(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 101924607 A
(43)申请公布日 2010.12.22

(21)申请号 201010268847.X

(22)申请日 2010.08.27

(71)申请人 华为终端有限公司
地址 518129 广东省深圳市龙岗区坂田华为基地 B 区 2 号楼

(72)发明人 李翔宇 雷鹏 钟鸣 贾志峰

(74)专利代理机构 北京同立钧成知识产权代理有限公司 11205
代理人 刘芳

(51)Int.Cl.
H04L 1/00(2006.01)
H04W 8/24(2009.01)
H04W 12/04(2009.01)

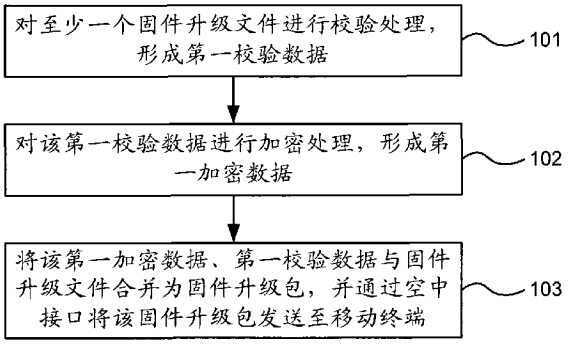
权利要求书 4 页 说明书 10 页 附图 5 页

(54)发明名称

基于固件空中传输技术的固件处理方法、装置及系统

(57)摘要

本发明实施例提供一种基于固件空中传输技术的固件处理方法、装置及系统。该方法包括：对至少一个固件升级文件进行校验处理，形成第一校验数据；对所述第一校验数据进行加密处理，形成第一加密数据；将所述第一加密数据、所述第一校验数据与所述固件升级文件合并为固升级包，并通过空中接口将所述固件升级包发送至移动终端。该装置包括：校验模块、加密模块和处理模块。该系统包括：服务器和移动终端。本发明实施例通过对固件升级文件进行校验、加密及合并处理，解决了现有技术中移动终端易受非法代码入侵的缺陷，能够快速实现多固件升级，并提升了移动终端的安全性。



CN 101924607 A

1. 一种基于固件空中传输技术的固件处理方法，其特征在于，包括：

对至少一个固件升级文件进行校验处理，形成第一校验数据；

对所述第一校验数据进行加密处理，形成第一加密数据；

将所述第一加密数据、所述第一校验数据与所述固件升级文件合并为固件升级包，并通过空中接口将所述固件升级包发送至移动终端。

2. 根据权利要求 1 所述的基于固件空中传输技术的固件处理方法，其特征在于，所述对至少一个固件升级文件进行校验处理，形成第一校验数据，包括：

对所述至少一个固件升级文件进行循环冗余校验处理，形成循环冗余校验数据作为所述第一校验数据；或者，

对所述至少一个固件升级文件进行 MD5 处理，形成 MD5 信息校验数据作为所述第一校验数据。

3. 根据权利要求 1 或 2 所述的基于固件空中传输技术的固件处理方法，其特征在于，所述对所述第一校验数据进行加密处理，形成第一加密数据，包括：

对所述第一校验数据进行私钥加密，将加密后的数据作为所述第一加密数据。

4. 根据权利要求 2 所述的基于固件空中传输技术的固件处理方法，其特征在于，当所述第一校验数据是循环冗余校验数据时，所述对所述第一校验数据进行加密处理，形成第一加密数据，包括：

对所述循环冗余校验数据和所述固件升级文件进行私钥加密，形成加密后的数据，所述加密后的数据包括加密后的循环冗余校验数据和加密后的固件升级文件；其中，所述加密后的循环冗余校验数据为所述第一加密数据，所述固件升级包中包括的固件升级文件为所述加密后的固件升级文件；或者，

对所述循环冗余校验数据进行 MD5 处理，形成循环冗余校验数据对应的 MD5 信息，并对所述对应的 MD5 信息进行私钥加密，形成所述第一加密数据。

5. 根据权利要求 1 所述的基于固件空中传输技术的固件处理方法，其特征在于，在所述对至少一个固件升级文件进行校验处理之前，还包括：

获取多个固件升级文件；其中，所述固件升级包中包括所述多个固件升级文件。

6. 一种基于固件空中传输技术的固件升级方法，其特征在于，包括：

通过空中接口接收服务器发送的固件升级包，并存储所述固件升级包至缓存分区；

对存储于所述缓存分区的所述固件升级包进行读取；其中，所述固件升级包中包括：第一加密数据、第一校验数据和固件升级文件；

对所述固件升级包中的第一加密数据进行解密，形成第二校验数据；

当所述第二校验数据和第一校验数据相一致时，根据所述固件升级包中的固件升级文件对相应的固件进行升级操作。

7. 根据权利要求 6 所述的基于固件空中传输技术的固件升级方法，其特征在于，所述对存储于所述缓存分区的所述固件升级包进行读取，包括：

遍历所述缓存分区，获取与所述固件升级包相对应的文件头；

从与所述固件升级包相对应的文件头中选取一个有效的文件头作为目标文件头；

根据所述目标文件头中的标识，读取与所述标识对应的数据包，并将所述数据包组成所述固件升级包。

8. 根据权利要求 7 所述的基于固件空中传输技术的固件升级方法，其特征在于，所述从与所述固件升级包相对应的文件头中选取一个有效的文件头作为目标文件头，包括：

在与所述固件升级包相对应的有效的文件头中选取块编号最大的文件头作为所述目标文件头，当存在多个块编号相等的文件头时，从所述多个块编号相等的文件头中选取闪存地址最大的文件头作为所述目标文件头。

9. 根据权利要求 6 所述的基于固件空中传输技术的固件升级方法，其特征在于，所述对所述固件升级包中的第一加密数据进行解密，形成第二校验数据，包括：

对所述固件升级包中的所述第一加密数据进行公钥解密，将解密后的数据作为第二校验数据。

10. 根据权利要求 9 所述的基于固件空中传输技术的固件升级方法，其特征在于，在所述对所述固件升级包中的第一加密数据进行解密，形成第二校验数据之后，还包括：

判断所述第二校验数据和第一校验数据是否一致；

所述判断所述第二校验数据和第一校验数据是否一致，包括：

当所述第一校验数据是循环冗余校验数据，并且所述第一加密数据是对所述循环冗余校验数据进行私钥加密的数据时，直接比较所述第二校验数据和第一校验数据是否相同；或者

当所述第一校验数据是 MD5 信息校验数据，并且所述第一加密数据是对所述 MD5 信息校验数据进行私钥加密的数据时，直接比较所述第二校验数据和第一校验数据是否相同；或者

当所述第一校验数据是循环冗余校验数据，并且所述第一加密数据是对所述循环冗余校验数据对应的 MD5 信息进行私钥加密的数据时，对所述固件升级包中的所述循环冗余校验数据进行 MD5 处理，形成第二 MD5 信息，并验证所述第二校验数据与所述第二 MD5 信息是否一致；其中，第二校验数据为所述固件升级包中的所述第一加密数据解密后形成的 MD5 信息。

11. 根据权利要求 6 至 10 中任一所述的基于固件空中传输技术的固件升级方法，其特征在于，在所述根据所述固件升级包中的固件升级文件对相应的固件进行升级操作之前，还包括：

对所述固件升级文件进行校验处理，形成第三校验数据；

验证所述第三校验数据与所述固件升级包中的第一校验数据是否一致；

如果一致，则根据所述固件升级包中的固件升级文件对相应的固件进行升级操作；否则，不对该固件升级文件对相应的固件进行升级操作，并丢弃所述固件升级文件。

12. 一种服务器，其特征在于，包括：

校验模块，用于对至少一个固件升级文件进行校验处理，形成第一校验数据；

加密模块，对所述校验模块形成的所述第一校验数据进行加密处理，形成第一加密数据；

处理模块，用于将所述第一加密数据、所述第一校验数据与所述固件升级文件合并为固件升级包，并通过空中接口将所述固件升级包发送至移动终端。

13. 根据权利要求 12 所述的服务器，其特征在于，所述校验模块包括：

循环冗余校验单元，用于对所述至少一个固件升级文件进行循环冗余校验处理，形成

循环冗余校验数据作为所述第一校验数据；和 / 或

MD5 单元，用于对所述至少一个固件升级文件进行 MD5 处理，形成 MD5 信息校验数据作为所述第一校验数据。

14. 根据权利要求 12 或 13 所述的服务器，其特征在于，所述加密模块包括：

第一加密单元，用于对所述第一校验数据进行私钥加密，将加密后的数据作为所述第一加密数据。

15. 根据权利要求 13 所述的服务器，其特征在于，所述加密模块包括：

第二加密单元，用于当所述第一校验数据是循环冗余校验数据时，对所述循环冗余校验数据和所述固件升级文件进行私钥加密，形成加密后的数据，该加密后的数据包括加密后的循环冗余校验数据和加密后的固件升级文件；其中，所述加密后的循环冗余校验数据为所述第一加密数据，所述固件升级包中包括的固件升级文件为所述加密后的固件升级文件；和 / 或

第三加密单元，用于当所述第一校验数据是循环冗余校验数据时，对所述循环冗余校验数据进行 MD5 处理，形成循环冗余校验数据对应的 MD5 信息，并对该对应的 MD5 信息进行私钥加密，形成所述第一加密数据。

16. 根据权利要求 12 所述的服务器，其特征在于，还包括：

获取模块，用于在所述校验模块对至少一个固件升级文件进行校验处理之前，获取多个固件升级文件；其中，所述固件升级包中包括所述多个固件升级文件。

17. 一种移动终端，其特征在于，包括：

接收模块，用于通过空中接口接收服务器发送的固件升级包，并存储所述固件升级包至缓存分区；

读取模块，用于对存储于所述缓存分区的所述固件升级包进行读取；其中，所述固件升级包中包括：第一加密数据、第一校验数据和固件升级文件；

解密模块，用于对所述读取模块读取的所述固件升级包中的第一加密数据进行解密，形成第二校验数据；

升级模块，用于当所述第二校验数据和第一校验数据相一致时，根据所述固件升级包中的固件升级文件对相应的固件进行升级操作。

18. 根据权利要求 17 所述的移动终端，其特征在于，所述读取模块包括：

遍历单元，用于遍历所述缓存分区，获取与所述固件升级包相对应的文件头；

选取单元，用于从与所述固件升级包相对应的文件头中选取一个有效的文件头作为目标文件头；

读取单元，用于根据所述选取单元选取的所述目标文件头中的标识，读取与所述标识对应的数据包，并将所述数据包组成所述固件升级包。

19. 根据权利要求 18 所述的移动终端，其特征在于，所述选取单元包括：

第一选取子单元，用于在与所述固件升级包相对应的有效的文件头中选取块编号最大的文件头作为所述目标文件头；

第二选取子单元，用于当存在多个块编号相等的文件头时，从所述多个块编号相等的文件头中选取闪存地址最大的文件头作为所述目标文件头。

20. 根据权利要求 17 所述的移动终端，其特征在于，所述解密模块具体用于对所述固

件升级包中的所述第一加密数据进行公钥解密，将解密后的数据作为第二校验数据。

21. 根据权利要求 20 所述的移动终端，其特征在于，还包括：

判断模块，用于在所述解密模块对所述固件升级包中的第一加密数据进行解密，形成第二校验数据之后，判断所述第二校验数据和第一校验数据是否一致；

所述判断模块包括：

第一比较单元，用于当所述第一校验数据是循环冗余校验数据，并且所述第一加密数据是对所述循环冗余校验数据进行私钥加密的数据时，直接比较所述第二校验数据和第一校验数据是否相同；

第二比较单元，用于当所述第一校验数据是 MD5 信息校验数据，并且所述第一加密数据是对所述 MD5 信息校验数据进行私钥加密的数据时，直接比较所述第二校验数据和第一校验数据是否相同；或

第三比较单元，用于当所述第一校验数据是循环冗余校验数据，并且所述第一加密数据是对所述循环冗余校验数据对应的 MD5 信息进行私钥加密的数据时，对所述固件升级包中的所述循环冗余校验数据进行 MD5 处理，形成第二 MD5 信息，并验证所述第二校验数据与所述第二 MD5 信息是否一致；其中，第二校验数据为所述固件升级包中的所述第一加密数据解密后形成的 MD5 信息。

22. 根据权利要求 17 至 21 中任一所述的移动终端，其特征在于，还包括：

校验模块，用于在所述升级模块根据所述固件升级包中的固件升级文件对相应的固件进行升级操作之前，对所述固件升级文件进行校验处理，形成第三校验数据；

验证模块，用于验证所述第三校验数据与所述固件升级包中的第一校验数据是否一致；

所述升级模块用于如果所述第三校验数据与所述第一校验数据一致，则根据所述固件升级包中的固件升级文件对相应的固件进行升级操作；否则，不对所述固件升级文件对相应的固件进行升级操作，并丢弃所述固件升级文件。

23. 一种基于固件空中传输技术的固件升级系统，其特征在于，包括：如权利要求 12 至 16 中任一所述的服务器，以及如权利要求 17 至 22 中任一所述的移动终端。

基于固件空中传输技术的固件处理方法、装置及系统

技术领域

[0001] 本发明实施例涉及无线通信技术领域，尤其涉及一种基于固件空中传输(Firmware Over The Air；以下简称：FOTA)技术的固件处理方法、装置及系统。

背景技术

[0002] 随着技术的发展，诸如手机等移动终端的功能越来越强大，移动终端中的软件（称为：固件）也越来越庞大。一旦移动终端推向市场而又需要对其固件进行升级时，由于用户分布面广，传统的升级方法，如制造商召回移动终端进行升级或移动终端通过互联网进行升级，几乎不可行。

[0003] 因此，利用FOTA技术，对移动终端固件升级的技术得到了应用。FOTA是利用移动终端的空中接口把升级的数据包发送给移动终端，由移动终端自行完成代码和文件系统等固件的升级。由于操作简单，可由用户自行完成，FOTA升级方法正越来越受到运营商的青睐。

[0004] 现有的FOTA升级的一般方法是，通过一定的算法，计算出某一个固件升级前后两个版本的升级包，然后通过移动终端的空中接口把该升级包下载到用户的移动终端，启动移动终端中的FOTA升级流程，完成固件的升级，并重启移动终端以启动升级后的固件。

[0005] 在实现本发明过程中，发明人发现现有技术中至少存在如下问题：固件升级的升级包通过空中接口直接传输至移动终端，给移动终端带来受非法代码入侵的威胁。

发明内容

[0006] 本发明实施例提供一种基于固件空中传输技术的固件处理方法、装置及系统，用以解决现有技术中移动终端易受非法代码入侵的缺陷，快速实现多固件升级，并提升移动终端的安全性。

[0007] 本发明实施例提供一种基于固件空中传输技术的固件处理方法，包括：

[0008] 对至少一个固件升级文件进行校验处理，形成第一校验数据；

[0009] 对所述第一校验数据进行加密处理，形成第一加密数据；

[0010] 将所述第一加密数据、所述第一校验数据与所述固件升级文件合并为固件升级包，并通过空中接口将所述固件升级包发送至移动终端。

[0011] 本发明实施例还提供一种基于固件空中传输技术的固件升级方法，包括：

[0012] 通过空中接口接收服务器发送的固件升级包，并存储所述固件升级包至缓存分区；

[0013] 对存储于所述缓存分区的所述固件升级包进行读取；其中，所述固件升级包中包括：第一加密数据、第一校验数据和固件升级文件；

[0014] 对所述固件升级包中的第一加密数据进行解密，形成第二校验数据；

[0015] 当所述第二校验数据和第一校验数据相一致时，根据所述固件升级包中的固件升级文件对相应的固件进行升级操作。

[0016] 本发明提供一种服务器，包括：

[0017] 校验模块，用于对至少一个固件升级文件进行校验处理，形成第一校验数据；

[0018] 加密模块，对所述校验模块形成的所述第一校验数据进行加密处理，形成第一加密数据；

[0019] 处理模块，用于将所述第一加密数据、所述第一校验数据与所述固件升级文件合并为固件升级包，并通过空中接口将所述固件升级包发送至移动终端。

[0020] 本发明还提供一种移动终端，包括：

[0021] 接收模块，用于通过空中接口接收服务器发送的固件升级包，并存储所述固件升级包至缓存分区；

[0022] 读取模块，用于对存储于所述缓存分区的所述固件升级包进行读取；其中，所述固件升级包中包括：第一加密数据、第一校验数据和固件升级文件；

[0023] 解密模块，用于对所述读取模块读取的所述固件升级包中的第一加密数据进行解密，形成第二校验数据；

[0024] 升级模块，用于当所述第二校验数据和第一校验数据相一致时，根据所述固件升级包中的固件升级文件对相应的固件进行升级操作。

[0025] 本发明实施例还提供一种基于固件空中传输技术的固件升级系统，包括：上述服务器和移动终端。

[0026] 本发明实施例的基于固件空中传输技术的固件处理方法、装置及系统，通过对固件升级文件进行校验、加密及合并处理，解决了现有技术中移动终端易受非法代码入侵的缺陷，能够快速实现多固件升级，并提升了移动终端的安全性。

附图说明

[0027] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作一简单地介绍，显而易见地，下面描述中的附图是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0028] 图 1 为本发明基于固件空中传输技术的固件处理方法一实施例的流程图；

[0029] 图 2 为本发明基于固件空中传输技术的固件升级方法一实施例的流程图；

[0030] 图 3 为本发明基于固件空中传输技术的固件升级方法另一实施例的流程图；

[0031] 图 4 为本发明服务器一实施例的结构示意图；

[0032] 图 5 为本发明服务器另一实施例的结构示意图；

[0033] 图 6 为本发明移动终端一实施例的结构示意图；

[0034] 图 7 为本发明移动终端另一实施例的结构示意图；

[0035] 图 8 为本发明基于固件空中传输技术的固件升级系统一实施例的系统框图。

具体实施方式

[0036] 为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明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发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，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，都属于本发明保护的范围。

[0037] 图 1 为本发明基于固件空中传输技术的固件处理方法一实施例的流程图。如图 1 所示，本发明实施例提供了一种基于固件空中传输技术的固件处理方法，包括：

[0038] 步骤 101、对至少一个固件升级文件进行校验处理，形成第一校验数据；

[0039] 步骤 102、对该第一校验数据进行加密处理，形成第一加密数据；

[0040] 步骤 103、将该第一加密数据、第一校验数据与固件升级文件合并为固件升级包，并通过空中接口将该固件升级包发送至移动终端。

[0041] 在本发明实施例中，上述步骤可以由服务器执行。移动终端中可能包含多个待升级的固件，如二进制文件、文件系统、升级执行脚本等。在服务器侧，首先对至少一个待升级固件的固件升级文件进行校验处理，形成第一校验数据；然后，对该第一校验数据进行加密处理，形成第一加密数据；最后，将所形成的第一加密数据、第一校验数据与固件升级文件合并为一个固件升级包，并把该固件升级包通过空中接口发送至待升级固件的移动终端，以使得该移动终端根据接收到的固件升级包进行固件升级。

[0042] 本发明实施例的基于固件空中传输技术的固件处理方法，通过对固件升级文件进行校验、加密及合并处理，形成固件升级包，并在移动终端中根据该固件升级包进行固件升级，解决了现有技术中移动终端易受非法代码入侵的缺陷，能够快速实现多固件升级，并提升了移动终端的安全性。

[0043] 在上述方法实施例的基础上，步骤 101 可以包括：

[0044] a1、对至少一个固件升级文件进行循环冗余校验 (Cyclic Redundancy Check；以下简称：CRC) 处理，形成 CRC 数据作为第一校验数据；或者

[0045] a2、对至少一个固件升级文件进行信息 - 摘要算法 5(Message-Digest Algorithm 5；以下简称：5MD5) 处理，形成 MD5 信息校验数据作为第一校验数据。

[0046] 服务器在对固件升级文件进行校验处理时，可以采取 CRC 方法，也可以采用 MD5 方法。采用 CRC 方法形成的校验数据的长度随着固件升级文件的长度的增加而成比例增加，采用 MD5 方法形成的校验数据的长度是固定的。在后续加密过程中，加密的数据越少效率越高，因此采用 MD5 方法进行校验处理是一个较佳的方案。

[0047] 在上述技术方案的基础上，步骤 102 可以包括：

[0048] b1、对该第一校验数据进行私钥加密，将加密后的数据作为第一加密数据。

[0049] 服务器可以利用内部存储的私钥对第一加密数据进行加密处理，该私钥与移动终端出厂时内置的公钥相匹配。

[0050] 进一步地，当上述第一校验数据是 CRC 数据，即采取 CRC 方法对固件升级文件进行处理时，步骤 102 可以包括：

[0051] b2、对该 CRC 数据和固件升级文件进行私钥加密，形成加密后的数据，该加密后的数据包括加密后的 CRC 数据和加密后的固件升级文件；其中，加密后的 CRC 数据为第一加密数据，此时，固件升级包中包括的固件升级文件为加密后的固件升级文件；或者

[0052] b3、对该 CRC 数据进行 MD5 处理，形成 CRC 数据对应的 MD5 信息，并对该对应的 MD5 信息进行私钥加密，形成第一加密数据。

[0053] 同时，当上述第一校验数据时 MD5 信息校验数据，即采用 MD5 方法对固件升级文件进行处理时，也可以先对该 MD5 信息校验数据进行 CRC 处理，形成 CRC 数据，再对该 CRC 数

据进行私钥加密，形成第一加密数据。

[0054] 也就是说，在对固件升级文件进行校验和加密处理的阶段，在进行私钥加密的步骤之前，可以对固件升级文件进行 CRC 处理或 MD5 处理或者二者的结合，并且不限定二者的先后顺序。

[0055] 另外，在上述步骤 101 之前，本发明实施例提供的基于固件空中传输技术的固件处理方法还可以包括：

[0056] c1、获取多个固件升级文件，此时，固件升级包中包括获取的多个固件升级文件。

[0057] 服务器可以根据表 1 中的顺序形成固件升级包。

[0058] 表 1

[0059]

名称	说明
第一加密数据	CRC 数据经过 MD5 处理，再经过下载代码私钥(KEY_A)加密后的 128byte 数据
CRC 数据	以下各个固件升级文件的 CRC 值列表，各个固件升级文件按照在固件升级包中的顺序，依次按照 CRC_LENGTH(32K Bytes)分段，做 CRC16 处理，每段的 CRC 值(2byte)依次排列，得到 CRC 数据。每个固件升级文件最后一段做 CRC 处理的长度如果不足 CRC_LENGTH，则按照实际长度做 CRC 处理
MOD1	固件升级文件一内容
MOD2	固件升级文件二内容
……	……

[0060] 图 2 为本发明基于固件空中传输技术的固件升级方法一实施例的流程图。如图 2 所示，本发明实施例提供了一种基于固件空中传输技术的固件升级方法，包括：

[0061] 步骤 201、通过空中接口接收服务器发送的固件升级包，并存储该固件升级包至缓存分区；

[0062] 步骤 202、对存储于缓存分区的固件升级包进行读取；其中，固件升级包包括：第一加密数据、第一校验数据和固件升级文件；

[0063] 步骤 203、对固件升级包中的第一加密数据进行解密，形成第二校验数据；

[0064] 步骤 204、当第二校验数据和第一校验数据相一致时，根据固件升级包中的固件升级文件对相应的固件进行升级操作。

[0065] 在本发明实施例中，上述步骤可以由移动终端执行。移动终端中可能包含多个待升级的固件，如二进制文件、文件系统、升级执行脚本等。在服务器侧对至少一个待升级固件的固件升级文件进行操作，并将形成的固件升级包通过空中接口发送至待升级固件的移动终端后，该移动终端将接收到的固件升级包存储于缓存 (CACHE) 分区。移动终端读取缓存分区中的固件升级包，该固件升级包中包括：第一加密数据、第一校验数据和固件升级文件，并对该固件升级包中的第一加密数据进行解密，形成第二校验数据，当第二校验数据与

第一校验数据一致时，根据该固件升级包中的固件升级文件对相应的固件进行升级操作。

[0066] 本发明实施例的基于固件空中传输技术的固件升级方法，移动终端接收到服务器对固件升级文件进行校验、加密及合并处理而形成的固件升级包后，对该固件升级包进行相应的解密操作，以进行固件升级，解决了现有技术中移动终端易受非法代码入侵的缺陷，能够快速实现多固件升级，并提升了移动终端的安全性。

[0067] 图 3 为本发明基于固件空中传输技术的固件升级方法另一实施例的流程图。如图 3 所示，在上述图 2 所示实施例的基础上，本发明还提出一种基于固件空中传输技术的固件升级方法，包括：

[0068] 步骤 301、通过空中接口接收服务器发送的固件升级包，并存储该固件升级包至缓存分区；

[0069] 步骤 302、遍历缓存分区，获取与固件升级包相对应的文件头；

[0070] 步骤 303、从与固件升级包相对应的文件头中选取一个有效的文件头作为目标文件头；

[0071] 在 CACHE 分区中，若存储某个文件，假设其标识 (ID) 为 ID_a，则需要在 CACHE 分区中写入包含 ID_a 的文件头；当更新该文件时，将其对应的文件头置为无效（即，在 CACHE 分区中写入一个文件名为“unlinked”、ID 为 ID_a 的文件头），然后重新写入新的文件头（假设更新后的文件的 ID 为 ID_b，则在 CACHE 分区中写入包含 ID_b 的文件头）。因此，在所有与固件升级包相对应的文件头中，删除与文件名为“unlinked”的文件头的 ID 相同的文件头，则剩余的文件头均为有效的文件头，从有效的文件头中选取一个作为目标文件头；

[0072] 步骤 304、根据目标文件头中的 ID，读取与该 ID 对应的数据包，并将这些数据包按顺序排列以组成固件升级包；

[0073] 步骤 305、对该固件升级包中的第一加密数据进行公钥解密，将解密后的数据作为第二校验数据；

[0074] 步骤 306、判断第二校验数据与第一校验数据是否一致，若一致，则执行步骤 307，否则，执行步骤 310；

[0075] 步骤 307、对固件升级文件进行校验处理，形成第三校验数据；

[0076] 在本发明实施例中，如果固件升级包中的固件升级文件为私钥加密后的固件升级文件，则需首先对其进行公钥解密，然后再进行校验处理；

[0077] 步骤 308、验证第三校验数据与固件升级包中的第一校验数据是否一致，若一致，则执行步骤 309，否则，执行步骤 310；

[0078] 步骤 309、根据固件升级包中的固件升级文件对相应的固件进行升级操作；

[0079] 步骤 310、不对该固件升级文件对相应的固件进行升级操作，并丢弃固件升级文件。

[0080] 在本发明实施例中，上述步骤可以由移动终端执行。在上述图 2 所示的方法实施例的基础上，移动终端接收到的固件升级包存储于 CACHE 分区，可以采用的是 yaffs2 文件系统，而移动终端中用于读取该固件升级包的模块 OEMSBL 不支持 yaffs2 文件系统，因此，OEMSBL 读取缓存分区中的固件升级包的操作可以包括：首先，遍历缓存分区，以获取所有与固件升级包相对应的文件头，如，获取所有符合升级包文件名要求的文件头；然后，在这些文件头中，凡是 ID 与文件名为“unlinked”的文件头的 ID 相同，则删除该文件

头；接着，从剩余的文件头中根据一定规则选取目标文件头，例如，可以在其中选取块编号(blocknum)最大的文件头作为目标文件头，当存在多个块编号相等的文件头时，从多个块编号相等的文件头中选取闪存(Flash)地址最大的文件头作为目标文件头；当选取出目标文件头后，读取与该目标文件头中的标识对应的数据包，并将这些数据包按顺序排列以组成完成的固件升级包。

[0081] 进一步地，上述步骤306可以具体包括：

[0082] d1、当第一校验数据是CRC数据，并且第一加密数据是对CRC数据进行私钥加密的数据时，直接比较第二校验数据和第一校验数据是否相同；或者

[0083] d2、当第一校验数据是MD5信息校验数据，并且第一加密数据是对MD5信息校验数据进行私钥加密的数据时，直接比较第二校验数据和第一校验数据是否相同；或者

[0084] d3、当第一校验数据是CRC数据，并且第一加密数据是对CRC数据对应的MD5信息进行私钥加密的数据时，对固件升级包中的CRC数据进行MD5处理，形成第二MD5信息，并验证第二校验数据与第二MD5信息是否一致；其中，第二校验数据为固件升级包中的第一加密数据解密后形成的MD5信息。

[0085] 移动终端对相应的固件进行升级的操作可以包括：OEMSBL对二进制文件的升级，并设置相关标志；以及移动终端中的另一个模块(RECOVERY)对文件系统的升级和对升级执行脚本的处理。待所有固件升级完成后，重新启动移动终端，即可使用升级后的各固件。

[0086] 本发明实施例的基于固件空中传输技术的固件升级方法，移动终端接收到服务器对固件升级文件进行校验、加密及合并处理而形成的固件升级包后，对该固件升级包进行相应的解密操作，以进行固件升级，解决了现有技术中操作繁琐及移动终端易受非法代码入侵的缺陷，能够快速实现多固件升级，并提升了移动终端的安全性。

[0087] 上述实施例所述的技术方案可以在智能手机中实现，假如该智能手机包含ARM9和ARM11两个CPU，主要包括以下模块和文件系统：OEMSBL、AMSS、EFS、BOOT和SYSTEM。利用本发明实施例的技术方案可以一次完成所有固件的升级，表2为一个典型的固件升级包。

[0088] 表2

[0089]

名称	说明
第一加密数据	CRC数据经过MD5处理，再经过下载代码私钥(KEY_A)加密后的128byte数据
CRC数据	以下各个固件升级文件的CRC值列表，各个固件升级文件按照在固件升级包中的顺序，依次按照CRC_LENGTH(32K Bytes)分段，做CRC16处理，每段的CRC值(2byte)依次排列，得到CRC数据。每个固件升级文件最后一段做CRC处理的长度如果不足CRC_LENGTH,则按照实际长度做CRC处理
SW_VER_LIST	允许升级的SW版本号列表
AMSS_HEAD	AMSS的头文件
FW_DIFF	所有待升级的软件的差分包
AMSS_ECC	AMSS的ECC数据
OEMSBL_HEADER	OEMSBL头文件
OEMSBL	OEMSBL内容
EFS	EFS文件系统
SOFTWARE_VER	当前升级的SW的版本号
FS_DIFF	ANDROID SYSTEM升级的差分包

[0090]

SCRIPT.ZIP	ANDROID RECOVERY 下执行的升级脚本

[0091] 在 OEMSBL 中，完成对 OEMSBL，AMSS，BOOT，EFS 的升级。在 RECOVERY 中完成 SYSTEM 和 SCRIPT.ZIP 的升级处理。整个升级过程手机只需要重启一次。

[0092] 该 FOTA 升级方案，在固件升级包下载过程中，支持断点续传。启动 FOTA 升级后，移动终端，如，手机，重启一次，完成对手机所有待升级固件的升级。升级过程中支持掉电保护，能够兼容 SCRIPT.ZIP 升级执行脚本的处理，具有良好的用户体验。

[0093] 图 4 为本发明服务器一实施例的结构示意图。如图 4 所示，本发明实施例提供了一种服务器，用于为移动终端提供固件升级包，包括：校验模块 41、加密模块 42 和处理模块 43。其中，校验模块 41 用于对至少一个固件升级文件进行校验处理，形成第一校验数据；加密模块 42 用于对校验模块 41 形成的第一校验数据进行加密处理，形成第一加密数据；处理模块 43 用于将第一加密数据、第一校验数据与固件升级文件合并为固件升级包，并通过空中接口将该固件升级包发送至移动终端。

[0094] 在本发明实施例中，移动终端中可能包含多个待升级的固件，如二进制文件、文件系统、升级执行脚本等。本发明实施例提供的服务器，首先对至少一个待升级固件的固件升级文件进行校验处理，形成第一校验数据；然后，对该第一校验数据进行加密处理，形成第一加密数据；最后，将所形成的第一加密数据、第一校验数据与固件升级文件合并为一个固件升级包，并把该固件升级包通过空中接口发送至待升级固件的移动终端，以使得该移动终端根据接收到的固件升级包进行固件升级。

[0095] 本发明实施例的服务器，通过对固件升级文件进行校验、加密及合并处理，形成固件升级包，并在移动终端中根据该固件升级包进行固件升级，解决了现有技术中移动终端易受非法代码入侵的缺陷，能够快速实现多固件升级，并提升了移动终端的安全性。

[0096] 图 5 为本发明服务器另一实施例的结构示意图。如图 5 所示，在上述服务器实施例的基础上，校验模块 41 可以包括 :CRC 单元 51 和 / 或 MD5 单元 52。其中，CRC 单元 51 用于对至少一个固件升级文件进行 CRC 处理，形成 CRC 数据作为第一校验数据 ;MD5 单元 52 用于对至少一个固件升级文件进行 MD5 处理，形成 MD5 信息校验数据作为第一校验数据。

[0097] 校验模块 41 在对固件升级文件进行校验处理时，可以采取 CRC 方法，也可以采用 MD5 方法。采用 CRC 方法形成的校验数据的长度随着固件升级文件的长度的增加而成比例增加，采用 MD5 方法形成的校验数据的长度是固定的。在后续加密过程中，加密的数据越少效率越高，因此采用 MD5 方法进行校验处理是一个较佳的方案。

[0098] 在上述技术方案的基础上，加密模块 42 可以包括 :第一加密单元 53。该第一加密单元 53 可以用于对第一校验数据进行私钥加密，将加密后的数据作为第一加密数据。

[0099] 第一加密单元 53 可以利用服务器内部存储的私钥对第一加密数据进行加密处理，该私钥与移动终端出厂时内置的公钥相匹配。

[0100] 进一步地，加密模块 42 可以包括 :第二加密单元 54 和 / 或第三加密单元 55。其中，第二加密单元 54 用于当第一校验数据是 CRC 数据时，对该 CRC 数据和固件升级文件进行私钥加密，形成加密后的数据，该加密后的数据包括加密后的 CRC 数据和加密后的固件升级文件 ;其中，加密后的 CRC 数据为第一加密数据，固件升级包中包括的固件升级文件为加密后的固件升级文件 ;第三加密单元 55 用于当第一校验数据是 CRC 数据时，对该 CRC 数据进行 MD5 处理，形成 CRC 数据对应的 MD5 信息，并对该对应的 MD5 信息进行私钥加密，形成第一加密数据。

[0101] 另外，本发明实施例所提供的移动终端，还可以进一步包括 :获取模块 56，该获取模块 56 在校验模块 41 对至少一个固件升级文件进行校验处理之前，获取多个固件升级文件 ;其中，固件升级包中包括上述多个固件升级文件。

[0102] 本发明实施例的服务器，通过对固件升级文件进行校验、加密及合并处理，形成固件升级包，并在移动终端中根据该固件升级包进行固件升级，解决了现有技术中操作繁琐及移动终端易受非法代码入侵的缺陷，能够快速实现多固件升级，并提升了移动终端的安全性。

[0103] 图 6 为本发明移动终端一实施例的结构示意图。如图 6 所示，本发明实施例提供了一种具有升级固件功能的移动终端，包括 :接收模块 61、读取模块 62、解密模块 63 和升级模块 64。其中，接收模块 61 用于通过空中接口接收服务器发送的固件升级包，并存储该固件升级包至缓存分区 65 ;读取模块 62 用于对存储于缓存分区 65 的该固件升级包进行读取，其中，固件升级包中包括 :第一加密数据、第一校验数据和固件升级文件 ;解密模块 63 用于对读取模块 62 读取的固件升级包中的第一加密数据进行解密，形成第二校验数据 ;升级模块 64 用于当第二校验数据和第一校验数据相一致时，根据固件升级包中的固件升级文件对相应的固件进行升级操作。

[0104] 在本发明实施例中，移动终端中可能包含多个待升级的固件，如二进制文件、文件系统、升级执行脚本等。在服务器侧对至少一个待升级固件的固件升级文件进行操作，并将

形成的固件升级包通过空中接口发送至待升级固件的移动终端后，该移动终端中的接收模块 61 将接收到的固件升级包存储于缓存 (CACHE) 分区 65。进一步地，读取模块 62 读取缓存分区 65 中的固件升级包，该固件升级包中包括：第一加密数据、第一校验数据和固件升级文件，解密模块 63 对该固件升级包中的第一加密数据进行解密，形成第二校验数据，当第二校验数据与第一校验数据一致时，升级模块 64 根据该固件升级包中的固件升级文件对相应的固件进行升级操作。

[0105] 本发明实施例的移动终端，接收模块接收到服务器对固件升级文件进行校验、加密及合并处理而形成的固件升级包后，校验模块对该固件升级包进行相应的解密操作，以进行固件升级，解决了现有技术中移动终端易受非法代码入侵的缺陷，能够快速实现多固件升级，并提升了移动终端的安全性。

[0106] 图 7 为本发明移动终端另一实施例的结构示意图。如图 7 所示，在上述移动终端实施例的基础上，读取模块 62 可以包括：遍历单元 71、选取单元 72 和读取单元 73。其中，遍历单元 71 用于遍历缓存分区 65，获取与固件升级包相对应的文件头；选取单元 72 用于从与固件升级包相对应的文件头中选取一个有效的目标文件头；读取单元 73 用于根据选取单元 72 选取的目标文件头中的标识，读取与该标识对应的数据包，并将这些数据包按顺序排列以组成固件升级包。

[0107] 在 CACHE 分区 65 中，若存储某个文件，假设其标识 (ID) 为 ID_a，则需要在 CACHE 分区中写入包含 ID_a 的文件头；当更新该文件时，将其对应的文件头置为无效（即，在 CACHE 分区中写入一个文件名为“unlinked”、ID 为 ID_a 的文件头），然后重新写入新的文件头（假设更新后的文件的 ID 为 ID_b，则在 CACHE 分区中写入包含 ID_b 的文件头）。因此，选取单元 72 在所有与固件升级包相对应的文件头中，删除与文件名为“unlinked”的文件头的 ID 相同的文件头，则剩余的文件头均为有效的文件头，从有效的文件头中选取一个作为目标文件头。

[0108] 在本发明实施例中，在上述图 6 所示技术方案的基础上，移动终端接收到的固件升级包存储于 CACHE 分区 65，可以采用的是 yaffs2 文件系统，而移动终端中用于读取该固件升级包的读取模块 62 可以为 OEMSBL，该 OEMSBL 不支持 yaffs2 文件系统，因此，遍历单元 71 遍历缓存分区，以获取所有与固件升级包相对应的文件头，如，获取所有符合升级包文件名要求的文件头；然后，选取单元 72 在这些文件头中，凡是 ID 与文件名为“unlinked”的文件头的 ID 相同，则删除该文件头，从剩余的文件头中根据一定规则选取目标文件头，例如，选取单元 72 可以包括用于在与固件升级包相对应的有效的文件头中选取 blocknum 最大的文件头作为目标文件头的第一选取子单元，和用于当存在多个 blocknum 相等的文件头时，从多个 blocknum 相等的文件头中选取 Flash 地址最大的文件头作为目标文件头的第二选取子单元；当选取出目标文件头后，读取单元 73 读取与该目标文件头中的标识对应的数据包，并将这些数据包按顺序排列以组成固件升级包。

[0109] 进一步地，解密模块 63 具体用于对固件升级包中的第一加密数据进行公钥解密，将解密后的数据作为第二校验数据。

[0110] 更进一步地，本发明实施例所提供的移动终端还可以包括：判断模块 74。该判断模块 74 用于在解密模块 63 对固件升级包中的第一加密数据进行解密，形成第二校验数据之后，判断第二校验数据和第一校验数据是否一致；该判断模块 74 可以包括：第一比较单

元 75、第二比较单元 76 和 / 或第三比较单元 77。其中，第一比较单元 75 用于当第一校验数据是 CRC 数据，并且第一加密数据是对该 CRC 数据进行私钥加密的数据时，直接比较第二校验数据和第一校验数据是否相同；第二比较单元 76 用于当第一校验数据是 MD5 信息校验数据，并且第一加密数据是对该 MD5 信息校验数据进行私钥加密的数据时，直接比较第二校验数据和第一校验数据是否相同；第三比较单元 77 用于当第一校验数据是 CRC 数据，并且第一加密数据是对该 CRC 数据对应的 MD5 信息进行私钥加密的数据时，对固件升级包中的 CRC 数据进行 MD5 处理，形成第二 MD5 信息，并验证第二校验数据与第二 MD5 信息是否一致；其中，第二校验数据为固件升级包中的第一加密数据解密后形成的 MD5 信息。

[0111] 再进一步地，本发明实施例中的移动终端还可以包括：校验模块 78 和验证模块 79。其中，校验模块 78 用于在升级模块 64 根据固件升级包中的固件升级文件对相应的固件进行升级操作之前，对固件升级文件进行校验处理，形成第三校验数据；验证模块 79 用于验证第三校验数据与固件升级包中的第一校验数据是否一致；此时，如果第三校验数据与第一校验数据一致，升级模块 64 用于根据固件升级包中的固件升级文件对相应的固件进行升级操作；否则，不对该固件升级文件对相应的固件进行升级操作，并丢弃该固件升级文件。

[0112] 本发明实施例的移动终端，接收模块接收到服务器对固件升级文件进行校验、加密及合并处理而形成的固件升级包后，校验模块对该固件升级包进行校验处理，并在校验通过后升级模块进行固件升级，解决了现有技术中操作繁琐及移动终端易受非法代码入侵的缺陷，能够快速实现多固件升级，并提升了移动终端的安全性。

[0113] 图 8 为本发明基于固件空中传输技术的固件升级系统一实施例的系统框图。如图 8 所述，本发明实施例提供了一种基于固件空中传输技术的固件升级系统，包括：服务器 81 和移动终端 82。

[0114] 本系统实施例中服务器 81 的功能如上述图 4 或图 5 所示实施例中的具体描述，移动终端 82 的功能如上述图 6 或图 7 所示实施例中的具体描述，在此不再赘述。

[0115] 本发明实施例的基于固件空中传输技术的固件升级系统，移动终端接收到服务器对固件升级文件进行校验、加密及合并处理而形成的固件升级包后，对该固件升级包进行校验处理，并在校验通过后进行固件升级，解决了现有技术中操作繁琐及移动终端易受非法代码入侵的缺陷，能够快速实现多固件升级，并提升了移动终端的安全性。

[0116] 本领域普通技术人员可以理解：实现上述方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成，前述的程序可以存储于一计算机可读取存储介质中，该程序在执行时，执行包括上述方法实施例的步骤；而前述的存储介质包括：ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

[0117] 最后应说明的是：以上实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围。

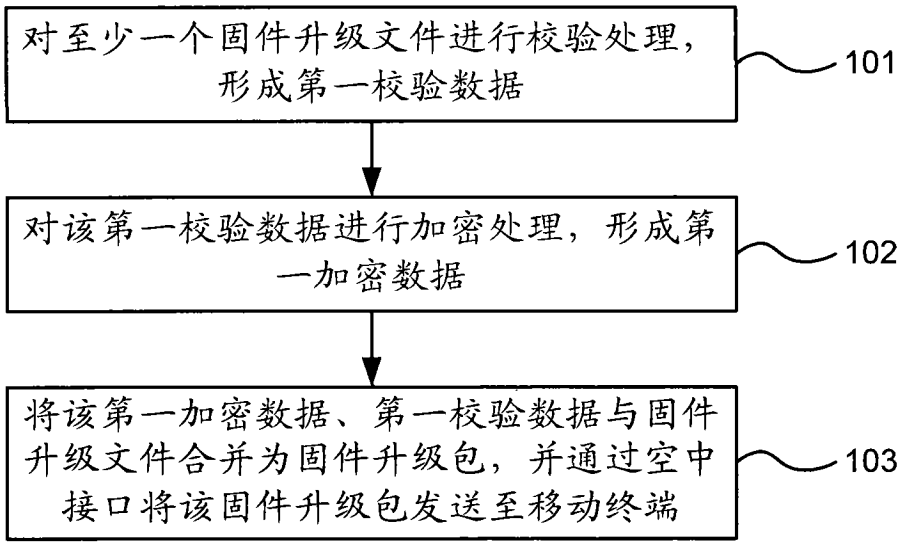

对至少一个固件升级文件进行校验处理，形成第一校验数据
101
对该第一校验数据进行加密处理，形成第一加密数据
102
将该第一加密数据、第一校验数据与固件升级文件合并为固件升级包，并通过空中接口将该固件升级包发送至移动终端
103

图 1

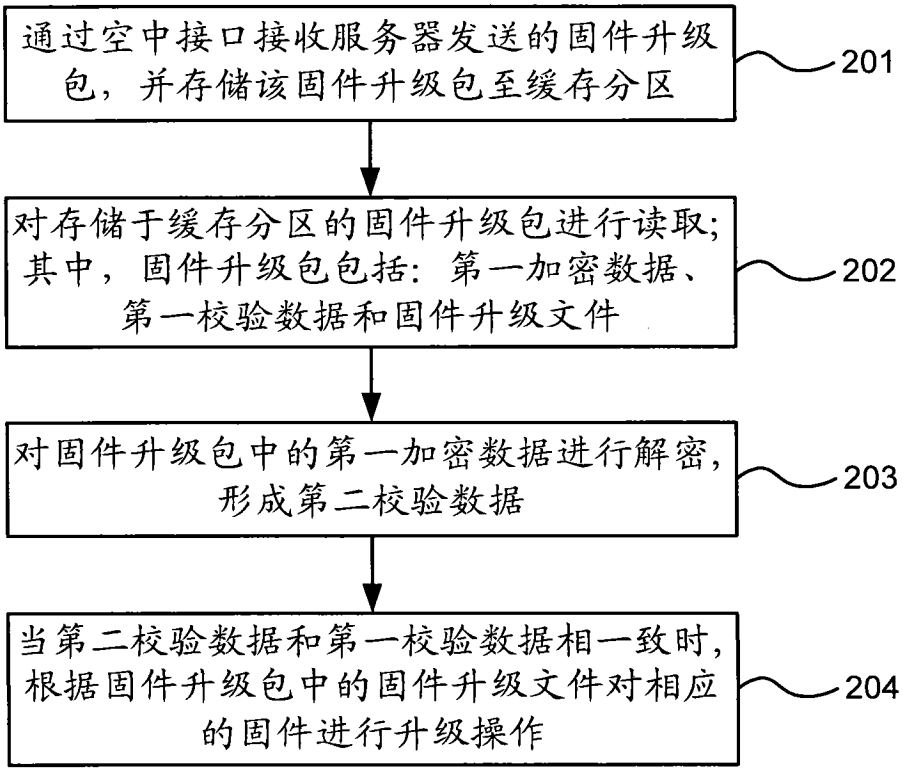

通过空中接口接收服务器发送的固件升级包，并存储该固件升级包至缓存分区
201
对存储于缓存分区的固件升级包进行读取；其中，固件升级包包括：第一加密数据、第一校验数据和固件升级文件
202
对固件升级包中的第一加密数据进行解密，形成第二校验数据
203
当第二校验数据和第一校验数据相一致时，根据固件升级包中的固件升级文件对相应的固件进行升级操作
204

图 2

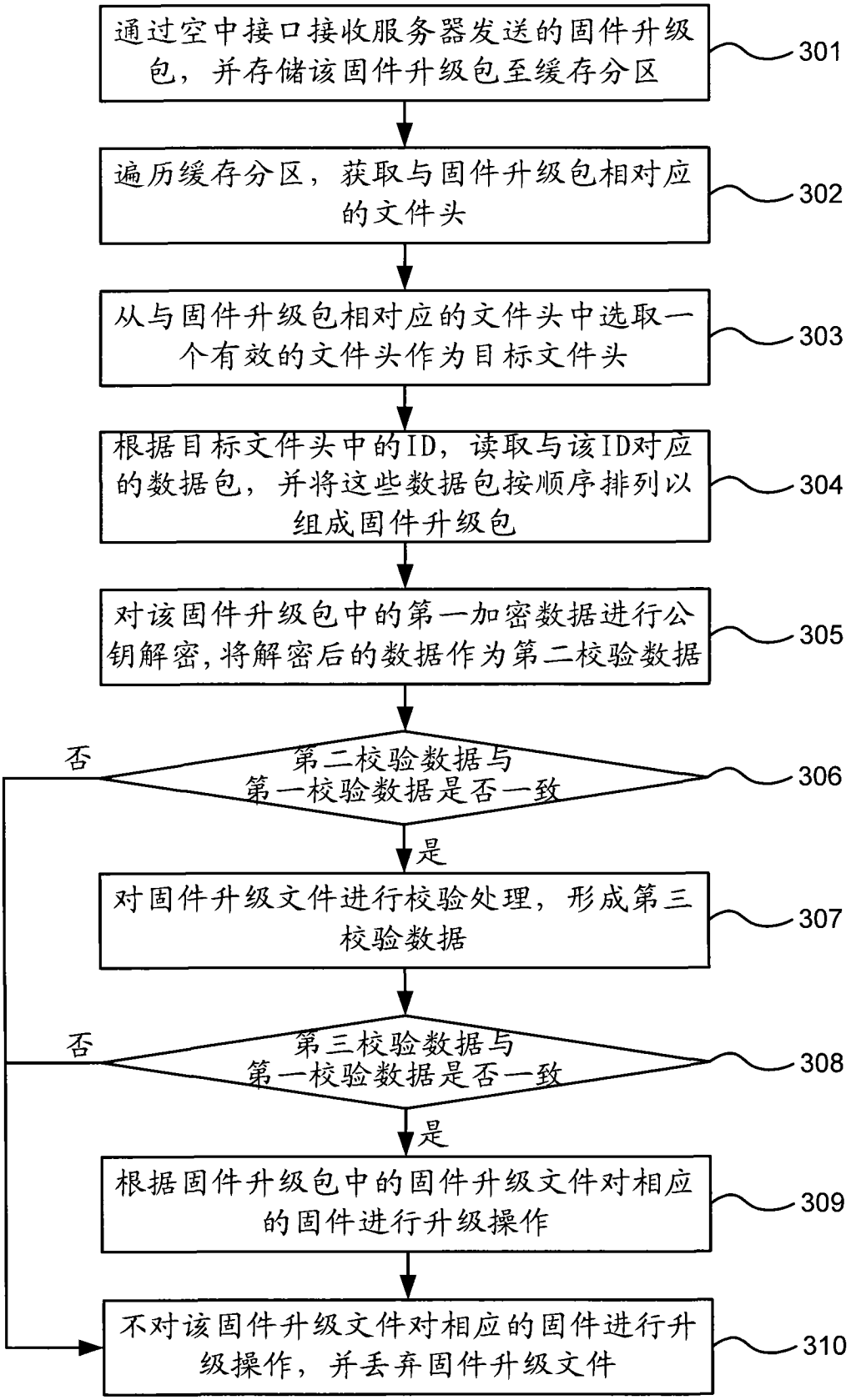

通过空中接口接收服务器发送的固件升级包，并存储该固件升级包至缓存分区
301
遍历缓存分区，获取与固件升级包相对应的文件头
302
从与固件升级包相对应的文件头中选取一个有效的文件头作为目标文件头
303
根据目标文件头中的ID，读取与该ID对应的数据包，并将这些数据包按顺序排列以组成固件升级包
304
对该固件升级包中的第一加密数据进行公钥解密，将解密后的数据作为第二校验数据
305
第二校验数据与第一校验数据是否一致
306
否
是
对固件升级文件进行校验处理，形成第三校验数据
307
第三校验数据与第一校验数据是否一致
308
否
是
根据固件升级包中的固件升级文件对相应的固件进行升级操作
309
不对该固件升级文件对相应的固件进行升级操作，并丢弃固件升级文件
310

图 3

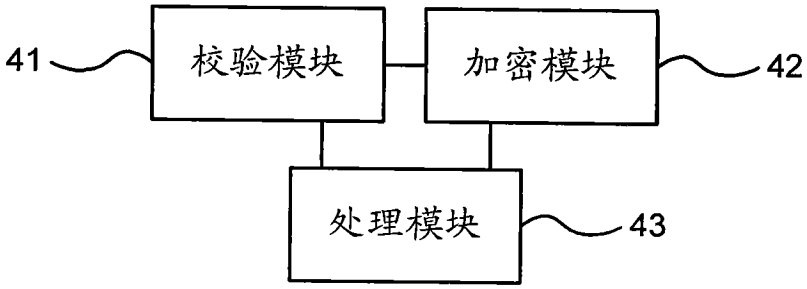

41
校验模块
加密模块
42
处理模块
43

图 4

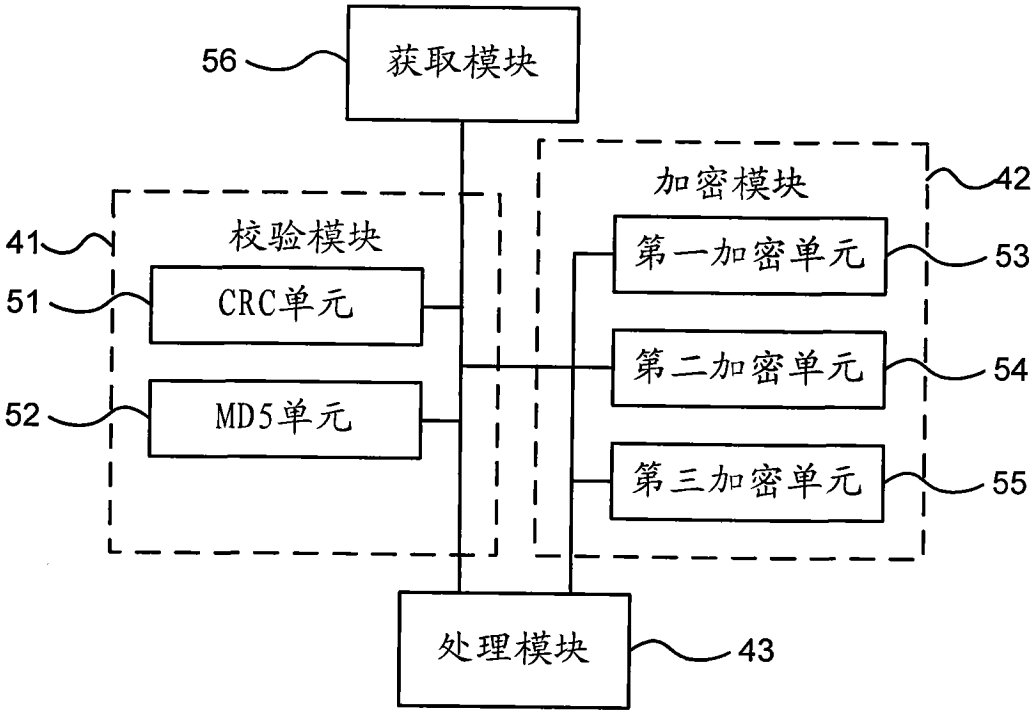

56
获取模块
加密模块
42
41
校验模块
第一加密单元
53
51
CRC单元
第二加密单元
54
52
MD5单元
第三加密单元
55
处理模块
43

图 5

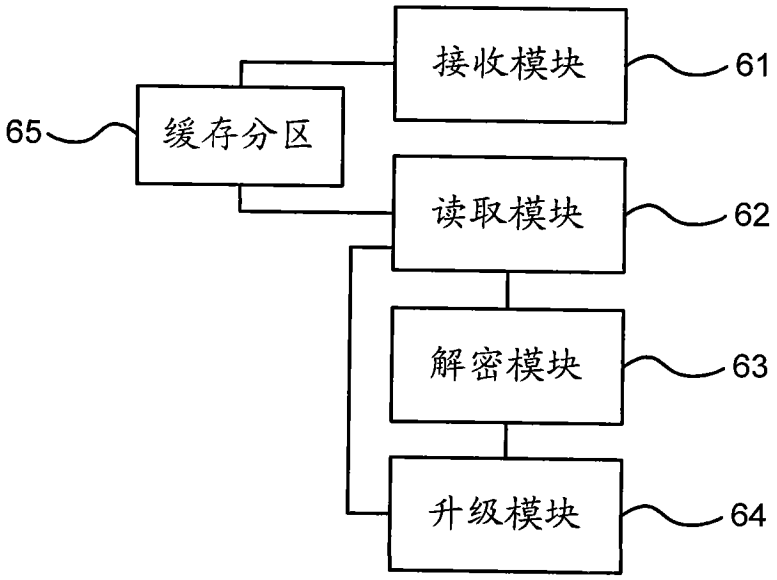


图 6

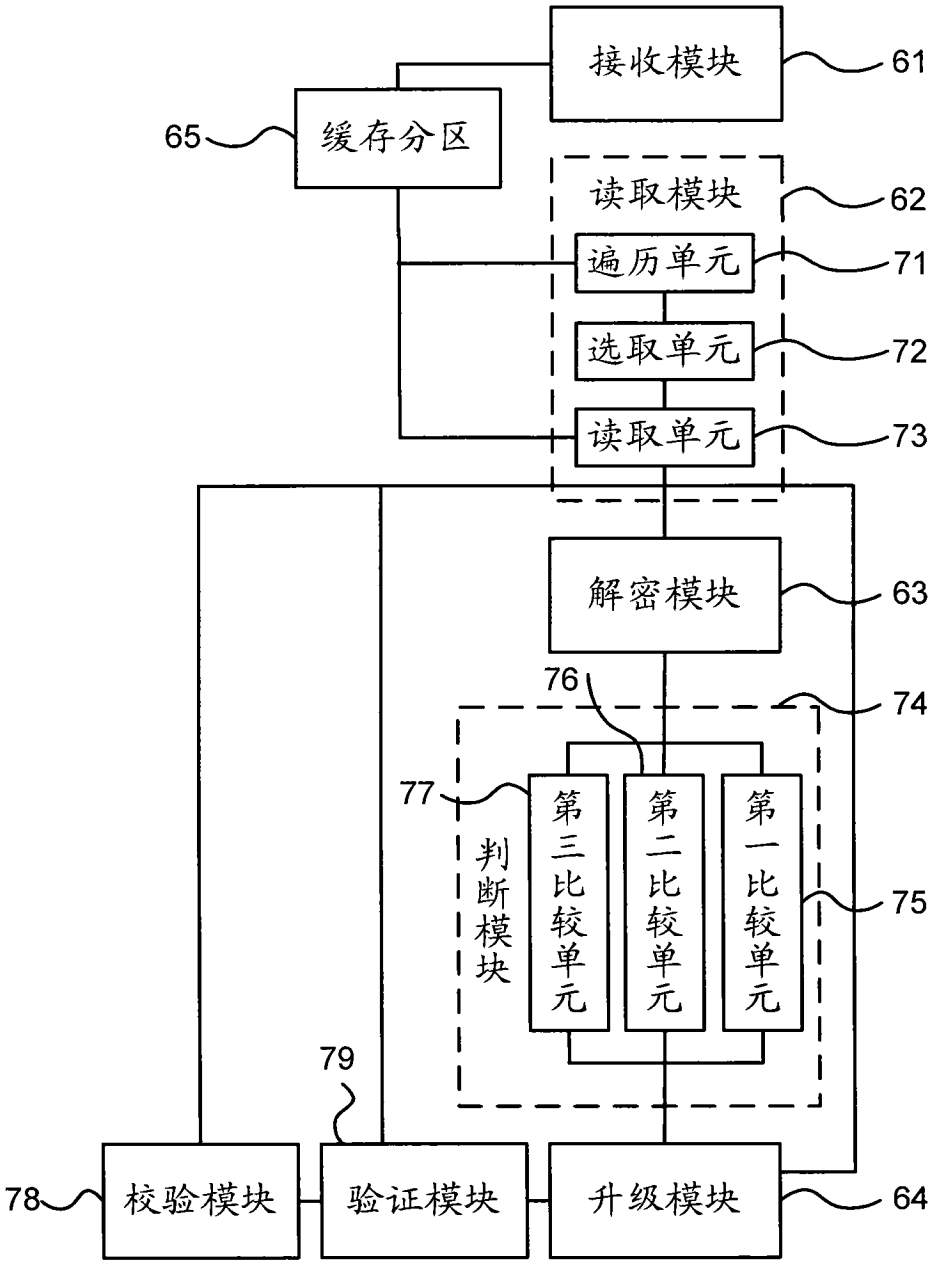

接收模块
61
65
缓存分区
读取模块
62
遍历单元
71
选取单元
72
读取单元
73
解密模块
63
76
74
77
第三比较单元
第二比较单元
第一比较单元
75
判断模块
79
78
校验模块
验证模块
升级模块
64

图 7

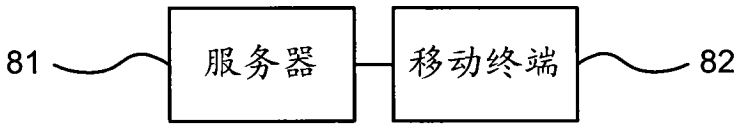

81
服务器
移动终端
82

图 8