



[12] 发明专利说明书

专利号 ZL 200380106795.4

[45] 授权公告日 2009 年 12 月 23 日

[11] 授权公告号 CN 100574188C

[22] 申请日 2003.10.9

WO01/33768A2 2001.5.10

[21] 申请号 200380106795.4

EP1248408A2 2002.10.9

[30] 优先权

US4200770 1980.4.29

[32] 2002.10.24 [33] US [31] 60/420,964

审查员 张行素

[32] 2003.6.24 [33] US [31] 10/602,176

[86] 国际申请 PCT/EP2003/011220 2003.10.9

[74] 专利代理机构 中国专利代理(香港)有限公司

[87] 国际公布 WO2004/038998 英 2004.5.6

代理人 杨凯 王忠忠

[85] 进入国家阶段日期 2005.6.20

[73] 专利权人 艾利森电话股份有限公司

地址 瑞典斯德哥尔摩

[72] 发明人 C·格伦曼

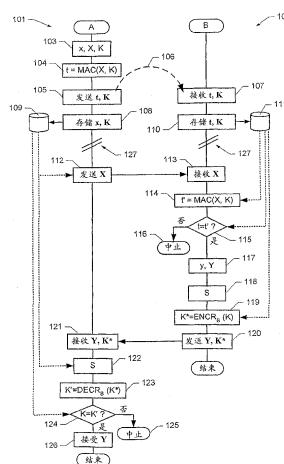
权利要求书 7 页 说明书 26 页 附图 5 页

[54] 发明名称

保密通信

[57] 摘要

一种在第一和第二通信单元之间提供保密通信的方法，包括在所述第一和第二通信单元之间产生共享秘密密钥的密钥交换，所述密钥交换包括用户交互；所述方法包括以下步骤：至少部分通过用户交互向所述第一和第二通信单元提供口令码；由所述第一通信单元生成所述共享秘密密钥的第一成分，并且由所述第二通信单元生成所述共享秘密密钥的第二成分，并将所生成的每个成分发送到所述对应的另一通信单元；由所述对应的接收通信单元基于至少所述口令码，对所述发送的第一和第二成分进行认证；以及仅在所述对应的接收成分成功通过认证时，由每个所述通信单元从至少所述对应的接收的第一成分或第二成分建立所述共享秘密密钥。



1. 一种在第一和第二通信单元之间提供保密通信的方法，所述方法包括在所述第一和第二通信单元之间产生共享秘密密钥的密钥交换，所述密钥交换包括用户交互；所述方法包括以下步骤：

- 至少部分通过用户交互向所述第一和第二通信单元提供口令码；
- 由所述第一通信单元生成所述共享秘密密钥的第一成分，由所述第二通信单元生成所述共享秘密密钥的第二成分，并将所生成的每个成分发送到对应的另一通信单元；
- 由对应的接收通信单元基于至少所述口令码对所述发送的第一和第二成分进行认证；以及
- 仅在对应的接收成分成功通过认证时，由每个所述通信单元从至少对应的接收的第一成分或第二成分建立所述共享秘密密钥；其特征在于：对所述发送的第一和第二成分进行认证的步骤包括通过计算消息认证码的标记值来对所述第一成分进行认证，所述标记值是从所述第一成分和所述口令码计算得到的。

2. 如权利要求 1 所述的方法，其特征在于：所述口令码能够通过用户交互来传送。

3. 如权利要求 1 所述的方法，其特征在于还包括：

- 由所述第二通信单元使用所述生成的共享秘密密钥对所述口令码加密；
- 将所述加密的口令码与所述生成的第二成分一起发送到所述第一通信单元；
- 由所述第一通信单元将所述加密的口令码解密；以及
- 将所述解密的口令码与提供给所述第一通信单元的所述口令码进行比较以对所述接收的第二成分进行认证。

4. 如权利要求 1 所述的方法，其特征在于：所述第一和第二成
分是 Diffie-Hellman 密钥交换协议的第一和第二公共密钥。

5. 如权利要求 1 所述的方法，其特征在于：向所述第一和第二
通信单元提供口令码的步骤包括由所述第一通信单元生成口令码并
且将所述生成的口令码经包括用户交互的通信信道发送到所述第二
通信单元。

6. 如权利要求 1 所述的方法，其特征在于：通过选择纠错码码
字的符号计算所述标记值，所述码字对应于所述第一成分，并且所述
符号由所述口令码标识。

7. 如权利要求 6 所述的方法，其特征在于还包括：从所述第一
成分计算单向散列函数的散列值以及通过选择纠错码码字的符号计
算所述标记值，所述码字对应于所述第一成分的所述散列值，并且所
述符号由所述口令码标识。

8. 如权利要求 6 所述的方法，其特征在于：所述纠错码是里德-
所罗门码。

9. 如权利要求 1 所述的方法，其特征在于包括：

- 由所述第一通信单元生成所述共享秘密密钥的所述第一成
分，并且将所述生成的第一成分发送到所述第二通信单
元；
- 由所述第二通信单元基于所述口令码对所述接收的第一成
分进行认证，并且在所述接收的第一成分被接受为真实可
靠时，从至少所述接收的第一成分生成所述共享秘密密
钥；
- 将所述第二通信单元生成的所述共享秘密密钥第二成分发
送到所述第一通信单元；以及
- 由所述对应第一通信单元基于所述口令码，对所述发送的第
二成分进行认证；并仅在所述接收的第一成分被接受为真
实可靠时，由所述第二通信单元生成所述共享秘密密钥。

10. 如权利要求9所述的方法，其特征在于所述方法还包括：

- 将所述口令码用作密钥，从所述第一成分计算消息认证码的第一消息标记；以及
- 将所述计算的第一消息标记提供给所述第二通信单元；以及其中，由所述第二通信单元基于所述口令码对所述接收的第一成分进行认证的所述步骤包括：
 - 将所述口令码用作密钥，从所述接收的第一成分计算所述消息认证码的第二消息标记；以及
 - 比较所述第一和第二消息标记以对所述接收的第一成分进行认证。

11. 一种在第一和第二通信单元之间提供保密通信的方法，所述方法包括注册步骤和密钥交换步骤；所述注册步骤包括：

- 由所述第一通信单元生成密钥交换机制的第一私有密钥值和对应的第一公共密钥；
- 由所述第一通信单元生成口令码；
- 由所述第一单元使用所述口令码，根据消息认证码计算所述第一公共密钥的消息标记；
- 使所述口令码和所述计算得到的标记值可由所述第二通信单元至少部分通过用户交互来访问；以及所述密钥交换步骤包括：
 - 由所述第一通信单元将所述第一公共密钥发送到所述第二通信单元；
 - 由所述第二通信单元使用所述口令码，根据所述消息认证码计算所述接收的第一公共密钥的所述标记值，并在所述计算得到的标记值与所述传送的标记值一致时，接受所述接收的第一公共密钥；
 - 由所述第二通信单元生成所述密钥交换机制的第二私有密钥值和对应的第二公共密钥；

- 由所述第二通信单元从所述第一公共密钥和所述第二私有密钥值计算所述密钥交换机制的共享秘密密钥；
- 由所述第二通信单元使用所述计算得到的共享秘密密钥对所述口令码加密；
- 由所述第二通信单元将所述第二公共密钥和所述加密的口令码发送到所述第一通信单元；
- 由所述第一通信单元从所述第二公共密钥和所述第一私有密钥值计算所述密钥交换机制的所述共享秘密密钥；以及
- 由所述第一通信单元使用所述第一通信单元计算得到的所述共享秘密密钥将所述发送的加密口令码解密，并在所述解密的口令码与所述第一通信单元原来生成的所述口令码一致时接受所述计算得到的共享秘密密钥。

12. 一种通过在第一与第二通信单元之间产生共享秘密密钥的密钥交换来至少在所述第一和第二通信单元之间提供保密通信的通信系统；所述密钥交换包括用户交互；所述通信系统包括：

- 至少部分通过用户交互向所述第一和第二通信单元提供口令码的部件；
- 由所述第一通信单元生成所述共享秘密密钥的第一成分，并且由所述第二通信单元生成所述共享秘密密钥的第二成分的部件；
- 将所生成的每个成分发送到对应的另一通信单元的部件；
- 由对应的接收通信单元基于所述口令码，对所述发送的第一和第二成分进行认证的部件；以及
- 仅在对应的接收成分成功通过认证时，由每个所述通信单元从至少所述对应的接收的第一成分或第二成分建立所述共享秘密密钥的部件；其特征在于：所述第一和第二通信单元每个包括用于计算消息认证码的标记值的处理部件，所述标记值是从所述第一成分和所述口令码计算得到的。

13. 如权利要求 12 所述的通信系统，其特征在于：所述第一通信单元包括适于生成所述口令码的处理部件和适于将所述生成的口令码提供给所述第二通信单元的输出部件。

14. 如权利要求 12 所述的通信系统，其特征在于：所述处理部件适于通过选择纠错码码字的符号来计算所述标记值，所述码字对应于所述第一成分，并且所述符号由所述口令码标识。

15. 如权利要求 14 所述的通信系统，其特征在于：所述处理部件还适于从所述第一成分计算单向散列函数的散列值以及适于通过选择纠错码码字的符号计算所述标记值，所述码字对应于所述第一成分的所述散列值，并且所述符号由所述口令码标识。

16. 如权利要求 14 所述的通信系统，其特征在于：所述纠错码是里德-所罗门码。

17. 一种通过产生共享秘密密钥的密钥交换来为另一通信单元提供保密通信的通信单元；所述密钥交换包括用户交互；所述通信单元包括数据处理部件、用户接口部件和通信接口，所述处理部件用于执行以下步骤：

- 至少部分通过用户交互，经所述用户接口部件生成要提供给所述另一通信单元的口令码；
- 生成并经所述通信接口发送所述共享秘密密钥的第一成分，并经所述通信接口接收所述共享秘密密钥的第二成分；所述第二成分由所述另一通信单元生成；
- 基于所述口令码对所述接收的第二成分进行认证；以及
- 仅在所述接收的第二成分成功通过认证时，从至少所述第二成分建立所述共享秘密密钥；其特征在于：所述处理部件还适于计算要提供给所述另一通信单元的消息认证码的标记值；所述标记值是从所述第一成分和所述口令码计算得到的。

18. 如权利要求 17 所述的通信单元，其特征在于：所述处理部

件还适于通过选择纠错码码字的符号计算所述标记值，所述码字对应于所述第一成分，并且所述符号由所述口令码标识。

19. 如权利要求 18 所述的通信单元，其特征在于：所述处理部件还适于从所述第一成分计算单向散列函数的散列值以及通过选择纠错码码字的符号计算所述标记值，所述码字对应于所述第一成分的所述散列值，并且所述符号由所述口令码标识。

20. 如权利要求 18 所述的通信单元，其特征在于：所述纠错码是里德-所罗门码。

21. 如权利要求 17 所述的通信单元，其特征在于：所述处理部件还适于

- 将与所述第二成分一起接收的加密口令码解密，所述解密使用所述共享秘密密钥；以及
- 仅在所述解密的口令码与所述生成的口令码一致时，接受所述接收的第二成分。

22. 一种通过产生共享秘密密钥的密钥交换为另一通信单元提供保密通信的通信单元；所述密钥交换包括用户交互；所述通信单元包括数据处理部件、存储部件和通信接口，所述处理部件适于执行产生共享秘密密钥的密钥交换；所述密钥交换包括：

- 至少部分通过用户交互接收并存储由另一通信单元生成的口令码；
- 经所述通信接口接收由所述另一通信单元生成的所述共享秘密密钥的第一成分；
- 基于所述口令码对所述接收的第一成分进行认证；
- 如果所述接收的第一成分成功通过认证，则从至少所述第一成分建立所述共享秘密密钥，并经所述通信接口发送所述共享秘密密钥的第二成分；其特征在于所述通信单元还适于在所述存储部件中存储消息认证标记；并且其中所述处理部件还适于：

- 从所述接收的第一成分和所述口令码计算消息认证码的标记值；以及
- 仅在所述计算得到的标记值与所述存储的消息认证标记一致时才接受所述接收的第一成分。

23. 如权利要求 22 所述的通信单元，其特征在于：所述处理部件还适于通过选择纠错码码字的符号来计算所述标记值，所述码字对应于所述第一成分，并且所述符号由所述口令码标识。

24. 如权利要求 23 所述的通信单元，其特征在于：所述处理部件还适于从所述第一成分计算单向散列函数的散列值以及适于通过选择纠错码码字的符号来计算所述标记值，所述码字对应于所述第一成分的所述散列值，并且所述符号由所述口令码标识。

25. 如权利要求 23 所述的通信单元，其特征在于：所述纠错码是里德-所罗门码。

26. 如权利要求 22 所述的通信单元，其特征在于：所述处理部件还适于：

- 将所述存储的口令码加密，所述加密使用所述共享秘密密钥；以及
- 经所述通信接口将所述加密的口令码与所述第二成分一起发送到所述另一通信单元。

保密通信

发明领域

本发明涉及在第一通信单元与第二通信单元之间的保密通信。

发明背景

在无线通信系统中，在参与的通信单元之间建立保密通信是一个重要的方面。在许多通信系统中，实施了为参与的通信单元提供共同共享秘密密钥的交换机制。一旦在两个单元之间建立了共享秘密，则可将共享秘密用于为这两个单元之间传送的消息提供加密和/或完整性保护。

在许多情况中，保密通信的建立是通过涉及用户交互的密钥交换来实现的，所述用户交互例如用户将例如密码或 PIN 等口令码输入一个或两个通信单元中。具体而言，在参与单元尚未建立任何保密关系，如共享秘密的情况下，用户交互可能是必需的。

短距离无线通信技术的一个示例是蓝牙技术，这是一种在全球可用的未授权的 ISM (工业、科学及医疗) 频带中 2.45 GHz 上工作的无线电通信技术。该频带提供 83.5 MHz 的无线电频谱。蓝牙是一种提供低成本、低功率无线电实现的技术。采用蓝牙，可以专门方式在所谓的微微网中连接个人装置。蓝牙标准（参阅“蓝牙系统规范、核心、版本 1.1”中的“基带规范”[“Baseband Specification” in “Specification of the Bluetooth System, Core, Version 1.1”, Bluetooth Special Interest Group, February 2001]）还包括多种保密机制。具体而言，蓝牙标准提供一种配对机制，该机制中，以前尚未连接的两个装置执行密钥交换，以便在两个蓝牙装置之间建立共享秘密，即所谓的链路密钥。链路密钥是从装置用户输入的 PIN 中

获得的。链路密钥随后用于保护蓝牙通信。

美国专利 4200770 中公开的所谓 Diffie-Hellman 密钥交换协议提供了具有共同秘密的两个装置。根据此协议，每个装置生成一个秘密密钥，从该秘密密钥获得公共密钥，并将公共密钥发送给另一装置。共享秘密随后由每个装置从其秘密密钥和另一装置的对应接收公共密钥生成。

此类密钥交换机制的一个一般问题是它可能受到中间人攻击的攻击，即，遭受保密违反，其中，恶意用户拦截并更改通信装置之间的消息。

由 C. Gehrman 和 K. Nyberg 所著的题为“蓝牙基带保密增强”的文章（“Enhancements to Bluetooth baseband security”，Proceedings of Nordsec 2001，Copenhagen，November 2001）描述了一种涉及用户交互的认证方案。具体而言，上述文章描述了一种对由匿名 Diffie-Hellman 密钥交换先前建立的共享秘密进行认证的方法。此方法基于一种假设，即，如果在 Diffie-Hellman 密钥交换中存在中间人，则在合法装置中建立的 Diffie-Hellman 密钥将不同。认证基于两个装置根据建立的共享秘密计算得到的检查值来进行。可将创建的检查值显示在两个装置上并由用户进行比较，或者由用户将一个装置计算出的检查值输入另一装置，以允许另一装置执行比较。

上述现有技术系统的问题在于它需要人工干预，在建立保密通信时需要进行对建立的共享秘密进行认证的用户交互。然而，在例如应快速建立实际的保密通信的情况下，这可能不合乎需要。

发明概述

上述其它问题由在第一和第二通信单元之间提供保密通信的方法予以解决，所述方法包括在所述第一和第二通信单元之间产生共享秘密密钥的密钥交换，所述密钥交换包括用户交互；所述方法

包括以下步骤：

- 至少部分通过用户交互向所述第一和第二通信单元提供口令码；
- 由所述第一通信单元生成所述共享秘密密钥的第一成分，并且由所述第二通信单元生成所述共享秘密密钥的第二成分，并将所生成的每个成分发送到所述对应的另一通信单元；
- 由所述对应的接收通信单元基于至少所述口令码对所述发送的第一和第二成分进行认证；以及
- 仅在所述对应的接收成分成功通过认证时，由每个所述通信单元从至少所述对应的接收的第一成分或第二成分建立所述共享秘密密钥。

本发明的优点在于可在实际密钥交换前确定口令码并将其提供给通信单元，并在以后实际密钥交换发生时，即实际创建共享秘密时使用。因此，无需在实际创建共享秘密期间为对共享秘密进行认证而进行用户交互，且不会损害所述方法的保密性。

本发明的又一优点在于它降低了与密钥交换相关的中间人攻击的风险，从而提高了通信系统的保密性。

口令码最好例如由第一单元自动创建，从而确保口令码的随机性。由通信单元之一生成的口令码经涉及用户交互的通信信道发送到另一通信单元，该通信信道与用于密钥交换的通信链路不同，由于敌人拦截该不同通信信道的风险降低，因此保密性得以提高。例如，涉及用户交互的不同通信信道可以是电话线、作为注册进程一部分发送的邮件或信函或诸如此类。口令码很短，最好是短到足以经人机界面或人人界面传送。例如，口令码可以是包括少于 10 个数字和/或字母和/或其它符号的字符串，例如 4-6 个十六进制数字，从而简化口令码的传送。例如，口令码可从已生成该代码的通信单元的显示器轻松地读出，经电话、通过邮件等方式传送，并键入另

一单元、电话、计算机等装置。

因此，用户交互涉及至少一个通信单元的用户从例如显示器读出口令码，输入口令码，或者至少执行表示授权传送口令码的用户输入等，即用户交互涉及至少由一个通信单元输出口令码，或由用户接收输入，例如，接收表示口令码的输入。在一些实施例中，用户交互还涉及人人界面，例如，通过将口令码从一个装置的用户传送到另一装置的用户。

密钥交换可基于产生共享秘密的任一适合的密钥交换机制，所述共享秘密最好是长度足以在随后的通信中提供足够的保密的共享秘密。在一个实施例中，密钥交换是 Diffie-Hellman 密钥交换。其它的密钥交换机制示例包括 RSA 密钥交换。根据本发明的密钥交换可基于一般的标准密钥交换机制，这是一个优点。

根据本发明的优选实施例，对所述发送的第一和第二成分进行认证的步骤包括通过计算消息认证码的标记值而对所述第一成分进行认证，所述标记值由所述第一成分和所述口令码计算得到，从而提供对所述第一成分的有效认证，从而提供高保密性并只需要很少的计算资源。消息认证码（MAC）最好是无条件的保密 MAC，即，即使通过大量计算资源也无法实际破解的 MAC。

根据又一优选实施例，通过选择纠错码如里德-所罗门码的码字的符号计算标记值；所述码字对应于所述第一成分，并且所述符号由所述口令码标识。因此，即使对短口令码也提供了高的认证保密性。

认证最好还包括从第一成分计算单向散列函数的散列值，以及通过选择纠错码码字的符号计算所述标记值；所述码字对应于所述第一成分的散列值，并且所述符号由所述口令码标识。因此，在维护高保密性的同时，可进一步缩减码字的长度。

术语通信单元包括任一装置或装置组；这些装置包括用于接收和/或发送通信信号如无线电通信信号等的合适电路以便于数据通

信。此类装置的示例包括便携式无线电通信设备和其它手持式或便携式装置。术语便携式无线电通信设备包括诸如移动电话、寻呼器、通信器即电子组织器、智能电话、个人数字助理（PDA）、手持式计算机等的所有设备。

通信单元的其它示例包括固定通信设备，例如包括无线通信接口的固定计算机或其它电子设备。在一个实施例中，通信单元之一可包括多个设备。例如，通信单元可包括计算机网络，该计算机网络包括例如提供至该计算机网络如 LAN 的无线接入的接入点。

例如，通信单元可根据蓝牙技术或任何其它无线通信技术例如无线 LAN 进行操作。

其它优选实施例在从属权利要求中公开。

要注意的是，上述及以下所述方法的特征可用软件实现，通过计算机可执行指令的执行，在数据处理系统或其它处理部件中执行。指令可以是从存储介质或经计算机网络从另一计算机加载到存储器如 RAM 中的程序代码组件。或者，所述特征可用硬连线的电路而非软件来实现，或者与软件组合来实现。

本发明可以不同的方式实施，包括上述方法和以下的通信系统和其它产品装置，每种方式均具有结合最先提及的方法所述的一个或多个益处和优点，并且每种方式具有一个或多个优选实施例，这些实施例对应于结合最先提及的方法所述的、并且在从属权利要求公开的优选实施例。

本发明还涉及一种通信系统，用于通过在第一与第二通信单元之间产生共享秘密密钥的密钥交换，至少在所述第一和第二通信单元之间提供保密通信；所述密钥交换包括用户交互；所述通信系统包括：

- 至少部分通过用户交互向所述第一和第二通信单元提供口令码的部件；
- 由所述第一通信单元生成所述共享秘密密钥的第一成分，

并且由所述第二通信单元生成所述共享秘密密钥的第二成分的部件；

- 将所生成的每个成分发送到所述对应的另一通信单元的部件；
- 由所述对应的接收通信单元基于所述口令码，对所述发送的第一和第二成分进行认证的部件；以及
- 仅在所述对应的接收成分成功通过认证时，由每个所述通信单元从至少所述对应的接收的第一成分或第二成分建立所述共享秘密密钥的部件。

本发明还涉及通过产生共享秘密密钥的密钥交换为另一通信单元提供保密通信的通信单元；所述密钥交换包括用户交互；所述通信单元包括数据处理部件、用户接口部件和通信接口；所述处理部件适于执行以下步骤：

- 生成至少部分要通过用户交互，经用户接口部件提供给所述另一通信单元的口令码；
- 生成并经所述通信接口发送所述共享秘密密钥的第一成分，以及经所述通信接口接收所述共享秘密密钥的第二成分；所述第二成分由所述另一通信单元生成；
- 基于所述口令码对所述接收的第二成分进行认证；以及
- 仅在所述接收的第二成分成功通过认证时，从至少所述第二成分建立所述共享秘密密钥。

本发明还涉及通过产生共享秘密密钥的密钥交换，为另一通信单元提供保密通信的通信单元；所述密钥交换包括用户交互；所述通信单元包括数据处理部件、存储部件和通信接口；所述处理部件适于执行产生共享秘密密钥的密钥交换；所述密钥交换包括：

- 至少部分通过用户交互接收并存储由另一通信单元生成的

口令码；

- 经所述通信接口接收由所述另一通信单元生成的所述共享秘密密钥的第一成分；
- 基于所述口令码对所述接收的第一成分进行认证；
- 如果所述接收的第一成分成功通过认证，则从至少所述第一成分建立所述共享秘密密钥，并经所述通信接口发送所述共享秘密密钥的第二成分。

此处，术语“处理部件”包括适用于执行上述功能的任何电路和/或装置。具体而言，上述术语包括通用或专用可编程微处理器、数字信号处理器（DSP）、专用集成电路（ASIC）、可编程逻辑阵列（PLA）、现场可编程门阵列（FPGA）、专用电子电路等或它们的组合。

通信接口可包括适用于经无线通信信道传送数据的任一合适电路或装置。例如，接口可包括无线电发送器和接收器，或使用另一种通信技术如红外信号等的发送器/接收器。

术语“存储部件”意在包括适用于数据存储的任何合适的装置或设备，例如，电可擦除可编程只读存储器（EEPROM）、闪存、可擦可编程只读存储器（EPROM）、随机存取存储器（RAM）。存储部件可以是通信单元的组成部分，或者它可以连接到所述单元，例如，以可拆装方式插入。例如，存储部件可以是移动存储介质，如存储卡、PCMCIA 卡、智能卡等。

附图简述

通过下面参照附图所述的实施例，可清楚本发明的上述和其它方面，附图中：

图 1 显示了保密密钥交换机制实施例的流程图；

图 2a-b 显示了保密密钥交换机制的其它实施例的流程图；

图 3 显示了基于纠错码计算消息认证码的方法的流程图；

图 4a-b 显示了基于里德-所罗门码计算消息认证码的方法的示例流程图；

图 5 显示了对应于图 4a-b 中 MAC 构造的多个构造示例的成功替代攻击概率的表格；

图 6 显示了两个通信单元的方框图；

图 7 显示了经计算机网络的接入点与计算机网络进行通信的便携式通信单元的方框图。

优选实施例详细说明

图 1 显示了保密密钥交换机制实施例的流程图。在两个单元(一般地标记为 A 和 B)要执行保密密钥交换以便建立共享秘密密钥时，它们执行下列步骤，其中，流程图左侧一般地由参考标记 101 指定的步骤由单元 A 执行，而流程图右侧一般地参考标记 102 指定的步骤由单元 B 执行。

以下的密钥交换基于用于密钥协商的所谓“Diffie-Hellman”方法。为便于理解以下说明，将对述 Diffie-Hellman 密钥协商进行简单描。更详细的描述可参考美国专利 US 4200770，该专利通过引用全部结合于本文中。

两个单元 A 和 B 希望建立共享秘密密钥时，它们就一个素数 $p > 2$ 和一个基数 g (即本原元 (primitive) mod p) 达成一致。参数 p 和 g 可硬编码到两个单元中，它们可由其中一个单元生成并传送到另一单元，可从第三方检索，或诸如此类。例如，为生成 p 和 g ，可以选择 p 的值，例如，将 p 值选择为大的随机数，例如包括 1000 比特或更多，并且可执行已知的素数测试以便测试 p 是否为素数。如果不是，则可选择新的 p 并进行测试直至找到素数为止。随后，选择随机数 g 并测试 g 是否为生成元 (generator)；如果不是，则选择新的 g 并进行测试直至找到生成元为止。

每个单元生成小于 p-1 的秘密数字。在下文中，由单元 A 生成的秘密数字称为 A，而由单元 B 生成的秘密数字称为 y。每个单元随后基于秘密值和上述参数生成公共密钥：单元 A 生成 $X=g^x \bmod p$ ，其中 mod 指模函数，即整数除法的余数。同样地，单元 B 生成 $Y=g^y \bmod p$ 。

这两个单元交换其公共密钥，并且每个单元根据以下等式计算共同的秘密值 S：

$$\text{单元 A: } S = (Y)^x \bmod p,$$

$$\text{单元 B: } S = (X)^y \bmod p.$$

其结果是，由于 $(g^y \bmod p)^x \bmod p = (g^x \bmod p)^y \bmod p$ ，因此单元 A 和 B 已建立了共同的秘密密钥 S 而无需传送秘密值 x 和 y。

现在参照图 1，在密钥交换的初始步骤 103 中，单元 A 生成随机数 x、对应的 Diffie-Hellman 公共密钥 X 和短的秘密字符串 K 或其它口令码。Diffie-Hellman 公共密钥 X 是如上所述基于单元 A 和 B 已协商好的对应参数 g 和 p 计算得到的。秘密字符串 K 最好从合适的密钥空间随机确定的，例如，字符串 K 可采取 4-6 个十六进制数字的形式。

在随后的步骤 104 中，单元 A 使用消息认证码（MAC）从公共密钥 X 计算标记值 t。此处，术语“消息认证码”指用于从发送方与接收方之间传送的消息计算标记值的任何合适函数，其中，该函数基于发送方与接收方之间的对称共享秘密。所述秘密值称为密钥。秘密密钥是 MAC 计算的输入变量。只有拥有正确的秘密密钥的人员能够计算任意消息的标记值。MAC 的标记值是完整性检查值，此值从原始消息数据计算得到并传送到消息的接收方。在收到受 MAC 保护的消息后，接收方基于接收到的数据计算对应的标记值。如果计算的标记值等于接收的标记值，则将消息作为真实可靠的消息接收。已知 MAC 的示例包括所谓的消息认证加密散列

(HMAC) 算法，该算法基于加密的单向散列函数，如保密散列算法 SHA-1 及消息摘要算法 MD5。MAC 在许多数据通信协议中用于提供数据完整性保护。下面将描述基于纠错码的 MAC 函数实施例。在步骤 104 中，MAC 函数的输入包括公共密钥 X，并且生成的秘密字符串 K 用作标记值 t 的 MAC 计算的密钥。可以理解，在密钥建立期间传送附加数据的一些实施例中，可从包括公共密钥 X 和附加数据的消息计算标记值，从而也为附加数据提供完整性保护。

在步骤 105 中，如图 1 中虚线箭头 106 所示，生成的秘密字符串 K 和计算得到的标记值 t 经涉及用户交互的合适通信信道传送到单元 B。例如，通过从单元 A 的显示器读出 K 和 t 的值，并将这些值键入单元 B 中，可将这些值从单元 A 发送到单元 B。在另一实施例中，可通过某些其它方式传送值，例如通过电信网络，将值作为例如电子邮件、SMS 之类的加密消息发送，或者通过涉及用户交互的任何其它合适的通信信道传送，所述任何其它通信信道最好是不同于要建立保密通信的通信信道。优点是，单元 A 和 B 不必彼此建立通信链路；它们甚至不必彼此相邻。例如，单元 A 的用户可通过电话、邮件或任何其它合适方式将秘密字符串和标记值传送到单元 B 的用户。此外，可在单元之间实际要建立共享秘密密钥（例如作为注册过程的一部分）前执行传送 K 和 t 的生成值的操作。在一个实施例中，标识符 ID 与 K 和 t 一起传送，以便有利于随后对 K 和 t 的检索。

在步骤 107 中，单元 B 接收 K 和 t 的值，在步骤 110 中，将它们存储在单元 B 的存储介质 111 中，例如，存储在便携式装置的 EEPROM 或 EEPROM 中，存储在智能卡、硬盘或任何其它合适的数据存储装置上。如果 K 和 t 值与标识符 ID 相关，则 K 和 t 值存储时可与该标识符相关，例如，将标识符用作索引。

同样地，在步骤 108 中，单元 A 在单元 A 的存储介质 109 中存储秘密字符串 K，其存储方式可与标识符 ID 相关。此外，单元

A 存储秘密值 x，公共密钥 X 的计算基于该值。

至此结束了初始注册过程。在单元 A 和 B 经通信链路实际连接时，执行包括实际密钥交换的以下步骤。如图 1 中线条 127 所示，这可在上述初始注册后立即进行，或在以后执行。

在步骤 112 中，单元 A 通过经无线通信链路向单元 B 发送公共密钥 X 而启动实际的密钥交换。在秘密字符串 K 与标识符 ID 相关的实施例中，单元 A 也发送该标识符。同样地，如果在步骤 104 中为公共密钥和一些附加数据计算了标记值 t，则该附加数据也从单元 A 发送到单元 B。

单元 B 从单元 A 接收公共密钥 X（步骤 113）时，在步骤 114 中，单元 B 从存储介质 111 检索秘密字符串 K；在一个实施例中，检索基于标识符 ID 进行。单元 B 基于秘密字符串 K 计算接收的公共密钥 X 的 MAC 标记值 t' 。

在步骤 115 中，单元 B 将计算得到的标记值 t' 与以前存储的标记值 t 进行比较。如果标记值不同，则拒绝接收的公共密钥（步骤 116）。例如，单元 B 可通过向单元 A 发送对应的消息和/或例如通过提供可视或可闻指示而将拒绝通知给用户，从而中止密钥交换。否则，即如果标记值相同，则接受公共密钥 X 并且处理过程继续到步骤 117。

在步骤 117 中，单元 B 如上所述生成秘密值 y 和对应的 Diffie-Hellman 公共密钥 Y。

在步骤 118 中，单元 B 生成对应的 Diffie-Hellman 共享秘密密钥 $S = (X)^y \bmod p$ 。

在步骤 119 中，单元 B 使用生成的共享秘密密钥 S 将从存储介质 111 中检索的秘密字符串 K 加密，产生加密的秘密字符串 K^* 。加密可基于任何基于对称秘密密钥的合适加密方法，如 AES、SAFER+、RC5、DES、3DES 等。

在步骤 120 中，单元 B 向单元 A 发送加密的秘密字符串 K^* 和

Diffie-Hellman 公共密钥 Y。同样地，在一个实施例中，单元 B 还发送对应的标识符 ID。

在步骤 121 中，单元 A 接收加密的秘密字符串 K* 和 Diffie-Hellman 公共密钥 Y。

在步骤 122 中，单元 A 利用存储在存储介质 109 中的秘密值 x 生成 Diffie-Hellman 共享秘密密钥 $S = (Y)^x \bmod p$ 。

在步骤 123 中，单元 A 使用生成的共享秘密密钥 S 将接收的加密秘密字符串 K* 解密，以获得解密的秘密字符串 K'。

在步骤 124 中，单元 A 将接收到的、经过解密的秘密字符串 K' 与单元 A 原来生成并存储在存储介质 109 中的秘密字符串 K 进行比较，如果秘密字符串不相等，则拒绝接收的公共密钥 Y，即丢弃生成的共享秘密密钥 S（步骤 125）。否则，处理过程继续到步骤 126。

在步骤 126 中，接受接收的公共密钥 Y，即，将计算的共享秘密密钥 S 接受为共享秘密。在一个实施例中，将对应的消息发送到单元 B，从而完成密钥交换。生成的共享秘密密钥现在可用于保护单元 A 与 B 之间的后续通信，例如，通过对这两个单元之间发送的消息进行加密和/或完整性保护。

可以理解，在替代实施例中，从单元 B 传送到单元 A 的公共密钥 Y 可通过不同的方法进行认证，例如，通过计算 MAC 值。通过包括加密的 K* 对 Y 进行认证的优点在于：可以使用相同的密钥多次而不会损害方法的保密性。

图 2a-b 显示了根据本发明其它实施例的密钥交换机制的流程图。如上述示例中一样，两个单元执行保密密钥交换以便建立共享的秘密密钥。与前面的示例不同，其中一个单元包括两个装置 B 和 C，而另一单元只包括一个装置，一般地标记为装置 A。初始注册过程在装置 A 与装置 C 之间执行。例如，装置 A 可以是便携式装置，如移动电话、PDA 等，装置 B 可以是计算机网络的接入点等，

而装置 C 可以是计算机网络的服务器计算机，下面将会结合图 7 对此进行更详细的描述。因此，在图 2a-b 中流程图左侧的步骤（一般地标记为 101）由装置 A 执行，而流程图中部的步骤（一般地标记为 202）由装置 B 执行，而流程图右侧的步骤（一般地标记为 201）由装置 C 执行。在图 2a-b 的示例中，由装置 A、B 或 C 执行的一些步骤与图 1 中单元 A 执行的步骤一致，其中，相同的标号指代对应的步骤。

现在参照图 2a，在初始步骤 103 中，装置 A 生成随机数 x、对应的 Diffie-Hellman 公共密钥 X 和短的秘密字符串 K，并且在随后的步骤 104 中，如上所述，装置 A 使用消息认证码（MAC），以秘密字符串 K 为密钥，从公共密钥 X 计算标记值 t。

在步骤 205 中，如虚线箭头 206 所示，生成的秘密字符串 K 和计算得到的标记值 t 经合适的通信信道传送到装置 C。如参照图 1 标号 105、106 和 107 所述，此通信对应于图 1 中装置 A 与 B 之间上述参数的传送。但在现有实施例中，所述参数在涉及用户交互的装置 A 与 C 之间传送。例如，K 和 t 的值可作为注册过程的一部分从装置 A 发送到装置 C。在一个实施例中，装置 A 的用户可从装置 A 读出秘密字符串和标记值，并将它们传送到装置 C 的用户，例如通过电话、邮件或任何其它合适的方式。在一个实施例中，装置 A 生成包括上述数据的消息，并将它发送到对包括装置 C 和接入点 B 的计算机网络具有权限的网络操作员。在一个实施例中，标识符 ID 与 K 和 t 值一起传送以便有利于随后对它们的检索。

在步骤 207 中，装置 C 接收 K 和 t 的值，在步骤 210 中，将它们存储在存储介质 211 中，例如，存储在用于管理计算机网络保密相关信息的密钥数据库中。如果 K 和 t 的值与标识符 ID 相关，则 K 和 t 值存储时可与该标识符相关，例如，将标识符用作索引。

同样地，在步骤 108 中，装置 A 在装置 A 的存储介质 109 中存储秘密字符串 K，其存储方式可能与标识符 ID 相关。此外，装

置 A 存储秘密值 x，公共密钥 X 的计算基于该值。可选地，装置 A 还可存储公共密钥 X。或者，公共密钥可在以后某个时间从私有密钥 X 重新生成。

至此结束了装置 A 与 C 之间的初始注册过程。在装置 A 和 B 经通信链路实际连接时，执行包括实际密钥交换的以下步骤。如线条 227 所示，这可在上述初始注册后立即进行，或在以后执行。

在步骤 112 中，装置 A 通过经无线通信链路向装置 B 发送公共密钥 X 及可选的附加数据而启动实际的密钥交换。在秘密字符串 K 与标识符 ID 相关的实施例中，装置 A 也发送该标识符。

在从装置 A 接收公共密钥 X（步骤 213）后，装置 B 从存储介质 211 检索秘密字符串 K 和标记值 t（步骤 208 和 209）。在一个实施例中，装置 B 可经计算机网络向装置 C 发送请求，例如，包括接收的标识符 ID。装置 C 响应该请求，从数据库 211 检索标记值和秘密字符串，并将它们发送给装置 B（步骤 208），由装置 B 接收它们（步骤 209）。在另一实施例中，装置 B 可经计算机网络直接访问数据库 211，装置 B 因此可直接从数据库检索参数。秘密字符串 K 和标记值 t 最好可经保密连接 222（例如加密的）和/或经保密计算机网络传送。

在步骤 214 中，装置 B 基于检索的秘密字符串 K 计算接收的公共密钥 X 的 MAC 标记值 t' 。

在步骤 215 中，装置 B 将计算得到的标记值 t' 与检索的标记值 t 进行比较。如果标记值不同，则拒绝接收的公共密钥（步骤 216）。否则，接受公共密钥 X 并且处理过程继续到步骤 217。

在步骤 217 中，装置 B 生成如上所述的秘密值 y 和对应的 Diffie-Hellman 公共密钥 Y。

在步骤 218 中，装置 B 生成对应的 Diffie-Hellman 共享秘密密钥 $S = (X)^y \bmod p$ 。

在步骤 219 中，如结合图 1 所述，装置 B 使用生成的共享秘密

密钥 S 将检索的秘密字符串 K 加密，从而产生加密的秘密字符串 K*。

在步骤 220 中，装置 B 向装置 A 发送加密的秘密字符串 K* 和 Diffie-Hellman 公共密钥 Y。同样地，在一个实施例中，装置 B 还发送对应的标识符 ID。

在步骤 121 中，装置 A 接收加密的秘密字符串 K* 和 Diffie-Hellman 公共密钥 Y。

在步骤 122 中，装置 A 通过使用存储在存储介质 109 中的秘密值 x 生成 Diffie-Hellman 共享秘密密钥 $S = (Y)^x \bmod p$ 。

在步骤 123 中，装置 A 使用生成的共享秘密密钥 S 将接收的加密秘密字符串 K* 解密，以获得对应的解密秘密字符串 K'。

在步骤 124 中，装置 A 将接收的、经过解密的秘密字符串 K' 与装置 A 原来生成并存储在存储介质 109 中的秘密字符串 K 进行比较，如果秘密字符串不相等，则拒绝接收的公共密钥 Y，即丢弃生成的共享秘密密钥 S(步骤 125)。否则，处理过程继续到步骤 126。

在步骤 126 中，接受接收的公共密钥 Y，即，将计算的共享秘密密钥 S 接受为共享秘密。在一个实施例中，将对应的消息发送到装置 B，从而完成密钥交换。生成的共享秘密密钥现在可用于保护装置 A 与 B 之间的后续通信，例如，通过对装置之间发送的消息进行加密和/或完整性保护。

现在参照图 2b，在此示例中，装置 C，即网络服务器等启动密钥交换过程。因此，在此实施例中，与图 2a 的示例相比，装置 A 和包括装置 B 与 C 的系统改变了角色，并且结合图 2a 所述的步骤现在由对应的另一装置执行。在下文中，对应的步骤由与图 2a 中相同的标号标记。具体而言，由装置 C 即网络服务器等执行上述分别生成随机数 x、对应的 Diffie-Hellman 公共密钥 X 和短秘密字符串 K 以及以秘密字符串 K 为密钥从公共密钥 X 计算标记值 t 的初始步骤 103 和 104。

相应地，在步骤 205 和 207 中，如上所述且如虚线箭头 206 所示，将生成的秘密字符串 K 和计算得到的标记值 t 经合适的通信信道从装置 C 传送到装置 A。可以理解，在此实施例中，由网络操作员发起通信。

在步骤 210 中，装置 A 在装置 A 的存储介质 109 中存储接收的数据。

同样地，在步骤 108 中，装置 C 将秘密字符串 K 和秘密值 x 存储在存储介质 211 中，例如，存储在用于管理计算机网络保密相关信息的密钥数据库。可以理解，同样在此实施例中，如结合图 2a 所述，秘密字符串 K 及由此的相关值 x、X 和 t 可与标识符 ID 相关。

至此结束了装置 A 与 C 之间的初始注册过程。在装置 A 和 B 经通信链路实际连接时，执行包括实际密钥交换的以下步骤。如线条 227 所示，这可在上述初始注册后立即进行，或在以后执行。同样地，在此实施例中，由装置 B 而非装置 A 启动密钥交换。

因此，装置 B 从存储介质 211 检索秘密字符串 K 和 Diffie-Hellman 密钥 x 与 X（步骤 228 和 229）。如上所述，这可通过直接数据库查询完成，通过经由（保密的）计算机网络发送到装置 C 的请求（例如包括接收的标识符 ID）完成，或诸如此类。

在步骤 112 中，装置 B 通过经无线通信链路向装置 A 发送公共密钥 X 及可选的附加数据来启动实际的密钥交换。

在步骤 213 中，装置 A 接收密钥 x，并且在步骤 214 中，装置 B 基于存储在装置 A 上的秘密字符串 K 计算接收的公共密钥 X 的 MAC 标记值 t'。

在步骤 215 中，装置 A 将计算得到的标记值 t' 与以前存储的标记值 t 进行比较。如果标记值不相等，则拒绝接收的公共密钥（步骤 216）。否则，接受公共密钥 X 并且处理过程继续到步骤 217。

在步骤 217 中，装置 A 如上所述生成秘密值 y 和对应的 Diffie-Hellman 公共密钥 Y。

在步骤 218 中，装置 A 生成对应的 Diffie-Hellman 共享秘密密钥 $S = (X)^y \bmod p$ 。

在步骤 219 中，如结合图 1 所述，装置 A 使用生成的共享秘密密钥 S 将秘密字符串 K 加密，产生加密的秘密字符串 K^* 。

在步骤 220 中，装置 A 向装置 A 发送加密的秘密字符串 K^* 和 Diffie-Hellman 公共密钥 Y。

在步骤 121 中，装置 B 接收加密的秘密字符串 K^* 和 Diffie-Hellman 公共密钥 Y。

在步骤 122 中，装置 B 通过使用从存储介质 211 检索的秘密值 x 生成 Diffie-Hellman 共享秘密密钥 $S = (Y)^x \bmod p$ 。

在步骤 123 中，装置 B 使用生成的共享秘密密钥 S 将接收的加密秘密字符串 K^* 解密，以获得对应的解密秘密字符串 K' 。

在步骤 124 中，装置 B 将接收的、经过解密的秘密字符串 K' 与装置 C 原来生成并从存储介质 211 检索的秘密字符串 K 进行比较，如果秘密字符串不相等，则拒绝接收的公共密钥 Y，即丢弃生成的共享秘密密钥 S（步骤 125）。否则，处理过程继续到步骤 126。

在步骤 126 中，接受接收的公共密钥 Y，即，将计算的共享秘密密钥 S 接受为共享秘密。在一个实施例中，将对应的消息发送到装置 A，从而完成密钥交换。生成的共享秘密密钥现在可用于保护装置 A 与 B 之间的后续通信，例如，通过对装置之间发送的消息进行加密和/或完整性保护。

可以理解，在一些实施例中，步骤 122、123、124 和 126 可以代之以由装置 C 来执行，从而避免了在装置 B 和 C 二者中均实际实施密钥交换算法的需要。在这种情况下，装置 B 只是简单地将从装置 A 接收到的密钥数据转发给装置 C，例如通过保密的计算机网络进行，其中要对密钥数据进行认证，进而如上所述加以处理。

因此，概而言之，上述示例公开了在第一通信单元与第二通信单元之间的一种密钥交换方法。所述方法包括注册阶段和密钥交换

阶段。所述注册阶段包括：

- 由所述第一通信单元生成密钥交换机制的第一私有密钥值和对应的第一公共密钥，所述密钥交换机制最好是Diffie-Hellman 密钥协商机制；
- 由所述第一通信单元生成口令码；
- 由所述第一单元使用所述口令码，根据消息认证码计算所述第一公共密钥的消息标记；以及
- 使所述口令码和所述计算得到的标记值可由所述第二通信单元访问。

实际的密钥交换阶段可在以后两个单元经通信链路连接并可经该通信链路交换消息的任一时间执行。此阶段包括：

- 由所述第一通信单元将所述第一公共密钥发送到所述第二通信单元；
- 由所述第二通信单元使用所述口令码，根据所述消息认证码计算所述接收的第一公共密钥的标记值，并在所述计算得到的标记值与所述第二通信单元可访问的所述标记值一致时，接受所述接收的第一公共密钥；
- 由所述第二通信单元生成所述密钥交换机制的第二私有密钥值和对应的第二公共密钥；
- 由所述第二通信单元从所述第一公共密钥和所述第二私有密钥值计算所述密钥交换机制的共享秘密密钥；
- 由所述第二通信单元使用所述计算得到的共享秘密密钥对所述口令码加密；
- 由所述第二通信单元将所述第二公共密钥和所述加密的数据项发送到所述第一通信单元；
- 由所述第一通信单元从所述第二公共密钥和所述第一私有密钥值计算所述密钥交换机制的所述共享秘密密钥；以及

- 由所述第一通信单元使用所述第一通信单元计算的所述共享秘密密钥将所述发送的加密数据项解密，并在所述解密的数据项与所述第一通信单元原来生成的所述口令码一致时接受所述计算得到的共享秘密密钥。

图 3 显示了基于纠错码计算消息认证码的方法的流程图。在图 3 的示例中，假定数据空间 D 的数据项 d 要使用消息认证码 (MAC) 进行认证。数据项 d 可以是例如上述方法中的消息，例如公共密钥 X，或通过合适的函数 h 从消息 M 导出的数据项，即， $d=h(M)$ ，这将在下面作更详细的讨论。为本示例的目的，数据项 d 也将称为消息。

通常，MAC 是从数据空间 D 和密钥空间 K 到标记空间 C 的映射 f ，即， $f: D \times K \rightarrow C$ ，其中，消息 $d \in D$ 和密钥 $k \in K$ 映射到标记 $t \in C$ ，即， $(d, k) \rightarrow t$ 。

MAC 用于保护消息的完整性，即，确保数据在从发送方到接收方的传输期间未被更改。在人工认证中，使用短的 MAC 值，即，长度少于 10-15 个数字和/或字符和/或其它符号的标记，从而使用户可传送和/或比较标记值。在此类人工认证方案中，保密性基于 MAC 函数的无条件保密性，而不是基于计算保密性。例如，如果将长散列码的散列函数用作 MAC 函数，则保密性基于计算保密性。

MAC 函数的无条件保密性可通过考虑不同类型的可能攻击而确定。一般考虑的两种主要攻击类型是冒名攻击和替代攻击。为便于理解以下说明，在此对这些类型的攻击作简要描述。更详细的说明可参考例如 G. Kabatianaskii、B. Smeets 和 T Johansson 所著的“关于基于纠错码的系统 A 码的基数” (“On the cardinality of systematic A-codes Via error correcting codes”， IEEE Transaction on Information theory， vol. IT-42， pp. 566-578， 1996），该文通过引用全部结合于本文中。

在冒名攻击中，攻击者尝试使接收方不观察合法发送方与接收方之间的任何现有数据交换而相信一些数据是从合法发送方发送的。另一方面，在替代攻击中，攻击者先观测某一数据 d ，随后将观测的数据替换为某个其它数据 $d' \neq d$ 。攻击者在冒名攻击和替代攻击中成功的概率分别表示为 P_I 和 P_S ，并且它们可表示如下

$$P_I = \max_{c \in C} P(c \text{ 是有效的}),$$

$$P_S = \max_{\substack{c, c' \in C \\ c \neq c'}} P(c' \text{ 是有效的} | c \text{ 是观测的}).$$

在上述密钥交换协议的场景中，攻击者将观测数据 d 替换为某一其它数据 d' 的概率是密钥交换方法的保密性的相关量度，即，将图 1 和图 2a 示例中从单元 A 发送到单元 B 以及图 2b 中从单元 B 发送到单元 A 的公共密钥替换为另一公共密钥的概率。在这种情形中，如果接收方将 d' 作为有效数据接受，则攻击者成功。在诸如蓝牙等短距离无线通信情况中，两个单元物理上彼此接近，并且两个单元在已发信号表示它们准备就绪时可能局限于仅接受数据。因此，如在此类情况下，可轻松避免冒名攻击，替代攻击的概率可视为保密性的更相关量度。此外，在图 1 和图 2 的情况下，由 MAC 函数计算得到的标记值通过不同于发送数据的通信链路的单独通信链路传送。这与标准 MAC 方案不同，在标准 MAC 方案中，数据和标记值均被发送并可能被攻击者观测到。利用这些假设，成功的替代攻击概率可表示为

$$P_S = \max_{\substack{d, d' \in D \\ d \neq d'}} P(f(d, k) = f(d', k) | d \text{ 是观察的}).$$

因此，假设密钥始终从密钥空间 K 中随机选择，则上述概率可表示为

$$P_S = \max_{\substack{d, d' \in D \\ d \neq d'}} \frac{|\{k \in K : f(d, k) = f(d', k)\}|}{|K|},$$

其中， $|\cdot|$ 是集合的基数，即 $|K|$ 是 K 的基数，并且上述等式中的

分子是对 d 和 d' 两者均产生相同 MAC 函数值的密钥空间 K 中所有密钥集的基数。因此，由上述等式可得出如下结论：为提供高保密性，则 MAC 函数 f 的冲突概率应该为低。

下面的 MAC 构造示例基于纠错码。为便于理解此说明，将考虑有限域 F_q 上的纠错码。具体而言，考虑 F_q 上码字长度为 n 的 q 进制码并将其表示为 V 。一般而言，编码是从消息到码字的映射，使得每个消息对应于唯一一个码字，并且每个码字包括多个符号。因此，代码 V 由所有矢量 $v \in V = \{v^{(d)} : d \in D\}$ 组成，其中， $v^{(d)} = (v_1^{(d)}, v_2^{(d)}, \dots, v_n^{(d)})$ ，即， $v_i^{(d)} \in F_q$ 是码字 $v^{(d)}$ 的码元。

两个 q 进制的 n 元组 x 与 y 之间的汉明距离 $d_H(x, y)$ 是不相同的 n 元组分量的数量，即， $d_H(x, y) = |\{i \in \{1, \dots, n\} : x_i \neq y_i\}|$ 。码 V 的最小距离为

$$d_H(V) = \min_{\substack{x, y \in V \\ x \neq y}} d_H(x, y),$$

即，码 V 的所有码字之间的最小距离。

下面将参照图 3 描述基于纠错码的 MAC 构造的示例。

在初始步骤 301 中，提供 MAC 构造的输入数据，即，要认证的消息 d 和要作为 MAC 函数输入的密钥 k 。

在步骤 302 中，选择索引 $i \in \{1, \dots, n\}$ 作为密钥 k 的函数 g ，即， $i = g(k)$ 。具体而言，如果密钥空间 K 具有 n 个元素，即， $|K| = n$ ，则每个 k 可唯一地映射到码元索引之一，并且每个索引对应于一个密钥。在一个实施例中，将密钥直接用作索引，即 $i = k$ 。

在步骤 303 中，将标记值 t 确定为与消息 d 对应的码 V 的码字 $v^{(d)}$ 的第 i 个码元，即，

$$t = f(d, k) = v_i^{(d)} = v_{g(k)}^{(d)}.$$

因此，标记值被确定为纠错码码字的一个选定码元，其中，该码字是与消息对应的码字，并且码元由密钥指定。所以，在上述示例中，得到一种 MAC，其中密钥空间大小等于 n ，而消息空间大小

等于编码空间大小。此外，替代攻击的上述概率 P_s 如下给出：

$$P_s = 1 - d_H(V)/n.$$

图 4a-b 显示了基于里德-所罗门码计算消息认证码的方法示例的流程图。

术语里德-所罗门 (RS) 码指这样一类纠错码，其中，通过与生成多项式的多项式除法定义码字；参见 I.S. Reed 和 G. Solomon 所著的“某些有限域上的多项式码”(“Polynomial Codes over Certain Finite Fields”, journal of Soc. Ind. Appl. Math., vol. 8, pp. 300-304, 1960)，该文通过引用全部结合于本文中。术语“里德-所罗门码”还将包括里德-所罗门码的变体，例如，所谓的广义里德-所罗门码。

在图 4a 的结构中，在初始步骤 401 中向 MAC 构造提供输入数据，即，要认证的消息 d 和用作 MAC 函数输入的密钥 k 。

在步骤 402 中，将消息表示为 F_q 上的 q 进制 τ 元组，即， $d=d_0, d_1, \dots, d_{\tau-1}$ ，其中， $d_i \in F_q$ 。因此，对应于消息的里德-所罗门 (RS) 编码多项式定义为

$$p^{(d)}x = d_0 + d_1x + d_2x^2 + \dots + d_{\tau-1}x^{\tau-1}.$$

在步骤 403 中，通过在密钥 k 指定的点求多项式值来计算 MAC 的标记值，即：

$$t = f(d, k) = v_k^{(d)} = p^{(d)}(k) = d_0 + d_1k + d_2k^2 + \dots + d_{\tau-1}k^{\tau-1}.$$

因此，密钥 k 指定了用作标记值的里德-所罗门码码元。可以理解，如上所述，码元可由密钥的任一合适函数指定。

还要注意的是，在此构造中，密钥是从有限域 F_q 中选择的，即 $k \in F_q$ 。因此，此构造具有以下属性： $n=q=|K|$ ，并且 $|D|=q^\tau=n^\tau$ 。因此，上述码的最小距离为 $d_H(V)=n-\tau+1$ ，因此成功替代攻击概率为 $P_s = (\tau-1)/n$ 。里德-所罗门码的优点就在于：它们是最小距离极大的长码。

上述内容还表示概率 P_s 随消息空间 D 的大小提高。

图 4b 显示了基于里德-所罗门码的 MAC 构造的另一实施例的流程图。

同样地，根据此构造，在初始步骤 404 中，提供 MAC 构造的输入数据，即，要认证的消息 d 和用作 MAC 函数输入的密钥 k。

在步骤 405 中，将单向散列函数 h 应用于消息。为便于理解此描述，术语“单向散列函数”指以数据项如字符串为输入，并产生固定长度的二进制值（散列）作为输出的算法。具体而言，此过程是不可逆的，即，找出产生给定散列值的数据项在计算上将是不可行的。同样地，找出产生相同散列值的两个任意数据项在计算上也将是不可行的。合适的散列函数的一个示例是标准保密散列算法 SHA-1。SHA-1 算法采用长度小于 264 比特的消息，并且产生 160 比特的消息摘要。单向散列函数的其它示例包括 MD4、MD5 等。散列函数 $\delta=h(d)$ 的输出随后用作里德-所罗门码的输入。在一个实施例中，将散列函数的输出截短，以便进一步使有效消息大小减小。

因此，在步骤 406 中，将散列值 δ 表示为 F_q 上的 q 进制 τ 元组，即， $\delta=\delta_0, \delta_1, \dots, \delta_{\tau-1}$ ，其中， $\delta_i \in F_q$ 。

在步骤 407 中，通过通过在密钥 k 指定的点求对应里德-所罗门编码多项式的值来计算 MAC 的标记值 t，即

$$t=f(\delta, k)=v_k^{(\delta)}=p^{(\delta)}(k)=\delta_0+\delta_1 k+\delta_2 k^2+\dots+\delta_{\tau-1} k^{\tau-1}.$$

因此，通过先将象 SHA-1 的单向散列函数应用于消息，减少消息空间的大小，从而降低成功替代攻击的概率 P_s ，而无需显著增加密钥长度或 MAC 输出的长度，即，标记的长度。所以，甚至对于短的密钥和短的消息标记，也可提供保密的认证，从而允许通过用户交互传送密钥和消息标记。

图 5 显示了说明对应于图 4a-b 的 MAC 构造的多个构造示例的成功替代攻击概率的表格。标记为 $\log_2|D|$ 的第一列包括以比特数表示的消息大小；标记为 $\log_2(n)$ 的第二列以比特数表示的密钥大小，

而最后一列显示了成功替代攻击的对应概率。例如，代码长度为 4 个十六进制数字和密钥大小为 4 个数字 ($n=q=16^4$, 即, $\log_2(n)=16$) 的码对 128 比特长的消息产生大约 2^{-13} 到 2^{-16} 的伪造概率。因此，截短成 128 比特并且密钥大小和代码大小为 4 个十六进制比特的 SHA-1 输出可产生足够高的保密性。如果密钥大小增加到 5 个数字 ($\log_2(n)=20$)，则概率进一步降低为大约 2^{-17} 或更小。

图 6 显示了包括通常标记为 A 和 B 的两个通信单元的通信系统的方框图。通信单元 A 和通信单元 B 经通信链路 605 彼此进行通信。

通信单元 A 包括处理单元 602、连接到处理单元的无线电通信单元 603、连接到处理器的存储介质 604 以及连接到处理的用户接口 606。

无线电通信单元 603 将通过无线电链路 605 从处理单元 602 接收的数据发送到通信单元 607，并且它从无线电链路接收数据，并将其转发到处理单元。例如，无线电通信单元 603 可基于蓝牙技术，并在 2.45 GHz 的 ISM 频带发送/接收。

处理单元 602，例如适当编程的微处理器，根据通信单元 A 实现的功能处理从其它单元接收的数据和要发送到其它单元的数据。具体而言，处理单元 602 经适当编程为执行上述保密功能，具体指以上所述的口令码和对应标记值生成、密钥交换和认证方法。

存储介质 604 如 EPROM、EEPROM、闪存等适于存储口令码 K 及密钥交换协议所必需的参数。

用户接口 606 包括用于显示生成的口令码 K 和对应标记值 t 的显示器，以便用户可读出所生成的值，并将它们传送给通信单元 B。

另外，用户接口 606 可包括数据输入部件，如键盘、小键盘、指示装置、触摸屏或诸如此类。

通信单元 B 包括处理单元 609、连接到处理单元的无线电通信单元 608、连接到处理单元的存储介质 610 及连接到处理单元的用

户接口 611。

无线电通信单元 609 对应于通信单元 A 的无线电通信单元 603，从而允许在无线电通信单元 A 与 B 之间进行无线电通信。

处理单元 609 根据通信单元实现的功能处理从其它单元接收的数据和要发送到其它单元的数据。具体而言，处理单元适当编程为执行上述保密功能，具体指如上所述并对应于单元 A 实现的密钥交换协议和认证机制的密钥交换和认证方法。

同样地，存储介质 604 如 EPROM、EEPROM、闪存等适于存储口令码 K、标记值 t 及密钥交换协议所必需的参数。

用户接口 611 包括输入装置，如小键盘、键盘、触摸屏或诸如此类，从而允许用户输入通信单元 A 生成的口令码 K 和对应的标记值 t。另外，用户接口可包括显示器、指示装置和/或诸如此类。

因此，图 6 的通信系统包括两个通信单元，例如两个便携式通信装置，如两个移动电话、一个移动电话和一台便携式计算机、两台便携式计算机，或类似电子设备的任意组合，这两个通信单元通过根据上述方法建立共享秘密密钥，经通信链路 605 建立保密通信。

在一个实施例中，处理单元和/或存储介质可以可拆装方式插入对应的通信单元中，从而允许要建立的保密关联独立于实际的单元。例如，存储介质和/或处理单元可由智能卡如 SIM 卡构成。

还要注意的是，通信单元还可包括在图 6 的示意框图中省略的组件。例如，通信单元还可包括连接到接收器的自动增益控制 (AGC) 单元、解码器、编码器或诸如此类。

图 7 显示了经计算机网络的接入点与计算机网络进行通信的便携式通信单元的方框图。

通信单元 A 对应于结合图 6 所述的通信单元 A。通信单元 A 包括处理单元 602、连接到处理单元的无线电通信单元 603、连接到处理单元的存储介质 604 及连接到处理单元的用户接口 606。这些组件已在上面作过更详细的描述。

通信单元 A 经无线通信链路 605 与通信网络 701 的接入点 702 进行通信。例如，通信网络 701 可以是无线 LAN、经一个或多个接入点提供无线接入的有线 LAN 或诸如此类。在图 7 中，其它网络组件分别由两个网络节点 703、704 例示。在图 7 的示例中，网络节点 703 是一个网络服务器计算机，其容纳与可经无线链路接入计算机网络 701 的多个单元的口令码和标记值的密钥数据库 705。因此，当单元 A 希望根据结合图 2a-b 所述的过程向计算机网络注册时，网络服务器 703 可充当该过程中装置 C 的角色。例如，根据图 2b 的实施例，在网络服务器 703 已生成口令密钥 K 和标记值 t 时，可将这些值发送到单元 A。例如，传送操作可由操作员作为初始化过程的一部分，通过经电话将数据传送给用户单元 A 的用户，通过发送电子邮件或诸如此类来引起。此外，数据存储在数据库 705 中。在单元 A 与接入点 B 建立连接时，在图 2b 的保密密钥交换过程中会检索和使用存储的参数。

在替代实施例中，接入点 B 包括或可访问密钥数据库，并且注册过程如结合图 1 所述，在单元 A 与接入点 B 之间直接执行。

应强调的是，术语“包括/包含”在此说明中使用时要理解为指明存在所述的功能、整数、步骤或组件，而未排除存在或添加一个或多个其它功能、整数、步骤、组件或它们的组合。

虽然已描述和显示了本发明的优选实施例，但本发明并不限于这些实施例，而是还可以所附权利要求书限定的主题范围内以其它方式体现。

本发明可通过包括几个不同单元的硬件实施，以及通过适当编程的计算机实施。在列举了几个部件的装置权利要求中，这些部件中的几个部件可体现为硬件的同一项，例如，如本文所述的适当编程的微处理器或计算机、一个或多个用户接口和/或一个或多个通信接口。互不相同的从属权利要求中记载了某些措施这一纯粹事实并不表示不能利用这些措施的组合。

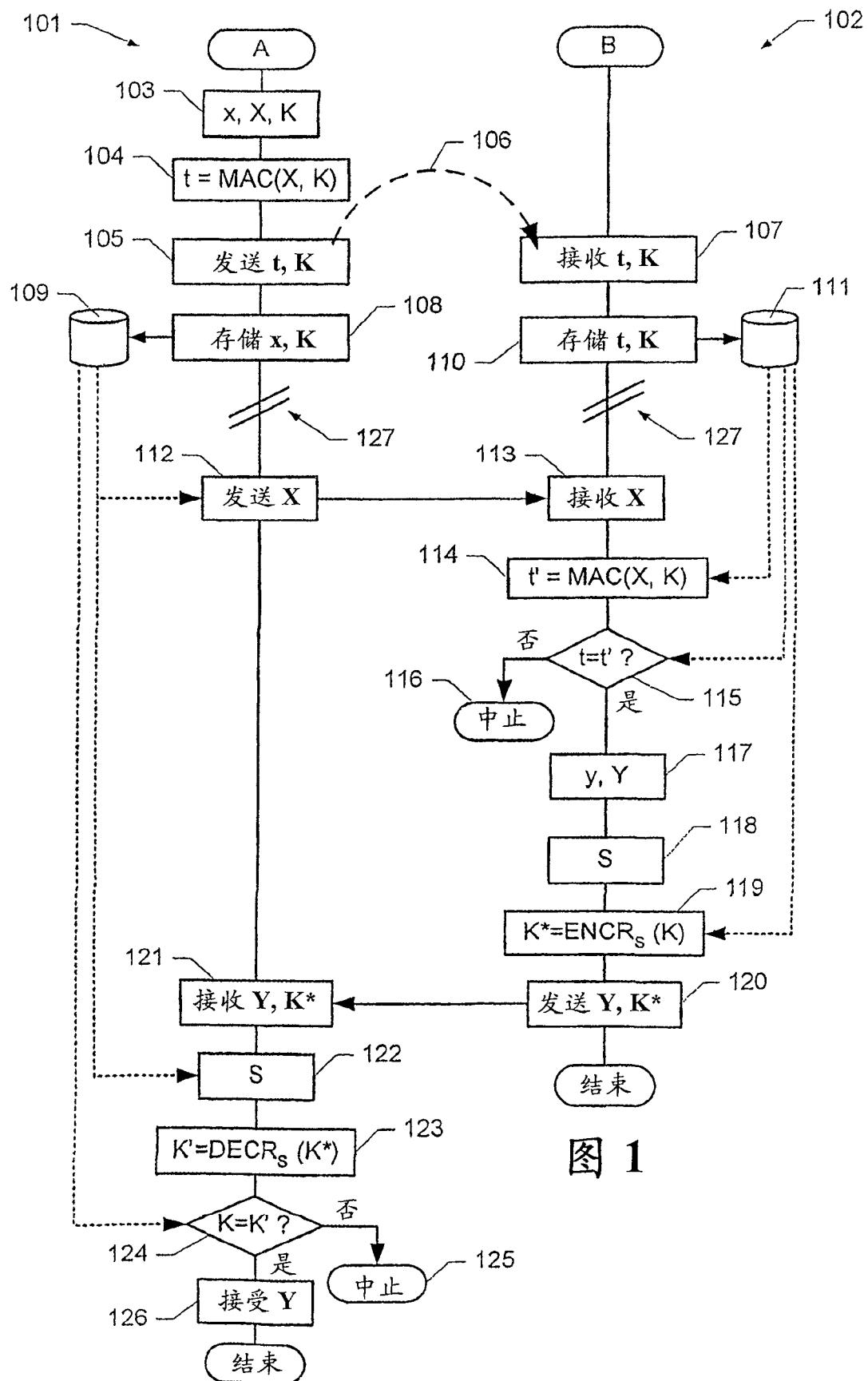


图 1

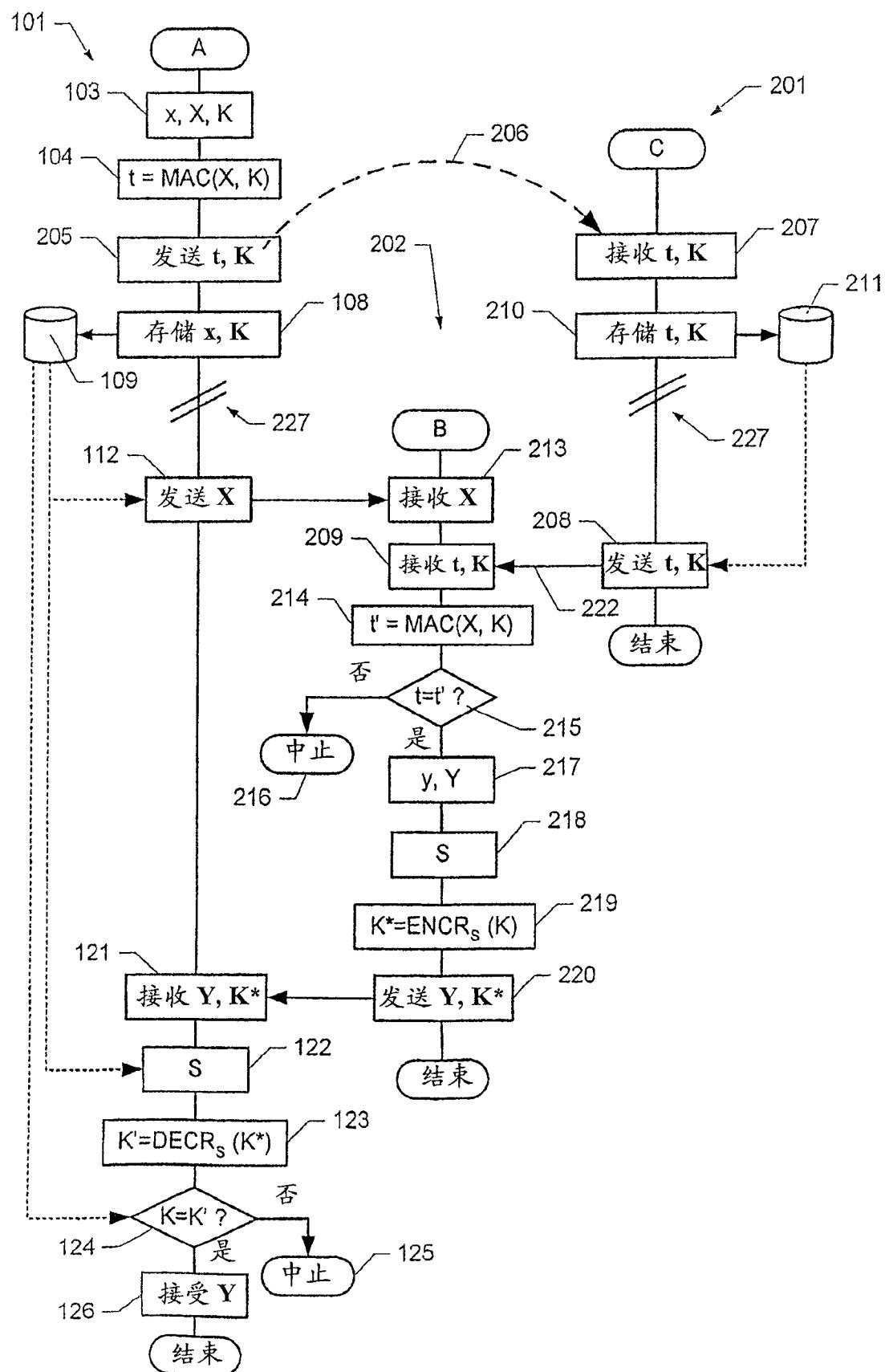


图 2a

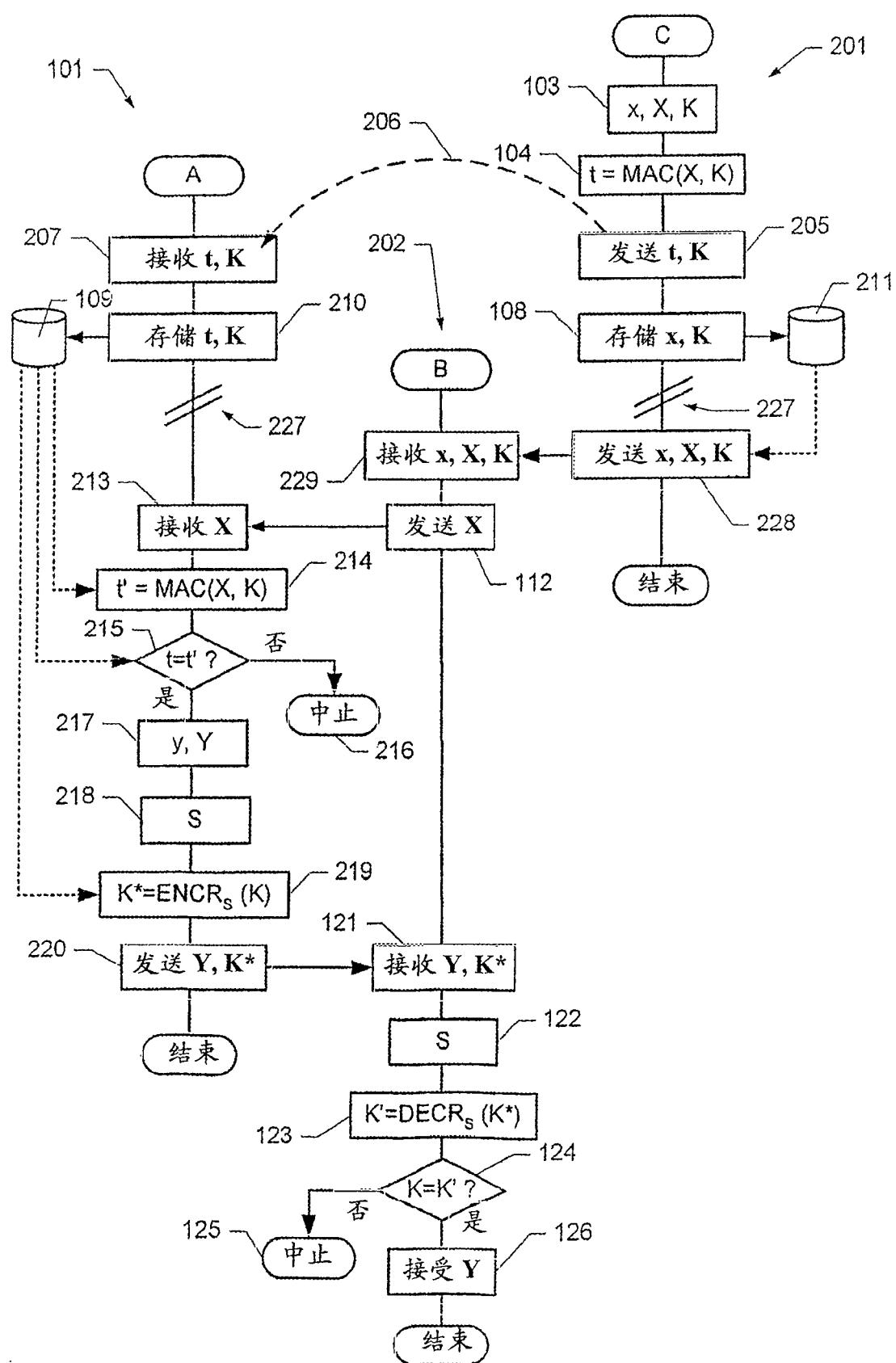


图 2b

图 3

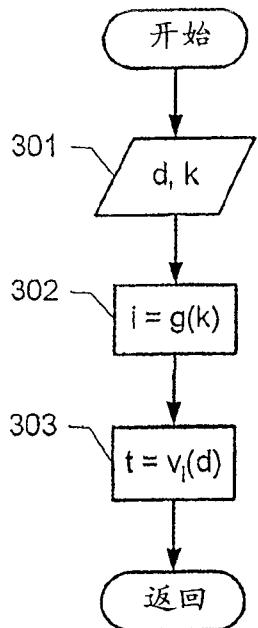
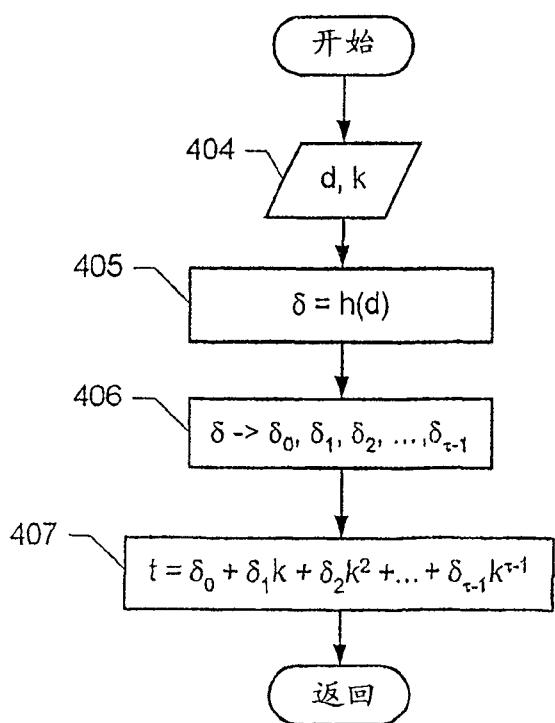
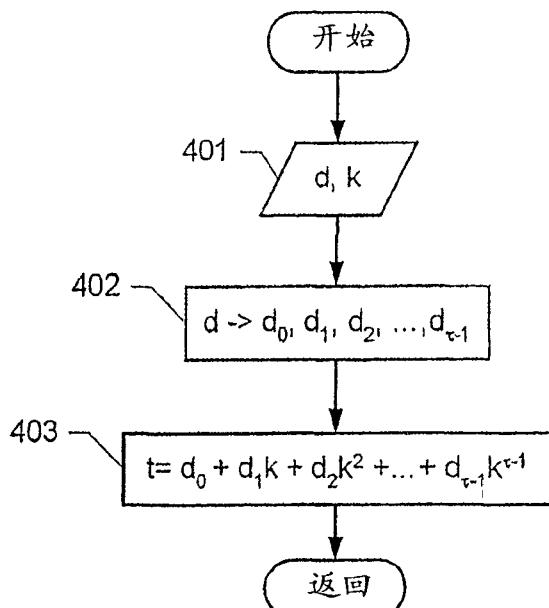


图 4a



$\log_2 D $	$\log_2(n)$	P_s
128	16	$2^{-13} - 2^{-16}$
256	16	$2^{-12} - 2^{-16}$
128	20	$2^{-17} - 2^{-20}$
256	20	$2^{-16} - 2^{-20}$

图 5

图 4b

图 6

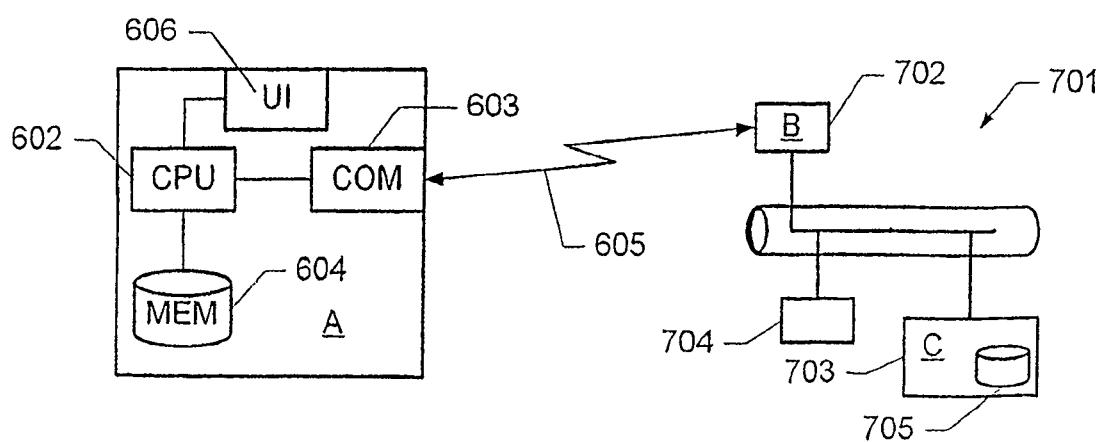
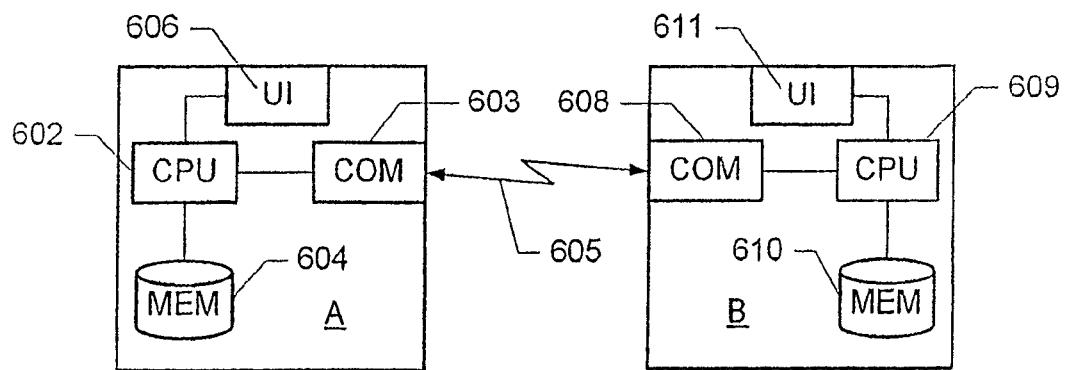


图 7