



(12)发明专利

(10)授权公告号 CN 106936588 B

(45)授权公告日 2020.04.24

(21)申请号 201710238153.3

(22)申请日 2017.04.13

(65)同一申请的已公布的文献号
申请公布号 CN 106936588 A

(43)申请公布日 2017.07.07

(73)专利权人 北京深思数盾科技股份有限公司
地址 100193 北京市海淀区西北旺东路10
号院东区5号楼5层510

(72)发明人 孙吉平 刘荣华

(74)专利代理机构 北京德琦知识产权代理有限
公司 11018

代理人 牛峥 王丽琴

(51)Int.Cl.

H04L 9/32(2006.01)

H04L 9/08(2006.01)

(56)对比文件

CN 104579690 A,2015.04.29,
CN 104579690 A,2015.04.29,
CN 104462882 A,2015.03.25,
CN 101246529 A,2008.08.20,
CN 101841525 A,2010.09.22,
CN 101662469 A,2010.03.03,
US 2011113235 A1,2011.05.12,

审查员 任悦

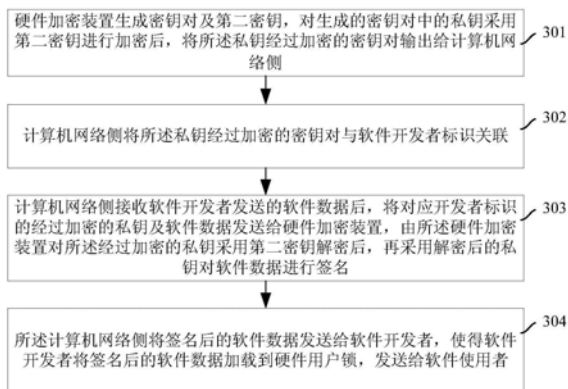
权利要求书2页 说明书6页 附图3页

(54)发明名称

一种硬件控制锁的托管方法、装置及系统

(57)摘要

本发明公开了一种硬件控制锁的托管方法、装置及系统,其中,所述硬件加密装置生成密钥对及第二密钥,对生成的密钥对中的私钥采用第二密钥进行加密后,将所述私钥经过加密的密钥对输出给计算机网络侧;所述计算机网络侧将所述私钥经过加密的密钥对与软件开发者标识关联;所述计算机网络侧接收软件开发者发送的软件数据后,将对应开发者标识的经过加密的私钥及软件数据发送给硬件加密装置,由所述硬件加密装置对所述经过加密的私钥采用第二密钥解密后,再采用解密后的私钥对软件数据进行签名;所述计算机网络侧将签名后的软件数据发送给软件开发者。本发明简单不繁琐且易于管理。



1. 一种硬件控制锁的托管方法,其特征在于,在计算机网络侧设置硬件加密装置,该方法还包括:

所述硬件加密装置生成密钥对及第二密钥,对生成的密钥对中的私钥采用第二密钥进行加密后,将所述私钥经过加密的密钥对输出给计算机网络侧;

所述计算机网络侧将所述私钥经过加密的密钥对与软件开发者标识关联;

所述计算机网络侧接收软件开发者发送的软件数据后,将对应软件开发者标识的经过加密的私钥及软件数据发送给硬件加密装置,由所述硬件加密装置对所述经过加密的私钥采用第二密钥解密后,再采用解密后的私钥对软件数据进行签名;

所述计算机网络侧将签名后的软件数据发送给软件开发者,使得软件开发者将签名后的软件数据加载到硬件用户锁,发送给软件使用者;

所述软件数据是软件开发者通过软件开发工具包SDK发送的,所述SDK是由计算机网络侧提供给软件开发者,软件开发者加载的。

2. 如权利要求1所述的方法,其特征在于,所述第二密钥为对称密钥或非对称密钥。

3. 如权利要求1所述的方法,其特征在于,所述计算机网络侧将所述私钥经过加密的密钥对与软件开发者标识关联之前,该方法还包括:

所述计算机网络侧经计算机网络侧的接入服务使得软件开发者接入到计算机网络侧并注册。

4. 如权利要求1所述的方法,其特征在于,所述计算机网络侧接收的软件数据为:软件开发者准备放入硬件用户锁的数据,使用硬件用户锁中的公钥对所述数据进行加密,得到软件数据;

所述SDK采用软件开发者的用户名及密码通过计算网络接入到计算机网络侧中;

所述硬件加密装置对所述经过加密的私钥采用第二密钥解密后,再采用解密后的私钥对软件数据进行签名的具体过程为:

所述SDK将软件数据发送给计算机网络侧请求签名;

计算机网络侧将对应软件开发者标识的所述经过加密的私钥发送给硬件加密装置,由所述硬件加密装置对所述经过加密的私钥采用第二密钥解密后,再采用解密后的私钥对软件数据进行签名后,将签名后的软件数据返回给所述SDK;

所述SDK将签名后的软件数据提供给软件开发者。

5. 一种硬件控制锁的托管装置,其特征在于,包括:设置单元、处理单元、收发单元、第二设置单元及第二收发单元,其中,

设置单元,用于生成密钥对及第二密钥,对生成的密钥对中的私钥采用第二密钥进行加密后,将所述私钥经过加密的密钥对通过收发单元输出给计算机网络侧的云端平台;

处理单元,用于通过收发单元接收到经过加密的私钥及软件数据,对经过加密的私钥采用第二密钥解密后,再采用解密后的私钥对软件数据进行签名后,通过收发单元发送给计算机网络侧的云端平台;

所述软件数据是软件开发者通过软件开发工具包SDK发送的,所述SDK是由计算机网络侧提供给软件开发者,软件开发者加载的;

第二设置单元,用于将私钥经过加密的密钥对与软件开发者标识关联;

第二收发单元,用于将接收到将对应软件开发者标识的经过加密的私钥及软件数据发

送给硬件加密装置;接收到签名后的软件数据后,将所述签名后的软件数据发送给软件开发者;

所述软件数据是软件开发者通过软件开发工具包SDK发送的,所述SDK是由计算机网络侧提供给软件开发者,软件开发者加载的。

6. 一种硬件控制锁的托管系统,其特征在于,包括硬件加密装置、计算机网络侧的云端平台及软件开发者实体,其中,

硬件加密装置,用于生成密钥对及第二密钥,对生成的密钥对中的私钥采用第二密钥进行加密后,将所述私钥经过加密的密钥对输出给计算机网络侧的云端平台;接收到经过加密的私钥及软件数据,对所述经过加密的私钥采用第二密钥解密后,再采用解密后的私钥对软件数据进行签名后,发送给计算机网络侧的云端平台;

计算机网络侧的云端平台,用于将私钥经过加密的密钥对与软件开发者标识关联;将接收到将对应软件开发者标识的所述经过加密的私钥及软件数据发送给硬件加密装置;接收到签名后的软件数据后,将所述签名后的软件数据发送给软件开发者实体;

软件开发者实体,用于向所述计算机网络侧的云端平台发送软件数据;接收所述计算机网络侧的云端平台发送的签名后的软件数据后,将所述签名后的软件数据加载到硬件用户锁中,发送给软件使用者;

所述软件数据是软件开发者实体通过软件开发工具包SDK发送的,所述SDK是由计算机网络侧提供给软件开发者实体,软件开发者实体加载的。

7. 如权利要求6所述的系统,其特征在于,所述系统还包括硬件锁集群服务器,具有多个,不同硬件锁集群服务器管理的硬件加密装置互为备份。

8. 如权利要求6或7所述的系统,其特征在于,还包括硬件锁代理服务器及数据库,其中,

硬件锁代理服务器,用于经计算机网络侧的接入服务接收软件开发者的硬件控制锁请求后,发送给所述计算机网络侧的云端平台;

数据库,用于计算机网络侧的云端平台在经计算机网络侧的接入服务接收到软件开发者的注册请求后,存储私钥经过加密的密钥对与软件开发者标识关联信息。

一种硬件控制锁的托管方法、装置及系统

技术领域

[0001] 本发明涉及对计算机软件安全性领域,特别涉及一种硬件控制锁的托管方法、装置及系统。

背景技术

[0002] 在计算机网络中,为了保证传输数据的合法性,都需要完备的证书体系。因此,硬件锁提供商提供了硬件锁,该硬件锁具有唯一的有效证书,用以标识身份。每次向硬件锁内输入数据,均会通过硬件锁的有效证书验证数据输入者的身份有效性及合法性,如果合法,则允许执行输入数据的操作,如果非法,则拒绝输入数据的操作。硬件锁包括硬件控制锁及硬件用户锁,硬件控制锁是由智能硬件及嵌入式系统组成,提供给软件开发者,用以向硬件用户锁签发授权数据;硬件用户锁是由智能硬件及嵌入式系统组成,由软件开发者将软件与其中的私钥一起打包售卖给最终的软件使用者,用于软件授权保护。

[0003] 图1为现有技术提供的软件开发者使用硬件锁的示意图,如图所示:软件开发者采用硬件控制锁生成对应输出数据端的多个硬件用户锁,对要发布的应用软件中的授权或/和重要算法等的的数据采用硬件用户锁的公钥进行加密后,再对加密的数据采用硬件控制锁中的私钥进行签名后,装载到硬件用户锁中,得到授权后的硬件用户锁发送给软件使用者。在这里,每个硬件控制锁在出厂前都会在内部生成一个非对称密钥对,密钥对中的私钥不能更替且不能被导出,用于对输入数据进行签名,密钥对中的公钥不能更替但可以导出给输出数据端,用于在后续对签名的数据进行验签。当输出数据端接收到数据之后,采用硬件控制锁中的公钥对数据进行验签通过后,再采用硬件用户锁的私钥对数据进行解密,并存储。在这里,每把硬件用户锁都会在内部生成一个非对称密钥对,密钥对中的私钥不能更替且不能导出,用于对输入数据进行解密,密钥对中的公钥不能更替可以导出,用于对输入数据进行加密。

[0004] 也就是说,在计算机网络中的输出数据端中具有硬件用户锁的公钥及硬件控制锁的私钥,依次对要输出的数据进行加密及签名,在计算机网络中的输入数据端具有硬件控制锁的公钥及硬件用户锁的私钥,依次对输入的数据进行解签及解密处理。

[0005] 图2为现有技术提供的软件使用过程图,如图所示,在软件发布的同时,会将软件中的一些授权或/和重要的数据写入到硬件锁中,一起提供给终端侧。当终端侧接收到后,启动软件,软件中的软件授权控制模块对锁访问模块进行控制,锁访问模块向软件的硬件锁发起授权验证请求,该请求携带终端侧输入的硬件控制锁的公钥及硬件用户锁的私钥;硬件锁的锁内入口模块(Entry)接收到并解析得到硬件控制锁的公钥及硬件用户锁的私钥后,由锁内的负载模块(Loader)对硬件锁中的安全数据区的数据进行验签及解密后,将数据返回给软件的锁访问模块,软件应用这些数据启动。

[0006] 采用这种方式由于软件必不可少的数据都被加密且签名后保存在硬件锁中等待验签及解密后才能使用,这样这一方面能够保证软件运行的安全性,软件不会被非法篡改;另一方面能够保证软件开发者的利益,使得非法终端侧由于无法对硬件锁中的数据解签及

解密,无法使用非授权的软件。但是,实现上述软件的授权方式,需要为派发的软件设置授权状态的硬件用户锁,目前硬件用户锁常常采用硬件锁提供商提供的手持式的硬件控制锁,由软件开发者将软件中的数据装载到硬件控制锁生成的硬件用户锁中,采用这种方式比较繁琐,不容易管理,常常无法保证不同软件的硬件锁的唯一性,给软件的发布制造了障碍。

发明内容

[0007] 有鉴于此,本发明实施例提供一种硬件控制锁的托管方法,该方法能够直接生成硬件锁,简单不繁琐且易于管理。

[0008] 本发明实施例还提供一种硬件控制锁的托管装置,该装置能够直接生成硬件锁,简单不繁琐且易于管理。

[0009] 本发明实施例还提供一种硬件控制锁的托管系统,该系统能够直接生成硬件锁,简单不繁琐且易于管理。

[0010] 根据上述目的,本发明是这样实现的:

[0011] 一种硬件控制锁的托管方法,在计算机网络侧设置硬件加密装置,该方法还包括:

[0012] 所述硬件加密装置生成密钥对及第二密钥,对生成的密钥对中的私钥采用第二密钥进行加密后,将所述私钥经过加密的密钥对输出给计算机网络侧;

[0013] 所述计算机网络侧将所述私钥经过加密的密钥对与软件开发者标识关联;

[0014] 所述计算机网络侧接收软件开发者发送的软件数据后,将对应开发者标识的经过加密的私钥及软件数据发送给硬件加密装置,由所述硬件加密装置对所述经过加密的私钥采用第二密钥解密后,再采用解密后的私钥对软件数据进行签名;

[0015] 所述计算机网络侧将签名后的软件数据发送给软件开发者,使得软件开发者将签名后的软件数据加载到硬件用户锁,发送给软件使用者。

[0016] 一种硬件控制锁的托管装置,包括:设置单元、处理单元及收发单元,其中,

[0017] 设置单元,用于生成密钥对及第二密钥,对生成的密钥对中的私钥采用第二密钥进行加密后,将所述私钥经过加密的密钥对通过收发单元输出给计算机网络侧的云端平台;

[0018] 处理单元,用于通过收发单元接收到经过加密的私钥及软件数据,对经过加密的私钥采用第二密钥解密后,再采用解密后的私钥对软件数据进行签名后,通过收发单元发送给计算机网络侧的云端平台。

[0019] 一种硬件控制锁的托管装置,包括:第二设置单元及第二收发单元,其中,

[0020] 第二设置单元,用于将私钥经过加密的密钥对与软件开发者标识关联;

[0021] 第二收发单元,用于将接收到将对应开发者标识的经过加密的私钥及软件数据发送给硬件加密装置;接收到签名后的软件数据后,将所述签名后的软件数据发送给软件开发者。

[0022] 一种硬件控制锁的托管系统,包括硬件加密装置、计算机网络侧的云端平台及请求者实体,其中,

[0023] 硬件加密装置,用于生成密钥对及第二密钥,对生成的密钥对中的私钥采用第二密钥进行加密后,将所述私钥经过加密的密钥对输出给计算机网络侧的云端平台;接收到

经过加密的私钥及软件数据,对所述经过加密的私钥采用第二密钥解密后,再采用解密后的私钥对软件数据进行签名后,发送给计算机网络侧的云端平台;

[0024] 计算机网络侧的云端平台,用于将私钥经过加密的密钥对与软件开发者标识关联;将接收到将对应开发者标识的所述经过加密的私钥及软件数据发送给硬件加密装置;接收到签名后的软件数据后,将所述签名后的软件数据发送给软件开发者;

[0025] 软件使用者,用于向所述计算机网络侧的云端平台发送软件数据;接收所述计算机网络侧的云端平台发送的签名后的软件数据后,将所述签名后的软件数据加载到硬件用户锁中,发送给软件使用者。

[0026] 由上述方案可以看出,本发明实施例在网络侧设置硬件加密装置,所述硬件加密装置生成密钥对及第二密钥,对生成的密钥对中的私钥采用第二密钥进行加密后,将所述私钥经过加密的密钥对输出给计算机网络侧;所述计算机网络侧将所述私钥经过加密的密钥对与软件开发者标识关联;所述计算机网络侧接收软件开发者发送的软件数据后,将对应开发者标识的经过加密的私钥及软件数据发送给硬件加密装置,由所述硬件加密装置对所述经过加密的私钥采用第二密钥解密后,再采用解密后的私钥对软件数据进行签名;所述计算机网络侧将所述签名后的软件数据发送给软件开发者,使得软件开发者将签名后的软件数据加载到硬件用户锁,发送给软件使用者。这样,软件开发者与计算机网络侧之间交互,就可以能够直接生成硬件用户锁,简单不繁琐且易于管理。

附图说明

[0027] 图1为现有技术提供的软件开发者使用硬件锁的示意图;

[0028] 图2为现有技术提供的软件使用过程图;

[0029] 图3为本发明实施例提供的硬件控制锁的托管方法流程图;

[0030] 图4为本发明实施例提供的硬件控制锁的托管装置结构一示意图;

[0031] 图5为本发明实施例提供的硬件控制锁的托管装置结构二示意图;

[0032] 图6为本发明实施例提供的硬件控制锁的托管系统结构示意图。

具体实施方式

[0033] 为使本发明的目的、技术方案及优点更加清楚明白,以下参照附图并举实施例,对本发明作进一步详细说明。

[0034] 本发明实施例为了使得软件开发者无需从硬件锁提供商获取硬件控制锁,且根据获取的硬件控制锁再生成硬件用户锁后,进行输入数据的硬件锁设置,造成了硬件锁提供商的管理复杂且繁琐,而且无法保证不同软件的硬件控制锁的唯一性的问题,采用了在网络侧设置硬件加密装置,所述硬件加密装置生成密钥对及第二密钥,对生成的密钥对中的私钥采用第二密钥进行加密后,将所述私钥经过加密的密钥对输出给计算机网络侧;所述计算机网络侧将所述私钥经过加密的密钥对与软件开发者标识关联;所述计算机网络侧接收软件开发者发送的软件数据后,将对应开发者标识的经过加密的私钥及软件数据发送给硬件加密装置,由所述硬件加密装置对所述经过加密的私钥采用第二密钥解密后,再采用解密后的私钥对软件数据进行签名;所述计算机网络侧将所述签名后的软件数据发送给软件开发者,使得软件开发者将签名后的软件数据及所述私钥经过加密的密钥对加载到硬件

用户锁,发送给软件使用者。

[0035] 这样,软件开发者与计算机网络侧之间交互,就可以能够直接生成硬件用户锁,简单不繁琐且易于管理。

[0036] 图3为本发明实施例提供的硬件锁生成方法流程图,在计算机网络侧设置了硬件加密装置,其具体步骤为:

[0037] 步骤301、硬件加密装置生成密钥对及第二密钥,对生成的密钥对中的私钥采用第二密钥进行加密后,将所述私钥经过加密的密钥对输出给计算机网络侧;

[0038] 在本发明中,采用第二密钥进行加密处理实际上就是生成对称密钥或非对称密钥,对所生成的密钥对加密,所生成的密钥不能查看其明文且明文也不能导出;所述第二密钥采用对称密钥时例如AES或DES密钥等,采用非对称密钥时例如ECC或RS密钥对;

[0039] 步骤302、计算机网络侧将所述私钥经过加密的密钥对与软件开发者标识关联;

[0040] 在本步骤中,所述软件开发者通过计算机网络,经计算机网络侧的接入服务接入到计算机网络侧并注册,再进行关联;

[0041] 步骤303、计算机网络侧接收软件开发者发送的软件数据后,将对应开发者标识的经过加密的私钥及软件数据发送给硬件加密装置,由所述硬件加密装置对所述经过加密的私钥采用第二密钥解密后,再采用解密后的私钥对软件数据进行签名;

[0042] 步骤304、所述计算机网络侧将签名后的软件数据发送给软件开发者,使得软件开发者将签名后的软件数据加载到硬件用户锁,发送给软件使用者;

[0043] 在本步骤中,软件开发者在使用硬件用户锁时,还需要获取所述私钥经过加密的密钥对中的公钥,获得所述私钥经过加密的密钥对中的公钥有两种方式,一种是计算机网络侧提供,一种为可以在本地获取。

[0044] 在该方法中,所述软件数据是软件开发者通过软件开发工具包(SDK)发送的,所述SDK是由计算机网络侧提供给软件开发者,软件开发者加载的。当然也可以通过请求者的计算机桌面软件、web浏览器或终端应用等等方式实现。

[0045] 在该方法中,所述硬件加密装置接收到软件开发者发送的软件数据后,采用软件开发者标识关联的经过加密的私钥对软件数据进行签名的具体过程为:

[0046] 软件开发者准备放入硬件用户锁的数据,使用硬件用户锁中的公钥对所述数据进行加密,得到软件数据;

[0047] 所述软件开发者使用SDK中的签名功能对软件数据进行签名,签名具体过程为:

[0048] SDK采用软件开发者的用户名及密码通过计算网络接入到计算机网络侧中;

[0049] SDK将软件数据发送给计算机网络侧请求签名;

[0050] 计算机网络侧将对应开发者标识的所述经过加密的私钥发送给硬件加密装置,由所述硬件加密装置对所述经过加密的私钥采用第二密钥解密后,再采用解密后的私钥对对软件数据进行签名后,将签名后的软件数据返回给SDK;

[0051] SDK将签名后的软件数据提供给软件开发者。

[0052] 这样,后续就可以将签名后的软件数据装载到硬件用户锁中,发送给软件使用者,这个过程与使用手持硬件控制锁的过程是一致的。

[0053] 也就是说,私钥经过加密的密钥对组成证书B,在软件开发者下载时,下载证书B及密钥对中的公钥,当然,为了保证安全性,计算机网络侧还可以对应软件开发者提供第二证

书,与证书B结合形成证书链C,与软件开发者进行关联后保存。

[0054] 软件开发者就可以将软件及硬件用户锁同时发布给软件使用者,软件使用者采用硬件用户锁中的密钥对中的公钥验证其中硬件用户锁中的数据签名的合法性,如果合法,再采用硬件用户锁中的私钥对加密数据进行解密,通过则表示输入数据正确,则将输入数据要求进行运算,并将结果返回给软件,用以软件运行。

[0055] 在该方法中,计算机网络侧包括硬件锁集群服务器,具有多个,不同硬件锁集群服务器存储的硬件加密装置互为备份。也就是说,每个硬件加密装置都有多个备用的硬件加密装置,以便某一硬件加密装置出现故障可以启动备用的硬件加密装置进行服务。在该方法中,不同硬件锁集群服务器可以作为异地灾备处理。这时,在发送所存储的硬件加密装置时,为一组硬件加密装置,所述一组硬件加密装置中具有一个服务的硬件加密装置及多个备份的硬件加密装置。

[0056] 在该方法中,还包括硬件锁代理服务器及数据库,其中,硬件锁代理服务器,用于经计算机网络侧的接入服务接收软件开发者的硬件控制锁请求后,发送给所述计算机网络侧的云端平台;数据库,用于计算机网络侧的云端平台经计算机网络侧的接入服务接收到软件开发者的注册请求后,存储私钥经过加密的密钥对与软件开发者标识关联信息。

[0057] 图4为本发明实施例提供的硬件控制锁的托管装置结构一示意图,就是硬件加密装置,包括设置单元、处理单元及收发单元,其中,

[0058] 设置单元,用于生成密钥对及第二密钥,对生成的密钥对中的私钥采用第二密钥进行加密后,将所述私钥经过加密的密钥对通过收发单元输出给计算机网络侧的云端平台;

[0059] 处理单元,用于通过收发单元接收到经过加密的私钥密钥及软件数据,对所述经过加密的私钥采用第二密钥解密后,再采用解密后的私钥对软件数据进行签名后,通过收发单元发送给计算机网络侧的云端平台。

[0060] 图5为本发明实施例提供的硬件控制锁的托管装置结构二意图,就是计算机网络侧的云端平台,包括:第二设置单元及第二收发单元,其中,

[0061] 第二设置单元,用于将私钥经过加密的密钥对与软件开发者标识关联;

[0062] 第二收发单元,用于将接收到将对应开发者标识的经过加密的私钥及软件数据发送给硬件加密装置;接收到签名后的软件数据后,将所述签名后的软件数据发送给软件开发者。

[0063] 图6为本发明实施例提供的硬件控制锁的托管系统结构图,包括硬件加密装置、计算机网络侧的云端平台及请求者实体,其中,

[0064] 硬件加密装置,用于生成密钥对及第二密钥,对生成的密钥对中的私钥采用第二密钥进行加密后,将所述私钥经过加密的密钥对输出给计算机网络侧的云端平台;接收到经过加密的私钥密钥及软件数据,对所述经过加密的私钥采用第二密钥解密后,再采用解密后的私钥对软件数据进行签名后,发送给计算机网络侧的云端平台;

[0065] 计算机网络侧的云端平台,用于将私钥经过加密的密钥对与软件开发者标识关联;将接收到将对应开发者标识的经过加密的私钥及软件数据发送给硬件加密装置;接收到签名后的软件数据后,将所述签名后的软件数据发送给软件开发者;

[0066] 软件使用者,用于向所述计算机网络侧的云端平台发送软件数据;接收所述计算

机网络侧的云端平台发送的签名后的软件数据后,将所述签名后的软件数据加载到硬件用户锁中,发送给软件使用者。

[0067] 在该系统中,还包括硬件锁集群服务器,具有多个,不同硬件锁集群服务器管理的硬件加密装置互为备份。

[0068] 在该系统中,还包括硬件锁代理服务器及数据库,其中,

[0069] 硬件锁代理服务器,用于经计算机网络侧的接入服务接收软件开发者的硬件控制锁请求后,发送给所述计算机网络侧的云端平台;

[0070] 数据库,用于计算机网络侧的云端平台在经计算机网络侧的接入服务接收到软件开发者的注册请求后,存储私钥经过加密的密钥对与软件开发者标识关联信息。

[0071] 在这里,硬件控制锁集群服务器具有多个,形成了云托管硬件锁系统,硬件锁代理服务器也具有多个,每个硬件锁代理服务器通过计算机网络都可以与其中的一个硬件锁集群服务器进行交互。

[0072] 软件开发者采用本发明实施例,根据注册的账号登录该系统,从而可以在线使用硬件锁提供商托管的硬件加密装置。

[0073] 本发明实施例提供的系统具备以下基础服务:1、用户注册功能,该功能面向软件开发者,只有在系统上注册的软件开发者才能使用该系统提供的托管硬件加密装置功能;2、托管硬件加密装置功能,这与背景技术中采用的手持硬件控制锁具有相同的功能,核心就是使用加密后的私钥进行数据签名功能;3、该系统具备安全通信信道及数据加密过程,确保数据在计算机网络上安全正确的传输;4、该系统提供了SDK、PC桌面软件、Web浏览器或/和手机应用等等方式,以便软件开发者可以方便在线使用该系统。

[0074] 从上述方案可以看出,本发明实施例就可以解决以下问题:软件开发者的硬件控制锁丢失或损毁,重新向硬件锁提供商申请定制硬件控制锁的滞后性问题;硬件锁提供商向使用者提供特定硬件控制锁,比如该特定硬件控制锁携带有软件开发者身份信息及软件安全标识信息的过程中可能造成的丢失、漏发、重复及物流等管理或交付安全问题;对于个人开发者则无需随时携带硬件控制锁进行开发测试,只需要能够接入计算机网络就可以随时随地地使用托管硬件加密装置;软件开发者无需担心硬件控制锁的丢失,以及由此带来的损失。

[0075] 以上举较佳实施例,对本发明的目的、技术方案和优点进行了进一步详细说明,所应理解的是,以上所述仅为本发明的较佳实施例而已,并不用以限制本发明,凡在本发明的精神和原则之内,所作的任何修改、等同替换和改进等,均应包含在本发明的保护范围之内。

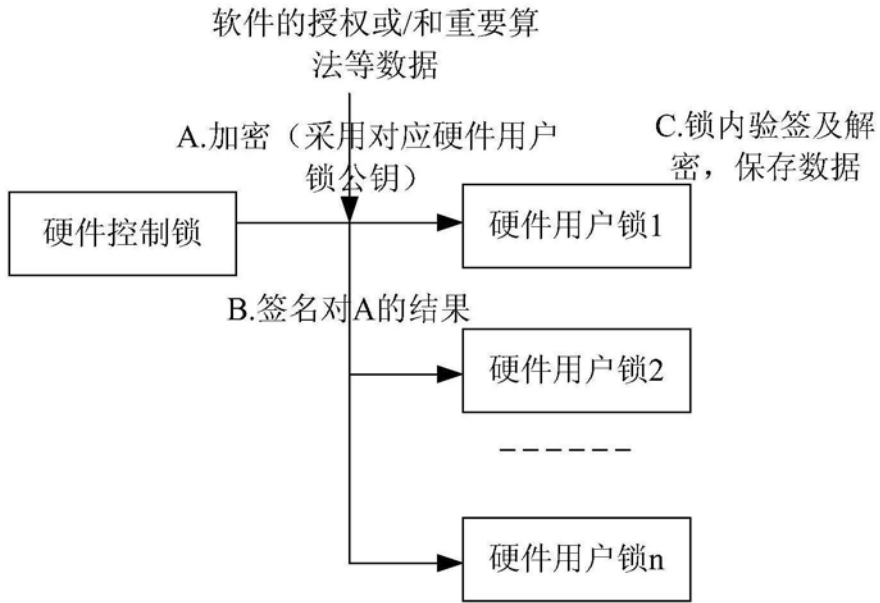


图1

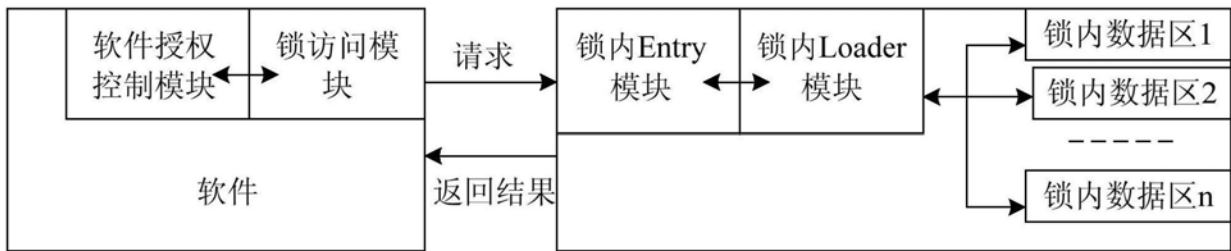


图2

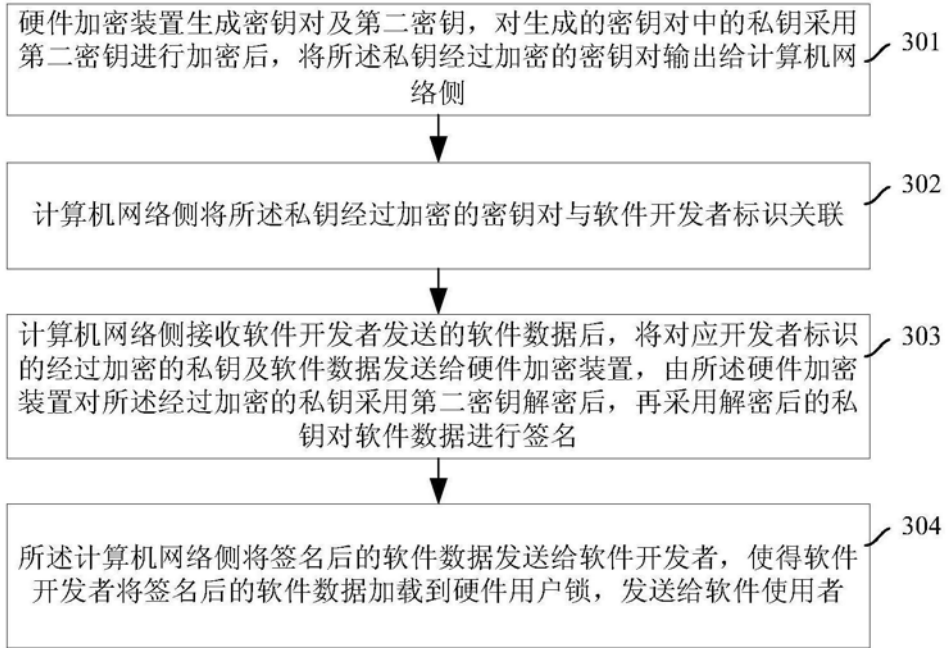


图3

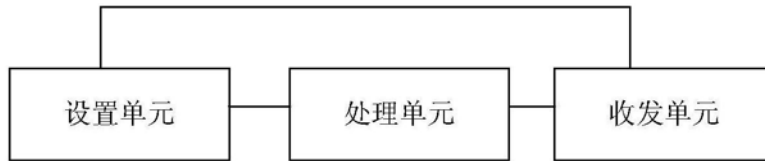


图4



图5

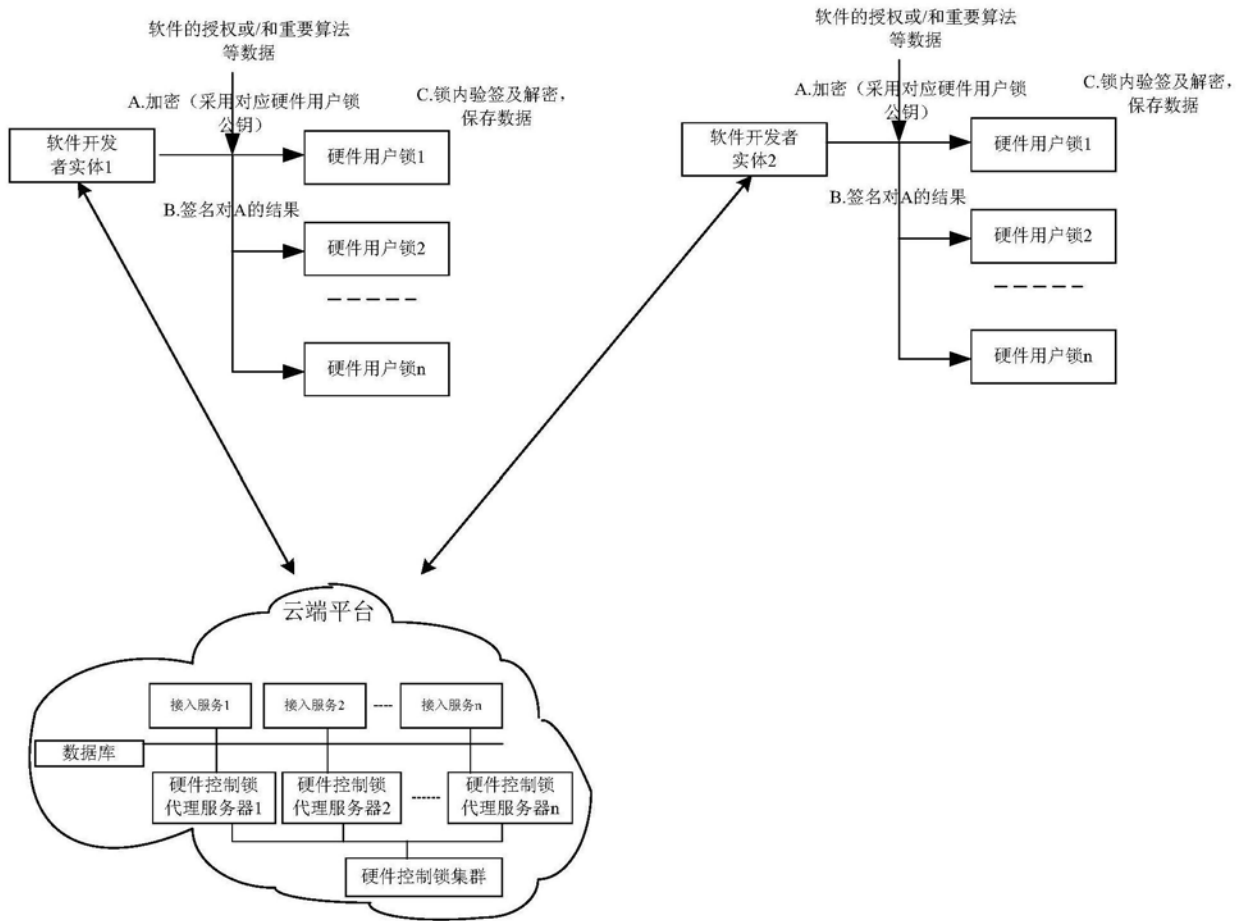


图6