(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 120513601 A
(43)申请公布日 2025.08.19

(21)申请号 202480007548.0

(22)申请日 2024.01.08

(30)优先权数据
23151546.1 2023.01.13 EP

(85)PCT国际申请进入国家阶段日
2025.07.11

(86)PCT国际申请的申请数据
PCT/FI2024/050005 2024.01.08

(87)PCT国际申请的公布数据
WO2024/149934 EN 2024.07.18

(71)申请人 古鲁洛吉克微系统公司
地址 芬兰图尔库

(72)发明人 T·卡尔凯宁

(74)专利代理机构 北京三友知识产权代理有限公司 11127
专利代理师 师玮 党晓林

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 9/32(2006.01)
H04L 9/40(2006.01)
H04L 9/30(2006.01)

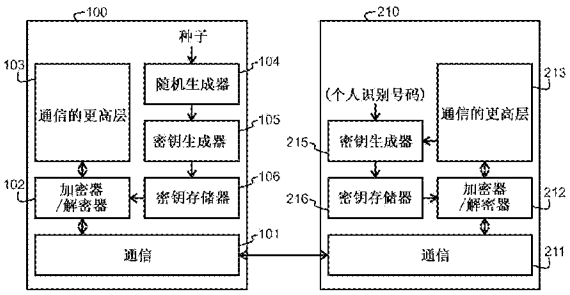
权利要求书2页 说明书10页 附图4页

(54)发明名称

使用用户设备利用秘密的方法和装置

(57)摘要

用户设备(210)可以在密码学保护的通信和/或数据的密码学认证中使用秘密。通信部分(211)被配置为将从可信外部源(100)接收到的秘密转发到密钥生成器(215)。密钥生成器(215)被配置为使用所述秘密作为密码种子来生成一个或更多个密钥,并且将所述一个或更多个密钥存储在密钥存储器(216)中。通信加密器和解密器部分(212)被配置为从所述密钥存储器(216)检索所述一个或更多个密钥,并且使用所述一个或更多个密钥对通过所述通信部分(211)执行的通信进行密码学保护。



CN 120513601 A

1.一种使用户设备(210)在以下的至少一项中使用秘密的装置:密码学保护的通信、数据的密码学认证,所述装置包括:

-通信部分(211);

-通信加密器和解密器部分(212);

-密钥生成器(215);以及

-密钥存储器(216);

其中,所述通信部分(211)被配置为将从可信外部源(100)接收到的秘密转发到所述密钥生成器(215),并且

其中,所述密钥生成器(215)被配置为使用所述秘密作为密码种子来生成一个或更多个密钥,并且将所述一个或更多个密钥存储在所述密钥存储器(216)中,

并且其中,所述通信加密器和解密器部分(212)被配置为:

-在将所述秘密转发到所述密钥生成器之前,使用所述秘密的假定发送者的公钥来验证与所述秘密关联地接收到的数字签名,以对所述接收的秘密的不变性和完整性进行密码学验证,以及

-从所述密钥存储器(216)检索所述一个或更多个密钥,并且使用所述一个或更多个密钥对通过所述通信部分(211)执行的通信进行密码学保护。

2.根据权利要求1所述的装置,其中:

-所述通信部分被配置为与对等方建立安全数字通信信道,并且此后通过所述安全数字通信信道接收所述秘密,从而使所述对等方表现为所述可信外部源。

3.根据权利要求2所述的装置,其中,所述通信部分被配置为使用传输层安全(也称为TLS)标准来建立所述安全数字通信信道。

4.根据前述权利要求中任一项所述的装置,其中,所述通信部分被配置为当所述通信加密器和解密器部分已从所述密钥存储器检索到所述一个或更多个密钥时,通过与用于通过所述通信部分执行的所述密码学保护的通信的信道不同的信道来接收所述秘密。

5.根据权利要求4所述的装置,其中,所述通信部分被配置为使用以下中的至少一项作为所述不同信道:电缆或光纤通信、近场无线通信、通过手动操作的用户接口的通信。

6.根据前述权利要求中任一项所述的装置,其中,所述通信加密器和解密器部分被配置为通过将与所述秘密相关联地接收到的公钥与所述秘密的所述假定发送者的单独获得的公钥进行比较来执行所述密码学验证。

7.根据前述权利要求中任一项所述的装置,其中,所述密钥生成器被配置为执行以下中的至少一项以生成所述一个或更多个密钥:

-使用所述秘密作为密钥生成算法的种子;

-使用所述秘密和从所述装置的用户接收到的信息作为密钥生成算法的输入信息。

8.根据权利要求8所述的装置,其中,所述装置被配置为在立即使用由所述密钥生成器生成的所述一个或更多个密钥中的至少一个密钥之后永久地丢弃所述至少一个密钥。

9.一种使用户设备在以下中的至少一项中使用秘密的方法:密码学保护的通信、数据的密码学认证,所述方法包括所述用户设备执行以下步骤:

-从所述用户设备外部的可信源接收秘密,

-对所述接收的秘密的不变性和完整性进行密码学验证,其中,所述密码学验证涉及使

用所述秘密的假定发送者的公钥来验证与所述秘密相关联地接收到的数字签名，

-在所述密码学验证之后，使用所述秘密作为密码种子来生成一个或更多个密钥，

-存储所述一个或更多个密钥以供以后使用，以及

-检索所述一个或更多个密钥，并且使用所述一个或更多个密钥对由所述用户设备执行的通信进行密码学保护。

10.根据权利要求9所述的方法，所述方法包括：

-与对等方建立安全数字通信信道，以及

-此后通过所述安全数字通信信道接收所述秘密，从而使所述对等方表现为所述可信外部源。

11.根据权利要求10所述的方法，其中，建立所述安全数字通信信道包括以下中的至少一项：

-使用传输层安全(也称为TLS)标准来建立所述安全数字通信信道；

-使用电缆或光纤通信作为所述安全数字通信信道；

-使用近场无线通信作为所述安全数字通信信道；

-使用通过手动操作的用户接口的通信作为所述安全数字通信信道。

12.根据权利要求9至11中任一项所述的方法，其中，所述密码学验证涉及将与所述秘密相关联地接收到的公钥与所述秘密的所述假定发送者的单独获得的公钥进行比较。

13.根据权利要求9至12中任一项所述的方法，其中，所述生成所述一个或更多个密钥包括以下中的至少一项：

-使用所述秘密作为密钥生成算法的种子；

-使用所述秘密和从装置的用户接收到的信息作为密钥生成算法的输入信息。

14.根据权利要求13所述的方法，所述方法包括在立即使用所述生成的一个或更多个密钥中的至少一个密钥之后永久地丢弃所述至少一个密钥。

15.一种计算机程序产品，所述计算机程序产品包括一个或更多个机器可读指令的一个或更多个集合，所述一个或更多个机器可读指令在由一个或更多个处理器执行时使得实现根据权利要求9至14中任一项所述的方法。

使用户设备利用秘密的方法和装置

技术领域

[0001] 本发明总体上涉及在数字设备之间的通信中使用数字服务所需的安全技术领域。具体而言,本发明涉及在用户设备中建立用于这种通信的秘密的任务,而不必依赖于用户设备的固有特征。这样的秘密的示例包括但不限于用户的加密密钥和签名密钥。

背景技术

[0002] 数字通信中的安全性涉及多个方面,诸如机密性(只有授权方可以访问一条信息)、认证(通信方必须确定他们正在与谁通信)、完整性(一条信息未被未经允许地修改)和不可否认性(一方不能成功地否认曾经发送了某条信息)。所有这些安全性方面必须最终体现在一条秘密的数字信息上(通常简明地称为秘密(secret))。为了提供足够的安全性以防止破解尝试,所述秘密必须随机地得到。

[0003] 数字设备根据自然法则以确定性方式工作,这使得它们产生任何种类的真实随机性成为一种挑战。为了可验证的信息机密性和保护,知道并验证所讨论的随机性的产生方式和来源是很重要的。理论上,随机性看上去可能是正确的,甚至可以通过各种随机性测试方法进行测试,但如果随机性是基于其变量可能被以某种方式操纵或预测的计算或逻辑函数确定性地产生的,则恶意方可能通过建模或蛮力破坏所述随机性。为此,代替伪随机性,已经开发了基于真随机性的各种方法。这样的方法的示例涉及从计算单元外部的数据流中收集随机性,例如难以预测的自然产生的噪声。

[0004] 广泛使用的PKI(公钥基础设施)技术是如何将秘密用于安全数字通信的一个很好的例子。通信设备可以随机地生成秘密密钥并使用数学算法来得到对应的公钥。公钥可以自由分发并用于将发往所述设备的通信加密。由于所讨论的设备是唯一知道秘密密钥的设备,所以没有其他人可以解密这种加密的通信。设备还可以使用其秘密密钥来对发出的传输进行数字签名,使得其他人可以通过成功地使用对应的公钥来验证正确的发起方。在这种情况下,信任的必要先决条件是在生成秘密密钥时最初涉及足够的随机性,使得恶意方不能使用公开可用的信息来猜测出秘密密钥。

[0005] 秘密密钥和公钥的生成和使用中所涉及的算法的示例是例如RSA(Rivest-Shamir-Adleman)、DSA(数字签名算法)和ECC(椭圆曲线密码术)。作为示例,如果使用最后提到的算法,则秘密密钥被称为URT_{SK},并且公钥被称为URT_{PK},并且可以使用称为Curve25519的算法从秘密密钥得到公钥。

[0006] 作为用例的示例,可以假设A方与B方之间的数字通信,其中A是中央运行的数字服务,并且B是个人用户。A方的装备可能已经由A自己组装和编程,并且由可信中立实体C验证用于安全操作。因此,可以信任该设备为A方随机生成用于通信的秘密的能力。另一方面,B方使用诸如智能手机或笔记本计算机的普通用户设备,这样的设备可能包括或不包括诸如被专门设计和编程以生成秘密的电路的固有特征。用户设备已经在国家X中被设计、制造和编程,并且如果存在所述电路,则其可以源自国家Y。B的用户设备生成足够随机性的秘密以供B方在通信中使用的能力取决于许多因素,其中很少或没有一个可以被A方或B方中的任

何一个检查或真正依赖。即使制造商确保他们的产品符合关于随机性的某些标准，也有工业、商业甚至政府级别的参与者可能既有动机有有手段在表面上似乎已通过验证的保密性的算法和硬件解决方案中植入后门。

[0007] 现有技术文献US2018/0026950A1描述了一种客户端应用，该客户端应用使用应用层密码密钥以密码方式保护应用数据。

[0008] 另一现有技术文献US2022/0070666A1描述了一种用于医疗传感器与计算设备之间的安全通信的方法。

[0009] 另一现有技术文献US10,963,593B1描述了在利用密钥管理系统和其他密码服务提供商的环境中增强信息安全的技术。

发明内容

[0010] 提供本发明内容是为了以简化的形式介绍一些概念，这些概念将在下面的具体实施方式中进一步描述。本发明内容不旨在标识所要求保护的主题的关键特征或必要特征，也不旨在用于限制所要求保护的主题的范围。

[0011] 目的是提供用于确保各方之间的安全数字通信而不必依赖于未知来源的随机性的方法和装置。

[0012] 根据第一方面，提供了一种用于使用户设备在密码学保护的通信和/或数据的密码认证中利用秘密的装置。该装置包括通信部分、通信加密器和解密器部分、密钥生成器和密钥存储器。通信部分被配置为将从可信外部源接收到的秘密转发到所述密钥生成器。所述密钥生成器被配置为使用所述秘密作为密码种子来生成一个或更多个密钥并将所述一个或更多个密钥存储在所述密钥存储器中。所述通信加密器和解密器部分被配置为在所述秘密被转发到所述密钥生成器之前，使用所述秘密的假定发送者的公钥来验证与所述秘密相关联地接收到的数字签名，以对所述接收的秘密的不变性和完整性进行密码学验证。所述通信加密器和解密器部分被配置为从所述密钥存储器检索所述一个或更多个密钥，并使用所述一个或更多个密钥对通过所述通信部分执行的通信进行密码学保护。

[0013] 根据实施方式，所述通信部分被配置为与对等方建立安全数字通信信道，并且此后通过所述安全数字通信信道接收所述秘密，从而使所述对等方表现为所述可信外部源。这至少涉及以下优点：人们可以依赖于在对等方的环境中生成的秘密的可信的高熵性质，并且仍然在所述装置中实现足够的数字安全性。

[0014] 根据实施方式，所述通信部分被配置为使用传输层安全(也称为TLS)标准来建立所述安全数字通信信道。这至少涉及可以使用标准化和公知方法的优点，而不必对所涉及的装置和软件提出非常特定的要求。

[0015] 根据一个实施方式，所述通信部分被配置为通过一不同信道来接收所述密钥，该信道不同于用于在所述通信加密器和解密器部分已从所述密钥存储器检索到所述一个或更多个密钥时通过所述通信部分执行的所述密码学保护的通信的信道。这至少涉及以下优点：当接收秘密时，可以避免用于所述密码学保护的通信的所述信道中涉及的潜在安全风险。

[0016] 根据实施方式，所述通信部分被配置为使用以下中的至少一个作为所述不同信道：光纤通信、近场无线通信、通过手动操作的用户接口的通信。这至少涉及以下优点：可以

实现与其他信道的充分区别,从而相应地提高安全性。

[0017] 根据实施方式,通信加密器和解密器部分被配置为通过将与所述秘密相关联地接收到的公钥与所述秘密的假定发送者的单独获得的公钥进行比较来执行所述密码学验证。这至少涉及以下优点:可以基于某些已知方法的知识来评估验证的可靠性。

[0018] 根据实施方式,所述密钥生成器被配置为执行以下中的至少一个以生成所述一个或更多个密钥:使用所述秘密作为密钥生成算法的种子;使用所述秘密和从所述装置的用户接收到的信息作为密钥生成算法的输入信息。这至少涉及以下优点:即使所述秘密的保密性遭到破坏,在破坏密钥生成算法的结果所用于的任何用途的安全性方面,仍会存在进一步的障碍。

[0019] 根据实施方式,所述装置被配置为在由密钥生成器生成的所述一个或更多个密钥中的至少一个密钥的立即使用之后永久地丢弃该密钥。这至少涉及以下优点:未被授权方对由所述装置存储的数据的非预期中间访问不会泄露丢弃的密钥,因为该密钥每次都将被重新生成,仅用于立即使用,然后再次被丢弃。

[0020] 根据第二方面,提供了一种使用户设备在以下至少一项中利用秘密的方法:通信的密码学保护;数据的密码认证。该方法包括用户设备从可信外部源接收秘密;对所述接收的秘密的不变性和完整性进行密码学验证,其中,所述密码学验证涉及使用所述秘密的假定发送者的公钥来验证与所述秘密相关联地接收到的数字签名;以及在所述密码学验证之后,使用所述秘密作为密码种子来生成一个或更多个密钥。该方法包括存储所述一个或更多个密钥以供以后使用,以及检索所述一个或更多个密钥并使用所述一个或更多个密钥以密码方式保护由所述用户设备执行的通信。

[0021] 根据一实施方式,该方法包括与对等方建立安全数字通信信道,然后通过所述安全数字通信信道接收所述秘密,从而使所述对等方表现为所述可信外部源。这至少涉及以下优点:人们可以依赖于在对等方的环境中生成的秘密的可信的高熵性质,并且仍然在所述装置中实现足够的数字安全性。

[0022] 根据实施方式,所述安全数字通信信道的建立包括以下中的至少一项:使用传输层安全(也称为TLS)标准来建立所述安全数字通信信道;使用光纤通信作为所述安全数字通信信道;使用近场无线通信作为所述安全数字通信信道;使用通过手动操作的用户接口的通信作为所述安全数字通信信道。这至少涉及以下优点:可以使用标准化和公知的方法,而不必对所涉及的装置和软件提出非常特定的要求。

[0023] 根据实施方式,所述密码学验证涉及将与所述秘密相关联地接收到的公钥与所述秘密的假定发送者的单独获得的公钥进行比较。这至少涉及以下优点:可以基于某些已知方法的知识来评估验证的可靠性。

[0024] 根据实施方式,所述一个或更多个密钥的所述生成包括以下中的至少一项:使用所述秘密作为密钥生成算法的种子;使用所述秘密和从所述装置的用户接收到的信息作为密钥生成算法的输入信息。这至少涉及以下优点:即使所述秘密的保密性遭到破坏,在破坏密钥生成算法的结果所用于的任何用途的安全性方面,仍会存在进一步的障碍。

[0025] 根据实施方式,该方法包括在所述生成的一个或更多个密钥中的至少一个的立即使用之后永久地丢弃该密钥。这至少涉及以下优点:未被授权方对由所述装置存储的数据的非预期中间访问不会泄露丢弃的密钥,因为该密钥每次都将被重新生成,仅用于立即使

用,然后再次被丢弃

[0026] 根据第三方面,提供了一种计算机程序产品,所述计算机程序产品包括一个或更多个机器可读指令的一个或更多个集合,所述一个或更多个机器可读指令在由一个或更多个处理器执行时使得实现上述类型的方法。

附图说明

[0027] 在附图中:

[0028] 图1示出了两个通信装置的部分,

[0029] 图2示出了两个通信装置的部分,

[0030] 图3示出了两个装置之间的通信,

[0031] 图4示出了由可信中央装置执行的动作,

[0032] 图5示出了由用户设备执行的动作,

[0033] 图6示出了消息中的内容的示例,

[0034] 图7图示了生成密钥的示例,

[0035] 图8示出了生成密钥的示例,以及

[0036] 图9示出了生成密钥的示例。

具体实施方式

[0037] 在以下描述中,参考附图,附图形成本公开的一部分,并且其中通过说明的方式示出了可以放置本公开的具体方面。应当理解,在不脱离本公开的范围的情况下,可以利用其他方面,并且可以进行结构或逻辑改变。因此,以下详细描述不应被视为具有限制意义,因为本公开的范围由所附权利要求限定。

[0038] 例如,应理解,结合所描述的方法的公开内容也可以适用于用于执行该方法的对应设备或系统,反之亦然。例如,如果描述了特定的方法步骤,则相应的设备可以包括执行所描述的方法步骤的单元,即使这样的单元没有在附图中明确描述或示出。另一方面,例如,如果基于功能单元描述了特定装置,则对应的方法可以包括执行所描述的功能的步骤,即使这样的步骤未在附图中明确描述或示出。此外,应当理解,除非另外特别指出,否则本文描述的各种示例方面的特征可以彼此组合。

[0039] 以下描述使用名称“可信中央装置”和“用户设备”。其中,前者是指计算机设备或一起构成可信计算环境的互连计算机设备的布置。这意味着可信中央装置的构成和操作是已知的,并且可由被相关方认为可信的一方验证。可信中央装置的示例涉及但不限于银行或政府机构的计算机系统。可以代替“可信中央装置”或除“可信中心装置”之外使用的其他名称至少是“可信环境”、“可信服务器”和“钱包提供商”。

[0040] 用户设备不一定是单个设备和/或不一定由单个人类用户使用,尽管这里表示的用户设备的最说明性示例是用户的智能电话、平板计算机或膝上型计算机。通常,用户设备是一种设备或一组互连的设备,其中,该设备或该组互连设备用于与一个或更多个可信中央装置进行安全的、密码学保护的数字通信。虽然可以假设对于所述数字通信(以及对于依赖于所述数字通信的服务),用户设备使用已安装的和/或可下载的已知类型的应用程序,但是这里所指的用户设备的构造和操作不是与可信中央装置的构造和操作类似地已知和

可验证的。

[0041] 在图1中,可信中央装置100包括通信收发器101、被指定为加密器和解密器部分102的密码引擎以及通信的更高层(higher layers of communication)103。通信的更高层103是所有这样的服务、应用和协议层的总体指定,它们可以利用可信中央装置100的能力来与其他设备和装置通信。

[0042] 可信中央装置100能够生成密码学保护通信所需的所有密码产品和密码元素。它包括随机源,其在图1中表示为随机生成器104。为了生成真正的随机性,它可以使用诸如环境噪声等的种子信息。在可信服务器环境中,通常将真实随机性的生成与概念HSM(硬件安全模块)相关联。例如,它可以是由可信中央装置使用的计算机房中的专门制造的电路板或设备。来自随机生成器104的输出是随机位串,密钥生成器105可以使用该随机位串来生成一个或更多个密钥。所生成的密钥被保存在密钥存储器106中,加密器和解密器部分102可以根据需要从密钥存储器106检索它们,以执行加密、解密、数字签名和密码学保护的通信所需的其他密码操作。

[0043] 在图1中,用户设备110基本上仅包括可信中央装置的所有对应部分的对应物:通信收发器111、加密器和解密器部分112、通信的更高层113、随机生成器114、密钥生成器115和密钥存储器116。这些部件彼此联接并且被布置为仅在较小的规模上执行动作,就像可信中央装置100的对应部分一样,因为用户设备110将需要与其进行密码学保护的通信的各方的数量通常比可信中央装置100的数量小得多。

[0044] 图1的布置涉及上面在现有技术的描述中分析的缺点。不能知道用户设备中的随机生成器114是否可以产生足够好随机性的比特串。更重要的是,无法知道用户设备中产生的秘密是否可信,因为存在关于软件和硬件两者的所谓隐藏后门的可能性。如果存在这种隐藏的后门,则当用户设备生成随机数时,它们可能被触发运行,从而损害了所生成的随机数将被使用的任何操作的可信度,这种情况并不罕见。

[0045] 在图2中,可信中央装置100具有与图1中相同的所有部分,尽管它们中的一些可能已经被编程为执行附加动作,这将在下面更详细地描述。用户设备210包括通信部分211、通信加密器和解密器部分212、密钥生成器215和密钥存储器216。用户设备210中的通信的更高层由框213表示。根据上面采取的实践,框213是可以利用用户设备210与其他设备和装置通信的能力的所有这样的服务、应用和协议层的总体指定。

[0046] 值得注意的是,出于这里讨论的目的,用户设备210无需自身包含随机生成器。自然也不排除这种可能,因为用户设备可以出于许多其他目的而利用或多或少的随机输入。通信部分211被配置为将从可信外部源接收到的秘密转发到密钥生成器215。在图2所示的示例性实施方式中,这种转发通过通信加密器和解密器部分212并且通过框213中的通信的更高层中的一些进行,其原因将在下面更详细的描述中变得显而易见。然后,密钥生成器215被配置为使用这种转发的秘密作为密码种子来生成一个或更多个密钥,并将它们存储在密钥存储器216中。通信加密器和解密器部分212被配置为从密钥存储器216检索一个或更多个密钥,并使用所述一个或更多个密钥对通过通信部分211执行的通信进行密码学保护。

[0047] 这里所指的密钥可以是例如用户的加密和/或签名密钥,用于PKI框架中。附加地或替代地,相同的原理可以用于生成和使用其他类型的密钥,例如用于建立安全通信信道

的类型的密钥,该安全通信信道的安全性不需要依赖于用户设备的制造商专用特征,和/或用于数据的密码学认证的类型的密钥。

[0048] 不(必须)使所述用户设备包括随机生成器依赖于向用户设备210提供来自可信中央装置100的秘密(即随机信息)的原理。图3中示出了利用该原理的示例通信序列。在图3左侧被标记为A的一方表示可信中央装置,而右侧被标记为B的一方表示用户设备。

[0049] 步骤301和302是可信中央装置可以采取的准备步骤,以便为图3所示的其余动作做好准备;它们可能已经非常早地执行,并且它们与图3中所示的其他步骤只有弱的概念联系。在步骤301中,可信中央布置生成随机种子,并且在步骤302中,可信中央布置利用所生成的随机种子来生成一个或更多个密钥,用于对要与用户设备执行的通信进行密码学保护。

[0050] 在步骤303,用户设备B中的通信部分和可信中央装置A中的对等方建立安全数字通信信道。这里使用对等方的概念来强调,虽然至少在一些实施方式中,可信中央布置可以是指由互连计算机设备共同构成的大型装置,这些设备共同构成可信计算环境,但是在给定时间,这种装置可能仅有有限部分参与了与单个用户设备的通信。

[0051] 用于在步骤303建立安全数字通信信道的方式和机制不太重要。作为示例,用户设备及其对等方中的通信部分可以被配置为使用传输层安全性或TSL标准来建立安全数字通信信道。作为另一示例,可以使用根据量子安全密码学(QSC)的算法。所述概念在撰写本文时正在开发中,并且可以替代地称为后量子密码学(PQC)或抗量子密码学(QRC)。作为另一示例,步骤303可以涉及使得用户设备足够靠近无线通信装置或与电缆(例如屏蔽电缆或光纤电缆)连接,以在被认为足够安全的情况下(例如在授权官员的监督下)在短距离上交换信息。作为又一示例,步骤303可以涉及使用光纤作为量子信道来建立用于通过双光子源对秘密进行编码和解码的电控偏振系统。这种光纤通信原理用于量子密钥传输(QKD),因此它也可以用于传输来自可信计算环境的秘密种子或盐值,其适合作为安全数字通信信道,因为它不能被常规方法破坏。

[0052] 在步骤303建立的安全数字通信信道涉及安全TLS连接的情况下,使用能够认证各方的通信协议是有利的。例如,当使用HTTPS协议时,用户设备应该至少使用基本Auth方法登录到可信中央装置。如果各方之间先前已就登录所需的令牌信息建立了信任,则更高级的OAuth2.x方法是更优选的。结合TLS,证书也可以用于各方之间的认证,在这种情况下,用户设备不需要以上述方式登录。在这种情况下,可信中央装置利用由可信中央装置自身或由另一个可信实体电子签名的证书来认证用户设备。通常可以描述这些替代方案,使得用户设备中的通信部分被配置为与对等方建立安全数字通信信道。通信部分还被配置为此后通过所述安全数字通信信道接收秘密。

[0053] 在可选步骤304,用户设备从可信中央装置请求随机种子。该步骤是可选的,因为在一些情况下,通信实体可能已经被编程为不需要来自用户设备的请求;可信中央装置可以主动开始向用户设备传输秘密。

[0054] 在步骤305,可信中央装置生成秘密以供用户设备稍后使用。在图3中,秘密被称为随机种子。为了在步骤305生成秘密,可信中央装置利用其认证能力,使得生成的秘密满足真正随机性的标准。必须注意的是,图3中所示的方法步骤的顺序不是强制性的:例如,可信中央装置实际上可能很早前就已经生成了所讨论的秘密。

[0055] 在步骤306,用户设备从可信中央装置接收秘密。如上面已经提到的,用户设备的通信部分可以被配置为通过它稍后将用于密码学保护的通信的相同信道来接收秘密(秘密然后将用于对通信进行密码学保护)。作为替代方案,通信部分可以被配置为通过与用于稍后通过所述通信部分执行的所述密码学保护的通信的信道不同的信道来接收所述秘密。这样的不同信道的示例包括但不限于近场无线通信和通过手动操作的用户接口(诸如小键盘或触敏显示器)的通信。

[0056] 在步骤308处,用户设备中的密钥生成器使用所接收的秘密作为密码种子来生成一个或更多个密钥。优选地,这个或这些密钥是PKI框架的密钥。所生成的一个或更多个密钥中的至少一个可以存储在用户设备的密钥存储器中。然而,根据有利的实施方式,用户的密钥存储器不用于存储用户的任何秘密密钥,而是每当需要秘密密钥时再次执行生成这样的秘密密钥的动作。如图3中的可选步骤307所示,在步骤308生成密钥之前,可以接收来自用户的PIN码或相应的个人非存储的信息。稍后在本文中更详细地描述如何将所接收的秘密用作密码种子以生成密钥(可能与PIN码等一起)的示例。

[0057] 由于所生成的密钥可以用于通信,因此可以进一步假设用户设备的通信加密器和解密器部分被配置为从所述密钥存储器(或直接从密钥生成步骤)检索一个或更多个所述密钥,并使用所述一个或更多个密钥对通过用户设备的通信部分执行的通信进行密码学保护。作为这种通信的一部分,在图3中示出了注册步骤309。用户设备可以例如要求可信中央装置在其数据库中存储用户设备使用先前传输的秘密作为密码学种子生成的公钥。在典型的PKI框架中,诸如签名密钥(在DSA中)或公共加密密钥(在ECC和RSA中)的公钥被存储(可能以签名的形式,如在DSA中)在数据库中和/或存储在用户设备的密钥存储器中的用户证书中。

[0058] 在每次需要秘密密钥时再次执行生成秘密密钥的动作的那些实施方式中,存储这样的秘密密钥并检索它以供以后使用的概念可以如下理解:在即时生成的秘密密钥可供使用时,在秘密密钥在短时间内存在于数字寄存器等中的意义上,秘密密钥变成被“存储”。当通信加密器和解密器部分然后使用秘密密钥对通信进行密码学保护时,通信加密器和解密器部分从所述数字寄存器等“检索”秘密密钥。换句话说,“存储以供以后使用”和“检索和使用”循环在时间上可能非常短,之后,秘密密钥被永久地从存储器中丢弃,并且如果再次需要它,则仅在以后的时刻重新生成。

[0059] 图4示出了图3的步骤305中可能涉及的子步骤的示例,即当可信中央装置准备向用户设备提供所请求的秘密时。步骤401表示实际生成所请求的秘密。在步骤402,可信中央装置为要传输到用户设备的秘密提供密码学保护。

[0060] 可以在步骤402处对秘密进行密码学保护,其中具有或不具有与在图3的步骤303处建立的安全数字通信信道的直接关联。如果已经在可信中央装置与用户设备之间建立了信任,则因此能够在各方之间共享非对称或对称的加密密钥。作为对称加密密钥的示例,可信中央装置和用户设备可以具有根据PSK(预共享密钥)模型的先前传送的一次性加密密钥,可信中央装置然后可以在步骤402使用该密钥,通过诸如AES256-CTR或ChaCha20算法的分组或队列密码(block or queue cipher)来保护秘密。作为非对称加密密钥的示例,可信中央装置和用户设备可能先前已经传送了彼此的公共ECC密钥,诸如用Curve25519算法生成的那些。在这些密钥之间,各方可以计算共同秘密,然后可以使用该共同秘密。可替代地,

可以通过分发从其产生加密密钥,以利用对应的分组或队列密码来保护随机性。

[0061] 为了在可信中央装置与用户设备之间安全地传送秘密,使得其机密性不受到损害,建议尝试使用几个安全层。如果不可能在可信中央装置与用户设备之间实现可靠的加密,则可以用可信中央装置的秘密签名密钥对秘密进行数字签名,使得其接收者可以通过使用可信中央装置的相应公共签名密钥对其进行检查来确保其不变性。作为这种实施方式的示例,使用基于Ed25519算法的EdDSA电子签名方法是成本有效且相对安全的。还建议接收者检查秘密的签名是否有效,即正确的可信中央装置已经对秘密进行了可验证的签名。可以通过使用可信中央装置的公共签名密钥来进行该检查。

[0062] 使用本身包括对要签名或检查的信息进行哈希处理的签名算法特别有利,以便防止旨在改变或伪造原始信息的攻击向量。要签名的信息的去中心化提高了安全性并加速了签名或验证过程,这是因为要签名的信息被改变为固定大小的哈希码,因此这使得难以改变或伪造要签名的信息,因为即使很小的改变也会导致分布式哈希的改变。这里,Ed25519签名密钥的DSA方法用作示例。它具有用于要签名的信息的内置哈希。如果使用不具有这种内置哈希的一些其他签名算法,则在这种情况下,强烈建议在生成签名之前,并因此在验证签名信息之前,用单向算法(例如SHA2或SHA3)对数据进行哈希处理。

[0063] 图4中的步骤403表示可信中央装置执行朝向用户设备发送密码学保护的秘密的动作。取决于所选择的通信方法,传输可以涉及在一个或更多个部分中进行传输。

[0064] 图5示出了图3的步骤308中可能涉及的子步骤的示例,即当用户设备使用接收到的秘密作为密码种子来生成一个或更多个密钥并将所述一个或更多个密钥存储在密钥存储器中时。再次,应当注意,优选地,从没有秘密密钥被存储在用户设备的密钥存储器中,而是每次需要时,优选地利用专门接收到的PIN码等再次生成秘密密钥。因此,这里所说的关于在密钥存储器中存储一个或更多个密钥的内容主要适用于存储公钥和/或涉及这种公钥的签名证书。

[0065] 步骤501表示用户设备执行接收包含秘密的传输的动作。如上所述,这些动作可以意味着通过有线或无线通信信道接收调制载波形式的数字信息。附加地或另选地,这些动作可以意味着其他接收方式,如光学读取QR码或其他光学可读信息或通过手动操作的用户接口接收信息。

[0066] 在图4中,假设可信中央装置使用一种或更多种方法在传输之前对所述秘密进行密码学保护。相应地,图5中的步骤502表示用户设备在将所接收的秘密转发到密钥生成器之前对所述秘密的不变性和完整性进行密码学验证。用于这种验证的确切方法基本上是可信中央装置在步骤402中使用的方法的已知对应物,其示例如上所述。下面参考图6描述一些另外的有利特征。可以注意到,在用户设备使用https协议登录到可信中央装置的优选实施方式中,用户设备可以使用用户标识符和密码或客户端证书作为登录信息。在这两种情况下,这样的标识信息已经以服务特定的方式配置到用户设备中。

[0067] 图6示意性地示出了数字传输的信息601。所述信息的子部分是框602所示的可信中央装置的公共(签名)密钥、框603所示的秘密的签名以及框604所示并指定为“盐值(SALT)”的秘密本身。完整的数字传输信息601可以被进一步加密以用于传输,例如通过使用预期接收者的公共密钥,使得成功进行解密需要知道相应的秘密密钥。

[0068] 可信中央装置可能已经使用ED25519算法来生成秘密签名密钥和对应的公共签名

密钥。在生成了秘密604之后,可信中央装置可以通过将所生成的秘密604、它已经使用秘密签名密钥从其计算得出的签名603以及公共签名密钥602放在一起来组成数字发送的信息601。可以注意到,可信中央装置在签名过程中不需要其自己的公共签名密钥602,因为它使用其秘密签名密钥来对要签名的信息进行签名。在该建议的实施方式中,为了方便起见,可信中央装置的公共签名密钥602被包括在传输的信息中,使得它与签名信息一起传输,并且用户设备不需要单独获得它。

[0069] 然后,当用户设备接收到数字传输的信息601时,它首先解密任何外层加密并检索公钥602、签名603和秘密604。如果公钥602与用户设备从其他来源知道的属于可信中央装置的公钥相同,则步骤502中的密码学验证动作可能涉及通过将与秘密604相关联地接收到的公钥602与所述秘密的假定发送者的单独获得的公钥进行比较来进行简单检查。作为更彻底的检查,用户设备可以使用所述秘密的假定发送者的公钥来验证与秘密604相关联地接收到的数字签名603。用户设备可以将所接收的数字传输信息601的解密内容输入到相应的ED25519算法,仅在该特定秘密是不可变的且完整(是可信中央装置最初生成并用其秘密签名密钥签名的秘密)的情况下,该算法才给出肯定结果。

[0070] 返回参考图5,在已经确保其已经以正确的原始形式接收到秘密之后,在步骤503,用户设备使用所述秘密作为密码种子来生成一个或更多个密钥,并将所述一个或更多个密钥存储在其密钥存储器中。图7和图8示出了密钥的生成可以如何发生的两个更详细的示例。

[0071] 在图7中,用户设备从可信中央装置接收到的秘密被指定为URT_{SALT}。图7的方法涉及使用所述秘密和从用户接收到的信息作为密钥生成算法的输入信息。从用户接收到的信息在图7中被指定为URT_{PIN},并且它可以是例如用户使用小键盘或触敏显示器输入的短PIN码。在步骤701,用户设备的密钥生成器使用哈希算法来产生秘密密钥URT_{SK},如下所示:

[0072] $URT_{SK}=Hash(URT_{PIN},URT_{SALT})$。

[0073] 可以以这种方式使用的哈希算法的示例是Argon2算法,该算法是数字密码学的技术领域中公知且广泛使用的。在步骤702,用户设备的密钥生成器使用Curve25519算法产生公钥URT_{PK},如下:

[0074] $URT_{PK}=Curve25519(URT_{SK})$

[0075] $=Curve25519(Hash(URT_{PIN},URT_{SALT}))$。

[0076] 生成的密钥URT_{SK}和URT_{PK}两者都可以被存储在用户设备的密钥存储器中,并用于对通过用户设备的通信部分执行的通信进行密码学保护。然而,如前所述,最好不要使秘密密钥URT_{SK}的存储时间比其立即使用所需的时间长。

[0077] 图8示出了一种稍微简单的方法,其中用户设备的密钥生成器仅使用接收到的秘密(而不使用从用户接收到的附加信息)作为密钥生成算法的种子。在图8中,接收到的秘密被指定为KEY_{SEED}。在步骤801处,用户装置的密钥生成器使用Ed25519算法来产生秘密和公共签名密钥KEY_{SK}和KEY_{PK},如下所示:

[0078] $KEY_{SK},KEY_{PK}=Ed25519(KEY_{SEED})$。

[0079] 替代方式可以是图9的步骤901和902中所示的方式,其表示如下产生秘密和公钥KEY_{SK}和KEY_{PK}:

[0080] $KEY_{SK},KEY_{PK}=Ed25519(Hash(URT_{PIN},URT_{SALT}))$。

[0081] 在更简单的实施方式中,用户设备可以使用接收到的秘密(或其一部分)例如作为加密密钥。因此,密钥生成器的先前定义的用于使用所接收的机密作为密码种子来生成一个或更多个密钥的动作应当被广义地解释,使得使用所述秘密或其一部分仅是使用所述秘密作为密码种子来生成一个或更多个密钥的一种方式。

[0082] 所提出的传递可信随机性的方法允许能够与可信中央装置通信的所有设备获得高质量的随机性,并因此实现安全密码学。例如,该技术使得用户能够利用他们已经存在的设备来使用各种电子商务服务,这些设备不包括用于实现高质量密码学功能的安全环境。此外,还可以开发新类型的消费产品,其能够利用甚至最简单的计算单元(例如,可穿戴设备或服装)进行安全的电子交易。该解决方案确保外部方不能操纵随机性(从中得到秘密信息)。此外,当利用这种加密算法时,该技术可以确保受保密的信息的非常高水平的安全性,这些加密算法能够利用随机性的全部熵来得到所述秘密,因此理论上可以抵抗甚至最强大的未来量子计算机的攻击。

[0083] 在不失去所寻求的效果的情况下,可以扩展或改变本文给出的任何范围或设备值。此外,除非明确不允许,否则任何实施方式可以与另一实施方式组合。

[0084] 尽管已经用结构特征和/或动作专用的语言描述了主题,但是应当理解,所附权利要求中定义的主题不必限于上述具体特征或动作。相反,上述具体特征和动作是作为实现权利要求的示例而公开的,并且其他等同特征和动作旨在落入权利要求的范围内。

[0085] 应当理解,上述益处和优点可以涉及一个实施方式或者可以涉及若干实施方式。实施方式不限于解决任何或所有所述问题的实施方式或具有任何或所有所述益处和优点的实施方式。将进一步理解,对“一个”项目的引用可以指那些项目中的一个或更多个。

[0086] 本文描述的方法的步骤可以以任何合适的顺序执行,或者在适当的情况下同时执行。另外,在不脱离本文描述的主题的精神和范围的情况下,可以从任何方法中删除各个框。上述任何实施方式的各方面可以与所描述的任何其他实施方式的各方面组合以形成进一步的实施方式,而不会失去所寻求的效果。本文中关于方法所解释的内容直接适用于由机器可读指令组成的计算机程序产品,所述机器可读指令在由一个或更多个处理器执行时引起所描述类型的方法的实施。

[0087] 术语“包括”在本文中用于表示包括所标识的方法、框或要素,但是这样的框或要素不包括排他性列表,并且方法或装置可以包含附加的框或要素。

[0088] 应当理解,以上描述仅作为示例给出,并且本领域技术人员可以进行各种修改。以上说明书、示例和数据提供了对示例性实施方式的结构和使用的完整描述。尽管上面已经以一定程度的特殊性或参考一个或更多个单独的实施方式描述了各种实施方式,但是本领域技术人员可以在不脱离本说明书的精神或范围的情况下对所公开的实施方式进行多种改变。

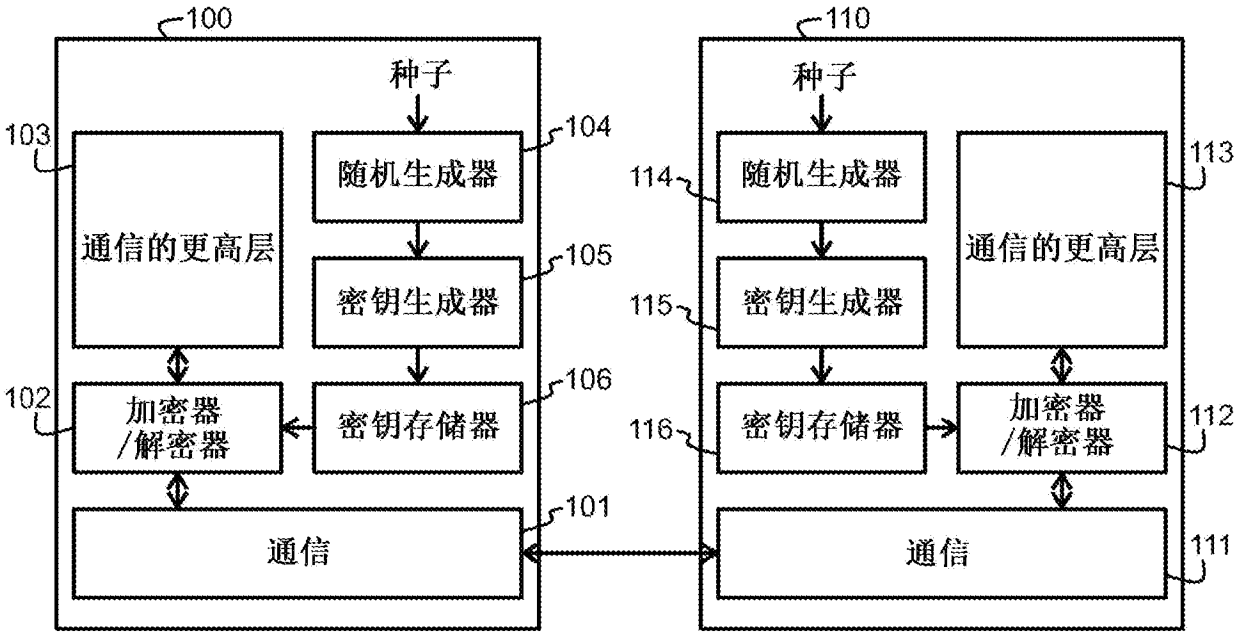

100
种子
103
随机生成器
104
通信的更高层
密钥生成器
105
102
加密器
/解密器
密钥存储器
106
101
通信
110
种子
114
随机生成器
113
通信的更高层
密钥生成器
115
116
密钥存储器
加密器
/解密器
112
通信
111

图1现有技术

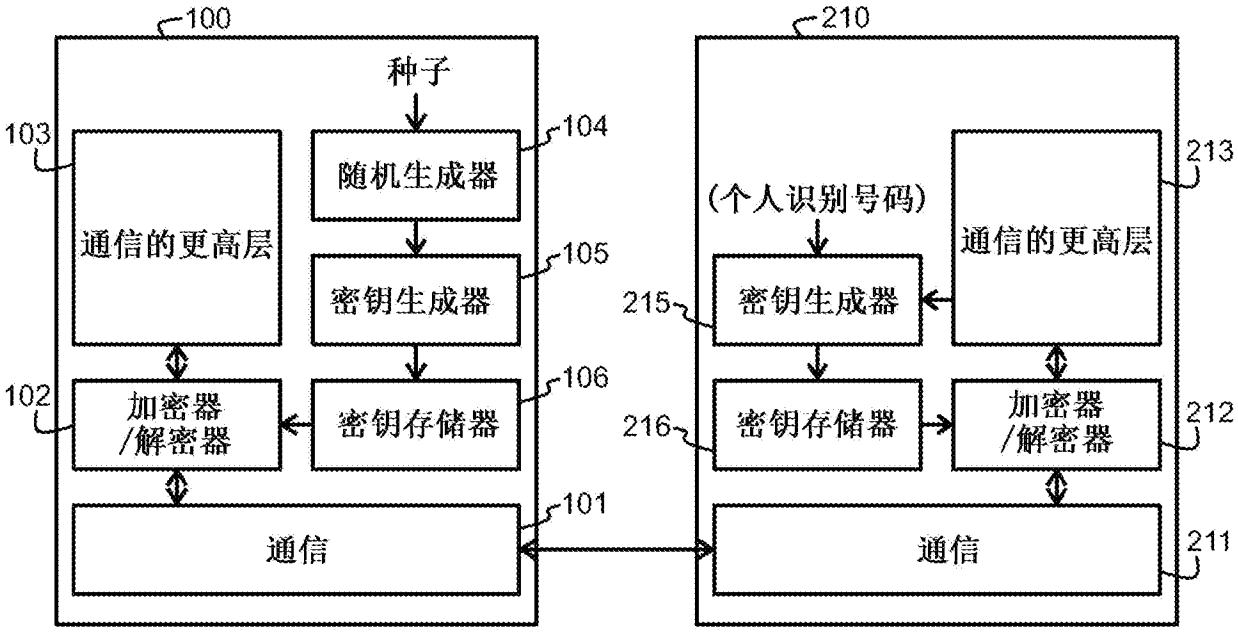

100
种子
103
随机生成器
104
通信的更高层
密钥生成器
105
102
加密器
/解密器
密钥存储器
106
101
通信
210
(个人识别号码)
213
通信的更高层
215
密钥生成器
216
密钥存储器
加密器
/解密器
212
通信
211

图2

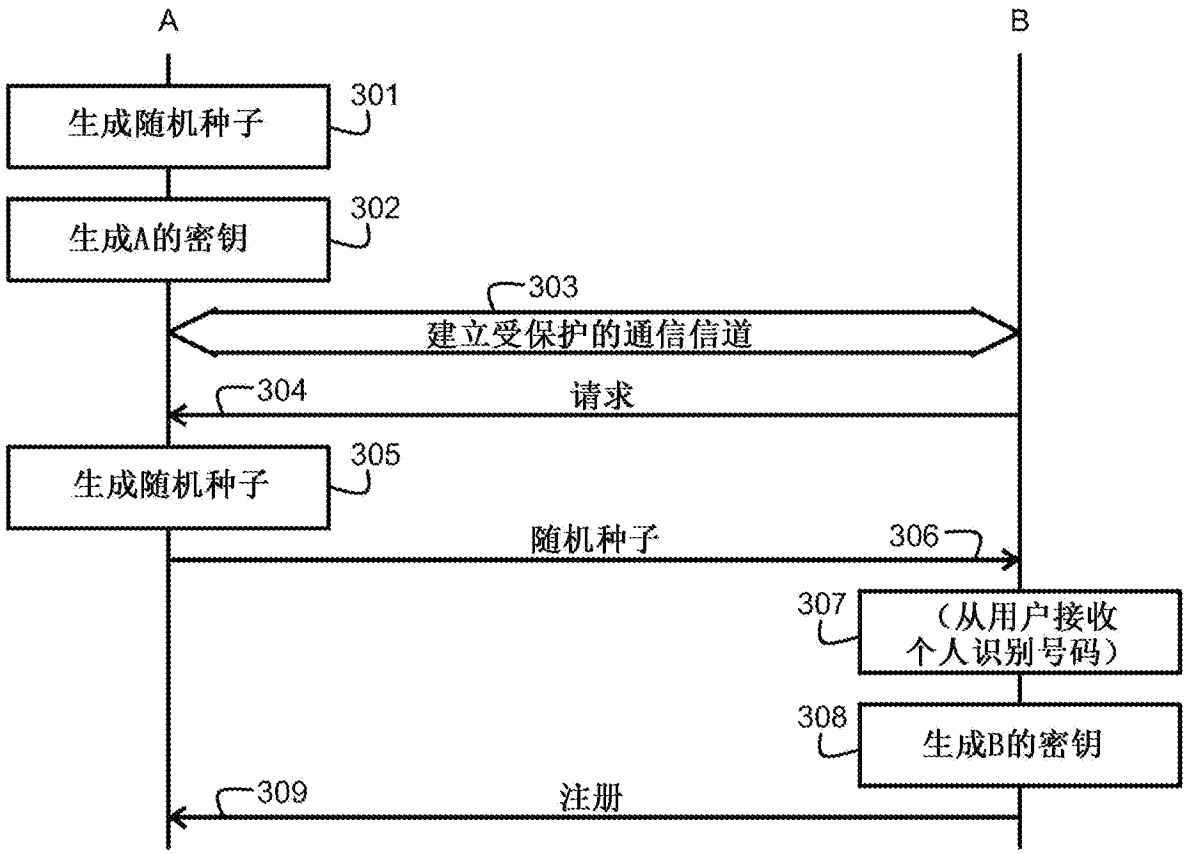

A
B
生成随机种子
301
生成A的密钥
302
303
建立受保护的通信信道
304
请求
生成随机种子
305
随机种子
306
307
（从用户接收
个人识别号码）
308
生成B的密钥
309
注册

图3

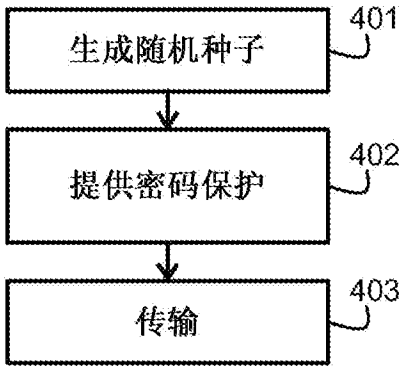

生成随机种子
401
提供密码保护
402
传输
403

图4

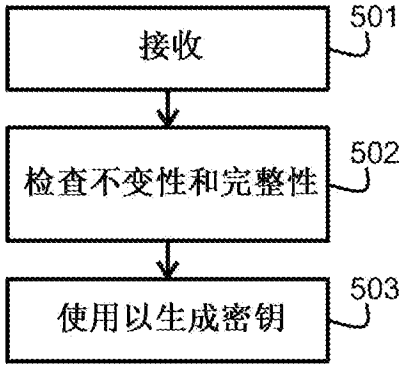

接收
501
检查不变性和完整性
502
使用以生成密钥
503

图5

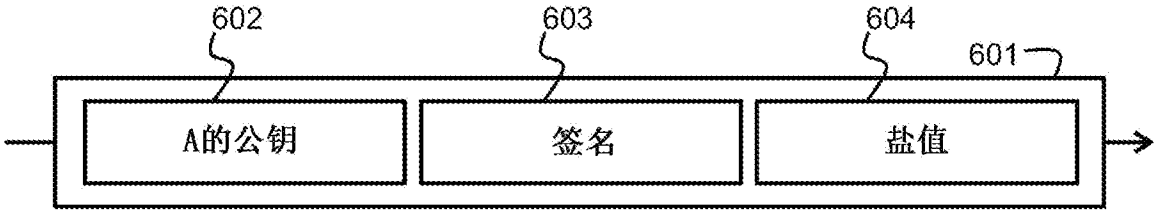

602
603
604
601
A的公钥
签名
盐值

图6

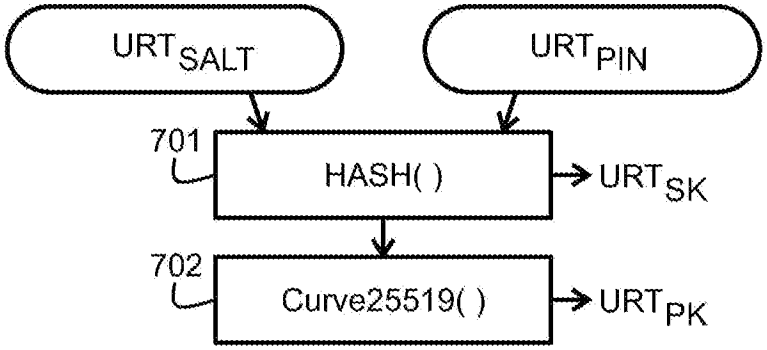

URT SALT
URT PIN
701
HASH( )
URT SK
702
Curve25519( )
URT PK

图7

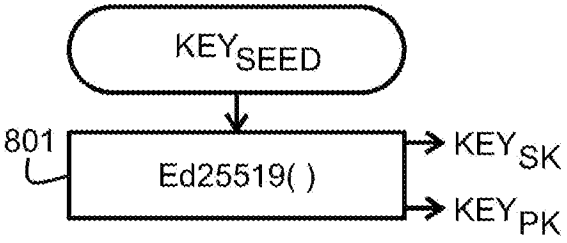

KEY SEED
801
Ed25519( )
KEY SK
KEY PK

图8

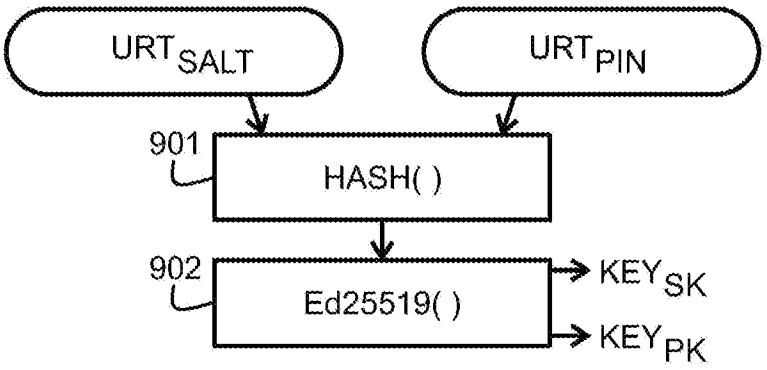


图9