基于整数的多对一全同态加密方案

王彩芬* 成玉丹 刘 超 赵 冰 许钦百
(西北师范大学计算机科学与工程学院 兰州 730070)

摘 要：全同态加密是在不解密密文的情况下直接对密文进行操作。现有的基于整数的全同态加密方案是针对两个参与者“一方加密，一方解密”(一对一)设计的，计算效率普遍低，明文空间小，不能应用于大数据、云计算等环境。为此，该文提出一种“多方加密，一方解密”(多对一)的全同态加密方案，该方案在保证安全性的基础上简化密钥生成过程，并在全同态运算过程中给出能够正确解密的加密方个数的具体范围。同时，在随机预言机模型下，基于近似最大公因子问题证明了方案的安全性。数值结果表明，该方案与已有方案相比不仅扩展了数据传输量，而且提高了效率。模拟实验表明，该方案在整数范围内具有可行性，满足用户对系统响应的需求，最后将明文空间扩展为3 bit，并与1 bit的方案做出了实验上的对比分析。

关键词：全同态加密；多对一；近似最大公因子问题；数据扩展
中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2018)09-2119-08
DOI: 10.11999/JEIT171194

Multiple to One Fully Homomorphic Encryption Scheme over the Integers

WANG Caifen CHENG Yudan LIU Chao ZHAO Bing XU Qinbai
(*College of Computer Science and Engineering*, *Northwest Normal University*, *Lanzhou* 730070, *China*)

Abstract: Fully homomorphic encryption allows any operation evaluation on encrypted data without decryption. The existing integer-based homomorphic encryption schemes are designed only for two participants namely one party encryption one party decryption (one-to-one), whose computational efficiency is generally low, plaintext space is small, so it can not be applied to big data, cloud computing and other actual scene. Therefore, a full homomorphic encryption scheme with multi-party encryption, one party decryption (multiple to one) is presented. The scheme simplifies the key generation process on the basis of guaranteeing the security, but also gives the range of the number of encrypted parties that can be decrypted accurately in the process of homomorphic operation. Meanwhile, in the random oracle model, the security of the new scheme is proved based on approximate Greatest Common Divisor (GCD) problem. Numerical analysis demonstrates that the presented scheme can not only extend the data traffic, but also improve the efficiency by comparing with the existing schemes. Simulation results show that proposed scheme is more practical in the range of integer, and meets the requirements of the users to the system response. Finally, the plaintext space is expanded to 3 bit, comparing and analysing the experiment with the scheme of 1 bit.

Key words: Fully homomorphic encryption; Multiple to one; Greatest Common Divisor (GCD) problem; Data expansion

1 引言

1978年，基于RSA公钥加密体制的乘法同态，Rivest[1]提出了同态加密的概念，即在不解密密文的情况下，通过对密文执行操作来实现对明文的操作，且其结果一致。同态加密的提出，受到了国内外学者的广泛关注，但该方案并没有完全的实现全同态，也不能任意次数的操作和处理密文。直到2009年Gentry在文献[2]中提出了第1个基于理想格全同态加密方案，在此文中，构造了一个可实现有限次同态计算的SomeWhat方案，通过同态解密来实现密文的更新，从而实现全同态加密。

收稿日期：2017-12-19；改回日期：2018-05-02；网络出版：2018-07-12
*通信作者： 王彩芬 wangcf@nwnu.edu.cn
基金项目：国家自然科学基金(61202395, 61562077, 61662069, 61662071)；甘肃省自然科学基金(145RJDA325)
Foundation Items: The National Natural Science Foundation of China (61202395, 61562077, 61662069, 61662071); The Natural Science Foundation of Gansu Province (145RJDA325)

基于Gentry的研究，国内外学者提出了很多改进方案。Dijk等人[3]提出了基于整数的全同态加密方案，称作DGHV方案，是第1个基于整数的全同态加密方案，并且提出能够同时加密多个bit数据的假设，但其缺点是计算复杂。同年，文献[4]优化了Gentry的方案，在允许可忽略概率解密错误这一优化条件的基础上，提出了速度较快的全同态加密方案，并且降低了计算复杂度，减少了对安全参数的依赖。Gentry等人[5]对Smart等人[6]提出的密文和密钥相对较小的全同态快速计算方案进行了优化，在降低计算复杂度的同时实现了全同态加密，文献[7]对DGHV方案提出了攻击方案。国内学者也提出了同态加密的改进方案，Tang等人[8]提出了较快速的基于整数上的全同态加密方案，但随后Gu等人[9]质疑其安全性，提出了相应的破解方案。光焱[10]等人提出了无证书全同态加密体制。基于Gentry和Smart在理想格上对全同态加密的研究，古春生[11]提出了基于理想格的全同态加密方案。熊婉君等人[12]对原有的整数加密方案进行了改进。同时，随着近年来大数据和云计算的发展，Hu等人[13]提出了基于云存储的全同态加密方案，对文献[3]的方案做了改进，缩短了公钥尺寸，扩展了单次可加密的数据量，降低了计算复杂度。

上述方案虽然都从不同层面研究了基于整数的同态加密，但只是实现了整数上一对一的同态加解密，并且计算复杂度高，效率低，在当前大数据和云计算的环境中应用有很大的局限性。例如若用户P_1需多次向云服务器传输数据，采用一对一同态加密时，服务器需服务多次，计算复杂度高且效率低下；若有多个用户需向服务器传输数据，在此情况下，服务器需管理大量的密钥且一次只能与一个用户通信，若采用多对一的同态加密技术既解决了密钥管理问题又能够实现多个参与者进行数据传输，提高了算法效率，增加了数据传输量。

2 预备知识

2.1 符号约定

本文所用参数都由$(\eta,\lambda,\tau,\cdots)$表示，其中$\lambda$表示安全参数。实数和整数由小写的英文字母$(p,q,x,y,\cdots)$表示，集合和域由大写的英文字母$(H,X,Y,\cdots)$表示。文中的数据都是对整数2取模后的操作，若有其他含义则另作说明。

对于实数z和整数p，用$q_p(z)$，$r_p(z)$分别表示z对p的商和余数。

对于大整数m和整数n，$[m]_n$表示m对n求模运算。

2.2 相关定义

定义 1[2] 同态加密：同态加密方案中包含4个算法：KeyGen(λ)，Encrypt(pk,m)，Decrypt(sk,c)，Evaluate$(\mathrm{pk},C,\boldsymbol{c})$。KeyGen$(\lambda)$：产生公私钥对$(\mathrm{pk},\mathrm{sk})$; Encrypt$(\mathrm{pk},m)$：在公钥pk下把明文$m$加密成密文$c$; Decrypt$(\mathrm{sk},c)$：用私钥sk解密密文$c$，得到明文$m$；Evaluate$(\mathrm{pk},C,\boldsymbol{c})$：输入一个公钥pk，电路$C$，和一个密文元组$\boldsymbol{c}=\langle c_1,c_2,\cdots,c_t\rangle$，输出另一个密文元组$\boldsymbol{c}$。

定义 2[3] 同态解密的正确性：对于任意的由KeyGen(λ)生成的密钥对，任意的t个明文bit $m_1,m_2,\cdots,m_t$，以及$c_i\leftarrow\mathrm{Encrypt}_\Phi(\mathrm{pk},m_i)$生成的任意密文元组$\boldsymbol{c}=\langle c_1,c_2,\cdots,c_t\rangle$，若Evaluate $(\mathrm{pk},C,\boldsymbol{c})$算法对任意给定的$t$个输入都能够正确解密，则称方案能够正确地同态解密。具体表示如下：Decrypt $(\mathrm{sk},\mathrm{Evaluate}(\mathrm{pk},C,\boldsymbol{c}))=C(m_1,m_2,\cdots,m_t)$。

定义3[3] 近似GCD问题：近似最大公因子问题是指：参数为ρ,η,γ，p为一个随机的η比特的素数，$x_0=pq_0$, $q_0\in Z\cap[0,2^\gamma/p)$ $D_\rho(p,q_0)=\{q\leftarrow[0,q_0)$, $r\leftarrow Z\cap(-2^\rho,2^\rho):x=pq+r\}$，求$p$的过程就是近似GCD问题。

2.3 SomeWhat同态加密方案

Dijk等人[3]在Gentry方案的基础上提出了基于整数的全同态加密方案(DGHV)，下面对DGHV方案做简单的介绍(详细方案参考文献[3])，DGHV方案是SomeWhat同态加密方案。

KeyGen(λ)：选取一个η位的奇整数$p\xleftarrow{\$}[2^{\eta-1},2^\eta)\cap(2Z+1)$作为私钥sk，选择$q_i\xleftarrow{\$}Z\cap[0,2^\gamma/p)$，$r_i\xleftarrow{\$}Z\cap(-2^\rho,2^\rho)$，其中$q_0$最大且为奇数，令$x_0=pq_0+r_0$，$x_i=[pq_i+r_i]_{x_0}$，$0\le i\le\tau$。公钥$\mathrm{pk}=\langle x_0,x_1,\cdots,x_\tau\rangle$。

Encrypt(pk,m)：随机选取一个集合$S\subseteq\{1,2,\cdots,\tau\}$和一个随机整数$r\leftarrow(-2^\rho,2^\rho)$，明文$m\in\{0,1\}$，输出密文$c\leftarrow\left[m+2r+\sum_{i\in S}x_i\right]_{x_0}$。

Decrypt(sk,c)：输出明文$m\leftarrow\Big[[c]_p\Big]_2$。

Evaluate$(\mathrm{pk},C,c_1,c_2,\cdots,c_t)$：输入公钥pk、电路$C$和$t$个密文$c_1,c_2,\cdots,c_t$，其中$c_i=\mathrm{Encrypt}(\mathrm{pk},m_i)$, $i=1,2,\cdots,t$。输出$c^*=\mathrm{Evaluate}(\mathrm{pk},C,c_1,c_2,\cdots,c_t)$且满足Decrypt $(\mathrm{sk},c^*)=C(m_1,m_2,\cdots,m_t)$。此算法的含义是：对密文任意操作后再解密，其结果和对明文进行操作是一致的。

不难证明DGHV加密方案满足加法和乘法的同态，具有全同态性。

虽然此方案满足全同态的特性，但存在以下不足：(1)只能是指定的一方加密一方解密，加解密

的参与者是2个；(2)每次只能对一个用户进行操作，单次可操作的数据量太少；(3)方案的效率低。

3　多对一同态加密模型及实现方案

目前提出的方案大多实现了整数上一对一的同态加解密，并且计算复杂度高，效率低，在当前大数据和云计算的环境中有很大的局限性，下面就多对一同态加密模型和实现方案作出详细解释。

3.1　多对一同态加密模型

实际应用中一对一的同态加解密存在很大的局限性，计算复杂且效率低。比如在云服务器的加解密中，多个用户P_i将信息用自己的私钥加密后上传到云服务器P，由于工作的需要P_i要对其加密的数据解密。若采用传统的“多对一”的思想，即用户P_i用P的公钥加密，P用自己的私钥解密，此时P_i就不能对数据解密，无法验证数据的正确性，若P_i和P采用一对一的方式通信，则P会管理大量的密钥。又因为P_i需多次上传数据到服务器，则P需要对P_i的数据处理多次，产生繁杂的数据运算。若P_i的密文之间具有同态性，这样P只需对密文运算即可，降低了运算代价。由以上的描述可知，P_i需要解密自己的密文，P也需要解密所有P_i的密文，若用户P_i和P_j的密文在P面前呈现同态性(即P对P_i和P_j等的所有密文进行运算之后再解密，可以得到与先解密后计算相同的结果)，这样既解决了密钥管理问题，又降低了计算复杂度。为此，本文提出了以下多对一同态加密模型。

此方案涉及一个解密方P和多个加密方P_i。假设明文空间M,P的公私钥对$(\mathrm{pk},\mathrm{sk})$,$P_i$的公私钥对$(\mathrm{pk}_i,\mathrm{sk}_i)$，密钥生成算法$\mathrm{KeyGen}(\lambda)$，加密算法$\mathrm{Encrypt}(\mathrm{pk},m)$，解密算法$\mathrm{Decrypt}(\mathrm{sk},c)$。除了具有一般同态加密算法的性质外，对任意的明文$m_1,m_2\in M$，还满足式(1)和式(2)，其中$\oplus$表示某种运算符，$i\neq j$。

$$D_{\mathrm{sk}}\big(E_{\mathrm{pk}_i}(m)\big)=m \tag{1}$$

$$D_{\mathrm{sk}}(E_{\mathrm{pk}}(m_1\oplus m_2))=D_{\mathrm{sk}}\big(E_{\mathrm{pk}_i}(m_1)\oplus E_{\mathrm{pk}_j}(m_2)\big) \tag{2}$$

式(1)表示的是多对一的性质，即解密方P可以解密多个加密方P_i加密的信息；式(2)说明多对一的一个重要性质，P_i和P_j加密的密文可由P解密且同态运算。

3.2　具体方案描述

本文基于文献[3]在一对一同态加密的基础上提出了多对一同态加密方案并且扩大了加密的数据量，提高了效率。在方案的证明过程中采用了文献[14]的思路证明了方案的正确性和全同态性。

3.2.1 参数选择　输入安全参数为λ，噪音长度为ρ，私钥长度为η，公钥长度为γ，公钥中整数的个数为τ。这些参数必须满足以下条件：$\rho=\omega(\log_2\lambda)$，为了能够抵抗噪音的蛮力攻击；$\eta\geq\rho\Theta(\lambda\log_2\lambda)^2$，为了能够支持足够深的电路同态评估；$\gamma=\omega\big(\eta^2\log_2\lambda\big)$，为了阻止各种基于格的攻击；$\tau\geq\gamma+(\omega\log_2\lambda)$，为了能够在GCD中使用剩余的哈希引理。若二次噪声参数为$\rho'=\rho+\omega(\log_2\lambda)$，其他参数的设置如下：$\rho=\lambda$，$\rho'=2\lambda$，$\eta=\widetilde{O}\big(\lambda^2\big)$，$\gamma=\widetilde{O}\big(\lambda^5\big)$，$\tau=\lambda+\gamma$。方案的复杂度是$\widetilde{O}\big(\lambda^{10}\big)$。

3.2.2 具体方案　本文方案的算法具体介绍如下：

KeyGen(λ)：加密系统由一个解密方P和多个加密方$P_i(i=0,1,\cdots,\tau)$组成。根据DGHV方案生成P的公私钥$\mathrm{sk}=p$,$\mathrm{pk}=\langle x_0,x_1,\cdots,x_\tau\rangle$。在多个加密方$P_i$的公私钥的生成阶段，此方案在文献[14]随机置换的基础上选用了随机向量变换，简化公钥的生成过程，且方案的安全性仍是基于近似GCD问题。$P_i(i=0,1,\cdots,\tau)$随机选择一个整数$p_i\xleftarrow{\$}[2^{\eta_i-1},2^{\eta_i})\cap(2Z+1)$作为私钥，即$\mathrm{sk}_i=p_i$。$P_i$对$P$的公钥pk进行向量变换，随机选取向量$\boldsymbol{Q}=\langle q_{i,0},q_{i,1},\cdots,q_{i,\tau}\rangle\xleftarrow{\$}Z\cap[0,2^{\gamma_i}/p_i)$和$\boldsymbol{R}=\langle r_{i,0},r_{i,1},\cdots,r_{i,\tau}\rangle\xleftarrow{\$}Z\cap(-2^{\rho_i},2^{\rho_i})$，使得$x_{i,0}\leftarrow x_0q_{i,0}+2r_{i,0}$，$x_{i,j}\leftarrow x_iq_{i,j}+2r_{i,j}$，$j\in\{0,1,2,\cdots,\tau_i\}$。假设$x_{i,0}$最大，则取$x_{i,j}\leftarrow[x_{i,j}]_{x_{i,0}}$，$P_i$的公钥$\mathrm{pk}_i=\langle x_{i,0},x_{i,1},\cdots,x_{i,\tau}\rangle$。

Encrypt(pk_i,m_i)：P_i随机选取一个集合$S_i\subseteq\{0,1,\cdots,\tau\}$和整数$t_i\leftarrow(-2^{\rho_i},2^{\rho_i})$。对于明文$m_i\in\{0,1\}$，输出密文：$c_i\leftarrow\Big[m_i+2t_i+\sum_{j\in S}x_{i,j}\Big]_{x_{i,0}}$。在此过程中对$x_{i,0}$求模是为了缩减密文的长度。

Decrypt$(\mathrm{sk}_i,c_i,\mathrm{sk})$：解密方法有两种。第1种是$P_i$用自己的私钥$\mathrm{sk}_i=p_i$解密得到$m_i\leftarrow\Big[[c_i]_{p_i}\Big]_2$；第2种是$P$根据自己的私钥$\mathrm{sk}=p$，解密得到$m_i\leftarrow\Big[[c_i]_p\Big]_2$。

Evaluate$(\mathrm{pk}_i,C,c_1,c_2,\cdots,c_t)$：输入公钥$\mathrm{pk}_i$、电路$C$和$t$个密文$c_1,c_2,\cdots,c_t$，其$c_i=\mathrm{Encrypt}(\mathrm{pk}_i,m_i)$，$i=1,2,\cdots,t$，输出$c^*=\mathrm{Evaluate}(\mathrm{pk}_i,C,c_1,c_2,\cdots,c_t)$且满足$\mathrm{Decrypt}(\mathrm{sk}/\mathrm{sk}_i,c^*)=C(m_1,m_2,\cdots,m_t)$。

3.2.3 方案的正确性证明　本文中多对一同态加密方案的解密涉及两种形式，即P/P_i通过解密算法能够成功解密，证明过程如下：

定理 1　$(\mathrm{pk}_i,\mathrm{sk}_i)$是$P_i$的密钥对，密文$c_i\leftarrow\mathrm{Encrypt}(\mathrm{pk}_i,m_i)$，$m_i\in\{0,1\}$，$P$使用解密算法$\mathrm{Decrypt}(\mathrm{sk},c_i)$能够成功解密$m_i$。

证明 $c_i \leftarrow \left[m_i + 2t_i + \sum_{j\in S} x_{i,j}\right]_{x_{i,0}}$ 因为$|x_{i,0}| > |x_{i,j}|,\ j \in \{0,1,\cdots,\tau_i\}$。所以存在$k_i$使得

$$c_i = m_i + 2t_i + \sum_{j\in S} x_{i,j} - k_i x_{i,0},\ |k_i| \le \tau_i \tag{3}$$

由KeyGen(λ)可得：$x_{i,0} \leftarrow x_0 q_{i,0} + 2r_{i,0}$，$x_{i,j} \leftarrow x_i q_{i,j} + 2r_{i,j}$，代入式(3)可得

$$\begin{aligned} c_i = {} & m_i + 2t_i + \sum_{j\in S} (x_i q_{i,j} + 2r_{i,j}) \\ & - k_i (x_0 q_{i,0} + 2r_{i,0}) \end{aligned} \tag{4}$$

根据DGHV方案有$x_i = pq_i + 2r_i$，所以代入式(4)整理得

$$\begin{aligned} c_i = {} & m_i + p\left(\sum_{j\in S} q_i q_{i,j} - k_i q_0 q_{i,0}\right) \\ & + 2\left(t_i + \sum_{j\in S} r_i q_{i,j} r_{i,j} - k_i r_0 q_{i,0} - k_i r_{i,0}\right) \end{aligned} \tag{5}$$

又因为 $\left|m_i + 2\left(t_i + \sum_{j\in S} r_{i,j} - k_i r_{i,0}\right)\right| < p_i$，令

$$a_i = \left(\sum_{j\in S} q_i q_{i,j} - k_i q_0 q_{i,0}\right)$$

$$b_i = \left(t_i + \sum_{j\in S} r_i q_{i,j} r_{i,j} - k_i r_0 q_{i,0} - k_i r_{i,0}\right)$$

则将a_i，b_i代入式(5)得到：$c_i = m_i + a_i p + 2b_i$，所以$m_i = \left[[c_i]_p\right]_2$。

综上所述，P使用解密算法Decrypt(sk, c_i)能够成功解密m_i。 证毕

定理 2 $(\mathrm{pk}_i, \mathrm{sk}_i)$是$P_i$的密钥对，密文$c_i \leftarrow \mathrm{Encrypt}(\mathrm{pk}_i, m_i)$，$m_i \in \{0,1\}$，$P_i$使用解密算法$\mathrm{Decrypt}(\mathrm{sk}_i, c_i)$能够成功解密$m_i$。

证明 $c_i \leftarrow \left[m_i + 2t_i + \sum_{j\in S} x_{i,j}\right]_{x_{i,0}}$。因为$|x_{i,0}| > |x_{i,j}|,\ j \in \{0,1,\cdots,\tau_i\}$。所以存在$k_i$使得

$$c_i = m_i + 2t_i + \sum_{j\in S} x_{i,j} - k_i x_{i,0},\ |k_i| \le \tau_i \tag{6}$$

对于任何一个j，都存在$q_{i,j}$和$r_{i,j}$，使得$x_{i,j} \leftarrow p_i q_{i,j} + 2r_{i,j}$，$x_{i,0} \leftarrow p_i q_{i,0} + 2r_{i,0}$，代入式(6)整理得

$$\begin{aligned} c_i = {} & m_i + p_i\left(\sum_{j\in S} q_{i,j} - k_i q_{i,0}\right) \\ & + 2\left(t_i + \sum_{j\in S} r_{i,j} - k_i r_{i,0}\right) \end{aligned} \tag{7}$$

又因为 $\left|m_i + 2\left(t_i + \sum_{j\in S} r_{i,j} - k_i r_{i,0}\right)\right| < p_i$，令 $a_i = \sum_{j\in S} q_{i,j} - k_i q_{i,0}$，$b_i = t_i + \sum_{j\in S} r_{i,j} - k_i r_{i,0}$，将$a_i$，$b_i$代入式(7)得：$c_i = m_i + a_i p_i + 2b_i$。所以$m_i = \left[[c_i]_{p_i}\right]_2$。

综上所述，P_i使用解密算法Decrypt(sk$_i$, c_i)能够成功解密m_i。 证毕

3.2.4 方案的同态性证明 本文方案是全同态加密方案，在全同态运算的过程中，就加法同态而言，噪声的增长与加法运算次数呈线性增长趋势，但对于乘法同态，噪声的增长与乘法运算次数呈指数增长趋势，所以同态问题的瓶颈就在于如何确定能够正确解密的乘法电路的深度，在本文中体现为多方加密时用户的个数，即用户的个数不能无限大，只有在一定的范围内才能够正确解密。下面是进行同态运算后能够正确解密的用户范围的确定。

由文献[3]可知**Encrypt**算法噪音最多是$2^{\rho'+2}$，算法**Evaluate**能够成功解密的约束是$2^{\eta-4} < p/8$。在加同态中噪声增加与τ选取有关。而乘同态中噪声增长和多项式的阶有关，即乘法门电路的深度d有关。

引理 1 假设布尔电路C有t个输入，$C^{\dagger}$是与整数有关的门电路，$f(x_1, x_2, \cdots, x_t)$是通过$C^{\dagger}$计算的多项式，d是多项式的阶。设|f|表示系数向量$\boldsymbol{f}$的范数，若$|\boldsymbol{f}| \cdot \left(2^{\rho'+2}\right)^d \le 2^{\eta-4}$，则$C \in \boldsymbol{C}_{\varepsilon}$。具体证明过程详见文献[3]。由此可得多项式的阶的范围是$d \le \dfrac{\eta - 4 - \log_2|\mathrm{f}|}{\rho' + 2}$。

在此方案中，将单次可传输的数据量由单个用户扩展到l个用户，对l个用户进行同态乘法运算，由引理1可得，若要能够正确解密，则同态乘法深度$d \le \dfrac{\eta - 4 - \log_2|\mathrm{f}|}{\rho' + 2}$，即$l \le \dfrac{\eta - 4 - \log_2|\mathrm{f}|}{\rho' + 2}$也就是说，能够正确同态解密的用户的个数应该在这个范围内。

在引理1的基础上，得到以下两个定理：

定理 3 $(\mathrm{pk}_i, \mathrm{sk}_i)$和$(\mathrm{pk}_j, \mathrm{sk}_j)$分别是$P_i$和$P_j$的密钥对，$P$可实现对$P_i$和$P_j$密文的加法和乘法的同态。

证明 对于任意的明文$m_i, m_j \in \{0,1\}$。$c_i \leftarrow \mathrm{Encrypt}(\mathrm{pk}_i, m_i)$，$c_j \leftarrow \mathrm{Encrypt}(\mathrm{pk}_j, m_j)$。由定理2可得：存在$a_i$，$b_i$，$a_j$，$b_j$使得$c_i = pa_i + 2b_i + m_i$，$c_j = pa_j + 2b_j + m_j$。设加密后的密文为：$c_i$，$c_j$，则有$c_i + c_j = p(a_i + a_j) + 2(b_i + b_j) + (m_i + m_j)$；$c_i \cdot c_i = p(a_i(pa_j + 2b_j + m_j) + a_j(2b_i + m_i)) + 2(2b_i b_j + b_i m_j + m_i b_j) + m_i m_j$。因为，$|2(b_i + b_j) + (m_i + m_j)| < p$，$|2(2b_i b_j + b_i m_j + m_i b_j) + m_i m_j| < p$。$P$根据3.2.1节的解密算法解密得：$D_{\mathrm{sk}}(c_i + c_j) = m_i + m_j$，即$D_{\mathrm{sk}}(E_{\mathrm{pk}}(m_i + m_j)) = D_{\mathrm{sk}}\left(E_{\mathrm{pk}_i}(m_i) + E_{\mathrm{pk}_j}(m_j)\right)$;

$D_{\mathrm{sk}}(c_i \cdot c_j) = m_i \cdot m_j$ ，即 $D_{\mathrm{sk}}(E_{\mathrm{pk}}(m_i \cdot m_j)) = D_{\mathrm{sk}}\left(E_{\mathrm{pk}_i}(m_i) \cdot E_{\mathrm{pk}_j}(m_j)\right)$ 。

综上所述，P可实现对P_i和P_j密文的加法和乘法的同态。　　证毕

定理 4　$(\mathrm{pk}_i, \mathrm{sk}_i)$是$P_i$的密钥对，则$P$和$P_i$可实现加法和乘法的同态。定理4的证明与定理3类似，篇幅有限，故定理4的证明省略。

3.2.5 方案的安全性证明　在该方案的构造过程中，为了提高传输效率，将单次可操作的传输量由一个用户扩展到多个用户。由3.2.1节的方案可知，解密方法有两种：(1)由解密方P用自己的私钥p进行解密得到明文消息；(2)由加密方P_i对自身加密的消息进行解密，私钥p_i。所以攻击者就有两种攻击方法：(1)恢复解密方的私钥p来攻破方案；(2)恢复加密方的私钥p_i来攻破方案，从而求解AGCD问题。下面通过定理5给出第2种攻击的安全性证明过程。

本方案的安全性证明借鉴文献[3]中安全性的证明方法，它的主要证明思路是使用攻击者A来构造求解困难问题的算法B，包括4个步骤：(1)利用困难问题产生方案的公钥$\mathrm{pk}/\mathrm{pk}_i$; (2)利用A构造求解$p/p_i$的商的最小比特位；(3)构造求解$p/p_i$的Binary-GCD算法；(4)恢复$p/p_i$。

定理 5　在3.2.1节的方案中固定参数$(\lambda, \rho, \eta, \gamma, \tau)$(安全系数$\lambda$)。任意优势为$\varepsilon$的攻击者A对此方案的攻击均可以转化为算法B以至少$\varepsilon/2$的优势解决AGCD问题。B的运行时间是$T_A$, λ和$1/\varepsilon$的多项式。

证明　用$q_p(z)$和$r_p(z)$表示z对p的商和余数，因此$z = q_p(z) \cdot p + r_p(z)$。攻击者A输入公钥$\mathrm{pk}_i$和密文$c_i$(公钥和密文均由方案3.2.1节的算法生成)，能正确输出明文的概率是$1/2 + \varepsilon$。

在参数相同时，A通过求解器B来解决AGCD问题。求解器B从分布$D_{r,\rho}(p)$中获得多个关于p的多项式样本，目标就是得到p_i。

步骤 1　创建公钥pk_i。B从分布$D_{r,\rho}(p)$得到$\tau+1$个样本：$x_0, x_1, \cdots, x_\tau \xleftarrow{\$} D_{\gamma,\rho}(p)$和两个随机向量$\boldsymbol{Q} = \langle q_{i,0}, q_{i,1}, \cdots, q_{i,\tau}\rangle$，$\boldsymbol{R} = \langle r_{i,0}, r_{i,1}, \cdots, r_{i,\tau}\rangle$。由3.2.1节的算法KeyGen($\lambda$)，得$\mathrm{pk}_i = \langle x_{i,0}, x_{i,1}, \cdots, x_{i,\tau}\rangle$。

步骤 2　高精度的LSB预测。B产生一系列整数，通过利用A来学习这些整数对于p_i的商的最小比特位来尝试恢复p_i。B调用子程序Learn-LSB$(z_{i,k}, pk_i)$[3]输出主要向量$\boldsymbol{b'}_k s$。

步骤 3　给定任意两个整数，$z_1 = q_p(z_1) \cdot p + r_p(z_1)$，$z_2 = q_p(z_2) \cdot p + r_p(z_2)$ $(r_p(z_i) \ll p)$，用Learn-LSB构建算法Binary-GCD(z_1, z_2)[3]得到$q_p(z)$的最小比特位。

步骤 4　恢复p。B选取一对元素$z_1^*, z_2^* \xleftarrow{\$} D_{\gamma,\rho}(p)$，执行Binary-GCD算法，得到$z_1^*, z_2^*$互质的可能性至少是$\pi^2/6 \approx 0.6$，因此GCD$(z_1^*, z_2^*)$将高概率输出元素$\tilde{z} = 1 \cdot p + r$，其中$|r| < 2^\rho$。获得$\tilde{z}$后，重复GCD算法，得到$q_p(z_1)$在所有迭代过程中的奇偶校验序列的二进制表示，则B得到$p = [z_1^*/q_p(z_1^*)]$。

总结：若可靠随机喻言机能计算出$[q_p(z)]_2$, $(r_p(z) \ll p)$，则B就可以恢复p。接下来分析在可靠随机喻言机模型下B成功的概率。事件G表示B在理想条件下成功概率是1/2，记negl为可忽略函数。

由步骤1可得，B产生公钥的分布与此方案产生的正确分布不可区分。文献[3]已证明对于私钥p，敌手A以ε的优势猜测加密的比特，B通过Learn-LSB子程序产生的密文在统计上接近于方案中密文的分布。p若满足：$\mathrm{sk} = p \in \left[2^{\eta-1}, 2^\eta\right)$是奇整数，则A的优势至少为$\varepsilon/2$。统计表明$p \in P$的概率至少是$\varepsilon/2$，则A的优势至少为$\varepsilon/4$。对于每一个$p \in P$，即$\mathrm{sk} = p$时，KeyGen算法总能以$\varepsilon/4$的概率输出$\mathrm{pk} \in \mathrm{PK}_p$。若$p \in D_{\gamma,\rho}(p)$且$p \in P$，事件G发生，则B产生正确密文的概率是$\varepsilon' - \mathrm{negl}$，则A返回正确结果的概率是$\varepsilon/4 - \mathrm{negl}$。当$p \in P$时，B在运行中恢复$p$的概率至少是$1/2 \cdot (\varepsilon/4 - \mathrm{negl})$, B重复调用子程序$(8/\varepsilon) \cdot \omega(\log_z \lambda)$次，此时B的时间复杂度是poly$(\lambda, 1/\varepsilon)$，所以B成功的概率至少是$\varepsilon/2$。至此，定理5证明完毕，此方案是IND-CPA安全的。

4　性能分析

4.1　方案比较

下面就文献[3]、文献[13]和本文方案从安全性、效率和加\解密的参与者方面做比较，衡量安全性的指标有：方案的安全性级别、基于的困难问题假设等；衡量效率的指标有：公/私钥的尺寸、加/解密算法的时间复杂度、算法的吞吐量等；加解密的参与者的指标有：是一方参与还是多方参与。具体比较情况如表1所示。

由表1的对比可以看出，本文方案沿用了基于整数的全同态加密方案的近似最大公因子的困难问题，安全级别满足IND-CPA安全。单次可传输的数据量由1 bit扩展到了l bit，并且将原来的一对一两个参与者增加到多对一多个参与者。

4.2　实验分析

本节给出在一定条件下运行时间的对比分析，主要是与文献[3]的对比：当公钥元素个数为5和10时，随着私钥长度的增加，公私钥产生时间、加密时间和解密时间的对比。

4.2.1 实验环境配置 实验环境配置示于表2。

4.2.2 实验数据分析 假设私钥长度的取值为3～15位(若私钥长度为3位，私钥的取值范围为$\mathrm{sk}\in(2^{-3},2^{3})$)，公钥的长度为30位，公钥元素个数分别为5和10，本文方案和文献[3]DGHV方案的对比如图1–图4。

由于DGHV方案和本文方案私钥的产生方式都是相同的，所以图1仅给出了一条曲线来表示私钥长度和私钥产生时间的关系，并且随着私钥长度的增加，私钥产生时间的增长几乎趋近一次函数。由图2可以看出，随着私钥长度的增加，公钥产生时间均呈现增长的趋势，当公钥元素个数为5时，本文方案较DGHV方案时间最大相差约为1.5 ms左右；当公钥元素个数为10时，两种方案的时间接近，当私钥长度达到12以上时，最大差值为0.5 ms左右。图3中，私钥长度增加，加密时间增长缓慢，公钥元素个数为10时，本文方案较DGHV方案，时间差值几乎接近0.2 ms。在图4中，公钥元素个数为5时，两种方案的解密时间相差0.1 ms，当公钥元素个数为10时，随着私钥长度的增加，差值逐渐减少。但由图3和图4可以很明显地看出，当公钥元素个数为10时，本文方案所花的时间明显地大于其他3种情况，但均在可接受的范围内。

表 1 方案的安全性、效率和加\解密的参与者比较

方案名称	文献[3]	文献[13]	本文方案
安全级别	IND-CPA	IND-CPA	IND-CPA
连续性	好	好	好
困难问题	近似最大公因子问题	近似最大公因子问题	近似最大公因子问题
公钥尺寸	$\tilde{O}(\lambda^{10})$	$\tilde{O}(\lambda^{7})$	$\tilde{O}(\lambda^{10})$
私钥尺寸	$\tilde{O}(\lambda^{2})$	$\tilde{O}(\lambda^{2})$	$\tilde{O}(\lambda^{2})$
单次传输数据量	1 bit	3 bit	l bit
加/解密的参与者	一对一	一对一	多对一

表 2 实验环境配置

计算机型号	操作系统	处理器	内存	开发环境	运算库	数据处理
HP Compad 8280 Elite	Windows 7(32位)	Inter Core i5～2400M (3.10 GHz)	4 GB	Visual C++ 6.0	PBC-0.4.7-VC	MATLAB 2010

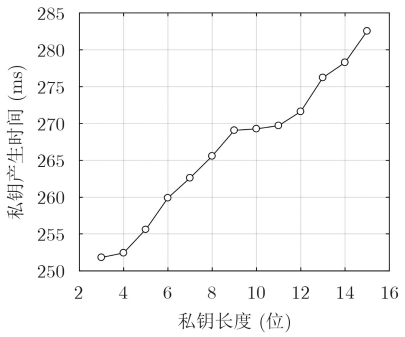

图 1 私钥长度与私钥产生时间的关系

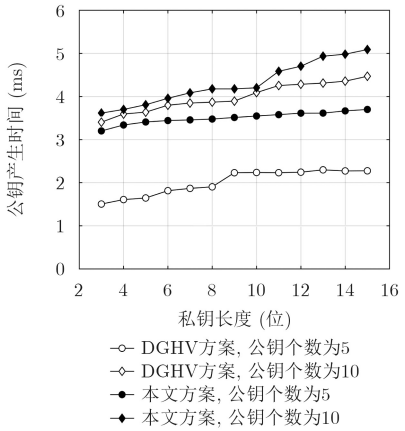

图 2 私钥长度与公钥产生时间的关系

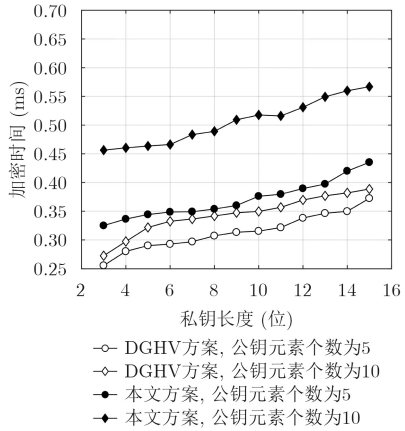

图 3 私钥长度与加密时间的关系

5 方案扩展

本文方案的明文空间$\{0,1\}$，但在实际应用中明文往往是一个较大的整数，所以本文方案还可以

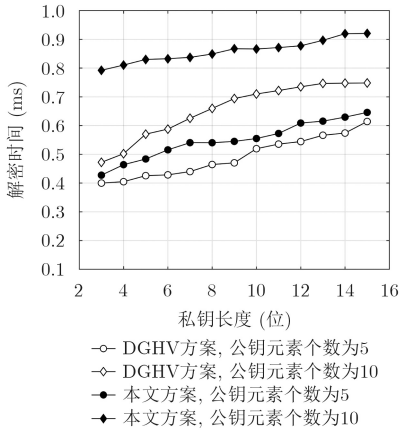

图 4 私钥长度与解密时间的关系

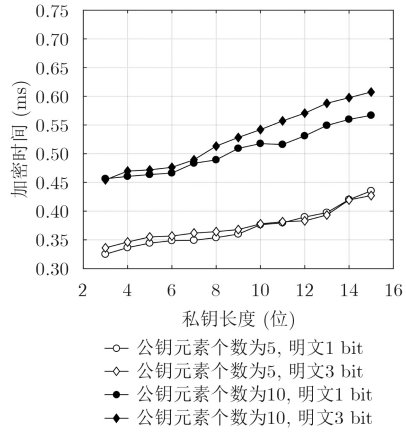

图 5 私钥长度与加密时间的关系

将明文空间扩展到$n$bit即$\{0,1\}^n$。对此有如下扩展算法：

KeyGen(λ)：与3.2.2节密钥的生成方式基本相同，不同在P_i对P的公钥pk进行向量变换，随机选取向量$\boldsymbol{Q}=\langle q_{i,0}, q_{i,1}, \cdots, q_{i,\tau}\rangle \xleftarrow{\$} Z\cap[0, 2^{\gamma_i}/p_i)$和向量$\boldsymbol{R}=\langle r_{i,0}, r_{i,1}, \cdots, r_{i,\tau}\rangle \xleftarrow{\$} Z\cap(-2^{\rho_i}, 2^{\rho_i})$，使得$x_{i,0}\leftarrow x_0q_{i,0}+2^nr_{i,0}$, $x_{i,j}\leftarrow x_iq_{i,j}+2^nr_{i,j}$, $j\in\{0,1,2,\cdots,\tau_i\}$。假设$x_{i,0}$最大，则取$x_{i,j}\leftarrow[x_{i,j}]_{x_{i,0}}$, P_i的公钥$\mathrm{pk}_i=\langle x_{i,0}, x_{i,1}, \cdots, x_{i,\tau}\rangle$。

Encrypt(pk_i, m_i)：P_i随机选取一个集合$S_i\subseteq\{0,1,\cdots,\tau\}$和随机的一个整数$t_i\leftarrow(-2^{\rho_i}, 2^{\rho_i})$。对于明文$m_i\in\{0,1\}^n$，输出密文：$c_i\leftarrow\left[m_i+2^nt_i+\sum_{j\in S}x_{i,j}\right]_{x_{i,0}}$。

Decrypt$(\mathrm{sk}_i, c_i, \mathrm{sk})$：解密的方法有两种。第1种是$P_i$用自己的私钥$\mathrm{sk}_i=p_i$解密得到$m_i\leftarrow\Big[[c_i]_{p_i}\Big]_{2^n}$；第2种是$P$根据自己的私钥$\mathrm{sk}=p$，解密得到$m_i\leftarrow\Big[[c_i]_{p}\Big]_{2^n}$。

至此，将该方案扩展为可加密n bit的全同态加密方案。在4.2节实验的基础上，设n=3，即扩展为3 bit，就本文方案和扩展方案做了实验上的对比分析，给出了私钥长度和加解密之间的关系。如图5，图6所示。

由图5可知，在本文方案中，公钥元素的个数为5，用户个数为1和3时，私钥长度增加，加密时间增长且基本趋于一致，当公钥元素个数为10时，私钥长度大于8以后，加密时间的差值约为0.05 ms。在图6中，解密时间在公钥元素个数相同时，它们各自的差值最大约为0.1 ms。

6　结束语

目前对全同态加密的研究主要是提高方案的执行率和安全性两个方面，但其研究对象基本是一对一的模型。本文基于整数的DGHV同态加密方案，提出了多对一的全同态加密方案，该方案的安全性基于AGCD问题，在效率上优于一对一的方案，而且增加了数据的传输量，并且通过实验证明了此方案的可行性。

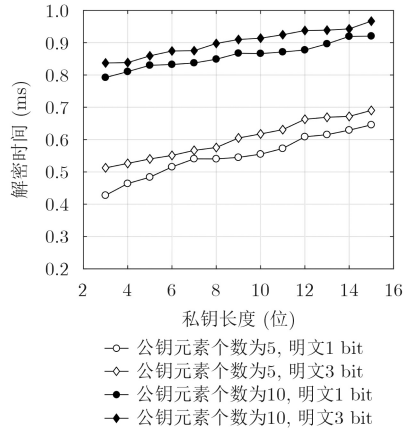

图 6 私钥长度与解密时间的关系

参 考 文 献

[1] RIVEST R. A method for obtaining digital signatures and public-key cryptosystems[J]. *Communications of the ACM*, 1978, 21(2): 120–126. doi: 10.1145/357980.358017.

[2] GENTRY C. Fully homomorphic encryption using ideal lattices[C]. ACM Symposium on Theory of Computing, Bethesda, USA, 2009: 169–178. doi: 10.1145/1536414.1536440.

[3] DIJK M, GENTRY C, HALEVI S, *et al*. Fully homomorphic encryption over the integers[C]. International Conference on the Theory and Applications of Cryptographic Techniques, Berlin, Heidelberg, 2010: 24–43. doi: 10.1007/978-3-642-13190-5_2.

[4] STEHLE D and STEINFELD R. Faster fully homomorphic encryption[C]. Advances in Cryptology-ASIACRYPT 2010, International Conference on the Theory and Application of Cryptology and Information Security, Singapore, 2010:

377–394. doi: 10.1007/978-3-642-17373-8_22.

[5] GENTRY C and HALEVI S. Implementing Gentry's fully-homomorphic encryption scheme[C]. Advances in Cryptology-EUROCRYPT 2011, International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, 2011: 129–148. doi: 10.1007/978-3-642-20465-4_9.

[6] SMART N and VERCAUTEREN F. Fully homomorphic encryption with relatively small Key and ciphertext sizes[C]. International Conference on Practice and Theory in Public Key Cryptography, Paris, France, 2010: 420–443.

[7] CHENAL M and TAHG Q. On key recovery attacks against existing somewhat homomorphic encryption schemes[J]. *Lecture Notes in Computer Science*, 2014, 8895: 239–258. doi: 10.1007/978-3-319-16295-9_13.

[8] TANG Dianhua and ZHU Shixiong. Faster fully homomorphic encryption scheme over integer[J]. *Computer Engineering & Applications*, 2012, 48(28): 117–122. doi: 10.3778/j.issn.1002-8331.2012.28.023.

[9] GU Chunsheng, JING Zhengjun, YU Zhimin *et al*. Breaking faster fully homomorphic encryption scheme over integer[J]. *Computer Engineering & Applications*, 2013, 49(21): 101–105. doi: 10.3778/j.issn.1002-8331.1201-0401.

[10] 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. doi: 10.3724/SP.J.1146.2012.01102.

GUANG Yan, GU Chunxiang, ZHU Yuefei, *et al*. Certificateless fully homomorphic encryption based on LWE problem[J]. *Journal of Electronics & Information Technology*, 2013, 35(4): 988–993. doi: 10.3724/SP.J.1146.2012.01102.

[11] 古春生. 近似理想格上的全同态加密方案[J]. 软件学报, 2015, 26(10): 2696–2719. doi: 10.13328/j.cnki.jos.004808.

Gu Chunsheng. Fully homomorphic encryption from approximate ideal lattices[J]. *Journal of Software*, 2015, 26(10): 2696–2719. doi: 10.13328/j.cnki.jos.004808.

[12] 熊婉君, 韦永壮, 王会勇. 一个基于整数的全同态加密改进方案[J]. 密码学报, 2016, 3(1): 67–78. doi: 10.13868/j.cnki.jcr.000110.

XIONG Wanjun, WEI Yongzhuang, and WANG Huiyong. An improved fully homomorphic encryption scheme over the integers[J]. *Journal of Cryptologic Research*, 2016, 3(1): 67–78. doi: 10.13868/j.cnki.jcr.000110.

[13] HU Renyuan, ZHANG Longjun, and QIN Yongzhen. Improved fully homomorphic encryption algorithm for cloud storage[C]. International Conference on Communications, Information Management and Network Security, Shanghai, China, 2016: 349–352. doi: 10.19353/j.cnki.dzsj.2016.11.024.

[14] 夏超.同态加密技术及其应用研究[D]. [硕士论文], 安徽大学, 2013.

XIA Chao. Research of homomorphic encryption technolosgy and application[D]. [Master dissertation], Anhui University, 2013.

王彩芬：女，1963 年生，教授，博士生导师，研究方向为密码学与信息安全.

成玉丹：女，1992 年生，硕士生，研究方向为密码学与信息安全.

刘 超：男，1989 年生，硕士生，研究方向为密码学与信息安全.

赵 冰：男，1994 年生，硕士生，研究方向为密码学与信息安全.

许钦百：男，1992 年生，硕士生，研究方向为密码学与信息安全.