[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 21/24 (2006.01)

[12] 发明专利说明书

专利号 ZL 200610116253.0

[45] 授权公告日 2009 年 3 月 11 日

[11] 授权公告号 CN 100468438C

[22] 申请日 2006.9.20

[21] 申请号 200610116253.0

[73] 专利权人 展讯通信(上海)有限公司

地址 201203 上海市浦东新区张江高科技园区松涛路 696 号 3 - 5 层

[72] 发明人 吕 玲 缪 晖

[56] 参考文献

CN1582422A 2005.2.16

CN1811784A 2006.8.2

US5337357A 1994.8.9

US2001/0010723A1 2001.8.2

CN1575446A 2005.2.2

审查员 吴 平

[74] 专利代理机构 上海浦一知识产权代理有限公司

代理人 丁纪铁

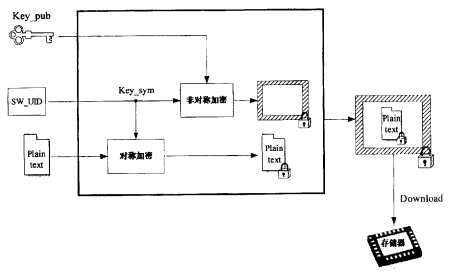
权利要求书 1 页 说明书 4 页 附图 1 页

[54] 发明名称

实现硬件和软件绑定的加密和解密方法

[57] 摘要

本发明公开了一种实现硬件和软件绑定的加密和解密方法，所述加密方法包括：对硬件序列号进行 HASH 变换得到一软件序列号；使用对称加密算法对软件明文进行加密；并使用一公用密钥通过非对称加密算法对对称密钥进行加密；最后将加密后的软件明文和对称密钥放在一起下载到存储器中。所述解密方法为：通过将使用一私用密钥对加密后的对称密钥进行解密得到一第一软件序列号和芯片对硬件序列号计算 HASH 值得到的第二软件序列号进行比较并解密的方法来得到实际的软件明文。 可实现软件产品和硬件产品的绑定，从而提高软件产品和硬件产品的安全性。



1、一种实现硬件和软件绑定的加密方法，其特征在于，所述方法包括以下步骤：

（1）将硬件序列号经过散列函数 HASH 变换得到一软件序列号；

（2）由所述软件序列号构成对称密钥，并通过对称加密算法对软件明文进行加密；

（3)使用一公用密钥通过非对称加密算法对所述对称密钥进行加密；

（4）将加密后的软件明文和加密后的对称密钥放在一起下载到存储器中。

2、一种对权利要求1中所述加密方法进行解密的方法，其特征在于，包括以下步骤：

（1）使用一私用密钥对加密后的对称密钥进行解密，得到一第一软件序列号；

（2）芯片对硬件序列号计算 HASH 值得到一第二软件序列号；

（3）对第一软件序列号和第二软件序列号进行比较，如果相同则进入步骤（4），否则进入步骤（5）；

（4）利用第二软件序列号对加密后的软件明文进行解密，得到实际的软件明文；

（5）验证失败，终止程序，发出告警信息。

实现硬件和软件绑定的加密和解密方法

技术领域

本发明涉及一种实现在带有中央处理器的终端系统的硬件和软件绑定的加密方法。本发明还涉及一种对上述加密方法进行解密的方法。

背景技术

目前在带有中央处理器的终端系统中，对软件的保护方法主要分为三类：上网注册、许可证（License）保护、软件加密。

前两类保护方法需要借助网络等外部途径来取得软件的正常使用权，适宜在连入网络的设备中使用。软件加密的方法主要有两种：加密狗和钥匙盘。加密狗是插在并口上的软硬件结合的软件加密产品。它一般都有几十或几百字节的非易失性存储空间可供读写，有的内部还增添了一个单片机。软件运行时通过向并口写入一定数据，判断从并口返回密码数据正确与否来检查加密狗是否存在。钥匙盘方式就是在特殊磁道里写入一定信息，软件在运行时通过校验这些信息判断其合法性。两者共同的特点都需要利用外部设备验证软件的合法性。对于很多功能简单、结构灵巧的便携设备（如手机等智能终端），采用上网注册或添加外设的方法就显得既不方便也不实用。

发明内容

本发明要解决的技术问题是提供一种实现硬件和软件绑定的加密方法，可实现软件产品和硬件产品的绑定，从而提高软件产品和硬件产品的

安全性。为此，本发明还提供一种对上述加密方法进行解密的方法。

为解决上述技术问题，本发明提供一种实现硬件和软件绑定的加密方法，包括以下步骤：

（1）将硬件序列号经过散列函数 HASH 变换得到一软件序列号；

（2）由所述软件序列号构成对称密钥，并通过对称加密算法对软件明文进行加密；

（3)使用一公用密钥通过非对称加密算法对所述对称密钥进行加密；

（4）将加密后的软件明文和加密后的对称密钥放在一起下载到存储器中。

同时，本发明还提供一种对所述加密方法进行解密的方法,包括步骤：

（1）使用一私用密钥对加密后的对称密钥进行解密，得到一第一软件序列号；

（2）芯片对硬件序列号计算 HASH 值得到一第二软件序列号；

（3）对第一软件序列号和第二软件序列号进行比较，如果相同则进入步骤（4），否则进入步骤（5）；

（4）利用第二软件序列号对加密后的软件明文进行解密，得到实际的软件明文；

（5）验证失败，终止程序，发出告警信息。

本发明由于采用了上述技术方案，具有这样的有益效果，即通过利用硬件序列号的某种变换作为软件加密的密钥，实现了软件产品和硬件产品的绑定，从而提高软件产品和硬件产品的安全性。

附图说明

图 1 是根据本发明的加密端的实现过程；

图 2 是根据本发明的解密端的实现过程。

具体实施方式

本发明包括加密和解密两部分。首先，硬件芯片中存储有一个代表芯片身份的唯一序列号（HW_UID），该序列号的长短由生产厂家自行决定，但绝对不能有重复。下面将从加密和解密两个方面详细介绍如何利用这个唯一序列号实现软、硬件的绑定。

如图 1 所示的实施例为根据本发明的加密端的实现过程。图中，Key_pub 表示公共密钥，用来进行非对称加密；Key_sym 表示对称密钥，用来进行对称加密；Plain text 表示要进行加密的软件明文；SW_UID 表示软件的唯一序列号。该软件加密的过程可通过以下四个步骤来实现：

（1）将 HW_UID 经过散列函数 HASH 变换得到 SW_UID；

（2）由 SW_UID 构成 Key_sym，通过对称加密算法对软件明文进行加密；

（3）Key_pub 通过非对称加密算法对 Key_sym 进行加密；

（4）加密后的 Plain text 和 Key_sym 放在一起下载到存储器中。

如图 2 所示的实施例为根据本发明的解密端的实现过程。其中，Key_prv 表示私有密钥，用来进行非对称解密，它同 HW_UID 一起存储于芯片的内部，并禁止任何外部设备的访问。该软件解密的过程可通过以下五个步骤来实现：

（1）用 Key_prv 对加密后的 Key_sym 进行解密，得到 SW_UID’；

（2）芯片对 HW_UID 计算 HASH 值得到 SW_UID；

（3）比较 SW_UID’和 SW_UID，如果相同则进入步骤（4），否则进入步骤（5）；

（4）利 SW_UID 对加密后的 Plain text 进行解密，得到 Plain text；

（5）验证失败，终止程序，发出告警信息。

在本发明中，上述方法中所提到的散列函数、对称加解密算法和非对称加解密算法并不局限于某种特定的方法，而是可以根据具体设计要求任意组合。

通过上述方法就实现了使用硬件芯片中的唯一序列号来实现软、硬件的绑定，从而提高了软件产品和硬件产品的安全性。

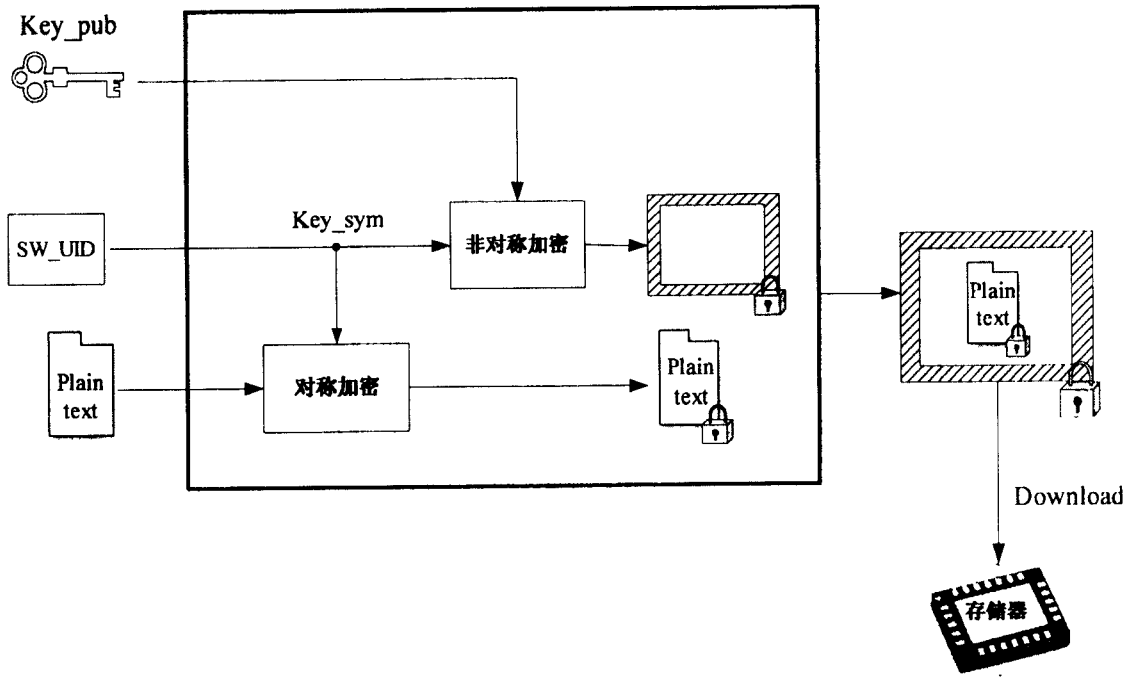

Key_pub
SW_UID
Key_sym
非对称加密
Plain text
对称加密
Plain text
Plain text
Download
存储器

图 1

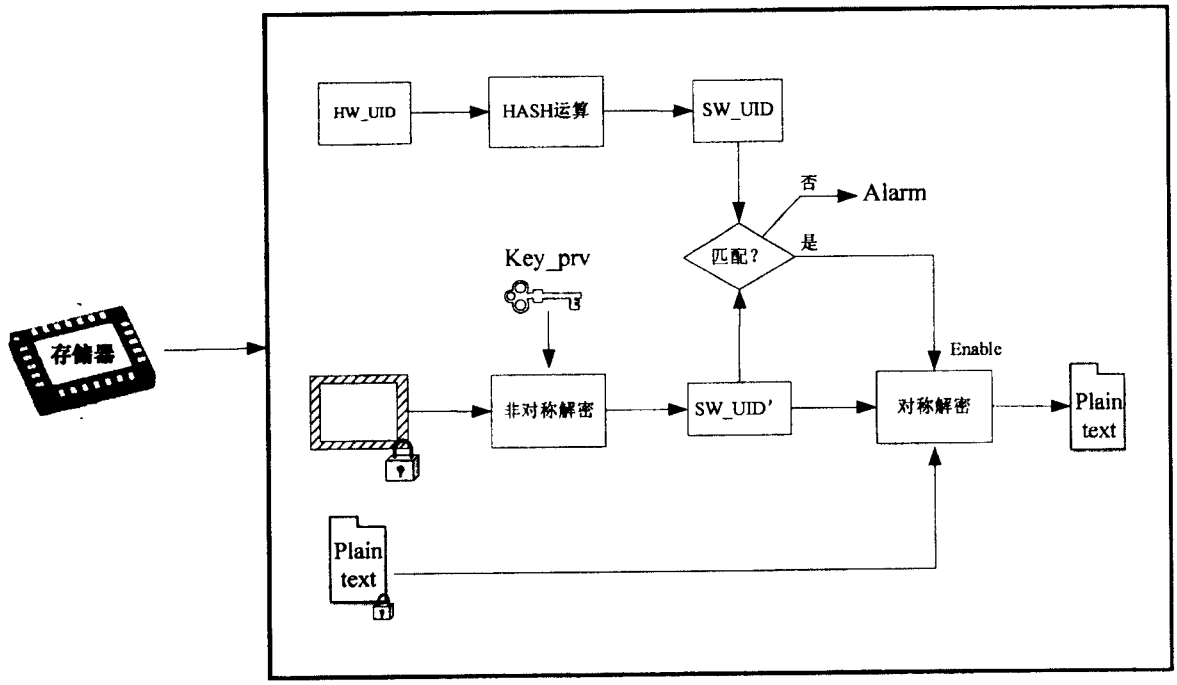

HW_UID
HASH运算
SW_UID
否
Alarm
匹配?
是
Key_prv
存储器
Enable
非对称解密
SW_UID'
对称解密
Plain text
Plain text

图 2