(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 103997409 A
(43)申请公布日 2014.08.20

(21)申请号 201410182640.9

(22)申请日 2014.02.17

(30)优先权数据
13305176.3 2013.02.15 EP
13305371.0 2013.03.26 EP

(71)申请人 汤姆逊许可公司
地址 法国伊西莱穆利诺

(72)发明人 M·乔伊 B·利伯特

(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 吕晓章

(51)Int.Cl.
H04L 9/32(2006.01)

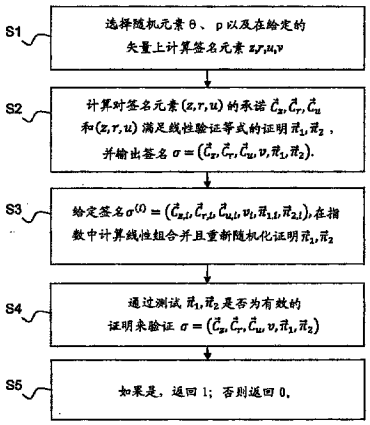
权利要求书2页 说明书9页 附图1页

(54)发明名称

产生和验证线性同态结构保留签名的加密设备和方法

(57)摘要

通过在处理器(120)中使用签名密钥 $sk=\{\chi_i,\gamma_i,\delta_i\}_{i=1}^{n}$ 通过计算 $z=\prod_{i=1}^{n}M_i^{-\chi_i}$，$r=\prod_{i=1}^{n}M_i^{-\gamma_i}$，$u=\prod_{i=1}^{n}M_i^{-\delta_i}$ 来计算签名元素(z，r，u)，并输出包含签名元素(z，r，u)的签名σ在矢量 $(M_1,\ldots,M_n)\in\hat{G}^n$ 上生成线性同态结构保留签名σ。该签名通过在处理器(220)中验证 $(M_1,\ldots,M_n)\neq(1_{\hat{G}},\ldots,1_{\hat{G}})$ 和(z，r，u)满足等式 $1_{G_T}=e(g_z,z)\cdot e(g_r,r)\cdot\prod_{i=1}^{n}e(g_i,M_i)$ $1_{G_T}=e(h_z,z)\cdot e(h,u)\cdot\prod_{i=1}^{n}e(h_i,M_i)$ 来进行验证；并且在验证成功的情形下确定该签名已经被成功地验证，否则该签名未被成功地验证。同样提供了完善方案和上下文隐藏方案。



CN 103997409 A

1. 一种在矢量$(M_1, \ldots, M_n) \in \hat{G}^n$上生成线性同态签名 σ 的方法，其中$\hat{G}$表示第一组，该方法包括在设备 (100) 的处理器 (120) 中：

- 使用签名密钥$sk = \{\chi_i, \gamma_i, \delta_i\}_{i=1}^n$通过计算

$z = \prod_{i=1}^n M_i^{-\chi_i}$，　　$r = \prod_{i=1}^n M_i^{-\gamma_i}$，　　$u = \prod_{i=1}^n M_i^{-\delta_i}$来计算签名元素 (z，r，u)，以及

- 输出包含该签名元素 (z，r，u) 的该签名 σ。

2. 根据权利要求 1 的方法，其中该签字密钥进一步包括元素$h_z^{\alpha_r}$，该方法进一步包括：

- 选择随机元素$\theta, \rho \xleftarrow{R} Z_p$；

- 计算进一步的签名元素 v = h^{ρ}，其中 h 是第二组的元素；

其中 z 的计算进一步包括乘以g_r^{θ}，r 的计算进一步包括乘以$g_Z^{-\theta}$，并且 u 的计算进一步包括乘以$(h_z^{\alpha_r})^{-\theta}$，其中 α_r 为整数以及 h，g_r 和 g_z 为该第二组的元素；

其中该签名进一步包括签名元素 v；以及

其中该第一组和该第二组是相同的。

3. 一种验证包括在矢量$(M_1, \ldots, M_n) \in \hat{G}^n$上的签名元素 (z，r，u) 的线性同态签名 σ 的方法，其中$\hat{G}$表示第一组，该方法包括在设备 (200) 的处理器 (220) 中：

- 验证$(M_1, \ldots, M_n) \neq (1_{\hat{G}}, \ldots, 1_{\hat{G}})$以及 (z，r，u) 满足第一等式

$1_{G_T} = e(g_z, z) \cdot e(g_r, r) \cdot \prod_{i=1}^n e(g_i, M_i)$以及第二等式$1_{G_T} = e(h_z, z) \cdot e(h, u) \cdot \prod_{i=1}^n e(h_i, M_i)$，其中 e(•，•) 表示对称的和可交换的配对，并且其中 h，h_z，h_i，g_r，g_i 和 g_z 是第二组的元素；以及

- 在该验证成功时确定该签名已经被成功地验证，否则该签名未被成功地验证。

4. 根据权利要求 3 的方法，其中该第二等式进一步包括项 e(H_G(τ)，υ)，其中 H_G(τ) 表示哈希函数，并且 τ 表示该签名矢量存在的子空间的标识符。

5. 一种用于在矢量$(M_1, \ldots, M_n) \in \hat{G}^n$上生成线性同态签名 σ 的设备 (100)，其中$\hat{G}$表示第一组，该设备 (100) 包括处理器 (120)，其被配置来：

- 使用签名密钥$sk = \{\chi_i, \gamma_i, \delta_i\}_{i=1}^n$，通过计算

$z = \prod_{i=1}^n M_i^{-\chi_i}$，　　$r = \prod_{i=1}^n M_i^{-\gamma_i}$，　　$u = \prod_{i=1}^n M_i^{-\delta_i}$来计算签名元素 (z，r，u)，以及

- 输出包括该签名元素 (z，r，u) 的该签名 σ。

6. 根据权利要求 5 的设备，其中该签字密钥进一步包括元素$h_z^{\alpha_r}$，该处理器进一步被配置来：

- 选择随机元素$\theta, \rho \xleftarrow{R} Z_p$；以及

- 计算进一步的签名元素 v = h^{ρ}，其中 h 是第二组的元素；

其中 z 的计算进一步包括乘以g_r^{θ}，r 的计算进一步包括乘以$g_Z^{-\theta}$，并且 u 的计算进一步包括乘以$(h_z^{\alpha_r})^{-\theta}$，其中 α_r 为整数以及 h，g_r 和 g_z 为该第二组的元素；

其中该签名进一步包括签名元素 v；以及

其中该第一组和该第二组是相同的。

7. 一种用于验证包括在矢量$(M_1, \ldots, M_n) \in \hat{G}^n$上的签名元素 (z，r，u) 的线性同态签

名 σ 的设备 (200)，其中$\hat{G}$表示第一组，该设备 (200) 包括处理器 (220)，其被配置来：

- 验证$(M_1,\ldots,M_n)\neq(1_{\hat{G}},\ldots,1_{\hat{G}})$以及 (z，r，u) 满足第一等式

$1_{G_T}=e(g_z,z)\cdot e(g_r,r)\cdot\prod_{i=1}^{n}e(g_i,M_i)$以及第二等式$1_{G_T}=e(h_z,z)\cdot e(h,u)\cdot\prod_{i=1}^{n}e(h_i,M_i)$，其中 e(•，•) 表示对称的和可交换的配对，并且其中 h，h_z，h_i，g_r，g_i 和 g_z 是第二组的元素；以及

- 在该验证成功时确定该签名已经被成功地验证，否则该签名未被成功地验证。

8. 根据权利要求 7 的设备，其中该第二等式进一步包括项 $e(H_G(\tau),\upsilon)$，其中 $H_G(\tau)$ 表示哈希函数，并且 τ 表示该签名矢量存在的子空间的标识符。

9. 一种用于在矢量$(M_1,\ldots,M_n)\in\hat{G}^n$上生成线性同态签名 σ 的设备 (100)，其中$\hat{G}$表示第一组，该设备包括处理器 (120)，其被配置来：

- 使用签名密钥$sk=\{h_Z^{\alpha_r},\chi_i,\gamma_i,\delta_i\}_{i=1}^{n}$，其中 h_z 为第二组的成员以及 α_r 为整数，通过计算

$z=g_r^{\theta}\cdot\prod_{i=1}^{n}M_i^{-\chi_i}$，$r=g_z^{-\theta}\cdot\prod_{i=1}^{n}M_i^{-\gamma_i}$，$u=(h_z^{\alpha_r})^{-\theta}\cdot\prod_{i=1}^{n}M_i^{-\delta_i}$，$\upsilon=h^{\rho}$来计算签名元素 (z，r，u)，

其中 $H_G(\tau)$ 表示哈希函数，并且 τ 表示该签名矢量存在的子空间的标识符；

- 分别生成对 z，r 以及 u 的承诺；

- 使用对 z，r 以及 u 的承诺生成 z，r 以及 u 满足预定的验证算法的证明；以及

输出包括签名元素 v、对 z，r 以及 u 的承诺以及该证明的该签名 σ。

10. 一种用于在矢量$(M_1,\ldots,M_n)\in\hat{G}^n$上验证线性同态签名 σ 的设备 (200)，其中$\hat{G}$表示第一组，该线性同态签名 σ 包括第一签名元素 v、分别对进一步的签名元素 z，r 以及 u 的承诺$\vec{C}_z,\vec{C}_r,\vec{C}_u$以及 z，r 和 u 满足预定的验证算法的证明$\vec{\pi}_1,\vec{\pi}_2$，其中该承诺已经使用矢量$\vec{f}_1,\vec{f}_2,\vec{f}_3$被生成，该设备包括处理器 (220)，其被配置来：

- 验证$(M_1,\ldots,M_n)\neq(1_{\hat{G}},\ldots,1_{\hat{G}})$以及该验证

$\prod_{i=1}^{n}E(g_i,(1_G,1_G,M_i))^{-1}=E(g_Z,\vec{C}_z)\cdot E(g_r,\vec{C}_r)\cdot E(\pi_{1,1},\vec{f}_1)\cdot E(\pi_{1,2},\vec{f}_2)\cdot E(\pi_{1,3},\vec{f}_3)$

以及$\prod_{i=1}^{n}E(h_i,(1_G,1_G,M_i))^{-1}\cdot E(H_G(\tau),(1_G,1_G,v))^{-1}$

$=E(h_Z,\vec{C}_z)\cdot E(h,\vec{C}_u)\cdot E(\pi_{2,1},\vec{f}_1)\cdot E(\pi_{2,2},\vec{f}_2)\cdot E(\pi_{2,3},\vec{f}_3)$，

其中 E(•，•) 表示逐坐标配对，并且其中 h，h_z，h_i，g_r，g_i 和 g_z 是第二组的元素；以及

- 在该验证成功时确定该签名已经被成功地验证，否则该签名未被成功地验证。

产生和验证线性同态结构保留签名的加密设备和方法

技术领域

[0001] 本发明一般涉及加密，特别是线性同态结构保留签名。

背景技术

[0002] 本部分意在向读者介绍与以下被描述和/或请求保护的本发明的各个方面相关的技术的各个方面。相信本讨论有助于为读者提供背景信息以促进对本发明各个方面的更好的理解。相应地，应当理解的是这些叙述就此而论被阅读，并不作为对现有技术的承认。

[0003] 线性同态签名在加密技术中众所周知。在D.Boneh、D.Freeman、J.katz、B.Waters的《Signing a Linear Subspace:Signature Schemes for Network Coding》(PKC'09，Lecture Notes in Computer Science5443，第68-87页，2009年）中给出定义。

[0004] 线性同态签名的其他示例在下列文件中可以找到：

[0005] • US7743253，公开日为2010年6月22日；D.-X.Charles、K.Jain、K.Lauter的《Digital signature for network coding》。

[0006] • D.Boneh、D.Freeman、J.katz、B.Waters的《Signing a Linear Subspace：Signature Schemes for Network Coding》(PKC'09，Lecture Notes in Computer Science，vol.5443，第68-87页，2009年）。

[0007] •R.Gennaro、J.Katz、H.Krawczyk、T.Rabin的《Secure Network Coding over the Integers》(PKC'10，Lecture Notes in Computer Science，vol.6056，第142-160页，2010年）。

[0008] •N.Attrapadung、B.Libert的《Homomorphic Network Coding Signatures in the Standard Model》(PKC'11，Lecture Notes in Computer Science，vol.6571，第17-34页，2011年）。

[0009] • D.Boneh、D.Freeman的《Linearly Homomorphic Signatures over Binary Fields and New Toolsfor Lattice-based Signatures》(PKC'11，Lecture Notes in Computer Science，vol.6571，第1-16页，2011年）。

[0010] • D.Boneh、D.Freeman的《Homomorphic Signatures for Polynomial Function》(Eurocrypt'11，Lecture Notes in Computer Science，vol.6632，第149-168页，2011年）。

[0011] • D.Freeman的《Improved security for linearly homomorphic sigNature：A generic framework》(PKC'12，Lecture Notes in Computer Science，vol.7269，第697-714页，2012年）。

[0012] • D.Catalano、D.Fiore、B.Warinschi的《Adaptive Pseudo-free Groups and Applications》(Eurocrypt'11，Lecture Notes in Computer Science，vol.6632，第207-223页，2011年）。

[0013] •D.CaTalano、D.Fiore、B.Warinschi的《Efficient Network Coding Signatures in the Standard Model》(PKC'12，Lecture Notes InComputer Science，vol.7293，第680-696页，2012年）。

[0014] 看上去在标准假设下的标准模型中的被证明是安全的方案中，最有效的方案是在N.Attrapadung、B.Libert、T.Peters的《Computing on Authenticated Data：New Privacy Definitiohs and Constructiohs》(Asiacrypt'12，LNCS7658，第367-385页，2012年）中的一个。

[0015] 该结构在加法群 $(Z_p, +)$ 上是同态的。也就是，下面的循环群为 $G = Z_p$ 以及被签名的消息包括文件标识符 $\tau \in \{0,1\}^L$ 以及Z_p^n的矢量。该方案使用定义在素数阶 p 的群$(G,\hat{G},G_T)$之间的双线性映射$e:G\chi\hat{G}\to G_T$。

[0016] Keygen(λ，n)：给定安全参数 $\lambda \in N$ 以及表示要被签名的矢量的维度的整数 $n \in ploy(\lambda)$，选择素数阶 $p>2^\lambda$ 的双线性群$(G,\hat{G},G_T)$。为一些 $L \in ploy(\lambda)$，选择$\alpha \xleftarrow{R} Z_p, \hat{g} \xleftarrow{R} \hat{G}, v \xleftarrow{R} G$以及$u_0,u_1,...,u_L \xleftarrow{R} G$。这些元素 $(u_0, u_1, \ldots, u_L) \in G^{L+1}$ 将被用来实现数论哈希函数 $H_G:\{0,1\}^L \to G$ 以使任一 L 位字符串 $m = m[1]...m[L] \in \{0,1\}^L$ 具有哈希值$H_G(m)=u_0\cdot\prod_{i=1}^{L}u_i^{m[i]}$。对 $i = 1$ 到 n，选取$g_i \xleftarrow{R} G$。最后，定义标识符空间 $\Gamma := \{0,1\}^L$。私钥为 $sk := \alpha$ 以及公共密钥包含

[0017] $pk := ((G,G_T),\hat{g},\hat{g}^\alpha,v,\{g_i\}_{i=1}^n,\{u_i\}_{i=0}^L)$。

[0018] $\mathbf{Sign}(sk,\tau,\vec{v})$：给定矢量$\vec{v}=(v_1,...,v_n)\in Z_p^n$，文件标识符 $\tau := \{0,1\}^L$ 以及私钥$sk=\alpha\in Z_p^n$，选择$r,s\xleftarrow{R}Z_p$。然后，计算签名$\sigma=(\sigma_1,\sigma_2,s)\in G\times\hat{G}\times Z_p$作为

[0019] $$\sigma_1=(g_1^{v_1}\cdots g_n^{v_n}\cdot v^s)^\alpha\cdot H_G(\tau)^r,\qquad \sigma_2=\hat{g}^r。$$

[0020] $\mathbf{SignDerive}(pk,\tau,\{\beta_i,\sigma^{(i)}\}_{i=1}^{\ell})$：给定 pk，文件标识符 τ 以及 1 元组 $(\beta_i, \sigma^{(i)})$，对于 $i = 1$ 到 l 解析每一个 $\sigma^{(i)}$ 为 $\sigma^{(i)} = (\sigma_{i,1}, \sigma_{i,2}, s_i)$。选择$\tilde{r}\xleftarrow{R}Z_P$。然后计算并输出 (σ_1, σ_2, s)，其中

[0021] $$\sigma_1=\prod_{i=1}^{\ell}\sigma_{i,1}^{\beta_i}\cdot H_G(\tau)^{\tilde{r}}\qquad \sigma_2=\prod_{i=1}^{\ell}\sigma_{i,2}^{\beta_i}\cdot\hat{g}^{\tilde{r}}\qquad s=\sum_{i=1}^{\ell}\beta_i\cdot s_i$$

[0022] $\mathbf{Verify}(pk,\tau,\vec{y},\sigma)$：给定 pk，签名 $\sigma = (\sigma_1, \sigma_2, s)$ 以及消息$(\tau,\vec{y})$，这里 $\tau \in \{0,1\}^L$ 并且$\vec{y}=(y_1,...,y_n)\in(Z_p)^n$，如果$\vec{y}=\vec{0}$返回⊥。否则，当且仅当满足以下时返回 1：

[0023] $$e(\sigma_1,\hat{g})=e(g_1^{y_1}\cdots g_n^{y_n}\cdot v^s,\hat{g}^\alpha)\cdot e(H_G(\tau),\sigma_2)\quad 。$$

[0024] 应当理解的是，在该结构中，在全零矢量$\vec{0}$上的签名是不被允许的。这并不是限制，由于在线性同态签名的所有应用中，合适长度的单位矢量 $(0,\ldots,1,\ldots,0)$ 被附加到签名的矢量。

[0025] 在Attrapadung等人的论文中，上面的方案被证明在Diffie-Hellman假定的变体下是不可伪造的。这个假定假设，给定$(g,\hat{g},g^a,\hat{g}^b)\in(G\times\hat{G})^2$，对于随机选择的 $\alpha, b \in Z_p$ 并且其中$(G,\hat{G})$是阶 p 的循环双线性群，没有概率多项式时间 (PPT) 算法可以计算 g^{ab}。在上文的版本中，该方案不是完全的上下文隐藏的（即，得到的签名不是统计学上独立于原来的那个的）。Attrapadung等人已经示出如何修改该方案以使它是完全的上下文隐藏的，代价是增加签名的长度［参见N.Attrapadung、B.Libert、T.Peters的《Efficient Completely Context-Hiding Quotable Signatures and Linearly Homomorphic Signatures》，PKC′ 93，LNCS7778，第386-404页，2013年］。

[0026] 现有技术中的线性同态签名仅仅对于矢量空间存在，其中每一个矢量的坐标属于一个群，像 $(Z_p, +)$，其中计算离散对数是容易的。因此，应该理解的是，人们希望有一种能够处理其坐标存在于有限阶 p 的离散－对数－硬性群 (discrete-logarithm-hard group)G 的矢量$\vec{M}_1 \in G^n$的方案。一个最大的困难是，在那样的群中，通常难以判断多个矢量$\vec{M}_1,\ldots,\vec{M}_{n-1} \in G^n$是否是线性相关的。一般说来，对于 n>2，完成这个的唯一已知的方法是计算 Z_p 中所有坐标的离散对数。

[0027] 因此应当理解的是，人们希望有一种线性同态签名方案，其中消息可以是具有特殊的代数结构的元素，即“结构－保留”签名方案（“structure-preserving”signature scheme)，本发明就提供了这样的方案。

发明内容

[0028] 在第一方面，本发明针对一种在矢量$(M_1, \ldots, M_n) \in \hat{G}^n$上生成线性同态签名 σ 的方法，其中$\hat{G}$表示第一群。设备的处理器使用签名密钥$sk = \{\chi_i, \gamma_i, \delta_i\}_{i=1}^n$通过计算$z = \prod_{i=1}^n M_i^{-\chi_i}, r = \prod_{i=1}^n M_i^{-\gamma_i}, u = \prod_{i=1}^n M_i^{-\delta_i}$来计算并输出包括签名元素 (z，r，u) 的签名 σ。

[0029] 在优选的实施例中，该签名密钥进一步包括元素$h_z^{\alpha_r}$，该处理器进一步选择随机元素$\theta, \rho \xleftarrow{R} Z_p$；计算进一步的签名元素 v ＝ h^ρ，其中 h 是第二群的元素；其中 z 的计算进一步包括乘以g_r^θ，r 的计算进一步包括乘以$g_Z^{-\theta}$，并且 u 的计算进一步包括乘以$(h_z^{\alpha_r})^{-\theta}$，其中 α_r 为整数以及 h，g_r 和 g_z 为第二群的元素；其中该签名进一步包括签名元素 v；以及其中该第一群和该第二群是相同的。

[0030] 在第二方面，本发明针对一种验证包括在矢量$(M_1, \ldots, M_n) \in \hat{G}^n$上的签名元素 (z，r，u) 的线性同态签名 σ 的方法，其中$\hat{G}$表示第一群。设备的处理器验证$(M_1,\ldots,M_n) \neq (1_{\hat{G}},\ldots,1_{\hat{G}})$以及 (z，r，u) 满足第一等式$1_{G_T} = e(g_z, z) \cdot e(g_r, r) \cdot \prod_{i=1}^n e(g_i, M_i)$，以及第二等式$1_{G_T} = e(h_z, z) \cdot e(h, u) \cdot \prod_{i=1}^n e(h_i, M_i)$，其中 e(•，•) 表示对称的且可交换的配对，并且其中 h，h_z，h_i，g_r，g_i 和 g_z 是第二群的元素；以及在该验证成功时确定该签名已经被成功地验证，否则该签名未被成功地验证。

[0031] 在第一实施例中，该第二等式进一步包括项 $e(H_G(\tau), \upsilon)$，其中 $H_G(\tau)$ 表示哈希函数，并且 τ 表示该签名矢量存在的子空间的标识符。

[0032] 在第三方面，本发明针对一种用于在矢量$(M_1, \ldots, M_n) \in \hat{G}^n$上生成线性同态签名 σ 的设备，其中$\hat{G}$表示第一群。该设备包括处理器，其被配置为：使用签名密钥$sk = \{\chi_i, \gamma_i, \delta_i\}_{i=1}^n$通过计算$z = \prod_{i=1}^n M_i^{-\chi_i}$，$r = \prod_{i=1}^n M_i^{-\gamma_i}$，$u = \prod_{i=1}^n M_i^{-\delta_i}$来计算签名元素 (z，r，u)，并输出包括签名元素 (z，r，u) 的签名 σ。

[0033] 在第一实施例中，该签名密钥进一步包括元素$h_z^{\alpha_r}$，该处理器进一步被配置为：选择随机元素$\theta, \rho \xleftarrow{R} Z_p$；以及计算进一步的签名元素 v ＝ h^ρ，其中 h 是第二群的元素；其中 z 的计算进一步包括乘以g_r^θ，r 的计算进一步包括乘以$g_Z^{-\theta}$，并且 u 的计算进一步包括乘以$(h_z^{\alpha_r})^{-\theta}$，其中 α_r 为整数以及 h，g_r 和 g_zZ 第二群的元素；其中该签名进一步包括签名元素

v；以及其中该第一群和该第二群是相同的。

[0034] 在第四方面，本发明针对一种用于验证包括在矢量$(M_1, \ldots, M_n) \in \hat{G}^n$上的签名元素(z，r，u)的线性同态签名σ的设备(200)，其中$\hat{G}$表示第一群。该设备包括处理器，其被配置为：验证$(M_1,\ldots,M_n) \neq (1_{\hat{G}},\ldots,1_{\hat{G}})$以及(z，r，u)满足第一等式$1_{G_T} = e(g_z,z)\cdot e(g_r,r)\cdot \prod_{i=1}^{n} e(g_i,M_i)$以及第二等式$1_{G_T} = e(h_z,z)\cdot e(h,u)\cdot \prod_{i=1}^{n} e(h_i,M_i)$，其中e(•，•)表示对称的且可交换的配对，并且其中h，h_z，h_i，g_r，g_i和g_z是第二群的元素；以及在该验证成功时确定该签名已经被成功地验证，否则该签名未被成功地验证。

[0035] 在第一实施例中，该第二等式进一步包括项e(H_G(τ)，υ)，其中H_G(τ)表示哈希函数，并且τ表示该签名矢量存在的子空间的标识符。

[0036] 在第五方面，本发明针对一种用于在矢量$(M_1, \ldots, M_n) \in \hat{G}^n$上生成线性同态签名σ的设备，其中$\hat{G}$表示第一群。该设备包括处理器，其被配置为：使用签名密钥$\mathrm{sk} = \{h_Z^{\alpha_r}, \chi_i, \gamma_i, \delta_i\}_{i=1}^{n}$，其中$h_z$为第二群的元素以及$\alpha_r$为整数，通过计算$z = g_r^{\theta}\cdot \prod_{i=1}^{n} M_i^{-\chi_i}, r = g_z^{-\theta}\cdot \prod_{i=1}^{n} M_i^{-\gamma_i}, u = (h_z^{\alpha_r})^{-\theta}\cdot \prod_{i=1}^{n} M_i^{-\delta_i}, \upsilon = h^{\rho}$来计算签名元素(z，r，u，v)，其中$H_G$(τ)表示哈希函数，并且τ表示该签名矢量存在的子空间的标识符；分别生成z，r以及u的承诺；使用z，r以及u的承诺生成z，r以及u满足预定的验证算法的证明；以及输出包括签名元素v、对z，r和u的承诺以及证明的该签名σ。

[0037] 在第六方面，本发明针对一种用于在矢量$(M_1, \ldots, M_n) \in \hat{G}^n$上验证线性同态签名σ的设备，其中$\hat{G}$表示第一群，该线性同态签名σ包括第一签名元素v，进一步的签名元素z，r和u相应的承诺$\vec{C}_z, \vec{C}_r, \vec{C}_u$，以及z，r和u满足预定的验证算法的证明$\vec{\pi}_1, \vec{\pi}_2$，其中该承诺已经使用矢量$\vec{f}_1, \vec{f}_2, \vec{f}_3$生成。该设备包括处理器，被配置来：验证$(M_1,\ldots,M_n) \neq (1_{\hat{G}},\ldots,1_{\hat{G}})$以及验证$\prod_{i=1}^{n} E(g_i,(1_{G_T},1_G,M_i))^{-1} = E(g_z,\vec{C}_z)\cdot E(g_r,\vec{C}_r)\cdot E(\pi_{1,1},\vec{f}_1)\cdot E(\pi_{1,2},\vec{f}_2)\cdot E(\pi_{1,3},\vec{f}_3)$以及$\prod_{i=1}^{n} E(h_i,(1_G,1_G,M_i))^{-1}\cdot E(H_G(\tau),(1_G,1_G,v))^{-1} = E(h_z,\vec{C}_z)\cdot E(h,\vec{C}_u)\cdot E(\pi_{2,1},\vec{f}_1)\cdot E(\pi_{2,2},\vec{f}_2)\cdot E(\pi_{2,3},\vec{f}_3)$，其中E(•，•)表示逐坐标配对(coordinate-wise pairing)，并且其中h，h_z，h_i，g_r，g_i和g_z是第二群的元素；以及在该验证成功时确定该签名已经被成功地验证，否则该签名未被成功地验证。

附图说明

[0038] 本发明优选的特性即将通过非限制性的示例参考附图被描述，其中：

[0039] 图1示出了根据本发明的优选实施例的一种结构保留的线性同态签名系统；以及

[0040] 图2示出了根据本发明的优选实施例的一种用于生成和验证上下文隐藏的线性同态结构保留签名的方法。

具体实施方式

[0041] 本发明的结构保留线性同态签名方案是基于M.Abe、K.Haralambiev、M.Ohkubo的《Signing on Elements in Bilinear Groups for Modular Protocol Design》(Cryptology ePrint Archive：Report2010/133，2010年)以及M.Abe、G. Fuchsbauer、J.Groth、

K.Haralambiev、M.Ohkubo 的《Structure-Preserving Signatures and Commitments to Group)》(Crypto'10,Lecture Notes in Computer Science,vol.6223,第209-236页,2010年)[参见第一个论文的附录C的描述]中提出的结构保留签名方案的变型。应当理解的是,该方案既不是也不意图是同态的,并且只允许关于给定的公钥签名一个消息。

[0042] 因此,第一个变型被做出以获得在离散-对数-硬性群上的线性同态签名方案,只要仅仅一个线性子空间(由$\hat{G}^n$的n-1个线性无关矢量张成)使用给定的密钥对(sk;pk)签名。这个第一方案如下被描述。在下面的符号中,pp表示包含素数阶$p>2^{\lambda}$的群$(G,\hat{G},G_T)$的公共参数集合,其中$\lambda \in N$为安全参数,在其上定义可以高效计算的双线性映射$e:G\times\hat{G}\to G_T$。

[0043] 图1示出了根据本发明优选的实施例的一种用于生成同态签名的加密签名设备100以及一种用于验证同态签名的加密签名设备200。该设备100、200的每一个包括被配置用来通讯的至少一个接口单元110、210,至少一个处理器("处理器")120、220以及被配置用来存储数据,诸如累加器和中间计算结果的至少一个存储器130、230。该图也示出了第一和第二计算机程序产品(非临时性存储介质)140、240,如包含存储的指令的CD-ROM或DVD,当通过处理器120,220执行时分别生成以及验证根据本发明的签名。

[0044] 一次性方案(One-time scheme)

[0045] Keygen(pp,n):给定pp以及要被签名的子空间的维度$n\in N$,选择生成器$h,g_z,g_r,z_z \xleftarrow{R} G$,对i=1到n,挑选$\chi_i,\gamma_i,\delta_i \xleftarrow{R} Z_p$。然后,对于每个$i\in\{1,\ldots,n\}$,计算$g_i=g_z^{\chi_i}g_r^{\gamma_i}, h_i=h_z^{\chi_i}h_r^{\delta_i}$。该公共密钥被定义为

[0046] $\mathrm{pk}=(g_z,g_r,h_z,h,\{g_i,h_i\}_{i=1}^n)\in G^{2n+4}$

[0047] 以及该私钥为$\mathrm{sk}=\{\chi_i,\gamma_i,\delta_i\}_{i=1}^n$。

[0048] Sign(sk,τ,(M_1,...,M_n)):使用$\mathrm{sk}=\{\chi_i,\gamma_i,\delta_i\}_{i=1}^n$对与标识符τ=ε相关联的矢量$(M_1,\ldots,M_n)\in\hat{G}^n$签名,计算

[0049]
$$z=\prod_{i=1}^n M_i^{-\chi_i}, r=\prod_{i=1}^n M_i^{-\gamma_i}, u=\prod_{i=1}^n M_i^{-\delta_i},$$
该签名包括$\sigma=(z,r,u)\in\hat{G}^3$。

[0050] $\mathbf{SignDerive}(\mathrm{pk},\tau,\{(\omega_i,\sigma^{(i)})\}_{i=1}^{\ell})$:给定pk,文件标识符τ以及l元组($\omega_i$,$\sigma^{(i)}$),对于i=1到l解析每一个签名$\sigma^{(i)}$为$\sigma^{(i)}=(z_i,r_i,u_i)\in\hat{G}^3$。计算

[0051] $$z=\prod_{i=1}^{\ell}Z_i^{\omega_i} \qquad r=\prod_{i=1}^{\ell}r_i^{\omega_i} \qquad u=\prod_{i=1}^{\ell}u_i^{\omega_i}$$

[0052] 并且返回σ=(z,r,u)。

[0053] Verify(pk,σ,τ,(M_1,...,M_n)):给定签名$\sigma=(z,r,u)\in\hat{G}^3$,矢量($M_1$,...,$M_n$)以及文件标识符τ=ε,当且仅当$(M_1,\ldots,M_n)\neq(1_{\hat{G}},\ldots,1_{\hat{G}})$以及(z,r,u)满足以下等式时返回1:,

[0054] $1_{G_T}=e(g_z,z)\cdot e(g_r,r)\cdot\prod_{i=1}^n e(g_i,M_i)$, $1_{G_T}=e(h_z,z)\cdot e(h,u)\cdot\prod_{i=1}^n e(h_i,M_i)$。

[0055] 可以证明的是,只要同时双配对(Simultaneous Double Pairing,SDP)假设

成立，在至多 n-1 个线性无关矢量$\vec{M}_1,\ldots,\vec{M}_{n-1}$上获取签名的攻击者就不能伪造在矢量$\vec{M}\notin \mathrm{span}(\vec{M}_1,\ldots,\vec{M}_{n-1})$上的签名。被描述在 Abe、Haralambiev 和 Ohkubo 的论文中的 SDP 假设是在$(G,\hat{G})$中给定元素 (g_z, g_r, h_z, h_u) ∈ G^4 的元组，找出非平凡元组 (non-trivial tuple) $(z,r,u)\in\hat{G}^3\setminus\{(1_{\hat{G}},1_{\hat{G}},1_{\hat{G}})\}$使得$e(g_z\cdot z)\cdot e(g_r\cdot r)=1_{G_T}$并且$e(h_z\cdot z)\cdot e(h_u\cdot u)=1_{G_T}$。

[0056] 完善方案 (Full-fledged scheme)

[0057] 一次性方案可升级为允许签名任意数量的线性子空间的线性结构。要做到这一点，对于双线性群$(G,\hat{G})$的结构，$G=\hat{G}$是必要的。换句话说，双线性映射 e :G×G → G_T 必须在相同的群 G 中具有其论证，因为它应该是对称的和可交换的。

[0058] 在该结构中，对于一些 L ∈ ploy(λ)，每一个文件标识符 τ 包括 L 位字符串。每一个签名的 u 分量可被看作具有文件标识符 τ 上的 Waters 签名$(h_z^{\alpha_r}\cdot H_G(\tau)^{-\rho}, h^{\rho})$的一次性方案的签名的聚合 (aggregation)[参见 B. Waters 的《Efficient Identity-Based Encryption Without Random Oracles》(Eurocrypt' 05, Lecture Notes in Computer Science, vol. 3494，第 114-127 页，2005 年)]。在本方案里，这样的 Waters 签名被用作签名随机器 θ ∈ Z_p 的支持。

[0059] Keygen(pp, n) :给定 pp 以及要被签名的子空间的维度 n ∈ N，执行如下步骤 :

[0060] 1. 选择$h\xleftarrow{R}G$以及$\alpha_z,\alpha_r,\beta_z\xleftarrow{R}Z_p$。定义$g_z=h^{\alpha_z}, g_r=h^{\alpha_r}$以及$h_z=h^{\beta_z}$。

[0061] 2. 对于每一个 i = 1 到 n，挑选$\chi_i,\gamma_i,\delta_i\xleftarrow{R}Z_p$并计算$g_i=g_z^{\chi_i}g_r^{\gamma_i}, h_i=h_z^{\chi_i}h_r^{\delta_i}$。

[0062] 3. 选择随机矢量$\vec{w}=(w_0,w_1,\ldots,w_L)\xleftarrow{R}G^{L+1}$，其定义了映射 τ = τ[1]... τ[L] ∈ $\{0,1\}^L$ 到$H_G(\tau)=w_0\cdot\prod_{K=1}^{L}w_k^{\tau[k]}$的哈希函数 $H_G:\{0,1\}^L\to G$。

[0063] 该公共密钥包含

[0064] $\mathrm{pk}=(g_Z,g_r,h_Z,h,\{g_i,h_i\}_{i=1}^n,\vec{w})\in G^{2n+4}\times G^{L+1}$

[0065] 同时该私钥为$\mathrm{sk}=(h_z^{\alpha_r},\{\chi_i,\gamma_i,\delta_i\}_{i=1}^n)$。

[0066] Sign(sk, τ, (M_1,...,M_n)) :为了使用$\mathrm{sk}=(h_z^{\alpha_r},\{\chi_i,\gamma_i,\delta_i\}_{i=1}^n)$关于文件标识符 τ 签名矢量 ($M_1$,...,$M_n$) ∈ G^n，选择$\theta,\rho\xleftarrow{R}Z_P$，并计算

[0067] $$z=g_r^{\theta}\cdot\prod_{i=1}^{n}M_i^{-\chi_i},\qquad r=g_Z^{-\theta}\cdot\prod_{i=1}^{n}M_i^{-\gamma_i},\qquad u=(h_Z^{\alpha_r})^{-\theta}\cdot\prod_{i=1}^{n}M_i^{-\delta_i}\cdot H_G(\tau)^{-\rho},\quad v=h^{\rho}$$

[0068] 该签名包括 σ = (z, r, u, v) ∈ G^4。

[0069] $\mathbf{SignDerive}(\mathrm{pk},\tau,\{\omega_i,\sigma^{(i)}\}_{i=1}^{\ell})$:给定 pk，文件标识符 τ 以及 l 元组 ($\omega_i$, $\sigma^{(i)}$)，对于 i = 1 到 l 解析每一个签名 $\sigma^{(i)}$ 为 $\sigma^{(i)}=(z_i,r_i,u_i,v_i)\in G^4$。然后选择$\rho'\xleftarrow{R}Z_P$，并计算

[0070] $$z=\prod_{i=1}^{\ell}Z_i^{\omega_i}\qquad r=\prod_{i=1}^{\ell}r_i^{\omega_i}\qquad u=\prod_{i=1}^{\ell}u_i^{\omega_i}\cdot H_G(\tau)^{-\rho'}\qquad v=\prod_{i=1}^{\ell}v_i^{\omega_i}\cdot h^{\rho'}$$

[0071] 并返回 σ = (z, r, u, v)。

[0072] Verify(pk, σ, τ, (M_1,...,M_n)) :给定签名 σ = (z, r, u, v) ∈ G^4，文件标识符 τ 以及矢量 (M_1,...,M_n)，当且仅当 (M_1,...,M_n) ≠ (1_G,...,1_G) 并且 (z, r, u, v) 满足下列等式时返回 1 :

[0073] $1_{G_T} = e(g_z, z) \cdot e(g_r, r) \cdot \prod_{i=1}^{n} e(g_i, M_i)$

$1_{G_T} = e(h_z, z) \cdot e(h, u) \cdot e(H_G(\tau), v) \cdot \prod_{i=1}^{n} e(h_i, M_i)$ 。

[0074] 应当理解的是，一次性方案是完善方案中每个签名中 θ = ρ = 0 的特殊情形。上下文隐藏方案 (Context-hiding scheme)

[0075] 应该理解的是，完善方案不提供完全的上下文隐藏的安全性，因为签名推导操作在不知道私钥的情况下不能重新随机化潜在的 θ (underlying θ)。在一些应用中，可能希望确保推导得到的签名和原始的签名是不可链接的 (unlinkable)，即使在计算上无界限的观察者的视野中。

[0076] 出于这个原因，优选的实施例是能够被证明是完全上下文隐藏的方案。该方案通过修改该完善方案获得。从本质上讲，签名者和完善方案中一样首先计算签名 σ = (z, r, u, v)。由于元素 (z, r, u) 不能被公开的重新随机化，签名者只能让它们在格罗斯 - 萨海承诺 (Groth-Sahai commitments) 内出现参见 J. Groth、A. Sahai 的《Efficient non-interactive proof systems for bilinear groups》(Eurocrypt ′ 08, Lecture Notes in Computer Science, vol. 4965, 第 415-432 页, 2008 年)] 并且增加承诺值满足该验证等式的非交互式证明。格罗斯 - 萨海证明的完美的可随机化属性 (在 M. Belenkiy、J. Camenisch、M. Chase、M. Kohlweiss、A. Lysyanskaya、H. Shacham 的《Randomizable Proofsand Delegatable Anonymous Credentials》(Crypto'09, Lecture Notes in Computer Science, vol. 5677, 第 108-125 页, 2009 年) 中证明) 保证了推导得到的签名将作为新生成的签名分发。

[0077] 在下面的描述中，也要求双线性映射 e : G×G → G_T 是对称的 (即 $G = \hat{G}$)。在下面的符号中，逐坐标配对 $E: G \times \hat{G}^3 \to G_T^3$ 被定义使得对于任一元素 h ∈ G 以及任一矢量 $\vec{g} = (g_1, g_2, g_3), E(h, \vec{g}) = (e(h, g_1), e(h, g_2), e(h, g_3))$。

[0078] 图 2 示出了下面方案的签名、签名推导以及验证。

[0079] Keygen(pp, n) : 给定 pp 以及要被签名的子空间的维度 n ∈ N, 执行如下步骤 :

[0080] 1. 选择 $h \xleftarrow{R} G$ 以及 $\alpha_z, \alpha_r, \beta_z \xleftarrow{R} Z_p$。定义 $g_z = h^{\alpha_z}, g_r = h^{\alpha_r}$ 以及 $h_z = h^{\beta_z}$。

[0081] 2. 对于每一个 I ∈ {1, ..., n}, 挑选 $\chi_i, \gamma_i, \delta_i \xleftarrow{R} Z_p$ 并计算 $g_i = g_z^{\chi_i} g_r^{\gamma_i}, h_i = h_z^{\chi_i} h^{\delta_i}$。

[0082] 3. 通过选择 $f1, f2 \xleftarrow{R} G$ 以及定义矢量 $\vec{f_1} = (f_1, 1, g) \in G^3, \vec{f_2} = (1, f_2, g) \in G^3$ 以及 $\vec{f_3} \xleftarrow{R} G^3$ 来选择格罗斯 - 萨海公共参考字符串。

[0083] 该公共密钥包含

[0084] $\mathrm{pk} = (g_z, g_r, h_z, h, \{g_i, h_i\}_{i=1}^n, f = (\vec{f_1}, \vec{f_2}, \vec{f_3})$

[0085] 同时私钥为 $\mathrm{sk} = (h_z^{\alpha_r}, (\chi_i, \gamma_i, \delta_i)_{i=1}^n)$。

[0086] Sign(sk, τ, (M_1, ..., M_n)) : 为了使用 $\mathrm{sk} = (h_z^{\alpha_r}, (\chi_i, \gamma_i, \delta_i)_{i=1}^n)$ 关于文件标识符 τ 签名矢量 (M_1, ..., M_n) ∈ G^n, 执行 :

[0087] 1. 选择 S1 $\theta, \rho \xleftarrow{R} Z_p$ 并计算

[0088] $$z = g_r^{\theta} \cdot \prod_{i=1}^{n} M_i^{-\chi_i}, \qquad r = g_Z^{-\theta} \cdot \prod_{i=1}^{n} M_i^{-\gamma_i},$$
$$u = (h_Z^{\alpha_r})^{-\theta} \cdot \prod_{i=1}^{n} M_i^{-\delta_i} \cdot H_G(\tau)^{-\rho}, \quad v = h^{\rho}$$

[0089] 2. 使用矢量$f = (\vec{f}_1, \vec{f}_2, \vec{f}_3)$,分别计算 S2 对 z,r 和 u 的承诺。

$$\vec{C}_z = (1_G, 1_G, z) \cdot \vec{f}_1^{\,v_{z,1}} \cdot \vec{f}_2^{\,v_{z,2}} \cdot \vec{f}_3^{\,v_{z,3}}$$

[0090] $$\vec{C}_r = (1_G, 1_G, r) \cdot \vec{f}_1^{\,v_{r,1}} \cdot \vec{f}_2^{\,v_{r,2}} \cdot \vec{f}_3^{\,v_{r,3}}$$
$$\vec{C}_u = (1_G, 1_G, u) \cdot \vec{f}_1^{\,v_{u,1}} \cdot \vec{f}_2^{\,v_{u,2}} \cdot \vec{f}_3^{\,v_{u,3}}$$

[0091] 使用这些承诺的随机性,生成 (z,r,u) 满足完善方案的验证等式的证明

[0092]
$$\vec{\pi}_1 = (\pi_{1,1}, \pi_{1,2}, \pi_{1,3}) \in G^3 \text{ 以及 } \vec{\pi}_2 = (\pi_{2,1}, \pi_{2,2}, \pi_{2,3}) \in G^3, \text{ 即:}$$
$$1_{G_T} = e(g_z, z) \cdot e(g_9, r) \cdot \prod_{i=1}^{n} e(g_i, M_i)$$

[0093] $1_{G_T} = e(h_z, z) \cdot e(h, u) \cdot e(H_G(\tau), v) \cdot \prod_{i=1}^{n} e(h_i, M_i)$。

[0094] 这些证明作为以下获得:

[0095] $$\vec{\pi}_1 = (\pi_{1,1}, \pi_{1,2}, \pi_{1,3}) = (g_z^{-v_{z,1}} \cdot g_r^{-v_{r,1}}, g_z^{-v_{z,2}} \cdot g_r^{-v_{r,2}}, g_z^{-v_{z,3}} \cdot g_r^{-v_{r,3}})$$

[0096] $$\vec{\pi}_2 = (\pi_{2,1}, \pi_{2,2}, \pi_{2,3}) = (h_z^{-v_{z,1}} \cdot h_r^{-v_{u,1}}, h_z^{-v_{z,2}} \cdot h_r^{-v_{u,2}}, h_z^{-v_{z,3}} \cdot h_r^{-v_{u,3}})$$

[0097] 以及满足验证等式

[0098]
$$\prod_{i=1}^{n} E(g_i, (1_G, 1_G, M_i))^{-1} = E(g_Z, \vec{C}_z) \cdot E(g_r, \vec{C}_r) \cdot E(\pi_{1,1}, \vec{f}_1) \cdot E(\pi_{1,2}, \vec{f}_2) \cdot E(\pi_{1,3}, \vec{f}_3)$$
$$\prod_{i=1}^{n} E(h_i, (1_G, 1_G, M_i))^{-1} \cdot E(H_G(\tau), (1_G, 1_G, v))^{-1} = E(h_z, \vec{C}_z) \cdot E(h, \vec{C}_u) \cdot E(\pi_{2,1}, \vec{f}_1) \cdot E(\pi_{2,2}, \vec{f}_2) \cdot E(\pi_{2,3}, \vec{f}_3)$$

[0099] 该签名包括$\sigma = (\vec{C}_z, \vec{C}_r, \vec{C}_u, v, \vec{\pi}_1, \vec{\pi}_2) \in G^{16}$。

[0100] **SignDerive**$(\mathrm{pk}, \tau, \{\omega_i, \sigma^{(i)}\}_{i=1}^{\ell})$:给定 pk,文件标识符 τ 以及 l 元组 $(\omega_i, \sigma^{(i)})$,对于 i = 1 到 l 解析每一个签名 $\sigma^{(i)}$ 为形式$\sigma_i = (\vec{C}_{z,i}, \vec{C}_{r,i}, \vec{C}_{u,i}, v_i, \vec{\pi}_{1,i}, \vec{\pi}_{2,i}) \in G^{16}$的元组。选择$\rho' \xleftarrow{R} Z_P$并计算

[0101]
$$\vec{C}_z = \prod_{i=1}^{\ell} \vec{C}_{z,i}^{\,\omega_i} \qquad \vec{C}_r = \prod_{i=1}^{\ell} \vec{C}_{r,i}^{\,\omega_i} \qquad \vec{C}_u = \prod_{i=1}^{\ell} \vec{C}_{u,i}^{\,\omega_i} \cdot H_G(\tau)^{-\rho'}$$
$$v = \prod_{i=1}^{\ell} v_i^{\omega_i} \cdot h^{\rho'} \qquad \vec{\pi}_1 = \prod_{i=1}^{\ell} \vec{\pi}_{1,i}^{\,\omega_i} \qquad \vec{\pi}_2 = \prod_{i=1}^{\ell} \vec{\pi}_{2,i}^{\,\omega_i}$$

[0102] 然后重新随机化 S3 承诺和证明并返回$\sigma = (\vec{C}_z, \vec{C}_r, \vec{C}_u, v, \vec{\pi}_1, \vec{\pi}_2)$。

[0103] Verify(pk, σ, τ, $(M_1, \ldots, M_n)$):给定对 (τ, $(M_1, \ldots, M_n)$) 以及声称的签名 σ,解析签名为$(\vec{C}_z, \vec{C}_r, \vec{C}_u, v, \vec{\pi}_1, \vec{\pi}_2)$。然后,当且仅当$(M_1, \ldots, M_n) \neq (1_G, \ldots, 1_G)$且 Sign 验证满足 S4 时,即

[0104]

$$\prod_{i=1}^{n} E(g_i,(1_G,1_G,M_i))^{-1} = E(g_z,\vec{C}_z)\cdot E(g_r,\vec{C}_r)\cdot E(\pi_{1,1},\vec{f}_1)\cdot E(\pi_{1,2},\vec{f}_2)\cdot E(\pi_{1,3},\vec{f}_3)$$

$$\prod_{i=1}^{n} E(h_i,(1_G,1_G,M_i))^{-1}\cdot E(H_G(\tau),(1_G,1_G,v))^{-1} = E(h_Z,\vec{C}_z)\cdot E(h,\vec{C}_u)\cdot E(\pi_{2,1},\vec{f}_1)\cdot E(\pi_{2,2},\vec{f}_2)\cdot E(\pi_{2,3},\vec{f}_3)$$

[0105] 时 S5 返回 1。

[0106] 该方案的不可伪造性可以在判定线性假设 (Decision Linear assumption) 情况下被证明，判定线性假设非正式地说判定维度为 3 的群元素的三个向量是否是线性相关是不可行的。此外，该方案是无条件的上下文隐藏的。

[0107] 本发明的优势在于，它能够允许签名者在不知道它们的离散对数的情况下签名包括群元素的向量。例如，该签名方案使得签名者不必知道下面的纯文本为密文签名成为可能。

[0108] 可以理解的是，本发明的方案可以用于在云计算服务中外包加密的数据集。此外，线性同态签名也可以作为匿名推荐系统中的正确聚合的证明。

[0109] 说明书和（适当的）权利要求和附图所公开的每个特征可以独立地或以任何适当的组合被提供。被描述为以硬件实现的特征也可以被实现为软件，反之亦然。权利要求中出现的附图标记仅仅用作举例说明，并不对权利要求的范围起到任何限制作用。

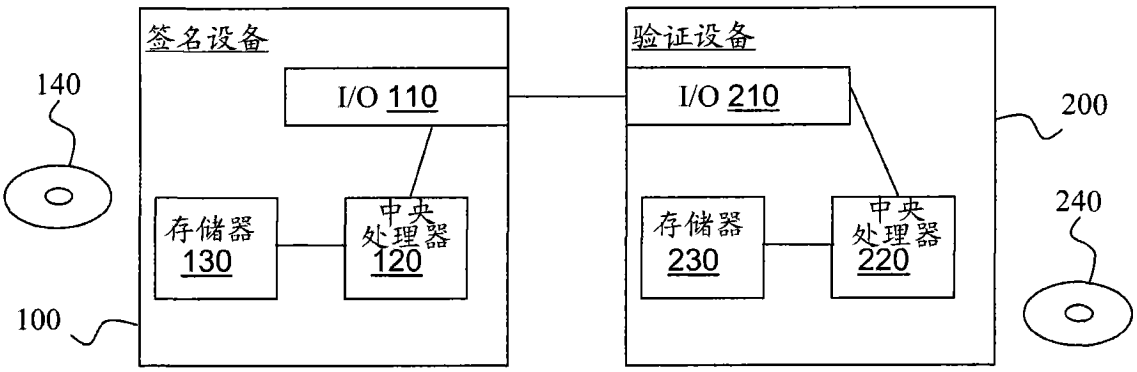

签名设备
I/O 110
存储器 130
中央处理器 120
140
100
验证设备
I/O 210
存储器 230
中央处理器 220
200
240

图 1

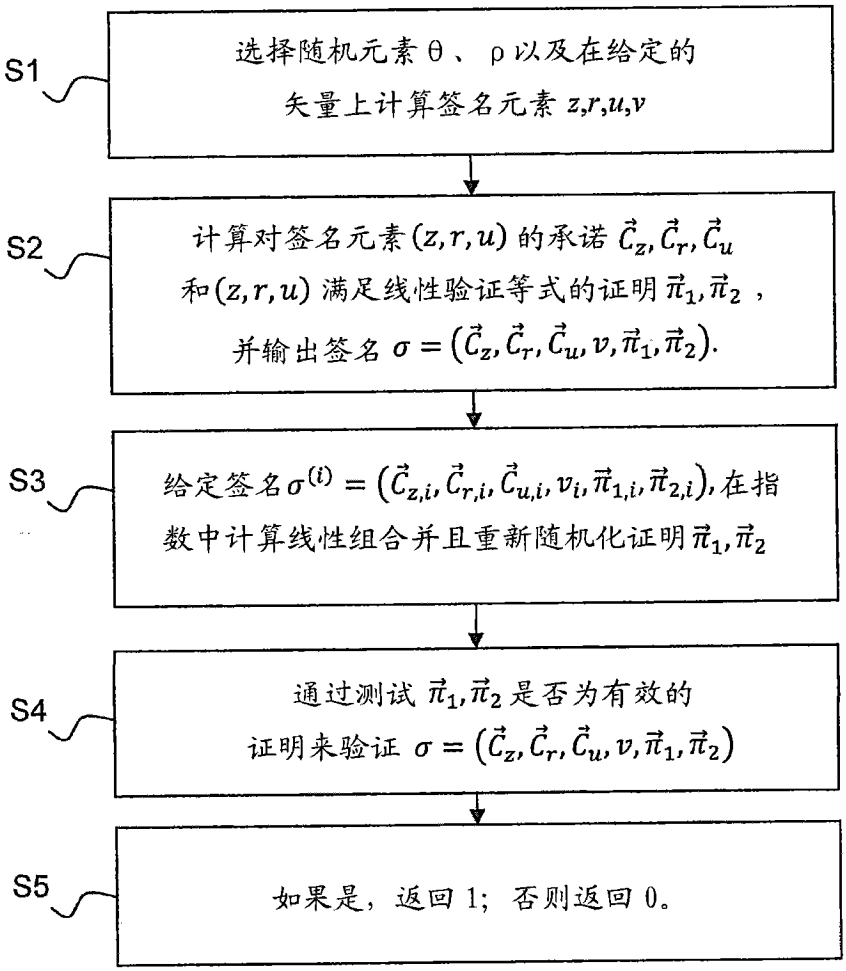

S1
选择随机元素 θ 、 ρ 以及在给定的矢量上计算签名元素 z,r,u,v
S2
计算对签名元素 (z,r,u) 的承诺 $\vec{C}_z,\vec{C}_r,\vec{C}_u$ 和 (z,r,u) 满足线性验证等式的证明 $\vec{\pi}_1,\vec{\pi}_2$ ，并输出签名 $\sigma=(\vec{C}_z,\vec{C}_r,\vec{C}_u,v,\vec{\pi}_1,\vec{\pi}_2)$.
S3
给定签名 $\sigma^{(i)}=(\vec{C}_{z,i},\vec{C}_{r,i},\vec{C}_{u,i},v_i,\vec{\pi}_{1,i},\vec{\pi}_{2,i})$，在指数中计算线性组合并且重新随机化证明 $\vec{\pi}_1,\vec{\pi}_2$
S4
通过测试 $\vec{\pi}_1,\vec{\pi}_2$ 是否为有效的证明来验证 $\sigma=(\vec{C}_z,\vec{C}_r,\vec{C}_u,v,\vec{\pi}_1,\vec{\pi}_2)$
S5
如果是，返回 1；否则返回 0。

图 2