基于整数近似 GCD 的全同态加密方案*

于志敏[1], 古春生[1,2], 景征骏[1,3]

(1. 江苏理工学院 计算机工程学院, 江苏 常州 213001; 2. 中国科学技术大学 计算机科学与技术学院, 合肥 230027; 3. 南京邮电大学 计算机学院, 南京 210003)

摘 要: 设计了基于整数近似 GCD 问题新的全同态加密方案。跟随 Gentry 设计模式,构造 somewhat 同态加密方案,并归约其安全性到整数近似 GCD;引入稀疏子集和难度假设来压缩解密电路,使其具有自举性;最后转换 somewhat 同态加密方案到全同态加密方案。与文献[1]方案相比,提出的 somewhat 同态加密方案更接近于文献[2]中公钥加密方案。

关键词: 近似整数最大公因数; 公钥方案; 全同态加密; 稀疏子集和问题

中图分类号: TP309.7 **文献标志码**: A **文章编号**: 1001-3695(2014)07-2105-04

doi:10.3969/j.issn.1001-3695.2014.07.044

Fully homomorphic encryption based on approximate integer GCD

YU Zhi-min[1], GU Chun-sheng[1,2], JING Zheng-jun[1,3]

(1. *School of Computer Engineering, Jiangsu University of Technology, Changzhou Jiangsu* 213001, *China*; 2. *School of Computer Science & Technology, University of Science & Technology of China, Hefei* 230027, *China*; 3. *College of Computer, Nanjing University of Posts & Telecommunications, Nanjing* 210003, *China*)

Abstract: This paper desiged a fully homomorphic encryption (FHE) scheme based on approximate integer GCD problem. Following Gentry's scheme, firstly, it construced a somewhat homomorphic encryption (SHE) scheme, and reduced its security to approximate integer GCD. Then it squashed decryption circuit to achieve bootstrapping by applying SSSP assumption. Finally, it transfered SHE into FHE. The SHE is closer to the public key scheme in literature[2] than [1].

Key words: approximate integer GCD; public key cryptosystem; FHE; SSSP

0 引言

全同态加密方案(FHE)允许对密文进行任意复杂的计算,而不需要解密密文,在云计算、匿名投票、垃圾邮件过滤等领域都有广泛应用。早在 1978 年,Rivest 等人[3]就提出了秘密同态的概念。多年来,设计 FHE 一直是密码学领域的研究热点和难点。但是直到 2009 年,Gentry[4,5]基于理想格问题设计出第一个全同态加密方案。Gentry 方案包括三种成分:a)设计 somewhat 同态加密方案;b)通过引入 SSSP 假设(即稀疏子集和问题假设),压缩解密算法复杂性;c)通过自引技术实现任意密文计算,从而实现全同态加密方案。

遵循 Gentry 设计模式,文献[1,6~8]设计了新的全同态加密方案,文献[1]中 FHE 方案与文献[5]中方案类似,但方案安全性基于整数近似 GCD 求解难度。特别地,文献[8]构造了基于 LWE(learning with error)[9]问题的 FHE 方案和新的自引技术,不依赖于 SSSP 假设。文献[10]设计了使用离散对数假设替换 SSSP 假设的全同态加密方案。

国内对于 FHE 的研究成果目前还不多见,大多是在现有方案基础上提出改进方案,如汤殿华等人[11]在文献[1]的基础上提出了一个整数上的全同态加密方案,与文献[1]相比,该方案基于部分近似最大公因子问题,具有较小的公钥尺寸、计算较快速的特点。但是该方案已经证明是不安全的[12]。徐鹏等人[13]则提出基于整数多项式环的全同态加密方案,该方案也存在安全问题,由其解密算法 $m=[c \bmod x] \bmod 2$ 可知,即使不知道私钥,给定密文可以直接求解出明文。林如磊等人[14]提出整数上的全同态加密方案的改进方案,该方案是将文献[1]中方案明文空间 Z_2 扩展为 Z_4,在密文膨胀率上有了一定提高。

本文首先构造 somewhat 同态加密方案,并将其安全性归约到求解近似整数最大公因数问题,然后跟随文献[1]中方法,将 somewhat 同态加密方案转换为全同态加密方案。目前,近似整数最大公因数问题求解难度还是一个开放问题,文献[1]中详细讨论了已知攻击方法,本文不再赘述。

与文献[1]类似,本文 FHE 方案也是基于整数上近似 GCD 问题,但它更接近于文献[2]中公钥加密方案。在某种意义上,本文是从另外一个视角设计基于整数近似 GCD 的全同态加密方案。

1 符号定义

本文采用希腊字母表示参数,其中 λ 为安全参数,实数和

收稿日期: 2013-08-15; **修回日期**: 2013-09-22 **基金项目**: 国家自然科学基金资助项目(61142007);江苏省普通高校研究生科研创新计划资助项目(CXZZ13_0493);江苏省属高校自然科学基金资助项目(13KJB520005);"青蓝工程"资助项目

作者简介:于志敏(1973-),男,吉林梅河口人,讲师,硕士,主要研究方向为网络与信息安全(619686056@qq.com);古春生(1971-),男,安徽繁昌人,副教授,博士,主要研究方向为网络与信息安全;景征骏(1978-),男,江苏丹阳人,讲师,博士研究生,主要研究方向为网络与信息安全.

整数用小写英文字母表示。

对一个实数 z,$\lceil z\rceil$ 表示上整数,即 $\lceil z\rceil \in [z, z+1)$,$\lfloor z\rfloor$ 表示下整数,即 $\lfloor z\rfloor \in (z-1, z]$,$\lfloor z\rceil$ 表示最近整数,即 $\lfloor z\rceil \in (z-\frac{1}{2}, z+\frac{1}{2}]$,$[z]$ 表示取 z 的整数部分,$\{z\}$ 表示取 z 的小数部分,即 $\{z\} = z - [z]$。

对一个实数 z 和一个整数 p,$q_p(z)$ 和 $r_p(z)$ 分别表示 z 除以 p 的商和剩余,即 $q_p(z) = \lfloor z/p\rceil$,$r_p(z) = z - q_p(z) \times p$,显然 $r_p(z) \in (-p/2, p/2]$。本文采用 $[z]_p$ 或 $z \bmod p$ 表示 z 模拟 p。

2 Somewhat 同态加密方案(SHE)

首先给出方案中用到的四个参数,这些参数都是安全参数 λ 的多项式。

γ 表示公钥整数的比特长度;η 表示私钥整数的比特长度;ρ 表示噪声整数的比特长度;τ 表示公钥中整数的数量。

ρ 要取足够大以防蛮力攻击,可以取 $\rho = \lambda$。η 为了能够支持足够深度电路来计算压缩解密电路,取 $\eta = \tilde{O}(\lambda^2)$。为防止各种格归约攻击整数近似 GCD 问题,取 $\gamma = \tilde{O}(\lambda^5)$。公钥整数数量 $\tau = \gamma + \lambda$。

2.1 SHE 构造

Somewhat 同态加密方案由密钥生成算法 KeyGen(λ)、加密算法 Encrypt(pk, m)、密文计算 Evaluate($pk, C, c_1, \cdots, c_t$)和解密算法 Decrypt(sk, c)构成,其中 λ 为安全参数。

1)密钥生成算法 KeyGen(λ) 随机选取的 η 比特长度的奇正整数 p,同时随机选取 $[0, 2^\gamma/p)$ 区间内的整数 $q_0, \cdots, q_\tau$,使之服从最大整数 q_i 为奇数。对 $q_0, \cdots, q_\tau$ 重新编号,满足 q_0 最大。随机选取 $[-2^\rho, 2^\rho]$ 区间内的整数 $r_0, \cdots, r_\tau$,令 $x_0 = q_0 p + r_0$,$x_i = [q_i p + r_i]_{x_0}$ $(i = 1, \cdots, \tau)$。公钥 $pk = \langle x_0, x_1, \cdots, x_\tau\rangle$,私钥 $sk = \langle p\rangle$。

2)加密算法 Encrypt($pk, m \in \{0,1\}$) 随机选取整数集 $S \subseteq \{1, 2, \cdots, \tau\}$ 和 $[-2^\rho, 2^\rho]$ 区间内的一个整数 r,计算并输出密文 $c \leftarrow [m\lfloor \frac{x_0}{2}\rceil + r + \sum_{i\in S} x_i]_{x_0}$。

3)密文计算 Evaluate($pk, C, c_1, \cdots, c_t$) 给定一个算术电路 C,输入 t 个密文,电路 C 的加法和乘法门应用于密文,执行整数上的所有操作,返回整数结果,其中加法运算 $c = c_1 + c_2$,乘法运算 $c = 2c_1 \times c_2$。

4)解密算法 Decrypt(sk, c) 计算 $c \bmod p$,如果 $|c \bmod p| > |\frac{p}{4}|$,则 $m = 1$,反之 $m = 0$。

2.2 SHE 正确性

首先证明解密算法是正确的,然后证明密文计算在允许的电路是正确的。

引理 1 方案能够正确解密。

证明 假定 $q_0 = (2k+1)p$,不失一般性,假定 r_0 为偶数,那么 $\lfloor \frac{x_0}{2}\rceil = \lfloor \frac{(2k+1)p + r_0}{2}\rceil = kp + \frac{p-1}{2} + \frac{r_0}{2}$。因为公钥生成过程中执行了 $[x_i]_{x_0}$,引入了另外的噪声,每个公钥元素中的噪声上限为 $2^{\rho+1}$,所以,加密一个比特,密文的噪声至多为 $|\tau 2^{\rho+1} + \frac{r_0}{2}| < (\tau+1)2^{\rho+1} << \frac{p}{4}$,所以,解密函数能正确执行。证毕。

引理 2 电路 C 的加法和乘法门应用于密文,执行整数上的所有操作,返回整数结果。输入密文 c_1、c_2,加法操作执行 $c = c_1 + c_2$,乘法操作执行 $c = 2c_1 \times c_2$。此方案是同态的。

证明 密文 $[c_1]_p = m_1 \times \frac{p-1}{2} + r_1$,$[c_2]_p = m_2 \times \frac{p-1}{2} + r_2$,其中 $r_1, r_2 < (\tau+1)2^{\rho+1}$。显然有 Decrypt($sk, c_1 + c_2$) $= m_1 \oplus m_2$,满足加法同态,而 $2[c_1]_p[c_2]_p = m_1 m_2 \frac{(p-1)^2}{2} + (m_1 r_2 + m_2 r_1)(p-1) + 2r_1 r_2$。因为 $\frac{(p-1)^2}{2} = \frac{p(p-3)}{2} + \frac{p+1}{2}$,并且 $\frac{p(p-3)}{2}$ 是 p 的倍数,可以不予考虑。$2[c_1]_p[c_2]_p = m_1 m_2 \frac{p+1}{2} - m_1 r_2 - m_2 r_1 + 2r_1 r_2$,显然有 Decrypt($sk, 2c_1 \times c_2$) $= m_1 m_2$,满足乘法同态。证毕。

引理 3 给定密文 $x_1, x_2, \cdots, x_t$ 作为输入,计算的多元多项式 $f(x_1, x_2, \cdots, x_t)$ 具有度 d,如果计算后的密文能够解密,必然满足 $|f| \times (\tau 2^{\rho+3})^d < \lfloor \frac{p}{4}\rfloor$,从而 $d \leqslant \frac{\eta - 2}{\rho + 3 + \log\tau + \log t}$。满足此条件的多项式称为允许计算的多项式。这里 $|f|$ 是 f 系数向量的一范数。

证明 两个未经过同态计算的密文相乘产生的噪声上限为 $\tau^2 2^{2\rho+6}$,计算 d 次的噪声上限 $(\tau 2^{\rho+3})^d$,所以经过计算多项式 f,噪声至多为 $|f| \times (\tau 2^{\rho+3})^d$,为保证解密正确,有 $|f| \times (\tau 2^{\rho+3})^d < \lfloor \frac{p}{4}\rfloor$,$p$ 是 η 比特位整数,所以 $|f| \times (\tau 2^{\rho+3})^d < 2^{\eta-2}$。$t$ 个密文输入的多项式 f,其系数向量的一范数 $|f| \leqslant t^d$,那么 d 满足 $d \leqslant \frac{\eta - 2}{\rho + 3 + \log\tau + \log t}$。证毕。

通过上述证明可知,方案 ε 的解密能够正确执行,该方案是同态的。

2.3 减小密文尺寸的一种优化

在加密过程中,为了降低密文尺寸,累加后模 x_0。但是在计算密文时无法同样处理,因为即使执行了一次密文的乘法,结果也会远远大于 x_0,如果进行模处理就会加上或减掉一个大的 x_0 倍数,将会产生不可容忍的错误。

在密文计算时,为了降低密文尺寸,给公钥加上更多的元素形如 $x_i' = q_i' p + r_i'$,其中 r_i' 如同通常的噪声那样在区间 $[-2^\rho, 2^\rho]$ 选取,而 q_i' 则远大于其他公钥元素中 q 的取值。对于 $i = 0, \cdots, \gamma$,令 $q_i' \leftarrow Z \cap [2^{\gamma+i-1}/p, 2^{\gamma+i}/p)$,$r_i' \xleftarrow{\$} Z \cap (-2^\rho, 2^\rho)$,$x_i' = 2q_i' p + r_i'$,保证了 $x_i' \in [2^{\gamma+i}, 2^{\gamma+i+1}]$。在密文计算过程中,每次密文的增长超过了 2^γ,本文将它依次模以 $x_\gamma', x_{\gamma-1}', \cdots, x_0'$,使密文比特长度不大于 γ。每次密文计算后其比特长度至多增长为原来的 2 倍,不大于 2γ,意味着采用上述优化方法只会添加少量噪声。

3 SHE 安全性

参数为 $(\rho, \eta, \gamma, \tau)$ 的 SHE 方案的语义安全性有如下定理:

定理 1　参数为(ρ,η,γ,τ)的 SHE 方案,在参数为(ρ,η,γ)的整数近似 GCD 问题难解的假设下是语义安全的,达到了 IND-CPA 安全。

本章在定义整数近似 GCD 问题后,将 SHE 方案安全性归约到求解整数近似 GCD 问题。

3.1　归约到整数近似 GCD 问题

对于给定 η 比特的奇正整数 p,γ 比特的整数,其分布为

$$D_{\gamma,\rho}(p)=\{q\xleftarrow{\$}Z\cap[0,2^{\gamma}/p),r\xleftarrow{\$}Z\cap[-2^{\rho},2^{\rho}],x=pq+r\}$$

定义 1　参数为(ρ,η,γ)的整数近似 GCD 问题是对于随机选取的 η 比特的奇正整数 p,通过在 $D_{\gamma,\rho}(p)$分布中采样多项式数量的样本来求解 p。

定理 2　对于 2.1 节定义的参数为(ρ,η,γ,τ)的 somewhat 同态模式,任何对于该加密模式具有优势 ε 的攻击者 A 都能够转换为算法 B 来求解参数为(ρ,η,γ)的整数近似 GCD 问题。B 成功的概率是 $\varepsilon/2$,运行时间可以用 A 的运行时间、λ 和 $1/\varepsilon$ 的多项式表示。

证明　对于 2.1 节定义的 somewhat 同态模式,A 具有优势 ε,意味着给定密文, A 输出正确明文的概率为 $1/2+\varepsilon$,而 ε 是不可忽略的。本文证明的基本思路是算法 B 首先创建公钥,然后类似文献[1,15]的方法,经过一个精度放大的步骤,把 A 包装成能够正确解密的可靠神谕,把随机高噪声密文下猜中加密位的能力转换为在任意低噪声整数预测其商的奇偶位的能力,最后利用该神谕来求解整数近似 GCD 问题。基于此思路,攻击分四个步骤:

a)生成公钥

B 从 $D_{\gamma,\rho}(p)$中随机采样 $\tau+1$ 个样本 $x_0,x_1,\cdots,x_\tau$,并重新对样本编号满足 x_0 为最大的正整数,之后依次计算 $x_i \bmod x_0$ $(i=1,2,\cdots,\tau)$。公钥$pk=\langle x_0,x_1,\cdots,x_\tau\rangle$。

b)包装猜解正确明文的神谕函数。

采用步骤 a)生成的公钥加密的密文作为输入,包装 A 成为获取明文的神谕函数。

Sub　Learn_LSB(z,pk)

输入:$pk=\langle x_0,x_1,\cdots,x_\tau\rangle$,$z$,满足 $z\in[0,2^{\gamma})$,$|r_p(z)|\leqslant 2^{\rho}$。

输出:LSB($q_p(z)$),即 $q_p(z)$的奇偶位 parity($q_p(z)$)。

1　$c=z\times\lfloor\frac{x_0}{2}\rceil$。

2　for $j=1$　to　poly(λ)/ε do。

3　　调用 A 猜测 c 对应的明文 $a_j\leftarrow A(pk,c)$。

4　　$b_j=a_j\oplus\text{parity}(z)$。

5　循环结束后输出 b_j 的多数票,即为 parity($q_p(z)$)。

因为 $c=z\times\lfloor\frac{x_0}{2}\rceil=(q_p(z)p+r_p(z))\times\lfloor\frac{x_0}{2}\rceil=q_p(z)p\times\lfloor\frac{x_0}{2}\rceil+r_p(z)\times\lfloor\frac{x_0}{2}\rceil$,显然,$\text{parity}(r_p(z))=\text{Decrypt}(sk,c)$,而 $\text{parity}(q_p(z))=\text{parity}(r_p(z))\oplus\text{parity}(z)$,$a_j$ 作为攻击者 A 猜解的 Decrypt(sk,c),所以输出 $a_j\oplus$ parity(z)的多数票即为 parity($q_p(z)$)。通过多项式次数调用,统计 A 猜测的结果,可得到可靠的神谕函数。

c)求解整数近似 GCD。

下面采用二进制 GCD 算法[16],把函数 Learn_LSB 作为恢复 parity(q_pz)的神谕来求解整数近似 GCD。选取 z_1、z_2 分别作为 Learn_LSB 的输入,求解函数如下:

Sub　binary_GCD(z_1,z_2)

1　如果 $z_2>z_1$,那么两者交换 $z_1\leftrightarrow z_2$,使 $z_1>z_2$。

2　调用神谕得到 LSB($q_p(z_1)$)、LSB($q_p(z_2)$),如果两者都为 1,则 $z_1=z_1-z_2$,显然更新后的 LSB($q_p(z_1)$)为 0。

3　如果 LSB($q_p(z_i)$)$=0(i=1,2)$,那么 $z_i=(z_i-\text{parity}(z_i))/2$。

4　重复步骤 1~3,直到 $z_2=0$。

因为 $p>>r_p(z_i)$,z_i 减去自身的奇偶性比特并不影响其除以 p 的商,只会影响剩余 $r_p(z_i)$,有 $q_p(z_i-\text{partiy}(z_i))=q_p(z_i)$。所以,若知道 $q_p(z_i)$为偶数,步骤中的 $z_i=(z_i-\text{parity}(z_i))/2$ 等价于 $q_p(z_i)=q_p(z_i)/2$ 以及 $r_p(z_i)=(r_p(z_i)-\text{partiy})/2$。如文献[1]所述,$r_p(z_i)$永远不会超过两个初始整数中最大的噪声,所以总是有 $p>>r_p(z_i)$。

经过至多 $O(\gamma)$次迭代,最后得到两个整数 z_1'、z_2',$z_2'=0$,而 $q_p(z_1')$恰好是 GCD($q_p(z_1)$,$q_p(z_2)$)的奇部分。如果 $q_p(z_1)$、$q_p(z_2)$互素,有 GCD($q_p(z_1)$,$q_p(z_2)$)$=1$,迭代得到的 $z_1'=1\times p+r$。因为两个随机整数互素的概率为 $6/\pi^2\approx 0.6$,要得到 GCD($q_p(z_1)$,$q_p(z_2)$)$=1$,只要尝试常数次就可以得到满意结果。

d)恢复 p。

令 $z_1'=1\times p+r$,再选取满足条件的整数 $z_2=z^*$,并对这对整数应用 binary_GCD,迭代过程输出 $q_p(z_2)$奇偶性,从而得到 $q_p(z^*)$的二进制表示。最后, $p=\lceil z^*/q_p(z^*)\rfloor$。

3.2　B 成功概率和计算复杂性分析

从 B 生成的公钥过程来看,公钥的元素完全是从分布 $D_{\gamma,\rho}(p)$中随机采样获得的,当 q_0 为奇数这个理想的好事件发生时,公钥元素与分布 $D_{\gamma,\rho}(p)$完全一致。因为理想事件 q_0 为奇数的概率为 1/2,所以采用该公钥加密的密文,攻击者 A 具有优势 ε,B 通过调用 poly(λ)/ε 次 A,把 A 具有的优势 ε 精度放大,获得密文解密的神谕, 进而调用此神谕求解近似 GCD 问题,B 具有的优势为 $\varepsilon/2$。另外,常数个整数欧几里得辗转除法所需时间也可以用 λ 的多项式表示。综上所述,B 总的运行时间可以用 A 的运行时间、λ 和 $1/\varepsilon$ 的多项式表示。证毕。

4　全同态加密方案(FHE)

在本文 SHE 的解密算法中,计算 c/p 过于复杂,使得该加密方案不具有自引能力,需要对解密算法进行压缩。本章采用了文献[1]中“稀疏子集和”方法压缩方案的解密电路,降低其计算复杂性,使该方案具有自举性,从而构造出全同态加密方案。压缩电路的基本思路是:在公钥中添加一部分私钥信息,使得方案能够实行密文同态计算的电路深度比解密电路深度更深,即当某个密文中噪声接近解密阈值时,方案就在密文同态意义下对密文进行解密,以产生新密文,新密文与原密文中明文相同,但其噪声已经变小,可以继续进行密文同态计算。

4.1　压缩解密算法

1)密钥生成算法 KeyGen(n)　如前文生成 $sk^*=p$ 和 pk^*。令 $x_p=\lfloor 2^k/p\rceil$,随机选择 Θ 比特海明重量为 θ 的向量,$s=\langle s_1,\cdots,s_\Theta\rangle$,并且令 $T=\{i:s_i=1\}$,其中 $\kappa=\gamma\eta/\rho$,$\theta=\lambda$,

$\Theta = \omega(\kappa \times \log\lambda)$。

选择随机整数 $u_i \in Z \cap [0, 2^{\kappa+1})$, $i = 1, \cdots, \Theta$, 满足 $\sum_{i \in S} u_i = x_p \pmod{2^{\kappa+1}}$。令 $y = \langle y_1, \cdots, y_\Theta \rangle$, 其中 $y_i = u_i / 2^\kappa$, 因此每个 y_i 是小于 2 的正实数, 在二进制小数点后有 κ 位的精度。同时, $[\sum_{i \in T} y_i]_2 = 1/p - \Delta_p$, $|\Delta_p| < 2^{-\kappa}$。对于向量 $\boldsymbol{s}$ 中每个比特 s_i 产生相应密文 s_i, 记比特密文向量为 $\boldsymbol{s}$。

输出私钥 $sk = \langle s, p \rangle$ 和公钥 $pk = \langle pk^*, \boldsymbol{s}, y \rangle$。

2)加密和密文计算　同前文产生密文 c^*, c^* 可以是初始密文, 也可以是经过密文计算后的密文, 输出 c^*。

3)解密算法 Decrypt(sk, c^*)　如果 $|\{[\sum_{i \in S} y_i]_2 \times c^*\}| > 1/4$ 成立, 则输出 $m = 1$, 反之, 输出 $m = 0$。

前文定义 somewhat 同态加密方案允许计算的密文多项式 $f(x_1, x_2, \cdots, x_t)$, 它的度 d 满足 $d \leqslant \dfrac{\eta - 2}{\rho + 3 + \log\tau + \log t}$。因此, 本节改进方案计算允许计算多项式也是正确的。

证明　计算允许计算多项式得到的密文 $c^* = q^* p + m \times \dfrac{p}{2} + r^*$, 因为同态计算后的噪声增加幅度不大于文献[1]中方案的幅度, 参考文献[1]中引理 2 的结论可知, $|r^*| < p/8$。由公钥生成算法可知 $[\sum_{i \in S} y_i]_2 = 1/p - \Delta_p$, $|\Delta_p| < 2^{-\kappa}$, 所以当 $m = 1$ 时, $|\{[\sum_{i \in S} y_i]_2 \times c^*\}| \in (3/8, 5/8)$, 而当 $m = 0$ 时, $|\{[\sum_{i \in S} y_i]_2 \times c^*\}| \in (-1/8, 1/8)$, 显然解密算法 Decrypt($sk, c^*$)能够正确执行。证毕。

4.2　压缩解密算法的复杂性和安全性分析

与文献[1]需要计算 Θ 次乘法和加法相比, 本方案解密电路只需 θ 次加法和一次乘法, 计算复杂性大大降低。方案中给定公钥中的向量 $\boldsymbol{y}$ 携带了私钥的信息, 这里引进了稀疏子集和(SSSP)的安全假设。SSSP 也称为低密度背包问题, 在文献[17,18]有详细讨论, 只要选择的 Θ 足够大, 就可以避免此类攻击。

4.3　实现全同态加密

在构造新的 SHE 后, 本文 FHE 方案的其他算法与文献[1]中相同。在引入 SSSP 假设后, FHE 的解密电路已经能够在同态密文下进行计算, 并且在密文同态解密后产生的新密文仍然能够进行至少一次同态密文计算。因此, 能够进行密文同态运算的次数不受限制, 从而实现了全同态加密方案。

4.4　本文方案与文献[1]方案的比较

本文方案与文献[1]方案安全性都基于整数近似 GCD 问题及 SSSP 难度假设, 两者公钥尺寸大小相当, 但文献[1]方案的解密算法需要 Θ 次乘法和加法, 而本文方案只需要一次乘法和少量加法运算, 这样节约了大量计算成本和通信成本, 两者比较如表 1 所示。

表 1　两个全同态方案的性能比较

方案	安全级别	基于的困难问题	通信成本	解密算法计算成本
文献[1]	IND-CPA	整数近似 GCD 问题及 SSSP 假设	较高	Θ 次乘法和 Θ 次加法
本文	IND-CPA	整数近似 GCD 问题及 SSSP 假设	较低	θ 次加法和 1 次乘法

5　结束语

本文基于整数近似 GCD 问题, 设计了新的全同态加密算法, 该方案跟随 Gentry 方案设计模式, 首先构造 somewhat 同态加密方案, 然后通过引入 SSSP 假设压缩解密电路, 把 somewhat 同态加密方案转换为全同态加密方案。与文献[1]中方案相比, 本文 somewhat 同态加密方案更接近于文献[2]中公钥加密方案。在某种意义上, 本文提供了研究设计基于整数近似 GCD 的全同态加密方案的新的视角。

参考文献:

[1] Van DIJK M, GENTRY C, HALEVI S, *et al*. Fully homomorphic encryption over the integers[C]//LNCS, vol 6110. Berlin: Springer, 2010: 24-43.

[2] REGEV O. New lattice-based cryptographic constructions[J]. Journal of the ACM, 2004, 51(6): 899-942.

[3] RIVEST R, ADLEMAN L, DERTOUZOS M. On data banks and privacy homomorphisms[J]. Foundations of Secure Computation, 1978, 7(1): 169-177.

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

[5] GENTRY C. Fully homomorphic encryption using ideal lattices[C]// Proc of STOC. New York: ACM Press, 2009: 169-178.

[6] GENTRY C, HALEVI S. Implementing gentry's fully-homomorphic encryption scheme[C]//LNCS, vol 6632. Berlin: Springer, 2011: 129-148.

[7] SMART N P, VERCAUTEREN F. Fully homomorphic encryption with relatively small key and ciphertext sizes[C]//LNCS, vol 6056. Berlin: Springer, 2010: 420-443.

[8] BRAKERSKI Z, VAIKUNTANATHAN V. Efficient fully homomorphic encryption from (standard) LWE[EB/OL]. (2011-08-04). http://eprint.iacr.org/2011/344.

[9] REGEV O. On lattices, learning with errors, random linear codes, and cryptography[C]//Proc of STOC. New York: ACM Press, 2005: 84-93.

[10] GENTRY C, HALEVI S. Fully homomorphic encryption without squashing using depth-3 arithmetic circuits [EB/OL]. (2011-09-14). http://eprint.iacr.org/2011/279.

[11] 汤殿华, 祝世雄, 曹云飞. 一个较快速的整数上的全同态加密方案[J]. 计算机工程与应用, 2012, 48(28): 117-122.

[12] 古春生, 景征骏, 于志敏. 破解较快速的整数上的全同态加密方案[J]. 计算机工程与应用, 2013, 49(21): 101-105.

[13] 徐鹏, 刘超, 斯雪明. 基于整数多项式环的全同态加密算法[J]. 计算机工程, 2012, 38(24): 1-4.

[14] 林如磊, 王箭, 杜贺. 整数上的全同态加密方案的改进[J]. 计算机应用研究, 2013, 30(5): 1515-1519.

[15] GOLDREICH O, SCHORR C P. RSA and Rabin functions: Certain parts are as hard as the whole[J]. SIAM Journal Comput, 1988, 17(2): 194-209.

[16] KNUTH D E. Seminumerial algorithms, volume 2 of the art of computer programming[M]. 3rd ed. Boston: Addion-Wesley, 1997: 79-85.

[17] NGUYEN P Q, SHPARLINSKI I. On the Insecurity of some server-aided RSA protocol[C]//LNCS, vol 2248. Berlin: Springer, 2001: 21-35.

[18] NGUYEN P Q, STERN J. Adapting density attacks to low-weight knapsacks[C]//LNCS, vol 3788. Berlin: Springer, 2005: 41-58.