(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2021 年 6 月 3 日 (03.06.2021)

WIPO | PCT

(10) 国际公布号
WO 2021/103802 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01) *H04L 9/14* (2006.01)
H04L 9/32 (2006.01)

(21) 国际申请号: PCT/CN2020/118318

(22) 国际申请日: 2020 年 9 月 28 日 (28.09.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201911176393.0 2019年11月26日 (26.11.2019) CN

(71) 申请人: 中国银联股份有限公司 (CHINA UNIONPAY CO., LTD.) [CN/CN]; 中国上海市浦东新区含笑路36号银联大厦, Shanghai 200135 (CN)。

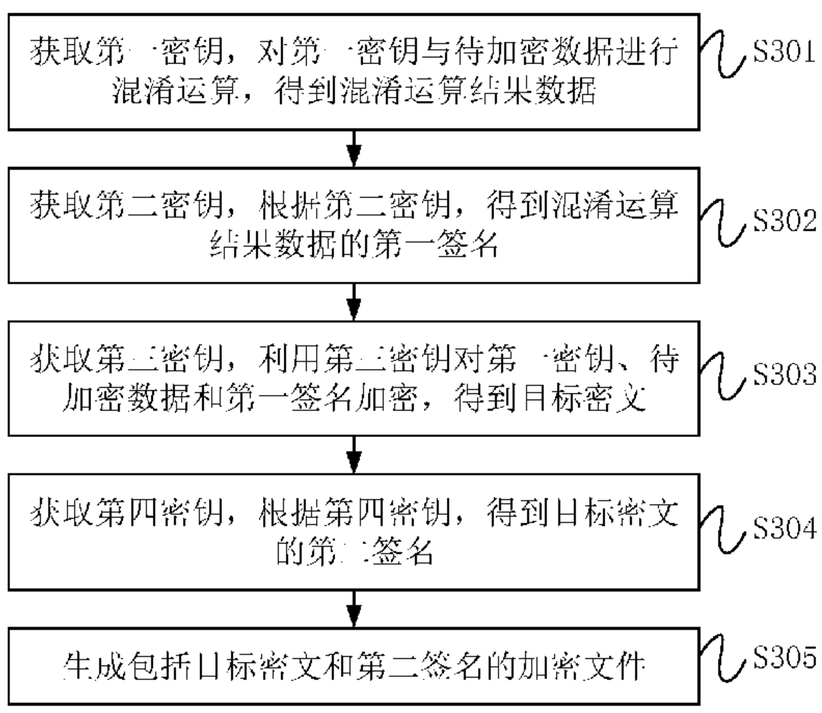
(72) 发明人: 陈林 (CHEN, Lin); 中国上海市浦东新区含笑路36号银联大厦, Shanghai 200135 (CN)。 许斌 (XU, Bin); 中国上海市浦东新区含笑路36号银联大厦, Shanghai 200135 (CN)。 杨森 (YANG, Sen); 中国上海市浦东新区含笑路36号银联大厦, Shanghai 200135 (CN)。

(74) 代理人: 北京东方亿思知识产权代理有限责任公司 (BEIJING EAST IP LTD.); 中国北京市东城区东长安街1号东方广场东方经贸城东2座1601室, Beijing 100738 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK,

(54) **Title:** METHODS AND APPARATUSES FOR ENCRYPTING AND DECRYPTING DATA, STORAGE MEDIUM AND ENCRYPTED FILE

(54) **发明名称**: 数据的加解密方法、装置、存储介质及加密文件



S301 Acquire a first key, and perform an obfuscation operation on the first key and data to be encrypted to obtain obfuscation operation result data
S302 Acquire a second key, and obtain a first signature of the obfuscation operation result data according to the second key
S303 Acquire a third key, and use the third key to encrypt the first key, the data, and the first signature to obtain target ciphertext
S304 Acquire a fourth key, and obtain a second signature of the target ciphertext according to the fourth key
S305 Generate an encrypted file comprising the target ciphertext and the second signature

图 2

(57) **Abstract:** The present application relates to the technical field of data processing, and provided are methods and apparatuses for encrypting and decrypting data, a storage medium, and an encrypted file. The method for encrypting data comprises: acquiring a first key, and performing an obfuscation operation on the first key and data to be encrypted to obtain obfuscation operation result data; acquiring a second key, and obtaining a first signature of the obfuscation operation result data according to the second key; acquiring a third key, and using the third key to encrypt the first key, the data, and the first signature to obtain target ciphertext; acquiring a fourth key, and obtaining a second signature of the target ciphertext according to the fourth key; and generating an encrypted file comprising the target ciphertext and the second signature. The security of data protection may be improved by using the technical solution of the present application.

[见续页]

WO 2021/103802 A1

LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

(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。

数据的加解密方法、装置、存储介质及加密文件

相关申请的交叉引用

本申请要求享有于 2019 年 11 月 26 日提交的名称为“数据的加解密方法、装置、存储介质及加密文件”的中国专利申请 201911176393.0 的优先权，该申请的全部内容通过引用并入本文中。

技术领域

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

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。

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。

发明内容

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。

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。

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。

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。

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。

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。

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。

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。

第八方面，本申请实施例提供一种加密文件，包括：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，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；第二签名，为根据第四密钥得到的所述目标密文的签名。

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

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。

图 1 为本申请实施例提供的数据的加解密方法的应用场景示意图；

图 2 为本申请第一方面提供的数据的加密方法的一实施例的流程图；

图 3 为本申请实施例提供的用户可见的加密文件的一示例的结构示意图；

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；

图 5 为本申请实施例提供的加密文件生成形式的一示例的示意图；

图 6 为本申请第二方面提供的数据的解密方法的一实施例的流程图；

图 7 为本申请第三方面提供的加密装置的一实施例的结构示意图；

图 8 为本申请第三方面提供的加密装置的另一实施例的结构示意图；

图 9 为本申请第四方面提供的解密装置的一实施例的结构示意图；

图 10 为本申请第四方面提供的解密装置的另一实施例的结构示意图；

图 11 为本申请第五方面提供的加密装置的一实施例的结构示意图。

具体实施方式

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。

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数据的加解密方法的应用场景示意图。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。

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。

图 2 为本申请第一方面提供的数据的加密方法的一实施例的流程图。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。

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。

待加密数据可为不希望泄露及不希望被篡改的数据，例如，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。

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，即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，即可将第一密钥作为混淆因子参与混淆运算，在此并不限定。

在一些示例中，第一密钥可以为公钥。

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。

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。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。

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。

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。第三密钥可为公钥或对称密钥，在此并不限定。

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。

第二签名是针对目标密文的签名。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。进一步地，第二密钥与第四密钥可为相同的密钥。

在步骤 S305 中，生成包括目标密文和第二签名的加密文件。

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。

例如，图 3 为本申请实施例提供的用户可见的加密文件的一示例的结构示意图。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。

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加密文件生成形式的一示例的示意图。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。

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。

例如，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。

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。

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。

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。

第二签名为根据第四密钥得到的所述目标密文的签名。

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。

在一些示例中，第一密钥为公钥。

在一些示例中，第三密钥为公钥或对称密钥。

在一些示例中，第二密钥与第四密钥为私钥。

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。

在一些示例中，第二密钥与第四密钥相同。

在一些示例中，上述混淆运算中的混淆因子包括第一密钥。

图 6 为本申请第二方面提供的数据的解密方法的一实施例的流程图。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。

在步骤 S401 中，接收包括目标密文和第二签名的加密文件。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

在一些示例中，上述混淆运算中的混淆因子包括第一密钥。

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。

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。

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。

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。

图 7 为本申请第三方面提供的加密装置的一实施例的结构示意图。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。

混淆运算模块 101 可用于获取第一密钥，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 102 可用于获取第二密钥，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 103 可用于获取第三密钥，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 102 还可用于获取第四密钥，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 104 可用于生成包括所述目标密文和所述第二签名

的加密文件。

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。

图 8 为本申请第三方面提供的加密装置的另一实施例的结构示意图。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。

接收模块 105 可用于接收解密装置生成并发送的第三密钥。

在一些示例中，第三密钥为公钥或对称密钥。

第一密钥生成模块 106 可用于生成第一密钥、第二密钥与第四密钥。

在一些示例中，第一密钥为公钥。

在一些示例中，第二密钥与第四密钥为私钥。

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。

在一些示例中，第二密钥与第四密钥相同。

在一些示例中，上述混淆运算中的混淆因子包括第一密钥。

图 9 为本申请第四方面提供的解密装置的一实施例的结构示意图。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。

接收模块 201 可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 202 可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。

第一验证模块 203 可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 204 可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。

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。

图 10 为本申请第四方面提供的解密装置的另一实施例的结构示意图。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。

安全确定模块 205 可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。

第二密钥生成模块 206 可用于生成并向加密装置发送第三密钥。

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。

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。

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。

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。

在一些示例中，上述混淆运算中的混淆因子包括第一密钥。

图 11 为本申请第五方面提供的加密装置的一实施例的结构示意图。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。

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(Application Specific Integrated Circuit ， 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。

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 可包括硬盘驱动器（Hard Disk Drive，HDD）、软盘驱动器、闪存、光盘、磁光盘、磁带或通用串行总线（Universal Serial Bus，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（Read-Only Memory，ROM）。在合适的情况下，该 ROM 可以是掩模编程的 ROM、可编程 ROM（Programmable Read-Only Memory，PROM）、可擦除 PROM（Erasable Programmable Read-Only Memory，EPROM）、电可擦除 PROM（Electrically Erasable Programmable Read-Only Memory，EEPROM）、电可改写 ROM（Electrically Alterable Read-Only Memory，EAROM）或闪存或者两个或更多个以上这些的组合。

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，以用于实现上述本申请第一方面的数据的加密方法的任一实施例。

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。

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。

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（Accelerated Graphics Port，AGP）或其他图形总线、增强工业标准架构（Enhanced Industry Standard Architecture，EISA）总线、前端总线（Front Side Bus，FSB）、超传输（HyperTransport，HT）互连、工业标准架构（Industrial Standard Architecture，ISA）总线、无限带宽互连、低引脚数（Low pin count，LPC）总线、存储器总线、微信道架构（Micro Channel Architecture，MCA）总线、外围组件互连（Peripheral Component Interconnect，PCI）总线、PCI-Express（PCI-X）总线、串行高级技术附件（Serial Advanced Technology Attachment，SATA）总线、视频电子标准协会局部（Video Electronics Standards Association Local Bus，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。

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，以用于实现上述本申请的第二方面的数据的解密方法的任一实施例，其余内容可参见上述实施例中的相关说明，在此不再赘述。

本申请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本申请第一方面中的数据的加密方法的任一实施例或本申请第二方面的数据的解密方法的任一实施例。计算机可读介质的示例可以是非暂态计算机可读介质，包括 ROM、RAM、磁碟或者光盘等。

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。

上面参考根据本申请的实施例的方法、装置（系统）和计算机程序产品的流程图和/或框图描述了本申请的各方面。应当理解，流程图和/或框图中的每个方框以及流程图和/或框图中各方框的组合可以由计算机程序指令实现。这些计算机程序指令可被提供给通用计算机、专用计算机、或其它可编程数据处理装置的处理器，以产生一种机器，使得经由计算机或其它可编程数据处理装置的处理器执行的这些指令使能对流程图和/或框图的一个或多个方框中指定的功能/动作的实现。这种处理器可以是但不限于是通用处理器、专用处理器、特殊应用处理器或者现场可编程逻辑电路。还可理解，框图和/或流程图中的每个方框以及框图和/或流程图中的方框的组合，也可以由执行指定的功能或动作的专用硬件来实现，或可由专用硬件和计算机指令的组合来实现。

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；数量词“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。

权 利 要 求 书

1、一种数据的加密方法，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，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，其中，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，其中，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，其中，

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，其中，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，其中，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，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，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，其中，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，其中，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，其中，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，其中，

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，其中，

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，其中，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，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，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，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，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，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。

21、一种加密文件，其特征在于，包括

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，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；

第二签名，为根据第四密钥得到的所述目标密文的签名。

22、根据权利要求 21 所述的加密文件，其中其特征在于，所述第一密钥为公钥。

23、根据权利要求 21 所述的加密文件，其中其特征在于，所述第三密钥为公钥或对称密钥。

24、根据权利要求 21 所述的加密文件，其中其特征在于，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。

25、根据权利要求 21 所述的加密文件，其中其特征在于，所述第二密钥与所述第四密钥相同。

26、根据权利要求 21 所述的加密文件，其中其特征在于，所述混淆运算中的混淆因子包括上述所述第一密钥。

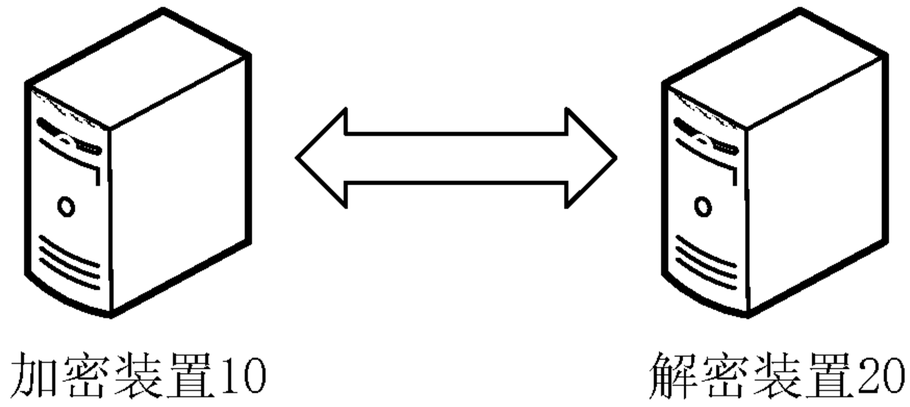

加密装置10
解密装置20

图 1

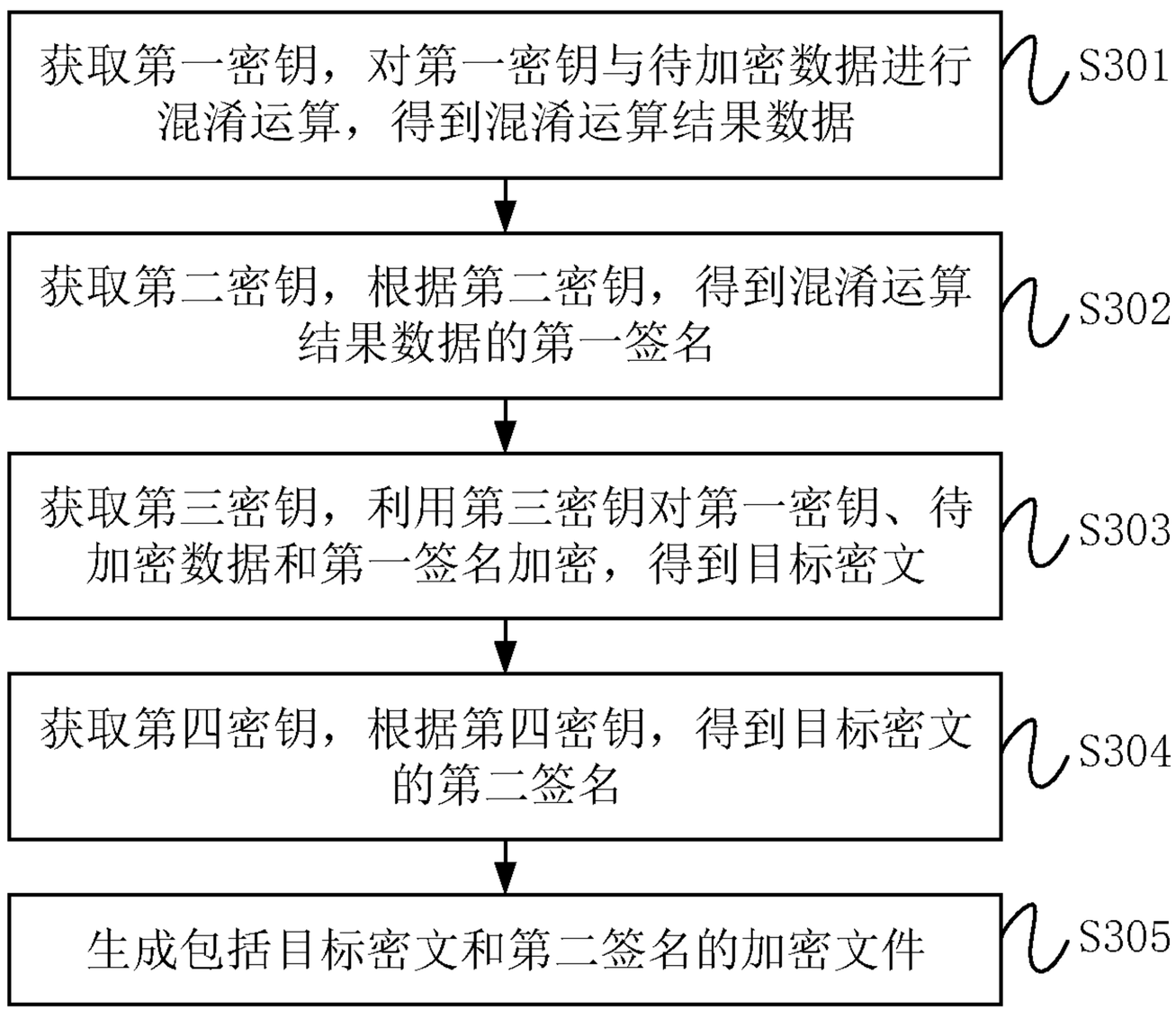

获取第一密钥，对第一密钥与待加密数据进行混淆运算，得到混淆运算结果数据
S301
获取第二密钥，根据第二密钥，得到混淆运算结果数据的第一签名
S302
获取第三密钥，利用第三密钥对第一密钥、待加密数据和第一签名加密，得到目标密文
S303
获取第四密钥，根据第四密钥，得到目标密文的第二签名
S304
生成包括目标密文和第二签名的加密文件
S305

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

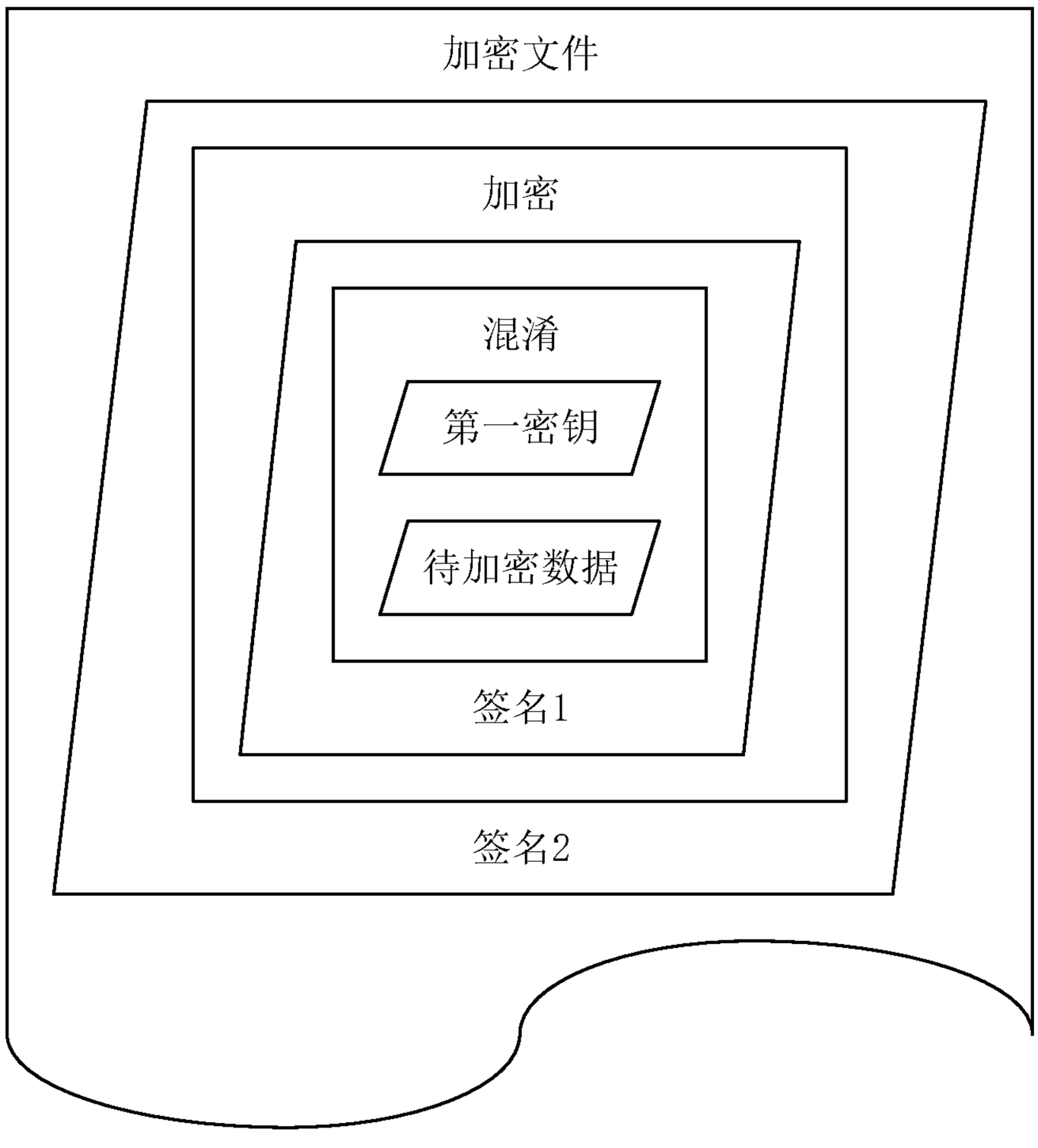


图 5

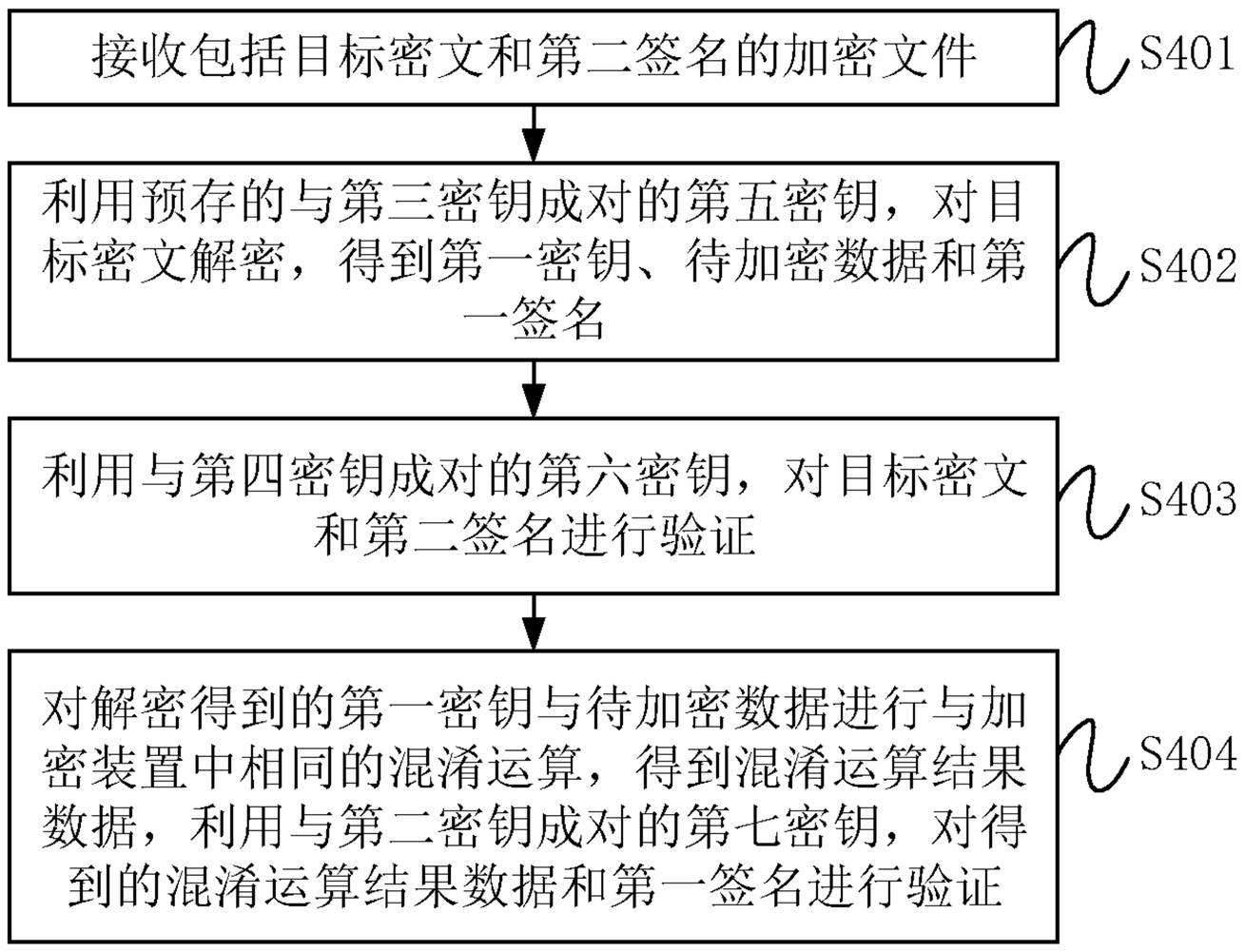

接收包括目标密文和第二签名的加密文件
S401
利用预存的与第三密钥成对的第五密钥，对目标密文解密，得到第一密钥、待加密数据和第一签名
S402
利用与第四密钥成对的第六密钥，对目标密文和第二签名进行验证
S403
对解密得到的第一密钥与待加密数据进行与加密装置中相同的混淆运算，得到混淆运算结果数据，利用与第二密钥成对的第七密钥，对得到的混淆运算结果数据和第一签名进行验证
S404

图 6

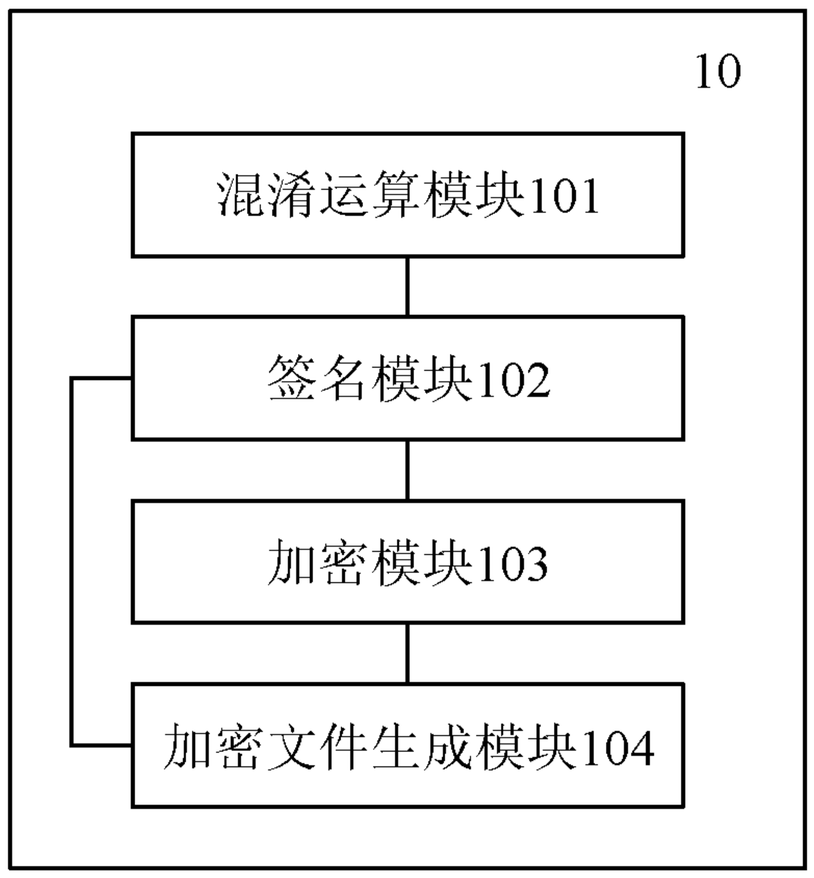

10
混淆运算模块101
签名模块102
加密模块103
加密文件生成模块104

图 7

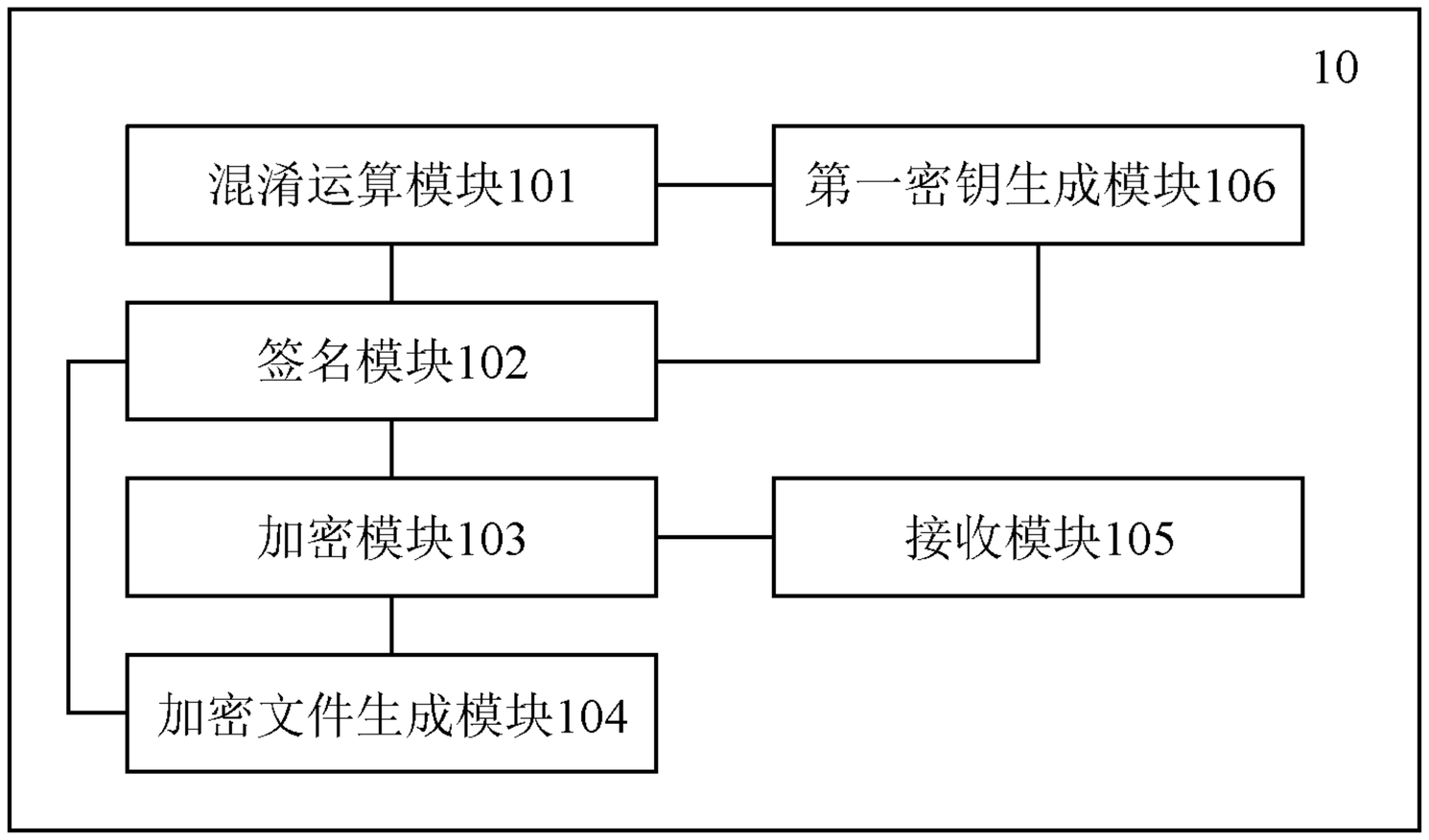

10
混淆运算模块101
第一密钥生成模块106
签名模块102
加密模块103
接收模块105
加密文件生成模块104

图 8

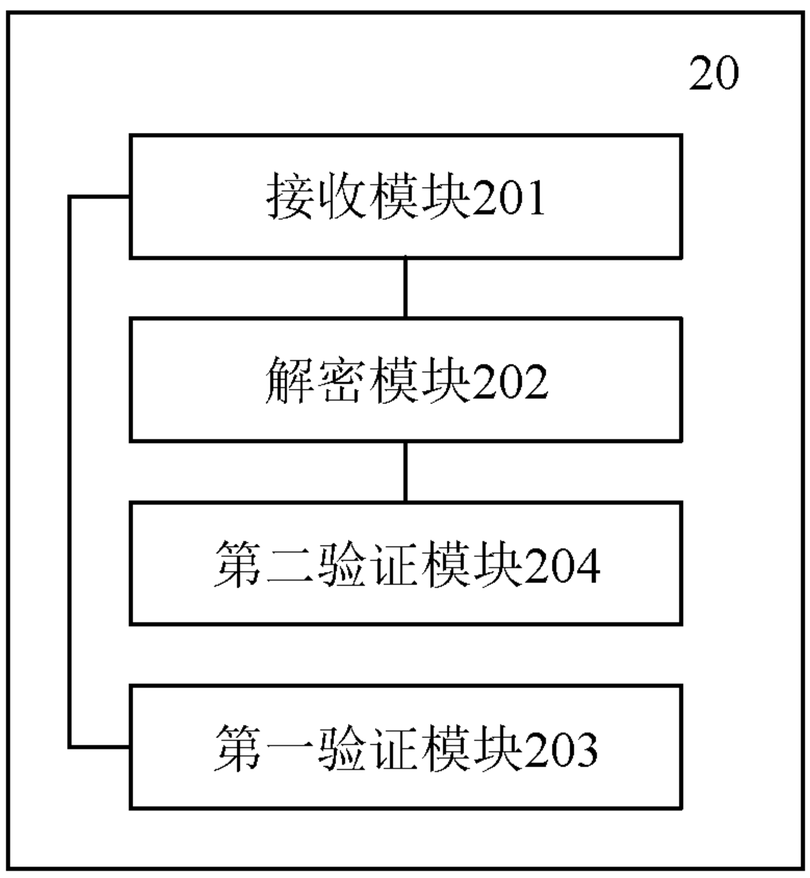

20
接收模块201
解密模块202
第二验证模块204
第一验证模块203

图 9

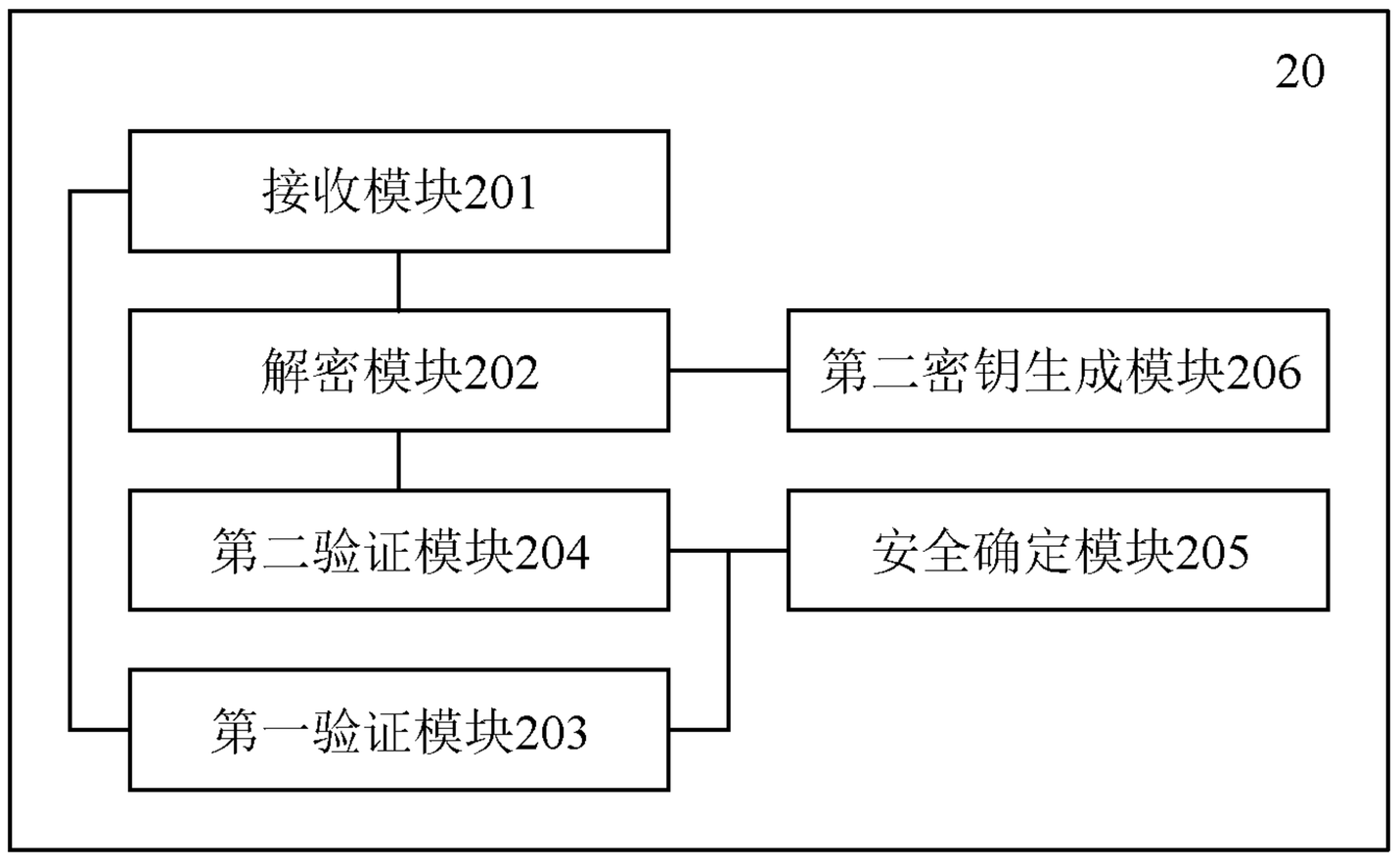

20
接收模块201
解密模块202
第二密钥生成模块206
第二验证模块204
安全确定模块205
第一验证模块203

图 10

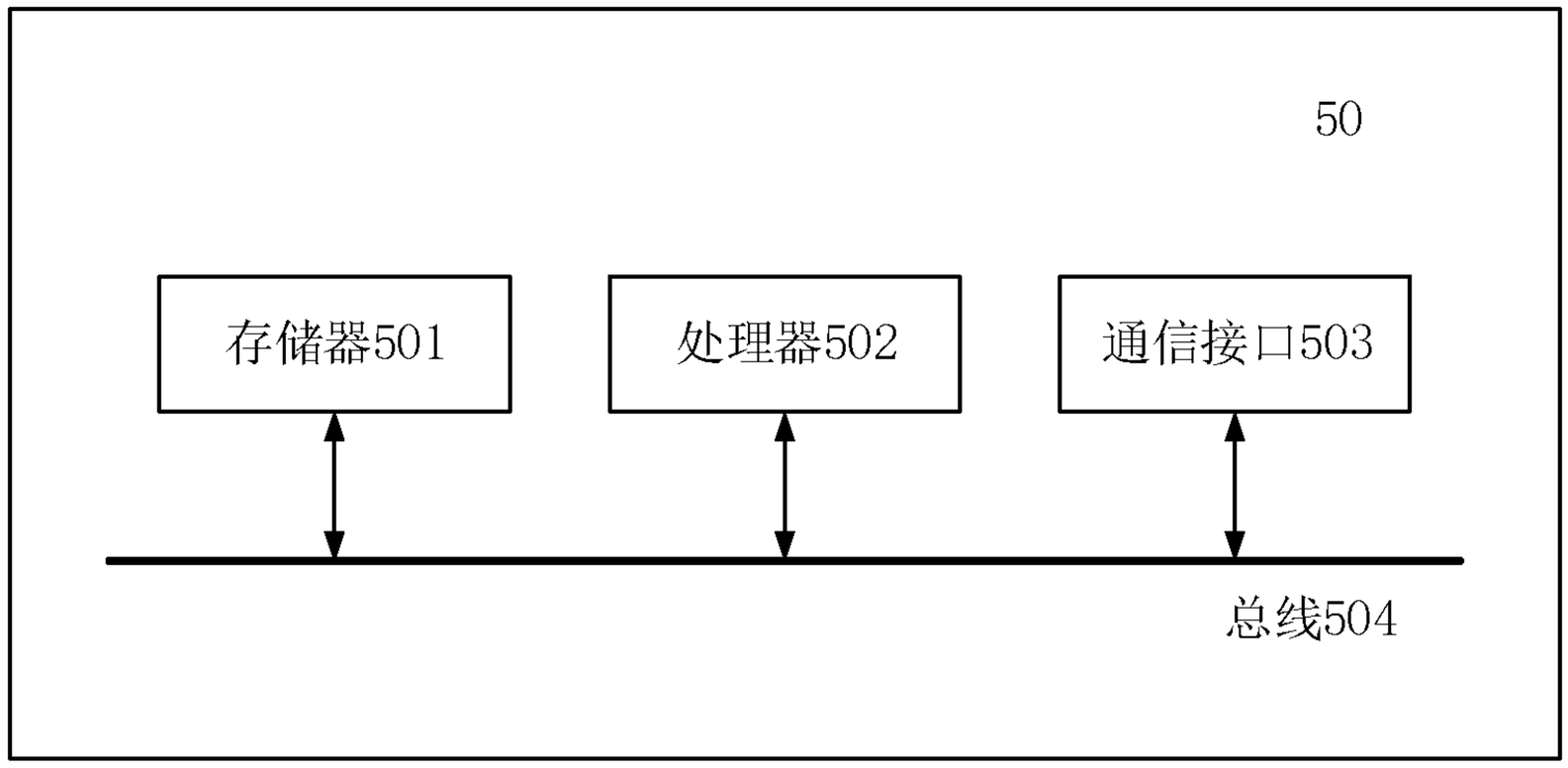

50
存储器501
处理器502
通信接口503
总线504

图 11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2020/118318

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)i; H04L 9/32(2006.01)i; H04L 9/14(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS; CNTXT; CNKI; VEN; USTXT; EPTXT; WOTXT: 原, 待, 加密, 解密, 篡改, 传输, 发送, 明文, 密钥, 公钥, 私钥, 混淆, 签名, 多重, 多级, 多层, 多次, 第一, 第二, encrypt, decrypt, plaintext, public, private, key, confusion, signature, multistage, multiple, first, second

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110891061 A (CHINA UNIONPAY CO., LTD.) 17 March 2020 (2020-03-17) description, paragraphs [0030]-[0040], [0058]-[0068]	1-26
Y	CN 110414190 A (YULONG COMPUTER TELECOMMUNICATION SCIENTIFIC (SHENZHEN) CO., LTD.) 05 November 2019 (2019-11-05) description, paragraphs [0049]-[0057]	1-26
Y	CN 108632296 A (CHINA SPORTS LOTTERY TECHNOLOGY GROUP CO., LTD.) 09 October 2018 (2018-10-09) description, paragraphs [0042]-[0045]	1-26
A	CN 109660542 A (BAIDU ONLINE NETWORK TECHNOLOGY (BEIJING) CO., LTD.) 19 April 2019 (2019-04-19) entire document	1-26
A	US 2007271469 A1 (LG ElECTRONICS INC) 22 November 2007 (2007-11-22) entire document	1-26

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 November 2020	**04 January 2021**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration (ISA/CN)** **No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088** **China** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2020/118318

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	110891061	A	17 March 2020	None			
CN	110414190	A	05 November 2019	None			
CN	108632296	A	09 October 2018	None			
CN	109660542	A	19 April 2019	None			
US	2007271469	A1	22 November 2007	KR	20020086226	A	18 November 2002
				KR	100493284	B1	03 June 2005
				US	20020169973	A1	14 November 2002
				US	7254838	B2	07 August 2007
				US	7877813	B2	25 January 2011

国际检索报告

国际申请号
PCT/CN2020/118318

A. 主题的分类

H04L 29/06(2006.01)i；H04L 9/32(2006.01)i；H04L 9/14(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNABS;CNTXT;CNKI;VEN;USTXT;EPTXT;WOTXT：原，待，加密，解密，篡改，传输，发送，明文，密钥，公钥，私钥，混淆，签名，多重，多级，多层，多次，第一，第二，encrypt，decrypt，plaintext，public，private，key，confusion，signature，multistage，multiple，first，second

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
PX	CN 110891061 A（中国银联股份有限公司）2020年 3月 17日 (2020 - 03 - 17) 说明书第[0030]-[0040]、[0058]-[0068]段	1-26
Y	CN 110414190 A（宇龙计算机通信科技深圳有限公司）2019年 11月 5日 (2019 - 11 - 05) 说明书第[0049]-[0057]段	1-26
Y	CN 108632296 A（中体彩科技发展有限公司）2018年 10月 9日 (2018 - 10 - 09) 说明书第[0042]-[0045]段	1-26
A	CN 109660542 A（百度在线网络技术北京有限公司）2019年 4月 19日 (2019 - 04 - 19) 全文	1-26
A	US 2007271469 A1 (LG ElECTRONICS INC) 2007年 11月 22日 (2007 - 11 - 22) 全文	1-26

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2020年 11月 16日	2021年 1月 4日

ISA/CN的名称和邮寄地址	受权官员
中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	穆剑 电话号码 86-（512）-88995975

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2020/118318

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	110891061	A	2020年 3月 17日	无			
CN	110414190	A	2019年 11月 5日	无			
CN	108632296	A	2018年 10月 9日	无			
CN	109660542	A	2019年 4月 19日	无			
US	2007271469	A1	2007年 11月 22日	KR	20020086226	A	2002年 11月 18日
				KR	100493284	B1	2005年 6月 3日
				US	20020169973	A1	2002年 11月 14日
				US	7254838	B2	2007年 8月 7日
				US	7877813	B2	2011年 1月 25日