



(12) 发明专利申请

(10) 申请公布号 CN 105450620 A

(43) 申请公布日 2016. 03. 30

(21) 申请号 201410520339. 4

(22) 申请日 2014. 09. 30

(71) 申请人 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 范建伟

(74) 专利代理机构 北京国昊天诚知识产权代理
有限公司 11315

代理人 许志勇

(51) Int. Cl.

H04L 29/06(2006. 01)

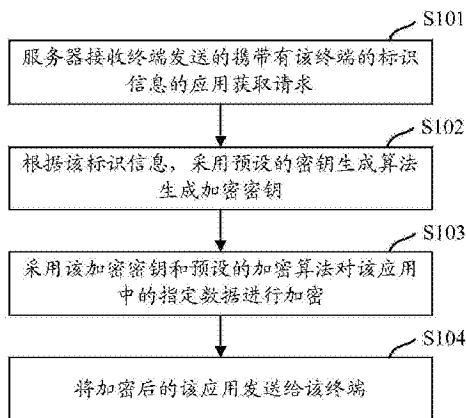
权利要求书3页 说明书12页 附图4页

(54) 发明名称

一种信息处理方法及装置

(57) 摘要

本申请公开了一种信息处理方法及装置,该方法服务器接收终端发送的携带有该终端的标识信息的应用获取请求,根据该标识信息,采用预设的密钥生成算法生成加密密钥,采用该加密密钥和预设的加密算法对该应用中的指定数据进行加密,将加密后的应用发送给该终端。通过上述方法,由于服务器是根据该终端的标识信息对应用中的指定数据进行加密的,因此,只有该终端才可根据自己的标识信息生成正确的解密密钥,而其它终端根据该其它终端的标识信息无法生成正确的解密密钥,从而也无法对应用中加密过的指定数据进行解密,因此,阻止了攻击者在其它终端上正常使用该应用。



1. 一种信息处理方法,其特征在于,包括:
接收终端发送的携带有所述终端的标识信息的应用获取请求;
根据所述应用获取请求中携带的标识信息,采用预设的密钥生成算法生成加密密钥;
采用所述加密密钥和预设的加密算法对所述应用中的指定数据进行加密;
将加密后的应用发送给所述终端。
2. 如权利要求 1 所述的方法,其特征在于,所述终端的标识信息用于唯一标识所述终端;或者
所述终端的标识信息用于标识至少两个终端。
3. 如权利要求 1 所述的方法,其特征在于,根据所述应用获取请求中携带的标识信息,采用预设的密钥生成算法生成加密密钥,具体包括:
确定所述标识信息的哈希 hash 值,作为密钥种子;
根据所述密钥种子,采用预设的密钥生成算法生成加密密钥。
4. 如权利要求 3 所述的方法,其特征在于,根据所述密钥种子,采用预设的密钥生成算法生成加密密钥,具体包括:
判断所述密钥种子的位数是否与所述密钥生成算法的适配密钥的位数相同;
若是,则将所述密钥种子确定为生成的加密密钥;
否则,将所述密钥种子转换为与所述适配密钥的位数相同的密钥种子,并将转换后的密钥种子确定为生成的加密密钥。
5. 如权利要求 1 所述的方法,其特征在于,所述应用中的指定数据包括:所述应用的数据库中的数据表。
6. 如权利要求 1 所述的方法,其特征在于,所述方法还包括:
接收终端发送的携带有所述终端的标识信息的密钥获取请求;
根据所述密钥获取请求中携带的标识信息,采用所述密钥生成算法生成解密密钥;
将所述解密密钥发送给所述终端。
7. 如权利要求 1 所述的方法,其特征在于,所述方法还包括:
接收所述终端发送的加密后的数据和所述终端的标识信息;
根据接收到的标识信息,采用所述密钥生成算法生成解密密钥;
采用与所述加密算法对应的解密算法以及所述解密密钥,对所述加密后的数据进行解密。
8. 一种信息处理方法,其特征在于,包括:
终端向服务器发送携带有所述终端的标识信息的应用获取请求;并
接收服务器返回的应用;
所述终端根据自身的标识信息,采用所述应用中内置的密钥生成算法生成解密密钥;
采用所述解密密钥和所述应用中内置的解密算法对所述应用中加密过的指定数据进行解密。
9. 如权利要求 8 所述的方法,其特征在于,所述终端根据自身的标识信息,采用所述应用中内置的密钥生成算法生成解密密钥,具体包括:
所述终端确定自身的标识信息的 hash 值,作为密钥种子;
根据所述密钥种子,采用所述应用中内置的密钥生成算法生成解密密钥。

10. 如权利要求 9 所述的方法,其特征在于,根据所述密钥种子,采用所述应用中内置的密钥生成算法生成解密密钥,具体包括:

判断所述密钥种子的位数是否与所述应用中内置的密钥生成算法的适配密钥的位数相同;

若是,则将所述密钥种子确定为生成的解密密钥;

否则,将所述密钥种子转换为与所述适配密钥的位数相同的密钥种子,并将转换后的密钥种子确定为生成的解密密钥。

11. 如权利要求 8 所述的方法,其特征在于,所述方法还包括:

所述终端根据自身的标识信息,采用所述应用中内置的密钥生成算法生成加密密钥;或者,向所述服务器发送携带有所述终端的标识信息的密钥获取请求,并接收所述服务器返回的加密密钥;

采用所述加密密钥和所述应用中内置的加密算法,对所述应用生成的数据进行加密;保存加密后的数据,或者,将加密后的数据和所述终端的标识信息发送给所述服务器。

12. 一种信息处理方法,其特征在于,包括:

终端向服务器发送携带有所述终端的标识信息的应用获取请求;

接收服务器返回的应用;

向所述服务器发送携带有所述终端的标识信息的密钥获取请求;

接收服务器返回的解密密钥,其中,所述解密密钥是所述服务器根据所述密钥获取请求携带的标识信息以及预设的密钥生成算法生成的;

所述终端采用所述解密密钥和所述应用中内置的解密算法对所述应用中加密过的指定数据进行解密。

13. 一种信息处理装置,其特征在于,包括:

接收模块,用于接收终端发送的携带有所述终端的标识信息的应用获取请求;

生成模块,用于根据所述应用获取请求中携带的标识信息,采用预设的密钥生成算法生成加密密钥;

加密模块,用于采用所述加密密钥和预设的加密算法对所述应用中的指定数据进行加密;

发送模块,用于将加密后的应用发送给所述终端。

14. 如权利要求 13 所述的装置,其特征在于,所述终端的标识信息用于唯一标识所述终端;或者

所述终端的标识信息用于标识至少两个终端。

15. 如权利要求 13 所述的装置,其特征在于,所述生成模块具体用于,确定所述标识信息的哈希 hash 值,作为密钥种子,根据所述密钥种子,采用预设的密钥生成算法生成加密密钥。

16. 如权利要求 15 所述的装置,其特征在于,所述生成模块具体用于,判断所述密钥种子的位数是否与所述密钥生成算法的适配密钥的位数相同,若是,则将所述密钥种子确定为生成的加密密钥,否则,将所述密钥种子转换为与所述适配密钥的位数相同的密钥种子,并将转换后的密钥种子确定为生成的加密密钥;

17. 如权利要求 13 所述的装置,其特征在于,所述应用中的指定数据包括:所述应用的

数据库中的数据表。

18. 如权利要求 13 所述的装置,其特征在于,所述接收模块还用于,接收终端发送的携带有所述终端的标识信息的密钥获取请求;

所述生成模块还用于,根据所述密钥获取请求中携带的标识信息,采用所述密钥生成算法生成解密密钥;

所述发送模块还用于,将所述解密密钥发送给所述终端。

19. 如权利要求 13 所述的装置,其特征在于,所述装置还包括:

解密模块,用于接收所述终端发送的加密后的数据和所述终端的标识信息,根据接收到的标识信息,采用所述密钥生成算法生成解密密钥,采用与所述加密算法对应的解密算法以及所述解密密钥,对所述加密后的数据进行解密。

20. 一种信息处理装置,其特征在于,包括:

发送模块,用于向服务器发送携带有所述终端的标识信息的应用获取请求;

接收模块,用于接收服务器返回的应用;

生成模块,用于根据自身的标识信息,采用所述应用中内置的密钥生成算法生成解密密钥;

解密模块,用于采用所述解密密钥和所述应用中内置的解密算法对所述应用中加密过的指定数据进行解密。

21. 如权利要求 20 所述的装置,其特征在于,所述生成模块具体用于,确定所述终端的标识信息的 hash 值,作为密钥种子,根据所述密钥种子,采用所述应用中内置的密钥生成算法生成解密密钥。

22. 如权利要求 20 所述的装置,其特征在于,所述生成模块具体用于,判断所述密钥种子的位数是否与所述应用中内置的密钥生成算法的适配密钥的位数相同,若是,则将所述密钥种子确定为生成的解密密钥,否则,将所述密钥种子转换为与所述适配密钥的位数相同的密钥种子,并将转换后的密钥种子确定为生成的解密密钥。

23. 如权利要求 20 所述的装置,其特征在于,所述装置还包括:

加密模块,用于根据自身的标识信息,采用所述应用中内置的密钥生成算法生成加密密钥,或者,向所述服务器发送携带有所述终端的标识信息的密钥获取请求,并接收所述服务器返回的加密密钥;并用于采用所述加密密钥和所述应用中内置的加密算法,对所述应用生成的数据进行加密;保存加密后的数据,或者,将加密后的数据和所述终端的标识信息发送给所述服务器。

24. 一种信息处理装置,其特征在于,包括:

第一发送模块,用于向服务器发送携带有所述终端的标识信息的应用获取请求;

第一接收模块,用于接收服务器返回的应用;

第二发送模块,用于向所述服务器发送携带有所述终端的标识信息的密钥获取请求;

第二接收模块,用于接收服务器返回的解密密钥,其中,所述解密密钥是所述服务器根据所述密钥获取请求携带的标识信息以及预设的密钥生成算法生成的;

解密模块,用于采用所述解密密钥和所述应用中内置的解密算法对所述应用中加密过的指定数据进行解密。

一种信息处理方法及装置

技术领域

[0001] 本申请涉及计算机技术领域,尤其涉及一种信息处理方法及装置。

背景技术

[0002] 在现代社会中,随着计算机信息技术的飞速发展,人们对数字知识产权的保护越来越重视。

[0003] 在现有技术中,各种应用一般用许可证 (license) 的方式来保护自己的数字知识产权,以阻止用户在未授权设备上使用该应用,也即,仅当应用对其所在设备的 license 校验成功后,才允许该设备运行该应用。例如,对于使用 java 语言开发的应用,在其源程序中,会有一段特定的代码对该应用所在设备的 license 的有效性进行校验,并根据校验结果判断是否允许该设备运行该应用,若 license 有效,则允许该设备运行该应用,否则,拒绝该设备运行该应用。

[0004] 但是,对于使用诸如 java 语言等解释型语言开发的应用,由于攻击者可对应用进行反编译分析获得源程序,进而,对源程序中用于判断 license 有效性的代码进行恶意修改,例如,可将该段代码的逻辑修改为若 license 无效,则允许该设备运行该应用,否则,拒绝该设备运行该应用,这样一来,未授权设备可正常运行该应用,持有有效 license 的设备反而无法运行该应用。因此,license 这种方式无法阻止攻击者在未授权设备上正常使用该应用。

发明内容

[0005] 本申请实施例提供一种信息处理方法及装置,用以解决现有技术中用 license 的方式无法阻止攻击者在未授权设备上使用应用的问题。

[0006] 本申请实施例提供的一种信息处理方法,包括:

[0007] 接收终端发送的携带有所述终端的标识信息的应用获取请求;

[0008] 根据所述应用获取请求中携带的标识信息,采用预设的密钥生成算法生成加密密钥;

[0009] 采用所述加密密钥和预设的加密算法对所述应用中的指定数据进行加密;

[0010] 将加密后的应用发送给所述终端。

[0011] 本申请实施例提供的一种信息处理方法,包括:

[0012] 终端向服务器发送携带有所述终端的标识信息的应用获取请求;并

[0013] 接收服务器返回的应用;

[0014] 所述终端根据自身的标识信息,采用所述应用中内置的密钥生成算法生成解密密钥;

[0015] 采用所述解密密钥和所述应用中内置的解密算法对所述应用中加密过的指定数据进行解密。

[0016] 本申请实施例提供的一种信息处理方法,包括:

- [0017] 终端向服务器发送携带有所述终端的标识信息的应用获取请求；
- [0018] 接收服务器返回的应用；
- [0019] 向所述服务器发送携带有所述终端的标识信息的密钥获取请求；
- [0020] 接收服务器返回的解密密钥，其中，所述解密密钥是所述服务器根据所述密钥获取请求携带的标识信息以及预设的密钥生成算法生成的；
- [0021] 所述终端采用所述解密密钥和所述应用中内置的解密算法对所述应用中加密过的指定数据进行解密。
- [0022] 本申请实施例提供的一种信息处理装置，包括：
- [0023] 接收模块，用于接收终端发送的携带有所述终端的标识信息的应用获取请求；
- [0024] 生成模块，用于根据所述应用获取请求中携带的标识信息，采用预设的密钥生成算法生成加密密钥；
- [0025] 加密模块，用于采用所述加密密钥和预设的加密算法对所述应用中的指定数据进行加密；
- [0026] 发送模块，用于将加密后的应用发送给所述终端。
- [0027] 本申请实施例提供的一种信息处理装置，包括：
- [0028] 发送模块，用于向服务器发送携带有所述终端的标识信息的应用获取请求；
- [0029] 接收模块，用于接收服务器返回的应用；
- [0030] 生成模块，用于根据自身的标识信息，采用所述应用中内置的密钥生成算法生成解密密钥；
- [0031] 解密模块，用于采用所述解密密钥和所述应用中内置的解密算法对所述应用中加密过的指定数据进行解密。
- [0032] 本申请实施例提供的一种信息处理装置，包括：
- [0033] 第一发送模块，用于向服务器发送携带有所述终端的标识信息的应用获取请求；
- [0034] 第一接收模块，用于接收服务器返回的应用；
- [0035] 第二发送模块，用于向所述服务器发送携带有所述终端的标识信息的密钥获取请求；
- [0036] 第二接收模块，用于接收服务器返回的解密密钥，其中，所述解密密钥是所述服务器根据所述密钥获取请求携带的标识信息以及预设的密钥生成算法生成的；
- [0037] 解密模块，用于采用所述解密密钥和所述应用中内置的解密算法对所述应用中加密过的指定数据进行解密。
- [0038] 本申请实施例提供的信息处理方法及装置，该方法服务器接收终端发送的携带有该终端的标识信息的应用获取请求，根据该标识信息，采用预设的密钥生成算法生成加密密钥，采用该加密密钥和预设的加密算法对该应用中的指定数据进行加密，将加密后的应用发送给该终端。通过上述方法，由于服务器是根据该终端的标识信息对应用中的指定数据进行加密的，因此，只有根据该终端的标识信息才能生成正确的解密密钥，而根据其它终端的标识信息无法生成正确的解密密钥，从而也无法对应用中加密过的指定数据进行解密，因此，阻止了攻击者在其它终端上正常使用该应用。

附图说明

[0039] 此处所说明的附图用来提供对本申请的进一步理解,构成本申请的一部分,本申请的示意性实施例及其说明用于解释本申请,并不构成对本申请的不当限定。在附图中:

[0040] 图 1 为本申请实施例提供的信息处理过程;

[0041] 图 2 为本申请实施例提供的生成加密密钥的过程;

[0042] 图 3 为本申请实施例提供的对应于图 1 的第一种信息处理过程;

[0043] 图 4 为本申请实施例提供的对应于图 1 的第二种信息处理过程;

[0044] 图 5 为本申请实施例提供的信息处理装置结构示意图;

[0045] 图 6 为本申请实施例提供的另一个信息处理装置结构示意图;

[0046] 图 7 为本申请实施例提供的另一个信息处理装置结构示意图。

具体实施方式

[0047] 为使本申请的目的、技术方案和优点更加清楚,下面将结合本申请具体实施例及相应的附图对本申请技术方案进行清楚、完整地描述。显然,所描述的实施例仅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做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。

[0048] 图 1 为本申请实施例提供的信息处理过程,具体包括以下步骤:

[0049] S101:服务器接收终端发送的携带有该终端的标识信息的应用获取请求。

[0050] 在本申请实施例中,所述的服务器可以是任意应用提供方的服务器,所述的终端包括但不限于:个人计算机(Personal Computer, PC)、手机、平板电脑等。

[0051] 服务器为终端提供了获取应用的接口,终端在从服务器中获取应用时,则可通过该接口向服务器发送携带有该终端的标识信息的应用获取请求,服务器则通过此接口接收终端发送的应用获取请求。其中,所述的接口可预先对应用获取请求的内容、格式进行定义,使得服务器能够正确识别接收到的应用获取请求,并进行后续处理。

[0052] 所述终端的标识信息可唯一标识该终端,例如,对于手机,该标识信息可以是该手机的移动设备国际身份码(International Mobile Equipment Identity, IMEI),每个 IMEI 可唯一标识一台手机、或其它移动设备,对于 PC,该标识信息可以是该 PC 的媒体接入控制层(Media Access Control, MAC) 地址,也即,物理地址,每个 MAC 地址可唯一标识一台 PC、或其它物理设备。当然,所述终端的标识信息也可标识至少两个终端。例如,对于手机,该标识信息还可以是该手机的生产批次数号,该生产批次数号可标识同一生产批次内生产的所有手机。

[0053] S102:服务器根据该标识信息,采用预设的密钥生成算法生成加密密钥。

[0054] 在本申请实施例中,可预先在应用中内置密钥生成算法,则服务器可根据应用获取请求携带的标识信息,采用该应用中内置的密钥生成算法生成加密密钥。具体的,服务器可从保存的该应用中获取预先内置在该应用中的密钥生成算法。

[0055] 另外,也可不在该应用中预先内置密钥生成算法,而是在服务器中预先保存多种密钥生成算法,则服务器在接收到终端发送的携带有该终端的标识信息的应用获取请求时,可从预先保存的各密钥生成算法中任意选择一种密钥生成算法,然后,根据该终端的标识信息,采用选择出的密钥生成算法生成加密密钥,并将选择出的该密钥生成算法内置在该应用中。

[0056] S103:服务器采用该加密密钥和预设的加密算法对该应用中的指定数据进行加密。

[0057] 类似的,可预先在应用中内置加密算法和相应的解密算法(解密算法用于后续终端对该应用中的加密过的指定数据进行解密),则服务器可采用步骤 S102 生成的加密密钥和该应用中内置的加密算法,对该应用中的指定数据进行加密。具体的,服务器可直接从该应用中获取预先内置在该应用中的加密算法。

[0058] 另外,也可不在该应用中预先内置加密算法,而是在服务器中预先保存多种加密算法,则服务器在通过上述步骤 S102 生成加密密钥后,可从预先保存的各加密算法中任意选择一种加密算法,然后,采用步骤 S102 生成的加密密钥和选择出的加密算法对该应用中的指定数据进行加密。当然,服务器还可将与选择出的加密算法对应的解密算法也内置在该应用中,使终端后续可采用该解密算法对该应用中加密过的指定数据进行解密。

[0059] 具体的,本申请中所述的加密算法可以是诸如 RSA、数据加密标准(Data Encryption Standard, DES)、三重数据加密标准(Triple Data Encryption Standard, 3DES)、国际数据加密算法(International Data Encryption Algorithm, IDEA)、安全哈希算法 1(Secure Hash Algorithm1, Sha1)、Sha256、Sha512、消息摘要算法第 5 版(Message Digest Algorithm5, MD5)、高级加密标准(Advanced Encryption Standard, AES)等,也可以是应用提供方的开发人员自行开发的加密算法,本申请中对服务器上预设的加密算法并不做限定。

[0060] 所述的应用中的指定数据可以是能够影响该应用的运行结果正确性的关键数据。

[0061] S104:服务器将加密后的应用发送给该终端。

[0062] 终端获得应用后,如果该应用是由该终端向服务器发送了应用获取请求(该应用获取请求中携带有该终端自身的标识信息)后从服务器接收到的,则该应用中的指定数据是基于该终端的标识信息进行加密的数据,从而,该终端根据该应用中内置的密钥生成算法和自身的标识信息,可生成正确的解密密钥,并可根据该解密密钥和该终端中内置的解密算法对该应用中加密过的指定数据进行解密,进而可正确地运行该应用,此时,该终端可称为已授权终端。而如果该应用并非是由该终端通过向服务器发送了应用获取请求后从服务器接收到的(如,通过从其它终端上复制得到的),则该应用中的指定数据不是基于该终端的标识信息加密的,该终端也就不能对该应用中加密过的该指定数据正确地解密,从而不能正确地运行该应用,此时,该终端可称为未授权终端。

[0063] 通过上述方法,即使未授权终端从已授权终端上复制了该应用,由于服务器发送给已授权终端的应用中的关键数据已经加密,且该未授权终端根据自身的标识信息无法生成正确的解密密钥(根据已授权终端的标识信息才能够生成正确的解密密钥),从而,该未授权终端无法对该应用中的加密过的关键数据正确地解密,因此,可以阻止攻击者在未授权终端上正常使用该应用。

[0064] 另外,由于终端的标识信息也可用于标识至少两个终端,在这种情况下,若服务器返回的应用是基于该标识信息加密的,则对于该应用,该标识信息所标识的所有终端均为已授权终端,也即,这些终端均可根据自身的标识信息生成正确的解密密钥并对该应用中加密过的指定数据进行解密,从而,在这些终端上均可以正常使用该应用。

[0065] 例如,假定所述终端为手机,则手机的标识信息可以为生产批序号。服务器根据

该手机的生产批次序号生成加密密钥,并采用该加密密钥和预设的加密算法对应用中的指定数据进行加密后,则该生产批次序号对应的所有手机均可生成正确的解密密钥,进而可对该加密后的应用进行解密,从而可以正常运行该应用。

[0066] 在本申请实施例中,服务器将加密后的应用发送给终端后,当该终端需要对该应用中加密的指定数据进行解密时,也可不自行生成解密密钥,而是可以向服务器发送携带有该终端的标识信息的密钥获取请求,以获取解密密钥,则服务器接收该终端发送的密钥获取请求后,可根据密钥获取请求中携带的标识信息,采用预设的密钥生成算法生成解密密钥,再将所述解密密钥发送给该终端。在这种情况下,由于生成解密密钥的过程是在服务器上进行,而不是在各个终端上进行,因此,也减小了密钥生成算法泄露的可能性,进一步增强了安全性。

[0067] 进一步的,在上述步骤 S102 中,服务器生成加密密钥的方法具体可以为:服务器确定应用获取请求中携带的终端的标识信息的哈希(hash)值,作为密钥种子,并根据该密钥种子,采用预设的密钥生成算法生成加密密钥。

[0068] 具体的,服务器可判断该密钥种子的位数是否与该密钥生成算法的适配密钥的位数相同,若相同,则将该密钥种子确定为生成的加密密钥,若不同,则将该密钥种子转换为与该密钥生成算法的适配密钥的位数相同的密钥种子,并将转换后的密钥种子确定为生成的加密密钥。

[0069] 其中,转换的方法具体可以为:将位数小于所述适配密钥的位数的密钥种子补齐,将位数大于所述适配密钥的位数的密钥种子截断,使得补齐后或截断后的密钥种子的位数与所述适配密钥的位数相同。例如,当所述密钥种子的位数小于所述密钥生成算法的适配密钥的位数时,确定所述密钥种子的 hash 值,将所述密钥种子与所述密钥种子的 hash 值组合得到的序列重新确定为密钥种子,并判断重新确定的密钥种子的位数是否与所述适配密钥的位数相同,直至确定的密钥种子的位数不小于所述适配密钥的位数为止,当所述密钥种子的位数大于所述密钥生成算法的适配密钥的位数时,将所述密钥种子截断为所述适配密钥的位数,并将截断后的密钥种子确定为生成的加密密钥,如图 2 所示。

[0070] 图 2 为本申请实施例提供的生成加密密钥的过程,具体包括以下步骤:

[0071] S201:服务器确定应用获取请求中携带的终端的标识信息的 hash 值,作为密钥种子。

[0072] 具体的,可采用单向散列算法(如 MD5)确定 hash 值。

[0073] S202:判断该密钥种子的位数是否与该密钥生成算法的适配密钥的位数相同,若相同,执行步骤 S206,否则,执行步骤 S203。

[0074] S203:判断该密钥种子的位数是否大于该密钥生成算法的适配密钥的位数,若是,执行步骤 S204,否则,执行步骤 S205。

[0075] S204:将该密钥种子截断为适配密钥的位数,并将截断后的密钥种子确定为生成的加密密钥。

[0076] 本申请中对截断的方式并不做限定。其中一种可行的方式为:从该密钥种子的最高位开始,向该密钥种子的最低位方向依次选取适配密钥的位数,将已选取的部分确定为生成的加密密钥,即,截断掉密钥种子中的未选取部分。

[0077] S205:确定该密钥种子的 hash 值,将该密钥种子与该密钥种子的 hash 值组合得到

的序列重新确定为密钥种子,返回步骤 S202。

[0078] 本申请中对组合的方式并不做限定。其中一种可行的方式为:将该密钥种子与该密钥种子的 hash 值首尾相接,得到一个序列,显然,该序列的位数为该密钥种子的位数和该密钥种子的 hash 值的位数之和,然后,可将该序列重新确定为密钥种子。

[0079] S206:将该密钥种子确定为生成的加密密钥。

[0080] 进一步的,在本申请实施例,对于依赖于底层数据源(底层数据源,一般为数据库中的数据表)才能正确运行的应用,只要对其数据库中的数据表进行加密后,即可阻止攻击者在未授权终端上正常使用该应用。因此,在上述步骤 S103 中,所述应用的指定数据包括:所述应用的数据库中的数据表。

[0081] 以游戏应用为例进行说明。很多游戏应用都使用数据库来对游戏中的各种数值进行设定和管理,这些数值可以是玩家角色(或游戏角色,或非玩家控制角色(Non Player Character, NPC)等游戏角色)的生命值、攻击值、防御值、物品和装备的标识(Identity, ID)等。玩家运行该应用时,该应用从数据库中读取各数据表,载入各种初始化数据,并在玩家的游戏过程中,根据玩家角色的活动,对各数据表进行实时操作(创建、删除、读取、写入等操作)。

[0082] 假定服务器上有游戏应用 A。游戏应用 A 的数据库中的某数据表记录了 3 个游戏角色 1~3 的相关数值(生命值、攻击值、防御值),该数据表为游戏应用 A 的指定数据(也即,待加密数据),如下表 1 所示。

[0083]

	生命值(二进制)	攻击值(二进制)	防御值(二进制)
游戏角色 1	1100	1000	1010
游戏角色 2	1100	1010	1000
游戏角色 3	1100	1001	1101

[0084] 表 1

[0085] 在上述表 1 中,分别示出了游戏角色 1~3 的生命值、攻击值、防御值。

[0086] 某玩家通过已授权手机向服务器获取该游戏应用,则服务器首先接收到该玩家发送的应用获取请求后,获取该游戏应用中内置的密钥生成算法和加密算法。假定该密钥生成算法为上例中所述的密钥生成算法,该加密算法具体为:将加密密钥与待加密数据按位作异或运算,将异或运算后所得的数据作为待加密数据对应的加密数据。

[0087] 然后,服务器根据该玩家发送的应用获取请求中携带的该手机的 IMEI,采用 MD5 计算出该 IMEI 的 128 位的 hash 值,假定该 hash 值用十六进制表示为:0xC8825DB10F2590EAAAD3B435B51404EE。

[0088] 由于对于上述表 1 所示的数据表,可以分别将数据表中的每一行中的数值首尾相接组合为一个序列,并对每一个序列加密(以下称为:按行加密),在这种情况下,使用位数和所述序列的位数相同的加密密钥可以比较方便地对所述序列加密。因此,获取的密钥生成算法的适配密钥的位数可为该序列的位数为数据表中的任意一行中的数值的位数之和(每行有 3 个数据,每个数据有 4 位,则该位数之和即为 12 位),进而,使用该密钥生成算法

生成的加密密钥也为 12 位。

[0089] 将计算出的 hash 值作为密钥种子,由于该 hash 值的位数(为 128 位)大于密钥生成算法的适配密钥的位数(为 12 位),因此,可从该密钥种子的最高位开始,向该密钥种子的最低位方向依次选取 12 位,截断掉密钥种子中的未选取部分,然后,可将剩余的已选取的 12 位确定为生成的用于按行加密的加密密钥,该按行加密的加密密钥用十六进制表示为 :0xC88,用二进制值表示为 110010001000)。

[0090] 用该加密密钥分别对表 1 按行加密,获得加密后的三个行序列的数值:

[0091] $110010001000 \oplus 110010001010 = 000000000010$;

[0092] $110010001000 \oplus 110010101000 = 000000100000$;

[0093] $110010001000 \oplus 110010011101 = 000000010101$ 。

[0094] 下表 2 示出了对表 1 按行加密后的数据表。

[0095]

	生命值(二进制)	攻击值(二进制)	防御值(二进制)
游戏角色 1	0000	0000	0010
游戏角色 2	0000	0010	0000
游戏角色 3	0000	0001	0101

[0096] 表 2

[0097] 在上述表 2 中,分别示出了按行加密后的游戏角色 1~3 的生命值、攻击值、防御值。

[0098] 服务器将加密后的游戏应用发送给该已授权手机,该已授权手机在运行该加密后的游戏应用时,可根据自身的 IMEI,采用该游戏应用中内置的密钥生成算法和解密算法对加密过的数据表进行解密,进而,可正常使用该游戏应用。而若攻击者在未授权手机上运行加密后的该游戏应用,由于该未授权手机根据自身的 IMEI 和该游戏应用中内置的密钥生成算法无法生成正确的解密密钥,从而无法对加密过的数据表进行解密,由于上述加密后的数值和原始数值不同,则会影响的该游戏应用的数值系统的计算结果的正确性,因此,攻击者也无法正常使用该加密后的游戏应用。

[0099] 另外,由于数据表中的同一列中数值可能相同,因此,在这种情况下,若仅对数据表按行加密,加密后的数据表中的该同一列中的数值仍然可能相同(如表 2 所示,表 2 中第 1 列的数值全都相同),则攻击者可能据此推断加密该数据表所采用的加密密钥和加密算法,增加了该加密密钥和该加密算法被破译的风险。因此,为了增强对数据表加密的强度,除了对数据表按行加密,还可以对加密后的数据表进行二次加密(所述的二次加密可以是按列加密,具体的,将数据表中的每一列中的数值首尾相接组合为一个序列,然后对该序列加密),经过二次加密后,该同一列中原本相同的数值变得不全相同。其中,二次加密时使用的加密密钥可通过另一种密钥生成算法生成。

[0100] 继续沿用上例对所述的二次加密(假定是按列加密)进行说明,服务器仍将计算出的 hash 值作为密钥种子,可从该密钥种子的最低位开始,向该密钥种子的最高位方向依次选取 12 位,截断掉密钥种子中的未选取部分,然后,可将剩余的已选取的 12 位确定为生

成的用于二次加密的加密密钥（此处采用了与生成用于按行加密的加密密钥时所使用截断方式不同的另一种截断方式），该用于二次加密的加密密钥用十六进制表示为：0x4EE，用二进制值表示为 010011101110。

[0101] 用该加密密钥对表 2 二次加密，获得二次加密后的三个列序列的数值：

[0102] $010011101110 \oplus 000000000000 = 010011101110$ ；

[0103] $010011101110 \oplus 000000100001 = 010011001111$ ；

[0104] $010011101110 \oplus 001000000101 = 011011101011$ 。

[0105] 下表 3 示出了对表 2 二次加密后的数据表。

[0106]

	生命值（二进制）	攻击值（二进制）	防御值（二进制）
游戏角色 1	0100	0100	0110
游戏角色 2	1110	1100	1110
游戏角色 3	1110	1111	1011

[0107] 表 3

[0108] 在上述表 3 中，分别示出了二次加密后的游戏角色 1～3 的生命值、攻击值、防御值。

[0109] 可以看出，在表 1 中，游戏角色 1～3 的生命值相同，在表 2 中，经过按行加密后的游戏角色 1～3 的生命值仍相同，而在表 3，经过二次加密后的游戏角色 1～3 的生命值已不全相同，因此，二次加密可以增加攻击者破解加密后的数据表的难度，增强了对数据表加密的强度。

[0110] 进一步的，终端在接收到服务器发送的加密后的应用并解密后，在运行该应用的过程中，该应用可能会生成需保存的数据（如历史数据等）或需反馈给服务器的数据，则终端可根据自身的标识信息，采用该应用中内置的密钥生成算法生成加密密钥，或者，该终端也可向服务器发送携带有该终端的标识信息的密钥获取请求，并接收服务器返回的加密密钥。进而，该终端可采用该加密密钥和该应用中内置的加密算法，对该应用生成的数据进行加密。最后再保存加密后的数据，或者，将加密后的数据和该终端的标识信息发送给服务器。服务器接收该终端发送的加密后的数据和该终端的标识信息，可根据接收到的标识信息，采用预设的密钥生成算法生成解密密钥，采用与终端采用的加密算法对应的解密算法以及该解密密钥，对加密后的数据进行解密。

[0111] 图 3 为本申请实施例提供的对应于图 1 的第一种信息处理过程，具体包括以下步骤：

[0112] S301：终端向服务器发送携带有该终端的标识信息的应用获取请求。

[0113] S302：终端接收服务器返回的应用。

[0114] 其中，该应用中的指定数据已经被服务器加密。

[0115] S303：终端根据自身的标识信息，采用该应用中内置的密钥生成算法生成解密密钥。

[0116] 在本申请实施例中，在应用中内置了加密该应用中的指定数据所采用的密钥生成

算法,以及用于解密该加密后的指定数据的解密算法。终端根据自身的标识信息,采用该应用中内置的密钥生成算法可生成解密密钥,生成解密密钥的方法和服务器生成加密密钥的方法相同,在此不再赘述。

[0117] S304:终端采用该解密密钥和该应用中内置的解密算法对该应用中的加密过的指定数据进行解密。

[0118] 终端对该应用中的加密过的指定数据进行解密,即为服务器对该指定数据进行加密的逆过程,在此不再赘述。

[0119] 通过上述方法,只有已授权终端才可根据自身的标识信息生成正确的解密密钥,而未授权终端根据自身的标识信息无法生成正确的解密密钥,从而也无法对应用中加密过的指定数据进行解密,因此,阻止了攻击者在未授权终端上正常使用该应用。

[0120] 进一步的,终端在运行应用的过程中,可能会生成需保存的数据(如历史数据等)或需反馈给服务器的数据,为了保证生成的数据的安全性,则终端可根据自身的标识信息,采用该应用中内置的密钥生成算法生成加密密钥,或者,该终端也可向服务器发送携带有该终端的标识信息的密钥获取请求,并接收服务器返回的加密密钥。进而,该终端可采用该加密密钥和该应用中内置的加密算法,对生成的数据进行加密。最后再保存加密后的数据,或者,将加密后的数据和该终端的标识信息发送给服务器处理。

[0121] 图4为本申请实施例提供的对应于图1的第二种信息处理过程,具体包括以下步骤:

[0122] S401:终端向服务器发送携带有该终端的标识信息的应用获取请求。

[0123] S402:该终端接收服务器返回的应用。

[0124] S403:该终端向服务器发送携带有该终端的标识信息的密钥获取请求。

[0125] S404:该终端接收服务器返回的解密密钥。

[0126] 其中,该解密密钥是服务器根据密钥获取请求携带的标识信息以及预设的密钥生成算法生成的。

[0127] S405:该终端采用该解密密钥和该应用中内置的解密算法对该应用中加密过的指定数据进行解密。

[0128] 通过上述方法,只有当服务器接收到的应用获取请求中携带的标识信息和密钥获取请求中携带的标识信息相同时,服务器才可根据密钥获取请求中携带的标识信息生成正确的解密密钥。因此,对于已授权终端从服务器获取的加密过的应用,即使将该加密过的应用复制到未授权终端上运行,由于未授权终端需要解密该应用时,向服务器发送的密钥获取请求中携带的是该未授权终端的标识信息,因此,服务器也无法生成正确的解密密钥,从而该未授权终端也无法对该应用进行解密,因此,阻止了攻击者在未授权终端上正常使用该应用。另外,由于生成解密密钥的过程是在服务器上进行,而不是在各个终端上进行,因此,也减小了密钥生成算法泄露的可能性,进一步增强了安全性。

[0129] 在本申请实施例中,为了进一步增强安全性,服务器发送给终端的应用中也可不内置密钥生成算法。当终端需要获取解密密钥时,可向服务器发送携带有该终端的标识信息的密钥获取请求,服务器根据该终端的标识信息和预设的密钥生成算法生成解密密钥,并发送给该终端,然后,该终端采用该解密密钥和该应用中内置的解密算法对该应用中加密过的指定数据进行解密。

[0130] 在本申请实施例中,也可不由服务器对应用中的指定数据加密,而是由终端在首次运行应用时,根据自身的标识信息,采用该应用中内置的密钥生成算法生成加密密钥,并使用该加密密钥和该应用中内置的加密算法对该应用中的指定数据进行加密。在应用运行过程中需要使用该指定数据时,该终端可再根据自身的标识信息,采用该应用中内置的密钥生成算法生成解密密钥,并使用该解密密钥和该应用中内置的解密算法对该应用中加密过的指定数据进行解密,从而获得该指定数据。此后,即使攻击者将该应用从该终端复制到其它终端上运行,根据其它终端的标识信息也无法生成正确的解密密钥,从而也无法对该应用中加密过的指定数据进行解密,因此,阻止了攻击者在其它终端上正常使用该应用。

[0131] 以上为本申请实施例提供的信息处理方法,基于同样的思路,本申请实施例还提供相应的信息处理装置,如图 5、图 6、图 7 所示。

[0132] 图 5 为本申请实施例提供的信息处理装置结构示意图,具体包括:

[0133] 接收模块 501,用于接收终端发送的携带有所述终端的标识信息的应用获取请求;

[0134] 生成模块 502,用于根据所述应用获取请求中携带的标识信息,采用预设的密钥生成算法生成加密密钥;

[0135] 加密模块 503,用于采用所述加密密钥和预设的加密算法对所述应用中的指定数据进行加密;

[0136] 发送模块 504,用于将加密后的应用发送给所述终端。

[0137] 所述生成模块 502 具体用于,确定所述标识信息的哈希 hash 值,作为密钥种子,根据所述密钥种子,采用预设的密钥生成算法生成加密密钥。

[0138] 所述生成模块 502 具体用于,判断所述密钥种子的位数是否与所述密钥生成算法的适配密钥的位数相同,若是,则将所述密钥种子确定为生成的加密密钥,否则,将所述密钥种子转换为与所述适配密钥的位数相同的密钥种子,并将转换后的密钥种子确定为生成的加密密钥。

[0139] 所述应用中的指定数据包括:所述应用的数据库中的数据表。

[0140] 所述装置还包括:

[0141] 所述接收模块 501 还用于,接收终端发送的携带有所述终端的标识信息的密钥获取请求;

[0142] 所述生成模块 502 还用于,根据所述密钥获取请求中携带的标识信息,采用所述密钥生成算法生成解密密钥;

[0143] 所述发送模块 504 还用于,将所述解密密钥发送给所述终端。

[0144] 所述装置还包括:

[0145] 解密模块 505,用于接收所述终端发送的加密后的数据和所述终端的标识信息,根据接收到的标识信息,采用所述密钥生成算法生成解密密钥,采用与所述加密算法对应的解密算法以及所述解密密钥,对所述加密后的数据进行解密。

[0146] 具体的上述如图 5 所示的装置可以位于服务器上。

[0147] 图 6 为本申请实施例提供的另一个信息处理装置结构示意图,具体包括:

[0148] 发送模块 601,用于向服务器发送携带有所述终端的标识信息的应用获取请求;

[0149] 接收模块 602,用于接收服务器返回的应用;

[0150] 生成模块 603,用于根据自身的标识信息,采用所述应用中内置的密钥生成算法生成解密密钥;

[0151] 解密模块 604,用于采用所述解密密钥和所述应用中内置的解密算法对所述应用中加密过的指定数据进行解密。

[0152] 所述生成模块 603 具体用于,确定自身的标识信息的 hash 值,作为密钥种子,根据所述密钥种子,采用所述应用中内置的密钥生成算法生成解密密钥。

[0153] 所述生成模块 603 具体用于,判断所述密钥种子的位数是否与所述应用中内置的密钥生成算法的适配密钥的位数相同,若是,则将所述密钥种子确定为生成的解密密钥,否则,将所述密钥种子转换为与所述适配密钥的位数相同的密钥种子,并将转换后的密钥种子确定为生成的解密密钥。

[0154] 所述装置还包括:

[0155] 加密模块 605,用于根据自身的标识信息,采用所述应用中内置的密钥生成算法生成加密密钥,或者,向所述服务器发送携带有所述终端的标识信息的密钥获取请求,并接收所述服务器返回的加密密钥;并用于采用所述加密密钥和所述应用中内置的加密算法,对所述应用生成的数据进行加密;保存加密后的数据,或者,将加密后的数据和所述终端的标识信息发送给所述服务器。

[0156] 具体的上述如图 6 所示的装置可以位于终端上。

[0157] 图 7 为本申请实施例提供的另一个信息处理装置结构示意图,具体包括:

[0158] 第一发送模块 701,用于向服务器发送携带有所述终端的标识信息的应用获取请求;

[0159] 第一接收模块 702,用于接收服务器返回的应用;

[0160] 第二发送模块 703,用于向所述服务器发送携带有所述终端的标识信息的密钥获取请求;

[0161] 第二接收模块 704,用于接收服务器返回的解密密钥,其中,所述解密密钥是所述服务器根据所述密钥获取请求携带的标识信息以及预设的密钥生成算法生成的;

[0162] 解密模块 705,用于采用所述解密密钥和所述应用中内置的解密算法对所述应用中加密过的指定数据进行解密。

[0163] 具体的上述如图 7 所示的装置可以位于终端上。

[0164] 本领域内的技术人员应明白,本发明的实施例可提供为方法、系统、或计算机程序产品。因此,本发明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,本发明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。

[0165] 本发明是参照根据本发明实施例的方法、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。

[0166] 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。

[0167] 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设备上,使得在计算机或其他可编程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。

[0168] 在一个典型的配置中,计算设备包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。

[0169] 内存可能包括计算机可读介质中的非永久性存储器,随机存取存储器(RAM)和/或非易失性内存等形式,如只读存储器(ROM)或闪存(flashRAM)。内存是计算机可读介质的示例。

[0170] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括,但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带,磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质,可用于存储可以被计算设备访问的信息。按照本文中的界定,计算机可读介质不包括暂存电脑可读媒体(transitory media),如调制的数据信号和载波。

[0171] 还需要说明的是,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、商品或者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、商品或者设备所固有的要素。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、商品或者设备中还存在另外的相同要素。

[0172] 本领域技术人员应明白,本申请的实施例可提供为方法、系统或计算机程序产品。因此,本申请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。

[0173] 以上所述仅为本申请的实施例而已,并不用于限制本申请。对于本领域技术人员来说,本申请可以有各种更改和变化。凡在本申请的精神和原理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权利要求范围之内。

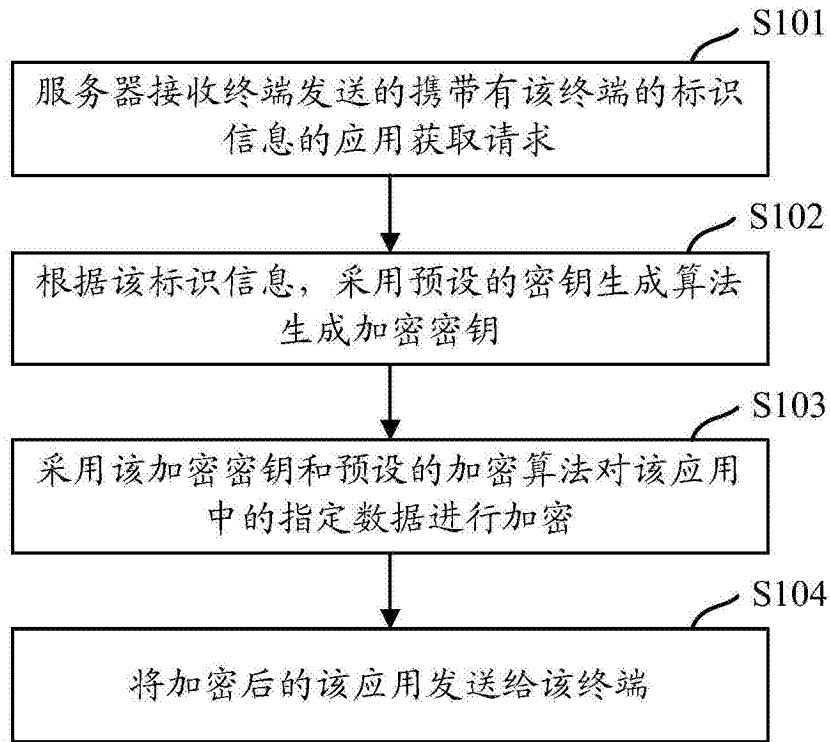


图 1

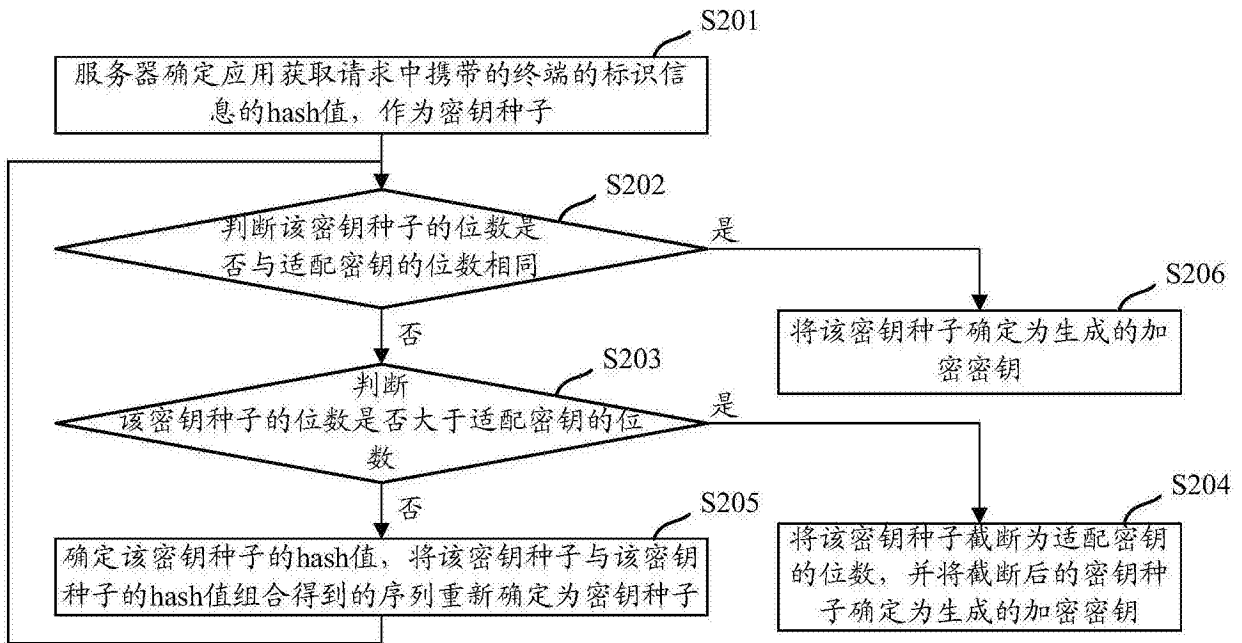


图 2

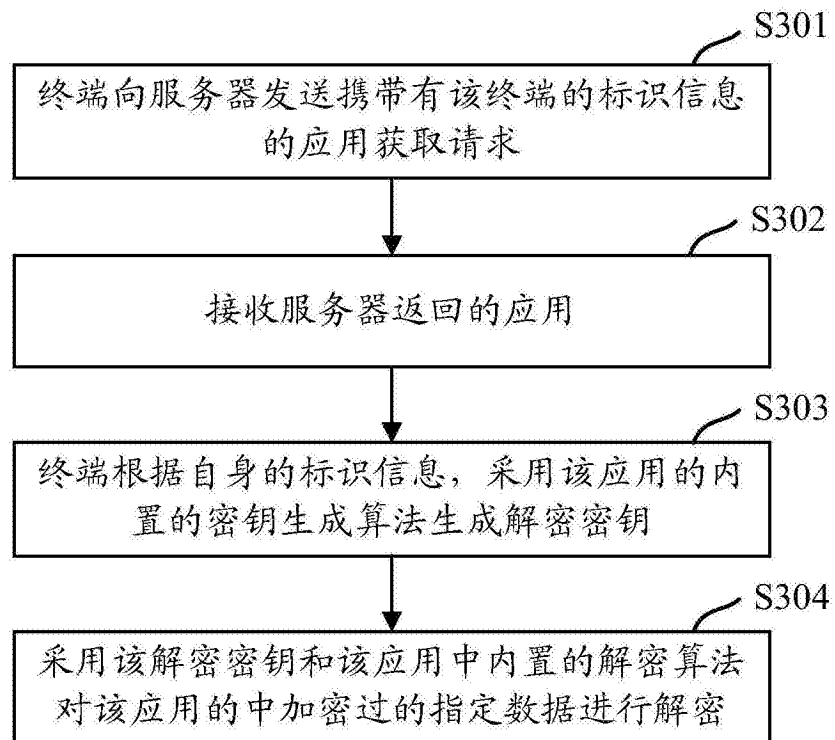


图 3

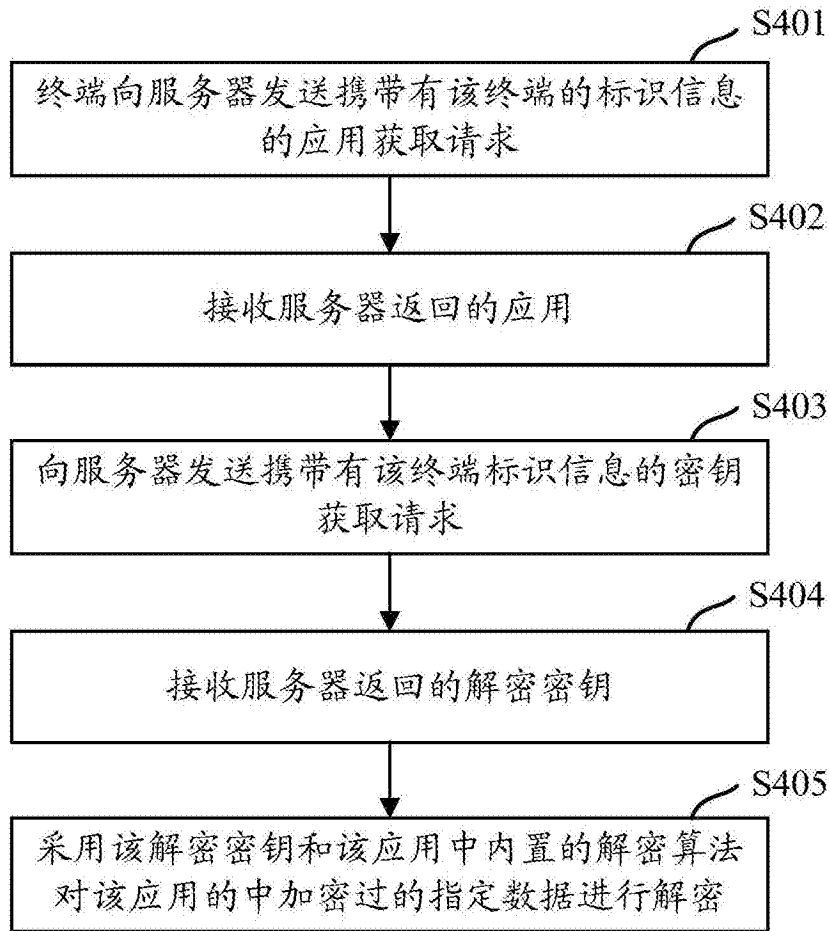


图 4

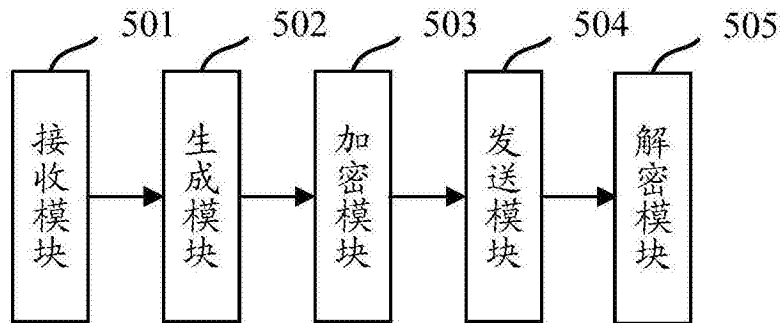


图 5

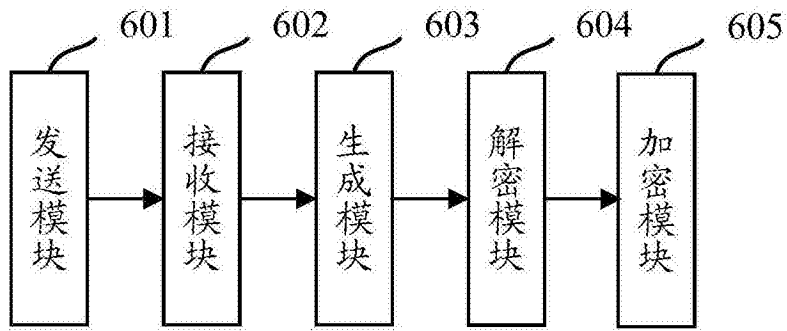


图 6

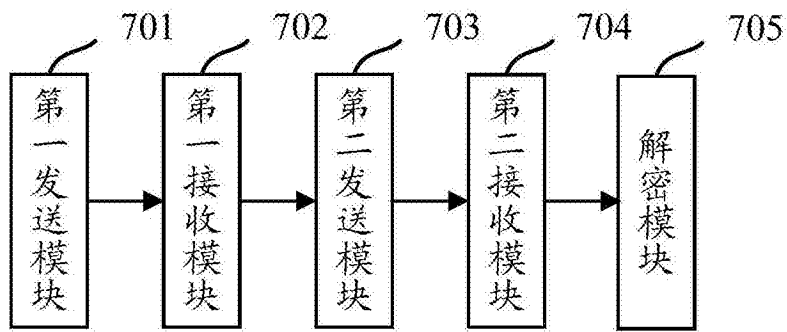


图 7