(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 1653743 B
(45)授权公告日 2010.08.11

(21)申请号 03810975.1

(22)申请日 2003.05.09

(30)优先权数据
20025024 2002.05.17 FI

(85)PCT申请进入国家阶段日
2004.11.15

(86)PCT申请的申请数据
PCT/FI2003/000360 2003.05.09

(87)PCT申请的公布数据
WO2003/098868 EN 2003.11.27

(73)专利权人 诺基亚有限公司
地址 芬兰埃斯波

(72)发明人 J·梅克莱 J·雅蒂宁

(74)专利代理机构 北京市金杜律师事务所 11256
代理人 冯谱

(51)Int.Cl.
H04L 9/08(2006.01)

(56)对比文件
WO 0//74005 A1,2001.10.04, 全文.
US 6363152 B1,2002.03.26, 全文.
US 5222137 A,1993.06.22, 全文.
EP 1107505 A2,2001.06.13, 全文.
EP 0774707 A1,1997.05.21, 全文.
US 5483598 A,1996.01.09, 全文.
WO 02/37403 A1,2002.05.10, 全文.
US 6021203 A,2000.02.01, 全文.
WO 01/95558 A1,2001.12.13, 全文.
WO 00/79457 A1,2000.12.28, 全文.
Jesse Walker.802.11 TGe Security Baseline Draft Text 4.IEEE,2001,1-47.
Niels Ferugson,MacFergus.Michael: an improved MIC for 802.11 WEP.IEEE,2002,1-27.

审查员 宋洁

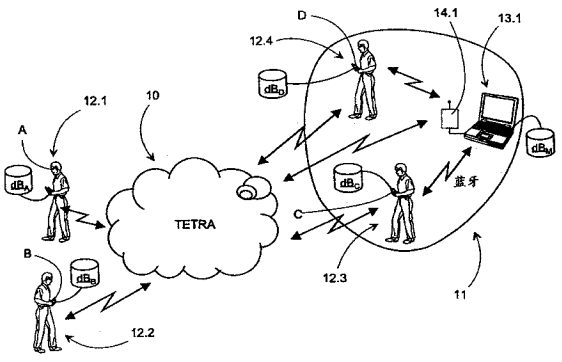
权利要求书 3 页 说明书 11 页 附图 10 页

(54)发明名称

用于安排数据加密的方法和系统及其对应的服务器

(57)摘要

本发明涉及一种数字无线数据通信网络中用于安排数据加密为一次一密乱码本加密的方法和系统。数据通信网络至少包括两个终端设备，终端设备用于管理索引加密密钥集，其中第一终端设备至少是发送机，而第二终端设备至少是接收机。数据加密适合在第一终端设备中分阶段进行，其中，选择加密密钥索引；利用所选择的加密密钥索引定义的加密密钥对待发送的数据进行加密；以及，把加密的数据发送到第二终端设备，其中相应地，在第二终端设备中，接收加密的数据，以及利用选择的、加密密钥索引指示的密钥对加密的数据进行解密。



CN 1653743 B

1. 一种用于在数据通信网络 (10,11) 中安排数据加密为一次一密乱码本加密的方法，其中，所述数据通信网络 (10,11) 包括至少两个终端设备，其中所述一次一密乱码本加密包括完整的一次一密乱码本加密和部分一次一密乱码本加密，所述至少两个终端设备用于管理所索引的加密密钥集，并且所述至少两个终端设备中的第一终端设备至少是发送机，所述至少两个终端设备中的第二终端设备至少是接收机，其中所述数据加密适合在第一终端设备中分阶段进行，其中，

- 选择加密密钥索引 (302-306,702)，

- 利用所选择的加密密钥索引定义的加密密钥对待发送的数据进行加密 (308,704)，以及

- 把加密的数据发送到第二终端设备 (309,705)，

其中相应地，第二终端设备用于

- 接收所述加密的数据 (401,706)，以及

- 利用选择的、所述加密密钥索引指示的加密密钥对所述加密的数据进行解密 (404,709)，

其中所述数据通信网络 (10,11) 还包括专用服务器终端设备 (13.1)，被安排成管理所索引的加密密钥集并将其分配到所述至少两个终端设备，其特征在于所述专用服务器终端设备 (13.1) 用于：

- 预先将所索引的加密密钥集分配到所述至少两个终端设备，允许在所述至少两个终端设备之间进行一对一或一对多的组通信，以及

- 根据建立的准则管理当前在所述至少两个终端设备中的所述加密密钥的可用性。

2. 如权利要求 1 所述的方法，其特征在于，除所索引的加密密钥之外，所索引的加密密钥附属的所述至少两个终端设备的标识符存储在所述专用服务器终端设备 (13.1) 中，其中在所述专用服务器终端设备 (13.1) 中更新所述至少两个终端设备时，

- 标识待更新的所述至少两个终端设备 (501,604,801.2)，

- 从所述至少两个终端设备接收至少一个使用的加密密钥索引 (501,803)，以及

- 根据建立的准则，发送命令给所述至少两个终端设备中一个或多个的终端设备，以删除对应的一个或多个加密密钥索引 (502,602)，

并且所述命令被用在所述至少两个终端设备中不能取消地删除选择的索引 (503.1,503.2,603)。

3. 如权利要求 2 所述的方法，其特征在于，关于所述至少两个终端设备中一个或多个终端设备，以下子阶段还与更新有关

- 接收并执行所述命令以删除所述一个或多个加密密钥索引 (503.1,503.2,603)，

- 向所述专用服务器终端设备 (13.1) 发送有关删除一个或多个加密密钥索引的确认 (504.1,504.2,604)。

4. 如权利要求 3 所述的方法，其特征在于，而且与更新有关，在专用服务器终端设备 (13.1) 中

- 接收 (505) 所述至少两个终端设备中至少一个终端设备的、删除一个或多个加密密钥索引的确认，并且该确认基于建立的第二准则，

- 最终删除 (507) 一个或多个加密密钥索引。

5. 如权利要求 1-4 中任何一项所述的方法，其特征在于，由所述第一终端设备选择所述加密密钥索引，在该选择之后，所述第一终端设备从所述专用服务器终端设备 (13.1) 中查询所选择的加密密钥索引的可用性，并且根据给出的信息，认可选择的加密密钥索引 (306) 或者选择新的加密密钥索引供检查 (302)。

6. 如权利要求 1-4 中任何一项所述的方法，其特征在于，由所述专用服务器终端设备 (13.1) 选择所述加密密钥索引，由此，在向第二终端设备发送时，所述第一终端设备从所述专用服务器终端设备 (13.1) 查询有效加密密钥索引。

7. 如权利要求 1-4 中任何一项所述的方法，其特征在于，所选择的加密密钥仅使用一次。

8. 如权利要求 7 所述的方法，其特征在于，作为一个子阶段，所述至少两个终端设备中的至少一个终端设备立即把有关使用所述加密密钥索引的信息发送到所述专用服务器终端设备 (13.1)。

9. 如权利要求 2-4 中任何一项所述的方法，其特征在于，对应于所述加密密钥索引的加密密钥至少使用两次，由此，所述至少两个终端设备用于保持每个使用的加密密钥索引的循环信息，而所述专用服务器终端设备 (13.1) 用于保持所述加密密钥索引的总循环信息。

10. 如权利要求 9 所述的方法，其特征在于，有关更新所述至少两个终端设备，所述专用服务器终端设备 (13.1) 在所述命令 (602) 之前还用于

- 从所述第一终端设备接收至少一个使用的加密密钥索引的循环信息 (803)，
- 将接收的循环信息合计为所述总循环信息 (803)，以及
- 将所述一个或多个加密密钥索引的总循环与所述建立的准则进行比较，据此得到判定来执行所述命令，以便删除所述加密密钥索引 (602)。

11. 如权利要求 1-4 中任何一项所述的方法，其特征在于，另外，当更新所述至少两个终端设备的加密密钥时，在所述专用服务器终端设备 (13.1) 中

- 将至少一个新的加密密钥索引添加到待更新的所述至少两个终端设备 (605)，
- 为一个或多个添加的加密密钥索引生成对应的加密密钥 (606)，
- 将一个或多个的加密密钥索引和对应的加密密钥发送到所述待更新的所述至少两个终端设备 (607)。

12. 如权利要求 11 所述的方法，其特征在于，在所述专用服务器终端设备 (13.1) 中，以下述方式生成所述加密密钥：在更新所述加密密钥之后，待更新的所述至少两个终端设备中的所述第一终端设备和第二终端设备与所述第一终端设备和第二终端设备之外的每个其它终端设备具有至少一个公共加密密钥。

13. 如权利要求 1-4 中任何一项所述的方法，其特征在于，对存储在所述至少两个终端设备中的加密密钥进行加密，由此在进行数据加密和 / 或对其进行解密之前对加密密钥的加密进行解密 (307’，403’)。

14. 如权利要求 1-4 中任何一项所述的方法，其特征在于，从专用服务器终端设备 (13.1) 到所述至少两个终端设备对所述加密密钥进行传输加密。

15. 如权利要求 1-4 中任何一项所述的方法，其特征在于，当所述第二终端设备的安全状态按照所述建立的准则破坏时，从使用中删除用在对应的第二终端设备中的那些加密密

钥。

16. 一种数字无线数据通信网络 (10,11) 中用于安排数据加密为一次一密乱码本加密的系统,其中所述数字无线数据通信网络 (10,11) 至少包括两个终端设备,所述终端设备包括 :

- 用于储存和管理所索引的加密密钥的装置,

- 用于按照加密密钥索引、通过选择的算法和加密密钥执行数据加密以及对加密进行解密的装置,

- 至少一个用于接收所索引的加密密钥的承载接口,

其中所述数字无线数据通信网络 (10,11) 还包括专用服务器终端设备 (13.1),所述专用服务器终端设备 (13.1) 按照建立的准则管理加密密钥并将其分配到所述至少两个终端设备,其特征在于所述专用服务器终端设备 (13.1) 用于预先将所索引的加密密钥集分配到所述至少两个终端设备,允许所述至少两个终端设备之间进行一对一或一对多的组通信,以及所述专用服务器终端设备 (13.1) 还用于根据建立的准则管理当前在所述至少两个终端设备中的所述加密密钥的可用性。

17. 如权利要求 16 所述的系统,其特征在于,将所索引的加密密钥分配到所述至少两个终端设备是通过无线局域网连接 (11) 进行的。

18. 如权利要求 16 或 17 所述的系统,其特征在于,将所索引的加密密钥分配到所述至少两个终端设备是通过本地数据通信连接进行的。

19. 一种数字无线数据通信网络 (10,11) 中用于安排数据加密为一次一密乱码本加密的设备 (13.1),其中在所述设备 (13.1) 中设置有所索引的加密密钥集,以及用于管理所索引的加密密钥并将其分配到至少两个终端设备的功能,其特征在于所述设备 (13.1) 用于预先将所索引的加密密钥集分配到所述至少两个终端设备,允许在所述至少两个终端设备之间进行一对一或一对多的组通信,以及其还用于根据建立的准则管理当前在所述至少两个终端设备中的所述加密密钥的可用性。

20. 如权利要求 19 所述的设备 (13.1),其特征在于,在所述设备 (13.1) 中,安排用于按照当前使用情况将待分配到所述至少两个终端设备的加密密钥的数目进行最佳化的功能。

用于安排数据加密的方法和系统及其对应的服务器

技术领域

[0001] 本发明涉及数字无线数据通信网络中用于安排数据加密为一次一密乱码本加密的方法，其中数据通信网络包括至少两个终端设备，终端设备用于控制索引加密密钥集，终端设备中第一终端设备至少是发送机，第二终端设备至少是接收机，数据加密适合在第一终端设备中分阶段 (in stages) 进行，其中

[0002] - 选择加密密钥索引，

[0003] - 通过用所选的加密密钥索引定义的加密密钥对待发送的数据进行加密，以及

[0004] - 把加密的数据发送到第二终端设备

[0005] 并且相应地在第二终端设备中

[0006] - 接收加密的数据，以及

[0007] - 通过用选择的、加密密钥索引指示的密钥对加密的数据进行解密。

[0008] 本发明还涉及对应的系统和服务器终端设备。

背景技术

[0009] 无线通信系统还缺乏一种使多个终端设备之间待进行的通信得到优质安全的加密构思的简单实施方式。今天采用的加密算法通常实施起来非常复杂。另外，诸如加密密钥的相关加密信息的分配很成问题并且具有风险。

[0010] 表示已知技术的加密协议有诸如 PGP 密码 (Pretty Good Privacy) 和 RSA 公共密钥加密 (Rivest-Shamir-Adelman public keyencryption)。可是，例如在无线通信环境使用中，其实现十分复杂并且费事。在其它环境下，其可用性亦有待提高。

[0011] 有关现有技术有专利公开 US6021203（微软公司）、WO0195558A1（松下）、US5222137（摩托罗拉公司）、和 US5483598(Digital 公司）。

[0012] 上述公开中，US5483598 给出了一种解决方案，基于一次一密乱码本加密的使用，并利用分配于发信者和收信者之间的固定秘密密钥，以及一次一密乱码本，可是，它是例如由加密的消息或是由加密密钥流产生的。实际上，系统在这方面是易受攻击的，因为通过足够长时间地分析加密的传输，有可能破解重复产生的加密密钥。

[0013] 从 WO01/74005(Hammersmith) 可以知道基于一次一密乱码本加密的解决方案，其中给出了向固定因特网中通信的几个终端设备分配密钥。这里，提供加密密钥主要是结合实际通信事件来进行。发信者从服务器下载加密密钥，并且服务器还提供密钥给消息的收信者。然后，发信者和收信者利用该下载的加密密钥彼此进行通信。这种一个密钥可用于基本上仅与一方通信的 1 对 1 分布结构在例如移动台环境中伴随着与加密密钥分配有关的缺点和制约。这就是为什么该公开中给出的加密方法仅适用于两方之间的通信中，或者至少在多方之间的通信中，在业务方面，例如由于持续的加密密钥查询，其实现非常费事。在用这种方式的处理中，成组通信的加密需要的加密密钥数目成指数增加。加密密钥的数目现主要依赖于用户组的大小。

发明内容

[0014] 本发明的目的是提供一种新的方法和系统，用于安排数据格式的业务中的加密，它基本上简化了所需的加密系统并提高了密钥管理的安全。按照本发明的方法的特征在权利要求 1 中给出，权利要求 16 给出了本发明的系统的特征，权利要求 19 给出了本发明的服务器的技术特征。

[0015] 按照本发明实施加密的方式具有与已知技术相比完全相反的方法，因为执行加密的算法能以其最有利的形式无限简化，由此得到的无限强大的加密模型实施还非常简单。上述方法和系统不涉及加密中要用的算法的实施，使之有可能有利地利用例如已经存在的加密算法。

[0016] 原理上，本发明给出的加密方法和系统完全不会被所有加密分析破解。它可以在例如已知的蜂窝网络、甚至在现有的终端设备中迅速和有利地实施，因为它易于结合到通信软件中。

[0017] 按照本发明的方法是基于一次一密乱码本加密机制，在终端设备之间提供通信，具有实际改进的安全级别和把加密中使用的信息分配到通信终端设备的安全方式。

[0018] 一次一密乱码本加密机制是唯一在理论上牢不可破的加密方法。用于加密算法中管理和分配加密密钥的新方式实际上改进了加密的安全级别，使之与目前用于无线通信中已知的方法相比较，在原理上完全牢不可破。按照本发明的系统包括至少一个终端设备用作服务器，和一个或一个以上在数据通信网络中彼此通信的终端设备。在几个终端设备之间的通信（1 对 N 通信）中，其中平滑分配加密密钥在实施运行及平滑一次一密乱码本加密模型中有瓶颈，按照本发明的方法显然具有特别的优点。被安排作为服务器的终端设备管理加密信息的使用、形成，并且还可能管理加密信息的分配。

[0019] 在系统中，通过数据通信网络从服务器终端设备为终端设备更新加密信息，加密信息被多个终端设备使用，以便对其业务进行加密。按照一个实施例，这样的加密信息例如可以包括加密密钥。

[0020] 按照第一有利的实施例，加密可能作为完整的一次一密乱码本加密来执行，在终端设备间的通信中已用过一次的加密密钥不二次使用。这样，对于加密，可以得到非常高的安全级别。

[0021] 按照另一个有利的实施例，加密还可以作为部分一次一密乱码本加密来执行。由此在多个终端设备间的通信中可以使用相同的加密密钥几次，而安全级别不会显著地降低。对于该实施例，例如在管理加密密钥的服务器终端设备对执行通信的终端设备暂时不可用的情况下，具有优点。另一个附加的优点是 :与加密信息有关的数据传输显著地减少，并且在终端设备中需要较少的储存容量储存加密信息。

[0022] 按照有利的实施例，加密信息的更新可以在无线局域网中完全自动进行，由此不需要终端设备的用户为此执行有关步骤。例如，对于出现在有限组 (limited group) 中的加密通信，上述实施例特别有利。由此，加密信息的更新可以由服务器终端设备来控制，该服务器终端设备按其自己的判断向终端设备发送加密信息。另一方面，终端设备还可以每次根据其更新需要自发地下载加密信息。

[0023] 传统上，加密密钥的分配是一次一密乱码本加密的唯一致命弱点。在按照本发明的方法中，当把加密密钥从服务器终端设备传送到终端设备时，还有可能对加密密钥的加

密使用甚至强大的加密。另一方面，如果安排密钥的分配，不用加密地传输密钥也是可能的，例如在无线局域网中，有可能控制对电信公司区域具有接入的用户。

[0024] 可应用本发明的无线数据通信网络的示例有基于 CDMA（码分多址）、TDMA（时分多址）和 FDMA（频分多址）技术的解决方案，以及基于这些的子规范及技术还在开发中。

[0025] 除了无线通信之外，按照本发明的方法和系统的应用的另一个有利目的是海量存储器，与其有关的巨大敏感信息被处理。

[0026] 按照本发明的方法、系统和服务器终端设备的特有特征出现在所附的权利要求书中，说明书部分给出了可以实现的更多优点。

附图说明

[0027] 按照本发明的方法、系统和服务器终端设备不限于本文给出的实施例，以下将参考附图进行更加详细地进行描述，其中，

[0028] 图 1 是按照本发明的系统的实施例的示例的示意图，

[0029] 图 2a 和 2b 示出数据结构的示例，

[0030] 图 3 是流程图，示出以完整的一次一密乱码本加密进行发送的终端设备中按照本发明的方法的第一实施例中的步骤的示例，

[0031] 图 4 是流程图，示出以完整的一次一密乱码本加密进行接收的终端设备中按照本发明的方法的第一实施例中的步骤的示例，

[0032] 图 5 是流程图，示出与更新加密信息有关的、图 3 和 4 中示出的实施例中的步骤的第一示例，

[0033] 图 6 是流程图，示出以完整的一次一密乱码本加密进行更新的、实施加密信息的另一方式，

[0034] 图 7 是流程图，示出部分一次一密乱码本加密进行发送和接收的终端设备中按照本发明的方法的另一实施例中的步骤的示例，

[0035] 图 8 是流程图，示出与更新加密信息有关的、部分一次一密乱码本加密中的另一示例，

[0036] 图 9a-d 示出在更新加密密钥中服务器数据库的示例，

[0037] 图 10a-c 示出终端设备失去其安全之后加密密钥管理的示例。

具体实施方式

[0038] 图 1 是按照本发明的系统的一个实施例的示例的示意图。按照本发明的系统和方法涉及按照一次一密乱码本加密模型在数字无线数据通信网络 10、11 中安排数据加密。数据通信网络 10、11 可以是有线网络，诸如 IP 网络（例如因特网、内部网、局域网），或者是无线的（例如 WLAN、CDMA、TDMA、FDMA，蓝牙）。

[0039] 数据通信网络 10、11，作为示例示出的情况中是无线的，包括至少两个彼此通信的终端设备 A-D，其中一个终端设备 A 至少用作发送机，而另一终端设备 B 至少用作接收机。终端设备 A、B 间的通信可以例如直接为数据格式，诸如 SMS 消息、或者电子邮件，或者间接为数据格式，诸如编码的语音。

[0040] 而且，数据通信网络 10、11 包括至少一个装备有连接装置 14.1 的专用服务器终端

设备 13.1。为此，数据库 dB_M 被安排用于储存加密信息，诸如索引加密密钥。而且，在服务器终端设备 13.1 中，除了所述索引加密密钥之外，附属的、终端设备 A-D 的 ID 标识符储存于其中。还可以有几个服务器终端设备，由此，例如可以通过某种已知方法（未示出），实现其数据库 dB_M 的同步。

[0041] 在所述服务器终端设备 13.1 中，还安排功能，诸如要在处理器环境下执行的程序或者对应的命令集，上述命令用于基于建立的准则管理那些索引加密密钥并将其分配到其它终端设备 A-D。本发明还这样涉及的服务器终端设备 13.1 例如可以是 PC 等，像在数据通信网络 10、11 中彼此通信的终端设备 A-D，只要是为其安排资源，用于管理、产生、和分配所述索引加密密钥。

[0042] 服务器终端设备 13.1 最好安排成易于监控其物理安全。定位服务器终端设备 13.1 的一种方式是良好保护的、最好锁定的位置（未示出），因为任何数据插入其中会引起加密模型损失。上述位置例如是在进行通信的公司、组织、用户组等的场所，其中通信组的成员有利地进行使用以定期进行访问。咖啡室或者商谈室等是一个示例。

[0043] 终端设备 A-D 还包括用于储存和管理索引加密密钥集的装置、用于进行数据加密和用于通过选择的算法以及按照加密密钥索引通过加密密钥对加密进行解密的装置、以及用于从数据通信网络 11 接收索引加密密钥的至少一个电信公司接口 (carrier interface)。对于索引加密密钥，数据库 dB_A、dB_B、dB_C、dB_D 被安排在终端设备 A-D 的存储器区域。通过程序执行的命令，在终端设备 A-D 的处理器环境中进行加密密钥的管理。按照本发明的方法对加密中使用的算法不设限制，但最好是基于随机加密密钥的。这样，加密算法甚至可以完全公开，诸如 XOR 加。

[0044] 按照一个有利的实施例，通过无线局域网连接 11，诸如 WLAN（无线局域网）或蓝牙，或者通过其它某种本地数据传输信道 (IrDA，RS-232)，灵活分配索引加密密钥给终端设备 C、D。通过利用例如蓝牙技术，可以自动更新密钥，因此它总是在用户 12.3、12.4 与其终端设备 C、D 对“更新节点”11 的访问进行支付时进行。

[0045] 如果有可能保证外界没有访问数据通信网络 11（例如蓝牙），则可以不用加密进行加密密钥的分配。而且，如果通过 IR 端口或者封闭空间中的数据电缆进行加密密钥的分配，则没有必要对密钥进行加密。

[0046] 在将加密密钥从服务器终端设备 13.1 传送到终端设备 A-D 时，还可以对加密密钥进行加密。在加密中使用的算法，例如根据物理条件可以相当自由地进行选择。

[0047] 作为在加密密钥的传输中执行加密的一种方式，可以提及一次一密乱码本加密的使用，由此在某种意义上使用加密方法两次。因此，以选择的算法进行密钥的加密，其中使用加密密钥的另一列表，特用于密钥的传送。该列表的密钥可以仅通过数据电缆在终端设备 A-D 中从服务器终端设备 13.1 再次下载。

[0048] 图 2a 示出一个说明示例，即储存在服务器终端设备 13.1 的索引加密密钥 S_N 的运行集。要作为整数出现的索引 N 位于记录的第一字段，而对应于索引 N 的加密密钥 S_N 位于第二字段并且是例如 16 进制的形式。

[0049] 图 2b 示出位于服务器终端设备 13.1 中的管理数据库 dB_M 的示例。对应于一个终端设备 A-D 的记录由终端设备 A-D 的 ID 字段（例如，用户标识符和 / 或终端设备 IMEI（国际移动设备身份））码、在终端设备 A-D 中最近下载的（有效）加密密钥 S_N 的索引 N、和位

于终端设备 A-D 中的备份加密密钥的索引 BACKUP_N 形成。ID 字段必需明确标识终端设备 A-D 和其用户 12.1、12.2、12.4、和 12.5。对于每一个终端设备 A-D，仅能储存预定数量的这些有效加密密钥 S_N（例如 40 个）。

[0050] 下面将描述按照本发明的方法的不同实施例，其中在原理上至少有两种不同类型。其中，根据系统中的参与者，在相同的终端设备 A-D 组中一次只能使用一个。

[0051] 图 3 是流程图，示出按照本发明的方法的第一实施例的示例，具有发送终端设备 A。该实施例作为一个完整的一次一密乱码本加密实施，其中选择的索引加密密钥 S_N 仅用一次，使用过的加密密钥 S_N 从系统的每一个终端设备 A-D 中删除。通过该方法的实施，得到非常高的加密安全级别。可是，实施方法需要足够储存容量的终端设备 A-D，因为要储存在它们中的加密密钥的列表可能由此变得非常长。

[0052] 终端设备 A 的用户 12.1 以某种方式产生消息 M，它将被发送并且可能是例如 SMS 或者电子邮件消息（步骤 301）。当产生了消息 M 并且在建立的方式中的用户 12.1 把他希望进行以一次一密乱码本加密明确加密的传输通知终端设备 A 时，终端设备 A 将按照一个实施例从安排在其存储器中的索引加密密钥数据库 dB_A 中选择加密密钥索引 N（步骤 302）。

[0053] 按照一个有利的实施例，在选择加密密压索引 N 之后，终端设备 A 通过数据通信网络 10 在服务器终端设备 13.1 中检查选择的索引 N 的可用性，例如 SMS 消息（步骤 303）。该实施例还可以不用任何检查过程而实施（步骤 303-306），因为在这种情况下，加密密钥 S_N 仅用一次。而且，在按照本发明的方法中，如果对于所有终端设备 A-D，加密密钥 S_N 的更新基本上是同时进行的，则检查过程（步骤 303-306）甚至是不必要的。可是，如果其它一些终端设备 B-D 恰好与终端设备 A 同时发送以相同的加密密钥 S_N 加密的消息，而服务器终端设备 13.1 还没有时间进行有关加密密钥 S_N 的更新并且向终端设备 A-D 发送有关删除命令（下文出现），则该检查过程（步骤 303-306）在所描述的实施例中是有利的预防措施。

[0054] 服务器终端设备 13.1 检查其自己的主数据库 dB_M 中索引 N 的可用性（步骤 304）并向查询终端设备 A 发送答复（步骤 305）。终端设备 A 接收信息并据此或者接受其选择的加密密钥索引 N 或者从其数据库 dB_A 选择新索引 N，用于以相同的方式进行检查（步骤 306）。

[0055] 按照另一个更有利的实施例，选择加密密钥索引 N 的过程（步骤 302-305）可以用如下的方式进行：发送终端设备 A 的用户 12.1 以某种方式指示消息 M 的收信者 B（步骤 302），然后，其中信息被转送到服务器终端设备 13.1（步骤 303）。应当指出，消息还可以有几个收信者 B-D。服务器终端设备 13.1 从其数据库 dB_M 选择适合于发送机 A 并适合于收信者 B 的加密密钥 S_N 相对应的索引 N（步骤 304），并将与此有关的信息发送到发送终端设备 A（步骤 305）。至于要在终端设备 A 中直接进行索引选择，上述间接实施例更加有利，因为业务量因此明显更小（未示出）。

[0056] 当发现可用索引 N 时，终端设备 A 利用与刚刚用于生成加密比特流选择的索引 N 相对应的加密密钥 S_N 进行消息 M 的加密（步骤 308）。如果加密密钥被加密存储在数据库 dB_A，其加密被解密（步骤 307'）。要发送的消息 M 的加密可以通过能由终端设备 A 的处理器装置运行的已知的加密算法来执行。

[0057] 加密之后，加密的消息 RM 和加密中使用的加密密钥 S_N 的索引 N 通过数据通信网

络 10 发送到消息的一个或一个以上收信者 B 的终端设备 12.2(步骤 309)。

[0058] 图 4 是流程图,示出按照本发明的方法的第一实施例的示例,具有接收终端设备 B。图 3 中所示的流程图在图 4 中继续。终端设备 B 以已知方式接收消息 RM 和索引 N(步骤 401)。终端设备 B 从其自己的索引密钥数据库 dB_B 中获取与索引 N 相对应的加密密钥 S_N(步骤 402)并利用相应种类的加密方法通过获取的加密密钥 S_N 对加密的消息进行解密(步骤 404)。如果加密密钥被加密,则在使用之前进行其解密(步骤 403')。如果消息 M 是示例中使用的 SMS 消息,则例如在显示器上将消息 M 示于终端设备 B 的用户 12.2(步骤 405)。

[0059] 在终端设备 A 例如已经将消息 M 发送到终端设备 B(步骤 309)和/或在终端设备 B 已经对消息 M 的加密进行解密(步骤 404)之后,按照该实施例的方法中的步骤将在与索引 N 对应的加密密钥 S_N 的使用中发送信息给服务器终端设备 13.1(步骤 310、406)。

[0060] 图 5 是流程图,示出结合图 3 和 4 中示出的实施例的、有关更新加密信息采用的措施的示例。服务器终端设备 13.1 标识发送所使用的索引 N 的终端设备 A、B,接收所使用的加密密钥索引 N,并将其登记为已使用(步骤 501)。然后,服务器终端设备 13.1 在其主要数据库 dB_M 中为有关的索引 N 在所有终端设备 A-D 上设置删除线标志。命令被发送到所有终端设备 A-D 以从其索引密钥数据库 dB_A、dB_B、dB_C、dB_D 删除对应的加密密钥索引 N(步骤 502)。

[0061] 终端设备 A-D 接收删除索引 N 的命令并执行从数据库 dB_A、dB_B、dB_C、dB_D 不可撤回地删除索引 N 和对应的加密密钥 S_N 的步骤(步骤 503.1-503.3)。终端设备 A-D 还向服务器终端设备 13.1 发送删除索引 N(步骤 503.1-503.3)的确认,服务器终端设备 13.1 对确认进行登记。当接收删除命令的所有终端设备 A-D 确认了删除时,服务器终端设备 13.1 最终还从其自己的主数据库 dB_M 删除与索引 N 对应的加密密钥 S_N(步骤 507)。

[0062] 上述实施例要求向每一个终端设备 A-D 发送删除命令(步骤 502),结果,在删除之后,要将确认从终端设备 A-D 发送到服务器 13.1(步骤 504.1-504.3)。这甚至可能导致繁重的业务。如果一个或一个以上终端设备 A-D 对数据通信网络 10、11 无效,则加密密钥列表 dB_A、dB_B、dB_C、dB_D 的同步在此情况下还可能变得成问题。大体上,如果服务器终端设备 13.1 不在使用,则其它通信的终端设备 A-D 至少在用完有效加密密钥之后也不在使用中。

[0063] 图 6 是流程图,示出执行加密信息更新的另一种实施方式。在此情况下,图 3、4、5 所示的发送-接收过程以利用索引 N(步骤 310、406)时向服务器终端设备 13.1 传输信息并以其在服务器终端设备 13.1 中登记(步骤 501)而结束。在该实施例中,图 3 所示选择步骤或检查索引 N 可用性的步骤(步骤 302-306)具有根本的重要性。

[0064] 在该实施例中,用于完整的一次一密乱码本加密中的索引加密密钥 S_N 的更新按照建立的准则或者在终端设备 A-D 的请求下或者由服务器终端设备 13.1 以自动方式执行。这最好通过无线局域网连接 11 来完成,例如,在用户 12.1、12.2、12.3、12.4 携带其终端设备 A-D 到达商业组织的处所或者其它一些受控区域时。

[0065] 终端设备 C 打开与服务器终端设备 13.1 的数据通信连接,反之亦然(步骤 601.1、601.2)。服务器终端设备 13.1 向终端设备 C 发送删除命令涉及的、使用的加密密钥索引 N 的列表(步骤 602)。

[0066] 终端设备 C 接收删除命令涉及的加密密钥列表,并按照接收的数据更新其自己的

数据库 dB_C（步骤 603）。关于更新，重要的是使用的加密密钥 S_N 从终端设备 C 的数据库 dB_C 中永久删除。如果这正巧在建立连接（步骤 601.1、601.2）的时候还没有完成，终端设备 C 将通知其自己的身份符号 ID（步骤 604），并在同时确认在其自己的数据库 dB_C 中已经做出的删除。服务器终端设备 13.1 通过其被安排的软件在其主要数据库 dB_M 中生成索引加密密钥 S_N，这基于已经接收到其记录中、对应于终端设备 C 的身份信息 ID，在终端设备 C 的数据库 dB_C 中存在同样多的空间用于有效索引加密密钥 S_N（步骤 605、606），或者基于其它某种有利的准则。

[0067] 形成这样的一个准则的一个示例是，服务器终端设备 13.1 估计终端设备 A-D 使用的加密密钥的数目，并基于该信息将加密密钥按照其加密密钥的消耗分配到每一个终端设备 A-D。为此，不同的终端设备 A-D 在其存储器中可以有不同数目的加密密钥。因此，服务器终端设备 13.1 可以例如按照用户组的大小及使用频率对加密密钥的数目进行最佳化。由此，例如如果存在许多终端设备，但是加密的通信在它们之间很少发生，则一次仅分配少数加密密钥给各个终端设备就足够了。

[0068] 在某些过程阶段中，服务器终端设备 13.1 检查其数据库 dB_M，以查找关于终端设备 C 的更新是否出现被设置用于删除的这种加密密钥，并且关于其删除，‘确认’是否已经从所有终端设备 A-D 到达。如果查找到，在服务器终端设备 13.1 中执行上述加密密钥的不可撤销删除（未示出）。

[0069] 在产生索引 N、对应的加密密钥 S_N 及储存在数据库 dB_M 之后，服务器终端设备 13.1 将索引加密密钥 S_N 发送到终端设备 C（步骤 607），终端设备 C 相应地进行接收（步骤 608）。终端设备 C 把接收到的索引加密密钥 S_N 储存在其自己的数据库 dB_C 中（1°，步骤 609）。最好在一个更新时间尽可能多地将加密密钥下载在终端设备 C 的存储器资源中。这用于进行以下补偿：虽然终端设备 A-D 很少下载加密密钥 S_N，然而它还会有足够的加密密钥 S_N 用于通信。另一方面，服务器终端设备 13.1 还可以按照建立的准则对要在终端设备 C 下载的加密密钥的数目进行最佳化。

[0070] 按照一个有利的实施例，终端设备 C 还可以例如利用用户 12.3 设置的码、或者利用无需用户 12.3 采取任何步骤从 SIM（用户身份模块）卡得到的 PIN（个人身份号）标识符，对已经接收的加密密钥 S_N 进行加密（2°，步骤 608’）。相应地，在进行数据加密和 / 或数据加密的解密之前，必需对加密密钥的加密进行解密。通过关闭从终端设备 C 到服务器终端设备 13.1 的连接，反之亦然，完成更新过程（步骤 610.1、610.2）。

[0071] 在阶段之后（步骤 610.1），终端设备 C 可以发送要删除的加密密钥索引 N 的列表给建立的终端设备 D，该终端设备 D 更新其自己的数据库 dB_D。相应地，如果终端设备 D 访问服务器 13.1 以获取加密密钥索引的更新的列表，它将其转播到终端设备 C。这样，有可能进一步降低所需更新通信的数量（未示出）。

[0072] 在该实施例中，与加密密钥 S_N 的使用和更新有关的数据通信可以保持在适中水平。在服务器终端设备 13.1 中，可以设置删除线标志，并仅在服务器终端设备 13.1 中储存使用加密密钥 S_N 的信息。仅在终端设备 A-D 开始加密密钥的更新交付时，发送待删除的加密密钥 S_N 的索引列表。

[0073] 对于两个终端设备 A、B 彼此进行通信的实施例，即使在它们不能与服务器终端设备 13.1 建立连接的情况下，也可以得到这样的优点。可是，系统的安全由此变得更差，因为

加密密钥可能已经被使用。实际上，利用这样的模式的有利情况特别是紧急情况，诸如加密基础结构已经被毁掉的情况下。

[0074] 图 7 是流程图，示出按照本发明的方法的另一个实施例的示例，具有发送和接收终端设备 A、B。在该实施例中，作为部分一次一密乱码本加密来进行加密，其中相同的密钥 S_N 可以使用至少两次。除了上面出现的消息的加密，这种重复使用的示例是通过采用对称算法的语音呼叫的加密。

[0075] 在部分一次一密乱码本加密中，相同的加密密钥 S_N 可以使用几次。用户 12.1 使用终端设备 A 产生例如 SMS 消息（步骤 701）。并且，终端设备 A 从其数据库 dB_A 中选择索引 N（步骤 702）。在该连接中，如果必要或可能的话，还可以进行图 3 所示的检查或者索引的选择过程（步骤 302-306）。现在，每一个终端设备 A-D 为了避免同步或服务器终端设备 13.1 的停机时间引起的问题，保持加密密钥 S_N 的循环信息 TUSE_N，它们已经没有向服务器终端设备 13.1 作任何确认而使用。由此，还可以在服务器终端设备 13.1 中保持加密密钥的总循环 USE_N 的信息。

[0076] 在终端设备 A 选择索引 N 时，各终端设备的循环变量 TUSE_N 增加（步骤 703）。消息 M 的加密、向终端设备 B 的传输、以及接收都以上述的方式发生（步骤 704-706）。终端设备 B 还可以用于增加对应的循环变量 TUSE_N（步骤 708）。剩余的阶段，诸如消息 M 的解密（步骤 708-709）及其向用户 12.2 的表示（步骤 710）可以以上面描述的完整的一次一密乱码本实施例的对应方式进行。

[0077] 关于部分一次一密乱码本加密实施例，得到以下优点：终端设备 A-D 的数据库 dB_A、dB_B、dB_C、dB_D 的同步没有问题，并且对终端设备 A-D 中数据库的存储器容量的需要较完整的一次一密乱码本加密中的要小。

[0078] 图 8 是流程图，示出用于图 7 所示部分一次一密乱码本加密的加密信息的更新的示例。

[0079] 当从待更新的终端设备 D 到服务器终端设备 13.1 的连接可能时，以已知的方式在两个方向进行设置（步骤 801.1、801.2）。终端设备 D 以建立的准则向服务器终端设备 13.1 发送一个或一个以上其索引 TSUE_N 的值（步骤 802）并将其设置在零（步骤 804）。所述准则例如可以是 TUSE_N>0。

[0080] 在服务器终端设备 13.1 中，对应的一个或一个以上索引 N 的循环 USE_N 的总数以接收的 TUSE_N 值增加（步骤 803）。如果 USE_N 超过为其建立的限定值 MAX（步骤 805），则为索引 N 设置删除标志，以便将其从加密密钥的列表中删除（步骤 806）。于是即使在最大循环条件未满足的情况下，也可能例如以图 6 中所示的方式从阶段（步骤 602）开始。

[0081] 关于该实施例，得到以下优点：在使用每一个加密密钥 S_N 之后，不必更新所有终端设备 A-D。虽然相同的加密密钥 S_N 可以由此使用几次，然而加密方法的安全级别不会显著地受到损害，因为可以为加密密钥 S_N 的重复数建立限定值，诸如 TUSE_N<4。可是，通过统计方法，加密密钥 S_N 的重复可以使得各密钥 S_N 的部分解密成为可能（例如，通过研究消息间的差异），但是，即使在最坏的情况下，也可能仅对 TUSE_N 消息进行解密。因此，在整体上，一个加密密钥 S_N 的解密不会损害系统的安全。如果必要，例如可为每一个第三密钥 S_N 建立 TUSE_N = 1，由此，最敏感的消息可以利用这些密钥来发送，并且，以这种方式确保在这些情况下不会出现密钥 S_N 的重复。

[0082] 下面，服务器终端设备 13.1 的加密密钥的管理将作为可能的实施例进行解释。通过在服务器终端设备 13.1 中安排的软件，目标是在加密密钥 S_N 生成的每一个循环中，产生最大数目的有效加密密钥 S_N，将其分配到终端设备 A-D。除此之外，在服务器终端设备 13.1 中，剩余加密密钥的所有置换作为 BACKUP（备份）密钥保持在数据库 dB_M 中。这些最好能作为 Hash 数据结构安排。由此，至少一个加密密钥总是存在，用于所有终端设备之间的通信，并且几个加密密钥对存在，用于一些终端设备对。还可能存储一个以上版本的各个置换，但是 BACKUP 列表的尺寸将增大。

[0083] 图 9a 示出一种情况，作为有效加密密钥列表 S_N 和 BACKUP 列表，其列表储存在服务器终端设备 13.1 中，并形成数据库 dB_M 的一部分。应当指出，示例不涉及实际加密密钥 S_N，但涉及与其对应的索引 N。每一行对应于一个终端设备 A-D。BACKUP 密钥 BACKUP_N 在这种情况下在列表的前端，并且其后跟有有效密钥 S_N。应当指出，也可以按相反的方式设置，因为列表大体上作为连续列表 (running list) 安排。由此，当列表“满”时，有效列表的生成将从其起点再次开始。在上述情况下，终端设备 A 的 BACKUP 密钥的索引为 BACKUP_N ＝ {7,9,10,11,12,14,16,19,22,28,29,32,33,34,35}，而实际有效密钥的索引为 N ＝ {36,37,38,39,40,41,42}。

[0084] 图 9b 示出当终端设备 B 在更新中与服务器终端设备 13.1 连接时的一个示例。每次当服务器终端设备 13.1 与终端设备 B 连接时，生成新的加密密钥 S_N。在该示例中，有效加密密钥的数目限制到 10。在这种情况下，服务器终端设备 13.1 为终端设备 B 生成一个新的加密密钥 S_N，N ＝ 64。一般地说，在最大数目的有效密钥 S_N 之内，生成尽可能多的密钥 S_N 是可能并且有利的。为了保持有效加密密钥 S_N 的数目在建立的限制之内（≤ 10），必须破坏这些密钥的其中之一。在这种情况下，待破坏的密钥是最早的一个有效密钥，即密钥 36，它现在是用于终端设备 A、C、D 的有效密钥 S_N。

[0085] 图 9c 示出了接着的阶段，最好对 BACKUP 列表搜索最早的 BACKUP 密钥，作为终端设备 A、C、D 的公共密钥。没有什么阻止对满足上述准则的其他密钥进行选择，但是该最早的密钥是最好的，因为加密密钥的列表由此能安排为循环和连续列表，减小终端设备 A-D 对存储密钥用的存储器容量的需要。

[0086] 对于选择的密钥，N ＝ 12，在服务器 13.1 中设置删除线标志，并且针对它的删除命令还被发送到所有终端设备 A、C、D。可是应该指出，关于删除的执行，终端设备 A、C、D 没有确定性，直到有关终端设备 A、C、D 再次由服务器终端设备 13.1 更新。可是，该密钥 12 不应再用于终端设备 A、C、D 的通信的加密。

[0087] 图 9d 示出一种情况，其中终端设备 A 现在与服务器 13.1 连接，用于更新其密钥列表。对于终端设备，新密钥 N ＝ 46 被下载，同时，确保密钥 N ＝ 12 成功删除。可以传输有效密钥的列表，以便以密钥 37 开始，由此相应地改变 BACKUP 列表。为终端设备 A 的加密密钥检查 BACKUP 列表，并搜索加密密钥的复制品出现。发现 7、34、35 是终端设备对 AD 的公共 BACKUP 密钥。由此为密钥 7 设置删除线标志是最有利的，以将其从终端设备 A 中删除，并在存储装置中留下密钥 34 和 35.

[0088] 按照本发明的加密协议由于以下事实而唯一：一次一密乱码本加密的能力不会失去，虽然一个或一个以上终端设备消失、被偷、或者以其他某种方式破坏其安全状态。这通过利用上述 BACKUP 密钥而成为可能。虽然加密密钥的列表在这样的情况下必须尽可能快

地被更新，然而还有可能的是其他终端设备可以继续其安全数据通信至少一些时间。

[0089] 当一些终端设备的安全级别基本上受到破坏时，例如，由于终端设备 B 被偷，由已经失去其安全的终端设备 B 使用中的加密密钥可以在服务器终端设备 13.1 中被设置，用于从其他终端设备 A、C、D 的使用中删除。终端设备 A、C、D 中存储的、已经从失去安全的终端设备 B 中确切删除的那些 BACKUP 密钥（图 2b）投入使用一段时间，直到新的有效加密密钥 S_N 被生成，并为终端设备 A、C、D 更新。

[0090] 图 10a-10c 示出这一情况的示例，其中一个终端设备 A-D 失去其数据安全，因为例如它被偷或者丢失。图 10a 示出初始状态。如果终端设备 B 失去其安全状态，则储存在其中的有效密钥和 BACKUP 密钥必需由其它终端设备 A、C、D 直接删除使用（图 10b）。

[0091] 从图 10c 看到，终端设备 A、C、D 还可以至少某种程度地继续其安全通信。所有终端设备 A、C、D 共用的 BACKUP 密钥是 12、29 和 32。终端设备 A 和 C 共用的密钥是 7、34 和 35，而终端设备 C 和 D 共用的密钥是 8。现在已经没有有效列表，并且实际上必需尽可能快地产生有效列表。

[0092] 可是，实际上总是有少量的 BACKUP 密钥存在。虽然某些终端设备 A-D 即使在完全正常的通信中用完了有效加密密钥 S_N，那也是可能的。一个解决方案可以允许在终端设备 A-D 之间的通信中使用 BACKUP 密钥对。

[0093] 要在终端设备 A-D 中为加密密钥 S_N 保留的存储器空间的大小依赖于终端设备 A-D 提供的存储器容量和几个因素，诸如系统使用的频繁程度、终端设备 A-D 平均用于更新的频繁程度，因此它可能变化很大。

[0094] 本发明特别具有以下优点：一个或者一个以上终端设备 A-D 消失、被偷或者其它安全损坏不会导致用户 12.1、12.2、12.3、12.4 的数据安全的最终损失（会发生在设有专用 PGP 密钥的终端设备消失的情况下），因为能以简单方式产生新的加密密钥。为此，按照本发明的加密模型适合易于丢失或者被偷的移动终端设备。

[0095] 按照一个更有利的实施例，终端设备 A-D 的加密密钥 S_N 的更新可以用以下方式来完成：不必把由服务器终端设备 13.1 产生的所有加密密钥 S_N 给它们。由此，可以不用基于建立的准则分配一个或者一个以上的加密密钥 S_N。一个这样的准则可以是：在 30 可除尽的每个加密密钥索引 N 之后，如此多的加密密钥保留用于成对的终端设备 AB、AC、AD、BC、BD、CD，因为它们可以成对。由此，对应于各索引 N 的加密密钥 S_N 仅分配到一个终端设备对。

[0096] 还有一个可能的、并且能容易地从前者推导出的实施例，其中对于终端设备 A-D 不必有任何完全公共的加密密钥，但是上面提出的种类的过程例如以某种周期方式被执行。对于 BACK_UP 密钥，也仅应用成对的类似密钥实施，它们有其自己分开的表。

[0097] 而且，加密密钥 S_N 的需要不必是成对的，但是所述方法还能以下述方式执行，除一个外，所有终端设备得到某一加密密钥。由此，在终端设备 N 的情况下，加密密钥例如可以在 3 个、4 个、5 个、…、N-1 个中共享。

[0098] 通过预先将加密密钥 S_N 分成部分组，其中只有某些加密密钥 S_N 分配到一些终端设备 A-D 中，得到以下优点，其中，当终端设备 A 的安全级别基本上变得更坏时（例如，被偷时），不需要移到已经给出的加密密钥 S_N 再用上，这对加密的安全级别可能有有害的影响。现在，具有未变安全级别的终端设备 B-D 可继续其安全的通信，因为它们还在保证各终

端设备 B-D 的加密密钥对。

[0099] 另外，虽然前面介绍了两个终端设备 A-D 之间的通信作为应用示例，然而按照本发明的方法可以直接归纳用于几个终端设备 A-D 之间的 1 对 N 组通信。按照本发明的方法由此为执行一次一密乱码本加密模型提供一种特殊功能和平滑实现，因为在按照本发明的方法中，加密密钥需要的数目例如不必依赖于用户 12.1-12.4 的组的大小。

[0100] 大体上，加密的数据可以是从电子邮件到 GSM 加密的语音的任何种类的数字信息，但是由于媒体丰富信息以较高的速率消耗一次一密乱码本，本发明在诸如 GSM-SMS 通信、电子邮件的文本消息中、或者在诸如地图（例如 MMS）的简单图像中最有利。

[0101] 本发明例如在以下情况下是理想的，其中商业企业具有国际运作、运输车辆或者大商业场所，它们可能被带有终端设备的 A-D 的所有用户 12.1、12.2、12.3、12.4 经常访问。

[0102] 按照本发明的方法可以通过示例使用的情况是公司职员在合同谈判中询问总公司指示的情况。另一个示例是守卫接收包含紧急目标地址的 SMS 消息。

[0103] 按照本发明的方法和系统的其它潜在用户组例如是，公司的旅行代表、贵重运输车辆、出租车队、救护车和保安公司、律师事务所和、医疗使用（秘密远程会诊）、机场人员、石油钻探设备、监狱和核电站、及政府使用。应用对象的其它示例是通过电话的银行交易，由此蓝牙 HUB 可以位于银行；M 商务，即移动商务，由此蓝牙 HUB 可以位于百货公司、基层、私下使用人权（in private use ofhuman right）和其它组等。

[0104] 应当理解，上述解释和有关附图仅用来说明按照本发明的方法和系统。因此，本发明不限于上述实施例或权利要求中限定的情况，对于本领域技术人员来说，显然有许多不同的变化和修改，它们可能落在所附权利要求书定义的发明构思的范围内。

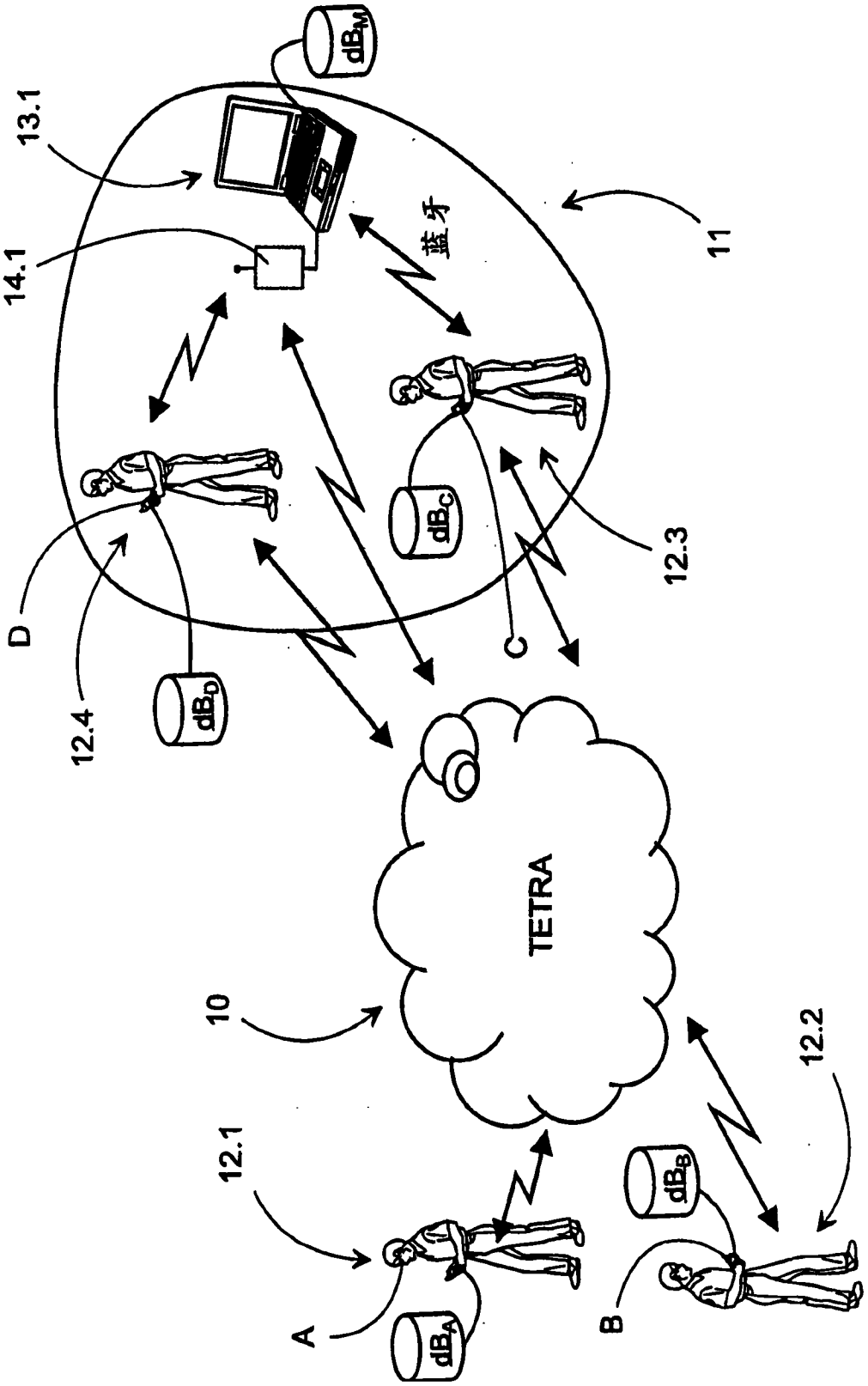


图 1

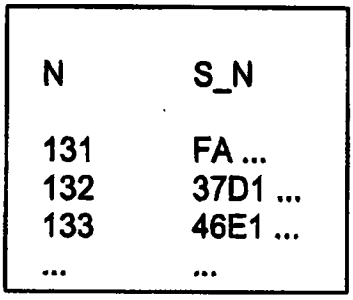


图 2a

ID	N		BACKUP_N				
050-5555555, 455 ...	117	127	57	88	99	101	
050-5556686, 567 ...	121	131	57	63	89	99	105
050-5557778, 988 ...	123	133	61	88	99	105	

图 2b

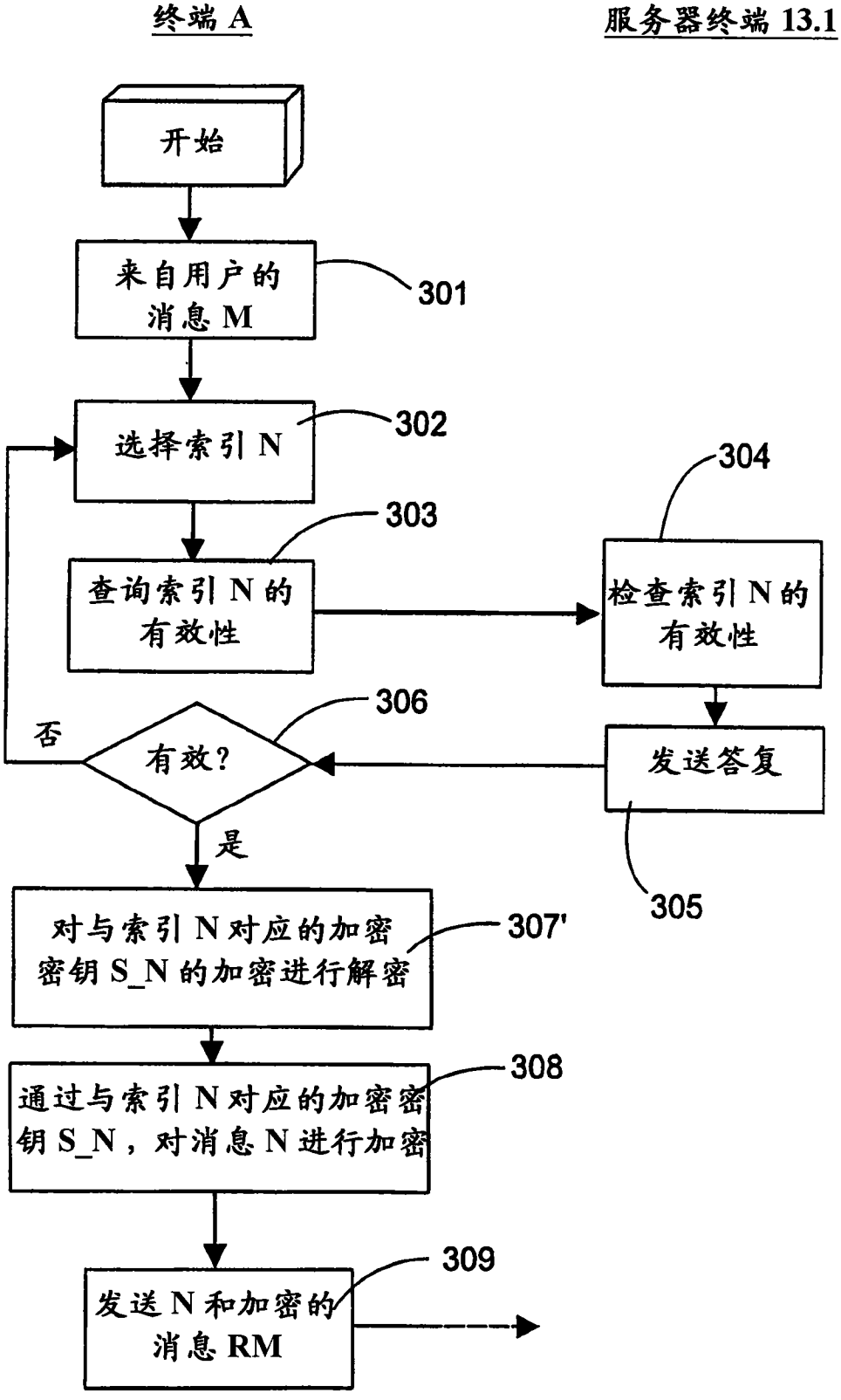

终端 A
服务器终端 13.1
开始
来自用户的消息 M
301
选择索引 N
302
303
查询索引 N 的有效性
304
检查索引 N 的有效性
306
否
有效?
发送答复
305
是
对与索引 N 对应的加密密钥 S_N 的加密进行解密
307'
通过与索引 N 对应的加密密钥 S_N，对消息 N 进行加密
308
发送 N 和加密的消息 RM
309

图 3

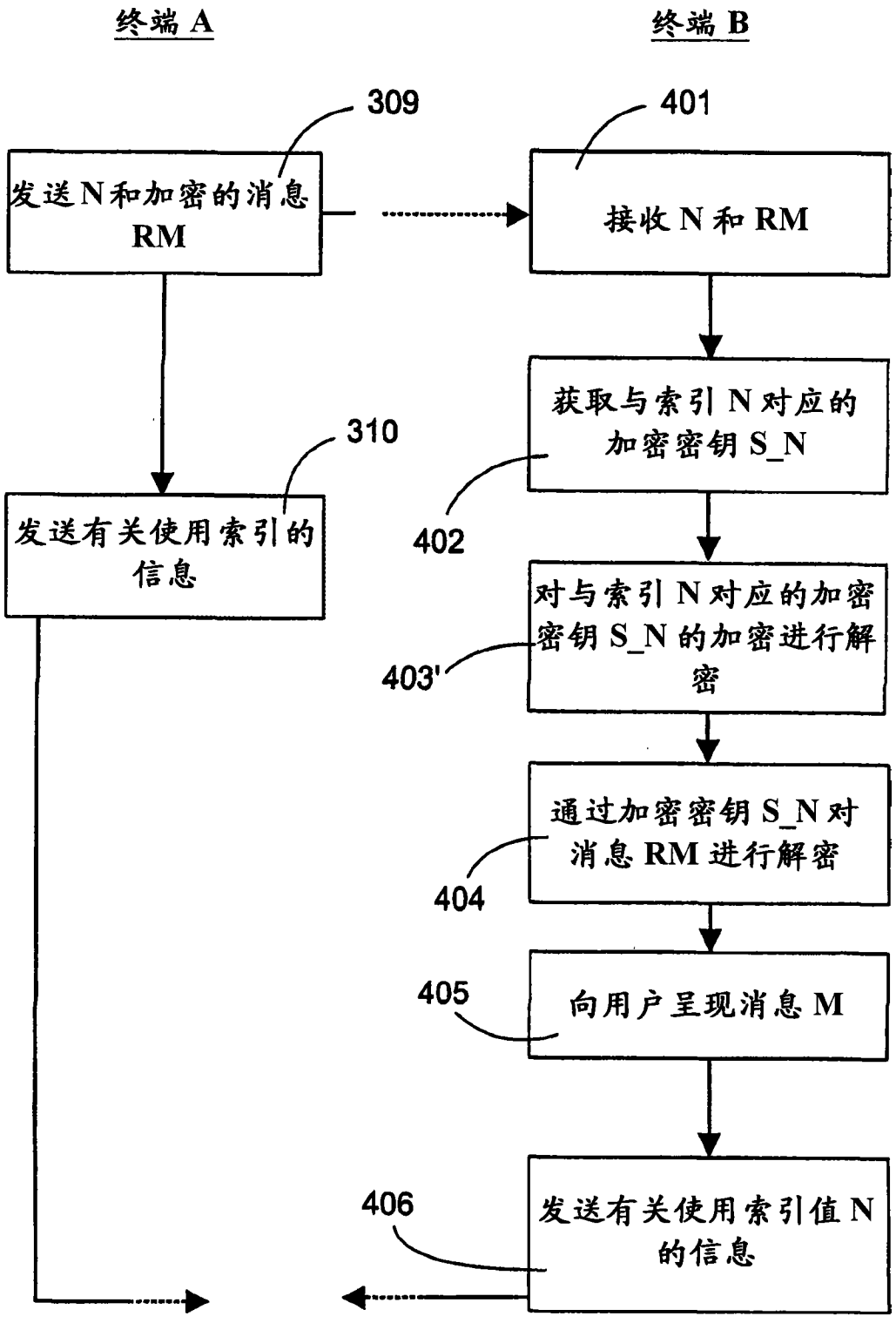

终端 A
终端 B
309
发送 N 和加密的消息 RM
401
接收 N 和 RM
获取与索引 N 对应的加密密钥 S_N
402
310
发送有关使用索引的信息
对与索引 N 对应的加密密钥 S_N 的加密进行解密
403'
通过加密密钥 S_N 对消息 RM 进行解密
404
向用户呈现消息 M
405
发送有关使用索引值 N 的信息
406

图 4

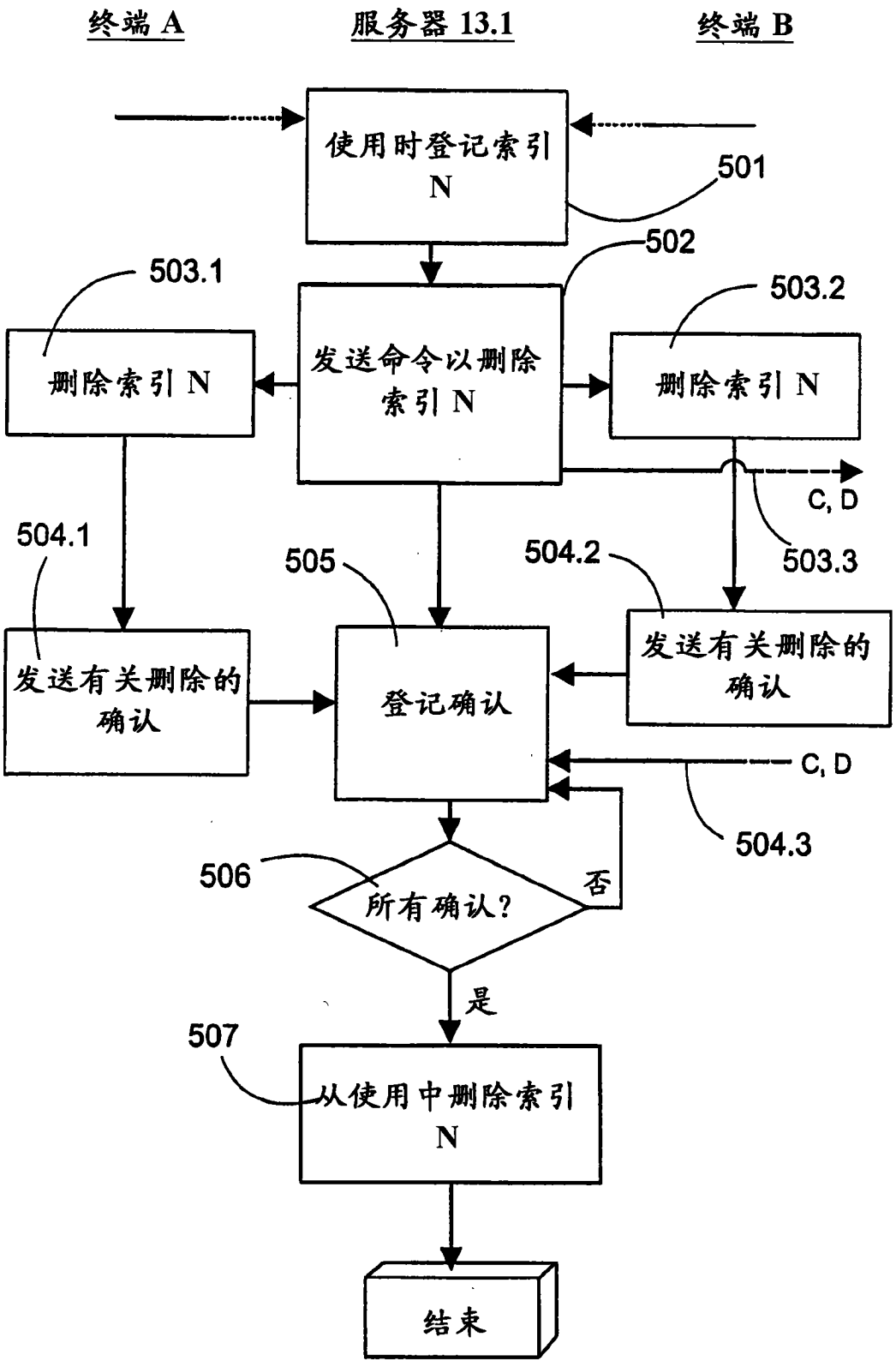

终端 A
服务器 13.1
终端 B
使用时登记索引 N
501
502
503.1
503.2
删除索引 N
发送命令以删除索引 N
删除索引 N
C, D
503.3
504.1
505
504.2
发送有关删除的确认
登记确认
发送有关删除的确认
C, D
504.3
506
所有确认?
否
是
507
从使用中删除索引 N
结束

图 5

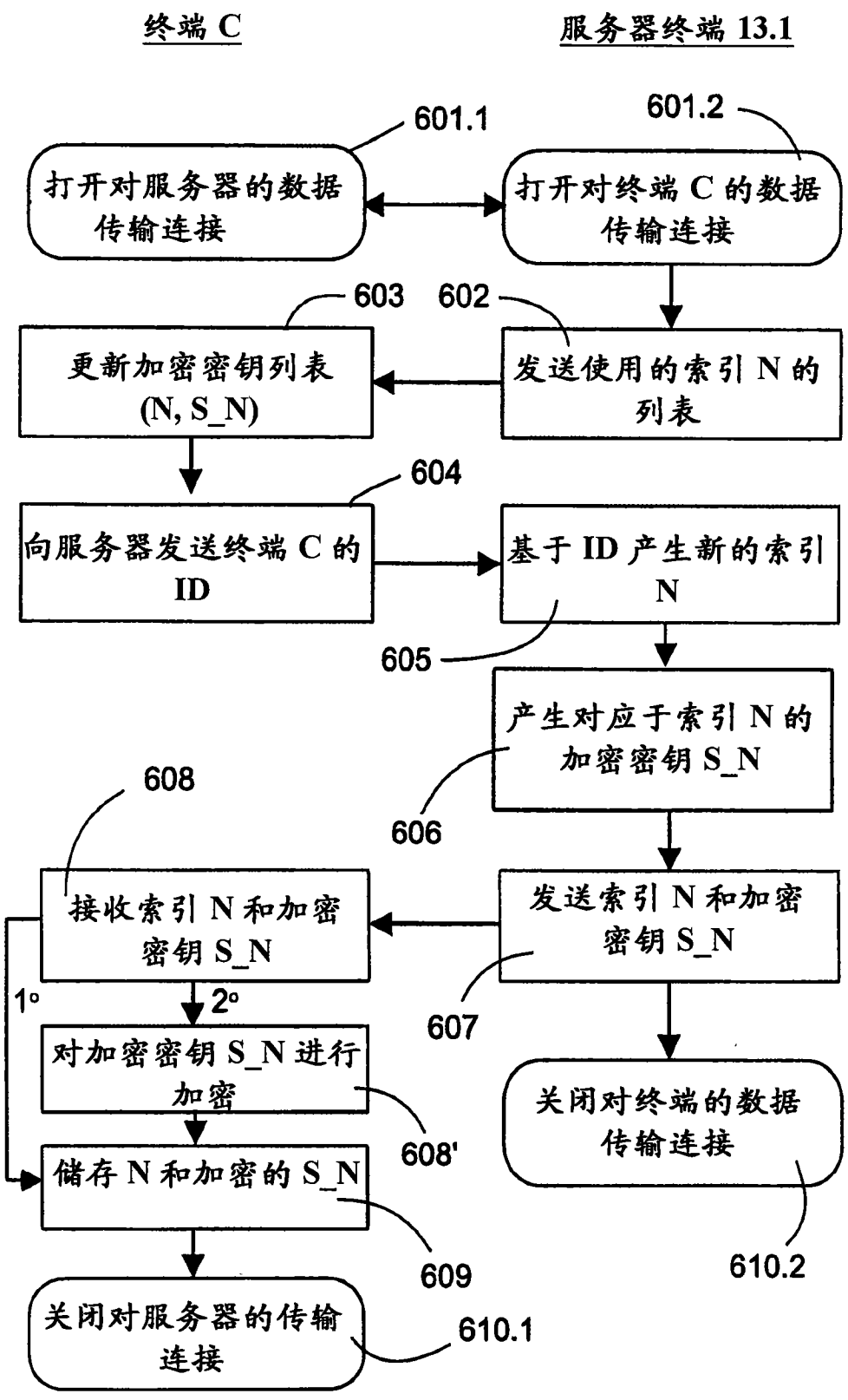

终端 C
服务器终端 13.1
601.1
601.2
打开对服务器的数据传输连接
打开对终端 C 的数据传输连接
603
602
更新加密密钥列表 (N, S_N)
发送使用的索引 N 的列表
604
向服务器发送终端 C 的 ID
基于 ID 产生新的索引 N
605
产生对应于索引 N 的加密密钥 S_N
606
608
接收索引 N 和加密密钥 S_N
发送索引 N 和加密密钥 S_N
607
1°
2°
对加密密钥 S_N 进行加密
608'
关闭对终端的数据传输连接
储存 N 和加密的 S_N
609
610.2
关闭对服务器的传输连接
610.1

图 6

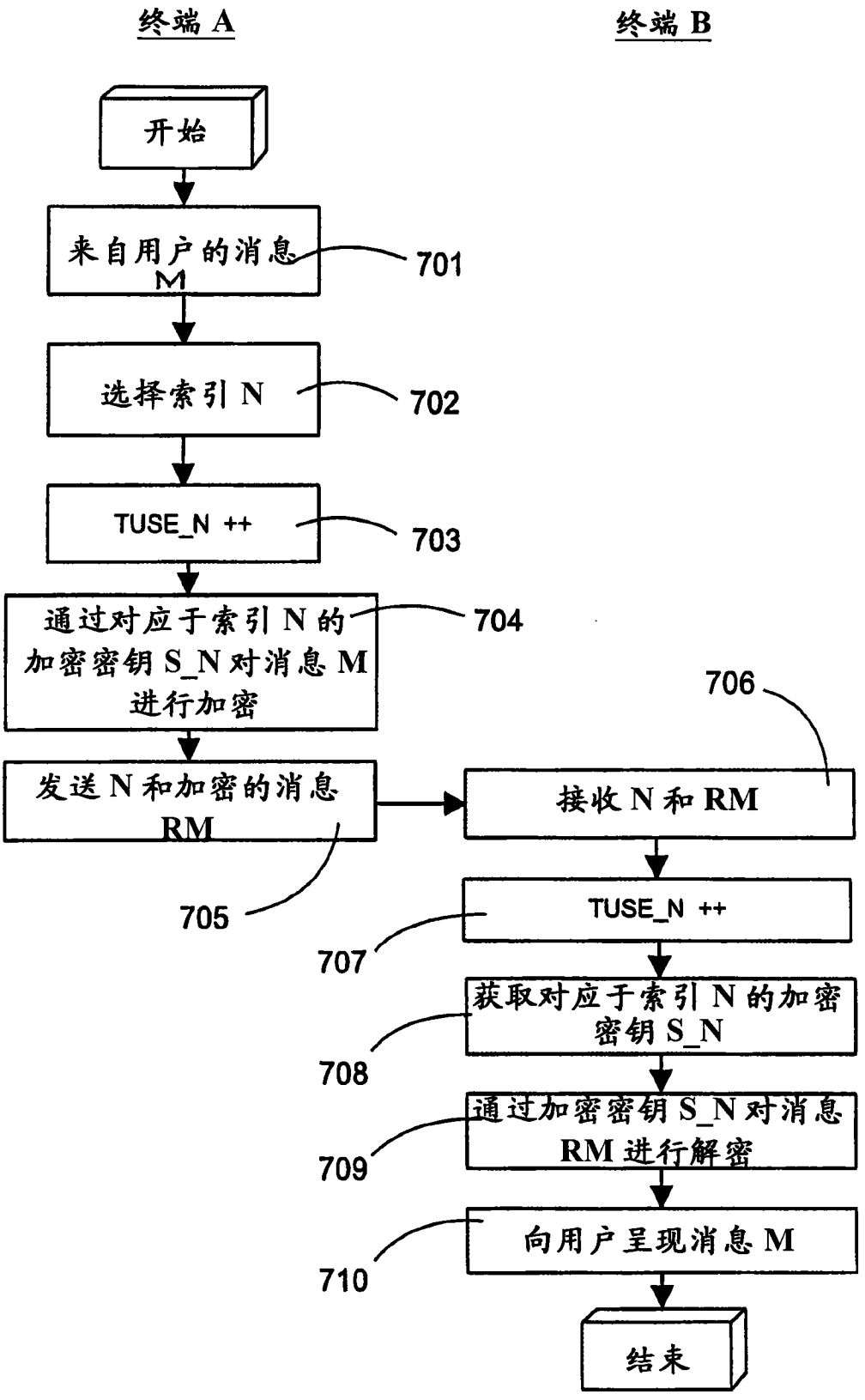

终端 A
终端 B
开始
来自用户的消息 M
701
选择索引 N
702
TUSE_N ++
703
通过对应于索引 N 的加密密钥 S_N 对消息 M 进行加密
704
发送 N 和加密的消息 RM
705
706
接收 N 和 RM
TUSE_N ++
707
获取对应于索引 N 的加密密钥 S_N
708
通过加密密钥 S_N 对消息 RM 进行解密
709
向用户呈现消息 M
710
结束

图 7

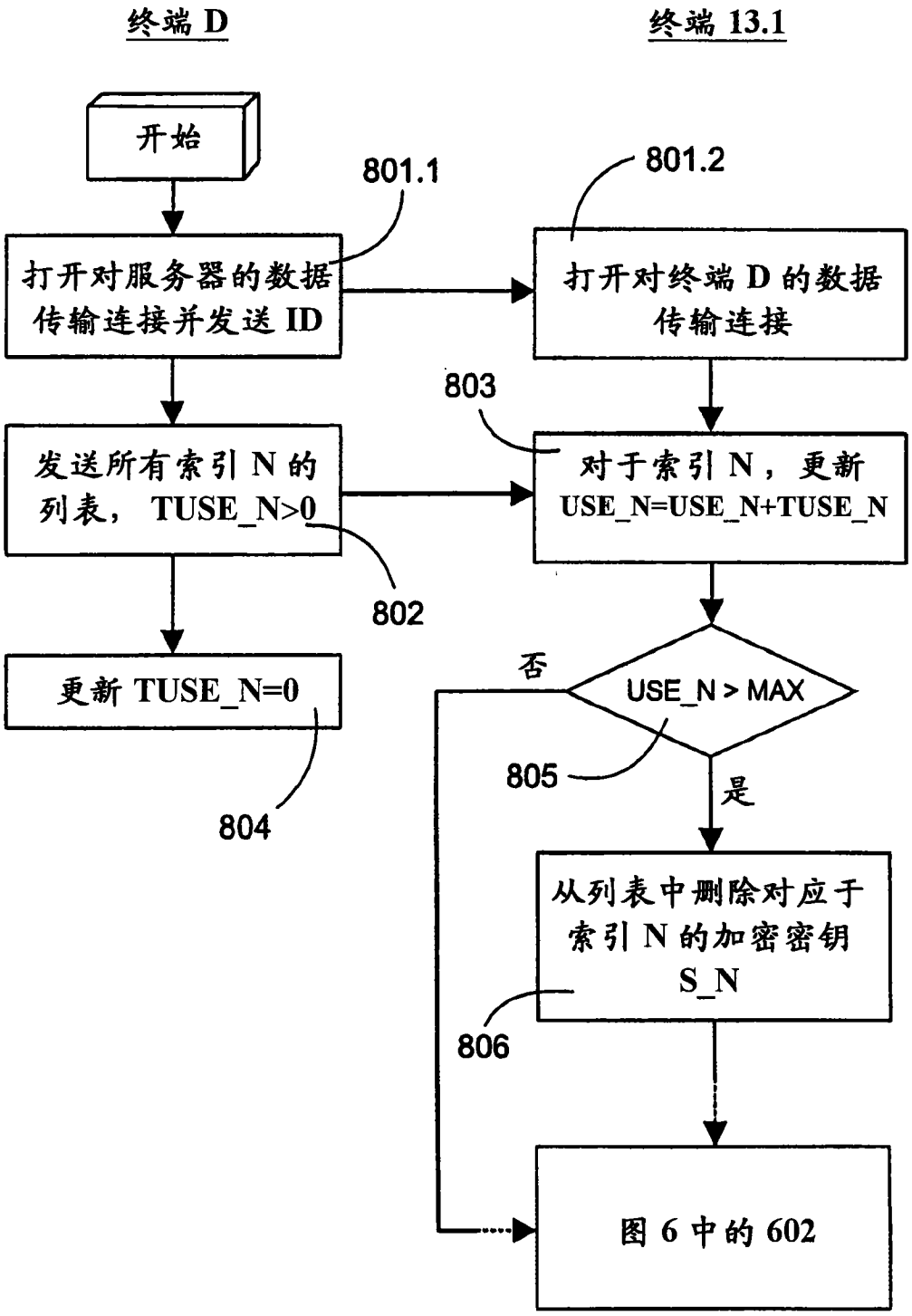

终端 D
终端 13.1
开始
801.1
801.2
打开对服务器的数据传输连接并发送 ID
打开对终端 D 的数据传输连接
803
发送所有索引 N 的列表，TUSE_N>0
对于索引 N，更新 USE_N=USE_N+TUSE_N
802
否
USE_N > MAX
更新 TUSE_N=0
805
是
804
从列表中删除对应于索引 N 的加密密钥 S_N
806
图 6 中的 602

图 8

图 9a

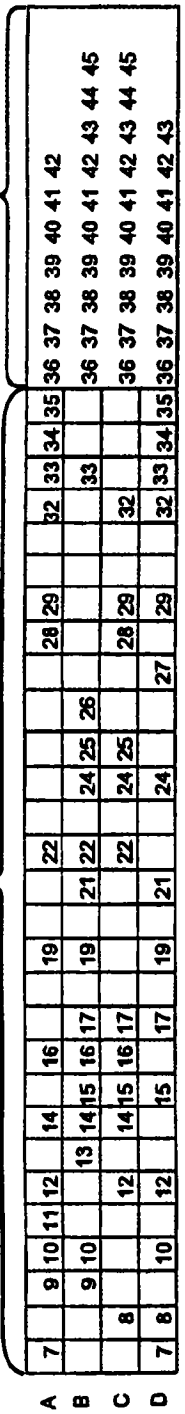


图 9b

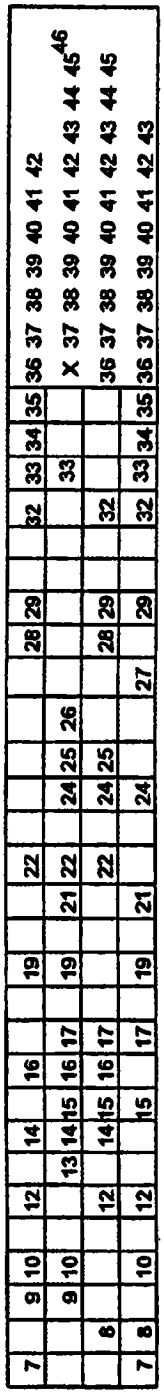


图 9c

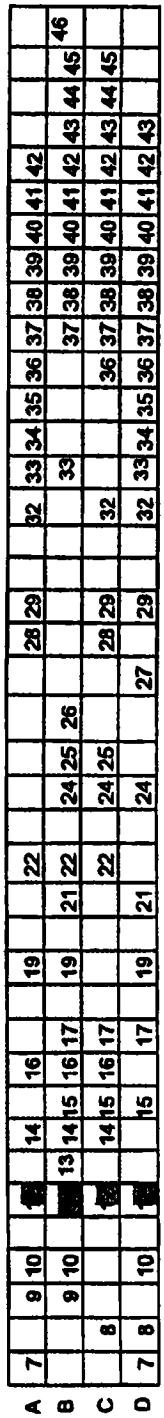
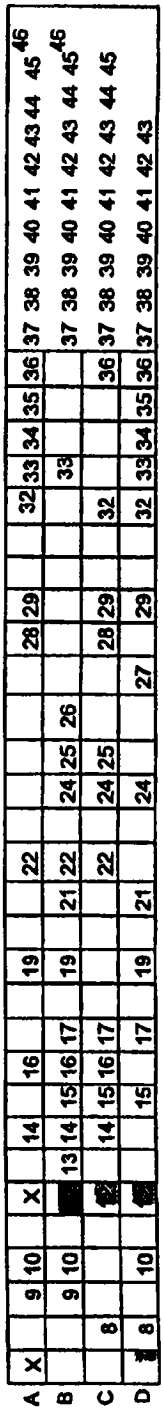


图 9d



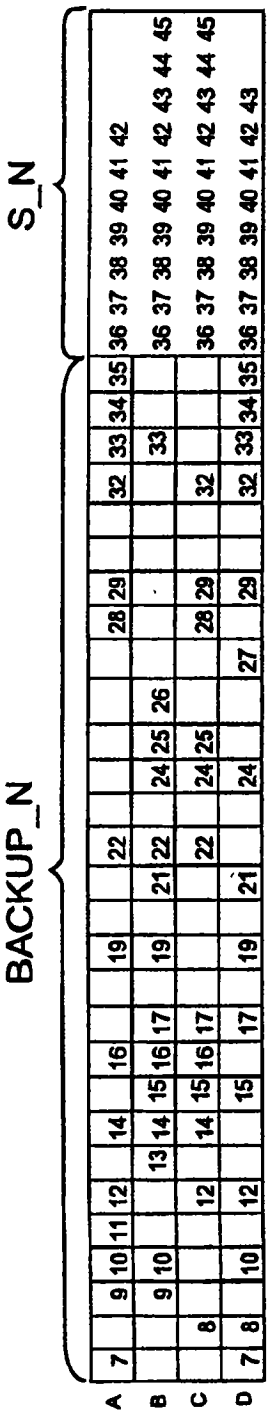


图 10a

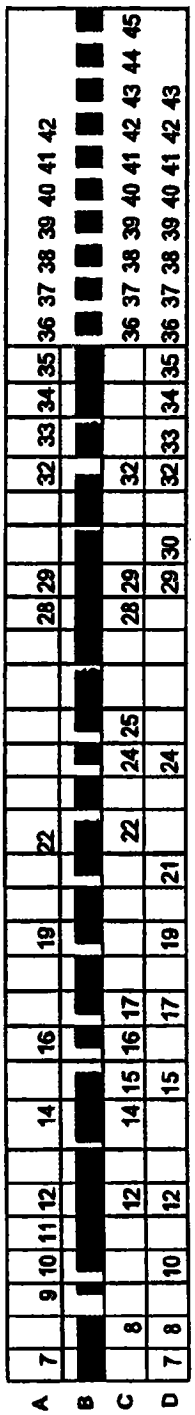


图 10b

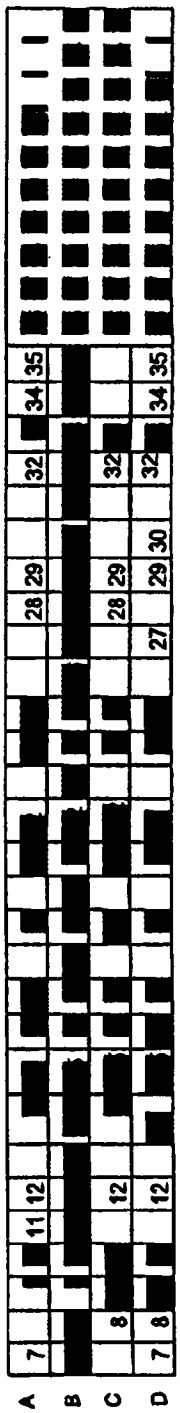


图 10c