计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2015.20131952
52(6):1389-1393,2015

具有循环安全性的同态加密方案的设计

杨晓元　周潭平　张　薇　吴立强
(武警工程大学网络与信息安全武警部队重点实验室　西安　710086)
(武警工程大学电子技术系　西安　710086)
(850301775@qq.com)

Application of a Circular Secure Variant of LWE in the Homomorphic Encryption

Yang Xiaoyuan, Zhou Tanping, Zhang Wei, and Wu Liqiang
(*Network and Information Security Key Laboratory, Engineering University of the Armed Police Force, Xi'an* 710086)
(*Electronics Department, Engineering University of the Armed Police Force, Xi'an* 710086)

Abstract Homomorphic encryption scheme is a powerful cryptographic system which allows for a variety of applications. Fully homomorphic encryption (FHE) permits arbitrary computations on encrypted data. The recent breakthrough work in 2009 by Craig Gentry has shown the possibility of FHE schemes, and has provided the first construction. Consequently, during the past five years, numerous FHE involving novel mathematical techniques and a number of application schemes have appeared. Indeed, the construction and application of homomorphic encryption schemes have great theoretic and practical meaning. Homomorphic encryption has important applications in cloud computing. However, almost all of the homomorphic encryption schemes share two common flaws that the multiplication depth must be set in advance and they all use secret keys of large scales. We construct a circularly secure re-linearization process based on the "special b" variant of the learning with errors problem (bLWE). Then, we present an efficient homomorphic encryption scheme. Compared with Brakerski et al's scheme, our scheme reduces the $L+1$ secret keys to one and doesn't need to know the multiplication depth in advance. Finally, we prove the chosen-plaintext attack (CPA) security of the homomorphic scheme and the circular security of the re-linearization process in standard model by reducing them into learning with errors problem(LWE) assumption.

Key words circular security; homomorphic encryption; learning with errors problem(LWE); lattice; standard model

摘　要 同态加密在云计算等领域具有重要的应用价值,针对现有同态加密方案中私钥个数多和需要预设乘法同态次数的缺陷,基于一个具有特殊 b 的误差学习问题(learning with errors problem, LWE)变种 bLWE(the "special b" variant of the learning with errors problem),得到具有循环安全性的重线性化过程,据此构造了一个较高效的同态加密方案.与 Brakerski 等人的方案相比,方案的构造者不需要事先知道服务器中乘法同态次数,且私钥个数由原来的 $L+1$ 个大幅度地缩小为 1 个.最后,在标准模型下对重线性化过程的循环安全性和方案的 CPA 安全性进行了严格证明.

关键词 循环安全;同态加密;LWE 问题;格;标准模型

中图法分类号 TP391

收稿日期:2013-12-24;**修回日期**:2014-06-25

基金项目:国家自然科学基金项目(61272492,61103230,61103231,61202492)

随着云计算及云存储技术的兴起,在许多实际应用,如代理计算、云存储、安全多方计算、电子投票等场合,都需要密码体制具有同态性质.具有同态性的密码体制,可以在不解密的情况下对密文数据进行运算,得到的结果解密后相当于对明文进行同样运算的结果.同态加密方案允许在服务器端直接对密文进行运算,从而极大地减少了数据存储服务的通信量及运算量[1].

1995 年,Benaloh[2] 提出了一种支持直接对密文做有限次加法操作的密码体制,这是首个以同态性为设计目标的公钥密码,密码学家利用它构造了许多应用方案,包括电子选举、在线扑克、非交互式可验证秘密共享等.这种加密方案只能进行一种同态运算(加法或乘法),称为半同态加密(semi-homomorphic encryption)[3].2005 年,由 Boneh, Goh, Nissim[4] 提出的 BGN 密码是第 1 个同时支持加法同态和乘法同态的语义安全加密体制,支持任意多次加法操作和一次乘法操作,这类方案虽然是双同态的,但只能计算密文的低次多项式,称为类同态加密方案.2009 年,Gentry 基于理想格上困难问题及稀疏子集和问题,设计出了第 1 个语义安全的全同态加密方案[3],即支持任意多次加法和任意多次乘法运算.2010 年欧洲密码学年会上,Dijk, Gentry, Halevi 等人[5] 构造了整数上的全同态加密方案,称为 DGHV 方案,该方案利用了 Gentry 的设计思想,但是用整数环上的类同态加密来替换 Gentry 方案中的理想格方案.2011 年,Brakerski 和 Vaikuntanathan[6] 采用了完全不同的构造,他们基于误差学习问题(learning with errors problem, LWE)假设构造了 BV11b 方案,从一个基本的类同态加密方案出发,利用重线性化(relinearization)和模数转换(modulus switching)2 种技术来得到 FHE(fully homomorphic encryption)方案.2011 年,Brakerski, Gentry 和 Vaikuntanathan[7] 利用类似方法构造了 BGV 方案,也采用了 BV11b 中的重线性化和模数转换方法,同时 BGV 方案中还设计了分级渐近的噪声管理方法,使乘法运算后的噪声增加较小,而计算量也较小.2012 年,Halevi[8] 利用 C++语言和 NTL 数学函数库编写了实现 BGV 方案的软件包.2013 年,Gentry, Sahai, Waters[9] 提出了近似特征值方法,据此构造了一个基于 LWE 问题的全同态方案,这个方案可以用来构造基于身份的全同态方案和基于属性的全同态方案.

但是由于现有重线性化过程没有达到循环安全性(circular security),所以上述大部分方案中每一次使用乘法同态都需要引入一个新的私钥.这导致了大部分的同态加密方案需要预设乘法同态次数和具有大量的私钥个数.本文针对现有基于 LWE 问题的同态加密方案特点,改进了重线性化过程,并且把新过程实例化到 Brakerski 和 Vaikuntanathan 的 BV11b 方案中,从而构造出了一个效率较高的同态加密方案.与 BV11b 方案相比,方案的构造者不再需要事先知道服务器中乘法同态次数,且私钥个数由原来的 $L+1$ 个大幅度地缩小为 1 个.最后,对方案进行了正确性分析,得到了方案中参数的取值范围,在标准模型下对重线性化过程的循环安全性和方案的 CPA(chosen-plaintext attack)安全性进行了证明.

1 预备知识

定义 1[6]. B 上限分布.一个在整数上分布的集合 $\{\chi_n\}_{n\in\mathbf{N}}$,叫作 B 上限分布,假如满足:$Pr_{e\xleftarrow{s}\chi_n}[|e|>B]\leqslant 2^{-\tilde{\Omega}(n)}$.

引理 1[10]. 矩阵向量的剩余 Hash 定理.令 $k\in\mathbb{N}$, $n\in\mathbb{N}$, $q\in\mathbb{N}$, $m\geqslant n\,\mathrm{lb}\,q+2k$, $\boldsymbol{A}\xleftarrow{S}\mathbb{Z}_q^{m\times n}$ 是随机均匀选取的矩阵,令 $\boldsymbol{r}\xleftarrow{S}\{0,1\}^m$, $\boldsymbol{y}\xleftarrow{S}\mathbb{Z}_q^n$,则 $\Delta((\boldsymbol{A},\boldsymbol{A}^{\mathrm{T}}r),(\boldsymbol{A},\boldsymbol{y}))\leqslant 2^{-k}$,其中 $\Delta(\boldsymbol{A},\boldsymbol{B})$ 表示 $\boldsymbol{A}$ 和 $\boldsymbol{B}$ 的分布距离.

定义 2[10]. 层级全同态加密.一类同态加密方案 $\{\varepsilon^{(L)}:L\in\mathbb{Z}^+\}$ 是层级全同态的,假如对于所有的 $L\in\mathbb{Z}^+$,他们都用一样的解密电路,$\varepsilon^{(L)}$ 紧凑计算的电路的最大深为 L(使用一些特殊门运算).$\varepsilon^{(L)}$ 紧凑计算的复杂性是安全参数、L 和电路大小的多项式(对于所有的 L).

定义 3[11]. LWE 问题.对于安全参数 λ,另 $n=n(\lambda)$ 是一个整数维.令 $q=q(\lambda)\geqslant 2$ 是一个整数.令 $\chi=\chi(\lambda)$ 是$\mathbb{Z}$上的分布.$LWE_{n,q,\chi}$ 问题就是区分下面的 2 个分布:1) $(\boldsymbol{a}_i,b_i)\in\mathbb{Z}_q^{n+1}$ 均匀地取自 $\mathbb{Z}_q^{n+1}$;2)选择 $e_i\leftarrow\chi$,均匀选择 $\boldsymbol{s}\leftarrow\mathbb{Z}_q^n$, $\boldsymbol{a}_i\leftarrow\mathbb{Z}_q^n$,计算 $b_i=\langle\boldsymbol{a}_i,\boldsymbol{s}\rangle+e_i$,得到 $(\boldsymbol{a}_i,b_i)\in\mathbb{Z}_q^{n+1}$,令这个分布为 $A_{q,s,\chi}$. $LWE_{n,q,\chi}$ 假设就是 $LWE_{n,q,\chi}$ 问题是困难的.

定义 $\boldsymbol{a}\leftarrow\Gamma_{d,q}^n$ 分布为:$(\boldsymbol{a}[1],\cdots,\boldsymbol{a}[n-1])\xleftarrow{U}\mathbb{Z}_q^{n-1}$, $\boldsymbol{a}[n]=d-\sum_{i=1}^{n-1}\boldsymbol{a}[i]\pmod q$.定义 $\|\boldsymbol{a}\|_1=\sum_{i=1}^{n}\boldsymbol{a}[i]\bmod q$,令 $\boldsymbol{a}^{-1}=\|\boldsymbol{a}\|_1\bmod q$.定义 $Powersof2(\boldsymbol{x}\in\mathbb{Z}_q^n,q)=(\boldsymbol{x},2\boldsymbol{x},\cdots,2^{\lfloor\mathrm{lb}q\rfloor}\boldsymbol{x})\in\mathbb{Z}_q^{n\lceil\mathrm{lb}q\rceil}$.

定义 4. 具有特殊 b 的 LWE 变种 bLWE(the "special b" variant of the learning with errors problem). 对于安全参数 λ,另 $n=n(\lambda)$ 是一个整数维. 令 $q=q(\lambda)\geqslant 2$ 是一个整数,$d\geqslant 1$ 是一个整数. 令 $\chi=\chi(\lambda)$ 是$\mathbb{Z}$上的分布. $bLWE_{n,q,d,\chi}$问题就是区分下面的 2 个分布:1)$(\boldsymbol{a},b)\in\mathbb{Z}_q^{n-1}\times\mathbb{Z}_q$ 均匀地取自$\mathbb{Z}_q^n$. 2)对于 $\boldsymbol{s}\xleftarrow{U}\mathbb{Z}_q^n$,$\boldsymbol{a}\leftarrow\Gamma_{d,q}^n$,$e\leftarrow\chi$,输出$(\boldsymbol{a}[1],\cdots,\boldsymbol{a}[n-1],b=\sum_{i=1}^{n}\boldsymbol{a}[i]\boldsymbol{s}[i]+2e)\in\mathbb{Z}_q^{n-1}\times\mathbb{Z}_q$,令这个分布为 $bA_{q,s,\chi}$. $bLWE_{n,q,d,\chi}$假设就是 $bLWE_{n,q,d,\chi}$问题是困难的(当 $d=1$ 时,$bLWE_{n,q,d,\chi}$ 问题记为 $bLWE_{n,q,\chi}$.)

2 方案描述

1) 参数设置

本方案的明文空间为 $GF(2)$. 方案中涉及的运算都是在模 q 的环中进行的. 令 $k\in\mathbb{N}$ 作为安全参数,$n\in\mathbb{N}$ 作为维度,一个正整数 $m\in\mathbb{N}$,一个奇数 q 作为模数,一个噪音分布 $\chi\in\mathbb{Z}_q$,限制上述参数取值使得 LWE 问题可以达到 2^λ 安全. 另外增加一个同态乘法深度的上限 $L\in\mathbb{N}$. 定义$(\boldsymbol{x}|\boldsymbol{y})$表示向量 $\boldsymbol{x}$ 和向量 $\boldsymbol{y}$ 的级联. 定义函数 $g_{i,j,\tau}(\boldsymbol{s})=2^\tau\boldsymbol{s}[i]\boldsymbol{s}[j]$. 令 $\boldsymbol{a}^{-1}=d=1 \bmod q$.

参数间的关系:维度 n 是安全参数 k 的多项式,$m\geqslant n\lg q+2k$ 是 n 的多项式. 模数 $q\in[2^{n^\varepsilon},2\times 2^{n^\varepsilon})$ 是 n 的亚指数(其中 $\varepsilon\in(0,1)$ 是个实数). 噪音分布 $\chi\in\mathbb{Z}_q$(产生实例绝对值的上限大概率小于 n). 深度的上限 $L\approx\lg n$.

2) $SH.Kengen(1^k)$

选取私钥 $\boldsymbol{s}=(\boldsymbol{s}[1],\boldsymbol{s}[2],\cdots,\boldsymbol{s}[n])\xleftarrow{U}\mathbb{Z}_q^n$,对于 $1\leqslant l\leqslant L$,$0\leqslant i\leqslant j\leqslant n$,$0\leqslant\tau\leqslant\lfloor\lg q\rfloor$,抽样 $\boldsymbol{a}_{l,i,j,\tau}\leftarrow\Gamma_{1,q}^n$,$e_{l,i,j,\tau}\xleftarrow{S}\chi$(为了简化乘法运算中的表达,增添一个新的变量 $\boldsymbol{s}[0]\triangleq 1$).

$\psi_{l,i,j,\tau}\triangleq(\boldsymbol{a}_{l,i,j,\tau}[0],\cdots,\boldsymbol{a}_{l,i,j,\tau}[n-1],b_{l,i,j,\tau}=\langle\boldsymbol{a}_{l,i,j,\tau},\boldsymbol{s}\rangle+2e_{l,i,j,\tau}+\|\boldsymbol{a}_{l,i,j,\tau}\|_1\times g_{i,j,\tau}(\boldsymbol{s}))\in\mathbb{Z}_q^{n-1}\times\mathbb{Z}_q$. 定义 $\Psi\triangleq\{\psi_{l,i,j,\tau}\}_{l,i,j,\tau}$ 表示上式的集合. $\boldsymbol{A}\xleftarrow{S}\mathbb{Z}_q^{m\times n}$和$\boldsymbol{e}\xleftarrow{S}\chi^m$,计算 $\boldsymbol{b}=\boldsymbol{A}\boldsymbol{s}+2\boldsymbol{e}\in\mathbb{Z}_q^m$.

输出私钥 $sk=\boldsymbol{s}$,运算密钥 $evk=\Psi$,公钥 $pk=(\boldsymbol{A},\boldsymbol{b})$. 公布运算密钥 $evk=\Psi$,公钥 $pk=(\boldsymbol{A},\boldsymbol{b})$.

3) $SH.Enc_{pk}(\mu)$

加密 1b 的明文 $\mu\in GF(2)$,随机选择一个向量 $\boldsymbol{r}\xleftarrow{S}\{0,1\}^m$. 定义:

$\boldsymbol{v}:=\boldsymbol{A}^{\mathrm{T}}\boldsymbol{r}$ 和 $w:=\boldsymbol{b}^{\mathrm{T}}\boldsymbol{r}+\mu$.

输出密文对$(\boldsymbol{v},w)$,再加上一个表示乘法深度的标志 l,新鲜密文的深度定义为 0,最后输出最终密文$((\boldsymbol{v},w),0)$.

4) $SH.Eval_{evk}(f,c_1,\cdots,c_t)$

$f:\{0,1\}^t\to\{0,1\}$,要求函数 f 可以被任意多输入的加法和 2 个输入的乘法表示,并且可以通过逐次运行加法或乘法得到. 最后,要求乘法运算的次数不超过 L(BV11b 方案中需要乘法运算的次数等于 L). 一个合法的密文由三元组组成,$c=((\boldsymbol{v},w),l)$,其中 l 表示密文的乘法深度. f 要求每层输入具有相同的乘法深度 l. 输入的密文$(\boldsymbol{v},w)$需要满足等式 $w-\langle\boldsymbol{v},\boldsymbol{s}\rangle=\mu+2e(\bmod q)$,其中 $2e$ 代表密文所带的噪音.

因为通过逐次地运行加法或乘法得到 f,所以本节详细分析方案中的同态门运算.

① 加法同态

输入:t 个密文 $c_1,\cdots,c_t$,其中 $c_i=((\boldsymbol{v}_i,w_i),l)$;

输出:$c_{\mathrm{add}}=((\boldsymbol{v}_{\mathrm{add}},w_{\mathrm{add}}),l):=((\sum_{i=1}^{t}\boldsymbol{v}_i,\sum_{i=1}^{t}w_i),l)$.

正确性分析:$w_{\mathrm{add}}-\langle\boldsymbol{v}_{\mathrm{add}},\boldsymbol{s}\rangle=\sum_{i=1}^{t}(w_i-\langle\boldsymbol{v}_i,\boldsymbol{s}\rangle)=\sum_{i=1}^{t}\mu_i+2\sum_{i=1}^{t}e_i(\bmod q)$.

可以看出产生的噪音就是所有输入噪音的和.

② 乘法同态

输入:$c=((\boldsymbol{v},w),l)$和 $c'=((\boldsymbol{v}',w'),l)$;

输出:$c_{\mathrm{mult}}=((\boldsymbol{v}_{\mathrm{mult}},w_{\mathrm{mult}}),l+1)$.

令 $\phi(\boldsymbol{x})\triangleq(w-\langle\boldsymbol{v},\boldsymbol{x}\rangle)(w'-\langle\boldsymbol{v}',\boldsymbol{x}\rangle)$,象征性地展开 $\phi(\boldsymbol{x})$,$\phi(\boldsymbol{x})=\sum_{\substack{0\leqslant i\leqslant j\leqslant n\\ \tau\in\{0,\cdots,\lfloor\lg q\rfloor\}}}h_{i,j,\tau}(2^\tau\boldsymbol{x}[i]\boldsymbol{x}[j])$.

设变量 $w_{\mathrm{mult}}=\sum_{\substack{0\leqslant i\leqslant j\leqslant n\\ \tau\in\{0,\cdots,\lfloor\lg q\rfloor\}}}h_{i,j,\tau}b_{l,i,j,\tau}$ 和 $\boldsymbol{v}_{\mathrm{mult}}=\sum_{\substack{0\leqslant i\leqslant j\leqslant n\\ \tau\in\{0,\cdots,\lfloor\lg q\rfloor\}}}h_{i,j,\tau}\boldsymbol{a}_{l,i,j,\tau}$,则有 $w_{\mathrm{mult}}-\langle\boldsymbol{v}_{\mathrm{mult}},\boldsymbol{s}\rangle=(\mu+2e)(\mu'+2e')+2\sum_{\substack{0\leqslant i\leqslant j\leqslant n\\ \tau\in\{0,\cdots,\lfloor\lg q\rfloor\}}}h_{i,j,\tau}e_{l,i,j,\tau}=\mu\mu'+2(\mu e'+e\mu'+2ee'+\sum_{\substack{0\leqslant i\leqslant j\leqslant n\\ \tau\in\{0,\cdots,\lfloor\lg q\rfloor\}}}h_{i,j,\tau}e_{l,i,j,\tau})$.

5) $SH.Dec(c)$

输入:c;

输出:$\mu^*=(w-\langle\boldsymbol{v},\boldsymbol{s}\rangle)(\bmod q)(\bmod 2)$.

3 方案分析

3.1 正确性分析

本文运用了循环安全的重线性化过程改进了BV11b方案中的实例 $\psi_{l,i,j,\tau}$,实质上是相当于限制了 $\boldsymbol{a}$ 的取值范围,这不会影响方案的正确性,所以借鉴BV11b方案关于正确性和效率的分析,可以得到以下的定理.

定理 1. 令 $n\geqslant 5$,$q\geqslant 2^{n^{\varepsilon}}\geqslant 3$,$\varepsilon\in\{0,1\}$. χ 是任意的 n 上限分布,$m=(n+1)\ \mathrm{lb}\ q+2k$,$\boldsymbol{a}^{-1}=1$,则SH方案是 $Arith[L=\Omega(\varepsilon\ \mathrm{lb}\ n),T=\sqrt{q}]$同态.

3.2 安全性分析

本节将在标准模型下对重线性化过程的循环安全性和方案的CPA安全性进行了严格证明.

引理 2. 对于 $n\geqslant 2$,$q\geqslant 1$,$d\geqslant 1$ 和分布 χ 有一个高效的归约从 $LWE_{n-1,q,\chi}$ 到 $bLWE_{n,q,\chi}$,归约的优势是 2^{-n}.

证明. 从给定的LWE预言机中取实例 $(\boldsymbol{a}',b')\in\mathbb{Z}_q^{n-1}\times\mathbb{Z}_q$,产生新的实例 $(\boldsymbol{a}',b)=(\boldsymbol{a}',b'+(d-\|\boldsymbol{a}'\|_1)\boldsymbol{s}[n])\in\mathbb{Z}_q^{n-1}\times\mathbb{Z}_q$,令 $\boldsymbol{a}=(\boldsymbol{a}'\mid(d-\|\boldsymbol{a}'\|_1)\in\mathbb{Z}_q^n$.

1) 假如 $(\boldsymbol{a}',b')\in\mathbb{Z}_q^{n-1}\times\mathbb{Z}_q$ 选自均匀分布,则表达式 $b=b'+(d-\|\boldsymbol{a}'\|_1)\boldsymbol{s}[n]$ 中 d 为常数、b' 和 $\boldsymbol{s}[n]$ 都是选自均匀分布,所以 b 与均匀分布的统计距离不超过 2^{-n}.

2) 假如 $(\boldsymbol{a}',b')\in\mathbb{Z}_q^{n-1}\times\mathbb{Z}_q$ 选自 $A_{q,s,\chi}$,则表达式 $b=b'+(d-\|\boldsymbol{a}'\|_1)\boldsymbol{s}[n]=\langle\boldsymbol{a},\boldsymbol{s}\rangle+2e$ 与 $bA_{q,s,\chi}$ 分布的统计距离不超过 2^{-n}. 归约得到证明. 证毕.

综上所述,假如 $LWE_{n-1,q,\chi}$ 问题是困难的,那么 $bLWE_{n,q,\chi}$ 问题是困难的,即 $bA_{q,s,\chi}$ 分布与均匀分布不可区分.

定理 2. 重线性化过程的循环安全性. 若 q,n,N,χ 等参数都是符合SH方案中重线性化过程中要求的参数,则FHE方案的私钥置换过程的循环安全性可以归约到 $bLWE_{n,q,\chi}$ 问题的困难性.

证明. 证明SH方案的重线性化过程具有循环安全性,就是要证明 $(\boldsymbol{a}[1],\cdots,\boldsymbol{a}[n-1],b=\langle\boldsymbol{a},\boldsymbol{s}\rangle+2e+Powersof2(\boldsymbol{s})[i])\in\mathbb{Z}_q^{n-1}\times\mathbb{Z}_q$ 不泄露私钥 $\boldsymbol{s}$ 的信息,即与均匀分布不可区分.

令 $g_i(\boldsymbol{s})=Powersof2(\boldsymbol{s})[i]$,$\boldsymbol{t}=\boldsymbol{s}+(g_i(\boldsymbol{s}),g_i(\boldsymbol{s}),\cdots,g_i(\boldsymbol{s}))\in\mathbb{Z}_q^n$.

因为在私钥置换过程中有 $\boldsymbol{a}^{-1}=1$,所以

$$b=\langle\boldsymbol{a},\boldsymbol{s}\rangle+2e+g_i(\boldsymbol{s})=$$
$$\langle\boldsymbol{a},\boldsymbol{s}\rangle+2e+\|\boldsymbol{a}\|_1\times g_i(\boldsymbol{s})=$$
$$\langle\boldsymbol{a},\boldsymbol{s}\rangle+2e+\langle\boldsymbol{a},(g_i(\boldsymbol{s}),g_i(\boldsymbol{s}),\cdots,g_i(\boldsymbol{s}))\rangle=$$
$$\langle\boldsymbol{a},\boldsymbol{s}+(g_i(\boldsymbol{s}),g_i(\boldsymbol{s}),\cdots,g_i(\boldsymbol{s}))\rangle+2e=$$
$$\langle\boldsymbol{a},\boldsymbol{t}\rangle+2e.$$

注意 $\boldsymbol{t}$ 只是关于 $\boldsymbol{s}$ 的函数,与 $\boldsymbol{a}$ 和 e 都相互独立. 又因为有 $\boldsymbol{s}\xleftarrow{U}\in\mathbb{Z}_q^n$,所以 $\boldsymbol{t}$ 的分布也是在 $\mathbb{Z}_q$ 中随机的,即 $\boldsymbol{t}$ 与均匀分布的统计距离最大为 2^{-n}. 则 $(\boldsymbol{a}[1],\cdots,\boldsymbol{a}[n-1],\langle\boldsymbol{a},\boldsymbol{t}\rangle+2e)\in\mathbb{Z}_q^{n-1}\times\mathbb{Z}_q$ 相当于 $bA_{q,t,\chi}$ 中的一个实例.

由引理2可以得到 $(\boldsymbol{a}[1],\cdots,\boldsymbol{a}[n-1],\langle\boldsymbol{a},\boldsymbol{t}\rangle+2e)\in\mathbb{Z}_q^{n-1}\times\mathbb{Z}_q$ 与均匀分布不可区分,所以上述重线性化过程是具有循环安全性的. 证毕.

定理 3. CPA安全. 令 q,n,N 等参数都是符合本文SH中要求的参数. 若BV11b方案中SH方案是CPA安全的,则本方案是CPA安全的.

本文用 A,B,C,D 分别代表Alice,Bob,Carol,David这4个人名. 采用 $Adv_{\mathrm{NSH}}^{\mathrm{CPA}}(\mathrm{C})$ 表示攻击者C攻破本方案的CPA概率,$Adv_{\mathrm{BV11b}}(\mathrm{D})$ 表示攻击者D攻破BV11b中SH方案的概率,$Adv_{LWE_n}(\mathrm{A})$ 表示攻击者A攻破 n 维LWE问题的概率,$Adv_{bLWE_n}(\mathrm{B})$ 表示攻击者B攻破 n 维bLWE问题的概率.

本文与BV11b中SH方案的不同之处在于运用了循环安全的重线性化过程,本文把BV11b中SH方案中的实例 $(\boldsymbol{a},b)\in\mathbb{Z}_q^n\times\mathbb{Z}_q$ 替换为 $(\boldsymbol{a}',b)\in\mathbb{Z}_q^{n-1}\times\mathbb{Z}_q$,所以有:

$$Adv_{\mathrm{NSH}}^{\mathrm{CPA}}(\mathrm{C})\leqslant Adv_{\mathrm{BV11b}}(\mathrm{D})+|Adv_{LWE_n}(\mathrm{A})-Adv_{bLWE_n}(\mathrm{B})|=Adv_{\mathrm{BV11b}}(\mathrm{D})+|Adv_{LWE_n}(\mathrm{A})-Adv_{LWE_{n-1}}(\mathrm{A})+Adv_{LWE_{n-1}}(\mathrm{A})-Adv_{bLWE_n}(\mathrm{B})|\leqslant Adv_{\mathrm{BV11b}}(\mathrm{D})+|Adv_{LWE_n}(\mathrm{A})-Adv_{LWE_{n-1}}(\mathrm{A})|+|Adv_{LWE_{n-1}}(\mathrm{A})-Adv_{bLWE_n}(\mathrm{B})|.$$

因为 $Adv_{\mathrm{BV11b}}(\mathrm{D})$,$|Adv_{LWE_n}(\mathrm{A})-Adv_{LWE_{n-1}}(\mathrm{A})|$,$|Adv_{LWE_{n-1}}(\mathrm{A})-Adv_{bLWE_n}(\mathrm{B})|$ 都是多项式内可以忽略的,所以方案是CPA安全的.

3.3 效率分析

注意到第2节方案中的私钥 $\boldsymbol{s}$ 不随乘法层数的变化而变化,所以可以不用预先设置乘法同态的次数.

本方案用具有循环安全性的重线性化过程改进BV11b方案. 表1给出了本方案和BV11b方案在公钥大小、私钥个数、乘法同态最大层数、重线性化过程中的安全性和方案的安全性的量化分析比较.

从表1可以看出,在安全参数相同的情况下,本方案在公钥大小和乘法同态最大层数 L 以及CPA安全性方面都与原方案相同,而得到的私钥个数较

Table 1 Efficiency Comparison Between BV11b[6] and Our Scheme

表 1 BV11b[6]和本方案的效率比较

Schemes	Public Key Size/b	Secret Key Number	Maximal Multiplicative Depth L	Circular Security	CPA Security
BV11b	$[m\times(n+1)]\,\mathrm{lb}\,q$	$L+1$	$\Omega(\varepsilon\,\mathrm{lb}\,n)$	No	Yes
Our Scheme	$[m\times(n+1)]\,\mathrm{lb}\,q$	1	$\Omega(\varepsilon\,\mathrm{lb}\,n)$	Yes	Yes

BV11b[6]方案由 $L+1$ 个大幅度地缩小为 1 个,所以本方案在效率方面较 BV11b 方案有明显提高.

4 结束语

本方案用具有循环安全性的重线性化过程改进了 BV11b 方案.在安全参数相同的情况下,具有如下优势:1)方案的构造者不再需要事先知道服务器中乘法同态次数; 2)本方案较 BV11b 方案的私钥个数由原来的 $L+1$ 个变为了 1 个.但是本方案还需要深入地探索和完善,主要包括以下 3 个方面:1)可将 bLWE 扩展成为基于 RLWE 问题的 RbLWE,应用于 GSW,BGV 等方案,这样有助于进一步提高效率; 2)构造循环安全非层级的全同态方案; 3)进一步提高方案的效率.

参 考 文 献

[1] Zhang Wei, Liu Shuguang, Zhong Weidong, et al. How to build a faster private information retrieval protocol? [J]. Journal of Ambient Intelligence and Humanized Computing, 2014, 5(21): 1-7

[2] Benaloh J. Dense probabilistic encryption [C/OL] //Proc of the Workshop on Selected Areas of Cryptography. 1994: 120-128. [2012-12-24]. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.33.3710

[3] 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

[4] Boneh D, Goh E J, Nissim K. Evaluating 2-DNF formulas on ciphertexts [G] //LNCS 3378: Theory of Cryptography. Berlin: Springer, 2005: 325-341

[5] Dijk M, Gentry C, Halevi S, et al. Fully homomorphic encryption over the integers [G] //LNCS 6110: Advances in Cryptology-EUROCRYPT 2010. Berlin: Springer, 2010: 24-43

[6] Brakerski Z, Vaikuntanathan V. Efficient fully homomorphic encryption from (standard) LWE [C] //Proc of the 52nd Annual Symp on Foundations of Computer Science. Los Alamitos, CA: IEEE Computer Society, 2011: 97-106

[7] Brakerski Z, Gentry C, Vaikuntanathan V. (Leveled) fully homomorphic encryption without bootstrapping [C] //Proc of the 3rd Innovations in Theoretical Computer Science Conf. New York: ACM, 2012: 309-325

[8] Halevi S. Design and implementation of a homomorphic encryption library [EB/OL]. [2012-04-09]. http://eprint.iacr.org/2012/181

[9] Gentry C, Sahai A, Waters B. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based [G] //LNCS 8042: Advances in Cryptology-CRYPTO 2013. Berlin: Springer, 2013: 75-92

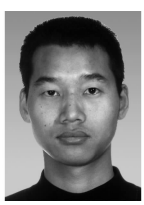
[10] Impagliazzo R, Levin L A, Luby M. Pseudo-random generation from one-way functions [C] //Proc of the 21st Annual ACM Symp on Theory of Computing. New York: ACM, 1989: 12-24

[11] Regev O. On lattices, learning with errors, random linear codes, and cryptography [J]. Journal of the ACM(JACM), 2009, 56(6): 34-34

Yang Xiaoyuan, born in 1959. PhD supervisor and master. His main research interests include information security and cryptology.

Zhou Tanping, born in 1989. PhD candidate. His main research interests include fully homomorphic encryption, encryption scheme based on lattice.

Zhang Wei, born in 1976. PhD and assistant professor. Her main research interests include fully homomorphic encryption, encryption scheme based on lattice.



Wu Liqiang, born in 1986. Master. His main research interests include encryption scheme based on lattice, security proof.