

[19] 中华人民共和国国家知识产权局

[51] Int. Cl⁷

H04M 3/38

H04M 11/00

H04K 1/00

H04L 9/00



[12] 发明专利申请公开说明书

[21] 申请号 03807031.6

[43] 公开日 2005 年 8 月 3 日

[11] 公开号 CN 1650603A

[22] 申请日 2003.2.12 [21] 申请号 03807031.6

[30] 优先权

[32] 2002. 2. 15 [33] US [31] 10/077,365

[32] 2002. 5. 6 [33] US [31] 10/139,873

[86] 国际申请 PCT/US2003/004387 2003.2.12

[87] 国际公布 WO2003/071770 英 2003.8.28

[85] 进入国家阶段日期 2004.9.27

[71] 申请人 高通股份有限公司

地址 美国加利福尼亚州

[72] 发明人 A·甘特曼 G·G·罗斯

[74] 专利代理机构 上海专利商标事务所有限公司

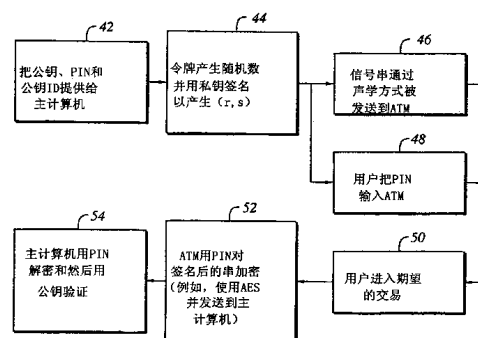
代理人 李家麟

权利要求书 3 页 说明书 6 页 附图 1 页

[54] 发明名称 声学双要素认证的系统和方法

[57] 摘要

一种手持令牌，用于生成代表着从公钥对(44)的私钥产生的数字签名的声学或其它无线信号，公钥是机密的，因为它仅为经授权的实体所知，例如银行计算机。来自所述令牌的信号可以被接收，例如被银行 ATM(46) 中的接收机接收，而要访问帐户还需要 PIN。用户把 PIN 输入到 ATM(48)，ATM(52) 用 PIN 给来自所述令牌的信号加密，通过无需安全的链路把它发送到银行计算机(54)，因为如果不知道由银行计算机持有的机密公钥，即使 PIN 被猜到也无从验证它就是正确的 PIN。



1. 一种认证方法, 包括

给授权计算机至少提供 PIN 和机密公钥;

在授权计算机和至少一个远离计算机的接收机之间建立通信链路, 通信链路不限于是安全的;

在接收机处接收至少一个代表至少一个私钥产生的信号的声学信号, 接收机把所述声学信号转换为签名信号;

在接收机处接收 PIN, PIN 和声学信号被分开接收;

用 PIN 对签名信号加密以产生加密的签名信号; 以及

把加密的签名信号发送给授权计算机以使用 PIN 和机密公钥验证签名。

2. 如权利要求 1 所述的方法, 其特征在于, 加密动作在接收机处完成。

3. 如权利要求 1 所述的方法, 其特征在于, 使用手持令牌发送所述声学信号。

4. 如权利要求 1 所述的方法, 其特征在于, 还包括把期望的交易输入到接收机, 只有在签名得到验证时, 授权计算机才授权接收机执行交易。

5. 如权利要求 1 所述的方法, 其特征在于, 签名这样验证:

用 PIN 给加密的签名信号解密以得到签名信号; 然后

使用机密公钥来验证签名信号。

6. 如权利要求 3 所述的方法, 其特征在于, 所述令牌通过把至少一个消息和私钥相结合而产生签名信号。

7. 如权利要求 6 所述的方法, 其特征在于, 所述消息至少包括至少一个时间戳的一部分。

8. 如权利要求 7 所述的方法, 其特征在于, 所述时间戳的一部分是比预先确定数有更多位的时间戳中预先确定数量的最低有效位。

9. 一个不限于是安全的链路上的双要素认证系统, 包括:

至少一个便携式令牌, 其产生至少一个代表数字签名消息的无线信号;

至少一个接收机, 其接收无线信号和 PIN, PIN 和无线信号被分开接收, 接收机用 PIN 给签名消息加密以得到加密的签名消息; 以及

至少一个授权计算机, 其在链路上接收至少一个加密的签名消息, 授权计算机访问 PIN 和机密公钥以试图验证签名消息;

10. 如权利要求 9 所述的系统, 其特征在于, 所述无线信号还至少表示机密公钥的 ID, 和对应于公钥的私钥签名后的消息, 以得到数字签名的消息。

11. 如权利要求 10 所述的系统, 其特征在于, 所述接收机向授权计算机发送加密签名消息、ID 和被签名的消息。

12. 如权利要求 10 所述的系统, 其特征在于, 所述授权计算机使用 PIN 对加密签名信号解密, 并通过使用 ID 和使用机密公钥访问机密公钥来验证签名消息。

13. 一种包括授权计算机的认证系统, 所述授权计算机访问至少一个 PIN 和一个机密公钥并通过链路和至少一个远离计算机的接收机通信, 通信链路不限于是安全的, 所述系统包括:

在接收机处接收至少一个代表从私钥产生的至少一个数字签名的无线信号的装置, 所述接收机把无线信号转换为签名信号;

用于在接收机处接收 PIN 的装置; 以及

用 PIN 对签名信号加密以产生加密签名信号的装置, 所述加密签名信号通过链路被发送给授权计算机以便使用所述 PIN 和机密公钥来验证签名。

14. 如权利要求 13 所述的系统, 其特征在于, 所述用于加密的装置在接收机中。

15. 如权利要求 13 所述的系统, 其特征在于, 还包括使用手持令牌发送无线信号的装置。

16. 如权利要求 13 所述的系统, 其特征在于, 还包括把期望的交易输入到接收机的装置, 只有在签名得到验证时, 授权计算机才授权接收机执行交易。

17. 如权利要求 13 所述的系统, 其特征在于, 包括:

使用 PIN 对加密签名信号解密以产生签名信号的装置; 以及

使用机密公钥验证签名信号的装置。

18. 如权利要求 15 所述的系统, 其特征在于, 所述令牌通过把至少一个消息和私钥相结合而产生签名信号。

19. 如权利要求 18 所述的系统, 其特征在于, 所述消息包括至少一个时间戳的至少一部分。

20. 如权利要求 18 所述的系统, 其特征在于, 所述消息还和伪随机数结合。

21. 如权利要求 13 所述的系统, 其特征在于, 所述无线信号是声学信号。

22. 如权利要求 9 所述的系统, 其特征在于, 所述无线信号是声学信号。

23. 一种计算机可读媒介, 包含控制计算机系统执行一种方法的程序, 所述方法包括:

向授权计算机提供至少一个 PIN 和一个机密公钥;

在授权计算机和至少一个远离计算机的接收机之间建立通信链路, 通信链路不限于是安全的;

在接收机处接收至少一个代表至少一个私钥产生的信号的声学信号, 接收机把所述声学信号转换为签名信号;

在接收机处接收 PIN, PIN 和声学信号被分开接收;

用 PIN 对签名信号加密以产生加密签名信号; 以及

把加密签名信号发送给授权计算机以使用 PIN 和机密公钥验证签名。

24. 如权利要求 23 所述的计算机可读媒介, 其特征在于, 所述加密动作在接收机处完成。

25. 如权利要求 23 所述的计算机可读媒介, 其特征在于, 还包括使用手持令牌发送所述声学信号。

26. 如权利要求 23 所述的计算机可读媒介, 其特征在于, 还包括把期望的交易输入到接收机, 只有在签名得到验证时, 授权计算机才授权接收机执行交易。

27. 如权利要求 23 所述的计算机可读媒介, 其特征在于, 签名这样验证:

用 PIN 对加密签名信号解密以产生签名信号; 然后

使用机密公钥验证所述签名信号。

28. 如权利要求 25 所述的计算机可读媒介, 其特征在于, 所述令牌通过把至少一个消息和私钥相结合而产生签名信号。

29. 如权利要求 28 所述的计算机可读媒介, 其特征在于, 所述消息包括至少一个时间戳的至少一部分。

30. 如权利要求 29 所述的计算机可读媒介, 其特征在于, 所述时间戳的一部分是比预先确定数有更多位的时间戳中预先确定数量的最低有效位。

声学双要素认证的系统和方法

有关申请

本申请是于 2002 年 2 月 15 日提交的美国专利申请第 10/077,365 号发明名称为“Method and Apparatus for Simplified Audio Authentication(简化的音频认证的方法和装置)”这一共同待批的专利申请的继续申请,这一专利申请通过引用被结合于此。

I. 发明领域

本发明一般涉及使用音频音调的认证。

II. 发明背景

随着因特网使用的增长,许多类型的便利型电子商务已经成为可能,诸如在线购买商品和服务、在线银行和使用连接到远程银行的自动柜员机(ATM)等等。但正是电子商务的便利性也使窃贼窃取宝贵信息和/或伪装成不想购买商品和不想从银行帐户提款等等的人更加容易。

因此,在电子交易中提供安全至关重要。为此,许多电子交易被加密来隐藏被交换的私人信息。但加密只是安全的一个方面,因为窃贼可能破解加密方法或进而持有诸如信用卡这类有效物品、伪装成所有者并参与加密的交易。

注意到这一点,就容易理解认证是安全的一个重要方面。在电子商务方面,试图认证的个人是通过计算机界面完成的。因此,如果没有普遍安装生物传感型计算机附件的基础设施,那么采取检验个人生物学特征来验证这人是他声称他是的人通常并不切实可行。

这使两个认证要素可用,即,基于个人所拥有的诸如信用卡或钥匙链之类物品认证一个人,或基于个人所知道的诸如密码或个人识别号(PIN)之类事物认证一个人。对一些特别敏感的诸如 ATM 提款之类的应用,也许两种要素都是需要的。

目前,ATM 用户把诸如信用卡之类的认证设备插入 ATM,然后输入 PIN。这种方法完成了双要素认证。但是,ATM 必须把卡上的秘密信息和 PIN 两者都发送到中

央银行计算机进行认证。因此，银行和 ATM 之间的链路必须安全，以防止窃贼在线路上窃听并发现认证要素两者，所述认证要素使窃贼能够从用户帐户上窃取金钱。这给链路基础设施带来巨大负担。

上面指出的专利申请揭示了手持的基于声波的“令牌”，个人可以操作它来向称作“认证器”、“验证器”或“接收机”的设备发出表示秘密信息的声学信号，以便基于这个信号认证这个人。在那些申请中公认，基于声波的令牌的有利条件是已经存在着用于接收和发送话音和来源于话音的电子信号的庞大的已安装的基础设施。具体地说，已经存在全球电话系统发送代表声学信息的数据，还有，除了电话，现在由这同一个系统（包含在因特网中）连接的许多计算设备都有麦克风和扬声器（或可以很容易修改成有它们）。

如这里公认的，用在 ATM 环境中时，声波令牌的优势在于以阻止 ATM 在没有机密密钥时能伪造私人信息的方式把令牌上的私人信息发送到 ATM。ATM 简单地把私人信息发送到中央银行计算机进行认证。这样，ATM 及 ATM 和银行的链路都无需安全来保护这个认证要素。但是，本发明还认识到第二个认证要素 PIN 仍然需要链路安全。这是因为 PIN 一般只有 4 到 6 位阿拉伯数字组成，攻击者可以窥探 ATM 和银行之间的链路，而如果通信允许猜测的 PIN 被验证，攻击者就可以简单地试验出大约百万个可能的 PIN 值并记住起作用的一个，直到攻击者能够偷取令牌并能够访问帐户。因此，不幸的是，银行和 ATM 之间的安全通信将仍然是必需的。

认识到上面的问题，提供了在这里揭示的发明。

发明内容

一种认证方法，包括最初向诸如银行计算机这样的授权计算机提供 PIN 和机密公钥，然后在授权计算机和远离计算机的诸如 ATM 这样的接收机之间建立通信链路。通信链路不限于是安全的。随后，用户的声学信号可以被接收机（例如 ATM）接收，信号代表私钥产生的数字签名，接收机把声学信号转换为签名信号。PIN 通过例如用户在与接收机相关联的数据输入设备上键入这样的方式也被接收机接收，所以 PIN 和声学信号分开地被接收。用 PIN 给签名信号加密得到一个加密的签名信号，然后把后者发到授权计算机以使用 PIN 和机密公钥来验证签名。

签名信号最好由接收机用 PIN 加密。另一方面，声学信号最好用手持令牌发送。期望的交易可以输入到接收机，只有在签名得到验证后，授权计算机才授权接

收机执行交易。

通过使用 PIN 给加密签名信号解密以得到签名信号，签名由授权计算机来验证。然后，所产生的签名信号使用机密公钥验证。

在一个优选实施例中，令牌通过把一消息和私钥结合而产生签名信号。所述消息可以包括时间戳的至少一部分，例如，比预先确定数有更多位的时间戳中预先确定数量的最低有效位。

另一方面，揭示了一种用于不限于是安全的链路上的双要素认证的系统。所述系统包括产生代表数字签名消息的无线信号的便携式令牌。接收机接收无线信号和 PIN，PIN 是和无线信号分开接收的。接收机用 PIN 给签名消息加密得到加密的签名消息。授权计算机通过链路接收加密的签名消息，并访问 PIN 和机密公钥以试图验证签名消息。

还有另一方面，认证系统包括至少访问 PIN 和机密公钥并通过链路和至少一个远离该计算机的接收机通信的授权计算机。通信链路不限于是安全的。系统包括用于在接收机中接收代表一数字签名的无线信号的装置，所述数字前面通过把消息和私钥相结合而产生。接收机把无线信号转换为签名信号。在接收机中的装置也接收 PIN。提供装置用 PIN 给签名信号加密以产生加密的签名信号。加密的签名信号通过链路被发送给授权计算机，以便使用 PIN 和机密公钥来验证签名。

本发明关于其结构和操作的两个方面的细节，参考附图可以更好理解。在整个附图中，相同的标号标识相应的部件。

附图简述

图 1 是基于音频认证的本发明系统的方框图；以及
图 2 是本发明逻辑的流程图。

优选实施例详述

最初参照图 1，显示了一个系统，一般指定为 10，所述系统包括可以被配置成钥匙链或其它小型设备的便携式手持令牌 12。但是，根据需要，本发明也可以应用于其它令牌配置，例如手持的或便携的象安放在交通工具（包括汽车、卡车、小船、飞机和火车）上的移动通信站，包括膝上型电脑、无线手机或电话、数据收发机、或寻呼和位置确定接收机。无线通信设备有时也可以称为用户终端、移动站、

移动单元、用户单元、移动无线电或无线电话、无线单元、或象在一些通信系统中那样简单地称为“用户”和“移动”。

不论如何，令牌 12 都能够产生可以被接收机 16 接收的声学信号，用多根线条 14 示意性地表示。接收机 16 和授权计算机 18 相关联。在说明性实施例中，接收机 16 是自动柜员机（ATM），授权计算机 18 是银行主计算机，但是可以理解，接收机 16 可以是一接收设备，所述接收设备与诸如建筑物、家、交通工具相关联，或与期望使用双要素认证限制对预先授权用户的访问的任何其它部件相关联。还可以理解，优选令牌 12 是一个产生声学信号的声波令牌，本发明的原理可以应用到其它无线信号生成令牌，包括那些可能使用电磁波无线通信原理（例如诸如蓝牙和红外这样的射频）来向接收机 16 发射下面揭示的数字签名的令牌。

优选声学信号 14 可以代表使用存储在令牌 12 的电子数据存储器 20 中的私钥产生的数字签名。伪随机数（PN）发生器 21 也可以包括在令牌 12 中。为了简略揭示也可以将相应的机密公钥或机密公钥标识存储在那里。

按照本领域中熟知的和（美国）国家标准技术研究所（NIST）联邦信息处理标准出版物 186-2. 一月. 2000 所阐明的私钥/公钥原理，令牌 12 中的签名算法（由令牌 12 中的微处理器 22 执行）接收私钥和要被签名的消息的至少一部分作为输入（并从而“结合”），加上来自 PN 发生器 21 的随机数“k”，以产生数字签名，即随机对（r, s）。微处理器 22 最好在收到来自诸如拨动开关、话音激活设备或按钮这样的或更多激活元件 24 的激活信号时立即执行签名算法。被签名的消息和对应于私钥的机密公钥的标识也最好包括在微处理器 22 产生的信号里。可以理解，微处理器 22 可以包括本领域中熟知的数字处理器、必要的时钟、模数转换电路和数模转换电路。

微处理器 22 访问数据存储器 20，使得在使用多个激活元件 24 时，一个或更多个激活元件可以和存储器 22 中的相应私钥相关联。电子签名信号被发送到音频扬声器 26 以便把电子签名信号转换为声学信号 14。声学信号可以是听得见的，也可以是听不见的。如果需要，也可以在令牌 12 中提供麦克风 28 来接收声学信号并把它们转换为电子信号，所述电子信号被送到微处理器 22 进行处理。使用电磁波无线原理时，扬声器 26 被取代，例如被射频发射机或红外发射机取代。

优选声学信号 14 被接收机 16 中的麦克风或其它声学接收设备 30 所接收。麦克风 30 把声学信号转换回电子签名信号（如果需要，还伴随着机密公钥 ID 和最初

的签名前消息)，然后根据需要发送到可以访问数据存储器 34 的微处理器 32。如果需要，也可以在接收机 16 中提供扬声器 36 以便把声学信号送回给令牌 12，由令牌 12 中的麦克风 28 接收所述信号。

当接收机 16 是 ATM 而授权计算机 18 是中央银行计算机时，授权计算机 18 可以包括一处理器 38，处理器 38 访问数据存储器 40 通过对从接收机 16 接收到的数字签名进行验证（或不验证）而选择性地准予授权。数据存储器 40 可以包括像列表或数据库表这样的数据结构，所述数据结构存储着和由信号代表的私钥相关联的机密公钥（和它的 ID）。无论如何，由于下面揭示的密码学的新颖用法，连接银行和 ATM 的链路 41 无需是安全的。

图 2 显示了本发明的逻辑。从方块 42 开始，和令牌 12 相关联的机密公钥，和公钥的 ID 一起，被提供给授权计算机 18（例如，主银行计算机）。而且还提供了用户的 PIN。这个提供过程是亲自或通过安全连接安全地完成的。“机密公钥”是指和本领域内熟知的私钥/公钥原理一致的公钥，除了机密公钥不可公开地访问而是仅被提供给例如主银行计算机这样的可信实体以外。

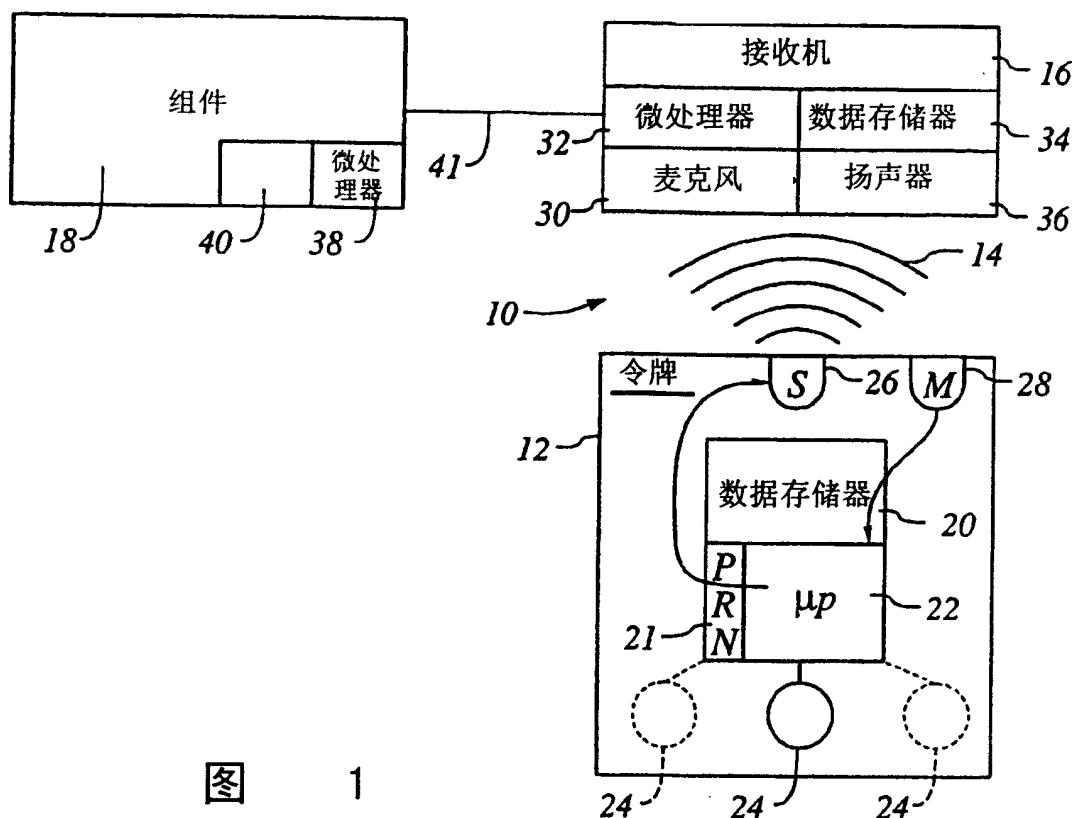
移到方块 44，在用户操作激活元件 24 之一时，令牌 12 中的签名算法接收私钥、伪随机数、以及诸如时间戳的全部或一部分这样的消息作为输入，以产生电子签名，例如随机对 (r, s) 。然后用户把认证的两个要素都输入到接收机 16。特别地，在方块 46 处，数字签名是以无线方式（例如，声学方式）和经签名的消息一起，如果需要还和相应的机密公钥的 ID 一起，被发送到接收机 16，在方块 48 处，用户使用如在多数 ATM 上提供的数字键区输入 PIN。在方块 50 处进入期望的交易（如提款、转账等等）。可以理解，方块 46、48 和 50 的步骤可以以任何顺序执行。

按照本发明，在方块 52，接收机 16 用 PIN 给签名 (r, s) 加密。这个加密可以是使用诸如 AES 加密原理的对称加密。经加密的签名与没有加密的机密公钥 ID 和没有加密的签名前的被签名的消息（例如，时间戳或它的两个最低有效位）一起被发送到主计算机处理器 38。

在方块 54，主处理器 38 先用 PIN 给数字签名解密。然后，通过使用机密公钥 ID 和最初的签名前的消息，处理器从数据存储器 40 中检取适当的机密公钥，并依照本领域中熟知的公钥/私钥原理来验证签名。如果验证成功，授权计算机 18 就用信号通知接收机 16 允许访问。在 ATM 验证器 16 和银行计算机授权计算机 18 的情况下，银行计算机用信号通知 ATM 执行所请求的交易。

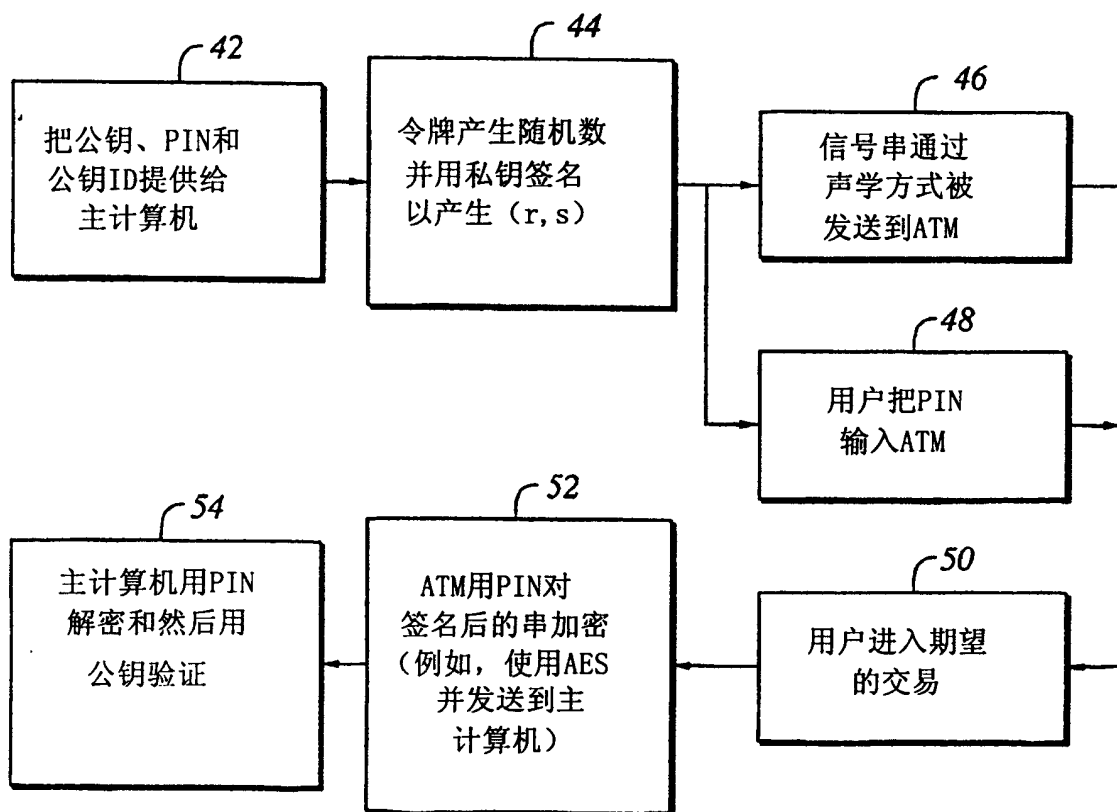
现在可以理解可能截取链路 41 上的 ATM—银行通信的攻击者不能推导出 PIN。特别地，使用“正确的”PIN 对签名解密和使用不正确的 PIN 对其解密会产生同等的结果：也就是不验证签名时不能被理解的随机对，也就是没有机密公钥和被签名的数据就不可能完成的事（注意只有时间戳的几个最低有效位被发送）。这一特征消除了链路 41 上对安全性的最后要求。

在这里详细地显示和描述的特定“声学双要素认证的系统和方法”完全能够达到本发明以上所述的目标，可以理解，这是本发明目前的优选实施例，是本发明广泛可构想的主题的代表，本发明的范围完全包括对本领域的熟练技术人员可能变得明显的其它实施例，从而，本发明的范围不受除了所附权利要求书之外的任何限制，在权利要求书中单数所指的元件，除非明确地说明之外不是要指“一个且只有一个”，而是“一个或更多”。对本领域的普通技术人员已经知道或将要知道的上述优选实施例中元件的所有结构性或功能性的等价物明确引用在此做为参考，而且都包含在本权利要求书中。此外，不必要求本发明解决致力于每个问题的设备或方法，仅仅因为它被包含在本权利要求书中。此外，本发明的没有任何元件、元素或方法步骤是要奉献给大众，不管这个元件、元素或方法步骤有没有明确地在权利要求书中陈述。这里没有权利要求元素要解释为是在 35 U. S. C § 112 第六节规定之下，除非这一条用“用于...的装置”明确叙述，或在方法权利要求的情况下这一条用“步骤”而不是“动作”叙述。



图

1



图

2