

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/12 (2006.01)



[12] 发明专利申请公开说明书

[21] 申请号 200480026338.9

[43] 公开日 2006 年 10 月 18 日

[11] 公开号 CN 1849774A

[22] 申请日 2004.9.13

[74] 专利代理机构 北京科龙寰宇知识产权代理有限公司
代理人 孙皓晨

[21] 申请号 200480026338.9

[30] 优先权

[32] 2003. 9. 12 [33] SE [31] 0302456 - 9

[32] 2003. 9. 12 [33] US [31] 60/502,254

[32] 2004. 2. 4 [33] SE [31] 0400238 - 2

[86] 国际申请 PCT/SE2004/001314 2004.9.13

[87] 国际公布 WO2005/027404 英 2005.3.24

[85] 进入国家阶段日期 2006.3.13

[71] 申请人 安全电子邮件哥德堡公司

地址 瑞典斯卡拉

[72] 发明人 彼得·达文

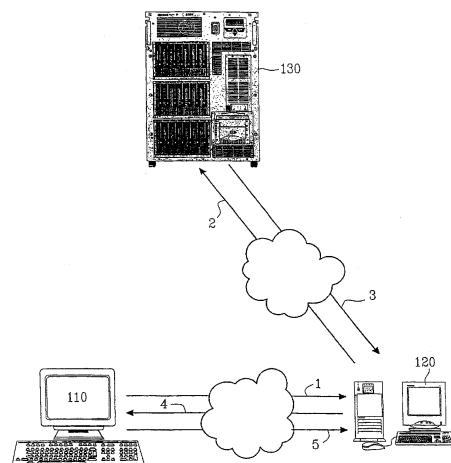
权利要求书 5 页 说明书 13 页 附图 3 页

[54] 发明名称

信息安全性

[57] 摘要

本发明涉及一种传送电子信息的方法，优选从第一个终端的第一个用户传送电子邮件到第二个终端的第二个用户，包括下列步骤：所述的第一个终端以加密形式传送所述电子邮件，所述加密的电子邮件是通过第一个密钥生成器用一个种子生成的密钥进行加密的，向所述第二个用户一次性提供所述种子，以便让所述第二个终端提供的第二个密钥生成器生成密钥，将所述的种子提供给所述的第二个终端并将所述的种子存储在所述的第二个终端中，当每次所述的第二个用户收到从所述的第一个用户发送的加密电子邮件时，所述的第二个终端利用所述的种子生成一个密钥，同步各个终端的计数值；根据所述的种子和各个终端的计数值生成所述的密钥，与其它终端无关。



1. 一种传送电子信息的方法，优选从第一个终端的第一个用户传送电子邮件到第二个终端的第二个用户，包括下列步骤：

- 所述的第一个终端以加密的形式传送所述的电子邮件，所述加密的电子邮件是通过第一个密钥生成器用一个种子生成的密钥进行加密的，
- 向所述第二个用户一次性提供所述的种子，以便用所述第二个终端提供的第二个密钥生成器生成密钥，
- 将所述的种子提供给所述的第二个终端并将所述的种子在所述的第二个终端中存储，
- 当每次所述第二个用户收到从所述第一个用户发送的加密电子邮件时，所述第二个终端利用所述的种子生成一个密钥，
- 同步各个终端的计数值；以及
- 根据所述的种子和各个终端的计数值生成所述的密钥，与其它终端无关。

2. 根据权利要求 1 的方法，其中所述的种子仅在第一次初始化时间获得。

3. 根据权利要求 1 的方法，其中如果所述的第一个种子不能用了，获得第二个种子。

4. 根据权利要求 1 的方法，其中每封加密的电子邮件获得一个动态序列号。

5. 根据权利要求 4 的方法，其中所述的动态序列号用于为相应的加密电子邮件生成密钥。

6. 根据权利要求 5 的方法，其中种予以动态的和可交换的方式至少在一个终端中保存，优选在所有的终端中保存。

7. 根据权利要求 1 或 6 的方法，其中所述的计数值在每个终端的计数器中生成，计数值的同步与计数器的同步有关。

8. 根据权利要求 1-7 中任何一个的方法，其中在计数器初始同步化之后，仅在需要时终端执行补充的同步化步骤。

9. 根据权利要求 1-8 中任何一个所述的方法，其中基于种子和计数值的所述密钥-生成操作是通过以非动态和不可改变方式存储于至少一个终端中的算法来实现的。

10. 根据权利要求 1 的方法，包括步骤：根据收到的种子生成一个委托的终端列

表。

11. 根据权利要求 10 的方法，包括只接收来自所述列表中注册的电子邮件。
12. 根据前述权利要求中任何一个的方法，包括所述的第一个用户通过电话、传真或书信至少一种方式提供给所述第二个用户所述的种子。
13. 根据前述权利要求中任何一个的方法，其中所述加密的电子邮件的附件与电子邮件一起被加密。
14. 根据前述权利要求中任何一个的方法，其中发送方提供一个带有设置参数的信息，设置的参数迫使收件方执行特定的操作。
15. 根据前述权利要求中任何一个的方法，其中给网络管理员提供管理员密码，该密码能让管理员读取信息并管理账户。
16. 根据权利要求 15 的方法，其中给管理员提供硬件单元生成唯一的序列号，该序列号起验证身份的目的。
17. 一种传送电子信息的系统，优选从第一个终端的第一个用户传送电子邮件到第二个终端的第二个用户，该系统进一步包括：
 - 所述第一个终端以加密邮件形式传送所述安全的电子邮件的方法，所述加密的电子邮件是通过第一个密钥生成器用一个种子生成的密钥进行加密的，
 - 向所述的第二个用户一次性提供所述的种子以便让第二个密钥生成器生成密钥的方法，
 - 将所述的种子提供给所述的第二个终端的方法并将所述的种子在所述的第二个终端中存储的方法，
 - 当每次所述的第二个用户收到从所述的第一个用户发送的加密电子邮件时，所述第二个终端利用所述的种子生成密钥的方法；
 - 每个终端包括一个密钥-生成单元，所述的密钥-生成单元包括存储器，相同的种子存储在存储器中；计数器，周期改变计数值；计算终端，适合在各个终端并与其它终端无关根据原始值和由计数器发出的计数值生成密钥；以及
 - 终端被设置为能感应到它们不同步的时候，然后重新设置为同步。
18. 根据权利要求 17 的系统，其中在至少一个终端存储种子的所述存储器是动

态存储器，以动态的和可交换的方式存储种子。

19. 根据权利要求 17 至 18 中任何一个的系统，其中至少一个终端的计算单元包括算法，该算法以非动态的和不能改变的方式存储，并优选为用硬件实现。

20. 根据权利要求 17 至 19 中任何一个的系统，其中终端之一是中央终端，它包含多个种子用于安全的加密传送，这些种子与若干个不同的终端有关，每个终端具有一个原始值。

21. 根据权利要求 17 至 20 中任何一个的系统，包括第一个单元用于生成唯一的序列号，第一个单元控制位于系统中的第二个单元，第二个单元生成序列号，如果它是正确的单元并且它们相互同步，那么该序列号与第一个单元生成的序列号相同。

22. 一种用于从第一个终端的第一个用户传送安全的电子邮件到第二个终端的第二个用户的计算机程序产品，包括代码用于：

- 加密并传送从所述第一个终端发送的所述电子邮件，
- 用所述的第一个种子在所述的第一个终端生成密钥，
- 获得所述的种子，以便在所述的第二个终端用第二个密钥生成器生成密钥，
- 将所述的种子在所述的第二个终端中存储，
- 当每次所述的第二个用户收到从所述的第一个用户发送的加密电子邮件时，所述的第二个终端利用所述存储的种子生成一个密钥；
- 每封加密的电子邮件获得一个动态序列号；
- 用所述的动态序列号为相应的加密电子邮件生成密钥；
- 同步各个终端的计数值；以及
- 根据所述的种子和各个终端的计数值生成所述的密钥，与其它终端无关。

23. 一种用于从第一个终端的第一个用户传送安全的电子邮件到第二个终端的第二个用户的传送信号，包括含有代码的信号，其中代码用于：

- 加密并传送从所述第一个终端发送的所述电子邮件，
- 在所述的第一个终端用所述的第一个种子生成密钥，
- 获得所述的种子，以便在所述的第二个终端用第二个密钥生成器生成密钥，
- 将所述的种子在所述的第二个终端中存储，
- 当每次所述第二个用户收到从所述第一个用户发送的加密电子邮件时，所

-
- 述的第二个终端利用所述存储的种子生成一个密钥，
 - 每封加密的电子邮件获得一个动态序列号；
 - 用所述的动态序列号为相应的加密电子邮件生成密钥；
 - 同步各个终端的计数值；以及
 - 根据所述的种子和各个终端的计数值生成所述的密钥，与其它终端无关。

24. 一种计算机可读介质，具有存储于其中的指令集，用于从第一个终端的第一个用户传送安全的电子邮件到第二个终端的第二个用户，所述的指令集包括代码用于：

- 加密并传送从所述第一个终端发送的所述电子邮件，
- 用所述的第一个种子在所述的第一个终端生成密钥，
- 获得所述的种子，以便在所述的第二个终端用第二个密钥生成器生成密钥，
- 将所述的种子在所述的第二个终端中存储，
- 当每次所述第二个用户收到从所述的第一个用户发送的加密电子邮件时，所述的第二个终端利用所述存储的种子生成一个密钥，
- 每封加密的电子邮件获得一个动态序列号；
- 用所述的动态序列号为相应的加密电子邮件生成密钥；
- 同步各个终端的计数值；以及
- 根据所述的种子和各个终端的计数值生成所述的密钥，与其它终端无关。

25. 根据权利要求 24 的介质，其中所述的介质是存储器单元。

26. 一种指令集的销售方法，该指令集用于传送并接收电子信息，尤其是用于从第一个终端的第一个用户发送到第二个终端的第二个用户的安全电子邮件，该方法包括：

- 所述的第一个终端以加密的方式传送所述安全的电子邮件，所述加密的电子邮件通过第一个密钥生成器用一个种子生成的密钥进行加密的，
- 给所述安全的电子邮件提供指明销售方地址的可读取信息，
- 从所述的销售方地址获得第二个指令集，用于解密所述的电子邮件，以及
- 把所述的第二个用户记为借方，由于他使用了所述的第二个指令集来加密新的电子邮件。

27. 根据权利要求 26 的方法，其中该方法是计算机化的。

-
28. 根据权利要求 26 的方法，其中所述的账单是根据定购和接收所述第二个指令集开具的。
 29. 根据权利要求 26 的方法，其中所述的第二个指令集是预先安装的指令集的进入密码。
 30. 一种过滤接收器上的电子邮件的方法，所述的电子邮件从第一个终端的第一个用户到达第二个终端的第二个用户的接收器上，所述的第一个终端以加密形式传送所述的电子邮件，所述加密的电子邮件是通过第一个密钥生成器用一个种子生成的密钥进行加密的，向所述第二个用户一次性提供所述的种子，以便用所述第二个终端提供的第二个密钥生成器生成密钥，所述第二个终端根据由所述种子产生的发件人-收件人关系，生成一份受信任的发件人列表，并根据所述列表进行接收电子邮件的操作。
 31. 根据权利要求 30 的方法，其中所述的操作是存储、删除或退回所述电子邮件中的一种。

信息安全性

技术领域

本发明涉及一种安全加密传送信息的方法以及系统，尤其是用于传送电子邮件和用于通信网络。

背景技术

随着互联网及其它网络的使用不断增加，通过电子邮件（email）通信现在已经是一种很普通的行为。每天通过互联网发送无数封电子邮件，包含许多类型的信息。电子邮件也在公司和企业中使用，用于国内外通信。很多电子邮件包含敏感和机密的信息。

不幸的是，不是所有的电子邮件都能到达它们的目的地，甚至可能被错误的地址接收。而且，通常未授权人很容易破解服务器或进入网络阅读电子邮件。

对于发送加密的电子邮件，已有许多方法：PGP（Pretty Good Privacy）（PGP 和 Pretty Good Privacy 是 PGP 公司的注册商标）是一个用于发送加密电子邮件的应用程序。这个应用程序是一个插件，用于基于使用公开密钥的电子邮件程序。两个用户交换公开密钥，于是能用公开密钥加密并解密电子邮件或其它文件。而且，如果电子邮件用收件人的公开密钥加密并传送，发件方不能存取电子邮件。

也可以用一个文件作为电子邮件的附件，并给收件人提供密码存取附件。

这两种方法意味着每次存取新的加密文件或电子邮件时，都必须使用密码或个人密钥（personal key）。密码或个人密钥可能被忘记，或被未授权者获得。而且，测试表明很多人为了避免忘记密码/个人密钥，使用姓，昵称等，这些很容易被猜到或甚至被记录。

国际专利申请 WO 02/077773 描述了一种系统、方法和计算机程序产品，它提供了一个加密的电子邮件阅读器和响应器。分布和初始化加密电子邮件的方法包括：第一个用户获得具有公/私钥加密的电子邮件客户软件应用程序的许可；由第一个用户提出请求，让第二个用户下载阅读器/响应器软件应用程序，以便在第一个用户和第二个用户之间交换加密的电子邮件；第二个用户下载并安装阅读器/响应器软件应用程序；第二个用户给第一个用户发送电子邮件，包括使用

阅读器/响应器软件应用程序的发送密钥功能嵌入一个未加密的公开密钥；第一个用户接收来自第二个用户的电子邮件，其中未加密的公开密钥被嵌入在电子邮件中；第一个用户向第二个用户发送第二封电子邮件以做出响应，其中阅读器/响应器软件应用程序使用第二个用户的未加密公开密钥来加密第二封电子邮件信息为加密信息；第二个用户将来自第一个用户、带有加密信息作为附件的第二封电子邮件接收到第三方电子邮件软件应用程序上，其中第三方电子邮件软件应用程序不同于阅读器/响应器软件应用程序和电子邮件客户软件应用程序；第二个用户打开附件，执行阅读器/响应器软件应用程序，允许没有电子邮件客户软件的用户阅读并响应由有电子邮件客户软件的用户创建并发送的加密电子邮件。

公开的美国申请 2002059529 涉及安全的电子邮件系统，对于预选出的电子邮件用户形成一个请求安全通信的共同参与用户组，包括安全列表服务器，共同参与用户组中的成员将所有安全的电子邮件发送到安全列表服务器上，该服务器包括用于储存证书数据的储存器和 CPU，CPU 将想要接收每封电子邮件信息的收件人的姓名与存储器中的数据相比较，并处理信息以促进向前认证传送，这种认证传送是按存储器数据的显示对收件人进行及时认证。

美国 2003140235 涉及一种在注册了生物特征集的发件人与注册了生物特征集的收件人之间交换电子信息的方法，该方法包括：a. 在发件人和收件人之间交换注册的生物特征集；b. 生成发件人的 live-scan（数字式掌纹扫描工具）生物特征集；c. 生成第一区别密钥，第一区别密钥源自发件人的 live-scan 生物特征集与发件人注册的生物特征集之间的差异；d. 用第一区别密钥加密信息；e. 用加密密钥对所述发件人的 live-scan 生物特征集进行加密；f. 把加密后的信息和所述加密后的发件人 live-scan 生物特征集传送给收件人；g. 收件人解密所述加密后的发件人 live-scan 生物特征集；h. 收件人通过计算所述发件人的 live-scan 生物特征集与发件人注册的生物特征集之间的差异，重新生成第一区别密钥；以及 i. 利用重新生成的第一区别密钥解密信息。

WO 01/91366 涉及一种在密码通信系统中生成伪随机密钥的装置和方法。如果给出一个使配置数据初始化的公用集，伪随机密钥可以通过密码通信系统的各种独立的伪随机密钥生成器重复生成。

WO 02/39660 涉及一种使用原地生成的密钥在多个用户和一个中央服务提

供者中间进行密码通信的系统和方法。每个用户与中央服务提供者进行通信，优选使用用户通信接口，该用户通信接口包括一个本地密钥生成器，在使用用户自己个人的种子值进行初始化以后，本地密钥生成器生成一个唯一的密钥。通过发布只有各个用户才有的不同用户个人种子，各个用户的本地密钥生成器生成唯一一组密钥。中央服务提供者也有一个本地密钥生成器，并且还优选拥有一份分配给授权用户的所有个人种子的副本。中央服务提供者优选在一种安全加密方式下与各个用户用由用户个人种子生成的密钥进行通信。通过使用生成唯一个人密钥的加密通信，向多个用户发布额外的公用种子值，然后通过使用生成密钥的信号加密，许可安全条件下存取所述的用户，从而导致从公用种子值到希望的用户组。

在 OTP 中：One-time pad 生成器程序是一个通过互联网发布的共享软件程序（<http://www.fourmilab.ch/onetime>）用于生成一次性密码本（one-time pads）或密码列表。

发明内容

根据本发明最优的实施方案，本发明的主要目的是提供一种安全的电子邮件系统，该系统允许对电子邮件进行加密和解密而不需要重复使用密码或个人密钥。本发明尤其涉及在至少两个远程站点生成同步加密密钥，用于加密并解密电子邮件或类似信息。

本发明另一个目的是提供一种电子邮件系统，该系统能过滤不受欢迎的电子邮件，即所谓的垃圾邮件。

本发明另一个目的是提供一种电子邮件系统，该系统能容易地购买安全电子邮件软件程序。

基于这些原因，根据最优的实施方案，本发明涉及一种传送电子信息的方法，优选从第一个终端的第一个用户传送电子邮件到第二个终端的第二个用户，包括下列步骤：所述的第一个终端以加密形式传送所述电子邮件，所述加密的电子邮件是通过第一个密钥生成器用一个种子生成的密钥进行加密的，向所述第二个用户一次性提供所述种子，以便让所述第二个终端提供的第二个密钥生成器生成密钥，将所述的种子提供给所述的第二个终端并将所述的种子存储在所述的第二个终端中，当每次所述的第二个用户收到从所述的第一个用户发送的加密电子邮件

时，所述的第二个终端利用所述的种子生成一个密钥，同步各个终端的计数值；根据所述的种子和各个终端的计数值生成所述的密钥，与其它终端无关。

最优先的是，种子仅在第一次初始化时间获得。如果所述的第一个种子不能用了，例如当应用程序被重新安装或在新的电脑上安装时，优选获得第二个种子。

根据一种实施方案，当有许多封电子邮件发送给收件人时，每封加密的电子邮件都获得一个动态序列号。这个动态序列号用来为相应的加密电子邮件生成一个密钥。

根据一种实施方案，本发明还进一步包括下列步骤：同步各个终端的计数值；根据所述的种子和各个终端的计数值生成所述的密钥，与其它终端无关。种子以动态的且可交换的方式至少保存在一个终端中，优选保存在所有的终端中。计数值在各个终端的计数器中生成，计数值的同步化与计数器的同步化有关。在计数器初始同步化之后，仅在需要时终端执行补充的同步化步骤。基于种子和计数值的密钥-生成操作是靠一个以非动态和不可改变方式存储在至少一个终端中的算法来实现的。

根据一个实施方案，本发明还包括如下步骤：根据收到的种子生成一个委托终端列表，并只接受来自所述列表中注册的电子邮件。因而，能阻止垃圾邮件。

出于安全原因，根据最优的实施方案，本发明包括所述的第一个用户通过电话、传真和书信至少一种方式提供给所述的第二个用户所述种子的步骤。

加密电子邮件的附件与电子邮件一起被加密。

本发明还涉及从第一个用户传送电子邮件到第二个用户的系统。该系统包括第一个终端和第二个终端，该系统进一步包括：所述第一个终端以加密邮件形式传送所述安全的电子邮件的方法，所述加密的电子邮件是通过第一个密钥生成器用一个种子生成的密钥进行加密的，向所述的第二个用户一次性提供所述的种子以便用第二个密钥生成器生成密钥的方法，将所述的种子提供给所述的第二个终端的方法并将所述的种子存储在所述的第二个终端中的方法，当每次所述第二个用户收到从所述第一个用户发送的加密电子邮件时所述第二个终端利用所述的种子生成密钥的方法。

各个终端包括密钥-生成单元，密钥-生成单元包括存储器，相同的种子存储在存储器中；计数器，周期改变计数值；和计算终端，适合在各个终端并与其它

终端无关，根据原始值和由计数器发出的计数值生成密钥。在至少一个终端存储种子的存储器是动态存储器，以动态的且可交换的方式存储种子。各终端被设置为能感应到它们不同步的时候，然后重新设置同步化。至少一个终端的计算单元包括算法，算法以非动态的且不能改变的方式存储，并优选用硬件实现。终端之一是中央终端，它包含多个种子用于安全的加密传送，这些种子与若干不同的终端有关，每个终端具有一个原始值。

本发明也涉及用于从第一个终端的第一个用户传送安全的电子邮件到第二个终端的第二个用户的计算机程序产品，包括代码用于：加密并传送所述第一个终端发送的所述电子邮件，用所述的第一个种子在所述的第一个终端生成密钥，获得所述的种子以便在所述的第二个终端用第二个密钥生成器生成密钥，将所述的种子在所述的第二个终端中存储，当每次所述第二个用户收到从所述第一个用户发送的加密电子邮件时，所述的第二个终端利用所述存储的种子生成一个密钥。

本发明还涉及用于从第一个终端的第一个用户传送安全的电子邮件到第二个终端的第二个用户的传送信号，包括含有代码的信号，其中代码用于：加密并传送从所述第一个终端发送的所述电子邮件，用所述的第一个种子在所述的第一个终端生成密钥，获得所述的种子以便在所述的第二个终端用第二个密钥生成器生成密钥，将所述的种子在所述的第二个终端中存储，当每次所述第二个用户收到从所述第一个用户发送的加密电子邮件时，所述的第二个终端利用所述存储的种子生成一个密钥。

本发明还涉及计算机可读介质，其中存储着用于从第一个终端的第一个用户传送安全的电子邮件到第二个终端的第二个用户的指令集，所述的指令集包括代码用于：加密并传送从所述第一个终端发送的所述电子邮件，用所述的第一个种子在所述的第一个终端生成密钥，获得所述的种子以便在所述的第二个终端用第二个密钥生成器生成密钥，将所述的种子在所述的第二个终端中存储，当每次所述第二个用户收到从所述第一个用户发送的加密电子邮件时，所述的第二个终端利用所述存储的种子生成一个密钥。该介质可以是存储器单元。

本发明还涉及指令集的销售方法，该指令集用于传送并接收从第一个终端的第一个用户到第二个终端的第二个用户的安全的电子邮件。该方法包括：所述的

第一个终端以加密的形式传送所述安全的电子邮件，所述加密的电子邮件是通过第一个密钥生成器用一个种子生成密钥进行加密的，在所述安全的电子邮件中提供了指明销售方地址的可存取信息，从所述销售方地址获得第二个指令集用于解密所述电子邮件，并把所述第二个用户记为借方，由于他使用了所述第二个指令集加密新的电子邮件。最优的方法是计算机化的。账单是根据定购和接收所述第二个指令集开具的。第二个指令集是预先安装的指令集的进入密码。

本发明还涉及过滤接收器上电子邮件的方法，电子邮件从第一个终端的第一个用户到达第二个终端的第二个用户的接收器，所述的第一个终端以加密形式传送所述电子邮件，所述加密的电子邮件是通过第一个密钥生成器用一个种子生成的密钥进行加密的，向所述的第二个用户一次性提供所述的种子，以便用所述第二个终端提供的第二个密钥生成器生成密钥，所述的第二个终端根据所述种子生成的发件人-收件人关系生成一份受信任的发件人列表，并根据所述的列表进行接收电子邮件操作。该操作可以是存储、删除或退回所述电子邮件之一。

附图说明

下面参照附图对本发明进行描述，并对本发明优选的实施方案进行描述，但优选的实施方案并不限制本发明：

图 1 是根据本发明的网络通信步骤的流程图。

图 2 是描述计算机终端的结构图。

图 3 是描述本发明一部分步骤的流程图。

图 4 是描述部分发明的流程图。

具体实施方式

基本上，本发明允许向发送方和接收方系统提供一个初始种子并生成，对于每封电子邮件都不同，但在各个发件人/收件人终端基于同一个种子生成相同的加密密钥，并且无需每次传送电子邮件时都提供这个种子。根据优选的实施方案，本发明是一个应用程序，是作为诸如 Microsoft Outlook, Lotus Notes, Outlook Express 等电子邮件程序的插件来实现的。下面，参照 Microsoft Outlook 给出一些非限制性的实施例。然而，可以理解，本发明通常能应用于任何数据通信应用

程序/系统，特别是电子邮件应用程序/系统。因而本发明也能应用于 SMS 和 MMS 传送。

图 1 描述的是两个用户使用计算机终端发送和接收电子邮件的示意性通信流程。发送终端用 110 表示，接收终端用 120 表示。很明显，作为例子只给出了两个终端，而本发明可以在若干个终端上使用。终端之间的通信通过互联网或使用电子邮件服务器例如运行 Exchange Server 的局域网上进行。

本发明的系统创建了一种电子邮件通信安全的方法。每对发件人/收件人的两个电子邮件地址之间的关系是唯一的（通道）。系统用每对发件人/收件人自己特定的加密密钥对每对发件人/收件人进行处理。

根据图 1 的流程图，终端 110 的用户发送（1）电子邮件给收件终端 120 的用户。终端 110 安装了本发明的应用程序，该应用程序对电子邮件进行加密。在下面的实施例中，假定发件人的电子邮件地址为“110@mail.com”，收件人的电子邮件地址为“120@mail.com”。用例如 SHS-1，Blowfish 或类似的常规加密算法加密电子邮件信息，并用加密密钥锁定电子邮件信息。如果加密应用程序检测到收件人不是委托的收件人其中之一，也就是说，该收件人不在向其提供解密应用程序或解密密码的收件人注册列表里面，应用程序要求发件人提供初始的密码或为特殊的收件人提供密码。由发件人提供的密码，例如 120xxx，与收件人的其它有关信息（如电子邮件地址）一起储存于系统中。该密码用于：

- 生成密钥并初始化有密钥的通道，例如 110120xxx，该通道用于传送电子邮件给收件人 120；

- 生成密钥，例如 120110xxxx，当接收来自 120 的电子邮件时，使用该密钥；以及

- 生成唯一的加密密钥用来传送电子邮件。密钥的生成将在下面进行详细描述。

应当指出的是通道在这里是指虚拟通道，并且与获得的发件人-收件人的关系有关。

如果收件人没有解密应用程序，电子邮件附带一封未加密的信息发给收件人，告知电子邮件被加密了，需要进入（2）程序提供者 130，例如一个互联网服务商，以获得/下载（3）解密程序。加密的电子邮件也可以作为信息邮件的附

件发送。如果密钥缺失，例如在安装完解密程序后，收件人没有收到解密许可，收件人被指示获得“密码”能生成密钥来解密电子邮件。例如，收件人可以给发件人打电话（4）获得（6）密码，对密钥的生成进行初始化。当安装了加密部分并输入了密码，加密的电子邮件可以被解密了。收件人的应用程序存储了发件人的信息并：

- 生成密钥并初始化有密钥的通道，例如 120110xxx，该通道用来传送电子邮件给发件人 110；

- 用密钥初始化通道，例如 110120xxx，当接收来自 120 的电子邮件时使用该通道；以及

- 生成唯一的加密密钥用于接收来自发件人 110 的电子邮件。

因此，创建了一个发件人-收件人关系。

在后续步骤中，即当关系创建完成后并且发件人和收件人都有了初始化的密钥，不需要重新交换密码或口令。在各个终端的发件人和收件人的应用程序将自动验证并生成加密/解密密钥，例如根据发件人/收件人的电子邮件地址。

下一次电子邮件从 110 发送到 120 时，发件人的应用程序检测到收件人 120 在注册列表中，并根据生成的通道为电子邮件生成一个新的唯一的加密密钥。该密钥用于加密信息。与电子邮件一起发送一个动态序列号，该动态序列号确定了电子邮件的次序和使用的密钥。

在收件人站点，解密应用程序检测到加密信息所使用的加密密钥的动态序列。解密应用程序根据动态序列号（和更早存储的密码）生成密钥并解密电子邮件。如果动态序列号没有按顺序，例如，一封较低序列号的电子邮件比一封较高序列号的电子邮件收到得晚，该应用程序生成并存储所有的密钥直至用于解密特定的加密电子邮件的序列号。于是所有存储的密钥可以用来解密不连续的电子邮件。这些密钥在存储器单元中存储并加密，在相应的加密电子邮件被解密后该密钥可以被销毁。因此，本发明也可允许延迟解密电子邮件，并且也可在离线的方式下解密。

发件方或电子邮件应用程序可以提供带有设置参数的信息，设置的参数强制收件方或电子邮件应用程序执行特定的操作。例如，发件方可以要求接收到的信息以特殊的方式存储，例如存储为加密的信息，否则根本不存储。这样确保了发

件方能确信信息在收件人处存储时，未经授权者不能存取信息。也是可以是其它可能的指示，上述的例子只是起例证性的目的，并非是对本发明的限定，例如发件方可以要求查阅后立即删除电子邮件信息，并且不允许电子邮件信息以任何方式存储，以使安全性最大化。

每个终端 210，例如一台普通的个人电脑，如附图 2 中所示，包括主处理器 240，ROM（只读存储器）250，RAM（随机存取存储器）260 和程序存储单元 270。ROM 包含指令集，例如用于终端的功能性操作。RAM 存储来自应用程序的指令。程序存储单元包括应用程序，如电子邮件应用程序，加密和解密应用程序等。

密钥-生成应用程序 280 包括，在存储单元或 RAM 中，相同的原始值 SID，被称作种子，优选以动态和/相互/可交换的方式。原始值的存储优选与引导应用程序初始化一起实现，并且通过安全通道，如加密的信息或电话或类似来实现是有利的。或许，原始值不需要，不过却被物理传送，而相关单元的用户可以自行输入预先同意的值来替代物理传送。另外，如果需要，原始值可以交换，但一种替代方案是在密钥-生成单元整个寿命期内都使用同一个的原始值。这种情况下，原始值不需要在动态存储器中存储，而是可以使用永久性存储器。

另外，密钥-生成应用程序控制计数器 281，使之周期性改变计数值 X；并控制计算单元/应用程序 282，使之适合在各个和每个单元且与其它单元无关，根据原始值和由计数器发出的计数值，生成密钥。

然而，计数器和计算单元在同一个单元中集成是有利的，同一个单元适合为处理器（CPU）。振荡器 283 或时钟同样能在处理器中集成，用于控制计数器也很好。优选使用实时时钟在 CPU 中集成。另外，计数器阶梯式增加，这样更容易使终端与其它终端保持一致（同步）。

如果提供相同的原始值在存储器中存储，并使计数器同步以传送相同的计数值，那么可以在若干个密钥-生成应用程序中生成相同的密钥，与其它的，即运行应用程序的各个终端无关。

于是这些密钥可以在终端之间用于加密或身份验证的目的。

而且，密钥-生成单元优选适合感应它们是否同步，如果它们不同步，实现同步。感应可以靠特殊的同步测试来完成，同步测试在密钥生成之前完成。

一种替代方案是，当使用不同的密钥时，可以先验证是否需要同步，之后可以重新设置为同步。例如可以通过单元之间交换计数值来实现同步。

根据一个实施例，计算单元包括算法 F，算法 F 对原始值（种子）、现有密钥和计数值进行哈希处理作为输入参数。之后，计数值一个数一个数的增加，即计数=计数+1。这一算法优选在计算单元的硬件中实现，或者可替代的是，算法在非动态和不能改变的存储器中存储。算法优选生成 160 位的密钥，当然其它长度的密钥也是可能的。每次，给密钥生成器一个指令产生一个新的密钥时，生成一个新的伪随机 160 位字码，该字码是根据“种子”和计数值计算出来的。

密钥-生成应用程序还可以进一步包括接口部分，用于通信单元和密钥-生成单元之间能进行通信。优选的是，这种通信包括向密钥-生成单元发出指令生成密钥，然后发出指令使生成的密钥返回到通信单元。

密钥-生成单元可以在硬件中实现并且以集成电路的形式执行，因此很难被篡改。然后电路可以添加到基本上任何类型的通信单元上，与其共同使用。例如，本发明的密钥-生成单元与电子邮件应用程序一起使用是可能的。

根据本发明的密钥-生成应用程序可以用于点对点通信或身份验证中的任何一种，即在两个终端之间，或在中央单元、电子邮件服务器或若干个用户、客户之间。这样的中央单元优选包括多个不同的密钥-生成应用程序，其中一个用于各个客户/用户/终端与中央单元之间的通信。另一种替代方案，密钥单元能包括若干不同的原始值，在这样情况下，对密钥-生成单元发出生密钥的命令也包括关于应该使用哪个原始值的信息。同样的，对于与中央单元通信的若干单元具有相同的密钥生成单元是可能的，能使他们与中央单元中同一个的密钥-生成单元通信。

下面借助上面所描述的系统对加密传送或身份验证进行描述。第一步，在一个终端生成电子邮件并用密钥生成应用程序生成的密钥对电子邮件进行加密。电子邮件可以包含一个或几个附件，例如字处理文件、图片文件、JAVA 小程序或任何其它数字数据。因此，根据本发明的电子邮件涉及带附件的和不带附件的信息两种。发送电子邮件到收件终端，并让收件人得到一个初始值，即所谓的密码或种子。将密码输入到收件方的解密应用程序中，未来希望相互通信的终端被创建，在这一过程中他们被提供以相同的原始值并且优选同步化。现在该系统已经

准备好使用了，在随后的时间里，初始化后经过任意一段时间可以使用系统，并且至少一个终端向其它终端认证自身。当其它终端确定给出的身份是否是已知的，它是否有相应的密钥-生成应用程序，即如上定义的密钥-生成应用程序，并带有相应的原始值，获得认证。如果是，程序继续进行到下一步，相反程序中断。

然后用计算得到的密钥执行加密/解密/身份验证。然而，应该理解的是，加密传送和身份验证当然可以在同一过程同时实现。加密和身份验证的实现可以借助基本上使用密钥的任何加密算法，例如已知的 DES 和 RC6，Bluefish 等。

本发明的另一个优点是应用程序能用作过滤器用于阻止不需要的电子邮件。如今，无数封广告电子邮件发送给收件人们，例如，Outlook 里有个功能叫做“垃圾邮件”，它根据名单或一些参数把收到的电子邮件放到一个垃圾邮件文件夹里。然而当发件人的名称和垃圾邮件的内容改变了，这个功能就不起作用了。本发明针对这个问题用下面的方法解决：

如上所述并参考图 3，收件终端或服务器包括发件人-收件人对列表，核对 300 用于在列表中核对对接收到的地址，和比较 310 用于将发件人的地址与存储的地址相比较。如果电子邮件能被解密，即发件人地址在列表中存在，电子邮件被解密 320 并传送给收件人。如果电子邮件不能被解密，即发件人的地址不在列表中，电子邮件或者移到垃圾邮件箱或者退回 330 给发件人。可以给退回的电子邮件附上一封信息，例如通知发件人需要加密程序才能发送电子邮件给希望的收件人。当然，不是列表中的发件人，但是收件人想要的发件人也可以发送电子邮件。由于这个原因，系统能存储 340 一份电子邮件的副本，或者只是通知收件人，这样发件人能得到通知要求其安装加密应用程序并从收件人处获得密码。很明显，过滤/阻止功能是一个可选的应用程序。

如上面所提到的，本发明还允许以简单的方式购买整个或部分应用程序。

附图 4 对自动购买系统 400 进行了描述。收件人 401 收到一封信息性电子邮件，其附件为加密电子邮件，获得解密程序。优选的是，该解密程序以免费或共享软件形式提供。而加密应用程序必须购买。当解密程序被下载时，加密程序也被下载，但只有提供了许可号、密码或类似，才能使用加密程序。由于这个原因，顾客被指向一个购买地址 410，例如在互联网上，能从那里获得许可。购买网站可能需要有关顾客的国家、语言等特定的信息，以便顾客能获得正确的版本。然

后顾客被重新定位到提供交易信息的定购网站 420。付款人可以用已知的方式进行交易，例如用信用卡、银行交易、现金交易等付款。根据交易方法，进行清算 430 或管理 440。如果交易被接受了，购买站点 420 给注册处 450 发送信息并给交货部门 460 发指令。交货部门或者发送程序包、许可号或者发送（安装并）运行加密程序所必需的任何其它信息。交货部门能产生程序包/许可信息。如果预先安装了程序，密码/许可号能通过（加密）电子邮件或从网站下载交付。

也可能给收件人提供发件人发的电子邮件并通知收件人到提供预付费程序下载以及密码的网站获得解密/加密应用程序来解密电子邮件。然而，这样情况下，收件人必须获得密码或其它进入程序的可能性。

也可能提供一种服务器设备，加密的电子邮件通过该设备，例如通过开辟地址通道来实现。这种情况下，每封电子邮件能分别记入借方（所谓的 ticker）而无需购买程序。

以上的实施例涉及网络，在那里用户使用两个终端存取电子邮件。本发明也能应用在用户使用不同终端的情况下。在这种情况下，加密/解密程序和种子能作为移动应用，例如以硬件插件（如 USB dongle）的形式，存储在信息载体介质如 CD 等上。因而，每次使用电子邮件应用程序时，都必须提供密钥/存储介质，以便从那里执行加密/解密应用程序。

在网络里，例如在组织机构或企业中，服务器处理客户所在的 IP 网络。客户只需要创建一条安全的电子邮件通道到正在运行的服务器上，这个服务器于是处理与网络上其它用户的安全联系。给每个用户提供一个唯一的密码，以便能根据本发明存取电子邮件信息并发送电子邮件信息。而且，可以给网络管理员提供管理员密码，管理员密码能让管理员读取信息并管理账户。为了进一步提高安全性，要求管理员必须使用硬件单元生成唯一的序列号是可能的，唯一的序列号用于身份验证的目的。这个唯一的序列号控制位于如中央服务器中的另一个的硬件或软件模块，基于服务器的模块生成序列号，如果它是正确的硬件单元并且它们相互之间同步，那么这个序列号与管理员模块生成的序列号相同。如果他们不相同，那么两个系统要试着相互同步几次。

管理员使用的这种硬件单元可以提供为例如，但不限于，硬件插件使用 USB（通用串行总线），RS232，RS485，以太网，Firewire，蓝牙，Centronics，

SecureDigital, PCMCIA, PC-Card 或类似的硬件连接标准。也可能使用软件模块来代替硬件单元，该软件模块或者在可管理的电脑上、工作站或类似的计算机设备上，或者在计算机介质存储设备上，该设备能连接到网络上或者能连接到在管理下连接到网络上的设备上。

还可能提供带有压缩工具的系统，用于压缩加密的电子邮件。任何传统的压缩方法都能使用。

可以选择的是，加密和/或解密的电子邮件能以解密或加密的形式保存。在这种情况下，优选电子邮件用密码进行加密。出于安全原因，尤其是在公司里，应该有个人密码和一个管理员密钥（网络管理员）。

以上描述和说明的实施方案不能限定本发明。在附加权利要求的范围内，根据应用、需求和需要，能以若干种方式对本发明进行改进。

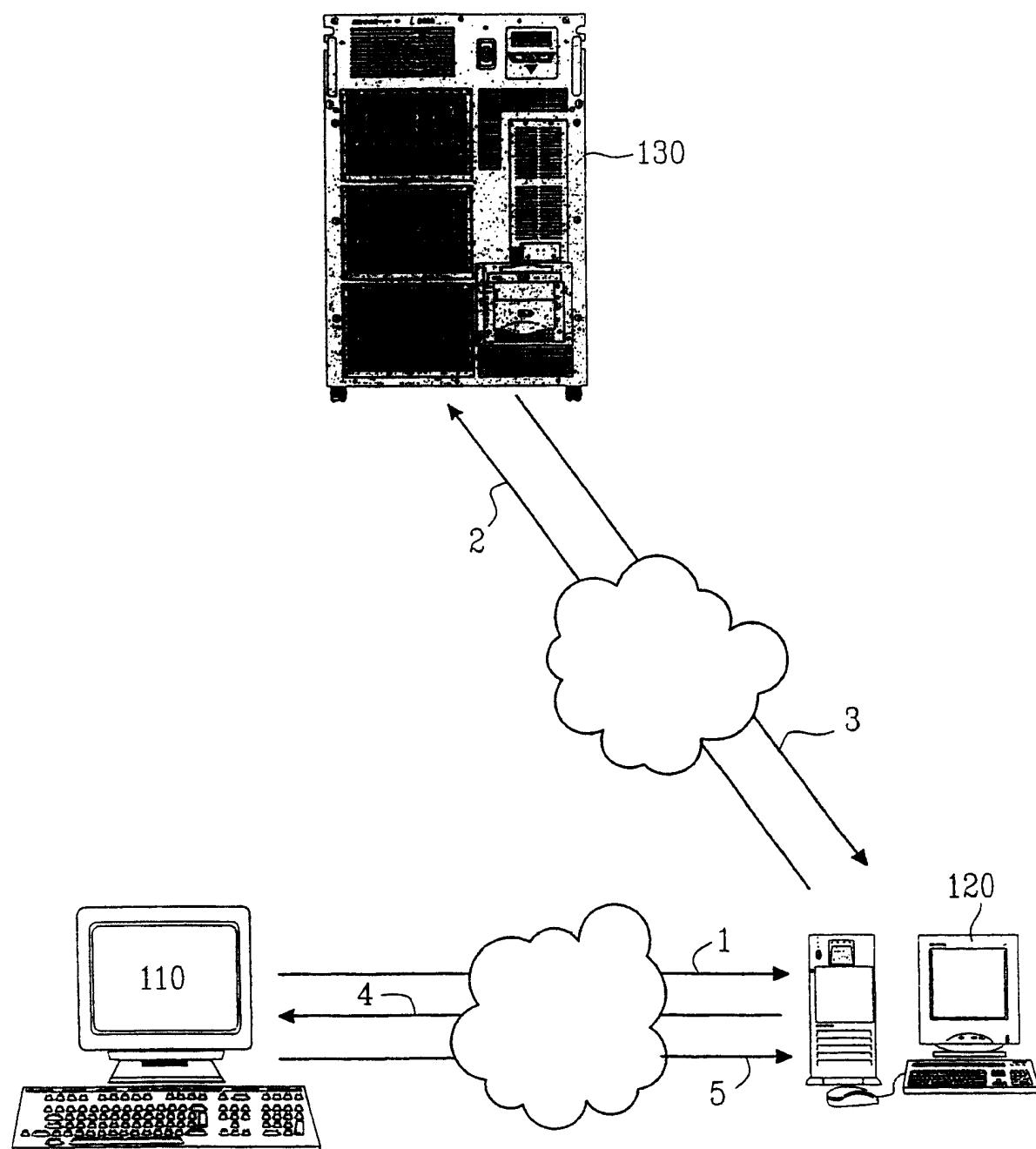


图 1

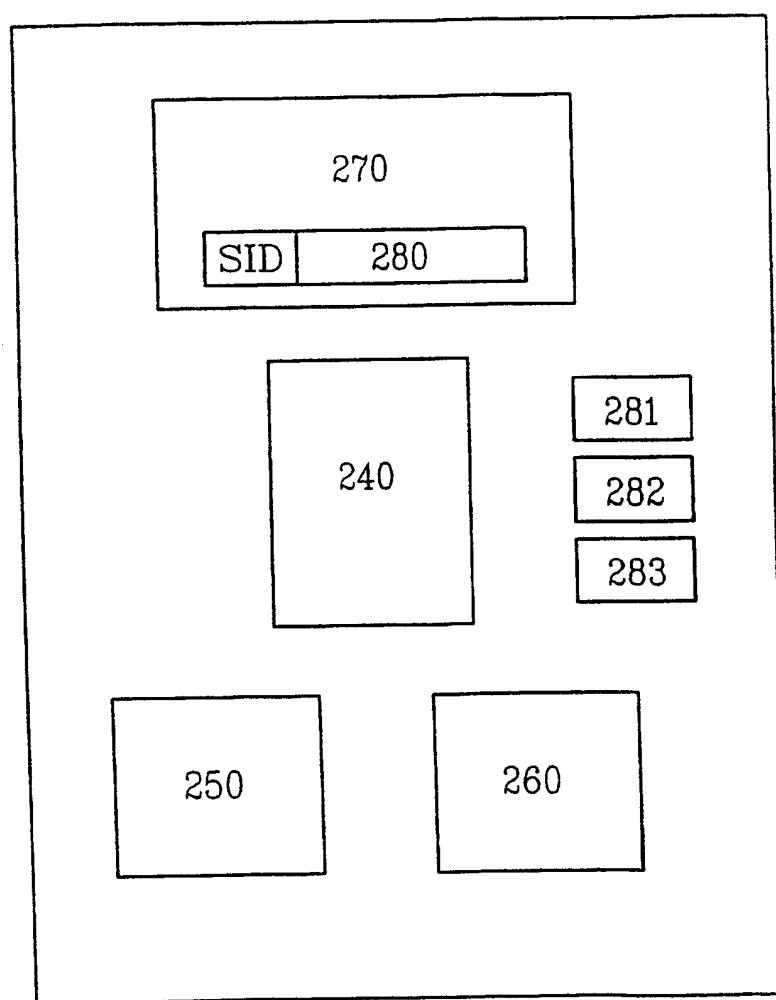


图 2

