











**定义 9(基于身份的哈希证明系统)**<sup>[10]</sup>. 一个哈希证明系统由以下 5 个算法(Setup,KeyGen,Encap,Encap\*,Decap)组成.

**Setup**( $1^n$ ):给定安全参数  $n$ ,输出一对主公钥  $mpk$  和主私钥  $msk$ ,并且生成参数  $(K,C,V,V',ID,SK,H_{(\cdot)},\mu)$ ,同样要求哈希函数  $H_{(\cdot)}$  是可以有效计算的.

**KeyGen**( $mpk,msk,id$ ):对于任意身份  $id \in ID$ ,利用  $mpk$  和  $msk$  提取一个身份私钥  $sk_{id}$ .

**Encap**( $mpk,id$ ):对于任意身份  $id \in ID$ ,该合法封装算法首先随机选取一个合法密文  $c \leftarrow V$  及其相关证据  $w$ ,然后计算相应封装密钥  $k = H(mpki, c, w)$ ,最后输出  $(c,k)$ .

**Encap\***( $mpk,id$ ):对于任意身份  $id \in ID$ ,该非法封装算法随机选取一个非法密文  $c \leftarrow V'$ ,最后输出  $c$ .

**Decap**( $mpk,sk_{id},c$ ):给定身份私钥  $sk_{id}$  和密文  $c$ ,该解封算法输出  $k = H_{sk_{id}}(c)$ .

与哈希证明系统不同,基于身份的哈希证明系统的合法密文与非法密文的不可区分需要通过一个攻击者和挑战者之间的交互式游戏进行定义和论证,并且该游戏的交互过程要求攻击者可以得到包括挑战身份在内的所有身份的私钥.该交互式游戏可以具体描述如下.

**Setup**:挑战者可以运行系统生成算法 **Setup**( $1^n$ )得到一个主公私钥对( $mpk,msk$ ),并且将主公钥  $mpk$  发送给攻击者.

**KeyGen1**:攻击者可以适应性地选择身份  $id \in ID$  向挑战者进行询问,挑战者返回该身份对应的身份私钥  $sk_{id}$ .

**Challenge**:攻击者选取任意身份  $id^* \in ID$  作为挑战身份进行询问.此时挑战者随机选取一个比特  $b \leftarrow \{0,1\}$ .如果  $b=0$ ,则挑战者向攻击者返回  $Encap(mpki, id^*)$ ,否则返回  $Encap^*(mpki, id^*)$ .

**KeyGen2**:与第 1 个阶段的身份私钥询问相同,攻击者可以适应性地选择身份  $id \in ID$  向挑战者进行询问,挑战者返回该身份对应的身份私钥  $sk_{id}$ .

**Output**:攻击者输出一个比特  $b' \leftarrow \{0,1\}$  作为整个游戏的输出.

如果  $b=b'$ ,则认为攻击者赢得了游戏.注意到,在以上游戏中,挑战者对于相同的身份  $id \in ID$  的私钥询问只能返回相同的身份私钥.同时,挑战身份  $id^* \in ID$  有可能在两个阶段的身份私钥询问阶段中被询问过.如果攻击者在以上游戏中成功的优势是可以忽略的,则意味着基于身份的哈希证明系统的合法密文和非法密文是不可区分的.

## 2 基于 LWE 假设的哈希证明系统

### 2.1 基于LWE假设的哈希证明系统的构造

基于 LWE 的哈希证明系统  $HPS=(Param, Pub, Priv)$ 可以按如下方式进行具体描述.

**Param**( $1^n$ ):给定安全参数  $n$ ,输出参数  $(group, K, C, V, V', PK, SK, H_{(\cdot)}, \mu)$ , 其中,

- $group = (\mathbb{Z}, q, m, \mathbf{A}, \beta, r)$ ,  $q$  是一个素数,  $m = 2n \log q$  是所用到的格的维数,随机均匀选取矩阵  $\mathbf{A} \leftarrow \mathbb{Z}_q^{m \times n}$ ,  $\beta \in (0, 1)$  和  $r = \sqrt{q\omega(\sqrt{\log m})}$  是两个实数,满足  $\beta q \geq 2\sqrt{n}$  和  $\beta \leq \sqrt{2\pi}/(r\sqrt{m} \cdot \omega(\sqrt{\log n}))$ .

- $V = \{\mathbf{As} + \mathbf{e} \bmod q : \mathbf{s} \leftarrow \mathbb{Z}_q^n, \mathbf{e} \leftarrow \bar{\nu}_\beta^m\}$ ,  $V' = \{\mathbf{As} + \mathbf{e} \bmod q : \mathbf{s} \leftarrow \mathbb{Z}_q^n, \|\mathbf{e}\| \geq \sqrt{q}/4\}$ ,  $K = \{0, 1\}$ .

- $SK$  是  $\mathbb{Z}^m$  上的离散高斯分布  $D_{\mathbb{Z}^m, r}$ ,  $PK = \mathbb{Z}_q^n$ .

- 对于任意私钥  $sk := \mathbf{v} \leftarrow D_{\mathbb{Z}^m, r}$ , 其对应的公钥为  $pk := \mathbf{y} = \mu(sk) = \mathbf{A}^T \mathbf{v} \bmod q$ .

**Pub**( $pk, c, w$ ):给定一个合法密文  $c := \mathbf{x} = \mathbf{As} + \mathbf{e} \bmod q \in V$ , 其对应的证据是  $\mathbf{s} \in \mathbb{Z}_q^n$ , 差错向量是  $\mathbf{e} \leftarrow \bar{\nu}_\beta^m$ . 计算  $z = \langle \mathbf{y}, \mathbf{s} \rangle \bmod q$ , 如果  $z$  与 0 之间的距离小于  $z$  与  $\lfloor q/2 \rfloor$  之间的距离, 输出  $k=0$ ; 反之, 输出  $k=1$ .

**Priv**( $sk, c$ ):给定密文  $c := \mathbf{x}$  和私钥  $sk := \mathbf{v}$ , 计算  $z = \langle \mathbf{v}, \mathbf{x} \rangle \bmod q$ , 如果  $z$  与 0 之间的距离小于  $z$  与  $\lfloor q/2 \rfloor$  之间的距离, 输出  $k=0$ ; 反之, 输出  $k=1$ .

由引理 4 可知, 在  $r = \sqrt{q\omega(\sqrt{\log m})} > \omega(\sqrt{\log m})$  的情况下, 离散高斯分布  $D_{\mathbb{Z}^m, r}$  是在多项式时间内有效抽

样的.上述哈希证明系统中的所有其他分布也都可以进行有效抽样.因此,该哈希证明系统中的所有计算都是可以有效进行的.

与文献[6,7,10]中的基于格的哈希证明系统相类似,本节所提构造中的模数是安全参数的亚指数,并且  $K = \{0,1\}$ .事实上,在从离散高斯分布  $D_{\mathbb{Z}_q^m, r}$  中独立选取多个私钥  $(\mathbf{v}_1, \dots, \mathbf{v}_l)$  的情况下,可以将封装密钥集合扩展为  $K = \{0,1\}^l$ .

## 2.2 哈希证明系统的证明

**定理 1.** 给定安全参数  $n$ , 令  $q = 2^{\omega(\log n)}$ ,  $m = 2n \log q$ ,  $r = \sqrt{q} \omega(\sqrt{\log m})$ ,  $2\sqrt{n}/q \leq \beta \leq \sqrt{2\pi}/(r\sqrt{2mn})$ , 则上述哈希证明系统 HPS 在 LWE 假设下是光滑的.

证明:整个证明过程可被分为以下 3 个部分:子集成员关系问题、正确性和光滑性.

**引理 12(子集和成员不可区分).** 上述基于 LWE 的哈希证明系统所对应的子集和成员关系问题是计算困难的.

证明:给定  $\mathbf{A} \leftarrow \mathbb{Z}_q^m$  作为公共参数中的随机矩阵,则合法密文和非法密文集合可分别表示为

$$V = \{\mathbf{A}\mathbf{s} + \mathbf{e} \bmod q : \mathbf{s} \leftarrow \mathbb{Z}_q^n, \mathbf{e} \leftarrow \bar{\psi}_\beta^m\}, \text{ 其中, } \beta q \geq 2\sqrt{n}$$

和

$$V' = \{\mathbf{A}\mathbf{s} + \mathbf{e} \bmod q : \mathbf{s} \leftarrow \mathbb{Z}_q^n, \|\mathbf{e}\| \geq \sqrt{q}/4\}.$$

显然,所有密文的集合  $C$  是  $\mathbb{Z}_q^m$  的一个子集.事实上,矩阵  $\mathbf{A}$  定义了格

$$\Lambda(\mathbf{A}) = \{\mathbf{y} \in \mathbb{Z}^m : \exists \mathbf{s} \in \mathbb{Z}_q^n \text{ s.t. } \mathbf{y} = \mathbf{A}\mathbf{s} \bmod q\}.$$

同时注意到,合法密文集合  $V$  中的所有元素到格  $\Lambda(\mathbf{A})$  的距离可以记为  $\|\mathbf{e}\|$ , 并且由引理 11 可知,

$$\|\mathbf{e}\| \leq \beta q \cdot \omega(\sqrt{\log m}) + \sqrt{m}/2.$$

相对而言,非法密文集合  $V'$  中的元素到格  $\Lambda(\mathbf{A})$  的距离比较远.由格  $\Lambda(\mathbf{A})$  的性质和参数  $\beta \leq \sqrt{2\pi}/(r\sqrt{2mn})$  可知,对于任意  $\mathbf{x} \in V$ , 其相应的证据就是使得  $\|\mathbf{x} - \mathbf{A}\mathbf{s}\| \leq \beta q \cdot \omega(\sqrt{\log m}) + \sqrt{m}/2$  成立的向量  $\mathbf{s} \in \mathbb{Z}_q^n$ . 进一步根据引理 10 可知,对于任意  $\mathbf{x} \in V$  和随机均匀  $\mathbf{u} \leftarrow \mathbb{Z}_q^m$  可知,  $(\mathbf{A}, \mathbf{x}) \approx_c (\mathbf{A}, \mathbf{u})$ . 因此,相关的子集和成员关系问题是计算困难的.证毕.  $\square$

**引理 13(正确性).** 上述基于 LWE 的哈希证明系统满足正确性的要求.

证明:给定公开矩阵  $\mathbf{A} \leftarrow \mathbb{Z}_q^m$  和合法密文  $\mathbf{x} \in V$ , 存在唯一的证据向量  $\mathbf{s} \in \mathbb{Z}_q^n$  和差错向量  $\mathbf{e} \leftarrow \bar{\psi}_\beta^m$  使得  $\mathbf{x} = \mathbf{A}\mathbf{s} + \mathbf{e} \bmod q$ . 因此,

$$\begin{aligned} \langle \mathbf{v}, \mathbf{x} \rangle \bmod q &= \langle \mathbf{v}, \mathbf{x} = \mathbf{A}\mathbf{s} + \mathbf{e} \rangle \bmod q \\ &= (\langle \mathbf{v}, \mathbf{A}\mathbf{s} \rangle + \langle \mathbf{v}, \mathbf{e} \rangle) \bmod q \\ &= (\langle \mathbf{A}^T \mathbf{v}, \mathbf{s} \rangle + \langle \mathbf{v}, \mathbf{e} \rangle) \bmod q \\ &= (\langle \mathbf{y}, \mathbf{s} \rangle + \langle \mathbf{v}, \mathbf{e} \rangle) \bmod q. \end{aligned}$$

由引理 7 可知,对于  $\mathbf{v} \leftarrow D_{\mathbb{Z}_q^m, r}$ , 其二范数以极大的概率满足  $\|\mathbf{v}\| \leq r\sqrt{m}$ . 根据  $\bar{\psi}_\beta$  的定义,令  $e_i = q \cdot t_i \bmod q$ , 其中,  $t_i$  是以 0 为期望、 $\beta^2/2\pi$  为方差的独立正态分布变量.因此,  $\|\mathbf{e} - \mathbf{t}\| \leq \sqrt{m}/2$ , 并且由柯西-施瓦兹不等式可知,  $|\langle \mathbf{v}, \mathbf{e} \rangle - \langle \mathbf{v}, \mathbf{t} \rangle| \leq rm/2$ . 进一步地,由于  $t_i$  是独立均匀选取的,  $\langle \mathbf{v}, \mathbf{t} \rangle$  也是一个以 0 为期望的正态分布,并且其标准差为  $\|\mathbf{v}\| \cdot \beta/\sqrt{2\pi} \leq r\sqrt{m} \cdot \beta/\sqrt{2\pi} \leq 1/\sqrt{2n}$ . 由正态变量的尾不等式可知,  $|\langle \mathbf{v}, \mathbf{t} \rangle| > 1$  的概率是可忽略的.因此,  $|\langle \mathbf{v}, \mathbf{e} \rangle| > rm/2 + 1$  的概率也是可忽略的.

注意到,由于  $\mathbf{s} \in \mathbb{Z}_q^n$  是随机均匀的,  $\langle \mathbf{y}, \mathbf{s} \rangle \bmod q$  也服从  $\mathbb{Z}_q$  上的均匀分布.对于正确性而言,只需要证明算法 Priv 输出错误比特的概率是可忽略的.通过分析得知,这个事件发生当且仅当  $\langle \mathbf{y}, \mathbf{s} \rangle \bmod q$  与  $\lfloor q/4 \rfloor$  或  $\lfloor 3q/4 \rfloor$  之间的距离小于  $rm/2 + 1$ . 令  $d = rm/2 + 1$ ,  $\langle \mathbf{y}, \mathbf{s} \rangle \bmod q$  有  $4d$  个取值使得算法 Priv 输出错误比特.此时,对于  $q = 2^{\omega(\log n)}$ ,

$$\frac{4d}{q} < \frac{4rm}{q} = \frac{8n\sqrt{q}\omega(\sqrt{\log m})\omega(\log n)}{q} = \frac{8n\sqrt{q}\omega(\sqrt{\log m})\omega(\log n)}{2^{\omega(\log n)}} \leq \text{negl}(n).$$

因此,对于任意合法密文向量  $\mathbf{x} \in V$ , 两种不同计算方式的输出是以极大概率相同的. 证毕.  $\square$

**引理 14(光滑性).** 上述基于 LWE 的哈希证明系统满足光滑性的要求.

证明:根据非法密文集合  $V'$  的定义可知,对于任意非法密文向量  $\mathbf{x} \in V'$ ,  $\mathbf{x}$  到格  $\Lambda(\mathbf{A})$  之间的距离大于  $\sqrt{q}/4$ . 由引理 3 可知,对于任意非零  $a \in \mathbb{Z}_q$ ,  $\text{dist}(a \cdot \mathbf{x}, \Lambda(\mathbf{A})) \geq \sqrt{q}/4$ . 此时,令  $\mathbf{A}' = (\mathbf{A} | \mathbf{x})$ . 由引理 2 可知, $\mathbf{x}$  与  $\mathbb{Z}_q^m$  上的均匀分布是统计不可区分的. 进一步可得  $\mathbf{A}'$  与  $\mathbb{Z}_q^{m \times (n+1)}$  上的均匀分布之间的统计距离是不可区分的,并且  $\lambda_1(\mathbf{A}') > \sqrt{q}/4$ . 接着由引理 6 和  $\Lambda(\mathbf{A}')$  与  $\Lambda^\perp(\mathbf{A}')$  之间的对偶关系可知,

$$\eta_c(\Lambda^\perp(\mathbf{A}')) \leq \omega(\sqrt{\log m}) \left/ \left( \frac{1}{q} \cdot \lambda(\Lambda(\mathbf{A}')) \right) \right. \leq \sqrt{q}\omega(\sqrt{\log m}).$$

由引理 8 和引理 9 可知,对于任意  $\mathbf{v} \leftarrow D_{\mathbb{Z}_q^m, r}$ , 其中,  $r \geq \sqrt{q}\omega(\sqrt{\log m})$ , 向量  $\mathbf{u}' = (\mathbf{A}')^T \cdot \mathbf{v} \bmod q$  与  $\mathbb{Z}_q^{n+1}$  上均匀分布之间的统计距离是可以忽略的. 因此,对于任意  $\mathbf{x} \in V'$ , 满足

$$(\mathbf{A}^T \cdot \mathbf{v}, \langle \mathbf{v}, \mathbf{x} \rangle \bmod q) \approx_s (\mathbf{A}^T \cdot \mathbf{v}, u),$$

其中,  $u$  是  $\mathbb{Z}_q$  上的随机均匀变量. 也就是说,在给定公钥  $\mathbf{y} = \mathbf{A}^T \mathbf{v} \bmod q$ 、非法密文向量  $\mathbf{x} \in V'$  的情况下,  $\langle \mathbf{v}, \mathbf{x} \rangle \bmod q$  和  $u$  仍然是统计不可区分的. 因此,该基于 LWE 假设的哈希证明系统是光滑的. 证毕.  $\square$

综上所述,由上面 3 个引理可知,定理 1 成立. 证毕.  $\square$

### 3 基于 LWE 假设的基于身份的哈希证明系统

#### 3.1 基于 LWE 假设的基于身份的哈希证明系统的构造

在基于身份的哈希证明系统的构造中,需要用到随机谕言机  $H: \{0,1\}^* \rightarrow \mathbb{Z}_q^n$ , 将任意身份映射为  $\mathbb{Z}_q^n$  中的向量. 本节所提出的基于 LWE 的基于身份的哈希证明系统 IB-HPS=(Setup,KeyGen,Encap,Encap\*,Decap)可按如下方式进行具体描述.

**Setup**( $1^n$ ):运行引理 1 中的陷门生成算法 TrapGen 生成矩阵  $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$  和陷门矩阵  $\mathbf{T} \in \mathbb{Z}^{m \times m}$ . 输出主公钥  $\text{mpk} := \mathbf{A}$ , 主私钥  $\text{msk} := \mathbf{T}$ .

**KeyGen**( $\text{mpk}, id, \text{msk}$ ):令  $\mathbf{u} = H(id)$ , 利用陷门矩阵  $\mathbf{T} \in \mathbb{Z}^{m \times m}$  运行 SampleSIS( $\mathbf{A}, \mathbf{T}, \mathbf{u}, r$ ) 抽取向量  $\mathbf{v} \in \mathbb{Z}^m$  使得  $\mathbf{A}^T \mathbf{v} \bmod q = \mathbf{u}$ . 输出身份私钥  $sk_{id} := \mathbf{v}$ .

**Encap**( $\text{mpk}, id$ ):令  $\mathbf{u} = H(id)$ , 随机选取  $\mathbf{s} \leftarrow \mathbb{Z}_q^n$  和  $\mathbf{e} \leftarrow \bar{\nu}_\beta^m$ , 计算  $\mathbf{x} = \mathbf{A}\mathbf{s} + \mathbf{e} \bmod q$ . 令  $z = \langle \mathbf{u}, \mathbf{s} \rangle \bmod q$ . 如果  $z$  与 0 之间的距离小于  $z$  与  $\lfloor q/2 \rfloor$  之间的距离, 令  $b=0$ ; 反之, 令  $b=1$ . 输出  $(c, k) := (\mathbf{x}, b)$ .

**Encap\***( $\text{mpk}, id$ ):随机选取  $\mathbf{s} \leftarrow \mathbb{Z}_q^n$  和向量  $\mathbf{e}$  满足  $\|\mathbf{e}\| \geq \sqrt{q}/4$ , 计算  $\mathbf{x} = \mathbf{A}\mathbf{s} + \mathbf{e} \bmod q$ . 输出  $c := \mathbf{x}$ .

**Decap**( $c, sk_{id}$ ):给定  $c := \mathbf{x} \in \mathbb{Z}_q^m$  和  $sk_{id} := \mathbf{v} \in \mathbb{Z}^m$ , 计算  $z = \langle \mathbf{v}, \mathbf{x} \rangle \bmod q$ . 如果  $z$  与 0 之间的距离小于  $z$  与  $\lfloor q/2 \rfloor$  之间的距离, 输出 0; 反之, 输出 1.

#### 3.2 基于身份的哈希证明系统的证明

**定理 2.** 给定安全参数  $n$ , 令  $q = 2^{\omega(\log n)}$ ,  $m = 2n \log q$ ,  $r = \sqrt{q}\omega(\sqrt{\log m})$ ,  $2\sqrt{n}/q \leq \beta \leq \sqrt{2\pi}/(r\sqrt{2mn})$ , 则上述基于身份的哈希证明系统 IB-HPS 在 LWE 假设下是光滑的.

证明:对于正确性而言,给定合法密文  $c := \mathbf{x} \in \mathbb{Z}_q^m$  和  $sk_{id} := \mathbf{v} \in \mathbb{Z}^m$ , 可知

$$\begin{aligned} \langle \mathbf{v}, \mathbf{x} \rangle \bmod q &= \langle \mathbf{v}, \mathbf{x} = \mathbf{A}\mathbf{s} + \mathbf{e} \rangle \bmod q \\ &= (\langle \mathbf{v}, \mathbf{A}\mathbf{s} \rangle + \langle \mathbf{v}, \mathbf{e} \rangle) \bmod q \\ &= (\langle \mathbf{A}^T \mathbf{v}, \mathbf{s} \rangle + \langle \mathbf{v}, \mathbf{e} \rangle) \bmod q \\ &= (\langle \mathbf{u}, \mathbf{s} \rangle + \langle \mathbf{v}, \mathbf{e} \rangle) \bmod q. \end{aligned}$$



由引理 13 可知,在上述定理 2 的参数设置下,  $\langle \mathbf{v}, \mathbf{e} \rangle \bmod q$  的值以极大的概率不会影响  $b=0$  或  $b=1$ .

对于光滑性而言,给定任意非法密文  $\mathbf{x} \in V'$  满足  $\text{dist}(\mathbf{x}, \Lambda(\mathbf{A})) \geq \sqrt{q}/4$ , 令  $\mathbf{A}' = (\mathbf{A} | \mathbf{x})$ . 与引理 14 中的分析相类似,可知  $\lambda_1(\mathbf{A}') \geq \sqrt{q}/4$ . 进一步地,由引理 6 可知,

$$\eta_c(\Lambda^{-1}(\mathbf{A}')) \leq \omega(\sqrt{\log m}) \left/ \left( \frac{1}{q} \cdot \lambda_1(\mathbf{A}') \right) \right. \leq \sqrt{q} \omega(\sqrt{\log m}).$$

由引理 5 可知,对于均匀随机向量  $\mathbf{u} = H(id)$ , 算法 SampleISIS 输出向量  $\mathbf{v}$  的分布与离散高斯分布  $D_{\mathbb{Z}_q^{m,r}}$  之间的统计距离是可忽略的. 因此,由引理 8 和引理 9 可知,向量  $\mathbf{u}' = (\mathbf{A}')^T \cdot \mathbf{v} \bmod q$  与  $\mathbb{Z}_q^{n+1}$  上均匀分布之间的统计距离是可以忽略的. 因此,对于任意  $\mathbf{x} \in V'$ , 满足

$$(\mathbf{A}'^T \cdot \mathbf{v}, \langle \mathbf{v}, \mathbf{x} \rangle \bmod q) \approx_s (\mathbf{A}'^T \cdot \mathbf{v}, u),$$

其中,  $u$  是  $\mathbb{Z}_q$  上的随机均匀变量. 也就是说,对于任意身份  $id$  使得  $\mathbf{u} = H(id)$ , 在给定  $\mathbf{u} = \mathbf{A}'^T \mathbf{v} \bmod q$ , 非法密文向量  $\mathbf{x} \in C \setminus V$  的情况下,  $\langle \mathbf{v}, \mathbf{x} \rangle \bmod q$  和  $u$  仍然是统计不可区分的. 因此,该基于 LWE 假设的哈希证明系统是光滑的.

对于合法密文和非法密文的计算不可区分问题而言,可以建立一个从有效的判定型 LWE 问题到有效区分合法密文和非法密文问题的黑盒归约. 即给定一个有效区分合法密文和非法密文的攻击者  $\mathcal{A}$ , 可以构造出一个有效算法  $\mathcal{B}$  用于判定一个谕言机  $\mathcal{O}$  是 LWE 谕言机还是均匀谕言机. 按照基于身份的哈希证明系统的定义要求,用下面的游戏描述  $\mathcal{B}$  和  $\mathcal{A}$  之间的交互过程.

**Setup:**  $\mathcal{B}$  首先对谕言机  $\mathcal{O}$  询问  $m$  次,得到  $\{(\mathbf{a}_i, b_i)_{i \in [m]}\}$ . 将  $\mathbf{a}_i^T$  作为矩阵  $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$  的第  $i$  个列向量,并将  $\mathbf{A}$  作为主公钥发送给攻击者  $\mathcal{A}$ .

**KeyGen1:**  $\mathcal{B}$  建立一个用于存储三元组  $(id, \mathbf{u}, \mathbf{v}) \in \{0,1\}^* \times \mathbb{Z}_q^n \times \mathbb{Z}_q^m$  的表  $L$ , 该表的初始值为空. 为了回答由  $\mathcal{A}$  提出的针对身份  $id$  的私钥提取询问,  $\mathcal{B}$  首先检查表  $L$  中是否存在  $(id, \cdot, \cdot)$  的三元组. 如果存在, 则将该三元组中的第 3 个元素  $\mathbf{v}$  作为相应的身份私钥  $sk_{id}$  返回给  $\mathcal{A}$ . 如果不存在这样的三元组, 则随机选取一个向量  $\mathbf{v} \leftarrow D_{\mathbb{Z}_q^{m,r}}$ , 将三元组  $(id, \mathbf{A}^T \mathbf{v}, \mathbf{v})$  添加到表  $L$  中, 并将  $\mathbf{v}$  作为相应的身份私钥  $sk_{id}$  返回给  $\mathcal{A}$ . 针对攻击者  $\mathcal{A}$  对于身份  $id$  的随机谕言机询问,  $\mathcal{B}$  首先检查表  $L$  中是否存在  $(id, \cdot, \cdot)$  的三元组. 如果存在, 则将该三元组中的第 2 个元素  $\mathbf{u}$  作为对身份  $id$  的随机谕言机输出值  $H(id)$  返回给  $\mathcal{A}$ . 如果不存在这样的三元组, 则随机选取一个向量  $\mathbf{v} \leftarrow D_{\mathbb{Z}_q^{m,r}}$ , 将三元组  $(id, \mathbf{A}^T \mathbf{v}, \mathbf{v})$  添加到表  $L$  中, 并将  $\mathbf{A}^T \mathbf{v}$  作为对身份  $id$  的随机谕言机输出值  $H(id)$  返回给  $\mathcal{A}$ .

**Challenge:**  $\mathcal{A}$  针对身份  $id^*$  向  $\mathcal{B}$  发出挑战询问,  $\mathcal{B}$  将向量  $\mathbf{c} = (b_1, \dots, b_m)^T$  作为挑战密文返还给  $\mathcal{A}$ .

**KeyGen2:**  $\mathcal{B}$  用 KeyGen1 中的方法回答  $\mathcal{A}$  的私钥提取询问和随机谕言机询问.

**Output:**  $\mathcal{B}$  得到从  $\mathcal{A}$  返回的一个比特  $b'$ , 并将其转发给判定型 LWE 问题的挑战者.

在真实的游戏,对于某个身份  $id$ , 攻击者  $\mathcal{A}$  所能得到的信息包括一个随机矩阵  $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ 、统计均匀的向量  $H(id) = \mathbf{u} \in \mathbb{Z}_q^n$  和一个随机向量  $sk_{id} := \mathbf{v} \in D_{\mathbb{Z}_q^{m,r}}$ . 对上述交互式游戏进行详细分析得知,由向量  $(\mathbf{a}_i)_{i \in [m]}$  生成的矩阵  $\mathbf{A}$  是均匀随机的. 由引理 5 和算法 SampleISIS 的性质可知,以上交互式游戏中  $H(id)$  和  $sk_{id}$  的联合分布与真实游戏中的分布是相同的. 因此,以上游戏对  $\mathcal{A}$  攻击环境的模拟是合理的.

进一步地,如果  $\mathcal{O}$  是 LWE 谕言机,则返回的挑战密文向量  $\mathbf{c} = (b_1, \dots, b_m)^T$  与算法 Encap( $id^*$ ) 的输出向量是同分布的. 反之,  $\mathbf{c} = (b_1, \dots, b_m)^T$  与算法 Encap\*( $id^*$ ) 的输出向量是同分布的. 因此,由  $\mathcal{A}$  可以构造一个有效区分 LWE 谕言机的算法  $\mathcal{B}$ .

综上所述,本节所提出的 IB-HPS 是光滑的. 证毕. □

#### 4 基于 LWE 假设的可更新哈希证明系统

通常,哈希证明系统可以直接用来构造抵抗密钥泄露攻击的加密方案. 但是前面提到的两个基于格的哈希证明系统只能用来构造相对泄露模型和有界泄露模型下的加密方案. 为了进一步构造能够抵抗连续泄露攻击的加密方案,本节将第 3 节中所提出的哈希证明系统扩展为可更新的哈希证明系统.

注意到, Yang 等人已经给出了一种构造可更新的哈希证明系统的方法<sup>[21]</sup>. 为了实现对密钥的安全更新, Yang 等人提出了一种新的抽样方法, 并且要求私钥具有两种不可区分性质. 但是, Yang 等人所提出的可更新哈希证明系统并不能抵抗潜在的量子攻击威胁. 因此, 如何设计具有后量子安全性的可更新哈希证明系统是一个有意义的研究问题.

通过对第 3 节中所提出的基于 LWE 哈希证明系统进行分析得知, 利用已有的高斯抽样算法 SampleISIS 的特性, 可以很容易地对其私钥进行更新. 并且由算法 SampleISIS 的输出值服从独立离散高斯分布的特性可以证明, 该更新方法是安全的. 但该构造中需要引入更新密钥作为算法 SampleISIS 的输入.

#### 4.1 可更新哈希证明系统的构造

基于 LWE 的可更新哈希证明系统 UHPS=(Param, Pub, Priv, KeyUpd)可按如下方式进行具体描述.

**Param**( $1^n$ ): 给定安全参数  $n$ , 输出参数  $(group, K, C, V, V', PK, SK, H_{(·)}, \mu)$ , 其中,

- $group = (\mathbb{Z}, q, m, \mathbf{A}, \mathbf{T}, \beta, r)$ ,  $q$  是一个素数,  $m = 2n \log q$  是所用到的格的维数, 随机、均匀选取矩阵  $\mathbf{A} \leftarrow \mathbb{Z}_q^{m \times n}$ ,  $\beta \in (0, 1)$  和  $r = \sqrt{q\omega(\sqrt{\log m})}$  是两个实数, 满足  $\beta q \geq 2\sqrt{n}$  和  $\beta \leq \sqrt{2\pi}/(r\sqrt{m} \cdot \omega(\sqrt{\log n}))$ . 运行陷门生成算法 TrapGen 生成矩阵  $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$  和陷门矩阵  $\mathbf{T} \in \mathbb{Z}^{m \times m}$ . 其中, 矩阵  $\mathbf{A}$  与  $\mathbb{Z}_q^{m \times n}$  上的均匀分布是统计不可区分的, 并且  $\|\tilde{\mathbf{T}}\| = O(\sqrt{n \log q})$ .

- $SK$  是  $\mathbb{Z}^m$  上的离散高斯分布  $D_{\mathbb{Z}^m, r}$ ,  $PK = \mathbb{Z}_q^n$ .

- 对于任意私钥  $sk := \mathbf{v} \leftarrow D_{\mathbb{Z}^m, r}$ , 其对应的公钥为  $pk := \mathbf{y} = \mu(sk) = \mathbf{A}^T \mathbf{v} \bmod q$ .

- $V = \{\mathbf{A}\mathbf{s} + \mathbf{e} \bmod q : \mathbf{s} \leftarrow \mathbb{Z}_q^n, \mathbf{e} \leftarrow \bar{\nu}_\beta^m\}$ ,  $V' = \{\mathbf{A}\mathbf{s} + \mathbf{e} \bmod q : \mathbf{s} \leftarrow \mathbb{Z}_q^n, \|\mathbf{e}\| \geq \sqrt{q}/4\}$ ,  $K = \{0, 1\}$ .

**Pub**( $pk, c, w$ ): 给定一个合法密文  $c := \mathbf{x} = \mathbf{A}\mathbf{s} + \mathbf{e} \bmod q \in V$ , 其对应的证据是  $\mathbf{s} \in \mathbb{Z}_q^n$ , 差错向量是  $\mathbf{e} \leftarrow \bar{\nu}_\beta^m$ . 计算  $z = \langle \mathbf{y}, \mathbf{s} \rangle \bmod q$ , 如果  $z$  与 0 之间的距离小于  $z$  与  $\lfloor q/2 \rfloor$  之间的距离, 输出  $k=0$ ; 反之, 输出  $k=1$ .

**Priv**( $sk, c$ ): 给定密文  $c := \mathbf{x}$  和私钥  $sk := \mathbf{v}$ , 计算  $z = \langle \mathbf{v}, \mathbf{x} \rangle \bmod q$ , 如果  $z$  与 0 之间的距离小于  $z$  与  $\lfloor q/2 \rfloor$  之间的距离, 输出  $k=0$ ; 反之, 输出  $k=1$ .

**KeyUpd**( $\mathbf{T}, sk$ ): 对于  $sk := \mathbf{v} \leftarrow D_{\mathbb{Z}^m, r}$ , 计算  $\mathbf{y} = \mathbf{A}^T \mathbf{v} \bmod q$ . 然后利用算法 SampleISIS 以  $\mathbf{T}$  和  $\mathbf{y}$  作为输入, 可以抽取新的  $sk' := \mathbf{v}' \leftarrow D_{\mathbb{Z}^m, r}$ , 使得  $\mathbf{A}^T \mathbf{v}' = \mathbf{A}^T \mathbf{v} \bmod q$ .

与第 3 节中的哈希证明系统相类似, 该可更新哈希证明系统中的所有操作都是可以有效完成的.

下面对本构造中用到的更新过程进行如下注解. 首先, 原有私钥和更新私钥所对应的公钥是完全一样的; 其次, 对应于一个公钥的所有不同私钥都是独立同分布的; 最后, 陷门矩阵  $\mathbf{T}$  被作为更新密钥进行使用, 即在没有  $\mathbf{T}$  的情况下, 私钥是没有办法更新的. 因此, 在直接利用该可更新哈希证明系统构造抗泄露加密方案时, 必须假设更新过程是可以免受泄露攻击的.

#### 4.2 可更新哈希证明系统的证明

**定理 3.** 给定安全参数  $n$ , 令  $q = 2^{\omega(\log n)}$ ,  $m = 2n \log q$ ,  $r = \sqrt{q\omega(\sqrt{\log m})}$ ,  $2\sqrt{n}/q \leq \beta \leq \sqrt{2\pi}/(r\sqrt{2mn})$ , 则上述可更新哈希证明系统 UHPS 在 LWE 假设下是光滑的.

### 5 参数对比与效率分析

本节从计算和存储代价两个方面出发, 在表 1~表 3 中详细对比分析本文 3 个新型构造和已有相关构造的差别. 为了使得该对比分析更加公平, 本文将所有参与对比分析的哈希证明系统的封装密钥调整为 1 个比特. 我们用 [7]a 和 [7]b 分别表示文献 [7] 中的哈希证明系统和基于身份的哈希证明系统.

此时, 用  $n$  表示安全参数,  $m$  是  $n$  的一个函数, 例如令  $m = 2n \log q$ ,  $c \in (0, 1)$  是一个常数. 用  $|pk|$  和  $|sk|$  分别表示公钥和私钥的尺寸,  $|mpk|$ ,  $|msk|$  和  $|sk_{id}|$  分别用来表示基于身份设置下密钥的尺寸. 用  $\mathbf{w}$  和  $\mathbf{a}$  分别表示  $\mathbb{Z}_q$  上的一个乘法运算和加法运算. 在文献 [21] 中, 分别用  $\mathbf{w}'$  和  $\mathbf{p}$  表示  $q$  阶素数循环群中的一个乘法运算和一个双线性映

射运算.

**Table 1** Comparison with other hash proof systems based on lattices  
表 1 与其他已有基于格的哈希系统的对比

	$ pk $	$ sk $	封装计算	解封装计算	密文尺寸	安全模型
[7]a	$nO(\log n)$	$mO(\log n)$	$n \cdot \tau + a$	$m \cdot \tau + a$	$(m+1)O(\log n)$	标准模型
文献[11]	$nO(\log n)$	$mO(\log n)$	$n \cdot \tau$	$m(n+2) \cdot \tau + m \cdot a$	$(m+n)O(\log n) + n$	标准模型
第 3 节的构造	$n^{1+c}$	$mn^c$	$n \cdot \tau$	$m \cdot \tau$	$mn^c$	标准模型

**Table 2** Comparison with other identity-based hash proof systems based on lattices  
表 2 与其他已有格上的基于身份的哈希系统的对比

	$ mpk $	$ msk $	$ sk_d $	封装计算	解封装计算	密文尺寸	安全模型
文献[3]	$mn^{1+c}$	$m^2 n^c$	$mn^c$	$n \cdot \tau + a$	$m \cdot \tau + a$	$(m+1)n^c$	理想模型
[7]b	$mn^{1+c}$	$m^2 n^c$	$mn^c$	$n \cdot \tau + a$	$m \cdot \tau + a$	$(m+1)n^c$	理想模型
第 4 节的构造	$mn^{1+c}$	$m^2 n^c$	$mn^c$	$n \cdot \tau + a$	$m \cdot \tau + a$	$mn^c$	理想模型

**Table 3** Comparison with other updatable hash proof systems  
表 3 与其他已有可更新哈希系统的对比

	$ pk $	$ sk $	封装计算	解封装计算	密文尺寸	安全假设	安全模型
文献[21]	$O(\log n)$	$nO(\log n)$	$q \cdot \tau'$	$n \cdot (\tau' + p)$	$nO(\log n)$	SXDH	标准模型
第 5 节的构造	$n^{1+c}$	$mn^c$	$n \cdot \tau + a$	$m \cdot \tau + a$	$mn^c$	LWE	标准模型

通过对表 1 进行分析得知,本文第 3 节的构造与已有相关构造相比,在解封装计算和密文尺寸方面具有一定的优势.通过对表 2 进行分析得知,本文第 4 节的构造与已有相关构造相比,在其他参数相等的前提下,密文尺寸具有明显优势.因此,利用基于身份的哈希证明系统所构造的方案将具有更高的效率优势.在表 3 中,虽然本文第 5 节的构造在效率方面不具有优势,但由于该构造是基于 LWE 假设的,所以能够抵抗潜在的量子计算攻击.

## 6 结 论

为了构造密文尺寸较小的可用于构造隐私保护方案的基于身份的哈希证明系统,本文首先基于标准 LWE 假设,在标准模型下成功构造了一个新的哈希证明系统,并利用随机格上离散高斯分布与光滑参数的性质,证明其是光滑的;再在随机谕言机的作用下,利用原像抽样函数将其推广得到基于身份的哈希证明系统.作为对所构造的新型哈希证明系统的进一步扩展,本文也在标准模型下提出一个可更新的哈希证明系统.最后,通过详细分析对比与已有相关构造的差别可知,本文构造的哈希证明系统具有一定的效率优势,并且可以抵抗潜在的量子计算攻击.

但本文构造的 3 个哈希证明系统所用到的模数都是亚指数的,因此存储和计算效率仍然相对较低.如何构造模数是多项式的哈希证明系统是进一步的研究方向.

## References:

- [1] Feng DG, Zhang M, Li H. Big data security and privacy protection. *Ji Suan Ji Xue Bao/Chinese Journal of Computers*, 2014,37(1):246–258 (in Chinese with English abstract).
- [2] Peng CG, Ding HF, Zhu YJ, Tian YL, Fu ZF. Information entropy models and privacy metrics methods for privacy protection. *Ruan Jian Xue Bao/Journal of Software*, 2016,27(8):1891–1903 (in Chinese with English abstract). <http://www.jos.org.cn/1000-9825/5096.htm> [doi: 10.13328/j.cnki.jos.005096]
- [3] Alwen J, Dodis Y, Naor M, Segev G, Walfish S, Wichs D, Walfish S, Wichs D. Public-Key encryption in the bounded-retrieval model. In: Gilbert H, ed. *Proc. of the 29th Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2010)*. Berlin: Springer-Verlag, 2010. 113–134.

- [4] Naor M, Segev G. Public-Key cryptosystems resilient to key leakage. In: Halevi S, ed. Proc. of the 29th Annual Int'l Cryptology Conf. (CRYPTO 2009). Berlin: Springer-Verlag, 2010. 18–35.
- [5] Chow SM, Dodis Y, Rouselakis Y, Waters B. Practical leakage-resilient identity-based encryption from simple assumptions. In: Al-Shaer E, Keromytis AD, Shmatikov V, eds. Proc. of the 17th ACM Conf. on Computer and Communications Security (CCS 2010). New York: ACM, 2010. 152–161.
- [6] Chen Y, Zhang ZY, Lin DD, Cao ZF. Anonymous identity-based hash proof system and its applications. In: Takagi T, Wang GL, Qin ZG, Jiang SQ, Yu Y, eds. Proc. of the 6th Int'l Conf. on Provable Security (ProvSec 2012). Berlin: Springer-Verlag, 2010. 143–160.
- [7] Chen Y, Zhang ZY, Lin DD, Cao ZF. Generalized (identity-based) hash proof system and its applications. Security and Communication Networks, 2016,9(12):1698–1716.
- [8] Chen Y, Zhang ZY, Lin DD, Cao ZF. Identity-Based extractable hash proofs and their applications. In: Boureau I, Owesarski P, Vaudenay S, eds. Proc. of the 12th Int'l Conf. on Applied Cryptography and Network Security (ACNS 2012). Berlin: Springer-Verlag, 2012. 153–170.
- [9] Chen Y, Zhang ZY, Lin DD, Cao ZF. CCA-Secure IB-KEM from identity-based extractable hash proof system. The Computer Journal, 2014,57(10):1537–1556.
- [10] Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions. In: Dwork C, ed. Proc. of the 40th Annual ACM Symp. on Theory of Computing (STOC 2008). New York: ACM, 2010. 197–206.
- [11] Katz J, Vaikuntanathan V. Smooth projective hashing and password-based authenticated key exchange from lattices. In: Matsui M, ed. Proc. of the 15th Int'l Conf. on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2009). Berlin: Springer-Verlag, 2009. 636–652.
- [12] Ajtai M. Generating hard instances of the short basis problem. In: Bratko I, Dzeroski S, eds. Proc. of the 16th Int'l Conf. on Machine Learning (ICALP 1999). Berlin: Springer-Verlag, 1999. 1–9.
- [13] Alwen J, Peikert C. Generating shorter bases for hard random lattices. Theory of Computing Systems, 2011,48(3):535–553.
- [14] Micciancio D, Regev O. Worst-Case to average-case reductions based on gaussian measures. SIAM Journal on Computing, 2007,37(1):267–302.
- [15] Peikert C. Limits on the hardness of lattice problems in  $l_p$  norms. Computational Complexity, 2008,17(2):300–351.
- [16] Regev O. On lattices, learning with errors, random linear codes, and cryptography. Journal of the ACM, 2009,56(6):34:1–34:40.
- [17] Agrawal S, Boneh D, Boyen X. Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE. In: Rabin T, ed. Proc. of the 30th Annual Cryptology Conf. (CRYPTO 2010). Berlin: Springer-Verlag, 2010. 98–115.
- [18] Agrawal S, Boneh D, Boyen X. Efficient lattice (H)IBE in the standard model. In: Gilbert H, ed. Proc. of the 29th Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2010). Berlin: Springer-Verlag, 2010. 553–572.
- [19] Cramer R, Shoup V. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In: Knudsen LR, ed. Proc. of the 21st Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2002). Berlin: Springer-Verlag, 2002. 45–64.
- [20] Hofheinz D, Kiltz E. Secure hybrid encryption from weakened key encapsulation. In: Menezes A, ed. Proc. of the 27th Annual Int'l Cryptology Conf. (CRYPTO 2007). Berlin: Springer-Verlag, 2007. 553–571.
- [21] Yang RP, Xu QL, Zhou Y., Zhang R, Hu C, Yu Z. Updatable hash proof system and its applications. In: Proc. of the 20th European Symp. on Research in Computer Security (ESORICS 2015). Berlin: Springer-Verlag, 2015. 266–285.

#### 附中文参考文献:

- [1] 冯登国,张敏,李昊.大数据安全与隐私保护.计算机学报,2014,37(1):246–258.
- [2] 彭长根,丁红发,朱义杰,田有亮,符祖峰.隐私保护的信息熵模型及其度量方法.软件学报,2016,27(8):1891–1903. <http://www.jos.org.cn/1000-9825/5096.htm> [doi: 10.13328/j.cnki.jos.005096]



来齐齐(1985—),男,河南新乡人,博士,讲师,主要研究领域为格公钥加密方案的设计与分析.



杨波(1963—),男,博士,教授,博士生导师,主要研究领域为格公钥加密方案的设计与分析.



陈原(1978—),女,博士,副教授,主要研究领域为密码学.



韩露露(1991—),男,硕士,主要研究领域为密码学,伪随机数发生器.



白健(1989—),男,工程师,主要研究领域为密码学,匿名隐私保护.

www.jos.org.cn

www.jos.org.cn