(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 1878062 B
(45)授权公告日 2010.06.23

(21)申请号 200610093558.4

(22)申请日 2006.06.06

(30)优先权数据
165685/2005 2005.06.06 JP

(73)专利权人 株式会社日立制作所
地址 日本东京都

(72)发明人 高桥阳介 真泽史郎 吉田显彦
高柳大悟

(74)专利代理机构 永新专利商标代理有限公司
72002
代理人 胡建新

(51)Int.Cl.
H04W 12/04(2009.01)
H04W 12/06(2009.01)

(56)对比文件
US 2004/0264699 A1,2004.12.30, 全文.
JP 特开2004-343448 A,2004.12.02, 全文.
CN 1313691 A,2001.09.19, 全文.
CN 1567812 A,2005.01.19, 全文.

审查员 阎赛

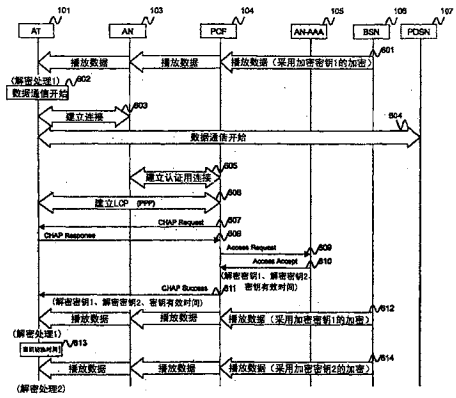
权利要求书 3 页 说明书 16 页 附图 16 页

(54)发明名称

解密密钥发送方法和认证装置

(57)摘要

一种解密密钥发送方法和认证装置，AT(101)只对期望接收的移动机有效发送解密密钥，用于解密从AN(103)通过播放信道发送的加密数据。AN-AAA(105)从AT接收包括终端识别符的终端认证用的消息，进行终端认证。AN-AAA(105)根据所接收的终端识别符，参照对应终端识别符预先存储了终端可以接收的内容的内容类别的内容注册表，获取对应的内容类别。AN-AAA(105)根据所获取的内容类别，参照对应内容类别预先存储了解密密钥和该解密密钥的有效时间的解密密钥数据库，获取对应的解密密钥和有效时间。AN-AAA(105)把认证结果和所获取的解密密钥和有效时间发送给PCF(104)或AT。



CN 1878062 B

1. 一种在无线通信系统中向无线终端发送解密密钥的解密密钥发送方法，内容服务器把使用从管理加密密钥及解密密钥的控制装置接收的加密密钥加密后的数据，通过广播信道发送给无线终端，无线终端使用对应于加密密钥的预先发送的解密密钥将所接收的数据解密，包括：

认证装置从控制装置接收内容类别或识别信息、对应的解密密钥及有效时间，将所接收的内容类别或识别信息、解密密钥及有效时间对应起来，存储在解密密钥数据库中的步骤；

认证装置从无线终端接收包括终端识别符的认证请求的步骤；

认证装置按照所接收的认证请求进行终端认证的步骤；

认证装置根据所接收的认证请求中的终端识别符，参照被预先对应地存储的终端识别符、终端能够接收的内容的内容类别或识别信息的内容注册数据库，获取对应的内容类别或识别信息的步骤；

认证装置根据所获取的内容类别或识别信息，参照解密密钥数据库获取对应的解密密钥和有效时间的步骤；

认证装置向无线终端或包控制装置发送所述进行终端认证的步骤的认证结果、和所获取的解密密钥及有效时间的步骤。

2. 根据权利要求 1 所述的解密密钥发送方法，在所述向无线终端或包控制装置发送的步骤中，认证装置在用于通知认证结果用的消息中包括所获取的解密密钥和有效时间，并发送该消息。

3. 根据权利要求 1 或 2 所述的解密密钥发送方法，在权利要求 1 的所有处理之后执行以下步骤：

终端再认证处理时，执行

第 1 步骤，包控制装置向无线终端发送附加了作为用于实施终端认证的呼叫信号的信息的终端呼叫信号；

第 2 步骤，无线终端按照所接收的终端呼叫信号，向认证装置发送包括终端识别符的认证请求；

第 3 步骤，认证装置按照所接收的认证请求再次进行终端认证，参照内容注册数据库和解密密钥数据库，获取内容类别或识别信息、具有当前时刻以后的有效时间的一个或多个解密密钥、和对应于解密密钥的一个或多个有效时间，并将获取的内容类别或识别信息、一个或多个解密密钥、和对应于解密密钥的一个或多个有效时间发送给无线终端或包控制装置。

4. 根据权利要求 3 所述的解密密钥发送方法，包控制装置对每个无线终端改变发送终端呼叫信号的时间，并发送该终端呼叫信号。

5. 根据权利要求 4 所述的解密密钥发送方法，还包括：

对于数据通信中的无线终端，

第 4 步骤，认证装置利用为了进行数据通信而建立的无线终端和无线基站的会话，从数据通信中的无线终端接收包括终端识别符的认证请求；

第 5 步骤，认证装置按照所接收的认证请求再次进行终端认证，参照内容注册数据库和解密密钥数据库，获取内容类别或识别信息、具有当前时刻以后的有效时间的一个或多

个解密密钥、和对应于解密密钥的一个或多个有效时间，并将获取的内容类别或识别信息、一个或多个解密密钥、和对应于解密密钥的一个或多个有效时间发送给无线终端或包控制装置。

6. 根据权利要求 5 所述的解密密钥发送方法，包控制装置对每个无线终端改变发送用于请求终端认证的消息的时间，并向无线终端发送该消息，

在所述第 4 步骤中，认证装置接收按照其所接收的用于请求终端认证的消息而从数据通信中的无线终端发送的认证请求。

7. 根据权利要求 5 或 6 所述的解密密钥发送方法，对数据通信中的无线终端执行所述第 4 和第 5 步骤，对不在数据通信中的无线终端执行所述第 1 ～第 3 步骤。

8. 根据权利要求 7 所述的解密密钥发送方法，在所述向无线终端或包控制装置发送的步骤中，认证装置向包控制装置发送认证结果、所获取的内容类别或识别信息、所获取的解密密钥及有效时间，

并且，还包括 ：

包控制装置向无线终端发送所接收的内容类别或识别信息、解密密钥和有效时间，并且将内容类别或识别信息和有效时间与用于识别该无线终端的终端识别符相对应，存储在呼叫控制数据库中的步骤 ；

包控制装置在存储于呼叫控制数据库的有效时间的结束时刻的规定时间之前，向对应于该有效时间的终端识别符表示的无线终端，发送用于请求终端认证的消息或终端呼叫信号的步骤。

9. 根据权利要求 8 所述的解密密钥发送方法，包控制装置在有效时间的结束时刻的规定时间之前的终端识别符有多个时，向相应的无线终端中的任一个无线终端发送用于请求终端认证的消息或终端呼叫信号，在向该无线终端发送了解密密钥之后或经过规定时间之后，向其他无线终端中的任一个发送用于请求终端认证的消息或终端呼叫信号。

10. 一种无线通信系统的认证装置，内容服务器把使用从管理加密密钥及解密密钥的控制装置接收的加密密钥加密后的数据，通过广播信道发送给无线终端，无线终端使用对应于加密密钥的预先发送的解密密钥将所接收的数据解密，包括 ：

解密密钥数据库，将所接收的内容类别或识别信息、解密密钥和有效时间相对应进行存储 ；

内容注册数据库，将终端识别符、终端能够接收的内容的内容类别或识别信息相对应预先进行存储 ；和

进行终端认证和解密密钥的发送的处理部，

所述处理部

从所述控制装置接收内容类别或识别信息、对应的解密密钥和有效时间，存储在所述解密密钥数据库中，

从所述无线终端接收包括终端识别符的认证请求，

按照所接收的认证请求进行终端认证，

根据所接收的认证请求中的终端识别符，参照所述内容注册数据库，获取对应的内容类别或识别信息，

根据所获取的内容类别或识别信息，参照所述解密密钥数据库，获取对应的解密密钥

和有效时间，

向所述无线终端或包控制装置发送认证结果、所获取的解密密钥及有效时间。

解密密钥发送方法和认证装置

技术领域

[0001] 本发明涉及一种解密密钥发送方法和认证装置，主要涉及可以通过播放信道进行被加密的数据发送的无线通信方法，特别涉及 CDMA 无线通信系统的解密密钥发送方法和认证装置。

背景技术

[0002] 在国际标准化机构的 3GPP2(3rdGeneration Partnership Project2) 中，对可以进行语音通信和数据通信的移动体通信方式即 cdma20001x 方式、和通过特定为数据通信专用来提高频率利用效率的移动体无线通信方式即 cdma2000 1xEV-DO(1x Evolution-Data Only) 方式，进行了标准化。cdma2000 1x 方式和 1xEV-DO 通信方式利用移动体网络实现一对一的终端进行通信的单点通信，但也在研究实现进行一对多的通信的多点通信。

[0003] 作为实现多点通信的技术要素，在无线接口中作为进行数据传输的信道，被称为 Broadcast channel 的播放信道已经标准化。例如，作为 cdma2000 1x 用，按照 3GPP2 标准即 C.S0001-D v1.0、C.S0002-D v1.0、C.S0003-D v1.0、C.S0004-D v1.0、C.S0005-D v1.0 进行了标准化。并且，例如作为 cdma2000 1xEV-DO 用，按照 C.S0054-0 v1.0 进行了标准化。把使用了播放信道的服务称为 BCMCS(Broadcast MulticastService)。

[0004] 以往在基地局 - 移动机之间的通信中使用的单点用信道，具有只有单一的移动机能够接收从基地局发送的数据的特征。另一方面，为了支持多点通信而被标准化的播放信道，可以接收电波的所有移动机具有能够接收从基地局发送的数据的特征。因此，使用播放信道发送的数据可以被所有移动机接收。由于只有所选择的移动机组能够接收数据，所以在讨论以下方式，即，进行数据的加密，利用单点通信等手段向所选择的移动机组预先发送解密该被加密的数据所需要的密钥（解密密钥）。关于向移动机发送解密密钥的方式，在 3GPP2 标准候补 X.P0022-0v.0.2 的第 7 章和第 10.2 章（非专利文献 1）中公开了以下方法，根据来自移动机的问询，发送被 XML(Extensible Markup Language) 格式化的解密密钥 (BAK, Broadcast Access Key)。

[0005] 图 24 表示提供 1xEV-DO 网络中的 BCMCS 时的系统结构图。该图表示使用 1xEV-DO 播放信道向多个移动机发送数据的情况。

[0006] 内容服务器 108 具有生成并发送播放信道用数据的功能。这些数据作为赋予了多点 IP 地址的 IP 包被发送给 BSN(Broadcast Serving Node)106。该 IP 包由内容服务器 108 使用由 BCMCS Controller 109 管理的加密密钥被加密后发送。内容服务器 108 发送播放数据时，预先从 BCMCSController 109 接收进行加密所需要的加密密钥。

[0007] 在 BSN106 接收的数据被实施了按照 IETF RFC1662 定义的 HDLC 相似成帧等成帧处理，并发送给包控制装置 PCF(Packet Control Function)104，以使移动机可以判断 IP 包边界。在 PCF104 中，缓冲从 BSN106 接收的包，并调整为符合无线频带的传输速度发送给基地局 AN(AccessNode)103。

[0008] 在 AN103 中，从 PCF104 接收的数据被使用播放信道无线发送。在播放信道上发送

的数据被作为移动机的 AT(Access Terminal)101、AT102 等多个移动机接收。管理与这些播放数据相关的信息、具有播放数据的加密解密中使用的加密和解密密钥的数据库、及移动机有无接收权限等的是 BCMCS Controller109。

[0009] 并且，该图所示的 AN-AAA(Access Network-Authentication、Authorization and Accounting)105 是在移动机认证时使用的认证服务器。例如，作为移动机的硬件，是用于认证无线连接是否被事业者允许的服务器。PDSN(Packet Data Serving Node)107 是用于支持与移动机的单点通信的、完结 PPP(Point-to-Point Protocol) 的节点。并且，PDSN107 是进行在因特网 111 中使用的依据 IP 协议的包、和在无线网络中使用的协议的中介的装置。AAA(Authentication、Authorization andAccounting)110 是在使用移动机的用户认证中使用的认证服务器，是用于认证是否允许使用移动机的用户通过无线连接进行向因特网 111 的连接的服务器。

[0010] 图 2 表示基于 3GPP2 标准候补即 X.P0022-0 的 Annex A 的解密密钥发送步骤。

[0011] BSN106 从内容服务器 108 接收用于在播放信道上发送的数据。该播放数据通过 PCF104 发送给 AN103。并且，在 AN103 中被接收的播放数据，被使用播放信道无线发送给 AT101(201)。此时，在 AT101 接收的数据被加密，由于 AT101 未持有用于解密的密钥（解密密钥），所以接收数据在 AT101 中被废弃。

[0012] 例如，在 AT101 的电源接通时，在 AT101 和 AN103 之间进行 1xEV-DO 对话的建立，其中进行在以后的处理中使用的无线协议的参数等的确定 (202)。AT101 根据所建立的 1xEV-DO 对话的信息，建立用于进行数据通信的连接 (203)。另外，该连接用于在 AT101 和 AN103 之间进行一对一的单点通信，是独立于播放信道之外准备的。步骤 203 ～ 215 的通信内容用于在该连接上进行通信，所以其他 AT 不能接收信息。

[0013] AN103 和 PCF104 在 AT101 建立连接后 (202)，首先检测已建立了连接，在使 AT101 可以通信之前，实施判断 AT101 是否被赋予了通信资格的终端认证。作为实施该终端认证用的准备，在 AN103 和 PCF104 之间建立认证用总线 (204)。

[0014] 为了在 AT101 和 PCF104 之间实施终端认证，使用在步骤 203 建立的连接和在步骤 204 建立的认证用总线，进行被 PPP 定义的 LCP(linkcontrol protocol) 的建立 (205)。PCF104 发送请求终端认证用的例如 CHAP Request 消息 (206)。AT101 使用在 CHAP Request 消息中接收的信息和由 AT101 持有的移动机固有信息等，计算认证符，把包括认证符的 CHAP Request 消息发送给 PCF104(207)。PCF104 使所接收的认证符包含于 Access Accept 消息中，并发送给 AN-AAA105(208)。AN-AAA105 计算所接收的认证符的妥当性，在判断为妥当时，向 PCF104 发送作为已通过终端认证的 Access Accept 消息 (209)。PCF104 向 AT101 发送用于通知认证已通过的 CHAP Success 消息 (210)。

[0015] 然后，在 AN103 和 PCF104 之间建立用于建立单点通信用的总线的数据用总线 (211)。并且，在 PCF104 和 PDSN107 之间也建立数据用总线 (212)。为了进行单点通信时所需要的成帧，在 AT101 和 PDSN107 之间建立 PPP(213)。

[0016] AT101 为了接收用于解密例如在步骤 201 示出的被加密的播放数据的密钥，向 BCMCS Controller109 发送 HTTP Information AcquisitionRequest 消息 (214)。BCMCS Controller109 向 AT101 发送包括解密密钥和该解密密钥有效期限信息 HTTP Information Acquisition Response 消息 (215)。

[0017] 然后，AT101 使用在步骤 215 接收的解密密钥，将从 AN103 发送的被加密的播放数据解密，可以接收数据 (216)。

[0018] 非专利文献 13GPP2 标准备选 X.P0022-0v.0.2、7 章及 10.2 章。

[0019] 非专利文献 2C.S0001-D v1.0、3GPP2 发行、2004 年 3 月

[0020] 非专利文献 3C.S0002-D v1.0、3GPP2 发行、2004 年 3 月

[0021] 非专利文献 4C.S0003-D v1.0、3GPP2 发行、2004 年 3 月

[0022] 非专利文献 5C.S0004-D v1.0、3GPP2 发行、2004 年 3 月

[0023] 非专利文献 6C.S0005-D v1.0、3GPP2 发行、2004 年 3 月

[0024] 非专利文献 7C.S0054-D v1.0、3GPP2 发行、2004 年 3 月

[0025] 非专利文献 8RFC1662、IETF 发行、1994 年 7 月

[0026] 在使用现有的播放信道的数据发送方式中，在将发送的数据不加密而发送时，期望接收数据的移动机以外的移动机也能够接收到数据。例如，会出现即使是与通信商的服务合同结束的移动机也可以接收数据的情况。因此为了只让期望的移动机才能接收数据，可以考虑将发送的数据加密进行发送，并发送用于将加密的数据解密的密钥（解密密钥）的方式。

[0027] 在以往的解密密钥发送方式中，移动机为了取得解密密钥，确保单播用的无线资源，通过使用了该资源的无线通信，与管理解密密钥的服务器进行通信，来取得解密密钥。图 2 是 P0022-0 的 Annex A 记载的步骤，在该步骤中，使用单播用的通道来取得解密密钥，因此需要步骤 211 ～步骤 215。这样，由于需要步骤 213 所示的 PDSN 的 PPP 通话终端及步骤 214 ～ 215 所示 BCMCS Controller 业务量处理，因此产生 PDSN 及 BCMCSController 的资源浪费。并且，为取得解密密钥的步骤多，取得解密密钥的时间长。

[0028] 这样，当不能确保用于取得解密密钥的无线资源时，则不能取得解密密钥，无法接收播放信道上发送的数据。因此，在从提供通信的基站接收无需把握通信实际状态的播放数据时，也需要从移动机进行取得解密密钥的通信，其结果，通信量增大，无线业务量及通信网业务量增加。

[0029] 而且，为了抑制用于取得解密密钥的通信量，在不进行通过播放信道发送的数据的加密时，如上所述，期望接收数据的移动机以外的移动机也能接收数据，因此不能认为是根本的解决方案。

[0030] 另外，在现有的方法中，为了在 PDSN107 和 AT101 之间建立 PPP，并进行与 BCMCS Controller109 之间的通信，必须在 PDSN107 进行管理和处理的会话数量增加，必须在 BCMCS Controller109 进行管理和处理的业务量增加。这样，PDSN107 和 BCMCS Controller109 所要求的处理能力变大，有时需要准备大量的设备。另外，由于需要 PPP 建立、与 BCMCSController 之间的通信，所以需要 AT101 得到解密密钥之前的处理时间，需要 AT101 从建立会话到开始接收播放数据的时间。

发明内容

[0031] 本发明鉴于以上问题，其一个目的在于提供解密密钥发送方法和认证装置，不增加用于获取解密密钥的特殊通信的通信量，即可仅对期望发送解密密钥的接收移动机安全地实施解密密钥的发送。并且，本发明的目的在于在通过播放信道接收数据的过程中不间

断地更新解密密钥。本发明的一个目的在于抑制会话数量的增加及业务量的增加的同时接收解密密钥。并且，本发明的一个目的在于缩短终端用于得到解密密钥的处理时间。另外，本发明的目的在于缩短终端开始会话后到播放数据的接收开始的时间。并且，本发明的一个目的在于通过使发送解密密钥的定时对每个无线终端错开，防止在同一时期通信集中。

[0032] 为了解决上述课题，本发明的一个特征是通过例如提供按照用于进行移动机的认证的步骤发送解密密钥的装置，仅向被允许接收用播放信道发送的数据的移动机发送解密密钥。本发明可以省略以往需要的 AT101 和 PDSN107 之间的 PPP 建立处理、AT101 和 BCMCS Controller109 之间发生的业务量，可以减少 PDSN107 和 BCMCS Controller109 的处理量，可以因业务量减少而降低处理延迟。

[0033] 另外，在本发明中，提供对一次发送过的解密密钥设置有效期限、且定期更新解密密钥的装置。这样一来，其一个特征是设置了当接收到一次解密密钥的移动机失去了接收播放信道上发送的数据的资格时不能继续接收数据的步骤。作为失去该数据的接收资格的一个例子，例举解除了移动机的合同的情况。

[0034] 本发明的无线通信系统的解密密钥发送方法，该无线通信系统例如具有由无线基站和无线终端构成的用于数据发送的播放信道，并采用对由上述播放信道发送的数据进行加密并发送的无线方式，该解密密钥发送方法的一个特征在于，

[0035] 以上述无线终端进行终端认证为契机，向用于进行上述终端认证的信号，传送解密上述被加密的数据的密钥。

[0036] 在上述的解密密钥发送方法中，为了进行解密密钥的更新，指定相对于当前正在发送的数据的第一解密密钥、相对于将来发送的预定数据的第二解密密钥或任意数的解密密钥、和所述第二解密密钥的使用开始时间，或者指定相对于所述任意数的各个解密密钥的使用开始时间，由此可以进行解密密钥的切换。

[0037] 并且，在上述的解密密钥发送方法中，以用于从所述无线基地局实施终端认证的呼叫信号为契机，开始终端认证，向所述无线终端传送所述第一解密密钥、所述第二解密密钥或所述任意数的解密密钥、和解密密钥的使用开始时间。

[0038] 在上述的解密密钥发送方法中，在所述无线基地局和所述无线终端使用单点通信用的连接进行通信的过程中，以从所述无线基地局发送用于实施终端认证的呼叫信号为契机，开始终端认证，向所述无线终端传送所述第一解密密钥、所述第二解密密钥或所述任意数的解密密钥、和解密密钥的使用开始时间。

[0039] 在上述的解密密钥发送方法中，利用所述无线终端改变所述无线基地局向所述无线终端发送所述呼叫信号的时间，由此可以分散用于发送解密密钥的业务量。

[0040] 根据本发明的第一解决方案，提供一种在无线通信系统中向无线终端发送解密密钥的解密密钥发送方法，内容服务器把使用从管理加密密钥及 / 或解密密钥的控制装置接收的加密密钥加密后的数据，通过播放信道发送给无线终端，无线终端使用对应加密密钥的预先发送的解密密钥将所接收的数据解密，包括 ：

[0041] 认证装置从控制装置接收内容类别或识别信息、对应的解密密钥和有效时间，将所接收的内容类别或识别信息、解密密钥和有效时间对应存储在解密密钥数据库中的步骤 ；

[0042] 认证装置从无线终端接收包括终端识别符的认证请求的步骤 ；

[0043] 认证装置按照所接收的认证请求进行终端认证的步骤；

[0044] 认证装置根据所接收的认证请求中的终端识别符，参照预先对应着存储了终端识别符、和终端可以接收的内容的内容类别或识别信息的内容注册数据库，获取对应的内容类别或识别信息的步骤；

[0045] 认证装置根据所获取的内容类别或识别信息，参照解密密钥数据库获取对应的解密密钥和有效时间的步骤；

[0046] 认证装置向无线终端或包控制装置发送所述进行终端认证的步骤的认证结果、和所获取的解密密钥和有效时间的步骤。

[0047] 根据本发明的第二解决方案，提供一种无线通信系统的认证装置，内容服务器把使用从管理加密密钥及／或解密密钥的控制装置接收的加密密钥加密后的数据，通过播放信道发送给无线终端，无线终端使用对应加密密钥的预先发送的解密密钥将所接收的数据解密，包括：

[0048] 解密密钥数据库，对应存储着所接收的内容类别或识别信息、解密密钥和有效时间；

[0049] 内容注册数据库，对应着预先存储了终端识别符、终端可以接收的内容的内容类别或识别信息；和

[0050] 进行终端认证和解密密钥的发送的处理部，

[0051] 所述处理部从所述控制装置接收内容类别或识别信息、对应的解密密钥和有效时间，存储在所述解密密钥数据库中，并从所述无线终端接收包括终端识别符的认证请求，按照所接收的认证请求进行终端认证，

[0052] 然后根据所接收的认证请求中的终端识别符，参照所述内容注册数据库，获取对应的内容类别或识别信息，

[0053] 并且根据所获取的内容类别或识别信息，参照所述解密密钥数据库获取对应的解密密钥和有效时间，

[0054] 最后向所述无线终端或包控制装置发送认证结果、和所获取的解密密钥和有效时间。

[0055] 根据本发明，可以提供一种解密密钥发送方法，不增加用于获取解密密钥的特殊通信的通信量，即可仅对所期望的接收移动机安全地实施解密密钥的发送。并且，根据本发明，在通过播放信道接收数据的过程中不间断地更新解密密钥。根据本发明，可以抑制对话数量的增加及业务量的增加，接收解密密钥。并且，根据本发明，可以缩短终端生成解密密钥的处理时间。另外，根据本发明，可以缩短终端开始对话后到播放数据的接收开始的时间。并且，根据本发明，可以使发送解密密钥的定时按照每个无线终端错开，防止同一时期的通信集中。

附图说明

[0056] 图 1 是用于发送解密密钥的 1xEV-DO 网络的结构图。

[0057] 图 2 是表示已知方法的解密密钥发送步骤的图。

[0058] 图 3 是表示终端认证时的解密密钥发送步骤的图。

[0059] 图 4 是表示解密密钥切换方法的图。

[0060] 图 5 是表示再认证处理的解密密钥发送步骤的图。

[0061] 图 6 是表示数据通信中的解密密钥发送步骤的图。

[0062] 图 7 是表示发送 3 个以上的数的解密密钥的步骤的图。

[0063] 图 8 是表示发送了 3 个以上的数的解密密钥时的密钥切换方法的图。

[0064] 图 9 是表示采用 AN-AAA 的密钥切换信息发送方法的图。

[0065] 图 10 是表示 AT 硬件的图。

[0066] 图 11 是表示 AT 的解密密钥数据库的图。

[0067] 图 12 是表示 AN-AAA 硬件的图。

[0068] 图 13 是表示 AN-AAA 的解密密钥数据库的图。

[0069] 图 14 是表示 AN-AAA 的加入者数据库的图。

[0070] 图 15 是表示 BCMCS Controller 硬件的图。

[0071] 图 16 是表示 BCMCS Controller 的加密密钥、解密密钥数据库的图。

[0072] 图 17 是表示内容服务器硬件的图。

[0073] 图 18 是表示内容服务器的加密密钥数据库的图。

[0074] 图 19 是表示 PCF 硬件的图。

[0075] 图 20 是表示 PCF 的解密密钥数据库的图。

[0076] 图 21 是表示 PCF 的呼叫控制数据库的图。

[0077] 图 22 是表示 Access Accept 消息格式的图。

[0078] 图 23 是 AN-AAA105 的认证、密钥发送处理的流程图。

[0079] 图 24 是以往的网络结构图。

具体实施方式

[0080] （硬件结构和数据格式）

[0081] 图 1 是本实施方式的 1xEV-DO 网络系统的结构图。

[0082] 以下，作为发明的实施方式的一例，以图 1 所示的 1xEV-DO 网络为基础进行说明。另外，除图 1 所示的系统以外，本发明也可以适用于具有能够发送加密数据的播放信道、并设有移动机认证的所有系统。

[0083] 本系统例如具有：AN（基地局）103；PCF（包控制装置）104；AN-NNN（认证装置）105；BSN(BCMCS 服务装置）106；PDSN（包数据服务装置）107；内容服务器 108；BCMCS Controller(BCMCS 控制装置）109；和 AAA110。并且，由于向 AT 发送播放数据的解密用的解密密钥，所以具有与管理解密密钥的 BCMCS Controller109 的连接。另外，关于各个装置，由于与上述说明的相同，所以省略说明。

[0084] 图 10 表示 AT 的硬件结构图。AT 具有：CPU1001，处理用于进行与 AN103 的通信的呼叫控制协议和数据传送机构；存储器 1002，被用作正在执行中的软件和数据处理的临时存储介质；外部存储装置 1003，具有管理将被加密的播放数据解密用的解密密钥的解密密钥数据库；调制解调器 1005，对发送给 AN103 的数据进行向无线信号的调制，并且进行从无线信号中取出从 AN103 接收的数据的解调；和进行无线接收及发送的 RF(Radio Rrequency) 电路 1006。各部分例如通过用于实现功能之间的通信的通信线即通信总线 1004 相连接。

[0085] AT 从 AN103 接收播放数据时，RF 电路 1006 进行电波的接收，调制解调电路 105 从

无线信号中取出数据。所取出的播放数据暂且被写入存储器 1002。CPU1001 为了进行写入存储器 1002 的接收数据的解密，访问具有解密密钥数据库的外部存储装置 1003，并获取对应的解密密钥。例如，参照解密密钥数据库的有效时间，获取对应当前时间的解密密钥。并且，CPU1001 进行写入存储器 1002 的接收数据的解密，由此完成播放数据的接收。

[0086] 图 11 表示由 AT 保存的解密密钥数据库的具体结构示例。在解密密钥数据库 1003 中包含 ：内容类别 1101 ；密钥类别 1102 ；密钥有效时间 1103 ；对应该内容类别 1101 和密钥有效时间 1103 的解密密钥 1104。在该数据库中可以包含多个内容信息。AT 在接收被加密的播放数据时，根据当前时间和所接收的播放数据的内容类别，选择写入该解密密钥数据库 1003 中的解密密钥，通过使用该解密密钥进行播放数据的解密。另外，也可以省略密钥类别。并且，内容类别也可以是用于识别各个内容的识别信息，还可以是表示内容的小组的信息。

[0087] 图 12 表示 AN-AAA105 的硬件结构图。AN-AAA105 具有 ：CPU1201，处理用于进行与 PCF104 和 BCMCS Controller 109 的通信的呼叫控制协议和终端认证时的计算、解密密钥的发送 ；存储器 1202，被用作正在执行中的软件和数据处理的临时存储介质 ；第 1 外部存储装置 1203，具有管理用于解密被加密的播放数据的解密密钥的解密密钥数据库 ；第 2 外部存储装置 1204，具有注册了终端认证中使用的密码的管理和可否向该移动机发送与哪种内容相关的解密密钥的加入者数据库 ；作为接口的网络 I/F1206，用于和 PCF104 和 BCMCS Controller 109 等外部装置进行通信。各部分例如通过用于实现功能之间的通信的通信线即通信总线 1204 相连接。并且，第 1 和第 2 外部存储装置也可以利用一个存储装置构成。

[0088] AN-AAA105 通过网络 I/F1206 从 PCF104 接收终端认证请求，该终端认证请求被暂且保存在存储器 1202 中。CPU1201 读取保存在存储器 1202 中的终端认证请求，为了获取对于生成了终端认证请求的移动机的密码，访问具有加入者数据库的外部存储装置 1204。CPU1201 确认在终端认证请求中接收的密码、和保存在具有加入者数据库的外部存储装置 1204 中的密码一致时（或者基于密码的认证符一致时），视为终端认证成功。并且，为了获取用于发送给移动机的解密密钥，访问具有解密密钥数据库的外部存储装置 1203，并获取解密密钥。CPU1201 通过网络 I/F1206 把终端认证成功的结果和解密密钥发送给 PCF104。另外，在终端认证不成功时，可以省略解密密钥的获取及发送。

[0089] 图 13 表示由 AN-AAA105 保存的解密密钥数据库 1203 的具体结构示例。在解密密钥数据库 1203 中包含 ：内容类别 1301 ；密钥类别 1302 ；密钥有效时间 1303 ；对应该内容类别 1301 和密钥有效时间 1303 的解密密钥 1304。在该数据库中可以包含多个内容信息。AN-AAA105 为了向终端认证成功的 AT 发送解密密钥，参照该解密密钥数据库 1203 获取所期望的解密密钥。另外，也可以省略密钥类别。AN-AAA105 预先从管理加密密钥和解密密钥的 BCMCS Controller 109 获取解密密钥等并存储。具体步骤将在后面叙述。

[0090] 图 14 表示由 AN-AAA105 保存的加入者数据库的具体结构示例。加入者数据库 1204 具有 ：在终端认证中使用的终端认证表 1401 ；表示允许终端接收哪个内容的注册状况的内容注册表 1402。

[0091] 终端认证表 1401 是表示移动机识别符 1403 和密码 1404 的对应关系的表。内容注册表 1402 是移动机识别符 1405 和表示是否允许该移动机接收内容的注册内容 1406 的对应表。终端认证表 1401 和内容注册表 1402 可以预先注册。另外，也可以利用一个表构

成这两个表 1401 和 1402。并且，除采用表结构外，也可以利用合适的形式存储。这一点对其他表也相同。

[0092] 图 15 表示 BCMCS Controller 109 的硬件结构图。BCMCS Controller109 具有：CPU1501，处理用于进行与 AN-AAA105 和内容服务器 108 的通信的呼叫控制协议；存储器 1502，被用作正在执行中的软件和数据处理的临时存储介质；外部存储装置 1503，具有管理对于各个播放数据内容的加密密钥和解密密钥的表的加密密钥及解密密钥数据库；作为接口的网络 I/F1505，用于和 AN-AAA105 及内容服务器 108 等外部装置进行通信。各部分例如通过用于实现功能之间的通信的通信线即通信总线 1504 相连接。BCMCS Controller 109 在向 AN-AAA105 和内容服务器 108 发送加密密钥和解密密钥时，CPU1501 访问具有加密密钥及解密密钥数据库的外部存储装置 1503，并获取加密密钥和解密密钥。这些密钥通过网络 I/F1505 发送给 AN-AAA105 和内容服务器 108。

[0093] 图 16 表示由 BCMCS Controller 109 保持的加密密钥及解密密钥数据库的具体结构示例。在加密密钥及解密密钥数据库 1503 中包含：内容类别 1601；密钥有效时间 1602；对应该密钥类别 1601 和密钥有效时间 1602 的加密密钥 1603 和解密密钥 1604。在该数据库中可以包含多个内容信息。BCMCS Controller 109 在向 AN-AAA105 发送解密密钥时、以及向内容服务器 108 发送加密密钥时，使用注册在该数据库中的信息。另外，各个信息可以预先手动或自动注册。

[0094] 图 17 表示内容服务器 108 的硬件结构图。内容服务器 108 包括：CPU1701，处理用于进行与 BSN106 和 BCMCS Controller 109 的通信的呼叫控制协议；存储器 1702，被用作正在执行中的软件和数据处理的临时存储介质；外部存储装置 1703，具有管理对于各个播放数据内容的加密密钥的表的加密密钥数据库；作为接口的网络 I/F1705，用于和 BSN106 及 BCMCS Controller 109 等外部装置进行通信。各部分例如通过用于实现功能之间的通信的通信线即通信总线 1704 相连接。

[0095] 内容服务器 108 从 BCMCS Controller 109 接收表示将播放数据加密所需要的加密密钥和解密密钥的有效时间的信息，并保存在具有加密密钥数据库的外部存储装置 1703 中。内容服务器 108 在发送播放数据时，使用保存在加密密钥数据库 1703 中的、对应于内容类别和当前时间的加密密钥信息，进行播放数据的加密，并通过网络 I/F1705 发送给 BSN106。

[0096] 图 18 表示由内容服务器 108 保持的加密密钥数据库 1703 的具体结构示例。在加密密钥数据库 1703 中包含：内容类别 1801；密钥有效时间 1802；对应于该密钥类别 1801 和密钥有效时间 1802 的加密密钥 1803。在该数据库中可以包含多个内容信息。内容服务器 108 在向 BSN106 发送播放数据时，使用保存在该数据库 1703 中的加密密钥 1803 进行加密。

[0097] 图 19 表示 PCF104 的硬件结构图。PCF104 具有：CPU1901，处理用于进行与 BSN106 和 AN103 的通信的呼叫控制协议；存储器 1902，被用作正在执行中的软件和数据处理的临时存储介质；第 3 外部存储装置 1903，具有管理对各个播放数据内容的解密密钥的表的解密密钥数据库；第 4 外部存储装置 1904，具有管理已发送给 AT 的解密密钥的呼叫控制数据库；作为接口的网络 I/F1906，用于和 BSN106 及 AN103 等外部装置进行通信。各部分例如通过用于实现功能之间的通信的通信线即通信总线 1905 相连接。

[0098] PCF104 把通过终端认证从 AN-AAA105 获取的解密密钥保存在具有解密密钥数据

库的外部存储装置 1903 中。并且，PCF104 为了管理已发送给 AT 的解密密钥，在具有呼叫控制数据库的外部存储装置 1904 中，按照每个移动机管理已发送的解密密钥及 / 或其有效时间。根据记录在呼叫控制数据库 1904 中的内容，可以进行解密密钥的再发送处理。

[0099] 图 20 表示由 PCF104 保存的解密密钥数据库的具体结构示例。在解密密钥数据库中包含 ：内容类别 2001 ；密钥有效时间 2002 ；对应该内容类别 2001 和密钥有效时间 2002 的加密密钥 2003。在该数据库中可以包含多个内容信息。PCF104 在进行终端认证时从 AN-AAA105 接收解密密钥，并在该数据库中保留记录。另外，也可以省略解密密钥数据库 1903。

[0100] 图 21 表示由 PCF104 保持的呼叫控制数据库的具体结构示例。呼叫控制数据库包括 ：识别移动机时使用的移动机识别符 2101 ；与已发送给通过移动机识别符 2101 识别的移动机的解密密钥对应的内容类别 2102 ；表示已发送给移动机的解密密钥的有效时间的已发送密钥有效时间 2103。PCF104 以记录在呼叫控制数据库中的内容为基础，确认密钥的有效时间，并可以用于判断密钥的再发送时间。例如，可以参照已发送密钥有效时间 2103，在有效时间的结束时间之前的规定时间，重新向 AT 发送解密密钥。另外，已发送密钥有效时间可以只存储对应最新的解密密钥的时间，也可以只存储最新的解密密钥的有效时间的结束时间。并且，还可以包括已发送的多个有效时间。

[0101] 图 22 表示从 AN-AAA105 向 PCF104 传送解密密钥时使用的 AccessAccept 消息的格式示例。Code 字段 2201 表示 Access Accept 消息的消息类别。Identifier 字段 2202 表示每当发送消息时被变更的值，在消息的再发送控制等中使用。Length 字段 2203 利用八位单位表示消息的整体长度。Response Authenticator 字段 2204 在进行 AN-AAA105 和 PCF104 之间的认证时使用。

[0102] 利用 Decryption Key 信息要素 2205 定义发送在本发明中使用的解密密钥和其有效时间用的字段。在 Vendor Id 字段 2206 中，作为示例表示设定按照 3GPP2 定义的值即 159FH。在 Vendor type 字段 2207 中，例如输入表示解密密钥包含于该信息要素中的值即 3FH。在 Vendor-length 字段 2208 中，以包含 Vendor-length 字段 2208 的长度存储着 Vendortype 字段 2207 以后的字段中包含的字段长度。

[0103] Content ID 字段 2209 表示内容的类别，Decryption Key 字段 2210 表示解密密钥。Start Time 字段 2211 表示解密密钥有效时间的开始时间，End Time 字段 2212 表示解密密钥有效时间的结束时间。另外，AN-AAA105 除了向 AT 发送 Access Accept 消息外，还可以在用于通知认证的通过 / 不通过的合适的消息信号中包含解密密钥、有效时间等。

[0104] （解密密钥发送步骤）

[0105] 图 3 表示终端认证时的解密密钥发送步骤。

[0106] 内容服务器 108 通过 BSN106、PCF104 向 AN103 发送播放数据。并且，在 AN103 接收的播放数据，被使用播放信道无线发送给 AT101(301)。此时，在 AT101 接收的数据被加密，由于 AT101 未持有用于解密的密钥（解密密钥），所以接收数据在 AT101 中被废弃。内容服务器 108 在发送播放数据时，使用在内部保持的保存于加密密钥数据库 1703 中的加密密钥，进行播放数据的加密，然后进行发送。

[0107] 在 AT101 和 AN103 之间进行 1xEV-DO 对话的建立 (302)。例如，可以借助电源接通等预先确定的合适的契机来建立。并且，建立用于进行单点通信的连接 (303)。另外，该

连接的建立是在建立 1xEV-DO 对话后首次建立的连接，所以作为实施终端认证的准备，在 AN103 和 PCF104 之间建立认证用总线 (304)。

[0108] 为了在 AT101 和 PCF104 之间实施终端认证，进行被 PPP 定义的 LCP 的建立 (305)。PCF104 发送用于请求终端认证的 CHAP Request 消息 (306)。AT101 使用在 CHAP Request 消息中接收的信息和由 AT101 持有的移动机固有信息等，计算认证符，把包括认证符和移动机识别符的 CHAP Response 消息发送给 PCF104(307)。另外，除了 CHAP Request 消息、CHAP Response 消息外，也可以使用合适的消息。

[0109] PCF104 把包含所接收的认证符和移动机识别符的 Access Request 消息发送给 AN-AAA105(308)。AN-AAA105 在判断所接收的认证符的妥当性时，向 PCF104 发送表示已通过终端认证的 Access Accept 消息 (309)。在本实施方式中，在该 Access Accept 消息中，例如发送用于解密在步骤 301 正发送的播放数据所需要的解密密钥（图中的当前的解密密钥）、用于解密将来发送的播放数据所需要的解密密钥（图中的将来的解密密钥）、和密钥的有效时间。关于这些信息的用途将在后面说明。

[0110] 图 23 是 AN-AAA105 的认证、密钥发送处理的流程图。另外，这些各个处理例如可以通过 AN-AAA105 的 CPU1201 执行。

[0111] 首先，AN-AAA105 接收 Access Request 消息 (S11，对应图 3 中的 308)，进行终端认证 (13)。例如，AN-AAA105 根据消息中包含的移动机识别符，参照加入者数据库 1204 的终端认证表，获取对应的密码。并且，AN-AAA105 根据移动机识别符和密码等，利用与 AT 相同的手法求出认证符，将所求出的认证符与 Access Request 消息中包含的认证符对比，如果一致则判断为已通过终端认证。另一方面，在不一致时，可以进行向 PCF104 发送表示认证不成功的信息等的规定处理。另外，除了计算认证符以外，例如，也可以采用通过对比移动机识别符和密码来进行认证等的合适的认证方法。

[0112] 在通过终端认证时，AN-AAA105 根据所接收的移动机识别符，参照加入者数据库 1204 的内容注册表，获取对应的注册内容的类别（例如识别符）(S15)。另外，根据所获取的注册内容的类别，参照解密密钥数据库 1203，获取对应的解密密钥和有效时间 (S17)。另外，解密密钥和有效时间可以分别获取预先确定的数。AN-AAA105 使 Access Accept 消息中包含所获取的解密密钥和有效时间，并发送给 PCF104 或 AT(S19，对应图 3 中的 309)。例如，AN-AAA105 在图 22 所示的 Access Accept 消息的格式中，可以分别把所获取的内容的类别存储在 Content ID 字段 2209 中，把所获取的解密密钥存储在 Descryption Key 字段 2210 中，把所获取的有效时间中的开始时间存储在 Start Time 字段 2211 中，把结束时间存储在 End Time 字段 2212 中，然后发送。

[0113] 返回图 3，PCF104 把从 AN-AAA105 接收的信息记录在保持于 PCF104 内部的解密密钥数据库和呼叫控制数据库中。例如，把 Access Accept 消息中包含的内容类别、有效时间、解密密钥分别对应着存储在解密密钥数据库中。此处，保存在数据库中的信息在进行解密密钥的切换时使用。PCF104 通过发送 CHAP Success 消息，通知 AT101 认证已通过。并且，PCF104 向 AT101 发送当前的解密密钥、将来的解密密钥、密钥有效时间 (310)。这些解密密钥等可以包含在 CHAP Success 消息中发送。并且，PCF104 对应发送了解密密钥的 AT101 的移动机识别符，把内容类别和所发送的密钥的有效时间存储在呼叫控制数据库 1904 中。另外，有效时间可以是所发送的多个有效时间中最迟的（最新的），也可以是从最早的时间到

最晚的时间的时间幅度，还可以是有效时间的结束时间。

[0114] AT101 对应在步骤 310 接收的内容类别，把有效时间和解密密钥保存在解密密钥数据库 1003 中，使用解密密钥，解密从 AN103 发送的被加密的播放数据 (311)。

[0115] 这样，通过在进行终端认证时发送用于解密播放数据的解密密钥，可以省略在图 2 的已知步骤中看到的AT101和PDSN107之间的PPP建立处理、及AT101和BCMCS Controller 109 之间的业务量。

[0116] 下面，说明密钥的更新。

[0117] 图 4 表示解密密钥切换方法的说明图。内容服务器 108 发送被加密的数据，例如，在从时间 t0 到时间 t3 之间（加密密钥 1 的有效时间），发送使用加密密钥 1 加密的数据 (401)。在此期间，由于使用加密密钥 1 加密，所以假定为了进行数据的解密需要解密密钥 1。并且，在时间 t3 以后，发送利用其他加密密钥 2 加密的数据，为了解密该期间的数据需要解密密钥 2(402)。

[0118] AT101 在时间 t0 的时间点保持解密密钥 1，并处于可以解调在时间 t0 的时间点从内容服务器 108 发送的使用加密密钥 1 加密的数据的状态 (403)。并且，AT101 为了能够解调内容服务器 108 从时间 t3 的时间点发送的使用加密密钥 2 加密的数据，在早于时间 t3 的时间 t1 的时间点获取解密密钥 2。因此，在从时间 t1 到时间 t3 之间（解密密钥 1 的有效时间），可以使用解密密钥 1 解调从内容服务器 108 发送的数据，同时保持解密密钥 2，以便在将来接收未来时间 t3 以后的数据时使用 (404)。在时间 t3 以后，将解密密钥 1 废弃，使用解密密钥 2 解调从内容服务器 108 发送的使用加密密钥 2 加密的数据 (405)。

[0119] AT102 在时间 t0 的时间点保持解密密钥 1，并处于可以解调在时间 t0 的时间点从内容服务器 108 发送的使用加密密钥 1 加密的数据的状态 (406)。AT102 为了能够解调内容服务器 108 从时间 t3 的时间点发送的使用加密密钥 2 加密的数据，在早于时间 t3 的时间 t2 的时间点获取解密密钥 2。因此，在从时间 t2 到时间 t3 之间，可以使用解密密钥 1 解调从内容服务器 108 发送的数据，同时保持解密密钥 2，以便在将来接收未来时间 t3 以后的数据时使用 (407)。在时间 t3 以后，将解密密钥 1 废弃，使用解密密钥 2 解调从内容服务器 108 发送的使用加密密钥 2 加密的数据 (408)。

[0120] 这样，在切换内容服务器 108 使用的加密密钥之前，预先向各个 AT 发送切换后的解密密钥，从而 AT 可以继续接收数据。并且，通过按照每个 AT 改变解密密钥的更新定时，可以使负荷不集中汇集于网络和无线上。

[0121] （第 1 解密密钥更新步骤）

[0122] 图 5 表示以再认证处理为契机向 AT 发送解密密钥的步骤。这些步骤例如可以在图 3 所示的处理之后执行。

[0123] BSN106 通过 PCF104 向 AN103 发送播放数据。并且，在 AN103 接收的播放数据，使用播放信道无线发送给 AT101(501)。此时，在 AT101 接收的数据被加密，由于 AT101 已经通过上述处理保持用于解密的密钥（解密密钥）即解密密钥 1，所以接收数据在 AT101 被解密（解密 1），并被正常接收。

[0124] PCF104 为了向 AT101 发送将来使用的解密密钥 2，经由 AN103 向 AT101 发送 AT 呼叫信号 (502)。PCF104 在步骤 309，在呼叫控制数据库中记录已发送给 AT101 的解密密钥的有效时间，AT 呼叫信号可以在该有效时间的结束时间之前的一定时间发送。此时，向呼

叫信号附加表示用于实施终端认证的呼叫信号的信息并发送。该呼叫信号发送契机为解密密钥有效时间期满之前的一定时间，为了避免在同一时期与正在接收播放数据的所有 AT 进行集中通信，可以采用按照每个 AT 错开时间发送的方式。例如，可以隔开预先确定的时间间隔，向各个 AT 发送 AT 呼叫信号，也可以在向发送了 AT 呼叫信号的 AT 发送了解密密钥后，向其他 AT 发送 AT 呼叫信号。

[0125] AT101 响应呼叫信号，建立用于在 AT101 和 AN103 之间进行单点通信的连接 (503)。在建立连接后，作为实施终端认证的准备，在 AN103 和 PCF104 之间建立认证用总线 (504)。

[0126] 并且，为了在 AT101 和 PCF104 之间实施终端认证，进行被 PPP 定义的 LCP 的建立 (505)。PCF104 发送用于请求终端认证的例如 CHAP Recquest 消息 (506)。AT101 使用在 CHAP Response 消息中接收的信息和由 AT101 持有的移动机固有信息等，计算认证符，把包括认证符的 CHAP Response 消息发送给 PCF104(507)。PCF104 向 AN-AAA105 发送包含所接收的认证符的 Access Request 消息 (508)。AN-AAA105 判断所接收的认证符的妥当性，在判断为妥当时，向 PCF104 发送表示已通过终端认证的 AccessAccept 消息 (509)。在该 Access Accept 消息中，发送为了解密在步骤 501 正发送的播放数据所需要的解密密钥 (图中的解密密钥 1)、为了解密将来发送的播放数据所需要的解密密钥 (图中的解密密钥 2)、和各个密钥的有效时间。并且，这些信息被保存在 PCF104 的解密密钥数据库和呼叫控制数据库中。另外，AN-AAA105 的具体处理与上述说明的相同。PCF104 通过发送 CHAP Success 消息，通知认证已通过，并向 AT101 发送解密密钥 1、解密密钥 2 和密钥有效时间 (510)。

[0127] AT101 使用在步骤 510 接收的解密密钥 1 或原来保持的解密密钥 1，解密从 AN103 发送的被加密的播放数据 (解密处理 1)，从而可以进行数据接收 (511)。

[0128] AT101 在到达通过步骤 510 接收的密钥有效时间的结束时间 (或下一个密钥的开始时间) 的时间点，把使用的解密密钥切换为解密密钥 2，使用解密密钥 2 解密播放数据 (解密处理 2)(512)。因此，对经过密钥切换时间，使用加密密钥 2 加密的播放数据，AT101 也能够不间断地持续接收 (513)。

[0129] (第 2 解密密钥更新步骤)

[0130] 图 6 表示 AT101 基于其他目的进行单点数据通信，在进行过程中更新解密密钥的步骤。由于已经正在进行单点通信，相比图 5 所示的进行 AT 呼叫的步骤，可以实现无线资源的有效利用。例如，AT 呼叫信号不再需要，由于 AT 和 AN103 的连接为了进行数据通信已经建立，所以不需要为了发送解密密钥而重新建立连接。

[0131] 例如，对已经正在通信中的 AT 优先进行解密密钥的更新，在解密密钥的有效时间期满之前 (或其规定时间之前)，可以只对没有进行单点通信的 AT 采用上述图 5 所示的方法。以下，表示对正在通信中的 AT 的解密密钥更新步骤。

[0132] BSN106 通过 PCF104 向 AN103 发送播放数据。并且，在 AN103 接收的播放数据，被使用播放信道无线发送给 AT101(601)。此时，在 AT101 接收的数据被加密，由于 AT101 保持有用于解密的密钥 (解密密钥) 即解密密钥 1，所以接收数据在 AT101 被解密，从而可以接收数据。

[0133] AT101 例如为了开始 Web 访问等的单点数据通信 (602)，在 AT101 和 AN103 之间建立连接 (603)。该数据通信的开始契机，假定为想要使用 AT101 进行数据通信的用户利

用 Web 浏览器访问主页时等，即使用 AT101 的用户的情况。AT101 和 PDSN107 通过 AN103、PCF104 进行单点数据通信 (604)。PCF104 识别正在数据通信中的 AT101，例如可以管理终端的识别符等。

[0134] PCF104 为了向 AT101 发送将来使用的解密密钥 2，与 AN103 之间进行认证用连接的建立处理 (605)。该认证用连接的建立契机为解密密钥有效时间期满之前的一定时间，为了避免在同一时期与正在接收播放数据的所有 AT 进行集中通信，可以采用按照每个 AT 错开时间实施的方式。为了在 AT101 和 PCF104 之间实施终端认证，进行被 PPP 定义的 LCP 的建立 (606)。PCF104 发送用于请求终端认证的 CHAP Request 消息 (607)，AT101 使用在 CHAP Response 消息中接收的信息和由 AT101 持有的移动机固有信息等，计算认证符，把包括认证符的 CHAP Response 消息发送给 PCF104(608)。PCF104 向 AN-AAA105 发送包含所接收的认证符的 AccessRequest 消息 (609)。AN-AAA105 判断所接收的认证符的妥当性，在判断为妥当时，向 PCF104 发送表示已通过终端认证的 Access Accept 消息 (610)。在该 Access Accept 消息中，发送为了解密在步骤 601 正发送的播放数据所需要的解密密钥（图中的解密密钥 1）、为了解密将来发送的播放数据所需要的解密密钥（图中的解密密钥 2）、和各个密钥的有效时间。另外，更具体的处理与上述说明的相同。PCF104 通过发送 CHAPSuccess 消息，通知 AT101 认证已通过，并向 AT101 发送当前的解密密钥、将来的解密密钥和密钥有效时间 (611)。

[0135] AT101 使用在步骤 611 接收的解密密钥 1 或原来保持的解密密钥 1，解密从 AN103 发送的被加密的播放数据（解密处理 1），从而可以进行数据接收 (612)。

[0136] AT101 在到达通过步骤 611 接收的密钥切换时间的时间点，把使用的解密密钥切换为解密密钥 2(613)。因此，对经过密钥切换时间，使用加密密钥 2 加密的播放数据，可以使用解密密钥 2 进行解密（解密处理 2），所以 AT101 能够不间断地持续接收 (614)。

[0137] （第 1 解密密钥更新步骤的变形）

[0138] 图 7 表示发送 3 个以上的多个（以后设为 n 个）解密密钥的步骤。BSN106 通过 PCF104 向 AN103 发送播放数据。并且，在 AN103 接收的播放数据，被使用播放信道无线发送给 AT101(701)。此时，在 AT101 接收的数据被加密，由于 AT101 保持着用于解密的密钥（解密密钥）即解密密钥 1，所以接收数据在 AT101 被解密，并被正常接收。

[0139] PCF104 为了向 AT101 发送将来使用的 n 个解密密钥，经由 AN103 向 AT101 发送 AT 呼叫信号 (702)。此时，向呼叫信号附加表示用于实施终端认证的呼叫信号的信息并发送。

[0140] AT101 响应呼叫信号，建立用于在 AT101 和 AN103 之间进行单点通信的连接 (703)。在建立连接后，作为实施终端认证的准备，在 AN103 和 PCF104 之间建立认证用总线 (704)。

[0141] 为了在 AT101 和 PCF104 之间实施终端认证，进行被 PPP 定义的 LCP 的建立 (705)。PCF104 发送用于请求终端认证的 CHAP Request 消息 (706)。AT101 使用在 CHAP Response 消息中接收的信息和由 AT101 持有的移动机固有信息等，计算认证符，把包括认证符的 CHAP Response 消息发送给 PCF104(707)。PCF104 向 AN-AAA105 发送包含所接收的认证符的 AccessRequest 消息 (708)。AN-AAA105 判断所接收的认证符的妥当性，在判断为妥当时，向 PCF104 发送表示已通过终端认证的 Access Accept 消息 (709)。在该 Access Accept 消息中，发送为了解密在步骤 701 正发送的播放数据所需要的解密密钥（图中的解密密钥

1)、为了解密将来发送的播放数据所需要的 n 个解密密钥（图中的解密密钥 2、…、解密密钥 n)、和各个解密密钥的有效时间。例如，AN-AAA105 分别从解密密钥数据库 1203 获取预先确定数的解密密钥和有效时间来进行通信。PCF104 通过发送 CHAP Success 消息，通知认证已通过，并向 AT101 发送当前的解密密钥、将来的解密密钥和密钥有效时间 (710)。

[0142] AT101 使用在步骤 710 接收的解密密钥 1 或原来保持的解密密钥，解密从 AN103 发送的被加密的数据，从而可以进行数据接收 (711)。

[0143] AT101 在到达通过步骤 710 接收的解密密钥 1 的密钥有效时间的结束时间或解密密钥 2 的开始时间的时间点，把解密密钥切换为解密密钥 2(712)。因此，对经过密钥切换时间，使用加密密钥 2 加密的播放数据，AT101 也能够不间断地持续接收 (713)。

[0144] 同样，AT101 在到达向通过步骤 710 接收的解密密钥 3 的密钥切换时间的时间点，把解密密钥切换为解密密钥 3(714)。因此，通过在步骤 710 预先向 AT101 发送多个解密密钥，AT101 不需要为了获取解密密钥而再次进行终端认证。并且，在步骤 702，AT101 未能正常接收呼叫信号时，虽然不能正常发送解密密钥，但由于预先发送了多个解密密钥，所以 AT101 能够继续接收播放数据 (715)。另外，在上述的数据通信中的解密密钥更新中，可以实现通信 3 个以上的多个解密密钥的变形。

[0145] 图 8 表示发送了 n 个解密密钥时的解密密钥切换方法的说明图。内容服务器 108 发送被加密的数据，在从时间 t0 到时间 t2 的期间（加密密钥 1 的有效期间），发送使用加密密钥 1 加密的数据 (801)。在此期间，由于使用加密密钥 1 加密，所以假定为了进行数据的解密需要解密密钥 1。并且，在从时间 t2 到时间 t3 的期间（加密密钥 2 的有效期间），发送使用加密密钥 2 加密的数据，为了进行数据的解密需要解密密钥 2(802)。在时间 tn 以后，发送利用加密密钥 n 加密的数据，为了解密该期间的数据需要解密密钥 n(803)。

[0146] AT101 在时间 t0 的时间点保存解密密钥 1，并处于可以解调在时间 t0 的时间点从内容服务器 108 发送的使用加密密钥 1 加密的数据的状态 (804)。AT101 为了能够解调内容服务器 108 从时间 t2 的时间点发送的使用加密密钥 2 加密的数据，例如需要在早于时间 t2 的时间 t1 的时间点获取解密密钥 2。在该图中，表示在时间 t1 的时间点同时获取解密密钥 2 ～解密密钥 n 的情况。因此，在从时间 t0 到时间 t2 之间，可以使用解密密钥 1 解调从内容服务器 108 发送的数据，同时为了准备接收在未来时间 t2 ～ t3 发送的数据，保持将来使用的解密密钥 2、在时间 t3 以后的使用的解密密钥 3、…、解密密钥 n(805)。在从时间 t2 到时间 t3 之间，已经没有必要保持解密密钥 1，所以保持解密密钥 2、解密密钥 3、…、解密密钥 n，使用解密密钥 2 进行播放数据的解调 (806)。在时间 tn 以后，使用解密密钥 n 解调从内容服务器 108 发送的使用加密密钥 n 加密的数据 (807)。并且，同样在合适的定时获取时间 tn+1 以后的解密密钥 n+1…。作为该定时，例如，参照存储在 PCF104 的呼叫控制数据库 1904 中的已发送密钥有效时间，可以在有效时间的结束时间之前的规定时间获取解密密钥 n+1…。

[0147] 此处，更加具体地说明按照每个 AT 错开时间进行解密密钥的更新的方法的示例。

[0148] PCF104 在呼叫控制数据库 1904 的某个项目到达已发送密钥有效时间的结束时间之前的规定时间时，向终端发送 AT 呼叫信号。在图 21 的示例中，PCF104 在到达有效时间的结束时间 10:00 之前的规定时间时（例如，30 分钟前），向有效时间的结束时间为 10:00 的移动机识别符的任一个（例如 #1）表示的 AT 发送 AT 呼叫信号（对应图 5 中的 502)。然

后，进行终端认证和新的解密密钥（例如，10:00 ～ 12:00 的有效时间的密钥 fghijk）的发送（对应图 5 中的 503 ～ 510）。此时，由于已向移动机识别符 #1 发送新的解密密钥，所以呼叫控制数据库 1904 中的已发送密钥有效时间，例如被改写为 10:00 ～ 12:00。

[0149] 然后，PCF104 向有效时间的结束时间为 10:00 的移动机识别符的任一个（例如 #2）表示的 AT 发送 AT 呼叫信号（对应图 5 中的 502）。与上述说明的相同，进行终端认证和新的解密密钥的发送（对应图 5 中的 503 ～ 510）。此时，对于移动机识别符 #2，由于已发送新的解密密钥，所以呼叫控制数据库 1904 中的已发送密钥有效时间，例如被改写为 10:00 ～ 12:00。因此，有效时间的结束时间为 10:00 的 AT 不再存在，所以 PCF104 结束当前时间的密钥的更新。

[0150] 并且，PCF104 在到达有效时间的结束时间 12:00 的规定时间前，与上述说明的相同，发送 AT 读出信号。另外，此处叙述了逐个发送解密密钥的情况，但在发送多个解密密钥时也相同。另外，在发送多个解密密钥时，对已发送密钥有效时间，可以存储已发送的多个密钥中最早的有效时间的开始时间、和最迟的有效时间的结束时间，还可以存储最迟的有效时间的开始时间和结束时间。

[0151] 这样，对成为发送解密密钥的对象的 AT，可以依次发送 AT 读出信号。并且，可以参照呼叫控制数据库中的已发送密钥有效时间，识别已发送新的解密密钥的 AT、和之后应该发送的 AT。

[0152] 图 9 表示在内容服务器 108 中加密播放数据时使用的加密密钥、和由 AN-AAA105 保持的解密密钥的发送步骤，该解密密钥为通过 AT 解密被内容服务器 108 加密的播放数据所需要的解密密钥。用于加密播放数据的加密密钥和解密密钥及密钥有效时间，通过 BCMCS Controller 109 进行设定。例如，图 16 所示的数据被存储在加密密钥和解密密钥数据库中。这些密钥的设定可以自动生成和自动设定，也可以由人进行手工设定。

[0153] 由 BCMCS Controller 109 设定的加密密钥，通过发送加密密钥更新请求，被通知给进行播放数据的加密的内容服务器 108。在该消息中，例如包括内容类别、用于加密播放数据的加密密钥、和表示密钥的有效时间的信息 (901)。另外，BCMCS Controller 109 参照加密密钥和解密密钥数据库 1503，可以获取一个或多个加密密钥及各个密钥的有效时间。内容服务器 108 正常接收加密密钥更新请求中包含的信息后，把加密密钥更新答复发送给 BCMCS Controller 109，由此通知 BCMCS Controller109 更新已正常完成 (902)。并且，内容服务器 108 把各个信息存储在加密密钥数据库 1703 中。

[0154] 由 BCMCS Controller 109 设定的解密密钥，通过发送解密密钥更新请求，被通知给管理解密密钥等发送给 AT 的信息的 AN-AAA105。在该消息中，例如包括内容类别、用于解密播放数据的解密密钥、和表示密钥的有效时间的信息 (903)。BCMCS Controller 109 可以从加密密钥和解密密钥数据库 1503 中，获取一个或多个解密密钥、对应的内容类别和各个密钥的有效时间，并进行发送。AN-AAA105 正常接收解密密钥更新请求中包含的信息后，把解密密钥更新答复发送给 BCMCS Controller 109，由此通知 BCMCS Controller 109 更新已正常完成 (904)。并且，AN-AAA105 对应着所接收的内容类别，将解密密钥和有效时间存储在解密密钥数据库 1203 中。另外，BCMCS Controller 109 可以按照预先确定的每个时间间隔、或者每当加密密钥和解密密钥数据库 1503 的信息被更新时等，发送加密密钥或解密密钥更新请求。并且，也可以根据 AN-AAA105 和内容服务器 108 的请求，发送加密密钥和

解密密钥。

[0155] 本发明例如可以应用于能够通过播放信道实现被加密数据的发送的无线通信相关产业中。

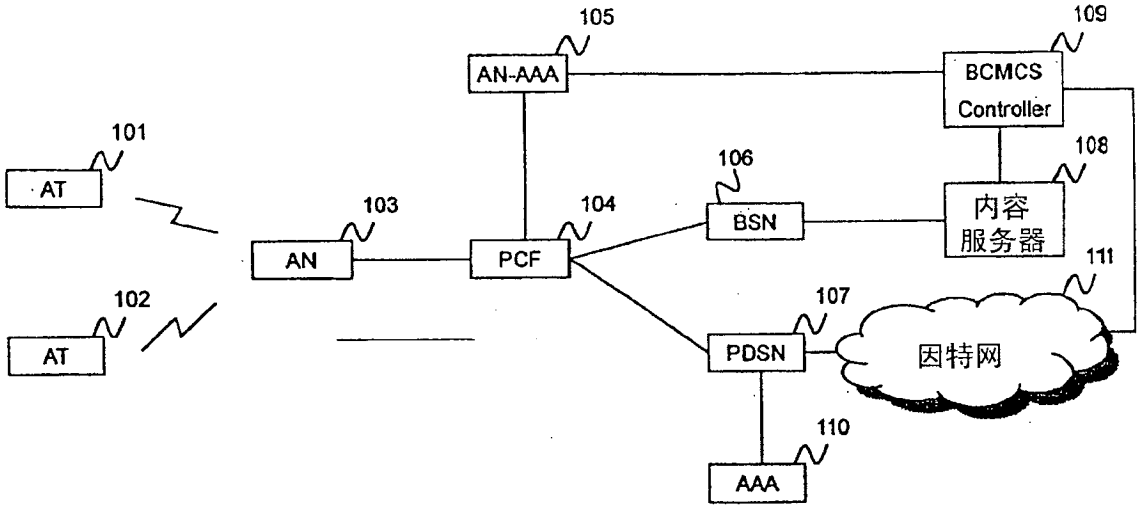

105
AN-AAA
109
BCMCS
Controller
101
AT
106
108
103
104
BSN
内容
服务器
AN
PCF
111
102
107
AT
PDSN
因特网
110
AAA

图 1

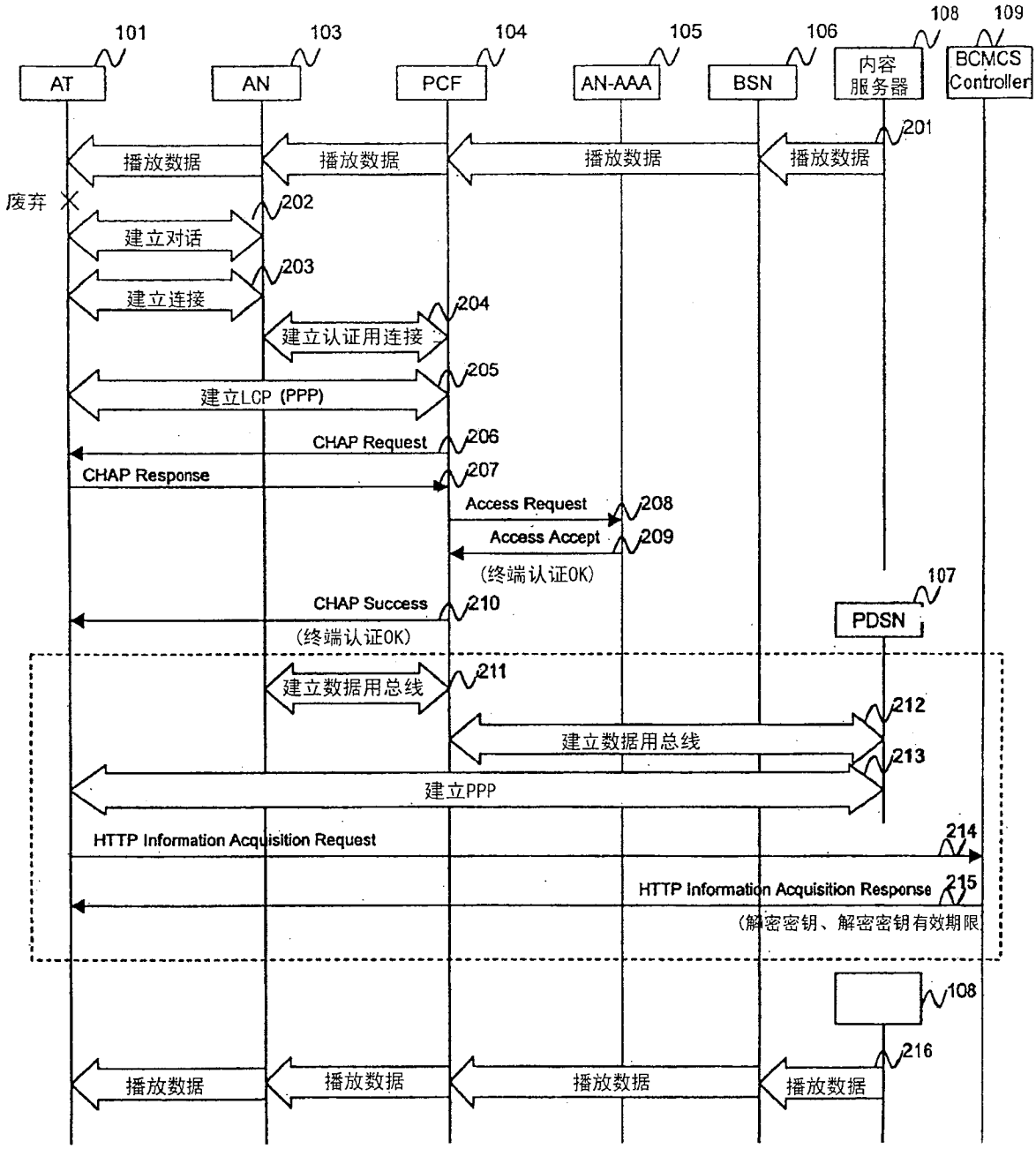

101
103
104
105
106
108
109
AT
AN
PCF
AN-AAA
BSN
内容服务器
BCMCS Controller
201
播放数据
播放数据
播放数据
播放数据
废弃
202
建立对话
203
建立连接
204
建立认证用连接
205
建立LCP (PPP)
CHAP Request
206
CHAP Response
207
Access Request
208
Access Accept
209
(终端认证OK)
107
PDSN
CHAP Success
210
(终端认证OK)
211
建立数据用总线
212
建立数据用总线
213
建立PPP
HTTP Information Acquisition Request
214
HTTP Information Acquisition Response
215
(解密密钥、解密密钥有效期限)
108
216
播放数据
播放数据
播放数据
播放数据

图 2

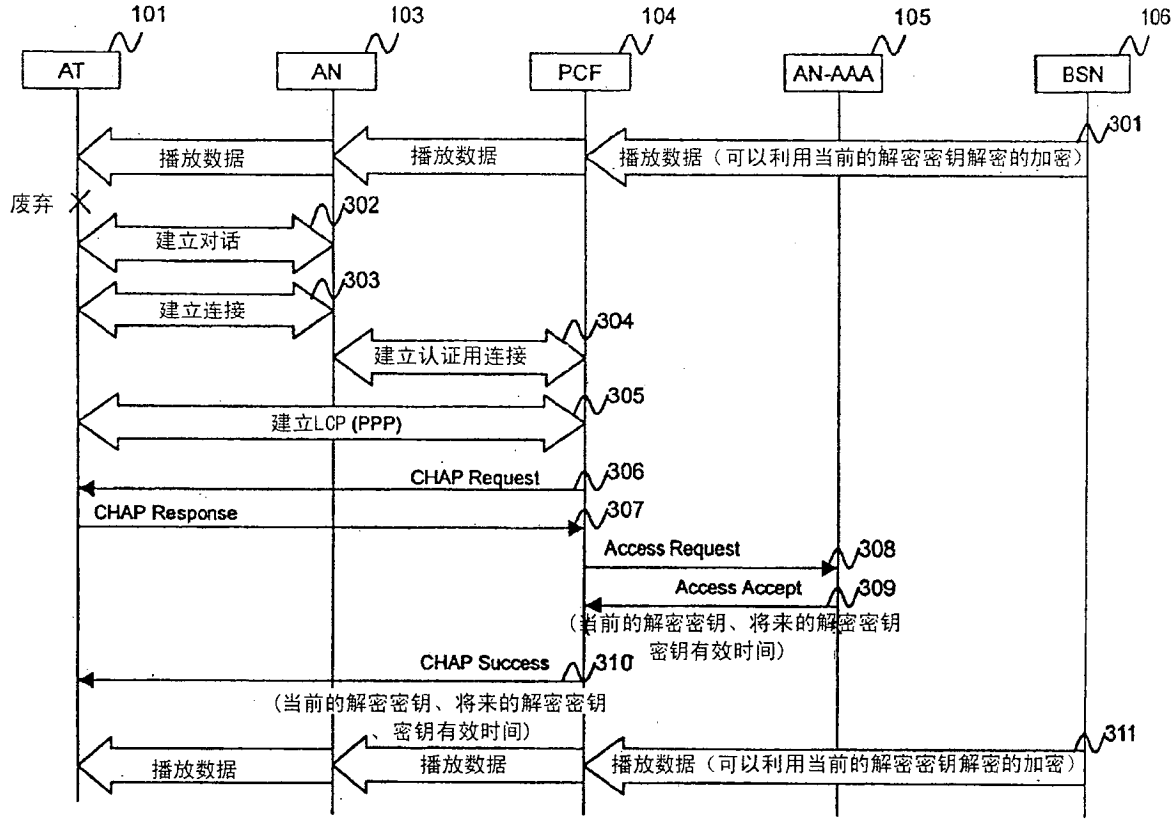
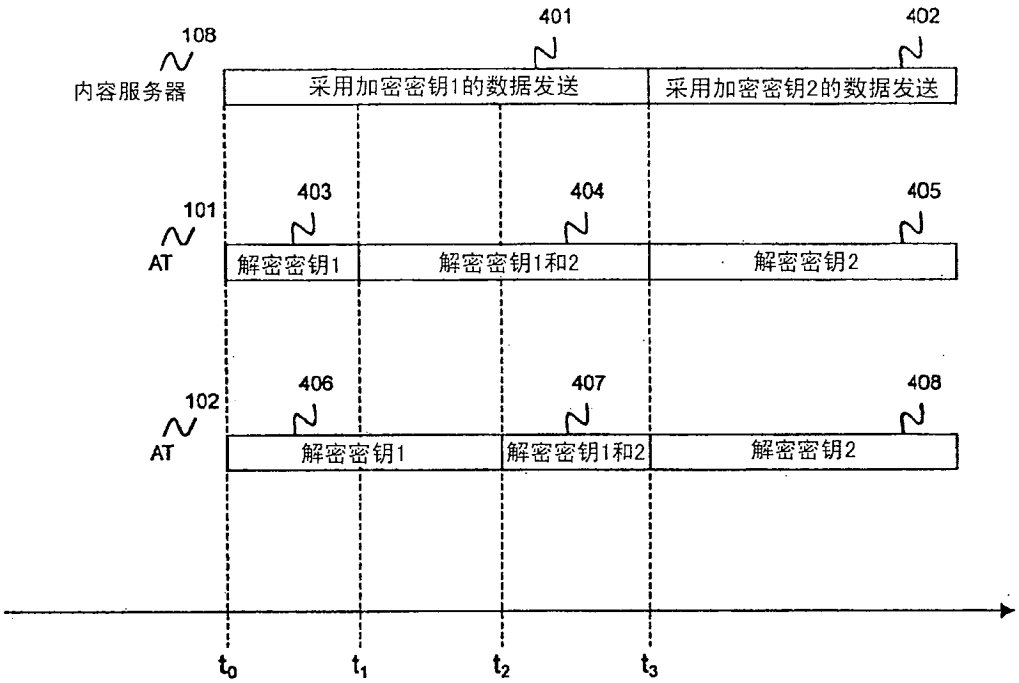

101
103
104
105
106
AT
AN
PCF
AN-AAA
BSN
301
播放数据
播放数据
播放数据（可以利用当前的解密密钥解密的加密）
废弃
302
建立对话
303
建立连接
304
建立认证用连接
305
建立LCP (PPP)
CHAP Request
306
CHAP Response
307
Access Request
308
Access Accept
309
（当前的解密密钥、将来的解密密钥
密钥有效时间）
CHAP Success
310
（当前的解密密钥、将来的解密密钥
、密钥有效时间）
311
播放数据
播放数据
播放数据（可以利用当前的解密密钥解密的加密）

图 3



基于AT101的解密密钥2接收、
基于AT102的解密密钥2接收、密钥切换时间

图 4

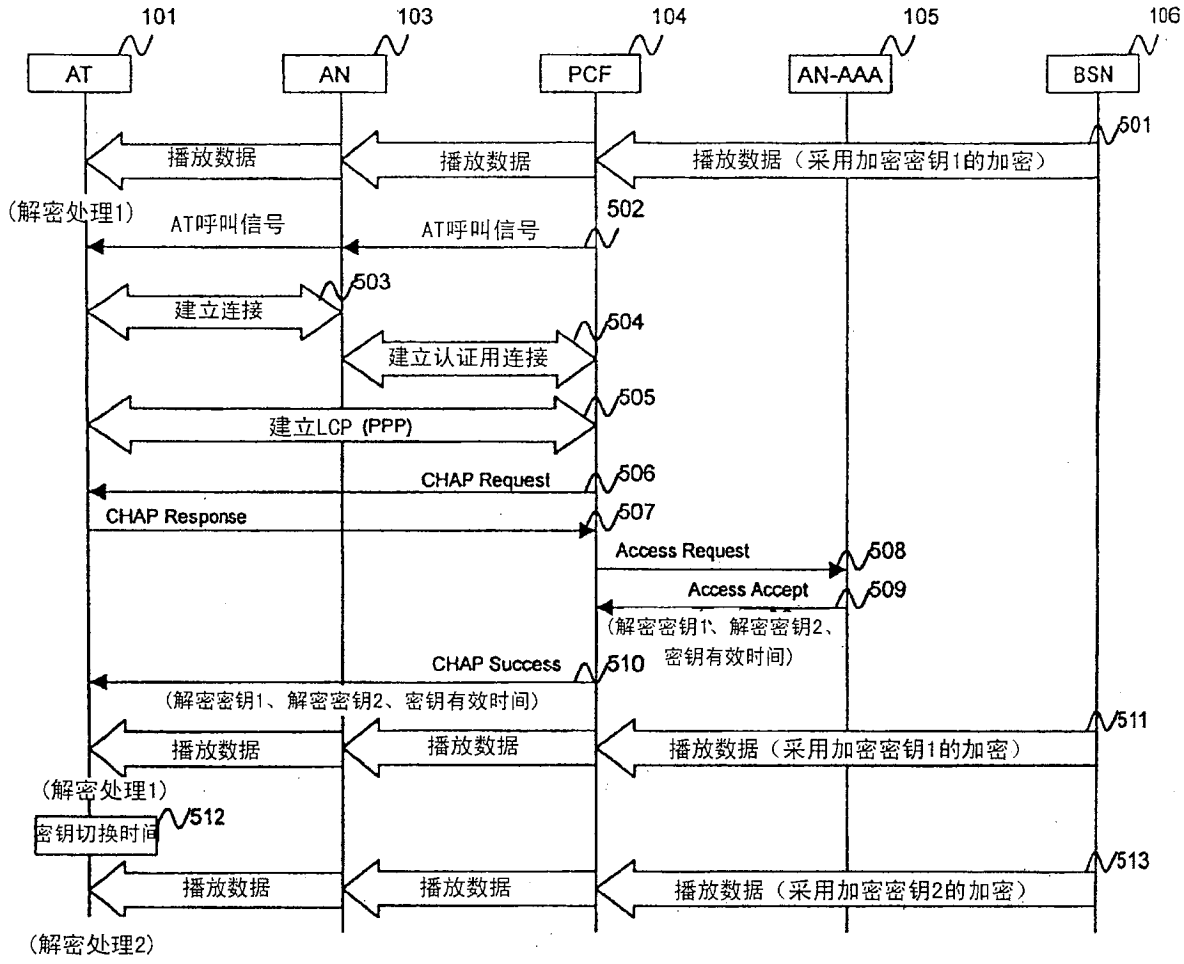

101
103
104
105
106
AT
AN
PCF
AN-AAA
BSN
501
播放数据
播放数据
播放数据（采用加密密钥1的加密）
(解密处理1)
AT呼叫信号
AT呼叫信号
502
503
建立连接
504
建立认证用连接
505
建立LCP (PPP)
CHAP Request
506
CHAP Response
507
Access Request
508
Access Accept
509
(解密密钥1、解密密钥2、
密钥有效时间)
CHAP Success
510
(解密密钥1、解密密钥2、密钥有效时间)
511
播放数据
播放数据
播放数据（采用加密密钥1的加密）
(解密处理1)
密钥切换时间
512
513
播放数据
播放数据
播放数据（采用加密密钥2的加密）
(解密处理2)

图 5

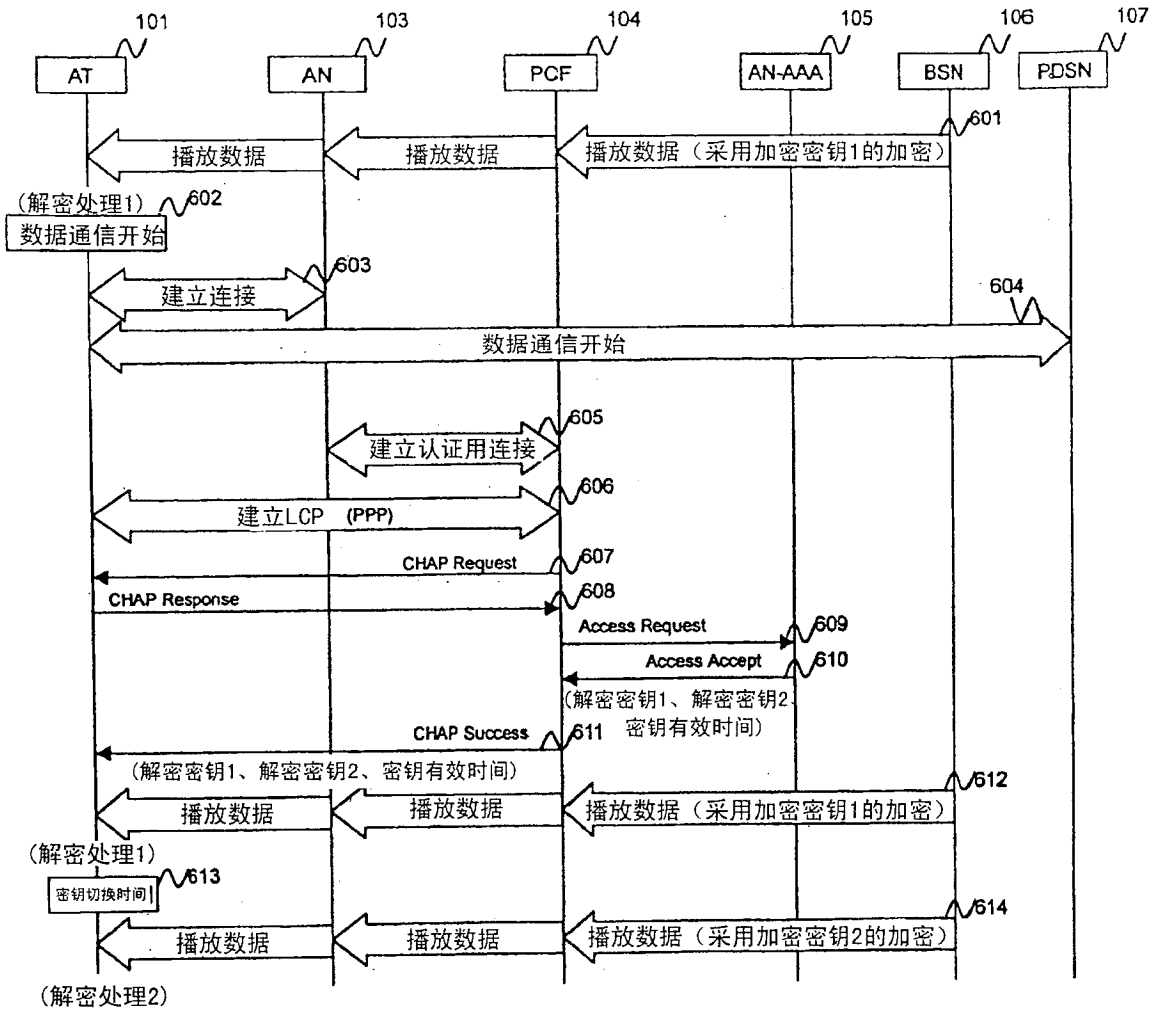

101
103
104
105
106
107
AT
AN
PCF
AN-AAA
BSN
PDSN
601
播放数据
播放数据
播放数据（采用加密密钥1的加密）
(解密处理1)
602
数据通信开始
603
建立连接
604
数据通信开始
605
建立认证用连接
606
建立LCP (PPP)
CHAP Request
607
CHAP Response
608
Access Request
609
Access Accept
610
(解密密钥1、解密密钥2
密钥有效时间)
CHAP Success
611
(解密密钥1、解密密钥2、密钥有效时间)
612
播放数据
播放数据
播放数据（采用加密密钥1的加密）
(解密处理1)
密钥切换时间
613
614
播放数据
播放数据
播放数据（采用加密密钥2的加密）
(解密处理2)

图 6

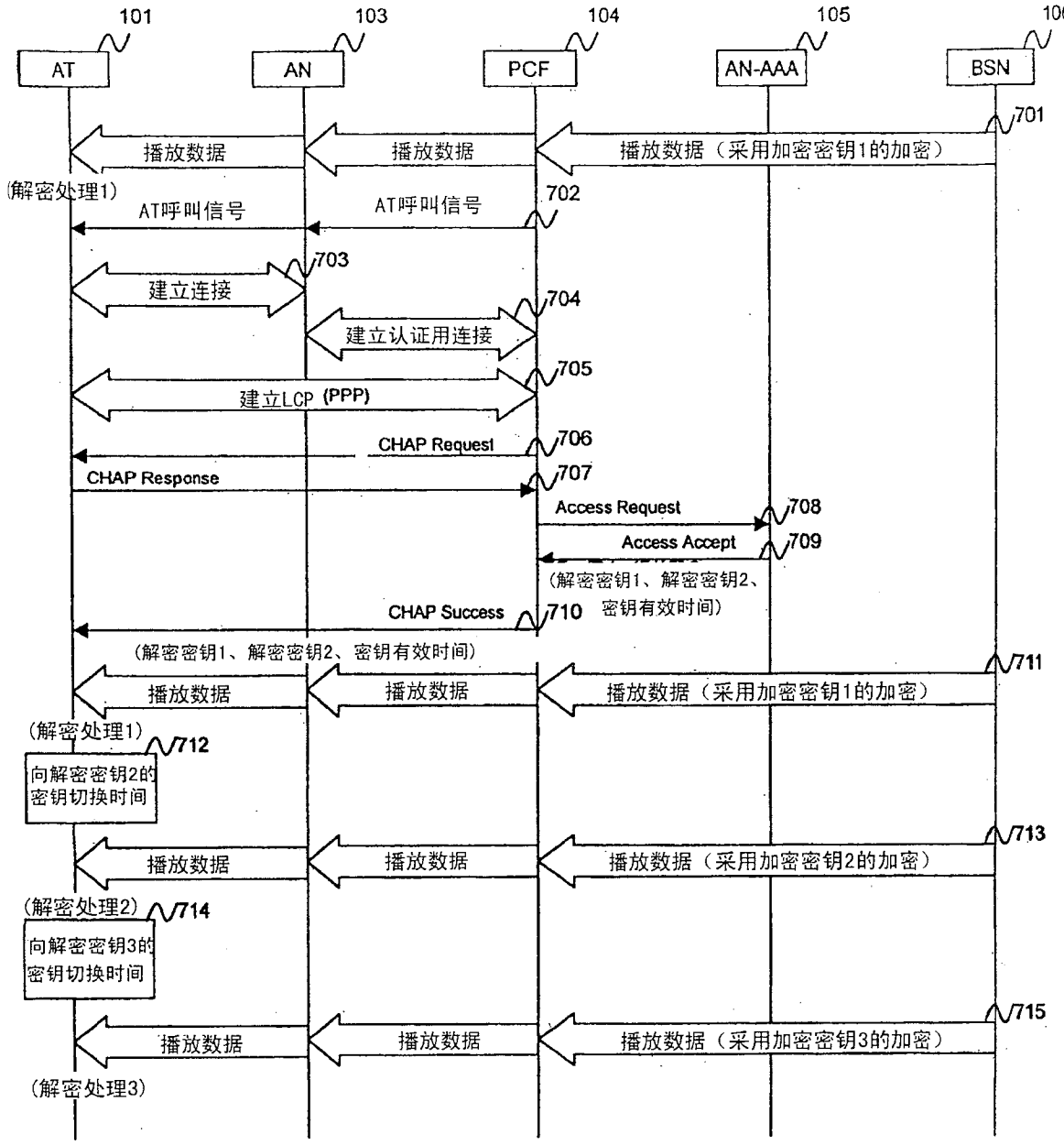

101
103
104
105
106
AT
AN
PCF
AN-AAA
BSN
701
播放数据
播放数据
播放数据（采用加密密钥1的加密）
(解密处理1)
AT呼叫信号
AT呼叫信号
702
703
建立连接
704
建立认证用连接
705
建立LCP (PPP)
CHAP Request
706
CHAP Response
707
Access Request
708
Access Accept
709
(解密密钥1、解密密钥2、
密钥有效时间)
CHAP Success
710
(解密密钥1、解密密钥2、密钥有效时间)
711
播放数据
播放数据
播放数据（采用加密密钥1的加密）
(解密处理1)
712
向解密密钥2的
密钥切换时间
713
播放数据
播放数据
播放数据（采用加密密钥2的加密）
(解密处理2)
714
向解密密钥3的
密钥切换时间
715
播放数据
播放数据
播放数据（采用加密密钥3的加密）
(解密处理3)

图 7

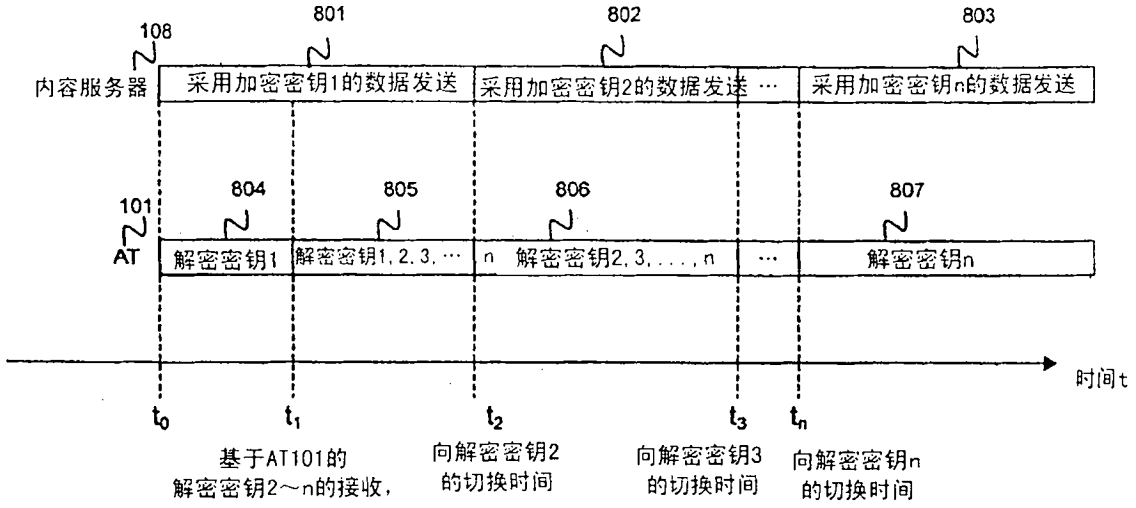

108
801
802
803
内容服务器
采用加密密钥1的数据发送
采用加密密钥2的数据发送 …
采用加密密钥n的数据发送
101
AT
804
805
806
807
解密密钥1
解密密钥1, 2, 3, …
n 解密密钥2, 3, . . . , n
…
解密密钥n
时间t
t_0
t_1
t_2
t_3
t_n
基于AT101的
解密密钥2～n的接收，
向解密密钥2
的切换时间
向解密密钥3
的切换时间
向解密密钥n
的切换时间

图 8

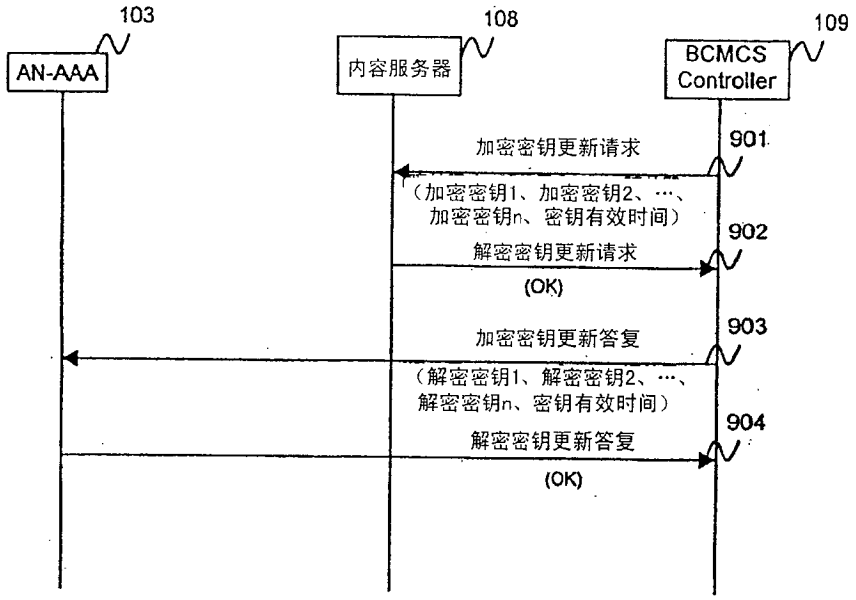

103
AN-AAA
108
内容服务器
109
BCMCS
Controller
加密密钥更新请求
901
（加密密钥1、加密密钥2、…、
加密密钥n、密钥有效时间）
902
解密密钥更新请求
(OK)
加密密钥更新答复
903
（解密密钥1、解密密钥2、…、
解密密钥n、密钥有效时间）
904
解密密钥更新答复
(OK)

图 9

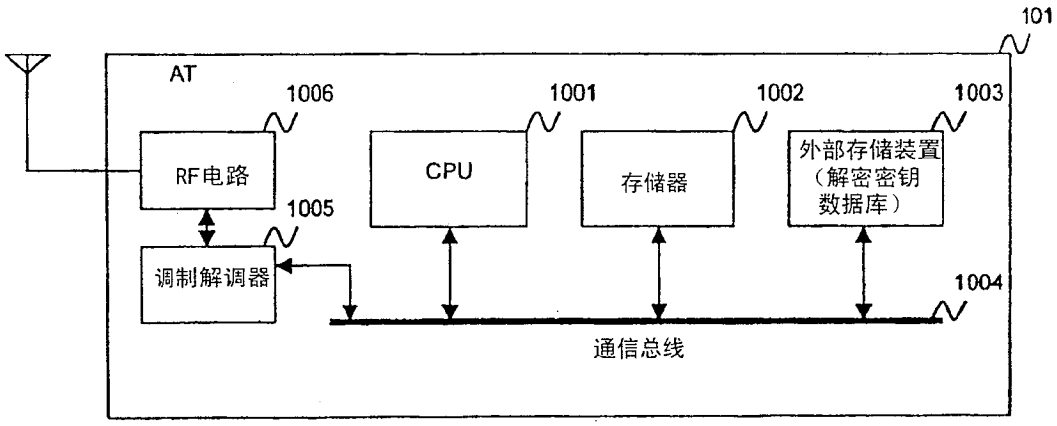
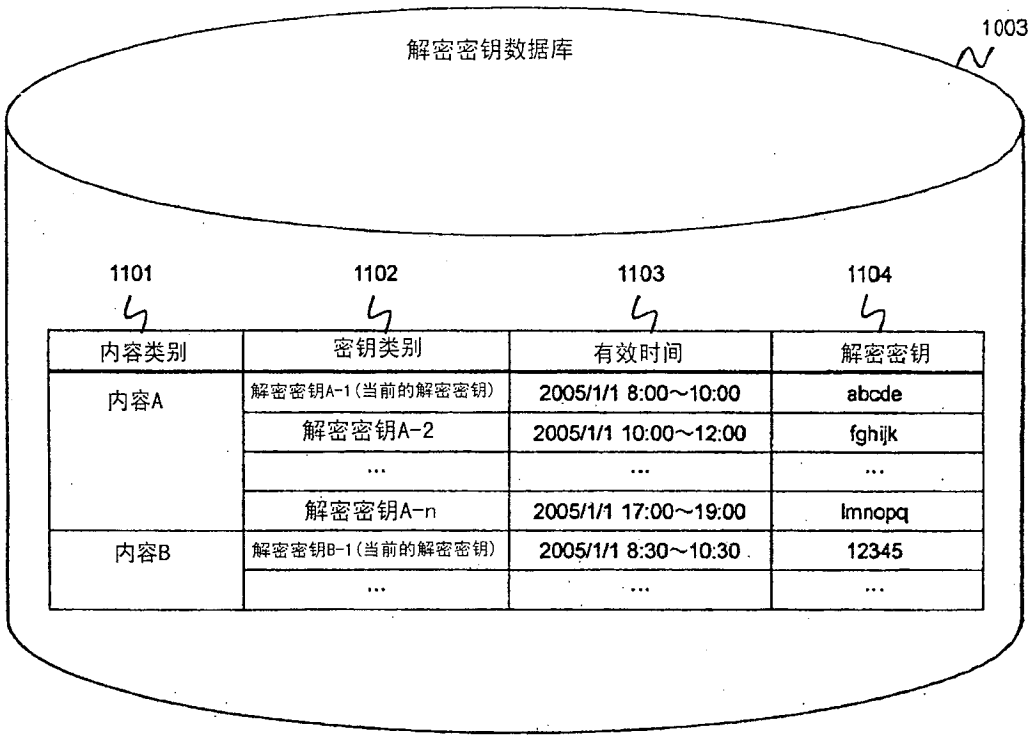


图 10



内容类别	密钥类别	有效时间	解密密钥
内容A	解密密钥A-1（当前的解密密钥）	2005/1/1 8:00～10:00	abcde
	解密密钥A-2	2005/1/1 10:00～12:00	fghijk
	…	…	…
	解密密钥A-n	2005/1/1 17:00～19:00	lmnopq
内容B	解密密钥B-1（当前的解密密钥）	2005/1/1 8:30～10:30	12345
	…	…	…

图 11

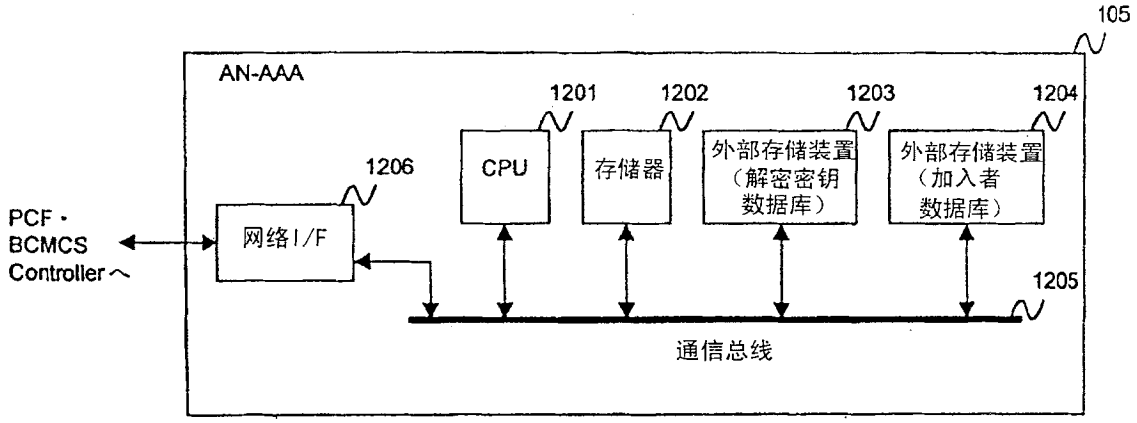
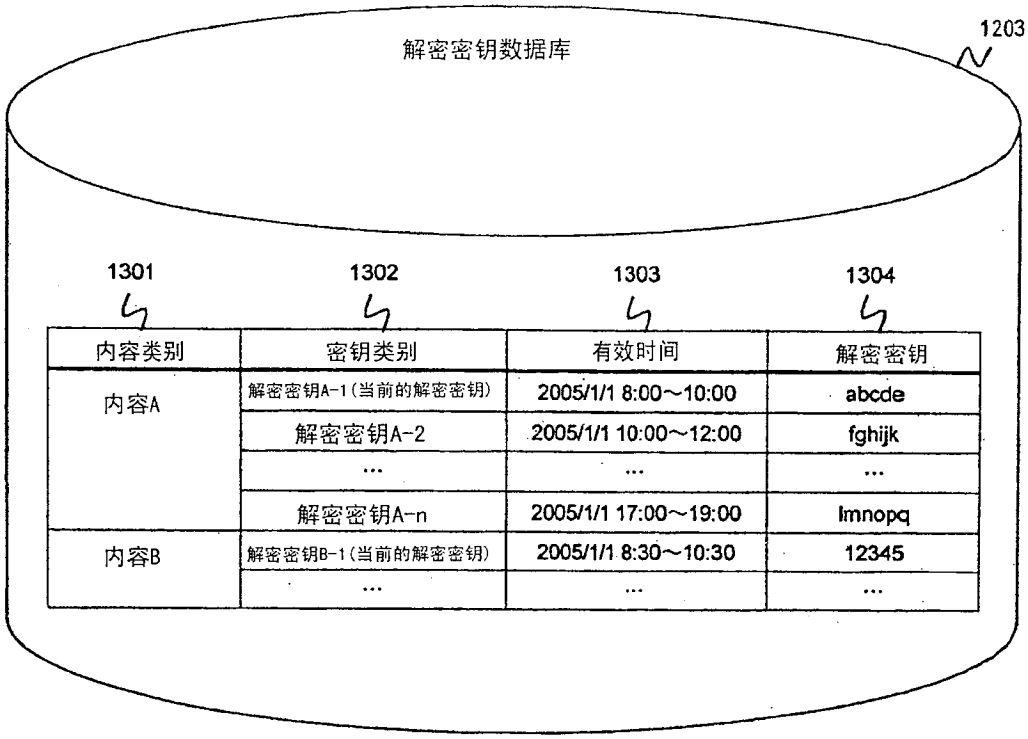


图 12



内容类别	密钥类别	有效时间	解密密钥
内容A	解密密钥A-1（当前的解密密钥）	2005/1/1 8:00～10:00	abcde
	解密密钥A-2	2005/1/1 10:00～12:00	fghijk
	…	…	…
	解密密钥A-n	2005/1/1 17:00～19:00	lmnopq
内容B	解密密钥B-1（当前的解密密钥）	2005/1/1 8:30～10:30	12345
	…	…	…

图 13

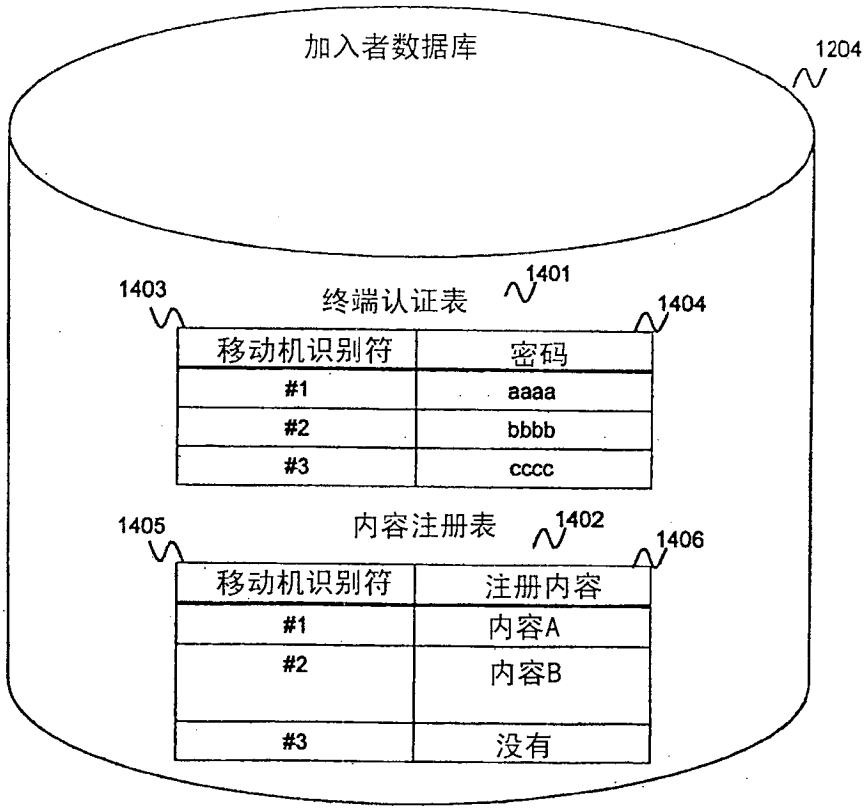

加入者数据库
1204
1403
终端认证表
1401
1404
移动机识别符
密码
#1
aaaa
#2
bbbb
#3
cccc
1405
内容注册表
1402
1406
移动机识别符
注册内容
#1
内容A
#2
内容B
#3
没有

图 14

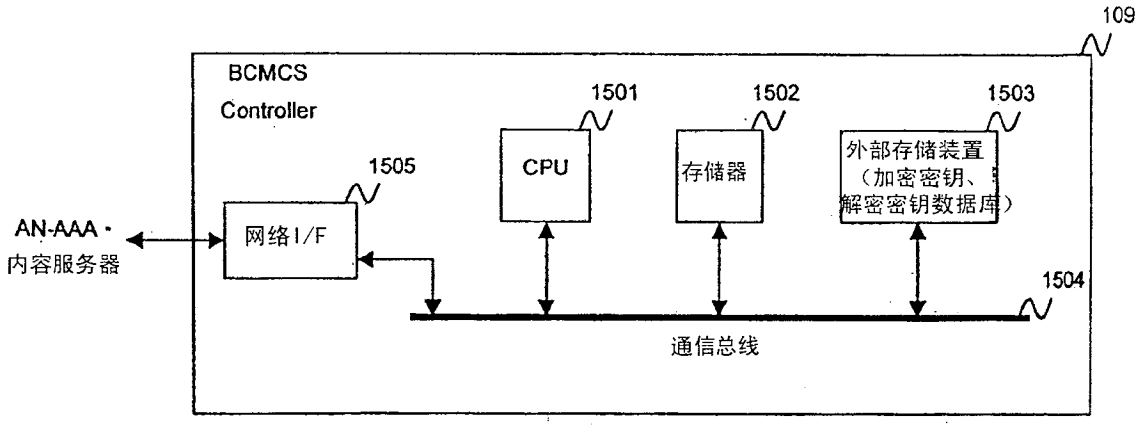
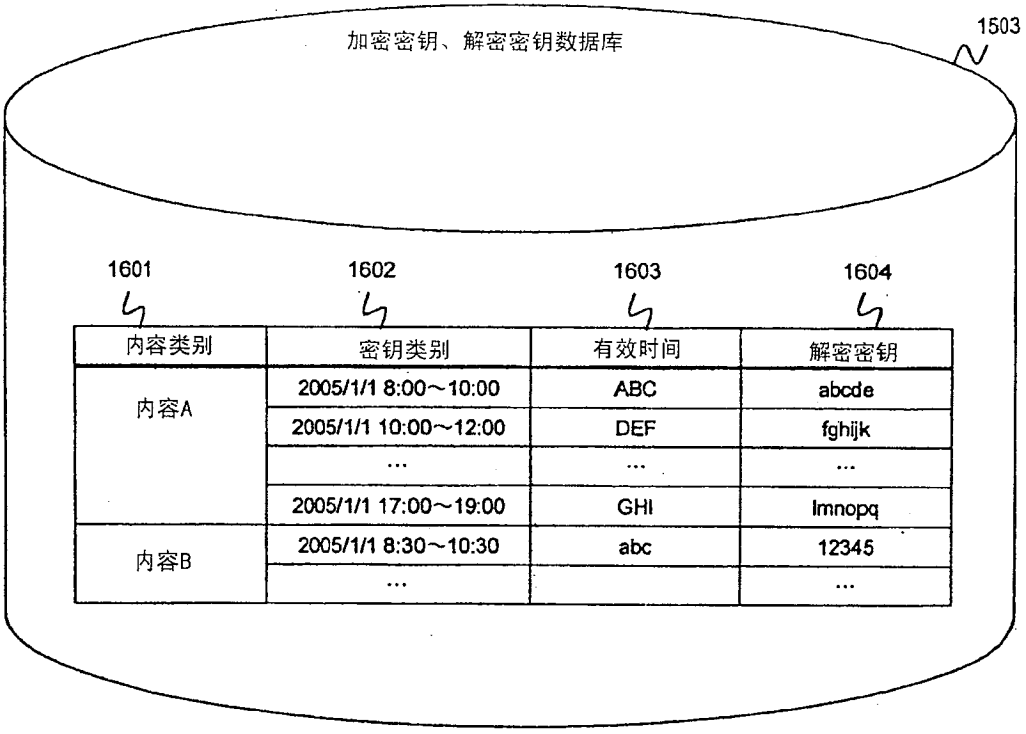

109
BCMCS
Controller
1501
1502
1503
CPU
存储器
外部存储装置
（加密密钥、
解密密钥数据库）
1505
AN-AAA·
内容服务器
网络I/F
1504
通信总线

图 15



内容类别	密钥类别	有效时间	解密密钥
内容A	2005/1/1 8:00～10:00	ABC	abcde
	2005/1/1 10:00～12:00	DEF	fghijk
	…	…	…
	2005/1/1 17:00～19:00	GHI	lmnopq
内容B	2005/1/1 8:30～10:30	abc	12345
	…		…

图 16

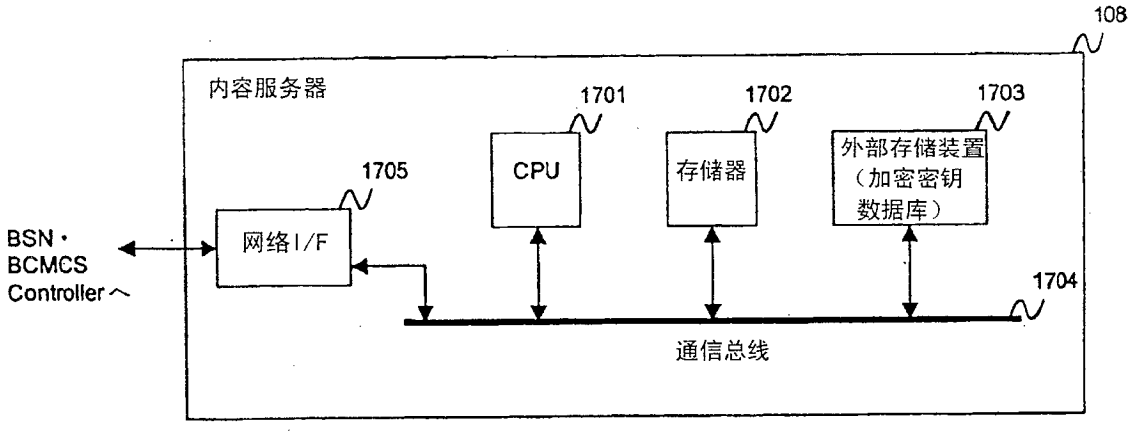


图 17

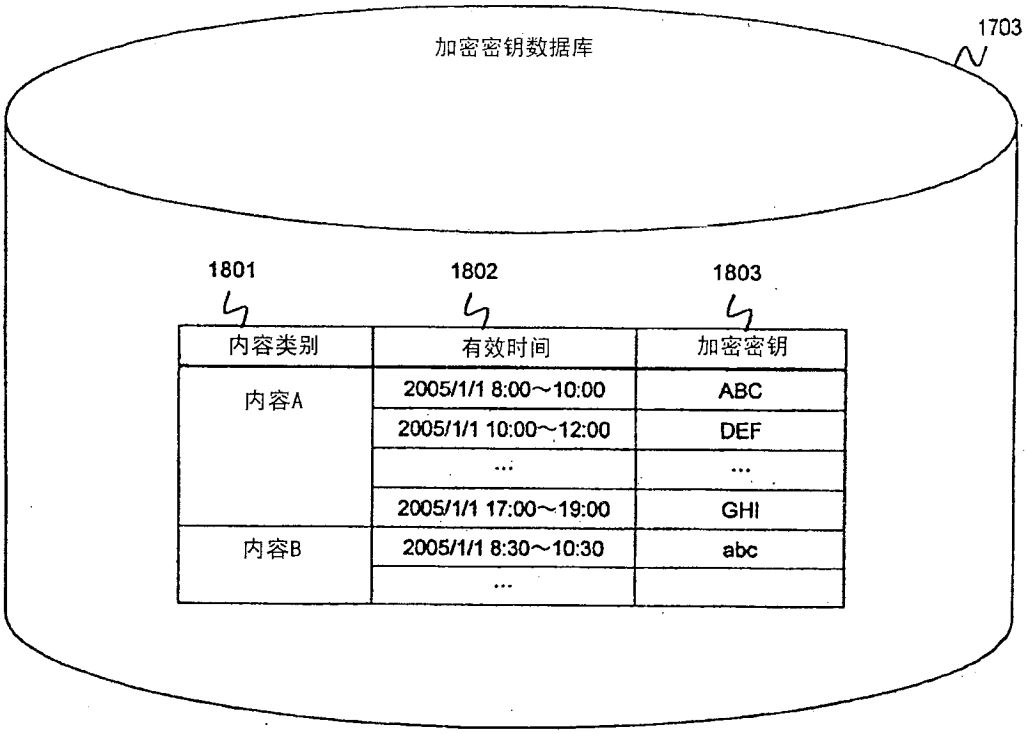

加密密钥数据库
1703
1801
1802
1803
内容类别
有效时间
加密密钥
内容A
2005/1/1 8:00～10:00
ABC
2005/1/1 10:00～12:00
DEF
...
...
2005/1/1 17:00～19:00
GHI
内容B
2005/1/1 8:30～10:30
abc
...

图 18

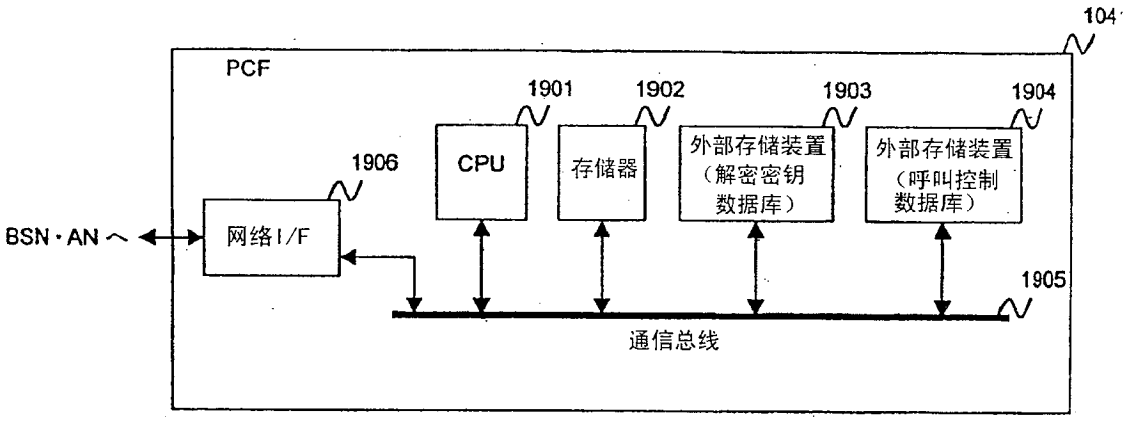
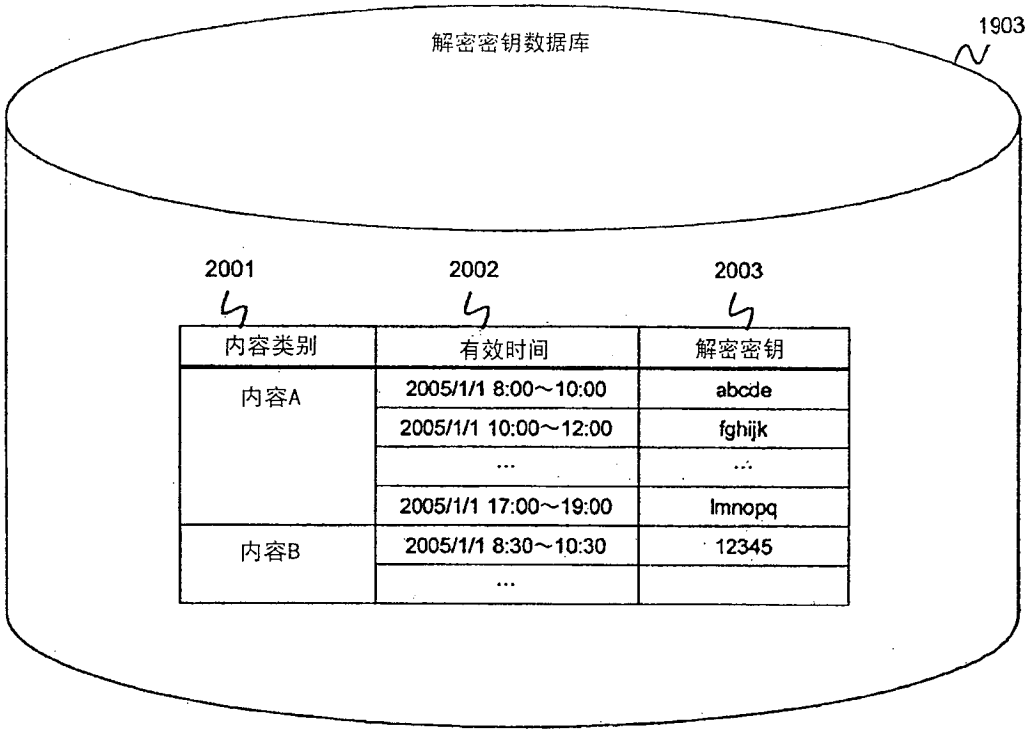
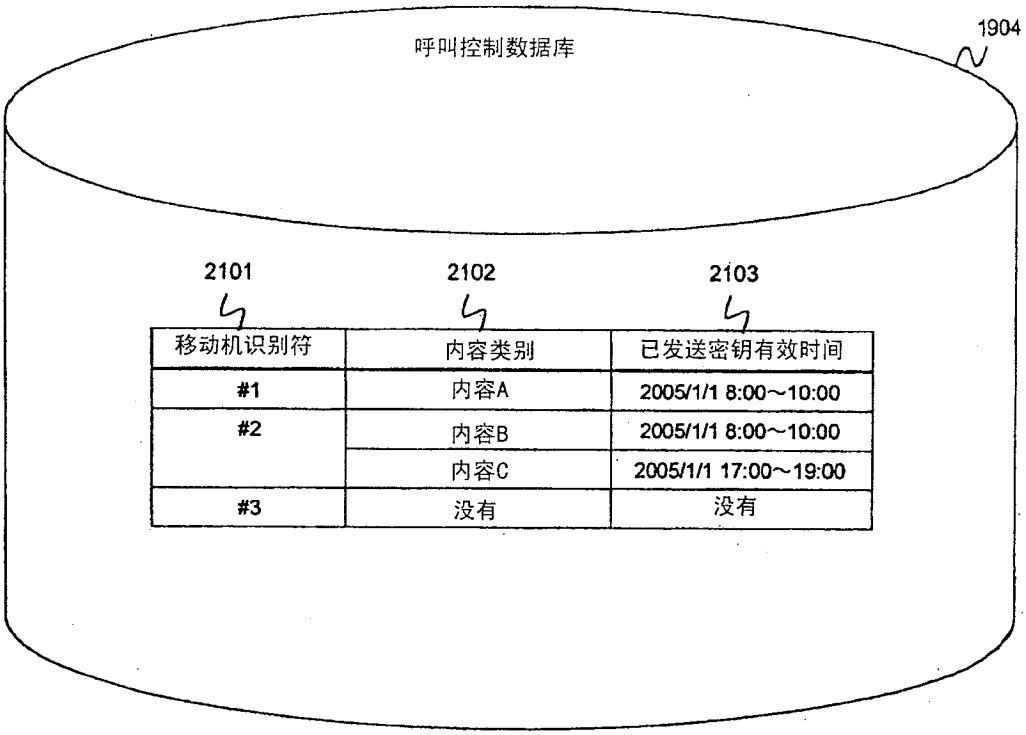

104
PCF
1901
1902
1903
1904
1906
CPU
存储器
外部存储装置
（解密密钥
数据库）
外部存储装置
（呼叫控制
数据库）
BSN·AN
网络I/F
1905
通信总线

图 19



内容类别	有效时间	解密密钥
内容A	2005/1/1 8:00～10:00	abcde
	2005/1/1 10:00～12:00	fghijk
	…	…
	2005/1/1 17:00～19:00	lmnopq
内容B	2005/1/1 8:30～10:30	12345
	…	

图 20



移动机识别符	内容类别	已发送密钥有效时间
#1	内容A	2005/1/1 8:00～10:00
#2	内容B	2005/1/1 8:00～10:00
	内容C	2005/1/1 17:00～19:00
#3	没有	没有

图 21

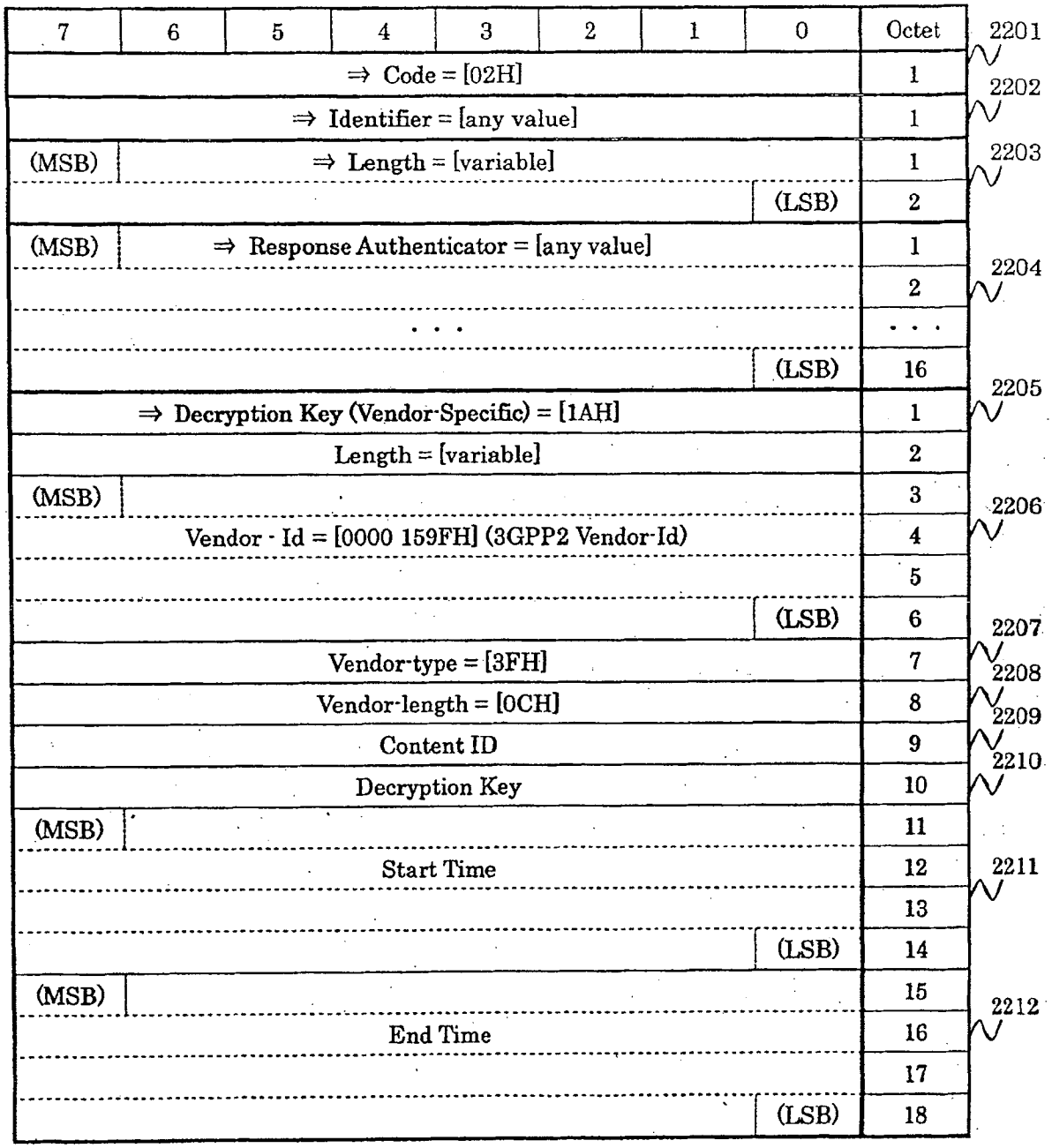

7 6 5 4 3 2 1 0 Octet
⇒ Code = [02H] 1
⇒ Identifier = [any value] 1
(MSB) ⇒ Length = [variable] 1
(LSB) 2
(MSB) ⇒ Response Authenticator = [any value] 1
2
. . . . . .
(LSB) 16
⇒ Decryption Key (Vendor-Specific) = [1AH] 1
Length = [variable] 2
(MSB) 3
Vendor - Id = [0000 159FH] (3GPP2 Vendor-Id) 4
5
(LSB) 6
Vendor-type = [3FH] 7
Vendor-length = [0CH] 8
Content ID 9
Decryption Key 10
(MSB) 11
Start Time 12
13
(LSB) 14
(MSB) 15
End Time 16
17
(LSB) 18
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212

图 22

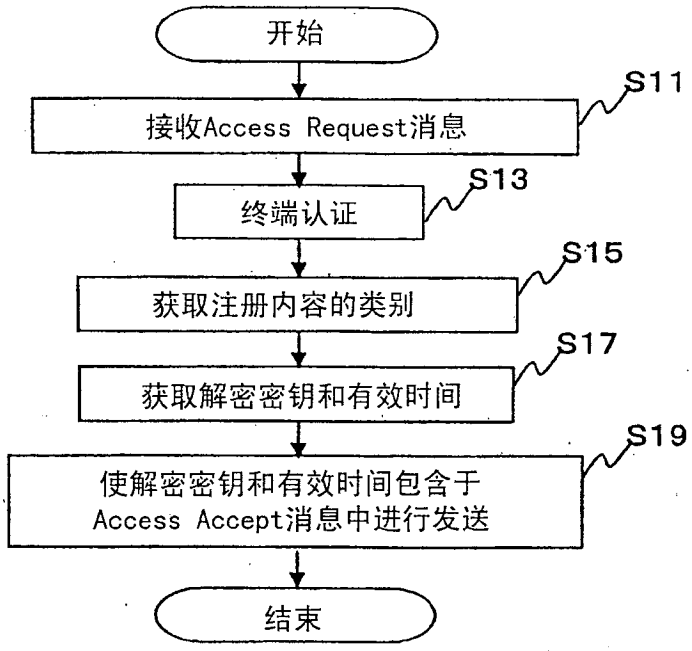

开始
S11
接收Access Request消息
S13
终端认证
S15
获取注册内容的类别
S17
获取解密密钥和有效时间
S19
使解密密钥和有效时间包含于
Access Accept消息中进行发送
结束

图 23

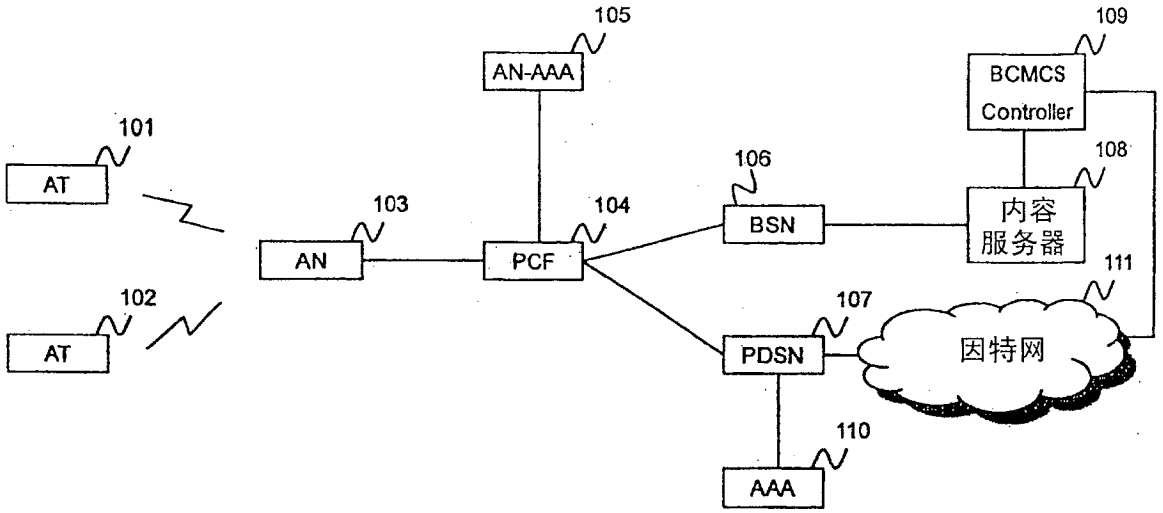

105
AN-AAA
109
BCMCS
Controller
101
AT
106
108
103
104
BSN
内容
服务器
AN
PCF
111
102
107
AT
PDSN
因特网
110
AAA

图 24