计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2020.20200422
57(10): 2117-2124, 2020

# 循环安全的同态加密方案

赵秀凤 付 雨 宋巍涛
(信息工程大学密码工程学院 郑州 450001)
(zhao_xiu_feng@163.com)

# Circular Secure Homomorphic Encryption Scheme

Zhao Xiufeng, Fu Yu, and Song Weitao
(*College of Cryptography Engineering*, *Information Engineering University*, *Zhengzhou* 450001)

**Abstract** Homomorphic encryption allows evaluation on encrypted data, and it is an important encryption technique to realize data privacy security in cloud computing, big data and machine learning. Constructions of fully homomorphic encryption employ a "bootstrapping" technique, which enforces the public key of the scheme to grow linearly with the maximal depth of evaluated circuits. This is a major bottleneck with regards to the usability and the efficiency of the scheme. However, the size of the public key can be made independent of the circuit depth if the somewhat homomorphic scheme can securely encrypt its own secret key. Achieving circular secure somewhat homomorphic encryption has been an interesting problem which is worth studying. This paper presents a circular secure public key homomorphic encryption scheme using noise flooding technique, and gives the security proof and parameter setting; furthermore, by introducing the refuse sampling technique, an optimized circular secure public key homomorphic encryption scheme is given, and the system parameters are reduced from the super polynomial level to the polynomial level, which greatly reduces the public key and ciphertext size. And then the computational complexity of ciphertext evaluation can be effectively improved and the performance of homomorphic encryption scheme be improved.

**Key words** homomorphic encryption; circular secure; learning with errors problem; noise flooding technique; reject sampling

**摘 要** 全同态加密可以对密文进行有效计算,是实现云计算、大数据以及机器学习中数据隐私安全的一项重要密码技术.利用"自举"技术可以构造全同态加密方案,但是使得运算密钥随着运算电路的深度线性增长,这是全同态加密方案实用性的一个主要瓶颈.然而,如果同态加密方案满足循环安全性,即可以对方案的私钥进行安全的加密,则可以使得运算密钥的规模独立于运算电路的深度.因此,满足循环安全性的同态加密方案是值得研究的一个问题.基于噪声淹没技术,给出了循环安全的公钥同态加密方案,并给出了安全性证明和参数设置;进一步,通过引入拒绝采样技术,给出了优化的循环安全公钥同态加密方案,在增加部分采样算法的代价下,将系统参数从超多项式级降低到多项式级,大大约减方案公钥和密文规模,从而可以有效改善密文运算的计算复杂性,提升同态加密方案的性能.

**收稿日期**:2019-06-10;**修回日期**:2020-07-24
**基金项目**:国家自然科学基金项目(61601515,61702578,61902428);河南省自然科学基金项目(162300410332);军事类研究生资助课题(JYKT910372019307)
This work was supported by the National Natural Science Foundation of China (61601515, 61702578, 61902428), the Natural Science Foundation of Henan Province of China (162300410332), and the Military Graduate Project (JYKT910372019307).

**关键词** 同态加密;循环安全;错误学习问题;噪声淹没技术;拒绝采样

**中图法分类号** TP391

当今世界,大数据、云计算等蓬勃发展,使互联网时代迈上一个新台阶.然而,云计算和大数据所具有的数据集中、资源共享、高度互联、全面开放等特点,一方面打破了传统 IT 领域的信息孤岛,另一方面也带来了更严峻的安全问题.云计算模式的核心是数据,本质是服务,特点是"零信任",因此,"数据在不可信环境下的安全计算(服务)"成为解决云计算安全的一个关键问题.2009 年 IBM 实验室的 Gentry 首次给出了"全同态加密"(fully homomorphic encryption, FHE)方案[1-2].全同态加密可以在不解密的情况下对密态数据进行各种运算,其结果在解密后与对明文进行相应运算的结果是一样的.全同态加密不仅能够对密文进行任意的盲操作,而且还能够对计算/操作行为本身进行加密的密码算法,因此,全同态加密真正从根本上解决了将数据及操作委托给第三方时的保密问题,使人们既可以充分利用云计算强大的计算和存储能力为用户提供海量密文处理服务,又可以自己管理保证数据安全的密钥,实现了"数据在不可信环境下安全计算(服务)".

Gentry 给出的 FHE 框架中利用 bootstrapping 技术实现了"全同态"特性,bootstrapping 技术的关键环节是在服务器端对同态计算的密文实施周期性的重加密操作,即对密文进行刷新,从而实现降低噪声的目的.为此需要对私钥 $s$ 的每一位进行加密,所得结果作为重加密的公钥.为了周期性实施重加密操作,需要引入公私钥链,公钥链($pk_1, pk_2, \cdots, pk_{l+1}$)以及加密后的私钥链($\overline{sk}_1, \overline{sk}_2, \cdots, \overline{sk}_l$),其中 $\overline{sk}_i = Enc(pk_{i+1}, sk_i)$, $i=1,2,\cdots,l$,密钥链的长度 $l$ 随着运算电路的深度线性增长.对于加密方案而言,只有加密方案满足密钥独立消息(key dependent message, KDM)安全,才可以保证加密方案在加密私钥相关消息的情况下也是安全的.因此,设计满足 KDM 的同态加密方案可以使得密钥链的长度与运算电路的深度无关,从而有效实现 FHE 方案公钥与密文规模约减,提高 FHE 方案的运算效率.

本文的主要贡献包括 2 个方面:

1) 给出了满足循环安全性的公钥同态加密方案,并给出了安全性证明和参数设置分析;

2) 通过引入拒绝采样技术,对上述满足循环安全性的同态加密方案进行了优化,将方案参数从超多项式级降低到多项式级,大大约减了参数规模,有效提升了方案的效率.

## 1 相关工作

关于循环安全的加密方案已有一些研究成果.Boneh 等人基于无随机 Oracle 的 DDH 假设构造了一个循环安全的公钥加密方案[3].Applebaum 等人根据基于错误学习(learning with error, LWE)问题的 Regev 加密方案[4],构造了循环安全的有效密码体制[5].在循环安全的同态加密方面,杨晓元等人[6]基于 LWE 问题的变形给出了一个对私钥的线性函数满足循环安全的 FHE 方案,但是这个困难假设并不是一个标准的困难假设.Zhao 等人[7]给出了矩阵 GSW 方案[8]满足循环安全性的一个充分条件,但是缺乏必要性证明.2011 年美国密码学年会,Brakerski 和 Vaikuntanathan[9]基于环 LWE 问题给出了一个循环安全的同态加密方案,称为 BV 方案.BV 方案实现循环安全性的基本思路是利用"噪声淹没技术"(noise flooding technique),即在原加密方案的基础上,再引入一个"宽高斯"分布的噪声,从而使得对密钥加密的密文与对普通明文加密的密文不可区分.由高斯分布的叠加性和不可区分性,保证挑战者模拟私钥的密文.

本文给出的循环安全的公钥同态加密方案,通过引入拒绝采样技术有效约减了密文模的规模,提升了同态运算的效率.该研究成果可以为同态加密方案设计与实现提供理论参考.

## 2 基础知识

本节主要介绍本文用到的基本定义和重要的引理.

### 2.1 离散高斯分布

标准方差为 $\sigma$、中心为 $c$ 的高斯分布定义为

$$\rho_{\sigma,c}(x)=\exp\left(\frac{-(x-c)^2}{2\sigma^2}\right), \forall x\in\mathbb{R}.$$

对于 $\forall \boldsymbol{x},\boldsymbol{c}\in\mathbb{R}^n$,离散高斯的分布概率密文函数定义为

$$\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{x})=\exp\left(\frac{-\|(\boldsymbol{x}-\boldsymbol{c})\|^2}{2\sigma^2}\right).$$

$\mathbb{Z}$ 和 $\mathbb{Z}^n$ 上的离散高斯分别定义为

$$D_{\sigma,c}(x)=\frac{\rho_{\sigma,c}(x)}{\rho_{\sigma,c}(\mathbb{Z})},$$

$$D^n_{\sigma,c}(\boldsymbol{x})=\frac{\rho_{\sigma,c}(\boldsymbol{x})}{\rho_{\sigma,c}(\mathbb{Z})^n}.$$

**引理 1**[10]. 令 $n\in N$,对于任意的实数 $\sigma=\omega(\sqrt{\log n})$,有 $Pr_{x\leftarrow D_{\mathbb{Z}^n,\sigma}}[\|\boldsymbol{x}\|>\sigma\sqrt{n}]\leqslant 2^{-n+1}$.

**引理 2**[11]. 令 $n\in N$,对于任意的实数 $\sigma=\omega(\sqrt{\log n})$,对任意的 $\boldsymbol{c}\in\mathbb{Z}^n$,$D_{\mathbb{Z}^n,\sigma}$ 和 $D_{\mathbb{Z}^n,\sigma,c}$ 之间的统计距离至多为 $\frac{\|\boldsymbol{c}\|}{\sigma}$.

**引理 3**[12]. 令 $n\in N$,$m=2n$,$f(x)=x^n+1$,令 $R=\mathbb{Z}[x]/(f(x))$.对于任意的 $s,t\in R$,

$$\|s\times t(\bmod f(x))\|\leqslant\sqrt{n}\times\|s\|\times\|t\|,$$

$$\|s\times t(\bmod f(x))\|_\infty\leqslant n\times\|s\|_\infty\times\|t\|_\infty.$$

**引理 4**[13]. 对于 $\sigma>0$,$r\geqslant\frac{1}{\sqrt{2\pi}}$,有:

$$Pr[\|\boldsymbol{x}\|_2>r\sigma\sqrt{n};\boldsymbol{x}\overset{\$}{\leftarrow}D_{\mathbb{Z}^n,\sigma}]<(\sqrt{2\pi e r^2}\times e^{-\pi r^2})^n.$$

特别地,当 $n=1$,$r=6$ 时,有:

$$Pr[\|\boldsymbol{x}\|_2>6\sigma;\boldsymbol{x}\overset{\$}{\leftarrow}D_{\mathbb{Z},\sigma}]<2^{-156.792}.$$

**引理 5**[14]. 令 $\lambda$ 为安全参数.$\Phi_m(x)=x^n+1$ 是度为 $n=\varphi(m)=m/2$ 的 $m$ 次分圆多项式.令 $\sigma\geqslant\omega(\sqrt{\log n})$ 为一个实数,$q\equiv 1(\bmod m)$ 为素数.令 $R=\mathbb{Z}[x]/\langle\Phi_m(x)\rangle$,则存在一个从 $2^{\omega(\log n)}\times(q/\sigma)$-近似 R-SVP 问题到 $\mathrm{RLWE}_{\Phi_m,q,\chi}$ 的随机归约算法,其中,$\chi=D_{\mathbb{Z}^n,\sigma}$ 为离散高斯分布.归约算法的运行时间为 $poly(n,q)$.

### 2.2 拒绝采样

拒绝采样技术由 Neumann 提出,给出了通过源概率分布采样得到目标概率分布采样的一个方法[15].PKC2008,Lyubashevsky 利用拒绝采样构造了基于格的身份识别协议[16].Crypt2013,Ducas 等人利用拒绝采样构造了基于格的 BLISS 数字签名算法[17].NIST 征集的多数后量子数字签名候选算法也采用了拒绝采样技术.

**引理 6.** 拒绝采样.令 $V$ 是任意一个集合,$h:V\to\mathbb{R}$ 和 $f:\mathbb{Z}^m\to R$ 为概率分布.若 $g_v$ 是以 $v$ 为索引的一簇概率分布,并且存在一个 $M\in\mathbb{R}$,使得:

$$\forall v\in V,\forall z\in\mathbb{Z}^m,M.g_v(z)\geqslant f(z),$$

那么,2 个算法输出的分布是相同的:

1) $v\leftarrow h$,$z\leftarrow g_v$,以概率 $f(z)/(M.g_v(z))$ 输出 $(z,v)$;

2) $v\leftarrow h$,$z\leftarrow f$,以概率 $1/M$ 输出 $(z,v)$.

### 2.3 同态加密的循环安全性定义

如果密钥由相应的公钥加密后依然是安全的,那么加密方案才能实现循环安全,即循环安全加密方案可以抵抗密钥相关消息攻击.给定安全参数 $\lambda$,令 $\mathcal{K}$ 为密钥空间,令 $f$ 为从 $\mathcal{K}$ 到 $\mathcal{C}$ 的函数.一个同态加密方案 $HE=\{KeyGen,Enc,Dec,Eval\}$ 关于 $f$ 满足循环安全性,如果对于所有的 PPT 敌手 $\mathcal{A}$,敌手 $\mathcal{A}$ 赢得下面游戏的概率是可忽略的:

1) 挑战者计算 $(pk,sk,evk)\leftarrow KeyGen(\lambda)$,并随机选择一位 $b\leftarrow\{0,1\}$;

2) 令 $f_+:\mathcal{M}\times\mathcal{M}\to\mathcal{M}$ 为一个函数,计算 $f_+(x,y)=x+y\in\mathcal{M}$.挑战者计算挑战密文并发送给敌手 $\mathcal{A}$.

$$c^*=\begin{cases}Eval_{evk}(f_+,Enc_{pk}(0),f(sk)), & b=0,\\ Enc_{pk}(0)\in\mathcal{C}, & \text{otherwise.}\end{cases}$$

3) 敌手 $\mathcal{A}$ 输出一个猜测位 $b'\in\{0,1\}$.

敌手 $\mathcal{A}$ 的优势定义为 $Adv(\mathcal{A})=\Pr[b=b']-1/2$.

在基于 LWE 的 FHE 方案中,$Eval_{evk}(f_+,Enc_{pk}(0),f(sk))$ 可以视为加密 $f(sk)$ 的密文.

## 3 循环安全的公钥同态加密方案

文献[9]给出了对称版本的支持私钥 $sk$ 的 $d$ 次多项式的 KDM 安全同态加密方案,我们称为 KDM.SKHE.这里,我们给出 KDM 安全的非对称版本的同态加密方案.令 $\mathcal{P}_d=\mathcal{P}_d[R_t]$ 为 $R_t$ 上度为 $d$ 的多项式集合,即:

$$\mathcal{P}_d=\left\{p(z)=\sum_{i=1}^{d}\alpha_i z^i,\alpha_i\in R_t\right\}.$$

为了实现对私钥 $sk$ 的多项式 $p(sk)$ 的 KDM 安全性,我们利用对称版本的方法,将标准的同态加密的密文 $(c_0,c_1)$ 扩展为 $(c_0,c_1,\cdots,c_d)$,其中 $d$ 为多项式 $p(sk)$ 的度.我们令 $d=2$,即我们考虑对私钥 $sk$ 的平方函数满足循环安全性的同态加密方案,记作 KDM.PKHE.

### 3.1 方案描述

具体算法描述为:

1) KDM.PKHE.$PamameterSet$.令 $\lambda$ 为安全参数.选择素数 $q$,$t\in\mathbb{Z}_q^*$,$f(x)=x^n+1\in\mathbb{Z}[x]$,以及多项式环 $R_q=\mathbb{Z}_q/\langle f(x)\rangle$ 上的离散高斯分布 $D_{\mathbb{Z}^n,\sigma}$ 和 $D_{\mathbb{Z}^n,\sigma'}$.$R_t$ 为方案的明文空间.

2) KDM.PKHE.$Keygen(1^\lambda)$.随机选择 $a_0\in R_q$,从离散高斯分布采样得到 $s,e_0\leftarrow D_{\mathbb{Z}^n,\sigma}$,计算

$b_0=a_0s+te_0$,输出私钥 $sk=s$ 和公钥 $pk=(a_0,b_0)$.

3) KDM.PKHE.$Enc(pk,m)$.对于消息 $m\in R_t$,按照方式生成密文 $\boldsymbol{c}=(c_0,c_1,c_2)\in R_q^3$:

首先生成 2 个二元组 $\{(a_i=a_0v_i+te_i,b_i=b_0v_i+te_i')\}_{i=1,2}$,其中 $a_i\xleftarrow{\$}R_q,v_i,e_i\xleftarrow{\$}D_{\mathbb{Z}^n,\sigma},e_i'\xleftarrow{\$}D_{\mathbb{Z}^n,\sigma'}$,然后计算密文 $c_0=b_1+m;c_1=b_2-a_1;c_2=-a_2$.

4) KDM.PKHE.$Dec(sk,c)$.令 $\boldsymbol{s}=(1,s^1,\cdots,s^d)$,计算 $\langle\boldsymbol{c},\boldsymbol{s}\rangle=\sum_{i=0}^{d}c_is^i$,当 $\|\langle\boldsymbol{c},\boldsymbol{s}\rangle\|_\infty<q/2$ 时解密正确,输出 $m=\langle\boldsymbol{c},\boldsymbol{s}\rangle \bmod t$.

$$\langle\boldsymbol{c},\boldsymbol{s}\rangle=\sum_{i=0}^{2}c_is^i=(b_1+m)+(b_2-a_1)\times s-a_2.s^2=m+\sum_{i=1}^{2}(b_i-a_is)s^{i-1}=m+\sum_{i=1}^{2}((a_0s+te_0)v_i+te_i'-(a_0v_i+te_i)s)\times s^{i-1}=m+\sum_{i=1}^{2}t(e_i'+e_0v_i-e_is)s^{i-1}.$$

故上述无穷范数小于 $q/2$ 时,则可以解密成功.

### 3.2 循环安全性证明

为了给出 KDM.PKHE 方案的循环安全性证明,我们首先证明引理:

**引理 7.** 设 $\xi$ 和 $\eta$ 是 $\mathbb{Z}_q$ 上 2 个独立的随机变量,且 $\xi$ 在 $\mathbb{Z}_q$ 上服从均匀分布,那么 $\xi+\eta$ 在 $\mathbb{Z}_q$ 上也服从均匀分布.

证明. 设 $\xi$ 和 $\eta$ 独立,则 $\forall z\in\mathbb{Z}_q$,有:

$$Pr[\xi+\eta=z \bmod q]=\sum_{i\in\mathbb{Z}_q}Pr[\xi=z-i \bmod q\ \wedge\ \eta=i]=\sum_{i\in\mathbb{Z}_q}Pr[\xi=z-i \bmod q]\times Pr[\eta=i].$$

由 $\xi$ 在 $\mathbb{Z}_q$ 上服从均匀分布知:

$$Pr[\xi=z-i \bmod q]\equiv\frac{1}{q},$$

因此有:

$$Pr[\xi+\eta=z \bmod q]=\frac{1}{q}\sum_{i\in\mathbb{Z}_q}Pr[\eta=i]=\frac{1}{q},$$

即 $\xi+\eta$ 在 $\mathbb{Z}_q$ 上服从均匀分布. 证毕.

**推论 1.** 设 $\xi$ 和 $\eta$ 是 $\mathbb{Z}_q^n$ 上 2 个独立的随机变量,且 $\xi$ 在 $\mathbb{Z}_q^n$ 上服从均匀分布,$\eta$ 服从离散高斯分布 $D_{\mathbb{Z}^n,\sigma}$,若 $\tau\sigma<\frac{q}{2}$,则:

$$\{\xi+\eta\}\approx U(\mathbb{Z}_q^n),$$

即 $\xi+\eta$ 的分布与 $\mathbb{Z}_q^n$ 上的均匀分布计算不可不可区分.

证明. 已知 $\eta$ 服从离散高斯分布 $D_{\mathbb{Z}^n,\sigma}$,根据引理 4,$\eta$ 分量 $\eta_i$ 的取值大约以概率 $1-\exp(\Omega(\tau^2))$ 满足 $|\eta_i|\leqslant\tau\sigma$.因此,若 $\tau\sigma<\frac{q}{2}$,则 $\eta$ 分量 $\eta_i$ 的取值以概率 $1-\exp(\Omega(\tau^2))$ 落于 $\mathbb{Z}_q$ 内.利用引理 7,可得 $\xi+\eta$ 的分布与 $\mathbb{Z}_q^n$ 上均匀分布计算不可区分. 证毕.

**定理 1.** 假设 $\tau\sigma<\frac{q}{2}$,且 $\sigma'=2^{\omega(\log n)}\sigma^2$,那么基于判定性 RLWE 假设,我们给出的公钥同态加密方案 KDM.PKHE 关于 $f(sk)=s^2$ 满足 KDM 安全性.

证明. 对于任意多项式时间的攻击者 $\mathcal{A}$,令 $\mathcal{A}$ 赢得方案 KDM 安全实验的优势为 $\varepsilon$.我们将通过实验 $G_0,G_1,G_2$ 来证明 $\varepsilon$ 是可忽略的,从而完成定理 1 的证明.

实验 $G_0$. 实验 $G_0$ 是真实的 KDM-CPA 安全实验,如 2.3 节定义中所述.在该实验中,挑战者按照加密算法生成挑战密文

$$c^*=\begin{cases}(c_0=b_1+s^2,c_1=b_2-a_1,c_2=-a_2), & b=0,\\ (c_0=b_1+0,c_1=b_2-a_1,c_2=-a_2), & b=1.\end{cases}$$

实验 $G_1$. 除了挑战密文的生成方式不同之外,实验 $G_1$ 和 $G_0$ 相同.实验 $G_1$ 中,挑战者按照 2 种方式生成 $f(sk)$ 的挑战密文:

当 $b=0$ 时,设置挑战密文为

$$c^*=(c_0'=a_1's+te_1',c_1'=a_2's+e_2',c_2'=-a_2'+1);$$

当 $b=1$ 时,设置挑战密文为

$$(c_0=b_1+0,c_1=b_2-a_1,c_2=-a_2).$$

其中,$a_1'=a_1+s,a_2'=a_2+1,e_1',e_2'\xleftarrow{\$}D_{\mathbb{Z}^n,\sigma'}$. 证毕.

**引理 8.** 假设离散高斯参数满足 $\sigma'=2^{\omega(\log n)}\sigma^2$ 和 $6\sigma<\frac{q}{2}$,则敌手区分实验 $G_1$ 和 $G_0$ 的概率是忽略的,即:

$$|adv(\mathcal{A},G_0)-adv(\mathcal{A},G_1)|<negl(\lambda). \quad (1)$$

证明. 对于消息 $s^2\in R_t$,考察同态加密方案的密文 $c_0$:

$$c_0=b_1+s^2=b_0v_1+te_1'+s^2=(a_0s+te_0)v_1+te_1'+s^2=a_0sv_1+te_0v_1+te_1'+s^2=(a_1-te_1)s+te_0v_1+te_1'+s^2=a_1s+te_0v_1+te_1'-te_1s+s^2=(a_1+s)s+t(e_1'+e_0v_1-e_1s). \quad (2)$$

令 $a_1'=a_1+s$,则式(2)等于 $a_1's+t(e_1'+e_0v_1-e_1s)$.

已知 $e_1'$ 的分布服从 $D_{\mathbb{Z}^n,\sigma'}$,令 $e_0v_1-e_1s=E$,根据引理 1 和引理 2 有:

$$\|E\|=\|e_0v_1-e_1s\|\leqslant\|e_0v_1\|+\|e_1s\|\leqslant$$
$$\sqrt{n}\|e_0\|\|v_1\|+\sqrt{n}\|e_1\|\|s\|\leqslant$$
$$2\sqrt{n}(\sigma\sqrt{n})^2=2n^{1.5}\sigma^2.$$

令 $\Delta=2n^{1.5}\sigma^2$,由 $\sigma'=2^{\omega(\log n)}\sigma^2$,有:

$$\frac{\Delta}{\sigma'}=\frac{2n^{1.5}\sigma^2}{2^{\omega(\log n)}\sigma^2}=2^{-\omega(\log n)}.$$

根据引理 2,离散高斯分布 $D_{\mathbf{Z}^n,\sigma'}$ 和离散高斯分布 $D_{\mathbf{Z}^n,\sigma',\Delta}$ 的统计距离是可忽略的,从而有 $e_1'+e_0v_1-e_1s$ 的分布与 $e_1'$ 的分布不可区分.因此,挑战者模拟的挑战密文 $c_0'=a_1's+te_1'$ 与真实的密文 $c_0$ 是不可区分的.

另外,考察同态加密方案的密文 $c_1$:

$$c_1=b_2-a_1=b_0v_2+te_2'-a_1=(a_0s+te_0)v_2+$$
$$te_2'-a_1=a_0sv_2+te_0v_2+te_2'-a_1=(a_2-te_2)s+$$
$$te_0v_2+te_2'-a_1=a_2s-te_2s+te_0v_2+te_2'-a_1=$$
$$a_2s-(a_1'-s)+t(e_2'+e_0v_2-e_2s)=$$
$$(a_2+1)s+t(e_2'+e_0v_2-e_2s)-a_1'. \quad (3)$$

令 $a_2'=a_2+1$,则式(3)等于 $a_2's+t(e_2'+e_0v_2-e_2s)-a_1'$.

同理由 $\sigma'=2^{\omega(\log n)}\sigma^2$,可得噪声 $e_1'$ 足以"淹没" $e_0v_1-e_1s$,即 $e_1'+e_0v_1-e_1s$ 的分布与 $e_1'$ 的分布不可区分.又 $a_2'=a_2+1$ 也服从 $R_q$ 上的均匀分布.因此,敌手模拟的挑战密文 $c_1'=a_2's+te_2'$ 与真实的密文 $c_1$ 不可区分.

因此,敌手区分实验 $G_1$ 和 $G_0$ 的概率是忽略的,引理 8 成立.

实验 $G_2$:除了挑战密文的生成方式不同之外,实验 $G_2$ 和 $G_2$ 相同.实验 $G_2$ 中,挑战者按照 2 种方式生成 $f(sk)$的挑战密文:

当 $b=0$ 时,设置挑战密文为

$$c^*=(c_0'=u_0,c_1'=u_1,c_2'=u_2);$$

当 $b=1$ 时,设置挑战密文为

$$(c_0=b_1+0,c_1=b_2-a_1,c_2=-a_2).$$

其中,$u_i(i=0,1,2)$为环 $R_q$ 中的随机元素. 证毕.

**引理 9.** 假设离散高斯参数满足 $\sigma'=2^{\omega(\log n)}\sigma^2$ 和 $6\sigma<\frac{q}{2}$,则敌手区分实验 $G_1$ 和 $G_0$ 的概率是忽略的,即

$$|adv(\mathcal{A},G_1)-adv(\mathcal{A},G_2)|<negl(\lambda). \quad (4)$$

证明. $a_1\xleftarrow{\$}R_q,s\xleftarrow{\$}D_{\mathbf{Z}^n,\sigma}$是独立的,根据推论 1,当 $6\sigma<\frac{q}{2}$时,$a'_1=a_1+s$ 的分布与 $R_q$ 上的均匀分布不可区分,也即 $a_1'$ 和 $a_1$ 的均服从 $R_q$ 上的均匀分布.由 $a_2'=a_2+1$ 也服从 $R_q$ 上的均匀分布.因此,$(a_1',a_1's+te_1')$和$(a_2',a_2's+e_2')$是 RLWE 问题的实例,从而有:

$$(a_1',a_1's+te_1')\approx(a_1',u_0),u_0\xleftarrow{\$}R_q.$$
$$(a_2',a_2's+e_2')\approx(a_2',u_1),u_1\xleftarrow{\$}R_q.$$

综上,有:

$$(a_1',a_1's+te_1',a_2's+e_2',-a_2')\approx(a_1',u_0,u_1,u_2),$$
$$u_i\xleftarrow{\$}R_q,i=0,1,2.$$

由于在实验 $G_2$ 中,挑战密文是与私钥 $s$ 独立的均匀随机的环元素,因此敌手的优势是可忽略的,即:

$$adv(\mathcal{A},G_2)=negl(\lambda). \quad (5)$$

综合式(1)(4)(5),有:

$$adv(\mathcal{A},G_0)=(adv(\mathcal{A},G_0)-adv(\mathcal{A},G_2))+$$
$$adv(\mathcal{A},G_2)\leqslant|adv(\mathcal{A},G_0)-adv(\mathcal{A},G_2)|+$$
$$adv(\mathcal{A},G_2)\leqslant|adv(\mathcal{A},G_0)-adv(\mathcal{A},G_1)|+$$
$$|adv(\mathcal{A},G_1)-adv(\mathcal{A},G_2)|+$$
$$adv(\mathcal{A},G_2)=negl(\lambda).$$

至此,我们证明了敌手的 KDM 安全性实验中的优势是可忽略的. 证毕.

### 3.3 参数设置

KDM.PKHE 方案中的参数并不是独立选择的,相互之间存在一些制约关系,下面给出详细分析.

1) 为了使得离散高斯分布 $D_{\mathbf{Z}^n,\sigma'}$ 可以"淹没" $D_{\mathbf{Z}^n,\sigma}$上采样的 2 次多项式,要求 $\sigma'=2^{\omega(\log n)}\sigma^2$.

2) 为了保证离散高斯分布 $D_{\mathbf{Z}^n,\sigma}$的采样 $s$ 位于明文空间 $R_t$ 内,要求 $t>\sigma\sqrt{n}$.

3) 为了保证解密正确性,需要满足$\|\langle\boldsymbol{c},\boldsymbol{s}\rangle\|_\infty<q/2$,即:

$$\left\|m+\sum_{i=1}^{2}t(e_i'+e_0v_i-e_is)s^{i-1}\right\|_\infty\leqslant$$
$$\|m\|_\infty+\left\|\sum_{i=1}^{2}t(e_i'+e_0v_i-e_is)s^{i-1}\right\|_\infty\leqslant$$
$$t+\sum_{i=1}^{2}\|t(e_i'+e_0v_i-e_is)s^{i-1}\|_\infty\leqslant$$
$$t+t\|(e_1'+e_0v_1-e_1s)\|_\infty+$$
$$tn\|(e_1'+e_0v_1-e_1s)\|_\infty\times\|s\|_\infty=$$
$$t\times2^{\omega(\log n)}\times\sigma^2<q/2.$$

故密文模 $q$ 满足 $q>t\times2^{\omega(\log n)}\times\sigma^2$ 可保证解密正确性.

## 4 改进方案

为了利用噪声淹没技术实现循环安全性,离散

高斯分布 $D_{\mathbf{Z}^n,\sigma'}$ 的标准方差 $\sigma'$ 需要满足 $\sigma'=2^{\omega(\log n)}\sigma^2$，而解密正确性要求模数 $q>t\times 2^{\omega(\log n)}\times\sigma^2$，因此，模数 $q$ 是 $n$ 的超多项式函数，使得 KDM.PKHE 方案的效率极低.下面，我们以 $d=2$ 这种情况为例，通过引入拒绝采样技术来约减 $\sigma'$ 的规模，进而降低 $q$ 的规模，并最终提高循环安全的 KDM.PKHE 方案效率.

### 4.1 方案描述

除了加密算法中噪声采样算法不同之外，改进方案同 KDM.PKHE 方案基本相同，记为 RS.KDM.PKHE.

1) RS.KDM.PKHE.$Pamameter Set$.令 $\lambda$ 为安全参数.选择素数 $q$，$t\in\mathbb{Z}_q^*$，$f(x)=x^n+1\in\mathbb{Z}[x]$，以及多项式环 $R_q=\mathbb{Z}_q/\langle f(x)\rangle$ 上的离散高斯分布 $D_{\mathbf{Z}^n,\sigma}$ 和 $D_{\mathbf{Z}^n,\sigma'}$.$R_t$ 为方案的明文空间，$\Delta=2n^{1.5}\sigma^2$.

2) RS.KDM.$PKHE.Keygen(1^\lambda)$.随机选择 $a_0\in R_q$，从离散高斯分布采样得到 $s,e_0\leftarrow D_{\mathbf{Z}^n,\sigma}$，计算 $b_0=a_0s+te_0$，输出私钥 $sk=s$ 和钥 $pk=(a_0,b_0)$.

3) RS.KDM.PKHE.$Enc(pk,m)$.对于消息 $m\in R_t$，按照如下方式生成密文 $\boldsymbol{c}=(c_0,c_1,c_2)\in R_q^3$：

① 计算 $a_i=a_0v_i+te_i$，其中 $v_i,e_i\leftarrow D_{\mathbf{Z}^n,\sigma}$.

② 重复采样 $e_i'\leftarrow D_{\mathbf{Z}^n,\sigma'}$，$i=1,2$，并以概率 $\dfrac{D_{\mathbf{Z}^n,\sigma'}}{M\times D_{\mathbf{Z}^n,\sigma',\Delta}}$ 计算 $b_i=b_0v_i+te_i'$.值得注意的是此处使用了拒绝采样技术，以一定概率对采样进行拒绝，其目的是通过拒绝采样降低参数 $\sigma'$ 的规模.

③ 计算对 $m$ 加密后的密文：

$$c_0=b_1+m;$$

$$c_1=b_2-a_1;$$

$$c_2=-a_2.$$

4) RS.KDM.PKHE.$Dec(sk,c)$.令 $\boldsymbol{s}=(1,s^1,s^2)$，计算 $\langle\boldsymbol{c},\boldsymbol{s}\rangle=\sum_{i=0}^{2}c_is^i$，当 $\|\langle\boldsymbol{c},\boldsymbol{s}\rangle\|_\infty<q/2$ 时解密正确，输出 $m=\langle\boldsymbol{c},\boldsymbol{s}\rangle \bmod t$.

### 4.2 方案正确性分析

在 RS.KDM.PKHE 方案的加密算法中，如果利用拒绝采样技术得到 $e_i'+e_0v_i-e_is$ 与 $e_i'$ 的分布不可区分，即 $e_i'$ 对 $D_{\mathbf{Z}^n,\sigma}$ 上采样进行“淹没”，则可以实现循环安全性证明中密钥的密文是均匀随机分布，安全性证明过程与定理 1 证明类似.

下面我们分析如何选择 $\sigma'$ 以及拒绝采样的重复次数 $M$ 使得加密算法中采样 $e_i'+e_0v_i-e_is$ 的分布服从分布 $D_{\mathbf{Z}^n,\sigma'}$.令 $e_0v_i-e_is=E_i$，根据引理 1 和引理 2 有：

$$\|E_i\|\leqslant\Delta=2n^{1.5}\sigma^2.$$

如图 1 所示($n=1$ 的情形)，我们令拒绝采样的目标概率分布是 $D_{\mathbf{Z}^n,\sigma'}$，源概率分布是 $D_{\mathbf{Z}^n,\sigma',E_i}$.为了利用拒绝采样技术，我们需要找到实数 $M$，使得对于所有的 $\boldsymbol{x}\in\mathbb{Z}^n$，有 $D_{\mathbf{Z}^n,\sigma'}(\boldsymbol{x})\leqslant M\times D_{\mathbf{Z}^n,\sigma',E_i}(\boldsymbol{x})$.根据高斯分布的定义有：

$$\frac{D_{\mathbf{Z}^n,\sigma'}(\boldsymbol{x})}{D_{\mathbf{Z}^n,\sigma',E_i}(\boldsymbol{x})}=\frac{\exp\left(\dfrac{-\|\boldsymbol{x}\|^2}{2\sigma'^2}\right)}{\exp\left(\dfrac{-\|(\boldsymbol{x}-E_i)\|^2}{2\sigma'^2}\right)}=\exp\left(\frac{-2\langle\boldsymbol{x},E_i\rangle+\|E_i\|^2}{2\sigma'^2}\right).$$

其中，根据引理 5，$\langle\boldsymbol{x},E_i\rangle$ 至少以概率 $1-\exp(-\Omega(\tau^2))$ 满足 $|\langle\boldsymbol{x},E_i\rangle|<\tau\sigma'E_i$.令 $\sigma'=\tau\Delta$，则有：

$$\frac{D_{\mathbf{Z}^n,\sigma'}(\boldsymbol{x})}{D_{\mathbf{Z}^n,\sigma',E_i}(\boldsymbol{x})}\leqslant\exp\left(1+\frac{1}{2\tau^2}\right).$$

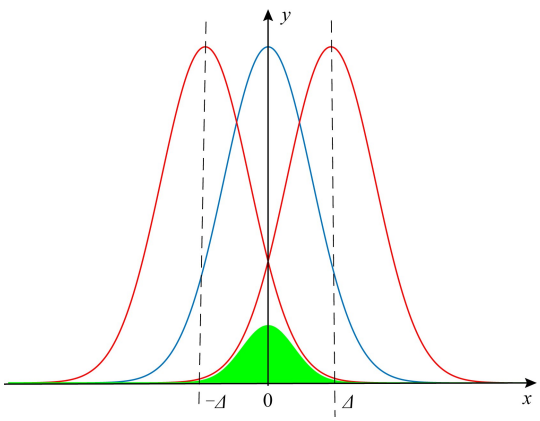


Fig. 1 Reject sampling technique

图 1 拒绝采样技术

因此，我们令 $M=\exp\left(1+\dfrac{1}{2\tau^2}\right)$，则根据拒绝采样的定义，源概率分布 $D_{\mathbf{Z}^n,\sigma',E_i}$ 以概率 $\dfrac{D_{\mathbf{Z}^n,\sigma'}(\boldsymbol{x})}{M\times D_{\mathbf{Z}^n,\sigma',E_i}(\boldsymbol{x})}$ 输出的采样服从目标分布 $D_{\mathbf{Z}^n,\sigma'}$.因此，离散高斯分布 $D_{\mathbf{Z}^n,\sigma'}$ 的标准方差满足 $\sigma'=\tau\Delta$，且期望的重复次数为

$$M=\exp\left(1+\frac{1}{2\tau^2}\right)\approx\exp(1).$$

### 4.3 方案性能分析

通过第 2 节分析可知，只要设置 $\sigma'=\tau\times\Delta=2\tau n^{1.5}\sigma^2$，即可以利用拒绝采样技术完成加密过程.如表 1 所示，RS.KDM.PKHE 方案中 $\sigma'$ 从 BV 的 KDM.SKHE 和 KDM.PKHE 方案中 $\sigma^2$ 的超多项式倍 $2^{\omega(\log n)}\times\sigma^2$ 降低为 $\sigma^2$ 的多项式倍 $poly(n)\times$

$\sigma^2$,大大约减了的 $\sigma'$ 的规模.根据解密正确性要求,密文模数 $q$ 的规模从 $2^{\omega(\log n)}\times\sigma^2\times t$ 降低到 $poly(n)\times\sigma^2\times t$,有效约减了密文规模,提升了同态运算的效率.

**Table 1 Parameter Setting**

**表 1 参数设置**

| Scheme | $\sigma$ | $\sigma'$ | $t$ | $q$ |
|---|---|---|---|---|
| KDM.SKHE[9] | $2^{\omega(\log n)}$ | $2^{\omega(\log n)}\times\sigma^2$ | $>\sigma\sqrt{n}$ | $2^{\omega(\log n)}\times\sigma^2\times t$ |
| KDM.PKHE | $2^{\omega(\sqrt{\log n})}$ | $2^{\omega(\log n)}\times\sigma^2$ | $>\sigma\sqrt{n}$ | $2^{\omega(\log n)}\times\sigma^2\times t$ |
| RS.KDM.PKHE | $2^{\omega(\sqrt{\log n})}$ | $poly(n)\times\sigma^2$ | $>\sigma\sqrt{n}$ | $poly(n)\times\sigma^2\times t$ |

### 4.4 循环安全的公钥同态加密方案

4.1 节中 RS.KDM.PKHE 方案关于度为 2 的多项式满足循环安全性,在这里我们将其扩展为关于度为 $d$ 的多项式满足循环安全性的方案.令 $\mathcal{P}_d=\mathcal{P}_d[R_t]$ 为 $R_t$ 上度为 $d$ 的多项式集合,即 $\mathcal{P}_d=\left\{p(z)=\sum_{i=1}^{d}\alpha_i z^i,\alpha_i\in R_t\right\}$.为了实现对私钥 $sk$ 的多项式 $p(sk)$ 的 KDM 安全性,将标准的 FHE 密文 $(c_0,c_1)$ 扩展为 $(c_0,c_1,\cdots,c_d)$,其中 $d$ 为多项式 $p(sk)$ 的度.

1) KDM.$Pamameter Set$.令 $\lambda$ 为安全参数.选择素数 $q,t\in\mathbb{Z}_q^*$,$f(x)=x^n+1\in\mathbb{Z}[x]$,以及多项式环 $R_q=\mathbb{Z}_q/\langle f(x)\rangle$ 上的离散高斯分布 $D_{\mathbf{Z}^n,\sigma}$ 和 $D_{\mathbf{Z}^n,\sigma'}$.令 $D$ 为 FHE 方案满足密文运算的深度.令参数 $d\leqslant D$ 为 FHE 方案满足 KDM 安全性的私钥函数的度.$R_t$ 为方案的明文空间.

2) KDM.$KeyGen(1^\lambda)$.随机选择 $a_0\in R_q$,从离散高斯分布采样得到 $s,e_0\leftarrow D_{\mathbf{Z}^n,\sigma}$,计算 $b_0=a_0s+te_0$,输出私钥 $sk=s$ 和公钥 $pk=(a_0,b_0)$.

3) KDM.$Enc(pk,m)$.对于消息 $m\in R_t$,按照如下方式生成密文 $\boldsymbol{c}=(c_0,c_1,\cdots,c_d)\in R_q^{d+1}$:

① 计算 $a_i=a_0v_i+te_i$,其中 $v_i,e_i\leftarrow D_{\mathbf{Z}^n,\sigma}$.

② 采样 $e_i'\leftarrow D_{\mathbf{Z}^n,\sigma'}$,重复采样 $e_i'\leftarrow D_{\mathbf{Z}^n,\sigma'}$,并以概率 $\frac{D_{\mathbf{Z}^n,\sigma'}}{D_{\mathbf{Z}^n,\sigma',\Delta}}$ 计算 $b_i=b_0v_i+te_i'$,得到 $d$ 个二元组:

$\{(a_i=a_0v_i+te_i,b_i=b_0v_i+te_i')\}_{i=1,2,\cdots,d}$.

③ 计算对 $m$ 加密后的密文:

$$c_0=b_1+m,$$

$$c_i=b_{i+1}-a_i,i=1,2,\cdots,d-1,$$

$$c_d=-a_d.$$

4) KDM.$Dec(sk,c)$.令 $\boldsymbol{s}=(1,s^1,\cdots,s^d)$,计算 $\langle\boldsymbol{c},\boldsymbol{s}\rangle=\sum_{i=0}^{d}c_is^i$,当 $\|\langle\boldsymbol{c},\boldsymbol{s}\rangle\|_\infty<q/2$ 时解密正确,输出:

$$m=\langle\boldsymbol{c},\boldsymbol{s}\rangle \bmod t.$$

## 5 结束语

本文基于噪声淹没技术给出了循环安全的公钥同态加密方案,并给出了安全性证明和参数设置.进一步,首次将拒绝采样技术引入到循环安全的同态加密方案构造方法中,给出了优化的循环安全公钥加密方案,使得系统参数从超多项式级降低到多项式级,有效约减了公钥规模和密文规模.

另一方面,由于拒绝采样技术的应用,导致加密算法的计算复杂性增加,但是考虑到同态加密方案的瓶颈在于密文运算,而不是新鲜密文的生成算法,而我们的方案将密文规模从超多项式级降低到多项式级,因此,可以有效降低密文运算的计算复杂性.总体而言,基于拒绝采样技术构造的循环安全性同态加密方案具有良好的性能.

## 参 考 文 献


[1] Gentry C. Fully homomorphic encryption using ideal lattices [C] //Proc of the 41st Annual ACM Symp on Theory of Computing (STOC). New York: ACM, 2009: 169-178

[2] Gentry C. A fully homomophic encryption scheme [D]. Stanford, CA: Stanford University, 2009

[3] Boneh D, Halevi S, Hamburg M, et al. Circular-secure encryption from secision Diffie-Hellman [G] //LNCS 5157: Advances in Cryptology (CRYPTO 2008). Berlin: Springer, 2008: 108-125

[4] Regev O. On lattices, learning with errors, random linear codes, and cryptography [J]. Journal of the Association for Computing Machinery, 2009, 56(6): 1-40

[5] Applebaum B, Cash D, Peikert C, et al. Fast cryptographic primitives and circular-secure encryption based on hard learning problems [G] //LNCS 5677: Advances in Cryptology (CRYPTO 2009). Berlin: Springer, 2009: 595-618

[6] Yang Xiaoyuan, Zhou Tanping, Zhang Wei, et al. Application of a circular secure variant of LWE in the homomorphic encryption [J]. Journal of Computer Research and Development, 2015, 52(6): 1389-1393 (in Chinese)

(杨晓元, 周谭平, 张薇, 等. 具有循环安全性的同态加密方案设计[J]. 计算机研究与发展, 2015, 52(6): 1389-1393)

[7] Zhao Xiufeng, Mao Hefeng, Liu Shuai, et al. Analysis on matrix GSW-FHE and optimizing bootstrapping [J]. Security and Communication Networks, 2018, 12, DOI: 10.1155/2018/6362010

[8] Hiromasa R, Abe M, Okamoto T. Packing messages and optimizing bootstrapping in GSW-FHE [G] //LNCS 9092: Proc of Int Workshop on Public Key Cryptography (PKC 2015). Berlin: Springer, 2015: 699-715

[9] Brakerski Z, Vaikuntanathan V. Fully homomorphic encryption from ring-LWE and security for key dependent messages [G] //LNCS 6841: Advances in Cryptology (CRYPTO 2011). Berlin: Springer, 2011: 505-524

[10] Micciancio D, Regev O. Worst-case to average-case reductions based on Gaussian measures [J]. SIAM Journal on Computing, 2007: 37(1): 267-302

[11] Goldwasser S, Kalai Y T, Peikert C. Robustness of the learning with errors assumption [C] //Proc of Symp on Innovations in Computer Science 2010. Beijing: Tsinghua University Press, 2010: 230-240

[12] Lyubashevsky V, Micciancio D. Generalized compact knapsacks are collision resistant [C] //Proc of Int Colloquium on Automata, Languages & Programming. Berlin: Springer, 2006: 144-155

[13] Stephens-Davidowitz N. Discrete Gaussian sampling reduces to CVP and SVP [J]. Computer Science, 2016: 1748-1764

[14] Lyubashevsky V, Peikert C, Regev O. On ideal lattices and learning with errors over rings [G] //LNCS 6110: Advances in Cryptology (EUROCRYPTO 2010). Berlin: Springer, 2010: 1-23

[15] von Neumann J. Various techniques used in connection with random digits, national bureau of standards [J]. Applied Math, 1951, (12): 36-38

[16] Lyubashevsky V. Lattice-based identification schemes secure under active attacks [G] //LNCS 4939: Proc of Int Workshop on Public Key Cryptography (PKC 2008). Berlin: Springer, 2008: 162-179

[17] Ducas L, Durmus A, Lepoint T, et al. Lattice signatures and bimodal Gaussians [G] //LNCS 8042: Advances in Cryptology (CRYPTO 2013). Berlin: Springer, 2013: 40-57

**Zhao Xiufeng**, born in 1977. Associate professor. Received her PhD degree from Shandong University. Her main research interests include cryptography protocols, lattice-based cryptography and homomorphic encryption.

**Fu Yu**, born in 1997. Master candidate. His main research interest is lattice-based cryptography protocol.

**Song Weitao**, born in 1989. Master, lecturer. His main research interests include fully homomorphic encryption and private information retrieval.