doi:10.3969/j.issn.1000-436x.2014.01.020

基于 RLWE 的全同态加密方案

汤殿华[1]，祝世雄[1]，王林[1]，杨浩淼[2]，范佳[1]
（1. 保密通信重点实验室，四川 成都 610041；2.电子科技大学 计算机学院，四川 成都 610054）

摘 要：基于 Kristin Lauter 等人的 somewhat 同态方案，提出“带密钥转换的重线性化技术”。结合该技术与“模转换”，设计了一个基于 RLWE 的非自举的层次化全同态加密方案。该方案的同态操作简单，而且给出的平凡门操作使得电路层结构更清晰。最后利用自举技术作为优化提升了方案的同态运算能力。
关键词：全同态加密；重线性化；模转换
中图分类号：TN918.4 **文献标识码**：A **文章编号**：1000-436X(2014)01-0173-10

Fully homomorphic encryption scheme from RLWE

TANG Dian-hua[1], ZHU Shi-xiong[1], WANG Lin[1], YANG Hao-miao[2], FAN Jia[1]
(1. Science and Technology on Communication Security Laboratory, Chengdu 610041,China;
2. College of Computer Science & Engineering, UEST of China, Chengdu 610054, China)

Abstract: Based on the somewhat homomorphic scheme of Kristin Lauter *et al*. a new technique, called Relinearization with key switching was presented. Combining this technique with modulus switching, a (leveled) fully homomorphic encryption scheme without bootstrapping from RLWE were designed. Homomorphic operations of this scheme is simple, and trivial gate operation given in the scheme can make level structure of circuit clearer. Finally, bootstrapping was used as optimization to evaluate capability of the proposed scheme.
Key words: fully homomorphic encryption; relinearization; modulus switching

1 引言

全同态加密能够在不解密的条件下实现对密文的任意计算，以致达到相应明文计算的效果。它具有广阔的应用前景，例如，云安全、加密数据库、密文检索等。“全同态加密”的概念是由 Rivest，Adleman，Dertouzos[1]于 1978 年首次提出。作为密码学界的一个公开问题，学者们对此进行了不断地探索，出现了一些方案[2~4]，但由于这些方案的同态计算能力非常有限。直至 2009 年，Gentry 基于理想格提出了第一个全同态加密方案[5,6]，才首次在理论上解决了这一公开问题。如今，全同态加密已经成为密码学的一个研究热点。

Gentry 所提方案[5,6]的核心思路是：一个自举型同态加密方案可以转化为一个全同态加密方案。所谓自举型就是方案能够同态计算自身的增强型解密电路。其构造框架为：首先构造一个 somewhat 同态加密方案，只能够进行有限次的同态计算；然后对其解密电路进行“压缩”，降低其电路深度；最后进行自举转化，获得一个自举型方案。在进行同态运算时，利用重加密（同态解密）来更新密文，降低密文中的噪声，从而取得全同态加密方案。

Gentry 的这一突破性工作掀起全同态加密的研究热潮，至此之后，出现了许多全同态加密方案。Dijk 等人基于整数理想提出了一个整数上的全同态加密方案[7]，其完全基于整数上的算术运算，概念简单，易于理解，但效率很差。Smart, Vercauteren 在 Gentry 方案的基础上，基于多项式上的素理想提出了具有相对较小的密钥和密文尺寸的全同态方案[8]，该方案加解密简单，但是密钥生成比较复杂。

收稿日期：2012-05-12；**修回日期**：2013-03-08
基金项目：国家自然科学基金资助项目（61206437）
Foundation Item: The National Natural Science Foundation of China (61206437)

Gentry，Halevi[9]对 Smart, Vercauteren 的方案进行了改进，得到一个较快的密钥生成算法和较简单的解密电路，并对方案进行了代码实现。

这些方案都是按照 Gentry 博士论文[6]中的框架来设计。这种框架具有这样的缺点：为了取得自举性，需要对 somewhat 同态方案的解密电路进行“压缩”，这需要一个额外的安全假设（稀疏子集和问题），导致方案的安全性较弱，再则在同态计算一个电路时，需要对每个电路门通过同态解密来进行密文更新，由于同态解密计算复杂度较高，导致效率很低。

2011 年，Gentry,Halevi[10]和 Brakerski, Vaikuntanathan[11]分别独立发现了一种不需要“压缩”步骤的构造方法，去除了额外的安全假设（稀疏子集和问题）。这些方案第一次偏离了 Gentry 的初始框架。之后，在 Brakerski,Vaikuntanathan 所提出的重线性化技术基础上，Gentry 提出了一个非自举的全同态加密方案[12]，其构造框架不同于 2009 年 Gentry 的初始框架：不需要“压缩”解密算法，也不需要在每个节点做“同态解密”来更新密文。而是通过“模转换”技术，更好地控制了噪声的增长，将每个门的计算复杂度做到了 $\tilde{\mathcal{O}}(\lambda L^3)$ (其中 λ 为安全参数、L 为电路深度)，然后他们使用自举作为优化，进一步降低到 $\tilde{\mathcal{O}}(\lambda^2)$，提高了全同态加密的效率。

本文以 Kristin Lauter 等人的 somewhat 方案[13]为基础，提出了带密钥转换的重线性化技术，消除了方案[13]中的“用私钥加密私钥”的循环安全假设，并以该技术作为本文全同态加密方案构造的基石。把 Gentry 的模转换技术移植到本方案中，然后结合带密钥转换的重线性化技术，提出了一个非自举的全同态加密方案。方案按照电路层进行同态操作，详细给出了平凡门（输入与输出相同电路门）、加法门、乘法门同态操作算法，这 3 种操作完全是基于多项式环上的运算，相比于文献[12]中复杂的矩阵运算，本方案的同态操作简单，易于理解。最后利用密钥转换的重线性化技术，提出了一种降低解密算法计算复杂度的新方法，使得方案可以不经过“压缩”就可以取得自举性，并以该自举作为优化，提升了本文全同态加密方案的同态能力。

2 准备知识

2.1 符号定义

本文方案将在整数多项式环 $R=\mathbb{Z}[x]/(f(x))$ 上进行构造，其中 $f(x)$ 为 n 次首一不可约多项式，一般设置为 $f(x)=x^n+1$， $n=2^m, m\in\mathbb{N}$ 。令 q 是一个奇素数，定义 $R_q=R/qR$，此环 R_q 中多项式整系数取自 $[-(q-1)/2,\cdots,(q-1)/2]$。

给定 R_q 上一个元素 $u(x)=u_0+u_1x+\cdots+u_{n-1}x^{n-1}$，可以将其写成向量形式 $u=(u_0,u_1,\cdots,u_{n-1})$，其 2-范数为 $\|u\|_2=\sqrt{\sum_{i=0}^{n-1}u_i^2}$ 和无穷范数为 $\|u\|_\infty=\max_{i=0,1,\cdots,n-1}|u_i|$。本文将利用无穷范数来分析方案的噪声以及同态计算能力（未做特别说明，$\|u\|$ 都表示为 u 的无穷范数）。R 上的乘法扩展因子 $\gamma_{\text{Mult}}=\sup\{\frac{\|u\cdot v\|}{\|u\|\cdot\|v\|},\forall u,v\in R\}$。

引理 1 （见文献[8]，引理 2）设 $n\in\mathbb{N}$，$f(x)=x^n+1$，由 $f(x)$ 生成的整数多项式环 $R=\mathbb{Z}[x]/(x^n+1)$，$\forall u,v\in R$，则有 $\|uv\|\leqslant n\|u\|\|v\|$。

本文中，规定 mod$q$ 的值取值范围为 $[-(q-1)/2,\cdots,(q-1)/2]$；log 表示以 2 为底的对数；对于 $a\leftarrow A$ 的表示：如果 A 是一个集合，$a\leftarrow A$ 表示在 A 中随机均匀选取一个元素 a。如果 A 是一个分布，$a\leftarrow A$ 表示在分布 $\mathcal{D}$ 随机抽样一个元素 a。如果 A 表示一个算法，$a\leftarrow A$ 表示运行算法 A 输出为 a。

2.2 RLWE 问题

首先定义一个分布 $A_{s,\chi}$：设 c 是 R 上的一个分布，此处 c 将取为离散高斯分布 $D_{\mathbb{Z}^n,\sigma}$ (见文献[13])。令 $s\in R_q$， $a\leftarrow R_q$ 为随机均匀选取，随机抽样一个差错 $e\leftarrow\chi$，计算 $b=a\cdot s+e$，则得到 2 个环元素 (a,b) 所构成的新分布定义为 $A_{s,\chi}$。同时将 $R_q\times R_q$ 上的均匀分布定义为 U。

Lyubaskevsky, Peikert 和 Regev 提出了 RLWE(ring learning with errors problem)问题[14]，并将此困难问题归约到多项式环理想格中的近似最短向量问题（SVP）。下面给出其定义。

定义 1 判别 RLWE 问题假设：$DRLWE_{n,q,\chi}$。由 $(a,b=as+e)$ 产生的分布 $A_{s,\chi}$ 与 $R_q\times R_q$ 上的均匀分布 U 是计算不可区分的，即 $A_{s,\chi}\approx U$。

定义 2 B 有界分布。如果一个分布 χ 满足：$\Pr_{e\leftarrow\chi}[|e|<B]\leqslant 1-negl(n)$。则称其为 B 有界分布。

引理 2 （见文献[15]，定理 4.4）设 $n\in\mathbb{N}$，对于任何一个实数 $\sigma>\omega(\sqrt{\log n})$，则有 $\Pr_{x\leftarrow D_{\mathbb{Z}^n,\sigma}}[\|x\|>\sigma\sqrt{n}\,]\leqslant 2^{-n+1}$。

2.3 同态加密

定义 3 同态加密方案。一个同态加密方案是概率多项式时间算法的一个四元组 HE=(KeyGen, Enc, Dec, Evaluate)，算法如下。

KeyGen：根据安全参数 λ，生成方案的公钥 pk、运算公钥 evk、私钥 sk。其中 evk 是运算布尔电路所需的公钥信息。

Enc：给出一个明文 $m\in\{0,1\}$，用公钥 pk 加密明文 m，得到密文 c。

Dec：输入私钥和密文 c，进行解密运算，输出明文 m'。

Evaluate：输入公钥 evk，t 输入的布尔电路 Cir（由模 2 加法门和乘法门组成），一组密文 $\vec{c}=(c_1,\cdots,c_t)$，其中 $c_i=Enc_{pk}(m_i)$。输出 $c^*=Evaluate\ (evk,Cir,\vec{c})$，且满足 $Dec\ (sk,c^*)=Cir\ (m_1,\cdots,m_2)$。

定义 4 $\mathcal{C}$-同态。设 $\mathcal{C}$ 是一个布尔电路的集合，HE 是一个同态加密方案，任取一个电路 $Cir\in\mathcal{C}$，设其输入线有 t 个。如果对任意的一组明文 $m_1,\cdots,m_t$ 和所对应的一组密文 $\vec{c}=(c_1,\cdots,c_t)$（其中 $c_i=Enc_{pk}(m_i)$），满足以下条件

$$\Pr[Dec_{sk}(Evalute(evk,Cir,(c_1,\cdots,c_t)))=Cir(m_1,\cdots,m_t)]=1-negl(\lambda)$$

则称该方案为 $\mathcal{C}$-同态，或者方案对于一个电路集合 $\mathcal{C}$ 是正确的。

定义 5 紧同态加密。如果存在一个多项式 $g=g(\lambda)$，使得 HE 方案的 Evaluate 算法的输出比特长度不超过 g，则称 HE 是一个紧同态加密方案。

注意：g 与所运算的电路 Cir 以及输入密文数无关。

定义 6 全同态加密。一个方案 HE 对所有的电路既是紧的，又是同态的，则称其是一个全同态加密方案。

本文所考虑的方案为单比特加密，即明文空间为{0,1}。下面给出单比特同态加密的 IND-CPA 安全。

定义 7 如果对于任意一个多项式时间敌手 $\mathcal{A}$，其在攻击游戏中的优势为

$$Adv_{CPA}[\mathcal{A}]=\left|\begin{matrix}\Pr[\mathcal{A}(pk,evk,HE.Enc_{pk}(0))=1]\\-\Pr[(pk,evk,HE.Enc_{pk}(1))=1]\end{matrix}\right|=negl(\lambda)$$

则称该同态加密方案是 IND-CPA 安全的。

3 Somewhat 同态加密方案

Somewhat 同态加密方案只能够进行有限次的同态操作，但可以将其转化为全同态加密方案，它是构造全同态的基础。本节描述 Kristin Lauter 等人的 Somewhat 同态加密方案，并分析其同态加和同态乘操作，然后提出了带密钥转换的重线性化技术，以及对 Gentry“模转换”技术的移植。本节对 somewhat 同态加密方案的分析将为第 4 节全同态加密方案的构造做准备。

3.1 方案描述

SHE.Setup($1^\lambda,1^\mu$)：选取一个 μ bit 的奇数 q，并建立多项式环 R_q 和离散高斯分布 χ，设多项式 x^n+1 的次数 $n=n(\lambda,\mu)$，离散高斯分布 $\chi=\chi(\lambda,\mu)$，以致方案所基于的 RLWE 问题对已知攻击是 2^λ 级安全的，令 $R=\mathbb{Z}[x]/(x^n+1)$，$R_q=R/qR$，公共参数 $params=(q,n,\chi)$。

SHE.KeyGen($params$)：在分布 χ 上随机选择一个元素 $s\leftarrow\chi$ 作为私钥，然后在 R_q 上随机均匀选取一个元素 $a_1\leftarrow R_q$，同时在分布 χ 选取一个差错 $e\leftarrow\chi$，计算 $a_0=-a_1s+2e$。设置私钥 $sk=s$，公钥 $pk=(a_0,a_1)$。

SHE.Enc(pk,m)：给定单比特消息 $m\in\{0,1\}$，将其转化为 R_2 上一个多项式，为了方便亦记为 m，即其常数项系数为消息比特，其余系数为 0。在分布 χ 上随机选取 $u\leftarrow\chi$，$g\leftarrow\chi$ 和 $r\leftarrow\chi$，根据公钥 $pk=(a_0,a_1)$ 计算密文为 $c_0=a_0u+2g+m, c_1=a_1u+2r$。输出密文 $ct=(c_0,c_1)$。

SHE.Dec(sk,ct)：根据给定的密文 $ct=(c_0,c_1)$，利用私钥 $sk=s$，计算 $m'=((c_0+c_1s)\bmod q)\bmod 2$。

3.2 解密正确性

将解密算法看成一个关于私钥 s 的线性函数 $f_{ct}(s)$

$$\begin{aligned}f_{ct}(s)&=c_0+c_1s\\&=a_0u+2g+m+(a_1u+2r)s\\&=-(a_1s+2e)u+2g+m+a_1us+2rs\\&=m+2(g+eu+rs)\\&\triangleq m+2\tilde{e}\end{aligned}$$

其中的加法和乘法都是环 R_q 上的运算，并将 $m+2\tilde{e}$ 称为噪声，如果噪声尺寸满足 $\|m+2\tilde{e}\|<q/2$，再对 $f_{ct}(s)$ 模 2 将正确地恢复出消息 m。本方案虽

然是单比特加密，但其实很容易扩展到多比特加密，只需要将方案中的 2 替换成一个更大的数值 t。

3.3 同态加与同态乘操作

设 2 个消息 m 与 m' 的加密分别为 $ct=(c_0,c_1)$，$ct'=(c_0',c_1')$。下面将分析如何根据 ct 和 ct' 来计算消息 $m+m'$ 和 mm' 的加密。根据上述对解密算法正确性可知

$$f_{ct}(s)=c_0+c_1s=m+2\tilde{e},\quad f_{ct'}(s)=c_0'+c_1's=m'+2\tilde{e}'$$

1) 同态加

将这 2 个关于 s 多项式相加

$$\begin{aligned}f_{ct}(s)+f_{ct'}(s)&=c_0+c_1s+c_0'+c_1's\\&=(c_0+c_0')+(c_1+c_1')s\\&=(m+m')+2(\tilde{e}+\tilde{e}')\end{aligned}$$

按照解密的计算形式，很容易看出其同态加之后的密文为 $ct_{\text{Add}}=(c_0+c_0',c_1+c_1')$，为了保证解密的正确性，需要满足 $\|(m+m')+2(\tilde{e}+\tilde{e}')\|<q/2$。

同态乘

将这 2 个关于 s 多项式相乘，得到

$$\begin{aligned}f_{ct}(s)f_{ct'}(s)&=(c_0+c_1s)(c_0'+c_1's)\\&=c_0c_0'+(c_0c_1'+c_0'c_1)s+c_1c_1's^2\\&=(m+2\tilde{e})(m'+2\tilde{e}')\\&=mm'+2(\tilde{e}m'+\tilde{e}'m+\tilde{e}\tilde{e}')\end{aligned}$$

其结果是一个关于 s 的一个二次多项式。可以看成密文为 $ct_{\text{Mult}}=(c_0c',c_0c_1'+c_0'c_1,c_1c_1')$，私钥为 $s\vec{k}=(1,s,s^2)$，在解密时进行内积 $<ct_{\text{Mult}},s\vec{k}>=c_0c'+(c_0c_1'+c_0'c_1)s+c_1c_1's^2$，然后模 2，解出消息 mm'，（为了正确解密，同样需要满足 $\|mm'+2(\tilde{e}m'+\tilde{e}'m+\tilde{e}\tilde{e}')\|<q/2$）。由此可见，经过一次同态乘法之后，密文由 2 个环元素变为 3 个，如此随着同态乘法的不断进行，导致密文尺寸随着乘法深度的增加成指数增长。

文献[13]中提出了一个重线性化技术，将密文的环元素始终控制在 2 个，使得密文尺寸独立于运算数目，但是其重线性化之后的解密密钥没有发生改变，而且需要“私钥加密私钥”的循环安全假设。下一小节将给出一个带密钥转换的重线性化技术，去除这种循环安全假设的要求。

3.4 密钥转换

1) 带密钥转换的重线性化

同态乘法产生的一个密文含有 3 个环元素，设为 $ct_{\text{Mult}}=(c_0,c_1,c_2)$，其对应的私钥为 s。下面通过带密钥转换的重线性化技术，将其密文 $ct_{\text{Mult}}=(c_0,c_1,c_2)$ 转化为 2 个环元素的密文 $ct_{\text{Mult}}^{\text{relin}}=(c_0^{\text{relin}},c_1^{\text{relin}})$，而且其对应于一个新的私钥 s'。在进行转化之前，需要一些辅助信息 $\Lambda=\{h_i,l_i\}_{i=0}^{\lceil\log q\rceil-1}$，其计算如下

$$h_i=(a_i,b_i=-(a_is'+2e_i)+2^is^2)\ i=0,1,2,\cdots,\lceil\log q\rceil-1$$

$$l_i=(a_i',b_i'=-(a_i's'+2e_i')+2^is)\ i=0,1,2,\cdots,\lceil\log q\rceil-1$$

其中，a_i,a_i' 是均匀分布独立随机选自 R_q，e_i,e_i' 是按 χ 分布独立随机选自 R_q。注意本节中的运算都是在环 R_q 上的。

安全性假设：h_i，l_i 这种形式的分布与 $R_q\times R_q$ 上的均匀分布是不可区分的，这样即使攻击者在知道 Λ 的条件下，方案仍是安全的。

带密钥转换的重线性化转化过程如下。

①将密文 $ct_{\text{Mult}}=(c_0,c_1,c_2)$ 中的多项式 c_1,c_2 按照成二进制表示，即 $c_1=\sum_{i=0}^{\lceil\log q\rceil-1}2^ic_{1,i}$，$c_2=\sum_{i=0}^{\lceil\log q\rceil-1}2^ic_{2,i}$，其中 $c_{1,i},c_{2,i}\in R_2$。

②按照下列式子计算 c_0^{reline}，c_1^{reline}。

$$c_0^{\text{reline}}=c_0+\sum_{i=0}^{\lceil\log q\rceil-1}c_{1,i}b_i'+\sum_{i=0}^{\lceil\log q\rceil-1}c_{2,i}b_i$$

$$c_1^{\text{reline}}=\sum_{i=0}^{\lceil\log q\rceil-1}c_{1,i}a_i'+\sum_{i=0}^{\lceil\log q\rceil-1}c_{2,i}a_i$$

③输出新密文 $ct_{\text{Mult}}^{\text{relin}}=(c_0^{\text{relin}},c_1^{\text{relin}})$。

为了验证该转化过程的正确性，使用新私钥 s' 对新密文 $ct_{\text{Mult}}^{\text{relin}}$ 进行解密

$$\begin{aligned}c_0^{\text{reline}}+c_1^{\text{reline}}s'&=c_0+\sum_{i=0}^{\lceil\log q\rceil-1}c_{1,i}b_i'+\sum_{i=0}^{\lceil\log q\rceil-1}c_{2,i}b_i+\\&\quad(\sum_{i=0}^{\lceil\log q\rceil-1}c_{1,i}a_i'+\sum_{i=0}^{\lceil\log q\rceil-1}c_{2,i}a_i)s'\\&=c_0+\sum_{i=0}^{\lceil\log q\rceil-1}c_{1,i}2^is+\sum_{i=0}^{\lceil\log q\rceil-1}c_{2,i}2^is^2-2\\&\quad(\sum_{i=0}^{\lceil\log q\rceil-1}c_{1,i}e'+\sum_{i=0}^{\lceil\log q\rceil-1}c_{2,i}e_i)\\&=c_0+c_1s+c_2s^2-2(\sum_{i=0}^{\lceil\log q\rceil-1}c_{1,i}e'+\sum_{i=0}^{\lceil\log q\rceil-1}c_{2,i}e_i)\\&=mm'+2e-2(\sum_{i=0}^{\lceil\log q\rceil-1}c_{1,i}e'+\sum_{i=0}^{\lceil\log q\rceil-1}c_{2,i}e_i)\end{aligned}$$

由上式可以看出，该转化过程引入了一个新噪

声项 $2(\sum_{i=0}^{\lceil \log q \rceil -1} c_{1,i}e' + \sum_{i=0}^{\lceil \log q \rceil -1} c_{2,i}e_i)$，则密文 $ct_{\text{Mult}}^{\text{relin}}$ 的噪声大小为：$\| mm' + 2e - 2(\sum_{i=0}^{\lceil \log q \rceil -1} c_{1,i}e' + \sum_{i=0}^{\lceil \log q \rceil -1} c_{2,i}e_i) \| < \| mm' + 2e \| + 4n \log qB$。当该噪声的无穷范数小于 $q/2$ 时，再进行摸 2，解密出消息 mm'。

2) 空白密钥转换

之所以称为“空白”密钥转换，是因为其未涉及同态运算。只是将对应于私钥 s 的密文 $ct = (c_0, c_1)$ 转化为对应于新私钥 s' 的新密文 $ct^{\text{next}} = (c_0^{\text{next}}, c_1^{\text{next}})$，且满足 $Dec(s, ct) = Dec(s', ct^{\text{next}})$。转化过程同样需要辅助信息 $\Lambda = \{h_i, l_i\}_{i=0}^{\lceil \log q \rceil -1}$，其具体过程如下。

① 将密文 $ct = (c_0, c_1)$ 中的 c_1 按二进制表示，即 $c_1 = \sum_{i=0}^{\lceil \log q \rceil -1} 2^i c_{1,i}$，其中 $c_{1,i} \in R_2$。

② 计算 c_0^{next} 和 c_1^{next}。

$$c_0^{\text{next}} = c_0 + \sum_{i=0}^{\lceil \log q \rceil -1} c_{1,i} b_i'$$

$$c_1^{\text{next}} = \sum_{i=0}^{\lceil \log q \rceil -1} c_{1,i} a_i'$$

③ 输出新密文 $ct^{\text{next}} = (c_0^{\text{next}}, c_1^{\text{next}})$。

同理，对“空白密钥转换”进行正确性验证

$$\begin{aligned} c_0^{\text{next}} + c_1^{\text{next}} s' &= c_0 + \sum_{i=0}^{\lceil \log q \rceil -1} c_{1,i} b_i' + \sum_{i=0}^{\lceil \log q \rceil -1} c_{1,i} a_i' s' \\ &= c_0 + \sum_{i=0}^{\lceil \log q \rceil -1} c_{1,i}(-(a_i' s' + 2e_i') + 2^i s) + \\ &\quad \sum_{i=0}^{\lceil \log q \rceil -1} c_{1,i} a_i' s' \\ &= c_0 + c_1 s - 2 \sum_{i=0}^{\lceil \log q \rceil -1} c_{1,i} e_i' \\ &= m + 2(e - \sum_{i=0}^{\lceil \log q \rceil -1} c_{1,i} e_i') \end{aligned}$$

由上计算过程可以看出，新密文 ct^{next} 引入了一个新的噪声项 $2\sum_{i=0}^{\lceil \log q \rceil -1} c_{1,i}e_i'$，则其噪声大小为：$\| m + 2(e - \sum_{i=0}^{\lceil \log q \rceil -1} c_{1,i}e_i') \| < \| m + 2e \| + 2n \log qB$，当其小于 $q/2$ 时，进行模 2 便可以解密出 m。

3.5 降低解密计算复杂度

密钥转换技术，不仅能够在同态运算中始终控制密文为 2 个环元素，而且还具有降低解密计算复杂度的优点。下面将给出该方法，以及分析其降低解密计算复杂度的原理。

环 R_q 上的运算可以分解为：先进行 R 上的多项式运算，然后再进行模 q。设 2 个 R_q 上的元素为 u, v，且 v 取自分布 χ。

$$u = u_0 + u_1 x + \cdots + u_{n-1} x^{n-1} \qquad v = v_0 + v_1 x + \cdots + v_{n-1} x^{n-1}$$

把它们写成向量的形式 $u = (u_0, u_1, \cdots, u_{n-1})$，$v = (v_0, v_1, \cdots, v_{n-1})$；则环 R_q 上的运算 $u \cdot v$ 可以表示如下

$$uv = (u_0, u_1, \cdots, u_{n-1}) \begin{bmatrix} v_0 & v_1 & v_2 & \cdots & v_{n-1} \\ -v_{n-1} & v_0 & v_1 & \cdots & v_{n-2} \\ -v_{n-2} & -v_{n-1} & v_0 & \cdots & v_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -v_1 & -v_2 & -v_3 & \cdots & v_0 \end{bmatrix} \triangleq uV$$

即环 R_q 中 2 个元素相乘，相当于并行进行了 n 次向量内积。一次内积产生了 $n\lceil \log B \rceil$ 个 $\lceil \log q \rceil + \lceil \log B \rceil - 1$ bit 二进制数相加，应用“Three-for-two”技术[16]，整个计算需要的电路深度为 $O(\log n + \log \log B)$。

如果将向量 $v = (v_0, v_1, \cdots, v_{n-1})$ 中最后 $n - n_1$ 连续分量取 0，即只有前 n_1 个分量是取自分布 χ。这样在计算 uv 时，就可以知道矩阵 $\boldsymbol{V}$ 中哪些位置为零，为零处就不需要进行乘法运算。其矩阵运算如下

$$uv = (u_0, u_1, \cdots, u_{n-1}) \begin{bmatrix} v_0 & v_1 & v_2 & \cdots & 0 \\ 0 & v_0 & v_1 & \cdots & 0 \\ 0 & 0 & v_0 & \cdots & v_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -v_1 & -v_2 & -v_3 & \cdots & v_0 \end{bmatrix}$$

可以看到，在每次向量内积运算中，所需要相加的数目就减少到 $n_1\lceil \log B \rceil$，其需要的电路深度就为 $O(\log n_1 + \log \log B)$，把此方法应用于本文方案的解密算法中，通过密钥转换技术，由于 $n_1 < n$，就可以降低解密算法的电路深度。

3.6 模转换技术

设密文 $ct = (c_0, c_1)$，解密过程：$Dec(ct, s) = ((c_0 + c_1 s) \bmod q) \bmod 2$。下面给出模转换技术，将

模 q 转化为模 p，并保证其在相同密钥 s 下解密的消息相同。

定义 8 算法 Scale。对于一个整数向量 x 和整数 q,p,t，定义 $x' \leftarrow Scale(x,q,p,t)$，是靠近 $(p/q)x$ 的一个 R 上的向量，且满足 $x' = \mathrm{x} \bmod t$。

例如：x=(74,37)，q=83，p=17，t=2 保留一位小数 $(p/q)\cdot x$=(17/83)·(74,37)=(15.2,7.6)，为了保证 $x' = x \bmod 2$，取 x'=(16,7)

定理 1 在环 $R = \mathbb{Z}[x]/(x^n+1)$ 上，设 $q>p>2$，且满足 $q = p = 1 \bmod 2$。令密文 $ct = (c_0,c_1) \in R_q \times R_q$。调用算法得到 $ct' \leftarrow Scale(ct,q,p,2)$，其中 $ct' = (c_0',c_1')$。则对于满足 $\|[c_0 + c_1 s]_q\| < q/2 - q/p(1+\|s\|)$ 的任何一个 $s \in R_q$，有以下式子成立

$$[c_0' + c_1' s]_q = [c_0 + c_1 s]_p \bmod 2 \text{ 且}$$

$$\|[c_0' + c_1' s]_p\| < (p/q)\|[c_0 + c_1 s]_q\| + 1 + n \cdot \|s\|$$

证明 存在某个 $k \in \mathbb{Z}$，使得 $e_q = [c_0 + c_1 s]_p = c_0 + c_1 s - kq$。要求对于同样的 k，也使得 $e_p = [c_0' + c_1' s]_p = c_0' + c_1' s - kp$ 成立，那么就需要满足 $\|e_p\| < p/2$。

$$\begin{aligned}
\|e_p\| &= \|c_0' + c_1' s - kp\| \\
&= \|p/q(c_0 + c_1 s) - kp + (c_0' + c_1' s) - p/q(c_0 + c_1 s)\| \\
&\leqslant \|p/q(c_0 + c_1 s) - kp\| + \|(c_0' + c_1' s) - p/q(c_0 + c_1 s)\| \\
&\leqslant p/q\|(c_0 + c_1 s) - kq\| + \|c_0' - (p/q)c_0\| \\
&\qquad + \|(c_1' - (p/q)c_1)s\| \\
&\leqslant (p/q)\|e_q\| + 1 + n\|s\| \\
&< p/2
\end{aligned}$$

为了使此不等式成立，需要满足：$\|e_q\| < q/2 - q/p(1+n\|s\|)$。由于 $q = p = 1 \bmod 2$，所以 $(c_0 + c_1 s - kq) = (c_0' + c_1' s - kp) \bmod 2$，即 $[c_0' + c_1' s]_q = [c_0 + c_1 s]_p \bmod 2$。 □

从该定理可以看出，通过调用算法 $ct' \leftarrow Scale(ct,q,p,2)$，将密文 ct 转化为新密文 ct'，同时其对应的模值由 q 转化为数值较小的 p，并保证了对应的消息不变。其中最重要优点的是：此转换技术降低了密文中的噪声，将噪声大小由 $\|e_q\|$ 降低到 $(p/q)\|e_q\| + 1 + n\|s\|$（注意 $p<q$），为减低噪声提供了一个非常高效的方法。

4 非自举的全同态加密方案

第 3 节所分析的技术，为本节全同态方案的构造做了充分的准备。本节将按 Brakerski,Gentry 所提出的全同态加密构造的新方法[12]，设计一个非自举的全同态加密方案，最后将自举作为本方案的优化，进一步提升其同态运算能力。

4.1 方案描述

本节将按照新的构造框架，利用以上所分析的“密钥转换”和“模转换”技术来构造一个基于 RLWE 的全同态加密方案。设参数 L 是本方案所需要的同态运算能力，即所能够同态计算布尔电路的深度。具体方案如下。

FHE.Setup(1^λ,1^L)：输入安全参数 λ，以及所要求方案能处理的电路层数 L。由此生成 $L+1$ 个模值 $q_i, i = 0,1,\cdots,L$，其各自的比特数为 $\mu_i = \mu_i(\lambda,L)$。设 $n = n(\lambda,L)$，生成一个多项式环 $R = \mathbb{Z}[x]/(x^n+1)$，每个电路层所用的多项式环相同，都为 R，只是所用的模值 q_i 不同（即第 i 电路层，使用的模值为 q_i）。对于噪声分布，每一电路层都采用相同的离散高斯分布 $\chi = \chi(\lambda,L)$。公共参数 $params = (\{q_j\}_{j=0}^L, n, \chi)$

FHE.KeyGen($params$)：为了建立 $L+1$ 层密钥，以致对应于 L 层的电路深度。首先在分布 χ 上独立选取密钥 $s_0,s_1,\cdots,s_L$，在 R_{q_L} 上随机均匀选取 $a_1 \leftarrow R_{q_L}$，同时在分布 χ 选取差错 $e \leftarrow \chi$，计算 $a_0 = -a_1 s_0 + 2e$。然后计算 $\psi_{\tau_i,i} = (h_{\tau_i,i\to i+1}, l_{\tau_i,i\to i+1})_{i=0}^L$

$$h_{\tau_i,i\to i+1} = (a_{\tau_i,i}, b_{\tau_i,i} = -(a_{\tau_i,i} \cdot s_{i+1} + 2e_{\tau_i,i}) + 2^{\tau_i} s_i^2),$$

$$\tau_i = 0,1,\cdots,\lceil \log q_i \rceil - 1$$

$$l_{\tau_i,i\to i+1} = (a'_{\tau_i,i}, b'_{\tau_i,i} = -(a'_{\tau_i,i} \cdot s_{i+1} + 2e'_{\tau_i,i}) + 2^{\tau_i} s_i),$$

$$\tau_i = 0,1,\cdots,\lceil \log q_i \rceil - 1$$

对于每个 i，$h_{\tau_i,i\to i+1}$ 和 $l_{\tau_i,i\to i+1}$ 的计算都是在 R_{q_i} 上的，其中 $a_{\tau_i,i}, a'_{\tau_i,i} \leftarrow R_{q_i}$，$e_{\tau_i,i}, e'_{\tau_i,i} \leftarrow \chi$ 都是独立选取的。设置私钥 $sk = (s_0,s_1,\cdots,s_L)$，公钥 $pk = (a_0,a_1)$，运算密钥 $evk = \{h_{\tau_i,i\to i+1}, l_{\tau_i,i\to i+1}\}_{i=1}^L$。

FHE.Enc(pk,m)：在分布 χ 上随机选取元素 $u \leftarrow \chi$，$g \leftarrow \chi$，$r \leftarrow \chi$。根据公钥 pk 计算密文为 $c_0 = a_0 u + 2g + m$，$c_1 = a_1 u + 2r$。输出密文 $ct = (c_0,c_1,0)$，其中 0 表示密文所处的电路层。在本方案中密文都有额外的信息来标识密文所处的

电路层，例如密文形式为 $ct=(c_0,c_1,j)$，表示该密文处于电路第 j 层。

FHE.Dec(sk,c)：假设密文为 $ct=(c_0,c_1,j)$，其对应于私钥 s_j，计算 $m'=((c_0+c_1s_j)\bmod q_j)\bmod 2$。

下面来分析同态操作：将电路中的门分为 3 种：平凡门、加法门、乘法门。其中平凡门是指入度出度都为 1，且输入输出相同的电路门。引入平凡门主要是有助于对电路的分层，使得层结构更清晰。

FHE.Triv(evk,ct)：此算法是将密文 $ct=(c_0,c_1,w)$ 转化到下一电路层密文 $ct^{*'}=(c_0^{*'},c_1^{*'},w+1)$，并保证所对应的消息不变，但是其未涉及同态加和同态乘操作，只是处理平凡门的密文层变化。算法如下。

1) 将密文 $ct'=(c_0',c_1')$ 中的 c_1' 按二进制表示，即 $c_1'=\sum_{i=0}^{\lceil\log q_w\rceil-1}2^i\cdot c_{1,i}'$，其中 $c_{1,i}'\in R_2$。

2) 按照下列式子计算 c_0^* 和 c_1^*，得到 $ct^*=(c_0^*,c_1^*,w)$

$$c_0^*=c_0'+\sum_{i=0}^{\lceil\log q_w\rceil-1}c_{1,i}'b_{i,w}'\ (\bmod q_w)$$

$$c_1^*=\sum_{i=0}^{\lceil\log q_w\rceil-1}c_{1,i}'a_{i,w}'\ (\bmod q_w)$$

3) 调用模转化算法，输出 $ct^{*'}\leftarrow Scale(ct^*,q_w,q_{w+1},2)$，即密文 $ct^{*'}=(c_0^{*'},c_1^{*'},w+1)$。

通过该算法，就将密文 ct' 由第 w 层转化到为第 $w+1$ 层的新密文 $ct^{*'}=(c_0^{*'},c_1^{*'},w+1)$。如果一个密文需要跳变的层数大于 1，则可以通过多次使用该算法，取得所需的密文。

FHE.Add(evk,ct,ct')：假设已经得到 2 个电路层相同的密文 $ct=(c_0,c_1,w)$ 和 $ct'=(c_0',c_1',w)$，如果密文电路层不同，可以使用算法 FHE.Triv 将其调整到相同。

1) 进行密文的加运算：$c_0^+=(c_0+c_0')\bmod q_w$ $c_1^+=(c_1+c_1')\bmod q_w$，得到密文 $ct^+=(c_0^+,c_1^+,w)$。

注意：此处同态加的入度不一定是 2，也可以是多个。其实将加法门的入度设定为 2，由此将电路分层，将导致更多噪声的引入。

2) 调用算法 FHE.Triv(evk,ct^+) 将密文 $ct^+=(c_0^+,c_1^+,w)$ 转化为第 $w+1$ 层的密文 $ct^{+'}=(c_0^{+'},c_1^{+'},w+1)$ (注意其层标识增加了 1)，输出密文 $ct^{+'}$，即为同态加后的密文。

FHE.Mult(evk,ct,ct')：同样设两密文的标识信息相同，如果不同，可以通过算法 FHE.Triv 进行调整。其具体步骤如下。

1) 进行密文的乘法运算：$ct_{\text{Mult}}=(c_0c',c_0c_1'+c_0'c_1,c_1c_1')=(c_0^*,c_1^*,c_2^*)$，其中都是 R_{q_w} 上的运算。

2) 将密文 $ct_{\text{Mult}}=(c_0^*,c_1^*,c_2^*)$ 中的多项式 c_1^*,c_2^* 按照二进制表示，即 $c_1^*=\sum_{i=0}^{\lceil\log q_w\rceil-1}2^i\cdot c_{1,i}^*$，$c_2^*=\sum_{i=0}^{\lceil\log q_w\rceil-1}2^ic_{2,i}^*$，其中 $c_{1,i}^*,c_{2,i}^*\in R_2$。

3) 进行重线性化，计算按照下列式子计算 c_0^{reline}，c_1^{reline}，得到密文 $ct^\times=(c_0^\times,c_1^\times,w)$

$$c_0^\times=c_0^*+\sum_{i=0}^{\lceil\log q_w\rceil-1}c_{1,i}^*b_{i,w}'+\sum_{i=0}^{\lceil\log q_w\rceil-1}c_{2,i}^*b_{i,w}\ (\bmod q_w)$$

$$c_1^\times=\sum_{i=0}^{\lceil\log q_w\rceil-1}c_{1,i}^*a_{i,w}'+\sum_{i=0}^{\lceil\log q_w\rceil-1}c_{2,i}^*a_{i,w}\ (\bmod q_w)$$

4) 调用模转换算法 $ct^{\times'}\leftarrow Scale(ct^\times,q_w,q_{w+1},2)$，输出密文 $ct^{\times'}=(c_0^{\times'},c_1^{\times'},w+1)$。

4.2　自举优化

自举是非常有用的技术，本节将利用密钥转换技术，使得方案取得自举性。由此将只有 L 层的同态运算能力提升到任意层。如图 1 所示。

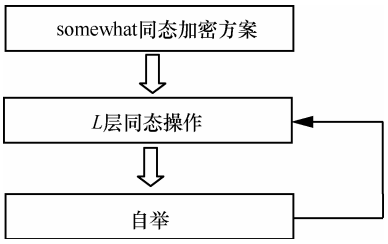

图 1　L 层的同态运算能力提升

经过 L 层电路的同态运算之后，设得到的密文为 $ct=(c_0,c_1,L)$，其对应的私钥为 s_L，模值为 q_L。使用一个结构较特殊的私钥 $s=(s[1],s[2],\cdots,s[n_1],0,\cdots,0)$，即 s 最后 $n-n_1$ 个元素全为零，而前 n_1 个元素取自离散高斯分布 $D_{\mathbb{Z}^{n_1},\sigma}$。在密钥转换前，需要一些辅助信息 $T=\{l_i\}_{i=0}^{\lceil\log q_L\rceil-1}$

$$l_\tau=(a_\tau',b_\tau'=-(a_\tau's_L+2e_\tau')+2^\tau s),$$

$$\tau=0,1,\cdots,\lceil\log q_L\rceil-1$$

其中，$a'\leftarrow R_{q_L}$，$e_\tau'\leftarrow\chi$，且其运算是多项式环 R_{q_L} 上的。

其转换 $ct^{\text{new}}\leftarrow\text{Trans}(ct,T)$ 算法如下。

1) 将密文 $ct=(c_0,c_1,L)$ 中的 c_1 按二进制表示，即 $c_1=\sum_{i=0}^{\lceil \log q_L \rceil -1} 2^i c_{1,i}$，其中 $c_{1,i}\in R_2$。

2) 按照下列式子计算 c_0^{new} 和 c_1^{new}，得到 $ct^{\text{new}}=(c_0^{\text{new}},c_1^{\text{new}})$

$$c_0^{\text{new}}=c_0+\sum_{i=0}^{\lceil \log q_L \rceil -1} c_{1,i}b_i' \pmod{q_L}$$

$$c_1^{\text{new}}=\sum_{i=0}^{\lceil \log q_L \rceil -1} c_{1,i}a_i' \pmod{q_L}$$

此时所获得的密文 ct^{new} 所对应的解密算法为：$Dec(ct^{\text{new}},s)=((c_0^{\text{new}}+c_1^{\text{new}}\cdot s) \bmod q_L) \bmod 2$。由 3.5 节的分析可知其对应的解密电路深度为 $O(\log n_1+\log\log B)$。可以选择合适的参数使得 $L\geqslant O(\log n_1+\log\log B)$，通过重加密（同态解密），将密文更新到这 L 层中的某一层，然后继续进行同态运算。

5 安全性证明

本文所提方案 FHE 是一个层次化的全同态加密方案，其安全性是基于 RLWE 问题假设。下面给出定理 5.1，将 FHE 的语义安全性归约到一系列的 DRLWE 问题：$\{\text{DRLWE}_{n,q_i,\chi}\}_{i=0}^{L}$。

定理 2 在 $\{\text{DRLWE}_{n,q_i,\chi}\}_{i=0}^{L}$ 问题假设下，本方案 FHE 是 CPA 安全的。特别地，如果 $\{\text{DRLWE}_{n,q_i,\chi}\}_{i=0}^{L}$ 都是 (t,ε) 困难的，那么方案 FHE 是 $(t-poly(\lambda),(L+2)\varepsilon)$-CPA 安全的。

证明 设 $\mathcal{A}$ 是对 FHE 的一个 IND-CPA 攻击者，$Adv_H[\mathcal{A}]$ 表示 $\mathcal{A}$ 在 hybrid H 中的攻击优势。在本安全性归约证明中，采用一系列混合的证明方法，如下。

Hybrid H_{L+1}：该 Hybrid 就是 $\mathcal{A}$ 对方案 FHE 的 IND-CPA 攻击游戏，其中攻击者获得由 FHE.KeyGen 算法产生的公钥 pk，evk。然后使用 FHE.Enc 产生 0 或者 1 的加密，则 $\mathcal{A}$ 在 H_{L+1} 的优势为

$$Adv_{H_{L+1}}[\mathcal{A}]=\left|\begin{matrix}\Pr[\mathcal{A}(pk,\text{FHE.Enc}(=0))\\ =1]-\Pr[\mathcal{A}(pk,\text{FHE.Enc}(1))=1]\end{matrix}\right|=\varepsilon$$

Hybrid H_l：H_l 与 H_{l+1} 基本是相同，除了评估公钥 evk 中 $\psi_{\tau_l,l}$ 的产生。在这里，所使用的 $\{\psi_{\tau_l,l}\}_{\tau_l=0}^{\lceil \log q_l \rceil -1}$ 并不按照方案中的那样生成，而是取自一个均匀分布，即 $\psi_{\tau_l,l}\leftarrow R_{q_l}\times R_{q_l}$。

那么就存在一个攻击者 $\mathcal{B}_l$ 在时间 $t+\text{p}oly(\lambda)$ 解决 $DRLWE_{n,q_l,\chi}$ 的优势为

$$DRLWE_{n,q_l,\chi}Adv[\mathcal{B}_l]\geqslant\left|Adv_{H_l}[\mathcal{A}]-Adv_{H_{l+1}}[\mathcal{A}]\right|$$

通过 H_{l+1} 到 H_l 这样的方式，不断将运算公钥中的 $\psi_{\tau_i,i}=(h_{\tau_i,i\to i+1},l_{\tau_i,i\to i+1})$ 替换成 $R_{q_l}\times R_{q_l}$ 上随机均匀选取的元素，最后在 H_1 中，运算公钥已经全部成为随机均匀分布上的元素。

Hybrid H_0：H_0 与 H_1 相同，除了公钥中 a_0 的选取。在 H_0 的公钥中的 a_0 是在 R_{q_0} 中均匀选取，而不是以 $-a_1s_0+2e$ 的方式产生。在 $DRLWE_{n,q_0,\chi}$ 假设下，H_0 与 H_1 是不可区分的。则存在对 $DRLWE_{n,q_0,\chi}$ 的一个攻击者 $\mathcal{B}_0$，在时间 $t+poly(\lambda)$ 的攻击优势为

$$DRLWE_{n,q_0,\chi}Adv[\mathcal{B}_0]\geqslant\left|Adv_{H_0}[\mathcal{A}]-Adv_{H_1}[\mathcal{A}]\right|$$

攻击 $\mathcal{B}_0$ 可以从 RLWE 预言机中随机抽样 a_0，然后使用 (a_0,a_1) 作为公钥。如果抽样来自分布 $A_{s,\chi}$，那么 a_0 就像 H_1 中产生，如果抽样来自随机均匀分布，那么 a_0 就如 H_0 中所产生。

Hybrid H_{rand}：H_{rand} 与 H_0 相同，除了其密文的产生。在 H_0 中密文是由 $c_0=a_0u+m$，$c_1=a_1u+2r$ 生成的，而 H_{rand} 的密文为均匀随机选自 $R_{q_0}\times R_{q_0}$，由于 a_0，a_1，u 也都是随机选自 R_{q_0}。则 $(a_0u+2g+m,a_1u+2r)$ 与 $R_{q_0}\times R_{q_0}$ 上的均匀分布统计不可区分，设其区分概率为 ε。

$$\left|Adv_{H_0}[\mathcal{A}]-Adv_{H_{\text{rand}}}[\mathcal{A}]\right|\leqslant\varepsilon$$

在 H_{rand} 中，公钥 pk，运算公钥 evk 以及密文都是随机均匀选取的，并与消息 m 无关。则有 $Adv_{H_{\text{rand}}}[\mathcal{A}]=0$。

综上所述

$$\begin{aligned}Adv_{CPA}[\mathcal{A}]\leqslant&\left|Adv_{H_{\text{L}+1}}[\mathcal{A}]-Adv_{H_{\text{L}}}[\mathcal{A}]\right|+\cdots+\\&\left|Adv_{H_{l+1}}[\mathcal{A}]-Adv_{H_l}[\mathcal{A}]\right|+\cdots+\\&\left|Adv_{H_0}[\mathcal{A}]-Adv_{H_{\text{rand}}}[\mathcal{A}]\right|\\\leqslant&\sum_{l=0}^{L}DRLWE_{n,q_l,\chi}Adv[\mathcal{B}_l]+\varepsilon\\\leqslant&(L+2)\varepsilon\end{aligned}$$

6 参数选择

本文所提方案的安全性是基于 RLWE 问题，目前对 RLWE 问题的参数设置主要是参考 Lindner,

Peikert 对 LWE 问题的研究成果[17]。本节也将以此对方案 FHE 进行参数选择。

6.1 RLWE 问题的参数选择

RLWE 问题所涉及的参数有：环 R 的多项式次数 n，模值 q，离散高斯分布 $D_{\mathbb{Z},\sigma}$。所以 RLWE 的安全性主要是由 (n,q,σ) 决定。

方案中使用的分布 χ 为 $D_{\mathbb{Z},\sigma}^{n}$，即各个分量按照 $D_{\mathbb{Z},\sigma}$ 进行抽样。离散高斯分布 $D_{\mathbb{Z},\sigma}$ 的概率密度函数为 $\exp(-\pi|x|^2/\sigma^2)$，根据文献[18]引理 1.5：$\Pr_{x\leftarrow D_{\mathbb{Z},\sigma}}\left[|x|>k\cdot\sigma\right]=erf(k/\sqrt{2})$。当 $k=9.2$，可使得 $erf(k/\sqrt{2})<2^{-64}$，可见离散高斯分布 $D_{\mathbb{Z},\sigma}$ 是一个有界分布，可以设置界 $B=9.2\sigma$。

定义 9　埃尔米特因子 δ^m。对于一个 m 维格 Λ 的一个格基 B，有这样一个参数 δ^m 使得 $\|b_1\|=\delta^m\det(\Lambda)^{1/m}$，其中 b_1 是格基 B 中最短的向量，δ 也被称为埃尔米特根因子。

Gamma,Nguyen[19]得出：给定 δ，约化出具有埃尔米特因子 δ^m 的格基所需要的时间主要取决于 δ。

对于文献[17]给出的区分攻击，为了使得其区分优势为 ε，需要找到一个长度为 $\alpha q/\sigma$ 的格向量，其中 $\alpha=\sqrt{\ln(1/\varepsilon)/\pi}$。Lindner,Peikert[17]使用了一个优化的攻击策略（一种格基约化方法），得到了具有埃尔米特因子 δ^m 的格基，该策略所能计算出最短向量的长度为 $2^{2\sqrt{n\log q\log\delta}}$，并给出了关于该攻击策略所需时间的一个粗略估计公式 $\log T=1.8/\log\delta-110$。如果 λ 为安全参数，即要求方案的安全级别为 $T=2^{\lambda}$，则有 $\log\delta=1.8/(\lambda+110)$，设置 $\lambda=128$，得到 $\delta\approx1.0052$。

由上可知，给定一个埃尔米特根因子 δ，使用 Lindner,Peikert 所给优化的攻击策略，计算出一个长度为 $2^{2\sqrt{n\log q\log\delta}}$ 的格向量，所花费的时间大约为 $2^{1.8/\log\delta-110}$，如果 $\alpha q/\sigma<2^{2\sqrt{n\log q\log\delta}}$，则在区分攻击中，取得的区分优势将小于 $\mathrm{e}^{-\alpha^2\pi}$。

根据 $\alpha q/\sigma<2^{2\sqrt{n\log q\log\delta}}$ 对本文所提方案的参数进行选择，例如设置区分优势为 $\varepsilon=2^{-64}$,攻击时间为 $T=2^{128}$，则 $\delta\approx1.0052$，$\alpha\approx3.758$。代入不等式得到 $1.910+\log q-\log\sigma\leqslant0.173\sqrt{n\log q}$。那么固定次数 n，就可以确定一系列 (q,σ) 的值。如 $n=1\,024,\lceil\log q\rceil=38,\sigma\approx55.062$；$n=2048,\lceil\log q\rceil=64,\sigma=9.69$。

6.2 全同态加密方案的参数选择

第 4 节所提出的非自举全同态加密方案，需要提前给一个电路深度 L，然后才能生成一个同态计算能力为 L 的加密方案。在此方案中除了需要设置参数 (n,σ)，还需要设置 $L+1$ 个模值 $(q_0,q_1,\cdots,q_L)$。下面将给出 $(q_0,q_1,\cdots,q_L)$ 的参数选取。

令第 i 层电路的密文噪声大小为 E_i。由方案的加密算法可知，新鲜密文的初始噪声为 $E_0\leqslant4nB^2+2B+1$。同态加和同态乘导致的噪声变化如下。

同态加

$$E_{i+1}\leqslant q_{i+1}/q_i\cdot(2E_i+2nB\log q_i)+1+n\|s\|$$

同态乘

$$E_{i+1}\leqslant q_{i+1}/q_i\cdot(n\cdot E_i^2+4nB\log q_i)+1+n\|s\|$$

由于同态乘的噪声增长比同态加大很多，所以主要考虑方案能够同态计算的乘法深度。模转换技术可以 q_{i+1}/q_i 的因子降低密文的噪声，假设通过 4.1 节的方案 FHE，可以把电路每一层的噪声控制在 E_0 以内，而只是每一层的模值 q_i 在不断地减小。

令 $\eta_{\mathrm{Reline},i}=(q_{i+1}/q_i)4nB\log q_i$，

$\eta_{\mathrm{Scale},i}=1+n\|s\|$，如果有以下 2 个条件成立。

1) $E_0\geqslant2(\eta_{\mathrm{Reline},i}+\eta_{\mathrm{Scale},i})$。

2) $q_{i+1}/q_i\geqslant2nE_0$。

那么有 $(q_{i+1}/q_i)\cdot nE_0^2+\eta_{\mathrm{Reline},i}+\eta_{\mathrm{Scale},i}\leqslant E_0$

对此进行粗略地估计：假设模值以 $1/2nE_0$ 的比率降低，经过 L 次同态操作之后，模值变为 $q_L=q_0/(2nE_0)^L$。为了保证解密的正确性，必须满足 $E_0\leqslant(q_0/(2nE_0)^L)/2$。那么 q_0 的比特长度为 $\log q_0\geqslant(L+1)\log(2nE_0)-\log n$，进一步得到 q_i 的比特长度为：$\log q_i\geqslant(L+1-i)\log(2nE_0)-\log n$。

由 $\alpha q/\sigma<2^{2\sqrt{n\log q\log\delta}}$ 得到 $(\log\alpha+\log q-\log\sigma)^2/4n\log q<\log\delta$，可以看出 q 的减小将使得 $\log\delta$ 减小。又因为 $\log T=1.8/\log\delta-110$，则攻击所花费的时间将会增加。所以只需要保证最大模值 RLWE 的安全性，亦保证了其他模值的 RLWE 安全性。

7 结束语

Brakerski, Gentry 在文献[12]中提出了不需要自举的全同态加密方案构造方法。他们的方案中的“密钥转换技术”使用了较复杂的矩阵运算。本文所提出的方案，通过在重线性化中引入密钥转换，

使得“密钥转换技术”形式简单。在同态运算电路时，本文给出了平凡门、加法门、乘法门的同态操作步骤，并将平凡门单独讨论，使电路的层结构更清晰。由于通过自举转化理论获得的全同态具有非常好的灵活性，不需要预先知道所需的同态运算能力，所以本章进一步分析了方案的自举性，给出一个降低解密算法复杂度的新方法，并由此使得方案具有自举性，提升了方案的同态运算能力。

参考文献：

[1] RIVEST R L, ADLEMAN L, DERTOUZOS M L. On data banks and privacy homomorphisms[A]. Foundations of Secure Computation[C]. 1978. 169-180.

[2] PAILLIER P. Public-key cryptosystems based on composite degree residuosity classes[A]. EUROCRYPT'99[C]. Spring, 1999. 223-238.

[3] RIVEST R L, SHAMIR A, ADLEMAN L. A method for obtaining digital signatures public key cryptosystem[J]. Communication of ACM, 1978, 21(1):120-126.

[4] BONEH D, GOH E J, NISSIM K. Evaluating 2-DNF formulas on ciphertexts[A]. Proceedings of Theory of Cryptography Conference 2005[C]. 2005. 325-342.

[5] GENTRY C. Fully homomorphic encryption using ideal lattices[A]. The 41st ACM Symposium on Theory of Computing (STOC)[C]. 2009. 169-178.

[6] GENTRY C. A Fully Homomorphic Encryption Scheme[D]. Standford: Stanford University, 2009.

[7] DIJK M, GENTRY C, HALEVI S, *et al*. Fully homomorphic encryptionover the integers[A]. Cryptology-EUROCRYPT'10[C]. 2010. 24-43.

[8] SMART N, VERCAUTEREN F. Fully homomorphic encryption with relatively small key and ciphertext sizes[A]. PKC 2010[C]. 2010. 420-443.

[9] GENTRY C, HALEVI S. Implementing gentry's fully-homomorphic encryption scheme[A]. EUROCRYPT, Lecture Notes in Computer Science[C]. 2011. 129-148.

[10] GENTRY C, HALEVI S. Fully homomorphic encryption without squashing using depth-3 arithmetic circuits[EB/OL].http://eprint.iacr.org/2011/279, 2011.

[11] BRAKERSKI Z, VAIKUNTANATHAN V. Efficient fully homomorphic encryption from (standard)lwe[EB/OL]. http://eprint.iacr.org/2011/344, 2011.

[12] BRAKERSKI Z, GENTRY C. Fully homomorphic encryption without bootstrapping[EB/OL]. http://eprint.iacr.org/, 2011.

[13] LAUTER K, NAEHRIG M, VAIKUNTANATHAN V. Can homo morphic encryption be practical?[EB/OL]. http://eprint.iacr.org/2011/405, 2011.

[14] LYUBASHEVSKY V, PEIKERT C, REGEV O. On ideal lattices and learning with errors over rings[A]. EUROCRYPT, Lecture Notes in Computer Science[C]. 2010. 1-23.

[15] MICCIANCIO D, REGEV O. Worst-case to average-case reductions based on gaussian measures[J]. SIAM J Comput, 2007. 37(1):267-302.

[16] KARP R M, RAMACHANDRAN V. A Survey of Parallel Algorithms for Shared-Memory Machines[R]. Technical Report CSD-88-408, UC Berkeley, 1988.

[17] LINDNER R, PEIKERT C. Better key sizes (and attacks) for LWE-based encryption[A]. Cryptology-CT-RSA 2011, Lecture Notes in Computer Science[C]. 2011. 319-339.

[18] BANASZCZYK W. New bounds in some transference theorems in the geometry of numbers[J]. Mathematische Annalen, 1993, 296(4): 625-635.

[19] GAMA N, NGUYEN P Q. Predicting lattice reduction[A]. Cryptology-EUROCRYPT 2008, Lecture Notes in Computer Science[C]. Springer, 2008. 31-51.

作者简介：

汤殿华（1986-），男，重庆人，保密通信重点实验室硕士，主要研究方向为全同态加密、格公钥密码。

祝世雄（1965-），男，重庆人，保密通信重点实验室研究员，主要研究方向为信息安全与保密通信。

王林（1983-），男，四川三台人，博士，保密通信重点实验室工程师，主要研究方向为密码学和信息安全。

杨浩淼（1977-），男，四川达州人，博士后，电子科技大学讲师，主要研究方向为基于身份的密码、格密码。

范佳（1982-），女，四川乐山人，博士，保密通信重点实验室工程师，主要研究方向为公钥密码学。