抗量子计算的装备保障云服务同态认证方案设计

张建航[1,2]，曹泽阳[1]，宋晓峰[2]，邢立鹏[2]
(1.空军工程大学防空反导学院，西安，710051；国防科技大学信息通信学院，西安，710106)

摘要 基于格理论设计的同态认证方案具有抗量子计算的属性，然而现有的标准格上设计的同态认证方案由于密钥存储量大，结构复杂导致方案实际运行效率相对偏低，不能应用于装备保障云服务中。基于NTRU格理论，设计了首个抗量子计算的面向装备保障云服务的线性同态认证方案，新方案利用NTRU密钥生成算法简化了系统的密钥，避免了庞大的密钥量，然后采用结构简洁的NTRU格上原像高斯抽样算法产生出线性同态认证值。证明结果与分析表明：新方案具有弱内容隐私性安全，在随机预言机模型下，新方案在NTRU-SIS问题困难性假设下满足适应性选择消息的存在性不可伪造性。通过与已有方案实现效率相比，新方案在密钥量、认证代价和通信代价方面均为最优。

关键词 抗量子计算；云服务；同态认证；NTRU格；原像高斯抽样算法
DOI 10.3969/j.issn.1009-3516.2020.02.016
中图分类号 TN918；TP309 **文献标志码** A **文章编号** 1009-3516(2020)02-0106-06

A Design of Homomorphous Authentication Scheme for Equipment Support Cloud Services with Resistant Quantum Computation

ZHANG Jianhang[1,2], CAO Zeyang[1], SONG Xiaofeng[2], XING Lipeng[2]
(1. Air and Missile Defense College, Air Force Engineering University, Xi'an 710051, China;
2. Information and Communication College, National University of Defense Technology, Xi'an 710106, China)

Abstract Aimed at the problems that the homomorphous signature schemes based on the lattice-based theory can resist the quantum computer attacks, however, the existing homomorphous signature schemes based on the standard lattice-based theory are inefficient due to their large key storage and complex structure, failing to be used for the equipment support cloud service, a first anti-quantum computing linear homomorphism authentication scheme for equipment assurance cloud service is designed based on the NTRU. The algorithm generated by the key of the NTRU is utilized for simplifying the system key quantity and avoiding the huge key quantity. And then the linear homomorphism authentication value is produced by using the simple structure of the NTRU lattice preimage sampleable algorithm. The results show that the scheme satisfies the weak context hiding property. And the scheme achieves existential unforgeability against adaptive chosen message under the NTRU-SIS (small integer solution) assumption in the random oracle model. Compared with the current scheme in effect, the new scheme is superior in the key quantity,

收稿日期：2019-09-19
基金项目：国家自然科学基金(61872448)；陕西省自然科学基金(2018JM6017)
作者简介：张建航(1979—)，男，陕西礼泉人，讲师，博士生，主要从事装备作战使用与保障、信息安全研究。E-mail：hzjh2006@126.com

引用格式：张建航，曹泽阳，宋晓峰，等.抗量子计算的装备保障云服务同态认证方案设计[J].空军工程大学学报(自然科学版)，2020，21(2)：106-111. ZHANG Jianhang, CAO Zeyang, SONG Xiaofeng, et al. A Design of Homomorphous Authentication Scheme for Equipment Support Cloud Services with Resistant Quantum Computation[J]. Journal of Air Force Engineering University (Natural Science Edition), 2020, 21(2): 106-111.

the certification cost and the communication cost.

Key words　resistant quantum computation; cloud services; homomorphous authentication; NTRU (Number Theory Research Unit) lattices; preimage Gaussian sampleable algorithm

装备保障信息网络是执行全部装备保障信息功能的网络，是保障信息化建设的重点内容，也是信息化装备保障的核心[1]。随着装备保障信息网络综合保障业务的不断扩展和保障对象的复杂多样化，在装备保障信息网络中建设云服务平台已成为实现高速、可靠装备保障的必然趋势。云服务提供高速便捷、功能多样服务的同时，也面临着诸多的安全威胁与挑战[2-3]。在保障云端数据的隐私性的同时，对云端数据来源与正确性的认证需求也越来越重要。如何保障云端数据的认证性，以及在云端数据进行第三方的外包计算时的可靠性验证，是一个需要解决的新问题。同态认证就是能够实现这样认证功能的关键技术。

Johnson、Molnar、Song 等[4]首次定义了同态认证的概念。随后，出现了诸多基于传统数论困难问题构造的同态认证方案[5-7]。但是，近年来随着量子算法的提出和量子计算机研制的快速发展，基于传统数论问题困难设计的同态认证方案都将面临着潜在的致命威胁[8-9]。基于格理论设计的密码方案是一类能够抗量子计算的密码，其具有线性结构且安全性高的显著优势[10]。Boneh 和 Freeman[11]首次给出了标准格上的线性同态认证方案，并且在文献[12]中给出了多项式同态认证方案。文献[13]在 Boneh 和 Freeman 工作的基础上进行了改进，给出了一个效率更高的线性同态认证方案。但是，这些线性同态方案显著的缺点是运行仍需要大量的存贮资源和计算资源，导致方案的运行过程效率偏低，实际应用价值较低。本文利用 NTRU 格[14]多项式环的结构优势，将 NTRU 密钥生成算法与 NTRU 格上原像高斯抽样算法相结合，设计出了首个面向装备保障云服务的高效线性同态认证方案，简化了系统的密钥量，提高了高斯抽样算法的运行效率，节约了算法运行过程中的计算资源。从理论上证明了新方案满足弱内容隐私性，且在随机预言机模型下，证明了新方案在 NTRU-SIS 问题困难性条件下达到了适应性选择身份和选择消息攻击下的存在性不可伪造性。

1　NTRU 格与高斯抽样

1.1　符号说明

设多项式环 $R=Z[x]/(x^n+1)$，$n=2^\kappa$，$R^\times$ 表示环 R 中可逆的元素组成的集合，环 R 模 q 的环为 $R_q=R/qR$。若 $\boldsymbol{f}=f(x)=\sum_{i=0}^{n-1}f_ix^i$，则下文中记 $\overline{\boldsymbol{f}}=\overline{f}(x)=f_0-\sum_{i=0}^{n-1}f_{n-i}x^i$。

1.2　NTRU 格理论方法

定义 1(格)　设 $\boldsymbol{B}=\{\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m\}\subset\boldsymbol{R}^n$，$\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m$ 为 m 个线性独立的向量，则：

$$\Lambda=\Lambda(\boldsymbol{B})=\{\sum_{i=1}^{m}x_i\boldsymbol{b}_i,x_i\in\mathbf{Z}\}$$

这样的集合 Λ 或 $\Lambda(\boldsymbol{B})$称为格。其中 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m$ 称为格 Λ 的一组基，简称格基。

定义 2(反循环矩阵)　由多项式向量 $\boldsymbol{f}$ 定义的反循环矩阵如下所述：

$$\boldsymbol{A}_n(\boldsymbol{f})=\begin{pmatrix}f_0 & f_1 & \cdots & f_{n-1}\\ -f_{n-1} & f_0 & \cdots & f_{n-2}\\ \vdots & \vdots & & \vdots\\ -f_1 & -f_2 & \cdots & f_0\end{pmatrix}=\begin{pmatrix}(\boldsymbol{f})\\ (x\cdot\boldsymbol{f})\\ \vdots\\ (x^{n-1}\cdot\boldsymbol{f})\end{pmatrix}$$

定义 3(NTRU 格)　设 $n=2^\kappa$，$\kappa\in\mathbf{Z}^+$，素数 $q\geqslant 2$。令多项式 $\boldsymbol{f},\boldsymbol{g}\in R$，$\boldsymbol{f}\in R^\times$，并且 $\boldsymbol{h}=\boldsymbol{g}\cdot\boldsymbol{f}^{-1}\bmod q$，那么由 $\boldsymbol{h}$ 和 q 决定的集合：

$$\Lambda_{\boldsymbol{h},q}=\{(\boldsymbol{u},\boldsymbol{v})\in R^2\mid\boldsymbol{u}+\boldsymbol{v}\cdot\boldsymbol{h}=0\bmod q\}$$

称为 NTRU 格。可知，NTRU 格 $\Lambda_{\boldsymbol{h},q}$是一个维数为 $2n$ 的满秩格。矩阵 $\boldsymbol{A}_{\boldsymbol{h},q}=\begin{pmatrix}-A_n(\boldsymbol{h}) & \boldsymbol{I}_n\\ q\boldsymbol{I}_n & \boldsymbol{O}_n\end{pmatrix}\in\boldsymbol{Z}_q^{2n\times 2n}$ 是 NTRU 格的一个基矩阵。

引理 1[15]令多项式 $\boldsymbol{f},\boldsymbol{g},\boldsymbol{F},\boldsymbol{G}\in R_q$，并且满足 $\boldsymbol{f}\cdot\boldsymbol{G}-\boldsymbol{g}\cdot\boldsymbol{F}=q$，$\boldsymbol{h}=\boldsymbol{g}\cdot\boldsymbol{f}^{-1}\bmod q$，那么，矩阵 $\boldsymbol{B}_{f,g}=\begin{pmatrix}A(\boldsymbol{g}) & -A(\boldsymbol{f})\\ A(\boldsymbol{G}) & -A(\boldsymbol{F})\end{pmatrix}$与矩阵 $\boldsymbol{A}_{\boldsymbol{h},q}$生成的 NTRU 格是相同的。

定义 4(NTRU-SIS 问题)　给定参数 n,m,q，给定多项式向量 $\boldsymbol{h}=\boldsymbol{g}\cdot\boldsymbol{f}^{-1}\bmod q$，则 NTRU-SIS 问题就是寻求 2 个非零的小系数多项式 $\boldsymbol{u},\boldsymbol{v}\in R_q$，$\|\boldsymbol{u}\|,\|\boldsymbol{v}\|\leqslant\beta(n)$并且满足 $\boldsymbol{u}+\boldsymbol{v}\cdot\boldsymbol{h}=0\bmod q$。

1.3　高斯抽样相关理论

定义 5(格中离散高斯分布)　在 m 维向量空间 $\boldsymbol{Z}^m$ 上，令格 $\Lambda\subset\boldsymbol{Z}^m$，给定高斯参数 $\sigma\in\mathbf{R}$ 和任意的 $\boldsymbol{c}\in\boldsymbol{R}^m$，定义 $\rho_{\sigma,\boldsymbol{c}}(x)=\exp(-\pi\frac{\|\boldsymbol{x}-\boldsymbol{c}\|^2}{\sigma^2})$ 和 $\rho_{\sigma,\boldsymbol{c}}(\Lambda)=\sum_{x\in L}\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{x})$，则在格 Λ 中的离散高斯分布定义为：

$$\forall \boldsymbol{y}\in\Lambda, D_{\Lambda,\sigma,c}(\boldsymbol{y})=\frac{\rho_{\sigma,c}(\boldsymbol{y})}{\rho_{\sigma,c}(\Lambda)}$$

其中,如果当 $\boldsymbol{c}=0$ 时,那么我们将 $D_{\Lambda,\sigma,0}$ 简记为 $D_{\Lambda,\sigma}$。

定义 6(原像高斯抽样[16]) 格上的原像高斯抽样分为 2 步计算:

Step1 高斯抽样。对高斯分布 $D_{\Lambda_q^{\perp}(A),\sigma,c}$ 的输入为格基 $\boldsymbol{B}$、高斯分布的标准方差 σ 以及向量 $\boldsymbol{c}\in\mathbf{Z}^n$。先预计算格基 $\boldsymbol{B}$ 的 Gram-Schmidt 正交化后的矩阵 $\tilde{\boldsymbol{B}}$,接着进行如下计算:

1)令 $\boldsymbol{v}_n\leftarrow 0, \boldsymbol{c}_n\leftarrow\boldsymbol{c}$, $i=n,n-1,\cdots,1$

a. 令 $c'_n=(\boldsymbol{c}_i,\tilde{\boldsymbol{b}_i})/(\tilde{\boldsymbol{b}_i},\tilde{\boldsymbol{b}_i})\in\mathbf{R}$,且 $\sigma'_i=\sigma_i/\|\tilde{\boldsymbol{b}_i}\|>0$;

b. 选取 $z\sim D_{\mathbf{Z},\sigma'_i,c'_i}$,$D_{\mathbf{Z},\sigma'_i,c'_i}$ 是整数集合 $\mathbf{Z}$ 上的高斯抽样。

c. 令 $\boldsymbol{c}_{i-1}\leftarrow\boldsymbol{c}_i\leftarrow z_i\boldsymbol{b}_i$,

并令 $\boldsymbol{v}_{i-1}\leftarrow\boldsymbol{v}_i\leftarrow z_i\boldsymbol{b}_i$;

2)输出 v_0。

Step2 原像输出。对任意给定的向量 $\boldsymbol{t}\in\boldsymbol{Z}^m$ 满足 $\boldsymbol{At}=\boldsymbol{u}\bmod q$,运行 STEP1 抽取向量 $-\boldsymbol{t}\in\boldsymbol{Z}^m$ 对应的向量为 $\boldsymbol{v}$,计算 $\boldsymbol{e}=\boldsymbol{t}+\boldsymbol{v}$。则有 $\boldsymbol{Ae}=\boldsymbol{u}\bmod q$,$\boldsymbol{u}$ 的原像是 $\boldsymbol{e}$。我们将原像高斯抽样函数简记为 SamplePre(·),也就是有 $\boldsymbol{e}\leftarrow$SamplePre($\boldsymbol{B},\sigma,\boldsymbol{u}$)。

引理 2[11] 假设 $\Lambda\subseteq\boldsymbol{Z}^n$ 是一个满秩的格,$\sigma\in\mathbf{R}$ 表示高斯分布的标准方差。设 $\boldsymbol{t}_i\in\boldsymbol{Z}^n$ 和 $\boldsymbol{x}_i$ 是 2 个相互线性独立的随机取自高斯分布 $D_{\Lambda+t_i,\sigma}$ 的向量,$i=1,2,\cdots,k$。设 $\boldsymbol{c}=(c_1,c_2,\cdots,c_k)\in\boldsymbol{Z}^k$,同时定义 $g:=\gcd(c_1,c_2,\cdots,c_k)$ 和 $t:=\sum_{i=1}^{k}c_it_i$。假设 $\sigma>\|\boldsymbol{c}\|\cdot\eta_\varepsilon(\Lambda)$,其中 ε 是一个任意小的正常数,$\eta_\varepsilon(\Lambda)$ 表示格 Λ 对应于 ε 的光滑参数。那么,可以得出 $z=\sum_{i=1}^{k}c_ix_i$ 的分布统计接近于高斯分布 $D_{g\Lambda+t,\|\boldsymbol{c}\|\sigma}$。

2 装备保障云服务同态认证方案设计

一个典型的装备保障云服务系统模型一般由 3 个实体构成。一是用户(User)。装备保障信息网络中的用户包括人、计算机、武器装备等,这些用户的大量数据文件存储在云服务器中,通过云服务器进行数据管理和应用;二是云服务器(Cloud Server)。云服务器主要对用户的数据进行管理,为各种用户提供不同需求的数据服务以及计算资源。三是密钥生成器(Key Generator)。密钥生成器用来产生云服务器中数据的认证密钥以及分配给各类用户公钥,即验证密钥。如图 1 所示,在装备保障信息网络同态认证的流程是:①密钥生成器产生系统需要的密钥,将认证私钥发送给云服务器,将公钥发送给不同的用户;②云服务器对存储的一组数据采用线性同态算法进行认证,并且将认证值和数据存储在同一个数据服务器上;③用户从云服务器中下载需要的数据;④用户对该组数据认证值的线性组合进行检查,对存储在云服务器的数据需要进行认证操作。如果通过验证,那么说明下载的数据线性组合是合法的完整的数据,这时用户可以放心使用该组数据,否则验证不通过,则用户认为该组数据不合法,不予接受。

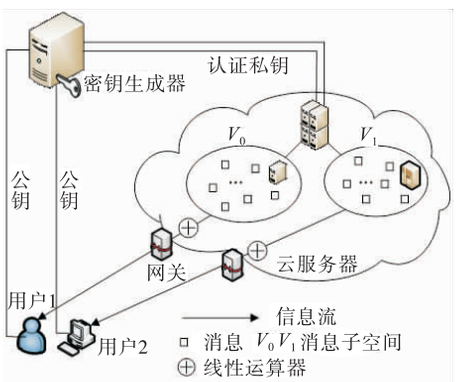

图 1 装备保障云服务同态认证模型

2.1 系统参数设置

给定安全参数 n,$n=2^\kappa$,$\kappa\in\mathbf{Z}^+$,素数 $q\geqslant 2$。令 $L\in\mathbf{Z}^+$ 是线性联合认证的最大个数。线性同态认证的深度为 $e\leqslant L$。设定高斯分布函数为 $D_{\Lambda,\sigma}$,$\sigma\geqslant\max\{\sqrt{n\ln(8nq)}\cdot q^{1/2+\varepsilon},\omega[(n\ln n)3/2]\}$。设定一个抗碰撞的哈希函数,$H:\{0,1\}^*\rightarrow\boldsymbol{Z}_q^n$。设定一个系数属于 $F_2=\{0,1\}$ 的线性函数 LF,也就是为 $LF(\boldsymbol{v}_1,\boldsymbol{v}_2,\cdots,\boldsymbol{v}_\ell)=\sum_{i=1}^{\ell}\alpha_i\boldsymbol{v}_i$,其中系数 $\alpha_i\in F_2=\{0,1\}$。

2.2 系统密钥生成

输入参数 $n,q,\sigma=1.17\sqrt{q/(2n)}$。系统密钥生成算法如表 1 所示。利用 NTRU 密钥生成算法,输出系统公钥 $\boldsymbol{h}=\boldsymbol{f}^{-1}\cdot g\bmod q$,系统私钥为矩阵 $\boldsymbol{B}\in\boldsymbol{Z}_q^{2n\times 2n}$,其中 $\boldsymbol{B}=\begin{pmatrix}A(\boldsymbol{g}) & -A(\boldsymbol{f})\\ A(\boldsymbol{g}') & -A(\boldsymbol{f}')\end{pmatrix}$。

表 1 系统密钥生成算法

输入 n,q,σ	输出:$mpk=\boldsymbol{h}$,$msk=\boldsymbol{B}\in\boldsymbol{Z}_q^{2n\times n}$
1)从高斯分布 D_σ^n 中随机抽取小系数多项式 $\boldsymbol{f},\boldsymbol{g}$;	
2)计算 Norm $\leftarrow\max(\|(\boldsymbol{g},\boldsymbol{f})\|,\|(\frac{q\bar{\boldsymbol{f}}}{\boldsymbol{f}\cdot\bar{\boldsymbol{f}}+\boldsymbol{g}\cdot\boldsymbol{g}},\frac{q\bar{\boldsymbol{g}}}{\boldsymbol{f}\cdot\bar{\boldsymbol{f}}+\boldsymbol{g}\cdot\boldsymbol{g}})\|)$;	
3)如果 Norm$>1.17\sqrt{q}$,那么返回 1);	

续表

输入 n,q,σ　　输出：$mpk=\boldsymbol{h},msk=\boldsymbol{B}\in\boldsymbol{Z}_q^{2n\times n}$
4）利用扩展欧几里得算法，计算 $\rho_f,\rho_g\in R$ 和 $r_f,r_g\in\mathbf{Z}$ 且满足以下条件： $-\rho_f\cdot\boldsymbol{f}=r_f \bmod (x^n+1)$ $-\rho_g\cdot\boldsymbol{g}=r_g \bmod (x^n+1)$
5）如果 $\gcd(r_f,r_g)\neq1$，或者 $\gcd(r_f,q)\neq1$，那么返回步骤 1）；
6）利用扩展欧几里得算法，计算 $u,v\in\mathbf{Z}$ 且满足条件 $u\cdot r_f+v\cdot r_g=1$；
7）计算 $\boldsymbol{f}'\leftarrow qv\rho_g,\boldsymbol{g}'\leftarrow -qu\rho_f$；
8）对 $\dfrac{\boldsymbol{f}'\cdot\overline{\boldsymbol{f}}+\boldsymbol{g}'\cdot\overline{\boldsymbol{g}}}{\boldsymbol{f}\cdot\overline{\boldsymbol{f}}+\boldsymbol{g}\cdot\overline{\boldsymbol{g}}}$ 进行截取最近整数运算，并将截取的结果记为 $k\in\mathbf{Z}$；
9）提取多项式 $\boldsymbol{f}',\boldsymbol{g}'$：$\boldsymbol{f}'\leftarrow\boldsymbol{f}'-k\cdot\boldsymbol{f},\boldsymbol{g}'\leftarrow\boldsymbol{g}'-k\cdot\boldsymbol{g}$；
10）计算 $h\leftarrow\boldsymbol{f}^{-1}\cdot\boldsymbol{g} \bmod q,B\leftarrow\begin{pmatrix}A(\boldsymbol{g}) & -A(\boldsymbol{f})\\ A(\boldsymbol{g}') & -A(\boldsymbol{f}')\end{pmatrix}$

2.3　同态认证过程

同态认证算法如表 2 所示。输入系统的参数 $n,q,\sigma,i,\boldsymbol{h},\boldsymbol{B},\alpha_i$，消息子空间的标签 $\tau\in\{0,1\}^n$，消息子空间 $\boldsymbol{V}=(\boldsymbol{v}_1,\boldsymbol{v}_2,\cdots,\boldsymbol{v}_\ell)$。输出联合认证值为 $\boldsymbol{e}\leftarrow\sum_{j=1}^{\ell}\alpha_j\boldsymbol{e}_j$，$\boldsymbol{e}_j=(\boldsymbol{e}'_j,\boldsymbol{e}''_j)\in\boldsymbol{Z}_q^{2n}$，并且满足条件 $\boldsymbol{e}'_j+\boldsymbol{e}''_j\cdot\boldsymbol{h}=\boldsymbol{h}_j$。

表 2　同态认证算法

输入 $n,q,\sigma,\tau,i,\ell,\boldsymbol{v},\boldsymbol{h},\boldsymbol{B},\alpha$　　输出：$\boldsymbol{e}_j,\boldsymbol{e}=\sum_{i=1}^{\ell}\alpha_j\boldsymbol{e}_j$
1）计算哈希函数 $\alpha_i\leftarrow H(\tau\|i),i\leqslant n$；
2）计算向量内积 $\boldsymbol{h}_{ij}\leftarrow<\alpha_i,\boldsymbol{v}_j>,j=1,2,\cdots,n$；
3）计算消息认证值 $\boldsymbol{e}_j=(\boldsymbol{e}'_j,\boldsymbol{e}''_j)\leftarrow\mathrm{SamplePre}(B,\sigma(\boldsymbol{h}_j,0)),j=1,2,\cdots\ell$；
4）提取消息子空间 $V_\tau(\upsilon_1,\upsilon_2,\cdots,\upsilon_\ell)$；
5）联合同态认证值 $\boldsymbol{e}\leftarrow\sum_{j=1}^{\ell}\alpha_j\boldsymbol{e}_j,j=1,2,\cdots,\ell$。

2.4　认证验证阶段

输入系统的安全参数 PP，消息子空间标签 $\tau\in\{0,1\}^n$，以及向量 $\boldsymbol{v}$ 对应的认证 $\boldsymbol{e}$ 以及线性函数 LF。接着，进行运行哈希函数 $\boldsymbol{a}_i\leftarrow H(\tau\|i)$，得 $\boldsymbol{a}_i\in\boldsymbol{Z}_q^n,i\leqslant n$。然后，计算向量 $\boldsymbol{a}_i$ 和向量 $\boldsymbol{v}_j$ 的内积 $\boldsymbol{h}_{ij}=<\boldsymbol{a}_i,\boldsymbol{v}_j>(\bmod q),i,j=1,2,\cdots,n$，记 $\boldsymbol{h}_j=(h_{j1},h_{j2},\cdots,h_{jn})^{\mathrm{T}}$，于是，当且仅当满足以下两条：

1）$\|\boldsymbol{e}_j\|\leqslant2\sigma\sqrt{n}$；

2）$\boldsymbol{e}'_j+\boldsymbol{e}''_j\cdot\boldsymbol{h}=\boldsymbol{h}_j \bmod q$。

则接受该认证值。

2.5　方案正确性证明

定理 1　本方案在给定的系统参数下，经过同态认证过程产生的认证值能够通过认证验证算法。

证明：一方面，哈希函数 $H:\{0,1\}^*\rightarrow\{0,1\}^n$ 是任意的比特串映射到长度为 n 的比特串，计算向量的内积 $h_{ij}=<\boldsymbol{a}_i,\boldsymbol{v}_j>(\bmod q)$，因为此哈希函数族满足加法和数乘同态性质，由原像高斯抽样算法可知，$\boldsymbol{e}_j$ 是向量 $\boldsymbol{h}_j$ 的原像抽样值，$\boldsymbol{e}'_j+\boldsymbol{e}''_j\cdot\boldsymbol{h}=\boldsymbol{h}_j \bmod q$，并且 $\|\boldsymbol{e}_j\|=\|(\boldsymbol{e}'_j,\boldsymbol{e}''_j)\|\leqslant\|\boldsymbol{e}'_j\|+\|\boldsymbol{e}''_j\|\leqslant2\sigma\sqrt{n}$。对于线性联合认证算法中输入系统公共参数 PP，消息子空间标签 $\tau\in\{0,1\}^n$，向量 $\boldsymbol{V}=(\boldsymbol{v}_1,\boldsymbol{v}_2,\cdots,\boldsymbol{v}_\ell)$ 对应的认证 $E=(e_1,e_2,\cdots,e_\ell)$ 以及线性函数 LF，则 $\sum_{i=1}^{\ell}\alpha_i\boldsymbol{v}_i$ 的线性联合认证为 $\sum_{i=1}^{\ell}\alpha_i\boldsymbol{e}_i$。因为 $\ell\leqslant L,\alpha_i\in F_2$，所以 $\|\sum_{i=1}^{\ell}\alpha_i\boldsymbol{e}_i\|\leqslant\sum_{i=1}^{\ell}\alpha_i\|\boldsymbol{e}_i\|\leqslant2L\sigma\sqrt{n}$ 成立。

另一方面，设线性联合认证值的输出为 $\sum_{i=1}^{\ell}\alpha_i\boldsymbol{e}_i=\sum_{i=1}^{\ell}\alpha_i(\boldsymbol{e}'_i,\boldsymbol{e}''_i),\alpha_i\in F_2$，其中 $\boldsymbol{e}_i=(\boldsymbol{e}'_i,\boldsymbol{e}''_i)$。因此，由于 $\boldsymbol{e}'_j+\boldsymbol{e}''_j\cdot\boldsymbol{h}=\boldsymbol{h}_j \bmod q,j=1,2,\cdots,\ell$，故而 $\sum_{j=1}^{\ell}\alpha_j(\boldsymbol{e}'_j+\boldsymbol{e}''_j\cdot\boldsymbol{h})=\sum_{j=1}^{\ell}\alpha_j\boldsymbol{e}'_j+\sum_{j=1}^{\ell}\alpha_j\boldsymbol{e}''_j\cdot\boldsymbol{h}$ 成立。也就是说，$\sum_{i=1}^{\ell}\alpha_i\boldsymbol{v}_i$ 的线性联合认证为 $\sum_{i=1}^{\ell}\alpha_i\boldsymbol{e}_i$。

3　方案的安全性证明与效率分析

3.1　弱内容隐私性

定理 2　本文所构造的新方案满足弱内容隐私性。

证明：不妨假设攻击者输出 2 个相互独立的 $\boldsymbol{V}_0$，$\boldsymbol{V}_1$ 以及线性函数 $LF_1,LF_2,\cdots,LF_s$，其中 $\boldsymbol{V}_b=(\boldsymbol{v}_1^{(b)},\boldsymbol{v}_2^{(b)},\cdots,\boldsymbol{v}_k^{(b)}),b=0,1$。$j=1,2,\cdots,k$，令 $\boldsymbol{e}_j^{(b)}$ 表示基向量 $\boldsymbol{V}_0,\boldsymbol{V}_1$ 的认证。根据原像高斯抽样算法可知，$\boldsymbol{e}_j^{(b)}$ 是统计近似服从高斯分布的。对挑战者随机选择一个比特 $b\in F_2$，令 $\boldsymbol{e}^{(b)}$ 为线性联合认证算法的输出 $\boldsymbol{e}_j^{(b)}$。

假设 $b=0$，$\boldsymbol{e}^{(0)}$ 是线性联合算法 $\boldsymbol{e}_j^{(b)}$ 是 $LF_i,i=1,2,\cdots,s$ 下的一个线性组合。由于 $\boldsymbol{e}^{(0)}{}_j\sim D_{\Lambda,\sigma}$，根据**引理 2**，从而 $\boldsymbol{e}^{(0)}\sim D_{\Lambda,\sigma,LF(V_0),LF}$。同样，假设 $b=1$，可知 $\boldsymbol{e}^{(1)}\sim D_{\Lambda,\sigma,LF(V_1),LF}$。又当 $i=1,2,\cdots,s$ 时，线性函数 $LF_i(\boldsymbol{V}_0)=LF_i(\boldsymbol{V}_1)$。于是，$\boldsymbol{e}^{(0)}$ 和 $\boldsymbol{e}^{(1)}$ 服从的高斯分布是统计接近的。也就是说，攻击者理论上无法判断出联合认证 $\boldsymbol{e}^{(0)}$ 或 $\boldsymbol{e}^{(1)}$ 是从哪个消息子空间 $\boldsymbol{V}_0$ 或 $\boldsymbol{V}_1$ 的认证联合而来的。因此，该方案满足弱内容隐私性。

3.2　存在性不可伪造性

定理 3　在 NTRU-SIS 问题困难性假设下，本文构造的方案在随机预言机模型下满足适应性选择

消息的存在性不可伪造性。

证明:对于任何一个具有多项式时间攻击能力的攻击者 A,它与挑战者 C 进行交互式游戏的过程设计具体如下:

1)系统建立:输入安全参数 n,挑战者 C 生成系统公共参数 PP,运行密钥生成算法产生系统公钥和认证私钥,然后挑战者 C 将系统公共参数 PP 发送给攻击者 A。

2)询问阶段:任意的攻击者 A 适应性地进行如下哈希询问和认证询问:

a. 询问哈希函数 H:攻击者适应性地选择消息子空间标签 τ_i 进行询问。挑战者首先查看形式为 $(\tau_i,\{\boldsymbol{a}_j,\boldsymbol{h}_{ij}\}_{j=1}^{n})$ 的列表 $L_1=(\tau_i,\{\boldsymbol{a}_j,\boldsymbol{h}_{ij}\}_{j=1}^{n})$,若列表中存在对应的哈希值 $\boldsymbol{a}_j$,$j=1,2,\cdots,n$,则将此结果返回给攻击者。否则,挑战者随机地选择服从高斯分布 D_{σ}^{2n} 的向量 $\boldsymbol{h}_{ij}=(\boldsymbol{h}'_{ij},\boldsymbol{h}''_{ij})$,$j=1,2,\cdots,n$,且 $\|\boldsymbol{h}_{ij}\|\leqslant 2\sigma\sqrt{n}$,$\boldsymbol{h}'_{ij},\boldsymbol{h}''_{ij}\in\boldsymbol{Z}_q^n$。然后,挑战者进行计算 $\boldsymbol{h}'_{ij}+\boldsymbol{h}''_{ij}\cdot\boldsymbol{h}=\boldsymbol{a}_j$,$j=1,2,\cdots,n$,最后挑战者将模拟的结果 $\boldsymbol{a}_j$,$j=1,2,\cdots,n$ 返回给攻击者,并将此询问的记录添加到列表 L_1 里。注意到,在攻击者进行哈希函数 H 的询问时,由于向量 $\boldsymbol{h}_{ij}$,$j=1,2,\cdots,n$ 是随机地选取自高斯参数 σ 大于光滑参数 σ 的高斯分布 D_{σ}^{2n},从而 $\boldsymbol{h}'_{ij}+\boldsymbol{h}''_{ij}\cdot\boldsymbol{h}=a_j(\mathrm{mod}\ q)$ 的分布是统计接近于均匀分布。因此,挑战者能够以压倒性的概率成功模拟随机预言机 H。

b. 认证询问:攻击者 A 对挑战者发起消息子空间 $\boldsymbol{V}_i$ 的一个新的基向量组 $\boldsymbol{v}_{i1},\boldsymbol{v}_{i2},\cdots,\boldsymbol{v}_{ik}$ 的签名询问时,挑战者先在形如 $(\tau_i,\boldsymbol{v}_i,\boldsymbol{e}_{ij})$,$i=1,2,\cdots,n$,$j=1,2,\cdots,k$ 的列表 $L_2=(\tau_i,\boldsymbol{v}_i,\boldsymbol{e}_{ij})$ 中进行查询,如果此列表中存在对应的认证 $\boldsymbol{e}_{ij}$,$j=1,2,\cdots,k$,则挑战者将此结果直接返回给攻击者。否则,挑战者从列表 L_1 中选取 $\boldsymbol{V}_i$ 对应的标签 τ_i。挑战者得到列表 L_1 中的存储记录 $(\tau_i,\{\boldsymbol{a}_j,\boldsymbol{h}_{ij}\}_{j=1}^{k})$。设矩阵第 j 列是向量 $\boldsymbol{h}_{ij}=(\boldsymbol{h}'_{ij},\boldsymbol{h}''_{ij})$,$j=1,2,\cdots,k$,$\boldsymbol{h}'_{ij},\boldsymbol{h}''_{ij}\in\boldsymbol{Z}_q^n$,的矩阵为 $\boldsymbol{H}\in\boldsymbol{Z}_q^{2n\times n}$。接下来,挑战者进行计算 $\boldsymbol{e}_{ij}=(\boldsymbol{e}'_{ij},\boldsymbol{e}''_{ij})\leftarrow\boldsymbol{H}\boldsymbol{v}_{ij}$,并发送 e_{ij} 给攻击者作为线性同态认证的值。最后,挑战者将该次询问记录存储在列表 L_2 中。

3)伪造阶段:攻击者 A 可以进行任意多次上述的哈希询问以及认证询问,直到自己认为询问满意为止。然后攻击者 A 利用已掌握的知识进行伪造出一个新的标签 $\tau^*\in\{0,1\}^n$ 以及消息 $\boldsymbol{v}_{ij}^*$ 的认证值 $\boldsymbol{e}_{ij}^*$。以下对攻击者的攻击情况分为 2 种攻击类型进行具体讨论:

a. 假设攻击是 Type1 类型:即对所有的 i,有 $\tau^*\neq\tau_i$,也就是所有消息子空间的标签 τ_i 从没有被进行认证询问过。这时,挑战者进行检查列表 L_1,找到标签 $\tau^*\neq\tau_i$ 和对应的 $(\tau_i^*,\{\boldsymbol{a}_j^*,\boldsymbol{h}_{ij}^*\}_{j=1}^{k})$。设 $\boldsymbol{h}'^*_{ij},\boldsymbol{h}''^*_{ij}\in\boldsymbol{Z}_q^n,\boldsymbol{h}_{ij}^*=(\boldsymbol{h}'^*_{ij},\boldsymbol{h}''^*_{ij})$,$j=1,2,\cdots,k$ 是矩阵 $\boldsymbol{H}^*\in\boldsymbol{Z}_q^{2n\times n}$ 的第 j 列,则 $\boldsymbol{H}^*\boldsymbol{v}_{ij}^*$ 是消息 $\boldsymbol{v}_{ij}^*$ 的认证值,也就是得到 $\boldsymbol{e}_{ij}^*=(\boldsymbol{e}'^*_{ij},\boldsymbol{e}''^*_{ij})\leftarrow\boldsymbol{H}^*\boldsymbol{v}_{ij}^*$。从而有,$\boldsymbol{e}'^*_{ij}+\boldsymbol{e}''^*_{ij}*\boldsymbol{h}=\boldsymbol{h}_{ij}^*\ \mathrm{mod}\ q$,由一般分叉引理[17],从而有 $(\boldsymbol{e}'_{ij}-\boldsymbol{e}'^*_{ij})+(\boldsymbol{e}''_{ij}-\boldsymbol{e}''^*_{ij})\cdot\boldsymbol{h}=0\ \mathrm{mod}\ q$ 成立。由于 $\|\boldsymbol{e}'_{ij}\|\leqslant\sigma\sqrt{n}$,$\|\boldsymbol{e}''_{ij}\|\leqslant\sigma\sqrt{n}$,并且 $\|\boldsymbol{e}'^*_{ij}\|\leqslant\sigma\sqrt{n}$,$\|\boldsymbol{e}''^*_{ij}\|\leqslant\sigma\sqrt{n}$。从而,可知 $\|\boldsymbol{e}'_{ij}-\boldsymbol{e}'^*_{ij}\|\leqslant\sigma\sqrt{n}$,并且 $\|\boldsymbol{e}''_{ij}-\boldsymbol{e}''^*_{ij}\|\leqslant\sigma\sqrt{n}$。当 $\boldsymbol{e}'_{ij}-\boldsymbol{e}'^*_{ij}\neq 0$,$\boldsymbol{e}''_{ij}-\boldsymbol{e}''^*_{ij}\neq 0$ 成立时,即得到 NTRU-SIS 问题的一个非零小整数解,这与 NTRU-SIS 问题困难性假设相矛盾。

b. 假设攻击是 Type2 类型:即存在某个或多个 i,使得 $\tau^*=\tau_i$ 成立,但是 $\boldsymbol{v}_{ij}^*\notin V_i$,也就是存在某个消息子空间的标签 τ_i 被认证询问过,但是消息 $\boldsymbol{v}_{ij}^*$ 不在该标签对应的消息子空间里。挑战者在列表 L_1 中找到标签 $\tau^*\neq\tau_i$ 和对应的 $(\tau_i^*,\{\boldsymbol{a}_j^*,\boldsymbol{h}_{ij}^*\}_{j=1}^{k})$,同时在列表 L_2 中找到 $\boldsymbol{h}_{ij},\boldsymbol{h}_{ij}^*$ 是矩阵 $\boldsymbol{H}^*\in\boldsymbol{Z}_q^{2n\times n}$ 的第 j 列,有 $\boldsymbol{e}'^*_{ij}+\boldsymbol{e}''^*_{ij}\cdot\boldsymbol{h}=\boldsymbol{h}_{ij}^*\ \mathrm{mod}\ q$,同情形 a 的讨论相似,此时由一般分叉引理[17],从而可得 $(\boldsymbol{e}'_{ij}-\boldsymbol{e}'^*_{ij})+(\boldsymbol{e}''_{ij}-\boldsymbol{e}''^*_{ij})\cdot\boldsymbol{h}=0\ \mathrm{mod}\ q$ 成立。由于 $\|\boldsymbol{e}'_{ij}\|\leqslant\sigma\sqrt{n}$,$\|\boldsymbol{e}''_{ij}\|\leqslant\sigma\sqrt{n}$,并且 $\|\boldsymbol{e}'^*_{ij}\|\leqslant\sigma\sqrt{n}$,$\|\boldsymbol{e}''^*_{ij}\|\leqslant\sigma\sqrt{n}$。从而,可知 $\|\boldsymbol{e}'_{ij}-\boldsymbol{e}'^*_{ij}\|\leqslant\sigma\sqrt{n}$,并且 $\|\boldsymbol{e}''_{ij}-\boldsymbol{e}''^*_{ij}\|\leqslant\sigma\sqrt{n}$。当 $\boldsymbol{e}'_{ij}-\boldsymbol{e}'^*_{ij}\neq 0$,$\boldsymbol{e}''_{ij}-\boldsymbol{e}''^*_{ij}\neq 0$ 成立时,同样也可得到 NTRU-SIS 问题的一个非零小整数解,这同样与 NTRU-SIS 问题困难性假设相矛盾。

综上所述,在 NTRU-SIS 问题困难性条件下,该方案在随机预言机模型下满足适应性选择消息的存在性不可伪造性。

3.3 效率的分析与比较

从表 3 数据可知,在空间复杂性方面,本文方案在认证密钥、认证值和通信代价的比较时都是最优的。在计算复杂度方面,由于与原像高斯抽样算法的计算开销而言,认证算法运行过程中的哈希函数、随机数选取、向量内积等运算量可以忽略不计,因此仅考虑算法中原像高斯抽样函数。以 1SamplePre(·)表示认证算法运行过程中包含 1 个原像高斯抽样函数子算法。事实上,原像高斯抽样算法运行速度的主要取决于输入的陷门基 $\boldsymbol{B}$ 经过 Gram-Schmidt 正交化后得到的矩阵范数 $\|\widetilde{B}\|$ 的计算复杂性。在文献[11]和[13]中,求解 $\|\widetilde{B}\|$ 的计算复杂度为 $O(n^3)$,而 NTRU 格的陷门基 $\|\widetilde{B}\|$ 的计算复杂度为 $O(n\log n)$,因此在 NTRU 格上运行原像高斯抽样 $1\mathrm{SamplePre}(\cdot)_{\mathrm{NTRU}}$ 的实际运行效率要比

1SamplePre(·)快速的多。综上所述，该方案在空间效率和计算效率方面均具有比较优势。

表 3　与已有抗量子同态认证方案效率的比较

	公钥尺寸	认证密钥	认证值	认证代价	通信代价
文献[11]	$mn\log 2q$	$4m^2\log 2q$	$2m\log q$	2SamplePre(·)	$2m+2m\log+n$
文献[13]	$mn\log q$	$m^2\log q$	$m\log q$	1SamplePre(·)	$m\log q+n$
本文方案	$n\log q$	$4n^2\log q$	$2n\log q$	1Samplepre(·)$_{NTRU}$	$2n\log q+n$

4　结语

为解决装备保障云服务中抗量子计算的安全认证问题，结合 NTRU 格简洁的几何结构，提出了一种基于 NTRU 格快速的面向计算资源和存储资源严重受限的装备保障信息网络的线性同态认证方案。从理论上证明了新方案的正确性和安全性，并对方案的运行效率进行了比较分析。这对于云计算环境下实现高效的装备保障信息网络同态认证具有重要的理论意义和应用价值。如何在标准模型下设计基于 NTRU 格的(分层)线性同态认证方案，将是下一步深入研究的内容。

参考文献

[1] 杨学强，黄俊. 装备保障信息化建设概论[M]. 北京：国防工业出版社，2011：145-147.

[2] 李顺东，窦家维，王道顺. 同态加密算法及其在云安全中的应用[J]. 计算机研究与发展，2015，52(6)：1378-1388.

[3] 张玉清，王晓菲，刘雪峰，等. 云计算环境安全综述[J]. 软件学报，2016，27(6)：1328-1348.

[4] JOHNSON R，MOLNAR D，SONG D X. et al. Homomorphic Signature Schemes[C]// The Cryptographers' Track at the RSA Conference 2002. San Jose，CA，USA：CT-RSA，2002：244-262.

[5] BONEH D，FREEMAN D M，KATZ J，et al. Signing a Linear Subspace：Signature Schemes for Network Coding[C]//The 12th International Conference on Practice and Theory in Public Key Cryptography. Irvine，CA，USA：PKC，2009：68-87.

[6] CHARLES D，JAIN K，LAUTER K. Signatures for Network Coding[J]. International Journal of Information and Coding Theory，2009，1(1)：3-14.

[7] GENNARO R，KATZ J，RABIN T. Secure Network Coding over the Integers[C]//The 13th International Conference on Practice and Theory in Public Key Cryptography. Paris，France：PKC，2010：142-160.

[8] GROVER L K. Quantum Mechanics Helps in Searching for a Needle in a Haystack[J]. Physical Review Letters，1997，79(2)：325-328.

[9] SHOR P W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer[J]. SIAM Journal on Computing，1997，26(5)：1484-1509.

[10] PEIKERT C. A Decade of Lattice Cryptography[J]. Foundations and Trends in Theoretical Computer Science，2016，10(4)：283-424.

[11] BONEH D，FREEMAN D M. Linearly Homomorphic Signatures over Binary Fields and New Tools for Lattice-Based Signatures[C]//The 14th International Conference on Practice and Theory in Public Key Cryptography. Taormina，Italy：PKC，2011：1-16.

[12] BONEH D，FREEMAN D. M. Homomorphic Signatures for Polynomial Functions[C]//The 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Tallinn，Estonia：EUROCRYPT，2011：149-168.

[13] WANG F H，HU Y P，WANG B C. Lattice-Based Linearly Homomorphic Signature Scheme over Binary Field[J]. Science China Information Science，2013，56：1-9.

[14] HOFFSTEUN J，PIPHER J，SILVERMAN J H. NTRU：A Ring-Based Public Key Cryptosystem[C]// Third International Symposiun，ANTS-III. Portland，Oregon，USA：ANTS，1998：267-288.

[15] DUCAS L，LYUBASHEVSKY V，PREST T. Efficient Identity-Based Encryption over NTRU Lattice[C]//The 20th International Conference on the Theory and Application of Cryptology and Information Security. Kaoshiung，Taiwan，China：[s. n.]，2014：22-41.

[16] GENTRY C，PEIKERT C，VAIKUNTANATHAN V. Trapdoors for Hard Lattices and New Cryptographic Constructions[C]// Proceedings of the Fortieth Annual ACM symposium on Theory of Computing. New York，NY，USA：ACM，2008：197-206.

[17] BELLARE M，NEVEN G. Multi-Signatures in the Plain Public-Key Model and a General Forking Lemma[C]//Proceedings of the 13th ACM Conference on Computer and Communications Security. New York，NY，USA：ACM，2006：390-399.

（编辑：徐楠楠）