(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 106534092 B
(45)授权公告日 2019.07.02

(21)申请号 201610948549.2

(22)申请日 2016.11.02

(65)同一申请的已公布的文献号
申请公布号 CN 106534092 A

(43)申请公布日 2017.03.22

(73)专利权人 西安电子科技大学
地址 710071 陕西省西安市雁塔区太白南路2号

(72)发明人 高军涛 王笠燕 李雪莲 王丹妮 王誉晓

(74)专利代理机构 陕西电子工业专利中心 61205
代理人 王品华

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)

(56)对比文件
CN 104618366 A,2015.05.13,
CN 104836790 A,2015.08.12,
CN 104320262 A,2015.01.28,

审查员 翟倩倩

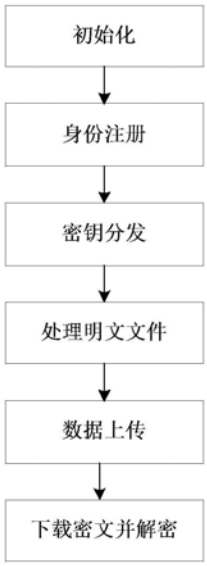
权利要求书3页 说明书6页 附图2页

(54)发明名称

基于消息依赖于密钥的隐私数据加密方法

(57)摘要

本发明公开了一种基于消息依赖于密钥的隐私数据加密方法,主要解决现有技术中未考虑明文和密钥的相关性和用电子邮件分发群组公钥带来的密钥相关攻击和密钥泄露问题。其实现步骤为:1.授权中心初始化系统参数;2.用户向授权中心进行身份验证;3.授权中心为通过身份验证的用户分发密钥;4.用户根据获得的密钥处理明文文件得到密文;5.用户将密文上传至云服务器;6.用户使用时,再向云服务器请求下载密文,请求通过后获得密文进行解密。本发明采用单用户模式下基于消息依赖于密钥的加密方法实现了对区块链钱包文件的安全加密,能够避免密钥泄漏,减轻密钥相关攻击,提高钱包文件的安全性。



CN 106534092 B

1.基于消息依赖于密钥的隐私数据加密方法,其特征在于,包括如下步骤:

(1)初始化:

(1a)授权中心确定第一安全参数λ、第二安全参数k、第三安全参数γ、关键字个数的参量τ和伯努利分布的参量$\theta=2^{-\lambda}$,定义明文矩阵的消息长度l、维数N、分组长度m,分别为l=l(λ)、N=N(λ)、m=m(λ);

(1b)授权中心定义纠错码的生成矩阵为$G=G_{m\times l}$,设置解纠错码的个数为d=(θ+σ)·m,根据生成矩阵G和解纠错码个数d选取一组二进制线性纠错码D,其中,$G_{m\times l}$表示生成矩阵为m×l阶,σ是(0,1)区间上选取的固定值;

(1c)对于任意比特串$K\in\{0,1\}^{\gamma}$,授权中心定义$P_K(x)$是$\{0,1\}^{\tau}$区间上的伪随机置换函数族,定义$F_K(x)$是定义域为$\{0,1\}^{\tau}$、值域为$\{0,1\}^{\gamma}$的第一伪随机函数族,定义$G_K(x)$是定义域为[1,n]、值域为{0,1}的第二伪随机函数族;

(1d)授权中心公开二进制线性纠错码D、纠错码的生成矩阵G、伪随机置换函数族$P_K(x)$、第一伪随机函数族$F_K(x)$、第二伪随机函数族$G_K(x)$和公共参数{l,m,N,θ};

(2)身份注册:

(2a)用户将个人身份信息提交给授权中心;

(2b)授权中心审核该用户提交的身份信息是否真实,若真实,则执行步骤(3),否则,拒绝注册;

(3)密钥分发:

(3a)授权中心定义有限域$\mathbb{Z}_2=\mathbb{Z}\bmod 2$,选取矩阵$\mathbf{S}\leftarrow\mathbb{Z}_2^{\lambda\times N}$作为用户加密明文的对称密钥,其中,$\mathbb{Z}$是整数环,2是素数;

(3b)授权中心为用户生成消息认证码HMAC操作所需的密钥k_{mac};

(3c)授权中心通过安全信道将消息$\{SPk_{mac}\ P\gamma P\tau\}$发送给用户;

其中,S是用户加密明文的对称密钥,γ是第三安全参数,τ是关键字个数的参量,P表示级联符号;

(3d)用户将对称密钥S、消息认证码HMAC密钥k_{mac}、第三安全参数γ和关键字个数的参量τ秘密保存;

(4)处理明文文件:

(4a)用户加密明文文件ε_j时,对其明文矩阵进行分块,定义每个明文矩阵块为$\mathbf{M}\in\mathbb{Z}_2^{l\times N}$,其中,1≤j≤n,n为明文文件总数;

(4b)用户根据对称密钥S加密每个明文矩阵块M,获得对应的密文矩阵块W:

W=(A,C),

其中,A是从$\mathbb{Z}_2^{m\times\lambda}$中随机选取的系数矩阵,C=A·S+E+G·M,S是对称密钥,G是纠错码D的生成矩阵,E是从$Ber_0^{m\times N}$中随机选取的噪声矩阵,Ber_0表示{0,1}上的伯努利分布,1的概率为θ,0的概率为1-θ;

(4c)将该明文文件ε_j所有的密文矩阵块W级联起来,得到该明文文件ε_j对应的密文文件ψ_j;

(4d)用户根据消息认证码HMAC密钥k_{mac}和密文文件ψ_j计算密文文件ψ_j的消息认证标签T_j:

T_j＝HMAC(k_{mac},ψ_j)，

其中，HMAC()表示消息认证标签生成算法；

(4e)用户随机均匀选取第一秘密值s∈{0,1}$^{\gamma}$、第二秘密值r∈{0,1}$^{\gamma}$，生成一个可记录2^{τ}个关键字(i,w_i)的索引字典，将索引字典和两个秘密值s、r秘密保存；

其中，i为标号，i∈[1,2^{τ}]，w_i为关键字，w_i∈{0,1}*，*表示任意长度；

(4f)用户生成明文文件ε_j的索引比特串I_j；

(5)数据上传：

(5a)用户通过安全的信道，将消息认证码密钥k_{mac}发送给云服务器，并将消息{I_j Pψ_j PT_j}上传至云服务器，其中，1≤j≤n，n为明文文件总数，P表示级联符号；

(5b)云服务器按照下式对每个密文文件进行完整性验证，验证结果用v_j表示：

v_j＝Verify(k_{mac},ψ_j,T_j)，

其中，1≤j≤n，n为明文文件总数，Verify()表示消息认证码HMAC的验证算法；

若v_j＝1，表明ψ_j在上传过程中未被篡改，则云服务器接收该消息，并将索引字符串I_j保存到索引字符串集合I中，同时向用户返回“ψ_j上传成功”的通知；

若v_j＝0，表明ψ_j在上传过程中被篡改，则云服务器拒绝接收该消息，并向用户返回“ψ_j上传错误”的通知；

(5c)用户根据收到的通知内容确定是否上传成功：

若用户接收到“ψ_j上传成功”的通知，表明ψ_j已经成功上传至云服务器；

若用户接收到“ψ_j上传错误”的通知，则返回步骤(5a)；

(6)下载密文并解密：

(6a)用户生成需下载文件中的关键字w_μ的陷门T_{w_μ}，并上传至云服务器；

(6b)云服务器根据陷门T_{w_μ}，对已存储的文件索引比特串集合I进行匹配检索，若匹配成功，云服务器给用户返回相应的密文ψ，继续步骤(6c)；若匹配失败，则云服务器给用户返回“检索失败”的通知；

(6c)用户解密密文ψ获得对应的明文文件ε。

2.根据权利要求1所述的方法，其特征在于，步骤(3b)中授权中心为用户生成消息认证码HMAC操作所需的密钥k_{mac}，按照下式计算：

k_{mac}＝HMAC-KeyGen(1^k)，

其中，k是授权中心选取的第二安全参数，HMAC-KeyGen(1^k)表示消息认证码的密钥生成算法，k_{mac}是生成的消息认证码密钥。

3.根据权利要求1所述的方法，其特征在于，步骤(4f)中用户生成明文文件ε_j的索引字符串I_j，按如下步骤进行：

(4f1)用户根据第一秘密值s选取伪随机置换函数族$P_K(x)$中的伪随机置换函数$P_s(x)$，根据第二秘密值r选取第一伪随机函数族$F_K(x)$中的函数$F_r(x)$；

(4f2)计算下标值r_i＝F_r(i)，i∈[1,2^{τ}]，根据r_i的值选取第二伪随机函数族$G_K(x)$中的函数$G_{r_i}(x)$；

(4f3)用户根据ε_j中是否包含关键字w_i，为明文文件ε_j生成一个2^{τ}长的初始比特串I'_j：

若明文文件ε_j包含关键字w_i，则置初始比特串I'_j的第P_s(i)位为1，即$I'_j[P_s(i)]$＝1；

若明文文件ε_j不包含关键字w_i，则置初始比特串I'_j的第$P_s(i)$位为0，即$I'_j[P_s(i)]=0$；

遍历i的所有值，得到初始比特串I'_j；

(4f4)用户将初始比特串I'_j第i位的值与函数值$G_{r_i}(j)$进行异或操作，即$I_j[i]=I'_j[i]\oplus G_{r_i}(j)$，得到索引比特串$I_j$的第i位的值，$i\in[1,2^\tau]$，⊕表示异或操作；

遍历i的所有值，得到索引比特串I_j。

4.根据权利要求1所述的方法，其特征在于，步骤(6a)中用户生成需下载文件中的关键字w_μ的陷门T_{w_μ}，按如下步骤进行：

(6a1)用户从索引字典中找到与关键字w_μ对应的标号μ；

(6a2)用户根据第一秘密值s选取伪随机置换函数族$P_K(x)$中的伪随机置换函数$P_s(x)$，根据第二秘密值r选取第一伪随机函数族$F_K(x)$中的函数$F_r(x)$；

(6a3)用户根据标号μ计算置换标号$p=P_s(\mu)$；

(6a4)用户根据置换标号p计算函数索引值$f=F_r(p)$；

(6a5)用置换标号p和函数索引值f，构成陷门$T_{w_\mu}=(p,f)$。

5.根据权利要求1所述的方法，其特征在于，步骤(6b)中云服务器根据陷门T_{w_μ}，对已存储的文件索引比特串集合I进行匹配检索，按如下步骤进行：

(6b1)云服务器将索引比特串I_j中置换标号p对应的位值与函数值$G_f(j)$进行异或操作，即$I'_j[p]=I_j[p]\oplus G_f(j)$，得到初始比特串$I'_j$中置换标号p对应的位值，其中，p是陷门$T_{w_\mu}$中的置换标号，f是陷门$T_{w_\mu}$中的函数索引值，$G_f(x)$是根据f的值从第二伪随机函数族$G_K(x)$中选取的伪随机函数，$I'_j[p]$表示初始比特串$I'_j$中置换标号p对应的位值，$I_j[p]$表示索引比特串$I_j$中置换标号p对应的位值，⊕表示异或操作；

(6b2)云服务器遍历j的所有值，若存在$j\in[1,n]$，使得初始比特串I'_j中置换标号p对应的位值为1，即$I'_j[p]=1$，则匹配成功；若不存在，则匹配失败。

6.根据权利要求1所述的方法，其特征在于，步骤(6c)中所述的用户解密密文ψ获得对应的明文文件ε，按如下步骤进行：

(6c1)用户根据对称密钥S和密文文件ψ中的每一个密文矩阵块W=(A,C)，计算中间矩阵Q：

$Q=C-A\cdot S$；

(6c2)用户对中间矩阵Q的每一列调用二进制线性纠错码D进行解码，得到相应的明文矩阵块M；

(6c3)用户将所有的明文矩阵块M级联起来，得到对应的明文文件ε。

基于消息依赖于密钥的隐私数据加密方法

技术领域

[0001] 本发明属于数据处理技术领域，特别涉及一种隐私数据加密方法，可以用于区块链中对钱包文件的加密、备份以及将其上传至云服务器的过程。

背景技术

[0002] 区块链是在网络上的一个去中心化的分布式共享账簿或者数据库，通过高冗余的方式来构建极高的安全性。有人将其称为“信任的机器”，也即在没有中央权威的情况下，对彼此的协作创造信任。区块链技术适用于一切缺乏信任的领域，因而其应用范围会越来越广。在未来的区块链中，随着用户交易量的增加，大量的公私钥对需要用户产生和存储。而这些密钥通常是由用户生成并存储在一个文件或简单的数据库中，可将其称为钱包。钱包是多个地址和解密密钥的简单集合。拥有私钥是使用比特币的唯一条件，因此私钥必须保密且必须进行备份，将备份上传至云服务器，以防意外丢失。因此，对钱包的加密安全问题就显得格外重要。在用户向授权中心注册成功后，授权中心向用户分发加密时的对称密钥。由于密钥管理漏洞或者安全性意识不强，用户有可能会将用于加密钱包的对称密钥直接作为生成交易所用公私钥对的初始私钥。若此时加密钱包，钱包里的明文和密钥有依赖作用，传统的安全定义不足以维护该方案的安全性。随后，在将密文备份上传至云服务器后，若用户因本地文件丢失等问题，需要从云服务器上对某文件进行下载时，为了不泄漏个人隐私信息以及明文信息，用户可能需要从云服务器上下载所有的密文，在本地解密之后才能得到自己想要的文件。这种情况下用户需要进行大量的解密操作，降低用户工作效率，并且损耗大量计算资源和存储资源。

[0003] 武汉科技大学在其申请的专利“一种有权限时间控制的云存储数据安全共享方法”(公开号:105072180A，申请号:201510475566.4，申请日:2015年08月06日)中公开了一种有权限时间控制的云存储数据安全共享方法。在该方法中，数据拥有者创建群组后，自动用公钥加密算法生成一对密钥，数据拥有者共享文件时，采用对称密码机制对文件加密，再用待分享群组的私钥对对称密钥加密，并将文件密文及密钥密文发送到云端，把该群组的公钥用电子邮箱发给待分享群组的所有用户，用户若有访问权限，则可以获得公钥，解密文件。该方法存在的不足之处是:首先该专利在用分享群组的私钥加密对称密钥时没有考虑“明文和密钥可能相关”的安全问题，可能会产生密钥相关攻击;其次，该专利中数据拥有者将群组公钥用电子邮件发给群组用户时，没有考虑电子邮件的安全问题，电子邮件一旦被恶意截取，就会泄漏密钥。

发明内容

[0004] 本发明的目的在于针对上述现有的不足，提出一种基于消息依赖于密钥的隐私数据加密方法，以避免密钥泄漏，提高钱包文件的安全性。

[0005] 本发明的技术方案是，首先由授权中心完成对用户的身份认证过程，然后用户获得对称加密的密钥，采用消息依赖于密钥KDM对称加密方案对明文进行加密生成密文，以抵

抗密钥相关攻击，与此同时，采用可搜索加密对明文生成索引，以进行对密文的可搜索，其实现步骤包括如下：

[0006] (1)初始化：

[0007] (1a)授权中心确定第一安全参数λ、第二安全参数k、第三安全参数γ、关键字个数的参量τ和伯努利分布的参量$\theta=2^{-\lambda}$，定义明文矩阵的消息长度l、维数N、分组长度m，分别为l＝l(λ)、N＝N(λ)、m＝m(λ)；

[0008] (1b)授权中心定义纠错码的生成矩阵为$G=G_{m\times l}$，设置解纠错码的个数为d＝(θ+σ)·m，根据生成矩阵G和解纠错码个数d选取一组二进制线性纠错码D，其中，$G_{m\times l}$表示生成矩阵为m×l阶，σ是(0,1)区间上选取的固定值；

[0009] (1c)对于任意比特串$K\in\{0,1\}^{\gamma}$，授权中心定义$P_K(x)$是$\{0,1\}^{\tau}$区间上的伪随机置换函数族，定义$F_K(x)$是定义域为$\{0,1\}^{\tau}$、值域为$\{0,1\}^{\gamma}$的第一伪随机函数族，定义$G_K(x)$是定义域为[1,n]、值域为{0,1}的第二伪随机函数族；

[0010] (1d)授权中心公开纠错码D、生成矩阵G、伪随机置换函数族$P_K(x)$、第一伪随机函数族$F_K(x)$、第二伪随机函数族$G_K(x)$和公共参数{l,m,N,θ}；

[0011] (2)身份注册：

[0012] (2a)用户将个人身份信息提交给授权中心；

[0013] (2b)授权中心审核该用户提交的身份信息是否真实，若真实，则执行步骤(3)，否则，拒绝注册；

[0014] (3)密钥分发：

[0015] (3a)授权中心定义有限域$\mathbb{Z}_2=\mathbb{Z}\bmod 2$，选取矩阵$\mathbf{S}\leftarrow\mathbb{Z}_2^{\lambda\times N}$作为用户加密明文的对称密钥，其中，$\mathbb{Z}$是整数环，2是素数；

[0016] (3b)授权中心为用户生成消息认证码HMAC操作所需的密钥k_{mac}；

[0017] (3c)授权中心通过安全信道将消息$\{S||k_{mac}||\gamma||\tau\}$发送给用户；

[0018] 其中，S是用户加密明文的对称密钥，γ是第三安全参数，τ是关键字个数的参量，||表示级联符号；

[0019] (3d)用户将对称密钥S、消息认证码HMAC密钥k_{mac}、第三安全参数γ和关键字个数的参量τ秘密保存；

[0020] (4)处理明文文件：

[0021] (4a)用户加密明文文件ε_j时，对其明文矩阵进行分块，定义每个明文矩阵块为$\mathbf{M}\in\mathbb{Z}_2^{l\times N}$，其中，1≤j≤n，n为明文文件总数；

[0022] (4b)用户根据对称密钥S加密每个明文矩阵块M，获得对应的密文矩阵块W：

[0023] W＝(A,C)，

[0024] 其中，A是从$\mathbb{Z}_2^{m\times\lambda}$中随机选取的系数矩阵，C＝A·S+E+G·M，S是对称密钥，G是纠错码D的生成矩阵，E是从$Ber_\theta^{m\times N}$中随机选取的噪声矩阵，Ber_θ表示{0,1}上的伯努利分布，1的概率为θ，0的概率为1-θ；

[0025] (4c)将该明文文件ε_j所有的密文矩阵块W级联起来，得到该明文文件ε_j对应的密文文件ψ_j；

[0026] (4d)用户根据消息认证码HMAC密钥k_{mac}和密文文件ψ_j计算密文文件ψ_j的消息认证

标签T_j：

[0027] $T_j=HMAC(k_{mac},\psi_j)$，

[0028] 其中，HMAC()表示消息认证标签生成算法；

[0029] (4e)用户随机均匀选取第一秘密值$s\in\{0,1\}^{\gamma}$、第二秘密值$r\in\{0,1\}^{\gamma}$，生成一个可记录2^{τ}个关键字(i,w_i)的索引字典，将索引字典和两个秘密值s、r秘密保存；

[0030] 其中，i为标号，$i\in[1,2^{\tau}]$，w_i为关键字，$w_i\in\{0,1\}^*$，*表示任意长度；

[0031] (4f)用户生成明文文件ε_j的索引比特串I_j；

[0032] (5)数据上传：

[0033] (5a)用户通过安全的信道，将消息认证码密钥k_{mac}发送给云服务器，并将消息$\{I_j||\psi_j||T_j\}$上传至云服务器，其中，$1\leqslant j\leqslant n$，n为明文文件总数，||表示级联符号；

[0034] (5b)云服务器按照下式对每个密文文件进行完整性验证，验证结果用v_j表示：

[0035] $v_j=Verify(k_{mac},\psi_j,T_j)$，

[0036] 其中，$1\leqslant j\leqslant n$，n为明文文件总数，Verify()表示消息认证码HMAC的验证算法；

[0037] 若$v_j=1$，表明ψ_j在上传过程中未被篡改，则云服务器接收该消息，并将索引字符串I_j保存到索引字符串集合I中，同时向用户返回“ψ_j上传成功”的通知；

[0038] 若$v_j=0$，表明ψ_j在上传过程中被篡改，则云服务器拒绝接收该消息，并向用户返回“ψ_j上传错误”的通知；

[0039] (5c)用户根据收到的通知内容确定是否上传成功：

[0040] 若用户接收到“ψ_j上传成功”的通知，表明ψ_j已经成功上传至云服务器；

[0041] 若用户接收到“ψ_j上传错误”的通知，则返回步骤(5a)；

[0042] (6)下载密文并解密：

[0043] (6a)用户生成需下载文件中的关键字w_μ的陷门T_{w_μ}，并上传至云服务器；

[0044] (6b)云服务器根据陷门T_{w_μ}，对已存储的文件索引比特串集合I进行匹配检索，若匹配成功，云服务器给用户返回相应的密文ψ，继续步骤(6c)；若匹配失败，则云服务器给用户返回“检索失败”的通知；

[0045] (6c)用户解密密文ψ获得对应的明文文件ε。

[0046] 本发明与现有技术相比，具有以下优点：

[0047] 第一，本发明由于考虑到明文和密钥的相关的情况，采用消息依赖于密钥KDM对称加密方案对明文进行加密，在出现密钥管理漏洞时，可以抵抗密钥相关攻击，提高了钱包文件的安全性。

[0048] 第二，本发明由于采用单用户对文件进行加密、上传及下载，所以避免了与其他用户共享密钥时存在的密钥泄露问题。

附图说明

[0049] 图1为本发明的实现流程图；

[0050] 图2为本发明中处理明文文件的示意图；

[0051] 图3为本发明中下载并解密密文的示意图。

具体实施方式

[0052] 下面结合附图对本发明做进一步的描述。

[0053] 参照图1,本发明的具体步骤如下。

[0054] 步骤1,初始化。

[0055] 授权中心确定第一安全参数λ、第二安全参数k、第三安全参数γ、关键字个数的参量τ和伯努利分布的参量$\theta=2^{-\lambda}$;定义明文矩阵的消息长度l、维数N、分组长度m,分别为l=l(λ)、N=N(λ)、m=m(λ);授权中心定义纠错码的生成矩阵为$G=G_{m\times l}$,设置解纠错码的个数为$d=(\theta+\sigma)\cdot m$,根据生成矩阵G和解纠错码个数d选取一组二进制线性纠错码D,其中,$G_{m\times l}$表示生成矩阵为m×l阶,σ是(0,1)区间上选取的固定值;

[0056] 对于任意比特串$K\in\{0,1\}^{\gamma}$,授权中心定义$P_K(x)$是$\{0,1\}^{\tau}$区间上的伪随机置换函数族,定义$F_K(x)$是定义域为$\{0,1\}^{\tau}$、值域为$\{0,1\}^{\gamma}$的第一伪随机函数族,定义$G_K(x)$是定义域为[1,n]、值域为{0,1}的第二伪随机函数族;

[0057] 授权中心公开纠错码D、生成矩阵G、伪随机置换函数族$P_K(x)$、第一伪随机函数族$F_K(x)$、第二伪随机函数族$G_K(x)$和公共参数{l,m,N,θ}。

[0058] 步骤2,身份注册。

[0059] 用户将个人身份信息提交给授权中心,授权中心审核该用户提交的身份信息是否真实,若真实,则执行步骤(3),否则,拒绝注册。

[0060] 步骤3,密钥分发。

[0061] (3a)授权中心定义有限域$\mathbb{Z}_2=\mathbb{Z}\bmod 2$,选取矩阵$\mathbf{S}\leftarrow\mathbb{Z}_2^{\lambda\times N}$作为用户加密明文的对称密钥,其中,$\mathbb{Z}$是整数环,2是素数;

[0062] (3b)授权中心利用消息认证码的密钥生成算法HMAC-KeyGen(1^k)为用户生成消息认证码HMAC操作所需的密钥k_{mac}:

[0063] k_{mac}=HMAC-KeyGen(1^k),

[0064] 其中,k是授权中心选取的第二安全参数;

[0065] (3c)授权中心通过安全信道将消息{S||k_{mac}||γ||τ}发送给用户;

[0066] (3d)用户将对称密钥S、消息认证码HMAC的密钥k_{mac}、第三安全参数γ和关键字个数的参量τ秘密保存。

[0067] 步骤4,处理明文文件。

[0068] 设定用户需要加密的明文文件总数为n,每个明文文件用ε_j表示,1≤j≤n,

[0069] 参照图2,用户处理明文文件ε_j的步骤如下:

[0070] (4a)用户对明文文件ε_j中的明文矩阵进行分块,定义每个明文矩阵块为$\mathbf{M}\in\mathbb{Z}_2^{l\times N}$,根据对称密钥S加密每个明文矩阵块M,获得对应的密文矩阵块W=(A,C),将明文文件ε_j所有的密文矩阵块W级联起来,得到明文文件ε_j对应的密文文件ψ_j;

[0071] 其中,A是从$\mathbb{Z}_2^{m\times\lambda}$中随机选取的系数矩阵,$C=A\cdot S+E+G\cdot M$,S是对称密钥,G是纠错码D的生成矩阵,E是从$Ber_\theta^{m\times N}$中随机选取的噪声矩阵,$Ber_\theta$表示{0,1}上的伯努利分布,1的概率为θ,0的概率为1-θ;

[0072] (4b)用户根据消息认证码HMAC密钥k_{mac}和密文文件ψ_j,利用下式计算密文文件ψ_j的消息认证标签T_j:

[0073] T_j＝HMAC(k_{mac},ψ_j)；

[0074] (4c)用户按如下步骤为明文文件ε_j生成索引比特串I_j：

[0075] (4c1)用户随机均匀选取第一秘密值s∈{0,1}$^{\gamma}$、第二秘密值r∈{0,1}$^{\gamma}$，生成一个可记录2^{τ}个关键字(i,w_i)的索引字典，其中，i为标号，i∈[1,2^{τ}]，w_i为关键字，w_i∈{0,1}*，*表示任意长度，将索引字典和两个秘密值s、r秘密保存；

[0076] (4c2)用户根据第一秘密值s选取伪随机置换函数族$P_K(x)$中的伪随机置换函数$P_s(x)$，根据第二秘密值r选取第一伪随机函数族$F_K(x)$中的函数$F_r(x)$；

[0077] (4c3)用户计算下标值r_i＝$F_r(i)$，i∈[1,2^{τ}]，根据r_i的值选取第二伪随机函数族$G_K(x)$中的函数$G_{ri}(x)$；

[0078] (4c4)用户根据ε_j中是否包含关键字w_i，为明文文件ε_j生成一个2^{τ}长的初始比特串I_j'：

[0079] 若明文文件ε_j包含关键字w_i，则置初始比特串I_j'的第$P_s(i)$位为1，即$I_j'[P_s(i)]$＝1；

[0080] 若明文文件ε_j不包含关键字w_i，则置初始比特串I_j'的第$P_s(i)$位为0，即$I_j'[P_s(i)]$＝0；

[0081] 遍历i的所有值，得到初始比特串I_j'；

[0082] (4c5)用户将初始比特串I_j'第i位的值与函数值$G_{ri}(j)$进行异或操作，即$I_j[i]=I_j'[i]\oplus G_{r_i}(j)$，得到索引比特串$I_j$的第i位的值，遍历i的所有值，得到索引比特串$I_j$。

[0083] 步骤5，数据上传。

[0084] (5a)用户通过安全的信道，将消息认证码密钥k_{mac}发送给云服务器，并将消息{I_j||ψ_j||T_j}上传至云服务器，其中，1≤j≤n，n为明文文件总数，||表示级联符号；

[0085] (5b)云服务器利用消息认证码HMAC的验证算法Verify()，对每个密文文件进行完整性验证，验证结果用v_j表示，即v_j＝Verify(k_{mac},ψ_j,T_j)，其中，1≤j≤n，n为明文文件总数；

[0086] 若v_j＝1，表明ψ_j在上传过程中未被篡改，则云服务器接收该消息，并将索引字符串I_j保存到索引字符串集合I中，同时向用户返回“ψ_j上传成功”的通知；

[0087] 若v_j＝0，表明ψ_j在上传过程中被篡改，则云服务器拒绝接收该消息，并向用户返回“ψ_j上传错误”的通知；

[0088] (5c)用户根据收到的通知内容确定是否上传成功：

[0089] 若用户接收到“ψ_j上传成功”的通知，表明ψ_j已经成功上传至云服务器；

[0090] 若用户接收到“ψ_j上传错误”的通知，则返回步骤(5a)。

[0091] 步骤6，下载密文并解密。

[0092] 参照图3，本步骤的具体实现如下：

[0093] (6a)用户生成需下载文件中的关键字w_μ的陷门T_{w_μ}，并上传至云服务器：

[0094] (6a1)用户从索引字典中找到与关键字w_μ对应的标号μ；

[0095] (6a2)用户根据第一秘密值s选取伪随机置换函数族$P_K(x)$中的伪随机置换函数$P_s(x)$，根据第二秘密值r选取第一伪随机函数族$F_K(x)$中的函数$F_r(x)$；

[0096] (6a3)用户根据标号μ计算置换标号p＝$P_s(\mu)$；

[0097] (6a4)用户根据置换标号p计算函数索引值f＝F_r(p)；

[0098] (6a5)用置换标号p和函数索引值f，构成陷门$T_{w_\mu}=(p,f)$；

[0099] (6b)云服务器根据陷门T_{w_μ}，对已存储的文件索引比特串集合I进行匹配检索：

[0100] (6b1)云服务器将索引比特串I_j中置换标号p对应的位值与函数值G_f(j)进行异或操作，即$I'_j[p]=I_j[p]\oplus G_f(j)$，得到初始比特串$I_j'$中置换标号p对应的位值，其中，p是陷门$T_{w_\mu}$中的置换标号，f是陷门$T_{w_\mu}$中的函数索引值，$G_f$(x)是根据f的值从第二伪随机函数族$G_K$(x)中选取的伪随机函数，$I_j'$[p]表示初始比特串$I_j'$中置换标号p对应的位值，$I_j$[p]表示索引比特串$I_j$中置换标号p对应的位值，⊕表示异或操作；

[0101] (6b2)云服务器遍历j的所有值，若存在j∈[1,n]，使得初始比特串I_j'中置换标号p对应的位值为1，即I_j'[p]＝1，则匹配成功，云服务器给用户返回相应的密文ψ，继续步骤(6c)；若不存在，则匹配失败，云服务器给用户返回“检索失败”的通知；

[0102] (6c)用户解密密文ψ获得对应的明文文件ε：

[0103] (6c1)用户根据对称密钥S和密文文件ψ中的每一个密文矩阵块W＝(A,C)，计算中间矩阵Q：

[0104] Q＝C-A•S；

[0105] (6c2)用户对中间矩阵Q的每一列调用纠错码D进行解码，得到相应的明文矩阵块M；

[0106] (6c3)用户将所有的明文矩阵块M级联起来，得到对应的明文文件ε。

[0107] 以上描述仅是本发明的一个具体实例，不构成对本发明的任何限制，显然对于本领域的专业人员来说，在了解了本发明内容和原理后，都可能在不背离本发明原理、结构的情况下，进行形式和细节上的各种修正和改变，但是这些基于本发明思想的修正和改变仍在本发明的权利要求保护范围之内。

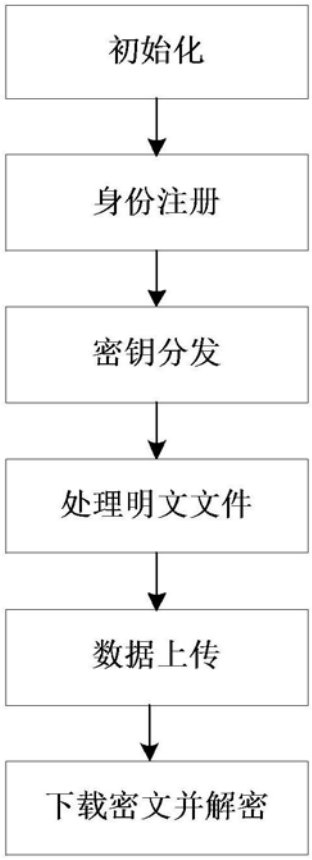

初始化
身份注册
密钥分发
处理明文文件
数据上传
下载密文并解密

图1

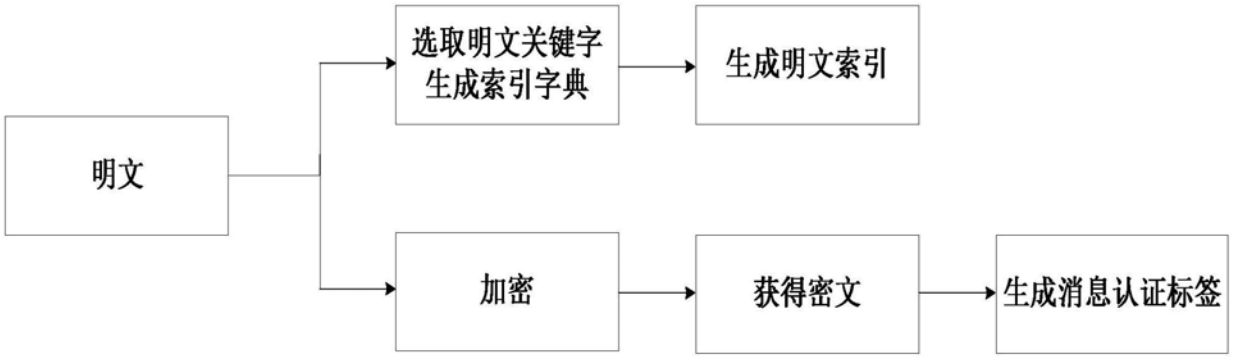

明文
选取明文关键字
生成索引字典
生成明文索引
加密
获得密文
生成消息认证标签

图2

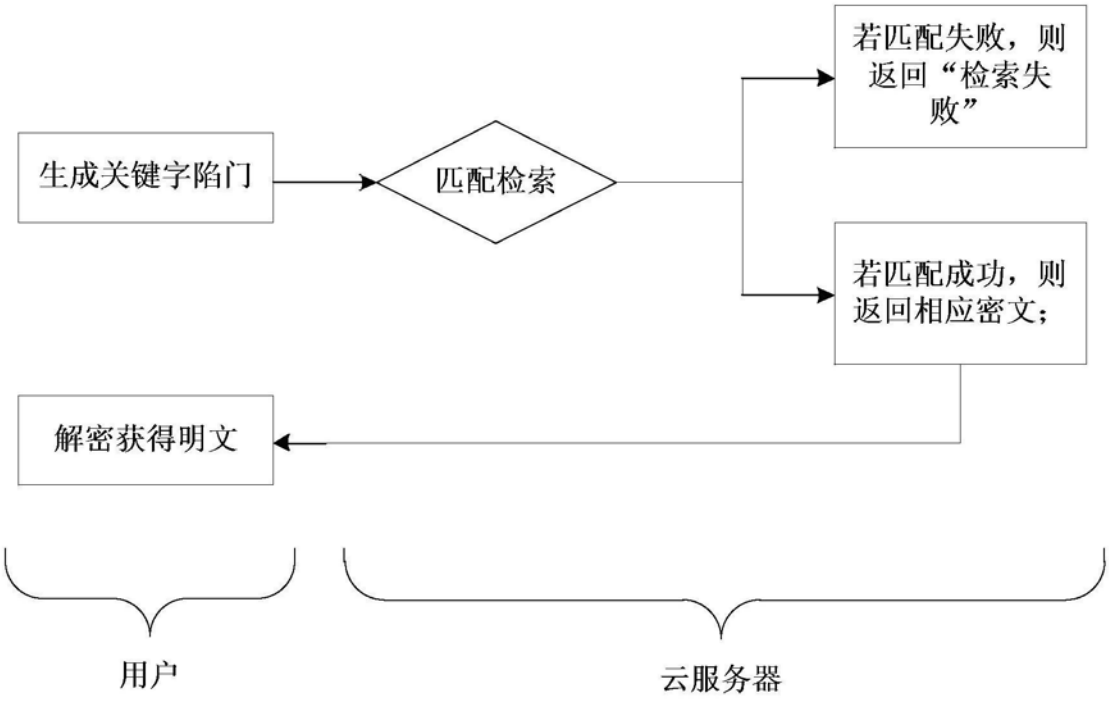


图3