具有较短公钥的批处理整数上的全同态加密*

罗炳聪[a], 柳 青[b], 马 远[a], 汤 瑜[a]
(云南大学 a. 信息学院; b. 软件学院, 昆明 650091)

摘 要: Coron 等人将批处理技术应用在整数上的全同态加密方案,可以在一个密文中同态地处理和加密一个明文向量,提高了原方案的效率,但它的公钥尺寸为 $\tilde{O}(\lambda^8)$。为了减小该方案的公钥尺寸,结合公钥元素的二次形式与密文压缩技术,提出一种批处理整数上全同态加密算法的改进方案,改进后方案的公钥尺寸为 $\tilde{O}(\lambda^{5.5})$,具有较小的公钥尺寸,并证明了该方案语义安全。

关键词: 全同态加密; 批处理; 公钥尺寸; 密文压缩; 二次形式
中图分类号: TN918.4 **文献标志码**: A **文章编号**: 1001-3695(2014)04-1180-05
doi:10.3969/j.issn.1001-3695.2014.04.054

Batch fully homomorphic encryption over integers with shorter public keys

LUO Bing-cong[a], LIU Qing[b], MA Yuan[a], TANG Yu[a]
(*a. School of Information Science & Engineering, b. School of Software, Yunnan University, Kunming* 650091, *China*)

Abstract: Coron et al applied batch technique to the fully homomorphic encryption scheme over the integers, which could homomorphicly process and encrypt a plaintext vector in a ciphertext and improved the efficiency of the original scheme. But it's public-key size was $\tilde{O}(\lambda^8)$. In order to reduce the public-key size, combined with the quadratic forms of public key elements and the ciphertext compression technique, this paper presented a variant batch fully homomorphic encryption scheme over the integers, which the public-key size was $\tilde{O}(\lambda^{5.5})$. The scheme had smaller public-key size. Finally, it proves that the scheme is semantically secure.

Key words: fully homomorphic encryption; batch; public-key size; ciphertext compression; quadratic form

0 引言

根据 RSA 公钥密码体制的乘法同态特性,Rivest 等人[1]在 1978 年提出了隐私同态的概念,即可以直接对密文进行操作而不需要将密文解密后再进行。在过去的三十多年中,密码学学者进行了大量的研究,但所提出的方案均不具备全同态的特性,即不能对密文进行任意复杂度的操作来实现对明文的相应操作。2009 年,IBM 研究员 Gentry[2,3] 利用理想格构造出第一个全同态加密方案。其构造步骤为:a)构造一个 SomeWhat 同态加密方案,因为密文中加入了噪声,而噪声的大小会随着对密文进行加法或乘法同态操作而增大,只有当噪声的大小低于某个阈值时解密才能正确进行,所以该方案只能对密文进行有限次的加法或乘法操作;b)压缩解密电路降低解密算法的复杂度来获取自举性,利用重加密技术刷新密文降低密文的噪声,使得密文的噪声在允许的范围之内,这些被刷新的密文又可以进行同态运算。不断地对密文进行刷新,这样密文就可以进行无限次的同态运算,实现了一个全同态加密方案。同态加密在保护云计算环境下用户数据的安全性与隐私、密文检索与处理以及多方计算中有着广泛的应用。自从 Gentry 在全同态加密上取得了突破性进展后,全同态加密已经成为密码学领域的研究热点。到目前为止,主要有以下三类不同的全同态加密方案:

a)2009 年,Gentry 提出的基于理想格的全同态加密方案。文献[4~7]从不同方面对该方案进行优化,Gentry 等人[8] 使用了一些优化技术,实现了 Gentry 所提出的全同态加密方案。按他们所描述的实现方案,在最安全的设置下,即当设置格的维数 $n=32\,768$ 时,公钥的尺寸约为 2.3 GB,在一个高端工作站上,密钥生成的时间是 2.2 h,加密需要 3 min,每次刷新密文需要 30 min。

b)2010 年,Dijk 等人[9] 根据 Gentry 的思路对简单代数结构上的全同态加密方案进行了研究,提出一种基于整数的全同态加密方案(DGHV)。该方案与 Gentry 提出的方案相比,由于方案中的所有操作都是基于整数而不是理想格,概念相对比较简单,但它的 SomeWhat 同态加密方案的公钥尺寸为 $\tilde{O}(\lambda^{10})$,全同态加密方案的公钥尺寸为 $\tilde{O}(\lambda^{13})$。文献[10~12]采用不同的公钥压缩技术来对方案进行优化,使得公钥的尺寸从 $\tilde{O}(\lambda^{10})$ 减小到了 $\tilde{O}(\lambda^5)$,文献[12]中还描述了一个使用模转换技术替换自举性实现的基于整数的全同态加密方案。文献[13]中使用批处理技术优化该方案,使得在一个密文中可以同态地处理和加密多个明文位,优化后方案的公钥尺寸为 $\tilde{O}(\lambda^8)$。

c)2011 年,Brakerski 等人[14,15] 基于容错学习问题(learning with errors, LWE)和环上的容错学习问题(ring learning with errors, RlWE)构造出一种不依赖理想格的全同态加密方

收稿日期: 2013-05-14; **修回日期**: 2013-06-27 **基金项目**: 云南省软件工程重点实验室开放基金资助项目(2011SE08)

作者简介: 罗炳聪(1987-),男,云南大理人,硕士研究生,主要研究方向为同态加密(bingcongluo@163.com);柳青(1963-),男,教授,主要研究方向为信息安全、软件工程;马远(1988-),男,硕士,主要研究方向为信息安全;汤瑜(1987-),男,硕士,主要研究方向为信息安全.

案。由于 LWE 问题的难解性是归约到一般格上的困难问题,因此这一方案的安全性比 Gentry 所提出的全同态加密方案的安全性要高,但它的公钥尺寸与它对密文进行乘法的次数成正比,因此,难以处理较复杂的密文运算。文献[16 ~ 18]对方案的加解密效率进行了优化,而对于如何控制公钥尺寸并无有效的解决方案[19]。

本文讨论如何在公钥尺寸方面对 DGHV 方案进行优化。Coron 等人[13]用批处理技术来优化 DGHV 方案,可以将 $l=\tilde{O}(\lambda^2)$ 个明文位加密到一个密文中,因此其密文扩展率从 $\tilde{O}(\lambda^5)$ 变为 $\tilde{O}(\lambda^3)$。重加密操作同时在 l 个明文槽中进行,而其代价就相当于原 DGHV 方案中的一次重加密,但是它的公钥尺寸变为了 $\tilde{O}(\lambda^8)$。本文结合公钥元素的二次形式和公钥压缩技术对提出的方案进行优化,使得优化后方案的公钥尺寸为 $\tilde{O}(\lambda^{5.5})$。相对于原 DGHV 方案,本文方案具有较短的公钥尺寸、较快的加解密效率。

1　准备知识

本章首先简单回顾由 Coron 等人[13]使用批处理技术优化的 DGHV 方案(BDGHV)。

1.1　符号及参数定义

对于一个实数 x,$\lceil x\rceil$、$\lfloor x\rfloor$ 和 $\lfloor x\rceil$ 分别表示对实数 x 向上、向下和就近取整数。对于一个实数 z 和一个整数 p,用 $q_p(z)$ 和 $r_p(z)$ 或者 $[z]_p$ 分别表示 z 除以 p 的商和余数。给定安全参数 λ,本文需要用到的参数有:公钥中整数 x_i 的位长 γ;私钥 p 的位长 η;噪声 r_i 的位长 ρ;公钥中 x_i 的个数 τ;加密过程中的次噪声参数 ρ'。

1.2　BDGHV 方案的 SomeWhat 同态加密

根据 Gentry 在其博士论文中所提出的全同态加密方案,全同态加密是在 SomeWhat 同态加密方案的基础上通过压缩解密电路获取自举性,然后通过自举转换来实现全同态加密。BDGHV 方案也是根据这个思路构造的。这里只对优化后的 SomeWhat 同态加密方案进行简单介绍。方案描述如下:

1) KeyGen(1^λ)　生成素数集合 $p_0,\cdots,p_{l-1}$,其中 p_i 的位长为 η,用 π 表示它们的乘积。定义一个没有噪声的公钥元素 $x_0=q_0\times\pi$,其中 q_0 满足:$q_0\leftarrow\mathbb{Z}\cap[0,2^\gamma/\pi)$,不包含素数因子且小于 2^{λ^2}。生成在 $\mathbb{Z}\cap[0,q_0)$ 均匀、独立分布的整数 x_i、x'_i 和 Π_i,当 $0\leqslant j\leqslant l-1$ 时,满足:

当 $1\leqslant i\leqslant\tau$ 时,$x_i \bmod p_j=2r_{i,j}$,其中 $r_{i,j}\leftarrow\mathbb{Z}\cap(-2^{\rho'-1},2^{\rho'-1})$;

当 $0\leqslant i\leqslant l-1$ 时,$x'_i \bmod p_j=2r'_{i,j}+\delta_{i,j}$,其中 $r'_{i,j}\leftarrow\mathbb{Z}\cap(-2^\rho,2^\rho)$;

当 $0\leqslant i\leqslant l-1$ 时,$\Pi_i \bmod p_j=2\tilde{\omega}_{i,j}+\delta_{i,j}\cdot 2^{\rho'+1}$,其中 $\tilde{\omega}_{i,j}\leftarrow\mathbb{Z}\cap(-2^\varphi,2^\varphi)$。

公钥 $pk=\langle x_0,(x_i)_{0\leqslant i\leqslant\tau},(x'_i)_{0\leqslant i\leqslant l-1},(\Pi_i)_{0\leqslant i\leqslant l-1}\rangle$,私钥 $sk=(p_j)_{0\leqslant j\leqslant l-1}$。

2) Encrypt($pk,m\in\{0,1\}^l$)　选择随机的整数向量 $\boldsymbol{b}=(b_i)_{1\leqslant i\leqslant\tau}\in(-2^\alpha,2^\alpha)^\tau$ 和 $\boldsymbol{b}'=(b'_i)_{0\leqslant i\leqslant l-1}\in(-2^{\alpha'},2^{\alpha'})^l$,计算密文 $c=[\sum_{i=0}^{l-1}m_i\cdot x'_i+\sum_{i=0}^{l-1}b'_i\cdot\Pi_i+\sum_{i=1}^{\tau}b_i\cdot x_i]_{x_0}$。

3) Decrypt(sk, c)　输出 $\boldsymbol{m}=(m_0,\cdots,m_{l-1})$,其中 $m_j\leftarrow[c]_{p_j} \bmod 2$。

4) Add(pk,c_1,c_2)　输出 $c_1+c_2 \bmod x_0$。

5) Mult(pk,c_1,c_2)　输出 $c_1\cdot c_2 \bmod x_0$。

方案中的参数要满足下面这些约束条件:为了避免针对噪声的暴力攻击 $\varphi\geqslant 2\lambda$;为了保证解密的正确性 $\eta\geqslant\alpha'+\varphi'+1+\log_2(l)$;为了评估压缩解密电路时支持同态操作 $\eta\geqslant\rho\cdot\Theta(\lambda\cdot\log^2\lambda)$;为了防止基于格的攻击 $\gamma=\omega(\eta^2\cdot\log\lambda)$;为了保证方案的语义安全需要 $\rho'\geqslant\rho+\lambda$ 和 $\alpha'\geqslant\alpha+\lambda$;为了在证明方案语义安全时可以应用剩余哈希引理(leftover hash lemma)要求 $\alpha\cdot\tau\geqslant\gamma+\lambda$ 和 $\tau\geqslant l\cdot(\rho'+2)+\lambda$。为满足上面的这些约束,可选取如下参数:$\varphi=2\lambda,\varphi'=3\lambda,\eta=\tilde{O}(\lambda^2),\gamma=\tilde{O}(\lambda^5),\alpha=\tilde{O}(\lambda^2),\alpha'=\tilde{O}(\lambda^2),l=\tilde{O}(\lambda^2),\tau=\tilde{O}(\lambda^3)$,其中 λ 为安全参数。

根据这些参数设置,公钥的尺寸为 $\tilde{O}(\lambda^8)$。事实上,根据文献[9]中的描述,为了防止格攻击,公钥 x_i 的位长 γ 至少应为 2^{23} 位。而此时,公钥的大小至少都是 2^{46} 位,如此大的公钥是不能在任何实际的密码系统中应用的。

2　SomeWhat 同态加密方案描述

2.1　构造 SomeWhat 同态加密方案

方案引入了新的参数 β,并将公钥元素从线性形式变为二次形式[10],即 $x_{i,j}=x_{i,0}\cdot x_{j,1}$,其中 $1\leqslant i,j\leqslant\beta$。本文只需存储 2β 个整数 $x_{i,b}$,就能产生 $\tau=\beta^2$ 个公钥元素 $x_{i,j}$ 来加密。同样,引入参数 μ,使得 $l=\mu^2$ 将明文空间从线性形式变为二次形式。参数的选取和文献[13]中的一样,即 $\varphi=2\lambda,\varphi'=3\lambda,\eta=\tilde{O}(\lambda^2),\gamma=\tilde{O}(\lambda^5),\alpha=\tilde{O}(\lambda^2),\alpha'=\tilde{O}(\lambda^2),l=\tilde{O}(\lambda^2),\tau=\tilde{O}(\lambda^3)$。

1) KeyGen(1^λ)　生成一个素数集合 $\{p_{i,j}\}_{1\leqslant i,j\leqslant\mu}$,其中 $p_{i,j}$ 的大小为 η 位,用 π 表示它们的乘积。定义一个没有噪声的公钥元素 $x_0=q_0\times\pi$,其中 q_0 满足:$q_0\leftarrow\mathbb{Z}\cap[0,2^\gamma/\pi)$,并且不包含素数因子且小于 2^{λ^2}。初始化随机种子为 se_1 的伪随机数生成器 f_1。使用 $f_1(se_1)$ 来产生整数集 $\chi_{i,b}$,其中 $\chi_{i,b}\in[0,x_0)$,$1\leqslant i\leqslant\beta$ 且 $b\in\{0,1\}$。对于所有的 $1\leqslant i\leqslant\mu$ 和 $b\in\{0,1\}$ 的 $\chi'_{i,b}$ 和 $\chi^{\Pi}_{i,b}$,计算下面几个 γ 位的整数:

a) 整数 $x_{i,b}=\chi_{i,b}-\delta_{i,b}(1\leqslant i\leqslant\beta)$,其中 $\delta_{i,b}=[\chi_{i,b}]_\pi+\xi_{i,b}\cdot\pi-\mathrm{CRT}_{p_{m,n}}(2r_{i,b,m,n})_{1\leqslant m,n\leqslant\mu}$,$r_{i,b,m,n}\leftarrow\mathbb{Z}\cap(-2^{\rho'-1},2^{\rho'-1})$,$\xi_{i,b}\leftarrow\mathbb{Z}\cap[0,2^{\lambda+\log_2(\mu^2)+\mu^2\cdot\eta}/\pi)$。

b) 整数 $x'_{i,b}=\chi'_{i,b}-\delta'_{i,b}(1\leqslant i\leqslant\mu)$,其中 $\delta'_{i,b}=[\chi'_{i,b}]_\pi+\xi'_{i,b}\cdot\pi-\mathrm{CRT}_{p_{m,n}}(2r'_{i,b,m,n})_{1\leqslant m,n\leqslant\mu}$,$r'_{i,b,m,n}\leftarrow\mathbb{Z}\cap(-2^\varphi,2^\varphi)$,$\xi'_{i,b}\leftarrow\mathbb{Z}\cap[0,2^{\lambda+\log_2(\mu^2)+\mu^2\cdot\eta}/\pi)$。

c) 整数 $\Pi_{i,b}=\chi^{\Pi}_{i,b}-\delta^{\Pi}_{i,b}(1\leqslant i\leqslant\mu)$,其中 $\delta^{\Pi}_{i,b}=[\chi^{\Pi}_{i,b}]_\pi+\xi^{\Pi}_{i,b}\cdot\pi-\mathrm{CRT}_{p_{m,n}}(2\tilde{\omega}_{i,b,m,n}+\delta_{i,b,m,n}\cdot 2^{\rho'+1})_{1\leqslant m,n\leqslant\mu}$,$\tilde{\omega}_{i,b,m,n}\leftarrow\mathbb{Z}\cap(-2^\varphi,2^\varphi)$,$\xi^{\Pi}_{i,b,m,n}\leftarrow\mathbb{Z}\cap[0,2^{\lambda+2\log_2(\mu)+\mu^2\cdot\eta}/\pi)$。

令公钥 $pk^*=\langle x_0,se_1,(\delta_{i,b})_{1\leqslant i\leqslant\beta,0\leqslant b\leqslant 1},(\delta_{i,b}{}')_{1\leqslant i\leqslant\mu,0\leqslant b\leqslant 1},(\delta^{\Pi}_{i,b})_{1\leqslant i\leqslant\mu,0\leqslant b\leqslant 1}\rangle$,相应的公钥元素 $x_{i,b},x'_{i,b},\Pi_{i,b}$ 就用上面的方法计算出。私钥 $sk^*=(p_{i,j})_{1\leqslant i,j\leqslant\mu}$。

2) Encrypt($pk,m_{i,j}\in\{0,1\}^{\mu\times\mu}$)　选择随机的整数矩阵 $\boldsymbol{b}=(b_{i,j})_{0\leqslant i,j\leqslant\beta}\in(-2^\alpha,2^\alpha)^{\beta\times\beta}$ 和 $\boldsymbol{b}'=(b'_{i,j})_{1\leqslant i,j\leqslant\mu}\in(-2^{\alpha'},2^{\alpha'})^{\mu\times\mu}$,计算密文 $c^*=[\sum_{1\leqslant i,j\leqslant\mu}m_{i,j}\cdot x'_{i,0}\cdot x'_{j,1}+\sum_{1\leqslant i,j\leqslant\mu}b'_{i,j}\cdot\Pi_{i,0}\cdot\Pi_{j,1}+\sum_{1\leqslant i,j\leqslant\beta}b_{i,j}\cdot x_{i,0}\cdot x_{j,1}]_{x_0}$。

3) Decrypt (sk, c^*, z) 输出 $m = (m_{i,j})$, 其中 $m_{i,j} \leftarrow [c^*]_{p_{i,j}}, 1 \leqslant i,j \leqslant \mu$。

4) Add(pk, c_1^*, c_2^*) 输出 $c_1^* + c_2^* \bmod x_0$。

5) Mult(pk, c_1^*, c_2^*) 输出 $c_1^* \cdot c_2^* \bmod x_0$。

由于加密时采用公钥元素的二次形式 $x_{i,j}$, 这样 γ 位的公钥元素个数从 τ 减少到 $2\sqrt{\tau}$, 减少到原来的一半。并且, 在生成密钥时不需要存储 γ 位的公钥元素 $x_{i,j}$, 而只需要存储 η 位的 $\delta_{i,b}$、$\delta'_{i,b}$和 $\delta^{\Pi}_{i,b}$就可以恢复出正确的公钥, 所以公钥尺寸的数量级变为 $2\beta \times (\mu^2 \times \eta + \lambda)$, 按照上面的参数取值即为 $\tilde{O}(\lambda^{5.5})$。私钥的尺寸为$\tilde{O}(\mu^2 \times \eta) = \tilde{O}(\lambda^4)$。

2.2 方案的正确性分析

定理 1 2.1 节描述的方案对于允许电路集合 C_ξ 是正确的。

在给出定理 1 的证明之前, 先给出两个相关的定义。

定义 1 批处理同态解密的正确性。对于一个有 t 个输入的电路 C, 如果对于任意由 KeyGen(1^λ) 产生的密钥对(sk, pk), 任意 t 个 μ^2 位的明文向量 $m_1, \cdots, m_t$, 以及任意的密文 $C = (c_1, \cdots, c_t)$, 其中 c_i = Encrypt (pk, m_i), 有 Decrypt (sk, Evaluate(pk, C, C)) = $C(m_1[i,j], \cdots, m_t[i,j])_{1 \leqslant i,j \leqslant \mu}$, 则称方案 ξ = (keyGen, Encrypt, Decrypt, Evalute) 是正确的。

定义 2 允许电路 C_ξ参照文献[9,13]中的定义, 对于任意的 $i \geqslant 1$ 和任意的整数集输入均小于$|\mu^{2i} 2^{i(\alpha' + \varphi' + 2)}|$实现的电路 C, 输出值的绝对值最大是 $2^{i(\eta - 3 - n)}$, 其中 $n = \lceil \log_2(\lambda + 1) \rceil$, 令 C_ξ 表示允许电路。

证明 假设由加密算法 Encrypt$(pk, m_{i,j} \in \{0,1\}^{\mu \times \mu})_{1 \leqslant i,j \leqslant \mu}$产生的密文为 c, 其包含整数向量 $b = (b_{i,j})_{0 \leqslant i,j \leqslant \beta} \in (-2^\alpha, 2^\alpha)^{\beta \times \beta}$和 $b' = (b'_{i,j})_{1 \leqslant i,j \leqslant \mu} \in (-2^{\alpha'}, 2^{\alpha'})^{\mu \times \mu}$ 满足 $c = \left[\sum_{1 \leqslant i,j \leqslant \mu} m_{i,j} \cdot x'_{i,0} \cdot x'_{j,1} + \sum_{1 \leqslant i,j \leqslant \mu} b'_{i,j} \cdot \Pi_{i,0} \cdot \Pi_{j,1} + \sum_{1 \leqslant i,j \leqslant \beta} b_{i,j} \cdot x_{i,0} \cdot x_{j,1}\right]_{x_0}$。

对于所有的 $1 \leqslant i,j \leqslant \mu$ 有

$$|c \bmod p_{i,j}| \leqslant \mu^2 \cdot 2^{\rho+1} + \tau 2^{\alpha+\rho'+1} + \mu^2 \cdot 2^{\alpha'+\rho'+1} \leqslant \mu^2 \cdot 2^{\alpha'+\rho'+2} \quad (1)$$

令 C 表示有 t 个输入的允许电路集合, 令 $C^\dagger$ 为电路在整数上的操作, 令 c_k = Encrypt$(pk, m_k[i,j])_{1 \leqslant i,j \leqslant \mu, 1 \leqslant k \leqslant t}$, 对于所有的 $1 \leqslant i,j \leqslant \mu$, 有

$$c \bmod p_{i,j} = C^\dagger(c_1, \cdots, c_t) \bmod p_{i,j} = C^\dagger(c_1 \bmod p_{i,j}, \cdots, c_t \bmod p_{i,j}) \bmod p_{i,j} \quad (2)$$

利用式(1)结合允许电路集合的定义, 得到$|C^\dagger(c_1 \bmod p_{i,j}, \cdots, c_t \bmod p_{i,j})| \leqslant 2^{\eta-4} \leqslant p_{i,j}/8$, 因此 $C^\dagger(c_1 \bmod p_{i,j}, \cdots, c_1 \bmod p_{i,j}) \bmod p_{i,j} = C^\dagger(c_1 \bmod p_{i,j}, \cdots, c_1 \bmod p_{i,j})$, 这意味着式(2)变为 $c \bmod p_{i,j} = C^\dagger(c_1 \bmod p_{i,j}, \cdots, c_t \bmod p_{i,j})$, 因此$[c \bmod p_{i,j}]_2 = C^\dagger([c_1 \bmod p_{i,j}]_2, \cdots, [c_t \bmod p_{i,j}]_2) = C(m_1[i,j], \cdots, m_t[i,j])$, 根据定义 1, 该方案是正确的。

2.3 方案的安全性分析

本方案所基于的困难问题是文献[10,20]中所提到的零错误近似最大公因子问题(error-free approximate-GCD problem), 下面给出相关定义。

定义 3[13] 零错误最大公因子问题(EF-AGCD)(ρ, η, γ)。零错误近似最大公因子问题是指对于一个随机的 η 位的素数 p, 给定 $y_0 = q_0 \cdot p$ 和分布 $D_\rho(p, q_0)$的多项式样本信息, 求素数 p。其中 $q_0 \in [0, 2^\gamma/p)$是一个随机整数, $D_\rho(p, q_0)$是指对于具体的 γ 位整数 p 和 q_0, 服从分布 $D_\rho(p, q_0)$ = {选择 $q \leftarrow [0, q_0)$, $r \leftarrow \mathbb{Z} \cap (-2^\rho, 2^\rho)$: 输出 $y = q \cdot p + r$}。

定义 4 零错误μ^2 决定性近似最大公因子问题(EF-μ^2-dAGCD$_{\lambda,\gamma,\eta}$)。零错误μ^2 决定性近似最大公因子问题是指随机选择 η 位的整数集$\{p_{i,j}\}_{1 \leqslant i,j \leqslant \mu}$, 它们的乘积用 π 表示; 一个随机的整数 q_0, 满足 $q_0 \leftarrow \mathbb{Z} \cap [0, 2^\gamma/\pi)$, 小于 2^{λ^2}且不含有素数因子; 一个随机的二进制位 b, 令 $v_0 = (0, \cdots, 0)$, $v_1 \leftarrow \{0,1\}^{\mu \times \mu}$。给定 $x_0 = q_0 (p_{i,j})_{1 \leqslant i,j \leqslant \mu}$, $z = O_{q_0,(p_{i,j})}(v_b)$ 和可以访问 $O_{q_0,(p_{i,j})}$的 Oracle, 猜出 b。

协议 1[21] 不可区分地选择明文攻击。假定 Malice 和一个预言机 Oracle 商定一个明文空间为 M, 密文空间为 C 的加密体制 ε。给定 ε 的加密密钥 k, Malice 选择明文消息 m_0, $m_1 \in M$ 发给 Oracle。如果这两条消息的长度不同, Oracle 把短的消息扩充, 使其与另一条消息一样长, Oracle 随机选择 $b \in \{0,1\}$ 进行加密, $c^* = \begin{cases} \varepsilon_k(m_0), b = 0 \\ \varepsilon_k(m_1), b = 1 \end{cases}$。Oracle 向 Malice 发送询问密文 $c^* \in C$, 密文是关于两个随机输入值的随机变量: 随机数 b 和 ε 的内部随机数。Malice 收到 c^* 后必须回答 0 或 1, 作为它对 Oracle 随机数 b 的猜测。得到概率优势 Adv, 即 Prob $[0 \leftarrow \text{Adversary}(c^*) \mid c^* = \varepsilon_k(m_0)] = \frac{1}{2} \pm \text{Adv}$。

定义 5 语义安全性、不可区分性的选择明文攻击(IND-CPA 安全性)。如果任何多项式有界的攻击者进行协议 1 的攻击游戏之后, 对于给出的概率优势 Adv 都是关于 k 的一个可忽略量, 则称安全参数为 k 的密码体制是语义安全的(IND-CPA 安全性)。

本节将把上述方案语义安全性规约到零错误近似最大公因子问题。为此得到定理 2, 由于该定理的证明和文献[13]中的定理 1 和引理 3 的证明过程类似, 此处只对定理 2 的证明过程进行简要的概述。

引理 1 在μ^2 决定性近似最大公因子问题的假设下, 上述方案是语义安全的。

引理 2 如果零错误近似最大公因子问题是困难的, μ^2 决定性近似最大公因子问题也是困难的。

定理 2 在零错误近似最大公因子问题的假设下, 上述方案是语义安全的。

证明 给定整数 q_0 和$(p_{i,j})_{1 \leqslant i,j \leqslant \mu}$, 构造预言机 Oracle $O_{q_0,(p_{i,j})}(v)$即输入向量 $v \in \mathbb{Z}^{\mu \times \mu}$, 输出 $x = \text{CRT}_{q_0,(p_{i,j})}(q, v_{i,j} + 2r_{i,j})$, 其中 $q \leftarrow [0, q_0)$, $r \leftarrow (-2^\rho, 2^\rho)$。用 $\text{CRT}_{q_0,(p_{i,j})}(q, a_{i,j})$来表示比 $x_0 = q_0 \cdot \prod_{i,j=1}^{\mu} p_{i,j}$小的唯一整数 u, 对所有的 $1 \leqslant i,j \leqslant \mu$, u 满足 $u \equiv q[q_0]$和 $u \equiv a_{i,j}[p_{i,j}]$。因此, 输入明文向量 v, Oracle $O_{q_0,(p_{i,j})}(v)$输出一个密文。$v_{i,j}$可以是$\{0,1\}$或任意的整数。

先证明引理 1 的正确性。按照定义, 要证明方案在该假设下的语义安全性, 就必须要证明使用公钥加密和预言机 Oracle $O_{q_0,(p_{i,j})}(v)$加密, 对区分一个密文是由零加密得到的还是由一个随机信息加密得到的有着相同的困难性。该引理的证明是采用基于游戏的证明方法。本文用一系列的游戏表示攻击者在收到公钥后输出两个 μ^2 位的明文 m_0 和 m_1, 挑战者随机地对这两个明文加密后, 攻击者能够正确地猜想出加密的明文是哪一个。接下来就要证明引理 2 的正确性, 结合引理 1 和 2, 就可以得到定理 2 是正确的, 所以该方案是语义安全的(以上的详细证明过程详见文献[13])。

3　全同态加密方案描述

本章将根据 Gentry 的构思,使用文献[9]中的压缩解密电路技术对方案进行压缩,以降低其解密算法的复杂性,最终使方案获得自举性,从而把 SomeWhat 同态加密方案转换为全同态加密方案。令 $k=\gamma+2+\lceil\log_2(\theta+1)\rceil$,$\theta=\lambda$ 和 $\Theta=\tilde{O}(\lambda^3)$。具体的方案描述如下:

1) KeyGen(1^λ)　按照 SomeWhat 同态加密方案的方法,生成 sk^* 和 pk^*。生成长度为 $\sqrt{\Theta}$ 的位向量 $s_{i,j}^{(0)}$ 和 $s_{i,j}^{(1)}$,其中 $1\leqslant i,j\leqslant\mu$。这个两个位向量满足如下条件:当 $i=j=t$ 时,$s_{i,j,t}^{(0)}=s_{i,j,t}^{(1)}=1$;每个 $s_{i,j}^{(b)}$ 中最多只含有一个非零位,其中 $k\lfloor\sqrt{B}\rfloor<i_1$,$j_1\leqslant(k+1)\lfloor\sqrt{B}\rfloor$,$k\in[0,\sqrt{\theta})$,$b\in\{0,1\}$,$B=\Theta/\theta$;集合 $S=\{(i_1,j_1):s_{i,j,i_1}^{(0)}\cdot s_{i,j,j_1}^{(1)}=1\}$ 中仅含 θ 个元素,其中 $k\lfloor\sqrt{B}\rfloor<i_1$,$j_1\leqslant(k+1)\lfloor\sqrt{B}\rfloor$。初始化随机种子为 se_2 的伪随机数生成器 f_2。使用 $f_2(se_2)$ 来产生整数 $u_{i_1,j_1}\in[0,2^{k+1})$,其中 $1\leqslant i_1,j_1\leqslant\sqrt{\Theta}$,$(i_1,j_1)\neq(i,j)_{1\leqslant i,j\leqslant\mu}$。计算 $(u_{i,j})_{1\leqslant i,j\leqslant\mu}$ 使得 $x_{p_{i,j}}=\sum_{(i_1,j_1)\in S}u_{i_1,j_1}\bmod 2^{k+1}$,其中 $x_{p_{i,j}}=\lfloor 2^k/p_{i,j}\rceil$ $(1\leqslant i,j\leqslant\mu)$。初始化随机种子为 se_3 的伪随机数生成器 f_3,使用 $f_3(se_3)$ 生成整数 $\chi_i^{(b)}\in[0,x_0]$,其中 $1\leqslant i\leqslant\lceil\sqrt{\Theta}\rceil$,$b\in\{0,1\}$。定义一个 γ 位的整数 $\sigma_i^{(b)}=\chi_i^{(b)}-\delta_i^{(b)}$,其中 $\delta_i^{(b)}=[\chi_i^{(b)}]_\pi+\xi_i^{(b)}\cdot\pi+\mathrm{CRT}_{p_{m,n},1\leqslant m,n\leqslant\mu}(2r_{i,m,n}^{(b)}+s_{m,n,i}^{(b)})$,$r_{i,m,n}^{(b)}\leftarrow\mathbb{Z}\cap(-2^\rho,2^\rho)$,$\xi_i^{(b)}\leftarrow\mathbb{Z}\cap[0,2^{\lambda+2\log_2(\mu)+\mu^2\cdot\eta}/\pi)$。所以,私钥 $sk=(s_{i,j}^{(0)},s_{i,j}^{(1)})_{1\leqslant i,j\leqslant\mu}$,公钥 $pk=[pk^*,se_2,(u_{i,j})_{1\leqslant i,j\leqslant\mu},se_3,(\delta_i^{(0)})_{0\leqslant i<\Theta},(\delta_i^{(1)})_{0\leqslant i<\Theta}]$。

2) Encrypt($pk,m_{i,j}\in\{0,1\}^{\mu\times\mu}$)　选择随机的整数矩阵 $b=(b_{i,j})_{0\leqslant i,j\leqslant\beta}\in(-2^\alpha,2^\alpha)^{\beta\times\beta}$ 和 $b'=(b'_{i,j})_{1\leqslant i,j\leqslant\mu}\in(-2^{\alpha'},2^{\alpha'})^{\mu\times\mu}$,计算密文 $c^*=[\sum_{1\leqslant i,j\leqslant\mu}m_{i,j}\cdot x'_{i,0}\cdot x'_{j,1}+\sum_{1\leqslant i,j\leqslant\mu}b'_{i,j}\cdot\Pi_{i,0}\cdot\Pi_{j,1}+\sum_{1\leqslant i,j\leqslant\beta}b_{i,j}\cdot x_{i,0}\cdot x_{j,1}]_{x_0}$。

3) Add(pk,c_1^*,c_2^*)　输出 $c_1^*+c_2^*\bmod x_0$。

4) Mult(pk,c_1^*,c_2^*)　输出 $c_1^*\cdot c_2^*\bmod x_0$。

5) Expand(pk,c^*)　输入密文 c^* 计算相应的扩展密文。首先使用 $f_2(se_2)$ 来计算 $(u_{i,j})_{1\leqslant i,j\leqslant\sqrt{\Theta}}$,令 $y_{i,j}=u_{i,j}/2^k$,计算 $z_{i,j}=[c^*\cdot y_{i,j}]_2$,在二进制小数点后保留 $n=\lceil\log_2(\theta+1)\rceil$ 位。定义矩阵 $z=(z_{i,j})$,所以扩展密文 $c=(c^*,z)$。

6) Decrypt(sk,c,z)　输出 $m=(m_{m,n})$,其中 $m_{m,n}\leftarrow[c^*-[\sum_{i,j}^{\sqrt{\Theta}}s_{m,n,i}^{(0)}\cdot s_{m,n,j}^{(1)}\cdot z_{i,j}]]_2$,$1\leqslant m,n\leqslant\mu$。

7) Recrypt(pk,c^*,z)　利用公钥 pk 恢复加密的私钥位 $\sigma_i^{(b)}$。在扩展密文 z 和加密的私钥位 $\sigma_i^{(b)}$ 上进行解密运算,输出的结果就是刷新的密文 c_{new}^*。

本文将批处理技术应用在原 DGHV 方案压缩解密电路的技术中来压缩本文方案的解密电路,最终得到一个拥有自举性的方案,但本文方案的重加密操作是并行地在 μ^2 个明文槽中进行,其复杂度就相当于原 DGHV 方案的一次重加密,经过重加密后输出一个原来 μ^2 位明文向量的新密文,但是它的噪声减小了。根据 Gentry 自举转换,得到一个可以评估任何电路深度的全同态加密方案。

4　方案性能分析

本文所提出方案的困难性假设是基于零错误近似 GCD 问题,其 SomeWhat 同态加密方案的公钥尺寸的数量级为 $\tilde{O}(\lambda^{5.5})$,私钥尺寸的数量级为 $\tilde{O}(\lambda^4)$,加法门和乘法门的操作复杂度均为 $\tilde{O}(\lambda^{1.5})$。下面将本文方案与文献[9,13]中的 SomeWhat 同态加密方案和全同态加密方案的效率和安全性进行比较,主要从安全级别、基于的困难问题、公钥尺寸、私钥尺寸以及密文的扩展率等方面进行比较,如表 1 和 2 所示。文中所给出的全同态加密方案的公钥尺寸的数量级为 $\tilde{O}(\gamma+(\beta+\sqrt{\Theta})(\mu^2\cdot\eta+\lambda))=\tilde{O}(\lambda^{5.5})$,其公钥尺寸的大小大约为 $2\gamma+2(\beta+\sqrt{\Theta})(\mu^2\cdot\eta+\lambda)$,再与文献[13]设置相同参数的情况下(如表 3 所示),本文全同态加密方案在最安全的设置下即当 $\lambda=72$ 时,公钥尺寸为 71.7 MB,而不是文献[13]中的 5.6 GB。表 3 中的四个安全级别 toy、small、medium 和 large 采用相同的 n 和 θ,它们的值分别为 4 和 15。

表 1　SomeWhat 同态加密方案性能比较(λ 为安全参数)

方案	安全级别	基于的困难问题	公钥选择	公钥尺寸	私钥尺寸	密文扩展率	门运算复杂度
DGHV	IND-CPA	近似 GCD 问题,稀疏子集和	大整数序列	$\tilde{O}(\lambda^{10})$	$\tilde{O}(\lambda^2)$	$\tilde{O}(\lambda^5)$	$\tilde{O}(\lambda^{3.5})$
BDGHV	IND-CPA	零错误近似 GCD 问题、稀疏子集和	大整数序列	$\tilde{O}(\lambda^8)$	$\tilde{O}(\lambda^4)$	$\tilde{O}(\lambda^3)$	$\tilde{O}(\lambda^{1.5})$
本文方案	IND-CPA	零错误近似 GCD 问题、稀疏子集和	矩阵	$\tilde{O}(\lambda^{5.5})$	$\tilde{O}(\lambda^4)$	$\tilde{O}(\lambda^3)$	$\tilde{O}(\lambda^{1.5})$

表 2　全同态加密方案性能比较(λ 为安全参数)

方案	安全级别	基于的困难问题	公钥选择	公钥尺寸	私钥尺寸	密文扩展率	门运算复杂度
DGHV	IND-CPA	近似 GCD 问题,稀疏子集和	大整数序列	$\tilde{O}(\lambda^{13})$	$\tilde{O}(\lambda^7)$	$\tilde{O}(\lambda^5)$	$\tilde{O}(\lambda^{3.5})$
BDGHV	IND-CPA	零错误近似 GCD 问题、稀疏子集和	大整数序列	$\tilde{O}(\lambda^8)$	$\tilde{O}(\lambda^5)$	$\tilde{O}(\lambda^3)$	$\tilde{O}(\lambda^{1.5})$
本文方案	IND-CPA	零错误近似 GCD 问题、稀疏子集和	矩阵	$\tilde{O}(\lambda^{5.5})$	$\tilde{O}(\lambda^{3.5})$	$\tilde{O}(\lambda^3)$	$\tilde{O}(\lambda^{1.5})$

表 3　本文全同态加密方案的公钥大小(λ 为安全参数)

instance	λ	$l=\mu^2$	ρ	η	$\gamma\times10^{-6}$	$\beta^2=\tau$	Θ	Pk size
toy	42	10	26	988	0.29	188	150	134 KB
small	52	37	41	1 558	1.6	661	555	1.1 MB
medium	62	138	56	2 128	8.5	2 410	2 070	8.8 MB
large	72	531	71	2 698	39	8 713	7 965	71.7 MB

由以上数值比较可以看出,相对于 DGHV 方案所基于的困难问题,本文所提出的方案困难性要弱一些,而本文的方案

一次同时对 l 个 bit 位进行加解密和 DGHV 方案一次对 1 个 bit 位进行加解密的代价是一样的,因此本文方案具有加解密效率更高、密文扩展率低和公/私钥尺寸短等特点,更易于在实际的密码系统中应用。相对于 BDGHV 方案,本文方案的公/私钥尺寸更短。

5 结束语

到目前为止,虽然全同态加密方案还不能在实际的密码系统中应用,但自 Gentry 构造出第一个基于理想格的全同态加密方案后,全同态加密已成为当前研究的热点,而研究的方向主要集中在提高方案的效率和安全性这两个方面。在效率方面的研究主要是提高方案的加解密效率和压缩方案的公钥尺寸。本文提出一个具有较短公钥尺寸的批处理整数上的全同态加密方案,并将其语义安全规约到零错误的近似最大公因子问题。相对于 Dijk 等人[9]的整数全同态方案,本方案具有较短的公钥尺寸、较高的加解密效率;相对于 Coron 等人[13]的批处理整数上的全同态加密方案,本方案具有较短的公钥尺寸。

参考文献:

[1] RIVEST R L, ADLEMAN L, DERTOUZOS M L. On data banks and privacy homomorphisms[C]//Proc of the 17th IEEE Annual Symposium on Foundations of Computer Science. [S. l.]: Academic Press, 1978:169-177.

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

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

[4] SMART N P, VERCAUTEREN F. Fully homomorphic encryption with relatively small key and ciphertext sizes[C]//Proc of the 13th International Conference on Practice and Theory in Public Key Cryptography. 2010:420-443.

[5] STEHLÉ D, STEINFELD R. Faster fully homomorphic encryption [C]//Proc of ASICRYPT. 2010:377-394.

[6] BRAKERSKI Z. Fully homomorphic encryption without modulus switching from classical GapSVP [C]//Advances in Cryptology-CRYPTO. Berlin: Springer, 2012:868-886.

[7] SMART N P, VERCAUTEREN F. Fully homomorphic SIMD operations[C]//Designs, Codes and Cryptography. [S. l.]: Springer, 2012:1-25.

[8] GENTRY C, HALEVI S. Implementing Gentry's fully-homomorphic encryption scheme[C]//Proc of the 30th Annual International Conference on Theory and Applications of Cryptographic Techniques: Advances in Cryptology. Berlin: Springer-Verlag, 2011:129-148.

[9] Van DIJK M, GENTRY C, HALEVI S, *et al*. Fully homomorphic encryption over the integers [C]//Advances in Cryptology-EUROCRYPT. Berlin: Springer, 2010:24-43.

[10] CORON J S, MANDAL A, NACCACHE D, *et al*. Fully homomorphic encryption over the integers with shorter public keys[C]//Advances in Cryptology-CRYPTO. Berlin: Springer, 2011:487-504.

[11] CORON J S, NACCACHE D, TIBOUCHI M. Optimization of fully homomorphic encryption [C]//IACR Cryptology ePrint Archive. 2011:440.

[12] CORON J S, NACCACHE D, TIBOUCHI M. Public key compression and modulus switching for fully homomorphic encryption over the integers[C]//Advances in Cryptology-EUROCRYPT. Berlin: Springer, 2012:446-464.

[13] CORON J S, LEPOINT T, TIBOUCHI M. Batch fully homomorphic encryption over the integers[C]//IACR Cryptology ePrint Archive. 2013.

[14] BRAKERSKI Z, VAIKUNTANATHAN V. Efficient fully homomorphic encryption from (standard) LWE[C]//Proc of the 52nd IEEE Annual Symposium on Foundations of Computer Science. 2011:97-106.

[15] BRAKERSKI Z, VAIKUNTANATHAN V. Fully homomorphic encryption from ring-LWE and security for key dependent messages[C]//Advances in Cryptology-CRYPTO. Berlin: Springer, 2011:505-524.

[16] GENTRY C. Fully homomorphic encryption without bootstrapping[J]. Security, 2011, 111(111):1-12.

[17] GENTRY C, HALEVI S, SMART N P. Fully homomorphic encryption with polylog overhead [C]//Proc of the 31st Annual International Conference on Theory and Applications of Cryptographic Techniques. Berlin: Springer-Verlag, 2012:465-482.

[18] GENTRY C, HALEVI S, SMART N. Better bootstrapping in fully homomorphic encryption[C]//Proc of the 15th International Conference on Practice and Theory in Public Key Cryptography. 2012:1-16.

[19] 光焱,顾纯祥,祝跃飞,等. 一种基于 LWE 问题的无证书全同态加密体制[J]. 电子与信息学报, 2013,35(4):988-993.

[20] CHEN Yuan-mi, NGUYEN P Q. Faster algorithms for approximate common divisors: breaking fully-homomorphic-encryption challenges over the integers [C]//Proc of the 31st Annual International Conference on Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2012:502-519.

[21] 吴晓园. 基于格的全同态加密方案的研究与设计[D]. 西安:西安电子科技大学,2012.

(上接第 1179 页)

[3] 南湘浩. CPK 组合公钥体制(v8.0)[J]. 信息安全与通信保密, 2013(3):39-41.

[4] 南湘浩. CPK 算法与标识认证[J]. 信息安全与通信保密,2006(9):12-16.

[5] 张福泰,孙银霞,张磊,等. 无证书公钥密码体制研究[J]. 软件学报,2011, 22(6):1316-1332.

[6] 侯孟波. 基于身份和无证书的两方认证密钥协商协议研究[D]. 济南:山东大学,2010.

[7] 胡亮,初剑峰,林海群,等. IBE 体系的密钥管理机制[J]. 计算机学报,2009,4(3):544-556.

[8] 南湘浩. CPK 标识认证[M]. 北京:国防工业出版社,2006.

[9] 赵建国. 组合公钥(CPK)技术的创新实践[J]. 信息安全与通信保密,2012(5):55-57.

[10] 赵美玲,张少武. 基于 ECC 的组合公钥技术的安全性分析[J]. 计算机工程,2008,34(1):156-157.

[11] 邵春雨,苏锦海,魏有国,等. 一种双矩阵组合公钥算法[J]. 电子学报, 2011,39(3):671-674.

[12] 邵春雨. 双矩阵组合公钥算法及应用研究[D]. 郑州:解放军信息工程大学,2010.

[13] 王公浩,王玟,吴铎,等. CPK 随机碰撞概率分析[J]. 信息安全与通信保密,2008(11):87-88.

[14] 荣昆,李益发. CPK 种子矩阵的优化设计方案[J]. 计算机工程与应用,2006,42(24):120-121.

[15] 邢海龙. 组合公钥 CPK 关键技术研究与应用[D]. 长沙:国防科技大学,2009.

[16] 马芯宇,龙翔,范修斌. 无碰撞 CPK 的种子库构建和选取方案[J]. 计算机工程与应用,2012,48(27):99-104.