[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/14 (2006.01)
H04L 9/32 (2006.01)

[12] 发明专利说明书

专利号 ZL 200410103115.X

[45] 授权公告日 2009 年 11 月 18 日

[11] 授权公告号 CN 100561913C

[22] 申请日 2004.12.31

[21] 申请号 200410103115.X

[73] 专利权人 联想（北京）有限公司

地址 100085 北京市海淀区上地信息产业基地创业路 6 号

[72] 发明人 尹 萍 韦 卫 宁晓魁 林 洋 郭轶尊

[74] 专利代理机构 北京德琦知识产权代理有限公司

代理人 王 琦 程殿军

[56] 参考文献

US2001/0034848A1 2001.10.25

CN1464676A 2003.12.31

US2005/0154877A1 2005.7.14

CN1635736A 2005.7.6

审查员 高 静

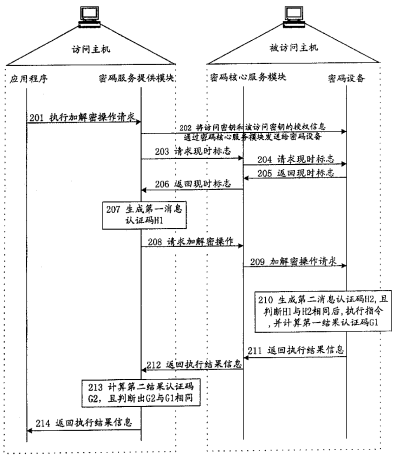
权利要求书 4 页 说明书 13 页 附图 2 页

[54] 发明名称

一种访问密码设备的方法

[57] 摘要

本发明提供了一种访问密码设备的方法，其关键是：在密钥创建时为所创建的密钥设置密钥授权信息，在密钥使用过程中发送方和接收方之间传送的信息，均应用密钥授权信息为其计算认证码，然后再将待传送的信息和已计算出的认证码传送给对方，接收方则根据认证码验证消息的完整性，以鉴别信息来源是否可靠，且传送途中是否被篡改过，当验证成功后，再执行后续操作。 应用本发明，密码设备既可以被远程访问也可以在本地访问，且能够使多个用户应用远程的不具备密码设备的主机访问密码设备，而仍然能够保证信息的安全特性。 由于本发明采用一次一密的加密方式，有效地抵御网络监听者的重播攻击。



1、一种访问密码设备的方法，其特征在于，在访问主机上设置用于远程调用密码设备的密码服务提供模块，在被访问主机上设置用于接收远程调用，并驱动密码设备执行操作的密码核心服务模块，创建每一密钥时为所创建的密钥设置密钥授权信息，该方法还包括以下步骤:

a、密码服务提供模块接收到来自应用程序的密码操作指令后，应用密钥授权信息对所述密码操作指令计算第一请求消息认证码，之后，将包含第一请求消息认证码和所述密码操作指令的密码操作请求通过密码核心服务模块发送给密码设备;

b、密码设备根据接收到的密码操作指令，利用已获得的密钥授权信息计算第二请求消息认证码，并判断计算出的第二请求消息认证码与接收到的第一请求消息认证码是否相同，如果相同，则执行步骤 c，否则返回错误信息，结束本流程;

c、密码设备执行密码操作请求中所指示的操作，并应用密钥授权信息对执行结果计算第一执行结果认证码，然后，将包含第一执行结果认证码和执行结果的信息发送给密码核心服务模块，由密码核心服务模块将接收到的信息解析为密码服务提供模块能够识别的信息后，再发送给密码服务提供模块;

d、密码服务提供模块应用密钥授权信息对接收到的执行结果计算第二执行结果认证码，并判断计算出的第二执行结果认证码与接收到的第一执行结果认证码是否相同，如果相同，则给应用程序返回执行结果信息，结束本流程；否则，给应用程序返回错误信息，结束本流程。

2、根据权利要求 1 所述的方法，其特征在于，

步骤 a 所述密码服务提供模块接收到的来自应用程序的密码操作指令为生成访问密钥的指令，该指令中包含有为即将生成的访问密钥设置的访问密钥授权信息，以及访问密钥的算法信息；所述计算第一请求消息认证码的方法为：获取现时标志，应用已获取的现时标志对所述访问密钥授权信息进行加密，将

加密后的访问密钥授权信息、访问密钥的算法信息、已获取的现时标志与来自应用程序的父密钥授权信息一起计算第一请求消息认证码;

步骤 b 所述计算第二请求消息认证码的方法为：密码设备应用接收到的访问密钥生成指令和已获取的现时标志，与已指定的父密钥授权信息一起计算第二请求消息认证码;

步骤 c 所述密码设备执行密码操作请求中所指示的操作的过程为：应用现时标志解密出访问密钥授权信息，执行密钥创建过程，生成访问密钥，然后应用已指定的父密钥将生成的访问密钥和该访问密钥的授权信息打包加密，将加密后的结果作为返回的结果信息；所述计算第一执行结果认证码的方法为：将返回的结果信息和现时标志一起用已指定的父密钥授权信息计算第一执行结果认证码;

步骤 d 所述计算第二执行结果认证码的方法为：密码服务提供模块根据接收到的信息，应用执行结果、已获取的现时标志，与访问密钥授权信息一起计算第二执行结果认证码。

3、根据权利要求 2 所述的方法，其特征在于，

如果访问主机是首次执行生成访问密钥指令，则所述父密钥授权信息是已预先设定的根密钥授权信息;

如果访问主机是非首次执行生成访问密钥指令，且已预先设定根密钥为该即将生成的访问密钥的父密钥，则所述父密钥授权信息是已预先设定的根密钥授权信息;

如果访问主机是非首次执行生成访问密钥指令，且已指定某个已存在的访问密钥 A 为该即将生成的访问密钥的父密钥，则在密码服务提供模块接收到的来自应用程序的密码操作请求为生成访问密钥的指令之前或之后，进一步包括：密码设备获取访问主机应用的访问密钥 A 及访问密钥 A 授权信息，且所述父密钥授权信息是被指定为父密钥的访问密钥 A 的访问密钥授权信息。

4、根据权利要求 1 所述的方法，其特征在于，

步骤 a 所述密码服务提供模块接收到的来自应用程序的密码操作请求为加解密操作指令，该指令中包含所应用的访问密钥、访问密钥授权信息及待加解密数据，所述计算第一请求消息认证码的方法为：密码服务提供模块应用接收到的加解密操作指令、已获取的现时标志，与来自应用程序的访问密钥授权信息一起计算第一请求消息认证码；

步骤 b 所述密码设备在密码服务提供模块接收到来自应用程序的加解密操作指令之前或之后，从密码服务提供模块获取该密码服务提供模块所在访问主机应用的访问密钥及访问密钥授权信息；所述计算第二请求消息认证码的方法为：密码设备应用接收到的加解密操作指令、已获取的现时标志与已获取的该访问主机所应用的访问密钥授权信息一起计算第二请求消息认证码；

步骤 c 所述密码设备执行密码操作请求中所指示的操作的过程为：利用该访问主机所应用的访问密钥对待加解密数据进行加解密操作，将加解密后的结果作为返回的结果信息；所述计算第一执行结果认证码的方法为：密码设备将自身的执行结果信息、已获取的现时标志，与访问密钥授权信息一起计算第一执行结果认证码；

步骤 d 所述计算第二执行结果认证码的方法为：密码服务提供模块根据接收到的信息，应用执行结果信息、已获取的现时标志，与访问密钥授权信息一起计算第二执行结果认证码。

5、根据权利要求 3 或 4 所述的方法，其特征在于，所述密码设备获取访问主机应用的访问密钥及访问密钥授权信息的方法为：

密码设备加载接收来自密码服务提供模块的该密码服务提供模块所在访问主机应用的访问密钥，用访问密钥的父密钥解密访问密钥获取该访问主机所应用的访问密钥明文及访问密钥授权信息的明文。

6、根据权利要求 1 所述的方法，其特征在于，步骤 b 所述返回错误信息的过程为：密码设备给密码核心服务模块返回错误信息，该信息经密码服务提供模块返回给应用程序。

7、根据权利要求2或4所述的方法，其特征在于，所述现时标志为：密码设备应密码服务提供模块在本次交互中的请求生成的数据串。

8、根据权利要求2或4所述的方法，其特征在于，所述现时标志为：由信息发送方自身当前生成的数据串与来自信息接收方的数据串共同组成的数据串，且所述信息发送方为密码设备，信息接收方为密码服务提供者，或者，所述信息发送方为密码服务提供者，信息接收方为密码设备。

一种访问密码设备的方法

技术领域

本发明涉及访问密码设备的技术领域，特别是指一种访问密码设备的方法。

背景技术

当今社会已进入信息化时代，计算机网络已逐渐应用于社会各个领域，伴随着国民经济信息化进程的推进和电子商务等网络新业务的兴起，社会对计算机网络的依赖程度越来越高。信息时代呼唤信息安全，而对数据进行加密是保护数据免受非法访问的常用方法。

目前，利用硬件，如加密卡等，进行密钥生成和加解密的操作具有速度快，不易篡改等优点，已经得到了广泛的应用。

在此，将具有加密卡，或具有类似加密卡功能的硬件，以及该硬件的驱动和所应用的数据库合起来称为密码设备，该密码设备一般将密钥信息存储在自身，通过限制访问权限达到对密钥进行保护的目的。在这种机制下，如果用户具有该密码设备的访问权限，则具有密钥的使用权限，可以利用该密码设备进行密钥生成，加解密数据等操作；如果用户不具有该密码设备的访问权限，则不能应用该密码设备。也就是说，上述密钥保护机制是基于对密码设备的访问权限的控制实现的。

具体应用时，密码设备的管理接口通常以动态链接库的形式提供一组函数接口，即由密码设备管理函数库构成密码设备的接口，执行密码操作的进程必须在本地调用该密码设备管理函数库才能访问到密码设备，驱动密码设备执行操作。根据现有的访问机制，远程访问密码设备很不安全，而且现有的密码设备也根本没有提供远程访问的接口。

上述访问密码设备的方法存在以下缺陷:

1）密码设备不能被远程访问。因为远程访问很不安全，而且现有的密码设备不支持远程访问。

2）每一密码设备只能由少数几个用户使用，如果同一密码设备的访问权限被多个用户共享，其秘密信息不再安全。

3）产生密钥、加解密等操作只能在具有密码设备及密码设备驱动的主机上执行，即只能在本地执行，在其他设备上无法执行。

4）密码设备有限的存储空间决定了其能够存放的密钥的个数有限。

发明内容

有鉴于此，本发明的目的在于提供一种访问密码设备的方法，不仅可以实现本地访问，还可以实现远程访问，同时能够保证信息的安全。

为达到上述目的，本发明的技术方案是这样实现的:

一种访问密码设备的方法，在访问主机上设置用于远程调用密码设备的密码服务提供模块，在被访问主机上设置用于接收远程调用，并驱动密码设备执行操作的密码核心服务模块，创建每一密钥时为所创建的密钥设置密钥授权信息，该方法还包括以下步骤:

a、密码服务提供模块接收到来自应用程序的密码操作指令后，应用密钥授权信息对所述密码操作指令计算第一请求消息认证码，之后，将包含第一请求消息认证码和所述密码操作指令的密码操作请求通过密码核心服务模块发送给密码设备;

b、密码设备根据接收到的密码操作指令，利用已获得的密钥授权信息计算第二请求消息认证码，并判断计算出的第二请求消息认证码与接收到的第一请求消息认证码是否相同，如果相同，则执行步骤 c，否则返回错误信息，结束本流程;

c、密码设备执行密码操作请求中所指示的操作，并应用密钥授权信息对执行结果计算第一执行结果认证码，然后，将包含第一执行结果认证码和执行结

果的信息发送给密码核心服务模块，由密码核心服务模块将接收到的信息解析为密码服务提供模块能够识别的信息后，再发送给密码服务提供模块；

d、密码服务提供模块应用密钥授权信息对接收到的执行结果计算第二执行结果认证码，并判断计算出的第二执行结果认证码与接收到的第一执行结果认证码是否相同，如果相同，则给应用程序返回执行结果信息，结束本流程；否则，给应用程序返回错误信息，结束本流程。

较佳地，步骤 a 所述密码服务提供模块接收到的来自应用程序的密码操作请求为生成访问密钥的指令，该指令中包含有为即将生成的访问密钥设置的访问密钥授权信息，以及访问密钥的算法信息；所述计算第一请求消息认证码的方法为：获取现时标志，应用已获取的现时标志对所述访问密钥授权信息进行加密，将加密后的访问授权密钥信息、访问密钥的算法信息、已获取的现时标志与来自应用程序的父密钥授权信息一起计算第一请求消息认证码；

步骤 b 所述计算第二请求消息认证码的方法为：密码设备应用接收到的访问密钥生成指令和已获取的现时标志，与已指定的父密钥授权信息一起计算第二请求消息认证码；

步骤 c 所述密码设备执行密码操作请求中所指示的操作的过程为：应用现时标志解密出访问密钥授权信息，执行密钥创建过程，生成访问密钥，然后应用已指定的父密钥将生成的访问密钥和该访问密钥的授权信息打包加密，将加密后的结果作为返回的结果信息；所述计算第一执行结果认证码的方法为：将返回的结果信息和现时标志一起用已指定的父密钥授权信息计算第一执行结果认证码；

步骤 d 所述计算第二执行结果认证码的方法为：密码服务提供模块根据接收到的信息，应用执行结果、已获取的现时标志，与访问密钥授权信息一起计算第二执行结果认证码。

较佳地，如果访问主机是首次执行生成访问密钥指令，则所述父密钥授权信息是已预先设定的根密钥授权信息；

如果访问主机是非首次执行生成访问密钥指令，且已预先设定根密钥为该即将生成的访问密钥的父密钥，则所述父密钥授权信息是已预先设定的根密钥授权信息；

如果访问主机是非首次执行生成访问密钥指令，且已指定某个已存在的访问密钥 A 为该即将生成的访问密钥的父密钥，则在密码服务提供模块接收到的来自应用程序的密码操作请求为生成访问密钥的指令之前或之后，进一步包括：密码设备获取访问主机应用的访问密钥 A 及访问密钥 A 授权信息，且所述父密钥授权信息是被指定为父密钥的访问密钥 A 的访问密钥授权信息。

较佳地，步骤 a 所述密码服务提供模块接收到的来自应用程序的密码操作请求为加解密操作指令，该指令中包含所应用的访问密钥、访问密钥授权信息及待加解密数据，所述计算第一请求消息认证码的方法为：密码服务提供模块应用接收到的加解密操作指令、已获取的现时标志，与来自应用程序的访问密钥授权信息一起计算第一请求消息认证码；

步骤 b 所述密码设备在密码服务提供模块接收到来自应用程序的加解密操作指令之前或之后，从密码服务提供模块获取该密码服务提供模块所在访问主机应用的访问密钥及访问密钥授权信息；所述计算第二请求消息认证码的方法为：密码设备应用接收到的加解密操作指令、已获取的现时标志与已获取的该访问主机所应用的访问密钥授权信息一起计算第二请求消息认证码；

步骤 c 所述密码设备执行密码操作请求中所指示的操作的过程为：利用该访问主机所应用的访问密钥对待加解密数据进行加解密操作，将加解密后的结果作为返回的结果信息；所述计算第一执行结果认证码的方法为：密码设备将自身的执行结果信息、已获取的现时标志，与访问密钥授权信息一起计算第一执行结果认证码；

步骤 d 所述计算第二执行结果认证码的方法为：密码服务提供模块根据接收到的信息，应用执行结果信息、已获取的现时标志，与访问密钥授权信息一起计算第二执行结果认证码。

较佳地，所述密码设备获取访问主机应用的访问密钥及访问密钥授权信息的方法为：

密码设备加载接收来自密码服务提供模块的该密码服务提供模块所在访问主机应用的访问密钥，用访问密钥的父密钥解密访问密钥获取该访问主机所应用的访问密钥明文及访问密钥授权信息的明文。

较佳地，步骤 b 所述返回错误信息的过程为：密码设备给密码核心服务模块返回错误信息，该信息经密码服务提供模块返回给应用程序。

较佳地，所述现时标志为：密码设备应密码服务提供模块在本次交互中的请求生成的数据串。

较佳地，所述现时标志为：由信息发送方自身当前生成的数据串与来自信息接收方的数据串共同组成的数据串，且所述信息发送方为密码设备，信息接收方为密码服务提供者，或者，所述信息发送方为密码服务提供者，信息接收方为密码设备。

从上述技术方案中可以看出，本发明的关键是：在密钥创建时为所创建的密钥设置密钥授权信息，在密钥使用过程中发送方和接收方之间传送的信息，均应用密钥授权信息为其计算认证码，然后再将待传送的信息和已计算出的认证码传送给对方，接收方则根据认证码验证消息的完整性，以鉴别信息来源是否可靠，且传送途中是否被篡改过，当验证成功后，再执行后续操作。应用本发明，将密钥保护机制由设备访问权限控制转为密钥使用权限控制，这样，本地操作不再是必须的，因而密码设备既可以被远程访问，也可以在本地访问。同时，由于本发明提供了信息的鉴别、完整性检查，解决了原有密钥保护机制下密码设备仅由一个用户在本地使用的缺陷，使得多个用户能够应用远程的不具备密码设备的主机访问密码设备，而仍然能够保证信息的安全特性。由于本发明采用一次一密的加密方式，因而能够有效地抵御网络监听者的重播攻击。另外，由于访问密码设备所需的密钥存储在密码设备之外，因此，所存放的密钥的个数可以大大增加，从理论上讲，所存放的

个数可以是无限的。

附图说明

图 1 所示为应用本发明一实施例的生成访问密钥的流程示意图；

图 2 所示为应用本发明一实施例的驱动密码设备进行加解密操作的流程示意图。

具体实施方式

下面结合附图，对本发明再做进一步地详细说明。

在本发明中，如前所述，将密码设备管理函数库、密码设备驱动和密码设备本身合起来称为“密码设备”，在密码设备管理函数库之上设置用于接收远程调用，并驱动密码设备执行操作的模块，并称该模块为“密码核心服务模块”，该密码设备和密码核心服务模块均位于被访问主机即密码设备所在的主机中；同时，在访问主机上设置用于执行远程调用密码设备的模块，并称该模块为“密码服务提供模块”。在实际应用中，访问主机和被访问主机可以是同一台主机，也可以是不同的主机，这样，既可实现本地调用密码设备，又可实现异地即远程调用密码设备。

众所周知，任一非对称密钥的密钥信息至少包括算法信息、私钥数据和公钥信息，其中的算法信息中包括算法标志、加密算法、签名算法、密钥长度，以及其他一些必要的参数信息等。

本发明预先在密码设备内创建一根密钥，该根密钥永远不离开密码设备。上述根密钥具备任一非对称密钥都包含的最基本的密钥信息，并且，在创建上述根密钥的同时为该根密钥设置密钥授权信息，并将其称之为根密钥授权信息。所谓密钥授权信息，是用于检验密钥使用者是否有权限使用该密钥的信息，其通常为一数据串，由密钥的创建者在创建密钥时设定。如果访问主机内的应用程序需要应用密码设备进行密码操作，其必须先获取用于驱动密码设备进行操作的密钥，并设定该密钥的密钥授权信息，因为密码设备

是根据使用者是否持有正确密钥授权信息来决定是否执行指令所指示的操作的。在此，将驱动密码设备进行密码操作的密钥称为访问密钥，将访问密钥的密钥授权信息称为访问密钥授权信息。

下面具体说明生成访问密钥及访问密钥授权信息，并应用访问密钥驱动密码设备执行加解密操作的过程。

图 1 所示为应用本发明一实施例的生成访问密钥的流程示意图。

步骤 101，访问主机中的应用程序发出生成访问密钥的指令。该指令中包含有为即将生成的访问密钥指定的父密钥，父密钥授权信息，为即将生成的访问密钥设置的访问密钥授权信息，以及访问密钥的算法等信息。

步骤 102，访问主机中的密码服务提供模块接收到上述指令后，向被访问主机中的密码核心服务模块发送现时标志请求，以获取现时标志。该现时标志实际为一随机的数据串，用于以后的加解密操作，以保证通信过程的安全性。

步骤 103，被访问主机中的密码核心服务模块将接收到的请求信息转换为密码设备能够识别的语言后，向密码设备发送现时标志请求。

步骤 104~步骤 105，被访问主机中的密码设备生成一数据串并保存该数据串为现时标志，之后将该数据串作为现时标志返回给密码核心服务模块，由密码核心服务模块将该现时标志返回给访问主机中的密码服务提供模块。

步骤 106~步骤 107，密码服务提供模块应用从被访问主机中获取的现时标志对访问密钥授权信息进行加密，之后，将加密后的访问授权密钥信息、访问密钥的算法信息、已获取的现时标志与来自应用程序的父密钥授权信息一起计算第一请求消息认证码 H1，然后，将包含生成访问密钥指令和第一请求消息认证码 H1 的密钥生成请求发送给被访问主机中的密码核心服务模块。

步骤 108，密码核心服务模块将接收到的请求信息转换为密码设备能够识别的语言后，向密码设备发送该密码操作请求信息。

步骤 109，密码设备应用接收到的访问密钥生成指令和自身已保存的现时标志，与已加载的父密钥的授权信息一起计算第二请求消息认证码 H2。之后，密码设备判断第一请求消息认证码 H1 与第二请求消息认证码 H2 是否相同，如果相同，则表明发送者持有正确的父密钥授权信息，且该密码操作请求信息在网络传送的过程中未经篡改，否则，表明发送者没有正确的父密钥授权信息，或者，该密码操作请求信息在网络传送的过程中已经被篡改。

在本实施例中，假设 H1 与 H2 相同，则密码设备应用现时标志对已加密的访问密钥授权信息进行解密，执行密钥创建过程，生成访问密钥。之后，密码设备应用上述父密钥的公钥将生成的访问密钥和该访问密钥的授权信息打包加密，将加密后的结果作为返回的结果信息。紧接着，密码设备将结果信息和现时标志一起用父密钥授权信息计算第一执行结果认证码 G1，然后执行步骤 110。

如果 H1 和 H2 不同，则密码设备给密码核心服务模块返回错误信息，该信息经密码服务提供模块返回给应用程序，之后结束本流程。

步骤 110~步骤 111，密码设备给密码核心服务模块发送执行结果信息，由密码核心服务模块将接收到的信息解析为密码服务提供模块能够识别的信息后，再发送给密码服务提供模块。该信息中包含执行结果和第一执行结果认证码 G1。

步骤 112，密码服务提供模块根据接收到的信息，应用执行结果和现时标志与父密钥授权信息一起计算第二执行结果认证码 G2。之后，密码服务提供模块判断第一执行结果认证码 G1 和第二执行结果认证码 G2 是否相同，如果相同，则表明该返回的执行结果来自密码设备，且该执行结果在网络传送的过程中未经篡改，否则，表明该返回的执行结果并非来自密码设备，或者该执行结果在网络传送的过程中已经篡改。在本实施例中，假设 G1 与 G2 相同，执行步骤 113。

如果 G1 与 G2 不同，则密码服务提供模块给应用程序返回错误信息，

结束本流程。

步骤 113，密码服务提供模块给应用程序返回结果信息，该结果信息为应用父密钥的公钥对访问密钥及访问密钥授权信息打包加密后的信息。也就是说，密码设备所生成的访问密钥，只有在密码设备中由父密钥的私钥解密后才能应用，对于访问主机这一端而言，其只拥有一个加密后的访问密钥信息。

至此，访问主机获取了访问密钥。由于访问密钥存储在密码设备之外，即存储在访问主机中，因此，所存放的密钥的个数可以大大增加，从理论上讲，所存放的个数可以是无限的。

对于图 1 所示流程，如果访问主机是首次执行生成访问密钥指令即首次创建访问密钥，则上述流程中的父密钥授权信息是已预先设定的根密钥授权信息；如果访问主机是非首次执行生成访问密钥指令即非首次创建访问密钥，且创建时指定根密钥为该即将创建的访问密钥的父密钥，则上述流程中的父密钥授权信息仍然是指已预先设定的根密钥授权信息；如果访问主机是非首次执行生成访问密钥指令即非首次创建访问密钥，且创建时指定某个已创建的访问密钥 A 为该即将创建的访问密钥的父密钥，则上述父密钥授权信息是被指定为父密钥的访问密钥 A 的访问密钥授权信息。当然，在最后一种情况下，访问主机应在应用程序发出生成访问密钥的指令之前或之后，将被指定为父密钥的访问密钥 A 的信息发送给密码设备，密码设备对该访问密钥 A 的信息进行解密，获取该访问密钥的明文及该访问密钥的密钥授权信息的明文。

图 2 所示为应用本发明一实施例的驱动密码设备进行加解密操作的流程示意图。

步骤 201，访问主机中的应用程序发出执行加解密操作的指令。该指令中包含有指示应用哪一个访问密钥的信息、该访问密钥的密钥授权信息以及待加解密的数据。通常，应用密钥句柄指示出需要哪一个访问密钥的信息。

步骤202，访问主机中的密码服务提供模块接收到上述指令后，将应用父密钥的公钥打包加密后的访问密钥和该访问密钥的授权信息通过密码核心服务模块发送给密码设备，密码设备应用父密钥的私钥解密接收到的信息，从而获取该访问主机所应用的访问密钥及访问密钥授权信息，访问主机中的密码服务提供模块在得到密码设备的成功响应后执行步骤203。

在具体实现时，本步骤也可以在步骤201之前执行，即在访问主机中的应用程序发出执行加解密操作的指令之前，密码服务提供模块将本访问主机所应用的访问密钥及访问密钥授权信息通过密码核心模块发送给密码设备，密码设备应用父密钥的私钥解密接收到的信息，获取该访问主机所应用的访问密钥及访问密钥授权信息。

步骤203，访问主机中的密码服务提供模块向被访问主机中的密码核心服务模块发送现时标志请求，以获取现时标志。该现时标志实际为一随机的数据串，用于以后的加解密操作，以保证通信过程的安全性。

步骤204，被访问主机中的密码核心服务模块将接收到的请求信息转换为密码设备能够识别的语言后，向密码设备发送现时标志请求。

步骤205~步骤206，被访问主机中的密码设备生成一数据串并保存该数据串为现时标志，之后将该数据串作为现时标志返回给密码核心服务模块，由密码核心服务模块将该现时标志返回给访问主机中的密码服务提供模块。

步骤207~步骤208，密码服务提供模块将接收到的加解密操作指令和从被访问主机中获取的现时标志，与来自应用程序的访问密钥授权信息一起计算第一请求消息认证码 H1，然后，将包含加解密操作指令和第一请求消息认证码 H1 的加解密操作请求发送给被访问主机中的密码核心服务模块。

步骤209，密码核心服务模块将接收到的请求信息转换为密码设备能够识别的语言后，向密码设备发送该密码操作请求信息。

步骤210，密码设备应用加解密请求信息中的加解密操作指令和已保存的现时标志，与已获得的访问密钥授权信息一起计算第二请求消息认证码

H2。之后，密码设备判断第一请求消息认证码 H1 与第二请求消息认证码 H2 是否相同，如果相同，则表明发送者持有正确的访问密钥授权信息，且该加解密操作请求在网络传送的过程中未经篡改，否则，表明发送者没有正确的访问密钥授权信息，或者，该加解密操作请求信息在网络传送的过程中已经篡改。在本实施例中，假设 H1 与 H2 相同，则密码设备应用访问密钥对操作指令中的数据信息执行加解密操作，然后，将加解密后的数据信息即执行结果和现时标志，与访问密钥授权信息一起计算第一执行结果认证码 G1，然后执行步骤 211。

如果 H1 和 H2 不同，则密码设备给密码核心服务模块返回错误信息，该信息经密码服务提供模块返回给应用程序，之后结束本流程。

步骤 211~步骤 212，密码设备给密码核心服务模块发送执行结果信息，由密码核心服务模块将接收到的信息解析为密码服务提供模块能够识别的信息后，再发送给密码服务提供模块。该信息中包含执行结果和第一执行结果认证码 G1。

步骤 213，密码服务提供模块根据接收到的信息，应用执行结果和现时标志与访问密钥授权信息一起计算第二执行结果认证码 G2。之后，密码服务提供模块判断第一执行结果认证码 G1 和第二执行结果认证码 G2 是否相同，如果相同，则表明该返回的执行结果来自密码设备，且该执行结果在网络传送的过程中未经篡改，否则，表明该返回的执行结果并非来自密码设备，或者该执行结果在网络传送的过程中已经篡改。在本实施例中，假设 G1 与 G2 相同，执行步骤 214。

如果 G1 与 G2 不同，则密码服务提供模块给应用程序返回错误信息，结束本流程。

步骤 214，密码服务提供模块给应用程序返回执行结果信息，即给应用程序返回加解密后的数据信息。

针对上述两个流程，在具体实现时，应用程序和密码服务提供模块之间

通过函数调用实现信息传递，密码核心服务模块与密码设备之间也是通过函数调用实现信息传递，密码服务提供模块与密码核心服务模块之间通过远程调用实现信息传递。

这样，用户既可以在本地访问密码设备，也可以在远程访问密码设备，而且同一密码设备可以被多个用户同时访问。由于每一用户应用各自的访问密钥，因此保证了信息的安全。

以上所述仅为一具体实施例，当然也可以有其他的实现方式。比如，可以由信息发送方自身当前生成的数据串与来自信息接收方的数据串共同组成的数据串作为当前的现时标志，以更好地保证信息安全。其中，所述信息发送方为密码设备，信息接收方为密码服务提供者，或者，所述信息发送方为密码服务提供者，信息接收方为密码设备。

基于上述实施方式，在步骤 106~步骤 107 和步骤 207~步骤 208 中，访问主机内的密码服务提供模块接收到来自密码设备的现时标志后，自身再产生一数据串 L1，将自身产生的数据串 L1 与从密码设备接收到的现时标志和起来作为当前计算第一消息认证码 H1 的现时标志，之后，将包含密码操作请求和第一请求消息认证码 H1 以及自身产生的数据串 L1 的操作请求发送给被访问主机中的密码核心服务模块。相应地，在步骤 109 和步骤 210 中，密码设备从请求信息中获取操作指令和密码服务提供模块生成的数据串 L1，之后，将自身生成的现时标志和该数据串 L1 合起来作为当前计算第二请求消息认证码 H2 的现时标志，然后，再执行后续操作。当密码设备生成执行结果信息后，密码设备再次产生一数据串 L2，将该数据串 L2 与已获得的数据串 L1 合起来作为当前计算第一执行结果认证码 G1 的现时标志，之后，将包含执行结果、第一执行结果认证码 G1 和数据串 L2 的执行结果信息发送给密码服务提供模块。相应地，在步骤 112 和步骤 213 中，密码服务提供模块根据接收到的信息，获取密码设备再次生成的数据串 L2，将该数据串 L2 与自身已生成的数据串 L1 合起来作为当前计算第二执行结果认证

码 G2 的现时标志，然后，再执行后续操作。这样，可以更好地抵御抗重播攻击。

以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

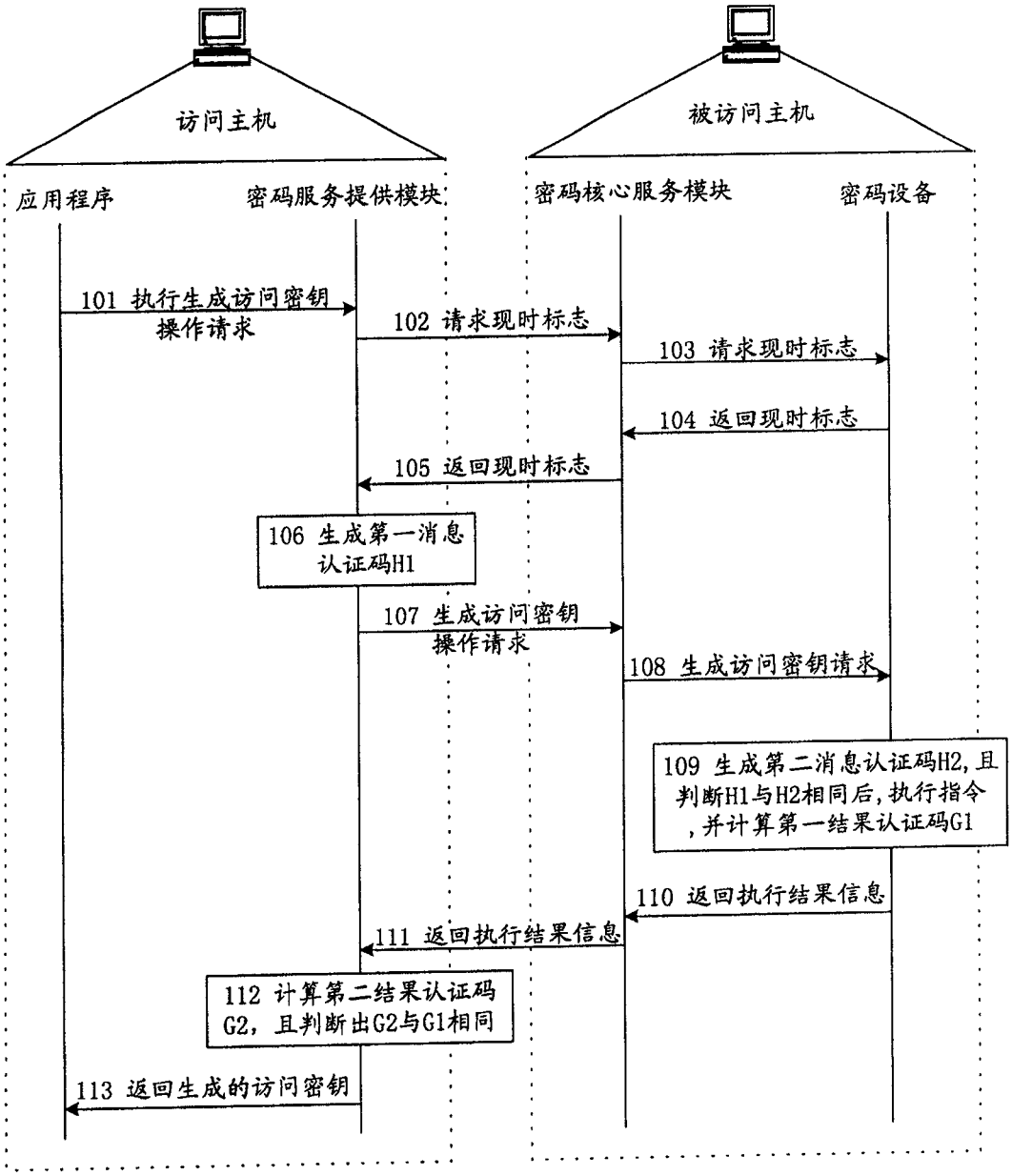

访问主机
被访问主机
应用程序
密码服务提供模块
密码核心服务模块
密码设备
101 执行生成访问密钥操作请求
102 请求现时标志
103 请求现时标志
104 返回现时标志
105 返回现时标志
106 生成第一消息认证码H1
107 生成访问密钥操作请求
108 生成访问密钥请求
109 生成第二消息认证码H2,且判断H1与H2相同后,执行指令,并计算第一结果认证码G1
110 返回执行结果信息
111 返回执行结果信息
112 计算第二结果认证码G2,且判断出G2与G1相同
113 返回生成的访问密钥

图 1

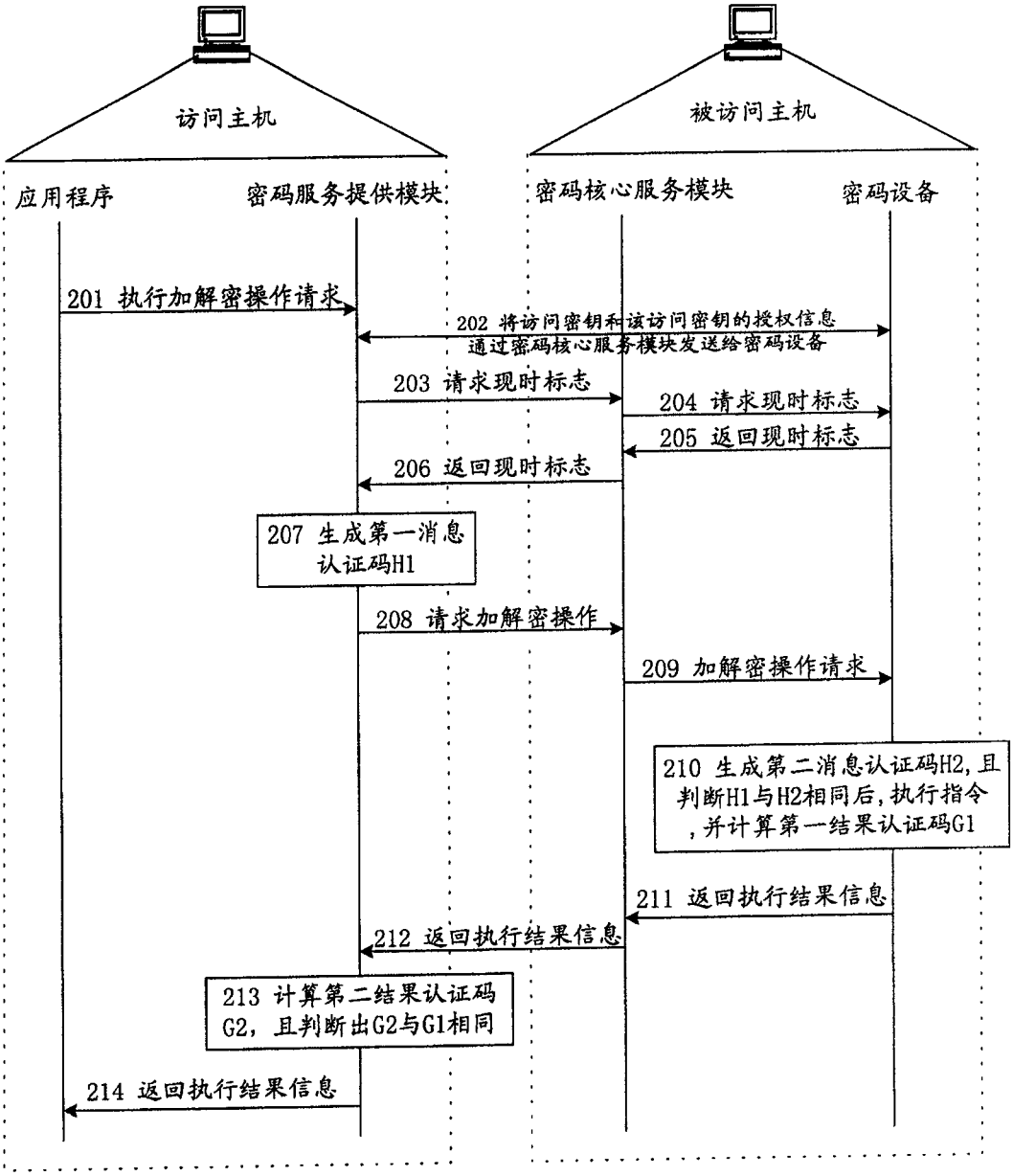

访问主机
被访问主机
应用程序
密码服务提供模块
密码核心服务模块
密码设备
201 执行加解密操作请求
202 将访问密钥和该访问密钥的授权信息
通过密码核心服务模块发送给密码设备
203 请求现时标志
204 请求现时标志
205 返回现时标志
206 返回现时标志
207 生成第一消息
认证码H1
208 请求加解密操作
209 加解密操作请求
210 生成第二消息认证码H2,且
判断H1与H2相同后,执行指令
,并计算第一结果认证码G1
211 返回执行结果信息
212 返回执行结果信息
213 计算第二结果认证码
G2，且判断出G2与G1相同
214 返回执行结果信息

图 2