(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 117666977 A
(43)申请公布日 2024.03.08

(21)申请号 202311668078.6

(22)申请日 2023.12.07

(71)申请人 矩阵时光数字科技有限公司
地址 210000 江苏省南京市中国(江苏)自由贸易试验区南京片区江淼路88号腾飞大厦b座11层

(72)发明人 赵呈洋 史钦锋 曹飞 赵健

(51)Int.Cl.
G06F 3/12(2006.01)
G06F 21/60(2013.01)
G06F 21/31(2013.01)
G06F 21/64(2013.01)
H04L 9/08(2006.01)
H04L 9/32(2006.01)
H04L 9/40(2022.01)

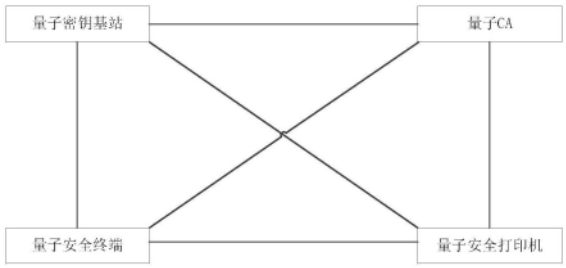
权利要求书3页 说明书9页 附图2页

(54)发明名称

一种全域量子安全打印系统及其工作方法

(57)摘要

本发明公开了一种全域量子安全打印系统及其工作方法,该系统包括量子安全终端、量子安全打印机、量子CA及量子密钥基站。该方法为:量子安全打印机及量子安全终端均向量子CA进行身份登记,获得量子身份,量子安全打印机开机后,量子安全终端和量子CA对量子安全打印机身份进行认证,而后量子安全终端向量子安全打印机发送待打印数据,量子安全打印机和量子CA对量子安全终端身份认证成功后,量子安全打印机会对待打印数据进行认证,认证成功后,进行数据打印。本发明构建量子执行环境,使得信息的安全性得到有效的保障;本发明增加身份识别功能和数据认证功能,保证数据信息来源合法的同时,也保证了数据信息的真实性。



CN 117666977 A

1.一种全域量子安全打印系统,其特征在于,所述系统包括量子安全终端、量子安全打印机、量子CA及量子密钥基站,所述量子安全终端、量子安全打印机均分别连接所述量子CA和所述量子密钥基站,所述量子CA与所述量子密钥基站相互连接,所述量子安全终端与所述量子安全打印机相互连接;

所述量子安全终端用于待打印数据的生成及量子安全打印机的身份认证;

所述量子CA用于身份的颁发及认证;

所述量子密钥基站用于量子密钥的生成及分发;

所述量子安全打印机用于执行数据打印,包括依次连接的网络通信模块、量子执行模块及数据打印模块;

所述网络通信模块用于执行所述量子安全打印机与外界设备的数据通信;

所述量子执行模块用于待打印数据的认证及量子安全终端的身份认证;

所述数据打印模块用于接收认证后的数据,并执行打印。

2.根据权利要求1所述的一种全域量子安全打印系统,其特征在于,所述量子执行模块包括量子加解密模块、量子密钥管理模块及量子身份认证模块,所述量子加解密模块与所述量子密钥管理模块、网络通信模块、数据打印模块分别连接,所述量子密钥管理模块与所述网络通信模块相互连接,所述量子身份认证模块与所述网络通信模块、量子密钥管理模块分别连接;

所述量子密钥管理模块用于量子密钥的生成及分发;

所述量子加解密模块中预置有加密算法,用于数据的加解密及认证;

所述量子身份认证模块用于量子安全终端的身份认证。

3.根据权利要求2所述的一种全域量子安全打印系统,其特征在于,所述量子执行模块还包括打印历史管理模块,所述打印历史管理模块与所述量子加解密模块连接,所述打印历史管理模块用于待打印数据的存储及打印历史记录的保存。

4.根据权利要求2或3所述的一种全域量子安全打印系统,其特征在于,所述量子安全终端、量子CA、量子密钥管理模块预置有相同的密钥池。

5.一种基于权利要求4所述的一种全域量子安全打印系统的工作方法,其特征在于,所述方法包括以下步骤:

步骤一、量子安全打印机及量子安全终端均向量子CA进行身份登记,量子CA向量子安全打印机颁发量子身份ID_a,量子CA向量子安全终端颁发量子身份ID_b,颁发完成后,量子安全打印机和量子CA均存储有量子身份ID_a,量子安全终端和量子CA均存储有量子身份ID_b;

步骤二、量子安全打印机进行用户身份认证,用户身份认证成功后,量子安全打印机开机;

步骤三、量子安全终端和量子CA基于量子身份ID_a对量子安全打印机进行身份认证,量子安全终端和量子CA对量子安全打印机身份认证均通过后,量子安全终端向量子安全打印机发送待打印数据;

步骤四、量子安全打印机和量子CA基于量子身份ID_b对量子安全终端进行身份认证,量子安全打印机和量子CA对量子安全终端身份认证均通过后,量子安全打印机对接收到的待打印数据进行认证,待打印数据认证通过后,进行待打印数据的打印。

6.根据权利要求5所述的一种全域量子安全打印系统的工作方法,其特征在于,所述方

法还包括：

步骤五、待打印数据完成打印后，量子安全打印机进行用户身份认证，用户身份认证成功后，量子安全打印机关机；

其中，步骤二和步骤五中，所述量子安全打印机通过生物识别方法进行用户身份认证。

7.根据权利要求5所述的一种全域量子安全打印系统的工作方法，其特征在于，步骤三中，所述量子身份ID_a包括公开身份ID_1和隐私身份ID_2，所述量子安全终端和所述量子CA基于量子身份ID_a对所述量子安全打印机进行身份认证的流程如下：

流程a1、量子安全打印机基于本地的隐私身份ID_2生成一次性身份$OTID_1$，量子CA基于本地的隐私身份ID_2生成一次性身份$OTID_2$；

流程a2、量子安全打印机基于本地公开身份ID_1及一次性身份$OTID_1$生成文件Sign，基于文件Sign，量子安全终端和量子CA对量子安全打印机的身份进行认证；

流程a3、量子安全终端和量子CA对量子安全打印机身份认证均通过后，量子安全终端向量子安全打印机发送待打印数据。

8.根据权利要求5所述的一种全域量子安全打印系统的工作方法，其特征在于，步骤四中，所述量子身份ID_b包括公开身份ID_3和隐私身份ID_4，所述量子安全打印机和所述量子CA基于量子身份ID_b对所述量子安全终端进行身份认证的流程如下：

流程b1、量子安全终端基于本地的隐私身份ID_4生成一次性身份$OTID_3$，量子CA基于本地的隐私身份ID_4生成一次性身份$OTID_4$；

流程b2、量子安全终端基于本地公开身份ID_3及一次性身份$OTID_3$生成文件Sign,,基于文件Sign,,量子安全打印机和量子CA对量子安全终端的身份进行认证；

流程b3、量子安全打印机和量子CA对量子安全终端身份认证均通过后，量子安全打印机对接收到的待打印数据进行认证。

9.根据权利要求4所述的一种全域量子安全打印系统的工作方法，其特征在于，步骤三中，所述量子安全终端向所述量子安全打印机发送待打印数据进一步包括：

所述量子安全终端对待打印数据data进行哈希计算，得到哈希值H(data)，所述量子安全终端从本地提取量子密钥r对待打印数据data及哈希值H(data)进行加密，得到加密数据$r \oplus [data, H(data)]$，并记录量子密钥r的位置标识，而后将加密数据$r \oplus [data, H(data)]$及密钥r的位置标识一并发送至所述量子安全打印机。

10.根据权利要求9所述的一种全域量子安全打印系统的工作方法，其特征在于，步骤四中，所述量子安全打印机对接收到的待打印数据进行认证进一步包括：

所述量子安全打印机中的量子加解密模块接收来自所述量子安全终端的加密数据$r \oplus [data, H(data)]$及密钥r的位置标识，所述量子加解密模块向所述量子密钥管理模块发送获取量子密钥的请求g及密钥r的位置标识，所述量子密钥管理模块根据请求g及密钥r的位置标识从本地密钥池拉取相应位置处的密钥，并将得到的密钥r′发送给所述量子加解密模块，所述量子加解密模块使用密钥r′对加密数据$r \oplus [data, H(data)]$进行解密，得到待打印数据data′和哈希值H(data)′，而后对解密得到的待打印数据data′进行哈希计算，得到哈希值H(data)″，将计算得到的哈希值H(data)″与解密得到的哈希值H(data)′进行比对，若比对相等，则解密后得到的待打印数据data′认证通过，否则认证不通过；

解密后得到的待打印数据data′认证通过后,所述量子加解密模块将待打印数据data′发送至所述打印历史管理模块和所述数据打印模块,所述数据打印模块接收待打印数据data′,并进行数据打印,所述打印历史管理模块对接收到的待打印数据data′进行存储,同时对打印历史记录也进行保存。

一种全域量子安全打印系统及其工作方法

技术领域

[0001] 本发明涉及信息安全领域,具体涉及一种全域量子安全打印系统及其工作方法。

背景技术

[0002] 现代打印机越来越智能化与网络化,打印业务随处可见,因电子产品需要电源并且很难保存几十年之久,打印业务中短期会持续大量存在。打印业务的安全涉及打印机硬件设备安全、信息流转安全、电源配件安全、环境安全等诸多事项。

[0003] 现有打印系统一般包括三大部分,分别是数据源头、网络传输及打印机。

[0004] 数据源头:一般是计算机(电脑、手机等智能终端设备),普通终端容易因攻击,而导致还未进入打印环节的数据泄密。

[0005] 网络传输:信息传输阶段,容易受到监听、拦截、篡改等风险。

[0006] 打印机:内部数据的安全性得不到有效保障,且还缺乏数据认证能力,使得数据的真实性受到质疑,同时也缺乏身份认证能力,使得数据来源的合法性无法确定。以激光打印机为例,传统激光打印机可以包括供电系统、直流控制系统、接口系统、激光扫描系统、成像系统及搓纸系统,系统之间是直接进行通信的,任何两个系统之间的数据被挟持都会导致该打印机所涉及到的信息安全受到威胁,且还缺乏数据认证能力,使得数据的真实性受到质疑,同时也缺乏身份认证能力,使得数据来源的合法性无法确定。

发明内容

[0007] 发明目的:本发明目的是提供一种全域量子安全打印系统及其工作方法,解决了当前打印机工作使用过程中所存在的信息安全问题。本发明构建量子执行环境,使得信息的安全性得到有效的保障;本发明增加身份识别功能,保证数据信息的来源合法,使得信息的安全性得到进一步的提升;本发明增加数据认证功能,使得数据信息的真实性得到保障。

[0008] 技术方案:一种全域量子安全打印系统,所述系统包括量子安全终端、量子安全打印机、量子CA及量子密钥基站,所述量子安全终端、量子安全打印机均分别连接所述量子CA和所述量子密钥基站,所述量子CA与所述量子密钥基站相互连接,所述量子安全终端与所述量子安全打印机相互连接;

[0009] 所述量子安全终端用于待打印数据的生成及量子安全打印机的身份认证;

[0010] 所述量子CA用于身份的颁发及认证;

[0011] 所述量子密钥基站用于量子密钥的生成及分发;

[0012] 所述量子安全打印机用于执行数据打印,包括依次连接的网络通信模块、量子执行模块及数据打印模块;

[0013] 所述网络通信模块用于执行所述量子安全打印机与外界设备的数据通信;

[0014] 所述量子执行模块用于待打印数据的认证及量子安全终端的身份认证;

[0015] 所述数据打印模块用于接收认证后的数据,并执行打印。

[0016] 进一步地,所述量子执行模块包括量子加解密模块、量子密钥管理模块及量子身

份认证模块,所述量子加解密模块与所述量子密钥管理模块、网络通信模块、数据打印模块分别连接,所述量子密钥管理模块与所述网络通信模块相互连接,所述量子身份认证模块与所述网络通信模块、量子密钥管理模块分别连接;

[0017] 所述量子密钥管理模块用于量子密钥的生成及分发;

[0018] 所述量子加解密模块中预置有加密算法,用于数据的加解密及认证;

[0019] 所述量子身份认证模块用于量子安全终端的身份认证。

[0020] 进一步地,所述量子执行模块还包括打印历史管理模块,所述打印历史管理模块与所述量子加解密模块连接,所述打印历史管理模块用于待打印数据的存储及打印历史记录的保存。

[0021] 进一步地,所述量子安全终端、量子CA、量子密钥管理模块预置有相同的密钥池。

[0022] 一种全域量子安全打印系统的工作方法,所述方法包括以下步骤:

[0023] 步骤一、量子安全打印机及量子安全终端均向量子CA进行身份登记,量子CA向量子安全打印机颁发量子身份ID_a,量子CA向量子安全终端颁发量子身份ID_b,颁发完成后,量子安全打印机和量子CA均存储有量子身份ID_a,量子安全终端和量子CA均存储有量子身份ID_b;

[0024] 步骤二、量子安全打印机进行用户身份认证,用户身份认证成功后,量子安全打印机开机;

[0025] 步骤三、量子安全终端和量子CA基于量子身份ID_a对量子安全打印机进行身份认证,量子安全终端和量子CA对量子安全打印机身份认证均通过后,量子安全终端向量子安全打印机发送待打印数据;

[0026] 步骤四、量子安全打印机和量子CA基于量子身份ID_b对量子安全终端进行身份认证,量子安全打印机和量子CA对量子安全终端身份认证均通过后,量子安全打印机对接收到的待打印数据进行认证,待打印数据认证通过后,进行待打印数据的打印。

[0027] 进一步地,所述方法还包括:

[0028] 步骤五、待打印数据完成打印后,量子安全打印机进行用户身份认证,用户身份认证成功后,量子安全打印机关机;

[0029] 其中,步骤二和步骤五中,所述量子安全打印机通过生物识别方法进行用户身份认证。

[0030] 进一步地,步骤三中,所述量子身份ID_a包括公开身份ID_1和隐私身份ID_2,所述量子安全终端和所述量子CA基于量子身份ID_a对所述量子安全打印机进行身份认证的流程如下:

[0031] 流程a1、量子安全打印机基于本地的隐私身份ID_2生成一次性身份$OTID_1$,量子CA基于本地的隐私身份ID_2生成一次性身份$OTID_2$;

[0032] 流程a2、量子安全打印机基于本地公开身份ID_1及一次性身份$OTID_1$生成文件Sign,基于文件Sign,量子安全终端和量子CA对量子安全打印机的身份进行认证;

[0033] 流程a3、量子安全终端和量子CA对量子安全打印机身份认证均通过后,量子安全终端向量子安全打印机发送待打印数据。

[0034] 进一步地,步骤四中,所述量子身份ID_b包括公开身份ID_3和隐私身份ID_4,所述量子安全打印机和所述量子CA基于量子身份ID_b对所述量子安全终端进行身份认证的流程如

下：

[0035] 流程b1、量子安全终端基于本地的隐私身份ID_4生成一次性身份$OTID_3$，量子CA基于本地的隐私身份ID_4生成一次性身份$OTID_4$；

[0036] 流程b2、量子安全终端基于本地公开身份ID_3及一次性身份$OTID_3$生成文件$Sign_,$，基于文件Sign,，量子安全打印机和量子CA对量子安全终端的身份进行认证；

[0037] 流程b3、量子安全打印机和量子CA对量子安全终端身份认证均通过后，量子安全打印机对接收到的待打印数据进行认证。

[0038] 进一步地，步骤三中，所述量子安全终端向所述量子安全打印机发送待打印数据进一步包括：

[0039] 所述量子安全终端对待打印数据data进行哈希计算，得到哈希值H(data)，所述量子安全终端从本地提取量子密钥r对待打印数据data及哈希值H(data)进行加密，得到加密数据$r \oplus [data, H(data)]$，并记录量子密钥r的位置标识，而后将加密数据$r \oplus [data, H(data)]$及密钥r的位置标识一并发送至所述量子安全打印机。

[0040] 进一步地，步骤四中，所述量子安全打印机对接收到的待打印数据进行认证进一步包括：

[0041] 所述量子安全打印机中的量子加解密模块接收来自所述量子安全终端的加密数据r⊕[data,H(data)]及密钥r的位置标识，所述量子加解密模块向所述量子密钥管理模块发送获取量子密钥的请求g及密钥r的位置标识，所述量子密钥管理模块根据请求g及密钥r的位置标识从本地密钥池拉取相应位置处的密钥，并将得到的密钥r′发送给所述量子加解密模块，所述量子加解密模块使用密钥r′对加密数据$r \oplus [data, H(data)]$进行解密，得到待打印数据data′和哈希值H(data)′，而后对解密得到的待打印数据data′进行哈希计算，得到哈希值H(data)″，将计算得到的哈希值H(data)″与解密得到的哈希值H(data)′进行比对，若比对相等，则解密后得到的待打印数据data′认证通过，否则认证不通过；

[0042] 解密后得到的待打印数据data′认证通过后，所述量子加解密模块将待打印数据data′发送至所述打印历史管理模块和所述数据打印模块，所述数据打印模块接收待打印数据data′，并进行数据打印，所述打印历史管理模块对接收到的待打印数据data′进行存储，同时对打印历史记录也进行保存。

[0043] 本发明的有益效果：

[0044] 1、本发明基于量子执行模块构建量子执行环境，实现硬件、软件的安全隔离，可以有效防御各种软件攻击，使得信息的安全性得到有效的保障；

[0045] 2、本发明基于量子执行模块实现身份认证功能，保证数据信息的来源合法，进一步提高信息的安全性；

[0046] 3、本发明基于量子执行模块实现数据认证功能，使得数据信息的真实性得到保障；

[0047] 4、本发明采用量子密钥进行数据信息的加解密，量子密钥一次一密，确保数据信息传输过程中的安全。

附图说明

[0048] 图1为本发明一种全域量子安全打印系统的结构组成示意图;

[0049] 图2为本发明量子安全打印机的结构组成示意图;

[0050] 图3为本发明一种全域量子安全打印系统的工作方法的步骤框图。

具体实施方式

[0051] 下面结合附图和实施例对本发明做进一步描述:

[0052] 现有打印系统一般包括三大部分,分别是数据源头、网络传输及打印机。数据源头:一般是计算机(电脑、手机等智能终端设备),普通终端容易因攻击,而导致还未进入打印环节的数据泄密;网络传输:信息传输阶段,容易受到监听、拦截、篡改等风险;打印机:内部数据的安全性得不到有效保障,且还缺乏数据认证能力,使得数据的真实性受到质疑,同时也缺乏身份认证能力,使得数据来源的合法性无法确定。

[0053] 以激光打印机为例,传统激光打印机可以包括供电系统、直流控制系统、接口系统、激光扫描系统、成像系统及搓纸系统,系统之间是直接进行通信的,任何两个系统之间的数据被挟持都会导致该打印机所涉及到的信息安全受到威胁,且还缺乏数据认证能力,使得数据的真实性受到质疑,同时也缺乏身份认证能力,使得数据来源的合法性无法确定。其中,接口系统作为打印机和计算机连接的桥梁,它负责把计算机传递过来的一定格式的数据翻译成DC板能处理的格式,并传递给DC板。DC板是直流控制系统,主要用来协调和控制打印机的各系统之间的工作,例如:从接口系统接收数据,驱动控制激光扫描单元、测试传感器、控制交直流电的分布、过压/欠流保护、节能模式、控制高压电的分布等。

[0054] 本发明在接口系统中部署有量子执行模块,基于量子执行模块构建量子执行环境,实现软硬件一体化的安全隔离,可以有效防御各种软件攻击,在保障数据安全性的同时,也因量子执行模块具有数据认证能力和身份认证能力,在确保数据真实性的同时,也确保了数据的来源合法。

[0055] 普通PC或移动端所使用的核心元器件、芯片、操作系统、APP来源多样,这些硬件或软件所存在的后门、漏洞,都有可能导致数据泄密,如:1、应用软件攻击,通过输入法窃取用户键盘输入信息,杀毒软件完全被绕过;2、操作系统攻击,操作系统收集各种错误日志主动上报的同时,也会将用户隐私数据上报;3、硬件芯片攻击,CPU自主传输数据至厂商。

[0056] 本发明将普通PC或移动端升级为量子安全终端,量子安全终端具有唯一的与外部互联网或专网连接的出入口,所有进出数据都会被强制量子加解密。

[0057] 如图1所示,本发明提出一种全域量子安全打印系统,该系统包括量子安全终端、量子安全打印机、量子CA及量子密钥基站,量子安全终端、量子安全打印机均分别连接量子CA和量子密钥基站,量子CA与量子密钥基站相互连接,量子安全终端与量子安全打印机相互连接。

[0058] 量子安全终端用于待打印数据的生成和量子安全打印机的身份认证。量子安全终端可以包括对外执行数据通信的网络通信模块、量子执行模块及打印数据生成模块。其中,打印数据生成模块用于本发明中待打印数据的生成或产生;量子安全终端中的量子执行模块与量子安全打印机中的量子执行模块相同,用于数据加解密,到量子CA处获取量子安全终端的量子身份,到量子密钥基站处预置密钥池,对量子安全打印机进行身份认证,配合量

子安全打印机和量子CA对量子安全终端进行身份认证,配合量子安全打印机实现待打印数据的认证等。

[0059] 量子CA用于身份的颁发及认证。本发明量子CA可以是例如专利数字证书生成、身份认证方法及量子CA认证中心与系统(202210185146.2)中所提到的CA认证中心。

[0060] 量子密钥基站用于量子密钥的生成及分发。本发明量子密钥基站可以是例如专利一种量子安全密钥分发方法及系统(202211092604.4)中所提到的密钥管理系统。

[0061] 如图2所示,量子安全打印机用于执行数据打印,包括依次连接的网络通信模块、量子执行模块及数据打印模块。

[0062] 网络通信模块与量子安全终端、量子CA及量子密钥基站分别连接,用于网络通信。

[0063] 数据打印模块用于接收认证后的数据,并执行打印。

[0064] 量子执行模块用于待打印数据的认证及量子安全终端的身份认证。

[0065] 量子执行模块包括量子加解密模块、量子密钥管理模块及量子身份认证模块,量子加解密模块与量子密钥管理模块、网络通信模块、数据打印模块分别连接,量子密钥管理模块与网络通信模块相互连接,量子身份认证模块与网络通信模块、量子密钥管理模块分别连接。

[0066] 量子执行模块还包括打印历史管理模块,打印历史管理模块与量子加解密模块连接,打印历史管理模块用于待打印数据的存储及打印历史记录的保存。

[0067] 量子加解密模块、量子密钥管理模块、量子身份认证模块均通过网络通信模块实现对外通信,量子加解密模块、量子身份认证模块均从量子密钥管理模块中获取量子密钥。

[0068] 量子密钥管理模块主要用于量子密钥的生成及分发。在本发明中,量子密钥管理模块还会进行量子密钥的安全检查及量子密钥的销毁。量子密钥管理模块可通过QKD单光子模式分发的密钥系统或通过物理线下预置的光量子产生真随机数,这里预置密钥包括线上线下两种方式,线下方式包括优盘等,线上方式包括从专有量子密钥传输网络传输密钥,例如,本发明量子密钥管理模块通过网络通信模块与量子密钥基站连接,量子密钥管理模块可以从量子密钥基站中获取密钥或补充密钥。量子密钥的安全检查是确保源头密钥与接收方密钥的一致性。密钥销毁是会话密钥使用一次后删除。

[0069] 本发明量子密钥管理模块、量子安全终端、量子CA均到量子密钥基站获取量子密钥,从而预置相同的密钥池,后续密钥池的补充也是由量子密钥基站进行补充的。

[0070] 量子加解密模块中预置有加密算法,用于数据的加解密及认证。量子加解密模块通过量子密钥配合一次一密实现对要发送的数据进行加密或对接收到的数据进行解密,同时,配合哈希算法对数据一致性进行认证。

[0071] 量子身份认证模块用于量子安全终端的身份认证。量子安全打印机启动,进行数据打印前,量子安全终端及量子CA需要对量子安全打印机的身份进行认证,认证通过后,量子安全打印机可以接收待打印数据。在接收到待打印数据后,量子安全打印机与量子CA需要再对量子安全终端的身份进行认证。量子安全打印机通过量子身份认证模块实现其身份的认证,及后续量子安全终端身份的认证。

[0072] 打印历史管理模块用于待打印数据的存储及打印历史记录的保存。打印历史记录包括打印文件数量、打印时间、打印文档标题等,打印历史记录方便后续的追踪查找。打印历史管理模块部署于量子执行模块中,只能对已存储的数据进行读取,不能进行修改,这样

可以确保所存储的打印数据内容及打印历史记录的不可篡改性和安全性。

[0073] 如图3所示,本发明还提出一种全域量子安全打印系统的工作方法,该方法包括以下步骤:

[0074] 步骤一、量子安全打印机及量子安全终端均向量子CA进行身份登记,量子CA向量子安全打印机颁发量子身份ID_a,量子CA向量子安全终端颁发量子身份ID_b,颁发完成后,量子安全打印机和量子CA均存储有量子身份ID_a,量子安全终端和量子CA均存储有量子身份ID_b。

[0075] 量子安全打印机中的量子身份认证模块通过网络通信模块向量子CA进行身份登记,量子CA向其颁发量子安全打印机的量子身份ID_a,量子安全打印机的量子身份ID_a包括公开身份ID_1和隐私身份ID_2,颁发完成后,量子CA和量子安全打印机中的量子身份认证模块均存储有量子安全打印机的公开身份ID_1和隐私身份ID_2。

[0076] 步骤二、量子安全打印机进行用户身份认证,用户身份认证成功后,量子安全打印机开机。

[0077] 量子安全打印机可通过生物识别方法对用户的身份进行认证,例如:指纹识别、人脸识别等,此处的用户,即为量子安全打印机授权的管理人员,若量子安全打印机对用户身份认证失败,则量子安全打印机无法正常开机。

[0078] 步骤三、量子安全终端和量子CA基于量子身份ID_a对量子安全打印机进行身份认证,量子安全终端和量子CA对量子安全打印机身份认证均通过后,量子安全终端向量子安全打印机发送待打印数据。

[0079] 量子安全终端与量子CA基于量子身份ID_a对量子安全打印机进行身份认证的流程如下:

[0080] 流程a1、量子安全打印机基于本地的隐私身份ID_2生成一次性身份$OTID_1$,量子CA基于本地的隐私身份ID_2生成一次性身份$OTID_2$。

[0081] 量子安全打印机中的量子身份认证模块基于本地的隐私身份ID_2生成一次性身份$OTID_1$,具体过程如下:

[0082] 量子身份认证模块从本地获取一个随机数用于生成不可约多项式P_1。量子身份认证模块与量子CA之间共享量子密钥x、y、z的位置标识,本发明密钥的位置标识即为:第M位开始取L个密钥。例如,预置的密钥池中有一组1024位长度的随机数,密钥a的位置信息为从第6位开始,长度为128;密钥b的位置信息为从140位开始,长度为128;密钥c的位置信息为从300位开始,长度为128。下文所涉及的密钥的位置标识也均表示相同的意思。

[0083] 量子身份认证模块基于共享量子密钥x、y、z的位置标识从量子密钥管理模块的密钥池中拉取相应位置处的量子密钥,得到量子密钥x、y、z。量子CA基于共享量子密钥x、y、z的位置标识从本地密钥池中拉取相应位置处的量子密钥,得到量子密钥x、y、z。

[0084] 量子身份认证模块基于不可约多项式P_1及量子密钥x得到哈希函数H_1,并基于该哈希函数H_1对本地的隐私身份ID_2做哈希计算,得到哈希值$H(ID_2)$,而后再使用量子密钥y对哈希值$H(ID_2)$进行加密,得到一次性身份$OTID_1$,即:

[0085] $$OTID_1 = H(ID_2) \oplus y。$$

[0086] 不可约多项式P_1除最高项以外每一项系数组成的字符串记为str1,量子身份认证模块使用量子密钥z加密字符串str1,得到$str1 \oplus z$,量子身份认证模块通过网络通信模块

将$str1 \oplus z$发送给量子CA。

[0087] 量子CA基于本地的隐私身份ID_2生成一次性身份$OTID_2$,具体过程如下:

[0088] 量子CA使用密钥z对$str1 \oplus z$进行解密,得到str1′,再基于str1′生成不可约多项式P_1'。量子CA基于不可约多项式P_1'及量子密钥x生成哈希函数H_1',并基于该哈希函数H_1'对本地隐私身份ID_2做哈希计算,得到哈希值$H(ID_2)'$,而后再使用密钥y对哈希值$H(ID_2)'$进行加密,得到一次性身份$OTID_2$,即:

[0089] $OTID_2 = H(ID_2)' \oplus y$。

[0090] 流程a2、量子安全打印机基于本地公开身份ID_1及一次性身份$OTID_1$生成文件Sign,基于文件Sign,量子安全终端和量子CA对量子安全打印机的身份进行认证。

[0091] 量子安全打印机中的量子身份认证模块基于本地公开身份ID_1及一次性身份$OTID_1$生成文件Sign,即:

[0092] $Sign=[ID_1, OTID_1]$。

[0093] 基于文件Sign,量子安全终端和量子CA对量子安全打印机的身份进行认证的过程如下:

[0094] S1、量子安全打印机中的量子身份认证模块从本地获取一个随机数,用于生成不可约多项式P_2,不可约多项式P_2除最高项以外每一项系数组成的字符串记为str2。

[0095] S2、量子安全打印机中的量子密钥管理模块与量子安全终端、量子CA预置相同的密钥池。

[0096] 量子安全打印机中的量子身份认证模块与量子安全终端、量子CA三方共享一组量子密钥u、v、w的位置标识。量子身份认证模块根据共享量子密钥u、v、w的位置标识从量子密钥管理模块的密钥池中获取量子密钥u、v、w,量子安全终端和量子CA根据共享量子密钥u、v、w的位置标识,分别从本地密钥池中获取量子密钥u、v、w。

[0097] 或者,量子身份认证模块记录从量子密钥管理模块的密钥池中提取的量子密钥u、v、w的位置标识,并将该位置标识发送给量子CA与量子安全终端。由于传输的只是密钥的位置标识,即使被黑客劫持,在没有相同的密钥池的情况下,也无法通过该位置标识得到对应的密钥。

[0098] S3、量子身份认证模块基于不可约多项式P_2及密钥u生成哈希函数H_2,使用哈希函数H_2对文件Sign进行哈希计算,得到哈希值H(Sign)。

[0099] 量子身份认证模块使用密钥v加密哈希值H(Sign),得到$v \oplus H(Sign)$;量子身份认证模块使用密钥w加密字符串str2,得到$w \oplus str2$。

[0100] 量子身份认证模块将$Sign$、$v \oplus H(Sign)$、$w \oplus str2$一并发送给量子安全终端。

[0101] S4、量子安全终端将接收到的文件Sign、加密的哈希值$v \oplus H(Sign)$、加密的字符串$w \oplus str2$一并发送给量子CA,量子安全终端和量子CA根据共享量子密钥u、v、w的位置标识,分别从本地密钥池中拉取相应位置处的量子密钥,得到量子密钥u、v、w。为和量子身份认证模块获得的量子密钥做区分,量子安全终端获得的量子密钥记为u_1'、v_1'、w_1',量子CA获得的量子密钥记为u″、v″、w″。

[0102] S5、量子安全终端使用密钥v′对加密的哈希值$v \oplus H(Sign)$进行解密,得到哈希值H(Sign)′,再使用密钥w′对加密的字符串$w \oplus str2$进行解密,得到字符串str2′,接着量子安

全终端基于字符串str2′生成不可约多项式P_2',再基于密钥u′和不可约多项式P_2'生产哈希函数H_2',使用哈希函数H_2'对文件Sign进行哈希计算,得到哈希值H′(Sign)′,将计算得到的哈希值H′(Sign)′与解密得到的哈希值H(Sign)′进行比较,若相等,则表示量子安全终端对量子安全打印机身份认证通过,否则量子安全终端对量子安全打印机身份认证不通过。

[0103] S6、量子CA使用密钥v″对加密的哈希值$v \oplus H(Sign)$进行解密,得到哈希值H(Sign)″,再使用密钥w″对加密的字符串$w \oplus str2$进行解密,得到字符串str2″,接着量子CA基于字符串str2″生成不可约多项式P_2'',再基于密钥u″和不可约多项式P_2''生产哈希函数H_2'',使用哈希函数H_2''对文件Sign进行哈希计算,得到哈希值H′(Sign)″,将计算得到的哈希值H′(Sign)″与解密得到的哈希值H(Sign)″进行比较,若相等,则哈希值比对通过,否则量子CA对量子安全打印机身份认证不通过。

[0104] 量子CA将接收到的文件Sign中的公开身份ID_1与量子CA中本地存储的公开身份ID_1进行比较,若相等,则公开身份比对通过,否则量子CA对量子安全打印机身份认证不通过。

[0105] 量子CA将接收到的文件Sign中的一次性身份$OTID_1$与量子CA中本地存储的一次性身份$OTID_2$进行比较,若相等,则一次性身份比对通过,否则量子CA对量子安全打印机身份认证不通过。

[0106] 只有当哈希值比对、公开身份比对及一次性身份比对均通过,则量子CA对量子安全打印机身份认证通过,若其中任意一个比对失败,则量子CA对量子安全打印机身份认证不通过。

[0107] 流程a3、量子安全终端和量子CA对量子安全打印机身份认证均通过后,量子安全终端向量子安全打印机发送待打印数据。

[0108] 量子安全终端对待打印数据data进行哈希计算,得到哈希值H(data)。量子安全终端从本地提取量子密钥r对待打印数据data及哈希值H(data)进行加密,得到加密数据$r \oplus [data, H(data)]$,并记录量子密钥r的位置标识。量子安全终端将加密数据$r \oplus [data, H(data)]$及密钥r的位置标识一并发送至量子安全打印机。

[0109] 步骤四、量子安全打印机和量子CA基于量子身份ID_b对量子安全终端进行身份认证,量子安全打印机和量子CA对量子安全终端身份认证均通过后,量子安全打印机对接收到的待打印数据进行认证,待打印数据认证通过后,进行待打印数据的打印。

[0110] 量子身份ID_b包括公开身份ID_3和隐私身份ID_4,量子安全打印机和量子CA基于量子身份ID_b对量子安全终端进行身份认证的流程如下:

[0111] 流程b1、量子安全终端基于本地的隐私身份ID_4生成一次性身份$OTID_3$,量子CA基于本地的隐私身份ID_4生成一次性身份$OTID_4$;

[0112] 流程b2、量子安全终端基于本地公开身份ID_3及一次性身份$OTID_3$生成文件$Sign_,$,基于文件$Sign_,$,量子安全打印机和量子CA对量子安全终端的身份进行认证;

[0113] 流程b3、量子安全打印机和量子CA对量子安全终端身份认证均通过后,量子安全打印机对接收到的待打印数据进行认证。

[0114] 量子安全打印机和量子CA基于量子身份ID_b对量子安全终端进行身份认证的过程,与量子安全终端和量子CA基于量子身份ID_a对量子安全打印机进行身份认证的过程相同,包括一次性身份的生成、基于一次性身份进行身份认证等,此处细节不再复述。

[0115] 量子安全打印机对接收到的待打印数据进行认证的具体过程如下：

[0116] 量子安全打印机中的量子加解密模块经由网络通信模块接收来自量子安全终端的加密数据$r \oplus [data, H(data)]$及密钥r的位置标识。量子加解密模块向量子密钥管理模块发送获取量子密钥的请求g及密钥r的位置标识，量子密钥管理模块根据请求g及密钥r的位置标识从本地密钥池拉取相应位置处的密钥，并将得到的密钥r′发送给量子加解密模块。量子加解密模块使用密钥r′对加密数据$r \oplus [data, H(data)]$进行解密，得到待打印数据data′和哈希值H(data)′，而后对解密得到的待打印数据data′采用与量子安全终端相同的哈希算法进行哈希计算，得到哈希值H(data)′′，将计算得到的哈希值H(data)″与解密得到的哈希值H(data)′进行比对，若比对相等，则解密后得到的待打印数据data′认证通过，否则认证不通过。

[0117] 解密后得到的待打印数据data′认证通过后，量子加解密模块将待打印数据data′发送至打印历史管理模块和数据打印模块，数据打印模块接收待打印数据data′，并进行数据打印，打印历史管理模块对接收到的待打印数据data′进行存储，同时对打印历史记录也进行保存，例如：打印时间、文件数量等等。

[0118] 通过上述过程，可以确保量子安全打印机是合法的，并且打印数据是从合法的量子安全终端处接收到的。进一步通过对待打印数据的认证，确保待打印数据在传输过程中未被篡改，保证了待打印数据的完整性。

[0119] 步骤五、待打印数据完成打印后，与开机时一样，量子安全打印机进行用户身份认证，用户身份认证成功后，量子安全打印机关机。

[0120] 量子安全打印机可通过生物识别方法对用户的身份进行认证，例如：指纹识别、人脸识别等，此处的用户，即为量子安全打印机授权的管理人员，若量子安全打印机对用户身份认证失败，则量子安全打印机无法正常关机。

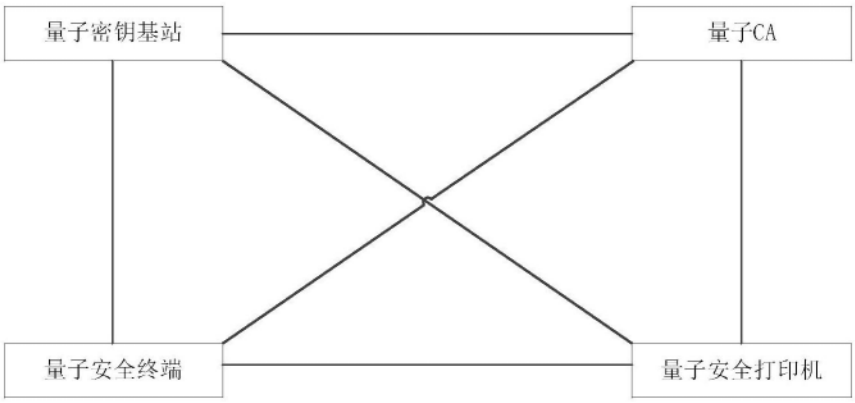

量子密钥基站
量子CA
量子安全终端
量子安全打印机

图1

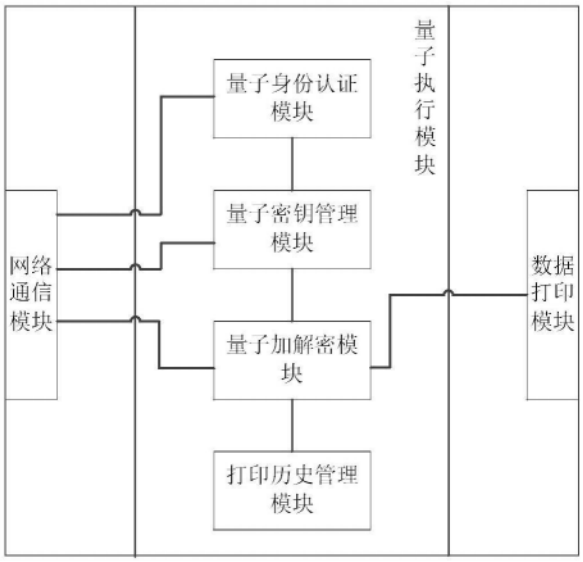

量子执行模块
量子身份认证模块
量子密钥管理模块
量子加解密模块
打印历史管理模块
网络通信模块
数据打印模块

图2

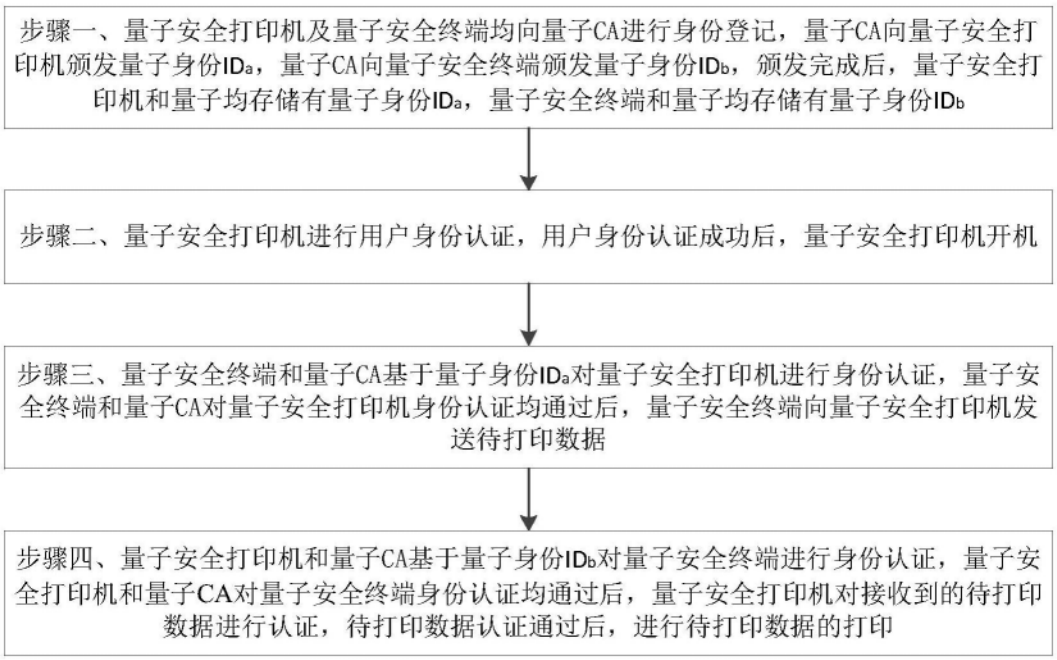

步骤一、量子安全打印机及量子安全终端均向量子CA进行身份登记，量子CA向量子安全打印机颁发量子身份IDa，量子CA向量子安全终端颁发量子身份IDb，颁发完成后，量子安全打印机和量子均存储有量子身份IDa，量子安全终端和量子均存储有量子身份IDb
步骤二、量子安全打印机进行用户身份认证，用户身份认证成功后，量子安全打印机开机
步骤三、量子安全终端和量子CA基于量子身份IDa对量子安全打印机进行身份认证，量子安全终端和量子CA对量子安全打印机身份认证均通过后，量子安全终端向量子安全打印机发送待打印数据
步骤四、量子安全打印机和量子CA基于量子身份IDb对量子安全终端进行身份认证，量子安全打印机和量子CA对量子安全终端身份认证均通过后，量子安全打印机对接收到的待打印数据进行认证，待打印数据认证通过后，进行待打印数据的打印

图3