(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 110891061 B
(45)授权公告日 2021.08.06

(21)申请号 201911176393.0

(22)申请日 2019.11.26

(65)同一申请的已公布的文献号
申请公布号 CN 110891061 A

(43)申请公布日 2020.03.17

(73)专利权人 中国银联股份有限公司
地址 200135 上海市浦东新区含笑路36号

(72)发明人 陈林 许斌 杨森

(74)专利代理机构 北京东方亿思知识产权代理有限责任公司 11258
代理人 贺琳

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/32(2006.01)
H04L 9/14(2006.01)

(56)对比文件
CN 106790261 A,2017.05.31
CN 110311884 A,2019.10.08
US 2002062438 A1,2002.05.23
CN 108632296 A,2018.10.09
CN 110035052 A,2019.07.19
CN 103886260 A,2014.06.25
赵万里.《证书漫游系统的设计与实现》.《中国优秀硕士学位论文全文数据库信息科技辑》.2007,第2007卷(第03期),I139-89.

审查员 肖丽金

权利要求书2页 说明书9页 附图6页

(54)发明名称

数据的加解密方法、装置、存储介质及加密文件

(57)摘要

本申请提供了一种数据的加解密方法、装置、存储介质及加密文件，涉及数据处理技术领域。该数据的加密方法，包括：获取第一密钥，对第一密钥与待加密数据进行混淆运算，得到混淆运算结果数据；获取第二密钥，根据第二密钥，得到混淆运算结果数据的第一签名；获取第三密钥，利用第三密钥对第一密钥、待加密数据和第一签名加密，得到目标密文；获取第四密钥，根据第四密钥，得到目标密文的第二签名；生成包括目标密文和第二签名的加密文件。利用本申请的技术方案能够提高数据保护的安全性。

CN 110891061 B

1.一种数据的加密方法,其特征在于,包括:

获取第一密钥,对所述第一密钥与待加密数据进行混淆运算,得到混淆运算结果数据;

获取第二密钥,根据所述第二密钥,得到所述混淆运算结果数据的第一签名;

获取第三密钥,利用所述第三密钥对所述第一密钥、所述待加密数据和所述第一签名加密,得到目标密文;

获取第四密钥,根据所述第四密钥,得到所述目标密文的第二签名;

生成包括所述目标密文和所述第二签名的加密文件。

2.根据权利要求1所述的方法,其特征在于,还包括:

接收解密装置生成并发送的所述第三密钥。

3.根据权利要求1所述的方法,其特征在于,所述第一密钥为所述加密装置生成的密钥,所述第一密钥为公钥。

4.根据权利要求1所述的方法,其特征在于,所述第三密钥为公钥或对称密钥。

5.根据权利要求1所述的方法,其特征在于,

所述第二密钥与所述第四密钥为所述加密装置生成的密钥;

所述第二密钥与所述第四密钥为私钥;

所述第一密钥为公钥,所述第二密钥和/或第四密钥为与所述第一密钥对应的私钥。

6.根据权利要求1或5所述的方法,其特征在于,所述第二密钥与所述第四密钥相同。

7.根据权利要求1所述的方法,其特征在于,所述混淆运算中的混淆因子包括所述第一密钥。

8.一种数据的解密方法,其特征在于,包括:

接收包括目标密文和第二签名的加密文件,所述第二签名为加密装置根据第四密钥得到的所述目标密文的签名;

利用预存的与第三密钥成对的第五密钥,对所述目标密文解密,得到第一密钥、待加密数据和第一签名;

利用与所述第四密钥成对的第六密钥,对所述目标密文和所述第二签名进行验证;

对解密得到的所述第一密钥与所述待加密数据进行与所述加密装置中相同的混淆运算,得到混淆运算结果数据,利用与第二密钥成对的第七密钥,对得到的所述混淆运算结果数据和所述第一签名进行验证,所述第一签名为所述加密装置根据所述第二密钥得到的所述混淆运算结果数据的签名。

9.根据权利要求8所述的方法,其特征在于,还包括:

若对所述目标密文和所述第二签名的验证成功,且对得到所述混淆运算结果数据和所述第一签名的验证成功,确定所述加密文件未被篡改。

10.根据权利要求8所述的方法,其特征在于,在所述接收包括目标密文和第二签名的加密文件之前,还包括:

生成并向所述加密装置发送所述第三密钥。

11.根据权利要求8所述的方法,其特征在于,所述第一密钥为所述加密装置生成的密钥,所述第一密钥为公钥。

12.根据权利要求8所述的方法,其特征在于,所述第三密钥为公钥或对称密钥。

13.根据权利要求8所述的方法,其特征在于,

所述第二密钥与所述第四密钥为所述加密装置生成的密钥；

所述第二密钥与所述第四密钥为私钥。

14.根据权利要求8所述的方法，其特征在于，

在所述第一密钥为公钥且所述第四密钥为与所述第一密钥对应的私钥的情况下，所述第六密钥为对所述目标密文解密得到的所述第一密钥；

在所述第一密钥为公钥且所述第二密钥为与所述第一密钥对应的私钥的情况下，所述第七密钥为对所述目标密文解密得到的所述第一密钥。

15.根据权利要求8所述的方法，其特征在于，所述混淆运算中的混淆因子包括上述第一密钥。

16.一种加密装置，其特征在于，包括：

混淆运算模块，用于获取第一密钥，对所述第一密钥与待加密数据进行混淆运算，得到混淆运算结果；

签名模块，用于获取第二密钥，根据所述第二密钥，得到所述混淆运算结果的第一签名；

加密模块，用于获取第三密钥，利用所述第三密钥对所述第一密钥、所述待加密数据和所述第一签名加密，得到目标密文；

所述签名模块，还用于获取第四密钥，根据所述第四密钥，得到所述目标密文的第二签名；

加密文件生成模块，用于生成包括所述目标密文和所述第二签名的加密文件。

17.一种解密装置，其特征在于，包括：

接收模块，用于接收包括目标密文和第二签名的加密文件，所述第二签名为加密装置根据第四密钥得到的所述目标密文的签名；

解密模块，用于利用预存的与第三密钥成对的第五密钥，对所述目标密文解密，得到第一密钥、待加密数据和第一签名；

第一验证模块，用于利用与所述第四密钥成对的第六密钥，对所述目标密文和所述第二签名进行验证；

第二验证模块，用于对解密得到的所述第一密钥与所述待加密数据进行与所述加密装置中相同的混淆运算，得到混淆运算结果数据，利用与第二密钥成对的第七密钥，对所述混淆运算结果数据和所述第一签名进行验证，所述第一签名为所述加密装置根据所述第二密钥得到的所述混淆运算结果数据的签名。

18.一种加密装置，其特征在于，包括处理器、存储器及存储在所述存储器上并可在所述处理器上运行的计算机程序，所述计算机程序被所述处理器执行时实现如权利要求1至7中任意一项所述的数据的加密方法。

19.一种解密装置，其特征在于，包括处理器、存储器及存储在所述存储器上并可在所述处理器上运行的计算机程序，所述计算机程序被所述处理器执行时实现如权利要求8至15中任意一项所述的数据的解密方法。

20.一种计算机可读存储介质，其特征在于，所述计算机可读存储介质上存储计算机程序，所述计算机程序被处理器执行时实现如权利要求1至7中任意一项所述的数据的加密方法或如权利要求8至15中任意一项所述的数据的解密方法。

数据的加解密方法、装置、存储介质及加密文件

技术领域

[0001] 本申请属于数据处理技术领域，尤其涉及一种数据的加解密方法、装置及加密文件。

背景技术

[0002] 随着网络技术的发展，利用网络传输数据方便了信息的传递。在数据传输过程中，数据有可能泄露或被篡改。在被传输的数据中存在敏感数据，敏感数据不希望发生泄露或被篡改。因此，包括敏感数据的数据的传输对传输安全性的要求较高。

[0003] 现阶段，加密装置会对数据即明文进行加密，将加密后的数据即密文传输至解密装置，解密装置对密文进行解密，从而得到明文。但是，在密文的传输过程中密文有可能被篡改，数据保护的安全性依然较低。

[0004] 申请内容

[0005] 本申请实施例提供了一种数据的加解密方法、装置、存储介质及加密文件，能够提高数据保护的安全性。

[0006] 第一方面，本申请实施例提供一种数据的加密方法，应用于加密装置，方法包括：获取第一密钥，对第一密钥与待加密数据进行混淆运算，得到混淆运算结果数据；获取第二密钥，根据第二密钥，得到混淆运算结果数据的第一签名；获取第三密钥，利用第三密钥对第一密钥、待加密数据和第一签名加密，得到目标密文；获取第四密钥，根据第四密钥，得到目标密文的第二签名；生成包括目标密文和第二签名的加密文件。

[0007] 第二方面，本申请实施例提供一种数据的解密方法，应用于解密装置，方法包括：接收包括目标密文和第二签名的加密文件，第二签名为加密装置根据第四密钥得到的目标密文的签名；利用预存的与第三密钥成对的第五密钥，对目标密文解密，得到第一密钥、待加密数据和第一签名；利用与第四密钥成对的第六密钥，对目标密文和第二签名进行验证；对解密得到的第一密钥与待加密数据进行与加密装置中相同的混淆运算，得到混淆运算结果数据，利用与第二密钥成对的第七密钥，对得到的混淆运算结果数据和第一签名进行验证，第一签名为加密装置根据第二密钥得到的混淆运算结果数据的签名。

[0008] 第三方面，本申请实施例提供一种加密装置，包括：混淆运算模块，用于获取第一密钥，对第一密钥与待加密数据进行混淆运算，得到混淆运算结果；签名模块，用于获取第二密钥，根据第二密钥，得到混淆运算结果的第一签名；加密模块，用于获取第三密钥，利用第三密钥对第一密钥、待加密数据和第一签名加密，得到目标密文；签名模块，还用于获取第四密钥，根据第四密钥，得到目标密文的第二签名；加密文件生成模块，用于生成包括目标密文和第二签名的加密文件。

[0009] 第四方面，本申请实施例提供一种解密装置，包括：接收模块，用于接收包括目标密文和第二签名的加密文件，第二签名为加密装置根据第四密钥得到的目标密文的签名；解密模块，用于利用预存的与第三密钥对应的第五密钥，对目标密文解密，得到第一密钥、待加密数据和第一签名；第一验证模块，用于利用与第四密钥成对的第六密钥，对目标密文

和第二签名进行验证;第二验证模块,用于对解密得到的第一密钥与待加密数据进行与加密装置中相同的混淆运算,得到混淆运算结果数据,利用与第二密钥成对的第七密钥,对混淆运算结果数据和第一签名进行验证,第一签名为加密装置根据第二密钥得到的混淆运算结果数据的签名。

[0010] 第五方面,本申请实施例提供一种加密装置,包括处理器、存储器及存储在存储器上并可在处理器上运行的计算机程序,计算机程序被处理器执行时实现第一方面的技术方案中的数据的加密方法。

[0011] 第六方面,本申请实施例提供一种解密装置,包括处理器、存储器及存储在存储器上并可在处理器上运行的计算机程序,计算机程序被处理器执行时实现第二方面的技术方案中的数据的解密方法。

[0012] 第七方面,本申请实施例提供一种计算机可读存储介质,计算机可读存储介质上存储计算机程序,计算机程序被处理器执行时实现第一方面的技术方案中的数据的加密方法或第二方面的技术方案中的数据的解密方法。

[0013] 本申请实施例提供一种数据的加解密方法、装置、存储介质及加密文件,对第一密钥与待加密数据进行混淆运算,对混淆运算后的第一密钥与待加密数据进行签名,得到第一签名。利用第三密钥,将第一密钥、待加密数据和得到的第一签名进行加密,对加密后的第一密钥、待加密数据和第一签名进行签名,得到第二签名,从而得到了包括第二签名和加密后的第一密钥、待加密数据和第一签名的加密文件。解密装置接收到的加密文件包括目标密文和第二签名,利用与第三密钥成对的第五密钥对目标密文解密,得到第一密钥、待加密数据和第一签名。利用与第四密钥成对的第六密钥,对目标密文和第二签名进行验证。对解密得到的第一密钥与待加密数据进行与加密装置中相同的混淆运算,利用与第二密钥成对的第七密钥,对混淆运算后的解密得到的第一密钥与待加密数据,和第一签名进行验证,完成解密和验证的全过程。加密装置通过混淆、签名、加密和再签名四重防护手段,对待加密数据进行了处理。若加密文件中的内容被篡改,则解密装置可通过验证检测得到,从而提高了数据保护的安全性。

附图说明

[0014] 从下面结合附图对本申请的具体实施方式的描述中可以更好地理解本申请其中,相同或相似的附图标记表示相同或相似的特征。

[0015] 图1为本申请实施例提供的一种数据的加解密方法应用的场景示意图;

[0016] 图2为本申请一实施例提供的一种数据的加密方法的流程图;

[0017] 图3为本申请实施例提供的一种用户可见的加密文件结构示意图;

[0018] 图4为本申请实施例提供的与图3所示的加密文件结构对应的明文结构的示意图;

[0019] 图5为本申请实施例提供的一种加密文件生成形式的示意图;

[0020] 图6为本申请一实施例提供的一种数据的解密方法的流程图;

[0021] 图7为本申请一实施例提供的一种加密装置的结构示意图;

[0022] 图8为本申请另一实施例提供的一种加密装置的结构示意图;

[0023] 图9为本申请一实施例提供的一种解密装置的结构示意图;

[0024] 图10为本申请另一实施例提供的一种解密装置的结构示意图;

[0025] 图11为本申请实施例提供的一种加密装置的结构示意图。

具体实施方式

[0026] 下面将详细描述本申请的各个方面的特征和示例性实施例。在下面的详细描述中，提出了许多具体细节，以便提供对本申请的全面理解。但是，对于本领域技术人员来说很明显的是，本申请可以在不需要这些具体细节中的一些细节的情况下实施。下面对实施例的描述仅仅是为了通过示出本申请的示例来提供对本申请的更好的理解。本申请决不限于下面所提出的任何具体配置和算法，而是在不脱离本申请的精神的前提下覆盖了元素、部件和算法的任何修改、替换和改进。在附图和下面的描述中，没有示出公知的结构和技术，以便避免对本申请造成不必要的模糊。

[0027] 本申请提供一种数据的加解密方法、装置及加密文件，可应用于对数据进行加密，以便于安全传输的场景中。图1为本申请实施例提供的一种数据的加解密方法应用的场景示意图。如图1所示，数据的加解密方法可应用于加密装置10和解密装置20。其中，加密装置10用于执行本申请实施例中数据的加密方法。解密装置20用于执行本申请实施例中数据的解密方法。

[0028] 在本申请中，加密装置可对待加密数据即明文进行混淆、签名、加密和再签名四层防护处理，从而使得在数据的传输过程中，数据难以被篡改，或者，若数据被篡改，解密装置在解密即验证过程中，可及时准确地发现数据被篡改的问题，从而提高了数据的安全性。

[0029] 图2为本申请一实施例提供的一种数据的加密方法的流程图。该数据的加密方法可应用于加密装置。如图2所示，该数据的加密方法可包括步骤S301至步骤S305。

[0030] 在步骤S301中，获取第一密钥，对第一密钥与待加密数据进行混淆运算，得到混淆运算结果数据。

[0031] 待加密数据可为不希望泄露及不希望被篡改的数据，比如，待加密数据可为敏感数据。在此对待加密数据的种类、数量和大小并不限定。

[0032] 混淆运算结果数据即为第一密钥与待加密数据混淆运算的结果数据。混淆运算所涉及的混淆算法可由加密装置和解密装置预先约定，该混淆算法可为非公开的混淆算法，也就是说，该混淆算法只有加密装置和解密装置可知，并不对外公开。在一些示例中，每次混淆运算可对应随机产生混淆因子，混淆因子会影响混淆算法中的局部变量，使得每次混淆运算均会有所不同，攻击者无法准确地获取每次混淆运算的混淆算法，因此难以获得待加密数据，或篡改待加密数据，从而进一步提高了数据保护的安全性。在另一些示例中，混淆运算中的混淆因子可包括第一密钥，也就是说，可将第一密钥作为混淆因子参与混淆运算，在此并不限定。

[0033] 在一些示例中，第一密钥可以为公钥。

[0034] 在步骤S302中，获取第二密钥，根据第二密钥，得到混淆运算结果数据的第一签名。

[0035] 根据第二密钥，对混淆运算结果数据进行签名，得到第一签名。具体地，在一些示例中，第一密钥为公钥，第二密钥可为与第一密钥对应的私钥，即第一密钥与第二密钥为一对公私钥。

[0036] 在步骤S303中，获取第三密钥，利用第三密钥对第一密钥、待加密数据和第一签名

加密，得到目标密文。

[0037] 在这里进行一次加密，利用第三密钥对第一密钥、待加密数据和第一签名的整体进行加密。加密后的第一密钥、待加密数据和第一签名即为目标密文。其中，第三密钥可为公钥或对称密钥，在此并不限定。

[0038] 在步骤S304中，获取第四密钥，根据第四密钥，得到目标密文的第二签名。

[0039] 第二签名是针对目标密文的签名。具体地，在一些示例中，第一密钥为公钥，第四密钥可为与第一密钥对应的私钥，即第一密钥与第四密钥为一对公私钥。更进一步地，第二密钥与第四密钥可为相同的密钥。

[0040] 在步骤S305中，生成包括目标密文和第二签名的加密文件。

[0041] 利用目标密文和第二签名生成加密文件，该加密文件包括目标密文和第二签名。需要说明的是，加密文件中还可包括不进行混淆、签名、加密的可公开的数据，在此并不限定。

[0042] 比如，图3为本申请实施例提供的一种用户可见的加密文件结构示意图。如图3所示，加密文件被打开后，在不经过解密处理的情况下，用户可见的是可公开的数据如可公开的内容说明信息等、目标密文和第二签名。图4为本申请实施例提供的与图3所示的加密文件结构对应的明文结构的示意图。如图4所示，假设待加密数据包括敏感数据1、敏感数据2和敏感数据3，则与加密文件结构对应的明文结构具体包括可公开的数据如可公开的内容说明信息等、第一密钥、敏感数据1、敏感数据2、敏感数据3、第一签名和第二签名。

[0043] 为了便于更直观地说明上述实施例中的混淆、签名、加密和再签名四层防护处理。图5为本申请实施例提供的一种加密文件生成形式的示意图。如图5所示，对第一密钥和待加密数据进行混淆运算；对混淆运算后的第一密钥和待加密数据进行签名，得到签名1；对第一密钥、待加密数据和签名1进行加密，对加密后的第一密钥、待加密数据和签名1进行签名，得到签名2；最终得到加密文件。

[0044] 在本申请实施例中，对第一密钥与待加密数据进行混淆运算，对混淆运算后的第一密钥与待加密数据进行签名，得到第一签名。利用第三密钥，将第一密钥、待加密数据和得到的第一签名进行加密，对加密后的第一密钥、待加密数据和第一签名进行签名，得到第二签名，从而得到了包括第二签名和加密后的第一密钥、待加密数据和第一签名的加密文件。通过混淆、签名、加密和再签名四重防护手段，对待加密数据进行了处理，从而提高了数据保护的安全性。

[0045] 比如，若目标密文被替换，则在后续解密过程中，会发生解密失败或得到错误数据，在发生解密失败或得到错误数据的情况下，对第二签名验证是不会成功的。同理，若第二签名被替换，则对第二签名的验证是不会成功的。若在加密文件传输的过程中发生了密钥的泄露导致待加密数据被篡改，由于第一签名是针对混淆后的第一密钥与待加密数据签名得到的，且混淆算法不对外公开，因此，在后续的解密过程中，被篡改后的待加密数据与第一签名的验证是不会成功的，提高了数据的安全性。

[0046] 在一些示例中，上述数据的加密方法还可包括接收解密装置生成并发送的第三密钥。即第三密钥为解密装置生成的。第一密钥、第二密钥和第四密钥均可为加密装置生成的。也就是说，本申请实施例中的数据的加密方法最少可只依赖解密装置提供的一个密钥即可实现混淆、签名、加密和再签名的过程，降低了解密装置需要承担的开发工作量，提高

了对加密装置、待加密数据和解密装置的保护的安全性。第二密钥和第四密钥可为相同的密钥，第一密钥与第二密钥可为成对的公私钥，则加密装置生成一对公私钥即可实现上述实施例中的第一密钥、第二密钥和第四密钥。

[0047] 本申请实施例还可提供一种加密文件，该加密文件包括目标密文和第二签名。

[0048] 目标密文为利用第三密钥对第一密钥、待加密数据和第一签名加密得到的密文。其中，所述第一签名为根据第二密钥得到的混淆运算结果数据的签名。所述混淆运算结果数据为对所述第一密钥与所述待加密数据进行混淆运算得到的数据。

[0049] 第二签名为根据第四密钥得到的所述目标密文的签名。

[0050] 加密文件的结构及生成形式可参见上述实施例中的图3、图4和图5，其中，关于加密文件、目标密文、第二签名等的具体内容可参见上述实施例中的相关说明，在此不再赘述。

[0051] 在一些示例中，第一密钥为公钥。

[0052] 在一些示例中，第三密钥为公钥或对称密钥。

[0053] 在一些示例中，第二密钥与第四密钥为私钥。

[0054] 进一步地，第一密钥为公钥，第二密钥和/或第四密钥为与第一密钥对应的私钥。

[0055] 在一些示例中，第二密钥与第四密钥相同。

[0056] 在一些示例中，上述混淆运算中的混淆因子包括第一密钥。

[0057] 图6为本申请一实施例提供的一种数据的解密方法的流程图。该数据的解密方法可应用于解密装置。如图6所示，该数据的解密方法可包括步骤S401至步骤S404。

[0058] 在步骤S401中，接收包括目标密文和第二签名的加密文件。

[0059] 为了便于与上述实施例中的数据的加密方法对应，本申请实施例中的数据的解密方法中涉及到的名称与上述数据的加密方法涉及到的名称对应。

[0060] 其中，第二签名为加密装置根据第四密钥得到的目标密文的签名。目标密文是加密装置利用第三密钥，对第一密钥、待加密数据和第一签名加密得到的密文。需要说明的是，本申请实施例中的加密文件已经过传输，在传输过程中，目标密文和第二签名有可能被篡改。

[0061] 在一些示例中，加密文件还可包括其他数据，比如可公开的数据等。

[0062] 在步骤S402中，利用预存的与第三密钥成对的第五密钥，对目标密文解密，得到第一密钥、待加密数据和第一签名。

[0063] 在一些示例中，第三密钥和第五密钥可为解密装置生成对称密钥或成对的公私钥，由解密装置将第三密钥发送给加密装置，以使得加密装置利用第三密钥对第一密钥、待加密数据和第一签名加密。解密装置利用与第三密钥成对的第五密钥可对目标密文解密，解密后的目标密文包括第一密钥、待加密数据和第一签名。

[0064] 在一些示例中，第一密钥为公钥。第三密钥可为公钥或对称密钥。若第三密钥为公钥，则第五密钥为与第三密钥成对的私钥。若第三密钥为对称密钥，则第五密钥与第三密钥为相同的密钥。

[0065] 在步骤S403中，利用与第四密钥成对的第六密钥，对目标密文和第二签名进行验证。

[0066] 解密装置可对目标密文和第二签名进行验证。若目标密文和第二签名验证成功，

表示目标密文和第二签名未被篡改。

[0067] 在一些示例中，第四密钥为私钥，第六密钥即为与第四密钥成对的公钥。进一步地，在第一密钥为公钥且第四密钥为与第一密钥对应的私钥的情况下，第六密钥即为对目标密文解密后得到的第一密钥。解密装置可在对目标密文解密的过程中获取得到第六密钥即第一密钥，不需在自身存储第六密钥，一方面可避免第六密钥由解密装置泄露，另一方面也便于对第六密钥的管理，即第六密钥是随目标密文而更新的。进一步提高了加、解密的安全性。

[0068] 在步骤S404中，对解密得到的第一密钥与待加密数据进行与加密装置中相同的混淆运算，得到混淆运算结果数据，利用与第二密钥成对的第七密钥，对得到的混淆运算结果数据和第一签名进行验证。

[0069] 其中，第一签名为加密装置根据第二密钥得到的混淆运算结果数据的签名。解密装置可对得到的混淆运算结果数据和第一签名进行验证，若得到的混淆运算结果数据和第一签名的验证成功，表示待加密数据、第一密钥和第一签名未被篡改。

[0070] 在一些示例中，第二密钥为私钥，第七密钥即为与第二密钥成对的公钥。进一步地，在第一密钥为公钥且第二密钥为与第一密钥对应的私钥的情况下，第七密钥即为对目标密文解密后得到的第一密钥。解密装置可在对目标密文解密的过程中获取得到第七密钥即第一密钥，不需在自身存储第七密钥，一方面可避免第七密钥由解密装置泄露，另一方面也便于对第七密钥的管理，即第七密钥是随目标密文而更新的。进一步提高了加、解密的安全性。

[0071] 在一些示例中，上述混淆运算中的混淆因子包括第一密钥。

[0072] 在本申请实施例中，解密装置接收到的加密文件包括目标密文和第二签名，利用与第三密钥成对的第五密钥对目标密文解密，得到第一密钥、待加密数据和第一签名。利用与第四密钥成对的第六密钥，对目标密文和第二签名进行验证。对解密得到的第一密钥与待加密数据进行与加密装置中相同的混淆运算，得到混淆运算结果数据，利用与第二密钥成对的第七密钥，对混淆运算结果数据和第一签名进行验证，完成解密和验证的全过程。若加密文件中的内容被篡改，则可通过验证检测得到，提高了数据保护的安全性。

[0073] 具体地，在上述实施例中，若对目标密文和第二签名的验证成功，且对得到混淆运算结果数据和第一签名的验证成功，确定加密文件未被篡改。

[0074] 在一些示例中，第三密钥可为解密装置生成的，对应地，上述实施例中的数据的解密方法还可包括生成并向加密装置发送第三密钥的步骤。

[0075] 在一些示例中，上述实施例中的第一密钥、第二密钥和第四密钥可为加密装置生成的密钥。也就是说，最少可只依赖解密装置提供的一个密钥即可实现加密装置执行的数据的加密方法中混淆、签名、加密和再签名的过程，降低了解密装置需要承担的开发工作量，提高了对加密装置、待加密数据和解密装置的保护的安全性。

[0076] 图7为本申请一实施例提供的一种加密装置的结构示意图。如图7所示，该加密装置10可包括混淆运算模块101、签名模块102、加密模块103和加密文件生成模块104。

[0077] 混淆运算模块101，用于获取第一密钥，对所述第一密钥与待加密数据进行混淆运算，得到混淆运算结果。

[0078] 签名模块102，用于获取第二密钥，根据所述第二密钥，得到所述混淆运算结果的

第一签名。

[0079] 加密模块103，用于获取第三密钥，利用所述第三密钥对所述第一密钥、所述待加密数据和所述第一签名加密，得到目标密文。

[0080] 所述签名模块102，还用于获取第四密钥，根据所述第四密钥，得到所述目标密文的第二签名。

[0081] 加密文件生成模块104，用于生成包括所述目标密文和所述第二签名的加密文件。

[0082] 在本申请实施例中，对第一密钥与待加密数据进行混淆运算，对混淆运算后的第一密钥与待加密数据进行签名，得到第一签名。利用第三密钥，将第一密钥、待加密数据和得到的第一签名进行加密，对加密后的第一密钥、待加密数据和第一签名进行签名，得到第二签名，从而得到了包括第二签名和加密后的第一密钥、待加密数据和第一签名的加密文件。通过混淆、签名、加密和再签名四重防护手段，对待加密数据进行了处理，从而提高了数据保护的安全性。

[0083] 图8为本申请另一实施例提供的一种加密装置的结构示意图。图8与图7的不同之处在于，图8所示的加密装置10还包括接收模块105和第一密钥生成模块106。

[0084] 接收模块105，用于接收解密装置生成并发送的第三密钥。

[0085] 在一些示例中，第三密钥为公钥或对称密钥。

[0086] 第一密钥生成模块106，用于生成第一密钥、第二密钥与第四密钥。

[0087] 在一些示例中，第一密钥为公钥。

[0088] 在一些示例中，第二密钥与第四密钥为私钥。

[0089] 进一步地，第一密钥为公钥，第二密钥和/或第四密钥为与第一密钥对应的私钥。

[0090] 在一些示例中，第二密钥与第四密钥相同。

[0091] 在一些示例中，上述混淆运算中的混淆因子包括第一密钥。

[0092] 图9为本申请一实施例提供的一种解密装置的结构示意图。如图9所示，该解密装置20可包括接收模块201、解密模块202、第一验证模块203和第二验证模块204。

[0093] 接收模块201，用于接收包括目标密文和第二签名的加密文件，第二签名为加密装置根据第四密钥得到的目标密文的签名；

[0094] 解密模块202，用于利用预存的与第三密钥成对的第五密钥，对目标密文解密，得到第一密钥、待加密数据和第一签名；

[0095] 第一验证模块203，用于利用与第四密钥成对的第六密钥，对目标密文和第二签名进行验证；

[0096] 第二验证模块204，用于对解密得到的第一密钥与待加密数据进行与加密装置中相同的混淆运算，得到混淆运算结果数据，利用与第二密钥成对的第七密钥，对混淆运算结果数据和第一签名进行验证，第一签名为加密装置根据第二密钥得到的混淆运算结果数据的签名。

[0097] 在本申请实施例中，解密装置接收到的加密文件包括目标密文和第二签名，利用与第三密钥成对的第五密钥对目标密文解密，得到第一密钥、待加密数据和第一签名。利用与第四密钥成对的第六密钥，对目标密文和第二签名进行验证。对解密得到的第一密钥与待加密数据进行与加密装置中相同的混淆运算，利用与第二密钥成对的第七密钥，对混淆运算后的解密得到的第一密钥与待加密数据，和第一签名进行验证，完成解密和验证的全

过程。若加密文件中的内容被篡改，则可通过验证检测得到，提高了数据保护的安全性。

[0098] 图10为本申请另一实施例提供的一种解密装置的结构示意图。图10与图9的不同之处在于，图10所示的解密装置20还可包括安全确定模块205和第二密钥生成模块206。

[0099] 安全确定模块205，用于若对目标密文和第二签名的验证成功，且对得到混淆运算结果数据和第一签名的验证成功，确定加密文件未被篡改。

[0100] 第二密钥生成模块206，用于生成并向加密装置发送第三密钥。

[0101] 在一些示例中，第一密钥为加密装置生成的密钥。第一密钥为公钥。

[0102] 在一些示例中，第三密钥为公钥或对称密钥。若第三密钥为公钥，第五密钥为与第三密钥对应的私钥。若第三密钥为对称密钥，第三密钥与第五密钥为相同的密钥。

[0103] 在一些示例中，第二密钥与第四密钥为加密装置生成的密钥。第二密钥与第四密钥为私钥。

[0104] 进一步地，在第一密钥为公钥且第四密钥为与第一密钥对应的私钥的情况下，第六密钥即为对目标密文解密得到的第一密钥。在第一密钥为公钥且第二密钥为与第一密钥对应的私钥的情况下，第七密钥即为对目标密文解密得到的第一密钥。

[0105] 在一些示例中，上述混淆运算中的混淆因子包括第一密钥。

[0106] 图11为本申请实施例提供的一种加密装置的结构示意图。如图11所示，加密装置50包括存储器501、处理器502及存储在存储器501上并可在处理器502上运行的计算机程序。

[0107] 在一个示例中，上述处理器502可以包括中央处理器(CPU)，或者特定集成电路(ASIC)，或者可以被配置成实施本申请实施例的一个或多个集成电路。

[0108] 存储器501可以包括用于数据或指令的大容量存储器。举例来说而非限制，存储器501可包括HDD、软盘驱动器、闪存、光盘、磁光盘、磁带或通用串行总线(USB)驱动器或者两个或更多个以上这些的组合。在合适的情况下，存储器501可包括可移除或不可移除(或固定)的介质。在合适的情况下，存储器501可在终端热点开启加密装置50的内部或外部。在特定实施例中，存储器501是非易失性固态存储器。在特定实施例中，存储器501包括只读存储器(ROM)。在合适的情况下，该ROM可以是掩模编程的ROM、可编程ROM(PROM)、可擦除PROM(EPROM)、电可擦除PROM(EEPROM)、电可改写ROM(EAROM)或闪存或者两个或更多个以上这些的组合。

[0109] 处理器502通过读取存储器501中存储的可执行程序代码来运行与可执行程序代码对应的计算机程序，以用于实现上述实施例中数据的加密方法。

[0110] 在一个示例中，加密装置50还可包括通信接口503和总线504。其中，如图11所示，存储器501、处理器502、通信接口503通过总线504连接并完成相互间的通信。

[0111] 通信接口503，主要用于实现本申请实施例中各模块、装置、单元和/或设备之间的通信。也可通过通信接口503接入输入设备和/或输出设备。

[0112] 总线504包括硬件、软件或两者，将加密装置50的部件彼此耦接在一起。举例来说而非限制，总线504可包括加速图形端口(AGP)或其他图形总线、增强工业标准架构(EISA)总线、前端总线(FSB)、超传输(HT)互连、工业标准架构(ISA)总线、无限带宽互连、低引脚数(LPC)总线、存储器总线、微信道架构(MCA)总线、外围组件互连(PCI)总线、PCI-Express(PCI-X)总线、串行高级技术附件(SATA)总线、视频电子标准协会局部(VLB)总线或其他合

适的总线或者两个或更多个以上这些的组合。在合适的情况下，总线504可包括一个或多个总线。尽管本申请实施例描述和示出了特定的总线，但本申请考虑任何合适的总线或互连。

[0113] 本申请实施例还可提供一种解密装置，解密装置的具体结构可参见图11所示的加密装置50。需要说明的是，解密装置中的处理器通过读取存储器中存储的可执行程序代码来运行与可执行程序代码对应的计算机程序，以用于实现上述实施例中数据的解密方法，其余内容可参见上述实施例中的相关说明，在此不再赘述。

[0114] 本申请一实施例还提供一种计算机可读存储介质，该计算机可读存储介质上存储有计算机程序，该计算机程序被处理器执行时可实现上述实施例中的数据的加密方法或数据的解密方法。

[0115] 需要明确的是，本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同或相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。对于加密文件实施例、装置实施例和计算机可读存储介质实施例而言，相关之处可以参见方法实施例的说明部分。本申请并不局限于上文所描述并在图中示出的特定步骤和结构。本领域的技术人员可以在领会本申请的精神之后，作出各种改变、修改和添加，或者改变步骤之间的顺序。并且，为了简明起见，这里省略对已知方法技术的详细描述。

[0116] 本领域技术人员应能理解，上述实施例均是示例性而非限制性的。在不同实施例中出现的不同技术特征可以进行组合，以取得有益效果。本领域技术人员在研究附图、说明书及权利要求书的基础上，应能理解并实现所揭示的实施例的其他变化的实施例。在权利要求书中，术语“包括”并不排除其他装置或步骤；不定冠词“一个”不排除多个；术语“第一”、“第二”用于标示名称而非用于表示任何特定的顺序。权利要求中的任何附图标记均不应被理解为对保护范围的限制。权利要求中出现的多个部分的功能可以由一个单独的硬件或软件模块来实现。某些技术特征出现在不同的从属权利要求中并不意味着不能将这些技术特征进行组合以取得有益效果。

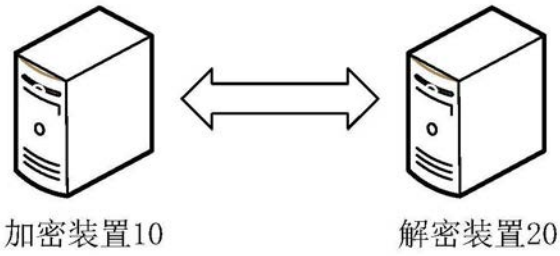
加密装置10
解密装置20

图1

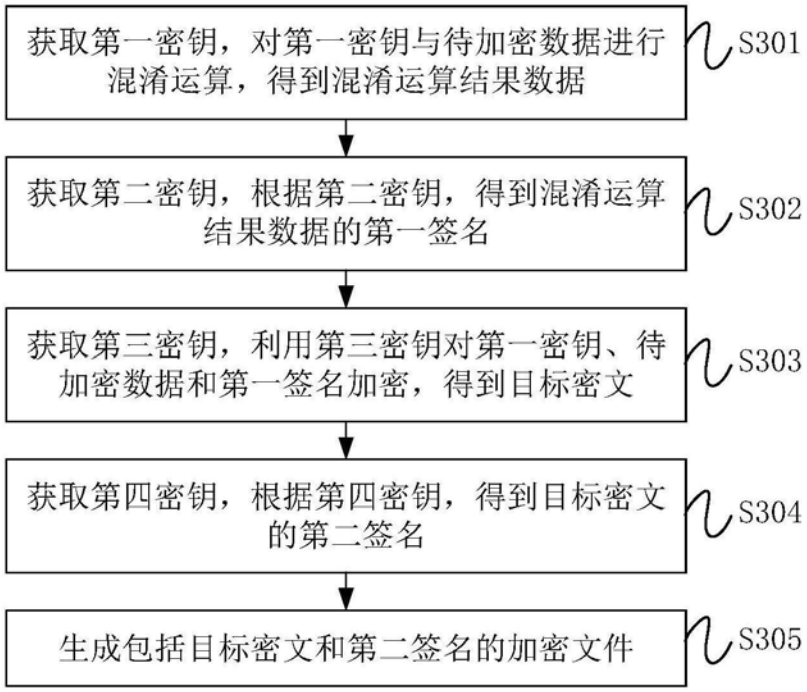
获取第一密钥，对第一密钥与待加密数据进行混淆运算，得到混淆运算结果数据
S301
获取第二密钥，根据第二密钥，得到混淆运算结果数据的第一签名
S302
获取第三密钥，利用第三密钥对第一密钥、待加密数据和第一签名加密，得到目标密文
S303
获取第四密钥，根据第四密钥，得到目标密文的第二签名
S304
生成包括目标密文和第二签名的加密文件
S305

图2

1	#可公开的数据
2	
3	目标密文
4	
5	第二签名
6	

图3

1	#可公开的数据
2	
3	第一密钥
4	
5	敏感数据1
6	敏感数据2
7	敏感数据3
8	
9	第一签名
10	
11	第二签名
12	

图4

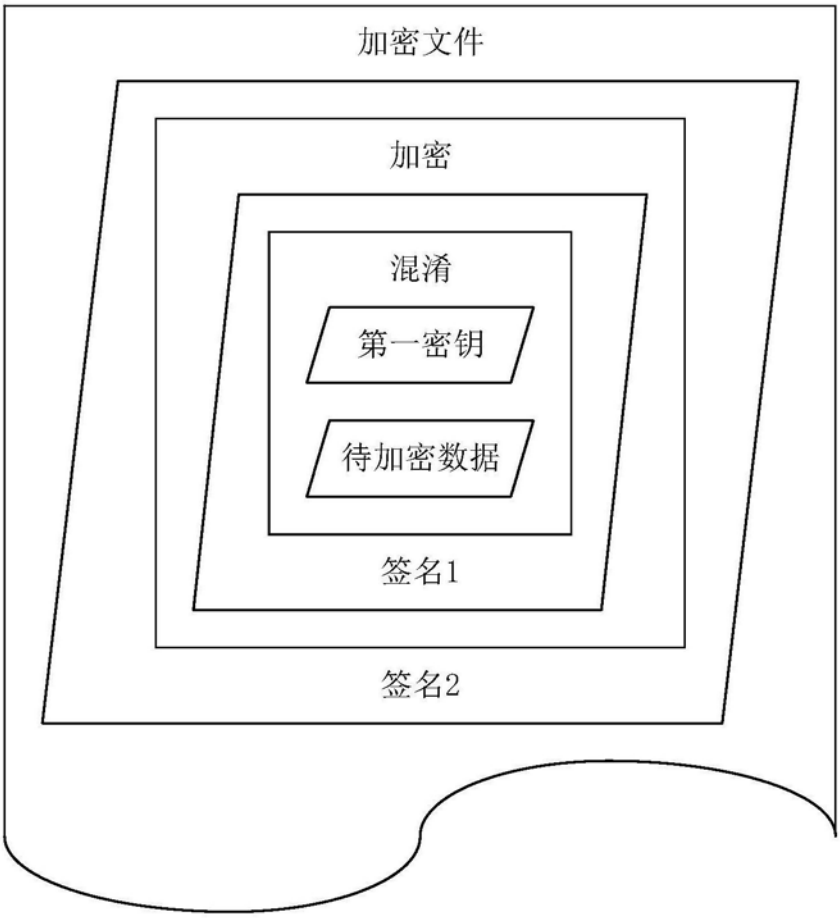
加密文件
加密
混淆
第一密钥
待加密数据
签名1
签名2

图5

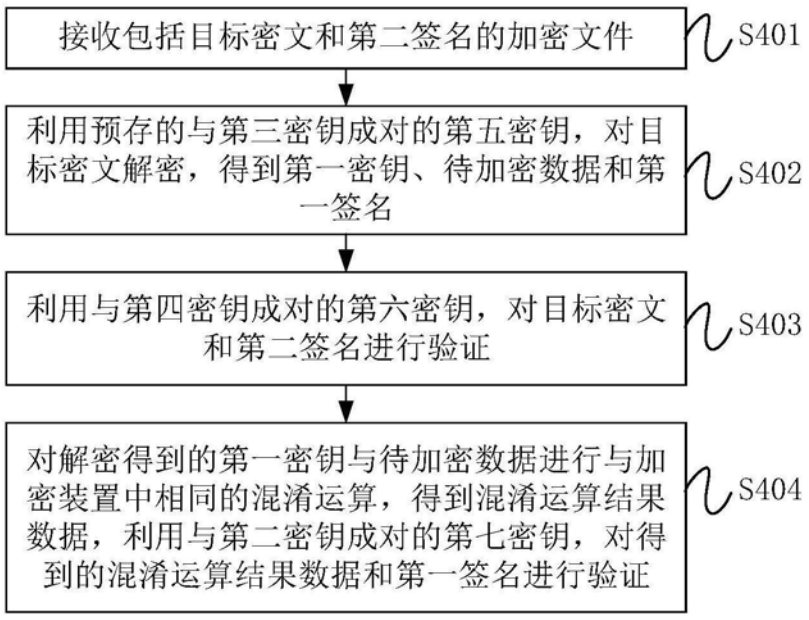
接收包括目标密文和第二签名的加密文件
S401
利用预存的与第三密钥成对的第五密钥，对目标密文解密，得到第一密钥、待加密数据和第一签名
S402
利用与第四密钥成对的第六密钥，对目标密文和第二签名进行验证
S403
对解密得到的第一密钥与待加密数据进行与加密装置中相同的混淆运算，得到混淆运算结果数据，利用与第二密钥成对的第七密钥，对得到的混淆运算结果数据和第一签名进行验证
S404

图6

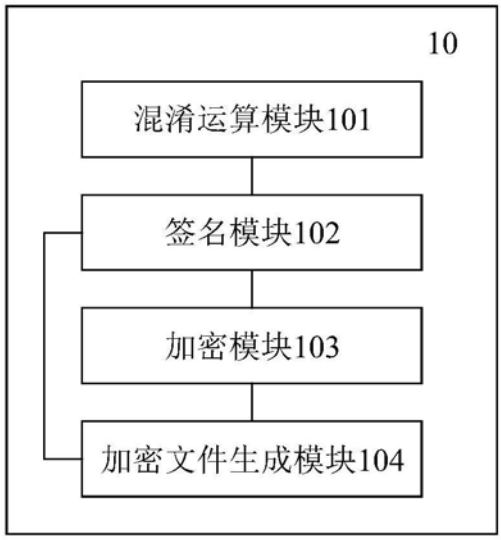
10
混淆运算模块101
签名模块102
加密模块103
加密文件生成模块104

图7

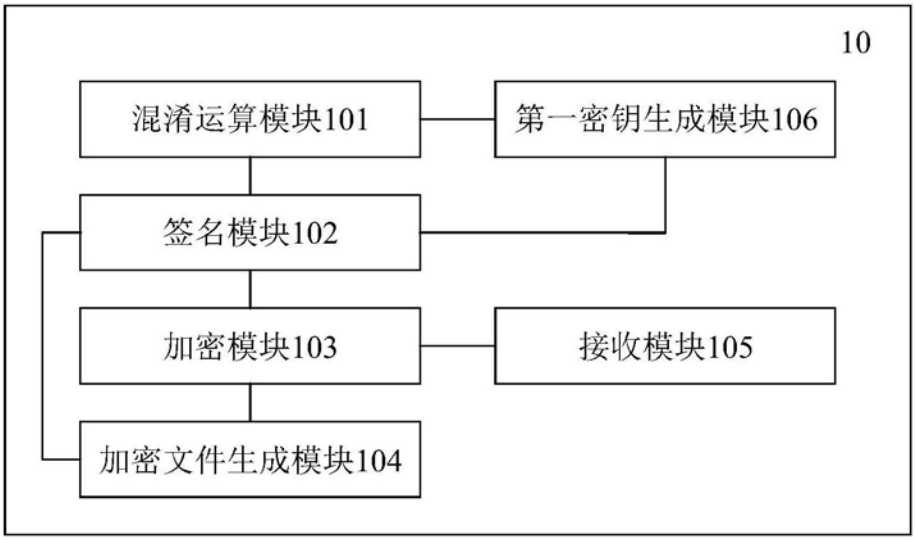
10
混淆运算模块101
第一密钥生成模块106
签名模块102
加密模块103
接收模块105
加密文件生成模块104

图8

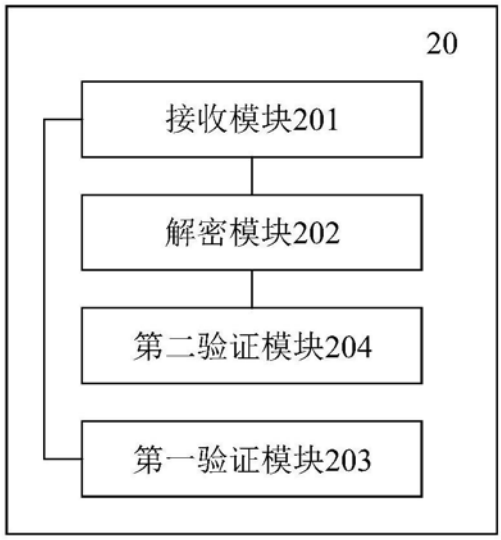
20
接收模块201
解密模块202
第二验证模块204
第一验证模块203

图9

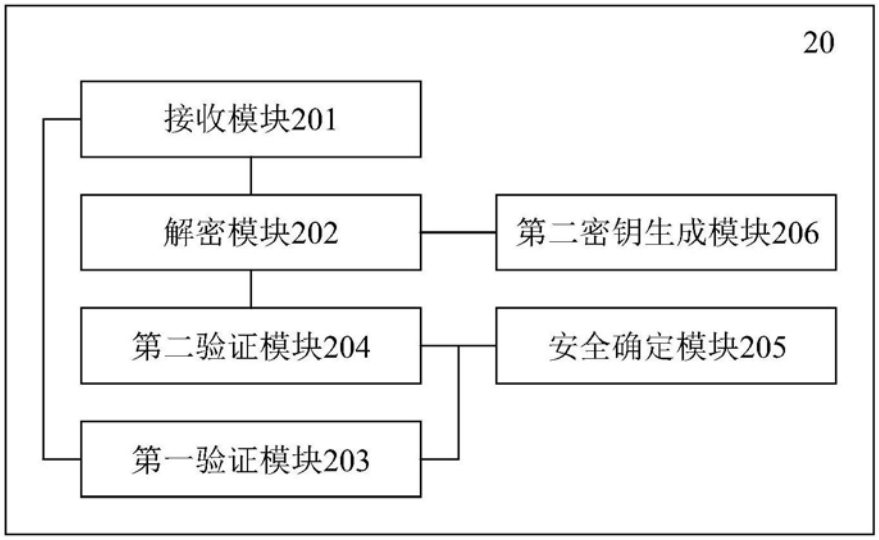
20
接收模块201
解密模块202
第二密钥生成模块206
第二验证模块204
安全确定模块205
第一验证模块203

图10

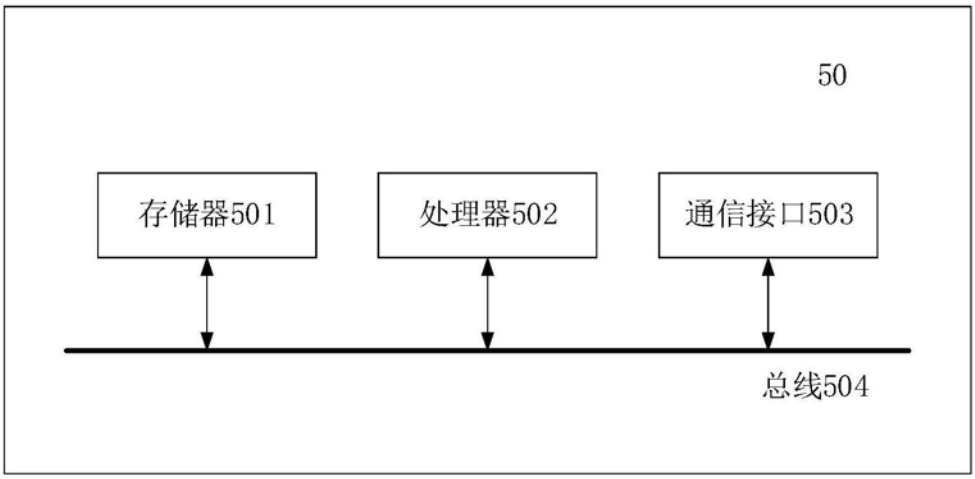

图11