(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 101989984 A
(43)申请公布日 2011.03.23

(21)申请号 201010260503.4

(22)申请日 2010.08.24

(71)申请人 北京易恒信认证科技有限公司
地址 100043 北京市石景山区石景山路 40 号信安大厦三层 E-G
申请人 北京联合智华微电子科技有限公司

(72)发明人 赵建国 李维刚

(74)专利代理机构 北京同恒源知识产权代理有限公司 11275
代理人 赵荣之

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/32(2006.01)
H04L 9/30(2006.01)

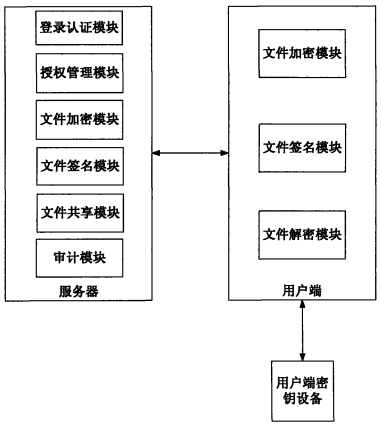
权利要求书 2 页 说明书 7 页 附图 4 页

(54)发明名称

电子文件安全共享系统及方法

(57)摘要

本发明公开了一种可实现机密文件安全存储和充分共享的电子文件安全共享系统，所述电子文件安全共享系统，包括文件加密模块，所述文件加密模块利用会话密钥对电子文件数据进行对称加密，并利用接收方标识（公钥）对会话密钥进行非对称加密，最后将加密后的对称密钥和加密后的电子文件数据打包为数字信封；以及文件解密模块，利用自身的私钥，对数字信封进行解密；本发明的电子文件安全共享方法，以 CPK 组合公钥或 CPK 复合公钥技术为基础，利用其灵活的数字签名和密钥交换能力，构建起一个从服务器到客户端，涵盖信息存储、传递到使用各个环节，集文件数据加密、访问控制、授权管理、动态密钥交换、过程审计跟踪为一体的保密文件管理体系。



CN 101989984 A

1. 电子文件安全共享系统，其特征在于：包括文件加密模块，所述文件加密模块利用会话密钥对电子文件数据进行对称加密，并利用服务器标识对会话密钥进行非对称加密，最后将加密后的会话密钥和加密后的电子文件密文数据打包为数字信封，并进行初始化授权后上传到服务器；

文件解密模块，利用用户自身的私钥，拆开数字信封得到会话密钥，再用会话密钥解密密文数据获得电子文件数据。

2. 如权利要求 1 所述的电子文件安全共享系统，其特征在于：还包括文件共享模块，主要用于进行动态密钥交换，当用户申请文件下载时，调用文件共享模块拆开数字信封取出会话密钥，再利用该用户的用户标识生成公钥，用该用户的公钥对会话密钥加密，并对电子文件密文数据重新打包为新的数字信封发送给用户。

3. 如权利要求 1 所述的电子文件安全共享系统，其特征在于：还包括授权管理模块，所述授权管理模块采用基于角色的访问控制授权管理策略，实现对文件上传和下载的访问控制，防止电子文件被越权访问。

4. 如权利要求 1 所述的电子文件安全共享系统，其特征在于：还包括文件签名模块，所述文件签名模块是在文件加密上传时对电子文件明文进行 CPK 数字签名，在用户下载后解密时验证数字签名，以保障上传文件的完整性和不可抵赖性。

5. 如权利要求 1 至 4 中任一项所述的电子文件安全共享系统，其特征在于：还包括登录认证模块和用户密钥设备，所述登录认证模块和用户密钥设备进行登录的交互认证；所述用户密钥设备内存储有用户私钥和用户标识信息，所述用户标识信息中含用户所在域种子公钥标识；认证模块中含种子公钥集，用以完成不同信任域的用户身份认证。

6. 如权利要求 5 所述的电子文件安全共享系统，其特征在于：还包括审计模块，用于记录用户登录及电子文件调用操作。

7. 电子文件安全共享方法，其特征在于：包括如下步骤：

A1) 根据随机数发生器产生的随机数据生成会话密钥；

A2) 利用会话密钥通过对称加密算法对电子文件数据进行加密；

A3) 用服务器标识通过种子公钥计算出服务器的标识公钥或复合公钥；

A4) 用服务器的标识公钥对会话密钥进行加密；

A5) 将加密后的会话密钥和电子文件密文数据打包成数字信封上传至服务器存储。

8. 如权利要求 7 所述的电子文件安全共享方法，其特征在于：所述步骤 A3) 具体包括如下步骤：用 hash 函数计算出服务器标识 hash 值 H，以 H 构建选取数列，从种子公钥集选取服务器所属信任域的种子公钥并利用椭圆曲线点运算生成服务器标识公钥。

9. 如权利要求 7 所述的电子文件安全共享方法，其特征在于：所述步骤 A3) 还包括如下步骤：用标识公钥验证随机公钥的数字签名，如果验证通过则将标识公钥与验证通过的随机公钥相复合，生成复合公钥。

10. 如权利要求 7 所述的电子文件安全共享方法，其特征在于：还包括如下步骤：

B1) 用户向服务器发出登录请求，服务器收到请求后，生成一个随机字符串，将该随机字符串返给客户端；

B2) 用户端接收到服务器端返回的随机字符串后，生成随机字符串与当前时间的摘要数据，开启用户密钥设备，将摘要数据送入用户密钥设备进行数字签名，然后将数字签名数

据、签名时间、签名者标识、签名者所在信任域标识打包为签名数据包，回送给服务器端；

B3) 服务器端从签名数据包中提取签名者标识和所在信任域标识，通过该用户所属信任域的种子公钥计算出用户的标识公钥，对签名数据包中的数字签名信息进行验证，若验证通过，则查询权限管理数据库，如该用户拥有相应的权限，则准许该用户登录并访问授权资源。

11. 如权利要求 7 所述的电子文件安全共享方法，其特征在于：还包括如下步骤：

C1) 用户登录文件服务器后，在授权范围内选定文件，并发出下载申请；

C2) 服务器接到下载申请后用自身的私钥拆开该文件的数字信封，取出会话密钥；

C3) 利用该用户的用户标识计算出其标识公钥或复合公钥；

C4) 利用标识公钥或复合公钥对会话密钥进行加密；

C5) 将加密后的会话密钥和电子文件数据打包成新的数字信封并发送给发出下载申请的用户，该用户接收到数字信封后，可利用自身的私钥对其进行拆封。

12. 如权利要求 7 至 11 中任一项所述的电子文件安全共享方法，其特征在于：还包括用户间的文件直接共享的步骤，具体包括步骤：

D1) 发送方选定发送文件；

D2) 发送方设定该文件对应接收方的标识和信任域标识，接收方用户可以是一个或多个；

D3) 发送方根据接收方用户标识和信任域标识自动选择对应的种子公钥矩阵，并分别计算各用户对应的标识公钥；

D4) 发送方产生随机数作为会话密钥，并对要发送的文件进行对称加密，并对其进行 CPK 数字签名，将签名附在电子密文之后，再利用接收方对应的标识公钥对会话密钥加密，将电子文件密文数据和会话密钥密文进行打包成数字信封，如接收方为多人，则重复步骤 D3) 和 D4)，形成多数字信封的电子密文文件；

D5) 发送方将数字信封发送给各接收方，接收方接收后用自己的私钥拆开数字信封，取出会话密钥，再解密数据得到原文件，并验证其数字签名以确定发件人的真实性和文件的完整性。

电子文件安全共享系统及方法

技术领域

[0001] 本发明提供涉及基于标识的认证技术，具体涉及一种基于 CPK 组合公钥算法或 CPK 复合公钥算法的电子文件（包括文档、图片、语音视频等数据类型）的共享系统及方法，属于信息安全技术领域。

背景技术

[0002] 当前，信息技术已经渗透到政府和企业日常运作的各个环节，数据和信息成为政府和企业运作的基础要素。信息技术的应用极大地提高了工作效率，但同时也增加了安全上的风险。因网络攻击、木马病毒侵袭或存储介质的保管不善造成保密数据、商业机密和个人隐私丢失和泄露，以及网络中传输数据文件被窃取、篡改的事件频繁发生，给政府、企业及个人带来了巨大的损失。威胁不仅来自外部也出自内部。据权威机构统计，80％的信息泄露出自内部。一般单位和企业的内部机密文件、核心技术资料等通常保存在服务器和个人计算机内。窃密者往往通过攻击或欺骗等手段，获取到特定权限，登录服务器，下载资料，或者通过攻击技术，非法从重要人员的计算机中窃取信息甚至设法将服务器和计算机搬走。因此，采取有效技术措施保证存放在服务器上和个人计算机内重要信息和数据的安全，妥善解决文件的安全存储和共享问题，成为亟待解决的现实问题。

[0003] 实现网络环境下的信息安全共享是信息化发展的客观要求。然而，既要最大限度地实现信息的充分共享，又要确保信息的安全本身就是相互矛盾的，也因此成为国际性难题。目前对文件数据的防护主要通过两种途径 ：一是从改善外部环境入手，通过采取网络物理隔离，防止非法接入，对存有文件数据的服务器采取严格的访问控制和授权管理等措施，防止文件数据丢失 ；二是利用密码技术对文件数据本身进行加密保护。这样，即使数据丢失，也不会造成泄密。问题的关键是，如何才能在保证信息充分共享的前提下，通过技术整合，将两种手段有机结合，构成严密的综合体系。

发明内容

[0004] 有鉴于此，为了解决上述问题，本发明公开了一种可实现机密文件的安全存储和充分共享的电子文件安全共享系统。

[0005] 本发明的目的是这样实现的 ：电子文件安全共享系统，包括 ：

[0006] 文件加密模块，所述文件加密模块利用会话密钥对电子文件数据进行加密，并利用接收方标识生成的公钥对会话密钥进行加密，最后将加密后的对称密钥和加密后的电子文件数据打包为数字信封，并进行初始化授权后上传到服务器 ；

[0007] 文件解密模块，利用自身的私钥，拆开数字信封得到会话密钥，再用会话密钥解密密文数据获得电子文件数据。

[0008] 进一步，所述电子文件安全共享系统还包括 ：

[0009] 文件共享模块，主要用于动态密钥交换，当用户申请文件下载时，调用文件共享模块拆开数字信封取出会话密钥，再利用该用户的用户标识生成公钥，用该用户的公钥对会

话密钥加密，并将电子文件数据重新打包为新的数字信封发送给用户。

[0010] 进一步，所述电子文件安全共享系统还包括授权管理模块，所述授权管理模块采用基于角色的访问控制授权管理策略，实现对文件上传和下载的访问控制，防止电子文件被越权访问。

[0011] 进一步，所述电子文件安全共享系统还包括文件签名模块，所述文件签名模块是在文件加密上传时对电子文件明文进行 CPK 数字签名，在用户下载后解密时验证数字签名，以保障上传文件的完整性和不可抵赖性。

[0012] 进一步，所述电子文件安全共享系统还包括登录认证模块和用户密钥设备，所述登录认证模块和用户密钥设备进行登录的交互认证，所述用户密钥设备内存储有用户私钥和用户标识信息（含用户所在域标识）；认证模块中含种子公钥集，可以完成不同信任域的用户身份认证。

[0013] 进一步，所述电子文件安全共享系统还包括审计模块，用于记录用户登录及电子文件调用操作。

[0014] 本发明还提供一种可实现机密文件的安全存储和充分共享的电子文件安全共享方法，包括如下步骤：

[0015] A1) 根据随机数发生器产生的随机数据生成会话密钥；

[0016] A2) 利用会话密钥通过对称密码算法对电子文件数据进行加密；

[0017] A3) 用服务器标识通过种子公钥计算出服务器的标识公钥或复合公钥；

[0018] A4) 用服务器的标识公钥或复合公钥对会话密钥进行加密；

[0019] A5) 将加密后的会话密钥和电子文件数据打包成数字信封并存放。

[0020] 进一步，所述步骤 A3) 具体包括如下步骤：用 hash 函数计算出服务器标识 hash 值 H，以 H 构建选取数列，从种子公钥集选取服务器所属信任域的种子公钥并利用椭圆曲线点运算生成用户标识公钥。

[0021] 进一步，所述步骤 A3) 还包括如下步骤：用标识公钥验证的随机公钥的数字签名，如果验证通过则将标识公钥与验证通过的随机公钥相复合，生成复合公钥。

[0022] 进一步，所述电子文件安全共享方法还包括如下步骤：

[0023] B1) 用户向服务器发出登录请求，服务器收到请求后，生成一个随机字符串，将该随机字符串返给客户端；

[0024] B2) 用户端接收到服务器端返回的随机字符串后，用 hash 函数生成随机字符串与当前时间的摘要数据，开启用户密钥设备，将摘要数据送入用户密钥设备进行数字签名，然后将数字签名数据、签名时间、签名者标识、签名者所在信任域标识打包为签名数据包，回送给服务器端；

[0025] B3) 服务器端从签名数据包中提取签名者标识和所在信任域标识，通过该用户所属信任域的种子公钥计算出用户的标识公钥，对签名数据包中的数字签名信息进行验证，若验证通过，则查询权限管理数据库，如该用户拥有相应的权限，则准许该用户登录并访问授权资源。

[0026] 进一步，所述电子文件安全共享方法还包括如下步骤：

[0027] C1) 用户登录文件服务器后，在授权范围内选定文件，并发出下载申请；

[0028] C2) 服务器接到下载申请后用自身的私钥拆开该文件的数字信封，取出会话密

钥；

[0029] C3) 利用该用户的用户标识计算出其标识公钥或复合公钥；

[0030] C4) 利用标识公钥或复合公钥对会话密钥进行加密；

[0031] C5) 将加密后的会话密钥和电子文件数据打包成新的数字信封并发送给发出下载申请的用户，该用户接收到数字信封后，可利用自身的私钥对其进行拆封。

[0032] 进一步，所述电子文件安全共享方法还包括用户间的文件直接共享，包括如下步骤：

[0033] D1) 发送方选定要进行发送的文件（一个或多个）；

[0034] D2) 发送方设定该文件对应接收方的用户标识和信任域标识，接收方可以是一个或多个；

[0035] D3) 发送方根据接收方用户标识和信任域标识自动选择对应的种子公钥矩阵，并分别计算各用户对应的标识公钥；

[0036] D4) 发送方产生随机数作为会话密钥，并对要发送的文件进行对称加密，并对其进行 CPK 数字签名，将签名附在电子密文之后，再利用接收方对应的标识公钥对会话密钥加密，将电子文件密文数据和会话密钥密文进行打包成数字信封，如接收方为多人，则重复步骤 D3) 和 D4)，形成多数字信封的电子密文文件；

[0037] D5) 发送方将数字信封发送给各接收方，接收方接收后用自己的私钥拆开数字信封（只有发送方指定的用户方可打开数字信封），取出会话密钥，再解密数据得到原文件，并验证其数字签名以确定发件人的真实性和文件的完整性。

[0038] 本发明的有益效果是：本发明的电子文件安全共享系统和方法，以 CPK 组合公钥或 CPK 复合公钥技术为基础，利用其灵活的数字签名和密钥交换能力，通过将文件的使用控制管理和数据加密两种手段紧密结合，构建起一个从服务器到客户端，涵盖信息存储、传递到使用各个环节，集文件数据加密、访问控制、授权管理、动态密钥交换、过程审计跟踪为一体的保密文件管理体系，不仅能够能使文件数据的管理使用处于严格的监管之下，保证其在存储状态下和网络传输过程中的安全，还可以通过数字签名，保证文档数据的真实性、完整性和不可抵赖性，从而实现数据、文件密码级的安全存储、传递和共享。本发明保密性强、效率高、能够支持大规模应用，而且体系结构简单、使用灵活方便、易于管理，广泛适用于政府、军队和企、事业单位，实现内部机密文件的安全存储和充分共享，有效地防止机密文件和要害数据的丢失问题。同时，该项技术也可以扩展应用到数字版权管理、视频点播等领域。

附图说明

[0039] 为了使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明作进一步的详细描述：

[0040] 图 1 示出了电子文件安全共享系统的结构示意图；

[0041] 图 2 示出了标识私钥、复合私钥及随机公钥生成过程示意图；

[0042] 图 3 示出了数字信封的制作过程示意图；

[0043] 图 4 示出了从种子公钥集计算标识公钥的过程示意图；

[0044] 图 5 示出了打开数字信封过程示意图；

[0045] 图 6 示出了认证登录过程示意图。

具体实施方式

[0046] 组合公钥算法(Combined Pubic Key,CPK)是基于标识的公钥算法,其密钥管理中心生成彼此对应的私钥计算参数(私钥计算基)和公钥计算参数(公钥计算基);根据第一用户提供的标识,利用所述私钥计算参数计算第一用户的私钥,并将所产生的私钥提供给第一用户;以及公布所述公钥计算参数,以使得第二用户在获得第一用户的标识后,可根据第一用户的标识,利用所述的公钥计算参数,计算第一用户的公钥。

[0047] 在提出了 CPK 算法的基础上,还提供了一种 CPK 芯片,CPK 芯片具有 CPK 算法功能单元、验证协议单元,在申请人的中国发明专利申请 2005100021564 基于标识的密钥产生装置及方法中具体实施方式所述,在本发明中全文引用。CPK 的算法功能单元和验证协议单元提供认证所需所有参数和协议,利用公钥矩阵则就能计算任何实体的公钥。

[0048] 在申请人申请号为 200810113495.3 的中国发明专利申请中还提出了 CPK 复合公钥算法:密钥由组合矩阵定义的标识(identity)密钥、和系统随机定义的随机(random)密钥、用户自行定义的更新(updating)密钥复合而成。在密钥交换中,密钥由标识密钥、系统(system)密钥复合而成。其中,标识密钥按组合公钥 CPK 体制生成;随机密钥通过随机数发生器生成。密钥交换中的密钥,均由密钥管理中心统一制定。

[0049] 本实施例即是基于 CPK 组合公钥算法或 CPK 复合公钥算法的电子文件安全共享系统和方法。

[0050] 参见图 1,所述电子文件安全共享系统部署在文件服务器端和用户端,在文件服务器端部署有文件加密模块、文件签名模块以及登录认证模块、授权管理模块、文件共享模块和审计模块,在客户端部署有文件加密模块、文件解密模块和文件签名模块,以及可用于连接用户端设备的用户密钥设备。其中登录认证模块和用户密钥设备通过 CPK 数字签名与验证协议进行登录的交互认证

[0051] 用户标识或服务器标识可根据需要自行定义,标识内容可以是人名、单位名称、代号等,要求在同一信任域中(共用同一种子密钥)所定义的标识具有唯一性,不能相互重复,所述用户标识信息中还包括信任域识别标记;

[0052] 密钥管理中心根据每个用户的标识为其生产私钥,写入用户密钥设备,并发放到每个用户。参见图 2,标识私钥及复合私钥生产方法如下:

[0053] 用 hash 函数计算出标识的 hash 值 H(ID),以 H(ID) 构建选取数列,从种子私钥集(用随机数发生器产生的一段数列构建)选取并经组合运算生成标识私钥(isk);将标识私钥写入用户密钥设备;

[0054] 如果使用 CPK 复合公钥算法,则用随机数发生器生成随机私钥 (ask),并通过椭圆曲线标量乘法运算生成与其相对应的随机公钥 (APK),将标识私钥与随机私钥相复合生成复合私钥,用标识私钥对随机公钥做数字签名,并将复合私钥连同经过数字签名的随机公钥一并写入用户密钥设备。

[0055] 为实现跨域认证和密钥交换,须在用户标识信息中定义种子公钥识别标记,并按照统一格式构建种子公钥集,由具有公信力的部门对种子公钥集做数字签名,保证其真实性,并将种子公钥集配置到登录认证模块以用户密钥设备。

[0056] 所述文件加密模块利用会话密钥通过对称算法对电子文件数据进行加密，并利用接收的方标识公钥（或复合公钥）对会话密钥进行加密，最后将加密后的对称密钥和加密后的电子文件数据打包为数字信封；服务器端存储的需要加密的电子文件，均利用服务器标识公钥加密打包为数字信封存储。

[0057] 文件解密模块，利用用户自身的私钥，拆开数字信封得到会话密钥，再用会话密钥解密密文数据获得电子文件数据。

[0058] 文件共享模块，主要用于动态密钥交换，当用户申请文件下载时，调用文件共享模块拆开数字信封取出会话密钥，再利用该用户的标识生成公钥，用该用户的公钥对会话密钥加密，将电子文件数据重新打包为新的数字信封并发送给申请用户。

[0059] 文件签名模块，所述文件签名模块是在文件加密上传时对电子文件明文进行 CPK 数字签名，在用户下载后解密时验证数字签名，以保障上传文件的完整性和不可抵赖性。

[0060] 服务器端还包括系统管理模块和授权管理模块，用于对管理员和用户进行信息管理和授权管理。包括管理员和用户的增加、查询、删除和基本信息维护，以及为管理员和用户分配分配资源权限；

[0061] 为加强安全审计，还可在服务器端设置审计模块，对用户登录、文件上传、文件下载及管理员进行的相应操作均将进行日志记录，用于对所有操作进行日后审计，保障用户和管理员对自己的行为负责，及出现泄密时可以进行有效的追溯。

[0062] 所述电子文件安全共享方法包括如下步骤：

[0063] A) 对电子文件进行加密存放，参见图 3，包括如下步骤：

[0064] A1) 根据随机数发生器产生的随机数据生成会话密钥；

[0065] A2) 利用会话密钥通过对称密钥算法对电子文件数据进行加密；

[0066] A3) 用服务器标识通过种子公钥计算出服务器的标识公钥或复合公钥；

[0067] A4) 用服务器的标识公钥或复合公钥对会话密钥进行加密；

[0068] A5) 将加密后的会话密钥和电子文件数据打包成数字信封并上传存放。

[0069] 上述步骤可由服务器完成，也可由用户完成后上传至服务器。

[0070] 计算标识公钥的方法如下：参见图 4，标识公钥计算：用 hash 函数计算出标识的 hash 值 H(ID)，以 H(ID) 构建选取数列，从种子公钥集（种子私钥经椭圆曲线点运算生成）选取并经椭圆曲线点运算生成标识公钥 (IPK)；

[0071] 复合公钥计算：首先用上述方法计算出标识公钥，用标识公钥验证对方提供的随机密钥的数字签名，如果验证通过则将计算出的标识公钥与验证通过的随机公钥相复合，生成复合公钥。

[0072] B) 对用户登录进行认证，使用者将用户密钥设备插入计算机终端，通过客户端浏览器输入文件服务器地址，系统将提示用户输入 PIN 码打开密钥设备，输入 PIN 码后，用户密钥设备被打开，为实现单点登录，可让用户密钥设备在被拔出前一直处于开启状态，并由用户密钥设备自动与服务器端的登录认证模块进行交互认证，参见图 6，其具体步骤如下：

[0073] B1) 用户将用户密钥设备与用户端计算机连接；

[0074] B2) 用户通过用户端计算机访问服务器时，服务器端生成一个随机字符串并返回用户端；

[0075] B3) 用户端接收到服务器端返回的随机字符串后，与当前时间一起计算生成摘要

数据，输入 PIN 码开启用户密钥设备，将摘要数据送入用户密钥设备进行数字签名；

[0076] B4) 用户密钥设备完成数字签名后，用户端将数字签名、签名时间、签名者标识、签名者所在信任域标识打包为签名数据包，回送给服务器端；

[0077] B5) 服务器端从签名数据包中提取签名者标识和所在信任域标识，通过该用户端所属信任域的种子公钥计算出用户的标识公钥，先使用标识公钥验证随机公钥的真实性，再将标识公钥与随机公钥计算得到复合公钥，利用复合公钥对签名数据包中的数字签名信息进行验证，如果验证通过，则证明用户身份的合法性及用户信息传送过程中未被篡改；

[0078] B6) 将签名时间与当前服务器时间进行比对，如出现超时，则判定签名失效，如未出现超时，则验证通过，服务器端允许用户登录；

[0079] B7) 用户登录其它服务器时，用户端将该服务器返回的随机字符串和摘要数据送入用户密钥设备进行数字签名，并自动执行步骤 4-6)，不再需要用户输入 PIN 码。

[0080] C) 用户从服务器下载电子文件的步骤如下：

[0081] C1) 用户登录文件服务器后，在授权范围内选定文件，并发出下载申请；

[0082] C2) 服务器接到下载申请后用自身的私钥拆开该文件的数字信封，取出会话密钥；

[0083] C3) 利用该用户的用户标识计算出其标识公钥或复合公钥；

[0084] C4) 利用标识公钥或复合公钥对会话密钥进行加密；

[0085] C5) 将加密后的会话密钥和电子文件数据打包成数字信封并发送给发出下载申请的用户，该用户接收到数字信封后，利用自身的私钥对其进行解封。

[0086] D) 此外，用户间还可直接进行文件交换，包括如下步骤：

[0087] D1) 发送方选定要进行发送的文件（一个或多个）；

[0088] D2) 发送方设定该文件对应接收方的用户标识和信任域标识，接收方可以是一个或多个；

[0089] D3) 发送方根据接收方用户标识和信任域标识自动选择对应的种子公钥矩阵，并分别计算各用户对应的标识公钥；

[0090] D4) 发送方产生随机数作为会话密钥，并对要发送的文件进行对称加密，并对其进行 CPK 数字签名，将签名附在电子密文之后，再利用接收方对应的标识公钥对会话密钥加密，将电子文件密文数据和会话密钥密文进行打包成数字信封，如接收方为多人，则重复步骤 D3) 和 D4)，形成多数字信封的电子密文文件；

[0091] D5) 发送方将数字信封发送给各接收方，接收方接收后用自己的私钥拆开数字信封（只有发送方指定的用户方可打开数字信封），取出会话密钥，再解密数据得到原文件，并验证其数字签名以确定发件人的真实性和文件的完整性。

[0092] 接收方对数字信封解密的过程如图 5 所示：利用自身的私钥对加密后的会话密钥进行解密，然后利用解密后的会话密钥对加密后的电子文件进行解密，获得原始的电子文件数据。

[0093] 为保证电子文件数据的真实性、完整性及不可抵赖性，发送方还可以用自身的私钥对文件数据作数字签名，数字签名及验证过程如下：

[0094] 1) 用 hash 函数计算被签名数据的 hash 值 H；

[0095] 2) 发送方用自身的私钥对 H 加密，连同自身的标识（使用复合密钥时还包括随机

公钥）一并提供给验证方；

[0096] 3) 验证方利用对方随签名数据提供的标识（随机公钥）计算出其标识或复合公钥；

[0097] 4) 用公钥解密签名数据取出 H，并用 hash 函数计算被签名数据的 hash 值 H；

[0098] 5) 将两个数据加以比对，如果一致则验证通过，证明数据是真实和完整性的。

[0099] 本实施例中数字签名及验证协议如下：

[0100] CPK 数字签名协议采用国际标准 ECDSA 签名协议，结合 TF-CPK 的特点，需要公开的参数有：

[0101] (1) 椭圆曲线群的五元参数组 (a，b，G，n，p)；

[0102] (2) 消息摘要函数 h；

[0103] (3) 种子公钥集 (P_0，P_1，...，$\mathbf{P}_{2^u\times v-1}$)；

[0104] (4) 签名方 A 发送的标识 ID 和伴随公钥 APK_A；

[0105] (5) 签名方 A 的标识密钥对伴随公钥 APK_A 的签名 sign1。

[0106] 1. 签名协议

[0107] 签名算法是对被签名数据先计算数字摘要，再利用 CPK 组合私钥对摘要进行加密，输出签名值。其数字签名算法描述如下：

[0108] (1) 随机选取 $k \in Zn$；

[0109] (2) 计算 $k \cdot G = (x, y)$（椭圆曲线群标量乘法）；

[0110] (3) 计算 $r = x \bmod n$；

[0111] (4) 计算 $S = k^{-1}(h(m)+csk_A \cdot r) \bmod n$；

[0112] (5)A 将 m 和签名 (r，S，sign1，APK_A) 发给 B。

[0113] 2. 验证协议

[0114] B 接收到 A 发来的被签名消息 m 和签名 (r，S，sign1，APK_A)，利用 TF-CPK 数字签名验证协议进行验证，其算法如下：

[0115] (1) 以 A 的标识生成选取数列，对种子公钥集进行选取与组合，生成标识公钥 IPK_A；

[0116] (2) 用标识公钥 IPK_A 和标识密钥对伴随公钥 APK_A 的签名 sign1 进行验证，验证通过表示 APK_A 是真实有效的，转入第三步；否则表示伴随公钥 APK_A 已经被篡改，验证失败，退出验证流程；

[0117] (3) 计算 $CPK_A = IPK_A + APK_A$（椭圆曲线点加运算）；

[0118] (4) 计算 $u_1 = h(m) \cdot S^{-1} \bmod n$；

[0119] $u_2 = r \cdot S^{-1} \bmod n$；

[0120] (5) 计算 $R = u_1 \cdot G + u_2 \cdot CPK_A$（椭圆曲线点加运算）；

[0121] 记 $R = (x', y')$；

[0122] 计算 $v = x' \bmod n$，若 $v = r$ 则验证通过，签名有效，否则签名无效。

[0123] 以上所述仅为本发明的优选并不用于限制本发明，显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

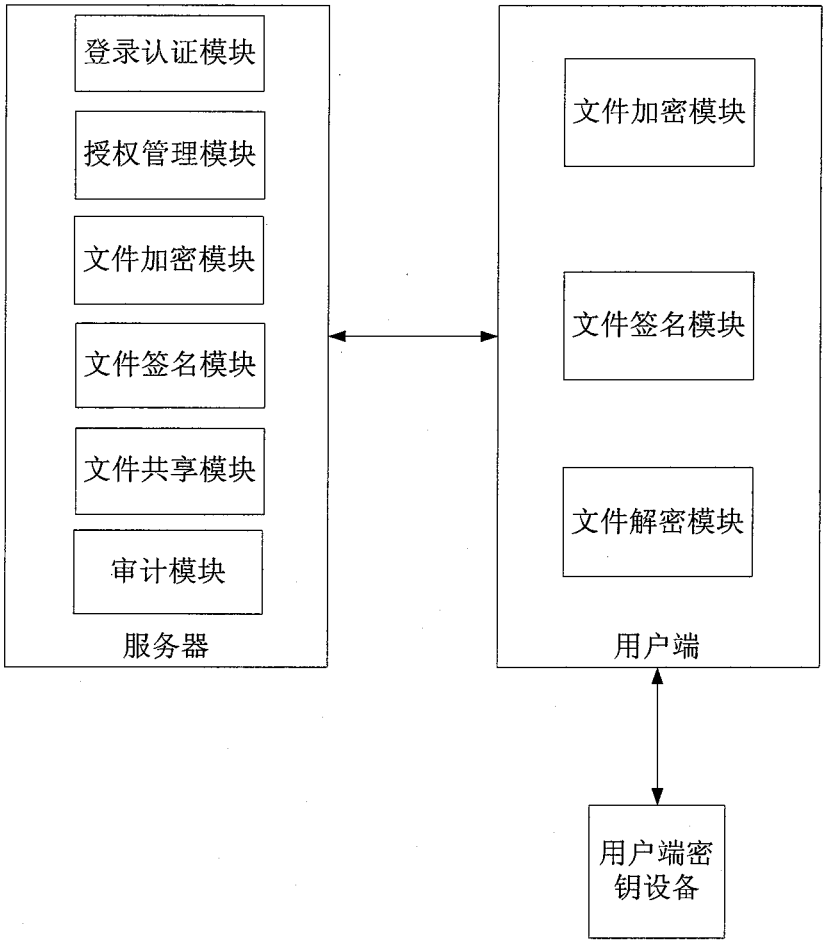

登录认证模块
授权管理模块
文件加密模块
文件签名模块
文件共享模块
审计模块
服务器
文件加密模块
文件签名模块
文件解密模块
用户端
用户端密钥设备

图 1

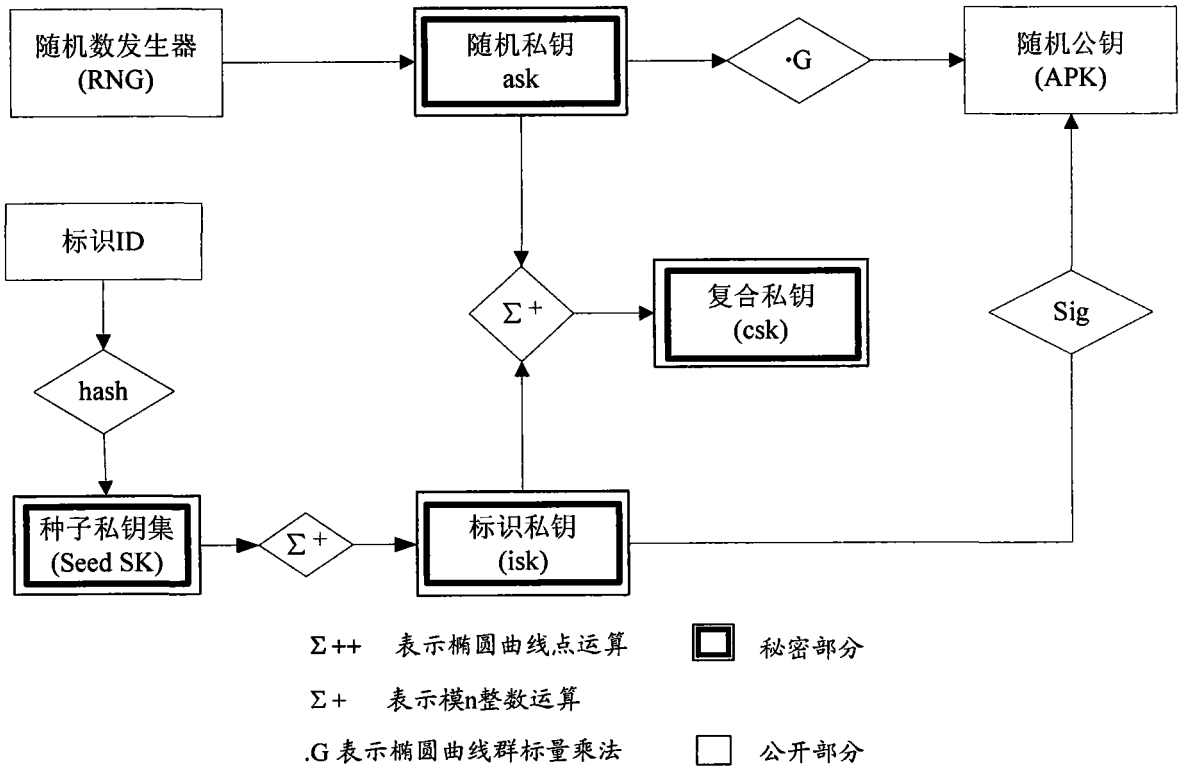

随机数发生器
(RNG)
随机私钥
ask
·G
随机公钥
(APK)
标识ID
Σ+
复合私钥
(csk)
Sig
hash
种子私钥集
(Seed SK)
Σ+
标识私钥
(isk)
Σ++ 表示椭圆曲线点运算
Σ+ 表示模n整数运算
.G 表示椭圆曲线群标量乘法
秘密部分
公开部分

图 2

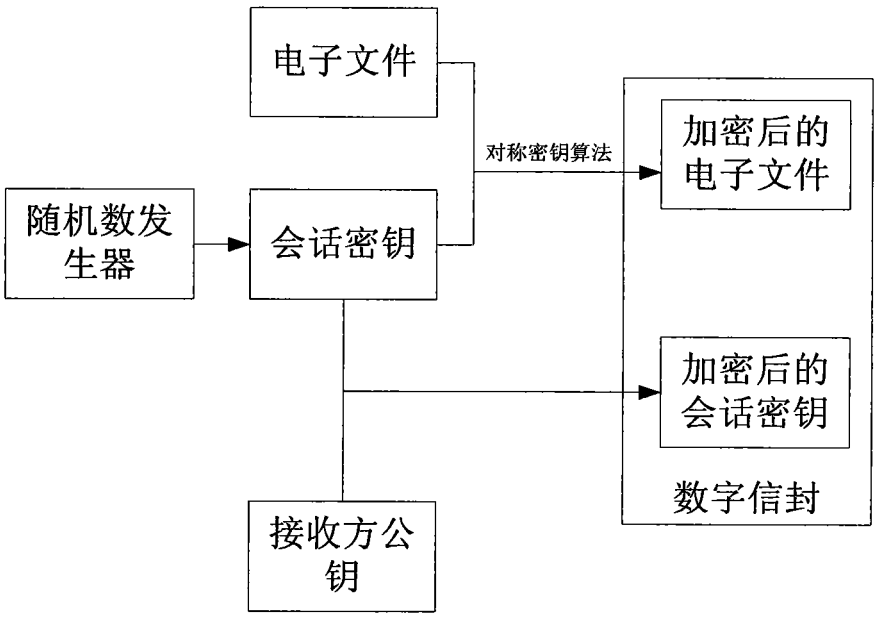

电子文件
对称密钥算法
加密后的
电子文件
随机数发
生器
会话密钥
加密后的
会话密钥
数字信封
接收方公
钥

图 3

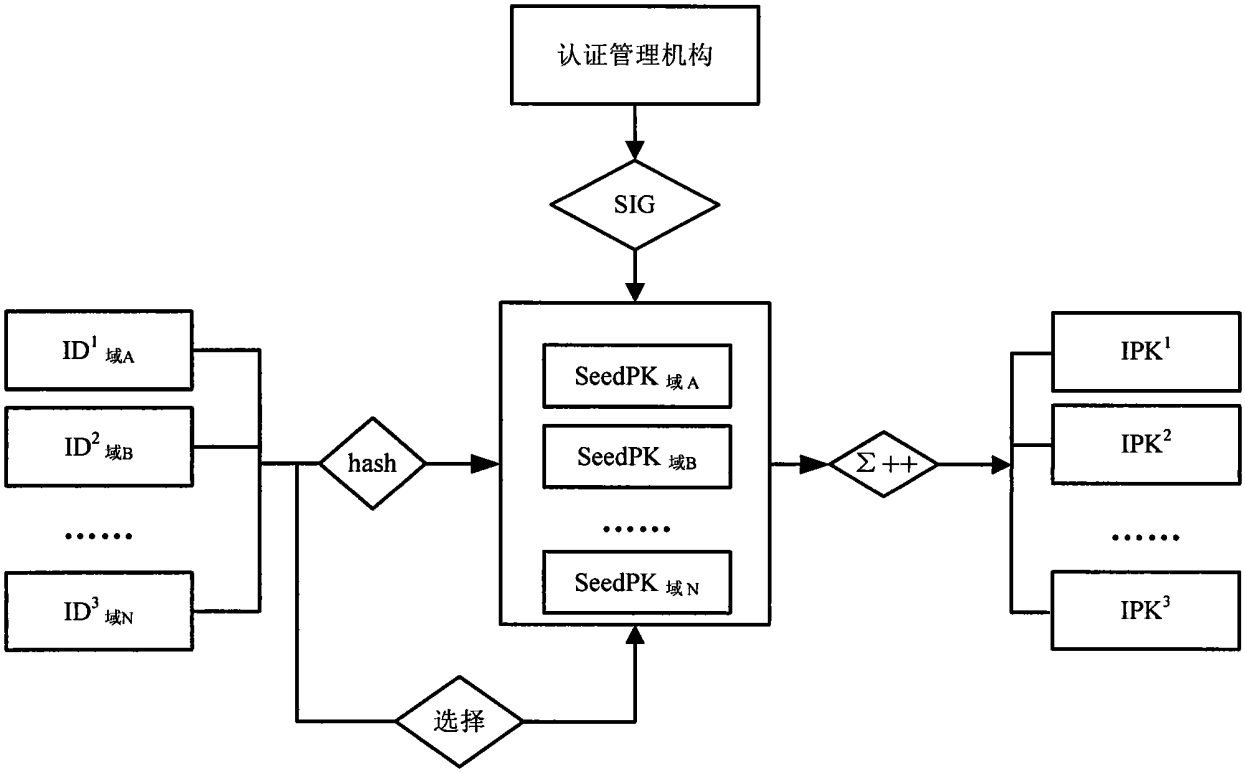

认证管理机构
SIG
ID[1] 域A
ID[2] 域B
……
ID[3] 域N
hash
SeedPK 域A
SeedPK 域B
……
SeedPK 域N
Σ ++
IPK[1]
IPK[2]
……
IPK[3]
选择

图 4

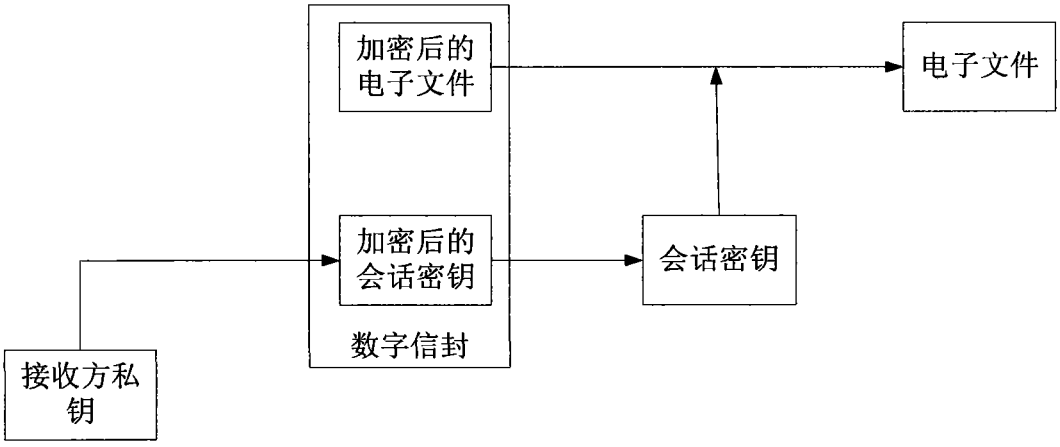

加密后的电子文件
电子文件
加密后的会话密钥
会话密钥
数字信封
接收方私钥

图 5

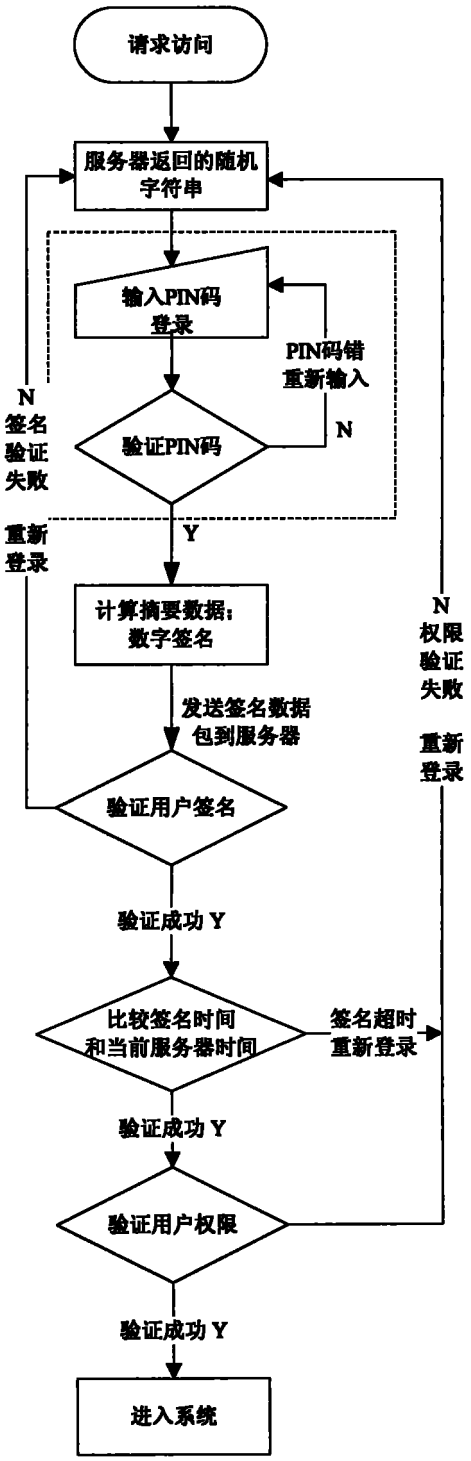

请求访问
服务器返回的随机字符串
输入PIN码登录
PIN码错重新输入
N
验证PIN码
N
签名验证失败
重新登录
Y
计算摘要数据：数字签名
发送签名数据包到服务器
N
权限验证失败
重新登录
验证用户签名
验证成功 Y
比较签名时间和当前服务器时间
签名超时重新登录
验证成功 Y
验证用户权限
验证成功 Y
进入系统

图 6