(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 118160272 A
(43)申请公布日 2024.06.07

(21)申请号 202280064999.9
(22)申请日 2022.06.22
(30)优先权数据
2021-161214 2021.09.30 JP
(85)PCT国际申请进入国家阶段日
2024.03.26
(86)PCT国际申请的申请数据
PCT/JP2022/024876 2022.06.22
(87)PCT国际申请的公布数据
WO2023/053622 JA 2023.04.06
(71)申请人 株式会社电装
地址 日本
(72)发明人 吉见英朗 安部真晃 东松古都
(74)专利代理机构 北京集佳知识产权代理有限公司 11227
专利代理师 金雪梅
(51)Int.Cl.
H04L 9/08(2006.01)
B60R 16/02(2006.01)
G06F 8/65(2006.01)
H04L 67/10(2006.01)

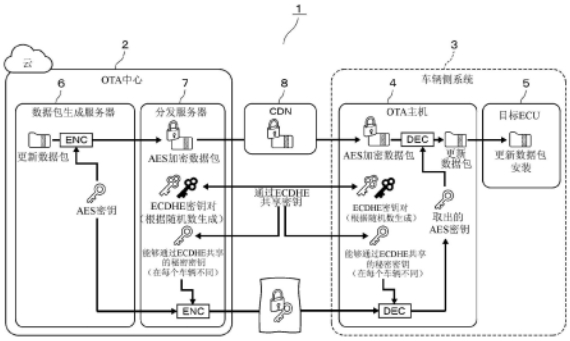
权利要求书3页 说明书44页 附图224页

(54)发明名称

数据通信系统、中心装置、主机装置以及秘密信息共享程序

(57)摘要

数据通信系统(1)具备将更新数据分发给主机装置的中心装置(2)、和将从中心装置下载的更新数据安装于重编对象的电子控制装置的主机装置(4)。中心装置以及主机装置的密钥配送采用迪菲-赫尔曼密钥共享(DHE)或者椭圆曲线迪菲-赫尔曼密钥共享(ECDHE)共享随机的秘密信息。中心装置基于该共享的秘密信息对用于加密更新数据的加密密钥进行加密,并将该已加密的加密密钥分发到主机装置。



CN 118160272 A

1.一种数据通信系统,具备中心装置(2)和主机装置(4),上述中心装置将更新数据分发给主机装置,上述主机装置将从上述中心装置下载的上述更新数据安装于重编对象的电子控制装置,其中,

上述中心装置以及上述主机装置的密钥配送采用迪菲-赫尔曼密钥共享(DHE)或者椭圆曲线迪菲-赫尔曼密钥共享(ECDHE)算法来共享随机的秘密信息,

上述中心装置基于该共享的秘密信息对用于加密更新数据的加密密钥进行加密,并将已加密的该加密密钥分发给上述主机装置。

2.一种数据通信系统,具备中心装置(2)和主机装置(4),上述中心装置将更新数据分发给主机装置,上述主机装置将从上述中心装置下载的上述更新数据安装于重编对象的电子控制装置,其中,

上述中心装置以及上述主机装置的密钥的配送采用迪菲-赫尔曼密钥共享(DHE)或者椭圆曲线迪菲-赫尔曼密钥共享(ECDHE)算法,

上述中心装置使用按照每个车辆型号或者按照每个车辆组共用的随机数作为用于DHE或者ECDHE的算法的秘密密钥来与上述主机装置共享秘密信息,并基于该共享的秘密信息对更新数据进行加密,

上述主机装置使用基于特定的规则的随机数作为用于DHE或者ECDHE的算法的秘密密钥来与上述中心装置共享秘密信息。

3.根据权利要求2所述数据通信系统,其中,

上述主机装置通过每个车辆型号的固定值、计数值、或者上述主机装置的软件版本的散列值的任意一个,或者它们的组合构成用于DHE或者ECDHE的算法的秘密密钥的特定的规则。

4.根据权利要求1~3中任意一项所述数据通信系统,其中,

上述中心装置在DHE或者ECDHE的密钥共享时,对发送给上述中心装置的密钥附加基于公开密钥加密的数字签名。

5.根据权利要求4所述数据通信系统,其中,

上述中心装置使用利用了RSA或者椭圆曲线DSA的加密算法的数字签名,作为上述数字签名。

6.一种中心装置,是将更新数据分发给主机装置的中心装置(2),其中,

密钥的配送采用迪菲-赫尔曼密钥共享(DHE)或者椭圆曲线迪菲-赫尔曼密钥共享(ECDHE)算法来与上述主机装置共享随机的秘密信息,基于该共享的秘密信息对用于加密更新数据的加密密钥进行加密,并将该的加密密钥分发给上述主机装置。

7.一种中心装置,是将更新数据分发给主机装置的中心装置(2),其中,

密钥的配送采用迪菲-赫尔曼密钥共享(DHE)或者椭圆曲线迪菲-赫尔曼密钥共享(ECDHE)算法,使用按照每个车辆型号或者按照每个车辆组共用的随机数作为用于DHE或者ECDHE的算法的秘密密钥来与上述主机装置共享秘密信息,并基于该共享的秘密信息对更新数据进行加密。

8.一种主机装置,是将从中心装置下载的更新数据安装于重编对象的电子控制装置的主机装置(4),其中,

密钥的配送采用迪菲-赫尔曼密钥共享(DHE)或者椭圆曲线迪菲-赫尔曼密钥共享

(ECDHE)算法来与上述中心装置共享随机的秘密信息。

9.一种主机装置,是将从中心装置下载的更新数据安装于重编对象的电子控制装置的主机装置(4),其中,

密钥的配送采用迪菲-赫尔曼密钥共享(DHE)或者椭圆曲线迪菲-赫尔曼密钥共享(ECDHE)算法,使用基于特定的规则的随机数作为用于DHE或者ECDHE的算法的秘密密钥来与上述中心装置共享秘密信息。

10.一种秘密信息共享程序,其中,

使将更新数据分发给主机装置的中心装置(2)执行:

秘密信息共享步骤,密钥的配送采用迪菲-赫尔曼密钥共享(DHE)或者椭圆曲线迪菲-赫尔曼密钥共享(ECDHE)算法来与上述主机装置共享随机的秘密信息;以及

加密密钥分发步骤,基于该共享的秘密信息对用于加密更新数据的加密密钥进行加密,并将该的加密密钥分发给上述主机装置。

11.一种秘密信息共享程序,其中,

使将更新数据分发给主机装置的中心装置(2)执行:

秘密信息共享步骤,密钥的配送采用迪菲-赫尔曼密钥共享(DHE)或者椭圆曲线迪菲-赫尔曼密钥共享(ECDHE)算法,使用按照每个车辆型号或者按照每个车辆组共用的随机数作为用于DHE或者ECDHE的算法的秘密密钥来与上述主机装置共享秘密信息;以及

加密密钥分发步骤,基于该共享的秘密信息对更新数据进行加密。

12.一种秘密信息共享程序,其中,

使将从中心装置下载的更新数据安装于重编对象的电子控制装置的主机装置(4)执行:

秘密信息共享步骤,密钥的配送采用迪菲-赫尔曼密钥共享(DHE)或者椭圆曲线迪菲-赫尔曼密钥共享(ECDHE)算法来与上述中心装置共享随机的秘密信息。

13.一种秘密信息共享程序,其中,

使将从中心装置下载的更新数据安装于重编对象的电子控制装置的主机装置(4)执行:

秘密信息共享步骤,密钥的配送采用迪菲-赫尔曼密钥共享(DHE)或者椭圆曲线迪菲-赫尔曼密钥共享(ECDHE)算法,使用基于特定的规则的随机数作为用于DHE或者ECDHE的算法的秘密密钥来与上述中心装置共享秘密信息。

14.一种数据通信系统,具备中心装置(2)、存储介质、以及主机装置(4),上述中心装置将更新数据分发给上述存储介质,上述主机装置将从上述存储介质读出的上述更新数据安装于重编对象的电子控制装置,其中,

上述中心装置以及上述主机装置的密钥配送采用迪菲-赫尔曼密钥共享(DHE)或者椭圆曲线迪菲-赫尔曼密钥共享(ECDHE)算法,

上述中心装置使用第一随机数作为用于DHE或者ECDHE的算法的秘密密钥,经由上述存储介质与上述主机装置共享秘密信息,并使用该共享的秘密信息对更新数据进行加密,

上述主机装置使用第二随机数作为用于DHE或者ECDHE的算法的秘密密钥,并经由上述存储介质与上述中心装置共享秘密信息。

15.根据权利要求14所述的数据通信系统,其中,

上述中心装置通过加密密钥对更新数据进行加密,基于上述共享的秘密信息对上述加密密钥进行加密,并将进行了上述加密的加密密钥分发给上述主机装置。

16.根据权利要求14所述的数据通信系统,其中,

上述中心装置使用上述共享的秘密信息作为加密密钥对更新数据进行加密。

17.根据权利要求14所述的数据通信系统,其中,

第一随机数以及第二随机数分别为随机的随机数。

18.根据权利要求14所述的数据通信系统,其中,

第一随机数是按照每个车辆型号或者按照每个车辆组共用的随机数,

第二随机数是基于特定的规则的随机数。

19.根据权利要求14所述的数据通信系统,其中,

上述主机装置将基于上述算法的上述主机装置的密钥保存于上述存储介质,

上述中心装置从上述存储介质上传上述保存的主机装置的密钥,

上述中心装置将基于上述算法的上述中心装置的密钥保存于上述存储介质,

上述主机装置从上述存储介质接收上述保存的中心装置的密钥。

20.根据权利要求14所述的数据通信系统,其中,

上述主机装置不与上述中心装置进行无线通信,而经由上述存储介质共享基于上述算法的秘密信息。

数据通信系统、中心装置、主机装置以及秘密信息共享程序

[0001] 相关申请的交叉引用

[0002] 本申请主张于2021年9月30日申请的日本申请编号2021－161214的优先权,并在此引用其全部内容。

技术领域

[0003] 本公开涉及数据通信系统、中心装置、主机装置以及秘密信息共享程序。

背景技术

[0004] 近年来,随着驾驶辅助功能、自动驾驶功能等车辆控制的多样化,搭载于电子控制装置(以下,称为ECU(Electronic Control Unit))的车辆控制、诊断等应用程序的规模增大。另外,随着功能改善等所带来的升级,重编ECU的应用程序的机会也增加。重编也有称为程序更新的情况。另一方面,随着通信网络的发展等,联网汽车的技术也普及。根据这样的情况,例如在专利文献1公开了通过OTA(Over The Air:空中下载)的技术从中心装置向车辆侧的主机装置分发对更新数据进行了打包的更新数据包的技术。主机装置是总括ECU的应用程序的重编的装置。从中心装置向主机装置分发的更新数据例如包含自动驾驶、先进驾驶辅助系统(ADAS(Advanced Driver-Assistance Systems))、多媒体等的应用程序、数据。

[0005] 专利文献1:日本特开2020－276424号公报

[0006] 由于在中心装置与主机装置之间共享更新数据包的加密密钥的密钥配送使用RSA(Rivest-Shamir-Adleman cryptosystem:里维斯特-沙米尔-阿德曼密码系统)的情况下不能够确保加密密钥的前向保密性,而不推荐RSA的利用作为密钥共享的加密算法。作为RSA的代替方法推荐能够确保前向保密性的迪菲-赫尔曼密钥共享(以下,称为DHE(Diffie-Hellman key exchange))或者椭圆曲线迪菲-赫尔曼密钥共享(以下,称为ECDHE(Elliptic curve Diffie-Hellman key exchange))。

[0007] 然而,DHE、ECDHE也根据在中心装置和主机装置双方生成的随机数生成共享密钥的种子,能够共享密钥的加密密钥成为按照每个车辆随机的密钥值。因此,若通过该加密密钥对更新数据包进行加密,则按照车辆成为不同的已加密的更新数据包,例如不会在按照车辆型号、特定的车辆组划分的组成为同一更新数据包。其结果,不能够实现基于内容分发网络(以下,称为CDN(Content Delivery Network))的更新数据包的高效的分发。

发明内容

[0008] 本公开的目的在于在适当地确保前向保密性的同时,适当地实现基于CDN的更新数据的高效的分发。

[0009] 根据本公开的一方式,具备将更新数据分发给主机装置的中心装置、和将从中心装置下载的更新数据安装于重编对象的电子控制装置的主机装置。中心装置以及主机装置的密钥配送采用迪菲-赫尔曼密钥共享(DHE)或者椭圆曲线迪菲-赫尔曼密钥共享(ECDHE)

共享随机的秘密信息。中心装置基于该共享的秘密信息对用于加密更新数据的加密密钥进行加密,并将该已加密的加密密钥分发到主机装置。

[0010] 在中心装置以及主机装置中,密钥的配送采用DHE或者ECDHE的算法来共享随机的秘密信息。在中心装置中,构成为基于该共享的秘密信息对用于加密更新数据的加密密钥进行加密,并将该已加密的加密密钥分发给主机装置。密钥的配送采用DHE或者ECDHE的算法,在中心装置与主机装置共享秘密信息,从而能够在适当地确保前向保密性的同时,适当地实现基于CDN的更新数据的高效的分发。

[0011] 根据本公开的一方式,具备将更新数据分发给主机装置的中心装置、和将从中心装置下载的更新数据安装于重编对象的电子控制装置的主机装置。中心装置以及主机装置的密钥的配送采用迪菲-赫尔曼密钥共享(DHE)或者椭圆曲线迪菲-赫尔曼密钥共享(ECDHE)。中心装置使用按照每个车辆型号或者按照每个车辆组共用的随机数作为DHE或者ECDHE的算法所使用的秘密密钥来与主机装置共享秘密信息,并基于该共享的秘密信息对更新数据进行加密。主机装置使用基于特定的规则的随机数作为DHE或者ECDHE的算法所使用的秘密密钥来与中心装置共享秘密信息。

[0012] 在中心装置以及主机装置中,密钥的配送采用DHE或者ECDHE的算法。构成为在中心装置中,使用按照每个车辆型号或者按照每个车辆组共用的随机数作为DHE或者ECDHE的算法所使用的秘密密钥来与主机装置共享秘密信息,并基于该共享的秘密信息对更新数据进行加密。在主机装置中,使用基于特定的规则的随机数作为DHE或者ECDHE的算法所使用的秘密密钥来与中心装置共享秘密信息。密钥的配送采用DHE或者ECDHE的算法,并在中心装置和主机装置共享秘密信息,从而能够在适当地确保前向保密性的同时,适当地实现基于CDN的更新数据的高效的分发。

附图说明

[0013] 在参照附图的同时通过下述的详细的记述,本发明的上述目的以及其它的目的、特征、优点变得更明确。该附图为如下。

[0014] 图1是表示第一实施方式的系统整体中的处理的流程的图,

[0015] 图2是OTA中心以及OTA主机的功能框图,

[0016] 图3是说明CTR模式的加密处理的图,

[0017] 图4是说明CTR模式的解密处理的图,

[0018] 图5是表示CBC模式与CTR模式的优点以及缺点的比较的图,

[0019] 图6是表示CBC模式与CTR模式的吞吐量的比较的图,

[0020] 图7是说明CBC模式的解密处理的图,

[0021] 图8是说明CTR模式的解密处理的图,

[0022] 图9是表示OTA中心的处理的图,

[0023] 图10是表示中心的处理的图,

[0024] 图11是表示OTA中心的处理的图,

[0025] 图12是表示OTA主机的处理的图,

[0026] 图13是表示OTA主机的处理的图,

[0027] 图14是表示OTA主机的处理的图,

[0028] 图15是说明第二实施方式的OFB模式的加密处理的图，

[0029] 图16是说明OFB模式的解密处理的图，

[0030] 图17是表示CBC模式与OFB模式的优点以及缺点的比较的图，

[0031] 图18是表示CBC模式与OFB模式的吞吐量的比较的图，

[0032] 图19是说明CTR模式的解密处理的图，

[0033] 图20是说明OFB模式的解密处理的图，

[0034] 图21是表示OTA中心的处理的图，

[0035] 图22是表示OTA中心的处理的图，

[0036] 图23是表示OTA中心的处理的图，

[0037] 图24是表示OTA主机的处理的图，

[0038] 图25是表示OTA主机的处理的图，

[0039] 图26是表示OTA主机的处理的图，

[0040] 图27是表示第三实施方式的系统整体中的处理的流程的图，

[0041] 图28是表示OTA中心的处理的图，

[0042] 图29是表示OTA中心的处理的图，

[0043] 图30是表示OTA中心的处理的图，

[0044] 图31是表示OTA主机的处理的图，

[0045] 图32是表示OTA主机的处理的图，

[0046] 图33是表示OTA主机的处理的图，

[0047] 图34是表示第四实施方式的系统整体中的处理的流程的图，

[0048] 图35是OTA中心以及OTA主机的功能框图，

[0049] 图36是表示OTA主机的处理的图，

[0050] 图37是表示OTA主机的处理的图，

[0051] 图38是表示OTA主机的处理的图，

[0052] 图39是表示第五实施方式的OTA主机的处理的图，

[0053] 图40是表示OTA主机的处理的图，

[0054] 图41是表示OTA主机的处理的图，

[0055] 图42是表示存储器容量与访问速度的关系的图，

[0056] 图43是表示第六实施方式的系统整体中的处理的流程的图，

[0057] 图44是OTA中心以及OTA主机的功能框图，

[0058] 图45是表示发送RP元数据的方式的图，

[0059] 图46是表示RP元数据的构成的图，

[0060] 图47是表示RP元数据的构成的图，

[0061] 图48是表示OTA中心的处理的图，

[0062] 图49是表示OTA中心的处理的图，

[0063] 图50是表示OTA中心的处理的图，

[0064] 图51是表示OTA中心的处理的图，

[0065] 图52是表示OTA主机的处理的图，

[0066] 图53是表示OTA主机的处理的图，

[0067] 图54是表示OTA主机的处理的图，

[0068] 图55是表示第七实施方式的系统整体中的处理的流程的图，

[0069] 图56是CCMP模式的功能，

[0070] 图57是说明基于CCMP模式的吞吐量的估计的图，

[0071] 图58是现有方式的功能框图，

[0072] 图59是说明基于现有方式的吞吐量的估计的图，

[0073] 图60是表示CCMP模式与现有方式的吞吐量的比较的图，

[0074] 图61是OTA中心以及OTA主机的功能框图，

[0075] 图62是表示OTA中心的处理的图，

[0076] 图63是表示OTA中心的处理的图，

[0077] 图64是表示OTA中心的处理的图，

[0078] 图65是表示OTA主机的处理的图，

[0079] 图66是表示OTA主机的处理的图，

[0080] 图67是表示OTA主机的处理的图，

[0081] 图68是表示第八实施方式的系统整体中的处理的流程的图,图69是GCMP模式的功能框图，

[0082] 图70是说明基于GCMP模式的吞吐量的估计的图，

[0083] 图71是表示GCMP模式与现有方式的吞吐量的比较的图，

[0084] 图72是表示OTA中心的处理的图，

[0085] 图73是表示OTA中心的处理的图，

[0086] 图74是表示OTA中心的处理的图，

[0087] 图75是表示OTA主机的处理的图，

[0088] 图76是表示OTA主机的处理的图，

[0089] 图77是表示OTA主机的处理的图，

[0090] 图78是表示第九实施方式的系统整体中的处理的流程的图，

[0091] 图79是表示OTA中心的处理的图，

[0092] 图80是表示OTA中心的处理的图，

[0093] 图81是表示OTA中心的处理的图，

[0094] 图82是表示OTA中心的处理的图，

[0095] 图83是表示OTA主机的处理的图，

[0096] 图84是表示OTA主机的处理的图，

[0097] 图85是表示OTA主机的处理的图，

[0098] 图86是表示OTA主机的处理的图，

[0099] 图87是表示第十实施方式的系统整体中的处理的流程的图，

[0100] 图88是表示CDN的成本比较的图，

[0101] 图89是表示CDN的成本比较的图，

[0102] 图90是表示各云服务的CDN价格表格的图，

[0103] 图91是表示各云服务运营商的储存方式的价格表格的图，

[0104] 图92是表示云服务运营商的流式传输方式中的每个流式传输大小的价格表格的

图，

[0105] 图93是表示各云服务运营商的流式传输方式中的每个流式传输大小的价格表格的图，

[0106] 图94是OTA中心以及OTA主机的功能框图，

[0107] 图95是表示OTA中心的处理的图，

[0108] 图96是表示OTA中心的处理的图，

[0109] 图97是表示OTA中心的处理的图，

[0110] 图98是表示OTA中心的处理的图，

[0111] 图99是表示第十一实施方式的系统整体中的处理的流程的图，

[0112] 图100是表示能够通过DHE或者ECDHE共享密钥的公用密钥的图，

[0113] 图101是表示OTA中心的处理的图，

[0114] 图102是表示OTA中心的处理的图，

[0115] 图103是表示OTA中心的处理的图，

[0116] 图104是表示OTA中心的处理的图，

[0117] 图105是表示OTA主机的处理的图，

[0118] 图106是表示OTA主机的处理的图，

[0119] 图107是表示OTA主机的处理的图，

[0120] 图108是表示OTA主机的处理的图，

[0121] 图109是表示第十二实施方式的系统整体中的处理的流程的图，

[0122] 图110是表示OTA中心的处理的图，

[0123] 图111是表示OTA中心的处理的图，

[0124] 图112是表示OTA中心的处理的图，

[0125] 图113是表示OTA主机的处理的图，

[0126] 图114是表示OTA主机的处理的图，

[0127] 图115是表示OTA主机的处理的图，

[0128] 图116是表示第十三实施方式的系统整体中的处理的流程的图，

[0129] 图117是说明CTR模式的加密处理的图，

[0130] 图118是说明CTR模式的解密处理的图，

[0131] 图119是表示OTA中心的处理的图，

[0132] 图120是表示OTA中心的处理的图，

[0133] 图121是表示OTA中心的处理的图，

[0134] 图122是表示OTA主机的处理的图，

[0135] 图123是表示OTA主机的处理的图，

[0136] 图124是表示OTA主机的处理的图，

[0137] 图125是表示第十四实施方式的系统整体中的处理的流程的图，

[0138] 图126是说明AES专用密钥的图，

[0139] 图127是表示OTA中心的处理的图，

[0140] 图128是表示OTA中心的处理的图，

[0141] 图129是表示OTA中心的处理的图，

[0142] 图130是表示OTA主机的处理的图，

[0143] 图131是表示OTA主机的处理的图，

[0144] 图132是表示OTA主机的处理的图，

[0145] 图133是表示第十五实施方式的系统整体中的处理的流程的图，

[0146] 图134是表示OTA中心的处理的图，

[0147] 图135是表示OTA中心的处理的图，

[0148] 图136是表示OTA主机的处理的图，

[0149] 图137是表示OTA主机的处理的图，

[0150] 图138是表示第十六实施方式的系统整体中的处理的流程的图，

[0151] 图139是表示来自中间攻击者的攻击的图，

[0152] 图140是表示附加数字签名的方式的图，

[0153] 图141是表示OTA中心的处理的图，

[0154] 图142是表示OTA中心的处理的图，

[0155] 图143是表示OTA中心的处理的图，

[0156] 图144是表示OTA主机的处理的图，

[0157] 图145是表示OTA主机的处理的图，

[0158] 图146是表示第十七实施方式的系统整体中的处理的流程的图，

[0159] 图147是表示OTA中心的处理的图，

[0160] 图148是表示OTA中心的处理的图，

[0161] 图149是表示OTA主机的处理的图，

[0162] 图150是表示OTA主机的处理的图，

[0163] 图151是表示OTA主机的处理的图，

[0164] 图152是表示第十八实施方式的系统整体中的处理的流程的图，

[0165] 图153是表示各云服务的CDN价格表格的图，

[0166] 图154是表示各云服务的CDN价格表格的图，

[0167] 图155是表示各云服务运营商的储存方式的价格表格的图，

[0168] 图156是表示各云服务运营商的储存方式的价格表格的图，

[0169] 图157是表示各云服务运营商的流式传输方式中的每个流式传输大小的价格表格的图，

[0170] 图158是表示各云服务运营商的流式传输方式中的每个流式传输大小的价格表格的图，

[0171] 图159是表示各云服务运营商的流式传输方式中的每个流式传输大小的价格表格的图，

[0172] 图160是表示各云服务运营商的流式传输方式中的每个流式传输大小的价格表格的图，

[0173] 图161是表示各云服务运营商的质量信息的图，

[0174] 图162是说明CDN供应商的选定的图，

[0175] 图163是表示OTA中心的处理的图，

[0176] 图164是表示OTA中心的处理的图，

[0177] 图165是表示OTA中心的处理的图，

[0178] 图166示出第十一实施方式的变形例，是表示系统整体中的处理的流程的一部分的图，

[0179] 图167是表示系统整体中的处理的流程的一部分的图，

[0180] 图168是表示系统整体中的处理的流程的一部分的图，

[0181] 图169是表示系统整体中的处理的流程的一部分的图，

[0182] 图170是表示OTA主机的处理的图，

[0183] 图171是表示PC的处理的图，

[0184] 图172是表示OTA中心的处理的图，

[0185] 图173是表示OTA主机的处理的图，

[0186] 图174示出第十二实施方式的变形例，是表示系统整体中的处理的流程的一部分的图，

[0187] 图175是表示系统整体中的处理的流程的一部分的图，

[0188] 图176是表示系统整体中的处理的流程的一部分的图，

[0189] 图177是表示系统整体中的处理的流程的一部分的图，

[0190] 图178是表示OTA主机的处理的图，

[0191] 图179是表示PC的处理的图，

[0192] 图180是表示OTA中心的处理的图，

[0193] 图181是表示OTA主机的处理的图，

[0194] 图182示出第十六实施方式的变形例，是表示系统整体中的处理的流程的一部分的图，

[0195] 图183是表示系统整体中的处理的流程的一部分的图，

[0196] 图184是表示系统整体中的处理的流程的一部分的图，

[0197] 图185是表示系统整体中的处理的流程的一部分的图，

[0198] 图186是表示OTA主机的处理的图，

[0199] 图187是表示PC的处理的图，

[0200] 图188是表示OTA中心的处理的图，

[0201] 图189是表示OTA主机的处理的图，

[0202] 图190是表示第十九实施方式的系统整体中的处理的流程的图，

[0203] 图191是表示活动通知生成部的处理的图，

[0204] 图192是表示CDN供应商选定部的处理的图，

[0205] 图193是表示CDN供应商选定部的处理的图，

[0206] 图194是表示第十九实施方式的第一变形例的系统整体中的处理的流程的图，

[0207] 图195是表示CDN供应商选定部的处理的图，

[0208] 图196是表示第十九实施方式的第二变形例的系统整体中的处理的流程的图，

[0209] 图197是表示选择表格的图，

[0210] 图198是表示CDN供应商选定部的处理的图，

[0211] 图199是表示CDN供应商选定部的处理的图，

[0212] 图200是表示性能测定部的处理的图，

[0213] 图201是表示CDN服务器确认部的处理的图，

[0214] 图202是表示第十九实施方式的第三变形例的系统整体中的处理的流程的图，

[0215] 图203是表示日志发送部3a的处理的图，

[0216] 图204是表示性能测定部的处理的图，

[0217] 图205是表示性能测定部的处理的图，

[0218] 图206示出第十九实施方式的第四变形例，是表示CDN供应商选定部7a的处理的图，

[0219] 图207是表示活动通知生成部的处理的图，

[0220] 图208是表示第十九实施方式的第五变形例的系统整体中的处理的流程的图，

[0221] 图209是表示轮循(round robin)记录的图，

[0222] 图210是表示CDN供应商选定部7a的处理的图，

[0223] 图211是表示切换部的处理的图，

[0224] 图212是表示第二十实施方式的系统整体中的处理的流程的图，

[0225] 图213是表示计算方法的图，

[0226] 图214是表示活动通知生成部的处理的图，

[0227] 图215是表示CDN供应商选定部的处理的图，

[0228] 图216是表示CDN供应商选定部的处理的图，

[0229] 图217是表示CDN供应商选定部的处理的图，

[0230] 图218是表示CDN供应商选定部的处理的图，

[0231] 图219是表示CDN供应商选定部的处理的图，

[0232] 图220是表示CDN供应商选定部的处理的图，

[0233] 图221是表示CDN供应商选定部的处理的图，

[0234] 图222是表示进展信息管理部的处理的图，

[0235] 图223是表示CDN供应商选定部的处理的图，

[0236] 图224是表示活动通知生成部的处理的图。

具体实施方式

[0237] 以下，参照附图对多个实施方式进行说明。另外，在后续的实施方式中，有时对与先行的实施方式重复的内容省略说明。

[0238] (第一实施方式)

[0239] 参照图1～图14对第一实施方式进行说明。如图1所示，数据通信系统1构成为具备OTA中心2、和搭载于车辆的车辆侧系统3，OTA中心2与车辆侧系统3能够进行数据通信。OTA中心2相当于中心装置。OTA中心2与车辆侧系统3处于一对多的关系，OTA中心2能够在与非特定的许多车辆侧系统3之间进行数据通信。

[0240] 车辆侧系统3具备OTA主机4、和目标ECU5。OTA主机4相当于主机装置。OTA主机4和目标ECU5例如与CAN(Controller Area Network:控制器局域网)(注册商标)等车载网络连接，经由车载网络以能够进行数据通信的方式连接。车载网络也可以是LIN(Local Interconnect Network:本地互联网)、FlexRay(注册商标)、CAN FD(CAN Flexible Data rate:可变速率的CAN)(注册商标)、Ethernet:以太网(注册商标)等。目标ECU5是成为应用

程序的重编对象的ECU,例如可以是进行自动驾驶系统的控制的ECU、进行ADAS系统的控制的ECU、进行多媒体系统的控制的ECU等的任何一个。应用程序是与应用的执行相关的程序,例如包含应用程序、固件程序、操作系统程序。

[0241] OTA中心2具备数据包生成服务器6、和分发服务器7。数据包生成服务器6是具有对更新数据进行打包生成更新数据包的功能的服务器。更新数据包例如是将储存了更新数据的多个文件压缩并储存的zip文件。分发服务器7是具有将通过数据包生成服务器6生成的更新数据包分发给车辆侧系统3的功能的服务器。

[0242] 例如若随着功能改善等所带来的升级,而产生ECU的应用程序的重编要求,则OTA中心2向车辆侧系统3、用户所持有的智能手机等移动信息终端分发活动通知。OTA中心2以得到了来自用户的下载同意为条件,将更新数据包配置在内容分发网络(以下,称为CDN(Content Delivery Network))8,并经由CDN8将更新数据包分发给OTA主机4。或者在更新数据包已经配置于CDN8的情况下,OTA中心2以得到了来自用户的下载同意为条件,使更新数据包从CDN8分发到OTA主机4。

[0243] OTA主机4若从OTA中心2下载更新数据包,则以得到了来自用户的安装同意为条件,将更新数据包转送至目标ECU5,将更新数据包安装于目标ECU5。将提供CDN8作为服务的运营商称为CDN供应商。另外,OTA主机4通过向CDN8的CDN服务器进行访问来获取更新数据包。

[0244] 在本实施方式中,为了实现车辆侧系统3中的先进加密标准(以下,简称为AES(Advanced Encryption Standard))的解密处理的高速化,作为加密模式,不采用一般的块加密的密码块链接模式(以下,称为CBC模式(Cipher Block Chaining Mode)),而采用作为流式加密的代表的计数器模式(以下,称为CTR模式(Counter Mode))。在本实施方式中,OTA中心2通过AES密钥以CTR模式对更新数据包进行加密。另外,车辆侧系统3通过AES密钥以CTR模式对更新数据包进行加密。另外,OTA中心2对每个车辆具备RSA(Rivest-Shamir-Adleman cryptosystem:里维斯特-沙米尔-阿德曼密码系统)公开密钥。OTA主机4在车辆制造阶段被写入RSA秘密密钥。

[0245] 如图2所示,OTA中心2具备公用密钥生成部2a、更新数据包加密部2b、公用密钥加密部2c、公用密钥储存部2d、加密数据包配置部2e、以及活动通知发送部2f,作为涉及加密的功能模块。更新数据包加密部2b相当于更新数据加密部。加密数据包配置部2e相当于加密数据配置部。通过具有CPU(Central Processing Unit:中央处理器)、RAM(Random Access Memory:随机存储器)、ROM(Read Only Memory:只读存储器),I/O(Input/Output:输入输出)等的微型计算机的硬件以及软件的协作实现各部2a～2f。CPU通过执行储存于ROM的包含加密程序、更新数据配置程序、秘密信息共享程序等的各种程序,实现OTA中心2的功能。

[0246] 公用密钥生成部2a生成AES密钥,作为用于加密更新数据包的公用密钥。数据包加密部2b通过生成的AES密钥以CTR模式对更新数据包进行加密。数据包加密部2b通过AES密钥执行对计数器值的AES块加密处理来对计数器值进行加密。数据包加密部2b对加密后的计数器值、和更新数据包进行异或(XOR)运算,将多个加密后的片断结合,生成通过AES密钥已加密的更新数据包。另外,计数器值例如是八位的数字,按照每一AES块增加“1”。

[0247] 公用密钥加密部2c通过RSA公开密钥对AES密钥进行加密。公用密钥储存部2d将通

过RSA公开密钥已加密的AES密钥储存在活动通知中。加密数据包配置部2e将通过AES密钥已加密的更新数据包配置于CDN8。活动通知发送部2f将储存了已加密的AES密钥的活动通知发送给重编对象的车辆侧系统3。活动通知发送部2f也可以将活动通知分发给用户所持有的智能手机等移动信息终端。

[0248] OTA主机4具备公用密钥获取部4a、公用密钥解密部4b、加密数据包获取部4c、块加密处理部4d、加密数据包解密部4e、以及安装处理部4f,作为涉及解密的功能模块。加密数据包获取部4c相当于加密数据获取部。加密数据包解密部4e相当于加密数据解密部。通过具有CPU、RAM、ROM、I/O等的微型计算机的硬件以及软件的协作实现各部4a～4f。CPU通过执行储存于ROM的包含解密程序、更新数据获取程序、秘密信息共享程序等的各种程序,实现OTA主机4的功能。

[0249] 公用密钥获取部4a若由于在OTA主机4接收了从OTA中心2发送的活动通知而获取活动通知,则从该获取的活动通知中获取已加密的AES密钥。公用密钥解密部4b通过RSA秘密密钥对已加密的AES密钥进行解密取出AES密钥。加密数据包获取部4c从CDN8下载并获取已加密的更新数据包。此时,块加密处理部4d与加密数据包获取部4c从CDN8下载并获取已加密的更新数据包并行地,通过AES密钥执行计数器值的AES块加密处理来对计数器值进行加密。加密数据包解密部4e对已加密的计数器值、和从CDN8下载的已加密的更新数据包进行异或(以下,XOR(Exclusively-OR)运算进行解密。安装处理部4f将进行了解密的更新数据包转送至目标ECU5,将更新数据包安装于目标ECU5。

[0250] CTR模式的加密处理如图3所示,CTR模式的解密处理如图4所示。如图5所示,相对于作为CBC模式的缺点的“不能够进行加密以及解密的前准备”、“不能够进行加密的并列处理”,作为CTR模式的优点能够列举“能够进行加密以及解密的前准备,所以能够高速化”、“能够进行加密以及解密的并列处理”。即,作为通过采用CTR模式作为加密模式有助于吞吐量的提高的优点,如图6所示,与采用一般的块加密的CBC模式的情况相比较,能够使吞吐量大约提高40％。

[0251] 如图7所示,在CBC模式的解密处理中,由于输入为密文,所以若不接收作为密文的更新数据包,则不能够开始解密处理。与此相对,如图8所示,在CTR模式的解密处理中,由于输入为计数器值,所以能够从接收作为密文的更新数据包之前开始解密处理。另外,由于相互没有依赖关系,所以也能够同时并列执行多个加密运算。

[0252] 接下来,参照图9～图14对上述的构成的作用进行说明。

[0253] (1－1)OTA中心2的处理(参照图9～图11)

[0254] OTA中心2生成用于对更新数据包进行加密的AES密钥(A011,相当于公用密钥生成步骤)。OTA中心2通过生成的AES密钥以CTR模式对更新数据包进行加密(A012,相当于更新数据加密步骤)。OTA中心2通过RSA公开密钥对AES密钥进行加密(A013,相当于公用密钥加密步骤)。OTA中心2将通过RSA公开密钥已加密的AES密钥储存在活动通知中(A014,相当于公用密钥储存步骤)。OTA中心2将通过AES密钥已加密的更新数据包配置于CDN8(A015,相当于加密数据配置步骤)。将更新数据包配置于CDN8表示将更新数据包配置于CDN8的原始服务器。OTA中心2将储存了已加密的AES密钥的活动通知发送给重编对象的车辆侧系统3(A016,相当于活动通知发送步骤)。

[0255] (1－2)OTA主机4的处理(参照图12～图14)

[0256] OTA主机4若由于在OTA主机4接收了从OTA中心2发送的活动通知而获取活动通知，则从该获取的活动通知中获取AES密钥(B011,相当于公用密钥获取步骤)。OTA主机4通过RSA秘密密钥对已加密的AES密钥进行解密取出AES密钥(B012,相当于公用密钥解密步骤)。OTA主机4从CDN8下载并获取已加密的更新数据包(B013,相当于加密数据获取步骤)。

[0257] 此时,OTA主机4与从CDN8下载并获取已加密的更新数据包并行地,通过AES密钥执行计数器值的AES块加密处理来对计数器值进行加密(B014,相当于块加密处理步骤)。OTA主机4对已加密的计数器值、和从CDN8下载的已加密的更新数据包进行XOR运算来进行解密(B015,相当于加密数据解密步骤)。OTA主机4将进行了解密的更新数据包转送至目标ECU5,将更新数据包安装于目标ECU5(B016,相当于安装处理步骤)。另外,不是通过CBC模式对更新数据包内的差分程序进行加密以及解密,而是通过CTR模式进行加密以及解密,从而对于目标ECU5中的解密处理也能够使吞吐量大约提高40％。

[0258] 如以上说明的那样根据第一实施方式,能够得到以下的作用效果。

[0259] 构成为采用CTR模式作为更新数据包的加密方式以及解密方式。相对于采用了CBC模式的以往技术,通过采用CTR模式,能够进行加密以及解密的前准备,能够进行加密以及解密的并列处理。由此,在OTA主机4从OTA中心2下载更新数据包时,能够享受CTR模式的优点,能够适当地提高吞吐量。

[0260] (第二实施方式)

[0261] 参照图15～图26对第二实施方式进行说明。第一实施方式构成为采用CTR模式作为加密模式,但第二实施方式采用输出反馈模式(以下,称为OFB模式(Output-FeedBack mode))作为加密模式。

[0262] 该情况下,数据包加密部2b通过生成的AES密钥以OFB模式对更新数据包进行加密。块加密处理部4d与加密数据包获取部4c从CDN8下载并获取已加密的更新数据包并行地,通过AES密钥执行基于IV(Initialization Vector:初始向量)值的AES流加密处理来对IV值进行加密。IV值是初始向量值,例如表示随机地生成的位串。加密数据包解密部4e对已加密的IV值、和从CDN8下载的已加密的更新数据包进行XOR运算来进行解密。

[0263] OFB模式的加密处理如图15所示,OFB模式的解密处理如图16所示。如图17所示,相对于作为CBC模式的缺点的“不能够进行加密以及解密的前准备”、“不能够进行加密的并列处理”,作为OFB模式的优点能够列举“能够进行加密以及解密的前准备,所以能够高速化”。即,作为采用OFB模式作为加密模式所带来的有助于吞吐量的提高的优点,如图18所示,与采用了一般的块加密的CBC模式的情况相比较,能够使吞吐量大约提高25％。

[0264] 如图19所示,在CTR模式的解密处理中,由于输入为计数器值,所以能够从接收作为密文的更新数据包之前开始解密处理。另外,由于相互没有依赖关系,所以也能够同时并列执行多个加密运算。与此相对,如图20所示,在OFB模式的解密处理中,由于相互有依赖关系,所以不能够同时并列执行多个加密运算。但是,能够并列执行对已加密的IV值与已加密的更新数据包进行XOR运算来进行解密的处理。因此,在OFB模式的解密处理中,虽然不能够使吞吐量提高至在第一实施方式中进行了说明的CTR模式的解密处理的程度,但与采用了CBC模式的情况相比较,能够使吞吐量提高。

[0265] 接下来,参照图21～图26对上述的构成的作用进行说明。

[0266] (2－1)OTA中心2的处理(参照图21～图23)

[0267] OTA中心2生成用于对更新数据包进行加密的AES密钥(A021,相当于公用密钥生成步骤)。OTA中心2通过生成的AES密钥以OFB模式对更新数据包进行加密(A022,相当于更新数据加密步骤)。OTA中心2通过RSA公开密钥对AES密钥进行加密(A023,相当于公用密钥加密步骤)。OTA中心2将通过RSA公开密钥已加密的AES密钥储存在活动通知中(A024,相当于公用密钥储存步骤)。OTA中心2将通过AES密钥已加密的更新数据包配置于CDN8(A025,相当于加密数据配置步骤)。OTA中心2将储存了已加密的AES密钥的活动通知发送到重编对象的车辆侧系统3(A026,相当于活动通知发送步骤)。

[0268] (2—2)OTA主机4的处理(参照图24～图26)

[0269] OTA主机4若由于在OTA主机4接收了从OTA中心2发送的活动通知而获取活动通知,则从该获取的活动通知中获取AES密钥(B021,相当于公用密钥获取步骤)。OTA主机4通过RSA秘密密钥对已加密的AES密钥进行解密取出AES密钥(B022,相当于公用密钥解密步骤)。OTA主机4从CDN8下载并获取已加密的更新数据包(B023,相当于加密数据获取步骤)。

[0270] 此时,OTA主机4与从CDN8下载并获取已加密的更新数据包并行地,通过AES密钥执行基于IV值的AES流加密处理来对IV值进行加密(B024,相当于块加密处理步骤)。OTA主机4对已加密的IV值、和从CDN8下载的已加密的更新数据包进行XOR运算来进行解密(B025,相当于加密数据解密步骤)。OTA主机4将进行了解密的更新数据包转送至目标ECU5,将更新数据包安装于目标ECU5(B026,相当于安装处理步骤)。另外,不是通过CBC模式对更新数据包内的差分程序进行加密以及解密,而是通过OFB模式进行加密以及解密,从而对于目标ECU5中的解密处理也能够使吞吐量提高大约25％。

[0271] 如以上说明的那样根据第二实施方式,能够得到以下的作用效果。

[0272] 构成为采用OFB模式作为更新数据包的加密方式以及解密方式。相对于采用CBC模式的以往技术,通过采用OFB模式,能够进行加密以及解密的前准备。由此,在OTA主机4从OTA中心2下载更新数据包时,能够享受OFB模式的优点,能够适当地提高吞吐量。

[0273] (第三实施方式)

[0274] 参照图27～图33对第三实施方式进行说明。第三实施方式采用超文本传输协议(以下,称为HTTP(Hypertext Transfer Protocol)),作为CDN8与OTA主机4之间的通信协议,通过向CDN8发送范围请求,并以流式传输方式下载更新数据包,与采用安全超文本传输协议(以下,称为HTTPS(Hypertext Transfer Protocol Secure))的情况相比实现分发成本的抑制。有根据CDN供应商,而在向CDN8的通信协议使用HTTP的情况和使用HTTPS的情况下CDN8的分发费用有差别的情况。在使用HTTPS的情况下,CDN8需要进行根据传输层安全(以下,称为TLS(Transport Layer Security))规定的握手处理、加密密钥交换处理、加密运算处理,而CDN8的CPU的处理负荷增大,所以HTTPS的分发费用成为与HTTP相比大约高三成的费用表格。因此,更新数据包的下载通过使用HTTP实现分发成本的抑制。在第三实施方式中,在从CDN8向车辆侧系统3分发更新数据包时不使用HTTPS。

[0275] 该情况下,活动通知发送部2f在OTA中心4与OTA主机4之间建立了TLS通信之后,将储存了已加密的AES密钥的活动通知发送到重编对象的车辆侧系统3。公用密钥获取部4a若由于在建立了TLS通信之后,在OTA主机4接收了从OTA中心2发送的活动通知而获取活动通知,则从该获取的活动通知中获取AES密钥。加密数据包获取部4c向CDN8发送范围请求而指定下载对象的数据范围,通过流式传输方式从CDN8下载并获取已加密的更新数据包。安装

处理部4f通过流式传输方式将进行了解密的更新数据包转送至目标ECU5,将更新数据包安装于目标ECU5。

[0276] 另外,虽然在本实施方式中,对在OTA主机4中,通过流式传输方式从CDN8获取已加密的更新数据包的情况进行说明,但也可以通过储存方式从CDN8获取已加密的更新数据包。在流式传输方式中,在通信时包含报头信息,所以通过使用HTTP能够进一步抑制分发成本。

[0277] 接下来,参照图28～图33对上述的构成的作用进行说明。

[0278] (3—1)OTA中心2的处理(参照图28～图30)

[0279] OTA中心2生成用于对更新数据包进行加密的AES密钥(A031)。OTA中心2通过生成的AES密钥以CTR模式对更新数据包进行加密(A032)。OTA中心2通过RSA公开密钥对AES密钥进行加密(A033)。OTA中心2将通过RSA公开密钥已加密的AES密钥储存在活动通知中(A034)。OTA中心2将通过AES密钥已加密的更新数据包配置于CDN8(A035)。OTA中心2在OTA中心4与OTA主机4之间建立了TLS通信之后,将储存了已加密的AES密钥的活动通知发送到重编对象的车辆侧系统3(A036)。

[0280] (3—2)OTA主机4的处理(参照图31～图33)

[0281] OTA主机4若由于在建立了TLS通信之后,在OTA主机4接收了从OTA中心2发送的活动通知而获取活动通知,则从该获取的活动通知中获取AES密钥(B031)。OTA主机4通过RSA秘密密钥对已加密的AES密钥进行解密取出AES密钥(B032)。OTA主机4向CDN8发送范围请求而指定下载对象的数据范围,通过流式传输方式从CDN8下载并获取已加密的更新数据包(B033)。即,OTA主机4通过指定下载对象的数据范围,通过分割流式传输方式从CDN8下载并获取更新数据包。

[0282] 此时,OTA主机4与加密数据包获取部4c从CDN8下载并获取已加密的更新数据包并行地,通过AES密钥执行计数器值的AES块加密处理来对计数器值进行加密(B034)。OTA主机4对已加密的计数器值、和从CDN8下载的已加密的更新数据包进行XOR运算来进行解密(B035)。OTA主机4通过流式传输方式将进行了解密的更新数据包转送至目标ECU5,将更新数据包安装于目标ECU5(B036)。

[0283] 如以上说明的那样根据第三实施方式,能够得到以下的作用效果。

[0284] 构成为采用HTTP作为CDN8与OTA主机4之间的通信协议,OTA主机4通过向CDN8发送范围请求以流式传输方式从该CDN8下载更新数据包。由此,相对于采用HTTPS作为通信协议的以往技术,能够适当地抑制OTA主机4从OTA中心2下载更新数据包时的分发成本。

[0285] (第四实施方式)

[0286] 参照图34～图38对第四实施方式进行说明。第四实施方式通过在得到来自用户的下载同意之前预先在后台执行全部的密钥流的计算,实现更新数据包的下载时的解密处理的高速化。

[0287] 该情况下,如图35所示,OTA主机4除了公用密钥获取部4a、公用密钥解密部4b、加密数据包获取部4c、块加密处理部4d、加密数据包解密部4e、安装处理部4f之外,还具备密钥流计算部4g。密钥流计算部4g在得到来自用户的下载同意之前预先在后台执行全部的密钥流的计算。加密数据包获取部4c以得到了来自用户的下载同意为条件,从CDN8下载并获取已加密的更新数据包。加密数据包解密部4e对计算出的密钥流、和从CDN8下载的已加密

的更新数据包进行XOR运算来进行解密。

[0288] 接下来,参照图36～图38对上述的构成的作用进行说明。

[0289] (4－1)OTA中心2的处理

[0290] OTA中心2的处理与在第一实施方式中进行了说明的OTA中心2的处理(图9～图11)相同。

[0291] (4－2)OTA主机4的处理(参照图36～图38)

[0292] OTA主机4若由于在OTA主机4接收了从OTA中心2发送的活动通知而获取活动通知,则从该获取的活动通知中获取AES密钥(B041)。OTA主机4通过RSA秘密密钥对已加密的AES密钥进行解密取出AES密钥(B042)。OTA主机4在得到来自用户的下载同意之前预先在后台执行全部的密钥流的计算(B043)。对各个密钥流附加有识别信息,表示对已加密的更新数据包的应用顺序。

[0293] OTA主机4通过将活动通知分发到车辆侧系统3、用户所持有的智能手机等移动信息终端,在HMI(Human Machine Interface:人机界面)显示下载同意画面(B044)。OTA主机4以得到了来自用户的下载同意为条件,从CDN8下载并获取已加密的更新数据包(B045)。OTA主机4对预先计算出的密钥流、和从CDN8下载的已加密的更新数据包进行XOR运算来进行解密(B046)。OTA主机4将进行了解密的更新数据包转送至目标ECU5,将更新数据包安装于目标ECU5(B047)。

[0294] 如以上说明的那样根据第四实施方式,能够得到以下的作用效果。

[0295] 构成为在得到来自用户的下载同意之前预先在后台执行全部的密钥流的计算。由此,能够使OTA主机4中的更新数据包的解密处理高速化,能够提高OTA主机4从OTA中心2下载更新数据包时的吞吐量。

[0296] (第五实施方式)

[0297] 参照图39～图42对第五实施方式进行说明。第四实施方式在得到来自用户的下载同意之前预先在后台执行全部的密钥流的计算,但第五实施方式在得到来自用户的下载同意之前预先在后台执行一部分的密钥流的计算。考虑CPU的缓冲存储器的存储器容量和AES加密运算的吞吐量来决定作为计算的对象的一部分的密钥流,成为能够保存于缓冲存储器的大小。

[0298] 该情况下,密钥流计算部4g在得到来自用户的下载同意之前预先在后台执行一部分的密钥流的计算。密钥流计算部4g与加密数据包获取部4c从CDN8下载并获取已加密的更新数据包并行地,生成密钥流并追加到缓冲存储器。

[0299] 接下来,参照图39～图42对上述的构成的作用进行说明。

[0300] (5－1)OTA中心2的处理

[0301] OTA中心2的处理与在第一实施方式进行了说明的OTA中心2的处理(图9～图11)相同。

[0302] (5－2)OTA主机4的处理(参照图39～图41)

[0303] OTA主机4若由于在OTA主机4接收了从OTA中心2发送的活动通知而获取活动通知,则从该获取的活动通知中获取AES密钥(B051)。OTA主机4通过RSA秘密密钥对已加密的AES密钥进行解密取出AES密钥(B052)。OTA主机4在得到来自用户的下载同意之前预先在后台执行一部分的密钥流的计算(B053)。

[0304] OTA主机4通过将活动通知分发到车辆侧系统3、用户所持有的智能手机等移动信息终端,在HMI显示下载同意画面(B054)。OTA主机4以得到了来自用户的下载同意为条件,从CDN8下载并获取已加密的更新数据包(B055)。OTA主机4对预先计算出的密钥流、和从CDN8下载的已加密的更新数据包进行XOR运算来进行解密(B056)。

[0305] 此时,OTA主机4与从CDN8下载并获取已加密的更新数据包并行地,生成密钥流并追加到缓冲存储器(B057),并计算剩余的密钥流。OTA主机4将进行了解密的更新数据包转送至目标ECU5,将更新数据包安装于目标ECU5(B058)。另外,存储器容量与访问速度的关系如图42所示,根据要求的访问速度来决定缓冲存储器的大小即可。

[0306] 如以上说明的那样根据第五实施方式,能够得到以下的作用效果。

[0307] 构成为在得到来自用户的下载同意之前预先在后台执行一部分的密钥流的计算。由此,能够节约OTA主机4的存储器使用量,并且使OTA主机4中的更新数据包的解密处理高速化,能够提高OTA主机4从OTA中心2下载更新数据包时的吞吐量。

[0308] (第六实施方式)

[0309] 参照图43～图54对第六实施方式进行说明。第六实施方式通过使加密方式包含于重编策略元数据(以下,称为RP元数据)等并从OTA中心2发送到OTA主机4,由OTA主机4确定加密方式。从OTA中心2向OTA主机4发送的加密方式包含加密算法、加密密钥长度、加密模式、消息认证码(以下,称为MAC(Message Authentication Code))算法等。

[0310] RP元数据包含更新数据包的构成信息,即表示更新数据包的构成种类的信息,是用于通过由OTA主机4检查其数据内容来防止更新数据包的分发错误的数据。通过使RP元数据为分发、主机以及目标的三层结构,即使在转送方式、平台的类型、更新数据包的种类等增大的情况下,也能够灵活地定义它们并进行应对,能够进行目标ECU5的重编。另外,也可以通过使加密方式包含于下载元数据(以下,称为DL元数据)等并从OTA中心2发送到OTA主机4,由OTA主机4确定加密方式。DL元数据包含用于下载多个目标ECU5中的每一个的更新数据包的信息,是规定OTA主机4应该掌握的内容的数据。

[0311] 如图44所示,OTA中心2除了公用密钥生成部2a、更新数据包加密部2b、公用密钥加密部2c、公用密钥储存部2d、加密数据包配置部2e、以及活动通知发送部2f之外,还具备RP元数据生成部2g、和RP元数据加密部2h。RP元数据生成部2g生成包含公用密钥加密方式的RP元数据。RP元数据加密部2h通过RSA公开密钥对RP元数据进行加密。

[0312] OTA主机4除了公用密钥获取部4a、公用密钥解密部4b、加密数据包获取部4c、块加密处理部4d、加密数据包解密部4e、以及安装处理部4f之外,还具备RP元数据获取部4h、RP元数据解密部4i、以及公用密钥加密方式确定部4j。RP元数据获取部4h从CDN8下载并获取已加密的RP元数据。RP元数据解密部4i通过RSA秘密密钥对已加密的RP元数据进行解密取出RP元数据。公用密钥加密方式确定部4j对RP元数据的内容进行解释确定公用密钥加密方式。

[0313] 另外,到从CDN8向OTA中心2的更新数据包的分发为止的流程如以下那样。从OTA中心2向OTA主机4或者用户所持有的移动信息终端发送活动通知。其后,通过OTA主机4向CDN8进行访问,从CDN8向OTA主机4发送RP元数据以及DL元数据,从CDN8向OTA中心2分发更新数据包。

[0314] 如图45所示,RP元数据以及DL元数据在更新数据包的下载之前从OTA中心2发送到

OTA主机4。如图46～图47所示,RP元数据包含RP元数据版本、分发层、主机层、目标层的信息。各信息如以下那样。

[0315] (a)RP元数据版本

[0316] RP元数据的版本,例如是“1.0.0”、“2.0.0”等版本信息。

[0317] (b)分发层

[0318] (b－1)通信协议

[0319] 与OTA中心2的通信所使用的协议,例如是表示Uptane(注册商标)、OMA－DM(Open Mobile Alliance-Device Management:开放移动联盟设备管理)等的信息。

[0320] (b－2)通信单元

[0321] 更新数据包的分发路径,是表示表示为OTA主机4的蜂窝、智能手机、USB存储器等的信息。

[0322] (c)主机层

[0323] 与OTA主机4相关的信息。

[0324] (c－1)PF

[0325] 是表示OTA主机4的平台(PF)例如为AP(AUTOSAR Adaptive Platform:AUTOSAR自适应平台)、CP(AUTOSAR Classic Platform:AUTOSAR经典平台)、AGL(Automotive Grade Linux:汽车级Linux)、Android(注册商标)等的信息。对于用于分发与ECU的平台对应的更新数据包的数据包结构,在一般社团法人JASPAR的规格中,规定能够应用于在标准化组织AUTOSAR的静态OS上进行动作的经典平台(CP)的数据要求。另外,在AUTOSAR中,规定能够应用于在动态OS上进行动作的新的类型的自适应平台(AP)的数据要求。AGL是车载Linux(注册商标),Android是Android Automotive OS。AP以及CP表示软件平台。软件平台也称为软件体系结构。在AP以及CP中,使用的操作系统、开发语言不同。在依据CP说明书进行动作的ECU和依据AP说明书进行动作的ECU中,能够接收的更新数据包的结构不同。这些更新数据包的结构的不同主要起因于ECU的处理性能的不同。一般而言,依据CP说明书进行动作的ECU的处理性能比较低,所以更新数据包所包含的规格数据等也以二进制数据记载,成为即使在处理性能较低的ECU中也容易进行解释以及处理的数据结构。另一方面,由于依据AP说明书进行动作的ECU的处理性能比较高,所以能够搭载对以某种语言记述的结构性的字符数据进行解析并转换为能够在程序中处理的数据结构的解析器功能,数据结构不是简单的二进制数据,而例如能够采用JSON(JavaScript Object Notation:JavaScript对象表示法)那样的面向对象的数据形式,所以成为灵活的数据结构。

[0326] (c－2)控制方式

[0327] 基于根据特定的格式设定的参数进行处理的参数、没有特定的格式而以更自由的记载形式进行处理的脚本等信息。

[0328] (c－3)加密方式

[0329] 包含加密算法、加密密钥长度、加密模式、Padding方式、加密密钥ID、签名算法、签名密钥ID、签名模式、散列算法、区域指定有无、偏移大小、保护数据大小的信息。

[0330] (d)目标层

[0331] 与目标ECU5相关的信息。

[0332] (d－1)PF

[0333] 与主机层相同。

[0334] (d—2)转送方式

[0335] 储存方式、流式传输的任意一个。

[0336] (d—3)控制方式

[0337] 与主机层相同。

[0338] (d—4)目标ID

[0339] 选项。

[0340] (d—5)加密方式

[0341] 与主机层相同。

[0342] 接下来,参照图48～图54对上述的构成的作用进行说明。

[0343] (6—1)OTA中心2的处理(参照图48～图51)

[0344] OTA中心2生成用于对更新数据包进行加密的公用密钥(A061)。OTA中心2通过生成的公用密钥以特定的加密模式对更新数据包进行加密(A062)。OTA中心2通过RSA公开密钥对公用密钥进行加密(A063)。OTA中心2将通过RSA公开密钥已加密的公用密钥储存在活动通知中(A064)。OTA中心2生成包含公用密钥加密方式的RP元数据(A065)。OTA中心2通过RSA公开密钥对RP元数据进行加密(A066)。OTA中心2将通过公用密钥已加密的更新数据包和通过RSA公开密钥已加密的RP元数据配置于CDN8(A067)。OTA中心2将储存了已加密的公用密钥的活动通知发送到重编对象的车辆侧系统3(A068)。

[0345] (6—2)OTA主机4的处理(参照图52～图54)

[0346] OTA主机4若由于在OTA主机4接收了从OTA中心2发送的活动通知而获取活动通知,则从该获取的活动通知中获取公用密钥(B061)。OTA主机4通过RSA秘密密钥对已加密的公用密钥进行解密取出公用密钥(B062)。OTA主机4从CDN8下载并获取已加密的RP元数据(B063)。OTA主机4通过RSA秘密密钥对已加密的RP元数据进行解密取出RP元数据(B064)。OTA主机4对RP元数据的内容进行解释确定公用密钥加密方式(B065)。OTA主机4从CDN8下载并获取已加密的更新数据包(B066)。在此以后,若为采用CTR模式作为特定的加密模式的情况则OTA主机4进行在第一实施方式中进行了说明的步骤B014以后的处理,若为采用OFB模式作为特定的加密模式的情况则进行在第二实施方式中进行了说明的步骤B024以后的处理。在其以外的加密模式的情况下也相同,根据与加密模式对应的顺序,进行更新数据包的、解密、向目标ECU的数据的转送。

[0347] 如以上进行说明的那样根据第六实施方式,能够得到以下的作用效果。

[0348] 构成为使加密方式包含于RP元数据或者DL元数据并从OTA中心2发送到OTA主机4。由此,在OTA主机4中能够确定加密方式。

[0349] (第七实施方式)

[0350] 参照图55～图67对第七实施方式进行说明。第七实施方式采用CCMP模式(Counter mode with Cipher-block chaining Message authentication code Protocol:计数器模式密码块链信息认证码协议)作为通信路加密和数据篡改对策。

[0351] 该情况下,如图56～图60所示,若对采用了CCMP模式的构成与作为现有方式采用了AES CBC—HMAC(Hashed Message Authentication Mode Code:散列消息认证码)SHA(Secure Hash Algorithm:安全散列算法)2的解密以及签名验证的构成进行比较,则虽然

硬件加速器的处理时间都与主核的处理时间相比占支配地位,但通过采用CCMP模式能够使吞吐量提高。

[0352] 如图61所示,OTA中心2除了公用密钥生成部2a、更新数据包加密部2b、公用密钥加密部2c、公用密钥储存部2d、加密数据包配置部2e、以及活动通知发送部2f之外,还具备MAC密钥生成部2i。MAC密钥生成部2i生成用于防止更新数据包的篡改的MAC。

[0353] OTA主机4除了公用密钥获取部4a、公用密钥解密部4b、加密数据包获取部4c、块加密处理部4d、加密数据包解密部4e、以及安装处理部4f之外,还具备MAC密钥获取部4k。MAC密钥获取部4k若由于在OTA主机4接收了从OTA中心2发送的活动通知而获取活动通知,则从该获取的活动通知中获取MAC密钥。

[0354] 接下来,参照图62～图67对上述的构成的作用进行说明。

[0355] (7－1)OTA中心2的处理(参照图62～图64)

[0356] OTA中心2生成用于对更新数据包进行加密的AES密钥、和用于防止更新数据包的篡改的MAC密钥(A071)。OTA中心2通过生成的AES密钥和MAC密钥以CCMP模式对更新数据包进行加密,附加MAC(A072)。OTA中心2通过RSA公开密钥对AES密钥和MAC密钥进行加密(A073)。OTA中心2将通过RSA公开密钥已加密的AES密钥和MAC密钥储存在活动通知中(A074)。OTA中心2将通过AES密钥和MAC密钥已加密的更新数据包配置于CDN8(A075)。OTA中心2将储存了已加密的AES密钥和MAC密钥的活动通知发送到重编对象的车辆侧系统3(A076)。

[0357] (7－2)OTA主机4的处理(参照图65～图67)

[0358] OTA主机4若由于在OTA主机4接收了从OTA中心2发送的活动通知而获取活动通知,则从该获取的活动通知中获取AES密钥和MAC(B071)。OTA主机4通过RSA秘密密钥对已加密的AES密钥和MAC密钥进行解密取出AES密钥和MAC密钥(B017)。OTA主机4从CDN8下载并获取已加密的更新数据包(B073)。

[0359] 此时,OTA主机4与从CDN8下载并获取已加密的更新数据包并行地,通过AES密钥执行计数器值的AES块加密处理对计数器值进行加密(B074)。OTA主机4对已加密的计数器值、和从CDN8下载的已加密的更新数据包进行XOR运算来进行解密(B075)。OTA主机4根据进行了解密的更新数据包的明文使用MAC密钥以AES－CBC模式生成MAC来进行验证(B076)。若MAC一致,则OTA主机4将进行了解密的更新数据包转送至目标ECU5,将更新数据包安装于目标ECU5(B077)。若MAC不一致,则OTA主机4结束处理。该情况下,OTA主机4也可以若由于MAC的不一致而结束处理,则记录表示由于MAC的不一致而结束了处理的日志,并且在未图示的HMI进行错误显示。或者,OTA主机4也可以对已加密的更新数据包进行XOR运算进行解密,与此同时将进行了解密的更新数据包转送至目标ECU5。该情况下,OTA主机4也可以构成为根据进行了解密的更新数据包的明文使用MAC密钥通过AES－CBC模式生成MAC并进行验证,在判定为MAC不一致的情况下,对目标ECU5通知安装的中止。

[0360] 如以上说明的那样根据第七实施方式,能够得到以下的作用效果。

[0361] 构成为采用CCMP模式作为OTA中心2与OTA主机4之间的通信路加密和数据篡改对策。通过采用CCMP模式,OTA主机4在从OTA中心2下载更新数据包时除了通信路加密之外还能够具备数据篡改对策。由此,能够提高安全,能够实现更安全的OTA分发。

[0362] (第八实施方式)

[0363] 参照图68～图77对第八实施方式进行说明。第八实施方式采用GCMP模式(Galois/Counter Mode Protocol:伽罗瓦计数器模式协议),作为通信路加密和数据篡改对策。

[0364] 该情况下,如图69～图71所示,若对采用了GCMP模式的构成与采用了CCMP模式的构成、作为现有方式采用了AES CBC—HMAC SHA2的解密以及签名验证的构成进行比较,则虽然硬件加速器的处理时间都与主核的处理时间相比占支配地位,但通过采用GCMP模式能够使吞吐量进一步提高。

[0365] 接下来,参照图72～图77对上述的构成的作用进行说明。

[0366] (8—1)OTA中心2的处理(参照图72～图74)

[0367] OTA中心2生成用于对更新数据包进行加密的AES密钥、和用于防止更新数据包的篡改的MAC密钥(A081)。OTA中心2通过生成的AES密钥和MAC密钥以GCMP模式对更新数据包进行加密,附加MAC(A082)。OTA中心2通过RSA公开密钥对AES密钥和MAC密钥进行加密(A083)。OTA中心2将通过RSA公开密钥已加密的AES密钥和MAC密钥储存在活动通知中(A084)。OTA中心2将通过AES密钥和MAC密钥已加密的更新数据包配置于CDN8(A085)。OTA中心2将储存了已加密的AES密钥和MAC密钥的活动通知发送至重编对象的车辆侧系统3(A086)。

[0368] (8—2)OTA主机4的处理(参照图75～图77)

[0369] OTA主机4若由于在OTA主机4接收了从OTA中心2发送的活动通知而获取活动通知,则从该获取的活动通知中获取AES密钥和MAC(B081)。OTA主机4通过RSA秘密密钥对已加密的AES密钥和MAC密钥进行解密取出AES密钥和MAC密钥(B082)。OTA主机4从CDN8下载并获取已加密的更新数据包(B083)。

[0370] 此时,OTA主机4与从CDN8下载并获取已加密的更新数据包并行地,通过AES密钥执行计数器值的AES块加密处理来对计数器值进行加密(B084)。OTA主机4对已加密的计数器值、和从CDN8下载的已加密的更新数据包进行XOR运算来进行解密(B085)。OTA主机4根据进行了解密的更新数据包的明文使用MAC密钥以GMAC模式生成MAC并进行验证(B086)。若MAC一致,则OTA主机将进行了解密的更新数据包转送至目标ECU5,将更新数据包安装于目标ECU5(B087)。

[0371] 如以上说明的那样根据第八实施方式,能够得到以下的作用效果。

[0372] 构成为采用GCMP模式作为OTA中心2与OTA主机4之间的通信路加密和数据篡改对策。通过采用GCMP模式,OTA主机4在从OTA中心2下载更新数据包时除了通信路加密之外还能够具备数据篡改对策。由此,能够提高安全,能够实现更安全的OTA分发。

[0373] (第九实施方式)

[0374] 参照图78～图86对第九实施方式进行说明。第九实施方式通过不仅采用CDN8,还采用智能手机、USB存储器等作为更新数据的分发路径,应对分发路径的多样性,来提高用户的OTA更新方式的自由度。智能手机、USB存储器相当于记录介质。其以后,例示智能手机、USB存储器作为存储介质进行说明,但也可以采用SD卡、微型SD卡、紧凑型闪存等作为存储介质。

[0375] 接下来,参照图79～图86对上述的构成的作用进行说明。

[0376] (9—1)OTA中心2的处理(参照图79～图82)

[0377] OTA中心2生成用于对更新数据包进行加密的公用密钥(A091)。OTA中心2通过生成

的公用密钥以特定的加密模式对更新数据包进行加密(A092)。OTA中心2通过RSA公开密钥对公用密钥进行加密(A093)。OTA中心2将通过RSA公开密钥已加密的公用密钥储存在活动通知中(A094)。OTA中心2生成包含公用密钥加密方式和分发路径的RP元数据(A095)。OTA中心2通过RSA公开密钥对RP元数据进行加密(A096)。OTA中心2将通过公用密钥已加密的更新数据包和通过RSA公开密钥已加密的RP元数据配置于CDN8(A097)。OTA中心2将储存了已加密的公用密钥的活动通知发送至重编对象的车辆侧系统3(A098)。

[0378] (9—2)OTA主机4的处理(参照图83～图86)

[0379] OTA主机4若由于在OTA主机4接收了从OTA中心2发送的活动通知而获取活动通知,则从该获取的活动通知中获取已加密的公用密钥(B091)。OTA主机4通过RSA秘密密钥对已加密的公用密钥进行解密取出公用密钥(B092)。OTA主机4从CDN8下载并获取已加密的RP元数据(B093)。OTA主机4通过RSA秘密密钥对已加密的RP元数据进行解密取出RP元数据(B094)。OTA主机4对RP元数据的内容进行解释确定公用密钥加密方式和分发路径(B095)。OTA主机4通过该确定出的分发路径获取已加密的更新数据包(B096)。即,OTA主机4在确定了智能手机作为分发路径的情况下,从CDN8经由智能手机以批量储存方式下载已加密的更新数据包。OTA主机4在确定了USB存储器作为分发路径的情况下,从CDN8经由USB存储器以批量储存方式下载已加密的更新数据包。其以后,若为采用了CTR模式作为特定的加密模式的情况则OTA主机4进行在第一实施方式进行了说明的步骤B014以后的处理,若为采用了OFB模式作为特定的加密模式的情况则进行在第二实施方式进行了说明的步骤B024以后的处理。

[0380] 如以上说明的那样根据第九实施方式,能够得到以下的作用效果。

[0381] 从CDN8经由智能手机或者USB存储器等记录介质获取更新数据包。能够使更新数据包的分发路径具有多样性,能够选择分发成本、可用性优越的分发路径。由此,能够适当地抑制OTA主机4从OTA中心2下载更新数据包时的分发成本,并且提高用户体验价值。另外,在上述的实施方式中,OTA主机4在步骤B095中对RP元数据的内容进行解释确定公用密钥加密方式和分发路径,但在RP元数据记载有多个分发路径的情况下,也可以能够从多个分发路径中选择任意一个。

[0382] (第十实施方式)

[0383] 参照图87～图98对第十实施方式进行说明。第十实施方式根据分发方式、作为分发区域的OTA对象区域、分发数据大小动态地选定多个CDN供应商作为更新数据包的向CDN8的配置目的地,来抑制分发成本。CDN的成本比较如图88～图89所示。价格表格如图90～图93所示。各CDN供应商根据日本或者北美等分发区域、分发数据大小等而价格的优劣不同,例如若参照图90,则在一个月分发100TB的数据大小的情况下,在日本CDN2最便宜,但在北美或者EU则CDN1最便宜。基于该情况根据分发方式、OTA对象区域、分发数据大小选定分发成本最便宜的CDN供应商。

[0384] 如图94所示,OTA中心2除了公用密钥生成部2a、更新数据包加密部2b、公用密钥加密部2c、公用密钥储存部2d、加密数据包配置部2e、以及活动通知发送部2f之外,还具备CDN供应商选定部2j。CDN供应商选定部2j参照CDN供应商管理数据库选定CDN供应商。

[0385] 接下来,参照图95～图98对上述的构成的作用进行说明。

[0386] (10—1)OTA中心2的处理(参照图95～图98)

[0387] OTA中心2生成用于对更新数据包进行加密的AES密钥(A101)。OTA中心2通过生成的AES密钥以CTR模式对更新数据包进行加密(A102)。OTA中心2通过RSA公开密钥对AES密钥进行加密(A103)。OTA中心2将通过RSA公开密钥已加密的AES密钥储存在活动通知中(A104)。OTA中心2确定分发方式(A105),确定OTA对象区域(A106),确定分发数据大小(A107),并从CDN供应商管理数据库以分发方式、OTA对象区域以及分发数据大小为关键词参照价格表格(A108)。该情况下,OTA中心2也可以以储存方式、流式传输方式等分发方式、日本、北美、EU(European Union:欧盟)等OTA对象区域、GB、TB、PB等分发数据大小中至少任意一个为关键词参照价格表格。OTA中心2按照区域选定分发成本最小的CDN供应商,并将通过AES密钥已加密的更新数据包配置于该选定的CDN8(A109,相当于CDN供应商选定步骤)。或者,OTA中心2也可以将通过AES密钥已加密的更新数据包配置于各CDN8。OTA中心2将储存了已加密的AES密钥、和用于能够访问选定的CDN供应商的更新数据包的数据储存目的地或者URI信息的活动通知发送到重编对象的车辆侧系统3(A110)。

[0388] (10—2)OTA主机4的处理

[0389] OTA主机4的处理与在第一实施方式中进行了说明的OTA主机4的处理(图12～图14)相同。

[0390] 如以上说明的那样根据第十实施方式,能够得到以下的作用效果。

[0391] 构成为参照CDN供应商管理数据库,根据分发方式、OTA对象区域以及分发数据大小从分发成本不同的多个CDN8中选定分发成本优越的CDN8,并将更新数据包配置于该选定的CDN8。能够适当地抑制OTA主机4从OTA中心2下载更新数据包时的分发成本。另外,通过在OTA中心2对更新数据包进行加密,在原理上即使对中途路径零信任,在安全上也没有妨碍。因此,没有在CDN8的边缘侧对更新数据进行加密的必要性,能够削减CDN8的处理负荷、安全功能。到更新数据包从OTA中心2到达OTA主机4为止,即使在中途路径数据篡改或者CDN8受到DDoS攻击,作为OTA系统也没有影响,介于中途路径的系统能够不需要智能的安全对策,例如网络应用防火墙、TLS通信、限定成为分发对象的OTA主机4的带签名的URL等多层防御的安全辅助对策。由此,能够以原价为基础降低OTA系统的运行成本,无论在哪个系统构成中都能够抑制分发成本。

[0392] (第十一实施方式)

[0393] 参照图99～图108对第十一实施方式进行说明。第十一实施方式在OTA中心2与OTA主机4之间的密钥配送采用迪菲-赫尔曼密钥共享(以下,称为DHE(Diffie-Hellman key exchange))或者椭圆曲线迪菲-赫尔曼密钥共享(以下,称为ECDHE(Elliptic curve Diffie-Hellman key exchange)),并且在OTA中心2中基于共享的按照每个车辆不同的秘密信息对AES密钥进行加密并分发给OTA主机4,从而在享受能够确保ECDHE的前向保密性这样的优点的同时,分发能够应用于CDN8的各车辆型号或者特定的车辆组能够应用的更新数据包。

[0394] 如图100所示,两者根据随机数(＝秘密密钥:a、b)生成并交换各自的公开密钥(A、B),并与自身的秘密密钥组合进行计算,从而秘密地共享秘密信息(S)。秘密密钥以及公开密钥对(a/A、b/B)在共享了秘密信息(S)之后能够废除,不需要在OTA中心2和OTA主机4双方储存于HSM(硬件安全模型),所以能够非常安全地共享秘密信息(S)。该共享的秘密信息(S)能够有效利用于公用密钥加密的密钥等,但由于原始数据为随机数(a、b),所以在每个OTA

主机为不同的密钥。

[0395] 接下来,参照图101～图108对上述的构成的作用进行说明。

[0396] (11－1)OTA中心2的处理(参照图101～图104)

[0397] OTA中心2生成用于对更新数据包进行加密的AES密钥(A111)。OTA中心2通过生成的AES密钥以CTR模式对更新数据包进行加密(A112)。OTA中心2根据随机数生成ECDHE的密钥对(A113)。OTA中心2通过ECDHE的算法与OTA主机4共享秘密密钥(A114,相当于秘密信息共享步骤)。OTA中心2通过秘密密钥对AES密钥进行加密(A115)。OTA中心2将通过秘密密钥已加密的AES密钥储存在活动通知中(A116)。OTA中心2将通过AES密钥已加密的更新数据包配置于CDN8(A117)。OTA中心2将储存了已加密的AES密钥的活动通知发送到重编对象的车辆侧系统3(A118,相当于加密密钥分发步骤)。

[0398] 这里,对步骤A114进行说明。若车辆的点火开关接通,且从上次的车辆构成信息的同步起经过规定期间,则OTA主机4向搭载于车辆的ECU询问程序版本而收集车辆构成信息。或者OTA主机4若从OTA中心2接收与活动相关的推送通知,则向ECU询问程序版本而收集车辆构成信息。OTA主机4若收集车辆构成信息,则在与OTA中心2之间建立TLS通信,将车辆构成信息发送到OTA中心2。此时,OTA主机4在收集车辆构成信息的同时,生成ECDHE的密钥对,若在与OTA中心2之间建立TLS通信,则将密钥对中OTA主机4的公开密钥发送到OTA中心2。另外,OTA主机4收集车辆构成信息的工序也能够应用于其它的实施方式。OTA中心2基于从OTA主机4获取的OTA主机4的公开密钥和OTA中心2的秘密密钥获取ECDHE的算法的秘密密钥。

[0399] (11－2)OTA主机4的处理(参照图105～图108)

[0400] OTA主机4根据随机数生成ECDHE的密钥对(B111)。OTA主机4通过ECDHE的算法与OTA中心2共享秘密密钥(B112,相当于秘密信息共享步骤)。OTA主机4若由于在OTA主机4接收了从OTA中心2发送的活动通知而获取活动通知,则从该获取的活动通知中获取AES密钥(B113)。OTA主机4通过秘密密钥对已加密的AES密钥进行解密取出AES密钥(B114)。OTA主机4从CDN8下载并获取已加密的更新数据包(B115)。

[0401] 此时,OTA主机4与从CDN8下载并获取已加密的更新数据包并行地,通过AES密钥执行计数器值的AES块加密处理对计数器值进行加密(B116)。OTA主机4对已加密的计数器值、和从CDN8下载的已加密的更新数据包进行XOR运算来进行解密(B117)。OTA主机4将进行了解密的更新数据包转送至目标ECU5,将更新数据包安装于目标ECU5(B118)。

[0402] 如以上说明的那样根据第十一实施方式,能够得到以下的作用效果。

[0403] 构成为OTA中心2与OTA主机4之间的密钥配送采用DHE或者ECDHE,在OTA中心2中基于共享的按照每个车辆不同的秘密信息对AES密钥进行加密并分发给OTA主机4。由此,能够在适当地确保ECDHE的前向保密性的同时,适当地实现基于CDN8的更新数据的高效的分发。

[0404] (第十一实施方式的变形例)

[0405] 参照图166～图173对第十一实施方式的变形例进行说明。在第十一实施方式中,以无线通信装置搭载于车辆,OTA主机4能够经由无线通信线路与OTA中心2、CDN8发送接收数据为前提进行了说明。然而,也有无线通信装置未搭载于车辆的情况、用户不喜欢使用无线通信线路的情况。在第十一实施方式的变形例中,对OTA主机4不经由无线通信线路与OTA中心2、CDN8发送接收数据,而取而代之例如使用SD卡等存储介质实施程序更新的状况进行说明。

[0406] OTA主机4以及OTA中心2与外部的数据转送使用存储介质。OTA主机4与存储介质之间的数据转送使用设置于车辆的用于存储介质的端口。设置于车辆的端口例如是设置于车辆导航装置、中心显示器装置、其它的车辆控制装置的端口等。

[0407] 将存储介质与个人计算机(以下,称为PC)连接来进行OTA中心2与存储介质之间的数据转送。例如将存储介质与PC连接,向OTA中心2或者CDN8的网站进行访问,通过对PC进行操作将保存于存储介质的数据上传到OTA中心2,或者通过对PC进行操作将保存于OTA中心2的数据下载到存储介质。另外,也能够代替PC而使用与存储介质对应的智能手机、平板终端等。也将与存储介质对应的PC、智能手机、平板终端等称为操作终端。

[0408] 参照图166～图169,对使用了SD卡作为存储介质的情况进行说明。该情况下,按照从OTA主机4向SD卡11的数据的转送、从SD卡11向OTA中心2的数据的上传、从OTA中心2向SD卡11的数据的下载、从SD卡11向OTA主机4的数据的转送的顺序进行处理。

[0409] 参照图166,对从OTA主机4向SD卡11的数据的转送进行说明。OTA主机4从目标ECU5获取软件版本信息等,将该获取的软件版本信息等作为车辆构成信息转送并保存于SD卡11。OTA主机4根据随机数生成ECDHE的密钥对,并将ECDHE公开密钥转送并保存到SD卡11。SD卡11保存从OTA主机4转送的车辆构成信息以及OTA主机4的ECDHE公开密钥。

[0410] 参照图167,对从连接了SD卡11的PC向OTA中心2的数据的上传进行说明。PC若连接SD卡11,则读出保存于SD卡11的车辆构成信息以及OTA主机4的ECDHE公开密钥,并将该读出的车辆构成信息以及OTA主机4的ECDHE公开密钥上传至OTA中心2。上传到OTA中心2的车辆构成信息在PKG生成服务器6中使用于活动有无的判定。上传到OTA中心2的OTA主机4的ECDHE公开密钥在分发服务器7中基于ECDHE的算法共享秘密密钥。该情况下的秘密密钥是按照每个车辆不同的秘密密钥。

[0411] 参照图168,对从OTA中心2向SD卡11的数据的下载进行说明。这里示出有活动的情况。OTA中心2将通过AES密钥已加密的更新数据包下载并保存到SD卡11。OTA中心2根据随机数生成ECDHE的密钥对,并将应该与OTA主机4共享的密钥(OTA中心2的ECDHE公开密钥)下载并保存到SD卡11。OTA中心2将储存了已加密的AES密钥的活动通知下载并保存到SD卡11。SD卡11保存从OTA中心2下载的更新数据包、OTA中心2的ECDHE公开密钥以及已加密的AES密钥。

[0412] 参照图169,对从SD卡11向OTA主机4的数据的转送进行说明。OTA主机4从SD卡11读出并获取保存于SD卡11的已加密的更新数据包、OTA中心2的ECDHE公开密钥以及已加密的AES密钥。

[0413] 接下来,参照图170～图174对上述的构成的作用进行说明。

[0414] (11－3)OTA主机4的处理(参照图170)

[0415] 若SD卡11与车辆侧系统3连接,且满足规定条件,则OTA主机4向目标ECU5要求软件版本信息等构成信息的发送,并获取从目标ECU5发送的软件版本信息等构成信息作为车辆构成信息(B1111)。OTA主机4若获取车辆构成信息,则将该获取的车辆构成信息转送并保存到SD卡11(B1112)。OTA主机4根据随机数生成ECDHE的密钥对(B1113)。该情况下,密钥对包含OTA主机4的ECDHE公开密钥和ECDHE秘密密钥。OTA主机4将OTA主机4的ECDHE公开密钥转送并保存到SD卡11(B1114)。SD卡11若像这样保存车辆构成信息以及OTA主机4的ECDHE公开密钥,则解除与车辆侧系统3的连接,并与PC连接。

[0416] (11－4)PC的处理(参照图171)

[0417] PC若连接SD卡11,则读出保存于SD卡11的车辆构成信息以及OTA主机4的ECDHE公开密钥,并将该读出的车辆构成信息以及OTA主机4的ECDHE公开密钥上传至OTA中心2(C1111)。PC等待从OTA中心2接收OTA主机4的ECDHE公开密钥、储存AES密钥的活动通知、已加密的更新数据包,并且等待没有活动的通知的接收(C1112、C1113)。PC若判定为从OTA中心2接收了OTA主机4的ECDHE公开密钥、储存AES密钥的活动通知、已加密的更新数据包(C1112:是),或者若判定为接收了没有活动的通知(C1113:是),则结束处理。

[0418] (11－5)OTA中心2的处理(参照图172)

[0419] OTA中心2生成用于对更新数据包进行加密的AES密钥,并通过AES密钥以CTR模式对更新数据包进行加密。OTA中心2获取从连接有SD卡11的PC上传的车辆构成信息以及OTA主机4的ECDHE公开密钥(A1111)。OTA中心2基于车辆构成信息判定是否有活动(A1112)。OTA中心2若判定为没有活动(A1112:否),则向PC发送没有活动的通知(A1113),并结束处理。

[0420] OTA中心2若判定为有活动(A1112:是),则根据随机数生成ECDHE的密钥对(A1114)。该情况下,密钥对为OTA中心2的ECDHE公开密钥和ECDHE秘密密钥。OTA中心2将OTA中心2的ECDHE公开密钥下载并保存到SD卡11(A1115)。OTA中心2根据OTA中心2的ECDHE秘密密钥和OTA主机4的ECDHE公开密钥生成ECDHE公用密钥(秘密密钥)(A1116),并通过该生成的ECDHE公用密钥(秘密密钥)对AES密钥进行加密(A1117)。OTA中心2将该已加密的AES密钥储存于活动通知,并将储存了该已加密的AES密钥的活动通知下载并保存到SD卡11(A1118)。OTA中心2将已加密的更新数据包下载并保存到SD卡11(A1119)。

[0421] (11－6)OTA主机4的处理(参照图173)

[0422] 若SD卡11与车辆侧系统3连接,则OTA主机4从SD卡11获取OTA中心2的ECDHE公开密钥、活动通知、更新数据包(B1121)。OTA主机4根据OTA主机4的ECDHE秘密密钥和OTA中心2的ECDHE公开密钥生成ECDHE公用密钥(秘密密钥)(B1122)。OTA主机4从活动通知取出已加密的AES密钥,并通过ECDHE公用密钥(秘密密钥)进行解密(B1123)。OTA主机4通过AES密钥执行计数器值的AES块加密处理来对计数器值进行加密(B1124)。OTA主机4对已加密的计数器值与已加密的更新数据包进行XOR运算来进行解密(B1125)。OTA主机4将进行了解密的更新数据包转送至目标ECU5,将更新数据包安装于目标ECU5(B1126)。

[0423] 根据这样的构成,能够不依赖于车辆侧系统3的无线通信功能,而在适当地确保ECDHE的前向保密性的同时,适当地实现基于CDN8的更新数据的高效的分发。另外,通过抑制OTA主机4与SD卡11之间的数据转送、OTA中心2与SD卡11之间的上传、下载的次数,能够提高对于用户来说的便利性。

[0424] (第十二实施方式)

[0425] 参照图109～图115对第十二实施方式进行说明。第十二实施方式在ECDHE的密钥共享中,通过使OTA中心2生成的随机数a为每个车辆型号的随机数(基于特定的规则的随机数),并利用每个车辆型号的固定值,计数值,或者OTA主机4的软件版本的散列值的任意一个,或者它们的组合作为在OTA主机4生成的随机数b,在每个车辆型号共用通过ECDHE共享的秘密密钥,在享受确保ECDHE的前向保密性的优点的同时,省略配送密钥的处理,对各车辆型号或者特定的车辆组能够应用的加密数据包进行CDN分发。

[0426] 接下来,参照图110～图115对上述的构成的作用进行说明。

[0427] (12－1)OTA中心2的处理(参照图110～图112)

[0428] OTA中心2根据在每个车辆型号或者每个车辆组共用的随机数生成ECDHE的密钥对(A121)。OTA中心2通过ECDHE的算法与OTA主机4共享秘密密钥(A122,相当于秘密信息共享步骤)。在本实施方式中,通过ECDHE的算法与OTA主机4共享的秘密密钥作为用于对更新数据包进行加密的AES密钥使用。并且,OTA主机4使用与OTA中心2共享的秘密密钥,作为用于对已加密的更新数据包进行解密的AES密钥。OTA中心2生成用于对更新数据包进行加密的AES密钥(A123)。OTA中心2通过生成的AES密钥以CTR模式对更新数据包进行加密(A124)。OTA中心2将通过AES密钥已加密的更新数据包配置于CDN8(A125)。OTA中心2将储存了已加密的AES密钥的活动通知发送到重编对象的车辆侧系统3(A126,相当于加密密钥分发步骤)。

[0429] (12－2)OTA主机4的处理(参照图113～图115)

[0430] OTA主机4根据在上述进行了说明的根据特定的规则生成的随机数生成ECDHE的密钥对(B121)。OTA中心2通过ECDHE的算法与OTA中心2共享秘密密钥(B122,相当于秘密信息共享步骤)。OTA主机4从CDN8下载并获取已加密的更新数据包(B123)。

[0431] 此时,OTA主机4与从CDN8下载并获取已加密的更新数据包并行地,通过AES密钥执行计数器值的AES块加密处理来对计数器值进行加密(B124)。OTA主机4对已加密的计数器值、和从CDN8下载的已加密的更新数据包进行XOR运算来进行解密(B125)。OTA主机4将进行了解密的更新数据包转送至目标ECU5,将更新数据包安装于目标ECU5(B126)。

[0432] 如以上说明的那样根据第十二实施方式,能够得到以下的作用效果。

[0433] 构成为OTA中心2与OTA主机4之间的密钥配送采用DHE或者ECDHE,在每个车辆型号共用通过ECDHE共享的秘密密钥。由此,能够在适当地确保ECDHE的前向保密性的同时,与第十一实施方式相比简化密钥配送的工作,并且适当地实现基于CDN8的更新数据的高效的分发。

[0434] (第十二实施方式的变形例)

[0435] 参照图174～图181对第十二实施方式的变形例进行说明。在第十二实施方式的变形例中,也与第十一实施方式的变形例相同,对OTA主机4不经由无线通信线路与OTA中心2、CDN8发送接收数据,而取而代之例如使用SD卡等存储介质实施程序更新的状况进行说明。

[0436] 参照图174,对从OTA主机4向SD卡11的数据的转送进行说明。OTA主机4从目标ECU5获取软件版本信息等,并将该获取的软件版本信息等作为车辆构成信息转送并保存于SD卡11。OTA主机4利用每个车辆型号的固定值,计数值,或者OTA主机4的软件版本的散列值的任意一个,或者它们的组合生成在每个车辆型号共用的ECDHE的密钥对,并将应该与OTA中心2共享的密钥(OTA主机4的ECDHE公开密钥)转送并保存到SD卡11。每个车辆型号的固定值、计数值,或者OTA主机4的软件版本的散列值的任意一个,或者它们的组合相当于特定的规则。SD卡11保存从OTA主机4转送的车辆构成信息以及OTA主机4的ECDHE公开密钥。

[0437] 参照图175,对从连接了SD卡11的PC向OTA中心2的数据的上传进行说明。PC若连接SD卡11,则读出保存于SD卡11的车辆构成信息以及OTA主机4的ECDHE公开密钥,并将该读出的车辆构成信息以及OTA主机4的ECDHE公开密钥上传至OTA中心2。上传到OTA中心2的车辆构成信息在PKG生成服务器6中使用于活动有无的判定。另外,上传到OTA中心2的OTA主机4的ECDHE公开密钥在分发服务器7中基于ECDHE的算法共享秘密密钥。该情况下的秘密密钥

是每个车辆型号共用的秘密密钥。

[0438] 参照图176,对从OTA中心2向SD卡11的数据的下载进行说明。OTA中心2根据在每个车辆型号或者每个车辆组共用的随机数生成ECDHE的密钥对,并将应该与OTA主机4共享的密钥(OTA中心2的ECDHE公开密钥)下载并保存到SD卡11。OTA中心2通过使用通过ECDHE共享的秘密密钥作为AES密钥来对更新数据包进行加密,并将已加密的更新数据包下载并保存到SD卡11。SD卡11保存从OTA中心2下载的OTA中心2的ECDHE公开密钥、更新数据包。

[0439] 参照图177,对从SD卡11向OTA主机4的数据的转送进行说明。OTA主机4读出并获取保存于SD卡11的已加密的更新数据包以及OTA中心2的ECDHE公开密钥。OTA主机4基于ECDHE的算法共享秘密密钥。OTA主机4使用通过ECDHE共享的秘密密钥作为AES密钥,对已加密的更新数据包进行解密。

[0440] 接下来,参照图178～图181对上述的构成的作用进行说明。

[0441] (12－3)OTA主机4的处理(参照图178)

[0442] 若SD卡11与车辆侧系统3连接,且满足规定条件,则OTA主机4向目标ECU5要求软件版本信息等构成信息的发送,并获取从目标ECU5发送的软件版本信息等构成信息作为车辆构成信息(B1211)。OTA主机4若获取车辆构成信息,则将该获取的车辆构成信息转送并保存至SD卡11(B1212)。OTA主机4根据基于特定的规则生成的随机数生成ECDHE的密钥对(B1213)。该情况下,密钥对包含OTA主机4的ECDHE公开密钥和ECDHE秘密密钥。OTA主机4将OTA主机4的ECDHE公开密钥转送并保存至SD卡11(B1214)。ECDHE的密钥对与第十二实施方式相同是根据特定的规则生成的随机数且在每个车辆型号共用。SD卡11若像这样保存车辆构成信息以及OTA主机4的ECDHE公开密钥,则解除与车辆侧系统3的连接,并与PC连接。

[0443] (12－4)PC的处理(参照图179)

[0444] PC若连接SD卡11,则读出保存于SD卡11的车辆构成信息以及OTA主机4的ECDHE公开密钥,并将该读出的车辆构成信息以及OTA主机4的ECDHE公开密钥上传至OTA中心2(C1211)。PC等待从OTA中心2接收储存OTA主机4的ECDHE公开密钥的活动通知、已加密的更新数据包,并且等待没有活动的通知的接收(C1212,C1213)。PC若判定为从OTA中心2接收了储存OTA主机4的ECDHE公开密钥的活动通知、已加密的更新数据包(C1212:是),或者若判定为接收了没有活动的通知(C1213:是),则结束处理。

[0445] (12－5)OTA中心2的处理(参照图180)

[0446] OTA中心2获取从连接SD卡11的PC上传的车辆构成信息以及OTA主机4的ECDHE公开密钥(A1211)。OTA中心2基于车辆构成信息判定是否有活动(A1212)。OTA中心2若判定为没有活动(A1212:否),则向PC发送没有活动的通知(A1213),并结束处理。

[0447] OTA中心2若判定为有活动(A1212:是),则根据在每个车辆型号或者每个车辆组共用的随机数生成ECDHE的密钥对(A1214)。该情况下,密钥对是OTA中心2的ECDHE公开密钥和ECDHE秘密密钥。OTA中心2将OTA中心2的ECDHE公开密钥下载并保存到SD卡11(A1215)。OTA中心2根据OTA中心2的ECDHE秘密密钥和OTA主机4的ECDHE公开密钥生成ECDHE公用密钥(秘密密钥)(A1216),并通过该生成的ECDHE公用密钥(秘密密钥)对更新数据包进行加密(A1217)。OTA中心2将已加密的更新数据包下载并保存至SD卡11(A1218)。

[0448] (12－6)OTA主机4的处理(参照图181)

[0449] 若SD卡11与车辆侧系统3连接,则OTA主机4从SD卡11获取OTA中心2的ECDHE公开密

钥、更新数据包(B1221)。OTA主机4根据OTA主机4的ECDHE秘密密钥和OTA中心2的ECDHE公开密钥生成ECDHE公用密钥(秘密密钥)(B1222)。OTA主机4通过AES密钥执行计数器值的AES块加密处理来对计数器值进行加密(B1223)。OTA主机4对已加密的计数器值和已加密的更新数据包进行XOR运算来进行解密(B1224)。OTA主机4将进行了解密的更新数据包转送至目标ECU5,将更新数据包安装于目标ECU5(B1225)。

[0450] 根据这样的构成,能够不依赖于车辆侧系统3的无线通信功能,而在适当地确保ECDHE的前向保密性的同时,与第十一实施方式相比简化密钥配送的工作,并且适当地实现基于CDN8的更新数据的高效的分发。另外,通过抑制OTA主机4与SD卡11之间的数据转送、OTA中心2与SD卡11之间的上传、下载的次数,能够提高对于用户来说的便利性。

[0451] (第十三实施方式)

[0452] 参照图116～图124对第十三实施方式进行说明。第十三实施方式并不是简单地应用CTR模式,而通过对计数器值进行研究,使之更安全。具体而言,通过在OTA中心2与OTA主机4之间首次通信的活动通知中加入Nonce,在计数器值加入Nonce,实现CTR模式的安全化。CTR模式的加入Nonce的加密处理如图117所示,CTR模式的加入Nonce的解密处理如图118所示。

[0453] 接下来,参照图119～图124对上述的构成的作用进行说明。

[0454] (13—1)OTA中心2的处理(参照图119～图121)

[0455] OTA中心2生成用于对更新数据包进行加密的AES密钥(A131)。OTA中心2生成基于随机数的Nonce(A132)。OTA中心2通过生成的AES密钥和Nonce以CTR模式对更新数据包进行加密(A133)。OTA中心2通过RSA公开密钥对AES密钥进行加密(A134)。也可以OTA中心2在通过RSA公开密钥对AES密钥进行加密的同时,也通过RSA公开密钥对Nonce进行加密。OTA中心2将通过RSA公开密钥已加密的AES密钥和Nonce储存在活动通知中(A135)。OTA中心2将通过AES密钥已加密的更新数据包配置于CDN8(A136)。OTA中心2将储存了已加密的AES密钥和Nonce的活动通知发送到重编对象的车辆侧系统3(A137)。

[0456] (13—2)OTA主机4的处理(参照图122～图124)

[0457] OTA主机4若由于在OTA主机4接收了从OTA中心2发送的活动通知而获取活动通知,则从该获取的活动通知中获取AES密钥和Nonce(B131)。OTA主机4通过RSA秘密密钥对已加密的AES密钥进行解密取出AES密钥(B132)。OTA主机4从CDN8下载并获取已加密的更新数据包(B133)。OTA主机4通过AES密钥和Nonce对从CDN8下载的已加密的更新数据包进行解密(B134)。OTA主机4将进行了解密的更新数据包转送至目标ECU5,将更新数据包安装于目标ECU5(B135)。

[0458] 如以上说明的那样根据第十三实施方式,能够得到以下的作用效果。

[0459] 构成为在OTA中心2与OTA主机4之间首次通信的活动通知中加入Nonce,在计数器值加入Nonce。由此,通过在计数器值加入Nonce,能够实现CTR模式的安全化。

[0460] (第十四实施方式)

[0461] 参照图125～图132对第十四实施方式进行说明。第十四实施方式对于用于加密的密钥,为了缩小密钥危险化时的影响范围,不在全部的车辆使用共用的密钥,而使用按照特定的车辆组的单位个体化的派生密钥,从而在维持CDN8的分发缓存效率的同时使密钥泄漏时的损失局部化,更安全地进行OTA分发。如图126所示,针对同一车辆型号以及年款将VIN

编号划分为多个,且每个分区使用不同的AES专用密钥。例如按照VIN编号AAA～CCC、VIN编号DDD～KKK、VIN编号SSS～ZZZ进行划分,使用不同的AES专用密钥。专用密钥数据库例如包含OEM码、车辆型号、年款、AES主密钥、种子值、根据VIN编号划分的AES专用密钥。

[0462] 接下来,参照图127～图132对上述的构成的作用进行说明。

[0463] (14—1)OTA中心2的处理(参照图127～图129)

[0464] OTA中心2根据AES主密钥和种子值生成用于对更新数据包进行加密的AES专用密钥(A141)。种子值例如是随机数、计数器值、时间戳等。OTA中心2通过生成的AES专用密钥之一和Nonce以CTR模式对更新数据包进行加密(A142)。OTA中心2通过RSA公开密钥对AES专用密钥进行加密(A143)。OTA中心2将通过RSA公开密钥已加密的AES专用密钥和Nonce储存在活动通知中(A144)。OTA中心2将通过AES专用密钥之一和Nonce已加密的更新数据包配置于CDN8(A145)。OTA中心2将储存了已加密的AES专用密钥和Nonce的活动通知发送到重编对象的车辆侧系统3(A146)。

[0465] (14—2)OTA主机4的处理(参照图130～图132)

[0466] OTA主机4若由于在OTA主机4接收了从OTA中心2发送的活动通知而获取活动通知,则从该获取的活动通知中获取AES专用密钥和Nonce(B141)。OTA主机4通过RSA秘密密钥对已加密的AES专用密钥进行解密取出AES专用密钥(B142)。OTA主机4从CDN8下载并获取已加密的更新数据包(B143)。OTA主机4通过AES专用密钥和Nonce对从CDN8下载的已加密的更新数据包进行解密(B144)。OTA主机4将进行了解密的更新数据包转送至目标ECU5,将更新数据包安装于目标ECU5(B145)。

[0467] 如以上说明的那样根据第十四实施方式,能够得到以下的作用效果。

[0468] 构成为对于用于加密的密钥来说并不在全部的车辆中使用共用的密钥,而使用按照特定的车辆组的单位进行了个体化的派生密钥。能够在维持CDN8的分发缓存效率的同时使密钥泄漏时的损失局部化。由此,能够提高OTA主机4从OTA中心2下载更新数据包时的安全性,能够实现更安全的OTA分发。

[0469] (第十五实施方式)

[0470] 参照图133～图137对第十五实施方式进行说明。第十五实施方式防备作为最差的事态的秘密密钥泄漏的情况而附加密钥版本在OTA中心2中进行管理,并且在OTA主机的HSM区域储存密钥更新用密钥以能够在OTA进行密钥更新。OTA中心2管理AES密钥的加密所使用的RSA公开密钥和其解密所使用的RSA秘密密钥的版本信息。通过管理版本信息,在更新RSA秘密密钥以及RSA公开密钥时不会降级。OTA中心2和OTA主机4具备在秘密密钥的更新时使用的密钥更新用密钥。在OTA中心2中,在秘密密钥泄漏时或者以定期间隔生成新的秘密密钥对,并且使用密钥更新用密钥生成密钥更新数据包,并将密钥更新数据包发送至OTA主机4,从而实现秘密密钥的密钥更新。

[0471] 接下来,参照图134～图137对上述的构成的作用进行说明。

[0472] (15—1)OTA中心2的处理(参照图134～图135)

[0473] OTA中心2生成新RSA秘密密钥和新RSA公开密钥的新的密钥对(A151)。OTA中心2通过密钥更新用密钥以CTR模式对生成的新RSA秘密密钥进行加密以及MAC运算,生成密钥更新数据包(A152)。OTA中心2将旧RSA公开密钥切换为新RSA公开密钥(A153)。OTA中心2将密钥更新数据包发送到重编对象的车辆侧系统3(A154)。

[0474] (15—2)OTA主机4的处理(参照图136～图137)

[0475] OTA主机4获取密钥更新数据包,通过密钥更新用密钥以CTR模式对新RSA秘密密钥进行解密以及MAC验证(B151)。OTA主机4将旧RSA秘密密钥切换为进行了解密的新RSA秘密密钥(B152)。

[0476] 如以上说明的那样根据第十五实施方式,能够得到以下的作用效果。

[0477] 构成为在秘密密钥泄漏时或者以定期间隔生成新的秘密密钥对,并且使用密钥更新用密钥生成密钥更新数据包,并将密钥更新数据包发送到OTA主机4。由此,通过进行秘密密钥的密钥更新,能够提高OTA主机4从OTA中心2下载更新数据包时的安全性,能够实现更安全的OTA分发。

[0478] (第十六实施方式)

[0479] 参照图138～图145对第十六实施方式进行说明。第十六实施方式在ECDHE的密钥共享时,为了对抗中间人攻击而安全地对附加数字签名且能够应用于加密数据包的密钥实现OTA中心2与OTA主机4之间的密钥共享。如图139～图140所示,DHE对于来自中间攻击者的攻击较脆弱,但通过附加数字签名对抗来自中间攻击者的攻击。作为数字签名使用使用了RSA或者椭圆曲线DSA的加密算法的数字签名。

[0480] 接下来,参照图141～图145对上述的构成的作用进行说明。

[0481] (16—1)OTA中心2的处理(参照图141～图143)

[0482] OTA中心2根据按照车辆型号或者按照车辆组制成的随机数生成ECDHE的密钥对(A161)。OTA中心2通过RSA秘密密钥对ECDHE密钥附加数字签名(A162)。这里,虽然是RSA秘密密钥,但并不限定于RSA秘密密钥,只要是公开密钥加密方式则能够代替,例如也可以是ECDSA(Elliptic Curve Digital Signature Algorithm:椭圆曲线数字签名算法)秘密密钥。OTA中心2将附加了数字签名的ECDHE公开密钥发送到重编对象的车辆侧系统3(A163)。OTA中心2通过ECDHE的算法与OTA主机4共享秘密密钥(A164)。OTA中心2生成用于对更新数据包进行加密的AES密钥(A165)。OTA中心2通过生成的AES密钥以CTR模式对更新数据包进行加密(A166)。OTA中心2将通过AES密钥已加密的更新数据包配置于CDN8(A167)。OTA中心2将储存了已加密的AES密钥的活动通知发送到重编对象的车辆侧系统3(A168)。

[0483] (16—2)OTA主机4的处理(参照图144～图145)

[0484] OTA主机4根据基于特定的规则生成的随机数生成ECDHE的密钥对(B161)。OTA主机4通过RSA公开密钥对从OTA中心2接收的ECDHE公开密钥进行数字签名验证(B162)。这里也与OTA中心2相同,并不限定于RSA公开密钥,只要是公开密钥加密方式则能够代替,例如也可以是ECDSA公开密钥。若验证结果正确,则OTA主机4通过ECDHE的算法与OTA中心2共享秘密密钥(B163)。其以后,OTA主机4进行在第十一实施方式中进行了说明的步骤B113以后的处理。

[0485] 如以上说明的那样根据第十六实施方式,能够得到以下的作用效果。

[0486] 构成为在ECDHE的密钥共享时附加数字签名。由此,通过附加数字签名,能够对抗来自中间攻击者的攻击,能够实现更安全的OTA分发。

[0487] (第十六实施方式的变形例)

[0488] 参照图182～图189对第十六实施方式的变形例进行说明。在第十六实施方式的变形例中,也与第十一实施方式以及第十二实施方式的变形例相同,对OTA主机4不经由无线

通信线路与OTA中心2、CDN8发送接收数据,而取而代之例如使用SD卡等存储介质实施程序更新的状况进行说明。第十六实施方式的变形例中的与第十二实施方式的变形例的主要的不同在于通过利用公开密钥加密方式的密钥对OTA中心2的ECDHE公开密钥实施数字签名来对抗来自中间攻击者的攻击这一点。

[0489] 在图182～图185中,分别示出从OTA主机4向SD卡11的数据的转送、从连接了SD卡11的PC向OTA中心2的数据的上传、从OTA中心2向SD卡11的数据的下载、从SD卡11向OTA主机4的数据的转送。与第十二实施方式的变形例的主要的不同如图184所示,OTA中心2通过公开密钥加密方式的密钥,例如RSA秘密密钥或者ECDSA秘密密钥对应该与OTA主机4共享的密钥(OTA中心2的ECDHE公开密钥)附加数字签名。OTA中心2将带签名的ECDHE公开密钥转送并保存到SD卡11。另外,如图185所示,OTA主机4从SD卡11读出带签名的ECDHE公开密钥,并使用保存于车辆侧系统3的RSA公开密钥进行验证。

[0490] 接下来,参照图186～图189对上述的构成的作用进行说明。

[0491] (16－3)OTA主机4的处理(参照图186)

[0492] 若SD卡11与车辆侧系统3连接,且满足规定条件,则OTA主机4向目标ECU5要求软件版本信息等构成信息的发送,并获取从目标ECU5发送的软件版本信息等构成信息作为车辆构成信息(B1611)。OTA主机4若获取车辆构成信息,则将该获取的车辆构成信息转送并保存至SD卡11(B1612)。OTA主机4根据基于特定的规则生成的随机数生成ECDHE的密钥对(B1613)。该情况下,密钥对包含OTA主机4的ECDHE公开密钥和ECDHE秘密密钥。OTA主机4将OTA主机4的ECDHE公开密钥转送并保存至SD卡11(B1614)。ECDHE的密钥对与第十二实施方式相同是根据特定的规则生成的随机数且对每个车辆型号共用。SD卡11若像这样保存车辆构成信息以及OTA主机4的ECDHE公开密钥,则解除与车辆侧系统3的连接,并与PC连接。

[0493] (16－4)PC的处理(参照图187)

[0494] PC若连接SD卡11,则读出保存于SD卡11的车辆构成信息以及OTA主机4的ECDHE公开密钥,并将该读出的车辆构成信息以及OTA主机4的ECDHE公开密钥上传至OTA中心2(C1611)。PC等待从OTA中心2接收储存OTA主机4的ECDHE公开密钥的活动通知、已加密的更新数据包,并且等待没有活动的通知的接收(C1612,C1613)。PC若判定为从OTA中心2接收了储存OTA主机4的ECDHE公开密钥的活动通知、已加密的更新数据包(C1612:是),或者若判定为接收了没有活动的通知(C1613:是),则结束处理。

[0495] (16－5)OTA中心2的处理(参照图188)

[0496] OTA中心2获取从连接SD卡11的PC上传的车辆构成信息以及OTA主机4的ECDHE公开密钥(A1611)。OTA中心2基于车辆构成信息判定是否有活动(A1612)。OTA中心2若判定为没有活动(A1612:否),则向PC发送没有活动的通知(A1613),并结束处理。

[0497] OTA中心2若判定为有活动(A1612:是),则根据在每个车辆型号或者每个车辆组共用的随机数生成ECDHE的密钥对(A1614)。该情况下,密钥对是OTA中心2的ECDHE公开密钥和ECDHE秘密密钥。OTA中心2通过RSA秘密密钥对OTA中心2的ECDHE公开密钥进行签名(A1615),并将签名完毕的OTA中心2的ECDHE公开密钥下载并保存至SD卡11(A1616)。OTA中心2根据OTA中心2的ECDHE秘密密钥和OTA主机4的ECDHE公开密钥生成ECDHE公用密钥(秘密密钥)(A1617),并通过该生成的ECDHE公用密钥(秘密密钥)对更新数据包进行加密(A1618)。OTA中心2将已加密的更新数据包下载并保存到SD卡11(A1619)。

[0498] (16－6)OTA主机4的处理(参照图189)

[0499] 若SD卡11与车辆侧系统3连接,则OTA主机4从SD卡11获取签名完毕的OTA中心2的ECDHE公开密钥、更新数据包(B1621)。OTA主机4通过RSA公开密钥对签名完毕的OTA中心2的ECDHE公开密钥进行验证(B1622)。OTA主机4判定验证结果是否正常(B1623),若判定为验证结果不正常而异常(B1623:否),则进行错误通知(B1624)。

[0500] OTA主机4若判定为验证结果正常(B1623:是),则根据OTA主机4的ECDHE秘密密钥和OTA中心2的ECDHE公开密钥生成ECDHE公用密钥(秘密密钥)(B1625)。OTA主机4通过AES密钥执行计数器值的AES块加密处理来对计数器值进行加密(B1626)。OTA主机4对已加密的计数器值、和已加密的更新数据包进行XOR运算来进行解密(B1627)。OTA主机4将进行了解密的更新数据包转送至目标ECU5,将更新数据包安装于目标ECU5(B1628)。

[0501] 根据这样的构成,能够不依赖于车辆侧系统3的无线通信功能,而对抗来自中间攻击者的攻击,能够实现更安全的OTA分发。另外,通过抑制OTA主机4与SD卡11之间的数据转送、OTA中心2与SD卡11之间的上传、下载的次数,能够提高对于用户来说的便利性。

[0502] (第十七实施方式)

[0503] 参照图146～图151对第十七实施方式进行说明。第十实施方式构成为按照区域从多个CDN供应商选定分发成本最小的CDN供应商,但第十七实施方式构成为静态地从多个CDN供应商选定能够降低分发成本的CDN供应商。具体而言,第十实施方式在OTA中心2对更新数据包进行加密之后,根据分发方式、OTA对象区域、分发数据大小使分发成本最小,然而第十七实施方式不在OTA中心2对更新数据包进行加密,而在通过TLS通信保护CDN8与OTA主机4之间之后,根据分发方式、OTA对象区域、分发数据大小使分发成本最小。

[0504] 接下来,参照图147～图151对上述的构成的作用进行说明。

[0505] (17－1)OTA中心2的处理(参照图147～图148)

[0506] OTA中心2确定分发方式(A171),确定OTA对象区域(A172),确定对车辆的通信协议是否使用TLS(A173),确定分发数据大小(A174),并以分发方式、OTA对象区域、通信协议以及分发数据大小为关键词从CDN供应商管理数据库参照价格表格(A175)。该情况下,也可以OTA中心2以分发方式、OTA对象区域、通信协议以及分发数据大小中至少任意一个为关键词参照价格表格。OTA中心2按照区域选定分发成本最小的CDN供应商,并将更新数据包配置于该选定的CDN8(A176)。OTA中心2将活动通知发送到重编对象的车辆侧系统3(A177)。

[0507] (17－2)OTA主机4的处理(参照图149～图151)

[0508] OTA主机4通过在OTA主机4接收从OTA中心2发送的活动通知而获取活动通知(B171)。OTA主机4为了获取更新数据包而与活动通知所记载的CDN供应商建立TLS通信(B172)。另外,若在活动通知记载有URI信息,则也可以不记载CDN供应商的信息。OTA主机4在建立了TLS通信之后,通过TLS通信协议交换AES的公用密钥。协商选择AES－CTR模式作为加密模式。OTA主机4基于URI信息从CDN8下载并获取通过TLS的AES公用密钥已加密的更新数据包(B173,相当于更新数据获取步骤)。

[0509] 此时,OTA主机4与从CDN8下载并获取已加密的更新数据包并行地,通过AES密钥执行计数器值的AES块加密处理对计数器值进行加密(B174)。OTA主机4对已加密的计数器值、和从CDN8下载的已加密的更新数据包进行XOR运算来进行解密(B175)。OTA主机4将进行了解密的更新数据包转送至目标ECU5,将更新数据包安装于目标ECU5(B176)。

[0510] 如以上说明的那样根据第十七实施方式,能够得到以下的作用效果。

[0511] 构成为不在OTA中心2对更新数据包进行加密,而在通过TLS通信保护CDN8与OTA主机4之间之后,根据分发方式、OTA对象区域、通信协议以及分发数据大小使分发成本最小。由此,能够适当地抑制OTA主机4从OTA中心2下载更新数据包时的分发成本。

[0512] (第十八实施方式)

[0513] 参照图152～图165第十八实施方式进行说明。第十八实施方式不仅考虑分发成本,而在综合地考虑CDN供应商的吞吐量、响应延迟时间等的基础上,选定最佳的CDN供应商,并且定期地检查CDN供应商的价格表格和质量特性,始终将CDN供应商管理数据库保持为最新的状态,始终选定在市场上最具有竞争优势性的CDN供应商。价格表格如图153～图160所示,各云服务运营商的质量信息如图161所示。如图162所示,若对CDN供应商A与CDN供应商B进行比较,则在分发成本这一点CDN供应商B优于CDN供应商A,但在吞吐量的加权以及响应延迟时间的加权这一点CDN供应商A优于CDN供应商B。若不仅考虑分发成本,而综合地考虑CDN供应商的吞吐量、响应延迟时间等,则能够导出不应该选定仅分发成本有优势的CDN供应商B,而应该选定在综合地考虑了CDN供应商的吞吐量、响应延迟时间等的基础上占优势的CDN供应商A的结论。

[0514] 接下来,参照图163～图165对上述的构成的作用进行说明。

[0515] (18－1)OTA中心2的处理(参照图163～图165)

[0516] OTA中心2确定分发方式(A181),确定OTA对象区域(A182),并以分发方式以及OTA对象区域为关键词从CDN供应商管理数据库参照价格表格(A183)。该情况下,OTA中心2也可以以分发方式以及OTA对象区域中至少任意一个为关键词参照价格表格。OTA中心2从CDN供应商管理数据库确定各CDN供应商的质量特性(A184)。OTA中心2基于每个区域的CDN供应商的分发成本以及质量特性,根据登记于CDN供应商选定逻辑数据库的CDN供应商选定逻辑按照区域选定最佳的CDN供应商,并将通过AES密钥已加密的更新数据包配置于该选定的CDN8(A185)。OTA中心2将储存了已加密的AES密钥的活动通知发送到重编对象的车辆侧系统3(A186)。

[0517] OTA中心2从网站自动获取各CDN供应商的价格表格,并更新CDN供应商管理数据库(A187)。OTA中心2测量各CDN供应商的吞吐量以及响应延迟时间,并更新CDN供应商管理数据库(A188)。例如分发服务器7定期地浏览各CDN供应商的网站并下载最新的价格表格。或者,分发服务器7在CDN供应商分发网站的更新信息的情况下,通过登录该分发服务,下载最新的价格表格。

[0518] (18－2)OTA主机4的处理

[0519] OTA主机4的处理与在第一实施方式中进行了说明的OTA主机4的处理(图12～图14)相同。

[0520] 如以上说明的那样根据第十八实施方式,能够得到以下的作用效果。

[0521] 不仅考虑分发成本,而在综合地考虑CDN供应商的吞吐量、响应延迟时间等的基础上,选定最佳的CDN供应商,并且定期地检查CDN供应商的价格表格和质量特性,始终将CDN供应商管理数据库保持为最新的状态,始终选定在市场上最具有竞争优势性的CDN供应商。由此,能够适当地抑制OTA主机4从OTA中心2下载更新数据包时的分发成本。

[0522] 另外,作为CDN的质量特性,并不限定于吞吐量、响应延迟时间,也能够考虑内容的

缓存命中率、过去的故障实绩等,能够使它们包含于CDN供应商管理数据库。另外,也能够定期地重新实施OTA中心2的连接目的地的CDN供应商的追加、删除,而与具有市场竞争力的CDN供应商连接。

[0523] (第十九实施方式)

[0524] 参照图90、图190～图193对第十九实施方式进行说明。上述的第十实施方式构成为按照区域从多个CDN供应商选定分发成本最小的CDN供应商。在第十九实施方式中,对CDN供应商的选定进行具体的说明。在第十九实施方式中,根据分发数据大小、作为分发区域的OTA对象区域(有时也称为地区(region))、分发方式从多个CDN供应商中动态地选定分发成本最小的CDN供应商,作为更新数据包的向CDN8的配置目的地。在第十九实施方式中,参照在上述的图90中进行了例示的价格表格进行说明。价格表格也可以是与图90不同的样式。

[0525] 如图190所示,在OTA中心2中,分发服务器7除了CDN供应商管理DB之外,还具备CDN供应商选定部7a、数据保存部7b、活动通知生成部7c、以及CDN分发部7d。CDN供应商选定部7a基于CDN供应商的选定所需要的信息亦即选定信息以及更新数据包的信息选定CDN供应商。在选定信息包含有与对象活动的数据大小、对象活动的分发对象车辆的台数、地区、分发方式相关的信息等。数据保存部7b除了保存活动信息之外,还保存能够识别通过CDN供应商选定部7a选定的CDN供应商的识别信息。在识别信息例如包含有CDN供应商的名称、确定CDN供应商的识别编号或者表示CDN供应商的URL等。活动通知生成部7c从数据保存部7b获取信息并生成分发给车辆等的活动通知。

[0526] CDN分发部7d具备与各CDN供应商对应的储存区域。例如储存区域具备储存区域A、储存区域B、储存区域C。CDN分发部7d的各储存区域与CDN服务器同步。即,CDN分发部7d例如在使数据从CDN服务器A分发到车辆侧系统3的情况下,将数据配置于储存区域A并转送至CDN服务器A。CDN服务器A若从CDN分发部7d转送数据,则将该转送的数据分发给车辆侧系统3。有时CDN分发部7d的各储存区域称为各CDN服务器的原始服务器。

[0527] 接下来,参照图191～图193对上述的构成的作用进行说明。另外,OTA中心2的更新数据包的加密等处理与第十实施方式或者其它的实施方式相同。另外,OTA主机4的处理与第一实施方式或者其它的实施方式相同。在第十九实施方式中,主要对CDN供应商的选定进行说明。

[0528] (19－1)活动通知生成部7c的处理(参照图191)

[0529] 若产生活动,则活动通知生成部7c例如从OEM服务器等外部获取活动信息(A191)。在活动信息包含有与对象活动的数据大小、对象活动的分发对象车辆的台数、地区、分发方式相关的信息。活动通知生成部7c将该获取的活动信息保存于数据保存部7b(A192)。有时将保存活动信息称为配置活动信息。

[0530] 活动通知生成部7c向CDN供应商选定部7a通知CDN供应商的选定要求(A193),并对来自CDN供应商选定部7a的选定通知的获取进行待机。活动通知生成部7c若从CDN供应商选定部7a获取选定通知(A194),则访问数据保存部7b,获取通过该CDN供应商选定部7a选定的CDN供应商的识别信息(A195)。

[0531] 活动通知生成部7c基于CDN供应商的识别信息生成包含该选定的CDN的URL的参数文件作为活动通知(A196)。活动通知生成部7c将该生成的活动通知分发给车辆侧系统3(A197)。

[0532] (19—2)CDN供应商选定部7a的处理(参照图192～图193)

[0533] CDN供应商选定部7a若获取从活动通知生成部7通知的CDN供应商的选定要求(A1911),则访问数据保存部7b,获取选定信息(A1912),并移至第一CDN选定处理(A1913)。

[0534] CDN供应商选定部7a若开始第一CDN选定处理,则计算表示从CDN服务器向更新对象车辆分发的数据大小的分发数据大小(A1921)。具体而言,CDN供应商选定部7a将对象活动的数据大小与该对象活动的分发对象车辆的台数相乘,计算预定从CDN服务器分发的分发数据大小。

[0535] CDN供应商选定部7a对每个CDN供应商反复以后的处理(A1922～A1929)。CDN供应商选定部7a基于先前计算出的分发数据大小以及与地区相关的地区信息从CDN供应商管理DB获取费用信息(A1923)。CDN供应商选定部7a例如在以北美为对象的30TB的活动的情况下,获取“北美”地区的“～10TB”和“～40TB”的费用信息。也可以对全部的数据大小获取费用信息。

[0536] CDN供应商选定部7a基于分发数据大小参照费用信息,计算分发收费额(A1924)。分发收费额的计算有按照CDN供应商而不同的可能性,根据CDN供应商中的分发收费额的计算方法决定。例如在根据图90的价格表格计算CDN1分发收费额的情况下,在地区为“北美”,分发数据大小为30TB的情况下,参照“～10TB”和“～40TB”的价格表格。

[0537] CDN供应商选定部7a判定研究对象的CDN供应商是否是进行与请求数对应的收费的CDN供应商(A1925)。CDN供应商选定部7a若判定为是不进行与请求数对应的收费的CDN供应商(A1925:否),则将分发收费额决定为CDN供应商的收费额(A1928),并结束该CDN供应商的收费额的计算,计算下一个CDN供应商的收费额。

[0538] CDN供应商选定部7a若判定为是进行与请求数对应的收费的CDN供应商(A1925:是),则计算请求数(A1926)。请求数根据分发方式而不同。在分发方式为储存方式的情况下,将活动的分发对象车辆的台数作为请求数。在分发方式为流式传输方式的情况下,将对象活动的数据大小除以流式传输时的组块大小,并与活动的分发对象车辆的台数相乘来计算请求数。

[0539] CDN供应商选定部7a若计算出请求数,则基于该计算出的请求数计算收费额(有时称为请求收费额)(A1927)。请求收费额是每个请求的收费额与请求数的乘积。CDN供应商选定部7a将分发收费额与请求收费额相加后的合计金额决定为CDN供应商的收费额(A1928),并结束研究对象的CDN供应商的收费额的计算,计算下一个CDN供应商的收费额。

[0540] CDN供应商选定部7a若对全部的CDN供应商计算出收费额,则选定分发成本最小的CDN供应商,即收费额最便宜的CDN供应商(A1930),并结束第一CDN选定处理。CDN供应商选定部7a若结束第一CDN选定处理,则将其选定结果即选定的CDN供应商的识别信息保存于数据保存部7b(A1914),并将选定结果通知给活动通知生成部7c(A1915)。

[0541] 如以上说明的那样根据第十九实施方式,能够得到以下的作用效果。

[0542] 构成为在分发服务器7中,参照CDN供应商管理DB,根据分发方式、OTA对象区域以及分发数据大小从分发成本不同的多个CDN8中选定分发成本有优势的CDN8,并将更新数据包配置于该选定的CDN8。由此,能够适当地抑制OTA主机4从OTA中心2下载更新数据包时的分发成本。

[0543] (第十九实施方式的变形例)

[0544] 参照图194～图211对第十九实施方式的变形例进行说明。这里,对第一变形例～第五变形例进行说明。

[0545] (第十九实施方式的第一变形例)

[0546] 参照图194～图195对第十九实施方式的第一变形例进行说明。第一变形例构成为通过使用DNS(域名系统)服务器,不变更向车辆侧系统3分发的活动通知所包含的CDN服务器的URL。在第十九实施方式中,对每个活动选定分发成本最小的CDN供应商。在活动通知包含有CDN服务器的URL。因此,若分发成本最小的CDN供应商变更,则活动通知所记载的URL变更。活动通知生成部7c每当生成活动通知则需要访问数据保存部7b获取CDN供应商的信息。

[0547] 与此相对,在第一变形例中,通过更新通过DNS设定部7e登记于DNS的URL和IP地址的转换信息,活动通知生成部7c能够始终在活动通知记载相同的URL。在分发成本最小的CDN供应商变更的情况下,通过变更DNS服务器12的信息,车辆侧系统3能够访问选定的CDN服务器。换句话说,在第十九实施方式中,各CDN服务器具有固有的IP地址,具有固有的URL。与此相对,在第一变形例中,特征在于各CDN服务器虽然具有固有的IP地址,但具有在CDN服务器中共用的URL。

[0548] 如图194所示,在OTA中心2,分发服务器7除了CDN供应商管理DB、CDN供应商选定部7a、数据保存部7b、活动通知生成部7c、以及CDN分发部7d之外,还具备DNS设定部7e。以下主要对与第十九实施方式不同的点进行说明。

[0549] DNS服务器12是提供对域名与IP地址进行转换的结构的服务器。在车辆侧系统3接收的活动通知包含有为了下载数据而访问的CDN服务器的URL。车辆侧系统3若接收活动通知,则向DNS服务器12询问该接收的活动通知所示出的URL。DNS服务器12将对于获取了询问的URL的IP地址发送至车辆侧系统3,或者将连接目的地转送到根据IP地址指定的地址。

[0550] DNS设定部7e保存CDN供应商的识别信息和IP地址。若通过CDN供应商选定部7a选定CDN供应商,则DNS设定部7e向DNS服务器12发送IP地址设定要求,设定在DNS的登记信息。

[0551] 接下来,参照图195对上述的构成的作用进行说明。

[0552] (19－3)CDN供应商选定部7a的处理(参照图195)

[0553] CDN供应商选定部7a若结束第一CDN选定处理,并将选定结果保存于数据保存部7b(A1914),则使IP地址设定要求从DNS设定部7e发送到DNS服务器12,通过DNS设定部7e设定在DNS的登记信息(A1931)。由此,即使CDN供应商变更,分发到车辆侧系统3的活动通知所包含的URL也不变更。在车辆侧系统3访问根据URL示出的CDN服务器时,DNS服务器12获取IP地址的询问,并将选定的CDN服务器的IP地址发送给车辆侧系统3。

[0554] 另外,DNS设定部7e也可以获取DNS服务器12的信息,或者保存上一次的向DNS服务器12的设定信息,在登记于DNS服务器12的CDN服务器与CDN供应商选定部7a选定的CDN服务器不同的情况下,向DNS服务器12发送IP地址的更新要求。活动通知生成部7c若从CDN供应商选定部7a获取选定通知,则生成包含固定的URL的活动通知。

[0555] 根据这样的构成,除了得到与第十九实施方式相同的作用效果之外,还能够使活动通知所包含的CDN的URL信息始终相同,能够提高安全。

[0556] (第十九实施方式的第二变形例)

[0557] 参照图196～图201对第十九实施方式的第二变形例进行说明。即使选择更新数据包的分发成本最小的CDN供应商,也有由于CDN服务器的维护、故障、访问集中等而通信速度

变慢的担心。本申请发明者们关注于基于分发成本和分发性能选择CDN供应商。

[0558] 在第二变形例中,在车辆侧系统3为了获取与活动通知所示出的URL对应的IP地址而询问DNS服务器12时,DNS服务器12确认CDN服务器的分发状况,若判定为不可分发,则向车辆侧系统3回答分发成本其次便宜的CDN服务器的IP地址。

[0559] 如图196所示,在OTA中心2,分发服务器7除了CDN供应商管理DB、CDN供应商选定部7a、数据保存部7b、活动通知生成部7c、CDN分发部7d、以及DNS设定部7e之外,还具备性能测定部7f。DNS服务器12具备CDN服务器确认部12a。在CDN分发部7d的储存区域配置有用于测定CDN服务器的性能的测试文件。性能测定部7f向CDN服务器发送测试文件的分发要求,使测试文件从CDN服务器分发,并测定测试文件的分发所需要的时间作为分发时间。分发时间例如是从开始测试文件的分发的时刻起到确定了测试文件的接收完成的时刻为止的时间。

[0560] 如图197所示,CDN供应商管理DB具备CDN服务器的选择表格。选择表格包含通过CDN供应商选定部7a决定的成本位次、和通过性能测定部7f判定出的分发标志。

[0561] 性能测定部7f对各CDN服务器根据测试文件的分发所需要的时间计算响应速度,并将基于该计算出的响应速度的判定结果输入到选择表格。性能测定部7f在响应速度在规定值以上的情况下,将该CDN服务器的分发标志设定为打开(TRUE),在响应速度小于规定值的情况下,将该CDN服务器的分发标志设定为关闭(FALSE)。

[0562] CDN服务器确认部12a在从车辆侧系统3获取了与URL对应的IP地址的询问时,判定根据URL指定的CDN服务器是否为能够分发的状态,若判定为不可分发,则回答其它的CDN服务器的IP地址。

[0563] 接下来,参照图198～图201对上述的构成的作用进行说明。

[0564] (19—4)CDN供应商选定部7a的处理(参照图198～图199)

[0565] CDN供应商选定部7a若在第一CDN选定处理中,对每个CDN供应商计算出收费额(A1921～A1929),则决定CDN供应商的成本位次(A1951)。即,CDN供应商选定部7a将分发成本最小的CDN供应商的位次决定为第一位,将分发成本其次便宜的CDN供应商的位次决定为第二位。CDN供应商选定部7a若将选定结果保存于数据保存部7b(A1914),则在CDN供应商管理DB的选择表格保存成本位次(A1941)。

[0566] (19—5)性能测定部7f的处理(参照图200)

[0567] 性能测定部7f对每个CDN供应商反复以后的处理(A1961～A1966)。性能测定部7f在分发服务器7启动中以恒定间隔或者通过分发服务器7的管理者在任意的时刻执行以后的处理。

[0568] 性能测定部7f访问CDN服务器(A1962),向CDN服务器发送测试文件的分发要求。性能测定部7f基于测试文件的分发所需要的时间计算响应速度,并判定该计算出的响应速度是否在规定值以上(A1963)。另外,也可以不计算响应速度而将分发所需要的时间与规定值比较,也可以将每个单位时间的分发数据大小与规定值进行比较。

[0569] 性能测定部7f若判定为响应速度在规定值以上(A1963:是),则判定为该CDN服务器是能够利用于分发的服务器,将分发标志设定为打开(A1964)。性能测定部7f若判定为该计算出的响应速度小于规定值(A1963:否),则判定为该CDN服务器是不能够利用于分发的服务器,而将分发标志设定为关闭(A1965)。

[0570] (19—6)CDN服务器确认部12a的处理(参照图201)

[0571] 在活动通知示出为了下载更新数据而访问的URL。车辆侧系统3对DNS服务器12询问为了下载更新数据包应该访问的IP地址。

[0572] CDN服务器确认部12a从车辆侧系统3对活动通知示出的URL获取IP地址的询问(A1971)。CDN服务器确认部12a向分发服务器7的CDN供应商管理DB查询活动通知所示出的CDN服务器的分发状况(A1972)。该情况下,CDN服务器相当于数据获取预定的CDN供应商,分发状况相当于分发标志。CDN服务器确认部12a若从分发服务器获取数据获取预定的CDN供应商的分发标志,则判定数据获取预定的CDN供应商是否能够使用(A1973)。即,CDN服务器确认部12a判定该获取的分发标志是打开或者关闭的哪一个。

[0573] CDN服务器确认部12a若判定为分发标志打开(A1973:是),则向车辆侧系统3回答与该CDN供应商对应的IP地址,或者将与车辆侧系统3的连接转送至该IP地址,切换为与活动通知的URL对应的CDN供应商(A1974)。CDN服务器确认部12a若判定为分发标志关闭(A1973:否),则将成本位次其次高的CDN供应商作为下一个优先级的CDN供应商,将下一个优先级的CDN供应商设定为数据获取预定的CDN供应商(A1975),并返回到步骤A1973。

[0574] 根据这样的构成,能够在尽量抑制分发成本的同时,选择正常运转的CDN服务器。另外,CDN服务器确认部12a也可以每经过恒定期间,则访问CDN供应商管理DB,要求选择表格的发送。该情况下,在从车辆侧系统3获取了IP地址的询问的情况下,也可以代替访问CDN供应商管理DB,而参照CDN服务器确认部12a保持的选择表格来判定数据获取预定的CDN供应商是否能够使用。另外,除了在尽量抑制分发成本的同时,选择正常运转的CDN服务器之外,还能够减少DNS服务器12与分发服务器7之间的通信。

[0575] (第十九实施方式的第三变形例)

[0576] 参照图202～图205对第十九实施方式的第三变形例进行说明。第三变形例在分发服务器7中,性能测定部7f基于来自车辆侧系统3的日志信息测定并评价CDN服务器的性能。另外,DNS服务器12从车辆侧系统3获取了对URL的IP地址的询问的情况下的动作与第二变形例相同。在第三变形例中也与第二变形例相同,CDN供应商管理DB具备选择表格。

[0577] 车辆侧系统3具备日志发送部3a。若结束从CDN服务器的更新数据的下载,则日志发送部3a向分发服务器7的性能测定部7f发送包含表示下载所需要的时间的下载时间的与下载相关的日志信息。与下载相关的日志信息也可以除了下载时间之外,还包含下载的数据包的识别信息、数据大小、下载中的最大吞吐量等信息。

[0578] 性能测定部7f若从日志发送部3a接收与下载相关的日志信息,则根据下载时间计算吞吐量,并将基于该计算出的吞吐量的判定结果输入到选择表格。性能测定部7f在吞吐量在规定值以上的情况下,将该CDN服务器的分发标志设定为打开(TRUE),在吞吐量小于规定值的情况下,将该CDN服务器的分发标志设定为关闭(FALSE)。

[0579] 接下来,参照图203～图205对上述的构成的作用进行说明。

[0580] (19－8)日志发送部3a的处理(参照图203)

[0581] 若结束从CDN服务器的更新数据包的下载(A1981),则日志发送部3a向分发服务器7发送包含表示下载所需要的时间的下载时间的与下载相关的日志信息(A1982)。

[0582] (19－9)性能判定部7f的处理(参照图204)

[0583] 性能判定部7f若从日志发送部3a接收与下载相关的日志信息(A1991),则根据下载时间计算吞吐量(A1992),并判定该计算出的吞吐量是否在规定值以上(A1993)。

[0584] 性能测定部7f若判定为该计算出的吞吐量在规定值以上(A1993:是),则判定为该CDN服务器是能够利用于分发的服务器,将分发标志设定为打开(A1994)。性能测定部7f若判定为该计算出的吞吐量小于规定值(A1993:否),则判定为该CDN服务器是不能够利用于分发的服务器,而将分发标志设定为关闭(A1995)。

[0585] (19—10)性能判定部7f的处理(参照图205)

[0586] 性能判定部7f定期地进行将分发标志关闭的CDN服务器的恢复处理。性能测定部7f向CDN供应商管理DB通知分发标志设定为关闭的CDN服务器的信息要求,确定分发标志设定为关闭的CDN服务器(A19101),并对每个CDN供应商反复以后的处理(A19102～A19107)。性能测定部7f在分发服务器7启动中,以恒定间隔或者通过分发服务器7的管理者在任意的时刻执行以后的处理。

[0587] 性能测定部7f向CDN服务器通知测试文件的分发要求,根据从CDN服务器分发的文件的下载时间计算吞吐量(A19103),并判定该计算出的吞吐量是否在规定值以上(A19104)。

[0588] 性能测定部7f若判定为该计算出的吞吐量在规定值以上(A19104:是),则将该分发标志从关闭变更为打开(A19105)。性能测定部7f若判定为该计算出的吞吐量小于规定值(A19104:否),则维持该分发标志的关闭(A19106)。另外,性能测定部7f也可以在分发服务器的系统启动时或者每隔规定期间,将CDN供应商管理DB的设定为关闭的分发标志打开。

[0589] 若像这样构成,则与为了确定CDN服务器的响应而向CDN服务器发送测试文件的分发要求的第二变形例不同,不需要向CDN服务器发送测试文件的分发要求,能够抑制对通信网络的负荷、成本。另外,也可以通过在车辆侧系统3设置测定更新数据包的下载速度的功能,若判定为吞吐量小于规定值,则将连接变更为其它的CDN服务器。

[0590] 也可以在从分发服务器7分发的活动通知中除了最初连接的CDN服务器的URL之外,还包含在该CDN服务器的吞吐量较低的情况下连接的预备的CDN服务器的URL。预备的CDN服务器例如是分发成本其次便宜的CDN服务器、预先决定的预备的CDN服务器。在指定多个CDN服务器作为预备的CDN服务器的情况下,也可以附加表示连接顺序的信息。

[0591] 车辆侧系统3若开始更新数据包的下载,则测定吞吐量,确认是否得到规定值以上的吞吐量。车辆侧系统3若判定为未得到规定值以上的吞吐量,则向DNS服务器12对活动通知所示出的预备的CDN服务器的URL询问IP地址,并将连接从最初的CDN服务器变更为新的CDN服务器。另外,由于在分发的数据中对每个数据包附加有识别信息,所以即使在更新数据包的下载的中途变更CDN服务器也能够继续下载更新数据包。

[0592] (第十九实施方式的第四变形例)

[0593] 参照图206～图207对第十九实施方式的第四变形例进行说明。第四变形例通过CDN供应商选定部7a选定多个CDN供应商,活动通知生成部7c对每个CDN供应商生成多个活动通知。在向车辆侧系统3分发活动通知时采用轮循方式指定不同的CDN服务器。

[0594] (19—11)活动通知生成部7c的处理(参照图206)

[0595] 活动通知生成部7c若获取CDN供应商的信息(A195),则对每个CDN供应商生成活动通知(A19111)。即,活动通知生成部7c对一个活动生成两个以上的活动通知。活动通知生成部7c以CDN服务器以轮循方式变更的方式分发活动通知(A19112)。活动通知生成部7c例如在选择了CDN11和CDN12两个CDN服务器的情况下,在分发活动通知时,对最初的车辆分发包

含CDN11的URL的活动通知,对下一个车辆分发包含CDN12的URL的活动通知,对更下一个车辆分发包含CDN11的URL的活动通知。

[0596] (19—12)CDN供应商选定部7a的处理(参照图207)

[0597] CDN供应商选定部7a在第十九实施方式中选定分发成本最小的CDN供应商,但在第四变形例中按照分发成本从低到高的顺序选定多个CDN供应商(A19121)。

[0598] 根据这样的构成,能够在抑制从CDN服务器的分发成本的同时,防止访问集中于特定的CDN服务器,通过防止访问的集中,能够防止吞吐量的降低。

[0599] (第十九实施方式的第五变形例)

[0600] 参照图208～图211对第十九实施方式的第五变形例进行说明。第四变形例选择抑制分发成本的多个CDN供应商,生成CDN服务器的信息不同的多个活动通知,并以CDN服务器以轮循方式变更的方式向车辆侧系统3分发活动通知。与此相对,第五变形例选择抑制分发成本的多个CDN供应商,生成一个活动通知,并分发给车辆侧系统3。在DNS服务器12从车辆侧系统3获取了与活动通知所示出的URL对应的IP地址的询问时,按照车辆侧系统3变更回答给车辆侧系统3的CDN服务器。换句话说,在DNS服务器12中,以轮循方式选择CDN服务器。

[0601] 如图208所示,DNS服务器12具备切换部12b。切换部12b在从车辆侧系统3获取了IP地址的询问时,以轮循方式依次变更回答给车辆侧系统3的IP地址。分发服务器具备DNS设定部7e。第五变形例的DNS设定部7e将图209所示的轮循记录发送给DNS服务器12。

[0602] (19—13)CDN供应商选定部7a的处理(参照图210)

[0603] CDN供应商选定部7a与第四变形例相同按照分发成本从低到高的顺序选定多个CDN供应商(A19121),设定轮循记录(A19131)。

[0604] (19—14)切换部12b的处理(参照图211)

[0605] DNS服务器12若从车辆侧系统3获取IP地址的询问(A19141),则参照轮循记录(A19142),将与记载的CDN服务器对应的IP地址发送给车辆侧系统3(A19143)。DNS服务器12每当从车辆侧系统3获取IP地址的询问则反复上述的处理,若从其它的车辆侧系统3获取IP地址的询问,则参照轮循记录,将与和上次不同的CDN服务器对应的IP地址发送到车辆侧系统3。即,DNS服务器12根据轮循方式依次将CDN服务器的IP地址发送到车辆侧系统3。

[0606] 根据这样的构成,能够在抑制从CDN服务器的分发成本的同时,防止访问集中于特定的CDN服务器,通过防止访问的集中,能够防止吞吐量的降低。

[0607] (第二十实施方式)

[0608] 参照图212～图224对第二十实施方式进行说明。

[0609] 第二十实施方式在能够对规定期间的多个活动获取信息的情况下,根据分发方式、作为分发区域的OTA对象区域、分发数据大小动态地选定多个CDN供应商,作为更新数据包的向CDN8的配置目的地,来抑制分发成本。规定期间例如是下个月。

[0610] 在上述的第十九实施方式中,对一个活动选定分发成本最小的CDN供应商。然而,活动也假定从OEM服务器登记预定在规定期间例如下个月开始分发的多个活动。在像这样预先对多个活动获取各活动的与数据大小、分发对象车辆的台数、OTA对象区域、分发方式相关的信息的情况下,有与如第十九实施方式那样对每个活动选定了CDN供应商的情况不同的CDN供应商成为分发成本最小的CDN供应商的可能性。

[0611] 如图212所示,OTA中心2具备CDN供应商管理DB、CDN供应商选定部7a、数据保存部

7b、活动通知生成部7c、CDN分发部7d、以及进展信息管理部7g。进展信息管理部7g保持表示在规定期间内以何种程度将活动分发到车辆侧系统3的预测值。活动登记于OTA中心2,即使像车辆侧系统3分发了活动通知,也不一定全部的车辆立即应用活动,从CDN服务器下载更新数据包。进展信息管理部7g为了更正确地预测从CDN服务器向车辆侧系统3的更新数据包的分发数据大小而保存预测值。虽然在本实施方式中,使规定期间为一个月进行说明,但也可以是其它的期间。

[0612] 参照图213,对第二十实施方式中的计算方法进行说明。在第二十实施方式中如后述那样通过三种计算方法计算CDN供应商的收费额。在第一计算方法中,在各活动中选定分发成本最小的CDN供应商。该情况下,有按照活动选定不同的CDN供应商的可能性。在图213中,例示对活动1选定CDN1,对活动2选定CDN2,对活动3选定CDN3的情况。

[0613] 在第二计算方法中,计算全部的活动的分发总数据大小,并基于该计算出的全部的活动的分发总数据大小选定分发成本最小的CDN供应商。该情况下,在全部的活动中选定同一CDN供应商。在图213中,例示对活动1～3选定CDN1的情况。在第三计算方法中,计算每种分发方式的活动的分发总数据大小,并基于该计算出的每种分发方式的活动的分发总数据大小选定分发成本最小的CDN供应商。作为每种分发方式,分别对流式传输方式和储存方式选定CDN供应商。在图213中,例示在活动1与活动2、3中分发方式不同,对活动1选定CDN1,对活动2、3选定CDN2的情况。

[0614] 接下来,参照图214～图224对上述的构成的作用进行说明。

[0615] (20－1)活动通知生成部7c的处理(参照图214)

[0616] 活动通知生成部7c例如从OEM服务器等外部获取预定分发的活动信息(A201)。在预定分发的活动信息包含有与分发开始日、对象活动的数据大小、对象活动的分发对象车辆的台数、地区、分发方式相关的信息。活动通知生成部7c将该获取的活动信息保存于数据保存部7b(A202)。

[0617] 活动通知生成部7c向CDN供应商选定部7a通知CDN供应商的选定要求(A203),并等待从CDN供应商选定部7a的选定通知的获取。活动通知生成部7c若从CDN供应商选定部7a获取选定通知(A204),则访问数据保存部7b,获取通过该CDN供应商选定部7a选定的CDN供应商的识别信息(A205)。

[0618] 活动通知生成部7c基于CDN供应商的识别信息生成包含该选定的CDN的URL的参数文件作为预定分发的活动通知(A206)。活动通知生成部7c将该生成的预定分发的活动通知分发到车辆侧系统3(A207)。

[0619] (20－2)CDN供应商选定部7a的处理(参照图215～图221)

[0620] CDN供应商选定部7a若获取从活动通知生成部7通知的CDN供应商的选定要求(A2011),则向数据保存部7b进行访问,获取选定信息(A2012)。该情况下,在选定信息包含有预定分发的全部的对象活动的数据大小、分发对象车辆的台数、地区、分发方式、各活动的分发开始日的信息。

[0621] CDN供应商选定部7a从进展信息管理部7g获取分发预测值(A2013)。CDN供应商选定部7a对每个活动计算分发数据大小(A2014)。具体而言,CDN供应商选定部7a将活动的数据大小、活动的分发对象车辆的台数以及分发预测值相乘,并进一步乘以与分发期间对应的修正值。根据活动,有将分发开始日设定为下月下旬的情况等分发期间较短的情况,所以

通过与分发期间对应的修正值进行调整。例如若为推迟分发开始日的结果是分发期间只有十天的情况,则三十天中十天为能够分发的期间所以设定0.3等作为修正值。

[0622] CDN供应商选定部7a移至第二CDN选定处理(A2015)。CDN供应商选定部7a若开始第二CDN选定处理,则依次移至基于第一计算方法的收费额的计算处理、基于第二计算方法的收费额的计算处理、以及基于第三计算方法的收费额的计算处理(A2021～A2023)。

[0623] CDN供应商选定部7a在基于第一计算方法的收费额的计算处理中,对每个活动选定分发成本最小的CDN供应商。CDN供应商选定部7a若开始基于第一计算方法的收费额的计算处理,则对每个活动反复其以后的处理(A2031～A2041),并且对每个CDN供应商反复(A2032～A2039)。CDN供应商选定部7a基于分发数据大小以及地区信息从CDN供应商管理DB获取费用信息(A2033)。CDN供应商选定部7a基于分发数据大小参照费用信息,计算分发收费额(A2034)。

[0624] CDN供应商选定部7a与第十九实施方式相同,判定研究对象的CDN供应商是否是进行与请求数对应的收费的CDN供应商,来决定CDN供应商的收费额(A2035～A2038)。CDN供应商选定部7a对每个CDN供应商并且对每个活动反复分发收费额的计算。另外,CDN供应商选定部7a若对一个活动计算全部的CDN供应商的收费额,则对该活动选定分发成本最小的CDN供应商(A2040)。

[0625] CDN供应商选定部7a若对全部的活动结束分发收费额的计算和CDN供应商的选定,则将全部的活动的分发收费额相加,计算总额(A2042),并结束基于第一计算方法的收费额的计算处理,移至基于第二计算方法的收费额的计算处理。

[0626] CDN供应商选定部7a在基于第二计算方法的收费额的计算处理中,基于预定分发的全部的活动的总分发数据大小选定一个CDN供应商。CDN供应商选定部7a若开始基于第二计算方法的收费额的计算处理,则将各活动的分发数据大小相加,计算分发总数据大小(A2051),并对每个CDN供应商反复其以后的处理(A2052～A2059)。CDN供应商选定部7a基于分发总数据大小以及地区信息从CDN供应商管理DB获取费用信息(A2053)。CDN供应商选定部7a基于分发总数据大小参照费用信息,计算分发收费额(A2054)。

[0627] CDN供应商选定部7a与第十九实施方式相同,判定研究对象的CDN供应商是否是进行与请求数对应的收费的CDN供应商,来决定CDN供应商的收费额(A2055～A2058)。CDN供应商选定部7a对每个CDN供应商反复分发收费额的计算。CDN供应商选定部7a选定分发成本最小的CDN供应商(A2060)。将预定分发的全部的活动的分发收费额相加,计算总额(A2061),并结束基于第二计算方法的收费额的计算处理,移至基于第三计算方法的收费额的计算处理。

[0628] CDN供应商选定部7a在基于第三计算方法的收费额的计算处理中,按每种分发方式汇总活动的基础上选定CDN供应商。CDN供应商选定部7a若开始基于第三计算方法的收费额的计算处理,则判定预定分发的活动的分发方式是否全部相同(A2071)。CDN供应商选定部7a若判定为预定分发的活动的分发方式全部相同,即预定分发的活动全部为流式传输方式,或者全部为储存方式(A2071:是),则与上述的基于第二计算方法的收费额的计算处理相同,所以结束基于第三计算方法的收费额的计算处理。

[0629] CDN供应商选定部7a若判定为预定分发的活动的分发方式并不全部相同,即作为预定分发的活动,流式传输方式和储存方式混在一起(A2071:否),则根据分发方式对活动

进行分组(A2072),对于流式传输方式的组移至流式传输方式的收费额计算处理(A2073),对于储存方式的组移至储存方式的收费额计算处理(A2074)。

[0630] CDN供应商选定部7a若开始流式传输方式的收费额计算处理,则计算通过流式传输方式分发的各活动的分发数据大小的合计值(A2081),并对每个CDN供应商反复其以后的处理(A2082～A2089)。CDN供应商选定部7a基于分发数据大小的合计值以及地区信息从CDN供应商管理DB获取费用信息(A2083)。CDN供应商选定部7a基于分发数据大小的合计值参照费用信息,计算分发收费额(A2084)。

[0631] CDN供应商选定部7a与第十九实施方式相同,判定研究对象的CDN供应商是否是进行与请求数对应的收费的CDN供应商,来决定CDN供应商的收费额(A2085～A2088)。CDN供应商选定部7a对每个CDN供应商反复分发收费额的计算。CDN供应商选定部7a选定流式传输方式的分发成本最小的CDN供应商(A2090),并结束流式传输方式的收费额计算处理。

[0632] 另一方面,CDN供应商选定部7a若开始储存方式的收费额计算处理,则计算通过储存方式分发的各活动的分发数据大小的合计值(A2091),并对每个CDN供应商反复其以后的处理(A2092～A2099)。CDN供应商选定部7a基于分发数据大小的合计值以及地区信息从CDN供应商管理DB获取费用信息(A2093)。CDN供应商选定部7a基于分发数据大小的合计值参照费用信息,计算分发收费额(A2094)。

[0633] CDN供应商选定部7a与第十九实施方式相同,判定研究对象的CDN供应商是否是进行与请求数对应的收费的CDN供应商,来决定CDN供应商的收费额(A2095～A2098)。CDN供应商选定部7a对每个CDN供应商反复分发收费额的计算。CDN供应商选定部7a选定储存方式的分发成本最小的CDN供应商(A20100),并结束储存方式的收费额计算处理。

[0634] CDN供应商选定部7a若结束基于第一计算方法的收费额的计算处理、基于第二计算方法的收费额的计算处理、以及基于第三计算方法的收费额的计算处理,则决定分发成本最小的计算方法(A2024),选定各活动的CDN供应商(A2025),并结束第二CDN选定处理。CDN供应商选定部7a若结束第二CDN选定处理,则将其选定结果即识别选定的CDN供应商的识别信息保存于数据保存部7b(A2016)。这里,CDN供应商选定部7a将识别预定分发的活动的CDN供应商的识别信息保存于数据保存部7b。CDN供应商选定部7a向活动通知生成部7c通知选定通知(A2017)。

[0635] (20－3)进展信息管理部7g的处理(参照图222)

[0636] 进展信息管理部7g保存表示在规定期间向车辆侧系统3分发何种程度的活动的预测值。假定根据从OEM服务器发送的实际的分发状况更新该预测值。

[0637] 进展信息管理部7g从OEM服务器获取分发状况(A20111)。进展信息管理部7g判定分发状况与该保存的预测值之差是否在规定值以上(A20112)。进展信息管理部7g若判定为分发状况与该保存的预测值之差不在规定值以上(A20112:否),则结束处理。

[0638] 进展信息管理部7g若判定为分发状况与该保存的预测值之差在规定值以上(A20112:是),则更新保存的预测值(A20113),并向CDN供应商选定部7a通知预测值的更新(A20114)。进展信息管理部7g既可以对全部的活动具有共用的一个预测值,也可以按照每个活动或者按照每个更新对象车辆,按照活动的种类具有不同的预测值。

[0639] (20－4)CDN供应商选定部7a的处理(参照图223)

[0640] CDN供应商选定部7a若获取从进展信息管理部7g通知的预测值的更新(A20121),

则获取选定信息(A20122),并从进展信息管理部7g获取分发预测值(A20123),对每个活动计算分发数据大小(A20124)。该情况下,CDN供应商选定部7a在计算分发数据大小时,作为考虑了分发天数的修正值。

[0641] CDN供应商选定部7a移至第二CDN选定处理(A20125),若结束第二CDN选定处理,则判定CDN供应商是否有变更(A20126)。CDN供应商选定部7a若判定为CDN供应商没有变更(A20126:否),则结束处理。在CDN供应商有变更的情况下,更新数据保存部7b中的选定结果。CDN供应商选定部7a若判定为CDN供应商有变更(A20126:是),则更新选定结果(A20127),并向活动通知生成部7c发送CDN变更通知(A20128)。另外,CDN供应商选定部7a也可以以规定间隔确认保存于进展信息管理部7g的预测值是否变更。

[0642] (20—5)活动通知生成部7c的处理(参照图224)

[0643] 活动通知生成部7c若获取从CDN供应商选定部7a通知的CDN变更通知(A20131),则访问数据保存部7b,获取更新后的CDN供应商的信息(A20132),并基于该获取的更新后的CDN供应商信息重新生成预定分发的活动通知(A20133)。

[0644] 如以上说明的那样根据第二十实施方式,能够得到以下的作用效果。

[0645] 构成为参照CDN供应商管理数据库,根据分发方式、OTA对象区域以及分发数据大小从分发成本不同的多个CDN8中选定分发成本有优势的CDN8,并将更新数据包配置于该选定的CDN8。能够适当地抑制OTA主机4从OTA中心2下载更新数据包时的分发成本。

[0646] (其它的实施方式)

[0647] 在上述的实施方式中,未载明流式传输方式或者储存方式的实施方式能够应用于流式传输方式和储存方式的任何的方式。

[0648] 在上述的一部分的实施方式中,记载了在建立了TLS通信的基础上从OTA中心2向OTA主机4发送活动通知。然而,也可以在全部的实施方式中,在建立了TLS通信的基础上从OTA中心2向OTA主机4发送活动通知。通过建立TLS通信,能够进一步提高安全。或者,也可以不建立TLS通信而从OTA中心2向OTA主机4发送活动通知。

[0649] 本实施方式的车辆侧系统3也可以是以下的构成。车辆侧系统3也可以构成为具备DCM(数据通信模块)和CGW(中央网关),DCM与CGW经由总线以能够进行数据通信的方式连接。CGW也称为中央ECU。总线例如可以是以太网、CAN(注册商标)总线等。

[0650] 也可以在CGW中实现OTA主机4的功能的一部分或者整体。作为一个例子,也可以DCM与CDN8、OTA中心2等外部进行数据通信,在CGW中实施OTA主机4的功能的全部。该情况下,DCM将通过与外部的无线通信接收的全部的数据转送至CGW。或者,也可以DCM除了与外部进行数据通信之外,还作为OTA主机4的下载器发挥作用。下载器的功能例如是指车辆构成信息的生成、元数据验证、数据包验证、活动信息的验证。或者,也可以在DCM中实现OTA主机4的功能。该情况下,在CGW安装有OTA主机4以外的功能。或者,也可以DCM与CGW一体化。

[0651] 也可以构成为CGW具有DCM的功能的一部分或者整体,也可以构成为DCM具有CGW的功能的一部分或者整体。即,在OTA主机4中,可以任意地构成DCM与CGW的功能分担。OTA主机4既可以由DCM以及CGW两个ECU构成,也可以由具有DCM的功能和CGW的功能的一个综合ECU构成。

[0652] 本公开依据实施方式进行了记述,但应该理解本公开并不限定于该实施方式、结构。本公开也包含各种变形例、同等范围内的变形。除此之外,也将各种组合、方式,甚至其

中仅包含一个要素、更多或者更少要素的其它的组合、方式纳入本公开的范畴、思想范围。

[0653] 能够通过记录于实体的存储器装置的软件以及执行该软件的计算机，仅通过软件，仅通过硬件，或者通过它们的组合提供各装置等提供的方法、功能。例如在通过作为硬件的电子电路提供控制部的情况下，能够通过包含许多的逻辑电路的数字电路，或者模拟电路提供该控制部。

[0654] 也可以由通过构成被编程为执行通过计算机程序具体化的一个或者多个功能的处理器以及存储器提供的专用计算机实现本公开所记载的控制部及其方法。或者，也可以由通过由一个以上的专用硬件逻辑电路构成处理器提供的专用计算机实现本公开所记载的控制部及其方法。另外，也可以由通过被编程为执行一个或者多个功能的处理器以及存储器与由一个以上的硬件逻辑电路构成的处理器的组合构成的一个以上的专用计算机实现本公开所记载的控制部及其方法。另外，计算机程序也可以作为能够通过计算机执行的指令，存储于计算机能够读取的非迁移有形记录介质。

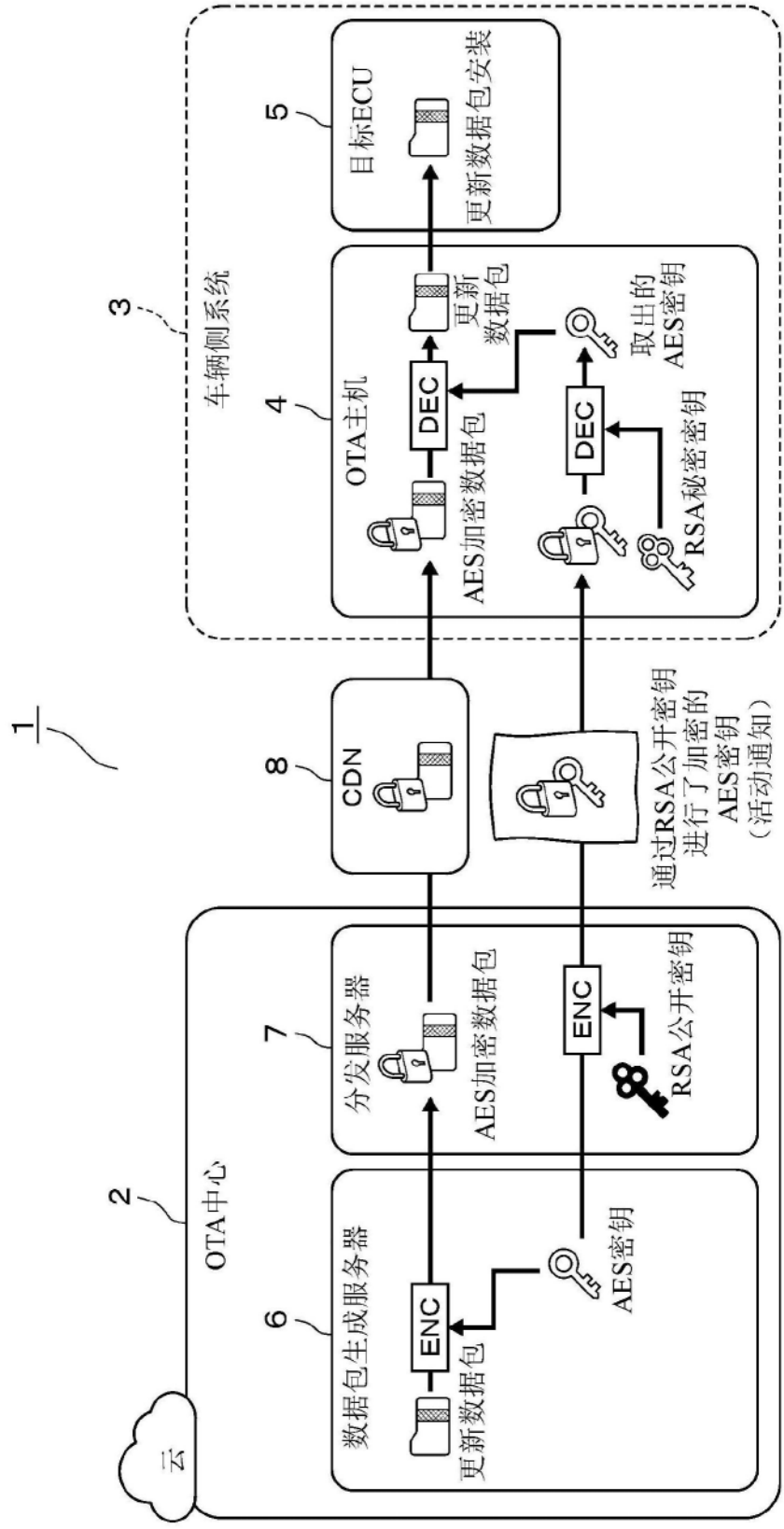

1
2
OTA中心
云
6
数据包生成服务器
更新数据包
ENC
AES密钥
7
分发服务器
AES加密数据包
RSA公开密钥
ENC
8
CDN
通过RSA公开密钥
进行了加密的
AES密钥
（活动通知）
3
车辆侧系统
4
OTA主机
AES加密数据包
DEC
更新
数据包
RSA秘密密钥
DEC
取出的
AES密钥
5
目标ECU
更新数据包安装

图1

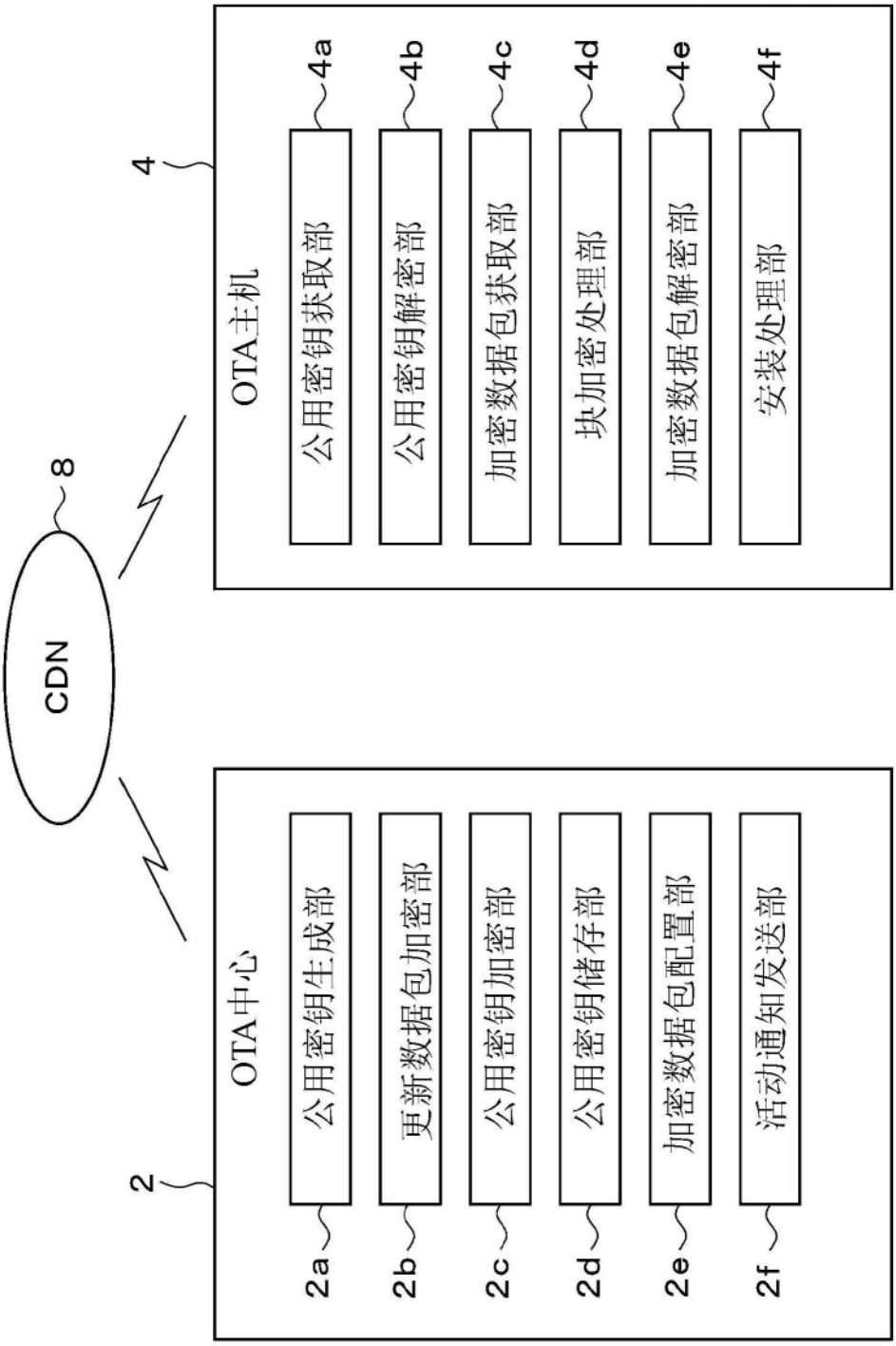

8
CDN
4
OTA主机
公用密钥获取部
4a
公用密钥解密部
4b
加密数据包获取部
4c
块加密处理部
4d
加密数据包解密部
4e
安装处理部
4f
2
OTA中心
公用密钥生成部
2a
更新数据包加密部
2b
公用密钥加密部
2c
公用密钥储存部
2d
加密数据包配置部
2e
活动通知发送部
2f

图2

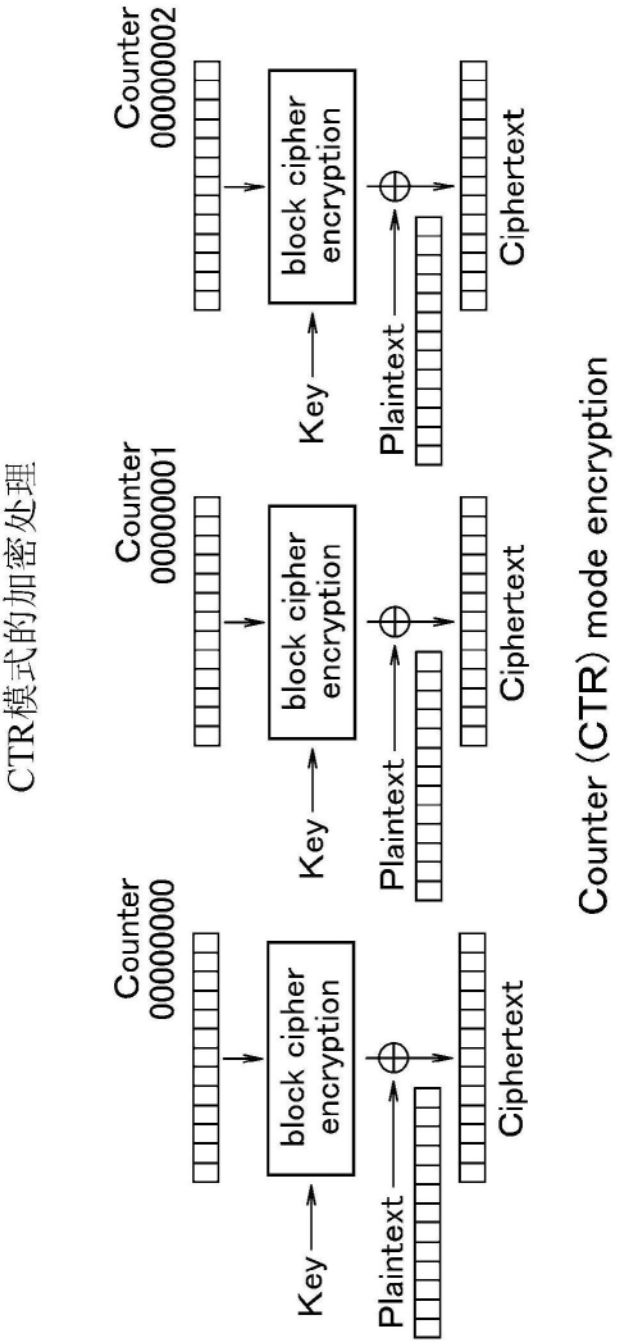

CTR模式的加密处理
Counter
00000000
Counter
00000001
Counter
00000002
block cipher
encryption
Key
Plaintext
Ciphertext
Counter (CTR) mode encryption

图3

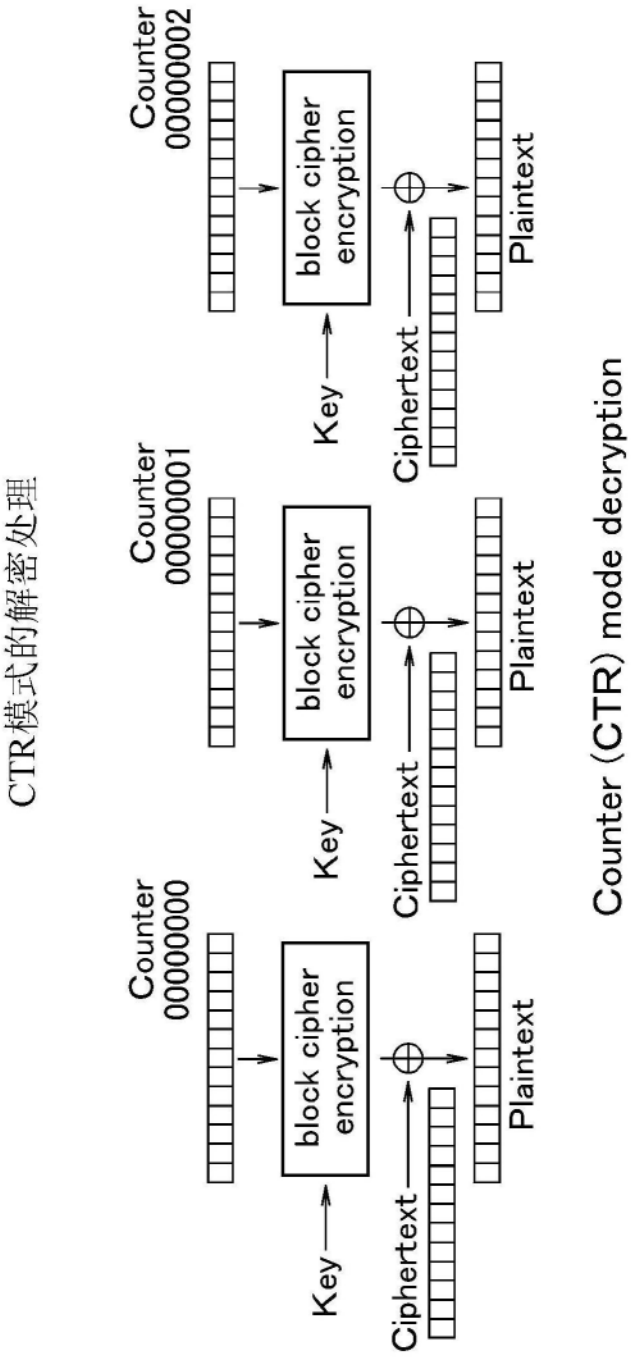

CTR模式的解密处理
Counter
00000000
Counter
00000001
Counter
00000002
block cipher
encryption
Key
Ciphertext
Plaintext
Counter (CTR) mode decryption

图4

	名字	优点	缺点	推荐
CBC模式	Cipher Block Chaining 密码块链接模式	・明文的反复不反映于密文，高安全	・若对有位单位的错误的密文进行解密，则一块整体和下一个对应的位成为错误（错误波及） ・不能够进行加密以及解密的前准备 ・不能够进行加密的并列处理	CRYPTOREC 推荐加密
CTR模式	Counter 计数器模式	・由于能够进行加密以及解密的前准备，所以能够高速化 ・能够进行加密的并列处理 ・若对有位单位的错误的密文进行解密，则错误仅限于明文的对应的位	・若主动攻击者对密码块进行位反转，则对应的明文块进行位反转	CRYPTOREC 推荐加密

图5

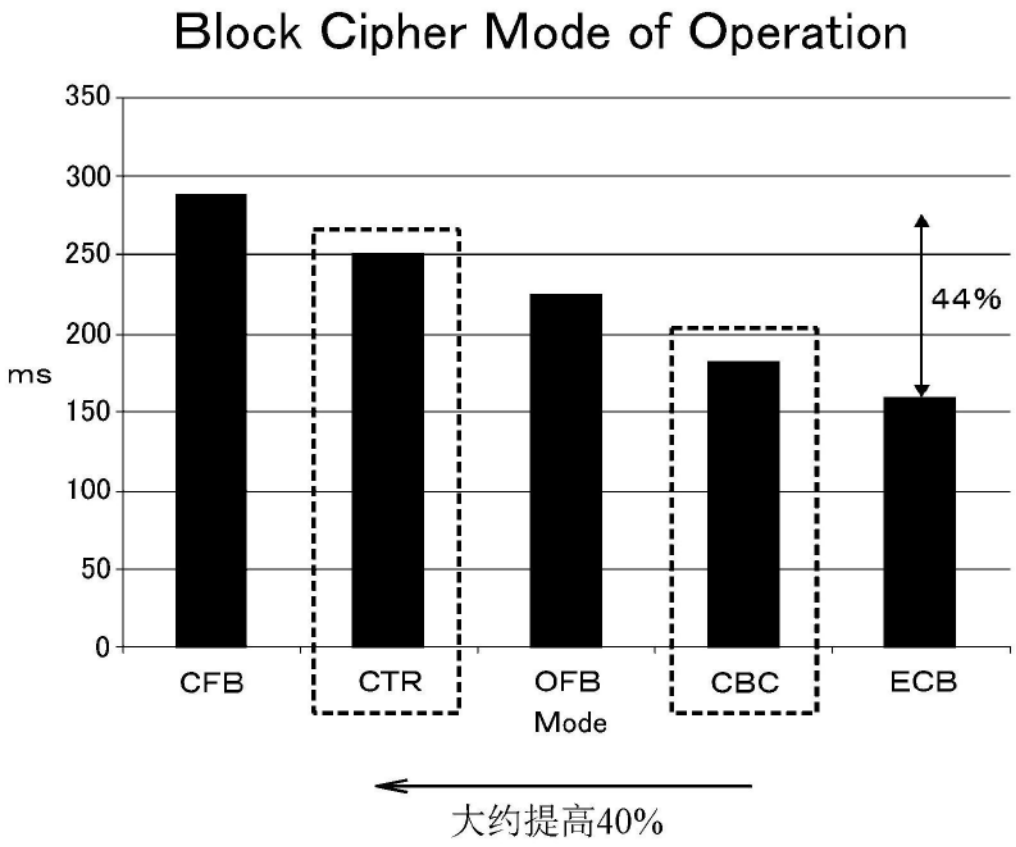

Block Cipher Mode of Operation
350
300
250
200
150
100
50
0
ms
44%
CFB
CTR
OFB
CBC
ECB
Mode
大约提高40%

图6

由于输入为密文，所以若不接收作为密文的更新数据包，
则不能够开始解密处理

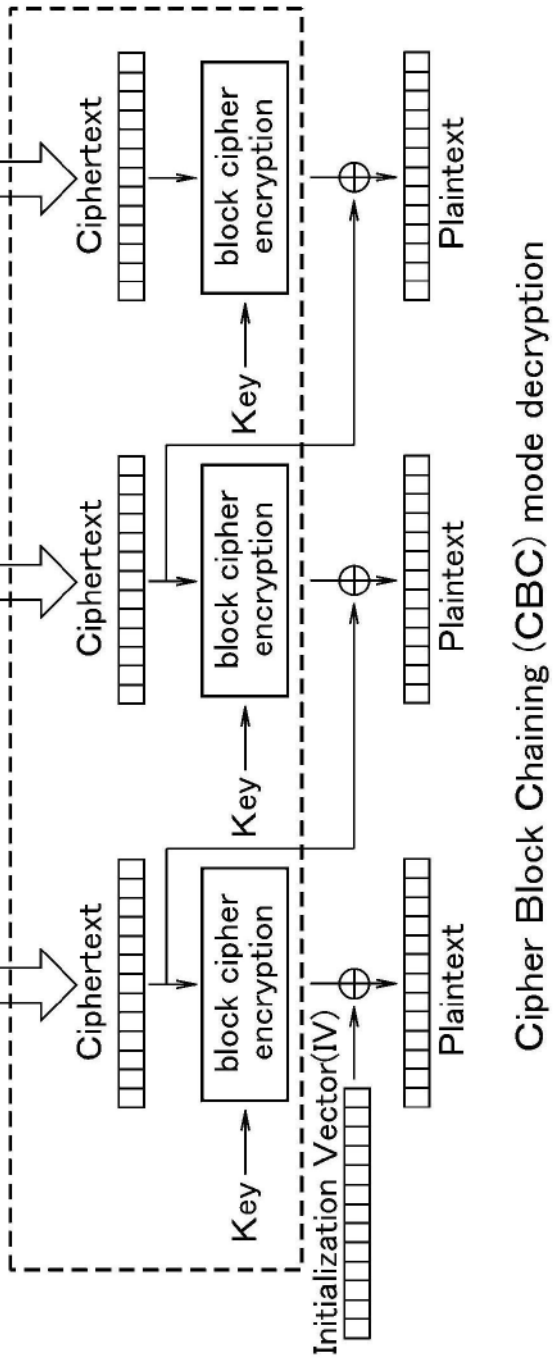


图7

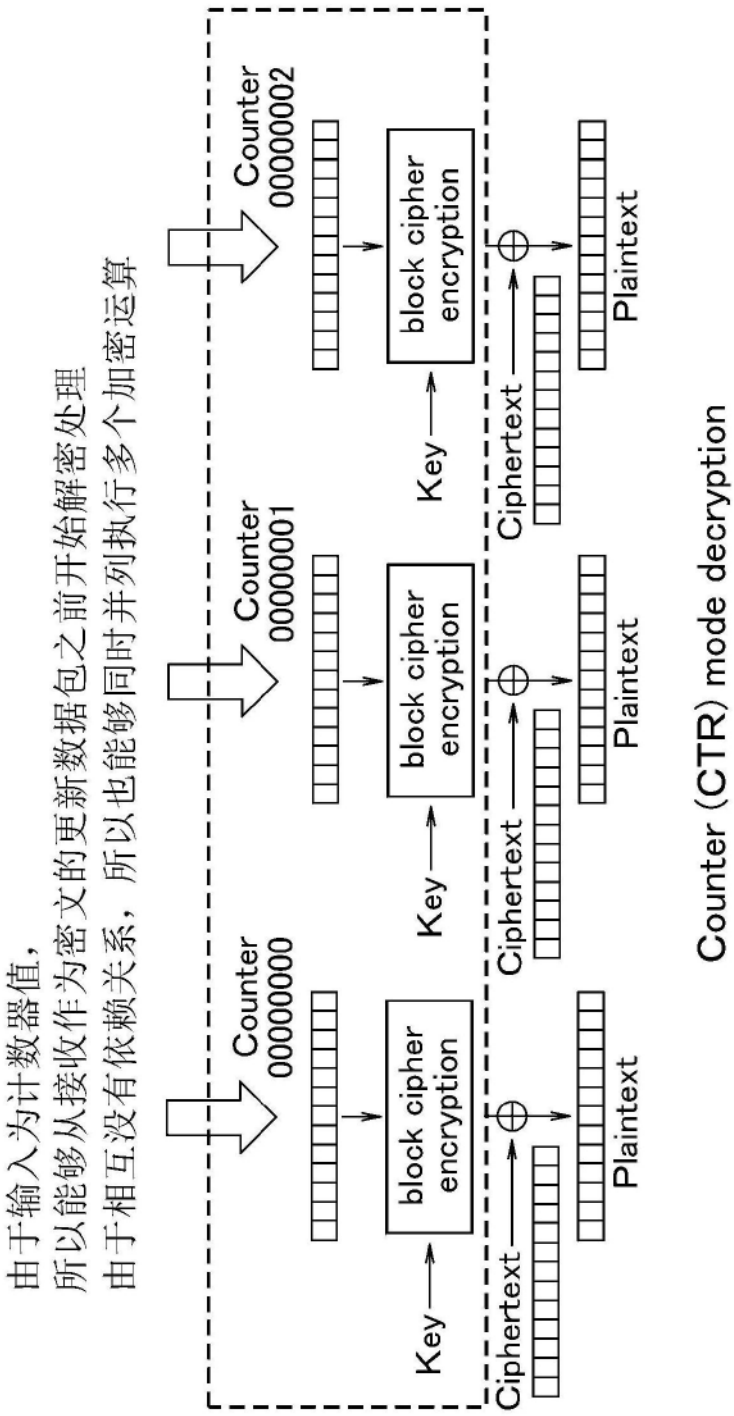

由于输入为计数器值，
所以能够从接收作为密文的更新数据包之前开始解密处理
由于相互没有依赖关系，所以也能够同时并列执行多个加密运算
Counter
00000000
Counter
00000001
Counter
00000002
block cipher
encryption
Key
Ciphertext
Plaintext
Counter (CTR) mode decryption

图8

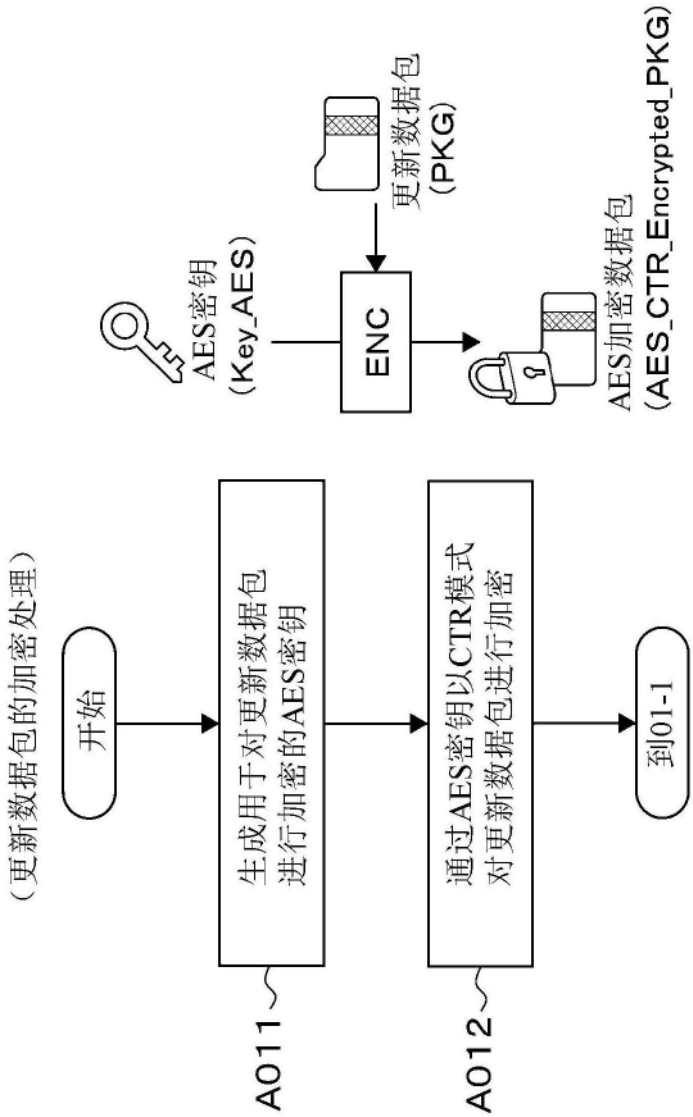

（更新数据包的加密处理）
开始
生成用于对更新数据包
进行加密的AES密钥
A011
通过AES密钥以CTR模式
对更新数据包进行加密
A012
到01-1
AES密钥
(Key_AES)
ENC
更新数据包
(PKG)
AES加密数据包
(AES_CTR_Encrypted_PKG)

图9

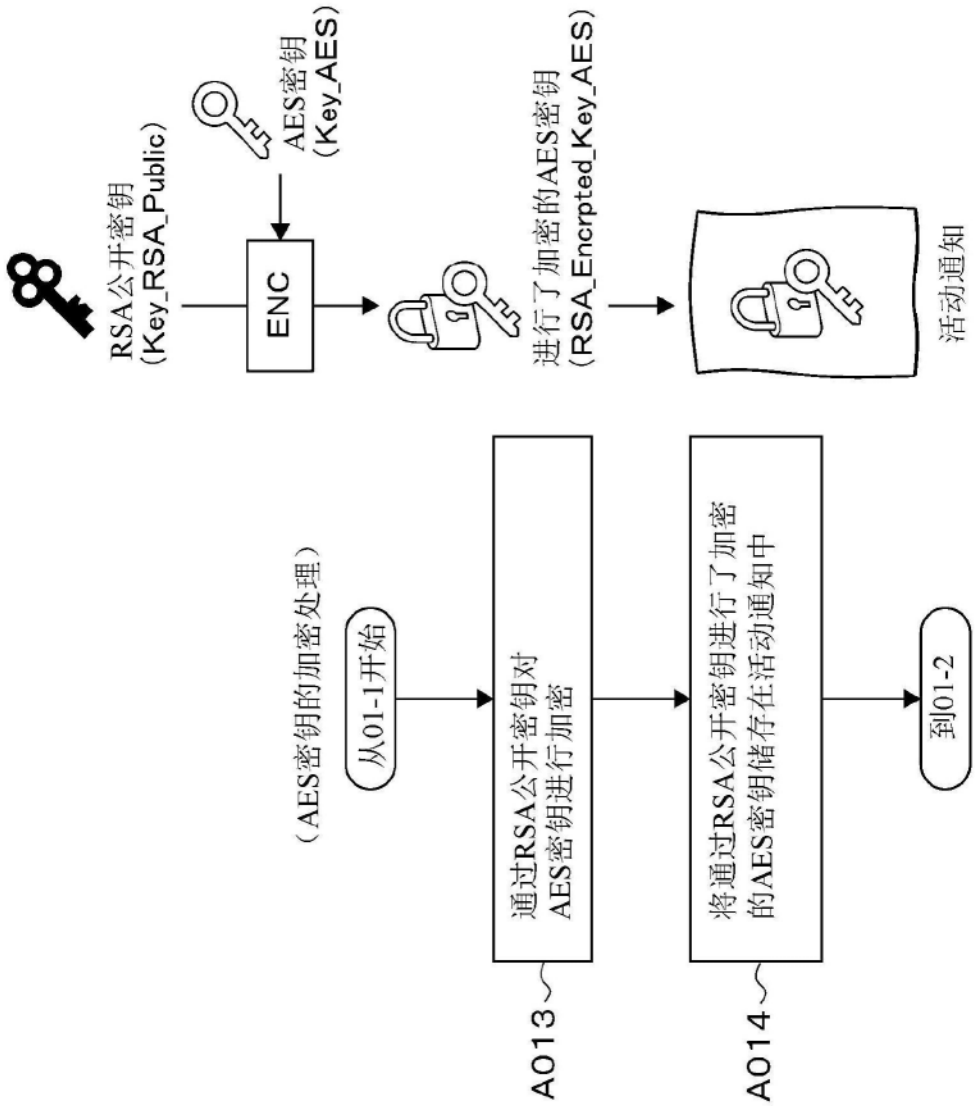

RSA公开密钥
(Key_RSA_Public)
AES密钥
(Key_AES)
ENC
进行了加密的AES密钥
(RSA_Encrpted_Key_AES)
活动通知
(AES密钥的加密处理)
从01-1开始
通过RSA公开密钥对
AES密钥进行加密
将通过RSA公开密钥进行了加密
的AES密钥储存在活动通知中
到01-2
A013
A014

图10

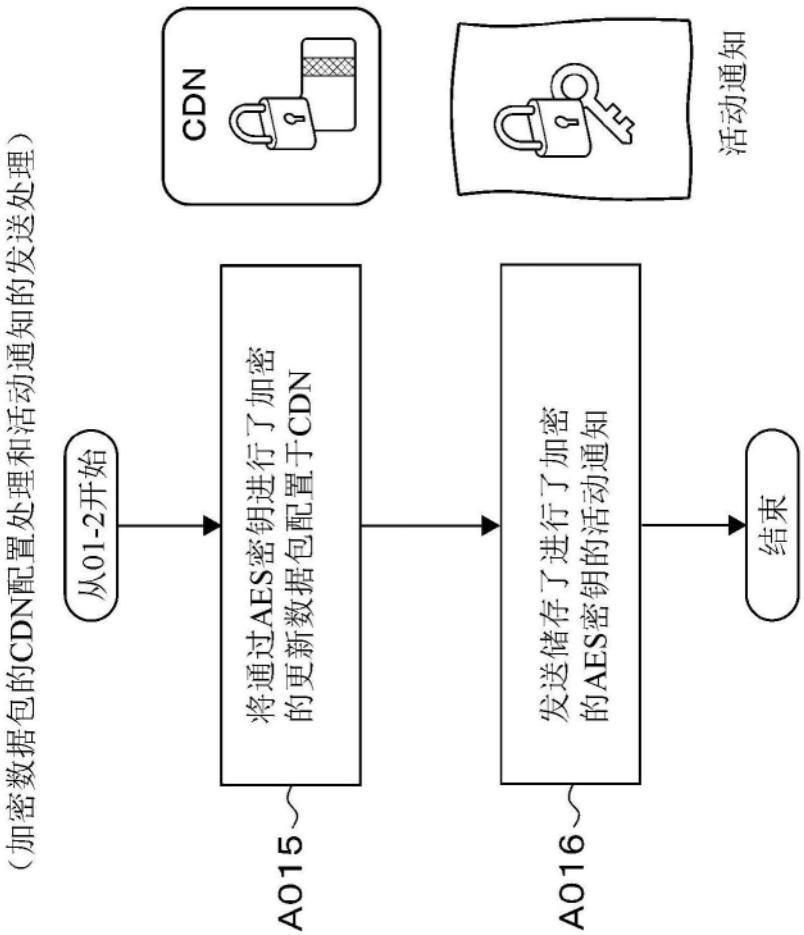

（加密数据包的CDN配置处理和活动通知的发送处理）
从01-2开始
将通过AES密钥进行了加密的更新数据包配置于CDN
A015
发送储存了进行了加密的AES密钥的活动通知
A016
结束
CDN
活动通知

图11

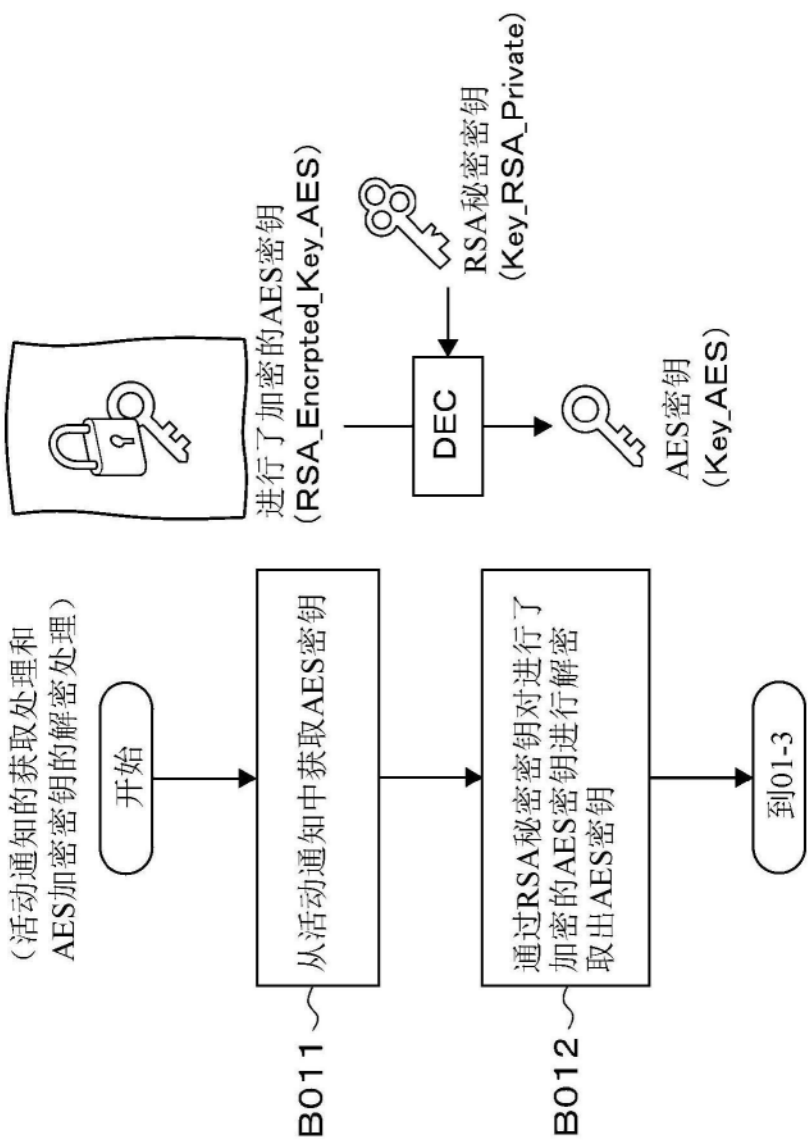

（活动通知的获取处理和
AES加密密钥的解密处理）
开始
从活动通知中获取AES密钥
B011
通过RSA秘密密钥对进行了
加密的AES密钥进行解密
取出AES密钥
B012
到01-3
进行了加密的AES密钥
(RSA_Encrpted_Key_AES)
DEC
RSA秘密密钥
(Key_RSA_Private)
AES密钥
(Key_AES)

图12

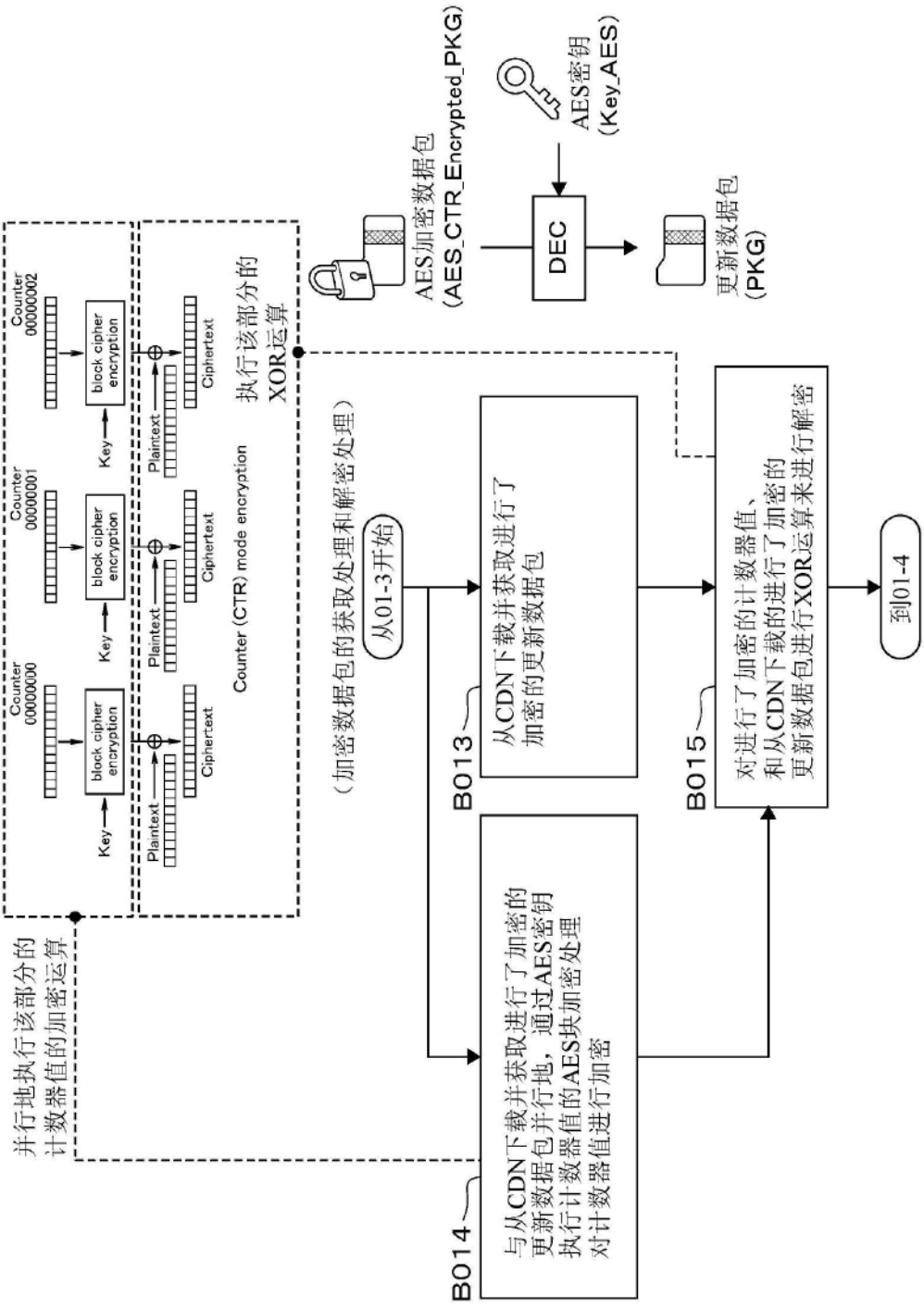

并行地执行该部分的
计数器值的加密运算
Counter
00000000
Counter
00000001
Counter
00000002
Key
block cipher
encryption
Plaintext
Ciphertext
Counter (CTR) mode encryption
执行该部分的
XOR运算
（加密数据包的获取处理和解密处理）
从01-3开始
B013
从CDN下载并获取进行了
加密的更新数据包
B014
与从CDN下载并获取进行了加密的
更新数据包并行地，通过AES密钥
执行计数器值的AES块加密处理
对计数器值进行加密
B015
对进行了加密的计数器值、
和从CDN下载的进行了加密的
更新数据包进行XOR运算来进行解密
到01-4
AES加密数据包
(AES_CTR_Encrypted_PKG)
DEC
AES密钥
(Key_AES)
更新数据包
(PKG)

图13

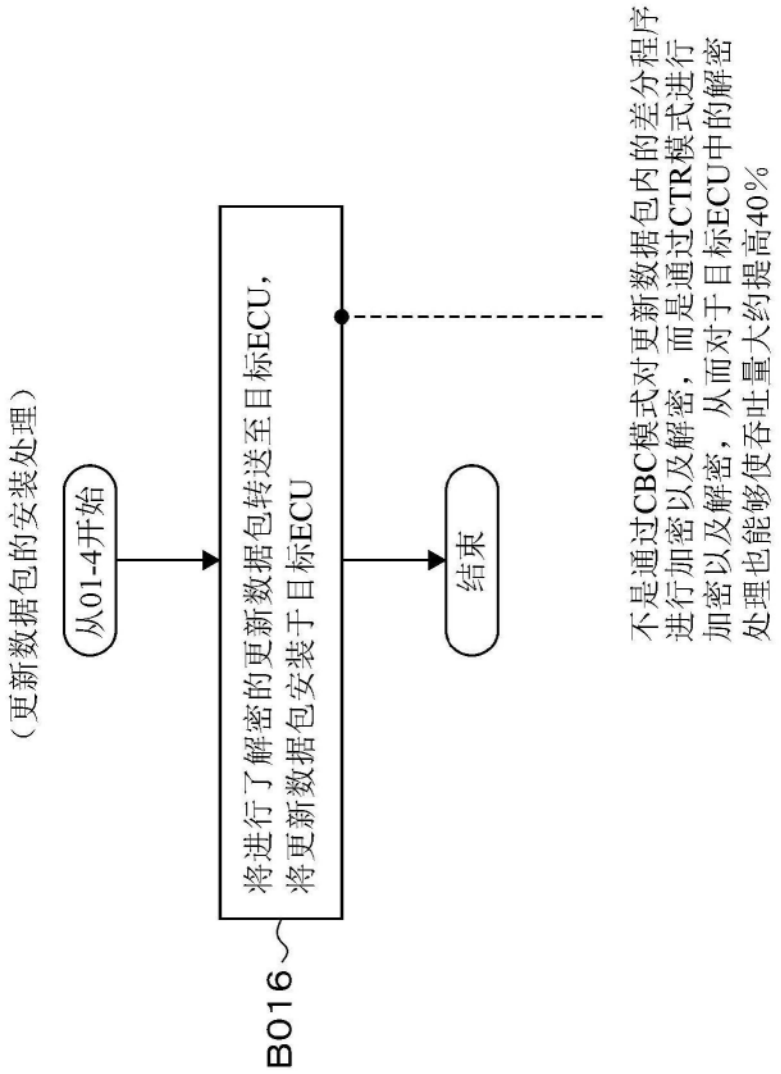

（更新数据包的安装处理）
从01-4开始
将进行了解密的更新数据包转送至目标ECU，
将更新数据包安装于目标ECU
B016
结束
不是通过CBC模式对更新数据包内的差分程序
进行加密以及解密，而是通过CTR模式进行
加密以及解密，从而对于目标ECU中的解密
处理也能够使吞吐量大约提高40％

图14

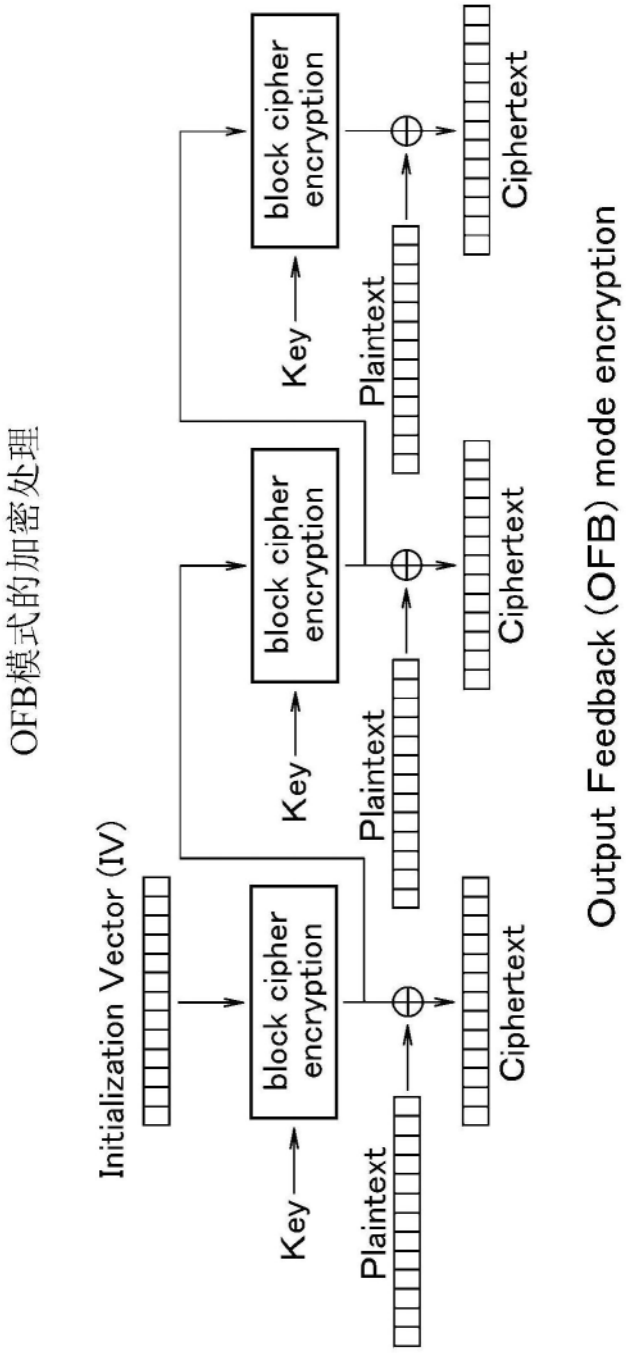

OFB模式的加密处理
Initialization Vector (IV)
block cipher encryption
Key
Plaintext
Ciphertext
Output Feedback (OFB) mode encryption

图15

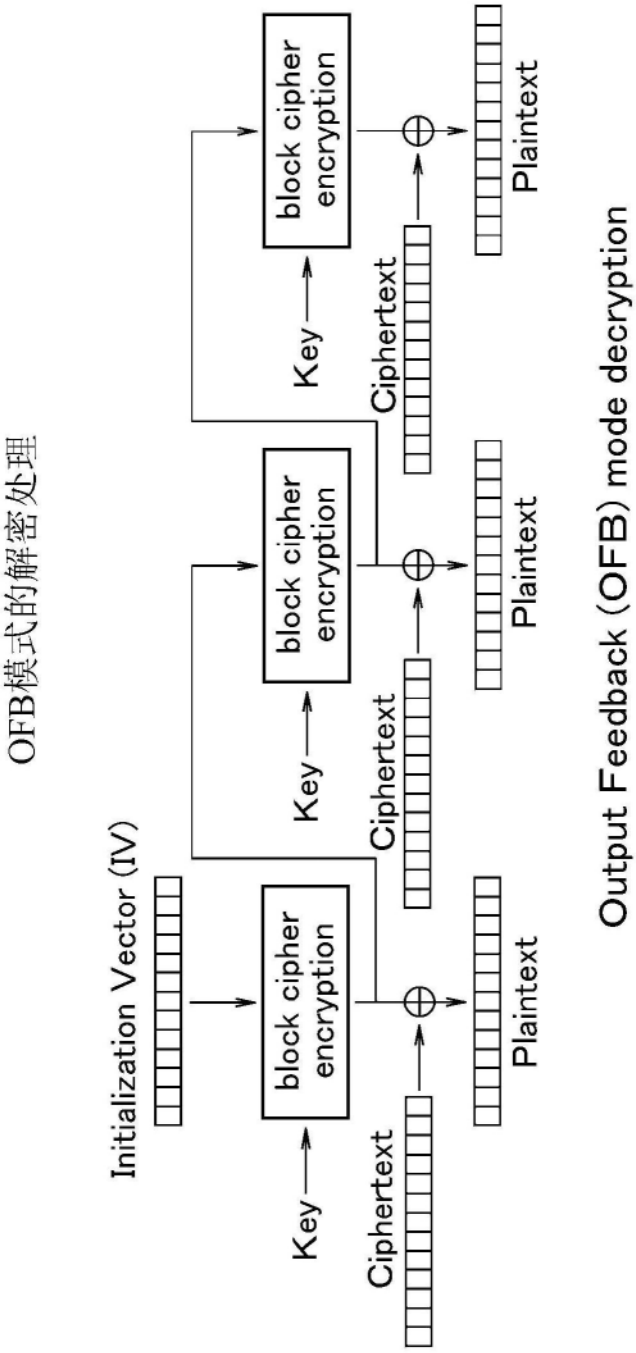

OFB模式的解密处理
Initialization Vector (IV)
block cipher encryption
Key
Ciphertext
Plaintext
Output Feedback (OFB) mode decryption

图16

	名字	优点	缺点	推荐
CBC模式	Cipher Block Chaining 密码块链接模式	·明文的反复不反映于密文，高安全	·若对有位单位的错误的密文进行解密，则一块整体和下一个对应的位成为错误（错误波及） ·不能够进行加密以及解密的前准备 ·不能够进行加密的并列处理	CRYPTOREC推荐加密
OFB模式	Output FeedBack 输出反馈模式	·由于能够进行加密以及解密的前准备，所以能够高速化 ·若对有位单位的错误的密文进行解密，则错误仅限于明文的对应的位	·若主动攻击者对密码块进行位反转，则对应的明文块进行位反转 ·不能够进行并列处理（加密以及解密双方）	CRYPTOREC推荐加密

图17

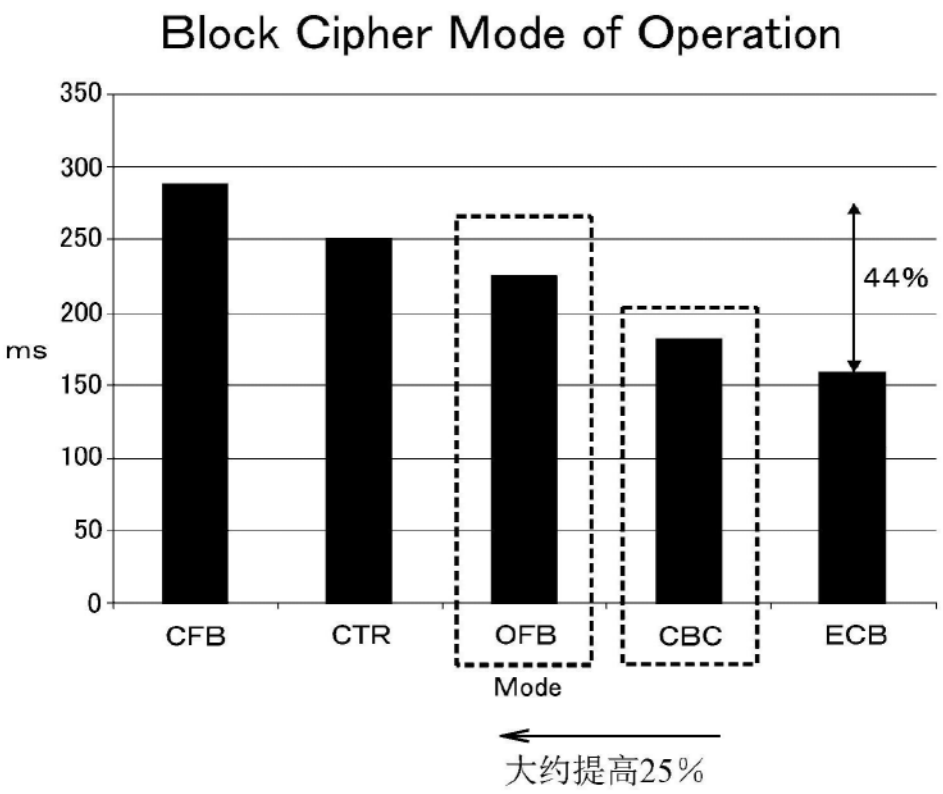

Block Cipher Mode of Operation
350
300
250
200
150
100
50
0
ms
44%
CFB
CTR
OFB
CBC
ECB
Mode
大约提高25%

图18

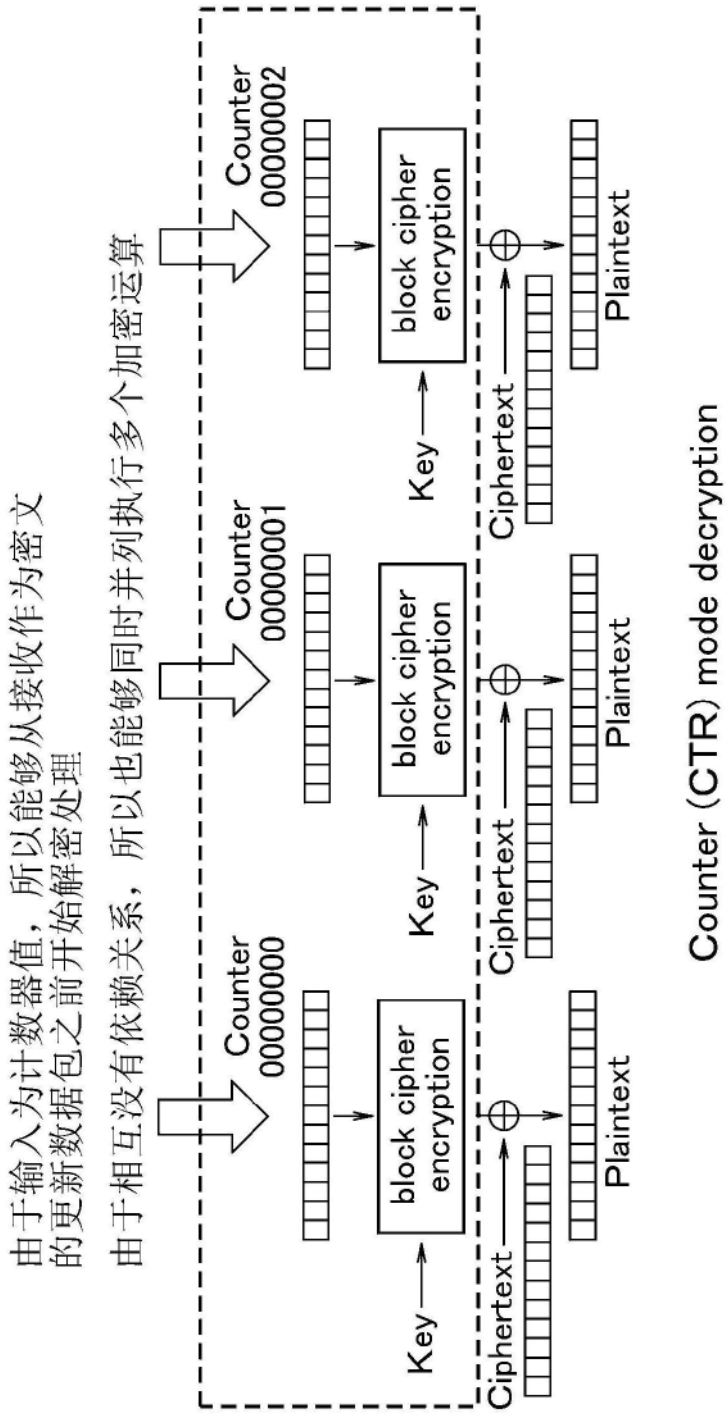

由于输入为计数器值，所以能够从接收作为密文
的更新数据包之前开始解密处理
由于相互没有依赖关系，所以也能够同时并列执行多个加密运算
Counter
00000000
Counter
00000001
Counter
00000002
block cipher
encryption
Key
Ciphertext
Plaintext
Counter (CTR) mode decryption

图19

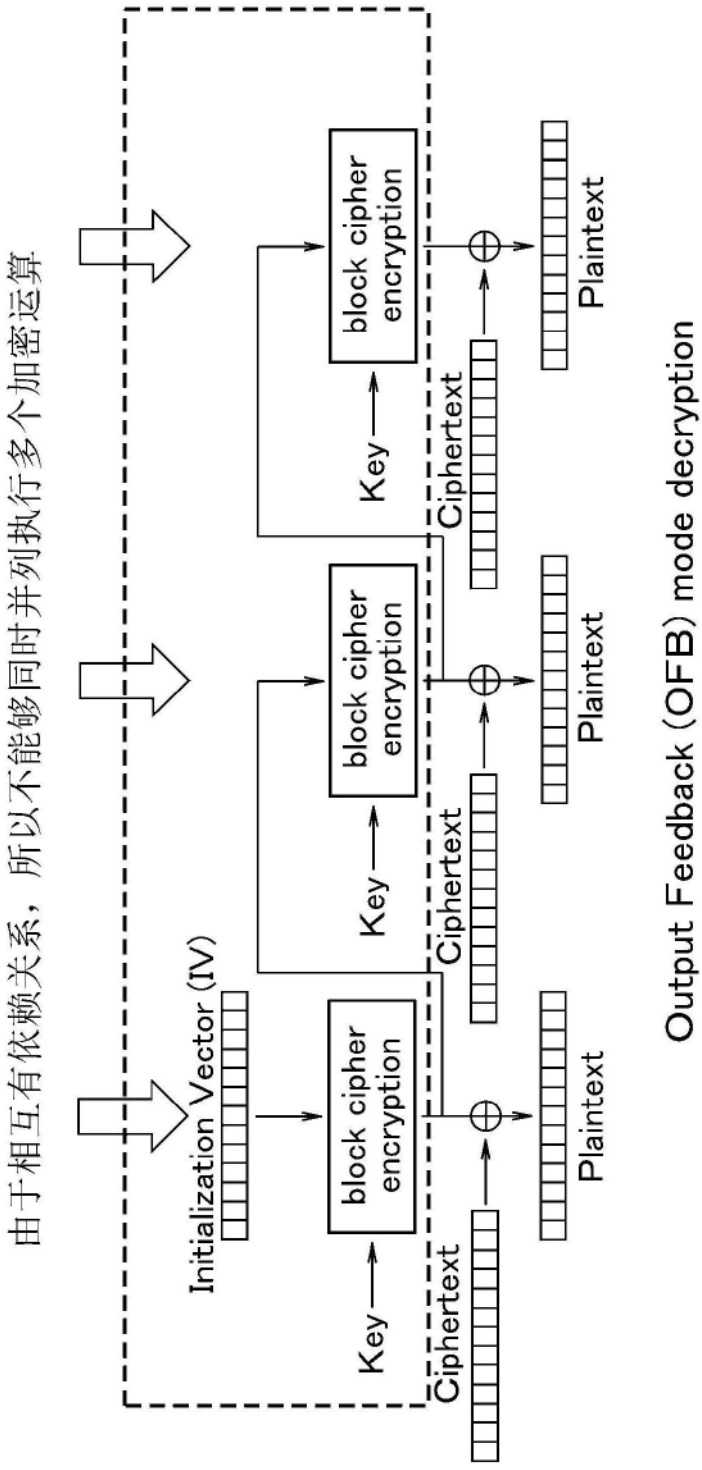

由于相互有依赖关系，所以不能够同时并列执行多个加密运算
Initialization Vector (IV)
block cipher encryption
Key
Ciphertext
Plaintext
Output Feedback (OFB) mode decryption

图20

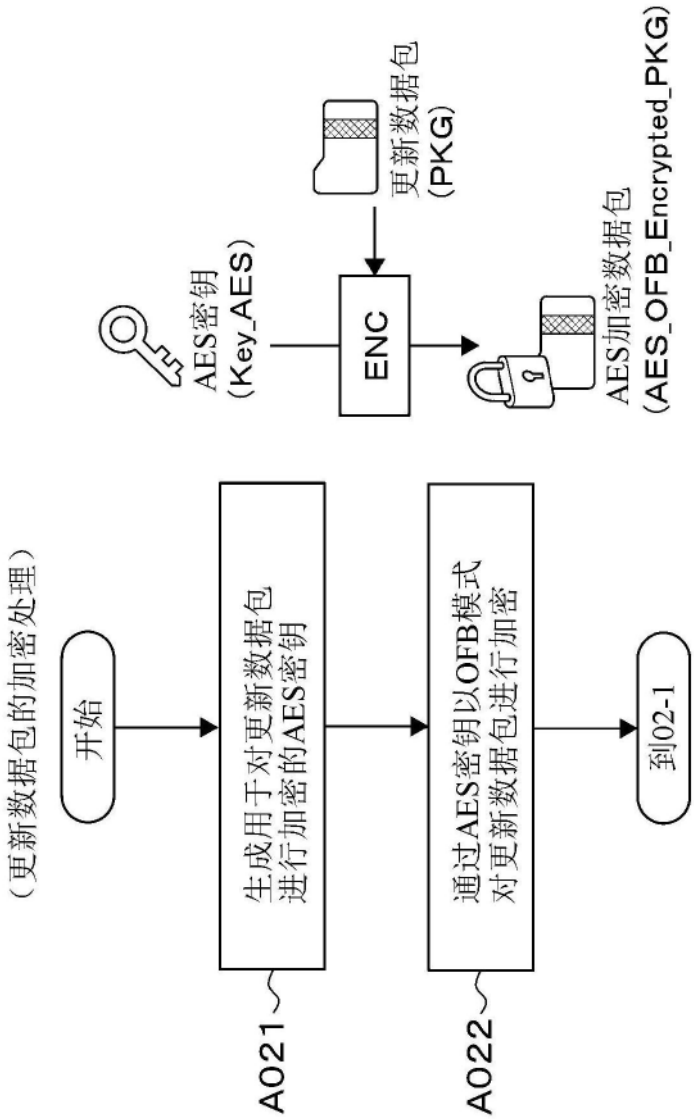

AES密钥
(Key_AES)
更新数据包
(PKG)
ENC
AES加密数据包
(AES_OFB_Encrypted_PKG)
(更新数据包的加密处理)
开始
生成用于对更新数据包
进行加密的AES密钥
通过AES密钥以OFB模式
对更新数据包进行加密
到02-1
A021
A022

图21

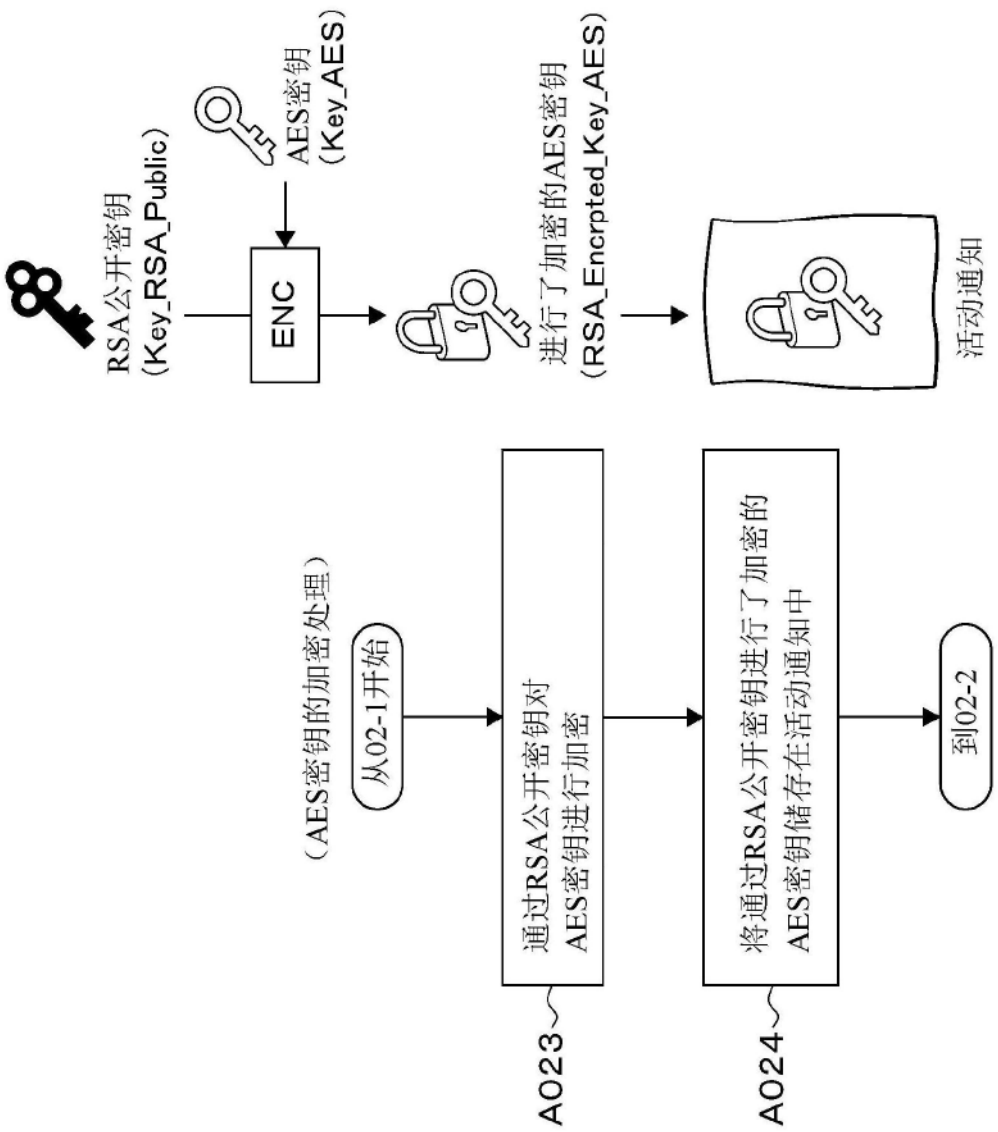

RSA公开密钥
(Key_RSA_Public)
AES密钥
(Key_AES)
ENC
进行了加密的AES密钥
(RSA_Encrpted_Key_AES)
活动通知
(AES密钥的加密处理)
从02-1开始
通过RSA公开密钥对
AES密钥进行加密
将通过RSA公开密钥进行了加密的
AES密钥储存在活动通知中
到02-2
A023
A024

图22

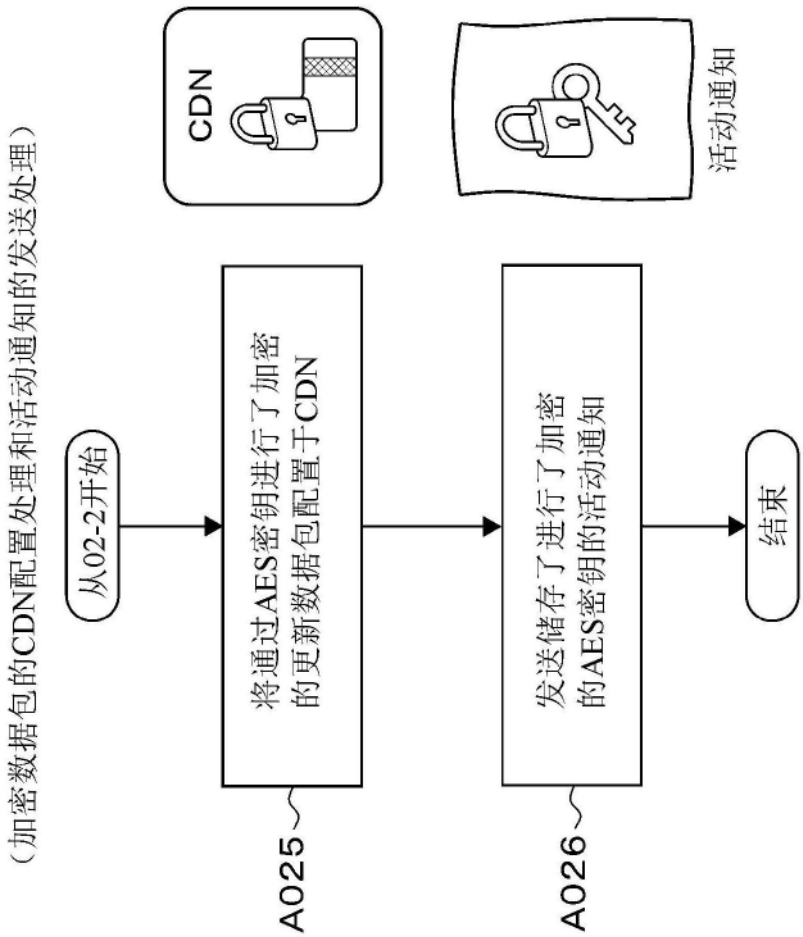

（加密数据包的CDN配置处理和活动通知的发送处理）
从02-2开始
将通过AES密钥进行了加密的更新数据包配置于CDN
A025
发送储存了进行了加密的AES密钥的活动通知
A026
结束
CDN
活动通知

图23

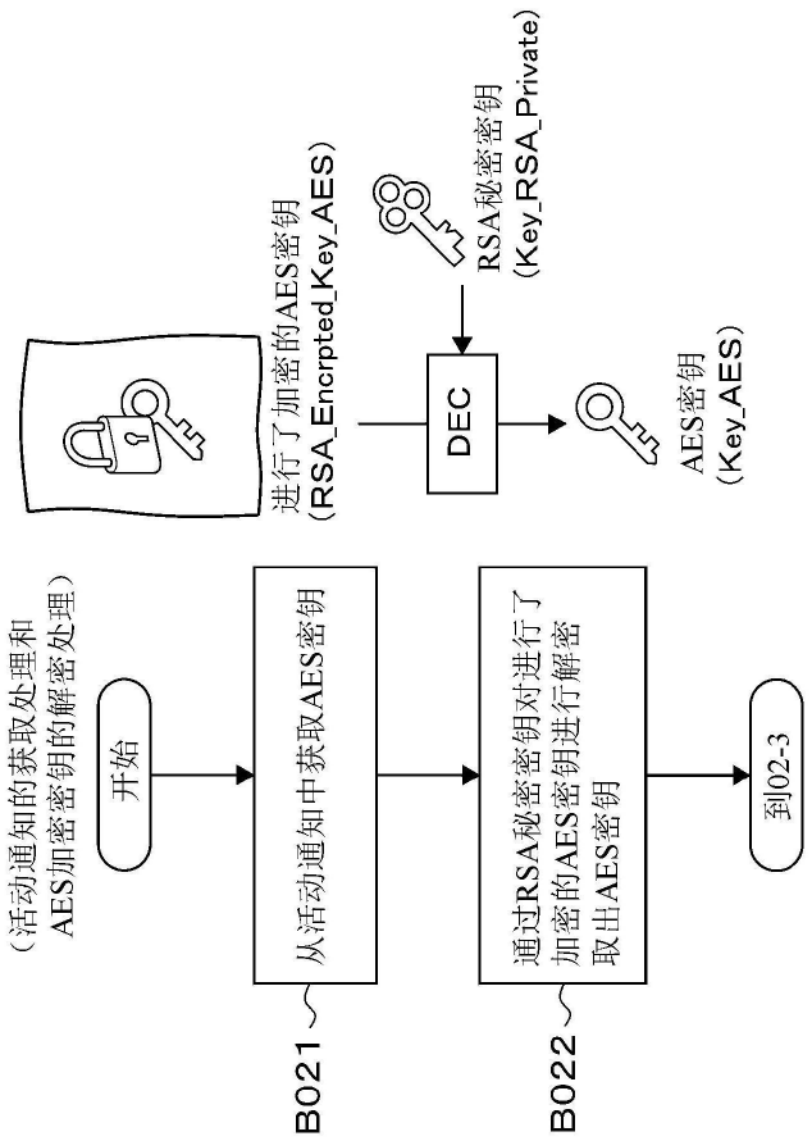

（活动通知的获取处理和
AES加密密钥的解密处理）
开始
从活动通知中获取AES密钥
B021
通过RSA秘密密钥对进行了
加密的AES密钥进行解密
取出AES密钥
B022
到02-3
进行了加密的AES密钥
(RSA_Encrpted_Key_AES)
DEC
RSA秘密密钥
(Key_RSA_Private)
AES密钥
(Key_AES)

图24

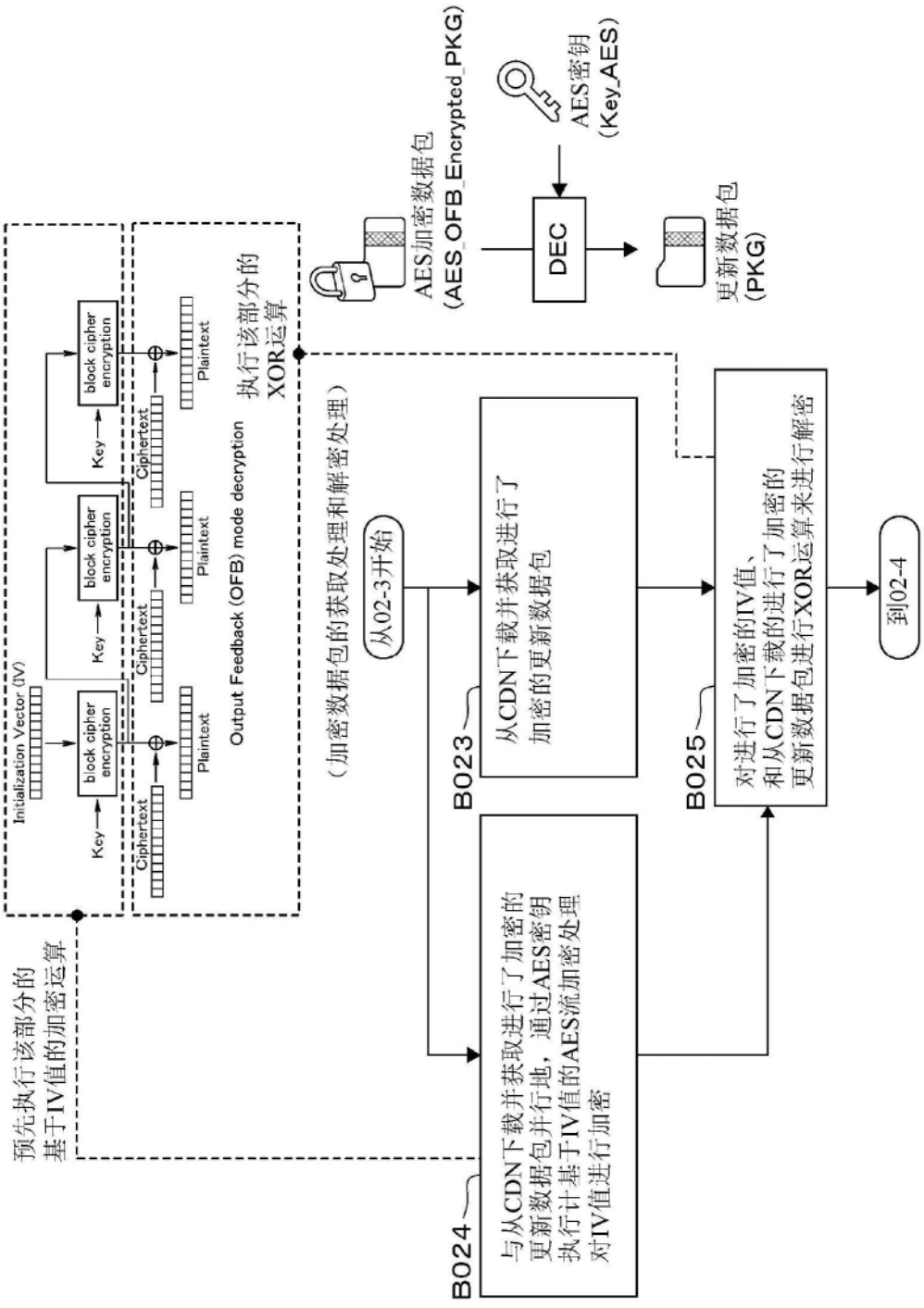

预先执行该部分的
基于IV值的加密运算
Initialization Vector (IV)
block cipher encryption
Key
Plaintext
Ciphertext
Output Feedback (OFB) mode decryption
执行该部分的
XOR运算
（加密数据包的获取处理和解密处理）
从02-3开始
B024
与从CDN下载并获取进行了加密的
更新数据包并行地，通过AES密钥
执行计基于IV值的AES流加密处理
对IV值进行加密
B023
从CDN下载并获取进行了
加密的更新数据包
B025
对进行了加密的IV值、
和从CDN下载的进行了加密的
更新数据包进行XOR运算来进行解密
到02-4
AES加密数据包
(AES_OFB_Encrypted_PKG)
DEC
AES密钥
(Key_AES)
更新数据包
(PKG)

图25

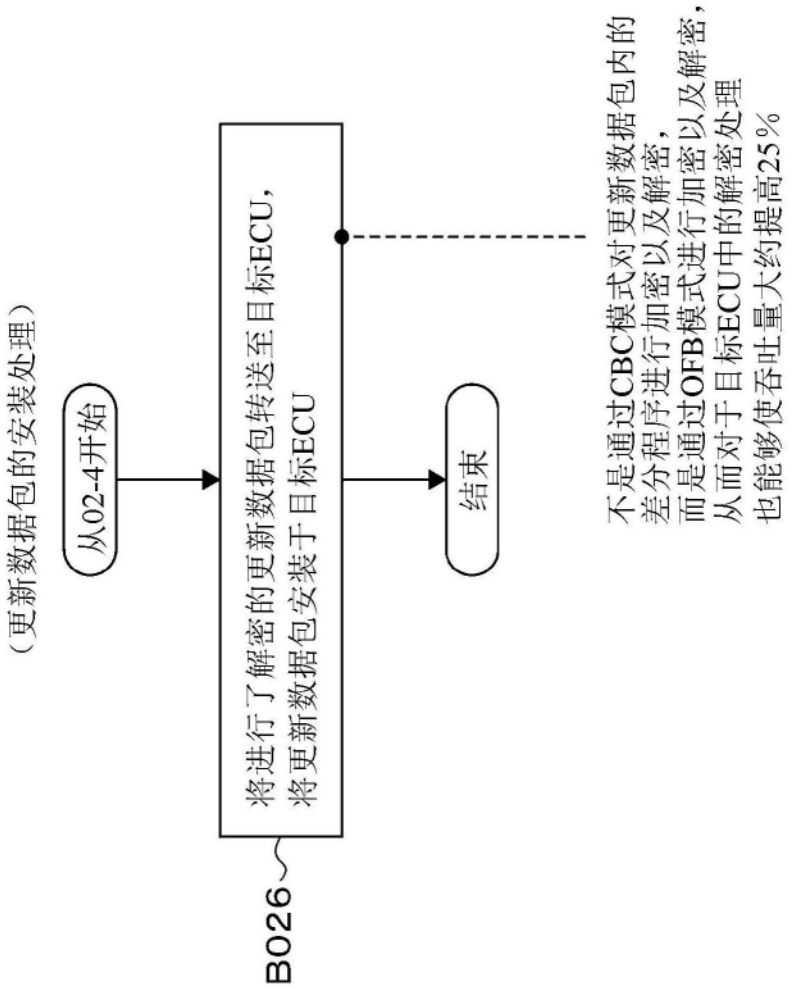

（更新数据包的安装处理）
从02-4开始
将进行了解密的更新数据包转送至目标ECU，
将更新数据包安装于目标ECU
B026
结束
不是通过CBC模式对更新数据包内的
差分程序进行加密以及解密，
而是通过OFB模式进行加密以及解密，
从而对于目标ECU中的解密处理
也能够使吞吐量大约提高25%

图26

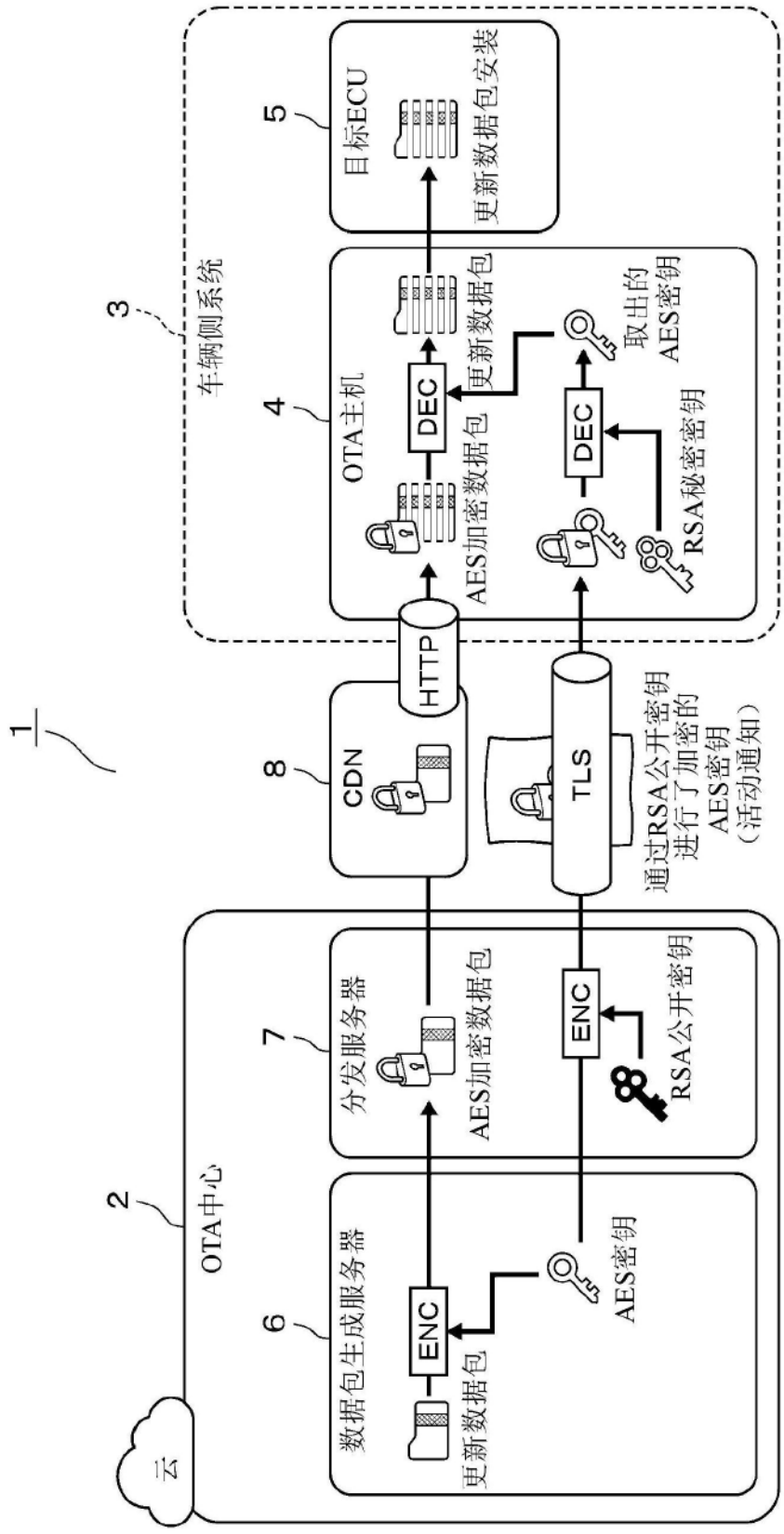

1
2
OTA中心
云
6
数据包生成服务器
更新数据包
ENC
AES密钥
7
分发服务器
AES加密数据包
ENC
RSA公开密钥
8
CDN
HTTP
TLS
通过RSA公开密钥
进行了加密的
AES密钥
（活动通知）
3
车辆侧系统
4
OTA主机
AES加密数据包
DEC
更新数据包
RSA秘密密钥
DEC
取出的
AES密钥
5
目标ECU
更新数据包安装

图27

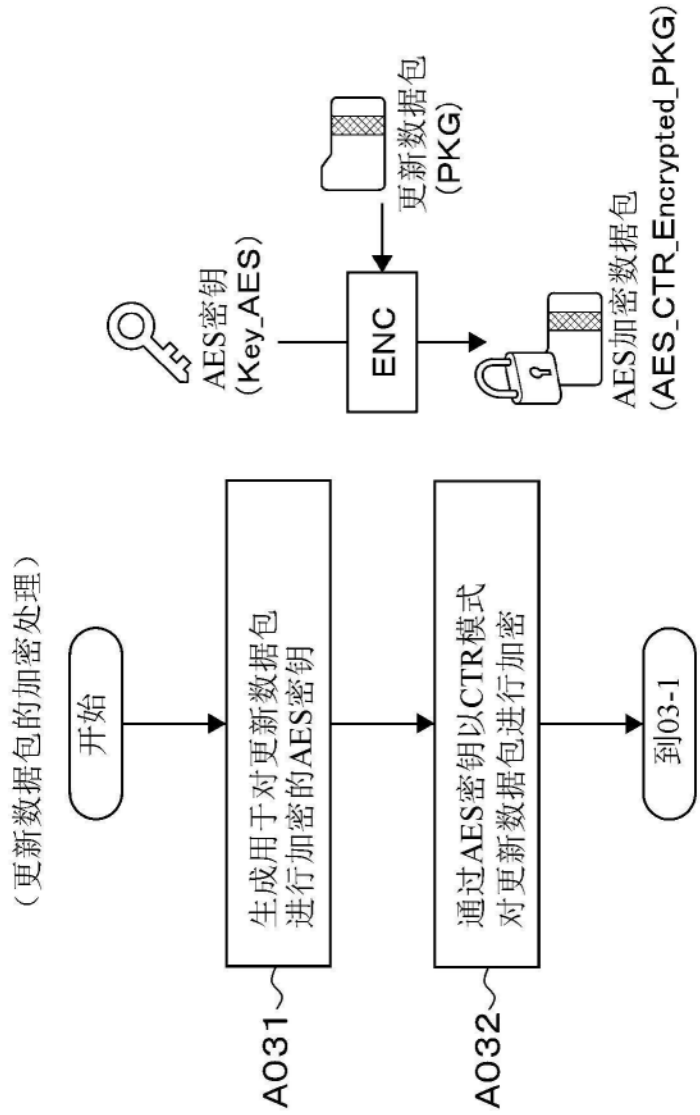

（更新数据包的加密处理）
开始
生成用于对更新数据包进行加密的AES密钥
A031
通过AES密钥以CTR模式对更新数据包进行加密
A032
到03-1
AES密钥
(Key_AES)
ENC
更新数据包
(PKG)
AES加密数据包
(AES_CTR_Encrypted_PKG)

图28

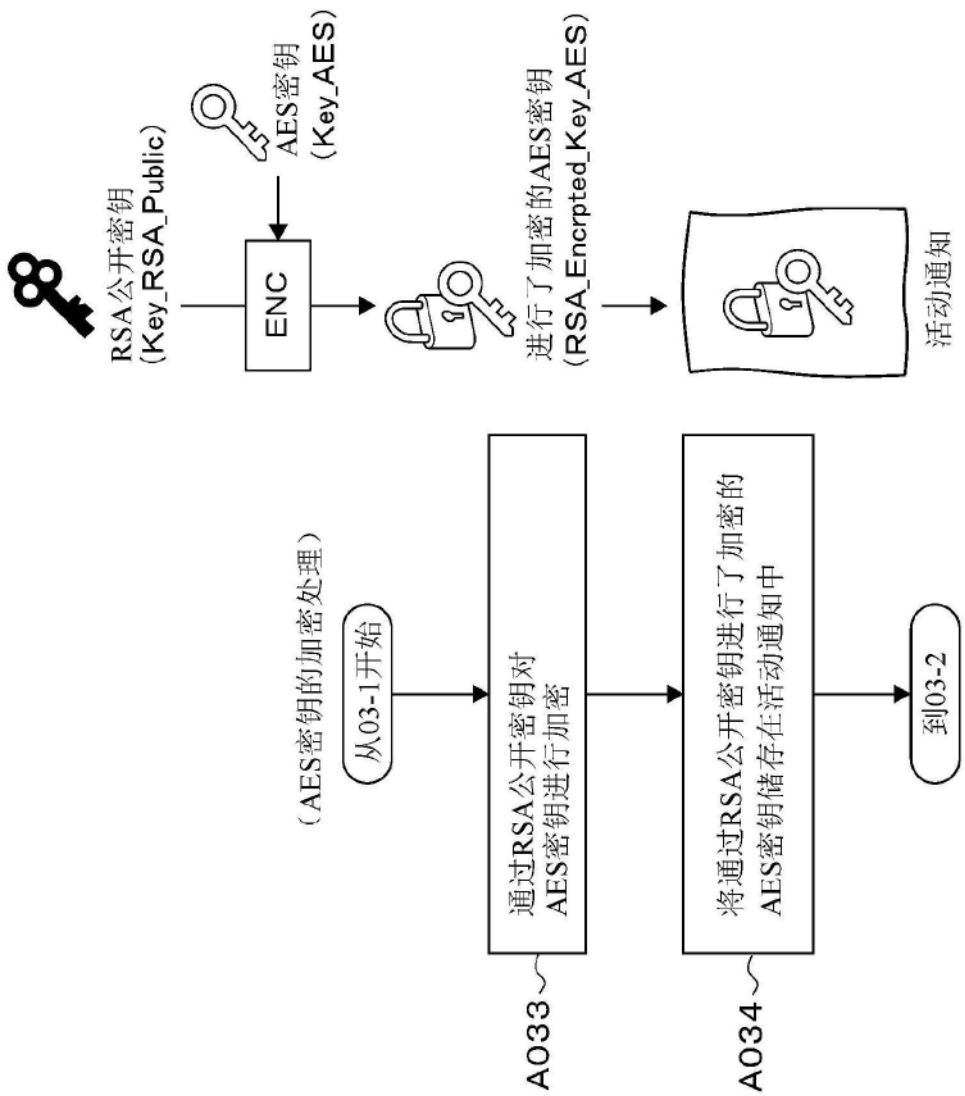

RSA公开密钥
(Key_RSA_Public)
AES密钥
(Key_AES)
ENC
进行了加密的AES密钥
(RSA_Encrpted_Key_AES)
活动通知
(AES密钥的加密处理)
从03-1开始
通过RSA公开密钥对
AES密钥进行加密
将通过RSA公开密钥进行了加密的
AES密钥储存在活动通知中
到03-2
A033
A034

图29

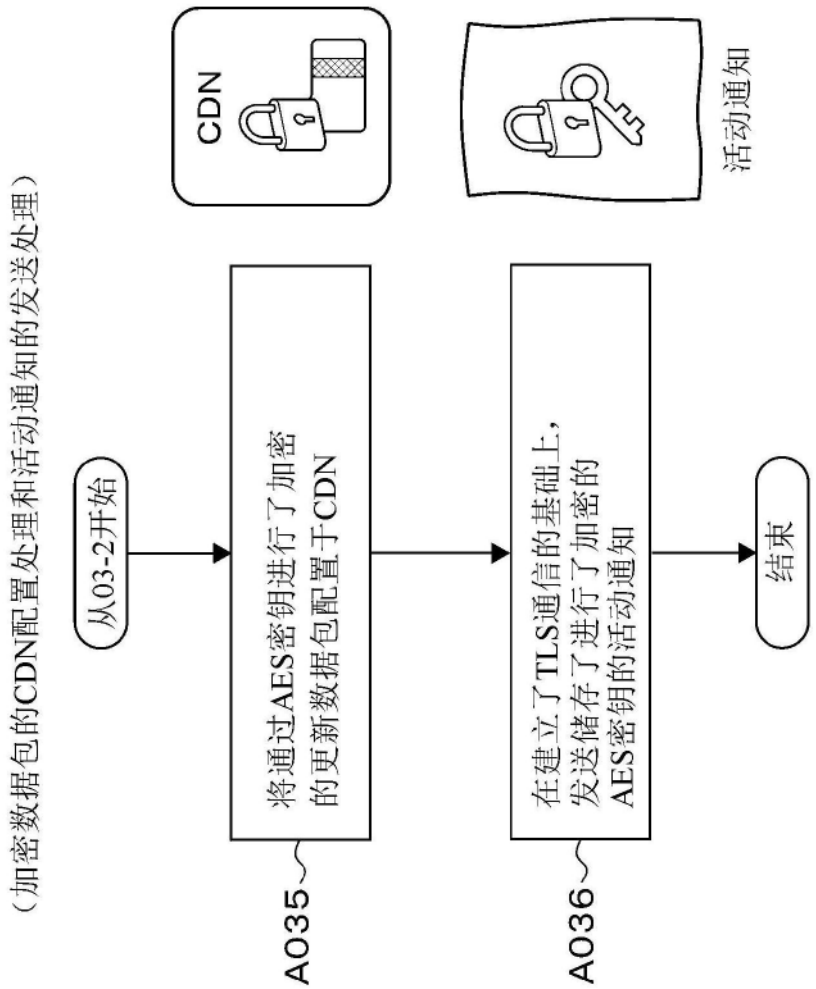

（加密数据包的CDN配置处理和活动通知的发送处理）
从03-2开始
将通过AES密钥进行了加密的更新数据包配置于CDN
A035
在建立了TLS通信的基础上，发送储存了进行了加密的AES密钥的活动通知
A036
结束
CDN
活动通知

图30

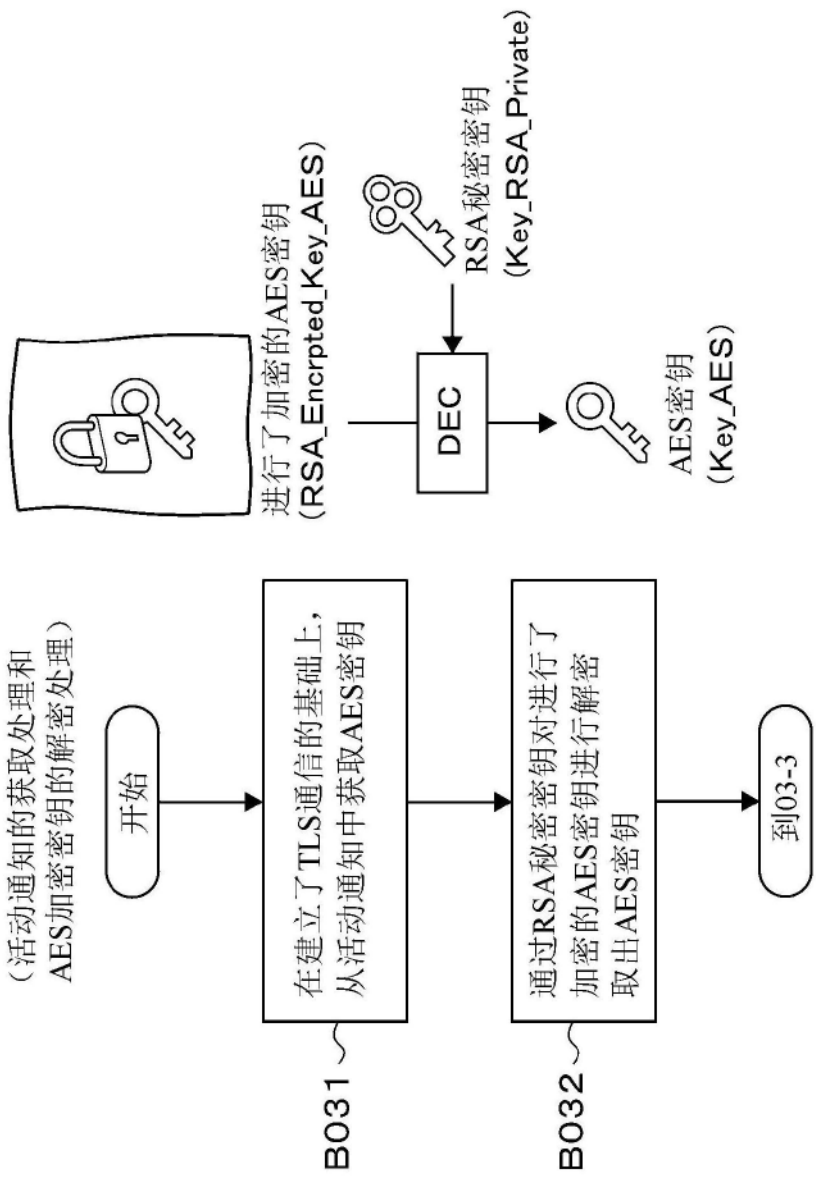

（活动通知的获取处理和
AES加密密钥的解密处理）
开始
在建立了TLS通信的基础上，
从活动通知中获取AES密钥
B031
通过RSA秘密密钥对进行了
加密的AES密钥进行解密
取出AES密钥
B032
到03-3
进行了加密的AES密钥
(RSA_Encrpted_Key_AES)
RSA秘密密钥
(Key_RSA_Private)
DEC
AES密钥
(Key_AES)

图31

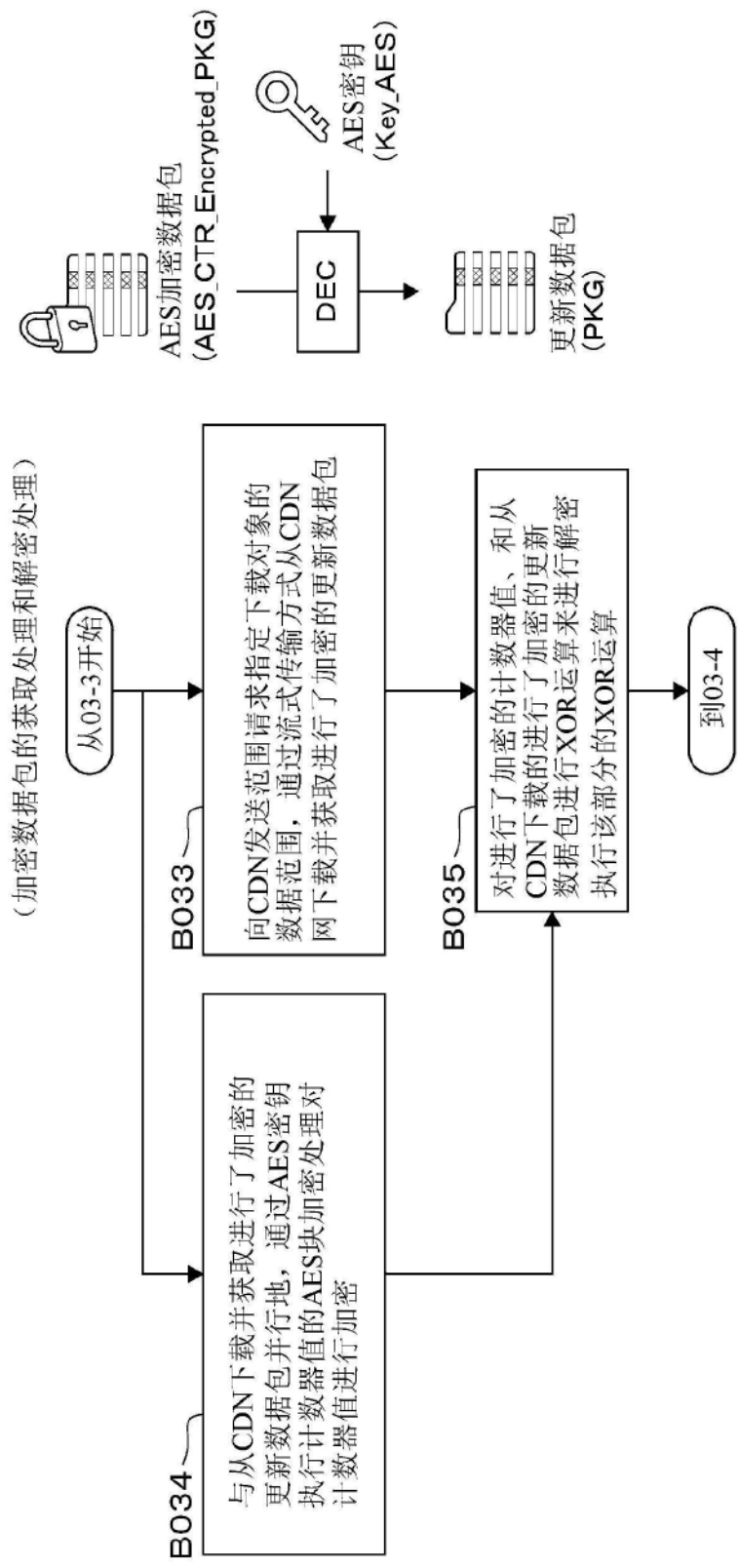

AES加密数据包
(AES_CTR_Encrypted_PKG)
AES密钥
(Key_AES)
DEC
更新数据包
(PKG)
（加密数据包的获取处理和解密处理）
从03-3开始
B033
向CDN发送范围请求指定下载对象的数据范围，通过流式传输方式从CDN网下载并获取进行了加密的更新数据包
B035
对进行了加密的计数器值、和从CDN下载的进行了加密的更新数据包进行XOR运算来进行解密执行该部分的XOR运算
到03-4
B034
与从CDN下载并获取进行了加密的更新数据包并行地，通过AES密钥执行计数器值的AES块加密处理对计数器值进行加密

图32

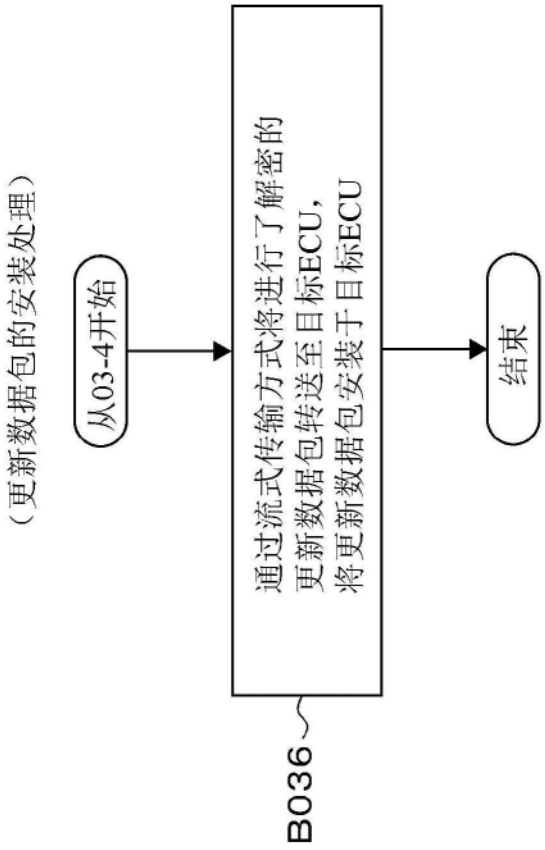

（更新数据包的安装处理）
从03-4开始
通过流式传输方式将进行了解密的
更新数据包转送至目标ECU，
将更新数据包安装于目标ECU
结束
B036

图33

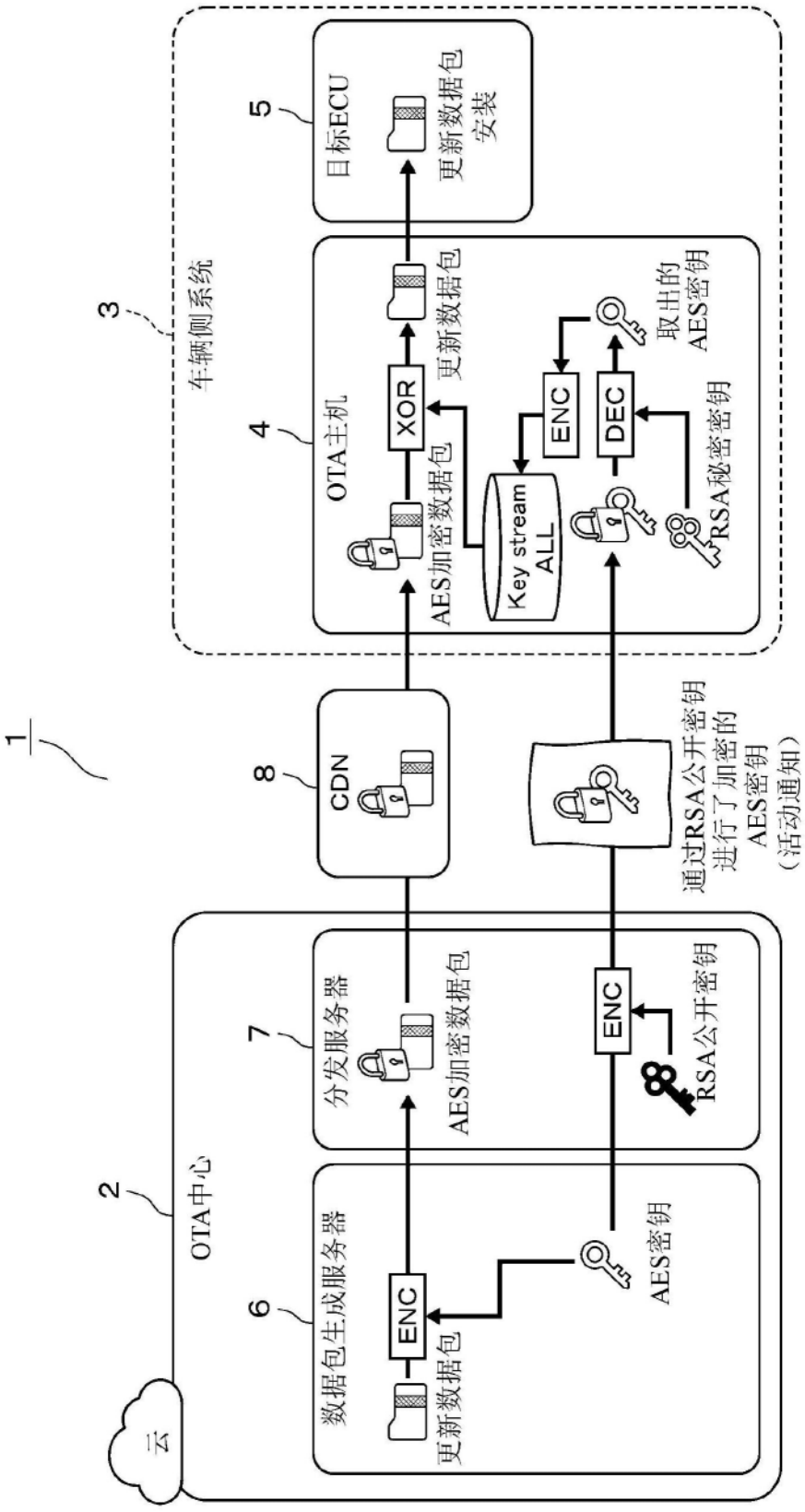

1
2
OTA中心
云
6
数据包生成服务器
更新数据包
ENC
AES密钥
7
分发服务器
AES加密数据包
RSA公开密钥
ENC
8
CDN
通过RSA公开密钥
进行了加密的
AES密钥
（活动通知）
3
车辆侧系统
4
OTA主机
AES加密数据包
XOR
更新数据包
Key stream
ALL
ENC
DEC
取出的
AES密钥
RSA秘密密钥
5
目标ECU
更新数据包
安装

图34

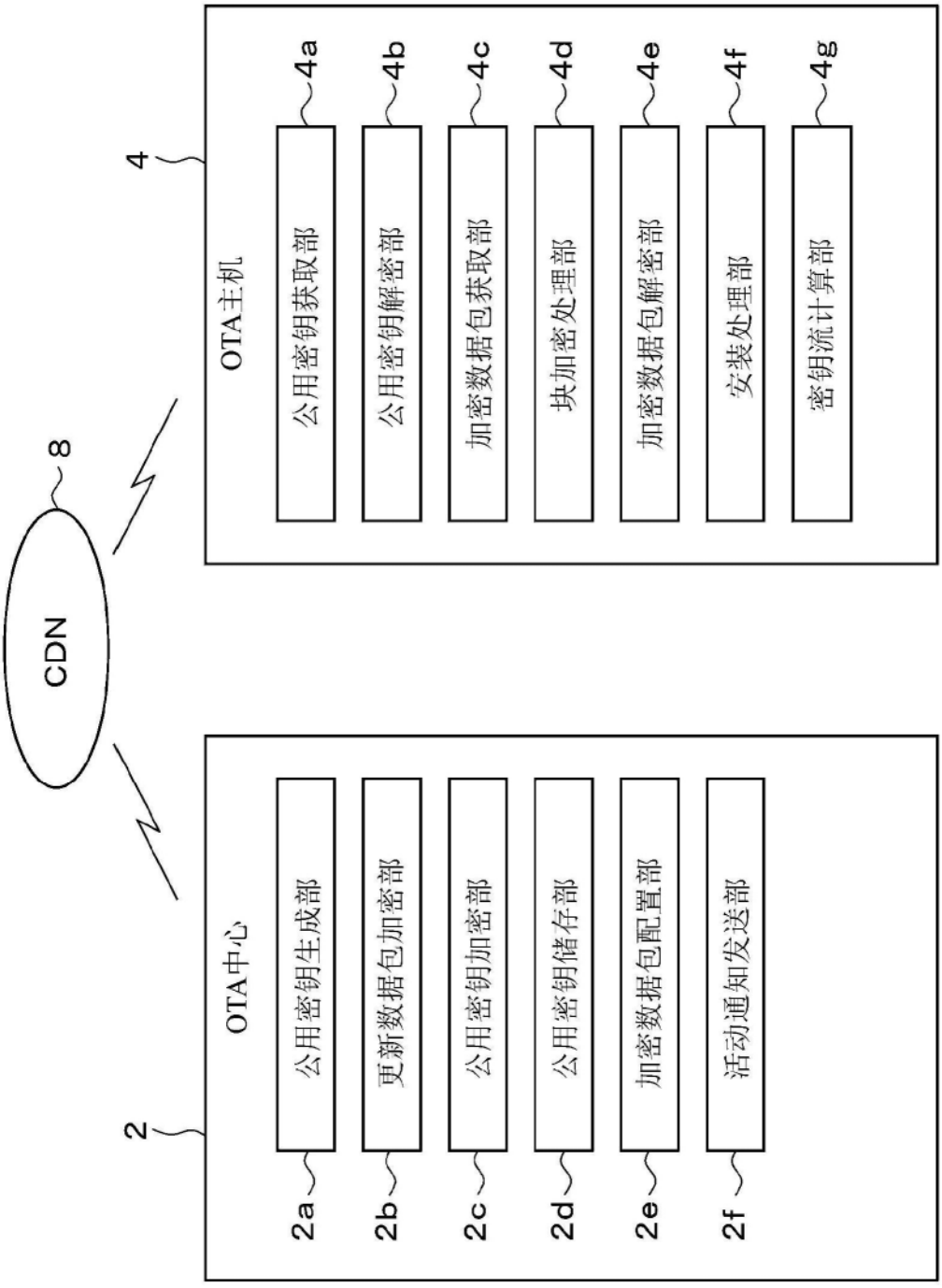

OTA中心
2
公用密钥生成部
2a
更新数据包加密部
2b
公用密钥加密部
2c
公用密钥储存部
2d
加密数据包配置部
2e
活动通知发送部
2f
CDN
8
OTA主机
4
公用密钥获取部
4a
公用密钥解密部
4b
加密数据包获取部
4c
块加密处理部
4d
加密数据包解密部
4e
安装处理部
4f
密钥流计算部
4g

图35

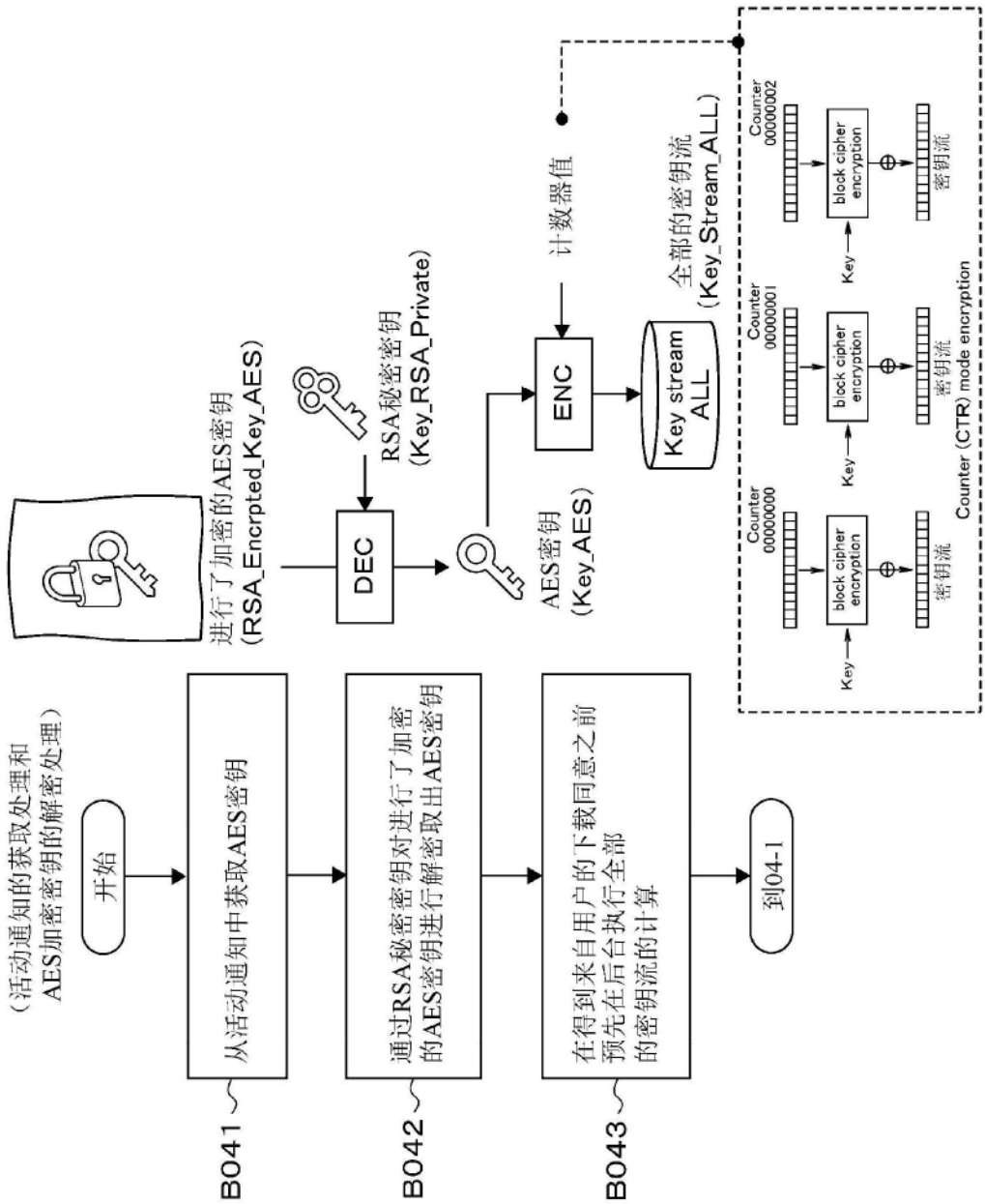

（活动通知的获取处理和
AES加密密钥的解密处理）
开始
从活动通知中获取AES密钥
通过RSA秘密密钥对进行了加密
的AES密钥进行解密取出AES密钥
在得到来自用户的下载同意之前
预先在后台执行全部
的密钥流的计算
到04-1
B041
B042
B043
进行了加密的AES密钥
(RSA_Encrpted_Key_AES)
DEC
RSA秘密密钥
(Key_RSA_Private)
AES密钥
(Key_AES)
ENC
计数器值
Key stream
ALL
全部的密钥流
(Key_Stream_ALL)
Counter
00000000
Counter
00000001
Counter
00000002
block cipher
encryption
Key
密钥流
Counter (CTR) mode encryption

图36

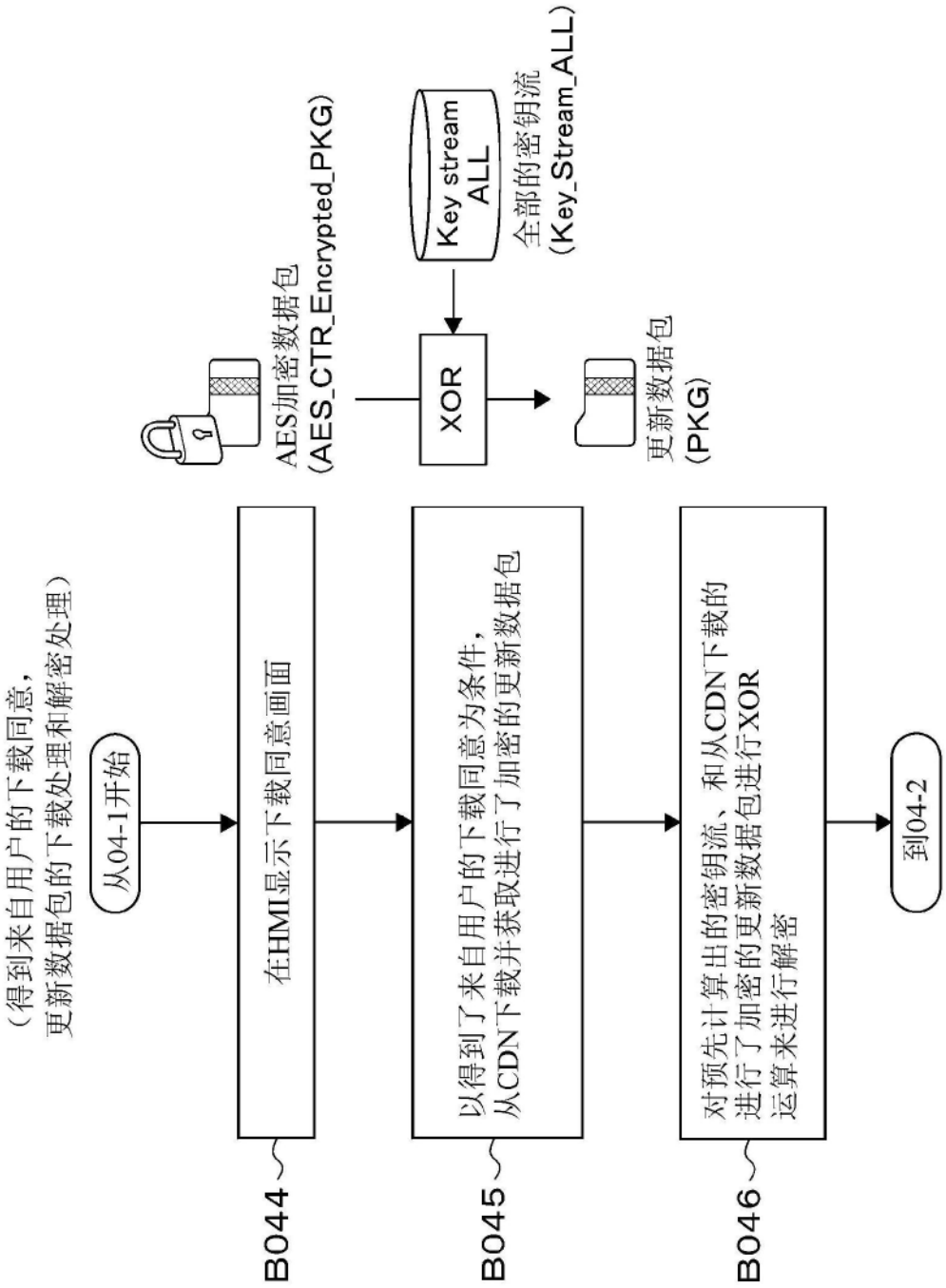

（得到来自用户的下载同意，
更新数据包的下载处理和解密处理）
从04-1开始
在HMI显示下载同意画面
以得到了来自用户的下载同意为条件，
从CDN下载并获取进行了加密的更新数据包
对预先计算出的密钥流、和从CDN下载的
进行了加密的更新数据包进行XOR
运算来进行解密
到04-2
B044
B045
B046
AES加密数据包
(AES_CTR_Encrypted_PKG)
Key stream
ALL
全部的密钥流
(Key_Stream_ALL)
XOR
更新数据包
(PKG)

图37

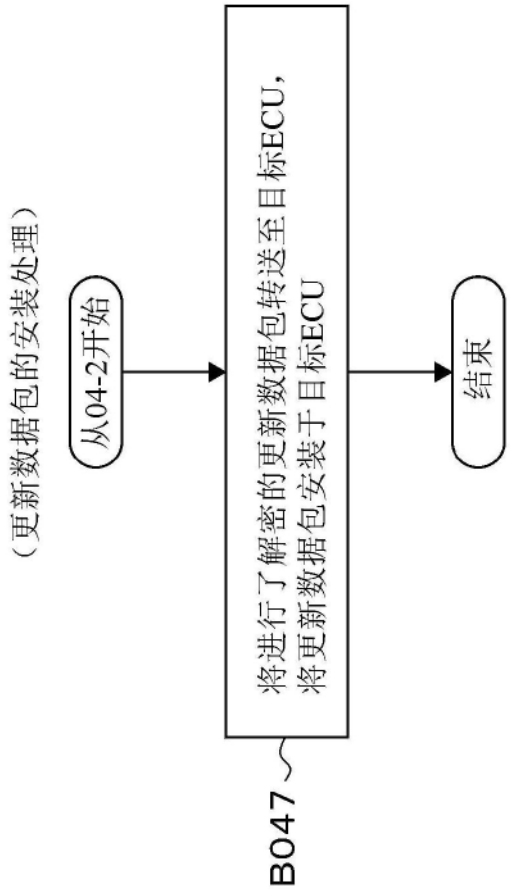

（更新数据包的安装处理）
从04-2开始
将进行了解密的更新数据包转送至目标ECU，
将更新数据包安装于目标ECU
结束
B047

图38

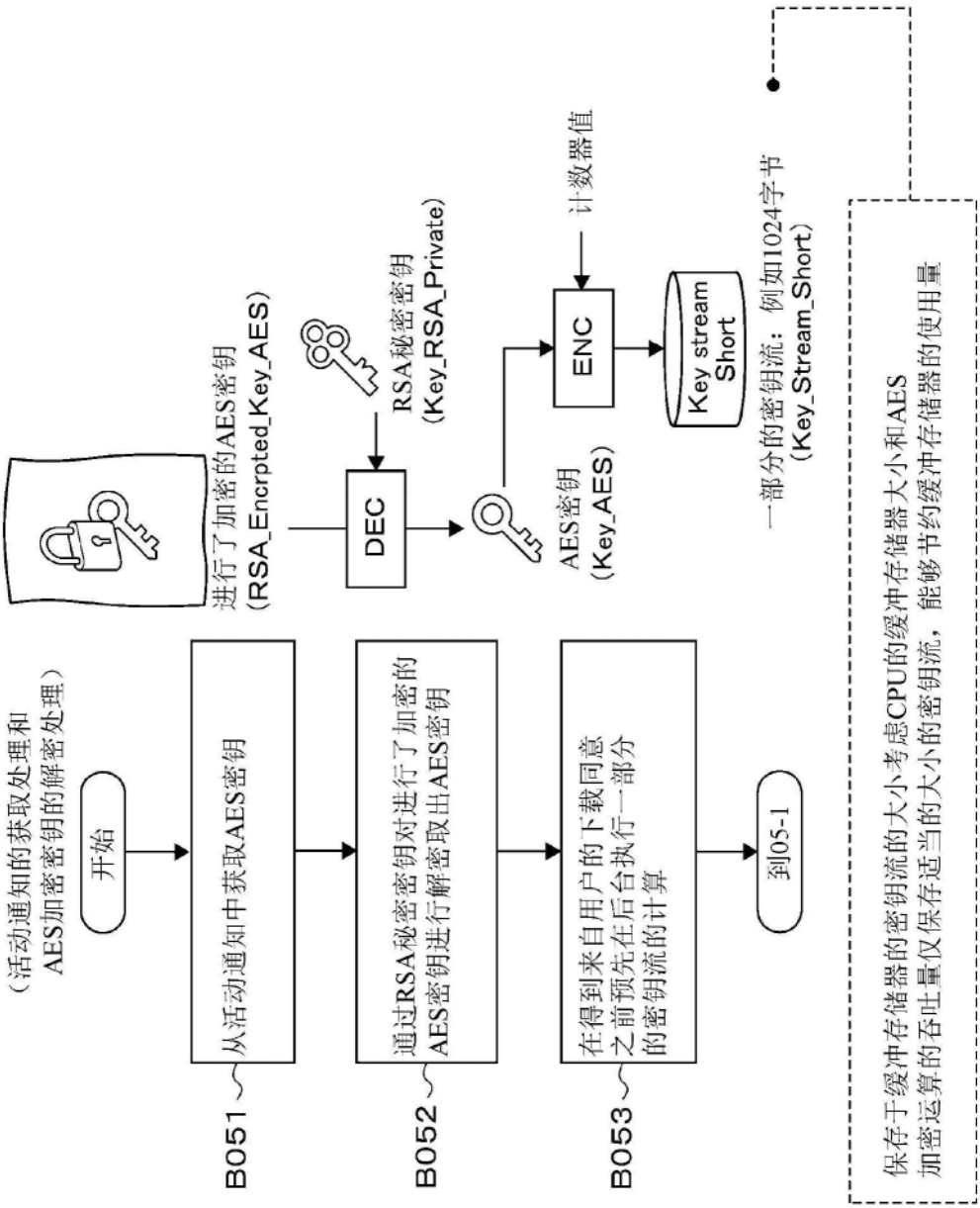

（活动通知的获取处理和
AES加密密钥的解密处理）
开始
B051
从活动通知中获取AES密钥
B052
通过RSA秘密密钥对进行了加密的
AES密钥进行解密取出AES密钥
B053
在得到来自用户的下载同意
之前预先在后台执行一部分
的密钥流的计算
到05-1
进行了加密的AES密钥
(RSA_Encrpted_Key_AES)
DEC
RSA秘密密钥
(Key_RSA_Private)
AES密钥
(Key_AES)
ENC
计数器值
Key stream
Short
一部分的密钥流：例如1024字节
(Key_Stream_Short)
保存于缓冲存储器的密钥流的大小考虑CPU的缓冲存储器大小和AES
加密运算的吞吐量仅保存适当的大小的密钥流，能够节约缓冲存储器的使用量

图39

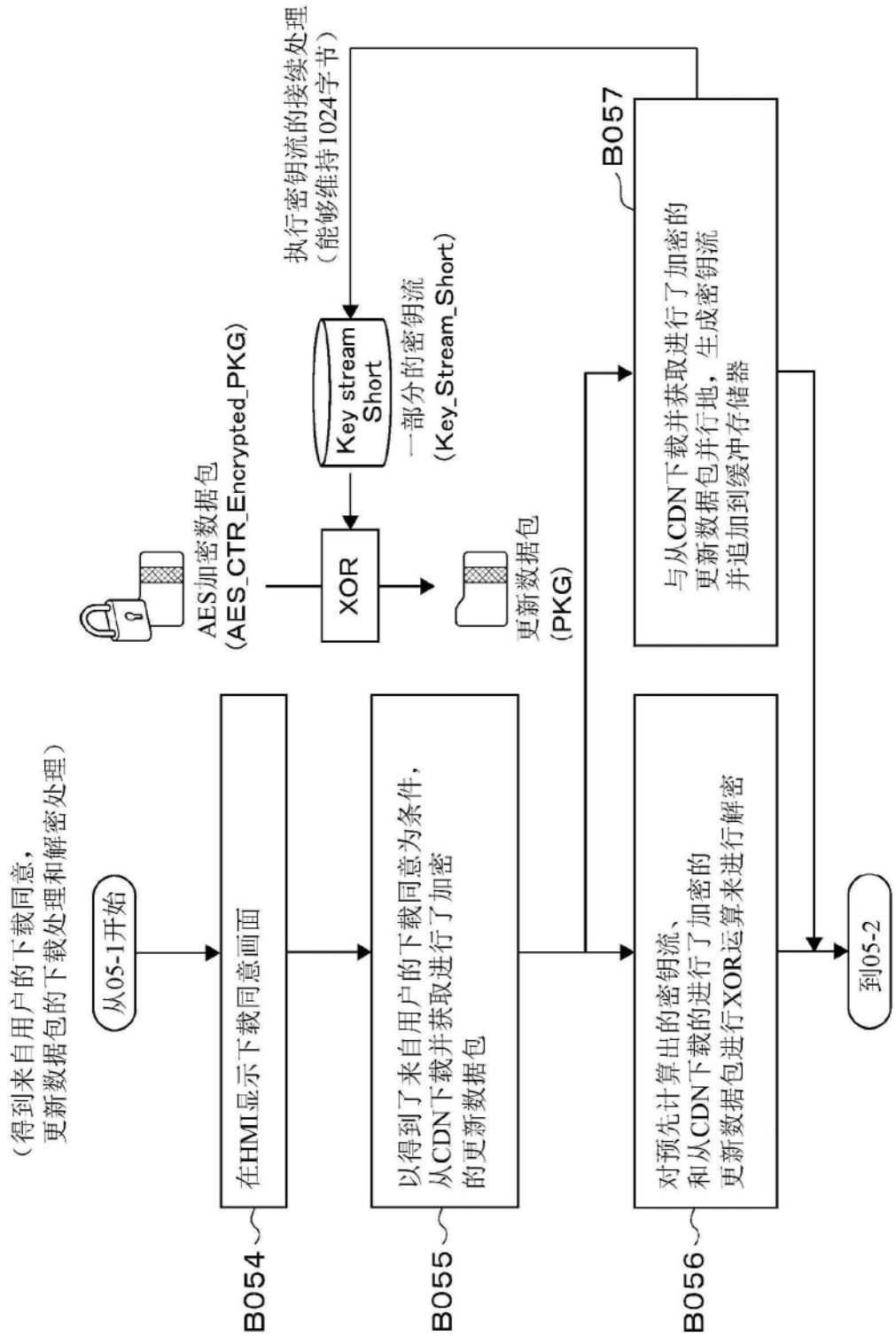

（得到来自用户的下载同意，
更新数据包的下载处理和解密处理）
从05-1开始
B054
在HMI显示下载同意画面
B055
以得到了来自用户的下载同意为条件，
从CDN下载并获取进行了加密
的更新数据包
B056
对预先计算出的密钥流、
和从CDN下载的进行了加密的
更新数据包进行XOR运算来进行解密
到05-2
B057
与从CDN下载并获取进行了加密的
更新数据包并行地，生成密钥流
并追加到缓冲存储器
更新数据包
(PKG)
XOR
AES加密数据包
(AES_CTR_Encrypted_PKG)
Key stream
Short
一部分的密钥流
(Key_Stream_Short)
执行密钥流的接续处理
（能够维持1024字节）

图40

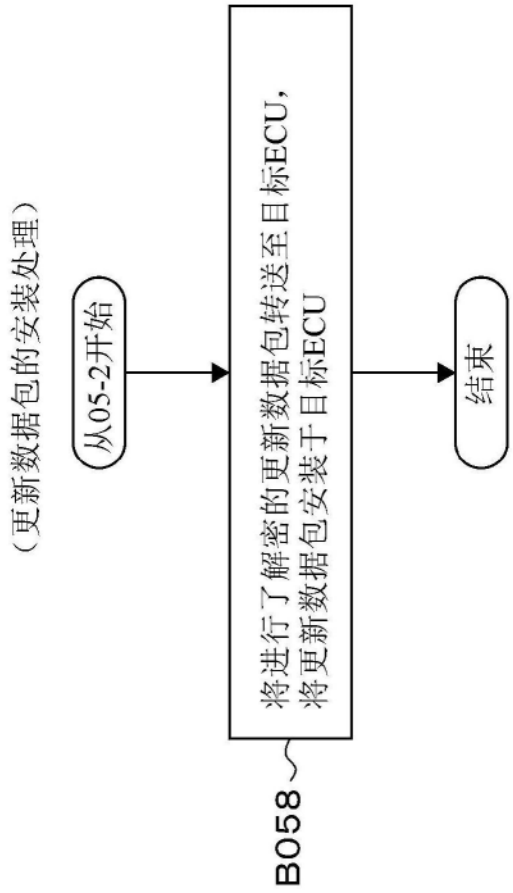

（更新数据包的安装处理）
从05-2开始
将进行了解密的更新数据包转送至目标ECU，
将更新数据包安装于目标ECU
B058
结束

图41

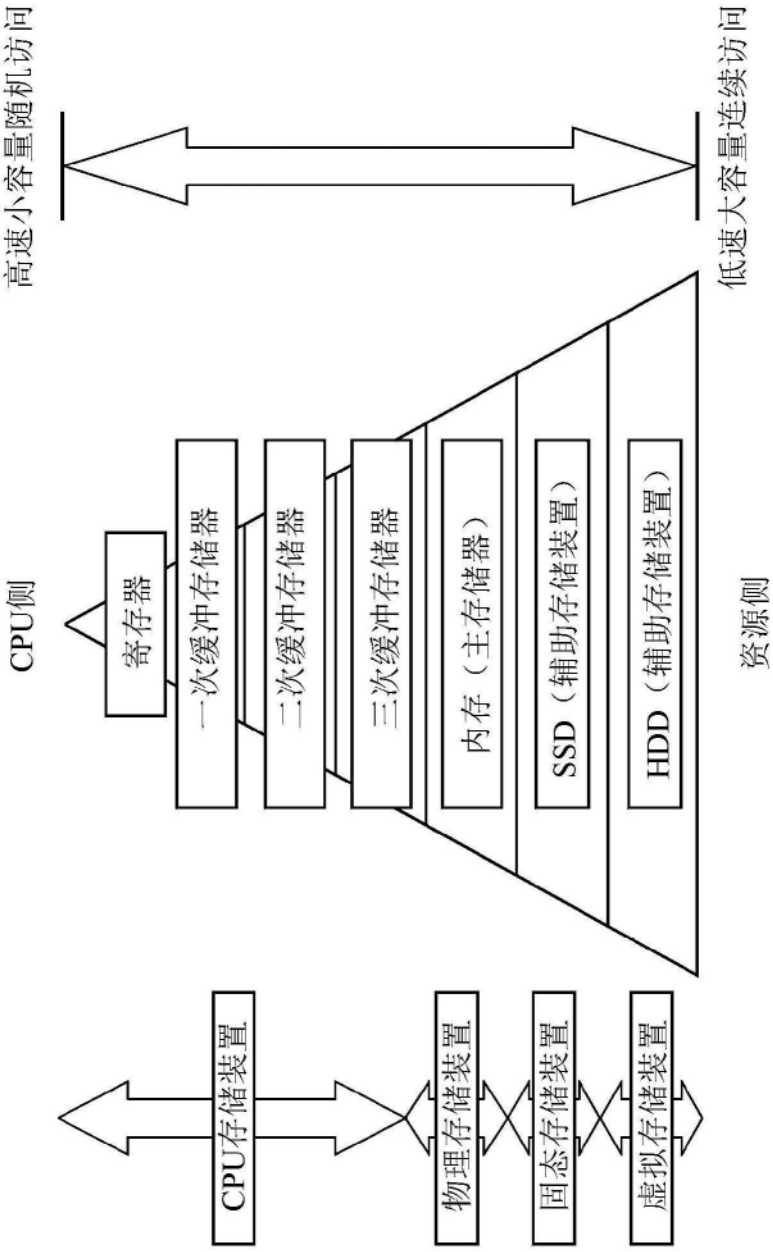

高速小容量随机访问
低速大容量连续访问
CPU侧
资源侧
寄存器
一次缓冲存储器
二次缓冲存储器
三次缓冲存储器
内存（主存储器）
SSD（辅助存储装置）
HDD（辅助存储装置）
CPU存储装置
物理存储装置
固态存储装置
虚拟存储装置

图42

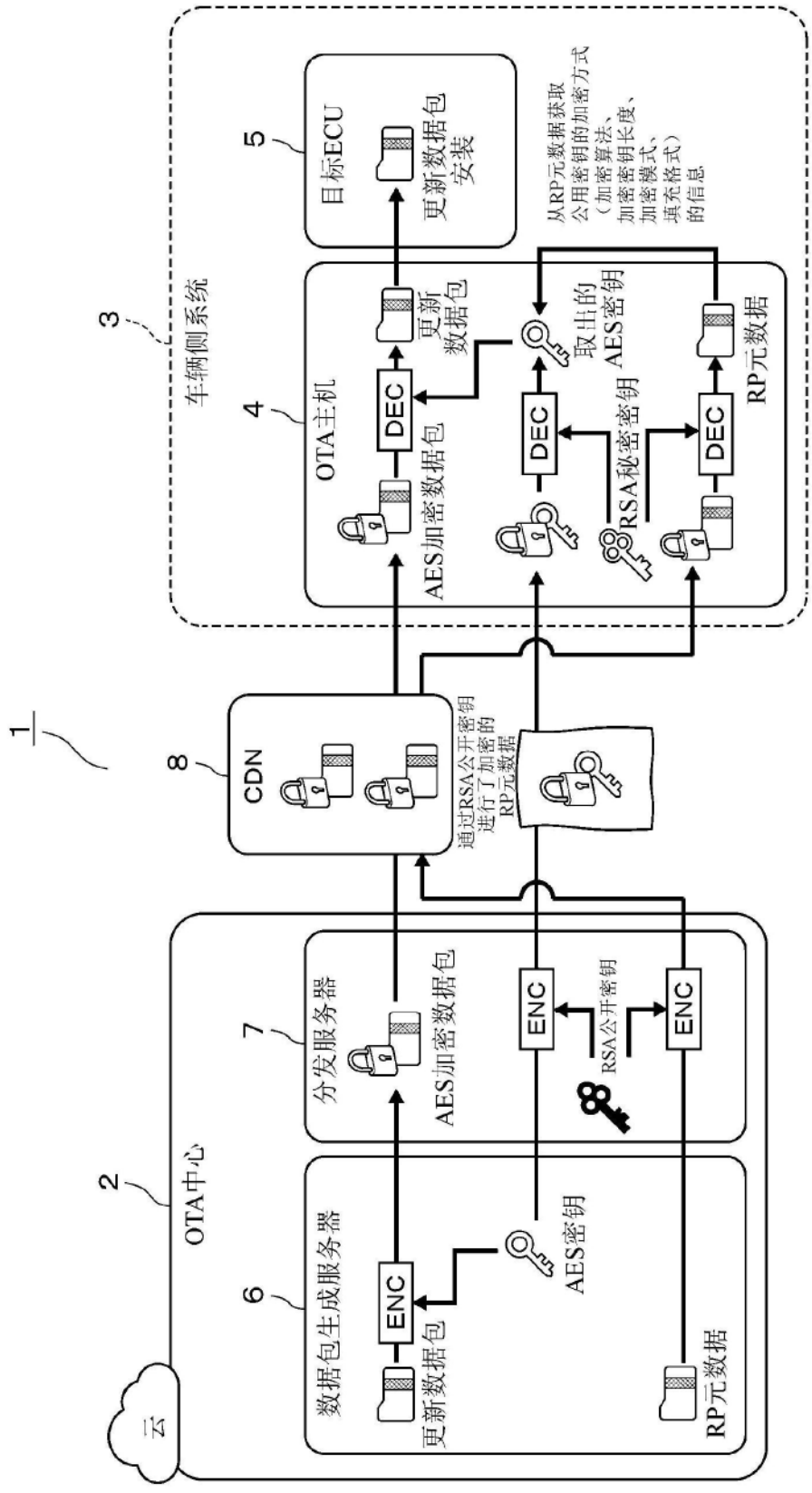

1
2
OTA中心
云
6
数据包生成服务器
更新数据包
ENC
AES密钥
RP元数据
7
分发服务器
AES加密数据包
ENC
RSA公开密钥
ENC
8
CDN
通过RSA公开密钥
进行了加密的
RP元数据
3
车辆侧系统
4
OTA主机
AES加密数据包
DEC
更新
数据包
DEC
RSA秘密密钥
DEC
取出的
AES密钥
RP元数据
从RP元数据获取
公用密钥的加密方式
（加密算法、
加密密钥长度、
加密模式、
填充格式）
的信息
5
目标ECU
更新数据包
安装

图43

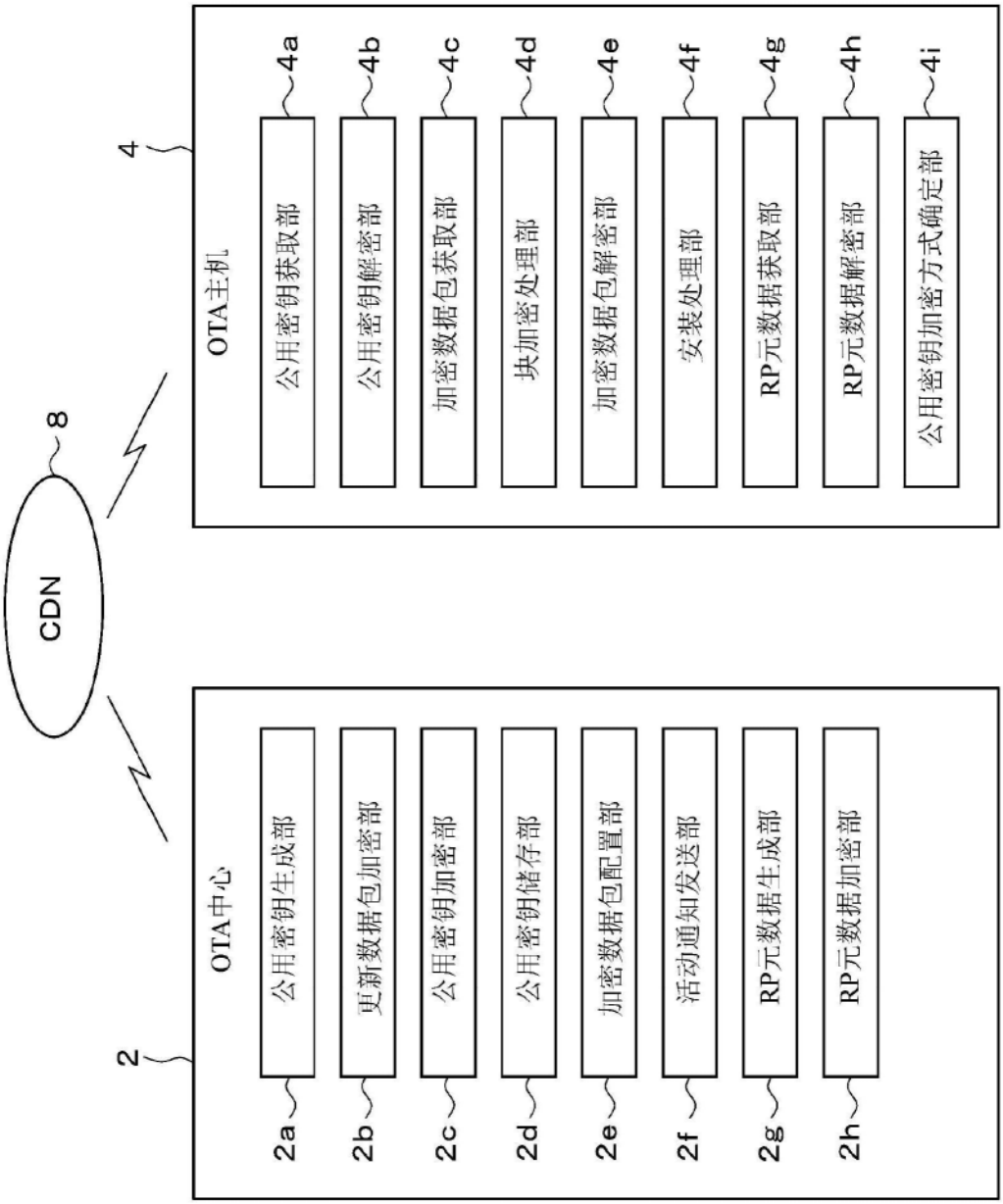

OTA中心
2
公用密钥生成部
2a
更新数据包加密部
2b
公用密钥加密部
2c
公用密钥储存部
2d
加密数据包配置部
2e
活动通知发送部
2f
RP元数据生成部
2g
RP元数据加密部
2h
CDN
8
OTA主机
4
公用密钥获取部
4a
公用密钥解密部
4b
加密数据包获取部
4c
块加密处理部
4d
加密数据包解密部
4e
安装处理部
4f
RP元数据获取部
4g
RP元数据解密部
4h
公用密钥加密方式确定部
4i

图44

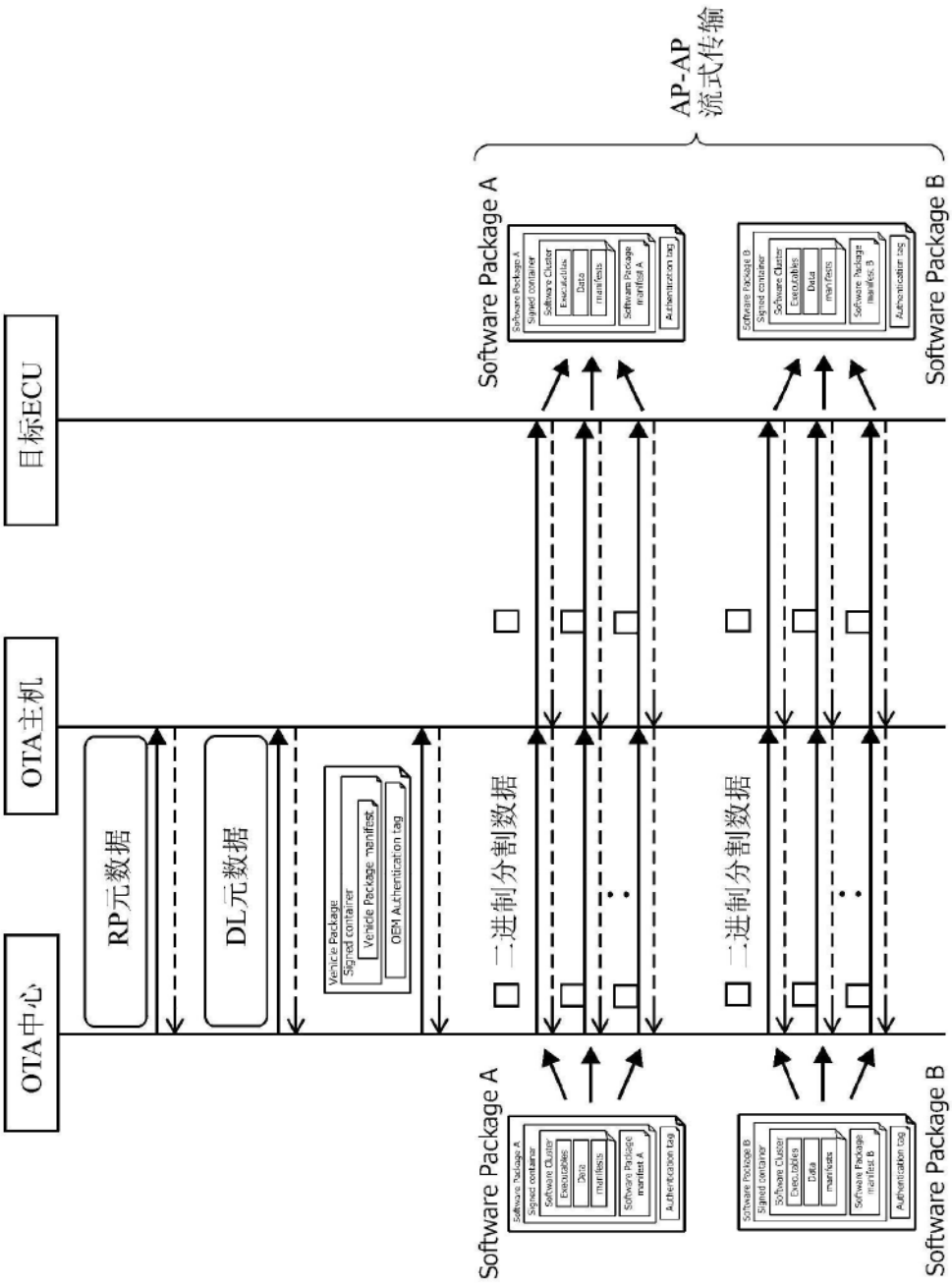

AP-AP
流式传输
目标ECU
OTA主机
OTA中心
RP元数据
DL元数据
Vehicle Package
Signed container
Vehicle Package manifest
OEM Authentication tag
二进制分割数据
二进制分割数据
Software Package A
Software Package B
Software Package A
Signed container
Software Cluster
Executables
Data
manifests
Software Package manifest A
Authentication tag
Software Package B
Signed container
Software Cluster
Executables
Data
manifests
Software Package manifest B
Authentication tag

图45

■ 重编策略元数据版本 ：1.0.0/2.0.0/…

■ 分发层
1.通信协议 ：Uptane/OMA-DM/SSL/…none
2.通信单元：蜂窝/智能手机/USB存储器

■ 主机层（可能存在多个）
PF ：AP/CP/AGL/Android/…
控制方式： ：参数/脚本 /…
加密方式
①加密算法 ：AES、3key-Tripple DES、CLEFIA（轻量加密）etc
②加密密钥长度 ：128bit、256bit、etc
③加密模式 ：CBC 模式、CTR 模式、OFB 模式、etc
④Padding方式 ：PKCS#5 padding、PKCS#7 padding、No padding、etc
⑤加密密钥ID ：1 （使用于加密密钥的确定）
⑥签名算法 ：MAC （公用密钥）、DSA（公开密钥）
⑦签名密钥ID ：2（使用于签名密钥的确定）
⑧签名模式 ：Enc then MAC、MAC then ENC、ENC and MAC、…
⑨散列算法 ：SHA2、SHA1、PHOTO（轻量加密）
⑩区域指定有无 ：选择文件整体或者范围指定
⑪偏移大小 ：0 （指定从前端第几字节开始保护；⑨仅为范围指定的情况）
⑫保护数据大小 ：1024（指定保护几字节；⑨仅为范围指定的情况）

图46

■目标层（可能存在多个）
PF ：AP/CP/AGL/Android/…
转送方式 ：储存方式/流式传输放松 /…
控制方式 ：参数/脚本 /…
目标ID ：（选项）
加密方式
①加密算法 ：AES、3key-Tripple DES、CLEFIA（轻量加密）, etc
②加密密钥长度 ：128bit、256bit、etc
③加密模式 ：CBC 模式 、CTR模式 、OFB模式 、etc
④Padding方式 ：PKCS#5 padding、PKCS#7 padding、No padding、etc
⑤加密密钥ID ：1 （使用于加密密钥的确定）
⑥签名算法 ：MAC （公用密钥）、DSA（公开密钥）
⑦签名密钥ID ：2（使用于签名密钥的确定）
⑧签名模式 ：Enc then MAC、MAC then ENC、ENC and MAC、…
⑨散列算法 ：SHA2、SHA1、PHOTO（轻量加密）
⑩区域指定有无 ：选择文件整体或者范围指定
⑪ 偏移大小 ：0 （指定从前端第几字节开始保护：⑨仅为范围指定的情况）
⑫ 保护数据大小 ：1024（指定保护几字节：⑨仅为范围指定的情况）

图47

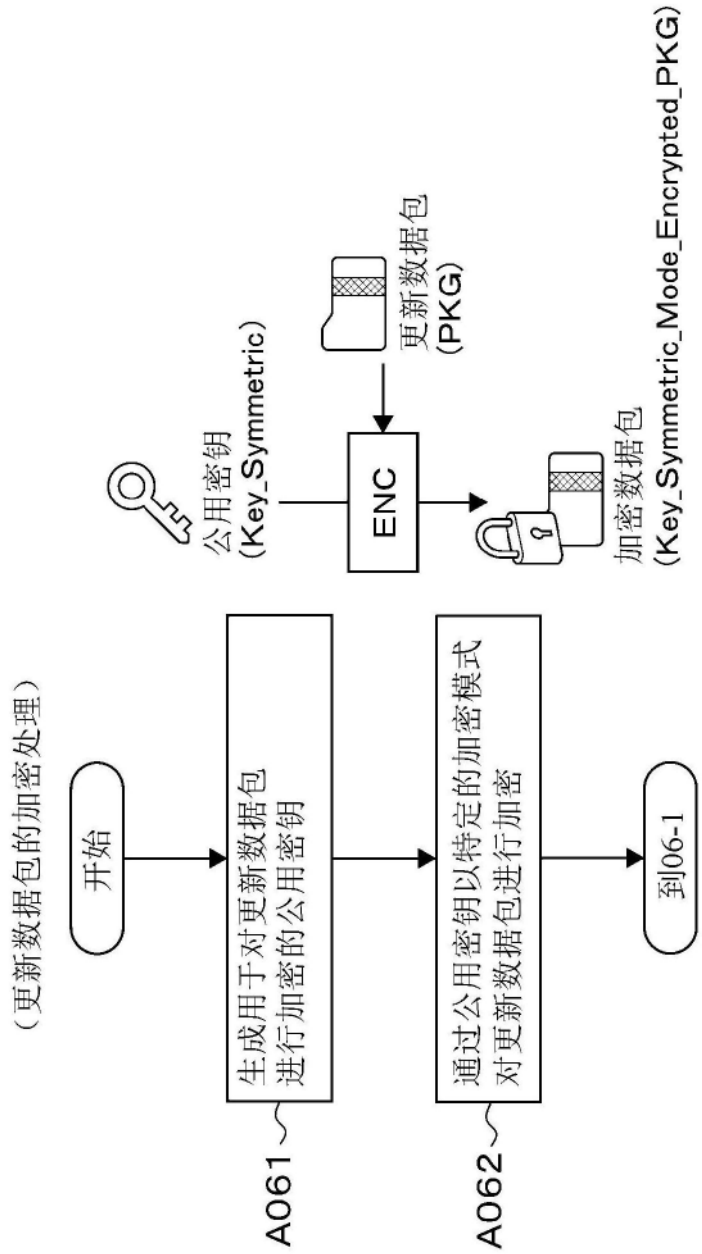

（更新数据包的加密处理）
开始
生成用于对更新数据包
进行加密的公用密钥
A061
通过公用密钥以特定的加密模式
对更新数据包进行加密
A062
到06-1
公用密钥
(Key_Symmetric)
更新数据包
(PKG)
ENC
加密数据包
(Key_Symmetric_Mode_Encrypted_PKG)

图48

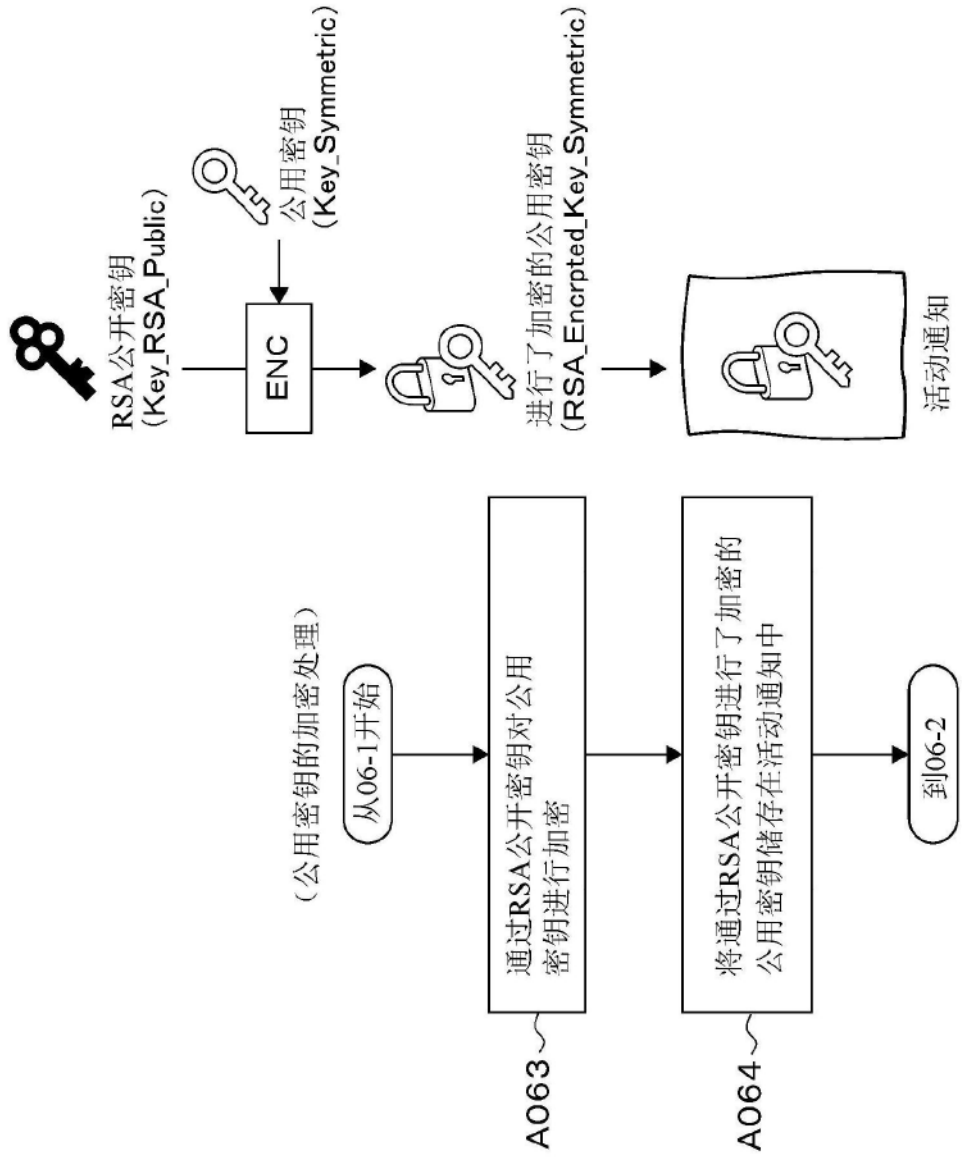

RSA公开密钥
(Key_RSA_Public)
公用密钥
(Key_Symmetric)
ENC
进行了加密的公用密钥
(RSA_Encrpted_Key_Symmetric)
活动通知
（公用密钥的加密处理）
从06-1开始
通过RSA公开密钥对公用
密钥进行加密
将通过RSA公开密钥进行了加密的
公用密钥储存在活动通知中
到06-2
A063
A064

图49

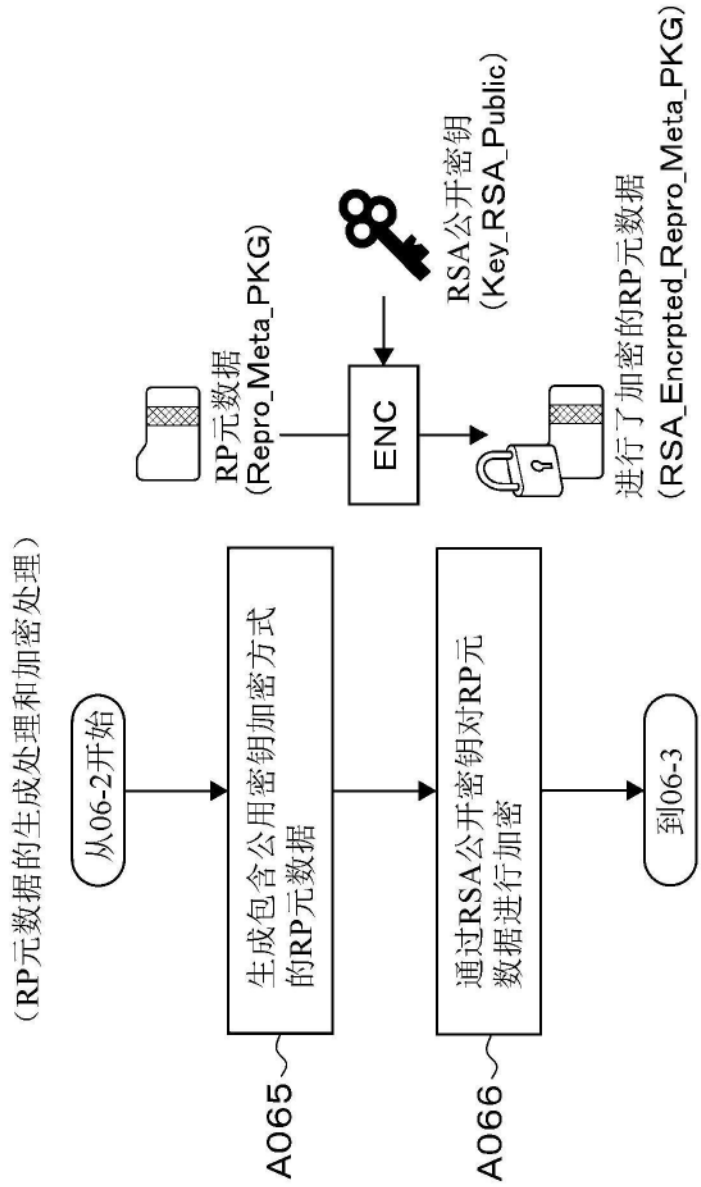

（RP元数据的生成处理和加密处理）
从06-2开始
生成包含公用密钥加密方式的RP元数据
A065
通过RSA公开密钥对RP元数据进行加密
A066
到06-3
RP元数据
(Repro_Meta_PKG)
ENC
RSA公开密钥
(Key_RSA_Public)
进行了加密的RP元数据
(RSA_Encrpted_Repro_Meta_PKG)

图50

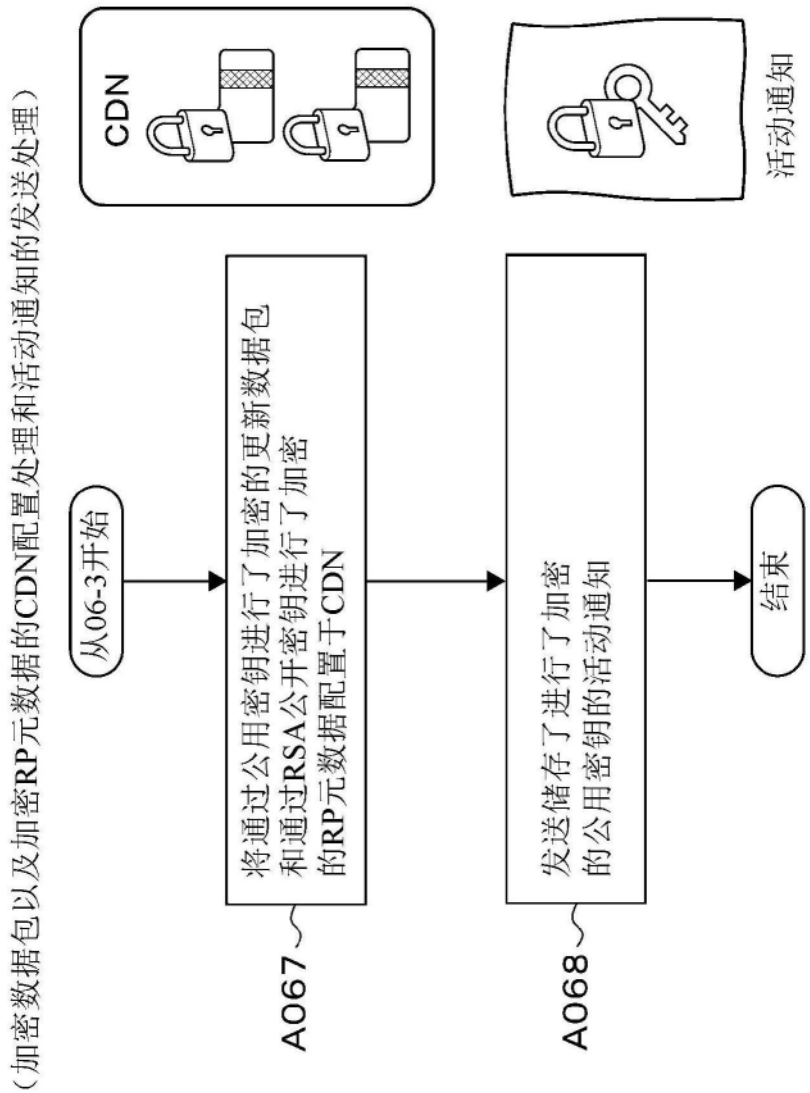

（加密数据包以及加密RP元数据的CDN配置处理和活动通知的发送处理）
从06-3开始
将通过公用密钥进行了加密的更新数据包和通过RSA公开密钥进行了加密的RP元数据配置于CDN
A067
发送储存了进行了加密的公用密钥的活动通知
A068
结束
CDN
活动通知

图51

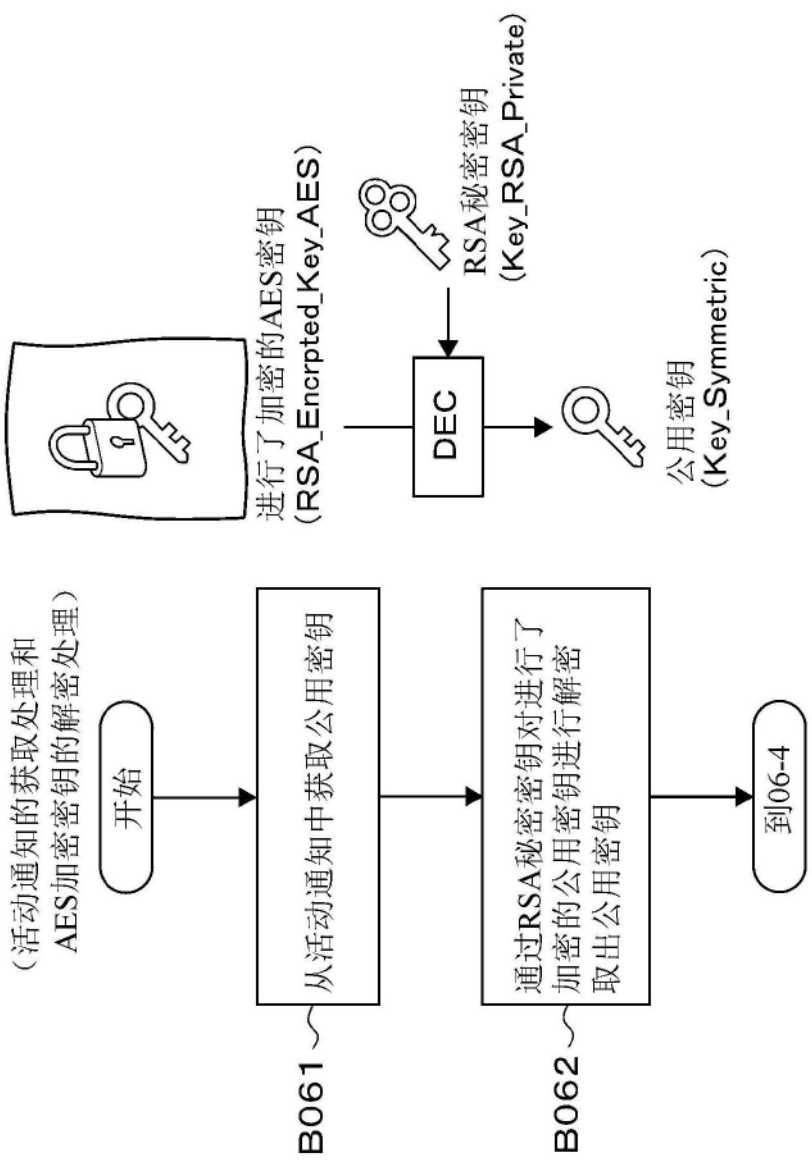

（活动通知的获取处理和
AES加密密钥的解密处理）
开始
从活动通知中获取公用密钥
B061
通过RSA秘密密钥对进行了
加密的公用密钥进行解密
取出公用密钥
B062
到06-4
进行了加密的AES密钥
(RSA_Encrpted_Key_AES)
DEC
RSA秘密密钥
(Key_RSA_Private)
公用密钥
(Key_Symmetric)

图52

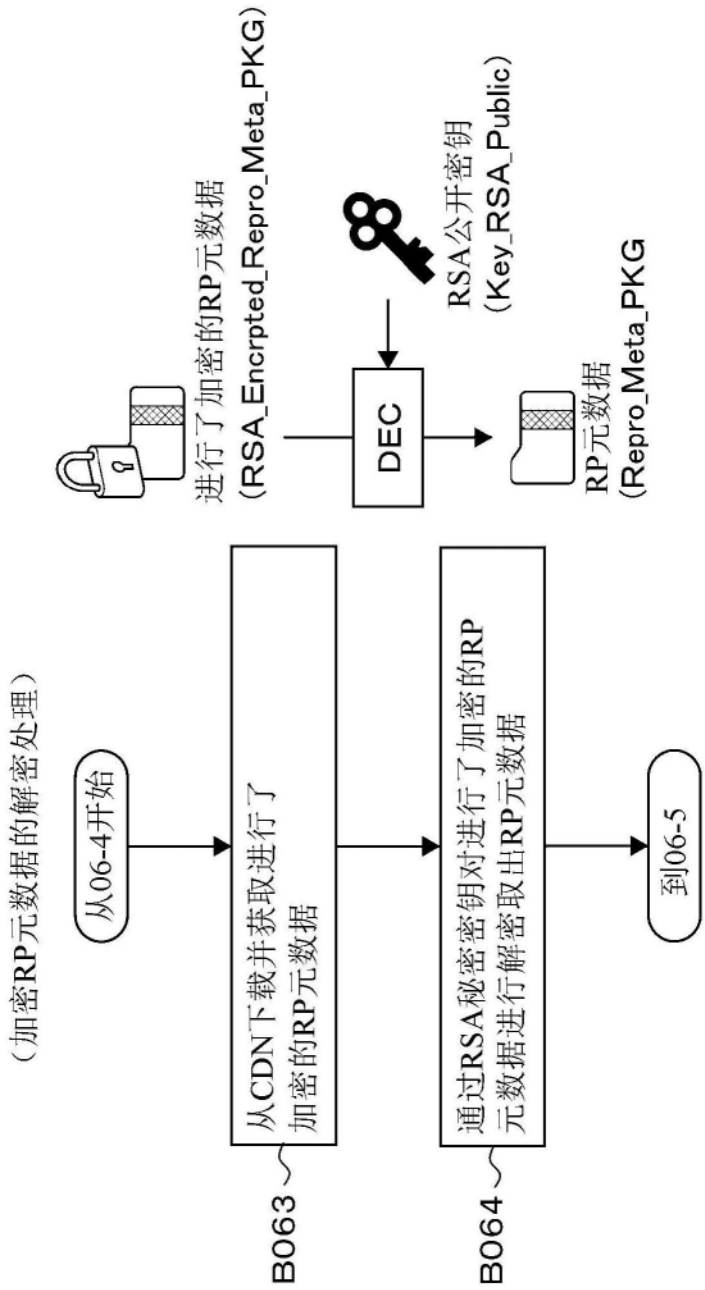

（加密RP元数据的解密处理）
从06-4开始
从CDN下载并获取进行了
加密的RP元数据
B063
通过RSA秘密密钥对进行了加密的RP
元数据进行解密取出RP元数据
B064
到06-5
进行了加密的RP元数据
(RSA_Encrpted_Repro_Meta_PKG)
DEC
RSA公开密钥
(Key_RSA_Public)
RP元数据
(Repro_Meta_PKG

图53

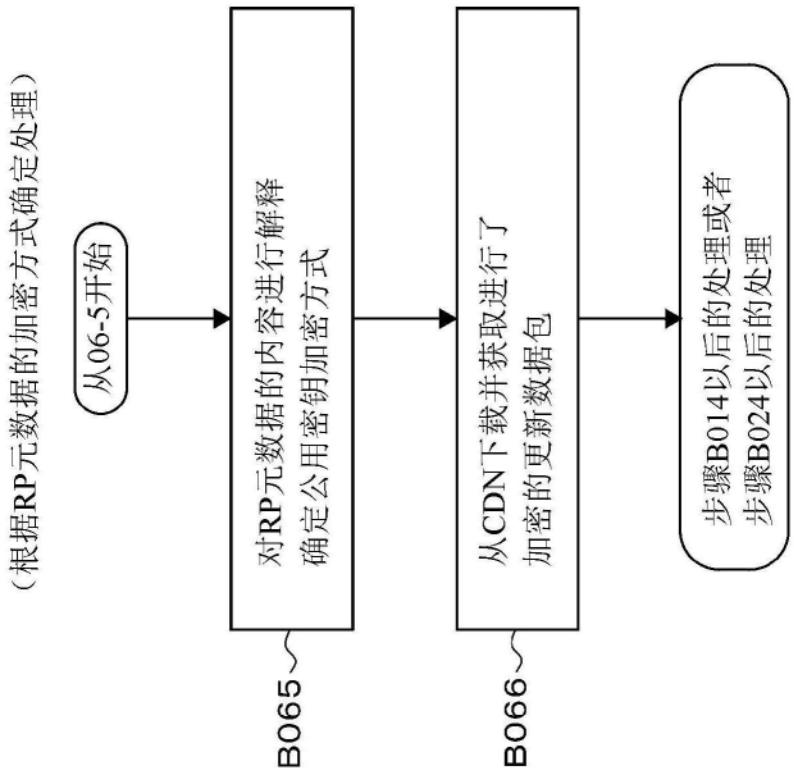

（根据RP元数据的加密方式确定处理）
从06-5开始
对RP元数据的内容进行解释
确定公用密钥加密方式
B065
从CDN下载并获取进行了
加密的更新数据包
B066
步骤B014以后的处理或者
步骤B024以后的处理

图54

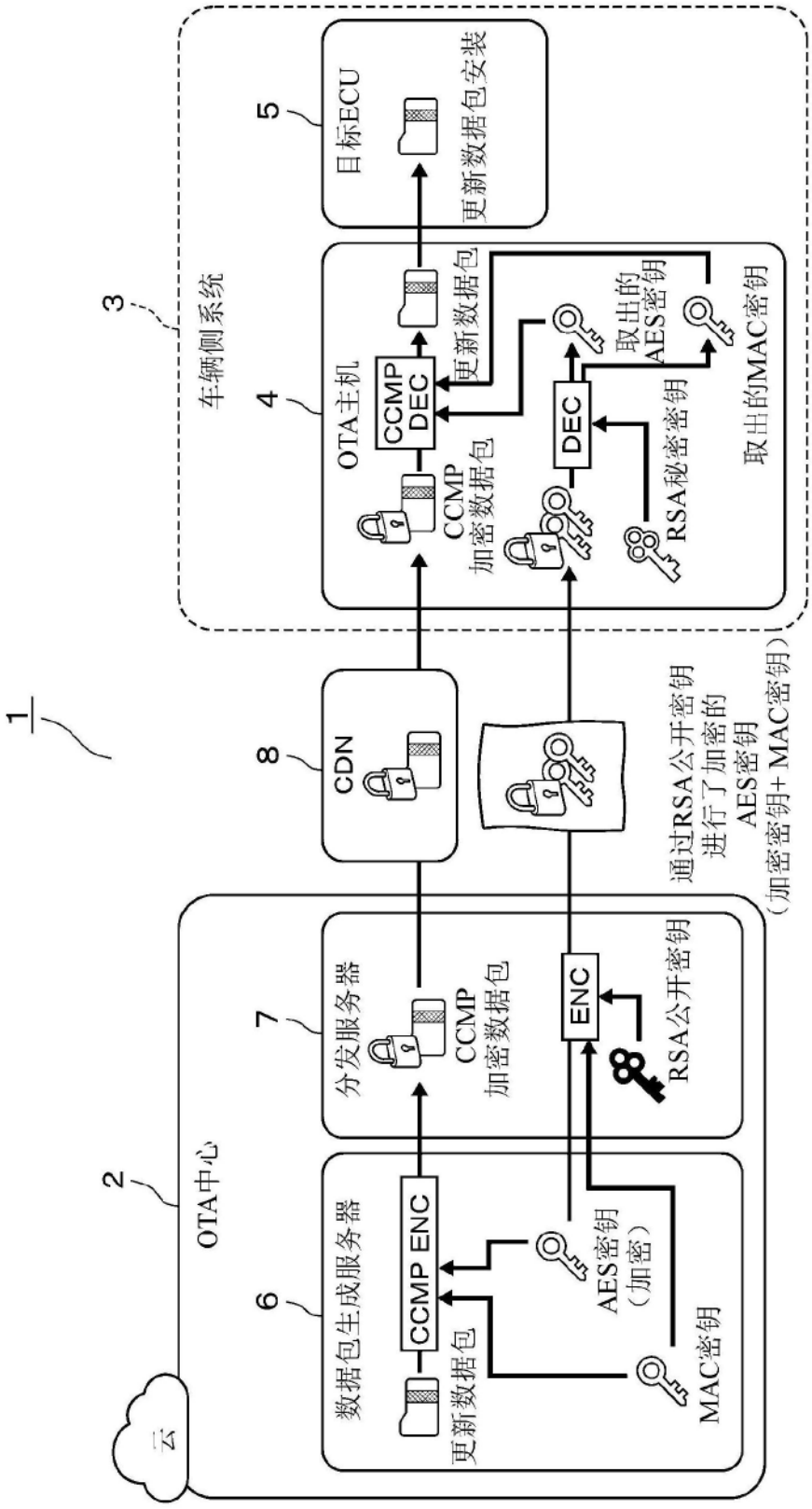

1
2
OTA中心
云
6
数据包生成服务器
CCMP ENC
更新数据包
AES密钥
（加密）
MAC密钥
7
分发服务器
CCMP
加密数据包
ENC
RSA公开密钥
8
CDN
通过RSA公开密钥
进行了加密的
AES密钥
（加密密钥+ MAC密钥）
3
车辆侧系统
4
OTA主机
CCMP
DEC
更新数据包
CCMP
加密数据包
DEC
取出的
AES密钥
RSA秘密密钥
取出的MAC密钥
5
目标ECU
更新数据包安装

图55

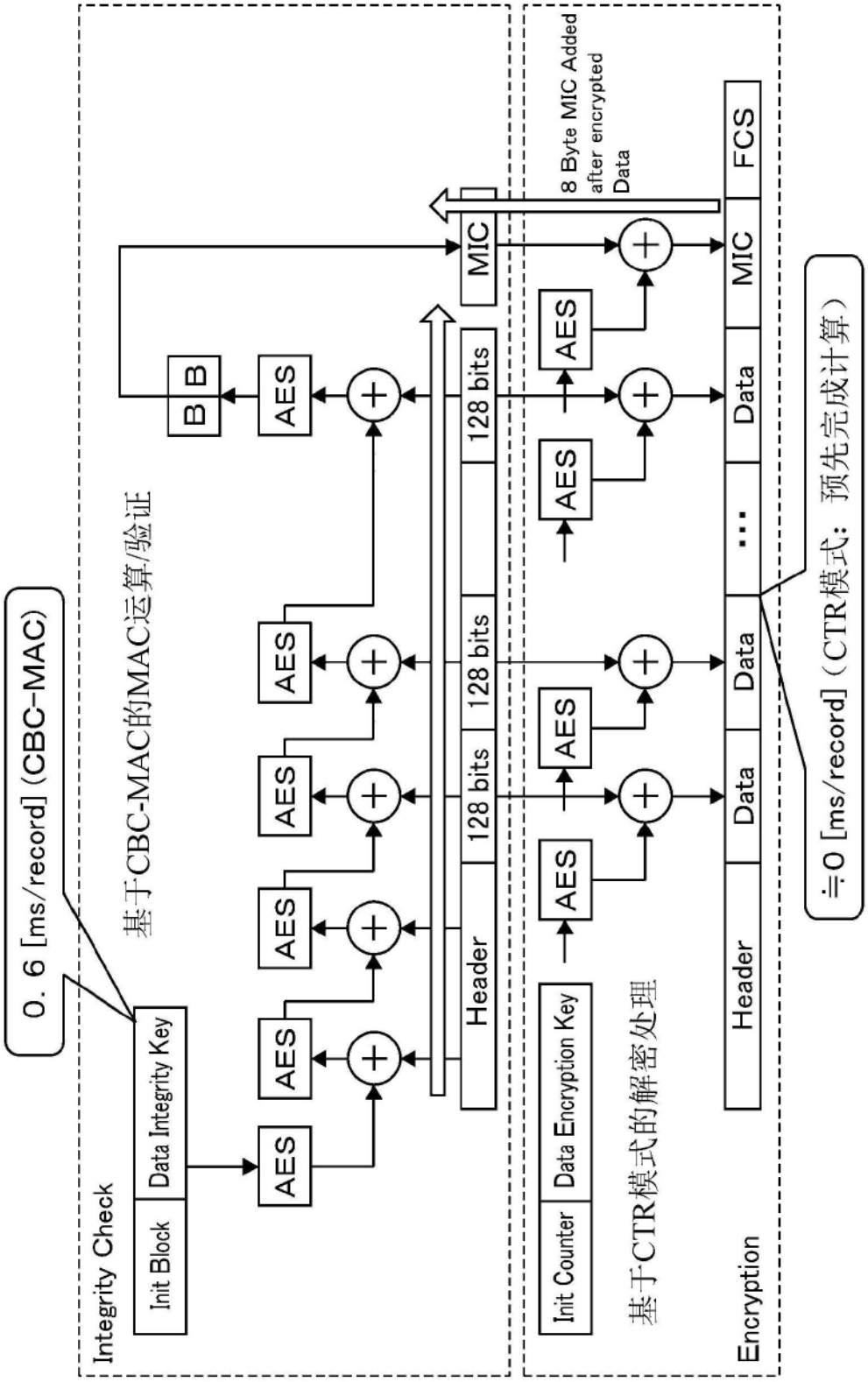

0. 6 [ms/record] (CBC-MAC)
基于CBC-MAC的MAC运算/验证
Integrity Check
Init Block
Data Integrity Key
AES
Header
128 bits
B B
MIC
8 Byte MIC Added after encrypted Data
Init Counter
Data Encryption Key
基于CTR模式的解密处理
Encryption
Data
FCS
÷0 [ms/record]（CTR模式：预先完成计算）

图56

基于CCMP模式的吞吐量的估计

由于AES解密为CTR模式，所以能够忽视（几十us量级）

	主核	HW硬件加速器
接收（解密+MAC运算处理）	613 [μs]	0. 6 [ms]（AES解密 ≒0ms + CBC-MAC 0. 6ms）

与主核相比较硬件加速器的处理时间占支配地位，所以根据其计算吞吐量：

数据量，以太网帧1518×11 = 16，698 [Byte]

的处理时间是 613[us] +0. 6[ms] = 1. 2 [ms]

吞吐量：15，796[Byte]

⇒ 数据吞吐量 ： 15，796 [B] × 8 [bit/B] ÷（1. 2/1000）[s] ≒ 105 [Mbps]

图57

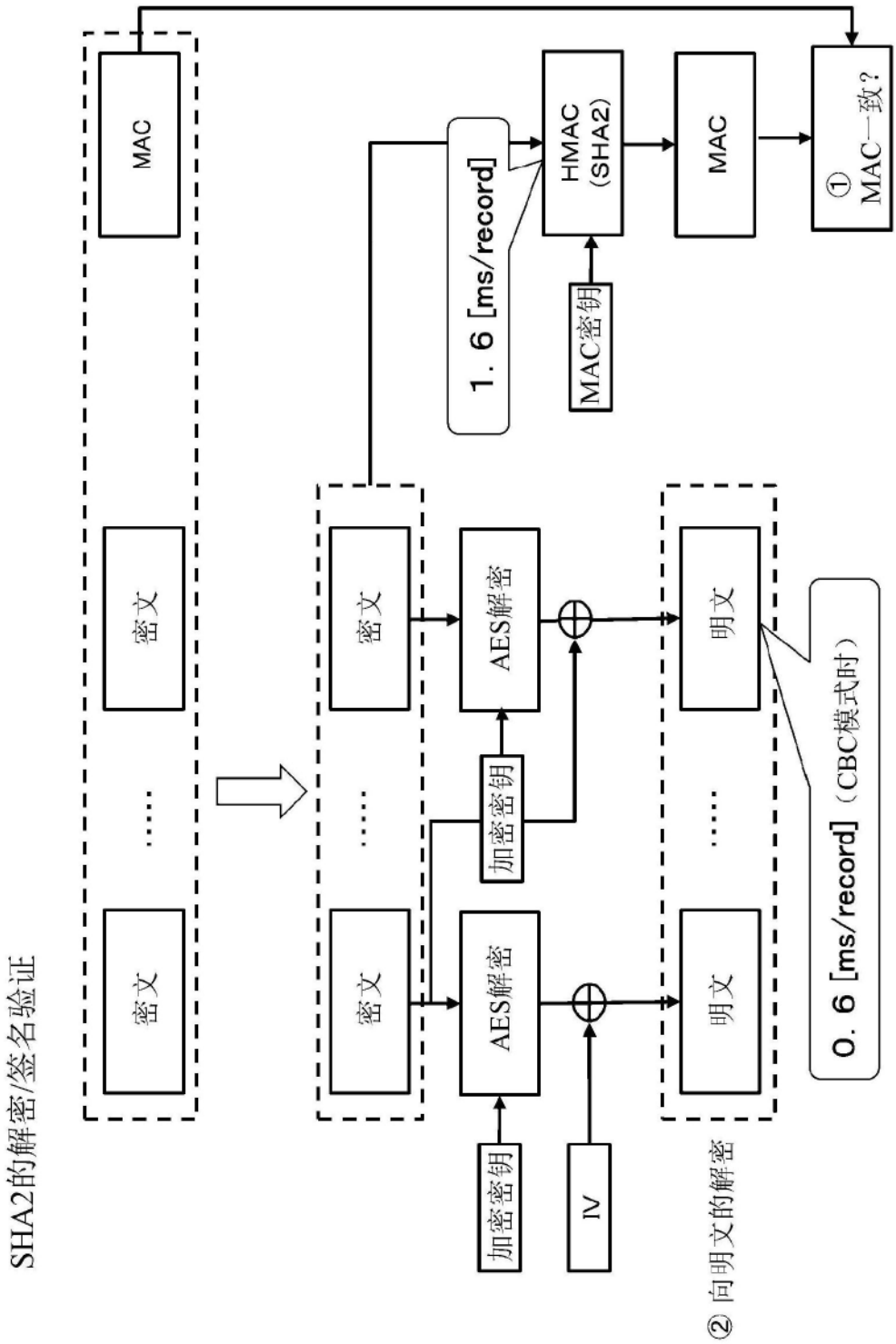

SHA2的解密/签名验证
MAC
密文
密文
密文
AES解密
AES解密
加密密钥
加密密钥
IV
明文
明文
明文
② 向明文的解密
0. 6 [ms/record]（CBC模式时）
1. 6 [ms/record]
HMAC (SHA2)
MAC密钥
MAC
① MAC一致?

图58

基于现有方式的吞吐量的估计

	主核	HW 硬件加速器
接收（解密+MAC运算处理）	613 [μs]	2. 2 [ms] （= AES解密 0. 6ms + HMAC 1. 6ms）

与主核相比较硬件加速器的处理时间占支配地位，所以根据其计算吞吐量

数据量:15，796[Byte]

以太网帧 1518×11 = 16，698 [Byte]

的处理时间是613[us]+2. 2[ms] = 2. 8 [ms]

⇒ 数据吞吐量 ： 15，796 [B] × 8 [bit/B] ÷ (2. 8/1000) [s] ≒ 45 [Mbps]

图59

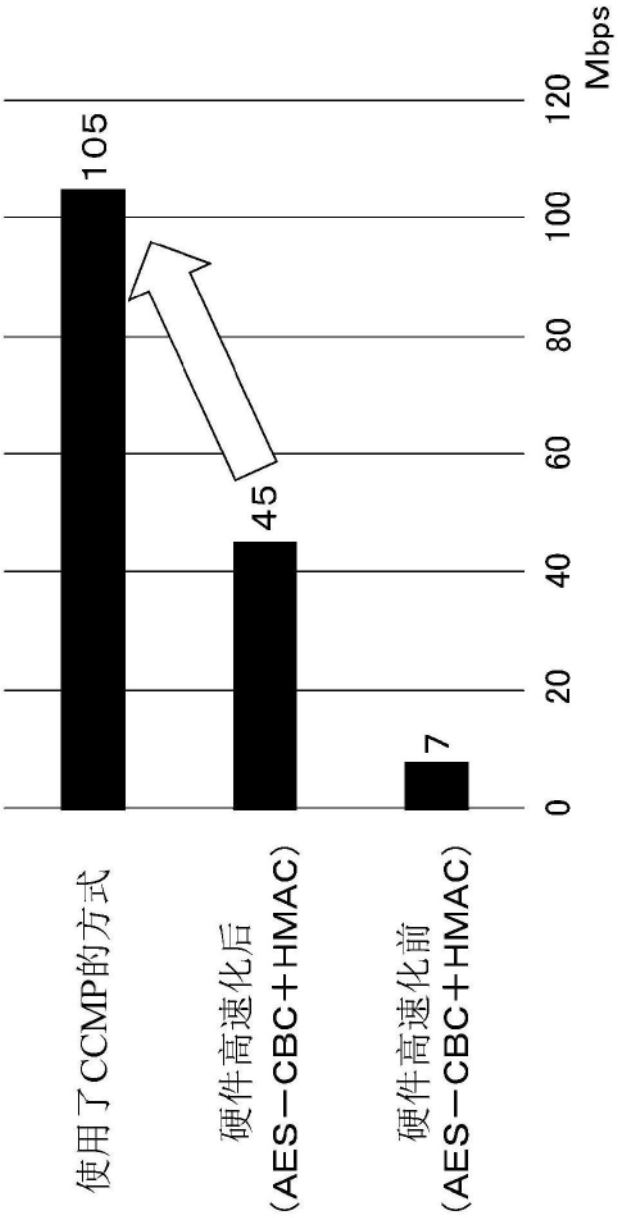

Mbps
120
100
80
60
40
20
0
105
45
7
使用了CCMP的方式
硬件高速化后
(AES－CBC＋HMAC)
硬件高速化前
(AES－CBC＋HMAC)

图60

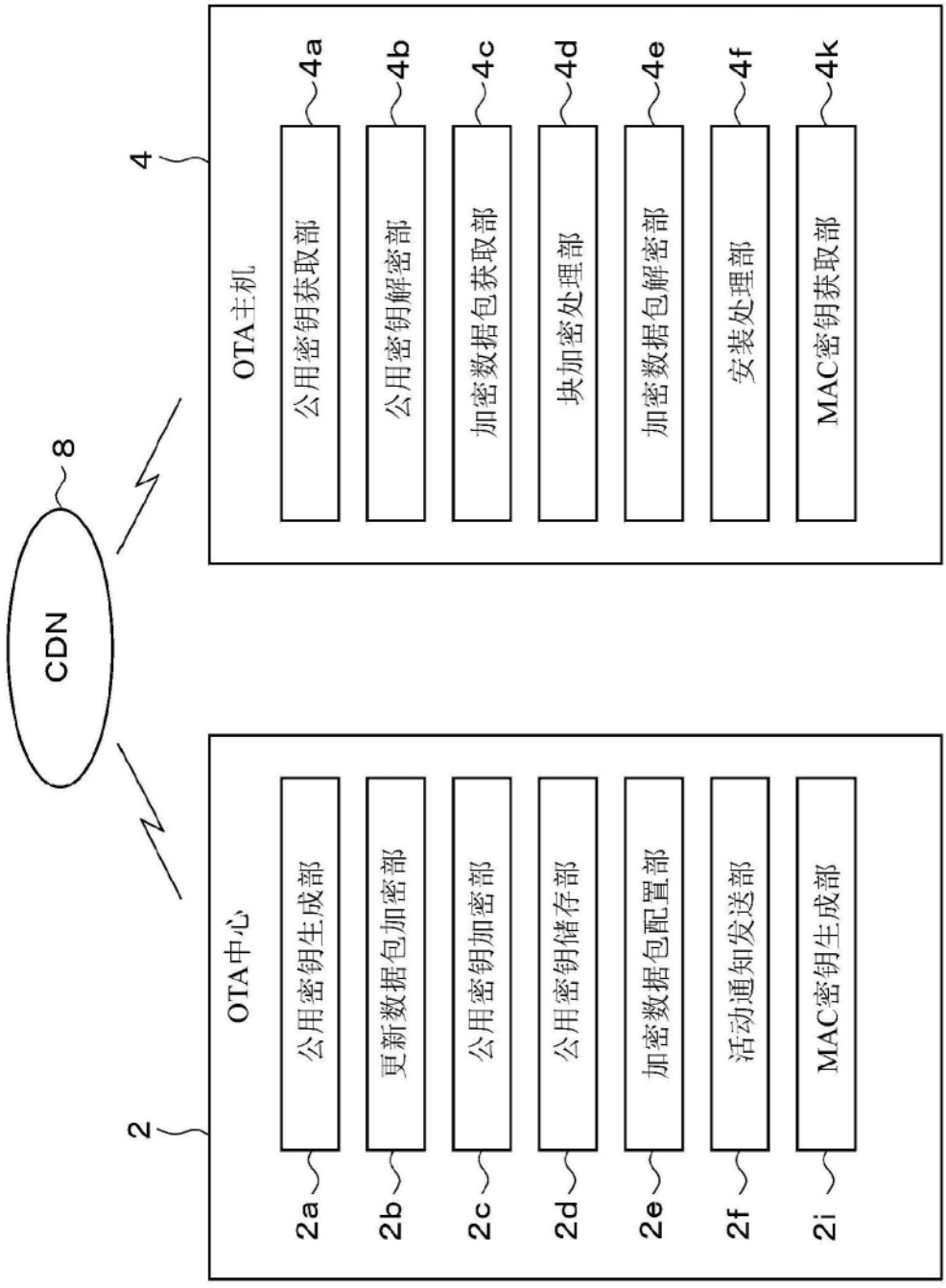

OTA中心
2
公用密钥生成部
2a
更新数据包加密部
2b
公用密钥加密部
2c
公用密钥储存部
2d
加密数据包配置部
2e
活动通知发送部
2f
MAC密钥生成部
2i
CDN
8
OTA主机
4
公用密钥获取部
4a
公用密钥解密部
4b
加密数据包获取部
4c
块加密处理部
4d
加密数据包解密部
4e
安装处理部
4f
MAC密钥获取部
4k

图61

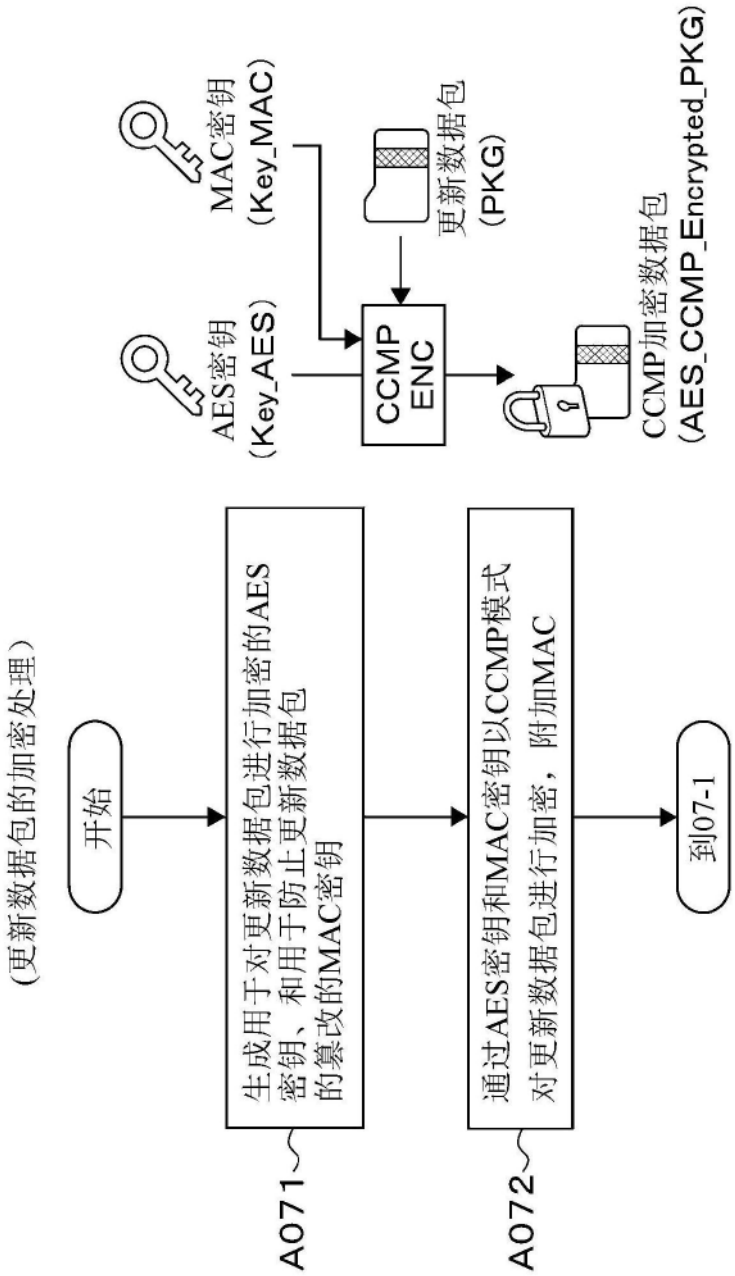

(更新数据包的加密处理)
开始
生成用于对更新数据包进行加密的AES密钥、和用于防止更新数据包的篡改的MAC密钥
A071
通过AES密钥和MAC密钥以CCMP模式对更新数据包进行加密，附加MAC
A072
到07-1
AES密钥 (Key_AES)
MAC密钥 (Key_MAC)
更新数据包 (PKG)
CCMP ENC
CCMP加密数据包 (AES_CCMP_Encrypted_PKG)

图62

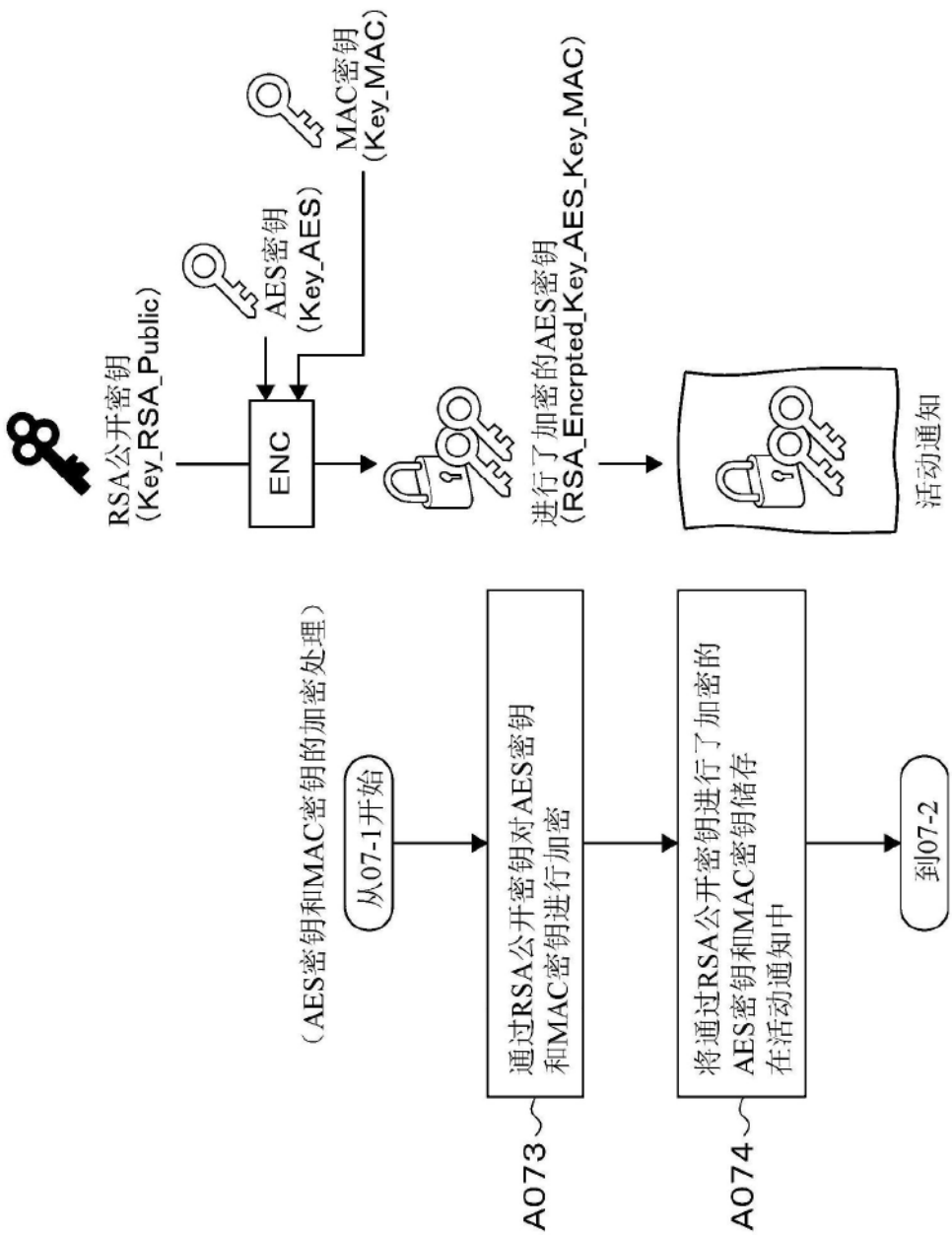

RSA公开密钥
(Key_RSA_Public)
AES密钥
(Key_AES)
MAC密钥
(Key_MAC)
ENC
进行了加密的AES密钥
(RSA_Encrpted_Key_AES_Key_MAC)
活动通知
（AES密钥和MAC密钥的加密处理）
从07-1开始
通过RSA公开密钥对AES密钥
和MAC密钥进行加密
将通过RSA公开密钥进行了加密的
AES密钥和MAC密钥储存
在活动通知中
到07-2
A073
A074

图63

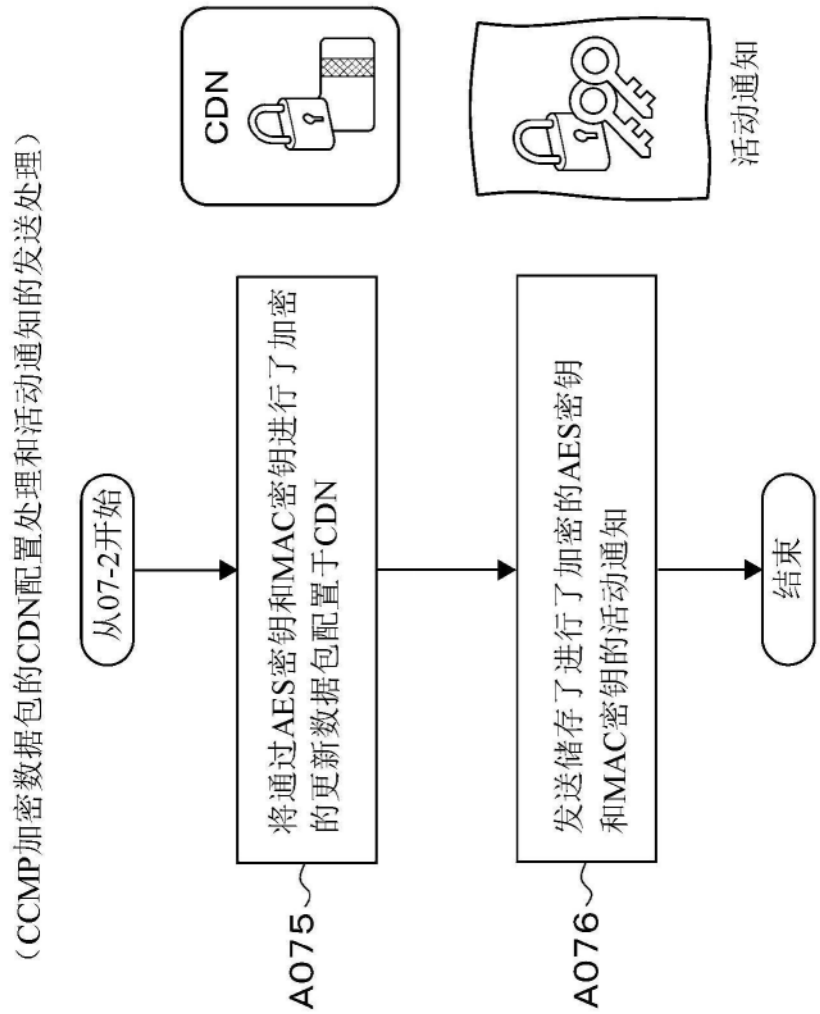

（CCMP加密数据包的CDN配置处理和活动通知的发送处理）
从07-2开始
将通过AES密钥和MAC密钥进行了加密的更新数据包配置于CDN
A075
发送储存了进行了加密的AES密钥和MAC密钥的活动通知
A076
结束
CDN
活动通知

图64

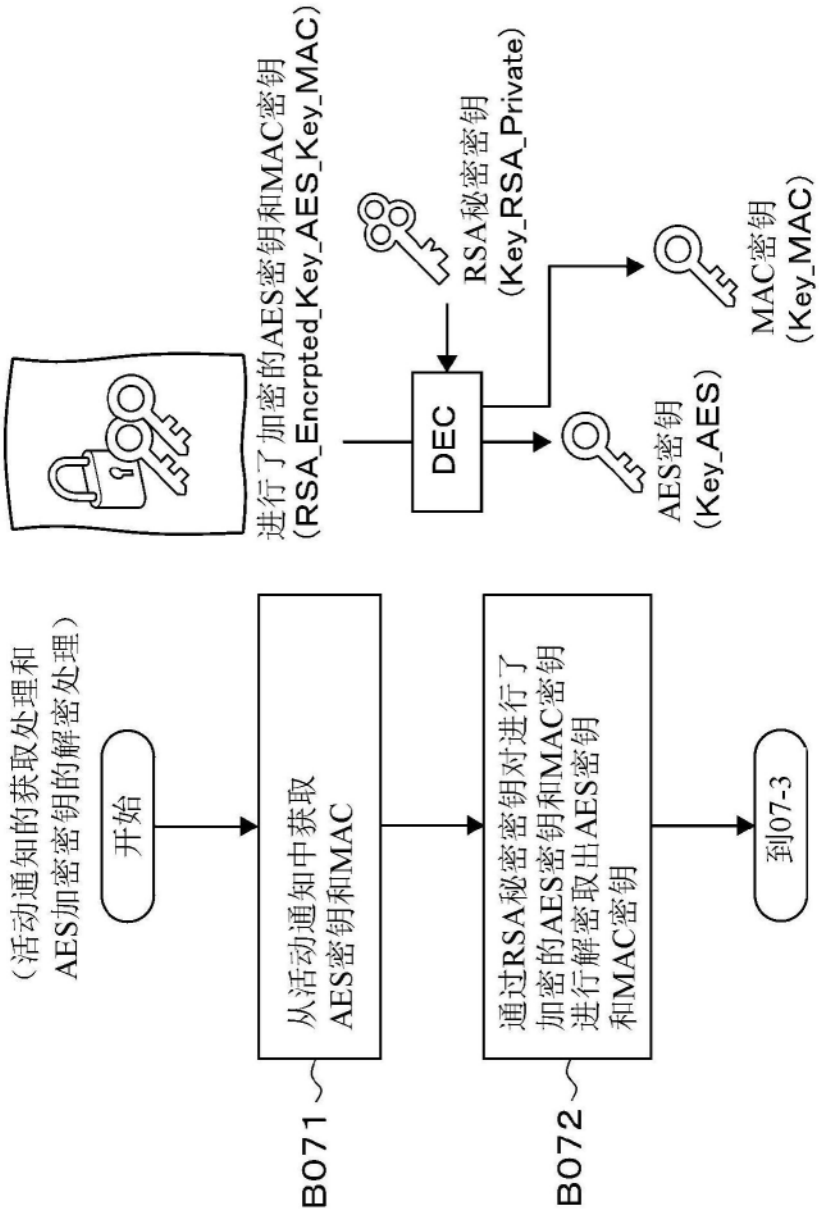

（活动通知的获取处理和
AES加密密钥的解密处理）
开始
从活动通知中获取
AES密钥和MAC
B071
通过RSA秘密密钥对进行了
加密的AES密钥和MAC密钥
进行解密取出AES密钥
和MAC密钥
B072
到07-3
进行了加密的AES密钥和MAC密钥
(RSA_Encrpted_Key_AES_Key_MAC)
DEC
RSA秘密密钥
(Key_RSA_Private)
AES密钥
(Key_AES)
MAC密钥
(Key_MAC)

图65

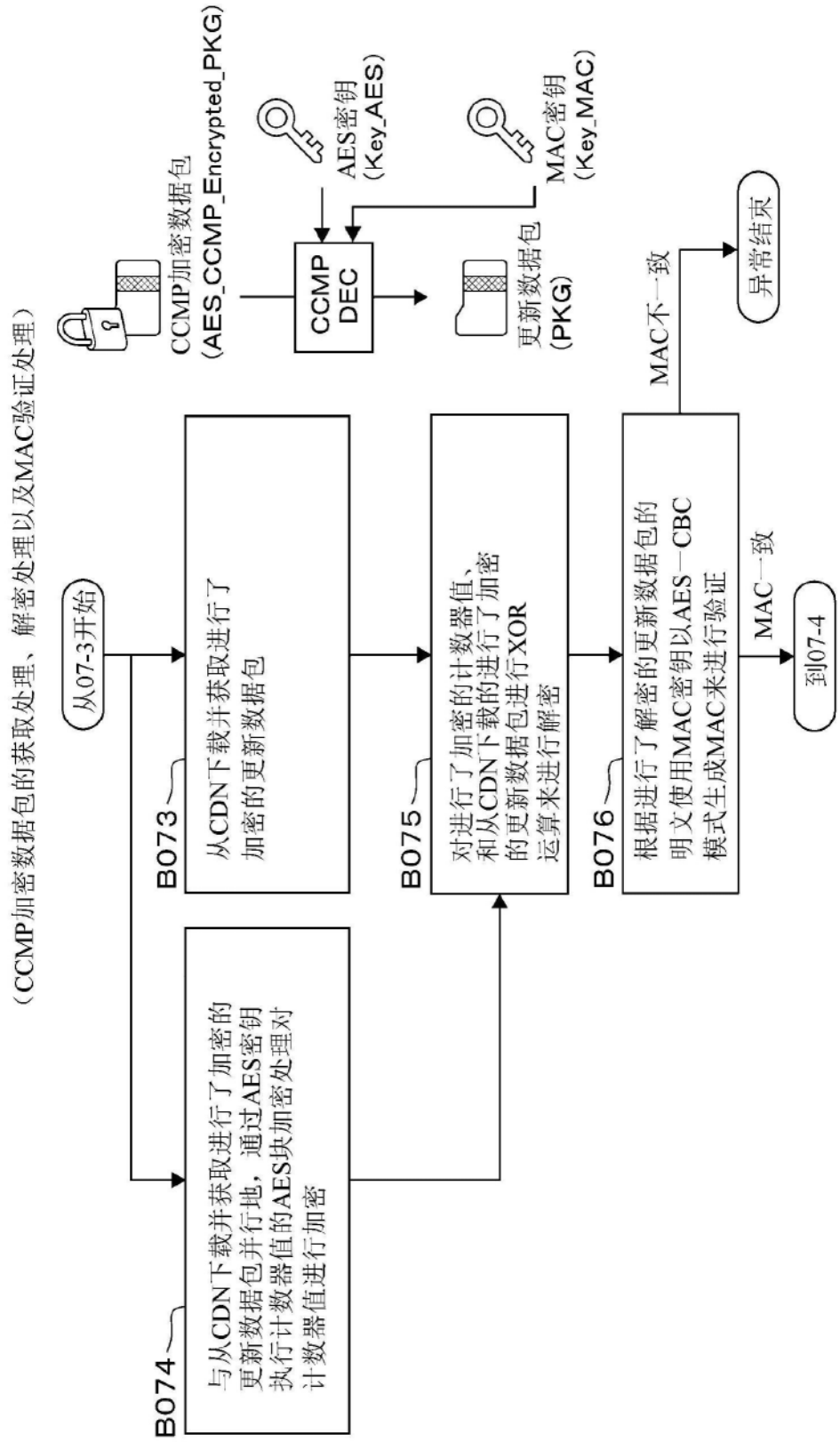

（CCMP加密数据包的获取处理、解密处理以及MAC验证处理）
从07-3开始
B073
从CDN下载并获取进行了加密的更新数据包
B074
与从CDN下载并获取进行了加密的更新数据包并行地，通过AES密钥执行计数器值的AES块加密处理对计数器值进行加密
B075
对进行了加密的计数器值、和从CDN下载的进行了加密的更新数据包进行XOR运算来进行解密
B076
根据进行了解密的更新数据包的明文使用MAC密钥以AES—CBC模式生成MAC来进行验证
CCMP加密数据包
(AES_CCMP_Encrypted_PKG)
AES密钥
(Key_AES)
MAC密钥
(Key_MAC)
CCMP
DEC
更新数据包
(PKG)
MAC不一致
异常结束
MAC一致
到07-4

图66

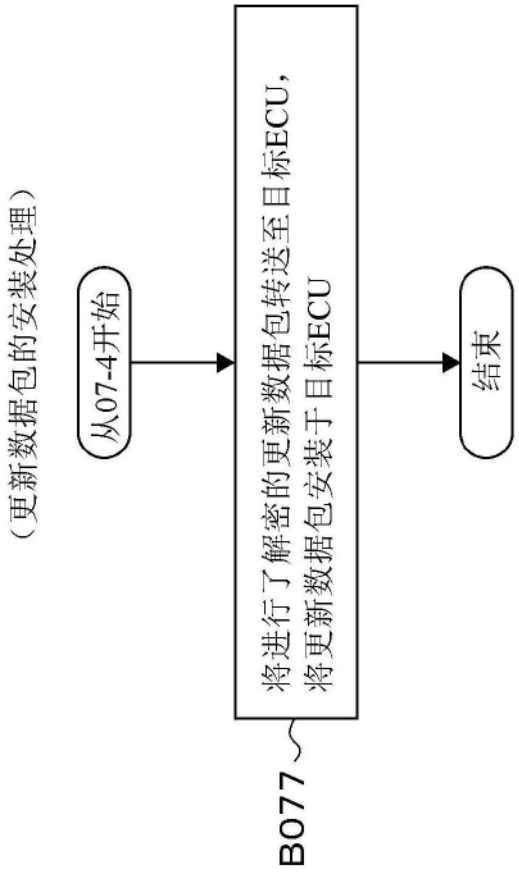

（更新数据包的安装处理）
从07-4开始
将进行了解密的更新数据包转送至目标ECU，
将更新数据包安装于目标ECU
结束
B077

图67

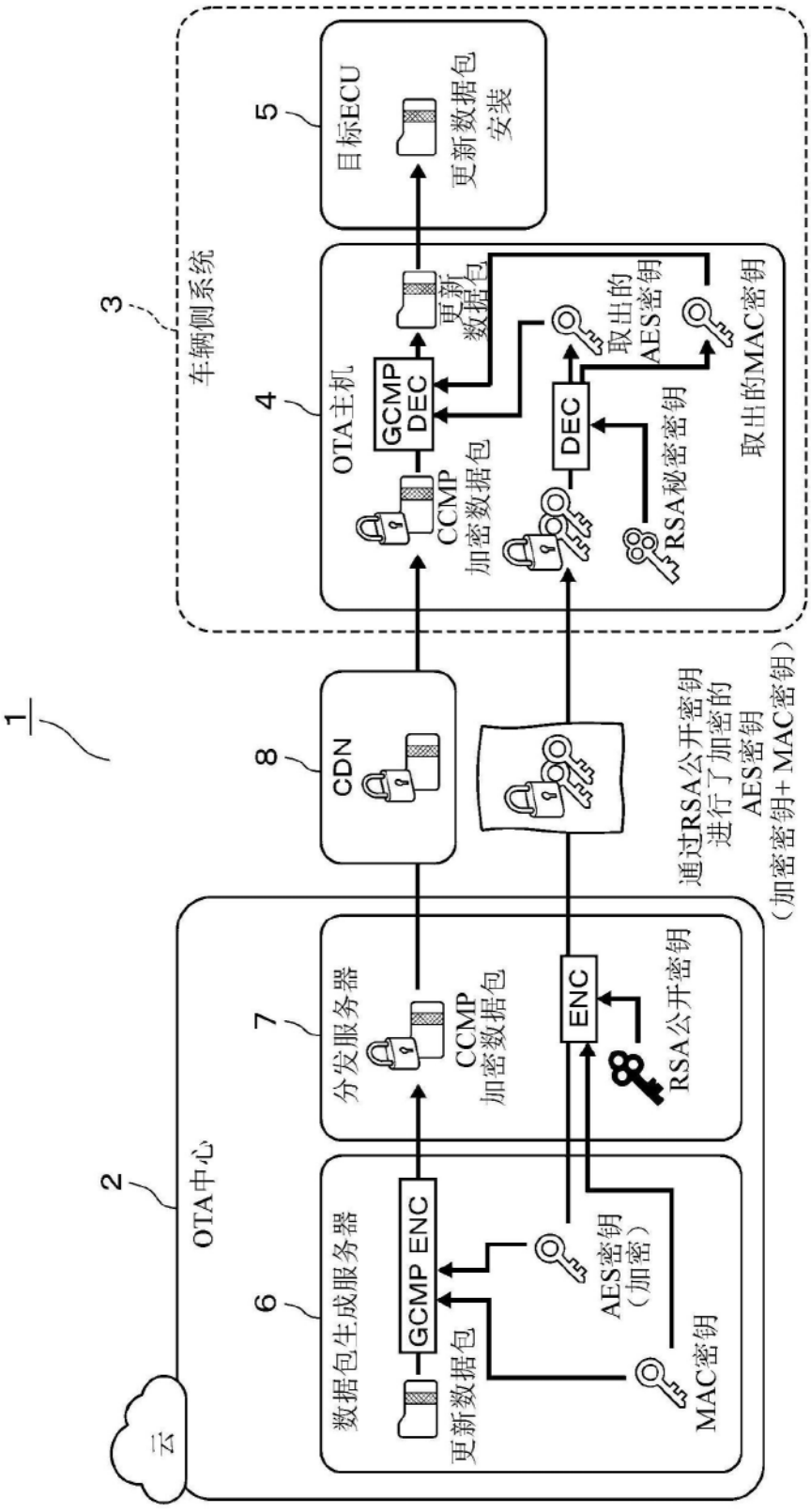

1
2
OTA中心
云
6
数据包生成服务器
更新数据包
GCMP ENC
MAC密钥
AES密钥
（加密）
7
分发服务器
CCMP
加密数据包
RSA公开密钥
ENC
8
CDN
通过RSA公开密钥
进行了加密的
AES密钥
（加密密钥+ MAC密钥）
3
车辆侧系统
4
OTA主机
CCMP
加密数据包
GCMP
DEC
更新
数据包
RSA秘密密钥
DEC
取出的
AES密钥
取出的MAC密钥
5
目标ECU
更新数据包
安装

图68

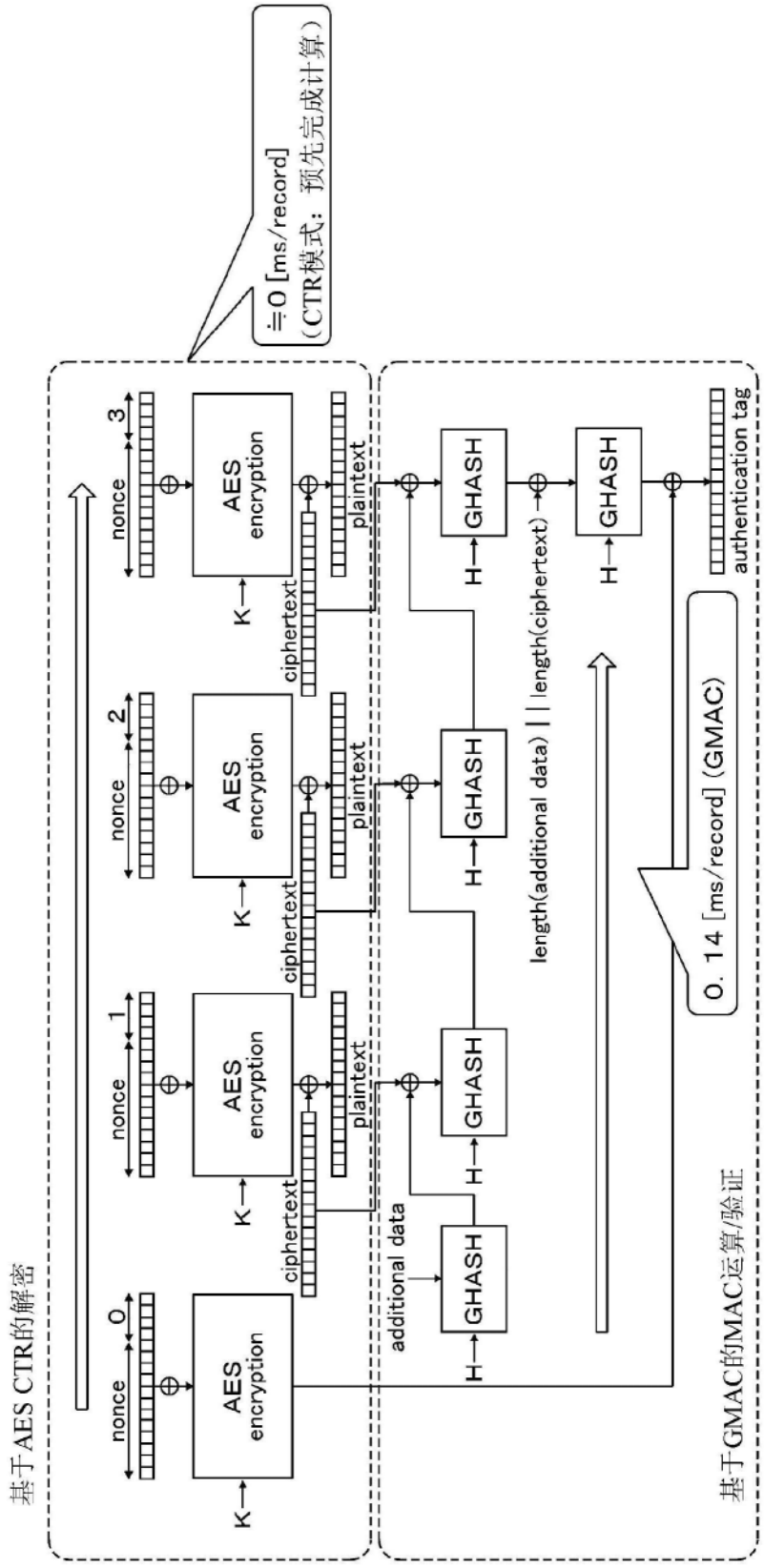

≒0 [ms/record]
(CTR模式：预先完成计算)
基于AES CTR的解密
基于GMAC的MAC运算/验证
nonce
AES encryption
K
plaintext
ciphertext
additional data
GHASH
H
length(additional data) | | length(ciphertext)
0. 14 [ms/record] (GMAC)
authentication tag

图69

基于GCMP模式的吞吐量的估计

由于AES解密为CTR模式，所以能够忽视（几十us量级）

	主核	硬件加速器
接收（解密+MAC运算处理）	613 [μs]	0. 6 [ms]（AES解密 ≒0ms + GMAC 0. 14ms）

与主核相比较硬件加速器的处理时间占支配地位，所以根据其计算吞吐量

数据量：15，796[Byte]

Ethernet以太网帧 1518×11 = 16，698 [Byte]

的处理时间是613[us] +0. 14[ms] = 0. 75 [ms]

⇒ 数据吞吐量 ： 15，796 [B] × 8 [bit/B] ÷ (0. 75/1000) [s] ≒ 170 [Mbps]

图70

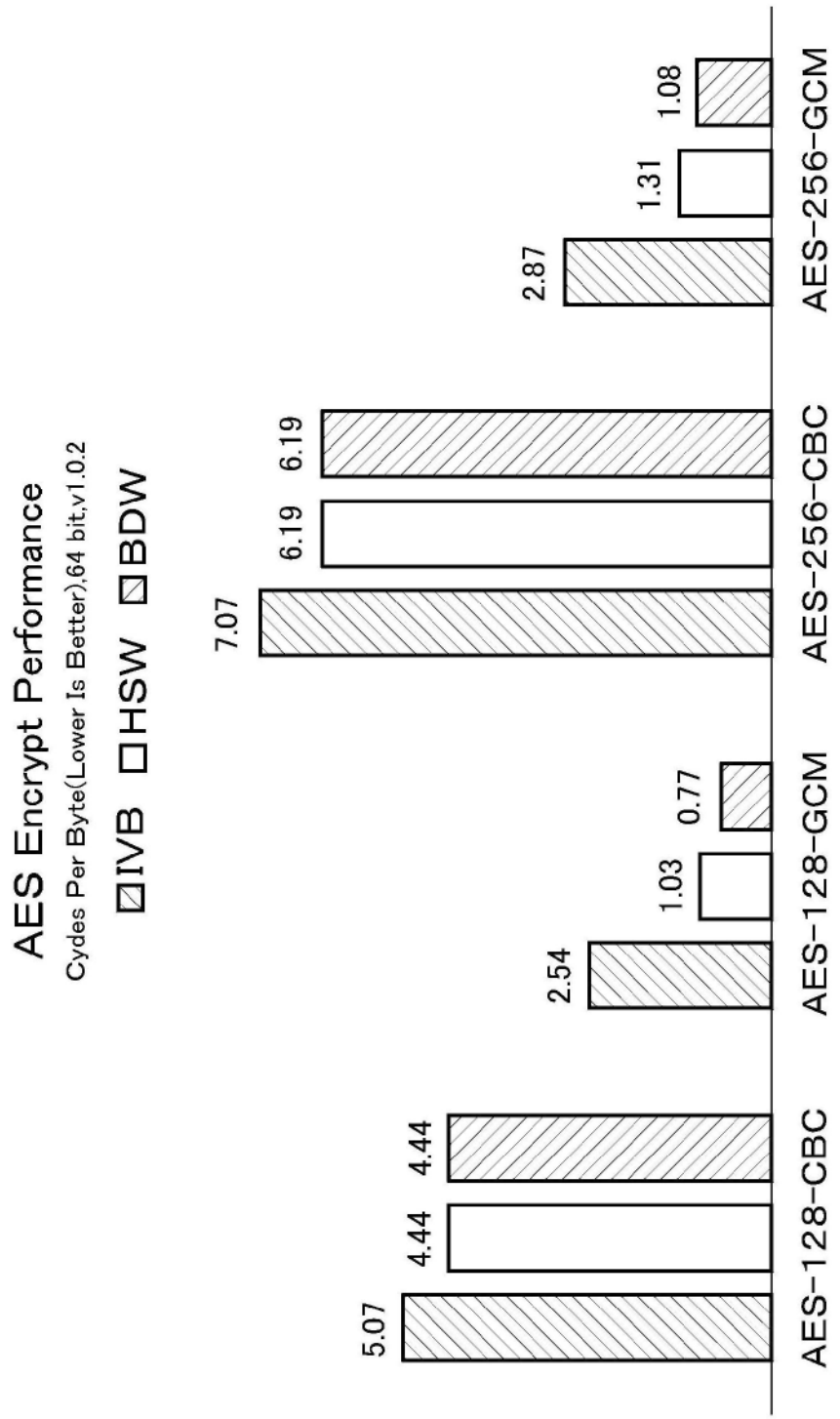

AES Encrypt Performance
Cydes Per Byte(Lower Is Better),64 bit,v1.0.2
IVB HSW BDW
5.07
4.44
4.44
2.54
1.03
0.77
7.07
6.19
6.19
2.87
1.31
1.08
AES-128-CBC
AES-128-GCM
AES-256-CBC
AES-256-GCM

图71

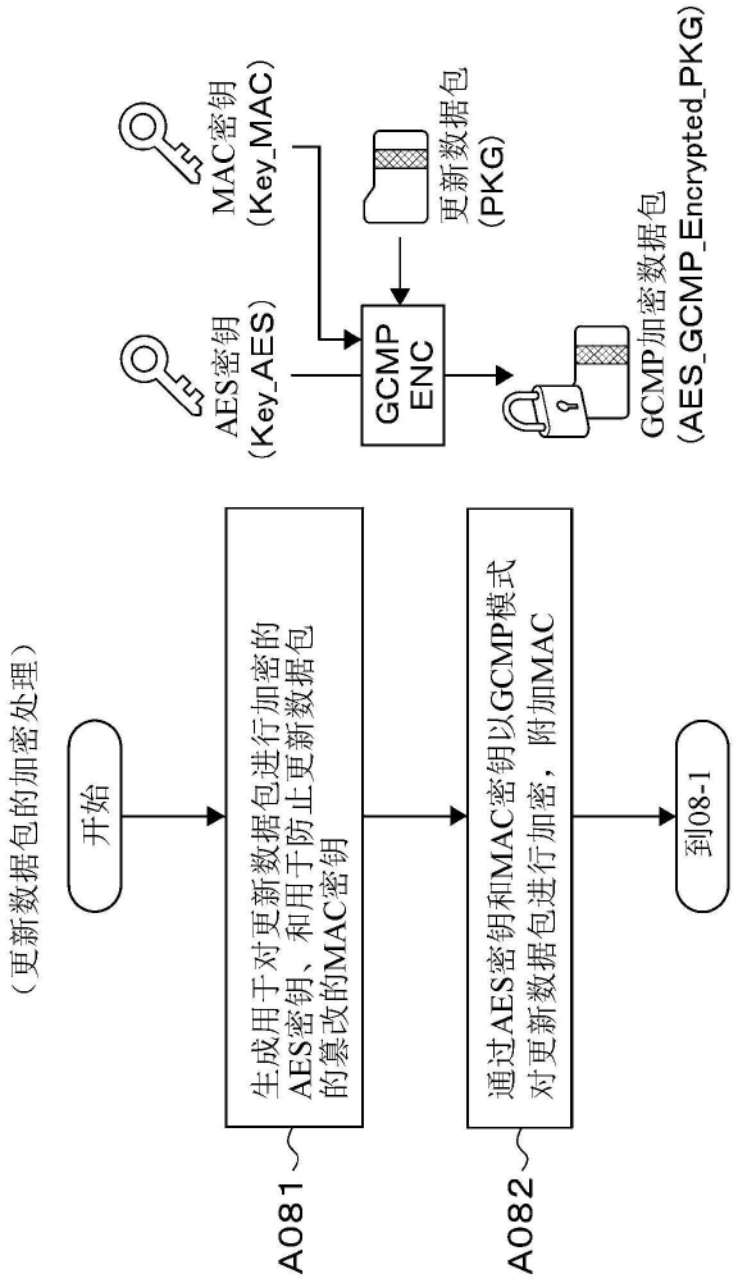

（更新数据包的加密处理）
开始
生成用于对更新数据包进行加密的AES密钥、和用于防止更新数据包的篡改的MAC密钥
A081
通过AES密钥和MAC密钥以GCMP模式对更新数据包进行加密，附加MAC
A082
到08-1
AES密钥 (Key_AES)
MAC密钥 (Key_MAC)
更新数据包 (PKG)
GCMP ENC
GCMP加密数据包 (AES_GCMP_Encrypted_PKG)

图72

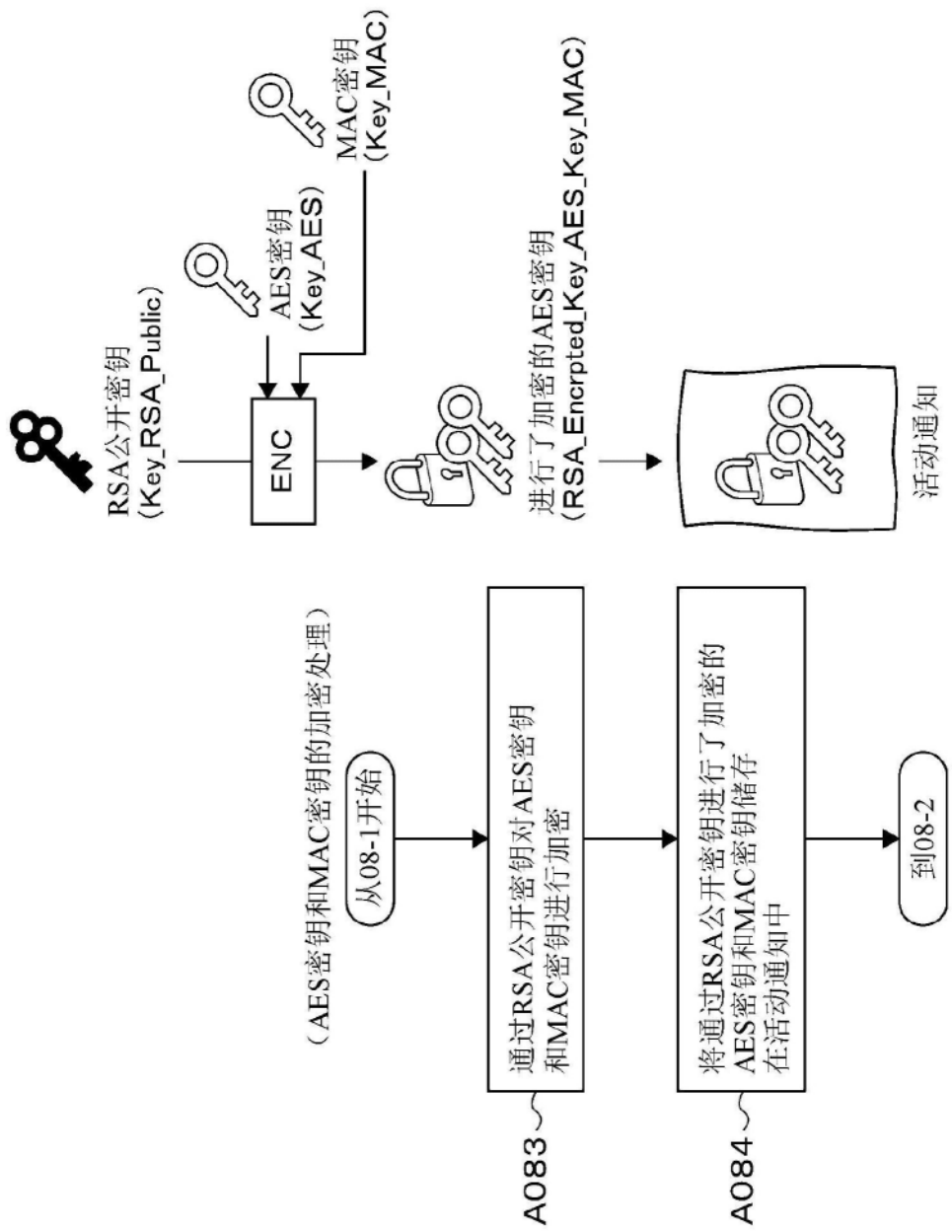

RSA公开密钥
(Key_RSA_Public)
AES密钥
(Key_AES)
MAC密钥
(Key_MAC)
ENC
进行了加密的AES密钥
(RSA_Encrpted_Key_AES_Key_MAC)
活动通知
（AES密钥和MAC密钥的加密处理）
从08-1开始
通过RSA公开密钥对AES密钥
和MAC密钥进行加密
将通过RSA公开密钥进行了加密的
AES密钥和MAC密钥储存
在活动通知中
到08-2
A083
A084

图73

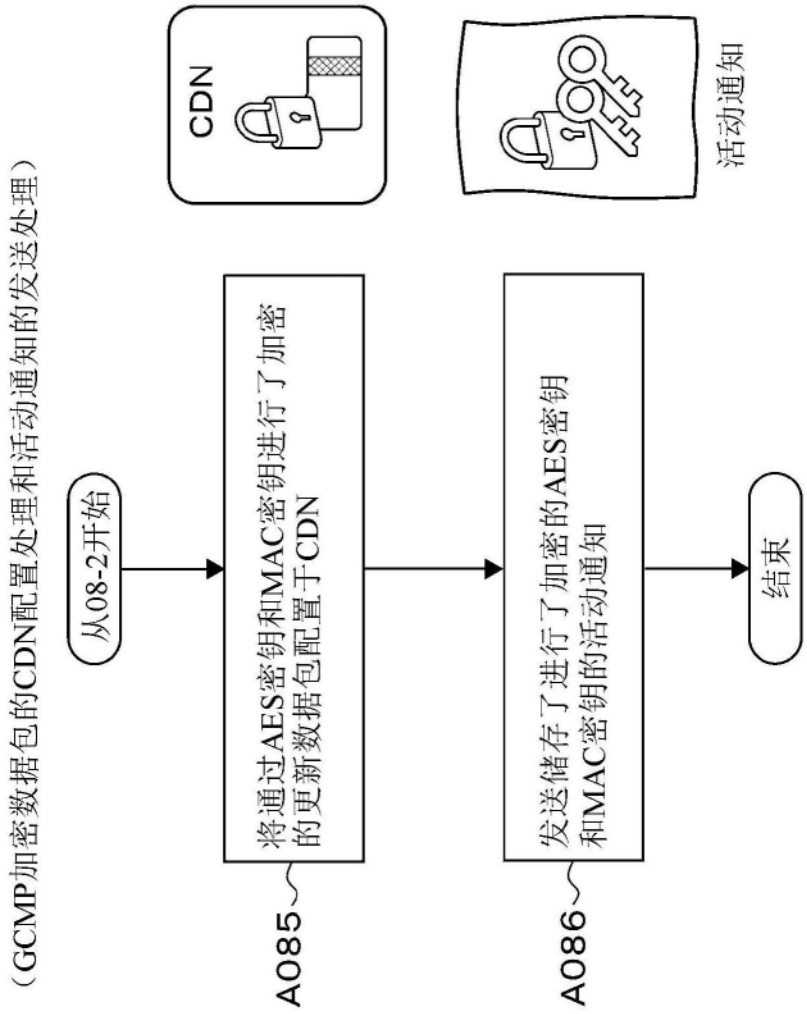

（GCMP加密数据包的CDN配置处理和活动通知的发送处理）
从08-2开始
将通过AES密钥和MAC密钥进行了加密的更新数据包配置于CDN
A085
发送储存了进行了加密的AES密钥和MAC密钥的活动通知
A086
结束
CDN
活动通知

图74

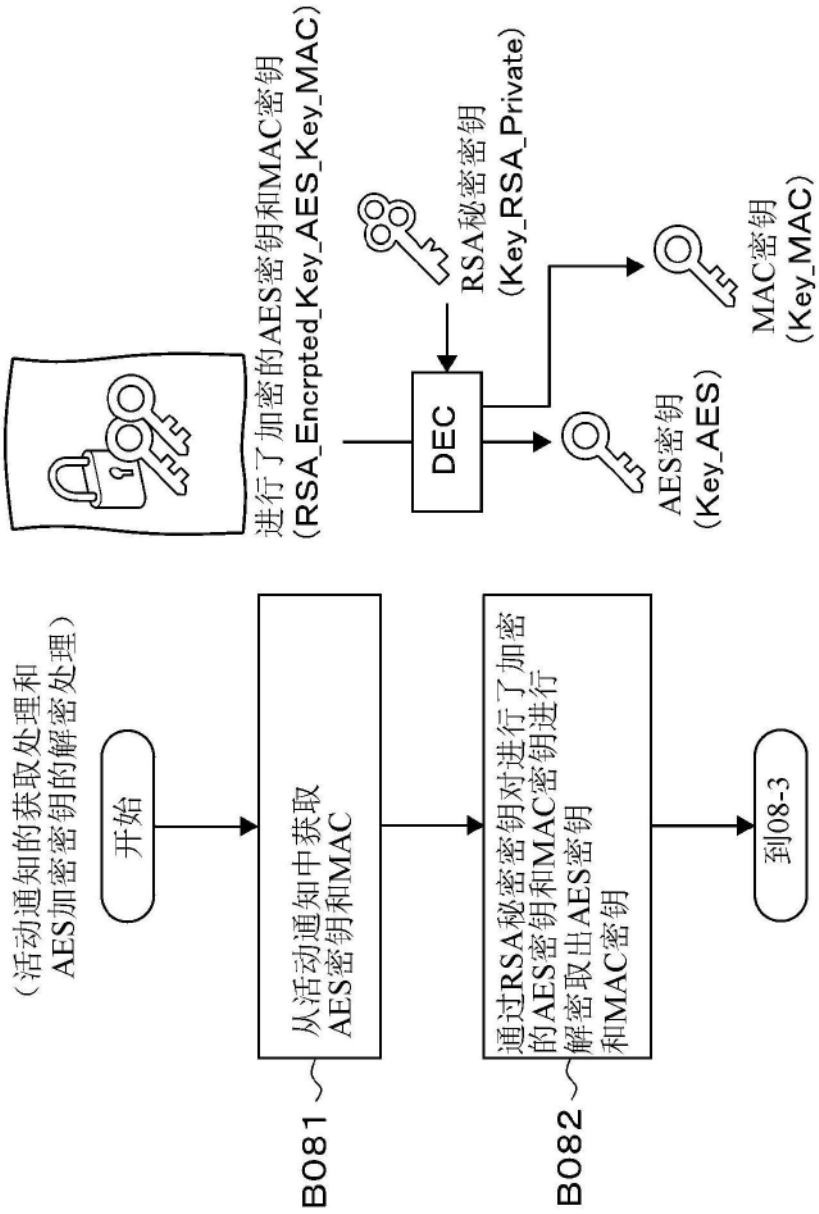

（活动通知的获取处理和
AES加密密钥的解密处理）
开始
从活动通知中获取
AES密钥和MAC
B081
通过RSA秘密密钥对进行了加密
的AES密钥和MAC密钥进行
解密取出AES密钥
和MAC密钥
B082
到08-3
进行了加密的AES密钥和MAC密钥
(RSA_Encrpted_Key_AES_Key_MAC)
DEC
RSA秘密密钥
(Key_RSA_Private)
AES密钥
(Key_AES)
MAC密钥
(Key_MAC)

图75

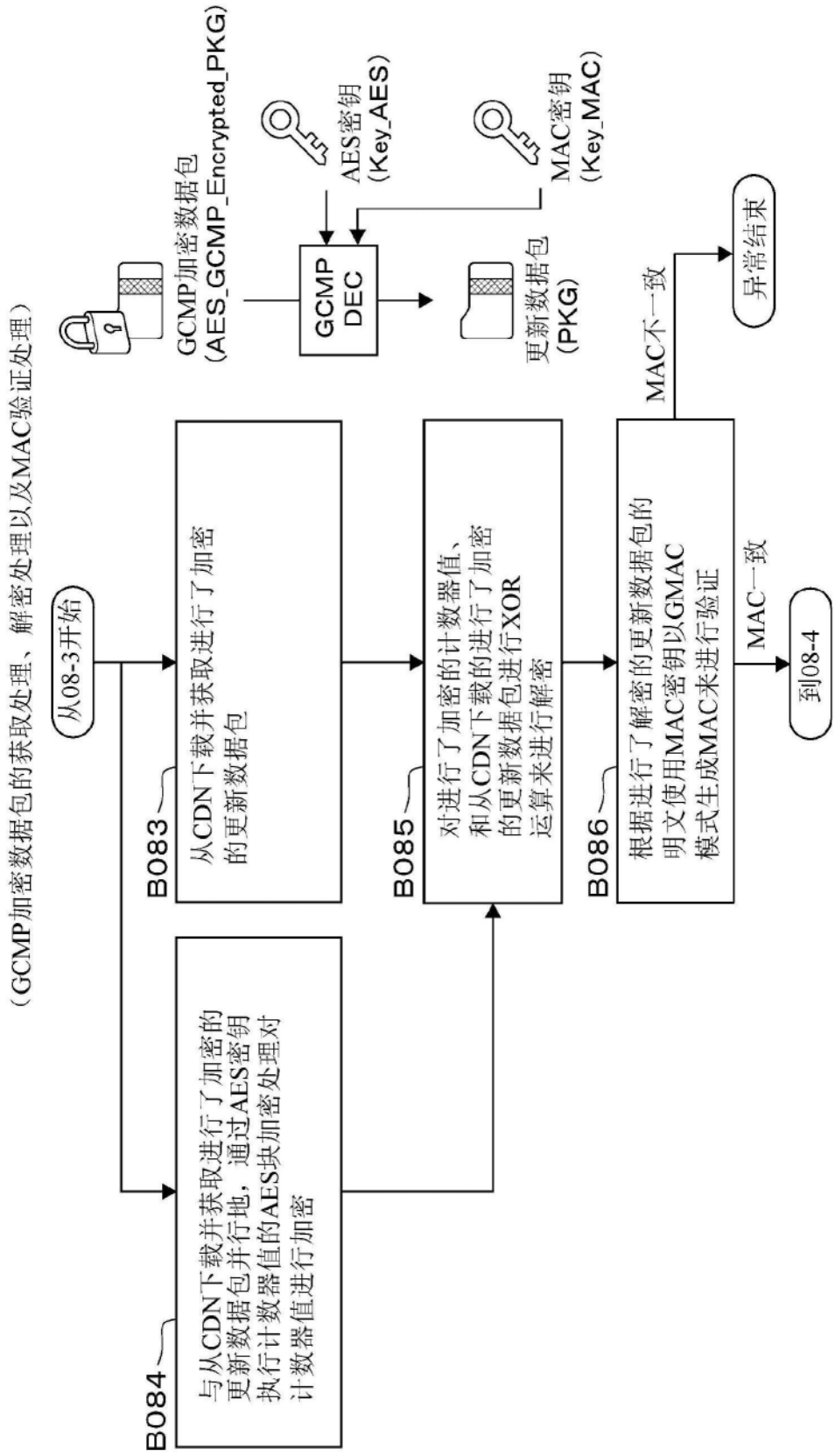

（GCMP加密数据包的获取处理、解密处理以及MAC验证处理）
从08-3开始
B083
从CDN下载并获取进行了加密的更新数据包
B084
与从CDN下载并获取进行了加密的更新数据包并行地，通过AES密钥执行计数器值的AES块加密处理对计数器值进行加密
B085
对进行了加密的计数器值、和从CDN下载的进行了加密的更新数据包进行XOR运算来进行解密
B086
根据进行了解密的更新数据包的明文使用MAC密钥以GMAC模式生成MAC来进行验证
MAC一致
到08-4
MAC不一致
异常结束
GCMP加密数据包
(AES_GCMP_Encrypted_PKG)
GCMP DEC
AES密钥
(Key_AES)
MAC密钥
(Key_MAC)
更新数据包
(PKG)

图76

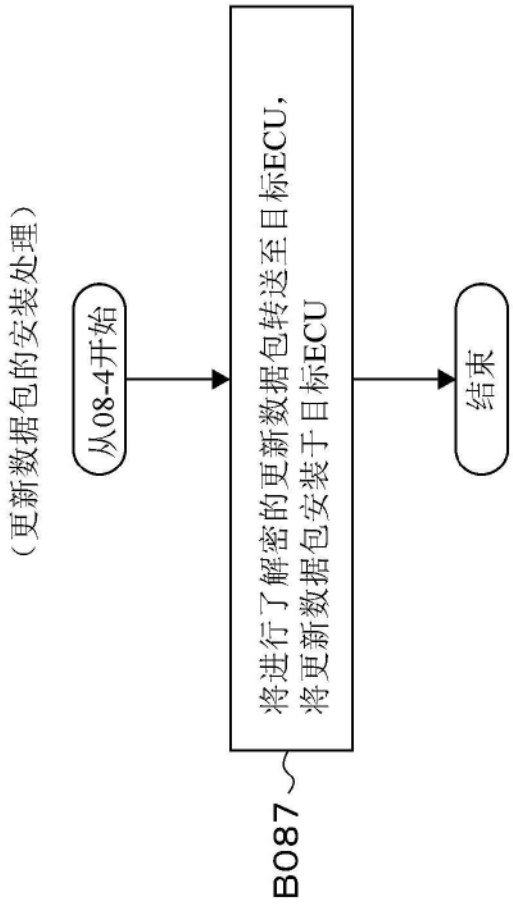

（更新数据包的安装处理）
从08-4开始
将进行了解密的更新数据包转送至目标ECU，
将更新数据包安装于目标ECU
结束
B087

图77

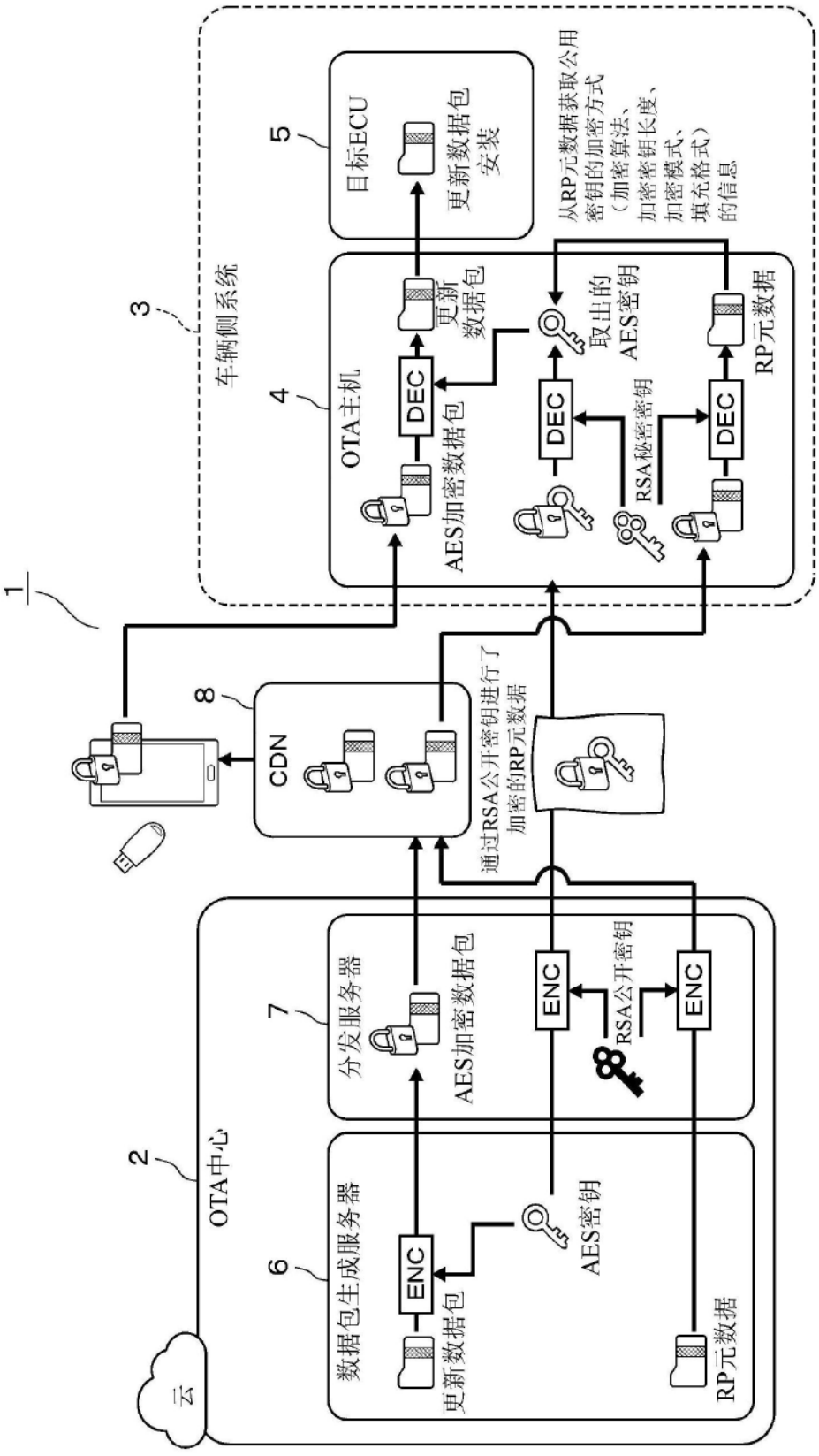

1
2
OTA中心
云
6
数据包生成服务器
更新数据包
ENC
AES密钥
RP元数据
7
分发服务器
AES加密数据包
ENC
RSA公开密钥
ENC
8
CDN
通过RSA公开密钥进行了加密的RP元数据
3
车辆侧系统
4
OTA主机
AES加密数据包
DEC
更新数据包
DEC
RSA秘密密钥
DEC
取出的AES密钥
RP元数据
从RP元数据获取公用密钥的加密方式（加密算法、加密密钥长度、加密模式、填充格式）的信息
5
目标ECU
更新数据包安装

图78

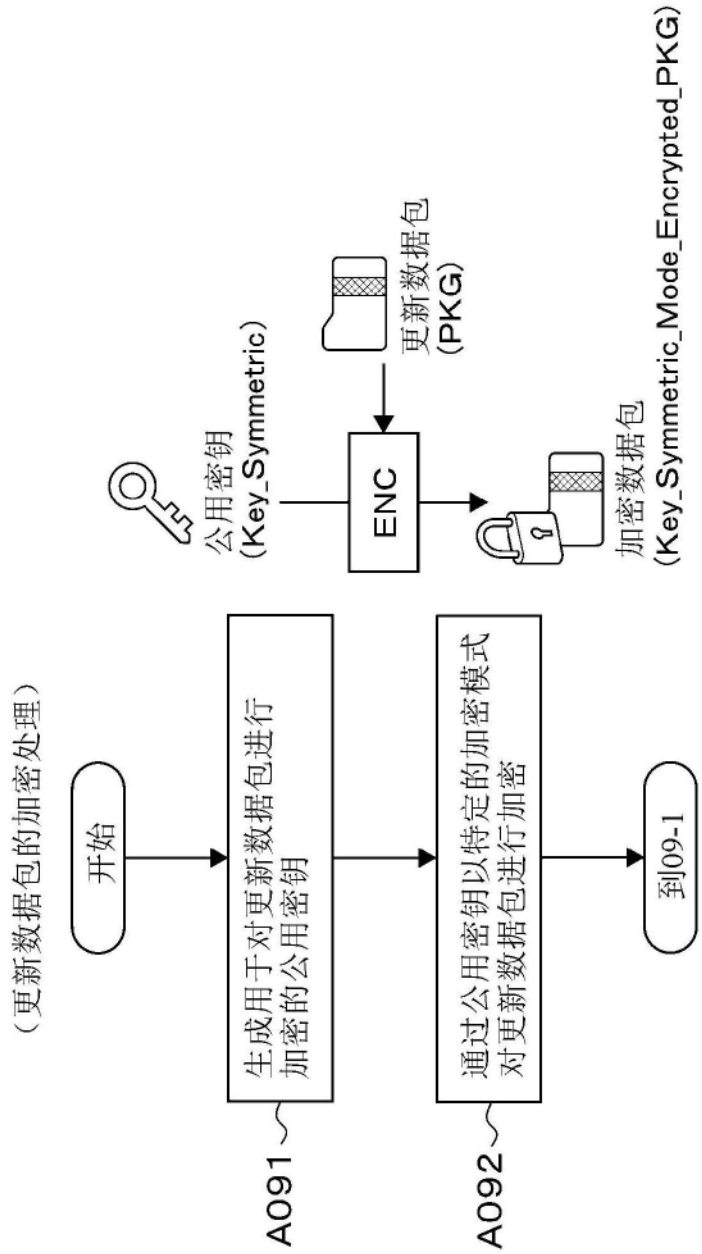

（更新数据包的加密处理）
开始
生成用于对更新数据包进行加密的公用密钥
A091
通过公用密钥以特定的加密模式对更新数据包进行加密
A092
到09-1
公用密钥
(Key_Symmetric)
ENC
更新数据包
(PKG)
加密数据包
(Key_Symmetric_Mode_Encrypted_PKG)

图79

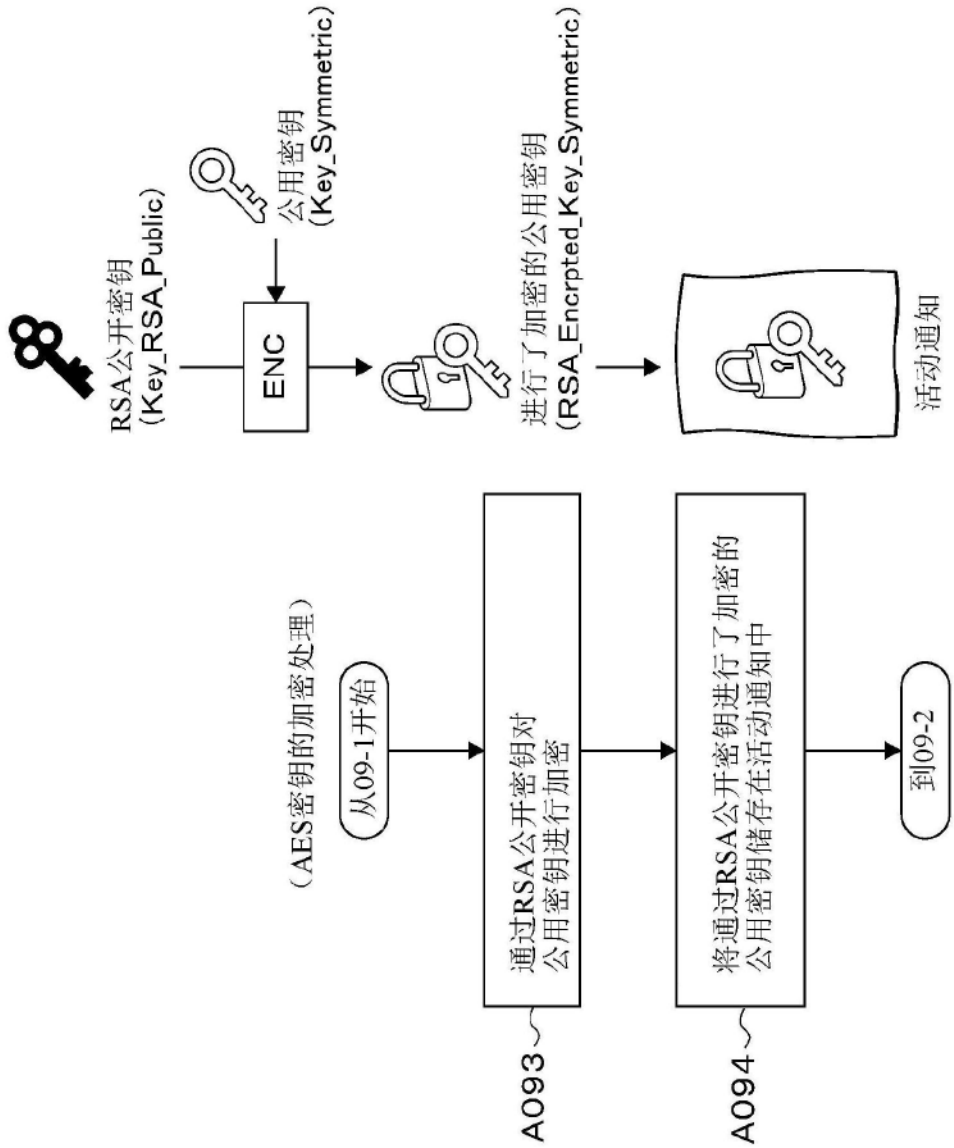

RSA公开密钥
(Key_RSA_Public)
公用密钥
(Key_Symmetric)
ENC
进行了加密的公用密钥
(RSA_Encrpted_Key_Symmetric)
活动通知
（AES密钥的加密处理）
从09-1开始
通过RSA公开密钥对
公用密钥进行加密
将通过RSA公开密钥进行了加密的
公用密钥储存在活动通知中
到09-2
A093
A094

图80

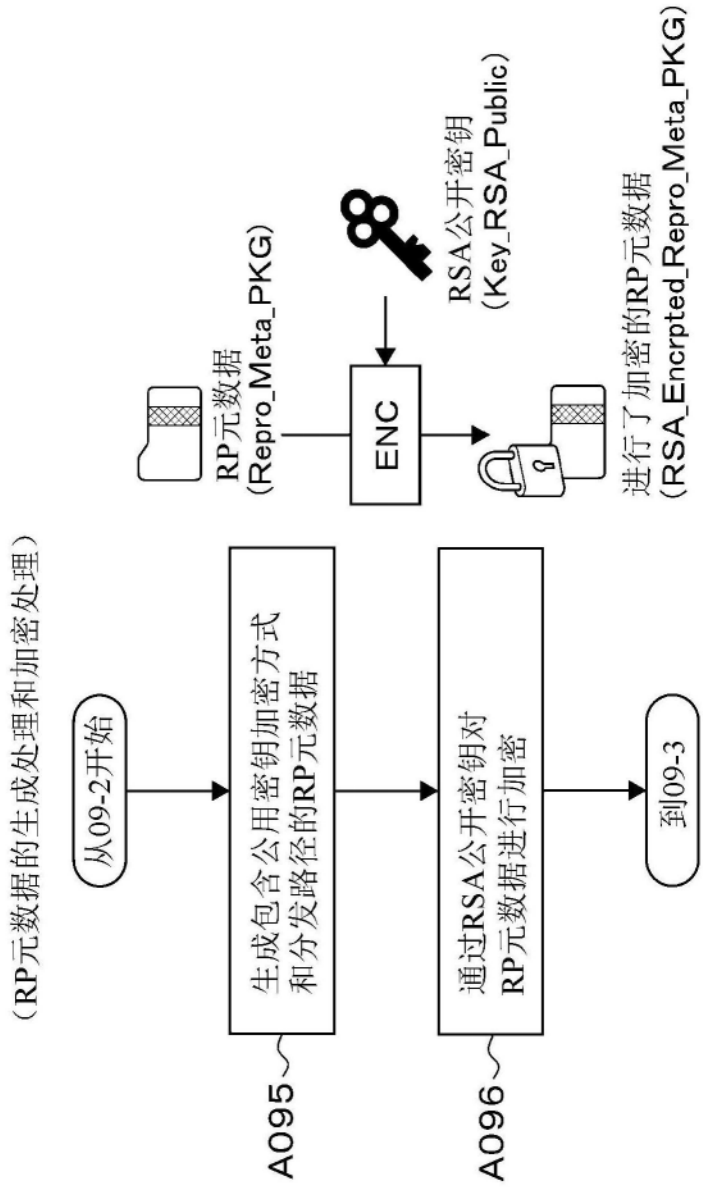

（RP元数据的生成处理和加密处理）
从09-2开始
生成包含公用密钥加密方式
和分发路径的RP元数据
A095
通过RSA公开密钥对
RP元数据进行加密
A096
到09-3
RP元数据
(Repro_Meta_PKG)
ENC
RSA公开密钥
(Key_RSA_Public)
进行了加密的RP元数据
(RSA_Encrpted_Repro_Meta_PKG)

图81

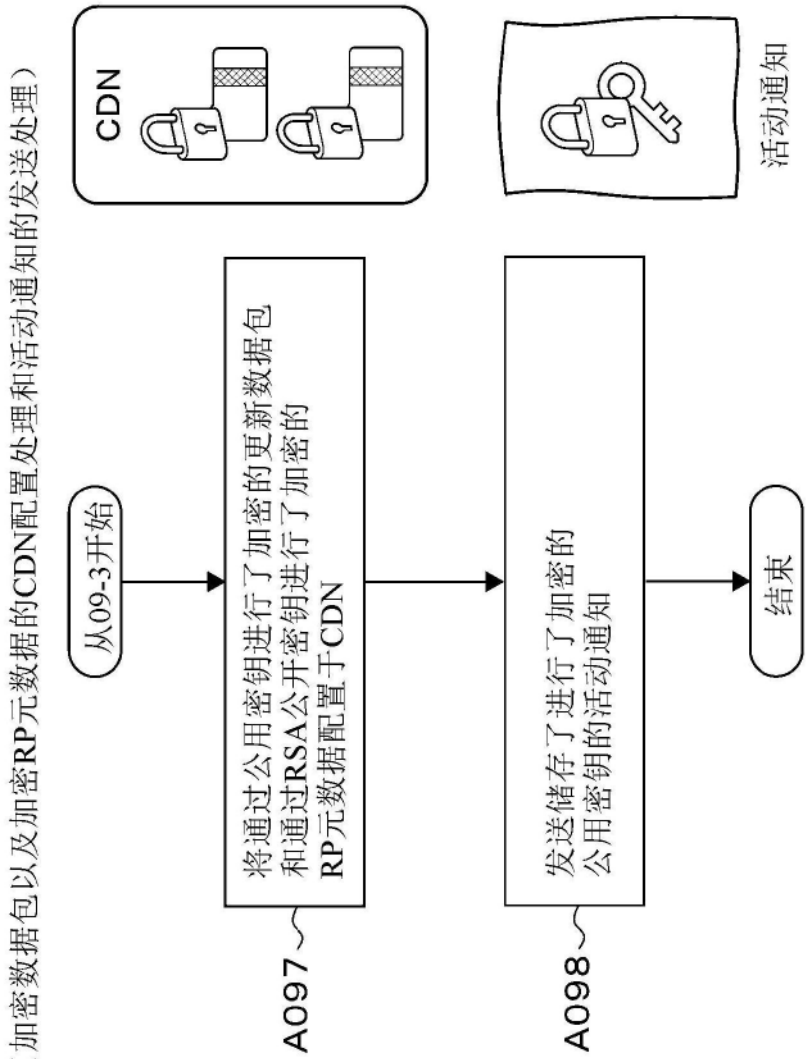

（加密数据包以及加密RP元数据的CDN配置处理和活动通知的发送处理）
从09-3开始
将通过公用密钥进行了加密的更新数据包和通过RSA公开密钥进行了加密的RP元数据配置于CDN
A097
发送储存了进行了加密的公用密钥的活动通知
A098
结束
CDN
活动通知

图82

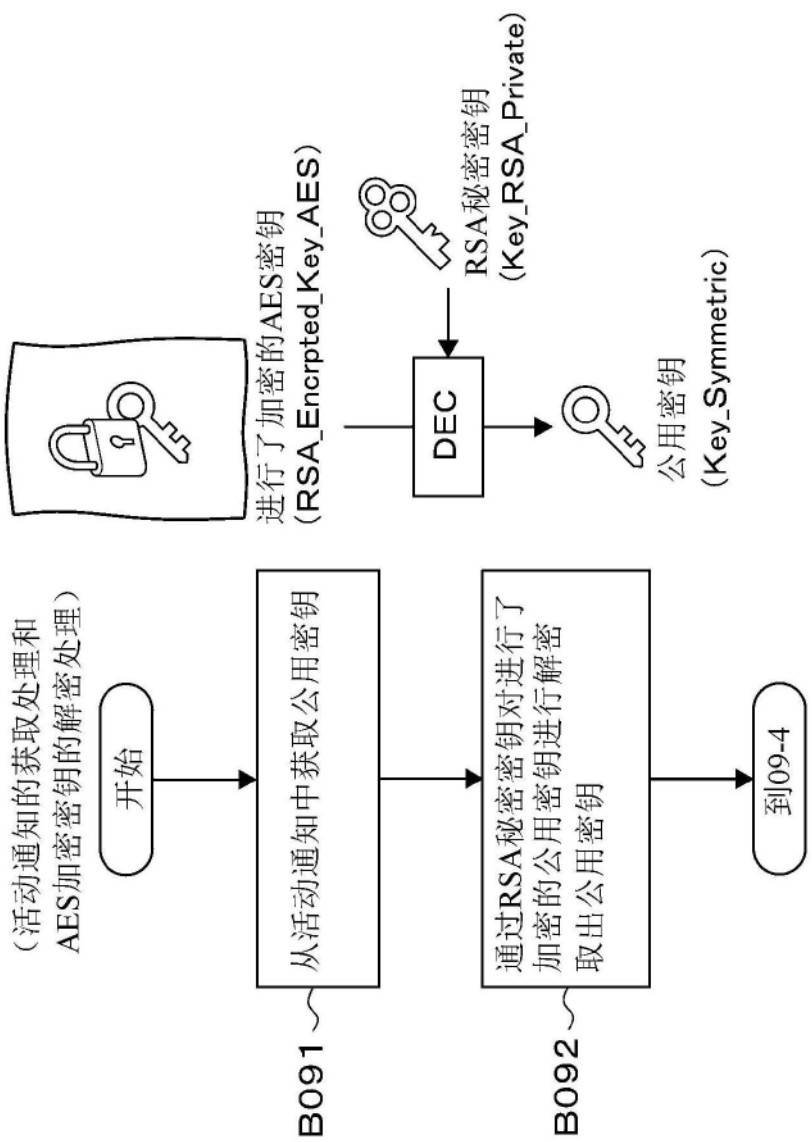

（活动通知的获取处理和
AES加密密钥的解密处理）
开始
从活动通知中获取公用密钥
B091
通过RSA秘密密钥对进行了
加密的公用密钥进行解密
取出公用密钥
B092
到09-4
进行了加密的AES密钥
(RSA_Encrpted_Key_AES)
DEC
RSA秘密密钥
(Key_RSA_Private)
公用密钥
(Key_Symmetric)

图83

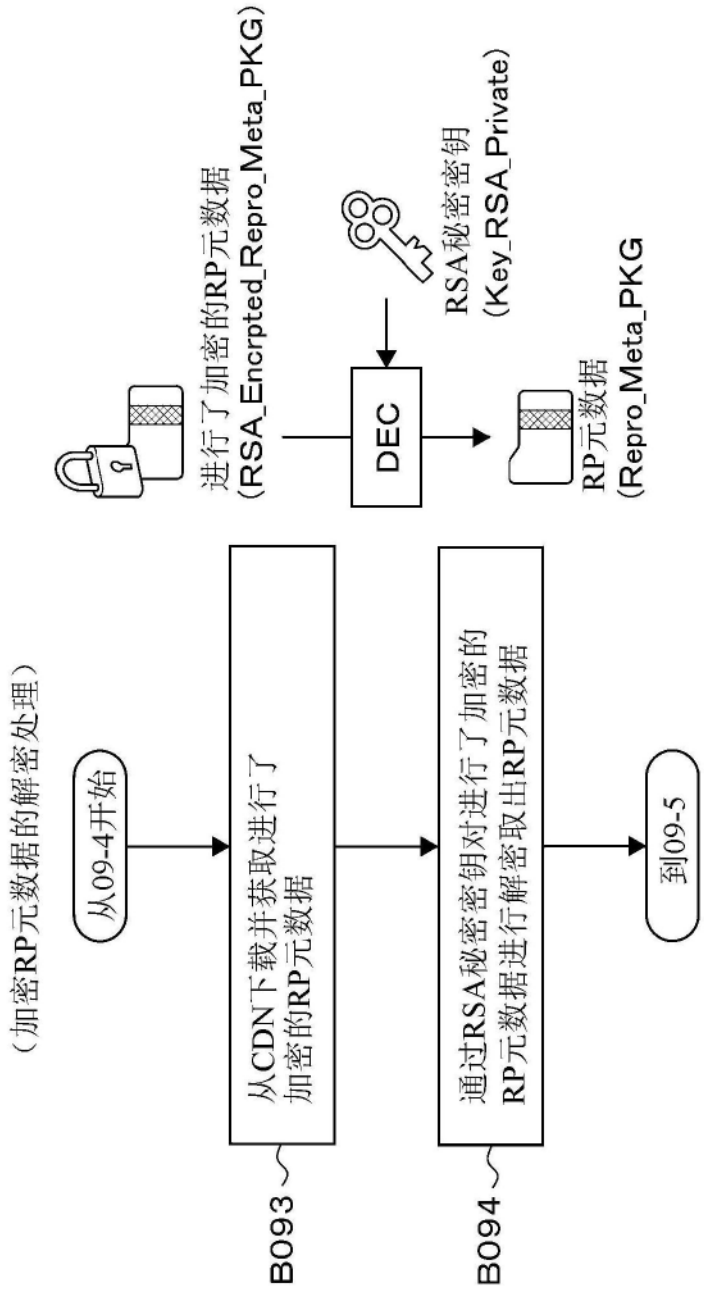

（加密RP元数据的解密处理）
从09-4开始
从CDN下载并获取进行了加密的RP元数据
B093
通过RSA秘密密钥对进行了加密的RP元数据进行解密取出RP元数据
B094
到09-5
进行了加密的RP元数据
(RSA_Encrpted_Repro_Meta_PKG)
DEC
RSA秘密密钥
(Key_RSA_Private)
RP元数据
(Repro_Meta_PKG

图84

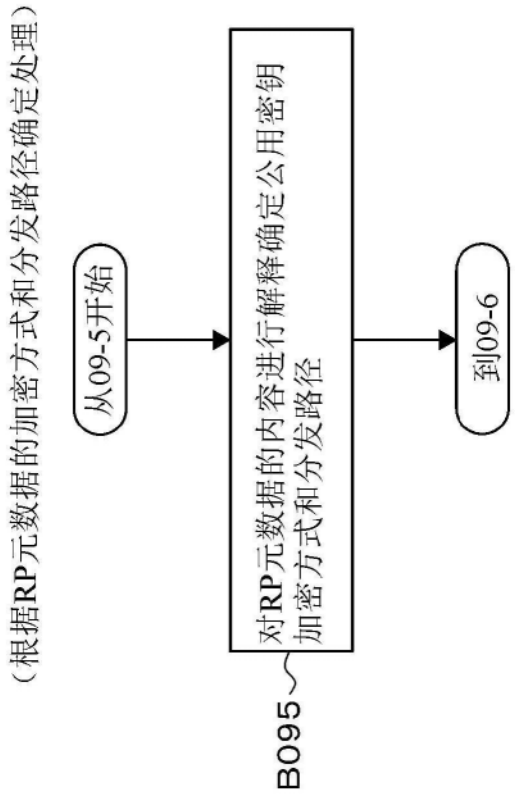

（根据RP元数据的加密方式和分发路径确定处理）
从09-5开始
对RP元数据的内容进行解释确定公用密钥
加密方式和分发路径
到09-6
B095

图85

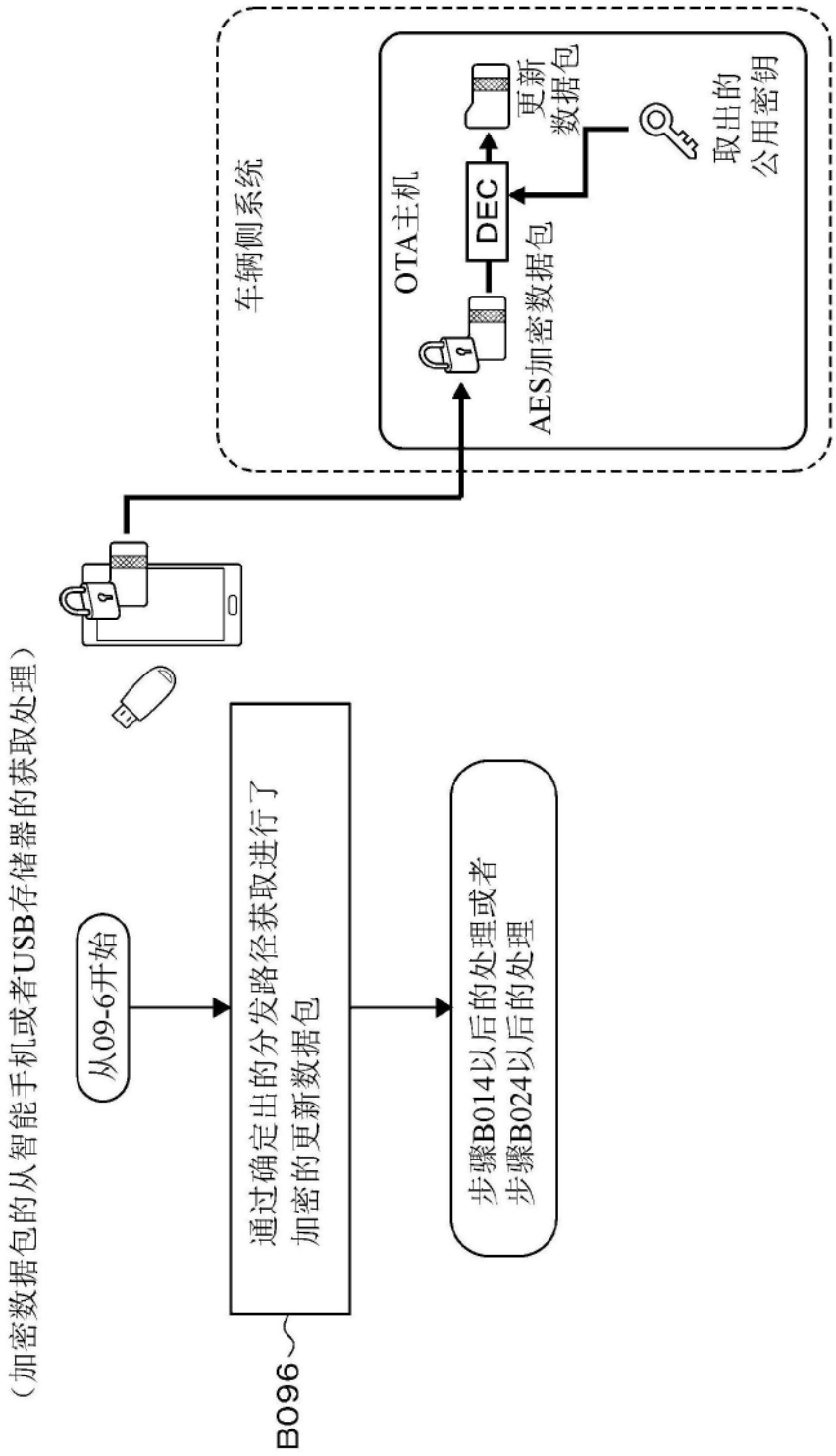

（加密数据包的从智能手机或者USB存储器的获取处理）
从09-6开始
通过确定出的分发路径获取进行了加密的更新数据包
B096
步骤B014以后的处理或者步骤B024以后的处理
车辆侧系统
OTA主机
AES加密数据包
DEC
更新数据包
取出的公用密钥

图86

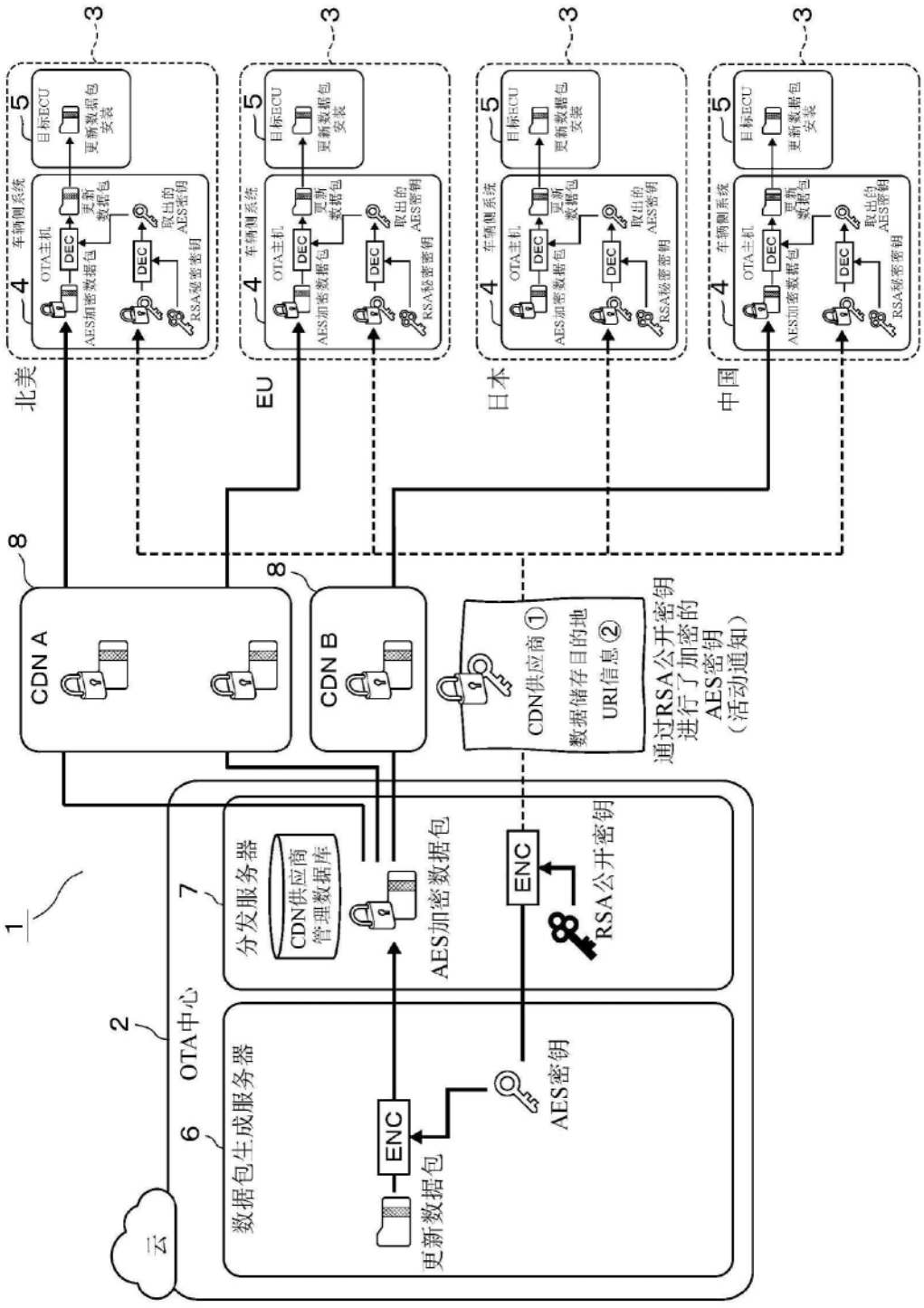

1
2
OTA中心
6
数据包生成服务器
云
更新数据包
ENC
AES密钥
7
分发服务器
CDN供应商
管理数据库
AES加密数据包
ENC
RSA公开密钥
8
CDN A
CDN B
8
CDN供应商 ①
数据储存目的地
URI信息 ②
通过RSA公开密钥
进行了加密的
AES密钥
（活动通知）
3
北美
EU
日本
中国
4
车辆侧系统
OTA主机
AES加密数据包
DEC
更新
数据包
DEC
取出的
AES密钥
RSA秘密密钥
5
目标ECU
更新数据包
安装

图87

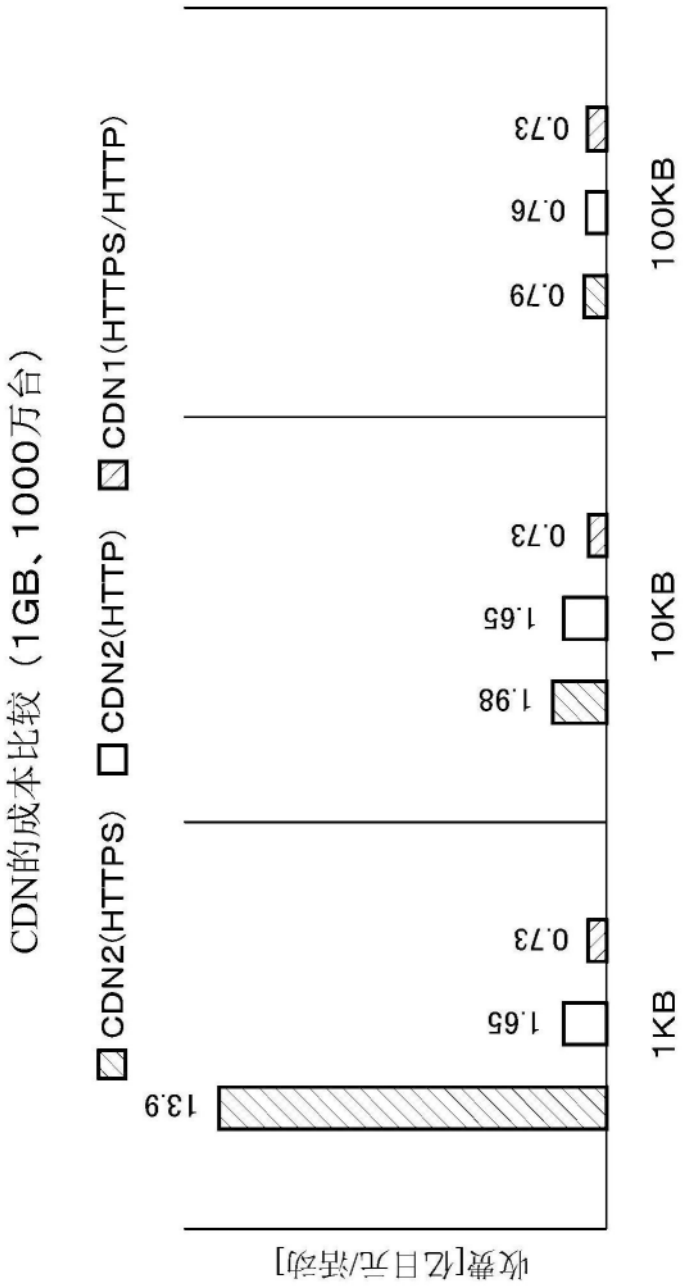

CDN的成本比较（1GB、1000万台）
CDN2(HTTPS)
CDN2(HTTP)
CDN1(HTTPS/HTTP)
收费[亿日元/活动]
1KB
10KB
100KB
13.9
1.65
0.73
1.98
1.65
0.73
0.79
0.76
0.73

图88

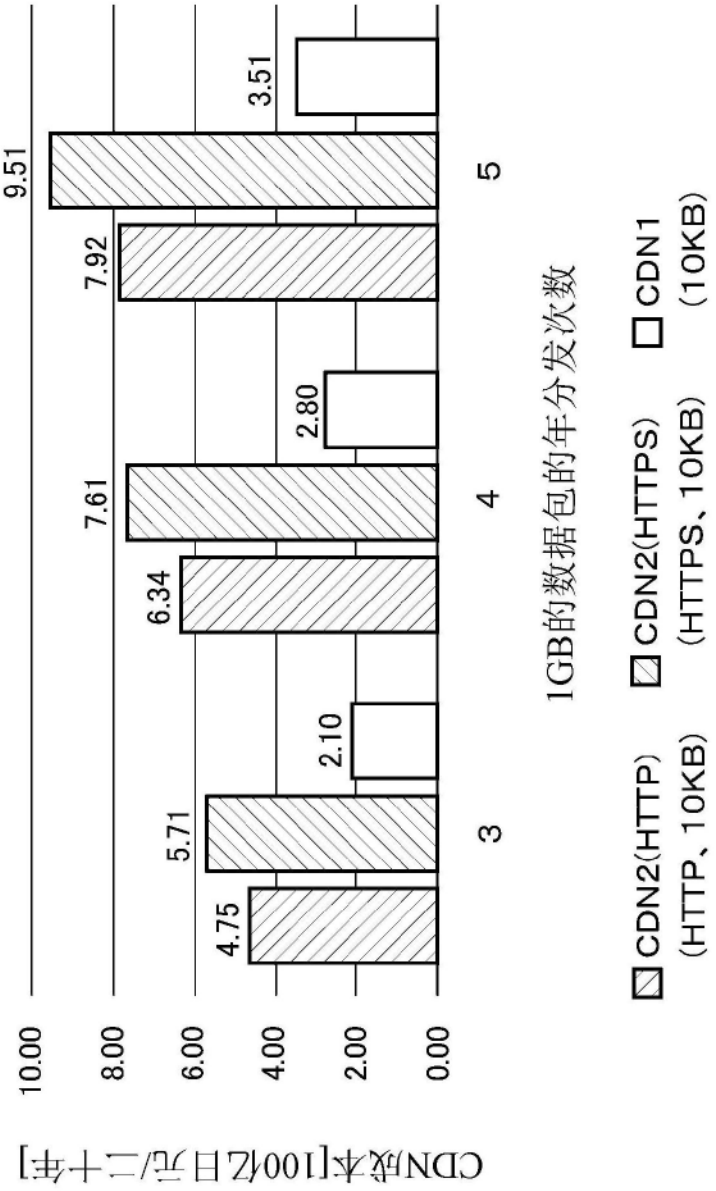

CDN成本[100亿日元/二十年]
10.00
8.00
6.00
4.00
2.00
0.00
9.51
7.92
7.61
6.34
5.71
4.75
3.51
2.80
2.10
5
4
3
1GB的数据包的年分发次数
CDN2(HTTP)
(HTTP、10KB)
CDN2(HTTPS)
(HTTPS、10KB)
CDN1
(10KB)

图89

CDN1	每一GB的收费表格						
	~10TB	~40TB	~100TB	~350TB	~500TB	~4PB	5PB~
日本	0.0129 USD	0.121 USD	0.112 USD	0.093 USD	0.075 USD	0.065 USD	0.065 USD
北美	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	每一GB的收费表格						
	~10TB	~40TB	~100TB	~350TB	~524TB	~4PB	5PB~
日本	0.114 USD	0.089 USD	0.086 USD	0.084 USD	0.080 USD	0.070 USD	0.060 USD
北美	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	HTTP方法的请求收费表格	
	HTTP请求	HTTPS请求
日本	0.009 USD	0.012 USD
北美	0.075 USD	0.010 USD
EU	0.009 USD	0.012 USD

图90

CDN1	储存方式 对象台数：200万台	收费表格			
		100MB	1GB	10GB	20GB
日本		245万日元	1452万日元	1亿4560万日元	2亿9120万日元
北美		125万日元	512万日元	5亿500万日元	10亿100万日元
EU		125万日元	512万日元	5亿500万日元	10亿100万日元

CDN2	储存方式 对象台数：200万台	收费表格			
		100MB	1GB	10GB	20GB
日本		189万日元	1760万日元	1亿3200万日元	2亿6400万日元
北美		88万日元	660万日元	4400万日元	8800万日元
EU		132万日元	660万日元	4400万日元	8800万日元

图91

CDN1	流式传输大小：1KB 对象台数：200万台	收费表格			
		100MB	1GB	10GB	20GB
日本		245万日元	1452万日元	1亿4560万日元	1亿9120万日元
北美		125万日元	512万日元	5亿500万日元	10亿100万日元
EU		125万日元	512万日元	5亿500万日元	10亿100万日元

CDN1	流式传输大小：10KB 对象台数：200万台	收费表格			
		100MB	1GB	10GB	20GB
日本		245万日元	1452万日元	1亿4560万日元	1亿9120万日元
北美		125万日元	512万日元	5亿500万日元	10亿100万日元
EU		125万日元	512万日元	5亿500万日元	10亿100万日元

CDN1	流式传输大小： 100KB 对象台数：200万台	收费表格			
		100MB	1GB	10GB	20GB
日本		245万日元	1452万日元	1亿4560万日元	1亿9120万日元
北美		125万日元	512万日元	5亿500万日元	10亿100万日元
EU		125万日元	512万日元	5亿500万日元	10亿100万日元

图92

CDN2	流式传输大小：1KB 对象台数：200万台	收费表格（HTTP/HTTPS）			
		100MB	1GB	10GB	20GB
日本		2169万日元/2829万日元	2亿1560万日元/2亿8160万日元	21亿1200万日元/27亿7200万日元	42亿2400万日元/55亿4400万日元
北美		1738万日元/2288万日元	1亿7160万日元/2亿2660万日元	16亿9400万日元/22亿4400万日元	33亿8800万日元/44亿8800万日元
EU		2112万日元/2772万日元	2亿460万日元/2亿7060万日元	20亿2400万日元/26亿8400万日元	40亿4800万日元/53亿6800万日元

CDN2	流式传输大小：10KB 对象台数：200万台	收费表格（HTTP/HTTPS）			
		100MB	1GB	10GB	20GB
日本		387万日元/453万日元	3740万日元/4400万日元	3亿3000万日元/3亿9600万日元	6亿6000万日元/7亿9200万日元
北美		253万日元/308万日元	2310万日元/2860万日元	2亿900万日元/2亿6400万日元	4亿8500万日元/5亿2800万日元
EU		330万日元/396万日元	2640万日元/3300万日元	2亿4200万日元/3亿800万日元	4亿8400万日元/6亿1600万日元

CDN2	流式传输大小：100KB 对象台数：200万台	收费表格（HTTP/HTTPS）			
		100MB	1GB	10GB	20GB
日本		209万日元/216万日元	1958万日元/2024万日元	1亿5180万日元/1亿5840万日元	3亿360万日元/3亿1680万日元
北美		105万日元/110万日元	825万日元/880万日元	6050万日元/6600万日元	1亿2100万日元/1亿3200万日元
EU		152万日元/158万日元	858万日元/924万日元	6380万日元/7040万日元	1亿2760万日元/1亿4080万日元

图93

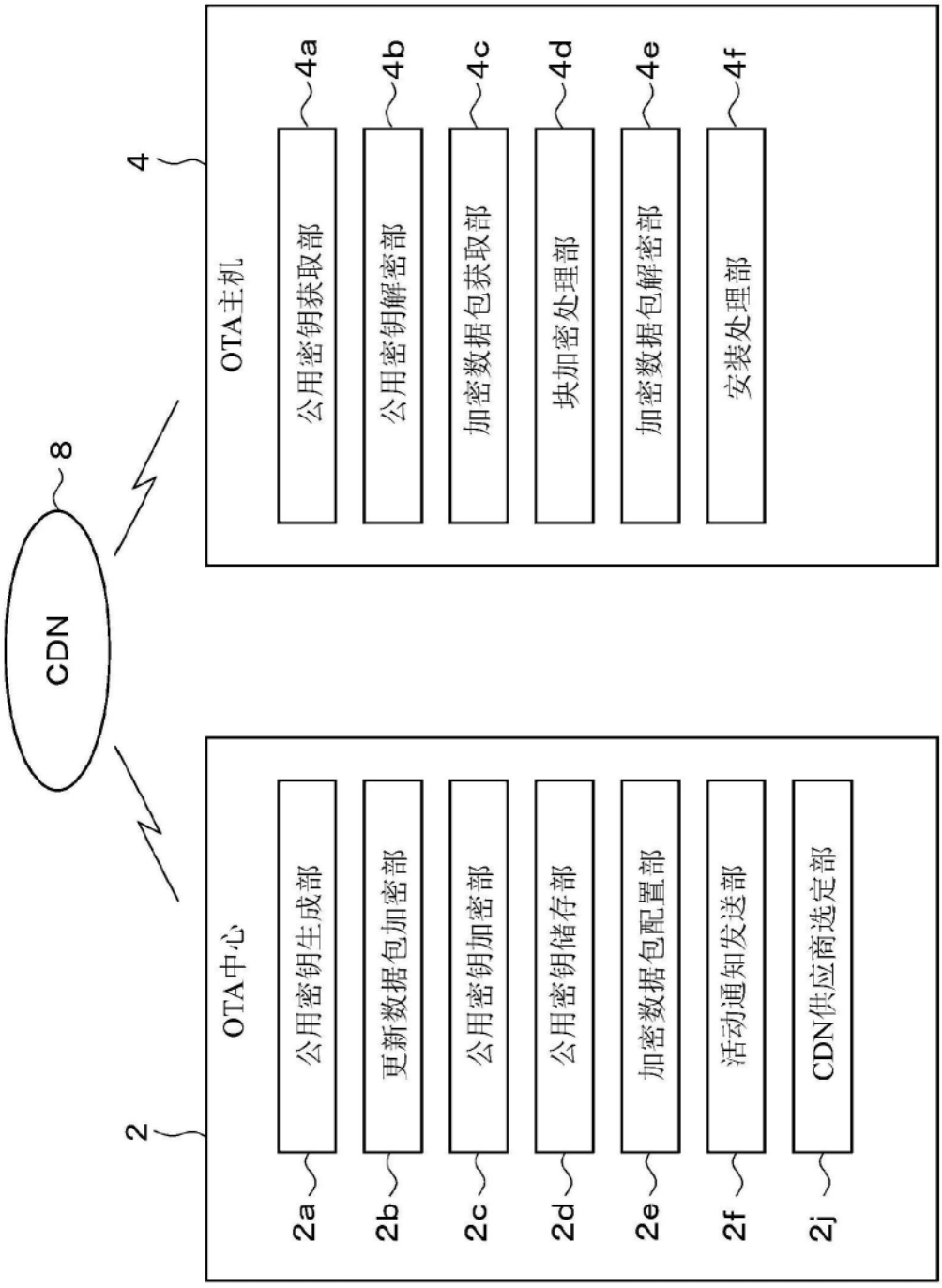

4
OTA主机
4a
公用密钥获取部
4b
公用密钥解密部
4c
加密数据包获取部
4d
块加密处理部
4e
加密数据包解密部
4f
安装处理部
8
CDN
2
OTA中心
2a
公用密钥生成部
2b
更新数据包加密部
2c
公用密钥加密部
2d
公用密钥储存部
2e
加密数据包配置部
2f
活动通知发送部
2j
CDN供应商选定部

图94

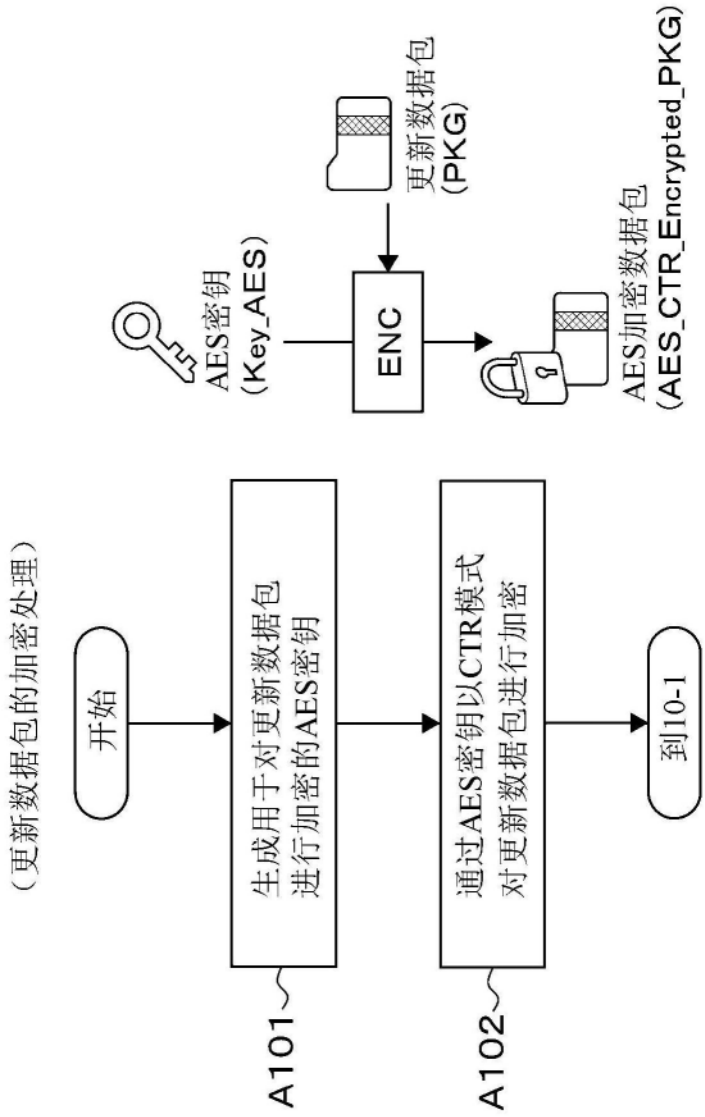

（更新数据包的加密处理）
开始
生成用于对更新数据包进行加密的AES密钥
A101
通过AES密钥以CTR模式对更新数据包进行加密
A102
到10-1
AES密钥
(Key_AES)
ENC
更新数据包
(PKG)
AES加密数据包
(AES_CTR_Encrypted_PKG)

图95

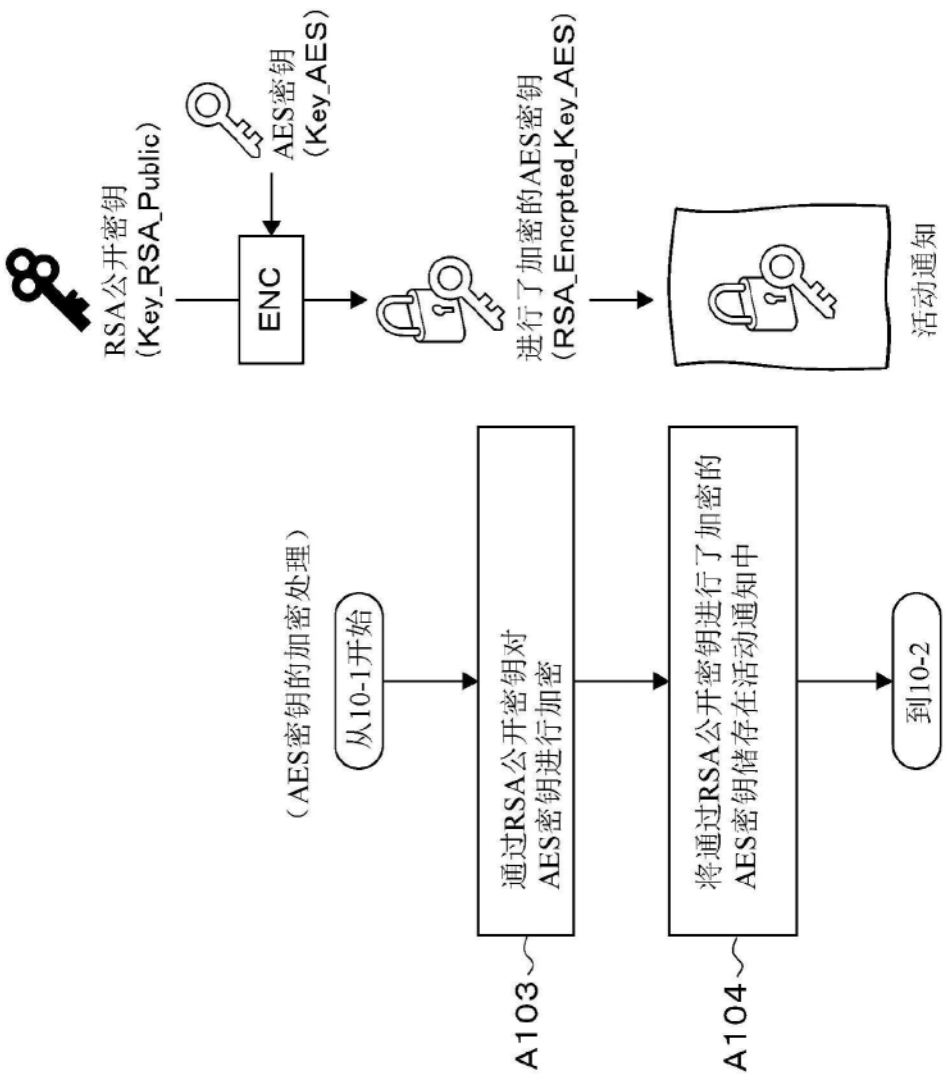

RSA公开密钥
(Key_RSA_Public)
AES密钥
(Key_AES)
ENC
进行了加密的AES密钥
(RSA_Encrpted_Key_AES)
活动通知
（AES密钥的加密处理）
从10-1开始
通过RSA公开密钥对
AES密钥进行加密
将通过RSA公开密钥进行了加密的
AES密钥储存在活动通知中
到10-2
A103
A104

图96

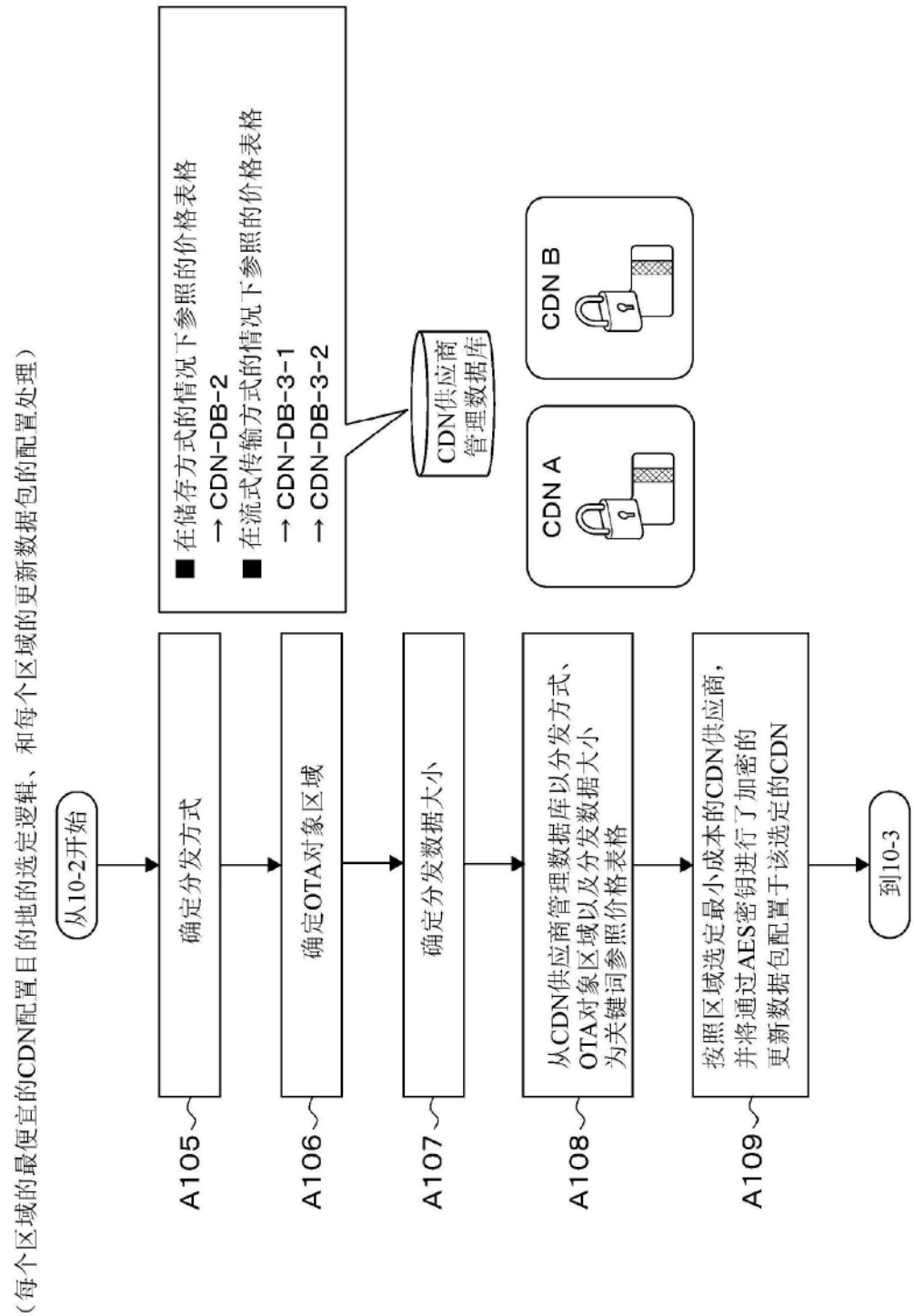

（每个区域的最便宜的CDN配置目的地的选定逻辑、和每个区域的更新数据包的配置处理）
从10-2开始
确定分发方式
A105
■ 在储存方式的情况下参照的价格表格
→ CDN-DB-2
■ 在流式传输方式的情况下参照的价格表格
→ CDN-DB-3-1
→ CDN-DB-3-2
CDN供应商管理数据库
确定OTA对象区域
A106
确定分发数据大小
A107
从CDN供应商管理数据库以分发方式、OTA对象区域以及分发数据大小为关键词参照价格表格
A108
按照区域选定最小成本的CDN供应商，并将通过AES密钥进行了加密的更新数据包配置于该选定的CDN
A109
到10-3
CDN A
CDN B

图97

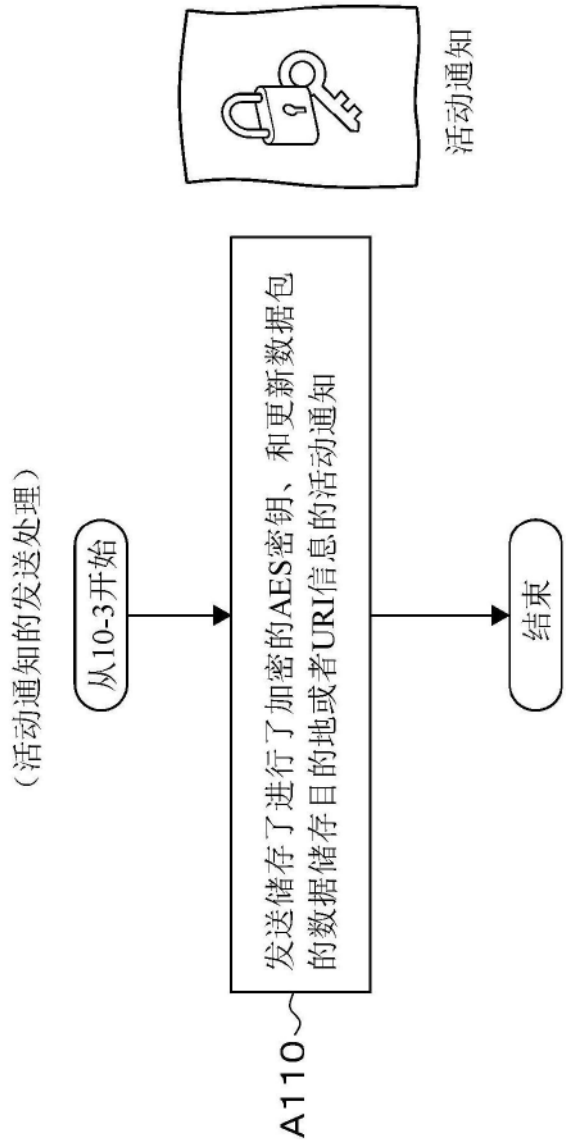

活动通知
（活动通知的发送处理）
从10-3开始
发送储存了进行了加密的AES密钥、和更新数据包的数据储存目的地或者URI信息的活动通知
结束
A110

图98

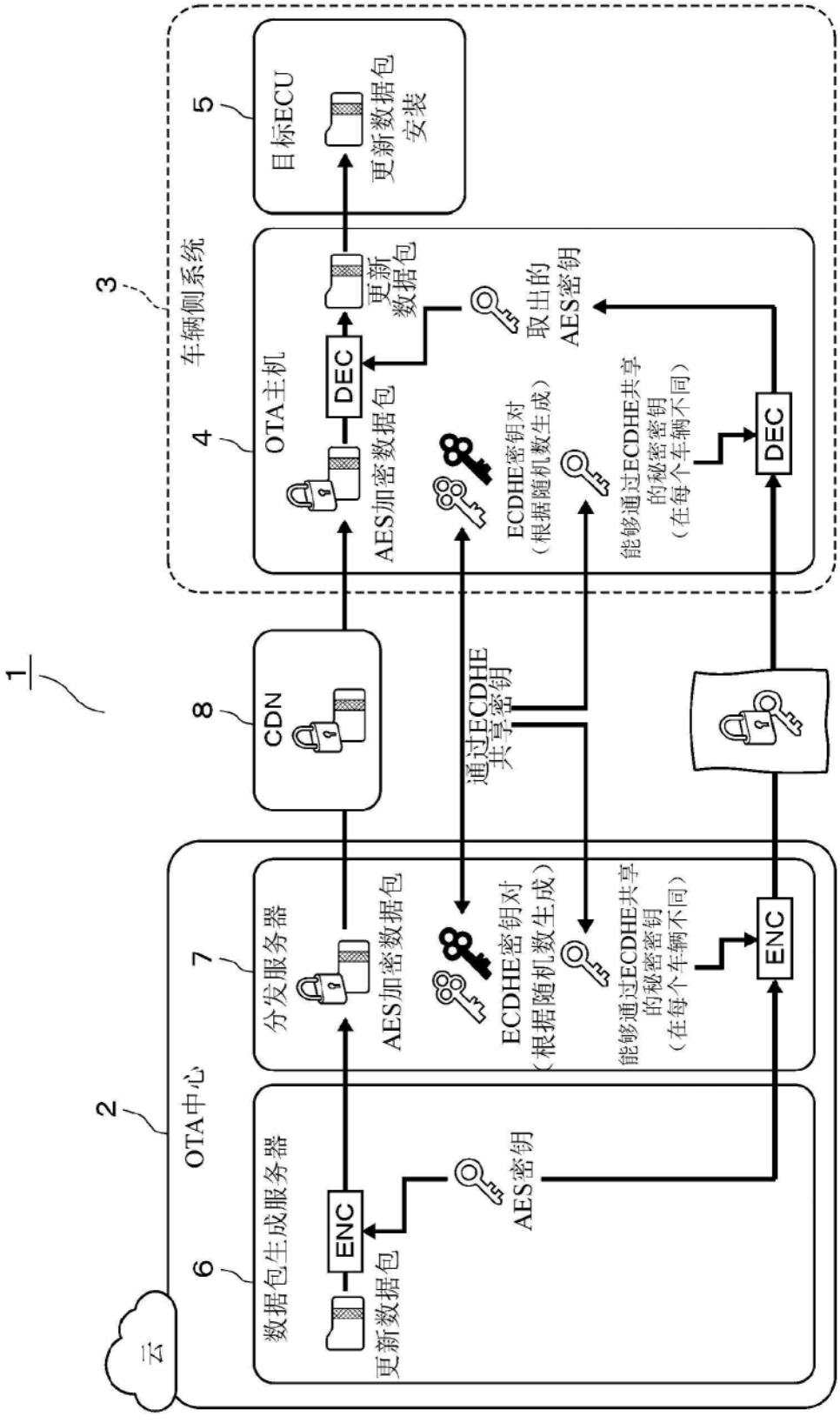

1
2
OTA中心
3
车辆侧系统
4
OTA主机
5
目标ECU
6
数据包生成服务器
7
分发服务器
8
CDN
云
ENC
DEC
更新数据包
AES加密数据包
AES密钥
ECDHE密钥对
（根据随机数生成）
通过ECDHE
共享密钥
能够通过ECDHE共享
的秘密密钥
（在每个车辆不同）
取出的
AES密钥
更新数据包
安装

图99

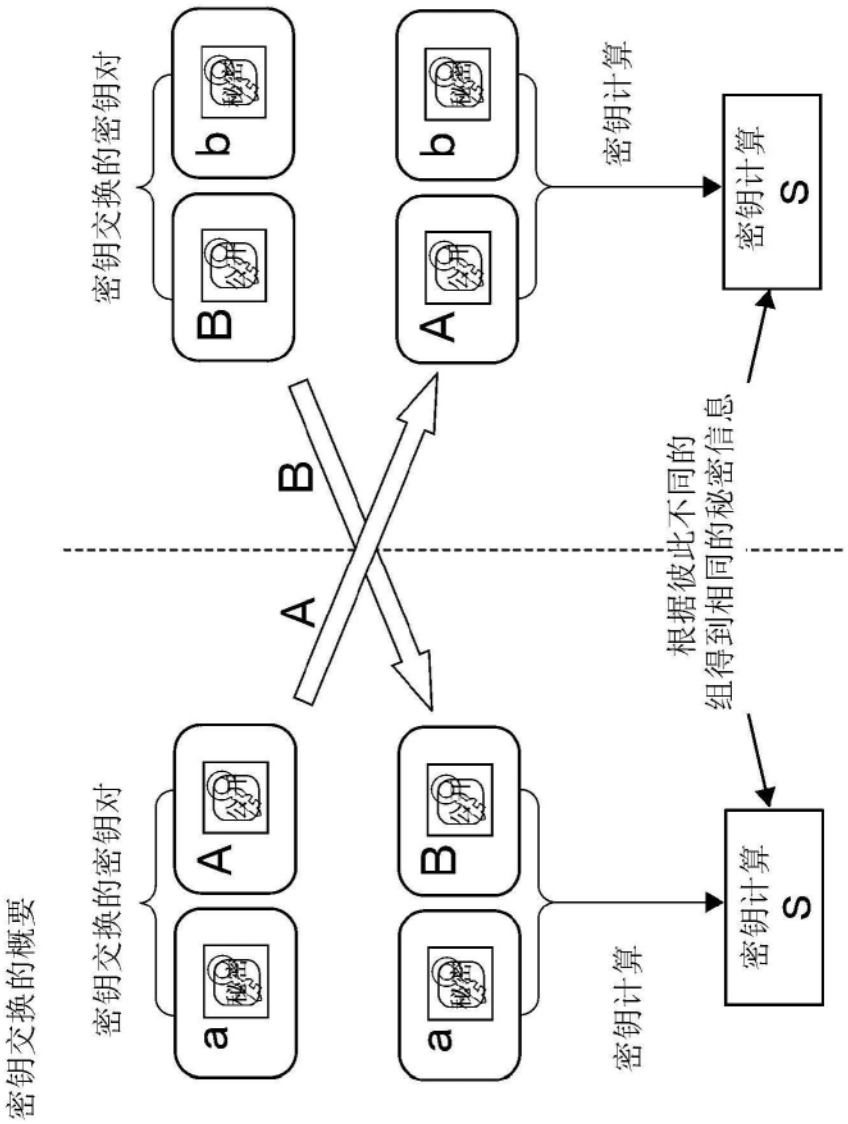

密钥交换的概要
密钥交换的密钥对
a
秘密
A
公开
密钥交换的密钥对
b
秘密
B
公开
A
B
密钥计算
密钥计算
根据彼此不同的
组得到相同的秘密信息
密钥计算
S
密钥计算
S

图100

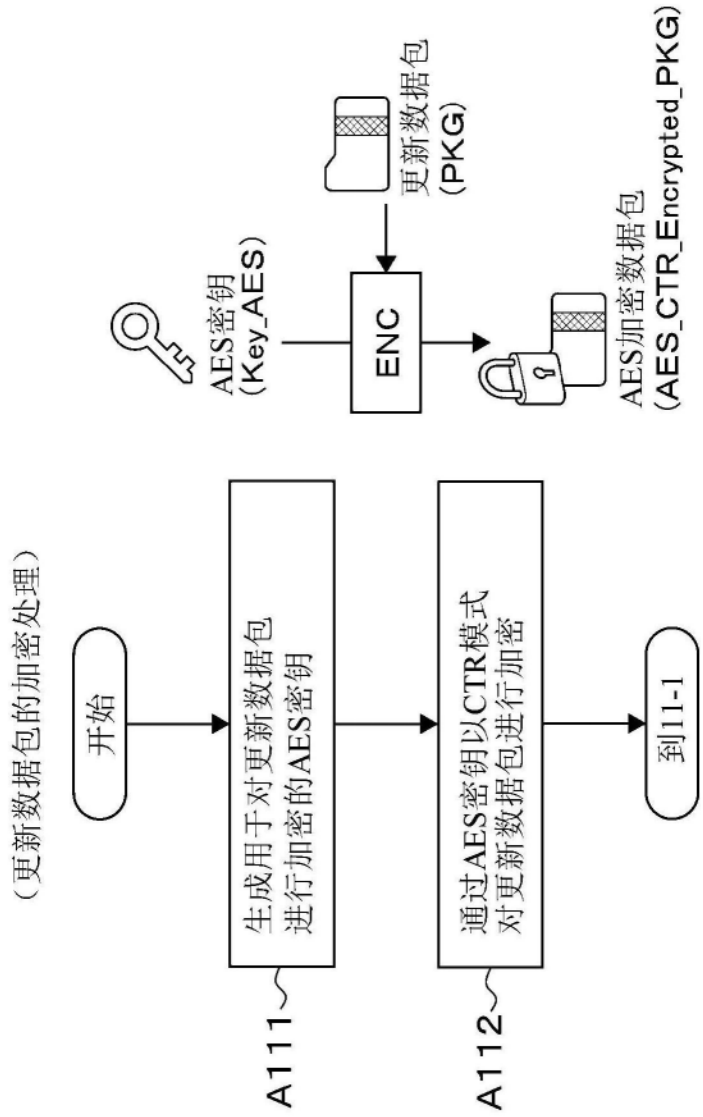

（更新数据包的加密处理）
开始
生成用于对更新数据包进行加密的AES密钥
A111
通过AES密钥以CTR模式对更新数据包进行加密
A112
到11-1
AES密钥
(Key_AES)
ENC
更新数据包
(PKG)
AES加密数据包
(AES_CTR_Encrypted_PKG)

图101

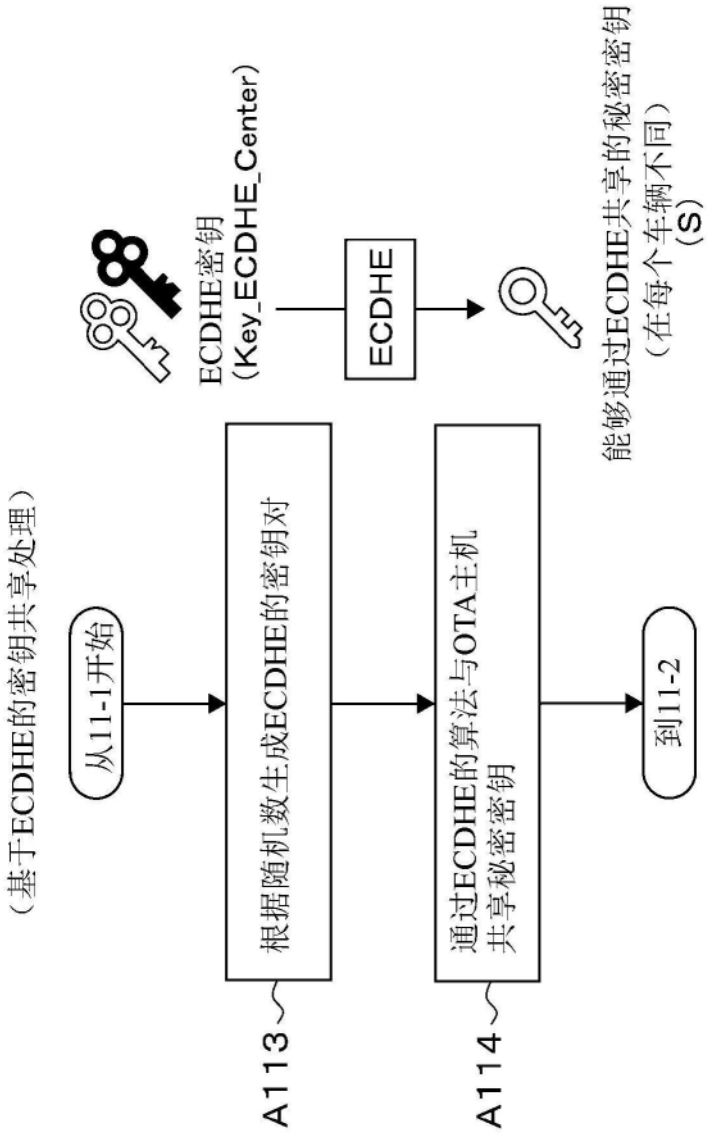

（基于ECDHE的密钥共享处理）
从11-1开始
根据随机数生成ECDHE的密钥对
A113
通过ECDHE的算法与OTA主机
共享秘密密钥
A114
到11-2
ECDHE密钥
(Key_ECDHE_Center)
ECDHE
能够通过ECDHE共享的秘密密钥
（在每个车辆不同）
(S)

图102

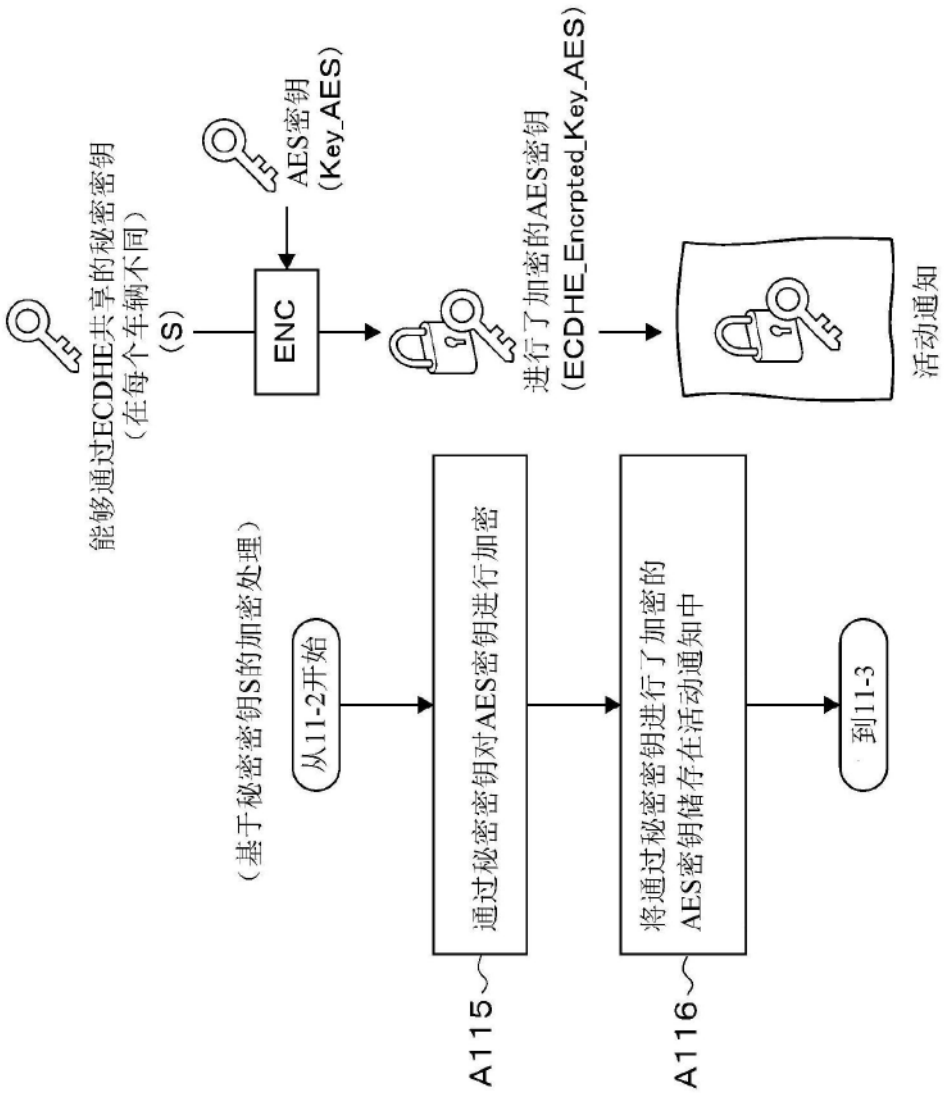

能够通过ECDHE共享的秘密密钥
（在每个车辆不同）
(S)
AES密钥
(Key_AES)
ENC
进行了加密的AES密钥
(ECDHE_Encrpted_Key_AES)
活动通知
（基于秘密密钥S的加密处理）
从11-2开始
通过秘密密钥对AES密钥进行加密
将通过秘密密钥进行了加密的
AES密钥储存在活动通知中
到11-3
A115
A116

图103

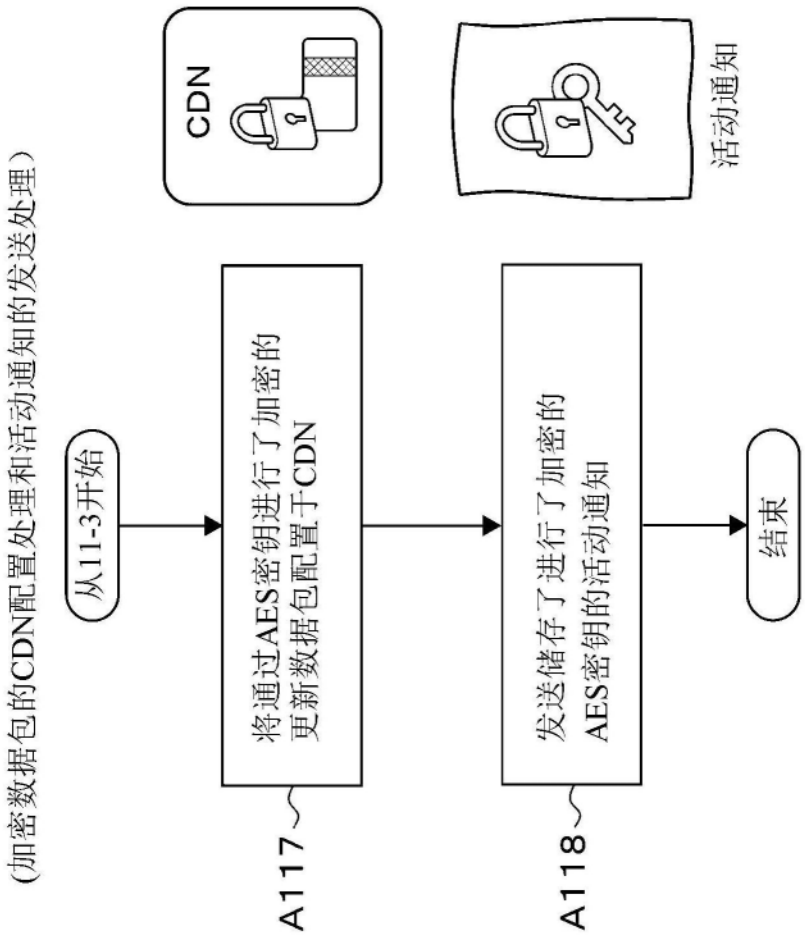

(加密数据包的CDN配置处理和活动通知的发送处理)
从11-3开始
将通过AES密钥进行了加密的更新数据包配置于CDN
A117
发送储存了进行了加密的AES密钥的活动通知
A118
结束
CDN
活动通知

图104

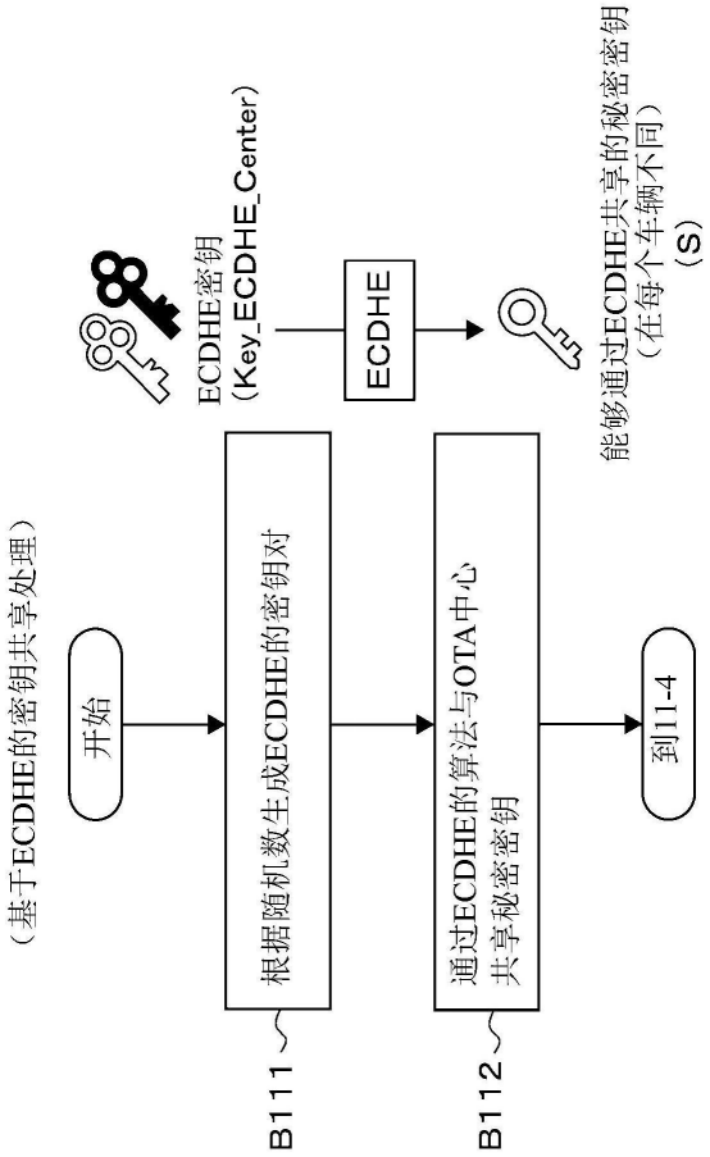

（基于ECDHE的密钥共享处理）
开始
根据随机数生成ECDHE的密钥对
B111
通过ECDHE的算法与OTA中心
共享秘密密钥
B112
到11-4
ECDHE密钥
（Key_ECDHE_Center）
ECDHE
能够通过ECDHE共享的秘密密钥
（在每个车辆不同）
(S)

图105

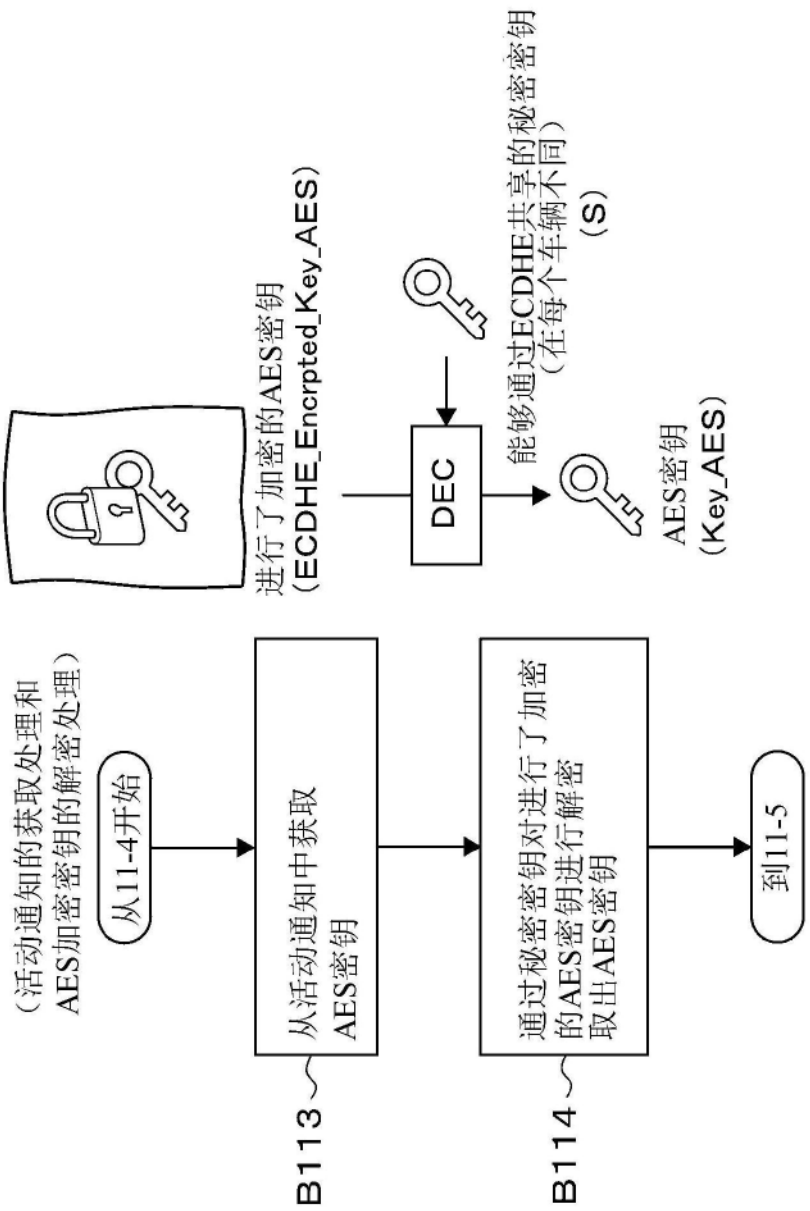

（活动通知的获取处理和
AES加密密钥的解密处理）
从11-4开始
从活动通知中获取
AES密钥
B113
通过秘密密钥对进行了加密
的AES密钥进行解密
取出AES密钥
B114
到11-5
进行了加密的AES密钥
（ECDHE_Encrpted_Key_AES）
DEC
能够通过ECDHE共享的秘密密钥
（在每个车辆不同）
（S）
AES密钥
（Key_AES）

图106

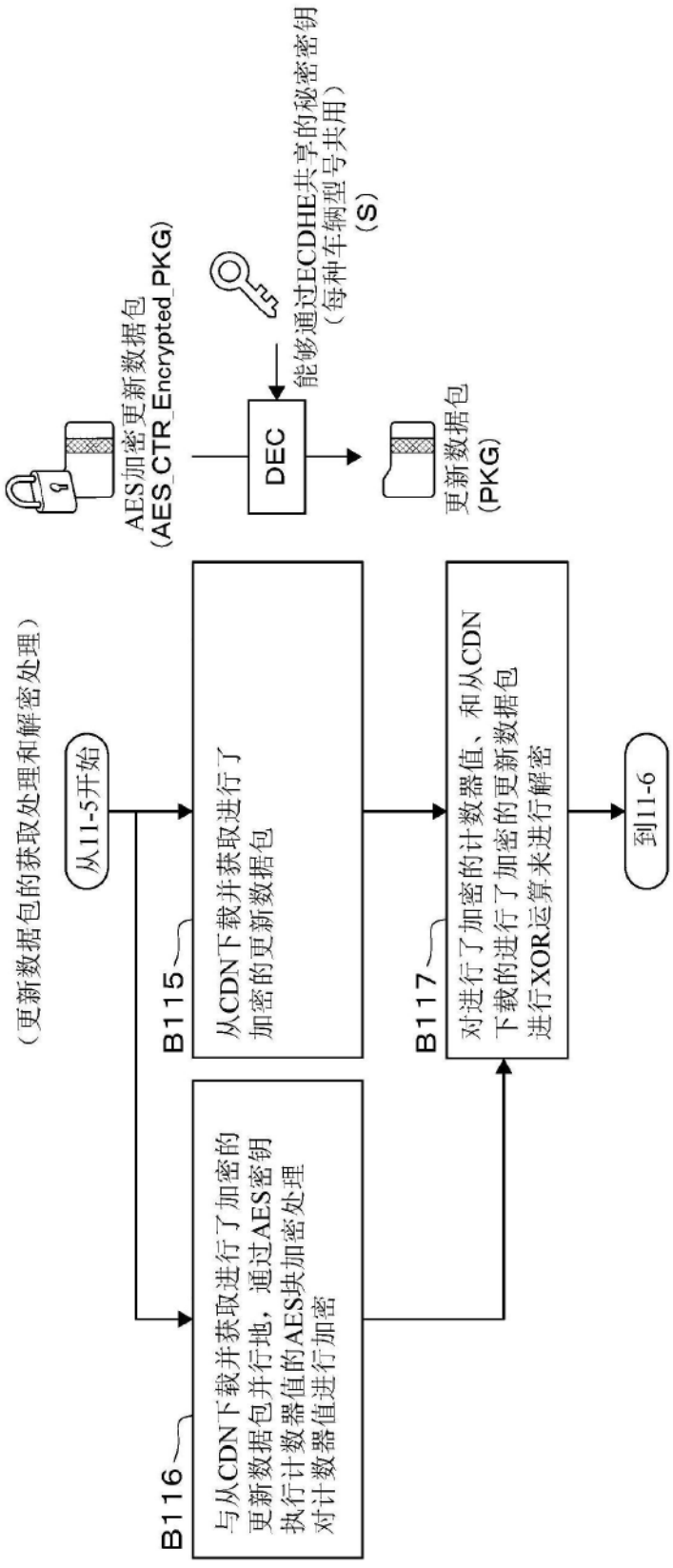

（更新数据包的获取处理和解密处理）
从11-5开始
AES加密更新数据包
(AES_CTR_Encrypted_PKG)
DEC
能够通过ECDHE共享的秘密密钥
（每种车辆型号共用）
(S)
更新数据包
(PKG)
B115
从CDN下载并获取进行了
加密的更新数据包
B116
与从CDN下载并获取进行了加密的
更新数据包并行地，通过AES密钥
执行计数器值的AES块加密处理
对计数器值进行加密
B117
对进行了加密的计数器值、和从CDN
下载的进行了加密的更新数据包
进行XOR运算来进行解密
到11-6

图107

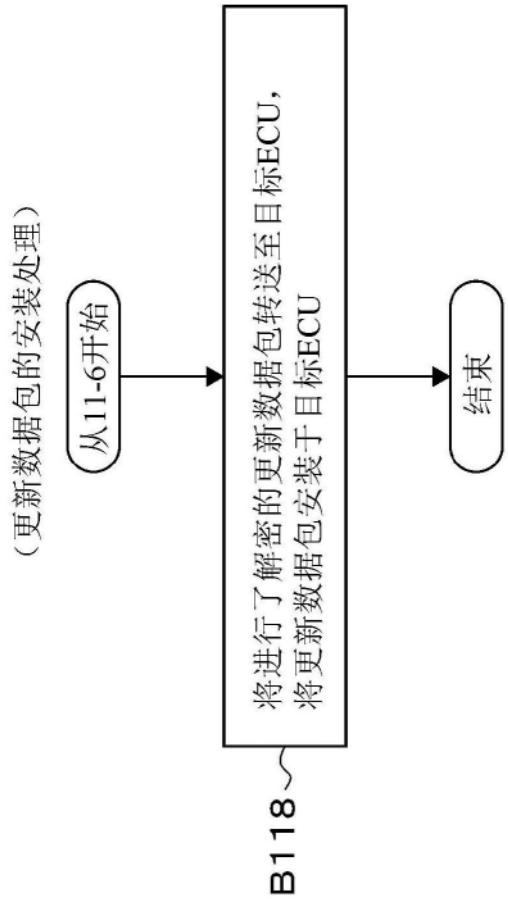

（更新数据包的安装处理）
从11-6开始
将进行了解密的更新数据包转送至目标ECU，
将更新数据包安装于目标ECU
结束
B118

图108

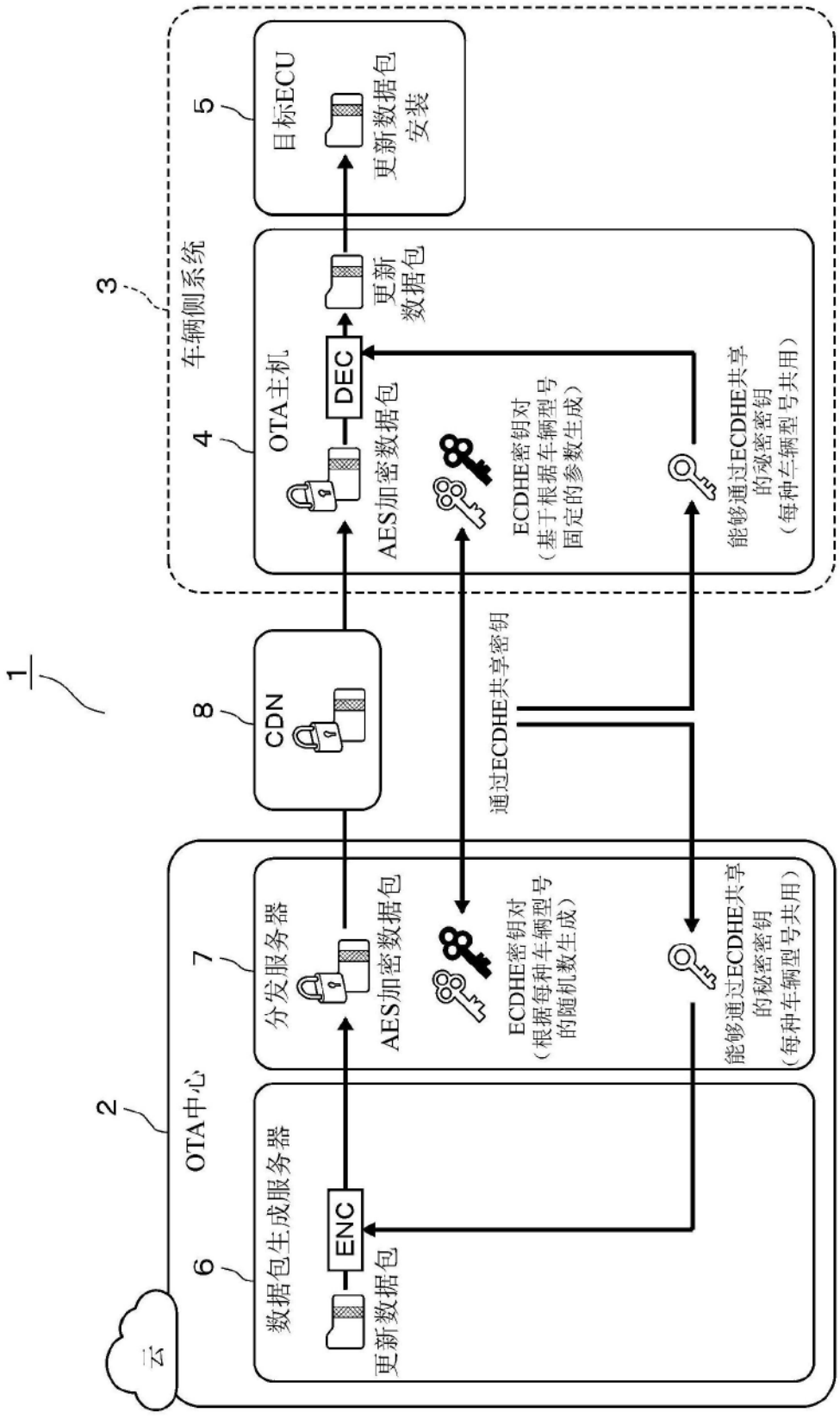

1
2
OTA中心
云
6
数据包生成服务器
更新数据包
ENC
7
分发服务器
AES加密数据包
ECDHE密钥对
（根据每种车辆型号的随机数生成）
能够通过ECDHE共享的秘密密钥（每种车辆型号共用）
8
CDN
通过ECDHE共享密钥
3
车辆侧系统
4
OTA主机
AES加密数据包
DEC
更新数据包
ECDHE密钥对
（基于根据车辆型号固定的参数生成）
能够通过ECDHE共享的秘密密钥（每种车辆型号共用）
5
目标ECU
更新数据包安装

图109

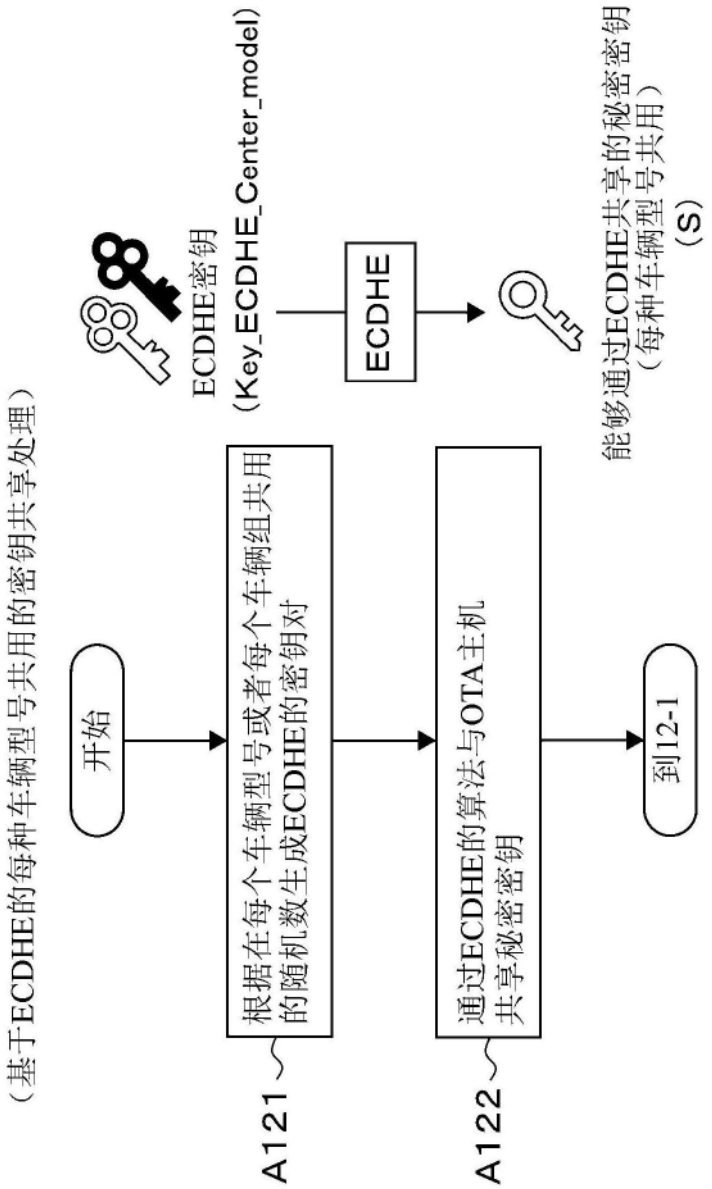

（基于ECDHE的每种车辆型号共用的密钥共享处理）
开始
根据在每个车辆型号或者每个车辆组共用的随机数生成ECDHE的密钥对
A121
通过ECDHE的算法与OTA主机共享秘密密钥
A122
到12-1
ECDHE密钥
(Key_ECDHE_Center_model)
ECDHE
能够通过ECDHE共享的秘密密钥
（每种车辆型号共用）
(S)

图110

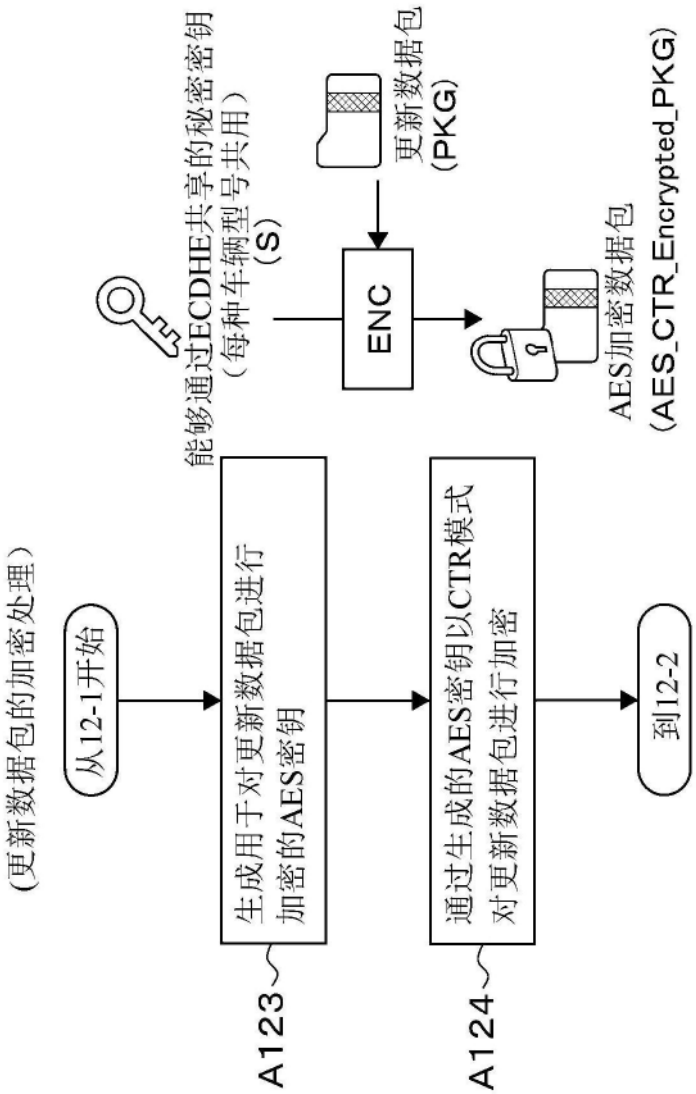

(更新数据包的加密处理)
从12-1开始
生成用于对更新数据包进行加密的AES密钥
A123
通过生成的AES密钥以CTR模式对更新数据包进行加密
A124
到12-2
能够通过ECDHE共享的秘密密钥（每种车辆型号共用）(S)
ENC
更新数据包(PKG)
AES加密数据包(AES_CTR_Encrypted_PKG)

图111

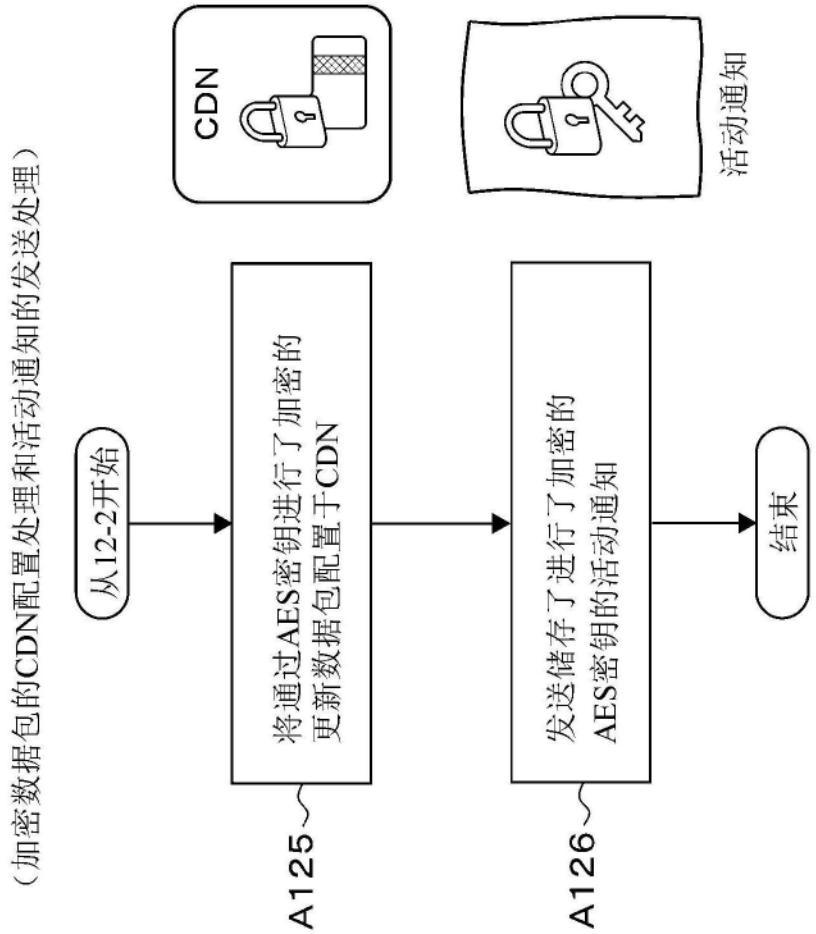

（加密数据包的CDN配置处理和活动通知的发送处理）
从12-2开始
将通过AES密钥进行了加密的更新数据包配置于CDN
A125
发送储存了进行了加密的AES密钥的活动通知
A126
结束
CDN
活动通知

图112

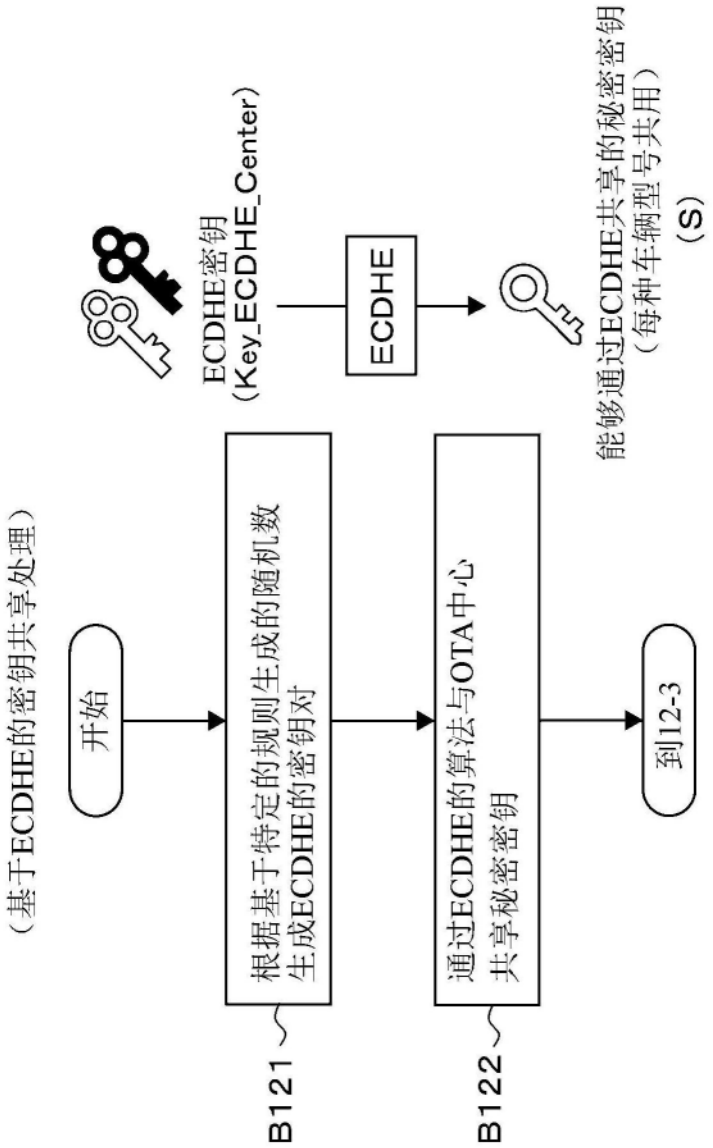

（基于ECDHE的密钥共享处理）
开始
根据基于特定的规则生成的随机数
生成ECDHE的密钥对
B121
通过ECDHE的算法与OTA中心
共享秘密密钥
B122
到12-3
ECDHE密钥
（Key_ECDHE_Center）
ECDHE
能够通过ECDHE共享的秘密密钥
（每种车辆型号共用）
（S）

图113

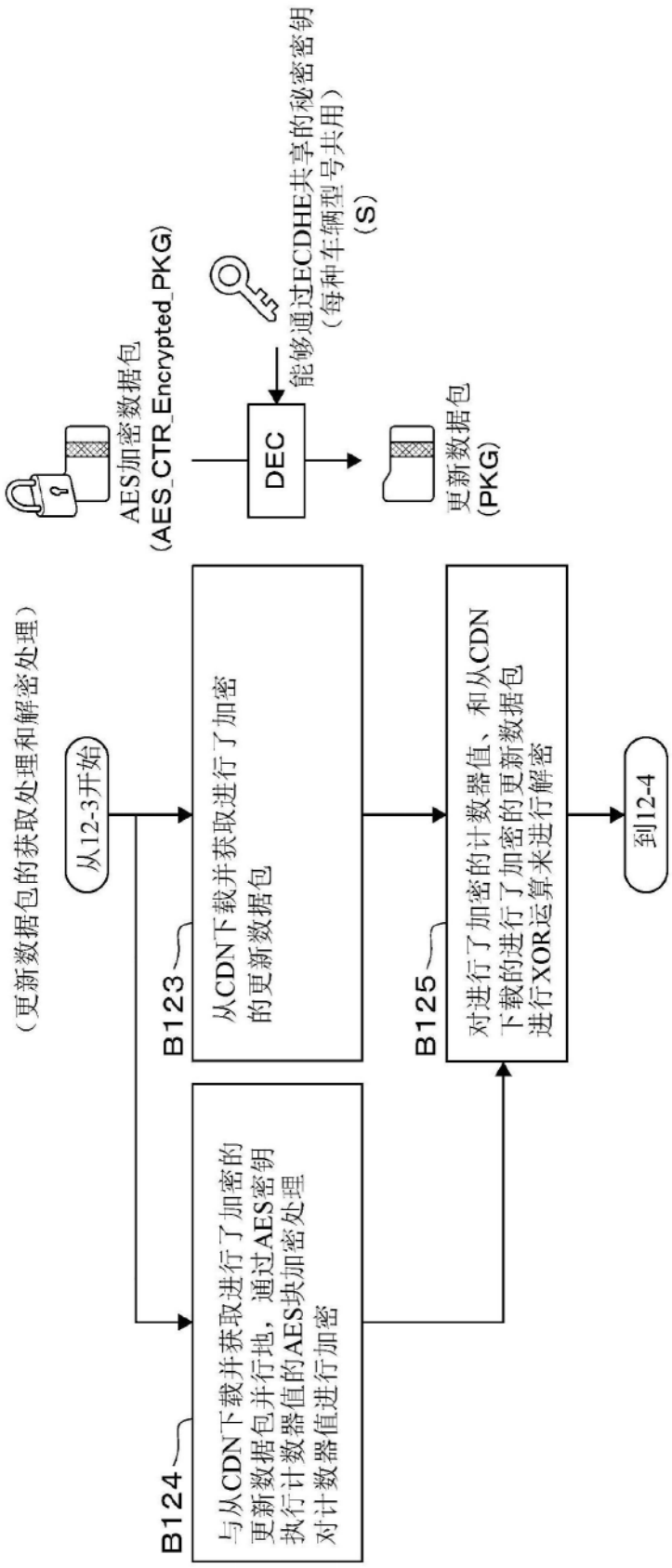

（更新数据包的获取处理和解密处理）
从12-3开始
B123
从CDN下载并获取进行了加密的更新数据包
B124
与从CDN下载并获取进行了加密的更新数据包并行地，通过AES密钥执行计数器值的AES块加密处理对计数器值进行加密
B125
对进行了加密的计数器值、和从CDN下载的进行了加密的更新数据包进行XOR运算来进行解密
到12-4
AES加密数据包
(AES_CTR_Encrypted_PKG)
DEC
能够通过ECDHE共享的秘密密钥
（每种车辆型号共用）
(S)
更新数据包
(PKG)

图114

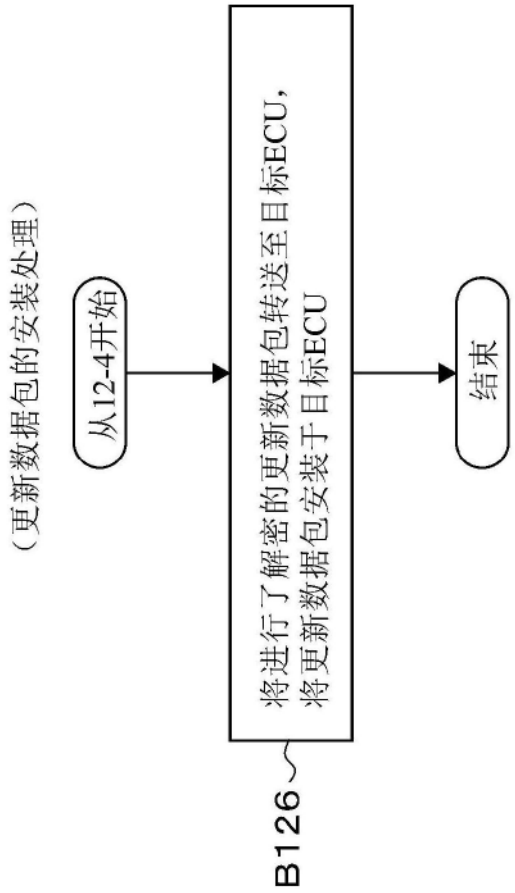

（更新数据包的安装处理）
从12-4开始
将进行了解密的更新数据包转送至目标ECU，
将更新数据包安装于目标ECU
B126
结束

图115

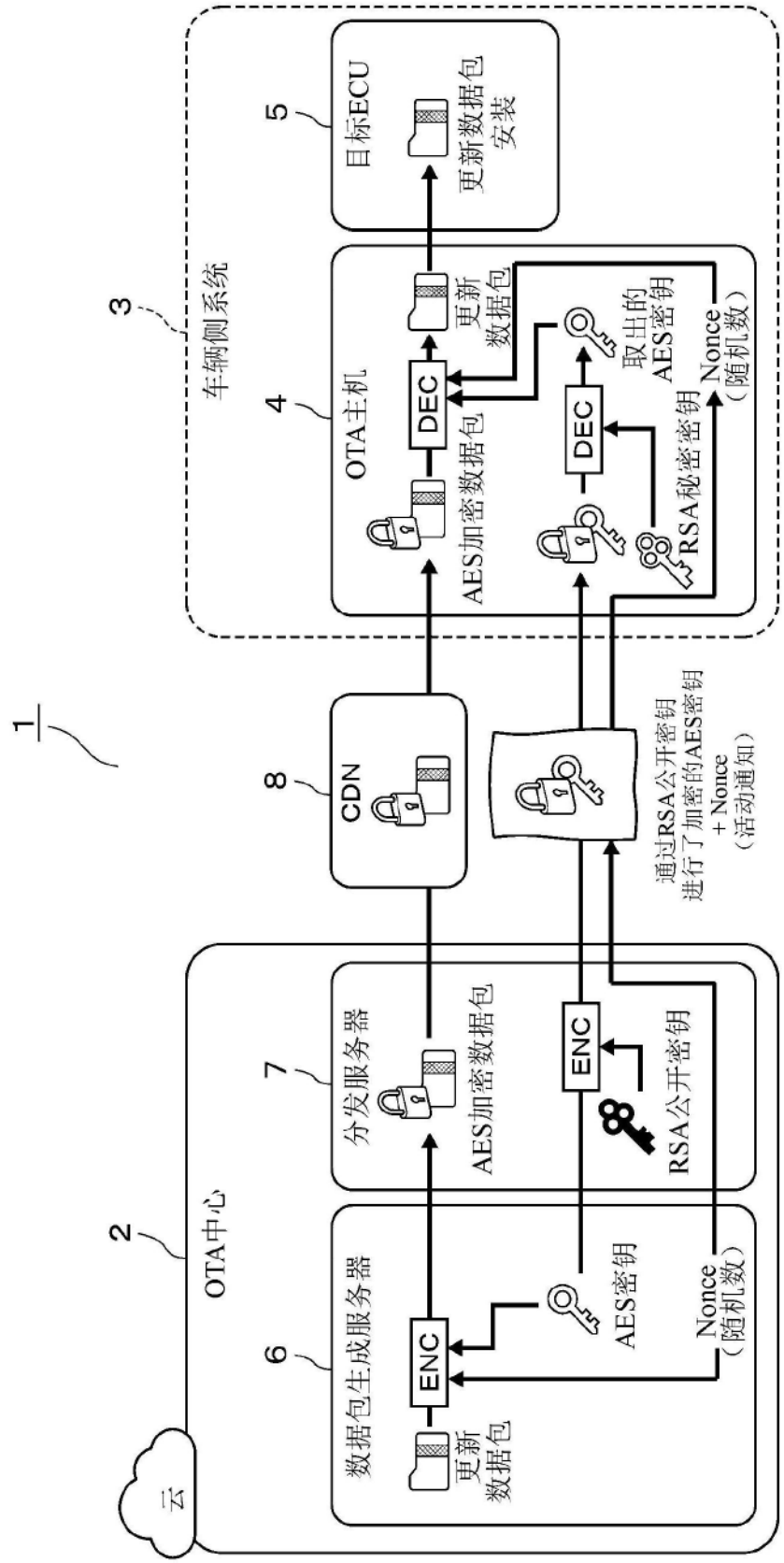

1
2
OTA中心
云
6
数据包生成服务器
ENC
更新数据包
AES密钥
Nonce（随机数）
7
分发服务器
AES加密数据包
ENC
RSA公开密钥
8
CDN
通过RSA公开密钥进行了加密的AES密钥 + Nonce（活动通知）
3
车辆侧系统
4
OTA主机
AES加密数据包
DEC
更新数据包
DEC
RSA秘密密钥
取出的AES密钥
Nonce（随机数）
5
目标ECU
更新数据包安装

图116

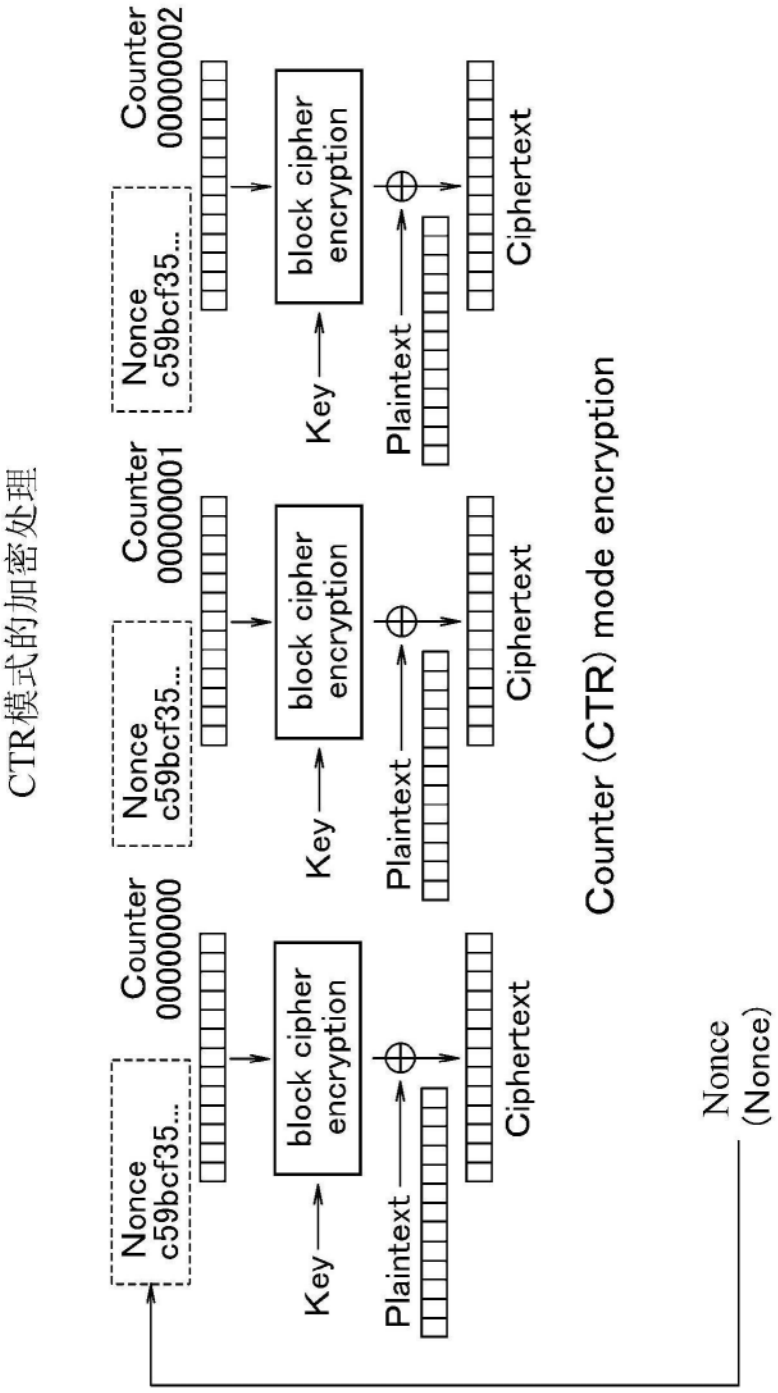

CTR模式的加密处理
Counter (CTR) mode encryption
Nonce
(Nonce)
Nonce c59bcf35...
Counter 00000000
Counter 00000001
Counter 00000002
block cipher encryption
Key
Plaintext
Ciphertext

图117

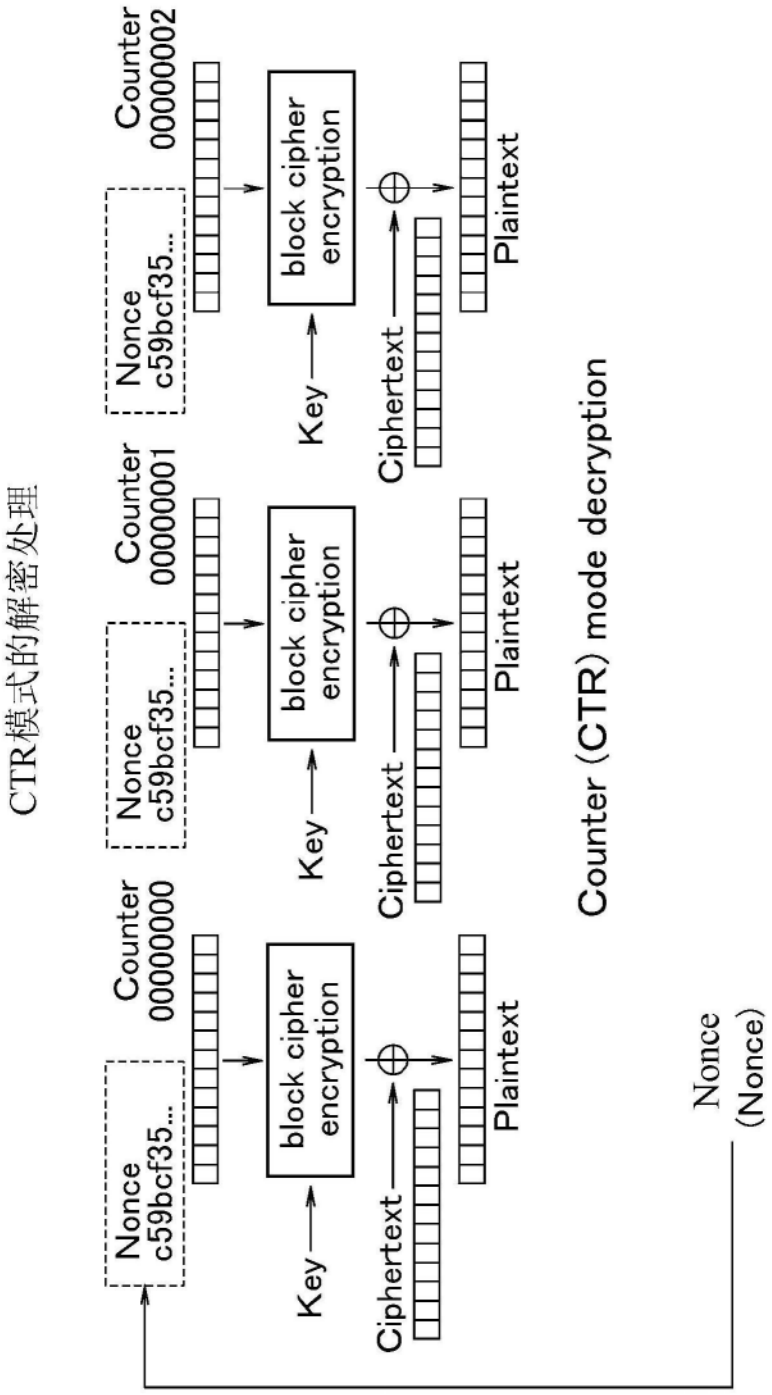

CTR模式的解密处理
Counter (CTR) mode decryption
Nonce
(Nonce)
Nonce c59bcf35...
Counter 00000000
Counter 00000001
Counter 00000002
block cipher encryption
Key
Ciphertext
Plaintext

图118

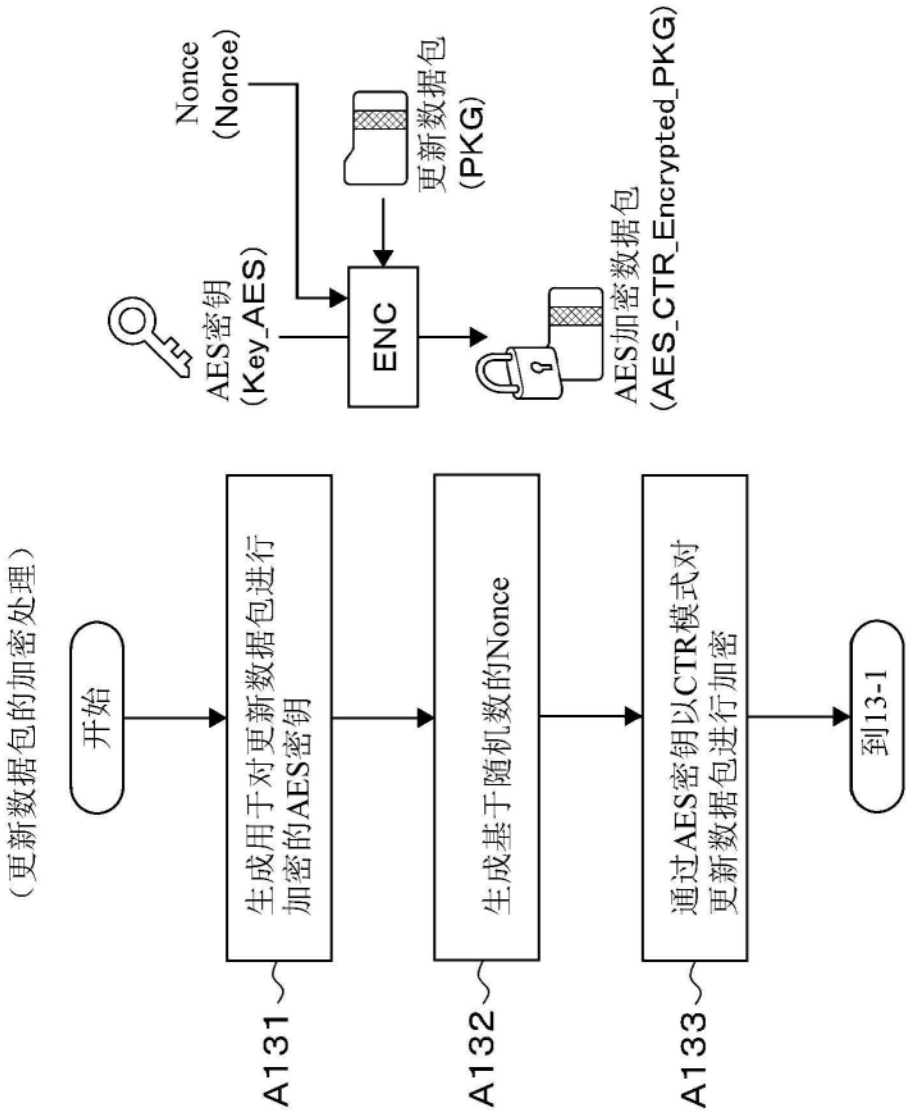

Nonce
(Nonce)
更新数据包
(PKG)
AES密钥
(Key_AES)
ENC
AES加密数据包
(AES_CTR_Encrypted_PKG)
（更新数据包的加密处理）
开始
生成用于对更新数据包进行加密的AES密钥
生成基于随机数的Nonce
通过AES密钥以CTR模式对更新数据包进行加密
到13-1
A131
A132
A133

图119

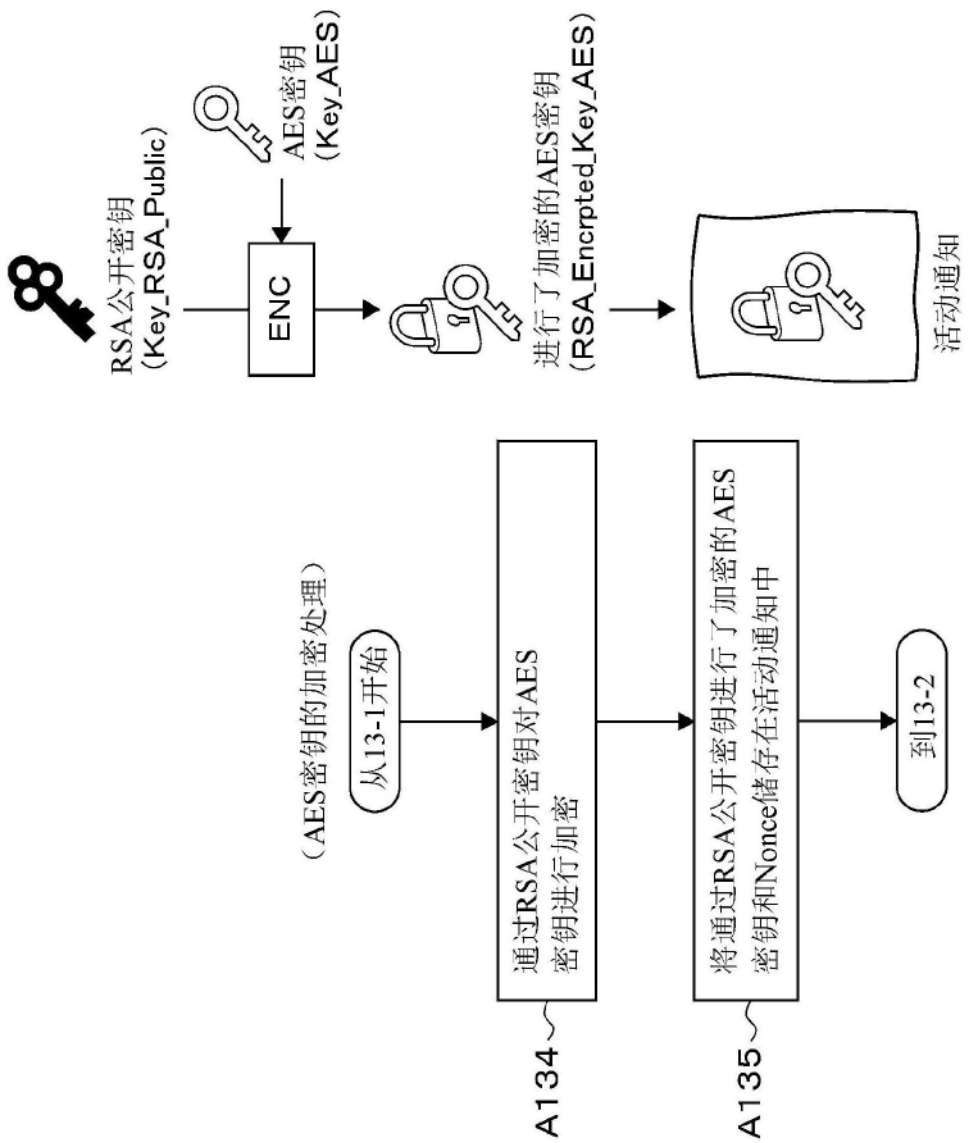

RSA公开密钥
(Key_RSA_Public)
AES密钥
(Key_AES)
ENC
进行了加密的AES密钥
(RSA_Encrpted_Key_AES)
活动通知
（AES密钥的加密处理）
从13-1开始
通过RSA公开密钥对AES
密钥进行加密
A134
将通过RSA公开密钥进行了加密的AES
密钥和Nonce储存在活动通知中
A135
到13-2

图120

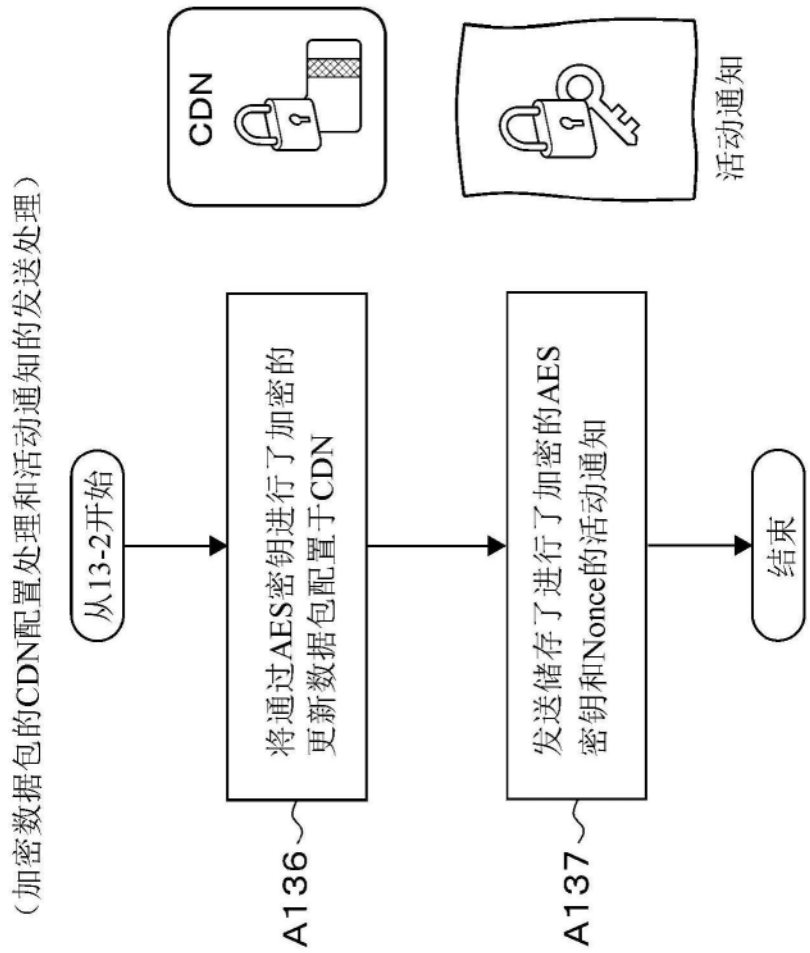

（加密数据包的CDN配置处理和活动通知的发送处理）
从13-2开始
将通过AES密钥进行了加密的更新数据包配置于CDN
A136
发送储存了进行了加密的AES密钥和Nonce的活动通知
A137
结束
CDN
活动通知

图121

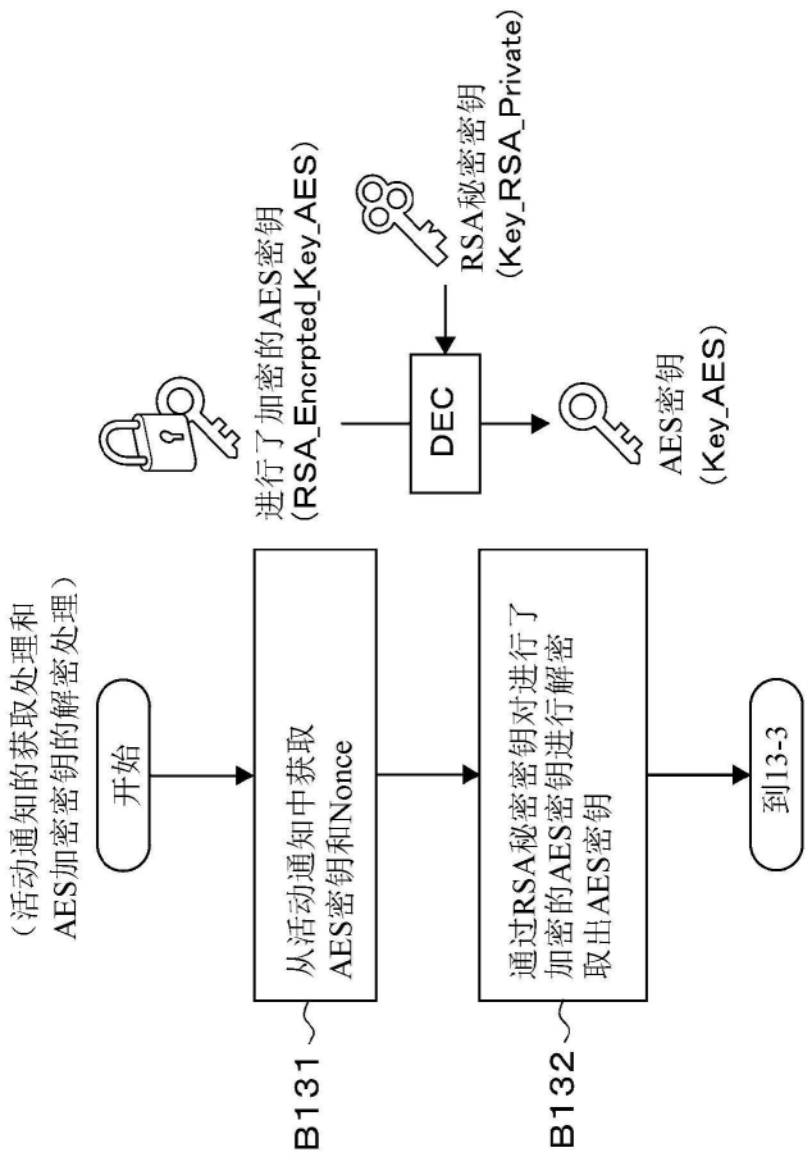

（活动通知的获取处理和
AES加密密钥的解密处理）
开始
从活动通知中获取
AES密钥和Nonce
B131
通过RSA秘密密钥对进行了
加密的AES密钥进行解密
取出AES密钥
B132
到13-3
进行了加密的AES密钥
(RSA_Encrpted_Key_AES)
RSA秘密密钥
(Key_RSA_Private)
DEC
AES密钥
(Key_AES)

图122

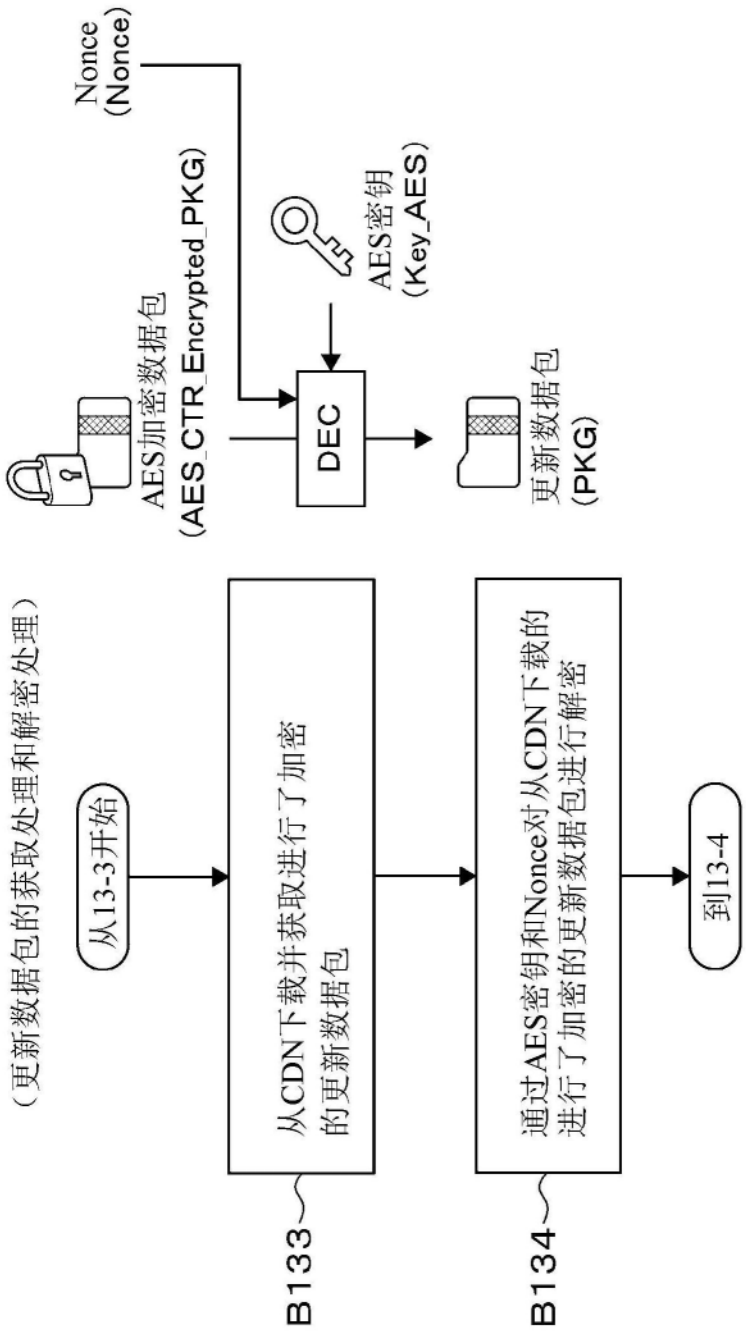

Nonce
(Nonce)
AES加密数据包
(AES_CTR_Encrypted_PKG)
AES密钥
(Key_AES)
DEC
更新数据包
(PKG)
（更新数据包的获取处理和解密处理）
从13-3开始
从CDN下载并获取进行了加密的更新数据包
通过AES密钥和Nonce对从CDN下载的进行了加密的更新数据包进行解密
到13-4
B133
B134

图123

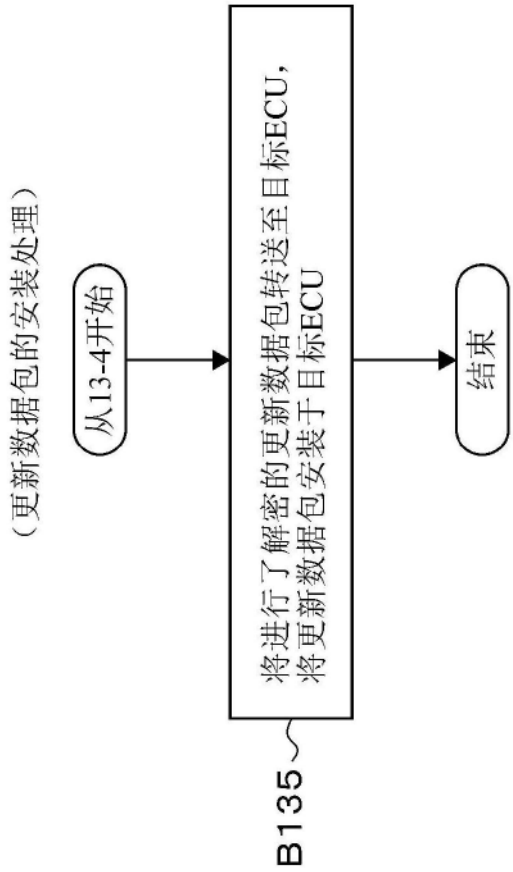

（更新数据包的安装处理）
从13-4开始
将进行了解密的更新数据包转送至目标ECU，
将更新数据包安装于目标ECU
结束
B135

图124

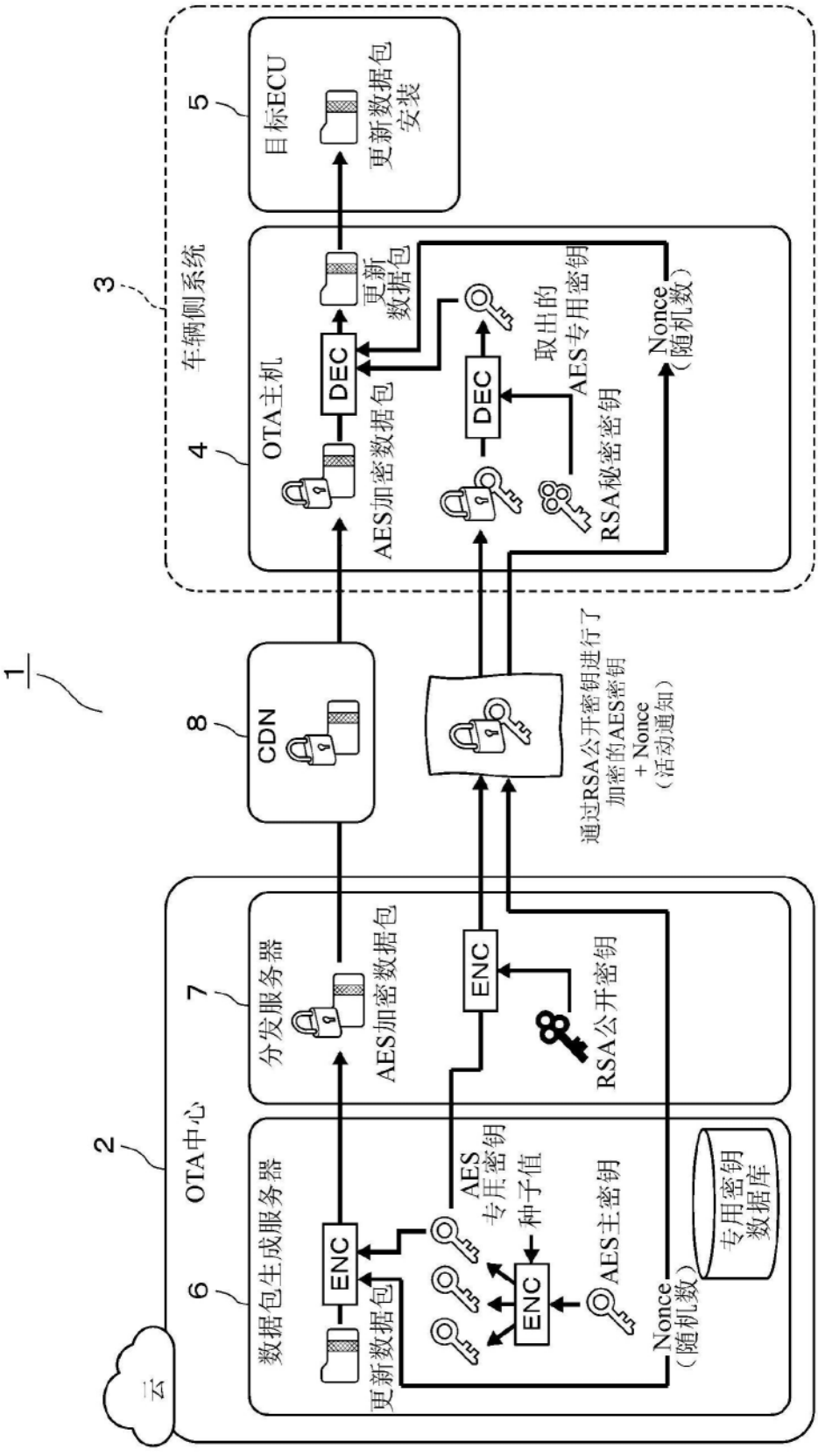

1
2
OTA中心
6
数据包生成服务器
更新数据包
ENC
AES
专用密钥
种子值
ENC
AES主密钥
Nonce
（随机数）
专用密钥
数据库
云
7
分发服务器
AES加密数据包
ENC
RSA公开密钥
8
CDN
通过RSA公开密钥进行了
加密的AES密钥
+ Nonce
（活动通知）
3
车辆侧系统
4
OTA主机
AES加密数据包
DEC
更新
数据包
DEC
取出的
AES专用密钥
RSA秘密密钥
Nonce
（随机数）
5
目标ECU
更新数据包
安装

图125

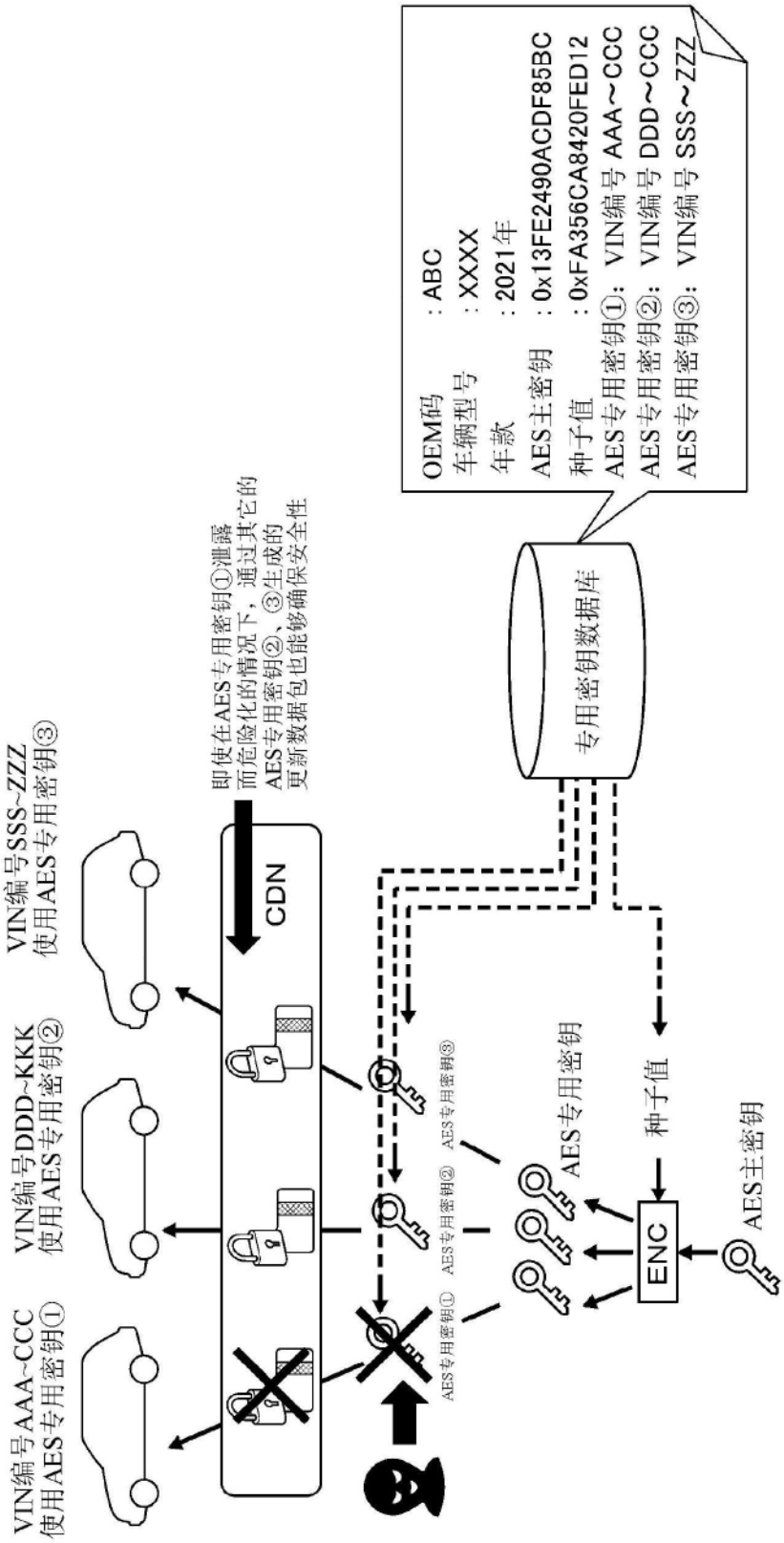

VIN编号AAA~CCC
使用AES专用密钥①
VIN编号DDD~KKK
使用AES专用密钥②
VIN编号SSS~ZZZ
使用AES专用密钥③
即使在AES专用密钥①泄露
而危险化的情况下，通过其它的
AES专用密钥②、③生成的
更新数据包也能够确保安全性
CDN
AES专用密钥①
AES专用密钥②
AES专用密钥③
AES专用密钥
种子值
ENC
AES主密钥
专用密钥数据库
OEM码 : ABC
车辆型号 : XXXX
年款 : 2021年
AES主密钥 : 0x13FE2490ACDF85BC
种子值 : 0xFA356CA8420FED12
AES专用密钥①：VIN编号 AAA~CCC
AES专用密钥②：VIN编号 DDD~CCC
AES专用密钥③：VIN编号 SSS~ZZZ

图126

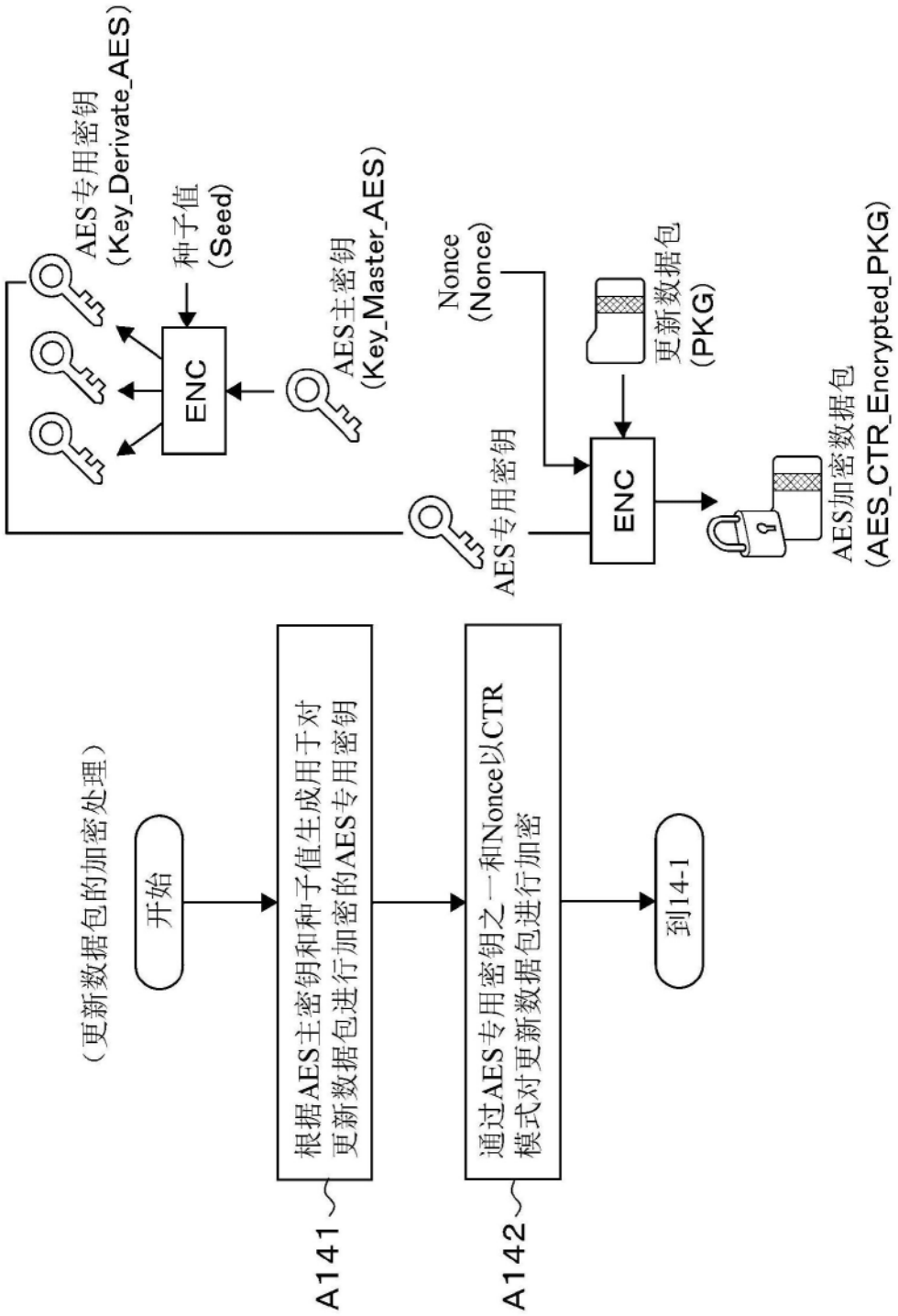

（更新数据包的加密处理）
开始
根据AES主密钥和种子值生成用于对更新数据包进行加密的AES专用密钥
A141
通过AES专用密钥之一和Nonce以CTR模式对更新数据包进行加密
A142
到14-1
AES专用密钥 (Key_Derivate_AES)
种子值 (Seed)
ENC
AES主密钥 (Key_Master_AES)
Nonce (Nonce)
更新数据包 (PKG)
AES专用密钥
ENC
AES加密数据包 (AES_CTR_Encrypted_PKG)

图127

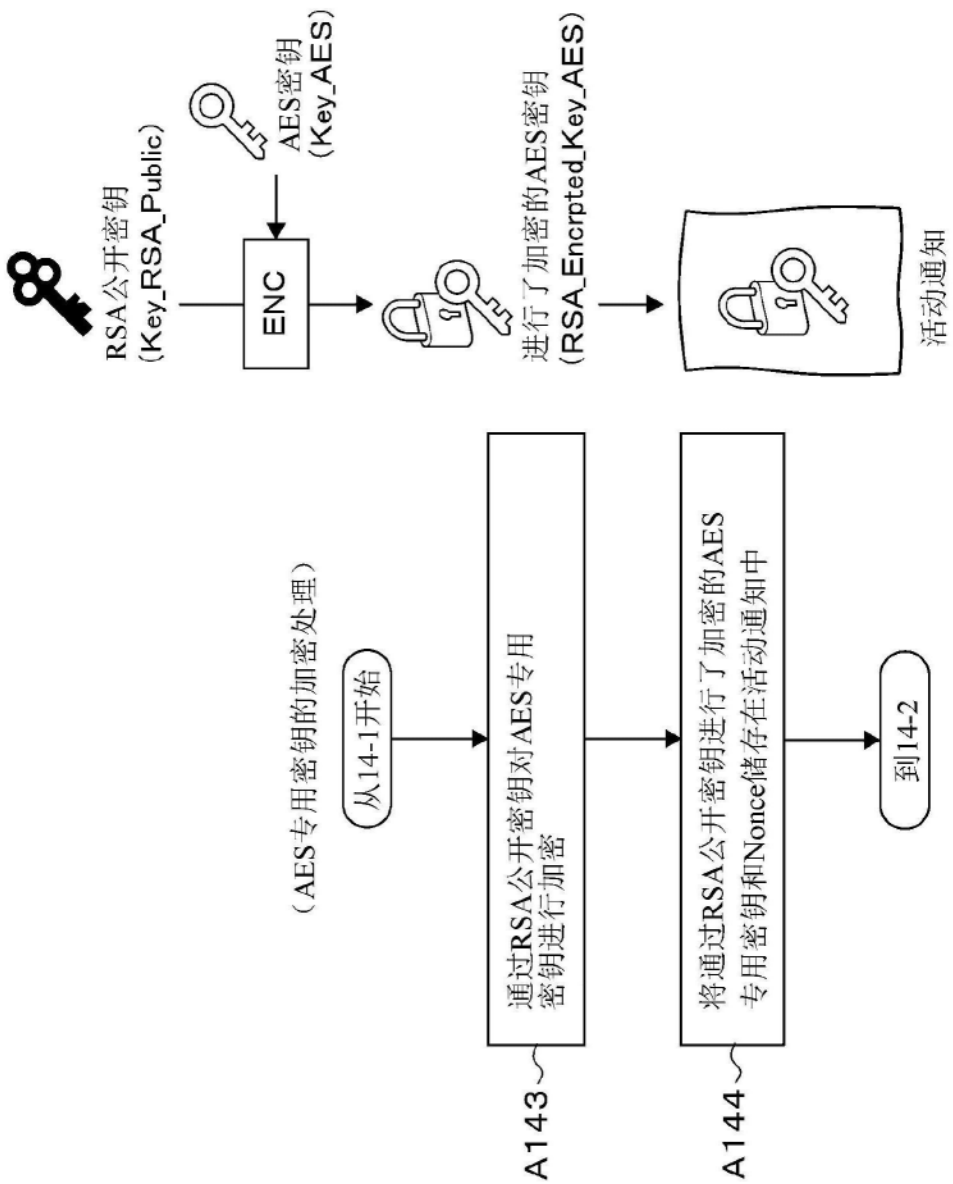

RSA公开密钥
(Key_RSA_Public)
AES密钥
(Key_AES)
ENC
进行了加密的AES密钥
(RSA_Encrpted_Key_AES)
活动通知
（AES专用密钥的加密处理）
从14-1开始
通过RSA公开密钥对AES专用
密钥进行加密
将通过RSA公开密钥进行了加密的AES
专用密钥和Nonce储存在活动通知中
到14-2
A143
A144

图128

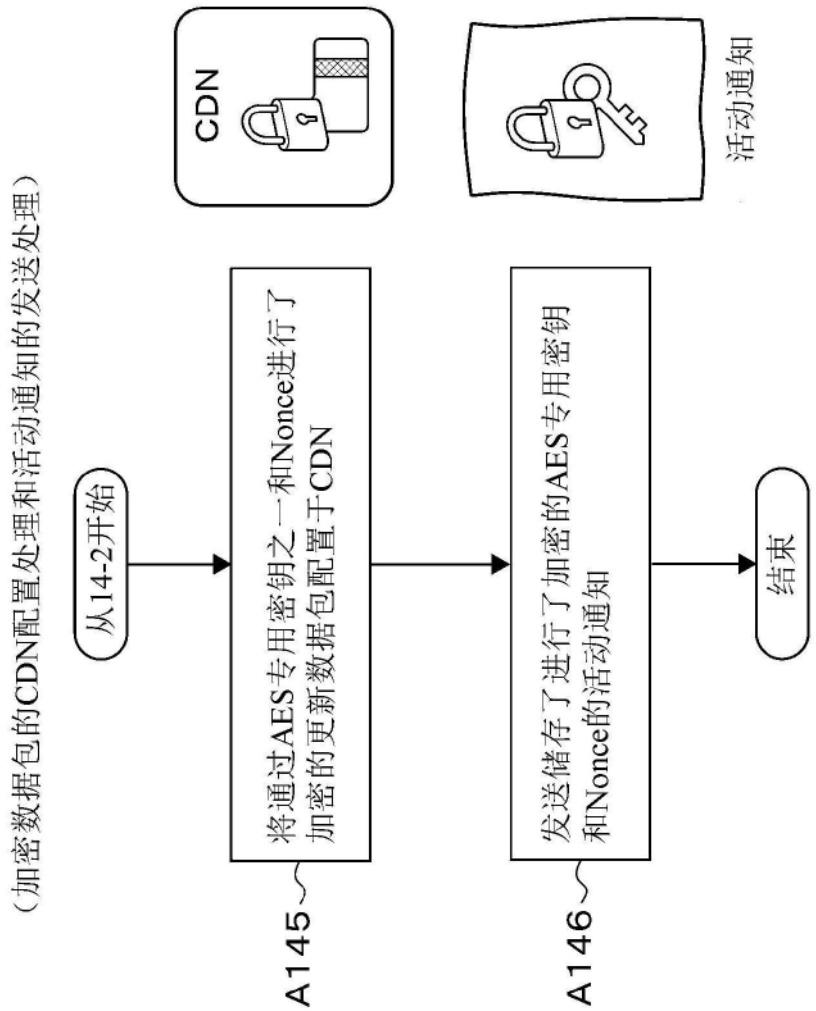

（加密数据包的CDN配置处理和活动通知的发送处理）
从14-2开始
将通过AES专用密钥之一和Nonce进行了加密的更新数据包配置于CDN
A145
发送储存了进行了加密的AES专用密钥和Nonce的活动通知
A146
结束
CDN
活动通知

图129

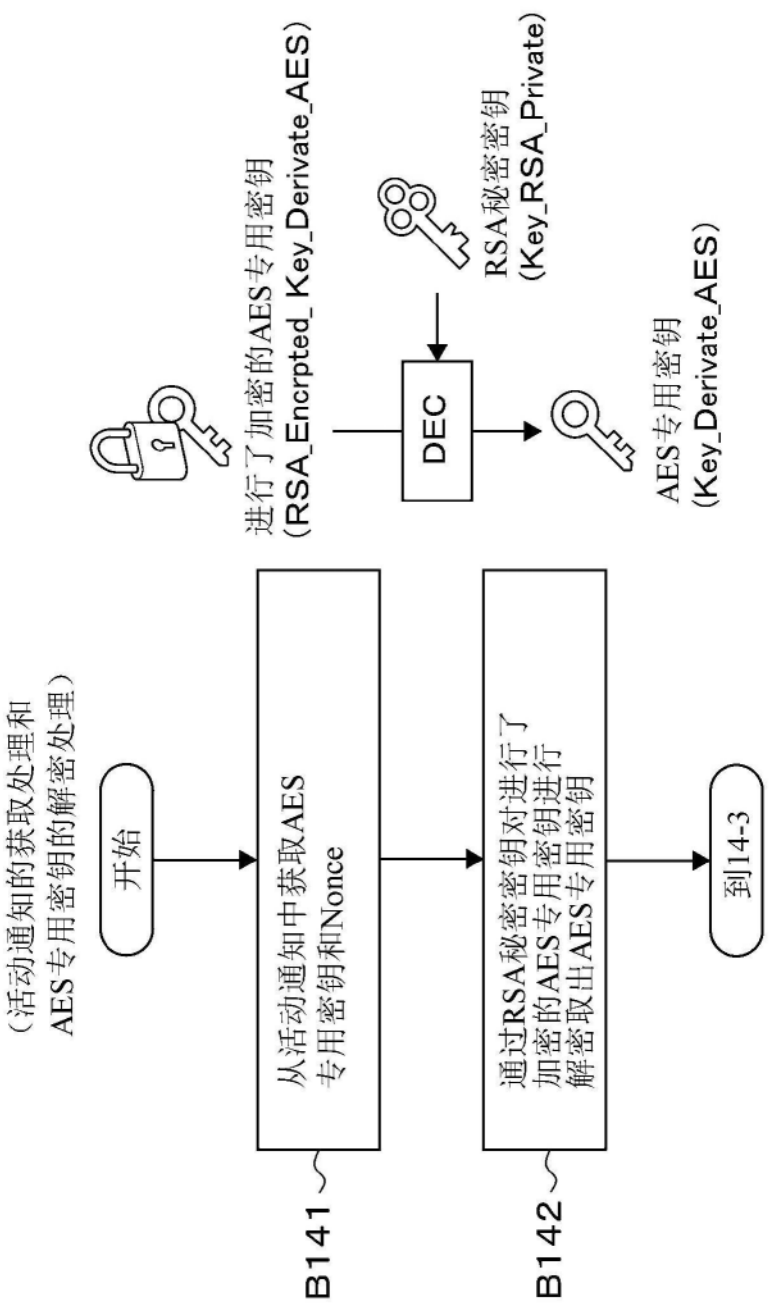

（活动通知的获取处理和
AES专用密钥的解密处理）
开始
从活动通知中获取AES
专用密钥和Nonce
B141
通过RSA秘密密钥对进行了
加密的AES专用密钥进行
解密取出AES专用密钥
B142
到14-3
进行了加密的AES专用密钥
(RSA_Encrpted_ Key_Derivate_AES)
DEC
RSA秘密密钥
(Key_RSA_Private)
AES专用密钥
(Key_Derivate_AES)

图130

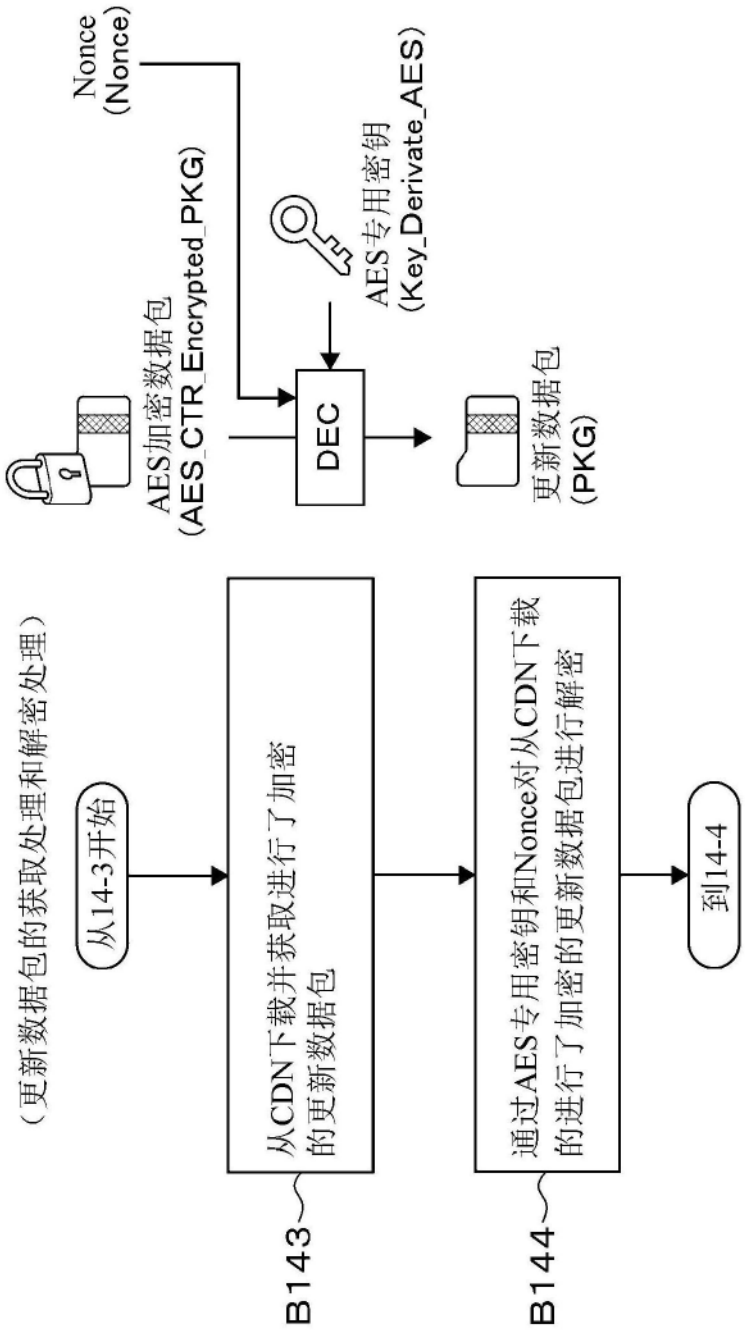

（更新数据包的获取处理和解密处理）
从14-3开始
从CDN下载并获取进行了加密的更新数据包
B143
通过AES专用密钥和Nonce对从CDN下载的进行了加密的更新数据包进行解密
B144
到14-4
AES加密数据包
(AES_CTR_Encrypted_PKG)
Nonce
(Nonce)
AES专用密钥
(Key_Derivate_AES)
DEC
更新数据包
(PKG)

图131

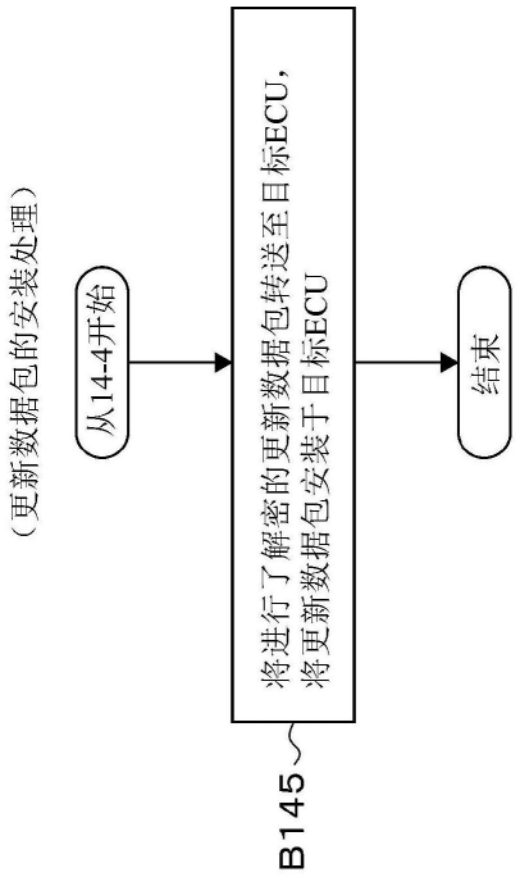

（更新数据包的安装处理）
从14-4开始
将进行了解密的更新数据包转送至目标ECU，
将更新数据包安装于目标ECU
结束
B145

图132

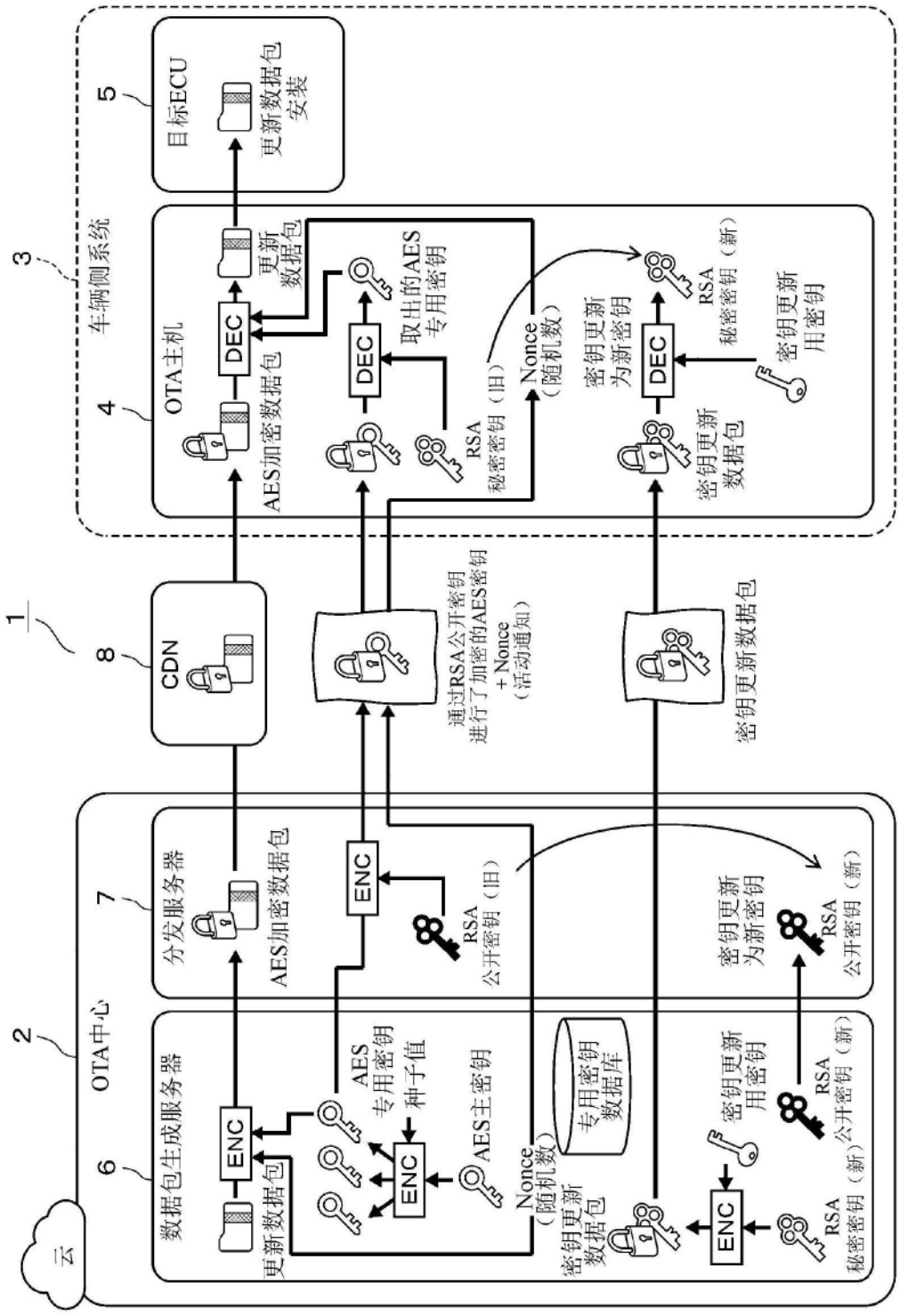

1
2
OTA中心
6
数据包生成服务器
ENC
更新数据包
AES
专用密钥
种子值
ENC
AES主密钥
Nonce
（随机数）
专用密钥
数据库
密钥更新
数据包
ENC
密钥更新
用密钥
RSA
秘密密钥（新）
RSA
公开密钥（新）
云
7
分发服务器
AES加密数据包
ENC
RSA
公开密钥（旧）
密钥更新
为新密钥
RSA
公开密钥（新）
8
CDN
通过RSA公开密钥
进行了加密的AES密钥
+ Nonce
（活动通知）
密钥更新数据包
3
车辆侧系统
4
OTA主机
AES加密数据包
DEC
更新
数据包
DEC
取出的AES
专用密钥
RSA
秘密密钥（旧）
Nonce
（随机数）
密钥更新
为新密钥
DEC
RSA
秘密密钥（新）
密钥更新数据包
密钥更新
用密钥
5
目标ECU
更新数据包
安装

图133

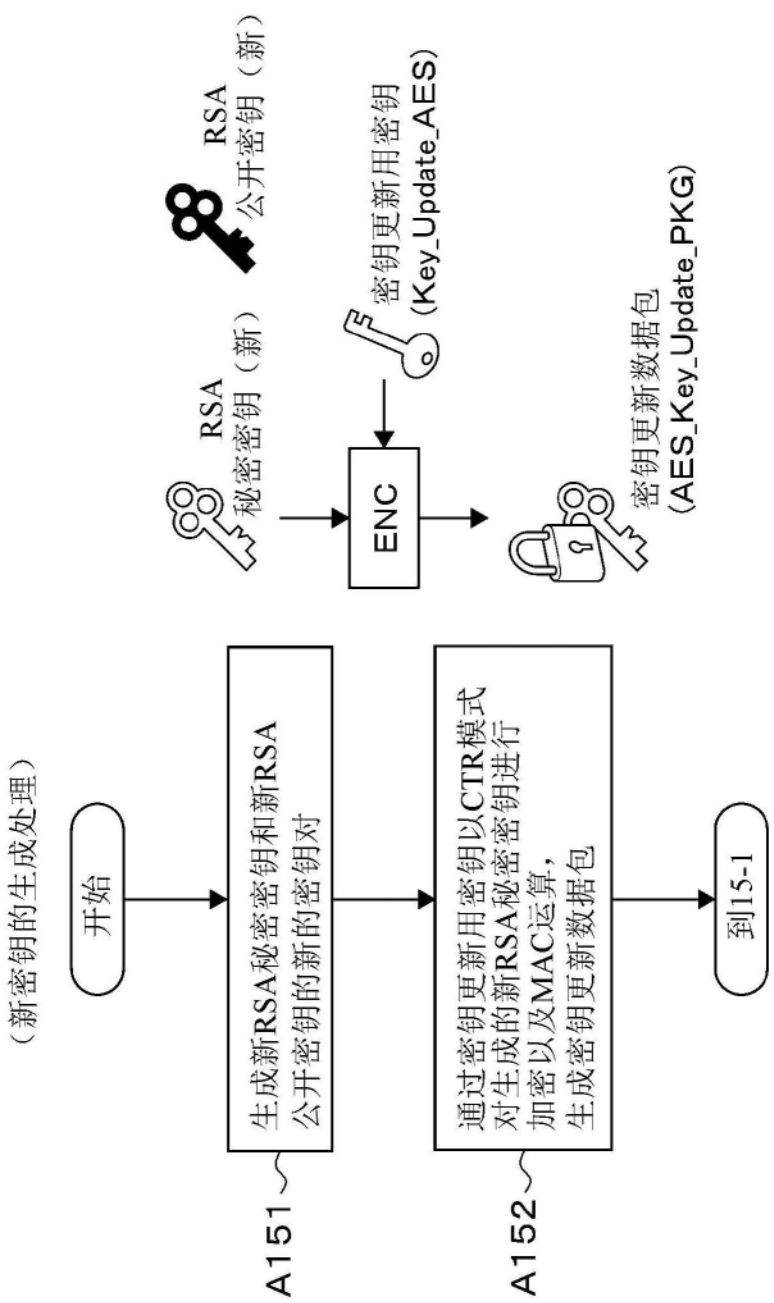

（新密钥的生成处理）
开始
生成新RSA秘密密钥和新RSA公开密钥的新的密钥对
A151
通过密钥更新用密钥以CTR模式对生成的新RSA秘密密钥进行加密以及MAC运算，生成密钥更新数据包
A152
到15-1
RSA 秘密密钥（新）
RSA 公开密钥（新）
密钥更新用密钥 (Key_Update_AES)
ENC
密钥更新数据包 (AES_Key_Update_PKG)

图134

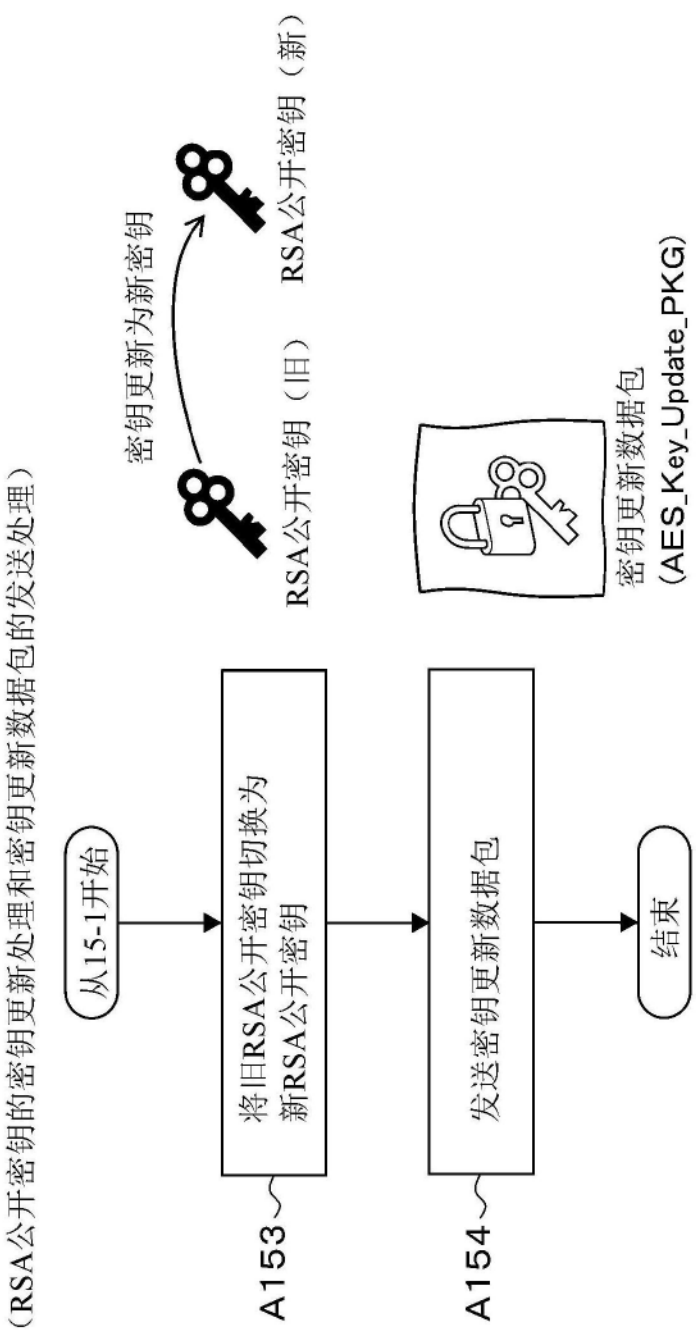

(RSA公开密钥的密钥更新处理和密钥更新数据包的发送处理)
从15-1开始
将旧RSA公开密钥切换为新RSA公开密钥
A153
发送密钥更新数据包
A154
结束
密钥更新为新密钥
RSA公开密钥（旧）
RSA公开密钥（新）
密钥更新数据包
(AES_Key_Update_PKG)

图135

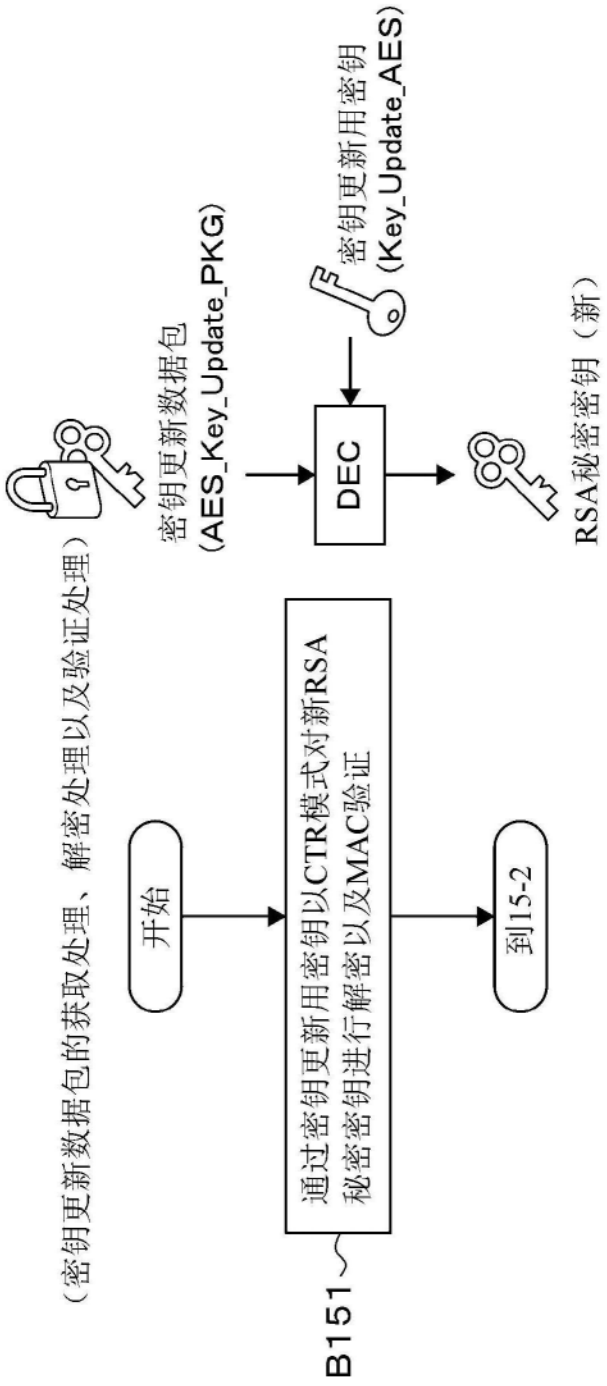

（密钥更新数据包的获取处理、解密处理以及验证处理）
密钥更新数据包
(AES_Key_Update_PKG)
密钥更新用密钥
(Key_Update_AES)
DEC
RSA秘密密钥（新）
开始
通过密钥更新用密钥以CTR模式对新RSA
秘密密钥进行解密以及MAC验证
到15-2
B151

图136

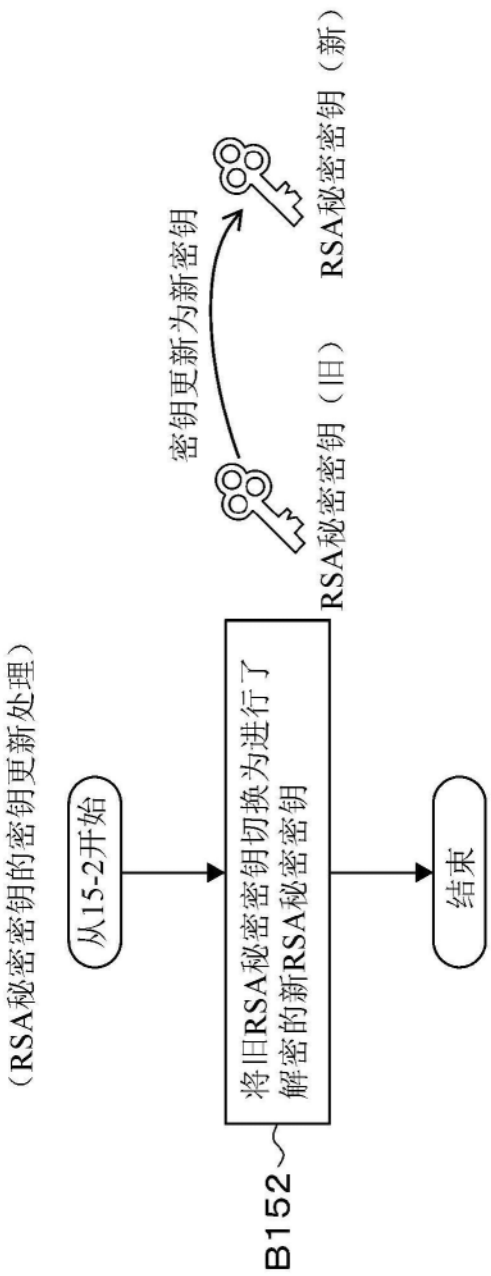

（RSA秘密密钥的密钥更新处理）
从15-2开始
将旧RSA秘密密钥切换为进行了解密的新RSA秘密密钥
B152
结束
密钥更新为新密钥
RSA秘密密钥（旧）
RSA秘密密钥（新）

图137

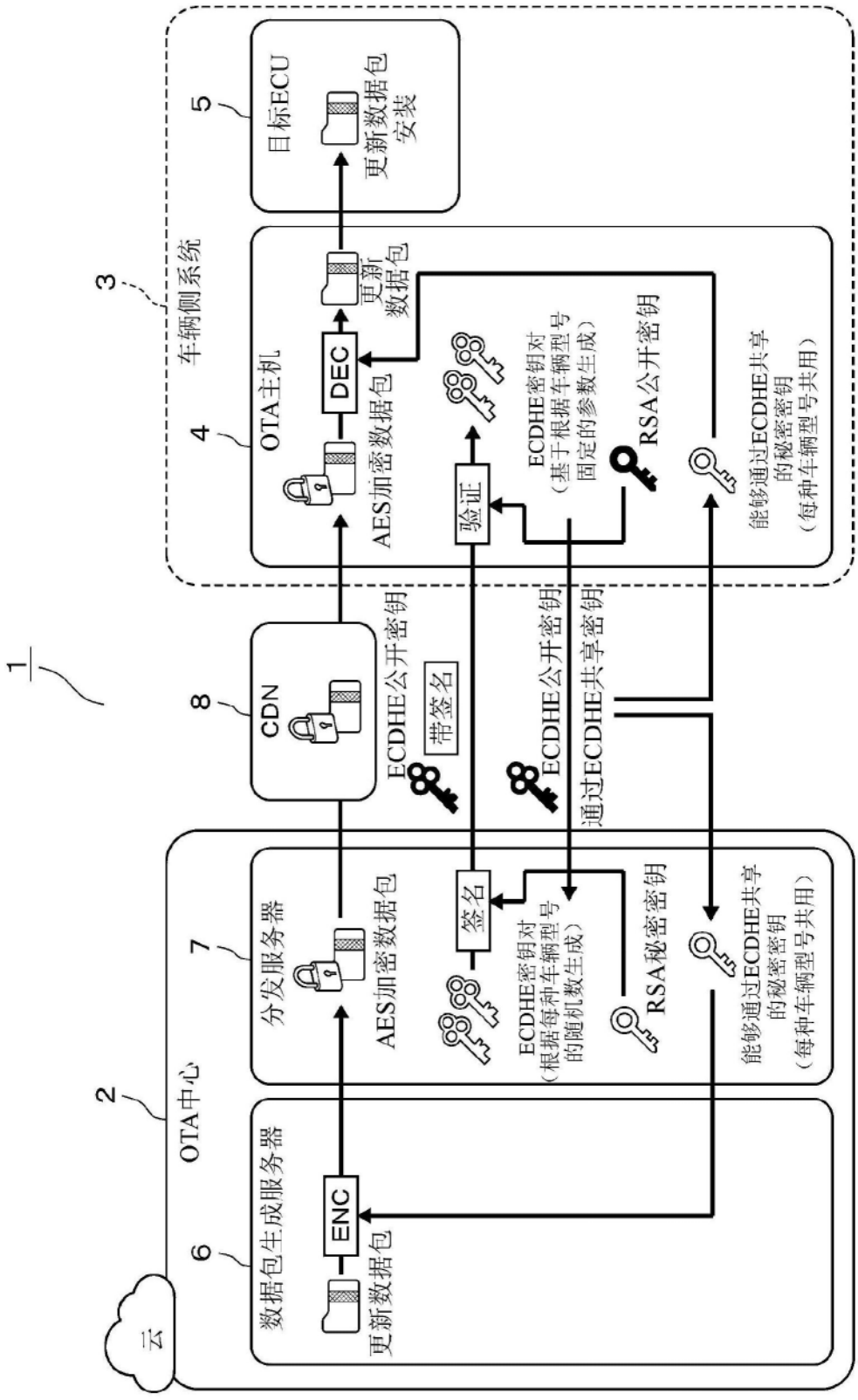

1
2
OTA中心
云
6
数据包生成服务器
更新数据包
ENC
7
分发服务器
AES加密数据包
签名
ECDHE密钥对
（根据每种车辆型号
的随机数生成）
RSA秘密密钥
能够通过ECDHE共享
的秘密密钥
（每种车辆型号共用）
8
CDN
ECDHE公开密钥
带签名
ECDHE公开密钥
通过ECDHE共享密钥
3
车辆侧系统
4
OTA主机
AES加密数据包
DEC
更新
数据包
验证
ECDHE密钥对
（基于根据车辆型号
固定的参数生成）
RSA公开密钥
能够通过ECDHE共享
的秘密密钥
（每种车辆型号共用）
5
目标ECU
更新数据包
安装

图138

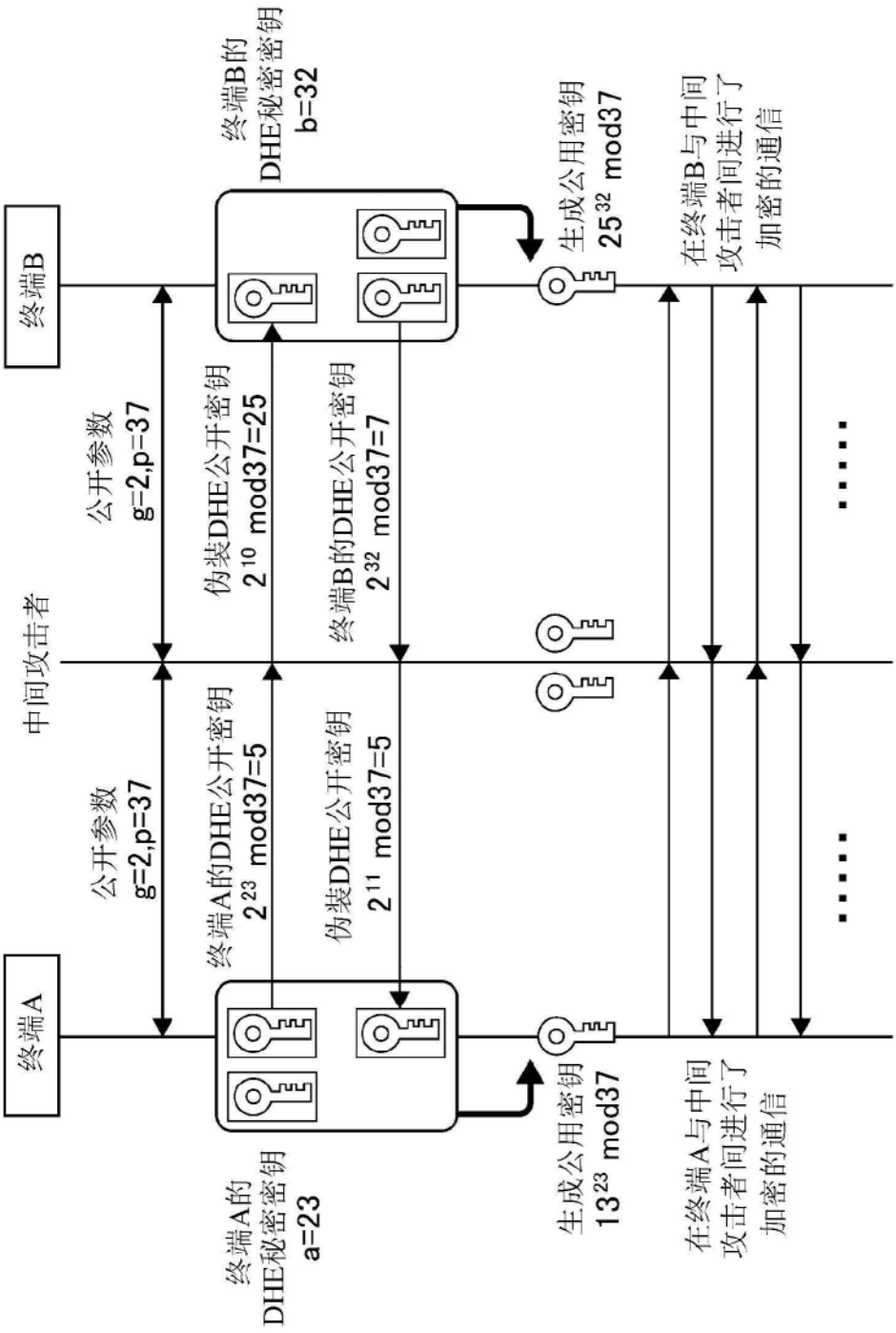

终端A
终端B
中间攻击者
公开参数
g=2,p=37
公开参数
g=2,p=37
终端A的DHE秘密密钥
a=23
终端B的DHE秘密密钥
b=32
终端A的DHE公开密钥
2^{23} mod37=5
伪装DHE公开密钥
2^{11} mod37=5
伪装DHE公开密钥
2^{10} mod37=25
终端B的DHE公开密钥
2^{32} mod37=7
生成公用密钥
13^{23} mod37
生成公用密钥
25^{32} mod37
在终端A与中间攻击者间进行了加密的通信
在终端B与中间攻击者间进行了加密的通信

图139

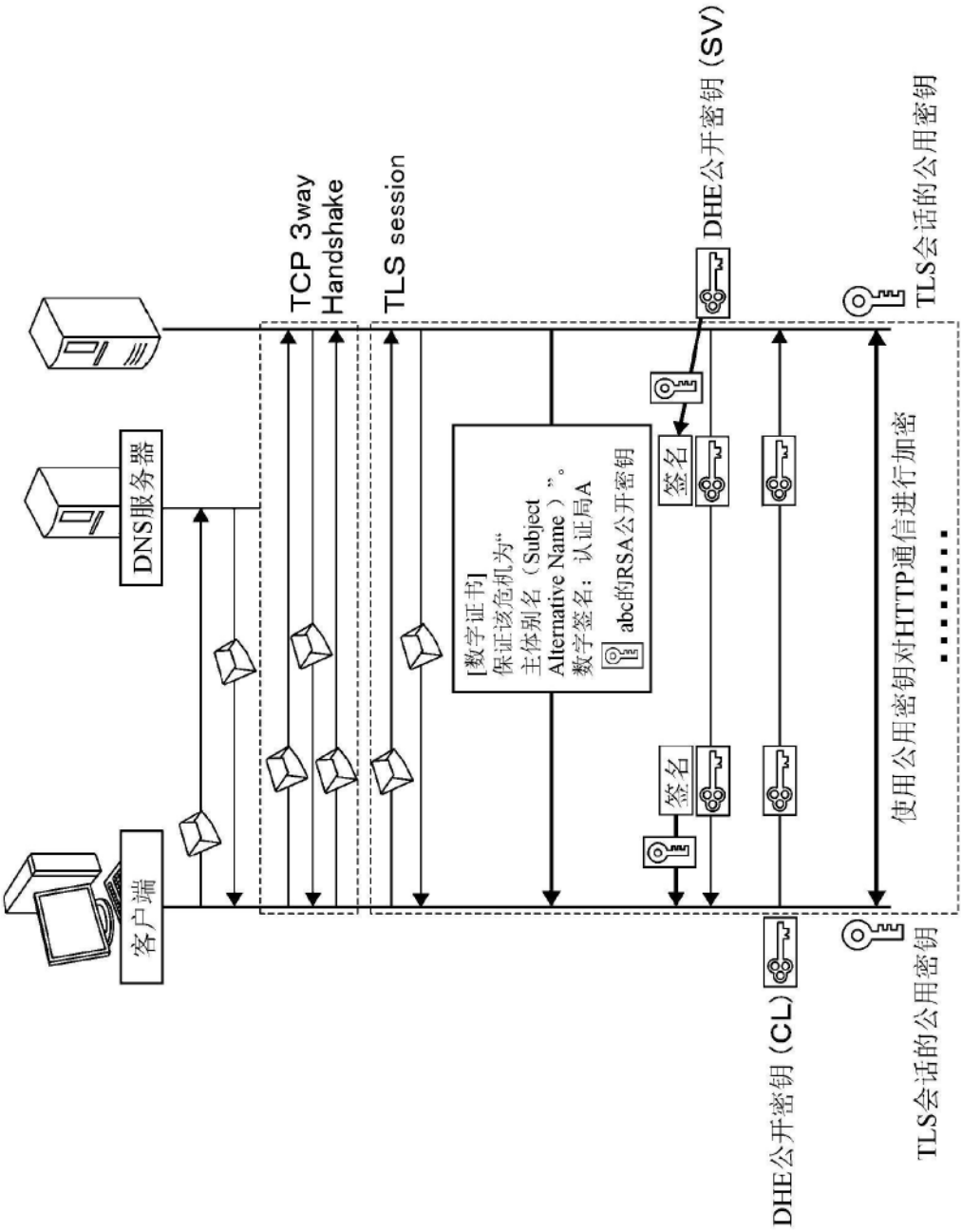

客户端
DNS服务器
TCP 3way Handshake
TLS session
[数字证书]
保证该危机为“
主体别名（Subject Alternative Name）”。
数字签名：认证局A
abc的RSA公开密钥
签名
签名
DHE公开密钥（SV）
TLS会话的公用密钥
使用公用密钥对HTTP通信进行加密
DHE公开密钥（CL）
TLS会话的公用密钥

图140

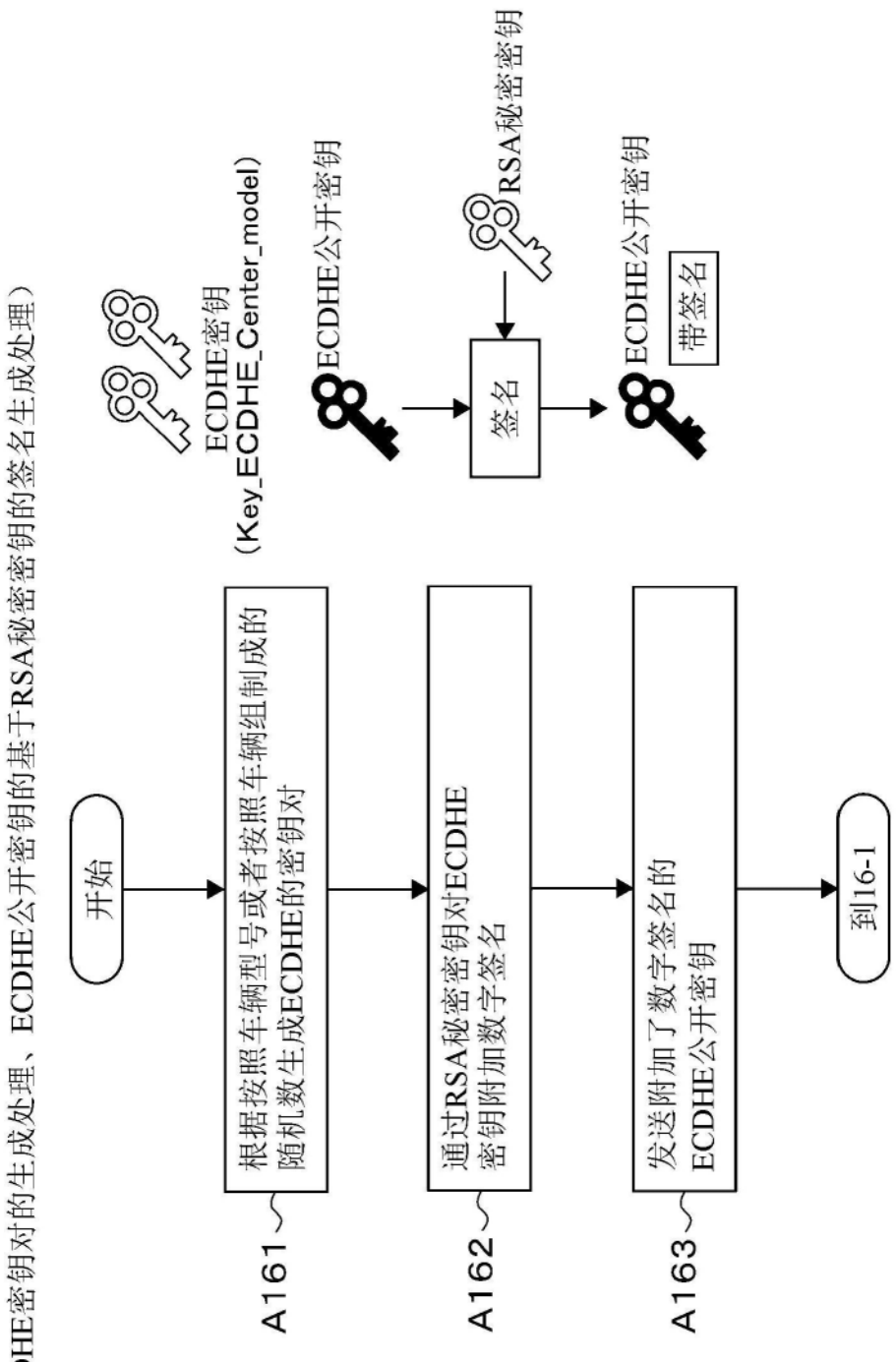

（ECDHE密钥对的生成处理、ECDHE公开密钥的基于RSA秘密密钥的签名生成处理）
开始
根据按照车辆型号或者按照车辆组制成的随机数生成ECDHE的密钥对
A161
通过RSA秘密密钥对ECDHE密钥附加数字签名
A162
发送附加了数字签名的ECDHE公开密钥
A163
到16-1
ECDHE密钥
(Key_ECDHE_Center_model)
ECDHE公开密钥
签名
RSA秘密密钥
ECDHE公开密钥
带签名

图141

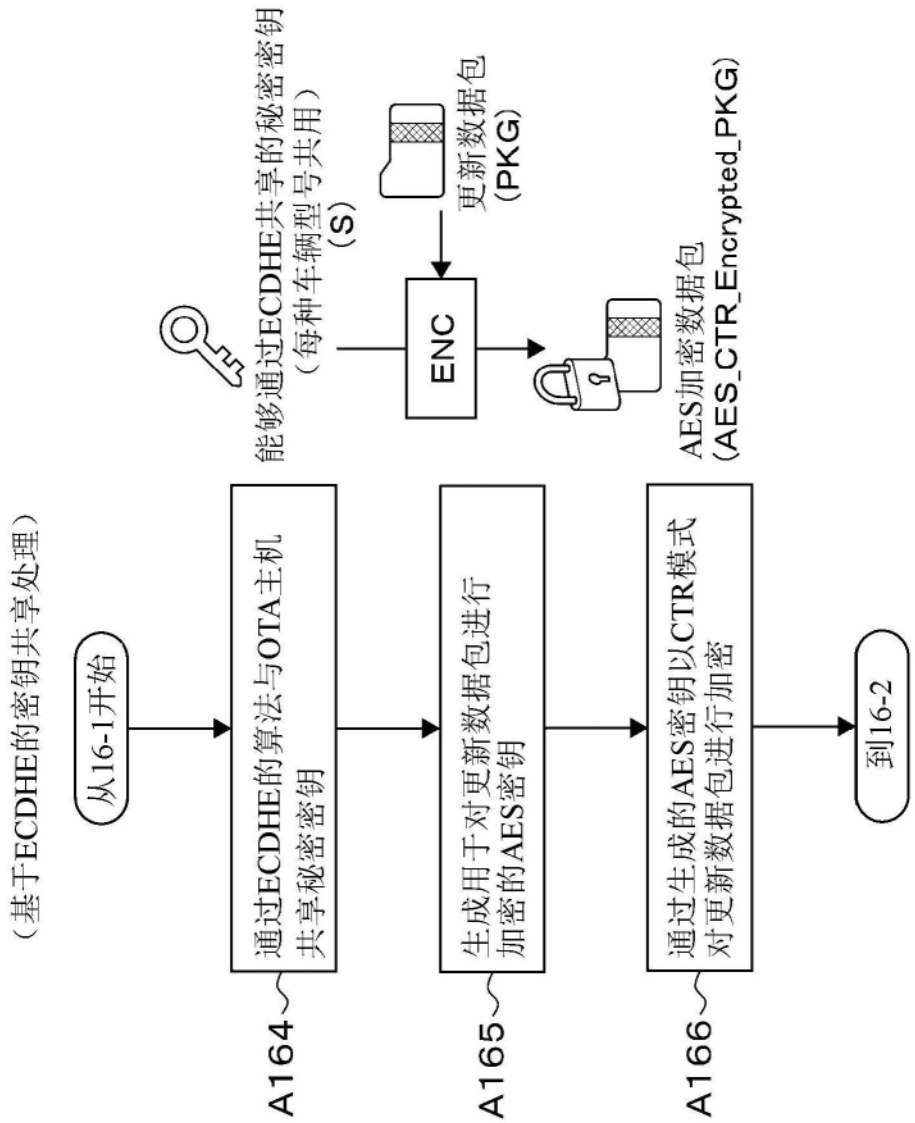

（基于ECDHE的密钥共享处理）
从16-1开始
通过ECDHE的算法与OTA主机
共享秘密密钥
A164
生成用于对更新数据包进行
加密的AES密钥
A165
通过生成的AES密钥以CTR模式
对更新数据包进行加密
A166
到16-2
能够通过ECDHE共享的秘密密钥
（每种车辆型号共用）
(S)
ENC
更新数据包
(PKG)
AES加密数据包
(AES_CTR_Encrypted_PKG)

图142

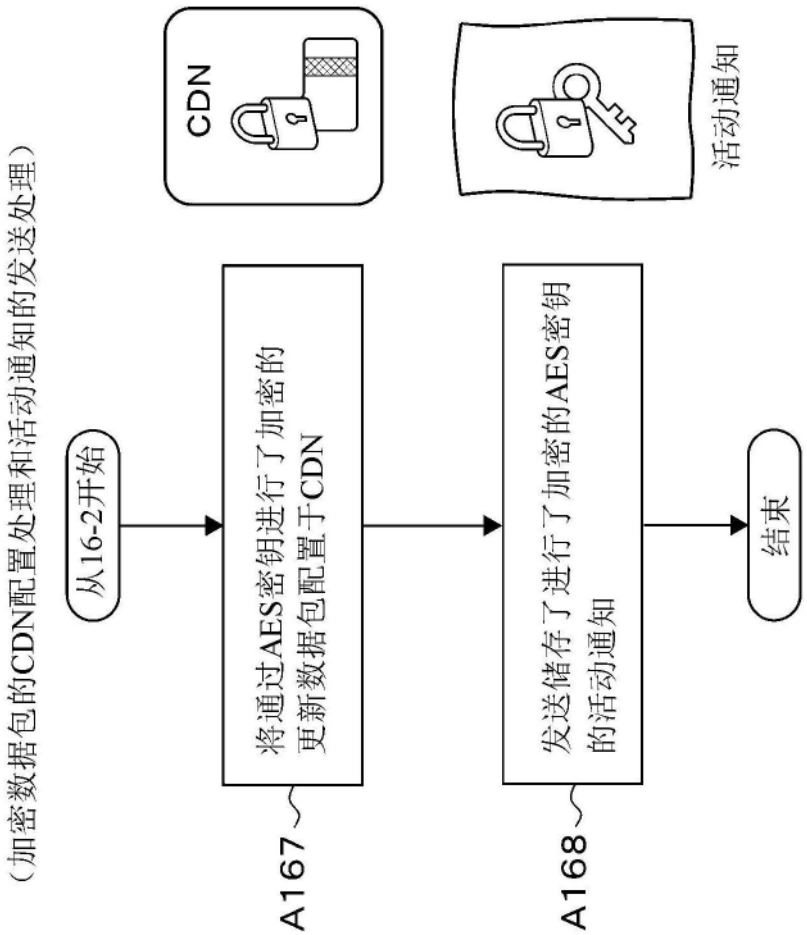

（加密数据包的CDN配置处理和活动通知的发送处理）
从16-2开始
将通过AES密钥进行了加密的更新数据包配置于CDN
A167
发送储存了进行了加密的AES密钥的活动通知
A168
结束
CDN
活动通知

图143

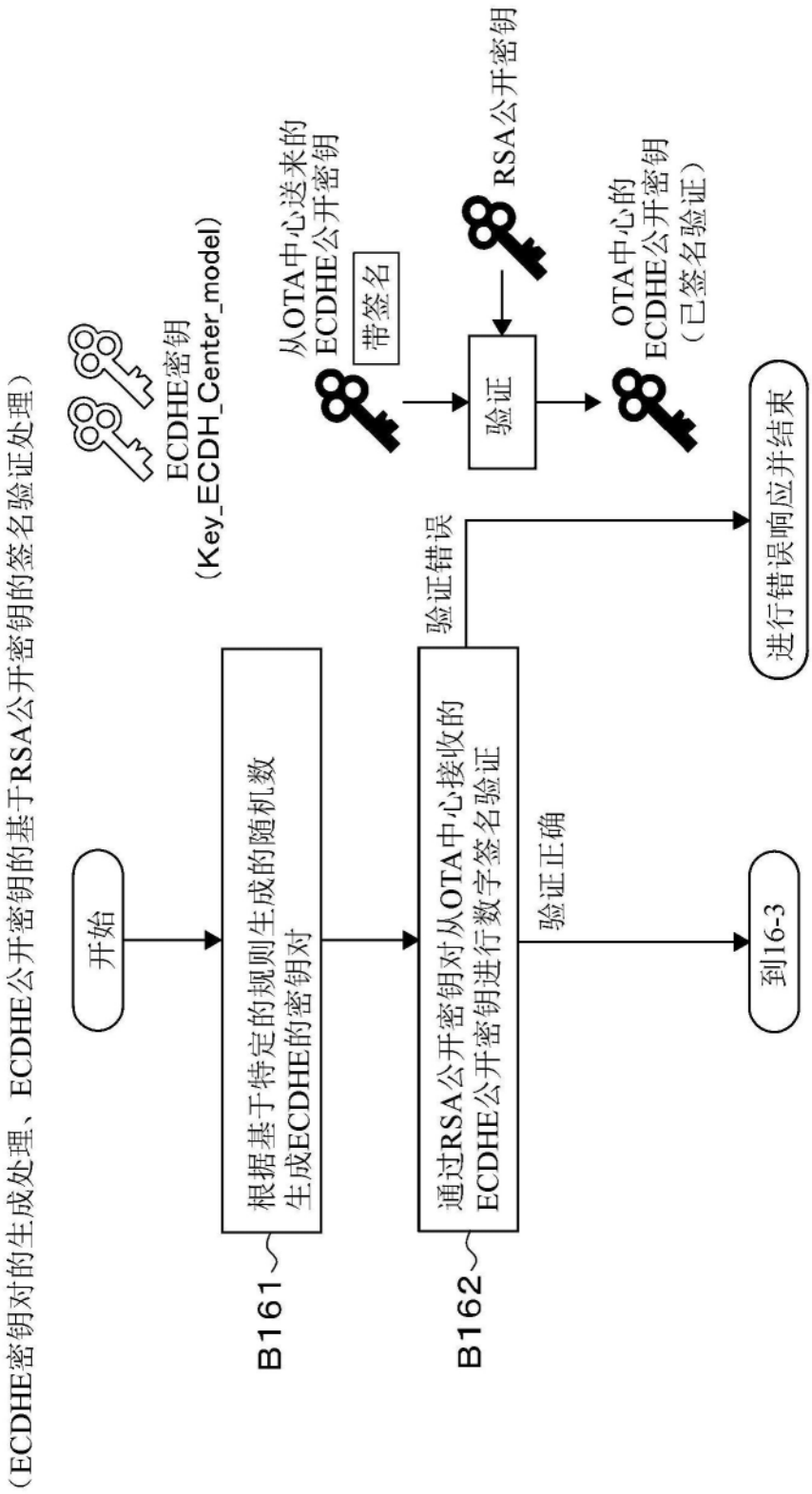

（ECDHE密钥对的生成处理、ECDHE公开密钥的基于RSA公开密钥的签名验证处理）
开始
根据基于特定的规则生成的随机数
生成ECDHE的密钥对
B161
ECDHE密钥
(Key_ECDH_Center_model)
通过RSA公开密钥对从OTA中心接收的
ECDHE公开密钥进行数字签名验证
B162
验证错误
验证正确
到16-3
进行错误响应并结束
从OTA中心送来的
ECDHE公开密钥
带签名
RSA公开密钥
验证
OTA中心的
ECDHE公开密钥
（已签名验证）

图144

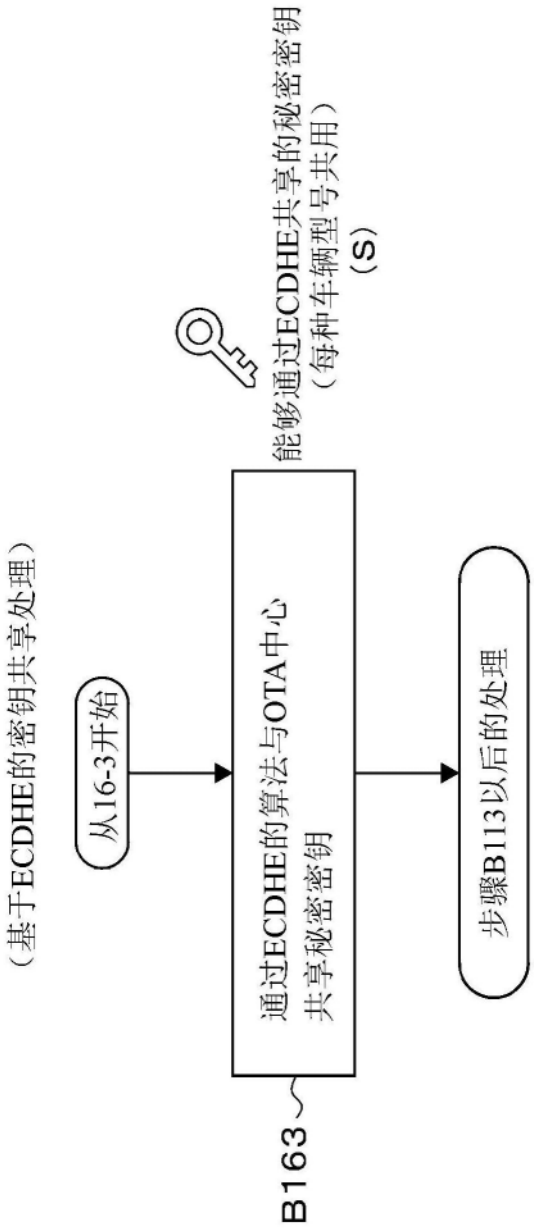

（基于ECDHE的密钥共享处理）
从16-3开始
通过ECDHE的算法与OTA中心
共享秘密密钥
B163
能够通过ECDHE共享的秘密密钥
（每种车辆型号共用）
(S)
步骤B113以后的处理

图145

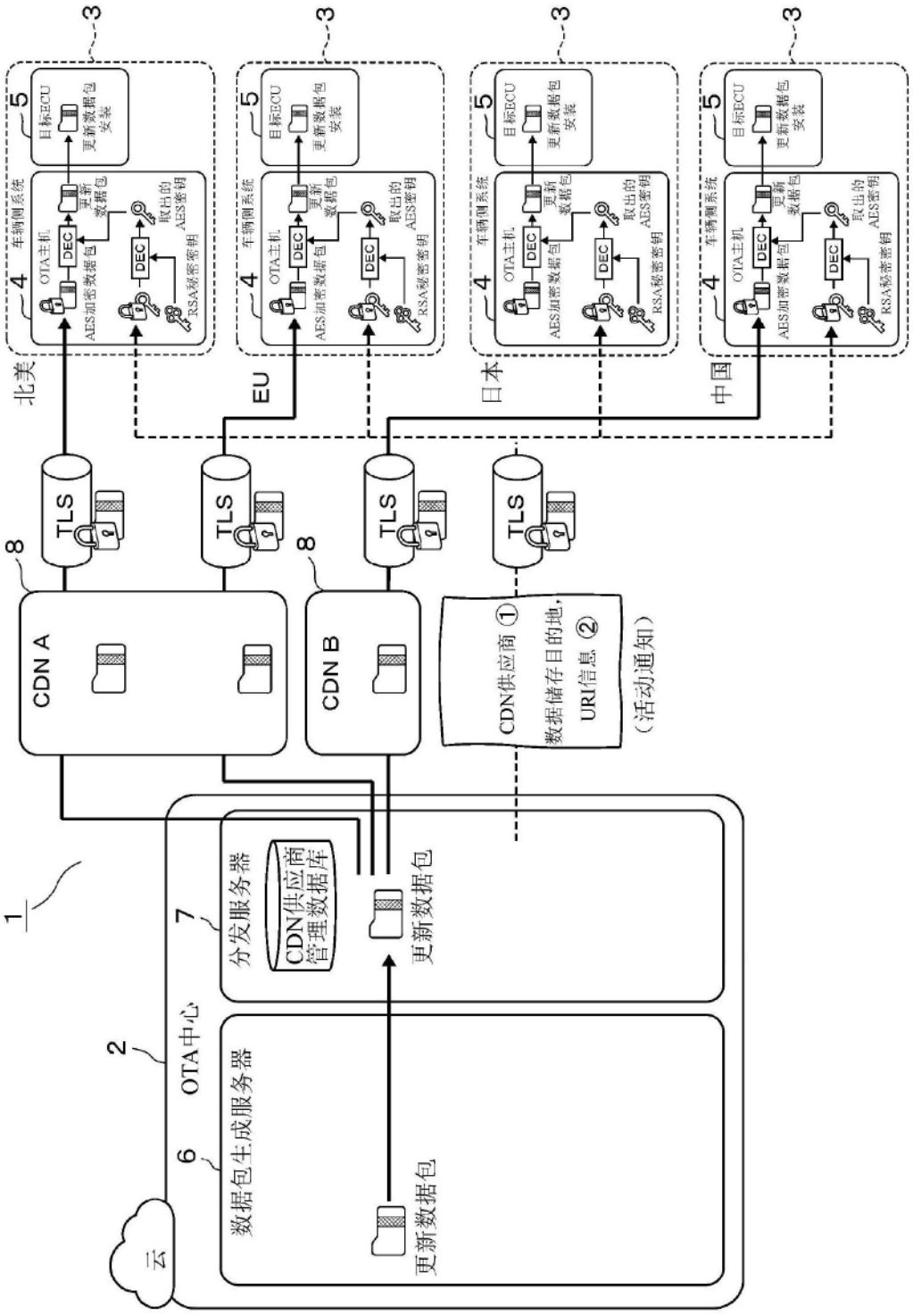

北美
EU
日本
中国
车辆侧系统
OTA主机
目标ECU
更新数据包安装
AES加密数据包
更新数据包
RSA秘密密钥
取出的AES密钥
DEC
TLS
CDN A
CDN B
CDN供应商 ①
数据储存目的地，
URI信息 ②
（活动通知）
1
2
OTA中心
6
数据包生成服务器
云
更新数据包
7
分发服务器
CDN供应商管理数据库
更新数据包

图146

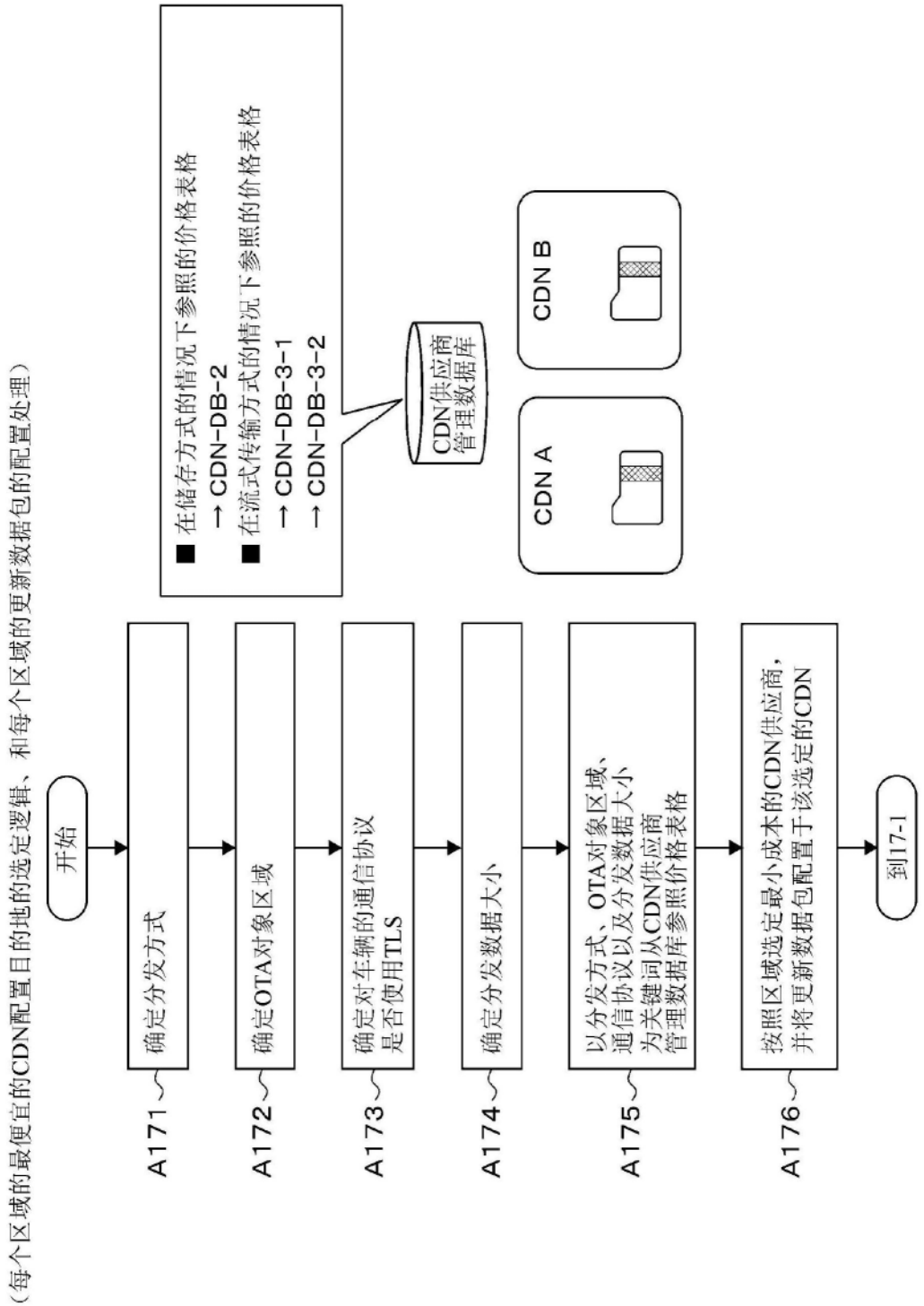

（每个区域的最便宜的CDN配置目的地的选定逻辑、和每个区域的更新数据包的配置处理）
开始
A171
确定分发方式
A172
确定OTA对象区域
A173
确定对车辆的通信协议
是否使用TLS
A174
确定分发数据大小
A175
以分发方式、OTA对象区域、
通信协议以及分发数据大小
为关键词从CDN供应商
管理数据库参照价格表格
A176
按照区域选定最小成本的CDN供应商，
并将更新数据包配置于该选定的CDN
到17-1
■ 在储存方式的情况下参照的价格表格
→ CDN-DB-2
■ 在流式传输方式的情况下参照的价格表格
→ CDN-DB-3-1
→ CDN-DB-3-2
CDN供应商
管理数据库
CDN A
CDN B

图147

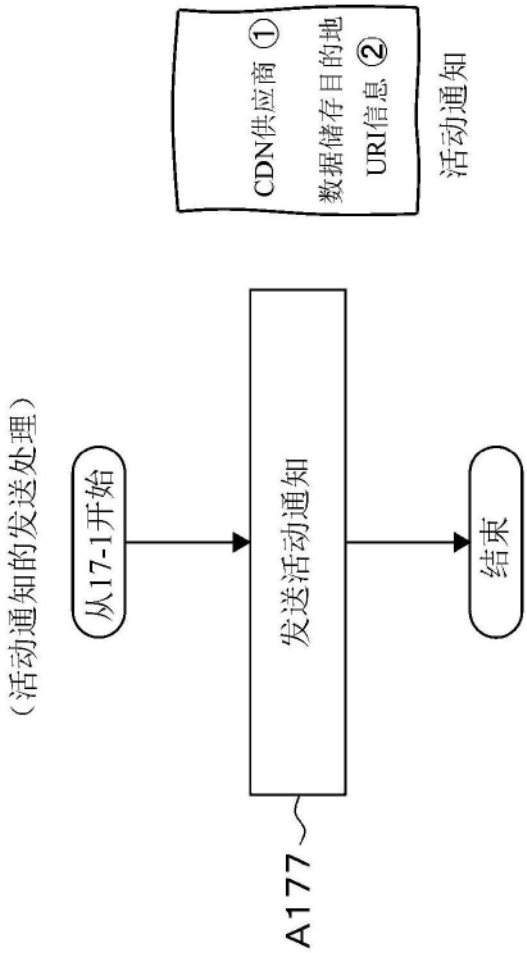

CDN供应商 ①
数据储存目的地
URI信息 ②
活动通知
（活动通知的发送处理）
从17-1开始
发送活动通知
结束
A177

图148

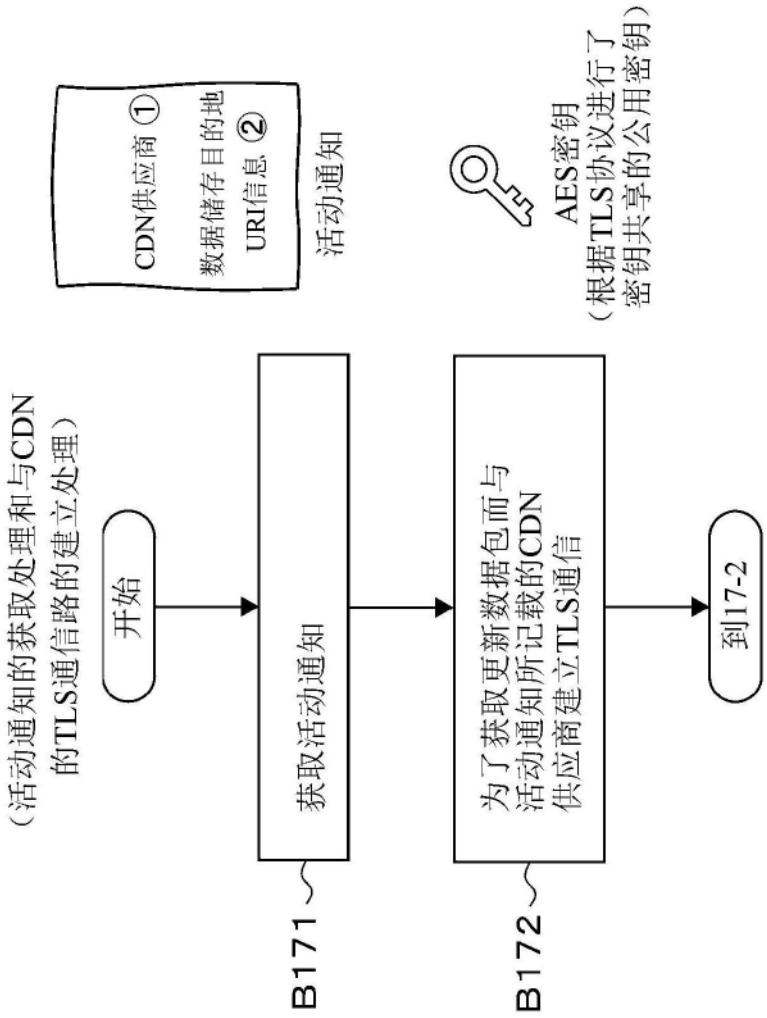

（活动通知的获取处理和与CDN的TLS通信路的建立处理）
开始
获取活动通知
B171
为了获取更新数据包而与活动通知所记载的CDN供应商建立TLS通信
B172
到17-2
CDN供应商 ①
数据储存目的地URI信息 ②
活动通知
AES密钥
（根据TLS协议进行了密钥共享的公用密钥）

图149

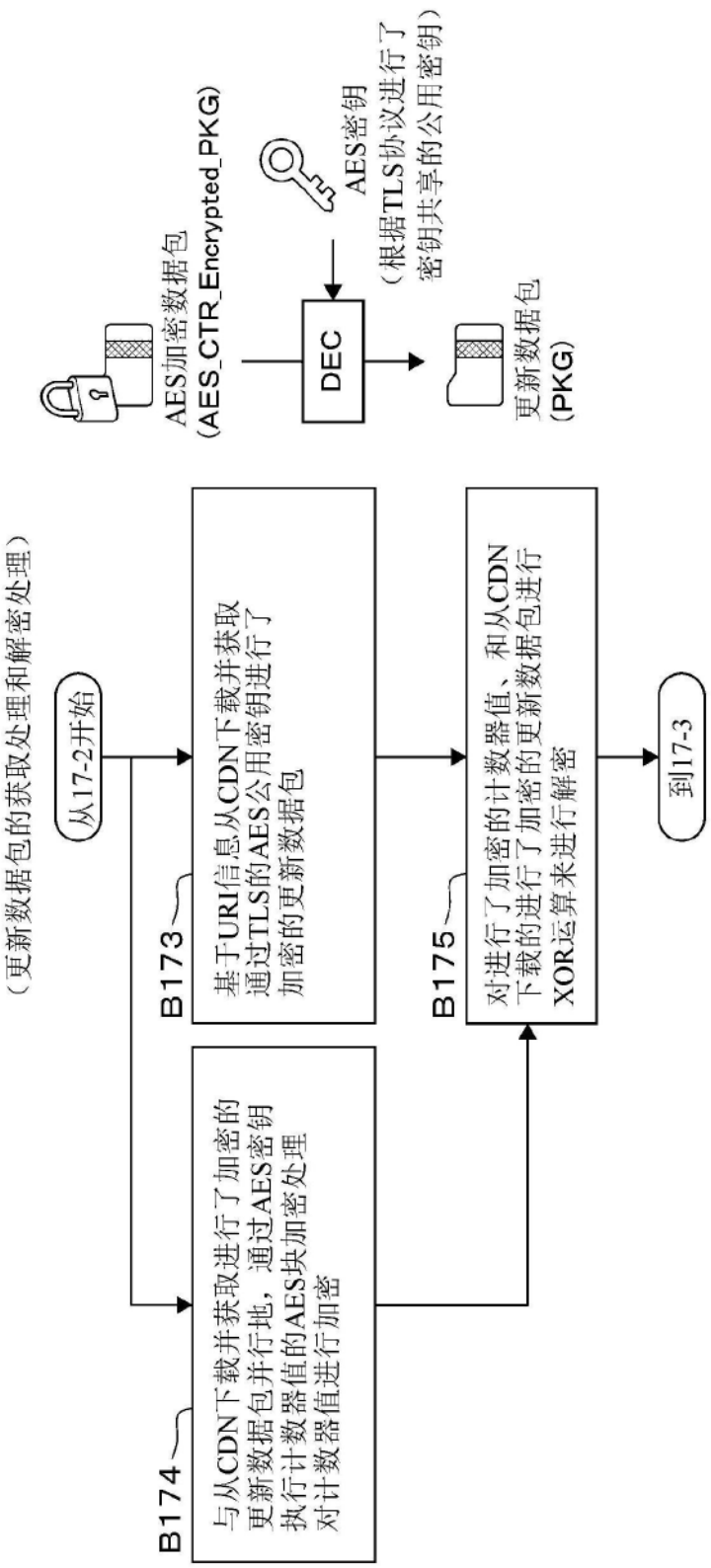

（更新数据包的获取处理和解密处理）
从17-2开始
B173
基于URI信息从CDN下载并获取
通过TLS的AES公用密钥进行了
加密的更新数据包
B174
与从CDN下载并获取进行了加密的
更新数据包并行地，通过AES密钥
执行计数器值的AES块加密处理
对计数器值进行加密
B175
对进行了加密的计数器值、和从CDN
下载的进行了加密的更新数据包进行
XOR运算来进行解密
到17-3
AES加密数据包
(AES_CTR_Encrypted_PKG)
DEC
AES密钥
（根据TLS协议进行了
密钥共享的公用密钥）
更新数据包
(PKG)

图150

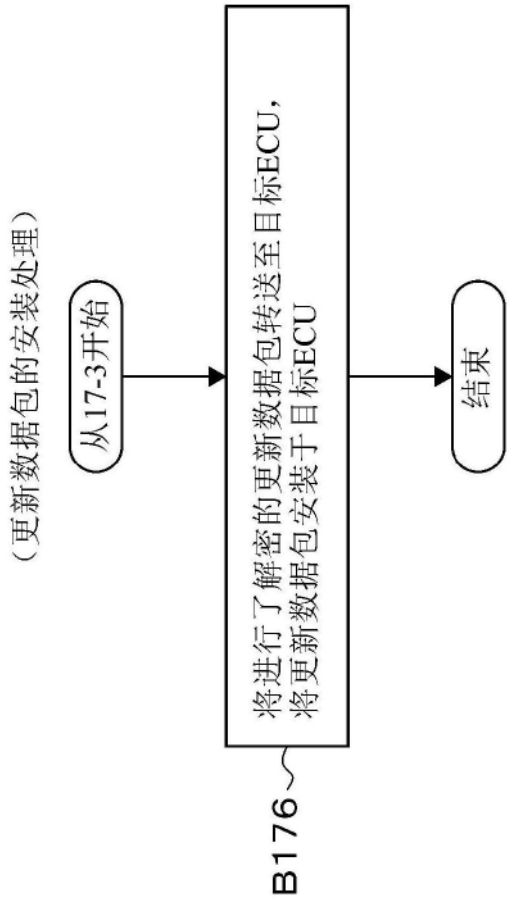

（更新数据包的安装处理）
从17-3开始
将进行了解密的更新数据包转送至目标ECU，
将更新数据包安装于目标ECU
结束
B176

图151

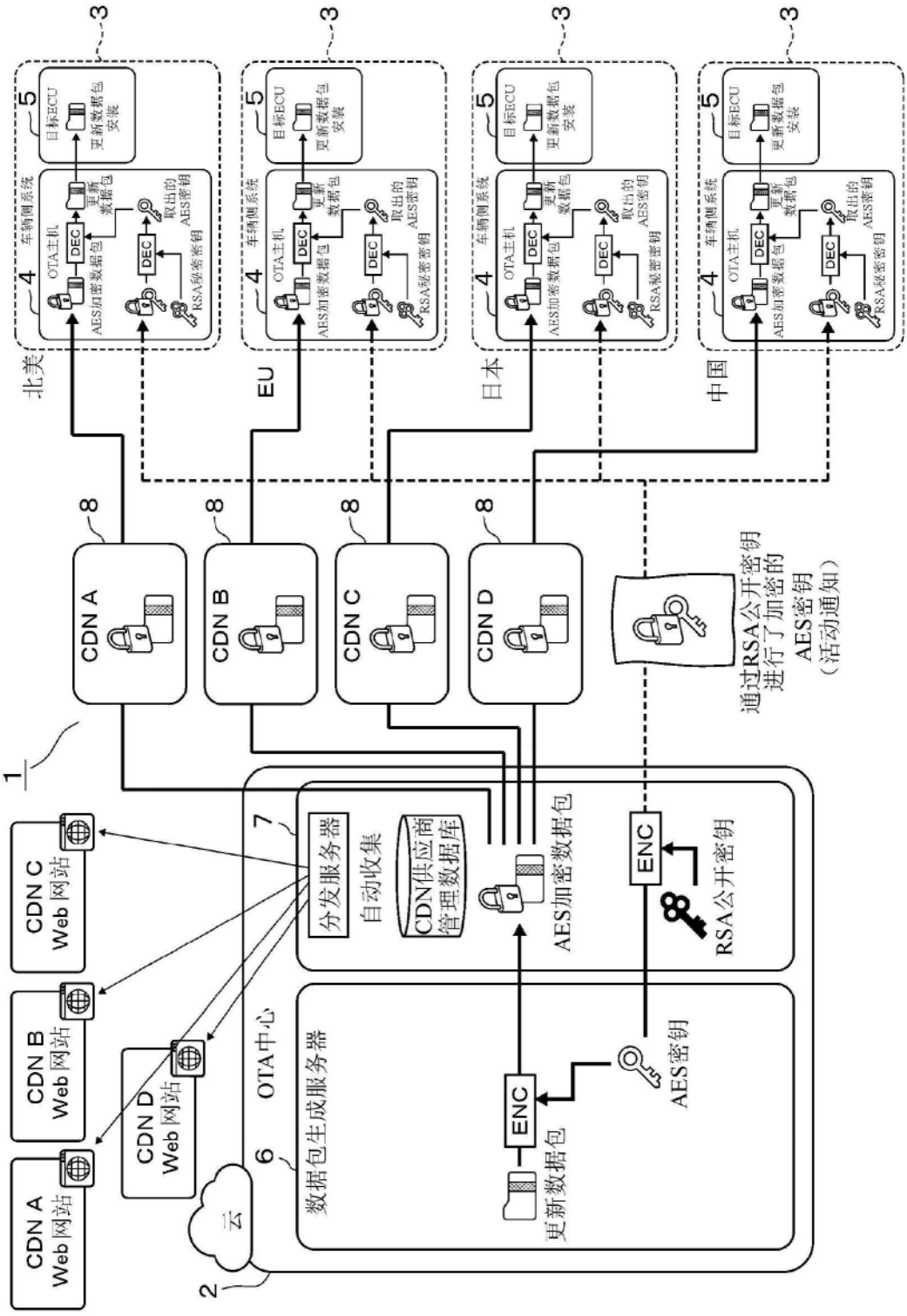

北美
EU
日本
中国
车辆侧系统
OTA主机
目标ECU
更新数据包安装
AES加密数据包
RSA秘密密钥
取出的AES密钥
DEC
CDN A
CDN B
CDN C
CDN D
通过RSA公开密钥进行了加密的AES密钥（活动通知）
OTA中心
数据包生成服务器
分发服务器
自动收集
CDN供应商管理数据库
AES加密数据包
ENC
RSA公开密钥
AES密钥
更新数据包
云
CDN A Web网站
CDN B Web网站
CDN C Web网站
CDN D Web网站

图152

CDN1	每一GB的收费表格						
	～10TB	～40TB	～100TB	～350TB	～500TB	～4PB	5PB～
日本	0.0129 USD	0.121 USD	0.112 USD	0.093 USD	0.075 USD	0.065 USD	0.065 USD
北美	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	每一GB的收费表格						
	～10TB	～40TB	～100TB	～350TB	～524TB	～4PB	5PB～
日本	0.114 USD	0.089 USD	0.086 USD	0.084 USD	0.080 USD	0.070 USD	0.060 USD
北美	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	HTTP方法的请求收费表格	
	HTTP请求	HTTPS请求
日本	0.009 USD	0.012 USD
北美	0.075 USD	0.010 USD
EU	0.009 USD	0.012 USD

图153

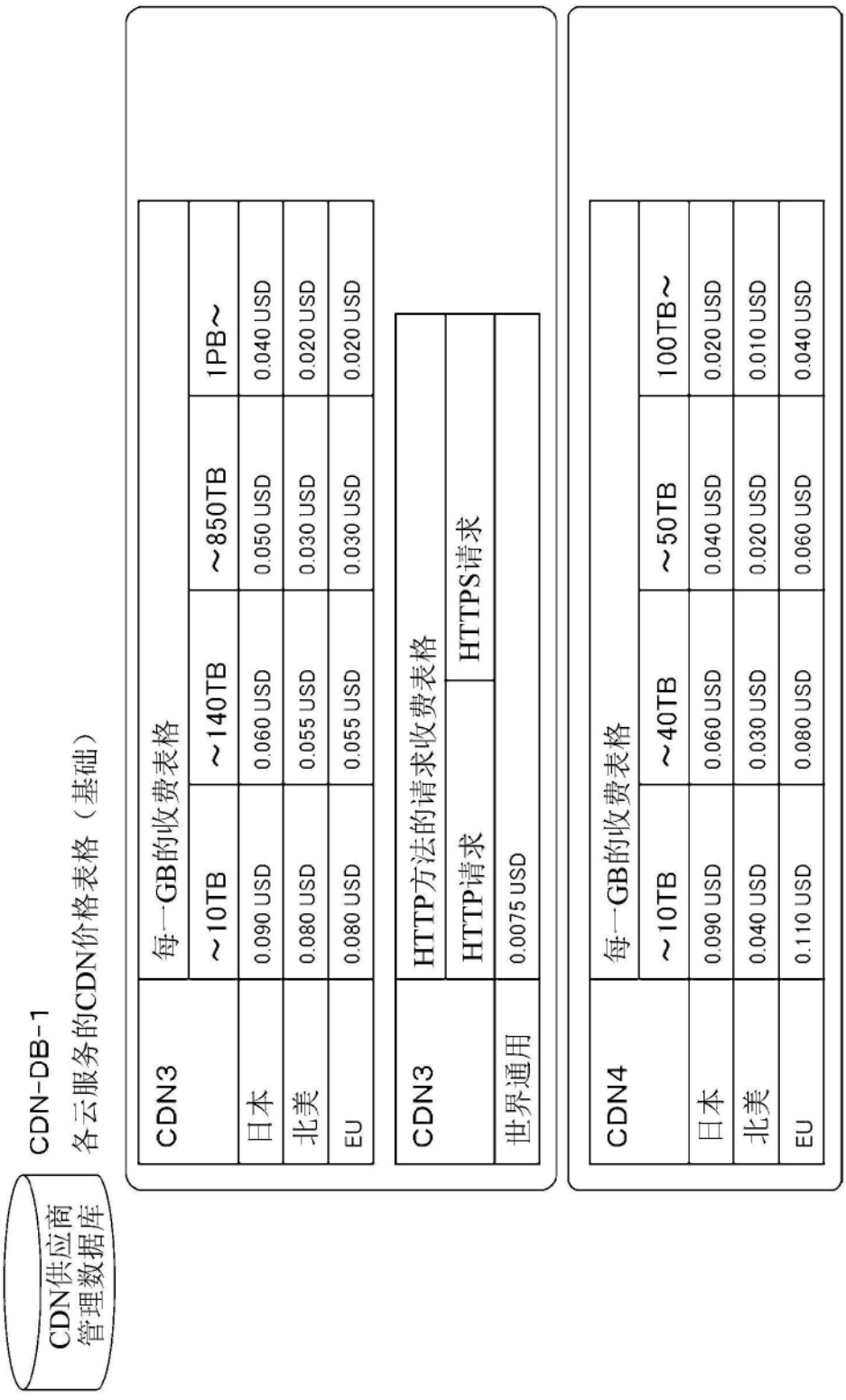

CDN供应商管理数据库
CDN-DB-1
各云服务的CDN价格表格（基础）
CDN3
每一GB的收费表格
～10TB
～140TB
～850TB
1PB～
日本
0.090 USD
0.060 USD
0.050 USD
0.040 USD
北美
0.080 USD
0.055 USD
0.030 USD
0.020 USD
EU
0.080 USD
0.055 USD
0.030 USD
0.020 USD
CDN3
HTTP方法的请求收费表格
HTTP请求
HTTPS请求
世界通用
0.0075 USD
CDN4
每一GB的收费表格
～10TB
～40TB
～50TB
100TB～
日本
0.090 USD
0.060 USD
0.040 USD
0.020 USD
北美
0.040 USD
0.030 USD
0.020 USD
0.010 USD
EU
0.110 USD
0.080 USD
0.060 USD
0.040 USD

图154

CDN1	储存方式 对象台数：200万台	收费表格			
		100MB	1GB	10GB	20GB
日本		245万日元	1452万日元	1亿4560万日元	2亿9120万日元
北美		125万日元	512万日元	5亿500万日元	10亿100万日元
EU		125万日元	512万日元	5亿500万日元	10亿100万日元

CDN2	储存方式 对象台数：200万台	收费表格			
		100MB	1GB	10GB	20GB
日本		189万日元	1760万日元	1亿3200万日元	2亿6400万日元
北美		88万日元	660万日元	4400万日元	8800万日元
EU		132万日元	660万日元	4400万日元	8800万日元

图155

CDN3	储存方式 对象台数：200万台	收费表格			
		100MB	1GB	10GB	20GB
日本		245万日元	1452万日元	1亿4560万日元	2亿9120万日元
北美		125万日元	512万日元	5亿500万日元	10亿100万日元
EU		125万日元	512万日元	5亿500万日元	10亿100万日元

CDN4	储存方式 对象台数：200万台	收费表格			
		100MB	1GB	10GB	20GB
日本		189万日元	1760万日元	1亿3200万日元	2亿6400万日元
北美		88万日元	660万日元	4400万日元	8800万日元
EU		132万日元	660万日元	4400万日元	8800万日元

图156

CDN供应商管理数据库
CDN-DB-3－1
各云服务运营商的流式传输方式中的每个流式传输大小的价格表格，流式传输大小
CDN1
储存方式： 1KB
对象台数： 200万台
收费表格
100MB
1GB
10GB
20GB
日本
245万日元
1452万日元
1亿4560万日元
2亿9120万日元
北美
125万日元
512万日元
5亿500万日元
10亿100万日元
EU
125万日元
512万日元
5亿500万日元
10亿100万日元
CDN1
储存方式： 10KB
对象台数： 200万台
收费表格
100MB
1GB
10GB
20GB
日本
245万日元
1452万日元
1亿4560万日元
2亿9120万日元
北美
125万日元
512万日元
5亿500万日元
10亿100万日元
EU
125万日元
512万日元
5亿500万日元
10亿100万日元
CDN1
储存方式：
100KB 对象台数： 200万台
收费表格
100MB
1GB
10GB
20GB
日本
245万日元
1452万日元
1亿4560万日元
2亿9120万日元
北美
125万日元
512万日元
5亿500万日元
10亿100万日元
EU
125万日元
512万日元
5亿500万日元
10亿100万日元

图157

CDN2	储存方式：1KB 对象台数：200万台	收费表格（HTTP/HTTPS）			
		100MB	1GB	10GB	20GB
日本		2169万日元/2829万日元	2亿1560万日元/2亿8160万日元	21亿1200万日元/27亿7200万日元	42亿2400万日元/55亿4400万日元
北美		1738万日元/2288万日元	1亿7160万日元/2亿2660万日元	16亿9400万日元/22亿4400万日元	33亿8800万日元/44亿8800万日元
EU		2112万日元/2772万日元	2亿460万日元/2亿7060万日元	20亿2400万日元/26亿8400万日元	40亿4800万日元/53亿6800万日元

CDN2	储存方式：10KB 对象台数：200万台	收费表格（HTTP/HTTPS）			
		100MB	1GB	10GB	20GB
日本		387万日元/453万日元	3740万日元/4400万日元	3亿3000万日元/3亿9600万日元	6亿6000万日元/7亿9200万日元
北美		253万日元/308万日元	2310万日元/2860万日元	3亿900万日元/2亿6400万日元	4亿8500万日元/5亿2800万日元
EU		330万日元/396万日元	2640万日元/3300万日元	2亿4200万日元/3亿800万日元	4亿8400万日元/6亿1600万日元

CDN2	储存方式：100KB 对象台数：200万台	收费表格（HTTP/HTTPS）			
		100MB	1GB	10GB	20GB
日本		209万日元/216万日元	1958万日元/2024万日元	1亿5180万日元/1亿5840万日元	3亿360万日元/3亿1680万日元
北美		105万日元/110万日元	825万日元/880万日元	6050万日元/6600万日元	1亿2100万日元/1亿3200万日元
EU		152万日元/158万日元	858万日元/924万日元	6380万日元/7040万日元	1亿2760万日元/1亿4080万日元

图158

CDN3	储存方式：1KB 对象台数：200万台	收费表格			
		100MB	1GB	10GB	20GB
日本		134万日元	457万日元	4567万日元	9130万日元
北美		134万日元	457万日元	4567万日元	9130万日元
EU		134万日元	457万日元	4567万日元	9130万日元

CDN3	储存方式：10KB 对象台数：200万台	收费表格			
		100MB	1GB	10GB	20GB
日本		132万日元	442万日元	4417万日元	8833万日元
北美		132万日元	442万日元	4417万日元	8833万日元
EU		132万日元	442万日元	4417万日元	8833万日元

CDN3	储存方式： 100KB 对象台数：200万台	收费表格			
		100MB	1GB	10GB	20GB
日本		132万日元	440万日元	4400万日元	8800万日元
北美		132万日元	440万日元	4400万日元	8800万日元
EU		132万日元	440万日元	4400万日元	8800万日元

图159

CDN4	储存方式：1KB 对象台数：200万台	收费表格			
		100MB	1GB	10GB	20GB
日本		44万日元	440万日元	4400万日元	8800万日元
北美		22万日元	220万日元	2200万日元	4400万日元
EU		88万日元	880万日元	8800万日元	1亿7600万日元

CDN4	储存方式：10KB 对象台数：200万台	收费表格			
		100MB	1GB	10GB	20GB
日本		44万日元	440万日元	4400万日元	8800万日元
北美		22万日元	220万日元	2200万日元	4400万日元
EU		88万日元	880万日元	8800万日元	1亿7600万日元

CDN4	储存方式：100KB 对象台数：200万台	收费表格			
		100MB	1GB	10GB	20GB
日本		44万日元	440万日元	4400万日元	8800万日元
北美		22万日元	220万日元	2200万日元	4400万日元
EU		88万日元	880万日元	8800万日元	1亿7600万日元

图160

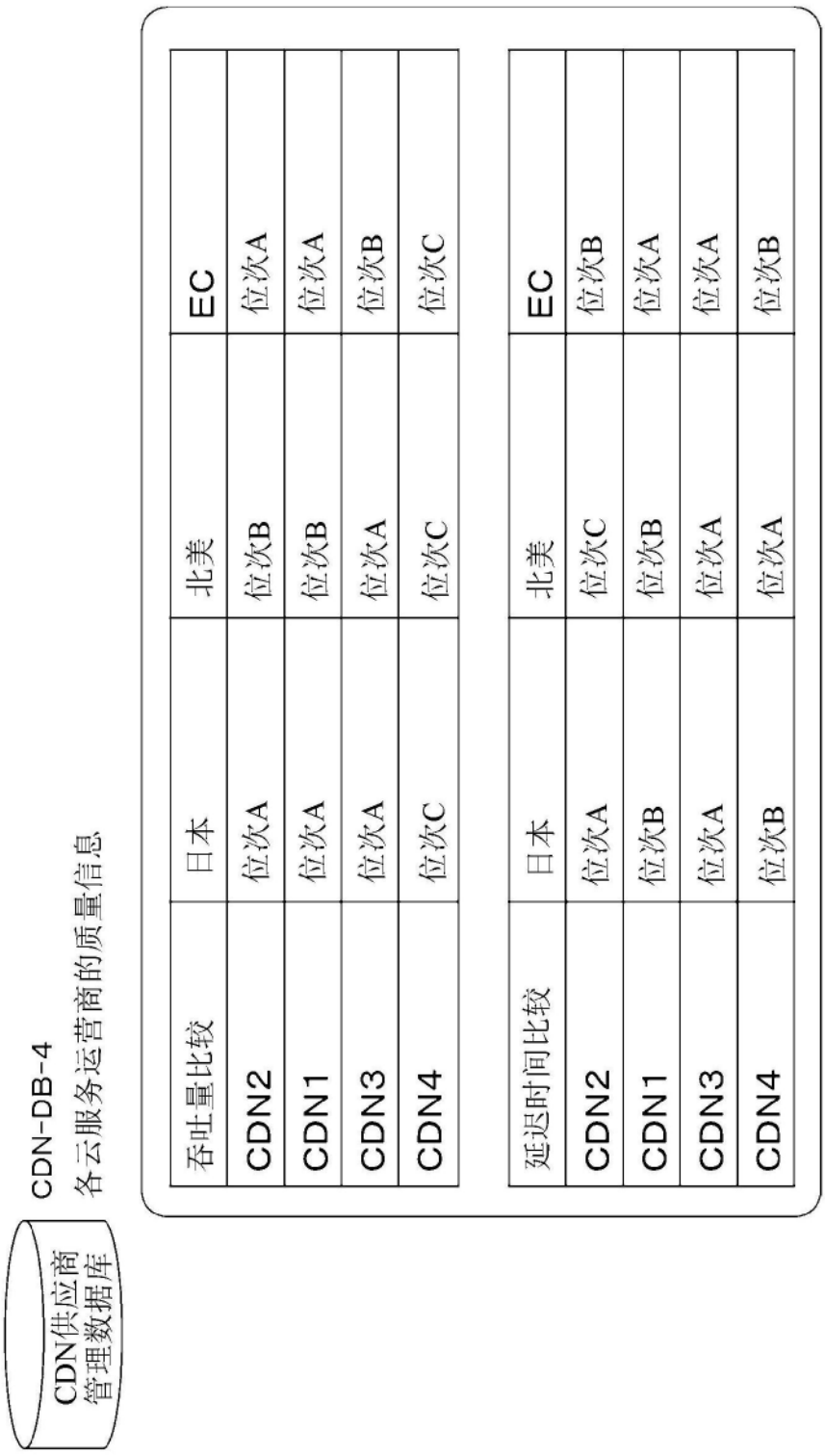

CDN供应商
管理数据库
CDN-DB-4
各云服务运营商的质量信息
吞吐量比较
日本
北美
EC
CDN2
位次A
位次B
位次A
CDN1
位次A
位次B
位次A
CDN3
位次A
位次A
位次B
CDN4
位次C
位次C
位次C
延迟时间比较
日本
北美
EC
CDN2
位次A
位次C
位次B
CDN1
位次B
位次B
位次A
CDN3
位次A
位次A
位次A
CDN4
位次B
位次A
位次B

图161

CDN供应商 选定逻辑	① 分发成本	② 吞吐量的加权	③ 响应延迟时间的加权
CDN供应商	分发成本（日元）	位次 A：0.8 位次 B：1.0 位次 C：1.2	位次 A：0.8 位次 B：1.0 位次 C：1.2

CDN供应商A：① 分发成本 一亿日元

② 吞吐量位次：位次A

③ 响应延迟时间位次：位次A

⬇ 该情况下CDN供应商A的评价额

①×②×③=1亿日元×0.8×0.8=0.64亿日元

CDN供应商B：① 分发成本 0.8亿日元

② 吞吐量位次：位次C

③ 响应延迟时间位次：位次C

⬇ 该情况下CDN供应商B的评价额

①×②×③=0.8亿日元×1.2×1.2=1.1亿日元

图162

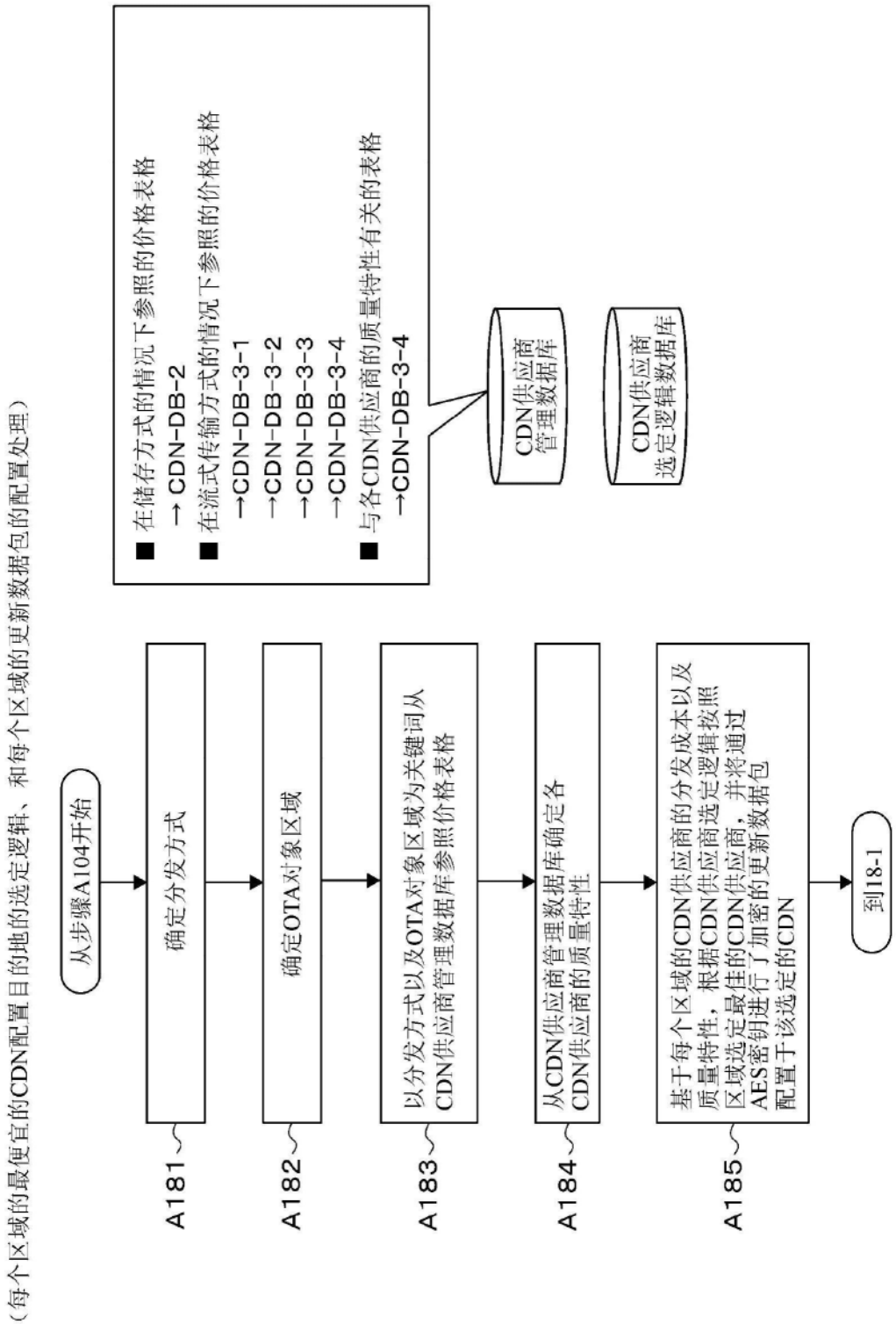

（每个区域的最便宜的CDN配置目的地的选定逻辑、和每个区域的更新数据包的配置处理）
从步骤A104开始
A181
确定分发方式
A182
确定OTA对象区域
A183
以分发方式以及OTA对象区域为关键词从CDN供应商管理数据库参照价格表格
A184
从CDN供应商管理数据库确定各CDN供应商的质量特性
A185
基于每个区域的CDN供应商的分发成本以及质量特性，根据CDN供应商选定逻辑按照区域选定最佳的CDN供应商，并将通过AES密钥进行了加密的更新数据包配置于该选定的CDN
到18-1
■ 在储存方式的情况下参照的价格表格
→ CDN-DB-2
■ 在流式传输方式的情况下参照的价格表格
→CDN-DB-3-1
→CDN-DB-3-2
→CDN-DB-3-3
→CDN-DB-3-4
■ 与各CDN供应商的质量特性有关的表格
→CDN-DB-3-4
CDN供应商管理数据库
CDN供应商选定逻辑数据库

图163

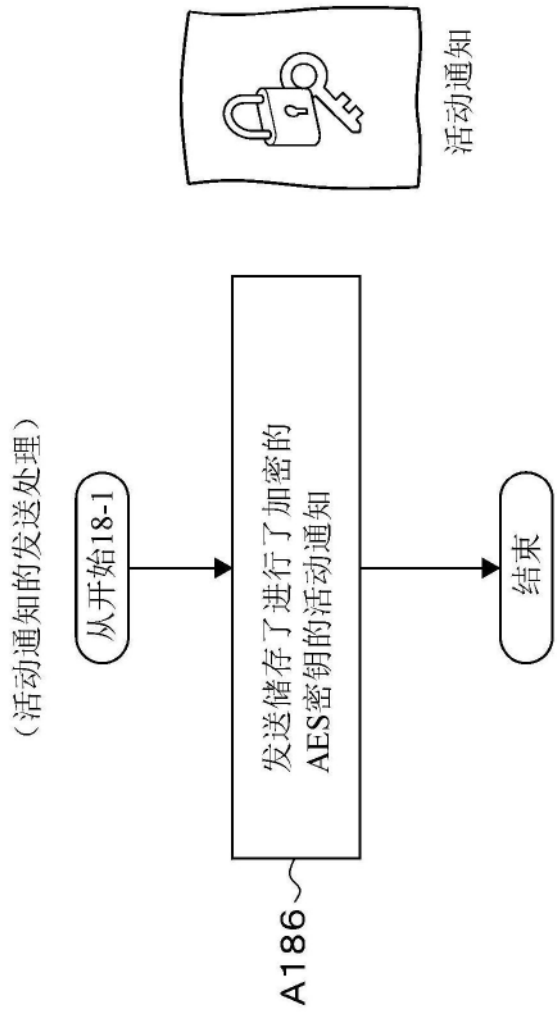


图164

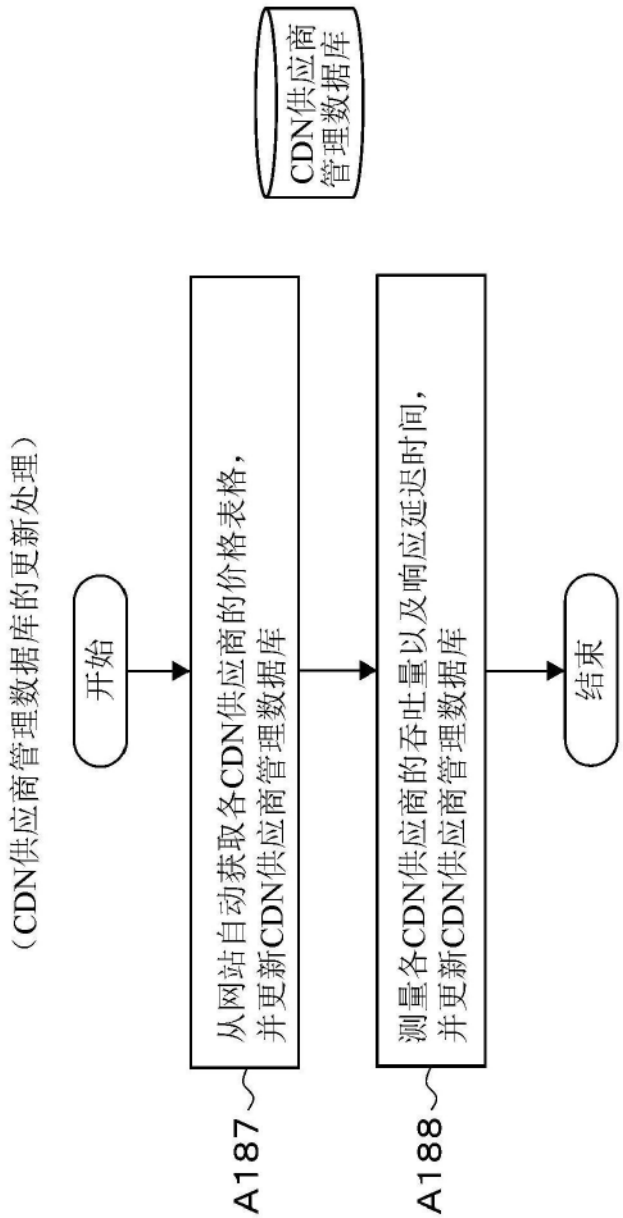

CDN供应商管理数据库
（CDN供应商管理数据库的更新处理）
开始
从网站自动获取各CDN供应商的价格表格，并更新CDN供应商管理数据库
A187
测量各CDN供应商的吞吐量以及响应延迟时间，并更新CDN供应商管理数据库
A188
结束

图165

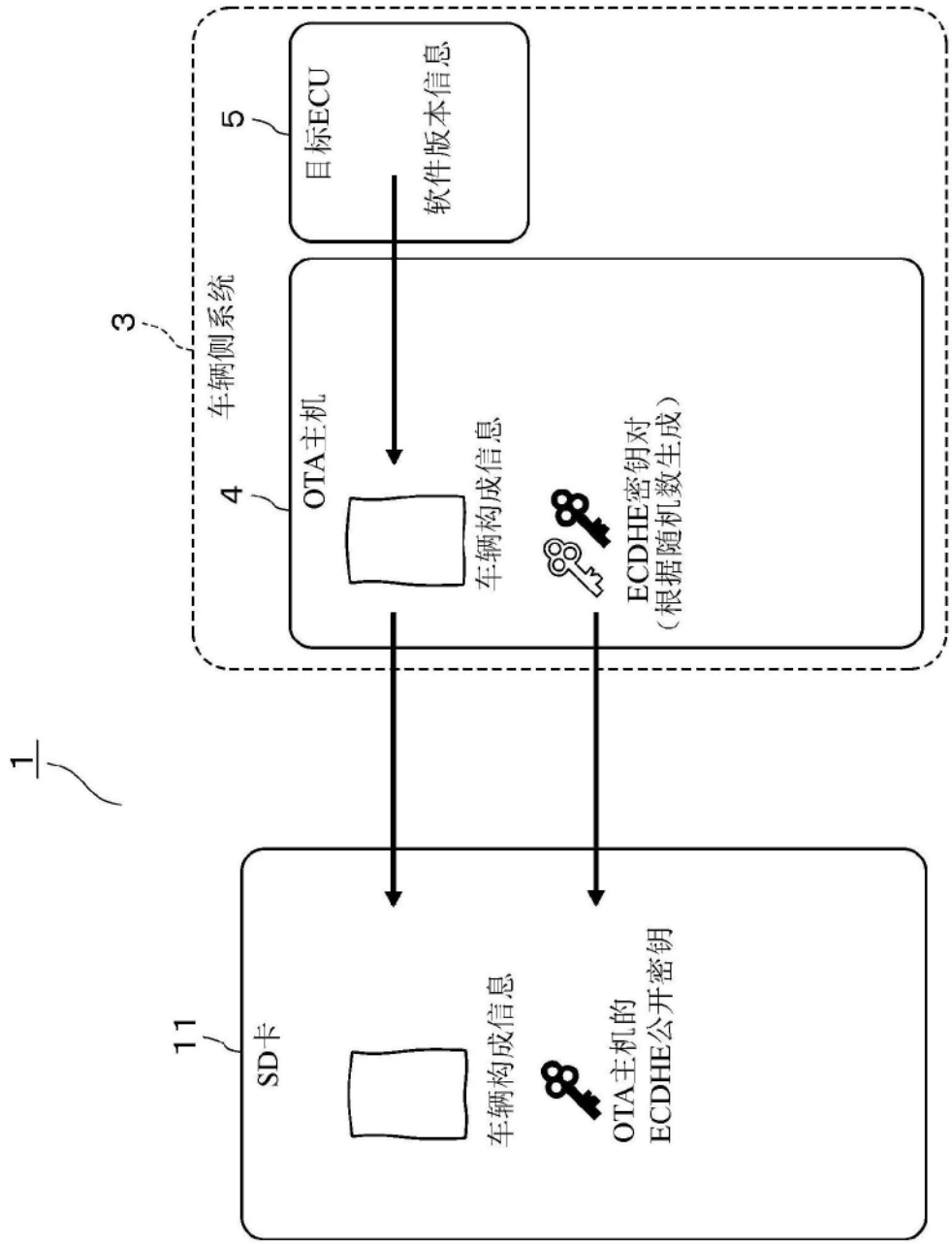

1
3
车辆侧系统
4
OTA主机
车辆构成信息
ECDHE密钥对
（根据随机数生成）
5
目标ECU
软件版本信息
11
SD卡
车辆构成信息
OTA主机的
ECDHE公开密钥

图166

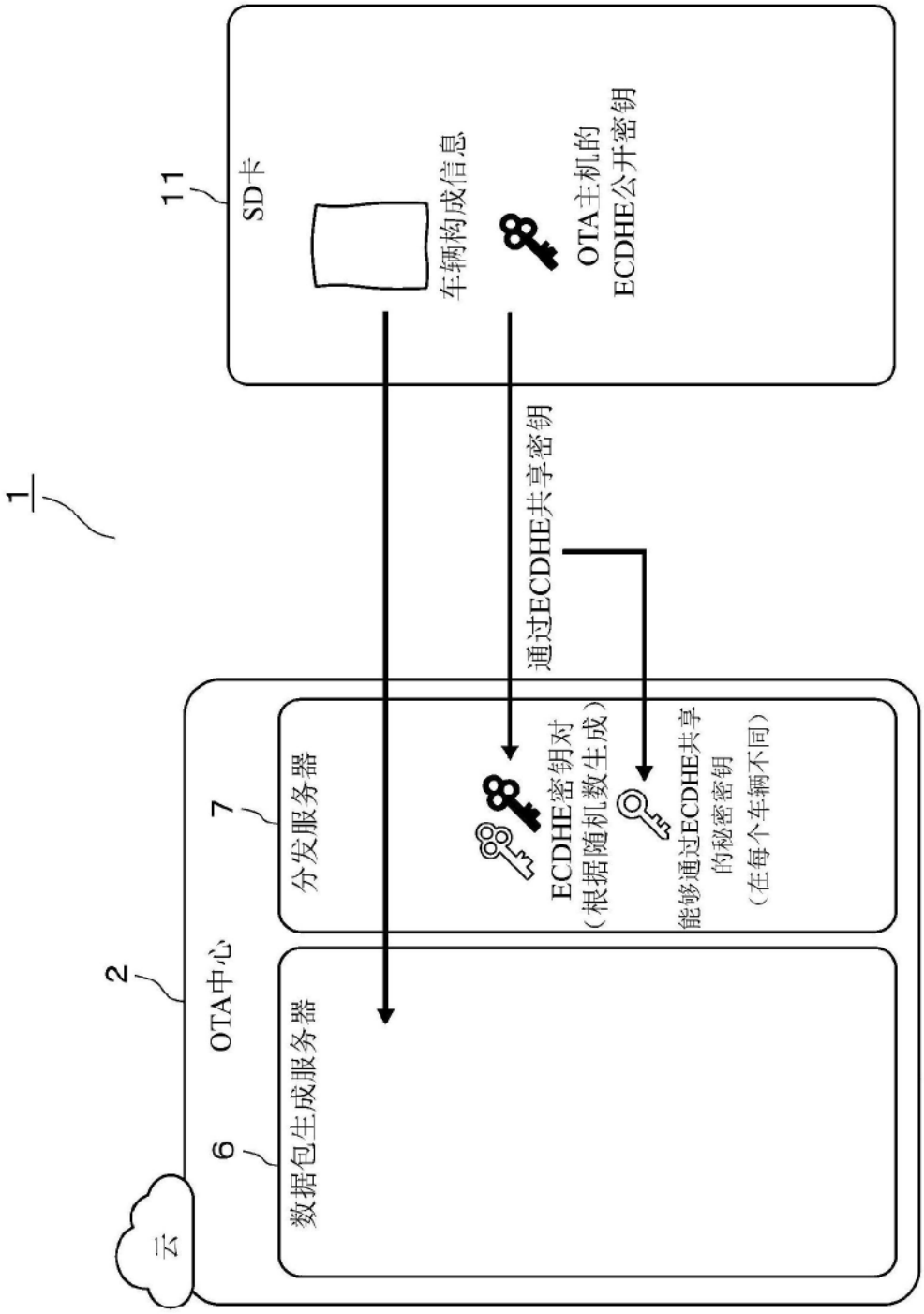

1
11
SD卡
车辆构成信息
OTA主机的
ECDHE公开密钥
通过ECDHE共享密钥
2
OTA中心
7
分发服务器
ECDHE密钥对
（根据随机数生成）
能够通过ECDHE共享
的秘密密钥
（在每个车辆不同）
6
数据包生成服务器
云

图167

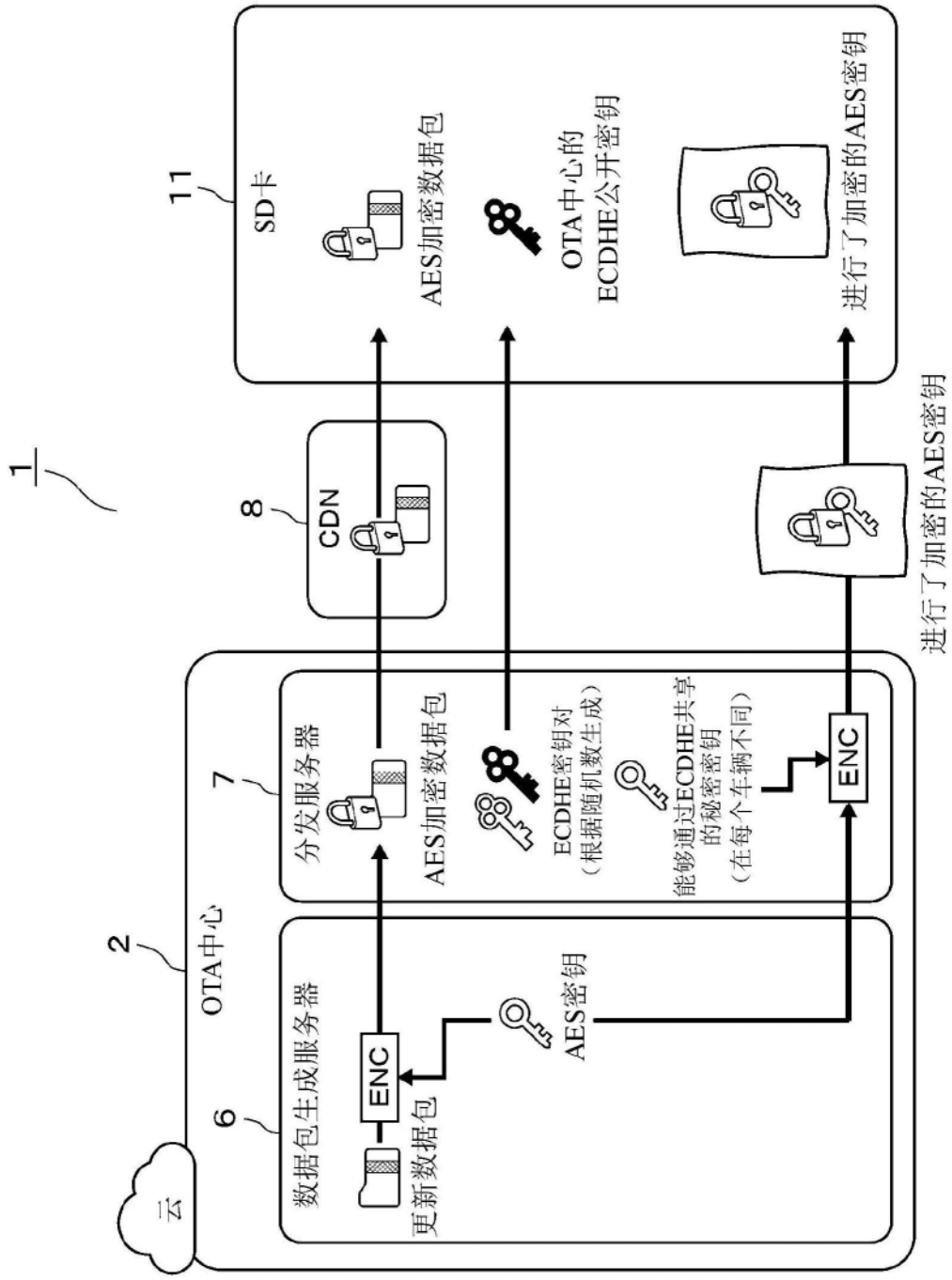

1
2
OTA中心
6
数据包生成服务器
更新数据包
ENC
AES密钥
云
7
分发服务器
AES加密数据包
ECDHE密钥对
（根据随机数生成）
能够通过ECDHE共享
的秘密密钥
（在每个车辆不同）
ENC
8
CDN
11
SD卡
AES加密数据包
OTA中心的
ECDHE公开密钥
进行了加密的AES密钥
进行了加密的AES密钥

图168

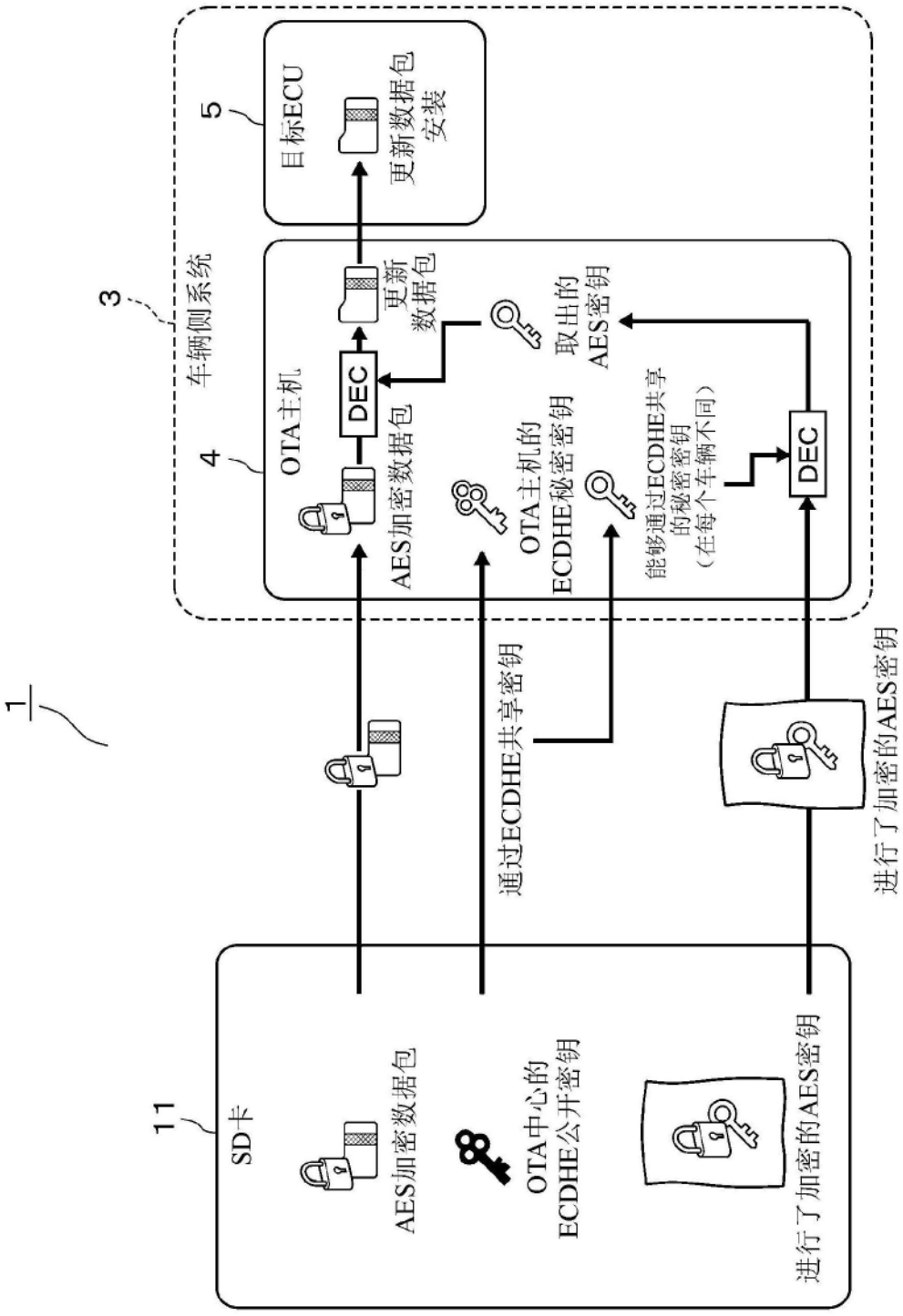

1
3
车辆侧系统
4
OTA主机
AES加密数据包
DEC
更新数据包
5
目标ECU
更新数据包安装
OTA主机的ECDHE秘密密钥
能够通过ECDHE共享的秘密密钥（在每个车辆不同）
取出的AES密钥
DEC
通过ECDHE共享密钥
进行了加密的AES密钥
11
SD卡
AES加密数据包
OTA中心的ECDHE公开密钥
进行了加密的AES密钥

图169

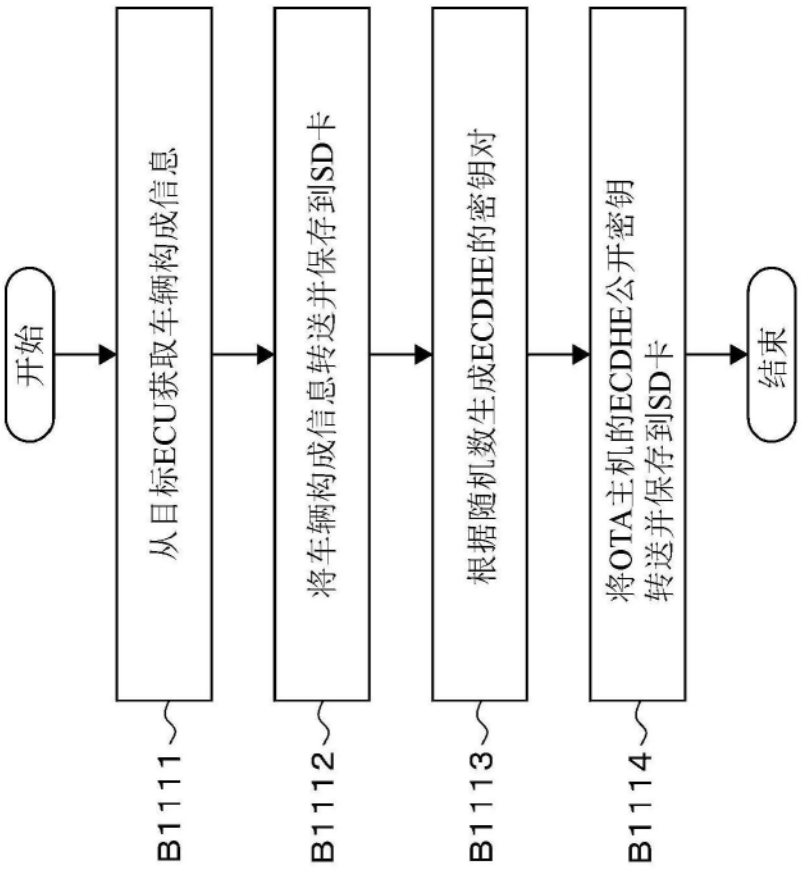

开始
从目标ECU获取车辆构成信息
将车辆构成信息转送并保存到SD卡
根据随机数生成ECDHE的密钥对
将OTA主机的ECDHE公开密钥
转送并保存到SD卡
结束
B1111
B1112
B1113
B1114

图170

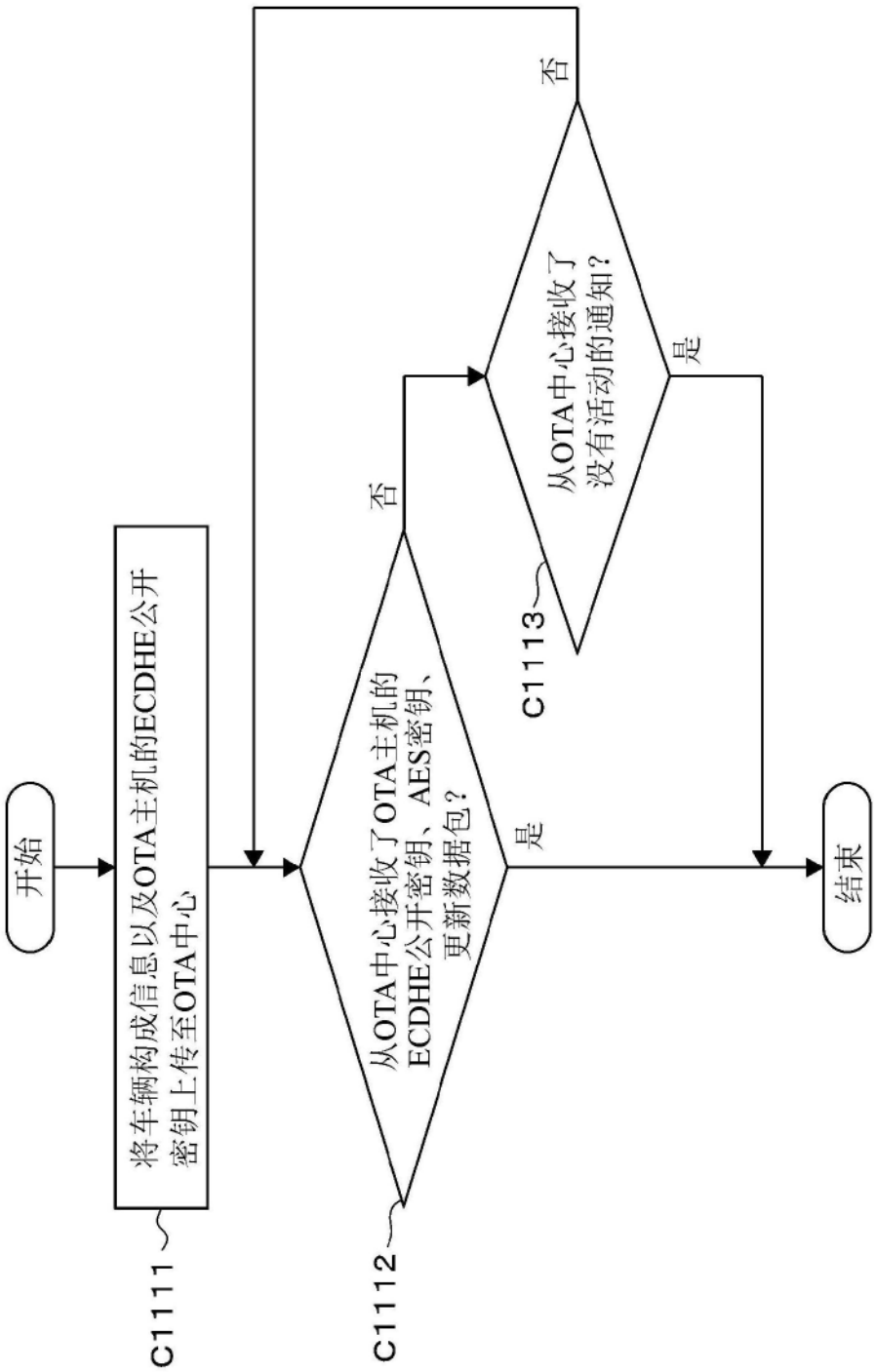

开始
将车辆构成信息以及OTA主机的ECDHE公开密钥上传至OTA中心
C1111
从OTA中心接收了OTA主机的ECDHE公开密钥、AES密钥、更新数据包？
C1112
否
是
从OTA中心接收了没有活动的通知？
C1113
否
是
结束

图171

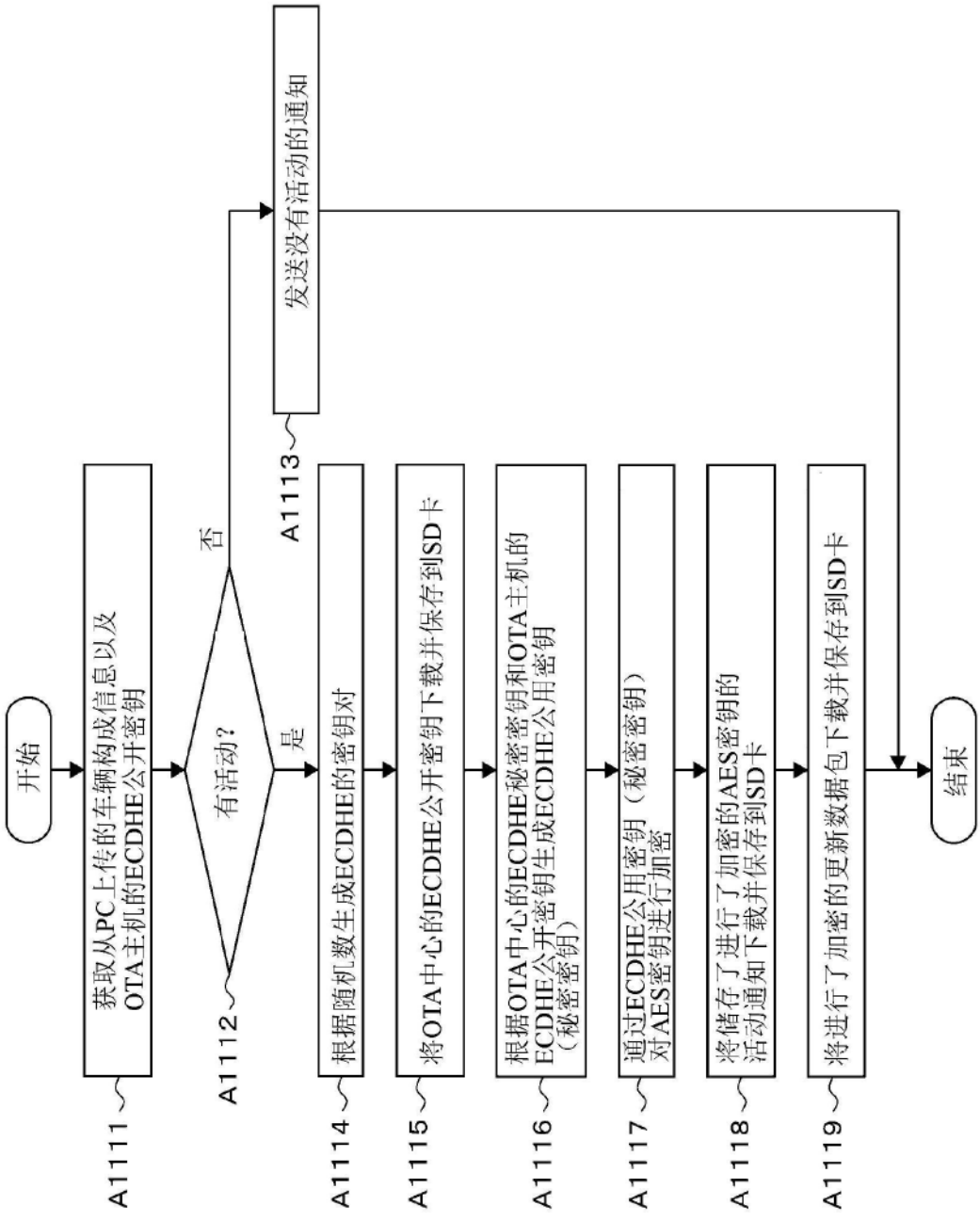

开始
获取从PC上传的车辆构成信息以及OTA主机的ECDHE公共密钥
A1111
有活动?
A1112
否
是
发送没有活动的通知
A1113
根据随机数生成ECDHE的密钥对
A1114
将OTA中心的ECDHE公共密钥下载并保存到SD卡
A1115
根据OTA中心的ECDHE秘密密钥和OTA主机的ECDHE公共密钥生成ECDHE公用密钥（秘密密钥）
A1116
通过ECDHE公用密钥（秘密密钥）对AES密钥进行加密
A1117
将储存了进行了加密的AES密钥的活动通知下载并保存到SD卡
A1118
将进行了加密的更新数据包下载并保存到SD卡
A1119
结束

图172

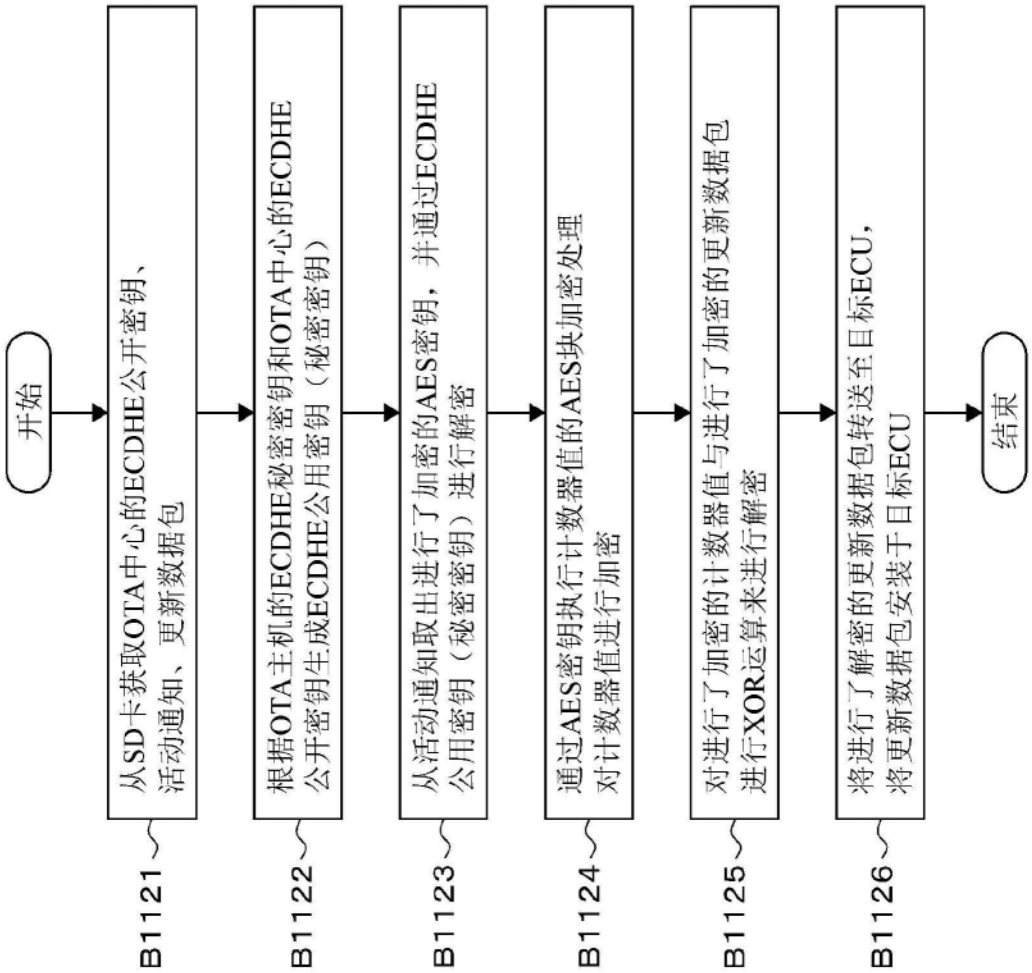

开始
从SD卡获取OTA中心的ECDHE公开密钥、活动通知、更新数据包
B1121
根据OTA主机的ECDHE秘密密钥和OTA中心的ECDHE公开密钥生成ECDHE公用密钥（秘密密钥）
B1122
从活动通知取出进行了加密的AES密钥，并通过ECDHE公用密钥（秘密密钥）进行解密
B1123
通过AES密钥执行计数器值的AES块加密处理对计数器值进行加密
B1124
对进行了加密的计数器值与进行了加密的更新数据包进行XOR运算来进行解密
B1125
将进行了解密的更新数据包转送至目标ECU，将更新数据包安装于目标ECU
B1126
结束

图173

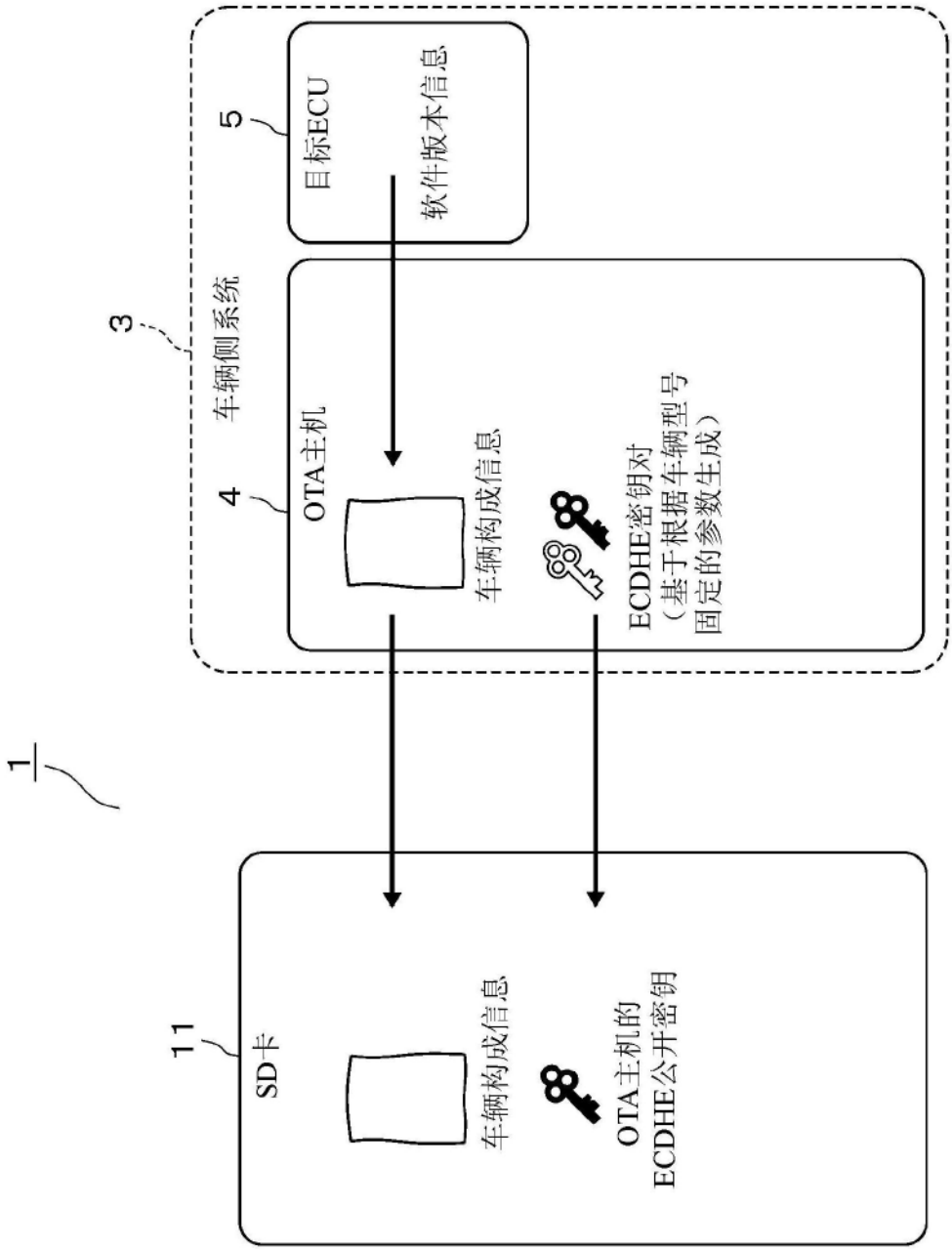

1
3
车辆侧系统
4
OTA主机
车辆构成信息
ECDHE密钥对
（基于根据车辆型号
固定的参数生成）
5
目标ECU
软件版本信息
11
SD卡
车辆构成信息
OTA主机的
ECDHE公开密钥

图174

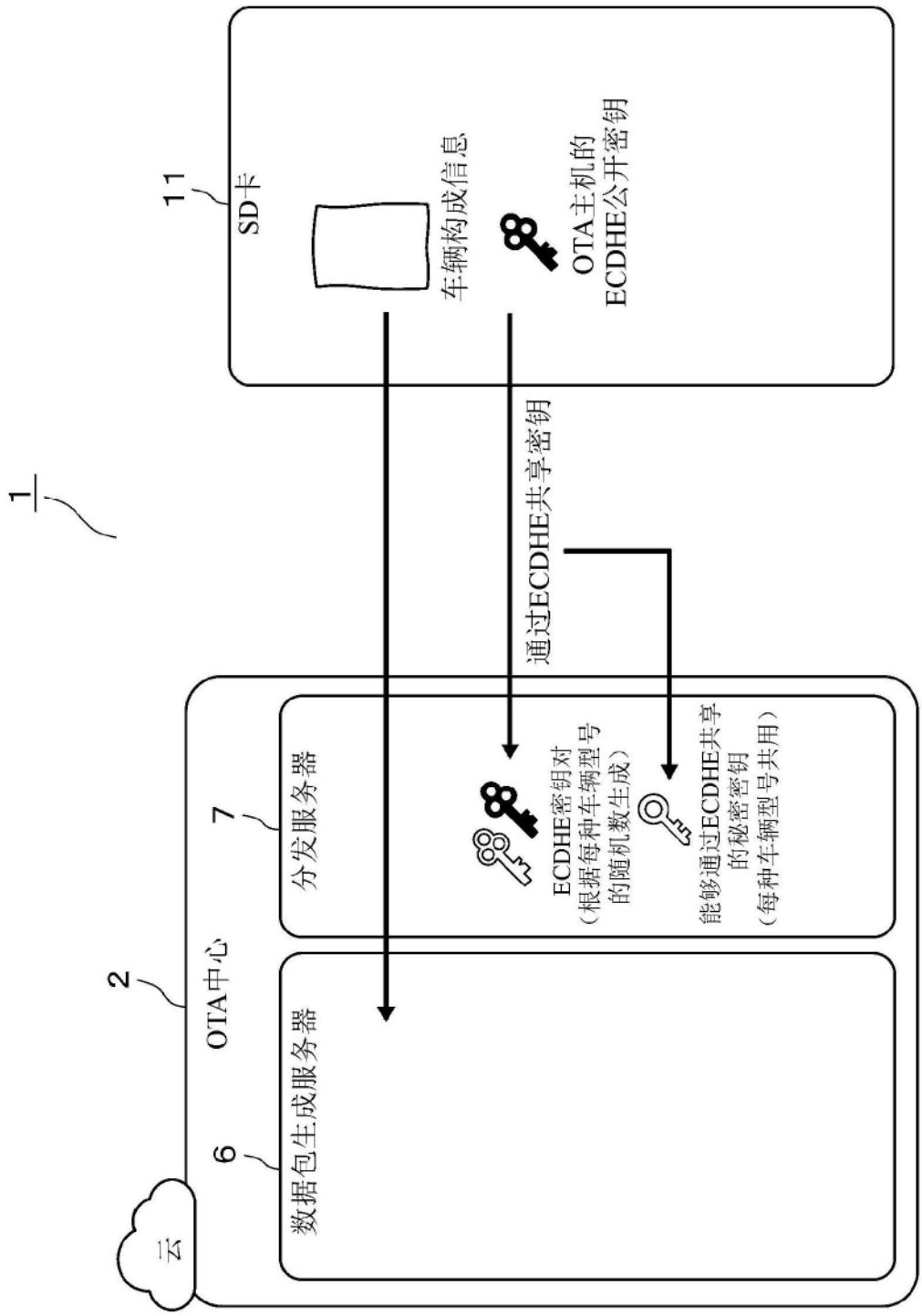

1
2
OTA中心
6
数据包生成服务器
7
分发服务器
云
11
SD卡
车辆构成信息
OTA主机的
ECDHE公开密钥
通过ECDHE共享密钥
ECDHE密钥对
（根据每种车辆型号
的随机数生成）
能够通过ECDHE共享
的秘密密钥
（每种车辆型号共用）

图175

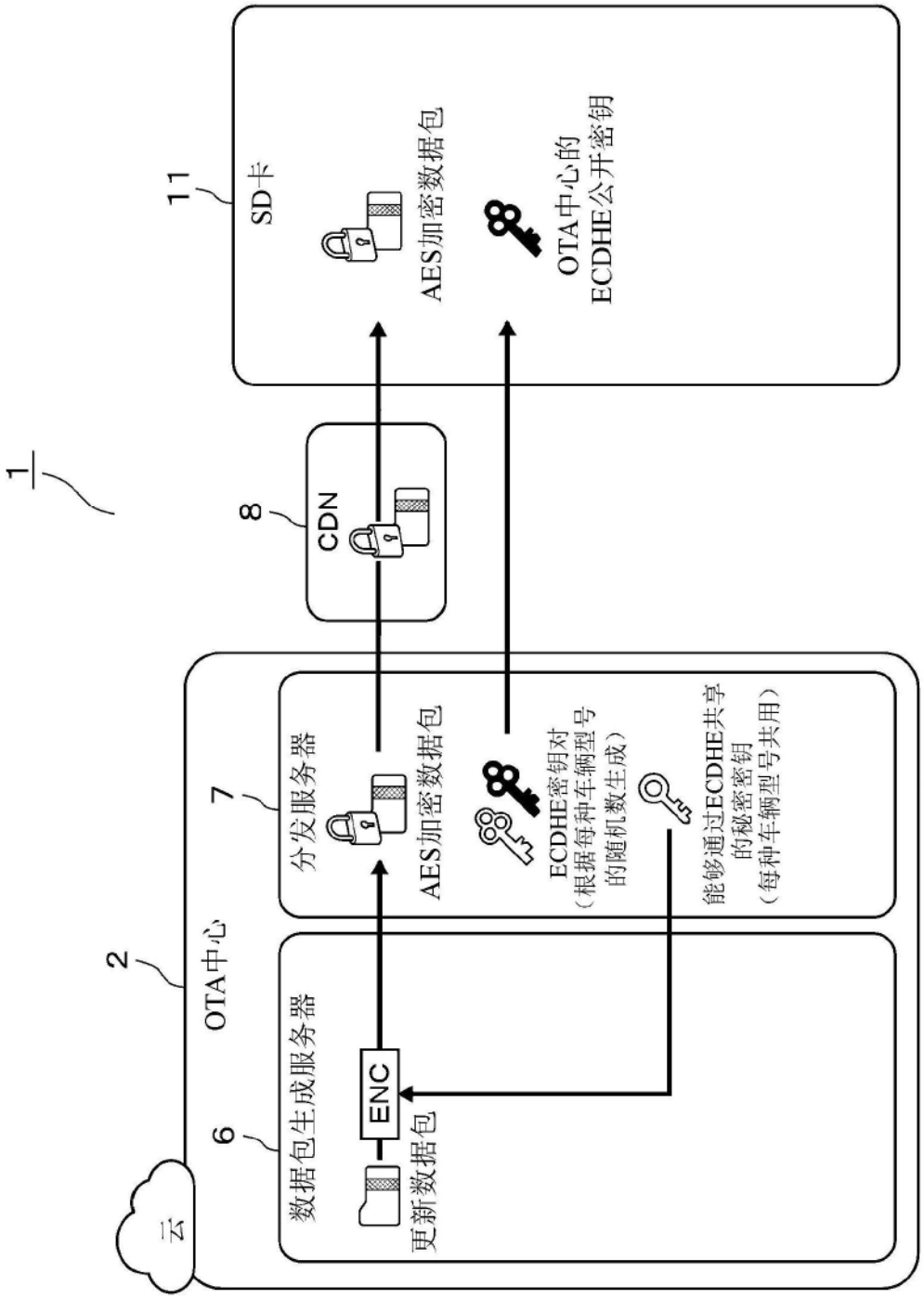

1
2
OTA中心
云
6
数据包生成服务器
更新数据包
ENC
7
分发服务器
AES加密数据包
ECDHE密钥对
（根据每种车辆型号
的随机数生成）
能够通过ECDHE共享
的秘密密钥
（每种车辆型号共用）
8
CDN
11
SD卡
AES加密数据包
OTA中心的
ECDHE公开密钥

图176

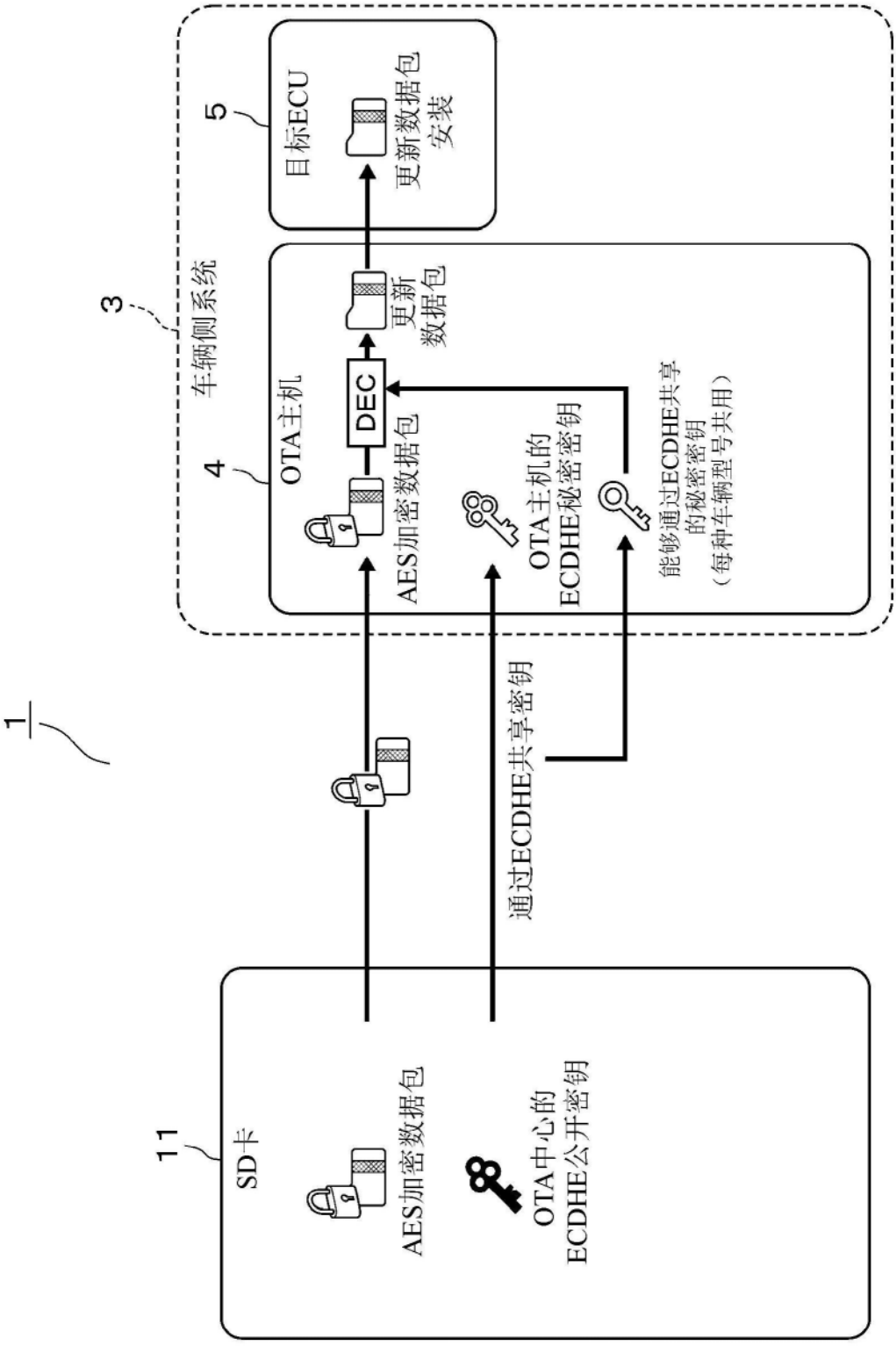

1
3
车辆侧系统
4
OTA主机
DEC
AES加密数据包
更新
数据包
OTA主机的
ECDHE秘密密钥
能够通过ECDHE共享
的秘密密钥
（每种车辆型号共用）
5
目标ECU
更新数据包
安装
通过ECDHE共享密钥
11
SD卡
AES加密数据包
OTA中心的
ECDHE公开密钥

图177

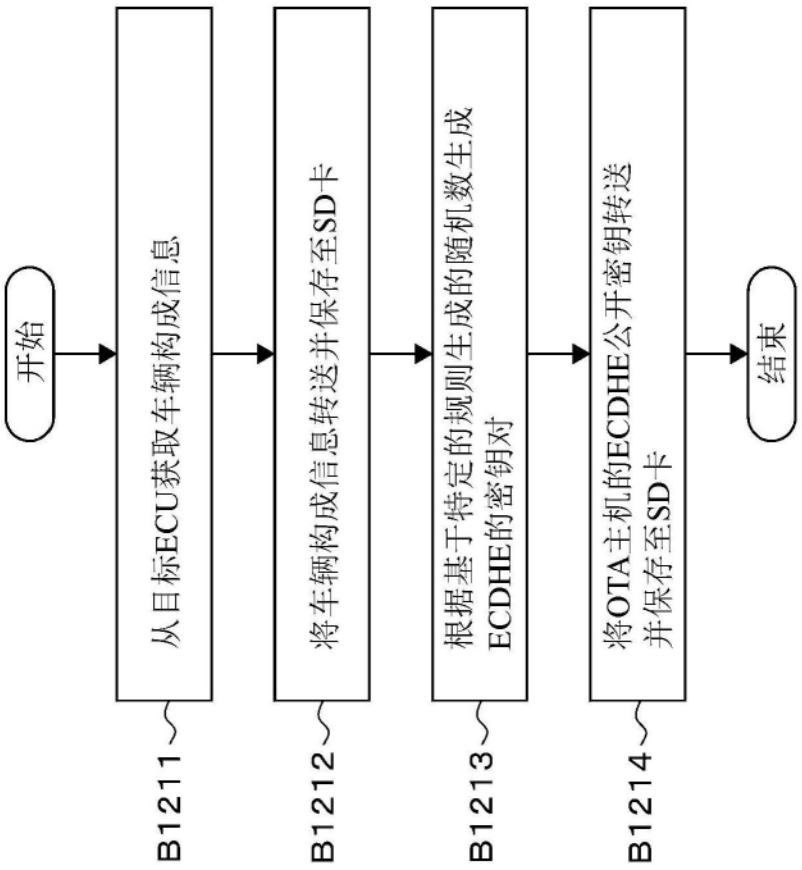

开始
从目标ECU获取车辆构成信息
将车辆构成信息转送并保存至SD卡
根据基于特定的规则生成的随机数生成ECDHE的密钥对
将OTA主机的ECDHE公开密钥转送并保存至SD卡
结束
B1211
B1212
B1213
B1214

图178

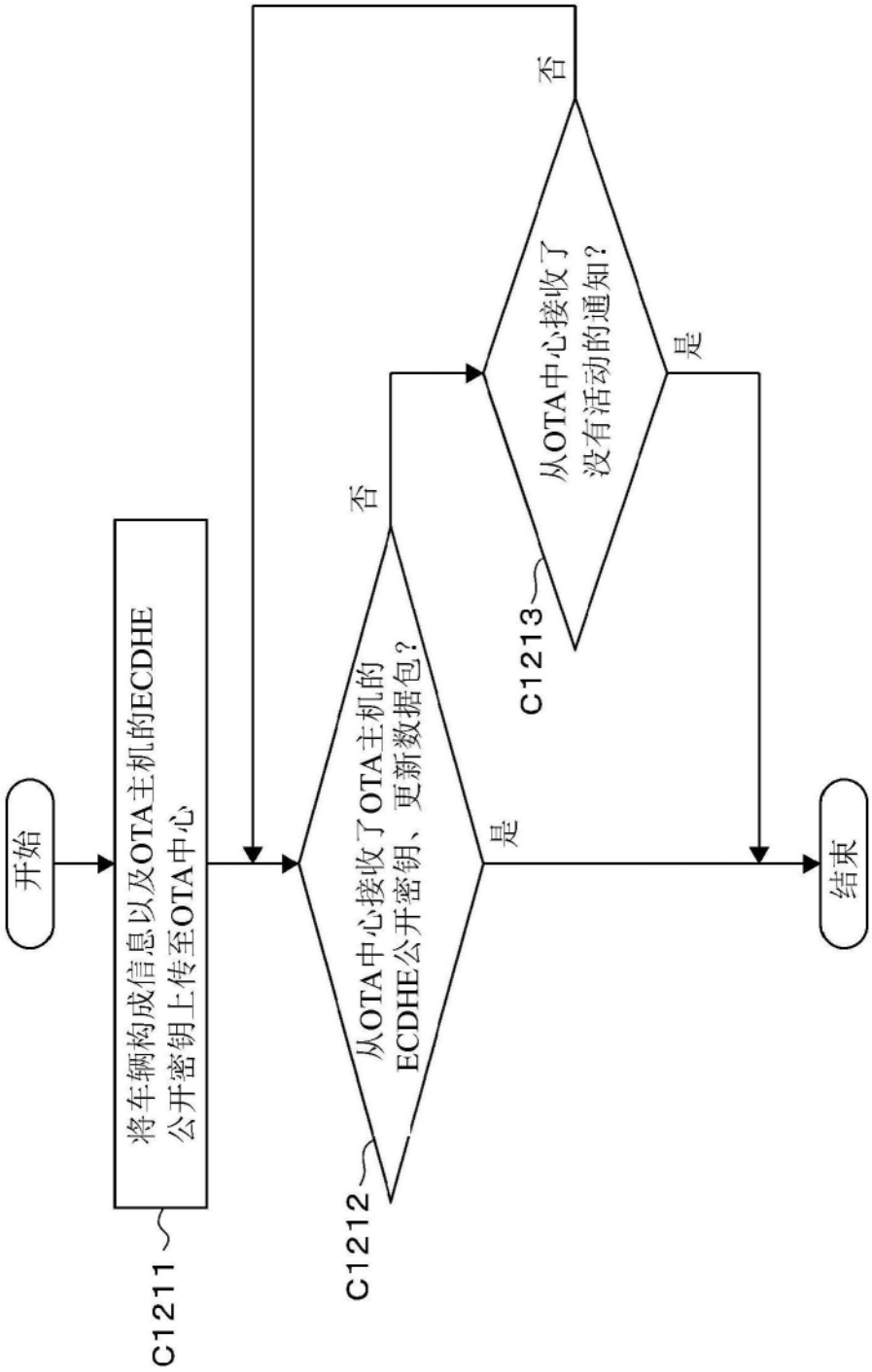

开始
将车辆构成信息以及OTA主机的ECDHE公开密钥上传至OTA中心
C1211
从OTA中心接收了OTA主机的ECDHE公开密钥、更新数据包?
C1212
否
是
从OTA中心接收了没有活动的通知?
C1213
否
是
结束

图179

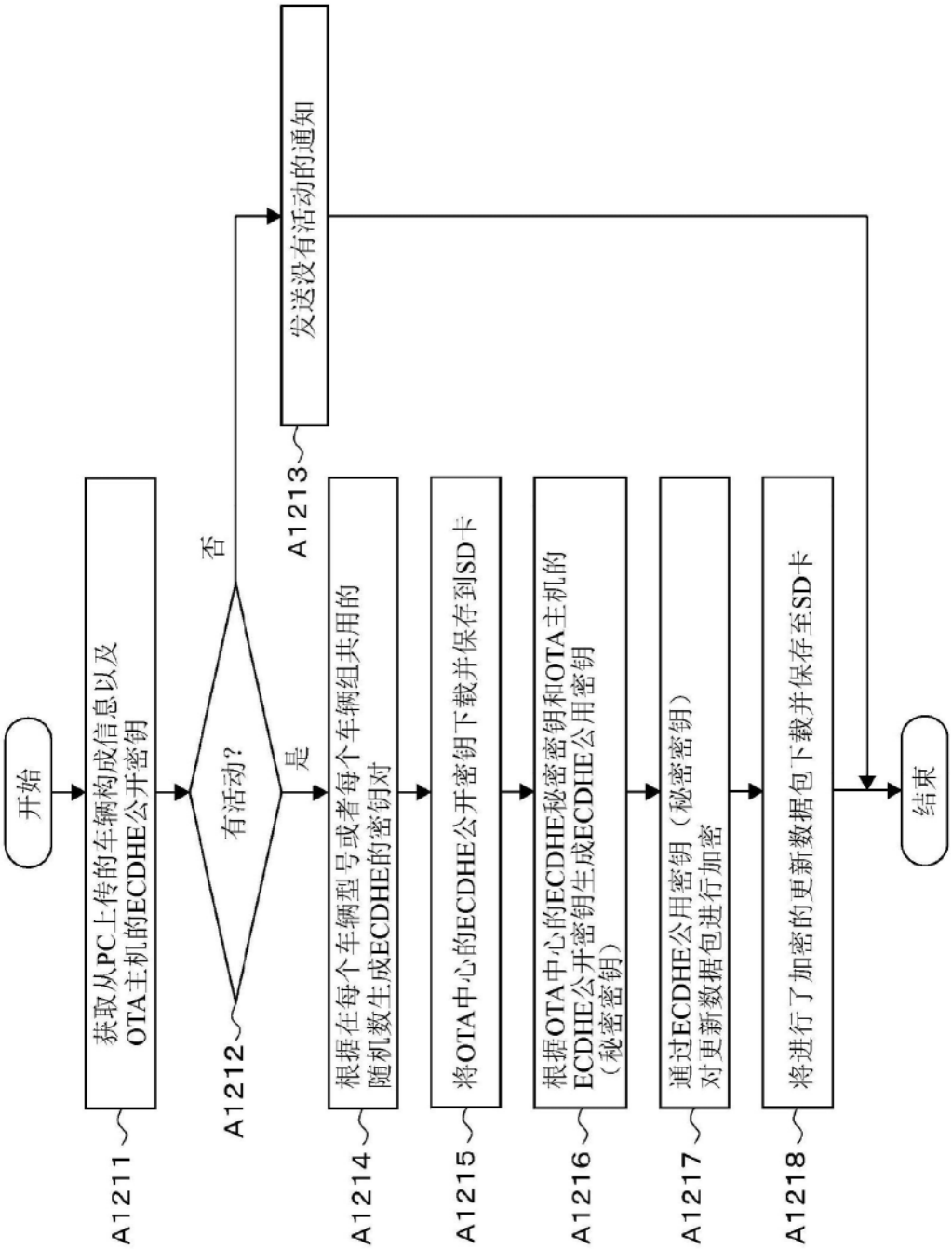

开始
获取从PC上传的车辆构成信息以及OTA主机的ECDHE公开密钥
A1211
有活动?
A1212
否
是
发送没有活动的通知
A1213
根据在每个车辆型号或者每个车辆组共用的随机数生成ECDHE的密钥对
A1214
将OTA中心的ECDHE公开密钥下载并保存到SD卡
A1215
根据OTA中心的ECDHE秘密密钥和OTA主机的ECDHE公开密钥生成ECDHE公用密钥（秘密密钥）
A1216
通过ECDHE公用密钥（秘密密钥）对更新数据包进行加密
A1217
将进行了加密的更新数据包下载并保存至SD卡
A1218
结束

图180

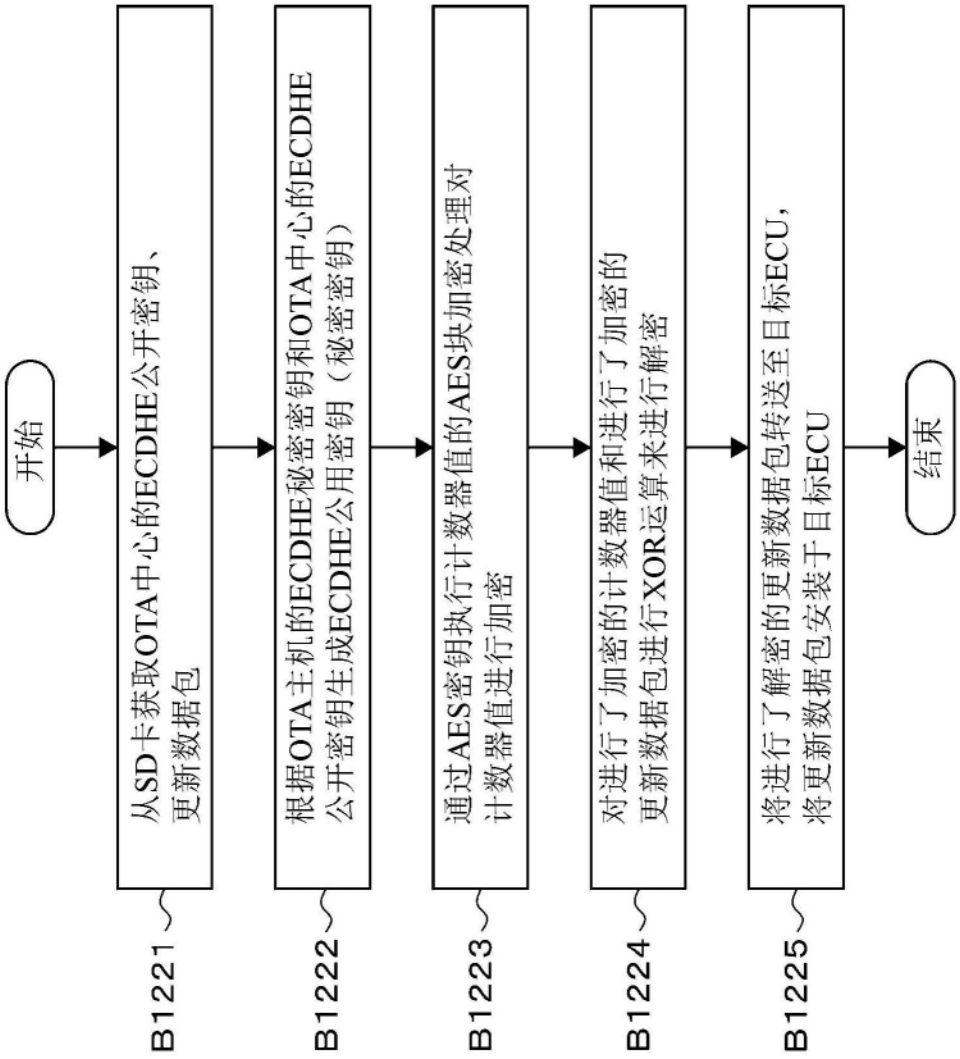

开始
从SD卡获取OTA中心的ECDHE公开密钥、
更新数据包
B1221
根据OTA主机的ECDHE秘密密钥和OTA中心的ECDHE
公开密钥生成ECDHE公用密钥（秘密密钥）
B1222
通过AES密钥执行计数器值的AES块加密处理对
计数器值进行加密
B1223
对进行了加密的计数器值和进行了加密的
更新数据包进行XOR运算来进行解密
B1224
将进行了解密的更新数据包转送至目标ECU，
将更新数据包安装于目标ECU
B1225
结束

图181

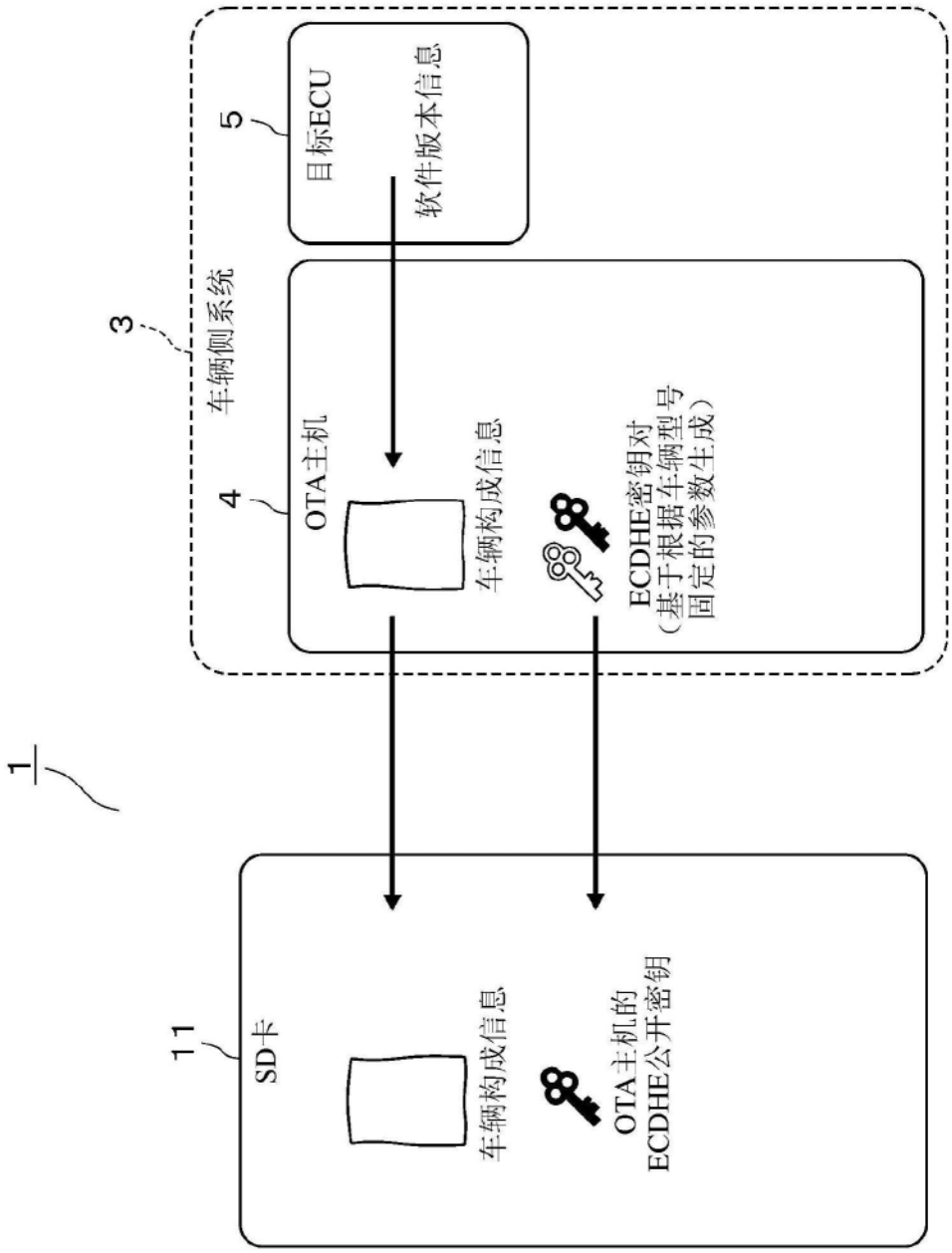

1
3
车辆侧系统
4
OTA主机
车辆构成信息
ECDHE密钥对
（基于根据车辆型号
固定的参数生成）
5
目标ECU
软件版本信息
11
SD卡
车辆构成信息
OTA主机的
ECDHE公开密钥

图182

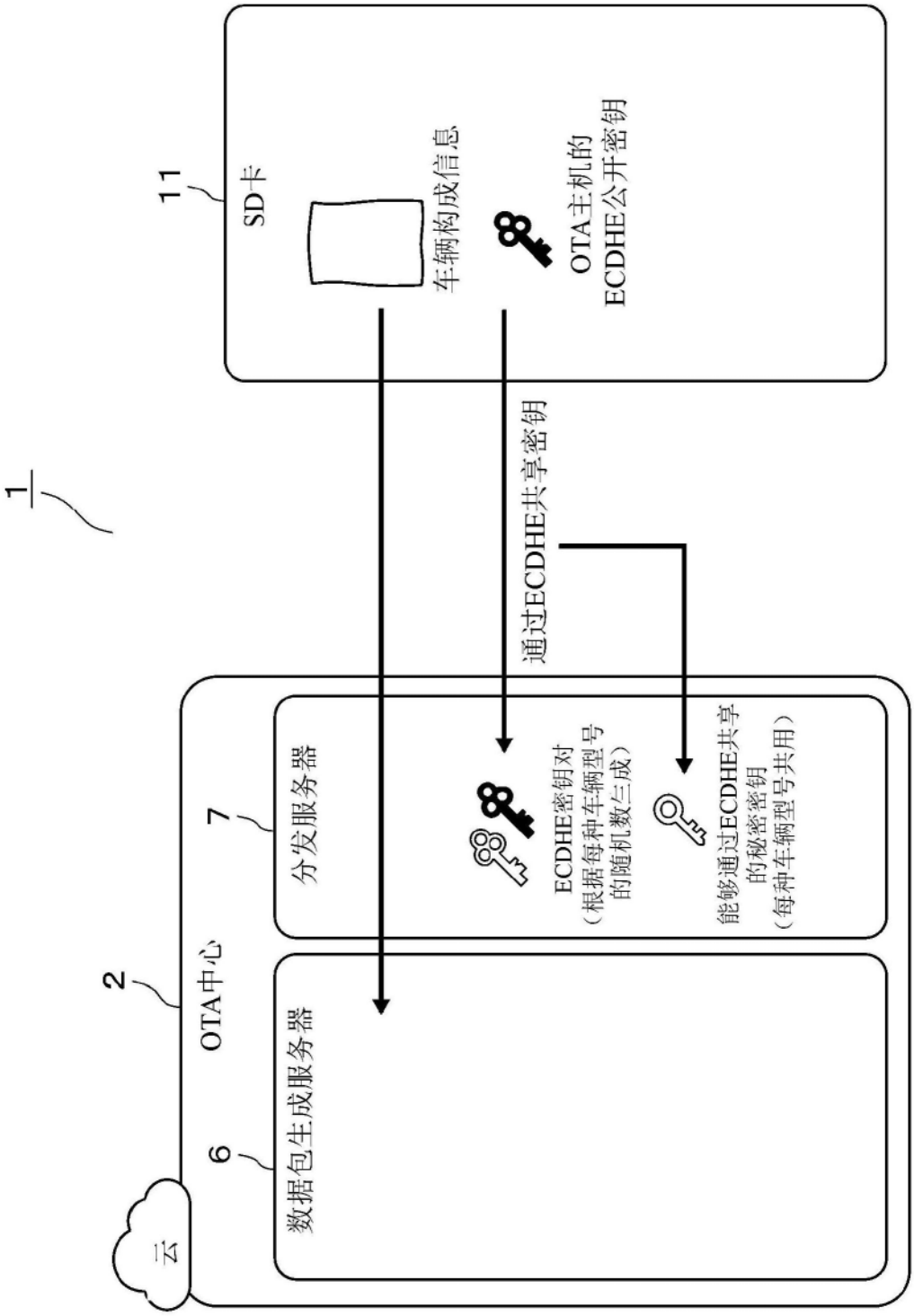

1
11
SD卡
车辆构成信息
OTA主机的
ECDHE公开密钥
通过ECDHE共享密钥
2
OTA中心
7
分发服务器
ECDHE密钥对
（根据每种车辆型号
的随机数生成）
能够通过ECDHE共享
的秘密密钥
（每种车辆型号共用）
6
数据包生成服务器
云

图183

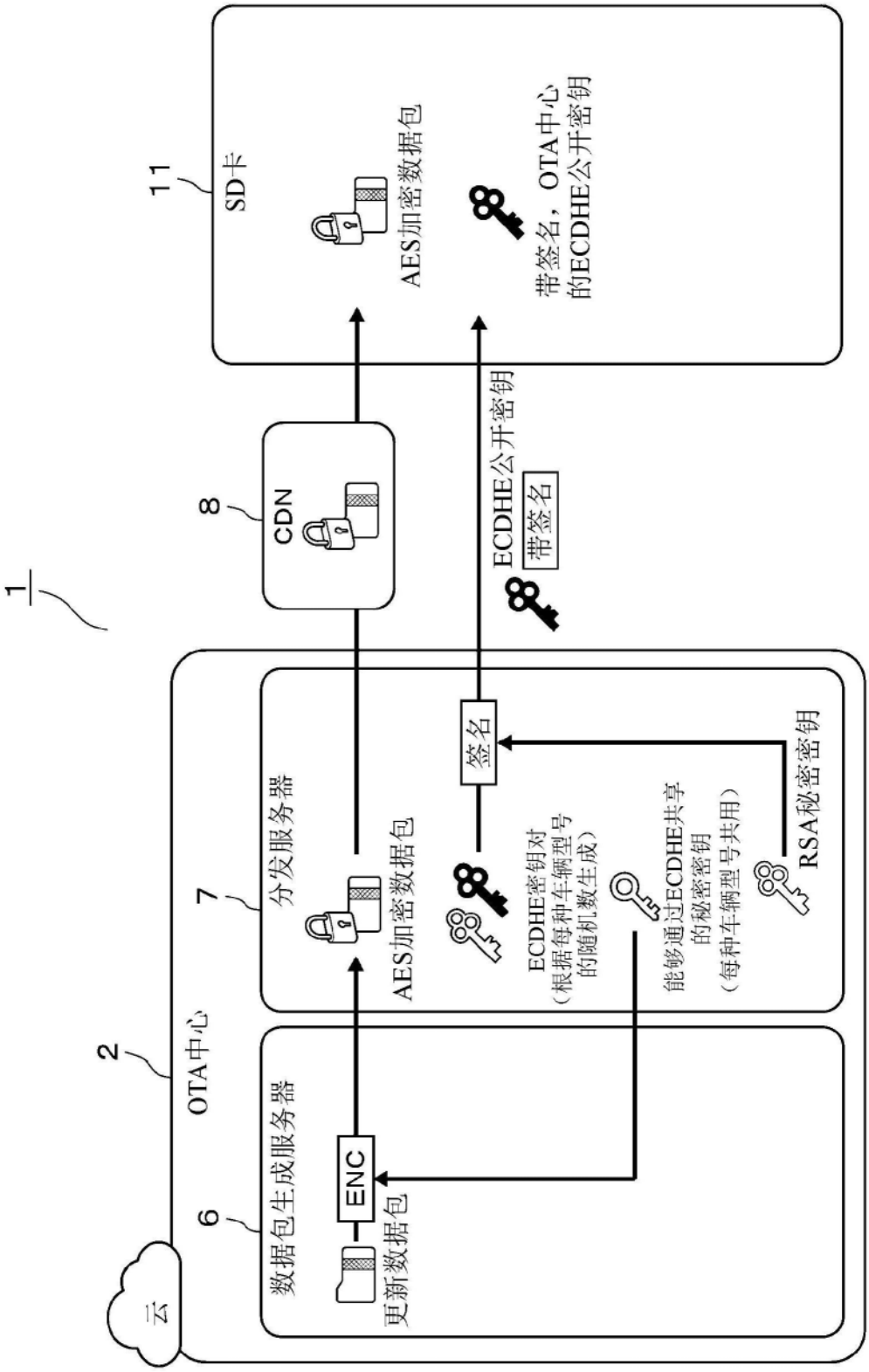

1
2
OTA中心
云
6
数据包生成服务器
ENC
更新数据包
7
分发服务器
AES加密数据包
ECDHE密钥对
（根据每种车辆型号
的随机数生成）
签名
能够通过ECDHE共享
的秘密密钥
（每种车辆型号共用）
RSA秘密密钥
8
CDN
ECDHE公开密钥
带签名
11
SD卡
AES加密数据包
带签名，OTA中心
的ECDHE公开密钥

图184

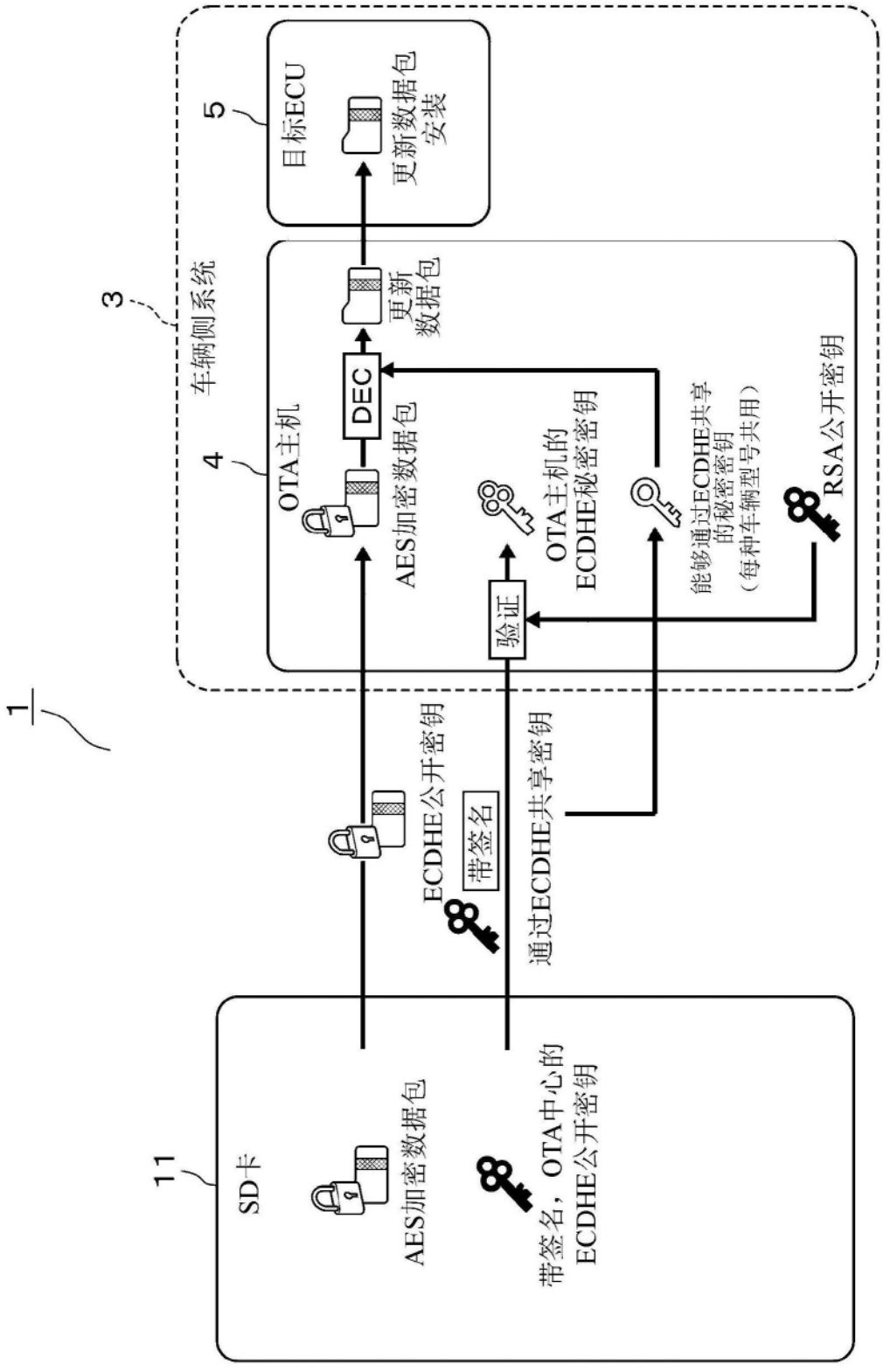

1
3
车辆侧系统
4
OTA主机
AES加密数据包
DEC
更新数据包
5
目标ECU
更新数据包安装
验证
OTA主机的ECDHE秘密密钥
能够通过ECDHE共享的秘密密钥（每种车辆型号共用）
RSA公开密钥
ECDHE公开密钥
带签名
通过ECDHE共享密钥
11
SD卡
AES加密数据包
带签名，OTA中心的ECDHE公开密钥

图185

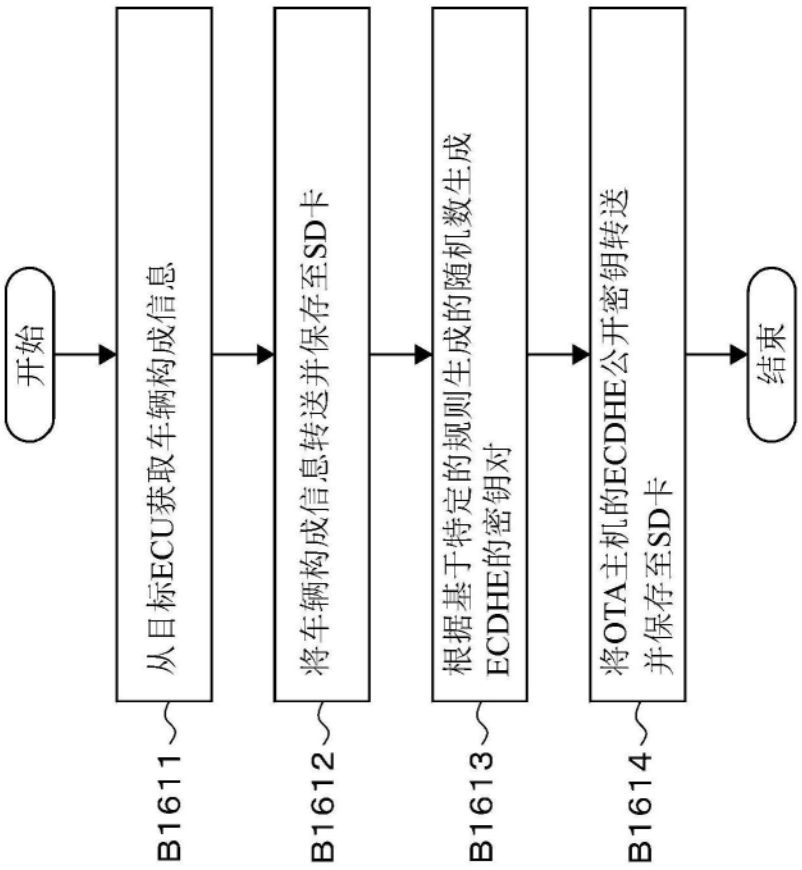

开始
从目标ECU获取车辆构成信息
将车辆构成信息转送并保存至SD卡
根据基于特定的规则生成的随机数生成ECDHE的密钥对
将OTA主机的ECDHE公开密钥转送并保存至SD卡
结束
B1611
B1612
B1613
B1614

图186

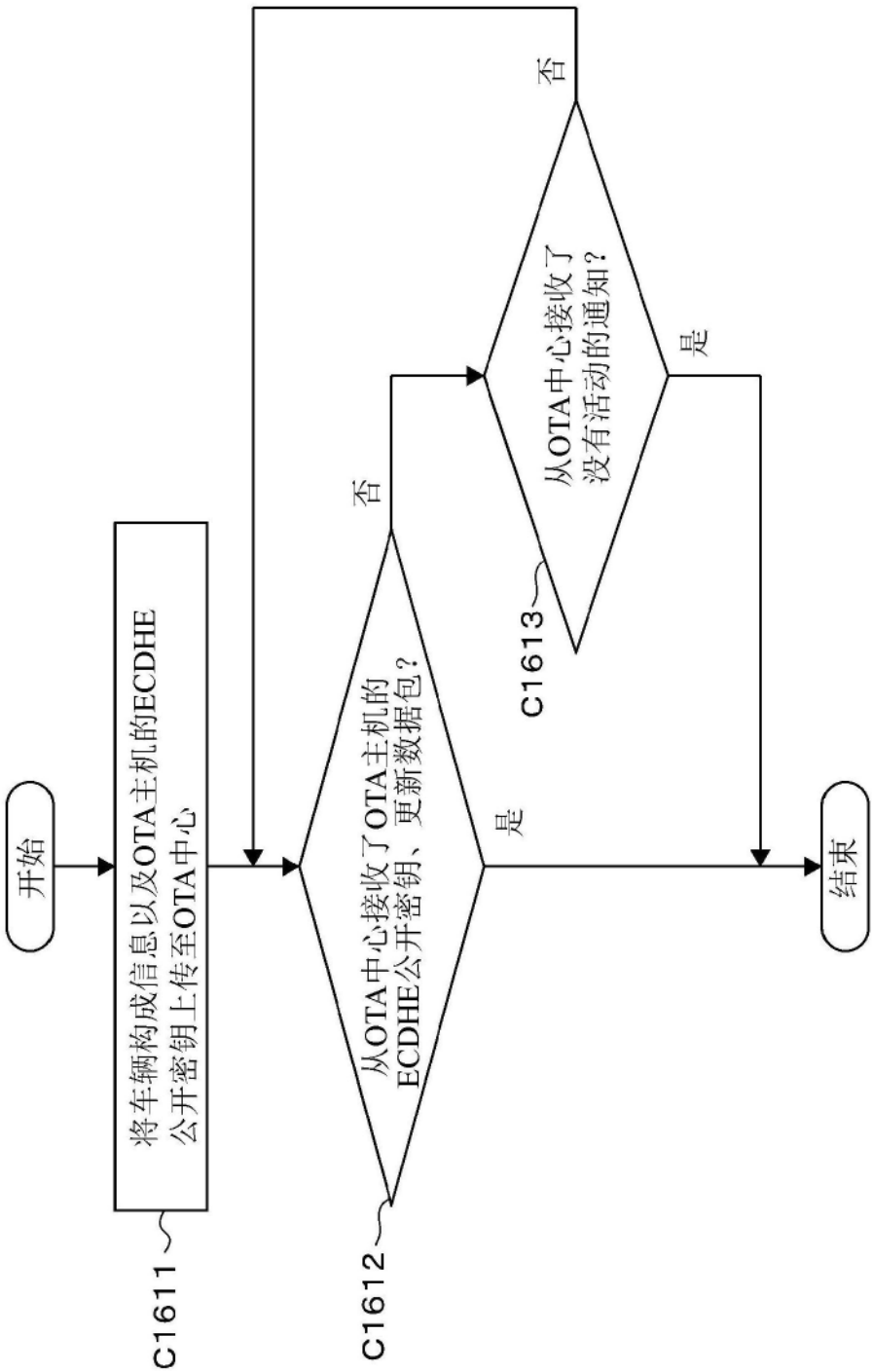

开始
将车辆构成信息以及OTA主机的ECDHE公开密钥上传至OTA中心
C1611
从OTA中心接收了OTA主机的ECDHE公开密钥、更新数据包？
C1612
否
是
从OTA中心接收了没有活动的通知？
C1613
否
是
结束

图187

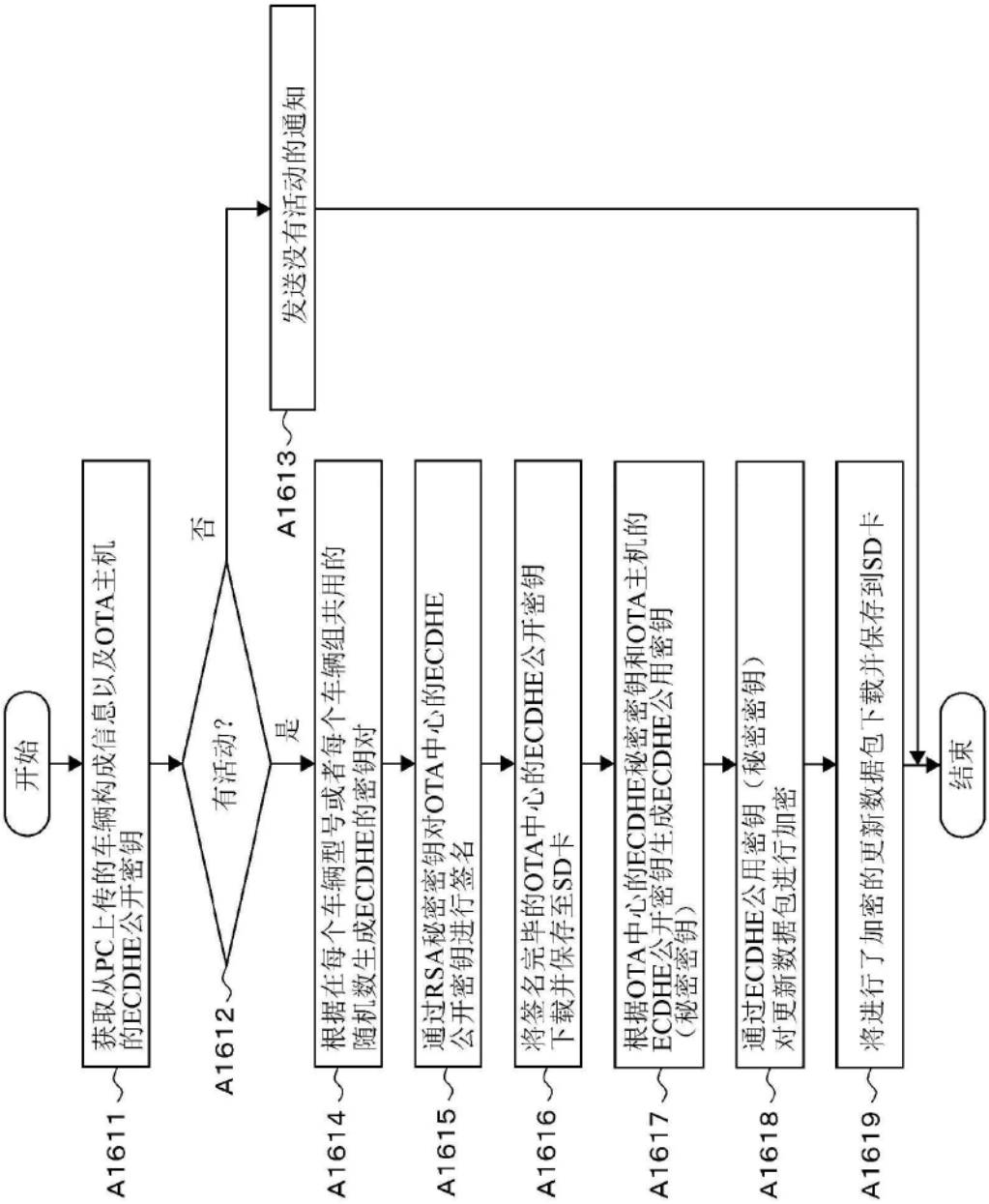

开始
获取从PC上传的车辆构成信息以及OTA主机的ECDHE公开密钥
A1611
有活动?
A1612
否
是
发送没有活动的通知
A1613
根据在每个车辆型号或者每个车辆组共用的随机数生成ECDHE的密钥对
A1614
通过RSA秘密密钥对OTA中心的ECDHE公开密钥进行签名
A1615
将签名完毕的OTA中心的ECDHE公开密钥下载并保存至SD卡
A1616
根据OTA中心的ECDHE秘密密钥和OTA主机的ECDHE公开密钥生成ECDHE公用密钥（秘密密钥）
A1617
通过ECDHE公用密钥（秘密密钥）对更新数据包进行加密
A1618
将进行了加密的更新数据包下载并保存到SD卡
A1619
结束

图188

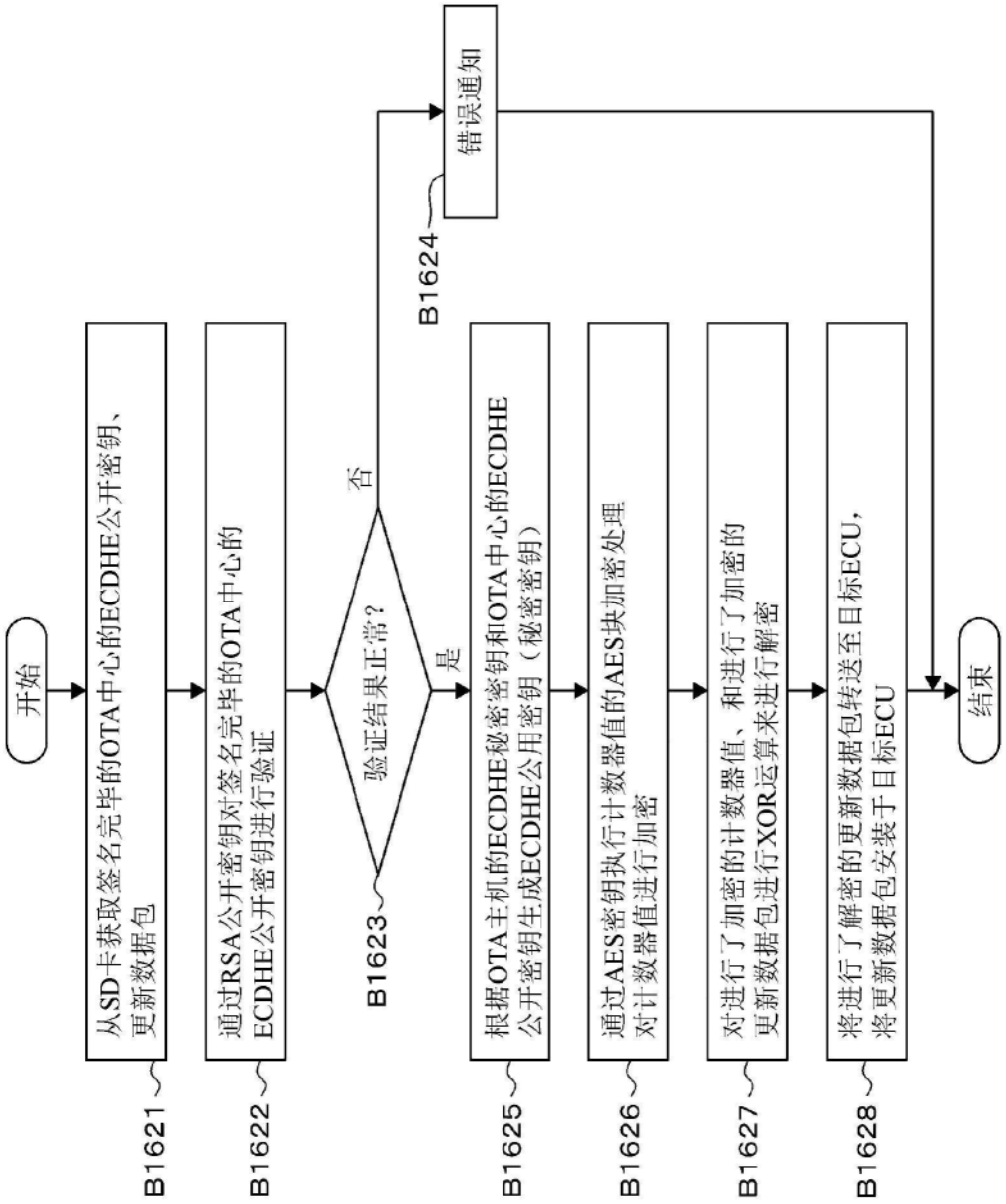

开始
从SD卡获取签名完毕的OTA中心的ECDHE公开密钥、更新数据包
B1621
通过RSA公开密钥对签名完毕的OTA中心的ECDHE公开密钥进行验证
B1622
验证结果正常？
B1623
否
是
错误通知
B1624
根据OTA主机的ECDHE秘密密钥和OTA中心的ECDHE公开密钥生成ECDHE公用密钥（秘密密钥）
B1625
通过AES密钥执行计数器值的AES块加密处理对计数器值进行加密
B1626
对进行了加密的计数器值、和进行了加密的更新数据包进行XOR运算来进行解密
B1627
将进行了解密的更新数据包转送至目标ECU，将更新数据包安装于目标ECU
B1628
结束

图189

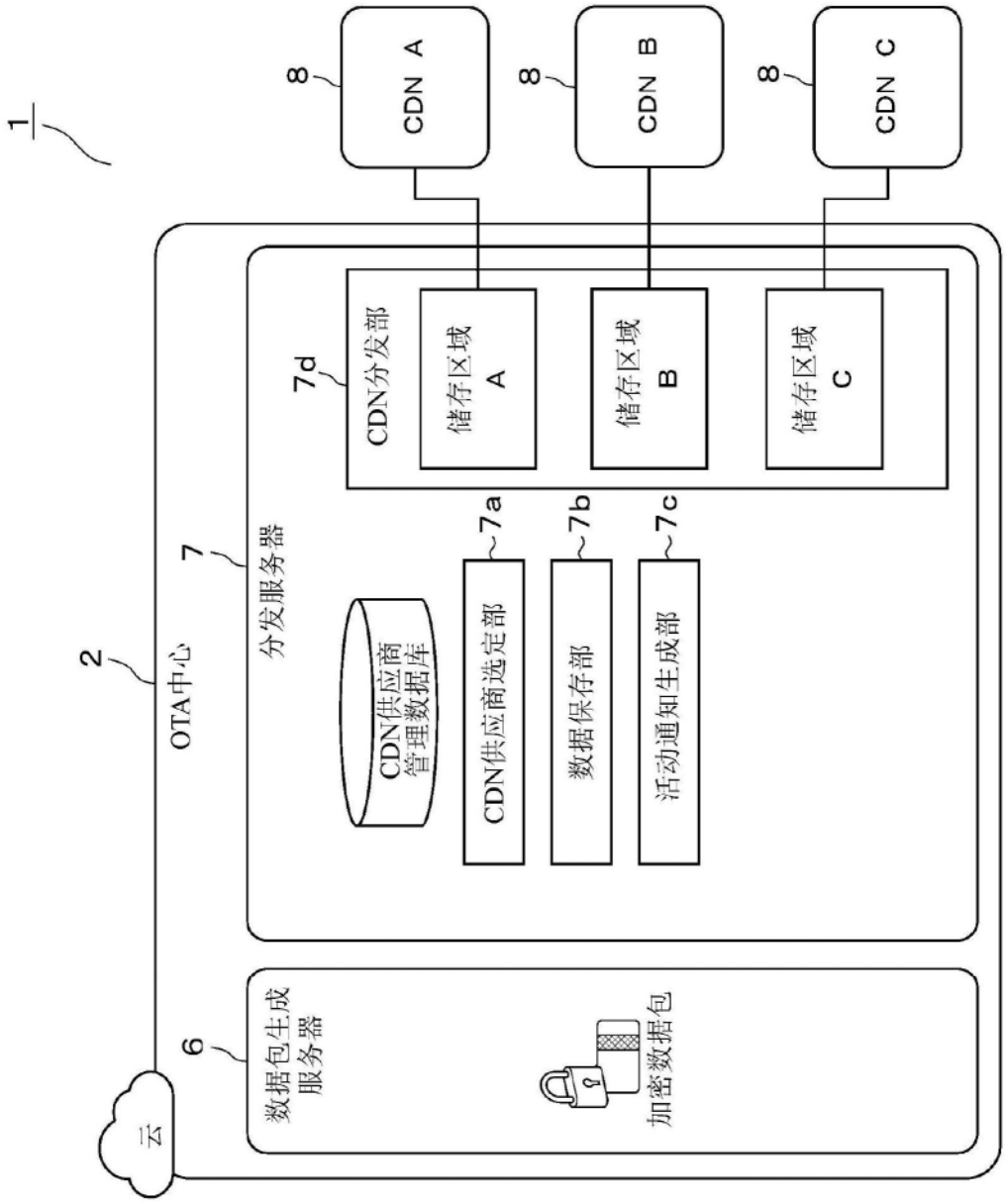

1
8
CDN A
8
CDN B
8
CDN C
2
OTA中心
7
分发服务器
7d
CDN分发部
储存区域 A
储存区域 B
储存区域 C
CDN供应商管理数据库
7a
CDN供应商选定部
7b
数据保存部
7c
活动通知生成部
6
数据包生成服务器
加密数据包
云

图190

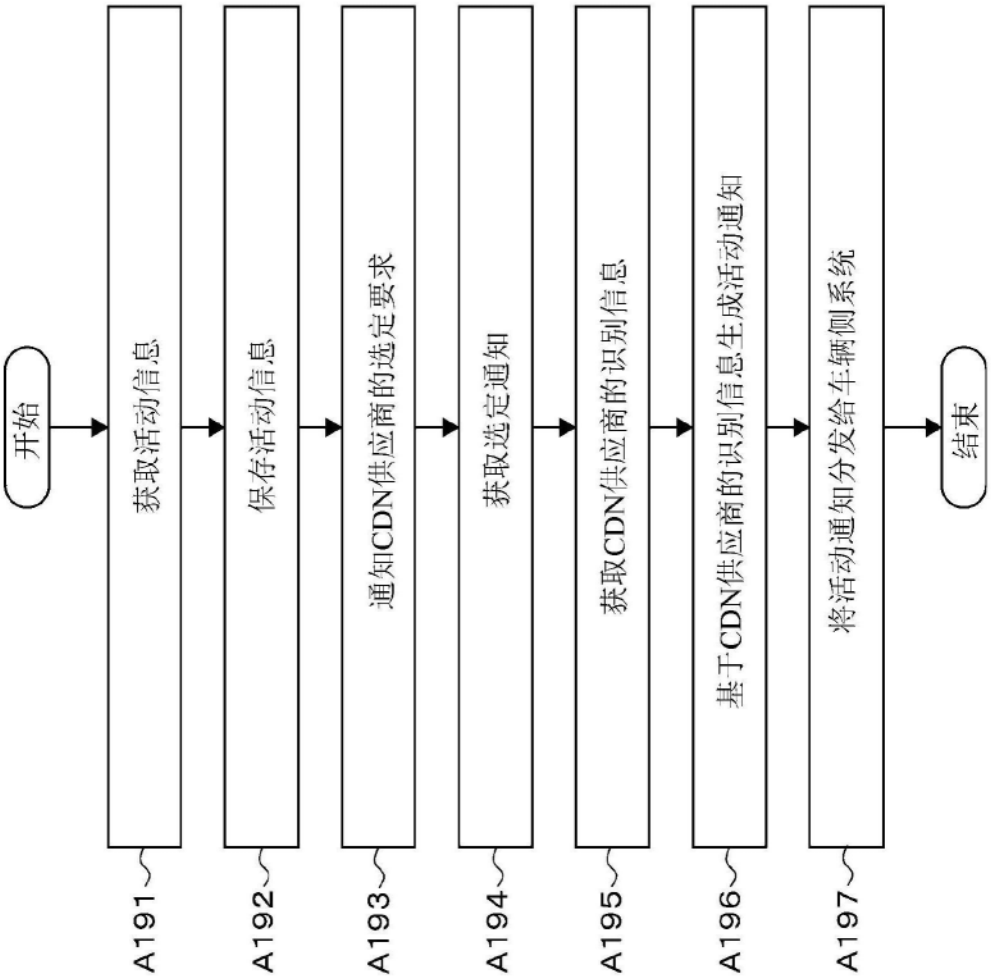

开始
获取活动信息
保存活动信息
通知CDN供应商的选定要求
获取选定通知
获取CDN供应商的识别信息
基于CDN供应商的识别信息生成活动通知
将活动通知分发给车辆侧系统
结束
A191
A192
A193
A194
A195
A196
A197

图191

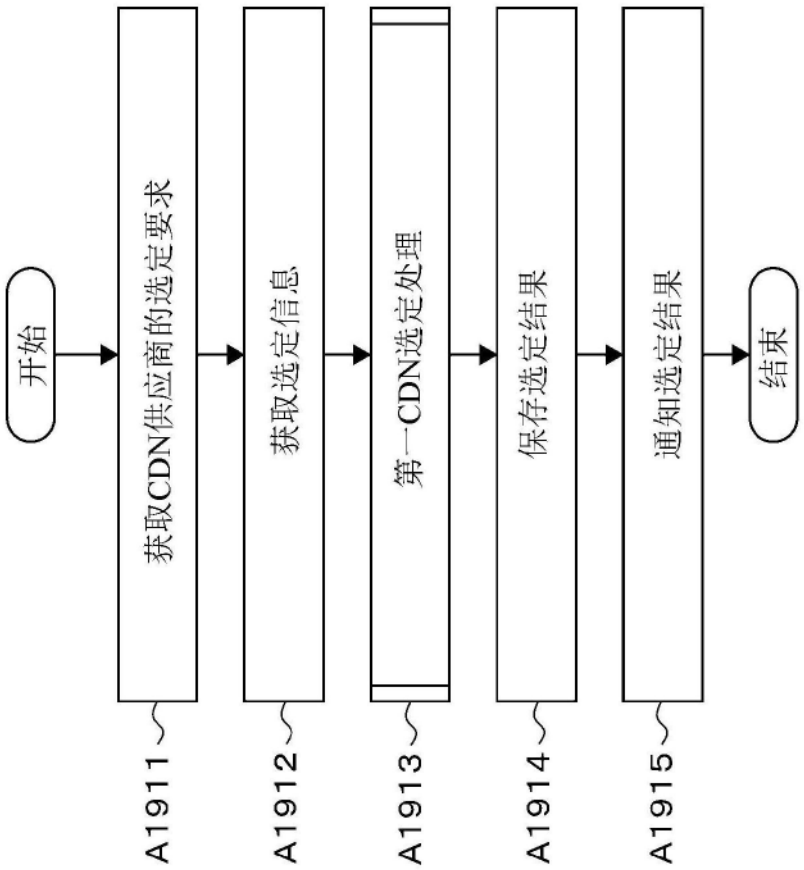

开始
获取CDN供应商的选定要求
获取选定信息
第一CDN选定处理
保存选定结果
通知选定结果
结束
A1911
A1912
A1913
A1914
A1915

图192

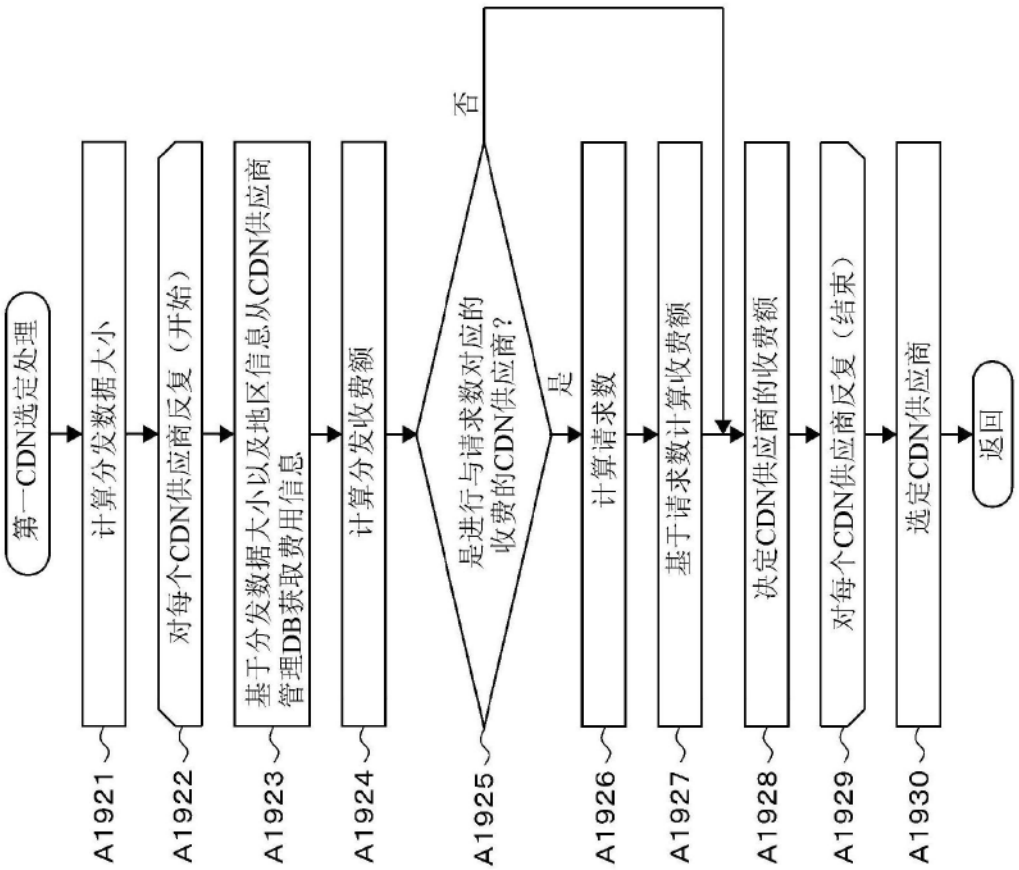

第一CDN选定处理
计算分发数据大小
对每个CDN供应商反复（开始）
基于分发数据大小以及地区信息从CDN供应商管理DB获取费用信息
计算分发收费额
是进行与请求数对应的收费的CDN供应商？
否
是
计算请求数
基于请求数计算收费额
决定CDN供应商的收费额
对每个CDN供应商反复（结束）
选定CDN供应商
返回
A1921
A1922
A1923
A1924
A1925
A1926
A1927
A1928
A1929
A1930

图193

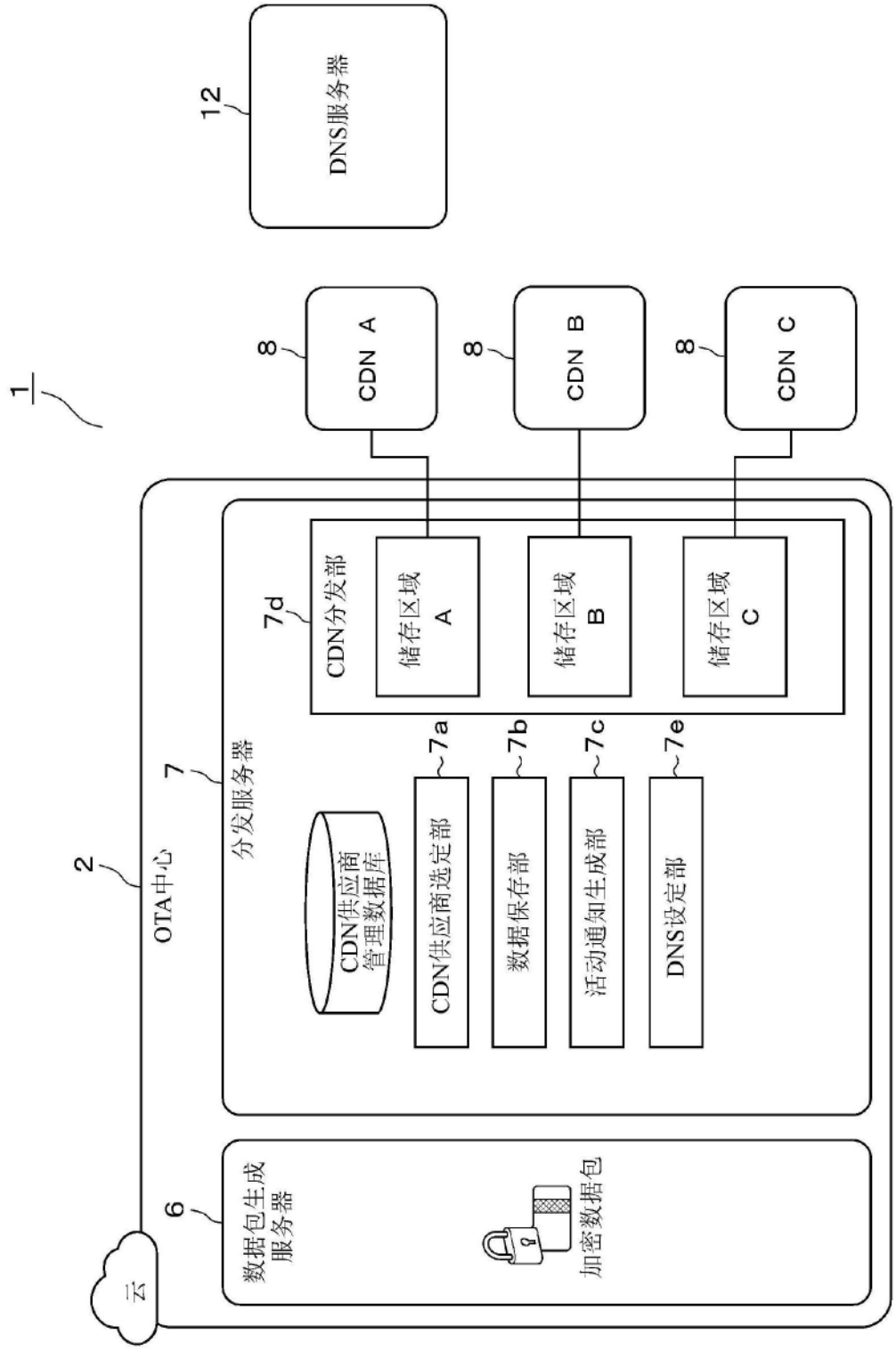

1
2
OTA中心
云
6
数据包生成
服务器
加密数据包
7
分发服务器
CDN供应商
管理数据库
7a
CDN供应商选定部
7b
数据保存部
7c
活动通知生成部
7e
DNS设定部
7d
CDN分发部
储存区域
A
储存区域
B
储存区域
C
8
CDN A
8
CDN B
8
CDN C
12
DNS服务器

图194

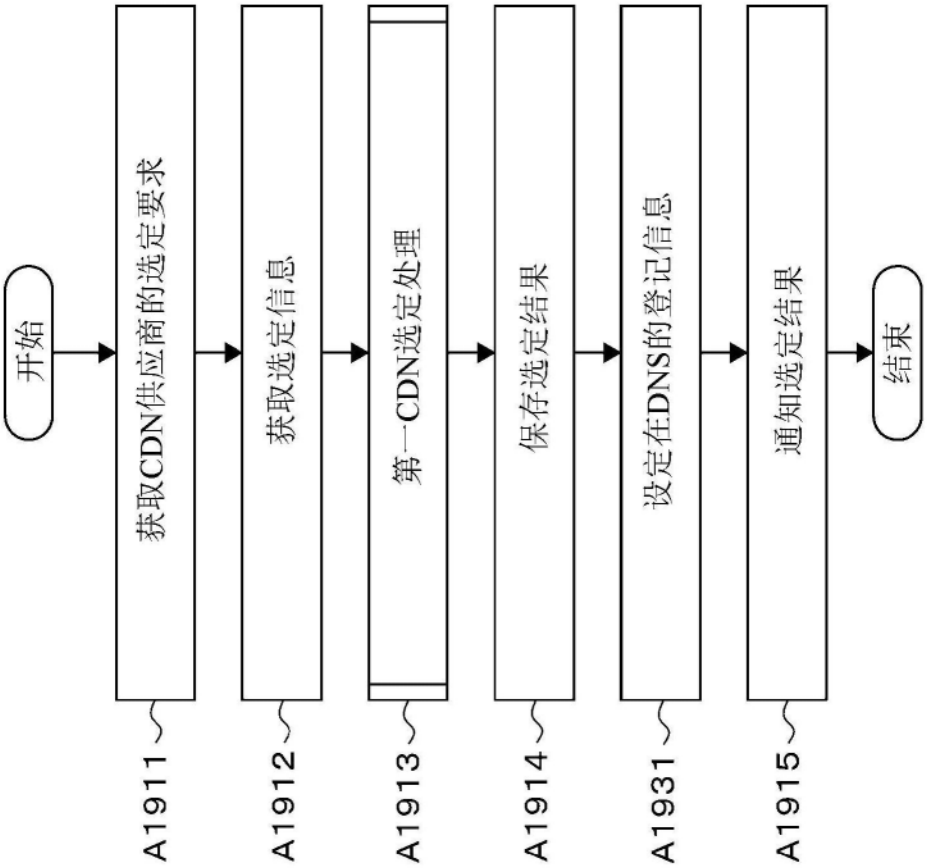

开始
获取CDN供应商的选定要求
获取选定信息
第一CDN选定处理
保存选定结果
设定在DNS的登记信息
通知选定结果
结束
A1911
A1912
A1913
A1914
A1931
A1915

图195

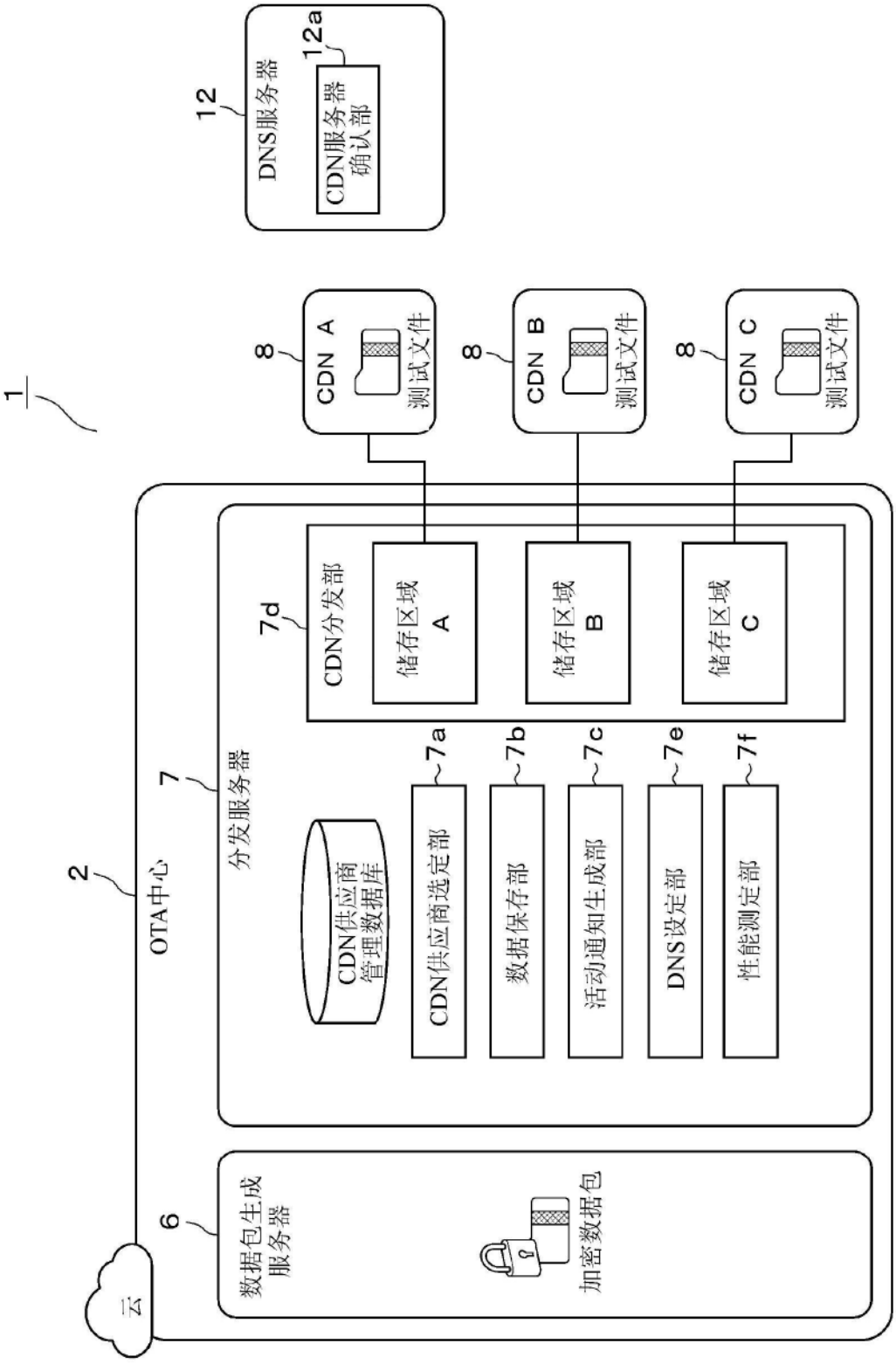

1
12
DNS服务器
12a
CDN服务器
确认部
8
CDN A
测试文件
8
CDN B
测试文件
8
CDN C
测试文件
2
OTA中心
7
分发服务器
7d
CDN分发部
储存区域
A
储存区域
B
储存区域
C
CDN供应商
管理数据库
7a
CDN供应商选定部
7b
数据保存部
7c
活动通知生成部
7e
DNS设定部
7f
性能测定部
6
数据包生成
服务器
加密数据包
云

图196

选择表格

CDN供应商	分发时间	分发标志	成本位次
AAA	Xms	FALSE	1
BBB	Yms	TRUE	2
CCC	Zms	TRUE	3

图197

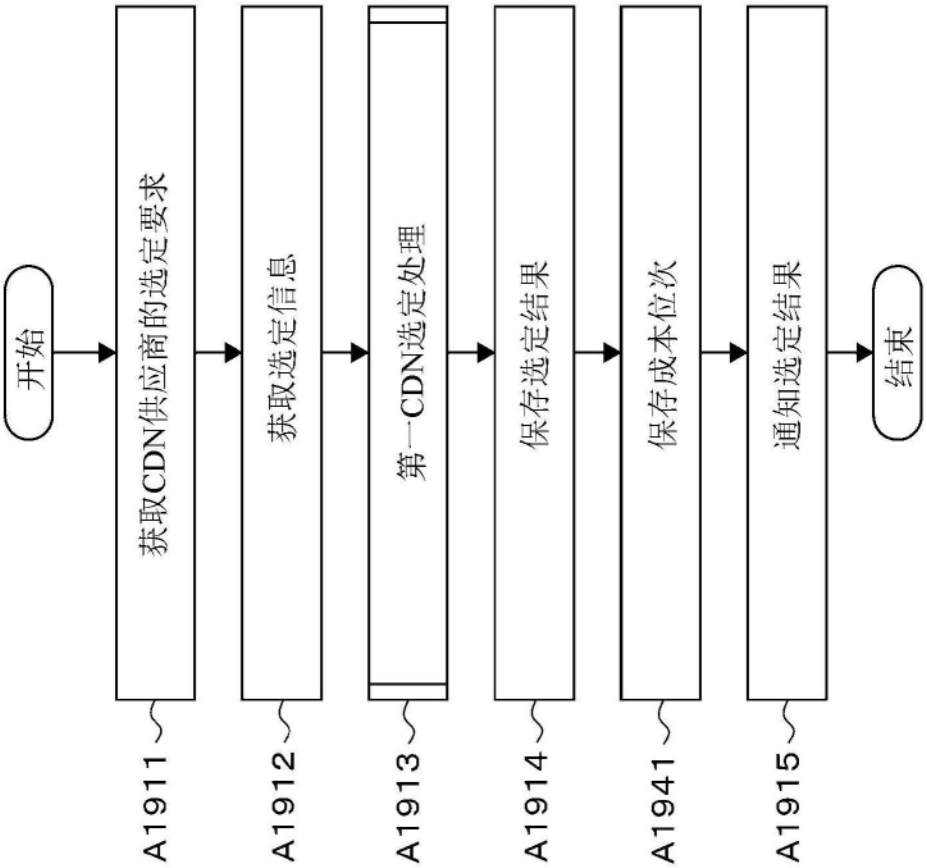

开始
获取CDN供应商的选定要求
获取选定信息
第一CDN选定处理
保存选定结果
保存成本位次
通知选定结果
结束
A1911
A1912
A1913
A1914
A1941
A1915

图198

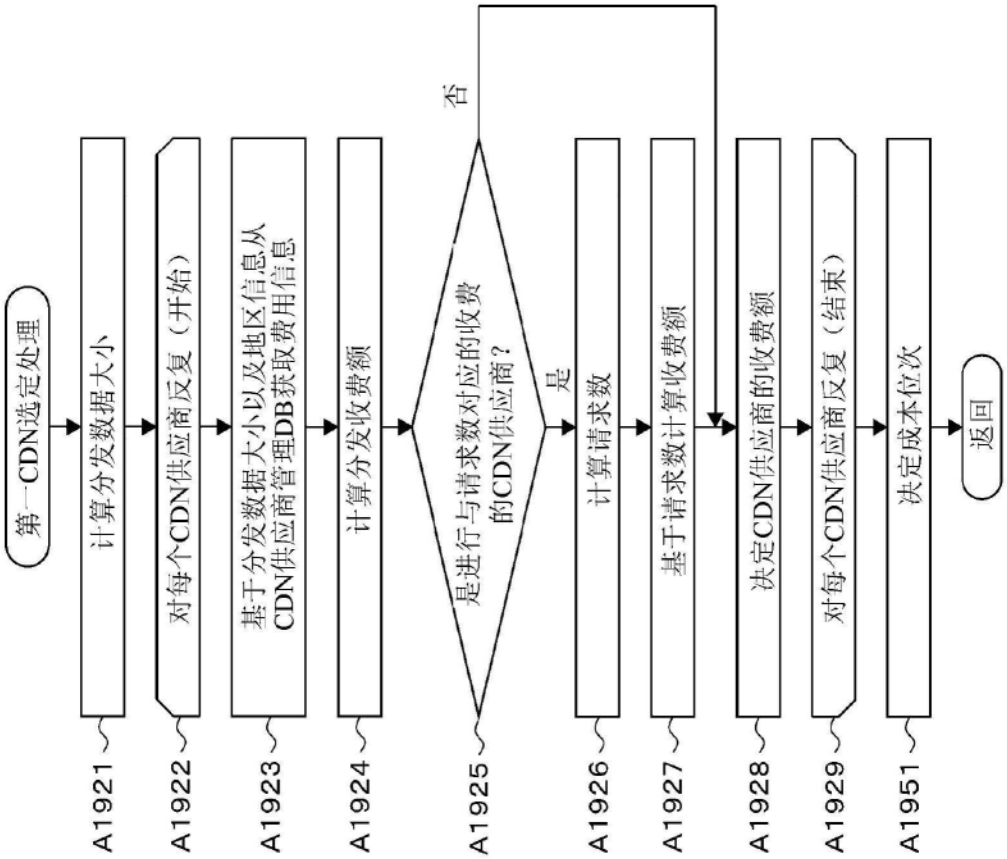

第一CDN选定处理
计算分发数据大小
对每个CDN供应商反复（开始）
基于分发数据大小以及地区信息从CDN供应商管理DB获取费用信息
计算分发收费额
是进行与请求数对应的收费的CDN供应商？
否
是
计算请求数
基于请求数计算收费额
决定CDN供应商的收费额
对每个CDN供应商反复（结束）
决定成本位次
返回
A1921
A1922
A1923
A1924
A1925
A1926
A1927
A1928
A1929
A1951

图199

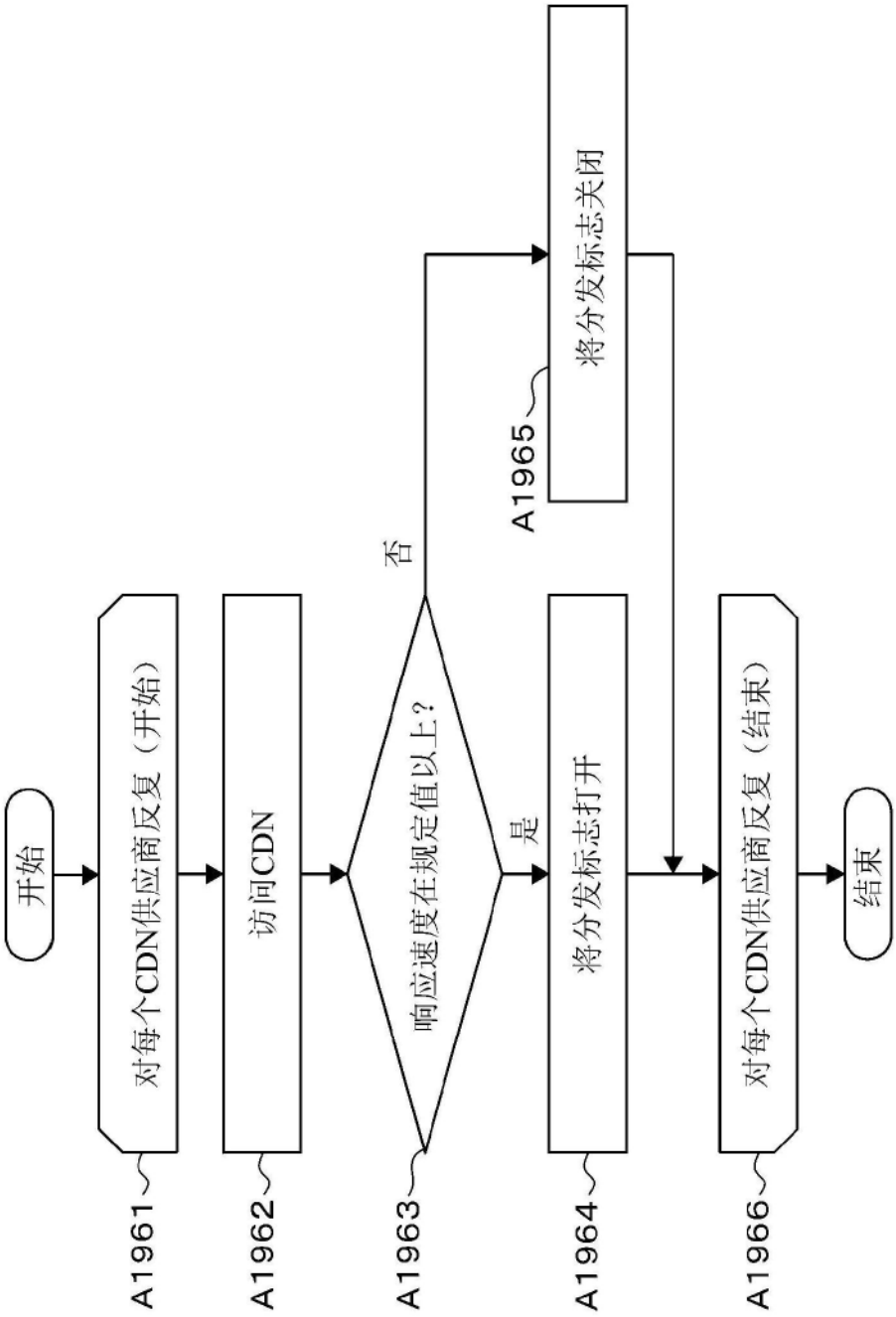

开始
对每个CDN供应商反复（开始）
A1961
访问CDN
A1962
响应速度在规定值以上？
A1963
否
是
将分发标志关闭
A1965
将分发标志打开
A1964
对每个CDN供应商反复（结束）
A1966
结束

图200

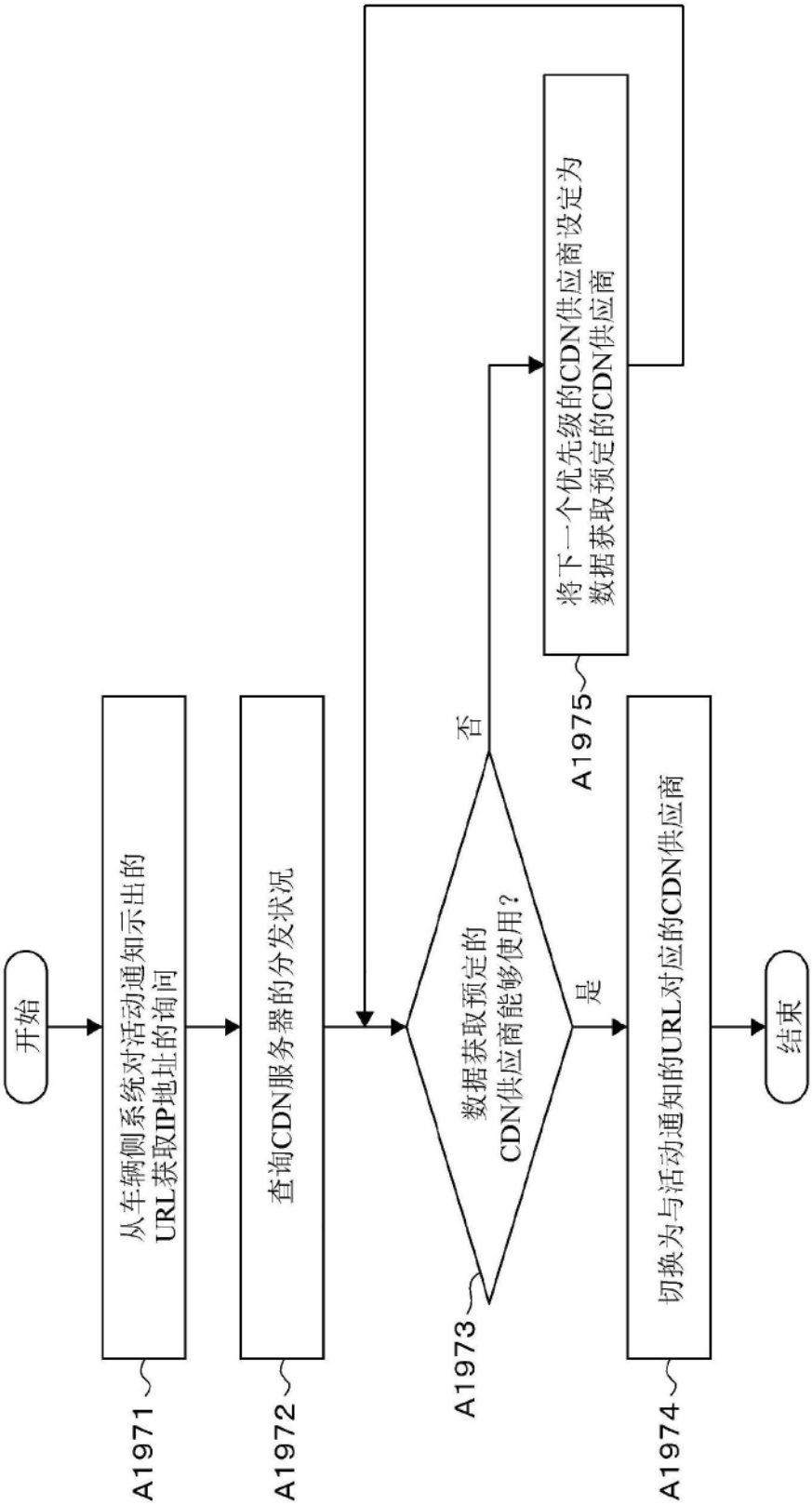

开始
从车辆侧系统对活动通知示出的URL获取IP地址的询问
A1971
查询CDN服务器的分发状况
A1972
数据获取预定的CDN供应商能够使用？
A1973
否
是
将下一个优先级的CDN供应商设定为数据获取预定的CDN供应商
A1975
切换为与活动通知的URL对应的CDN供应商
A1974
结束

图201

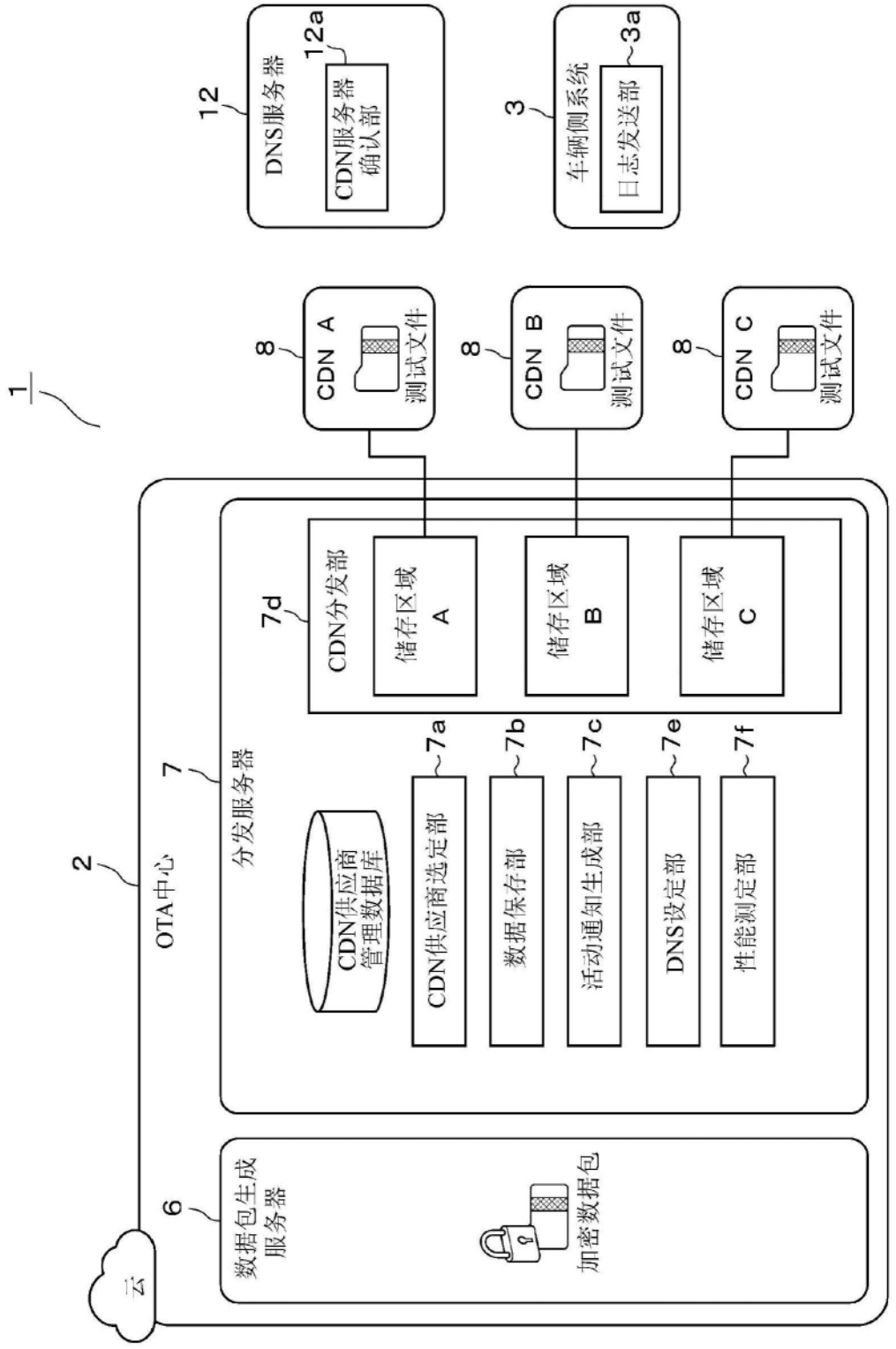

1
2
OTA中心
6
数据包生成服务器
加密数据包
云
7
分发服务器
7a
CDN供应商选定部
7b
数据保存部
7c
活动通知生成部
7e
DNS设定部
7f
性能测定部
CDN供应商管理数据库
7d
CDN分发部
储存区域A
储存区域B
储存区域C
8
CDN A
测试文件
8
CDN B
测试文件
8
CDN C
测试文件
12
DNS服务器
12a
CDN服务器确认部
3
车辆侧系统
3a
日志发送部

图202

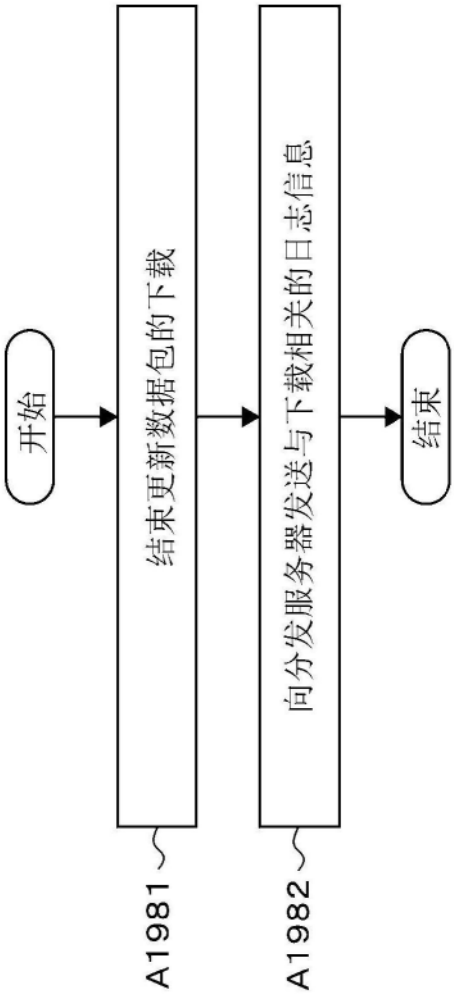


图203

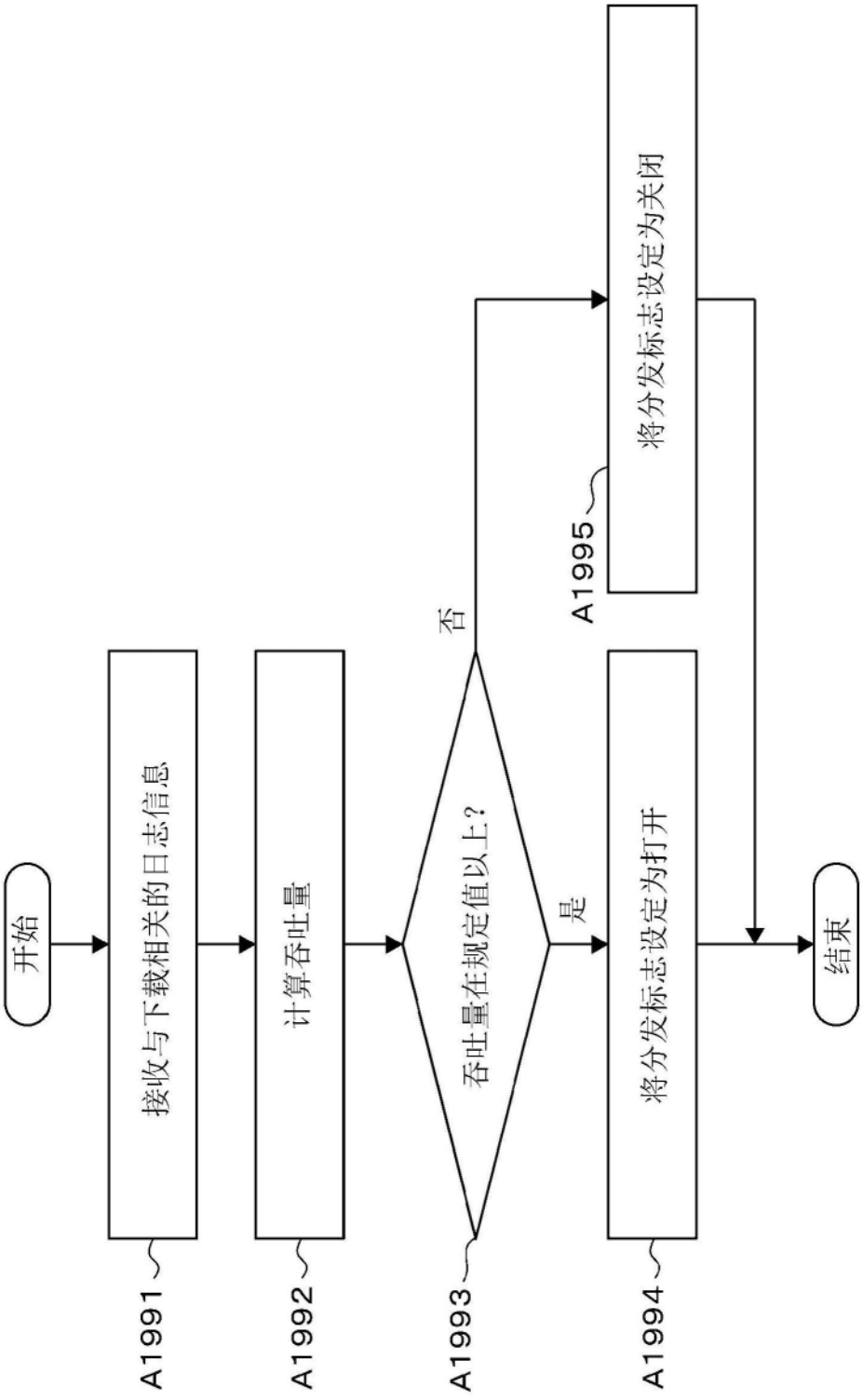

开始
接收与下载相关的日志信息
计算吞吐量
吞吐量在规定值以上？
否
是
将分发标志设定为关闭
将分发标志设定为打开
结束
A1991
A1992
A1993
A1994
A1995

图204

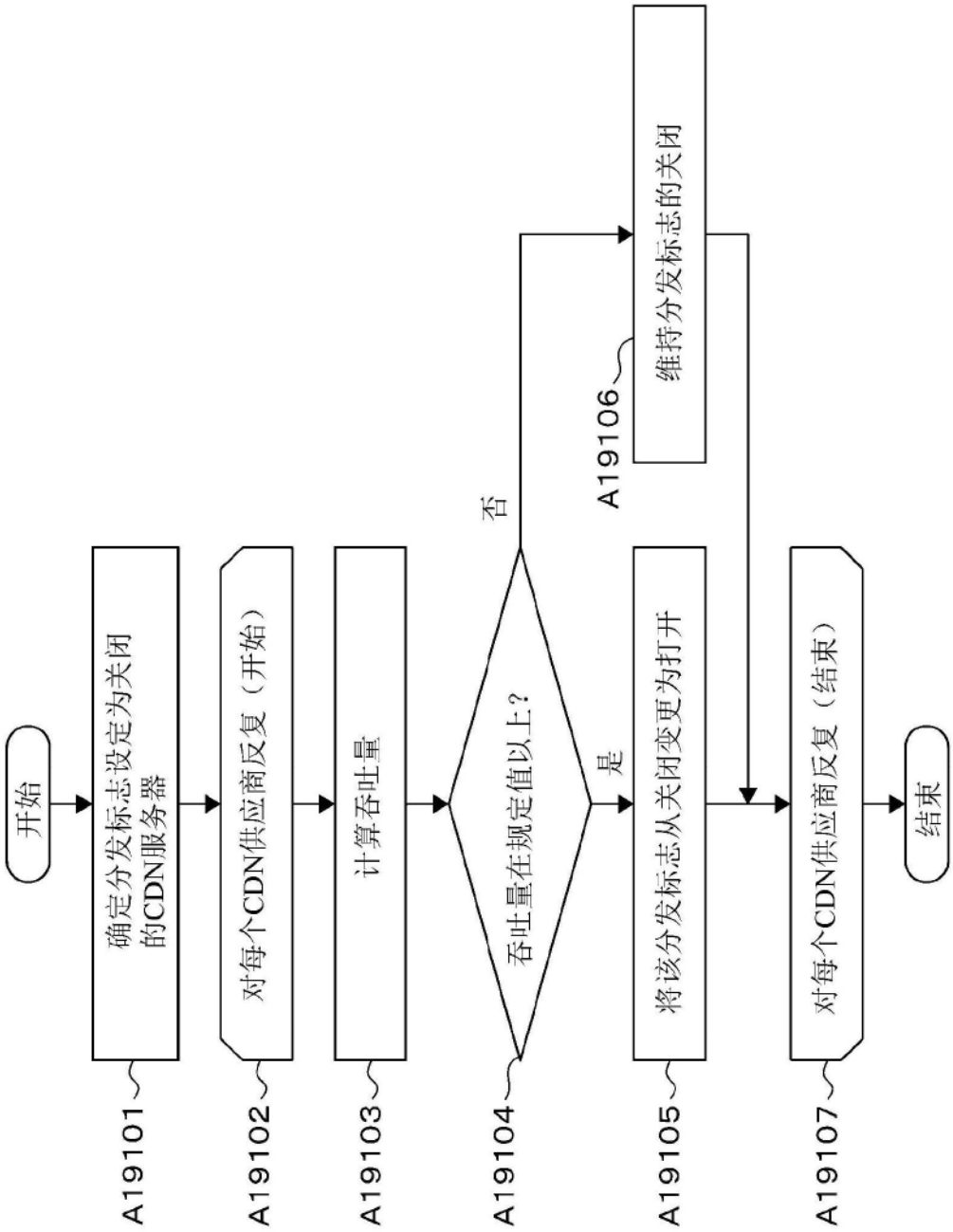

开始
确定分发标志设定为关闭的CDN服务器
对每个CDN供应商反复（开始）
计算吞吐量
吞吐量在规定值以上?
否
是
维持分发标志的关闭
将该分发标志从关闭变更为打开
对每个CDN供应商反复（结束）
结束
A19101
A19102
A19103
A19104
A19105
A19106
A19107

图205

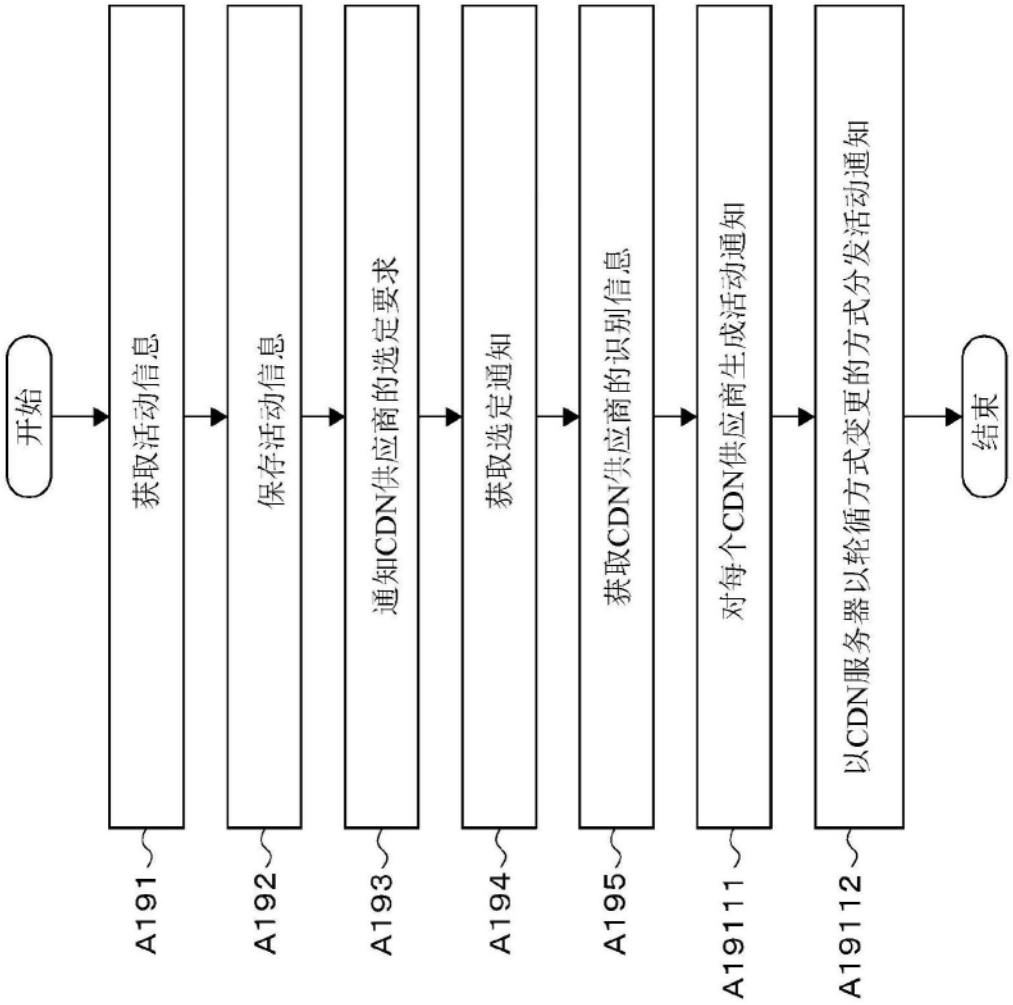

开始
获取活动信息
保存活动信息
通知CDN供应商的选定要求
获取选定通知
获取CDN供应商的识别信息
对每个CDN供应商生成活动通知
以CDN服务器以轮循方式变更的方式分发活动通知
结束
A191
A192
A193
A194
A195
A19111
A19112

图206

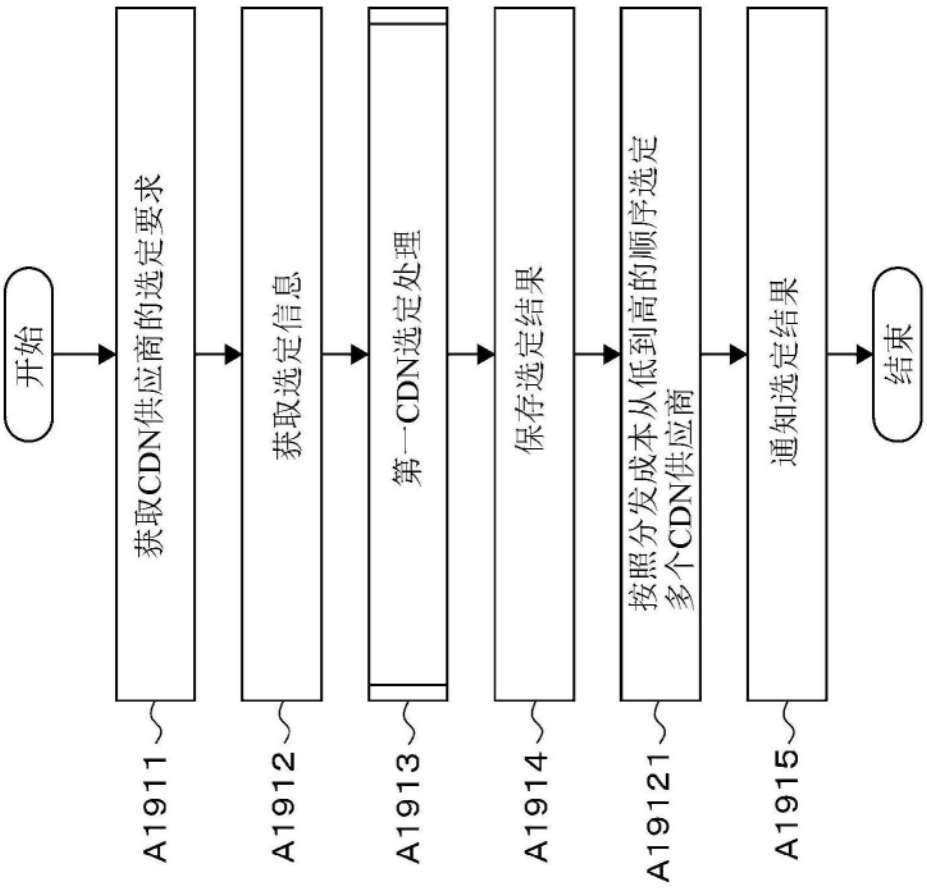

开始
获取CDN供应商的选定要求
获取选定信息
第一CDN选定处理
保存选定结果
按照分发成本从低到高的顺序选定多个CDN供应商
通知选定结果
结束
A1911
A1912
A1913
A1914
A19121
A1915

图207

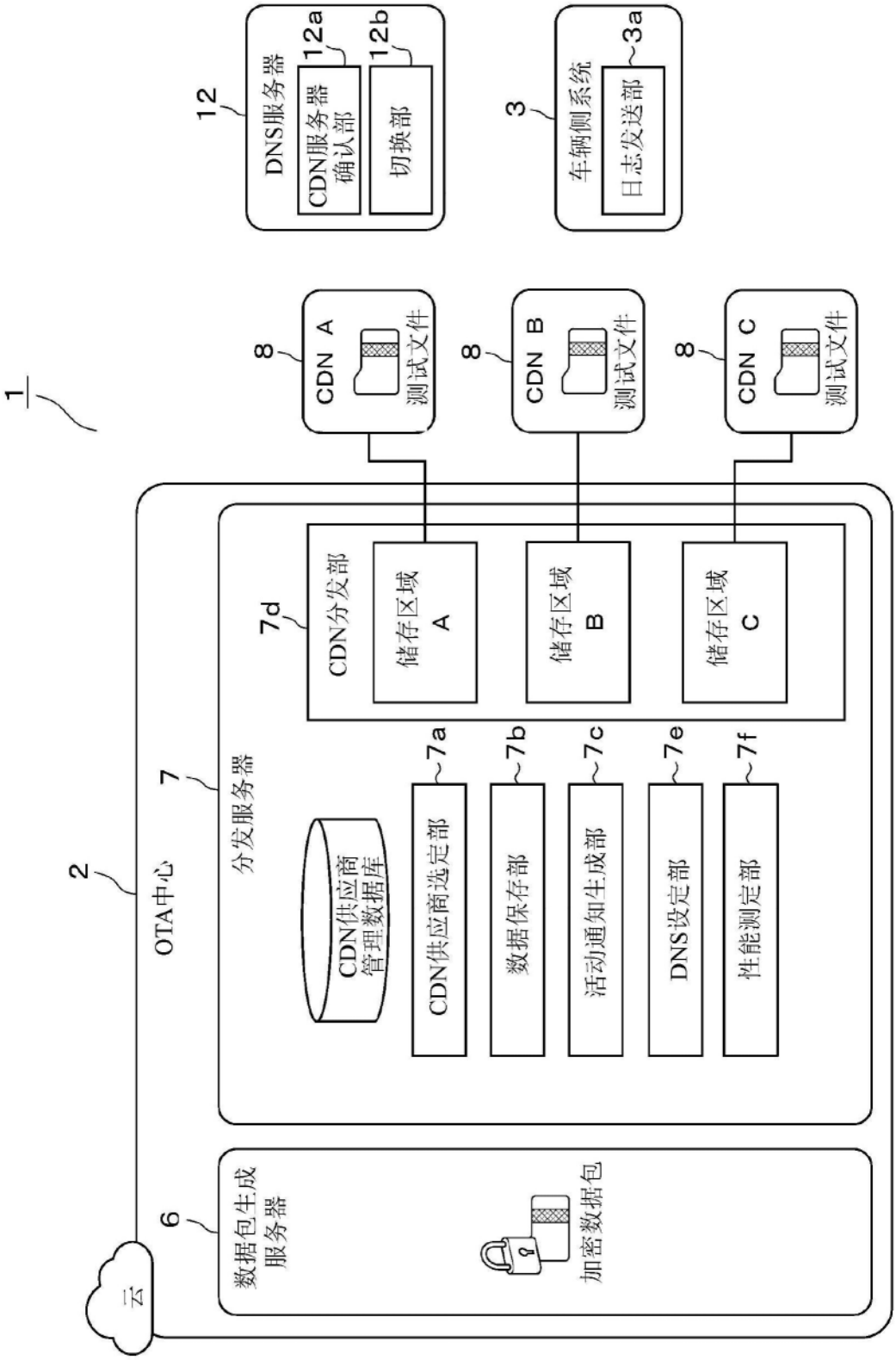

1
2
OTA中心
云
6
数据包生成服务器
加密数据包
7
分发服务器
7a
CDN供应商选定部
7b
数据保存部
7c
活动通知生成部
7e
DNS设定部
7f
性能测定部
CDN供应商管理数据库
7d
CDN分发部
储存区域A
储存区域B
储存区域C
8
CDN A
测试文件
8
CDN B
测试文件
8
CDN C
测试文件
12
DNS服务器
12a
CDN服务器确认部
12b
切换部
3
车辆侧系统
3a
日志发送部

图208

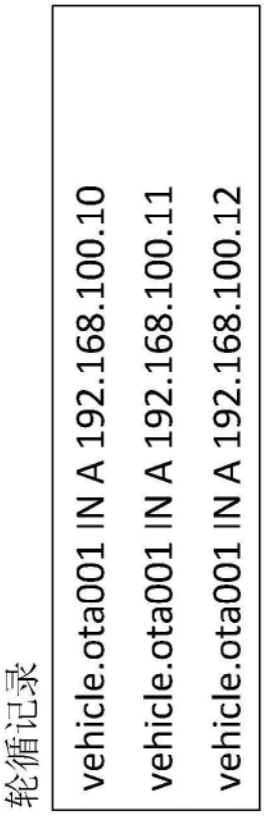

轮循记录
vehicle.ota001 IN A 192.168.100.10
vehicle.ota001 IN A 192.168.100.11
vehicle.ota001 IN A 192.168.100.12

图209

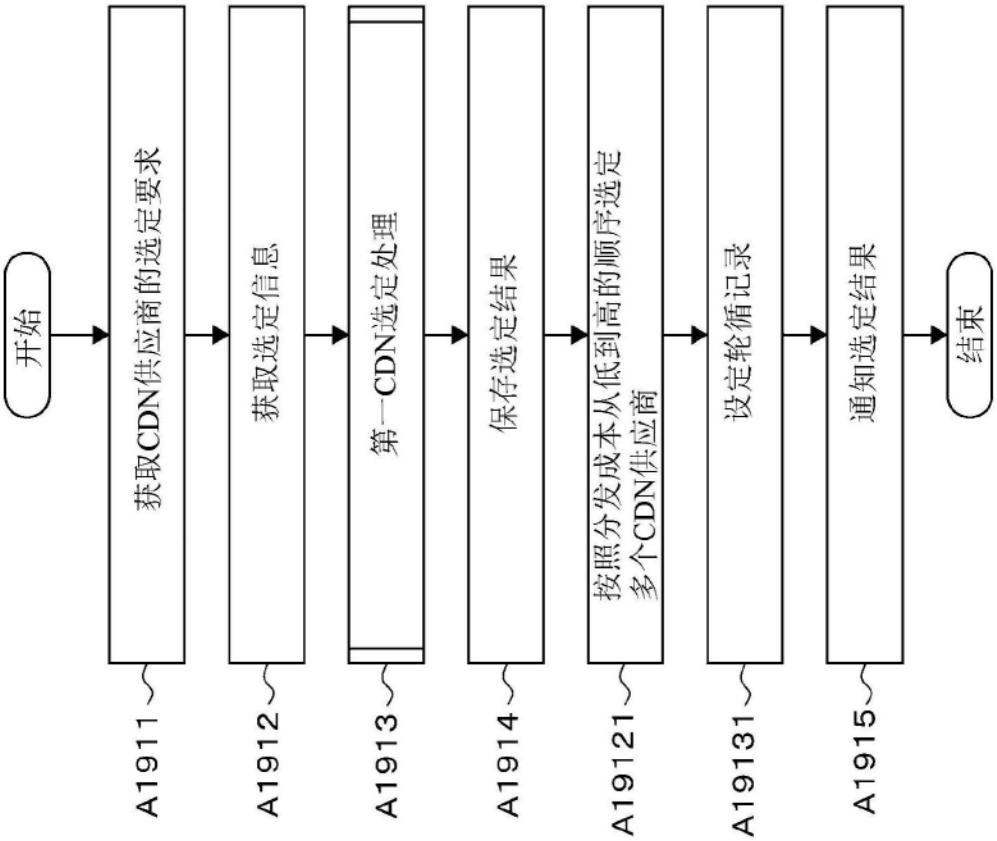

开始
获取CDN供应商的选定要求
获取选定信息
第一CDN选定处理
保存选定结果
按照分发成本从低到高的顺序选定多个CDN供应商
设定轮循记录
通知选定结果
结束
A1911
A1912
A1913
A1914
A19121
A19131
A1915

图210

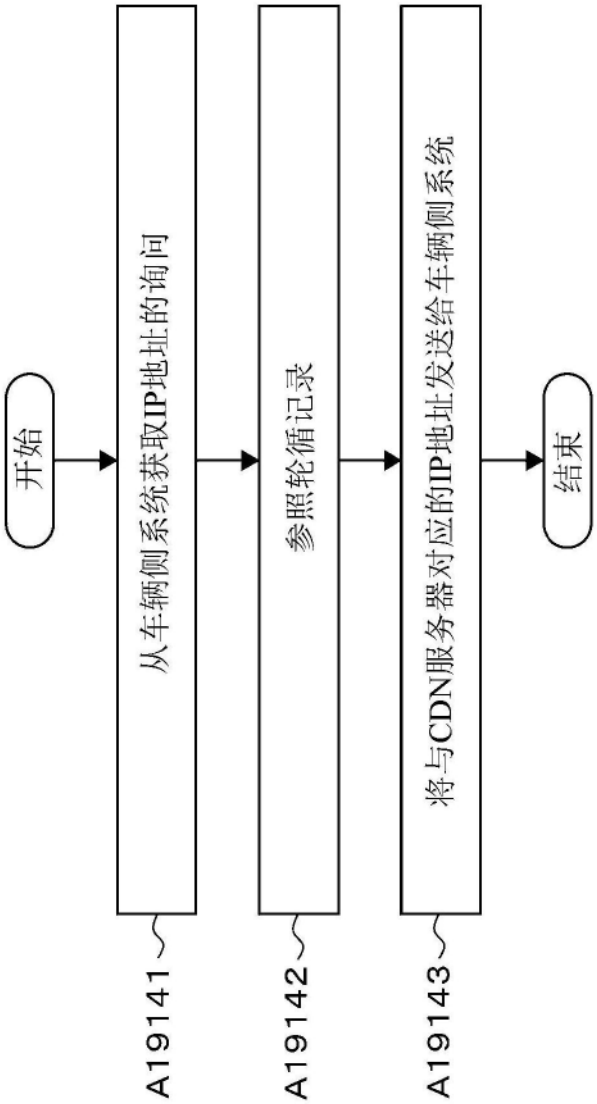

开始
从车辆侧系统获取IP地址的询问
参照轮循记录
将与CDN服务器对应的IP地址发送给车辆侧系统
结束
A19141
A19142
A19143

图211

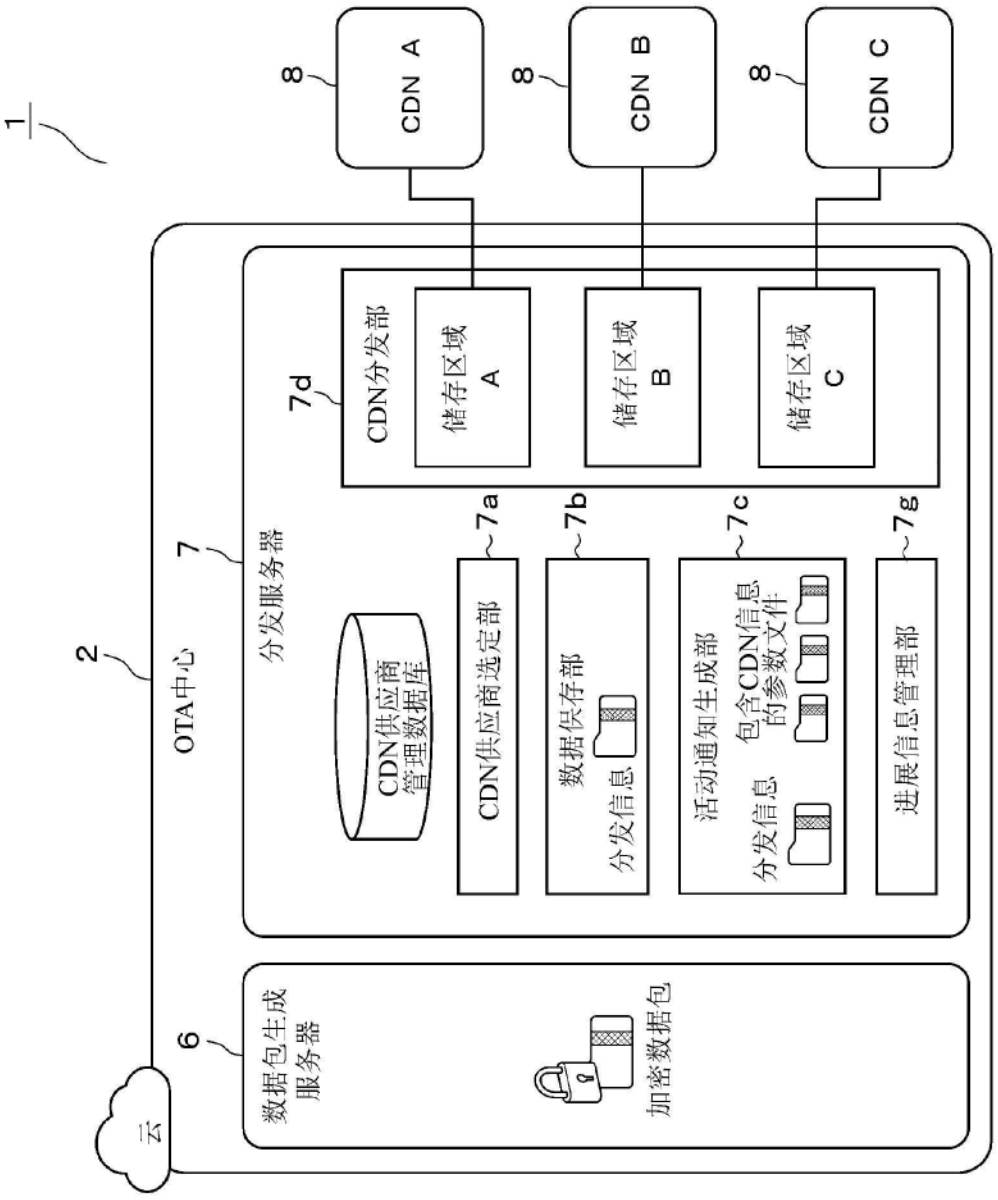

1
8
CDN A
8
CDN B
8
CDN C
2
OTA中心
7
分发服务器
7d
CDN分发部
储存区域 A
储存区域 B
储存区域 C
7a
CDN供应商选定部
7b
数据保存部
分发信息
7c
活动通知生成部
分发信息
包含CDN信息的参数文件
7g
进展信息管理部
CDN供应商管理数据库
6
数据包生成服务器
加密数据包
云

图212

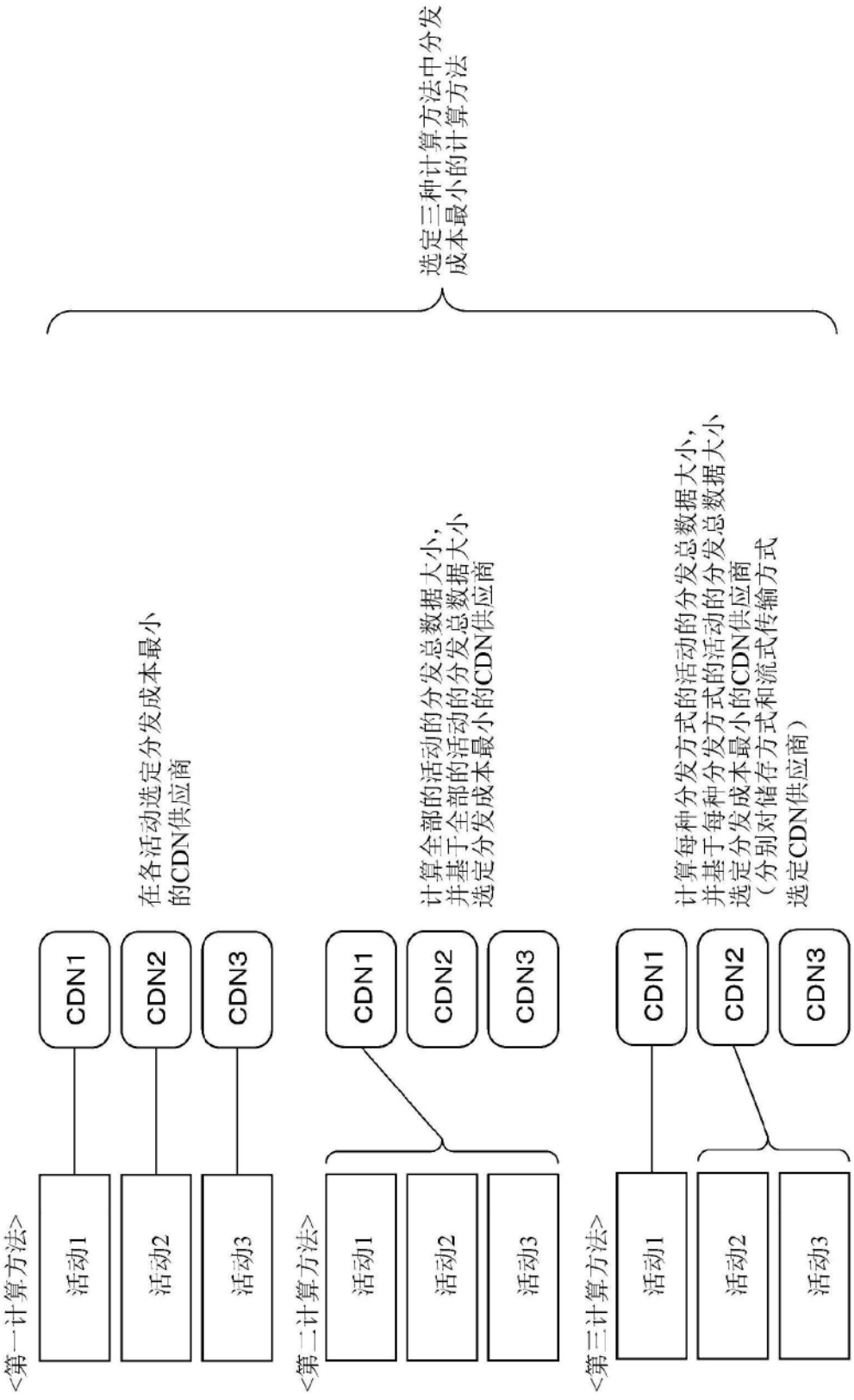

选定三种计算方法中分发
成本最小的计算方法
<第一计算方法>
活动1
活动2
活动3
CDN1
CDN2
CDN3
在各活动选定分发成本最小
的CDN供应商
<第二计算方法>
活动1
活动2
活动3
CDN1
CDN2
CDN3
计算全部的活动的分发总数据大小，
并基于全部的活动的分发总数据大小
选定分发成本最小的CDN供应商
<第三计算方法>
活动1
活动2
活动3
CDN1
CDN2
CDN3
计算每种分发方式的活动的分发总数据大小，
并基于每种分发方式的活动的分发总数据大小
选定分发成本最小的CDN供应商
（分别对储存方式和流式传输方式
选定CDN供应商）

图213

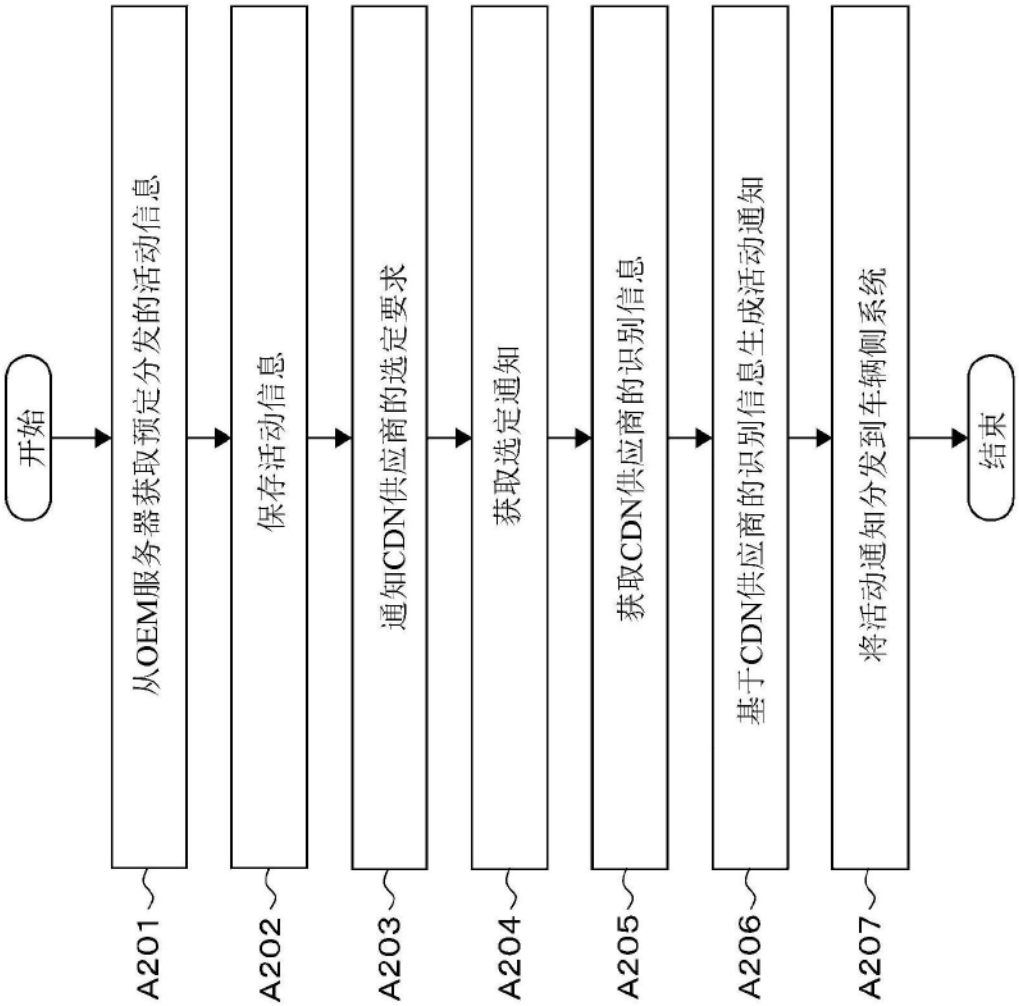

开始
从OEM服务器获取预定分发的活动信息
保存活动信息
通知CDN供应商的选定要求
获取选定通知
获取CDN供应商的识别信息
基于CDN供应商的识别信息生成活动通知
将活动通知分发到车辆侧系统
结束
A201
A202
A203
A204
A205
A206
A207

图214

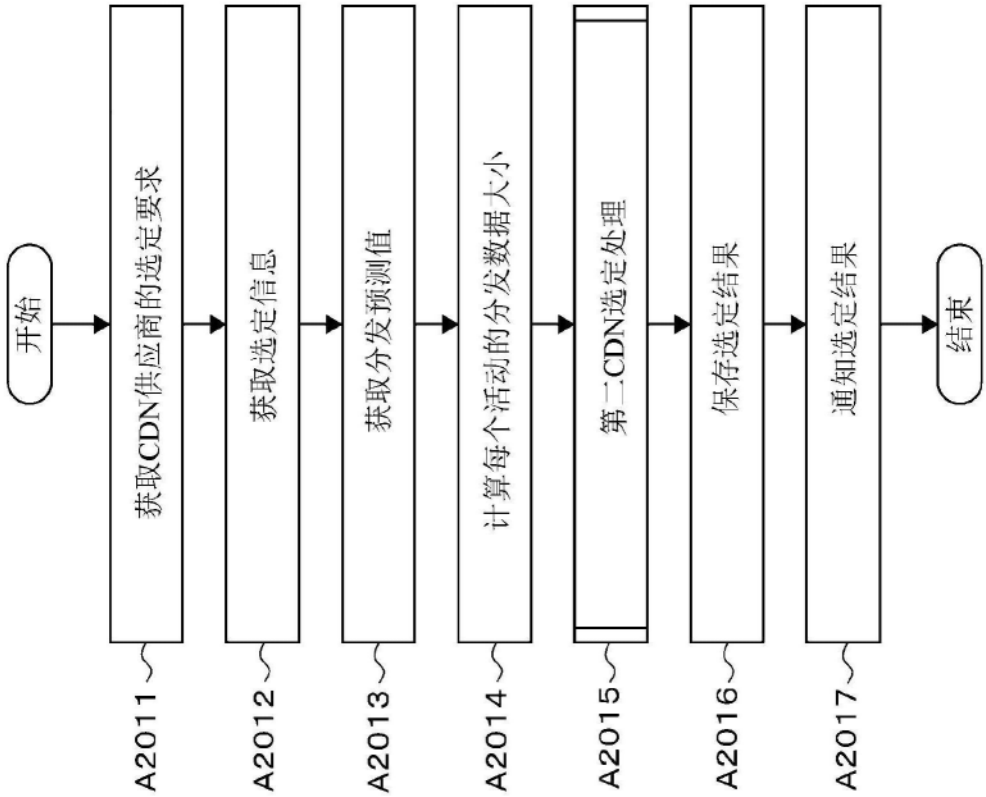

开始
获取CDN供应商的选定要求
获取选定信息
获取分发预测值
计算每个活动的分发数据大小
第二CDN选定处理
保存选定结果
通知选定结果
结束
A2011
A2012
A2013
A2014
A2015
A2016
A2017

图215

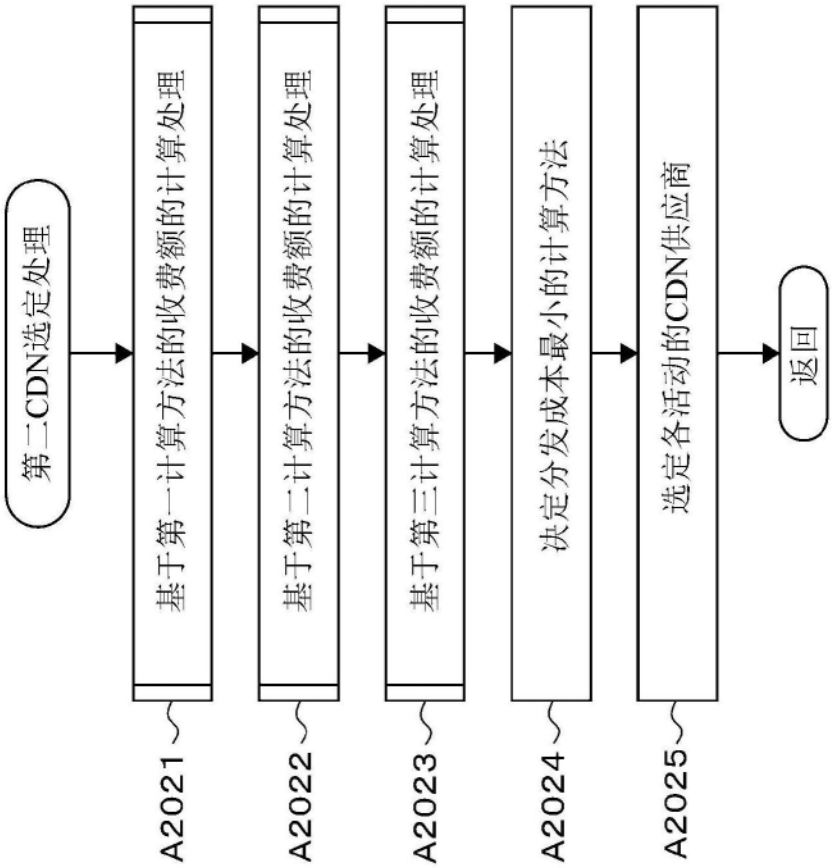

第二CDN选定处理
基于第一计算方法的收费额的计算处理
基于第二计算方法的收费额的计算处理
基于第三计算方法的收费额的计算处理
决定分发成本最小的计算方法
选定各活动的CDN供应商
返回
A2021
A2022
A2023
A2024
A2025

图216

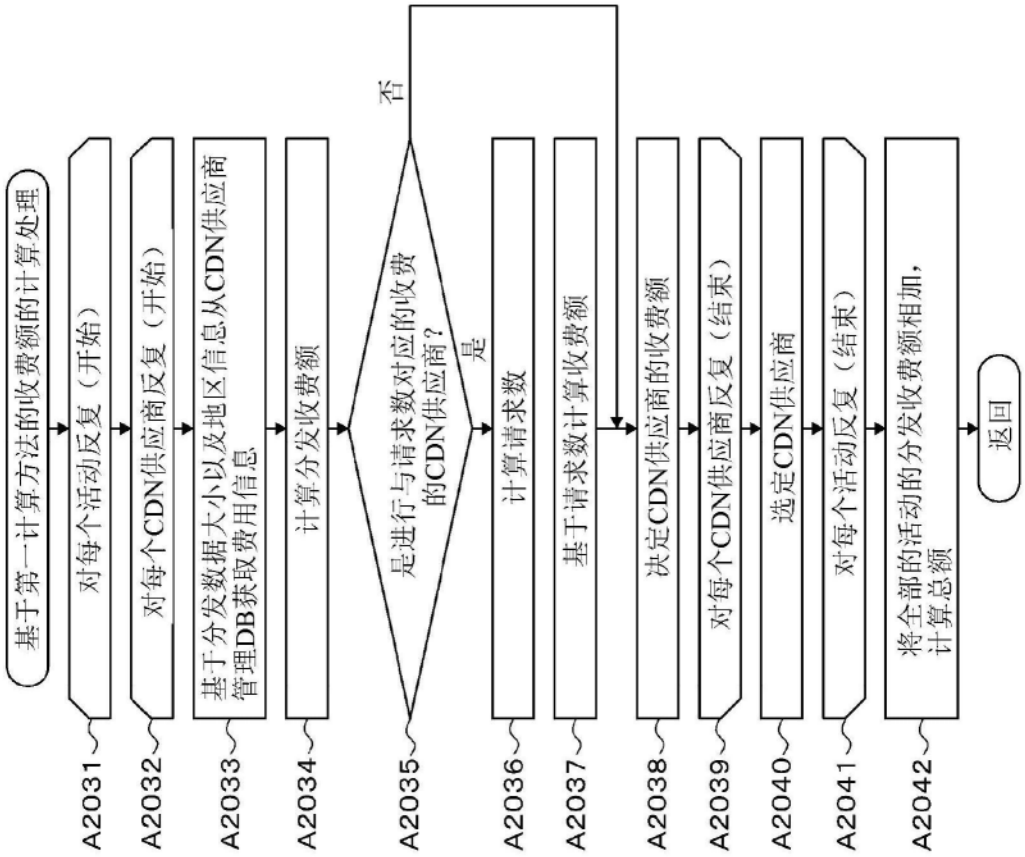

基于第一计算方法的收费额的计算处理
对每个活动反复（开始）
对每个CDN供应商反复（开始）
基于分发数据大小以及地区信息从CDN供应商管理DB获取费用信息
计算分发收费额
是进行与请求数对应的收费的CDN供应商？
否
是
计算请求数
基于请求数计算收费额
决定CDN供应商的收费额
对每个CDN供应商反复（结束）
选定CDN供应商
对每个活动反复（结束）
将全部的活动的分发收费额相加，计算总额
返回
A2031
A2032
A2033
A2034
A2035
A2036
A2037
A2038
A2039
A2040
A2041
A2042

图217

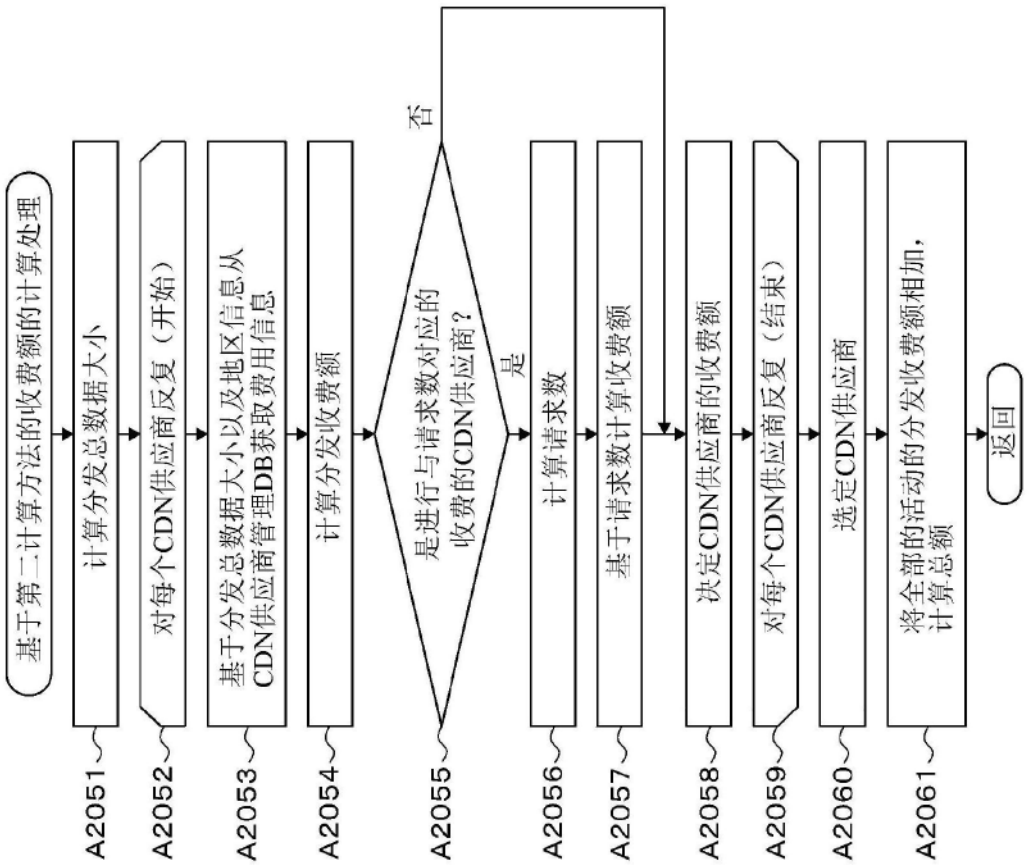

基于第二计算方法的收费额的计算处理
计算分发总数据大小
对每个CDN供应商反复（开始）
基于分发总数据大小以及地区信息从CDN供应商管理DB获取费用信息
计算分发收费额
是进行与请求数对应的收费的CDN供应商？
否
是
计算请求数
基于请求数计算收费额
决定CDN供应商的收费额
对每个CDN供应商反复（结束）
选定CDN供应商
将全部的活动的分发收费额相加，计算总额
返回
A2051
A2052
A2053
A2054
A2055
A2056
A2057
A2058
A2059
A2060
A2061

图218

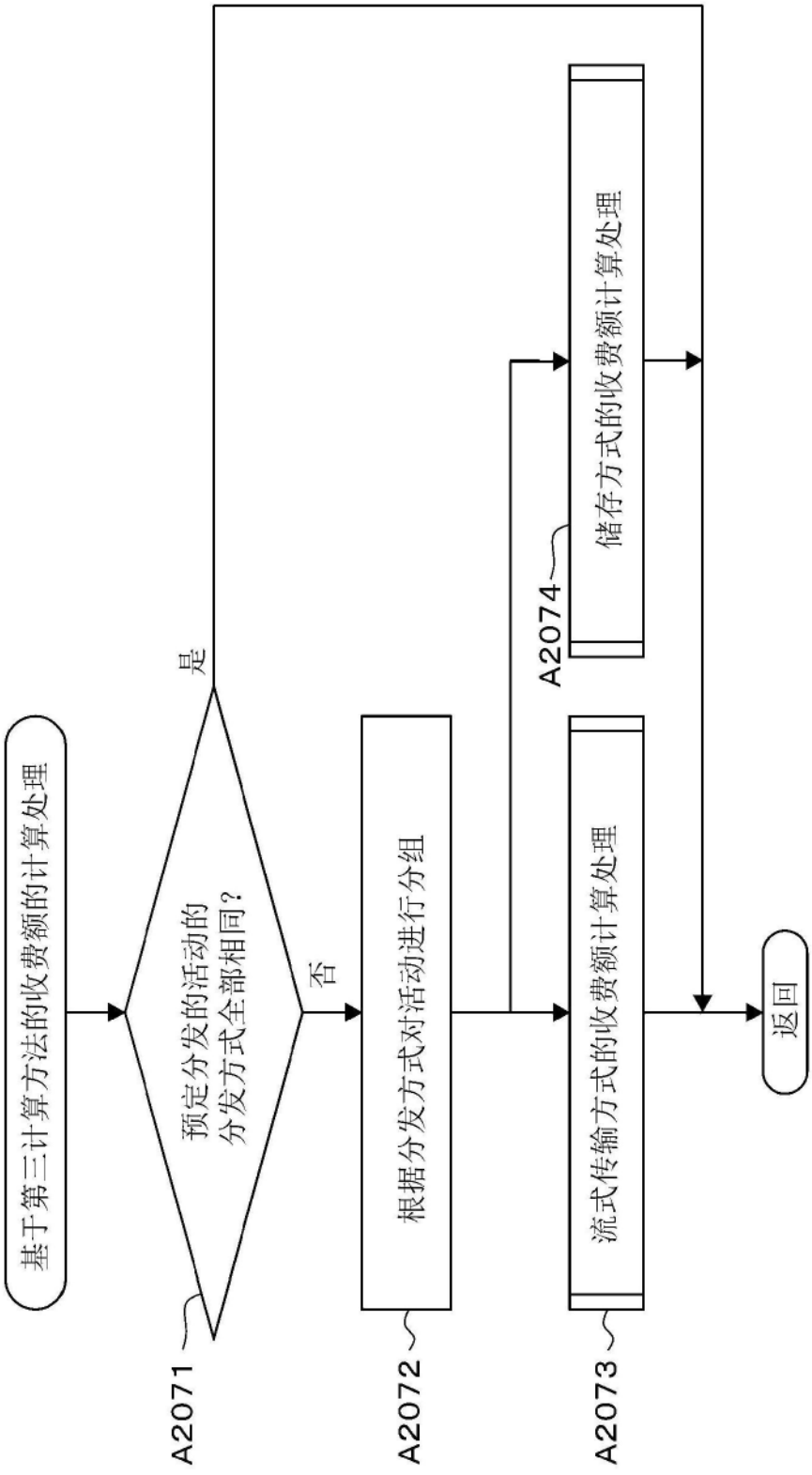

基于第三计算方法的收费额的计算处理
预定分发的活动的
分发方式全部相同？
是
否
A2071
根据分发方式对活动进行分组
A2072
流式传输方式的收费额计算处理
A2073
储存方式的收费额计算处理
A2074
返回

图219

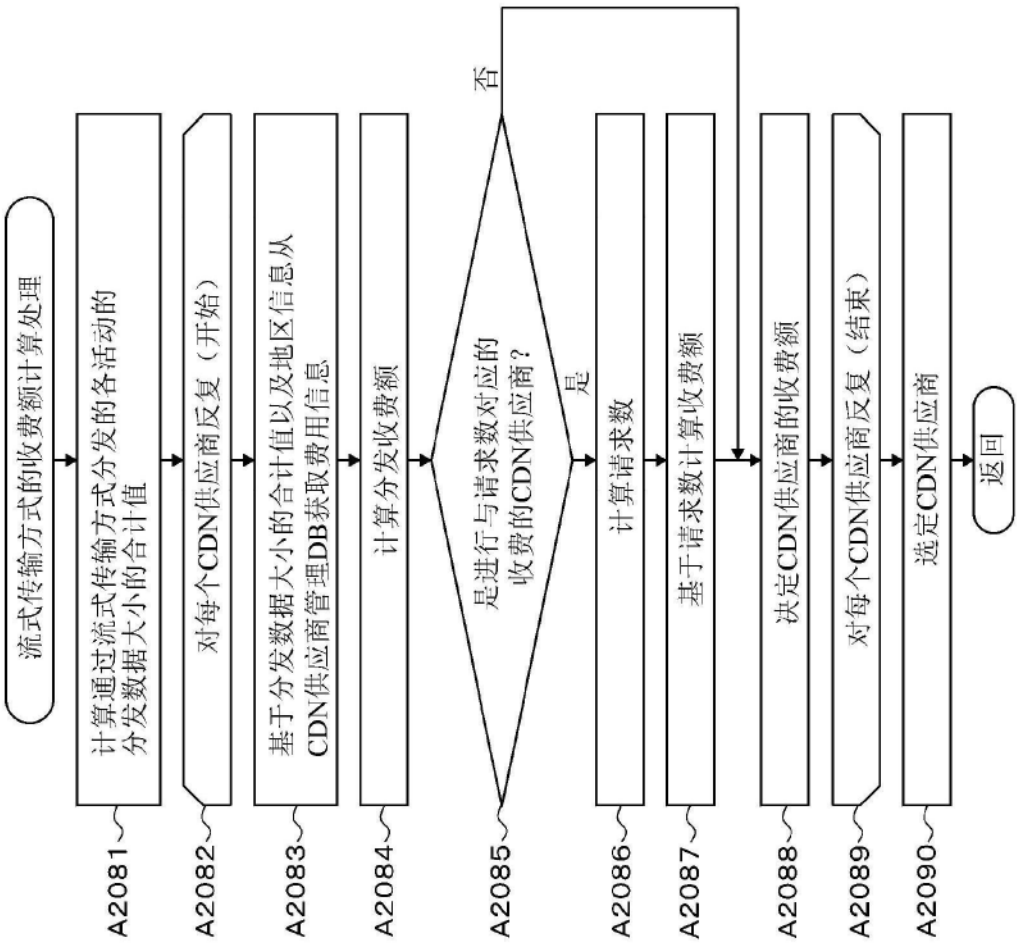

流式传输方式的收费额计算处理
计算通过流式传输方式分发的各活动的分发数据大小的合计值
A2081
对每个CDN供应商反复（开始）
A2082
基于分发数据大小的合计值以及地区信息从CDN供应商管理DB获取费用信息
A2083
计算分发收费额
A2084
是进行与请求数对应的收费的CDN供应商？
否
是
A2085
计算请求数
A2086
基于请求数计算收费额
A2087
决定CDN供应商的收费额
A2088
对每个CDN供应商反复（结束）
A2089
选定CDN供应商
A2090
返回

图220

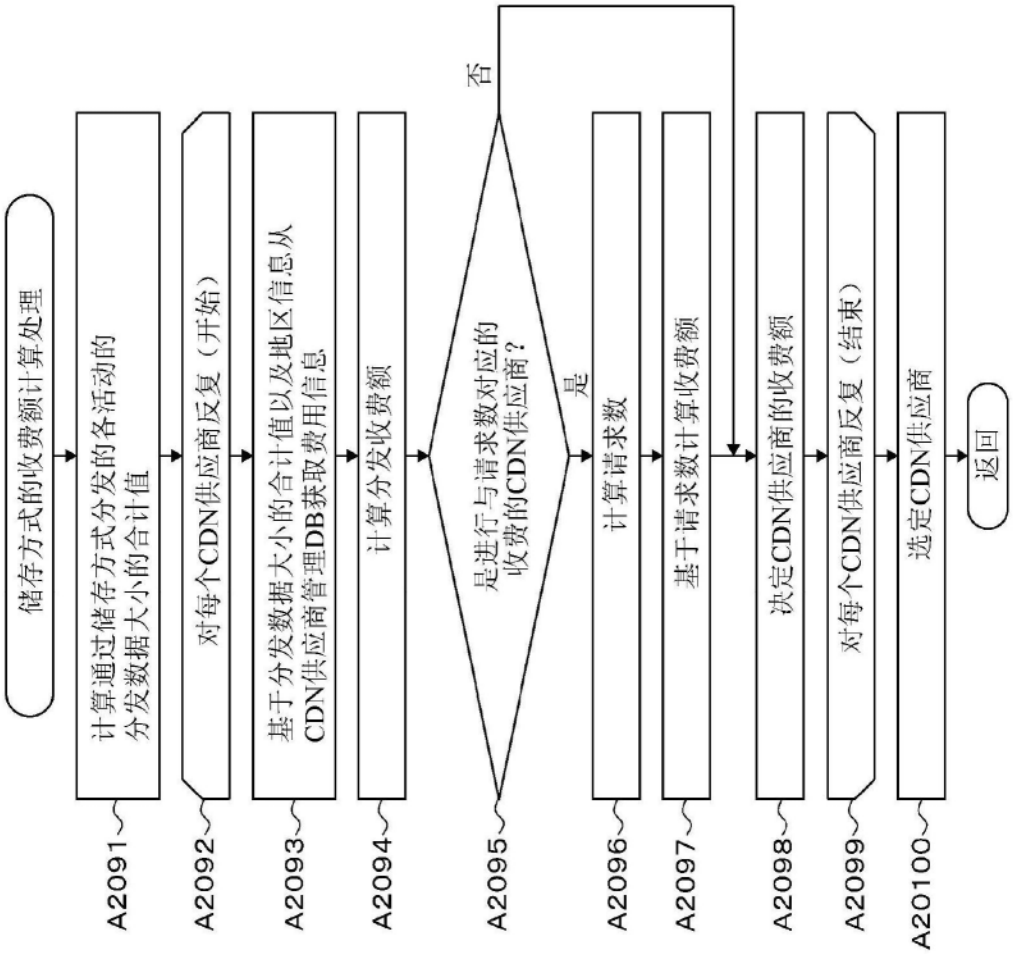

储存方式的收费额计算处理
计算通过储存方式分发的各活动的分发数据大小的合计值
对每个CDN供应商反复（开始）
基于分发数据大小的合计值以及地区信息从CDN供应商管理DB获取费用信息
计算分发收费额
是进行与请求数对应的收费的CDN供应商？
否
是
计算请求数
基于请求数计算收费额
决定CDN供应商的收费额
对每个CDN供应商反复（结束）
选定CDN供应商
返回
A2091
A2092
A2093
A2094
A2095
A2096
A2097
A2098
A2099
A20100

图221

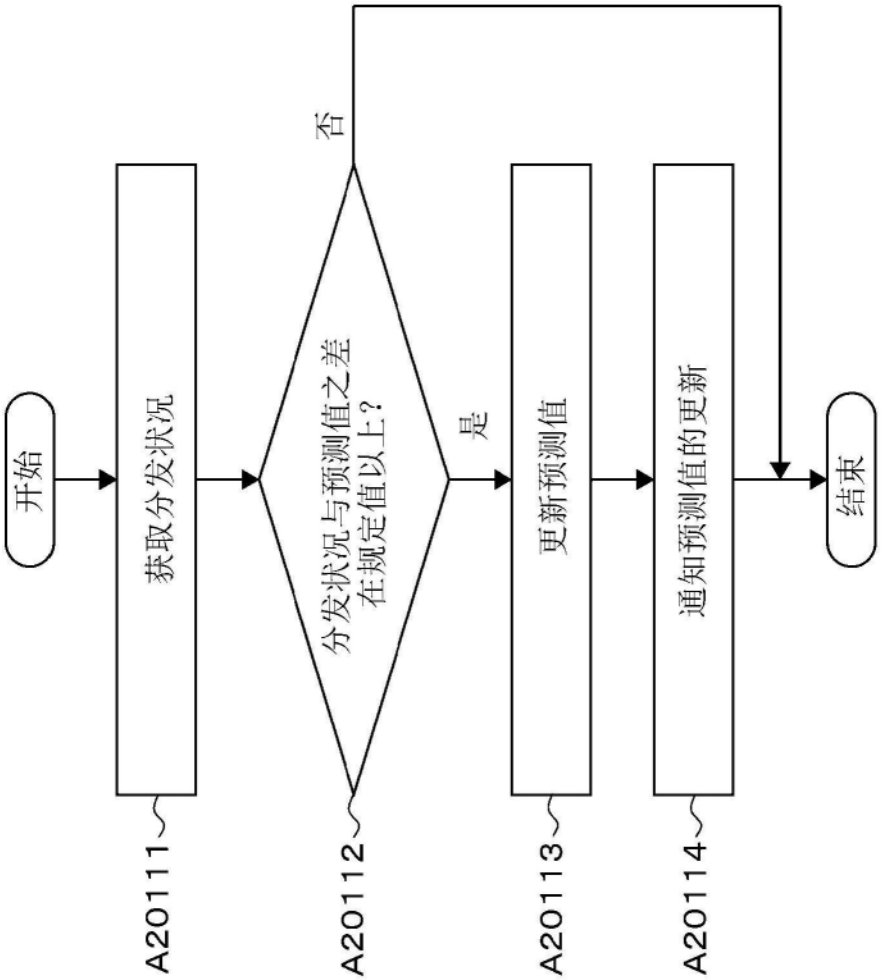

开始
获取分发状况
A20111
分发状况与预测值之差在规定值以上?
A20112
否
是
更新预测值
A20113
通知预测值的更新
A20114
结束

图222

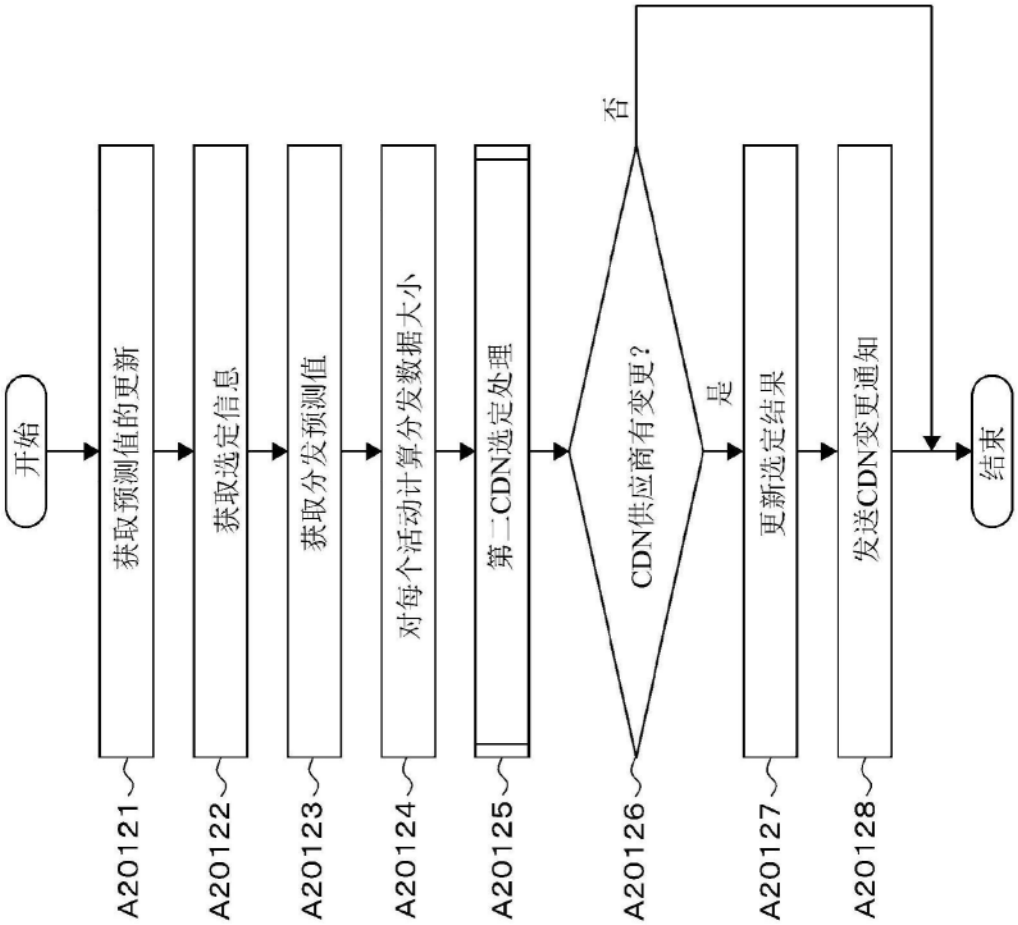

开始
获取预测值的更新
获取选定信息
获取分发预测值
对每个活动计算分发数据大小
第二CDN选定处理
CDN供应商有变更?
否
是
更新选定结果
发送CDN变更通知
结束
A20121
A20122
A20123
A20124
A20125
A20126
A20127
A20128

图223

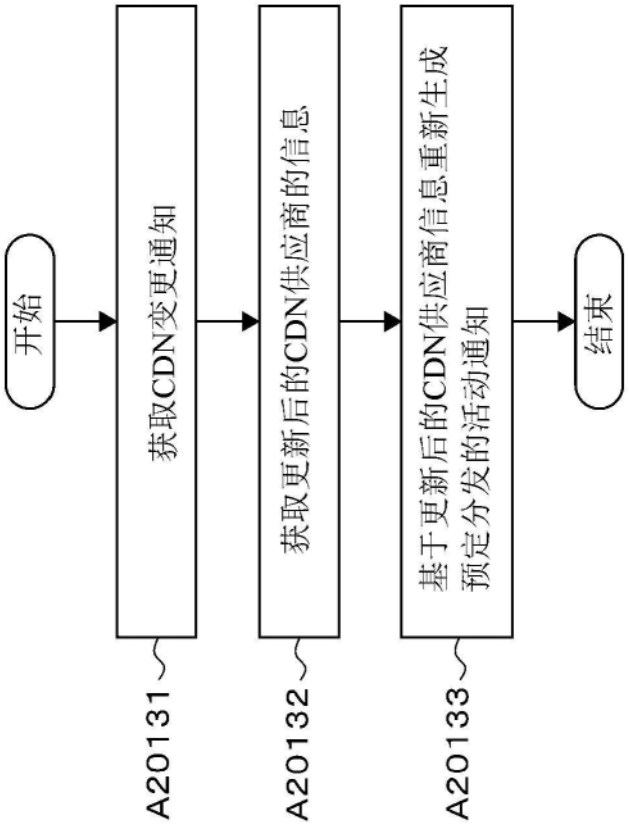

开始
获取CDN变更通知
获取更新后的CDN供应商的信息
基于更新后的CDN供应商信息重新生成预定分发的活动通知
结束
A20131
A20132
A20133

图224