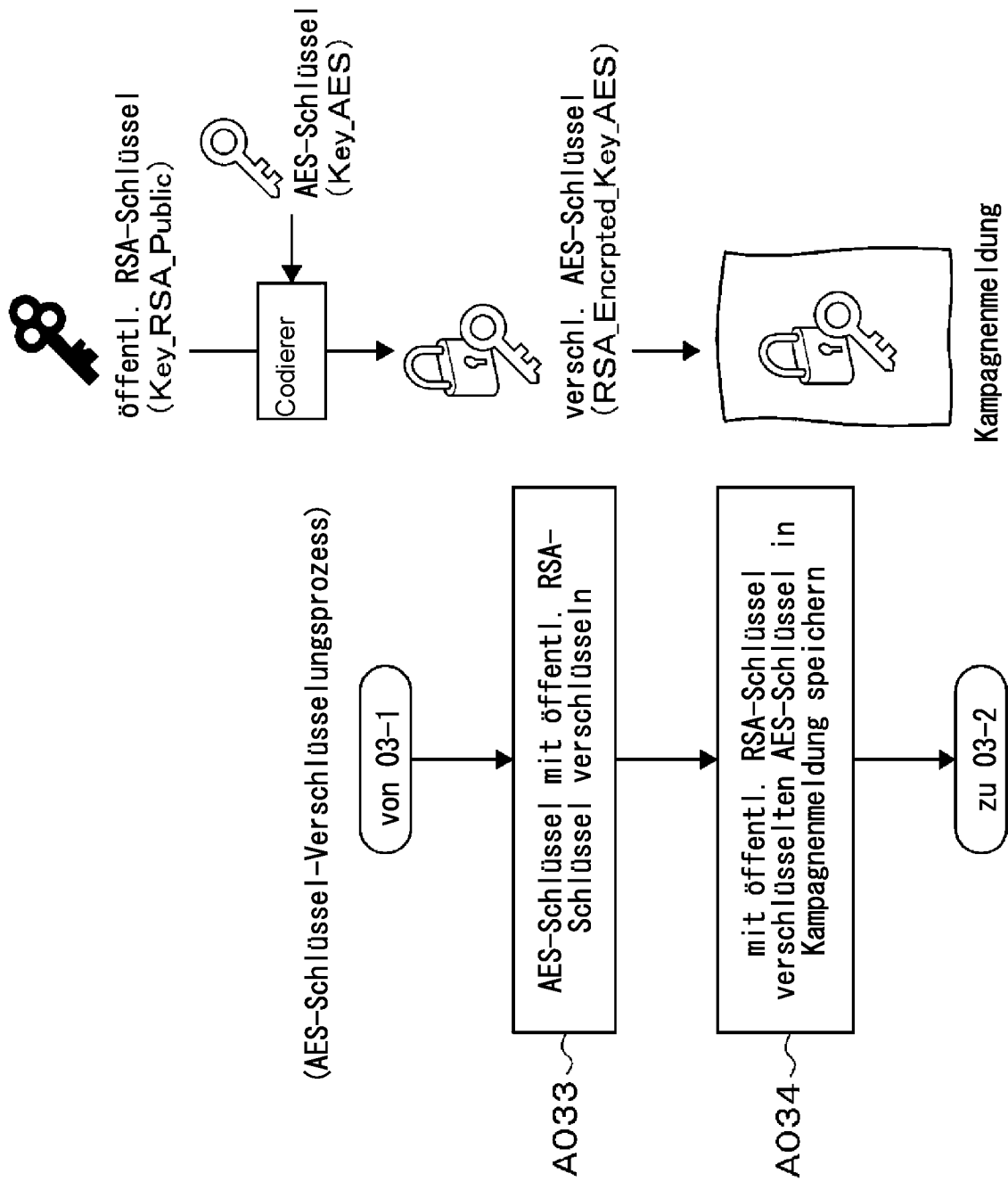


FIG. 30

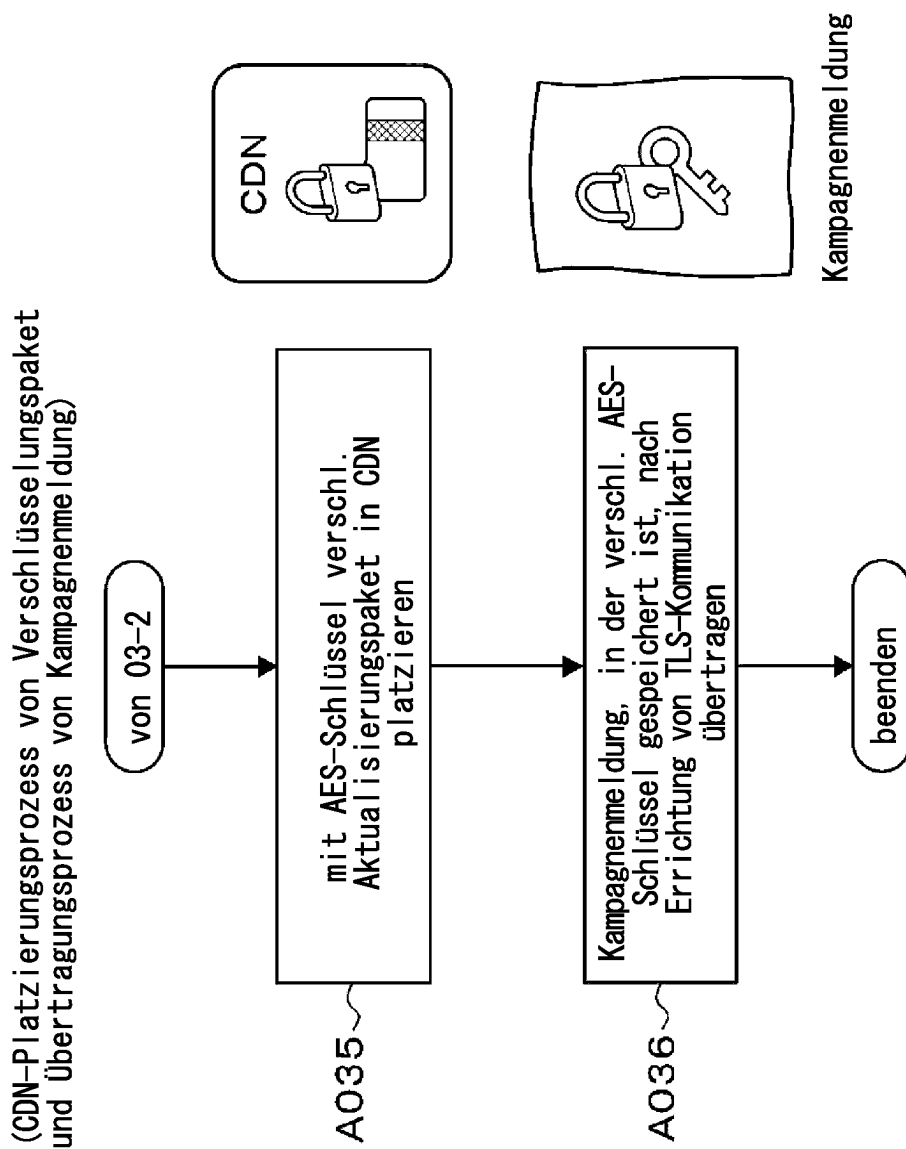


FIG. 31

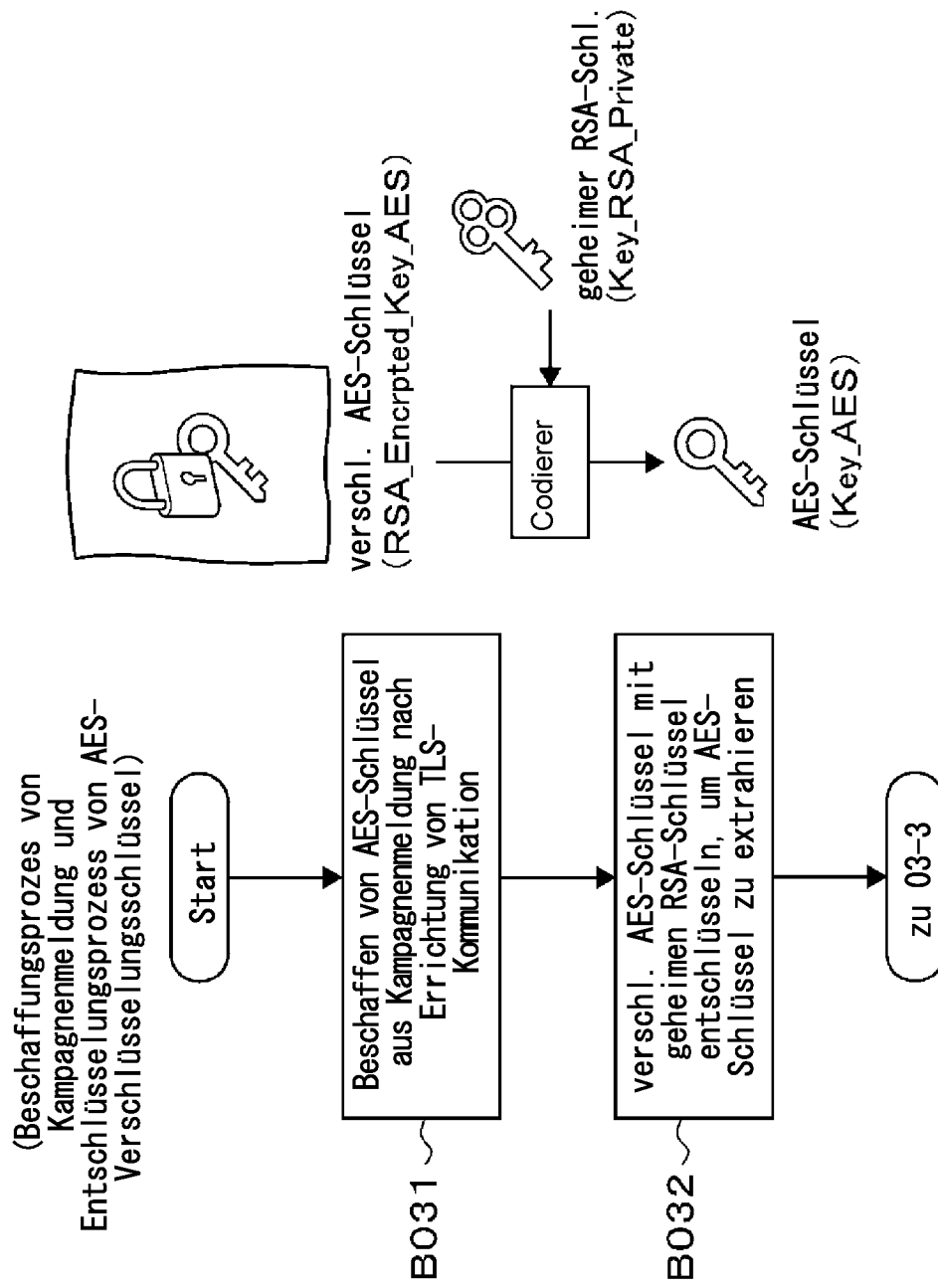


FIG. 32

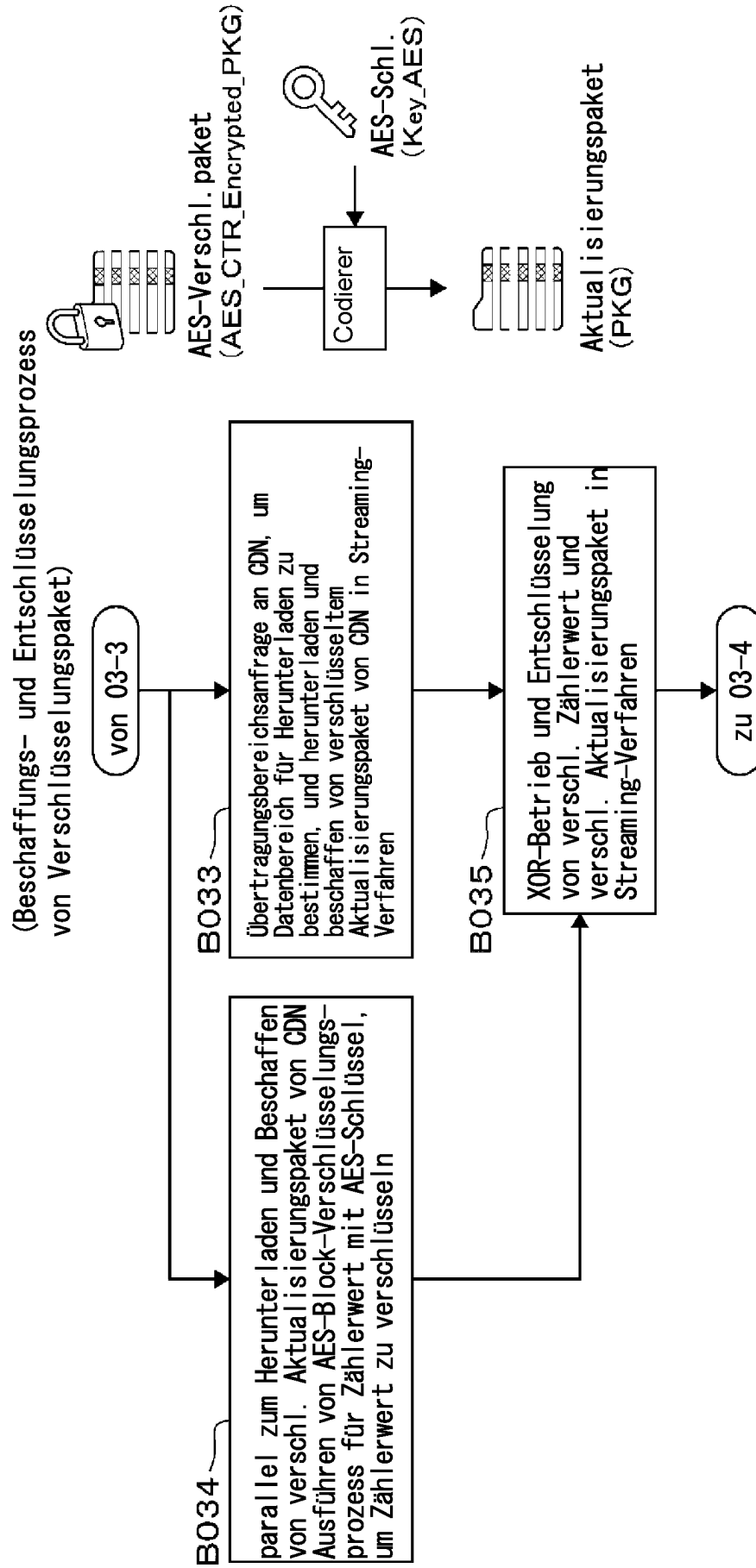


FIG. 33

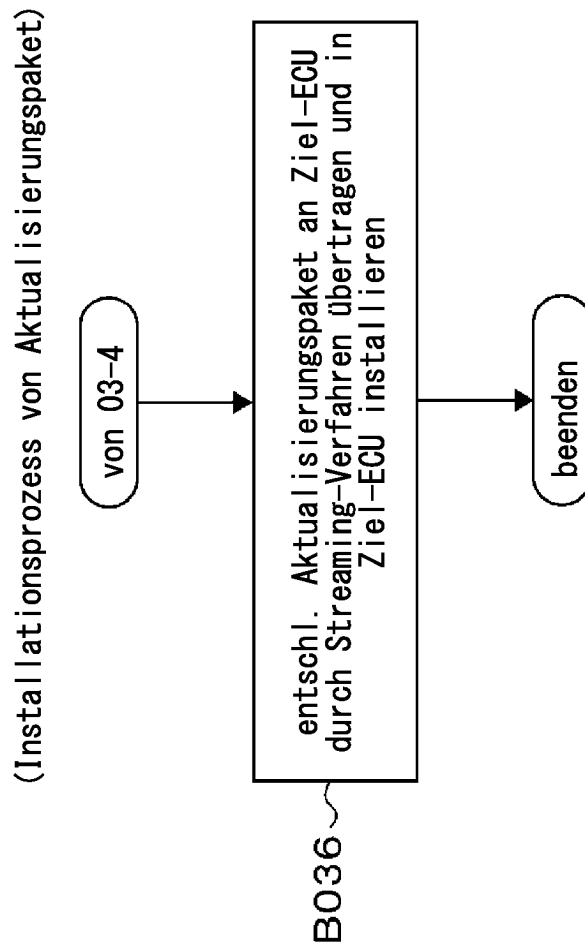
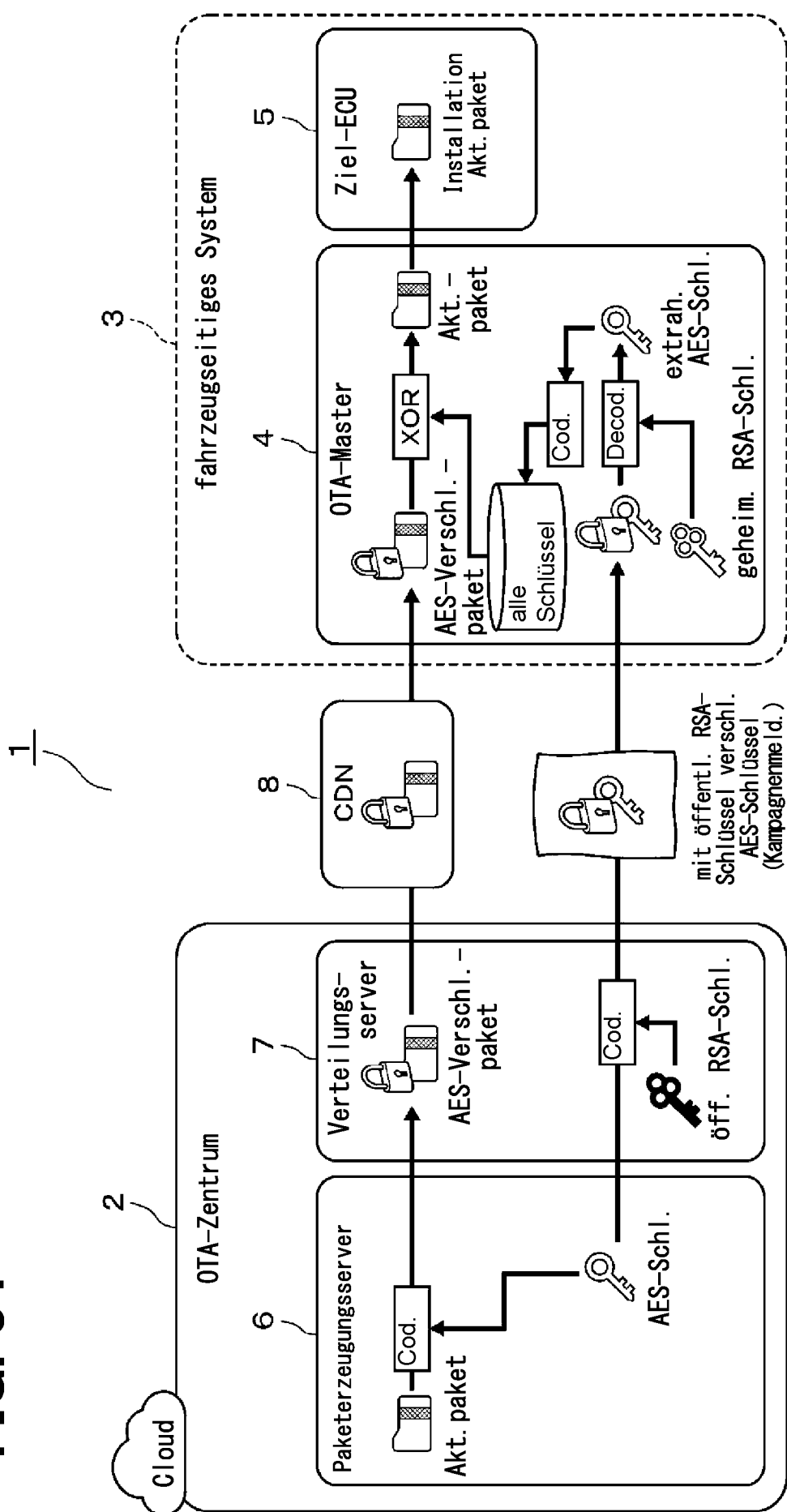


FIG. 34



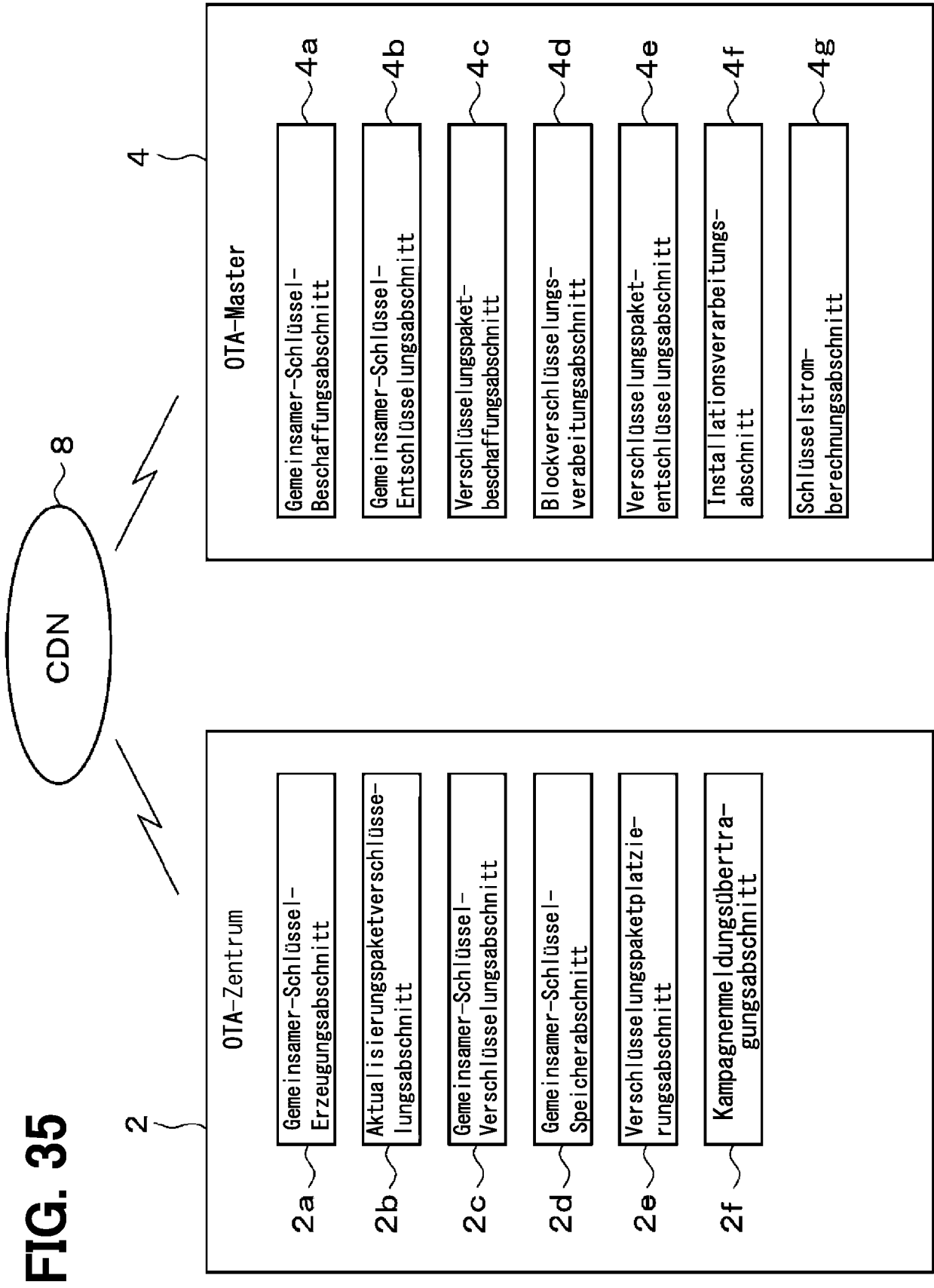


FIG. 36

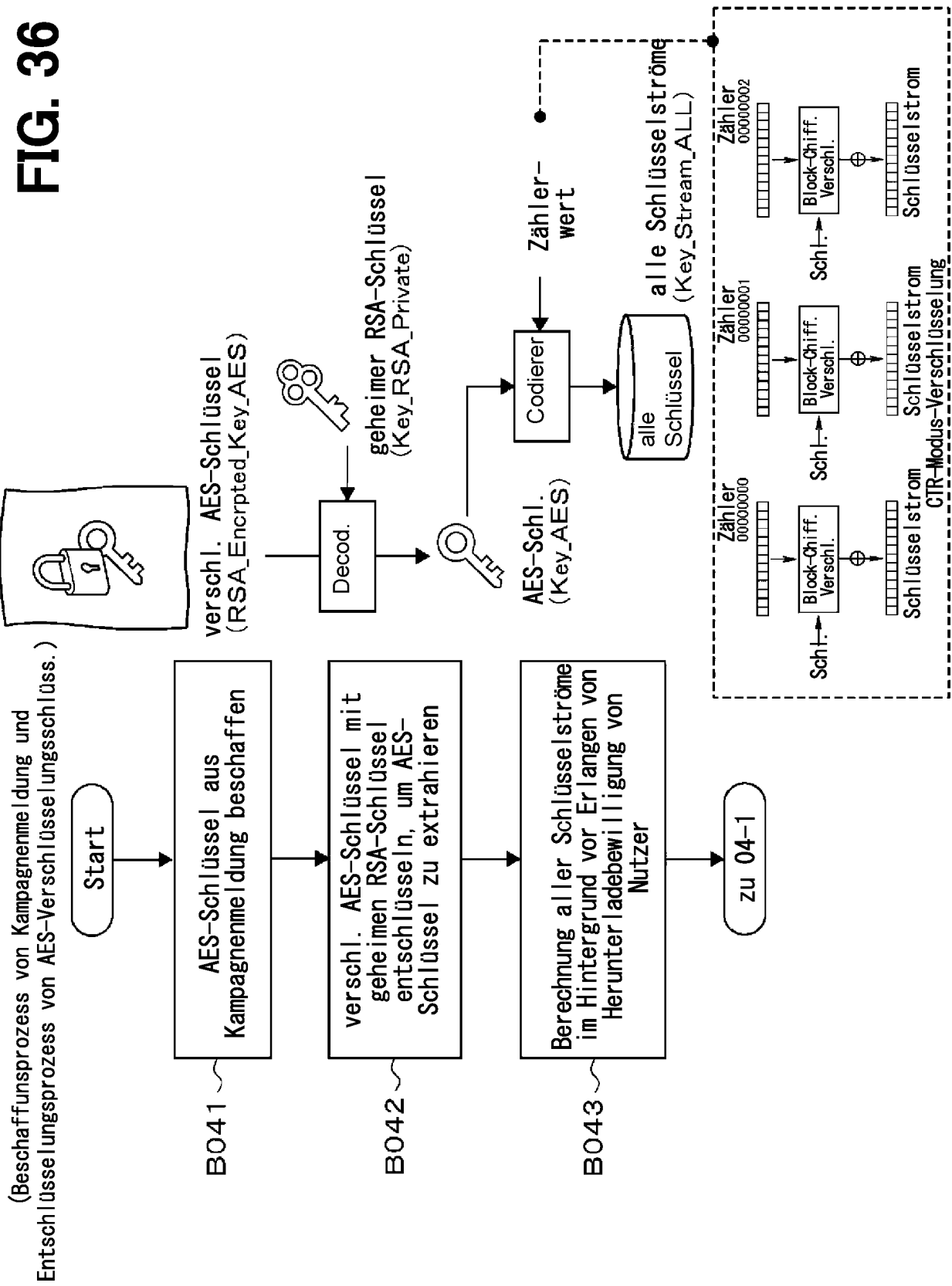


FIG. 37

(Herunterlade- und Entschlüsselungsprozess von Aktualisierungspaket mit erlangter Herunterladebewilligung von Nutzer)

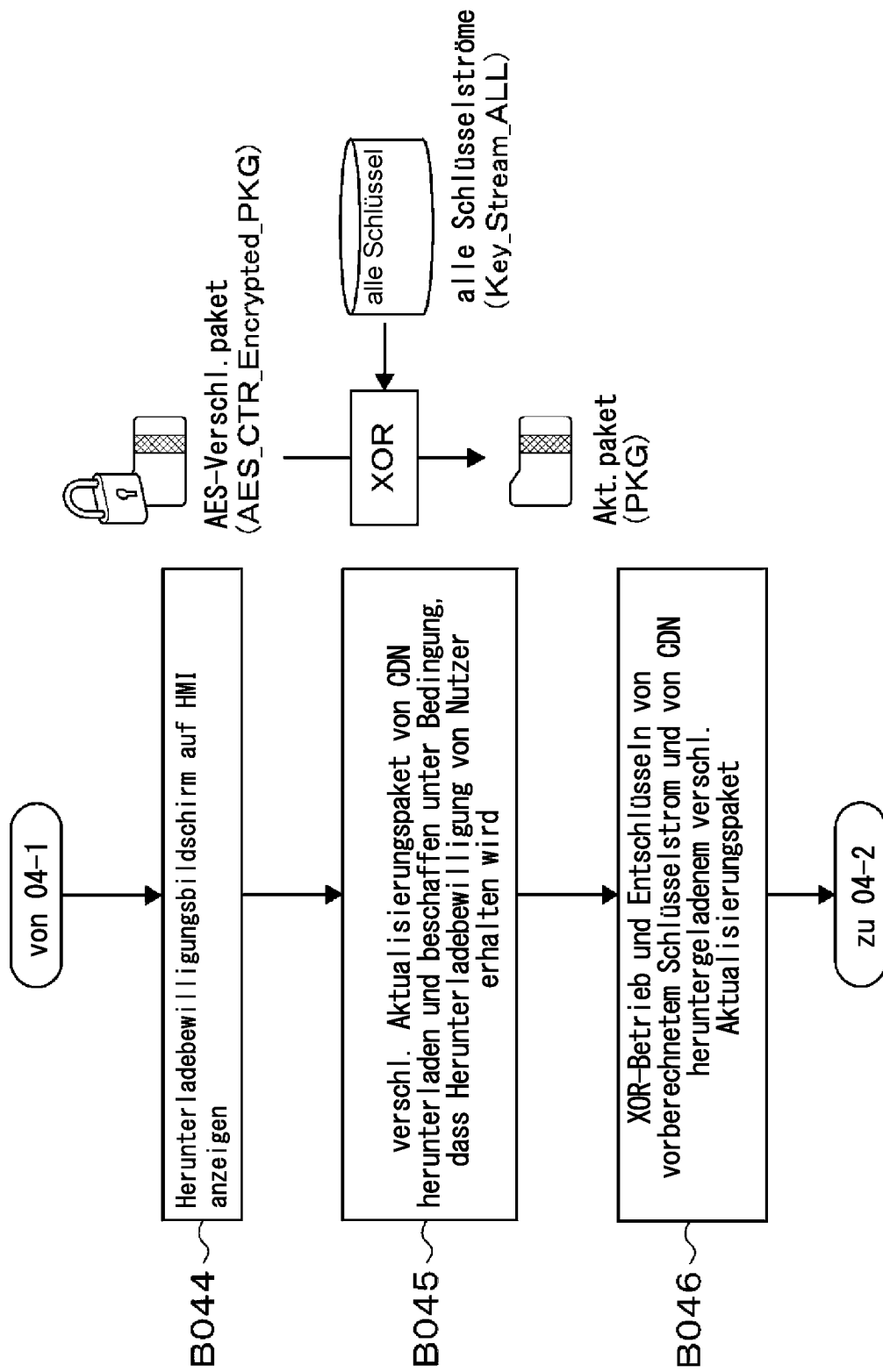
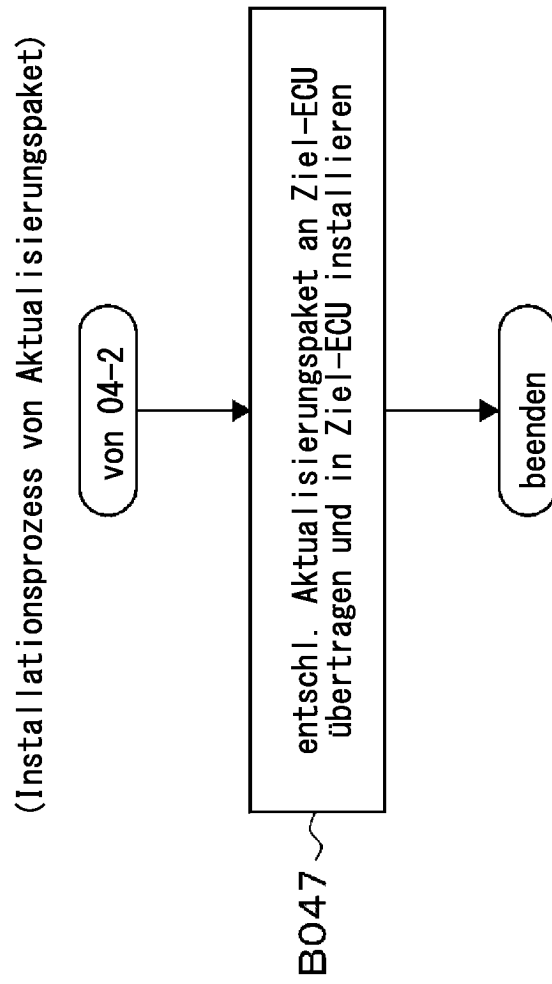


FIG. 38



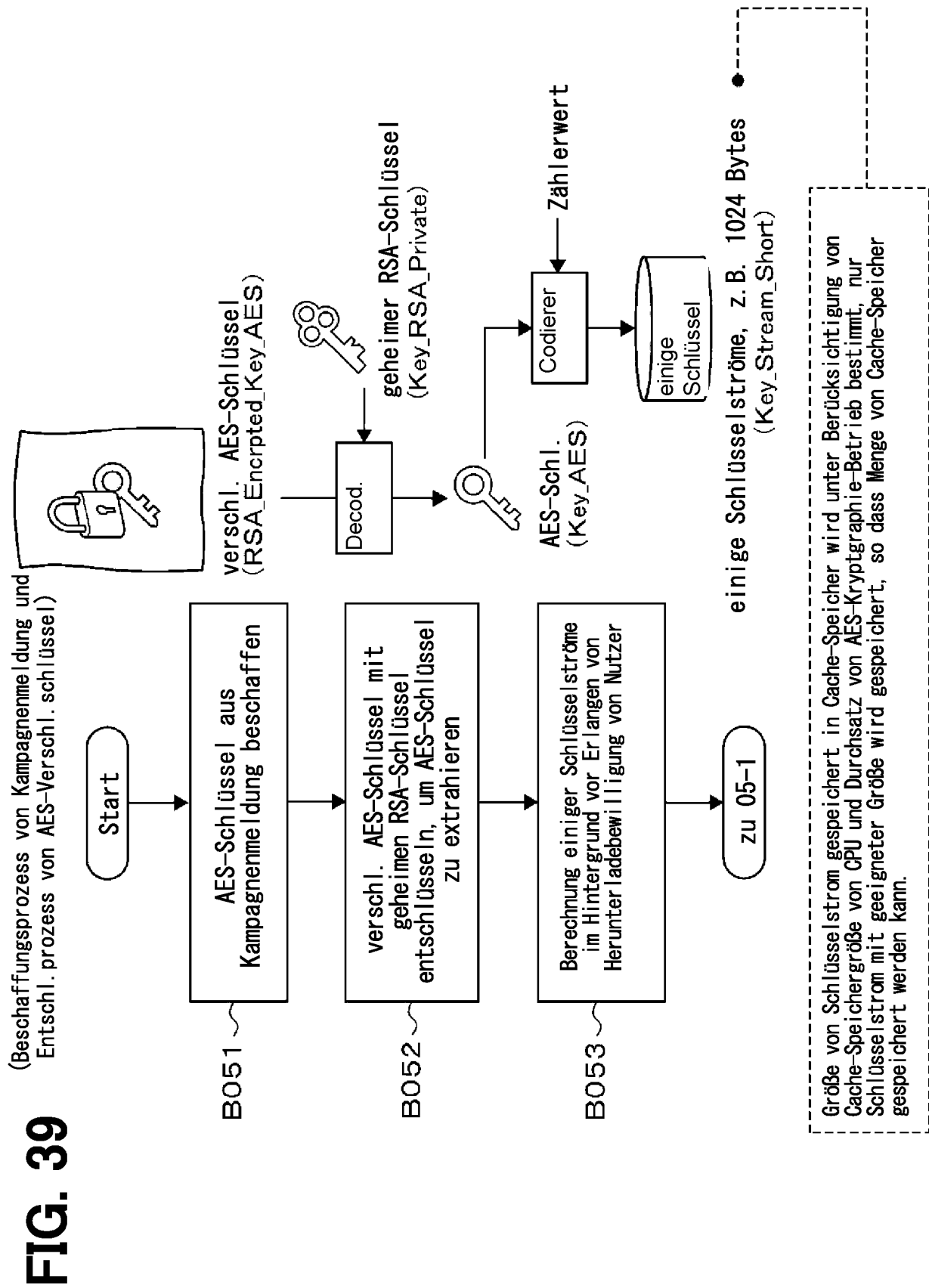


FIG. 40

(Herunterlade- und Entschlüsselungsprozess von Aktualisierungspaket nach Erhalt von Herunterladebewilligung von Nutzer)

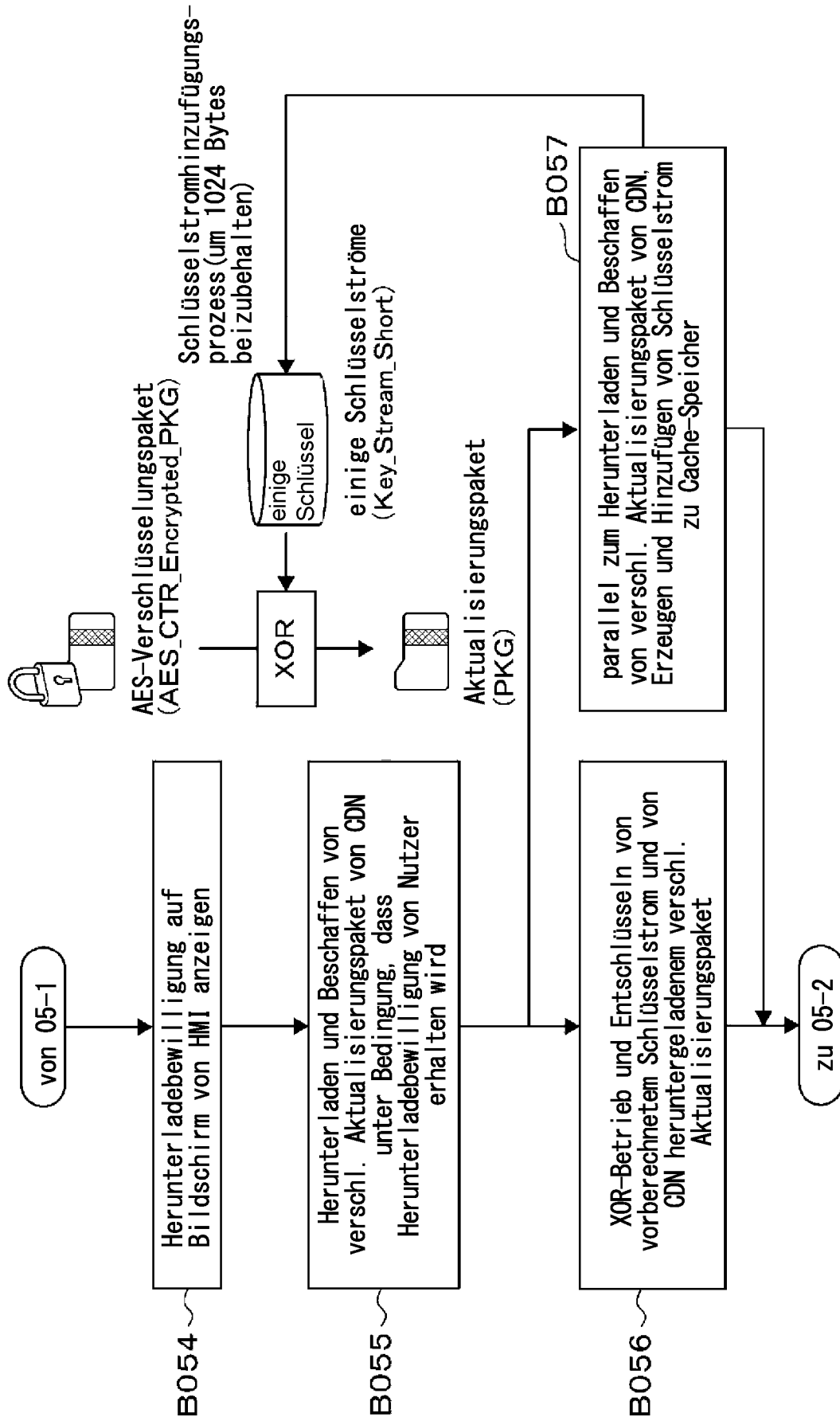


FIG. 41

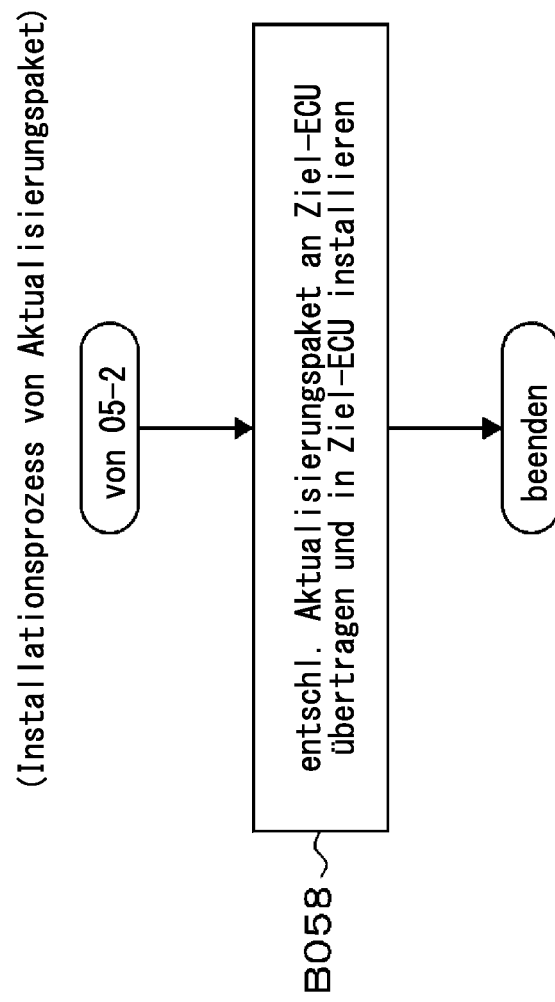


FIG. 42

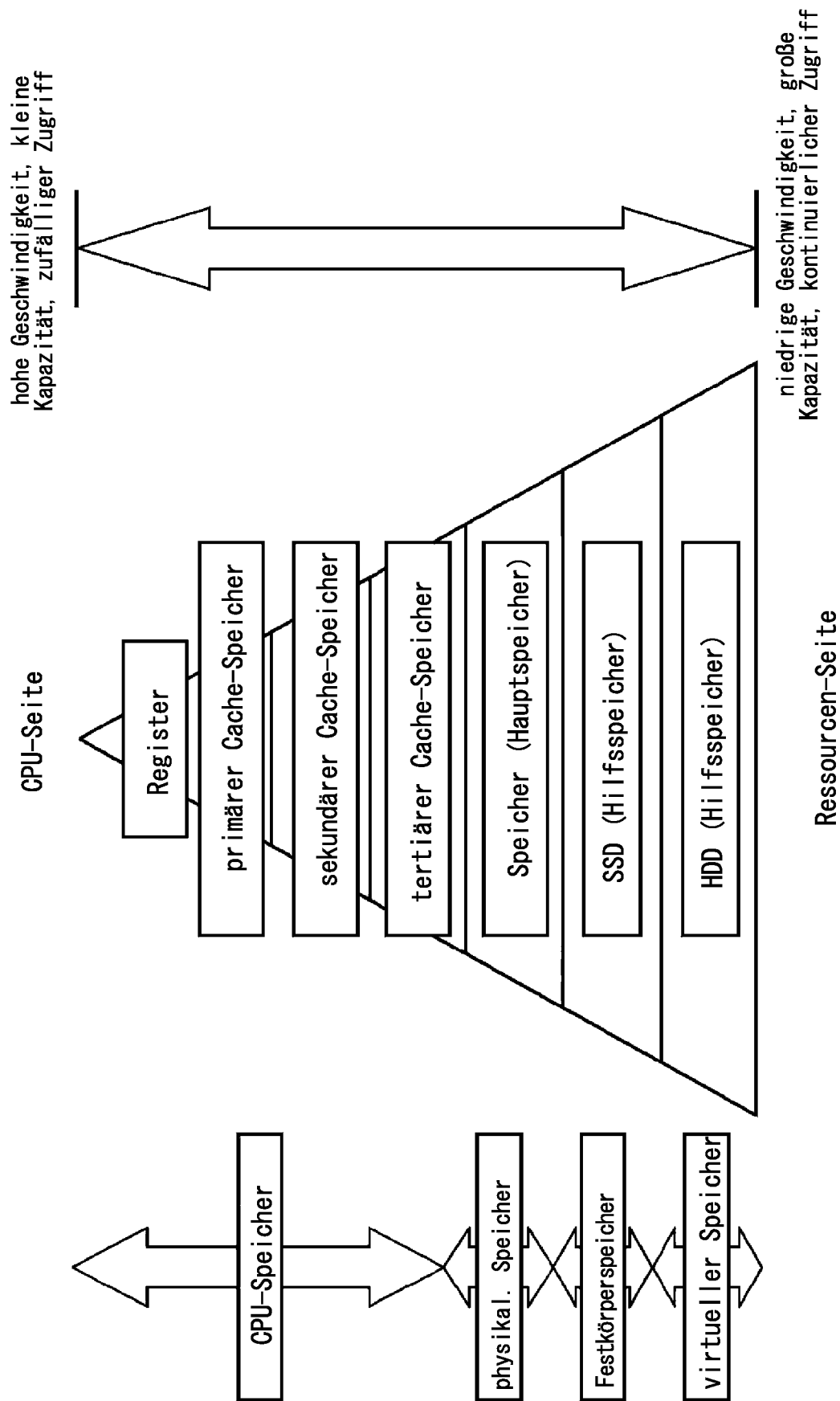
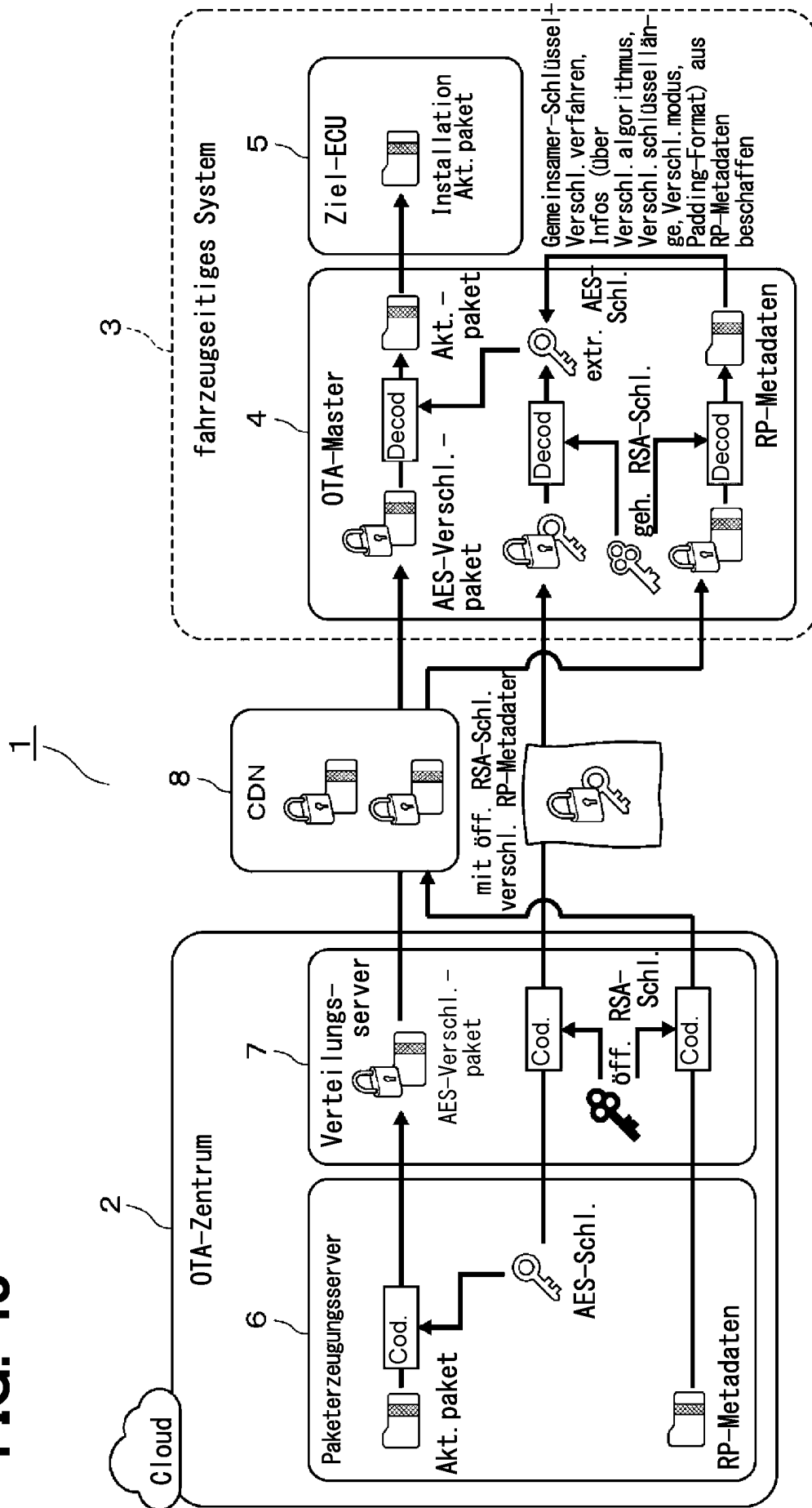


FIG. 43



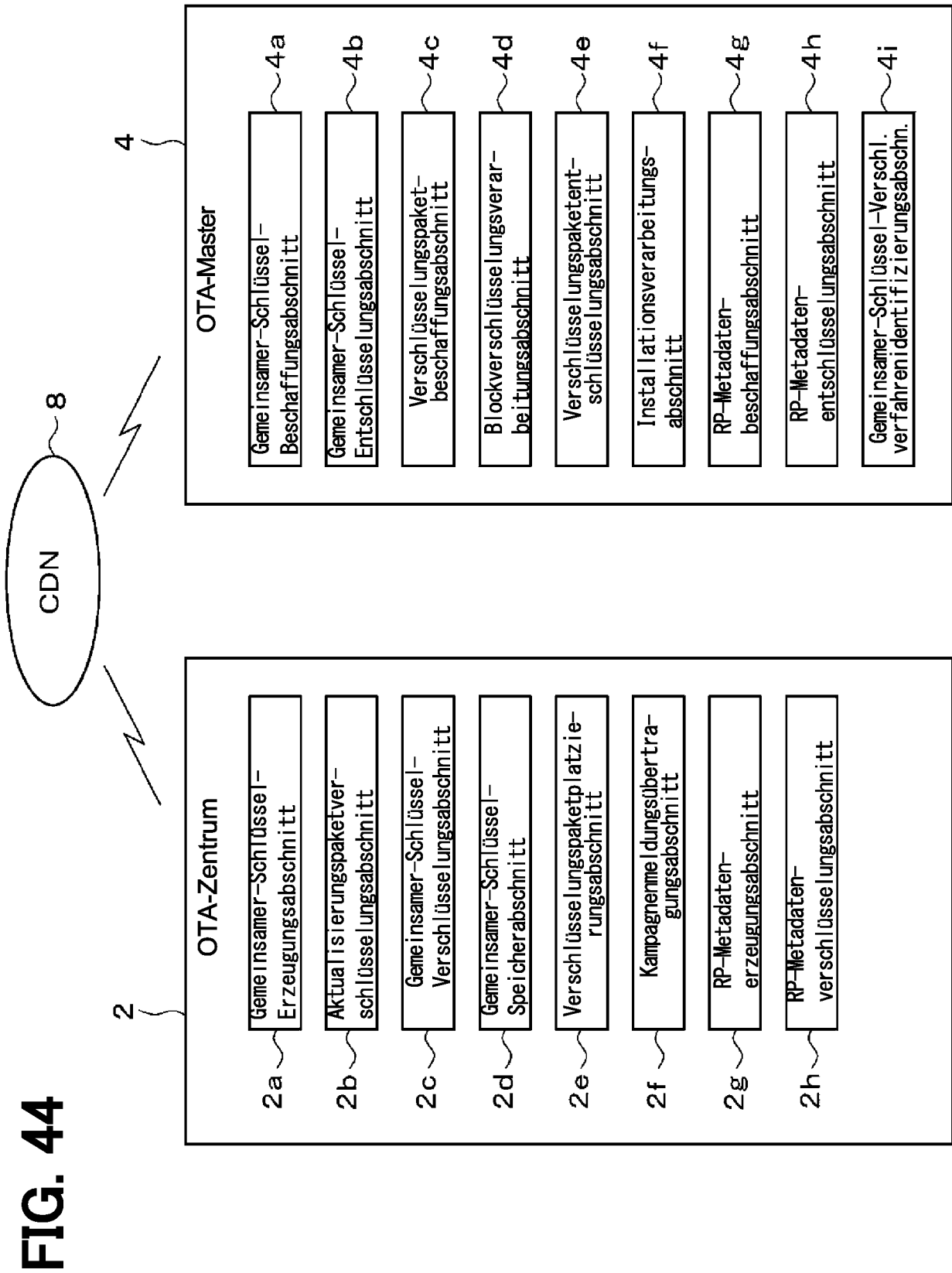


FIG. 45

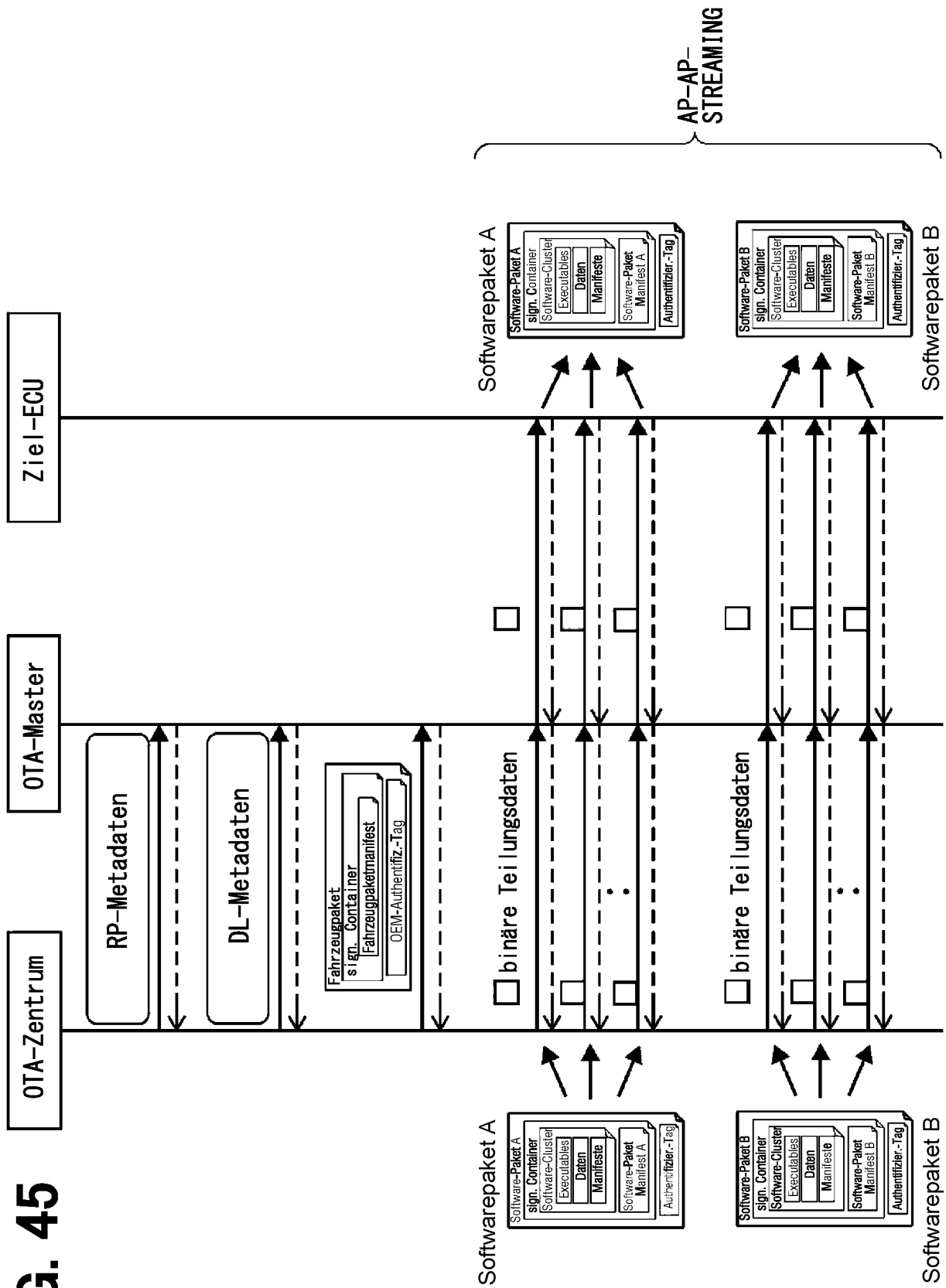


FIG. 46

■Neuprogrammierungs-Konzept-Metadatenversion :1.0.0/2.0.0/...	
■Verteilungsschicht	
1. Kommunikationsprotokoll	:Uptane/OMA-DM/SSL/... keins
2. Kommunikationsmittel	:Mobil/Smartphone/USB-Speicher
■Masterschicht (es kann mehrere Schichten geben)	
PF	:AP/CP/AGL/Android/...
Steuerungsverfahren	:Parameter/SCRIPT/...
Verschlüsselungsverfahren	
(1) Verschl.algorithmus	:AES, 3key-Trippl DES, CLEFIA (leichte Verschl.) etc.
(2) Verschl.schlüssellänge	:128 Bit, 256 Bit, etc.
(3) Verschl.modus	:CBC-Modus, CTR-Modus, OFB-Modus, etc.
(4) Padding-Verfahren	:PKCS#5-Padding, PKCS#7-Padding, kein Padding, etc.
(5) Verschl.schlüssel-ID	:1 (zum Identifizieren von Verschl.schlüssel verwendet)
(6) Signatur-Algorithmus	:MAC (gemeins. Schl.), DSA (öff. Schlüssel)
(7) Signatur-Schl.-ID	:2 (zum Identifizieren von Signaturschlüssel verwendet)
(8) Signaturmodus	:Cod. dann MAC, MAC dann Cod., Cod. und MAC, ...
(9) Hash-Algorithmus	:SHA2, SHA1,Photo (leichte Verschlüsselung)
(10) Regionenbezeichnung vorhanden/abwesend	:gesamte Datei auswählen oder Bereichsbezeichn.
(11) Offset-Größe	:0 (Datenbestimmung, von denen Byte von Kopf zu schützen ist: Nur wenn (9) spezifizierter Bereich ist)
(12) Schutzdatengröße	:1024 (Bestimmen,wieviele Bytes zu schützen sind: Nur wenn (9) spezifizierter Bereich ist)

FIG. 47

■ Zielschicht	(es kann mehrere Schichten geben)
PF	: AP/CP/AGL/Android/...
Übertragungsverfahren	: Speicherverfahren/Streaming-Verfahren/...
Steuerungsverfahren	: Parameter/SCRIPT /...
Ziel-ID	: (optional)
Verschlüsselungsverfahren	
(1) Verschl. algorithmus	: AES, 3key-Trippl DES, CLEFIA (leichte Verschl.), etc.
(2) Verschl. schlüssellänge	: 128 Bit, 256 Bit, etc.
(3) Verschl. modus	: CBC-Modus, CTR-Modus, OFB-Modus, etc.
(4) Padding-Verfahren	: PKCS#5-Padding, PKCS#7-Padding, kein Padding, etc. : 1 (zum
(5) Verschl. schlüssel-ID	Identifizieren von Verschlüsselungsschlüssel verwendet)
(6) Signaturalgorithmus	: MAC (gemeins. Schlüssel), DSA (öffentlicher Schlüssel)
(7) Signaturschlüssel-ID	: 2 (zum Identifizieren von Signaturschlüssel verwendet)
(8) Signaturmodus	: Cod. dann MAC, MAC dann Cod., Cod. und MAC, ...
(9) Hash-Algorithmus	: SHA2, SHA1, Photo (leichte Verschlüsselung)
(10) Regionenbezeichnung vorhanden/abwesend	: gesamte Datei auswählen oder Bereichsbezeichn.
(11) Offset-Größe	: 0 (Datenbestimmung, von denen Byte von Kopf zu schützen ist: Nur wenn (9) spezifizierter Bereich ist)
(12) Schutzdatengröße	: 1024 (Bestimmen, wieviele Bytes zu schützen sind: Nur wenn (9) spezifizierter Bereich ist)

FIG. 48

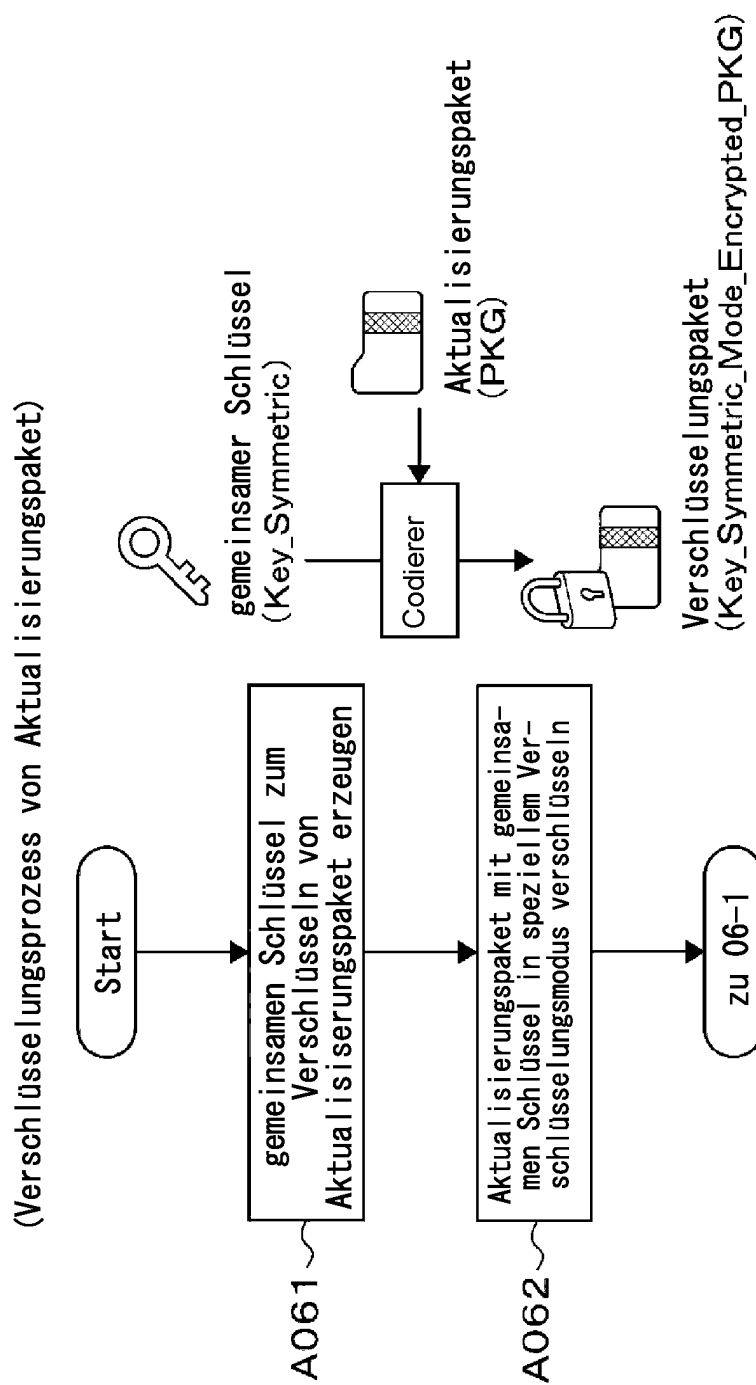


FIG. 49

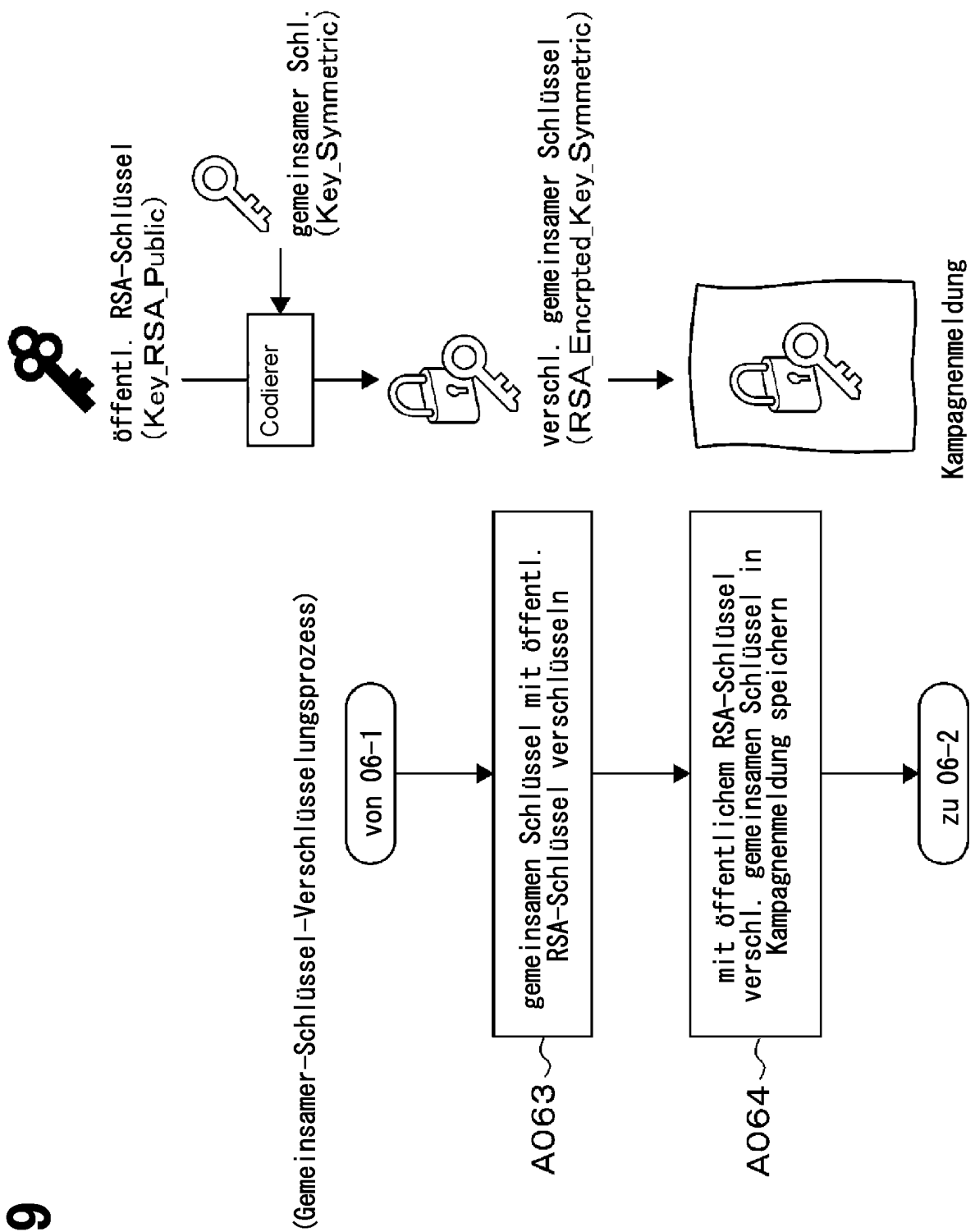


FIG. 50

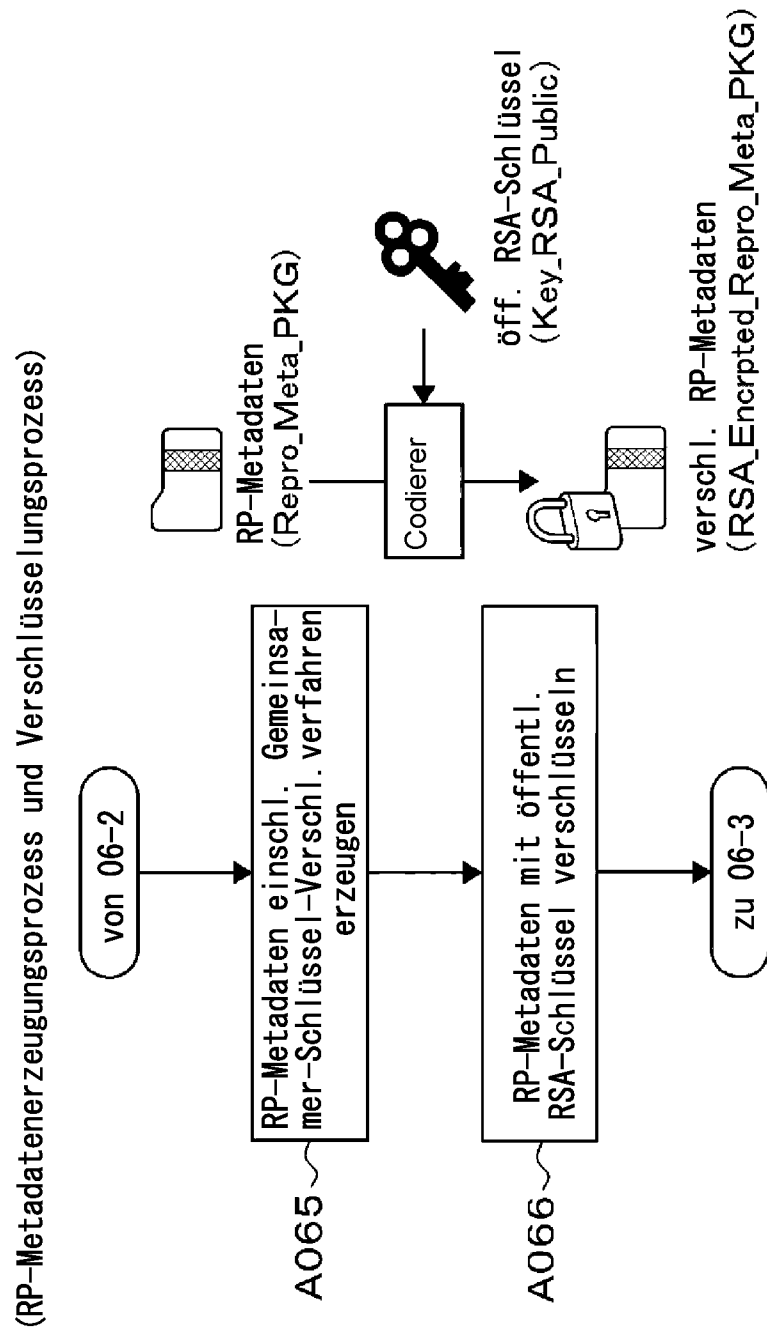


FIG. 51

(CDN-Platzierungsprozess von Verschlüsselungspaket und Verschlüsselungs-RP-Metadaten und Übertragungsprozess von Kampagnenmeldung)

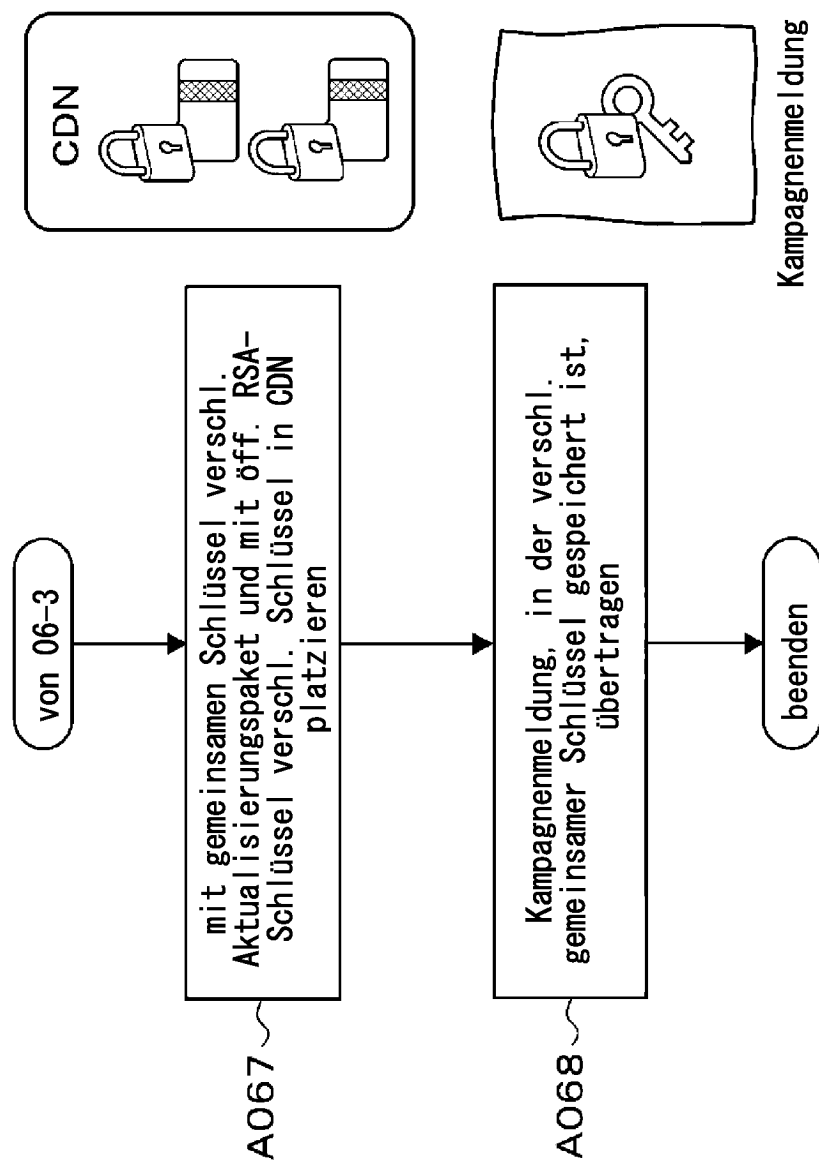


FIG. 52

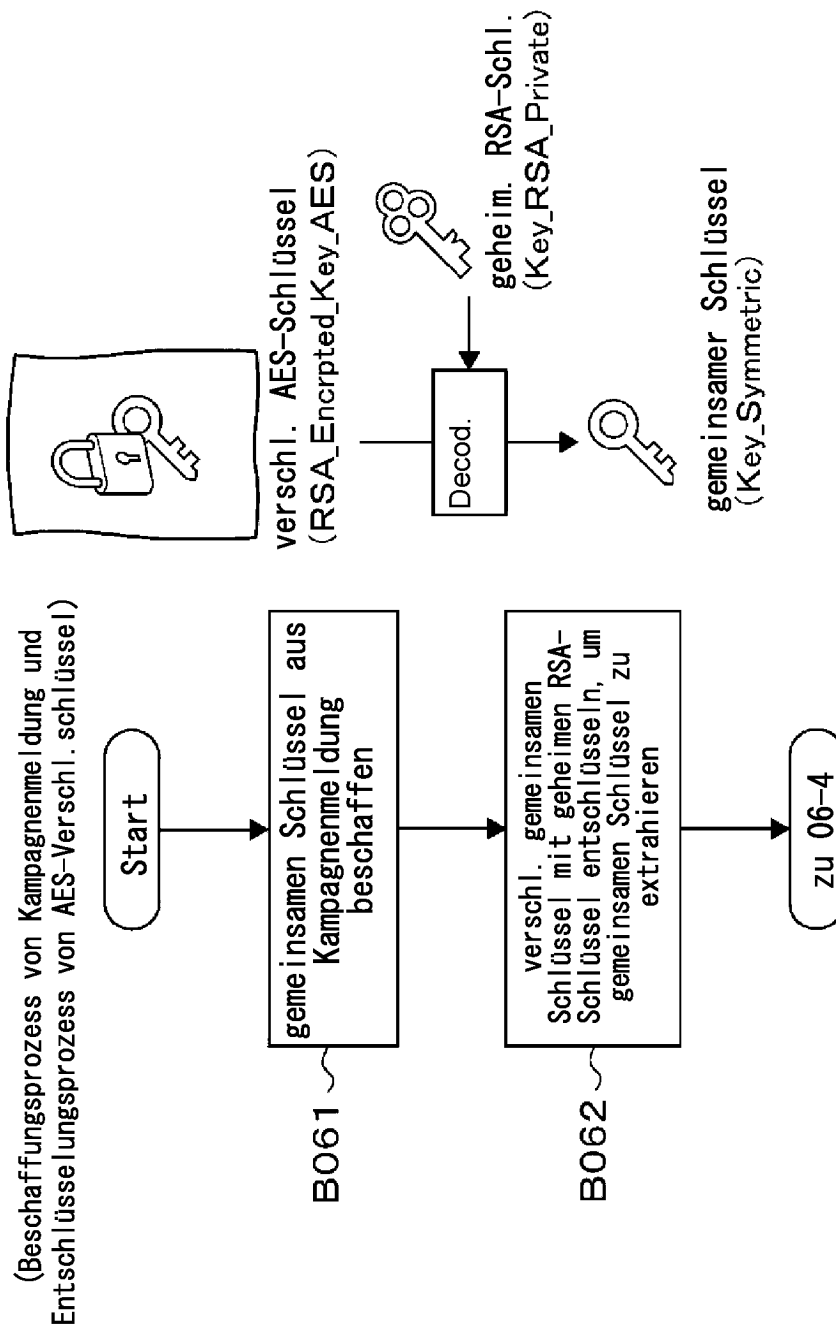


FIG. 53

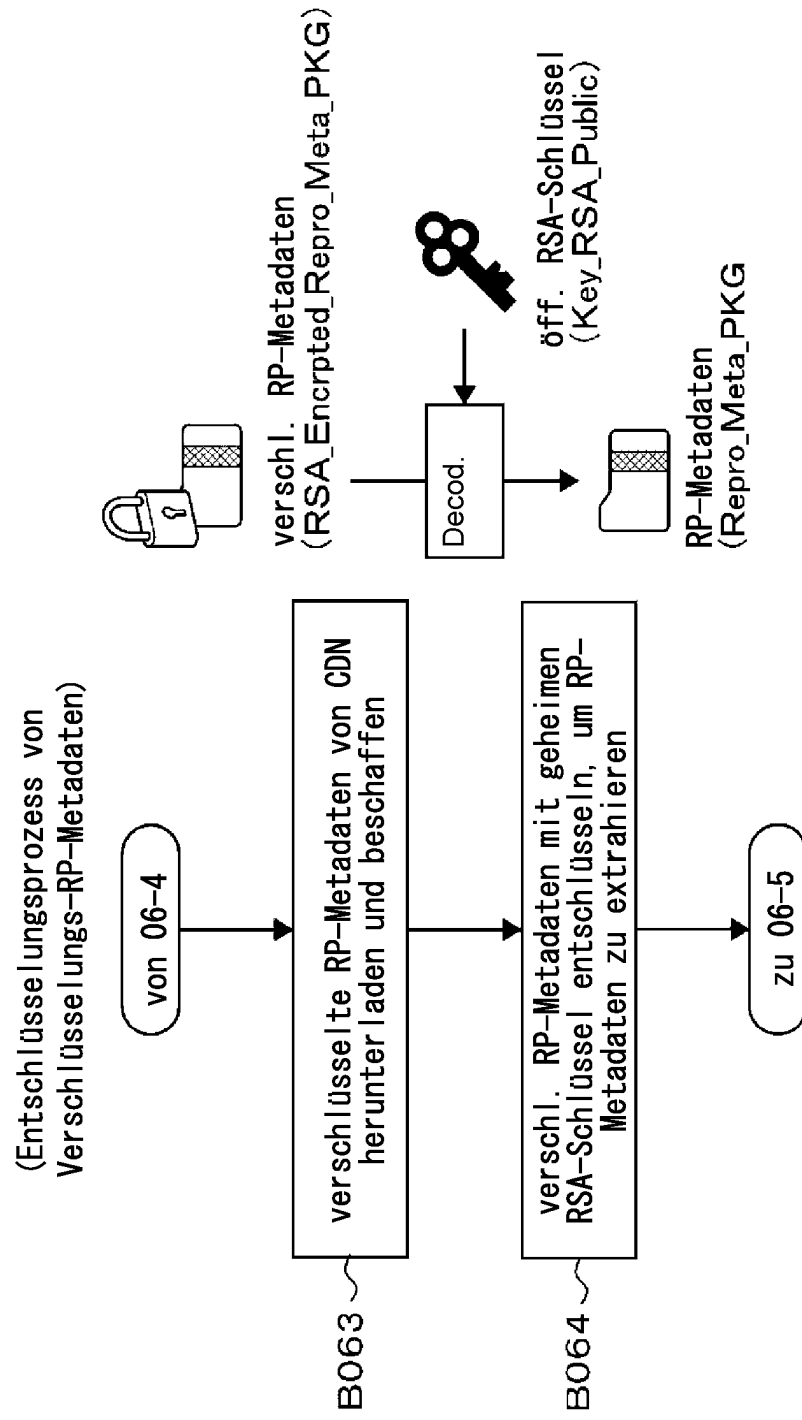


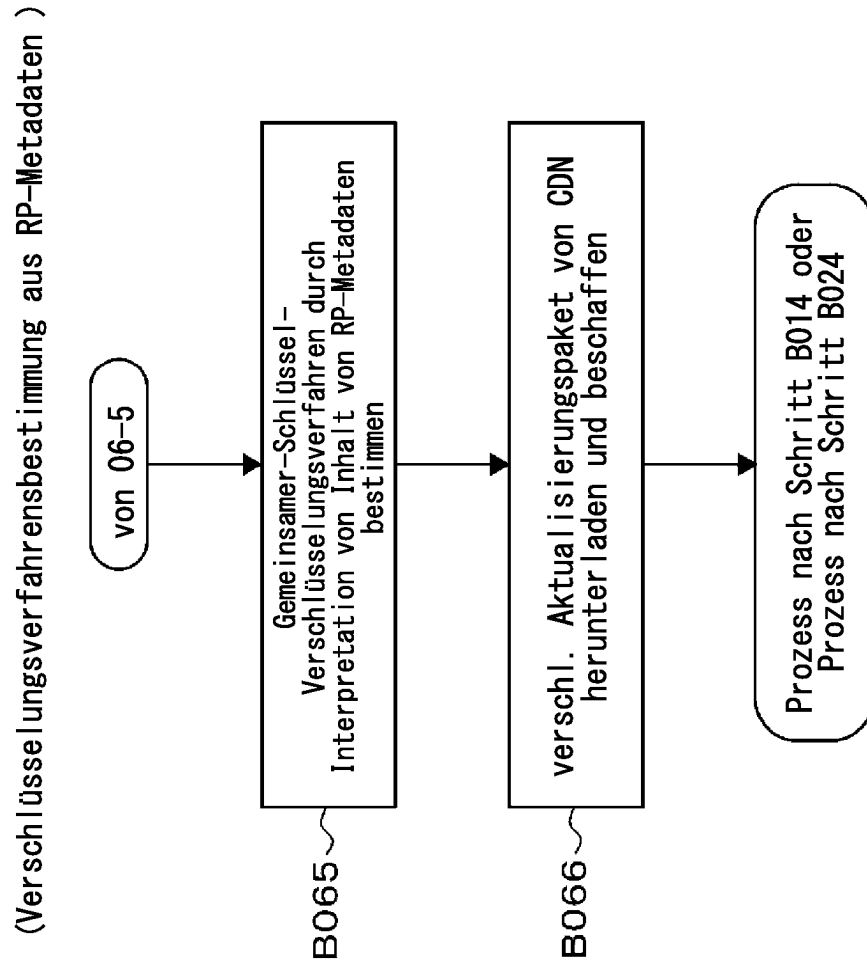
FIG. 54

FIG. 55

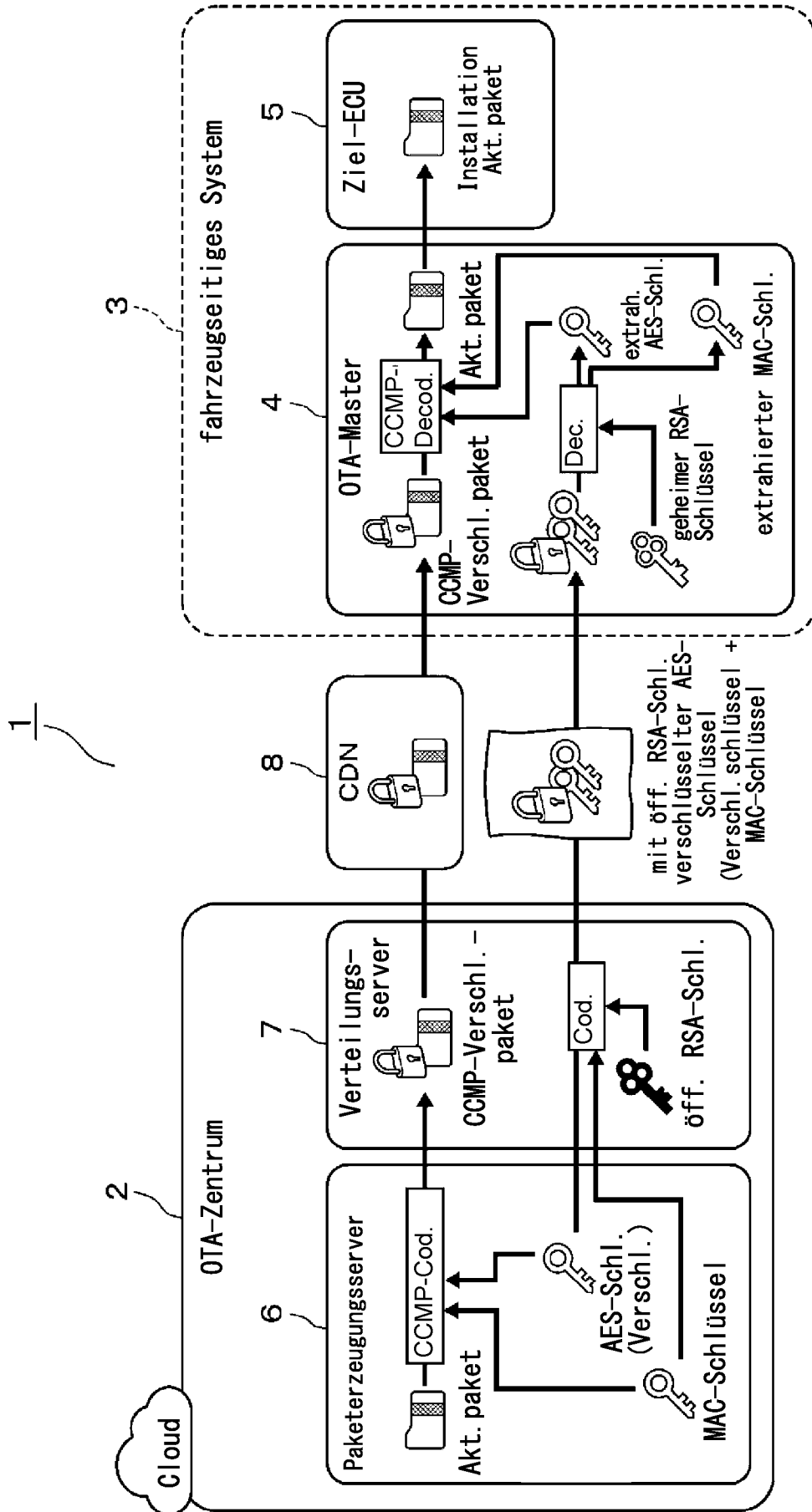


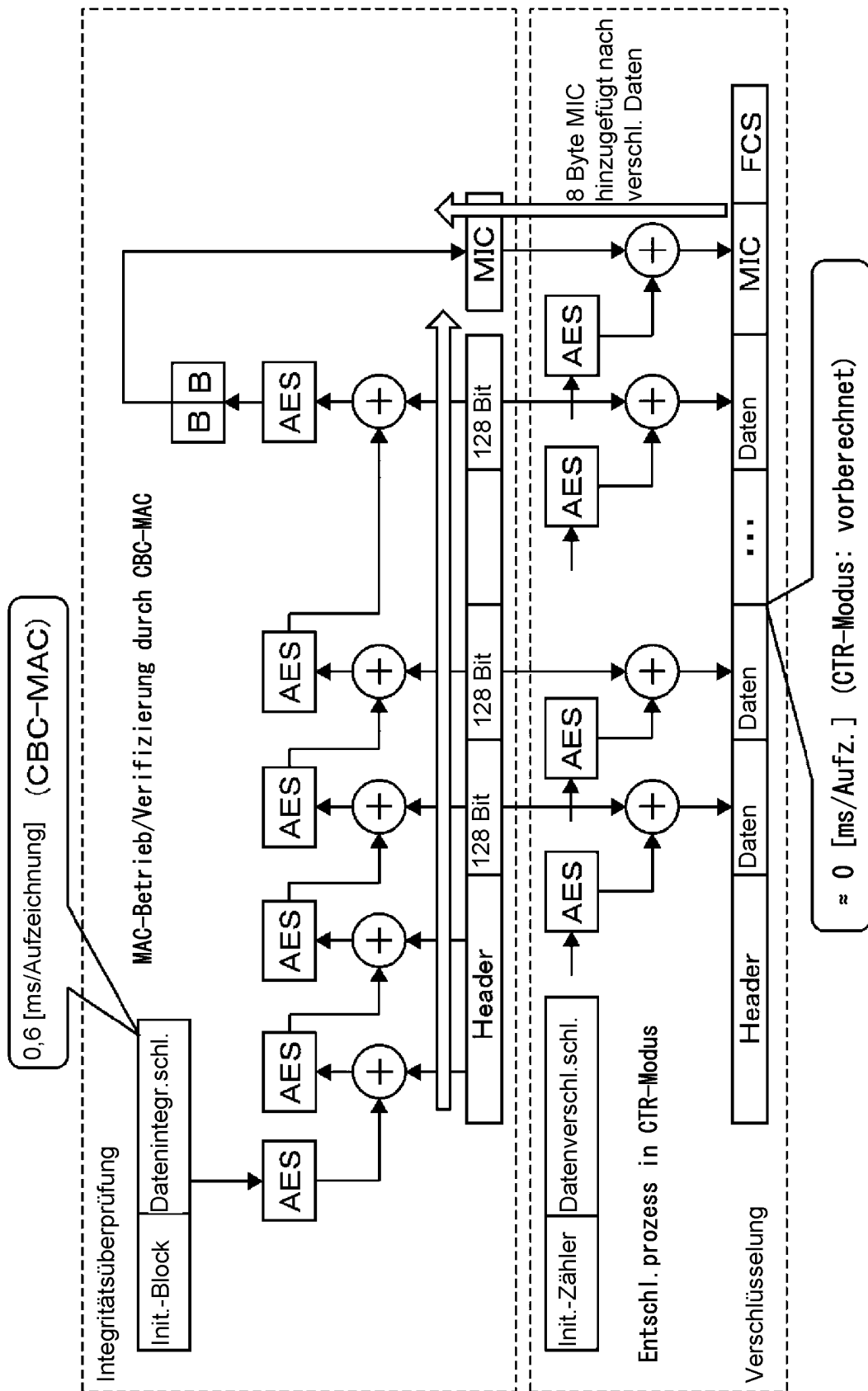
FIG. 56

FIG. 57

Schätzung von Durchsatz in CMP-Modus

AES-Entschlüsselung vernachlässigbar, da CTR-Modus (Ordnung von wenigen + μ s)

	Hauptkern	HW-Beschleuniger
Empfang (Entschlüssel.- und MAC-Betriebsprozess)	613 [μ s]	0,6 [ms] (AES-Entschl. $\approx$ 0 ms + CBC-MAC 0,6 ms)

Durchsatz hier berechnen, da Verarbeitungszeit von HW-Beschleuniger im Vergleich zu Hauptkern dominant ist
Datenmenge: 15.796 [Byte]
Verarbeitungszeit von Ethernet-Frame $1518 \times 11 = 16.698$ [Byte] ist 613 [μ s] + 0,6 [ms] = 1,2 [ms].

->Datendurchsatz: $15.796 \text{ [B]} \times 8 \text{ [Bit/B]} \div (1,2/1000) \text{ [s]} \approx 105 \text{ [Mbps]}$

FIG. 58

AES CBC-HMAC SHA2 Entschlüsselung/Signaturverifizierung

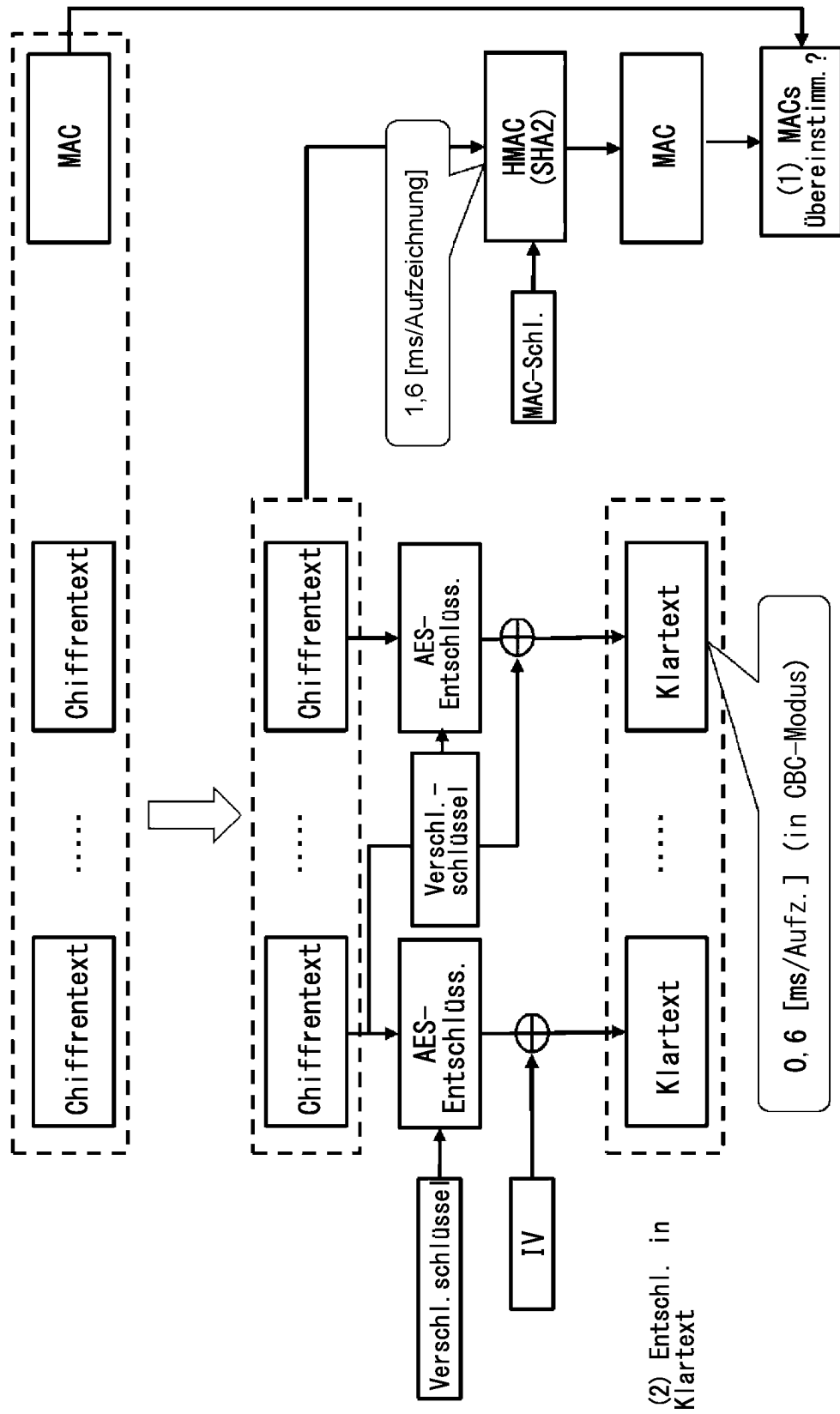


FIG. 59

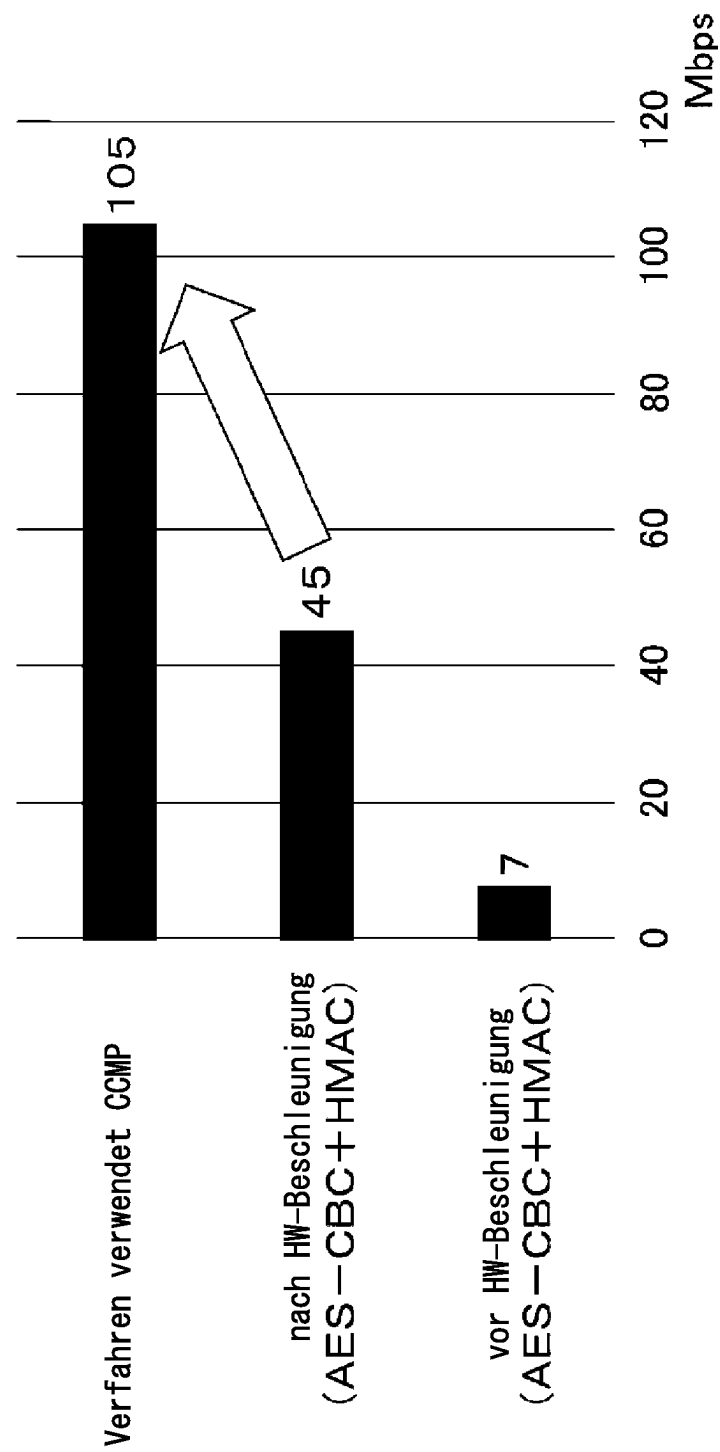
Schätzung von Durchsatz gemäß herkömmlichen Verfahren

	Hauptkern	HW-Beschleuniger
Empfang (Entschlüssel.- und MAC-Betriebsprozess)	613 [μs]	2,2 [ms] (= AES-Entschl. 0,6 ms + HMAC 1,6 ms)

Durchsatz hier berechnen, da Verarbeitungszeit von HW-Beschleuniger im Vergleich zu Hauptkern dominant ist
Datenmenge: 15.796 [Byte]

Verarbeitungszeit von Ethernet-Frame $1518 \times 11 = 16.698$ [Byte] ist 613 [us] + 2,2 [ms] = 2,8 [ms].

→Datendurchsatz: $15.796 \text{ [B]} \times 8 \text{ [bit/B]} \div (2,8/1000) \text{ [s]} \approx 45 \text{ [Mbps]}$

FIG. 60

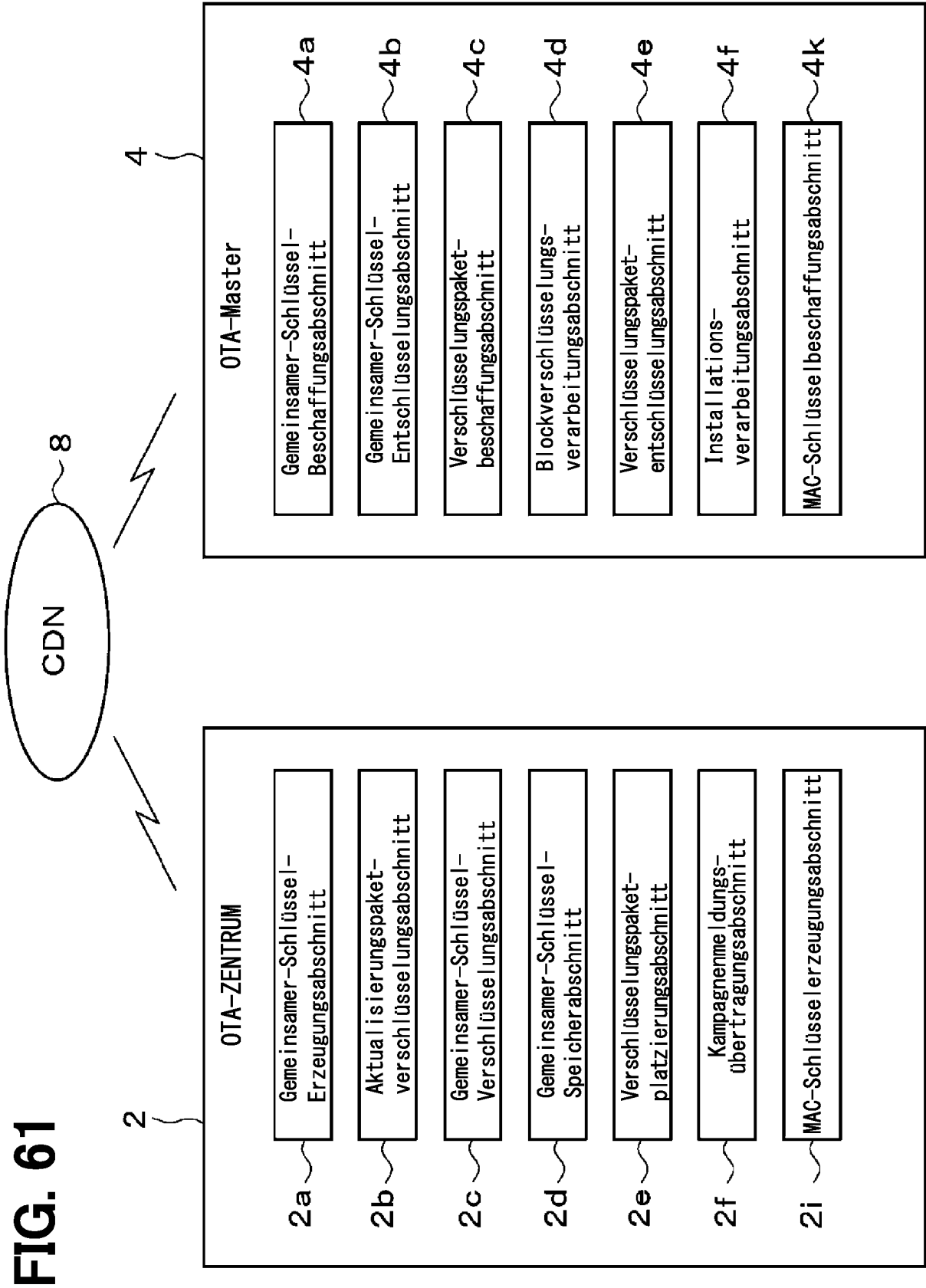


FIG. 62

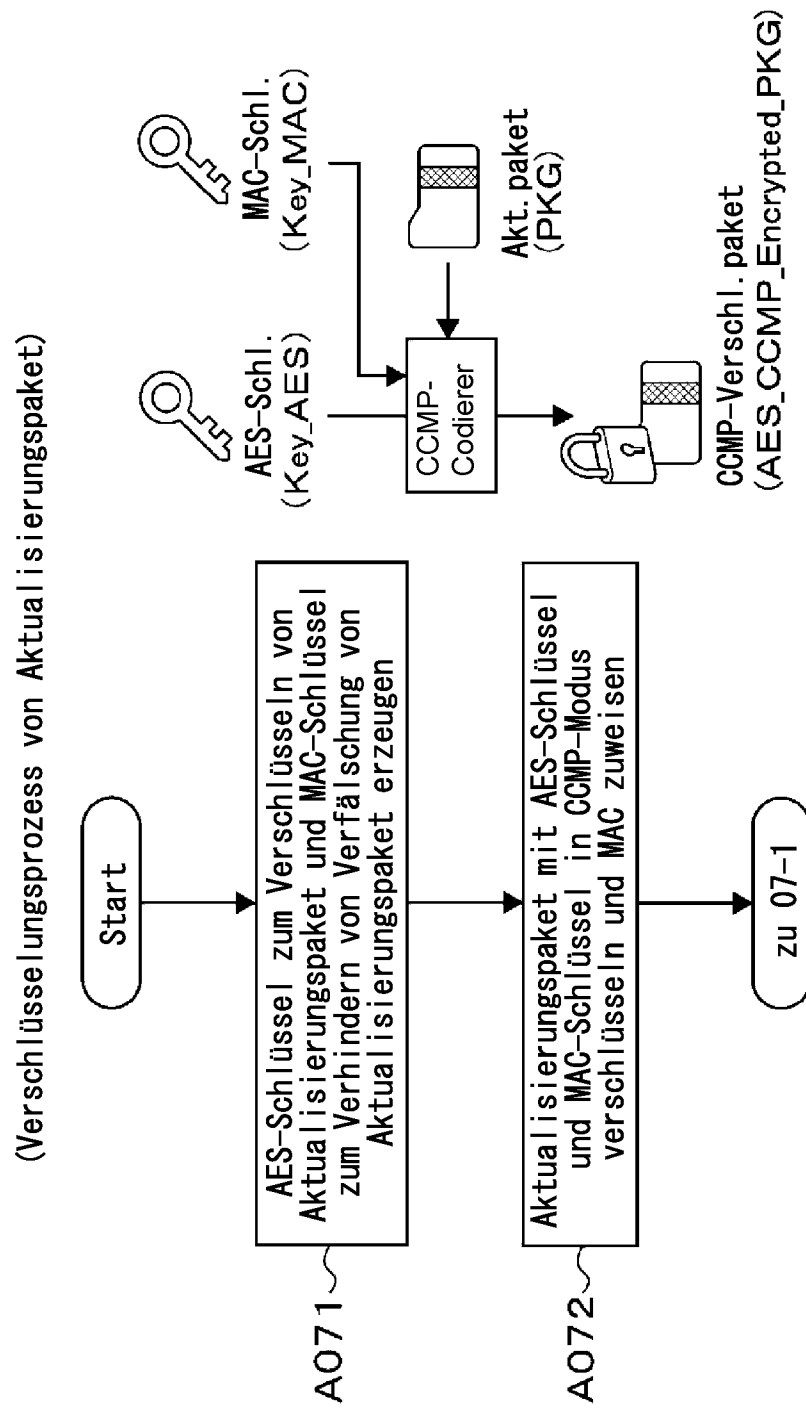


FIG. 63

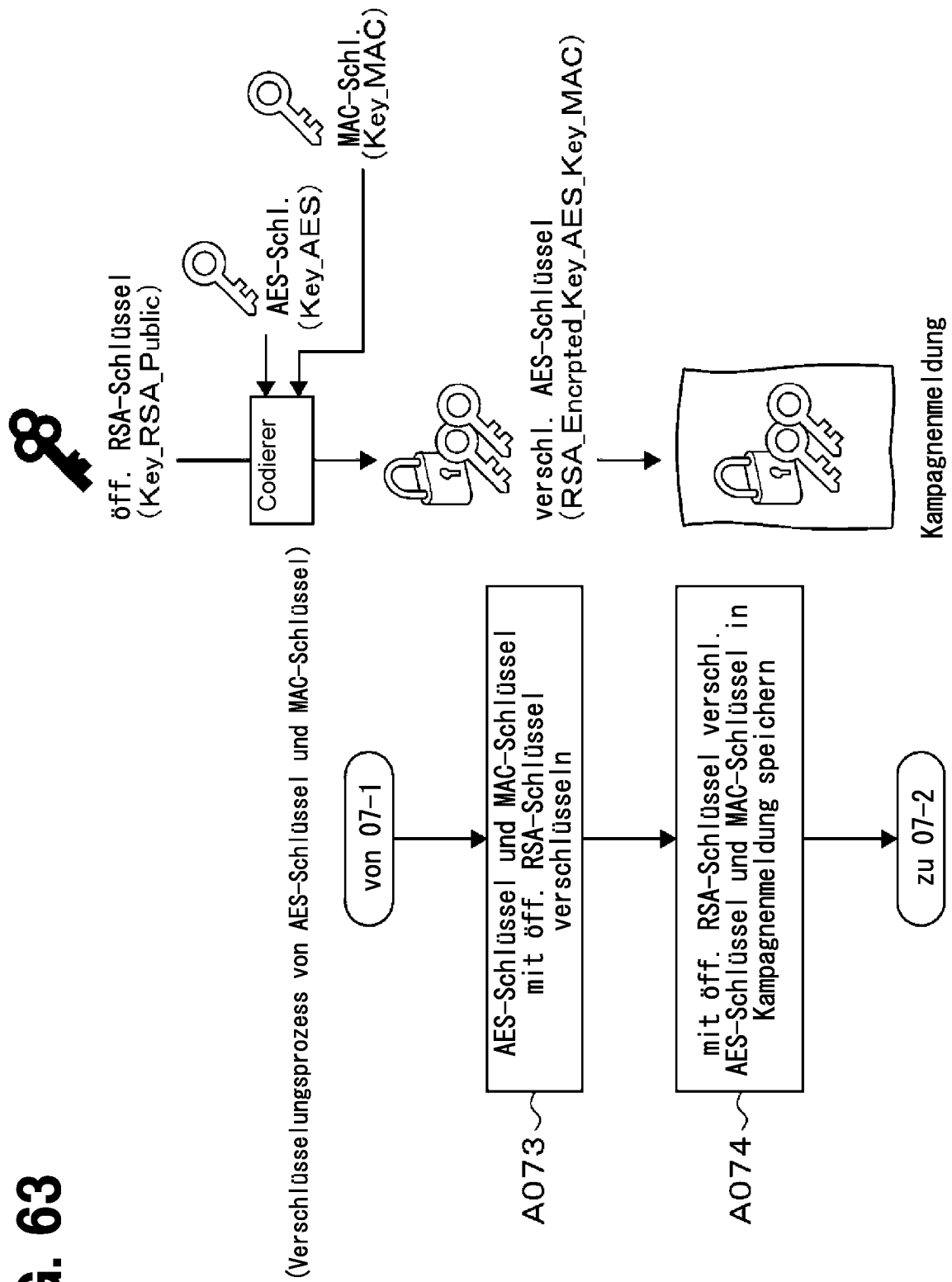


FIG. 64

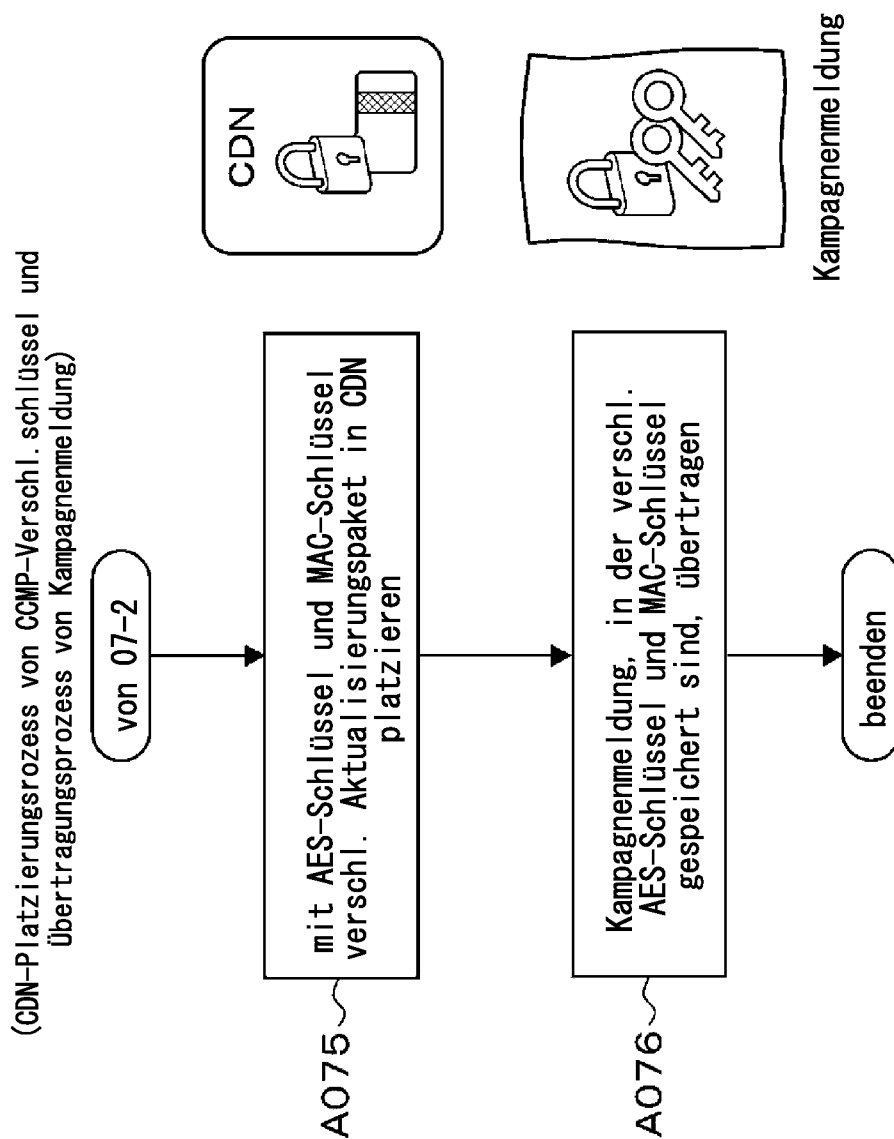


FIG. 65

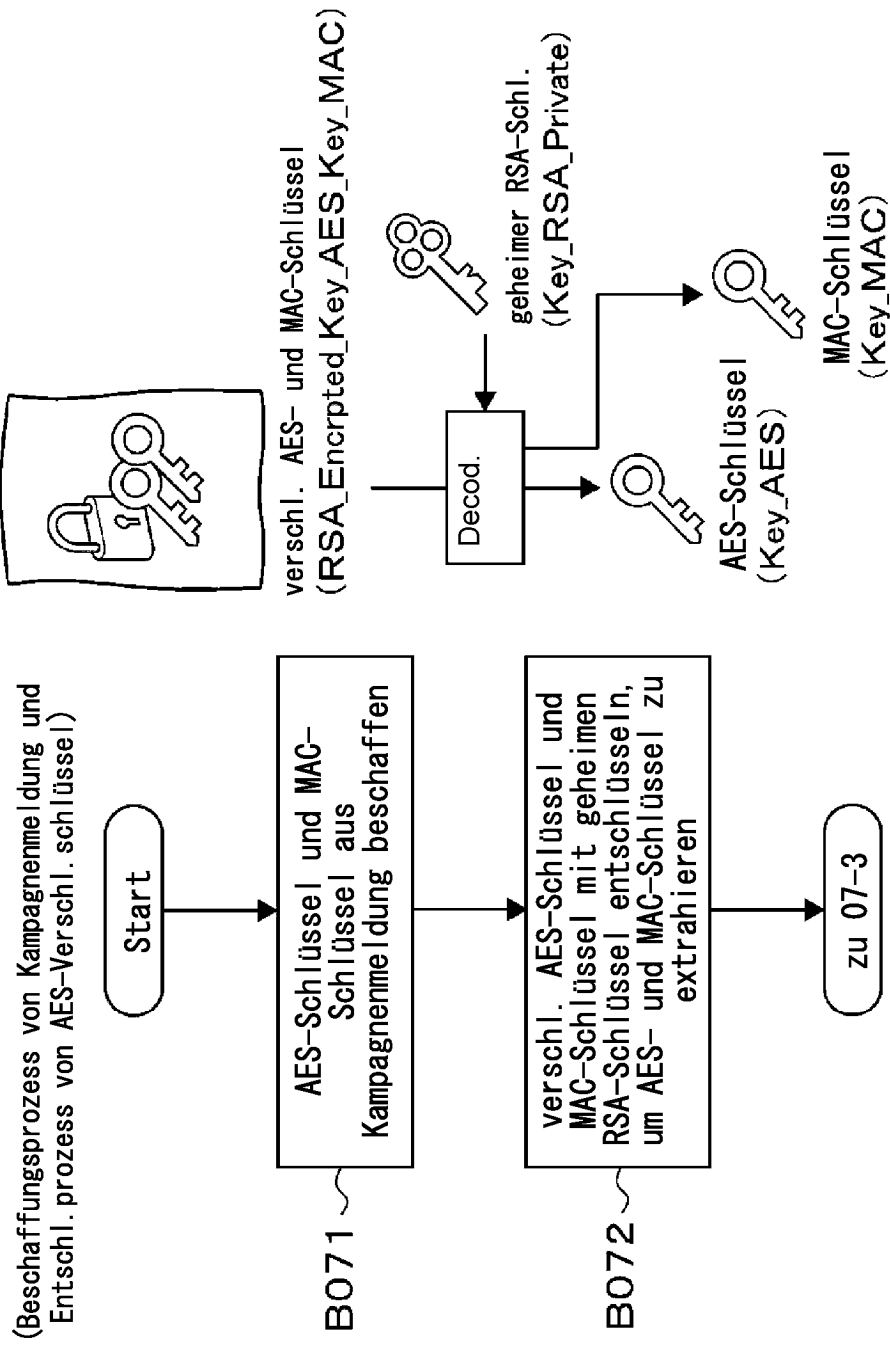


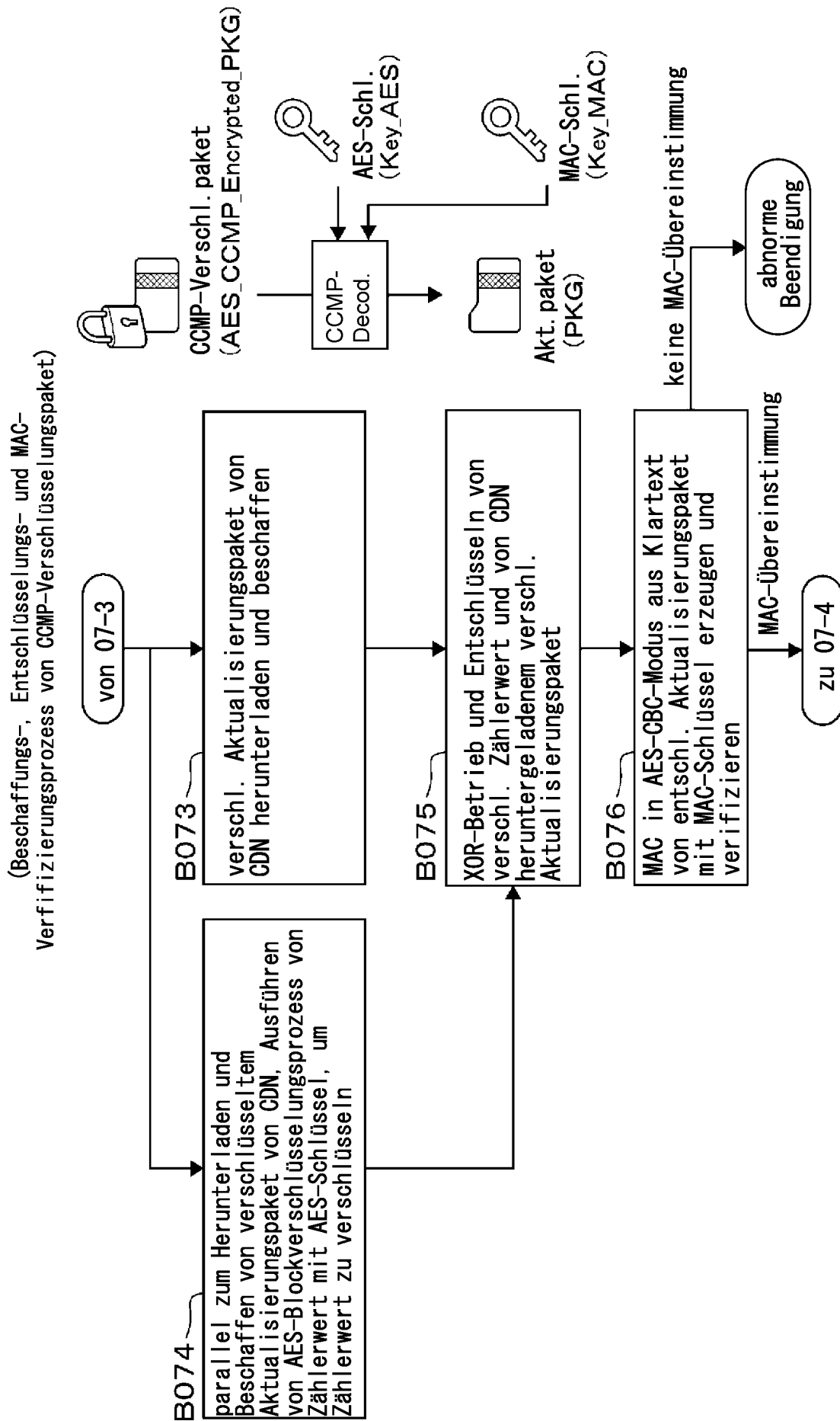
FIG. 66

FIG. 67

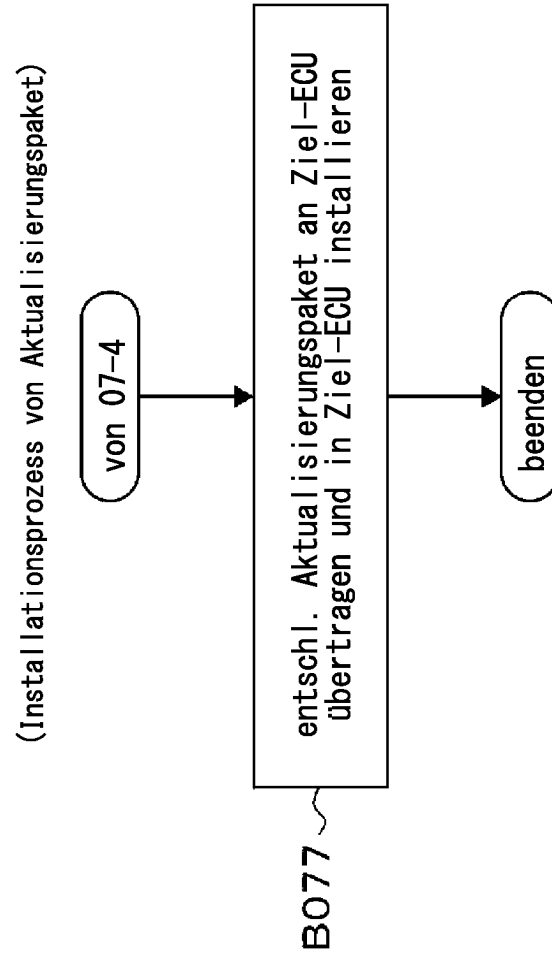


FIG. 68

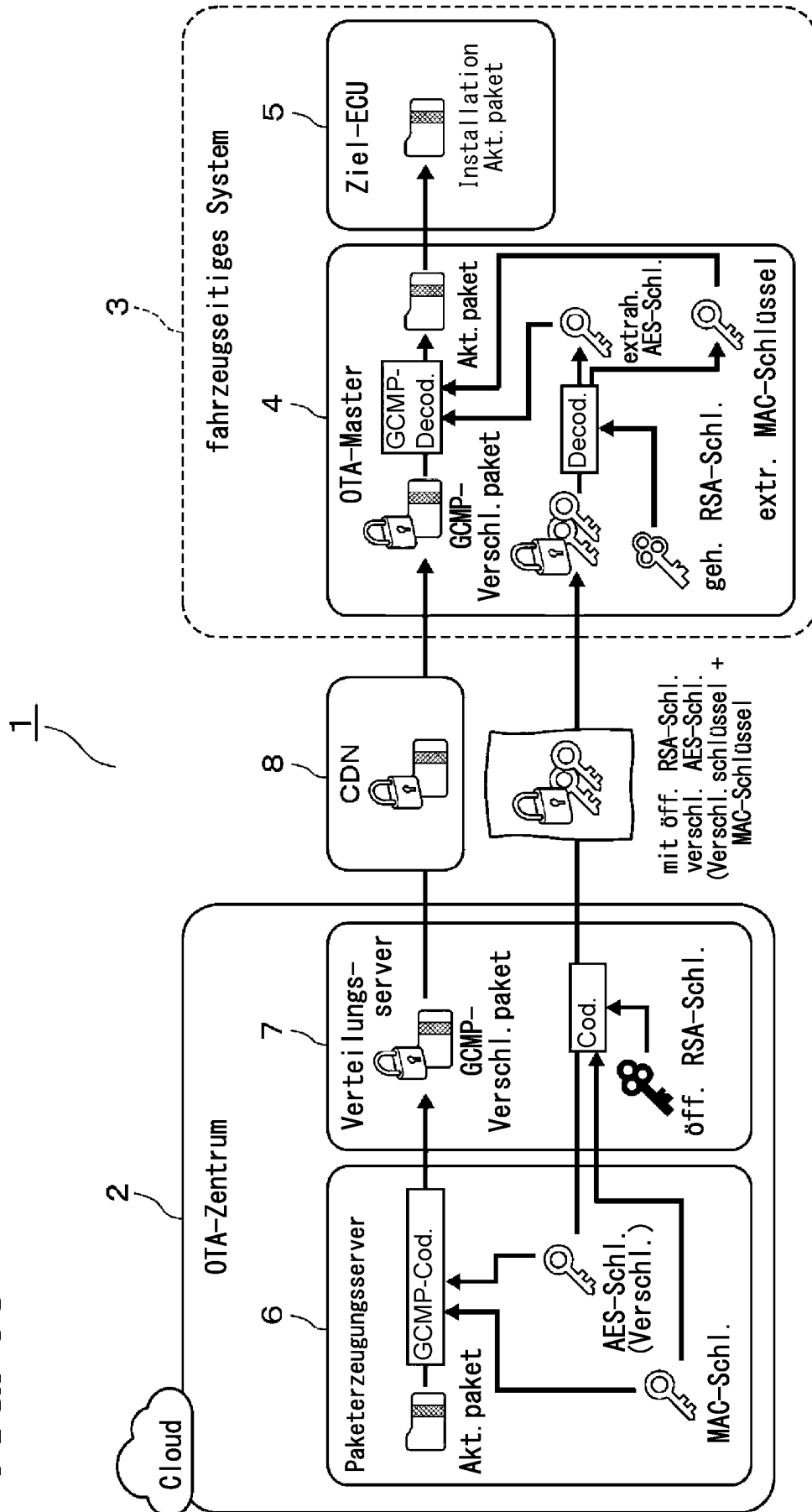


FIG. 69

Entschlüsselung mit AES in CTR

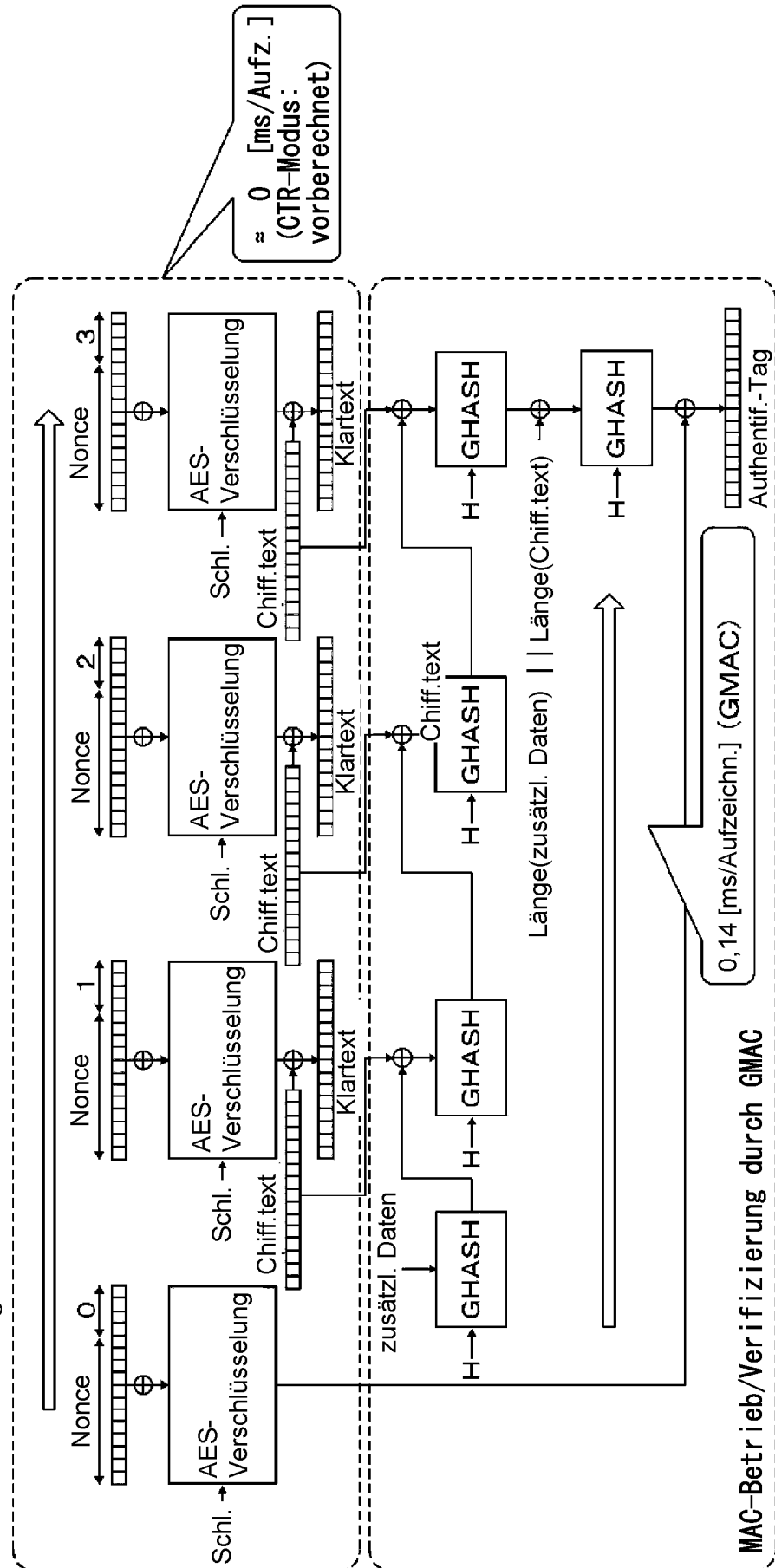


FIG. 70

Schätzung von Durchsatz in GCM-Modus

AES-Entschlüsselung vernachlässigbar, da CTR-Modus (Ordnung von wenigen + μ s)



	Hauptkern	HW-Beschleuniger
Empfang (Entschl. + MAC-Betriebsprozess)	613 [μ s]	0,6 [ms] (AES-Verschl. $\approx$ 0 ms + GMAC 0,14 ms)

Durchsatz hier berechnen, da Verarbeitungszeit von HW-Beschleuniger im Vergleich zu Hauptkern dominant ist
Datenmenge: 15.796 [Byte]
Verarbeitungszeit von Ethernet-Frames $1518 \times 11 = 16$ und 698 [Byte] ist 613 [μ s] + 0,14 [ms] = 0,75 [ms].
→ Datendurchsatz: $15.796 \text{ [B]} \times 8 \text{ [bit/B]} \div (0,75/1000) \text{ [s]} \approx 170 \text{ [Mbps]}$

FIG. 71

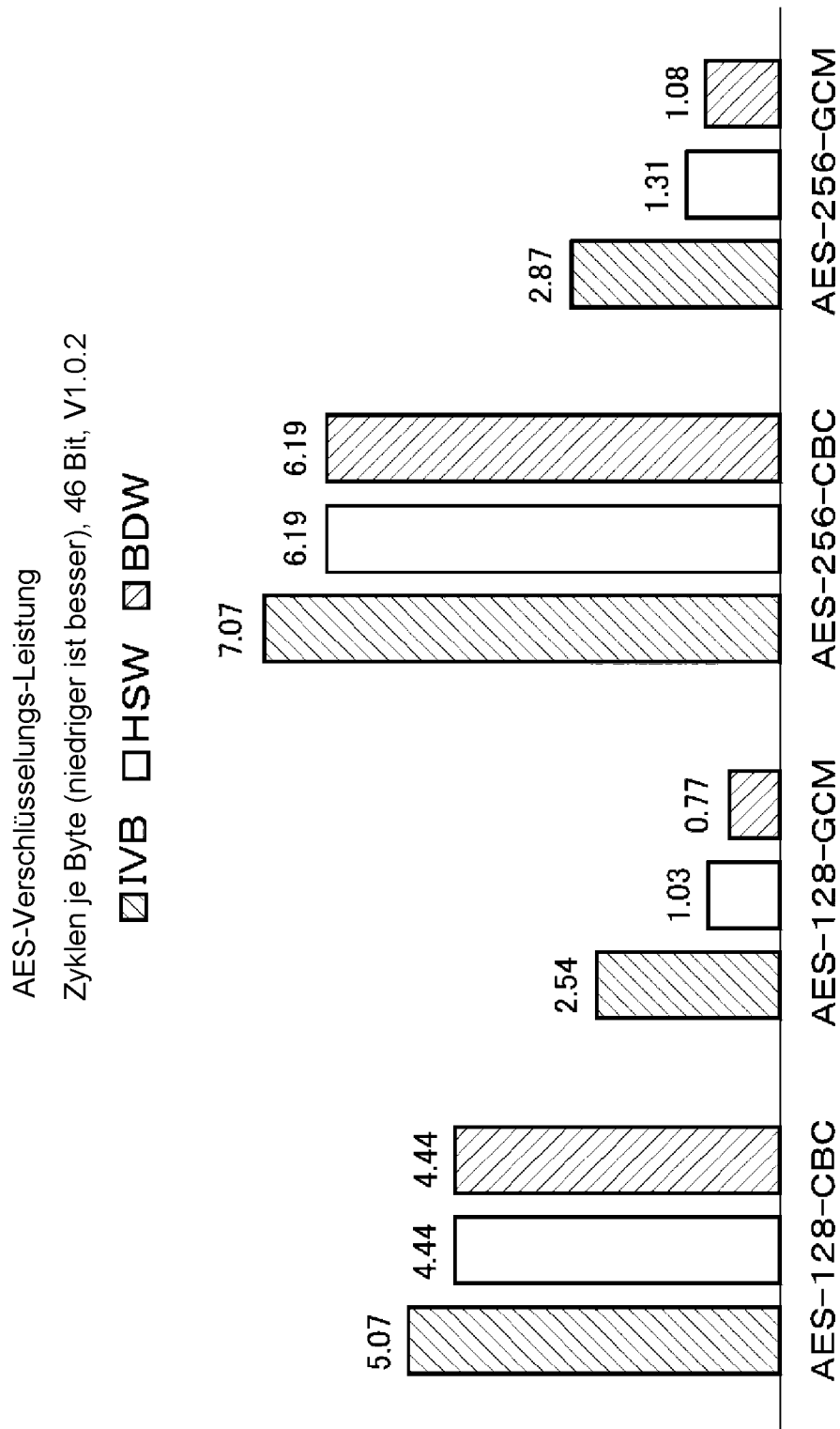


FIG. 72

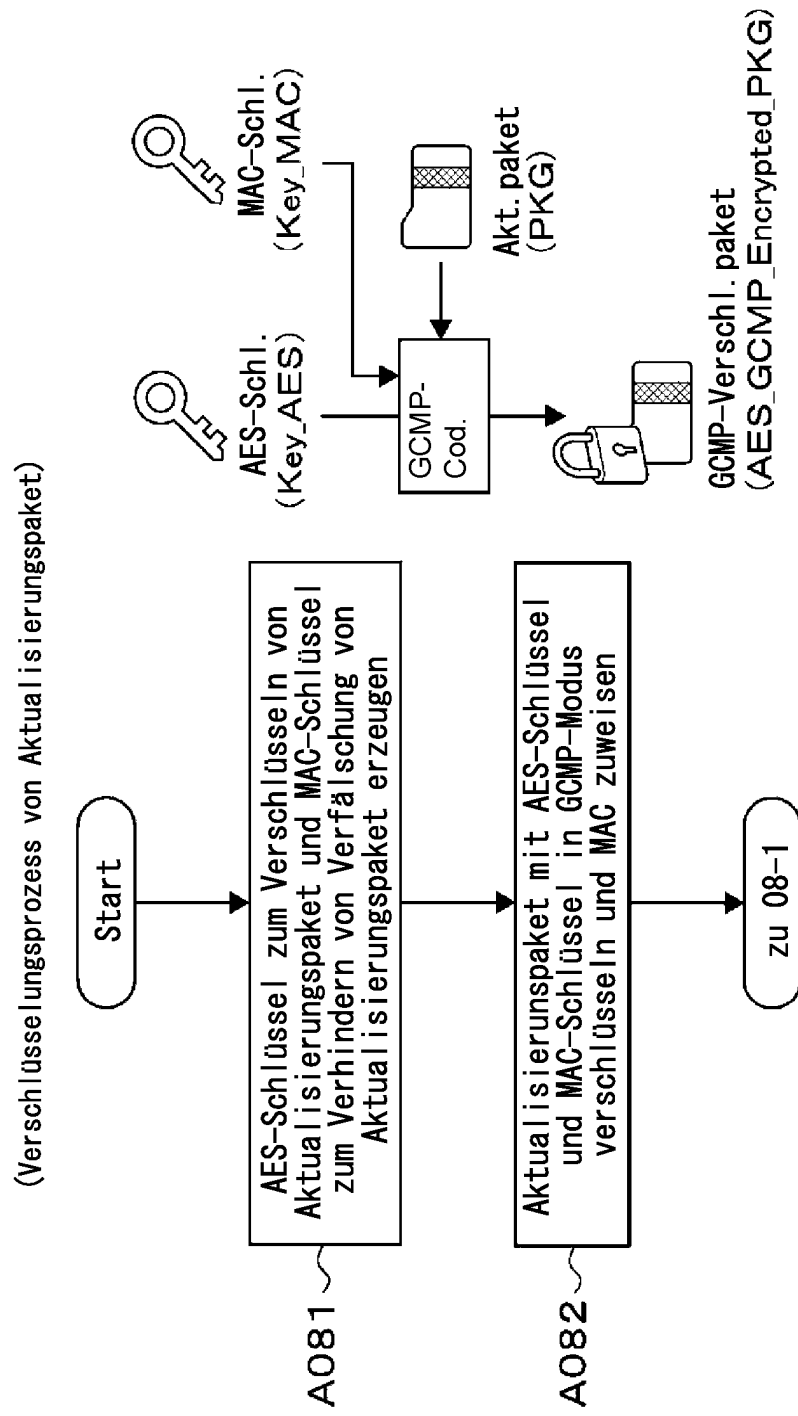


FIG. 73

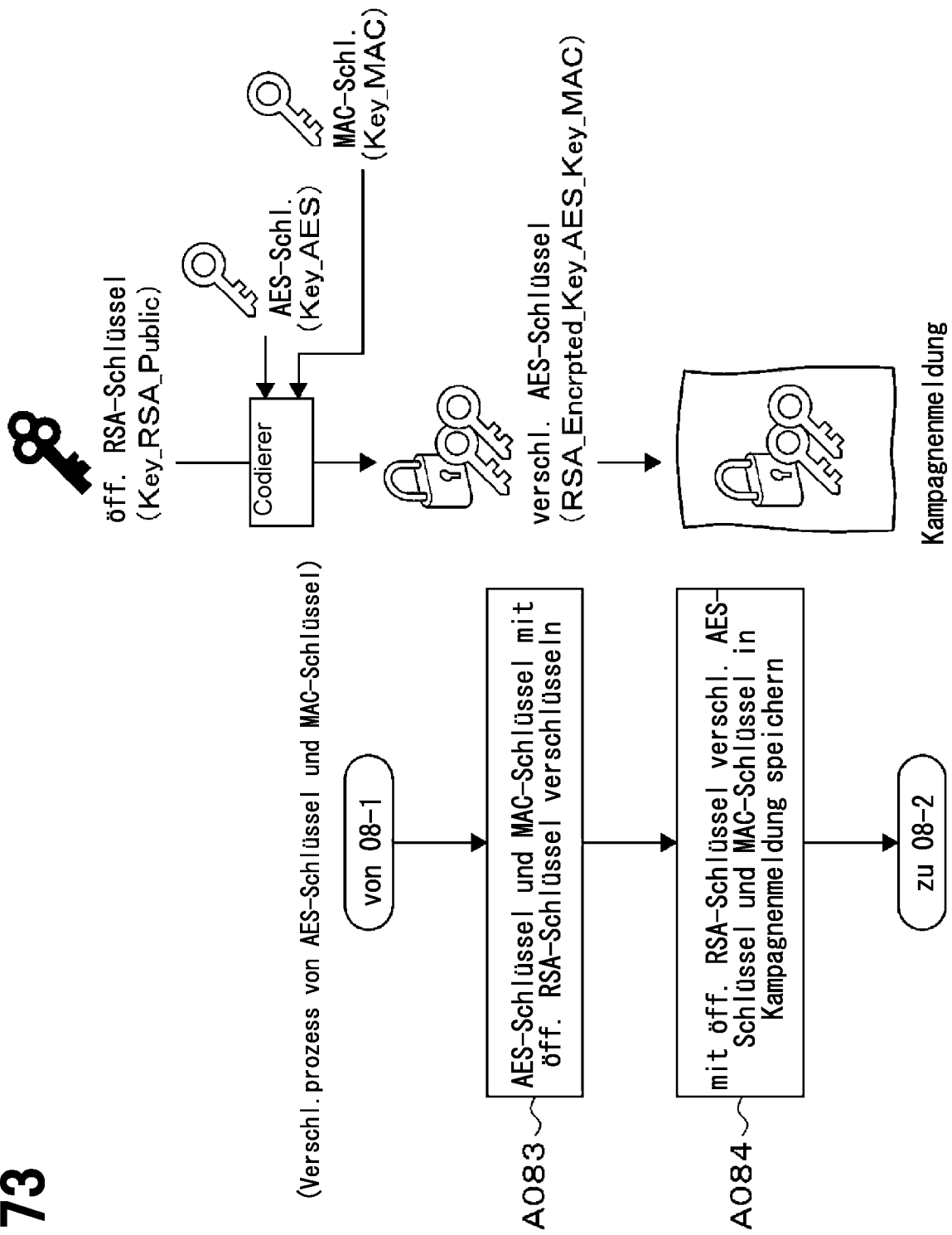


FIG. 74

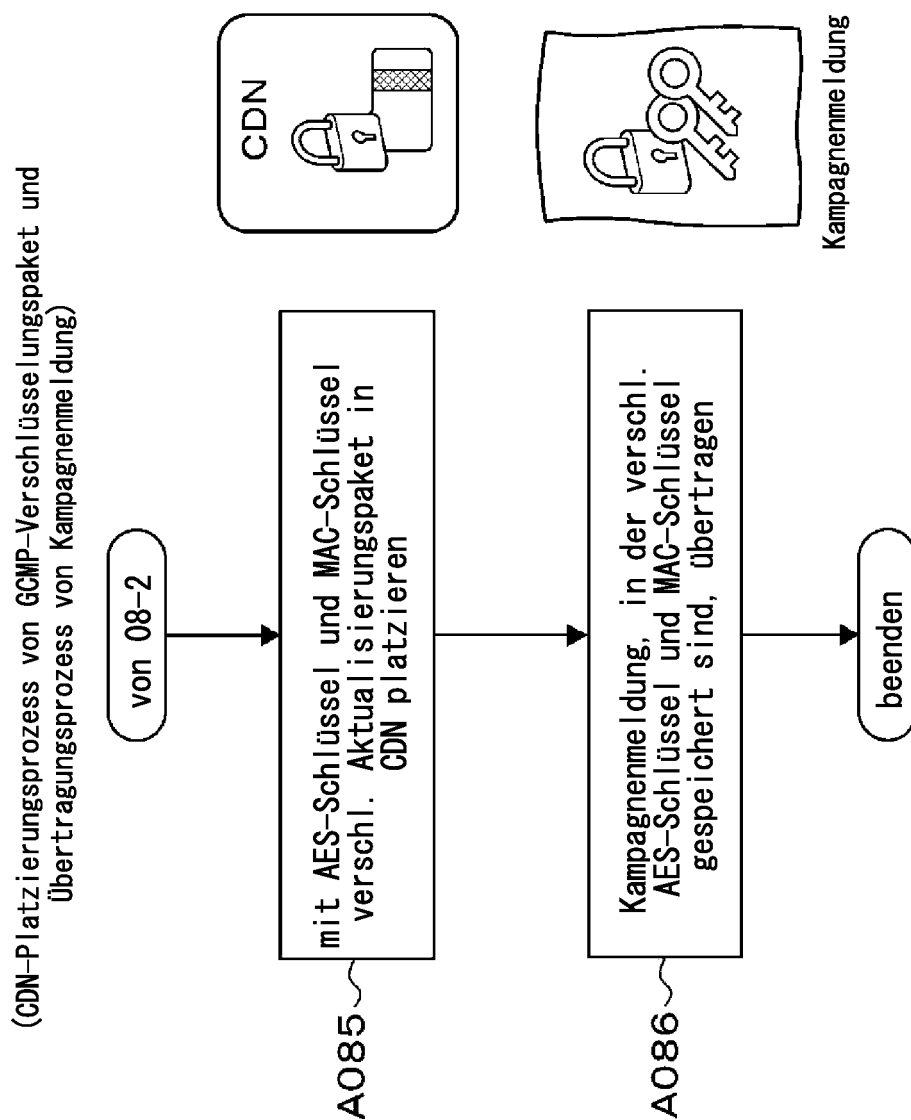


FIG. 75

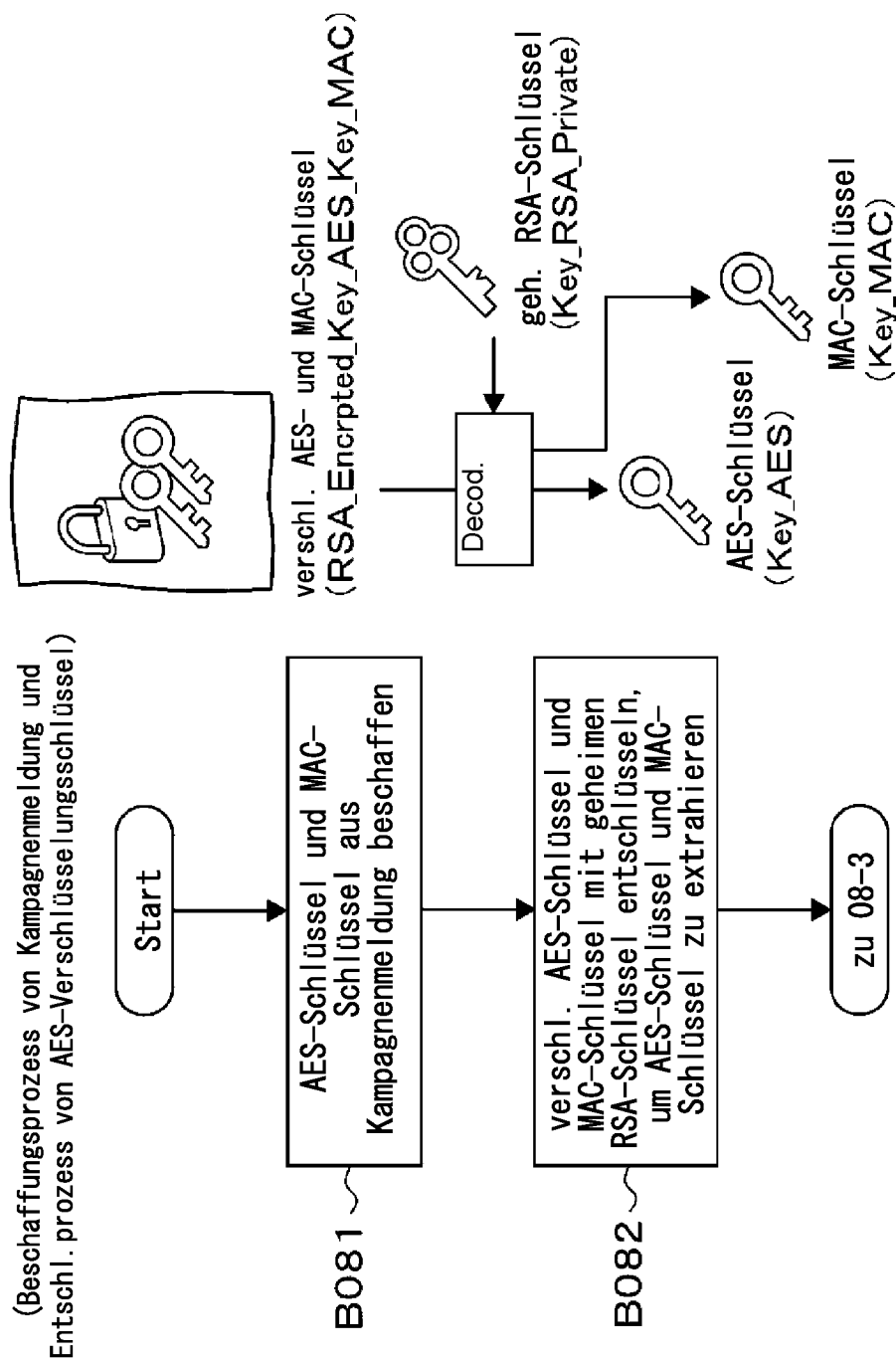


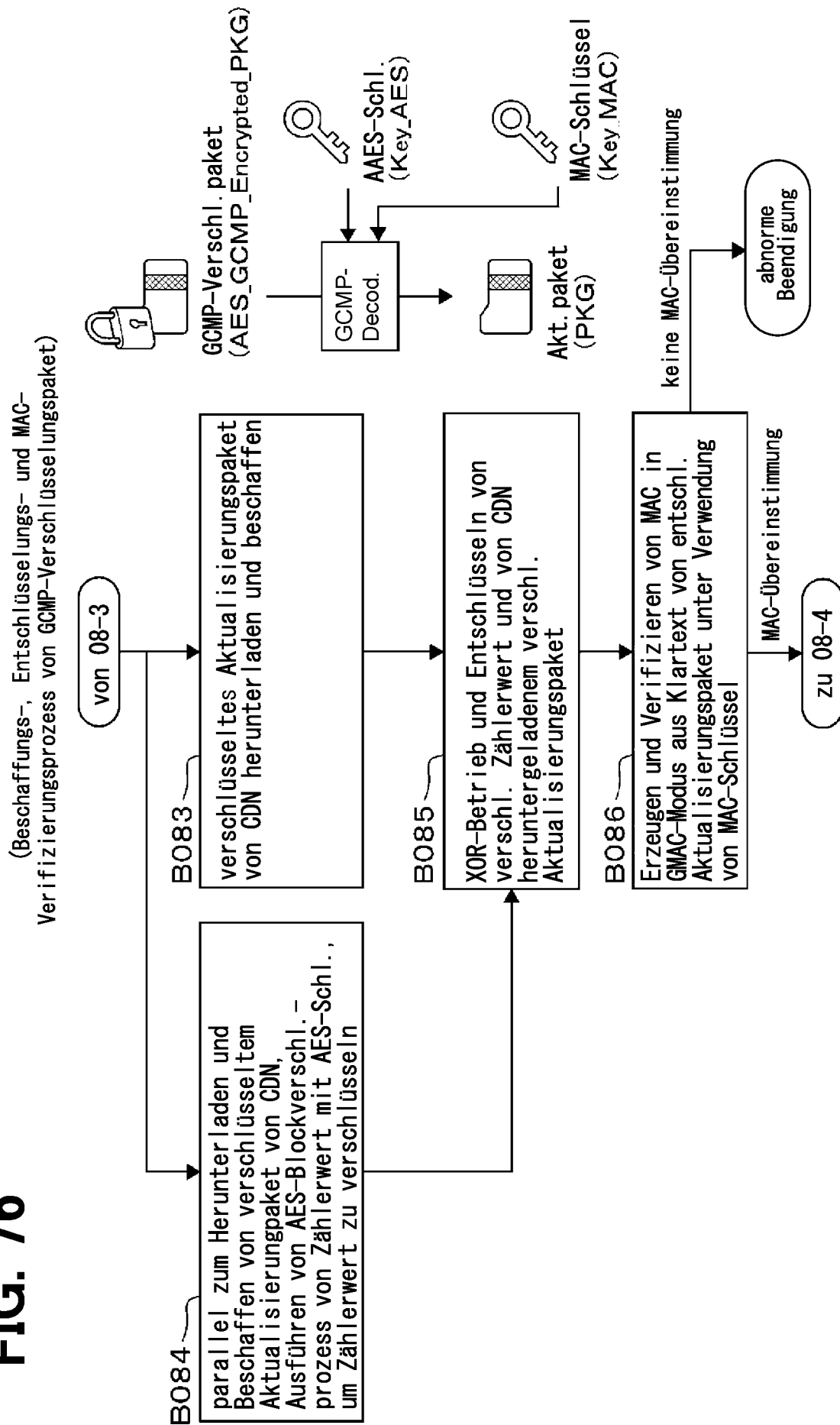
FIG. 76

FIG. 77

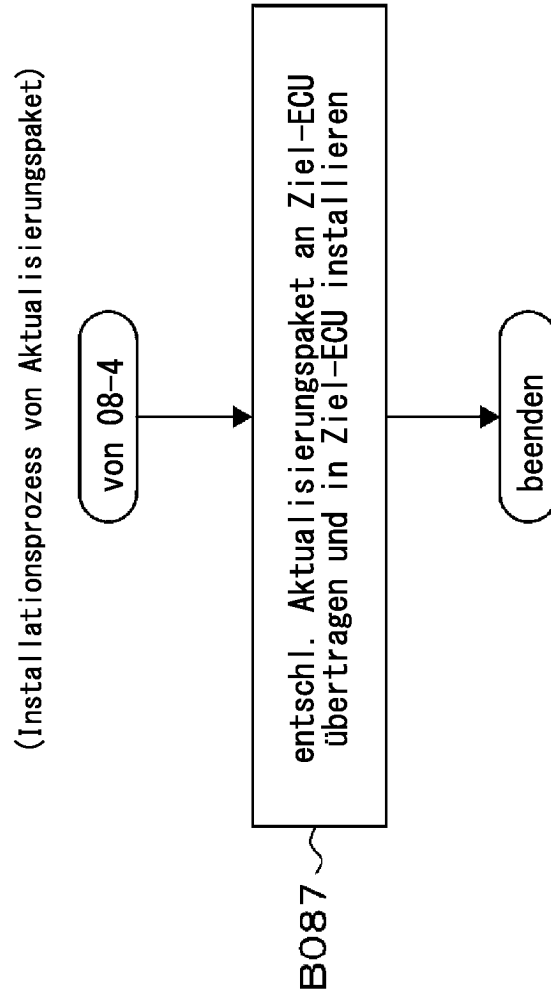


FIG. 78

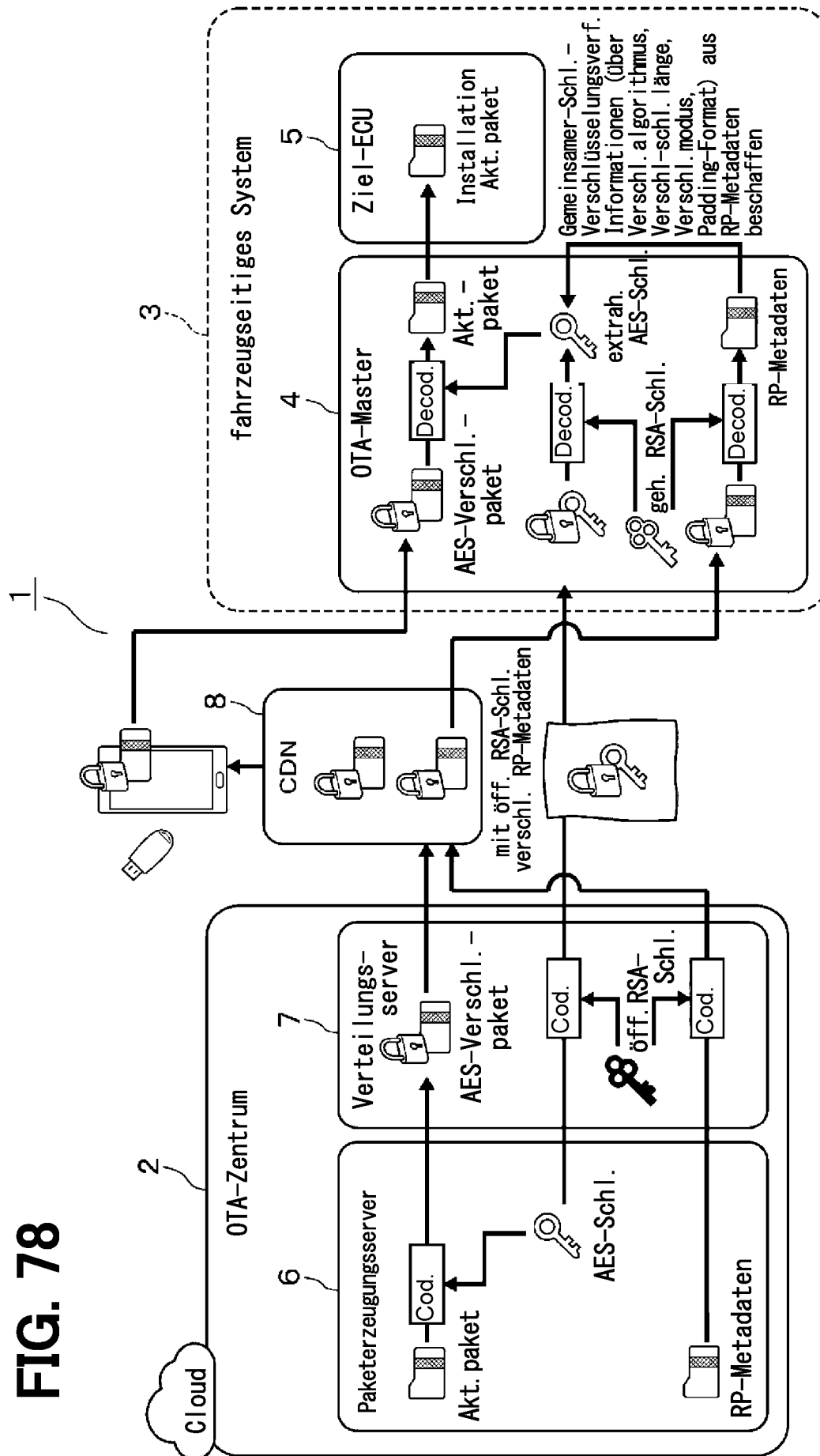


FIG. 79

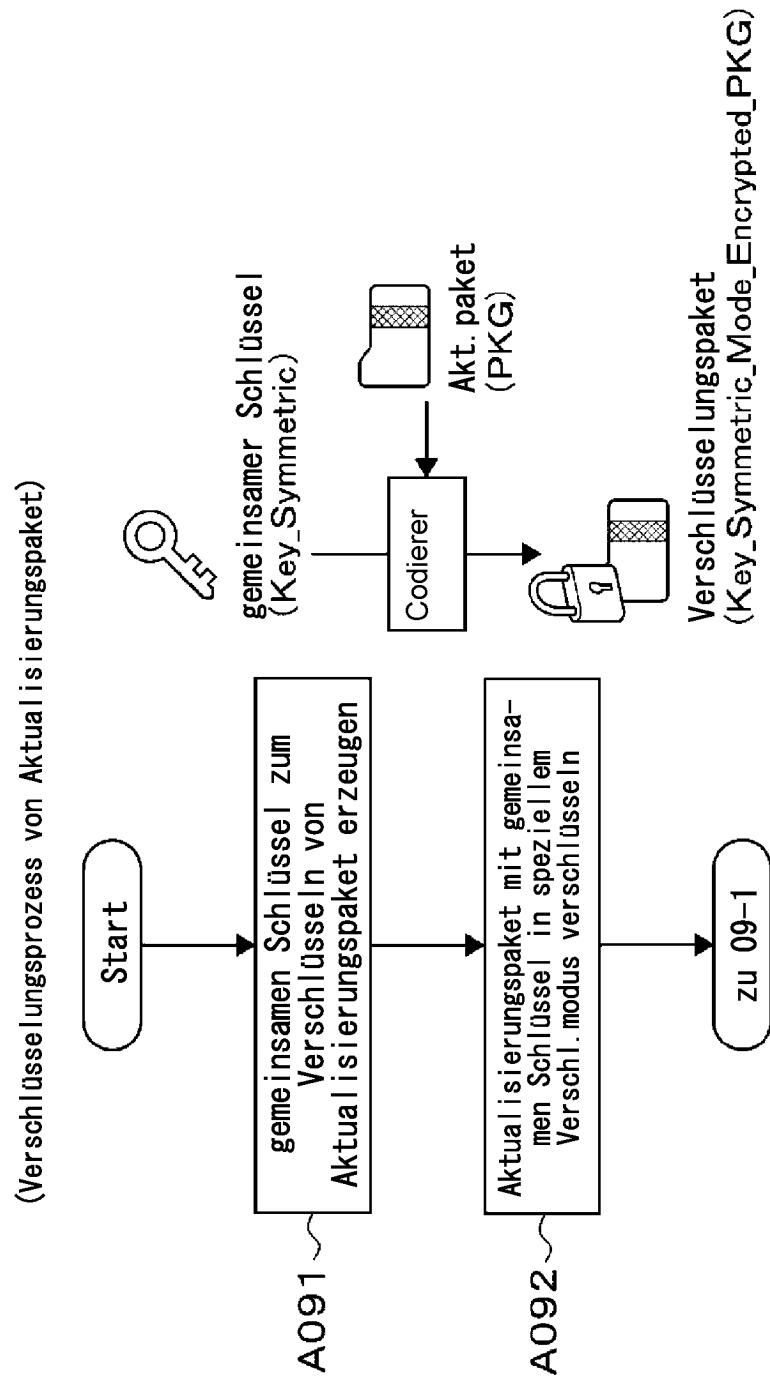


FIG. 80

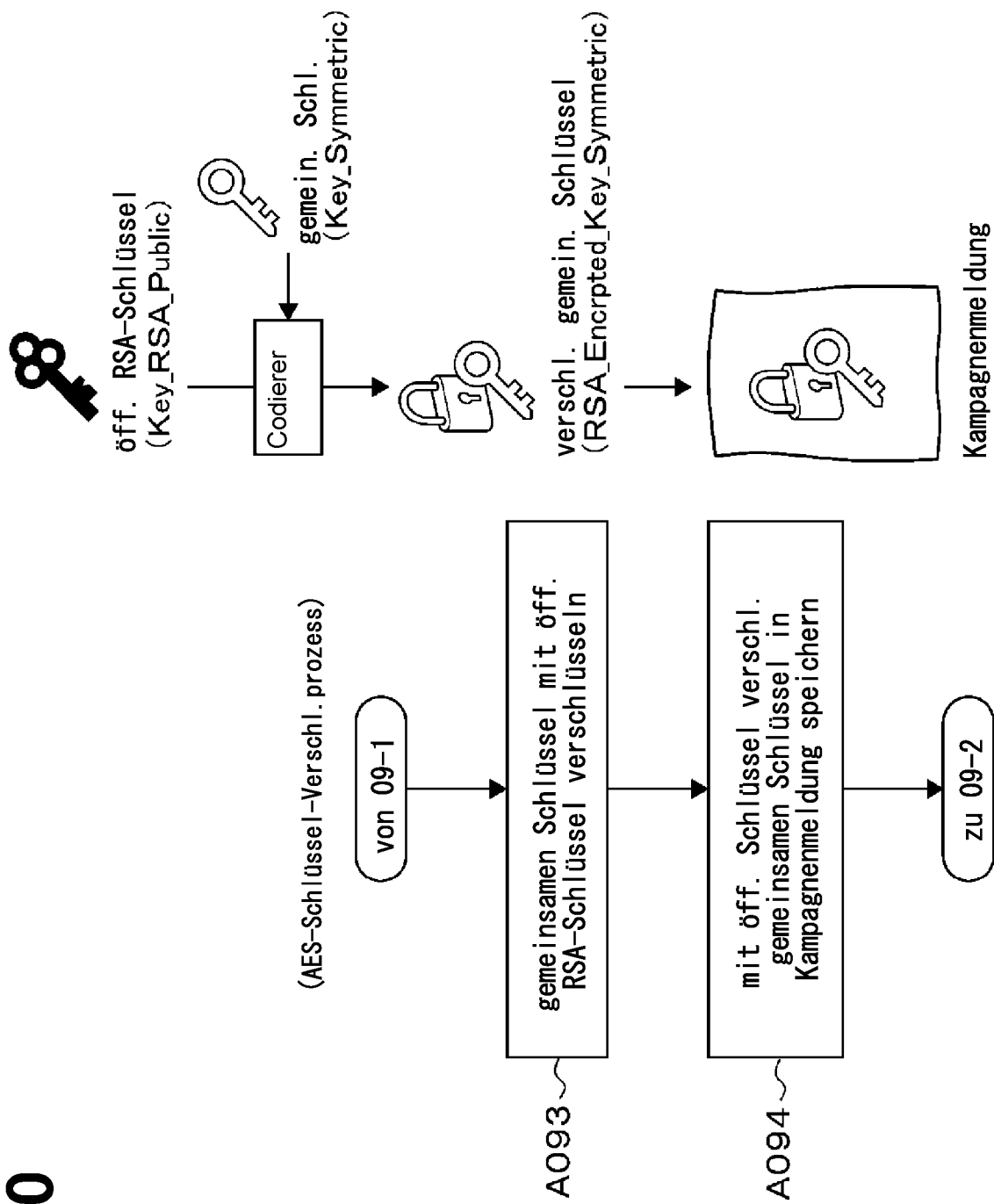


FIG. 81

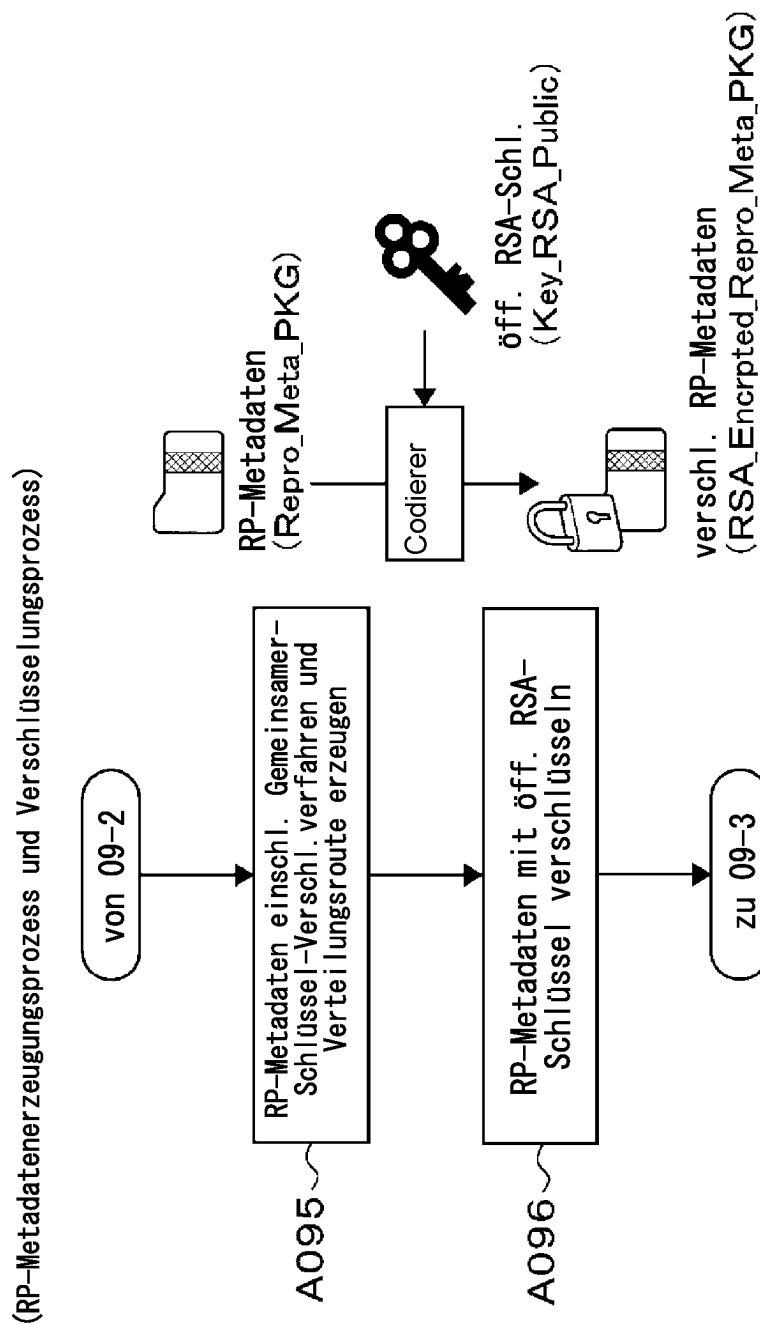


FIG. 82

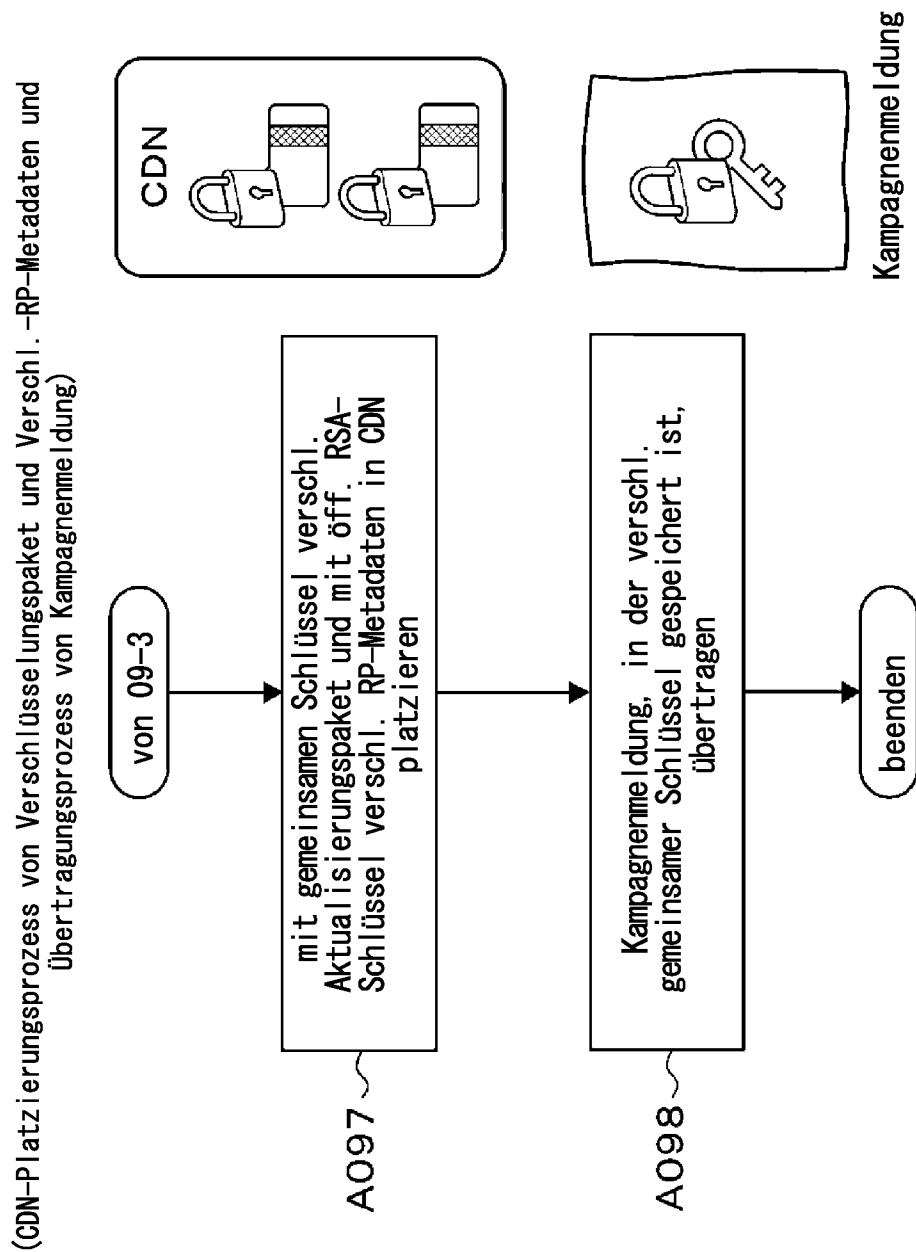


FIG. 83

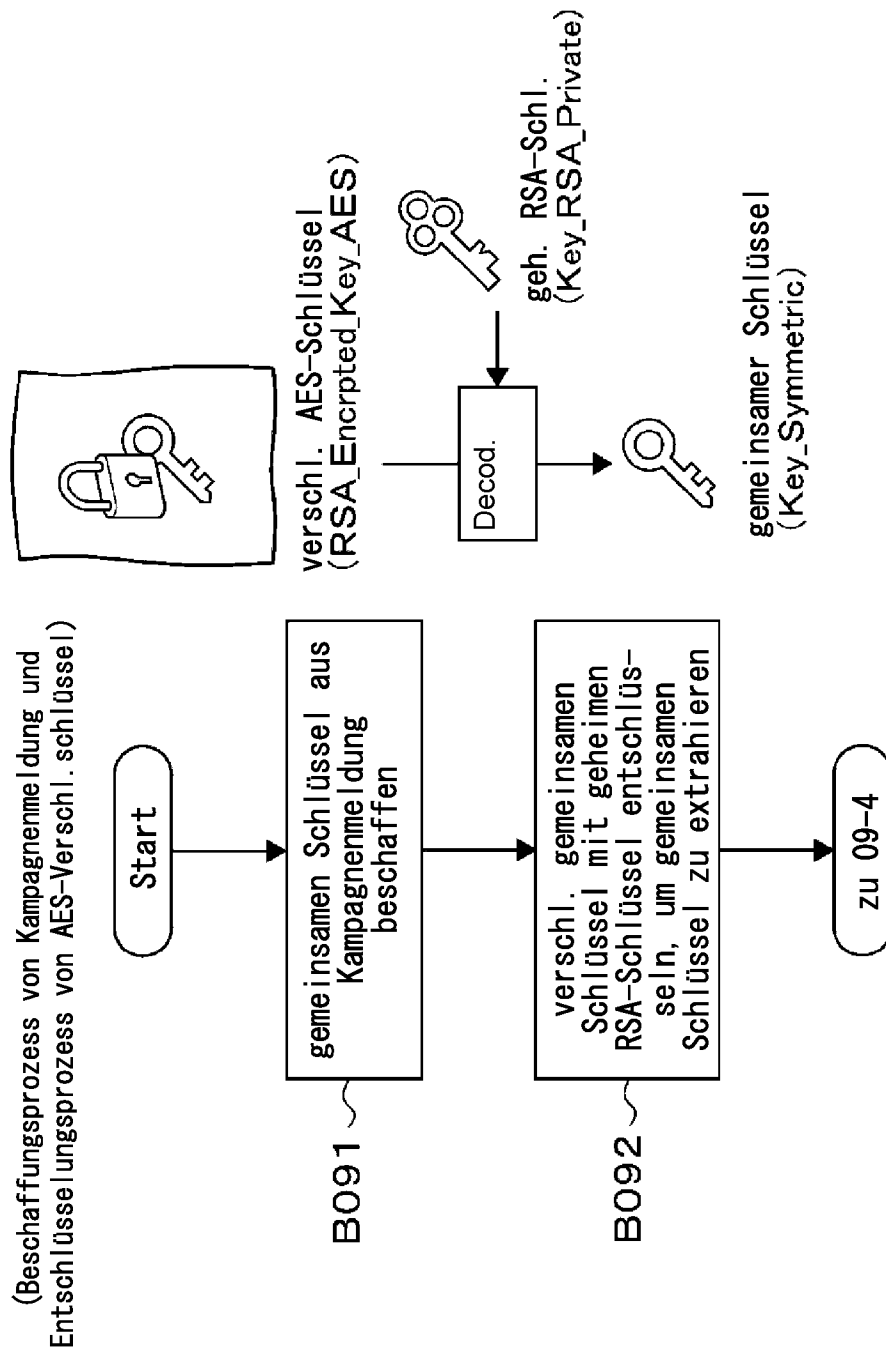


FIG. 84

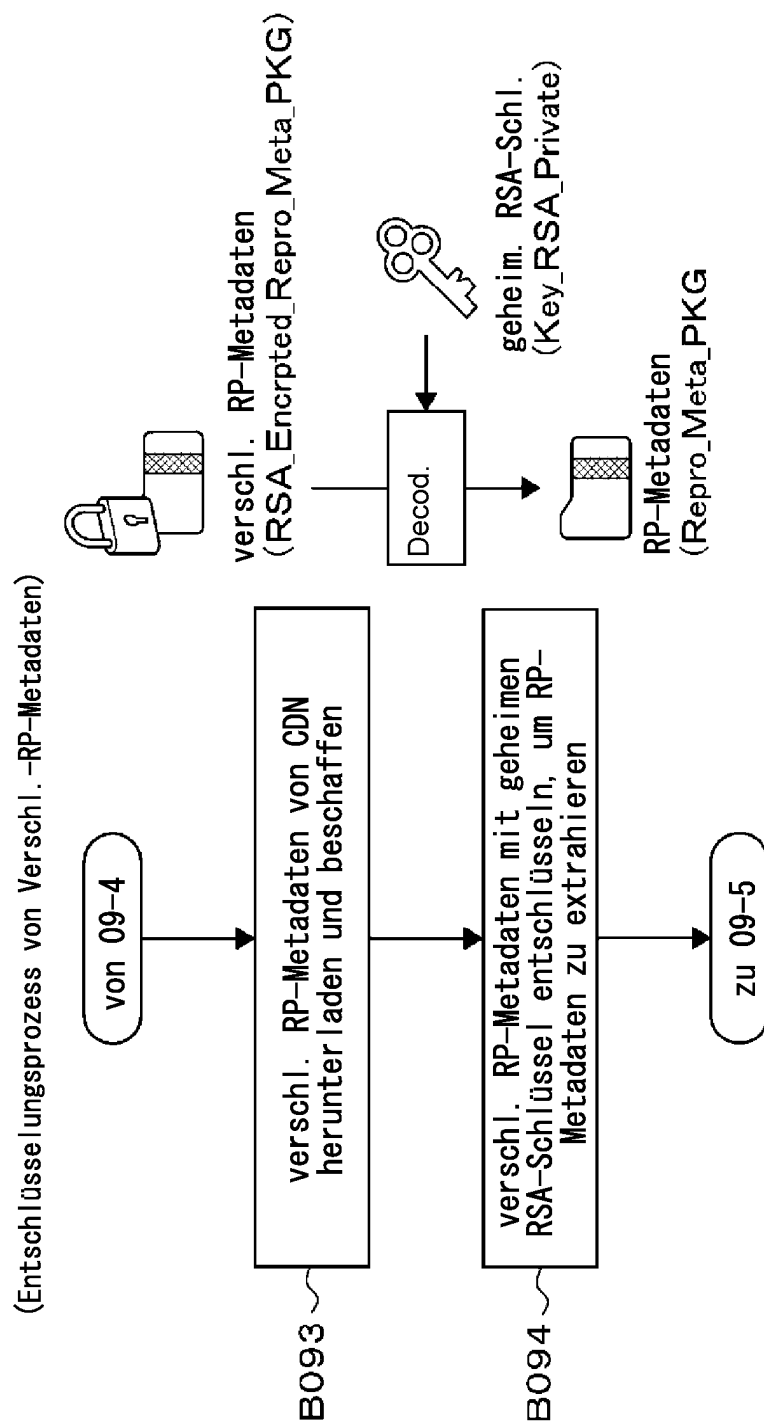


FIG. 85

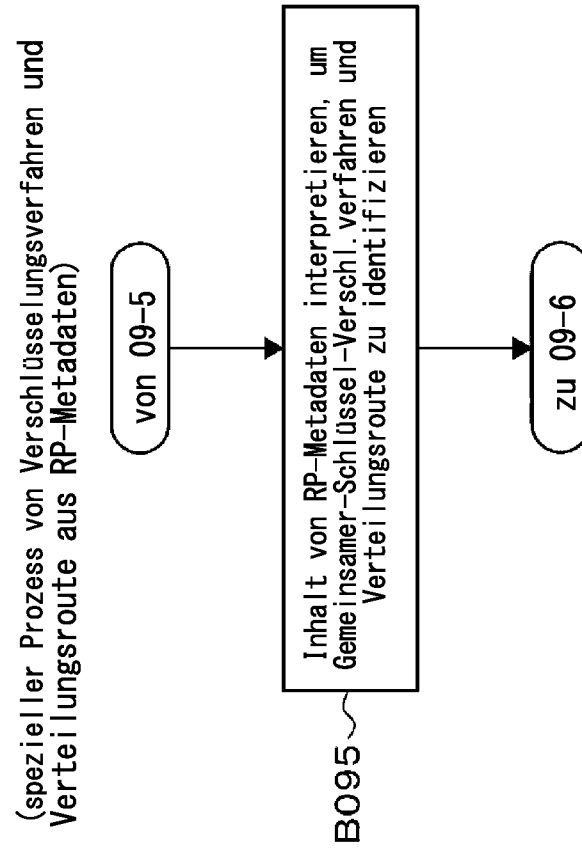
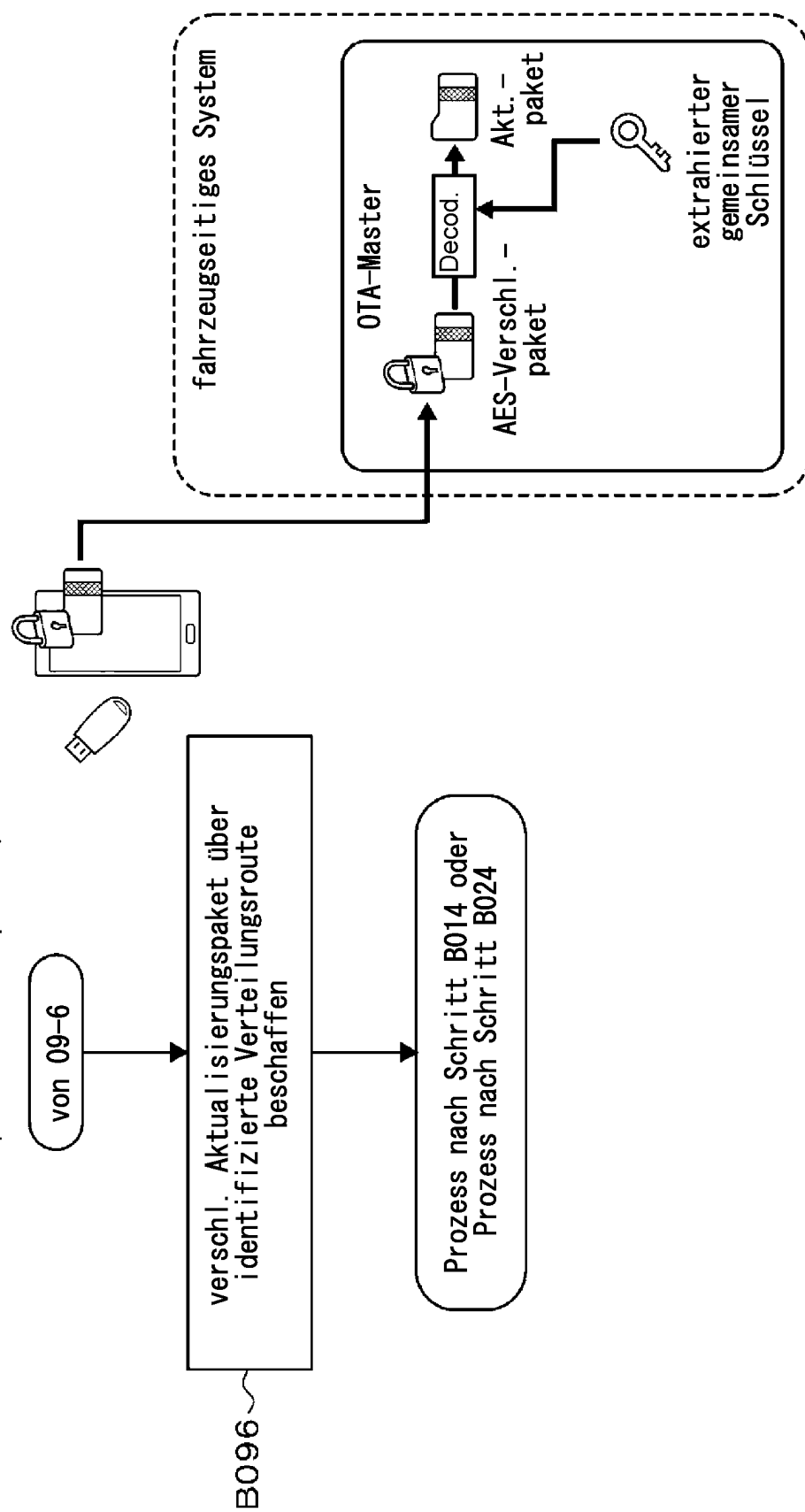


FIG. 86

(Prozess zum Beschaffen von Verschl. paket
von Smartphone oder USB-Speicher)



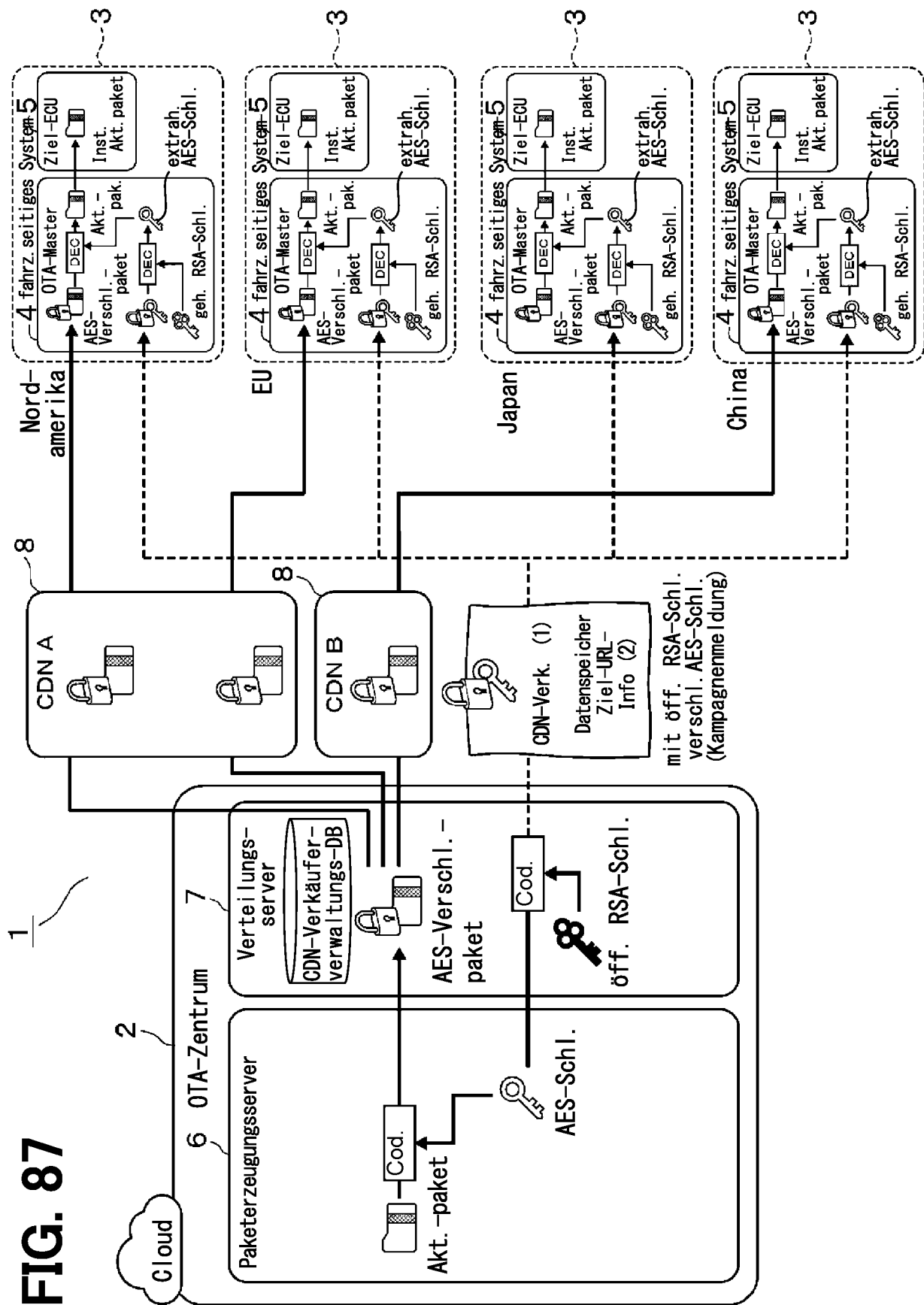


FIG. 88

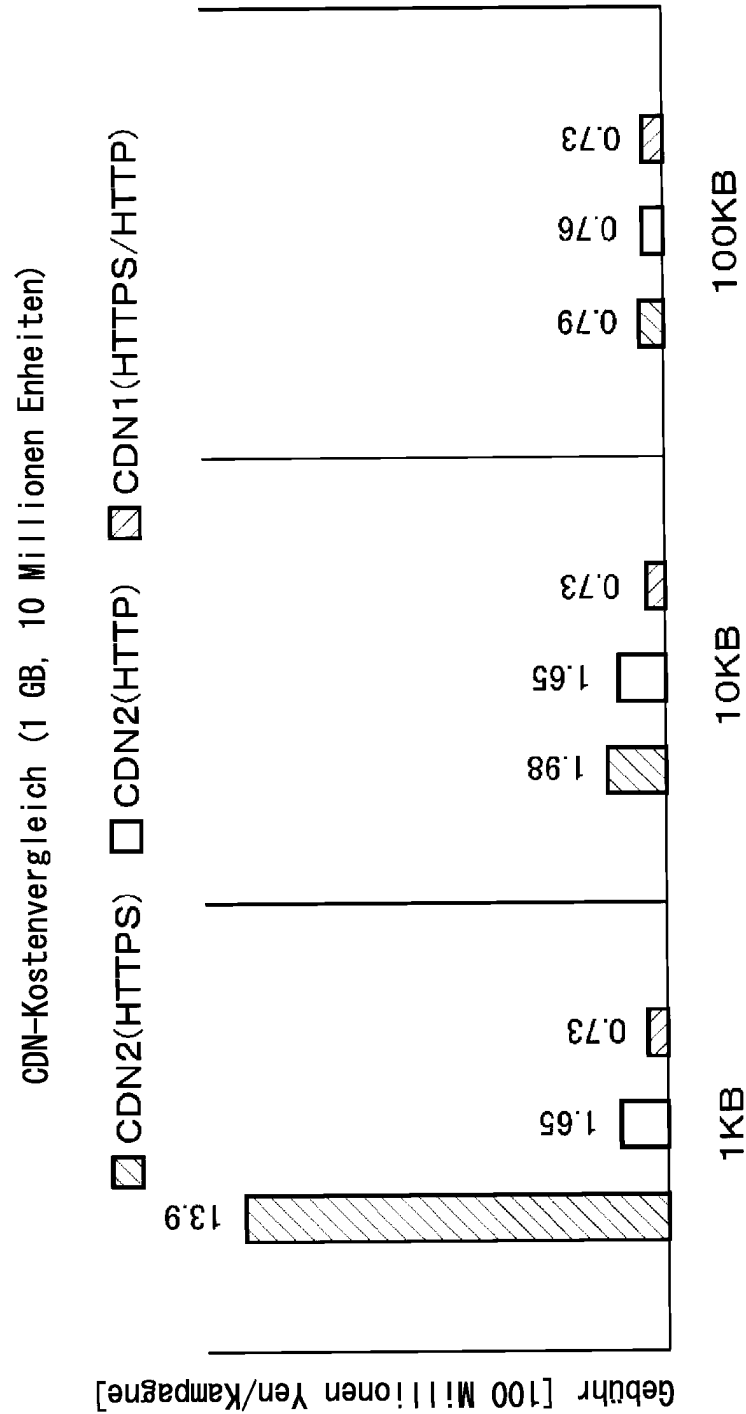


FIG. 89

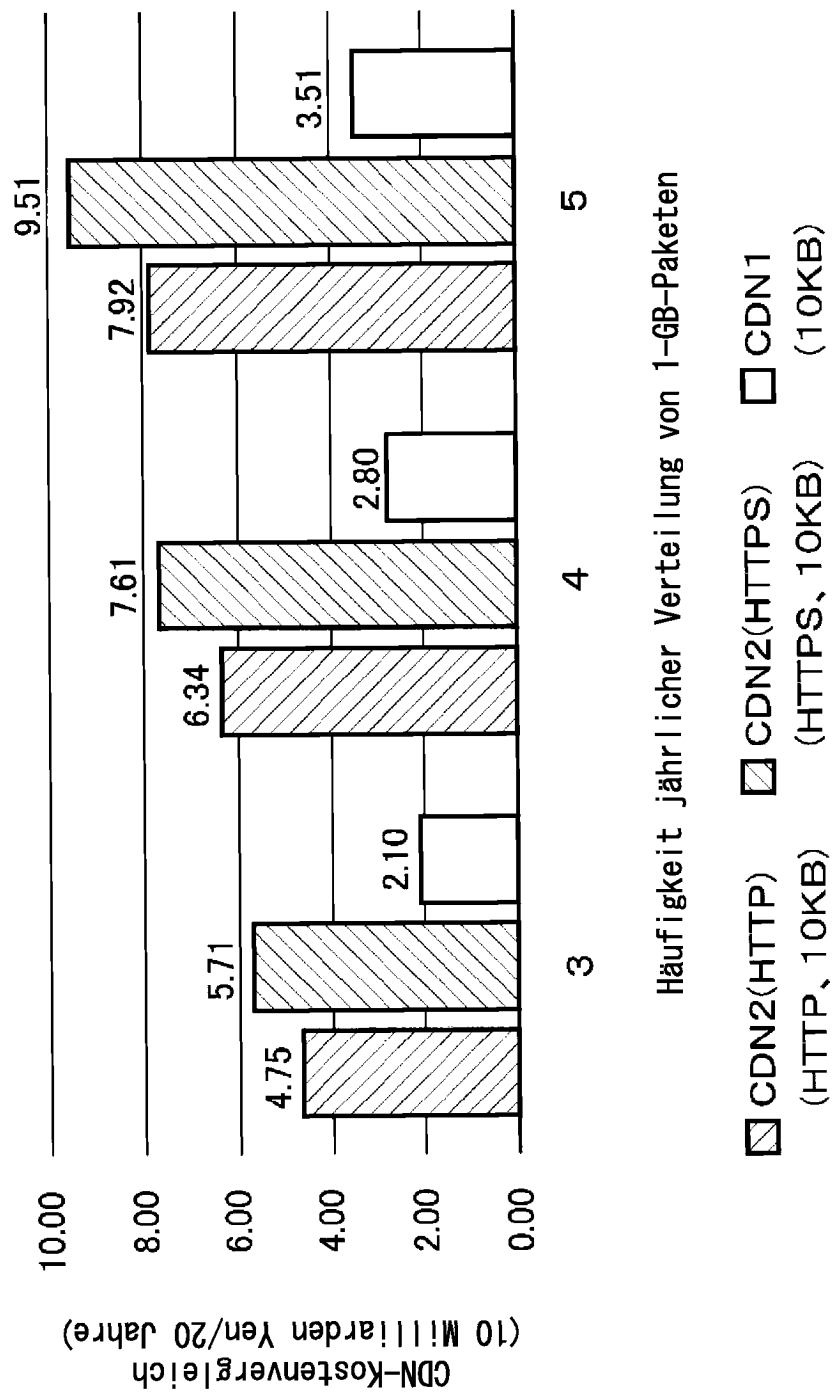


FIG. 90

CDN-Verkäufer-
verwaltungs-DB

CDN-DB-1

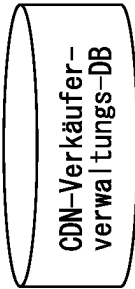
CDN-Preistabelle jeweiliger Cloud-Dienste (Basis)

CDN1	Gebührentabelle je GB						
	~10TB	~40TB	~100TB	~350TB	~500TB	~4PB	5PB~
Japan	0.0129 USD	0.121 USD	0.112 USD	0.093 USD	0.075 USD	0.065 USD	0.065 USD
Nordamerika	0.081 USD	0.075 USD	0.056 USD	0.037 USD	0.028 USD	0.023 USD	0.023 USD
EU	0.081 USD	0.075 USD	0.056 USD	0.037 USD	0.028 USD	0.023 USD	0.023 USD

CDN2	Gebührentabelle je GB						
	~10TB	~40TB	~100TB	~350TB	~524TB	~4PB	5PB~
Japan	0.114 USD	0.089 USD	0.086 USD	0.084 USD	0.080 USD	0.070 USD	0.060 USD
Nordamerika	0.085 USD	0.080 USD	0.060 USD	0.040 USD	0.030 USD	0.025 USD	0.020 USD
EU	0.085 USD	0.080 USD	0.060 USD	0.040 USD	0.030 USD	0.025 USD	0.015 USD

CDN2	Anfragegebührentabelle für HTTP-Verfahren	
	HTTP-Anfrage	HTTPS-Anfrage
Japan	0.009 USD	0.012 USD
Nordamerika	0.075 USD	0.010 USD
EU	0.009 USD	0.012 USD

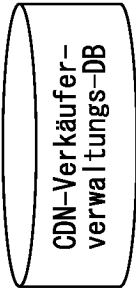
FIG. 91



CDN-DB-2
Preistabelle von Speicherverfahren jeweiliger Cloud-Dienst-Geschäftsbetreiber

CDN1	Speicherverfahren Anzahl Ziel- fahrzeuge: 2 Millionen	Gebührentabelle			
		100MB	1GB	10GB	20GB
Japan		2,45 Millio. Yen	14,52 Millio. Yen	145,6 Millio. Yen	291,2 Millio. Yen
Nordamerika		1,25 Millio. Yen	5,12 Millio. Yen	505 Millio. Yen	1 Millia. Yen 1 Millio. Yen
EU		1,25 Millio. Yen	5,12 Millio. Yen	505 Millio. Yen	1 Millia. Yen 1 Millio. Yen

CDN2	Speicherverfahren Anzahl Ziel- fahrzeuge: 2 Millionen	Gebührentabelle			
		100MB	1GB	10GB	20GB
Japan		1,89 Millio. Yen	17,6 Millio. Yen	132 Millio. Yen	264 Millio. Yen
Nordamerika		880.000 Yen	6,6 Millio. Yen	44 Millio. Yen	88 Millio. Yen
EU		1,32 Millio. Yen	6,6 Millio. Yen	44 Millio. Yen	88 Millio. Yen



CDN-DB-3-1

FIG. 92

Preistabelle für jeweilige Streaming-Größen in Streaming-Verfahren jeweiliger Cloud-Dienst-Geschäftsbetreiber

CDN1	Streaming-Größe: 1KB Anzahl Ziel- fahrzeuge: 2 Millio.	Gebührentabelle			
		100MB	1GB	10GB	20GB
Japan		2,45 Million. Yen	14,52 Million. Yen	145,6 Million. Yen	291,2 Million. Yen
Nordamerika		1,25 Million. Yen	5,12 Million. Yen	505 Million. Yen	1 Million. 1 Million. Yen
EU		1,25 Million. Yen	5,12 Million. Yen	505 Million. Yen	1 Million. 1 Million. Yen

CDN1	Streaming-Größe: 10KB Anzahl Ziel- fahrzeuge: 2 Millio.	Gebührentabelle			
		100MB	1GB	10GB	20GB
Japan		2,45 Million. Yen	14,52 Million. Yen	145,6 Million. Yen	291,2 Million. Yen
Nordamerika		1,25 Million. Yen	5,12 Million. Yen	505 Million. Yen	1 Million. 1 Million. Yen
EU		1,25 Million. Yen	5,12 Million. Yen	505 Million. Yen	1 Million. 1 Million. Yen

CDN1	Streaming-Größe: 100KB Anzahl Ziel- fahrzeuge: 2 Millio.	Gebührentabelle			
		100MB	1GB	10GB	20GB
Japan		2,45 Million. Yen	14,52 Million. Yen	145,6 Million. Yen	291,2 Million. Yen
Nordamerika		1,25 Million. Yen	5,12 Million. Yen	505 Million. Yen	1 Million. 1 Million. Yen
EU		1,25 Million. Yen	5,12 Million. Yen	505 Million. Yen	1 Million. 1 Million. Yen

FIG. 93

CDN-DB-3-2

CDN-Verkäufer-
verwaltungs-DB

Preistabelle für jeweilige Streaming-Größen in Streaming-Verfahren jeweiliger Cloud-Dienst-Geschäftsbetreiber

CDN2	Streaming-Größe: 1KB Anzahl Ziel- fahrzeuge: 2 Millio.	Gebührentabelle (HTTP/HTTPS)		
		100MB	1GB	10GB
Japan		21,69 Million. Yen/ 28,29 Million. Yen	215,6 Million. Yen/ 281,6 Million. Yen	2112 Million. Yen/ 2772 Million. Yen
Nordamerika		17,38 Million. Yen/ 22,88 Million. Yen	171,6 Million. Yen/ 226,6 Million. Yen	1694 Million. Yen/ 2244 Million. Yen
EU		21,12 Million. Yen/ 27,72 Million. Yen	204,6 Million. Yen/ 270,6 Million. Yen	2024 Million. Yen/ 2684 Million. Yen

CDN2	Streaming-Größe: 10KB Anzahl Ziel- fahrzeuge: 2 Millio.	Gebührentabelle (HTTP/HTTPS)		
		100MB	1GB	10GB
Japan		3,87 Million. Yen/ 4,53 Million. Yen	37,4 Million. Yen/ 44 Million. Yen	330 Million. Yen/ 396 Million. Yen
Nordamerika		2,53 Million. Yen/ 3,08 Million. Yen	23,1 Million. Yen/ 28,6 Million. Yen	209 Million. Yen/ 264 Million. Yen
EU		3,3 Million. Yen/ 3,96 Million. Yen	26,4 Million. Yen/ 33 Million. Yen	242 Million. Yen/ 308 Million. Yen

CDN2	Streaming-Größe: 100 KB Anzahl Ziel- fahrzeuge: 2 Millio.	Gebührentabelle (HTTP/HTTPS)		
		100MB	1GB	10GB
Japan		2,09 Million. Yen/ 2,16 Million. Yen	19,58 Million. Yen/ 20,24 Million. Yen	151,8 Million. Yen/ 158,4 Million. Yen
Nordamerika		1,05 Million. Yen/ 1,1 Million. Yen	8,25 Million. Yen/ 8,8 Million. Yen	60,5 Million. Yen/ 66 Million. Yen
EU		1,52 Million. Yen/ 1,58 Million. Yen	8,58 Million. Yen/ 9,24 Million. Yen	63,8 Million. Yen/ 70,4 Million. Yen

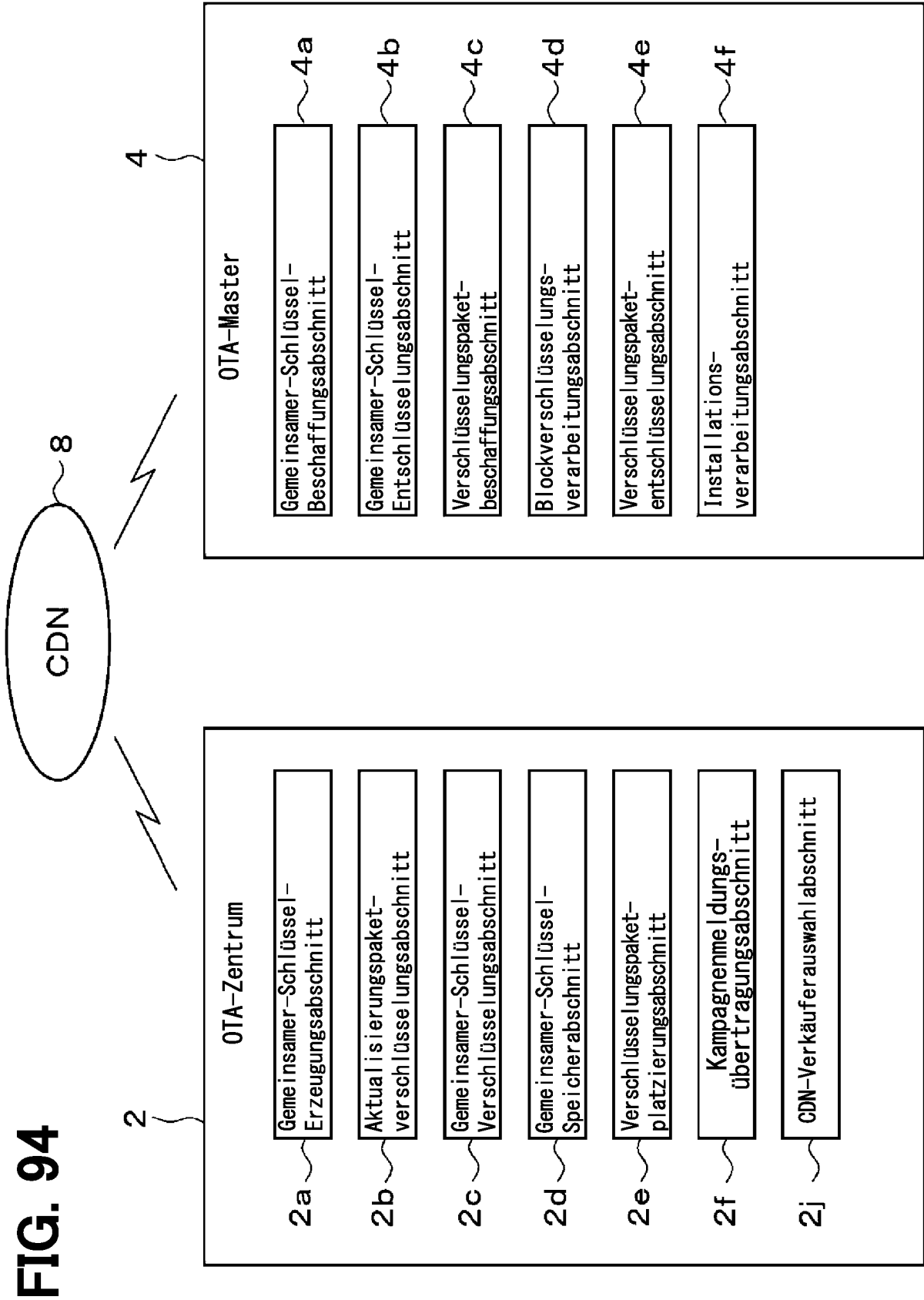


FIG. 95

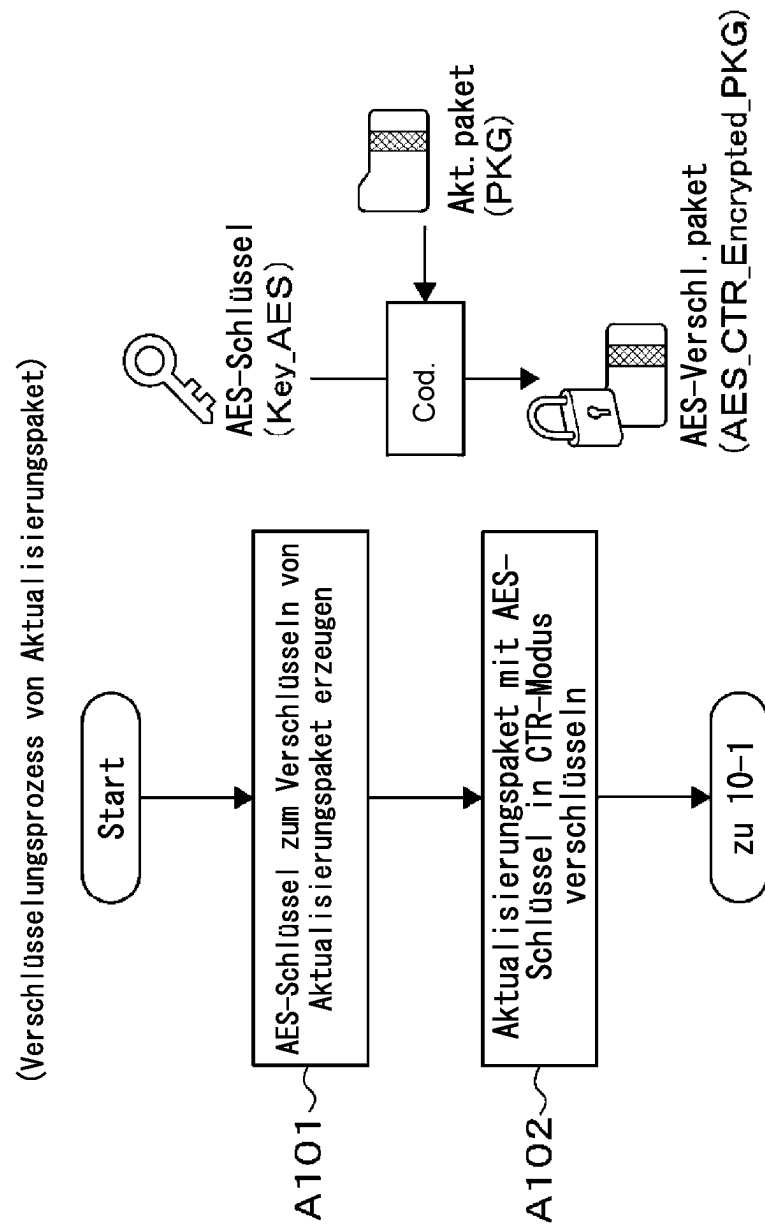
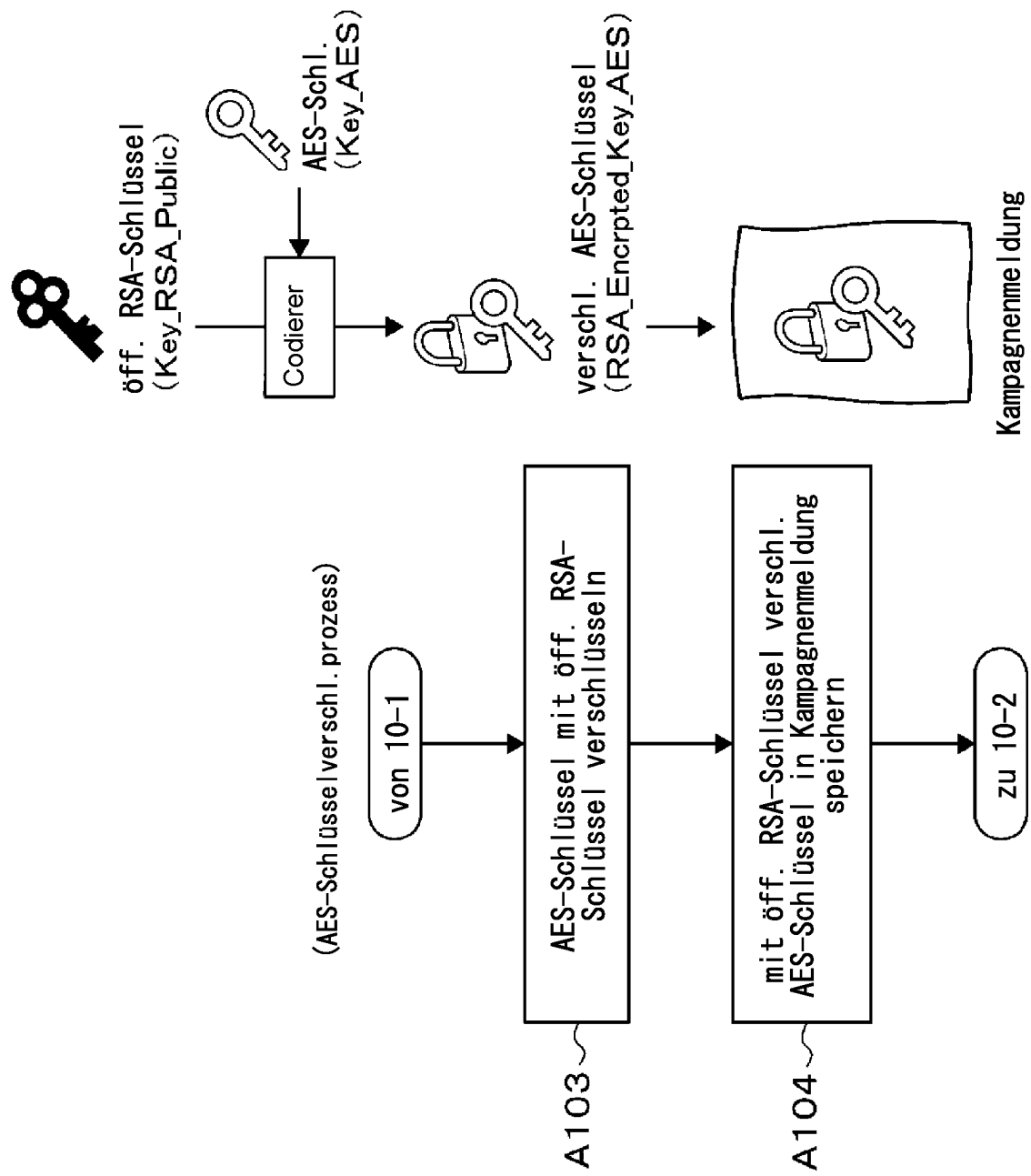


FIG. 96



(Auswahllogik von CDN-Platzierungsziel mit niedrigstem Preis für jeweilige Bereiche und Platzierungsprozess von Akt.paket für jeweilige Bereiche)

FIG. 97

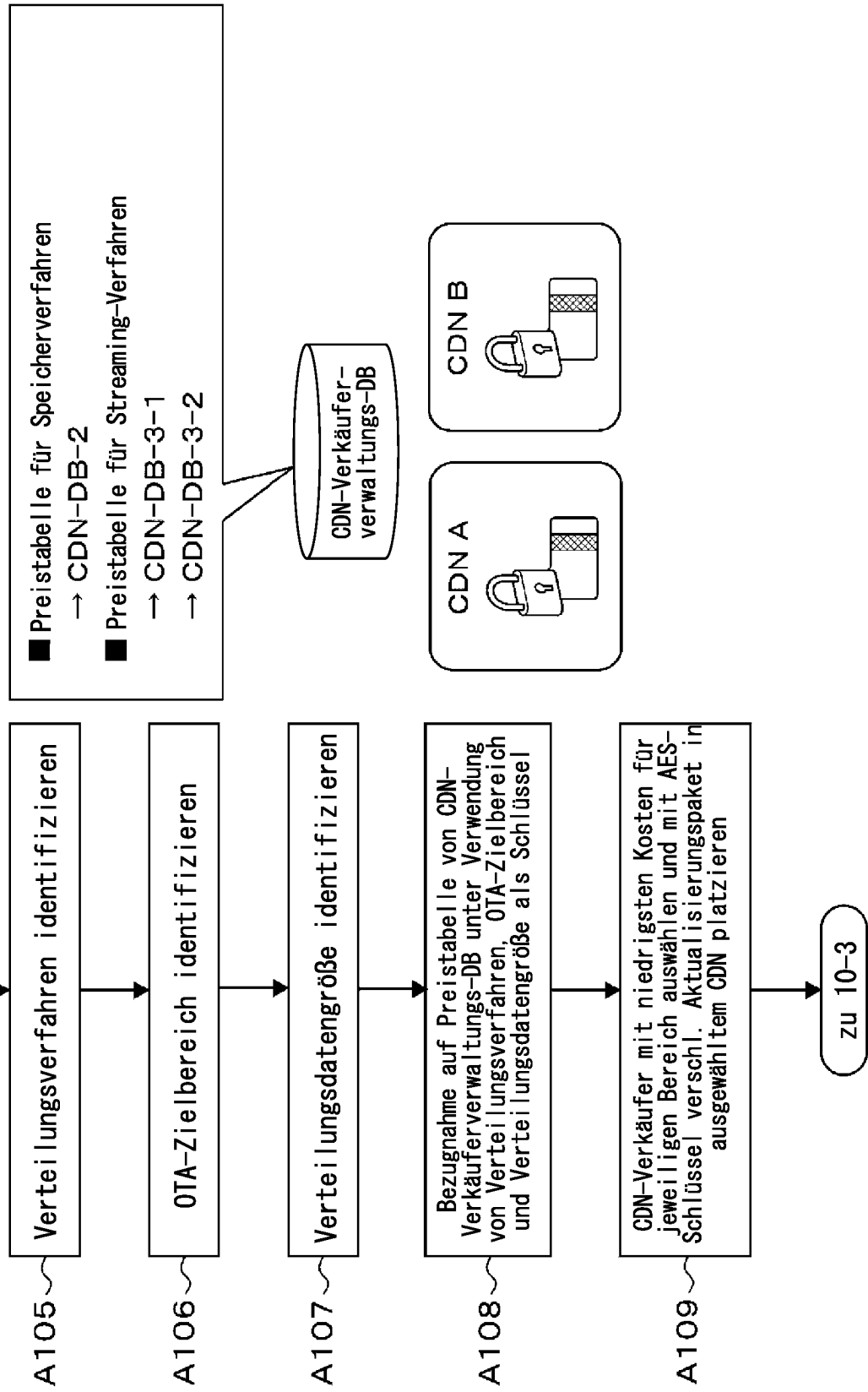


FIG. 98

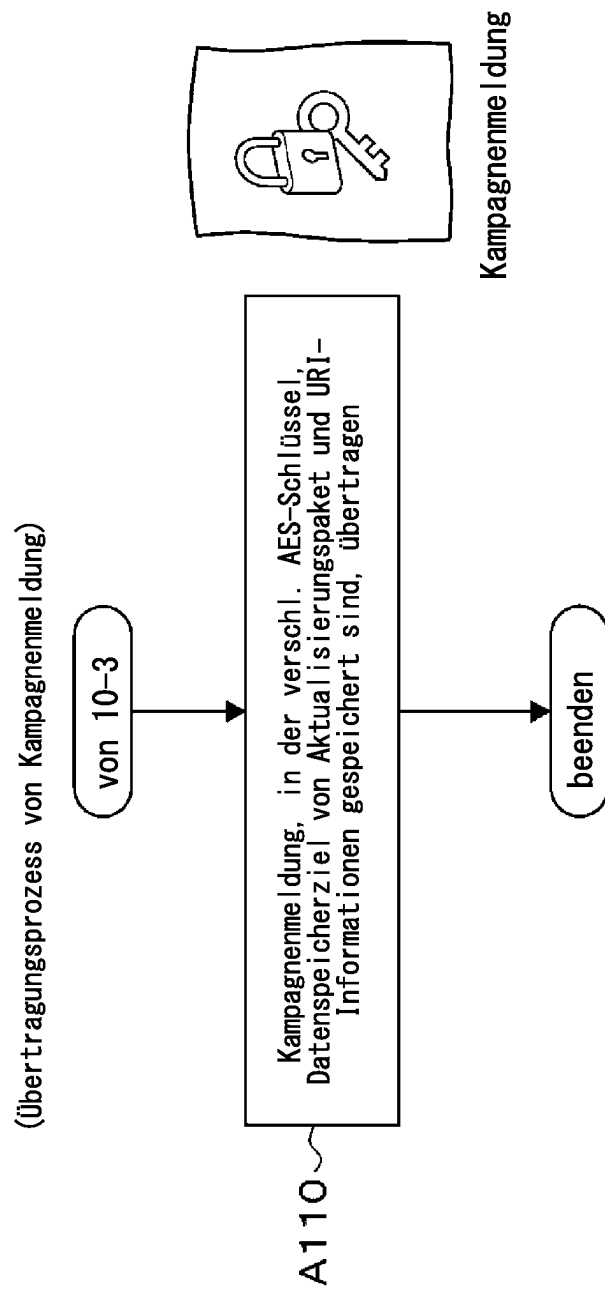


FIG. 99

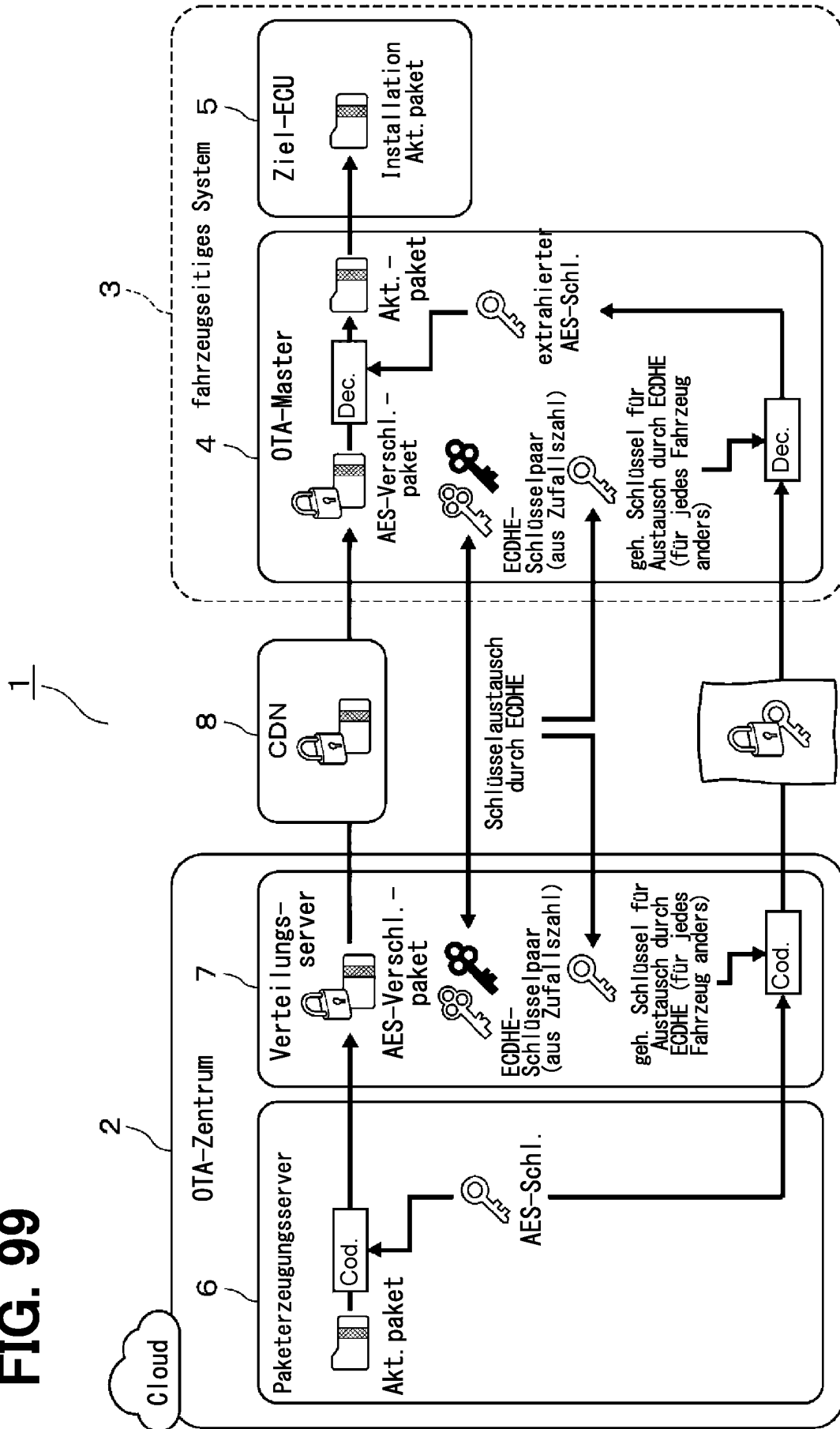


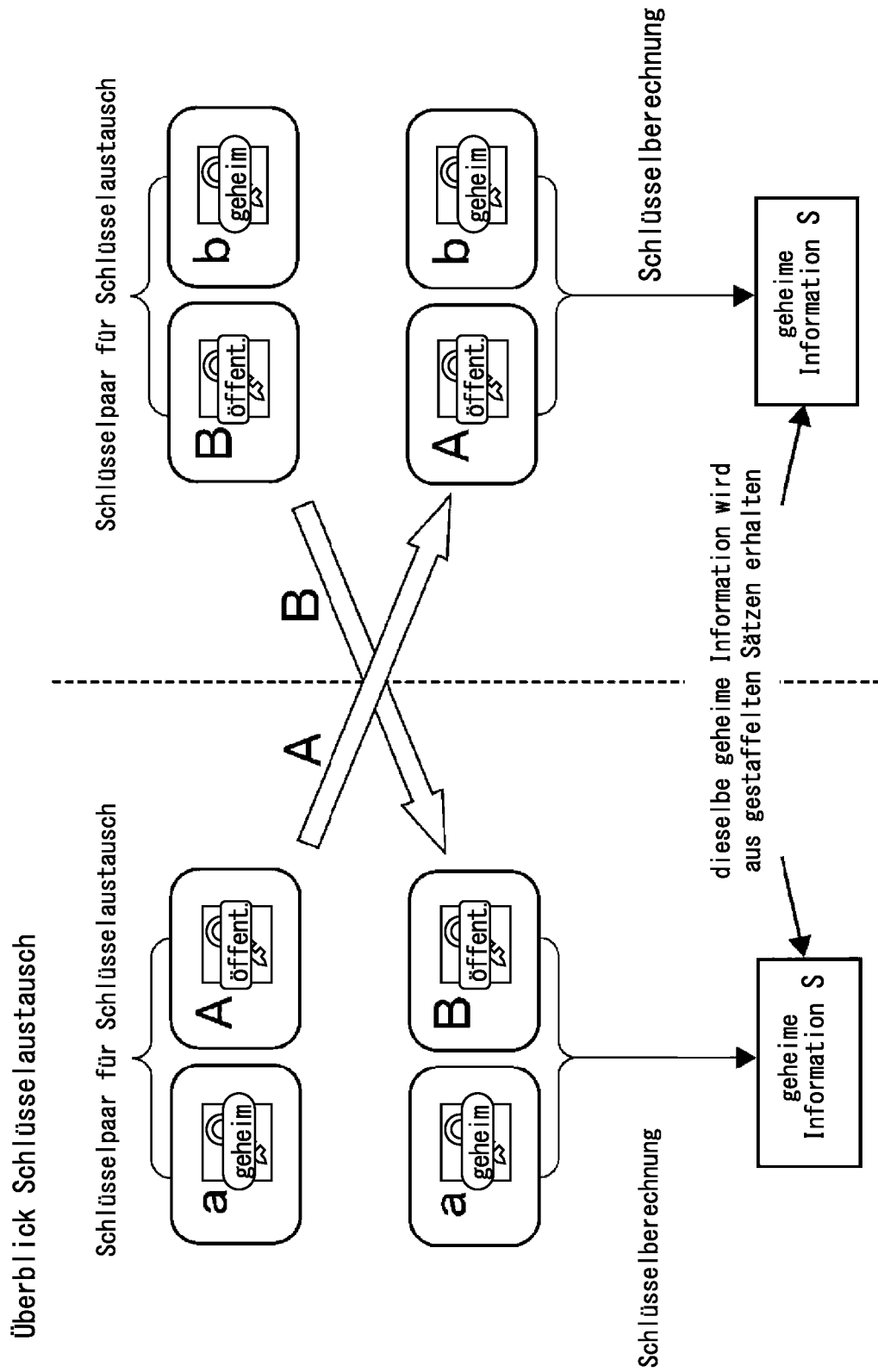
FIG. 100

FIG. 101

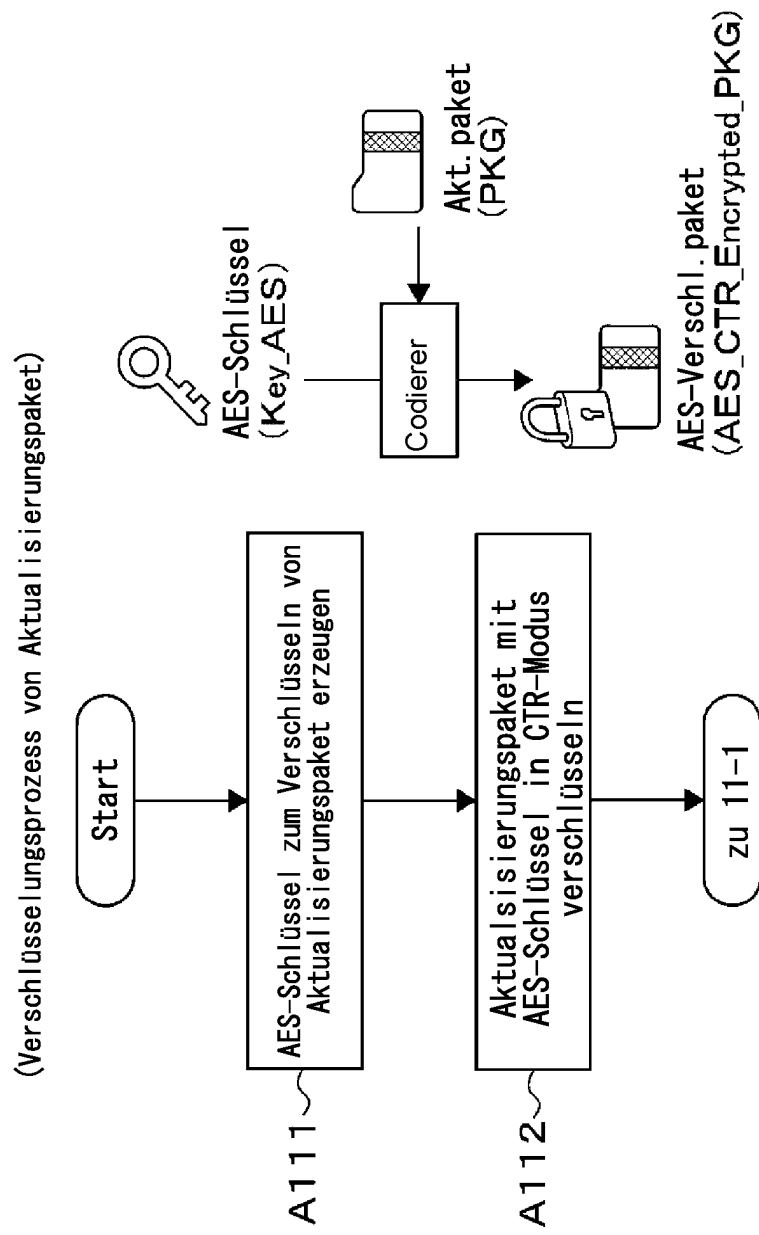


FIG. 102

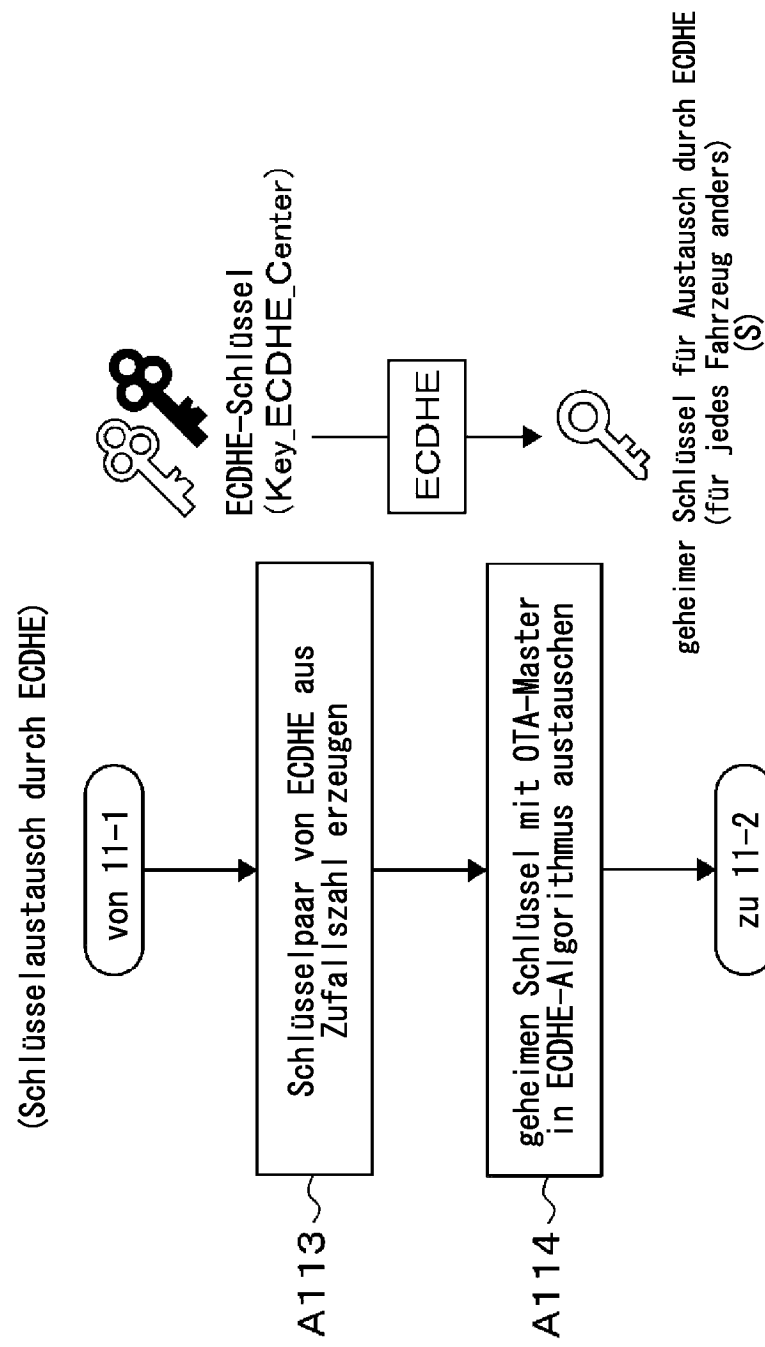


FIG. 103

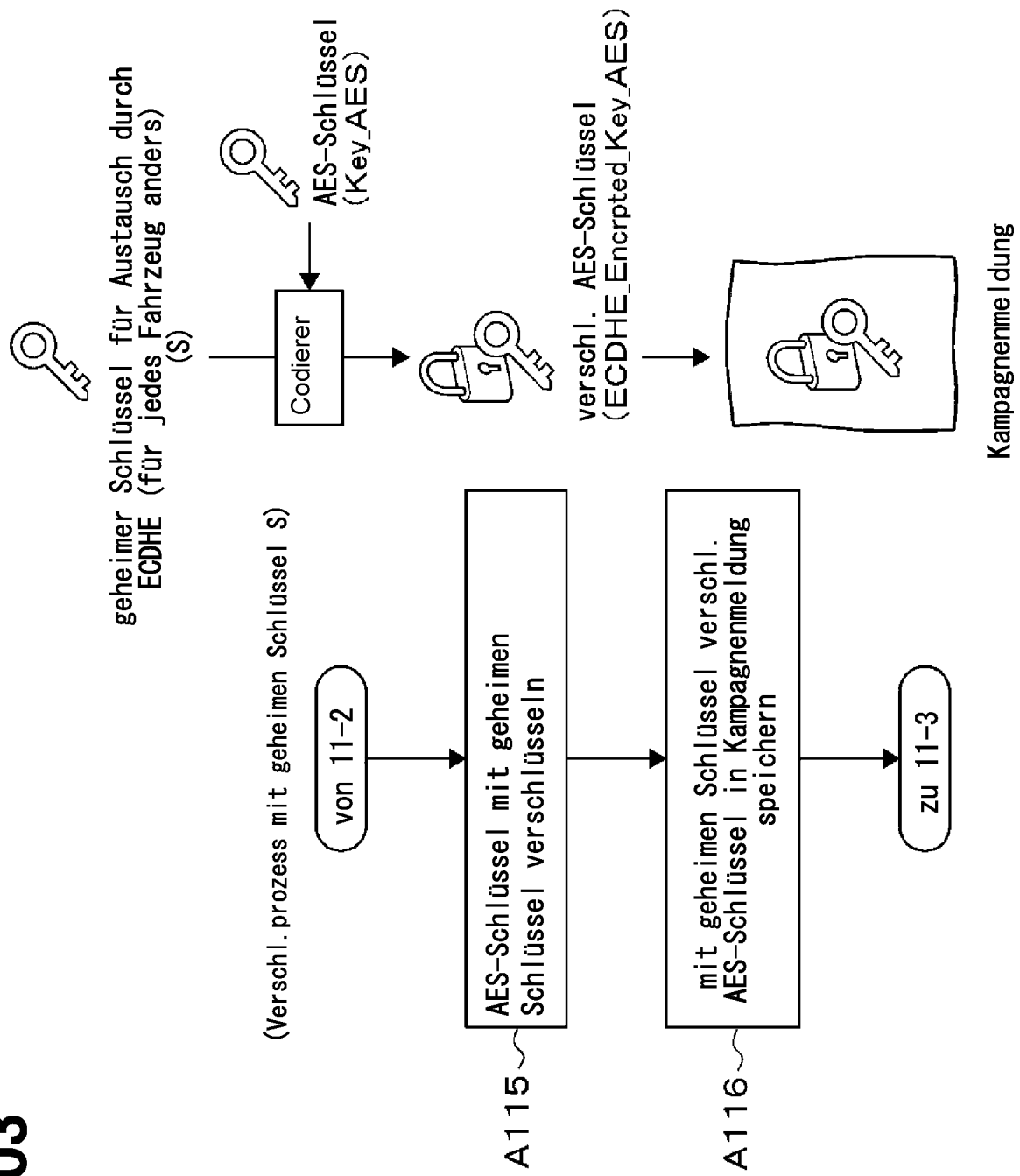


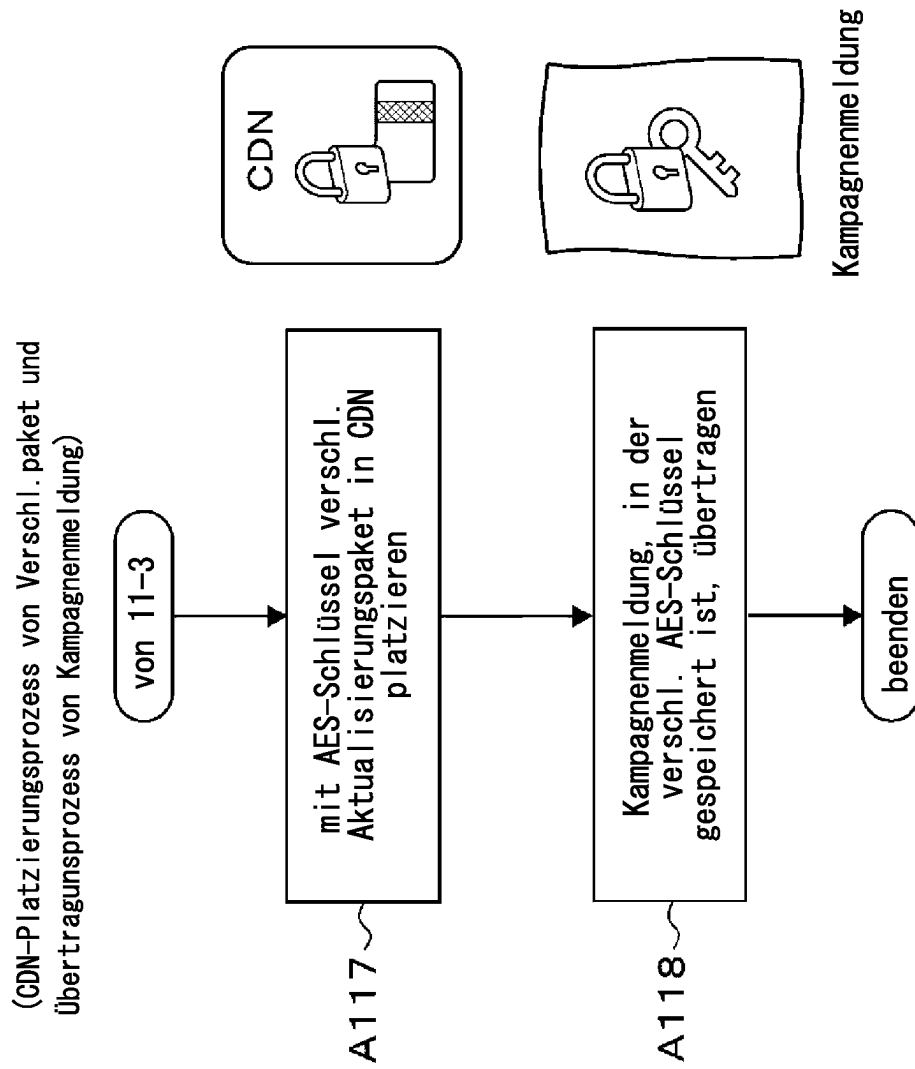
FIG. 104

FIG. 105

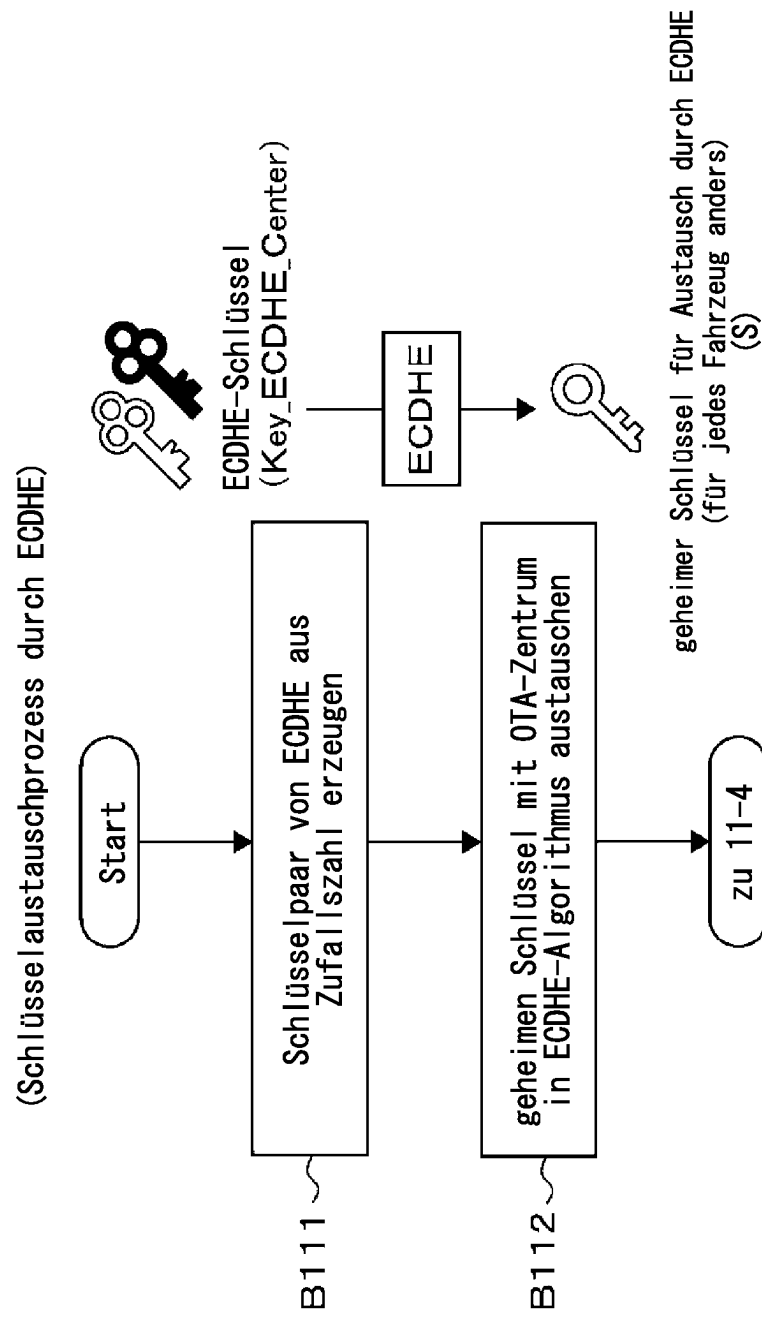


FIG. 106

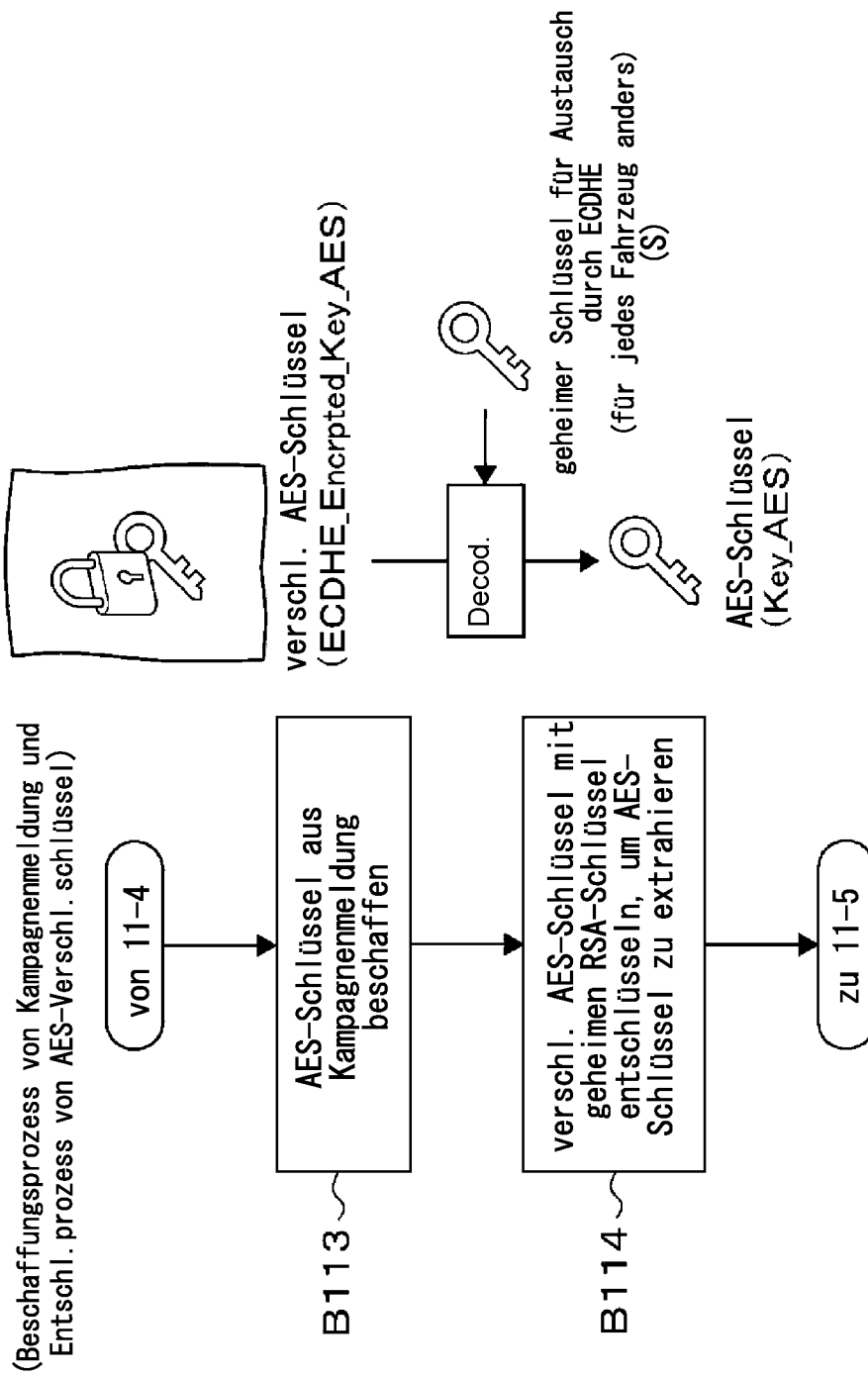


FIG. 107

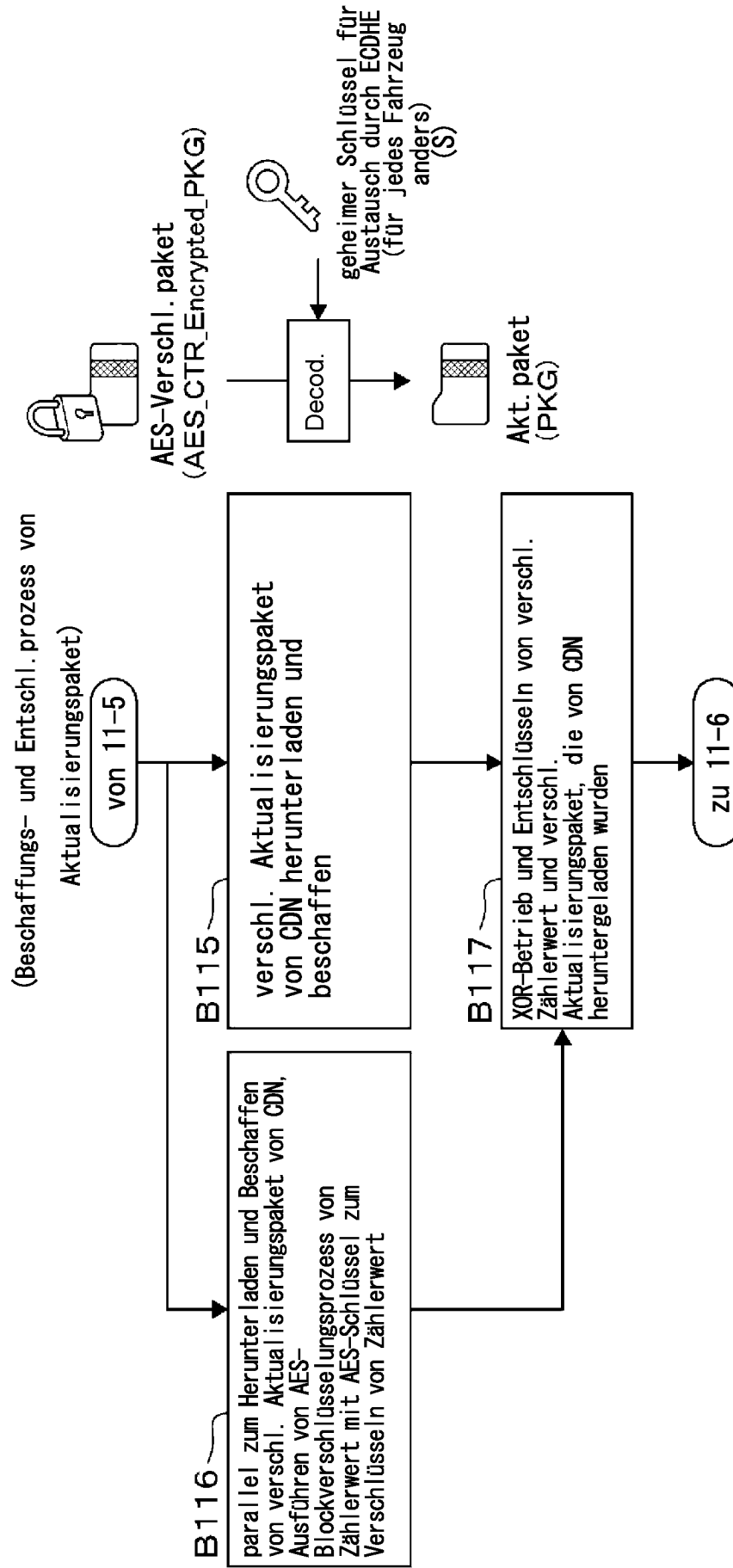


FIG. 108

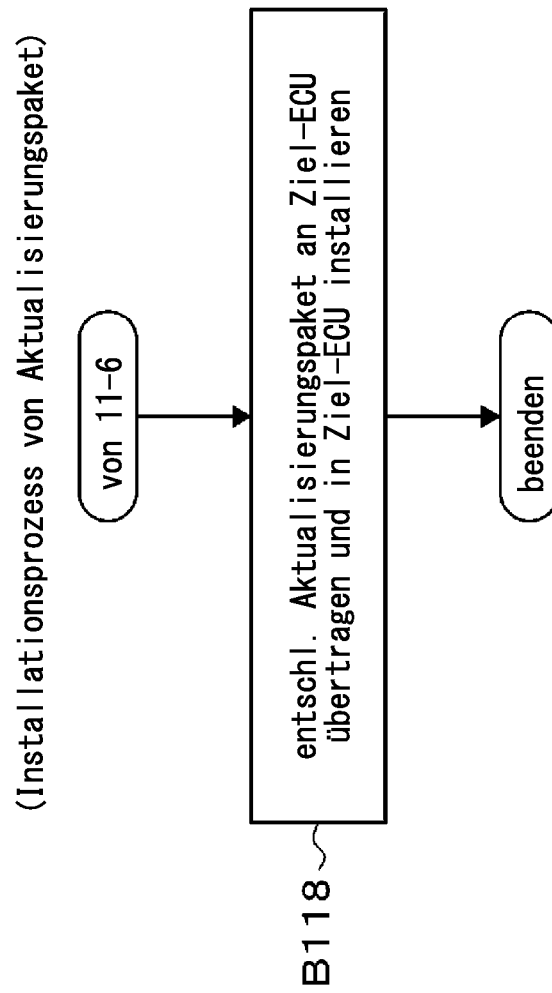


FIG. 109

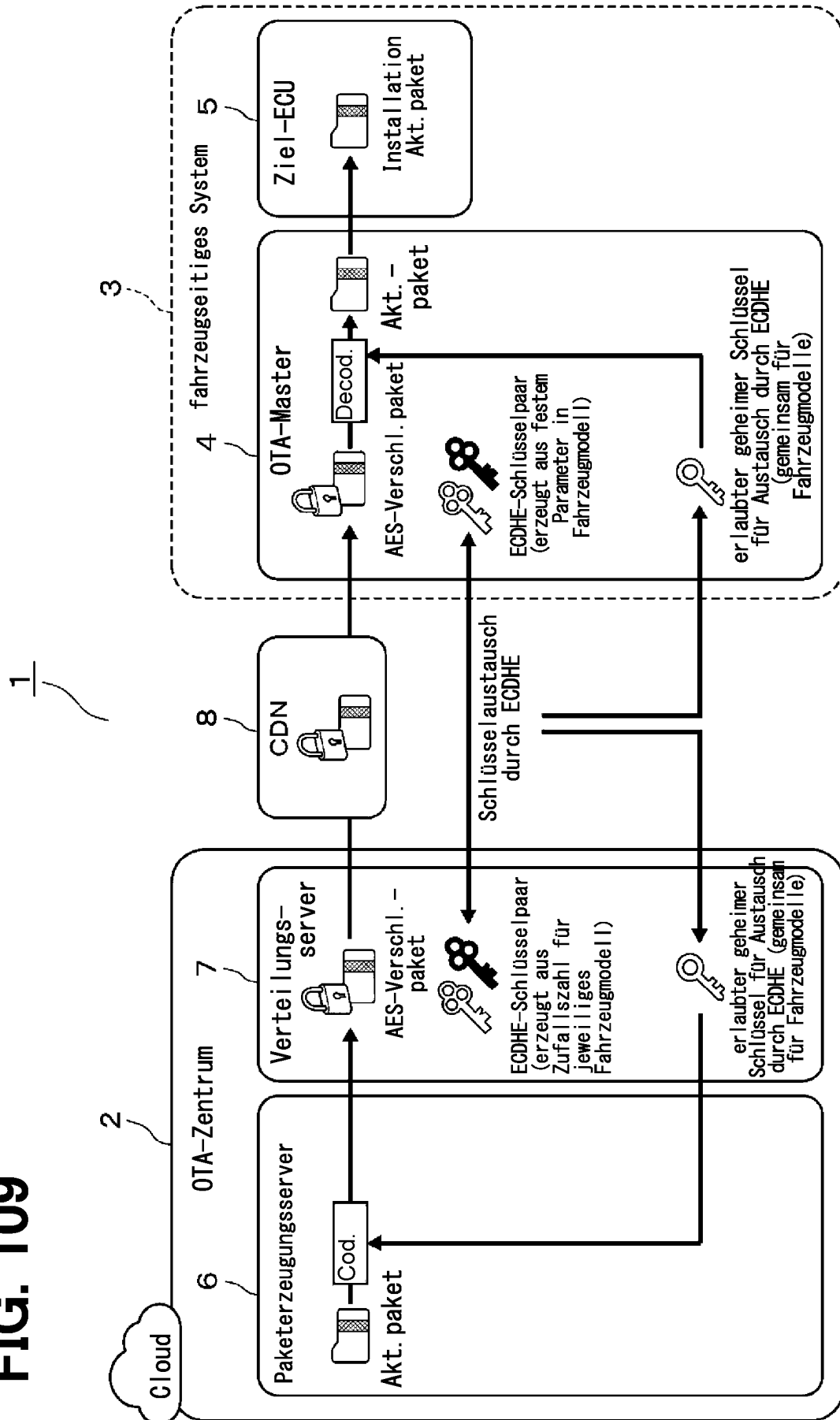


FIG. 110

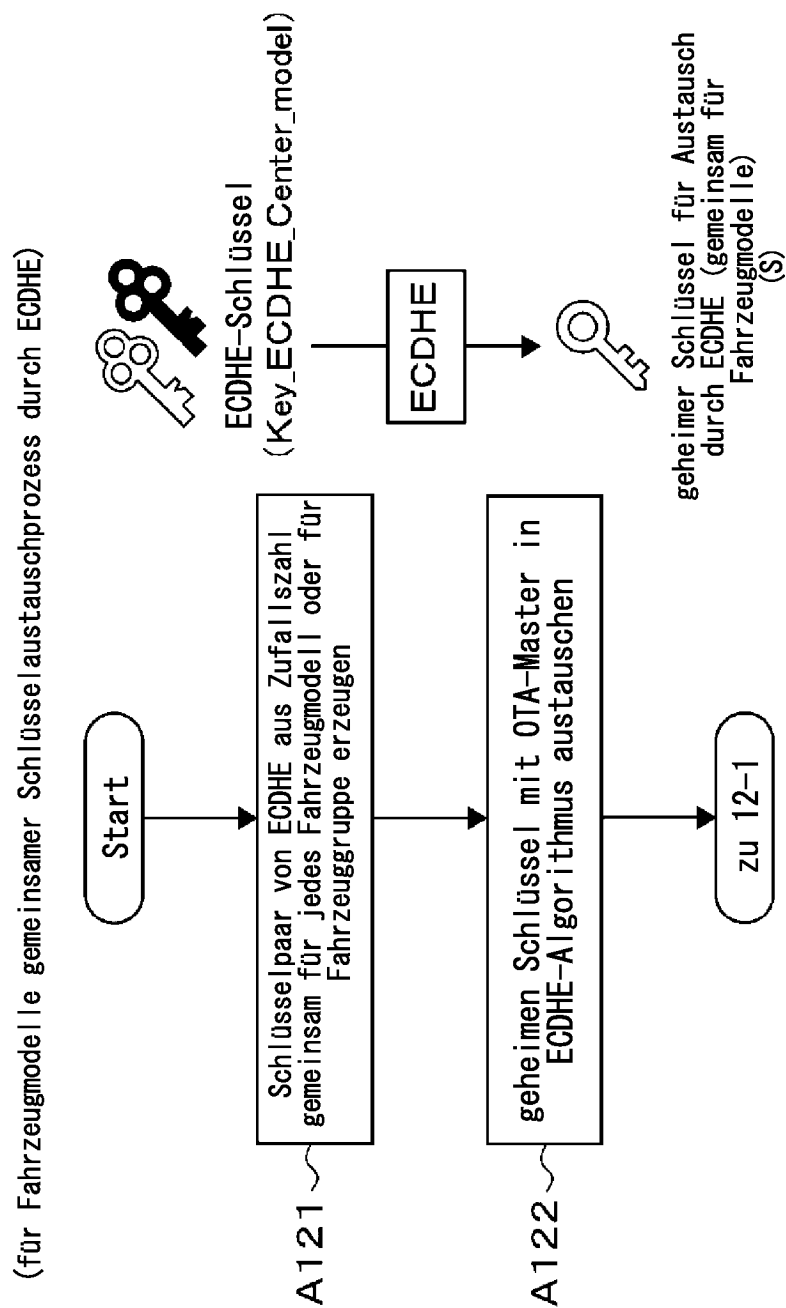


FIG. 111

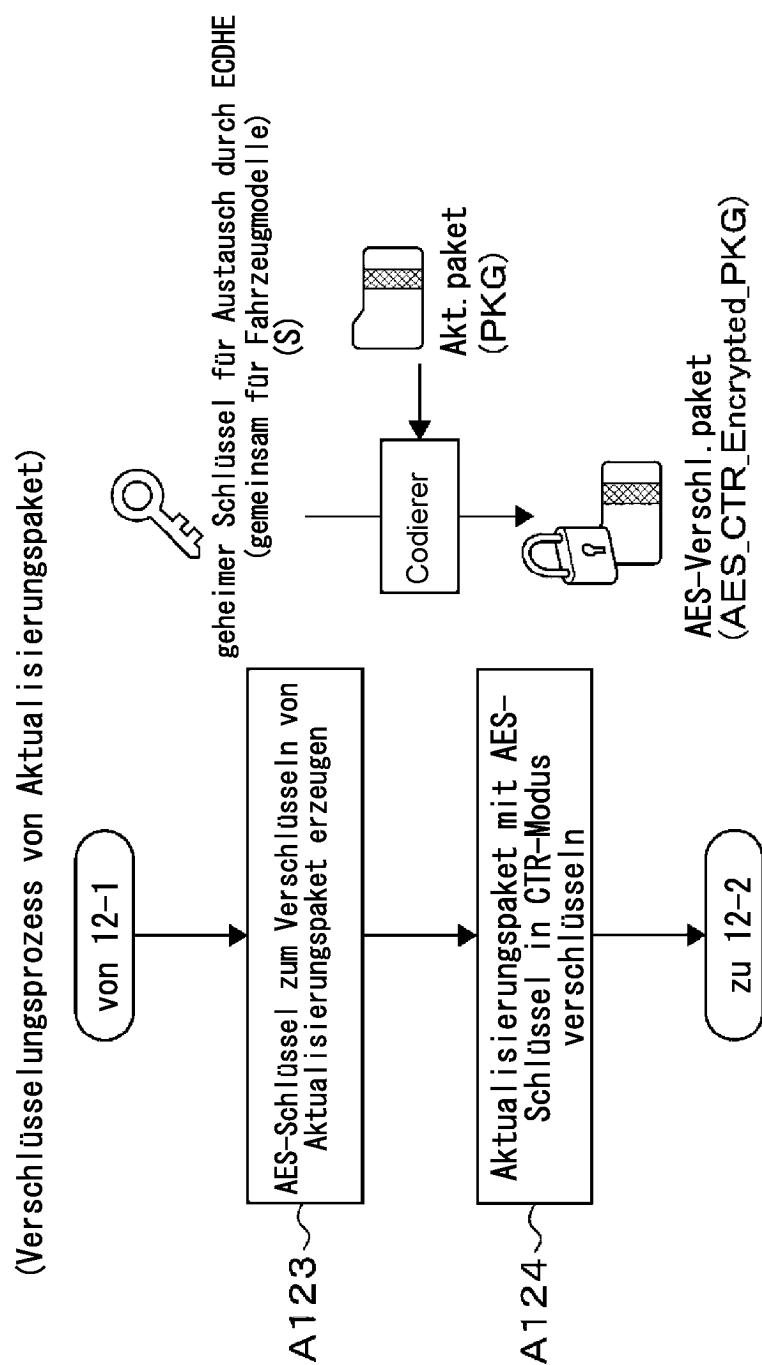


FIG. 112

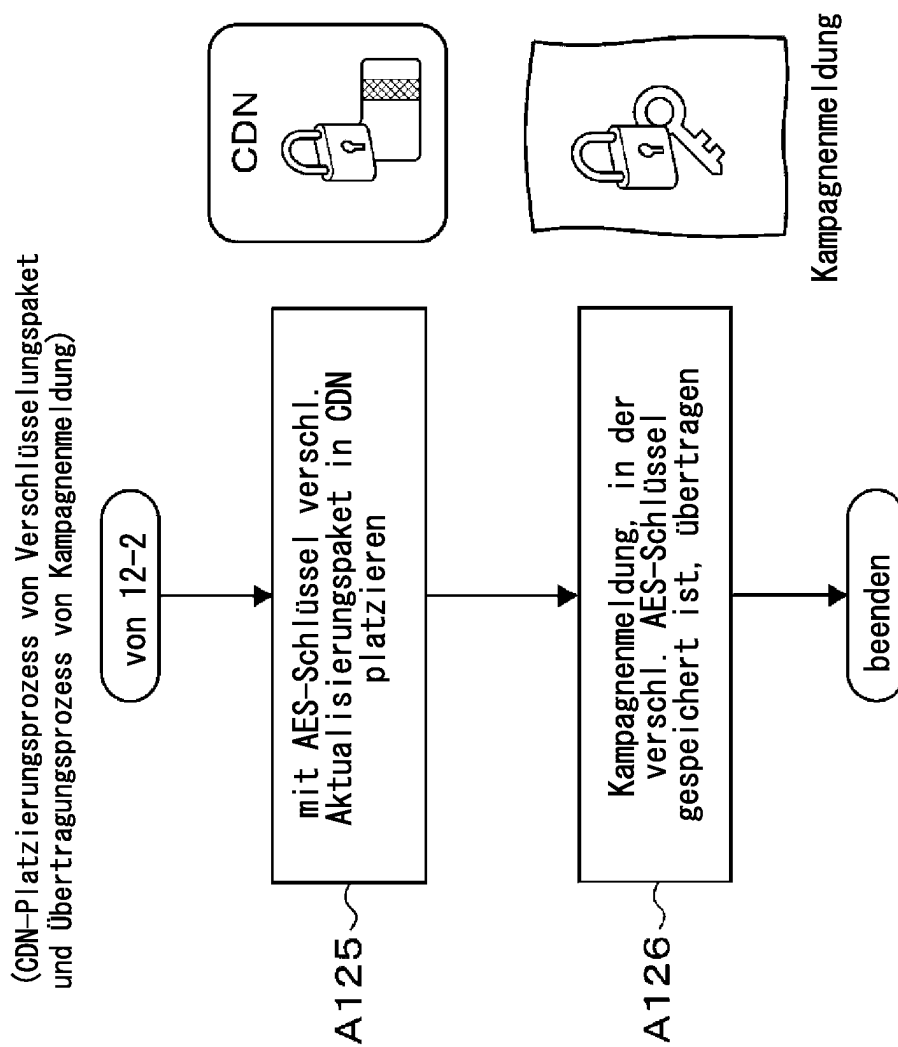


FIG. 113

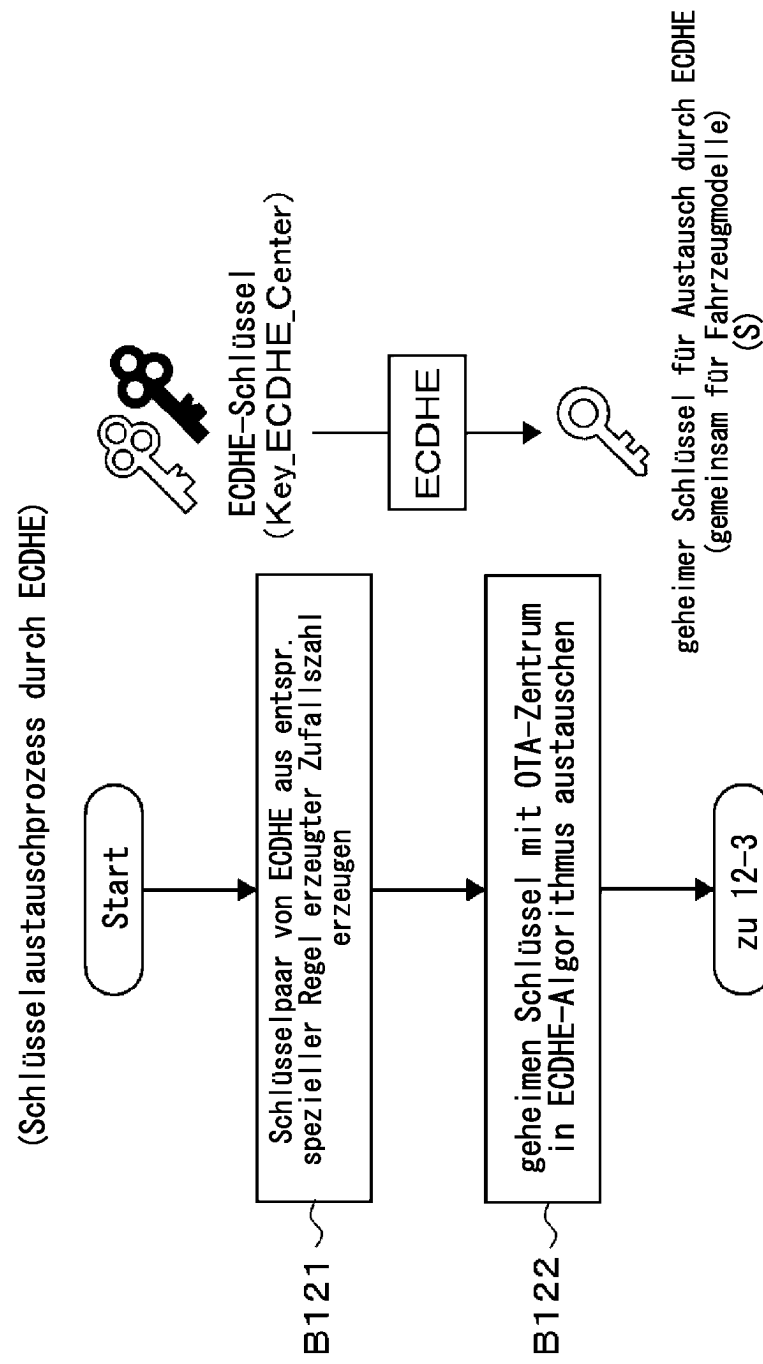


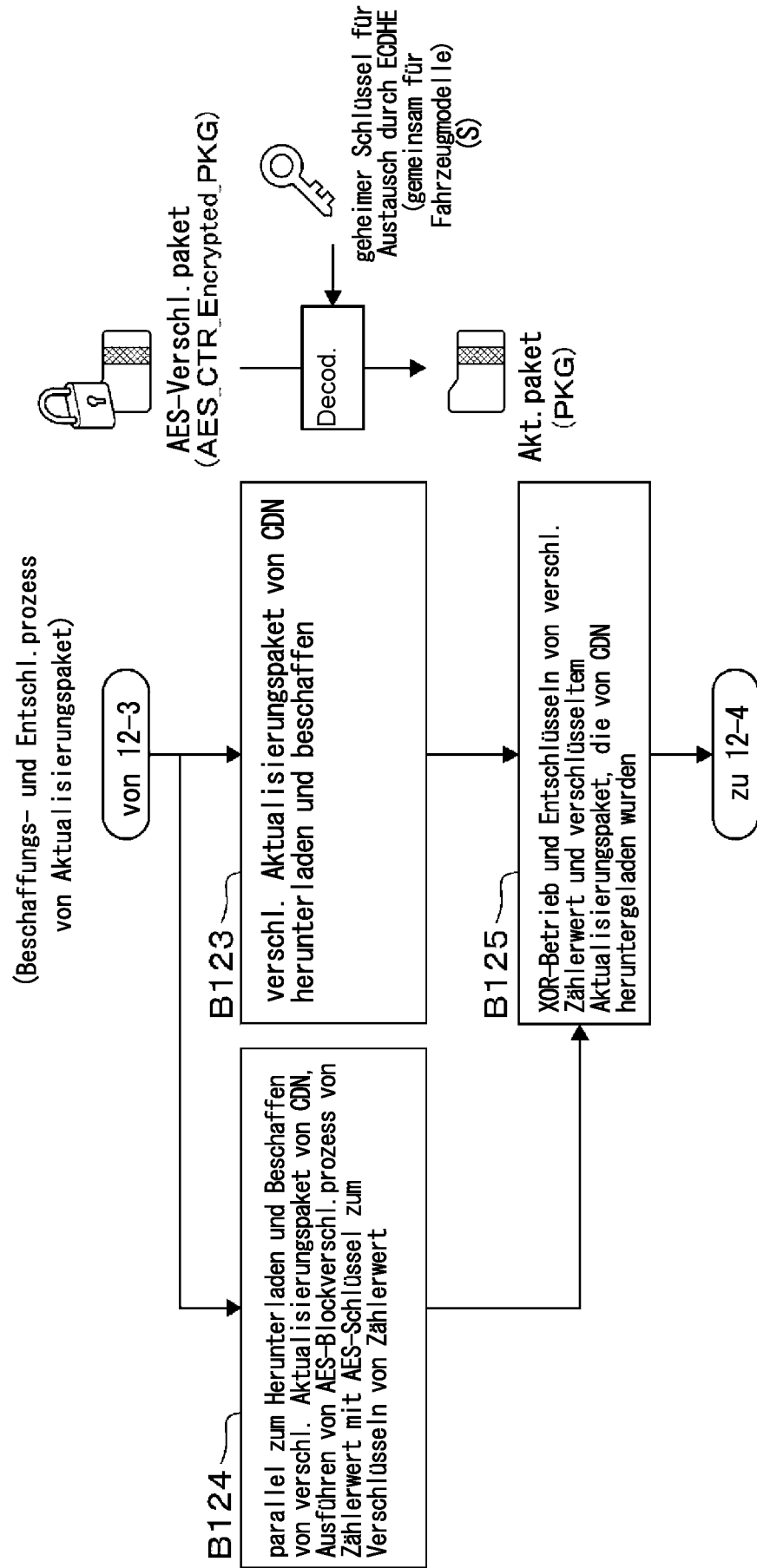
FIG. 114

FIG. 115

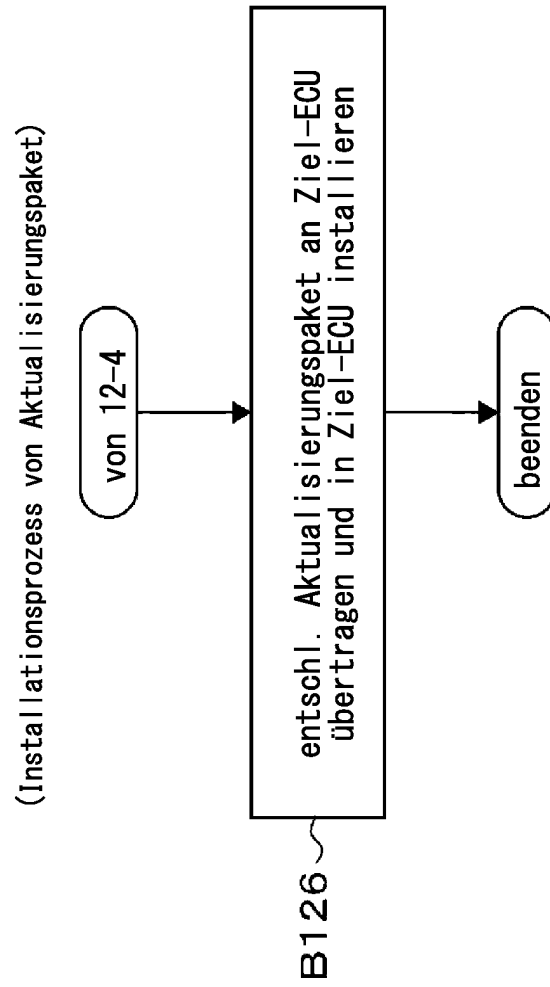


FIG. 116

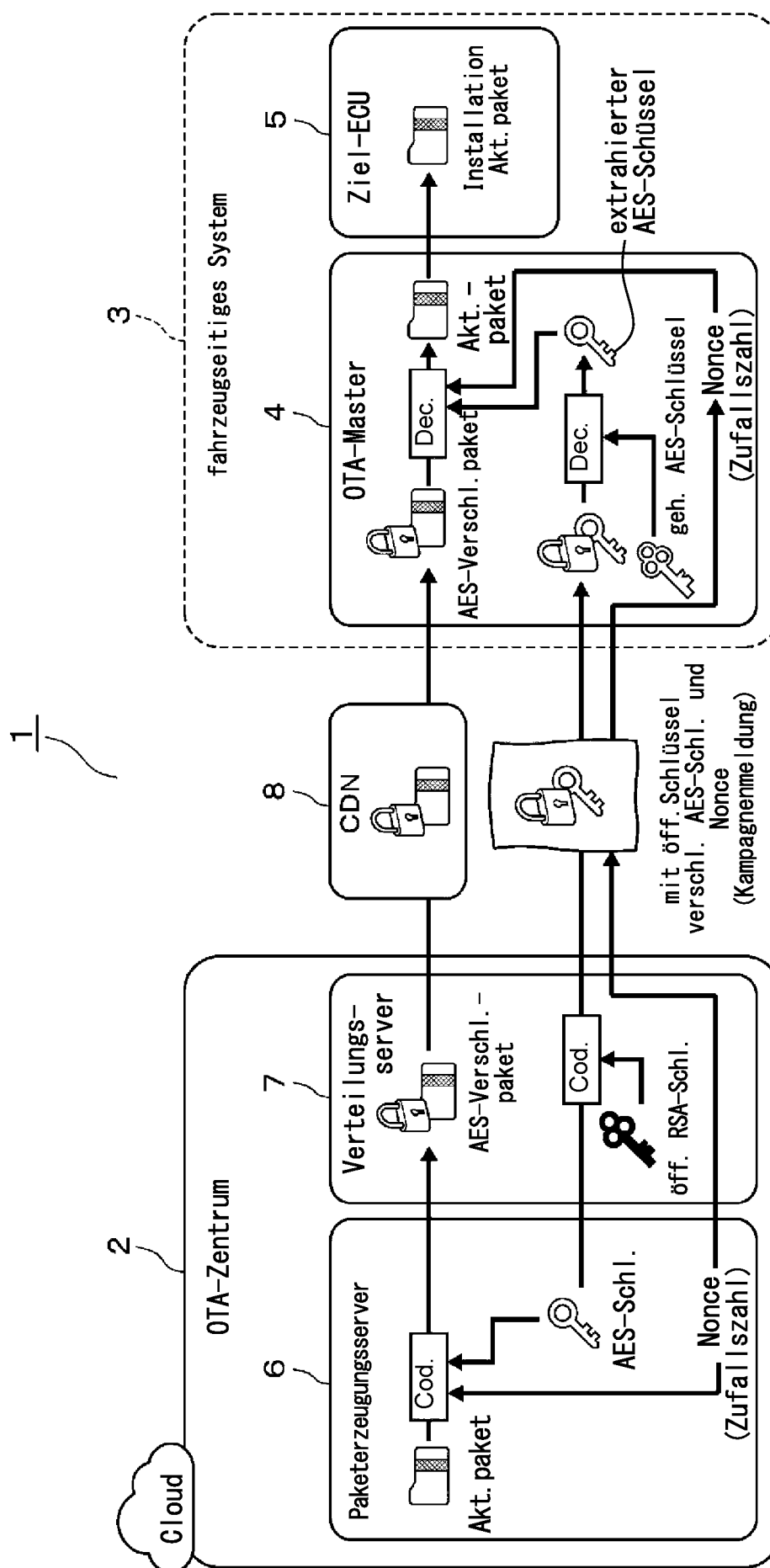


FIG. 117

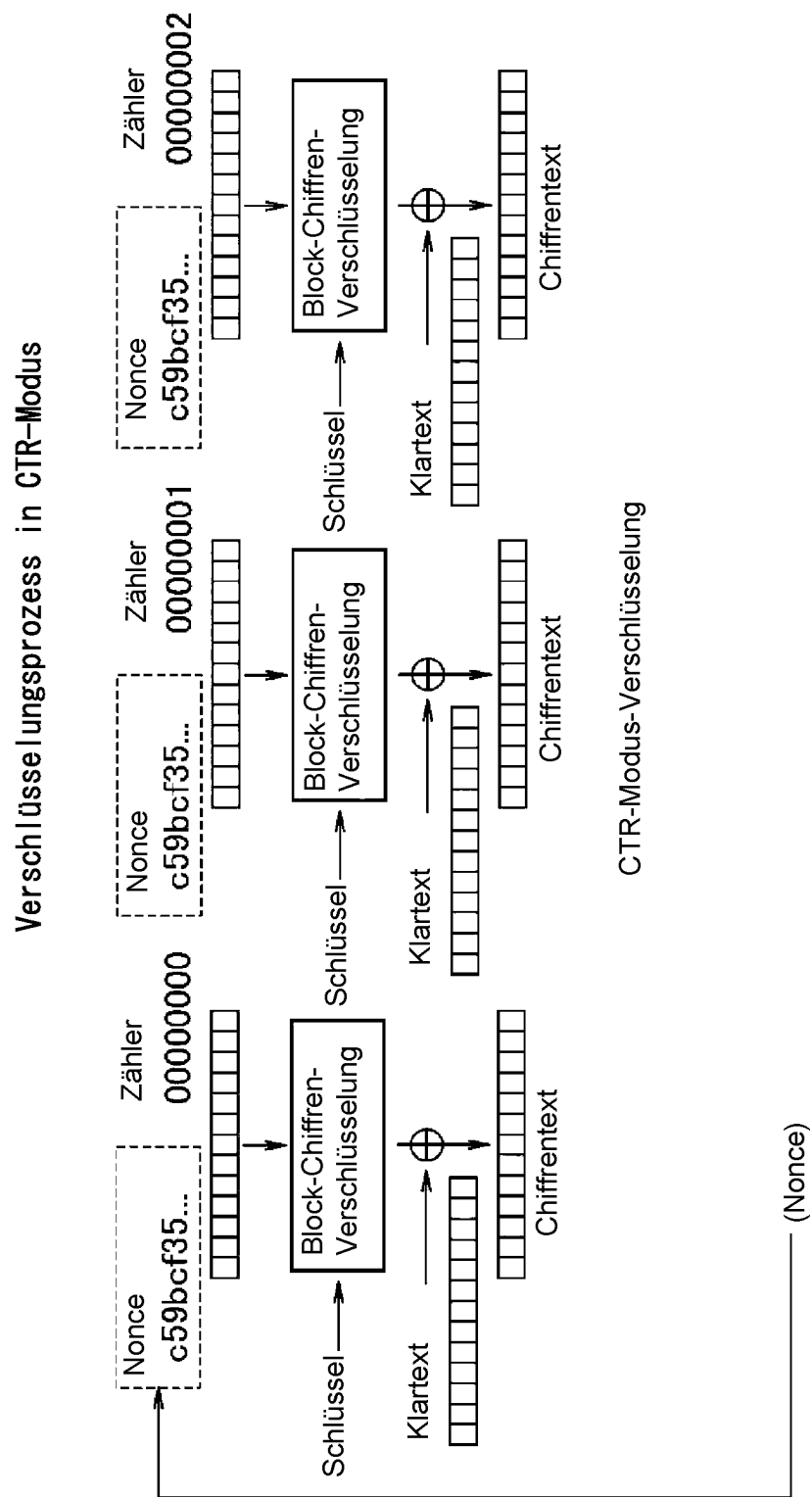


FIG. 118

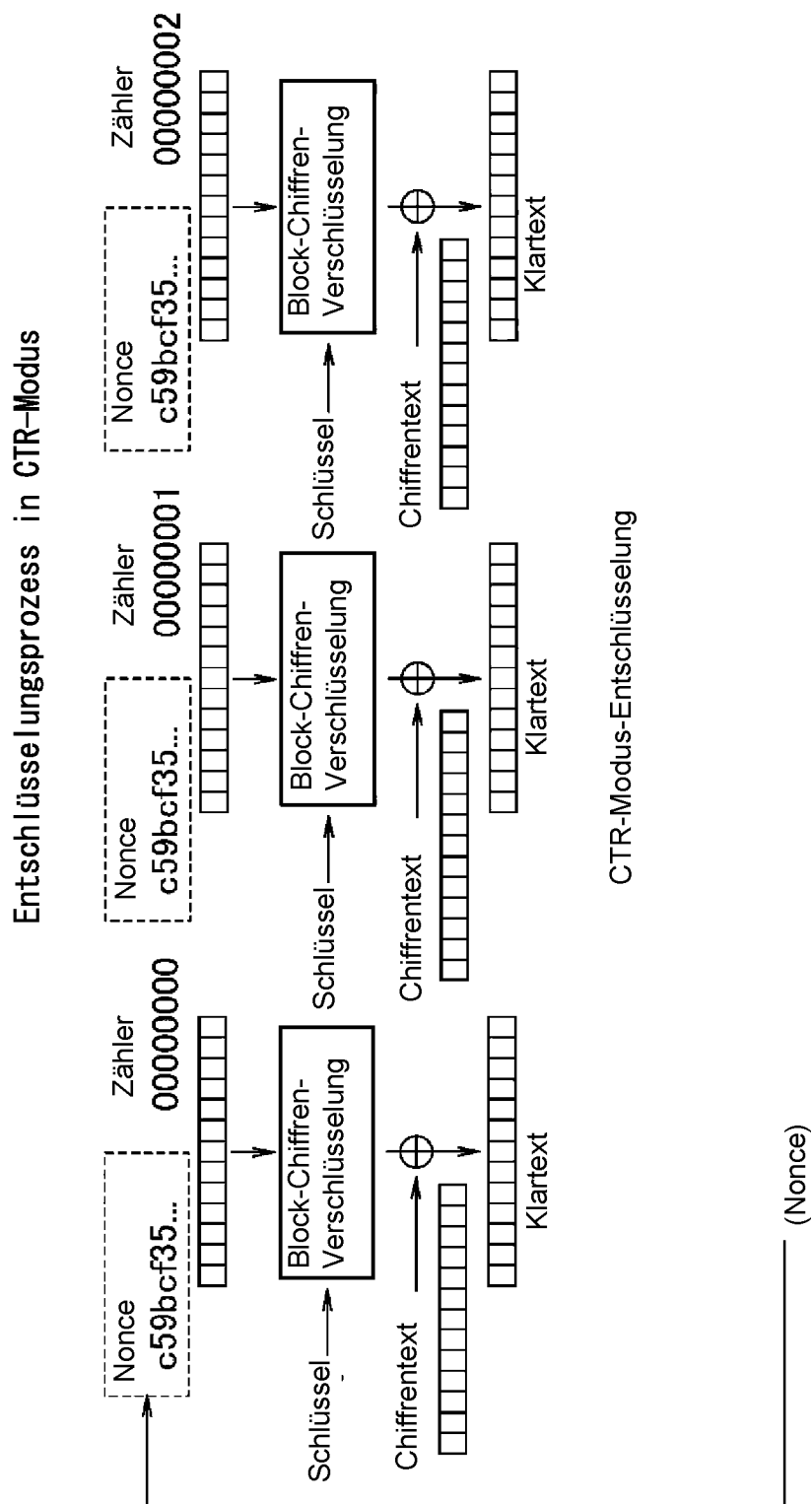


FIG. 119

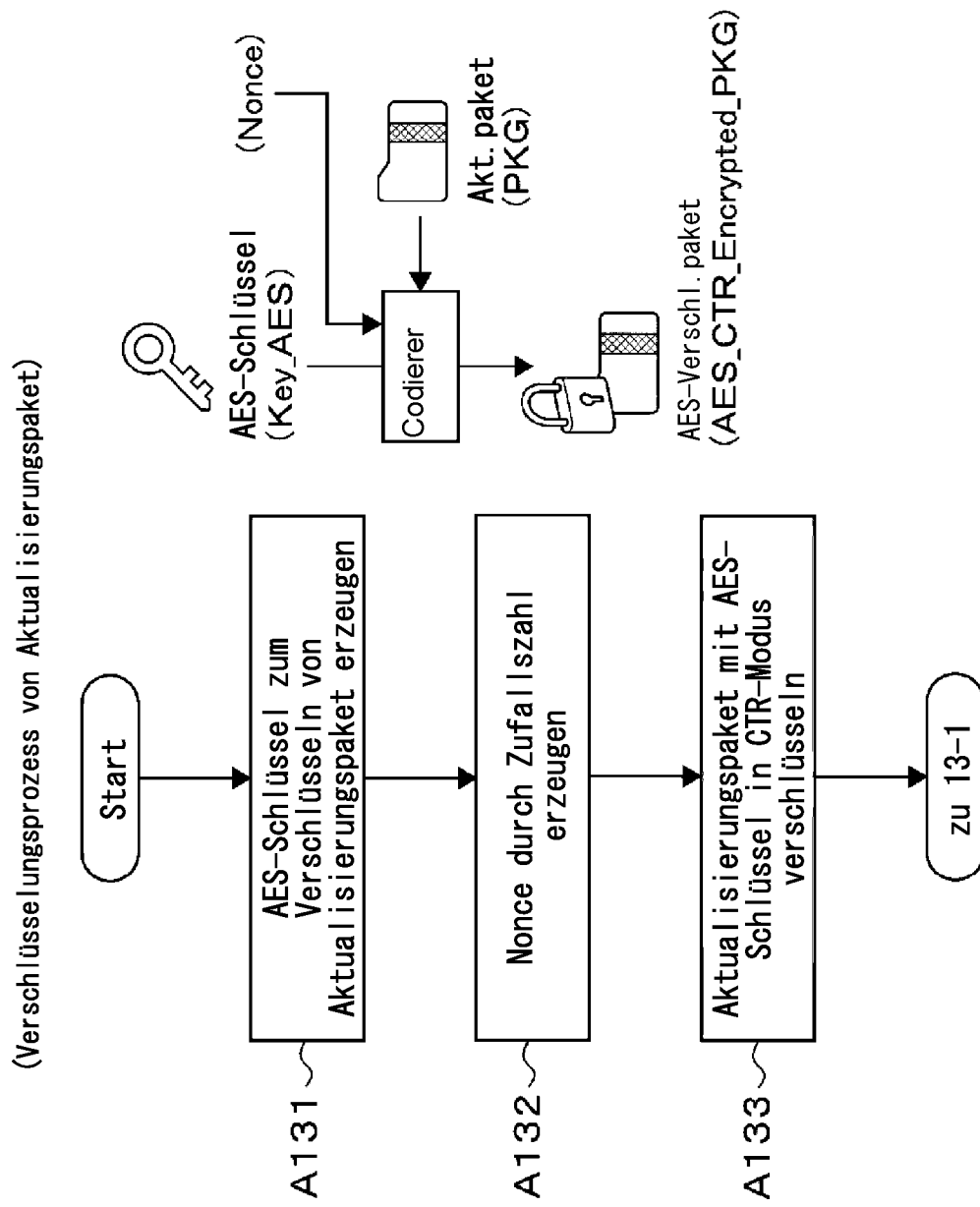


FIG. 120

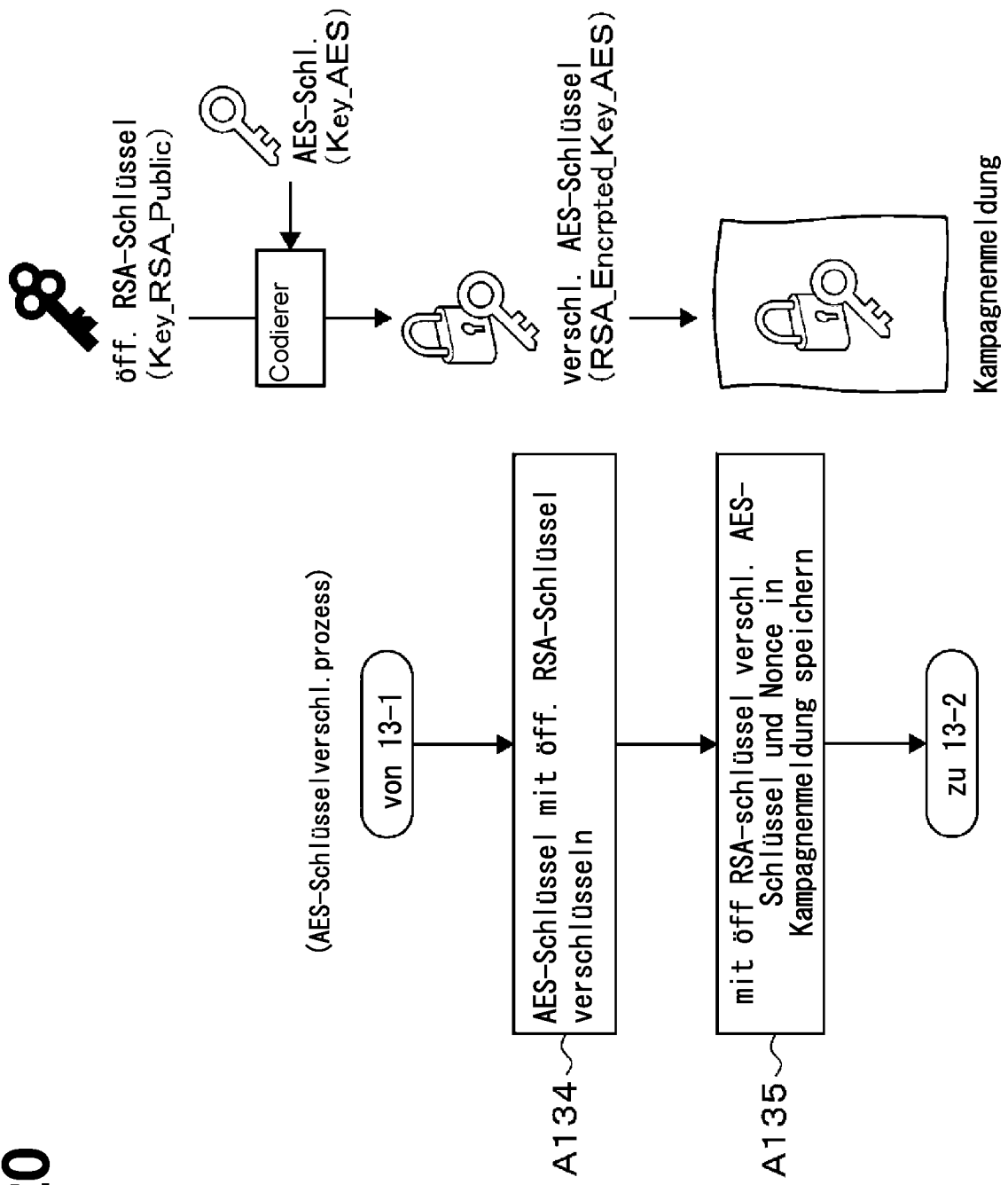


FIG. 121

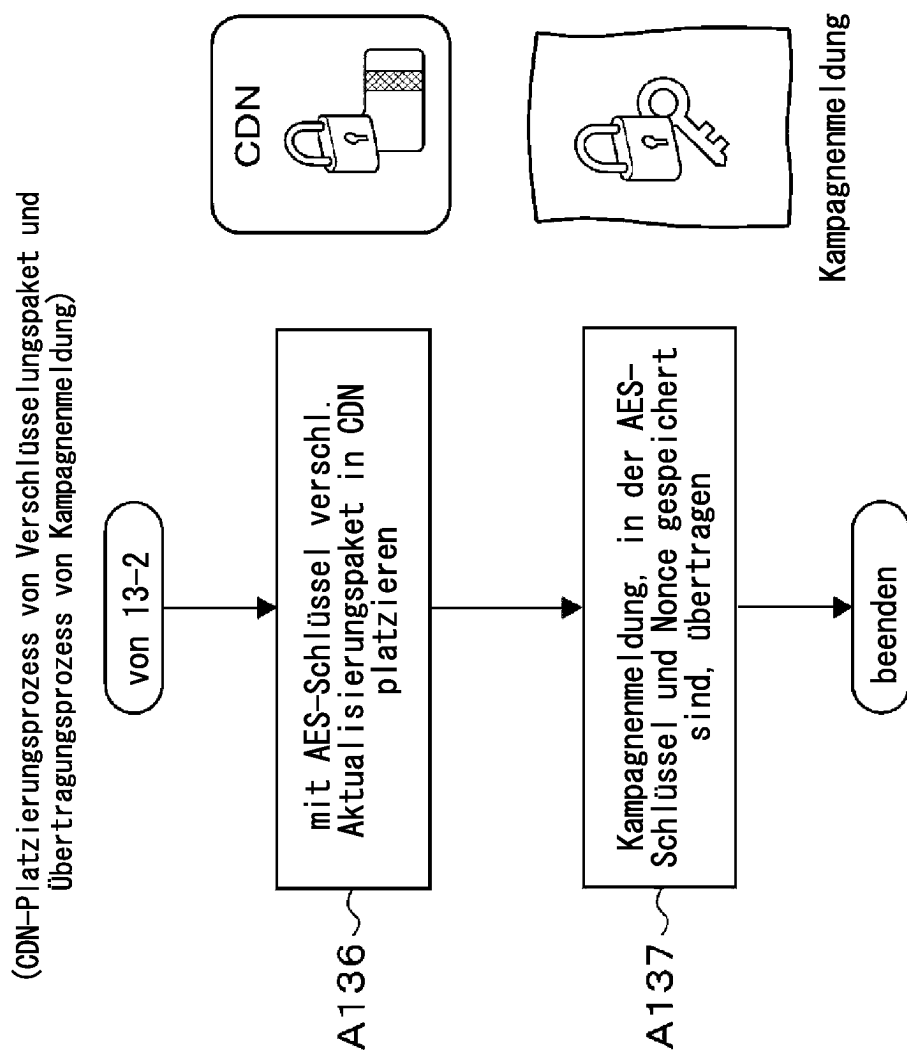


FIG. 122

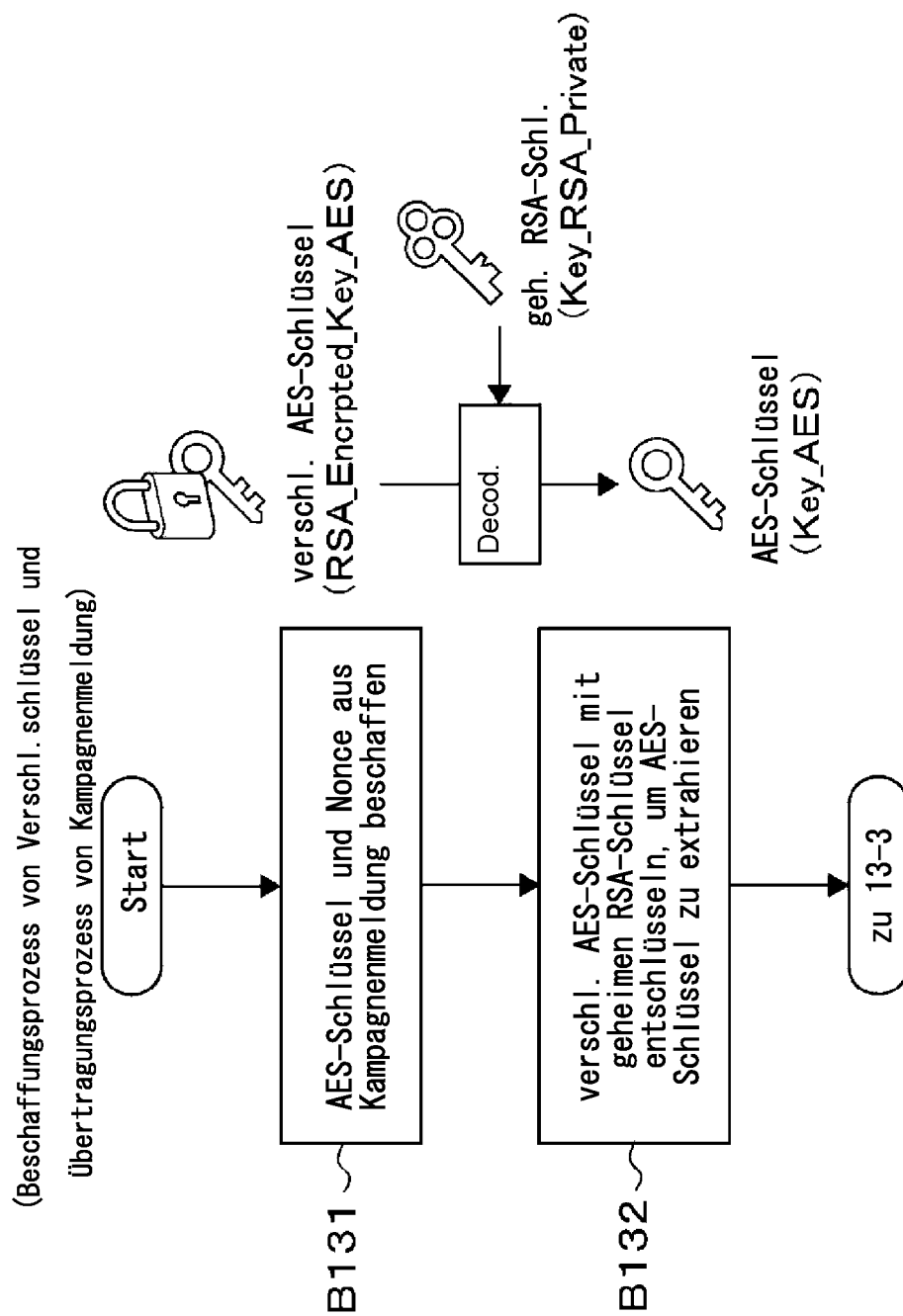


FIG. 123

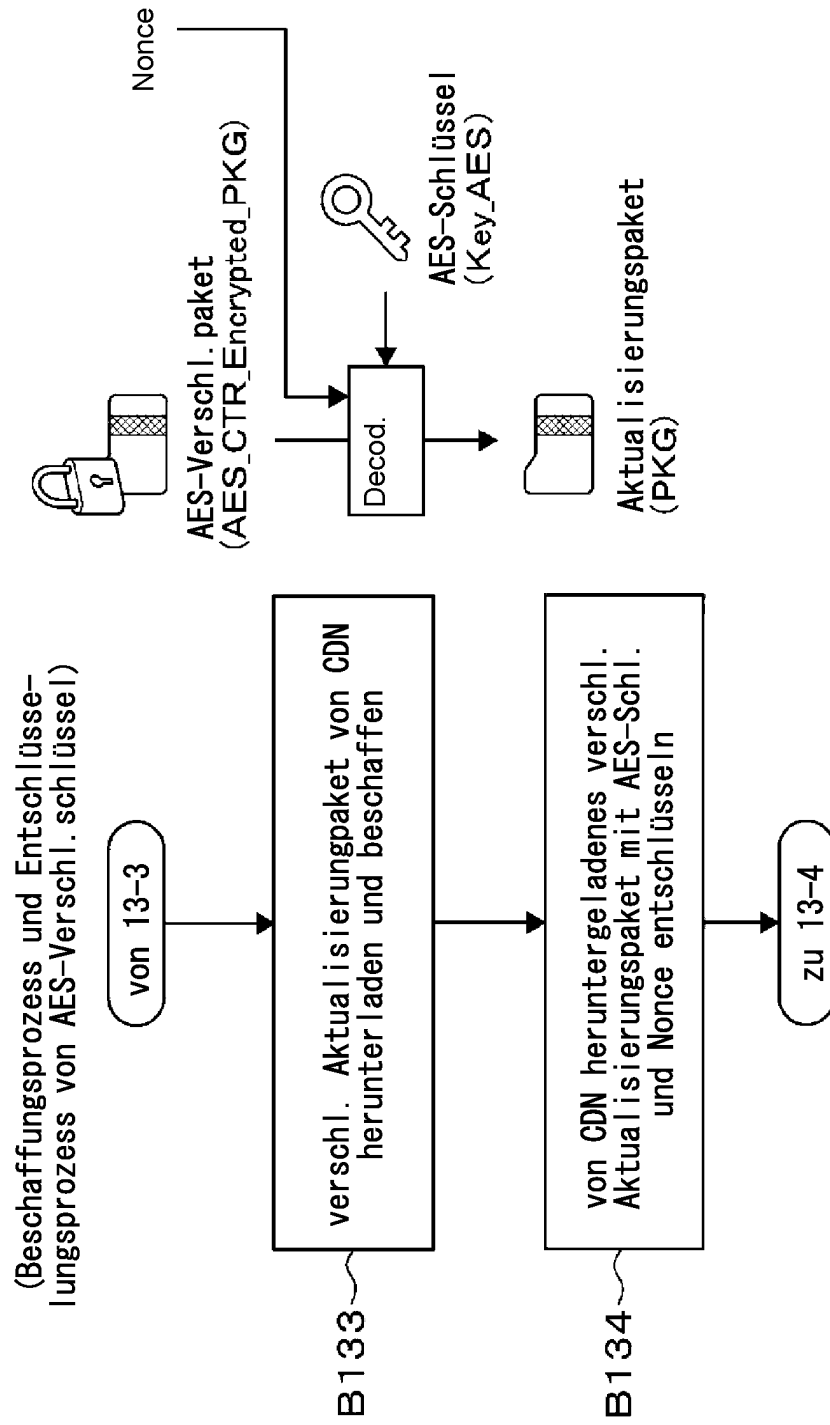


FIG. 124

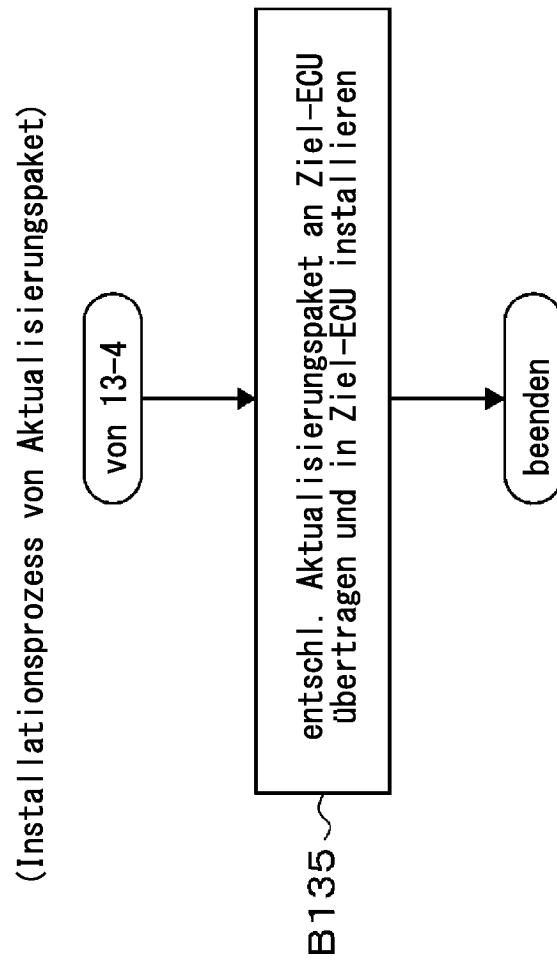


FIG. 125

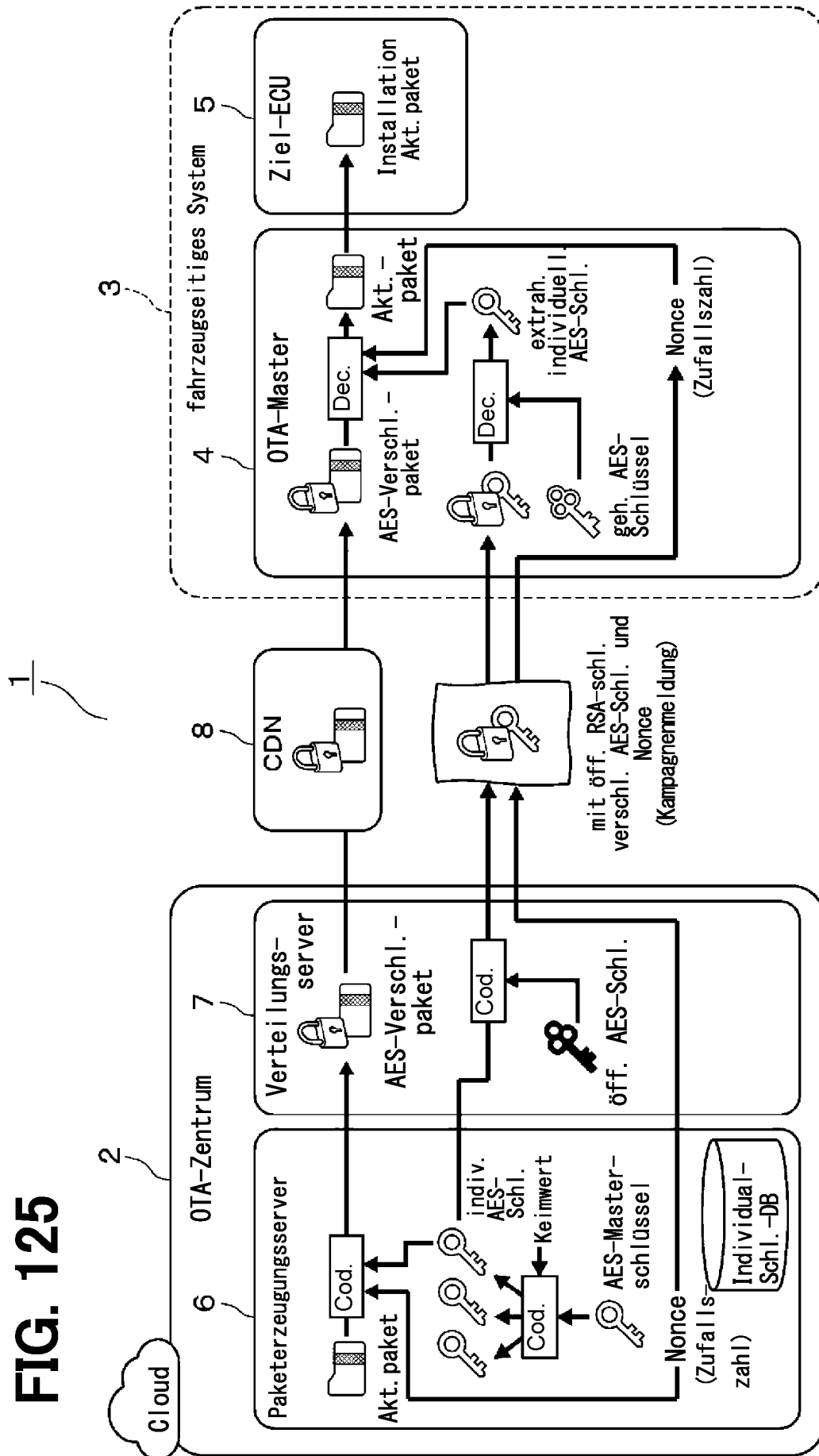


FIG. 126

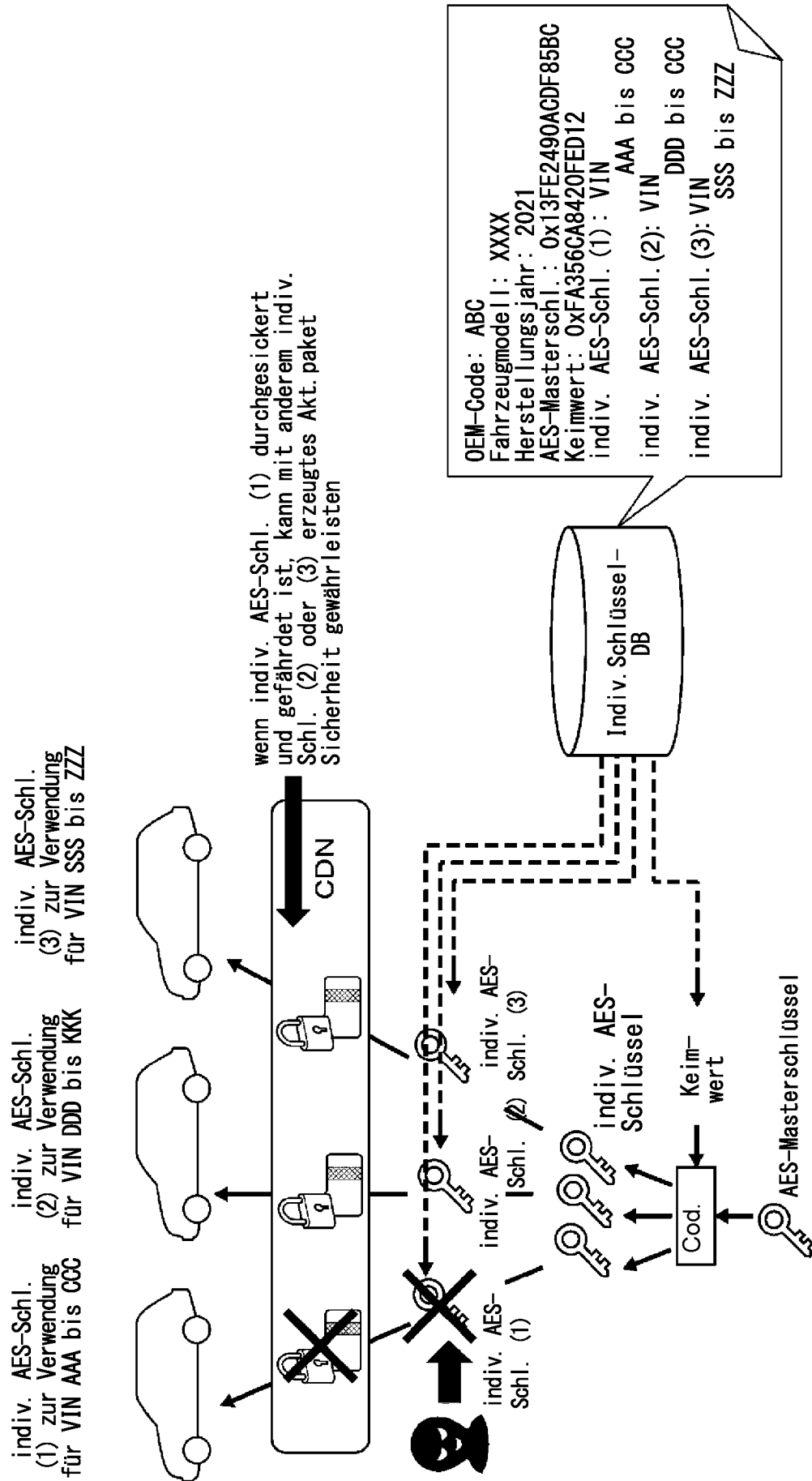


FIG. 127

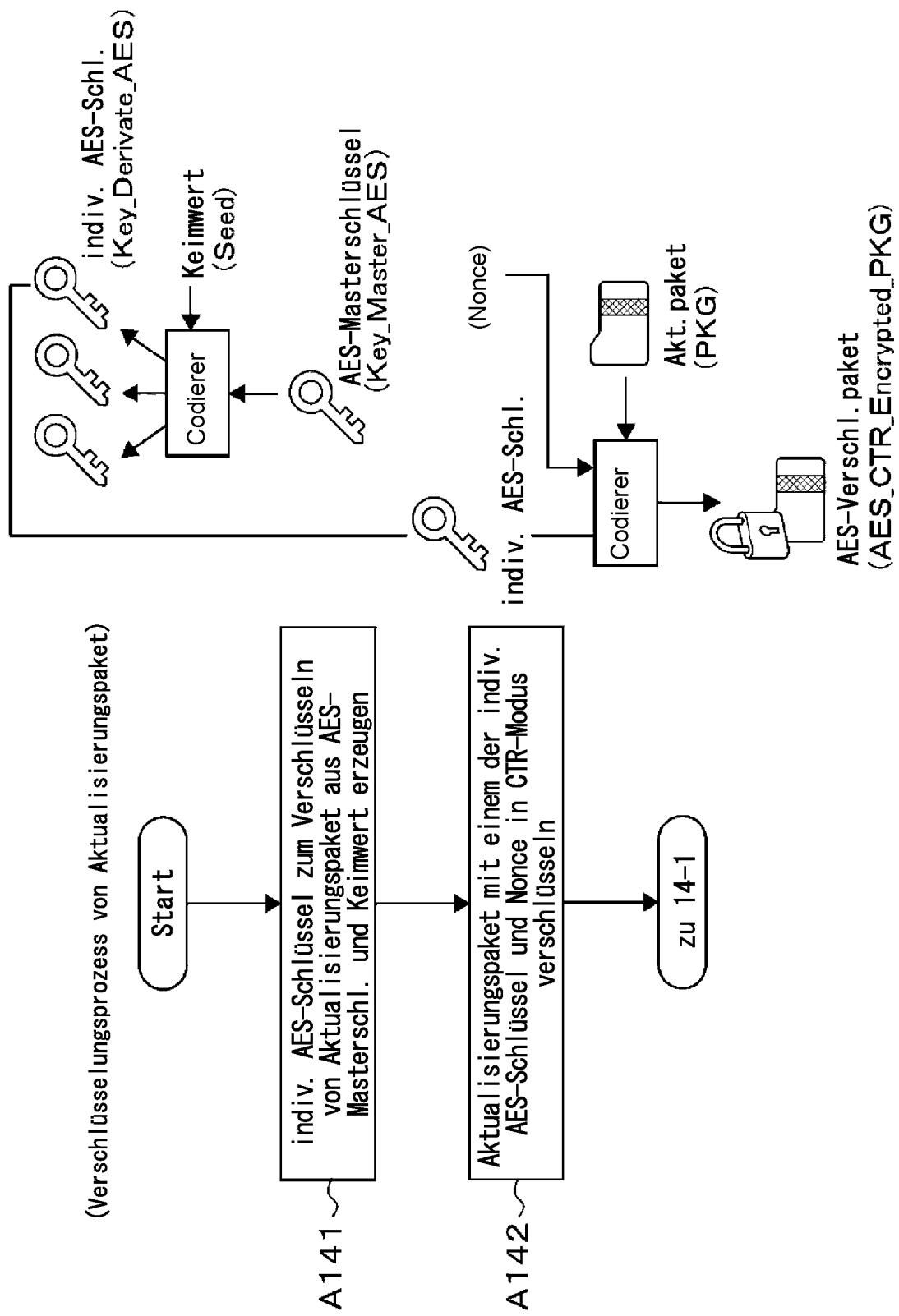


FIG. 128

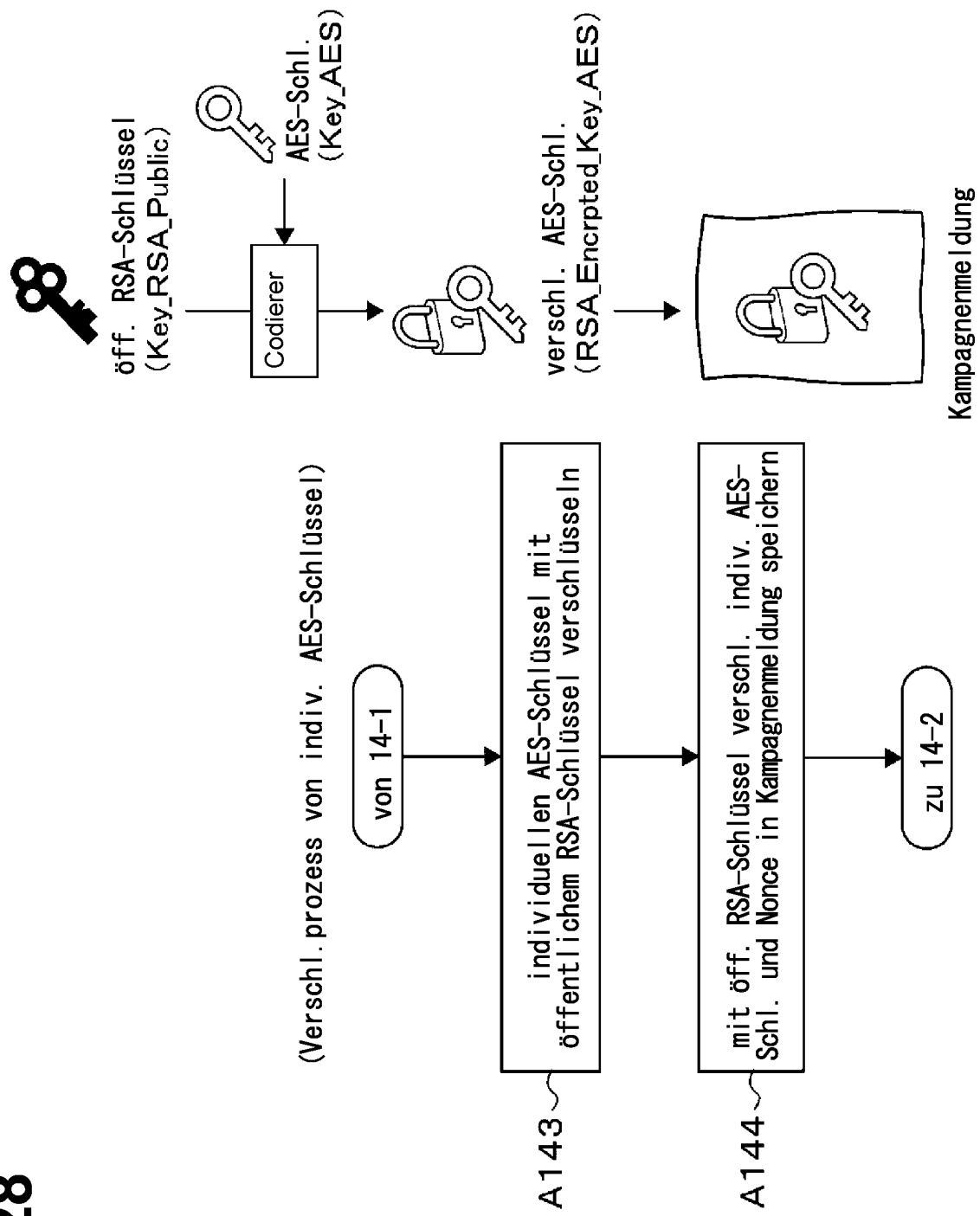


FIG. 129

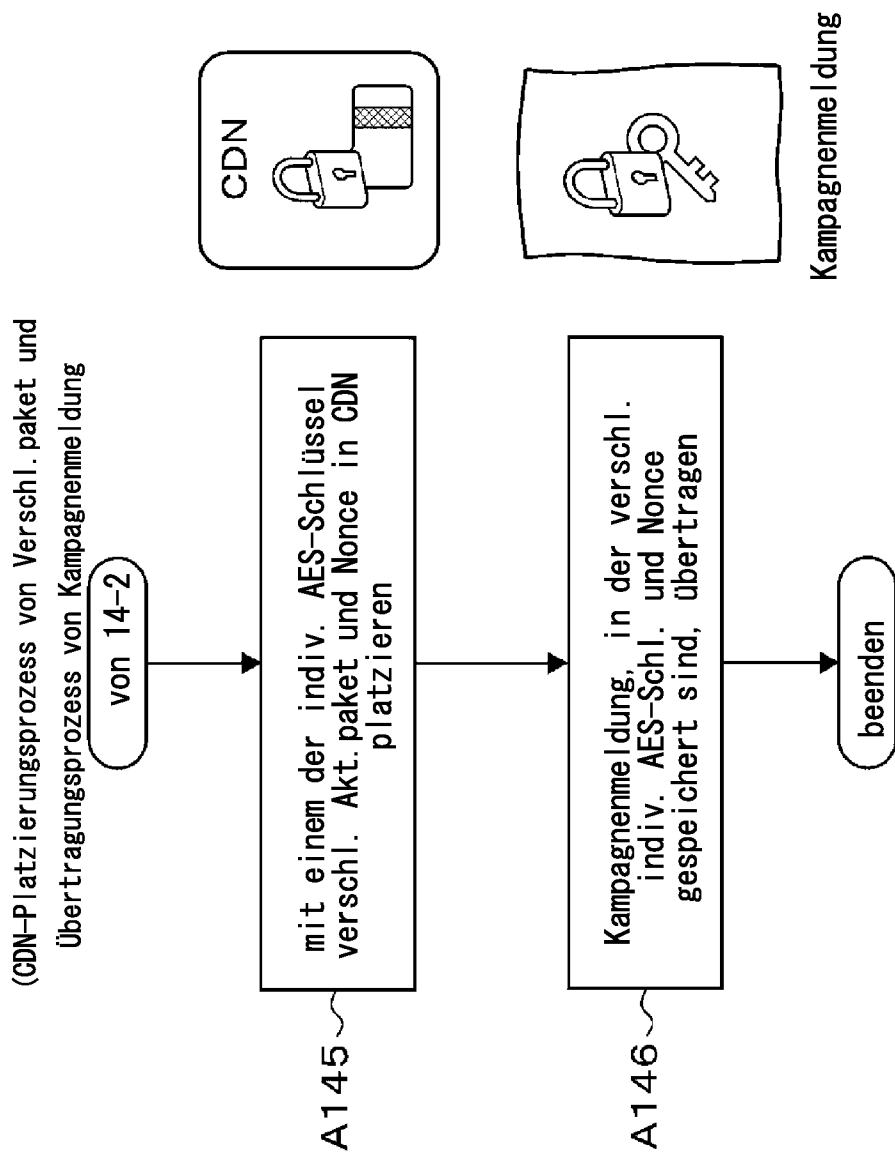


FIG. 130

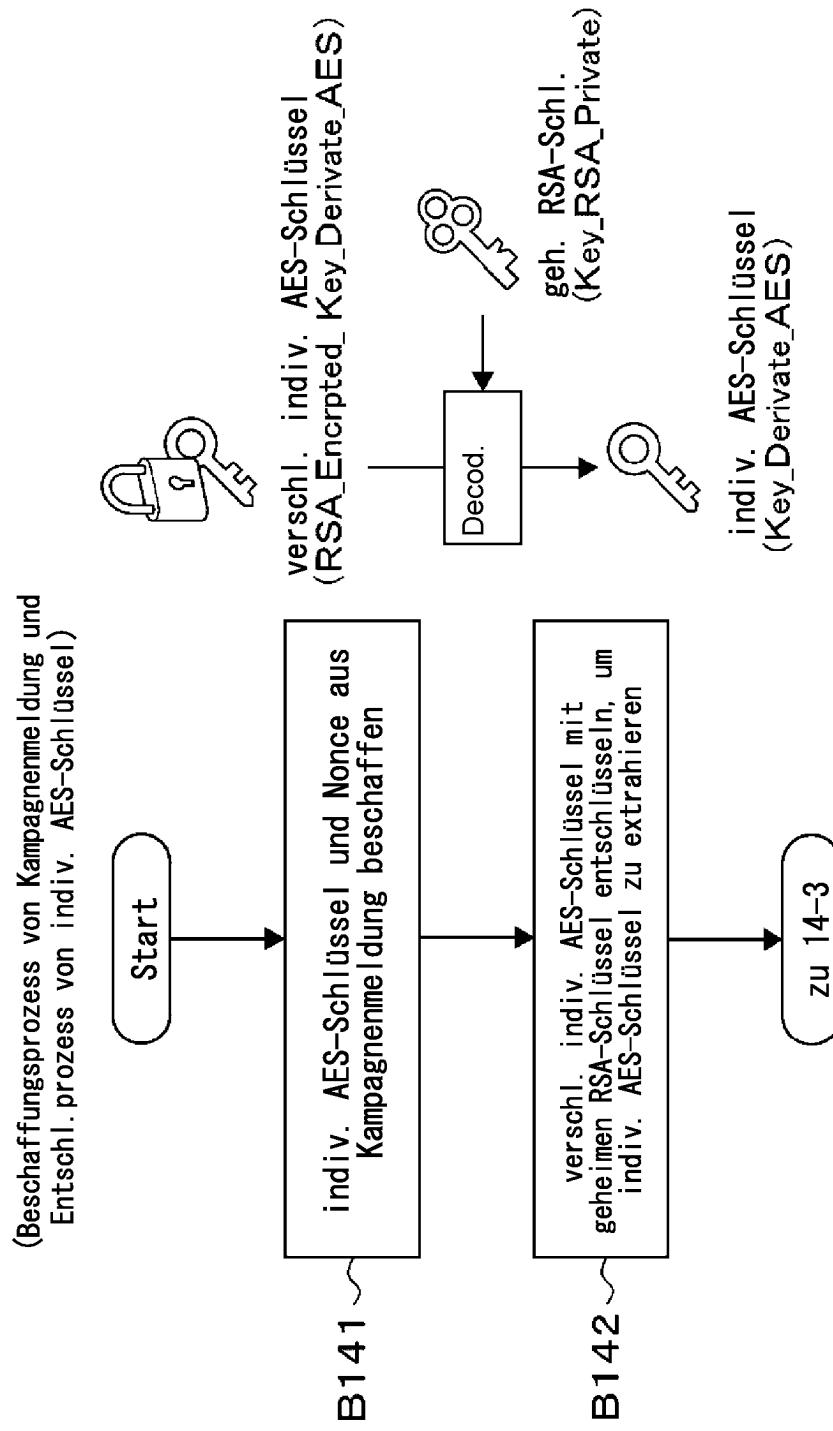


FIG. 131

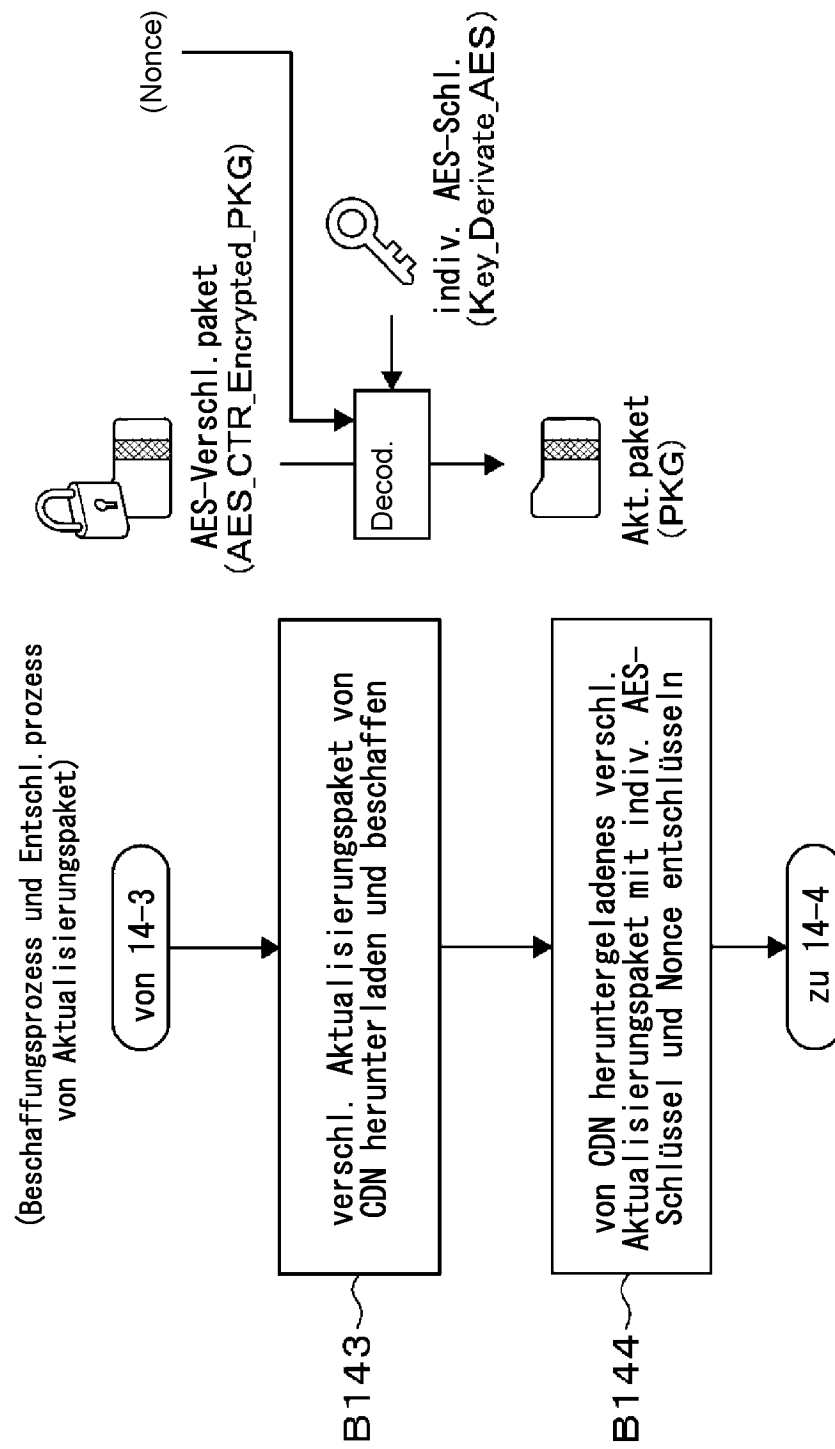
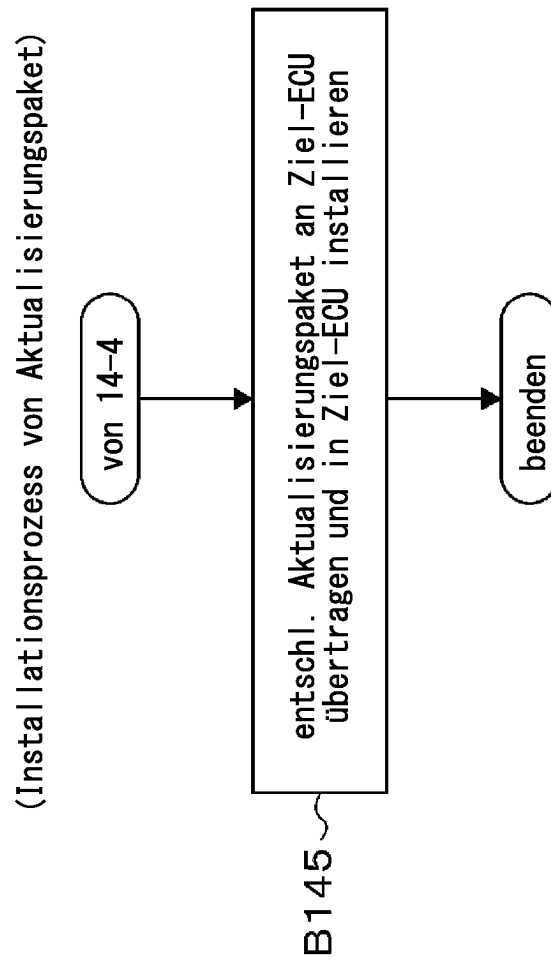


FIG. 132



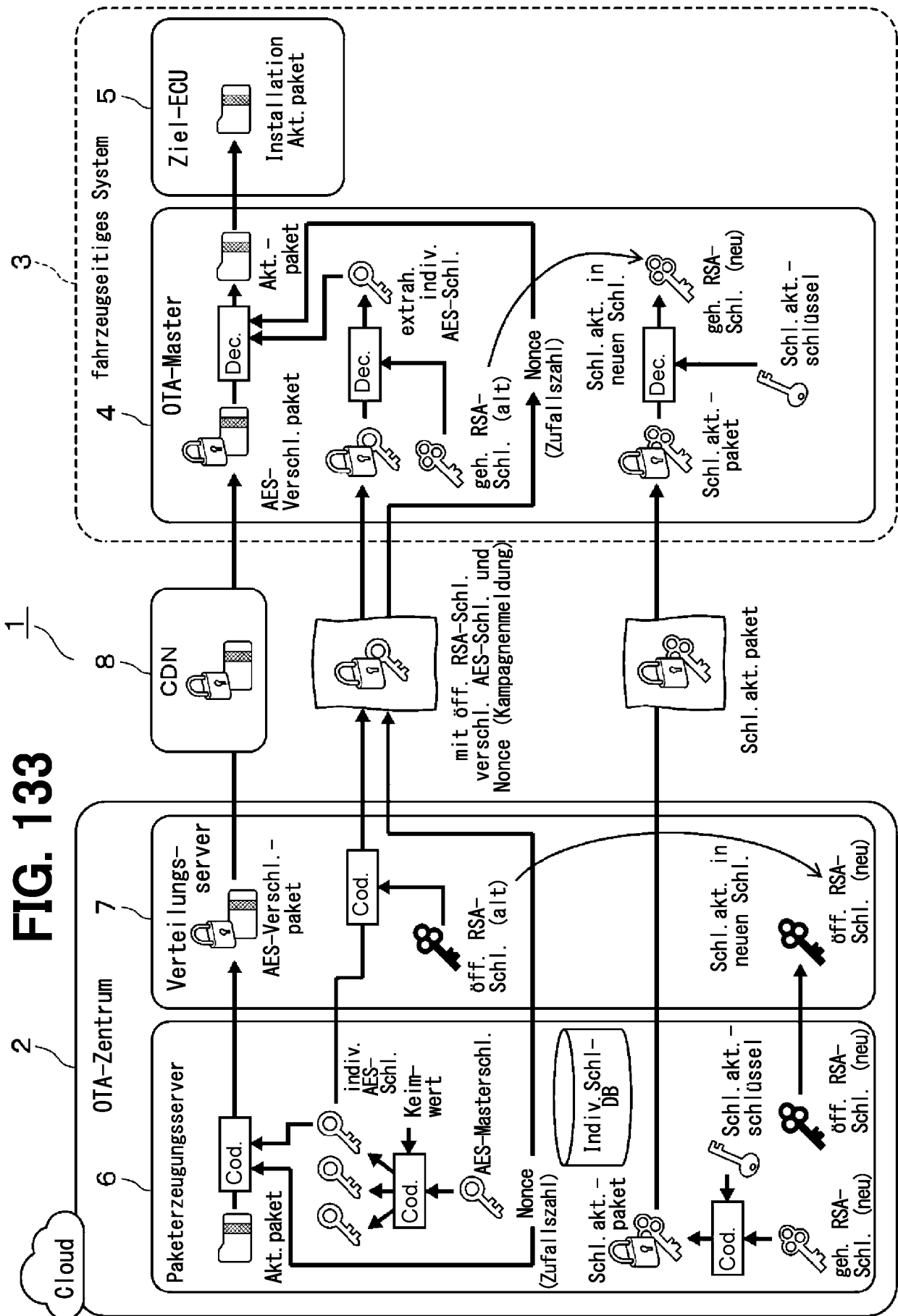


FIG. 134

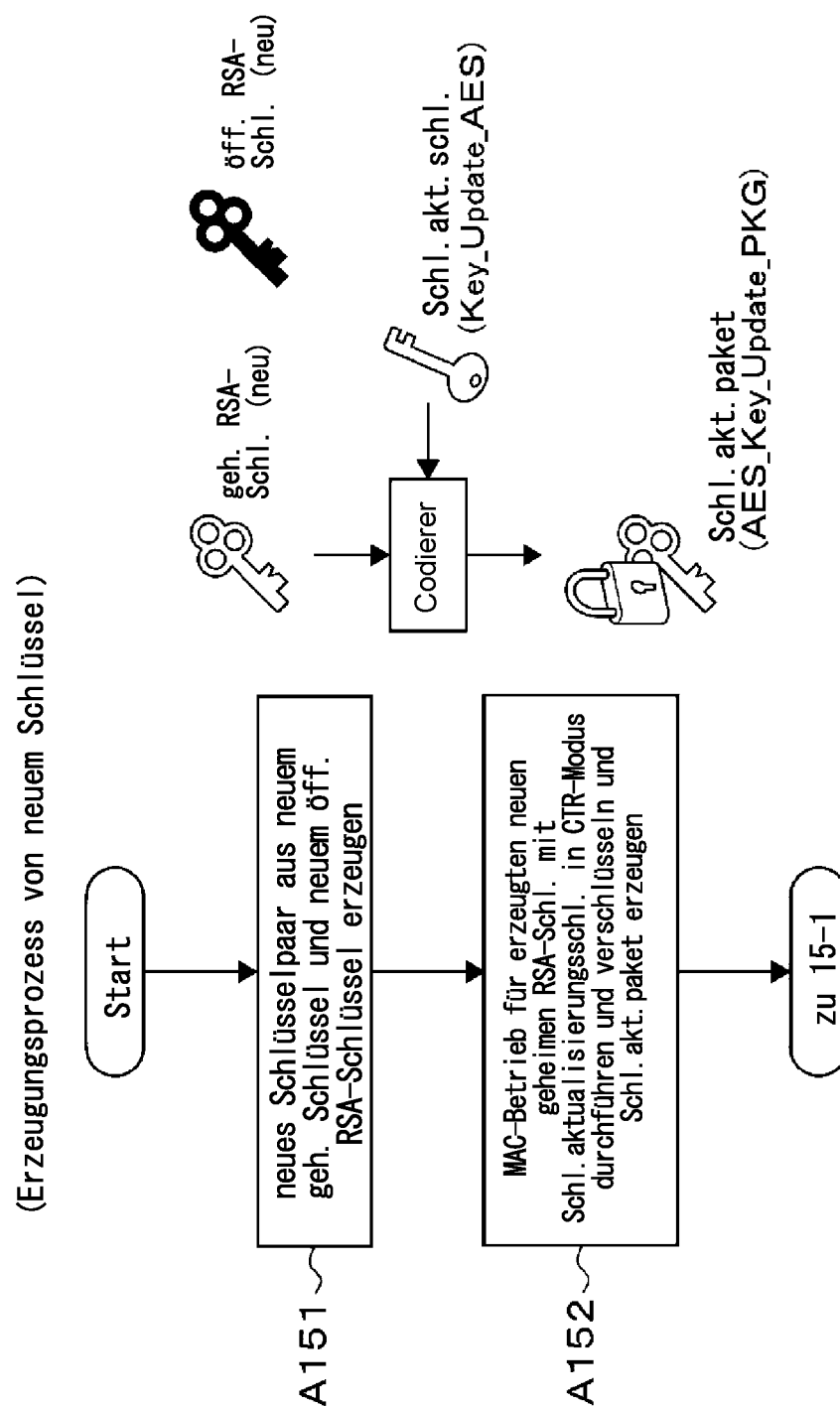


FIG. 135

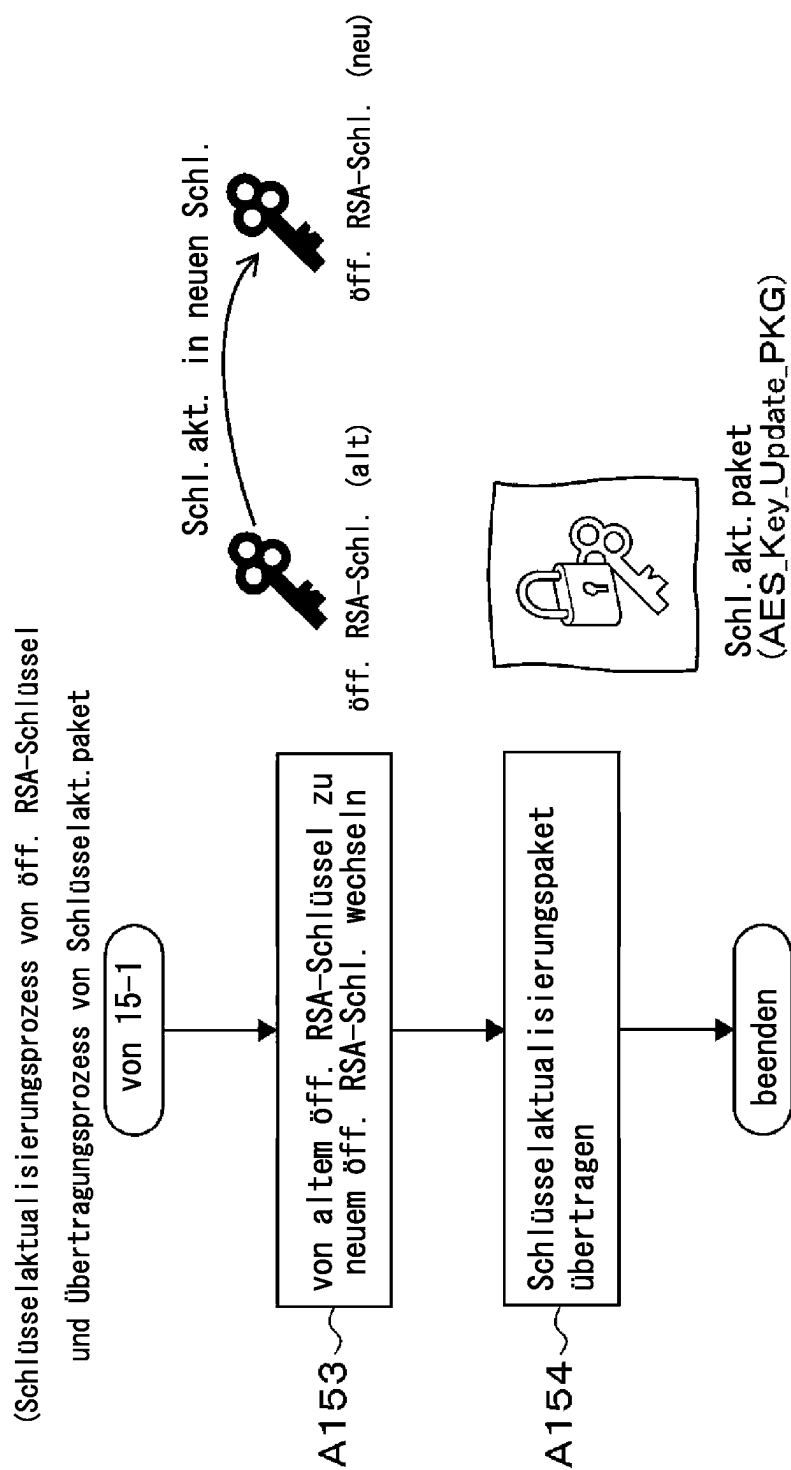


FIG. 136

(Beschaffungsprozess, Entschl.prozess und
Verifizierungsprozess von Schlüsselaktualisierungspaket)

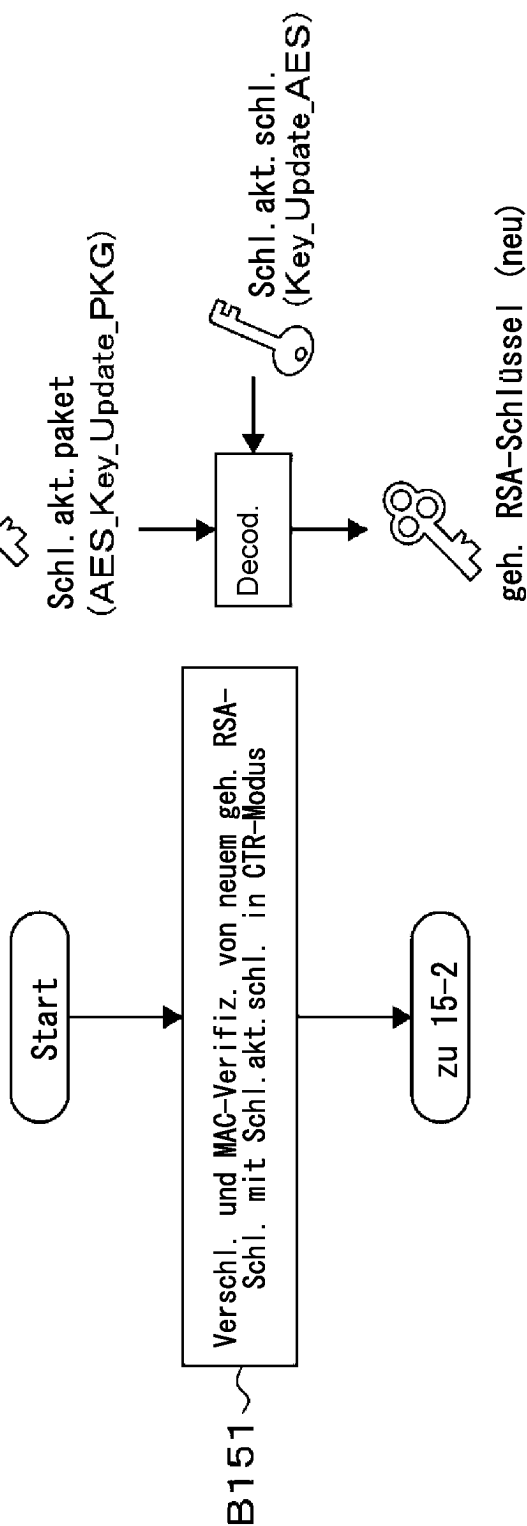


FIG. 137

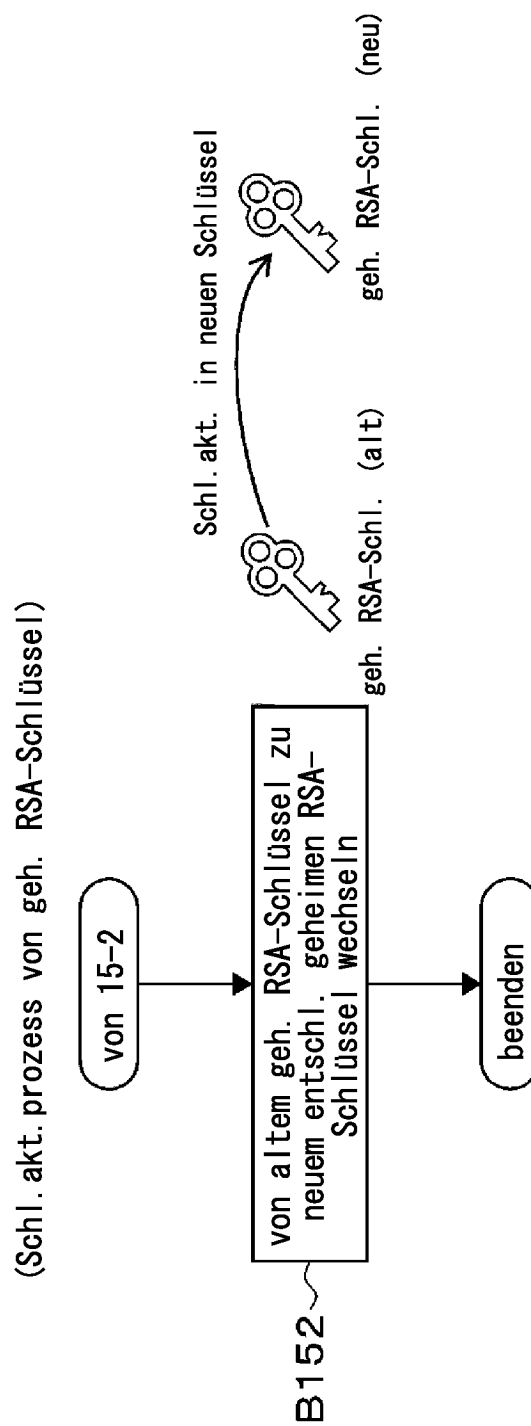


FIG. 139

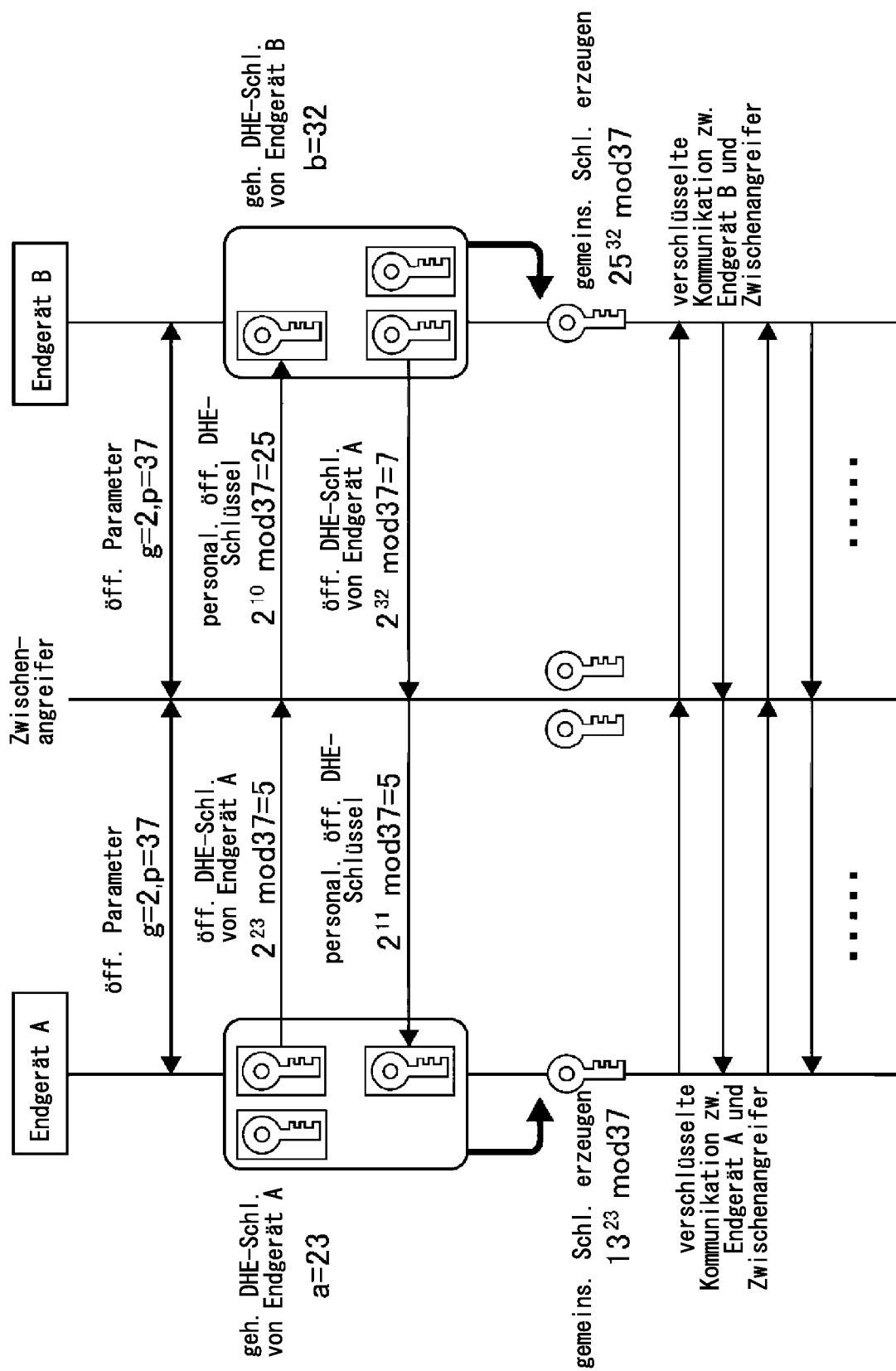


FIG. 140

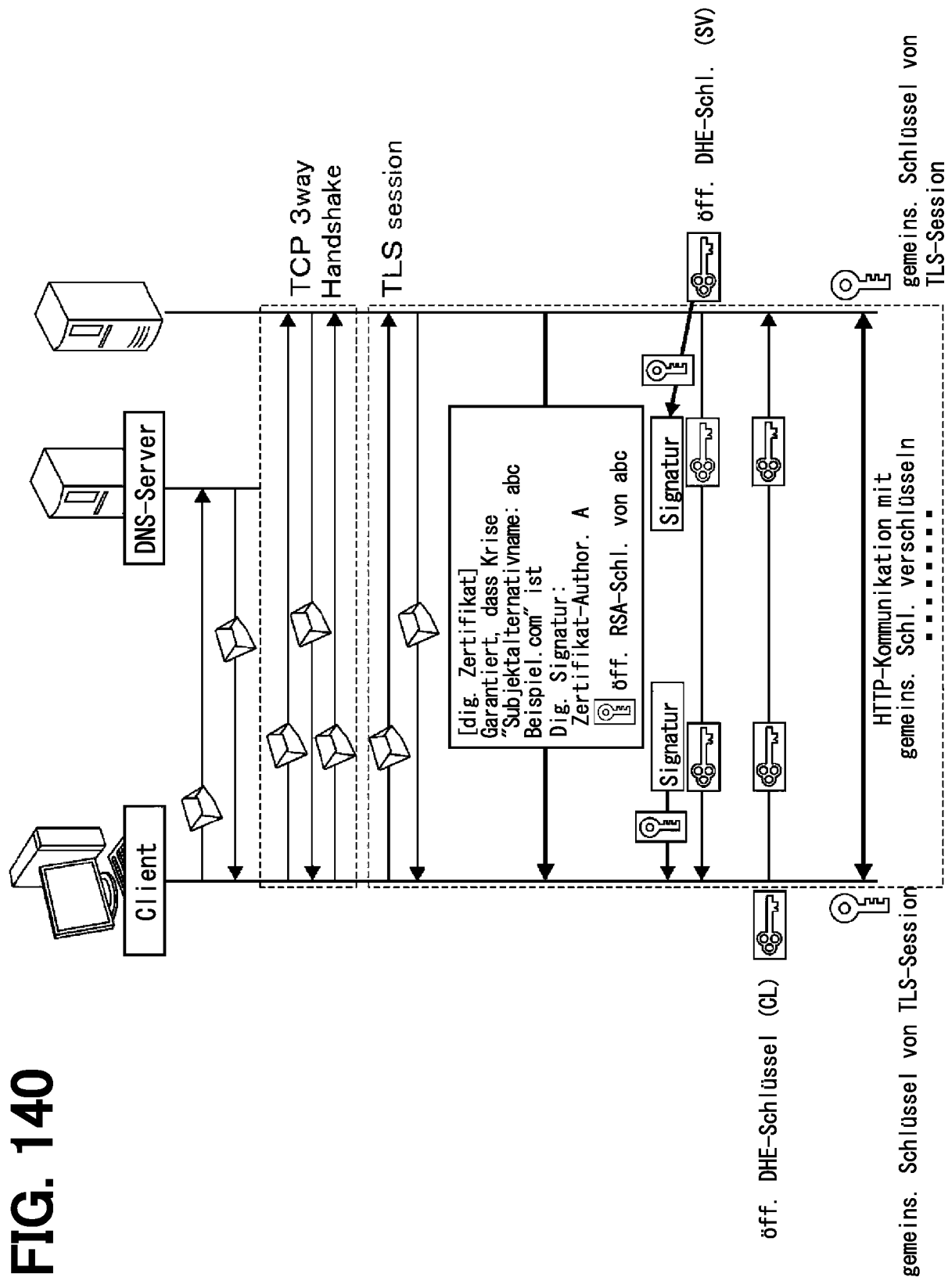


FIG. 141

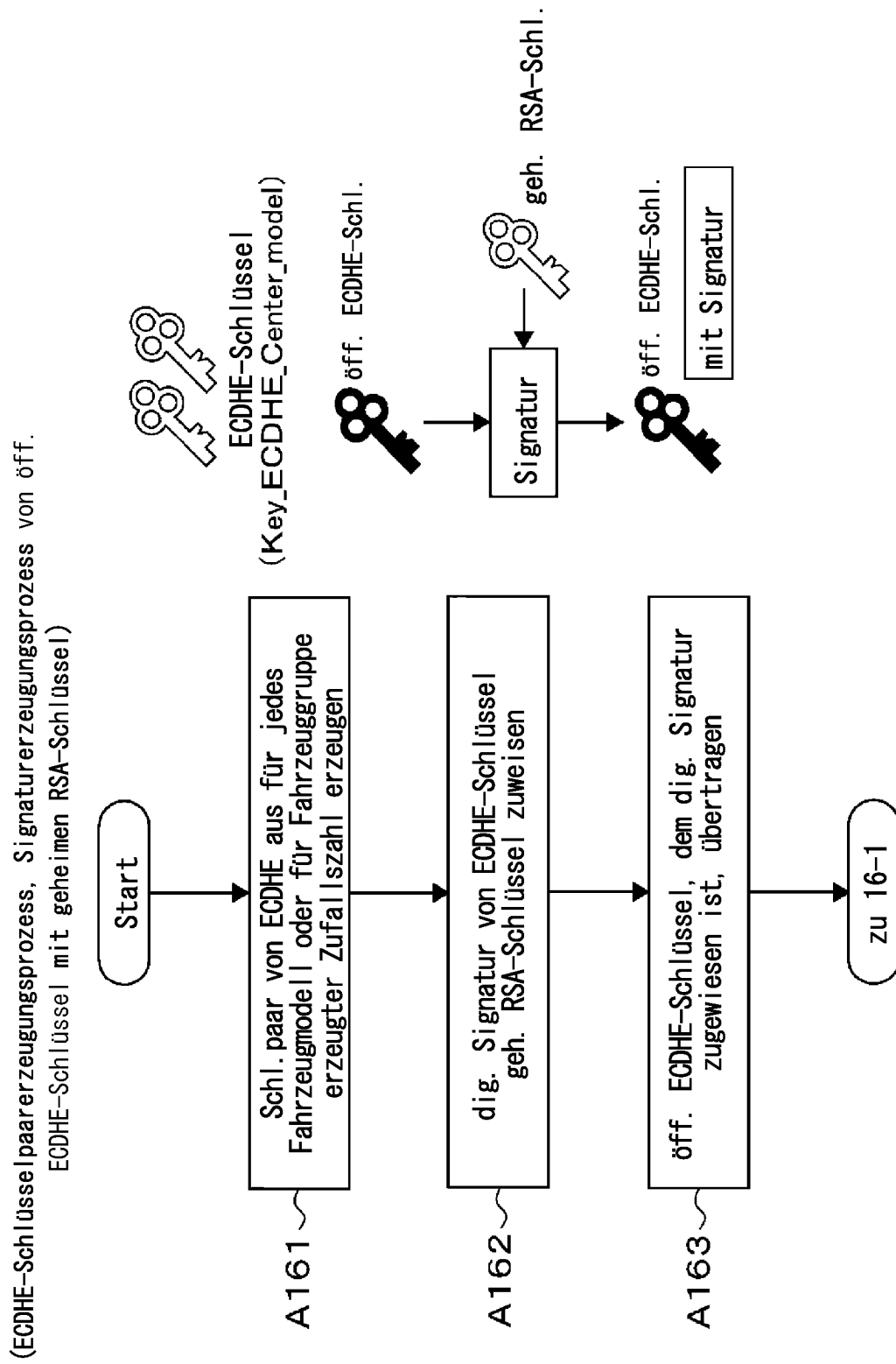


FIG. 142

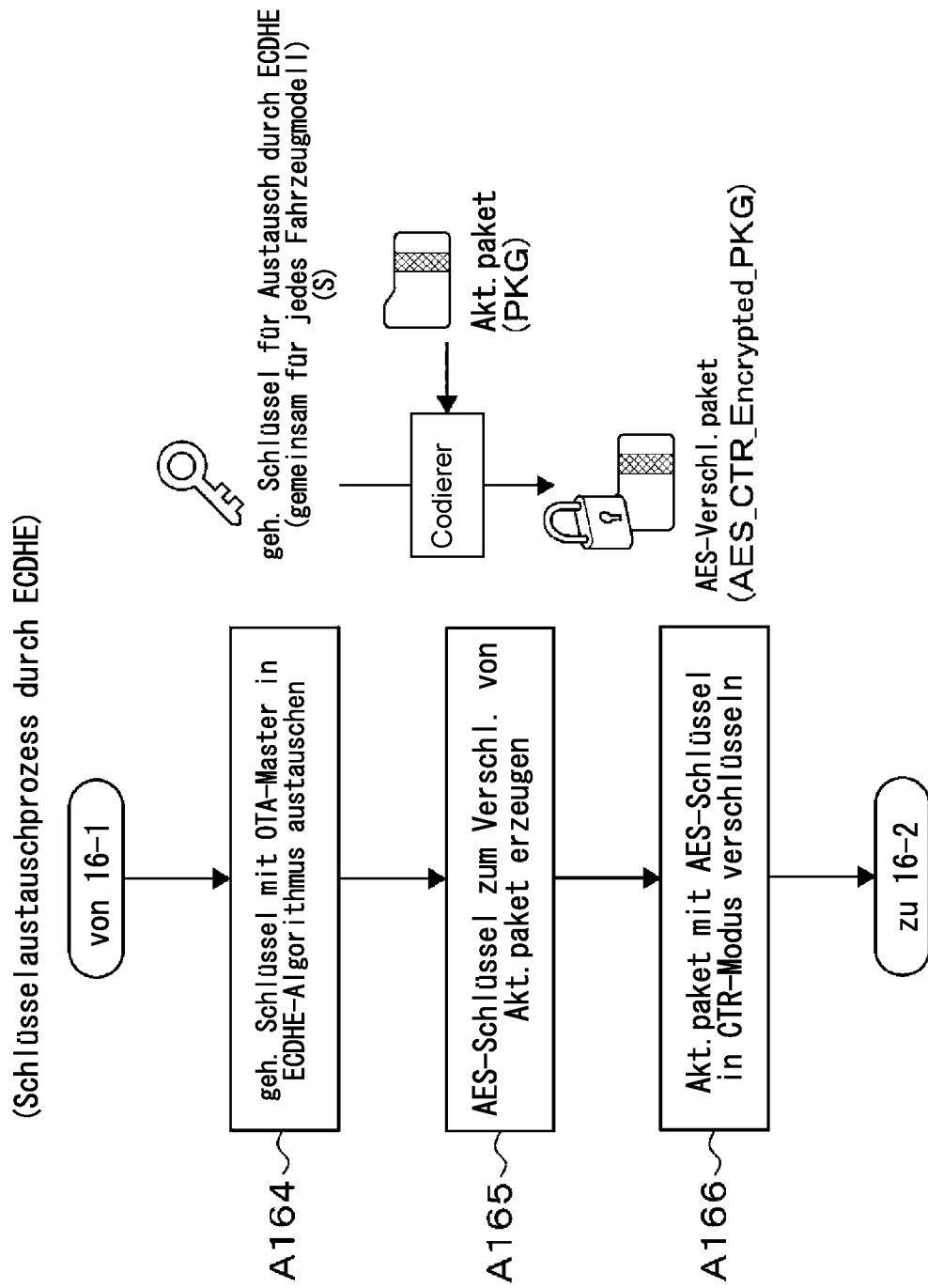


FIG. 143

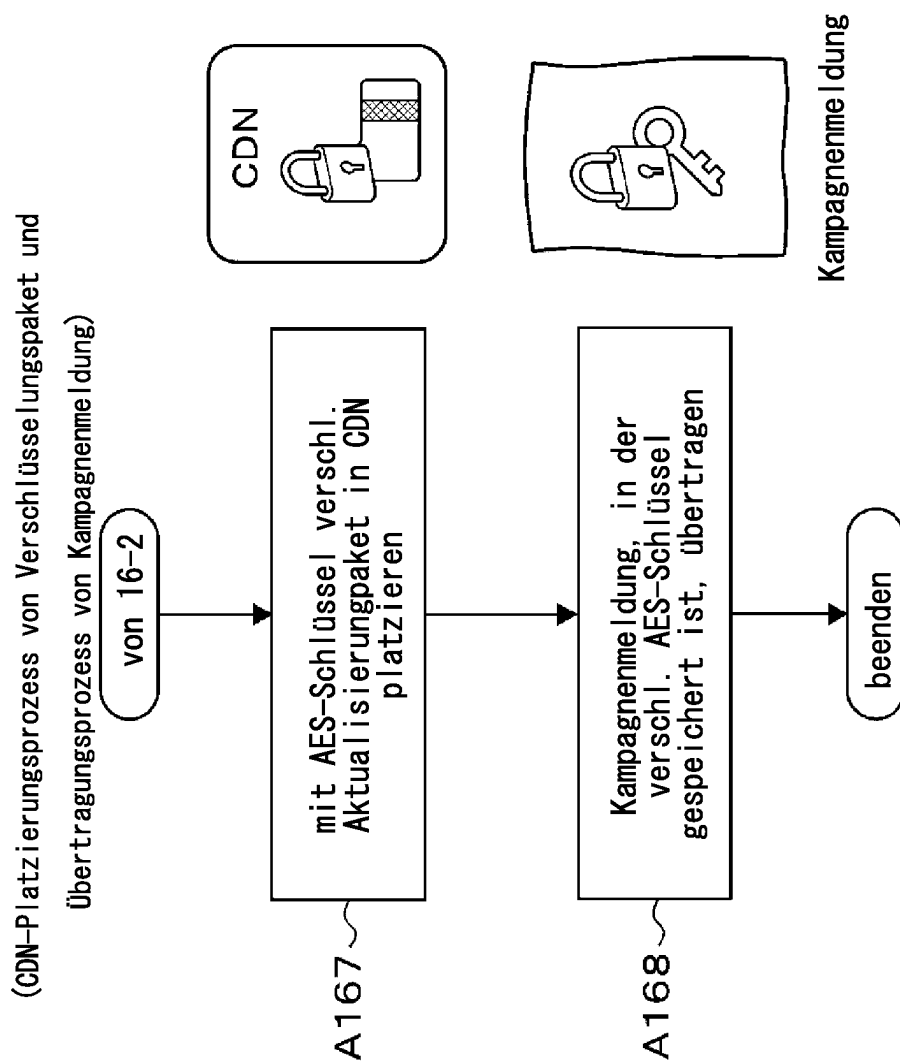


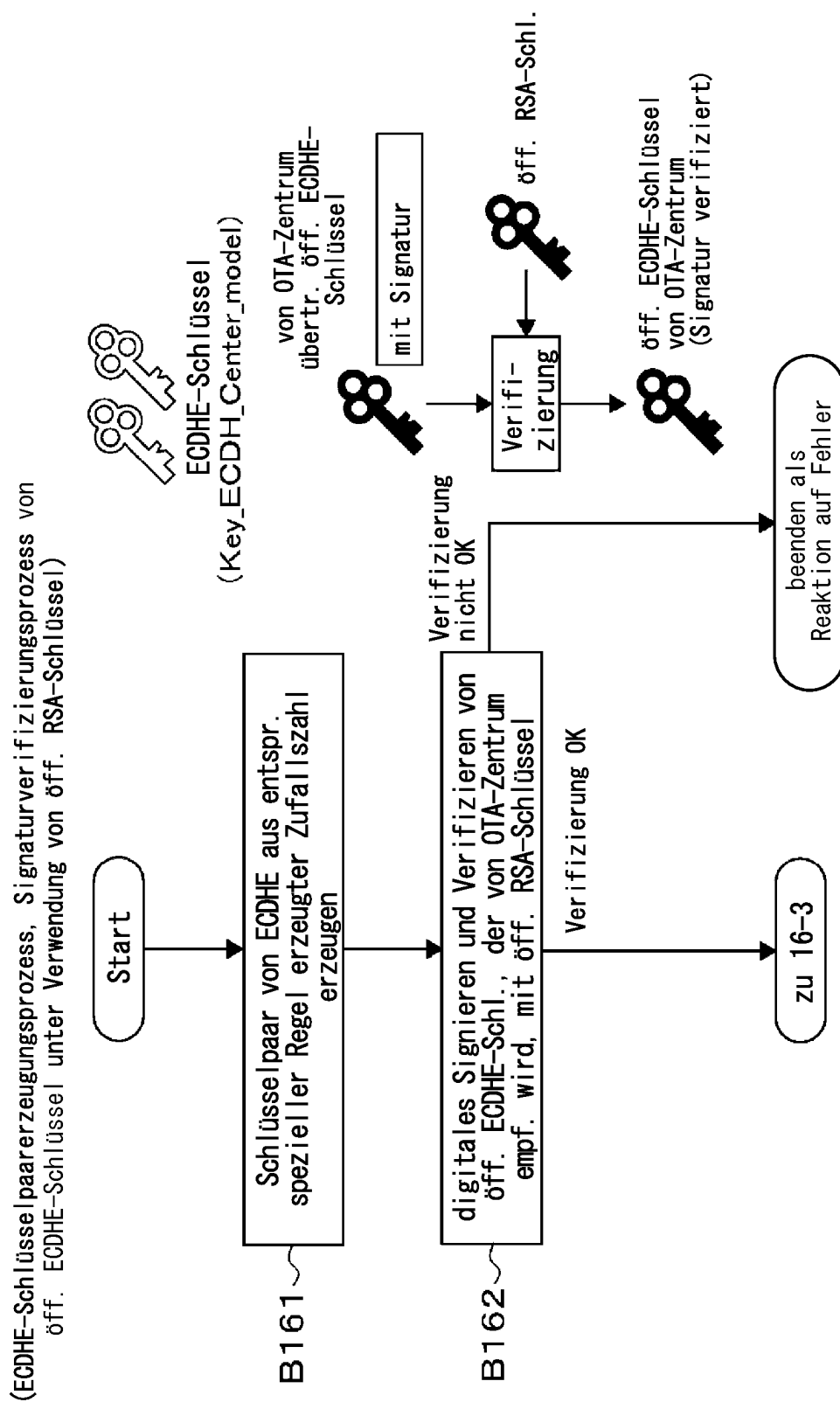
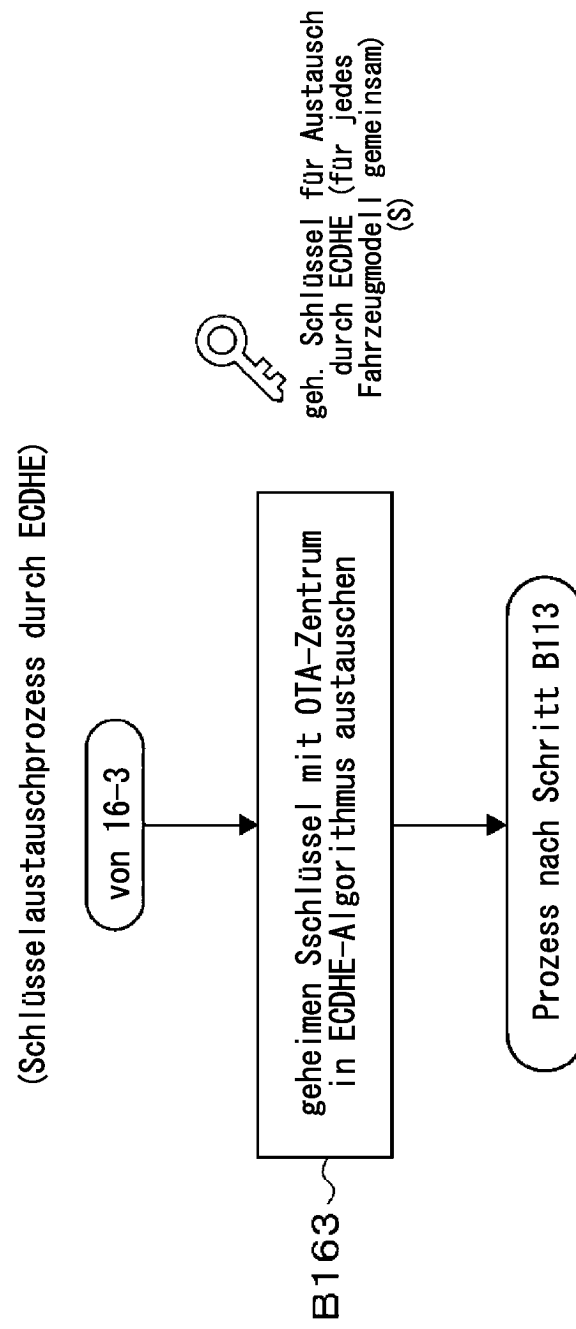
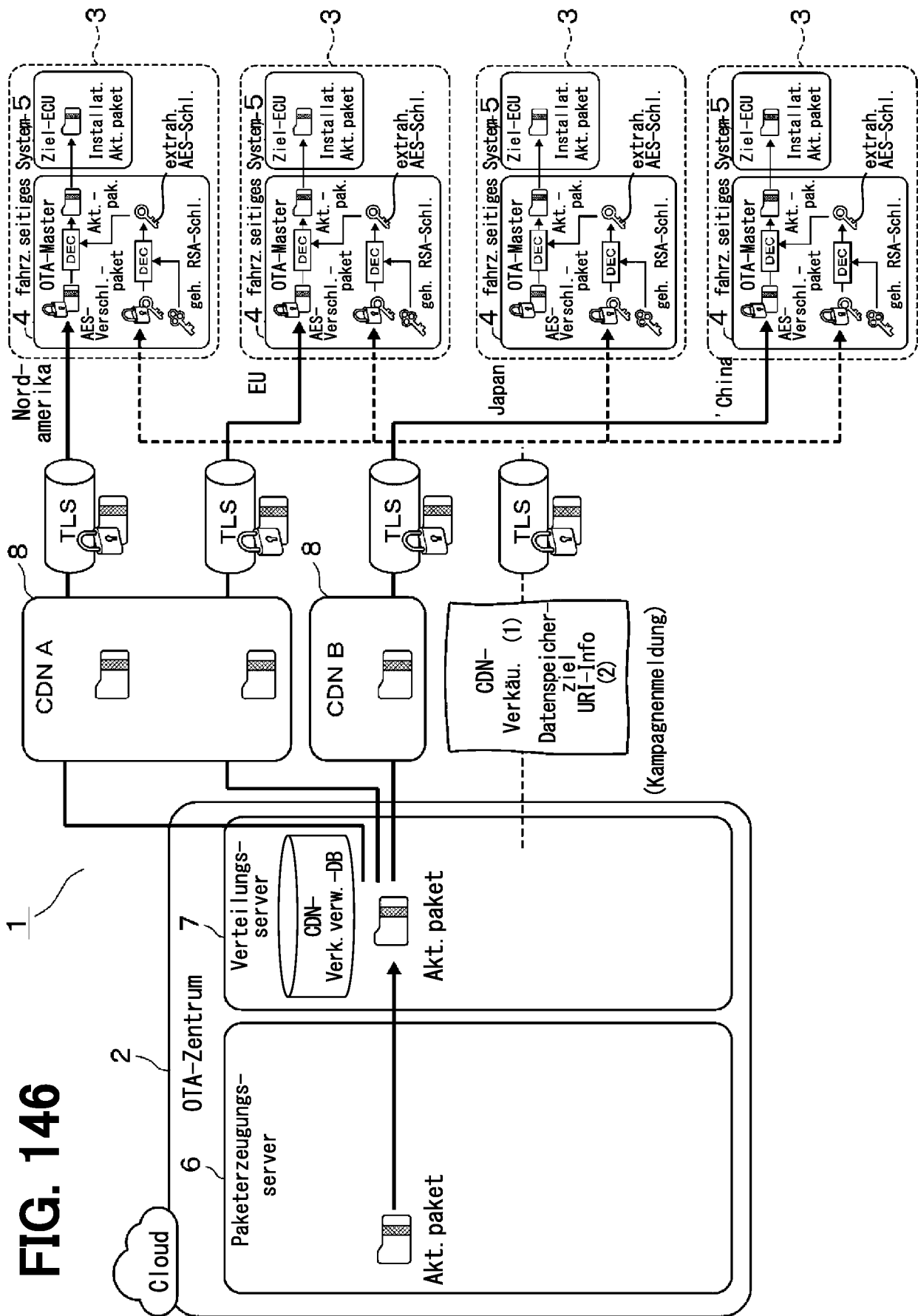
FIG. 144

FIG. 145





(Auswahllogik von CDN-Platzierungsziel mit niedrigstem Preis für jeden Bereich und Platzierungsprozess von Aktualisierungspaket für jeden Bereich)

FIG. 147

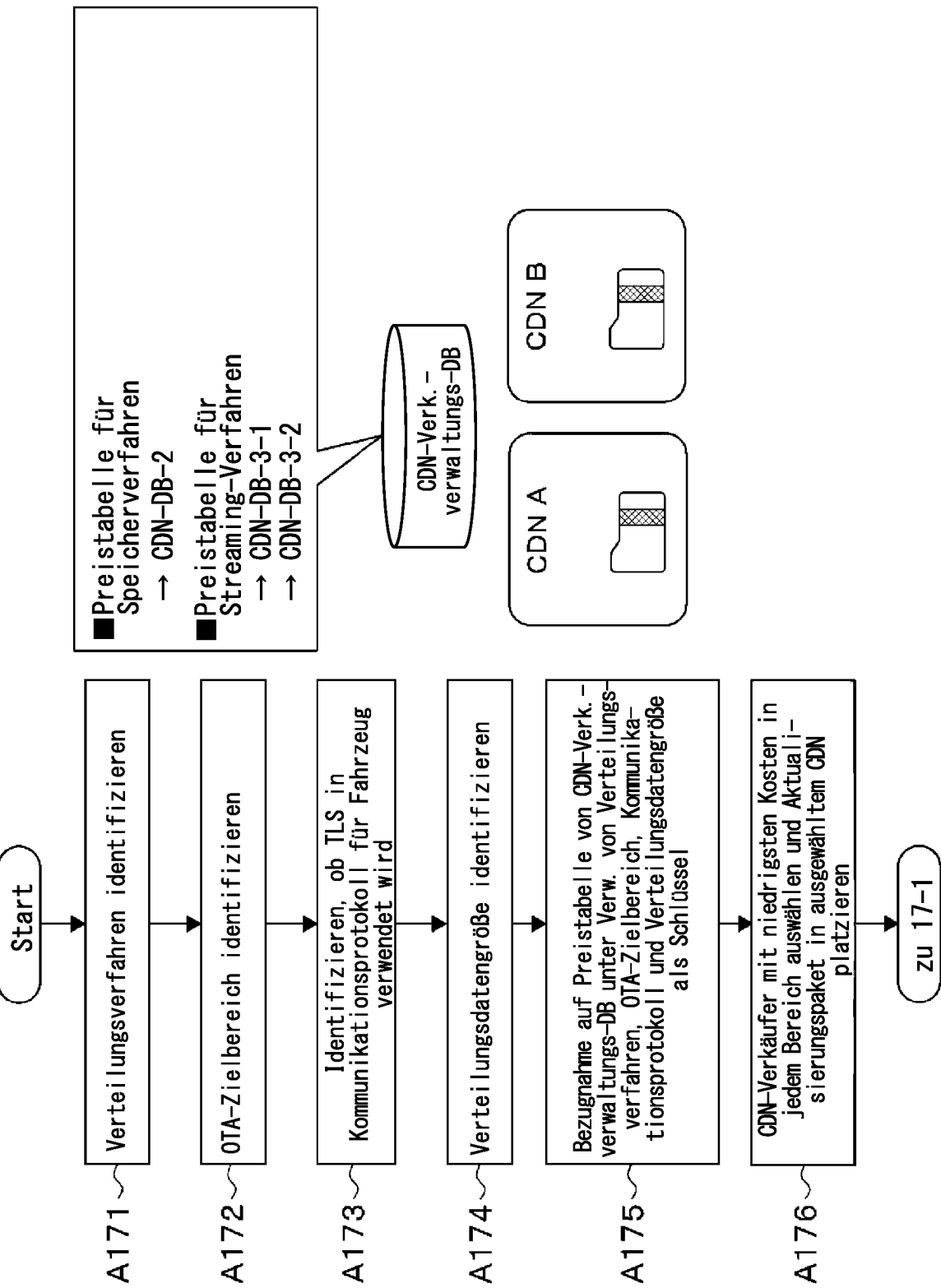


FIG. 148

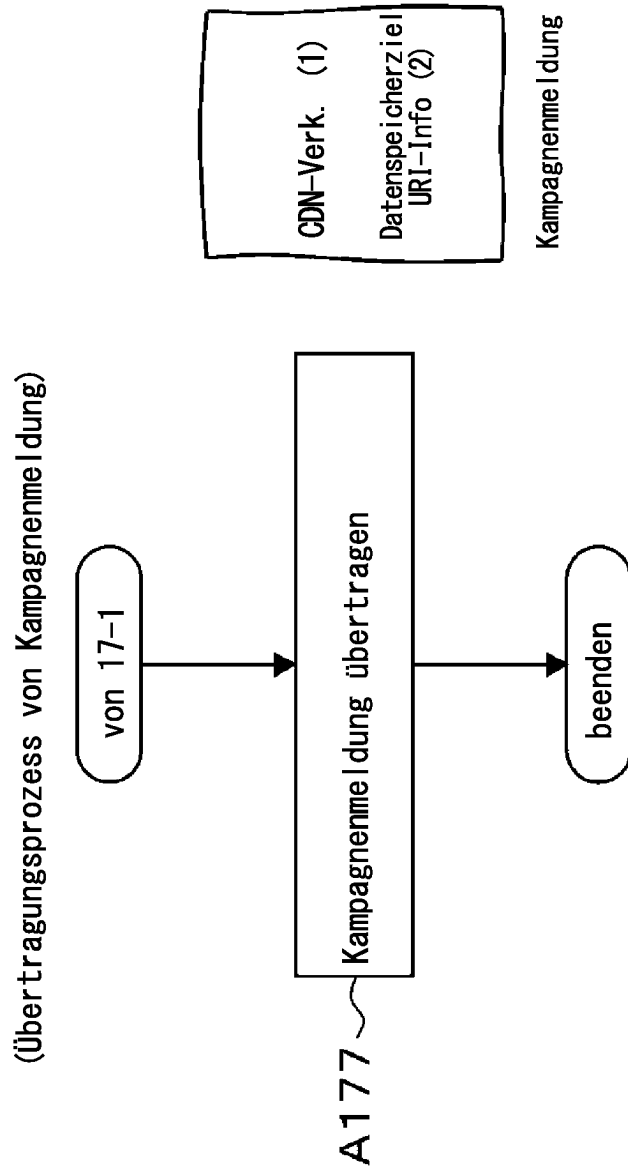


FIG. 149

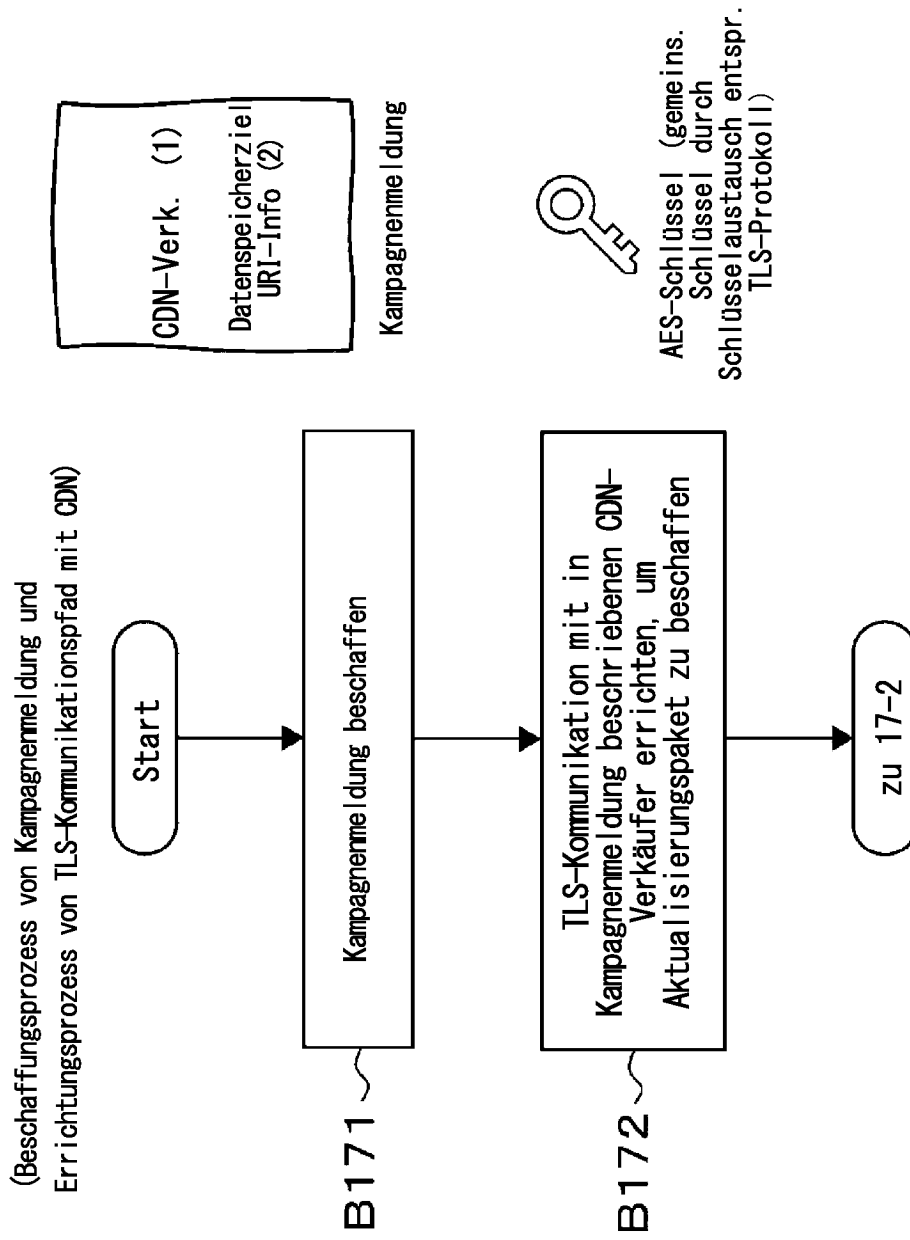


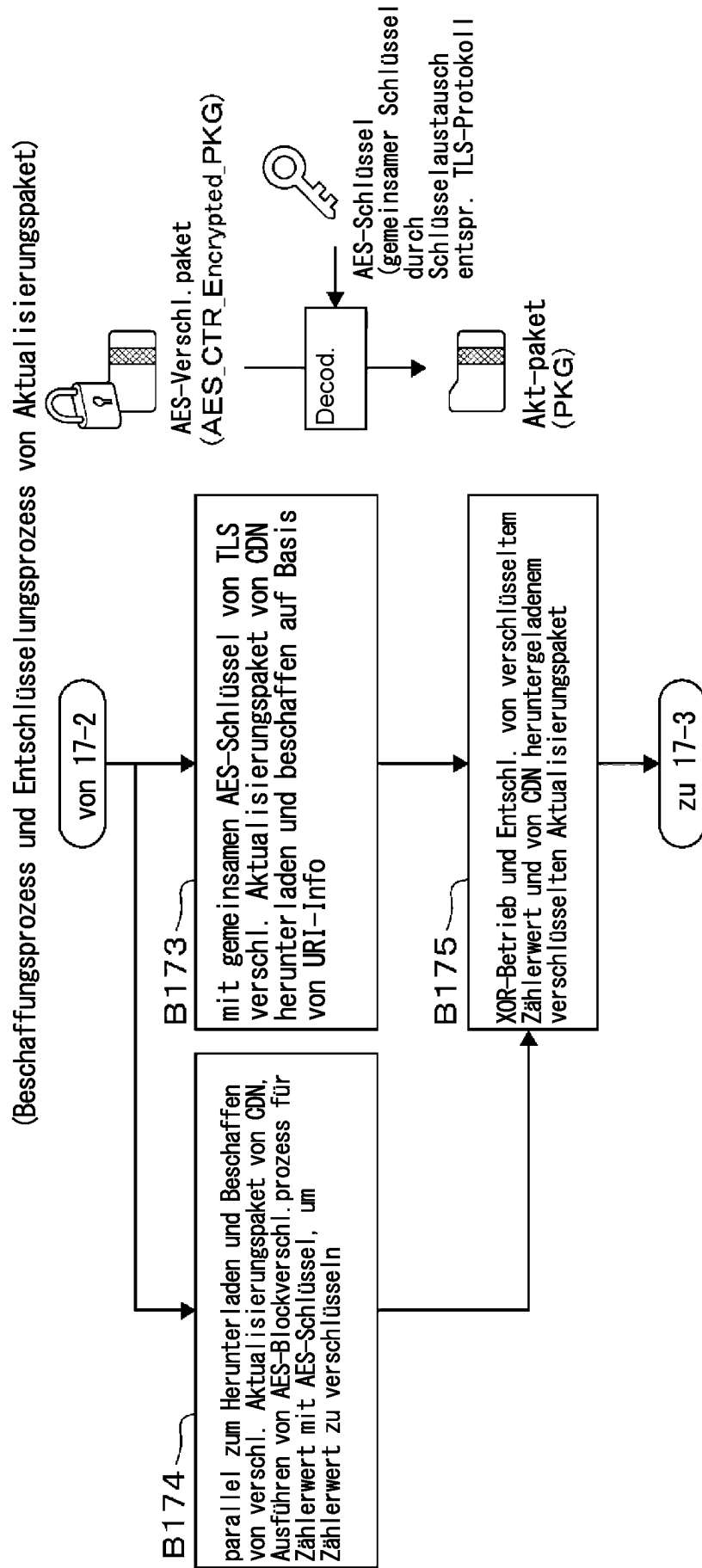
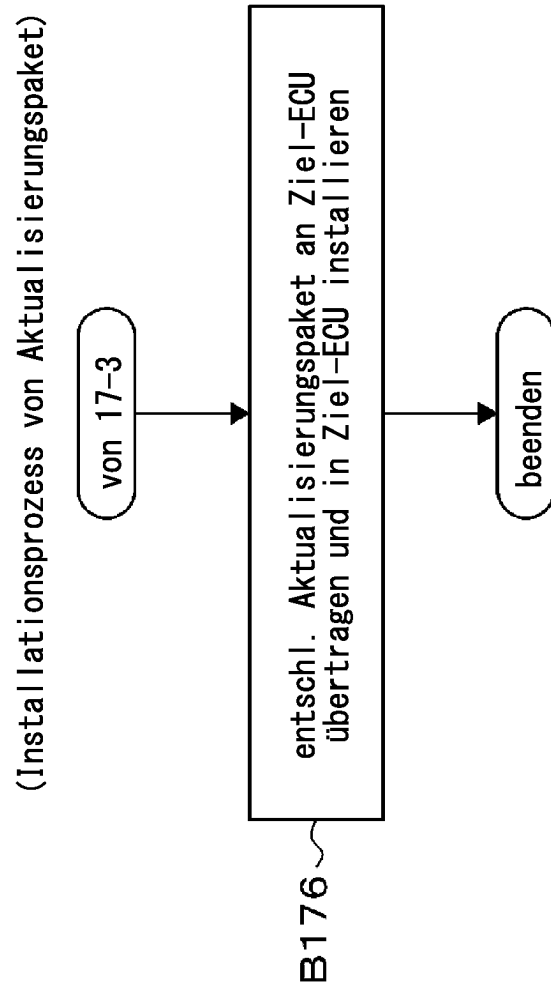
FIG. 150

FIG. 151



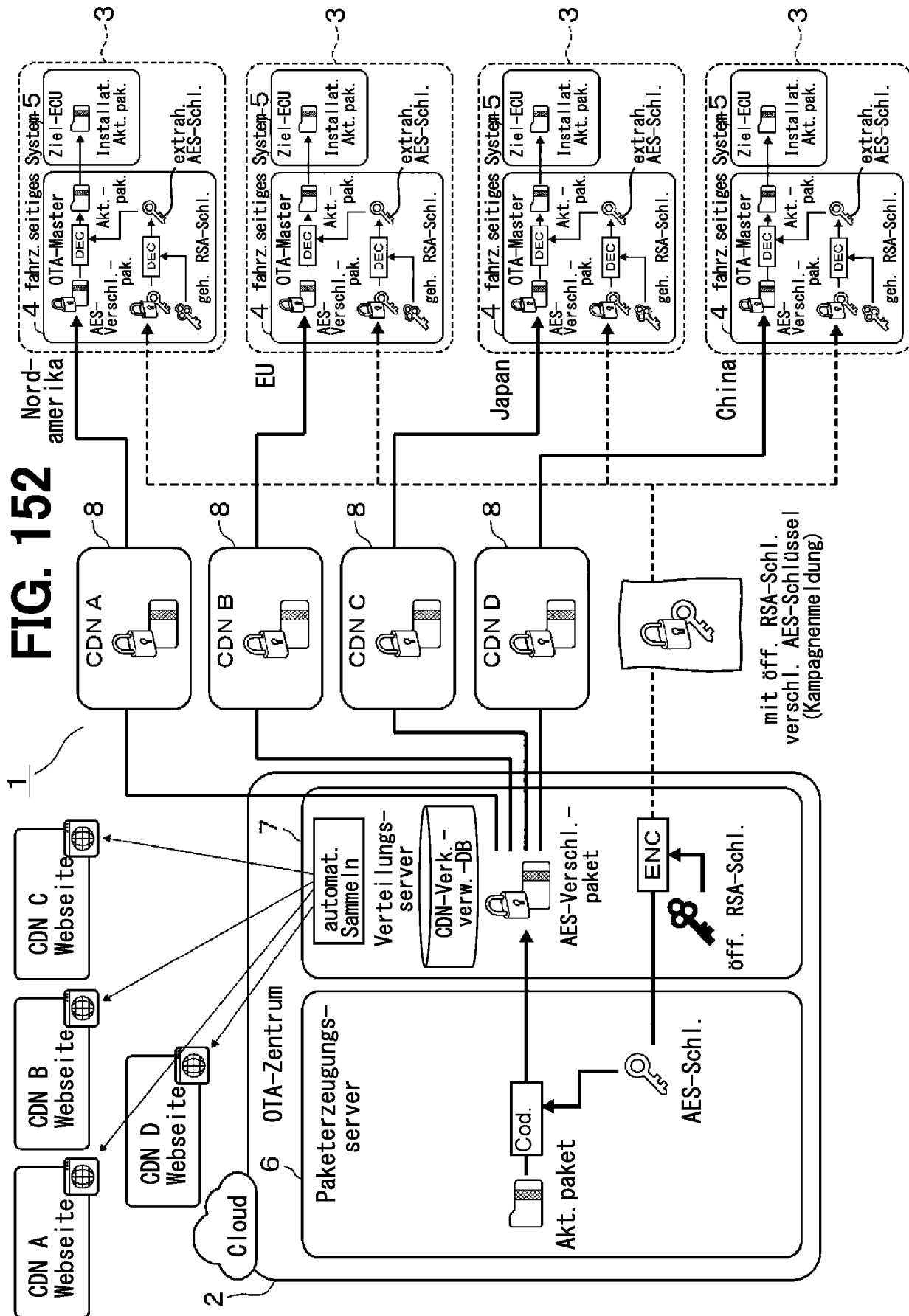
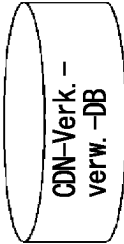


FIG. 153



CDN-DB-1
CDN-Preistabelle für jeden Cloud-Dienst (Basis)

CDN1	Gebührentabelle je GB						
	~10TB	~40TB	~100TB	~350TB	~500TB	~4PB	5PB~
Japan	0.0129 USD	0.121 USD	0.112 USD	0.093 USD	0.075 USD	0.065 USD	0.065 USD
Nordamerika	0.081 USD	0.075 USD	0.056 USD	0.037 USD	0.028 USD	0.023 USD	0.023 USD
EU	0.081 USD	0.075 USD	0.056 USD	0.037 USD	0.028 USD	0.023 USD	0.023 USD

CDN2	Gebührentabelle je GB						
	~10TB	~40TB	~100TB	~350TB	~524TB	~4PB	5PB~
Japan	0.114 USD	0.089 USD	0.086 USD	0.084 USD	0.080 USD	0.070 USD	0.060 USD
Nordamerika	0.085 USD	0.080 USD	0.060 USD	0.040 USD	0.030 USD	0.025 USD	0.020 USD
EU	0.085 USD	0.080 USD	0.060 USD	0.040 USD	0.030 USD	0.025 USD	0.015 USD

CDN2	Anfragegebührentabelle für HTTP-Verfahren	
	HTTP-Anfrage	HTTPS-Anfrage
Japan	0.009 USD	0.012 USD
Nordamerika	0.075 USD	0.010 USD
EU	0.009 USD	0.012 USD

FIG. 154



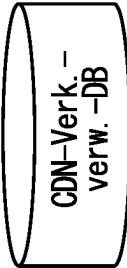
CDN-DB-1

CDN-Preistabelle für jeden Cloud-Dienst (Basis)

CDN3				
Gebührentabelle je GB				
		~10TB	~140TB	~850TB
Japan		0.090 USD	0.060 USD	0.050 USD
Nordamerika		0.080 USD	0.055 USD	0.030 USD
EU		0.080 USD	0.055 USD	0.030 USD
CDN3				
Anfragegebührentabelle für HTTP-Verfahren				
			HTTP-Anfrage	HTTPS-Anfrage
universal			0.0075 USD	

CDN4				
Gebührentabelle je GB				
		~10TB	~40TB	~50TB
Japan		0.090 USD	0.060 USD	0.040 USD
Nordamerika		0.040 USD	0.030 USD	0.020 USD
EU		0.110 USD	0.080 USD	0.060 USD

FIG. 155



CDN-DB-2
Preistabelle von Speicherverfahren jedes Cloud-Dienst-Geschäftsbetreibers

CDN1	Speicherverfahren Anzahl Zielfahrz. : 2 Million.	Gebührentabelle			
		100MB	1GB	10GB	20GB
Japan		2, 45 Millio. Yen	14, 52 Millio. Yen	145, 6 Millio. Yen	291, 2 Millio. Yen
Nordamerika		1, 25 Millio. Yen	5, 12 Millio. Yen	505 Millio. Yen	1001 Millio. Yen
EU		1, 25 Millio. Yen	5, 12 Millio. Yen	505 Millio. Yen	1001 Millio. Yen

CDN2	Speicherverfahren Anzahl Zielfahrz. : 2 Million.	Gebührentabelle			
		100MB	1GB	10GB	20GB
Japan		1, 89 Millio. Yen	17, 6 Millio. Yen	132 Millio. Yen	264 Millio. Yen
Nordamerika		880. 000 Yen	6, 6 Millio. Yen	44 Millio. Yen	88 Millio. Yen
EU		1, 32 Millio. Yen	6, 6 Millio. Yen	44 Millio. Yen	88 Millio. Yen

FIG. 156

CDN-Verk.-
verw.-DB

CDN-DB-2
Preistabelle von Speicherverfahren jedes Cloud-Dienst-Geschäftsbetreibers

CDN3	Speicherverfahren Anzahl Zielfahrz. : 2 Million.	Gebührentabelle			
		100MB	1GB	10GB	20GB
Japan		2, 45 Millio. Yen	14, 52 Millio. Yen	145, 6 Millio. Yen	291, 2 Millio. Yen
Nordamerika		1, 25 Millio. Yen	5, 12 Millio. Yen	505 Millio. Yen	1001 Millio. Yen
EU		1, 25 Millio. Yen	5, 12 Millio. Yen	505 Millio. Yen	1001 Millio. Yen

CDN4	Speicherverfahren Anzahl Zielfahrz. : 2 Million.	Gebührentabelle			
		100MB	1GB	10GB	20GB
Japan		1, 89 Millio. Yen	17, 6 Millio. Yen	132 Millio. Yen	264 Millio. Yen
Nordamerika		880. 000 Yen	6, 6 Millio. Yen	44 Millio. Yen	88 Millio. Yen
EU		1, 32 Millio. Yen	6, 6 Millio. Yen	44 Millio. Yen	88 Millio. Yen

FIG. 157

CDN-Verk. –
verw. –DB

CDN-DB-3-1

Preistabelle für jede Streaming-Größe in Streaming-Verfahren jedes Cloud-Dienst-Geschäftsbetreibers

CDN1	Streaming-Größe: 1KB Anzahl Zielfahrz. : 2 Million.	Gebührentabelle		
		100MB	1GB	10GB
Japan		2, 45 Millio. Yen	14, 52 Millio. Yen	145, 6 Millio. Yen
Nordamerika		1, 25 Millio. Yen	5, 12 Millio. Yen	505 Millio. Yen
EU		1, 25 Millio. Yen	5, 12 Millio. Yen	505 Millio. Yen

CDN1	Streaming-Größe: 10KB Anzahl Zielfahrz. : 2 Million.	Gebührentabelle		
		100MB	1GB	10GB
Japan		2, 45 Millio. Yen	14, 52 Millio. Yen	145, 6 Millio. Yen
Nordamerika		1, 25 Millio. Yen	5, 12 Millio. Yen	505 Millio. Yen
EU		1, 25 Millio. Yen	5, 12 Millio. Yen	505 Millio. Yen

CDN1	Streaming-Größe: 100KB Anzahl Zielfahrz. : 2 Million.	Gebührentabelle		
		100MB	1GB	10GB
Japan		2, 45 Millio. Yen	14, 52 Millio. Yen	145, 6 Millio. Yen
Nordamerika		1, 25 Millio. Yen	5, 12 Millio. Yen	505 Millio. Yen
EU		1, 25 Millio. Yen	5, 12 Millio. Yen	505 Millio. Yen

FIG. 158

CDN-Verk. –
verw. –DB

CDN-DB-3-2

Preistabelle für jede Streaming-Größe in Streaming-Verfahren jedes Cloud-Dienst-Geschäftsbetreibers

CDN2	Streaming-Größe: 1KB Anzahl Zielfahrz. : 2 Million.	Gebührentabelle (HTTP/HTTPS)		
		100MB	1GB	10GB
Japan		21,69 Millio. Yen/ 28,29 Millio. Yen	215,6 Millio. Yen/ 281,6 Millio. Yen	2112 Millio. Yen/ 2772 Millio. Yen
Nordamerika		17,38 Millio. Yen/ 22,88 Millio. Yen	171,6 Millio. Yen/ 226,6 Millio. Yen	1694 Millio. Yen/ 2244 Millio. Yen
EU		21,12 Millio. Yen/ 27,72 Millio. Yen	204,6 Millio. Yen/ 270,6 Millio. Yen	2024 Millio. Yen/ 2684 Millio. Yen

CDN2	Streaming-Größe: 10KB Anzahl Zielfahrz. : 2 Million.	Gebührentabelle (HTTP/HTTPS)		
		100MB	1GB	10GB
Japan		3,87 Millio. Yen/ 4,53 Millio. Yen	37,4 Millio. Yen/ 44 Millio. Yen	330 Millio. Yen/ 396 Millio. Yen
Nordamerika		2,53 Millio. Yen/ 3,08 Millio. Yen	23,1 Millio. Yen/ 28,6 Millio. Yen	209 Millio. Yen/ 264 Millio. Yen
EU		3,3 Millio. Yen/ 3,96 Millio. Yen	26,4 Millio. Yen/ 33 Millio. Yen	242 Millio. Yen/ 308 Millio. Yen

CDN2	Streaming-Größe: 100KB Anzahl Zielfahrz. : 2 Million.	Gebührentabelle (HTTP/HTTPS)		
		100MB	1GB	10GB
Japan		2,09 Millio. Yen/ 2,16 Millio. Yen	19,58 Millio. Yen/ 20,24 Millio. Yen	151,8 Millio. Yen/ 158,4 Millio. Yen
Nordamerika		1,05 Millio. Yen/ 1,1 Millio. Yen	8,25 Millio. Yen/ 8,8 Millio. Yen	60,5 Millio. Yen/ 66 Millio. Yen
EU		1,52 Millio. Yen/ 1,58 Millio. Yen	8,58 Millio. Yen/ 9,24 Millio. Yen	63,8 Millio. Yen/ 70,4 Millio. Yen

FIG. 159

CDN-Verk. –
verw. –DB

CDN-DB-3-3

Preistabelle für jede Streaming-Größe in Streaming-Verfahren jedes Cloud-Dienst-Geschäftsbetreibers

CDN3	Streaming-Größe: 1KB Anzahl Zielfahrz.: 2 Million.	Gebührentabelle		
		100MB	1GB	10GB
Japan		1, 34 Millio. Yen	4, 57 Millio. Yen	45, 67 Millio. Yen
Nordamerika		1, 34 Millio. Yen	4, 57 Millio. Yen	45, 67 Millio. Yen
EU		1, 34 Millio. Yen	4, 57 Millio. Yen	45, 67 Millio. Yen

CDN3	Streaming-Größe: 10KB Anzahl Zielfahrz.: 2 Million.	Gebührentabelle		
		100MB	1GB	10GB
Japan		1, 32 Millio. Yen	4, 42 Millio. Yen	44, 17 Millio. Yen
Nordamerika		1, 32 Millio. Yen	4, 42 Millio. Yen	44, 17 Millio. Yen
EU		1, 32 Millio. Yen	4, 42 Millio. Yen	44, 17 Millio. Yen

CDN3	Streaming-Größe: 100KB Anzahl Zielfahrz.: 2 Million.	Gebührentabelle		
		100MB	1GB	10GB
Japan		1, 32 Millio. Yen	4, 4 Millio. Yen	44 Millio. Yen
Nordamerika		1, 32 Millio. Yen	4, 4 Millio. Yen	44 Millio. Yen
EU		1, 32 Millio. Yen	4, 4 Millio. Yen	44 Millio. Yen

FIG. 160

CDN-Verk. -
verw. -DB

CDN-DB-3-4

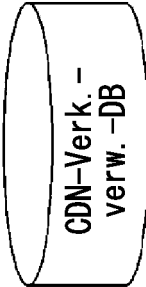
Preistabelle für jede Streaming-Größe in Streaming-Verfahren jedes Cloud-Dienst-Geschäftsbetreibers

CDN4	Streaming-Größe: 1KB Anzahl Zielfahrz. : 2 Million.	Gebührentabelle			
		100MB	1GB	10GB	20GB
Japan		440. 000 Yen	4, 4 Millio. Yen	44 Millio. Yen	88 Millio. Yen
Nordamerika		220. 000 Yen	2, 2 Millio. Yen	22 Millio. Yen	44 Millio. Yen
EU		880. 000 Yen	8, 8 Millio. Yen	88 Millio. Yen	176 Millio. Yen

CDN4	Streaming-Größe: 10KB Anzahl Zielfahrz. : 2 Million.	Gebührentabelle			
		100MB	1GB	10GB	20GB
Japan		440. 000 Yen	4, 4 Millio. Yen	44 Millio. Yen	88 Millio. Yen
Nordamerika		220. 000 Yen	2, 2 Millio. Yen	22 Millio. Yen	44 Millio. Yen
EU		880. 000 Yen	8, 8 Millio. Yen	88 Millio. Yen	176 Millio. Yen

CDN4	Streaming-Größe: 100KB Anzahl Zielfahrz. : 2 Million.	Gebührentabelle			
		100MB	1GB	10GB	20GB
Japan		440. 000 Yen	4, 4 Millio. Yen	44 Millio. Yen	88 Millio. Yen
Nordamerika		220. 000 Yen	2, 2 Millio. Yen	22 Millio. Yen	44 Millio. Yen
EU		880. 000 Yen	8, 8 Millio. Yen	88 Millio. Yen	176 Millio. Yen

FIG. 161



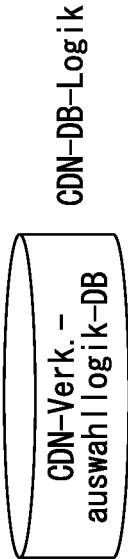
CDN-DB-4

Qualitätsinformation über jeden Cloud-Dienst-Geschäftsbetreiber

Durchsatzvergleich				
	Japan	Nordamerika	EU	
CDN2	Rang A	Rang B	Rang A	
CDN1	Rang A	Rang B	Rang A	
CDN3	Rang A	Rang A	Rang B	
CDN4	Rang C	Rang C	Rang C	

Verzögerungsvergleich				
	Japan	Nordamerika	EU	
CDN2	Rang A	Rang C	Rang B	
CDN1	Rang B	Rang B	Rang A	
CDN3	Rang A	Rang A	Rang A	
CDN4	Rang B	Rang A	Rang B	

FIG. 162



CDN-Verkäufer- auswahl logik	(1) Verteilungs- kosten	(2) Gewichtung von Durchsatz	(3) Gewichtung von Antwortverzögerungszeit
CDN-Verkäufer	Verteilungskosten (Yen)	Rang A: 0,8 Rang B: 1,0 Rang C: 1,2	Rang A: 0,8 Rang B: 1,0 Rang C: 1,2

CDN-Verkäufer A: (1) Verteilungskosten: 100 Millionen Yen
(2) Durchsatzrang: Rang A
(3) Antwortverzögerungszeitrang: Rang A
→ In diesem Fall Reputationsrang von CDN-Verkäufer A
 $(1) \times (2) \times (3) = 100 \text{ Millionen Yen} \times 0,8 \times 0,8 = 64 \text{ Millionen Yen}$

CDN-Verkäufer B: (1) Verteilungskosten: 80 Millionen Yen
(2) Durchsatzrang: Rang C
(3) Antwortverzögerungszeitrang: Rang C
→ In diesem Fall Reputationsrang von CDN-Verkäufer B
 $(1) \times (2) \times (3) = 80 \text{ Millionen Yen} \times 1,2 \times 1,2 = 110 \text{ Millionen Yen}$

FIG. 163

(Auswahllogik von CDN-Platzierungsziel mit niedrigstem Preis für jeden Bereich und Platzierungsprozess von Aktualisierungspaket für jeden Bereich)

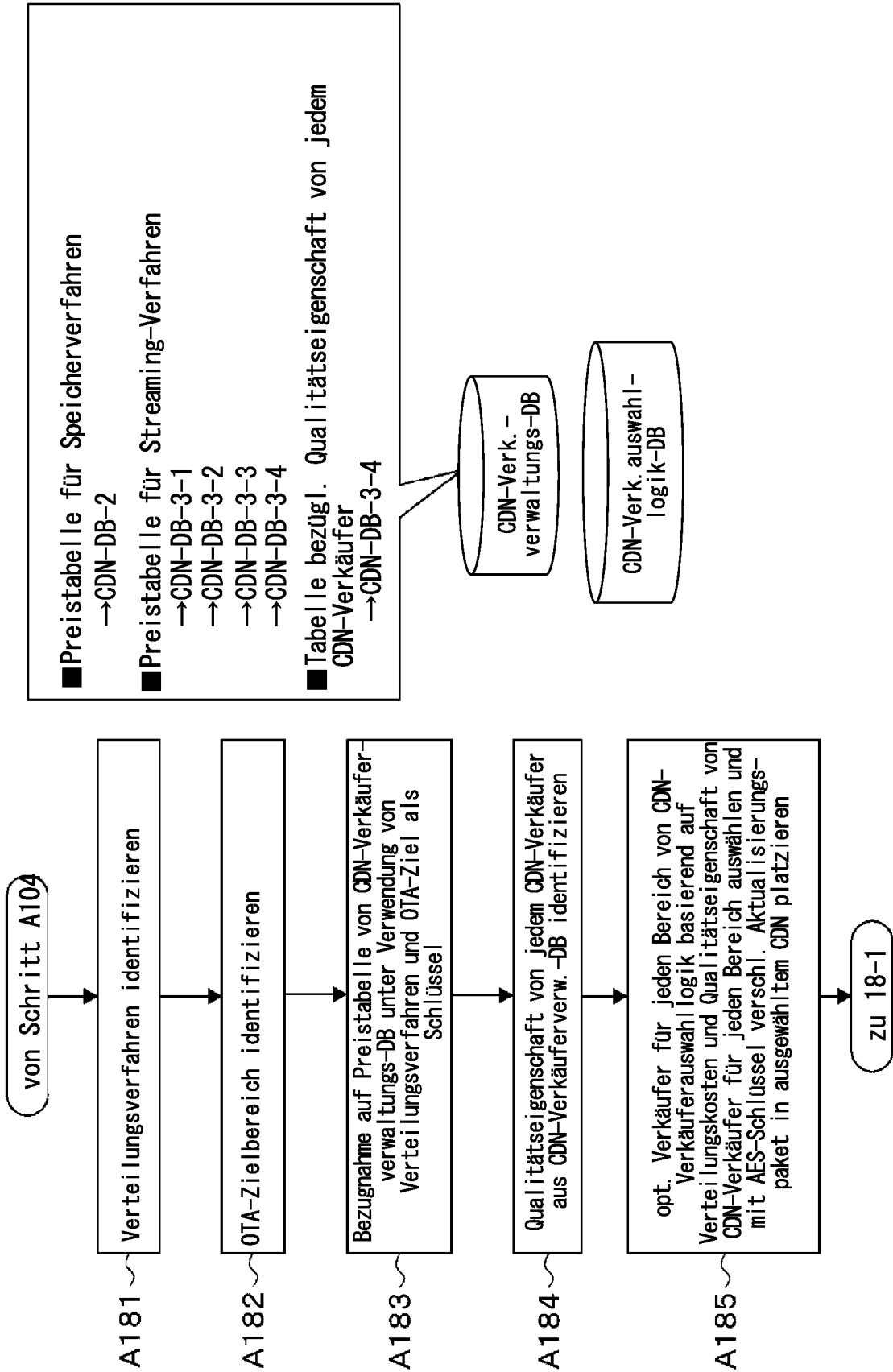


FIG. 164

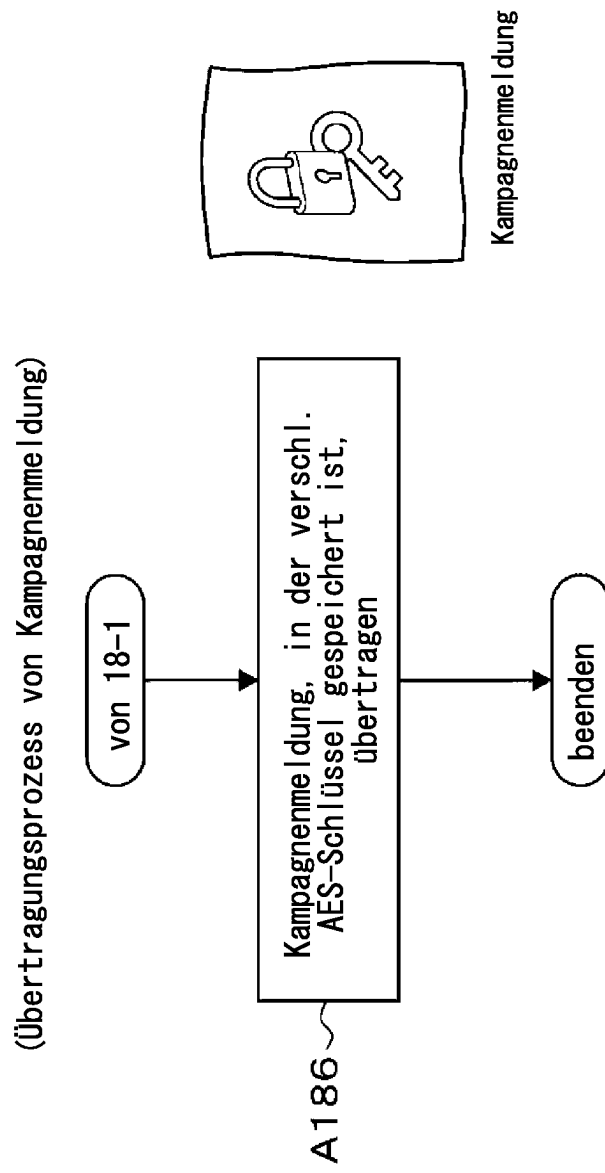


FIG. 165

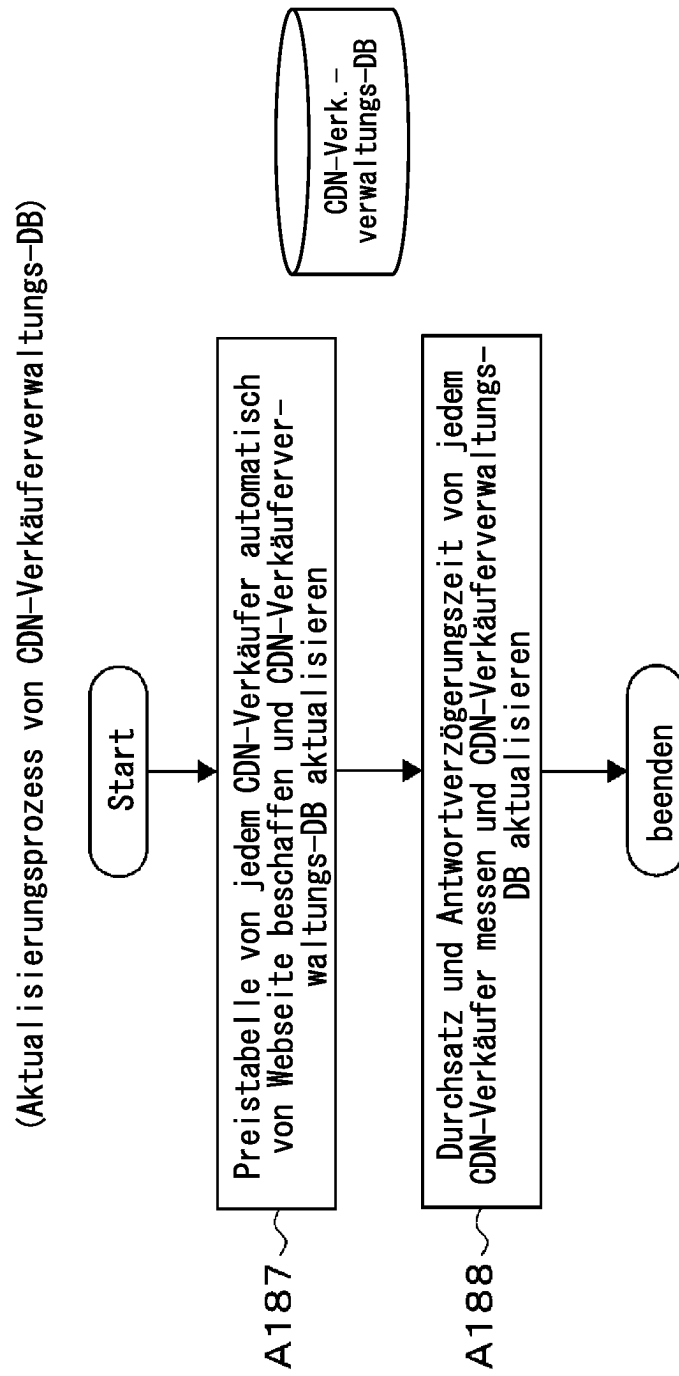


FIG. 166

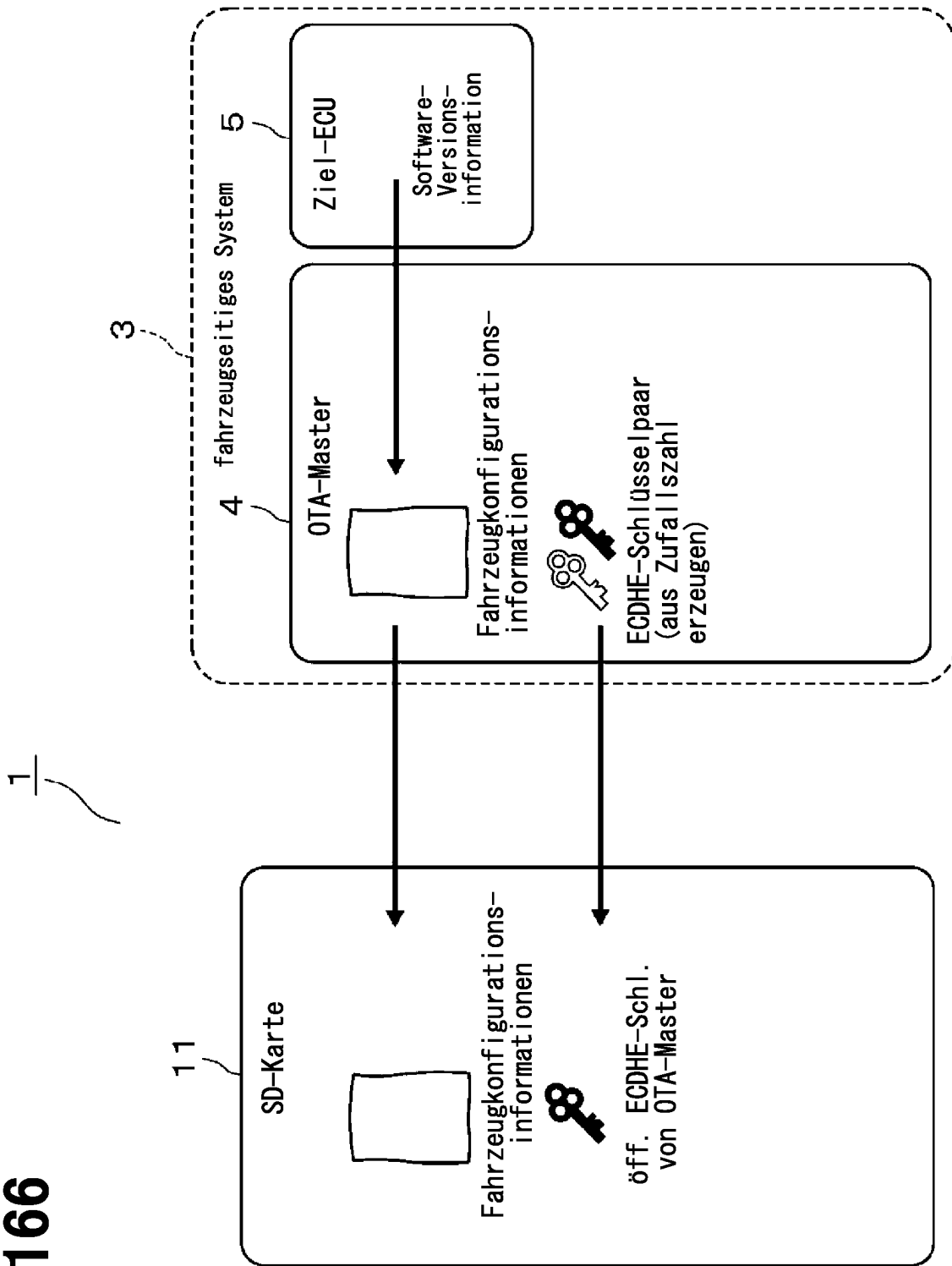


FIG. 167

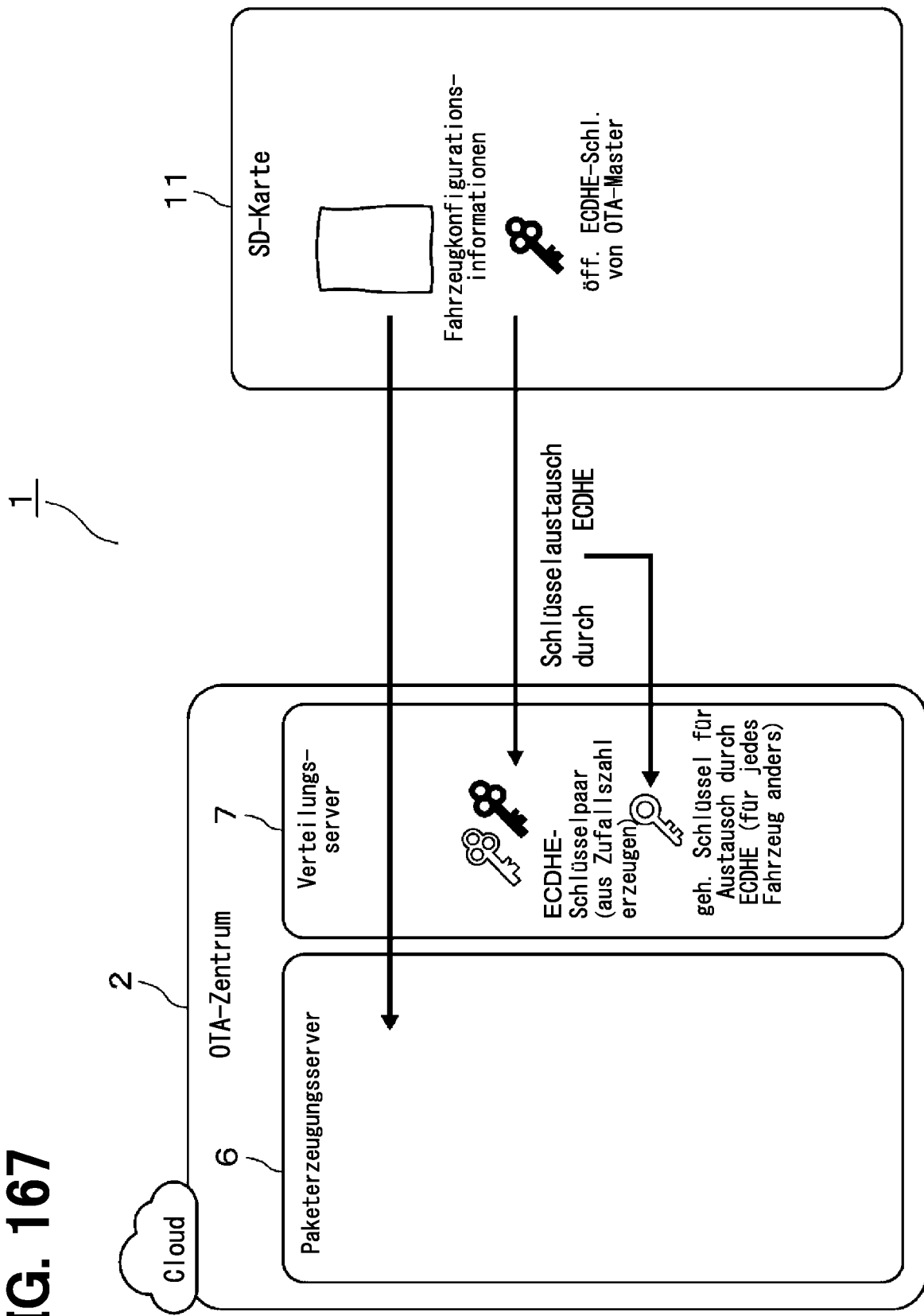


FIG. 168

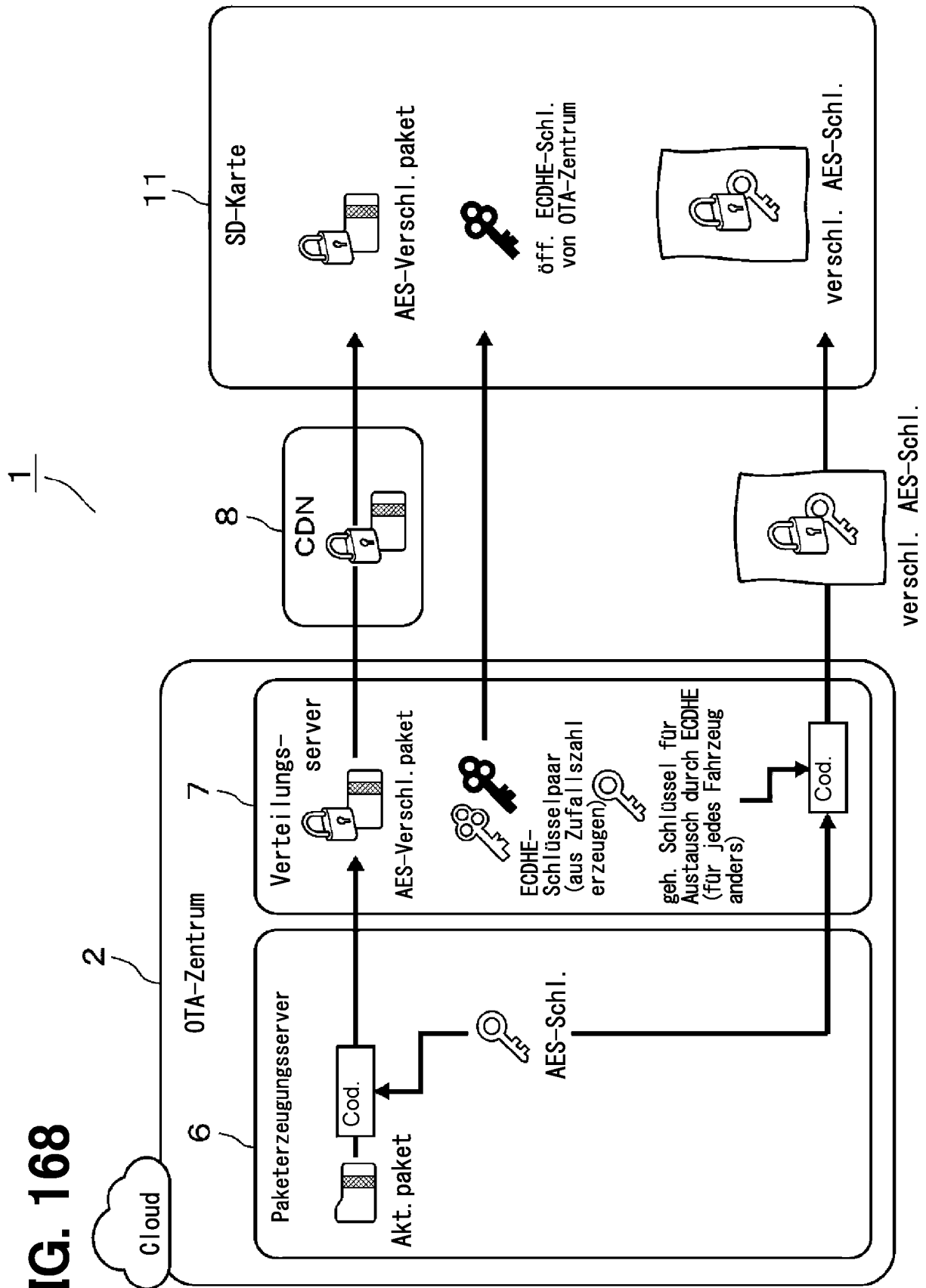


FIG. 169

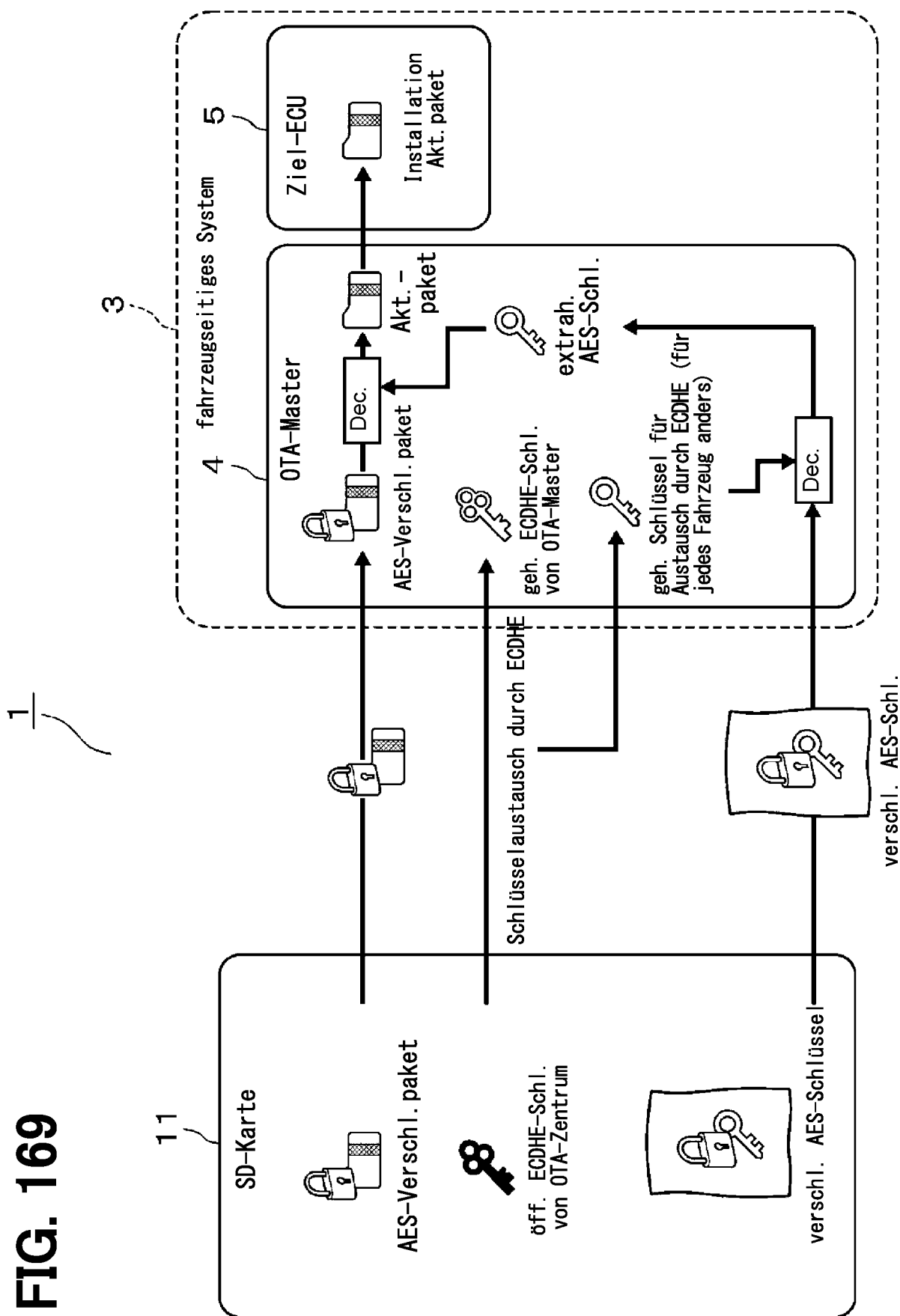


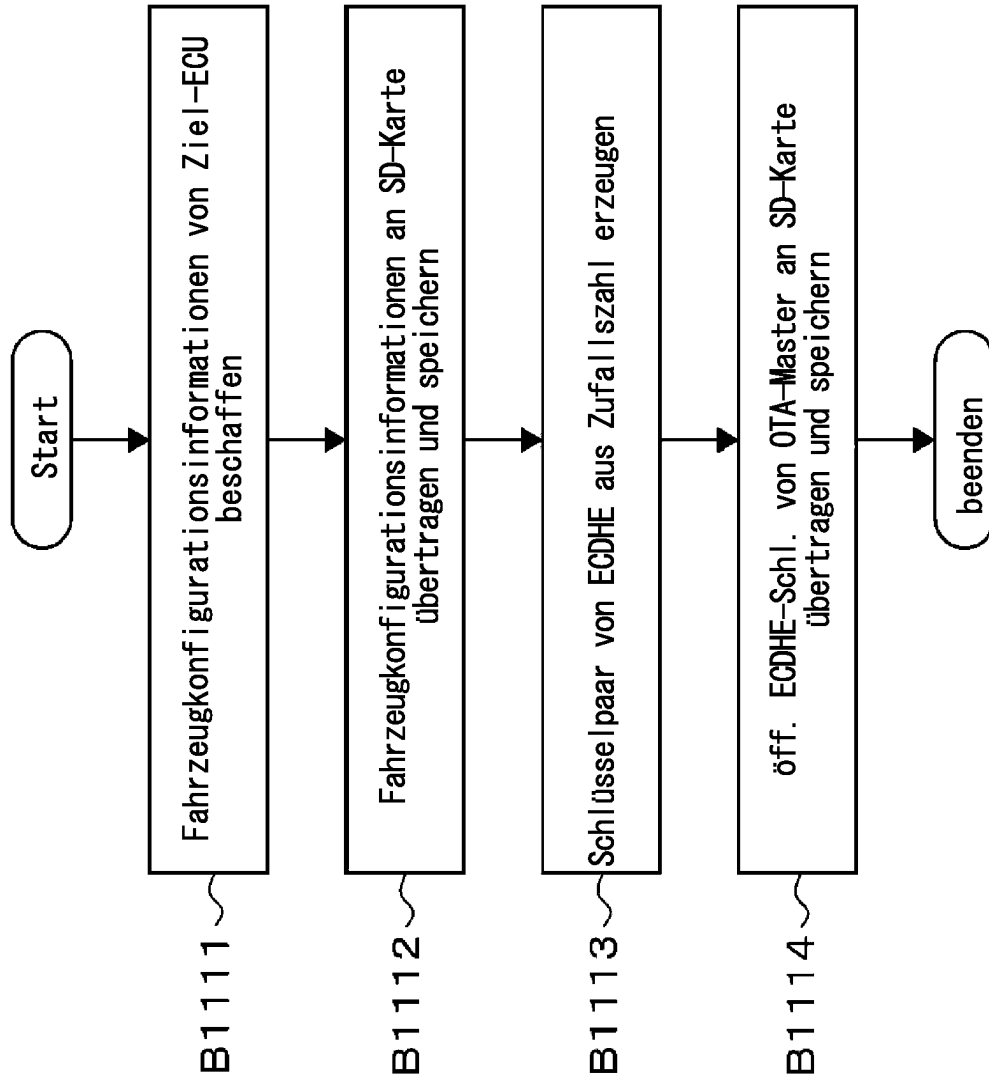
FIG. 170

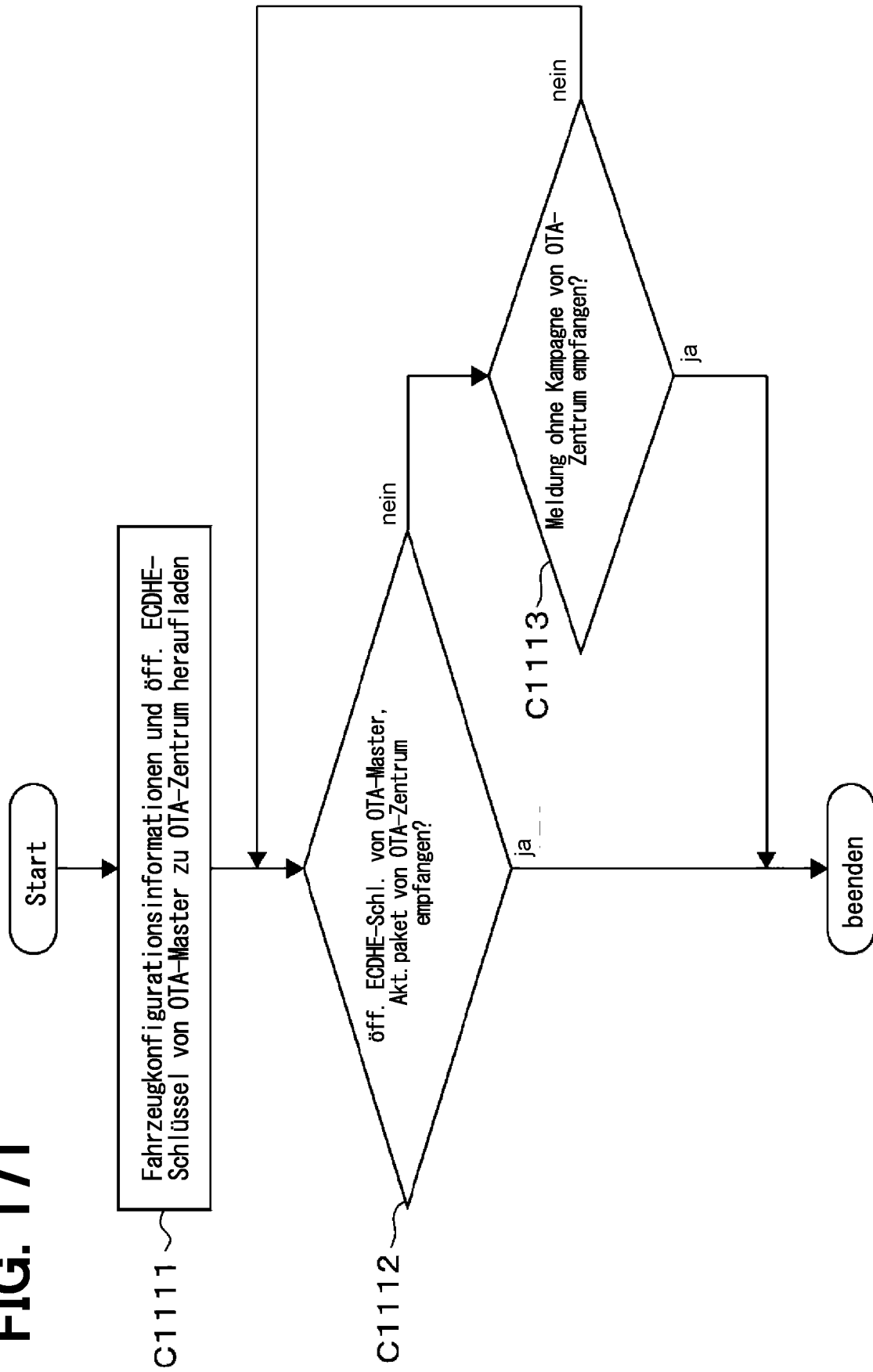
FIG. 171

FIG. 172

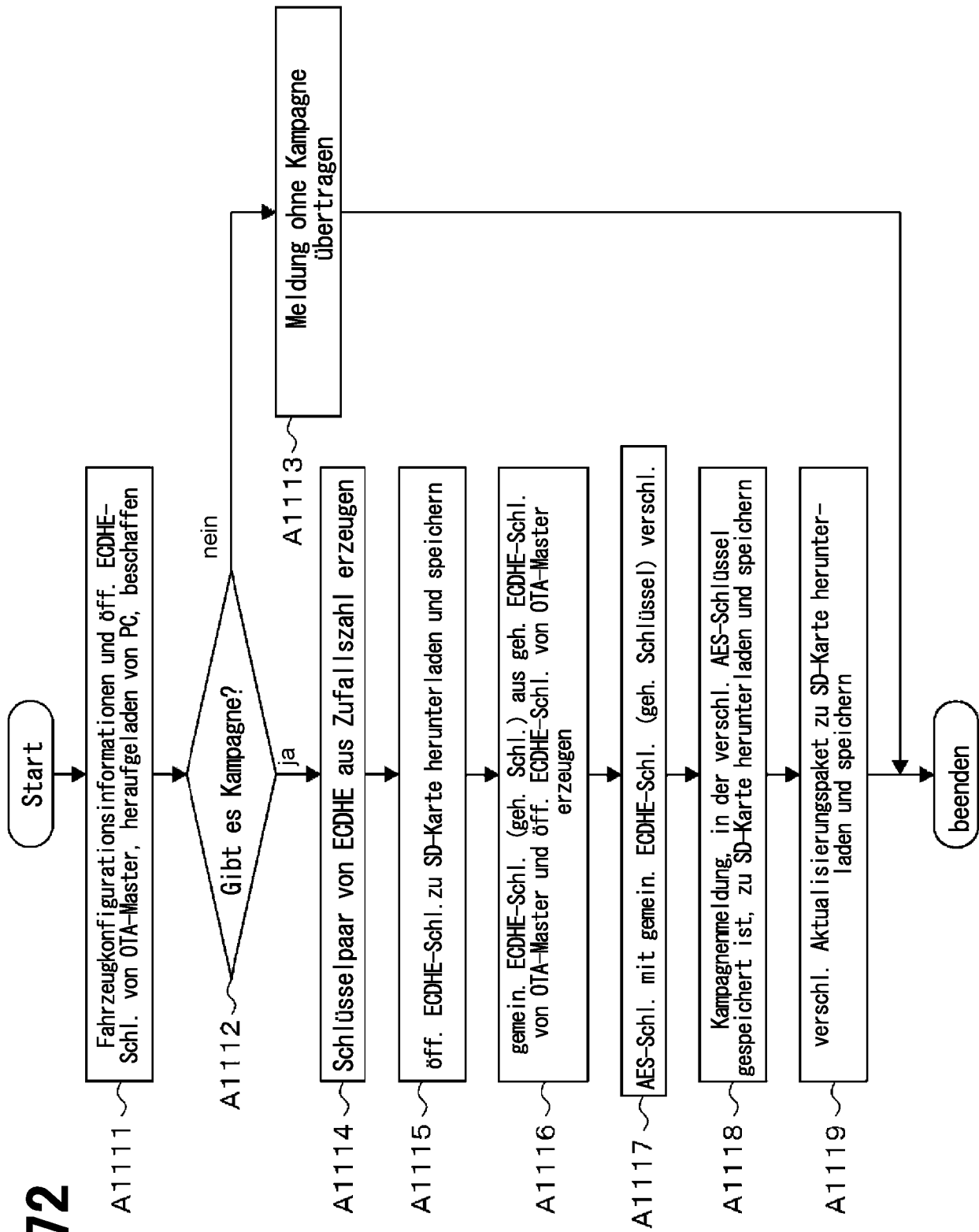


FIG. 173

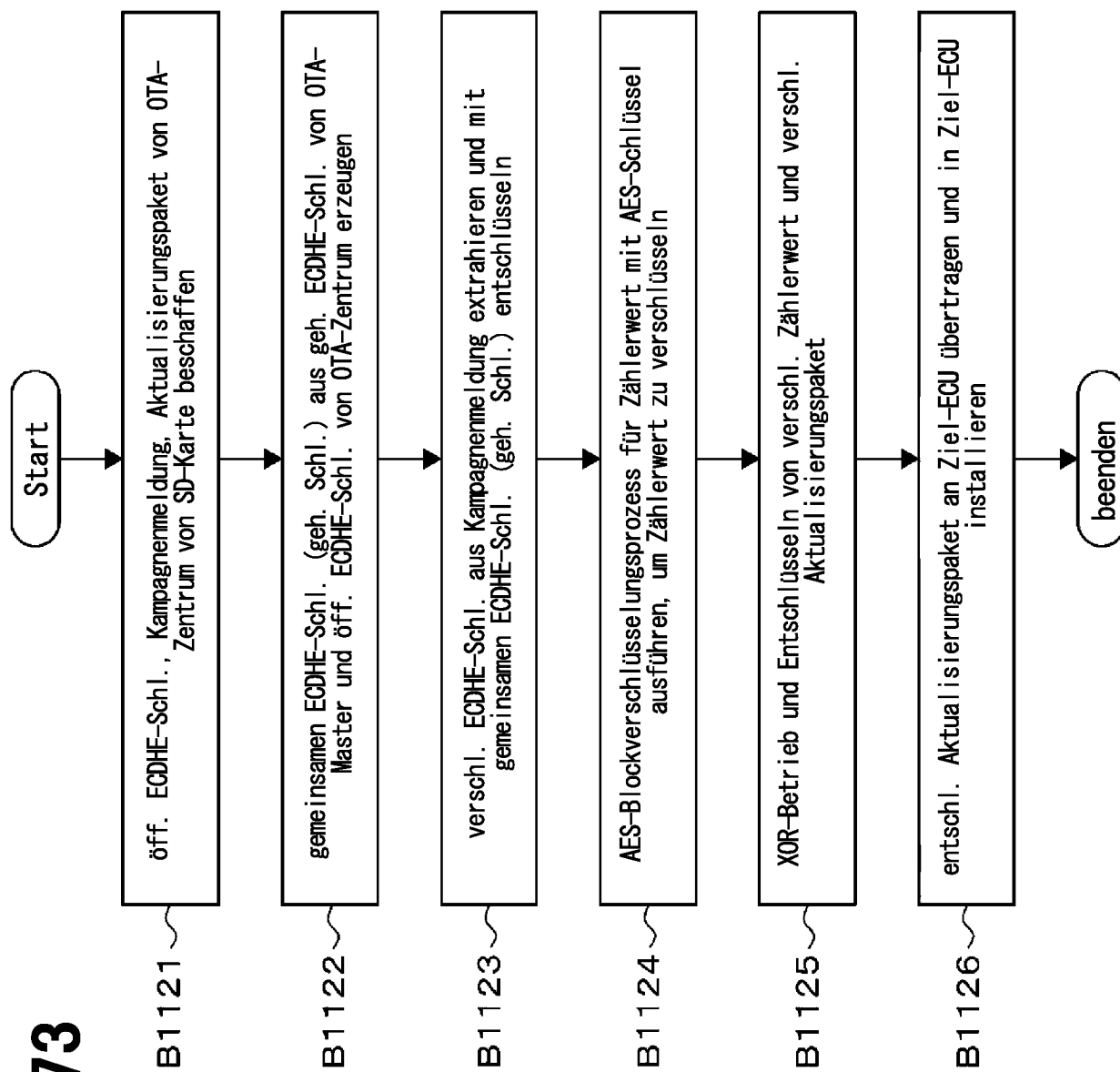


FIG. 174

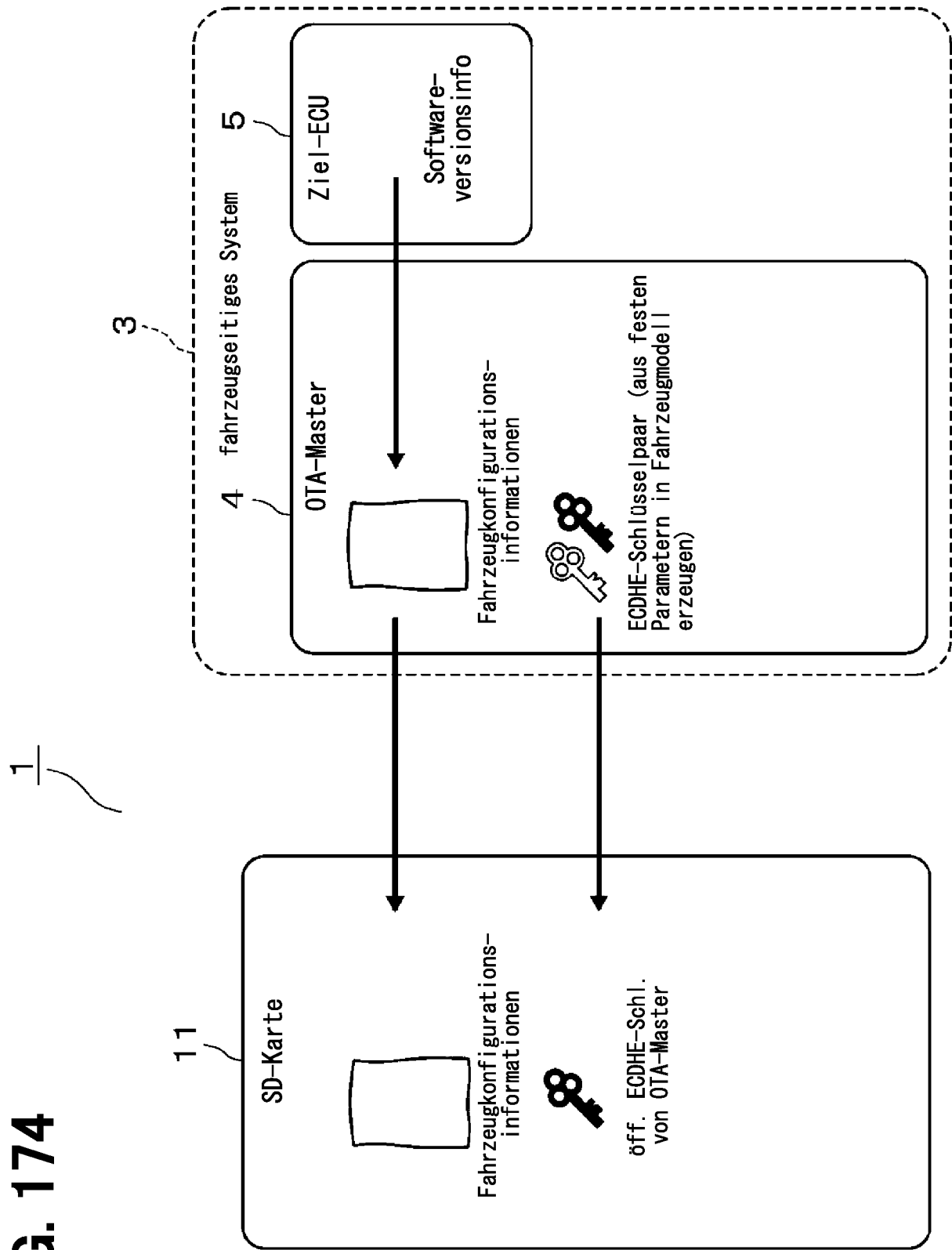


FIG. 175

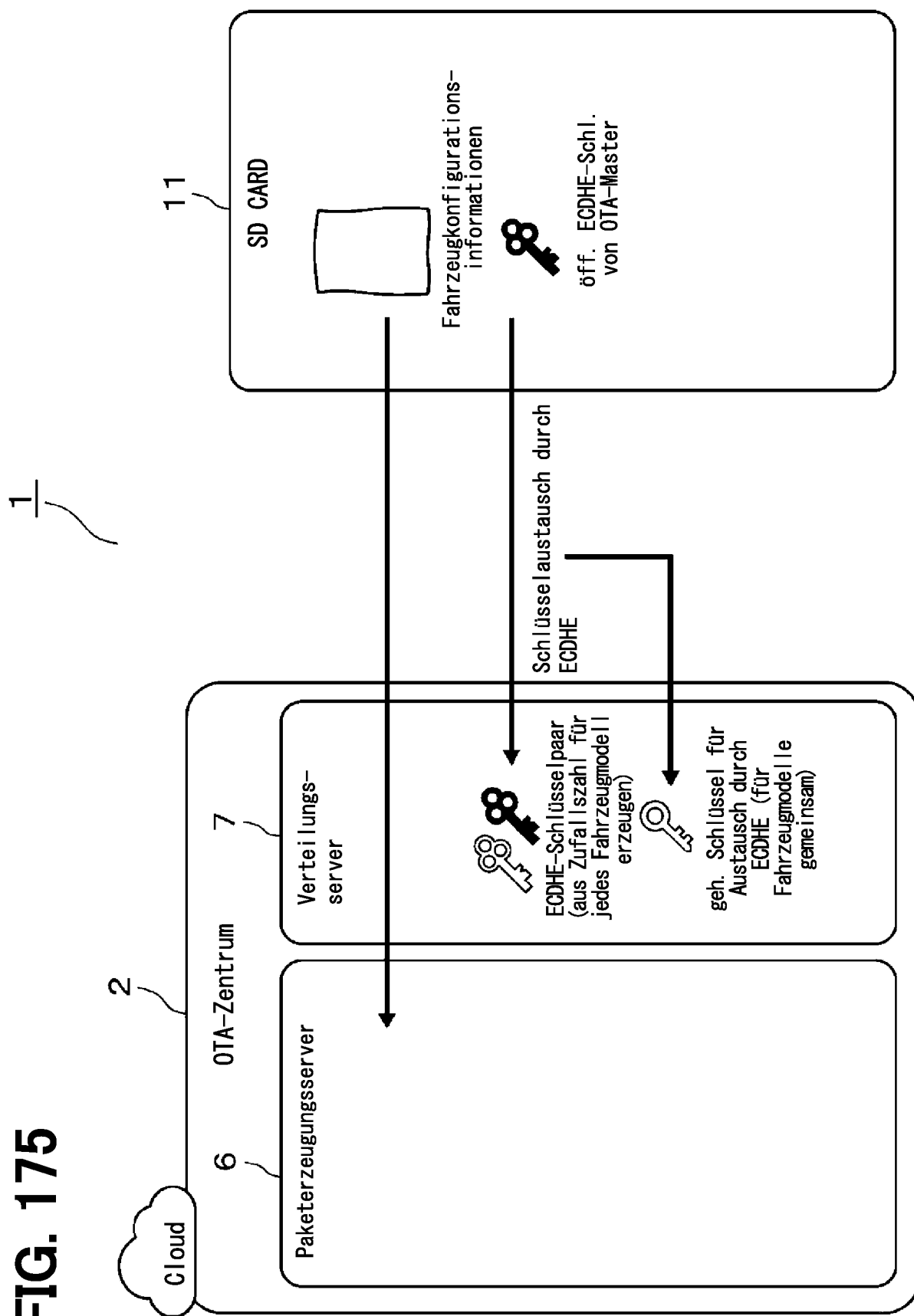


FIG. 176

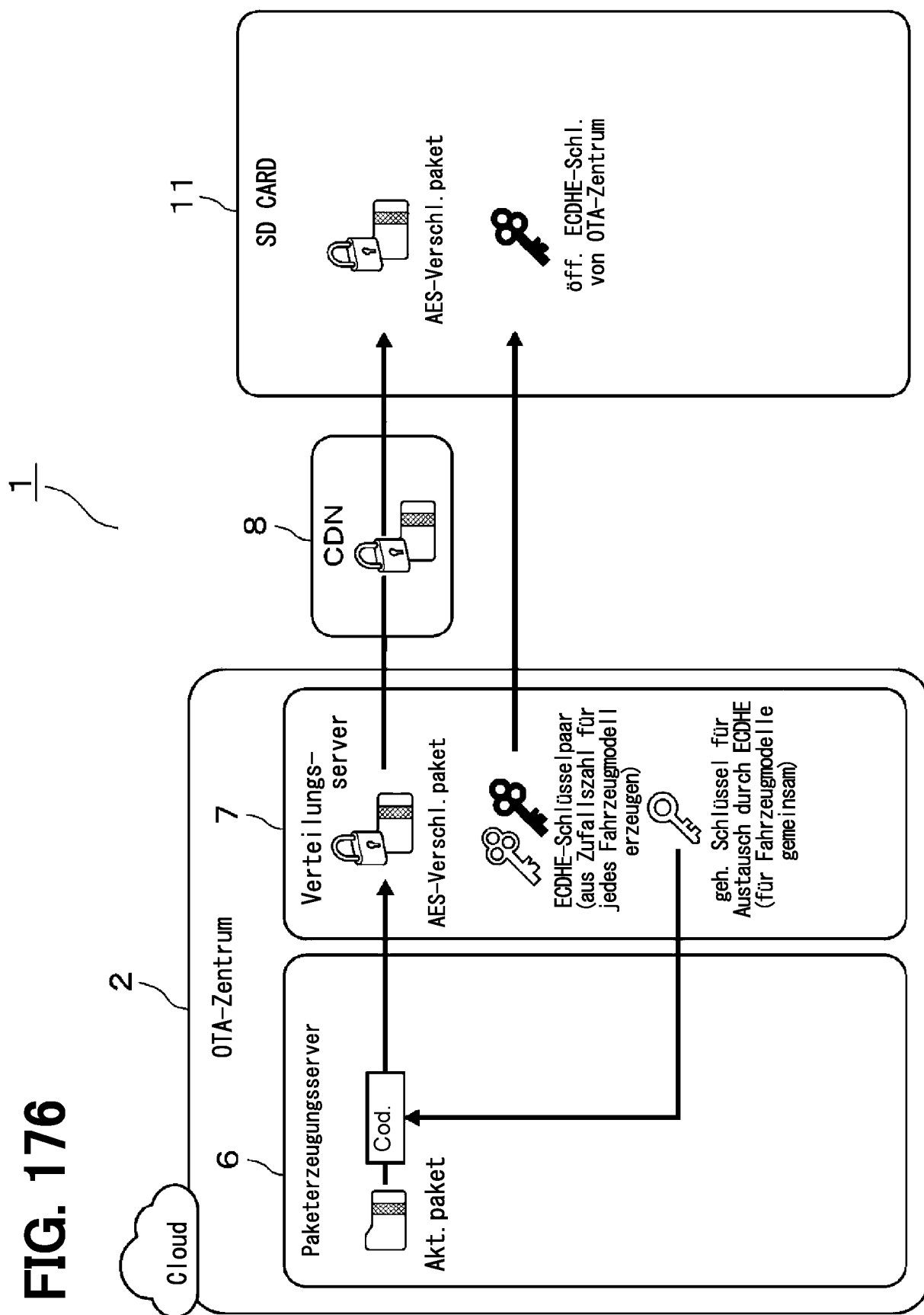


FIG. 177

1

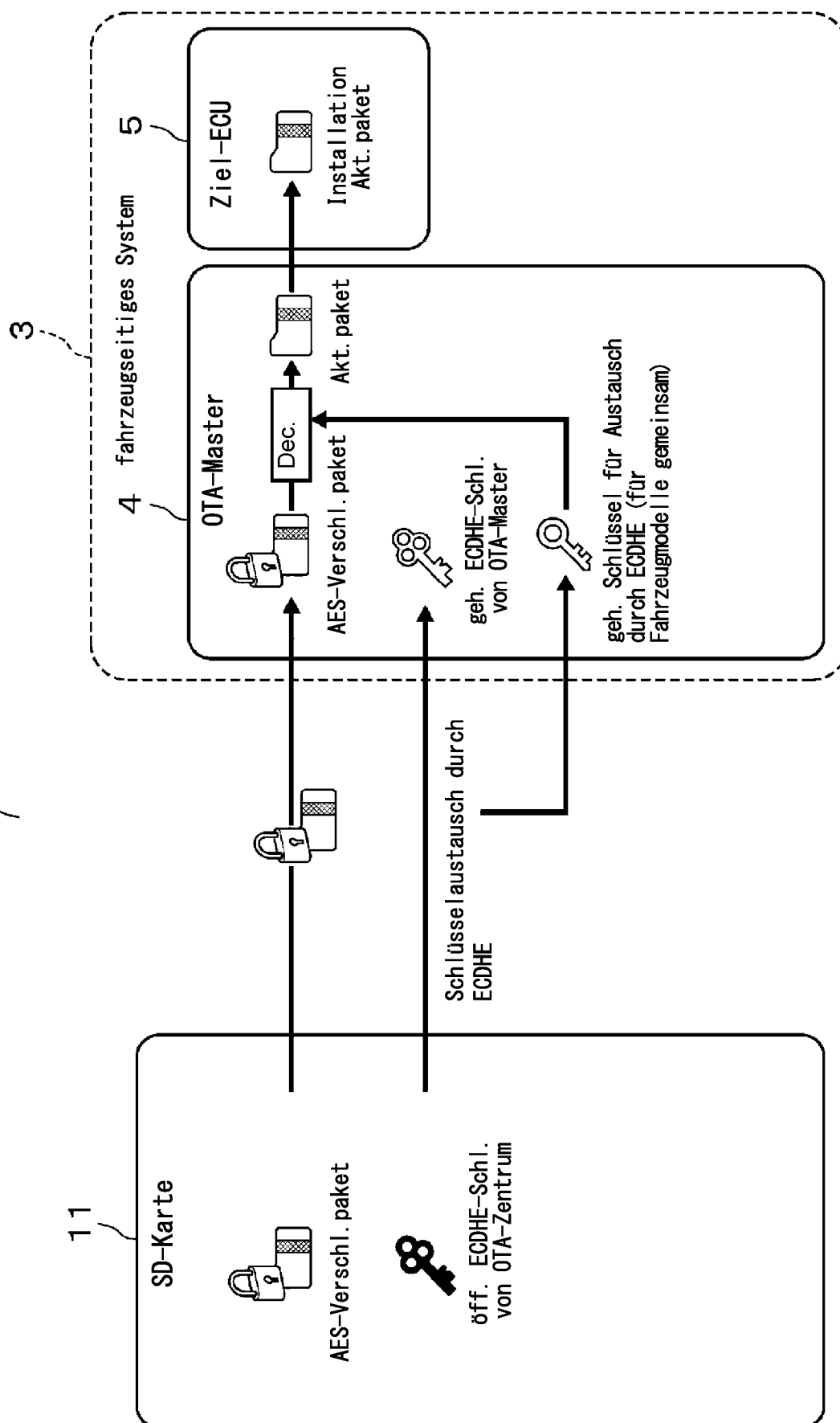


FIG. 178

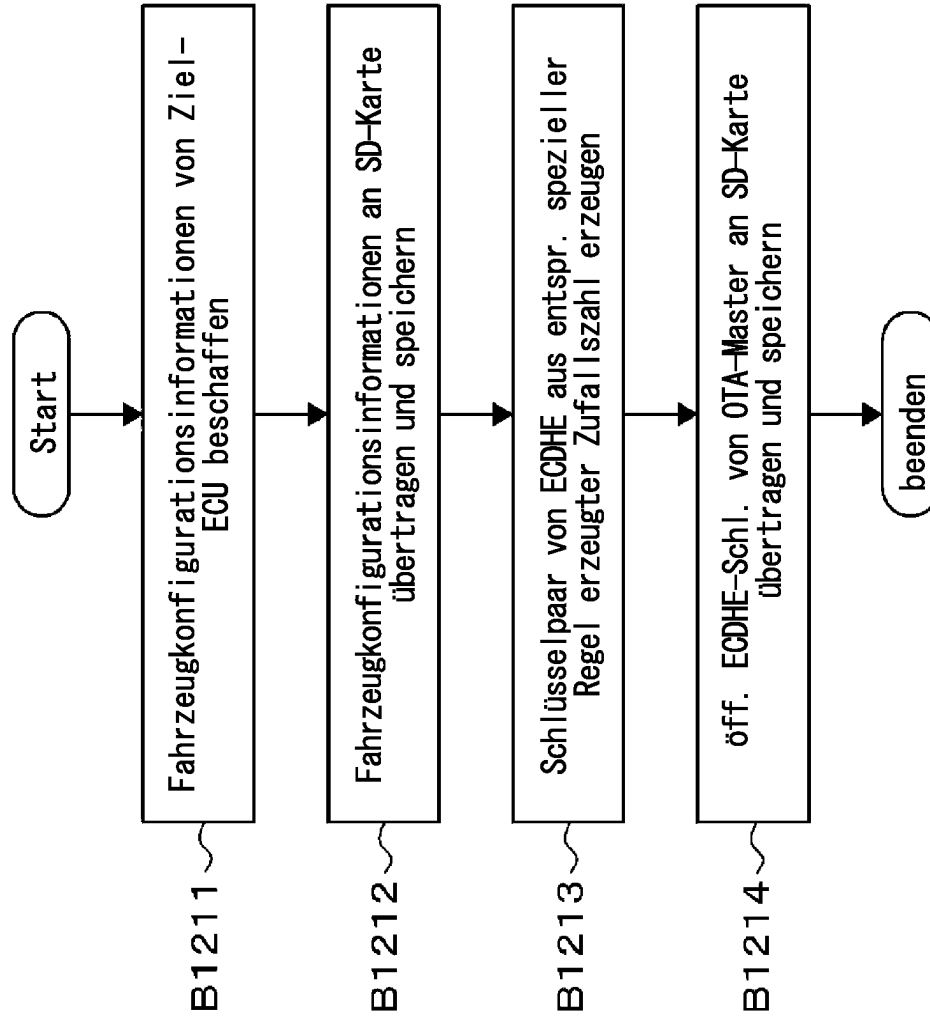


FIG. 179

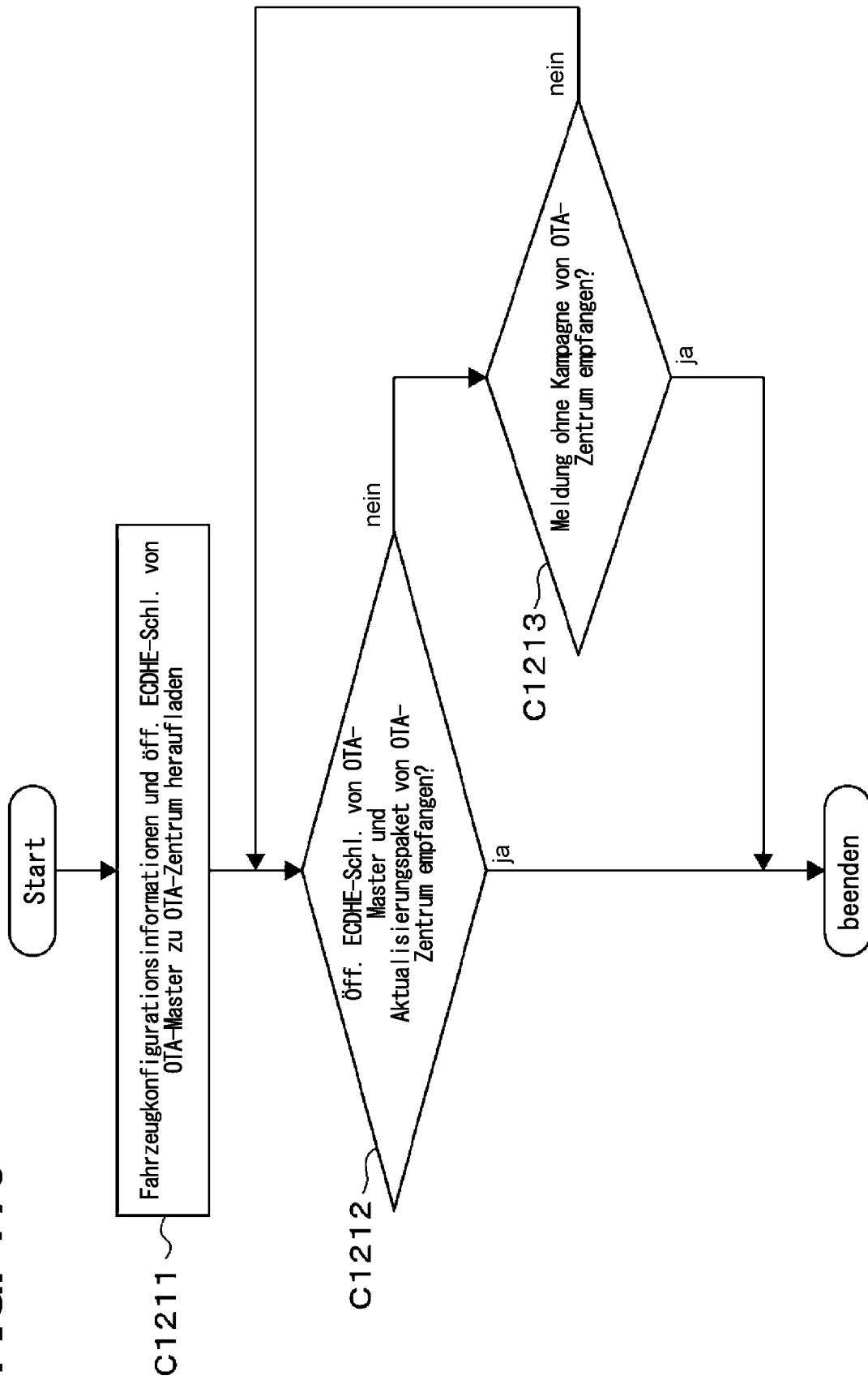


FIG. 180

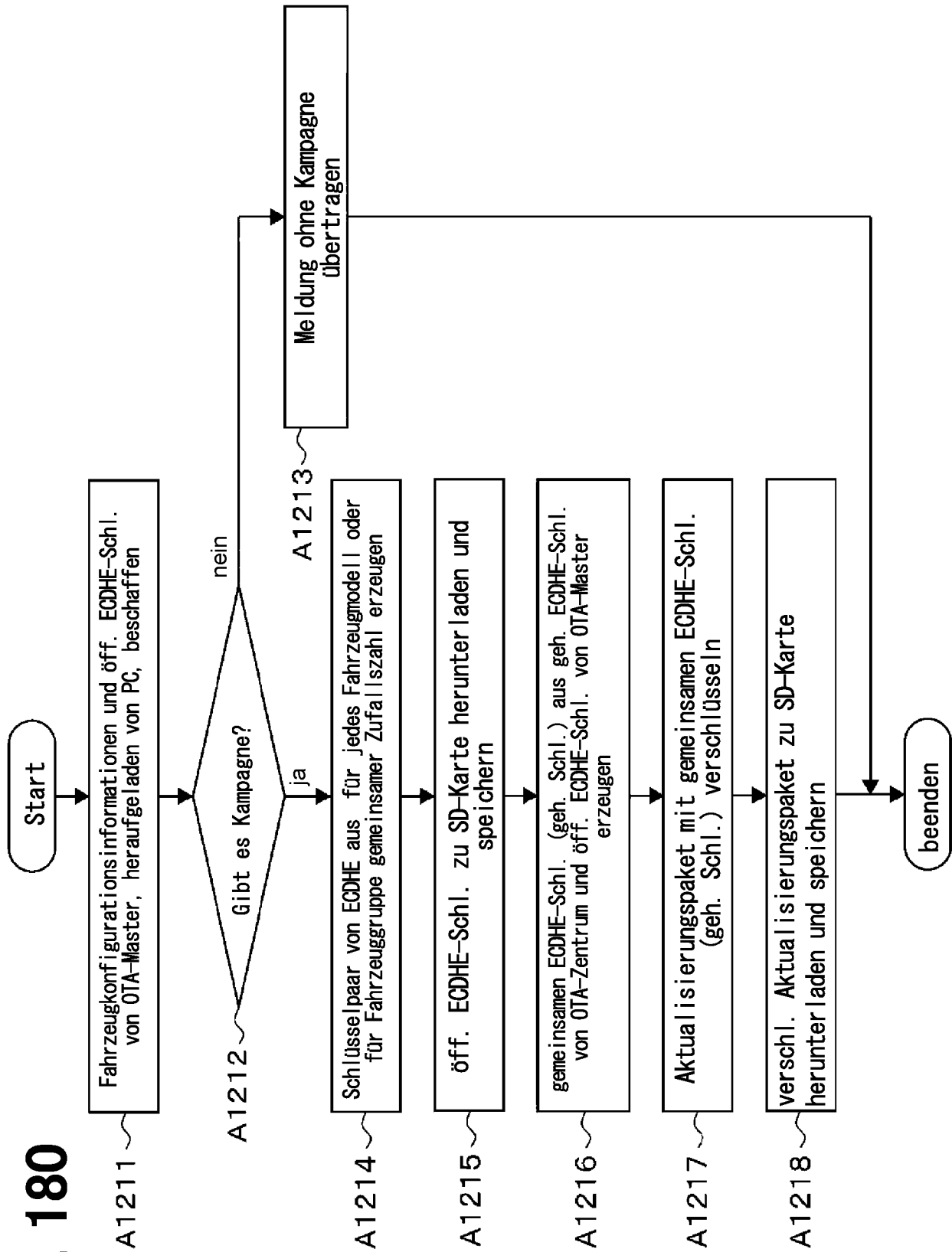
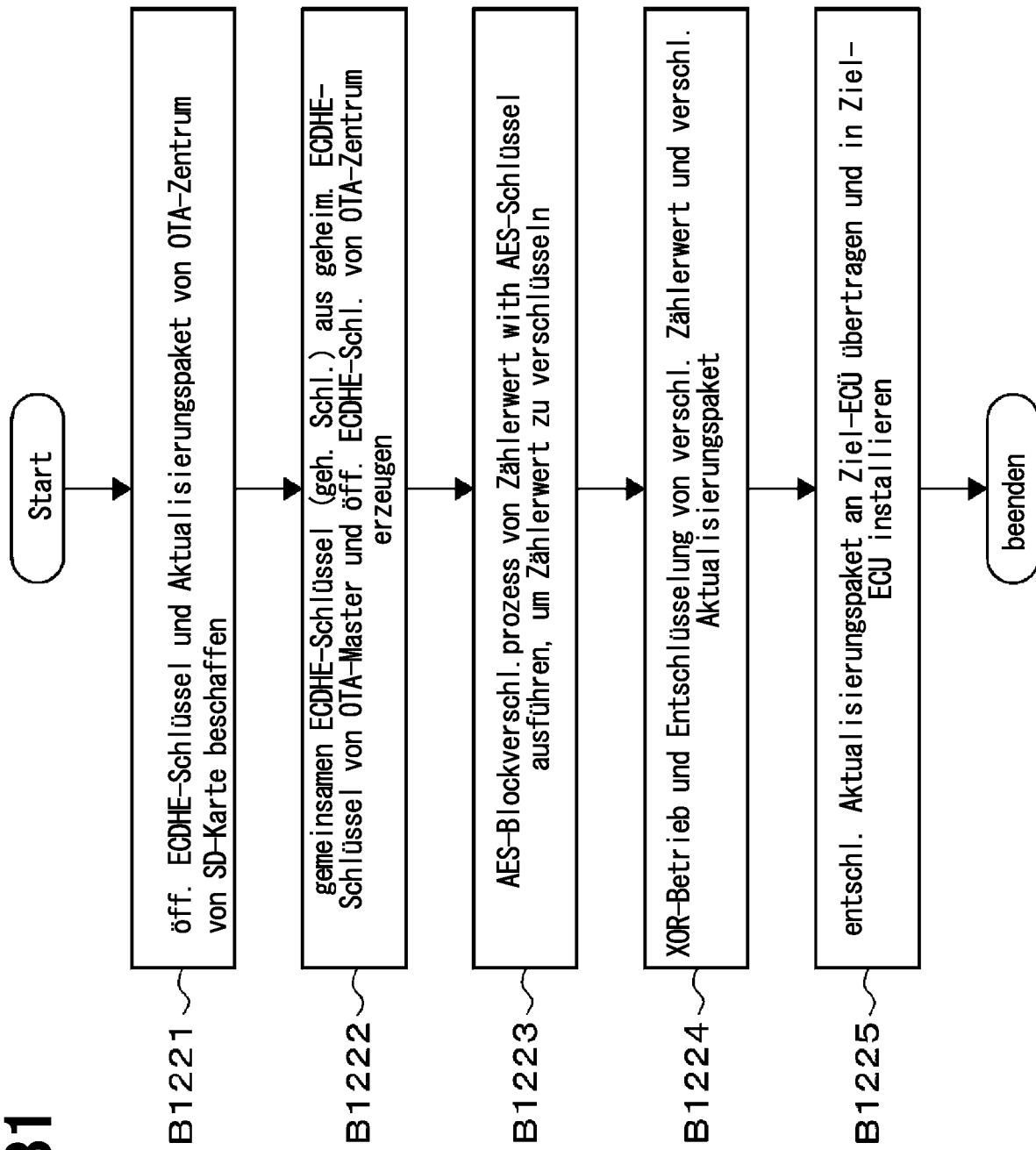


FIG. 181

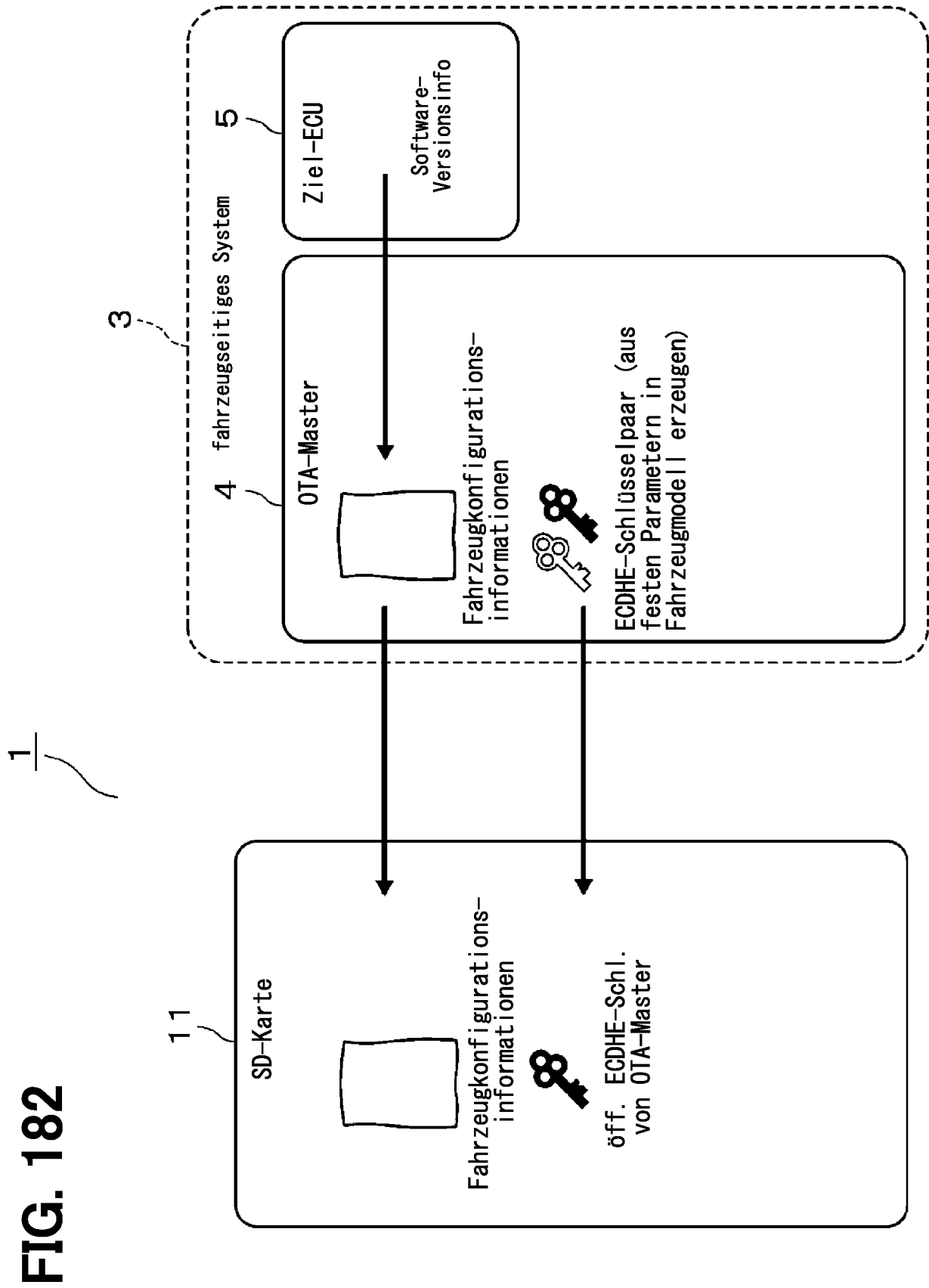


FIG. 183

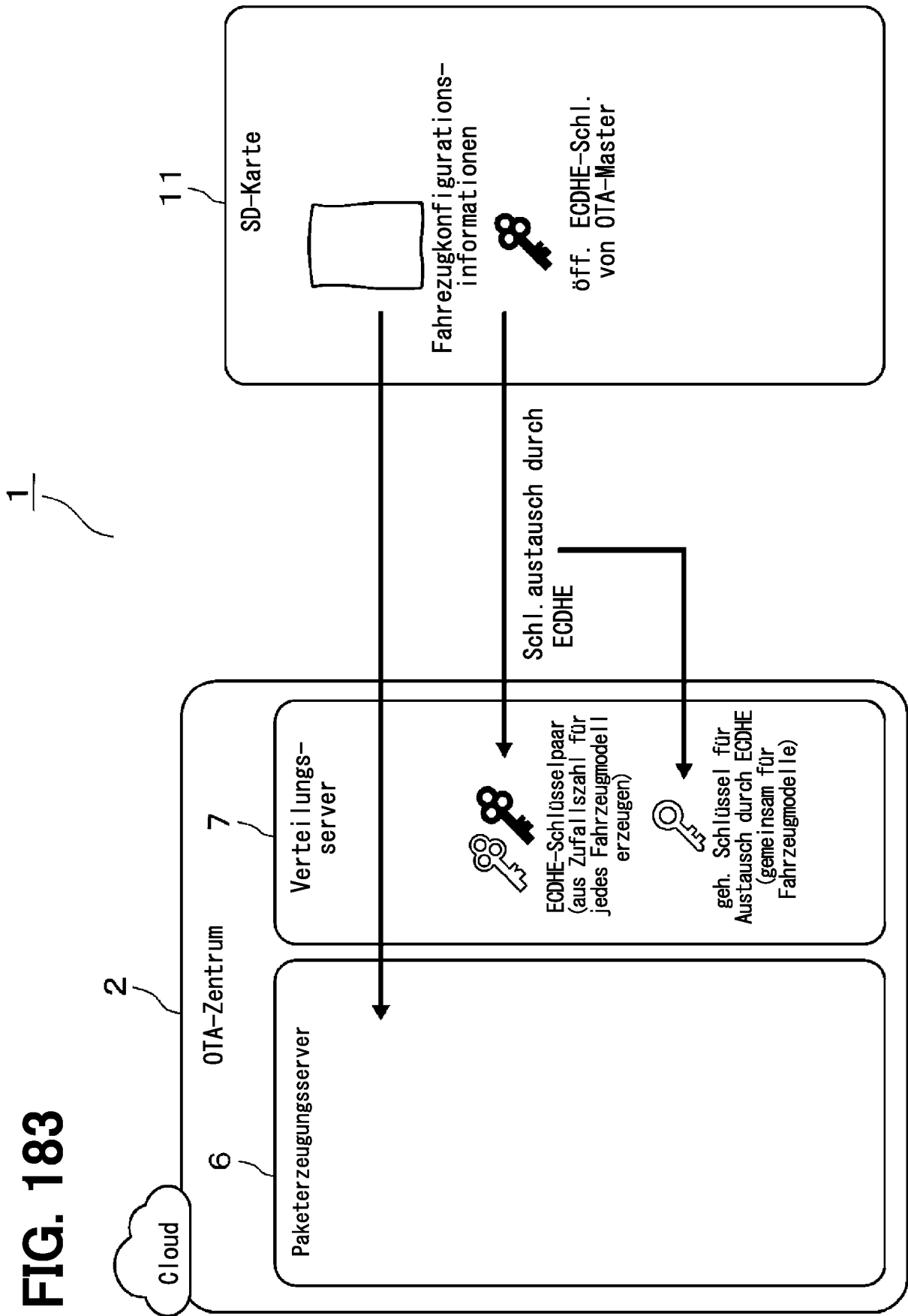


FIG. 184

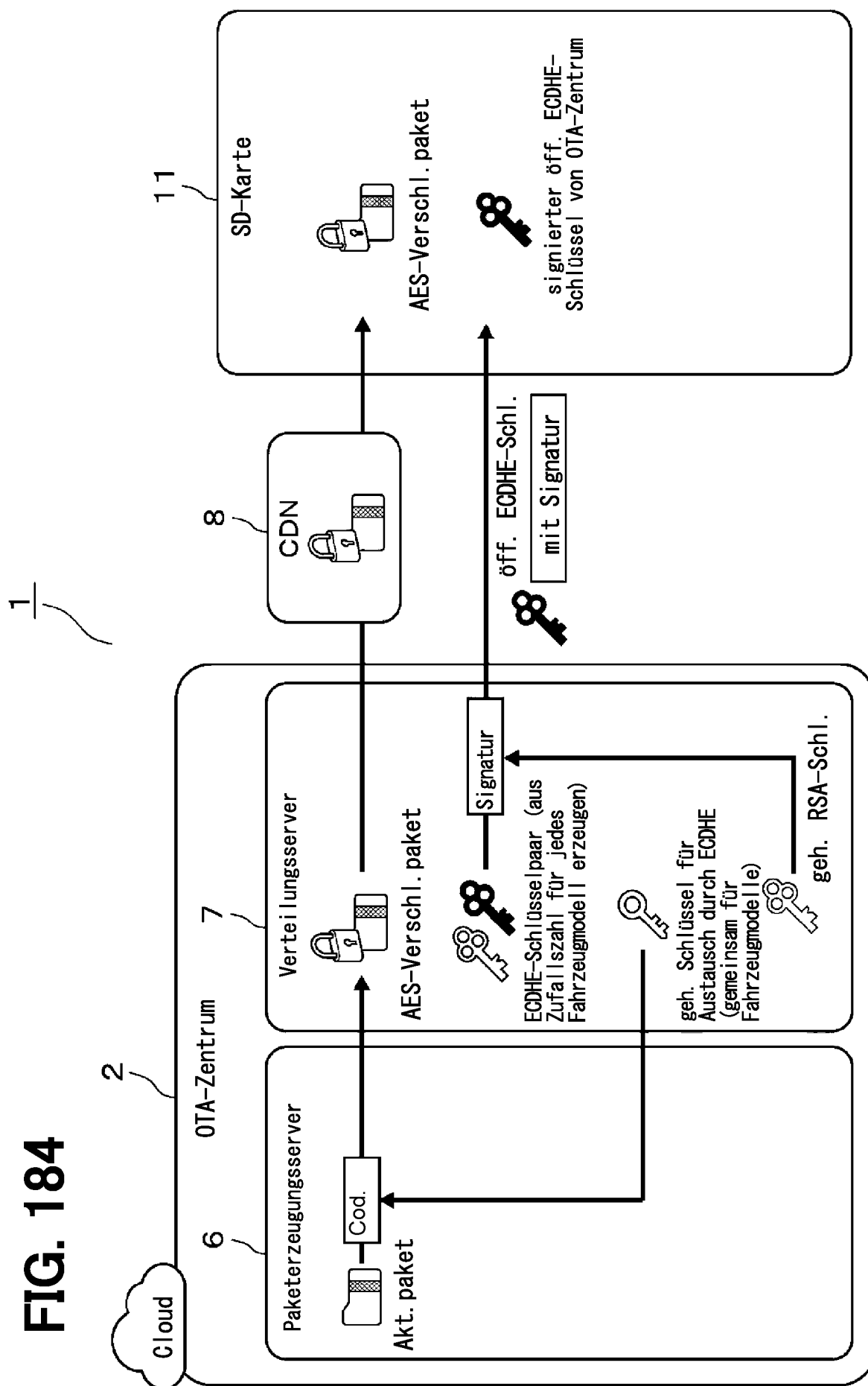


FIG. 185

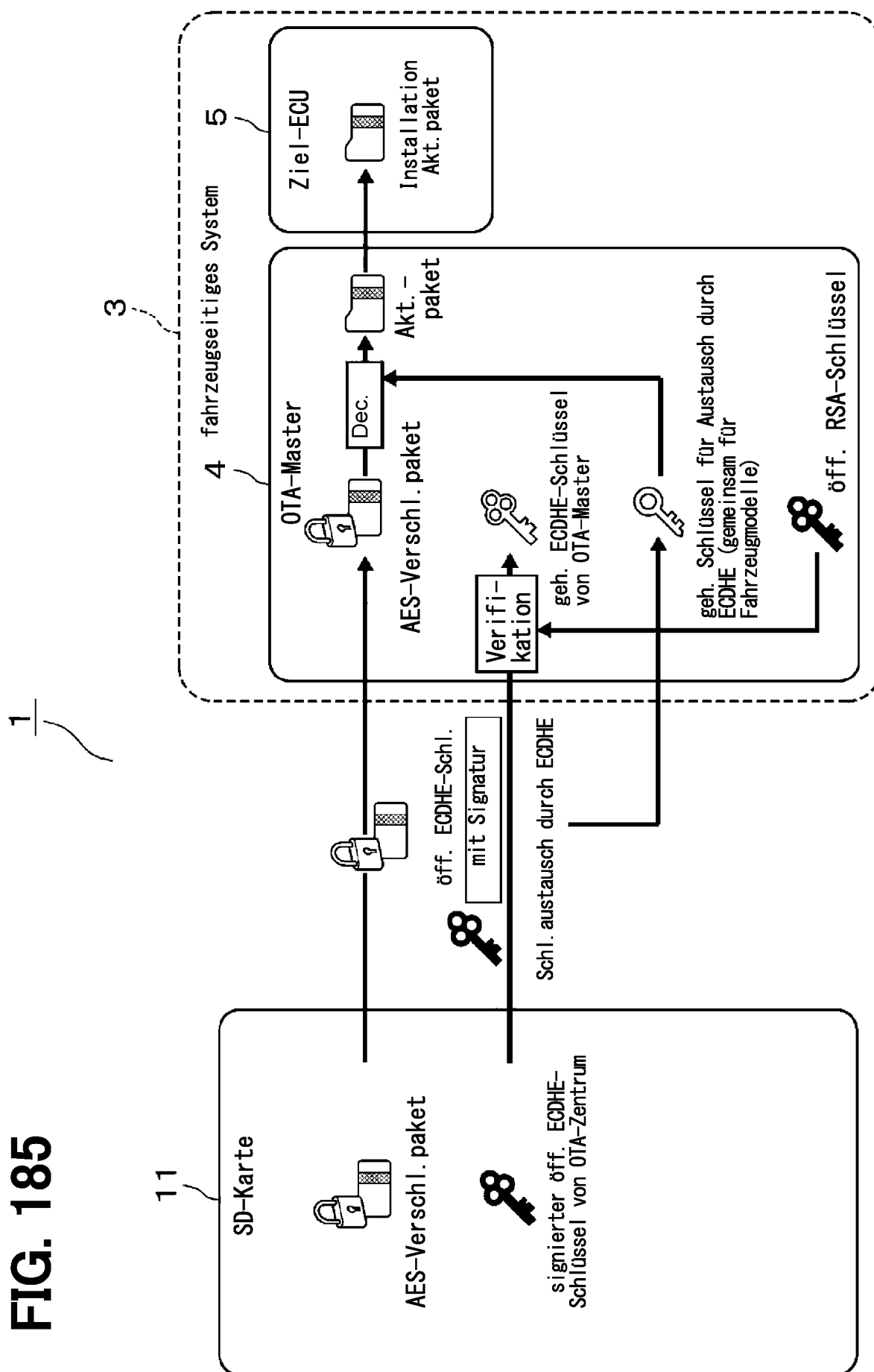


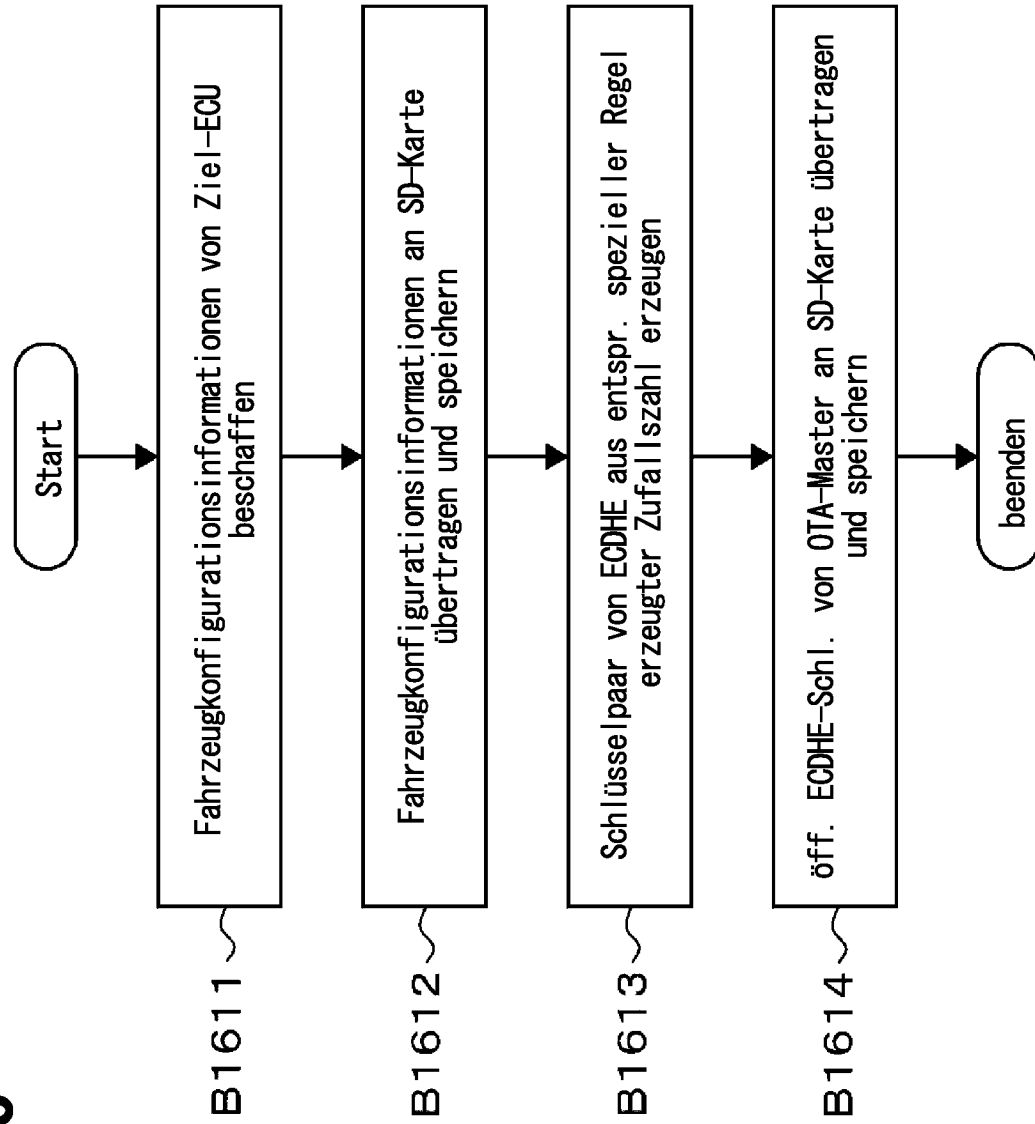
FIG. 186

FIG. 187

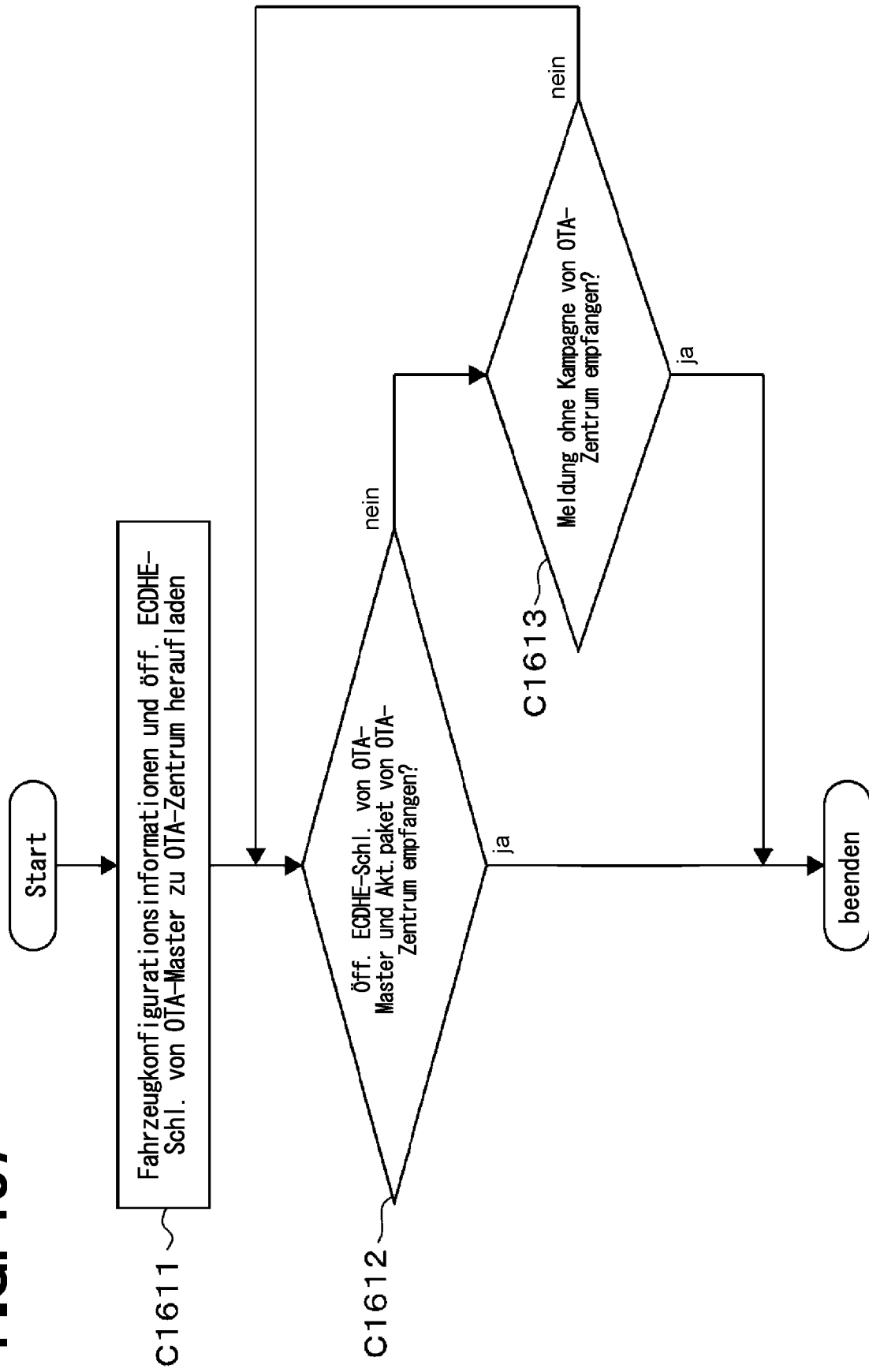


FIG. 188

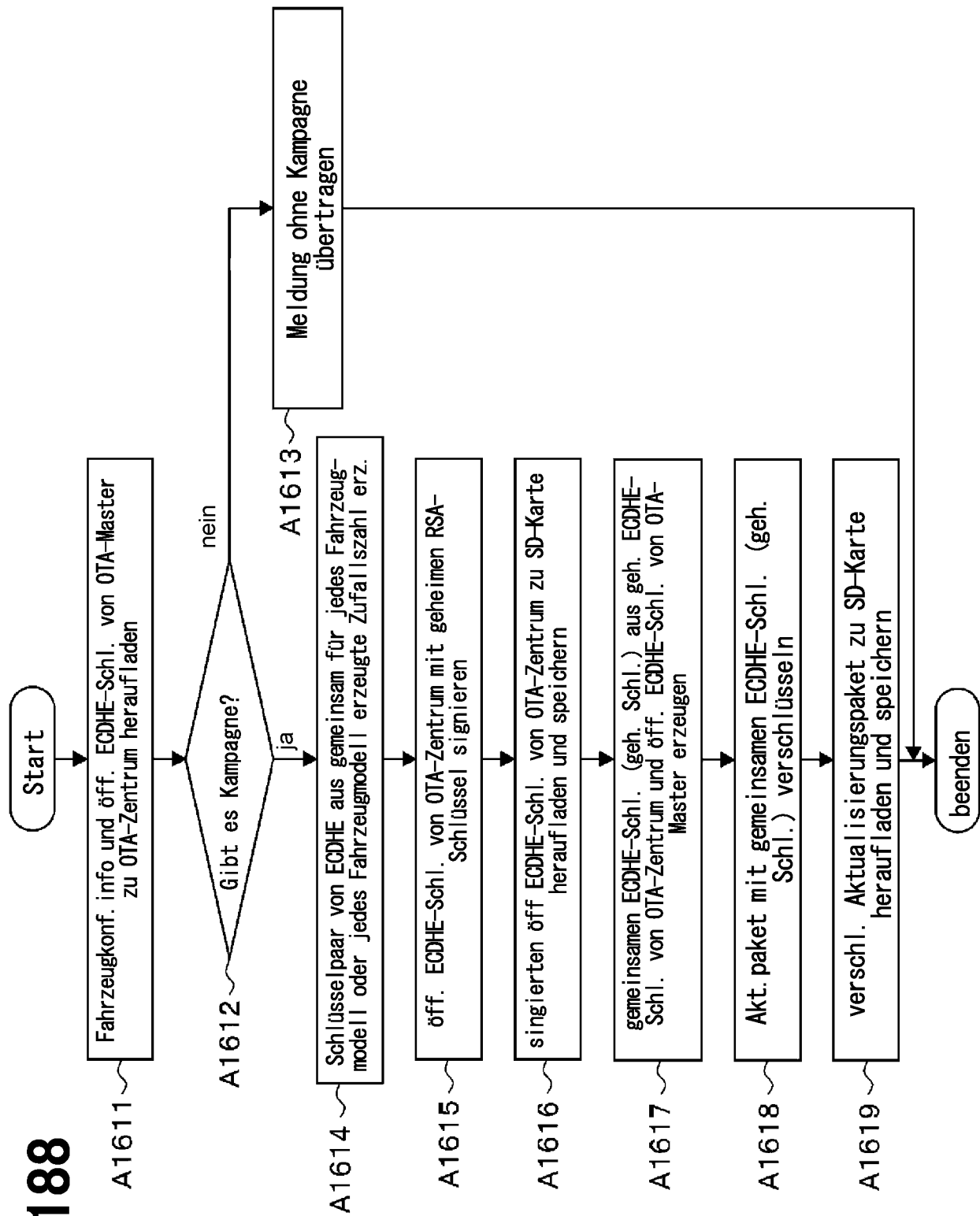


FIG. 189

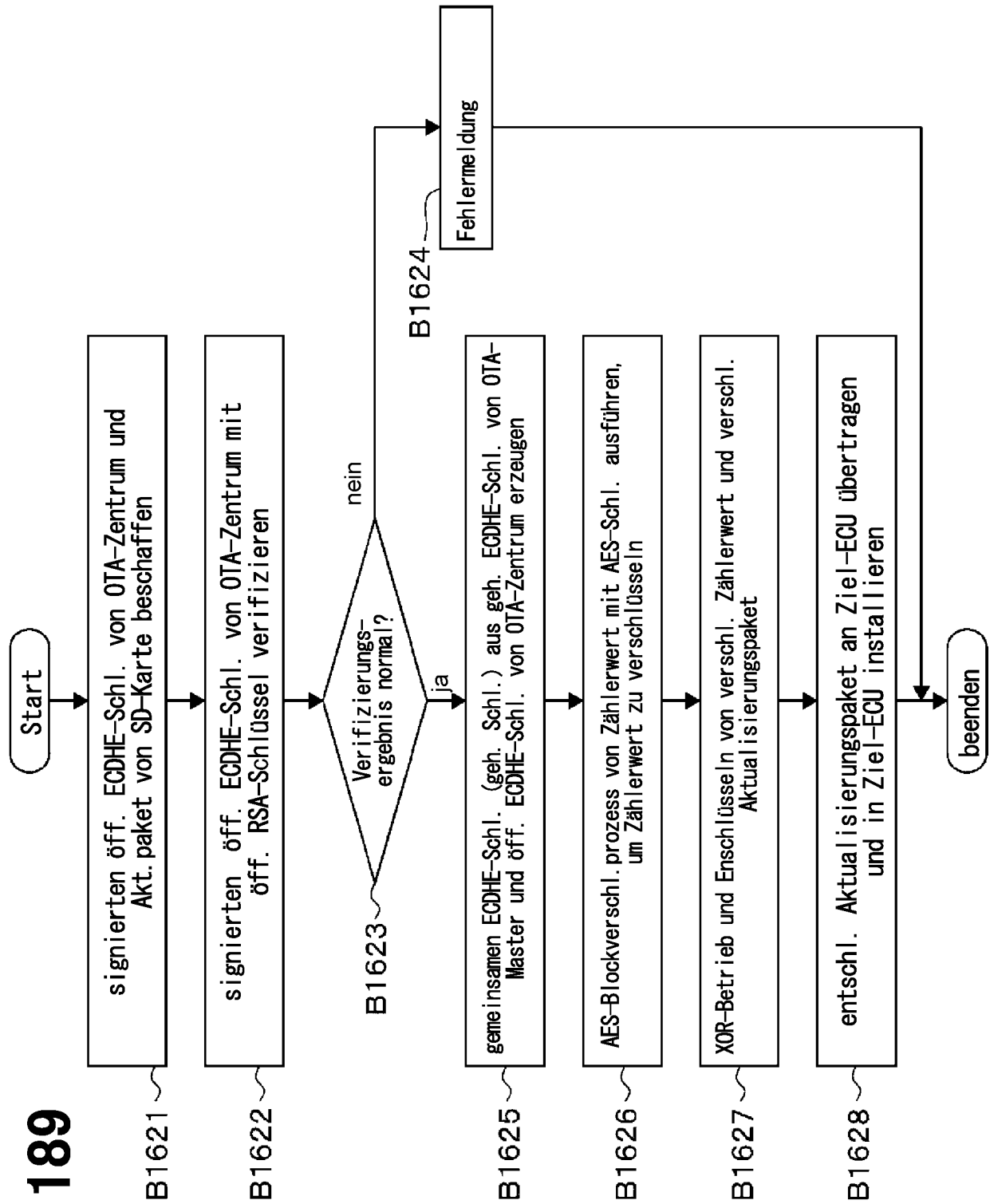


FIG. 190

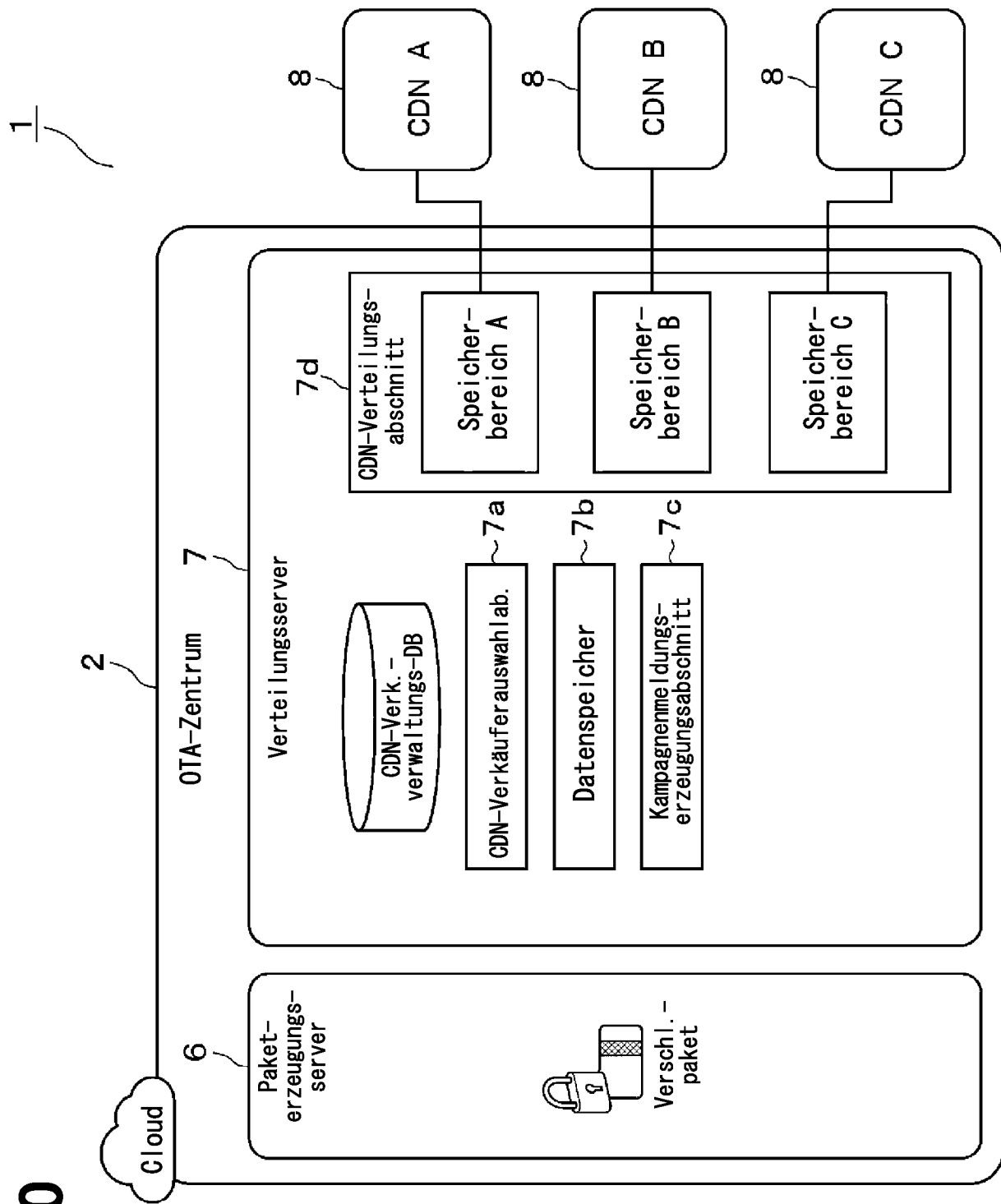


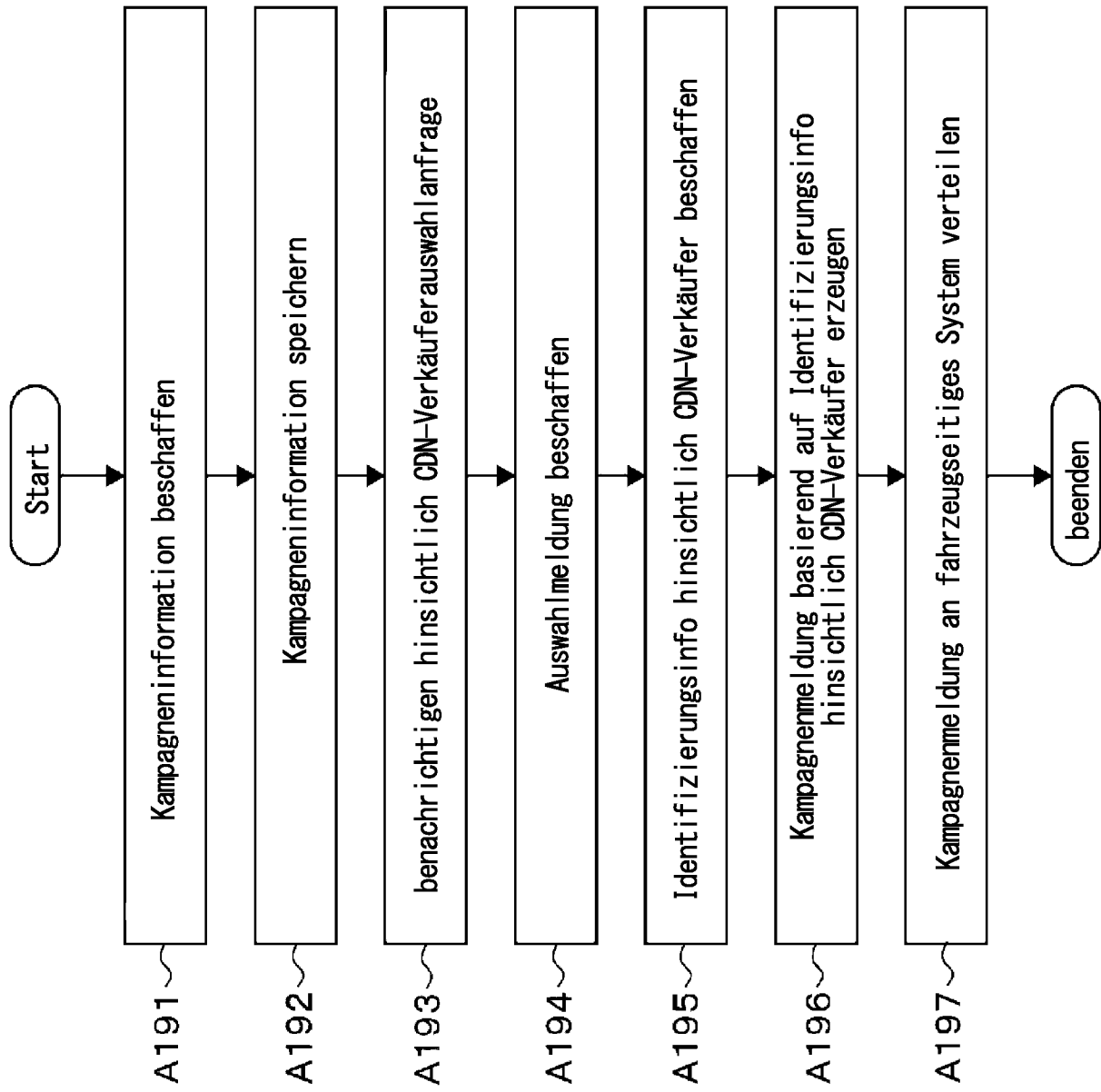
FIG. 191

FIG. 192

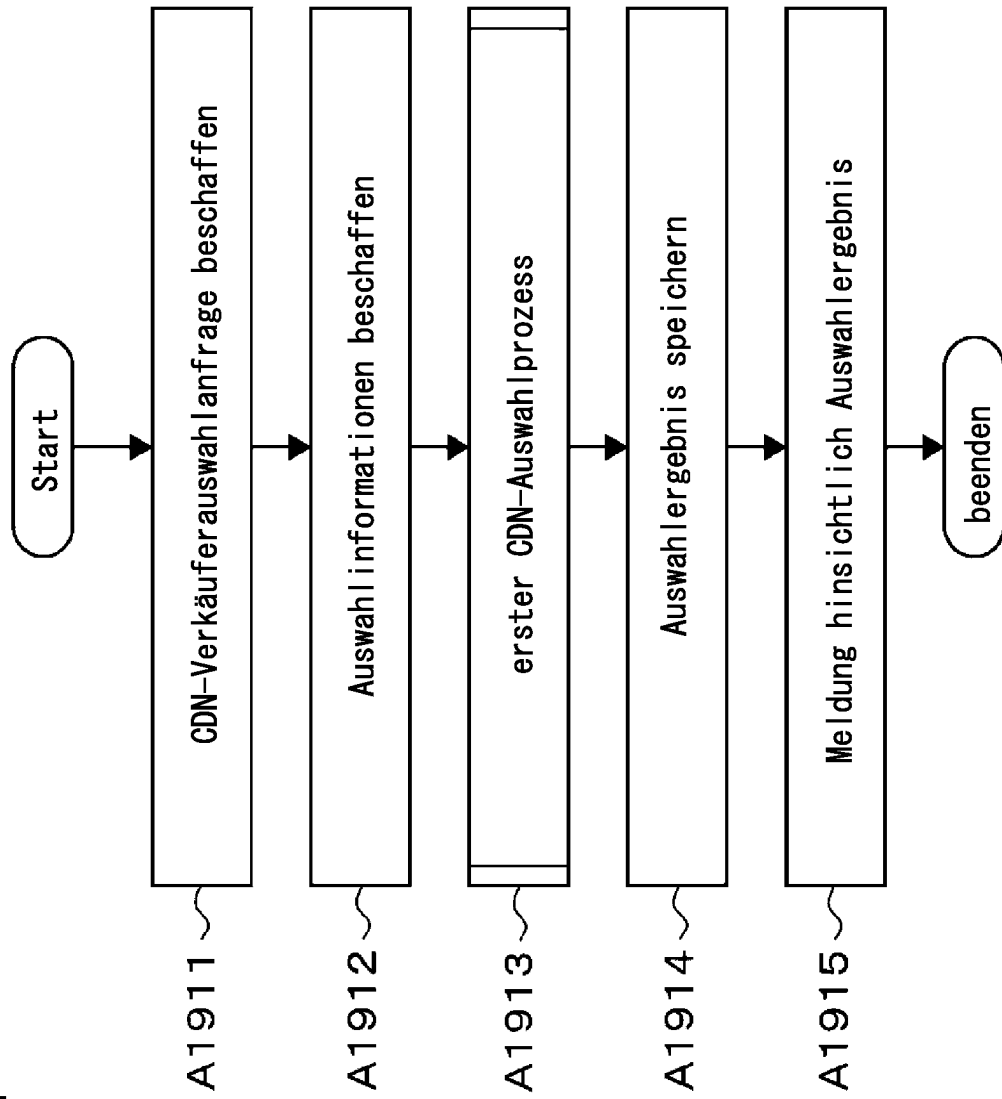
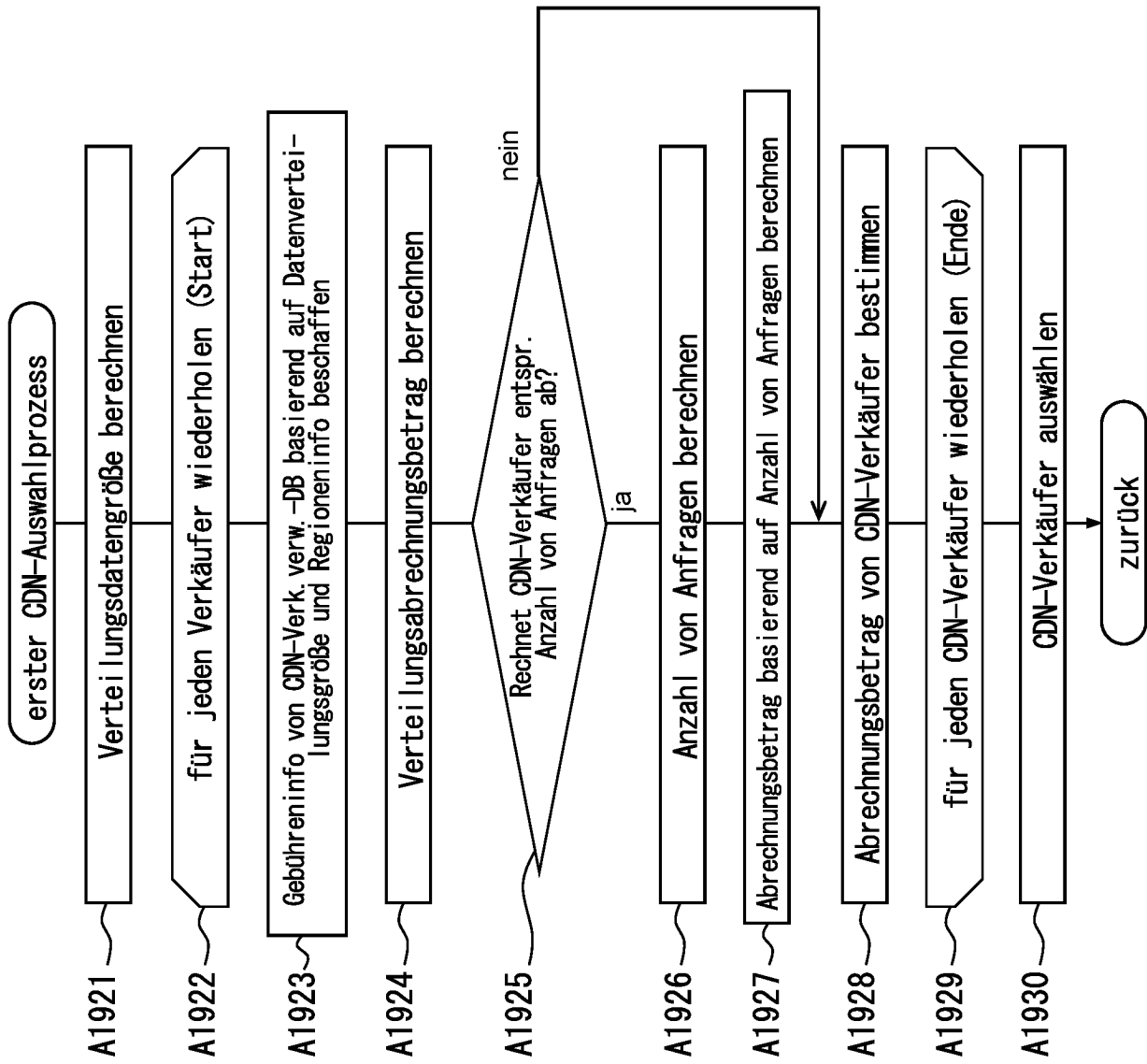


FIG. 193



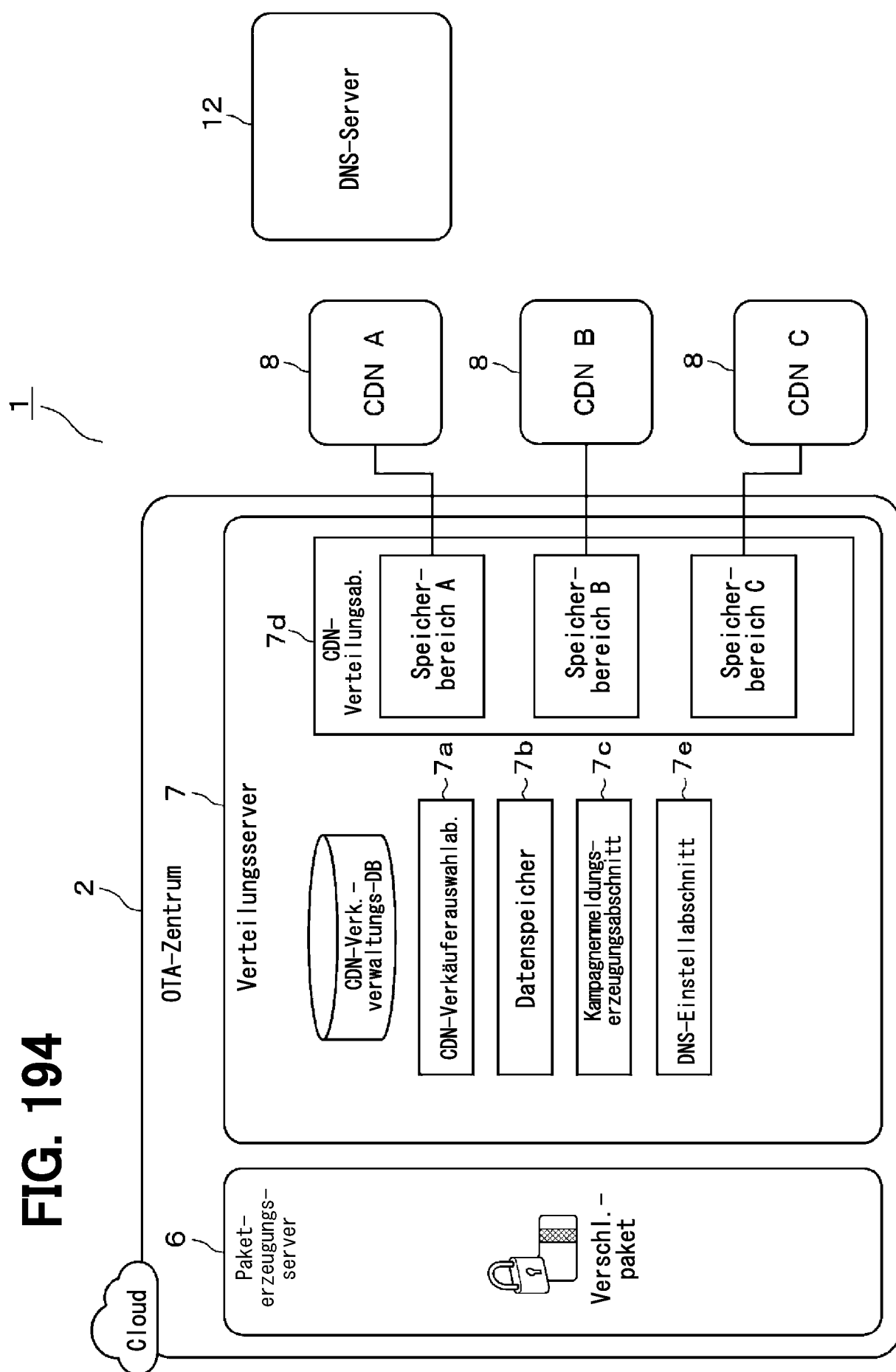


FIG. 195

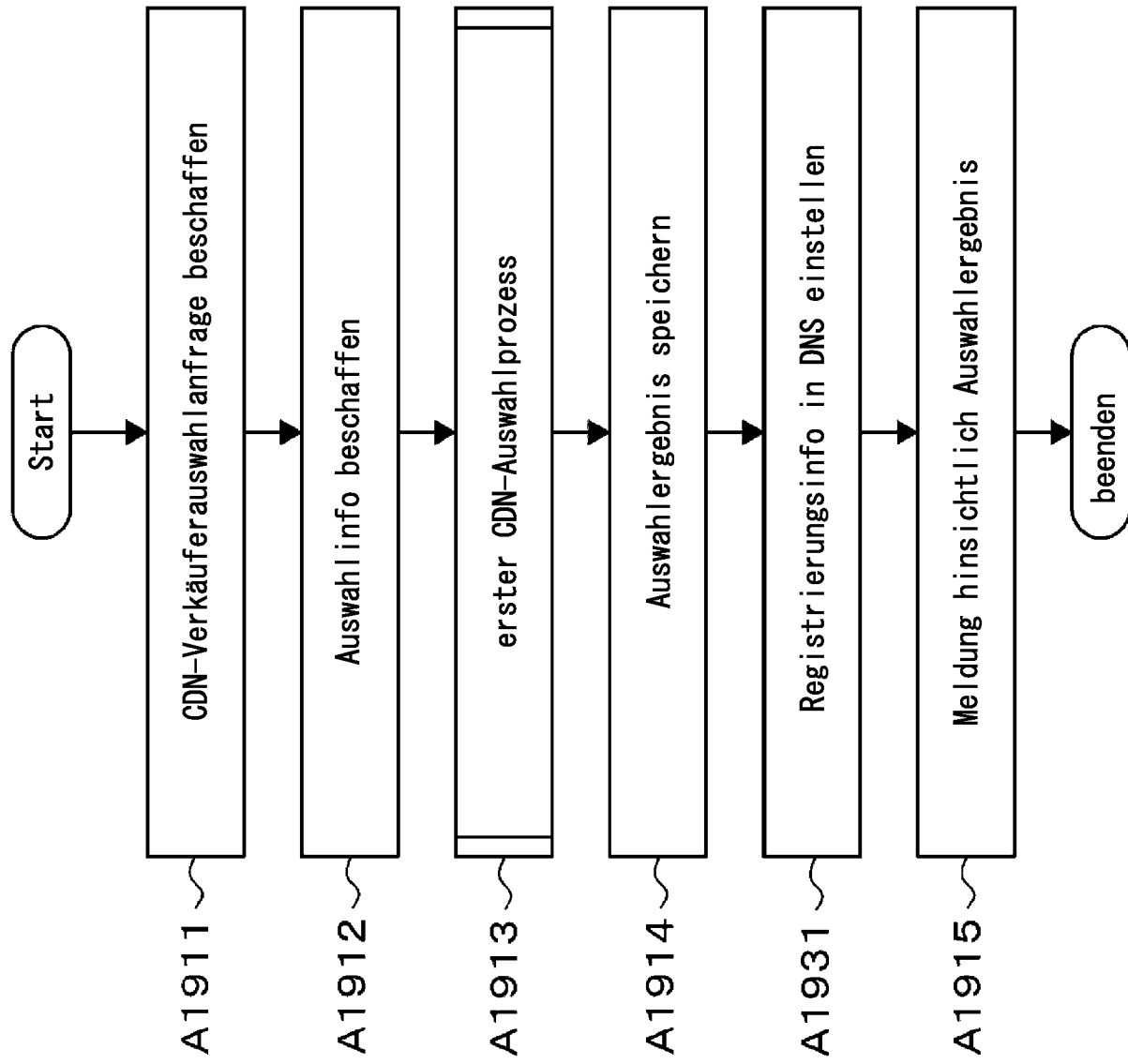


FIG. 196

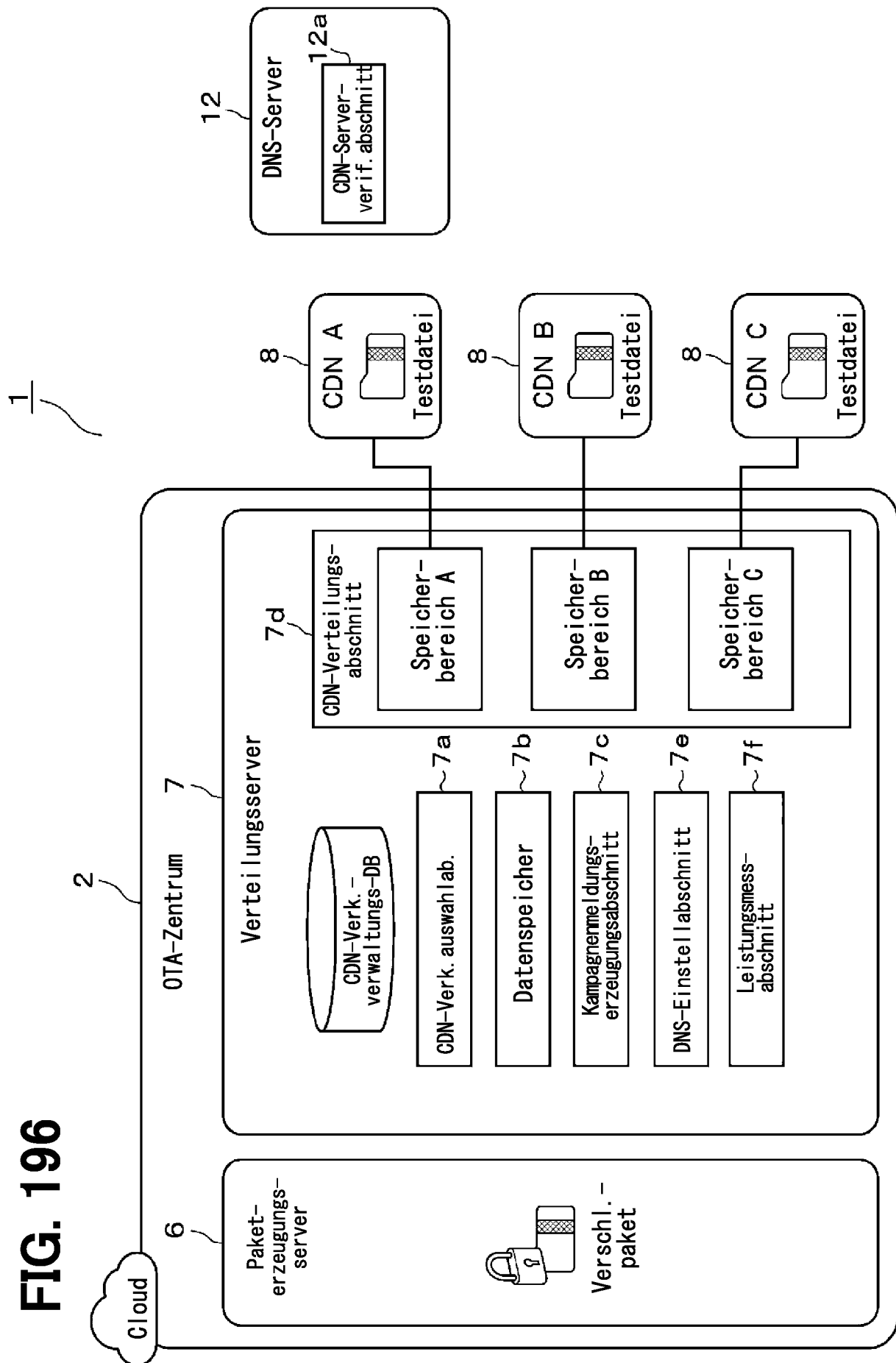


FIG. 197

Auswahl tabelle

CDN-Verkäufer	Verteilungs-zeit	Verteilungs-Flag	Kostenrang
AAA	Xms	falsch	1
BBB	Yms	wahr	2
CCC	Zms	wahr	3

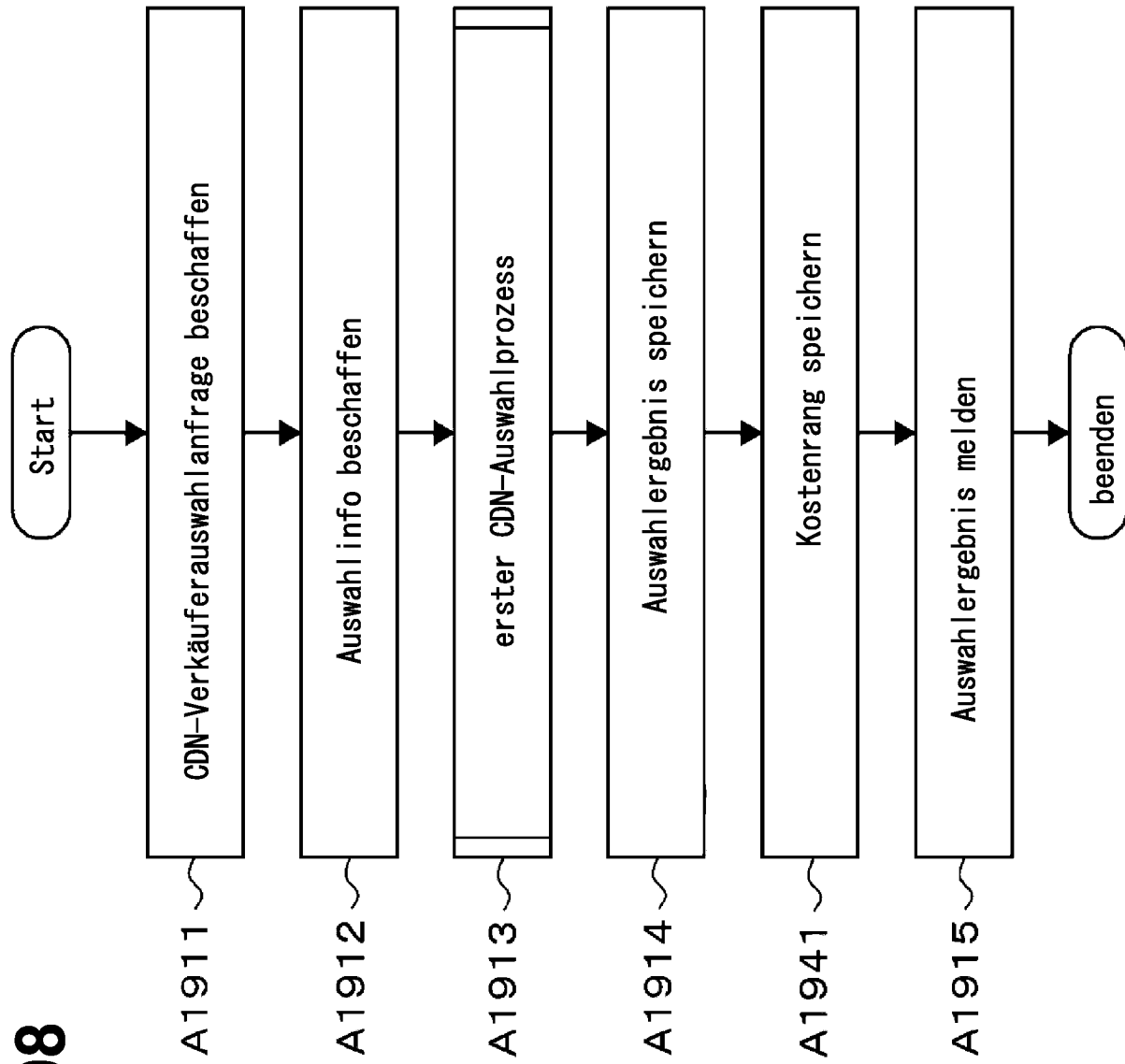
FIG. 198

FIG. 199

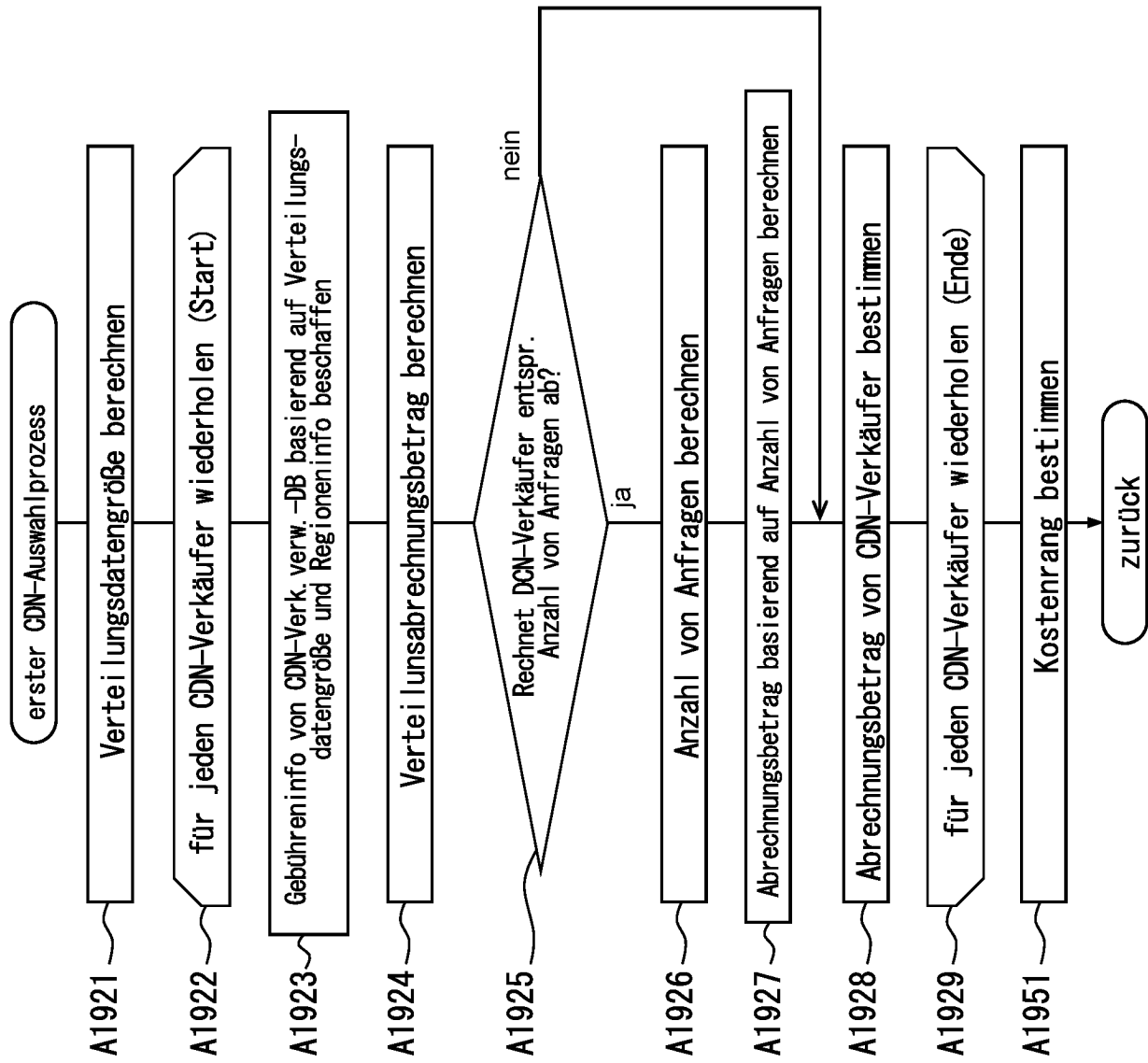


FIG. 200

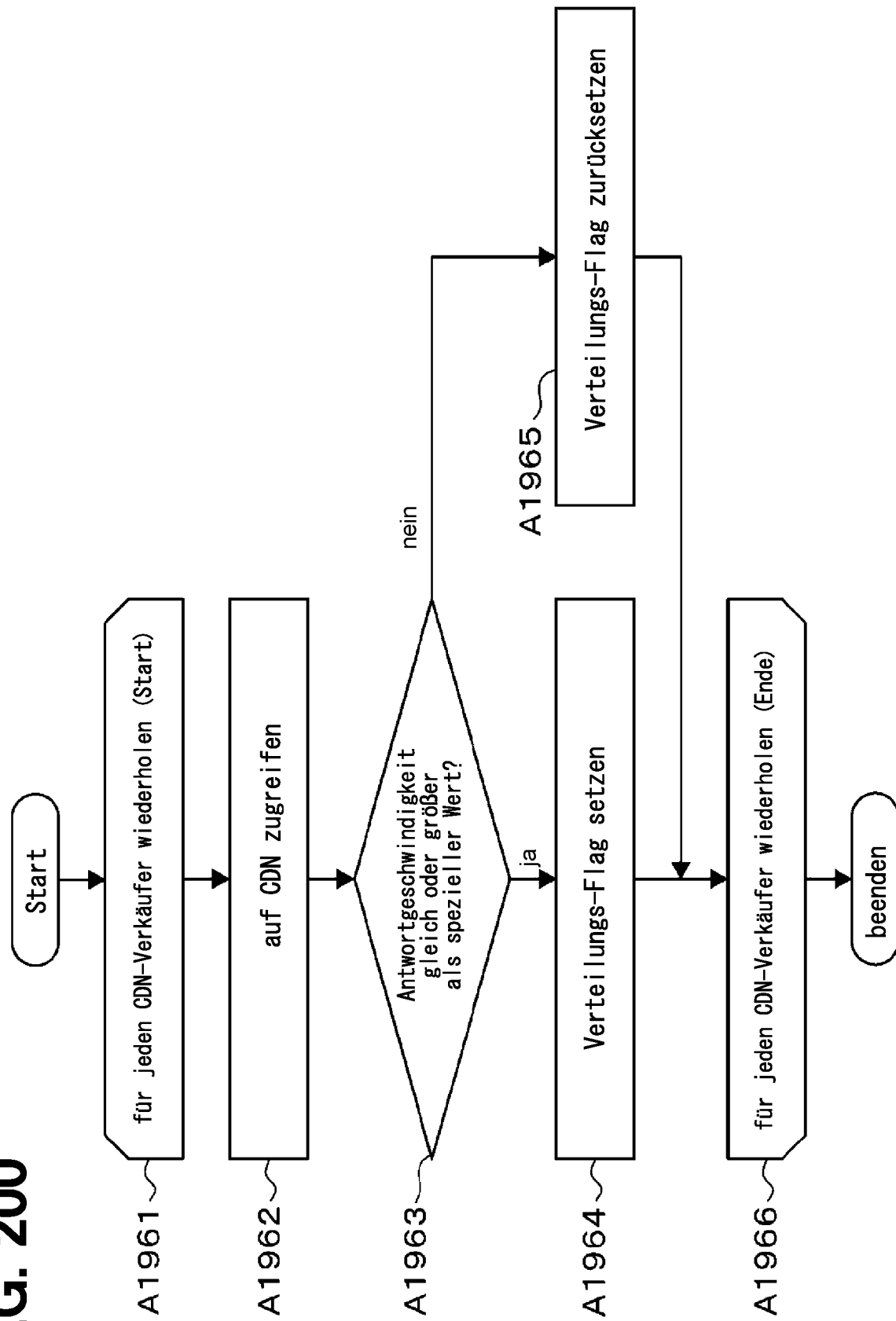


FIG. 201

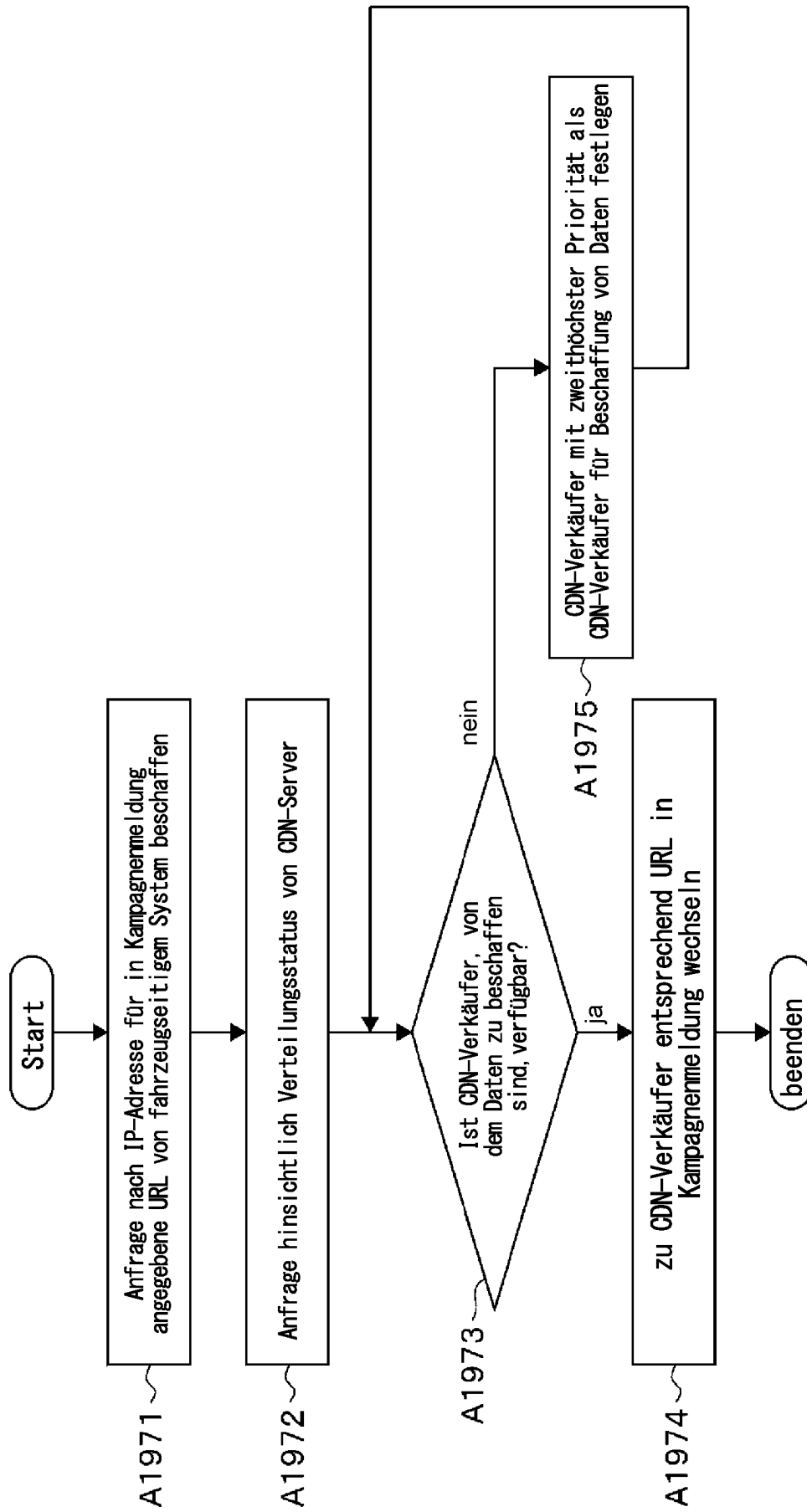


FIG. 202

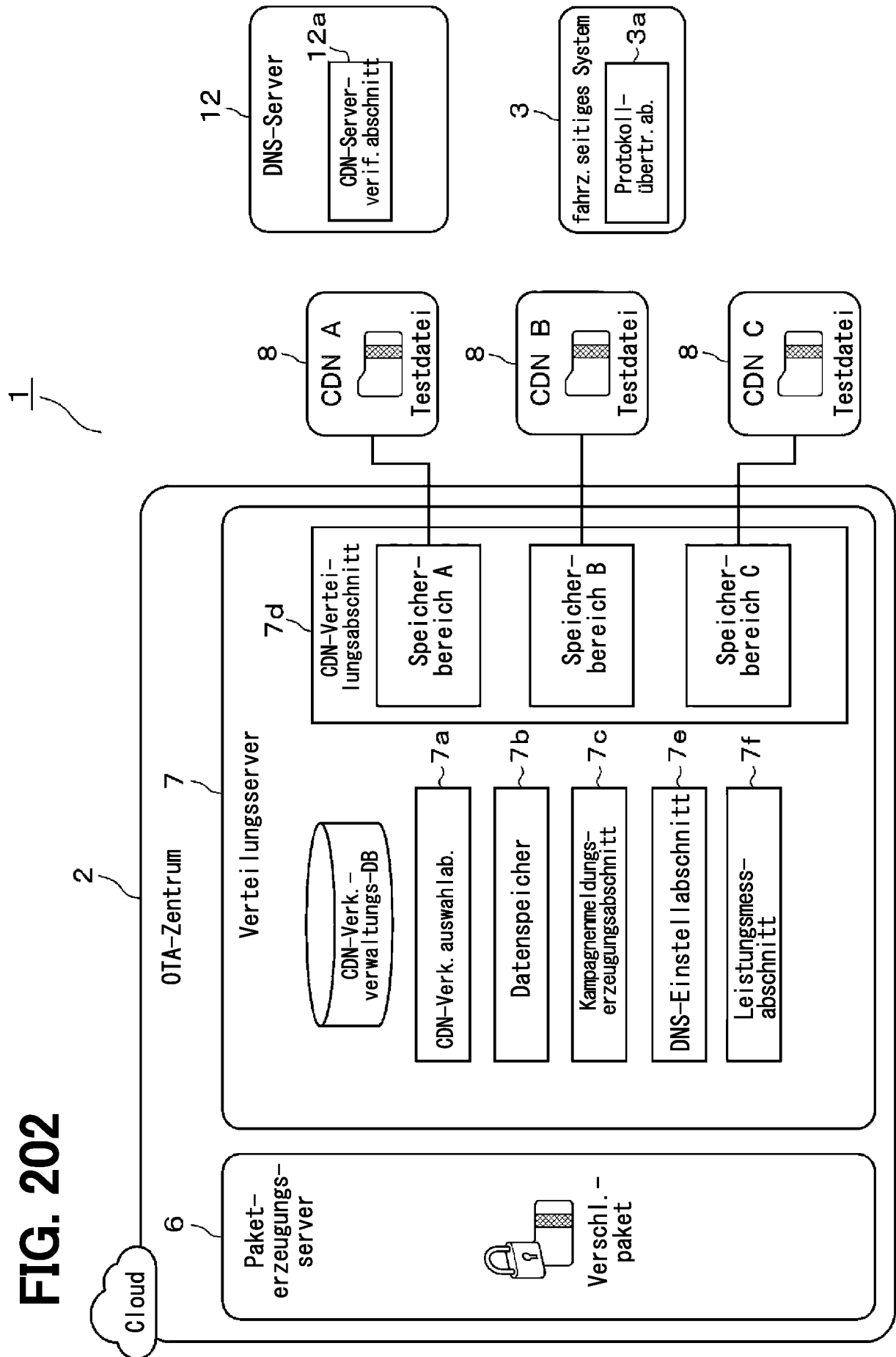


FIG. 203

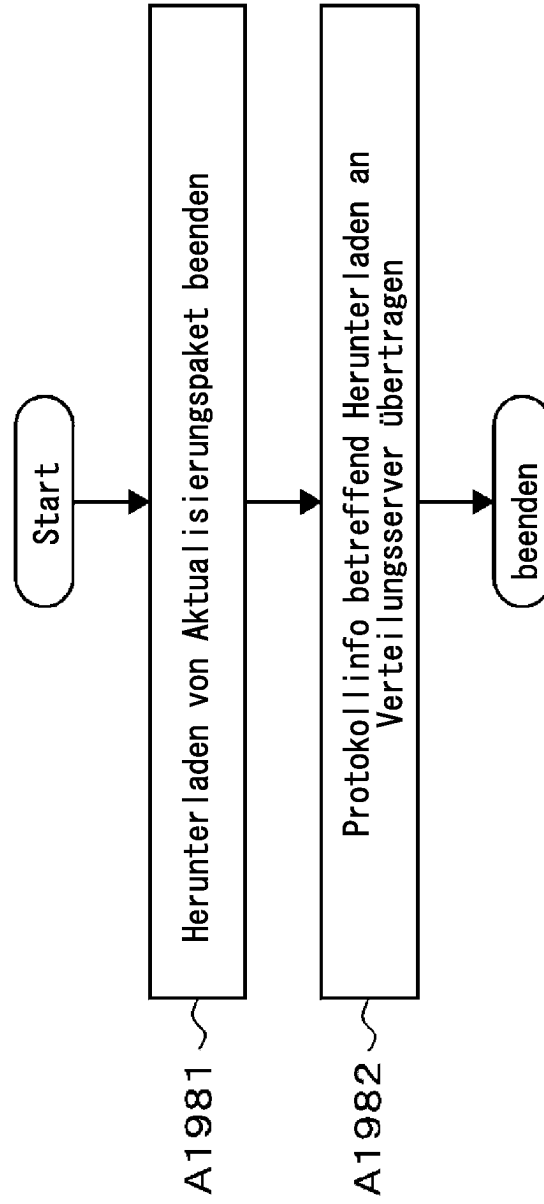


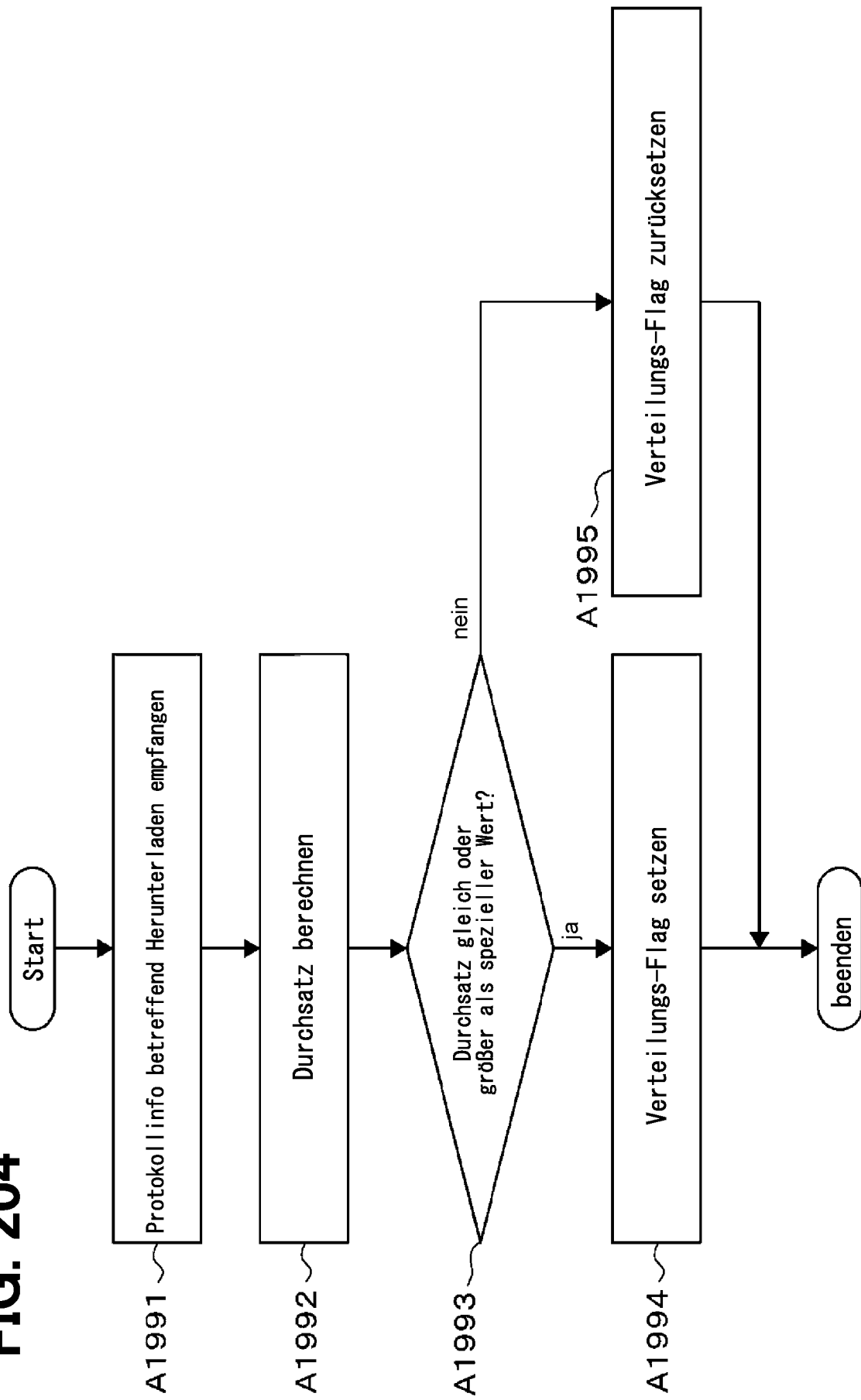
FIG. 204

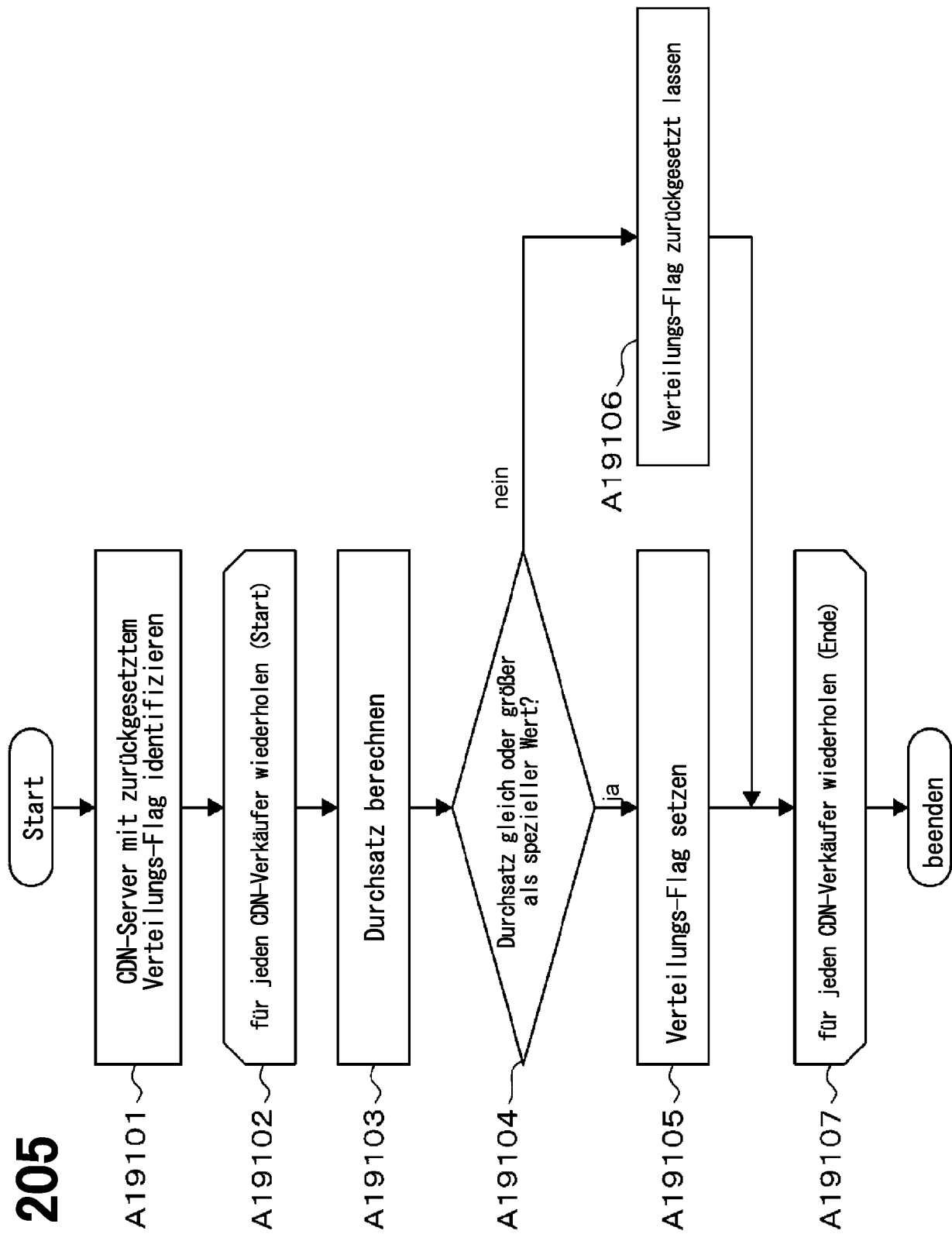
FIG. 205

FIG. 206

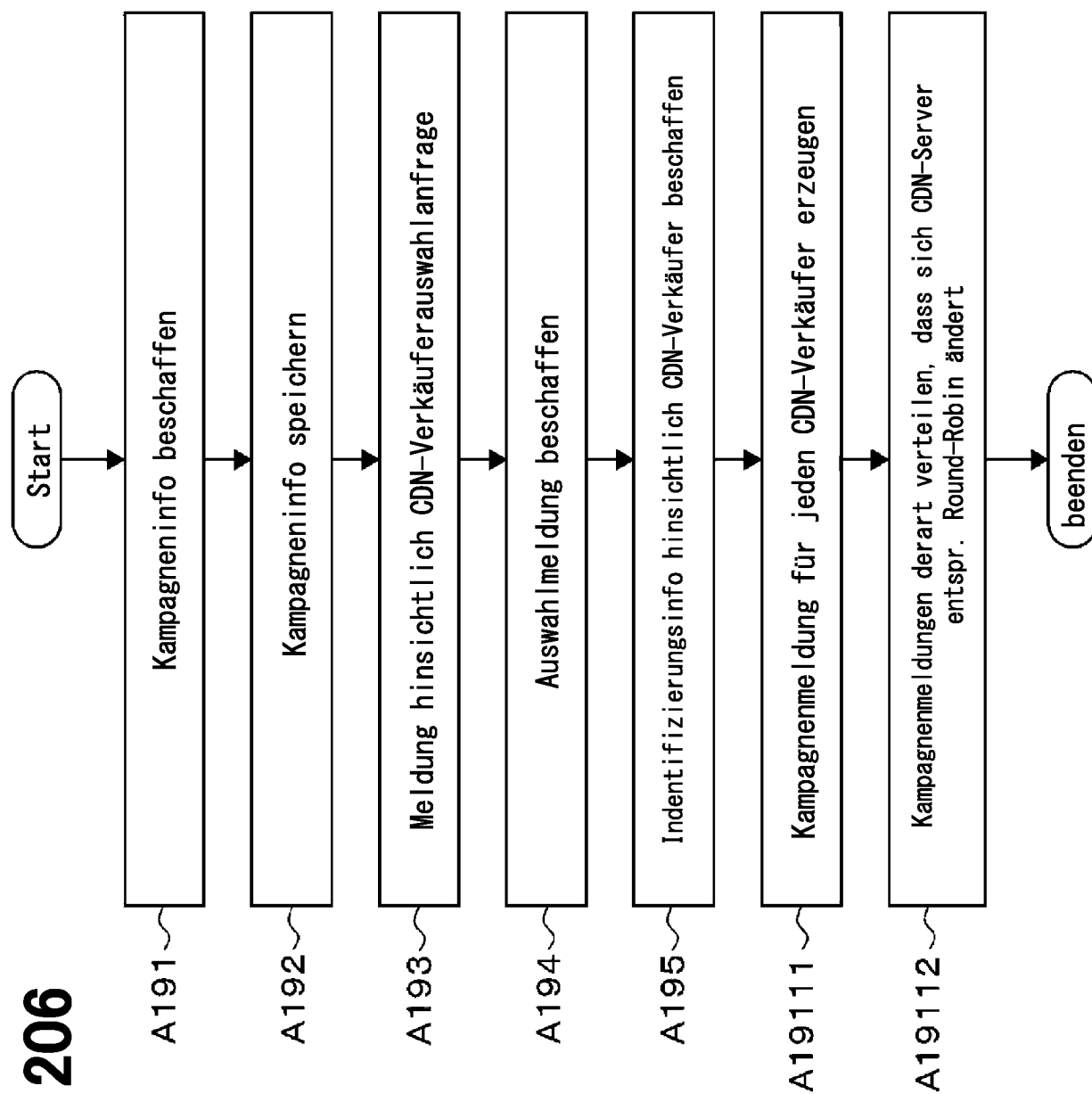


FIG. 207

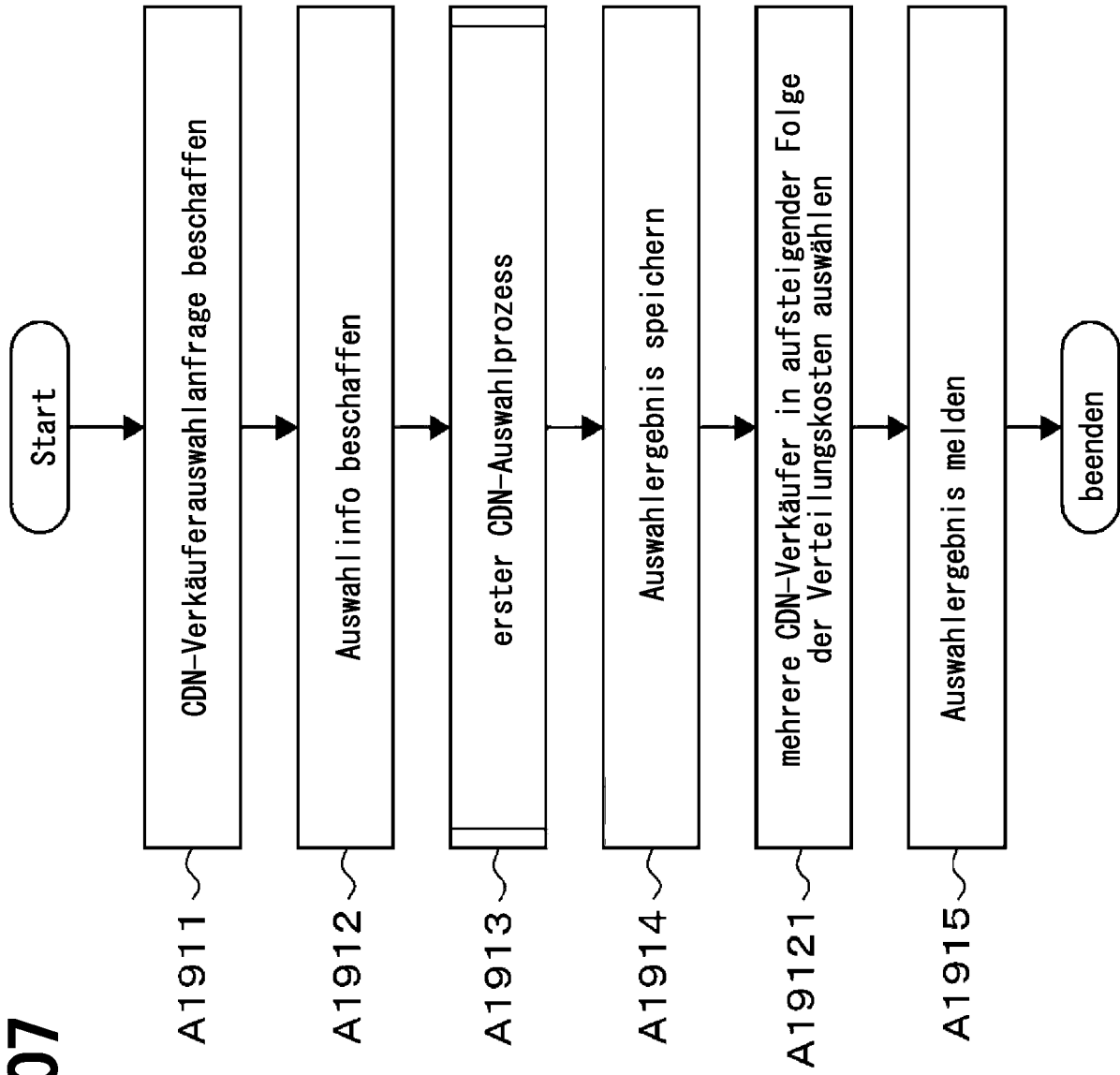


FIG. 208

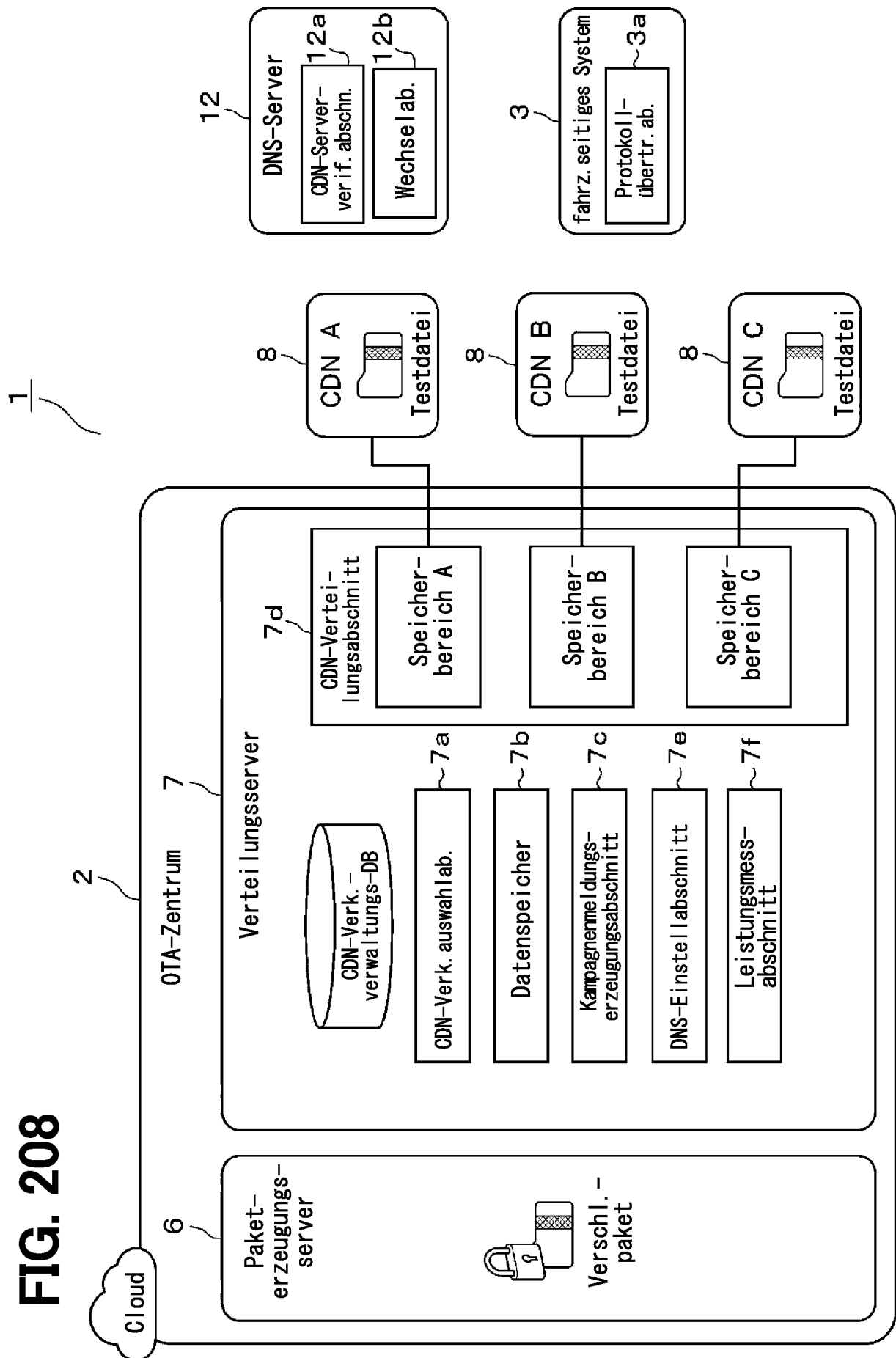


FIG. 209

Round-Robin-Aufzeichnung

vehicle.ota001 IN A 192.168.100.10
vehicle.ota001 IN A 192.168.100.11
vehicle.ota001 IN A 192.168.100.12

FIG. 210

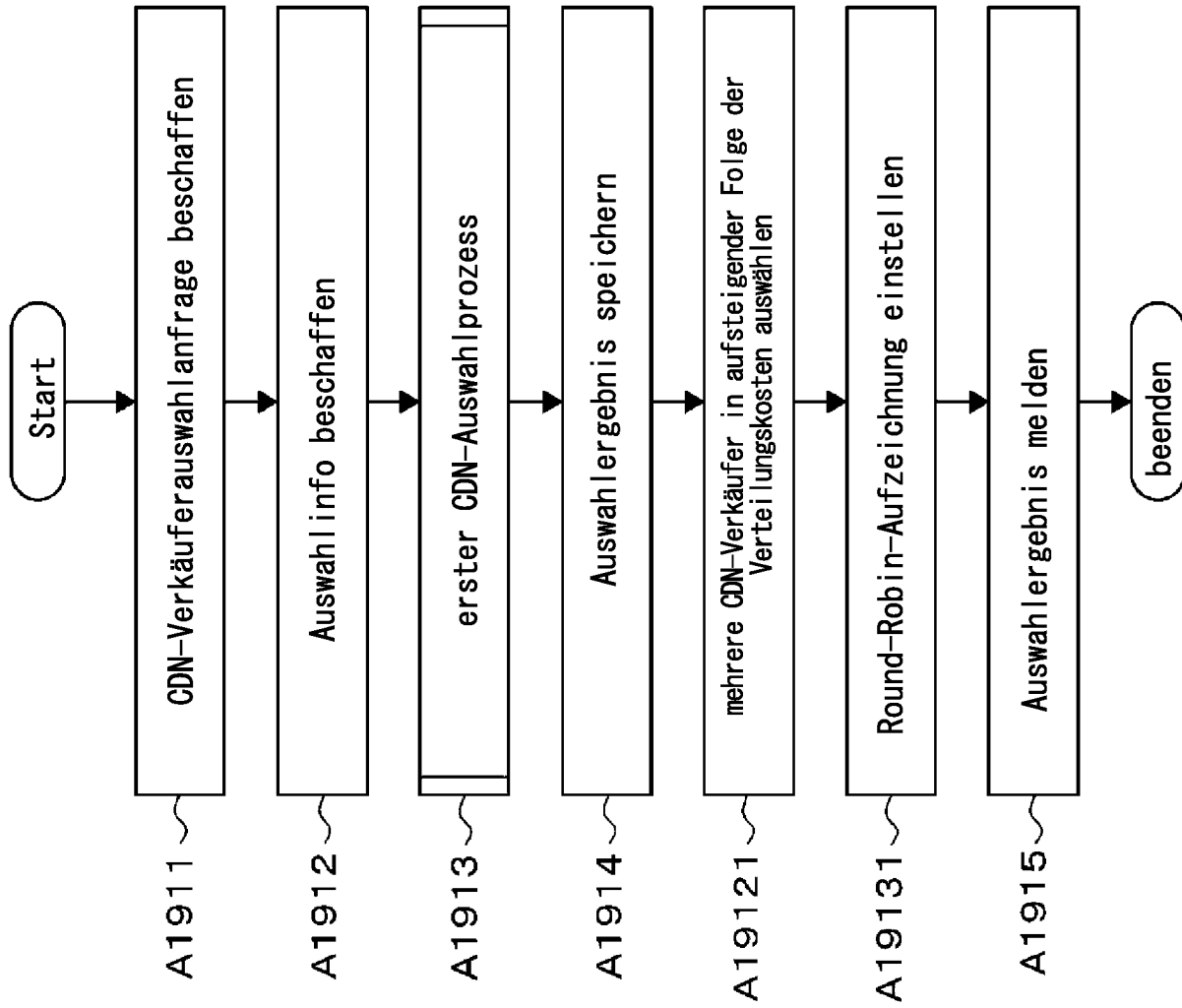


FIG. 211

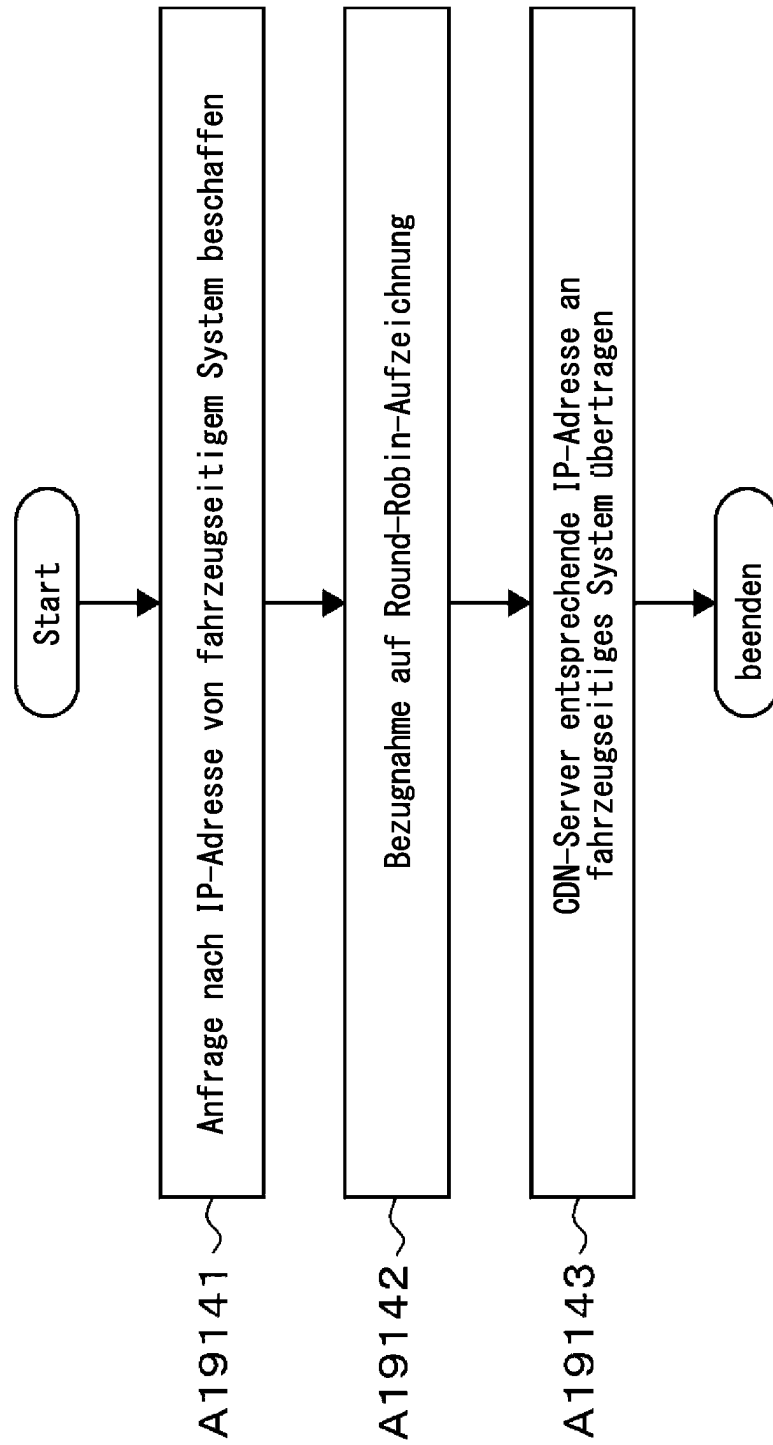


FIG. 212

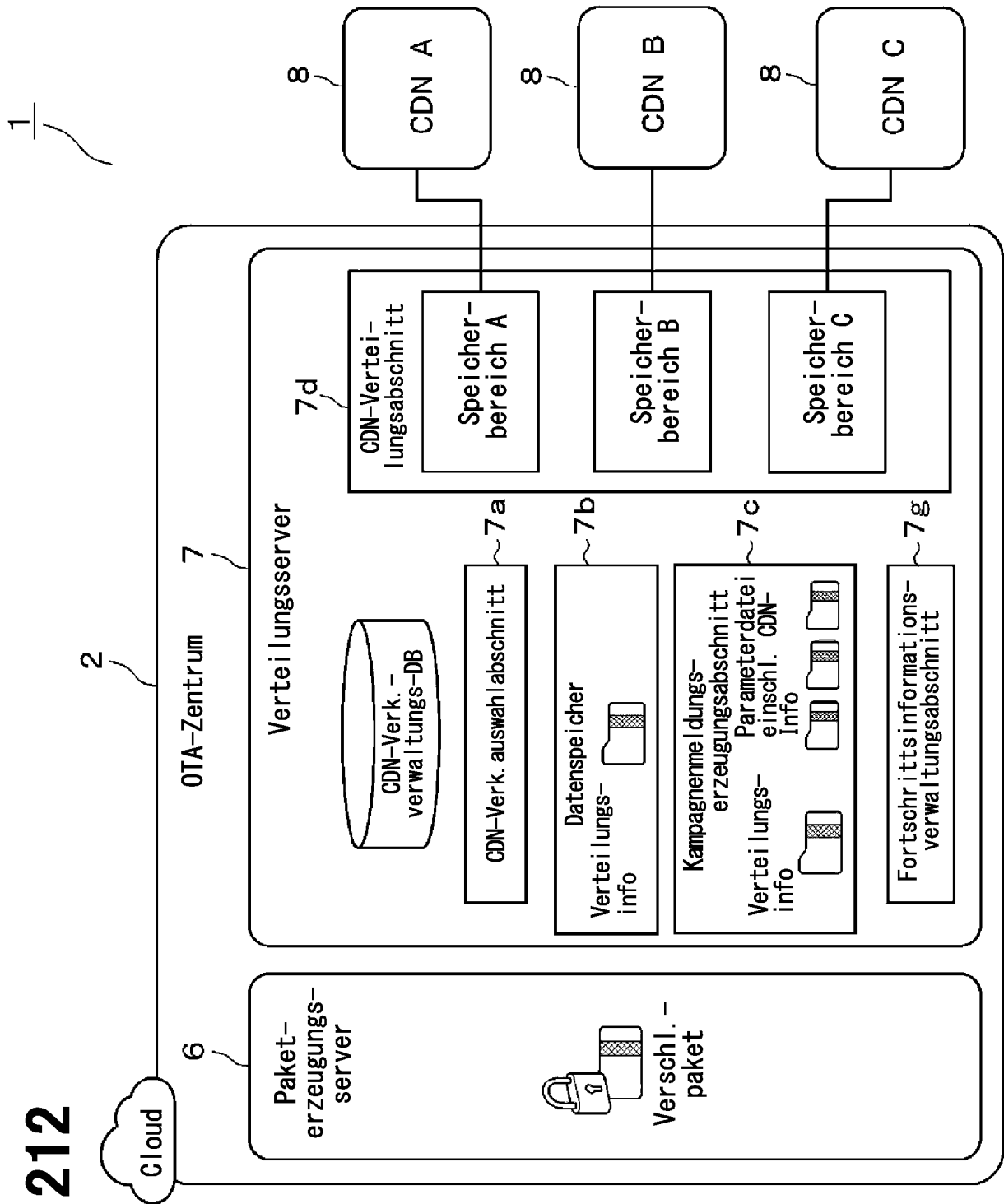


FIG. 213

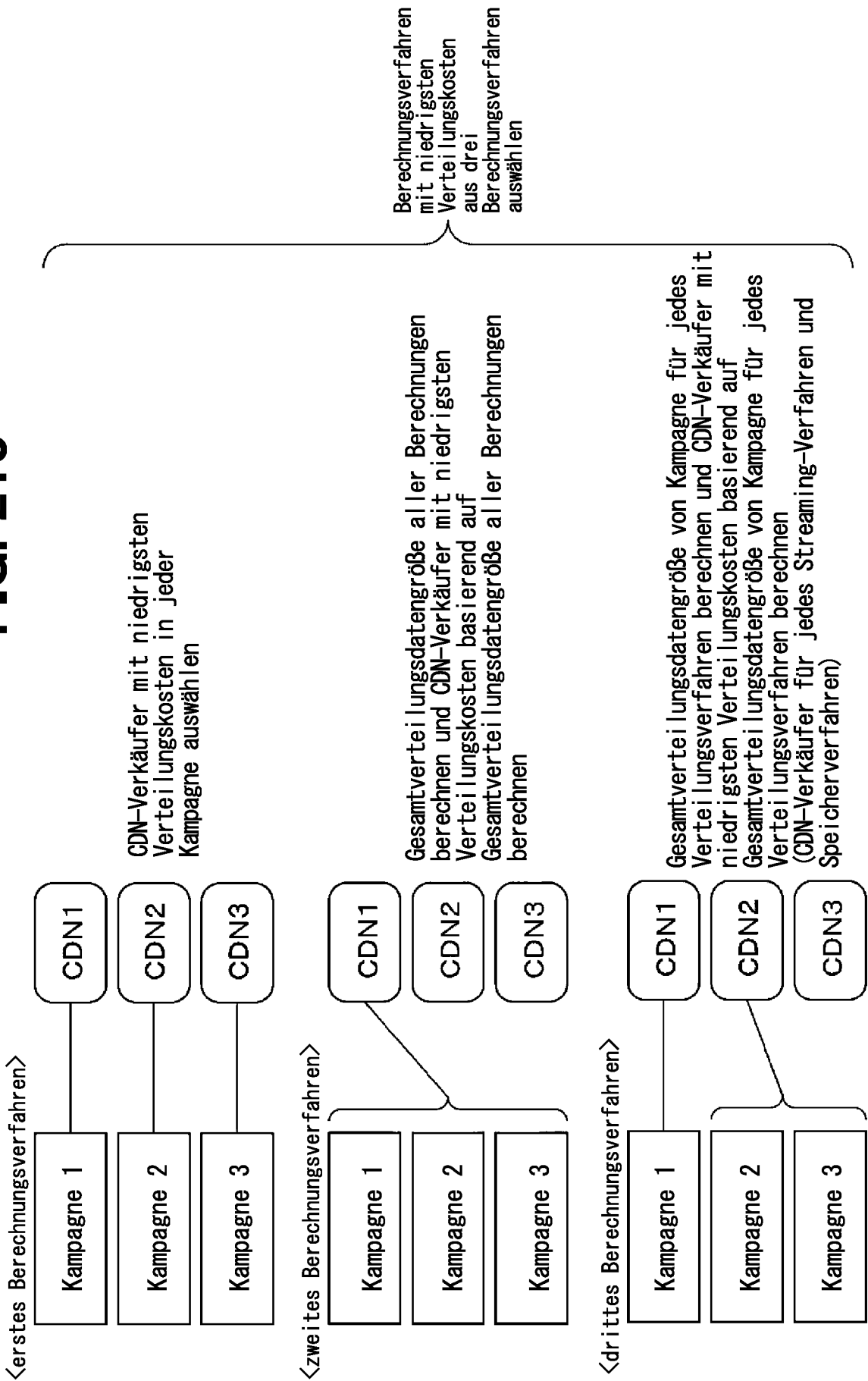


FIG. 214

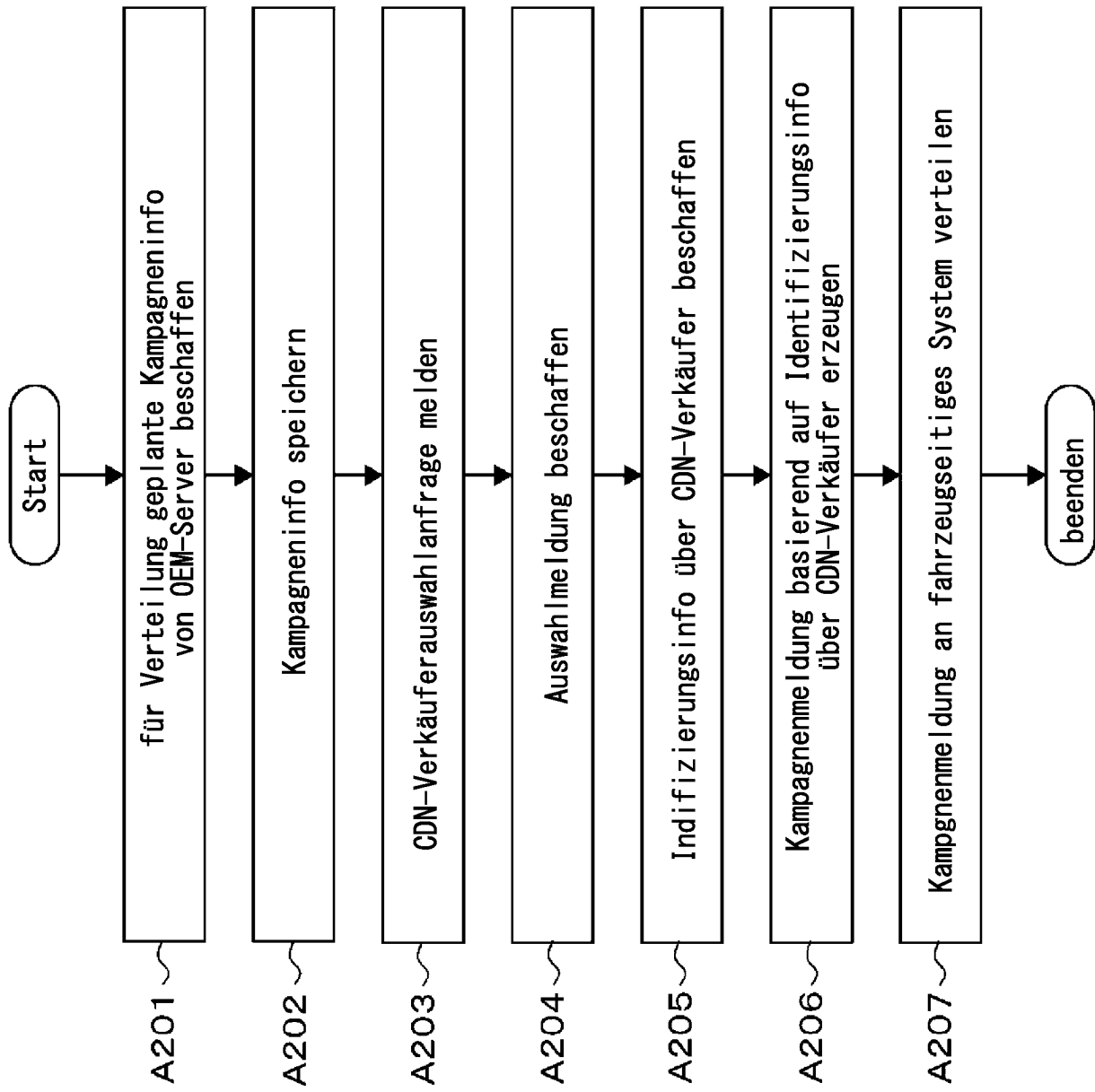


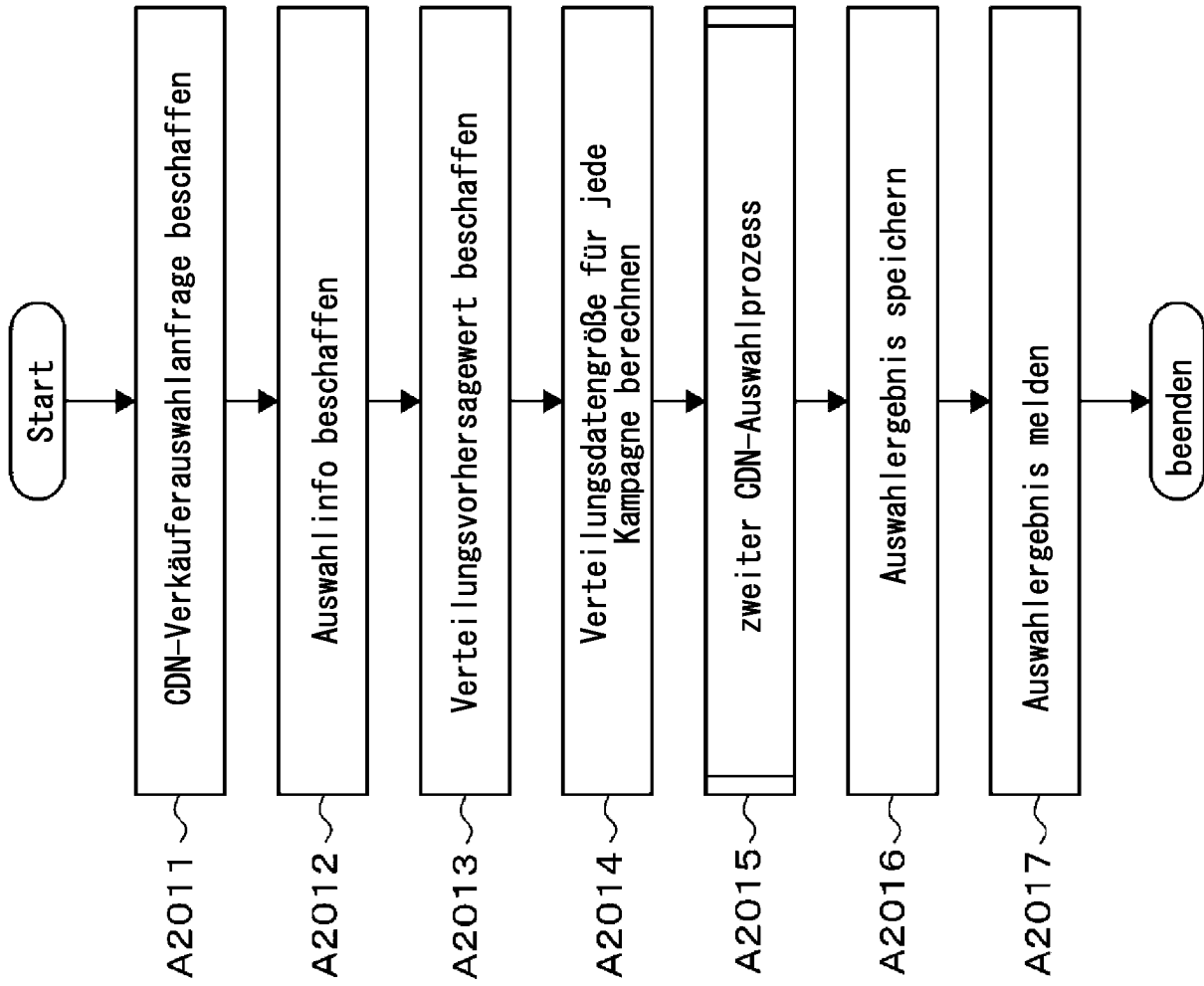
FIG. 215

FIG. 216

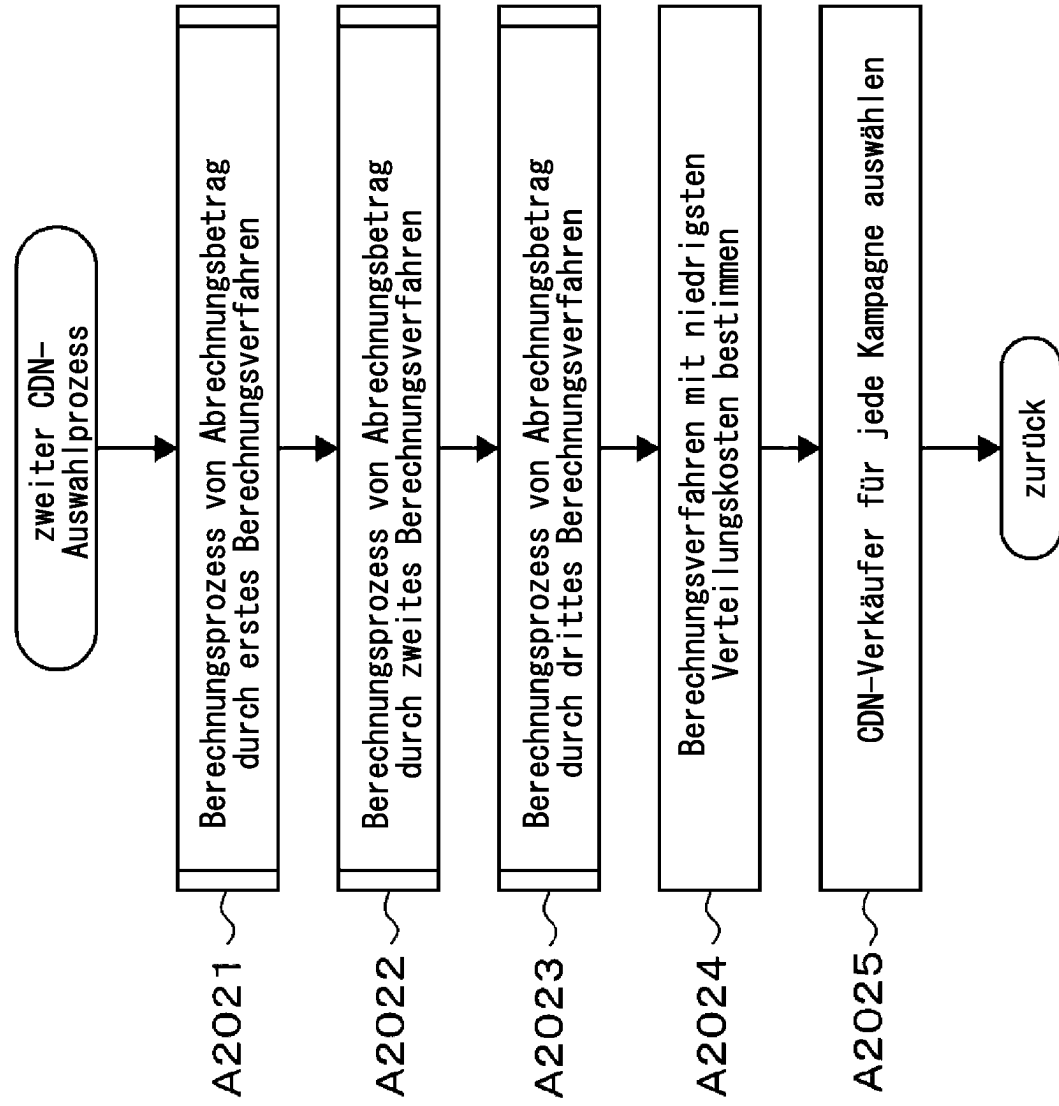


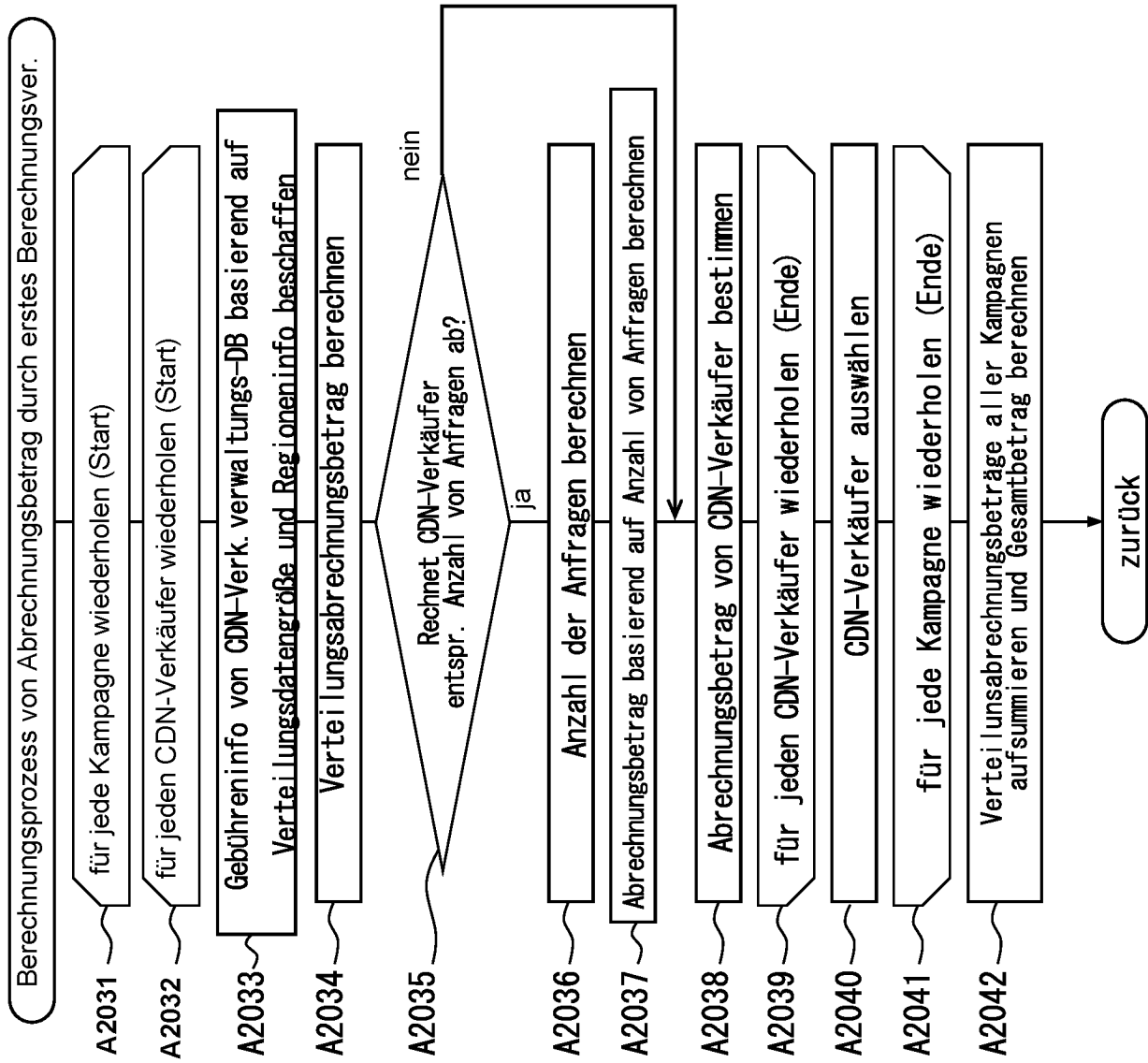
FIG. 217

FIG. 218

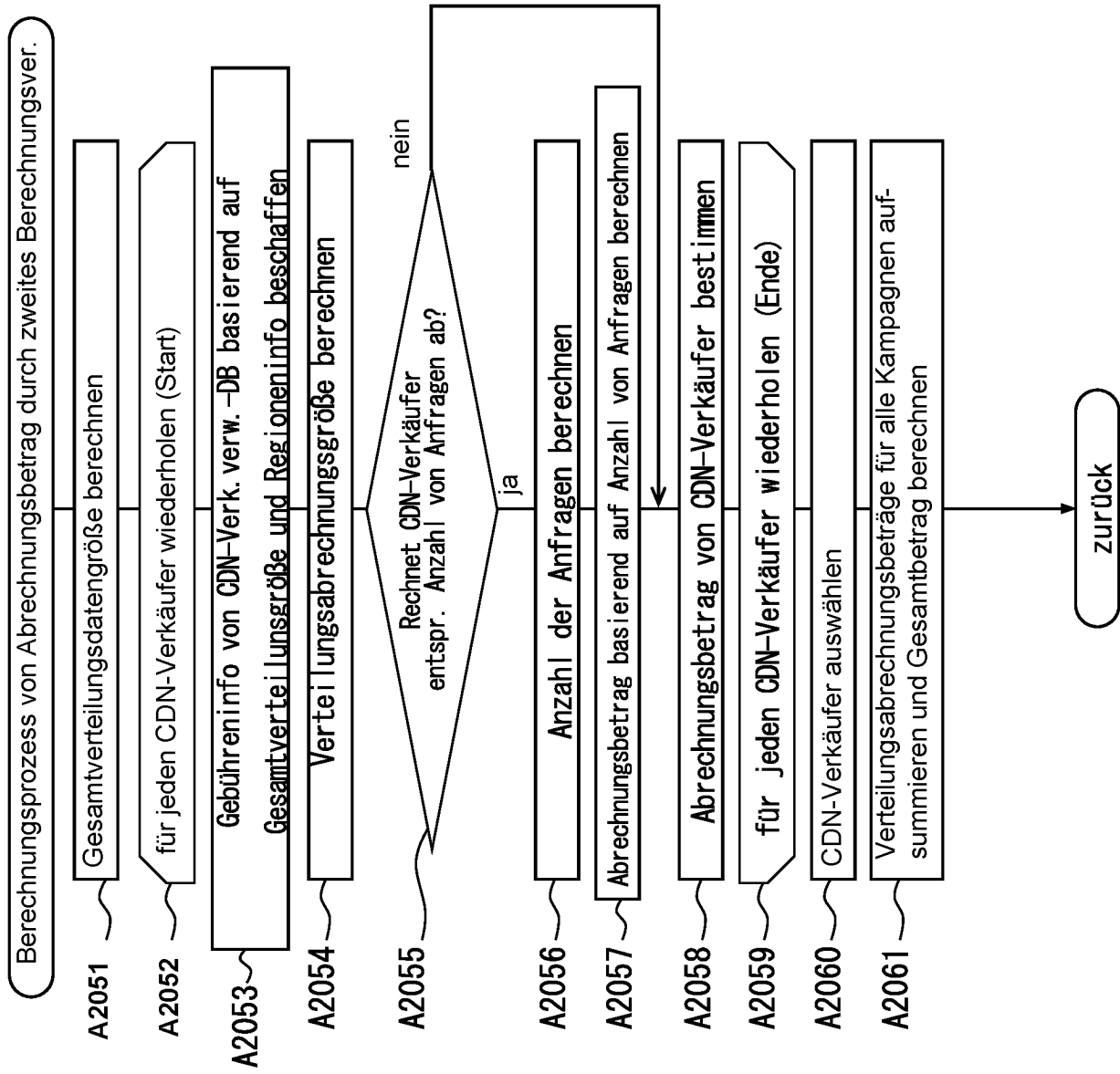


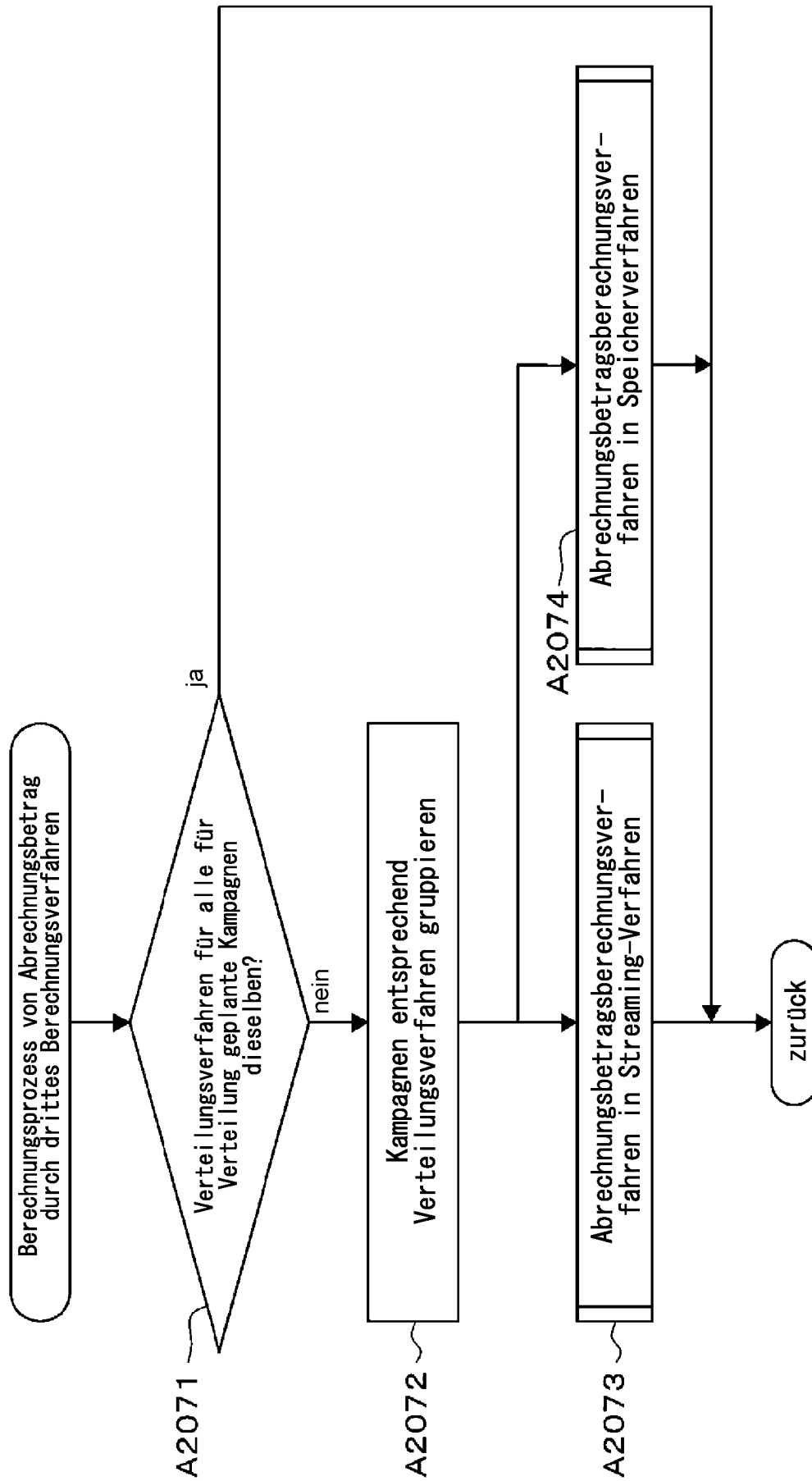
FIG. 219

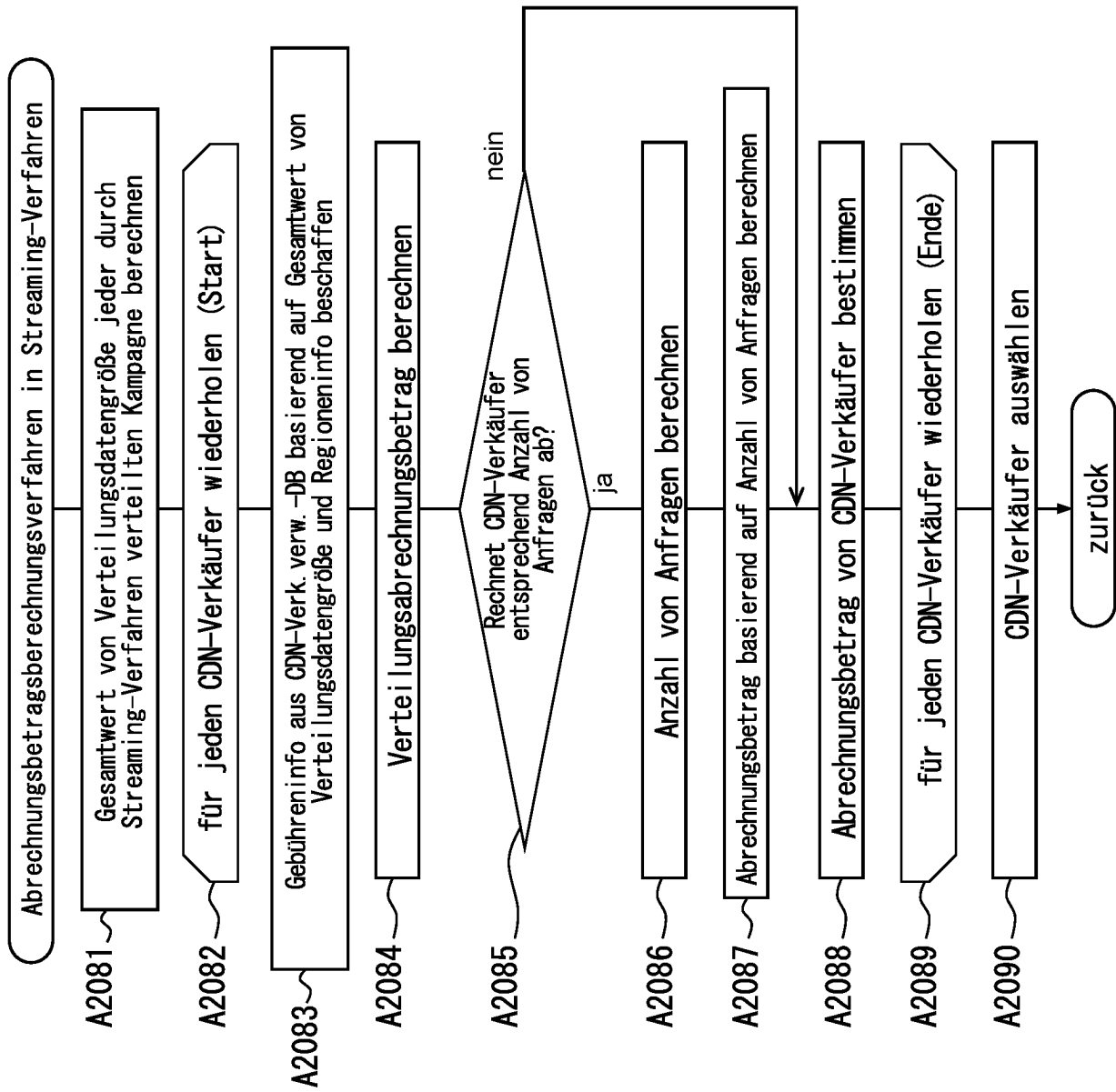
FIG. 220

FIG. 221

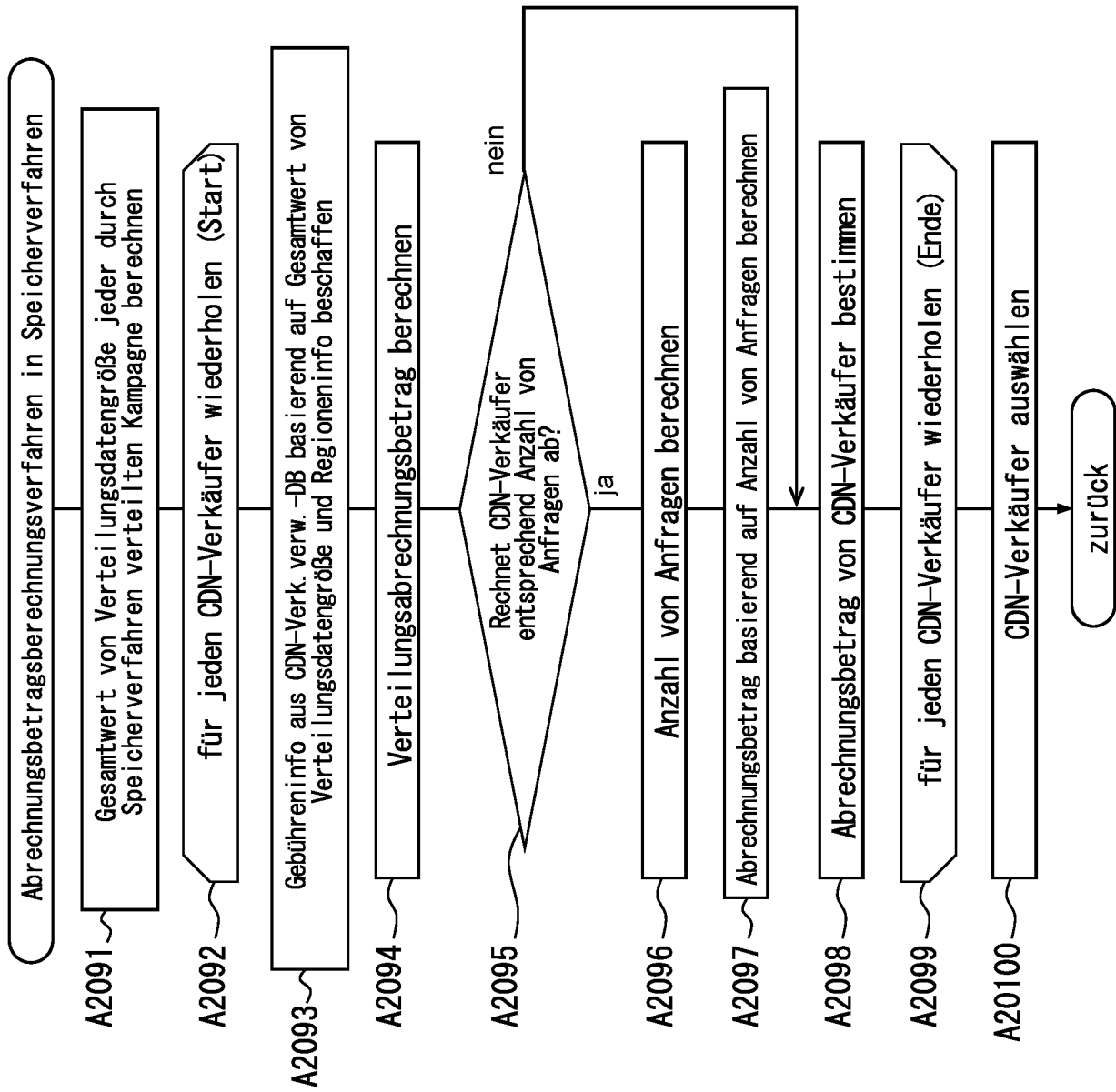


FIG. 222

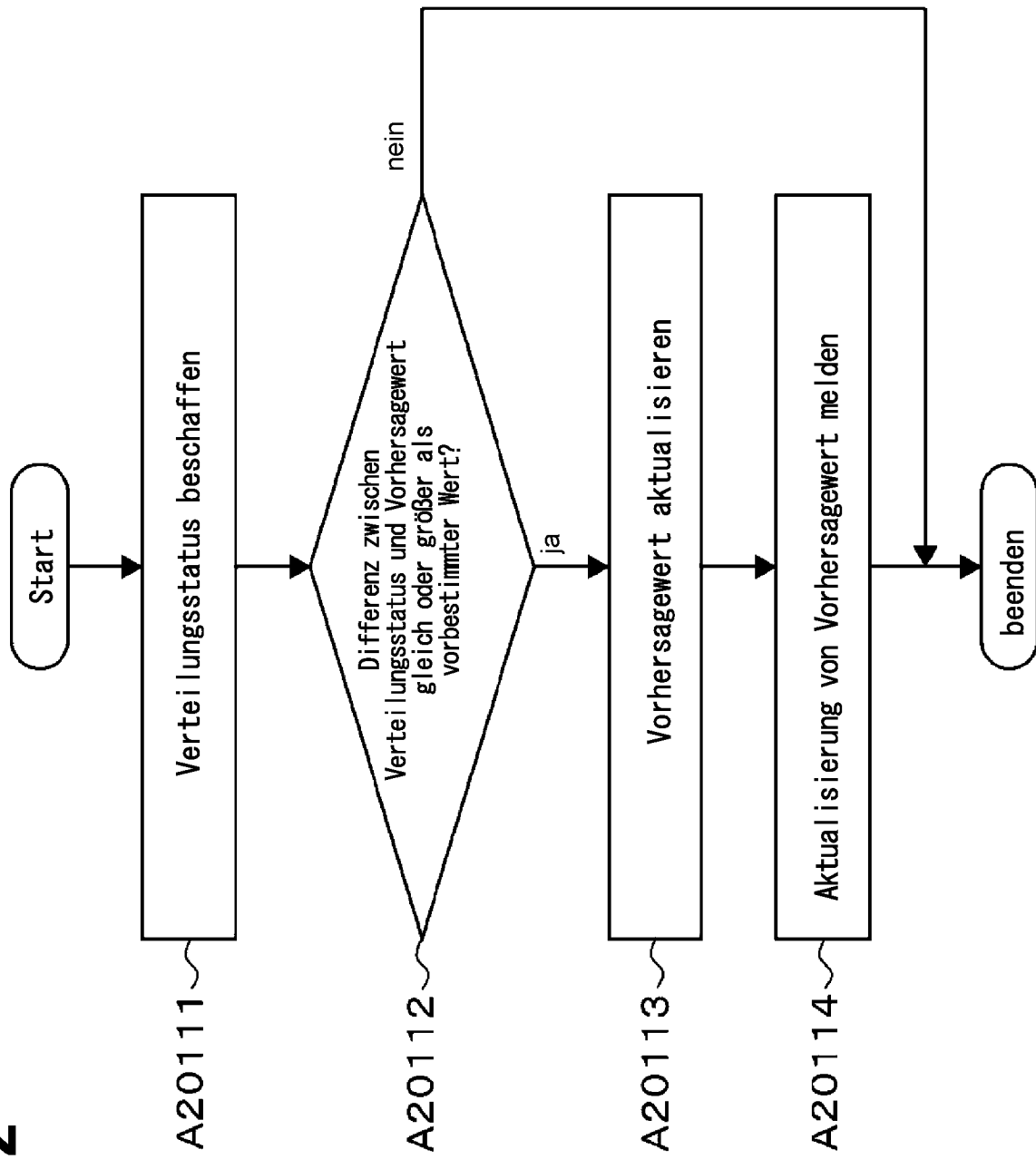


FIG. 223

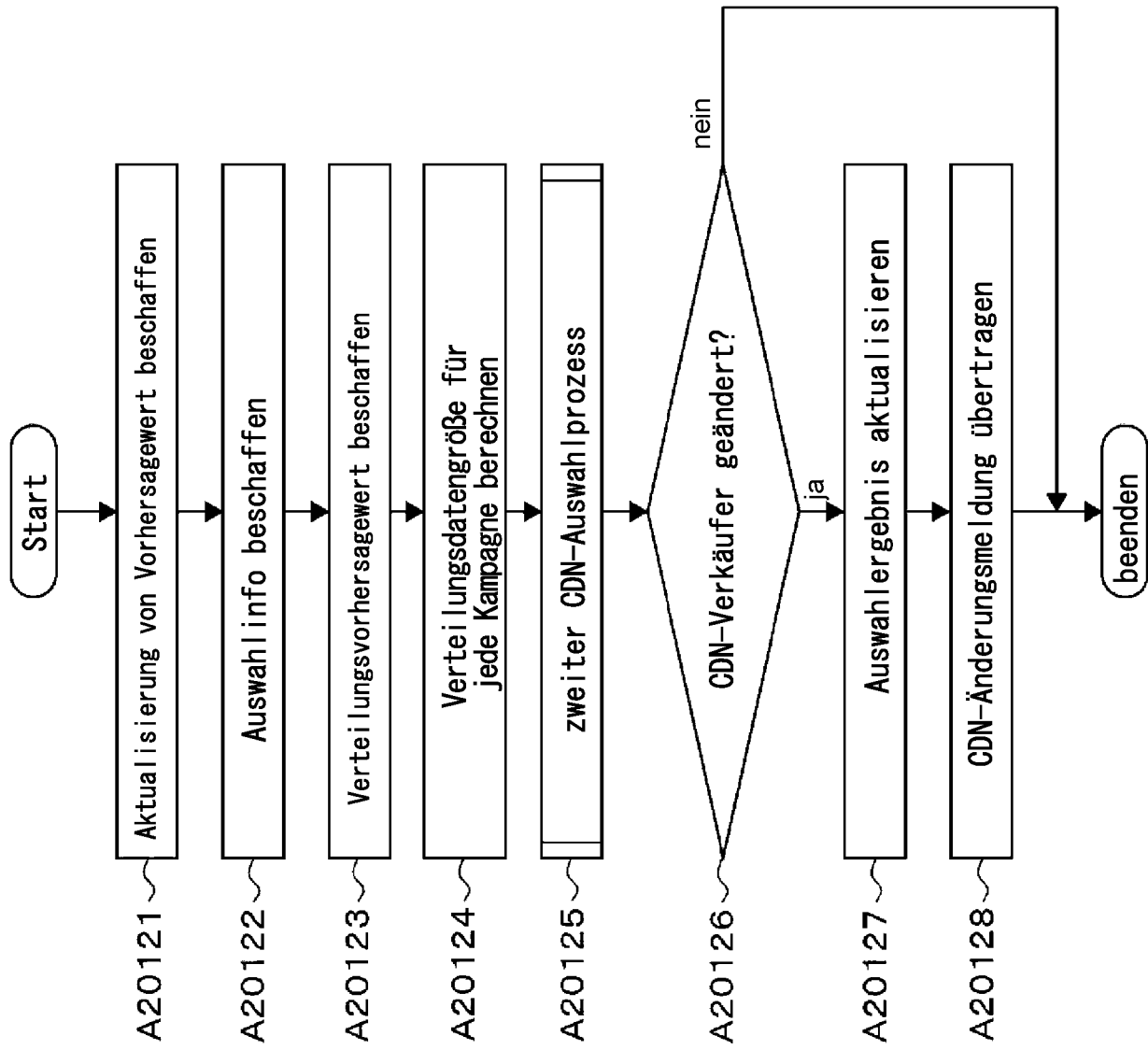


FIG. 224

