一种基于 LWE 问题的无证书全同态加密体制

光 焱* 顾纯祥 祝跃飞 郑永辉 费金龙
(信息工程大学网络空间安全学院 郑州 450002)

摘 要：全同态加密在云计算等领域具有重要的应用价值，然而，现有全同态加密体制普遍存在公钥尺寸较大的缺陷，严重影响密钥管理与身份认证的效率。为解决这一问题，该文将无证书公钥加密的思想与全同态加密体制相结合，提出一种基于容错学习(LWE)问题的无证书全同态加密体制，利用前像可采样陷门单向函数建立用户身份信息与公钥之间的联系，无须使用公钥证书进行身份认证；用户私钥由用户自行选定，不存在密钥托管问题。体制的安全性在随机喻示模型下归约到判定性 LWE 问题难解性，并包含严格的可证安全证明。

关键词：全同态加密；无证书公钥加密；容错学习问题；前像可采样陷门单向函数
中图分类号：TP309 **文献标识码**： A **文章编号**：1009-5896(2013)04-0988-06
DOI: 10.3724/SP.J.1146.2012.01102

Certificateless Fully Homomorphic Encryption Based on LWE Problem

Guang Yan Gu Chun-xiang Zhu Yue-fei Zheng Yong-hui Fei Jin-long
(*Institute of Cyberspace Security*, *Information Engineering University*, *Zhengzhou* 450002, *China*)

Abstract: Fully homomorphic encryption has important application in cloud computing. However, the existing fully homomorphic encryption schemes share a common flaw that they all use public keys of large scales. And this flaw may cause inefficiency of these schemes in the key and identity management. To solve this problem, a certificateless fully homomorphic encryption scheme is presented based on Learning With Errors (LWE) problem. The scheme builds the connection between the user's identity and its public key with the trapdoor one-way function with preimage sampling so that the certificates are no longer necessary. The private keys are chosen by the users without key escrow. In the random oracle model, the security of the scheme strictly reduces to hardness of decisional LWE problem.

Key words: Fully homomorphic encryption; Certificateless public-key encryption; Learning With Errors (LWE) problem; Trapdoor one-way function with preimage sampling

1 引言

全同态加密又称隐私同态[1]，其思想源自 RSA 公钥加密所具备的乘法同态特性：将同一公钥加密下的若干密文相乘，乘积解密所得的明文恰好等于原密文各自对应明文的乘积。全同态加密允许在没有私钥的情况下，对加密数据进行各种有意义的运算和操作，因而能够实现敏感数据在加密状态下的计算外包，有效解决当前云计算发展中所面临的数据安全以及隐私保护问题。

2009 年，Gentry[2]基于“理想格”(ideal lattice)代数结构，设计出第 1 个真正意义上的全同态加密体制(Gentry 体制)，并使得理想格上的全同态加密体制设计成为密码学领域一个新的研究热点[3–6]。

2011 年，Brakerski 和 Vaikuntanathan[7]基于容错学习问题(Learning With Errors, LWE)[8]构造出第 1 种不依赖理想格的全同态加密体制(BV 体制)。由于 LWE 问题的难解性归约到一般格上的困难问题，因此这一体制具备比 Gentry 体制更可靠的安全性保证。BV 体制的缺陷在于其公钥尺寸与所能执行的密文乘法次数成正比，因而难以处理较复杂的密文运算。截止目前，针对该体制的改进[9–11]主要集中在进一步提高计算效率上，而对于如何控制公钥尺寸并无有效的解决方案。

作为公钥加密体制的一种，全同态加密在应用中同样需要考虑身份认证的问题。公钥证书能够解决这一问题，但同时也为系统带来计算、存储、通信与管理等方面的额外开销。特别对于全同态加密体制，由于其公钥通常具有较大的尺寸(安全参数的指数)，因此与证书相关的开销将严重影响这些体制在实际应用中的效率。

为此，本文将无证书公钥加密(certificateless

2012-08-28 收到，2012-11-12 改回
国家自然科学基金(61072047)和河南省科技攻关计划(112102210007)资助课题
*通信作者：光焱 gyinarmy@126.com

public key encryption)[12]的思想与全同态加密体制相结合，提出一种无证书的全同态加密体制。用户公钥与其身份信息一一对应，因而无须借助证书进行认证，克服了公钥尺寸对体制应用效率的影响；私钥生成中心(Private Key Generation center, PKG)利用前向可采样的陷门单向函数的性质提取用户的部分私钥(partial-sk)，并借助二重加密的方法，使用户的完整私钥与其自行选择的一组秘密值相关联，杜绝了私钥托管问题。体制的安全性在随机喻示模型下归约到判定性 LWE 问题的难解性。

本文的第 2 节介绍相关的背景知识；第 3 节描述无证书全同态加密体制的模型并给出其安全性定义；第 4 节介绍体制设计细节；第 5 节给出了该体制的在随机喻示模型下的安全性证明；第 6 节对全文进行总结。

2　基础知识

2.1 符号

本文中，向量被默认为具有列向量的形式，使用粗体小写字母表示，例如 $\boldsymbol{e}$；$\boldsymbol{e}^{\mathrm{T}}$ 表示向量 $\boldsymbol{e}$ 的转置；向量的第 i 个分量表示为 $\boldsymbol{e}[i]$。矩阵用粗体大写字母表示，例如 $\boldsymbol{A}^{m\times n}$；向量集合 S 的长度定义为其中最长向量的欧几里得范数，记做 $\|S\|$。

对于概率分布 $D, x\xleftarrow{R} D$ 表示随机选取符合分布 D 的变量 x; 对于集合 $S, x\xleftarrow{D} S$ 则表示从 S 中依分布 D 选取元素 x。集合 S 上两个概率分布 X 和 Y 之间的统计距离定义为 $\frac{1}{2}\sum_{s\in S}|X(s)-Y(s)|$，若对于包含 n 个变量的集合 S，该距离是 n 的可忽略函数，则称 X 和 Y 称为“不可区分”的。

2.2 LWE 问题

Regev[8]给出了 LWE 问题的判定性问题(DLWE)到格上 SVP 问题的量子归约。2009 年，Peikert[13]改进了这一归约，使归约过程不再依赖量子算法。

在定义 LWE 问题之前，首先给出 Regev 定义的两个概率分布：(1) $D_{\Lambda,r,c}$ 是格 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，当 $\boldsymbol{c}=\boldsymbol{0}$ 时，简写为 $D_{\Lambda,r}$；特别地，对于整数 $q\geq 2$，将 Z_q 上的离散正态分布 $D_{Z_q,r}$ 称为“错误分布”，记做 χ。(2)对于取定的正整数 n 和 Z_q^n 上的向量 $\boldsymbol{s}$，定义一个 $Z_q^n\times Z_q$ 上的概率分布 $A_{\boldsymbol{s},\chi}$，其变量具备 $(\boldsymbol{a}, \boldsymbol{a}^{\mathrm{T}}\cdot\boldsymbol{s}+x)$ 的形式，其中 $\boldsymbol{a}$ 是 Z_q^n 上均匀分布的变量，而 x 则随机取自错误分布 χ，加法和向量乘法运算均在模 q 意义下进行。

定义 1　LWE 问题和 DLWE 问题[8]　对于整数 $q=q(n)$ 和 Z_q 上的错误分布 χ，$\mathrm{LWE}_{n,m,q,\chi}$ 问题定义为：给出 m 个 $A_{s,\chi}$ 上相互独立的变量，求出其中包含的向量 $\boldsymbol{s}$。该问题的判定性问题记做 $\mathrm{DLWE}_{n,m,q,\chi}$，要求在同样的条件下，以不可忽略的概率区分两组变量，每组 m 个，分别取自 $Z_q^n\times Z_q$ 上的均匀分布和 $A_{\boldsymbol{s},\chi}$。

2.3 前像可采样陷门单向函数

Gentry 等人[14]提出一种前像可采样的陷门单向函数，函数实现从离散正态分布到近似均匀分布的映射，并在拥有陷门的情况下，将近似均匀分布还原为最初的离散正态分布，输出满足原分布的变量。在定义函数之前，首先给出一个命题：

命题 1[14]：　对于素数 $q=q(n)$ 和 $m\geq 5n\log q$，存在一个多项式时间算法，输入为参数 1^n，输出一个矩阵 $\boldsymbol{A}\in Z_q^{n\times m}$ 和满秩的向量集合 $S\subset \Lambda^{\perp}(\boldsymbol{A},q)=\{\boldsymbol{e}\in Z_q^m : \boldsymbol{A}\cdot\boldsymbol{e}=\boldsymbol{0}\bmod q\}$，其中 $\Lambda^{\perp}(\boldsymbol{A},q)$ 可以看做 Z_q^m 上的格，矩阵 $\boldsymbol{A}$ 的概率分布与 $Z_q^{n\times m}$ 上的均匀分布不可区分，S 的长度 $\|S\|\leq m^{2.5}$。

在命题 1 的基础上定义函数 f_A：

定义 2[14]　**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 $f_{\boldsymbol{A}}(\boldsymbol{e})=\boldsymbol{A}\cdot\boldsymbol{e}\bmod q$，满足性质(1)当输入向量 $\boldsymbol{e}$ 取自分布 $D_{Z_q^m,r}$ 时，函数输出向量的概率分布与 Z_q^n 上的均匀分布不可区分；(2)在陷门 S 的作用下，逆函数 $f_A^{-1}(\boldsymbol{u}): Z_q^n\to Z_q^m$ 的输出向量 $\boldsymbol{e}'$ 服从分布 $D_{Z_q^m,r}$，且满足 $\boldsymbol{A}\cdot\boldsymbol{e}'=\boldsymbol{u}\bmod q$。

3　无证书的全同态加密体制模型

本小节给出无证书的全同态加密体制的模型及其安全性定义，新体制在原有模型的基础上增加了密文运算算法，描述密文同态运算的能力。

定义 3　无证书的全同态加密(CertificateLess Fully Homomorphic Encryption, CLFHE)体制模型

无证书全同态公钥加密体制 CLFHE(Setup, Extract, Secret, Skgen, Pkgen, Enc, Dec, Eval)包含 8 个算法，前 7 个与原有定义相同：Setup 和 Extract 算法由 PKG 执行，前者生成系统的主密钥 msk 和公开参数 params，后者基于用户身份信息 id 计算出部分私钥 partial-$\mathrm{sk}_{\mathrm{id}}$；用户在收到部分私钥之后，依次执行 Secret, Skgen 和 Pkgen 算法，选择秘密值，并结合部分私钥和身份信息生成自身的公私钥对。加解密算法 Enc 和 Dec 在获得错误的输入时返回错误标识 $\perp$。密文运算算法 Eval 为 CLFHE 体制所独有，其输入为运算 $f:\{0,1\}^t\to\{0,1\}$ 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：

$$\mathrm{Dec}_{\mathrm{sk}_{\mathrm{id}}}(c)=f(\mathrm{Dec}_{\mathrm{sk}_{\mathrm{id}}}(c_1),\cdots,\mathrm{Dec}_{\mathrm{sk}_{\mathrm{id}}}(c_t)) \qquad (1)$$

无证书公钥加密的安全模型中包含两类攻击

者，第1类攻击者模拟外部攻击者，由于没有公钥证书存在，因此攻击者能够替换任何用户的公钥，但无法取得系统的主密钥；第2类攻击者模拟诚实但好奇的PKG，拥有系统主密钥但不替换用户公钥。考虑到密文同态运算特性，CLFHE体制采用选择明文攻击下的不可区分安全性定义(IND-CPA)，并将明文空间定为{0,1}。

定义 4　无证书全同态加密的 IND-CPA 安全性　定义通过一个攻击者与挑战者之间的游戏描述，分为以下几个阶段：

(1)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 params 交给攻击者，对于第 2 类攻击者，挑战者还需对其公开系统的主密钥 msk。

(2)喻示访问阶段 1：提供了 3 个可供攻击者访问的喻示，分别是部分私钥喻示、身份私钥喻示和身份公钥喻示。

部分私钥提取喻示：攻击者提供一个用户身份 id，挑战者运行部分私钥提取算法 Extract，得到该用户的部分私钥 partial-$\mathrm{sk}_{\mathrm{id}}$，并将其返回给攻击者。

私钥喻示：攻击者提供一个用户身份 id，挑战者运行算法 Skgen 得到该用户的私钥 $\mathrm{sk}_{\mathrm{id}}$，并将其返回给攻击者。

公钥喻示：攻击者提供一个用户身份 id，挑战者运行算法 Pkgen 得到该用户的公钥 $\mathrm{pk}_{\mathrm{id}}$，并将其返回给攻击者。

其中的部分私钥喻示专为第 1 类攻击者而设，第 2 类攻击者由于本身拥有主密钥因而无需访问此喻示。第 1 类攻击者在这一阶段除了访问喻示之外，还能够对任意用户的公钥进行篡改，包括即将选定的挑战身份 id^*所对应的公钥 $\mathrm{pk}_{\mathrm{id}^*}$。

(3)挑战阶段：上一阶段结束后，攻击者选定一个挑战身份 id^*交给挑战者，要求 id^*未曾作为上一阶段部分私钥提取喻示和私钥喻示的输入。挑战者随机选择明文 $m^* \in \{0,1\}$，用 $\mathrm{pk}_{\mathrm{id}^*}$进行加密。若加密算法输出错误标识 $\perp$，则攻击者攻击失败(第 1 类攻击者所篡改的公钥无法实现正确的加密)；否则，挑战者将得到的目标密文 c^*交还给攻击者。

(4)喻示访问阶段 2：攻击者仍然具备访问各种喻示的能力(id^*不能作为部分私钥提取喻示和私钥喻示的输入)。

(5)猜测阶段：攻击者对目标密文 c^*所对应的明文进行猜测，输出猜测结果 m'，当 $m'=m^*$ 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 $\mathrm{Adv}_{\mathrm{IND\text{-}CPA}}$，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-CPA 安全的。

4　体制构造

本节按照第 3 节定义的模型，给出 CLFHE 体制的具体构造，包含 8 个算法：

(1)初始化算法 CLFHE-Setup(1^λ)：依据命题 1 生成一个随机均匀分布的矩阵 $\boldsymbol{A} \in Z_q^{n\times m}$ 及其陷门 $S \in \Lambda^{\perp}(\boldsymbol{A},q)$，其中 n 是安全参数 λ 的多项式，$m \geq 5n\log q$，$q \in [2^{n^{\varepsilon}}, 2\cdot 2^{n^{\varepsilon}}]$ 是一个奇数且 $\varepsilon \in (0,1)$，由此得到前像可采样陷门单向函数 f_A。算法输出矩阵 $\boldsymbol{A}$ 及其陷门 S，分别作为 CLFHE 体制的公开参数 params 和主密钥 msk。

(2)部分私钥提取算法 CLFHE-Extract(A, S, id)：首先利用一个哈希函数 $H:\{0,1\}^* \to Z_q^n$ 对身份 id 进行哈希运算，得到向量 $\boldsymbol{u}=H(\mathrm{id})$，在随机喻示模型下该向量的概率分布为 Z_q^n 上的均匀随机分布。利用函数 f_A 及其陷门 S 对 $\boldsymbol{u}$ 进行前像采样，得到向量 $\boldsymbol{e} \leftarrow f_A^{-1}(\boldsymbol{u})$，根据定义 2 可知，$\boldsymbol{e}$ 的分布满足 $D_{Z_q^m,r}$。向量 $\boldsymbol{e}$ 作为用户 id 的部分私钥 partial-$\mathrm{sk}_{\mathrm{id}}$，由 PKG 通过安全信道发送给用户。

(3)秘密值算法 CLFHE-Secret(A, id)：由用户执行，随机选择 L 个 Z_q^n 中均匀分布向量$\{\boldsymbol{e}_1,\cdots,\boldsymbol{e}_L\}$作为其身份 id 对应的秘密值 x_{id}。

(4)私钥生成算法CLFHE-Skgen(id, $\boldsymbol{e}$,$\{\boldsymbol{e}_1,\cdots,\boldsymbol{e}_L\}$)：由用户执行，将秘密值 $x_{\mathrm{id}}=\{\boldsymbol{e}_1,\cdots,\boldsymbol{e}_L\}$ 作为其私钥。

(5)公钥生成算法 CLFHE-Pkgen(id, $\boldsymbol{e}$, $\{\boldsymbol{e}_1,\cdots,\boldsymbol{e}_L\}$)：记 $\boldsymbol{e}_0=\boldsymbol{e}$，依次以 $\boldsymbol{e}_l$ 为密钥，对 $\boldsymbol{e}_{l-1}$ 分量的二项式乘积进行 Regev 加密，得到一组密文：

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

其中 $\boldsymbol{a}_{l,i,j,\tau} \xleftarrow{R} Z_q^n$，$x_{l,i,j,\tau} \xleftarrow{R} \chi$。记 $\mathrm{evk}_{\mathrm{id}} = \{\varphi_{l,i,j,\tau}\}_{l,i,j,\tau}$ 为运算公钥，用于密文乘法，使相乘前后密文形式保持一致。其原理在密文运算部分详细介绍。算法输出身份 id 的公钥 $\mathrm{pk}_{\mathrm{id}}=\{\boldsymbol{u},\mathrm{evk}_{\mathrm{id}}\}$。

(6)加密算法 CLFHE-Enc(id, $\mathrm{pk}_{\mathrm{id}}$, m)：对消息比特 $m\in\{0,1\}$ 的加密分为两步进行：第 1 步称为“基础加密”，是对文献[14]中“对偶加密体制”的改进，借助重线性化技术实现全同态加密的功能；第 2 步称为“基础乘法”，利用下文中的密文乘法运算 CLFHE-Mult，将消息比特 m 和比特“1”在密文域下相乘，乘积密文作为最终的加密结果输出。下面给出两个子算法的细节：

基础加密　BasicEnc(id,$\mathrm{pk}_{\mathrm{id}}$,$m$)　随机选择向量 $\boldsymbol{s} \xleftarrow{R} Z_q^n$, $\boldsymbol{x} \xleftarrow{R} \chi^n$，计算 $\boldsymbol{p}=\boldsymbol{A}^{\mathrm{T}}\boldsymbol{s}+2\boldsymbol{x} \in Z_q^m$。

以 $\mathrm{pk}_{\mathrm{id}}$ 中的向量 $\boldsymbol{u}$ 作为公钥，计算 $c'=(\boldsymbol{p},v=<\boldsymbol{u}^{\mathrm{T}},\boldsymbol{s}>+2x+b)\in Z_q^m\times Z_q$ 作为基础加密的密文，其中 $x\xleftarrow{R}\chi$。

BasicEnc 算法的解密密钥是用户的部分私钥 $\boldsymbol{e}$，根据部分私钥提取算法可知 $\boldsymbol{u}=(\boldsymbol{A}\cdot\boldsymbol{e})\bmod q$，因此 BasicEnc 算法的明文 $m=((v-<\boldsymbol{e}^{\mathrm{T}},\boldsymbol{p}>)\cdot\bmod q)\bmod 2$。

基础乘法 BasicMult(id,$\mathrm{pk}_{\mathrm{id}}$, c')　首先对比特“1”加密，计算 $c_1=\mathrm{BasicEnc}(\mathrm{id},\boldsymbol{u},1)$；进而利用 $\mathrm{pk}_{\mathrm{id}}$ 中的运算公钥 $\{\varphi_{1,i,j,\tau}\}_{i,j,\tau}$，计算 $c=\mathrm{CLFHE\text{-}Mult}_{\mathrm{evk}}(c_1,c')$，输出 c 作为加密算法的最终结果。

(7)解密算法 CLFHE-Dec(id, $\mathrm{sk}_{\mathrm{id}}$, c)：输入密文 $c=(\boldsymbol{p},v)$ 以及私钥 $\mathrm{sk}_{\mathrm{id}}=\{\boldsymbol{e}_1,\cdots,\boldsymbol{e}_L\}$，选择合适的 $\boldsymbol{e}_i$ 计算 $m=((v-<\boldsymbol{e}_i^{\mathrm{T}},\boldsymbol{p}>)\bmod q)\bmod 2$ 并输出。

(8)密文运算算法 $\mathrm{CLFHE\text{-}Eval}_{\mathrm{evk}}(f,c_1,\cdots,c_t)$：由 CLFHE-Enc 算法的定义可以看出，CLFHE 体制的密文运算本质上是 BasicEnc 算法的密文运算，因此下文中的密文形式和解密运算均沿用 BasicEnc 算法，而所得结果同样适用于加密算法 CLFHE-Enc。密文运算算法的设计只考虑两种基本运算：加法和两个乘数的乘法；对于输入的运算函数 f，首先需将 f 分解成上述基本运算的组合。运算过程中的密文形式为记$((\boldsymbol{p},v),l)$，标志位 l 标明该密文的“级别”，基础密文 c' 的级别为 0; CLFHE-Enc 算法输出的密文级别为 1。密文加法和乘法运算的输入必须为同级别密文，每次乘法运算之后，所得结果密文的级别增加一级。解密 l 级密文必须使用私钥中对应的向量 $\boldsymbol{e}_l$。

密文加法 $\mathrm{CLFHE\text{-}Add}(c_1,\cdots,c_t)$　设输入为 t 个同级的密文 $c_1,\cdots,c_t$，其中 $c_i=((\boldsymbol{p}_i,v_i),l)$，则

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

由于加解密算法的主体是向量内积运算，因此具备加法同态属性。密文 c_{add} 的噪声向量为输入密文噪声向量之和，当 c_{add} 的噪声小于 $q/2$ 时，对 c_{add} 解密得到的明文消息等于 t 个明文消息之和。

密文乘法 $\mathrm{CLFHE\text{-}Mult}_{\mathrm{evk}}(c,c')$　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_{mult}，其构造采用重线性化技术实现：在假设满足乘法同态的前提下，c_{mult} 的解密函数表示如下(以密钥 $\boldsymbol{e}_l$ 为未知数)：

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

进一步将其展开成 $\boldsymbol{e}_l$ 分量的二次项形式，可得

$$\phi(\boldsymbol{e}_l)=\sum_{\substack{0\le i\le j\le m\\ \tau\in\{0,\cdots,\lfloor\log q\rfloor\}}}h_{i,j,\tau}\cdot(2^{\tau}\cdot\boldsymbol{e}_l[i]\cdot\boldsymbol{e}_l[j])\tag{5}$$

其中 $\boldsymbol{e}_l[0]=1$，系数 $h_{i,j,\tau}\in\{0,1\}$ 是两个输入密文分量的组合经二项展开之后的结果。

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

$$\begin{aligned}2^{\tau}\boldsymbol{e}_l[i]\boldsymbol{e}_l[j]&=b_{l+1,i,j,\tau}-<\boldsymbol{a}_{l+1,i,j,\tau},\boldsymbol{e}_{l+1}>-2\cdot x_{l,i,j,\tau}\\&\approx b_{l+1,i,j,\tau}-<\boldsymbol{a}_{l+1,i,j,\tau},\boldsymbol{e}_{l+1}>\end{aligned}\tag{6}$$

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

$$\phi(\boldsymbol{e}_{l+1})=v_{\mathrm{mult}}-<\boldsymbol{e}_{l+1}^{\mathrm{T}},\boldsymbol{p}_{\mathrm{mult}}>\tag{7}$$

其中

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

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

因此，乘积 $c_{\mathrm{mult}}=((\boldsymbol{p}_{\mathrm{mult}},v_{\mathrm{mult}}),l+1)$，当噪声部分 $\sum_{\substack{0\le i\le j\le m\\ \tau\in\{0,\cdots,\lfloor\log q\rfloor\}}}2\cdot h_{i,j,\tau}\cdot x_{l,i,j,\tau}$ 小于 $q/2$ 时，对其解密可得到明文：

$$m_{\mathrm{mult}}=((v_{\mathrm{mult}}-<\boldsymbol{e}^{\mathrm{T}},\boldsymbol{p}_{\mathrm{mult}}>)\bmod q)\bmod 2=m\cdot m'\tag{8}$$

5　安全性证明与效率分析

5.1 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 是离散正态分布 $D_{Z_q^m,r}$，$r\ge\omega(\sqrt{\log m})$，$m\ge 5n\log q$。在随机喻示模型和 $\mathrm{DLWE}_{n,q,\chi}$ 假设下，CLFHE 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多项式时间的攻击者 A(可能为第 1 类或第 2 类攻击者)，用优势 $\mathrm{Adv}_{\mathrm{Game}}[A]$定义 A 在 Game 中获胜的概率。

Game0：Game0 即定义 4 中的 IND-CPA 游戏，分 5 个阶段进行，攻击者 A 尝试区分挑战密文 c^* 所对应的明文 $m_0=0$ 或 $m_1=1$，其优势定义为

$$\begin{aligned}\mathrm{Adv}_{\mathrm{CPA}}[A]=|&\Pr[A(\mathrm{pk},\mathrm{CLFHE\text{-}Enc}_{\mathrm{pk}}(m_0))=1]\\&-\Pr[A(\mathrm{pk},\mathrm{CLFHE\text{-}Enc}_{\mathrm{pk}}(m_1))=1]|\end{aligned}\tag{9}$$

Game1：Game1 对 Game0 中的私钥喻示和公钥喻示进行修改。私钥喻示在输出私钥的同时，保存一份喻示访问列表 $\mathrm{List}_{\mathrm{sk}}$={id,$\mathrm{sk}_{\mathrm{id}}$}。公钥喻示在收到访问请求{id}后，首先查询该列表，若{id}在 $\mathrm{List}_{\mathrm{sk}}$ 中，公钥喻示按照 CLFHE-Pkgen 算法，在部分私钥 $\boldsymbol{e}$ 和私钥 $\mathrm{sk}_{\mathrm{id}}$ 的基础上计算出运算公钥 $\mathrm{evk}_{\mathrm{id}}$，与 $\boldsymbol{u}$ 一起组成身份 id 的公钥，反馈给攻击者；反之，若{id}没有在 $\mathrm{List}_{\mathrm{sk}}$ 中出现，公钥喻示在

$Z_q^n \times Z_q$ 上随机选择一组满足均匀分布的 $(\boldsymbol{a}_{l,i,j,\tau}, b_{l,i,j,\tau})$，与 $\boldsymbol{u}$ 一同输出。

攻击者 A 区分 Game0 和 Game1 的概率等于其区分 $(\boldsymbol{a}_{l,i,j,\tau}, b_{l,i,j,\tau})$ 是真实公钥抑或随机值的概率。由于 CLFHE 体制的即用户 id 所选择的秘密值，因此除非用{id}访问私钥喻示，否则无论 A 是第 1 类攻击者或第 2 类攻击者，均无法得知私钥 $\{\boldsymbol{e}_1, \cdots, \boldsymbol{e}_L\}$，所以区分 $(\boldsymbol{a}_{l,i,j,\tau}, b_{l,i,j,\tau})$ 对于攻击者 A 来说构成 L 个 $\mathrm{DLWE}_{n,m^2\cdot\log q,q,\chi}$ 问题实例，故而可知

$$\begin{aligned}&|\operatorname{Adv}_{\mathrm{Game1}}[A] - \operatorname{Adv}_{\mathrm{Game0}}[A]| \\ &= 1 - \prod_{l=1}^{L}(1 - \operatorname{Adv}_{\mathrm{DLWE}_{n,m^2\cdot\log q,q,\chi}}[A_l]) \end{aligned} \tag{10}$$

Game2：Game2 修改了挑战者生成挑战密文 $c^* = (\boldsymbol{p}^*, v^*)$ 的方式，c^* 仍然分两步生成，首先进行以 $\boldsymbol{u}$ 为公钥的基础加密，随后执行基础乘法。然而第 1 步中，中间结果 $(\boldsymbol{p}^*)'$ 不再通过计算 $\boldsymbol{A}^{\mathrm{T}}\boldsymbol{s} + 2\boldsymbol{x}$ 得到，而是直接从 Z_q^m 中随机均匀抽取；第 2 步与原算法相同：

$$\boldsymbol{p}^* := \sum_{\substack{0\le i\le j\le m \\ \tau\in\{0,\cdots,\lfloor\log q\rfloor\}}} h_{i,j,\tau}\cdot \boldsymbol{a}_{1,i,j,\tau}$$

A 在 Game2 和 Game1 中优势的差值需要根据其类型分别进行分析：

当 A 为第 2 类攻击者时(记为 A_2)，A_2 拥有挑战身份 id^* 的部分私钥 $\boldsymbol{e}^*$，同时也是基础加密算法的解密密钥，因此若 A_2 得到能够得到 $(\boldsymbol{p}^*)'$，即可通过直接解密区分 Game1 与 Game2。然而加密算法的输出为第 2 步的结果 $\boldsymbol{p}^*$，由 Game1 可知，A_2 通过访问公钥喻示得到的运算密钥 $\boldsymbol{a}_{1,i,j,\tau}$ 是一个随机值，因此 A_2 无法获得关于 $(\boldsymbol{p}^*)'$ 的信息，其区分 Game1 与 Game2 的概率为 0。

记 A_1 为第 1 类攻击者，A_1 具备篡改公钥的能力，因此能够通过篡改 $\boldsymbol{a}_{1,i,j,\tau}$ 使加密算法中的基础乘法失效，直接得到 $(\boldsymbol{p}^*)'$ 的值；然而 A_1 无法通过喻示访问获得挑战身份 id^* 的部分私钥 $\boldsymbol{e}^*$，且向量 $\boldsymbol{s}$ 是 Z_q^n 中的均匀随机分布，因此区分 $(\boldsymbol{p}^*)'$ 对 A_1 而言等价于解决 $\mathrm{DLWE}_{n,1,q,\chi}$ 问题的实例，由此可知：

$$\begin{aligned}&|\operatorname{Adv}_{\mathrm{Game2}}[A_1] - \operatorname{Adv}_{\mathrm{Game1}}[A_1]| \\ &= \mathrm{DLWE}_{n,1,q,\chi}\operatorname{Adv}[A_1]\end{aligned} \tag{11}$$

Game3：在 Game3 中，挑战者给出的挑战密文 c^* 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。对 Game3 中攻击者优势的分析与 Game2 类似，分析对象由 $(\boldsymbol{p}^*)'$ 变为 $(v^*)'$。在随机喻示模型下，公钥向量 $\boldsymbol{u}$ 满足 Z_q^n 中的均匀随机分布，因此区分 $v = <\boldsymbol{u}^{\mathrm{T}}, \boldsymbol{s}> + 2x + m$ 对于第 1 类攻击者而言是一个 $\mathrm{DLWE}_{n,1,q,\chi}$ 问题实例，即

$$\begin{aligned}&|\operatorname{Adv}_{\mathrm{Game3}}[A_1] - \operatorname{Adv}_{\mathrm{Game2}}[A_1]| \\ &= \mathrm{DLWE}_{n,1,q,\chi}\operatorname{Adv}[A_1]\end{aligned} \tag{12}$$

第 2 类攻击者优势差仍为 0。

至此，在 Game3 中，攻击者 A 得到公钥和挑战密文都是均匀随机的值，与目标明文 m^* 无关，因此攻击者 A 在 Game3 中的优势为零，即 $\operatorname{Adv}_{\mathrm{Game4}}[A] = 0$。

结合式(10)–式(12)，取两类攻击者优势的最大值，可得

$$\begin{aligned}\operatorname{Adv}_{\mathrm{CPA}}[A] \le 1 - \prod_{l=0}^{L}\left(1 - \operatorname{Adv}_{\mathrm{DLWE}_{n,m^2\cdot\log q,q,\chi}}[A_l]\right) \\ + 2\cdot\operatorname{Adv}_{\mathrm{DLWE}_{n,1,q,\chi}}[A]\end{aligned} \tag{13}$$

在 $\mathrm{DLWE}_{n,m,q,\chi}$ 假设下 $\operatorname{Adv}_{\mathrm{CPA}}[A]$ 可忽略，CLFHE 体制的 IND-CPA 安全性得证。 证毕

5.2 效率分析

本小节对 CLFHE 体制的效率进行对比分析。由于现有的无证书加密体制都没有考虑同态加密的特性，因此在效率方面无从比较；而在全同态加密方面，我们选择现有体制中计算效率相对较高的 BV 体制作为参照对象。

两种体制的设计都基于 LWE 问题，因此具备相似的结构。在算法参数方面，二者拥有相同长度的密文以及私钥，其公钥都可分成加密公钥和运算公钥两部分，而其中造成主要开销的运算公钥长度同为 $Ln^2\log^2 q$ bit。在计算复杂度方面，两种体制的解密算法使用完全相同的运算；而加密时，为了避免服务器掌握用户私钥，CLFHE 体制采用二次加密的方式处理明文，使得其加密算法复杂度相对 BV 体制有所增加：其中 BasicEnc 算法的计算复杂度与 BV 体制加密算法大致相当，而 BasicMult 算法则需要额外 $(n+1)^2$ 次 Z_q 上的加法运算(最坏情况)。

CLFHE 体制的效率优势主要体现在其无证书属性上。由于 CLFHE 体制的用户公钥与身份信息绑定，因此无需借助证书进行合法性认证。相比之下，BV 体制则必须建立可信的第三方认证中心(CA)，负责公钥证书的分发与管理。以 X.509 证书标准为例，若取 m=16128, n=192, q=4096, L=10 作为 BV 体制的参数，则 CA 签发每份证书的过程需要对至少 50.6 Mbit 的数据(包含证书以及公钥本身)进行哈希，并对结果进行签名(通常使用 RSA 算法)；而在加密或密文运算之前，加密方需要首先获取对方的证书，并对其中的公钥进行认证。证书通常由 CA 集中存储和管理，而用户身份变更所导致的证书更新、撤销等操作也会带来相应的计算和通信开销。表 1 给出两种体制在上述参数条件下的效

表 1 两种体制效率对比

体制	加密复杂度 (模 q 意义下)	解密复杂度 (模 q 意义下)	公钥尺寸 (Mbit)	可信 第三方	计算开销 (证书签发/认证)	存储开销 (每份证书)	通信开销 (一次认证)
BV 体制[7]	3.11×10^6 次乘 3.11×10^6 次加	192 次乘 192 次加	50.6	需要	证书主体哈希运算 一次 RSA 加/解密	50.6 Mbit	50.6 Mbit
CLFHE 体制	3.11×10^6 次乘 3.14×10^6 次加	192 次乘 192 次加	50.6	不需要	无	无	无

率对比，其中所列的 3 种开销特指与证书相关的应用开销，而不包含加解密算法本身的计算量。

6　结束语

随着云计算的快速发展，越来越多的企业和个人选择将数据的存储和处理外包给云端的服务器，由此带来的数据保密和隐私问题引起了广泛的关注。全同态加密能够实现密文域上的各种运算，在云计算领域具有重要的应用价值，然而，现有全同态加密体制中普遍存在的公钥尺寸偏大的问题，将增加密钥管理和身份认证的开销，对其应用领域和实际效率产生制约。本文提出的无证书全同态加密体制，融合了两种公钥密码体制各自的特点，具备全同态运算能力，无需使用公钥证书，且不存在私钥托管问题。本文的设计思想具有一定通用性，并且为现有体制的进一步改进指出一种可行的途径，例如考虑放宽对公钥尺寸的要求，以换取更高的计算效率。

参 考 文 献

[1] Rivest R, Adleman L, and Dertouzos M. On data banks and privacy homomorphisms[C]. Proceedings of IEEE 17nd Annual Symposium on Foundations of Computer Science (FOCS1978) Ann Arbor, Michigan, USA, October 16–18, 1978: 169–177.

[2] Gentry C. Fully homomorphic encryption using ideal lattices[C]. Proceedings of 41rd ACM Symposium on Theory of Computing (STOC2009), Bethesda, Maryland, USA, May 31–June 2, 2009: 169–178.

[3] Van Dijk M, Craig Gentry, Halevi S, *et al*.. Fully homomorphic encryption over the integers[C]. Proceedings of EUROCRYPT2010, Riviera, French, May 30–June 3, 2010: 24–43.

[4] Smart N P and Vercauteren F. Fully homomorphic encryption with relatively small key and ciphertext sizes[C]. Proceedings of 13th International Conference on Practice and Theory in Public Key Cryptography (PKC2010), Paris, France, May 26–28, 2010: 420–443.

[5] Gentry C and Halevi S. Implementing gentry's fully-homomorphic encryption scheme[C]. Proceedings of EUROCRYPT2011, Tallinn, Estonia, May 15–19, 2011: 129–148.

[6] Stehlé D and Steinfeld R. Faster fully homomorphic encryption[C]. Proceedings of ASIACRYPT2010, Singapore, December 5–9, 2010: 377–394.

[7] Brakerski Z and Vaikuntanathan V. Efficient fully homomorphic encryption from (standard) LWE[C]. Proceedings of IEEE 52nd Annual Symposium on Foundations of Computer Science(FOCS2011), Palm Springs, CA, USA, October 22–25, 2011: 97–106.

[8] Regev O. On lattices, learning with errors, random linear codes, and cryptography[C]. Proceedings of 37rd ACM Symposium on Theory of Computing (STOC2005), Baltimore, MD, USA, May 22–24, 2005: 84–93.

[9] Brakerski Z, Gentry C, and Vaikuntanathan V. Fully homomorphic encryption without bootstrapping[C]. Proceedings of Innovations in Theoretical Computer Science 2012, Cambridge, MA, USA, January 8–10, 2012: 309–325.

[10] Gentry C, Halevi S, and Smart N P. Fully homomorphic encryption with Polylog Overhead[C]. Proceedings of EUROCRYPT2012, Canbridge, UK, April 15–19, 2012: 465–482.

[11] Gentry C, Halevi S, and Smart N. Better bootstrapping in fully homomorphic encryption[C]. Proceedings of 15th International Conference on Practice and Theory in Public Key Cryptography, Darmstadt, Germany, May 21–23, 2012: 1–16.

[12] Al-Riyami S S and Paterson K G. Certificateless Public Key Cryptography[C]. Proceedings of ASIACRYPT2003, Taipei, Nov. 30–Dec. 4, 2003: 452–473.

[13] Peikert C. Public-key cryptosystems from the worst-case shortest vector problem: extended abstract[C]. Proceedings of 41rd ACM Symposium on Theory of Computing (STOC2009), Bethesda, Maryland, USA, May 31–June 2, 2009: 333–342.

[14] Gentry C, Peikert C, and Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions[C]. Proceedings of 40rd ACM Symposium on Theory of Computing(STOC2008), Victoria, British Columbia, Canada, Mar. 29–30, 2008: 197–206.

光　焱：　男，1983 年生，博士生，研究方向为同态加密、云计算与网络安全.

顾纯祥：　男，1976 年生，副教授，研究方向为密码学与网络安全.

祝跃飞：　男，1964 年生，教授，研究方向为密码学与网络安全.

郑永辉：　男，1976 年生，讲师，研究方向为密码学.

费金龙：　男，1964 年生，讲师，研究方向为网络安全.