(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 106549927 B
(45)授权公告日 2020.11.13

(21)申请号 201510613959.7

(22)申请日 2015.09.23

(65)同一申请的已公布的文献号
申请公布号 CN 106549927 A

(43)申请公布日 2017.03.29

(73)专利权人 阿里巴巴集团控股有限公司
地址 英属开曼群岛大开曼资本大厦一座四层847号邮箱

(72)发明人 陈虓将 刘彦梅

(74)专利代理机构 北京三友知识产权代理有限公司 11127
代理人 李辉

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

(56)对比文件
CN 1505029 A,2004.06.16
CN 1697371 A,2005.11.16
CN 104283680 A,2015.01.14
CN 103248476 A,2013.08.14
CN 101174942 A,2008.05.07

审查员 申杨

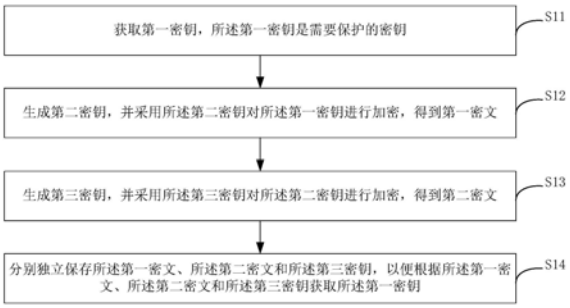
权利要求书2页 说明书7页 附图3页

(54)发明名称

密钥保存、获取方法和装置

(57)摘要

本发明提出一种密钥保存、获取方法和装置，该密钥保存方法包括：获取第一密钥，所述第一密钥是需要保护的密钥；生成第二密钥，并采用所述第二密钥对所述第一密钥进行加密，得到第一密文；生成第三密钥，并采用所述第三密钥对所述第二密钥进行加密，得到第二密文；分别独立保存所述第一密文、所述第二密文和所述第三密钥，以便根据所述第一密文、所述第二密文和所述第三密钥获取所述第一密钥。该方法能够提高密钥保存的安全性，保证信息安全。



CN 106549927 B

1.一种密钥保存方法,其特征在于,包括:

获取第一密钥,所述第一密钥是需要保护的密钥;

生成第二密钥,并采用所述第二密钥对所述第一密钥进行加密,得到第一密文;

生成第三密钥,并采用所述第三密钥对所述第二密钥进行加密,得到第二密文;

分别独立保存所述第一密文、所述第二密文和所述第三密钥,以便根据所述第一密文、所述第二密文和所述第三密钥获取所述第一密钥;

其中,所述采用所述第二密钥对所述第一密钥进行加密,得到第一密文,包括:

调用库文件中预设的第一加密算法,采用所述第二密钥并根据所述第一加密算法,对所述第一密钥进行加密,得到第一密文;和/或,

所述采用所述第三密钥对所述第二密钥进行加密,得到第二密文,包括:

调用库文件中预设的第二加密算法,采用所述第三密钥并根据所述第二加密算法,对所述第二密钥进行加密,得到第二密文;

其中,所述库文件由第三方生成并进行加固处理,所述第二密钥、所述第三密钥、所述第一加密算法和所述第二加密算法定时或临时更新。

2.根据权利要求1所述的方法,其特征在于,所述分别独立保存所述第一密文、所述第二密文和所述第三密钥,包括:

将所述第一密文作为独立文件保存;

将所述第二密文保存在配置文件中;

将所述第三密钥保存在源代码中。

3.根据权利要求2所述的方法,其特征在于,还包括:

对所述第二密文进行形式转换,以便将形式转换后的第二密文保存在配置文件中;和/或,

对所述第三密钥进行形式转换,以便将形式转换后的第三密钥保存在源代码中。

4.根据权利要求1-3任一项所述的方法,其特征在于,

所述生成第二密钥包括:

随机生成第二密钥;和/或,

所述生成第三密钥包括:

随机生成第三密钥。

5.一种密钥获取方法,其特征在于,包括:

获取独立保存的第一密文、第二密文和第三密钥;

采用所述第三密钥对所述第二密文进行解密,获取第二密钥;

采用所述第二密钥对所述第一密文进行解密,获取第一密钥,所述第一密钥是需要保护的密钥;

其中,所述采用所述第三密钥对所述第二密文进行解密,获取第二密钥,包括:

调用库文件中预设的第二解密算法,采用所述第三密钥并根据所述第二解密算法,对所述第二密文进行解密,得到第二密钥;和/或,

所述采用所述第二密钥对所述第一密文进行解密,获取第一密钥,包括:

调用库文件中预设的第一解密算法,采用所述第二密钥并根据所述第一解密算法,对所述第一密文进行解密,得到第一密钥;

其中，所述库文件由第三方生成并进行加固处理，所述第二密钥、所述第三密钥、所述第一解密算法和所述第二解密算法定时或临时更新。

6.根据权利要求5所述的方法，其特征在于，所述获取独立保存的第一密文、第二密文和第三密钥，包括：

从独立文件中获取第一密文；

从配置文件中获取第二密文；

从源代码中获取第三密钥。

7.根据权利要求6所述的方法，其特征在于，

所述从配置文件中获取第二密文，包括：

从配置文件中获取形式转换后的第二密文，对所述形式转换后的第二密文进行解码，获取第二密文；和/或，

所述从源代码中获取第三密钥，包括：

从源代码中获取形式转换后的第三密钥，对所述形式转换后的第三密钥进行解码，获取第三密钥。

8.一种密钥保存装置，其特征在于，包括：

获取模块，用于获取第一密钥，所述第一密钥是需要保护的密钥；

第一加密模块，用于生成第二密钥，并采用所述第二密钥对所述第一密钥进行加密，得到第一密文；

第二加密模块，用于生成第三密钥，并采用所述第三密钥对所述第二密钥进行加密，得到第二密文；

保存模块，用于分别独立保存所述第一密文、所述第二密文和所述第三密钥，以便根据所述第一密文、所述第二密文和所述第三密钥获取所述第一密钥；

其中，所述第一加密模块具体用于：调用库文件中预设的第一加密算法，采用所述第二密钥并根据所述第一加密算法，对所述第一密钥进行加密，得到第一密文；和/或，

所述第二加密模块具体用于：调用库文件中预设的第二加密算法，采用所述第三密钥并根据所述第二加密算法，对所述第二密钥进行加密，得到第二密文；

其中，所述库文件由第三方生成并进行加固处理，所述第二密钥、所述第三密钥、所述第一加密算法和所述第二加密算法定时或临时更新。

9.一种密钥获取装置，其特征在于，包括：

获取模块，用于获取独立保存的第一密文、第二密文和第三密钥；

第一解密模块，用于采用所述第三密钥对所述第二密文进行解密，获取第二密钥；

第二解密模块，用于采用所述第二密钥对所述第一密文进行解密，获取第一密钥，所述第一密钥是需要保护的密钥；

其中，所述第一解密模块具体用于：调用库文件中预设的第二解密算法，采用所述第三密钥并根据所述第二解密算法，对所述第二密文进行解密，得到第二密钥；和/或，

所述第二解密模块具体用于：调用库文件中预设的第一解密算法，采用所述第二密钥并根据所述第一解密算法，对所述第一密文进行解密，得到第一密钥；

其中，所述库文件由第三方生成并进行加固处理，所述第二密钥、所述第三密钥、所述第一解密算法和所述第二解密算法定时或临时更新。

密钥保存、获取方法和装置

技术领域

[0001] 本发明涉及信息安全技术领域，尤其涉及一种密钥保存、获取方法和装置。

背景技术

[0002] 随着计算机技术的发展和互联网的普及，人们对信息安全越来越重视。为了保证信息安全，出现了传输层安全协议(Transport Layer Security，TLS)等加密协议。TLS协议基于非对称加密算法通过数字证书认证机构(Certificate Authority，CA)授权的证书来分发公钥，和公钥对应的私钥在服务端妥善保管。

[0003] 目前服务端在保存私钥时，都是以明文的形式存放在服务端本地文件中。但是，明文形式很容易造成私钥泄露，影响信息安全。

发明内容

[0004] 本发明旨在至少在一定程度上解决相关技术中的技术问题之一。

[0005] 为此，本发明的一个目的在于提出一种密钥保存方法，该方法可以提高密钥保存的安全性，保证信息安全。

[0006] 本发明的另一个目的在于提出一种密钥获取方法。

[0007] 本发明的另一个目的在于提出一种密钥保存装置

[0008] 本发明的另一个目的在于提出一种密钥获取装置。

[0009] 为达到上述目的，本发明第一方面实施例提出的密钥保存方法，包括：获取第一密钥，所述第一密钥是需要保护的密钥；生成第二密钥，并采用所述第二密钥对所述第一密钥进行加密，得到第一密文；生成第三密钥，并采用所述第三密钥对所述第二密钥进行加密，得到第二密文；分别独立保存所述第一密文、所述第二密文和所述第三密钥，以便根据所述第一密文、所述第二密文和所述第三密钥获取所述第一密钥。

[0010] 本发明第一方面实施例提出的密钥保存方法，通过对需要保护的密钥进行加密后保存，相对于明文保存方式，可以提高安全性，并且，对加密处理的第二密钥也进行加密，以及，对各种信息独立保存，可以进一步提高安全性。

[0011] 为达到上述目的，本发明第二方面实施例提出的密钥获取方法，包括：获取独立保存的第一密文、第二密文和第三密钥；采用所述第三密钥对所述第二密文进行解密，获取第二密钥；采用所述第二密钥对所述第一密文进行解密，获取第一密钥，所述第一密钥是需要保护的密钥。

[0012] 本发明第二方面实施例提出的密钥获取方法，通过两次解密才获取需要保护的密钥，可以提高密钥安全性，另外，通过将解密所需信息独立保存，实现权限分离，进一步提高安全性。

[0013] 为达到上述目的，本发明第三方面实施例提出的密钥保存装置，包括：获取模块，用于获取第一密钥，所述第一密钥是需要保护的密钥；第一加密模块，用于生成第二密钥，并采用所述第二密钥对所述第一密钥进行加密，得到第一密文；第二加密模块，用于生成第

三密钥，并采用所述第三密钥对所述第二密钥进行加密，得到第二密文；保存模块，用于分别独立保存所述第一密文、所述第二密文和所述第三密钥，以便根据所述第一密文、所述第二密文和所述第三密钥获取所述第一密钥。

[0014] 本发明第三方面实施例提出的密钥保存装置，通过对需要保护的密钥进行加密后保存，相对于明文保存方式，可以提高安全性，并且，对加密处理的第二密钥也进行加密，以及，对各种信息独立保存，可以进一步提高安全性。

[0015] 为达到上述目的，本发明第四方面实施例提出的密钥获取装置，包括：获取模块，用于获取独立保存的第一密文、第二密文和第三密钥；第一解密模块，用于采用所述第三密钥对所述第二密文进行解密，获取第二密钥；第二解密模块，用于采用所述第二密钥对所述第一密文进行解密，获取第一密钥，所述第一密钥是需要保护的密钥。

[0016] 本发明第四方面实施例提出的密钥获取装置，通过两次解密才获取需要保护的密钥，可以提高密钥安全性，另外，通过将解密所需信息独立保存，实现权限分离，进一步提高安全性。

[0017] 本发明附加的方面和优点将在下面的描述中部分给出，部分将从下面的描述中变得明显，或通过本发明的实践了解到。

附图说明

[0018] 本发明上述的和/或附加的方面和优点从下面结合附图对实施例的描述中将变得明显和容易理解，其中：

[0019] 图1是本发明一实施例提出的密钥保存方法的流程示意图；

[0020] 图2是本发明另一实施例提出的密钥保存方法的流程示意图；

[0021] 图3是本发明另一实施例提出的密钥获取方法的流程示意图；

[0022] 图4是本发明另一实施例提出的密钥获取方法的流程示意图；

[0023] 图5是本发明另一实施例提出的密钥保存装置的结构示意图；

[0024] 图6是本发明另一实施例提出的密钥获取装置的结构示意图。

具体实施方式

[0025] 下面详细描述本发明的实施例，所述实施例的示例在附图中示出，其中自始至终相同或类似的标号表示相同或类似的模块或具有相同或类似功能的模块。下面通过参考附图描述的实施例是示例性的，仅用于解释本发明，而不能理解为对本发明的限制。相反，本发明的实施例包括落入所附加权利要求书的精神和内涵范围内的所有变化、修改和等同物。

[0026] 图1是本发明一实施例提出的密钥保存方法的流程示意图，该方法包括：

[0027] S11：获取第一密钥，所述第一密钥是需要保护的密钥。

[0028] 当确定需要保护的密钥后，可以获取明文的密钥作为第一密钥。

[0029] S12：生成第二密钥，并采用所述第二密钥对所述第一密钥进行加密，得到第一密文。

[0030] 一些实施例中，第二密钥可以是随机生成的，通过随机生成，实现加入干扰因子，提高安全性。

[0031] 在采用密钥进行加密时，可以获取预设的加密算法，通过预设的加密算法对信息进行加密。

[0032] 在采用第二密钥对第一密钥进行加密时，则可以获取预设的第一加密算法，从而根据所述第一加密算法实现加密。

[0033] 一些实施例中，第一加密算法可以保存在库文件中，库文件是第三方生成的，另外，库文件还被第三方做了防调试等加固处理。由于是第三方生成并做了防调试等加固处理，开发和运维工程师并不知道算法实现，因此可以进一步提高安全性。

[0034] S13：生成第三密钥，并采用所述第三密钥对所述第二密钥进行加密，得到第二密文。

[0035] 一些实施例中，第三密钥也是随机生成的，从而提高安全性。

[0036] 另外，加密时，可以是调用预设的第二加密算法，采用第三密钥以及预设的第二加密算法对第二密钥进行加密，得到第二密文。

[0037] S14：分别独立保存所述第一密文、所述第二密文和所述第三密钥，以便根据所述第一密文、所述第二密文和所述第三密钥获取所述第一密钥。

[0038] 一些实施例中，将所述第一密文作为独立文件保存；将所述第二密文保存在配置文件中；将所述第三密钥保存在源代码中。

[0039] 一些实施例中，在保存第二密文和第三密钥之前，可以对第二密钥和第三密钥进行形式转换，以更好地在配置文件和源代码中保存。例如，可以对第二密钥和第三密钥进行base64转换。Base64转换是一种基于64个可打印字符来标识二进制数据的表示方法。

[0040] 本实施例中，通过对需要保护的密钥进行加密后保存，相对于明文保存方式，可以提高安全性，并且，对加密处理的第二密钥也进行加密，以及，对各种信息独立保存，可以进一步提高安全性。

[0041] 图2是本发明另一实施例提出的密钥保存方法的流程示意图，本实施例中，第一密钥用Ka表示，第二密钥用Kb表示，第三密钥用Kc表示，第一密文用Ta表示，第二密文用Tb表示。

[0042] 参见图2，该方法包括：

[0043] S201：获取需要保存的密钥Ka。

[0044] 例如，获取明文的Ka。

[0045] S202：随机生成密钥Kb。

[0046] 通过采用随机方式可以提高安全性。

[0047] S203：用Kb加密Ka得到密文Ta。

[0048] 例如，加密算法是aes-256-cbc，则采用Kb对Ka进行aes-256-cbc加密，得到Ta。

[0049] S204：将Ta保存在独立文件中。

[0050] 其中，Tb可以具体是二进制数，将二进制数作为独立文件保存。

[0051] S205：随机生成密钥Kc。

[0052] S206：用Kc加密Kb得到密文Tb。

[0053] 例如，加密算法是aes-256-cbc，则采用Kc对Kb进行aes-256-cbc加密，得到Tb。

[0054] 另外，采用Kb加密Ka，以及Kc加密Kb采用的加密算法可以是保存在库文件中的，库文件可以由第三方生成。

[0055] S207:对Tb进行Base64转换。

[0056] 其中,形式转换后的Tb用Base64(Tb)表示。

[0057] 加密后的Tb是二进制数,经过Base64转换可以转换为可见字符集。

[0058] S208:将Base64(Tb)保存在配置文件中。

[0059] S209:对Kc进行Base64转换。

[0060] 其中,形式转换后的Kc用Base64(Kc)表示。

[0061] S210:将Base64(Kc)保存在源代码中。

[0062] 以上为一份密钥Ka的保存过程,如果想要得到密钥Ka,密文Ta/密文Tb/密钥Kc是缺一不可的,而这三部分被放在独立文件/配置文件/源代码分别进行保存,每部分都需要独立的权限来获取,可以采用分离权限的方式达到保证Ka保密性的目的。

[0063] 如果需要保存多份密钥,可以按照以上流程生成多组对应的Base64(Kc)和Base64(Tb)和Ta。其中,在保存时可以对应同一组的Base64(Kc)、Base64(Tb)和Ta设置相同的标识信息,以便根据同一个标识信息关联同一组的Base64(Kc)、Base64(Tb)和Ta。

[0064] 另外,以上流程可以在服务端执行。上述随机生成的Kb和Kc,以及两次加密时的每种加密算法中的一项或多项可以定期或紧急更新,以降低系统被破解的风险。

[0065] 本实施例中,通过对需要保护的密钥进行加密,可以保密明文的密钥。通过对加密处理采用的密钥也进行加密,可以保证加密密钥的安全。通过将相关参数分别保存,可以实现权限分离,提高安全性。通过随机生成加密密钥,可以实现引入干扰因子的目的,也可以提高安全性。通过采用由第三方产生的加密算法,可以避免加密算法泄露,也可以提高安全性。通过定期或临时更新密钥和算法,降低系统被破解的危险,也可以提高安全性。

[0066] 图3是本发明另一实施例提出的密钥获取方法的流程示意图,该方法包括:

[0067] S31:获取独立保存的第一密文、第二密文和第三密钥。

[0068] 例如,从独立文件中获取第一密文;从配置文件中获取第二密文;从源代码中获取第三密钥。

[0069] 可选的,所述从配置文件中获取第二密文,包括:

[0070] 从配置文件中获取形式转换后的第二密文,对所述形式转换后的第二密文进行解码,获取第二密文;和/或,

[0071] 所述从源代码中获取第三密钥,包括:

[0072] 从源代码中获取形式转换后的第三密钥,对所述形式转换后的第三密钥进行解码,获取第三密钥。

[0073] S32:采用所述第三密钥对所述第二密文进行解密,获取第二密钥。

[0074] 其中,对第二密文进行解密时的算法选择与第二密文的加密算法一致。

[0075] S33:采用所述第二密钥对所述第一密文进行解密,获取第一密钥,所述第一密钥是需要保护的密钥。

[0076] 其中,对第一密文进行解密时的算法选择与第一密文的加密算法一致。

[0077] 本实施例中,通过两次解密才获取需要保护的密钥,可以提高密钥安全性,另外,通过将解密所需信息独立保存,实现权限分离,进一步提高安全性。

[0078] 图4是本发明另一实施例提出的密钥获取方法的流程示意图,该方法包括:

[0079] S41:从配置文件中读取Base64(Kc)。

[0080] 其中，Base64(Kc)表示对Kc进行Base64转换后的字符。

[0081] S42：进行Base64解码，得到Kc。

[0082] 通过解码处理，得到原始的Kc。

[0083] S43：从源代码中读取Base64(Tb)。

[0084] S44：进行Base64解码，得到Tb。

[0085] 类似对Kc的处理，通过解码，也可以得到Tb。

[0086] S45：用Kc解密Tb，得到密钥Kb。

[0087] 其中，解密时的算法与相应的加密算法一致，从而可以在解密后得到Kb。例如，采用Kc对Tb进行aes-256-cbc解密，得到密钥Kb。

[0088] S46：从独立文件中读取Ta。

[0089] S47：用Kb解密Ta，得到密钥Ka。

[0090] 其中，用Kb解密Ta的算法与生成Ta的加密算法一致，从而可以在解密后得到Ka。例如，采用Kb对Ta进行aes-256-cbc解密，得到密钥Ka。

[0091] 以上为一份密钥Ka的恢复流程，如果保存了多份密钥，则通过每组分别恢复的方式得到每组最初保存的密钥。其中，在保存多组密钥时，可以通过相同的标识信息关联同一组的Base64(Kc)、Base64(Tb)和Ta。

[0092] 本实施例中，通过从相互独立的内容中获取相关信息，可以实现权限分离，提高安全性。通过解密处理获取需要保护的密钥，可以提高密钥保护的安全性。通过对解密密钥也需要解密获取，可以进一步提高安全性。

[0093] 图5是本发明另一实施例提出的密钥保存装置的结构示意图，该装置50包括：获取模块51、第一加密模块52、第二加密模块53和保存模块54。

[0094] 获取模块51，用于获取第一密钥，所述第一密钥是需要保护的密钥；

[0095] 当确定需要保护的密钥后，可以获取明文的密钥作为第一密钥。

[0096] 第一加密模块52，用于生成第二密钥，并采用所述第二密钥对所述第一密钥进行加密，得到第一密文；

[0097] 一些实施例中，第二密钥可以是随机生成的，通过随机生成，实现加入干扰因子，提高安全性。

[0098] 在采用密钥进行加密时，可以获取预设的加密算法，通过预设的加密算法对信息进行加密。

[0099] 在采用第二密钥对第一密钥进行加密时，则可以获取预设的第一加密算法，从而根据所述第一加密算法实现加密。

[0100] 一些实施例中，第一加密算法可以保存在库文件中，库文件是第三方生成的，另外，库文件还被第三方做了防调试等加固处理。由于是第三方生成并做了防调试等加固处理，开发和运维工程师并不知道算法实现，因此可以进一步提高安全性。

[0101] 第二加密模块53，用于生成第三密钥，并采用所述第三密钥对所述第二密钥进行加密，得到第二密文；

[0102] 一些实施例中，第三密钥也是随机生成的，从而提高安全性。

[0103] 另外，加密时，可以是调用预设的第二加密算法，采用第三密钥以及预设的第二加密算法对第二密钥进行加密，得到第二密文。

[0104] 一些实施例中，所述采用所述第二密钥对所述第一密钥进行加密，得到第一密文，包括：

[0105] 调用库文件中预设的第一加密算法，采用所述第二密钥并根据所述第一加密算法，对所述第一密钥进行加密，得到第一密文；和/或，

[0106] 所述采用所述第三密钥对所述第二密钥进行加密，得到第二密文，包括：

[0107] 调用库文件中预设的第二加密算法，采用所述第三密钥并根据所述第二加密算法，对所述第二密钥进行加密，得到第二密文；

[0108] 其中，所述库文件是第三方生成的。

[0109] 一些实施例中，所述生成第二密钥包括：随机生成第二密钥；和/或，

[0110] 所述生成第三密钥包括：随机生成第三密钥。

[0111] 保存模块54，用于分别独立保存所述第一密文、所述第二密文和所述第三密钥，以便根据所述第一密文、所述第二密文和所述第三密钥获取所述第一密钥。

[0112] 一些实施例中，所述分别独立保存所述第一密文、所述第二密文和所述第三密钥，包括：

[0113] 将所述第一密文作为独立文件保存；

[0114] 将所述第二密文保存在配置文件中；

[0115] 将所述第三密钥保存在源代码中。

[0116] 一些实施例中，在保存第二密文和第三密钥之前，可以对第二密钥和第三密钥进行形式转换，以更好地在配置文件和源代码中保存。例如，可以对第二密钥和第三密钥进行base64转换。Base64转换是一种基于64个可打印字符来标识二进制数据的表示方法。

[0117] 因此，保存模块还用于：对所述第二密文进行形式转换，以便将形式转换后的第二密文保存在配置文件中；和/或，对所述第三密钥进行形式转换，以便将形式转换后的第三密钥保存在源代码中。

[0118] 本实施例中，通过对需要保护的密钥进行加密后保存，相对于明文保存方式，可以提高安全性，并且，对加密处理的第二密钥也进行加密，以及，对各种信息独立保存，可以进一步提高安全性。

[0119] 图6是本发明另一实施例提出的密钥获取装置的结构示意图，该装置60包括：获取模块61、第一解密模块62、第二解密模块63。

[0120] 获取模块61，用于获取独立保存的第一密文、第二密文和第三密钥；

[0121] 可选的，所述获取模块61具体用于：

[0122] 从独立文件中获取第一密文；

[0123] 从配置文件中获取第二密文；

[0124] 从源代码中获取第三密钥。

[0125] 可选的，所述从配置文件中获取第二密文，包括：

[0126] 从配置文件中获取形式转换后的第二密文，对所述形式转换后的第二密文进行解码，获取第二密文；和/或，

[0127] 所述从源代码中获取第三密钥，包括：

[0128] 从源代码中获取形式转换后的第三密钥，对所述形式转换后的第三密钥进行解码，获取第三密钥。

[0129] 第一解密模块62，用于采用所述第三密钥对所述第二密文进行解密，获取第二密钥；

[0130] 其中，对第二密文进行解密时的算法选择与第二密文的加密算法一致。

[0131] 第二解密模块63，用于采用所述第二密钥对所述第一密文进行解密，获取第一密钥，所述第一密钥是需要保护的密钥。

[0132] 其中，对第一密文进行解密时的算法选择与第一密文的加密算法一致。

[0133] 本实施例中，通过两次解密才获取需要保护的密钥，可以提高密钥安全性，另外，通过将解密所需信息独立保存，实现权限分离，进一步提高安全性。

[0134] 需要说明的是，在本发明的描述中，术语“第一”、“第二”等仅用于描述目的，而不能理解为指示或暗示相对重要性。此外，在本发明的描述中，除非另有说明，“多个”的含义是指至少两个。

[0135] 流程图中或在此以其他方式描述的任何过程或方法描述可以被理解为，表示包括一个或更多个用于实现特定逻辑功能或过程的步骤的可执行指令的代码的模块、片段或部分，并且本发明的优选实施方式的范围包括另外的实现，其中可以不按所示出或讨论的顺序，包括根据所涉及的功能按基本同时的方式或按相反的顺序，来执行功能，这应被本发明的实施例所属技术领域的技术人员所理解。

[0136] 应当理解，本发明的各部分可以用硬件、软件、固件或它们的组合来实现。在上述实施方式中，多个步骤或方法可以用存储在存储器中且由合适的指令执行系统执行的软件或固件来实现。例如，如果用硬件来实现，和在另一实施方式中一样，可用本领域公知的下列技术中的任一项或他们的组合来实现：具有用于对数据信号实现逻辑功能的逻辑门电路的离散逻辑电路，具有合适的组合逻辑门电路的专用集成电路，可编程门阵列(PGA)，现场可编程门阵列(FPGA)等。

[0137] 本技术领域的普通技术人员可以理解实现上述实施例方法携带的全部或部分步骤是可以通过程序来指令相关的硬件完成，所述的程序可以存储于一种计算机可读存储介质中，该程序在执行时，包括方法实施例的步骤之一或其组合。

[0138] 此外，在本发明各个实施例中的各功能单元可以集成在一个处理模块中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个模块中。上述集成的模块既可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。所述集成的模块如果以软件功能模块的形式实现并作为独立的产品销售或使用时，也可以存储在一个计算机可读取存储介质中。

[0139] 上述提到的存储介质可以是只读存储器，磁盘或光盘等。

[0140] 在本说明书的描述中，参考术语“一个实施例”、“一些实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本发明的至少一个实施例或示例中。在本说明书中，对上述术语的示意性表述不一定指的是相同的实施例或示例。而且，描述的具体特征、结构、材料或者特点可以在任何的一个或多个实施例或示例中以合适的方式结合。

[0141] 尽管上面已经示出和描述了本发明的实施例，可以理解的是，上述实施例是示例性的，不能理解为对本发明的限制，本领域的普通技术人员在本发明的范围内可以对上述实施例进行变化、修改、替换和变型。

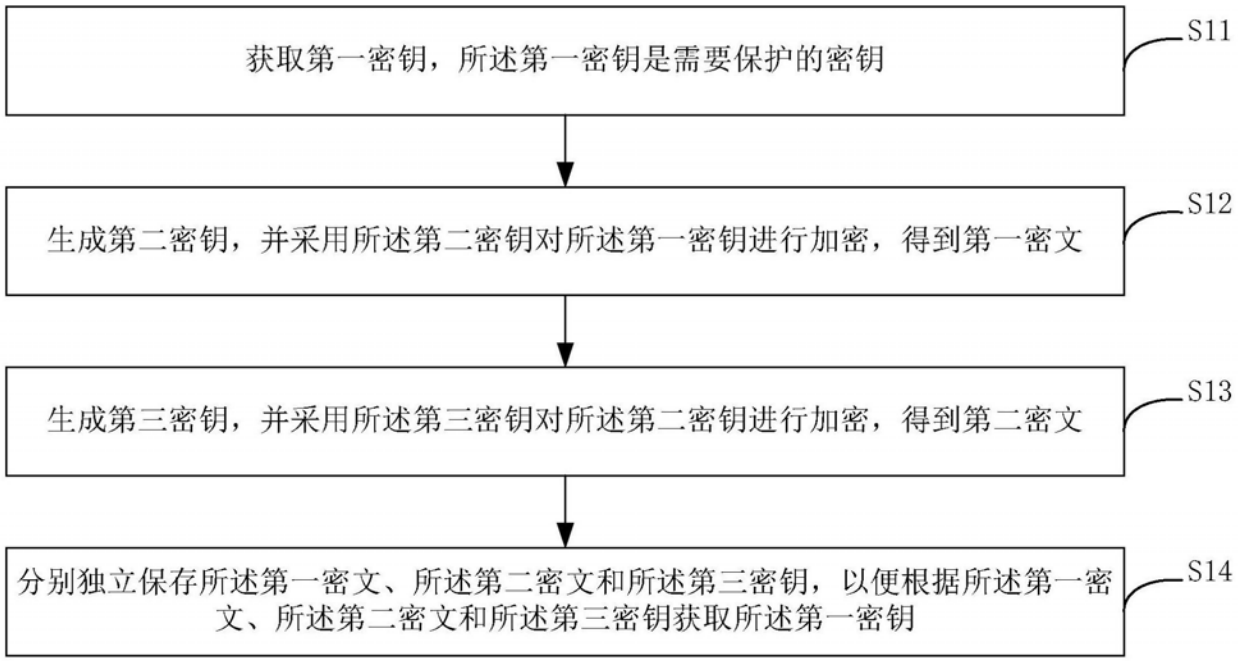

获取第一密钥，所述第一密钥是需要保护的密钥
S11
生成第二密钥，并采用所述第二密钥对所述第一密钥进行加密，得到第一密文
S12
生成第三密钥，并采用所述第三密钥对所述第二密钥进行加密，得到第二密文
S13
分别独立保存所述第一密文、所述第二密文和所述第三密钥，以便根据所述第一密文、所述第二密文和所述第三密钥获取所述第一密钥
S14

图1

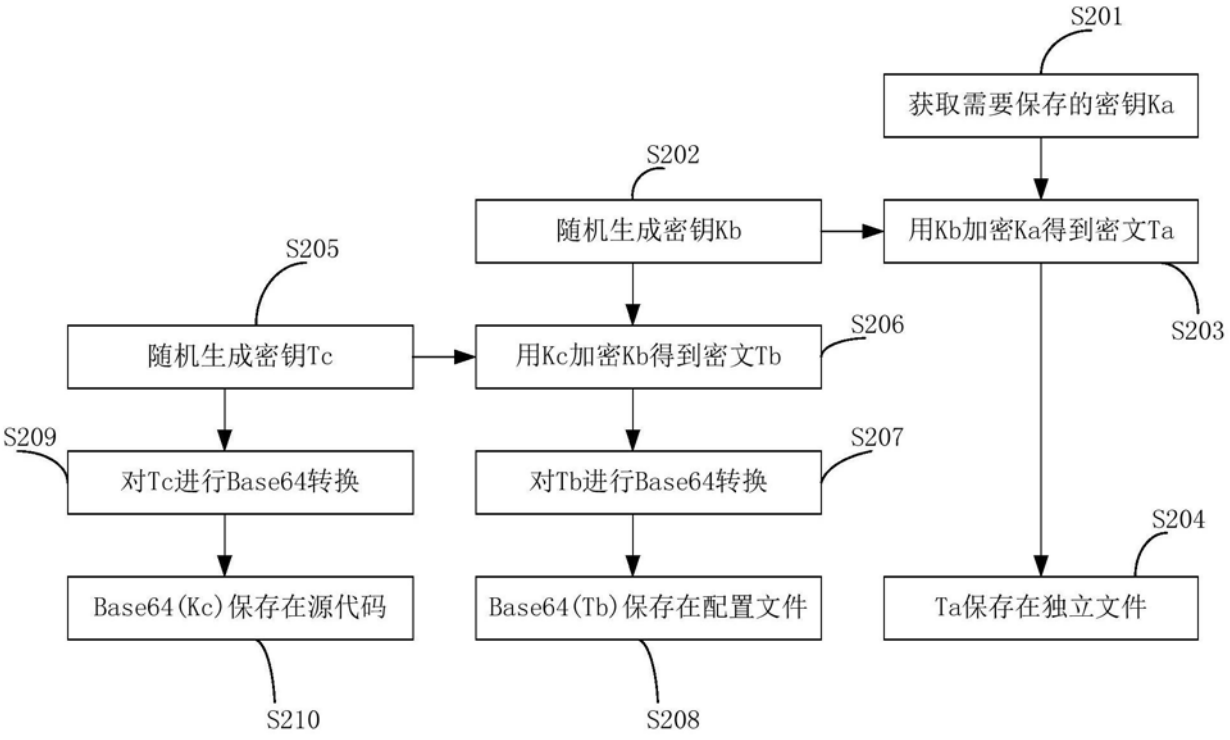

S201
获取需要保存的密钥Ka
S202
随机生成密钥Kb
用Kb加密Ka得到密文Ta
S203
S205
随机生成密钥Tc
用Kc加密Kb得到密文Tb
S206
S209
对Tc进行Base64转换
S207
对Tb进行Base64转换
S204
Base64(Kc)保存在源代码
Base64(Tb)保存在配置文件
Ta保存在独立文件
S210
S208

图2

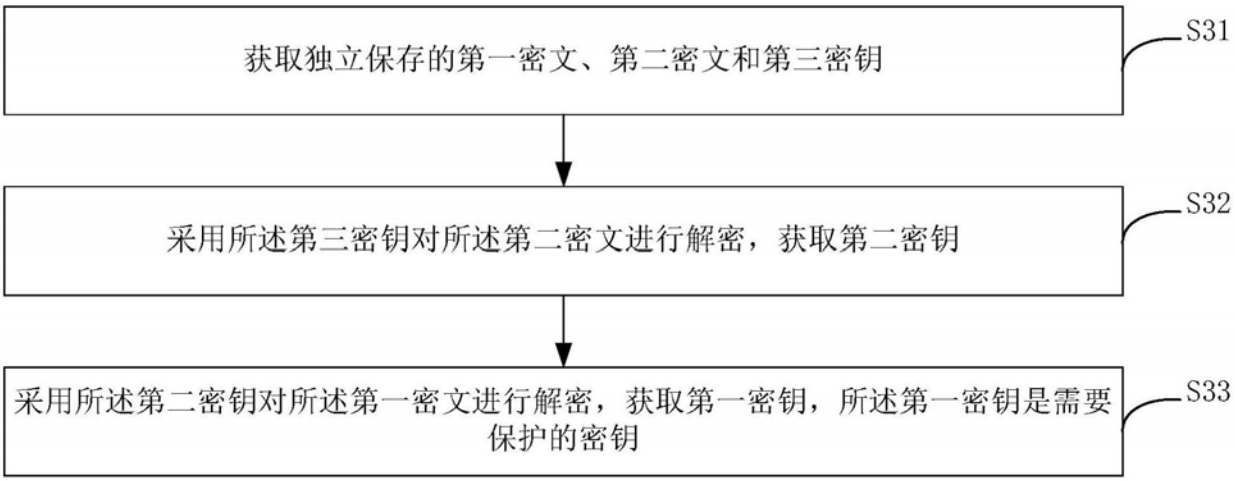

获取独立保存的第一密文、第二密文和第三密钥
S31
采用所述第三密钥对所述第二密文进行解密，获取第二密钥
S32
采用所述第二密钥对所述第一密文进行解密，获取第一密钥，所述第一密钥是需要保护的密钥
S33

图3

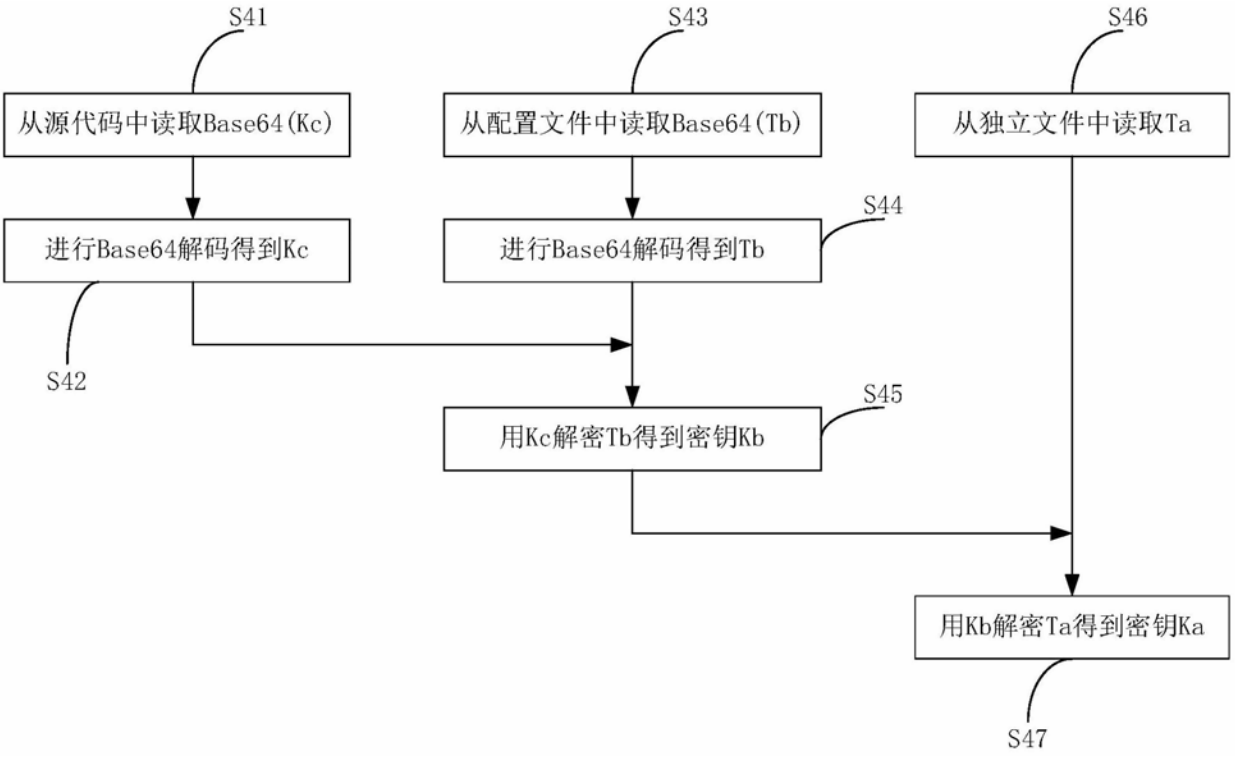

S41
从源代码中读取Base64(Kc)
进行Base64解码得到Kc
S42
S43
从配置文件中读取Base64(Tb)
进行Base64解码得到Tb
S44
S45
用Kc解密Tb得到密钥Kb
S46
从独立文件中读取Ta
用Kb解密Ta得到密钥Ka
S47

图4

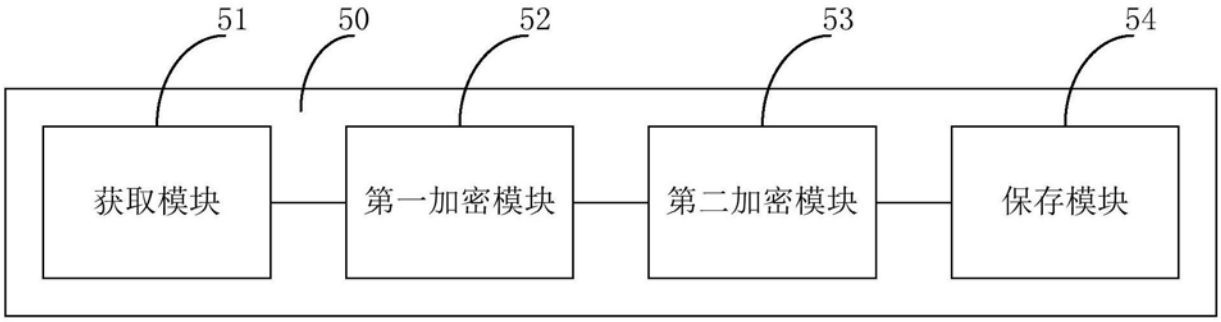

51
50
52
53
54
获取模块
第一加密模块
第二加密模块
保存模块

图5

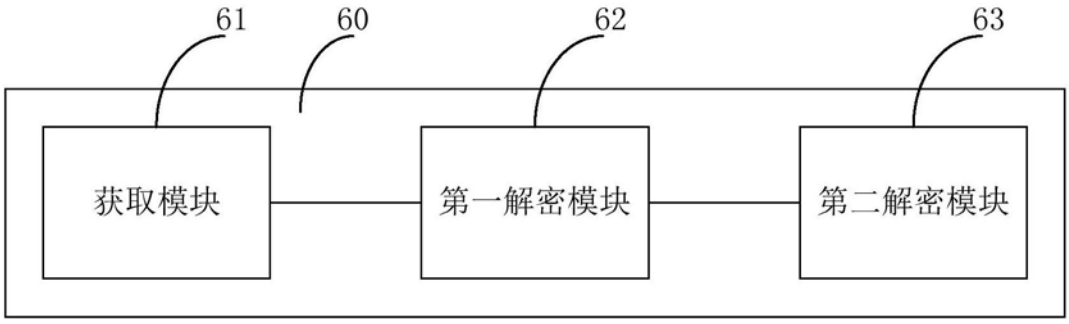

61
60
62
63
获取模块
第一解密模块
第二解密模块

图6