基于批处理技术的RLWE全同态加密方案

李孟天 胡 斌
(信息工程大学 郑州 450001)

摘 要 信息技术和网络通信的不断发展促使了大数据与云计算的产生,用户的数据安全和隐私保护逐渐成为学术界的研究重点。全同态加密是近年来新兴的一门研究学科,有着广阔的应用前景和重要的研究意义,能够支持在密文上做任意运算,且解密后等同于对明文做相同的操作,这一特性在云计算的安全性上有着重要应用。2011年,Lauter等提出了基于RLWE的同态加密方案,针对该方案,文中结合批处理技术设计了一种新的方案,利用中国剩余定理将多个"明文槽"打包到一个密文中,并进行同态运算操作。每次密文乘法操作后会造成噪声的指数增长,通过调用构造的密钥转换技术和模转换技术,来约减密文的噪声尺寸,保证能够正确解密且进行下一次同态运算。最后,对方案的安全性和效率进行了分析,结果表明在保证CPA安全的前提下,所提方案的加密效率是原始方案的n倍。

关键词 全同态加密,批处理技术,密钥转换,模转换

中图法分类号 TP309.7 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2019.03.031

RLWE-based Fully Homomorphic Encryption Scheme with Batch Technique

LI Meng-tian HU Bin
(Information Engineering University, Zhengzhou 450001, China)

Abstract The development of information technology and network communication promotes the emergence of big data and cloud computing. The security and privacy of user's data have gradually become the focus of academic research. Fully Homomorphic Encryption (FHE) is a new research subject, and it has a broad application prospect and important research significance in recent years. It supports arbitrary computation on encrypted data which is equivalent to do the same operations on corresponding plaintext. This feature has important applications in the security of cloud computing. In 2011, Lauter et al. proposed a RLWE-based Homomorphic Encryption scheme, aiming at the scheme, this paper designed a new scheme combined with the batch technique. Concretely, the technique packs multiple "plaintext slots" into a ciphertext by using the Chinese Remainder Theorem, and then performs homomorphic operations on it. Considering the exponential growth of the noise in each multiplication operation, this paper used the key switch and module switch technique to reduce the noise size in ciphertext, which ensure the correct decryption and the next homomorphic computation. Finally, this paper analyzed the security and efficiency of the scheme. It is proved that the proposed scheme is CPA security and the efficiency of encryption is n times to the original scheme.

Keywords Fully homomorphic encryption, Batch technique, Key switch, Module switch

1 引言

在云计算中,用户的数据都存放在云端的资源节点上[1],当用户需要数据时,其便将数据的计算结果通过网络发送给用户。由于用户的数据都存放在云端,因此普通用户不具有对自己私密数据的完全控制能力,确保数据安全性的最优方法就是对传输的数据和存储的数据进行加密处理。为了使云服务提供商能够继续向用户提供高效、快捷的各种技术服务(如数据检索、访问控制、数据挖掘等),云服务提供商必须能对加密数据进行各种复杂的操作。显然,传统的密码体制无法满足这样的需求,全同态加密应运而生。

全同态加密(Fully Homomorphic Encryption, FHE)方案能够在任何布尔电路或运算函数上对密文做任意运算,并且运算结果的解密等同于对明文做相同的运算。加密后的数据允许不可信服务器在没有解密私钥的情况下做任何运算操作。这一良好特性使其在云安全、云计算、加密数据库以及密

到稿日期:2018-01-17 返修日期:2018-05-21 本文受国家自然科学基金项目(62702548)资助。

李孟天(1993-),男,硕士,主要研究领域为密码学与信息安全,E-mail:skyli1993@163.com;胡 斌(1971-),男,教授,博士生导师,主要研究领域为密码学与信息安全,E-mail:hb2110@126.com(通信作者)。

文检索等领域具有广阔的应用前景。同态加密的思想是由 Rivest 等[2]于 1978 年首次提出的。同态加密的设计理念从部分同态加密(Somewhat Homomorphic Encryption,SWHE)到全同态加密经历了三十余年。2009 年,Gentry[3]首次构造出一种基于理想格的全同态加密方案,其能够进行任意深度的加法和乘法运算。2010 年,Gentry 等[4]第一次尝试实现 Gentry 方案,该方案可以将单比特消息的同态加密扩展为多比特,支持 SIMD 操作。2011 年,Smart 等[5]利用中国剩余定理(Chinese Remainder Theorem,CRT)对密文进行打包,使得每个密文可以加密一个明文向量,而不是单个明文。2011 年,Brakerski 等[6]提出了一个基于 LWE 问题的 FHE 方案,利用密钥转换技术和模转换技术使方案不需要同态解密技术,就可以实现自启动。2012 年,Gentry 等[7]对该技术进行了更深层次的研究。

Lauter 等[8]提出的 LNV11 部分同态加密方案是基于 RLWE 这一困难问题的,该方案每次只能加密一个明文比特,且对应的公钥、私钥规模远大于加密的明文规模,效率上有待提升。本文针对该方案,利用中国剩余定理,结合文献[5]中"明文槽"点的概念,实现对明文的打包;并结合扩展的密钥转换技术和模转换技术,提出了基于 RLWE 的批处理同态加密方案。该方案较为直观,一次可加密 $O(n\lambda)$ 个明文,相较于 LNV11 方案,结构更为清晰,在效率上提高了 n 倍。

2 预备知识

2.1 符号说明

若 A 表示一个算法,则 $x\leftarrow A$ 表示 x 是通过运行算法 A 得到的;若 A 是一个集合,则 $x\leftarrow A$ 表示 x 是从集合 A 中随机选出的。对于任意整数 q,记 $\mathbb{Z}_q=[-q/2,q/2)\cap\mathbb{Z}$,对于整数 x,令 $[x]_q$ 表示 $x(\mathrm{mod}\ q)\in\mathbb{Z}_q$。令向量 $\boldsymbol{y}$ 是一个多维向量,则 y_i 表示向量 $\boldsymbol{y}$ 的第 i 个分量。令向量 $\boldsymbol{a},\boldsymbol{b}$ 表示两个维数为 m 的向量,设 $\boldsymbol{a}\odot\boldsymbol{b}=(a_i\cdot b_i)_{i\in[1,\cdots,m]}$,$\langle\boldsymbol{a},\boldsymbol{b}\rangle=(\sum a_i\cdot b_i)_{i\in[1,\cdots,m]}$。

未定元为 x 的多项式用小写英文字母表示,如 $f(x)$。通过多项式 $f(x)$ 定义域上的元素,如 $\mathbb{Z}[x]/f(x)$ 等。令环 $R=\mathbb{Z}[x]/\Phi_m(x)$,其中 $\Phi_m(x)$ 是次数为 $n=\phi(m)$ 的分圆多项式。给定多项式 $f(x)=a_nx^n+\cdots+a_1x+a_0$,令 $\|f(x)\|_\infty$ 表示其无穷范数,即 $\|f(x)\|_\infty=\max(|r_1|,\cdots,|r_n|)$,并令 $\|f(x)\|_1=\sum_{i=0}^{n}|a_i|$ 和 $\|f(x)\|_2=\sqrt{\sum_{i=0}^{n}|a_i|^2}$ 分别表示其 1-范数和 2-范数。定义 R 上的扩展因子为 $\delta_R=\max\{\|a\cdot b\|_\infty/(\|a\|_\infty\cdot\|b\|_\infty):a,b\in R\}$。

2.2 分圆多项式和中国剩余定理

定义 1[5](分圆多项式) 设 K 是特征为 p 的域,m 是一个不能被 p 整除的正整数,ζ_m 是 K 上的一个 m 次本原单位根,则多项式:

$$\Phi_m(x)=\prod_{i=1,gcd(i,m)=1}^{m}(x-\zeta^i)$$

称为 K 上的 m 次分圆多项式。在有理数域 $\mathbb{Q}$ 上添加一个 m 次本原单位根,得到域扩张 $K=\mathbb{Q}(\zeta_m)$,称为 m 次分圆域。

关于有限域上的分圆多项式,有如下定理。

定理 1[9] 设 F_p 为有限域,m 为正整数,且 $gcd(m,p)=1$,则分圆多项式 $\Phi_m(x)$ 在 $F_p[x]$ 上可分解为 l 个不同 d 次不可约多项式 $f_i(x)$ 的乘积,即 $\Phi_m(x)=\prod_{i=0}^{l-1}f_i(x)$。其中,$d$ 是满足 $p^d\equiv1(\mathrm{mod}\ m)$ 的最小整数,$l=\phi(m)/d$。

证明:设 ζ_m 是 F_p 上任一 m 次本原单位根,且 $\zeta_m\in F_{p^k}$ 当且仅当 $\zeta_m^{p^k}=\zeta_m$。当 $k=d$ 时,有 $\zeta_m\in F_{p^d}$,且因为 $\zeta_m^{p^k}=\zeta_m\Leftrightarrow p^k\equiv1(\mathrm{mod}\ m)$,由 d 的最小性可知 $\zeta_m\notin F_{q^k}$ 的真子域,所以 ζ_m 在 F_q 上的极小多项式是 d 次的不可约多项式。又由 ζ_m 是任一本原单位根可知,$\Phi_m(x)$ 的每一个不可约多项式都为 d 次,而分圆多项式 $\Phi_m(x)$ 的次数为 $\phi(m)$,因此可分解为 $l=\phi(m)/d$ 个不同 d 次不可约多项式 $f_i(x)$ 的乘积。证毕。

定义 2[5,16](中国剩余定理) 设 $m_0,\cdots,m_{l-1}$ 是 $l\geqslant2$ 个两两互素的大于 1 的整数,令 $M=m_0m_1\cdots m_l$,则同余方程组

$$\begin{cases}g(x)\equiv r_0(x)\ \mathrm{mod}\ f_0(x)\\ g(x)\equiv r_1(x)\ \mathrm{mod}\ f_1(x)\\ \quad\vdots\\ g(x)\equiv r_{l-1}(x)\ \mathrm{mod}\ f_{l-1}(x)\end{cases}$$

有唯一解:$x\equiv\sum_{i=0}^{l-1}a_ib_iM_i(\mathrm{mod}\ M)$,其中 $M_i=M/m_i$,且 $b_i\equiv1/M_i(\mathrm{mod}\ m_i)$。

由上述定义,将数域上的中国剩余定理推广到多项式环上。

设 $f_0(x),\cdots,f_{l-1}(x)$ 是 $(l\geqslant2)$ 个两两既约的多项式,且令 $f(x)=f_0(x)\cdot f_1(x)\cdot\cdots\cdot f_{l-1}(x)$,那么对于任意的多项式 $r_0(x),\cdots,r_{l-1}(x)$,$\exists\, g(x)\in\mathbb{R}[x]$,使得同余方程组

$$\begin{cases}g(x)\equiv r_0(x)\ \mathrm{mod}\ f_0(x)\\ g(x)\equiv r_1(x)\ \mathrm{mod}\ f_1(x)\\ \quad\vdots\\ g(x)\equiv r_{l-1}(x)\ \mathrm{mod}\ f_{l-1}(x)\end{cases}$$

有唯一解:$g(x)=\sum_{i=0}^{l-1}r_i(x)h_i(x)m_i(x)(\mathrm{mod}\ f(x))$,其中 $m_i(x)=f(x)/f_i(x)$,$h_i(x)=1/m_i(x)(\mathrm{mod}\ f_i(x))$。

本文的工作是基于代数结构 $R_p=R/pR=\mathbb{Z}_p[x]/\Phi_m(x)$ 的,$\Phi_m(x)$ 是次数为 $\phi(m)$ 的分圆多项式,$\phi(\cdot)$ 是欧拉函数。R_p 中的元素是系数在区间 $[-p/2,p/2)$ 中的多项式,其运算是在 $\mathbb{Z}_p$ 上的加法和乘法。多项式 $\Phi_m(x)$ 在模 p 下可分解成 l 个不同的因子 $f_i(x)$,每个次数均为 d,满足 $p^d\equiv1(\mathrm{mod}\ m)$,且有 $l\cdot d=\phi(m)$。结合中国剩余定理,有以下同构关系:

$$\begin{aligned}R_p&=\mathbb{Z}_p[x]/f_0(x)\cdot f_1(x)\cdot\cdots\cdot f_{l-1}(x)\\&\cong\mathbb{Z}_p[x]/f_0(x)\times\cdots\times\mathbb{Z}_p[x]/f_{l-1}(x)\\&\cong\mathbb{F}_{p^d}\times\cdots\times\mathbb{F}_{p^d}=\mathbb{L}_0\times\cdots\times\mathbb{L}_{l-1}\end{aligned}$$

即 R_p 同构于 l 个 $\mathbb{L}_i$ 的直积;也就是说,R_p 上的元素与 l 个在 $\mathbb{F}_{p^d}\cong\mathbb{Z}_p[x]/f_i(x)$ 中的元素有映射关系。不妨设 $\mathbb{L}_i$ 为一个

“槽”点，即 R_p 中的元素与 l 个槽点建立了关系。具体如下：

$$\psi:\begin{cases}\mathbb{F}_{p^d}^{l}\to\mathbb{Z}_p[x]/f_0(x)\times\cdots\times\mathbb{Z}_p[x]/f_{l-1}(x)\\(m_0,\cdots,m_{l-1})\mapsto(\psi_0(m_0),\cdots,\psi_{l-1}(m_{l-1}))\end{cases}$$

$$\varphi:\begin{cases}\mathbb{Z}_p[x]/f_0(x)\times\cdots\times\mathbb{Z}_p[x]/f_{l-1}(x)\to R_p\\(h_0,\cdots,h_{l-1})\mapsto\sum_{i=0}^{l-1}h_iH_i(x)M_i(x)\end{cases}$$

其中，$M_i(x)=\Phi_m(x)/f_i(x)$，$H_i(x)=1/M_i(x)\pmod{f_i(x)}$。

显然有，$CRT_p=\psi\circ\varphi$ 是 $\mathbb{F}_{p^d}^{l}$ 到 R_p 的同构映射，且每个 ψ_i 是 $\mathbb{F}_{p^d}$ 到 $\mathbb{Z}_p[x]/f_i(x)$ 的一个同构映射。

2.3 RLWE 问题

RLWE 问题（Ring Learning with Errors Problem）是由 Lyubaskevsky 等[10]在 2010 年的欧密会上提出的。

定义 3[10]（RLWE 问题）　设安全参数为 λ，令 $f(x)=x^n+1$，其中 $n=n(\lambda)$ 是 2 的幂次，整数 $q=q(\lambda)\geqslant 2$，令 $R=\mathbb{Z}[x]/f(x)$，且 $R_q=R/qR$，$\chi=\chi(\lambda)$ 是 R 上的一个离散高斯分布。随机均匀采样 $s\leftarrow R_q$，$a_i\leftarrow R_q$，选取噪声 $e_i\leftarrow\chi$，令 $b_i=a_i\cdot s+e_i$。Decision-RLWE$_{n,q,\chi}$ 问题为：随机均匀采样的 $(a_i,b_i)\in R_q^2$ 与 $(a_i,b_i=a_i\cdot s+e_i)\in R_q^2$ 计算不可区分；Search-RLWE$_{n,q,\chi}$ 问题为：对于 $(a_i,b_i=a_i\cdot s+e_i)\in R_q^2$，给出 a_i,b_i 的值，求解 s。

RLWE 问题具有重要意义，Lyubashevsky 等证明了理想格上的最短向量问题（SVP）可以归纳为 RLWE 问题。

定义 4[8]（高斯函数）　设 $\mathbb{R}$ 是实数集，$\sigma>0$，向量 $\boldsymbol{x},\boldsymbol{c}\in\mathbb{R}^n$，则 n 维高斯函数定义为：$\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{x})=\exp\left(\frac{-\pi\|\boldsymbol{x}-\boldsymbol{c}\|^2}{\sigma^2}\right)$，其中 c 为中心，σ 为标准差。

定义 5[8]（离散高斯分布）　设 Λ 是 n 维格，$\mathbb{R}$ 是实数集，$\sigma>0$，向量 $\boldsymbol{x},\boldsymbol{c}\in\mathbb{R}^n$，则 Λ 上的离散高斯分布为 $D_{\Lambda,\sigma,\boldsymbol{c}}(\boldsymbol{x})=\frac{\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{x})}{\rho_{\sigma,\boldsymbol{c}}(\Lambda)}$。

其中，$\rho_{\sigma,\boldsymbol{c}}(\Lambda)=\sum_{\boldsymbol{x}\in\Lambda}\rho_{\sigma,\boldsymbol{c}}(x)$ 表示格 Λ 上 $\rho_{\sigma,\boldsymbol{c}}$ 的离散积分。

对于多项式 $a(x)\in R_q=\mathbb{Z}_q[x]/f(x)$，一般有两种将其映射成向量的方法：系数嵌入和正则嵌入。系数嵌入是一种较为直观、简单的方法，$a(x)=\sum_{i=0}^{n-1}a_ix^i$，其系数嵌入可定义为：

$$a(x)\mapsto(a_0,a_1,\cdots,a_{n-1})\in\mathbb{Z}_q^n$$

该嵌入是多项式环上元素到模 q 下的 n 维整数向量的映射，多项式的加法运算可对应于向量的按位加，但多项式的乘法运算较为复杂，不能简单地对应于向量的按位乘。

在文献[17]中，Regev 等对正则嵌入进行了相关描述。

定义 6[17]（正则嵌入）　令 $\zeta=\exp(\pi\sqrt{-1}/n)$，从 $R_q=\mathbb{Z}_q[x]/f(x)$ 到复数域 $\mathbb{C}^n$ 上的向量空间的映射 σ 为：

$$\sigma:a(x)\mapsto(a(\zeta),a(\zeta^3),\cdots,a(\zeta^{2n-1}))\in\mathbb{C}^n$$

则称 σ 为正则嵌入映射，其中 $a(x)\in R_q$，$f(x)=x^n+1$。

由上述定义，我们利用正则嵌入将 $R_q=\mathbb{Z}_q[x]/f(x)$ 上的多项式映射成复数域上的向量，则多项式的加法和乘法可映射成向量上的按位加法和乘法操作，这使得计算更直观、简洁，便于运算。

2.4 全同态加密的基本概念

定义 7[15]（同态加密，Homomorphic Encryption，HE 方案）　同态加密方案 ε 一般包括 4 个概率多项式时间算法：密钥生成算法 KeyGen、加密算法 Encrypt、解密算法 Decrypt 和最为重要的同态计算算法 Evaluate。

KeyGen(λ)：输入安全参数 λ，输出公钥 pk、私钥 sk 以及用于计算密文的密钥 evk。

Encrypt($pk,\boldsymbol{m}$)：输入公钥 pk、明文 $\boldsymbol{m}$，用 pk 对明文 $\boldsymbol{m}$ 进行加密，输出密文向量 $\boldsymbol{c}$。

Decrypt($sk,\boldsymbol{c}$)：输入私钥 sk、密文 $\boldsymbol{c}$，用 sk 对密文进行解密，输出明文 $\boldsymbol{m}$。

Evaluate($evk,f,\boldsymbol{c}$)：输入计算密钥 evk、门电路 f 以及密文 $\boldsymbol{c}=(c_0,\cdots,c_{l-1})$，其中 c_i 为明文 m_i 的加密，输出另一密文 c^*，且满足 Decrypt(sk,c^*)$=f(m_0,\cdots,m_{l-1})$。

定义 8[15]（正确同态解密）　若同态加密方案 $\varepsilon=$(KeyGen，Encrypt，Decrypt，Evaluate) 对门电路函数 f 可以正确同态解密，对于有 l 个输入的门电路 f，任意的公私钥对 $(sk,pk)\leftarrow$ KeyGen(λ)、l 比特明文 $\boldsymbol{m}=(m_0,\cdots,m_{l-1})$ 以及相应密文 $\boldsymbol{c}=(c_0,\cdots,c_{l-1})$，满足 Decrypt($sk$，Evaluate($evk$，$f$，$\boldsymbol{c}$))$=f(m_0,\cdots,m_{l-1})$。

定义 9[15]（同态加密的紧致性）　在同态加密方案 $\varepsilon=$(KeyGen，Encrypt，Decrypt，Evaluate) 中，若存在一个多项式 $b=b(\lambda)$，使得若同态计算算法 Evaluate 输出的密文长度不超过 b，则该方案满足紧致性。

定义 10[15]（部分同态加密）　若同态加密方案 $\varepsilon=$(KeyGen，Encrypt，Decrypt，Evaluate) 满足加法同态和乘法同态，且能够执行有限步电路深度的同态计算，即 Evaluate 算法可以计算的多项式次数低于解密电路的深度，则该方案为部分同态加密方案。

定义 11[15]（全同态加密）　若同态加密方案对所有的布尔电路 f 既满足同态性，又满足紧致性，则该方案是一个全同态加密方案。

3 LNV11 部分同态加密方案

部分同态加密方案只能进行有限次的同态操作，但它是转化为全同态加密方案的基础。本节首先对文献[8]中的部分同态方案进行描述，并给出相应的密钥转换技术和模转换技术。

3.1 LNV11 部分同态加密方案的描述

参数设定（$params$）：n 是维数，且为 2 的幂次；分圆多项式为 $f(x)=x^n+1$；q 为模，且为素数，满足 $q\equiv1\pmod{2n}$，同时 n，q 和 $f(x)$ 共同定义了环 $R:=\mathbb{Z}[x]/f(x)$ 和密文空间 $R_q:=R/qR=\mathbb{Z}_q[x]/f(x)$；$\sigma$ 是错误参数，定义了一个离散高

斯分布 $\chi=D_{\mathbf{Z}^n,\sigma}$；素数 $t<q$，方案中明文空间为 $R_t=\mathbb{Z}_t[x]/f(x)$。

该部分同态加密方案 SHε 由 4 个算法构成：SH. Keygen，SH. Enc，SH. Dec 和 SH. Eval。

SH. Keygen($params$)：随机选取一个环元素 $s\leftarrow\chi$，且令私钥 sk 为 s。随机均匀选取环元素 $a_1\leftarrow R_q$ 和一个错误 $e\leftarrow\chi$，且令公钥 pk 为 $(a_0=-(a_1s+te),a_1)$。

SH. Enc(pk,m)：给定公钥 pk 和明文 $m\in R_t$，随机选取 $u\leftarrow\chi$ 和 $f,g\leftarrow\chi$，计算密文 $ct=(c_0,c_1)=(a_0u+tg+m,a_1u+tf)$。

SH. Dec($sk,ct=(c_0,c_1)$)：首先计算 $\tilde{m}=c_0+c_1\cdot s$，输出明文 $m=\tilde{m}(\mathrm{mod}\ p\ \mathrm{mod}\ t)$。

SH. Eval($ct=(c_0,c_1),ct'=(c_0',c_1')$)：

SH. Add(pk,ct,ct')：令 $ct=(c_0,c_1)$ 和 $ct'=(c_0',c_1')$ 为两个密文，同态加操作为密文向量的按位加，即 $ct_{\mathrm{add}}=(c_0+c_0',c_1+c_1')\in R_q^2$。

SH. Mult(pk,ct,ct')：令 v 为变量元，计算 $(c_0+c_1\cdot v)\cdot(c_0'+c_1'\cdot v)$，结果为 $c_0c_0'+(c_0c_1'+c_0'c_1)v+c_1c_1'v^2$，其可看作关于 v 的二次多项式，则乘法操作输出的密文是 $ct_{\mathrm{mlt}}=(c_0c_0',c_0c_1'+c_0'c_1,c_1c_1')$。

3.2 解密正确性

下面对 3.1 节中的部分同态加密方案的正确性进行验证。

由部分同态加密方案可知，解密算法为：

$$\begin{aligned}&\mathrm{SH.Dec}(sk,ct=(c_0,c_1))\\&=(c_0+c_1s)(\mathrm{mod}\ p\ \mathrm{mod}\ t)\\&=a_0u+tg+m+a_1us+tfs\\&=(-a_1s+te)u+tg+m+a_1us+tfs\\&=m+t(eu+g+fs)\\&=m+t\tilde{e}(\mathrm{mod}\ p\ \mathrm{mod}\ t)\\&=m\end{aligned}$$

这样就得到了原始的明文多项式 $m\in R_t$。称 $m+t\tilde{e}$ 为噪声，且若满足 $\|m+t\tilde{e}\|<p/2$，则可进行正确解密。

3.3 密钥转换和模转换技术

对于 3.1 节中的方案而言，同态加法产生的一个密文仅含有两个环元素，即环元素个数没有发生改变；而同态乘法 $ct_{\mathrm{mlt}}=(c_0c_0',c_0c_1'+c_0'c_1,c_1c_1')$，记作 $ct_{\mathrm{mlt}}=(\hat{c}_0,\hat{c}_1,\hat{c}_2)$，对应私钥为 $sk=(1,s,s^2)$，其解密后是两个明文的乘积，即 $\hat{c}_0+\hat{c}_1s+\hat{c}_2s^2=mm'(\mathrm{mod}\ p\ \mathrm{mod}\ t)$。由此，密文的同态乘操作将导致维数的迅速膨胀，密文大小随着乘法操作数的增加而呈指数增长。针对这一现象，一是通过密钥转换技术[5]使维数始终保持在初始状态；二是利用模转换技术[5]约减密文中的噪声。

3.3.1 密钥转换技术

密钥转换算法的目的是约减密文向量的维数，减小密文尺寸，即密文 $ct_{\mathrm{mlt}}=(\hat{c}_0,\hat{c}_1,\hat{c}_2)$ 转换成 $ct'_{\mathrm{mlt}}=(\hat{c}_0',\hat{c}_1')$，对应的私钥从 $sk=(1,s,s^2)$ 转换成 $sk'=(1,s')$。算法过程如下：

随机均匀选取 $a_i,a_i'\leftarrow R_q$，错误元素 $e,e'\leftarrow\chi$，计算 $d_i=-(a_is'+te)+t^is^2$ 和 $d_i'=-(a_i's'+te')+t^is$，且令 $h_i=(a_i,d_i=-(a_is'+te)+t^is^2)$，$l_i=(a',d_i'=-(a_i's'+te')+t^is)$。其中，$i=0,\cdots,\lceil\log_t^q\rceil-1$。

设 $\tau_{sk\to sk'}=\{h_i,l_i\}_{i=0}^{\lfloor\log_t^q\rfloor-1}$ 为辅助信息，且该分布在 $R_q\times R_q$ 上的均匀分布是不可区分的，这样就保证了其安全性。

令 $\hat{c}_1\leftarrow\sum_{i=0}^{\lceil\log_t^q\rceil-1}\hat{c}_{1,i}t^i,\hat{c}_2\leftarrow\sum_{i=0}^{\lceil\log_t^q\rceil-1}\hat{c}_{2,i}t^i$，其中 $\hat{c}_{1,i},\hat{c}_{2,i}\in R_t$，计算：$\hat{c}_0^{\mathrm{relin}}\leftarrow\hat{c}_0+\sum_{i=0}^{\lceil\log_t^q\rceil-1}\hat{c}_{2,i}d_i,\hat{c}_1^{\mathrm{relin}}\leftarrow\sum_{i=0}^{\lceil\log_t^q\rceil-1}\hat{c}_{2,i}a_i$。

令 $\hat{c}_0'\leftarrow\hat{c}_0^{\mathrm{relin}}+\sum_{i=0}^{\lceil\log_t^q\rceil-1}\hat{c}_{1,i}d_i',\hat{c}_1'\leftarrow\hat{c}_1^{\mathrm{relin}}+\sum_{i=0}^{\lceil\log_t^q\rceil-1}\hat{c}_{1,i}a_i'$，新密文即为 $(\hat{c}_0',\hat{c}_1')$，对应私钥为 $sk'=(1,s')$。

为验证上述技术的正确性，用私钥 $sk'=(1,s')$ 对 $(\hat{c}_0',\hat{c}_1')$ 进行解密：

$$\begin{aligned}&\hat{c}_0'+\hat{c}_1's'\\&=\hat{c}_0^{\mathrm{relin}}+\sum_{i=0}^{\lceil\log_t^q\rceil-1}\hat{c}_{1,i}d_i'+(\hat{c}_1^{\mathrm{relin}}+\sum_{i=0}^{\lceil\log_t^q\rceil-1}\hat{c}_{1,i}a_i')s'\\&=\hat{c}_0+\sum_{i=0}^{\lceil\log_t^q\rceil-1}\hat{c}_{2,i}d_i+\sum_{i=0}^{\lceil\log_t^q\rceil-1}\hat{c}_{1,i}d_i'+\sum_{i=0}^{\lceil\log_t^q\rceil-1}\hat{c}_{2,i}a_is'+\\&\quad\sum_{i=0}^{\lceil\log_t^q\rceil-1}\hat{c}_{1,i}a_i's'\\&=\hat{c}_0+\sum_{i=0}^{\lceil\log_t^q\rceil-1}\hat{c}_{2,i}t^is^2-\sum_{i=0}^{\lceil\log_t^q\rceil-1}\hat{c}_{2,i}te+\sum_{i=0}^{\lceil\log_t^q\rceil-1}\hat{c}_{1,i}t^is-\\&\quad\sum_{i=0}^{\lceil\log_t^q\rceil-1}\hat{c}_{1,i}te'\\&=\hat{c}_0+\hat{c}_1s+\hat{c}_2s^2-t(\sum_{i=0}^{\lceil\log_t^q\rceil-1}\hat{c}_{1,i}e'+\sum_{i=0}^{\lceil\log_t^q\rceil-1}\hat{c}_{2,i}e)\\&=mm'+\hat{e}\\&=mm'(\mathrm{mod}\ p\ \mathrm{mod}\ t)\end{aligned}$$

3.3.2 模转换技术

模转换技术的目的是约减密文中的噪声，每次同态乘法后，密文中的噪声尺寸会呈指数增长，多次运算后，可能会出现解密不正确的情况。为解决这一问题，运用模转换技术，可以减小密文中噪声的大小，将模 q 转化成模 p，且二者皆对应于同一个私钥 s，进而降低噪声，提高乘法运算的效率。Scale 算法的具体描述如下。

设 $[\cdot]$ 为取整符号，$[a]$ 表示一个接近 a 的整数。设 q,p,t 为整数，且 $q>p>t$，$\boldsymbol{y}$ 为整数向量，则 $\mathrm{Scale}(\boldsymbol{y},q,p,t)=[(p/q)\cdot\boldsymbol{y}]=\boldsymbol{y}'$，且满足：$\boldsymbol{y}'\equiv\boldsymbol{y}(\mathrm{mod}\ t)$。

例：令 $\boldsymbol{y}=(86,42),q=97,p=23,t=2$，则：$\mathrm{Scale}(\boldsymbol{y},q,p,t)=[(p/q)\cdot\boldsymbol{y}]=[(23/97)\cdot(86,42)]=[(20.3916,9.9588)]$，且要满足 $\boldsymbol{y}'\equiv\boldsymbol{y}(\mathrm{mod}\ t)$，则 $\boldsymbol{y}'=(20,10)$。

定理 2[11] 上述 $\boldsymbol{y},\boldsymbol{y}'=\mathrm{Scale}(\boldsymbol{y},q,p,t)$，对于满足 $\|\langle\boldsymbol{y},$

$\boldsymbol{s}\rangle_q \| < q/2-(q/p)\cdot \| \boldsymbol{s} \|$ 的任何 $\boldsymbol{s}$，有：$\langle \boldsymbol{y}', \boldsymbol{s}\rangle_p = \langle \boldsymbol{y}, \boldsymbol{s}\rangle_q \bmod t$，且 $\| [\boldsymbol{y}', \boldsymbol{s}]_p \| < ((p/q)\cdot \| \langle \boldsymbol{y}, \boldsymbol{s}\rangle_q \| + \| \boldsymbol{s} \|$。

由上述定义可知，该算法可将在模 q 下的密文 ct 转换成在模 p 下的密文 $\boldsymbol{ct}'$，且保证对应的明文不变，二者均对应相同的私钥 $\boldsymbol{s}$。

4　批处理同态加密方案

本节在第 3 节所述方案的基础上，通过应用数域上的中国剩余定理(CRT)构造支持批处理的同态加密方案，将多个明文打包后加密到一个密文中，并将上节中分析的两种技术应用到该方案中，降低了密文膨胀率，提高了加密效率。

4.1　构造批处理同态加密方案

批处理同态加密方案包括批同态参数设置、批同态密钥生成算法、批同态加密算法、批同态解密算法和批同态运算算法 5 个步骤，利用上节分析的密钥转换技术和模转换技术构造批处理全同态加密方案，具体如下。

Batch. FHE. Setup(1^λ, 1^L)：设安全参数为 λ，电路层数为 L，令 $R=\mathbb{Z}[x]/\Phi_m(x)$，其中 $\Phi_m(x)=\prod_{i=0}^{l-1} f_i(x)$ 是分圆多项式，且每个 $f_i(x)$ 的次数都为 d，其中 $\phi(m)=n=dl=n(\lambda, L)$。共有 $L+1$ 个素数模，$q_0<q_1<\cdots<q_L$，对应地，第 i 层的电路多项式环为 $R_{q_i}=\mathbb{Z}[x]_{q_i}/\Phi_m(x)$，且每层电路的离散高斯分布为 $\chi(\lambda, L)$。选择一个素整数 t，满足 $t<q_0$，$\mathbb{F}_{p^d}^l$ 是明文向量空间，映射 CRT_p 是 $\mathbb{F}_{p^d}^l$ 到 R_p 的同构映射。

Batch. FHE. Keygen($params$)：随机选取 $L+1$ 个环元素 $s_i \leftarrow \chi$，随机均匀选取环元素 $a_i \leftarrow R_{q_i}$ 和错误元素 $e \leftarrow \chi$，且 $b_i=-a_i\cdot s_i+te$，其中 $i=0,1,\cdots,L$。令 $\boldsymbol{a}=(a_0, a_1, \cdots, a_L)$，$\boldsymbol{b}=(b_0, b_1, \cdots, b_L)$，设置公钥 $pk=(\boldsymbol{b}, \boldsymbol{a})$，私钥 $sk=\boldsymbol{s}=(s_0, s_1, \cdots, s_L)$。

Batch. FHE. Enc(pk, $\{(m_{i,0}, \cdots, m_{i,l-1})\}_{i=0}^L$)：给定公钥 pk 和明文 $(m_{i,0}, \cdots, m_{i,l-1}) \in \mathbb{F}_{p^d}^l$，其中 $i=0,1,\cdots,L$。加密过程如下：

1)利用中国剩余定理计算明文 $m_i \leftarrow CRT_p(m_{i,0}, \cdots, m_{i,l-1}) \in R_p$；

2)令 $\boldsymbol{m}=(m_0, \cdots, m_L)$；

3)随机选取 $u \leftarrow \chi$，$f \leftarrow \chi$ 和 $g \leftarrow \chi$，并令 $\boldsymbol{f}=(f, f, \cdots, f)$ 和 $\boldsymbol{g}=(g, g, \cdots, g)$，二者的元素个数均为 $L+1$；

4)输出密文：$\boldsymbol{ct}=(\boldsymbol{c}_0, \boldsymbol{c}_1)=((\boldsymbol{b}u+t\boldsymbol{g}+\boldsymbol{m}), (\boldsymbol{a}u+t\boldsymbol{f})) \in R_q^{(L+1)\times 2}$。

Batch. FHE. Dec(sk, $\boldsymbol{ct}$)解密过程如下：

1)计算

$\boldsymbol{m}=(m_0, \cdots, m_L)=(\boldsymbol{c}_0+\boldsymbol{c}_1\odot \boldsymbol{s})(\bmod p \bmod t) \in R_p^{L+1}$；

2)输出

$(m_{i,0}, \cdots, m_{i,l-1}) \leftarrow CRT_p^{-1}(m_i) \in \mathbb{F}_{p^d}^l$。

Batch. FHE. Eval($\boldsymbol{ct}=(\boldsymbol{c}_0, \boldsymbol{c}_1)$, $\boldsymbol{ct}'=(\boldsymbol{c}_0', \boldsymbol{c}_1')$)：

Batch. FHE. Add(evk, $\boldsymbol{ct}$, $\boldsymbol{ct}'$)：

令 $\boldsymbol{ct}=(\boldsymbol{c}_0, \boldsymbol{c}_1)$，$\boldsymbol{ct}'=(\boldsymbol{c}_0', \boldsymbol{c}_1')$ 为两个密文，且在同一电路层，同态加操作即按位加：$\boldsymbol{ct}_{\text{add}}=(\boldsymbol{c}_0+\boldsymbol{c}_0', \boldsymbol{c}_1+\boldsymbol{c}_1') \in R_q^{(L+1)\times 2}$。

若不在同一电路层，则通过多次调用算法 $Scale(\boldsymbol{ct}', q_i, q_{i-1}, t)$，使二者处于相同的电路层。

Batch. FHE. Mult(evk, $\boldsymbol{ct}$, $\boldsymbol{ct}'$)：

1)考虑在同一电路层的乘法操作(若不在同一电路层，则多次调用模转换算法)。令 $\boldsymbol{v}=(v_0, v_1, \cdots, v_L)$ 为 $L+1$ 维变量元向量，计算 $(\boldsymbol{c}_0+\boldsymbol{c}_1\odot \boldsymbol{v})\odot(\boldsymbol{c}_0'+\boldsymbol{c}_1'\odot \boldsymbol{v})$，将其看作关于 $\boldsymbol{v}$ 的二次多项式向量，其系数即为密文乘法操作输出的密文 $\boldsymbol{ct}_{\text{mlt}}$。

2)调用算法 KeySwitch($\boldsymbol{sk}'$, $\boldsymbol{sk}''$, $(\boldsymbol{c}_0, \boldsymbol{c}_1, \boldsymbol{c}_2)$)，得到 $\boldsymbol{ct}'=(\boldsymbol{c}_0, \boldsymbol{c}_1)$；

3)调用算法 Scale($\boldsymbol{ct}'$, q_i, q_{i-1}, $\boldsymbol{t}$)，得到在模 q_{i-1} 下的密文。

现对上述乘法操作做具体说明：设 $\boldsymbol{c}_0=(\boldsymbol{b}u+t\boldsymbol{g}+\boldsymbol{m})=(c_{0,0}, c_{0,1}, \cdots, c_{0,L})$，$\boldsymbol{c}_1=(\boldsymbol{a}u+t\boldsymbol{f})=(c_{1,0}, c_{1,1}, \cdots, c_{1,L})$，同理有，$\boldsymbol{c}_0'=(c'_{0,0}, c'_{0,1}, \cdots, c'_{0,L})$，$\boldsymbol{c}_1'=(c'_{1,0}, c'_{1,1}, \cdots, c'_{1,L})$，则有：

$$
\begin{aligned}
&(\boldsymbol{c}_0+\boldsymbol{c}_1\odot \boldsymbol{v})\odot(\boldsymbol{c}_0'+\boldsymbol{c}_1'\odot \boldsymbol{v})\\
&=\boldsymbol{c}_0\odot \boldsymbol{c}_0'+(\boldsymbol{c}_0\odot \boldsymbol{c}_1'+\boldsymbol{c}_1\odot \boldsymbol{c}_0')\odot \boldsymbol{v}+\boldsymbol{c}_1\odot \boldsymbol{c}_1'\odot \boldsymbol{v}\odot \boldsymbol{v}\\
&=(c_{0,0}\cdot c'_{0,0}, \cdots, c_{0,L}\cdot c'_{0,L})+((c_{0,0}\cdot c'_{1,0}+c_{1,0}\cdot c'_{0,0})\cdot v_0, \cdots, (c_{0,L}\cdot c'_{1,L}+c_{1,0}\cdot c'_{0,0})\cdot v_L)+(c_{1,0}\cdot c'_{1,0}\cdot v_0^2, \cdots, c_{1,L}\cdot c'_{1,L}\cdot v_L^2)\\
&=((c_{0,0}\cdot c'_{0,0}+(c_{0,0}\cdot c'_{1,0}+c_{1,0}\cdot c'_{0,0})\cdot v_0+c_{1,0}\cdot c'_{1,0}\cdot v_0^2), \cdots, (c_{0,L}\cdot c'_{0,L}+(c_{0,L}\cdot c'_{1,L}+c_{1,0}\cdot c'_{0,0})\cdot v_L+c_{1,L}\cdot c'_{1,L}\cdot v_L^2))
\end{aligned}
$$

将其看作关于 v_i 的二次多项式向量，则密文乘法操作输出的密文为：

$$\boldsymbol{ct}_{\text{mlt}}=\{(c_{0,i}\cdot c'_{0,i}, c_{0,i}\cdot c'_{1,i}+c_{1,i}\cdot c'_{0,i}, c_{1,i}\cdot c'_{1,i})_{i\in[0,L]}\}$$

Gentry 等[6]实现了打包密文中不同槽间数据的移动与运算，利用该置换 π_{CRT} 技术，可以在不“解包”的情况下，同态地批处理密文。本文构造方案中利用中国剩余定理对明文槽进行打包，通过利用上述置换 π_{CRT} 可以实现对明文槽间的任意同态置换。

4.2　解密正确性

下面对上述方案的解密正确性进行验证。由加密算法可知：

$$
\begin{aligned}
\boldsymbol{ct}&=(\boldsymbol{c}_0, \boldsymbol{c}_1)=((\boldsymbol{b}u+t\boldsymbol{g}+\boldsymbol{m}), (\boldsymbol{a}u+t\boldsymbol{f}))\\
&=((b_0u+tg+m_0, \cdots, b_Lu+tg+m_L), (a_0u+tf, \cdots, a_Lu+tf))
\end{aligned}
$$

由上式和 Batch. FHE. Dec(sk, $\boldsymbol{ct}$)，可得：

$$
\begin{aligned}
\boldsymbol{m}&=(m_0, \cdots, m_L)=(\boldsymbol{c}_0+\boldsymbol{c}_1\odot \boldsymbol{s})(\bmod p \bmod t)\\
&=(b_0u+tg+m_0, \cdots, b_Lu+tg+m_L)+(a_0u+tf, \cdots, a_Lu+tf)\odot(s_0, \cdots, s_L)\\
&=(b_0u+tg+m_0, \cdots, b_Lu+tg+m_L)+(a_0us_0+tfs_0, \cdots, a_Lus_L+tfs_L)
\end{aligned}
$$

$$=(b_0u+tg+m_0+a_0us_0+tfs_0,\cdots,b_Lu+tg+m_L+a_Lus_L+tfs_L)$$

$$=(m_0+t(eu+g+fs_0),\cdots,m_L+t(eu+g+fs_L))\ (\mathrm{mod}\ p\ \mathrm{mod}\ t)=(m_0,m_1,\cdots,m_L)=\boldsymbol{m}$$

若 $\max(\|t(eu+g+fs_i)\|_{i\in[0,L]})<\frac{p}{2}$，则可进行正确解密，进而通过中国剩余定理求出初始明文，即 $(m_{i,0},\cdots,m_{i,l-1})\leftarrow CRT_p^{-1}(m_i)\in\mathbb{F}_{p^d}^l$。

4.3 加密方案的同态性

本节分析上述方案的同态性。令 $\boldsymbol{ct}$ 和 $\boldsymbol{ct}'$ 为上述同态加密方案的密文，二者分别加密明文 $\boldsymbol{m}$ 和 $\boldsymbol{m}'$，对应私钥为 $\boldsymbol{s}$，且 $\boldsymbol{m}=(m_0,\cdots,m_L)=(\boldsymbol{c}_0+\boldsymbol{c}_1\odot\boldsymbol{s})(\mathrm{mod}\ p\ \mathrm{mod}\ t)\in R_p^{L+1}$。

4.3.1 加法同态性

令 $\boldsymbol{ct}_{\mathrm{add}}=\boldsymbol{ct}+\boldsymbol{ct}'=(\boldsymbol{c}_0+\boldsymbol{c}_0{}',\boldsymbol{c}_1+\boldsymbol{c}_1{}')$，则对其进行解密，有：

$$(\boldsymbol{c}_0+\boldsymbol{c}_0{}',(\boldsymbol{c}_1+\boldsymbol{c}_1{}')\odot\boldsymbol{s})=(\boldsymbol{c}_0+\boldsymbol{c}_0{}',\boldsymbol{c}_1\odot\boldsymbol{s}+\boldsymbol{c}_1{}'\odot\boldsymbol{s})=(\boldsymbol{c}_0,\boldsymbol{c}_1\odot\boldsymbol{s})+(\boldsymbol{c}_0{}',\boldsymbol{c}_1{}'\odot\boldsymbol{s})(\mathrm{mod}\ p\ \mathrm{mod}\ t)=\boldsymbol{m}+\boldsymbol{m}'$$

根据 4.2 节的表述，因为噪声足够小于 $p/2$，所以上式可正确解密，因此方案满足加法同态性。

4.3.2 乘法同态性

由 4.1 节知，密文乘法操作输出的密文为

$$\boldsymbol{ct}_{\mathrm{mlt}}=\{(c_{0,i}\cdot c'_{0,i},c_{0,i}\cdot c'_{1,i}+c_{1,i}\cdot c'_{0,i},c_{1,i}\cdot c'_{1,i})_{i\in[0,L]}\}$$

利用私钥 $\boldsymbol{s}$ 对其进行解密，有：

$$\boldsymbol{ct}_{\mathrm{mlt}}\odot(1,\boldsymbol{s},\boldsymbol{s}\odot\boldsymbol{s})$$

$$=\{(c_{0,i}\cdot c'_{0,i},c_{0,i}\cdot c'_{1,i}+c_{1,i}\cdot c'_{0,i},c_{1,i}\cdot c'_{1,i})_{i\in[0,L]}\}\odot(1,\boldsymbol{s},\boldsymbol{s}\odot\boldsymbol{s})$$

$$=((c_{0,0}\cdot c'_{0,0}+(c_{0,0}\cdot c'_{1,0}+c_{1,0}\cdot c'_{0,0})\cdot s_0+c_{1,0}\cdot c'_{1,0}\cdot s_0^2),\cdots,(c_{0,L}\cdot c'_{0,L}+(c_{0,L}\cdot c'_{1,L}+c_{1,0}\cdot c'_{0,0})\cdot s_L+c_{1,L}\cdot c'_{1,L}\cdot s_L^2))$$

$$=(c_{0,0}\cdot c'_{0,0},\cdots,c_{0,L}\cdot c'_{0,L})+((c_{0,0}\cdot c'_{1,0}+c_{1,0}\cdot c'_{0,0})\cdot s_0,\cdots,(c_{0,L}\cdot c'_{1,L}+c_{1,0}\cdot c'_{0,0})\cdot s_L)+(c_{1,0}\cdot c'_{1,0}\cdot s_0^2,\cdots,c_{1,L}\cdot c'_{1,L}\cdot s_L^2)$$

$$=\boldsymbol{c}_0\odot\boldsymbol{c}_0{}'+(\boldsymbol{c}_0\odot\boldsymbol{c}_1{}'+\boldsymbol{c}_1\odot\boldsymbol{c}_0{}')\odot\boldsymbol{s}+\boldsymbol{c}_1\odot\boldsymbol{c}_1{}'\odot\boldsymbol{v}\odot\boldsymbol{s}$$

$$=(\boldsymbol{c}_0+\boldsymbol{c}_1\odot\boldsymbol{s})\odot(\boldsymbol{c}_0{}'+\boldsymbol{c}_1{}'\odot\boldsymbol{s})(\mathrm{mod}\ p\ \mathrm{mod}\ t)$$

$$=\boldsymbol{m}\odot\boldsymbol{m}'$$

假设二者噪声相乘后仍小于 $p/2$，上式可正确解密，所以方案满足乘法同态性。

4.4 扩展的密钥转换技术

密文乘法操作使元素个数从 $2(L+1)$ 增长到 $3(L+1)$，共增加了 $(L+1)$ 个元素，导致密文尺寸空间迅速膨胀，其对应的私钥也会呈相应倍数增长，从而影响解密效率。基于 Brakerski 等[7]的密钥转换技术，结合本文构造的批处理同态加密方案，给出适配的扩展密钥转换技术，以减小密文尺寸和对应的私钥维数。

为使表达更清晰直观，不妨设 $(c_{0,i}\cdot c'_{0,i},c_{0,i}\cdot c'_{1,i}+c_{1,i}\cdot c'_{0,i},c_{1,i}\cdot c'_{1,i})\xleftarrow{\triangle}(c_{0,i},c_{1,i},c_{2,i})$。令 $(\boldsymbol{c}_0,\boldsymbol{c}_1,\boldsymbol{c}_2)\leftarrow\{(c_{0,i},c_{1,i},c_{2,i})\}_{i=0}^{L}$，即 $\boldsymbol{c}_0=(c_{0,0},c_{0,1}\cdots,c_{0,L})$，$\boldsymbol{c}_1,\boldsymbol{c}_2$ 同理，则 $(\boldsymbol{c}_0,\boldsymbol{c}_1,\boldsymbol{c}_2)$ 对应私钥为 $sk'=(1,\boldsymbol{s},\boldsymbol{s}\odot\boldsymbol{s})$。现给出扩展的密钥转换算法 KeySwitch$(sk',sk'',(\boldsymbol{c}_0,\boldsymbol{c}_1,\boldsymbol{c}_2))$，将密文 $\boldsymbol{ct}_{\mathrm{mlt}}=(\boldsymbol{c}_0,\boldsymbol{c}_1,\boldsymbol{c}_2)$ 转换成 $\boldsymbol{ct}'_{\mathrm{mlt}}=(\boldsymbol{c}_0{}',\boldsymbol{c}_1{}')$，相应地，私钥转换为 $sk''=(1,\boldsymbol{s}')$。具体算法如算法 1 所示。

算法 1 KeySwitch$(sk',sk'',(\boldsymbol{c}_0,\boldsymbol{c}_1,\boldsymbol{c}_2))$

输入：sk′，sk″，$\mathbf{ct}_{\mathrm{mlt}}=(\mathbf{c}_0,\mathbf{c}_1,\mathbf{c}_2)$

输出：$\mathbf{ct}'=(\mathbf{c}_0,\mathbf{c}_1)$

计算：i From 0 to L

$\mathrm{b}_{\kappa_i,i}=-(\mathrm{a}_{\kappa_i,i}\mathrm{s}_i'+\mathrm{te})+\mathrm{t}^{\kappa_i}\mathrm{s}_i^2$

$\mathrm{b}'_{\kappa_1,i}=-(\mathrm{a}'_{\kappa_1,i}\mathrm{s}_i'+\mathrm{te}')+\mathrm{t}^{\kappa_i}\mathrm{s}_i$

其中，$\kappa_i=0,\cdots,\lceil\log_{\mathrm{t}}^{q_i}\rceil-1$。且令 $\mathrm{h}_{\kappa_i,i}=(\mathrm{a}_{\kappa_i,i},\mathrm{b}_{\kappa_i,i}=-(\mathrm{a}_{\kappa_i,i}\mathrm{s}_i'+\mathrm{te})+\mathrm{t}^{\kappa_i}\mathrm{s}_i^2)$，$\mathrm{l}_i=(\mathrm{a}'_{\kappa_1,i},\mathrm{b}'_{\kappa_1,i}=-(\mathrm{a}'_{\kappa_i,i}\mathrm{s}_i'+\mathrm{te}')+\mathrm{t}^{\kappa_i}\mathrm{s}_i)$，并设 $\tau_{\mathrm{sk}'\to\mathrm{sk}''}=\{\mathrm{h}_{\kappa_i,i},\mathrm{l}_{\kappa_i,i}\}_{\kappa_i=0}^{\lceil\log_{\mathrm{t}}^{q_i}\rceil-1}$ 为辅助信息。

令：

$$\mathbf{c}_1\leftarrow(\sum_{\kappa_1=0}^{\lceil\log_{\mathrm{t}}^{q_i}\rceil-1}c_{1,0,\kappa_1}\mathrm{t}^{\kappa_i},\cdots,\sum_{\kappa_i=0}^{\lceil\log_{\mathrm{t}}^{q_i}\rceil-1}\mathbf{c}_{1,\mathrm{L},\kappa_1}\mathrm{t}^{\kappa_i})$$

$$\mathbf{c}_2\leftarrow(\sum_{\kappa_i=0}^{\lceil\log_{\mathrm{t}}^{q_i}\rceil-1}c_{2,0,\kappa_1}\mathrm{t}^{\mathrm{i}},\cdots,\sum_{\kappa_i=0}^{\lceil\log_{\mathrm{t}}^{q_i}\rceil-1}c_{2,\mathrm{L},\kappa_1}\mathrm{t}^{\kappa_i})$$

其中，$c_{1,i,\kappa_i},c_{2,i,\kappa_i}\in\mathrm{R}_{\mathrm{t}}$。计算：

$$\mathbf{c}_0^{\mathrm{relin}}\leftarrow\mathbf{c}_0+(\sum_{\kappa_j=0}^{\lceil\log_{\mathrm{t}}^{q_i}\rceil-1}c_{2,0,\kappa_i}\mathrm{b}_{\kappa_i,i},\cdots,\sum_{\mathrm{j}=0}^{\lceil\log_{\mathrm{t}}^{q_i}\rceil-1}c_{2,\mathrm{L},\kappa_i}\mathrm{b}_{\kappa_i,i})$$

$$\mathbf{c}_1^{\mathrm{relin}}\leftarrow(\sum_{\kappa_i=0}^{\lceil\log_{\mathrm{t}}^{q_i}\rceil-1}c_{2,0,\kappa_i}\mathrm{a}_{\kappa_i,i},\cdots,\sum_{\kappa_i=0}^{\lceil\log_{\mathrm{t}}^{q_i}\rceil-1}c_{2,\mathrm{L},\kappa_i}\mathrm{a}_{\kappa_i})$$

$$\mathbf{c}_0{}'\leftarrow\mathbf{c}_0^{\mathrm{relin}}+(\sum_{\kappa_i=0}^{\lceil\log_{\mathrm{t}}^{q_i}\rceil-1}c_{1,0,\kappa_i}\mathrm{b}'_{\kappa_i,i},\cdots,\sum_{\kappa_i=0}^{\lceil\log_{\mathrm{t}}^{q_i}\rceil-1}c_{1,\mathrm{L},\kappa_i}\mathrm{b}'_{\kappa_i})$$

$$\mathbf{c}_1{}'\leftarrow\mathbf{c}_1^{\mathrm{relin}}+(\sum_{\kappa_i=0}^{\lceil\log_{\mathrm{t}}^{q_i}\rceil-1}c_{1,0,\kappa_i}\mathrm{a}'_{\kappa_i,i},\cdots,\sum_{\kappa_i=0}^{\lceil\log_{\mathrm{t}}^{q_i}\rceil-1}c_{1,\mathrm{L},\kappa_i}\mathrm{a}'_{\kappa_i})$$

新密文即为 $(\mathbf{c}_0{}',\mathbf{c}_1{}')$，其对应的私钥为 $(1,\mathbf{s}')$。

定理 3 算法 1 是正确的，且转换得到的新密文 $(\boldsymbol{c}_0{}',\boldsymbol{c}_1{}')$ 能够利用相应私钥 $(1,\boldsymbol{s}')$ 进行正确解密。

证明：用私钥 $sk'=(1,s')$ 对 $(\boldsymbol{c}_0{}',\boldsymbol{c}_1{}')$ 进行解密：

$$\boldsymbol{c}_0{}'+\boldsymbol{c}_1{}'\cdot\boldsymbol{s}'$$

$$=\boldsymbol{c}_0+(\sum_{\kappa_i=0}^{\lceil\log_{\mathrm{t}}^{q_i}\rceil-1}c_{2,0,\kappa_i}b_{\kappa_i,i},\cdots,\sum_{\kappa_i=0}^{\lceil\log_{\mathrm{t}}^{q_i}\rceil-1}c_{2,L,\kappa_i}b_{\kappa_i,i})+(\sum_{\kappa_i=0}^{\lceil\log_{\mathrm{t}}^{q_i}\rceil-1}c_{1,0,\kappa_i}b'_{\kappa_i,i},\cdots,\sum_{\kappa_i=0}^{\lceil\log_{\mathrm{t}}^{p}\rceil-1}c_{1,L,\kappa_i}b'_{\kappa_i,i})+(\sum_{\kappa_i=0}^{\lceil\log_{\mathrm{t}}^{q_i}\rceil-1}c_{2,0,\kappa_i}a_{\kappa_i,i}s_0,\cdots,\sum_{\kappa_i=0}^{\lceil\log_{\mathrm{t}}^{q_i}\rceil-1}c_{2,L,\kappa_i}a_{\kappa_i,i}s_L)+(\sum_{\kappa_i=0}^{\lceil\log_{\mathrm{t}}^{q_i}\rceil-1}c_{1,0,\kappa_i}a'_{\kappa_i,i}s_0,\cdots,\sum_{\kappa_i=0}^{\lceil\log_{\mathrm{t}}^{q_i}\rceil-1}c_{1,L,\kappa_i}a'_{\kappa_i,i}s_L)$$

观察上式可知，每个向量中的元素形式是一样的，不妨对各向量的第一项的加和进行研究，进而得到整个向量的结果，即：

$$c_{0,0}+\sum_{\kappa_i=0}^{\lceil\log_{\mathrm{t}}^{q_i}\rceil-1}c_{2,0,\kappa_i}b_{\kappa_i,i}+\sum_{\kappa_i=0}^{\lceil\log_{\mathrm{t}}^{q_i}\rceil-1}c_{1,0,\kappa_i}b'_{\kappa_i,i}+\sum_{\kappa_i=0}^{\lceil\log_{\mathrm{t}}^{q_i}\rceil-1}c_{2,0,\kappa_i}a_{\kappa_i,i}s_0+\sum_{\kappa_i=0}^{\lceil\log_{\mathrm{t}}^{q_i}\rceil-1}c_{1,0,\kappa_i}a'_{\kappa_i,i}s_0$$

将 $b_{\kappa_i,i},b'_{\kappa_i,i}$ 的值代入上式，有：

$$c_{0,0}+\sum_{\kappa_i=0}^{\lceil\log_{\xi}^{q_i}\rceil-1}c_{2,0,\kappa_i}b_{\kappa_i,i}+\sum_{\kappa_i=0}^{\lceil\log_{\xi}^{q_i}\rceil-1}c_{1,0,\kappa_i}b'_{\kappa_i,i}+\sum_{\kappa_i=0}^{\lceil\log_{\xi}^{q_i}\rceil-1}c_{2,0,\kappa_i}a_{\kappa_i,i}s_0+\sum_{\kappa_i=0}^{\lceil\log_{\xi}^{q_i}\rceil-1}c_{1,0,\kappa_i}a'_{\kappa_i,i}s_0$$

$$=c_{0,0}+\sum_{\kappa_i=0}^{\lceil\log_{\xi}^{q_i}\rceil-1}c_{2,0,\kappa_i}t^{\kappa_i}s_0^2-\sum_{\kappa_i=0}^{\lceil\log_{\xi}^{q_i}\rceil-1}c_{2,0,\kappa_i}te+\sum_{\kappa_i=0}^{\lceil\log_{\xi}^{q_i}\rceil-1}c_{1,0,\kappa_i}t^{\kappa_i}s_0-\sum_{\kappa_i=0}^{\lceil\log_{\xi}^{q_i}\rceil-1}c_{1,0,\kappa_i}te'$$

$$=c_{0,0}+c_{1,0}\cdot s_0+c_{2,0}\cdot s_0^2-t\Big(\sum_{\kappa_i=0}^{\lceil\log_{\xi}^{q_i}\rceil-1}c_{1,0,\kappa_i}e'+\sum_{\kappa_i=0}^{\lceil\log_{\xi}^{q_i}\rceil-1}c_{2,0,\kappa_i}e\Big)$$

$$=m_0m_0'+\tilde{e}_0=m_0m_0'(\mathrm{mod}\ q_i\ \mathrm{mod}\ t)$$

故整体向量为：

$$\boldsymbol{c}_0'+\boldsymbol{c}_1'\cdot\boldsymbol{s}'=(m_0m_0',m_1m_1',\cdots,m_Lm_L')(\mathrm{mod}\ q_i\ \mathrm{mod}\ t)$$

证毕。

4.5　模转换技术

在进行一次密文乘法后，首先利用 KeySwitch 算法对密文维数进行约减，进入到下一层电路。本节在此基础上，通过构造模转换算法来进一步减小密文噪声，具体算法如算法 2 所示。

算法 2　Scale($\boldsymbol{ct}$, q_i, q_{i-1}, t)

输入：$\mathbf{ct}$, $\mathrm{q_i}$, $\mathrm{q_{i-1}}$, t

输出：$\mathbf{ct}'$

计算：

1. $\mathbf{ct}'=[(\mathrm{q_{i-1}}/\mathrm{q_i})\cdot\mathbf{ct}]$；

2. $\mathbf{ct}'\equiv\mathbf{ct}(\mathrm{mod\ t})$。

5　安全性分析与参数选择

5.1　安全性分析

本文方案的安全性是基于 RLWE 问题的，它具备安全、高效等特点，故被广泛应用于全同态密码设计中，其安全性主要取决于 3 个参数：环 R_q 的多项式 $\Phi_m(x)$ 的次数 n、模的数值 q 以及离散高斯分布的标准差 σ。由下面给出的定理 4，将方案的安全性归约到 DRLWE 问题上。

定义 12(IND-CPA 安全)　设有某公钥加密方案 ε，在有界多项式时间内，若存在一个极小函数 $negl(\lambda)$，使得敌手 $\mathcal{A}$ 的优势

$$Adv_{\mathrm{CPA}}[\mathcal{A}]\overset{\triangle}{=}|\Pr[\mathcal{A}(pk,\mathrm{HE.Enc}(0)=1)-\Pr[\mathcal{A}(pk,\mathrm{HE.Enc}(1)=1)]|=negl(\lambda)$$

则该加密方案 ε 是 IND-CPA 安全的。

定理 4[11]　在 $\{\mathrm{DRLWE}_{n,q_i,\chi}\}_{i=0}^{L}$ 问题下，该方案是 CPA 安全的，并且是循环安全的。

证明：令 $\mathcal{A}$ 是对 FHE 方案的一个 IND-CPA 敌手，$Adv_H[\mathcal{A}]$ 表示在一系列 hybird H 中的攻击优势，具体证明如下。

Hybird H_{L+1}：该 Hybird 是 $\mathcal{A}$ 对 Batch. FHE 的 IND-CPA 攻击游戏，敌手得到由 Batch. FHE. Keygen 算法生成的 $pk,evk=\psi_{\kappa_l,l}=\{h_{\kappa_l,l},l_{\kappa_l,l}\}_{\kappa_l=0}^{\lceil\log_{\xi}^{q_l}\rceil-1}$。用 Batch. FHE. Enc 算法对 0 和 1 进行加密，$\mathcal{A}$ 在 H_{L+1} 中的优势为：

$$Adv_{H_{L+1}}[\mathcal{A}]=|\Pr[\mathcal{A}(pk,\mathrm{HE.Enc}(0)=1)-\Pr[\mathcal{A}(pk,\mathrm{HE.Enc}(1)=1)]|=negl(\lambda)$$

Hybird H_L：该 Hybird 与 H_{L+1} 除了运算公钥 evk 的生成不同外，其余都相同。具体来说，运算公钥取自均匀分布，与方案中的生成方式不同，即 $\psi_{\kappa_L,L}\leftarrow R_{q_L}\times R_{q_L}$。

存在一个在时间 $t+poly(\lambda)$ 内解决 $\mathrm{DRLWE}_{n,q_L,\chi}$ 问题的敌手 $\mathcal{B}_L$，且优势为：

$$\mathrm{DRLWE}_{n,q_L,\chi}Adv[\mathcal{B}_L]\geqslant1/2\cdot|Adv_{H_{L+1}}[\mathcal{A}]-Adv_{H_L}[\mathcal{A}]|$$

按照 H_{L+1} 到 H_L 的方法，将运算公钥由方案中的生成方式逐次替换成在 $R_{q_L}\times R_{q_L}$ 上一致均匀选取的方式，如此操作，直到在 H_1 中运算公钥 evk 全部被替换为一致均匀选取的元素。

Hybird H_0：该 Hybird 与 H_1 除了对公钥中 $\boldsymbol{b}$ 的选取不同外，其余基本相同。在 H_0 中，b_i 不再以 $b_i=-a_i\cdot s_i+te$ 的方式产生，而是在 R_{q_i} 中均匀选取。由于在 $\mathrm{DRLWE}_{n,q_0,\chi}$ 假设下，H_1 与 H_0 是计算不可区分的，那么存在在时间 $t+poly(\lambda)$ 内解决问题的敌手 $\mathcal{B}_0$，其优势为：

$$\mathrm{DRLWE}_{n,q_0,\chi}Adv[\mathcal{B}_0]\geqslant1/2\cdot|Adv_{H_1}[\mathcal{A}]-Adv_{H_0}[\mathcal{A}]|$$

敌手 $\mathcal{B}_0$ 从 RLWE 预言机中进行 $L+1$ 随机采样 b_i，并将它们作为公钥($\boldsymbol{b},\boldsymbol{a}$)。若采样取自分布 $A_{s,\chi}$，则 b_i 由 H_1 的生成方式产生；若采样取自均匀分布，则 b_i 由 H_0 的生成方式产生。

Hybird H_{rand}：该 Hybird 与 H_0 除了密文产生方式不同外，其余基本相同。在 H_{rand} 中，密文不再以方案中的方式产生，而是取自一致均匀分布的 $R_{q_i}\times R_{q_i}$。由于 b_i 也是取自均匀分布的，因此($\boldsymbol{bu}+t\boldsymbol{g}+\boldsymbol{m}$)，($\boldsymbol{au}+t\boldsymbol{f}$)与 $R_{q_i}\times R_{q_i}$ 上的均匀分布不可区分，故有：

$$|Adv_{H_{\mathrm{rand}}}[\mathcal{A}]-Adv_{H_o}[\mathcal{A}]|\leqslant negl(\lambda)$$

注意到，在 H_{rand} 中，公钥和密文都是随机均匀选取的，与明文信息相互独立，因此 $Adv_{H_{\mathrm{rand}}}[\mathcal{A}]=0$。

综上可得：

$$Adv_{\mathrm{CPA}}[\mathcal{A}]\leqslant\frac{1}{2}\cdot|Adv_{H_{L+1}}[\mathcal{A}]-Adv_{H_L}[\mathcal{A}]|+\cdots+\frac{1}{2}\cdot|Adv_{H_1}[\mathcal{A}]-Adv_{H_0}[\mathcal{A}]|+|Adv_{H_{rand}}[\mathcal{A}]-Adv_{H_o}[\mathcal{A}]|$$

$$\leqslant2\sum_{i=0}^{L}\mathrm{DRLWE}_{n,q_i,\chi}Adv[\mathcal{B}_i]+negl(\lambda)$$

由此得证。证毕。

5.2　参数设置和效率分析

离散高斯分布 $\chi=D_{\mathbf{Z}^n,\sigma}$，关于标准差 σ，有如下引理。

引理 1[12]　设 $n\in\mathbb{N}$，$\forall\sigma>\omega(\sqrt{\log n})$，对于 $\boldsymbol{x}\leftarrow D_{\mathbf{Z}^n,\sigma}$，有 $\Pr[\|\boldsymbol{x}\|_\infty>\sigma\sqrt{n}]\leqslant2^{-n+1}$。

由引理 1 知，高斯分布中的元素的界为 $\sigma\sqrt{n}$。

定义 13[13](埃尔米特因子 δ^m)　设一个 m 维格为 Λ，其中一个格基为 $\boldsymbol{B}$，$\exists\delta^m$，$\exists\|b_1\|=\delta^m\det(\Lambda)^{\frac{1}{m}}$，其中 b_1 是格

基 $\boldsymbol{B}$ 中的最短向量，δ 也被称为埃尔米特根因子。

定理 5[13] 给定 δ，约化出具有埃尔米特因子 δ^m 的格基所需的时间主要取决于 δ。

定理 6[14] 给定一个埃尔米特根因子 δ，计算出最短向量的长度为 $\alpha \cdot \frac{q}{\sigma} \leqslant 2^{2\sqrt{n\log q/\log\sigma}}$，其中 $\alpha = \sqrt{\ln(1/\varepsilon)/\pi}$，所需时间约为 $\log T = 1.8/\lg\delta - 110$。

故可以根据 $\alpha \cdot q/\sigma \leqslant 2^{2\sqrt{n\log q/\log\sigma}}$ 确定本文方案的参数。根据实际，不妨令区分优势为 $\varepsilon = 2^{-64}$，取安全参数 $\lambda = 128$，攻击时间 $T = 2^{128}$，则可计算出 $\alpha \approx 3.758$，$\sigma \approx 1.005$，将其代入 $\alpha \cdot q/\sigma \leqslant 2^{2\sqrt{n\log q/\log\sigma}}$ 得 $1.910 + \log q - \log\sigma \leqslant 0.173\sqrt{n\log q}$，通过确定 n 即可得到 q，σ 的值。如 $n = 512$ 时，$|\log q| = 20$，$\sigma = 13.41$。

具体参数设置如表 1 所列。

表 1 参数设置

Table 1 Parameter setting

n	$\log q$	σ
256	19	6.58
512	20	13.41
1024	38	55.06
2048	64	9.69

下面将本文提出的批处理同态加密方案与第 3 节中的方案进行对比，结果如表 2 所列。对比分析后可以看出，本方案在效率上有明显的提高。

表 2 效率分析

Table 2 Eiffciency analysis

	明文数	密文尺寸	公钥规模	私钥规模
方案	$O(n\lambda)$	$O(\lambda\log_t^{qB})$	$O(\lambda\delta_R)$	$O(\lambda B)$
LNV11	$O(1)$	$O(\log_t^{qB})$	$O(\delta_R)$	$O(B)$
BGV12	$O(n)$	$O(\log qB)$	$O(n\log^2 q)$	$O(n\log B)$

本文运用中国剩余定理对明文进行打包，使方案效率得到明显提升：公、私钥规模是 LNV11 方案的 λ 倍，但一次处理的明文数有显著提高，是原始方案的 $n\lambda$ 倍，进而加密效率有着较大提升。综合可知，本文方案较 LNV11 方案在效率上提升了 n 倍，更具有实际应用的可行性。

结束语 在当前大数据与云计算的背景下，全同态加密的应用前景十分广泛。本文基于文献[8]的部分同态加密方案，提出了基于 RLWE 的批处理同态加密方案。该方案利用中国剩余定理(CRT)打包多个明文槽到一个密文中。文中给出了打包密文的同态操作结果，利用两种技术约减了噪声，使方案可以进行多次同态操作，提高了加密运算的效率，并给出了方案的参数设定以及效率对比。实验分析表明本文方案具备较高的实用价值。

参 考 文 献

[1] FENG D G, ZHANG M, ZHANG Y, et al. Study on Cloud Computing Security [J]. Journal of Software, 2011, 22(1): 71-83. (in Chinese)
冯登国，张敏，张妍，等. 云计算安全研究[J]. 软件学报，2011，22(1)：71-83.

[2] RIVEST R L, ADLMAN L, DERTOUZOS M L. On data banks and privacy homomorphisms[J]. Foundations of Secure Computation, 1978, 4(11): 169-180.

[3] GENTRY C. Fully homomorphic encryption using ideal lattices [C]// Proc. of the 41st Annual ACM Symposium on Theory of Computing. New York: ACM Press, 2009: 169-178.

[4] GENTRY C, HALEVI S. Implementing Gentry's Fully-Homomorphic Encryption Scheme [C] // EUROCRYPT. 2011: 129-148.

[5] SMART N P, VERCAUTEREN F. Fully homomorphic SIMD operations[J]. Designs, Codes and Cryptography, 2014, 71(1): 57-81.

[6] BRAKERSKI Z, VAIKUNTANATHAN V. Efficient Fully Homomorphic Encryption from (Standard) LWE[C] // Foundations of Computer Science. IEEE, 2011: 97-106.

[7] GENTRY C, HALEVI S, SMART N P. Fully homomorphic encryption with polylog overhead[C] // Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg, 2012: 465-482.

[8] NAEHRIG M, LAUTER K, VAIKUNTANATHAN V. Can homomorphic encryption be practical? [C]// Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop. ACM, 2011: 113-124.

[9] LIDL R, NIEDERREITER H. Finite fields[M]. Cambridge: Cambridge University Press, 1997.

[10] LYUBASHEVSKY V, PEIKERT C, REGEV O. On ideal lattices and learning with errors over rings[C] // Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg, 2010: 1-23.

[11] BRAKERSKI Z, GENTRY C, VAIKUNTANATHAN V. (Leveled) fully homomorphic encryption without bootstrapping[J]. ACM Transactions on Computation Theory (TOCT), 2014, 6(3): 13.

[12] MICCIANCIO D. The shortest vector in a lattice is hard to approximate to within some constant[J]. SIAM Journal on Computing, 2001, 30(6): 2008-2035.

[13] GAMA N, NGUYEN P. Predicting lattice reduction[C] // Advances in Cryptology-EUROCRYPT 2008. 2008: 31-51.

[14] LINDNER R, PEIKERT C. Better Key Sizes (and Attacks) for LWE-Based Encryption[C] // CT-RSA. 2011: 319-339.

[15] GENTRY C. A fully homomorphic encryption scheme[D]. Stanford University, 2009.

[16] CHEON J, KIM J, LEE M, et al. CRT-based fully homomorphic encryption over the integers [J]. Information Sciences, 2015, 310: 149-162.

[17] REGEV O. On lattices, learning with errors, random linear codes, and cryptography[C] // Acm Symposium on Theory of Computing. ACM, 2005.