(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 110474898 A
(43)申请公布日 2019.11.19

(21)申请号 201910726635.2

(22)申请日 2019.08.07

(71)申请人 北京明朝万达科技股份有限公司
地址 100097 北京市海淀区蓝靛厂南路25号嘉友国际大厦北区2层

(72)发明人 袁朝 喻波 王志海 秦凯 安鹏 郭岩岭

(74)专利代理机构 北京润泽恒知识产权代理有限公司 11319
代理人 莎日娜

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

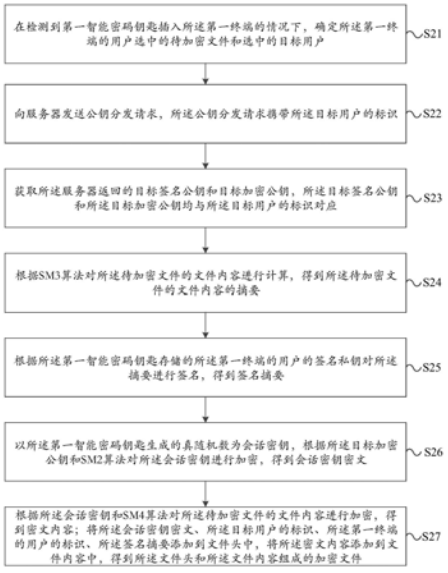
权利要求书3页 说明书13页 附图5页

(54)发明名称

数据加解密和密钥分布方法、装置、设备及可读存储介质

(57)摘要

本申请实施例提供了一种数据加密方法，所述方法应用于第一终端，所述方法包括：在检测到第一智能密码钥匙插入所述第一终端的情况下，确定所述第一终端的用户选中的待加密文件和选中的目标用户；根据SM3算法对所述待加密文件的文件内容进行计算，得到所述待加密文件的文件内容的摘要；根据所述第一智能密码钥匙存储的所述第一终端的用户的签名私钥对所述摘要进行签名，得到签名摘要；以所述第一智能密码钥匙生成的真随机数为会话密钥，根据所述目标加密公钥和SM2算法对所述会话密钥进行加密，得到会话密钥密文；根据所述会话密钥和SM4算法对所述待加密文件的文件内容进行加密，得到密文内容；以提高加密数据的安全性。



CN 110474898 A

1.一种数据加密方法,其特征在于,所述方法应用于第一终端,所述方法包括:

在检测到第一智能密码钥匙插入所述第一终端的情况下,确定所述第一终端的用户选中的待加密文件和选中的目标用户;

向服务器发送公钥分发请求,所述公钥分发请求携带所述目标用户的标识;

获取所述服务器返回的目标签名公钥和目标加密公钥,所述目标签名公钥和所述目标加密公钥均与所述目标用户的标识对应;

根据SM3算法对所述待加密文件的文件内容进行计算,得到所述待加密文件的文件内容的摘要;

根据所述第一智能密码钥匙存储的所述第一终端的用户的签名私钥对所述摘要进行签名,得到签名摘要;

以所述第一智能密码钥匙生成的真随机数为会话密钥,根据所述目标加密公钥和SM2算法对所述会话密钥进行加密,得到会话密钥密文;

根据所述会话密钥和SM4算法对所述待加密文件的文件内容进行加密,得到密文内容;将所述会话密钥密文、所述目标用户的标识、所述第一终端的用户的标识、所述签名摘要添加到文件头中,将所述密文内容添加到文件内容中,得到所述文件头和所述文件内容组成的加密文件。

2.根据权利要求1所述的方法,其特征在于,在根据SM3算法对所述待加密文件的文件内容进行计算,得到所述待加密文件的文件内容的摘要之后,所述方法还包括:

接收所述第一终端的用户输入的第一PIN码;

将所述第一PIN码与所述第一智能密码钥匙存储的第二PIN码进行匹配;

在所述第一PIN码与所述第二PIN码匹配成功的情况下,验证所述第一智能密码钥匙存储的所述第一终端的用户的签名证书和加密证书的有效性;

根据所述第一智能密码钥匙存储的所述第一终端的用户的签名私钥对所述摘要进行签名,包括:

在所述第一终端的用户的签名证书和所述加密证书均有效的情况下,根据所述第一智能密码钥匙存储的所述第一终端的用户签名私钥,对所述摘要进行签名。

3.一种密钥发布方法,其特征在于,所述方法应用于用户终端,所述方法包括:

在检测到智能密码钥匙插入所述用户终端的情况下,将所述智能密码钥匙与所述用户终端的用户标识进行绑定;

获取所述智能密码钥匙存储的所述用户终端的签名公钥和所述用户终端的加密公钥;

向服务器发送公钥发布请求,所述公钥发布请求携带所述用户终端的用户标识;

将所述用户终端的用户标识、所述用户终端的签名公钥以及所述用户终端的加密公钥发送至服务器进行公钥发布,并接收服务器返回的公钥发布结果。

4.根据权利要求3所述的方法,其特征在于,在检测到智能密码钥匙插入所述用户终端的情况下,将所述智能密码钥匙与所述用户终端的用户标识进行绑定之后,所述方法还包括:

接收所述用户终端的用户输入的第三PIN码;

将所述第三PIN码与所述智能密码钥匙存储的第四PIN码进行匹配;

在所述第三PIN码与所述第四PIN码匹配成功的情况下,验证所述智能密码钥匙存储的

所述用户终端的签名证书和所述用户终端的加密证书的有效性；

获取所述智能密码钥匙存储的所述用户终端的签名公钥和所述用户终端的加密公钥，包括：

在所述智能密码钥匙存储的所述用户终端的签名证书和所述用户终端的加密证书均有效的情况下，获取所述智能密码钥匙存储的所述用户终端的签名公钥和所述用户终端的加密公钥。

5.根据权利要求3或4所述的方法，其特征在于，所述智能密码钥匙中存储的所述用户终端的加密证书、所述用户终端的签名证书、所述用户终端的签名公钥以及所述用户终端的加密公钥，是管理终端从证书管理机构申请后导入该智能密码钥匙的。

6.一种数据解密方法，其特征在于，所述方法应用于第二终端，所述方法包括：

在检测到第二智能密码钥匙插入所述第二终端的情况下，确定目标用户选中的加密文件；其中，所述第二智能密码钥匙与所述目标用户对应；

获取所述加密文件中的会话密钥密文、第一终端的用户的标识、签名摘要以及密文内容；

向服务器发送公钥分发请求，所述公钥分发请求携带所述第一终端的用户的标识；

获取所述服务器返回的所述第一终端的用户的签名公钥，所述第一终端的用户的签名公钥与所述第一终端的用户的标识对应；

根据第二智能密码钥匙存储的目标加密私钥对所述会话密钥密文进行解密，得到会话密钥；其中，所述目标加密私钥与所述目标用户的标识对应；

根据所述会话密钥对所述密文内容进行解密，得到明文内容；

根据所述第一终端的用户的签名公钥对所述签名摘要进行验签，得到验签后的摘要；

根据SM3算法对所述明文内容进行计算，得到所述明文内容的摘要；

将所述验签后的摘要与所述明文内容的摘要进行对比，在所述验签后的摘要与所述明文内容的摘要一致的情况下，将所述明文内容写入新建文件，完成所述加密文件的解密。

7.一种数据加密装置，其特征在于，所述装置应用于第一终端，所述装置包括：

第一确定模块模块，用于在检测到第一智能密码钥匙插入所述第一终端的情况下，确定所述第一终端的用户选中的待加密文件和选中的目标用户；

第一公钥分发模块，用于向服务器发送公钥分发请求，所述公钥分发请求携带所述目标用户的标识；

第一获取模块，用于获取所述服务器返回的目标签名公钥和目标加密公钥，所述目标签名公钥和所述目标加密公钥均与所述目标用户的标识对应；

第一计算模块，用于根据SM3算法对所述待加密文件的文件内容进行计算，得到所述待加密文件的文件内容的摘要；

第一签名模块，用于根据所述第一智能密码钥匙存储的所述第一终端的用户的签名私钥对所述摘要进行签名，得到签名摘要；

会话加密模块，用于以所述第一智能密码钥匙生成的真随机数为会话密钥，根据所述目标加密公钥和SM2算法对所述会话密钥进行加密，得到会话密钥密文；

内容加密模块，用于根据所述会话密钥和SM4算法对所述待加密文件的文件内容进行加密，得到密文内容；将所述会话密钥密文、所述目标用户的标识、所述第一终端的用户的

标识、所述签名摘要添加到文件头中，将所述密文内容添加到文件内容中，得到所述文件头和所述文件内容组成的加密文件。

8.一种密钥发布装置，其特征在于，所述装置应用于用户终端，所述装置包括：

绑定模块，用于在检测到智能密码钥匙插入所述用户终端的情况下，将所述智能密码钥匙与所述用户终端的用户标识进行绑定；

第二获取模块，用于获取所述智能密码钥匙存储的所述用户终端的签名公钥和所述用户终端的加密公钥；

公钥发布模块，用于向服务器发送公钥发布请求，所述公钥发布请求携带所述用户终端的用户标识；

发送模块，用于将所述用户终端的用户标识、所述用户终端的签名公钥以及所述用户终端的加密公钥发送至服务器进行公钥发布，并接收服务器返回的公钥发布结果。

9.一种数据解密装置，其特征在于，所述装置应用于第二终端，所述装置包括：

第二确定模块，用于在检测到第二智能密码钥匙插入所述第二终端的情况下，确定目标用户选中的加密文件；其中，所述第二智能密码钥匙与所述目标用户对应；

第三获取模块，用于获取所述加密文件中的会话密钥密文、第一终端的用户的标识、签名摘要以及密文内容；

第二公钥分发模块，用于向服务器发送公钥分发请求，所述公钥分发请求携带所述第一终端的用户的标识；

第三获取模块，用于获取所述服务器返回的所述第一终端的用户的签名公钥，所述第一终端的用户的签名公钥与所述第一终端的用户的标识对应；

会话解密模块，用于根据第二智能密码钥匙存储的目标加密私钥对所述会话密钥密文进行解密，得到会话密钥；其中，所述目标加密私钥与所述目标用户的标识对应；

内容解密模块，用于根据所述会话密钥对所述密文内容进行解密，得到明文内容；

验签模块，用于根据所述第一终端的用户的签名公钥对所述签名摘要进行验签，得到验签后的摘要；

第二计算模块，用于根据SM3算法对所述明文内容进行计算，得到所述明文内容的摘要；

对比模块，用于将所述验签后的摘要与所述明文内容的摘要进行对比，在所述验签后的摘要与所述明文内容的摘要一致的情况下，将所述明文内容写入新建文件，完成所述加密文件的解密。

10.一种计算机可读存储介质，其上存储有计算机程序，其特征在于，该程序被处理器执行时实现如权利要求1-6任一所述的方法中的步骤。

11.一种电子设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其特征在于，所述处理器执行时实现如权利要求1-6任一所述的方法的步骤。

数据加解密和密钥分布方法、装置、设备及可读存储介质

技术领域

[0001] 本申请实施例涉及计算机技术领域，尤其涉及一种数据加密、密钥发布以及数据解密方法、装置、电子设备及可读存储介质。

背景技术

[0002] 随着信息科学与互联网技术的飞跃发展，数据安全问题愈演愈烈，网络与信息安全已获得到前所未有的关注。数据防泄漏系统作为数据安全的终端防护手段，得到了广泛的关注和使用，其中的数据的点对点加解密作为该系统的重要组成之一，对整个系统的使用和发展也起着关键性的作用。

[0003] 相关技术中，数据防泄漏系统中实现数据的点对点加密所采用的技术方案是：通过使用内嵌到程序中的加密公私钥和签名公私钥，伪随机数以及RSA、DES、SHA1等算法，对数据进行点对点加密；但相关技术中，由于伪随机数的安全性较差，且加密公私钥和签名公私钥内嵌到程序容易被不法分子破解，导致该方式生成的加密数据的安全性较低，存在数据泄漏的风险。

发明内容

[0004] 本申请实施例提供一种数据加密、密钥发布以及数据解密方法、装置、电子设备及可读存储介质，以提高加密数据的安全性。

[0005] 本申请实施例第一方面提供了一种数据加密方法，所述方法应用于第一终端，所述方法包括：

[0006] 在检测到第一智能密码钥匙插入所述第一终端的情况下，确定所述第一终端的用户选中的待加密文件和选中的目标用户；

[0007] 向服务器发送公钥分发请求，所述公钥分发请求携带所述目标用户的标识；

[0008] 获取所述服务器返回的目标签名公钥和目标加密公钥，所述目标签名公钥和所述目标加密公钥均与所述目标用户的标识对应；

[0009] 根据SM3算法对所述待加密文件的文件内容进行计算，得到所述待加密文件的文件内容的摘要；

[0010] 根据所述第一智能密码钥匙存储的所述第一终端的用户的签名私钥对所述摘要进行签名，得到签名摘要；

[0011] 以所述第一智能密码钥匙生成的真随机数为会话密钥，根据所述目标加密公钥和SM2算法对所述会话密钥进行加密，得到会话密钥密文；

[0012] 根据所述会话密钥和SM4算法对所述待加密文件的文件内容进行加密，得到密文内容；将所述会话密钥密文、所述目标用户的标识、所述第一终端的用户的标识、所述签名摘要添加到文件头中，将所述密文内容添加到文件内容中，得到所述文件头和所述文件内容组成的加密文件。

[0013] 可选地，在根据SM3算法对所述待加密文件的文件内容进行计算，得到所述待加密

文件的文件内容的摘要之后，所述方法还包括：

[0014] 接收所述第一终端的用户输入的第一PIN码；

[0015] 将所述第一PIN码与所述第一智能密码钥匙存储的第二PIN码进行匹配；

[0016] 在所述第一PIN码与所述第二PIN码匹配成功的情况下，验证所述第一智能密码钥匙存储的所述第一终端的用户的签名证书和加密证书的有效性；

[0017] 根据所述第一智能密码钥匙存储的所述第一终端的用户的签名私钥对所述摘要进行签名，包括：

[0018] 在所述第一终端的用户的签名证书和所述加密证书均有效的情况下，根据所述第一智能密码钥匙存储的所述第一终端的用户签名私钥，对所述摘要进行签名。

[0019] 本申请实施例第二方面提供了一种密钥发布方法，所述方法应用于用户终端，所述方法包括：

[0020] 在检测到智能密码钥匙插入所述用户终端的情况下，将所述智能密码钥匙与所述用户终端的用户标识进行绑定；

[0021] 获取所述智能密码钥匙存储的所述用户终端的签名公钥和所述用户终端的加密公钥；

[0022] 向服务器发送公钥发布请求，所述公钥发布请求携带所述用户终端的用户标识；

[0023] 将所述用户终端的用户标识、所述用户终端的签名公钥以及所述用户终端的加密公钥发送至服务器进行公钥发布，并接收服务器返回的公钥发布结果。

[0024] 可选地，在检测到智能密码钥匙插入所述用户终端的情况下，将所述智能密码钥匙与所述用户终端的用户标识进行绑定之后，所述方法还包括：

[0025] 接收所述用户终端的用户输入的第三PIN码；

[0026] 将所述第三PIN码与所述智能密码钥匙存储的第四PIN码进行匹配；

[0027] 在所述第三PIN码与所述第四PIN码匹配成功的情况下，验证所述智能密码钥匙存储的所述用户终端的签名证书和所述用户终端的加密证书的有效性；

[0028] 获取所述智能密码钥匙存储的所述用户终端的签名公钥和所述用户终端的加密公钥，包括：

[0029] 在所述智能密码钥匙存储的所述用户终端的签名证书和所述用户终端的加密证书均有效的情况下，获取所述智能密码钥匙存储的所述用户终端的签名公钥和所述用户终端的加密公钥。

[0030] 可选地，所述智能密码钥匙中存储的所述用户终端的加密证书、所述用户终端的签名证书、所述用户终端的签名公钥以及所述用户终端的加密公钥，是管理终端从证书管理机构申请后导入该智能密码钥匙的。

[0031] 本申请实施例第三方面提供了一种数据解密方法，所述方法应用于第二终端，所述方法包括：

[0032] 在检测到第二智能密码钥匙插入所述第二终端的情况下，确定目标用户选中的加密文件；其中，所述第二智能密码钥匙与所述目标用户对应；

[0033] 获取所述加密文件中的会话密钥密文、第一终端的用户的标识、签名摘要以及密文内容；

[0034] 向服务器发送公钥分发请求，所述公钥分发请求携带所述第一终端的用户的标

识；

[0035] 获取所述服务器返回的所述第一终端的用户的签名公钥，所述第一终端的用户的签名公钥与所述第一终端的用户的标识对应；

[0036] 根据第二智能密码钥匙存储的目标加密私钥对所述会话密钥密文进行解密，得到会话密钥；其中，所述目标加密私钥与所述目标用户的标识对应；

[0037] 根据所述会话密钥对所述密文内容进行解密，得到明文内容；

[0038] 根据所述第一终端的用户的签名公钥对所述签名摘要进行验签，得到验签后的摘要；

[0039] 根据SM3算法对所述明文内容进行计算，得到所述明文内容的摘要；

[0040] 将所述验签后的摘要与所述明文内容的摘要进行对比，在所述验签后的摘要与所述明文内容的摘要一致的情况下，将所述明文内容写入新建文件，完成所述加密文件的解密。

[0041] 本申请实施例第四方面提供一种数据加密装置，所述装置应用于第一终端，所述装置包括：

[0042] 选中模块，用于在检测到第一智能密码钥匙插入所述第一终端的情况下，确定所述第一终端的用户选中的待加密文件和选中的目标用户；

[0043] 第一公钥分发模块，用于向服务器发送公钥分发请求，所述公钥分发请求携带所述目标用户的标识；

[0044] 第一获取模块，用于获取所述服务器返回的目标签名公钥和目标加密公钥，所述目标签名公钥和所述目标加密公钥均与所述目标用户的标识对应；

[0045] 第一计算模块，用于根据SM3算法对所述待加密文件的文件内容进行计算，得到所述待加密文件的文件内容的摘要；

[0046] 第一签名模块，用于根据所述第一智能密码钥匙存储的所述第一终端的用户的签名私钥对所述摘要进行签名，得到签名摘要；

[0047] 会话加密模块，用于以所述第一智能密码钥匙生成的真随机数为会话密钥，根据所述目标加密公钥和SM2算法对所述会话密钥进行加密，得到会话密钥密文；

[0048] 内容加密模块，用于根据所述会话密钥和SM4算法对所述待加密文件的文件内容进行加密，得到密文内容；将所述会话密钥密文、所述目标用户的标识、所述第一终端的用户的标识、所述签名摘要添加到文件头中，将所述密文内容添加到文件内容中，得到所述文件头和所述文件内容组成的加密文件。

[0049] 可选地，所述装置还包括：

[0050] 第一接收模块，用于接收所述第一终端的用户输入的第一PIN码；

[0051] 第一匹配模块，用于将所述第一PIN码与所述第一智能密码钥匙存储的第二PIN码进行匹配；

[0052] 第一验证模块，用于在所述第一PIN码与所述第二PIN码匹配成功的情况下，验证所述第一智能密码钥匙存储的所述第一终端的用户的签名证书和加密证书的有效性；

[0053] 第一签名模块包括：

[0054] 第一签名子模块，用于在所述第一终端的用户的签名证书和所述加密证书均有效的情况下，根据所述第一智能密码钥匙存储的所述第一终端的用户签名私钥，对所述摘要

进行签名。

[0055] 本申请实施例第五方面提供一种密钥发布装置，所述装置应用于用户终端，所述装置包括：

[0056] 绑定模块，用于在检测到智能密码钥匙插入所述用户终端的情况下，将所述智能密码钥匙与所述用户终端的用户标识进行绑定；

[0057] 第二获取模块，用于获取所述智能密码钥匙存储的所述用户终端的签名公钥和所述用户终端的加密公钥；

[0058] 公钥发布模块，用于向服务器发送公钥发布请求，所述公钥发布请求携带所述用户终端的用户标识；

[0059] 发送模块，用于将所述用户终端的用户标识、所述用户终端的签名公钥以及所述用户终端的加密公钥发送至服务器进行公钥发布，并接收服务器返回的公钥发布结果。

[0060] 可选地，所述装置还包括

[0061] 第二接收模块，用于接收所述用户终端的用户输入的第三PIN码；

[0062] 第二匹配模块，用于将所述第三PIN码与所述智能密码钥匙存储的第四PIN码进行匹配；

[0063] 第二验证模块，用于在所述第三PIN码与所述第四PIN码匹配成功的情况下，验证所述智能密码钥匙存储的所述用户终端的签名证书和所述用户终端的加密证书的有效性；

[0064] 第二获取模块包括：

[0065] 第二获取子模块，用于在所述智能密码钥匙存储的所述用户终端的签名证书和所述用户终端的加密证书均有效的情况下，获取所述智能密码钥匙存储的所述用户终端的签名公钥和所述用户终端的加密公钥。

[0066] 可选地，所述智能密码钥匙中存储的所述用户终端的加密证书、所述用户终端的签名证书、所述用户终端的签名公钥以及所述用户终端的加密公钥，是管理终端从证书管理机构申请后导入该智能密码钥匙的。

[0067] 本申请实施例第六方面提供一种数据解密装置，所述装置应用于第二终端，所述装置包括：

[0068] 确定模块，用于在检测到第二智能密码钥匙插入所述第二终端的情况下，确定目标用户选中的加密文件；其中，所述第二智能密码钥匙与所述目标用户对应；

[0069] 第三获取模块，用于获取所述加密文件中的会话密钥密文、第一终端的用户的标识、签名摘要以及密文内容；

[0070] 第二公钥分发模块，用于向服务器发送公钥分发请求，所述公钥分发请求携带所述第一终端的用户的标识；

[0071] 第三获取模块，用于获取所述服务器返回的所述第一终端的用户的签名公钥，所述第一终端的用户的签名公钥与所述第一终端的用户的标识对应；

[0072] 会话解密模块，用于根据第二智能密码钥匙存储的目标加密私钥对所述会话密钥密文进行解密，得到会话密钥；其中，所述目标加密私钥与所述目标用户的标识对应；

[0073] 内容解密模块，用于根据所述会话密钥对所述密文内容进行解密，得到明文内容；

[0074] 验签模块，用于根据所述第一终端的用户的签名公钥对所述签名摘要进行验签，得到验签后的摘要；

[0075] 第二计算模块，用于根据SM3算法对所述明文内容进行计算，得到所述明文内容的摘要；

[0076] 对比模块，用于将所述验签后的摘要与所述明文内容的摘要进行对比，在所述验签后的摘要与所述明文内容的摘要一致的情况下，将所述明文内容写入新建文件，完成所述加密文件的解密。

[0077] 本申请实施例第七方面提供一种计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时实现如本申请第一、第二以及第三方面所述的方法中的步骤。

[0078] 本申请实施例第八方面提供一种电子设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行时实现本申请第一、第二以及第三方面所述的方法的步骤。

[0079] 采用本申请实施例提供的一种数据加密方法，本申请包括以下优点：

[0080] 1)本申请通过将加密公私钥、签名公私钥、加密证书和签名证书导入至智能密码钥匙中，在对数据的加密和解密过程中均需要使用相应的智能密码钥匙，且只有合法持有相应智能密码钥匙的持有人才能进行相应的加密和解密处理，不同于相关技术中，将加密公私钥和签名公私钥内嵌至程序中，易破解，导致数据易泄漏。

[0081] 2)本申请通过采用智能密码钥匙中的真随机数对数据进行加密，真随机数具有不可重现性，因此，相同的明文数据每一次的加密结果都不一样，从而增强了加密数据的破解难度。

[0082] 3)本申请通过采用SM2、SM3以及SM4等国密算法对数据进行加密，不同于相关技术中，采用RSA、DES以及SHA1等算法，本申请采用的算法更加复杂，安全性更高，更不易被破解。

附图说明

[0083] 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的描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0084] 图1是本申请一实施例提出的一种密钥发布方法的流程图；

[0085] 图2是本申请一实施例提出的一种数据加密方法的流程图；

[0086] 图3是本申请一实施例提出的一种数据解密方法的流程图；

[0087] 图4是本申请一实施例提出的一种数据加密装置的示意图；

[0088] 图5是本申请一实施例提出的一种密钥发布装置的示意图；

[0089] 图6是本申请一实施例提出的一种数据解密装置的示意图。

具体实施方式

[0090] 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清楚、完整地描述，显然，所描述的实施例是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

[0091] 本申请的发明人在实现本申请的过程中发现，相关技术中，数据防泄漏系统中实现数据的点对点加密所采用的技术方案是：通过使用内嵌到程序中的加密公私钥和签名公私钥，伪随机数以及RSA、DES、SHA1等算法，对数据进行点对点加密；由于伪随机数的安全性较差，且加密公私钥和签名公私钥内嵌到程序容易被不法分子破解，导致该方式生成的加密数据的安全性较低，存在数据泄漏的风险。

[0092] 为解决相关技术中，数据防泄漏系统中采用的点对点加密生成的加密数据的安全性不高的技术缺陷，本申请提出以下方法：

[0093] 首先，对需要进行数据加解密的终端进行系统初始化，具体地，系统管理员从控制台配置点对点加密策略，配置完成后同步数据。终端上安装的客户端的心跳模块发送请求，服务器接到请求后处理策略下发，并将点对点加密策略下发给客户端。客户端更新本地策略文件。

[0094] 参考图1，图1是本申请一实施例提出的一种密钥发布方法的流程图。如图1所示，所述方法应用于用户终端，该方法包括以下步骤：

[0095] 步骤S11：在检测到智能密码钥匙插入所述用户终端的情况下，将所述智能密码钥匙与所述用户终端的用户标识进行绑定。

[0096] 在本实施例中，智能密码钥匙是指各个用户所持有的不同的智能密码钥匙，不同的智能密码钥匙可以插入不同的用户终端，也可以插入同一用户终端，但一个智能密码钥匙只能唯一绑定一个用户标识，该用户标识是当前在用户终端操作的用户所携带的标识。其中，所述用户终端包括下述的第一终端和第二终端，所述用户标识包括但不限于：该用户注册的账号和该用户的身份证账号。

[0097] 示例地，以智能密码钥匙A、智能密码钥匙B以及智能密码钥匙C为例，当用户1持有智能密码钥匙A，将智能密码钥匙A插入终端A时，该智能密码钥匙A与用户1的用户标识进行唯一绑定，则智能密码钥匙B和智能密码钥匙C只能分别绑定别的用户标识。

[0098] 在本实施例中，智能密码钥匙是一种USB接口的硬件设备，其内置单片机或智能卡芯片，设有存储空间，用于存储加密公私钥、签名公私钥、加密证书和签名证书，以及生成真随机数。

[0099] 步骤S12：获取所述智能密码钥匙存储的所述用户终端的签名公钥和所述用户终端的加密公钥。

[0100] 在一种可选的实施方式中，步骤S12之前还包括以下步骤：

[0101] 接收所述用户终端的用户输入的第三PIN码；

[0102] 将所述第三PIN码与所述智能密码钥匙存储的第四PIN码进行匹配；

[0103] 在所述第三PIN码与所述第四PIN码匹配成功的情况下，验证所述智能密码钥匙存储的所述用户终端的签名证书和所述用户终端的加密证书的有效性；

[0104] 获取所述智能密码钥匙存储的所述用户终端的签名公钥和所述用户终端的加密公钥，包括：

[0105] 在所述智能密码钥匙存储的所述用户终端的签名证书和所述用户终端的加密证书均有效的情况下，获取所述智能密码钥匙存储的所述用户终端的签名公钥和所述用户终端的加密公钥。

[0106] 在本实施例中，通过对第三PIN码和第四PIN码进行匹配，保证只有与智能密码钥

匙进行唯一绑定的合法持有人才能使用该智能密码钥匙，防止拾到智能密码钥匙的人恶意使用或非法伪造。

[0107] 在本实施例中，在验证智能密码钥匙的持有人合法后，进一步验证所述智能密码钥匙中存储的所述用户终端的签名证书和所述用户终端的加密证书的有效性，具体地，验证所述用户终端的签名证书和所述用户终端的加密证书的有效性的方法采用现有技术中的：数字证书有效期验证、根证书验证以及CRL验证，在此不再赘述。所述签名证书和加密证书中均包括：用户终端的标识、用户终端的公钥、证书序列号、证书发行者名称、证书的失效日期以及证书管理机构的签名。

[0108] 通过上述技术方案，在验证持有智能密码钥匙的用户终端的用户合法、以及智能密码钥匙中存储的所述用户终端的签名证书和所述用户终端的加密证书有效之后，才获取所述智能密码钥匙存储的所述用户终端的签名公钥和所述用户终端的加密公钥，增强公钥发布的安全性，防止非法伪造公钥。

[0109] 步骤S13：向服务器发送公钥发布请求，所述公钥发布请求携带所述用户终端的用户标识。

[0110] 步骤S14：将所述用户终端的用户标识、所述用户终端的签名公钥以及所述用户终端的加密公钥发送至服务器进行公钥发布，并接收服务器返回的公钥发布结果。

[0111] 在本实施例中，用户终端将所述用户终端的用户标识、所述用户终端的签名公钥以及所述用户终端的加密公钥发送至服务器进行公钥发布后，服务器在本地保存所述用户终端的用户标识、所述用户终端的签名公钥以及所述用户终端的加密公钥，便于后续根据所述用户终端的用户标识调用相应的用户终端的签名公钥以及相应的用户终端的加密公钥对数据进行加解密。

[0112] 在一种可选的实施方式中，所述智能密码钥匙中存储的所述用户终端的加密证书、所述用户终端的签名证书、所述用户终端的签名公钥以及所述用户终端的加密公钥，是管理终端从证书管理机构申请后导入该智能密码钥匙的。

[0113] 在本实施例中，在智能密码钥匙插入所述用户终端之前，管理员首先在管理终端上插入所述智能密码钥匙，并向证书管理机构申请加密证书、签名证书、签名公钥以及加密公钥，然后将上述申请的加密证书、签名证书、签名公钥以及加密公钥导入至所述智能密码钥匙中，最后，将所述智能密码钥匙分发给用户终端。

[0114] 在上述步骤S11中，所述智能密码钥匙与所述用户终端的用户标识进行绑定之后，当前智能密码钥匙中存储的向证书管理机构申请的加密证书、签名证书、签名公钥以及加密公钥均与用户终端的用户标识进行绑定。

[0115] 参考图2，图2是本申请一实施例提出的一种数据加密方法的流程图。如图2所示，所述方法应用于第一终端，该方法包括以下步骤：

[0116] 步骤S21：在检测到第一智能密码钥匙插入所述第一终端的情况下，确定所述第一终端的用户选中的待加密文件和选中的目标用户。

[0117] 在本实施例中，第一智能密码钥匙为第一终端的用户唯一绑定的智能密码钥匙，第一终端的用户为在第一终端上操作的用户，第一终端的用户为待加密文件的加密方，目标用户为对加密文件实现解密的唯一解密方。第一终端的用户选中目标用户，即为选中目标用户的标识，例如：选中目标用户的账号。

[0118] 步骤S22:向服务器发送公钥分发请求,所述公钥分发请求携带所述目标用户的标识。

[0119] 步骤S23:获取所述服务器返回的目标签名公钥和目标加密公钥,所述目标签名公钥和所述目标加密公钥均与所述目标用户的标识对应。

[0120] 在本实施例中,第一终端向服务器发送公钥分发请求,服务器根据公钥分发请求中携带的目标用户的标识,从服务器中找到目标签名公钥和目标加密公钥,同时,第一终端将接收到的目标签名公钥和目标加密公钥保存在本地。

[0121] 步骤S24:根据SM3算法对所述待加密文件的文件内容进行计算,得到所述待加密文件的文件内容的摘要。

[0122] 在本实施例中,SM3算法(国产哈希算法)是国密算法,相较于相关技术中的:采用SHA1算法对待加密文件的文件内容进行计算,得到所述待加密文件的文件内容的摘要,采用SM3算法的安全性更高,更不易被破解。

[0123] 在一种实施方式中,步骤S24之后,还包括以下步骤:

[0124] 接收所述第一终端的用户输入的第一PIN码;

[0125] 将所述第一PIN码与所述第一智能密码钥匙存储的第二PIN码进行匹配;

[0126] 在所述第一PIN码与所述第二PIN码匹配成功的情况下,验证所述第一智能密码钥匙存储的所述第一终端的用户的签名证书和加密证书的有效性;

[0127] 根据所述第一智能密码钥匙存储的所述第一终端的用户的签名私钥对所述摘要进行签名,包括:

[0128] 在所述第一终端的用户的签名证书和所述加密证书均有效的情况下,根据所述第一智能密码钥匙存储的所述第一终端的用户签名私钥,对所述摘要进行签名。

[0129] 在本实施例中,在第一终端的用户使用其自身的签名私钥对摘要签名之前,对第一终端的用户进行验证,保证持有第一智能密码钥匙的第一终端的用户的合法性,从而使得只有合法持有人才能对待加密文件的摘要进行签名,进一步保证对待加密文件进行加密的安全性,防止拾到第一智能密码钥匙的人恶意使用或非法伪造。

[0130] 步骤S25:根据所述第一智能密码钥匙存储的所述第一终端的用户的签名私钥对所述摘要进行签名,得到签名摘要。

[0131] 在本实施例中,采用第一智能密码钥匙中存储的第一终端的用户的签名私钥对所述摘要进行签名,其中,签名是指用SM3算法从待加密文件中生成报文摘要,然后使用第一终端的用户的签名私钥对所述摘要进行加密,得到签名摘要。

[0132] 由于第一终端的用户的签名私钥存储于第一智能密码钥匙中,且第一智能密码钥匙与第一终端的用户进行了唯一绑定,使得只有第一智能密码钥匙的合法持有人才能对所述摘要进行签名,不同于相关技术中,对摘要进行签名的签名私钥内嵌于程序中,导致签名私钥易被盗取,增强了待加密文件的加密安全性;且签名私钥存储于第一智能密码钥匙的硬件设备中,具有不可复制性,更进一步加强了签名私钥的使用安全性。

[0133] 步骤S26:以所述第一智能密码钥匙生成的真随机数为会话密钥,根据所述目标加密公钥和SM2算法对所述会话密钥进行加密,得到会话密钥密文。

[0134] 在本实施例中,SM2算法是国密算法,为非对称加解密算法,相较于相关技术中的:采用RSA算法实现非对称加解密,SM2算法比RSA算法更加复杂,安全性更高,更不易被破解。

[0135] 步骤S27:根据所述会话密钥和SM4算法对所述待加密文件的文件内容进行加密,得到密文内容;将所述会话密钥密文、所述目标用户的标识、所述第一终端的用户的标识、所述签名摘要添加到文件头中,将所述密文内容添加到文件内容中,得到所述文件头和所述文件内容组成的加密文件。

[0136] 在本实施例中,采用真随机数对所述待加密文件的文件内容进行加密,真随机数具有不可重现性,因此,相同的明文数据每一次的加密结果都不一样,从而增强了加密文件的破解难度。

[0137] 在本实施例中,SM4算法是国密算法,为对称加解密算法,相较于相关技术中:采用DES算法实现对称加解密,SM4算法比DES算法更加复杂,安全性更高,更不易被破解。

[0138] 参考图3,图3是本申请一实施例提出的一种数据解密方法的流程图。如图3所示,所述方法应用于第二终端,该方法包括以下步骤:

[0139] 步骤S31:在检测到第二智能密码钥匙插入所述第二终端的情况下,确定目标用户选中的加密文件;其中,所述第二智能密码钥匙与所述目标用户对应。

[0140] 在本实施例中,第二智能密码钥匙为目标用户唯一绑定的智能密码钥匙;由于待加密文件在加密时,是使用目标用户的目标加密公钥和SM2的非对称加密算法进行加密的,因此,对加密文件进行解密时,必须使用目标用户的目标加密私钥进行解密,目标用户为对加密文件实现解密的唯一解密方。

[0141] 步骤S32:获取所述加密文件中的会话密钥密文、第一终端的用户的标识、签名摘要以及密文内容。

[0142] 在本实施例中,所述会话密钥密文、第一终端的用户的标识以及签名摘要存储于加密文件的文件头中,所述密文内容存储于加密文件的文件内容中。

[0143] 步骤S33:向服务器发送公钥分发请求,所述公钥分发请求携带所述第一终端的用户的标识。

[0144] 步骤S34:获取所述服务器返回的所述第一终端的用户的签名公钥,所述第一终端的用户的签名公钥与所述第一终端的用户的标识对应。

[0145] 在本实施例中,由于待加密文件在加密的过程中,采用第一终端的用户的签名私钥对摘要进行签名,因此,对加密文件的解密需要第一终端的用户的签名公钥。由本申请公开的密钥发布方法可知,第一终端的用户的加密公钥和签名公钥均发送至服务器进行公钥发布,并保存至本地,因此,第二终端向服务器发送公钥分发请求,服务器根据公钥分发请求中的第一终端的用户的标识,从服务器中找到第一终端的用户的签名公钥,同时,第一终端将接收到的第一终端的用户的签名公钥保存在本地。

[0146] 步骤S35:根据第二智能密码钥匙存储的目标加密私钥对所述会话密钥密文进行解密,得到会话密钥;其中,所述目标加密私钥与所述目标用户的标识对应。

[0147] 在本实施例中,所述会话密钥密文是所述目标加密公钥对所述会话密钥采用SM2的非对称算法进行加密后得到的,因此,对会话密钥密文进行解密时,需要使用所述目标用户的目标加密私钥。

[0148] 而目标加密私钥存储于与所述目标用户唯一绑定的第二智能密码钥匙中,不可导出,因此,对加密文件的解密过程必须要使用对应的智能密码钥匙,不同于相关技术中,加密公私钥和签名公私钥内嵌于程序中,易破解,存在数据泄漏的风险。

[0149] 在一种实施方式中，在步骤S35之前，还包括以下步骤：

[0150] 接收所述目标用户输入的第五PIN码；

[0151] 将所述第五PIN码与所述第二智能密码钥匙存储的第六PIN码进行匹配；

[0152] 在所述第五PIN码与所述第六PIN码匹配成功的情况下，验证所述第二智能密码钥匙存储的所述目标用户的签名证书和所述目标用户的加密证书的有效性；

[0153] 根据所述第二智能密码钥匙存储的目标加密私钥对所述会话密钥密文进行解密，包括：

[0154] 所述目标用户的签名证书和加密证书均有效的情况下，根据所述第二智能密码钥匙存储的目标加密私钥对所述会话密钥密文进行解密。

[0155] 在本实施例中，在根据第二智能密码钥匙存储的目标加密私钥对会话密钥密文进行解密之前，对目标用户进行验证，保证持有第二智能密码钥匙的目标用户的合法性，增强加密文件的解密安全性，防止拾到第二智能密码钥匙的人恶意使用或非法伪造，避免加密文件中的数据泄漏。

[0156] 步骤S36：根据所述会话密钥对所述密文内容进行解密，得到明文内容。

[0157] 在本实施例中，由于对待加密文件的文件内容进行加密时是采用的会话密钥和SM4的对称加解密算法，因此，对加密文件的密文内容采用相同的会话密钥进行解密，得到明文内容。

[0158] 步骤S37：根据所述第一终端的用户的签名公钥对所述签名摘要进行验签，得到验签后的摘要。

[0159] 步骤S38：根据SM3算法对所述明文内容进行计算，得到所述明文内容的摘要。

[0160] 步骤S39：将所述验签后的摘要与所述明文内容的摘要进行对比，在所述验签后的摘要与所述明文内容的摘要一致的情况下，将所述明文内容写入新建文件，完成所述加密文件的解密。

[0161] 在本实施例中，为了验证所述加密文件是否被篡改，将明文内容的摘要与验签后的摘要进行对比，若一致，则证明该加密文件没有被篡改，此时，将明文内容写入新建文件，完成所述加密文件的解密，保证解密后的文件的完整性。

[0162] 基于同一发明构思，本申请一实施例提供一种数据加密装置。参考图4，图4是本申请一实施例提出的一种数据加密装置的示意图。如图4所示，所述装置应用于第一终端，该装置包括：

[0163] 选中模块401，用于在检测到第一智能密码钥匙插入所述第一终端的情况下，确定所述第一终端的用户选中的待加密文件和选中的目标用户；

[0164] 第一公钥分发模块402，用于向服务器发送公钥分发请求，所述公钥分发请求携带所述目标用户的标识；

[0165] 第一获取模块403，用于获取所述服务器返回的目标签名公钥和目标加密公钥，所述目标签名公钥和所述目标加密公钥均与所述目标用户的标识对应；

[0166] 第一计算模块404，用于根据SM3算法对所述待加密文件的文件内容进行计算，得到所述待加密文件的文件内容的摘要；

[0167] 第一签名模块405，用于根据所述第一智能密码钥匙存储的所述第一终端的用户的签名私钥对所述摘要进行签名，得到签名摘要；

[0168] 会话加密模块406，用于以所述第一智能密码钥匙生成的真随机数为会话密钥，根据所述目标加密公钥和SM2算法对所述会话密钥进行加密，得到会话密钥密文；

[0169] 内容加密模块407，用于根据所述会话密钥和SM4算法对所述待加密文件的文件内容进行加密，得到密文内容；将所述会话密钥密文、所述目标用户的标识、所述第一终端的用户的标识、所述签名摘要添加到文件头中，将所述密文内容添加到文件内容中，得到所述文件头和所述文件内容组成的加密文件。

[0170] 所述装置还包括：

[0171] 第一接收模块，用于接收所述第一终端的用户输入的第一PIN码；

[0172] 第一匹配模块，用于将所述第一PIN码与所述第一智能密码钥匙存储的第二PIN码进行匹配；

[0173] 第一验证模块，用于在所述第一PIN码与所述第二PIN码匹配成功的情况下，验证所述第一智能密码钥匙存储的所述第一终端的用户的签名证书和加密证书的有效性；

[0174] 第一签名模块包括：

[0175] 第一签名子模块，用于在所述第一终端的用户的签名证书和所述加密证书均有效的情况下，根据所述第一智能密码钥匙存储的所述第一终端的用户签名私钥，对所述摘要进行签名。

[0176] 基于同一发明构思，本申请一实施例提供一种密钥发布装置。参考图5，图5是本申请一实施例提出的一种密钥发布装置的示意图。如图5所示，所述装置应用于用户终端，该装置包括：

[0177] 绑定模块501，用于在检测到智能密码钥匙插入所述用户终端的情况下，将所述智能密码钥匙与所述用户终端的用户标识进行绑定；

[0178] 第二获取模块502，用于获取所述智能密码钥匙存储的所述用户终端的签名公钥和所述用户终端的加密公钥；

[0179] 公钥发布模块503，用于向服务器发送公钥发布请求，所述公钥发布请求携带所述用户终端的用户标识；

[0180] 发送模块504，用于将所述用户终端的用户标识、所述用户终端的签名公钥以及所述用户终端的加密公钥发送至服务器进行公钥发布，并接收服务器返回的公钥发布结果。

[0181] 所述装置还包括

[0182] 第二接收模块，用于接收所述用户终端的用户输入的第三PIN码；

[0183] 第二匹配模块，用于将所述第三PIN码与所述智能密码钥匙存储的第四PIN码进行匹配；

[0184] 第二验证模块，用于在所述第三PIN码与所述第四PIN码匹配成功的情况下，验证所述智能密码钥匙存储的所述用户终端的签名证书和所述用户终端的加密证书的有效性；

[0185] 第二获取模块包括：

[0186] 第二获取子模块，用于在所述智能密码钥匙存储的所述用户终端的签名证书和所述用户终端的加密证书均有效的情况下，获取所述智能密码钥匙存储的所述用户终端的签名公钥和所述用户终端的加密公钥。

[0187] 所述智能密码钥匙中存储的所述用户终端的加密证书、所述用户终端的签名证书、所述用户终端的签名公钥以及所述用户终端的加密公钥，是管理终端从证书管理机构

申请后导入该智能密码钥匙的。

[0188] 基于同一发明构思，本申请一实施例提供一种数据解密装置。参考图6，图6是本申请一实施例提出的一种数据解密装置的示意图。如图6所示，所述装置应用于第二终端，所述装置应用于用户终端，该装置包括：

[0189] 确定模块601，用于在检测到第二智能密码钥匙插入所述第二终端的情况下，确定目标用户选中的加密文件；其中，所述第二智能密码钥匙与所述目标用户对应；

[0190] 第三获取模块602，用于获取所述加密文件中的会话密钥密文、第一终端的用户的标识、签名摘要以及密文内容；

[0191] 第二公钥分发模块603，用于向服务器发送公钥分发请求，所述公钥分发请求携带所述第一终端的用户的标识；

[0192] 第三获取模块604，用于获取所述服务器返回的所述第一终端的用户的签名公钥，所述第一终端的用户的签名公钥与所述第一终端的用户的标识对应；

[0193] 会话解密模块605，用于根据第二智能密码钥匙存储的目标加密私钥对所述会话密钥密文进行解密，得到会话密钥；其中，所述目标加密私钥与所述目标用户的标识对应；

[0194] 内容解密模块606，用于根据所述会话密钥对所述密文内容进行解密，得到明文内容；

[0195] 验签模块607，用于根据所述第一终端的用户的签名公钥对所述签名摘要进行验签，得到验签后的摘要；

[0196] 第二计算模块608，用于根据SM3算法对所述明文内容进行计算，得到所述明文内容的摘要；

[0197] 对比模块609，用于将所述验签后的摘要与所述明文内容的摘要进行对比，在所述验签后的摘要与所述明文内容的摘要一致的情况下，将所述明文内容写入新建文件，完成所述加密文件的解密。

[0198] 基于同一发明构思，本申请另一实施例提供一种计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时实现如本申请上述任一实施例所述的方法中的步骤。

[0199] 基于同一发明构思，本申请另一实施例提供一种电子设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行时实现本申请上述任一实施例所述的方法中的步骤。

[0200] 对于装置实施例而言，由于其与方法实施例基本相似，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[0201] 本说明书中的各个实施例均采用递进的方式描述，每个实施例重点说明的都是与其他实施例的不同之处，各个实施例之间相同相似的部分互相参见即可。

[0202] 本领域内的技术人员应明白，本申请实施例的实施例可提供为方法、装置、或计算机程序产品。因此，本申请实施例可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请实施例可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0203] 本申请实施例是参照根据本申请实施例的方法、终端设备(系统)、和计算机程序

产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理终端设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理终端设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0204] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理终端设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0205] 这些计算机程序指令也可装载到计算机或其他可编程数据处理终端设备上，使得在计算机或其他可编程终端设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程终端设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0206] 尽管已描述了本申请实施例的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例做出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本申请实施例范围的所有变更和修改。

[0207] 最后，还需要说明的是，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。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者终端设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者终端设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者终端设备中还存在另外的相同要素。

[0208] 以上对本申请所提供的一种数据加密、密钥发布以及数据解密方法方法、装置、存储介质和电子设备，进行了详细介绍，本文中应用了具体个例对本申请的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本申请的方法及其核心思想；同时，对于本领域的一般技术人员，依据本申请的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本申请的限制。

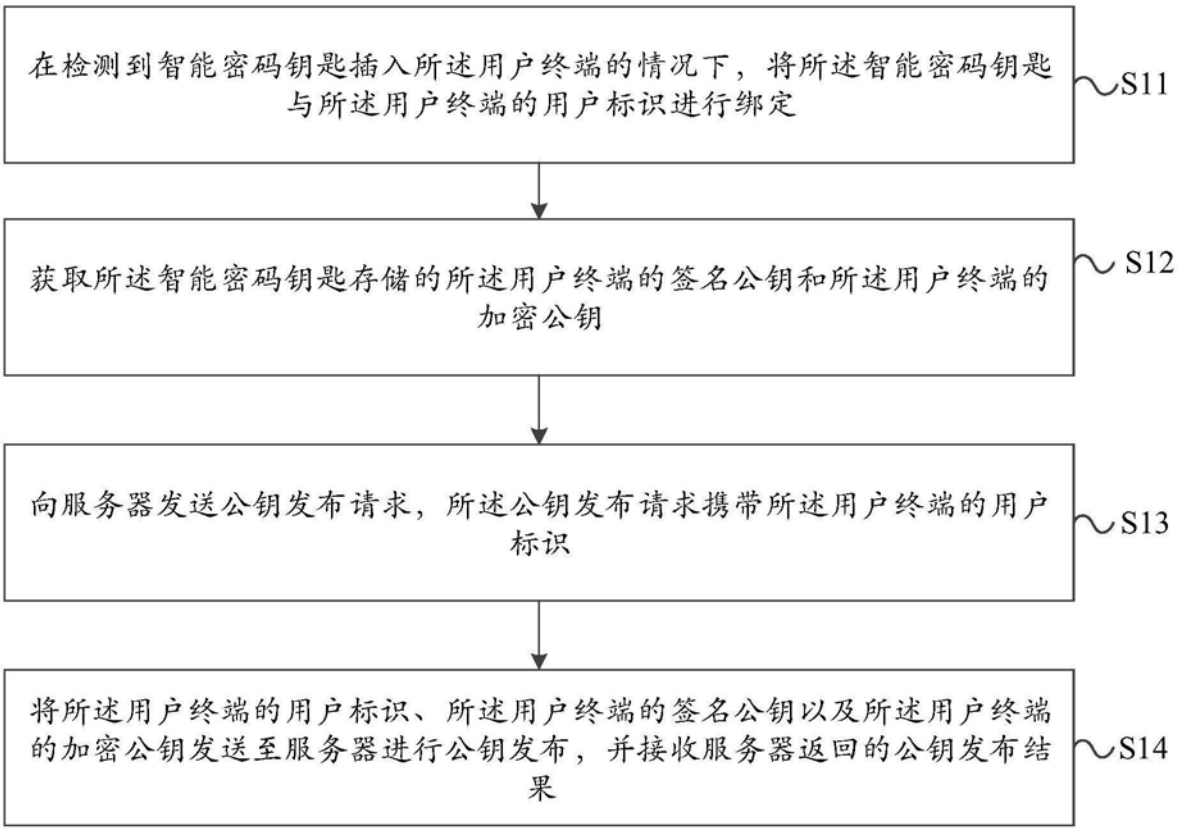

在检测到智能密码钥匙插入所述用户终端的情况下，将所述智能密码钥匙与所述用户终端的用户标识进行绑定
S11
获取所述智能密码钥匙存储的所述用户终端的签名公钥和所述用户终端的加密公钥
S12
向服务器发送公钥发布请求，所述公钥发布请求携带所述用户终端的用户标识
S13
将所述用户终端的用户标识、所述用户终端的签名公钥以及所述用户终端的加密公钥发送至服务器进行公钥发布，并接收服务器返回的公钥发布结果
S14

图1

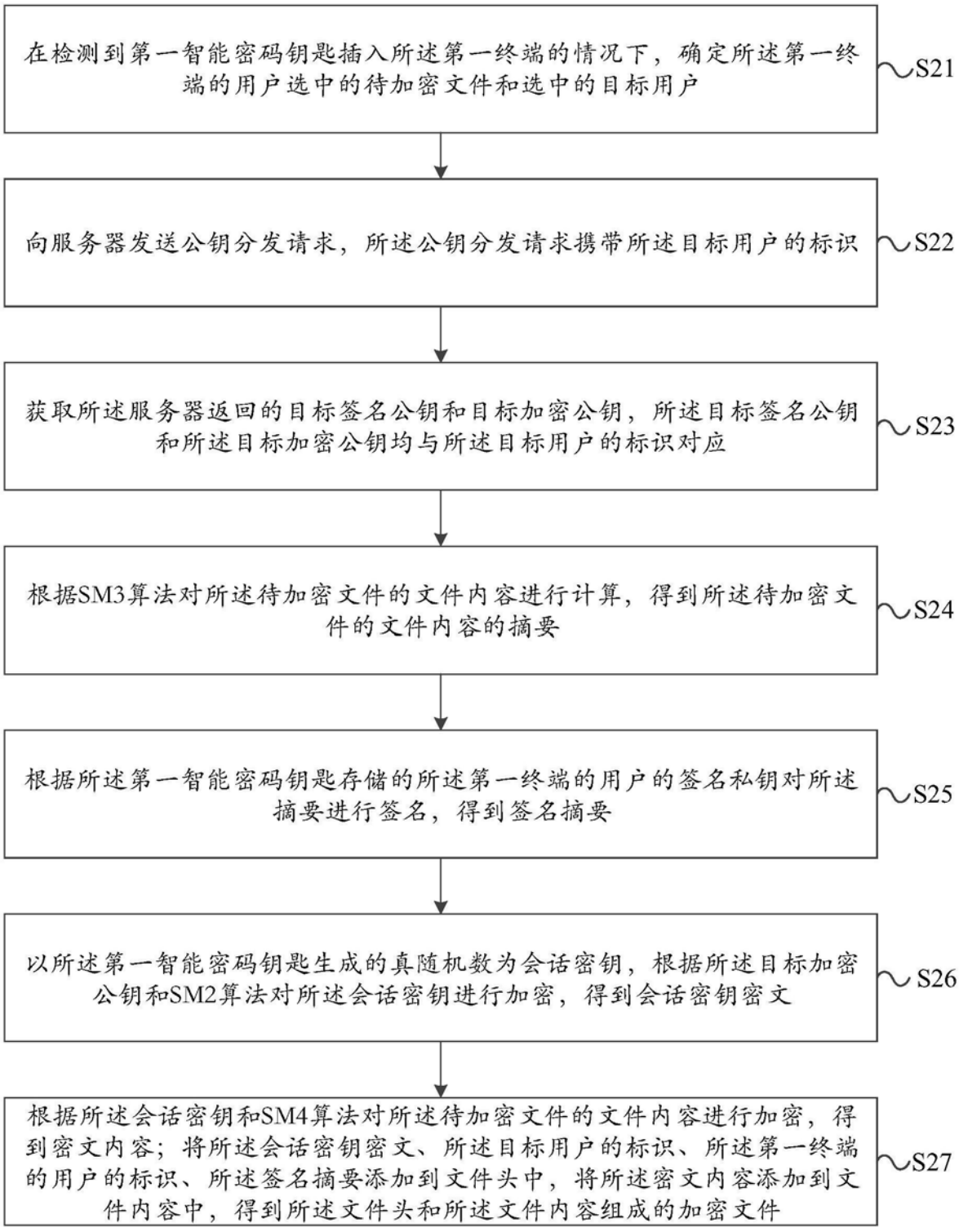

在检测到第一智能密码钥匙插入所述第一终端的情况下，确定所述第一终端的用户选中的待加密文件和选中的目标用户
S21
向服务器发送公钥分发请求，所述公钥分发请求携带所述目标用户的标识
S22
获取所述服务器返回的目标签名公钥和目标加密公钥，所述目标签名公钥和所述目标加密公钥均与所述目标用户的标识对应
S23
根据SM3算法对所述待加密文件的文件内容进行计算，得到所述待加密文件的文件内容的摘要
S24
根据所述第一智能密码钥匙存储的所述第一终端的用户的签名私钥对所述摘要进行签名，得到签名摘要
S25
以所述第一智能密码钥匙生成的真随机数为会话密钥，根据所述目标加密公钥和SM2算法对所述会话密钥进行加密，得到会话密钥密文
S26
根据所述会话密钥和SM4算法对所述待加密文件的文件内容进行加密，得到密文内容；将所述会话密钥密文、所述目标用户的标识、所述第一终端的用户的标识、所述签名摘要添加到文件头中，将所述密文内容添加到文件内容中，得到所述文件头和所述文件内容组成的加密文件
S27

图2

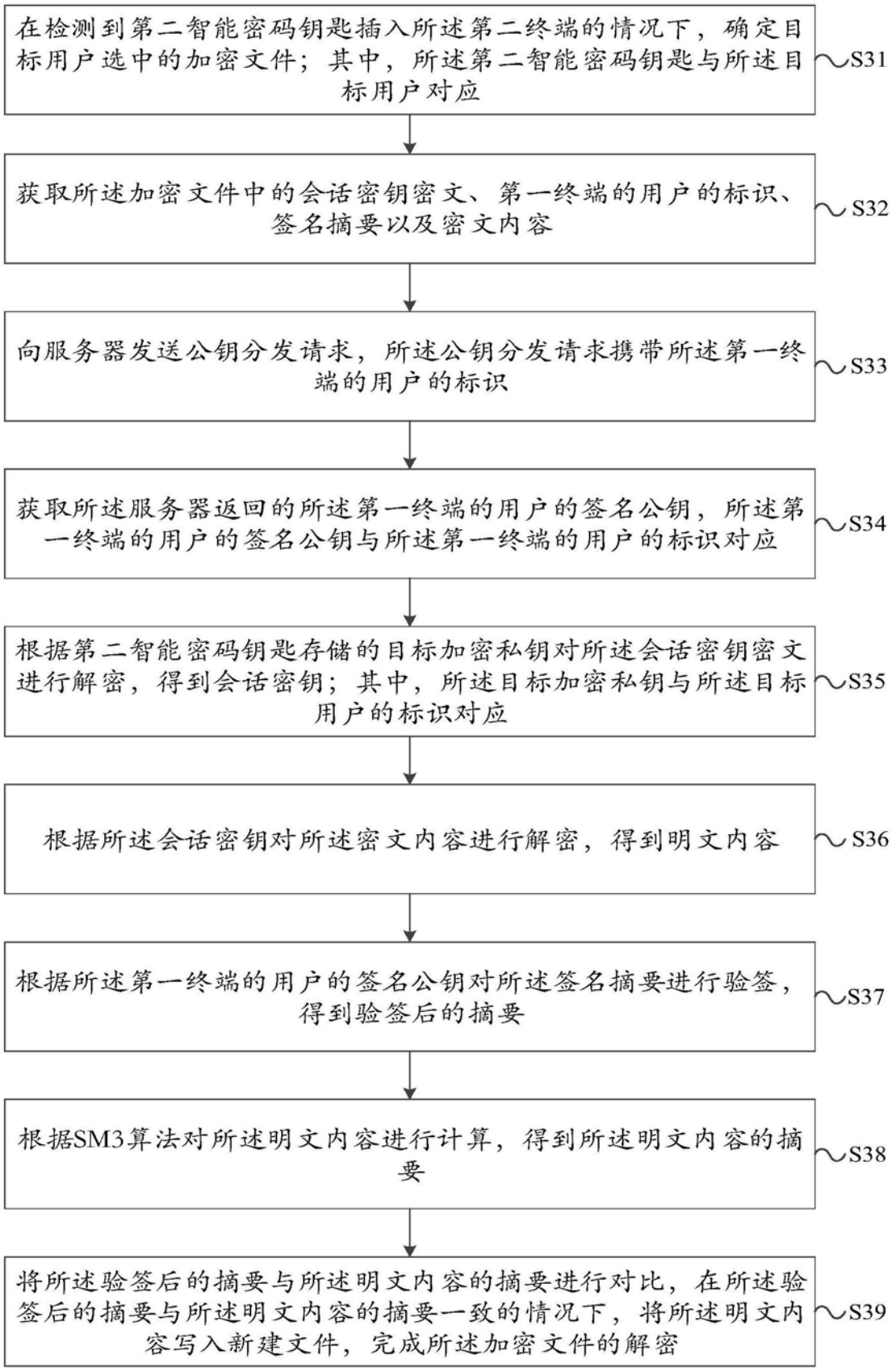

在检测到第二智能密码钥匙插入所述第二终端的情况下，确定目标用户选中的加密文件；其中，所述第二智能密码钥匙与所述目标用户对应
S31
获取所述加密文件中的会话密钥密文、第一终端的用户的标识、签名摘要以及密文内容
S32
向服务器发送公钥分发请求，所述公钥分发请求携带所述第一终端的用户的标识
S33
获取所述服务器返回的所述第一终端的用户的签名公钥，所述第一终端的用户的签名公钥与所述第一终端的用户的标识对应
S34
根据第二智能密码钥匙存储的目标加密私钥对所述会话密钥密文进行解密，得到会话密钥；其中，所述目标加密私钥与所述目标用户的标识对应
S35
根据所述会话密钥对所述密文内容进行解密，得到明文内容
S36
根据所述第一终端的用户的签名公钥对所述签名摘要进行验签，得到验签后的摘要
S37
根据SM3算法对所述明文内容进行计算，得到所述明文内容的摘要
S38
将所述验签后的摘要与所述明文内容的摘要进行对比，在所述验签后的摘要与所述明文内容的摘要一致的情况下，将所述明文内容写入新建文件，完成所述加密文件的解密
S39

图3

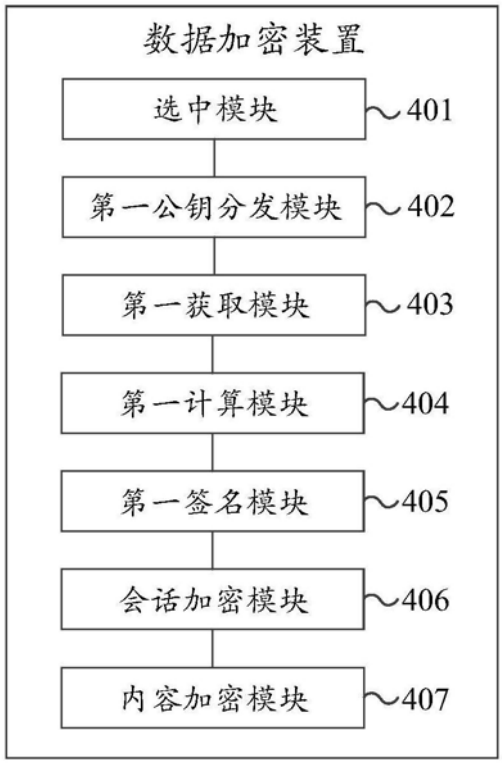

数据加密装置
选中模块
401
第一公钥分发模块
402
第一获取模块
403
第一计算模块
404
第一签名模块
405
会话加密模块
406
内容加密模块
407

图4

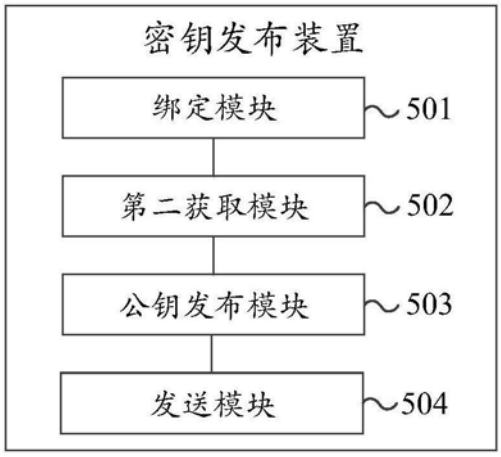

密钥发布装置
绑定模块
501
第二获取模块
502
公钥发布模块
503
发送模块
504

图5

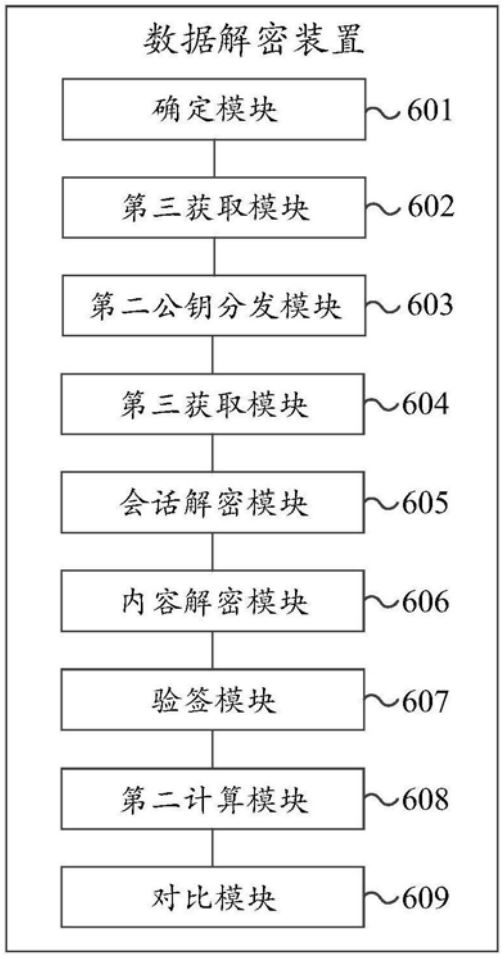

数据解密装置
确定模块
601
第三获取模块
602
第二公钥分发模块
603
第三获取模块
604
会话解密模块
605
内容解密模块
606
验签模块
607
第二计算模块
608
对比模块
609

图6