(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 106789082 A
(43)申请公布日 2017.05.31

(21)申请号 201710017610.6

(22)申请日 2017.01.11

(71)申请人 西南石油大学
地址 610500 四川省成都市新都区新都大道8号

(72)发明人 张晓均 张新鹏 张源 刘勇

(74)专利代理机构 成都点睛专利代理事务所（普通合伙）51232
代理人 葛启函

(51)Int.Cl.
*H04L 9/32*(2006.01)
*H04L 9/00*(2006.01)
*H04L 29/06*(2006.01)

权利要求书2页 说明书6页

(54)发明名称

基于无线体域网的云存储医疗数据批量自审计方法

(57)摘要

本发明属于信息安全技术领域，具体涉及基于无线体域网的云存储医疗数据批量自审计方法。本发明方法设计的密码算法的安全性基于离散对数困难问题，能够确保恶意云服务器不能产生伪造的审计证明响应信息欺骗云用户通过审计验证过程。在审计方法中，云用户利用线性同态聚合签名算法构造同态线性认器，可以同时批量审计多个医疗数据文件的完整性，并且审计过程不需要计算开销较大的双线性对运算，特别适用于需要轻量级计算量，存储空间有限，需要高效实现无线体域网的应用场景。

CN 106789082 A

1.基于无线体域网的云存储医疗数据批量自审计方法,其特征在于,包括以下步骤:

a.系统初始化:系统对医疗数据文件进行分块处理获得多个医疗数据块,并生成签名算法的公私钥对;同时生成用于对医疗数据文件的身份标识进行轻量级签名的公私钥对,系统再选取一个轻量级对称加密算法及其对称密钥;

b.签名产生:用户首先调用伪随机数发生器和伪随机函数产生每个医疗数据块的同态消息认证码的匹配系数,并采用与步骤a中相同的签名算法计算同态消息认证码的数字签名,同时分别对不同的医疗数据文件的身份标识计算数字签名产生医疗数据文件标签,并将多个医疗数据文件进行对称加密;最后将这些数字签名以及医疗数据文件的密文发送到云服务器,并在本地客户端删除这些数据;

c.审计证明产生:由用户产生一个审计挑战信息,并将挑战信息发送给云服务器;云服务器收到审计挑战信息后,产生多个医疗数据文件的聚合审计证明响应信息,并返回给用户;

d.审计证明验证:用户得到聚合的审计证明响应信息之后,利用与步骤a中相同的签名算法的公钥以及对称加密算法的密钥验证这个聚合的审计证明响应信息的有效性。

2.根据权利要求1所述的基于无线体域网的云存储医疗数据批量自审计方法,其特征在于,所述步骤a的具体方法为:

a1.将医疗数据文件F分成n个医疗数据块,这n个医疗数据块分别进一步分成在$Z_q$中的k个元素;F表示为:$F=\begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix}=\begin{pmatrix} f_{1,1} & \cdots & f_{1,k} \\ \vdots & \ddots & \vdots \\ f_{n,1} & \cdots & f_{n,k} \end{pmatrix}\in Z_q^{n\times k}$;

a2.用户选取$g\in Z_p^*$,满足$g^q\equiv 1 \mod p$,随机地选取私钥x,满足1<x<q,计算公钥$y=g^x \mod p$;用户选取一个轻量级对称加密算法$\varphi$,设置对称密钥为τ,并选取一个轻量级数字签名算法SSig,其公私钥对为(spk,ssk);

a3.系统产生伪随机数发生器PRG:$K_{prg}\rightarrow Z_q^k$,伪随机函数PRF:$K_{prf}\times I\rightarrow Z_q$,其中$K_{prg}$,$K_{prf}$分别为PRG和PRF的私钥集合,I为文件中每个数据块的索引指数集合;系统随机选取对称密钥对skp=($sk_{prg}$,$sk_{prf}$),其中$sk_{prg}\in K_{prg}$,$sk_{prf}\in K_{prf}$。

3.根据权利要求2所述的基于无线体域网的云存储医疗数据批量自审计方法,其特征在于,所述步骤b的具体方法为:

b1.对于$1\le \ell \le L$,L为医疗数据文件的总数,$\ell$为当前选定的医疗数据文件编号,给定每一个医疗数据文件$F_\ell=\{f_{\ell,1},\cdots,f_{\ell,n}\}$包含n个医疗数据块,其中每一个医疗数据块$f_{\ell,j}=(f_{\ell,j,1},\cdots,f_{\ell,j,k})\in Z_q^k$, $j=1,2,\cdots,n$;医疗文件$F_\ell$的身份标识为$id_\ell$,为了确保医疗数据文件身份标识的唯一性,用户调用一个轻量级数字签名算法SSig计算$id_\ell$的标签$tag_\ell=id_\ell \| SSig_{ssk}(id_\ell)$;

b2.用户利用伪随机数发生器PRG和伪随机函数PRF分别产生随机向量$\varsigma_\ell=(\varsigma_{\ell,1},\cdots,\varsigma_{\ell,k})\leftarrow PRG(sk_{prg})\in Z_q^k$,随机数$\xi_{\ell,j}\leftarrow PRF(sk_{prf},id_\ell\|j)\in Z_q$;用户计算医疗数据块$f_{\ell,j}=(f_{\ell,j,1},\cdots,f_{\ell,j,k})$的同态消息认证码$\sigma_{\ell,j}=\sum_{\theta=1}^{k}\varsigma_{\ell,\theta}f_{\ell,j,\theta}+\xi_{\ell,j}\in Z_q$;然后,用户利用私钥x

计算$\sigma_{\ell,j}$的数字签名如下：

b21.随机选择$r_{\ell,j} \leftarrow Z_q$，计算$s_{\ell,j} \equiv g^{r_{\ell,j}} \mod p$，$s'_{\ell,j} \equiv s_{\ell,j} \mod q$；

b22.计算$t_{\ell,j} = (s'_{\ell,j} r_{\ell,j} + \sigma_{\ell,j} x) \mod q$；

b23.输出同态消息认证码$\sigma_{\ell,j}$的数字签名$\delta_{\ell,j} = (s_{\ell,j}, t_{\ell,j})$；定义这些签名的集合为$\Omega_\ell = \{\delta_{\ell,j}\}_{1 \le j \le n}$；

b3.对于1≤1≤L，给定每一个医疗数据文件$F_\ell = \{f_{\ell,1}, \cdots, f_{\ell,n}\}$，为了确保用户的医疗数据文件的机密性，用户调用对称加密算法$\varphi$，对称密钥为τ，将$f_{\ell,j} = (f_{\ell,j,1}, \cdots, f_{\ell,j,k})$加密为$f'_{\ell,j} = (f_{\ell,j,1} + \varphi_\tau(1, id_\ell \| j), \cdots, f_{\ell,j,k} + \varphi_\tau(k, id_\ell \| j))$，则$F_\ell = \{f_{\ell,1}, \cdots, f_{\ell,n}\}$加密为$F'_\ell = (f'_{\ell,1}, \cdots, f'_{\ell,n})$；

b4.用户发送$\{F'_\ell, tag_\ell, \Omega_\ell\}$给云服务器，并在客户本地端删除这些信息。

4.根据权利要求3所述的基于无线体域网的云存储医疗数据批量自审计方法，其特征在于，所述步骤c的具体方法为：

c1.用户首先取回每一个医疗数据文件标签$tag_\ell$，并利用公钥spk验证签名$SSig_{ssk}(id_\ell)$的有效性；当验证完标签的有效性之后，用户产生审计挑战信息如下：

c11.从{1,2,…,n}中随机选取一个含有c个元素的子集$\mathcal{L} = \{l_1, \cdots, l_c\}$；

c12.对于每一个$j \in \mathcal{L}$，用户产生相应的随机值$\beta_j \in Z_q$，最后用户发送审计挑战信息$chal = \{(j, \beta_j)\}_{j \in \mathcal{L}}$给云服务器；

c2.一旦接收到审计挑战信息$chal = \{(j, \beta_j)\}_{j \in \mathcal{L}}$，云服务器产生审计证明响应信息如下：

c21.计算组合信息块$u_{\ell,\theta} = \sum_{j \in \mathcal{L}} \beta_j f'_{\ell,j,\theta} \mod q$，其中θ∈{1，…，k}，得到$u_\ell = (u_{\ell,1}, \cdots, u_{\ell,\theta}, \cdots, u_{\ell,k})$；

c22.计算聚合签名$s = \Pi_{\ell=1}^{L} \Pi_{j \in \mathcal{L}} s_{\ell,j}^{\beta_j s_{\ell,j}} \mod p$，$t = \Sigma_{\ell=1}^{L} \Sigma_{j \in \mathcal{L}} \beta_j t_{\ell,j} \mod q$；

c23.云服务器发送$(\{u_\ell\}_{1 \le \ell \le L}, s, t, \{id_\ell\}_{1 \le \ell \le L})$作为审计证明响应信息给用户。

5.根据权利要求4所述的基于无线体域网的云存储医疗数据批量自审计方法，其特征在于，所述步骤d的具体方法为：

d1.对于每一个$1 \le \ell \le L$，计算$\varsigma_\ell = (\varsigma_{\ell,1}, \cdots, \varsigma_{\ell,k}) \leftarrow PRG(sk_{prg}) \in Z_q^k$，$\xi_{\ell,j} \leftarrow PRF(sk_{prf}, id_\ell \| j) \in Z_q$，$j \in \mathcal{L}$；

d2.计算$\omega_{\ell,1} = \sum_{\theta=1}^{k} \varsigma_{\ell,\theta} u_{\ell,\theta} + \sum_{j \in \mathcal{L}} \beta_j \xi_{\ell,j} \in Z_q$，$\omega_{\ell,2} = \sum_{\theta=1}^{k} \sum_{j \in \mathcal{L}} \varsigma_{\ell,\theta} \beta_j \varphi_\tau(\theta, id_\ell \| j) \in Z_q$，其中1≤θ≤k，$1 \le \ell \le L$；

d3.验证方程$g^t = s \prod_{\ell=1}^{L} y^{\omega_{\ell,1} - \omega_{\ell,2}} \mod p$是否成立，若成立，则审计证明响应有效，若不成了，则审计证明响应无效。

# 基于无线体域网的云存储医疗数据批量自审计方法

## 技术领域

[0001] 本发明属于信息安全技术领域，具体涉及基于无线体域网的云存储医疗数据批量自审计方法。

## 背景技术

[0002] 随着无线通信、低功耗集成、传感器技术的迅速发展，无线传感网络开始广泛应用于智能电网、医疗健康、工业控制等各个领域。作为无线传感器网络的一个重要应用，无线体域网已日益受到学术界和医学界的重视。无线体域网使用传感器节点收集患者的心率、脉搏、体温等医疗信息。这些医疗数据需要被及时处理的同时还需要从医生处及时获得反馈。由于受到存储、处理、供能等有限的资源制约，依靠传统的无线体域网要达到这些目的是相当困难的。因此，需要无线体域网与云计算平台集成来存储和处理实时的医疗数据。

[0003] 云辅助无线体域网配备了强大的基于云计算和存储资源，将医疗传感器植入患者的体表并周期性地收集健康医疗信息并通过移动设备或是互联网发送给云辅助医疗系统。一旦收到这些数据，云辅助医疗系统发送数据到相关医疗工作者做临床诊断并将其存储于云存储系统。此外，患者的家人与亲属亦同样可以通过云辅助医疗系统检索相关健康状态信息。对于许多慢性疾病，医疗工作者对大量的数据进行的详尽分析以辅助实现正确地诊断。一旦收到医疗工作者的指令，云辅助系统使用它基于云的强大计算资源来有效、迅速地完成所下达的任务。

[0004] 存储于云服务器上的健康医疗数据，可以作为医生临床诊断的基础。虽然云存储服务带来了许多便利优势，例如成本效益，更方便的数据访问。但是在云存储拥有这些优势的同时，它同时对患者的外包医疗数据带来了新的安全性威胁。一旦这些医疗数据遭到攻击者的恶意篡改，都会造成医生的临床误诊致使患者病情加重甚至具有死亡的危险，因此云服务器上的健康医疗数据的完整性变得格外重要。出于对医疗数据完整性以及安全性的考虑，患者需要使用一个完整性审计方案来确保患者的医疗数据在云服务器上能够正确地存储。目前典型的云存储数据完整性审计方案，由于需要计算开销很大的双线性对运算，并不适用于云辅助的无线体域网的应用场景。因此设计轻量级的具有隐私保护性能的云辅助无线体域网的医疗数据完整性安全审计方案是一项具有重要意义的研究工作。

## 发明内容

[0005] 本发明的目的是，提供一种适用于无线体域网的云存储医疗数据批量自审计方法。

[0006] 本发明的技术方案为：基于无线体域网的云存储医疗数据批量自审计方法，其特征在于，包括以下步骤：

[0007] a.系统初始化：系统对医疗数据文件进行分块处理获得多个医疗数据块，并生成签名算法的公私钥对；同时生成用于对医疗数据文件的身份标识进行轻量级签名的公私钥对，系统再选取一个轻量级对称加密算法及其对称密钥；

[0008] b.签名产生:用户首先调用伪随机数发生器和伪随机函数产生每个医疗数据块的同态消息认证码的匹配系数,并采用与步骤a中相同的签名算法计算同态消息认证码的数字签名,同时分别对不同的医疗数据文件的身份标识计算数字签名产生医疗数据文件标签,并将多个医疗数据文件进行对称加密;最后将这些数字签名以及医疗数据文件的密文发送到云服务器,并在本地客户端删除这些数据;

[0009] c.审计证明产生:由用户产生一个审计挑战信息,并将挑战信息发送给云服务器;云服务器收到审计挑战信息后,产生多个医疗数据文件的聚合审计证明响应信息,并返回给用户;

[0010] d.审计证明验证:用户得到聚合的审计证明响应信息之后,利用与步骤a中相同的签名算法的公钥以及对称加密算法的密钥验证这个聚合的审计证明响应信息的有效性。

[0011] 进一步的,所述步骤a的具体方法为:

[0012] a1.将医疗数据文件F分成n个医疗数据块,这n个医疗数据块分别进一步分成在$Z_q$($Z_q$是模q剩余类环,q是素数)中的k个元素;F表示为:$F=\begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix}=\begin{pmatrix} f_{1,1} & \cdots & f_{1,k} \\ \vdots & \ddots & \vdots \\ f_{n,1} & \cdots & f_{n,k} \end{pmatrix}\in Z_q^{n\times k}$;

[0013] a2.用户选取$g\in Z_p^*$($Z_p$是模p剩余类环,p是素数),满足$g^q\equiv 1 \bmod p$,随机地选取私钥x,满足1<x<q,计算公钥$y=g^x \bmod p$;用户选取一个轻量级对称加密算法$\varphi$,设置对称密钥为τ,并选取一个轻量级数字签名算法SSig,其公私钥对为(spk,ssk);

[0014] a3.系统产生伪随机数发生器$PRG:K_{prg}\to Z_q^k$,伪随机函数PRF:$K_{prf}\times I\to Z_q$,其中$K_{prg}$,$K_{prf}$分别为PRG和PRF的私钥集合,I为文件中每个数据块的索引指数集合;系统随机选取对称密钥对skp=($sk_{prg}$,$sk_{prf}$),其中$sk_{prg}\in K_{prg}$,$sk_{prf}\in K_{prf}$。

[0015] 进一步的,所述步骤b的具体方法为:

[0016] b1.对于$1\le \ell \le L$,L为医疗数据文件的总数,$\ell$为当前选定的医疗数据文件编号,给定每一个医疗数据文件$F_\ell=\{f_{\ell,1},\cdots,f_{\ell,n}\}$包含n个医疗数据块,其中每一个医疗数据块$f_{\ell,j}=(f_{\ell,j,1},\cdots,f_{\ell,j,k})\in Z_q^k,\ j=1,2,\cdots,n$;医疗文件$F_\ell$的身份标识为$id_\ell$,为了确保医疗数据文件身份标识的唯一性,用户调用一个轻量级数字签名算法SSig计算$id_\ell$的标签$tag_\ell=id_\ell \| SSig_{ssk}(id_\ell)$;

[0017] b2.用户利用伪随机数发生器PRG和伪随机函数PRF分别产生随机向量$\varsigma_\ell=(\varsigma_{\ell,1},\cdots,\varsigma_{\ell,k})\leftarrow PRG(sk_{prg})\in Z_q^k$,随机数$\xi_{\ell,j}\leftarrow PRF(sk_{prf},id_\ell\|j)\in Z_q$;用户计算医疗数据块$f_{\ell,j}=(f_{\ell,j,1},\cdots,f_{\ell,j,k})$的同态消息认证码$\sigma_{\ell,j}=\sum_{\theta=1}^{k}\varsigma_{\ell,\theta}f_{\ell,j,\theta}+\xi_{\ell,j}\in Z_q$;然后,用户利用私钥x计算$\sigma_{\ell,j}$的数字签名如下:

[0018] b21.随机选择$r_{\ell,j}\leftarrow Z_q$,计算$s_{\ell,j}\equiv g^{r_{\ell,j}} \bmod p$,$s'_{\ell,j}\equiv s_{\ell,j} \bmod q$;

[0019] b22.计算$t_{\ell,j}=(s'_{\ell,j}r_{\ell,j}+\sigma_{\ell,j}x) \bmod q$;

[0020] b23.输出同态消息认证码$\sigma_{\ell,j}$的数字签名$\delta_{\ell,j}=(s_{\ell,j},t_{\ell,j})$;定义这些签名的集合为$\Omega_\ell=\{\delta_{\ell,j}\}_{1\le j\le n}$;

[0021] b3.对于1≤l≤L,给定每一个医疗数据文件$F_\ell=\{f_{\ell,1},\cdots,f_{\ell,n}\}$,为了确保用户的医疗数据文件的机密性,用户调用对称加密算法$\varphi$,对称密钥为τ,将$f_{\ell,j}=(f_{\ell,j,1},\cdots,f_{\ell,j,k})$加密为$f'_{\ell,j}=(f_{\ell,j,1}+\varphi_\tau(1,id_\ell\|j),\cdots,f_{\ell,j,k}+\varphi_\tau(k,id_\ell\|j))$,则$F_\ell=\{f_{\ell,1},\cdots,f_{\ell,n}\}$加密为$F'_\ell=(f'_{\ell,1},\cdots,f'_{\ell,n})$;

[0022] b4.用户发送$\{F'_\ell,tag_\ell,\Omega_\ell\}$给云服务器,并在客户本地端删除这些信息。

[0023] 进一步的,所述步骤c的具体方法为:

[0024] c1.用户首先取回每一个医疗数据文件标签$tag_\ell$,并利用公钥spk验证签名$SSig_{ssk}(id_\ell)$的有效性;当验证完标签的有效性之后,用户产生审计挑战信息如下:

[0025] c11.从{1,2,…,n}中随机选取一个含有c个元素的子集$\mathcal{L}=\{l_1,\cdots,l_c\}$;

[0026] c12.对于每一个$j\in\mathcal{L}$,用户产生相应的随机值$\beta_j\in Z_q$,最后用户发送审计挑战信息$chal=\{(j,\beta_j)\}_{j\in\mathcal{L}}$给云服务器;

[0027] c2.一旦接收到审计挑战信息$chal=\{(j,\beta_j)\}_{j\in\mathcal{L}}$,云服务器产生审计证明响应信息如下:

[0028] c21.计算组合信息块$u_{\ell,\theta}=\sum_{j\in\mathcal{L}}\beta_j f'_{\ell,j,\theta} \mod q$,其中θ∈{1,…,k},得到$u_\ell=(u_{\ell,1},\cdots,u_{\ell,\theta},\cdots,u_{\ell,k})$;

[0029] c22.计算聚合签名$s=\Pi_{\ell=1}^{L}\Pi_{j\in\mathcal{L}}s_{\ell,j}^{\beta_j s_{\ell,j}} \mod p$, $t=\Sigma_{\ell=1}^{L}\Sigma_{j\in\mathcal{L}}\beta_j t_{\ell,j} \mod q$;

[0030] c23.云服务器发送$(\{u_\ell\}_{1\le\ell\le L},s,t,\{id_\ell\}_{1\le\ell\le L})$作为审计证明响应信息给用户。

[0031] 进一步的,所述步骤d的具体方法为:

[0032] d1.对于每一个$1\le\ell\le L$,计算$\varsigma_\ell=(\varsigma_{\ell,1},\cdots,\varsigma_{\ell,k})\leftarrow PRG(sk_{prg})\in Z_q^k,\xi_{\ell,j}\leftarrow PRF(sk_{prf},id_\ell\|j)\in Z_q$, $j\in\mathcal{L}$;

[0033] d2.计算$\omega_{\ell,1}=\sum_{\theta=1}^{k}\varsigma_{\ell,\theta}u_{\ell,\theta}+\sum_{j\in\mathcal{L}}\beta_j\xi_{\ell,j}\in Z_q$, $\omega_{\ell,2}=\sum_{\theta=1}^{k}\sum_{j\in\mathcal{L}}\varsigma_{\ell,\theta}\beta_j\varphi_\tau(\theta,id_\ell\|j)\in Z_q$,其中1≤θ≤k,$1\le\ell\le L$;

[0034] d3.验证方程$g^t=s\prod_{\ell=1}^{L}y^{\omega_{\ell,1}-\omega_{\ell,2}} \mod p$是否成立,若成立,则审计证明响应有效,若不成了,则审计证明响应无效。

[0035] 本发明的有益效果为,本发明方法设计的密码算法的安全性基于离散对数困难问题,能够确保恶意云服务器不能产生伪造的审计证明响应信息欺骗云用户通过审计验证过程。在审计方法中,云用户利用线性同态聚合签名算法构造同态线性认器,可以同时批量审计多个医疗数据文件的完整性,并且审计过程不需要计算开销较大的双线性对运算,特别适用于需要轻量级计算量,存储空间有限,需要高效实现无线体域网的应用场景。

## 具体实施方式

[0036] 下面详细描述本发明的技术方案:

[0037] 本发明的步骤分为四个部分:

[0038] 系统初始化:系统对医疗数据文件进行分块处理,并生成Schnorr变型签名算法的

公私钥对，生成用于对医疗数据文件的身份标识进行轻量级签名的公私钥对，系统再选取一个轻量级对称加密算法及其对称密钥。

[0039] 签名产生步骤：用户首先调用伪随机数发生器和伪随机函数产生每个医疗数据块的同态消息认证码的匹配系数，并采用Schnorr变型签名算法计算同态消息认证码的数字签名，同时分别对不同的医疗数据文件的身份标识计算数字签名产生医疗数据文件标签，并将多个医疗数据文件进行对称加密。最后将这些数字签名以及医疗数据文件的密文发送到云服务器，并在本地客户端删除这些数据。

[0040] 审计证明产生步骤：为了能够同时批量审计外包存储在云服务器上的医疗数据的完整性，用户产生一个审计挑战信息，并将挑战信息发送给云服务器。云服务器收到挑战信息后，产生多个医疗数据文件的聚合审计证明响应信息，并返回给用户。

[0041] 审计证明验证步骤：用户得到这个聚合的审计证明响应信息之后，利用Schnorr变型签名算法的公钥以及对称加密算法的密钥验证这个聚合的审计证明响应信息的有效性。

[0042] 以下给出一个具体实例说明：

[0043] 本发明所要解决的技术问题是，适用于无线体域网的云存储医疗数据完整性批量自审计方法。

[0044] 该批量自审计方法包括以下基本步骤：Setup，SigGen，ProofGen，VerifyProof。

[0045] Setup：包括以下三个子步骤：

[0046] (1)将医疗数据文件F分成n个医疗数据块，这n个医疗数据块分别进一步分成在$Z_q$中的k个元素。F表示如下：$F=\begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix}=\begin{pmatrix} f_{1,1} & \cdots & f_{1,k} \\ \vdots & \ddots & \vdots \\ f_{n,1} & \cdots & f_{n,k} \end{pmatrix}\in Z_q^{n\times k}$。

[0047] (2)用户选取$g\in Z_p^*$，满足$g^q\equiv 1 \pmod p$，随机地选取私钥x，满足1<x<q，计算公钥$y=g^x \bmod p$。接着用户选取一个轻量级对称加密算法$\varphi$(设置对称密钥为τ)，并选取一个轻量级数字签名算法SSig，其公私钥对为(spk，ssk)。

[0048] (3)系统产生伪随机数发生器$PRG: K_{prg}\rightarrow Z_q^k$，伪随机函数PRF：$K_{prf}\times I\rightarrow Z_q$，其中$K_{prg}$，$K_{prf}$分别为PRG和PRF的私钥集合，I为文件中每个数据块的索引指数集合。接着系统随机选取对称密钥对$skp=(sk_{prg},sk_{prf})$，其中$sk_{prg}\in K_{prg}$，$sk_{prf}\in K_{prf}$。

[0049] SigGen：用户同时产生L个医疗数据文件的数字签名，以及产生这L个医疗数据文件的密文如下：

[0050] (1)对于$1\le \ell\le L$，给定每一个医疗数据文件$F_\ell=\{f_{\ell,1},\cdots,f_{\ell,n}\}$包含n个医疗数据块，其中每一个医疗数据块$f_{\ell,j}=(f_{\ell,j,1},\cdots,f_{\ell,j,k})\in Z_q^k$，$j=1,2,\cdots,n$。医疗文件$F_\ell$的身份标识为$id_\ell$，为了确保医疗数据文件身份标识的唯一性，用户调用一个轻量级数字签名算法SSig计算$id_\ell$的标签$tag_\ell=id_\ell\| SSig_{ssk}(id_\ell)$。

[0051] (2)用户利用伪随机数发生器PRG和伪随机函数PRF分别产生随机向量$\varsigma_\ell=(\varsigma_{\ell,1},\cdots,\varsigma_{\ell,k})\leftarrow PRG(sk_{prg})\in Z_q^k$，随机数$\xi_{\ell,j}\leftarrow PRF(sk_{prf},id_\ell\|j)\in Z_q$。用户计算医疗数据块$f_{\ell,j}=(f_{\ell,j,1},\cdots,f_{\ell,j,k})$的同态消息认证码$\sigma_{\ell,j}=\sum_{\theta=1}^{k}\varsigma_{\ell,\theta}f_{\ell,j,\theta}+\xi_{\ell,j}\in Z_q$。然后，用户利用私钥x

计算$\sigma_{\ell,j}$的数字签名如下：

[0052] (2a)随机选择$r_{\ell,j} \leftarrow Z_q$，计算$s_{\ell,j} \equiv g^{r_{\ell,j}} \mod p$，$s'_{\ell,j} \equiv s_{\ell,j} \mod q$；

[0053] (2b)计算$t_{\ell,j} = (s'_{\ell,j} r_{\ell,j} + \sigma_{\ell,j} x) \mod q$；

[0054] (2c)输出同态消息认证码$\sigma_{\ell,j}$的数字签名$\delta_{\ell,j} = (s_{\ell,j}, t_{\ell,j})$。定义这些签名的集合为$\Omega_\ell = \{\delta_{\ell,j}\}_{1 \le j \le n}$。

[0055] (3)对于1≤1≤L,给定每一个医疗数据文件$F_\ell = \{f_{\ell,1}, \cdots, f_{\ell,n}\}$，为了确保用户的医疗数据文件的机密性，用户调用对称加密算法$\varphi$(对称密钥为τ)将$f_{\ell,j} = (f_{\ell,j,1}, \cdots, f_{\ell,j,k})$加密为$f'_{\ell,j} = (f_{\ell,j,1} + \varphi_\tau(1, id_\ell \| j), \cdots, f_{\ell,j,k} + \varphi_\tau(k, id_\ell \| j))$，这样$F_\ell = \{f_{\ell,1}, \cdots, f_{\ell,n}\}$加密为$F'_\ell = (f'_{\ell,1}, \cdots, f'_{\ell,n})$。

[0056] 最后，用户发送$\{F'_\ell, tag_\ell, \Omega_\ell\}$给云服务器，并在客户本地端删除这些信息。

[0057] ProofGen:用户产生审计挑战信息，云服务器对此产生审计证明响应信息，步骤如下：

[0058] (1)用户首先取回每一个医疗数据文件标签$tag_\ell$，并利用公钥spk验证签名$SSig_{ssk}(id_\ell)$的有效性。当验证完标签的有效性之后，用户产生审计挑战信息如下：

[0059] (1a)从{1,2,…,n}中随机选取一个含有c个元素的子集$\mathcal{L} = \{l_1, \cdots, l_c\}$；

[0060] (1b)对于每一个$j \in \mathcal{L}$，用户产生相应的随机值$\beta_j \in Z_q$，最后用户发送审计挑战信息$chal = \{(j, \beta_j)\}_{j \in \mathcal{L}}$给云服务器。

[0061] (2)一旦接收到审计挑战信息$chal = \{(j, \beta_j)\}_{j \in \mathcal{L}}$，云服务器产生审计证明响应信息如下：

[0062] (2a)计算组合信息块$u_{\ell,\theta} = \sum_{j \in \mathcal{L}} \beta_j f'_{\ell,j,\theta} \mod q$，其中θ∈{1,…,k}，这样得到$u_\ell = (u_{\ell,1}, \cdots, u_{\ell,\theta}, \cdots, u_{\ell,k})$；

[0063] (2b)计算聚合签名$s = \Pi_{\ell=1}^{L} \Pi_{j \in \mathcal{L}} s_{\ell,j}^{\beta_j s_{\ell,j}} \mod p$，$t = \Sigma_{\ell=1}^{L} \Sigma_{j \in \mathcal{L}} \beta_j t_{\ell,j} \mod q$。

[0064] (2c)云服务器发送$(\{u_\ell\}_{1 \le \ell \le L}, s, t, \{id_\ell\}_{1 \le \ell \le L})$作为审计证明响应信息给用户。

[0065] VerifyProof:用户按照如下步骤验证审计证明响应信息的有效性：

[0066] (1)对于每一个$1 \le \ell \le L$，计算$\varsigma_\ell = (\varsigma_{\ell,1}, \cdots, \varsigma_{\ell,k}) \leftarrow PRG(sk_{prg}) \in Z_q^k$，$\xi_{\ell,j} \leftarrow PRF(sk_{prf}, id_\ell \| j) \in Z_q$，$j \in \mathcal{L}$。

[0067] (2)计算$\omega_{\ell,1} = \sum_{\theta=1}^{k} \varsigma_{\ell,\theta} u_{\ell,\theta} + \sum_{j \in \mathcal{L}} \beta_j \xi_{\ell,j} \in Z_q$，$\omega_{\ell,2} = \sum_{\theta=1}^{k} \sum_{j \in \mathcal{L}} \varsigma_{\ell,\theta} \beta_j \varphi_\tau(\theta, id_\ell \| j) \in Z_q$，其中1≤θ≤k，$1 \le \ell \le L$。

[0068] (3)验证方程$g^t = s \prod_{\ell=1}^{L} y^{\omega_{\ell,1} - \omega_{\ell,2}} \mod p$是否成立。

[0069] 审计证明验证过程正确性如下：

$$g^{t}=g^{t=\sum_{\ell=1}^{L}\sum_{j\in\mathcal{L}}\beta_j t_{\ell,j}(\mathrm{mod}\,q)} \mod p$$

$$=\prod_{\ell=1}^{L} g^{\sum_{j\in\mathcal{L}}\beta_j t_{\ell,j}} \mod p$$

$$=\prod_{\ell=1}^{L} g^{\sum_{j\in\mathcal{L}}\beta_j(s'_{\ell,j}r_{t,j}+\sigma_{t,j}x(\mathrm{mod}q))} \mod p$$

$$=\prod_{\ell=1}^{L} g^{\sum_{j\in\mathcal{L}}\beta_j s'_{\ell,j}r_{t,j}}\, g^{\sum_{j\in\mathcal{L}}\beta_j\sigma_{t,j}x} \mod p$$

[0070]
$$=\prod_{\ell=1}^{L}\left(\prod_{j\in\mathcal{L}} s_{\ell,j}^{\beta_j s_{t,j}}\right) y^{\sum_{j\in\mathcal{L}}\beta_j\sigma_{t,j}} \mod p$$

$$=s\prod_{\ell=1}^{L} y^{\sum_{j\in\mathcal{L}}\beta_j\sum_{\theta=1}^{k}(\varsigma_{\ell,\theta}f_{t,j,\theta}+\xi_{t,j})} \mod p$$

$$=s\prod_{\ell=1}^{L} y^{\sum_{\theta=1}^{k}\varsigma_{\ell,\theta}\sum_{j\in\mathcal{L}}\beta_j f_{t,j,\theta}+\sum_{j\in\mathcal{L}}\beta_j\xi_{t,j}} \mod p$$

$$=s\prod_{\ell=1}^{L} y^{\sum_{\theta=1}^{k}\varsigma_{\ell,\theta}(u_{\ell,\theta}-\sum_{j\in\mathcal{L}}\beta_j\varphi_{\tau}(\theta,id_t\|j))+\sum_{j\in\mathcal{L}}\beta_j\xi_{t,j}} \mod p$$

$$=s\prod_{\ell=1}^{L} y^{\sum_{\theta=1}^{k}\varsigma_{\ell,\theta}u_{\ell,\theta}+\sum_{j\in\mathcal{L}}\beta_j\xi_{t,j}-\sum_{\theta=1}^{k}\sum_{j\in\mathcal{L}}\varsigma_{\ell,\theta}\beta_j\varphi_{\tau}(\theta,id_t\|j)} \mod p$$

[0071]
$$=s\prod_{\ell=1}^{L} y^{\varpi_{\ell,1}-\varpi_{\ell,2}} \mod p$$

[0072] 这样方程$g^{t}=s\prod_{\ell=1}^{L} y^{\varpi_{\ell,1}-\varpi_{\ell,2}} \mod p$成立。

[0073] 本发明基于无线体域网以及云计算的前沿应用场景，通过设计新颖的安全数字聚合签名算法，即设计并改进Schnorr数字签名算法为线性同态聚合签名算法，并进一步构造轻量级审计方案，使之能够有效适用于云辅助的无线体域网，帮助患者验证存储在云辅助医疗系统的健康数据的完整性，且有效检测出云医疗数据是否被篡改，从而防止医生的临床误诊。该发明方法设计的密码算法的安全性基于离散对数困难问题，能够确保恶意云服务器不能产生伪造的审计证明响应信息欺骗云用户通过审计验证过程。在审计方法中，云用户利用线性同态聚合签名算法构造同态线性认器，可以同时批量审计多个医疗数据文件的完整性，并且审计过程不需要计算开销较大的双线性对运算，特别适用于需要轻量级计算量，存储空间有限，需要高效实现无线体域网的应用场景。