(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112583588 B
(45)授权公告日 2022.06.21

(21)申请号 202011461594.8

(22)申请日 2020.12.08

(65)同一申请的已公布的文献号
申请公布号 CN 112583588 A

(43)申请公布日 2021.03.30

(73)专利权人 四川虹微技术有限公司
地址 610000 四川省成都市中国(四川)自由贸易试验区成都高新区天府四街199号1栋33层

(72)发明人 杨国东 刘建敏 杨超 翟栋 葛纪鑫

(74)专利代理机构 北京超凡宏宇专利代理事务所(特殊普通合伙) 11463
专利代理师 余菲

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 9/32(2006.01)
H04L 9/06(2006.01)
H04L 9/40(2022.01)

(56)对比文件
CN 111953705 A,2020.11.17
CN 110278080 A,2019.09.24
CN 110247762 A,2019.09.17
CN 106533659 A,2017.03.22
陈铁明等.LogIDStamp:一个基于IBE的日志身份戳系统.《浙江工业大学学报》.2011,(第03期),全文.
雷蕾等.支持策略隐藏的加密云存储访问控制机制.《软件学报》.2016,(第06期),全文.
Liqun Chen ect..Cross-Domain Password-Based Authenticated Key Exchange Revisited.《2013 Proceedings IEEE INFOCOM》.2013,全文.

审查员 刘慧敏

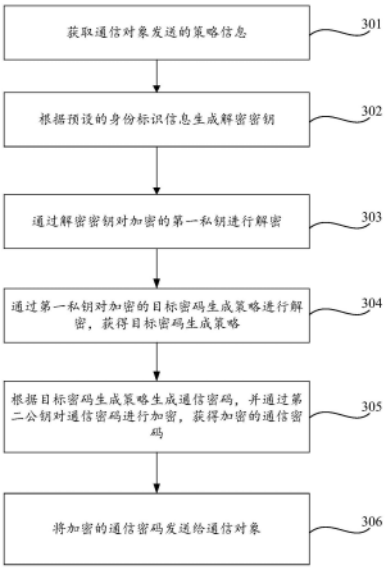
权利要求书2页 说明书9页 附图3页

(54)发明名称

一种通信方法及装置、可读存储介质

(57)摘要

本申请提供一种通信方法及装置、可读存储介质。通信方法包括:获取通信对象发送的策略信息;所述策略信息包括通过第一公钥加密的目标密码生成策略;根据预设的身份标识信息生成解密密钥;通过所述解密密钥对加密的第一私钥进行解密;其中,所述第一私钥与所述第一公钥对应,所述第一私钥的加密密钥根据所述身份标识信息生成;通过所述第一私钥对所述加密的目标密码生成策略进行解密,获得所述目标密码生成策略;根据所述目标密码生成策略生成通信密码,并通过第二公钥对所述通信密码进行加密,获得加密的通信密码;将所述加密的通信密码发送给所述通信对象。该通信方法用以提高密钥的安全性,进而实现安全可靠的通信。



CN 112583588 B

1.一种通信方法,其特征在于,包括:

获取通信对象发送的策略信息;所述策略信息包括通过第一公钥加密的目标密码生成策略;

根据预设的身份标识信息生成解密密钥;

通过所述解密密钥对加密的第一私钥进行解密;其中,所述第一私钥与所述第一公钥对应,所述第一私钥的加密密钥根据所述预设的身份标识信息生成;

通过所述第一私钥对所述加密的目标密码生成策略进行解密,获得所述目标密码生成策略;

根据所述目标密码生成策略生成通信密码,并通过第二公钥对所述通信密码进行加密,获得加密的通信密码;

将所述加密的通信密码发送给所述通信对象;

在所述获取通信对象发送的策略信息之前,所述方法还包括:

将至少一个可选择的密码生成策略和第一证书发送给所述通信对象,以使所述通信对象根据所述至少一个可选择的密码生成策略和所述第一证书中的所述第一公钥生成所述策略信息;所述第一证书为自身的证书;

在所述将至少一个可选择的密码生成策略发送给所述通信对象之前,所述方法还包括:

将自身的SSL版本信息发送给所述通信对象;

接收所述通信对象返回的第二证书和所述通信对象的SSL协议版本;所述第二证书为所述通信对象的证书;

验证所述第二证书是否为合法证书;

对应的,所述将至少一个可选择的密码生成策略和第一证书发送给所述通信对象,包括:

在确定所述第二证书为合法证书时,将至少一个可选择的密码生成策略和第一证书发送给所述通信对象。

2.根据权利要求1所述的通信方法,其特征在于,所述验证所述第二证书是否为合法证书,包括:

获取信任证书库;

判断所述第二证书是否属于所述信任证书库中的证书;

若所述第二证书属于所述信任证书库中的证书,确定所述第二证书为合法证书;

若所述第二证书不属于所述信任证书库中的证书,确定所述第二证书为不合法证书。

3.根据权利要求1所述的通信方法,其特征在于,在所述将至少一个可选择的密码生成策略和第一证书发送给所述通信对象之前,所述方法还包括:

根据预设的通信密码约束条件从本地存储的密码生成策略中确定出所述至少一个可选择的密码生成策略。

4.根据权利要求1所述的通信方法,其特征在于,所述策略信息还包括所述通信对象通过第二私钥对所述加密的目标密码生成策略进行签名生成的签名信息,在所述通过所述第一私钥对所述策略信息进行解密,获得所述目标密码生成策略之前,所述方法还包括:

通过所述第二公钥对所述签名信息进行验证;

对应的，所述通过所述第一私钥对所述加密的目标密码生成策略进行解密，获得所述目标密码生成策略，包括：

在所述签名信息验证通过后，通过所述第一私钥对所述策略信息进行解密，获得所述目标密码生成策略。

5.根据权利要求1所述的通信方法，其特征在于，所述将所述加密的通信密码发送给所述通信对象，包括：

通过所述第一私钥对所述加密的通信密码进行签名，生成签名信息；

将所述签名信息和所述加密的通信密码发送给所述通信对象。

6.根据权利要求1所述的通信方法，其特征在于，所述根据预设的身份标识信息生成解密密钥，包括：

根据预设的身份标识信息和KDF密钥派生算法生成所述解密密钥。

7.一种通信装置，其特征在于，包括：

获取模块，用于获取通信对象发送的策略信息；所述策略信息包括通过第一公钥加密的目标密码生成策略；

第一生成模块，用于根据预设的身份标识信息生成解密密钥；

解密模块，用于通过所述解密密钥对加密的第一私钥进行解密；其中，所述第一私钥与所述第一公钥对应，所述第一私钥的加密密钥根据所述身份标识信息生成；通过所述第一私钥对所述加密的目标密码生成策略进行解密，获得所述目标密码生成策略；

第二生成模块，用于根据所述目标密码生成策略生成通信密码，并通过第二公钥对所述通信密码进行加密，获得加密的通信密码；

发送模块，用于将所述加密的通信密码发送给所述通信对象；

所述发送模块还用于：将自身的SSL版本信息发送给所述通信对象；接收所述通信对象返回的第二证书和所述通信对象的SSL协议版本；所述第二证书为所述通信对象的证书；验证所述第二证书是否为合法证书；在确定所述第二证书为合法证书时，将至少一个可选择的密码生成策略和第一证书发送给所述通信对象，以使所述通信对象根据所述至少一个可选择的密码生成策略和所述第一证书中的所述第一公钥生成所述策略信息；所述第一证书为自身的证书。

8.一种可读存储介质，其特征在于，所述可读存储介质上存储有计算机程序，所述计算机程序被计算机运行时执行如权利要求1-6任一项所述的方法。

一种通信方法及装置、可读存储介质

技术领域

[0001] 本申请涉及通信技术领域，具体而言，涉及一种通信方法及装置、可读存储介质。

背景技术

[0002] 现有技术中，服务端与设备端之间在进行数据通信时，通常都会通过对称的通信密码对通信的数据进行加密。针对该通信密码，可在服务端与设备端正式交互数据之前，通过相互的认证生成。

[0003] 但是，不管是服务端，还是设备端，所应用的加密密钥都是明文数据，导致该加密密钥很容易被其他设备截取并仿冒，即密钥的安全性较低，由此，导致通信不够安全可靠。

发明内容

[0004] 本申请实施例的目的在于提供一种通信方法及装置、可读存储介质，用以提高密钥的安全性，进而实现安全可靠的通信。

[0005] 第一方面，本申请实施例提供一种通信方法，包括：获取通信对象发送的策略信息；所述策略信息包括通过第一公钥加密的目标密码生成策略；根据预设的身份标识信息生成解密密钥；通过所述解密密钥对加密的第一私钥进行解密；其中，所述第一私钥与所述第一公钥对应，所述第一私钥的加密密钥根据所述身份标识信息生成；通过所述第一私钥对所述加密的目标密码生成策略进行解密，获得所述目标密码生成策略；根据所述目标密码生成策略生成通信密码，并通过第二公钥对所述通信密码进行加密，获得加密的通信密码；将所述加密的通信密码发送给所述通信对象。

[0006] 在本申请实施例中，与现有技术相比，用于对第一公钥加密的目标密码生成策略进行解密的第一私钥，通过加密密钥进行加密，并且该加密密钥对应的解密密钥并不是明文数据，在需要使用时，才利用身份标识信息进行现场生成，进而，在保证解密密钥的安全性的情况下，提高了第一私钥的安全性；在第一私钥的安全性提高的基础上，目标密码生成策略的安全性也得到保证，最终生成的通信密码的安全性也更高；通过安全性更高的通信密码，两个通信方之间的通信也更加安全可靠。

[0007] 作为一种可能的实现方式，在所述获取通信对象发送的策略信息之前，所述方法还包括：将至少一个可选择的密码生成策略和第一证书发送给所述通信对象，以使所述通信对象根据所述至少一个可选择的密码生成策略和所述第一证书中的所述第一公钥生成所述策略信息；所述第一证书为自身的证书。

[0008] 在本申请实施例中，通过提供可选择的密码生成策略给通信对象，使通信对象基于该可选择的密码生成策略反馈更合理和更可靠的目标密码生成策略。

[0009] 作为一种可能的实现方式，在所述将至少一个可选择的密码生成策略发送给所述通信对象之前，所述方法还包括：将自身的SSL版本信息发送给所述通信对象；接收所述通信对象返回的第二证书和所述通信对象的SSL协议版本；所述第二证书为所述通信对象的证书；验证所述第二证书是否为合法证书；对应的，所述将至少一个可选择的密码生成策略

和第一证书发送给所述通信对象，包括：在确定所述第二证书为合法证书时，将至少一个可选择的密码生成策略和第一证书发送给所述通信对象。

[0010] 在本申请实施例中，通过对通信对象的证书验证，保证通信对象的证书合法性，实现与通信对象之间更安全可靠的通信。

[0011] 作为一种可能的实现方式，所述验证所述第二证书是否为合法证书，包括：获取信任证书库；判断所述第二证书是否属于所述信任证书库中的证书；若所述第二证书属于所述信任证书库中的证书，确定所述第二证书为合法证书；若所述第二证书不属于所述信任证书库中的证书，确定所述第二证书为不合法证书。

[0012] 在本申请实施例中，通过信任证书库对第二证书进行合法性验证，提高验证的效率和可靠性。

[0013] 作为一种可能的实现方式，在所述将至少一个可选择的密码生成策略和第一证书发送给所述通信对象之前，所述方法还包括：根据预设的通信密码约束条件从本地存储的密码生成策略中确定出所述至少一个可选择的密码生成策略。

[0014] 在本申请实施例中，通过通信密码约束条件，实现本地存储的密码生成策略的初步筛选，进而提高密码生成策略的选定效率。

[0015] 作为一种可能的实现方式，所述策略信息还包括所述通信对象通过第二私钥对所述加密的目标密码生成策略进行签名生成的签名信息，在所述通过所述第一私钥对所述策略信息进行解密，获得所述通信密码生成策略之前，所述方法还包括：通过所述第二公钥对所述签名信息进行验证；对应的，所述通过所述第一私钥对所述加密的目标密码生成策略进行解密，获得所述目标密码生成策略，包括：在所述签名信息验证通过后，通过所述第一私钥对所述策略信息进行解密，获得所述目标密码生成策略。

[0016] 在本申请实施例中，策略信息中还包括签名信息，通过第二公钥对该签名信息进行验证，实现对该策略信息的有效性验证，提高该策略信息的安全性。

[0017] 作为一种可能的实现方式，所述将所述加密的通信密码发送给所述通信对象，包括：通过所述第一私钥对所述加密的通信密码进行签名，生成签名信息；将所述签名信息和所述加密的通信密码发送给所述通信对象。

[0018] 在本申请实施例中，在发送加密的通信密码时，通过对加密的通信密码进行签名，生成签名信息，以使通信对象可以对该加密的通信密码进行有效性验证，提高该加密的通信密码的安全性。

[0019] 作为一种可能的实现方式，根据预设的身份标识信息和KDF密钥派生算法生成所述解密密钥。

[0020] 在本申请实施例中，通过KDF(Key Derivation Function，密钥派生函数)密钥派生算法生成解密密钥，实现解密密钥的快速生成。

[0021] 第二方面，本申请实施例提供一种通信装置，包括：用于实现第一方面以及第一方面的任意一种可能的实现方式中所述的通信方法的各个功能模块。

[0022] 第三方面，本申请实施例提供一种可读存储介质，所述可读存储介质上存储有计算机程序，所述计算机程序被计算机运行时执行如第一方面以及第一方面的任意一种可能的实现方式中所述的方法。

附图说明

[0023] 为了更清楚地说明本申请实施例的技术方案，下面将对本申请实施例中所需要使用的附图作简单地介绍，应当理解，以下附图仅示出了本申请的某些实施例，因此不应被看作是对范围的限定，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他相关的附图。

[0024] 图1为本申请实施例提供的通信系统的示意图；

[0025] 图2为本申请实施例提供的电子设备的示意图；

[0026] 图3为本申请实施例提供的通信方法的流程图；

[0027] 图4为本申请实施例提供的通信装置的功能结构框图。

[0028] 图标：100-通信系统；101-通信设备；102-服务器；200-电子设备；201-存储器；202-通信模块；203-总线；204-处理器；400-通信装置；401-获取模块；402-第一生成模块；403-解密模块；404-第二生成模块；405-发送模块。

具体实施方式

[0029] 下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行描述。方法实施例中的具体操作方法也可以应用于装置实施例或系统实施例中。在本申请的描述中，除非另有说明，“至少一个”包括一个或多个。“多个”是指两个或两个以上。例如，A、B和C中的至少一个，包括：单独存在A、单独存在B、同时存在A和B、同时存在A和C、同时存在B和C，以及同时存在A、B和C。在本申请中，“/”表示或的意思，例如，A/B可以表示A或B；本文中的“和/或”仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A和/或B，可以表示：单独存在A，同时存在A和B，单独存在B这三种情况。

[0030] 请参照图1，为本申请实施例提供的一种通信系统100的示意图。

[0031] 在本实施例中，通信系统100可以包括一个或多个通信设备101，以及服务器102，每个通信设备101均与服务器102连接，可以实现通信设备101与服务器102之间的数据通信，例如数据传输、数据访问等。

[0032] 其中，通信设备101与服务器102之间可以采用HTTP(Hyper Text Transfer Protocol over SecureSocket Layer，超文本传输安全协议)进行通信。

[0033] 不管是多个通信设备101之间的通信，还是通信设备101与服务器102之间的通信，为了保证通信的安全性，比如：保证传输的数据不被盗取；保证传输的数据不被篡改等，可能采用：通信方的身份认证、通信数据的加密等各种安全保障措施。

[0034] 基于此，本申请实施例提供一种通信方法，在保证用以加密数据的密钥的安全性的基础上，提高通信的安全性和可靠性。该通信方法可以应用于通信设备101，也可以应用于服务器102。在现有技术中，服务器102所采用的通信安全保障措施已经比较全面，因此，该通信方法若应用于通信设备101，提高通信的安全性和可靠性的效果更佳。

[0035] 在对该通信方法进行介绍前，先对该通信方法运行的环境进行介绍。

[0036] 请参照图2，电子设备200包括：存储器201、通信模块202、总线203和处理器204。其中，处理器204、通信模块202和存储器201通过总线203连接。

[0037] 在本申请实施例中，电子设备200可以为服务器102，也可以为终端(即通信设备101。当电子设备200为服务器102时，例如可以为网络服务器、数据库服务器、云服务器或由

多个子服务器构成的服务器集成等;或者,当电子设备200为通信设备101时,例如可以为个人电脑、平板电脑、智能手机、个人数字助理等。当然,上述列举的设备是为了便于理解本申请实施例,其不应作为对本申请实施例的限定。

[0038] 本申请实施例中,存储器201存储实现本申请实施例提供的通信方法所需要的程序。

[0039] 存储器201可以包括但不限于RAM(Random Access Memory,随机存取存储器),ROM(Read Only Memory,只读存储器),PROM(Programmable Read-Only Memory,可编程只读存储器),EPROM(Erasable Programmable Read-Only Memory,可擦除只读存储器),EEPROM(Electric Erasable Programmable Read-Only Memory,电可擦除只读存储器)等。

[0040] 总线203可以是ISA(Industry Standard Architecture,工业标准体系结构)总线、PCI(Peripheral Component Interconnect,外设部件互联标准)总线或EISA(Enhanced Industry Standard Architecture,扩展工业标准结构)总线等。总线可以分为地址总线、数据总线、控制总线等。为便于表示,图2中仅用一个双向箭头表示,但并不表示仅有一根总线或一种类别的总线。

[0041] 处理器204用于执行存储器201中存储的可执行模块,例如计算机程序。本申请实施例揭示的流程或定义的装置所执行的方法可以应用于处理器204中,或者由处理器204实现。处理器204在接收到执行指令后,通过总线203调用存储在存储器201中的程序后,处理器204通过总线203控制通信模块202则可以实现运行通信方法的流程。

[0042] 处理器204可以是一种集成电路芯片,具有信号处理能力。处理器204可以是通用处理器,包括CPU(Central Processing Unit,中央处理器)、NP(Network Processor,网络处理器)等;还可以是数字信号处理器、专用集成电路、现成可编程门阵列或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。其可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

[0043] 图2所示的电子设备200的组件和结构只是示例性的,而非限制性的,根据需要,电子设备200也可以具有其他组件和结构。

[0044] 基于上述硬件运行环境和应用场景的介绍,请参照图3,为本申请一实施例提供的通信方法的流程图,该通信方法包括:步骤301、步骤302、步骤303、步骤304、步骤305和步骤306。

[0045] 步骤301:获取通信对象发送的策略信息。策略信息包括通过第一公钥加密的目标密码生成策略。

[0046] 步骤302:根据预设的身份标识信息生成解密密钥。

[0047] 步骤303:通过解密密钥对加密的第一私钥进行解密。其中,第一私钥与第一公钥对应,第一私钥的加密密钥根据身份标识信息生成。

[0048] 步骤304:通过第一私钥对加密的目标密码生成策略进行解密,获得目标密码生成策略。

[0049] 步骤305:根据目标密码生成策略生成通信密码,并通过第二公钥对通信密码进行加密,获得加密的通信密码。

[0050] 步骤306:将加密的通信密码发送给通信对象。

[0051] 与现有技术相比，用于对第一公钥加密的目标密码生成策略进行解密的第一私钥，通过加密密钥进行加密，并且该加密密钥对应的解密密钥并不是明文数据，在需要使用时，利用身份标识信息进行现场生成，进而，在保证解密密钥的安全性的情况下，提高了第一私钥的安全性；在第一私钥的安全性提高的基础上，目标密码生成策略的安全性也得到保证，最终生成的通信密码的安全性也更高；通过安全性更高的通信密码，两个通信方之间的通信也更加安全可靠。

[0052] 接下来对结合步骤301-步骤306对该通信方法进行详细的介绍。

[0053] 假设该通信方法应用于服务器102，则通信对象为任一通信设备101；假设该通信方法应用于通信设备101，则通信对象为服务器102。为了便于理解本申请实施例所提供的技术方案，在后续的实施例中，以任一通信设备101作为该通信方法的执行主体，以服务器102作为该通信对象。

[0054] 服务器102所发送的策略信息中包括通过第一公钥加密的目标密码生成策略。该目标密码生成策略为通信密码对应的生成策略，该通信密码用于服务器102与通信设备101之间的对称加密通信，因此，该生成策略中可以包括：加密方案，比如对称加密算法。

[0055] 第一公钥可以理解为通信设备101的第一私钥对应的公钥，比如：第一私钥为通信设备101的证书的私钥，则第一公钥为通信设备101的证书的公钥。第一私钥可以理解为非对称加密中的私钥，相应的，第一公钥可以理解为非对称加密中与该私钥对应的公钥，私钥为证书持有者(即通信设备101)所用的密钥，公钥为与证书持有者交互的对象(即服务器102)所用的密钥。

[0056] 作为一种可选的实施方式，服务器102从可选择的密码生成策略中选定一种目标密码生成策略，然后发送给通信设备101。其中，可选择的密码生成策略可以由服务器102确定，也可以由通信设备101确定。如果由服务器102确定，则服务器102从本地存储的密码生成策略中确定可选择的密码生成策略即可。如果是由通信设备101确定，则在步骤301之前，该方法还包括：将至少一个可选择的密码生成策略和第一证书发送给通信对象，以使通信对象根据至少一个可选择的密码生成策略和第一证书中的第一公钥生成所述策略信息；第一证书为自身的证书。

[0057] 其中，第一证书可以理解为通信设备101的证书，该证书对应第一公钥和第一私钥。

[0058] 作为一种可选的实施方式，至少一个可选择的密码生成策略的确定过程包括：根据预设的通信密码约束条件从本地存储的密码生成策略中确定出至少一个可选择的密码生成策略。

[0059] 本地存储的密码生成策略可以为通信设备101所支持的对称加密算法。

[0060] 对应的，通信密码约束条件可以是通信密码的加密程度、或者复杂度等。通常来说，对称加密算法可以设置用于表征加密程度或者加密复杂度的评级信息，基于该评级信息，便可以确定各个加密算法的加密程度或者加密复杂度。比如：约束条件中，加密程度需大于预设的程度，或者加密复杂度需大于预设的复杂度，或者加密程度和加密复杂度都需要达到预设的等级或者值。

[0061] 在本申请实施例中，通过通信密码约束条件，实现本地存储的密码生成策略的初步筛选，进而提高密码生成策略的选定效率。

[0062] 在通信设备101确定出至少一个可选择的密码生成策略以后，将至少一个可选择的密码生成策略和第一证书一并发送给服务器102，其中，第一证书的作用为：使服务器102得知第一私钥对应的第一公钥。

[0063] 对于服务器102来说，在接收到至少一个可选择的密码生成策略以后，从至少一个可选择的密码生成策略中确定出目标密码生成策略。服务器102端在选择目标密码生成策略时，也可以基于预设的选择条件进行选择，比如：服务器102所支持的密码生成策略；服务器102所需求的通信密码复杂度和加密程度等。

[0064] 在服务器102确定出目标密码生成策略以后，通过第一公钥对该目标密码生成策略进行加密，然后发送给通信设备101。

[0065] 在本申请实施例中，如果服务器102基于可选择的密码生成策略不能确定出目标密码生成策略，比如：可选择的密码生成策略的加密复杂度太低，此时，服务器102可再次与通信设备101进行交互，请求新的满足条件的可选择的密码生成策略。或者，服务器102直接确定出可选择的密码生成策略，然后发送给通信设备101，待通信设备101反馈以后，服务器102再从中确定出目标密码生成策略。

[0066] 在本申请实施例中，服务器102的身份对于通信设备101来说，也具有可验证性，因为，不排除服务器102存在着冒用或者不安全情况。因此，在步骤301之前，该方法还包括：通信设备101将自身的SSL(Secure socket layer，安全套接字协议)版本信息发送给服务器102；接收服务器102返回的第二证书和服务器102的SSL协议版本；第二证书为服务器102的证书；验证第二证书是否为合法证书。对应的，将至少一个可选择的密码生成策略和第一证书发送给通信对象，包括：在确定第二证书为合法证书时，将至少一个可选择的密码生成策略和第一证书发送给服务器102。

[0067] 其中，SSL是基于HTTP的通信方式中所用的协议，在其他通信方式中，也可以采用其他协议，在本申请实施例中不作限定。

[0068] 通信设备101将其SSL版本同步给服务器102，服务器102也将其SSL版本同步给通信设备101，以保证SSL版本的一致性。

[0069] 在服务器102确定版本的一致性后，将第二证书发送给通信设备101，通信设备101对该证书的合法性进行验证。作为一种可选的实施方式，该验证过程包括：获取信任证书库；判断第二证书是否属于信任证书库中的证书；若第二证书属于信任证书库中的证书，确定第二证书为合法证书；若第二证书不属于信任证书库中的证书，确定第二证书为不合法证书。

[0070] 在这种实施方式中，通信设备101上存储有信任证书库，该信任证书库中的证书都是合法证书，如果第二证书是该证书库中的证书，则为合法证书；如果第二证书不是该证书库中的证书，则不是合法证书。

[0071] 在本申请实施例中，通过信任证书库对第二证书进行合法性验证，提高验证的效率和可靠性。

[0072] 除了这种可选的实施方式，通信设备101也可以采用其他方式进行验证，比如：请求第三方证书机构对该证书的合法性进行验证，第三方证书机构可以是第三方CA(Certificate Authority，证书机构)。

[0073] 除了合法性验证，通信设备101还可以对该第二证书的有效性进行验证，有效性验

证可采用本领域成熟的验证方式，在此不作具体介绍。

[0074] 在本申请实施例中，在通信设备101将第一证书发送给服务器102后，服务器102同样的也可以对第一证书的合法性、有效性等进行验证，验证方式与通信设备101的验证方式相同，在此不再重复介绍。

[0075] 在本申请实施例中，服务器102在对目标密码生成策略进行加密后，将其发送给通信设备101，为了保证加密的目标密码生成策略的安全性和有效性，服务器102还可以通过第二证书对应的第二私钥对该加密的目标密码生成策略进行签名，生成签名信息，基于该签名信息，在步骤301之前，该方法还包括：通过第二公钥对签名信息进行验证。

[0076] 其中，第二公钥为第二证书对应的公钥，第二公钥与第二私钥同样采用非对称加密算法。在服务器102签名时，可以先对加密的目标密码生成策略进行哈希计算，得到哈希值，然后通过第二私钥对哈希值进行签名。因此，在通信设备101验证时，可以先通过第二公钥对哈希值进行解密，得到对应的哈希值；然后利用加密的目标密码生成策略进行哈希计算，得到哈希值；将这两个哈希值进行比对，若比对结果为一致，则确定签名信息经过验证，加密的目标密码生成策略为有效数据；若比对结果不一致，则确定签名信息未通过验证，加密的目标密码生成策略为非有效数据。

[0077] 对应的，如果签名信息验证没有通过，则不执行后续的步骤；如果签名信息验证通过，则继续执行后续的步骤，即步骤303，包括：在签名信息验证通过后，通过第一私钥对策略信息进行解密，获得目标密码生成策略。

[0078] 在步骤302中，预设的身份标识信息可以是通信设备101的身份标识，也可以是将通信设备101的身份标识进行各种复杂的变换后，生成的更安全的身份标识，在本申请实施例不作限定。

[0079] 作为一种可选的实施方式，步骤302包括：根据预设的身份标识信息和KDF密钥派生算法生成解密密钥。

[0080] 在本申请实施例中，除了KDF密钥派生算法，也可以采用其他可实施的密钥派生算法，或者通信设备101自定义的密钥派生算法等，在本申请实施例中不作限定。

[0081] 在步骤303中，通过该解密密钥对加密的第一私钥进行解密，获得第一私钥。其中，第一私钥的加密密钥根据身份标识信息生成。

[0082] 第一私钥的加密密钥和解密密钥可以理解为对称加密的密钥。当基于同一信息，同一密钥派生算法时，所派生出的密钥是相同的，因此，可以保证加密密钥和解密密钥的一致性。

[0083] 在步骤304中，通过第一私钥对加密的目标密码生成策略进行解密。可以理解，第一私钥和第一公钥是非对称的密钥，因此，服务器102利用第一公钥加密的信息，通信设备101可以利用第一私钥进行解密，获得目标密码生成策略。

[0084] 在步骤305中，通信设备101按照目标密码生成策略中规定的加密算法，可以生成对应的通信密码。该过程与密钥派生的过程同理，在此不再重复介绍。

[0085] 进一步地，在步骤306中，通信设备101将加密的通信密码同步给服务器102即可。

[0086] 可以理解，由于通信设备101需要将通信密码同步给服务器102，为了保证该同步过程中通信密码的安全性，所以通信设备101可以利用第二公钥对该通信密码加密，然后服务器102在接收到该通信密码以后，利用第二公钥对应的第二私钥对其进行解密，获得通信

密码。即，通信密码的密钥采用非对称加密的方式。

[0087] 在本申请实施例中，对于通信设备101来说，通信密码的安全性保障措施除了加密，还可以在加密的基础上进行签名。因此，作为一种可选的实施方式，步骤306包括：通过第一私钥对加密的通信密码进行签名，生成签名信息；将签名信息和加密的通信密码发送给服务器102。

[0088] 其中，通信设备101基于加密的通信密码计算出一个哈希值，然后利用第一私钥对该哈希值进行签名，完成签名信息的生成。

[0089] 在通信设备101将签名信息和加密的通信密码同步给服务器102以后，服务器102利用第一公钥先对该签名信息进行验证：利用第一公钥解密出签名信息中的哈希值，然后利用加密的通信密码计算出哈希值，将这两个哈希值进行对比，如果比对结果一致，则该签名信息通过验证；如果比对结果不一致，则该签名信息未通过验证。

[0090] 在该签名信息通过验证后，服务器102再利用第二私钥对加密的通信密码进行解密，获得通信密码。如果该签名信息未通过验证，则服务器102可以请求通信设备101重新发送加密的通信密码，并反馈加密的通信密码可能被篡改的提示信息。

[0091] 在服务器102成功的获得通信密码以后，可以发送对应的反馈信息给通信设备101，然后，下一次的通信过程中，服务器102与通信设备101之间传输的数据可以利用该通信密码实现对称加密。

[0092] 从上述实施例的介绍可以看出，本申请实施例所提供的通信方法，在服务器102和通信设备101的通信过程中，没有包含任何的明文数据，不管是加密密钥，还是解密密钥，还是通信密码，还是第一公钥、第二公钥、第一私钥、第二私钥，即这些数据的安全性和可靠性得到保证，进而服务器102与通信设备101之间的通信的安全性和可靠性也得到保证。

[0093] 请参照图4，本申请实施例中还提供一种通信装置400，包括获取模块401、第一生成模块402、解密模块403、第二生成模块404、发送模块405。

[0094] 获取模块401用于：获取通信对象发送的策略信息；所述策略信息包括通过第一公钥加密的目标密码生成策略。第一生成模块402用于：根据预设的身份标识信息生成解密密钥。解密模块403用于：通过所述解密密钥对加密的第一私钥进行解密；其中，所述第一私钥与所述第一公钥对应，所述第一私钥的加密密钥根据所述身份标识信息生成；通过所述第一私钥对所述加密的目标密码生成策略进行解密，获得所述目标密码生成策略；第二生成模块404用于：根据所述目标密码生成策略生成通信密码，并通过第二公钥对所述通信密码进行加密，获得加密的通信密码；发送模块405用于将所述加密的通信密码发送给所述通信对象。

[0095] 在本申请实施例中，发送模块405还用于：将至少一个可选择的密码生成策略和第一证书发送给所述通信对象，以使所述通信对象根据所述至少一个可选择的密码生成策略和所述第一证书中的所述第一公钥生成所述策略信息；所述第一证书为自身的证书。

[0096] 在本申请实施例中，发送模块405还用于将自身的SSL版本信息发送给所述通信对象。通信装置400还包括接收模块，用于接收所述通信对象返回的第二证书和所述通信对象的SSL协议版本；所述第二证书为所述通信对象的证书；通信装置400还包括验证模块，用于验证所述第二证书是否为合法证书。发送模块405具体用于在确定所述第二证书为合法证书时，将至少一个可选择的密码生成策略和第一证书发送给所述通信对象。

[0097] 在本申请实施例中，获取模块401还用于获取信任证书库；验证模块具体用于判断所述第二证书是否属于所述信任证书库中的证书；若所述第二证书属于所述信任证书库中的证书，确定所述第二证书为合法证书；若所述第二证书不属于所述信任证书库中的证书，确定所述第二证书为不合法证书。

[0098] 在本申请实施例中，通信装置400还包括确定模块，用于根据预设的通信密码约束条件从本地存储的密码生成策略中确定出所述至少一个可选择的密码生成策略。

[0099] 在本申请实施例中，验证模块还用于通过所述第二公钥对所述签名信息进行验证。解密模块403具体还用于在所述签名信息验证通过后，通过所述第一私钥对所述策略信息进行解密，获得所述目标密码生成策略。

[0100] 在本申请实施例中，发送模块405具体用于：通过所述第一私钥对所述加密的通信密码进行签名，生成签名信息；将所述签名信息和所述加密的通信密码发送给所述通信对象。

[0101] 在本申请实施例中，第一生成模块402具体用于：根据预设的身份标识信息和KDF密钥派生算法生成所述解密密钥。

[0102] 本申请实施例还提供一种存储介质，在存储介质上存储有一个或者多个程序，该一个或者多个程序可被一个或者多个处理器执行，以实现本实施例中的通信方法。

[0103] 在本申请所提供的实施例中，应该理解到，所揭露装置和方法，可以通过其它的方式实现。以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，又例如，多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些通信接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

[0104] 另外，作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0105] 再者，在本申请各个实施例中的各功能模块可以集成在一起形成一个独立的部分，也可以是各个模块单独存在，也可以两个或两个以上模块集成形成一个独立的部分。

[0106] 在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。

[0107] 以上所述仅为本申请的实施例而已，并不用于限制本申请的保护范围，对于本领域的技术人员来说，本申请可以有各种更改和变化。凡在本申请的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本申请的保护范围之内。

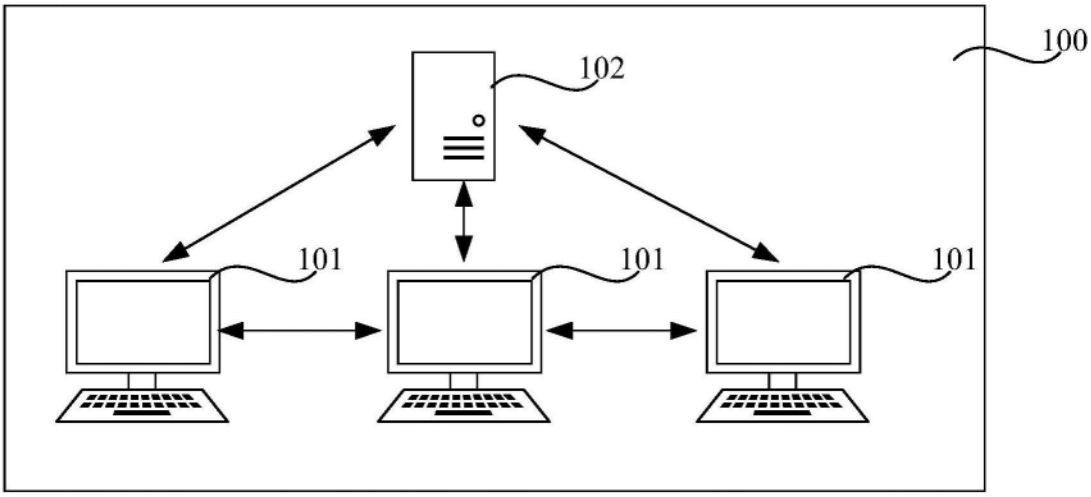


图1

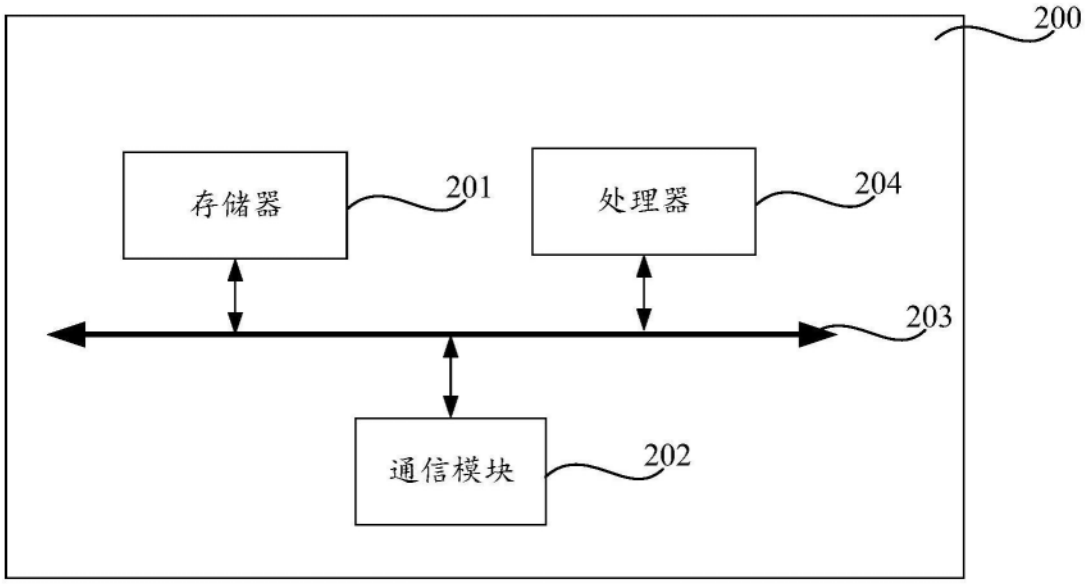


图2

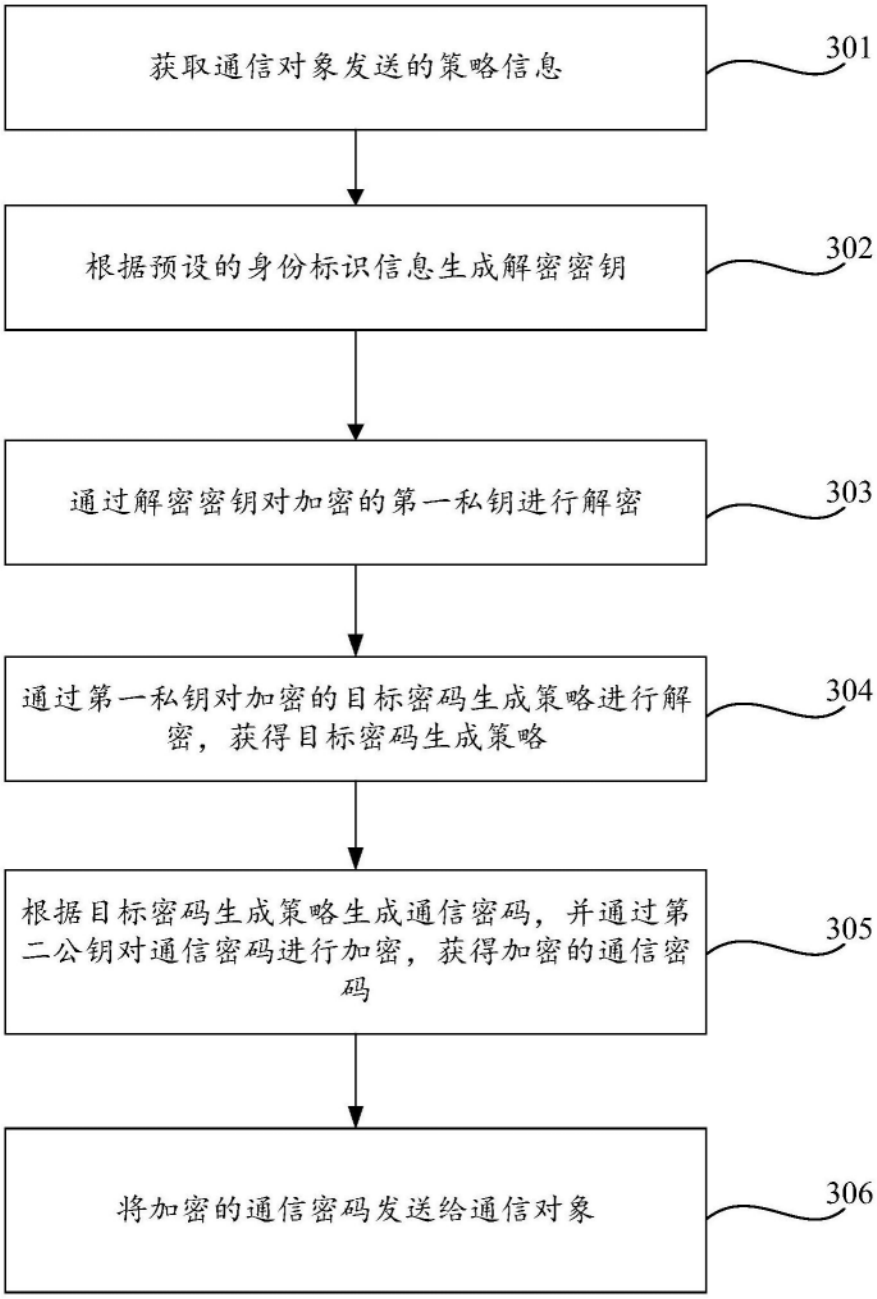

获取通信对象发送的策略信息
301
根据预设的身份标识信息生成解密密钥
302
通过解密密钥对加密的第一私钥进行解密
303
通过第一私钥对加密的目标密码生成策略进行解密，获得目标密码生成策略
304
根据目标密码生成策略生成通信密码，并通过第二公钥对通信密码进行加密，获得加密的通信密码
305
将加密的通信密码发送给通信对象
306

图3

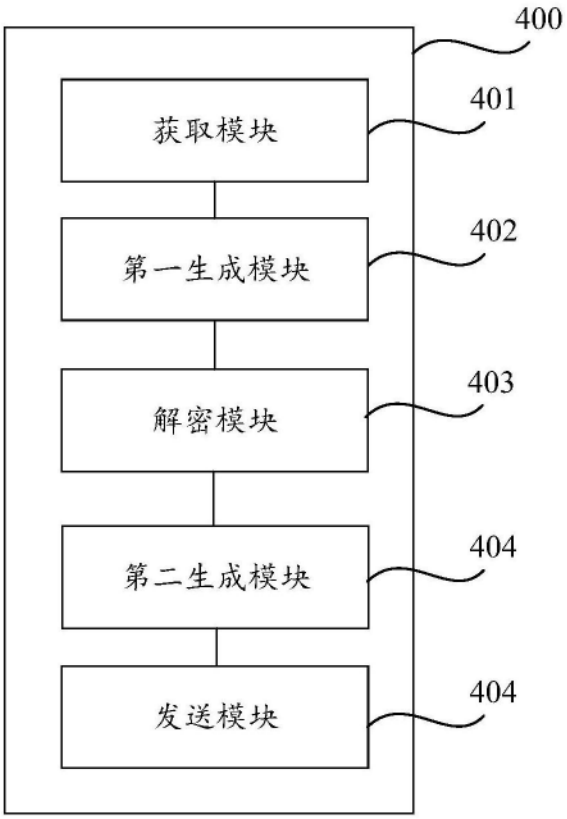


图4