(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 103338450 A
(43)申请公布日 2013.10.02

(21)申请号 201310260829.0

(22)申请日 2013.06.26

(71)申请人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼

(72)发明人 赵兴军 崔洋

(74)专利代理机构 广州三环专利代理有限公司 44202
代理人 郝传鑫 熊永强

(51)Int.Cl.
H04W 12/06(2009.01)

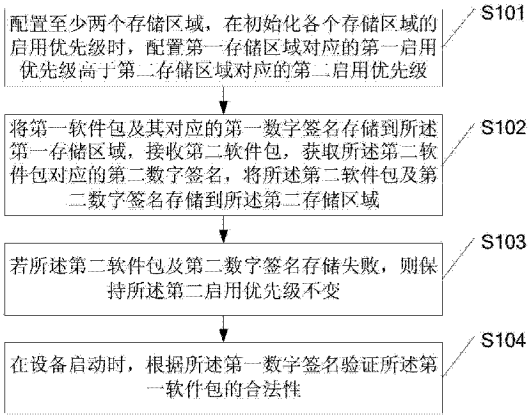
权利要求书2页 说明书8页 附图3页

(54)发明名称

一种验证方法及设备

(57)摘要

本发明实施例公开了一种验证方法，包括：配置至少两个存储区域，在初始化各个存储区域的启用优先级时，配置第一存储区域对应的第一启用优先级高于第二存储区域对应的第二启用优先级；将第一软件包及其对应的第一数字签名存储到所述第一存储区域，接收第二软件包，获取所述第二软件包对应的第二数字签名，将所述第二软件包及第二数字签名存储到所述第二存储区域；若所述第二软件包及第二数字签名存储失败，则保持所述第二启用优先级不变；在设备重启时，根据所述第一数字签名验证所述第一软件包的合法性。本发明实施例还公开了一种验证设备。采用本发明，可提高设备工作的可靠性，确保设备在软件升级验证失败时仍能正常工作。



CN 103338450 A

1. 一种验证方法，其特征在于，包括：

配置至少两个存储区域，在初始化各个存储区域的启用优先级时，配置第一存储区域对应的第一启用优先级高于第二存储区域对应的第二启用优先级；

将第一软件包及其对应的第一数字签名存储到所述第一存储区域，接收第二软件包，获取所述第二软件包对应的第二数字签名，将所述第二软件包及第二数字签名存储到所述第二存储区域；

若所述第二软件包及第二数字签名存储失败，则保持所述第二启用优先级不变；

在设备重启时，根据所述第一数字签名验证所述第一软件包的合法性。

2. 如权利要求 1 所述的方法，其特征在于，若所述第二软件包及第二数字签名存储成功，则更新所述第二启用优先级，使得所述第二启用优先级高于所述第一启用优先级，在所述设备重启时，根据所述第二数字签名验证所述第二软件包的合法性。

3. 如权利要求 2 所述的方法，其特征在于，所述获取所述第二软件包对应的第二数字签名，将所述第二软件包及第二数字签名存储到第二存储区域，包括：

通过 RSA 加密算法获取所述第二软件包的加密密钥和解密密钥；

对所述第二软件包进行哈希计算得到所述第二软件包的第一摘要；

利用所述加密密钥对所述第一摘要进行加密得到所述第二软件包对应的第二数字签名；

将所述第二软件包及第二数字签名存储到所述第二存储区域。

4. 如权利要求 3 所述的方法，其特征在于，所述在所述设备重启时，根据所述第二数字签名验证所述第二软件包的合法性，包括：

在所述设备重启时，比较所述第一启用优先级及所述第二启用优先级的优先级高低；

读取启用优先级高的第二存储区域中的第二数字签名和第二软件包；

利用所述解密密码对所述第二数字签名进行解密，得到所述第二软件包的第二摘要；

判断所述第一摘要是否和第二摘要相同；

若相同，则加载所述第二软件包。

5. 如权利要求 1-4 任一项所述的方法，其特征在于，还包括：

若接收到第三软件包，则获取所述第三软件包对应的第三数字签名，根据所述第一启用优先级及第二启用优先级的高低，选择启用优先级低的存储区域存储所述第三软件包及第三数字签名，并更新存储所述第三软件包及第三数字签名的存储区域的启用优先级，使得存储所述第三软件包及第三数字签名的存储区域的启用优先级高于其他存储区域的启用优先级。

6. 一种验证设备，其特征在于，包括：

配置模块，用于配置至少两个存储区域，在初始化各个存储区域的启用优先级时，配置第一存储区域对应的第一启用优先级高于第二存储区域对应的第二启用优先级；

存储模块，用于将第一软件包及其第一数字签名存储到第一存储区域，接收第二软件包，获取所述第二软件包对应的第二数字签名，将所述第二软件包及第二数字签名存储到第二存储区域；

更新模块，用于若所述第二软件包及第二数字签名存储失败，则保持所述第二启用优先级不变；

验证模块，用于在设备重启时，根据所述第一数字签名验证所述第一软件包的合法性。

7. 如权利要求 6 所述的设备，其特征在于，包括：

所述更新模块还用于若所述第二软件包及第二数字签名存储成功，则更新所述第二启用优先级，使得所述第二启用优先级高于所述第一启用优先级；

所述验证模块还用于在所述设备重启时，根据所述第二数字签名验证所述第二软件包的合法性。

8. 如权利要求 7 所述的设备，其特征在于，所述存储模块包括：

密钥获取单元，用于通过 RSA 加密算法获取所述第二软件包的加密密钥和解密密钥；

哈希计算单元，对所述第二软件包进行哈希计算得到所述第二软件包的第一摘要；

签名获取单元，用于利用所述加密密钥对所述第一摘要进行加密得到所述第二软件包对应的第二数字签名；

保存单元，用于将所述第二软件包及第二数字签名存储到所述第二存储区域。

9. 如权利要求 8 所述的设备，其特征在于，所述验证模块包括：

比较单元，用于在所述设备重启时，比较所述第一启用优先级及所述第二启用优先级的优先级高低；

读取单元，读取启用优先级高的第二存储区域中的第二数字签名和第二软件包；

解密单元，利用所述解密密码对所述第二数字签名进行解密，得到所述第二软件包的第二摘要；

判断单元，用于判断所述第一摘要是否和第二摘要相同；

加载单元，用于当所述判断单元判定所述第一摘要和第二摘要相同时，加载所述第二软件包。

10. 如权利要求 6-9 任一项所述的设备，其特征在于，包括：

所述存储模块还用于若接收到第三软件包，则获取所述第三软件包对应的第三数字签名，根据所述第一启用优先级及第二启用优先级的高低，选择启用优先级低的存储区域存储所述第三软件包及第三数字签名；

所述更新模块还用于更新存储所述第三软件包及第三数字签名的存储区域的启用优先级，使得存储所述第三软件包及第三数字签名的存储区域的启用优先级高于其他存储区域的启用优先级。

一种验证方法及设备

技术领域

[0001] 本发明涉及通信技术领域，尤其涉及一种验证方法及设备。

背景技术

[0002] 随着通信技术的不断发展，无线网络架构扁平化、移动网络 IP 化、基站设备形态小型化，部署场地灵活化等趋势导致了基站特别是小型基站受到越来越多的安全威胁。对于一些部署在未受运营商管控场地的基站，基站设备上的软件或关键配置数据可能被篡改，让该设备按照攻击者的意图工作。为了防范攻击者对软件或关键配置数据的篡改，需要对设备上的软件或关键配置数据进行完整性保护，设备商通过对这些软件或关键配置数据进行 RSA 完整性数字签名，在使用这些安全敏感数据前，先对其完整性进行验证，如果验证失败，则意味着这些数据被篡改了，则设备不能使用这些数据。对设备上的软件或关键配置数据进行完整性保护的目的是防止其被篡改，但是，如果在进行完整性数字签名时，数字签名存储失败，则设备在进行完整性验证时将会读取存储失败的不完整数字签名进行验证，误判软件或关键配置数据被篡改，从而导致软件或关键配置数据加载失败，尤其在对设备上的软件或关键配置数据升级更新时，将导致升级更新失败，设备相关软件功能缺失甚至无法启动。

发明内容

[0003] 本发明实施例所要解决的技术问题在于，提供一种验证方法。可提高设备工作的可靠性，确保设备在软件升级验证失败时仍能正常工作。

[0004] 本发明实施例第一方面提供了一种验证方法，包括：

[0005] 配置至少两个存储区域，在初始化各个存储区域的启用优先级时，配置第一存储区域对应的第一启用优先级高于第二存储区域对应的第二启用优先级；

[0006] 将第一软件包及其对应的第一数字签名存储到所述第一存储区域，接收第二软件包，获取所述第二软件包对应的第二数字签名，将所述第二软件包及第二数字签名存储到所述第二存储区域；

[0007] 若所述第二软件包及第二数字签名存储失败，则保持所述第二启用优先级不变；

[0008] 在设备重启时，根据所述第一数字签名验证所述第一软件包的合法性。

[0009] 在第一方面的第一种可能的实现方式中，若所述第二软件包及第二数字签名存储成功，则更新所述第二启用优先级，使得所述第二启用优先级高于所述第一启用优先级，在所述设备重启时，根据所述第二数字签名验证所述第二软件包的合法性。

[0010] 结合第一方面的第一种可能的实现方式，在第二种可能的实现方式中，所述获取所述第二软件包对应的第二数字签名，将所述第二软件包及第二数字签名存储到第二存储区域，包括：

[0011] 通过 RSA 加密算法获取所述第二软件包的加密密钥和解密密钥；

[0012] 对所述第二软件包进行哈希计算得到所述第二软件包的第一摘要；

[0013] 利用所述加密密钥对所述第一摘要进行加密得到所述第二软件包对应的第二数字签名；

[0014] 将所述第二软件包及第二数字签名存储到所述第二存储区域。

[0015] 结合第一方面的第二种可能的实现方式，在第三种可能的实现方式中，所述在所述设备重启时，根据所述第二数字签名验证所述第二软件包的合法性，包括：

[0016] 在所述设备重启时，比较所述第一启用优先级及所述第二启用优先级的优先级高低；

[0017] 读取启用优先级高的第二存储区域中的第二数字签名和第二软件包；

[0018] 利用所述解密密码对所述第二数字签名进行解密，得到所述第二软件包的第二摘要；

[0019] 判断所述第一摘要是否和第二摘要相同；

[0020] 若相同，则加载所述第二软件包。

[0021] 结合第一方面或结合第一方面的第一或第二或第三种可能的实现方式，在第四种可能的实现方式中，若接收到第三软件包，则获取所述第三软件包对应的第三数字签名，根据所述第一启用优先级及第二启用优先级的高低，选择启用优先级低的存储区域存储所述第三软件包及第三数字签名，并更新存储所述第三软件包及第三数字签名的存储区域的启用优先级，使得存储所述第三软件包及第三数字签名的存储区域的启用优先级高于其他存储区域的启用优先级。

[0022] 本发明实施例第二方面提供了一种验证设备，包括：

[0023] 配置模块，用于配置至少两个存储区域，在初始化各个存储区域的启用优先级时，配置第一存储区域对应的第一启用优先级高于第二存储区域对应的第二启用优先级；

[0024] 存储模块，用于将第一软件包及其第一数字签名存储到第一存储区域，接收第二软件包，获取所述第二软件包对应的第二数字签名，将所述第二软件包及第二数字签名存储到第二存储区域；

[0025] 更新模块，用于若所述第二软件包及第二数字签名存储失败，则保持所述第二启用优先级不变；

[0026] 验证模块，用于在设备重启时，根据所述第一数字签名验证所述第一软件包的合法性。

[0027] 在第二方面的第一种可能的实现方式中，所述更新模块还用于若所述第二软件包及第二数字签名存储成功，则更新所述第二启用优先级，使得所述第二启用优先级高于所述第一启用优先级；

[0028] 所述验证模块还用于在所述设备重启时，根据所述第二数字签名验证所述第二软件包的合法性。

[0029] 结合第二方面的第一种可能的实现方式，在第二种可能的实现方式中，所述存储模块包括：

[0030] 密钥获取单元，用于通过 RSA 加密算法获取所述第二软件包的加密密钥和解密密钥；

[0031] 哈希计算单元，对所述第二软件包进行哈希计算得到所述第二软件包的第一摘要；

[0032] 签名获取单元，用于利用所述加密密钥对所述第一摘要进行加密得到所述第二软件包对应的第二数字签名；

[0033] 保存单元，用于将所述第二软件包及第二数字签名存储到所述第二存储区域。

[0034] 结合第二方面的第二种可能的实现方式，在第三种可能的实现方式中，所述验证模块包括：

[0035] 比较单元，用于在所述设备重启时，比较所述第一启用优先级及所述第二启用优先级的优先级高低；

[0036] 读取单元，读取启用优先级高的第二存储区域中的第二数字签名和第二软件包；

[0037] 解密单元，利用所述解密密码对所述第二数字签名进行解密，得到所述第二软件包的第二摘要；

[0038] 判断单元，用于判断所述第一摘要是否和第二摘要相同；

[0039] 加载单元，用于当所述判断单元判定所述第一摘要和第二摘要相同时，加载所述第二软件包。

[0040] 结合第二方面或结合第一方面的第一或第二或第三种可能的实现方式，在第四种可能的实现方式中，所述存储模块还用于若接收到第三软件包，则获取所述第三软件包对应的第三数字签名，根据所述第一启用优先级及第二启用优先级的高低，选择启用优先级低的存储区域存储所述第三软件包及第三数字签名；

[0041] 所述更新模块还用于更新存储所述第三软件包及第三数字签名的存储区域的启用优先级，使得存储所述第三软件包及第三数字签名的存储区域的启用优先级高于其他存储区域的启用优先级。

[0042] 实施本发明实施例，具有如下有益效果：

[0043] 通过配置至少两个存储区域，且利用第一存储区域存储当前使用的第一数字签名和第一软件包，利用第二存储区域存储新接收的第二数字签名和第二软件包，并配置第一存储区域的启用优先级高于第二区域的启用优先级，这样即使第二数字签名和第二软件包存储失败，也可以根据启用优先级高的第一存储区域中存储的第一数字签名和第一软件包进行验证，正常使用相关软件功能及启动设备，从而提高了设备工作的可靠性，确保了设备在软件升级验证失败时仍能正常工作。

附图说明

[0044] 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简单地介绍，显而易见地，下面描述中的附图仅仅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。

[0045] 图 1 是本发明验证方法的第一实施例的流程示意图；

[0046] 图 2 是本发明验证方法的第二实施例的流程示意图；

[0047] 图 3 是本发明验证方法的第三实施例的流程示意图；

[0048] 图 4 是本发明验证设备的第一实施例的组成示意图；

[0049] 图 5 是图 4 所述验证设备的存储模块的组成示意图；

[0050] 图 6 是图 4 所述验证设备的验证模块的组成示意图。

具体实施方式

[0051] 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，所描述的实施例仅仅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，都属于本发明保护的范围。

[0052] 请参照图 1，为本发明验证方法的第一实施例的流程示意图，在本实施例中，所述方法包括以下步骤：

[0053] S101，配置至少两个存储区域，在初始化各个存储区域的启用优先级时，配置第一存储区域对应的第一启用优先级高于第二存储区域对应的第二启用优先级。

[0054] 具体地，所述存储区域用于存储软件包、软件包对应的数字签名、启用优先级的相关信息。其可以是磁碟、光盘、FLASH 闪存、只读存储记忆体（Read-Only Memory，简称 ROM）或随机存储记忆体（Random Access Memory，简称 RAM）等。

[0055] S102，将第一软件包及其对应的第一数字签名存储到所述第一存储区域，接收第二软件包，获取所述第二软件包对应的第二数字签名，将所述第二软件包及第二数字签名存储到所述第二存储区域。

[0056] 具体地，所述第一软件包与第二软件包可以是同一软件的不同版本，也可以是同一软件的不同配置数据等。在本实施例中，所述第一软件包为设备当前使用的软件包。其可以是设备初始使用的软件包，也可以是上一次更新的软件包。在设备启动时，将根据所述第一软件包计算第一数字签名并保存在所述第一存储区域，在没有接收到新的软件包时，设备上电启动，则会默认读取所述第一存储区域中的第一数字签名对所述第一软件包进行完整性验证，当验证通过时，则加载所述第一软件包，执行相关程序。若验证失败，则不会加载所述第一软件包。对于各种系统而言，所述第一软件包可以是操作系统，也可以是普通的应用软件，若所述第一软件包对应于普通应用软件，验证失败时将导致相应的软件无法启动，从而无法使用该软件对应的功能；若所述第一软件包对应于操作系统，验证失败时将导致设备无法进行操作系统，从而无法启动设备。而对于通信领域中较多采用的嵌入式操作系统，其操作系统和软件应用一般集成在一起，第一软件包对应的可以是设备商的应用程序、高层软件，也可以是嵌入式操作系统如 vxWorks、LINUX 等，他们可以独立升级也可以同时升级。对于嵌入式操作系统，若验证失败将直接导致设备无法启动，从而造成不可预料的损失。因此，在实施例中，配置至少两个存储区域分别进行相关数字签名和软件包的存储，为后续选择对应存储区域中的数字签名和软件包进行验证提供了基础。

[0057] 所述第二软件包为所述第一软件包的更新升级包。当接收到所述第二软件包时，可通过 RSA 加密算法获取所述第二软件包的加密密钥 SK 和解密密钥 PK，对所述第二软件包进行哈希计算可得到所述第二软件包的第一摘要，利用所述加密密钥对所述第一摘要进行加密即可得到所述第二软件包对应的第二数字签名，在存储所述第二软件包及第二数字签名时，将所述第二软件包及第二数字签名存储到所述第二存储区域。

[0058] S103，若所述第二软件包及第二数字签名存储失败，则保持所述第二启用优先级不变。

[0059] 在存储所述第二软件包及第二数字签名时，通常使用 FLASH 闪存写入完成。由于

写入需要一定的时间，若在写入过程中，遇到断电、误开关、误操作、软件包超出容量等原因导致写入失败时，将保持所述第二存储区域的第二启用优先级保持不变，即按照原始配置保持所述第二启用优先级低于所述第一启用优先级。需要说明的是，启用优先级的更新在存储所述第二软件包及第二数字签名之后，只有在所述第二软件包及第二数字签名存储完毕之后才会触发启用优先级的更新，否则不更新，保持原有的启用优先级。

[0060] S104，在设备重启时，根据所述第一数字签名验证所述第一软件包的合法性。

[0061] 由于所述第二软件包及第二数字签名存储失败，若在设备重启时，读取第二存储区域中不完整的数字签名和软件包进行验证的话将导致验证失败，相关软件功能无法使用甚至无法启动设备。但是，在本实施例中，因为在所述第二存储区域之外，还存在所述第一存储区域，且由于所述第二软件包及第二数字签名存储失败，所述第二启用优先级保持不变，即按照原始配置保持所述第一启用优先级高于所述第二启用优先级。因此，在设备重启时，将根据启用优先级的高低，选择启用优先级高的第一存储区域中的数字签名验证所述第一软件包的合法性。从而解决在软件包更新时，由于数字签名和软件包存储失败导致验证失败，相关软件功能无法使用甚至设备无法启动的问题。

[0062] 需要说明的是，设备重启为存储所述第二软件包及第二数字签名之后的下一次启动，其可以在尝试存储所述第二软件包及第二数字签名之后立即进行，也可以在尝试存储所述第二软件包及第二数字签名一段时间之后再进行。

[0063] 通过配置至少两个存储区域，且利用第一存储区域存储当前使用的第一数字签名和第一软件包，利用第二存储区域存储新接收的第二数字签名和第二软件包，并配置第一存储区域的启用优先级高于第二区域的启用优先级，这样即使第二数字签名和第二软件包存储失败，也可以根据启用优先级高的第一存储区域中存储的第一数字签名和第一软件包进行验证，正常使用相关软件功能及启动设备，从而提高了设备工作的可靠性，确保了设备在软件升级验证失败时仍能正常工作。

[0064] 若存在三个存储区域，则可以在初始化启用优先级时，依次配置第一存储区域、第二存储区域、第三存储区域的启用优先级分别为第一启用优先级、第二启用优先级、第三启用优先级、且第一启用优先级高于第二、第三启用优先级，当接收到新的软件包时，可选择第二或第三存储区域中的任意一个进行新软件包及其数字签名的存储，如选择启用优先级最低的存储区域存储，且在存储成功后更新对应存储区域的启用优先级高于第一启用优先级，这样在设备重启时，将选择新的数字签名和软件包进行验证。

[0065] 请参照图 2，为本发明验证方法的第二实施例的流程示意图，在本实施例中，所述方法包括以下步骤：

[0066] S201，配置至少两个存储区域，且第一存储区域对应的第一启用优先级高于第二存储区域对应的第二启用优先级。

[0067] S202，将第一软件包及其对应的第一数字签名存储到所述第一存储区域，接收第二软件包，获取所述第二软件包对应的第二数字签名，将所述第二软件包及第二数字签名存储到所述第二存储区域。

[0068] S203，若所述第二软件包及第二数字签名存储失败，则保持所述第二启用优先级不变。

[0069] S204，在设备重启时，根据所述第一数字签名验证所述第一软件包的合法性。

[0070] S205，若所述第二软件包及第二数字签名存储成功，则更新所述第二启用优先级，使得所述第二启用优先级高于所述第一启用优先级，在所述设备重启时，根据所述第二数字签名验证所述第二软件包的合法性。

[0071] 具体地，验证合法性的过程如下：

[0072] 在所述设备重启时，比较所述第一启用优先级及所述第二启用优先级的优先级高低；

[0073] 读取启用优先级高的第二存储区域中的第二数字签名和第二软件包；

[0074] 利用所述解密密码对所述第二数字签名进行解密，得到所述第二软件包的第二摘要；

[0075] 判断所述第一摘要是否和第二摘要相同；

[0076] 若相同，则加载所述第二软件包。若不同，则不加载所述第二软件包。

[0077] 相对于普通验证过程，增加了启用优先级比较的过程。从而确保使用启用优先级高的存储区域中的内容进行验证。

[0078] 在本实施例中，给出了所述第二软件包及第二数字签名存储成功后的验证方法，由于所述第二软件包及第二数字签名存储成功，所以需要对所述第二启用优先级进行更新，确保所述第二启用优先级高于所述第一启用优先级。例如，原始配置时，第一启用优先级为 2，第二启用优先级为 1，则所述第二软件包及第二数字签名存储失败时保持优先级不变，设备将根据第一启用优先级启用第一存储区域中的第一数字签名和第一软件包进行验证；而在所述第二软件包及第二数字签名存储成功后，更新所述第二启用优先级，例如提升 2 使得第二启用优先级由 1 变为 3，这样在所述设备重启时，将根据新的第二启用优先级启用第二存储区域中的第二数字签名和第二软件包进行验证，若验证通过，设备将加载所述第二软件包，使用新版本的软件或参数配置。

[0079] 通过对启用优先级的更新，确保在第二数字签名和第二软件包存储成功时，将优先使用新的软件包，在确保设备工作可靠性的前提下，实现软件更新后的即时使用。

[0080] 请参照图 3，为本发明验证方法的第三实施例的流程示意图，在本实施例中，所述方法包括以下步骤：

[0081] S301，配置至少两个存储区域，且第一存储区域对应的第一启用优先级高于第二存储区域对应的第二启用优先级。

[0082] S302，将第一软件包及其对应的第一数字签名存储到所述第一存储区域，接收第二软件包，获取所述第二软件包对应的第二数字签名，将所述第二软件包及第二数字签名存储到所述第二存储区域。

[0083] S303，若所述第二软件包及第二数字签名存储失败，则保持所述第二启用优先级不变。

[0084] S304，在设备重启时，根据所述第一数字签名验证所述第一软件包的合法性。

[0085] S305，若所述第二软件包及第二数字签名存储成功，则更新所述第二启用优先级，使得所述第二启用优先级高于所述第一启用优先级，在所述设备重启时，根据所述第二数字签名验证所述第二软件包的合法性。

[0086] S306，若接收到第三软件包，则获取所述第三软件包对应的第三数字签名，根据所述第一启用优先级及第二启用优先级的高低，选择启用优先级低的存储区域存储所述第三

软件包及第三数字签名，并更新存储所述第三软件包及第三数字签名的存储区域的启用优先级，使得存储所述第三软件包及第三数字签名的存储区域的启用优先级高于其他存储区域的启用优先级。

[0087] 在本实施例中，增加了接收第三软件包后对第三软件包的处理。若第二软件包和第二数字签名存储成功，则第二启用优先级将更新为高于第一启用优先级，此时若接收到第三软件包，则根据前文描述的获取数字签名的方法获取对应的第三数字签名并将第三数字签名和第三软件包存储至启用优先级低的第一存储区域，且存储成功后将更新第一存储区域的第一启用优先级，使得第一启用优先级高于第二启用优先级；若存储失败则保持启用优先级不变。

[0088] 若第二软件包和第二数字签名存储失败，则第二启用优先级低于第一启用优先级，此时若接收到第三软件包，则获取第三数字签名后将第三数字签名和第三软件包存储至启用优先级低的第二存储区域，后续处理类似，此处不再赘述。

[0089] 当然，也可以保持第一存储区域中的第一数字签名、第一软件包、第一启用优先级一直不变，在接收到第三软件包时，先更新所述第二启用优先级使得第二启用优先级低于第一启用优先级，再按照第一实施例及第二实施例中的验证方法进行处理。

[0090] 请参照图 4，为本发明验证设备的第一实施例的组成示意图。在本实施例中，所述设备包括：

[0091] 配置模块 10，用于配置至少两个存储区域，且第一存储区域对应的第一启用优先级高于第二存储区域对应的第二启用优先级；

[0092] 存储模块 20，用于将第一软件包及其第一数字签名存储到第一存储区域，接收第二软件包，获取所述第二软件包对应的第二数字签名，将所述第二软件包及第二数字签名存储到第二存储区域；

[0093] 更新模块 30，用于若所述第二软件包及第二数字签名存储失败，则保持所述第二启用优先级不变；

[0094] 验证模块 40，用于在设备重启时，根据所述第一数字签名验证所述第一软件包的合法性。

[0095] 所述更新模块 30 还用于若所述第二软件包及第二数字签名存储成功，则更新所述第二启用优先级，使得所述第二启用优先级高于所述第一启用优先级；

[0096] 所述验证模块 40 还用于在所述设备重启时，根据所述第二数字签名验证所述第二软件包的合法性。

[0097] 在另一种实施方式中，所述存储模块 20 还可用于若接收到第三软件包，则获取所述第三软件包对应的第三数字签名，根据所述第一启用优先级及第二启用优先级的高低，选择启用优先级低的存储区域存储所述第三软件包及第三数字签名；

[0098] 所述更新模块 30 还可用于更新存储所述第三软件包及第三数字签名的存储区域的启用优先级，使得存储所述第三软件包及第三数字签名的存储区域的启用优先级高于其他存储区域的启用优先级。

[0099] 请参照图 5，为图 4 所述验证设备的存储模块 20 的组成示意图，在本实施例中，所述存储模块 20 包括：

[0100] 密钥获取单元 21，用于通过 RSA 加密算法获取所述第二软件包的加密密钥和解密

密钥；

[0101] 哈希计算单元 22，对所述第二软件包进行哈希计算得到所述第二软件包的第一摘要；

[0102] 签名获取单元 23，用于利用所述加密密钥对所述第一摘要进行加密得到所述第二软件包对应的第二数字签名；

[0103] 保存单元 24，用于将所述第二软件包及第二数字签名存储到所述第二存储区域。

[0104] 请参照图 6，为图 4 所述验证设备的验证模块 40 的组成示意图，在本实施例中，所述验证模块 40 包括：

[0105] 比较单元 41，用于在所述设备重启时，比较所述第一启用优先级及所述第二启用优先级的优先级高低；

[0106] 读取单元 42，读取启用优先级高的第二存储区域中的第二数字签名和第二软件包；

[0107] 解密单元 43，利用所述解密密码对所述第二数字签名进行解密，得到所述第二软件包的第二摘要；

[0108] 判断单元 44，用于判断所述第一摘要是否和第二摘要相同；

[0109] 加载单元 45，用于当所述判断单元判定所述第一摘要和第二摘要相同时，加载所述第二软件包。

[0110] 需要说明的是，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它实施例的不同之处，各个实施例之间相同相似的部分互相参见即可。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。

[0111] 通过上述实施例的描述，本发明具有以下优点：

[0112] 通过配置至少两个存储区域，且利用第一存储区域存储当前使用的第一数字签名和第一软件包，利用第二存储区域存储新接收的第二数字签名和第二软件包，并配置第一存储区域的启用优先级高于第二区域的启用优先级，这样即使第二数字签名和第二软件包存储失败，也可以根据启用优先级高的第一存储区域中存储的第一数字签名和第一软件包进行验证，正常使用相关软件功能及启动设备，从而提高了设备工作的可靠性，确保了设备在软件升级验证失败时仍能正常工作。

[0113] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述的程序可存储于一计算机可读取存储介质中，该程序在执行时，可包括如上述各方法的实施例的流程。其中，所述的存储介质可为磁碟、光盘、只读存储记忆体（Read-Only Memory，简称 ROM）或随机存储记忆体（Random Access Memory，简称 RAM）等。

[0114] 以上所揭露的仅为本发明较佳实施例而已，当然不能以此来限定本发明之权利范围，因此依本发明权利要求所作的等同变化，仍属本发明所涵盖的范围。

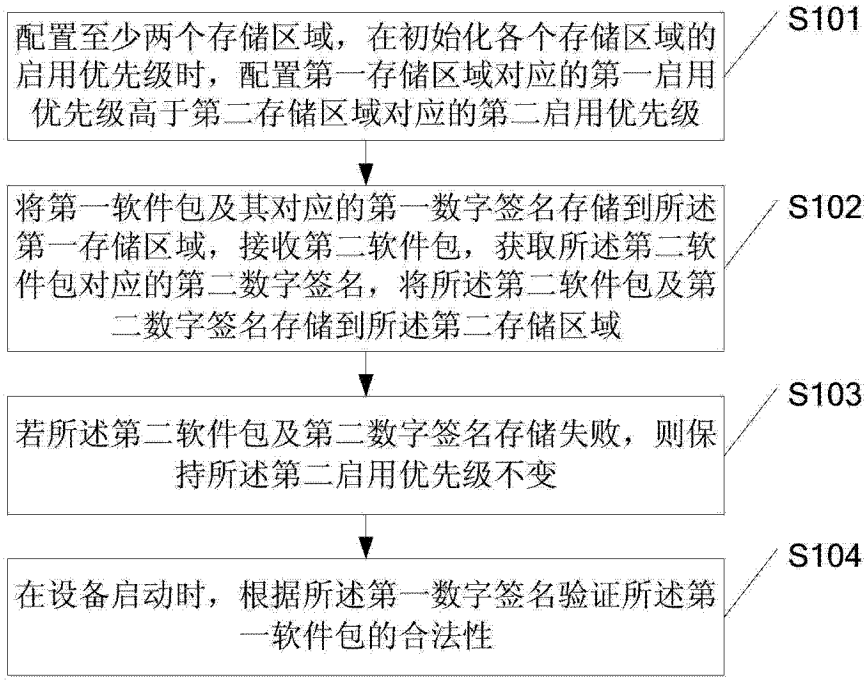

配置至少两个存储区域，在初始化各个存储区域的启用优先级时，配置第一存储区域对应的第一启用优先级高于第二存储区域对应的第二启用优先级
S101
将第一软件包及其对应的第一数字签名存储到所述第一存储区域，接收第二软件包，获取所述第二软件包对应的第二数字签名，将所述第二软件包及第二数字签名存储到所述第二存储区域
S102
若所述第二软件包及第二数字签名存储失败，则保持所述第二启用优先级不变
S103
在设备启动时，根据所述第一数字签名验证所述第一软件包的合法性
S104

图 1

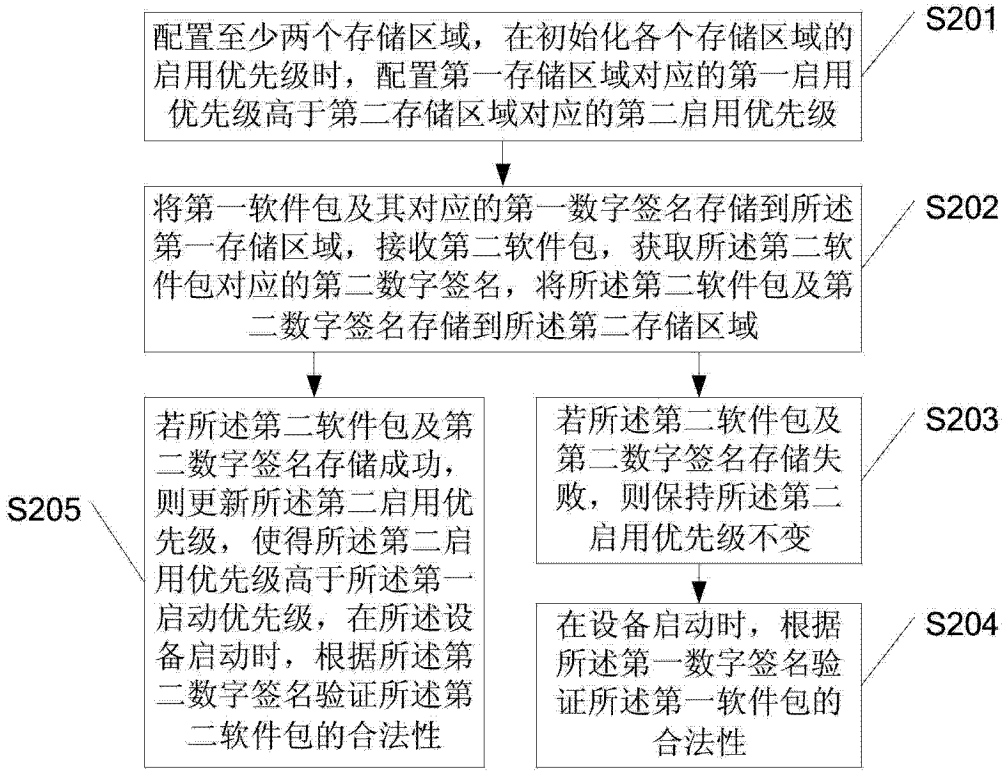

配置至少两个存储区域，在初始化各个存储区域的启用优先级时，配置第一存储区域对应的第一启用优先级高于第二存储区域对应的第二启用优先级
S201
将第一软件包及其对应的第一数字签名存储到所述第一存储区域，接收第二软件包，获取所述第二软件包对应的第二数字签名，将所述第二软件包及第二数字签名存储到所述第二存储区域
S202
若所述第二软件包及第二数字签名存储成功，则更新所述第二启用优先级，使得所述第二启用优先级高于所述第一启动优先级，在所述设备启动时，根据所述第二数字签名验证所述第二软件包的合法性
S205
若所述第二软件包及第二数字签名存储失败，则保持所述第二启用优先级不变
S203
在设备启动时，根据所述第一数字签名验证所述第一软件包的合法性
S204

图 2

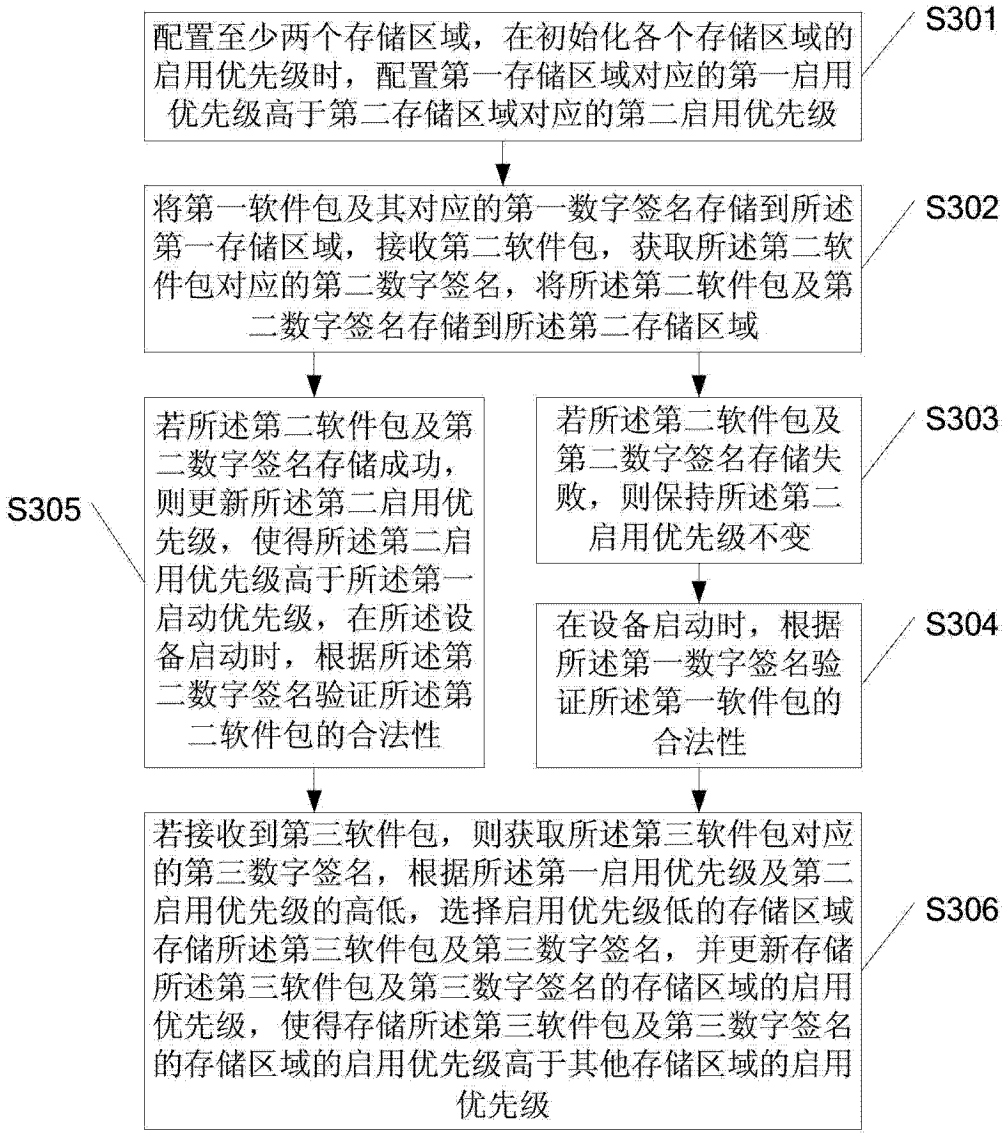

配置至少两个存储区域，在初始化各个存储区域的启用优先级时，配置第一存储区域对应的第一启用优先级高于第二存储区域对应的第二启用优先级
S301
将第一软件包及其对应的第一数字签名存储到所述第一存储区域，接收第二软件包，获取所述第二软件包对应的第二数字签名，将所述第二软件包及第二数字签名存储到所述第二存储区域
S302
若所述第二软件包及第二数字签名存储成功，则更新所述第二启用优先级，使得所述第二启用优先级高于所述第一启动优先级，在所述设备启动时，根据所述第二数字签名验证所述第二软件包的合法性
S305
若所述第二软件包及第二数字签名存储失败，则保持所述第二启用优先级不变
S303
在设备启动时，根据所述第一数字签名验证所述第一软件包的合法性
S304
若接收到第三软件包，则获取所述第三软件包对应的第三数字签名，根据所述第一启用优先级及第二启用优先级的高低，选择启用优先级低的存储区域存储所述第三软件包及第三数字签名，并更新存储所述第三软件包及第三数字签名的存储区域的启用优先级，使得存储所述第三软件包及第三数字签名的存储区域的启用优先级高于其他存储区域的启用优先级
S306

图 3

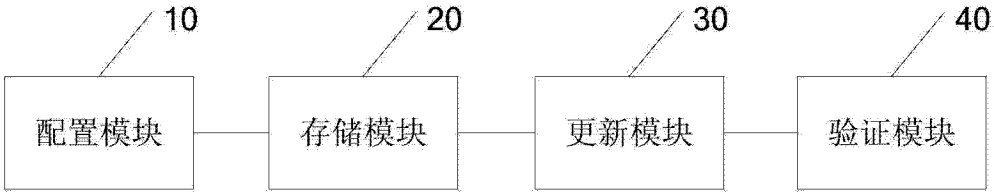

10
配置模块
20
存储模块
30
更新模块
40
验证模块

图 4

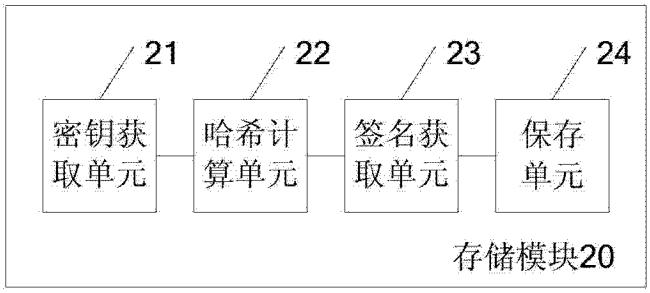

21
22
23
24
密钥获取单元
哈希计算单元
签名获取单元
保存单元
存储模块20

图 5

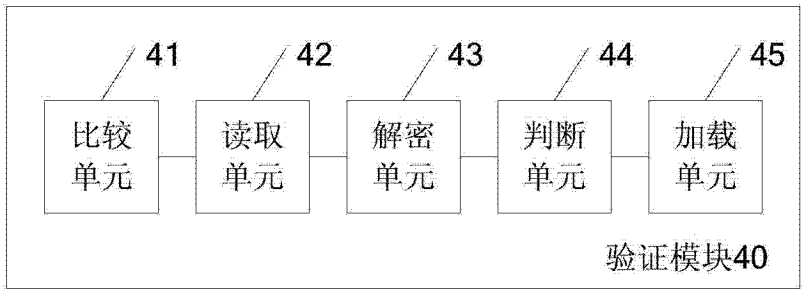

41
42
43
44
45
比较单元
读取单元
解密单元
判断单元
加载单元
验证模块40

图 6