doi:10.3969/j.issn.1000-436x.2014.02.015

利用容错学习问题构造基于身份的全同态加密体制

光焱[1,2]，祝跃飞[1]，费金龙[1,2]，顾纯祥[1,2]，郑永辉[1,2]
(1. 解放军信息工程大学 四院，河南 郑州 450002；2. 解放军信息工程大学 数学工程与先进计算国家重点实验室，河南 郑州 450002)

摘 要：基于容错学习问题构造的一类全同态加密体制在云计算安全领域具有重要的潜在应用价值，但同时普遍存在着公钥尺寸较大的缺陷，严重影响其身份认证与密钥管理的效率。将基于身份加密的思想与基于容错学习问题的全同态加密相结合，提出一种基于身份的全同态加密体制，能够有效克服公钥尺寸对于全同态加密应用效率的影响。在随机喻示模型下，体制的安全性归约到容错学习问题难解性和陷门单向函数单向性，并包含严格的安全性证明。

关键词：LWE 问题；全同态加密；基于身份加密；随机喻示模型
中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2014)02-0111-07

Identity-based fully homomorphic encryption from learning with error problem

GUANG Yan[1,2], ZHU Yue-fei[1], FEI Jin-long[1,2], GU Chun-xiang[1,2], ZHENG Yong-hui[1,2]
(1. Fourth Institute, PLA Information Engineering University, Zhengzhou 450002, China; 2. State Key Laboratory of Mathematical Engineering and Advanced Computing, PLA Information Engineering University, Zhengzhou 450002, China)

Abstract: The fully homomorphic encryption schemes based on learning with errors problem own a great potential value in the cloud computing security. However, the existing schemes share a common flaw of large sized public keys, which may cause inefficiency of such schemes in the key and identity management. An identity-based fully homomorphic encryption scheme was presented. The scheme compromises the merits of both identity-based and fully homomorphic encryption schemes, and it overcomes the above mentioned flaw. The security of the proposed scheme reduces to the hardness of learning with errors problem and the one-wayness of trapdoor function in the random oracle model.

Key words: learning with error problem; fully homomorphic encryption; identity-based encryption; random oracle model

1 引言

容错学习（LWE, learning with error）问题是机器学习领域的困难问题，O. Regev[1]在 2005 年首次提出该问题，并将其难度归约到格上最短向量问题（SVP, shortest vector problem）的最坏情况难解性。基于 LWE 问题设计的公钥加密体制[1,2]继承了格上密码体制的优势，拥有较高的渐近效率、简单的计算形式，并且能够抵抗量子攻击。

全同态加密是 2012 年来广受关注的一种新型加密体制，除了具备普通公钥加密体制的功能之外，全同态加密能够在不解密的前提下，实现针对密文的运算。基于全同态加密的特殊能力，能够实现密文检索、安全多方计算等多种新型技术，从而为当前云计算发展中日益凸显的数据安全以及隐私保护等问题提供了一条可行的解决之道。2009 年，IBM 公司研究员 C. Centry[3]基于理想格（ideal lattice）上的最短向量问题（SVP, shortest vector problem），构造出第一个真正意义上的全同态加密体制，此后，具备相似功能的密码体制的设计与分

收稿日期：2012-11-01；**修回日期**：2013-03-07
基金项目：国家自然科学基金资助项目（61072047）；河南省科技攻关计划基金资助项目（112102210007）；郑州市科技创新团队基金资助项目（10CXTD150）
Foundation Items：The National Natural Science Foundation of China (61072047); The Key Scientific and Technological Project of Henan Province (112102210007); The Municipal Science and Technology Innovation Team Project of Zhengzhou (10CXTD150)

析成为密码学领域一个新的研究热点[4~7]。

2011 年，Z. Brakerski 和 V. Vaikuntanathan[8]首次提出基于 LWE 问题的全同态加密体制，在 Regev 体制[1]的基础上，利用“重线性化”技术实现密文域上的全同态运算能力。由于 LWE 问题的难度规约不依赖于理想格的特殊结构，因此该体制拥有比 Gentry 体制更可靠的安全性保证。然而，由于重线性化过程需要借助一组额外的运算公钥（evaluation key），且尺寸与密文乘法的次数成正比，因此，在完成较复杂的密文运算时，公钥尺寸将成为该体制的一个严重缺陷。虽然在此后的研究中，该体制的计算效率得到了更进一步的优化[9~11]，但对于其公钥尺寸大的问题，目前仍无十分有效的解决方案。

作为公钥加密体制，全同态加密在安全多方计算等云计算应用中需要考虑身份认证的问题，有效的方法是使用公钥证书。公钥证书由可信的证书中心负责签发，包含身份—公钥对以及公钥有效期等信息。证书的引入有效解决了公钥所属身份的认证问题，但同时，由于证书中心的存在，不可避免地给整个密码系统带来计算、存储、通信与管理等方面的额外开销。在全同态加密应用领域，这一问题受到较大尺寸公钥的影响，显得尤为突出。

基于身份加密[12]是一种无须使用公钥证书进行身份认证的密码系统。系统中的每个用户拥有唯一的公开身份信息，用户公钥根据该信息直接计算得出，因此无须认证；用户私钥由第三方私钥生成中心（KGC, key generation center）利用其掌握的系统主密钥（master key）生成，并安全地传递给用户。基于身份加密无须考虑与证书有关的开销，因此能够克服公钥尺寸对密码体制实际应用效率的影响。迄今为止，该领域的研究已经取得较多成果[13]，但现有基于身份加密体制均不具备密文域上同态运算的能力。

本文在前人工作基础上，提出基于身份全同态加密体制的模型，融合了基于身份加密和全同态加密的功能，并采用选择明文和选择身份攻击下不可区分性（IND-ID-CPA）作为安全性定义。在体制设计方面，本文将重线性化技术应用于 Regev 体制的对偶算法，实现密文域上的同态运算；设计与全同态加密相配套的私钥提取算法，涵盖密文运算所需的运算公钥。文章给出了新体制在随机喻示模型下的严格安全性证明，将其安全性归约到 LWE 问题难解性和前像可采样陷门单向函数的单向性上。

2 基础知识

2.1 符号说明

向量在本文中用粗体小写字母表示，如 $\boldsymbol{e}$；其第 i 个分量用 $\boldsymbol{e}[i]$表示；所有向量均被默认具有列向量的形式，其转置表示为 $\boldsymbol{e}^{\mathrm{T}}$；矩阵用粗体大写字母表示，如 $\boldsymbol{A}^{m\times n}$；对于一个向量集合 S，定义其长度为其中所有向量欧几里得范数的最大值，并将其记做 $\|S\|$。

设 D 为任意一个概率分布，$x\xleftarrow{R}D$ 表示从中随机选取一个变量 x；对于集合 S，$x\xleftarrow{D}S$ 则表示从中依分布 D 选取一个元素 x。在同一个集合 S 上的 2 个概率分布 X 和 Y 之间，可以计算“统计距离”，表达式为 $\frac{1}{2}\sum_{s\in S}|X(s)-Y(s)|$。假设集合 S 中包含的元素个数为 n，而 2 个概率分布间的统计距离是 n 的可忽略函数，则称 X 和 Y 是“概率不可区分”的。

2.2 LWE 问题

在提出 LWE 问题的同时，O. Regev 给出了该问题到格上 SVP 问题的一个量子归约（即归约过程中假设量子算法的存在）。2009 年，C. Peikert[14]针对同一问题给出了新的归约，使其不再依赖量子算法。

在给出 LWE 问题的定义之前，首先介绍几个与之相关的概率分布：1）格 Λ 上以格点 $\boldsymbol{c}$ 为中心，标准差为 $r/\sqrt{2\pi}$ 的离散正态分布，记为 $D_{\Lambda,r,\boldsymbol{c}}$，当 $\boldsymbol{c}=0$ 时，简记为 $D_{\Lambda,r}$；2）将 Z_q 上的离散正态分布 0 为中心，标准差 $r/\sqrt{2\pi}$ 的离散正态分布称为“错误分布”，记做 χ；3）取定正整数 n，对于 Z_q^n 上的 n 维向量 $\boldsymbol{s}$，定义 $Z_q^n\times Z_q$ 上的概率分布 $A_{\boldsymbol{s},\chi}$，其变量形如 $(\boldsymbol{a},\boldsymbol{a}^{\mathrm{T}}\boldsymbol{s}+x)$，其中 $\boldsymbol{a}$ 在 Z_q^n 上均匀分布，x 随机取自错误分布 χ，向量间的加法和乘法运算均在模 q 意义下进行。

定义 1 （LWE 问题[1]）设 n 为正整数，$q=q(n)$，χ 是 Z_q 上的错误分布，$LWE_{n,m,q,\chi}$ 问题定义为：给出 m 个 $A_{\boldsymbol{s},\chi}$ 上相互独立的变量，求其对应的向量 $\boldsymbol{s}$。

LWE 问题的判定性问题记为 $DLWE_{n,m,q,\chi}$，在上述参数条件下，给定两组变量，每组 m 个，分别取自 $Z_q^n\times Z_q$ 上的均匀分布和 $A_{\boldsymbol{s},\chi}$，要求以不可忽略的概率对其进行区分。

LWE 问题的难解性可由以下命题刻画。

命题 1[14]　令 $r=r(n)\in(0,1)$ 和奇数 $q=q(n)$ 满足条件 $rq>2\sqrt{n}$。若存在一个攻击者 A 在多项式时间内解决 $DLWE_{n,m,q,\chi}$ 问题，则存在一个有效算法以参数 $O(n/r)$ 逼近格上的 SIVP 问题和 GapSVP 问题。

2.3　前像可采样陷门单向函数

文献[15]中提出了一种被称为“前向可采样陷门单向函数”的代数结构，能够实现从离散正态分布到近似均匀分布的映射；同时，存在一个对应的陷门 S（通常情况下是一个向量集合），在其作用下对映射求逆，能够输出一个满足原离散正态分布的随机变量。

首先通过一个命题说明前向可采样陷门单向函数的存在性。

命题 2[15]　设 n 为正整数，素数 $q=q(n)$ 是一个素数，$m\geqslant 2n\log q$，则存在一个多项式时间算法，输入 1^n，输出矩阵 $\boldsymbol{A}\in Z_q^{n\times m}$ 和向量集合 $S\subset\Lambda^{\perp}(\boldsymbol{A},q)=\{\boldsymbol{e}\in Z_q^m:\boldsymbol{Ae}=\boldsymbol{0}\bmod q\}$，其中 $\Lambda^{\perp}(\boldsymbol{A},q)$ 可以看做 Z_q^m 上的格，输出的结果满足条件：1）矩阵 $\boldsymbol{A}$ 的概率分布与 $Z_q^{n\times m}$ 上的均匀分布概率不可区分；2）S 的长度 $\|S\|\leqslant m^{2.5}$。

在此基础上定义函数 f_A。

定义 2[15]　前像可采样陷门单向函数。

对于命题 2 中的矩阵 $\boldsymbol{A}$，函数 $f_A:Z_q^m\to Z_q^n$ 定义为 $f_A(\boldsymbol{e})=\boldsymbol{Ae}\bmod q$，其中输入向量 $\boldsymbol{e}$ 取自分布 $D_{Z_q^m,r}$，其中 $r\geqslant\omega(\sqrt{\log m})$。函数 f_A 的逆函数 $f_A^{-1}:Z_q^n\to Z_q^m$ 首先计算 $\boldsymbol{At}=\boldsymbol{u}\bmod q$ 的一个特解 $\boldsymbol{t}$，随后利用集合 S 作为陷门进行前像采样，得到满足分布 $D_{\Lambda^{\perp},r,-\boldsymbol{t}}$ 的向量 $\boldsymbol{v}$，计算 $\boldsymbol{e}=\boldsymbol{t}+\boldsymbol{v}$ 作为逆函数的输出。

函数 f_A 的单向性可以归约到非齐次小整数解问题（ISIS, inhomogeneous small integer solution problem）的难解性。

命题 3[15]　（f_A 陷门单向性）在 ISIS 问题难解性假设下，函数 f_A 是一个前像可采样陷门单向函数，即 1）对于输入 $\boldsymbol{e}\xleftarrow{R}D_{Z_q^m,r}$，函数输出向量的概率分布与 Z_q^n 上的均匀分布概率不可区分；2）以集合 S 作为陷门，逆函数 $f_A^{-1}(\boldsymbol{u})$ 输出向量 $\boldsymbol{e}'$ 服从分布 $D_{Z_q^m,r}$，且满足 $\boldsymbol{Ae}'=\boldsymbol{u}\bmod q$。

3　基于身份的全同态加密体制模型

本节提出一种基于身份的全同态加密体制的模型，模型结合了基于身份加密体制和全同态加密 2 种不同体制的特点，并同时具备二者的功能。模型的安全性定义仍然沿用了标准的选择明文和选择身份攻击下的不可区分安全（IND-ID-CPA），根据全同态加密的特点，取{0,1}作为选择明文的取值空间。

定义 3　基于身份的全同态加密体制模型。

模型包含 5 个算法，分别是初始化、私钥提取、加密、解密和密文运算算法。

初始化算法 Setup：算法生成加密体制的一对公开参数（*param*）和主私钥（*msk*）。

私钥提取算法（Extract）：根据公开参数 *param*、主私钥 *msk* 和身份 *id*，为每个身份生成一个身份私钥 sk_{id}。

加密算法 Enc：利用公开参数 *param*、身份 *id* 和明文消息 $m\in\{0,1\}$，生成与身份 *id* 相关的密文 c。

解密算法 Dec：根据密文 c 和其对应的身份私钥 sk_{id}，计算出明文消息 m。

密文运算算法 Eval：算法的输入为运算 $f:\{0,1\}^t\to\{0,1\}$ 和属于同一身份 *id* 的一组密文 $(c_1,\cdots,c_t)$，输出为一个新的密文 c，满足

$$Dec_{sk_{id}}(c)=f(Dec_{sk_{id}}(c_1),\cdots,Dec_{sk_{id}}(c_t)) \quad (1)$$

下面给出这一模型的安全性定义。

定义 4　基于身份全同态加密的 IND-ID-CPA 安全性。

定义一个攻击者与挑战者之间进行的游戏，分为以下几个阶段。

初始化阶段：挑战者运行加密体制的初始化算法，将生成的公开参数 *param* 交给攻击者。

喻示访问阶段：在这一阶段，攻击者自由选择身份 $id_1,\cdots,id_q$ 访问私钥提取喻示，获得相应的身份私钥 $sk_{id_1},\cdots,sk_{id_q}$。

挑战阶段：上一阶段结束后，攻击者生成一个挑战身份 id^*，交给挑战者，要求 $id^*\notin\{id_1,\cdots,id_q\}$。挑战者随机选择明文 $b^*\in\{0,1\}$，用身份 id^* 进行加密，得到目标密文 c^* 并交还给攻击者。

猜测阶段：在猜测阶段，攻击者仍然具备访问私钥提取喻示的能力（id^* 例外），攻击者试图猜测

目标密文 c^* 所对应的明文 b'，当 $b'=b^*$ 时，认为攻击者在攻击游戏中获胜。

攻击者在游戏中获胜的概率与 1/2 的差值记为攻击者的优势 $Adv_{IND\text{-}ID\text{-}CPA}$，若对于任何多项式时间的攻击者，该优势可忽略，则称该体制是 IND-ID-CPA 安全的。

4 体制构造

本节给出一种基于身份的全同态加密体制构造方案，方案采用两层结构设计，首先构造底层基于 LWE 问题的同态加密体制，并以此为基础，通过设计私钥提取算法实现基于身份加密的功能。

4.1 基础同态加密体制

基础同态加密体制（BHE）的基本参数包括一个公开的随机均匀分布的矩阵 $\boldsymbol{A}\in Z_q^{n\times m}$ 和其对应的前像可采样陷门单项函数 f_A，。其中 n 是安全参数 λ 的多项式，$m\geqslant 2n\log q$，$q\in[2^{n^\varepsilon},2^{n^\varepsilon+1})$ 是一个奇数且 $\varepsilon\in(0,1)$。函数 f_A 的输入向量满足分布 $D_{Z^m,r}$，且 $r\geqslant\omega(\sqrt{\log m})$，以保证前像采样的正确性。矩阵 $\boldsymbol{A}$ 的陷门 S 在 BHE 体制中不发挥作用，但用于构造基于身份加密体制的密钥提取算法，生成用户私钥。

密钥生成算法 BHE-KeyGen(1^n)：，随机选择 $\boldsymbol{e}_0\xleftarrow{R}D_{Z^m,r}$ 和 L 个 Z_q^n 中均匀分布的向量 $\boldsymbol{e}_1,\cdots,\boldsymbol{e}_L$，作为 BHE 体制的私钥，计算 $\boldsymbol{u}=f_A(\boldsymbol{e}_0)$ 作为公钥。同时计算

$$\varphi_{j,i,j,\tau}:=(\boldsymbol{a}_{l,i,j,\tau},b_{l,i,j,\tau}:=<\boldsymbol{a}_{l,i,j,\tau},\boldsymbol{e}_l>+2\cdot x_{l,i,j,\tau}+2^\tau\cdot\boldsymbol{e}_{l-1}[i]\cdot\boldsymbol{e}_{l-1}[j])\in Z_q^n\times Z_q \tag{2}$$

其中，$\boldsymbol{a}_{l,i,j,\tau}\xleftarrow{R}Z_q^n$，$x_{l,i,j,\tau}\xleftarrow{R}\chi$。定义 $evk=\{\varphi_{l,i,j,\tau}\}_{l,i,j,\tau}$ 为运算公钥，用于执行密文乘法运算。

加密算法 BHE-Enc($\boldsymbol{u}$，b)：当加密消息比特 $m\in\{0,1\}$ 时，随机选择向量 $\boldsymbol{s}\xleftarrow{R}Z_q^n$，$\boldsymbol{x}\xleftarrow{R}\chi^n$，计算 $\boldsymbol{p}=\boldsymbol{A}^{\mathrm{T}}\boldsymbol{s}+2\boldsymbol{x}\in Z_q^m$。输出密文 $c=(\boldsymbol{p},v=<\boldsymbol{u}^{\mathrm{T}},\boldsymbol{s}>+2x+m)\in Z_q^m\times Z_q$，其中 $x\xleftarrow{R}\chi$。

解密算法 BHE-Dec($\boldsymbol{e}_i$,(**p**, v))：计算 $m=((v-<\boldsymbol{e}_i^{\mathrm{T}},\boldsymbol{p}>)\bmod q)\bmod 2$。

密文运算算法 BHE-Eval(f, c_1, …, c_t, evk)：首先将 f 表示成两输入乘法运算和任意输入加法运算的分级组合形式。运算过程中的密文形式为$((\boldsymbol{p},c),l)$，标志位 l 标明该密文的“级别”，每次密文加法与乘法运算的输入必须为同级密文，且每次乘法运算之后，乘积密文的级别增加一级。在解密时，不同级数的密文对应不同的私钥，解密 l 级密文所需的私钥为 $\boldsymbol{e}_l$。

密文加法 BHE-Add(c_1, …, c_t)：设输入为 t 个同为 l 级的密文 $c_1,\cdots,c_t$，其中 $c_i=((\boldsymbol{p}_i,v_i),l)$，则

$$c_{\mathrm{add}}=((\boldsymbol{p}_{\mathrm{add}},v_{\mathrm{add}}),l)=((\sum_i\boldsymbol{p}_i,\sum_i v_i),l) \tag{3}$$

密文 c_{add} 的噪声向量为输入密文噪声向量之和，依据解密算法 BHE-Dec，当噪声小于 $q/2$ 时，对 c_{add} 进行解密得到的明文消息等于 t 个明文消息之和。

密文乘法 BHE-Mult(c, c’, evk)：设乘法运算的输入为密文 $c=((\boldsymbol{p},v),l)$ 和 $c'=((\boldsymbol{p}',v'),l)$，将乘积密文记为 $c_{\mathrm{mult}}=((\boldsymbol{p}_{\mathrm{mult}},v_{\mathrm{mult}}),l+1)$。$c_{\mathrm{mult}}$ 的构造采用重线性化技术实现：首先写出 c_{mult} 的解密函数（未知数为密钥向量）

$$\phi(\boldsymbol{e}_l)=\phi_{(\boldsymbol{p},v)\cdot(\boldsymbol{p}',v')}(\boldsymbol{e}_l)=(v-<\boldsymbol{e}_l^T,\boldsymbol{p}>)\cdot(v'-<\boldsymbol{e}_l^{\mathrm{T}},\boldsymbol{p}'>) \tag{4}$$

进一步将其展开成二次项的形式，可得

$$\phi(\boldsymbol{e}_l)=\sum_{0\leqslant i\leqslant j\leqslant m}h_{ij}\boldsymbol{e}_l[i]\boldsymbol{e}_l[j] \tag{5}$$

其中，$\boldsymbol{e}_l[0]=1$，系数 $h_{i,j}\in Z_q$ 可以由输入密文的分量计算得到。

为了控制误差，将系数 $h_{i,j}$ 表示成其二项展开的形式，即

$$h_{i,j}=\sum_{\tau=0}^{\lfloor\log q\rfloor}h_{i,j,\tau}2^\tau \tag{6}$$

其中，$h_{i,j,\tau}\in\{0,1\}$，此时函数 $\phi(\boldsymbol{e}_l)$ 可以表示成

$$\phi(\boldsymbol{e}_l)=\sum_{\substack{0\leqslant i\leqslant j\leqslant m\\ \tau\in\{0,\cdots,\lfloor\log q\rfloor\}}}h_{i,j,\tau}(2^\tau\boldsymbol{e}_l[i]\boldsymbol{e}_l[j]) \tag{7}$$

根据运算密钥 $\varphi_{l,i,j,\tau}=(\boldsymbol{a}_{l,i,j,\tau},b_{l,i,j,\tau})$ 的属性

$$2^\tau\boldsymbol{e}_l[i]\boldsymbol{e}_l[j]=b_{l+1,i,j,\tau}-<\boldsymbol{a}_{l+1,i,j,\tau},\boldsymbol{e}_{l+1}>-2x_{l,i,j,\tau} \tag{8}$$

对 $\phi(\boldsymbol{e}_l)$ 中的所有二项式 $2^\tau\boldsymbol{e}_l[i]\cdot\boldsymbol{e}_l[j]$ 进行替换，即 $\phi(\boldsymbol{e}_l)$ 转换成密钥 $\boldsymbol{e}_{l+1}$ 的函数

$$\phi(\boldsymbol{e}_{l+1})=\text{BHE-Dec}(\boldsymbol{e}_{l+1},(\boldsymbol{p}_{\mathrm{mult}},v_{\mathrm{mult}})) \tag{9}$$

其中，

$$\boldsymbol{p}_{\mathrm{mult}}:=\sum_{\substack{0\leqslant i\leqslant j\leqslant m\\ \tau\in\{0,\cdots,\lfloor\log q\rfloor\}}}h_{i,j,\tau}\boldsymbol{a}_{l+1,i,j,\tau}$$

$$v_{mult} := \sum_{\substack{0\leqslant i\leqslant j\leqslant m \\ \tau\in\{0,\cdots,\lfloor\log q\rfloor\}}} h_{i,j,\tau}b_{l+1,i,j,\tau}$$

当噪声 $\sum_{\substack{0\leqslant i\leqslant j\leqslant m \\ \tau\in\{0,\cdots,\lfloor\log q\rfloor\}}} 2h_{i,j,\tau}x_{l,i,j,\tau}$ 小于 $q/2$ 时，对 c_{mult} 解密可以得到

$$m_{\text{mult}} = ((v_{\text{mult}} - <\boldsymbol{e}^{\text{T}}, \boldsymbol{p}_{\text{mult}}>) \bmod q) \bmod 2 = mm' \quad (10)$$

4.2　基于身份的全同态加密体制

本节给出的基于身份全同态加密体制（IBFHE）利用散列函数 $H:\{0,1\}^* \to Z_q^n$ 将身份 *id* 映射成 BHE 体制的公钥向量 $\boldsymbol{u}$。密钥提取算法在提取身份私钥的同时，还生成身份 *id* 的运算公钥，用于密文同态运算。

初始化算法 IBFHE-Setup(1^n)：按照命题 2 生成矩阵 $\boldsymbol{A}\in Z_q^{n\times m}$ 及其陷门 $S\in \Lambda^{\perp}(\boldsymbol{A},q)$，分别作为 IBFHE 体制的公开参数和主私钥。

私钥提取算法 IBFHE-Extract($\boldsymbol{A}$, S, *id*)：私钥包含 L+1 个向量 $\{\boldsymbol{e}_0,\cdots,\boldsymbol{e}_L\}$，若身份—密钥对 $(id,\{\boldsymbol{e}_0,\cdots,\boldsymbol{e}_L\})$ 已经存在，算法返回 $\{\boldsymbol{e}_0,\cdots,\boldsymbol{e}_L\}$，否则计算身份 *id* 的公钥 $\boldsymbol{u}=H(id)$，并利用陷门 S 对 $\boldsymbol{u}$ 进行前像采样，得到向量 $\boldsymbol{e}\leftarrow f_A^{-1}(\boldsymbol{u})$，根据命题 3 可知，$\boldsymbol{e}$ 的概率分布满足 $D_{Z_q^m,r}$。调用 BHE-KeyGen(1^n) 算法，设 $\boldsymbol{e}_0=\boldsymbol{e}$，在 Z_q^n 中均匀随机选择其余 L 个私钥 $\boldsymbol{e}_1,\cdots,\boldsymbol{e}_L$，计算 $evk_{id}=\{\varphi_{l,i,j,\tau}\}_{l,i,j,\tau}$ 作为身份 *id* 的运算公钥。存储 $(id,\{\boldsymbol{e}_0,\cdots,\boldsymbol{e}_L\})$，返回 $\{\boldsymbol{e}_0,\cdots,\boldsymbol{e}_L\}$ 并将 evk_{id} 公开。

加密算法 IBFHE-Enc(A, *id*, m)：为身份 *id* 加密消息比特 $m\in\{0,1\}$，首先计算其公钥 $\boldsymbol{u}=H(id)\in Z_q^n$，随后调用 BHE 体制的加密算法，得到密文 c=($\boldsymbol{p}$, v)← BHE-Enc($\boldsymbol{u}$, m)。

解密算法 IBFHE-Dec($\boldsymbol{e}_i$, ($\boldsymbol{p}$, v))：调用 BHE 体制的解密算法，计算 m = BHE-Dec($\boldsymbol{e}_i$, ($\boldsymbol{p}$, v))，密钥 $\boldsymbol{e}_i$ 的选择取决于密文的级别。

密文运算算法 IBFHE-Eval(f, c_1, …, c_t, evk)：f 的表示和运算过程中密文的形式与 BHE-Eval 算法相同。对于 f 中的密文加法运算，直接调用 BHE-Add 算法。进行密文乘法运算时，首先取得运算公钥 $\{\varphi_{l,i,j,\tau}\}_{l,i,j,\tau}$，随后调用 BHE-Mult 算法。值得注意的是，与初次加密时使用的用户公钥 $\boldsymbol{u}$ 不同，用户的运算公钥不仅与身份 *id* 有关，同时也与私钥 $\{\boldsymbol{e}_0,\cdots,\boldsymbol{e}_L\}$ 的选择有关。因此，在进行密文乘法运算之前，负责运算的服务器必须首先访问私钥提取服务器处的运算公钥列表，得到与密文所属身份 *id* 相对应的运算公钥 evk_{id}。这虽然与基于身份加密的要求不完全相同，但并不影响体制的实际应用。由于运算公钥仅与用户身份和私钥有关，只有私钥拥有者才能生成合法的运算公钥，因此即使攻击者对运算公钥进行篡改，也只能影响密文运算的正常进行，而不会造成泄密。因此，在云计算环境中，负责密文处理的云服务器可以无条件信任其所获得的运算公钥的安全性，而无须对其所属的身份进行证书认证。

5　安全性证明

定理 1　设系统参数 $n=n(\lambda)$，$k=k(\lambda)$，$q=q(\lambda)$ 和 $L=L(\lambda)$ 都是安全参数 λ 的多项式，χ^m 是 Z_q 上的 m 维离散正态分布 $D_{Z_q^m,r}$，$r\geqslant\omega(\sqrt{\log m})$，$m\geqslant 2n\log q$。在命题 3 以及 $DLWE_{n,q,\chi}$ 假设的前提下，BHE 体制是 IND-CPA 安全的。

证明　定理证明采用基于游戏（Game-based）的证明方法。初始游戏中包含一个 IND-CPA 攻击者 A，用优势 $Adv_{Game}[A]$来定义 A 在 Game 中获胜的概率。

Game0：Game0 即标准的 IND-CPA 游戏：挑战者调用 BHE-KeyGen 算法生成公钥 *pk* 和运算密钥 *evk*，并将其交给攻击者 A。A 具备访问加密喻示的能力。挑战者输出挑战密文 c^*，攻击者尝试区分 c^* 所对应的明文 $m_0=0$ 或 $m_0=1$。Game0 中攻击者的优势为

$$Adv_{CPA}[A] = |\Pr[A(pk, BHE\text{-}Enc_{pk}(m_0)=1] - \Pr[A(pk, BHE\text{-}Enc_{pk}(m_1)=1]| \quad (11)$$

Game1：Game1 与 Game0 的区别在于公钥的生成方式。Game1 中的公钥 $\boldsymbol{u}$ 不通过私钥 $\boldsymbol{e}_0$ 和函数 f_A 计算得到，而是直接从 Z_q^n 中均匀随机抽取。根据命题 3 的结论，攻击者 A 无法区分 Game0 与修改后的 Game1，因此

$$|Adv_{Game1}[A] - Adv_{CPA}[A]| = 0 \quad (12)$$

Game2：Game2 与 Game1 的区别在于运算密钥 *evk* 的生成方式，在 Game1 中，挑战者不再通过计算的方式生成运算密钥，而是从 $Z_q^n\times Z_q$ 中均匀随机

抽取一组 $\{\varphi_{l,i,j,\tau}\}_{l,i,j,\tau}$ 交给攻击者 A。因此，A 在 Game2 与 Game1 中优势的差值等于其成功区分两组运算密钥的概率，即 A 成功解决 L 个 $DLWE_{n,m^2\cdot\log q,q,\chi}$ 实例中至少一个的概率

$$\begin{aligned}&|Adv_{\text{Game2}}[A]-Adv_{\text{Game1}}[A]|\\&=1-\prod_{l=0}^{L}(1-Adv_{DLWE_{n,m^2\cdot\log q,q,\chi}}[A_l])\end{aligned}\tag{13}$$

Game3：在 Game3 中，加密算法被修改，密文中的 $\boldsymbol{p}$ 不再通过 $\boldsymbol{A}^{\mathrm{T}}\boldsymbol{s}+2\boldsymbol{x}$ 进行计算，而是直接从 Z_q^m 中随机均匀抽取。显然，Game1 与 Game2 中 A 优势的差值等于其解决 $DLWE_{n,m,q,\chi}$ 问题的优势

$$|Adv_{\text{Game3}}[A]-Adv_{\text{Game2}}[A]|=DLWE_{n,m,q,\chi}Adv[A]\tag{14}$$

Game4：在 Game4 中，挑战者给出的挑战密文 $c^*=(\boldsymbol{p},v)$ 不再由加密算法生成，而是直接从 $Z_q^m\times Z_q$ 均匀随机抽取。Game4 与 Game3 的区别仅在于 v 的生成方式，由于 Game3 的公钥 $\boldsymbol{u}$ 是 Z_q^n 中的均匀随机向量，因此 $v=<\boldsymbol{u}^{\mathrm{T}},\boldsymbol{s}>+2x+m$ 可以看做 $DLWE_{n,1,q,\chi}$ 问题的实例，由此可知

$$|Adv_{\text{Game4}}[A]-Adv_{\text{Game3}}[A]|=DLWE_{n,1,q,\chi}Adv[A]\tag{15}$$

至此，在 Game4 中，挑战者所给出的公钥和密文都是均匀随机，与明文{0,1}无关，因此攻击者 A 在 Game4 中的优势为零，即 $Adv_{\text{Game4}}[A]=0$。

结合式(12)~式(15)，可得

$$\begin{aligned}&Adv_{CPA}[A]\\&=1-\prod_{l=0}^{L}(1-Adv_{DLWE_{n,m^2\cdot\log q,q,\chi}}[A_l])+\\&\quad Adv_{DLWE_{n,m,q,\chi}}[A]+Adv_{DLWE_{n,1,q,\chi}}[A]\end{aligned}\tag{16}$$

因此，在 $DLWE_{n,m,q,\chi}$ 假设下，$Adv_{CPA}[A]$ 可忽略，BHE 体制是 IND-CPA 安全的。 □

定理 2 若 BHE 体制是标准模型下 IND-CPA 安全的，并且其公钥 $\boldsymbol{u}$ 在 Z_q^n 上均匀随机分布，则 IBFHE 体制在随机喻示模型下是 IND-ID-CPA 安全的。

证明 假设存在一个针对 IBFHE 体制的多项式时间攻击者 A，在 IND-ID-CPA 游戏中的优势为 ε（不可忽略），则可以基于 A 的能力，构造出一个针对 BHE 体制的攻击者 B，其在 IND-CPA 游戏中的优势为 $c\varepsilon$，c 为某特定常数。

假设攻击者 A 在访问 Q_{hash} 次散列函数喻示的条件下的优势为 ε，采用如下方法构造 B。

输入：作为 BHE 体制的攻击者，B 的输入为 BHE 体制的公共矩阵 $\boldsymbol{A}\in Z_q^{n\times m}$，公钥 $\boldsymbol{u}^*\in Z_q^n$ 以及运算公钥 $evk^*=\{\varphi_{l,i,j,\tau}^*\}_{l,i,j,\tau}$。

模拟 IBFHE 攻击游戏。

1) 模拟随机喻示：B 首先随机选取 $i\in[Q_{\text{hash}}]$，对于 A 的第 j 次访问 id_j，若 $j=i$，保存四元组 $(id_j,\boldsymbol{u}^*,evk^*,\perp)$，并输出 $\boldsymbol{u}^*$作为给 A 的反馈；若 $j\neq i$，则调用 BHE-Keygen 算法，生成密钥 $(\boldsymbol{u}_j,evk_{id_j},\{\boldsymbol{e}_{j0},\cdots,\boldsymbol{e}_{jL}\})$，保存 $(id_j,\boldsymbol{u}_j,evk_{id_j},\{\boldsymbol{e}_{j0},\cdots,\boldsymbol{e}_{jL}\})$ 并反馈 $\boldsymbol{u}_j$ 给 A。

2) 模拟私钥解析喻示：当 A 用身份 id 访问私钥解析喻示时，可以认为其已经用 id 访问过随机喻示，因此 B 只须查询已存储的四元组 $(id_j,\boldsymbol{u}_j,evk_{id_j},\{\boldsymbol{e}_{j0},\cdots,\boldsymbol{e}_{jL}\})$，取其中的私钥 $\{\boldsymbol{e}_{j0},\cdots,\boldsymbol{e}_{jL}\}$ 反馈给 A。若对应的私钥为 $\perp$，B 反馈一个随机向量，模拟中止。

3) 模拟目标密文：当 A 生成挑战身份 id^*时（IBFHE 体制的挑战明文默认为{0,1}），不失一般地认为 A 已经用 id^*访问过随机喻示，若 $id^*\neq id_i$，B 输出随机值，同时模拟中止；否则，B 将{0,1}交给 BHE 体制攻击游戏的挑战者，得到目标密文 c^*，并将其作为 IBFHE 攻击游戏的目标密文反馈给 A。

输出：当 A 终止并输出结果 m'时，B 也终止并输出相同的结果 m'。

由 S 的构造可以看出，在模拟过程中，B 没有终止并最终输出结果的概率为 $1/Q_{\text{hash}}$（即 $id^*=id_i$ 的概率），此时 B 成功模拟出 IBFHE 攻击游戏的环境。根据假设，A 在这种情况下攻击成功的优势为 ε，因此 B 攻击 BHE 体制的优势为 $\varepsilon/Q_{\text{hash}}$。 □

6 结束语

随着云计算的快速发展，云端数据保密和用户隐私保护等安全需求凸显，引发了对于全同态加密等新型密码技术的广泛关注。基于容错学习问题的全同态加密体制具有较高的计算效率和安全性，是目前研究的热点，但其公钥尺寸的缺陷始终难以得到根本解决。本文提出的基于身份全同态加密体制，借助基于身份加密的特点，避免了与身份认证和管理有关的系统开销，从而杜绝公钥尺寸对于全同态加密应用效率的影响。本文的设计思想为全同态加密体制的设计和改进指出了一种可行的途径，

即在基于身份加密的前提下，通过放宽对公钥尺寸的限制，获取更高的计算效率。

参考文献：

[1] REGEV O. On lattices, learning with errors, random linear codes, and cryptography[A]. Proceeding of the 37th ACM Symposium on Theory of Computing (STOC2005) [C]. Baltimore, MD, USA, 2005.84-93.

[2] LYUBASHEVSKY V, PEIKERT C, REGEV O. On ideal lattices and learning with errors over rings[A]. Proceeding of the 29th Annual Eurocrypt Conference[C]. Riviera, French, 2010.1-23.

[3] GENTRY C. Fully homomorphic encryption using ideal lattices[A]. Proceeding of the 40st ACM Symposium on Theory of Computing (STOC2009)[C]. Bethesda, Maryland, USA, 2009.169-178.

[4] DIJK M V, GENTRY C, HALEVI S, *et al*. Fully homomorphic encryption over the integers[A]. Proceeding of the 29th Annual Eurocrypt Conference[C]. Riviera, French, 2010.24-43.

[5] SMART N P, VERCAUTEREN F. Fully homomorphic encryption with relatively small key and ciphertext sizes[A]. Proceeding of the 13th International Conference on Practice and Theory in Public Key Cryptography (PKC2010)[C]. Paris, France, 2010.420-443.

[6] GENTRY C, HALEVI S. Implementing gentry's fully homomorphic encryption scheme[A]. Proceeding the 30th Annual Eurocrypt Conference[C]. Tallinn, Estonia, 2011.129-148.

[7] STEHL´E D, STEINFELD R. Faster fully homomorphic encryption [A]. Proceeding of the 16th Annual Asiacrypt Conference [C]. Singapore, 2010.377-394.

[8] BRAKERSKI Z, VAIKUNTANATHAN V. Efficient fully homomorphic encryption from (standard) LWE[A]. Proceeding of IEEE 52nd Annual Symposium on Foundations of Computer Science(FOCS2011)[C]. Palm Springs, CA, USA, 2011.97-106.

[9] BRAKERSKI Z, GENTRY C, VAIKUNTANATHAN V. Fully homomorphic encryption without bootstrapping[A]. Proceeding of Innovations in Theoretical Computer Science 2012[C]. Cambridge, MA, USA, 2012.309-325.

[10] GENTRY C, HALEVI S, SMART N P. Fully homomorphic encryption with polylog overhead[A]. Proceeding of the 31st Annual Eurocrypt Conference[C]. Canbridge, UK, 2012.465-482.

[11] GENTRY C, HALEVI S, SMART N P. Better bootstrapping in fully homomorphic encryption[A]. Proceeding of 15th International Conference on Practice and Theory in Public Key Cryptography[C]. Darmstadt, Germany, 2012.1-16.

[12] SHAMIR A. Identity-based cryptosystems and signature schemes[A]. Proceeding of the 8th Annual International Cryptology Conference[C]. Santa Barbara, California, USA, 1984.47-53.

[13] HU L, LIU Z L, SUN T, *et al*. Survey of security on identity-based cryptography[J]. Journal of Computer Research and Development, 2009, 46(9): 1537-1548.

[14] PEIKERT C. Public-key cryptosystems from the worst-case shortest vector problem: extended abstract[A]. Proceeding of The 41st ACM Symposium on Theory of Computing (STOC2009) [C]. Bethesda, Maryland, USA, 2009.333-342.

[15] GENTRY C, PEIKERT C, VAIKUNTANATHAN V. Trapdoors for hard lattices and new cryptographic constructions[A]. Proceeding of the 40th ACM Symposium on Theory of Computing (STOC2008) [C]. Victoria, British Columbia, Canada, 2008.197-206.

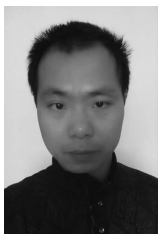
作者简介：

光焱（1983-），男，安徽枞阳人，博士，解放军信息工程大学讲师，主要研究方向为网络与信息安全，全同态加密。

祝跃飞（1962-），男，浙江杭州人，解放军信息工程大学教授、博士生导师，主要研究方向为密码学、信息安全。

费金龙（1980-），男，河南巩义人，硕士，解放军信息工程大学讲师，主要研究方向为网络与信息安全。

顾纯祥（1976-），男，安徽霍山人，博士，解放军信息工程大学副教授、硕士生导师，主要研究方向为网络与信息安全。



郑永辉（1976-），男，江西乐平人，博士，解放军信息工程大学讲师，主要研究方向为密码学、网络与信息安全。